



System Management Services (SMS) 1.6 管理者マニュアル

Sun Fire™ ハイエンドシステム

Sun Microsystems, Inc.
www.sun.com

Part No. 819-6418-10
2006 年 6 月, Revision A

コメントの送付: <http://www.sun.com/hwdocs/feedback>

Copyright 2006 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

米国 Sun Microsystems, Inc. (以下、米国 Sun Microsystems 社とします)は、本書に記述されている技術に関する知的所有権を有しています。これら知的所有権には、<http://www.sun.com/patents>に掲載されているひとつまたは複数の米国特許、および米国ならびにその他の国におけるひとつまたは複数の特許または出願中の特許が含まれています。

本書およびそれに付属する製品は著作権法により保護されており、その使用、複製、頒布および逆コンパイルを制限するライセンスのもとにおいて頒布されます。サン・マイクロシステムズ株式会社による事前の許可なく、本製品および本書のいかなる部分も、いかなる方法によっても複製することが禁じられます。

本製品のフォント技術を含む第三者のソフトウェアは、著作権法により保護されており、提供者からライセンスを受けているものです。

本製品の一部は、カリフォルニア大学からライセンスされている Berkeley BSD システムに基づいていることがあります。UNIX は、X/Open Company Limited が独占的にライセンスしている米国ならびに他の国における登録商標です。

本製品は、株式会社モリサワからライセンス供与されたリュウミン L-KL (Ryumin-Light) および中ゴシック BBB (GothicBBB-Medium) のフォント・データを含んでいます。

本製品に含まれる HG 明朝 L と HG ゴシック B は、株式会社リコーがリョービマジクス株式会社からライセンス供与されたタイプフェイスマスタをもとに作成されたものです。平成明朝体 W3 は、株式会社リコーが財団法人日本規格協会 文字フォント開発・普及センターからライセンス供与されたタイプフェイスマスタをもとに作成されたものです。また、HG 明朝 L と HG ゴシック B の補助漢字部分は、平成明朝体 W3 の補助漢字を使用しています。なお、フォントとして無断複製することは禁止されています。

Sun、Sun Microsystems、Java、AnswerBook2、docs.sun.com、OpenBoot、Sun BluePrints、Sun Fire、Sunsolve は、米国およびその他の国における米国 Sun Microsystems 社の商標もしくは登録商標です。サンのロゴマークおよび Solaris は、米国 Sun Microsystems 社の登録商標です。

すべての SPARC 商標は、米国 SPARC International, Inc. のライセンスを受けて使用している同社の米国およびその他の国における商標または登録商標です。SPARC 商標が付いた製品は、米国 Sun Microsystems 社が開発したアーキテクチャーに基づくものです。

OPENLOOK、OpenBoot、JLE は、サン・マイクロシステムズ株式会社の登録商標です。

ATOK は、株式会社ジャストシステムの登録商標です。ATOK8 は、株式会社ジャストシステムの著作物であり、ATOK8 にかかる著作権その他の権利は、すべて株式会社ジャストシステムに帰属します。ATOK Server/ATOK12 は、株式会社ジャストシステムの著作物であり、ATOK Server/ATOK12 にかかる著作権その他の権利は、株式会社ジャストシステムおよび各権利者に帰属します。

本書で参照されている製品やサービスに関しては、該当する会社または組織に直接お問い合わせください。

OPEN LOOK および Sun™ Graphical User Interface は、米国 Sun Microsystems 社が自社のユーザーおよびライセンス実施権者向けに開発しました。米国 Sun Microsystems 社は、コンピュータ産業用のビジュアルまたはグラフィカル・ユーザーインターフェースの概念の研究開発における米国 Xerox 社の先駆者としての成果を認めるものです。米国 Sun Microsystems 社は米国 Xerox 社から Xerox Graphical User Interface の非独占的ライセンスを取得しており、このライセンスは米国 Sun Microsystems 社のライセンス実施権者にも適用されます。

U.S. Government Rights—Commercial use. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

本書は、「現状のまま」をベースとして提供され、商品性、特定目的への適合性または第三者の権利の非侵害の黙示の保証を含みそれに限定されない、明示的であるか黙示的であるかを問わない、なんらの保証も行われぬものとします。

本書には、技術的な誤りまたは誤植のある可能性があります。また、本書に記載された情報には、定期的に変更が行われ、かかる変更は本書の最新版に反映されます。さらに、米国サンまたは日本サンは、本書に記載された製品またはプログラムを、予告なく改良または変更することがあります。

本製品が、外国為替および外国貿易管理法(外為法)に定められる戦略物資等(貨物または役務)に該当する場合、本製品を輸出または日本国外へ持ち出す際には、サン・マイクロシステムズ株式会社の事前の書面による承諾を得ることのほか、外為法および関連法規に基づく輸出手続き、また場合によっては、米国商務省または米国所轄官庁の許可を得ることが必要です。

原典:	System Management Services (SMS) 1.6 Administrator Guide Part No: 819-4660-10 Revision A
-----	--



Adobe PostScript

目次

はじめに xxi

1. System Management Service の概要 1
 - Sun Fire ハイエンドシステム 1
 - 冗長な SC 2
 - SMS の機能 3
 - 前回の SMS リリースで提供された機能 5
 - SMS 1.6 リリースで提供された新機能 5
 - VCMON 5
 - システムアーキテクチャー 6
 - SMS 管理環境 6
 - 管理者のネットワーク接続 7
 - SMS オペレーティングシステム 8
 - ▼ SC を使用して開始する 8
 - SMS コンソールウィンドウ 11
 - ▼ コンソールウィンドウをローカルで表示する 11
 - チルドエスケープシーケンス 13
 - 遠隔コンソールセッション 14
 - Sun Management Center 15

2. SMS 1.6 のセキュリティー	17
ドメインセキュリティーの概要	18
システムコントローラのセキュリティーの概要	18
冗長システムコントローラ	19
SC ネットワークインタフェース	20
メイン SC ネットワークインタフェース	20
ドメイン - SC 通信 (scman0) インタフェース	20
SC - SC 通信 (scman1) インタフェース	21
スペア SC ネットワークインタフェース	21
メインとスペアのネットワークインタフェースの構成例	22
SMS 1.6 での変更	24
デフォルトでのセキュリティー保護 (新規インストール)	24
選択によりセキュリティー保護を行う (アップグレード)	24
インストール内容の変更	25
前提条件と制限事項	25
サポートの取得	26
smsinstall コマンドによる初期または新規の SMS インストール (デフォルトでのセキュリティー保護)	26
Solaris Security Toolkit のカスタマイズ	27
任意選択として行うドメインのセキュリティー保護	27
smsupgrade コマンドによる SMS のアップグレードインストール (選択によるセキュリティー保護)	27
任意選択として行うドメインのセキュリティー保護	28
Solaris Security Toolkit によるシステムコントローラのセキュリティー保護	28
Solaris Security Toolkit ソフトウェア	29
Solaris Security Toolkit ドライバのカスタマイズ	29
▼ I1 トラフィックを無効にする (ドメインの除外)	30
▼ FTP または Telnet を使用可能にする	31
▼ ドライバファイルの内容を表示する	31

▼ Solaris Security Toolkit の実行を解除する 32

3. SMS における管理特権 35

管理特権の概要 35

プラットフォーム管理者グループ 37

プラットフォームオペレータグループ 39

プラットフォーム保守グループ 39

ドメイン管理者グループ 41

ドメイン構成グループ 43

スーパーユーザーの特権 44

すべての特権のリスト 44

4. SMS の内部動作 51

起動のフロー 51

SMS デーモン 52

Capacity on Demand デーモン 56

ドメイン構成エージェント 57

ドメインステータス監視デーモン 58

ドメイン X サーバー 59

エラーおよび障害処理デーモン 60

イベントログアクセスデーモン 61

イベントレポートデーモン 62

環境ステータス監視デーモン 62

フェイルオーバー管理デーモン 63

FRU アクセスデーモン 64

ハードウェアアクセスデーモン 65

キー管理デーモン 67

管理ネットワークデーモン 71

メッセージロギングデーモン 72

OpenBoot PROM サポートデーモン	73
プラットフォーム構成データベースデーモン	74
プラットフォームの構成	75
ドメインの構成	76
システムボードの構成	77
SMS 起動デーモン	77
スクリプト	78
スペアモード	80
メインモード	80
ドメイン固有のプロセス起動	81
監視および再起動	81
SMS のシャットダウン	81
タスク管理デーモン	81
環境変数	82
5. SMS ドメイン構成	85
ドメイン構成ユニット	86
ドメイン構成の条件	86
DCU の割り当て	87
静的および動的なドメイン構成	87
グローバルな自動動的再構成	88
プラットフォーム管理者のための構成	88
使用可能構成要素リスト	89
▼ 使用可能構成要素リストを設定する	89
ドメインの構成	91
▼ コマンド行でドメイン名を命名または変更する	91
▼ コマンド行でドメインにボードを追加する	92
▼ コマンド行でドメインからボードを削除する	94
▼ コマンド行でドメイン間でボードを移動する	95

- ▼ ドメインのデフォルトを設定する 96
- ▼ ボードステータスを取得する 97
- ▼ ドメインステータスを取得する 99
- 仮想時刻 101
- 日時の設定 102
 - ▼ SC で日付を設定する 102
 - ▼ ドメイン eng2 で日付を設定する 102
 - ▼ SC で日付を表示する 102
 - ▼ ドメイン eng2 で日付を表示する 103
- NTP の構成 103
 - ▼ ntp.conf ファイルを作成する 103
- 仮想 ID PROM 106
 - flashupdate コマンド 106
- ドメイン管理者のための構成 106
 - ドメインの構成 107
 - ▼ コマンド行でドメインにボードを追加する 107
 - ▼ コマンド行でドメインからボードを削除する 109
 - ▼ コマンド行でドメイン間でボードを移動する 111
 - ▼ ドメインのデフォルトを設定する 113
 - ▼ ボードステータスを取得する 114
 - ▼ ドメインステータスを取得する 114
 - ▼ デバイスステータスを取得する 115
- 仮想キースイッチ 116
 - setkeyswitch コマンド 116
 - ▼ ドメイン A で仮想キースイッチを設定する 119
 - ▼ ドメイン A で仮想キースイッチ設定を表示する 119
- 仮想 NVRAM 119
 - OpenBoot PROM 変数の設定 120

- ▼ 周期的なドメインパニックから回復する 122
- ▼ ドメイン A で OpenBoot PROM のセキュリティーモード変数を設定する 123
- ▼ OpenBoot PROM 変数を確認する 123

機能が低下した構成の設定の変更 124

setbus コマンド 124

- ▼ すべてのアクティブドメインの全バスを両方の CSB で使用する 125

showbus コマンド 125

- ▼ すべてのアクティブドメインの全バスを表示する 125

6. 自動診断および自動回復 127

自動診断および自動回復の概要 127

ドメイン停止に関係するハードウェアエラー 128

致命的でないドメインハードウェアエラー 131

POST 検出ハードウェア障害 133

電子メールイベント通知の有効化 133

- ▼ 電子メールイベント通知を有効にする 135

電子メールテンプレートの設定 135

電子メール制御ファイルの設定 138

電子メールイベント通知のテスト 142

- ▼ 電子メールイベント通知をテストする 142

テスト電子メールの作成に失敗した場合の対処法 143

診断および回復情報の取得 144

診断イベントの確認 144

イベントログの確認 145

7. Capacity on Demand 147

COD の概要 148

COD ライセンス取得プロセス 148

COD RTU ライセンスの割り当て	149
インスタントアクセス CPU	150
ホットスペアとして使用するインスタントアクセス CPU	150
資源の監視	150
COD の開始	151
COD RTU ライセンスの管理	151
▼ COD RTU ライセンスキーを取得して COD ライセンスデータベースに追加する	151
▼ COD ライセンスデータベースから COD ライセンスキーを削除する	153
▼ COD ライセンス情報を表示する	153
COD 資源の起動	155
▼ インスタントアクセス CPU を使用可能にし、ドメイン RTU ライセンスを予約する	156
COD 資源の監視	158
COD システムボード	158
▼ COD システムボードを特定する	158
COD 資源使用状況	159
▼ 資源ごとに COD 使用状況を表示する	159
▼ ドメインごとに COD 使用状況を表示する	160
▼ 資源とドメインごとに COD 使用状況を表示する	162
構成解除された COD CPU とライセンスを受けていない COD CPU	164
その他の COD 情報	165
8. ドメイン制御	167
ドメインの起動	167
キースイッチ制御	168
電源制御	168
▼ システムボードの電源をコマンドラインから投入および切断する	168

▼ 電源障害から回復する	170
ドメインの要求による再起動	170
ASR (Automatic System Recovery: 自動システム回復)	171
ドメインの再起動	171
ドメインの中止またはリセット	172
ハードウェア制御	173
電源投入時自己診断 (POST)	173
ブラックリストの編集	174
プラットフォームおよびドメインのブラックリスト	174
▼ コンポーネントをブラックリストに登録する	175
▼ ブラックリストからコンポーネントを削除する	178
ASR ブラックリスト	180
電源制御	180
ファンの制御	181
ホットプラグ操作	181
取り外し	182
取り付け	183
SC のリセットおよび再起動	183
▼ メインまたはスペアの SC をリセットする	183
HPU の LED	183
9. ドメインサービス	187
管理ネットワークの概要	188
I1 ネットワーク	188
I2 ネットワーク	190
外部ネットワークの監視	191
MAN のデーモンとドライバ	193
管理ネットワークのサービス	193
ドメインコンソール	193

	メッセージロギング	195
	動的再構成	195
	ネットワーク起動および Solaris ソフトウェアのインストール	195
	SC のハートビート	196
10.	ドメインステータス関数	197
	ソフトウェアのステータス	197
	ステータスコマンド	198
	showboards コマンド	198
	showdevices コマンド	198
	showenvironment コマンド	198
	showobpparams コマンド	199
	showpcimode コマンド	199
	showplatform コマンド	199
	showxirstate コマンド	202
	Solaris ソフトウェアのハートビート	202
	ハードウェアのステータス	202
	ハードウェア構成	203
	環境ステータス	203
	▼ ドメイン A の環境ステータスを表示する	203
	ハードウェアエラーのステータス	204
	SC のハードウェアおよびソフトウェアのステータス	205
11.	ドメインイベント	207
	メッセージロギング	207
	ログファイルの維持管理	208
	ログファイルの管理	212
	ドメイン再起動イベント	213
	ドメイン再起動の初期化	213

ドメイン起動の障害	214
ドメインパニックイベント	215
ドメインパニック	215
ドメインパニックハング	216
反復ドメインパニック	216
Solaris ソフトウェアハングイベント	217
ハードウェア構成イベント	218
ホットプラグイベント	218
ホットアンプラグイベント	218
POST 初期化構成イベント	218
環境イベント	219
温度超過イベント	220
電源障害イベント	220
範囲外電圧イベント	221
電力不足イベント	221
ファン障害イベント	221
クロック障害イベント	221
ハードウェアエラーイベント	222
ドメイン停止イベント	223
CPU 検出イベント	223
レコード停止イベント	224
他の ASIC 障害イベント	224
SC 障害イベント	224
12. SC フェイルオーバー	225
概要	226
障害の監視	227
ファイルの伝達	228
フェイルオーバーの管理	229

起動	229
メイン SC	229
スペア SC	230
フェイルオーバーの CLI コマンド	230
setfailover コマンド	230
showfailover コマンド	232
コマンド同期	234
cmdsycn CLI	235
initcmdsycn コマンド	235
savecmdsycn コマンド	236
cancelcmdsycn コマンド	236
runcmdsync コマンド	236
showcmdsycn コマンド	236
データの同期	236
setdatasync コマンド	237
showdatasync コマンド	237
障害および回復	238
メイン SC のフェイルオーバー (メイン制御のフェイルオーバー)	239
メイン SC の障害 (スペアがメインの役割を引き継ぐ場合)	241
I2 ネットワークの障害	242
メイン SC の障害 (I2 ネットワークも停止している場合)	242
障害の回復および再起動	242
I2 障害の回復	243
再起動および回復	243
クライアントフェイルオーバーの回復	244
セキュリティ	245
13. SMS ユーティリティ	247
SMS バックアップユーティリティ	247

SMS 復元ユーティリティ	248
SMS バージョンユーティリティ	249
バージョンの切り替え	250
▼ 連続する 2 つの SMS バージョンが共存している場合に、バージョンを切り替える	251
SMS 構成ユーティリティ	252
UNIX グループ	252
アクセス制御リスト (ACL)	252
ネットワーク構成	253
MAN 構成	254
A. SMS マニュアルページ	255
B. エラーメッセージ	259
SMSHelp のインストール	259
▼ SUNWSMSjh パッケージをインストールする	259
▼ SMSHelp を起動する	260
エラーの種類	264
エラーのカテゴリ	264
用語集	267
索引	281

目次

図 3-1	プラットフォーム管理者の特権	38
図 3-2	プラットフォームオペレータの特権	39
図 3-3	プラットフォーム保守の特権	40
図 3-4	ドメイン管理者の特権	42
図 3-5	ドメイン構成者の特権	43
図 3-6	スーパーユーザーの特権	44
図 4-1	Sun Fire ハイエンドシステムのソフトウェアコンポーネント	53
図 4-2	CODD でのクライアントサーバーの関係	57
図 4-3	DCA でのクライアントサーバーの関係	58
図 4-4	DSMD でのクライアントサーバーの関係	59
図 4-5	DXS におけるクライアントサーバーの関係	60
図 4-6	EFHD におけるクライアントサーバーの関係	61
図 4-7	ELAD でのクライアントサーバーの関係	62
図 4-8	ERD におけるクライアントサーバーの関係	62
図 4-9	ESMD におけるクライアントサーバーの関係	63
図 4-10	FOMD におけるクライアントサーバーの関係	64
図 4-11	FRAD におけるクライアントサーバーの関係	65
図 4-12	HWAD におけるクライアントサーバーの関係	67
図 4-13	KMD におけるクライアントサーバーの関係	71
図 4-14	MAND におけるクライアントサーバーの関係	72

図 4-15	MLD におけるクライアントサーバーの関係	73
図 4-16	OSD におけるクライアントサーバーの関係	74
図 4-17	PCD におけるクライアントサーバーの関係	75
図 4-18	SSD におけるクライアントサーバーの関係	78
図 4-19	TMD におけるクライアントサーバーの関係	82
図 6-1	ドメイン停止に関係するハードウェアエラーに対する自動診断および自動回復プロセス	128
図 6-2	致命的でないドメインハードウェアエラーの自動診断プロセス	131
図 6-3	電子メールテンプレートと作成された電子メールの例	138
図 9-1	管理ネットワークの概要	188
図 9-2	Sun Fire E25K/15K の I1 ネットワークの概要	189
図 9-3	I2 ネットワークの概要	190
図 9-4	外部ネットワークの概要	191
図 12-1	フェイルオーバーの障害カテゴリ	239

表目次

表 1-1	チルドの使用法	13
表 3-1	すべてのグループ特権のリスト	45
表 4-1	デーモンおよびプロセス	54
表 4-2	環境変数の例	83
表 6-1	電子メールテンプレートファイルのイベントタグ	136
表 6-2	電子メール制御ファイルのパラメータ	140
表 6-3	エラーおよび障害イベント情報を表示する <code>showlogs(1M)</code> コマンドのオプション	146
表 7-1	COD ライセンス情報	154
表 7-2	COD 資源を構成するときの <code>setupplatform</code> コマンドのオプション	155
表 7-3	<code>showcodusage</code> で表示される資源情報	160
表 7-4	<code>showcodusage</code> で表示されるドメイン情報	161
表 7-5	COD のコンポーネント、構成、およびイベント情報の取得	165
表 8-1	Sun Fire ハイエンドサーバーに有効な <i>location</i>	177
表 8-2	Sun Fire ハイエンドサーバーに有効な <i>location</i>	179
表 10-1	ドメインステータスの種類	200
表 10-2	ドメインステータスの種類	201
表 11-1	SMS ログの種類に関する情報	209
表 11-2	MLD のデフォルト設定	212
表 12-1	フェイルオーバーの状態を変更するためのオプション	231
表 12-2	フェイルオーバーメカニズムの状態	233

表 12-3	showfailover の障害文字列	234
表 12-4	fomd によるハードウェアおよびソフトウェアの障害カテゴリ	238
表 12-5	フェイルオーバーの障害カテゴリ	239
表 13-1	SMS バージョン間の切り替え	249
表 B-1	エラーの種類	264
表 B-2	エラーのカテゴリ	264

コード例

- コード例 6-1 プラットフォームログファイルの Dstop と自動診断イベントメッセージの例 129
- コード例 6-2 Solaris により特定された致命的でないドメインハードウェアエラーと、ドメインイベントメッセージの例 132
- コード例 6-3 POST 自動診断イベントメッセージの例 133
- コード例 6-4 イベント電子メールの例 134
- コード例 6-5 デフォルトのサンプル電子メールテンプレート 135
- コード例 6-6 電子メール制御ファイル (event_email.cf) 139
- コード例 6-7 電子メール制御ファイルの例 141

はじめに

『System Management Services (SMS) 1.6 管理者マニュアル』では、SMS ソフトウェアに関連する各種の管理および監視タスクの実行方法について説明します。

お読みになる前に

このマニュアルは、UNIX® システム、特に Solaris™ オペレーティングシステム (Solaris OS) に基づく UNIX システムに関する実務的知識のある Sun Fire™ ハイエンドシステム管理者を対象としています。そのような知識がない場合は、使用しているシステムに付属の Solaris ユーザーおよびシステム管理者向けのマニュアルをお読みください。また、UNIX システム管理のトレーニングの受講を検討してください。

次世代の Sun Fire サーバーファミリの製品はすべて、疎結合クラスタとして構成できます。ただし、このマニュアルでは、Sun Fire ハイエンドシステムのクラスタ構成のシステム管理については説明しません。

マニュアルの構成

このマニュアルは次の章で構成されています。

第 1 章では、System Management Services ソフトウェアの概要と、そのコマンド行インタフェースについて説明します。

第 2 章では、ドメインおよびシステムコントローラ上のセキュリティーについて説明します。

第 3 章では、管理者特権について説明します。

第 4 章では、SMS ドメインの内部動作と、その使用方法について説明します。

第 5 章では、ドメインの構成、オプション、および手順について説明します。

第 6 章では、自動診断機能およびドメイン回復機能について説明します。

第 7 章では、Capacity on Demand (COD) について説明します。

第 8 章では、制御機能について説明します。

第 9 章では、使用可能なネットワークサービスと、その使用方法について説明します。

第 10 章では、ステータスの監視について説明します。

第 11 章では、イベントの監視について説明します。

第 12 章では、システムコントローラ (SC) のフェイルオーバーについて説明します。

第 13 章では、バックアップの作成と復元、ネットワークとユーザーグループの構成、および SMS ソフトウェアのアップグレードに使用される SMS ユーティリティーについて説明します。

付録 A では、SMS のマニュアルページのリストを示します。

付録 B では、SMS のエラーメッセージについて説明します。

UNIX コマンド

このマニュアルには、システムの停止、システムの起動、およびデバイスの構成などに使用する基本的な UNIX コマンドと操作手順に関する説明は含まれていない可能性があります。これらについては、以下を参照してください。

- 使用しているシステムに付属のソフトウェアマニュアル
- 下記にある Solaris オペレーティングシステム (OS) のマニュアル

<http://docs.sun.com>

書体と記号について

書体または記号	意味	例
AaBbCc123	コマンド名、ファイル名、ディレクトリ名、画面上のコンピュータ出力、コード例。	.login ファイルを編集します。 ls -a を実行します。 % You have mail.
AaBbCc123	ユーザーが入力する文字を、画面上のコンピュータ出力と区別して表します。	% su Password:
<i>AaBbCc123</i>	コマンド行の可変部分。実際の名前や値と置き換えてください。	rm <i>filename</i> と入力します。
『 』	参照する書名を示します。	『Solaris ユーザーマニュアル』
「 」	参照する章、節、または、強調する語を示します。	第 6 章「データの管理」を参照。 この操作ができるのは「スーパーユーザー」だけです。
\	枠で囲まれたコード例で、テキストがページ行幅を超える場合に、継続を示します。	% grep `^#define` \ XV_VERSION_STRING'

シェルプロンプトについて

シェル	プロンプト
UNIX の C シェル	sc_name:sms-user:> または domain_id:sms-user:>
UNIX の Bourne シェルと Korn シェル	>
スーパーユーザー (シェルの種類を問わない)	#

関連マニュアル

SMS のマニュアルは、次の URL で参照できます。

http://www.sun.com/products-n-solutions/hardware/docs/Servers/High-End_Servers/Sun_Fire_e25K-e20K/SW_FW_Documentation/SMS/index.html

その他のマニュアルについては、次に示すページの「検索」にマニュアル名を入力すると検索できます。

<http://www.sun.com/documentation/>

用途	タイトル	Part No.	形式	場所
ソフトウェアの概要	『Sun Fire ハイエンドシステムソフトウェアの概要』	819-6409-10	PDF HTML	オンライン
インストール	『System Management Services (SMS) 1.6 インストールマニュアル』	819-6414-10	PDF HTML	オンライン
リファレンス (マニュアルページ)	『System Management Services (SMS) 1.6 リファレンスマニュアル』	819-6419-10	PDF HTML	オンライン
ご使用にあたって	『System Management Services (SMS) 1.6 ご使用にあたって』	819-6421-10	PDF HTML	オンライン
動的再構成	『Sun Fire ハイエンド/ミッドレンジシステム Dynamic Reconfiguration ユーザーマニュアル』	819-3187-10	PDF HTML	オンライン
OpenBoot	『OpenBoot™ 4.x Command Reference Manual』	816-1177-10	PDF HTML	オンライン
サイト計画	『Sun Fire 15K/12K システムサイト計画の手引き』	817-3201-10	PDF HTML	オンライン
セキュリティー	『Solaris Security Toolkit 4.2 管理マニュアル』	819-3789-10	PDF HTML	オンライン
セキュリティー	『Solaris Security Toolkit 4.2 リファレンスマニュアル』	819-3793-10	PDF HTML	オンライン

用途	タイトル	Part No.	形式	場所
セキュリティ	『Solaris Security Toolkit 4.2 ご使用にあたって』	819-3796-10	PDF HTML	オンライン
セキュリティ	『Solaris Security Toolkit 4.2 マニュアルページガイド』	819-3794-10	PDF HTML	オンライン
Solaris 10 OS IP サービス	『Solaris のシステム管理 (IP サービス)』	819-0380	PDF HTML	オンライン

マニュアル、サポート、およびトレーニング

Sun のサービス	URL
マニュアル	http://www.sun.com/documentation/
サポート	http://jp.sun.com/support/
トレーニング	http://jp.sun.com/training/

Sun 以外の Web サイト

このマニュアルで紹介する Sun 以外の Web サイトが使用可能かどうかについては、Sun は責任を負いません。このようなサイトやリソース上、またはこれらを経由して利用できるコンテンツ、広告、製品、またはその他の資料についても、Sun は保証しておらず、法的責任を負いません。また、このようなサイトやリソース上、またはこれらを経由して利用できるコンテンツ、商品、サービスの使用や、それらへの依存に関連して発生した実際の損害や損失、またはその申し立てについても、Sun は一切の責任を負いません。

コメントをお寄せください

マニュアルの品質改善のため、お客様からのご意見およびご要望をお待ちしております。コメントは下記よりお送りください。

<http://www.sun.com/hwdocs/feedback>

ご意見をお寄せいただく際には、下記のタイトルと Part No. を記載してください。

『System Management Services (SMS) 1.6 管理者マニュアル』、Part No. 819-6418-10

第1章

System Management Service の概要

このマニュアルでは、Sun Fire ハイエンドサーバーシステムの System Management Services (SMS) 1.6 ソフトウェアについて説明します。

この章では、以下の項目を説明します。

- 1 ページの「Sun Fire ハイエンドシステム」
- 3 ページの「SMS の機能」
- 6 ページの「システムアーキテクチャー」
- 6 ページの「SMS 管理環境」
- 15 ページの「Sun Management Center」

Sun Fire ハイエンドシステム

Sun Fire ハイエンドシステムのシステムコントローラ (SC) は CP1500 または CP2140 ベースの多機能なプリント回路基板 (PCB) で、Sun Fire システムの操作および制御に必須の重要なサービスと資源を提供します。

Sun Fire ハイエンドシステムは、「プラットフォーム」とも呼ばれます。プラットフォーム内にあるシステムボードは、個別に起動できる複数のシステム (「動的システムドメイン」または単に「ドメイン」と呼びます) に論理的にグループ化できません。

単一の Sun Fire システムで同時に存在できるドメインの数は、E25K および 15K では 18 個まで、E20K および 12K では 9 個までです。この章ではドメインの概要を説明します。詳細な説明については、第 5 章を参照してください。SMS ソフトウェアを使うと、プラットフォーム自体と同様にドメインも制御および監視の対象にすることができます。

SC は、Sun Fire システムに対して次のようなサービスを提供します。

- システム構成全体を管理します。
- システムドメインの起動イニシエータとして動作します。
- システムドメインの `syslog` (システムログ) ホストとして機能します。SC は、LAN 規模の `syslog` ホストの `syslog` クライアントとすることも可能であることに注意してください。
- 同期ハードウェアクロックソースを提供します。
- 動的ドメインの設定と構成を行います。
- システム環境情報 (電源、ファン、温度の状態など) を監視します。
- 現場交換可能ユニット (FRU、Field-Replaceable Unit) のログデータを集中管理します。
- デュアル SC 構成での冗長性と自動 SC フェイルオーバーを提供します。
- 仮想ホスト ID に基づいてドメインのデフォルトネームサービスを提供するとともに、ドメインの MAC アドレスを提供します。
- プラットフォーム管理用の管理役割を提供します。

冗長な SC

1 台の Sun Fire プラットフォームには 2 つの SC があります。Sun Fire プラットフォームを制御する SC は「メイン SC」と呼ばれ、バックアップとして動作するもう一方の SC は「スペア SC」と呼ばれます。メイン SC で動作するソフトウェアは両方の SC を監視して、自動フェイルオーバーを実行すべきタイミングを判断します。

2 つの SC を同じ構成にします。同じ構成にするものには、Solaris オペレーティングシステム (OS)、SMS ソフトウェア、セキュリティの変更、パッチのインストールなど、あらゆるシステム構成が含まれます。

注 - フェイルオーバーをサポートするには、両方の SC を同じバージョンの Solaris OS および SMS ソフトウェアで構成してください。

SC 間のフェイルオーバー機能は、メイン SC とスペア SC で動作するデーモンによって制御されます。これらのデーモンは、Sun Fire プラットフォーム内に組み込まれたプライベート通信パスを介して通信します。このようなデーモンの通信以外に、2 つの SC 間に特別な信頼関係はありません。

SMS ソフトウェアパッケージは、SC にインストールされます。また、SMS は Ethernet 接続を介して Sun Fire ハイエンドシステムと通信します。193 ページの「管理ネットワークのサービス」を参照してください。

注 – SMS 1.6 は、I2 ネットワーク上で SMS 1.4.1 と通信することはできません。一方の SC で SMS 1.4.1 が動作し、他方の SC で SMS 1.6 が動作している場合は、I2 ネットワークテストで問題が発見されます。この場合、これらの SC は高可用 SRAM (HASRAM) を介して通信を行います。I2 ネットワークの詳細は、190 ページの「I2 ネットワーク」を参照してください。

SMS の機能

SMS 1.6 は、Solaris 8 2/04、Solaris 9 4/04、Solaris 10 3/05、Solaris 10 1/06、および Solaris 10 6/06 OS が動作している Sun Fire ハイエンドドメインをサポートしています。また、SMS 1.6 は、システムコントローラ上の Solaris 10 1/06、Solaris 10 6/06、Solaris 9 4/04、Solaris 9 9/04、および Solaris 9 9/05 OS をサポートしています。SMS ソフトウェアに含まれている各コマンドは、遠隔から実行できます。

注 – SMS 1.6 に対してサポートされているファームウェアバージョンは、5.2.0 です。

注 – SMS の多くのコマンドのグラフィカルユーザーインターフェースは、SunTM Management Center により提供されます。詳細は、15 ページの「Sun Management Center」を参照してください。

SMS を使用すると、「プラットフォーム」管理者は次のタスクを実行できます。

- 「ドメイン構成ユニット」(DCU) を論理的にグループ化して、複数のドメインを管理します。DCU は、CPU ボードおよび I/O ボードなどのシステムボードです。ドメインは、独自に OS を実行して自身の作業負荷を処理できます。第 5 章を参照してください。
- ドメインを動的に再構成することで、ドメインがマルチユーザーモードで動作を継続したまま、現在インストールされているシステムボードを OS と論理的に接続したり切り離したりすることができます。この機能は「動的再構成」と呼ばれます。詳細については、『System Management Services (SMS) 1.6 Dynamic Reconfiguration ユーザーマニュアル』を参照してください。システムボードは、ドメインに接続されていなければ物理的に脱着でき、その間もシステムはマルチユーザーモードで実行できます。
- スクリプトを使用して、ドメインに対して自動化された動的再構成を実行します。詳細については、『System Management Services (SMS) 1.6 Dynamic Reconfiguration ユーザーマニュアル』を参照してください。

- 1つ、または複数のシステムボードやドメインの温度、電流レベル、および電圧レベルを監視および表示します。
- プラットフォーム内のコンポーネントへの電源供給を監視および制御します。
- 電源投入時自己診断 (POST) などの診断プログラムを実行します。

また、SMS は以下のタスクも実行できます。

- プラットフォーム管理者に、電源装置の過熱または故障など、差し迫った障害の警告を發します。
- プラットフォーム管理者に、ソフトウェアのエラーまたは障害が発生したことを通知します。
- 単独ポイントの障害がないかを調べるためにデュアル SC 構成を監視し、検出された障害の状況に応じて、メイン SC からスペアへフェイルオーバーを自動的に実行します。
- システムソフトウェアの障害 (たとえばパニック) の後で、ドメインを自動的に再起動します。
- SC 環境とドメインの間の対話を記録します。
- Sun Fire ハイエンドシステムのデュアルグリッド電源オプションをサポートします。

SMS を使用すると、「ドメイン」管理者は次のタスクを実行できます。

- 「ドメイン構成ユニット」(DCU) を論理的にグループ化して、複数のドメインを管理します。DCU は、CPU ボードおよび I/O ボードなどのシステムボードです。ドメインは、独自に OS を実行して自身の作業負荷を処理できます。第 5 章を参照してください。
- 管理者が特権を持っているドメインを起動します。
- 管理者が特権を持っているドメインを動的に再構成することで、ドメインがマルチユーザーモードで動作を継続したまま、現在インストールされているシステムボードを OS と論理的に接続したり切り離したりすることができます。この機能は「動的再構成」と呼ばれます。詳細については、『System Management Services (SMS) 1.6 Dynamic Reconfiguration ユーザーマニュアル』を参照してください。システムボードは、ドメインに接続されていなければ物理的に脱着でき、その間もシステムはマルチユーザーモードで実行できます。
- スクリプトを使用して、管理者が特権を持つドメインに対して自動化された動的再構成を実行します。詳細については、『System Management Services (SMS) 1.6 Dynamic Reconfiguration ユーザーマニュアル』を参照してください。
- 管理者が特権を持つ 1 つ、または複数のシステムボードやドメインの温度、電流レベル、および電圧レベルを監視および表示します。
- 管理者が特権を持つ、電源投入時自己診断 (POST) などの診断プログラムを実行します。

前回の SMS リリースで提供された機能

前回の SMS リリースでは次の機能が提供されました。

- 動的なシステムドメイン (DSD) 構成
- 構成済みドメインサービス
- ドメイン制御機能
- 自動診断および自動ドメイン回復
- Capacity on Demand (COD)
- ドメインステータスのレポート
- ハードウェア制御機能
- ハードウェアステータスの監視、レポート、および処理
- ハードウェアエラーの監視、レポート、および処理
- システムコントローラ (SC) のフェイルオーバー
- 構成可能な管理者特権
- 動的 FRUID

SMS 1.6 リリースで提供された新機能

SMS 1.6 では、次の新機能が提供されています。

- ドメインにおける Solaris 10 OS 以降のサポート
- システムコントローラ上の Solaris 10 1/06 および 6/06 OS のサポート
- UltraSPARC® IV 1.65 GHz プロセッサのサポート
- UltraSPARC IV+ 1.8 GHz プロセッサのサポート準備
- 電圧コア監視 (VCMON)
- 2G バイト DIMM
- 改善されたメモリーリフレッシュ速度
- システムコントローラに対するデフォルトのセキュリティー保護
- Solaris Security Toolkit 4.2 のサポート
- Availability (AVL) 2.0 FS-2 ソフトウェアのサポート (Solaris 10 6/06 が必要)
 - UltraSPARC IV+ プロセッサ診断拡張機能
 - アンカー付きページリタイア
 - データパス診断調整 (ドメイン FMA および SC)
 - サポートされているプラットフォーム: UltraSPARC III エンタープライズサーバー、Sun Fire V1280 および Netra 1280 と、Sun Fire 15K ファミリー

VCMON

SMS ソフトウェアに電圧コア監視パラメータ (VCMON) が追加されました。VCMON を有効にすると、プロセッサの電圧変化 (ドリフト) が監視されます。電圧の上昇を検知すると (これは、通常、ソケット接続に関連した問題があることを示す)、VCMON はユーザーに FMA イベントの発生を通知し、そのプロセッサのコンポーネント健全状態 (CHS) を *faulty* (障害あり) とマークします。

システムアーキテクチャー

SMS は、分散型クライアントサーバーアーキテクチャーを使用します。init(1M) が、1 つの `ssd(1M)` プロセスを起動します (必要に応じて再起動する)。ssd は、他のすべての SMS プロセスを監視し、必要に応じて再起動します。図 4-1 を参照してください。

Sun Fire ハイエンドシステムプラットフォーム、SC、および他のワークステーションは Ethernet を介して通信します。SMS の操作を行うには、ローカルエリアネットワーク (LAN) 上のほかのワークステーションから SC に遠隔ログインして、SC コンソール上でコマンドを入力します。SMS の操作 (たとえば、プラットフォームの監視および制御) を行うには、そのプラットフォームまたはドメインの適切な特権を持つユーザーとしてログインする必要があります。

注 – メイン SC 上の SMS を停止して、スペア SC の電源を切断すると、ドメインが正常にシャットダウンされて、プラットフォームの電源が切断されます。SMS を停止せずにそのままスペア SC の電源を切断すると、SMS がプラットフォームの電源を切断する時間がなくなるため、ドメインがクラッシュします。

デュアルシステムコントローラは、Sun Fire ハイエンドシステムプラットフォーム内でサポートされています。一方の SC がプライマリまたはメインのシステムコントローラに指定され、他方がスペアのシステムコントローラになります。メイン SC に障害が発生すると、フェイルオーバー機能が自動的にスペア SC に切り換えます。詳細については第 12 章を参照してください。

ほとんどのドメイン構成ユニットはアクティブコンポーネントです。つまり、DCU の電源を切断する場合は切断前にシステムの状態を確認する必要があります。



注意 – 拡張ボードなどのボードを取り付けている場合は、ボードの電源投入または切断の状態に関係なく常に回路ブレーカをオンにしておいてください。

詳細は、180 ページの「電源制御」を参照してください。

SMS 管理環境

Sun Fire ハイエンドシステムでの管理タスクのセキュリティは、グループ特権の要件により保護されます。SMS は、次に示す 39 個の UNIX グループを `/etc/group` ファイルにインストールします。

- platadmn - プラットフォームの管理者
- platoper - プラットフォームのオペレータ
- platsvc - プラットフォームの保守担当者
- dmn[A...R]admn - ドメイン [domain-id | domain-tag] の管理者 (18 個)
- dmn[A...R]rcfg - ドメイン [domain-id | domain-tag] の構成者 (18 個)

管理者は `smsconfig(1M)` を使用して、プラットフォームおよびドメインのグループのメンバーの追加、削除、および一覧表示を実行できます。また、`-a`、`-r`、および `-l` オプションを使用して、プラットフォームおよびドメインのディレクトリ特権を設定できます。

また `smsconfig` では、`-g` オプションを使用して、NIS (ネットワーク情報サービス) の管理対象であるグループなどの別のグループ名を使用するように SMS を構成できます。グループ情報のエント리는、`/etc/nsswitch.conf` ファイルに指定されている任意のソースから取得できます (`nsswitch.conf(4)` を参照してください)。たとえば、ドメイン A のドメインタグが **Production Domain** である場合、管理者は同名の NIS グループを作成して、NIS グループの方を、デフォルトの `dmnaadmn` の代わりにドメイン A 管理者グループとして使用するように SMS を構成できます。詳細は、第 3 章および `smsconfig` のマニュアルページを参照してください。

管理者のネットワーク接続

サポートされている管理モデル (複数の管理特権および複数の管理者) だけでなく、システムコントローラが組み込まれているという Sun Fire ハイエンドシステムの物理的アーキテクチャーの性質のより、Sun Fire ハイエンドシステムを管理するには、管理者はワークステーションからの遠隔ネットワーク接続を使用して、SMS コマンドインタフェースに接続します。



注意 – Sun Fire ハイエンドシステムの SC への `tip` セッションがアクティブであるときに遠隔ワークステーションを停止すると、両方の SC が停止し、**OpenBoot™** の `ok` プロンプトが表示されます。これはドメインには影響を与えないため、遠隔システムの電源を再度投入してから、`ok` プロンプトで `go` と入力すると、SC を復元できます。ただし、遠隔ワークステーションを停止する前には、すべての `tip` セッションを終了するようにしてください。

管理者自身を識別するための情報 (パスワード) が提供され、要注意のデータが表示される可能性もあるので、遠隔ネットワーク接続のセキュリティーを確保することが重要です。管理用のネットワークを物理的に分離することで、Sun Fire ハイエンドシステム上でのセキュリティーが提供されます。各 SC では、複数の物理的な外部ネットワーク接続を使用できます。SMS ソフトウェアは外部ネットワーク接続を 2 本までサポートします。

Sun Fire ハイエンドシステムのネットワークについての詳細は、193 ページの「管理ネットワークのサービス」を参照してください。Sun Fire ハイエンドシステムのセキュリティ保護の詳細は、第 2 章の 28 ページの「Solaris Security Toolkit によるシステムコントローラのセキュリティ保護」を参照してください。

SMS オペレーティングシステム

SMS では、プログラムに含まれるさまざまな機能をコマンド行インタフェース (CLI) から使用できます。CLI コマンドを使用して、SC、およびシステム上のドメインを操作できます。

このマニュアルの例では、*sc-name* は `sc0` であり、*sms-user* はシステムにログインしている管理者、オペレータ、構成者、または保守担当者の *user-name* です。

ユーザーに割り当てられる特権は、ユーザーがどのプラットフォームまたはドメインのグループに属するかにより決まります。この例では、特に断らないかぎり、*sms-user* はプラットフォームおよびドメインの管理者特権の両方を持っているものと仮定します。

SMS ユーザーグループの機能および作成の詳細については、第 3 章と『System Management Services (SMS) 1.6 インストールマニュアル』を参照してください。

▼ SC を使用して開始する

1. SC を起動します。

注 – この手順では、`smsconfig -m` がすでに実行されているものと仮定します。`smsconfig -m` がまだ実行されていないと、SMS の開始を試みた時点で次のエラーが表示され、SMS は終了します。

```
sms: smsconfig(1M) has not been run. Unable to start sms services.
```

2. SC にログインして、SMS ソフトウェアの起動が完了したことを確認します。次のように入力します。

```
sc0:sms-user:> showplatform
```

プラットフォーム特権を持っている場合は、次のような出力が表示されます。

```
sc0:sms-user:> showplatform

PLATFORM:
=====
Platform Type: Sun Fire 15000

CSN:
====
Chassis Serial Number: 353A00053

COD:
====
Chassis HostID : 5014936C37048
PROC RTUs installed : 8
PROC Headroom Quantity : 0
PROC RTUs reserved for domain A : 4
PROC RTUs reserved for domain B : 0
PROC RTUs reserved for domain C : 0
PROC RTUs reserved for domain D : 0
PROC RTUs reserved for domain E : 0
PROC RTUs reserved for domain F : 0
PROC RTUs reserved for domain G : 0
PROC RTUs reserved for domain H : 0
PROC RTUs reserved for domain I : 0
PROC RTUs reserved for domain J : 0
PROC RTUs reserved for domain K : 0
PROC RTUs reserved for domain L : 0
PROC RTUs reserved for domain M : 0
PROC RTUs reserved for domain N : 0
PROC RTUs reserved for domain O : 0
PROC RTUs reserved for domain P : 0
PROC RTUs reserved for domain Q : 0
PROC RTUs reserved for domain R : 0

Available Component List for Domains:
=====
Available for domain newA:
    SB0 SB1 SB2 SB7
    IO1 IO3 IO6
Available for domain engB:
    No System boards
    No IO boards
Available for domain domainC:
    No System boards
    IO0 IO1 IO2 IO3 IO4
Available for domain eng1:
    No System boards
    No IO boards
```

```

Available for domain E:
    No System boards
    No IO boards
Available for domain domainF:
    No System boards
    No IO boards
Available for domain dmnG:
    No System boards
    No IO boards
Available for domain domain H:
    No System boards
    No IO boards
Available for domain I:
    No System boards
    No IO boards
Available for domain dmnJ:
    No System boards
    No IO boards
Available for domain K:
    No System boards
    No IO boards
Available for domain L:
    No System boards
    No IO boards
Available for domain M:
    No System boards
    No IO boards
Available for domain N:
    No System boards
    No IO boards
Available for domain O:
    No System boards
    No IO boards
Available for domain P:
    No System boards
    No IO boards
Available for domain Q:
    No System boards
    No IO boards
Available for domain dmnR:
    No System boards
    No IO boards

```

Domain Ethernet Addresses:

```

=====
Domain ID   Domain Tag   Ethernet Address
A           newA        8:0:20:b8:79:e4
B           engB        8:0:20:b4:30:8c
C           domainC     8:0:20:b7:30:b0
D           -           8:0:20:b8:2d:b0
E           eng1        8:0:20:f1:b7:0
F           domainF     8:0:20:be:f8:a4
G           dmnG        8:0:20:b8:29:c8
H           -           8:0:20:f3:5f:14
I           -           8:0:20:be:f5:d0
J           dmnJ        UNKNOWN
K           -           8:0:20:f1:ae:88
L           -           8:0:20:b7:5d:30
M           -           8:0:20:f1:b8:8

```

```

N           -           8:0:20:f3:5f:74
O           -           8:0:20:f1:b8:8
P           -           8:0:20:b8:58:64
Q           -           8:0:20:f1:b7:ec
R           dmnR        8:0:20:f1:b7:10

```

Domain Configurations:

=====

DomainID	Domain Tag	Solaris Nodename	Domain Status
A	newA	-	Powered Off
B	engB	sun15-b	Keyswitch Standby
C	domainC	sun15-c	Running OBP
D	-	sun15-d	Running Solaris
E	eng1	sun15-e	Running Solaris
F	domainF	sun15-f	Running Solaris
G	dmnG	sun15-g	Running Solaris
H	-	sun15-g	Solaris Quiesced
I	-	-	Powered Off
J	dmnJ	-	Powered Off
K	-	sun15-k	Booting Solaris
L	-	-	Powered Off
M	-	-	Powered Off
N	-	sun15-n	Keyswitch Standby
O	-	-	Powered Off
P	-	sun15-p	Running Solaris
Q	-	sun15-q	Running Solaris
R	dmnR	sun15-r	Running Solaris

この時点で、SMS プログラムの使用を開始できます。

SMS コンソールウィンドウ

SMS コンソールウィンドウは、SC からドメイン上の Solaris OS へのコマンド行インタフェースを提供します。

▼ コンソールウィンドウをローカルで表示する

1. まだログインしていない場合は、SC にログインします。

注 - console を実行するドメインについてのドメイン特権が必要です。

2. 次のように入力します。

```
sc0:sms-user:> console -d domain-indicator option
```

ここで次の点に留意します。

-d *domain-indicator* を使用するドメインを指定します。

domain-id - ドメインの ID。有効な *domain-id* は、A ~ R で、大文字と小文字は区別されません。

domain-tag - *addtag(1M)* を使用してドメインに割り当てた名前。

-f **Force**

ドメインコンソールウィンドウをロックされた書き込み特権でオープンし、オープンしている他のセッションをすべて終了し、新しいセッションがオープンされないようにします。これにより、セッションが排他になります。このコマンドは、コンソールを排他的に使用する必要があるとき（たとえば、専有的なデバッグ処理）にだけ使用してください。複数セッションモードを復元するには、ロックを解放 (~^) するか、コンソールセッションを終了 (~.) します。

-g **Grab**

コンソールウィンドウをロック解除された書き込み特権でオープンします。ほかのセッションに「ロックなしの書き込み」権がある場合は、新しいコンソールウィンドウにより権利が奪われます。ほかのセッションにロック権がある場合、**Grab** による要求は拒否されて読み取り専用のセッションが開始されます。

-l **Lock**

コンソールウィンドウをロックされた書き込み特権でオープンします。ほかのセッションに「ロックなしの書き込み」権がある場合は、新しいコンソールウィンドウにより権利が奪われます。ほかのセッションにロック権がある場合、要求は拒否されて読み取り専用のセッションが開始されます。

-r **Read Only**

コンソールウィンドウを読み取り専用モードでオープンします。

`console` コマンドはドメインの仮想 `console` ドライバへの遠隔接続を作成し、コマンドを実行するためのウィンドウを、指定されたドメイン (*domain-id* または *domain-tag*) のコンソールウィンドウにします。

ドメインでコンソールウィンドウが開いていないときに `console` がオプションなしで起動された場合、コンソールウィンドウは排他的な「ロックされた書き込み」モードのセッションとして開きます。

ドメインで 1 つ以上の排他的でないコンソールウィンドウが実行中のときに `console` がオプションなしで起動された場合、コンソールウィンドウは読み取り専

用モードで表示されます。

ロックされた書き込み権の方が、セキュリティー保護が強力です。ロックされた書き込み権が削除されるのは、他のコンソールが `console -f` で開かれた場合か、実行中の他のコンソールウィンドウで `~*` (チルドアスタリスク) が入力された場合だけです。どちらの場合も、新しいコンソールのセッションは「排他的なセッション」で、ほかのすべてのセッションは強制的にドメインの仮想コンソールから切り離されません。

`console` コマンドは、IOSRAM (Input Output Static Random Access Memory) または内部管理ネットワークのいずれかを使用して、ドメイン内のコンソール通信を行うことができます。通信パスを手動で切り替えるには、`~=` (チルド等号) コマンドを使用します。この方法は、ネットワークが操作できなくなり、コンソールセッションがハングアップしたように思われる場合に便利です。

ドメインには同時に多数のコンソールセッションを接続できますが、書き込み権を持つコンソールは 1 つだけです。その他のすべてのコンソールは、読み取り専用権を持ちます。書き込み権は、ロックまたはロック解除のいずれかのモードになります。

チルドエスケープシーケンス

ドメインコンソールウィンドウでの行の 1 文字めにチルド (`~`) が入力されると、次の表に示すような特別な動作の実行をコンソールに指示するエスケープ信号として解釈されます。

表 1-1 チルドの使用法

文字	説明
<code>~?</code>	ステータスメッセージ
<code>~.</code>	コンソールセッションの切断。
<code>~#</code>	OpenBoot PROM または <code>kadb</code> へのブレイク。
<code>~@</code>	ロックなしの書き込み権を取得。オプション <code>-g</code> を参照してください。
<code>~^</code>	書き込み権の解放。
<code>~=</code>	通信パスをネットワークと IOSRAM の間で切り換え。 <code>~=</code> は、専有モードでだけ使用可能 (<code>~*</code> を参照)
<code>~&</code>	ロックされた書き込み権を獲得。オプション <code>-l</code> を参照。この信号は、読み取り専用、またはロック解除された書き込みのセッションでのみ実行することができます。
<code>~*</code>	ロックされた書き込み権を獲得し、開いているほかのセッションをすべて終了してから、新しいセッションの開始を禁止します。オプション <code>-f</code> を参照。多重セッションモードを復元するには、ロックを開放するか、またはこのセッションを終了します。

rlogin コマンドも、新しい行の先頭にチルドがあれば、チルドエスケープシーケンスを処理します。行の先頭でチルドシーケンスを送信する必要があり、かつ rlogin を使用して接続している場合には、チルドを 2 個指定します (1 番目のチルドはエスケープされ、2 番目が rlogin のチルドになります)。あるいは、rlogin のウィンドウで実行する場合には、行の先頭にチルドを入力しないでください。

コンソールセッションを終了するために `kill -9` コマンドを使用する場合、`console` コマンドが実行されたウィンドウまたは端末は `raw` モードになり、ハングアップしたように見えます。この状態をエスケープするには、`CTRL-J` を押し、次に `stty sane` と入力して、さらに `CTRL-J` を押します。

ドメインコンソールウィンドウで、`vi(1)` が正常に実行され、エスケープシーケンス (チルド付きのコマンド) が意図のとおり動作するのは、環境変数 `TERM` の設定がコンソールウィンドウの設定と同じである場合だけです。

たとえば、次のメッセージが表示されます。

```
sc0:sms-user:> setenv TERM xterm
```

ウィンドウのサイズを変更するには、次のように入力します。

```
sc0:sms-user:> stty rows 20 cols 80
```

ドメインコンソールの詳細については、第 9 章、および `console` のマニュアルページを参照してください。

遠隔コンソールセッション

システムコントローラがハングアップしてコンソールを直接操作できない場合に備えて、SMS には、ハングアップした SC に遠隔接続するための `smsconnectsc` コマンドがあります。このコマンドは、メイン SC またはスベア SC のどちらからでも操作できます。`smsconnectsc` コマンドの詳細および例については、`smsconnectsc` のマニュアルページを参照してください。

外部コンソール接続を使用してハングアップした SC に接続することもできますが、外部コンソールを使用し、同時に `smsconnectsc` コマンドを実行することはできません。

Sun Management Center

Sun Fire ハイエンドシステムの Sun Management Center は、クライアントサーバーの考え方に基づいて、標準的な SNMP (ネットワーク管理プロトコル) ベースの管理構造をインテリジェントで自立的な新しいエージェント技術および管理技術に統合する高度な監視および管理ツールです。

Sun Management Center は、Sun Fire システムのグラフィカルユーザーインターフェース (GUI) および SNMP 管理エージェントのインフラストラクチャーとして使用します。Sun Management Center のこうした特長と機能の説明は、このマニュアルには記載されていません。詳細は、www.docs.sun.com で入手可能な Sun Management Center の最新マニュアルを参照してください。

第2章

SMS 1.6 のセキュリティ

この章では、SMS 1.6 と Sun Fire ハイエンド (E20K/12K および E25K/15K) システムに関するセキュリティの概要について説明します。セキュリティオプションは、各システムのドメインのセキュリティ保護 (任意選択として推奨) とシステムコントローラのセキュリティ保護 (強く推奨) のほか、全体的なシステム強化によって構成されます。強化とは、システムのセキュリティを向上させるために Solaris OS 構成を変更することを意味します。

これらの推奨事項は、セキュリティが重視される環境に適用されます。特に、システムコントローラの稼働時間の要件または Sun Fire サーバー上の情報が組織にとって重要である環境にお勧めします。

システムコントローラは、Sun Fire ハイエンドシステムを構成するハードウェアコンポーネントを制御します。SC はフレーム全体の中心的な制御ポイントであるため、侵入者の攻撃対象になります。信頼性、可用性、保守性、およびセキュリティ (RASS) を向上させるには、悪意のある誤使用や攻撃からシステムコントローラを保護する必要があります。次に、ドメインとシステムコントローラのセキュリティに関連した事項の概要を説明します。

この章では、次の項目を説明します。

- 18 ページの「ドメインセキュリティの概要」
- 18 ページの「システムコントローラのセキュリティの概要」
- 24 ページの「SMS 1.6 での変更」
- 26 ページの「smsinstall コマンドによる初期または新規の SMS インストール (デフォルトでのセキュリティ保護)」
- 27 ページの「smsupgrade コマンドによる SMS のアップグレードインストール (選択によるセキュリティ保護)」

ドメインセキュリティの概要

Sun Fire ハイエンドシステムプラットフォームのハードウェアは、1つ以上の環境に区分化して、Solaris OS の別々のイメージを実行できます。こうした環境は、「動的システムドメイン」(DSD) または「ドメイン」と呼ばれます。

論理的には、ドメインは物理的に分離されたサーバーと同等です。Sun Fire ハイエンドシステムのハードウェアによって、ドメイン環境の厳密な分離が強制されます。こうした設計のため、複数のドメインで共有されているハードウェアに障害が発生しないかぎり、1つのドメインでのハードウェアエラーは他のドメインに影響しません。ドメインが別個のサーバーのように動作するように、Sun Fire のソフトウェアは、ドメインの厳密な分離が実現されるように設計および実装されています。

SMS はすべてのドメインにサービスを提供します。こうしたサービスを提供する際にも、クライアントドメインから取得したデータが、他者から見えるデータへ漏洩することはありません。これは特に、コンソールの文字 (管理者パスワードを含む) のバッファーなどの要注意データや、クライアントドメインのデータを含む I/O バッファーのように、要注意データになりうるデータについて該当します。

SMS は、管理者の特権を制限します。この制限によって、外部からのシステムパスワードへの攻撃によって損害を受ける露出部分を制限するだけでなく、管理者の誤りによって発生する可能性のある損害の程度を制御することができます。第3章を参照してください。

システムコントローラのセキュリティの概要

システムコントローラのセキュリティ保護は、無許可のアクセスに抵抗し、かつ条件が厳しい環境でも正しく稼働するように Sun Fire ハイエンドシステムを構成する上での、最優先事項です。システムコントローラのセキュリティ対策を行う前に、システム上で実行されるサービスとデーモンについて理解する必要があります。この節では、システムコントローラに固有のソフトウェア、サービス、およびデーモンについて説明します。機能は概要レベルで説明し、詳細情報についてはほかの Sun マニュアルへの参照を示しています。この節では、システムコントローラを正しく動作させる上で必要となる基本的な機能を示します。

システムコントローラ (SC) は、Sun Fire フレーム内に装備される多機能システムボードです。これらの SC は、SMS ソフトウェアの実行を目的とした専用コンポーネントです。SMS ソフトウェアは、動的ドメインの構成、各ドメインに対するコンソールアクセスの提供、ドメインの電源投入または切断の制御、Sun Fire ハイエンドシステムの稼働と監視に欠かせないその他の機能の提供などに使用されます。

次に、システムコントローラが Sun Fire ハイエンドシステムに提供する数多くのサービスの概要を示します。

- システム構成全体を管理します。
- ドメインの起動イニシエータとして動作します。
- ドメインの syslog ホストとしての役割を果たします。SC は、LAN 規模の syslog ホストの syslog クライアントとなることもできます。
- 同期ハードウェアクロックソースを提供します。
- 動的ドメインの設定と構成を行います。
- システム環境情報 (電源、ファン、温度の状態など) を監視します。
- 現場交換可能ユニット (FRU、Field-Replaceable Unit) のログデータを集中管理します。
- 冗長性と自動化された SC フェイルオーバーを提供します。
- ドメインの仮想ホスト ID と MAC アドレスに基づいて、デフォルトのネームサービスをドメインに提供します。
- フレーム管理用の管理役割を提供します。

冗長システムコントローラ

Sun Fire フレームには、2 つのシステムコントローラがあります。どちらのシステムコントローラに対してもセキュリティー推奨事項は同じです。Sun Fire プラットフォームを制御する SC は「メイン SC」と呼ばれ、バックアップとして動作するもう一方の SC は「スペア SC」と呼ばれます。SC 上で動作するソフトウェアは、システムコントローラを監視し、自動フェイルオーバーを行うタイミングを判断します。

注 – ここでの構成例では、メイン SC は sc0、スペア SC は sc1 です。

2 つのシステムコントローラを同じ構成にすることをお勧めします。同じ構成にするものには、あらゆるシステム構成 (Solaris OS、セキュリティーの変更、パッチのインストールなど) のほか、同じバージョンの SMS ソフトウェアが含まれます。

システムコントローラ間のフェイルオーバー機能は、メインシステムコントローラとスペアシステムコントローラで動作するデーモンによって制御されます。これらのデーモンは、Sun Fire フレーム内に組み込まれたプライベート通信バスを介して通信します。このようなデーモンの通信以外に、2 つのシステムコントローラ間に特別な信頼関係はありません。

SC ネットワークインタフェース

SC では、プラットフォーム、ドメイン、およびほかのシステムコントローラとの通信のためにいくつかのネットワークインタフェースが使用されます。これらのインタフェースのほとんどは、`/etc/hostname.*` エントリで通常の Ethernet ネットワーク接続として定義されています。

メイン SC ネットワークインタフェース

通常、メイン SC (この例では `sc0`) には `/etc` ディレクトリ内に置かれた 2 つのファイルがあり、次のような内容になっています。

```
# more /etc/hostname.scman0
192.168.103.1 netmask + broadcast + private up
# more /etc/hostname.scman1
192.168.103.33 netmask + private up
```

さらに、通常のメイン SC の `/etc/netmasks` には、対応するエントリが存在しません。

```
10.1.72.0 255.255.248.0
192.168.103.0 255.255.255.224
192.168.103.32 255.255.255.252
```

注 - これらの SC 例では、経路指定されていない (RFC 1918) インターネットプロトコル (IP) アドレスを使用しています。Sun Fire システムコントローラを導入する際には、このタイプの IP アドレスを使用することをお勧めします。SMS ソフトウェアは、内部的な SC ネットワーク接続を公開ではなく非公開として定義します。

ドメイン - SC 通信 (scman0) インタフェース

`/etc/hostname.scman0` エントリは、I1 SMS 管理ネットワーク (MAN) またはドメイン - SC MAN を設定します。この例での最初の IP アドレス、`192.168.103.1` は、メイン SC 上でのみ常に使用できるように SMS ソフトウェアによって制御されます。

セキュリティ上の観点から見て、ドメインとシステムコントローラ間の I1 MAN ネットワークの誤使用またはこのネットワーク上における攻撃は、ドメイン分離に悪影響を与える可能性があります。Sun Fire ハイエンドシャーシ内の I1 ネットワークのハードウェア実装は、SC - ドメイン通信とドメイン - SC 通信だけを許可することによってこれらの問題に対処しています。I1 MAN ネットワークは、システムコント

ローラ間に個別のポイントツーポイント物理ネットワーク接続として実装されます。Sun Fire E20K/12K サーバーでは 9 個のドメイン、Sun Fire E25K/15K サーバーでは 18 個のドメインのそれぞれにこのネットワークを確立できます。これらの各接続の終端は、各ドメイン上の I/O ボードと SC です。

システムコントローラ上では、運用と管理を簡易化するため、複数に分離したこれらのネットワークが 1 つのメタインタフェースとして統合されます。この統合は、I1 MAN ドライバソフトウェアによって行われます。このソフトウェアは、ドメイン分離を適用するとともに、冗長通信パスへのフェイルオーバーを行います。

I1 ネットワークのハードウェア実装では、I1 ネットワーク上でのドメイン間の直接通信は許可されません。このようにネットワークを実装することで、各 SC - ドメインネットワーク接続はほかの接続から物理的に分離されます。

注 - scman0 ネットワークは通常の IP ベースネットワークトラフィックをサポートしますが、Sun Fire 管理トラフィックによる使用だけにとどめるべきです。この内部ネットワークをほかのトラフィックに使用すると、プラットフォーム全体の信頼性、可用性、保守性、セキュリティに影響を与える可能性があります。詳細は、scman (7D) と dman (7D) のマニュアルページを参照してください。

SC - SC 通信 (scman1) インタフェース

I2 MAN または SC - SC MAN の構成には、/etc/hostname.scman1 エントリを使用します。両方のシステムコントローラに IP アドレスが与えられるこのネットワーク接続は、2 つのシステムコントローラ間のハートビート接続用です。

Sun Fire ハイエンドシャーシでは、I1 MAN ネットワーク接続、I2 MAN ネットワーク接続とも内部的に実装されます。外部的な配線は使用されません。

スペア SC ネットワークインタフェース

スペア SC の物理ネットワークインタフェースは、メイン SC と同じです。scman0 ネットワークインタフェースは、Solaris OS によりメイン SC と同じ方法と情報を使用してスペア SC 上の /etc/hostname.scman0 ファイルを通して plumb されます。メインシステムコントローラとスペアシステムコントローラの違いは、スペアではインタフェースが無効であることです。I/O ハブ上のスペアシステムコントローラの scman0 ポートは無効にされ、mand はスペア上の scman0 にはパス情報を提供しません。

SC - SC 通信用である scman1 インタフェースの構成情報は次のとおりです。

```
# more /etc/hostname.scman1
192.168.103.34 netmask + broadcast + private up
```

スペア SC 側の対応する /etc/netmasks 情報は次のとおりです。

```
10.1.72.0 255.255.248.0
192.168.103.0 255.255.255.224
192.168.103.32 255.255.255.252
```

メインとスペアのネットワークインタフェースの構成例

メイン SC のステータスを検証するには、次のコマンドを使用します。

```
# showfailover -r
MAIN
```

メイン SC (sc0) では、このネットワーク構成例が次のように表示されます。

```
# ifconfig -a
lo0: flags=1000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232
index 1 inet 127.0.0.1 netmask ff000000

hme0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500
index 2 inet 10.1.72.80 netmask fffff800 broadcast 10.1.79.255
ether 8:0:20:a8:db:2e

scman0: flags=
1008843<UP,BROADCAST,RUNNING,MULTICAST,PRIVATE,IPv4> mtu 1500
index 3 inet 192.168.103.1 netmask fffffe0 broadcast
192.168.103.31 ether 8:0:20:a8:db:2e

scman1: flags=
1008843<UP,BROADCAST,RUNNING,MULTICAST,PRIVATE,IPv4> mtu 1500
index 4 inet 192.168.103.33 netmask ffffffff broadcast
192.168.103.35 ether 8:0:20:a8:db:2e
```

注 - scman0 ネットワークは通常の IP ベースネットワークトラフィックをサポートしますが、Sun Fire 管理トラフィックによる使用だけにとどめるべきです。この内部ネットワークをほかのトラフィックに使用すると、プラットフォーム全体の信頼性、可用性、保守性、セキュリティーに影響を与える可能性があります。詳細は、scman (7D) と dman (7D) のマニュアルページを参照してください。

スペア SC (sc1) では、このネットワーク構成例が次のように表示されます。

```
# ifconfig -a
lo0: flags=1000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232
index 1
    inet 127.0.0.1 netmask ff000000

hme0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500
index 2
inet 10.1.72.81 netmask ffffffff broadcast 10.1.72.255 ether
8:0:20:a8:ba:c7

scman0: flags=
1008843<UP,BROADCAST,RUNNING,MULTICAST,PRIVATE,IPv4> mtu 1500
index 3 inet 192.168.103.1 netmask fffffffe0 broadcast
192.168.103.31 ether 8:0:20:a8:ba:c7

scman1: flags=
1008843<UP,BROADCAST,RUNNING,MULTICAST,PRIVATE,IPv4> mtu 1500
index 4
inet 192.168.103.34 netmask ffffffff broadcast 192.168.103.35
ether 8:0:20:a8:ba:c7
```

SMS 1.6 での変更

Solaris Security Toolkit 4.2 ソフトウェアは Solaris 9 OS または Solaris 10 OS で動作し、安全な Solaris OS システムを構築および保守するための、自動化された、拡張可能かつスケーラブルなメカニズムを提供します。Solaris Security Toolkit ソフトウェアを使用すると、システムのセキュリティーを強化および監査できます。

SMS 1.6 を使用したシステムのセキュリティーオプションは、ソフトウェアが新規インストールされるのか、アップグレードとしてインストールされるのかによって異なります。

デフォルトでのセキュリティー保護 (新規インストール)

SMS バージョンを新規インストールする場合は、`smsinstall` コマンドを使用し、これによってインストールの一環として自動的にセキュリティーが強化されます (デフォルトでのセキュリティー保護)。つまり、システムコントローラがセキュリティー保護される際にシステムが強化されます。この例では、インストールの一環としてダウンロードされる Solaris Security Toolkit (SST) 4.2.0 ソフトウェアを使用して、ドメインのセキュリティー保護を手動で行うことも可能です。SMS 1.6 を新規インストールする場合は、26 ページの「`smsinstall` コマンドによる初期または新規の SMS インストール (デフォルトでのセキュリティー保護)」に進んでください。

注 – Solaris 10 OS 上でサポートされる SST の最小バージョンは 4.2.0 です。Solaris 8 および 9 OS でサポートされる SST の最小バージョンは 4.1.1 です。

選択によりセキュリティー保護を行う (アップグレード)

アップグレードによりインストールする場合は、システムのセキュリティーが自動的に強化されることはありません。この例では、`smsupgrade` コマンドが使用され、アップグレードの一環として Solaris Security Toolkit ソフトウェアがインストールされたあと、このソフトウェアを使用してシステムのセキュリティー状態の強化、強化解除、監査を行うことができます (選択によるセキュリティー保護)。この処理は、システムコントローラとドメインを含めて行われます。SMS 1.6 へのアップグレードを行う場合と、SMS 強化後の作業を行う場合は、27 ページの「`smsupgrade` コマンドによる SMS のアップグレードインストール (選択によるセキュリティー保護)」に進んでください。

インストール内容の変更

次に、SMS 1.6 のインストール内容に発生した主な変更を示します。この変更は、使用されるインストール方法には関係ありません。

- SMS は、Solaris Security Toolkit Version 4.2 が存在するかどうかを自動的に確認します。Version 4.2 よりも前のバージョンが存在すると、インストール処理が一時的に停止し、継続する前に、その互換性のないバージョンを削除ことを求めるプロンプトが表示されます。互換性のないバージョンが削除されると、インストール処理が再開され、Solaris Security Toolkit Version 4.2 が自動的にインストールされます。
- FixModes ソフトウェアと MD5 ソフトウェアは、このリリースでは SMS 1.6 インストールの一環として自動的にインストールされます。
- フィルタリング機能が向上したため、I1 MAN ネットワーク上の ARP トラフィックは無効にしないでください。

前提条件と制限事項

ここでの推奨事項は、Sun Fire システムコントローラをセキュリティーで保護して、サポート対象の構成とするために実行可能な作業に関するいくつかの前提条件と制限事項に基づいています。

注 – このマニュアル内で示す推奨事項は System Management Services (SMS) 1.6 ソフトウェアを対象としており、SMS 1.6 と前のリリースの相違点については説明していません。可能な場合は、すべてのユーザーが、使用しているソフトウェアを SMS 1.6 にアップグレードすることをお勧めします。

Solaris OS の強化は、さまざまに解釈できます。強化された SC 構成を確立する場合は、使用できるすべての Solaris OS オプションの強化に取り組みます。つまり、強化できるものはすべて強化されます。サービスとデーモンを現状のままに維持するのが望ましい場合は、それらの強化または変更を行いません。

注 – 環境によっては、このマニュアルで説明しているレベルまで Solaris OS 構成を強化することが妥当ではない場合があります。また、ここで推奨している強化処理の一部だけを実行する環境もあります。このような場合もその構成はサポート対象となりますが、このマニュアルで示す推奨事項の枠を越える付加的な強化はサポートされません。

Solaris Security Toolkit の Sun Fire ハイエンドサーバー SC モジュールのコピーをカスタマイズすることで、一部の強化スクリプトを無効にすることができます。デフォルトモジュールを変更する場合は、これらのファイルのコピーに変更を加えることを強くお勧めします。この方法によって、より新しいバージョンの Solaris Security Toolkit へのアップグレードが容易になります。

注 – システムコントローラの強化には、明示的に許可されていないものは拒否されるという標準のセキュリティー規則が適用されます。

システムコントローラにインストールできる追加のソフトウェア (Sun Remote Services Event Monitoring、Sun Remote Services Net Connect、Sun Management Center ソフトウェアなど) についての説明は、このマニュアルから除外されました。このような種類のソフトウェアをインストールする場合は、インストールによって発生するセキュリティー上の暗黙の影響を慎重に検討することをお勧めします。

サポートの取得

Solaris Security Toolkit ソフトウェア (sunfire_15k_sc-secure.driver) によって実装された、Sun Fire ハイエンドシステムの SC 構成は、Sun のサポート対象となります。強化された SC がサポートされるのは、Solaris Security Toolkit を使用してセキュリティー変更を加えた場合だけです。

smsinstall コマンドによる初期または新規の SMS インストール (デフォルトでのセキュリティー保護)

この場合は、smsinstall コマンドを使用して SMS 1.6 ソフトウェアをインストールします。インストール処理の一環としてデフォルトでの自動セキュリティー保護が実行され、これによりシステムのシステムコントローラは自動的に強化され、セキュリティー保護されます。

強化作業は、Sun Fire 15K/12K SC モジュール sunfire_15k_sc-secure.driver によって行われます。デフォルトで実装されるこの Solaris Security Toolkit ドライバは、無効にできるサービスをすべて、SMS に悪影響を与えることなく無効にします。ユーザーは必要なだけサービスを有効にできますが、SMS インストールソフトウェアによって無効にされたサービスの数を超えてサービスを無効にすることはできません。

Solaris Security Toolkit のカスタマイズ

システムに含まれるサービスとデーモンの一部を Solaris Security Toolkit によって無効にする必要があると判断する場合があります。特定のニーズに合うように Solaris Security Toolkit ソフトウェアをカスタマイズする方法については、29 ページの「Solaris Security Toolkit ドライバのカスタマイズ」を参照してください。

任意選択として行うドメインのセキュリティー保護

次のサイトで入手できる次の Sun BluePrints™ Online の文書に示されている方法でシステムドメインをセキュリティー保護することによって、システムをさらに強化することもできます。

<http://www.sun.com/security/blueprints>

- 『Securing the Sun Fire high-end Domains』
- 『Solaris Operating System Security – Updated for Solaris 8 (2/04) Operating System』
- 『Solaris Operating System Security – Updated for Solaris 9 (4/04) Operating System』

smsupgrade コマンドによる SMS のアップグレードインストール (選択によるセキュリティー保護)

この場合は、smsupgrade コマンドを使用して SMS 1.6 ソフトウェアをインストールします。デフォルトでの自動強化は実行されません。ただし、アップグレードの一環として Solaris Security Toolkit ソフトウェアがインストールされるため、このソフトウェアを使用してシステムのセキュリティー状態の強化、強化解除、監査を手動で行うことができます。

利用できるセキュリティー対策は次のとおりです。

強く推奨:

- Solaris Security Toolkit を使用し、システムコントローラのセキュリティー保護を行います。

任意選択:

- ドメインをセキュリティー保護します。
- SC の MAN ドライバからドメインを除外することにより、SC とそのドメイン間の IP トラフィックをすべて無効にします。

任意選択として行うドメインのセキュリティー保護

ドメインの独立性が特に重要なシステムでは、独立させる必要があるドメインと SC 間の IP 接続を無効にすることをお勧めします。

システムコントローラのセキュリティー保護を行う方法については、28 ページの「Solaris Security Toolkit によるシステムコントローラのセキュリティー保護」を参照してください。選択によるドメインのセキュリティー保護を行う方法については、次のサイトで次の Sun BluePrints Online の文書を参照してください。

<http://www.sun.com/security/blueprints>

- 『Securing the Sun Fire high-end Domains』
- 『Solaris Operating System Security – Updated for Solaris 8 (2/04) Operating System』
- 『Solaris Operating System Security – Updated for Solaris 9 (4/04) Operating System』

Solaris Security Toolkit によるシステムコントローラのセキュリティー保護

システムコントローラのセキュリティー保護を効果的に行うには、システムコントローラで動作する Solaris OS ソフトウェアと、Sun Fire ハイエンドプラットフォームの構成の両方を変更する必要があります。Solaris Security Toolkit ソフトウェアにカスタマイズしたモジュールを追加することで、Solaris OS インストールとこれらの推奨事項の実装が簡略化されます。このようなモジュール使用すると、セキュリティーに関する推奨事項は自動的に実装されます。

Solaris Security Toolkit ソフトウェアは、常時更新されています。smsupgrade コマンドを実行すると、このコマンドの処理の一環として Solaris Security Toolkit Version 4.2 がダウンロードされます。Solaris Security Toolkit が最新バージョンであるかを SMS のインストール時に確認するには、次の Web サイトを参照してください。

<http://www.sun.com/security/jass>

新しいバージョンをダウンロードした場合は、SMS zip ファイルの Bundled_Products ディレクトリにそのバージョンをインストールし、同じ名前を使用して古いパッケージを置き換えてください。ダウンロードした Solaris Security Toolkit パッケージは解凍する必要があります。

注 – Solaris Security Toolkit パッケージを手動でインストールする方法については、『Solaris Security Toolkit Installation Guide』を参照してください。

注 – システムコントローラ的一方を強化する場合は、あらかじめフェイルオーバーを無効にしてください。フェイルオーバーを元どおり有効にするには、必ず両方のシステムコントローラの強化およびテストが完了したあとで有効にしてください。

注 – Solaris Security Toolkit は、パフォーマンス向上とソフトウェア構成についての構成変更には使用できません。

Solaris Security Toolkit ソフトウェア

smsupgrade コマンドを実行すると、その処理内容の一環として Solaris Security Toolkit ソフトウェアの Version 4.2 が SMS zip ファイル内に含まれ、システムコントローラにインストールされます。情報メッセージでは、Solaris Security Toolkit のインストールの進捗が表示されます。また、ほかのセキュリティーソフトウェアのインストール作業と、システムコントローラを強化するための Solaris OS の変更の実装作業を自動化するために、Solaris Security Toolkit ソフトウェアを使用することがユーザーに勧められます。

いずれかのバージョンの Solaris Security Toolkit が SC にすでにインストールされている場合は、SMS パッケージをインストールする前に smsupgrade が中止され、ユーザーは smsupgrade を再起動する前に、Solaris Security Toolkit に関連したカスタマイズがある場合はそれを保存し、古い Solaris Security Toolkit パッケージを削除するように求められます。

Solaris Security Toolkit ドライバのカスタマイズ

ユーザーは、Solaris Security Toolkit を使用してシステムのサービスとデーモンの一部を無効にする必要があると判断する場合があります。また、Solaris Security Toolkit で使用できるスクリプトが無効になっている場合にそれらを有効にする場合もあります。

SC 上で各種のその他のサービスを有効にして強化をカスタマイズする方法については、『Solaris Security Toolkit Administrative Manual』の第7章を参照してください。有効な状態に維持する必要があるサービスがあるが、Solaris Security Toolkit によってそれらが自動的に無効にされるという場合は、そのデフォルトを無効にすることができます。

このツールキットによって特定のサービスが無効に設定されるのを防ぐには、ドライブ内の該当する終了スクリプトの呼び出しをコメントにします。たとえば、使用している環境でネットワークファイルシステム (NFS) ベースのサービスが必要な場合には、それらを有効なままに維持できます。sunfire_15k_domain-hardening.driver スクリプトのコピー内で、disable-nfs-server.fin スクリプトと disable-rpc.fin スクリプトの前に # 記号を付け、これらをコメントにします。

Solaris Security Toolkit によるドライブスクリプトの編集と作成の詳細は、Solaris Security Toolkit のマニュアルを参照してください。

注 – この節で行うインストール作業と変更作業の間、Telnet や FTP など、SC への暗号化されていないアクセスメカニズムはすべて無効になります。強化作業では、SC シリアルポートを介したコンソールシリアルアクセスは無効になりません。

システムコントローラに変更を加える場合は、Solaris Security Toolkit に含まれるファイルを変更する必要があります。次に、これらのオプションの一部を使用する手順を示します。

▼ I1 トラフィックを無効にする (ドメインの除外)

ドメインを除外するには、I1 ネットワーク構成から除外されるようにドメインネットワークインタフェースの構成を解除し、続いて mand デーモンを起動します。

注 – 前のバージョンでは SMS では、SST ソフトウェアを使用してドメインと SC 間の I1 ネットワークを使用不可にすることによって、システムコントローラとの通信からそのドメインを除外することができました。この機能は最新の SST バージョンではサポートされておらず、この手順で示されているように手動で実行する必要があります。

- ユーザー権限で、除去するドメインの MAN ホスト名として NONE を指定します。次に、ドメイン A の例を示します。

```
#smsconfig -m I1 A

Enter the MAN hostname for DA-I1 [ DA-I1 ]: NONE

Network: I1 DA-I1
Hostname: NONE   IP Address: NONE

Do you want to accept these settings? [y,n]y

#pkill -HUP mand
```

▼ FTP または Telnet を使用可能にする

注 – Solaris Security Toolkit の `user.init` ファイルは、次のようなユーザー定義の変数を含めるように編集すべきです。

- FTP を使用可能にするには、Solaris Security Toolkit の `user.init` ファイルで `JASS_SVCS_ENABLE = ftp` と設定します。
- Telnet を使用可能にするには、Solaris Security Toolkit の `user.init` ファイルで `JASS_SVCS_ENABLE = telnet` と設定します。

詳細は、『Solaris Security Toolkit 管理マニュアル』の第 7 章の「強化構成のカスタマイズ」を参照してください。

▼ ドライバファイルの内容を表示する

- ドライバファイルの内容を表示して Solaris OS の変更についての情報を確認する方法については、`/opt/SUNWjass/Documentation` ディレクトリ内または次の Web を通して利用できる Solaris Security Toolkit のマニュアルを参照してください。

<http://www.sun.com/security/jass>

▼ Solaris Security Toolkit の実行を解除する

Solaris Security Toolkit を実行するごとに、`/var/opt/SUNWjass/run` に実行ディレクトリが 1 つ作成されます。これらのディレクトリの名前は、その実行が開始された日時に基づいています。コンソールに出力を表示するほかに、Solaris Security Toolkit ソフトウェアは `/var/opt/SUNWjass/run` ディレクトリにログファイルを作成します。



注意 – どのような状況下でも `/var/opt/SUNWjass/run` ディレクトリの内容は変更しないでください。ファイルを変更すると、内容が壊れ、Solaris Security Toolkit ソフトウェアの機能 (undo など) を使用する場合に予期しないエラーが発生する可能性があります。

`/var/opt/SUNWjass/run` ディレクトリ内に格納されたファイルは、システムで行われた変更を追跡するとともに、`jass-execute` 取り消し機能を有効にします。

注 – デフォルトでは、Solaris Security Toolkit は、以前の実行の取り消し中にバックアップされたファイルを上書きします。場合によっては、実行以降にファイルに加えられた変更がこのアクションによって上書きされます。上書き変更に不安を感じる場合は、`-n` (no force: 強制なし) オプションを使用し、変更されたファイルが上書きされないようにしてください。このオプションの詳細は、Solaris Security Toolkit のマニュアルを参照してください。

- 単一の実行または複数の実行を取り消すには、`jass-execute -u` コマンドを使用します。

たとえば、2 つの Solaris Security Toolkit が個別に実行されているシステムで、次の例に示すように 2 つめの実行を解除できます。

```
# pwd
/opt/SUNWjass
# ./jass-execute -u
Please select a JASS run to restore through:
1. September 25, 2005 at 06:28:12
   (/var/opt/SUNWjass/run/20050925062812)
2. December 10, 2005 at 19:04:36
   (/var/opt/SUNWjass/run/20051210190436)
3. Restore from all of them
Choice('q' to exit)? 2
./jass-execute: NOTICE: Restoring to previous run
//var/opt/SUNWjass/run/20021210190436

=====
undo.driver: Driver started.
=====
[...]
```

`jass-execute` コマンドで使用できる機能とオプションの詳細については、Solaris Security Toolkit のマニュアルを参照してください。

第3章

SMS における管理特権

この章では、SMS 1.6 と Sun Fire ハイエンドサーバーシステムに関する管理特権の概要を説明します。この章では、次の項目を説明します。

- 35 ページの「管理特権の概要」
- 37 ページの「プラットフォーム管理者グループ」
- 39 ページの「プラットフォームオペレータグループ」
- 39 ページの「プラットフォーム保守グループ」
- 41 ページの「ドメイン管理者グループ」
- 43 ページの「ドメイン構成グループ」
- 44 ページの「スーパーユーザーの特権」
- 44 ページの「すべての特権のリスト」

管理特権の概要

SMS では、ドメインの管理特権とプラットフォームの管理特権が分離されています。たとえば、各ドメインにわたるシステム管理の特権と、プラットフォーム全体にわたるシステム管理の特権を別々に割り当てることができます。また、プラットフォームのオペレータおよびドメインの構成者に相当するユーザーに、特権のサブセットを割り当てることができます。管理特権の付与は、アクションを開始した個人を監査により特定できるように行います。

SMS は、サイトで設定された Solaris ユーザーアカウントを使用し、これらアカウントに対して、Solaris の *group* メンバーシップを使用して管理特権を与えます。この方法により、デフォルトの特権の作成および整理をサイト単位で柔軟に行えます。たとえば、管理者特権を代表する同一の Solaris グループに複数のドメインを割り当てれば、ドメインのグループを 1 セットのドメイン管理者で管理できます。

SMS は、複数の管理役割を個人の管理者に割り当てることができ、サイト単位で柔軟に行えます。たとえば、構成されているすべての管理特権グループに属するグループメンバーシップを持つ、単一のユーザーアカウントを設定できます。

- 「プラットフォーム管理者」は、プラットフォームのハードウェアを管理します。実行中のドメインで使用中のハードウェアに関しては制限がありますが、プラットフォーム管理者は、最終的にはサーバーのハードウェアの電源を切断することで、実行中のドメインをシャットダウンできます。
- 各「ドメイン管理者」は管理するドメインの Solaris コンソールを利用でき、ドメインで実行されるソフトウェア、またはドメインに割り当てられているハードウェアを管理する特権を持ちます。
- 各種の管理特権のレベルに応じて、「プラットフォームオペレータ」または「ドメイン構成者」に対して、状態および監視の特権のサブセットを提供します。

SMS で提供される管理特権では、現行の製品の保守のためにだけ提供されている機能へアクセスできます。

管理特権の構成は、スーパーユーザーが `smsconfig -g` を使用して自由に変更できます。このとき SMS を停止または再起動する必要はありません。

SMS は、`smsconfig` コマンドの `- a` および `- r` オプションを使用して、SMS のグループへのディレクトリアクセスを設定する Solaris アクセス制御リスト (ACL) ソフトウェアを実装しています。ACL はプラットフォームおよびドメインのディレクトリへのアクセスを制限して、ファイルシステムのセキュリティーを提供します。ACL の詳細については、『Solaris のシステム管理 (セキュリティーサービス)』を参照してください。

プラットフォーム管理者グループ

プラットフォーム管理者 (platadm) グループとして特定されるグループでは、構成の制御、環境の状態を取得する手段、ドメインにボードを割り当てる機能、電源の制御、およびその他の保守プロセッサ機能が提供されます。つまり、プラットフォーム管理者グループは、ドメインの制御およびインストールと保守に関する各コマンド

へのアクセス以外のすべてのプラットフォーム特権を持ちます (図 3-1)。

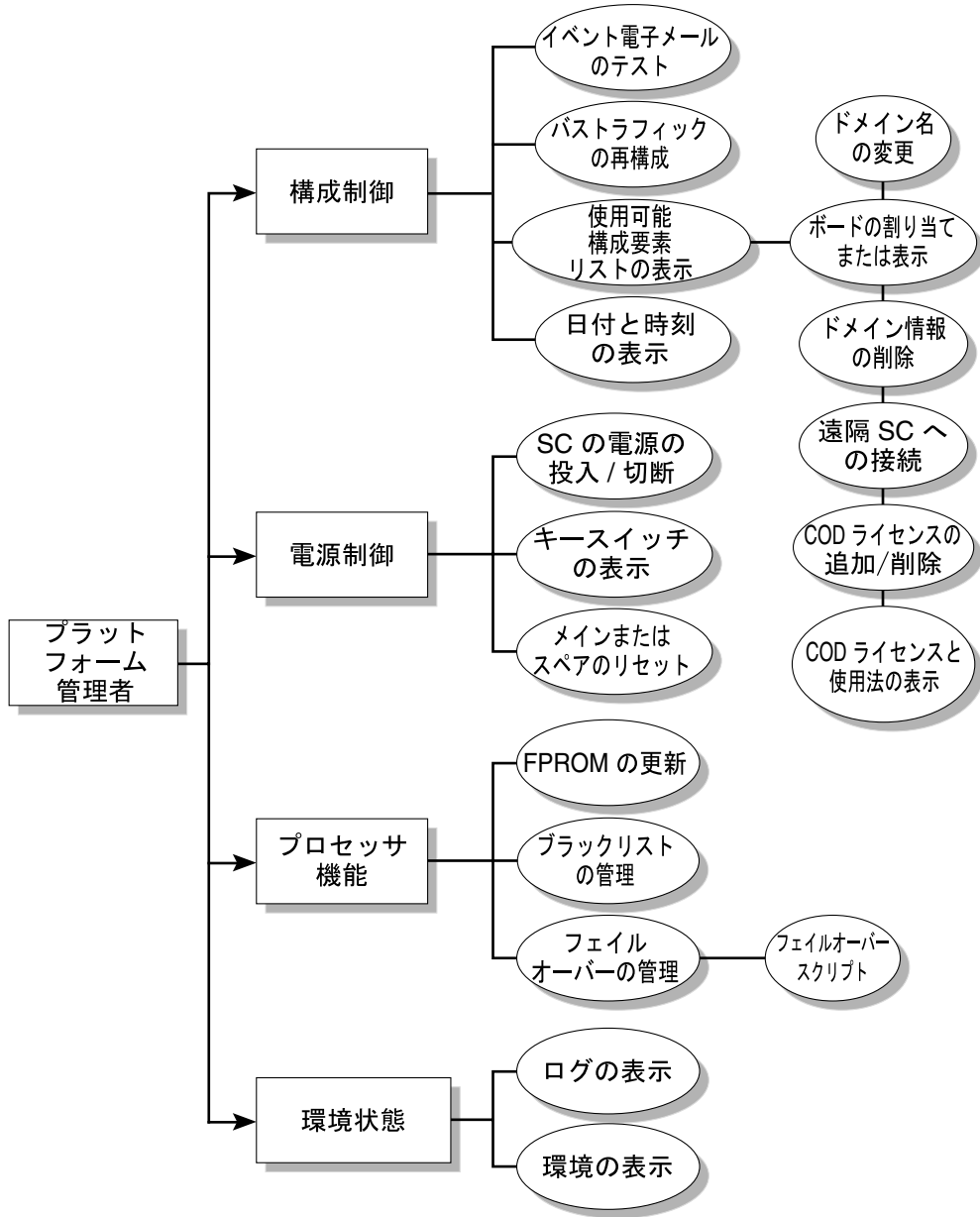


図 3-1 プラットフォーム管理者の特権

プラットフォームオペレータグループ

プラットフォームオペレータ (platoper) グループは、プラットフォーム特権のサブセットを持ちます。このグループが行えるプラットフォーム制御は、電源の制御だけです。このため、プラットフォームオペレータグループはプラットフォームの電源と状態の特権に制限されます (図 3-2)。

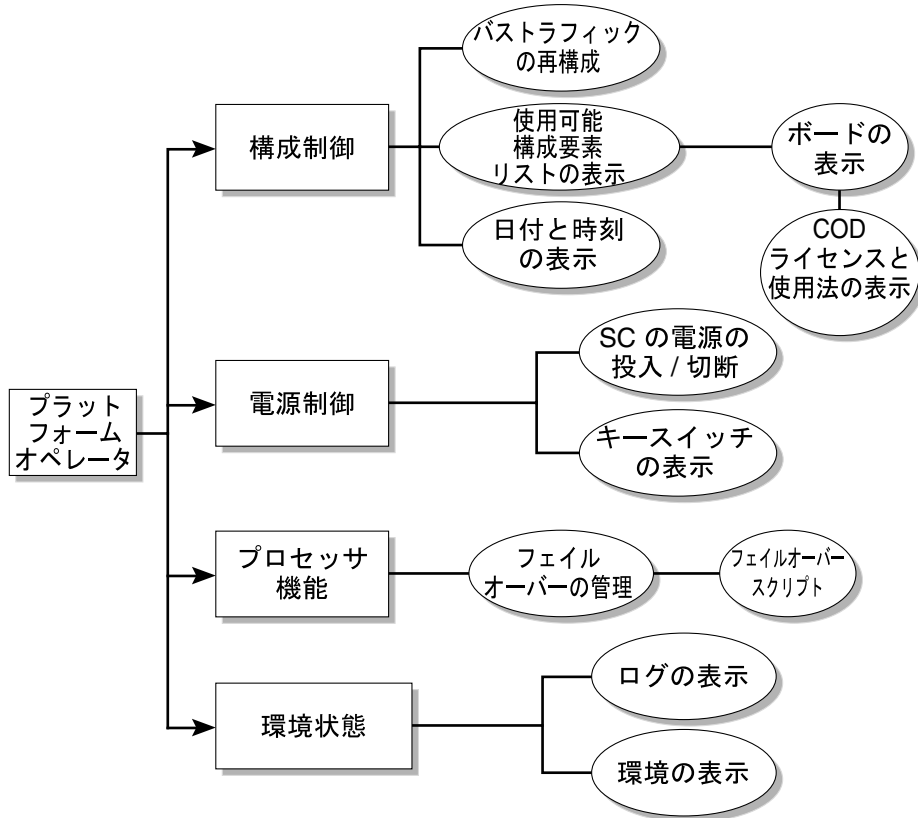


図 3-2 プラットフォームオペレータの特権

プラットフォーム保守グループ

プラットフォーム保守 (platsvc) グループは、プラットフォーム保守コマンドの特権に加えて、プラットフォーム制御およびプラットフォーム構成状態の特権の一部も持ちます (図 3-2)。

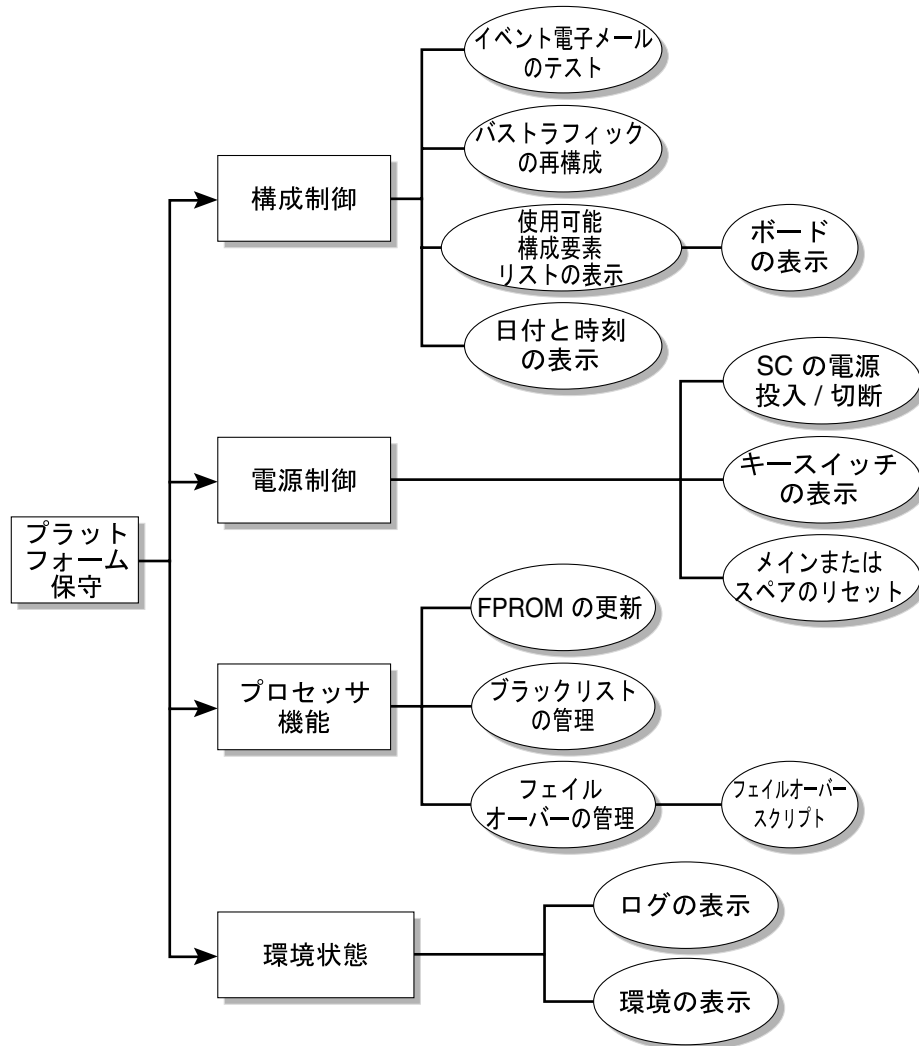
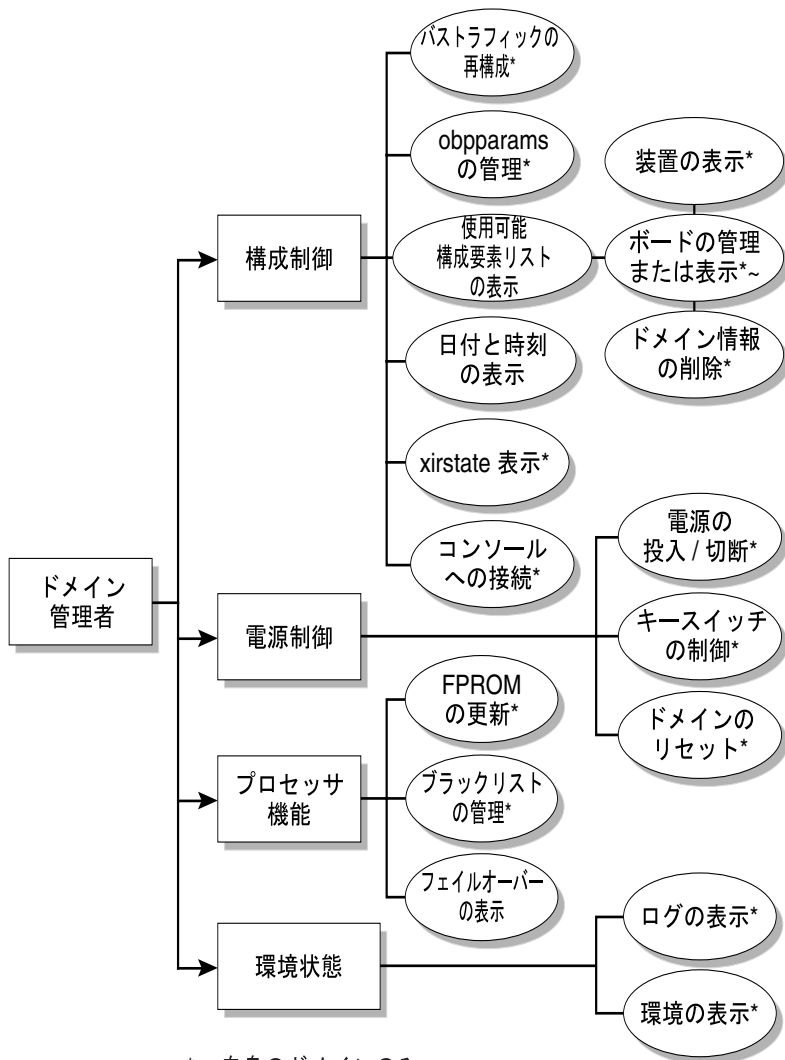


図 3-3 プラットフォーム保守の特権

ドメイン管理者グループ

ドメイン管理者 (`dmn[domain-id]admin`) グループでは、それぞれのドメインのコンソールにアクセスできるほか、それぞれのドメインに直接または間接に影響を与える操作を実行できます。このため、ドメイン管理グループはドメイン制御、ドメイン状態、およびコンソールを使用できますが、プラットフォーム全体の制御やプラットフォームの資源割り当てはできません (図 3-4)。

Sun Fire ドメインは 18 個まで (A-R) 作成でき、各ドメインは *domain-id* で識別されます。このため、ドメイン管理者のグループは 18 個あり、それぞれのドメインへのアクセスを厳密に制御します。



* = 自身のドメインのみ

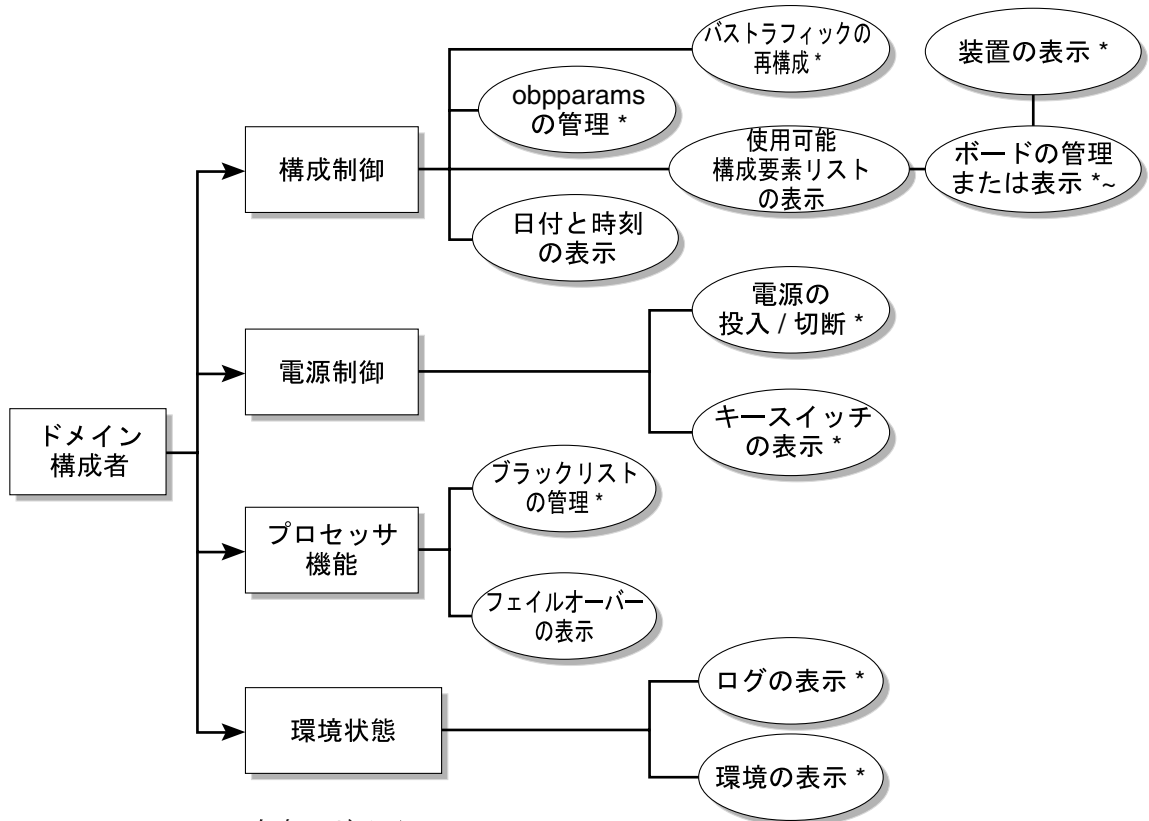
~ = ボードがドメインの使用可能構成要素リスト内に存在しなければならない

図 3-4 ドメイン管理者の特権

ドメイン構成グループ

ドメイン構成 (dmn[domain-id]rcfg) グループは、ドメイン管理者グループの特権のサブセットを持ちます。ドメイン構成グループでは、ドメインにあるボードの電源制御、あるいはドメインで装着または取り外すボードの (再) 構成以外のドメイン制御はできません (図 3-5)。

Sun Fire ドメインは 18 個まで作成でき、*domain-id* で識別されます。このため、ドメイン構成グループは 18 個あり、それぞれのドメインへのアクセスを厳密に制御できます。



* = 自身のドメインのみ

~ = ボードがドメインの使用可能構成要素リスト内に存在しなければならない

図 3-5 ドメイン構成者の特権

スーパーユーザーの特権

スーパーユーザーの特権は、インストール、ヘルプ、および状態の特権に制限されま
す (図 3-6)。

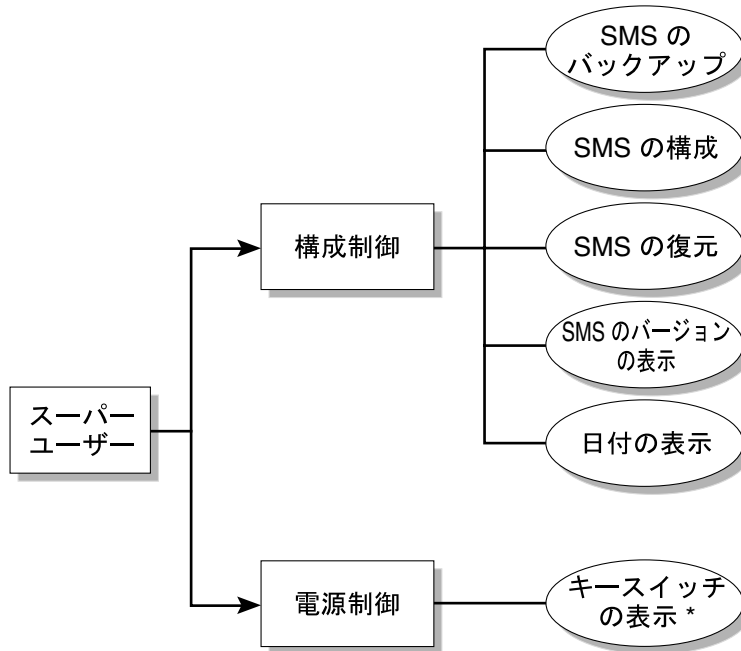


図 3-6 スーパーユーザーの特権

すべての特権のリスト

表 3-1 に、すべてのグループ特権を示します。

表 3-1 すべてのグループ特権のリスト

コマンド	グループの特権					
	プラットフォーム管理者	プラットフォームオペレータ	ドメイン管理者	ドメイン構成者	プラットフォーム保守担当	スーパーユーザー
addboard	プラットフォーム管理者の特権だけを持つユーザーは、 <code>-c assign</code> だけを実行できます。	不可	ドメイン X の管理者特権だけを持つユーザーは、各自のドメインでこのコマンドを実行できません。ボードがドメインに割り当てられていない場合、そのボードはドメインの使用可能構成要素リストになければなりません。	ドメイン X の構成者特権だけを持つユーザーは、各自のドメインでこのコマンドを実行できません。ボードがドメインに割り当てられていない場合、そのボードはドメインの使用可能構成要素リストになければなりません。	不可	不可
addcodlicense	可	不可	不可	不可	不可	不可
addtag	可	不可	不可	不可	不可	不可
cancelcmdsync	可	可	可	可	可	不可
console	不可	不可	可 (自分のドメインだけ)	不可	不可	不可

表 3-1 すべてのグループ特権のリスト (続き)

コマンド	グループの特権					
	プラット フォーム 管理者	プラット フォーム オペレー タ	ドメイン 管理者	ドメイン 構成者	プラット フォーム 保守担当	スーパー ユーザー
deleteboard	プラット フォーム管理 者の特権だけ を持つユー ザーは、ボー ド(複数の場 合あり)が <i>assign</i> の状態 で、実行中の ドメインでア クティブでな い場合にだけ <i>-c unassign</i> を 実行できま す。	不可	ドメイン X の 管理者特権だ けを持つユー ザーは、各自 のドメインで このコマンド を実行できま す。ボードが ドメインに割 り当てられて いない場合、 そのボードは ドメインの使 用可能構成要 素リストにな ければなりま せん。	ドメイン X の 構成者特権だ けを持つユー ザーは、各自 のドメインで このコマンド を実行できま す。ボードが ドメインに割 り当てられて いない場合、 そのボードは ドメインの使 用可能構成要 素リストにな ければなりま せん。	不可	不可
deletecodlicense	可	不可	不可	不可	不可	不可
deletetag	可	不可	不可	不可	不可	不可
disablecomponent	可 (プラット フォームのみ)	不可	可 (自分のドメ インだけ)	可 (自分のドメ インだけ)	不可	不可
enablecomponent	可 (プラット フォームのみ)	不可	可 (自分のドメ インだけ)	可 (自分のドメ インだけ)	不可	不可
flashupdate	可	不可	可 (自分のドメ インだけ)	不可	不可	不可
help	可	可	可	可	可	可
initcmdsync	可	可	可	可	可	不可

表 3-1 すべてのグループ特権のリスト (続き)

コマンド	グループの特権					
	プラットフォーム管理者	プラットフォームオペレータ	ドメイン管理者	ドメイン構成者	プラットフォーム保守担当	スーパーユーザー
moveboard	プラットフォーム管理者の特権だけを持つユーザーは、ボードが <i>assign</i> の状態であり、ボードが取り外されるドメインでアクティブでない場合にだけ <i>-c unassign</i> を実行できます。	不可	ユーザーは、関係するドメインの両方に属している必要があります。ドメインに取り付けるボードがまだドメインに割り当てられていない場合、そのボードはドメインの使用可能構成要素リストになければなりません。	ユーザーは、関係するドメインの両方に属している必要があります。ドメインに取り付けるボードがまだドメインに割り当てられていない場合、そのボードはドメインの使用可能構成要素リストになければなりません。	不可	不可
poweron	可	不可	可 (自分のドメインだけ)	可 (自分のドメインだけ)	不可	不可
poweroff	可	不可	可 (自分のドメインだけ)	可 (自分のドメインだけ)	不可	不可
rcfgadm	プラットフォーム管理者の特権だけを持つユーザーは、 <i>-x assign</i> を実行できます。このユーザーは、ボードが <i>assign</i> の状態で、実行中のドメインでアクティブでない場合にだけ <i>-x unassign</i> を実行できます。	不可	ドメイン X の管理者特権だけを持つユーザーは、各自のドメインでこのコマンドを実行できます。ボードがドメインに割り当てられていない場合、そのボードはドメインの使用可能構成要素リストになければなりません。	ドメイン X の構成者特権だけを持つユーザーは、各自のドメインでこのコマンドを実行できます。ボードがドメインに割り当てられていない場合、そのボードはドメインの使用可能構成要素リストになければなりません。	不可	不可
reset	不可	不可	可 (自分のドメインだけ)	不可	不可	不可
resetsc	可	不可	不可	不可	不可	不可

表 3-1 すべてのグループ特権のリスト (続き)

コマンド	グループの特権					
	プラットフォーム管理者	プラットフォームオペレータ	ドメイン管理者	ドメイン構成者	プラットフォーム保守担当	スーパーユーザー
runcmdsync	可	可	可	可	可	不可
savecmdsync	可	可	可	可	可	不可
setbus	可	不可	可 (自分のドメインだけ)	可 (自分のドメインだけ)	不可	不可
setcsn	可	不可	不可	不可	可	不可
setdatasync	可	可	可	可	可	不可
setdate	可	不可	可 (自分のドメインだけ)	不可	不可	不可
setdefaults	可	不可	可 (自分のドメインだけ)	不可	不可	不可
setfailover	可	不可	不可	不可	不可	不可
setkeyswitch	不可	不可	可 (自分のドメインだけ)	不可	不可	不可
setobpparams	不可	不可	可 (自分のドメインだけ)	可 (自分のドメインだけ)	不可	不可
setupplatform	可	不可	不可	不可	不可	不可
showboards	可	可	可 (自分のドメインだけ)	可 (自分のドメインだけ)	可	不可
showbus	可	可	可 (自分のドメインだけ)	可 (自分のドメインだけ)	可	不可
showcmdsync	可	可	可	可	可	不可
showcodlicense	可	可	不可	不可	不可	不可
showcodusage	可	可	不可	不可	不可	不可
showcomponent	可	可	可 (自分のドメインだけ)	可 (自分のドメインだけ)	可	不可
showdatasync	可	可	可	可	可	不可
showdate	可 (プラットフォームのみ)	可 (プラットフォームのみ)	可 (自分のドメインだけ)	可 (自分のドメインだけ)	可 (プラットフォームのみ)	不可
showdevices	不可	不可	可 (自分のドメインだけ)	可 (自分のドメインだけ)	不可	不可

表 3-1 すべてのグループ特権のリスト (続き)

コマンド	グループの特権					
	プラットフォーム 管理者	プラットフォーム オペレータ	ドメイン 管理者	ドメイン 構成者	プラットフォーム 保守担当	スーパー ユーザー
showenvironment	可	可	可 (自分のドメインだけ)	可 (自分のドメインだけ)	可	不可
showfailover	可	可	不可	不可	可	不可
showkeyswitch	可	可	可 (自分のドメインだけ)	可 (自分のドメインだけ)	可	不可
showlogs	可 (プラットフォームのみ)	可 (プラットフォームのみ)	可 (自分のドメインだけ)	可 (自分のドメインだけ)	可 (プラットフォームのみ)	不可
showobpparams	不可	不可	可 (自分のドメインだけ)	可 (自分のドメインだけ)	不可	不可
showplatform	可	可	可 (自分のドメインだけ)	可 (自分のドメインだけ)	可	不可
showxirstate	不可	不可	可 (自分のドメインだけ)	不可	不可	不可
smsbackup	不可	不可	不可	不可	不可	可
smsconfig	不可	不可	不可	不可	不可	可
smsconnectsc	可	不可	不可	不可	不可	不可
smsrestore	不可	不可	不可	不可	不可	可
smsversion	不可	不可	不可	不可	不可	可
testemail	可	不可	不可	不可	可	不可

第4章

SMS の内部動作

SMS の操作は一般に、一連のデーモンとコマンドにより実行されます。この章では、SMS の動作の概要を示し、SMS のデーモン、プロセス、コマンド、およびシステムファイルについて説明します。詳細については、『System Management Services (SMS) 1.6 リファレンスマニュアル』を参照してください。



注意 - /opt/SUNWSMS にあるファイルに変更を加えると、システムに重大な障害が発生する可能性があります。この章で説明される各ファイルへの変更は、十分な経験を積んだシステム管理者だけが行な。ってください。

この章では、次の項目を説明します。

- 51 ページの「起動のフロー」
- 52 ページの「SMS デーモン」

起動のフロー

SMS の起動時に発生するイベントは、次のとおりです。

1. ユーザーが、Sun Fire ハイエンド (CPU/ディスクおよび DVD-ROM) プラットフォームに電源を入れます。SC 上の Solaris OS が自動的に起動します。
2. 起動プロセス中に /etc/init.d/sms スクリプトが呼び出されます。このスクリプトはセキュリティを確保するため、MAN ネットワーク上での転送、ブロードキャスト、およびマルチキャストを無効化します。続いて、このスクリプトは SMS ソフトウェアを起動するためのバックグラウンド処理を起動し、このバックグラウンド処理は `ssd` を起動して監視します。`ssd` は SMS の起動デーモンで、すべての SMS のデーモンおよびサーバーの起動と監視を担当します。

- 次に `ssd(1M)` は、デーモンとプロセス、`mld`、`pcd`、`hwad`、`tmd`、`dsmd`、`esmd`、`mand`、`osd`、`dca`、`efe`、`codd`、`efhd`、`elad`、`erd`、`smnptd`、`picld`、`wcapp` も起動します。

SMS デーモンについての詳細は、52 ページの「SMS デーモン」を参照してください。efe の詳細は、<http://docs.sun.com> で入手可能な Sun Management Center の最新のマニュアルを参照してください。

- デーモンが起動したら、`console` などの SMS コマンドを使用できます。

SMS の起動には数分間を要します。起動中に実行したコマンドがエラーメッセージを返した場合、起動は完了していません。起動が完了すると、「SMS software start-up complete」というメッセージがプラットフォームのログに出力されます。このログの内容は、`showlogs(1M)` コマンドで表示できます。

SMS デーモン

SMS 1.6 の各デーモンは、Sun Fire ハイエンドシステム上で中心的な役割を果たします。デーモンは、API を使ってクライアントに SMS サービスを提供する持続的プロセスです。

注 – SMS デーモンは `ssd` により起動されるので、コマンド行から手動で起動しないでください。デーモンに対して `kill` コマンドを発行すると、SMS ソフトウェアの堅牢性に重大な影響を与えるため、Sun の保守担当者から特に要求されないかぎり、このコマンドを発行しないでください。

デーモンは常に実行されており、システムの起動時に初期化され、必要なときにいつでも再起動されます。

各デーモンの詳細は、対応するマニュアルページで説明されています。ただし、`efe` コマンドについては、Sun Management Center のマニュアルで別に参照してください。

この節では、SMS の各デーモンの相互関係、およびデーモンにアクセスする CLI について説明します。

図 4-1 に、Sun Fire ハイエンドシステムのソフトウェアコンポーネントとその高度な対話を示します。

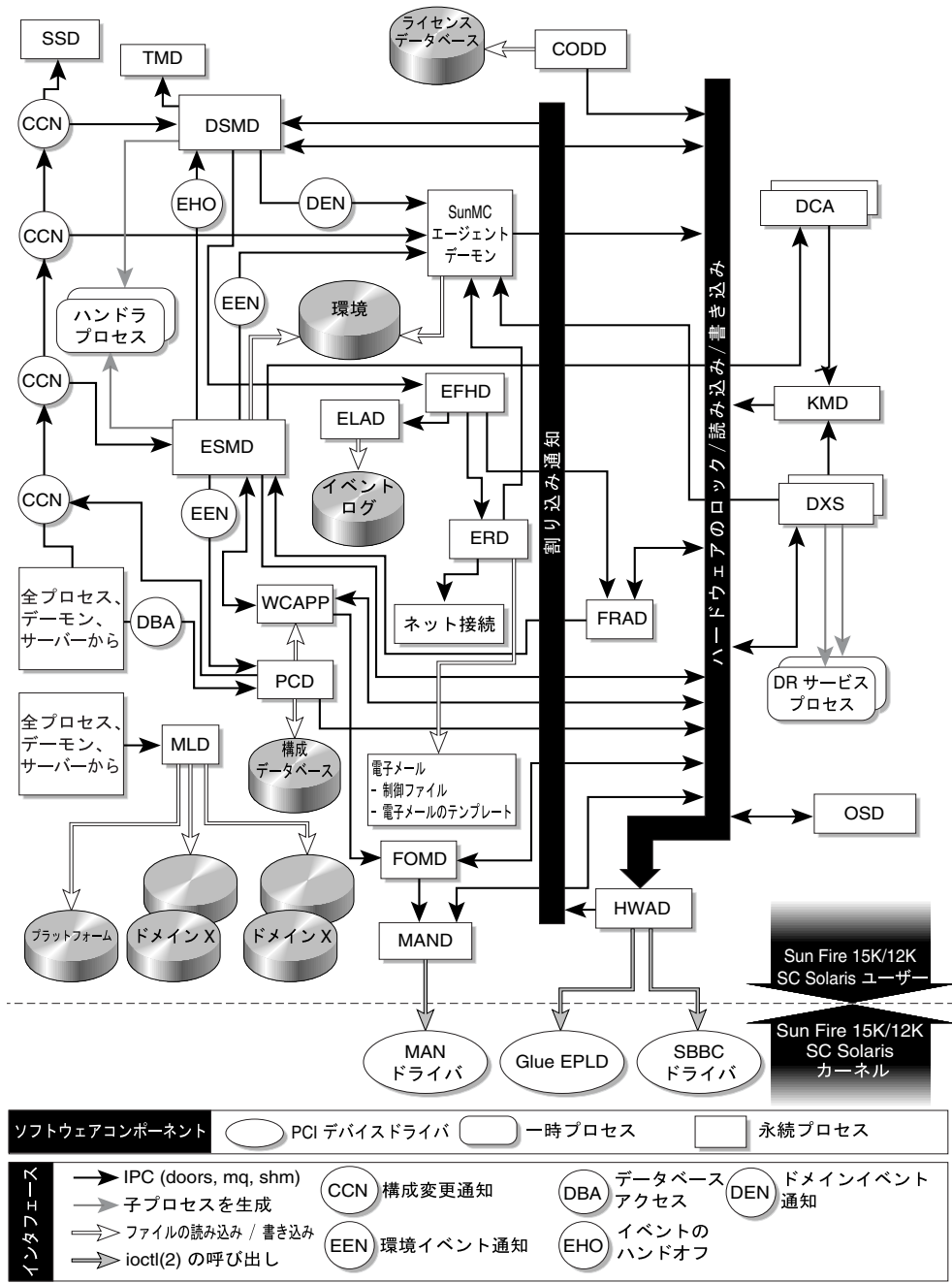


図 4-1 Sun Fire ハイエンドシステムのソフトウェアコンポーネント

注 - ドメイン X サーバー (dxs) およびドメイン構成エージェント (dca) はデーモンではありませんが、主要なサーバープロセスであるため次の表および節で説明します。各ドメインは、dxs と dca のインスタンスを実行します。インスタンスの最大数 (ドメインごとに各デーモンに 1 つのインスタンス) は、Sun Fire 15K/E25K の場合 18 個で、Sun Fire 12K/E20K の場合 9 個です。

表 4-1 デーモンおよびプロセス

デーモンの名前	説明
codd	capacity on demand デーモンは、使用される COD 資源を監視し、その資源が COD ライセンスデータベースファイルのライセンスと一致していることを確認します。このデーモンは、SMS 起動デーモンによって自動的に起動されます。
dca	ドメイン構成エージェントは、システムコントローラ上の dca と、指定されたドメイン上のドメイン構成サーバー (dcs) との通信メカニズムを提供します。最大 18 個までのすべてのドメインに、dca デーモンのインスタンスがそれぞれ 1 つあります。このデーモンは、SMS 起動デーモンによって自動的に起動されます。
dsmd	ドメインステータス監視デーモンは、Sun Fire 15K/E25K 上では最大 18 個、Sun Fire 12K/E20K 上では最大 9 個のドメインについて、ドメインのステータス、CPU リセット条件、および Solaris OS ハートビートを監視します。このデーモンは、SMS 起動デーモンによって自動的に起動されます。
dxs	ドメイン X サーバーは、ドメインにソフトウェアのサポートを提供する。提供するサポートには、動的再構成 (DR)、ホットプラグ可能な PCI I/O ボードのサポート、ドメインドライバの要求およびイベント、および仮想コンソールのサポートなどがあります。Sun Fire 15K/E25K では最大 18 個、Sun Fire 12K/E20K では最大 9 個の各ドメインに、dxs デーモンのインスタンスが 1 つずつあります。このデーモンは、SMS 起動デーモンによって自動的に起動されます。
efe	イベントフロントエンドデーモンは Sun Management Center の一部として、Sun Management Center エージェントと SMS との間を仲介します。efe の詳細については、『Sun Management Center 3.5 Sun Fire 15K/12K システムのための補足マニュアル』を参照。
efhd	エラーおよび障害処理デーモンは自動エラー診断を実行し、障害に関連するコンポーネントの健全性ステータスを更新します。このデーモンは、SMS 起動デーモンによって自動的に起動されます。
elad	イベントログアクセスデーモンは、SMS イベントログへのアクセスを制御します。このイベントログには、自動診断 (AD) エンジンによって特定された障害およびエラーイベントが記録されます。また、このデーモンは、現在のイベントログがサイズの限度に達して最も古いアーカイブファイルが削除されたときに、新しいイベントログファイルを開始します。

表 4-1 デーモンおよびプロセス (続き)

デーモンの名前	説明
erd	イベントレポートデーモンは、障害イベントメッセージをプラットフォームとドメインのログにレポートし、障害情報を Sun Management Center および Sun Remote Services Net Connect に提供し、障害イベントメッセージを含む電子メールレポートを配信します。このデーモンは、SMS 起動デーモンによって自動的に起動されます。
esmd	環境状態監視デーモンは、ファントレイ、電源装置、および温度などのシステムキャビネットの環境条件を監視します。このデーモンは、SMS 起動デーモンによって自動的に起動されます。
fomd	フェイルオーバー監視デーモンは、ローカルおよび遠隔の SC で発生した障害を検出して、適切なアクションを起こします (つまり、フェイルオーバーを開始します)。このデーモンは、SMS 起動デーモンによって自動的に起動されます。
frad	FRU アクセスデーモンは、SMS デーモンが Sun Fire ハイエンドシステム上で任意の現場交換可能ユニット (FRU) の SEEPROM (Serial Electrically Erasable Programmable Read-only Memory) にアクセスできるメカニズムを提供します。このデーモンは、SMS 起動デーモンによって自動的に起動されます。
hwad	ハードウェアアクセスデーモンは、SMS デーモンへのハードウェアアクセスを提供し、すべてのデーモンについては、ハードウェアに対して排他的にアクセス、制御、監視、および構成ができるメカニズムを提供します。このデーモンは、SMS 起動デーモンによって自動的に起動されます。
kmd	キー管理デーモンは、ドメインで動作中の SC とサーバー間の通信のセキュリティ保護に必要な、IPSec セキュリティ関連付け (SA) を管理します。このデーモンは、SMS 起動デーモンによって自動的に起動されます。
mand	管理ネットワークデーモンは MAN ドライバをサポートし、必要なネットワーク構成を提供します。mand の役割は、fomd で指定される。このデーモンは、SMS 起動デーモンによって自動的に起動されます。
mlD	メッセージロギングデーモンは、プラットフォームおよびドメインに対してメッセージロギングのサポートを提供します。このデーモンは、SMS 起動デーモンによって自動的に起動されます。
osd	OpenBoot PROM サーバーデーモンは、ドメインに存在するメールボックスを介して、ドメイン上で動作中の OpenBoot PROM プロセスに対してソフトウェアによるサポートを提供します。ドメインの OpenBoot PROM がメールボックスに要求を書き込むと、osd デーモンがその要求を実行します。メイン SC 上では、ドメインの起動を行います。このデーモンは、SMS 起動デーモンによって自動的に起動されます。

表 4-1 デーモンおよびプロセス (続き)

デーモンの名前	説明
pcd	プラットフォーム構成データベースデーモンは、プラットフォーム、ドメイン、およびシステムボードの構成データへの制御されたアクセスを提供および管理します。このデーモンは、SMS 起動デーモンによって自動的に起動されます。
ssd	SMS 起動デーモンは、すべての主要な SMS デーモンおよびサーバーを起動、停止、および監視します。
tmd	タスク管理デーモンは、SMS のスケジューリングなどのタスク管理サービスを提供します。setkeyswitch などのコマンドは、tmd を使用してハードウェアの電源投入時自己診断の起動をスケジューリングします。このデーモンは、SMS 起動デーモンによって自動的に起動されます。
wcapp	オプションの wPCI アプリケーションデーモンは、Sun Fire Link クラスタリング機能を実装し、外部 Sun Fire Link ファブリックマネージャサーバーに情報を提供します。wcapp の詳細は、『Sun Fire Link ファブリック管理者マニュアル』を参照。

Capacity on Demand デーモン

capacity on demand デーモン (codd (1M)) は、メインシステムコントローラ (SC) で実行されるプロセスです。

このプロセスは、次の役割を担当します。

- 使用される COD 資源を監視し、その資源が COD ライセンスデータベースファイルのライセンスと一致していることを確認する
- インストールされているライセンス、資源の使用状況、およびボードの状態に関する情報を提供する
- COD ライセンスキーの追加または削除の要求を処理する
- ヘッドルームの数とドメイン RTU (right-to-use) ライセンスの予約を構成する

図 4-2 は、COD デーモン (CODD) と SMS デーモンおよび CLI コマンドの関係を示します。

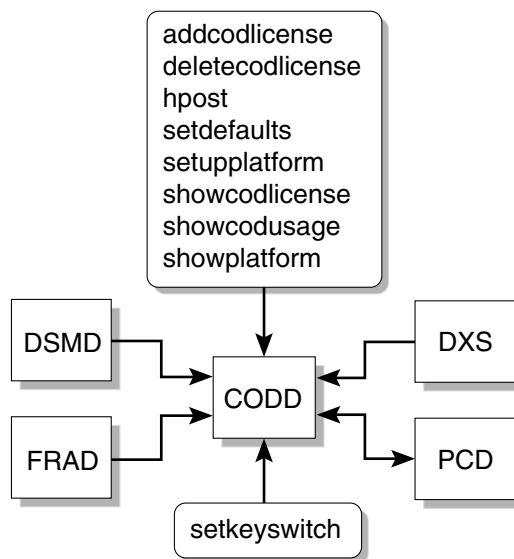


図 4-2 CODD でのクライアントサーバーの関係

ドメイン構成エージェント

ドメイン構成エージェントデーモン `dca(1M)` は、Solaris 8、Solaris 9、または Solaris 10 ドメインで実行中のアプリケーションとドメイン構成サーバー (`dcs`) の通信を可能にすることで、遠隔からの動的再構成 (DR) をサポートします。SC で実行されるドメインごとに、1つの `dca` が対応します。各 `dca` は、対応する `dcs` とは管理ネットワーク (MAN) を介して通信します。

`ssd(1M)` は、ドメインが作成されると `dca` を開始します。`ssd` は、ドメインの動作中に `dca` が終了されると、`dca` を再起動します。`dca` はドメインが停止するときに終了します。

`dca` は、動的再構成の要求を待機する SMS アプリケーションです。DR (動的再構成) 要求を受信すると、`dca` は `dcs` セッションを作成します。セッションが確立されると、`dca` は要求を `dcs` へ転送します。`dcs` は DR 要求を受け取り、その処理結果を `dca` へ送信します。結果が送信されると、セッションは終了します。遠隔からの DR 操作は、`dca` が DR 操作の結果を返信した時点で完了します。

図 4-3 は、ドメイン構成エージェント (DCA) と SMS デーモンおよび CLI の関係を示します。

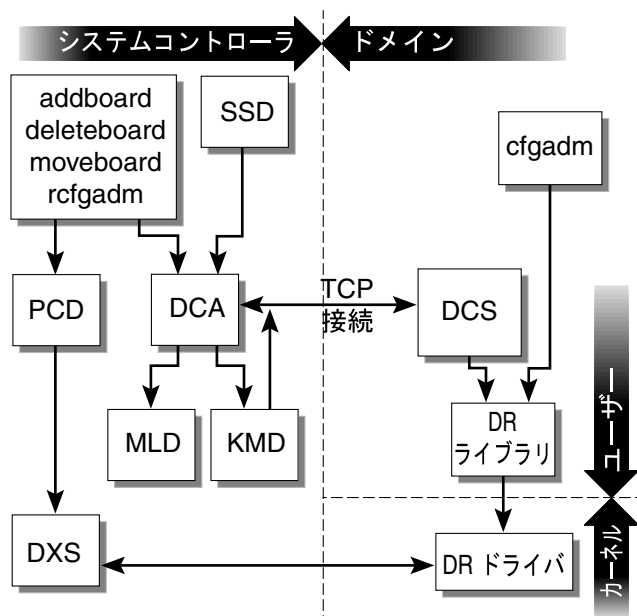


図 4-3 DCA でのクライアントサーバーの関係

ドメインステータス監視デーモン

ドメインステータス監視デーモン `dsmd(1M)` は、ドメイン状態のシグニチャー、CPU リセット条件、および Solaris ハートビートを Sun Fire 15K では最大 18 個のドメイン、Sun Fire 12K システムでは最大 9 個のドメインで監視します。また、このデーモンはハードウェア障害に関するドメイン停止イベントも処理します。

`dsmd` は、再起動トランザクションフローおよびパニックトランザクションフローで発生する可能性があるタイムアウトを検出して、さまざまなドメインハンガアップ条件を処理します。

`dsmd` は、ドメイン X サーバー (`dxs(1M)`) および Sun Management Center に対してすべてのドメイン状態の変更を通知してから、ドメイン状態のシグニチャー、ドメイン停止イベント、および自動システム回復 (ASR) のポリシーに基づいてドメインを自動的に復元します。ASR のポリシーは、1 つ以上のドメインがアクティブでなくなったあとに、適切に構成されたドメインがすべて動作するようにシステムを復元するための各種手続きから成り立っています。ドメインがアクティブでなくなる原因

は、ソフトウェアまたはハードウェアの障害や、不適切な環境条件などです。詳細については、171 ページの「ASR (Automatic System Recovery: 自動システム回復)」および223 ページの「ドメイン停止イベント」を参照してください。

また dsmd は、ドメイン停止に関連する自動診断 (AD) 情報も efhd に渡します。

図 4-4 は、DSMD と SMS デーモンおよび CLI の関係を示します。

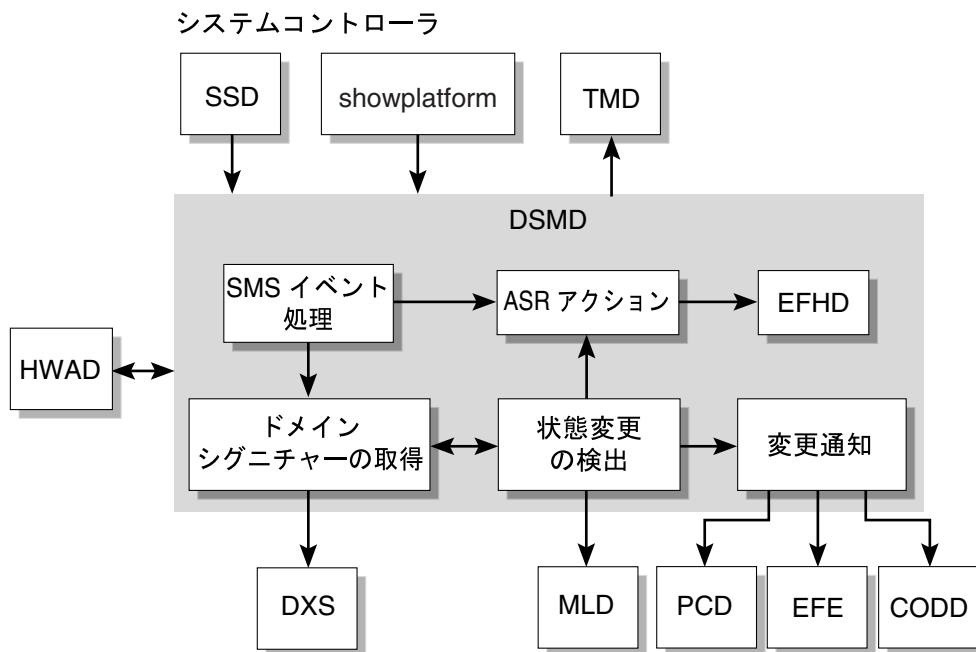


図 4-4 DSMD でのクライアントサーバーの関係

ドメイン X サーバー

ドメイン X サーバー dxs(1M) は、実行中のドメインのソフトウェアをサポートします。このサポートには、仮想コンソール機能、動的再構成のサポート、および HPCI のサポートが含まれます。dxs は、ドメインドライバの要求およびイベントを処理します。dxs は、HPCI スロットのステータスを取得および設定するためのインタフェースを提供します。スロットの状態には、カセットの有無、カセットが存在した場合のカセットの電力、周波数、健全性が含まれます。このインタフェースにより、HPCI カセットをホットプラグ操作する際の電源の制御が可能となります。

仮想コンソール機能によって、console プログラムを実行している 1 人以上のユーザーが、ドメインの仮想コンソールにアクセスできるようになります。dxs は、SMS コンソールアプリケーションと、ドメインの仮想 console ドライバの間のリンクとして動作します。

1 つの Sun Fire 15K システムは、18 個までのドメインを個別にサポートできます。1 つの Sun Fire 12K ドメインは 9 個までのドメインをサポートできます。各ドメインには SC によるソフトウェアサポートが必要な場合もありますが、dxs がこのサポートを提供します。ドメインに関連する以下のプロジェクトに、dxs のサポートが必要です。

- DR
- HPCI
- 仮想コンソール

各 Sun Fire ハイエンドシステムドメインには、ドメイン X サーバーが 1 台あります。dxs は ssd によりすべてのアクティブなドメイン (OS ソフトウェアを実行するドメイン) で開始され、ドメインがシャットダウンされるときに終了します。

図 4-5 は、DXS と SMS デーモンの関係を示します。

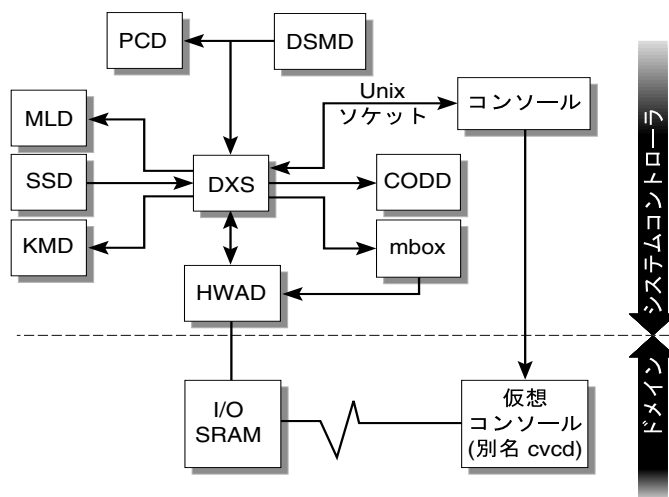


図 4-5 DXS におけるクライアントサーバーの関係

エラーおよび障害処理デーモン

エラーおよび障害処理デーモン efhd(1M) は、次の処理を行います。

- dsmd(1M) から渡されたドメイン停止情報に基づいて、自動エラー診断を実行します。

- 診断エンジン (SMS または Solaris OS) または POST によって障害が特定されたときに、障害が発生したコンポーネントの健全性ステータスを更新します。
- エラーのレポートを行う erd(1M) に障害イベントを渡します。

図 4-5 は、EFHD と SMS デーモンの関係を示します。

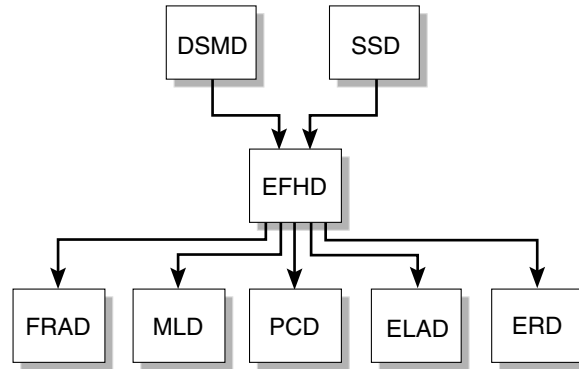


図 4-6 EFHD におけるクライアントサーバーの関係

イベントログアクセスデーモン

イベントログアクセスデーモン elad (1M) は、SMS イベントログへのアクセスを制御します。このイベントログには、Sun Fire ハイエンドシステムで、自動診断 (AD) エンジンまたは POST 診断エンジンによって特定される障害およびエラーイベントが記録されます。elad は、イベントログがいっぱいになったときに、イベントのアーカイブも行います。

図 4-7 は、イベントログアクセスデーモン (ELAD) と SMS デーモンおよび CLI コマンドの関係を示します。

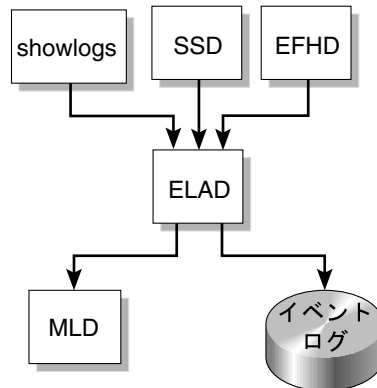


図 4-7 ELAD でのクライアントサーバーの関係

イベントレポートデーモン

イベントレポートデーモン `erd(1M)` は、障害イベントテキストメッセージをプラットフォームとドメインのログに書き込み、障害情報を **Sun Management Center** および **Sun Remote Services (SRS) Net Connect** に配信し、障害イベントメッセージが含まれた電子メールを送信するレポートサービスを提供します。

`erd` は、電子メールイベント通知があるたびに、電子メール制御ファイルと電子メールテンプレートファイルを読み取ります。

図 4-8 は、イベントレポートデーモン (ERD) と SMS デーモンの関係を示します。

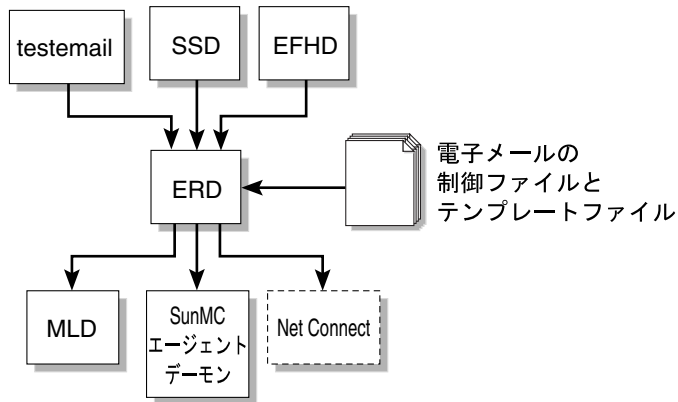


図 4-8 ERD におけるクライアントサーバーの関係

環境ステータス監視デーモン

環境ステータス監視デーモン `esmd(1M)` は、電圧、温度、ファントレー、電源装置、クロックフェージングなどの、システムキャビネットの環境条件を監視します。

`esmd` は異常な条件を記録し、必要に応じてハードウェアの保護する処置を実行します。

`esmd` の詳細については、219 ページの「環境イベント」を参照してください。

図 4-9 は、ESMD と SMS デーモンの関係を示します。

システムコントローラ

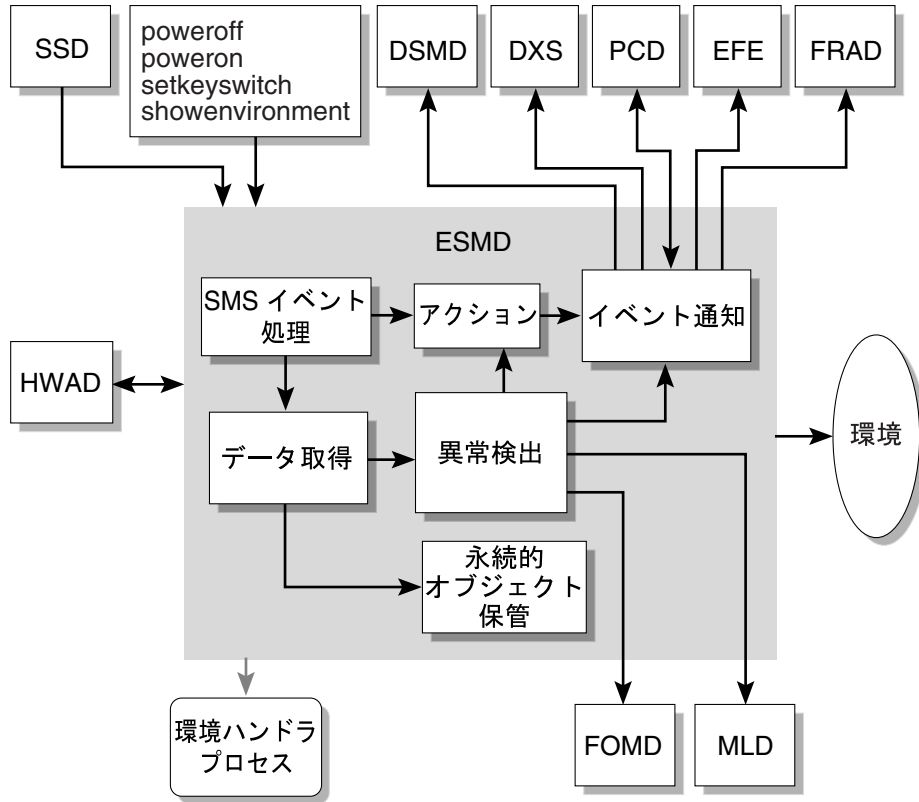


図 4-9 ESMD におけるクライアントサーバーの関係

フェイルオーバー管理デーモン

SC フェイルオーバーメカニズムの中心には、フェイルオーバー管理デーモン (fomd(1M)) があります。fomd はローカルおよび遠隔の SC の障害を検出し、適切な処置 (フェイルオーバーまたはテイクオーバーの開始) を実行します。fomd は、2 つの SC 間で重要な構成データの同期が保たれていることをテストして確認します。fomd はメイン SC およびスペア SC の両方で実行されます。

fomd についての詳細は、第 12 章を参照してください。

図 4-10 は、FOMD と SMS デーモンの関係を示します。

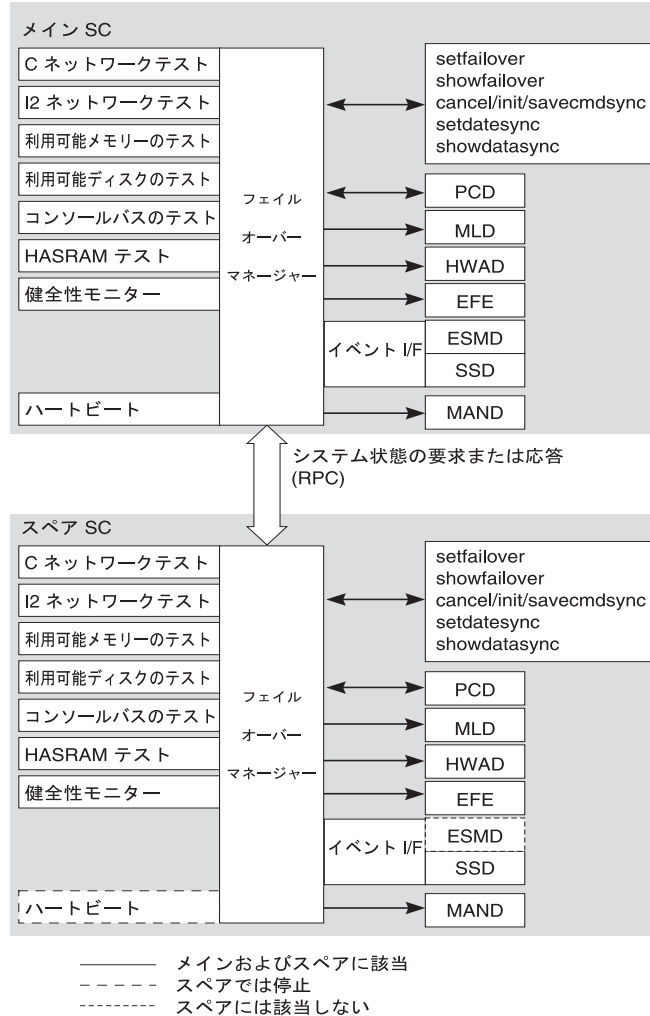


図 4-10 FOMD におけるクライアントサーバーの関係

FRU アクセスデーモン

FRU アクセスデーモン frad(1M) は、SMS 用の現場交換可能ユニット (FRU) アクセスデーモンです。SC がアクセス可能な Sun Fire ハイエンドプラットフォーム内の任意の SEEPROM へのアクセスは、frad が制御します。frad では、Solaris プラット

フォーム情報と制御ライブラリデーモン (PICLD) を使用して FRU データのアクセスを向上させる、動的 FRUID がサポートされています。FRU の情報は Sun の保守担当者だけが使用するものであり、ユーザーには意識されません。

frad は ssd により開始されます。

図 4-11 は、FRAD と SMS デーモンの関係を示します。

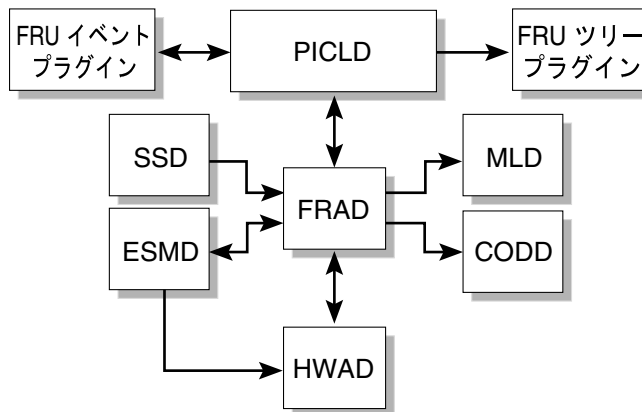


図 4-11 FRAD におけるクライアントサーバーの関係

ハードウェアアクセスデーモン

ハードウェアアクセスデーモン `hwad(1M)` は、SMS デーモンへのハードウェアアクセスを提供し、すべてのデーモンについては、ハードウェアに対して排他的にアクセス、制御、監視、および構成ができるメカニズムを提供します。

`hwad` は、起動されればメインモードまたはスペアモードのどちらでも実行できます。`hwad` がどちらの役割を担当するかは、フェイルオーバーデーモン (`fomd(1M)`) によって決まります。

`hwad` は、メインとスペアの両方で次の処理を行います。

- すべてのドライバ (`sbbc`、`echip`、`gchip`、および `consbus`) を開き、`ioctl(2)` への呼び出しを各ドライバとのインタフェースとして使用します。
- ローカルなシステムクロックを構成して、システムにある各ボードのクロックソースを指定します。
- SC 間割り込みを無効にします。
- SBBC システムの割り込みを許可するレジスタを消去することにより、DARB 割り込みを使用不可にします。
- `echip` ドライバからの割り込みを待機する `echip` インタフェースを作成します。起動時の `Echip` ドライバからの割り込みは、SC ハートビート割り込みです。

メイン SC では、hwad は次の処理を行います。

- 装置存在レジスタの内容を読み取って、システム内に存在するボードを識別し、それらをクライアントからアクセスできるようにします。
- I²C ステアリングを制御し、マシンに存在するすべてのボードの構成部品を初期化します。
- クロックがフェーズロックされていることを確認します。フェーズロックされている場合、hwad は、すべてのクロックソースがメイン SC を指し示していることを確認します。クロックがフェーズロックされていない場合には、hwad はクロックソースを変更せず、自動クロックスイッチを使用不可にします。
- DARB 割り込みを初期化して許可し、PCI 割り込みの生成を可能にします。gchip でのクロック障害割り込み、Echip でのコンソールバスエラー割り込み、echip での電源装置障害割り込みをすべて不可にします。
- イベントの割り込みハンドラを初期化し、mand、dsmd、および各 osd のサービスイベントに対するスレッドを作成します。
- 18 個のドメインに対して、IOSRAM インタフェースを作成します。このインタフェースにより、SC とドメインの間の通信が可能になります。

スペア SC では、hwad は次の処理を行います。

- メイン SC のクロックに対してスペア SC を設定します。
- リファレンス選択を 0 に設定します。
- SC 間割り込みを初期化します。

hwad は、動的再構成 (DR) では、IOSRAM (トンネルスイッチ) との通信を指定します。

hwad は dsmd(1M) に通知して、dstop または rstop が存在するかどうかを確認します。また、発生した Mbox 割り込みの種類に応じて、関連する SMS デーモン (複数可) に通知します。

hwad は、コンソールバスおよび JTAG のエラーを検出および記録します。

SC 上の Sun Fire ハイエンドシステムへのハードウェアアクセスは、PCI バスまたはコンソールバスのいずれかを通じて行います。PCI バスを通じて、次のものにアクセスできます。

- SC 起動バスコントローラ (BBC) 内部レジスタ
- SC ローカル JTAG インタフェース
- クロックおよび電源の制御または状態を示すグローバル I²C 装置

コンソールバスを通じて、以下のものにアクセスできます。

- 各種の特定用途集積回路 (ASIC)
- 読み取りまたは書き込み用チップ
- 温度およびチップレベルの電源制御や状態に関係する各種ボード上のローカルな I²C 装置

図 4-12 は、HWAD と SMS デーモンおよび CLI の関係を示します。

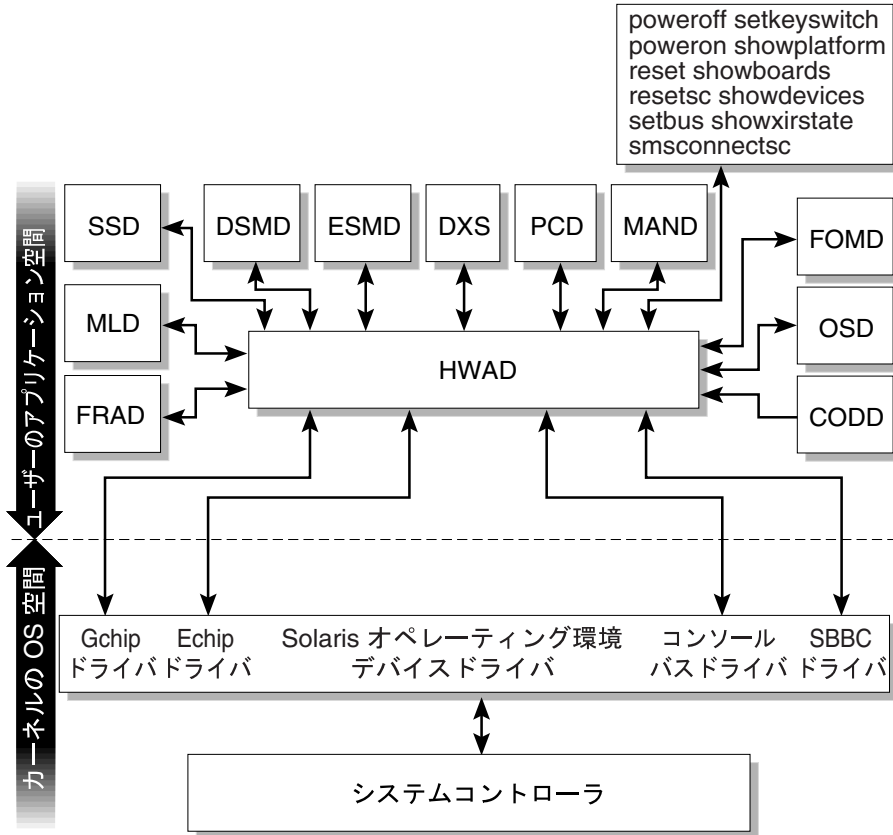


図 4-12 HWAD におけるクライアントサーバーの関係

キー管理デーモン

キー管理デーモン `kmd(1M)` は、SC とドメインの間のソケット通信に関するセキュリティーを管理するメカニズムを提供します。

現在のデフォルト構成では、SC 上の `dca(1M)` および `dxs` クライアントに関する認証ポリシーが含まれています。これらのクライアントは、ドメインの `dcs(1M)` および `cvcd(1M)` サーバーに接続します。

`kmd` は、ドメインで実行中の SC およびサーバー間の通信のセキュリティー確保に必要な、IPSec セキュリティー関連付け (SA) を管理します。

kmd は、SC 上のクライアントにより開始されたドメイン上のサーバーへの接続に関する、ソケットごとのポリシーを管理します。

システムの起動時に、kmd はアクティブな各ドメインへのドメインインタフェースを作成します。アクティブなドメインには有効な IOSRAM があり、Solaris OS が実行中です。ドメイン変更のイベントにより、ドメインの kmd インタフェースの作成または削除をトリガーできます。

kmd は、ドメイン上のクライアントが開始した SC 上のサーバーへの接続に関する、共有ポリシーを管理します。kmd のポリシーマネージャは、構成ファイルを読み取って、セキュリティの関連付けの管理に使用されるポリシーを格納します。kmd で受信された要求は現在のポリシーのセットと比較されて、要求が有効であり、要求のとおり各種のパラメータを設定できることが確認されます。

静的なグローバルポリシーは、ipsecconf(1M) および関連データファイル (/etc/inet/ipsecinit.conf) を使用して構成されます。グローバルポリシーは、各ドメインで開始される、SC への接続で使用されます。対応するエントリは、kmd の構成ファイル中に作成されます。ドメインから SC への接続での共有セキュリティ関連付けは、ドメインがアクティブになるときに kmd により作成されます。

注 – 正常に動作するには、ipsecconf で作成されたポリシーと、kmd で作成されたポリシーを一致させてください。

kmd の構成ファイルは、SC とドメイン間、およびドメインと SC 間で開始された接続のどちらでも使用されます。kmd 構成ファイルは、/etc/opt/SUNWSMS/config/kmd_policy.conf に入っています。

次に、kmd の構成ファイルのフォーマットを示します。

```
dir:d_port:protocol:sa_type:aut_alg:encr_alg:domain:login
```

ここで次の点に留意します。

dir	sctodom または domtosc 文字列を使用して識別されます。
d_port	接続先ポートです。
protocol	tcp または udp 文字列を使用して識別されます。
sa_type	セキュリティの関連付けの種類を示します。有効な選択肢は、ah または esp 文字列です。
auth_alg	認証アルゴリズムを示します。認証アルゴリズムは、none または hmac-md5 文字列を使用するか、このフィールドを空白にすることで識別されます。

<code>encr_alg</code>	暗号化アルゴリズムを示します。暗号化アルゴリズムは、 <code>none</code> または <code>des</code> 文字列を使用するか、このフィールドを空白にすることで識別されま す。
<code>domain</code>	ドメインと関連付けられている <i>domain-id</i> を示 します。有効な <i>domain-id</i> は、整数 0 ~ 17 と空白文 字です。 <i>domain-id</i> フィールドに空白文字を使用す ると、すべてのドメインを適用対象としてポリ シーが定義されます。特定のドメインが対象のポ リシーは、すべてのドメインに適用されるポリ シーよりも優先されます。
<code>login_name</code>	ポリシーの影響を受けるユーザーのログイン名で す。現在、これには <code>sms-dxs</code> 、 <code>sms-dca</code> 、および <code>sms-mlid</code> が含まれます。

たとえば、次のメッセージが表示されます。

```
# Copyright (c) 2004 by Sun Microsystems, Inc.
# All rights reserved.
#
# This is the policy configuration file for the SMS Key Management Daemon.
# The policies defined in this file control the desired security for socket
# communications between the system controller and domains.
#
# The policies defined in this file must match the policies defined on the
# corresponding domains. See /etc/inet/ipsecinit.conf on the Sun Fire ハイエンド
# system domain.
# See also the ipsec(7P), ipsecconf(1M) and sckmd(1M) man pages.
#
# The fields in the policies are a tuple of eight fields separated by the pipe
# '|' # character.
#
# <dir>|<d_port>|<protocol>|<sa_type>|<auth_alg>|<encr_alg>|<domain>|<login>|
#
# <dir>          --- direction to connect from. Values: sctodom, domtosc
# <d_port>       --- destination port
# <protocol>     --- protocol for the socket. Values: tcp, udp
# <sa_type>      --- security association type. Values: ah, esp
# <auth_alg>     --- authentication algorithm. Values: none, md5, sha1
# <encr_alg>     --- encryption algorithm. Values: none, des, 3des
# <domain>      --- domain id. Values: integers 0 - 17, space
#                A space for the domain id defines a policy which applies
#                to all domains. A policy for a specific domain overrides
#                a policy which applied to all domains.
# <login>       --- login name. Values: Any valid login name
#
# -----
sctodom|665|tcp|ah|md5|none| |sms-dca|
sctodom|442|tcp|ah|md5|none| |sms-dxs|
```


図 4-13 は、KMD と SMS デーモンの関係を示します。

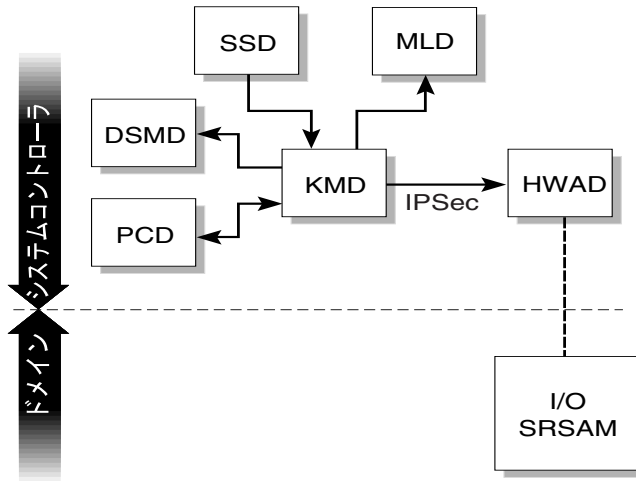


図 4-13 KMD におけるクライアントサーバーの関係

管理ネットワークデーモン

管理ネットワークデーモン `mand(1M)` は、管理ネットワーク (MAN) をサポートします。MAN ネットワークについての詳細は、193 ページの「管理ネットワークのサービス」を参照してください。デフォルトでは `mand` はスペアモードで起動し、フェイルオーバーデーモン (`fomd(1M)`) によってメインモードに切り換えるよう指定したときに、メインモードに切り換わります。`mand` がどちらの役割を担当するかは、`fomd` によって決まります。

システムの起動時に、`mand` はスペアとして起動し、SC 間のプライベートネットワークを構成します。この情報は、`smsconfig(1M)` コマンドにより作成される `/etc/opt/SUNWSMS/config/MAN.cf` というファイルから取得されます。フェイルオーバーデーモン (`fomd(1M)`) が、`mand` にメインの役割を引き継ぐよう指示します。

メインの役割では、`mand` は次の処理を行います。

- プラットフォーム構成データベース (`pcd`) のドメイン変更イベントを登録して、ドメインのアクティブなボードのリストに加えられた変更を追跡します。
- `domain_tag` と IP アドレス とのマッピングを `pcd` に作成します。
- 現在のドメイン構成で `scman(7d)` ドライバを初期化します。
- `hwad` のイベントを登録し、`dman(7d)` ドライバからのアクティブな Ethernet 情報を追跡します。
- `scman` ドライバと `pcd` を、必要に応じて更新します。

- ドメインに電源投入されたとき (setkeyswitch がオンのとき) に、ドメインのキースイッチイベントを登録し、システム起動の MAN 情報を各ドメインに通知します。この情報には、Ethernet および MAN IP のアドレス情報と、ドメインでの初期ソフトウェアインストール時に使用されるアクティブなボードのリストが含まれます。

図 4-14 は、MAND と SMS デーモンの関係を示します。

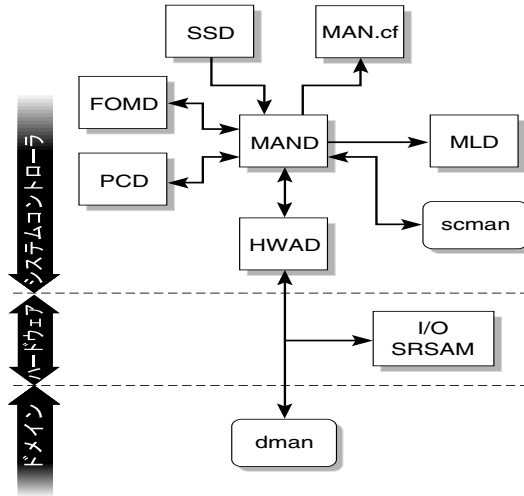


図 4-14 MAND におけるクライアントサーバーの関係

メッセージロギングデーモン

メッセージロギングデーモン mld(1M) は、ほかのすべての SMS デーモンおよびプロセスの出力をキャプチャーします。mld は、`/var/opt/SUNWSMS/adm/.logger` ファイルにある File、Level、および Mode の 3 つの構成命令をサポートしています。

- File - メッセージファイルが出力されるデフォルトの場所を指定します。デフォルトは `msgdaemon` で、この値は変更するべきではありません。
 - プラットフォームのメッセージは、SC の `/var/opt/SUNWSMS/adm/platform/messages` に格納されます。
 - ドメインのメッセージは、SC の `/var/opt/SUNWSMS/adm/domain-id/messages` に格納されます。
 - ドメインの console のメッセージは、SC の `/var/opt/SUNWSMS/adm/domain-id/console` に格納されます。
 - ドメインの syslog のメッセージは、SC の `/var/opt/SUNWSMS/adm/domain-id/syslog` に格納されます。

- **Level** - ログに記録する必要があるメッセージの最小レベルを指定します。サポートされているレベルは、NOTICE、WARNING、ERR、CRIT、ALERT、および EMERG です。デフォルトのレベルは NOTICE です。
- **Mode** - メッセージの冗長性を指定します。2つのモード、verbose と terse を使用できます。デフォルトは verbose モードです。

mld は、各メッセージログファイルのサイズを監視します。メッセージログの種類ごとに、mld は一度に最大 10 個のメッセージファイル、つまり x.0 から x.9 までを保持します。ログメッセージの詳細は、207 ページの「メッセージロギング」を参照してください。

図 4-15 は、メッセージロギングデーモン (MLD) と SMS デーモンおよび CLI の関係を示します。

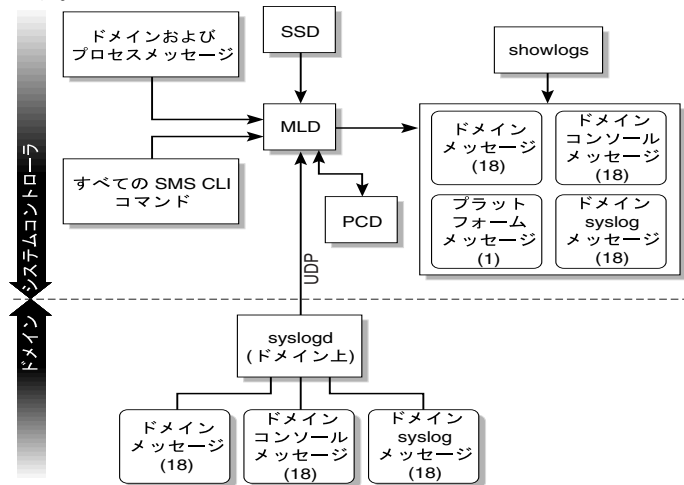


図 4-15 MLD におけるクライアントサーバーの関係

OpenBoot PROM サポートデーモン

OpenBoot PROM サポートデーモン osd(1M) は、ドメインで動作中の OpenBoot PROM プロセスをサポートします。osd と OpenBoot PROM との通信は、ドメイン上にあるメールボックスを介して行われます。osd デーモンは、OpenBoot PROM のメールボックスを監視します。OpenBoot PROM がメールボックスに要求を書き込むと、osd が要求を実行します。

osd は、構成済みのドメインがない場合でも、SC 上で常に実行されています。osd は、OpenBoot PROM 用の仮想時刻 (TOD) サービス、仮想 NVRAM (非揮発性のランダムアクセスメモリー)、および仮想 REBOOTINFO を提供し、さらに自動ドメイン回復を容易にするための dsmd(1M) へのインターフェースを提供します。また、osd

は `setobpparams(1M)`、`showobpparams(1M)`、`setdate(1M)`、および `showdate(1M)` の各コマンドへのインタフェースも提供します。詳細については、第 5 章を参照。

`osd` は、他の SMS プロセスにインタフェースをまったくエクスポートしないという点で信頼できるデーモンです。`osd` は、OpenBoot PROM メールボックスとの読み取りおよび書き込みを排他的に行います。OpenBoot PROM メールボックスは、各ドメインに 1 つあります。

`osd` には主に 2 つのタスクがあります。ドメイン構成の現在の状態を維持すること、および OpenBoot PROM メールボックスを監視することです。

図 4-16 は、OpenBoot PROM サポートデーモン (OSD) と SMS デーモンおよび CLI の関係を示します。

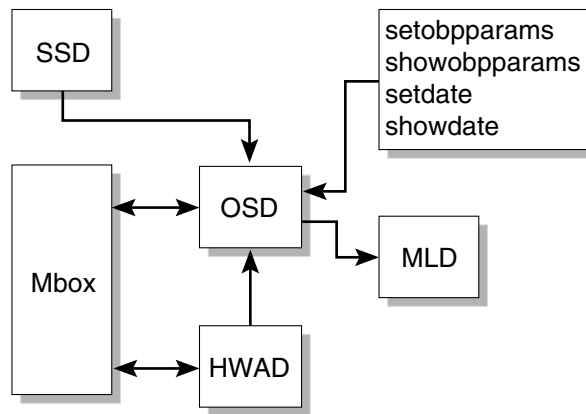


図 4-16 OSD におけるクライアントサーバーの関係

プラットフォーム構成データベースデーモン

プラットフォーム構成デーモン `pcd(1M)` は、SC 上で実行する Sun Fire ハイエンドシステム管理デーモンで、プラットフォームおよびドメインの構成データへのアクセスを管理および提供することが主な役割です。

`pcd` は、Sun Fire システムの構成を示す一連の情報を管理します。データベースの情報は、物理的にはフラットファイルの集まりであり、各ファイルはその内容で識別できます。データベース情報にアクセスする場合、SMS アプリケーションはすべて必ず `pcd` を経由しなければなりません。

プラットフォーム構成データの管理以外に、`pcd` はプラットフォーム構成が変更された場合の通知も行います。システム内でプラットフォーム構成に永続的な変更があったとき、`pcd` は、受信登録済みのクライアントに対して変更の通知を送信します。

図 4-17 は、プラットフォーム構成データベースデーモン (PCD) と SMS デーモンおよび CLI の関係を示します。

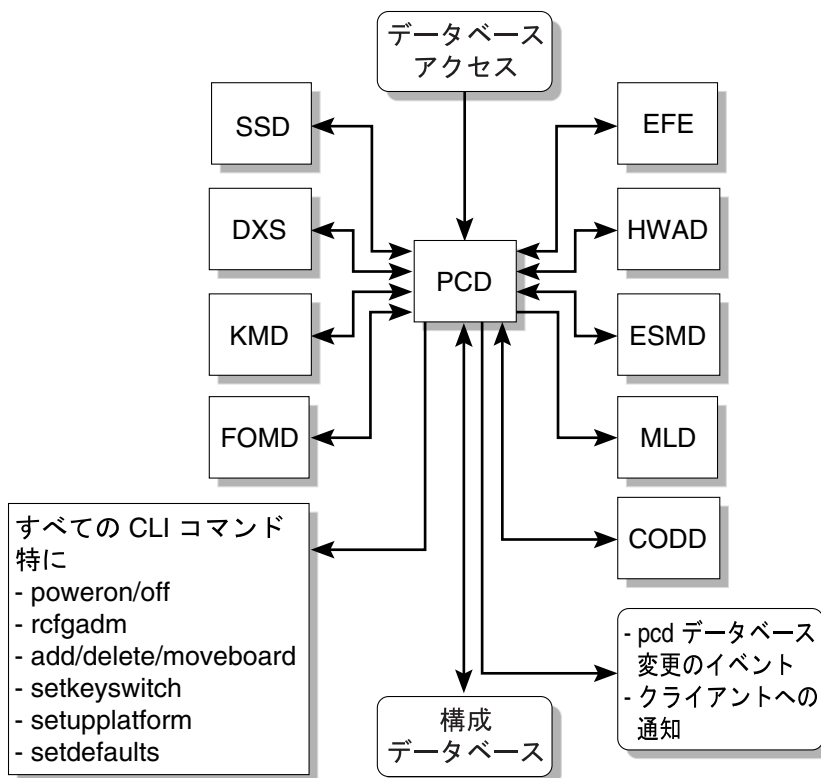


図 4-17 PCD におけるクライアントサーバーの関係

プラットフォームの構成

以下の情報で、プラットフォームを一意に識別できます。

- プラットフォームの種類
- プラットフォーム名
- シャーシのホスト ID

シャーシのホスト ID は、COD ライセンスを取得するために、COD 機能でプラットフォームを特定する際にのみ使用されます。シャーシのホスト ID はセンターブレーンのシリアル番号で、システム内部に記録されています。シャーシのホスト ID を表示するには、`showplatform -p cod` コマンドを実行します。

- シャーシのシリアル番号

シャーシのシリアル番号は Sun Fire ハイエンドシステムを特定する番号で、メッセージとイベントでプラットフォームを特定するときに使用されます。この番号は、サービスプロバイダがイベントと保守アクションを該当するシステムに関連付けるときにも使用されます。シャーシのシリアル番号は、システムシャーシ正面の下部中央付近に貼付されているラベルに印刷されています。SMS 1.4 からは、シャーシのシリアル番号は、Sun での製造時に SMS をインストールして出荷するシステム上に自動的に記録されます。シャーシのシリアル番号を表示するには、`showplatform -p csn` コマンドを実行します。

前のバージョンの SMS から SMS 1.6 以降にアップグレードする場合は、`setcsn(1M)` コマンドを使用して、シャーシのシリアル番号を記録してください。setcsn コマンドについての詳細は、『System Management Services (SMS) 1.6 リファレンスマニュアル』のコマンドの説明を参照してください。

- キャッシュ可能なアドレススライスマップ
- システムのクロック周波数
- システムクロックの種類
- SC IP アドレス
- SC0 から SC1 の IP アドレス
- SC1 から SC0 の IP アドレス
- SC から SC の IP ネットマスク
- COD インスタントアクセス CPU (ヘッドルーム)

ドメインの構成

次に、ドメインに関連する情報を示します。

- *domain-id*
- *domain-tag*
- OS のバージョン (現在は未使用)
- OS の種類 (現在は未使用)
- 使用可能構成要素リスト
- 割り当てられているボードのリスト
- アクティブなボードのリスト
- Golden IOSRAM I/O ボード
- ドメインの仮想キースイッチ設定
- アクティブな Ethernet I/O ボード
- ドメイン作成時刻
- ドメインダンプの状態
- ドメイン起動の優先順位

- IP ホストアドレス
- ホスト名
- ホストのネットマスク
- ホストのブロードキャストアドレス
- 仮想 OpenBoot PROM アドレス
- 物理 OpenBoot PROM アドレス
- COD RTU ライセンス予約

システムボードの構成

以下に、システムボードに関連する情報を示します。

- 拡張ボードの位置
- スロットの位置
- ボードの種類
- ボードの状態
- ボードに割り当てられたドメインID
- 使用可能構成要素リストの状態
- ボードテストの状態
- ボードテストのレベル
- ボードメモリークリア状態
- COD 使用可能フラグ

SMS 起動デーモン

SMS 起動デーモン `ssd(1M)` は、すべての SMS デーモンおよびドメイン X サーバーの起動と管理を担当します。

`ssd` は、特定ファイルの可用性および Sun Fire ハイエンドシステムの可用性に関して環境を調査し、環境変数を設定し、さらにメイン SC の `esmd(1M)` を起動します。`esmd` は関連するハードウェアコンポーネントをポーリングして、環境の変更状況を監視します。異常な状況を検出すると、`esmd` は自身でそれを処理するか、またはイベントを生成して、対応するイベントハンドラに適切なアクションを実行させたり、現在のハンドラの状態を更新させたりします。イベントハンドラには、たとえば `dsmd` や `pcd` などがあります。Sun Management Center も、インストールされている場合には、イベントハンドラに含まれます。`ssd` の主な役割は、SMS のデーモンとサーバーを常時、確実に動作させることです。

図 4-18 は、SSD と SMS デーモンの関係を示します。

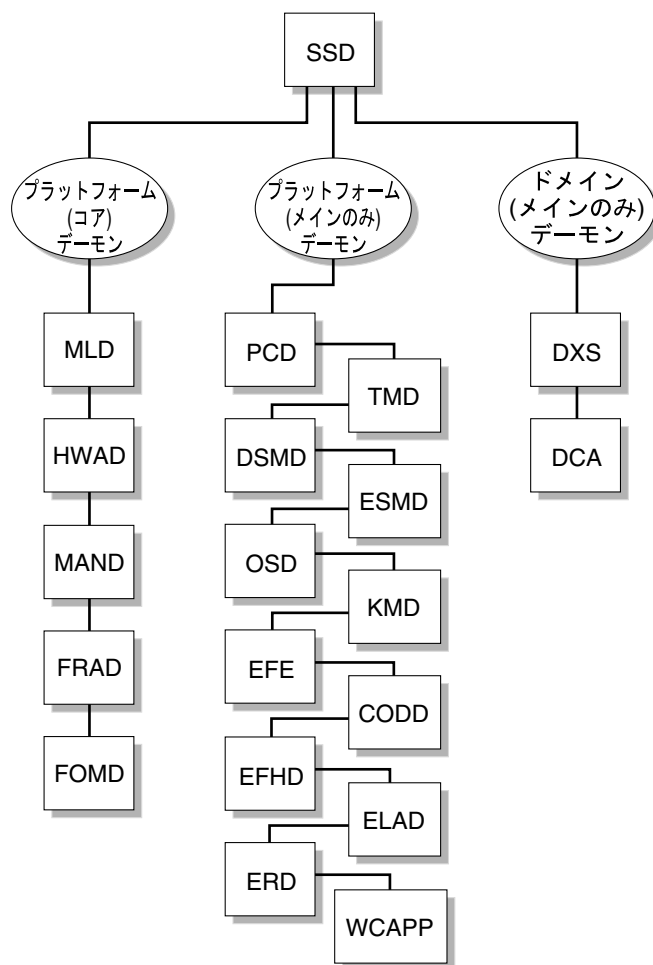


図 4-18 SSD におけるクライアントサーバーの関係

スクリプト

ssd は、構成ファイル `ssd_start` を使用して、起動する SMS コンポーネントとそれらの起動順序を判断します。この構成ファイルは、`/etc/opt/SUNWSMS/startup` ディレクトリにあります。



注意 – このファイルが、システム構成ファイルです。このファイルの編集を誤ると、システムが動作しなくなる可能性があります。このスクリプトで編集すべきフィールドは、`args` だけです。特定のオプションについては、デーモンのマニュアルページを参照してください (スクリプトの構文には、特に注意してください)。

`ssd_start` は、以下のフォーマットのエントリからなります。

`name:args:nice:role:type:trigger:startup-timeout:shut down-timeout:uid:start-order:stop-order`

ここで次の点に留意します。

<code>name</code>	プログラムの名前です。
<code>args</code>	有効なプログラムオプションまたは引数です。詳細については、デーモンのマニュアルページを参照してください。
<code>nice</code>	プロセスの優先順位を調整する値を指定します。この値は 変更しないでください 。
<code>role</code>	デーモンがプラットフォームまたはドメインに固有のものであるかどうかを指定します。
<code>type</code>	プログラムがデーモンまたはサーバーのどちらであるかを指定します。
<code>trigger</code>	プログラムが自動的に開始されるべきか、またはイベント受信時に開始されるべきかを指定します。
<code>startup-timeout</code>	<code>ssd</code> がプログラムの起動を待機する時間を秒単位で示します。
<code>stop-timeout</code>	<code>ssd</code> がプログラムのシャットダウンを待機する時間を秒単位で示します。
<code>uid</code>	関連付けられたプログラムの実行に使用される <code>user-id</code> です。
<code>start-order</code>	<code>ssd</code> がデーモンを起動する順序を定義します。この値は 変更しないでください 。デフォルト値を変更すると、SMS デーモンが正しく機能しなくなる可能性があります。
<code>stop-order</code>	<code>ssd</code> がデーモンを停止する順序を定義します。この値は 変更しないでください 。デフォルト値を変更すると、SMS デーモンが正しく機能しなくなる可能性があります。

スペアモード

ssd が起動するときは、必ず spare モードで起動します。ssd が起動するとプラットフォームのコアとなるデーモンが実行中なので、ssd は fomd(1M) に対して自身の役割を問い合わせます。fomd が spare を返した場合、ssd はスペアモードのままです。fomd が main を返した場合、ssd は main モードに移行します。

初期の問い合わせフェーズの後、ssd がモードを切り替えるのは fomd からイベントを受信した場合だけです。

spare モードでは、ssd は主要な platform 役割のすべてを開始および監視し、ssd_start ファイルに記述されているプログラムを auto で (自動的に) 起動します。現在、このファイルには次のプログラムが記述されています。

- mld
- hwad
- mand
- frad
- fomd

main モードのときに ssd が spare イベントを受信した場合、ssd は主要な platform 役割を除くすべてのプログラムをシャットダウンして、ssd_start ファイルにあるプログラムを auto で (自動的に) 起動します。

メインモード

ssd は、main イベントを受信するまでは spare モードのままです。この時点で ssd が開始して、すでに実行中のデーモンのほかに、ssd_start ファイルに記述されているメイン platform 役割、event 起動プログラムのすべてを開始および監視します。このファイルには次のプログラムが記述されています。

- pcd
- tmd
- dsmd
- esmd
- osd
- kmd
- efe
- codd
- efhd
- elad
- erd
- wcapp

最後に、すべての platform 役割、event 起動プログラムを開始した後で、ssd は pcd に照会して、どのドメインがアクティブであるかを判別します。これらの各ドメインについて、ssd は domain 役割と、ssd_start ファイルに記述されている event 起動プログラムのすべてを開始します。

ドメイン固有のプロセス起動

ssd は、pcd からのドメイン開始および停止のイベントを、ドメイン固有のサーバーを開始および停止するための命令として使用します。

命令を受信すると、ssd は domain 役割と、ssd_start ファイルに記述されている event 起動プログラム (識別されたドメインのもの) のすべてを開始または停止します。

監視および再起動

いったんプロセスを開始した ssd は、プロセスを監視するとともに、プロセスが失敗した場合には再開します。

SMS のシャットダウン

SMS ソフトウェアのアップグレードなど、特定の状況では SMS ソフトウェアを停止します。ssd は、自分自身と、自分の制御下にあるすべての SMS デーモンおよびサーバーを停止するメカニズムを提供します。

ssd は、自分の制御下にあるすべての SMS ソフトウェアコンポーネントにシャットダウンするよう通知します。すべての SMS ソフトウェアコンポーネントがシャットダウンした後で、ssd は自身をシャットダウンします。

タスク管理デーモン

タスク管理デーモン tmd(1M) は、タスク管理サービス (たとえば SMS のスケジューリングなど) を提供する。タスク管理デーモンにより、ハードウェアのテストとソフトウェアの構成を並行して実施する場合に起こりうるさまざまな衝突が減少します。

現時点では、tmd によりエクスポートされる唯一のサービスは hpost(1M) スケジューリングサービスです。Sun Fire ハイエンドシステムでは、hpost は次に示す 2 つの要素に基づいてスケジューリングされます。

- hpost の制限事項。プラットフォームが最初に起動したときにドメインが構成されていないと、hpost の単一のインスタンスがすべての拡張ボードについて排他的な制御を取得し、センタープレーン ASIC を構成します。以後のすべての hpost 呼び出しは、この処理が完了するのを待ってから進むこととなります。

任意の拡張ボード 1 つに 1 度に作用できるのは、単一の hpost 呼び出しだけです。分割拡張ボードなしで構成された Sun Fire ハイエンドシステムの場合は、この制限にかかわらず複数の hpost 呼び出しを実行できます。ただし、システムが分割拡張ボードありで構成されているときは、この制限事項の影響を受けます。

- システム全体での hpost 起動数の制限。システムを飽和させずに同時に起動できる hpost の数には制限があります。hpost 呼び出しの数を制限する機能は、`ssd_startup` の `-t` オプションを使用して実行できます。



注意 – デフォルト値を変更すると、システムの機能に悪影響を与える場合があります。Sun のサービス担当者から指示されないかぎり、このパラメータは調節しないでください。

図 4-19 は、TMD と SMS デーモンの関係を示します。

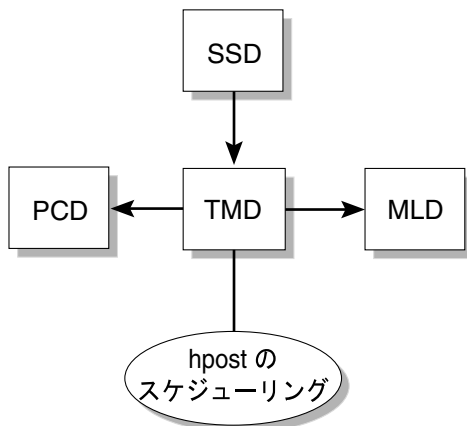


図 4-19 TMD におけるクライアントサーバーの関係

環境変数

SMS 環境の基本的なデフォルト値は、SMS のコマンドを実行する構成ファイルに設定されている**必要があります**。

- `PATH` に `/opt/SUNWSMS/bin` を追加
- `LD_LIBRARY_PATH` に `/opt/SUNWSMS/lib` を追加
- `MANPATH` に `/opt/SUNWSMS/man` を追加

ログイン時にほかの環境変数を設定すると、時間を節約できます。表 4-2 に、便利な SMS 環境変数をいくつか示します。

表 4-2 環境変数の例

変数	説明
SMSETC	その他の SMS 関連ファイルが格納されている /etc/opt/SUNWSMS/ ディレクトリへのパス
SMSLOGGER	メッセージロギングのためのファイル .logger が格納されている /var/opt/SUNWSMS/adm ディレクトリへのパス
SMSOPT	SMS パッケージのバイナリ、ライブラリ、およびオブジェクトファイル、構成ファイルおよび起動ファイルが格納されている /opt/SUNWSMS/ ディレクトリへのパス
SMSVAR	プラットフォームおよびドメインのメッセージファイルおよびデータファイルが格納されている /var/opt/SUNWSMS/ ディレクトリへのパス

SMS ドメイン構成

「動的システムドメイン」(DSD) は、サーバーのサブセットである独立した環境で、固有のファームウェアのバージョンおよび固有の Solaris OS のバージョンを実行することができます。各ドメインは、互いに独立しています。ドメインの継続的な稼働は、他のドメインでソフトウェア障害やハードウェア障害が発生しても影響を受けることはありません。

システムコントローラ (SC) は、システムボードを「動的システムドメイン」(または、単に「ドメイン」と呼ぶ) に論理的にグループ化できるコマンドをサポートします。ドメインは、専用の OS の実行および自分自身の作業負荷の処理を実行できます。ドメインは、他のドメインの稼働に影響を与えずに作成および削除が可能です。ドメインは、さまざまな目的に使用することができます。たとえば、ドメインで新しいバージョンの OS をテストしたり、開発環境およびテスト環境を設定したりできます。この手法では、問題が起こったときでもシステムのそれ以外の部分は影響を受けません。

1つの区分に1つのドメインを割り当てて、さまざまな区分をサポートするように複数のドメインを構成することもできます。一時的にシステムを1つのドメインで再構成すれば、週末の期間中に大規模なジョブを実行させておくことが可能です。

Sun Fire 15K システムは、最大 18 ドメインを構成することができます。Sun Fire 12K システムは、最大 9 ドメインを構成することができます。

ドメイン構成を行うと、ドメインとサーバーのハードウェアコンポーネントの間にマッピングが確立されます。各種のシステム管理パラメータおよび各ドメインのポリシーの確定も、ドメイン構成の中に含まれます。この章は、Sun Fire ハイエンドシステムが提供するドメイン構成機能のすべての側面について解説します。

この章では、次の項目を説明します。

- 86 ページの「ドメイン構成ユニット」
- 86 ページの「ドメイン構成の条件」
- 87 ページの「DCU の割り当て」
- 88 ページの「プラットフォーム管理者のための構成」
- 106 ページの「ドメイン管理者のための構成」
- 124 ページの「機能が低下した構成の設定の変更」

ドメイン構成ユニット

ドメイン構成ユニット (DCU) は、単独のドメインへの割り当てが可能なハードウェアユニットです。ドメインは、このハードウェアコンポーネントを使用して構築します。ドメインに割り当てられない DCU を **ドメイン無し** と呼びます。

すべての DCU はシステムボードで、またすべてのシステムボードは DCU です。Sun Fire ハイエンドシステムの DCU の構成は以下のとおりです。

- システムボード
- Sun Fire HsPCI I/O ボード (HPCI)
- Sun Fire HsPCI+ I/O ボード (HPCI+)
- Sun Fire MaxCPU ボード (MCPU)
- Sun Fire Link wPCI ボード (WPCI)

Sun Fire ハイエンドシステムのハードウェアには通常システムボードが 1 枚以上必要で、構成するドメインごとに I/O タイプのボードが 1 枚以上必要です。csb、exb ボード、および SC は DCU ではありません。

注 – MaxCPU ボードにメモリーは搭載されていません。ドメインを設定するには、通常の CPU ボードが 1 枚以上必要です。

ドメイン構成の条件

以下の条件が満たされれば、システムボードの任意のグループからドメインを作成することができます。

- 他のドメインが使用していないボードがあります。
- 1 枚以上のボードに CPU とメモリーがあります。
- 1 枚以上の I/O ボードがあります。
- 1 枚以上のボードにネットワークインタフェースがあります。
- ボードに、独立したドメインをサポートする十分なメモリーがあります。
- 新規ドメインの名前が重複しません。(addtag (1M) コマンドで指定される。)
- 工場から出荷されたドメイン用の idprom.image ファイルがあります。
idprom.image ファイルが誤って削除されていたり破壊されていてバックアップがない場合には、ご購入先に連絡してください。

- 1つ以上の起動ディスクが、ドメインに分類される複数のボードの1つに接続されています。ドメインに専用のディスクがない場合は、ネットワークからのドメインの起動が可能な1つ以上のネットワークインタフェースがあります。

DCU の割り当て

ドメインに DCU を割り当てるには、DCU (システムボード) で以下に示す 3 つの論理操作のいずれかを行います。

- ドメインに (ドメイン無しから) ボードを追加します。
- ドメインのボードを取り外します。 (ボードをドメイン無しにする。)
- ドメイン間でボードを移動します。

静的および動的なドメイン構成

DCU の割り当てには 3 つの論理的な操作がありますが、基礎となる実装は 4 つのドメイン構成処理が元となります。

- アクティブでないドメインにボードを追加します。
- アクティブではないドメインからボードを取り外します。
- アクティブなドメインにボードを追加します。
- アクティブなドメインからボードを取り外します。

最初の 2 つのドメイン構成操作は、アクティブではないドメイン (OS ソフトウェアが稼働していないドメイン) に適用されます。これらの操作を、「静的なドメイン構成」操作と呼びます。あとの 2 つのドメイン構成操作は、アクティブなドメイン (OS ソフトウェアが稼働しているドメイン) に適用され、「動的なドメイン構成」操作と呼びます。

動的ドメイン構成では、DCU 常駐の資源 (CPU、メモリー、I/O デバイスなど) を Solaris OS の制御下に導入またはその制御下から削除するために、ドメインの Solaris ソフトウェアとの対話が必要になります。Sun Fire ハイエンドシステムの動的再構成 (DR) は、ドメインの Solaris 環境から動的構成サービスを要求するために、SC などの外部エージェント用に遠隔 DR と呼ばれる機能を提供します。

SC コマンドのユーザーインタフェースは、要求されたタスクを実行するために必要に応じて遠隔 DR を利用します。ローカルの自動 DR では、ドメインで実行中のアプリケーションが実行すべき DR 操作を認識したり、必要に応じて資源の変更を調整することができます。これは、特にアクティブな資源をドメインの使用から外す場合に、DR 操作の成功の可能性を高めます。DR についての詳細は、『System Management Services (SMS) 1.6 Dynamic Reconfiguration ユーザーマニュアル』を参照してください。

ドメインをローカルの自動 DR で構成する場合は、SC から遠隔 DR 操作を起動するとそのドメインの自動 DR 操作を利用することができます。Sun Fire ドメインで使用可能な自動 DR 機能では、crontab (1) ファイルの中に単純なスクリプトを作成および配置し、時間を指定して単純なプラットフォーム再構成を実行することができます。

SMS を使用すると、アクティブな (実行中の) ドメインに対してボードの追加と削除ができます。ドメインで遠隔 DR 操作を起動するには、そのドメインの管理特権が必要です。SMS は、ドメイン単位で個別の管理者に対して、ドメインでの遠隔 DR の起動を許可します。

遠隔 DR のインタフェースは安全です。ドメインでの DR 操作の起動にはスーパーユーザー特権が必要であるために、遠隔 DR サービスは登録済みの認証リモートエージェントに対してのみ提供されます。

DCU 割り当て操作を起動するユーザーのコマンドインタフェースは、対象となるドメインにローカルの自動 DR 機能があるかどうかに関係なく同一です。

SMS は、addboard、deleteboard、moveboard を使用して、静的ドメイン構成などのアクティブなドメインに対するボードの追加または削除を行います。詳細については、『System Management Services (SMS) 1.6 Dynamic Reconfiguration ユーザーマニュアル』を参照してください。

グローバルな自動動的再構成

遠隔 DR およびローカルの自動 DR の機能は、グローバル自動 DR と呼ばれる機能の構成要素です。グローバル自動 DR では、Sun Fire システム上でシステムボード資源の自動再分配に使用できるフレームワークを採用しています。この再分配は、生産計画、ドメインの資源利用率、ドメイン機能の優先度などの要因をベースにすることができます。グローバル自動 DR は、Sun Fire ハイエンドシステムのリソース利用のポリシーを記述する入力をカスタマから受け付け、そのポリシーに基づいて自動的に Sun Fire 資源を整理して、最も効果的に利用します。DR についての詳細は、『System Management Services (SMS) 1.6 Dynamic Reconfiguration ユーザーマニュアル』を参照してください。

プラットフォーム管理者のための構成

この節では、プラットフォーム管理者が使用可能な構成サービスについて簡単に説明します。

使用可能構成要素リスト

各ドメイン (A ~ R) には、管理者または構成者が目的のドメインに割り当てる場合に使用可能なボードの 0- ボードリストがあります。プラットフォーム管理者は `setupplatform (1M)` コマンドを使用して、ボードをドメインの使用可能構成要素リストに追加することができます。使用可能構成要素リストの更新には、以下のタスクを実行するための `pcd` が必要です。

- ドメイン構成の使用可能構成要素リストを更新します
- 使用可能構成要素リストの内容を更新して、現時点で**使用可能な**ドメインを表示します
- 管理者および構成者のそれぞれのドメインの使用可能構成要素リストに追加されたボードを、`dxs` に通知する

`pcd` が、追加されたボードについて `dxs` に知らせます。続いて `dxs` が、稼働しているドメインに**使用可能な**ボードが搭載されたことを知らせます。

▼ 使用可能構成要素リストを設定する

`setupplatform` は、ドメインの使用可能構成要素リストを設定します。`domain-id` または `domain-tag` を指定する場合は、ボードリストを指定してください。パラメータの数値を指定しないと、現在の数値がそのまま使用されます。

1. SC ウィンドウで、プラットフォーム管理者としてログインします。

2. 次のコマンドを入力します。

```
sc0:sms-user:> setupplatform -d domain-indicator -a location
```

ここで次の点に留意します。

-a 指定したドメインの使用可能構成要素リストにスロットを追加します。

-d domain-indicator 以下を使用してドメインを指定します。

domain-id - ドメインの ID。有効な *domain-id* は、A ~ R で、大文字と小文字は区別されません。

domain-tag - `addtag(1M)` を使用してドメインに割り当てた名前。

location ボード (DCU) の位置です。

指定できる *location* の範囲は次のとおりです。

Sun Fire 15K/E25K で有効な形式	Sun Fire 12K/E20K で有効な形式
SB(0...17)	SB(0...8)
IO(0...17)	IO(0...8)

次の例は、SB0、IO1、IO2 のボードをドメイン A で使用可能にする場合です。

```
sc0:sms-user:> setupplatform -d A -a SB0 IO1 IO2
```

ここで、プラットフォーム管理者は、`addboard (1M)` コマンドを使用してドメイン A にボードを割り当てるか、その作業をドメイン管理者に任せることができます。

プラットフォーム管理者は、`addboard` コマンドの `-c assign` オプションの特権だけを持っています。それ以外のすべてのボードの構成にはドメイン特権が必要です。詳細は、`addboard` のマニュアルページを参照してください。

ドメインの構成

▼ コマンド行でドメイン名を命名または変更する

Sun Fire ハイエンドシステムではドメインを作成する必要はありません。18 個のドメインがすでに確立しています。ドメインは A～R までであり、大文字/小文字は区別されません。これらのドメインの指示子はカスタマイズが可能です。ここでは、一意のドメイン名の命名方法について説明します。

注 – 先に進む前に、86 ページの「ドメイン構成の条件」を参照してください。以下の条件を満たすためにシステム構成の変更が必要な場合は、サービスプロバイダに問い合わせてください。

1. SC にログインします。
2. 次のコマンドを入力します。

```
sc0:sms-user:> addtag -d domain-indicator new-tag
```

ここで次の点に留意します。

-d domain-indicator 以下を使用してドメインを指定します。

domain-id - ドメインの ID。有効な *domain-id* は、A ～ R で、大文字と小文字は区別されません。

domain-tag - `addtag(1M)` を使用してドメインに割り当てた名前。

new-tag ドメインに命名する新しい名前です。この名前は、SC で制御されるすべてのドメイン内で重複しない名前であればなりません。

ドメインの命名は省いてもかまいません。

次の例は、ドメイン A に `dmnA` という名前を付ける場合です。

```
sc0:sms-user:> addtag -d A dmnA
```

▼ コマンド行でドメインにボードを追加する

1. SC にログインします。

注 – プラットフォーム管理者による `-c assign` オプションの使用は制限されています。このオプションを使用できるのは、**使用可能**と分類されたボードに対してだけです (**アクティブ**と分類されているボードではない)。

システムボードは、追加するドメインに対して**使用可能**の状態であることが必要です。ボードの状態の判定には、`showboards (1M)` コマンドを使用してください。

2. 次のコマンドを入力します。

```
sc0:sms-user:> addboard -d domain-indicator -c assign location...
```

ここで次の点に留意します。

-d domain-indicator 以下を使用してドメインを指定します。

domain-id - ドメインの ID。有効な *domain-id* は、A ~ R で、大文字と小文字は区別されません。

domain-tag - addtag(1M) を使用してドメインに割り当てた名前。

-c assign 現在の構成状態から assign された (割り当て済み) 状態にボードが移行するよう指定します。

location ボード (DCU) の位置です。複数の位置を指定できます。

指定できる *location* の範囲は次のとおりです。

Sun Fire 15K/E25K で有効な形式	Sun Fire 12K/E20K で有効な形式
SB(0...17)	SB(0...8)
IO(0...17)	IO(0...8)

たとえば、次のメッセージが表示されます。

```
sc0:sms-user:> addboard -d C -c assign SB0 IO1 SB1 IO2
```

ドメイン C に対して**使用可能**であった SB0、IO1、SB1、IO2 は、ドメイン C に割り当てられました。

addboard はタスクを同期的に実行し、コマンドが完了するまでユーザーに制御を返しません。このコマンドの実行が失敗しても、対象のボードは実行前の状態には戻りません。dxs エラーまたは dca エラーがドメインのログに記録され、pcd はプラットフォームログファイルにエラーを報告します。発生したエラーが回復可能であれば、コマンドを再試行できます。**回復不可能**な場合、対象のボードを使用するためにはドメインを再起動する必要があります。

▼ コマンド行でドメインからボードを削除する

注 – プラットフォーム管理者による `-c unassign` オプションの使用は制限されています。このオプションを使用できるのは、割り当て済みと分類されたボードに対してだけです (アクティブと分類されたボードではない)。

1. SC にログインします。

システムボードは、削除する予定のドメインに対して割り当て済みの状態でなければなりません。ボードの状態の判定には、`showboards (1M)` コマンドを使用してください。

2. 次のコマンドを入力します。

```
sc0:sms-user:> deleteboard -c unassign location...
```

ここで次の点に留意します。

`-c unassign` 現在の構成状態から割り当て解除状態へのボードの移行を指定します。

`location` ボード (DCU) の位置です。複数の位置を指定できます。

指定できる `location` の範囲は次のとおりです。

Sun Fire 15K/E25K で有効な形式	Sun Fire 12K/E20K で有効な形式
SB(0...17)	SB(0...8)
IO(0...17)	IO(0...8)

たとえば、次のメッセージが表示されます。

```
sc0:sms-user:> deleteboard -c unassign SB0
```

ドメインに対して割り当て済みであった `SB0` は、そのドメインに対して使用可能になりました。

`deleteboard` に失敗しても、ボードは実行前の状態には戻りません。 `dxs` エラーまたは `dca` エラーがドメインのログに記録され、`pcd` はプラットフォームログファイルにエラーを報告します。発生したエラーが回復可能であれば、コマンドを再試行できます。回復不可能な場合、対象のボードを使用するためにはドメインを再起動する必要があります。

▼ コマンド行でドメイン間でボードを移動する

注 – プラットフォーム管理者による `-c assign` オプションの使用は制限されています。このオプションを使用できるのは、**割り当て済み**と分類されたボードに対してだけです。**アクティブ**な状態のボードには使用できません。

1. SC にログインします。

システムボードは、削除する予定のドメインに対して**割り当て済み**の状態でなければなりません。ボードの状態の判定には、`showboards (1M)` コマンドを使用してください。

2. 次のコマンドを入力します。

```
sc0:sms-user:> moveboard -d domain-indicator -c assign location
```

ここで次の点に留意します。

- d domain-indicator** 以下を使用してドメインを指定します。
- domain-id* - ドメインの ID。有効な *domain-id* は、A ~ R
で、大文字と小文字は区別されません。
- domain-tag* - addtag(1M) を使用してドメインに割り当て
た名前。
- c assign** 現在の構成状態から assign された (割り当て済み) 状態
にボードが移行するよう指定します。
- location* ボード (DCU) の位置です。

指定できる *location* の範囲は次のとおりです。

Sun Fire 15K/E25K で有効な形式	Sun Fire 12K/E20K で有効な形式
SB(0...17)	SB(0...8)
IO(0...17)	IO(0...8)

moveboard は、タスクを同期的に実行し、コマンドが完了するまで制御をユーザーに戻しません。moveboard を使用するときは、1 つの *location* だけを指定することができます。

たとえば、次のメッセージが表示されます。

```
sc0:sms-user:> moveboard -d C -c assign SB0
```

SB0 は、以前のドメインから移動してドメイン C に割り当てられました。

moveboard に失敗しても、ボードは実行前の状態には戻りません。dxs エラーまたは dca エラーがドメインのログに記録され、pcd はプラットフォームログファイルにエラーを報告します。発生したエラーが回復可能であれば、コマンドを再試行できます。回復不可能な場合、対象のボードを使用するためには、エラー発生時にそのボードが含まれていたドメインを再起動する必要があります。

▼ ドメインのデフォルトを設定する

SMS の setdefaults(1M) コマンドは、すでにアクティブになっているドメインからすべてのインスタンスを削除します。

1. SC にログインします。

プラットフォーム管理者はすべてのドメインのデフォルトを設定できますが、一度に設定できるのは1つのドメインだけです。ドメインをアクティブでない状態にして、`setkeyswitch` を `off` に設定する必要があります。

`setdefaults` コマンドは、ネットワーク情報とログファイル以外のすべての `pcd` エントリを削除します。これには、`NVRAM` と起動パラメータデータの削除も含まれます。

デフォルトでは、`NVRAM` と起動パラメータデータを削除するかどうかプロンプトが表示されます。このとき「`no`」と答えると、データは保持されます。`-p` オプションを使用すると、プロンプトは表示されず、データは自動的に保持されます。

2. 次のコマンドを入力します。

```
sc0:sms-user:> setdefaults -d domain-indicator [-p]
```

ここで次の点に留意します。

`-d domain-indicator` 以下を使用してドメインを指定します。

domain-id - ドメインの ID。有効な *domain-id* は、A ~ R で、大文字と小文字は区別されません。

domain-tag - `addtag(1M)` を使用してドメインに割り当てた名前。

`-p` プロンプトを表示せずに、`NVRAM` と起動パラメータデータを保持します。

`setdefaults` についての詳細は、`setdefaults` のマニュアルページまたは『System Management Services (SMS) 1.6 リファレンスマニュアル』を参照してください。

▼ ボードステータスを取得する

1. SC にログインします。

プラットフォーム管理者は、すべてのドメインのボードステータスを取得することができます。

2. 次のように入力します。

```
sc0:sms-user:> showboards [-d domain-id] [-d domain-tag]
```

ボードステータスが表示されます。

次の例は、Sun Fire 15K システムでプラットフォーム管理者特権を持つユーザーに対するボード情報の一部です。すべてのドメインのドメインステータスが表示されます。Sun Fire 12K システムでは、9 つのドメインが表示されます。

```
sc0:sms-user:> showboards
```

Location	Pwr	Type	Board Status	Test Status	Domain
----	---	----	-----	-----	-----
SB0	On	CPU	Active	Passed	domainC
SB1	On	CPU	Active	Passed	A
SB2	On	CPU	Active	Passed	A
SB3	On	CPU	Active	Passed	engB
SB4	On	CPU	Active	Passed	engB
SB5	On	CPU	Active	Passed	engB
SB6	On	CPU	Active	Passed	A
SB7	On	CPU	Active	Passed	domainC
SB8	Off	CPU	Available	Unknown	Isolated
SB9	On	CPU	Active	Passed	dmnJ
SB10	Off	CPU	Available	Unknown	Isolated
SB11	Off	CPU	Available	Unknown	Isolated
SB12	Off	CPU	Assigned	Unknown	engB
SB13	-	Empty Slot	Available	-	Isolated
SB14	Off	CPU	Assigned	Failed	domainC
SB15	On	CPU	Active	Passed	P
SB16	On	CPU	Active	Passed	domainC
SB17	-	Empty Slot	Assigned	-	dmnR
IO0	-	Empty Slot	Available	-	Isolated
IO1	On	HPCI	Active	Passed	A
IO2	On	MCPU	Active	Passed	engB
IO3	On	MCPU	Active	Passed	domainC
IO4	On	HPCI+	Available	Degraded	domainC
IO5	Off	HPCI+	Assigned	Unknown	engB
IO6	On	HPCI	Active	Passed	A
IO7	On	HPCI	Active	Passed	dmnJ
IO8	On	WPCI	Active	Passed	Q
IO9	On	HPCI+	Assigned	iPOST	dmnJ
IO10	Off	HPCI	Assigned	Unknown	engB
IO11	Off	HPCI	Assigned	Failed	engB
IO12	Off	HPCI	Assigned	Unknown	engB
IO13	-	Empty Slot	Available	-	Isolated
IO14	Off	HPCI+	Available	Unknown	Isolated
IO15	On	HPCI	Active	Passed	P
IO16	On	HPCI	Active	Passed	Q
IO17	-	Empty Slot	Assigned	-	dmnR

▼ ドメインステータスを取得する

1. SC にログインします。

プラットフォーム管理者は、すべてのドメインのドメインステータスを取得することができます。

2. 次のコマンドを入力します。

```
sc0:sms-user:> showplatform -d domain-indicator
```

ここで次の点に留意します。

`-d domain-indicator` 以下を使用してドメインを指定します。

`domain-id` - ドメインの ID。有効な `domain-id` は、A ~ R で、大文字と小文字は区別されません。

`domain-tag` - `addtag(1M)` を使用してドメインに割り当てた名前。

ステータスリストが表示されます。

次の例は、Sun Fire 15K システムでプラットフォーム管理者特権を持つユーザーに対するドメイン情報の一部です。すべてのドメインのドメインステータスが表示されます。Sun Fire 12K システムでは、9つのドメインが表示されます。

```
sc0:sms-user:> showplatform
...
Domain configurations:
=====
Domain ID Domain Tag      Solaris Nodename  Domain Status
A          newA          sun15-b0          Powered Off
B          engB          sun15-b1          Keyswitch Standby
C          domainC       sun15-b2          Running OBP
D          eng1          sun15-b3          Loading Solaris
E          -             sun15-b4          Running Solaris
F          domainF       sun15-b5          Running Solaris
G          dmnG          sun15-b6          Running Solaris
H          -             sun15-b7          Solaris Quiesced
I          -             sun15-b8          Powered Off
J          dmnJ          sun15-b9          Powered Off
K          -             sun15-b10         Booting Solaris
L          -             sun15-b11         Powered Off
M          -             sun15-b12         Powered Off
N          -             sun15-b13         Keyswitch Standby
O          -             sun15-b14         Powered Off
P          -             sun15-b15         Running Solaris
Q          -             sun15-b16         Running Solaris
R          dmnR          sun15-b17         Running Solaris
```

仮想時刻

Solaris 環境では、ハードウェアの時刻 (TOD) チップが提供する機能に基づいて Solaris システムの日時がサポートされます。通常は、Solaris ソフトウェアは起動時に TOD 取得サービスを使用してシステムの現在の日時を読み取ります。それ以降は、Solaris ソフトウェアは高分解能のハードウェアタイマーを使用して現在の日時を提示するか、時間情報プロトコル (NTP) が構成されている場合には、これを使用してシステムの現在の日時を、より正確であると考えられるタイム資源に同期させます。

SC は、リアルタイムクロックを備えたプラットフォーム上の唯一のコンピュータです。ドメインの仮想 TOD は、そのリアルタイムクロック値のオフセット値として格納されます。各ドメインは、`setdate (1M)` の代わりに NTP サービスを使用して動作中のシステムの日時を管理するように構成できます。NTP についての詳細は、103 ページの「NTP の構成」を参照するか、Solaris 9 Reference Manual Collection の「man pages section 1M: System Administration Commands」にある `xntpd (1M)` のマニュアルページを参照してください。

注 – NTP は、目的に応じた動作をさせる場合にドメインへのインストールおよび構成が必要な独立したパッケージです。NTP をインストールする前に、ドメインで `setdate` を実行してください。

ただし、システムの日時は Solaris ソフトウェアの動作中に管理されるため、現在の TOD 値と現在のシステム日時との間に誤差が検出される場合は、TOD を設定することによって起動時の TOD 値の精度が保たれます。

Sun Fire ハイエンドシステムのハードウェアは Sun Fire ドメインに対して物理的な TOD チップを供給しないため、SMS は Solaris 環境に必要な時刻サービスを各ドメインに提供します。各ドメインには TOD サービスが提供されています。この TOD サービスは、他のドメインに提供されている同サービスから論理的に分離されています。このような相違によって、Sun Fire ハイエンドシステムドメイン上のシステムの日時は、スタンドアロンサーバーの場合と同様に柔軟に管理できます。あるドメインを実際の時刻とは異なる時刻に構成して稼働させるというまれな状況でも、Sun Fire ハイエンドシステムの TOD サービスにより、実際の時間で稼働しているほかのドメインに提供されている TOD 値に悪影響を与えずに済みます。

時刻設定は、`setdate (1M)` を使用して行います。`setdate` を実行するには、プラットフォーム管理者の特権が必要です。詳細は、44 ページの「すべての特権のリスト」を参照してください。

日時の設定

setdate (1M) では、SC プラットフォーム管理者はシステムコントローラの日時の値を設定することができます。日時の設定が済むと、setdate (1M) はユーザーに対して現在の日時を表示します。

▼ SC で日付を設定する

1. SC にログインします。
2. 次のコマンドを入力します。

```
sc0:sms-user:> setdate 021210302000.00
System Controller: Tue Feb 12 10:30 2002 US/Pacific
```

オプションで、setdate (1M) でドメイン TOD を設定することができます。ドメインのキースイッチの位置を、off または standby にしてください。このコマンドをドメインで実行するには、プラットフォームの管理者特権が必要です。

▼ ドメイン eng2 で日付を設定する

1. SC にログインします。
2. 次のコマンドを入力します。

```
sc0:sms-user:> setdate -d eng2 021210302000.00
Domain eng2: Tue Feb 12 10:30 2002 US/Pacific
```

showdate (1M) は、SC の現在の日時を表示します。

▼ SC で日付を表示する

1. SC にログインします。
2. 次のコマンドを入力します。

```
sc0:sms-user:> showdate
System Controller: Tue Feb 12 10:30 2002 US/Pacific
```

オプションで、showdate (1M) で指定したドメインの日時を表示することができます。スーパーユーザーまたはプラットフォームかドメイングループの任意のメンバーは、showdate を実行することができます。

▼ ドメイン eng2 で日付を表示する

1. SC にログインします。
2. 次のコマンドを入力します。

```
sc0:sms-user:> showdate -d eng2
Domain eng2: Tue Feb 12 10:30 2002 US/Pacific
```

NTP の構成

Solaris OS 用のNTP デーモン `xntpd(1M)` は、SC とドメインの間で時刻設定の同期を維持するメカニズムを提供します。OpenBoot PROM は、ドメインの起動時に SC から時刻を取得します。NTP は、その時点以降はドメイン上でその時刻の同期を維持します。

NTP の構成は、システム管理者から提供される情報を基にしています。

NTP パッケージは、ローカルのリファレンスクロックをサポートするようにコンパイルされています。これは、別のシステムまたはネットワークのクロックをポーリングするのではなく、システムは時刻について自分自身をポーリングすることを意味します。ポーリングは、ネットワークのループバックインタフェースを通して実行されます。IP アドレス番号は `127.127.1.0` です。ここでは、`setdate` による SC の時刻設定方法、および SC の内部の時刻クロックをリファレンスクロックとして使用するように `ntp.conf` ファイルで設定する方法について説明します。

NTP は、SC クロックとドメインクロック間の差を追跡することもできます。NTP は、`ntp.conf` ファイルでドリフトファイル宣言がされている場合は、SC クロックとの接続を失ったドメインクロックを修正します。ドリフトファイル宣言は、NTP デーモンに対してデーモンが計算するクロック周波数の誤差を格納するファイル名を指定します。`ntp.conf` ファイルでのドリフトファイル宣言の例については、以下の手順を参照してください。

`ntp.conf` ファイルが存在しない場合は、次の手順に従ってファイルを作成します。`ntp.conf` ファイルは、SC とドメインの両方に必要です。

▼ `ntp.conf` ファイルを作成する

1. メイン SC にスーパーユーザーとしてログインします。
2. `/etc/inet` ディレクトリに移動して、NTPの `server` ファイルを NTP 構成ファイルにコピーします。

```
sc0:# cd /etc/inet
sc0:# cp ntp.server ntp.conf
```

3. テキストエディタを使用して、前の手順で作成した `/etc/inet/ntp.conf` ファイルを編集します。

Solaris 9 OS の `ntp.conf` ファイルは、`/etc/inet` にあります。

次は、メインの SC の `ntp.conf` ファイルのサーバー行の例で、クロックの同期をとります。

```
server 127.127.1.0
fudge 127.127.1.0 stratum 13
driftfile /var/ntp/ntp.drift
statsdir /var/ntp/ntpstats/
filegen peerstats file peerstats type day enable
filegen loopstats file loopstats type day enable
filegen clockstats file clockstats type day enable
```

4. ファイルを編集して閉じます。
5. NTP デーモンを停止してから起動します。

```
sc0:# /etc/init.d/xntpd stop
sc0:# /etc/init.d/xntpd start
```

6. スペア SC にスーパーユーザーとしてログインします。
7. `/etc/inet` ディレクトリに移動して、NTPの `server` ファイルを NTP 構成ファイルにコピーします。

```
sc1:# cd /etc/inet
sc1:# cp ntp.server ntp.conf
```

8. テキストエディタを使用して、前の手順で作成した `/etc/inet/ntp.conf` ファイルを編集します。

Solaris 9 OS の `ntp.conf` ファイルは、`/etc/inet` にあります。

次は、スペアの SC の `ntp.conf` ファイルのサーバー行の例で、クロックの同期をとります。

```
server 127.127.1.0
fudge 127.127.1.0 stratum 13
driftfile /var/ntp/ntp.drift
statsdir /var/ntp/ntpstats/
filegen peerstats file peerstats type day enable
filegen loopstats file loopstats type day enable
filegen clockstats file clockstats type day enable
```

9. NTP デーモンを停止してから起動します。

```
sc1:# /etc/init.d/xntpd stop
sc1:# /etc/init.d/xntpd start
```

10. 各ドメインにスーパーユーザーでログインします。
11. /etc/inet ディレクトリに移動して、NTP の *client* ファイルを NTP 構成ファイルにコピーします。

```
domain-id:# cd /etc/inet
domain-id:# cp ntp.client ntp.conf
```

12. テキストエディタを使用して、前の手順で作成した /etc/inet/ntp.conf ファイルを編集します。

Solaris 9 OS の ntp.conf ファイルは、/etc/inet にあります。

Solaris 9 OS では、以下に示すような行をドメインの /etc/inet/ntp.conf ファイルに追加することができます。

```
server main-sc-hostname prefer
server spare-sc-hostname
```

13. ファイルを編集して閉じます。
14. 初期設定ディレクトリに移動して、ドメイン上で NTP デーモンを再起動します。

```
domain-id:# /etc/init.d/xntpd stop
domain-id:# /etc/init.d/xntpd start
```

NTP は、現在はドメインにインストールされて実行中です。ドメインごとに手順 10 ~ 14 を繰り返します。

NTP デーモンについての詳細は、Solaris 9 Reference Manual Collection の「man pages section 1M: System Administration Commands」にある xntpd (1M) のマニュアルページを参照してください。

仮想 ID PROM

構成可能な各ドメインには、ホスト ID やドメインの Ethernet アドレスなどのドメインに関する情報を特定するための仮想 ID PROM があります。ホスト ID は、同じプラットフォーム上のすべてのドメインで一意です。Ethernet アドレスは世界中で 1 つしかありません。

Sun Fire ハイエンドシステムのシステム管理ソフトウェアは、ドメインから読み取りが可能で書き込みはできない識別情報を収めた仮想 ID PROM を、構成の可能な各ドメインに提供します。提供される情報は、Solaris 環境の条件を満たします。

flashupdate コマンド

SMS で提供される flashupdate(1M) コマンドでは、システムコントローラ (SC) のフラッシュ PROM を更新することも、SMS ソフトウェアのアップグレード後や適用可能なパッチのインストール後にドメインの CPU と MaxCPU ボード上のフラッシュ PROM を更新することもできます。flashupdate は、どのような更新の前にも、現在のフラッシュ PROM とフラッシュイメージファイルの情報の両方を表示します。

注 – SC FPROM を更新した場合には、SC をリセットする必要があります。OpenBoot PROM (ok) プロンプトで `reset-all` コマンドを実行してください。flashupdate の実行中には、対象のシステムボードに対して、CLI コマンドはいっさい実行すべきではありません。対象のシステムボードに影響を与えるような SMS コマンドを実行する前に、flashupdate の実行が完了するまで待ってください。

注 – flashupdate コマンドの実行後、動的再構成操作によってシステムの電源投入時自己診断 (POST) の制御アプリケーション hpost がボードごとに実行されるまで、新しいファームウェアはシステムボード上でアクティブになりません。単一のボードに対して hpost を実行する場合は、`deleteboard(1M)` コマンドまたは `addboard(1M)` コマンドを使用してください。ドメイン内のすべてのボードに対しては、`setkeyswitch(1M)` コマンドを使用してください。

flashupdate コマンドの詳細および例については、flashupdate のマニュアルページを参照してください。

ドメイン管理者のための構成

この節では、ドメイン管理者が使用可能な構成サービスについて簡単に説明します。

ドメインの構成

addboard、deleteboard、およびmoveboardの各コマンドは、プラットフォーム管理者よりもドメイン管理者に多くの機能を提供します。

▼ コマンド行でドメインにボードを追加する

1. 該当ドメインで、ドメイン管理者として SC にログインします。

注 – ドメイン管理者がドメインにボードを追加するには、そのボードをドメインの**使用可能構成要素リスト**に登録してください。

システムボードは、追加するドメインに対して**使用可能**または**割り当て済み**の状態であることが必要です。ボードの状態の判定には、showboards (1M) コマンドを使用してください。

2. 次のコマンドを入力します。

```
sc0:sms-user:> addboard -d domain-indicator -c function location
```

ここで次の点に留意します。

- d domain-indicator** 以下を使用してドメインを指定します。
- domain-id* - ドメインの ID。有効な *domain-id* は、A ~ R
で、大文字と小文字は区別されません。
- domain-tag* - addtag(1M) を使用してドメインに割り当て
た名前。
- c function** 現在の構成状態から新しい構成状態のボードに移行するよ
う指定します。
- location* ボード (DCU) の位置です。

構成状態は次のようになります。

- assign** ボードを論理ドメインに割り当てます。ボードはドメイン
に含まれていますが、アクティブではありません。
- connect** 割り当てられたボードを、接続済み / 構成解除済み状態に
移行します。これは中間状態であり、スタンドアロン実装
状態ではありません。
- configure** 割り当てられたボードを、接続済み / 構成済み状態に移行
します。ボード上のハードウェア資源は、Solaris ソフト
ウェアで使用することができます

-c function オプションを指定しない場合は、デフォルトで **configure** の状態が設
定されます。構成状態についての詳細は、**addboard(1M)** のマニュアルページを参
照してください。

複数の位置を指定できます。

指定できる *location* の範囲は次のとおりです。

Sun Fire 15K/E25K で有効な形式	Sun Fire 12K/E20K で有効な形式
SB(0...17)	SB(0...8)
IO(0...17)	IO(0...8)

たとえば、次のように入力します。

```
sc0:sms-user:> addboard -d C -c assign SB0 IO1 SB1 IO2
```

この例の SB0、IO1、SB1、IO2 は、ドメイン C に対して使用可能な状態から割り当て済みの状態に変更されました。

addboard はタスクを同期的に実行し、コマンドが完了するまでユーザーに制御を返しません。ボードの電源が投入されていない場合またはボードをテストする場合は、`-c connect|configure` オプションを指定するとコマンドがボードの電源を投入してテストを実行します。

addboard に失敗しても、ボードは実行前の状態には戻りません。dxs エラーまたは dca エラーがドメインのログに記録され、pcd はプラットフォームログファイルにエラーを報告します。発生したエラーが回復可能であれば、コマンドを再試行できます。回復不可能な場合、対象のボードを使用するためにはドメインを再起動する必要があります。

▼ コマンド行でドメインからボードを削除する

1. 該当ドメインで、ドメイン管理者として SC にログインします。

システムボードは、削除する予定のドメインに対して割り当て済みかアクティブの状態であればなりません。ボードの状態の判定には、`showboards (1M)` コマンドを使用してください。

2. 次のコマンドを入力します。

```
sc0:sms-user:> deleteboard -c function location
```

ここで次の点に留意します。

- | | |
|--------------------|-----------------------------------|
| <i>-c function</i> | 現在の構成状態から新しい構成状態のボードに移行するよう指定します。 |
| <i>location</i> | ボード (DCU) の位置です。 |

以下の構成状態があります。

- | | |
|--------------------|--|
| <i>unconfigure</i> | 割り当てられたボードを、接続済みまたは構成解除済みの状態に移行します。ボード上のハードウェア資源を Solaris で使用することはできません。 |
| <i>disconnect</i> | 割り当てられたボードを、接続解除済みまたは構成解除済みの状態に移行します。 |
| <i>unassign</i> | 現在の論理ドメインからボードの割り当てを解除します。ボードはドメインに含まれておらず、使用可能に変わります。 |

-c function オプションを指定しない場合は、デフォルトで *unassign* が設定されます。構成状態についての詳細は、*deleteboard(1M)* のマニュアルページを参照してください。

複数の位置を指定できます。

指定できる *location* の範囲は次のとおりです。

Sun Fire 15K/E25K で有効な形式	Sun Fire 12K/E20K で有効な形式
SB(0...17)	SB(0...8)
IO(0...17)	IO(0...8)

たとえば、次のように入力します。

```
sc0:sms-user:> deleteboard -c unassign SB0
```

この例の *SB0* は、ドメインに対して割り当て済みの状態から使用可能な状態に変更されました。

注 – ドメイン管理者は、ボードの構成解除および接続解除を実行できますが、ドメインの使用可能構成要素リストに `deleteboard [location]` フィールドが指定されていない場合、ドメインからボードを削除することはできません。

`deleteboard` に失敗しても、ボードは実行前の状態には戻りません。dxs エラーまたは dca エラーがドメインのログに記録され、pcd はプラットフォームログファイルにエラーを報告します。発生したエラーが回復可能であれば、コマンドを再試行できます。回復不可能な場合、対象のボードを使用するためにはドメインを再起動する必要があります。

▼ コマンド行でドメイン間でボードを移動する

注 – 対象となる両方のドメインのドメイン管理者特権が必要です。

1. 該当ドメインで、ドメイン管理者として SC にログインします。

システムボードは、削除する予定のドメインに対して割り当て済みかアクティブの状態であればなりません。ボードの状態の判定には、`showboards (1M)` コマンドを使用してください。

2. 次のコマンドを入力します。

```
sc0:sms-user:> moveboard -d domain-indicator -c function location
```

ここで次の点に留意します。

- d domain-indicator** これは、ボードの移動先となるドメインです。以下を使用してドメインを指定します。
- domain-id* - ドメインの ID。有効な *domain-id* は、A ~ R で、大文字と小文字は区別されません。
- domain-tag* - addtag(1M) を使用してドメインに割り当てた名前。
- c function** 現在の構成状態から新しい構成状態にボードが移行するように指定します。
- location* ボード (DCU) の位置です。

以下の構成状態があります。

- assign** 現在の論理ドメインからボードを構成解除します。ボードの状態を *available* (使用可能) に変更して、論理ドメインからボードを移動します。ボードを新しい論理ドメインに割り当てます。ボードは新しいドメインに含まれていますが、アクティブではありません。
- connect** 割り当てられたボードを、接続済みまたは構成解除済みの状態に移行します。これは中間状態であり、スタンドアロン実装状態ではありません。
- configure** 割り当てられたボードを、接続済みまたは構成済みの状態に移行します。ボード上のハードウェア資源は、Solaris ソフトウェアで使用することができます

-c オプションが指定されない場合は、デフォルトの設定状態は *configure* になります。構成状態についての詳細は、*moveboard(1M)* のマニュアルページを参照してください。

指定できる *location* の範囲は次のとおりです。

Sun Fire 15K/E25K で有効な形式	Sun Fire 12K/E20K で有効な形式
SB(0...17)	SB(0...8)
IO(0...17)	IO(0...8)

moveboard は、タスクを同期的に実行し、コマンドが完了するまで制御をユーザーに戻しません。ボードの電源が投入されていない場合またはボードをテストする場合は、`-c connect|configure` を指定すると、コマンドはボードの電源を投入してテストを実行します。moveboard を使用するときは、1 つの *location* だけを指定することができます。

moveboard に失敗しても、ボードは実行前の状態には戻りません。dxs エラーまたは dca エラーがドメインのログに記録され、pcd はプラットフォームログファイルにエラーを報告します。発生したエラーが回復可能であれば、コマンドを再試行できます。回復不可能な場合、対象のボードを使用するためには、エラー発生時にそのボードが含まれていたドメインを再起動する必要があります。

▼ ドメインのデフォルトを設定する

SMS の `setdefaults(1M)` コマンドは、すでにアクティブになっているドメインからすべてのインスタンスを削除します。

1. SC にログインします。

プラットフォーム管理者はすべてのドメインのデフォルトを設定できますが、一度に設定できるのは 1 つのドメインだけです。ドメインはアクティブではなく、`setkeyswitch` が `off` に設定されている必要があります。`setdefaults` コマンドは、ネットワーク情報、ログファイル、および (任意の) NVRAM と起動パラメータデータを除き、すべての pcd エントリを削除します。

2. 次のコマンドを入力します。

```
sc0:sms-user:> setdefaults -d domain-indicator
```

ここで次の点に留意します。

`-d domain-indicator` 以下を使用してドメインを指定します。

domain-id - ドメインの ID。有効な *domain-id* は、A ~ R で、大文字と小文字は区別されません。

domain-tag - `addtag(1M)` を使用してドメインに割り当てた名前。

`setdefaults` についての詳細は、`setdefaults` のマニュアルページまたは『System Management Services (SMS) 1.6 リファレンスマニュアル』を参照してください。

▼ ボードステータスを取得する

1. SC にログインします。

ドメイン管理者は、特権を持つドメインについてのみデバイスステータスを取得することができます。

2. 次のコマンドを入力します。

```
sc0:sms-user:> showboards [-d domain-id|domain-tag]
```

ボードステータスが表示されます。

次の例は、ドメイン A のドメイン管理者特権を持つユーザーに対するボード情報の一部です。

```
sc0:sms-user:> showboards -d A
```

Location	Pwr	Type	Board Status	Test Status	Domain
SB1	On	CPU	Active	Passed	A
SB2	On	CPU	Active	Passed	A
IO1	On	HPCI	Active	Passed	A

▼ ドメインステータスを取得する

1. SC にログインします。

ドメイン管理者は、特権を持つドメインについてのみドメインステータスを取得することができます。

2. 次のコマンドを入力します。

```
sc0:sms-user:> showplatform -d domain-indicator
```

ここで次の点に留意します。

-d *domain-indicator* 以下を使用してドメインを指定します。

domain-id - ドメインの ID。有効な *domain-id* は、A ~ R
で、大文字と小文字は区別されません。

domain-tag - addtag(1M) を使用してドメインに割り当て
た名前。

ステータスリストが表示されます。

次の例は、ドメインの newA、engB、domainC のドメイン管理者特権を持つユーザーに対するドメイン情報の一部です。

```
sc0:sms-user:> showplatform
...
Domain configurations:
=====
Domain ID Domain Tag      Solaris Nodename   Domain Status
A          newA          sun15-b0           Powered Off
B          engB          sun15-b1           Keyswitch Standby
C          domainC       sun15-b2           Running OBP
```

▼ デバイスステータスを取得する

1. SC にログインします。

ドメイン管理者は、特権を持つドメインについてのみデバイスステータスを取得することができます。

2. 次のコマンドを入力します。

```
sc0:sms-user:> showdevices [-d domain-id|domain-tag]
```

デバイスステータスが表示されます。

次の例は、ドメイン A のドメイン管理者特権を持つユーザーに対するデバイス情報の一部です。

```
sc0:sms-user:> showdevices IO1
```

IO Devices

domain	location	device	resource	usage
A	IO1	sd3	/dev/dsk/c0t3d0s0	mounted filesystem "/"
A	IO1	sd3	/dev/dsk/c0t3s0s1	dump device (swap)
A	IO1	sd3	/dev/dsk/c0t3s0s1	swap area
A	IO1	sd3	/dev/dsk/c0t3d0s3	mounted filesystem "/var"
A	IO1	sd3	/var/run	mounted filesystem "/var/run"

仮想キースイッチ

各 Sun Fire ハイエンドシステムドメインには仮想キースイッチがあります。Sun Enterprise サーバーの物理的なキースイッチと同様に、Sun Fire ハイエンドシステムドメインの仮想キースイッチはドメインの電源を投入するかどうか、起動時に強化診断を実行するかどうか、特定の処理 (フラッシュ PROM の更新、ドメインの reset コマンドなど) を許可するかどうかを制御します。

仮想キースイッチで構成されたドメインだけが、起動時に電源が投入され、監視されて、問題が起こったときに自動的に回復処置が実行されます。

仮想キースイッチの設定は、setkeyswitch (1M) を使用して行います。setkeyswitch を実行するには、指定されたドメインのドメイン管理者特権が必要です。詳細は、44 ページの「すべての特権のリスト」を参照してください。

setkeyswitch コマンド

setkeyswitch (1M) は、仮想キースイッチの位置を指定された値に変更します。pcd (1M) は、SC の電源再投入の間または電源装置の電源再投入の間で、各仮想キースイッチの状態を維持します。

setkeyswitch(1M) は、構成済みの各プロセッサの起動バス SRAM をロードする役割を持ちます。すべてのプロセッサが起動され、そのうちの 1 つが起動プロセッサに指定されます。setkeyswitch(1M) は、Sun Fire ハイエンドシステムドメインのメモリーに OpenBoot PROM をロードし、起動プロセッサで OpenBoot PROM を起動します。

OpenBoot PROM の主な役割は、OS を外部記憶装置から、またはネットワーク経由で起動して構成することです。また、ハードウェアとソフトウェアを対話的にテストするための多彩な機能も備えています。

setkeyswitch(1M) のコマンド構文は次のとおりです。

```
sc0:sms-user:> setkeyswitch -d domain-indicator [-q -y|-n]
on|standby|off|diag|secure -l level
```

ここで次の点に留意します。

- | | |
|----------------------------|--|
| -d <i>domain-indicator</i> | 以下を使用してドメインを指定します。

<i>domain-id</i> - ドメインの ID。有効な <i>domain-id</i> は、A ~ R で、大文字と小文字は区別されません。

<i>domain-tag</i> - addtag(1M) を使用してドメインに割り当てた名前。 |
| -q | 非出力。プロンプトを含むすべての stdout へのメッセージを抑制します。単独で使用すると -q は、デフォルトですべてのプロンプトに対して -n オプションを指定します。-y または -n オプションと併用する場合は、-q はすべてのユーザープロンプトを無効にして、選択されたオプションに基づいて自動的に Y または N を回答します。 |
| -n | すべてのプロンプトに自動的に no と応答します。プロンプトは、-q オプションを指定しないかぎり表示されます。 |
| -y | すべてのプロンプトに対して自動的に yes と応答します。プロンプトは、-q オプションを指定しないかぎり表示されます。 |
| -l <i>level</i> | システムの起動時に使用される hpost レベルを指定します。 |

次のオペランドがサポートされています。

- on

- off または standby の位置からは、on はドメインに割り当てられたすべてのボードの電源を投入します (電源が未投入の場合)。これで、ドメインが起動します。
 - diag 位置からは、on は位置変更であり、動作しているドメインには影響を与えません。
 - secure の位置からは、on は書き込み権をドメインに戻します。
 - standby
 - on、diag、または secure の位置からは、standby はオプションで確認プロンプトを表示します。「yes」と応答すると、ドメインがリセットおよび構成解除に適した状態にあるかどうか (OS が動作していない状態など) が判定されます。
 - ドメインがリセットと構成解除が可能な状態にある場合には、setkeyswitch がそのドメインに割り当てられていたすべてのボードをリセットして構成解除します。
 - ドメインが適切な状態にない場合は、リセットと構成解除が発生する前に setkeyswitch によってドメインが正常にシャットダウンされます。
 - off の位置からは、standby はドメインに割り当てられたすべてのボードの電源を投入します (電源が未投入の場合)。
 - off
 - on、diag、または secure の位置からは、off はオプションで確認プロンプトを表示します。「yes」と応答すると、ドメインの電源切断に適した状態にあるかどうか (OS が動作していない状態など) が判定されます。
 - ドメインが電源を切断できる状態にある場合には、setkeyswitch がそのドメインに割り当てられていたすべてのボードの電源を切断します。電源を切断できる状態にない場合には、setkeyswitch は中止し、メッセージをドメインのログに記録します。
 - standby の位置からは、off はドメインのすべてのボードの電源を切断します。
 - diag
 - off または standby の位置からは、diag はドメインに割り当てられたすべてのボードの電源を投入します (電源が未投入の場合)。ドメインは、POST が冗長モードで起動され、diag レベルがデフォルト以上に設定されることを除いて、on 位置の場合と同じ稼働状態になります。
 - on の位置からは、diag は位置の変更のみを行います。ただし、ドメインの自動システム回復 (ASR) 時には電源投入時自己診断 (POST) が冗長モードで起動され、diag レベルがデフォルト以上に設定されます。
 - secure の位置からは、diag はドメインへの書き込み権を復元し、ASR 時には、POST は冗長モードで起動され、diag レベルはデフォルトに設定されます。
- ASR についての詳細は、171 ページの「ASR (Automatic System Recovery: 自動システム回復)」を参照してください。
- secure

- off または standby の位置からは、secure はドメインに割り当てられたすべてのボードの電源を投入します (電源が未投入の場合)。ドメインは、secure がドメインに対する書き込み権を削除する場合を除いて、on の場合と同じ稼働状態になります。たとえば、flashupdate と reset は動作しません。
- on の位置からは、secure はドメインへの書き込み権を削除します。diag の位置からは、secure はドメインへの書き込み権を削除します (diag の例の説明を参照)。

▼ ドメイン A で仮想キースイッチを設定する

1. SC にログインします。

ドメイン管理者は、特権を持つドメインについてのみ仮想キースイッチを設定することができます。

2. 次のコマンドを入力します。

```
sc0:sms-user:> setkeyswitch -d A on
```

showkeyswitch (1M) は、指定したドメインの仮想キースイッチの位置を表示します。各仮想キースイッチの状態は、pcd (1M) により SC のパワーサイクルの間または電源の物理パワーサイクルの間で維持されます。スーパーユーザーまたはプラットフォームかドメイングループの任意のメンバーは、showkeyswitch を実行することができます。

▼ ドメイン A で仮想キースイッチ設定を表示する

1. SC にログインします。

ドメイン管理者は、特権を持つドメインについてのみキースイッチステータスを取得することができます。

2. 次のコマンドを入力します。

```
sc0:sms-user:> showkeyswitch -d A
Virtual keyswitch position: ON
```

仮想 NVRAM

各ドメインには、OpenBoot PROM 変数などの OpenBoot PROM データを収めた仮想 NVRAM があります。OpenBoot PROM は SC に格納された 2 値画像で、/opt/SUNWSMS/hostobjs にあります。これは、setkeyswitch が起動時にドメインにダウンロードしたものです。すべてのドメインに対して 1 つの OpenBoot PROM のバージョンだけがあります。

SMS ソフトウェアは、各ドメインに仮想 NVRAM を提供し、OpenBoot PROM がこのデータの完全な読み取り/書き込みができるようにします。

ほとんどの NVRAM 変数の読み取りまたは書き込みに使用できるインタフェースは、OpenBoot PROM だけです。例外は、OpenBoot PROM を定義済みの作業状態にしたり、OpenBoot PROM の稼働を妨げる問題点を診断するために変更が必要となる、OpenBoot PROM 変数です。これらの変数は、OpenBoot PROM インタフェースの交換値ではありません。

ドメインの NVRAM にある一定限度の OpenBoot PROM 変数値は、setobpparams (1M) を使用して SMS で読み取りおよび書き込みすることができます。set/showobpparams を実行するには、ドメイン管理者特権が必要です。実行中のドメインで変数を変更するときは、変更内容を有効にするためにドメインの再起動が必要です。

注 – ここで説明した以外の方法での setobpparams の使用は、OpenBoot PROM コマンドおよびその依存関係をよく理解している熟練したシステム管理者に限定してください。

OpenBoot PROM 変数の設定

setobpparams (1M) は、以下の構文に基づいてドメインの仮想 NVRAM 変数と REBOOTINFO データのサブセットを設定および取得します。

```
sc0: sms-user:> setobpparams -d domain-indicator param=value...
```

ここで次の点に留意します。

-d domain-indicator 以下を使用してドメインを指定します。

domain-id - ドメインの ID。有効な *domain-id* は、A ~ R で、大文字と小文字は区別されません。

domain-tag - addtag(1M) を使用してドメインに割り当てた名前。

`param=value` は次に示す変数の 1 つであり、対応する値は次のとおりです。

変数	=	デフォルト値	説明
<code>diag-switch?</code>	=	<code>false</code>	<code>false</code> に設定すると、デフォルトの起動ドライブは <code>boot-device</code> で指定され、デフォルトの起動ファイルは <code>boot-file</code> で指定されます。 <code>true</code> に設定すると、 OpenBoot PROM は診断モードで実行され、正しいデフォルトの起動デバイスまたはファイルを指定するには <code>diag-device</code> または <code>diag-file</code> の設定が必要です。これらのデフォルトの起動デバイスとファイルの設定には、 <code>setobpparams</code> は使用できません。 OpenBoot PROM の <code>setenv(1)</code> を使用してください。
<code>auto-boot?</code>	=	<code>false</code>	<code>true</code> に設定すると、ドメインは電源投入または 全リセット のあと、自動的に起動します。使用される起動デバイスと起動ファイルは、 <code>diag-switch</code> の設定で決まります (前述の説明を参照)。 <code>boot-device</code> と <code>boot file</code> は、どちらも <code>setobpparams</code> で設定することはできません。パニックが繰り返し発生している間など、 <code>ok</code> プロンプトを使用できない場合には、 <code>setobpparams</code> を使用して <code>auto-boot?</code> を <code>false</code> に設定してください。 <code>setobpparams</code> を使用して <code>auto-boot?</code> を <code>false</code> に設定すると、再起動変数は無効になります。システムは自動起動せず、 OpenBoot PROM で停止します。この時点で新しい NVRAM 変数を指定できます。122 ページの「周期的なドメインパニックから回復する」を参照してください。

変数	=	デフォルト値	説明
security-mode	=	none	ファームウェアのセキュリティーレベルです。security-mode で有効な変数は以下のとおりです。 <ul style="list-style-type: none"> • none - パスワード不要 (デフォルト)。 • command - boot (1M) および go を除くすべてのコマンドにパスワードが必要です。 • full - go を除くすべてのコマンドにパスワードが必要です。
use-nvramrc?	=	false	true に設定すると、この変数はシステム起動時に NVRAMRC でコマンドを実行します。
fcode-debug?	=	false	true に設定すると、この変数はプラグインデバイスの FCodes の名前フィールドを組み込みます。

次の例は、setobpparams を有効にする場合です。

▼ 周期的なドメインパニックから回復する

繰り返し発生するパニックをドメイン A が検出します。

1. ドメイン管理者特権で SC にログインします。
2. 自動再起動を停止します。

```
sc0:sms-user:> setkeyswitch -d A standby
sc0:sms-user:> setobpparams -d A 'auto-boot?=false'
```

注 – 大部分のシェル (ただし、すべてではない) では、疑問符が特殊文字として扱われないように、変数の値の前後に単一引用符を付ける必要があります。

3. ドメインを再ポストします。

```
sc0:sms-user:> setkeyswitch -d A off
sc0:sms-user:> setkeyswitch -d A on
```

- ドメインに OK プロンプトが表示されたら、破壊されていない新しい起動デバイスに NVRAM 変数を設定します。

```
ok setenv boot-device bootdisk-alias
```

ここで次の点に留意します。

bootdisk-alias 作成済みのユーザー定義のエイリアスです。起動デバイスは、OS をインストール済みの起動ディスクと一致させます。

- 起動デバイス用の新しいエイリアスを設定したので、ここで以下のように入力してディスクを起動します。

```
ok boot
```

OpenBoot 変数についての詳細は、『OpenBoot 4.x Command Reference Manual』を参照してください。

▼ ドメイン A で OpenBoot PROM のセキュリティーモード変数を設定する

- SC にログインします。

ドメイン管理者は、特権を持つドメインについてのみ OpenBoot PROM を設定することができます。

- 次のコマンドを入力します。

```
sc0:sms-user:> setobpparams -d A security-mode=full
```

security-mode は *full* に設定されました。go を除くすべてのコマンドに、ドメイン A のパスワードが必要です。変更を有効にするには、動作中のドメインを再起動してください。

▼ OpenBoot PROM 変数を確認する

- SC にログインします。

ドメイン管理者は、特権を持つドメインについてのみ OpenBoot PROM を設定することができます。

2. 次のコマンドを入力します。

```
sc0:sms-user:> showobpparams -d domain-indicator
```

ここで次の点に留意します。

`-d domain-indicator` 以下を使用してドメインを指定します。

`domain-id` - ドメインの ID。有効な `domain-id` は、A ~ R で、大文字と小文字は区別されません。

`domain-tag` - `addtag(1M)` を使用してドメインに割り当てた名前。

SMS NVRAM の更新は、OpenBoot PROM の起動時 (またはドメインの再起動時) に OpenBoot PROM に対して行われます。詳細は、『OpenBoot 4.x Command Reference Manual』を参照してください。

機能が低下した構成の設定の変更

ほとんどの場合は、ドメインのクラッシュを引き起こすハードウェア障害は、POST またはそれ以降のドメインの自動回復起動時に OpenBoot PROM により検出され、ドメイン構成から除去されます。ただし、障害が一時的なものであったり、周期的なドメインの障害や再起動を引き起こす障害を起動時のテストで検出できない場合があります。この場合は、Sun Fire ハイエンドのシステム管理ソフトはドメイン管理者が提供する構成または構成ポリシーに基づき、ドメイン環境の安定動作を目的としてドメイン構成からハードウェアを除去します。

以下のコマンドは、プラットフォームまたはドメインの管理者が実行することができます。ドメイン管理者の操作は、特権を持つドメインに限定されます。

setbus コマンド

`setbus(1M)` は、ドメイン内のアクティブな拡張ボード上のバストラフィックを動的に再構成してセンタープレーンサポートボード (CSB) を使用します。両方の CSB を使用するの *normal* モードです。1 つの CSB を使用するの *degraded* モードです。

setbus は、電源が投入されていてもアクティブでないボードをリセットします。その結果、接続可能状態のボードはなくなります。取り付け可能状態についての詳細は、『System Management Services (SMS) 1.6 Dynamic Reconfiguration ユーザーマニュアル』を参照してください。

setbus を実行するには、指定されたドメインのプラットフォーム管理者特権またはドメイン管理者特権が必要です。

この機能により、システムの電源を落とさずに CSB をスワップすることができます。有効なバスは以下のとおりです。

- a - アドレスバスを構成します
- d - データバスを構成します
- r - 応答バスを構成します

▼ すべてのアクティブドメインの全バスを両方の CSB で使用する

1. SC にログインします。

ドメイン管理者は、特権を持つドメインについてのみバスを設定することができます。

2. 次のコマンドを入力します。

```
sc0:sms-user:> setbus -c CS0,CS1
```

バストラフィックの再設定についての詳細は、setbus (1M) のマニュアルページを参照してください。

showbus コマンド

showbus(1M) は、アクティブドメイン内の拡張ボードのバス構成を表示します。この情報は、デフォルトでスロットの順番で設定を表示します。showbus は、プラットフォームまたはドメイングループの任意のメンバーで実行することができます。

▼ すべてのアクティブドメインの全バスを表示する

1. SC にログインします。

2. 次のコマンドを入力します。

```
sc0:sms-user:> showbus
```

バストラフィックの再構成についての詳細は、`showbus (1M)` のマニュアルページを参照してください。

第6章

自動診断および自動回復

この章では、自動エラー診断機能およびドメイン回復機能について説明します。この章では、次の項目を説明します。

- 127 ページの「自動診断および自動回復の概要」
- 133 ページの「電子メールイベント通知の有効化」
- 142 ページの「電子メールイベント通知のテスト」
- 144 ページの「診断および回復情報の取得」

自動診断および自動回復の概要

Sun Fire ハイエンドシステムでハードウェアエラーが発生すると、システムコントローラは、特定の診断およびドメイン回復手順を実行します。次に示す自動診断エンジン (DE) が、システムとそのドメインの可用性に影響を与えるハードウェアエラーを特定し、診断します。

- SMS 診断エンジン

SMS DE は、ドメイン停止 (dstop) を伴うハードウェアエラーを診断します。

- Solaris OS 診断エンジン

Solaris OS DE (Solaris DE と呼ばれる) は、致命的ではないドメインのハードウェアエラーを特定し、システムコントローラに報告します。

- POST 診断エンジン

POST DE は、電源投入時自己診断の実行中に発生したハードウェアテスト障害を特定します。

以下では、さまざまな診断エンジンによってハードウェアエラーが特定されたときに実行される、診断および回復手順について説明します。

ドメイン停止に関係するハードウェアエラー

図 6-1 に、SMS 診断エンジンによって dstop に関係するハードウェアエラーが特定されたときに実行される、基本的な診断およびドメイン回復手順を示します。

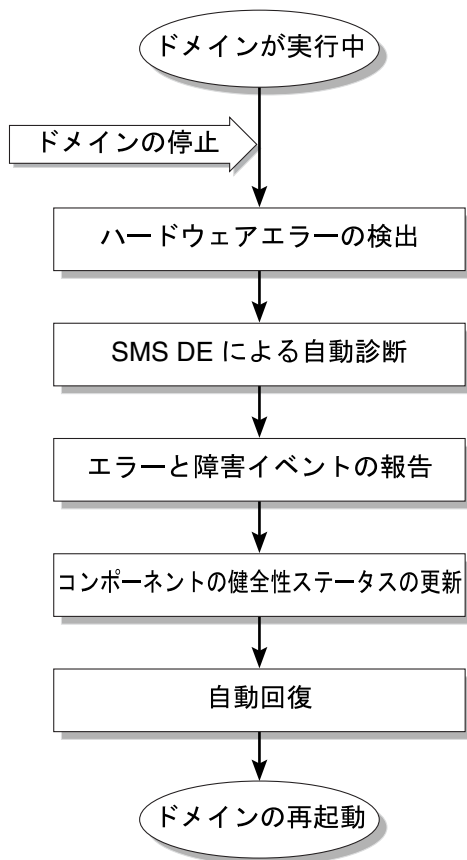


図 6-1 ドメイン停止に関係するハードウェアエラーに対する自動診断および自動回復プロセス

図 6-1 のプロセスについて、以下で簡単に説明します。

- ハードウェアエラーの検出。CPU ボード、プロセッサ、I/O コントローラ、およびメモリーバンクを含むハードウェアエラーに関する情報が、システムコントローラから提供されます。

dstop が発生すると、ダンプファイルが作成されます。このファイル (`/var/opt/SUNWSMS/sms-version/adm/domain-id/dump/dsmd.dstop.yymmdd.hhmm.ss`) には、dstop に関係するドメインハードウェアエラーが記録されます。

- 自動診断。SMS DE により、`dstop` ダンプファイルに記録されたハードウェアエラーから障害が判定されます。DE では、エラーの原因である 1 つまたは複数の FRU を特定することができます。ハードウェアエラーによっては、DE で特定されるのが 1 つの障害が発生した FRU であることも、1 つ以上の疑わしい FRU であることもあります。

DE で複数の FRU が特定された場合、障害が発生した FRU を決定するためには、サービスプロバイダによる詳細な分析が必要となることがあります。

- エラーと障害イベントの報告。DE では、以下の方法により診断情報を報告します。
 - ドメインとプラットフォームのログファイルへの自動診断障害メッセージの表示。

コード例 6-1 に、ドメインが停止したときに表示される情報と、ドメイン D で発生した障害イベントについて説明する自動診断メッセージを示します。イベントメッセージは [AD] インジケータ以降に示されます。イベントメッセージの内容については、144 ページの「診断イベントの確認」を参照してください。

コード例 6-1 プラットフォームログファイルの `Dstop` と自動診断イベントメッセージの例

```
Jul 30 14:23:26 2005 smshostname dsmd[14838]-D(): [2516 589424843782403 ERR
EventHandler.cc 136] Domain stop has been detected in domain D
Jul 30 14:23:27 2005 smshostname dsmd[14838]-D(): [2525 589425136691417 NOTICE
SysControl.cc 2360] Taking hardware configuration dump. Dump
file: -D/var/opt/SUNWSMS/SMS1.6/adm/D/dump/dsmd.dstop.030730.1423.27
Jul 30 14:24:37 2005 smshostname erd[14864]-D(): [11900 589495236849691 CRIT Mes
sageReportingService.cc 381] [AD] Event: SF15000-8000-GK CSN: 352A00005
DomainID: D ADInfo: 1.SMS-DE.1.6 Time: Wed Jul 30 14:23:27 PDT 2005
Recommended-Action: Service action required
```

- 電子メールによる障害イベントの通知。詳細は、133 ページの「電子メールイベント通知の有効化」を参照してください。
- 障害イベントの通知 (Sun Management Center を使用している場合)。詳細は、『Sun Management Center Sun Fire ハイエンドシステムのための追補マニュアル』を参照してください。
- 障害イベントの通知 (Sun Remote Services (SRS) Net Connect を使用中で、それに合わせて Net Connect を構成している場合)。

SRS Net Connect の一般的な情報については、以下の Web サイトを参照してください。

<http://www.sun.com/srs>

SRS Net Connect 製品マニュアルについては、次の Web サイトを参照してください。

<https://srsnetconnect3.sun.com>

および

<http://docs.sun.com>

- **showlogs(1M)** コマンドによるイベントログ出力 (プラットフォーム管理者特権を持っている場合)。

`showlogs` コマンドでのイベント出力は、プラットフォームとドメインのメッセージログやイベント電子メールに記載されている診断情報を補足するものです。`showlogs` コマンドでのイベント出力は、サービスプロバイダでさらに詳しいトラブルシューティングを行う際に使用することができます。表示されるイベント情報についての詳細は、144 ページの「診断および回復情報の取得」を参照してください。

注 – これらのイベントメッセージが表示されたとき、あるいはこれらのイベントが通知されたときは、サービスプロバイダに連絡してください。サービスプロバイダでは、自動診断情報を確認して、適切な保守アクションを開始します。

- コンポーネントの健全性ステータスの更新。SMS DE は、影響を受けた各コンポーネントの診断情報を記録し、この健全性履歴をコンポーネントの健全性ステータス (CHS) の一部として保持します。
- 自動回復。ドメイン回復プロセスの一部として、POST では影響を受けたコンポーネントの更新された健全性ステータスを確認し、CHS 情報を使用して、システムから構成解除するコンポーネントを決定します。そして、該当するコンポーネントが構成解除され、ドメインが再起動されます。

致命的でないドメインハードウェアエラー

図 6-2 に、致命的でないドメインハードウェアエラーの診断で実行する基本的な手順です。これらのエラーによってドメインが停止することはありません。

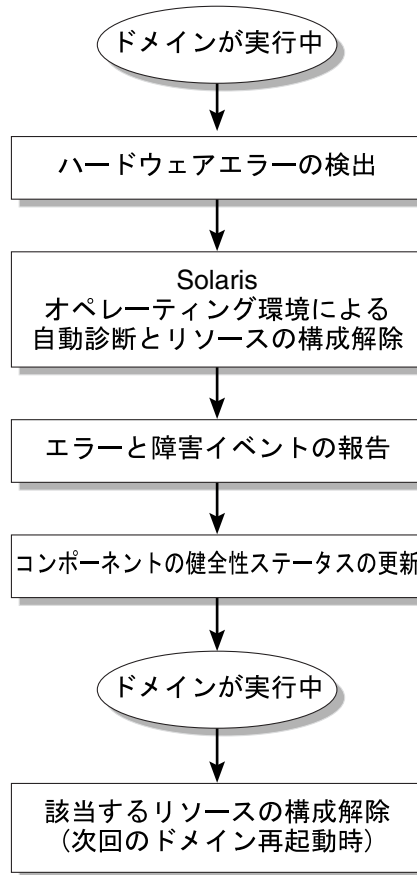


図 6-2 致命的でないドメインハードウェアエラーの自動診断プロセス

図 6-2 の手順は、以下の相違点を除けば、128 ページの「ドメイン停止に関するハードウェアエラー」の節で説明した手順と同じです。

- ハードウェアエラーの検出。Solaris OS は、致命的でないドメインハードウェアエラーが発生したことを判定し、そのエラーをシステムコントローラに報告します。影響を受けたドメインは停止されません。
- 自動診断とリソースの構成解除。Solaris OS によって、障害と、その障害の原因となっているリソースが特定されます。場合によっては、Solaris OS により、影響を受けたリソースの構成が解除されることもあります。たとえば、モジュール内で

致命的でないエラーが発生したために、CPU モジュールがオフラインになったり、仮想メモリページにエラーが含まれていたために、そのページが使用されなくなったりすることがあります。

- エラーと障害イベントの報告。Solaris OS から、SMS DE と同じチャネルを通して診断情報が提供されます。診断情報は、ドメインおよびプラットフォームログに表示されるイベントメッセージ、障害イベント通知または電子メールイベント通知、および `showlogs(1M)` によるイベント出力です。なお、Sun Management Center を使用している場合に、障害イベント通知が報告され、SMS または SRS Net Connect を構成した場合に、SMS 内または SRS Net Connect 経由により電子メールイベント通知が報告されます。

コード例 6-2 に、致命的でないハードウェアエラーの診断と、表示されるイベントメッセージ情報を示します。イベントメッセージは、[DOM] インジケータ以降の部分です。イベントメッセージの内容については、144 ページの「診断イベントの確認」を参照してください。

コード例 6-2 Solaris により特定された致命的でないドメインハードウェアエラーと、ドメインイベントメッセージの例

```
Sep 12 14:47:24 2005 smshostname dsmd[7839]: [0 876197473671508 ERR
SoftErrorHandler.cc 577] E$ Slot 3 SubSlot 5
Sep 12 14:47:25 2005 smshostname dsmd[7839]: [2552 876198449525014 ERR
SoftErrorHandler.cc 592] Soft Error: Comp ID : 0x62 Error Code: 3 Error Type: 1
Error Bit/Pin: 104
Sep 12 14:47:58 2005 smshostname erd[17227]: [11900 876231607099583 CRIT
MessageReportingService.cc 243] [DOM] Event: SF15000-8000-FF CSN: 352A00006
DomainID: D ADInfo: 1.SF-SOLARIS-DE.5-9-cs3:4791004-on81:08/18/2005 Time: Fri
Sep 12 14:47:38 PDT 2005 Recommended-Action: Service action required
```

注 – これらのイベントメッセージが表示されたとき、あるいはこれらのイベントが通知されたときは、サービスプロバイダに連絡してください。サービスプロバイダでは、自動診断情報を確認して、適切な保守アクションを開始します。

- **コンポーネントの健全性ステータスの更新。**SMS では、Solaris OS から提供された情報を使用して、影響を受けたハードウェアリソースのコンポーネントの健全性ステータスを更新します。
- **該当するリソースの構成解除。**障害の発生したドメインリソースを Solaris OS が前もって構成解除できなかった場合、次のドメイン再起動時にシステムから構成解除されます。

POST 検出ハードウェア障害

POST が実行されてシステムボードコンポーネントのテストと構成が行われると、自己診断で問題が発見されたコンポーネントは自動的にシステムから構成解除されます。それに応じて、影響を受けたコンポーネントの健全性ステータスも POST により更新されます。

コード例 6-3 に、POST DE によって報告された、ドメイン B に関する自動診断イベントメッセージを示します。イベントメッセージの内容については、144 ページの「診断イベントの確認」を参照してください。

コード例 6-3 POST 自動診断イベントメッセージの例

```
Sep  8 13:31:16 2005 smshostname erd[11987]: [11900 240509936296585 C  
RIT  
MessageReportingService.cc 243] [AD] Event: SF15000-8000-4L CSN: 352A00005  
DomainID: B ADInfo: 1.POST-DE.1.4.1 Time: Mon Sep  8 13:30:47 PDT 2005  
Recommended-Action: Service action required
```

これらのイベントメッセージが表示されたとき、あるいはこれらのイベントが通知されたときは、サービスプロバイダに連絡して、適切な保守アクションを開始するよう依頼してください。

電子メールイベント通知の有効化

電子メールイベント通知は、ドメイン障害イベントが発生したときに、指定された受信者に知らせる電子メール通知を自動的に生成する、任意指定の機能です。手動でプラットフォームやドメインのメッセージログを監視しなくても、重大な障害イベントの通知をただちに受信できます。

コード例 6-4 は、2つのコンポーネントが指摘されている (障害の原因である疑いもたれている) 障害イベントを報告している電子メールの例です。以下では、電子メールの内容と通知の制御方法を説明します。

コード例 6-4 イベント電子メールの例

```
Date: Tue, 19 Aug 2005 10:45:28 -0600 (MDT)
Subject: FAULT: SF15000, csn: 352A00007, main fault class: list.suspects
From: smshostname@xyz.com
To: undisclosed-recipients:;

FAULT: platform: SF15000, csn: 352A00007, main fault class: list.suspects
EVENT CODE: SF15000-8000-GK
EMBEDDED FAULT(S): fault.board.sb.1112
fault.board.ex.1112

Fault event in domain(s) R at Fri Jun 27 00:08:05 PDT 2005.
Fault severity = SMIEVENT_SEV_FATAL <7>
Indictment Count: 2
Indictment list:
sb11
ex11
```

以下のファイルが連携し合うことにより、イベント電子メールが作成されます。

- 電子メールテンプレート

このテンプレートでは、電子メールで報告するイベント情報を特定します。この情報には、電子メールの件名と、電子メールで報告する特定のイベント項目 (タグ) が含まれます。

- 電子メール制御ファイル (event_email.cf)

このファイル (/etc/opt/SUNWSMS/SMS/config/event_email.cf) では、特定のイベント情報、すなわちイベントクラスと、イベントによって影響を受けたドメインを使用して、指定する電子メール受信者と、報告するイベント情報を制御する電子メールテンプレートを指定します。

注 – イベント電子メール機能では、標準の sendmail ユーティリティを使用し、指定した電子メール受信者に電子メールを送信します。

▼ 電子メールイベント通知を有効にする

1. 電子メールテンプレートファイルで、電子メールで報告するイベントタグを指定します。

SMS で提供されているサンプル電子メールテンプレート(sample_email) をコピーし、コピーしたファイルを編集します。電子メールテンプレートの変更方法については、135 ページの「電子メールテンプレートの設定」を参照してください。

2. 電子メール制御ファイルで、電子メールの受信者と、使用する電子メールテンプレートを特定するパラメータを設定します。

SMS に含まれている電子メール制御ファイル(event_email.cf) を編集し、電子メール通知パラメータを指定します。

電子メール制御ファイルの変更方法については、138 ページの「電子メール制御ファイルの設定」を参照してください。

注 - 電子メール通知機能を使用する場合、電子メールの着信先アドレスを確認して、承認されているドメインだけに関するイベント通知を受信者が受信するようにします。担当者の職責や承認の有無に変更があったときは、適切なセキュリティ分離を維持するプロセスを導入し、必ず実施してください。

電子メールテンプレートの設定

sample_email (/etc/opt/SUNWSMS/SMS/config/templates) というサンプル電子メールテンプレートファイルが SMS で提供されています。コード例 6-5 にデフォルトのテンプレートを示します。小なり大なり括弧内のテキストは、イベント電子メールの本文に表示されるイベント情報を示します。

コード例 6-5 デフォルトのサンプル電子メールテンプレート

```
# Sample Email Template File - This sample is intended to convey
# a terse fault event notification to a pager.
#
# The following is the subject line for the email with the event
# descriptor from the event and the platform model and serial
# number inserted.
#
FAULT: <PLATFORM_MODEL>, serial# <PLATFORM_SERIAL_NUMBER>, code <EVENT_CODE>
#
# The following lines are the body of the email notification.
#
Fault event in domain(s) <EVENT_DOMAINS_AFFECTED> at <EVENT_TIMESTAMP>.
Fault severity = <EVENT_SEVERITY>
```

コード例 6-5 デフォルトのサンプル電子メールテンプレート (続き)

```

Indictment Count: <EVENT_INDICTMENT_COUNT>
Indictment list:
<EVENT_INDICTMENT_LIST>

Member fault list:
<EVENT_FAULT_MEMBERS>
# End of email template.

```

このサンプルテンプレートファイルをそのまま使用することも、このサンプルテンプレートファイルを新規ファイルにコピーし、そのコピーしたファイルを編集して、電子メールに含まれる追加イベントタグや別のイベントタグを特定できるようにすることもできます。サンプルテンプレートファイルのコピーや名前の変更を行うには、スーパーユーザー特権が必要です。ファイル名には任意の文字列を指定できます。

ファイルを編集する場合は、電子メールの件名と本文で報告するイベントタグを指定します。これらのタグは、ファイルの新しい行またはコメント行でない行 (# 記号が行頭に付いていない行) で指定します。電子メールテンプレートで指定できるタグのリストについては、表 6-1 を参照してください。

表 6-1 電子メールテンプレートファイルのイベントタグ

イベントタグ	表示される情報
<EVENT_CLASS>	イベントのカテゴリ (エラーレポート、障害イベント、または疑わしい障害のリスト) を示す、ドットで区切られた英数テキスト文字列。たとえば、list.suspects のように表示されます。
<EVENT_CODE>	イベントタイプを一意に識別する、ダッシュで区切られた英数字文字列。たとえば、SF15000-8000-GK のように表示されます。イベントコードは、イベントに関する障害クラスを要約したもので、そのイベントの詳細な情報をご購入先が取得するときに使用します。
<EVENT_DE_NAME>	障害イベントの判定に使用する診断エンジン (DE) の名前。SMS-DE、SF-SOLARIS-DE、または POST-DE のいずれかになります。
<EVENT_DE_VERSION>	イベントの判定に使用する診断エンジンのバージョン。
<EVENT_DOMAINS_AFFECTED>	イベントの影響を受けたドメインを、コンマで区切って列挙したリスト。
<EVENT_FAULT_MEMBERS>	障害イベントに関連する障害イベントクラスのリスト。たとえば、fault.board.sb.1112 のように表示されます。
<EVENT_INDICTMENT_COUNT>	障害イベントの原因となっている、あるいはその疑いがあるコンポーネントの数。
<EVENT_INDICTMENT_LIST>	障害の原因と指摘されたコンポーネント。各コンポーネントは 1 行ずつ表示されます。

表 6-1 電子メールテンプレートファイルのイベントタグ (続き)

イベントタグ	表示される情報
<EVENT_SEVERITY>	0 ～ 7 のレベルで表したイベントの重要度。たとえば、テストイベントメッセージの重要度は 2 で、ドメインが停止するような障害イベントの重要度は 7 (SMIEVENT_SEV_FATAL) です。
<EVENT_TIMESTAMP>	イベントが発生した日時。
<PLATFORM_SERIAL_NUMBER>	Sun Fire ハイエンドシステムの特定に使用するシャーシのシリアル番号。
<PLATFORM_MODEL>	イベントの影響を受けた製品のモデル番号 (SF15000、SFE25000、SF12000 または SFE20000)。

図 6-3 はカスタマイズされた電子メールテンプレートで、コード例 6-4 は、このテンプレートから作成された電子メールの例です。

カスタマイズされた電子メールテンプレート :

```
# Sample Email Template File - This sample is intended to convey
# a terse fault event notification to a pager.
#
# The following is the subject line for the email with the event
# descriptor from the event and the platform model and serial
# number inserted.
#
FAULT: platform: <PLATFORM_MODEL>, csn: <PLATFORM_SERIAL_NUMBER>, main fault class: <EVENT_CLASS>
EVENT CODE: <EVENT_CODE>
EMBEDDED FAULT(S): <EVENT_FAULT_MEMBERS>
#
# The following lines are the body of the email notification.
#
Fault event in domain(s) <EVENT_DOMAINS_AFFECTED> at <EVENT_TIMESTAMP>.
Fault severity = <EVENT_SEVERITY>

Indictment Count: <EVENT_INDICTMENT_COUNT>
Indictment list: <EVENT_INDICTMENT_LIST>
# End of email template.
```

次の障害イベントの電子メールが作成される :

```
Date: Tue, 21Jun 2005 10:45:28 -0600 (MDT)
Subject: FAULT: platform: SF15000, csn: 352A00007, main fault class: list.suspects
From: smshostname@xyz.COM
To: undisclosed-recipients;;

FAULT: platform: SF15000, csn: 352A00007, main fault class: list.suspects
EVENT CODE: SF15000-8000-GK
EMBEDDED FAULT(S): fault.board.sb.1112
fault.board.ex.1112

Fault event in domain(s) R at Tue Aug 19 10:45:18 MDT 2005.
Fault severity = SMIEVENT_SEV_INFO <7>

Indictment Count: 2
Indictment list:
sb11
ex11
```

図 6-3 電子メールテンプレートと作成された電子メールの例

電子メール制御ファイルの設定

電子メール制御ファイルには、次のことを実行する電子メール通知パラメータが含まれています。

- イベントクラスと、イベントが発生したドメインに基づいて、電子メールの受信者を特定します。
- 使用する電子メールテンプレートを特定します。

- イベントメッセージ構造を、イベント電子メールの添付ファイルとして送信するかどうかを指定します。

これらの通知パラメータを、SMS で提供されている電子メール制御ファイル (/etc/opt/SUNWSMS/SMS/config/event_email.cf) で指定します。このファイル (コード例 6-6) には、シャープ (#) 記号が行頭に付いたコメント行が含まれています。これらのコメント行で、ファイルの更新方法が説明されています。

コード例 6-6 電子メール制御ファイル (event_email.cf)

```
#
# Copyright (c) 2004 by Sun Microsystems, Inc.
# All rights reserved.
#
# Email Control File
#
# ident "@(#)event_email.cf 1.6      03/08/19 SMI"
#
# The following fields are required to receive email notification of fault
# events
# Event_Class Domains Template From Include-event? Recipients Script
# Event_Class and Domains are regular expressions filtering for specific event
# types and affected domains. Domains are required to be upper case.
# The following example, uncommented, generates an email for any List Event
# containing a Fault Event, affecting any domain, and sends it to
# two recipients.
# The Packed Event List is included as an attachment to the email.
#
# Event_Class Domains Template From Include-event? Recipients Script
#^fault[.] [A-R] sample_email FMA@xyz.com Y adm@xyz.com,adm2xyz.com sendmail.sh
#
#
# The following example, uncommented, generates an email for any Event
# that contains a Fault Event and affects domains A through C. The Packed
# Event List is not sent as an attachment. The user would be required to add his
# custom fault_email template to the directory
# /etc/opt/SUNWSMS/config/templates, and for tag
# replacement to work should refer to the documentation, or look at the
# sample_email template in that directory.
#^fault[.] [A-C] fault_email FMA@xyz.com N admin.manager@xyz.com sendmail.sh
```

テキストエディタを使用してファイルを編集し、新しい行またはコメント行でない行に通知パラメータを追加します。電子メール制御ファイルを編集して、必要な電子メールパラメータを追加するには、スーパーユーザー特権が必要です。各パラメータは、スペースまたはタブで区切ります。ドメイン、イベントクラス、または電子メール

ルテンプレートごとに、異なるイベント電子メールメッセージの配布方法を指定する複数の通知行を入力できます。設定する通知パラメータについては、表 6-2 で説明します。

Event_Class と *Domains* パラメータは、正規表現を使用して、範囲や特定の一致条件で指定することができます。regex(5) マニュアルページで説明されているように、電子メール制御ファイルでは、拡張正規表現がサポートされています。いくつかの有効な正規表現の例を以下に示します。

- . (ピリオド) - 任意の 1 文字に対応します。
- ^ (サーカムフレックス) - この文字列から始まる文字列に対応します。たとえば、`^fault` は、`fault` から始まる任意の文字列になります。
- [BDG] - B、D、G のうちのいずれかの 1 文字に対応します。
- [B-F] - B から F までの間の任意の 1 文字 (つまり、B、C、D、E、F のいずれか) に対応します。

表 6-2 電子メール制御ファイルのパラメータ

電子メール制御パラメータ	説明
<i>Event_Class</i>	フィルタとして使用する障害イベントクラス。 このパラメータが広範囲のイベントクラスに適用されるように、イベントクラスを正規表現で指定します。たとえば、デフォルトの書式 <code>fault.*</code> では、「 <code>fault</code> 」というイベント名の障害イベントが、すべてイベント電子メールに報告されます。
<i>Domains</i>	フィルタとして使用するドメイン。デフォルトの書式 [A-R] では、A から R までのドメインで発生した障害イベントが電子メールで特定されます。ドメインは大文字で指定します。
<i>Template</i>	電子メールの内容の作成に使用する電子メールテンプレートファイルの名前。
<i>From</i>	電子メールの作成者の電子メールアドレス。
<i>Include-event?</i>	以下の状態のいずれかです。 <ul style="list-style-type: none">● Y - はい、イベントメッセージ構造の 2 進ファイルを、電子メールの添付ファイルとして含めます。このファイルは、サービスプロバイダによるトラブルシューティングの際に使用できます。● N - いいえ、イベントメッセージ構造の 2 進ファイルを、電子メールの添付ファイルとして含めません。
<i>Recipients</i>	イベント電子メールを受信する個人の電子メールアドレス。各アドレスはコマンドで区切ります。
<i>Script</i>	指定した受信者に電子メールを送信する際に使用するシェルスクリプト。 <code>/etc/opt/SUNWSMS/config/scripts</code> の <code>sendmail.sh</code> スクリプトが標準のスクリプトであり、デフォルトで使用されるが、この標準のスクリプトの代わりに独自に作成したスクリプトを同じディレクトリで使用することもできます。

コード例 6-7 は、更新された電子メール制御ファイルで、通知パラメータがファイルの最後に追加されています。sendmail.sh スクリプトを使用して、指定した 2 人の受信者にイベント電子メールが送信されます。A から C までのドメインで発生したすべての障害イベントに対してイベント電子メールが作成され、sample_email というテンプレートファイルを基にして書式が設定されます。電子メールとともに、イベントメッセージ構造が 2 進ファイルの添付ファイルとして送信されます。

コード例 6-7 電子メール制御ファイルの例

```
#
# Copyright (c) 2004 by Sun Microsystems, Inc.
# All rights reserved.
# Email Control File
#
# ident "@(#)event_email.cf 1.1      03/03/12 SMI"
#
# The following fields are required to receive email notification of fault
# events
# Event_Class Domains Template From Include-event? Recipients-Script
# Event_Class and Domains are regular expressions filtering for specific event
# types and affected domains. Domains are required to be upper case.
# The following example, uncommented, generates an email for any List Event
# containing a Fault Event, affecting any domain, and sends it to
# two recipients. Recipients are email addresses separated by commas if there
# are more than 1. Embedded blanks are not permitted in the Recipients list.
# The Packed Event List is included as an attachment to the email.
#
# Event_Class Domains Template From Include-event? Recipients Script
#^fault[.] [A-R] sample_email FMA@xyz.com Y adm1@xyz.com,adm2@xyz.com sendmail.sh
#
#
# The following example, uncommented, generates an email for any Event
# that contains a Fault Event and affects domains A through C. The Packed
# Event List is not sent as an attachment. The user would be required to add his
# custom fault_email template to the directory
# /etc/opt/SUNWSMS/config/templates, and for tag
# replacement to work should refer to the documentation, or look at the
# sample_email template in that directory.
#
#^fault[.] [A-C] sample_email FMA@xyz.com Y adm1@xyz.com,adm2@xyz.com sendmail.sh
^fault[.] [A-C] sample_email FMA@xyz.com Y adm1@xyz.com,adm2@xyz.com sendmail.sh
```

電子メールイベント通知のテスト

testemail(1M) コマンドを使用して、電子メールイベント通知を確認します。このコマンドを使用すると、イベントを追跡し、電子メール制御ファイルに加えられた変更をチェックすることもできます。

▼ 電子メールイベント通知をテストする

1. 133 ページの「電子メールイベント通知の有効化」の説明に従って、電子メールイベントテンプレートと電子メール制御ファイルを設定します。
2. SC ウィンドウで、プラットフォーム管理者またはプラットフォーム保守としてログインし、以下のように入力します。

```
sc0:sms-user:> /opt/SUNWSMS/SMS/lib/smsadmin/testemail -c event-class-list -d domain-id [-i resource-indictment-list]
```

ここで次の点に留意します。

event-class-list は、追跡対象となる 1 つ以上の障害イベントクラスのリストです。

domain-id には、A-R の間のドメインを 1 つ指定します。

resource-indictment-list は、省略可能なリストで、指定した各イベントクラスに割り当てる 1 つ以上のコンポーネントを指定します。コンポーネントの有効値のリストについては、testemail(1M) マニュアルページを参照してください。

たとえば、次のコマンドはドメイン A からイベントタイプ `fault.test.email` を生成します。

```
sc0:sms-user:> /opt/SUNWSMS/SMS/lib/smsadmin/testemail -c fault.test.email -d A
```

3. テストイベントがプラットフォームまたはドメインメッセージログに記録されたことを確認します。

たとえば、次のようなメッセージがプラットフォームのメッセージログに表示されません。

```
Aug 19 10:45:28 2005smshostname [6696:1]: [11917 682823530704603 ERR teste mailApp.cc 345] Test fault with code SF15000-8000-Y1 generated by user root using testEmailReporting - please ignore
```


4. テストイベントが正常にメッセージログに記録された場合は、指定した受信者がテスト電子メールを受信したことを確認します。

たとえば、テスト電子メールは次のように表示されます。

```
Date: Tue, 19 Aug 2005 10:45:28 -0600 (MDT)
Subject: FAULT: SF15000, serial# 352A0008, code SF15000-8000-Y1
From: smshostname@xyz.com
To: undisclosed-recipients:;

FAULT: SF15000, serial# 352A0008, code SF15000-8000-Y1
Fault event in domain(s) A at Tue Aug 19 10:45:18 MDT 2005.
Fault severity = SMIEVENT_SEV_INFO <2>
Indictment Count: 0
Indictment list:

Member fault list:
fault.test.email
```

テスト電子メールが作成されなかった場合は、次の節を参考にしてトラブルシューティングを行なってください。

テスト電子メールの作成に失敗した場合の対処法

テスト電子メール通知が受信されなかった場合は、次の操作を行なってください。

1. 電子メールイベントテンプレートと電子メール制御ファイルを調べて、ファイルが正しく設定されていることを確認します。
2. ドメインとプラットフォームのメッセージログを調べて、テストイベントが記録されていることを確認します。
3. `sendmail` デーモンが実行されていることを確認します。たとえば、次のメッセージが表示されます。

```
sc0:sms-user:> ps -ef | grep sendmail
  root   256      1  0   Aug 06 ?          0:05 /usr/lib/sendmail -bd -q15m
 sms-user 525 28546  0 21:23:15 pts/27   0:00 grep sendmail
```

`sendmail` デーモンが実行されていない場合は、インストールの設定を修正しなければならない可能性があります。手順 4 に進みます。

4. スーパーユーザーとしてログインして sendmail デーモンを再起動することにより、手動で sendmail を起動して、次回再起動するまで実行されるようにします。

```
sc0:# /usr/lib/sendmail -bd -q15m &
```

5. SC 上の /var/log/syslog を調べ、電子メールが Mail Transfer Agent (MTA) である sendmail によって送信されたかどうかを確認します。

sendmail が設定されていない場合や、正しく設定されていなかった場合は、エラーメッセージがこのログファイルに表示されるはずですが。

6. ドメインおよびネームサーバーの IP アドレス (システムコントローラの外部に電子メールメッセージを配信するため) が /etc/resolv.conf ファイルで指定されていることを確認します。
7. sendmail.sh を再起動します。

```
sc0:#:/etc/inet.d/sendmail stop
sc0:#:/etc/inet.d/sendmail start
```

診断および回復情報の取得

ここでは、診断エラーを監視し、障害およびエラーイベントに関する追加情報を取得するさまざまな方法について説明します。

診断イベントの確認

loghost サーバーが構成されている場合は、自動診断 [AD] およびドメイン [DOM] イベントメッセージがプラットフォームメッセージログとドメインのコンソール、または syslog ホストに表示されます。[AD] または [DOM] イベントメッセージ (コード例 6-1、コード例 6-2、およびコード例 6-3 を参照) には、次の情報が含まれています。

- [AD] または [DOM] - メッセージの開始位置。AD は、SMS または POST 自動診断エンジンによって、イベントメッセージが作成されたことを示します。DOM は、影響を受けたドメインの Solaris OS によって、自動診断イベントメッセージが作成されたことを示します。

- **Event** - イベントのコード。イベントタイプを一意に識別する、ダッシュで区切られた文字列です。このコードは、イベントと関連プラットフォームに関する詳細な情報を取得するときに、ご購入先が使用します。
- **CSN** - シャーシのシリアル番号。使用している **Sun Fire** ハイエンドシステムを特定します。
- **DomainID** - ハードウェアエラーによって影響を受けたドメイン。有効なドメインは **A** から **R** までです。
- **ADInfo** - 自動診断メッセージのバージョン、診断エンジンの名前 (**SMS-DE**、**SF-SOLARIS-DE**、または **POST-DE**)、および診断エンジンのバージョン (使用中の **SMS** のバージョンまたは **Solaris OS** のバージョン)。
- **Time** - 自動診断の西暦年、月、日、曜日、タイムゾーン、時刻 (時、分、秒)。
- **Recommended-Action: Service action required** - サービスプロバイダに連絡して以降の保守アクションを依頼するように、プラットフォームやドメイン管理者に指示しています。また、自動診断メッセージの最後であることも示します。

イベントログの確認

プラットフォームの管理者特権、またはプラットフォームの保守特権を持っている場合は、`showlogs` コマンドを使用して、イベントログの内容を確認し、特定のタイプのイベントに関する詳細な情報を取得することができます。表示される情報は、サービスプロバイダがトラブルシューティングの際にも使用できます。

イベントログに記録されている、次のタイプ (クラス) のイベント情報を取得できません。

- **Ereports** - 予期しないコンポーネントの動作または状態についてのデータを提供するエラーレポート。
- **List events** - ハードウェアエラーに関係する障害イベントまたは疑わしい障害をリストで提供するリストイベント。

表 6-3 は、`showlogs` コマンドを使用してイベント情報を表示する方法の一部を示しています。

表 6-3 エラーおよび障害イベント情報を表示する showlogs(1M) コマンドのオプション

コマンドのオプション	説明
<code>showlogs -E -p e</code>	イベントログの最後のイベントを要約して表示します。
<code>showlogs -E -p e number</code>	イベントの最後の <i>number</i> 個のイベントデータを要約して表示します。たとえば、 <code>showlogs -E -p e 3</code> では、イベントログの最後 3 つの簡潔なイベント情報が表示されます。
<code>showlogs -p e list</code>	イベントログの最後のリストイベントを表示します。
<code>showlogs -p e ereport</code>	イベントログの最後の ereport (エラーレポート) を表示します。エラーレポートには、予期しない状態や動作など、ハードウェアに関する特定の情報が含まれます。
<code>showlogs -d domain-ID -p e number</code>	指定したドメインの最後の <i>number</i> 個のイベントを表示します。
<code>showlogs -E -p e event-code</code>	指定したイベントコードのイベントログ情報を要約して表示します。

showlogs コマンドのオプションの詳細と、イベントの出力例については、『System Management Services (SMS) 1.6 リファレンスマニュアル』の showlogs(1M) コマンドの説明を参照してください。

Capacity on Demand

Sun Fire ハイエンドシステムは、システムボード上に複数のプロセッサ (CPU) を搭載して構成されています。これらのボードは、初期システム構成の一部、またはアドオンコンポーネントとしてすでに購入いただいています。ボード上の CPU の使用権は、初期購入価格に含まれています。

Capacity on Demand (COD) オプションは、必要になった時点で代金を支払って使用できる、予備の処理リソースを提供します。COD オプションでは、ライセンスのない COD システムボードを購入してシステムに取り付けます。各 COD システムボードには 4 つの CPU が搭載されており、これらの CPU が使用可能な処理リソースとみなされます。しかし、このボードに対する COD RTU (right-to-use) ライセンスも購入するまで、COD CPU を使用する権利はありません。COD RTU ライセンスを購入すると、ライセンスキーを受け取り、ライセンスに応じた個数の COD プロセッサが使用できるようになります。

SMS ソフトウェアに含まれている COD コマンドを使用して、COD 資源の割り当て、起動、監視を行います。

この章では、次の項目を説明します。

- 148 ページの「COD の概要」
- 151 ページの「COD の開始」
- 151 ページの「COD RTU ライセンスの管理」
- 155 ページの「COD 資源の起動」
- 158 ページの「COD 資源の監視」

COD の概要

COD オプションでは、使用しているシステムに取り付ける COD システムボード上で追加の CPU リソースが提供されます。Sun Fire ハイエンドシステムは、最小数の標準 (アクティブ) システムボード構成で出荷されますが、標準のシステムボードと COD システムボードの両方を混在させて、最大で 18 個まで取り付けることができます。システムの各ドメインには、アクティブな CPU が少なくとも 1 つ必要です。

COD オプションが必要となり、現在 COD システムボードがシステムに構成されていない場合は、COD システムボードの購入についてご購入先に連絡してください。購入先の販売担当者がサービス代理店と協力して、COD システムボードをお使いのシステムに取り付けいたします。

以下では、COD オプションの主要要素について説明します。

- 148 ページの「COD ライセンス取得プロセス」
- 149 ページの「COD RTU ライセンスの割り当て」
- 150 ページの「インスタントアクセス CPU」
- 150 ページの「資源の監視」

COD ライセンス取得プロセス

COD CPU 資源を使用可能にするには、COD RTU ライセンスが必要です。COD のライセンスを取得するには、次のタスクを実行します。

1. COD 資源を使用可能にするための COD RTU ライセンス証明書と COD RTU ライセンスキーを取得します。

COD RTU ライセンスは、購入先からいつでも購入することができます。次に、購入した COD 資源用のライセンスキーを Sun License Center から取得します。

2. COD RTU ライセンスキーを COD ライセンスデータベースに入力します。

COD 資源を使用できるようにするライセンスキーを、COD ライセンスデータベースに格納します。COD ライセンスデータベースには、`addcodlicense(1M)` コマンドを使用して、このライセンス情報を記録します。COD RTU ライセンスは、システムにインストールされているすべての COD CPU リソースに使用できます。

ライセンス取得タスクについての詳細は、151 ページの「COD RTU ライセンスキーを取得して COD ライセンスデータベースに追加する」を参照してください。

COD RTU ライセンスの割り当て

COD オプションでは、購入した COD システムボード数と COD RTU ライセンス数によって使用できる COD CPU の個数が決まり、この個数の COD CPU を使用できるようにシステムが構成されます。取得した COD RTU ライセンスは、プールされた使用可能ライセンスの集まりとして扱われます。

COD システムボードが含まれているドメインを使用可能にするか、動的再構成 (DR) 操作により COD システムボードがドメインに接続されると、次の処理が自動的に実行されます。

- 現在インストールされている COD RTU ライセンスを確認します。
- COD ボード上の各 CPU に対して (ライセンスプールから) COD RTU ライセンスを取得します。

COD RTU ライセンスは、「先着順」で CPU に割り当てられます。ただし、`setupplatform(1M)` コマンドを使用すると、特定の数の RTU ライセンスを特定のドメインに割り当てることができます。詳細は、156 ページの「インスタントアクセス CPU を使用可能にし、ドメイン RTU ライセンスを予約する」を参照してください。

十分な数の COD RTU ライセンスがなく、ライセンスを COD CPU に割り当てられない場合には、その COD CPU はドメインに構成されず、ライセンスがないものとみなされます。ドメインに割り当てられてもアクティブでない COD CPU は、未使用とみなされます。

COD システムボードの COD CPU に必要な数の COD RTU ライセンスがない場合は、システムはライセンスがない CPU を無効にしてそのボードをドメイン内に組み込みます。どの CPU にも COD RTU ライセンスがないと、システムはボード全体を無効にし、そのボードをドメインに組み込まないようにします。詳細と例については、164 ページの「構成解除された COD CPU とライセンスを受けていない COD CPU」を参照してください。

DR 操作によってドメインから COD システムボードを使用不可にするか、COD システムボードが含まれているドメインが正常にシャットダウンされると、そのボード上の CPU に対する COD RTU ライセンスが解放されて、使用可能ライセンスのプールに追加されます。

`showcodusage` コマンドを使用すると、COD の使用状況と COD RTU ライセンスの状態を確認できます。COD 情報を表示する `showcodusage` などのコマンドについての詳細は、159 ページの「COD 資源使用状況」を参照してください。

注 – Sun Fire ハイエンドシステム (Sun Fire 25K/E15K、20K/E20K、6800、4810、4800、および 3800 サーバー) 間で COD CPU/メモリーボードを移動することはできませんが、そのボードに関連付けられているライセンスキーは購入時の元のプラットフォームに限定されているため、移転することはできません。

インスタントアクセス CPU

COD RTU ライセンスの購入プロセスが完了する前に COD CPU 資源が必要となった場合は、「インスタントアクセス CPU」(「ヘッドルーム」とも呼ばれる)という限定された個数の資源を一時的に使用可能にすることができます。Sun Fire ハイエンドシステムで使用可能なインスタントアクセス CPU の最大数は 8 個です。

インスタントアクセス CPU は、デフォルトでは Sun Fire ハイエンドシステムで使用不可になっています。インスタントアクセス CPU を使用する場合は、`setupplatform(1M)` コマンドを使用してこれらの資源を起動します。使用するインスタントアクセス CPU (ヘッドルーム) の数が使用可能な COD ライセンス数を越えていることを通知する警告メッセージが、プラットフォームのコンソールにログとして表示されます。インスタントアクセス CPU 用の COD RTU ライセンスキーを取得して COD ライセンスデータベースに追加すると、この警告メッセージは表示されなくなります。

インスタントアクセス CPU の起動方法についての詳細は、151 ページの「COD RTU ライセンスキーを取得して COD ライセンスデータベースに追加する」を参照してください。

ホットスペアとして使用するインスタントアクセス CPU

障害が発生した非 COD CPU を交換する際に、用意されているインスタントアクセス CPU を一時的に使用可能にすることができます。この場合、インスタントアクセス CPU は、「ホットスペア」(障害が発生した非 COD CPU の代わりにただちに使用可能なスペアの CPU) と見なされます。しかし、障害が発生した非 COD CPU の交換が終わったら、インスタントアクセス CPU を無効にする必要があります (156 ページの「インスタントアクセス CPU を使用可能にし、ドメイン RTU ライセンスを予約する」を参照)。インスタントアクセス CPU を継続使用する場合は、購入先に連絡して、使用しているインスタントアクセス CPU の COD RTU ライセンスを購入してください。

資源の監視

インスタントアクセス CPU (ヘッドルーム) の使用可能への切り替えやライセンス違反など、COD イベントに関する情報はプラットフォームのログに記録され、`showlogs` コマンドを使用して表示することができます。

`showcodusage(1M)` コマンドなどのその他のコマンドは、COD コンポーネントと COD 構成に関する情報を提供します。COD の情報と状態を取得する方法についての詳細は、158 ページの「COD 資源の監視」を参照してください。

COD の開始

Sun Fire ハイエンドシステムで COD を使用するには、事前に必要事項を完了しておいてください。必要事項には、次のタスクが含まれています。

- メインとスペア両方のシステムコントローラ (SC) に同じバージョンの SMS ソフトウェアをインストールします。
ソフトウェアのアップグレードの詳細は、『System Management Services (SMS) 1.6 インストールマニュアル』を参照してください。

注 – SMS 1.3 より前のバージョンの SMS ソフトウェアでは、COD システムボードは認識されません。

- 購入先に連絡し、以下の事項を実行する。
 - Sun Fire ハイエンドシステムの標準の購入同意契約に加え、COD 契約追補に署名します。
 - COD システムボードを購入し、取り付けの準備をします。
- 151 ページの「COD RTU ライセンスキーを取得して COD ライセンスデータベースに追加する」の説明に従って、COD RTU ライセンス取得プロセスを実行します。

COD RTU ライセンスの管理

COD RTU ライセンス管理には、COD RTU ライセンスキーを取得して COD ライセンスデータベースに追加する作業が含まれます。また、必要に応じて、ライセンスデータベースから COD RTU ライセンスを削除することもできます。

▼ COD RTU ライセンスキーを取得して COD ライセンスデータベースに追加する

1. ご購入先に連絡して、使用可能にする COD CPU ごとに COD RTU ライセンスを購入します。

購入した各 CPU ライセンスに対して、Sun から COD RTU ライセンス証明書が送付されます。ライセンス証明書に貼付されている COD RTU ライセンスステッカーに、使用権シリアル番号が記載されています。COD RTU ライセンスキーを取得するときにこのシリアル番号を使用します。

2. Sun License Center に連絡し、以下の情報を提供して COD RTU ライセンスキーを取得します。

- COD RTU ライセンス証明書のライセンスステッカーに記載されている COD RTU シリアル番号。
- シャーシのホスト ID。この ID は、プラットフォームを一意に識別するものです。

シャーシのホスト ID は、プラットフォーム管理者として `showplatform -p cod` コマンドを実行すると入手できます。

Sun License Center への連絡方法については、受け取った COD RTU ライセンス証明書を参照するか、下記の Sun License Center の Web サイトで確認してください。

<http://www.sun.com/licensing>

購入した COD 資源の RTU ライセンスキーが記載された電子メールメッセージが、Sun License Center から送信されます。

3. `addcodlicense (1M)` コマンドを使用して、このライセンスキーを COD ライセンスデータベースに追加します。

SC ウィンドウで、プラットフォーム管理者としてログインし、以下のように入力します。

```
sc0:sms-user:> addcodlicense license-signature
```

ここで、*license-signature* は、Sun License Center から割り当てられた完全な COD RTU ライセンスキーです。このライセンスキーの文字列を、Sun License Center から受信した電子メールからコピーすることもできます。

4. `showcodlicense -r` コマンドを実行して、指定したライセンスキーが COD ライセンスデータベースに追加されていることを確認します (153 ページの「COD ライセンス情報を表示する」を参照)。

追加した COD RTU ライセンスキーが、`showcodlicense(1M)` コマンドの出力リストに表示されているはずです。

▼ COD ライセンスデータベースから COD ライセンスキーを削除する

1. SC ウィンドウで、プラットフォーム管理者としてログインし、以下のように入力します。

```
sc0:sms-user:> deletecodlicense license-signature
```

ここで次の点に留意します。

license-signature は、COD ライセンスデータベースから削除する完全な COD RTU ライセンスキーです。

システムでは、ライセンスの削除によって COD RTU ライセンス違反が発生しないことを確認します。使用中の COD 資源数に対して COD ライセンス数が足りない場合に、COD RTU ライセンス違反が発生します。ライセンスを削除すると COD RTU ライセンス違反が発生する場合は、SC ではライセンスキーを削除しません。

注 - `deletecodlicense(1M)` コマンドに `-f` オプションを付けて指定すると、ライセンスキーを強制的に削除することができます。しかし、ライセンスキーの削除によって、ライセンス違反が発生したり、RTU ライセンス予約を必要以上に割り当ててしまう可能性があるので注意してください。システムにインストールされている RTU ライセンスより RTU ドメイン予約が多い場合に、RTU ライセンスの過剰割り当てが発生します。詳細は、『System Management Services (SMS) 1.6 リファレンスマニュアル』の `deletecodlicense(1M)` コマンドの説明を参照してください。

2. `showcodlicense -r` コマンドを実行して、ライセンスキーが COD ライセンスデータベースから削除されていることを確認します (次の手順を参照)。

削除されたライセンスキーは、`showcodlicense` コマンドの出力リストに表示されていないはずで

▼ COD ライセンス情報を表示する

1. SC ウィンドウで、プラットフォーム管理者としてログインし、以下のいずれかを入力して COD ライセンス情報を表示します。

- 変換された形式でライセンスデータを表示するには、次のように入力します。

```
sc0:sms-user:> showcodlicense
```

たとえば、次のメッセージが表示されます。

```
sc0:sms-user:> showcodlicense
```

Description	Lic Ver	Expiration	Count	Status	Cls	Tier Num	Req
PROC	01	NONE	16	GOOD	1	1	0

表 7-1 では、showcodlicense による出力の COD ライセンス情報について説明します。

表 7-1 COD ライセンス情報

項目	説明
説明	資源 (プロセッサ) の種類
Lic Ver	ライセンスのバージョン番号
Expiration	なしサポートされていない (有効期限はない)
Count	指定した資源に対して許可されている RTU ライセンス数
Status	以下の状態のいずれかです。 <ul style="list-style-type: none"> • GOOD - 資源のライセンスが有効であることを示します。 • EXPIRED - 資源のライセンスが有効でないことを示します。
Cls	適用されません。
Tier Num	適用されません。
Req	適用されません。

- 未処理のライセンスキー形式でライセンスデータを表示するには、次のように入力します。

```
sc0:sms-user:> showcodlicense -r
```

COD 資源のライセンスキーシグニチャーが表示されます。たとえば、次のメッセージが表示されます。

```
sc0:sms-user:> showcodlicense -r
01:5014936C37048:45135285:0201000000:8:00000000:000000000000000000000000
```

注 – 上記の COD RTU ライセンスキーは一例として記載したもので、有効なライセンスキーではありません。

showcodlicense(1M) コマンドの詳細は、『System Management Services (SMS) 1.6 リファレンスマニュアル』のコマンドの説明を参照してください。

COD 資源の起動

インスタントアクセス CPU を使用可能にし、特定のドメインに COD RTU ライセンスを割り当てるには、`setupplatform` コマンドを使用します。表 7-2 で、COD 資源を構成するときに使用できる `setupplatform` コマンドの各種のオプションについて説明します。

表 7-2 COD 資源を構成するときの `setupplatform` コマンドのオプション

<code>setupplatform</code> コマンドのオプション	説明
<code>setupplatform -p cod</code>	インスタントアクセス CPU (ヘッドルーム) を使用可能または使用不可にし、ドメインの COD RTU ライセンスを割り当てます。
<code>setupplatform -p cod headroom-number</code>	インスタントアクセス CPU (ヘッドルーム) を使用可能または使用不可にします。
<code>setupplatform -p cod -d domainid RTU-number</code>	特定のドメインに対して、指定した数の COD RTU ライセンスを予約します。

`setupplatform` コマンドのオプションについての詳細は、『System Management Services (SMS) 1.6 リファレンスマニュアル』のコマンドの説明を参照してください。

▼ インスタントアクセス CPU を使用可能にし、ドメイン RTU ライセンスを予約する

1. SC ウィンドウで、プラットフォーム管理者としてログインし、以下のように入力します。

```
sc0:sms-user:> setupplatform -p cod
```

COD パラメータ (ヘッドルーム数とドメイン RTU 情報) を入力するようプロンプトが表示されます。たとえば、次のメッセージが表示されます。

```
sc0:sms-user:> setupplatform -p cod
PROC RTUs installed: 12
PROC Headroom Quantity (0 to disable, 8 MAX) [0]:0
PROC RTUs reserved for domain A (12 MAX) [0]: 4
PROC RTUs reserved for domain B (8 MAX) [2]: 4
PROC RTUs reserved for domain C (4 MAX) [0]: 0
PROC RTUs reserved for domain D (4 MAX) [0]:?
PROC RTUs reserved for domain E (4 MAX) [0]?
PROC RTUs reserved for domain G (4 MAX) [0]?
PROC RTUs reserved for domain H (4 MAX) [0]?
PROC RTUs reserved for domain I (4 MAX) [0]?
PROC RTUs reserved for domain J (4 MAX) [0]?
PROC RTUs reserved for domain K (4 MAX) [0]?
PROC RTUs reserved for domain L (4 MAX) [0]?
PROC RTUs reserved for domain M (4 MAX) [0]?
PROC RTUs reserved for domain N (4 MAX) [0]?
PROC RTUs reserved for domain O (4 MAX) [0]?
PROC RTUs reserved for domain P (4 MAX) [0]?
PROC RTUs reserved for domain Q (4 MAX) [0]?
PROC RTUs reserved for domain R (4 MAX) [0]?
```

表示されるプロンプトについて、以下のことに注意してください。

- インスタントアクセス CPU (ヘッドルーム) 数

括弧内のテキストは、インスタントアクセス CPU (ヘッドルーム) の最大許容数を示しています。角括弧内の数値は、現在構成されているインスタントアクセス CPU 数です。

インスタントアクセス CPU (ヘッドルーム) 機能を使用不可にするには、0 を入力します。ヘッドルーム数を使用不可にできるのは、使用されているインスタントアクセス CPU がないときのみです。

- ドメインの予約

括弧内のテキストは、ドメイン用に予約可能な RTU ライセンスの最大数を示しています。角括弧内の数値は、現在ドメインに割り当てられている RTU ライセンス数です。

2. showplatform(1M) コマンドを実行して、COD 資源の構成を確認します。

```
sc0:sms-user:> showplatform -p cod
```

たとえば、次のメッセージが表示されます。

```
sc0:sms-user:> showplatform -p cod

COD:
====
Chassis HostID : 5014936C37048
PROC RTUs installed: 8
PROC Headroom Quantity: 0
PROC RTUs reserved for domain A : 4
PROC RTUs reserved for domain B : 0
PROC RTUs reserved for domain C : 0
PROC RTUs reserved for domain D : 0
PROC RTUs reserved for domain E : 0
PROC RTUs reserved for domain F : 0
PROC RTUs reserved for domain G : 0
PROC RTUs reserved for domain H : 0
PROC RTUs reserved for domain I : 0
PROC RTUs reserved for domain J : 0
PROC RTUs reserved for domain K : 0
PROC RTUs reserved for domain L : 0
PROC RTUs reserved for domain M : 0
PROC RTUs reserved for domain N : 0
PROC RTUs reserved for domain O : 0
PROC RTUs reserved for domain P : 0
PROC RTUs reserved for domain Q : 0
PROC RTUs reserved for domain R : 0
```

注 – シャーシのホスト ID は、COD ライセンスを取得するために使用されます。Chassis HostID が UNKNOWN と表示された場合は、センタープレーンサポートボードの電源を入れて、シャーシのホスト ID を入手してください。この場合、電源投入後 1 分間ほど待ってから、showplatform コマンドを再度実行し、シャーシのホスト ID を表示してください。

COD 資源の監視

この節では、COD 資源の使用状況を追跡し、COD 情報を入手するさまざまな方法について説明します。

COD システムボード

`showboards(1M)` コマンドを使用すると、システムのどのシステムボードが COD ボードであるかを判定することができます。

▼ COD システムボードを特定する

- SC ウィンドウで、プラットフォーム管理者としてログインし、以下のように入力します。

```
sc0:sms-user:> showboards -v
```

表示される情報には、ボードの割り当てとテスト状態が示されます。COD CPU ボードは、CPU (COD) と表示されます。

たとえば、次のメッセージが表示されます。

```
sc0:sms-user:> showboards -v
Location      Pwr    Type of Board  Board Status  Test Status  Domain
-----
SC0           On     SC             Main          -            -
SC1           On     SC             Spare         -            -
PS0           On     PS             -            -            -
PS1           On     PS             -            -            -
.
.
.
SB0           Off    CPU            Available     Unknown     Isolated
SB1           -     Empty Slot     Available     -           Isolated
SB2           Off    CPU            Available     Unknown     Isolated
SB3           -     Empty Slot     Available     -           Isolated
SB4           On     CPU (COD)      Assigned     Unknown     A
SB5           -     Empty Slot     Available     -           Isolated
SB6           On     CPU (COD)      Active        Passed      B
SB7           -     Empty Slot     Available     -           Isolated
SB8           -     Empty Slot     Available     -           Isolated
SB9           -     Empty Slot     Available     -           Isolated
SB10          -     Empty Slot     Available     -           Isolated
SB11          -     Empty Slot     Available     -           Isolated
SB12          Off    CPU (COD)      Assigned     Unknown     C
.
.
.
```

COD 資源使用状況

使用しているシステムでの COD 資源の使用状況に関する情報を取得するには、`showcodusage(1M)` コマンドを使用します。

▼ 資源ごとに COD 使用状況を表示する

- SC ウィンドウで、プラットフォーム管理者としてログインし、以下のように入力します。

```
sc0:sms-user:> showcodusage -p resource
```

たとえば、次のメッセージが表示されます。

```
sc0:sms-user:> showcodusage -p resource
Resource:
=====
Resource      In Use   Installed  Licensed  Status
-----
PROC          4        12         12        OK: 8 available
```

表 7-3 では、showcodusage(1M) コマンドを使用して表示した COD 資源の情報について説明します。

表 7-3 showcodusage で表示される資源情報

項目	説明
Resource	COD 資源 (プロセッサ)。
In Use	現在システムで使用されている COD CPU 数。
Installed	システムに取り付けられている COD CPU 数。
Licensed	インストールされている COD RTU ライセンス数。
Status	次の COD 状態のいずれかになります。 <ul style="list-style-type: none">• OK - 使用中の COD CPU に対して十分なライセンスがあることを示し、その他に使用可能な COD 資源数と、使用可能なインスタントアクセス CPU (ヘッドルーム) 数を表示します。• HEADROOM - 使用中のインスタントアクセス CPU 数。• VIOLATION - ライセンス違反があることを示します。使用中の COD CPU 数のうち、利用可能な COD RTU ライセンスを超過する部分がライセンス違反になります。COD ライセンスデータベースから COD ライセンスキーを強制的に削除したが、そのライセンスキーに関連付けられていた COD CPU がまだ使用中である場合に、このライセンス違反が発生することがあります。

▼ ドメインごとに COD 使用状況を表示する

- SC ウィンドウで、プラットフォーム管理者またはドメイン管理者としてログインし、以下のように入力します。

```
sc0:sms-user:> showcodusage -p domains -v
```

出力結果には、すべてのドメインの CPU の状態が含まれています。たとえば、次のメッセージが表示されます。

```

sc0:sms-user:> showcodusage -p domains -v
Domains:
=====
Domain/Resource   In Use   Installed   Reserved   Status
-----
A - PROC          0        4           4
   SB4 - PROC     0        4
   SB4/P0                Unused
   SB4/P1                Unused
   SB4/P2                Unused
   SB4/P3                Unused
B - PROC          4        4           4
   SB6 - PROC     4        4
   SB6/P0                Licensed
   SB6/P1                Licensed
   SB6/P2                Licensed
   SB6/P3                Licensed
C - PROC          0        4           0
   SB12 - PROC    0        4
   SB12/P0                Unused
   SB12/P1                Unused
   SB12/P2                Unused
   SB12/P3                Unused
.
.
.

```

表 7-4 では、ドメインごとに表示した COD 資源の情報について説明します。

表 7-4 showcodusage で表示されるドメイン情報

項目	説明
Domain/Resource	各ドメインの COD 資源 (プロセッサ)。未使用プロセッサは、まだドメインに割り当てられていなかった COD CPU です。
In Use	現在ドメインで使用されている COD CPU 数。

表 7-4 showcodusage で表示されるドメイン情報 (続き)

項目	説明
Installed	ドメインに取り付けられている COD CPU 数。
Reserved	ドメインに割り当てられている COD RTU ライセンス数。
Status	次の CPU の状態のいずれかになります。 <ul style="list-style-type: none">• Licensed - COD CPU は COD RTU ライセンスを持っています。• Unused - COD CPU は使用されていません。• Unlicensed - COD CPU は COD RTU ライセンスを取得できず、使用されていません。

▼ 資源とドメインごとに COD 使用状況を表示する

- SC ウィンドウで、プラットフォーム管理者としてログインし、以下のように入力します。

```
sc0:sms-user:> showcodusage -v
```

表示される情報には、資源とドメインそれぞれについての使用状況情報が含まれています。

たとえば、次のメッセージが表示されます。

```
sc0:sms-user:> showcodusage -v
Resource:
=====
Resource   In Use   Installed   Licensed   Status
-----
PROC           4           4           16   OK: 12 available
Domains:
=====
Domain/Resource   In Use   Installed   Reserved   Status
-----
A - PROC           0           0           0
B - PROC           0           0           0
  SB6 - PROC       0           0
    SB6/P0                Unused
    SB6/P1                Unused
    SB6/P2                Unused
    SB6/P3                Unused
C - PROC           0           0           0
  SB12 - PROC      0           0
    SB12/P0                Unused
    SB12/P1                Unused
    SB12/P2                Unused
    SB12/P3                Unused
D - PROC           4           4           0
  SB4 - PROC       4           4
    SB4/P0                Licensed
    SB4/P1                Licensed
    SB4/P2                Licensed
    SB4/P3                Licensed
  SB16 - PROC      4           4
    SB16/P0                Unused
    SB16/P1                Unused
    SB16/P2                Unused
    SB16/P3                Unused
E - PROC           0           0           0
F - PROC           0           0           0
G - PROC           0           0           0
.
.
.
R - PROC           0           0           0
Unused - PROC      0           0           12
```

構成解除された COD CPU とライセンスを受けていない COD CPU

COD システムボードを使用するドメインを起動した場合、COD RTU ライセンスを取得できない COD CPU は、構成解除された CPU、またはライセンスのない CPU として表示されます。次の項目を表示すると、構成解除された COD CPU やライセンスのない COD CPU を判定することができます。

■ setkeyswitch on 操作でのメッセージの出力

COD RTU ライセンスを取得しなかった COD CPU は、構成解除された (deconfigured) CPU として特定されます。COD システムボード上の COD CPU がすべて構成解除されている場合は、setkeyswitch on 操作が COD システムボードを使用不可にし、setkeyswitch on 操作も次の例に示すように失敗します。

```
sc0:sms-user:> setkeyswitch -d A on
.
.
.
Acquiring licenses for all good processors...
Proc SB03/P0    deconfigured: no license available.
Proc SB03/P2    deconfigured: no license available.
Proc SB03/P3    deconfigured: no license available.
Proc SB03/P1    deconfigured: no license available.
No minimum system left after Check CPU licenses (for COD)! Bailing out!
.
.
.
Deconfigure Slot0: 00008
Deconfigure EXB:  00008
POST (level=16, verbose=40, -H3.0) execution time 3:08
# SMI Sun Fire 15K POST log closed Fri Jul 26 15:15:53 2002
```

■ showcodusage(1M) コマンドの出力

ドメインの COD CPU の状態を取得する場合は、160 ページの「ドメインごとに COD 使用状況を表示する」を参照してください。Unlicensed 状態は、COD CPU に対する COD RTU ライセンスが取得できず、その COD CPU はドメインで使用されていないことを示しています。

その他の COD 情報

表 7-5 では、その他のシステムコントローラコマンドを使用して取得できる COD の構成とイベントの情報をまとめています。これらのコマンドについての詳細は、『System Management Services (SMS) 1.6 リファレンスマニュアル』の説明を参照してください。

表 7-5 COD のコンポーネント、構成、およびイベント情報の取得

コマンド	表示される情報
showlogs	ライセンス違反やヘッドルームの使用可能への切り替えなど、プラットフォームコンソールにログとして記録される COD イベントに関する情報
showplatform -p cod	現在の COD 資源構成 <ul style="list-style-type: none">• 使用中のインスタントアクセス CPU (ヘッドルーム) 数• ドメインの RTU ライセンス予約 シャーシのホスト ID

第8章

ドメイン制御

この章では、ドメインソフトウェアとサーバーハードウェアを制御する機能について説明します。制御機能は、管理者の判断で実行できます。SMS でも、制御機能によって ASR (Automatic System Recovery : 自動システム回復) が利用できるため便利です。

ドメイン制御機能では、ドメイン上で実行されるソフトウェアを制御します。これには、ドメインを起動したり中断したりできる機能が含まれます。ドメイン制御機能は、ドメイン管理者だけが実行できます。

この章では、以下の項目を説明します。

- 167 ページの「ドメインの起動」
- 173 ページの「ハードウェア制御」

ドメインの起動

ここでは、ドメイン内で Solaris OS を起動する際のさまざまな側面について説明します。

setkeyswitch(1M) コマンドは、ドメインの起動を開始および処理する役割を果たします。このコマンドは、必要に応じてドメインハードウェアの電源を投入し、POST を起動して論理ドメイン内のハードウェアを Sun Fire ハイエンドシステムの物理ハードウェアドメインでテストおよび構成します。また、ドメイン上で Solaris OS を起動するために必要な OpenBoot PROM をダウンロードして実行します。

仮想キースイッチが適切に設定されたドメインだけが、起動制御の対象となります。116 ページの「仮想キースイッチ」を参照してください。

OpenBoot PROM の起動パラメータは、ドメインの仮想 NVRAM に格納されます。osd(1M) コマンドは OpenBoot PROM に対して起動パラメータの値を提供し、OpenBoot PROM は指定されたとおりにドメインの起動を実行します。

特定のパラメータ、特にドメインの起動に失敗したときに OpenBoot PROM 自体からは調整できないパラメータは、setobpparams(1M) によって設定し、次の起動試行の際に有効にすることができます。

キースイッチ制御

ドメインのキースイッチ制御 (116 ページの「仮想キースイッチ」を参照) では、ドメインの起動を手動で開始します。

setkeyswitch コマンドは、正しく構成されたドメインのキースイッチ制御が off または standby の位置から、いずれかの on の位置に移動されたときに、そのドメインを起動します。

setobpparams(1M) コマンドは、手動で開始した (キースイッチ制御) ドメインの起動処理を OpenBoot PROM で停止できる手段を提供します。詳細は、120 ページの「OpenBoot PROM 変数の設定」および setobpparams のマニュアルページを参照してください。

電源制御

次に示すコンポーネントの電源は、poweron および poweroff コマンドを使用して制御できます。

- ファントレイ
- センタープレーンサポートボード
- 拡張ボード
- システムボード
- 標準 PCI ボード
- ホットプラグ可能な PCI および PCI+ ボード
- MaxCPU ボード
- wPCI ボード
- システムコントローラ (スペアのみ、poweroff または resetsc を使用してスペアの電源を投入できる)

▼ システムボードの電源をコマンドラインから投入および切断する

プラットフォーム管理者は、システム全体の電源を制御でき、*location* オプションを使用せずにこれらのコマンドを実行できます。ドメイン管理者は、それぞれのドメインに割り当てられたシステムボードの電源を制御できます。ドメインの権限だけを持つユーザーは、*location* オプションを使用する必要があります。

- システムコンポーネントの電源を投入するには、次のコマンドを入力します。

```
sc0:sms-user:> poweron location
```

location は、電源を投入するシステムコンポーネントの場所であり、ユーザーがドメイン管理者である場合は、そのユーザーが特権を持つコンポーネントの場所です。

詳細は、`poweron(1M)` のマニュアルページを参照してください。

- システムコンポーネントの電源を切断するには、次のコマンドを入力します。

```
sc0:sms-user:> poweroff location
```

location は、電源を切断するシステムコンポーネントの場所であり、ユーザーがドメイン管理者である場合は、そのユーザーが特権を持つコンポーネントの場所です。

警告メッセージの後で、*y* または *n* のいずれかを入力します。

```
!!!WARNING!!!WARNING!!!WARNING!!!WARNING!!!WARNING!!!  
!!!WARNING!!!WARNING!!!WARNING!!!WARNING!!!WARNING!!!  
  
This will trip the breakers on PS at PS5, which must be turned on  
manually!  
  
Are you sure you want to continue to power off this component?  
(yes/no)? y
```



注意 – コンポーネントの電源を切断する前に、`DR` を使用してそのコンポーネントをドメインから削除してください。事前にコンポーネントをドメインから削除せずに電源を切断すると、ドメイン停止 (`DStop`) が発生します。コンポーネントを交換するためにその電源を切断する場合は、`poweroff(1M)` コマンドを使用します。ドメインからコンポーネントを削除せずに、ブレーカを使用してそのコンポーネントの電源を切断することはしないでください。このような操作も `DStop` を引き起こす可能性があります。ドメインからコンポーネントを削除したあとであれば、ブレーカを使用してコンポーネントの電源を切断しても `DStop` は発生しません。

詳細は、`poweroff(1M)` のマニュアルページを参照してください。

ドメインで OS が活発に動作しているときにシステムの電源を切断しようとする、コマンドは失敗し、ウィンドウのメッセージパネルにメッセージが表示されます。その場合は、動作中のドメインに対して `setkeyswitch domain-id standby` コマンドを実行すると、プロセッサを正常に停止できます。シャットダウンが完了した時点で、コマンドを再発行して電源を切断できます。

停電のためプラットフォームの電源が失われる場合は、`pcd` によって、電源が失われる前の各ドメインの最後の状態が記録および保存されます。

▼ 電源障害から回復する

SC でのみ電源が失われた場合、SC の電源を投入してください。Sun Fire ハイエンドシステムのドメインは、1 つの SC の電源が失われても影響を受けません。SC とドメインの両方の電源が失われた場合は、以下の手順で電源障害から回復してください。スイッチの場所については、『Sun Fire 15K/12K システムサイト計画の手引き』を参照してください。



注意 – SMS を停止せずに両方の SC の電源を切断すると、ドメインがクラッシュします。

1. Sun Fire ハイエンドシステムのバルク電源と、SC の電源スイッチを手動で切断します。
2. 電源が復元したら、Sun Fire ハイエンドシステムのバルク電源を手動で投入します。
3. SC の電源を手動で投入します。

これによって SC が起動し、SMS デーモンが開始されます。SC プラットフォームのメッセージファイルを参照して、SMS デーモンの完了をチェックしてください。

回復プロセスが完了するのを待ちます。電源が投入されて Solaris OS が実行されているドメインは、OS の実行状態に戻ります。OpenBoot PROM のドメインは、やがて OpenBoot PROM の実行状態に戻ります。

回復プロセスは、SMS の操作が実行される前に完了させる必要があります。ドメインのメッセージファイルをモニターして、回復プロセスが完了したかどうかを判断することができます。

ドメインの要求による再起動

SMS はドメイン管理ソフトウェア (Solaris ソフトウェアまたは `dsmd`) からの要求に応じてドメインを再起動します。ドメインソフトウェアは、以下の状況で再起動サービスを要求します。

- ユーザーが再起動要求を実行した場合。たとえば、Solaris の `reboot(1M)` コマンドまたは `OpenBoot PROM` の起動コマンド `reset-all` など。
- Solaris ソフトウェアがパニック状態になった場合。
- CPU で検出された `RED_mode` やウオッチドッグリセットの状態をトラップした場合。

ASR (Automatic System Recovery: 自動システム回復)

ASR (Automatic System Recovery : 自動システム回復) は、ソフトウェアまたはハードウェアの障害や許容できない環境条件によって、1つまたは複数のドメインがアクティブでない状態に陥った後、システムを復元して正しく構成されたドメインを実行できるようにするための手順で構成されます。

SMS ソフトウェアは、ASR の一部としてソフトウェアから発行された再起動要求をサポートしています。クラッシュしたドメインは、すべて `dsmd` によって自動的に再起動されます。

ASR が必要な状況は、ドメインをクラッシュさせる障害 (パニックなど) が検出された際に、ドメインソフトウェアによってドメインの起動が要求される場合です。

ドメインソフトウェアのハングの検出など、217 ページの「Solaris ソフトウェアハングイベント」で説明されているような他の状況もあります。その場合、SMS は回復プロセスの一部としてドメインの起動を実行します。

`dsmd` ソフトウェアは `OpenBoot PROM` パラメータの `auto-boot?` を無視します。`auto-boot?` は、サービスプロセッサのないシステム上で、システムが電源投入リセットの状況で自動的に再起動するのを回避できるパラメータです。`dsmd` はキースイッチ制御を無視しません。キースイッチが `off` または `standby` に設定されている場合、キースイッチ設定はドメインが ASR の再起動アクションの対象かどうかを判断する際に考慮されます。

ドメインの再起動

一般に、ドメインの高速再起動は以下のような状況で可能です。

- 最後の起動以降、ハードウェアに起因する深刻なエラーがない場合。
- SMS が既存のドメイン資源の信頼性を疑問視するような障害が発生していない場合。

SMS はハードウェアのモニタリングやエラーの検出および応答を行うため、SMS は最後の起動以降に記録されたハードウェアエラーに基づいて、高速再起動を要求するかどうかを決定します。

POST は、指定された入力の数に基づいてハードウェア構成を制御しますが、ブラックリストのデータに関係なく (174 ページの「ブラックリストの編集」を参照)、ハードウェア構成が変更されているかどうかを判断し、高速再起動を回避します。システム管理で高速再起動が要求された場合、POST は現在の入力によって示されるハードウェア構成が、最後の起動で使用されたハードウェア構成と一致しているかどうかを確認します。一致していない場合、POST は高速 POST 処理に失敗します。システム管理ソフトウェアでは、フルテスト (低速) のドメイン起動を要求して、この種の POST 障害から回復します。

Sun Fire ハイエンドシステム管理ソフトウェアは、制御可能なドメインの起動プロセスの一部に費やされる時間を最少限に抑えます。

ドメインの中止またはリセット

ドメインソフトウェアを中止したり、ドメインソフトウェアまたはハードウェアに対してリセットを発行する必要がある、特定のエラー状況がドメインで発生する場合があります。この節では、dsmd によって提供されるドメインの中止およびリセット機能について説明します。

dsmd ソフトウェアは、ドメインの Solaris OS を中止し、ドメインをパニック状態にしてコアイメージを取得することを要求するためのソフトウェア主導のメカニズムを提供します。ユーザーの操作は必要ありません。

SMS には `reset(1M)` コマンドが用意されており、ユーザーはこのコマンドを使用してドメインソフトウェアを中止し、ドメインハードウェアに対してリセットを実行できます。

`reset` コマンドが実行されると、OpenBoot PROM に制御が渡されます。ユーザーインタフェースで `reset` コマンドが実行された場合、OpenBoot PROM はそのデフォルト構成を使用して、Solaris 環境に対してドメインを起動するかどうかを決定します。dsmd によって `reset` コマンドが実行された場合、OpenBoot PROM は Solaris OS に対してドメインを強制的に起動するパラメータを提供します。

`reset` コマンドは通常、指定されたドメインのすべての CPU ポートに対して信号を送信します。これはハードリセットであり、ハードウェアをクリーンな状態にします。ただし `-x` オプションを使用すると、`reset` コマンドは指定されたドメインのプロセッサに対して XIR 信号を送信できます。これはソフトウェアで行われ、ソフト

リセットと見なされます。仮想キースイッチが安全位置にある場合は、エラーメッセージが発行されます。デフォルトでは、オプションの "Are you sure?" プロンプトが表示されます。たとえば、次のメッセージが表示されます。

```
sc0:sms-user:> reset -d C
Do you want to send RESET to domain C? [y|n]:y
RESET to processor 4.1.0 initiated.
RESET to processor 4.1.1 initiated.
RESET initiated to all processors for domain: C
```

詳細は、`reset` のマニュアルページを参照してください。

メインまたはスペアの SC をリセットする方法については、183 ページの「SC のリセットおよび再起動」を参照してください。

ホットプラグ可能ユニット (HPU) の電源投入のリセットが行なわれたときに正しい状態を反映させるため、LED を備えた HPU のインジケータ LED が、SMS ソフトウェアによって点灯または消灯されます。

ハードウェア制御

ハードウェア制御は、プラットフォームハードウェアの構成や制御を行う機能です。いくつかの機能はドメイン上で実行されます。

電源投入時自己診断 (POST)

システム管理サービスソフトウェアは、POST を 2 つの状況で起動します。

1. POST はドメインの起動時に実行され、そのドメインで利用可能なすべてのハードウェア機能をテストおよび構成します。

POST はセルフテストで問題が発見されたハードウェアコンポーネントをすべて除去し、正しく動作するハードウェアを使用して起動可能なドメインの構築を試みます。

POST は、障害の分析に役立つ詳細な診断機能を提供します。ハードウェアの障害が原因だと明示されずにドメインが再起動される場合は、POST でドメイン構成の確認のみを行い、テストは行わないことを要求できます。

2. システムボードをドメインに追加する DR 操作の前に、POST が起動されてシステムボードのコンポーネントのテストおよび構成が実行されます。

POST によって候補のシステムボードが機能することが示されると、DR 操作でシステムボードを物理 (ハードウェア) ドメインに安全に組み込むことができます。

POST は通常は自動的に実行されますが、POST の自動実行に影響する表示可能なユーザーインターフェースがあります。

- ブラックリストファイルを使用して、POST でハードウェア構成から除外したいコンポーネントを追加または削除できます。これらの編集可能なファイルについては、174 ページの「ブラックリストの編集」で説明しています。

これによって、システムボードなどの DCU 上で動作する標準のドメイン構成インターフェースよりも、ドメインで使用されるハードウェアコンポーネントを綿密に制御できます。

- `setkeyswitch` コマンドは、POST を起動してドメインのテストおよび構成を実行します。ドメインを起動する際は、通常および最大の診断テストレベルの設定が利用できます。
- `addboard` および `moveboard` コマンドは、POST を起動してシステムボードのテストおよび構成を実行し、動作中の Solaris ドメインにそのシステムボードを追加するための DR 操作を支援します。
- POST で、LED を備えた FRU のコンポーネントに問題が発見されると、FRU の障害 LED が点灯します。

ブラックリストの編集

SMS は 3 つのブラックリストをサポートしています。具体的には、プラットフォーム用、ドメイン用、そして内部の ASR (自動システム回復) 用のブラックリストです。

プラットフォームおよびドメインのブラックリスト

編集可能なブラックリストファイルでは、POST によって使用不可であると見なされる特定のハードウェア資源を指定します。ブラックリストで指定されたハードウェア資源は、ドメインの相互接続で調査、テスト、または構成されません。

通常、これらのブラックリストファイルは空であり、存在しなくてもかまいません。

ここでは、ブラックリスト機能は資源管理の目的で使用されます。

ブラックリストによって、実在するすべてのハードウェアよりも少ないシステムを構成できます。ブラックリストの用途としては、ベンチマークを行う場合や、メモリーの使用を制限して DR でのボード切り離しを高速化する場合、およびトラブルシューティングで構成を検証する場合などがあります。

Sun Fire ハイエンドシステムの POST では、プラットフォーム用とドメイン用に、次に示す 2 つの編集可能で標準的なブラックリストファイルをサポートしています。


```
/etc/opt/SUNWSMS/config/platform/blacklist
```

```
/etc/opt/SUNWSMS/config/domain-id/blacklist
```

2つのファイルは論理的に結合していると見なされます。

注 – ブラックリストファイルでは、物理的な場所に基づいて資源を指定します。コンポーネントを物理的に移動した場合は、対応するブラックリストのエントリもすべて変更する必要があります。

ブラックリストファイルでは、位置指定などを行うことで、ブラックリストに登録されるコンポーネントを論理的に指定します。また、ブラックリストは特定のコンポーネントに伴って移動せず、ホットプラグ処理を通じてそのコンポーネントの位置に残ります。

▼ コンポーネントをブラックリストに登録する

1. SC にログインします。

ブラックリストファイルを編集するには、プラットフォーム管理者、ドメイン管理者、またはドメイン構成者の特権が必要です。

2. 次のコマンドを入力します。

```
sc0:sms-user:> disablecomponent [-d domain-indicator] location
```

ここで次の点に留意します。

-d domain-indicator 次のいずれかを使ってドメインを指定します。
domain-id - ドメインの ID。有効な *domain-id* は、A ~ R で、
大文字と小文字は区別されません。
domain-tag - addtag(1M) を使用してドメインに割り当てた名
前。

location 以下の項目で構成されるコンポーネント位置のリスト。

```
board-loc/proc/bank/logical-bank  
board-loc/proc/bank/all-dimms-on-that-bank  
board-loc/proc/bank/all-banks-on-that-proc  
board-loc/proc/bank/all-banks-on-that-board  
board-loc/proc  
board-loc/cassette  
board-loc/bus  
board-loc/paroli-link
```

domain-indicator を指定しない場合は、プラットフォームのブラックリストが編集されます。コンポーネントの場所は、すべてスラッシュで区切って指定します。
location 形式は、オプションであり、特定の位置にあるボード上の特定のコンポーネントを指定するために使用されます。

location 引数が複数の場合は、スペースで区切ります。

表 8-1 Sun Fire ハイエンドサーバーに有効な *location*

場所	Sun Fire 15K/E25K で有効な形式	Sun Fire 12K/E20K で有効な形式
<i>board-loc</i>	SB(0...17) IO(0...17) CS(0 1) EX (0...17)	SB(0...8) IO(0...8) CS(0 1) EX (0...8)
プロセッサ / プロセッサペア (<i>proc</i>)	P(0...3) PP(0 1)	P(0...3) PP(0 1)
<i>bank</i>	B	B
<i>logical-bank</i>	L(0 1)	L(0 1)
<i>all-dimms-on-that-bank</i>	D	D
<i>all-banks-on-that-proc</i>	B	B
<i>all-banks-on-that-board</i>	B	B
<i>HsPCI cassette</i>	C(3 5)V(0 1)	C(3 5)V(0 1)
<i>HsPCI+ cassette</i>	C3V(0 1 2) および C5V0	C3V(0 1 2) および C5V0
<i>bus</i>	ABUS DBUS RBUS (0 1)	ABUS DBUS RBUS (0 1)
<i>paroli-link</i>	PAR(0 1)	PAR(0 1)

プロセッサ位置は、単一のプロセッサまたはプロセッサペアを示します。システムボード上には 4 つのプロセッサが存在します。ボード上のプロセッサペアは、*procs* 0 と 1、および *procs* 2 と 3 です。

注 – プロセッサペアの一方の CPU/メモリープロセッサをブラックリストに登録すると、両方のプロセッサが使用されなくなります。

MaxCPU には、*proc* 0 および 1 の 2 つのプロセッサと、*proc* ペア (PP0) が 1 つだけあります。このボードの場所として PP1 を使用すると、*disablecomponent* は終了してエラーメッセージを表示します。

HsPCI および HsPCI+ アセンブリには、ホットプラグが可能なカセットが内蔵されています。

バス位置には、アドレス、データおよび応答の 3 つがあります。

注 – システムコントローラのセンタープレーンサポートボードまたはバスの無効化に *disablecomponents* コマンドを使用しないでください。

▼ ブラックリストからコンポーネントを削除する

1. SC にログインします。
2. 次のコマンドを入力します。

```
sc0:sms-user:> enablecomponent [-d domain-indicator] location
```

ここで次の点に留意します。

-d domain-indicator 次のいずれかを使ってドメインを指定します。
domain-id - ドメインの ID。有効な *domain-id* は、A ~ R で、大文字と小文字は区別されません。
domain-tag - `addtag(1M)` を使用してドメインに割り当てた名前。

location 次の項目で構成されるコンポーネント位置のリスト。

```
board-loc/proc/bank/logical-bank  
board-loc/proc/bank/all-dimms-on-that-bank  
board-loc/proc/bank/all-banks-on-that-proc  
board-loc/proc/bank/all-banks-on-that-board  
board-loc/proc  
board-loc/cassette  
board-loc/bus  
board-loc/paroli-link
```

domain-indicator を指定しない場合は、プラットフォームのブラックリストが編集されます。コンポーネントの場所は、すべてスラッシュで区切って指定します。
location 形式は、オプションであり、特定の位置にあるボード上の特定のコンポーネントを指定するために使用されます。

location 引数が複数の場合は、スペースで区切ります。

表 8-2 Sun Fire ハイエンドサーバーに有効な *location*

場所	Sun Fire 15K/E25K で有効な形式	Sun Fire 12K/E20K で有効な形式
<i>board-loc</i>	SB(0...17) IO(0...17) CS(0 1) EX (0...17)	SB(0...8) IO(0...8) CS(0 1) EX (0...8)
プロセッサ / プロセッサペア (<i>proc</i>)	P(0...3) PP(0 1)	P(0...3) PP(0 1)
<i>bank</i>	B	B
<i>logical-bank</i>	L(0 1)	L(0 1)
<i>all-dimms-on-that-bank</i>	D	D
<i>all-banks-on-that-proc</i>	B	B
<i>all-banks-on-that-board</i>	B	B
<i>HsPCI cassette</i>	C(3 5)V(0 1)	C(3 5)V(0 1)
<i>HsPCI+ cassette</i>	C3V(0 1 2) および C5V0	C3V(0 1 2) および C5V0
<i>bus</i>	ABUS DBUS RBUS (0 1)	ABUS DBUS RBUS (0 1)
<i>paroli-link</i>	PAR(0 1)	PAR(0 1)

プロセッサ位置は、単一のプロセッサまたはプロセッサペアを示します。CPU/メモリーボード上には 4 つのプロセッサが存在します。ボード上のプロセッサペアは、procs 0 と 1、および procs 2 と 3 です。

注 – プロセッサペアの一方の CPU またはメモリープロセッサをブラックリストに登録すると、どちらのプロセッサも使用されなくなります。

MaxCPU には、procs 0 と 1、および 1 つのみの *proc* ペア (PP0) の 2 つのプロセッサがあります。このボードの場所として PP1 を使用すると、*disable component* コマンドは終了し、エラーメッセージを表示します。

HsPCI および HsPCI+ アセンブリには、ホットプラグが可能なカセットが内蔵されています。

バスの場所は、アドレス、データ、応答の 3 つがあります。

詳細は、*enablecomponent(1M)* および *disablecomponent(1M)* のマニュアルページを参照してください。

ASR ブラックリスト

障害が繰り返し(ときどき)発生するハードウェアは、さまざまな理由で以降のドメイン構成から除外する必要があります。このような障害は、コンポーネントを物理的に交換するまで、ときどき発生する可能性があります。障害のあるコンポーネントは、CPU ボード上の1つのプロセッサなど、サブコンポーネントである場合もあります。そのコンポーネントを交換するまで、その他のコンポーネントのサービスについては電源を切断して運用を中止したくないと考えるでしょう。ハードウェアが損傷している場合は、POST を実行するたびにその障害を検出するのは時間の浪費です。障害がときどき発生する場合は、POST 実行時にその障害を回避せず、OS が実行されている場合のみエラーにするとよいでしょう。

この障害を回避するには、`esmd` コマンドで別の ASR ブラックリストファイルを作成および編集します。環境条件により電源が切断されているコンポーネントは自動的にリストに登録され、POST から除外されます。`poweron`、`setkeyswitch`、`addboard`、および `moveboard` の各コマンドは、除外するコンポーネントに関して ASR ブラックリストを照会します。`poweron` 以外の各コマンドを実行すると、警告メッセージが表示されます。`poweron` では、警告メッセージではなく、コンポーネントの電源投入を継続するか中止するかを問い合わせるメッセージが表示されます。詳細は、`enablecomponent(1M)`、`disablecomponent(1M)` および `showcomponent(1M)` のマニュアルページを参照してください。

電源制御

メインの SC は、Sun Fire ハイエンドシステムのラックに収められた以下のコンポーネントの電源を制御します。

- Sun Fire ハイエンドシステムボード
- Sun Fire ハイエンドシステムの HsPCI I/O ボードにある HsPCI アダプタのスロット
- Sun Fire ハイエンドシステムの HsPCI+ I/O ボードにある HsPCI+ アダプタのスロット
- システムコントローラ (電源切断のみ)
- センタープレーンサポートボード
- wPCI ボード
- 拡張ボード
- 48V電源
- AC バルク電源モジュール
- ファントレイ

Sun Fire ハイエンドシステムの I/O ラックでの電源制御については、183 ページの「HPU の LED」を参照してください。

SMS は、Sun Fire ハイエンドシステムの HsPCI I/O ボード内の HPCI アダプタスロットの電源の投入または切断を要求する `rcfgadm(1M)` コマンドを提供することによって、ドメインの Solaris コマンドインタフェース (`cfgadm(1M)`) をサポートしています。詳細は、`rcfgadm` のマニュアルページを参照してください。

116 ページの「仮想キースイッチ」で説明されているキースイッチ制御インタフェースの `setkeyswitch` コマンドを使用すると、ドメインに割り当てられたハードウェアの電源をユーザーが投入または切断できます。

電源操作は、すべて電源制御ソフトウェアによってログに記録されます。

電源制御ソフトウェアは、コンポーネントの電源を投入または切断するためのすべてのハードウェア要件に従います。たとえば、SMS はコンポーネントの電源を投入する前に、適切な電源が利用可能かどうかをチェックします。電源制御インタフェースは、ハードウェア要件に違反している場合にはユーザー指定による電源投入または切断の操作を行いません。ハードウェア要件またはハードウェア推奨手順に従わずに実行された電源操作は、メッセージログに記録されます。

デフォルトでは、電源制御ソフトウェアはソフトウェアの実行に影響する電源操作を拒否します。電源制御ユーザーインタフェースには、このデフォルト動作を変更して、実行中のソフトウェアをクラッシュさせる危険を冒しても、電源操作を強制的に完了させる方法があります。このような電源操作の強制変更は、メッセージログに記録されます。

183 ページの「HPU の LED」で説明されているように、SMS は LED を備えた HPU のインジケータ LED を点灯または消灯して、HPU の電源が投入または切断された場合に正確な状態を反映させます。

ファンの制御

`esmd` コマンドは、Sun Fire ハイエンドシステムのファンの速度を制御します。一般に、ファンの速度はノイズレベルを最小に抑えながら適切に冷却を行えるもっとも遅い速度に設定されます。

ホットプラグ操作

ホットプラグとは、電源が投入され、1 つ以上のドメインが活発に動作しているプラットフォームで、それらのドメインに影響を与えずにボードを物理的に挿入または取り外すことができる機能を指します。ホットプラグ操作の際には、ボードはすべてのドメインから切り離されます。

ホットプラグ可能なハードウェアコンポーネントは、ホットプラグ可能ユニット (HPU) と呼ばれます。HPU を安全に取り外すことができる場合は、HPU 上の取り外し可能インジケータ LED が点灯します。取り外し可能 LED の詳細は、183 ページの「HPU の LED」を参照してください。ボード存在レジスタは、HPU が存在するかどうかを示し、HPU の着脱を感知します。

Sun Fire ハイエンドシステムの HsPCI および HsPCI+ I/O アセンブリには、HsPCI および HsPCI+ I/O アセンブリが取り付けられたスロットに関連する取り外し可能インジケータ LED が装備されています。各スロットは、スロットの電源を制御するホットプラグコントローラを備えており、スロット内のアダプタの存在を検出できます。ただし、SMS が他の Sun Fire ハイエンドシステムの HPU をサポートするのは異なり、HsPCI および HsPCI+ I/O アセンブリのホットプラグを制御するソフトウェアは、ドメイン上の Solaris OS の一部です。

SMS を使用すると、ユーザーがアダプタスロットの電源を投入および切断できます。

SMS ソフトウェアは、ドメインから実行可能なソフトウェアインタフェースを提供し、I/O ボード上のアダプタスロットに関連するハードウェアデバイスを制御します。

注 – この節のこれ以降のホットプラグの説明目的に関して、HPU にはホットプラグ可能な I/O アダプタは含まれていません。

SMS ソフトウェアは、Sun Fire ハイエンドシステムのラック内にあるすべての HPU のホットプラグサービスを可能にするサポートを必要に応じて提供します。

HPU がすべてのドメインから切り離されると、ホットプラグ操作に必要なソフトウェアサポートは電源切断の制御のみになります。

動的再構成 (DR) により、ドメインから DCU (システムボード) が切り離されます。

取り外し

HPU が取り外されると、HPU の存在インジケータによってその不在が検出され、203 ページの「ハードウェア構成」で説明されているようにハードウェア構成ステータスが変更されます。

ホットアンプラグの際に予想されるユーザーの対話モードは次のとおりです。

取り外す HPU を直接操作します。

HPU のインジケータ LED に、HPU が取り外し可能でないと表示されている場合は、poweroff コマンドを使用して HPU の電源切断を要求します。

電源切断機能で HPU がドメインによって使用されていることが検出されると、電源切断機能はエラーとなり、まず DR を使用して HPU のアクティブな使用を解除する必要がありますが示されます。

詳細については、『System Management Services (SMS) 1.6 Dynamic Reconfiguration ユーザーマニュアル』を参照してください。

取り付け

新たに挿入された HPU の存在が検出され、203 ページの「ハードウェア構成」で説明しているようにハードウェア構成ステータスの変更として報告されます。

SC のリセットおよび再起動

SC はメインとスペアの SC に対してソフトウェア処理型のリセットをサポートし、システムコントローラの外付けのリセットボタンと同様の機能を提供します。SC は、主にフェイルオーバーの後にリセットされます。メインの SC ソフトウェアがスペアの SC (存在する場合) をリセットしたり、その逆を行うことも可能です。SC は自身をリセットすることはできません。

▼ メインまたはスペアの SC をリセットする

`resetsc (1M)` コマンドは、他方の SC にリセット信号を送信します。他の SC が存在しない場合、`resetsc` コマンドはエラーになって終了します。

- 次のコマンドを入力します。

```
sc0:sms-user:> resetsc
"About to reset other SC. Are you sure you want to continue?" (y
or [n])? y
```

詳細は、`resetsc` のマニュアルページを参照してください。

HPU の LED

LED は、ホットプラグ可能ユニット (HPU) のステータスを反映します。LED は 3 つのグループで構成されます。

- 動作インジケータ LED は、電源がオンの場合に点灯します。
- 取り外し可能 LED は、HPU が取り外し可能な場合に点灯します。
- 障害 LED は、HPU のハードウェアエラーが検出された場合に点灯します。

この節では、SMS ソフトウェアが準拠する HPU の LED 制御のポリシーについて説明します。

システムコントローラを除くすべての Sun Fire ハイエンドシステムの HPU は、メインのシステムコントローラで実行されている SMS ソフトウェアの制御により、電源が投入されテストされます。

特に電源投入時リセットのときの LED の初期状態は、電源投入時リセットのときに POST が自動的に実行されることを前提として設計されています。この前提条件を満たす Sun Fire ハイエンドシステムの HPU は、システムコントローラだけです。システムコントローラの電源が投入されると、プロセッサは PROM から SC-POST コードの実行を開始します。

その他のすべての HPU は、POST によってテストされるものと、SMS ソフトウェアによってテスト (または監視) されるものがあります。通常は電源投入後すぐにテストが実行されますが、必ずしもそうならない場合もあります。

さらに、一方のドメインから他方のドメインに動的に再構成される HPU の電源投入の際には、POST を何度も実行することが可能です。POST と SMS の両方で同じ物理 HPU の障害を検出することも可能です。両者の違いは、システムコントローラと他の Sun Fire ハイエンドシステムの HPU との間の電源やテストの制御で、それらの管理に対するポリシーが異なります。

システムコントローラは、次の状態を示す、3 組の HPU の LED を提供します。

- SC 全体の状態
- CP1500 または CP2140 スロットの状態
- SC スペアスロットの状態

Sun Fire ハイエンドシステムのラックに電源が投入されると、システムコントローラに電源が供給されます。動作インジケータ LED と 取り外し可能インジケータ LED は、ハードウェアによって適切に初期化されます。障害を正確に反映し、SC-POST の実行を妨げる問題が存在することがわかるように、3 つの障害 LED がすべて点灯します。

スペアのシステムコントローラの電源が切断されると、SMS ソフトウェアは、スペアのシステムコントローラの動作インジケータ LED を消灯して、取り外し可能インジケータ LED を点灯します。SMS ソフトウェアが実行されているメイン SC の電源が切断されると、SMS ソフトウェアは動作インジケータや取り外し可能 LED を調整できなくなります。

SC-POST は以下の処理を行います。

- SC のテスト完了時に障害が検出されなかった場合、SC-POST は SC 障害 LED を消灯します。
- HPCI スロットのテスト完了時に障害が検出されなかった場合、SC-POST は SC スペアスロット障害 LED を消灯します。
- 制御ボードのテスト完了時に、制御ボードや SC メインスロットまたは SC スペアスロットで障害が検出されなかった場合、SC-POST は SC 障害 LED を消灯します。

SC-OpenBoot PROM ファームウェアおよび SMS ソフトウェアは、ハードウェアエラーを検出すると、システムコントローラ上の該当する障害 LED を点灯します。

システムコントローラ以外の HPU の LED を管理する際は、以下のポリシーが適用されます。

- Sun Fire ハイエンドシステムのラックに収められた、LED を備えたすべての非 SC HPU に関して、SMS は HPU に電源が供給されたときに動作インジケータ LED が常時点灯することを保証します。
- Sun Fire ハイエンドシステム内に収められた、LED を備えたすべての非 SC HPU に関して、SMS は HPU を安全に取り外すことができる場合のみ取り外し可能インジケータ LED が常時点灯することを保証します。HPU の取り外しや、Sun Fire ハイエンドシステムのハードウェアおよび実行中のソフトウェアの正常かつ連続的な動作を維持する際には、安全上の注意事項が適用されます。

注 – Sun Fire ハイエンドシステムは、HPU の電源投入時または電源投入リセットの実行時に、動作インジケータ LED を適切に点灯し、取り外し可能インジケータ LED を適切に消灯します。

- ほとんどの場合、障害 LED とそれらの表示動作は、SC HPU と非 SC HPU では異なります。

SC では、障害 LED は電源投入時に点灯し、テスト期間中は点灯が維持され、障害が検出されなかった場合は消灯します。

障害は、SC-POST が以降の障害 LED を点灯できた後に検出されます。

SC が POST によってテストされている短時間を除いて、SC の障害 LED は電源投入以降に障害が発生したことを示します。非 SC HPU の場合も同様です (障害 LED の点灯は、電源投入以降に障害が検出されたことを示します)。Sun Fire ハイエンドシステム内の、LED を備えたすべての非 SC HPU については、SMS は電源投入または電源投入リセットが発生した場合に障害インジケータ LED を消灯します。

- POST (173 ページの「電源投入時自己診断 (POST)」を参照) またはハードウェア監視ソフトウェア (219 ページの「環境イベント」、222 ページの「ハードウェアエラーイベント」、および 224 ページの「SC 障害イベント」を参照) によって、SMS が HPU の障害インジケータ LED を常時点灯させるように指示された場合、SMS はそれに従います。183 ページの「HPU の LED」で説明しているように、障害インジケータは、次の電源投入または電源投入リセットによって消灯されるまで点灯します。

第9章

ドメインサービス

Sun Fire ハイエンドシステムハードウェアは、SC と各ドメインを接続するための、内部のプライベートなポイントツーポイントの Ethernet 接続を備えています。このネットワークは管理ネットワーク (Management Network : MAN) と呼ばれ、各ドメインにサポートサービスを提供するために使用されます。この章では、これらのサービスについて説明します。

この章では、以下の項目を説明します。

- 188 ページの「管理ネットワークの概要」
- 193 ページの「管理ネットワークのサービス」

管理ネットワークの概要

管理ネットワーク (MAN) 機能は、SC と各ドメインとのプライベートなポイントツーポイントのネットワーク接続を管理します。あるドメイン宛てのパケットは、SC と他のドメイン (図 9-1) とのネットワーク接続ではルーティングできません。

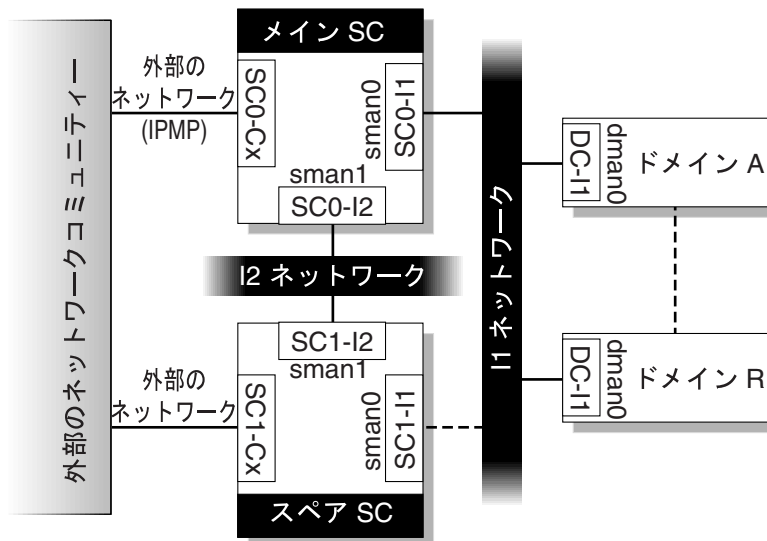


図 9-1 管理ネットワークの概要

I1 ネットワーク

MAN をサポートするために Sun Fire ハイエンドシステムのシャーシに組み込まれたハードウェアは複雑です。このハードウェアでは、各 SC に 18 個のネットワークインタフェースカード (NIC) が搭載されています。これらの NIC は、Sun Fire 15K システムでは 18 個の拡張 I/O スロットに、Sun Fire 12K システムでは 9 個の拡張 I/O スロットにそれぞれ装着された NIC に、ポイントツーポイント形式で接続されています。この設計により、SC と DSD とのポイントツーポイントの Ethernet リンクの数、その DSD で構成された I/O ボードの数によって異なります。SC の各 NIC は、I/O ボード上のハブや NIC に接続されています。NIC は I/O ボードに内蔵されている 1 つの部品であり、独立したアダプタカードではありません。同様に、Ethernet ハブも I/O ボード上に配置されています。このインテリジェントハブは、統計情報を収集できます。

これらのポイントツーポイントのリンクは、総称して I1 ネットワークと呼ばれるます。任意のドメインに複数の I/O ボードを配置できるため、SC からドメインへの複数の冗長ネットワーク接続が可能です。図 9-2 は、Sun Fire E25K/15K のネットワークの概要を示しています。

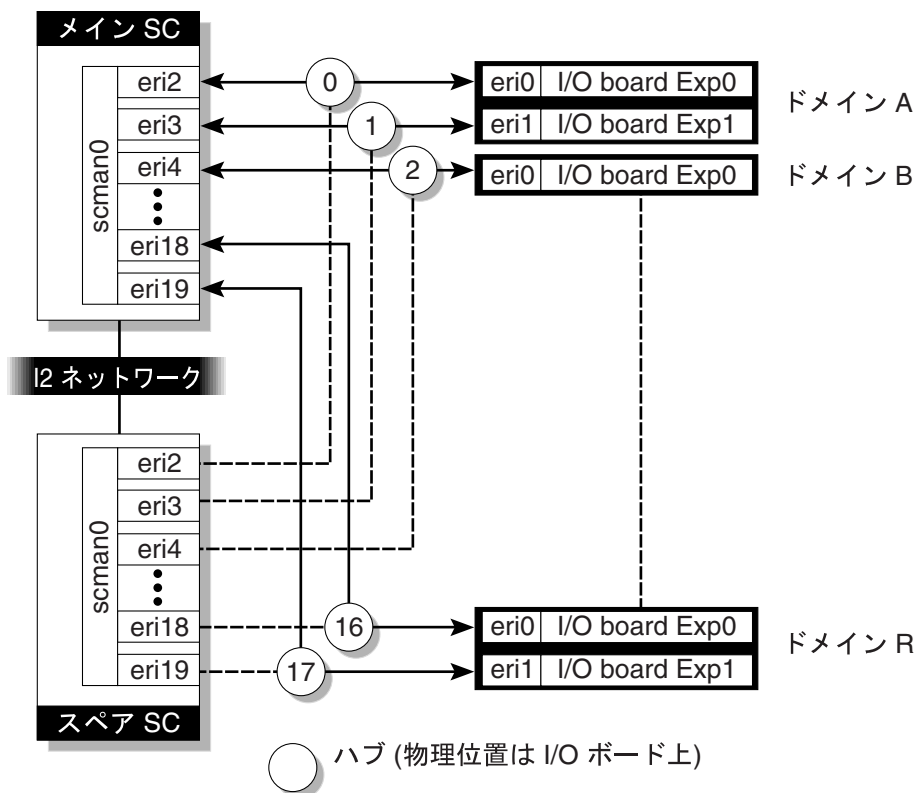


図 9-2 Sun Fire E25K/15K の I1 ネットワークの概要

注 - I1 MAN ネットワークはプライベートなネットワークであり、汎用のネットワークではありません。このネットワークを介して、外部の IP トラフィックをルーティングすることはできません。MAN へのアクセスは、システムコントローラとドメインに制限されています。

SC 上では、MAN ソフトウェアは I1 ネットワークのメタインタフェースを作成し、Solaris OS に対して 1 つのネットワークインタフェース `scman0` を提供します。詳細は、Solaris の `scman(1M)` のマニュアルページを参照してください。

MAN ソフトウェアは通信エラーを検出して、代替パスが利用できる場合は自動的にパスを切り替えます。MAN ソフトウェアは、I1 ネットワーク上のネットワークトラフィックのドメインの切り離しも行います。同様のソフトウェアはドメイン側で動作します。

I2 ネットワーク

2つの NIC で構成されるシステムコントローラ (2 台) の間にも、内部ネットワークが存在します。このネットワークは I2 ネットワークと呼ばれる。これは SC 間のプライベートなネットワークで、I1 ネットワークからは完全に独立しています。

MAN ソフトウェアは I2 ネットワークのメタインタフェースも作成します。このインタフェースは、Solaris ソフトウェアに対し `scman1` として提供されます。I1 ネットワークと同様に I2 ネットワークにも、パスの障害を検出して、代替パスが利用できる場合はパスを切り替えるメカニズムがあります。

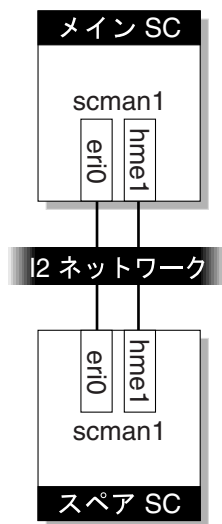


図 9-3 I2 ネットワークの概要

SC 上の仮想ネットワークアダプタは、標準のネットワークアダプタとして提供されます。このネットワークアダプタは、ほかのネットワークアダプタ (`qfe`、`hme` など) と同様に管理できます。この仮想ネットワークアダプタは、`ndd(1M)`、`netstat(1M)`、`ifconfig(1M)` などの通常のシステム管理ツールを使用して管理できます。セキュリティ上の理由から、これらのツールで Ethernet アドレスの変更などを行なってはなりません。

MAN は、特別な性質を持つ IP ネットワークとして動作し、管理されます (たとえば、MAN ソフトウェアによる IP 転送は許可されません)。そのため MAN は、前述した例外はありますが、他の IP ネットワークと同じように動作します。ユーザーのサイト構成やセキュリティー要件に基づいて、ドメインをユーザーのネットワークに接続することができます。ドメインの接続については、このマニュアルでは説明していません。『Solaris のシステム管理 (資源管理とネットワークサービス)』を参照してください。

外部ネットワークの監視

Sun Fire ハイエンドシステムの外部ネットワークの監視機能では、SC から顧客のネットワーク (コミュニティ) への利用度の高いネットワーク接続を提供します。この機能は、Solaris 9 OS で提供される IP ネットワークマルチパス (IPMP) のフレームワークに基づいて構築されています。IPMP の詳細は、『Solaris のシステム管理 (IP サービス)』を参照してください。

「外部ネットワーク」は、コミュニティで構成されます。1 つまたは 2 つのコミュニティで構成することも、あるいはコミュニティをゼロにすることもできます。コミュニティがゼロであるということは、外部ネットワークが監視されないことを意味します。インストールの際は、ユーザーコミュニティはノードをネットワークに接続する SC 上の RJ45 ジャックにケーブルで物理的に接続されます。

外部ネットワークの接続の詳細は、『Sun Fire 15K/12K システムサイト計画の手引き』を参照してください。図 9-4 は、外部ネットワークの概要を示しています。

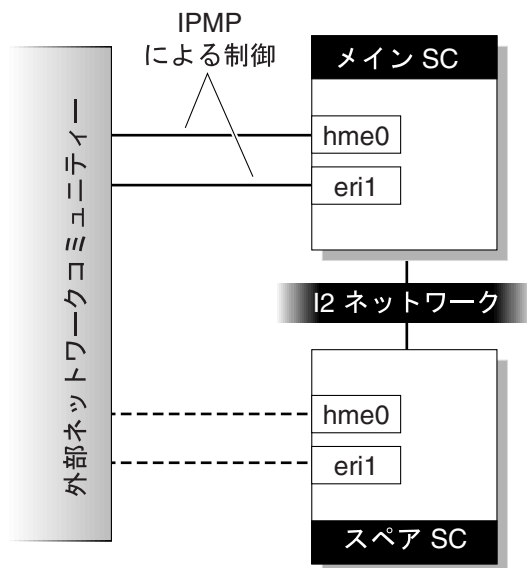


図 9-4 外部ネットワークの概要

「コミュニティ」という用語は、ユーザーのサイトの IP ネットワークを指します。たとえば、エンジニアリングコミュニティや会計コミュニティなどです。「コミュニティ名」は「インタフェースグループ名」として使用されます。「インタフェースグループ」は、同じコミュニティに接続されているネットワークインタフェースのグループです。

外部ネットワークの監視機能を構成するには、各システムコントローラに対して追加 IP アドレスをいくつか割り当てる必要があります。

アドレスは次のように分類されます。

- テストアドレス – 各システムコントローラの外部ネットワークインタフェースに割り当てられる IP アドレスです。各 IP テストアドレスは、割り当て先の特定のネットワークインタフェースの状態をテストする際に使用されます。各ネットワークインタフェースには、それぞれ 1 つの IP テストアドレスが永続的に割り当てられます。これらの IP テストアドレスは、特定のネットワークインタフェースに固定的に関連付けられます。ネットワークインタフェースに障害が発生すると、そのネットワークインタフェースに関連付けられた IP テストアドレスにはアクセスできなくなります。
- フェイルオーバーアドレス – フェイルオーバーアドレスは 2 種類あります。
 - SC パスグループ専用アドレス – 各システムコントローラの特定のインタフェースグループに割り当てられる IP アドレスです。これらの IP アドレスは、コミュニティの特定のシステムコントローラに対して利用度の高い IP 接続を提供するために使用されます。SC パスグループ専用アドレスには、インタフェースグループ内の 1 つ以上のネットワークインタフェースが機能しているかぎりアクセスできます。

注 – SC パスグループ専用アドレスは、インタフェースグループ内にネットワークインタフェースが 1 つしかない場合は不要です。グループ内にはフェイルオーバー対象の他のネットワークインタフェースがないため、テストアドレスとコミュニティフェイルオーバーアドレスだけが必要です。

- コミュニティフェイルオーバーアドレス – メイン SC の特定のコミュニティ (つまり Community C1) に割り当てられる IP アドレスです。これらは、SC0 または SC1 のどちらかのメイン SC への IP 接続を提供するために使用されます。

すべての外部ソフトウェアは、SC と通信する際にコミュニティフェイルオーバーアドレスを参照する必要があります。このアドレスは、常にメイン SC に接続されます。このため、フェイルオーバーが発生しても、外部のクライアントは SC にアクセスするために自分の構成を変更する必要はありません。SC のフェイルオーバーについての詳細は、第 12 章を参照してください。

MAN のデーモンとドライバ

MAN のデーモンやデバイスドライバについての詳細は、SMS の `mand(1M)` のマニュアルページ、および Solaris の `scman(1M)`、`dman(1M)` の各マニュアルページを参照してください。詳細については、71 ページの「管理ネットワークデーモン」を参照。

管理ネットワークのサービス

SC とドメインの間で MAN が提供する主なネットワークサービスは以下のとおりです。

- ドメインコンソール
- メッセージロギング
- 動的再構成 (DR)
- ネットワーク起動 / Solaris のインストール
- システムコントローラ (SC) のハートビート

ドメインコンソール

ドメイン内で実行されるソフトウェア (OpenBoot PROM、`kadb`、および Solaris ソフトウェア) では、重要な通信を行う際にシステムコンソールが使用されます。

ドメインコンソールはログインセッションをサポートしていて安全です。なぜなら、Solaris 環境のデフォルト設定では、コンソールで「スーパーユーザー」のログインのみ受け付けることが可能だからです。ドメインコンソールには、遠隔管理者がパブリックネットワーク経由で安全にアクセスできます。

コンソールの動作は、ドメイン内で実行されているソフトウェアの状態を反映します。ユーザーエントリの文字エコーは、ドメインに接続された 9600 ボーのシリアル端末の文字エコーとほぼ同じです。ユーザー入力のエコーでない出力文字は、通常、実行されたコマンドからの出力かコマンドインタプリタからの出力のいずれかです。または Solaris ソフトウェアからの非要請ログメッセージの場合もあります。ユーザー入力エコーの応答の待ち時間は、他のドメインでのアクティビティーや、ドメインに対する SMS のサポートアクティビティーによって、大幅に変動することはありません。

ドメインコンソールから、ドメインの Solaris ソフトウェアに対して `kadb` を実行できます。ドメイン上で実行されている OpenBoot PROM との対話には、ドメインコンソールが使用されます。コンソールは、Solaris ソフトウェアからのログメッセー

ジの出力先として使用できます。詳細は `syslog.conf(4)` を参照してください。コンソールは、ドメイン上でソフトウェア (Solaris、OpenBoot PROM、kadb) が実行されている場合に使用できます。

複数の接続を開いて、ドメインコンソールの出力を表示することができます。ただし、デフォルトは排他的に**ロックされた**接続です。

詳細は、11 ページの「SMS コンソールウィンドウ」を参照してください。

ドメイン管理者は、ほかのドメインが行なっているドメインコンソールの接続を強制的に切断することができます。

ドメインコンソールから OpenBoot PROM または kadb に強制的に割り込むこともできますが、お勧めできません。これは、物理コンソールを備えた Sun SPARC® システムで使用できる L1-A または STOP-A の物理的なキー操作に相当します。SMS は、以降のドメインクラッシュの分析に備えて、コンソールの出力履歴を収集します。各ドメインのコンソール出力のログは、`/var/opt/SUNWSMS/adm/domain-id/console` で参照できます。

Sun Fire ハイエンドシステムは、共有メモリーコンソールを利用したり、コンソールの別のネットワークデータパスを利用するためのハードウェアを提供します。共有メモリーコンソールに使用されるハードウェアは、コンソールデータの転送の際に直接的に応答時間を課すことは少ないですが、すべてのドメインに対し、他の監視や制御の目的でも使用されるため、ハードウェア資源の競合によって起こる応答時間のリスクが存在します。

MAN はプライベートなネットワークパスを備えており、ドメインコンソールのトラフィックを安全に SC に転送します。詳細は、193 ページの「管理ネットワークのサービス」を参照してください。コンソールはデュアルパスの特性を備えているため、Solaris ソフトウェアが実行されている場合は、最低でも 1つのパスが許容可能なコンソール応答時間を提供します。デュアルパスコンソールは、エラーに直面した場合に威力を発揮します。デュアルパスコンソールは、一方のドメインコンソールのパスに障害を発見すると、自動的に他方のドメインコンソールのパスにフェイルオーバーします。デュアルパスコンソールでは、使用するドメインコンソールのパスをユーザー主導で選択できます。

`smsconfig(1M)` コマンドは、管理ネットワークデーモン `mand(1M)` が使用するホスト名、IP アドレス、およびネットマスクの初期設定またはそれ以降の変更を行うことができる、SC 構成ユーティリティです。71 ページの「管理ネットワークデーモン」を参照してください。

`mand` デーモンは、プラットフォーム構成データベース (`pcd`) でこれらの各フィールドを初期化および更新します。

`mand` デーモンは、`ssd` によって自動的に起動されます。管理ネットワークデーモンは、メイン SC 上では `main` モード、スペア SC 上では `spare` モードで実行されます。

詳細は、SMS の `console(1M)`、`mand(1M)`、`smsconfig(1M)` の各マニュアルページ、および Solaris の `dman(1M)`、`scman(1M)` の各マニュアルページを参照してください。

メッセージロギング

MAN は、重要な syslog メッセージのコピーをドメインから SC のディスクストレージに転送するよう構成されている場合、この転送を行います。これは、ドメインがクラッシュしたり起動不能できなくなったりした場合の障害分析に役立ちます。詳細は、208 ページの「ログファイルの維持管理」を参照してください。

動的再構成

MAN ソフトウェアレイヤーを使用すると、MAN ハードウェアに対するインタフェースを簡素化できます。MAN ソフトウェアは、DSD によって使用される動的再構成 (DR) を処理します。その際にドメイン管理者やプラットフォーム管理者によるネットワーク構成は必要としません。

MAN を使用するドメイン内のソフトウェアは、現在どの SC がメイン SC なのかを区別する必要はありません。動的再構成についての詳細は、『System Management Services (SMS) 1.6 Dynamic Reconfiguration ユーザーマニュアル』を参照してください。

ネットワーク起動および Solaris ソフトウェアのインストール

SC は、各ドメインに対してネットワークから Solaris の起動を行うサービスを提供します。

注 – ディスクレスの Sun Fire ハイエンドシステムドメインを SC のネットワークサービスによって完全にサポートすることはできません。SC のネットワーク起動サービスは、主にドメインの致命的なディスク障害からの回復を目的としています。

Solaris ソフトウェアをドメインにはじめてインストールすると、以降のシステム再起動の際にそれを MAN に接続するネットワークインタフェースが自動的に作成されます。MAN を構成したり使用する際に必要なドメイン管理者のタスクは、これ以外にありません。

MAN はプライベートネットワークとして構成されます。管理ネットワークに割り当てられるデフォルトアドレスは、プライベートネットワーク用に予約されている IP アドレス空間を使用して提供されます。Sun Fire ハイエンドシステムがプライベートな顧客ネットワークに接続されていて、選択された MAN のデフォルト IP アドレス範囲がその顧客ネットワークですでに使用されている場合は、MAN のデフォルトアドレスの割り当てを変更することができます。

SC は、Solaris ソフトウェアの 2 つ以上の異なるバージョンを実行しているドメインの同時ネットワーク起動をサポートしています。

SC は、一度に 1 つだけのドメインに対するソフトウェアのインストールサービスを提供します。

SC のハートビート

I2 ネットワークは、システム間のコントローラ通信を提供します。このネットワークはハートビートネットワークとも呼ばれます。メイン SC の SMS のフェイルオーバーメカニズムでは、スペア SC の健全性を判定する手段の 1 つとして、このネットワークを利用します。詳細は、第 12 章を参照してください。I2 ネットワークについての詳細は、190 ページの「I2 ネットワーク」を参照してください。

第10章

ドメインステータス関数

ステータス関数は、サーバーのハードウェアやソフトウェアのステータスを示す測定値を返します。このため、これらの関数はステータスを表示するための値と、モニターソフトウェアへ入力するための値を提供する際に使用されます。モニターソフトウェアは、ステータス関数を定期的に調べて、戻り値が通常の動作制限内かどうか検証します。この章では、ステータス関数を使用するモニター関数やイベント検出関数について説明します。

この章では、以下の項目を説明します。

- 197 ページの「ソフトウェアのステータス」
- 202 ページの「ハードウェアのステータス」
- 205 ページの「SC のハードウェアおよびソフトウェアのステータス」

ソフトウェアのステータス

ソフトウェアのステータスは、ドメインで実行されているソフトウェアによって提供されるステータス情報で構成されます。現在実行されているソフトウェアコンポーネント (たとえば POST、OpenBoot PROM、または Solaris ソフトウェア) の識別情報が得られます。その他のステータス情報 (起動、実行、パニック) も得られます。

SMS ソフトウェアで提供される次のコマンドは、ドメイン内で現在実行されているソフトウェアがあれば、そのステータスを表示します。

- showboards
- showdevices
- showenvironment
- showobpparams
- showpcimode
- showplatform
- showxirstate

ステータスコマンド

この節では、SMS のドメインステータスコマンドについて説明します。

showboards コマンド

`showboards(1M)` コマンドは、DCU の割り当て情報およびステータスを表示します。この情報には、場所、電源、ボードのタイプ、ボードのステータス、テストステータス、およびドメインが含まれます。

プラットフォーム管理者の場合は、オプションを何も指定しないと、`showboards` コマンドによって、**割り当て済みの DCU** や**使用可能な DCU** を含むすべての DCU が表示されます。ドメイン管理者または構成者の場合、`showboards` は、そのユーザーが特権を持つドメインの DCU だけを表示します。これには、ドメインの使用可能構成要素リストにある、`assigned` または `available` のボードが含まれます。

`domain-indicator` を指定すると、このコマンドは目的のドメインに対して `assigned` または `available` である DCU を表示します。`-v` オプションを使用すると、`showboards` は DCU を含むすべてのボードを表示します。

詳細や例については、97 ページの「ボードステータスを取得する」および `showboards` のマニュアルページを参照してください。

showdevices コマンド

`showdevices(1M)` コマンドは、システムボード上に構成された物理デバイスや、これらのデバイスで使用可能なリソースを表示します。使用状況情報は、システム資源をアクティブに管理しているアプリケーションおよびサブシステムによって提供されます。必要な場合は、管理対象の資源をオフラインで問い合わせることによって、システムボードの DR 操作による影響の予測を表示できます。

`showdevices` コマンドは、1 つ以上の Sun Fire ハイエンドシステムドメインからデバイス情報を収集します。このコマンドは、`dca(1M)` をプロキシとして使用して、ドメインから情報を収集します。

詳細や例については、97 ページの「ボードステータスを取得する」および `showdevices` のマニュアルページを参照してください。

showenvironment コマンド

`showenvironment(1M)` コマンドは、位置、センサー、値、ユニット、年数、ステータスなどの環境データを表示します。ファントレーについては、電源、速度、ファン番号が表示されます。バルク電源については、電源、値、ユニット、ステータスが表示されます。

domain-indicator を指定すると、ユーザーがそのドメインに対するドメイン特権を持っている場合に、そのドメインに関連する環境データが表示されます。ドメインが指定されていない場合は、そのユーザーに許可されるすべてのドメインデータが表示されます。

DCU (CPU や I/O など) はドメインに属しているため、これらのステータスを表示するにはドメイン特権が必要です。ファントレー、バルク電源、または他のボードなどに関連する環境データは、ドメインの許可がなくても表示できます。-p オプションを使用すれば、温度、電圧、電流、障害、バルク電源ステータス、およびファントレーステータスの個別のレポートを指定することもできます。-p オプションがない場合は、すべてのレポートが表示されます。

詳細や例については、203 ページの「環境ステータス」および `showenvironment` のマニュアルページを参照してください。

showobpparams コマンド

`showobpparams(1M)` コマンドは、OpenBoot PROM の起動パラメータを表示します。`showobpparams (1M)` コマンドを使用すると、ドメイン管理者は、`setkeyswitch (1M)` によって OpenBoot PROM に渡される仮想 NVRAM および REBOOT パラメータを表示できます。

詳細や例については、120 ページの「OpenBoot PROM 変数の設定」および `showobpparams` のマニュアルページを参照してください。

showpcimode コマンド

`showpcimode(1m)` コマンドは、使用しているサーバーの V2HPCIX I/O ボード上にあるすべての PCI-X スロットのモード設定を一覧表示します。この設定は `setpcimode` コマンドによって指定されます。`normal` というステータスを返すスロットは、PCI-X モードで動作しています。`pci_only` というステータスを返すスロットは、PCI モードで強制的に動作しています。

V2HPCIX ボードでない I/O ボードを指定すると、このコマンドはエラーを返しません。

showplatform コマンド

`showplatform(1M)` コマンドは、使用可能構成要素リストと、各ドメインのドメインステータスを表示します。

ドメインは、*domain-tag* が存在すればそれによって識別されます。それ以外の場合は、*domain-id* の A ~ R のいずれかの文字で識別されます。文字セットは大文字と小文字の区別があります。`Solaris` の *hostname* が存在すればそれ表示されます。ドメインに *hostname* が割り当てられていない場合は、Unknown が表示されます。

表 10-1 に、ドメインステータスを一覧表示します。

表 10-1 ドメインステータスの種類

ステータス	説明
Unknown	ドメイン状態が判断できませんでした。Ethernet アドレスの場合、ドメイン idprom イメージファイルが存在しません。ご購入先にご連絡ください。
Powered Off	ドメインの電源が切断されています。
Keyswitch Standby	ドメインのキースイッチが STANDBY 位置になっています。
Running Domain POST	ドメイン電源投入時自己診断が実行中です。
Loading OBP	ドメインの OpenBoot PROM がロードされています。
Booting OBP	ドメインの OpenBoot PROM が起動中です。
Running OBP	ドメインの OpenBoot PROM が実行中です。
In OBP Callback	ドメインが停止され OpenBoot PROM に戻されています。
Loading Solaris	OpenBoot PROM が Solaris ソフトウェアをロードしています。
Booting Solaris	ドメインが Solaris ソフトウェアを起動しています。
Domain Exited OBP	ドメインの OpenBoot PROM が終了しました。
OBP Failed	ドメインで OpenBoot PROM の実行に失敗しました。
OBP in sync Callback to OS	OpenBoot PROM が Solaris ソフトウェアに同期コールバックをしています。
Exited OBP	OpenBoot PROM が終了しました。
In OBP Error Reset	ドメインがエラーリセット状態に陥り、OpenBoot PROM に戻っています。
Solaris Halted in OBP	Solaris ソフトウェアが停止し、ドメインが OpenBoot PROM になっています。
OBP Debugging	OpenBoot PROM がデバッガとして使用されています。
Environmental Domain Halt	環境に起因する緊急事態によってドメインがシャットダウンしました。
Booting Solaris Failed	OpenBoot PROM が動作しているが、起動に失敗しました。
Loading Solaris Failed	OpenBoot PROM が動作しているが、ロードに失敗しました。
Running Solaris	Solaris ソフトウェアがドメイン上で実行中です。
Solaris Quiesce In-Progress	Solaris ソフトウェアが休止されています。

表 10-1 ドメインステータスの種類 (続き)

ステータス	説明
Solaris Quiesced	Solaris ソフトウェアが休止しました。
Solaris Resume In-Progress	Solaris ソフトウェアを再開しています。
Solaris Panic	Solaris ソフトウェアがパニックに陥り、パニックフローが開始されました。
Solaris Panic Debug	Solaris ソフトウェアがパニックに陥り、デバッガモードに移行中。
Solaris Panic Continue	デバッガモードが終了しました (パニックフローは続行)。
Solaris Panic Dump	パニックダンプが開始されました。
Solaris Halt	Solaris ソフトウェアが停止しています。
Solaris Panic Exit	Solaris ソフトウェアがパニックによって終了しました。
Environmental Emergency	環境的な緊急事態が検出されました。
Debugging Solaris	Solaris ソフトウェアをデバッグしています。ハング状態ではありません。
Solaris Exited	Solaris ソフトウェアが終了しました。
Domain Down	ドメインがダウンしており、 <code>setkeyswitch</code> によってキースイッチが ON、DIAG、または SECURE に設定されている。
In Recovery	ドメインで自動システム回復が実行中です。

表 10-2 ドメインステータスの種類

ドメインのステータスには、2 種類の状態が反映されます。1 つは `dsmd` がドメインの復元を試みている状態、もう 1 つは `dsmd` によるドメイン復元が失敗に終わった状態です。後者の場合は、常に「Domain Down」と表示されます。前者の場合は、「Domain Down」またはその他のステータスが表示されます。どちらの場合にも「Domain Down」から回復するには、`setkeyswitch off`、`setkeyswitch on` を使用します。

```
sc0:sms-user:> setkeyswitch off
sc0:sms-user:> setkeyswitch on
```

詳細や例については、99 ページの「ドメインステータスを取得する」および `showplatform` のマニュアルページを参照してください。

showxirstate コマンド

showxirstate (1M) コマンドは、プロセッサにリセットパルスが送信されたあとの CPU ダンプ情報を表示します。この保存状態ダンプは、異常なドメイン動作の原因を解析するために使用できます。showxirstate は、そのドメイン内にあるすべてのアクティブプロセッサのリストを作成し、各プロセッサの保存状態情報 (プロセッサシグニチャーを含む) を取得します。

showxirstate コマンドのデータは、デフォルトでは /var/opt/SUNWSMS/adm/domain-id/dump に保存されます。

詳細や例については、showxirstate のマニュアルページを参照してください。

Solaris ソフトウェアのハートビート

Solaris 環境の通常動作時には、SC から読み取り可能なハートビートインジケータが定期的に作成されます。dsmd デーモンは、実行中の Solaris システムのハートビート更新の欠如を、Solaris システムのハングアップとして検出します。ハングの状態が検出されるのは Solaris ソフトウェアだけで、それ以外のソフトウェアコンポーネントのハングは検出されません。

注 – Solaris ソフトウェアのハートビートを、SC 対 SC (ハードウェア) のハートビートやハートビートネットワークと混同しないでください。どちらもフェイルオーバーの状態を判定する際に使用されます。詳細は、196 ページの「SC のハートビート」を参照してください。

Solaris ハートビートの応答が発生するのは、dsmd コマンドが Solaris ハートビートを完全に更新できない障害を検出して、Solaris ソフトウェアがハングしていることを示す場合に限られます。Solaris ソフトウェアのハングが検出されると、dsmd コマンドは ASR を実行します。

ハードウェアのステータス

ハードウェアのステータス関数は、ハードウェア構成、検出されたハードウェアの障害、およびプラットフォームの環境状態に関する情報をレポートします。

ハードウェア構成

Sun Fire ハイエンドシステムのシステム管理ソフトウェアでは、以下のハードウェア構成ステータスを取得できます。

- 各ボードに物理的に存在するハードウェアコンポーネント (POST によって検出)
- POST に失敗したため使用されていないハードウェアコンポーネント
- システムボードなどの HPU の存在の有無
- POST が実行されたときにブラックリストに存在していたため使用されないハードウェアコンポーネント (173 ページの「電源投入時自己診断 (POST)」を参照)
- 各 FRU の EEPROM の内容 (パーツ番号やシリアル番号を含む)

注 – SC 上で実行中の SMS が取得できるハードウェア構成ステータスは、存在の有無に限定されます。これには、I/O アダプタの装着位置や、I/O アダプタに接続されているデバイスなど、I/O 構成に関する情報は含まれません。このような情報は、I/O アダプタを所有しているドメインで実行中のソフトウェアだけが取得できます。

この節で説明している機能でサポートされているハードウェア構成には、I/O アダプタや I/O デバイスは含まれません。showboards コマンドは、存在するハードウェアコンポーネントをすべて表示します。

174 ページの「ブラックリストの編集」で説明しているように、現在のコンポーネントのブラックリストの内容は、いつでも表示したり変更したりできます。

環境ステータス

以下のハードウェア環境の測定値が取得できます。

- 温度
- 電源の電圧およびアンペア数
- ファンのステータス (停止、低速、高速、障害)
- 電源のステータス
- 障害

showenvironment コマンドは、Sun Fire ハイエンドシステムのラック内で取得できるすべての環境測定値を表示します。

▼ ドメイン A の環境ステータスを表示する

1. SC にログインします。

プラットフォーム管理者は、プラットフォーム全体のすべての環境ステータスを表示できます。ドメイン管理者は、特権を持つドメインの環境ステータスのみを表示できます。

2. 次のコマンドを入力します。

```
sc0:sms-user:> showenvironment -d A
```

183 ページの「HPU の LED」で説明しているように、Sun Fire ハイエンドシステムの HPU の動作インジケータ LED は、その HPU の電源が投入されていることを視覚的に表示し、取り外し可能 LED は、その HPU が取り外し可能であることを視覚的に表示します。

ハードウェアエラーのステータス

dsmcd デーモンは、Sun Fire ハイエンドシステムハードウェアの動作ステータスを監視して、エラーをレポートします。いくつかのエラーの発生は、SC に直接報告されます (各 ASIC のエラーレジスタは、エラーサマリーレジスタを提供する SC の SBBC に伝播されます)。いくつかのエラーの発生は、SC に対する割り込みによって示されますが、いくつかのエラーステータスについては、SC がハードウェアレジスタでエラーの兆候を監視する必要があります。ハードウェアエラーが検出されると、esmd コマンドは定められた手順に従ってハードウェアエラーのステータスを収集したり、クリアしたりします。

Sun Fire ハイエンドシステムのハードウェアでは、以下のタイプのエラーが発生することがあります。

- ドメインの停止。ドメイン内のすべてのハードウェア動作を終了させる致命的なハードウェアエラー
- 記録の停止。データ転送エラー (CE ECC など) が発生したときに、ハードウェアによるトランザクション履歴の収集が停止します。
- SPARC プロセッサのエラー状態 (RED-state、ウォッチドッグリセットなど)
- ASIC で検出された致命的でないハードウェアエラー

ハードウェアエラーのステータスは、一般にステータスとしてレポートされません。その代わりに、ハードウェアエラーが発生した場合は、イベント処理関数によってさまざまなアクションが実行されます (エラーログの記録、ASR の実行など)。これらの関数については、第 11 章で説明しています。

注 - 183 ページの「HPU の LED」で説明しているように、障害 LED は POST が完了したあとに、最終電源投入時以降、または電源投入時リセット以降に障害が発見された Sun Fire ハイエンドシステムの HPU を識別します。

SC のハードウェアおよびソフトウェアのステータス

SMS が正しく動作するかどうかは、SC 上のハードウェアと Solaris ソフトウェアが正しく動作するかどうかによって決まります。メインからスペアへのシステムコントローラの自動フェイルオーバーをサポートするには、スペア上でハードウェアとソフトウェアが正常に動作している必要があります。メインシステムコントローラ上で実行されている SMS ソフトウェアは、スペアによって検出可能な方法でソフトウェアまたはハードウェアの障害を診断できるくらい十分に機能しているか、あるいはスペアによって検出可能な方法で機能しなくなっている必要があります。

注 – フェイルオーバーをサポートするには、両方の SC で同一バージョンの Solaris OS および SMS ソフトウェアが構成されている必要があります。

SC-POST は、システムコントローラのハードウェアステータスを判定します。SC-POST は、電源投入時または電源投入リセット時にシステムコントローラをテストして構成します。

SC が機能しなくなると、SC は起動しません。

制御ボードが機能しなくなると、SC は通常どおり起動しますが、制御ボードのデバイスにはアクセスできません。システムコントローラの起動に必要なハードウェアの動作レベルは、実質的にスタンドアロンの SC で必要な動作レベルと同じです。

SC-POST は、診断結果を SC のコンソールシリアルポート (TTY-A) に出力します。さらに、SC-POST は診断ステータスの簡潔な概要メッセージを NVRAM バッファに残します。このメッセージは Solaris ドライバが読み取ることができ、Solaris ソフトウェアの起動時に記録または表示されます。

SC のファームウェアおよびソフトウェアは、SC のハードウェア障害を識別したり修正するための情報を表示します。

SC のファームウェアおよびソフトウェアは、システムコントローラのハードウェアが機能していることを検証するソフトウェアインタフェースを提供します。これによって、稼動中のシステムコントローラは、高可用性 SC 構成のメイン SC として選択されます。

システムコントローラの LED は、183 ページの「HPU の LED」で説明しているように、電源や検出されたハードウェア障害に関するステータスを視覚的に表示します。

Solaris ソフトウェアは、自己診断と自動復旧 (パニックと再起動) のレベルを提供します。Solaris ソフトウェアは、SC のハードウェアウォッチドッグロジックを利用して、ハング状態をトラップし、強制的に自動復旧再起動を行います。

SCの間には、4つのハードウェア通信パス (Ethernet 接続2つ、ハードウェアネットワーク、および SC 対 SC のハートビート信号) があります。各 SC はこれらのパスを、使用度の高い SC の構成で使用して、ほかの SC のハングや障害を検出します。

SMS は、使用度の高くない SC の構成でも自己診断を実施し、自動障害復旧手順を定めます。

SMS ソフトウェアは復旧の際に、プラットフォームのハードウェアを必要に応じて既存の有効な構成に戻すか、またはそれが不可能なことをレポートします。

SMS ソフトウェアは、現場で1回だけ発生したソフトウェア障害の工学的診断を有効にするために十分な情報を記録してログをとります。

SMS ソフトウェアは、自己を初期化して完全に機能するようになるのにかなりの時間がかかります。この間に、ユーザーインターフェースは予測可能な状態で機能します。ユーザーコマンドの拒否は、システムを初期化するためであると明示されるとともに、適切な間隔を空けて再試行するようにアドバイスされます。

SMS のソフトウェア環境では、分散型クライアント / サーバーアーキテクチャーが使用されます。初期化をまだ完了していないプロセスと対話しようとして、SMS の初期化の際に発生したエラーは、静的に処理されます。

第11章

ドメインイベント

イベント監視では、処置が必要な状況を検出するために、周期的にドメインとハードウェアの状態を確認します。実行するアクションはその状況に応じて決定され、状況の報告やそれを処理する自動手続きの初期化が伴います。この章では、監視により検出されるイベントと、検出されたイベントに応じて実行されるアクションに関する要件を説明します。

この章では、以下の項目を説明します。

- 207 ページの「メッセージロギング」
- 213 ページの「ドメイン再起動イベント」
- 215 ページの「ドメインパニックイベント」
- 217 ページの「Solaris ソフトウェアハングイベント」
- 218 ページの「ハードウェア構成イベント」
- 219 ページの「環境イベント」
- 222 ページの「ハードウェアエラーイベント」
- 224 ページの「SC 障害イベント」

メッセージロギング

SMS は、イベントに応じて実行されるユーザー監視表示の記録や更新以外の重要なアクションをすべて記録します。重要なドメインソフトウェアイベントのログメッセージとその応答アクションは、`/var/opt/SUNWSMS/adm/domain-id/messages` に格納されている、影響を受けたドメインのメッセージログファイルに書き込まれます。ログに記録される内容は、後にハードウェアやソフトウェアを保守するための情報です。

SMS は、`/var/opt/SUNWSMS/adm/platform/messages` に格納されているプラットフォームログファイルに、重要なハードウェアイベントのログメッセージを書き込みます。SMS は、影響を受けたドメインの1つ以上に明らかに作用する可能性のある重要なハードウェアイベントについてのログメッセージを、`/var/opt/SUNWSMS/adm/domain-id/messages` に書き込みます。

ドメインソフトウェアシステムに障害を発生させるイベントに応じて実行されるアクションには、影響を受けたすべてのドメインの ASR (自動システム回復) 再起動があります。ただし、ドメインハードウェア (または起動可能なそのサブセット) が安全かつ正常な動作の要件を満たしていることを条件とします。

また、SMS は、ドメインコンソール、syslog、イベント、ポスト、およびダンプ情報の記録と、sms_core ファイルの管理も行います。

ログファイルの維持管理

SMS ソフトウェアは、記録するすべてのサーバー情報のコピー (SC に常駐) を管理します。showlogs(1M) コマンドを使うと、ログ情報にアクセスできます。

プラットフォームメッセージログファイルには、そのプラットフォームの管理者が次のコマンドを使用する場合のみアクセスできます。

```
sc0:sms-user:> showlogs
```

構成されたドメインに関連する SMS ログ情報には、そのドメインの管理者だけがアクセスできます。SMS は、各ドメインのログファイルを個別に維持します。ファイルにアクセスするには、次のコマンドを入力します。

```
sc0:sms-user:> showlogs -d domain-indicator
```

ここで次の点に留意します。

-d domain-indicator 以下を使用してドメインを指定します。

domain-id - ドメインの ID。有効な *domain-id* は、A ~ R で、大文字と小文字を区別しません。

domain-tag - addtag(1M) を使用してドメインに割り当てた名前。

SMS は、SC 上のドメインの syslog ファイルのコピーを /var/opt/SUNWSMS/adm/*domain-id*/syslog で維持します。この syslog 情報には、そのドメインの管理者だけがアクセスできます。

情報にアクセスするには、次のコマンドを入力します。

```
sc0:sms-user:> showlogs -d domain-indicator -p s
```

Solaris コンソールの出力ログは、ドメインのクラッシュ前に何が発生したのかを判断するための貴重な情報として管理されています。コンソール出力は、クラッシュしたドメインの SC 上の /var/opt/SUNWSMS/adm/domain-id/console で参照できません。console 情報には、そのドメインの管理者だけがアクセスできます。

情報にアクセスするには、次のコマンドを入力します。

```
sc0:sms-user:> showlogs -d domain-indicator -p c
```

reset コマンドで生成される XIR 状態ダンプは、showxirstate を使用して表示できます。詳細については、showxirstate のマニュアルページを参照してください。

ドメインポストログはサービス診断用に用意されており、showlogs や SMS CLI では表示されません。

/var/tmp/sms_core.daemon ファイルはバイナリで、表示できません。

SC 上の各種ログファイルを利用できるため、1 つまたは複数のドメインの起動を妨げる問題の分析および正常化をサポートすることができます。詳細については、showlogs のマニュアルページを参照してください。

注 – パニックになったドメインのパニックダンプは、SC 上ではなくドメイン上の /var/crash ログに収録されています。

表 11-1 に、SMS ログ情報の種類とその説明を示します。

表 11-1 SMS ログの種類に関する情報

種類	説明
ファームウェアバージョン管理	ファームウェア起動時にファームウェアバージョンの不適当な構成が自動的に正常化および記録されます。
電源投入時自己診断	故障 LED。故障 LED が点灯した理由を詳しく述べるプラットフォームおよびドメインメッセージ。
電源制御	すべての電源操作が記録されます。
電源制御	ハードウェア要件またはハードウェア推奨手順に違反する電源操作。
電源制御	電源操作を強制完了するためのオーバーライドの使用。
ドメインコンソール数	コンソール出力を自動的に標準ファイルに記録します。
ハードウェア構成	メッセージログでパート番号を使用してボードの種類を識別します。

表 11-1 SMS ログの種類に関する情報 (続き)

種類	説明
障害とエラーイベントの監視およびアクション	イベントログに書き込まれたすべての障害イベントまたはエラーレポートの一覧。
イベントの監視およびアクション	すべての重要な環境イベント (アクションを起こすのに必要なイベント)。
イベントの監視およびアクション	環境イベントに応じて起こされるすべての重要なアクション。
ドメインイベントの監視およびアクション	すべての重要なドメインソフトウェアおよびその応答アクション。
イベントの監視およびアクション	重要なハードウェアイベントがプラットフォームログに書き込まれます。
イベントの監視およびアクション	すべての重要なクロック入力障害、クロック入力切り換え障害、およびフェーズロックの損失と取得。
ドメインイベントの監視およびアクション	1 つまたは複数のドメインに大きく影響する重要なハードウェアイベントがドメインログに書き込まれます。
ドメイン起動初期化	ドメインを起動するそれぞれの重要ステージを通じて、各起動の初期化と推移をドメインログに書き込みます。
ドメインの起動に失敗	起動障害がドメインログに記録されます。
ドメイン起動障害	すべての ASR 回復試行動作がドメインログに記録されます。
ドメインパニック	ドメインパニックがドメインログに記録されます。
ドメインパニック	すべての ASR 回復試行動作がドメインログに記録されます。
ドメインパニックハング	発生した各ドメインハングとそれに付随する情報がドメインログに記録されます。
ドメインパニック	ドメインパニックおよびドメインハングの後のすべての ASR 回復試行動作がドメインログに記録されます。
反復ドメインパニック	反復ドメインパニック後のすべての ASR 回復試行動作がドメインメッセージログに記録されます。
Solaris OS ハングイベント	すべての OS ハングイベントがドメインメッセージログに記録されます。
Solaris OS ハングイベント	OS ハングイベントはすべて、Solaris ハングの分析用コアイメージを取得するために、ドメインパニックを引き起こします。この情報およびそれ以降の回復動作は、ドメインメッセージログに記録されます。

表 11-1 SMS ログの種類に関する情報 (続き)

種類	説明
Solaris OS ハングイベント	SMS は、ドメインソフトウェアがパニック要求を満足できないかどうかを監視します。パニック要求に適合していないと判断するとすぐに、SMS はドメインを終了させ、ASR 再起動を初期化します。それ以降のすべての回復アクションは、ドメインメッセージファイルに記録されます。
ホットプラグイベント	ドメインに対するシステムボードのすべての HPU 挿入イベントがドメインメッセージログに記録されます。
ホットアンプラグイベント	HPU 取り外しについてのすべての情報がプラットフォームメッセージログに記録されます。
ホットアンプラグイベント	ドメインからの HPU 取り外しについてのすべての情報がドメインメッセージログに記録されます。
POST 初期化構成イベント	すべての POST 初期化ハードウェア構成の変更が /var/opt/SUNWSMS/adm/domain-id/post ディレクトリに記録されます。
環境イベント	許容動作範囲外のすべてのセンサー測定値を、環境イベントとしてプラットフォームログファイルに記録します。
環境イベント	1 つまたは複数のドメインに影響するすべての環境イベントがドメインメッセージログに記録されます。
環境イベント	環境イベントに応じて実行される重要なアクションがプラットフォームメッセージログに記録されます。
環境イベント	ドメイン内の環境イベントに応じて実行される重要なアクションがドメインメッセージログに記録されます。
ハードウェアエラーイベント	ハードウェアエラーおよび関連情報がプラットフォームメッセージログに記録されます。
ハードウェアエラーイベント	ドメイン内のハードウェアエラーおよび関連情報がドメインメッセージファイルに記録されます。
ハードウェアエラーイベント	データが収集されたハードウェアエラーについてのログエントリにデータファイルの名前が入ります。
ハードウェアエラーイベント	ハードウェアエラーイベントに応じて実行されるすべての重要なアクションがプラットフォームメッセージログに記録されます。
ハードウェアエラーイベント	ドメインに影響するハードウェアエラーイベントに応じて実行されるすべての重要なアクションがドメインメッセージログに記録されます。
SC 障害イベント	すべての SC ハードウェア障害および関連する情報がプラットフォームメッセージログに記録されます。
SC 障害イベント	SC フェイルオーバーイベントがプラットフォームメッセージログに記録されます。

ログファイルの管理

SMS は、必要に応じてログファイルを管理し、許容範囲内で SC のディスク使用レベルを保持します。

メッセージログデーモン (mld) は、メッセージログのサイズ、ディレクトリごとのファイル数、および 10 分刻みの時間経過を監視します。mld デーモンは、最初の限度に到達すると開始します。表 11-2 に、MLD のデフォルト設定を一覧表示します。

表 11-2 MLD のデフォルト設定

	ファイルのサイズ (K バイト単位)	ファイル数	保有期間 (日数単位)
SMI イベントログ	2500	10	0
プラットフォームメッセージ数	2500	10	0
ドメインメッセージ数	2500	10	0
ドメインコンソール数	2500	10	0
ドメインの syslog 数	2500	10	0
ドメインポスト数	20000*	1000	0
ドメインダンプ数	20000*	1000	0
<i>sms-core.daemon</i>	100000	20	0

* ファイルごとではなくディレクトリごとの総計

ディレクトリ数が 20 個とすると、これらのデフォルトにより約 4G バイトのログが格納されることとなります。



注意 – 表 11-2 に示したパラメータは、ファイル

/etc/opt/SUNWSMS/config/mld_tuning に格納されています。mld は、なんらかの変更が有効になるたびに停止して再起動する必要があります。このファイルの編集については、システムディスクの使用に経験を積んだ管理者のみが担当すべきです。このファイルでパラメータを不適切に変更してしまうと、ディスクがあふれ、SC をハングまたはクラッシュさせてしまう可能性があります。

- ログメッセージファイルがサイズの限度に達したら、mld は次の処理を行います。

もっとも古いメッセージファイルが message.9 であるか、またはコアファイルが sms_core.daemon.1 でないかぎり、もっとも古いメッセージファイルの x.X から始めて、そのファイルを x.X+1 に移し、x.X-1 から処理を始めます。

たとえば、messages は messages.0 になり、messages.0 は messages.1 になり、messages.9 まで順送りされます。messages が 2.5M バイトに達すると、messages.9 は削除され、すべてのファイルの接尾辞が 1 だけ増やされて、新しい空の messages ファイルが作成されます。

- ログファイルがファイル数の限度に達したら、m1d は次の処理を行います。
messages または sms_core.daemon の数が限度に達したら、もっとも古いメッセージファイルまたはコアファイルが削除されます。
- ログファイルの生成後の時間経過が限度に達したら、m1d は次の処理を行います。
メッセージファイルは、その生成後に x 日が経過すると削除されます。

注 – デフォルトでは、時間経過の限度 (*_log_keep_days) はゼロに設定され、使用されません。

- postdate.time.sec.log または dump-name.date.time.sec ファイルが、ファイルサイズ、数、または時間経過の限度に達すると、m1d はディレクトリ内のもっとも古いファイルを削除します。

注 – ポストファイルはサービス診断用に用意され、表示対象ではありません。

詳細については、m1d および showlogs のマニュアルページと、72 ページの「メッセージロギングデーモン」を参照してください。

ドメイン再起動イベント

SMS は、ドメインソフトウェアの状態 (197 ページの「ソフトウェアのステータス」を参照) を監視し、ドメイン再起動イベントを検出します。

ドメイン再起動の初期化

ドメインソフトウェアは自分自身を再起動することはできないので、SMS ソフトウェアがすべてのドメイン再起動の初期シーケンスを制御します。その結果、SMS は常にドメイン再起動の初期化イベントを認識しています。

SMS ソフトウェアは、各再起動の初期化とドメインを起動するそれぞれの重要ステージを通じての推移をドメイン固有のログファイルに記録します。

ドメイン起動の障害

SMS ソフトウェアは、ドメイン再起動の障害をすべて検出します。

SMS は、ドメイン再起動の障害を検出するとすぐに、再起動の障害イベントをドメイン固有のメッセージログに記録します。

SC に常駐するドメインごとのログファイルは、障害分析に利用することができません。再起動の障害をログに記録することに加え、SMS は208 ページの「ログファイルの維持管理」の説明のように、重要なドメイン常駐ログの複製およびドメインコンソール出力のトランスクリプトを管理できます。

ドメイン再起動の障害は次のように処理されます。

- **reboot** 要求または **reset** 要求への応答は、常に高速起動手続きです。
- ソフトウェア障害からドメインを回復しようとする最初の試みでは、すみやかな再起動手続きが使用されます。
- ハードウェア障害からドメインを回復しようとする最初の試みでは、**reboot** 手続きが使用されます。POST デフォルト診断レベルは、**reboot** 手続きで使用されません。
- POST の実行時にドメインの回復が失敗した場合、**dsmd** は最初の回復試行動作の失敗後に、ドメイン回復が 6 回連続して失敗するまで、デフォルトの診断レベルで POST を再試行します。
- IOSRAM レイアウト時、OpenBoot PROM のダウンロードおよびジャンプ時、OpenBoot PROM の実行時、または Solaris ソフトウェアの起動時に、ドメイン回復が失敗した場合には、**dsmd** はデフォルトの診断レベルで POST を再実行します。このタイプのそれ以後の障害では、回復動作ごとに **dsmd** は、以前のレベルより高いテスト診断レベルで POST を実行します。**dsmd** デーモンは、最初の回復試行動作の失敗後に、デフォルトレベルでドメイン回復を 6 回まで再試行しますつまり、**dsmd** はドメイン回復試行動作を合計で最大 7 回行います。
- システムが回復して、Solaris ソフトウェアが起動されると、4 時間以内のドメイン障害は反復的なドメイン障害として扱われ、より高い診断レベルで POST を実行することで回復されます。
- Solaris ソフトウェアを 4 時間実行したときにドメイン障害が出ない場合は、ドメインは正常に回復され健全な状態にあると見なされます。

それ以後のドメインハードウェア障害は、**reboot** 手続きにより処理されます。

それ以後のドメインソフトウェア障害は高速再起動手続きにより処理され、**reboot** または **reset** 要求は高速起動手続きにより処理されます。

SMS は、起動に失敗したドメインを起動するために、すべての ASR メソッドを適宜実行します。すべての回復試行動作は、ドメイン固有のメッセージログに記録されます。

ドメインパニックイベント

ドメインがパニック状態になると、回復再起動を初期化できるように dsmd に通知します。パニックはドメインソフトウェア状態の変化として報告されます (197 ページの「ソフトウェアのステータス」を参照)。

ドメインパニック

ドメイン上の Solaris ソフトウェアがパニックになると dsmd デーモンに通知されます。

dsmd はドメインパニックを検出するとすぐに、パニックイベントをドメイン固有のメッセージログに記録します。

SC に常駐するドメインごとのログファイルは、ドメインパニックの分析に利用することができます。パニックログに加え、SMS は 208 ページの「ログファイルの維持管理」の説明のように、重要なドメイン常駐ログの複製およびドメインコンソール出力のトランスクリプトを管理できます。

一般的に、ハードウェアエラーの兆候がない最初のパニックの後には、SMS はドメインを起動するために高速再起動を試みるよう要求します。詳細は、171 ページの「ドメインの再起動」を参照してください。

dsmd デーモンはパニックイベントを次のように処理します。

- POST の実行時にドメインの回復が失敗した場合、dsmd デーモンは最初の回復試行動作の失敗後に、ドメイン回復が 6 回連続して失敗するまで、デフォルトの診断レベルで POST を再試行します。
- IOSRAM レイアウト時、OpenBoot PROM のダウンロードおよびジャンプ時、OpenBoot PROM の実行時、または Solaris ソフトウェアの起動時に、ドメイン回復が失敗した場合には、dsmd デーモンはデフォルトの診断レベルで POST を再実行します。このタイプのそれ以後の障害では、回復動作ごとに dsmd は、以前のレベルより高いテスト診断レベルで POST を実行します。dsmd デーモンは、最初の回復試行動作の失敗後に、デフォルトレベルでドメイン回復を 6 回まで再試行します。つまり、dsmd はドメイン回復試行動作を最高で 7 回行います。
- システムが回復して、Solaris ソフトウェアが起動されると、4 時間以内のドメイン障害は反復的なドメイン障害として扱われ、より高い診断レベルで POST を実行することで回復されます。
- Solaris ソフトウェアの起動から 4 時間以内にドメイン障害が発生しなければ、そのドメインは正常に回復され健全であると見なされます。
それ以後のドメインハードウェア障害は、reboot 手続きにより処理されます。

それ以後のドメインソフトウェア障害は高速再起動手続きにより処理され、reboot または reset 要求は高速起動手続きにより処理されます。

この回復アクションは、ドメイン固有のメッセージログに記録されます。

ドメインパニックハング

Solaris パニックダンプロジックは、パニック時にハングする危険性を最小限に抑えるよう再設計されました。パニック状況では、通常機能が停止しているか、またはパニックにより無効にされているために、Solaris ソフトウェアの動作が異常になる場合があります。パニックになった Solaris ドメインの ASR 再起動動作は、そのドメインが再起動を要求できるようになるまでにハングしていても開始されます。

パニックになったドメインの通常のハートビート監視 (217 ページの「Solaris ソフトウェアハングイベント」を参照) は、パニックになった Solaris ドメインが ASR 再起動要求まで進めない状況を検出するには妥当または十分でないことがあります。このため、dsmd は必要に応じて特別な措置を講じて、ドメインパニックハングイベントを検出します。

パニックハングイベントを検出するとすぐに、dsmd は各イベントの発生を、その情報とともにドメイン固有のメッセージログに記録します。

SMS は、ドメインパニックハング (存在する場合) を検出すると、ただちにドメインパニックを終了させて (172 ページの「ドメインの中止またはリセット」を参照)、ドメインの ASR 再起動を開始します。dsmd は、これらの回復アクションをドメイン固有のメッセージログに記録します。

SC に常駐するログファイルは、パニックハングの分析に利用することができます。dsmd デーモンは、パニックハングイベントログに加え、208 ページの「ログファイルの維持管理」の説明のように、SC 上の重要なドメイン常駐ログの複製およびドメインコンソール出力のトランスクリプトを維持します。

反復ドメインパニック

パニックイベントから回復した直後に 2 番目のドメインパニックが検出された場合には、dsmd はそのドメインパニックを反復ドメインパニックイベントとして分類します。

反復ドメインパニックイベント後に再起動を試みる場合、パニックに対して行われる標準のロギング動作に加え、次のアクションが実行されます。

- 連続する反復ドメインパニックイベントでは、SMS は、管理者が指定した次の未試行の縮退設定に対して、より高い診断テストレベルで POST の実行を試行します (124 ページの「機能が低下した構成の設定の変更」を参照)。

- すべての縮退構成が試行されると、その後の反復ドメインパニックイベントは、最後に指定された縮退構成を使用して、フルテストレベルの起動を続行します。
- 反復ドメインパニックイベントが発生したことを確認すると、dsmd は、ただちに使用可能な ASR 方法を試行して、安定したドメインソフトウェア環境を起動します。dsmd デーモンは、すべての回復試行動作をドメイン固有のメッセージログに記録します。

Solaris ソフトウェアハングイベント

dsmd デーモンは、202 ページの「Solaris ソフトウェアのハートビート」で説明しているように、Solaris ソフトウェアの動作中に各ドメインの Solaris ハートビートを監視します (197 ページの「ソフトウェアのステータス」を参照)。ハートビートインジケータが一定期間更新されない場合、Solaris ソフトウェアハングイベントが発生します。

dsmd デーモンは Solaris ソフトウェアハングを検出します。

Solaris ハングを検出するとすぐに、dsmd はイベントをイベント情報を含めてドメイン固有のメッセージログに記録します。

dsmd は、Solaris ハングを検出するとすぐに、Solaris ハングの分析用のコアイメージを取得できるように、ドメインソフトウェアにパニックを発生させるよう要求します (172 ページの「ドメインの中止またはリセット」を参照)。SMS は、この回復アクションをドメイン固有のメッセージログに記録します。

dsmd デーモンは、ドメインソフトウェアがパニック要求に応じることができない場合を監視します。dsmd デーモンは、パニック要求に応じていないことを確認すると、ただちにドメインを終了させて (172 ページの「ドメインの中止またはリセット」を参照)、ASR 再起動を開始します。dsmd デーモンは、これらの回復アクションをドメイン固有のメッセージログに記録します。

パニックの結果として取得されたコアイメージは、そのドメインのみで分析に使用できますが、SC 常駐ログファイルはドメインハング分析の支援に使用できます。dsmd デーモンは、Solaris ハングイベントログに加え、SC 上の重要なドメイン常駐ログの複製およびドメインコンソール出力のトランスクリプトを保守できます。

ハードウェア構成イベント

ハードウェア構成ステータスの変更は、ハードウェア構成イベントと見なされます。esmd は、Sun Fire ハイエンドシステムで次のハードウェア構成イベントを検出します。

ホットプラグイベント

ホットプラグ可能ユニット (HPU) の挿入はホットプラグイベントです。次のアクションが発生します。

- SMS は、HPU 挿入イベントを検出し、各イベントと追加情報をプラットフォームメッセージログファイルに記録します。
- 挿入された HPU がドメインの論理構成でのシステムボードである場合、SMS はドメインのメッセージログファイルにその装着も記録します。

ホットアンプラグイベント

ホットプラグ可能ユニット (HPU) の取り外しはホットアンプラグイベントです。次のアクションが発生します。

- ホットアンプラグイベントが発生するとすぐに、SMS は HPU の取り外しをプラットフォームメッセージログファイルに記録するログエントリを作成します。
- 論理ドメイン構成からのシステムボードの取り外しを検出するホットアンプラグイベントは、該当するドメインのメッセージログファイルにその取り外しを記録します。

POST 初期化構成イベント

POST は、再起動や動的再構成などのドメイン関連イベントに応じて、適宜各種サーバーコンポーネントに対して実行できます。203 ページの「ハードウェア構成」の説明のように、SMS は POST からの状態とテスト失敗コンポーネントを識別する状態を含みます。このため、コンポーネントの POST ステータスの変更はハードウェア構成イベントと見なされます。SMS は、POST 主導のハードウェア構成の変更を、プラットフォームメッセージログに記録します。

環境イベント

一般に環境イベントは、ハードウェア状態測定値が通常の動作範囲を超えたときに検出されます。許容動作範囲は、ハードウェアとサーバー構成により異なります。

esmd デーモンは、各センサーから返された測定値が許容動作範囲内に収まっているかどうかを確認します。esmd デーモンは、許容動作範囲外のセンサー測定値をすべて環境イベントとしてプラットフォームログファイルに記録します。

また、esmd デーモンは、環境イベントに対する応答として実行された重要なアクション (情報の記録またはユーザー表示の更新より重要なアクションなど) もプラットフォームログファイルに記録します。

esmd デーモンは、1 つ以上のドメインに影響する重要な環境イベント応答アクションを、その影響を受けるドメインのログファイルに記録します。

esmd デーモンは、環境イベントが発生したハードウェアおよび無効なコンポーネントに依存している他のハードウェアを動作から除外することで、それらのイベントを処理します。ただし、そのハードウェアの動作を継続させても、ハードウェアの損傷またはハードウェア機能エラーが発生しない場合には、引き続き稼働させることもできます。

環境イベントの処理オプションは、イベントの特性により異なります。すべてのイベントには、それを処理しなければならない時間枠があります。イベントの中にはドメインソフトウェアを終了するもの、終了しないものがあります。イベント応答アクションは、esmd がそのイベントの時間枠で応答するものです。

esmd が環境イベントに行う応答は、ファン速度の高速化など数多くあります。電源切断を必要とする環境イベントが検出されると、esmd は次のいずれかの修正処置を実行します。

- esmd デーモンは、時間の制約を満たすオプションがほかにない場合には即時の電源切断を使用します。
- 環境イベントが即時電源切断を必要とせず、かつコンポーネントが MaxCPU ボードであれば、esmd は動作中のドメインから危険にさらされているボードを DR して、電源切断を試行します。
- 環境イベントが即時電源切断を必要とせず、かつコンポーネントがセンタープレーンサポートボード (CSB) なら、esmd はバストラフィックを再設定してもう 1 つの CSB のみを使用し、そのコンポーネントの電源切断を試行します。
- 環境イベントが即時電源切断を必要とせず、かつコンポーネントのボードの種類が MaxCPU と CSB 以外の場合、esmd はできるかぎり dsmd に環境条件を通知し、dsmd は正常型シャットダウンをドメインに送ります。ドメインは、コミットされていないメモリーバッファを物理記憶領域にフラッシュします。

ソフトウェアがまだ実行中であり、影響を受けたハードウェアの削除後に実行可能なドメイン構成が残っている場合は、dsmd はドメインの回復を試みます。

最後の 2 つのオプションのいずれかが指定の環境条件に割り振られた時間よりも長い時間を要する場合、esmd はドメインソフトウェアの状態とは無関係にコンポーネントの電源を即時切断します。

SMS は、環境イベントの原因として識別できるホットプラグ可能ユニットの障害インジケータを点灯させます。

環境イベント応答アクションにシステムコントローラのシャットダウンが含まれていないかぎり、ソフトウェア操作が環境イベントや次の応答アクションで終了されたすべてのドメインには、できるだけ早く ASR 再起動が行われます。

安全で正常な動作を保証するために Sun Fire ハイエンドシステムが課す制約に従って動作できる起動可能なハードウェアがある場合は、ASR 再起動がすぐに始まりません。

注 – (たとえば、両方の SC の電源を切断するよう要求されて) システムコントローラが動作しなくなると、Sun Fire ハイエンドプラットフォームの自己回復アクションが実行される可能性はまったくなくなります。この状況では、回復アクションの中には人間の介入を必要とするものがあります。外部監視エージェントは Sun Fire ハイエンドプラットフォームの動作を回復できない場合もありますが、そのエージェントは管理者に Sun Fire ハイエンドプラットフォームのシャットダウンを通知するうえで重要な役割を果たすことができます。

次の節では、Sun Fire ハイエンドシステム上で発生可能な各種の環境イベントについてももう少し詳しく説明します。

温度超過イベント

esmd デーモンは、高温になりすぎている Sun Fire ハイエンドシステムのハードウェアの温度測定値を監視します。臨界温度しきい値を超過した場合には、影響を受けるハードウェアの電源を切断することで、できるだけすみやかに処理します。温度が高くても臨界温度に達していない場合は、正常な停止や MCPU ボードの DR などのゆるやかな回復アクションを試みて対処します。

電源障害イベント

完全な電源障害が発生した場合、是正手段はほぼないといえます。正常な停止を行わずにプラグを抜き取ったときは、プラットフォーム全体、ドメイン、さらに SC が停止します。電源が回復すると、最終回復アクションが講じられます (173 ページの「電源投入時自己診断 (POST)」を参照)。

範囲外電圧イベント

Sun Fire ハイエンドシステムの電圧を監視して、範囲外イベントを検出します。範囲外電圧の処理は、219 ページの「環境イベント」の冒頭で概説した一般原則に従います。

電力不足イベント

168 ページの「電源制御」の説明のように、ボードの電源投入前に妥当な電力かどうかをチェックすることに加え、電源装置の障害ではサーバーが電力不足のままになることがあります。システムには、障害に備えて電源装置を冗長的に装備します。esmd デーモンは、大容量の電源装置ハードウェアの障害に対する応答として、ロギング以外にはどのようなアクションも実行しません。電流不足イベントの処理は、219 ページの「環境イベント」の冒頭で概説した一般原則に従います。

ファン障害イベント

esmd デーモンは、ファンが連続動作しているかどうかを監視します。ファンに障害があれば、ファン障害イベントが発生します。ファン障害の処理は、219 ページの「環境イベント」の冒頭で概説した一般原則に従います。

クロック障害イベント

esmd は、クロックが連続動作しているかどうかを監視します。クロックに障害が発生すると、esmd は 10 分ごとにメッセージをログに記録します。ボード上のクロックセレクタがそのクロックを使用して自動的に起動することがないように、手動によるオーバーライドを有効にすることもできます。クロックが正常な状態に戻ったときに、esmd は手動によるオーバーライドを無効にして、メッセージをログに記録します。

フェーズロックが失われると、esmd デーモンはすべてのボードでの手動によるオーバーライドを有効にして、メッセージをログに記録します。フェーズロックが元に戻ると、esmd はすべてのボードでの手動によるオーバーライドを無効にして、メッセージをログに記録します。

ハードウェアエラーイベント

204 ページの「ハードウェアエラーのステータス」の説明のように、Sun Fire ハイエンドシステムにハードウェアエラーが発生すると、複数のメカニズムにより SC で認識されます。SC で直接認識できるエラーの中には、PCI 割り込みによって SC 上の UltraSPARC プロセッサに直接報告されるものと、Sun Fire ハイエンドシステムのハードウェアレジスタの監視を通じてのみ検出されるものがあります。

上記以外にも、ドメインで動作中のプロセッサにより検出されるハードウェアエラーがあります。ドメインで動作中のドメインソフトウェアは、それらエラーがドメインで発生していることを検出し、そのエラーを SC に報告します。SC がハードウェアエラーの発生を認識するメカニズムと同じように、ハードウェアエラー後にハードウェアが保持するエラー状態は、個々のエラーにより異なります。

dsmd デーモンは次の機能を実行します。

- SC が認識できるすべてのハードウェアエラーを検出するのに必要なメカニズムを実装します
- ドメインソフトウェアインタフェースを実装し、ドメイン検出ハードウェアエラーの報告を受け取ります
- ハードウェアエラーのデータを収集し、エラー状態を解消します
- ハードウェアエラーと関連情報を必要に応じてプラットフォームメッセージログに記録します
- 影響を受けたすべてのドメインのドメインメッセージログファイルに、ハードウェアエラーを記録します

ハードウェアエラーに応じて収集されたデータがログファイルへの記録に適していない場合は、SC 上の `/var/opt/SUNWSMS/adm/domain-id/dump` 内の一意の名前のファイルに保存できます。

SMS は、ハードウェアエラーの原因として識別できるホットプラグ可能なユニットの障害 LED を点灯させます。

ハードウェアエラーに対する応答として実行されるアクション (前述のような情報の収集および記録以外) には 2 つの要素があります。まず、障害を特定されたハードウェアを使用しないようにすると、特定種類のハードウェアエラーをそれ以上発生しないようにできます。次に、ハードウェアエラーの結果としてクラッシュしたすべてのドメイン、または最初の種類のアクションの結果として停止したすべてのドメインには、ASR 再起動アクションが実行されます。

注 - ハードウェアが停止されておらず、障害が発生していると識別されていない場合でも、ASR 再起動アクションは完全な POST 検証の対象になります。POST は、テストに不合格のハードウェアコンポーネントを、ハードウェア構成から削除します。

検出された各ハードウェアエラー、およびドメインソフトウェアから報告された各ハードウェアエラーに応答して、`dsmd` は適切な是正措置を講じます。自動診断とドメイン回復が行われる場合もあれば (第 6 章を参照)、ハードウェアエラーによって停止したドメインごとに、完全な POST 検証を伴う ASR 再起動が開始される場合もあります。

注 – ハードウェアエラー後のドメインの ASR 再起動に伴う問題は、214 ページの「ドメイン起動の障害」の説明のように、ドメイン起動失敗イベントとして検出され、回復アクションが実行されます。

`dsmd` デーモンは、ハードウェアエラーに対する応答として実行されるすべての重要なアクション (情報の記録またはユーザー表示の更新より重要なアクションなど) をプラットフォームログファイルに記録します。ハードウェアエラーが 1 つまたは複数のドメインに影響を与えると、`dsmd` は影響を受けたドメインのメッセージログファイルに重要な応答アクションを記録します。

以下では、Sun Fire ハイエンドシステムで検出および処理されるハードウェアエラーの種類を簡単に説明します。

ドメイン停止イベント

ドメイン停止は、影響を受けたドメインをただちに終了させる回復不能のハードウェアエラーです。ハードウェア状態ダンプは、影響を受けたドメインの ASR 再起動を `dsmd` が初期化する前に取得されます。これらのファイルは、`/var/opt/SUNWSMS/adm/domain-id/dump` に格納されます。

`dsmd` デーモンは、これらのイベントをドメインメッセージログファイルに記録します。また、イベントログファイルにも記録します。

CPU 検出イベント

`RED_state` またはウォッチドッグのリセットは、低レベルのドメインソフトウェア (OpenBoot PROM または `kadb`) にトラップされます。これらのリセットはエラーを報告し、ドメインの ASR 再起動の初期化を要求します。

XIR 信号 (`reset -x`) も低レベルのドメインソフトウェア (OpenBoot PROM または `kadb`) にトラップされます。これはソフトウェアの制御を保持します。ドメインは手動で再起動しなければなりません。

レコード停止イベント

修正可能なデータ伝送エラー (CE ECC エラーなど) が原因で、Sun Fire ハイエンドシステムの ASIC の通常のトランザクション履歴レコード機能が停止することがあります。SMS は、伝送エラーをレコード停止として報告します。SMS はこれらの ASIC のトランザクション履歴バッファをダンプし、レコード停止を処理するときにトランザクション履歴レコード機能をふたたび有効にします。dsmd デーモンは、ドメインログファイルにレコード停止を記録します。

他の ASIC 障害イベント

ドメイン停止またはレコード停止以外の ASIC 検出ハードウェア障害には、コンソールバスエラーがあります。これは、ドメインに影響する場合としない場合があります。ハードウェア自体はどのドメインも終了させませんが、ドメインソフトウェアはハードウェア障害に耐えられないか、またはパニックまたはハングを起こすことがあります。dsmd デーモンは、ドメインログファイルにイベントを記録します。

SC 障害イベント

SMS は、メインの SC ハードウェアと実行中のソフトウェア状態のほか、スペアの SC が存在すればそのハードウェアと実行中のソフトウェアを監視します。利用度の高い SC 構成では、SMS は自動 SC フェイルオーバー処理により、メインの SC 上のハードウェアまたはソフトウェアの障害や、メインの SC へのハードウェア制御パス (たとえば、コンソールバスや内部ネットワーク接続) で検出された障害を処理します。これは、メインの責任をスペアの SC に譲渡し、旧メインの SC を (不具合の可能性のある) スペアとして残します。

SMS は、メインとスペアの SC のハードウェアに障害があるかどうかを監視します。

SMS は、ハードウェア障害と関連情報をプラットフォームメッセージログに記録します。

SMS は、特定されたハードウェア障害によってシステムコントローラ上の障害 LED を点灯させます。

詳細は、第 12 章を参照してください。

第12章

SC フェイルオーバー

SC フェイルオーバーは、Sun Fire ハイエンドシステムの管理操作に高可用性機能を追加して、システムの稼働時間を最大にします。Sun Fire ハイエンドシステムには2つのSCがあります。フェイルオーバーは、高可用性の2つのSCシステム構成のソフトウェアをサポートします。

メインSCは、Sun Fire ハイエンドシステム全体のすべての資源を提供します。メインSC上、またはメインSCからほかのシステムデバイスへのハードウェア制御パス(制御バスインタフェースやEthernetインタフェースなど)上でハードウェアまたはソフトウェアの障害が発生すると、SCフェイルオーバーソフトウェアは自動的にスペアSCへのフェイルオーバーを引き起こします。スペアSCは、メインSCとして動作することを認識して、すべてのメインSCの処理を継続します。2つのSCを使用する高可用性システム構成では、SMSのデータ、構成、ログファイルはスペアSC上に複製されます。アクティブドメインは、この切り換えの影響は受けません。

注 – フェイルオーバーをサポートするには、両方のSCで同一バージョンのSolaris OSおよびSMSソフトウェアが構成されている必要があります。

この章では、以下の項目を説明します。

- 226 ページの「概要」
- 227 ページの「障害の監視」
- 228 ページの「ファイルの伝達」
- 229 ページの「フェイルオーバーの管理」
- 230 ページの「フェイルオーバーのCLIコマンド」
- 234 ページの「コマンド同期」
- 236 ページの「データの同期」
- 238 ページの「障害および回復」
- 245 ページの「セキュリティ」

概要

現在の高可用性 SC 構成では、一方の SC は他方の SC に対する「ホットスペア」として機能します。

フェイルオーバーは、Sun Fire ハイエンドシステムの管理で単独ポイントの障害を除去します。fomd デーモンは、可能なかぎり多くの複数ポイント障害を特定して処理します。フェイルオーバーのシナリオは、238 ページの「障害および回復」に示してあります。

SC フェイルオーバーのどの時点でも、SC の一時的なサービスの停止を除いて、フェイルオーバープロセスが構成済みまたは実行中のドメインに悪影響を与えることはありません。

高可用性 SC システムでの処理は以下のようになります。

- メイン SC でソフトウェア障害またはハードウェア障害が検出されると、fomd は自動的にスペア SC に対してフェイルオーバーを行います。
- スペア SC は、メイン SC との通信が停止したことを検出すると、テイクオーバーを起動してメインの役割を引き継ぎます。

SC フェイルオーバーメカニズムの中心には、フェイルオーバー管理デーモン (fomd (1M)) があります。このデーモンは、メインとスペアの両方の SC にインストールされます。

fomd デーモンは以下の処理を実行します。

- SC の役割 (メインまたはスペア) を判定します。
- 定期的な健全性ステータスのメッセージ要求という形で、遠隔 SC のハードウェアとソフトウェアの全般的な健全性ステータスを要求します。このメッセージは、2 つの SC 間に存在する SMS 管理ネットワーク (MAN) を介して送信されます。
- 回復可能および回復不能なハードウェアおよびソフトウェアの障害の確認と処理を行います。
- 2 つの SC 間で制御分割の状態が発生する可能性を排除するため、あらゆる試みを行います。「制御分割」とは、両方の SC がそれぞれをメイン SC であると見なす場合をいいます。
- メイン SC の障害から回復するための時間を 5 ～ 8 分用意します。回復時間に含まれるのは、fomd が障害を検出し、障害について了解して、メイン SC の処理をスペア SC に引き継ぐまでの時間です。
- SC フェイルオーバーの発生をプラットフォームのメッセージログに記録します。

SC フェイルオーバーの影響を受けるサービスは以下のとおりです。

- すべてのネットワーク接続
- SC からドメインおよびドメインから SC への IOSRAM 通信またはメールボックス通信

■ メイン SC で動作しているあらゆるプロセス

接続を確立するために、メイン SC のホスト名を把握している必要はありません。SMS の構成 (smsconfig (1M) のマニュアルページを参照) の一環として、論理ホスト名が作成されています。これはメイン SC で常にアクティブになります。使用しているネットワークデータベースでの論理ホスト名の作成に関する情報は、『Sun Fire 15K/12K システムサイト計画の手引き』および『System Management Services (SMS) 1.6 インストールマニュアル』を参照してください。

SC フェイルオーバーで影響を受けた処理は、フェイルオーバーの完了後に回復することができます。影響を受けた処理を再起動すると、その処理が再開して完了するまで実行されます。

fomd が提供するすべての自動処理機能は、オペレータが SC フェイルオーバー後に介入しなくても再開します。完了の前に SC フェイルオーバーによって割り込まれた回復アクションが再開します。

障害の監視

フェイルオーバーには 3 つのタイプがあります。

1. メイン起動

メイン主導フェイルオーバーでは、回復不能なローカルのハードウェアまたはソフトウェア障害、あるいはオペレータの要求のいずれかに対する応答として、メイン SC で実行中の fomd がスペア SC に制御を渡します。

2. スペア起動 (テイクオーバー)

スペア主導フェイルオーバー (テイクオーバー) では、スペアで実行中の fomd によって、メイン SC が正常に動作していないと判断されます。

3. 間接トリガーのテイクオーバー

SC 間の I2 ネットワークパスが停止し、メインに障害がある場合、メインは自身をスペアの役割に切り替えます。これを検出したスペア SC は、メインの役割になります。

最後の 2 つのシナリオでは、スペア側の fomd がメイン SC をリセットすることによって、メインの並存が回避されます。

ソフトウェアの制御またはユーザーの指示によりフェイルオーバーが発生すると、fomd はフェイルオーバーメカニズムを無効にします。そのため、2 つの SC 間での処理の継続が繰り返される可能性が回避されます。

ファイルの伝達

fomd の目的の 1 つは、2 つの SC 間に存在するインターコネクトを通してメイン SC からスペア SC にデータを伝達することです。このデータの中には、構成、データ、ログのファイルが含まれます。

fomd デーモンは以下の処理を実行します。

- すべての SMS 固有ファイルを、起動時にメインからスペアの SC に伝達します。この中に含まれるのは、すべてのドメインデータディレクトリ、pcd 構成ファイル、/etc/opt/SUNWSMS/config ディレクトリ、/var/opt/SUNWSMS/adm のプラットフォームとドメインのファイル、.logger ファイルです。ユーザーが作成したアプリケーションファイルは、cmdsycn スクリプトで指定されていなければ伝達されません。
- 前回の伝達サイクル以降に変更されたファイルだけが伝達されます。
- フェイルオーバーでは、スペア SC がメインの役割を引き継ぐ前に、すべての変更済みの SMS ファイルを伝達します。

データを転送するには、I2 ネットワークが稼働している必要があります。

注 一方の SC で smsconfig -m を使ってネットワーク構成に変更を加えた場合には、もう一方の SC にも必ず同じ変更を加えてください。ネットワーク構成が、他方の SC に自動的に反映されることはありません。

2 つの SC 間の両方のインターコネクトに問題がある場合でも、メインおよびスペアの SC の高可用性 SRAM (HASRAM) に対するアクセスが完全であれば、フェイルオーバーは行われます。両方のインターコネクトに障害があれば、SMS データの伝達は行われず、スペア SC で同様のデータが作成されます。フェイルオーバーでは、新しいメインの fomd はデータの現在の状態を維持し、その状態を記録して、データの現在の状態に関する情報をほかの SMS デーモンと SMS クライアントに提供します。

2 つの SC 間のどちらかのインターコネクトがふたたび健全になると、各 SMS ファイルの時刻表示に応じてデータが転送されます。ファイルの時刻表示が現在のスペア SC のものより前なら、そのファイルは転送されます。ファイルの時刻表示がスペア SC のものより後なら、何も処理されません。

フェイルオーバーは、以下の 2 つの条件がどちらも満たされる場合は発生しません。

- 2 つの SC の両方のインターコネクトに障害があります
- 両方の HASRAM へのアクセスに障害があります

この場合は、四重障害と見なされ、フェイルオーバーは 1 つ以上のリンクが復元されるまで無効になります。

フェイルオーバーの管理

この節では、起動、メイン SC の役割、およびスペア SC の役割について説明します。

起動

注 – Solaris OS バージョンが異なるメイン SC とスペア SC 間のフェイルオーバーは、Sun 構成としてサポートされません。

フェイルオーバーソフトウェアが動作するためには、システムに 2 つの SC が存在する必要があります。メインおよびスペアの役割の判定には、一部で SC 番号を使用します。このスロット番号は、指定された SC がどちらかの役割を担う妨げにはなりません。役割の引き継ぎ方法を制御するだけです。

SMS が先に起動した方の SC がメインになります。両方の SC 上で SMS が実質的に同時に起動した場合には、他方の SC がメインでない、または他方の SC で SMS が実行されていないと先に判定した方の SC がメインになります。

起動中の SC0 が SC1 に役割を問い合わせた結果、SC1 の役割が確定できないと、SC0 がメインになります。SC0 はこの過程で SC1 をリセットします。SC1 をリセットするのは、メイン SC の並存 (分割ブレイクとして知られる状態) を避けるためです。フェイルオーバー機能が無効な場合でも、このリセット処理は実行されます。

メイン SC

メイン SC で実行中の fomd は、起動時にハードウェアとネットワークインタフェースの定期テストを開始します。最初は、健全性を示す 1 つ以上のステータス応答を遠隔 (スペア) SC から受け付けられないかぎり、フェイルオーバーメカニズムは (内部で) 使用不可になります。

最初の起動時にメインの fomd がローカルの障害を検出すると、以下のすべての条件が満たされる場合にフェイルオーバーが行われます。

1. I2 ネットワークが障害の原因ではない。
2. 遠隔 SC が健全ある (健全性ステータス応答で指示される)。
3. フェイルオーバーメカニズムが無効になっていない。

スペア SC

起動時は、スペア SC で fomd が稼働してソフトウェア、ハードウェア、ネットワークインタフェースの定期テストを開始します。

最初の起動時にスペア SC で実行中の fomd は、ローカルの障害を検出すると問題点があることをメインの fomd に通知します。

フェイルオーバーの CLI コマンド

この節では、setfailover コマンドおよび showfailover コマンドについて説明します。

setfailover コマンド

setfailover コマンドは、SC フェイルオーバーメカニズムの状態を変更します。デフォルトの状態は on です。次に、setfailover コマンドの使用例を示します。

```
# setfailover [-q] [-y|-n] [on|off|force]
```

クロックに障害のあるスペア SC へのフェイルオーバーを強制すると、影響を受けるドメインでドメイン停止 (dstop) が発生することがあります。setfailover コマンドは、スペア SC 上の障害のあるクロックを検出し、障害のある SC へのフェイルオーバーを誤って強制することがないように、もう一度確認するためのプロンプトを表示します。ただし、-q (非出力) オプションおよび -y (すべてのプロンプトに yes) オプションを指定すると、障害のある SC を確認できません。



注意 - -q オプションを指定すると、確認プロンプトを含むすべてのプロンプトが抑制されます。-q オプションと -y オプションの両方を指定すると、スペア SC に障害があっても、スペア SC へのフェイルオーバーが強制されます。SC に障害がある場合は、この強制フェイルオーバーによって Dstop が発生する可能性があります。

次に、スペア SC 上の障害のあるクロックを検出する `setfailover` コマンドの例を示します。

```
# setfailover force
Forcing failover. Do you want to continue (yes/no)? yes
The spare clock input on some boards might be bad. Forcing a
failover now is likely to cause the affected domains to domain stop
(Dstop).
Do you want to continue (yes/no)? no
```

表 12-1 では、SC フェイルオーバーの状態について説明します。

表 12-1 フェイルオーバーの状態を変更するためのオプション

状態	意味
<code>[-q]</code>	非表示モードを有効にします。この場合、プロンプトを含め、 <code>stdout</code> に対するすべてのメッセージが抑制されます。単独で使用されると、 <code>-q</code> はデフォルトですべてのプロンプトに対して <code>-n</code> オプションを指定します。 <code>-y</code> オプションまたは <code>-n</code> オプションのどちらかとともに使用すると、 <code>-q</code> はすべてのユーザープロンプトを抑制し、選択されたオプションに基づいて自動的に <code>yes</code> または <code>no</code> で応答します。
<code>[-y -n]</code>	<code>-y</code> を指定すると、すべてのプロンプトに対して自動的に <code>yes</code> と応答します。プロンプトは、 <code>-q</code> オプションとともに使用しないかぎり表示されます。このオプションは慎重に使用してください。 <code>-n</code> を指定すると、すべてのプロンプトに自動的に <code>no</code> と応答します。プロンプトは、 <code>-q</code> オプションとともに使用しないかぎり表示されます。
<code>on</code>	フェイルオーバーまたはオペレータの要求により、フェイルオーバーが使用不可となっていたシステムのフェイルオーバーを使用可能にします。このオプションは、フェイルオーバーを再び使用可能にすることだけをコマンドに指示する。フェイルオーバーを再び使用可能にできない場合は、それ以降に <code>showfailover</code> コマンドを使用すると使用可能への移行を妨げた現在の障害が表示されます。
<code>off</code>	フェイルオーバーメカニズムを使用不可にします。このオプションは、メカニズムがふたたび使用可能になるまでフェイルオーバーを起動しません。
<code>force</code>	フェイルオーバーをスペア SC に強制します。スペア SC は、使用可能で健全でなければなりません。

注 – SMS 1.6 にパッチを適用する必要がある場合には、パッチをインストールする前にフェイルオーバーを使用不可にする必要があります。『System Management Services (SMS) 1.6 インストールマニュアル』を参照してください。

詳細と用例については、setfailover のマニュアルページを参照してください。

showfailover コマンド

showfailover コマンドでは、SC フェイルオーバーメカニズムの状態を監視し、現在のステータスを表示することができます。-v オプションは、すべての監視対象コンポーネントの現在のステータスを表示します。

```
xc30p13-sc0:sms-svc:13> showfailover -v
SC Failover Status:      ACTIVE
Status of Shared Memory:
HASRAM (CSB at CS0): .....Good
HASRAM (CSB at CS1): .....Good
Status of xc30p13-sc0:
Role: .....MAIN
SMS Daemons: .....Good
System Clock: .....Good
Private I2 Network: .....Good
Private HASRAM Network:.....Good
Public Network.....NOT TESTED
System Memory: .....38.9%
S Disk Status:
/: .....17.4%
Console Bus Status:
EXB at EX1: .....Good
EXB at EX2: .....Good
  EXB at EX4: .....Good
Status of xc30p13-sc1:
Role: .....SPARE
SMS Daemons: .....Good
System Clock: .....Good
Private I2 Network: .....Good
Private HASRAM Network:.....Good
Public Network: .....NOT TESTED
System Memory: .....34.2%
Disk Status:
/: .....17.1%
Console Bus Status:
EXB at EX1: .....Good
EXB at EX2: .....Good
EXB at EX4: .....Good
```

-r オプションは、SC の役割を表示します。役割には、メイン、スペア、未定義があります。たとえば、次のメッセージが表示されます。

```
sc0:sms-user:> showfailover -r
MAIN
```

オプションを指定しない場合は、次のように状態情報だけが表示されます。

```
sc0:sms-user:> showfailover
SC Failover Status: state
```

フェイルオーバーメカニズムには、ACTIVATING、ACTIVE、DISABLED、および FAILED の 4 つの状態があります。表 12-2 では、4 つの状態について説明します。

表 12-2 フェイルオーバーメカニズムの状態

状態	意味
ACTIVATING	フェイルオーバーメカニズムが ACTIVE 状態に移行する準備をしている状態。フェイルオーバーは、すべてのテストにパスし、ファイルの同期が完了した時点でアクティブになります。
ACTIVE	フェイルオーバーメカニズムが使用可能になり、正常に動作している状態。
DISABLED	フェイルオーバーの発生またはオペレータの要求 (setfailover をオフに指定) により、フェイルオーバーメカニズムが使用できなくなった状態。
FAILED	フェイルオーバーが可能になるのを妨げる障害をフェイルオーバーメカニズムが検出したか、あるいはフェイルオーバーがまだ完全にアクティブになっていません。

showfailover は、フェイルオーバープロセスが監視する各ネットワークインタフェースリンクの状態も表示します。表示形式は次のとおりです。

```
network iff device name: [GOOD|FAILED]
```

showfailover は、障害状態を表す障害文字列を返します。それぞれの障害文字列には、対応するコードがあります。以下の表に、コードおよび対応する障害文字列の定義を示します。

表 12-3 では、showfailover コマンドの障害文字列について説明します。

表 12-3 showfailover の障害文字列

文字列	説明
None	障害はありません。
S-SC EXT NET	スペア SC の外部ネットワークインタフェースに障害が発生しました。
S-SC CONSOLE BUS	スペア SC のコンソールバスのバスでエラーが検出されました。
S-SC LOC CLK	スペア SC のローカルクロックで障害が発生しました。
S-SC DISK FULL	スペア SC システムがフルです。
S-SC IS DOWN	スペア SC が停止しているか、応答しません。I2 ネットワークまたは HASRAM が停止していることが原因でこのメッセージが返された場合には、スペア SC は動作を継続している可能性があります。スペア SC にログインして確認してください。
S-SC MEM EXHAUSTED	スペア SC のメモリーまたはスワップ空間を使い果たしました。
S-SC SMS DAEMON	スペア SC 上で少なくとも 1 つの SMS デーモンが開始または再開できませんでした。
S-SC INCOMPATIBLE SMS VERSION	スペア SC で異なるバージョンの SMS ソフトウェアが動作している。両方の SC で同じバージョンの SMS を実行する必要があります。
I2 NETWORK/HASRAM DOWN	SC 間の通信インタフェースが 2 つとも停止している。スペア SC で動作している SMS のバージョンとその状態が、メイン SC 側で認識できません。スペア SC の停止を宣言し、その影響に関するメッセージのログを記録します。ファイル伝達など、依存するサービスは利用できなくなります。

詳細と用例については、showfailover のマニュアルページを参照してください。

コマンド同期

コマンドの実行中に SC フェイルオーバーが発生したときは、新しいメイン SC で同じコマンドを再起動することができます。

すべてのコマンドおよび処理は、以下の操作を実行します。

- コマンドまたは処理の開始を指定します。

- コマンドまたは処置の完了を取り消すか、または指示します。
- SMS がコマンドを再開する目的で使用できるすべての状態遷移および関連データを保持します

fomd は、次のコマンド同期サポートを提供します。

- フェイルオーバーのあとに影響を受けた任意のドメインまたはすべてのドメインの ASR 再起動を、自動的に再開するための dsmd (1M) に対するコマンド同期のサポート
- フェイルオーバーのあとの最後の DR 操作を再開するための、すべての SMS DR 関連デーモンと CLI に対するコマンド同期のサポート

コマンド同期のサポートを必要とする SMS の 4 つの CLI コマンドは、addboard、deleteboard、moveboard、rcfgadm です。

cmdsyc CLI

cmdsyc コマンドは、cmdsyc 記述子によるスクリプトまたはコマンドの初期化、既存の cmdsyc 記述子の実行ポイントの更新、またはスペア SC の回復アクションリストからの cmdsyc 記述子の取り消しの機能を提供します。コマンドまたはスクリプトは、cmdsyc 封筒でも実行可能です。

スペアへの SC フェイルオーバーでは、スペア SC での cmdsyc 記述子の初期化によって、最後の実行ポイントセットからの対象スクリプトまたはコマンドの再起動または再開をスペア SC で行うことができます。これらのコマンドはメイン SC でのみ実行されるものであり、スペアで実行されても現在の cmdsyc リストには影響しません。

使用可能なスペア SC がない場合には、cmdsyc コマンドでコマンドまたはスクリプトが起動されても処理は実行されません。つまり、コマンドは通常どおりに実行されますが、プラットフォームログのログエントリでは cmdsyc の実行が失敗したことが示されます。

initcmdsyc コマンド

initcmdsyc(1M) コマンドは、cmdsyc 記述子を作成します。対象のスクリプトやコマンドおよびそれらの関連パラメータは、cmdsyc データの一部として保存されます。*initcmdsyc* コマンドの終了コードは、処理を参照するためにそれ以降の cmdsyc コマンドで使用可能な cmdsyc 記述子を提供します。対象コマンドまたはスクリプトは実際には実行されません。詳細は、*initcmdsyc (1M)* のマニュアルページを参照してください。

savecmdsyc コマンド

savecmdsyc(1M) コマンドは、定義済みの cmdsyc 記述子に新しい実行ポイントを保存します。これにより、識別子に対応する位置で対象コマンドまたはスクリプトを再起動することができます。対象コマンドまたはスクリプトは、この実行ポイントでの再起動の機能をサポートします。実行ポイントが指定されていない場合は、対象のコマンドまたはスクリプトの先頭で再起動が実行されます。詳細は、savecmdsyc (1M) のマニュアルページを参照してください。

cancelcmdsyc コマンド

cancelcmdsyc(1M) コマンドは、スペアの再起動リストから cmdsyc 記述子を削除します。このコマンドを実行すると、cmdsyc 記述子に対応する対象コマンドまたはスクリプトはフェイルオーバーの際にスペア SC で再起動されません。すべての対象コマンドまたはスクリプトでは、正常または異常終了フローのあとに cancelcmdsyc シーケンスだけでなく initcmdsyc コマンドシーケンスも必ず含まれるように注意してください。詳細は、cancelcmdsyc (1M) のマニュアルページを参照してください。

runcmdsyc コマンド

runcmdsyc(1M) コマンドは、cmdsyc ラッパーの下で、指定された対象コマンドまたはスクリプトを実行します。先頭以外の実行ポイントでは再起動することはできません。対象のコマンドまたはスクリプトは、cmdsyc 記述子の作成の後でシステムコマンドを通して実行されます。システムコマンドの終了時に、cmdsyc リストから cmdsyc 記述子から削除され、システムコマンドの終了コードがユーザーに戻されます。詳細は、runcmdsyc (1M) のマニュアルページを参照してください。

showcmdsyc コマンド

showcmdsyc (1M) コマンドは、現在の cmdsyc 記述子リストを表示します。詳細は、showcmdsyc (1M) のマニュアルページを参照してください。

データの同期

SMS では、カスタマイズされたデータ同期が setdatasync(1M) コマンドによって提供されます。setdatasync を使用すると、データ伝達リストに追加する、またはリストから削除するユーザー作成ファイルを指定できます。

setdatasync コマンド

setdatasync では、自動フェイルオーバーのデータ同期プロセスの一環としてメインからスペアシステムコントローラ (SC) へコピーされるファイルを特定します。両方の SC において、指定するユーザーファイルとそのユーザーファイルの格納ディレクトリに対する読み取り、書き込み許可が必要です。また、プラットフォーム管理特権かドメイン管理特権も必要です。

データ同期プロセスでは、メイン SC 上のユーザー作成ファイルが変更されているかどうかチェックされます。メイン SC 上のユーザー作成ファイルが最後の伝達以降に変更されている場合は、スペア SC にも再伝達されています。デフォルトのデータ同期プロセスでは、指定されたファイルを 60 分ごとに調べますが、setdatasync を使用して、ユーザーファイルの変更の確認頻度を指定することもできます。

ファイルをデータ伝達リストに追加せずに、setdatasync コマンドを使用して、指定したファイルをスペア SC に伝達することもできます。

setdatasync backup を使用すると、fomd による自動ファイル伝達の速度を低下させる可能性があります。

setdatasync backup の実行に要する時間は、転送するファイル数に比例します。ファイル転送速度に影響を与えるその他の要素には、転送ファイルの平均サイズ、SC 上の利用可能メモリー量、SC の負荷 (CPU サイクルとディスクトラフィック)、I2 ネットワークが機能しているかどうかなどがあります。

次の統計情報は、平均ファイルサイズが 200K バイトであることを前提としています。

- I2 ネットワークが機能している、わずかに負荷がかかったシステムでは、FOMD は毎分約 750 ファイルを転送できます。
- I2 ネットワークが機能していない、わずかに負荷がかかったシステムでは、毎分約 250 ファイルの転送が可能です。

注 – このコマンドを使用する前に、再伝達の制約について理解しておくことをお勧めします。詳細および例については、setdatasync (1M) のマニュアルページを参照してください。

showdatasync コマンド

showdatasync コマンドを使用すると、メイン SC からスペア SC に伝達 (コピー) されるファイルの現在のステータスを表示できます。showdatasync コマンドは、setdatasync を使用して登録されたファイルとその状態のリストも提供します。データ適用は、スペア SC 上のデータをメイン SC 上のデータと同期して、SC フェイルオーバーが発生した場合にスペア SC がメイン SC とともに最新の状態になっているようにします。

詳細は、showdatasync (1M) のマニュアルページを参照してください。

障害および回復

高可用性構成では、fomd はローカルと遠隔の SC に対するフェイルオーバーメカニズムを管理します。fomd デーモンは、ローカルのハードウェアおよびソフトウェアの障害を検出して、実行すべき適切な措置を判断します。

fomd デーモンは、表 12-4 で説明する障害の検出を担当します。

表 12-4 fomd によるハードウェアおよびソフトウェアの障害カテゴリ

カテゴリ	説明
a	SC の制御ボード (CB)/CPU ボードに対してローカルなすべての関連ハードウェアバス
b	外部ネットワークインタフェース
c	SC 間の I2 ネットワークインタフェース
d	回復不能なソフトウェア障害。このカテゴリは、SMS ソフトウェアコンポーネント (デーモン) がクラッシュしてから 3 回の試行のあとで再起動できない場合、ファイルシステムがフルの場合、ヒープを使い果たした場合などに該当します。

図 12-1 にフェイルオーバーの障害カテゴリを示します。

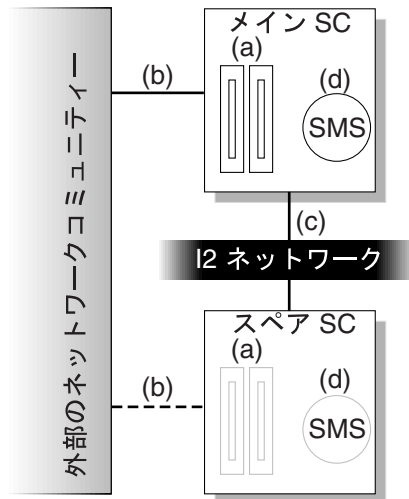


図 12-1 フェイルオーバーの障害カテゴリ

表 12-5 に、カテゴリがフェイルオーバーメカニズムにどのように影響するかを示します。フェイルオーバーメカニズムは稼動しているものとします。

表 12-5 フェイルオーバーの障害カテゴリ

障害ポイント	メイン SC	スペア SC	フェイルオーバー	注意
a	X		X	スペアへのフェイルオーバーの発生。
a		X	使用不可	メイン SC への影響はないが、スペア SC はハードウェア障害の影響を受けるためにフェイルオーバーは使用不可となります。
b	X			スペアへのフェイルオーバー。
b		X	影響なし	スペア SC の外部ネットワークインタフェースで障害が発生した場合は、フェイルオーバーメカニズムへの影響はありません。
c			影響なし	メインおよびスペアの SC は障害を記録します。
d	X		X	健全と見なされるスペア SC へのフェイルオーバー。
d		X	使用不可	このポイントではスペア SC は不健全と見なされるためにフェイルオーバーは使用不可となります。

メイン SC のフェイルオーバー (メイン制御のフェイルオーバー)

SC フェイルオーバー時のメインの fomd イベントは、次の順序で発生します。

1. 障害を検出します。
2. ハートビートの生成を停止します。
3. 遠隔のフェイルオーバーソフトウェアにテイクオーバータイマーの起動を通知します。このタイマーの目的は、何らかの理由でメインがハングアップしてカウント 10 まで達しない場合に、遠隔 (スペア) SC が処理を引き継ぐための代替手段を提供することです。
4. SMS ソフトウェアをスペアモードで起動します。
5. 論理 IP インタフェースを削除します。
6. コンソールバスのケーシングメカニズムを使用可能にします。

7. 変更されたすべての SMS ファイルのスペア SC または HASRAM への伝達を引き起こします。
8. ファイル伝達の監視を停止します。
9. メイン専用の各デーモンを終了し、メイン SC の役割を UNKNOWN に設定します。
10. スペアフェイルオーバーイベントを記録します。
11. メインの役割が引き継がれたことを、遠隔 (スペア) のフェイルオーバーソフトウェアに通知します。スペアに通知する前にテイクオーバータイマーが期限切れになると、遠隔 SC が自発的に処理を引き継ぎます。

フェイルオーバー時のスペアの fomd イベントは、次の順序で発生します。

1. メインの fomd からメッセージを受け取ってメインの役割を引き継ぐか、テイクオーバータイマーがタイムアウトします。メッセージを受け取った場合は、テイクオーバータイマーは停止します。
2. 前のメイン SC をリセットします。
3. スペア fomb をメインの役割に構成するよう hwad、frad および mand に通知します。
4. メインの役割を引き継ぎます。
5. ハートビート割り込みの生成を開始します。
6. 論理 IP インタフェースを設定します。
7. コンソールバスのケーシングメカニズムを使用不可にします。
8. SMS ソフトウェアをメインモードで起動します。
9. 割り込みを受信する DARB をセットアップします。
10. スペアからメインへの逆方向の役割イベントを記録します。
11. これでスペア SC はメインとなり、fomd がフェイルオーバーメカニズムを非アクティブにします。

メイン SC の障害 (スペアがメインの役割を引き継ぐ場合)

このシナリオでは、メイン SC との通信の喪失に反応してスペア SC がメインの制御を引き継ぎます。このタイプのフェイルオーバーのもっとも重要な側面は、制御分割条件の防止です。もう 1 つの前提条件は、フェイルオーバーメカニズムが非アクティブになっていないことです。非アクティブになっていると、テイクオーバーは実行されません。

スペアの fomd は以下の処理を実行します。

- メイン SC が健全であることを確認します。

スペアの fomd から見ると、この現象は 2 つの条件によって引き起こされる可能性があります。2 つの条件とは、メイン SC がまったく動作していない場合と、I2 ネットワークインタフェースが停止している場合です。

前者の場合にはフェイルオーバーが必要ですが (フェイルオーバーメカニズムがアクティブな場合)、後者の場合は不要です。どちらのケースかを特定するために、スペアの fomd はメイン SC からハートビート割り込みの存在をポーリングして、メイン SC が稼働中であることを判定します。ハートビート割り込みが受信されている場合、あるいはフェイルオーバーメカニズムが非アクティブまたは無効になっている場合は、フェイルオーバーは発生しません。

割り込みが検出されていないが、フェイルオーバーメカニズムが非アクティブな場合には、オペレータが CLI コマンドの `setfailover` を使用してフェイルオーバーメカニズムを手動でアクティブにしないかぎり、スペアの fomd はテイクオーバーを試行しません。それ以外は、スペア SC が健全なら、スペアの fomd はメインの役割の引き継ぎに進みます。

- 遠隔 (メイン) SC のリセットによりテイクオーバーを開始します。

以下に、フェイルオーバーでのスペアの fomd のイベントを順番に示します。

1. 自分自身をメインとして再構成します。この中には、I²C バスの制御の引き継ぎ、メイン SC の論理 IP アドレスの設定、必要な SMS ソフトウェアデーモンの起動が含まれます。
2. ハートビート割り込みの生成を開始します。
3. 論理 IP インタフェースを設定します。
4. コンソールバスのケーシングを使用不可にします。
5. SMS ソフトウェアをメインモードで起動します。
6. DARB 割り込みを設定します。
7. テイクオーバーイベントを記録します。
8. これで、スペアの fomd はメインとなり、フェイルオーバーメカニズムをオフにします。

I2 ネットワークの障害

以下に、I2 ネットワーク障害の後で発生するイベントを順番に示します。

1. メインの fomd は、I2 ネットワークが健全ではないことを検出します。
2. メインの fomd は、スペア SC へのファイルの伝達とデータのチェックポイント処理を停止します。
3. スペアの fomd は、I2 ネットワークが健全ではないことを検出します。
スペアの fomd から見ると、この現象は2つの条件によって引き起こされます。メイン SC が完全な誤動作を起こしている場合および I2 ネットワークインタフェースが停止している場合です。前者の場合の適切な処置はフェイルオーバーですが、後者では違います。どちらのケースかを特定するために、fomd はメイン SC からハートビート割り込みの存在をポーリングして、メイン SC が稼働中であることを判定します。ハートビート割り込みが存在する場合は、fomd はスペアをスペアのままだに保持します。
4. スペアの fomd は、ローカルディスクのチェックポイントデータをクリアします。

メイン SC の障害 (I2 ネットワークも停止している場合)

以下に、メイン SC の障害の後で発生するイベントを順番に示します。

1. メインの fomd は障害を検出します。
直前に通知されたスペア SC の状態が健全であった場合は、メインの fomd はハートビートの生成を中止します。それ以外は、フェイルオーバーは継続されません。
コンソールバスへのアクセスが依然として使用可能であれば、メインのフェイルオーバーソフトウェアは残りのすべての重要ファイルの HASRAM への伝達を完了して、任意またはすべての重要な状態情報を HASRAM にフラッシュします。
2. メインの fomd は、SMS ソフトウェアをスペアモードに再構成します。
3. メインの fomd は、メイン SC の論理 IP アドレスを削除します。
4. メインの fomd は、ハートビート割り込みの生成を停止します。

障害の回復および再起動

この節では、障害の回復および再起動のプロセスについて説明します。

12 障害の回復

以下に、I2 ネットワークの障害回復で発生するイベントを順番に示します。

1. メインの fomd は、I2 ネットワークが健全であることを検出します。
健全性ステータスの応答メッセージによってスペア SC の健全性が指示されると、fomd はフェイルオーバーを使用可能にして、フェイルオーバーメカニズムはオペレータによってオフにされていないと見なし、ログファイルの完全な再同期を実行してスペア SC に対してデータのチェックポイント処理を行います。
2. スペアの fomd は、I2 ネットワークが健全であることを検出します。
スペアの fomd は、フェイルオーバーを使用不可にしてローカルディスクのチェックポイントデータをクリアします。

再起動および回復

以下に、再起動および回復で発生するイベントを順番に示します。再起動および回復のシナリオは、2 つの状況で発生します。

メイン SC がマスターリセットを受信するか、メイン SC の UltraSPARC プロセッサがリセットを受信する場合

1. SSCPOST は問題なく合格したものとします。SSCPOST が失敗して OS が起動できなければ、そのメインは稼働できない状態です。
2. すべての SSC Solaris ドライバは問題なく組み込まれているものとします。SBBC ドライバが組み込まれない場合は、241 ページの「メイン SC の障害 (スペアがメインの役割を引き継ぐ場合)」を参照してください。ほかにも組み込まれないドライバがある場合は、239 ページの「メイン SC のフェイルオーバー (メイン制御のフェイルオーバー)」を参照してください。
3. メインの fomd が起動します。
4. 遠隔 SC がすでにメインの役割を引き継いでいると fomd が判定した場合は、244 ページの「スペア SC がマスターリセットを受信するか、スペア SC の UltraSPARC プロセッサがリセットを受信する場合」の 5 を参照してください。それ以外は、この手順の 5 に進みます。
5. fomd は、メインの論理 IP アドレスを設定し、残りの SMS ソフトウェアを起動します。
6. SMS デーモンは、必要に応じて回復モードで起動します。
7. メインの fomd は、ハートビート割り込みの生成を開始します。
8. この時点で、メイン SC は完全に回復します。

スペア SC がマスターリセットを受信するか、スペア SC の UltraSPARC プロセッサがリセットを受信する場合

1. SSCPOST は問題なく合格したものとします。SSCPOST が失敗して OS が起動できなければ、そのスペアは稼働できない状態です。
2. すべての SSC Solaris ドライバは問題なく組み込まれているものとします。SBBC ドライバが組み込まれない場合、またはそれ以外のドライバが組み込まれない場合は、スペア SC は稼働不能と見なされます。
3. fomd が起動します。
4. fomd は、SC を適切なスペアであると判定してスペアの役割を引き継ぎます。
5. fomd は、遠隔 (最初にメインであると見なされる) SC からのハートビート割り込みの存在をチェックします。
構成可能な時間が経過してもハートビート割り込みが検出されない場合は、フェイルオーバーメカニズムの状態が確認されます。使用可能でかつ起動されていれば、fomd はテイクオーバーを起動します。243 ページの「メイン SC がマスターリセットを受信するか、メイン SC の UltraSPARC プロセッサがリセットを受信する場合」の「5」を参照してください。それ以外は、fomd はハートビート割り込みの存在およびフェイルオーバーメカニズムの状態の監視を継続します。
6. fomd は、ハードウェア、ソフトウェア、およびネットワークインタフェースの定期チェックを開始します。
7. fomd は、ローカルのメイン SC の IP アドレスを設定します。
8. この時点で、スペア SC は完全に回復します。

クライアントフェイルオーバーの回復

以下に、クライアントフェイルオーバーの回復で発生するイベントを示します。回復のシナリオは、以下の 2 つのケースで発生します。

メイン SC の障害 – スペア SC からの回復

何らかの処理を実行中のクライアントは、再発データのチェックポイント処理を行うことで手動で回復されます。

メイン SC の障害 (I2 ネットワークが停止している場合) – スペア SC からの回復

I2 ネットワークが停止しているため、すべてのチェックポイントデータが削除されます。クライアントは、回復を実行することはできません。

回復を完了した時点で、再起動手順を続行できます。

メイン SC の再起動 (スペア SC が停止している場合)

状況は、244 ページの「メイン SC の障害 - スペア SC からの回復」と同じです。

スペア SC の再起動

回復は必要ありません。

セキュリティ

フェイルオーバー固有のすべてのネットワークトラフィック (健全性ステータス要求または応答メッセージやファイル伝達パケット) は、2 つの SC 間に存在するインターコネクトネットワークを介してのみ送信されます。

第13章

SMS ユーティリティー

この章では、SMS のバックアップ、構成、復元、バージョンのユーティリティーについて解説します。これらのユーティリティーの詳細および例については、『System Management Services (SMS) 1.6 リファレンスマニュアル』およびオンラインのマニュアルページを参照してください。

この章では、以下の項目を説明します。

- 247 ページの「SMS バックアップユーティリティー」
- 248 ページの「SMS 復元ユーティリティー」
- 249 ページの「SMS バージョンユーティリティー」
- 252 ページの「SMS 構成ユーティリティー」

SMS バックアップユーティリティー

smsbackup は、SMS のオペレーティング環境を維持管理するファイルの cpio (1) アーカイブを作成します。

注 – このユーティリティーは SC 上で実行します。このユーティリティーを使用しても、SC やドメインの OS とドメインのアプリケーションデータを定期的または適宜にバックアップする必要がなくなるわけではありません。

ドメインへのボードの追加またはドメインからのボードの削除などで、SMS 環境を変更したときは、システムコントローラの現在のバックアップファイルを維持するために smsbackup を必ず再実行してください。

バックアップファイルの名前は smsbackup.X.X.cpio です。X.X はバックアップを行なったアクティブなバージョンを表します。

smsbackup ユーティリティーは、すべての構成、プラットフォーム構成データベース、SMS、およびログファイルを保存します。つまり、SMS はバックアップを作成したときの作業状態に SMS を戻すのに必要なすべてを保存します。

バックアップは、自動的には実行されません。SMS 環境を変更するときは、バックアップを実行する必要があります。この処理は、サイトの要件に応じて定期的に行われる root cron ジョブに組み込んで自動化することができます。

バックアップのログファイルは、`/var/sadm/system/logs/smsbackup` に格納されます。smsbackup を実行するときは、対象となる位置を指定する必要があります。

注 - 対象となる位置は、有効な UNIX ファイルシステム (UFS) ディレクトリである必要があります。smsbackup は、一時的なファイルシステムディレクトリに対して実行することはできません。

smsbackup を実行すると、処理の成功または失敗が必ず通知されます。

smsbackup を実行するには、スーパーユーザー特権が必要です。詳細と用例については、smsbackup のマニュアルページを参照してください。

SMS バックアップファイルを `smsrestore (1M)` コマンドを使用して復元します。

SMS 復元ユーティリティー

smsrestore ユーティリティーは、smsbackup(1M) によって作成されたバックアップファイルから SMS のオペレーティング環境を復元します。新しいディスクに SMS ソフトウェアをインストールした後またはハードウェアの交換や追加の後には、smsrestore を使用して SMS 環境を復元することができます。smsrestore を正しく実行するには、事前にフェイルオーバーを無効化し、SMS を停止しておく必要があります。詳細は、『System Management Services (SMS) 1.6 インストールマニュアル』の「SMS の停止および開始」を参照してください。

エラーが発生した場合は、smsrestore がエラーメッセージを `/var/sadm/system/logs/smsrestore` に書き込みます。

注 - このユーティリティーは SC 上で実行され、SC の OS、ドメインの OS、またはドメインのアプリケーションデータは復元しません。

smsrestore ユーティリティーは、バックアップされていないファイルを復元することはできません。ドメインの停止などで SMS 環境を変更したときは、システムコントローラの現在のバックアップファイルを維持するために smsbackup を必ず再実行してください。

smsrestore を実行するには、スーパーユーザー特権が必要です。詳細と用例については、smsrestore のマニュアルページを参照してください。

SMS バージョンユーティリティー

smsversion(1M) ユーティリティーは、同一の OS に共存している連続バージョンの SMS を管理します。SMS の連続バージョンとは、SMS 1.5 と SMS 1.6 など、バージョン番号が連続しているバージョンです。つまり、smsversion を使用して SMS 1.2 と SMS 1.6 を、または SMS 1.4.1 から SMS 1.6 へ直接切り替えることはできません。

注 – バージョンを SMS 1.6 から以前にインストールしたバージョンに切り替えると、SC のセキュリティに影響が生じます。『System Management Services (SMS) 1.6 インストールマニュアル』の「SMS のバージョンの切り替え」を参照してください。

smsversion ユーティリティーを使用すると、同じ OS 上に共存している連続したバージョンの SMS を双方向に切り替えることができます。表 13-1 に、これを使用する場合の条件を示します。

表 13-1 SMS バージョン間の切り替え

条件	説明
新機能	新バージョンの SMS でサポートされている機能 (デフォルト機能による SC のセキュリティ保護など) は、旧バージョンではサポートされない場合があります。SMS を古いバージョンに切り替えると、これら新機能が失われる場合があります。また、新機能の設定が失われる場合もあります。

条件	説明
フラッシュPROMの違い	SMS のバージョンを切り替える場合、CPU フラッシュ PROM を、正しいファイルを使用して再フラッシュする必要があります。これらファイルは、 <code>/opt/SUNWSMS SMS_version/firmware</code> ディレクトリに格納されています。バージョンを切り替えた後、 <code>flashupdate (1M)</code> を使用して PROM を再フラッシュします。フラッシュ PROM の更新についての詳細は、 <code>flashupdate</code> マニュアルページと『System Management Services (SMS) 1.6 インストールマニュアル』を参照してください。

連続リリースの SMS を切り替える場合、たとえば SMS 1.6 を SMS 1.5 に切り替える場合には、`smsversion` を実行する前に SMS を停止する必要があります。詳細は、『System Management Services (SMS) 1.6 インストールマニュアル』の「SMS の停止および開始」を参照してください。`smsversion` ユーティリティは、システムとドメインに関する重要な情報をバックアップしてから、目的の SMS バージョンに切り替えます。あとで、連続する元の SMS バージョンに (たとえば SMS 1.6 から SMS 1.5 に) 切り替えて戻すこともできます。

注 – バージョンが異なる Solaris OS 間 (Solaris 8 と Solaris 9 など) では、SMS のバージョンが連続していても切り替えはサポートされません。Solaris 8 バージョンで SMS を使用していた環境から、Solaris 9 バージョンにアップグレードしたあと、旧バージョンに戻すには Solaris 8 の再インストールが必要になります。`smsversion` コマンドを使用して、SMS 1.6 が実行されている Solaris 10 から SMS 1.5 に戻す切り替えは、以前の OS を再インストールしないかぎりサポートされません。詳細については、『System Management Services (SMS) 1.6 インストールマニュアル』を参照してください。

オプションを省略すると `smsversion` は使用中の SMS のバージョンを表示し、インストール済み SMS のバージョンが 1 つだけであればそのまま終了します。

`smsversion` の実行中にエラーが発生すると、エラーメッセージが `/var/sadm/system/logs/smsversion` に出力されます。

`smsversion` を実行するには、スーパーユーザー特権が必要です。詳細と用例については、`smsversion` のマニュアルページを参照してください。

バージョンの切り替え

注 – SMS 1.6 から以前にインストールしたバージョンの SMS に切り替えると、SC のセキュリティに影響が生じます。詳細については、『System Management Services (SMS) 1.6 インストールマニュアル』を参照してください。

▼ 連続する 2 つの SMS バージョンが共存している場合に、バージョンを切り替える

メイン SC で次の手順を実行します。

1. 現在の構成が安定しており、さらに smsbackup でバックアップ済みであることを確認します。

安定しているということは、smsconfig、poweron、poweroff、setkeyswitch、cfgadm、rcfgadm、addtag、deletetag、addboard、moveboard、deleteboard、setbus、setdefaults、setobpparams、setupplatform、enablecomponent、または disablecomponent の各コマンドは実行するべきでないということです。

2. setfailover off を実行してフェイルオーバーを無効化します。

スペア SC で次の手順を実行します。

3. /etc/init.d/sms stop を実行します。

4. smsversion を実行します。

5. smsrestore を実行します。

6. 必要に応じて smsconfig -m を実行し、再起動します。

復元した smsbackup の作成後に、smsconfig -m を使用してネットワーク構成を変更した場合にのみ、smsconfig -m を実行してください。

メイン SC で次の手順を実行します。

7. /etc/init.d/sms stop を実行して SMS を停止します。

スペア SC で次の手順を実行します。

8. smsconfig -m を実行した場合は SC を再起動します。このコマンドを実行しなかった場合は、/etc/init.d/sms start を実行します。

SC の起動後、この SC がメイン SC になります。

9. 必要な場合は、flashupdate を使用して、CPU のフラッシュ PROM を更新します。

元のメイン SC で次の手順を実行します。

- 手順 4 ~ 6 と 8 を繰り返します。

新しいメイン SC で次の手順を実行します。

- setfailover on を実行してフェイルオーバーを有効化します。

詳細については、『System Management Services (SMS) 1.6 インストールマニュアル』を参照してください。

SMS 構成ユーティリティー

smsconfig ユーティリティーは、MAN ネットワークを構成し、MAN デーモン mand(1M) によって使用されるホスト名と IP アドレスの設定を変更して、ドメインディレクトリのアクセス制御リスト (ACL) を管理します。また、現在の構成も表示します。

UNIX グループ

smsconfig ユーティリティーは、SMS によって使用される UNIX グループを構成してユーザー特権を記述します。SMS はデフォルトで、各 SC にローカルにインストールされた一連の UNIX グループを使用します。-g オプションを指定して smsconfig ユーティリティーを実行すると、これらのグループをカスタマイズできます。また、-a オプションを指定すればユーザーグループへのユーザーの追加、-r オプションを指定すればグループからのユーザーの削除をそれぞれ実行できます。

登録ユーザーの追加、削除、および一覧表示に関する情報と用例については、『System Management Services (SMS) 1.6 インストールマニュアル』と smsconfig(1M) のマニュアルページを参照してください。

アクセス制御リスト (ACL)

従来の UNIX ファイル保護は、次の 3 つのユーザークラスに対して読み取り、書き込み、実行を許可します。つまり、ファイル所有者、ファイルグループ、その他です。ドメイン情報の保護と分離を行う目的で、各ドメインのデータへのアクセスは未承認のすべてのユーザーに対して拒否されます。ただし、SMS デーモンは承認ユーザーと見なされ、ドメインのファイルシステムへのフルアクセス権を持ちます。たとえば、次のとおりです。

- sms-esmd は、各ドメインディレクトリの \$SMSSETC/config/[A-R] にあるブ ラックリストファイルを読み取る必要があります。
- sms-osd は、各ドメインの \$SMSSETC/config/[A-R] ディレクトリにある bootparamdata ファイルに対して読み取りおよび書き込みを行うことができる 必要があります。
- sms-dsmd は、すべてのドメインの hpost ログの \$SMSVAR/adm/[A-R]/post に 書き込む必要があります。

smsconfig ユーティリティーは、ドメイン管理者がドメインに対するフルアクセス権を持つように、ドメインディレクトリに関連付けられた ACL エントリを設定します。モードフィールドの右にあるプラス記号 (+) は、ACL が定義済みのディレクトリを示します。

```
domain-id:sms-user:> ls -al
total 6
drwxrwxrwx  2 root      bin           512 May 10 12:29 .
drwxrwxr-x 23 root      bin          1024 May 10 12:29 ..
-rw-rw-r--+ 1 root      bin           312 May  4 16:15 blacklist
```

ACL にユーザーアカウントを登録するには、『System Management Services (SMS) 1.6 インストールマニュアル』に説明するように、ユーザーが有効な SMS グループに属している必要があります。

注 – ACL などの UFS 属性は、UFS ファイルシステムでのみサポートされます。ACL エントリのあるディレクトリを /tmp ディレクトリに復元またはコピーすると、すべての ACL エントリが失われます。UFS ファイルおよびディレクトリの一時的な格納には、/var/tmp ディレクトリを使用します。

ネットワーク構成

smsconfig はそのネットワーク内で 1 つまたは複数のインタフェース指示を個々に設定することができます。デフォルトでは、smsconfig は 3 つすべての内部ネットワーク (MAN、I1、および I2) の構成を走査します。

個々のネットワークを構成するには、コマンド行に *net-id* を付加します。MAN の *net-id* には、I1、I2、および C を指定します。

目的のドメインとその *net-id* を指定して、エンタープライズネットワーク内で単独のドメインを構成します。MAN の *hostname* として NONE というワードを指定すれば、任意のドメインを I1 MAN から除外できます。

注 – MAN ネットワークの構成または構成の変更が完了したあとで変更を有効にするには、SC を再起動してください。

smsconfig を実行するには、スーパーユーザー特権が必要です。詳細と例については、『System Management Services (SMS) 1.6 インストールマニュアル』、smsconfig のマニュアルページ、および 193 ページの「管理ネットワークのサービス」を参照してください。

MAN 構成

`smsconfig -m` と入力すると、次の処理が実行されます。

1. `/etc/hostname.scman[01]` を作成します。
2. `smsconfig` の外部ネットワークプロンプトへの入力に応じて、`/etc/hostname.hme0` および `/etc/hostname.eri1` を作成します。
3. `/etc/netmasks` および `/etc/hosts` を更新します。
4. OpenBoot PROM 変数を `local-mac-address?=true` に設定します (デフォルトは `false`)。

`smsconfig` の詳細については、`smsconfig(1M)` のマニュアルページ、および 193 ページの「管理ネットワークのサービス」を参照してください。

SMS マニュアルページ

SMS マニュアルページは、Sun Fire ハイエンドシステムのマニュアルセットの『System Management Services (SMS) 1.6 リファレンスマニュアル』およびオンラインで用意されています (SMS パッケージをインストールしている場合)。

SMS マニュアルページのリストを以下に示します。

- **addboard (1M)** – ドメインに対するボードの割り当て、接続、構成を行います
- **addcodlicense(1M)** – Capacity on Demand (COD) RTU (Right-To-Use) ライセンスキーを COD ライセンスデータベースに追加します
- **addtag (1M)** – ドメインにドメイン名 (タグ) を割り当てます
- **cancelcmdsync (1M)** – コマンド同期リストからコマンド同期記述子を削除します
- **codd(1M)** – Capacity on Demand デーモン
- **console (1M)** – ドメインのコンソールにアクセスします
- **dca (1M)** – ドメイン構成エージェント
- **deleteboard (1M)** – ドメインからのシステムボードの構成解除、切り離しおよび割り当ての解除を行います
- **deletecodlicense(1M)** – COD RTU ライセンスキーを COD ライセンスデータベースから削除します
- **deletetag (1M)** – ドメインに関連付けられたドメイン名 (タグ) を削除します
- **disablecomponent (1M)** – 指定されたコンポーネントをブラックリストに追加します
- **dsmd (1M)** – ドメインステータスの監視デーモン
- **dxs (1M)** – ドメインの X サーバー
- **efhd(1M)** – エラーおよび障害処理デーモン
- **elad(1M)** – イベントログアクセスデーモン
- **erd(1M)** – イベントレポートデーモン
- **enablecomponent (1M)** – 指定されたコンポーネントを ASR ブラックリストから削除します

- esmd (1M) - 環境ステータスの監視デーモン
- flashupdate (1M) - システムボードの PROM を更新します
- fomd (1M) - フェイルオーバー管理デーモン
- frad (1M) - FRU アクセスデーモン
- help (1M) - SMS コマンドのヘルプ情報を表示します
- hpost (1M) - Sun Fire ハイエンドシステムの電源投入時自己診断 (POST) の制御アプリケーション
- hwad (1M) - ハードウェアアクセスデーモン
- initcmdsinc (1M) - 回復するスクリプトを特定するコマンド同期記述子を作成します
- kmd (1M) - キー管理デーモン
- mand (1M) - 管理ネットワークデーモン
- mld (1M) - メッセージロギングデーモン
- moveboard (1M) - ドメイン間でシステムボードを移動します
- osd (1M) - OpenBoot PROM サーバーデーモン
- pcd (1M) - プラットフォーム構成データベースデーモン
- poweroff (1M) - 電源切断を制御します
- poweron (1M) - 電源投入を制御します
- rcfgadm (1M) - 遠隔構成管理
- reset (1M) - 指定されたドメインのすべてのポート (CPU または I/O) にリセットを送信します
- resetsc (1M) - スペア SC にリセットを送信します
- runcmdsync (1M) - フェイルオーバー後の回復のために指定されたスクリプトを準備します
- savecmdsinc (1M) - フェイルオーバー後に処理を再開できるスクリプト内の位置を特定するマーカーを追加します
- setbus (1M) - ドメインのアクティブな拡張ボードで動的なバス再構成を実行します
- setcsn(1M) - Sun Fire ハイエンドシステムのシャーシのシリアル番号を設定します
- setdatasync (1M) - データ同期で使用されるデータ伝達リストを変更します
- setdate (1M) - システムコントローラまたはドメインの日時を設定します
- setdefaults (1M) - すでにアクティブになっているドメインからすべてのインスタンスを削除します
- setfailover (1M) - SC フェイルオーバーメカニズムの状態を変更します
- setkeyswitch (1M) - 仮想キースイッチの位置を変更します
- setobpparams (1M) - OpenBoot PROM 変数を設定します

- `setpcimode(1M)` - 使用しているサーバーの V2HPCIX I/O ボード上にある PCI-X スロットの設定を変更します
- `setupplatform (1M)` - ドメインの使用可能構成要素リストを設定します
- `showboards (1M)` - システムボードの割り当て情報とステータスを表示します
- `showbus (1M)` - アクティブなドメインの拡張ボードのバス構成を表示します
- `showcmdsycn (1M)` - 現在のコマンド同期リストを表示します
- `showcodlicense(1M)` - COD ライセンスデータベースに格納されている現在の COD RTU ライセンスを表示します
- `showcodusage(1M)` - COD 資源の現在の使用統計情報を表示します
- `showcomponent (1M)` - コンポーネントの ASR ブラックリストのステータスを表示します
- `showdatasync (1M)` - フェイルオーバーに対する SMS データ同期のステータスを表示します
- `showdate (1M)` - システムコントローラまたはドメインの日時を表示します
- `showdevices (1M)` - システムボードのデバイスおよび資源の使用情報を表示します
- `showenvironment (1M)` - 環境データを表示します
- `showfailover (1M)` - SC フェイルオーバーのステータスまたは役割を表示します
- `showkeyswitch (1M)` - 仮想キースイッチの位置を表示します
- `showlogs (1M)` - メッセージログファイル、イベントログ、または Event Dictionary Database を表示します
- `showobpparams (1M)` - OpenBoot PROM の起動パラメータを表示します
- `showpcimode(1M)` - 使用しているサーバーの V2HPCIX I/O ボード上にあるすべての PCI-X スロットのモード設定を一覧表示します
- `showplatform (1M)` - ドメインのボード使用可能構成要素リストを表示します
- `showxirstate (1M)` - プロセッサにリセットパルスを送信したあとで CPU ダンプ情報を表示します
- `smsbackup (1M)` - SMS 環境をバックアップします
- `smsconfig (1M)` - SMS 環境を構成します
- `smsconnectsc (1M)` - 遠隔 SC コンソールにアクセスします
- `smsinstall`: SMS ソフトウェアをインストールします。
- `smsrestore (1M)` - SMS 環境を復元します
- `smsupgrade`: システムにインストールされている既存の SMS ソフトウェアをアップグレードします。
- `smsversion (1M)` - SMS ソフトウェアのアクティブバージョンを表示します
- `ssd (1M)` - SMS 起動デーモン

- testemail(1M) – イベントメッセージのロギングと電子メールによるイベントの通知を含む、イベントレポート機能のテストを行います
- tmd (1M) – タスク管理デーモン
- wcapp(1M) – wPCI アプリケーションデーモン

エラーメッセージ

ここでは、ユーザーに表示される SMS のエラーメッセージについて説明します。エラーの種類とエラー番号の範囲を一覧にまとめます。個々のエラーを表示するには、SMSHelp ソフトウェアパッケージ (SUNWSMSjh) をインストールしておく必要があります。ここでは、SUNWSMSjh が SMS ソフトウェアのインストール時にインストールされなかった場合に、単体でインストールする手順について説明します。

SMSHelp の各エラーには、エラー ID、メッセージのテキスト、メッセージの意味、詳細情報の参照箇所 (該当する場合)、および推奨される復旧作業や分析の手順が表示されます。

この章では、以下の項目を説明します。

- 259 ページの「SMSHelp のインストール」
- 264 ページの「エラーの種類」
- 264 ページの「エラーのカテゴリ」

SMSHelp のインストール

この節では、標準的なインストールユーティリティである pkgadd を使用して、SUNWSMSjh パッケージを手動でインストールする方法を説明します。

▼ SUNWSMSjh パッケージをインストールする

1. SC にスーパーユーザーとしてログインします。

2. サーバー上で SUNWSMSjh パッケージをロードします。

```
# pkgadd -d . SUNWSMSjh
```

各パッケージの著作権、商標、および使用許諾についての画面が表示されます。次に、パッケージをインストールするために pkgadd(1M) が行なっている処理についてのメッセージが表示されます。インストールされているファイルおよびディレクトリについての表示もあります。システムの構成に応じて、次のようなメッセージが表示されます。

```
This package contains scripts which will be executed  
with superuser permission during the process of installing this  
package.
```

```
Do you want to continue with the installation of this  
package [y,n,?]
```

3. 順次表示されるプロンプトでは `y` と入力してインストールを続行します。
この段階までのインストールが完了すると、SUNWSMSjh パッケージのインストールが済んでスーパーユーザーのプロンプトが表示されます。
4. スーパーユーザーとしてログアウトします。

▼ SMSHelp を起動する

1. SC に、プラットフォームまたはドメインのグループの特権を持つユーザーとしてログインします。
2. 端末のウィンドウで、次のように入力します。

```
sc0:sms-user:> smshelp &
```

SMS ヘルプブラウザが表示されます。各ペインのサイズは、必要に応じて変更できます。これには、ペインの縦スクロールバーの右側にポインタを置いて左マウスボタンを押し、そのまま右方向にドラッグします。

3. エラーメッセージを選択し、その message_code を書き留めます。

エラーメッセージは、プラットフォームおよびドメインのログに記録されます。
メッセージのフォーマットは、syslog(3) の規則に従います。

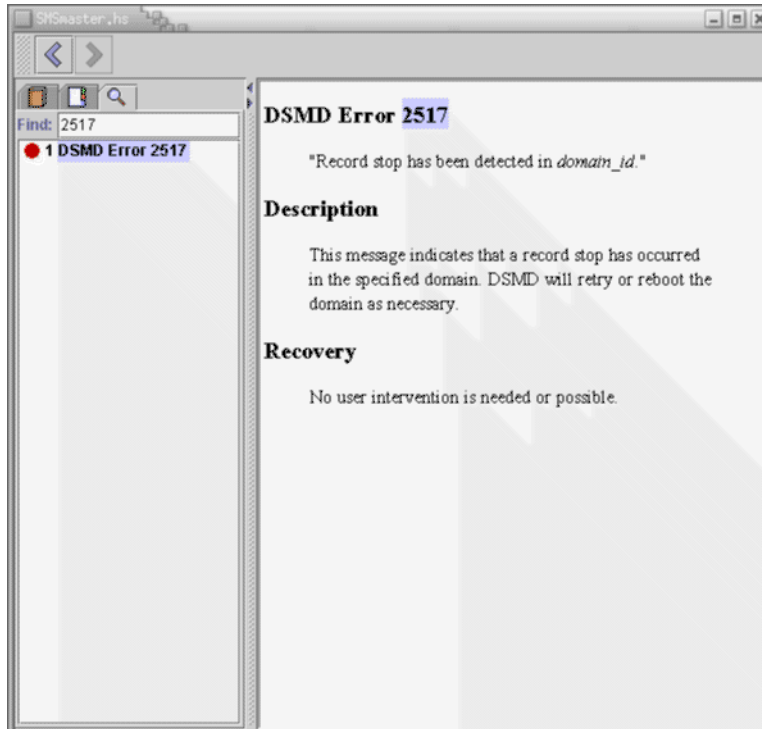
```
timestamp host process_name [pid]: [message_code  
high_res_timestamp level source_code_file_name  
source_code_line_num] message_text
```

たとえば、次のメッセージが表示されます。

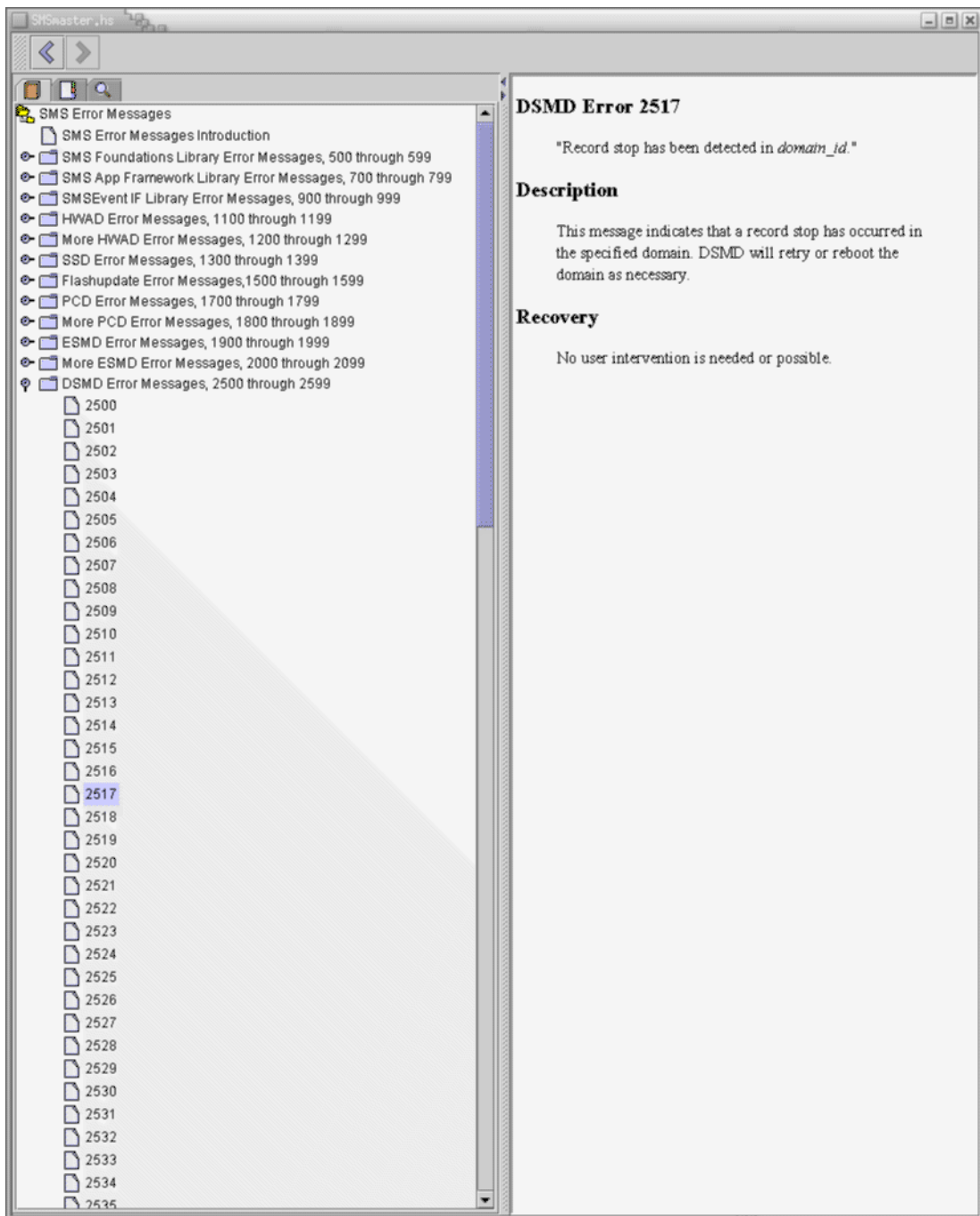
```
Feb 2 18:36:14 2002 xc17-sc0 dsmd[117469]-B(): [2517  
16955334989087 WARNING EventHandler.cc 121] Record stop has been  
detected in domain B.
```

message_code を使用すると、ブラウザの最上部にある検索アイコンでクイック検索を実行するか、目次をスクロールできます。

- クイック検索を実行するには、次の例のように示すように、検索アイコンをクリックしてエラーメッセージ番号を入力し、Return キーを押します。



- 目次をスクロールするには、次の例に示すように、そのエラーメッセージを含むメッセージフォルダ、この場合は「DSMD Error Messages, 2500 through 2599」を左クリックし、続いてエラー 2517 をクリックします。



エラーの種類

この節では、SMSHelp のエラーメッセージに表示される 6 種類のエラーについて説明します (表 B-1)。

表 B-1 エラーの種類

エラー	説明
EMERG	通常はすべてのユーザーにブロードキャストされるパニック状況。
ALERT	すぐに修正されるべき状況。たとえば、システムデータベースの破壊など。
CRIT	危険な状況についての警告。たとえば、ハードウェア装置の障害など。
ERROR	その他すべてのエラー。
WARNING	警告メッセージ。
NOTICE	エラー状況ではないが、特に対処が必要と思われる状況。

エラーのカテゴリ

表 B-2 に、SMS のさまざまなエラーカテゴリを示します。エラー番号が連続していない箇所がありますが、これは内部またはサービス向けに予約されたエラーメッセージ群が存在するためです。

表 B-2 エラーのカテゴリ

エラー番号	メッセージグループ
0 ~ 499	DEBUG、INFO、および POST のメッセージ用に予約。
500 ~ 699	SMS Foundation Library のメッセージ用に予約。
700 ~ 899	SMS Application Framework のメッセージ用に予約。
900 ~ 1099	SMSEvent IF Library のメッセージ用に予約。
1100 ~ 1299	HWAD のデーモンおよびライブラリのメッセージ用に予約。
1300 ~ 1499	ssd のメッセージ用に予約。

表 B-2 エラーのカテゴリ (続き)

エラー番号	メッセージグループ
1500 ~ 1699	flashupdate のメッセージ用に予約。
1700 ~ 1899	pcd のメッセージ用に予約。
1900 ~ 2099	esmd のメッセージ用に予約。
2500 ~ 2699	dsmd のメッセージ用に予約。
2700 ~ 2899	addtag のメッセージ用に予約。
2900 ~ 3099	deletetag のメッセージ用に予約。
3100 ~ 3299	Permissions のメッセージ用に予約。
3300 ~ 3499	domain-tag のメッセージ用に予約。
3500 ~ 3699	addboard のメッセージ用に予約。
3700 ~ 3899	tmd のメッセージ用に予約。
4100 ~ 4299	showkeyswitch のメッセージ用に予約。
4300 ~ 4499	dca のメッセージ用に予約。
4500 ~ 4699	libscdr プラグインのメッセージ用に予約。
4700 ~ 4899	osd のメッセージ用に予約。
4900 ~ 5099	dxs のメッセージ用に予約。
5100 ~ 5299	deleteboard のメッセージ用に予約。
5300 ~ 5499	setkewswitch のメッセージ用に予約。
5500 ~ 5699	libdrcmd のメッセージ用に予約。
5700 ~ 5899	moveboard のメッセージ用に予約。
5900 ~ 6099	setupplatform のメッセージ用に予約。
6100 ~ 6299	Power 関係のコマンドのメッセージ用に予約。
6300 ~ 6499	xir ライブラリのメッセージ用に予約。
6500 ~ 6699	showplatform のメッセージ用に予約。
6700 ~ 6899	Help メッセージ用に予約。
6900 ~ 7099	reset のメッセージ用に予約。
7100 ~ 7299	showboards のメッセージ用に予約。
7300 ~ 7499	libshowboards のメッセージ用に予約。
7500 ~ 7699	autolock のメッセージ用に予約。
7700 ~ 7899	mand のメッセージ用に予約。
7900 ~ 8099	showenvironment のメッセージ用に予約。

表 B-2 エラーのカテゴリ (続き)

エラー番号	メッセージグループ
8100 ~ 8299	resetsc のメッセージ用に予約。
8300 ~ 8499	動的バス再構成のメッセージ用に予約。
8500 ~ 8699	fomd のメッセージ用に予約。
8700 ~ 8899	kmd のメッセージ用に予約。
8900 ~ 9099	setdefaults のメッセージ用に予約。
9100 ~ 9299	mld のメッセージ用に予約。
9300 ~ 9499	showdevices のメッセージ用に予約。
9500 ~ 9699	showxirstate のメッセージ用に予約。
9700 ~ 9899	COD のメッセージ用に予約。
9900 ~ 10000	frad のメッセージ用に予約。
10100 ~ 10299	fruevent のメッセージ用に予約。
10300 ~ 10499	smsconnectsc のメッセージ用に予約。
10700 ~ 10899	EFE のメッセージ用に予約。
11100 ~ 11299	rcfgadm のメッセージ用に予約。
11300 ~ 11499	datasync のメッセージ用に予約。
11500 ~ 11699	EFHD のメッセージ用に予約。
11700 ~ 11899	ELAD のメッセージ用に予約。
11900 ~ 12099	ERD のメッセージ用に予約。
12100 ~ 12299	イベントユーティリティーのメッセージ用に予約。
12300 ~ 12499	Wcapp のメッセージ用に予約。
12500 ~ 12699	FRUID 関連のメッセージ用に予約。
12700 ~ 12799	EBD のエラーメッセージ用に予約。
50000 ~ 50099	SMS 汎用のメッセージ用に予約。

用語集

A

- ACL 「アクセス制御リスト (ACL)」を参照してください。
- ADR 「動的再構成の自動化 (ADR)」を参照してください。
- ASIC 「特定用途集積回路 (ASIC)」を参照してください。
- ASR 自動システム回復
- AXQ Sun Fire ハイエンドシステムの拡張ボード上にある ASIC。

B

- BBC 起動バスコントローラ。CPU および I/O ボード (システムコントローラボードも含む) で使用される ASIC で、起動バスを PROM バスおよび console バスへ接続する。
- BBSRAM 「起動バス SRAM (BBSRAM)」を参照してください。

C

Capacity on Demand (COD)

予備の処理リソース (CPU) を提供するオプション。この CPU は、Sun Fire ハイエンドシステム上に装着された COD システムボードに搭載されている。COD CPU に対する COD RTU (right-to-use) ライセンスを購入すると、使用できるようになる。

CASM 「キャッシュ可能な アドレススライスマップ (CASM)」を参照してください。

CHS コンポーネントの健全性ステータス。

CLI コマンド行インタフェース

cmdsycn コマンドの同期。SC のフェイルオーバー中に共同で回復を制御する複数のコマンドのこと。たとえば、cancelcmdsycn、initcmdsycn、および savecmdsycn などがある。

CMR Coherent Memory Replication の略。メモリーの内容の複製が一貫していること。

CPU Central Processing Unit の略。中央演算装置。

CSB センタープレーンサポートボード

D

DARB Sun Fire ハイエンドシステムのセンタープレーンにある ASIC で、データ調停を処理する。

DARB 割り込み Sun Fire ハイエンドシステムのセンタープレーン上の DARB ASIC のいずれかまたはその両方からの信号によって開始される、SC プロセッサの割り込み。DARB は、Dstop、Recordstop、および非エラー要求の 3 種類のイベントに対応して、この割り込み信号を表明する。これらのイベントは、AXQ ASIC のシステムレジスタにドメインプロセッサが書き込むことにより開始される、注意を促すためのものである。

DCU 「ドメイン構成ユニット (DCU)」を参照してください。

DE 診断エンジン。

DHCP Dynamic Host Configuration Protocol の略。

DIMM 「デュアルインラインメモリーモジュール (DIMM)」を参照してください。

domain-id ドメインのドメイン ID。

domain-tag	addtag(1M) を使用して割り当てられたドメイン名。
DR	動的再構成。
DR	「動的再構成 (DR)」を参照してください。
DRAM	「ダイナミック RAM (DRAM)」を参照してください。
DSD	動的システムドメイン。
DSD	動的システムドメイン。「ドメイン」を参照してください。
dstop	「ドメイン停止」を参照してください。

E

Ecache	「外部キャッシュ (Ecache)」を参照してください。
ECC	Error Correction Code の略。エラー訂正コード。
EEPROM	Electrically Erasable Programmable Read-Only Memory の略。電氣的に消去できるプログラム可能な読み出し専用メモリー。
Ethernet アドレス	各 Ethernet ネットワークアダプタに割り当てられている一意な番号。Ethernet アドレスは 48 ビットの数値で、IEEE により管理されている。ハードウェアのベンダーは、自社の製品に組み込むために多数の Ethernet アドレスを取得している。「MAC アドレス」も参照。

F

Fireplane	Sun Fire ハイエンドシステムのセンタープレーン。
FPRM	Flash Programmable Read-Only Memory の略。プログラム可能な読み出し専用フラッシュメモリー。
FRU	Field Replaceable Unit の略。現場交換可能ユニット。
FRUID	Field Replaceable Unit Identification の略。現場交換可能ユニットの検証。

G

- GDCD** 「グローバルドメイン構成記述子 (*GDCD*)」を参照してください。
- GUI** グラフィカルユーザーインターフェース。

H

- HA** 高可用性。
- HASRAM** 高可用性 SRAM。
- headroom** 「インスタントアクセス *CPU*」を参照してください。
- HPCI** ホットプラグ可能な PCI I/O ボード。
- hpost** ホスト POST は、SC により実行される POST コードである。通常、このコードは SC のローカルディスクにある。
- HPU** ホットプラグ可能ユニット。実行中のシステムから分離できるハードウェアコンポーネントで、ハードウェアやソフトウェアに障害を与えることなしにシステムから脱着できるもの。
- HsPCI** 「*HPCI*」を参照してください。

I

- I1 ネットワーク** 各 SC 上には、18 個のネットワークインターフェース (NIC) がある。これらは、Sun Fire ハイエンドシステム上の各拡張 I/O スロットに装着された NIC とポイントツーポイント方式で接続される。これらのポイントツーポイントのリンクは、総称して **I1 ネットワーク** と呼ばれる。
- I2 ネットワーク** システムコントローラごとに 2 つの NIC からなる、2 つのシステムコントローラ間の内部ネットワーク。**I2 ネットワーク** は専有ネットワークではなく、**I1 ネットワーク** とは完全に分離している。
- I²C** IC 間のバス。各種システムで、LED の点灯、システムクロックリソースの設定、thermal 情報の取得などに使用される 2 線のバス。
- IDPROM** 識別 PROM。Sun Fire ハイエンドシステム内部の機構、たとえばコンピュータの機種、製造日、Ethernet アドレス、シリアル番号およびホスト ID に固有の情報を保持している。

- ioctl** 装置およびストリームに対して各種の制御機能を実行するシステムコール。ストリームでないもの場合は、装置固有の制御機能がこの呼び出しで実行される。
- IOSRAM** Input-Output Static Random-Access Memory の略。
- IP** Internet Protocol の略。インターネットプロトコル。
- IP リンク** ノードがリンク層で通信するために使用する通信媒体。リンク層は、IPv4 や IPv6 の直下の層である。たとえば、Ethernet (シンプルまたはブリッジ) や ATM ネットワークがある。
- IPMP** IP Network Multipathing の略。同一の IP リンク (たとえば、Ethernet) に接続されている複数のネットワークインタフェースカードに対して、負荷分散およびフェイルオーバーを提供する Solaris ソフトウェア。
- IPv4** Internet Protocol version 4 の略。
- IPv6** Internet Protocol version 6 の略。IPv6 では、アドレス空間が 32 ビットから 128 ビットへ拡大された。IPv6 は、IPv4 と下位互換である。

J

- JTAG** IEEE 標準 1149.1 で規定されているシリアルスキャンインタフェース。JTAG という名前は、当初このインタフェースを設計した Joint Test Action Group に由来する。
- JTAG+** Sun により開発された、JTAG の拡張機能。ボードに信号を送るための制御ラインが追加され、リングアドレスはシリアルデータラインに移動している。単に JTAG と呼ばれることも多い。

K

- kadb** ユーザーインタフェースを備えた対話的なカーネルデバッグ。詳細については、Solaris マニュアルページの `kadb(1M)` を参照。

L

- LAN** Local Area Network の略。ローカルエリアネットワーク。
- LCD** Liquid crystal display の略。液晶ディスプレイ。

LED Light emitting diode の略。発光ダイオード。

LSF Load Sharing Facility の略。負荷分散機能。

M

MAC アドレス ネットワークインタフェースに割り当てられる、全世界を通じて一意なシリアル番号。MAC アドレスの配布は、IEEE により管理されている。詳細については、「Ethernet アドレス」を参照。

MAN SMS Management Network の略。SMS 管理ネットワーク。

MaxCPU デュアル CPU ボード。

Mbox SC および OpenBoot PROM 上の SMS ソフトウェアとドメイン上の Solaris OS の間でメッセージを渡すメカニズム。

MIB Management Information Base の略。管理情報ベース。

N

NFS Network File System の略。ネットワークファイルシステム。

NIC 「ネットワークインタフェースカード (NIC)」を参照してください。

NIS+ Netowrkr Information Service Plus のこと。セキュアで階層的なネットワーク命名サービス。

NTP 「時間情報プロトコル (NTP)」を参照してください。

NVRAM Non-Volatile Read-only Memory の略。不揮発性読み取り専用メモリー。

O

OBP 「OpenBoot PROM」を参照してください。

OpenBoot PROM ソフトウェアの層の 1 つで、構成済みの Sun Fire ハイエンドシステムの制御を hpost(1M) から取得し、メモリーに何らかのデータ構造を構築してから、オペレーティングシステムを起動する。IEEE 1275 準拠の OpenBoot PROM。

OS Operating System の略。オペレーティングシステム。

OSR Operating System Resource の略。オペレーティングシステム資源。

P

- PCB Printed Circuit Board の略。プリント回路基板。
- platform 1 台の物理的コンピュータ。
- POR Power-On-Reset の略。電源投入時リセット。
- POST 「電源投入時自己診断 (POST)」を参照してください。
- PROM Programmable Read Only Memory の略。プログラム可能な読み出し専用メモリー。

R

- RAM Random Access Memory の略。ランダムアクセスメモリー。
- RARP Reverse Address Resolution Protocol の略。
- RASS Reliability, Availability, Serviceability, and Security の略。信頼性、可用性、保守性、およびセキュリティー。
- RPC Remote Procedure Call の略。
- rstop 「記録停止」を参照してください。
- RTU Right To Use の略。使用权。

S

- SA Security Association の略。セキュリティーの関連付け。
- SBBC 「BBC」を参照してください。
- SC システムコントローラ。システムの監視および制御を補助する Nordica ボード。
- SEEPROM Serial EEPROM の略。シリアル EEPROM。

- SMP** Symmetric Multi-Processor の略。シンメトリックマルチプロセッサ。
- SMS** System Management Services のソフトウェア。Sun Fire ハイエンドシステムの SC 上で実行され、Sun Fire ハイエンドシステムプラットフォームに制御または監視の機能を提供する。
- SNMP** Simple Network Management Protocol の略。
- Solaris OS** Solaris オペレーティングシステム。
- SRAM** 「スタティック RAM (SRAM)」を参照してください。
- SRS** Sun Remote Services の略。
- SST** Solaris Security Toolkit の略。
-

T

- TCP/IP** Transmission Control Protocol/Internet Protocol の略。転送制御プロトコル/インターネットプロトコル。
- TOD** 本日の時刻。
-

U

- UltraSPARC** Sun Fire ハイエンドシステムで使用されているプロセッサモジュールのこと。
- URL** Uniform Resource Locator の略。
-

V

- VCMON** Voltage Core (CPU) Monitoring の略。
- VM** Volume Manager (Veritas) の略。 -
-

W

- wPCI** Sun Fire Link I/O ボード。

X

XIR eXternally Initiated Reset の略。外部から開始されたリセット。ドメインにある CPU へ「ソフト」リセット信号を送信する。XIR では、ドメインは再起動されない。リセット信号を受信すると、CPU は OpenBoot PROM のプロンプトに移行する。

あ

**アービトレーション
ストップ**

Sun Fire ハイエンドシステム ASIC のいずれかがパリティエラーまたは同等の重大なシステムエラーを検出したときに発生する状況。バス調停が動かなくなるため、すべてのバスが停止する。

**アクセス制御リスト
(ACL)**

アクセス制御リスト (ACL) には、システム上におけるファイルアクセス権とフォルダアクセス権が含まれる。ACL を使用して、ファイルまたはフォルダへのアクセス権を、所有者、所有者のグループ、その他、および特定のユーザーおよびグループについて定義したり、これらのカテゴリごとにデフォルトのアクセス権を定義したりできる。

アクティブなドメイン

オペレーティングシステムソフトウェアを実行しているドメイン。

アクティブなボード

ボードは、connected/unconfigured 状態の場合にアクティブとみなされる。

**アクティブなボードの
リスト**

ドメインで使用中的であるボードのリスト。pcd(1M) デーモンがこのリストの状態を保持する。

**インスタントアクセス
CPU**

Sun Fire ハイエンドシステムの COD システムボード上にある、ライセンスのない COD CPU。COD CPU に対する COD RTU (right-to-use) ライセンスを購入すると、最大 8 つまでの COD CPU をただちに使用できるようになる。「ヘッドルーム」とも呼ばれる。

**インタフェース
グループ**

同一のコミュニティーに接続するネットワークインタフェースのグループ。

**インタフェースグループ
名**

特定のインタフェースグループに名前を付ける文字列識別子。Sun Fire ハイエンドシステムの外部ネットワーク監視のコンテキストでは、特定のコミュニティーと関連付けられている名前をインタフェースグループ名という。

か

- 外部キャッシュ (Ecache)** 8M バイトの同期スタティック RAM による二次キャッシュで、各プロセッサごとにローカルに使用される。コードおよびデータの両方に使用される。外部キャッシュは直接マップのキャッシュである。
- 外部ネットワーク** ネットワークのノードへ接続するために物理的なケーブルを必要とするネットワーク。Sun Fire ハイエンドシステムの場合は、Sun Fire システムの前面にある RJ45 ジャックで接続されるネットワークのこと。「外部ネットワーク インタフェース」を参照してください。
- 外部ネットワーク インタフェース** Sun Fire ハイエンドシステムコントローラの前面にある複数の RJ45 ジャックの 1 つ。
- 仮想キースイッチ** SC は、各ドメインに仮想キースイッチを提供して、各ドメインの起動プロセスを制御する。setkeyswitch(1M) コマンドが、各ドメインの仮想キースイッチの設定を制御する。可能な設定値は、on、off、standby、diag、および secure である。
- 環境監視** システムには、温度、電圧、および電流を監視するセンサーが多数取り付けられている。SC のデーモンである esmd および dsmd は装置を定期的に調べて、環境データを入手可能にしている。障害を回避するために、SC は各種のコンポーネントをシャットダウンすることがある。
- 起動バス** プロセッサポートコントローラ ASIC で制御される、バイト幅の低速バス。診断コードおよび起動コードの実行に使用される。UltraSPARC は、リセットから抜け出すときに起動バスからコードの実行を開始する。Sun Fire ハイエンドシステムでは、BBSRAM が 起動バス上の唯一のコンポーネントである。
- 起動バス SRAM (BBSRAM)** 各プロセッサ PC ASIC に装着されている、容量が 256 KB のスタティック RAM。PC を通じて、JTAG またはプロセッサについて読み込みおよび書き込みを行うためにアクセスできる。起動バス SRAM はさまざまな場合に hpost(1M) および OpenBoot PROM 起動コードとともにダウンロードされて、ダウンロードされたコードと SC の間で共有されるデータを提供する。
- 記録停止** 訂正できるデータ転送エラー。
- キャッシュ可能なアドレススライスマップ (CASM)** キャッシュ可能なアドレスを適切な拡張ボードと対応づける AXQ 内のテーブル。
- クラスタ** 相互に接続されたコンピュータシステムが共同で処理を行うまとまり。各コンピュータが個別に OS イメージを実行するが、全体で単一のコンピュータ資源とみなされる。

グローバルドメイン構成 記述子 (GDCD)	hpost(1M) が選択する、単一の構成の記述子。GDCD は、OpenBoot PROM へ渡される構造の一部である。
コミュニティ	ほかのネットワークから物理的に分離された、カスタマーサイトにある IP ネットワーク。
コミュニティ名	特定のコミュニティに名前を付ける文字列識別子。Sun Fire ハイエンドシステムの外部ネットワーク監視のコンテキストでは、コミュニティ名はインタフェースグループ名として使用される。「インタフェースグループ名」を参照してください。

さ

システムボード	次世代の Sun Fire サーバーには、5 種類のシステムボードがある。そのうち 4 種類が、Sun Fire ハイエンドシステムに搭載されている。5 種類のシステムボードは、システムボード、I/O ボード、WCI ボード、Sun Fire ハイエンドシステム PCI コントローラボード、および Sun Fire ハイエンドシステムコンパクト PCI コントローラボードである。
自動システム回復 (ASR)	ソフトウェアまたはハードウェアの障害または不適切な環境条件などが原因で 1 つまたは複数のドメインがアクティブでなくなった場合に、システムを復元して、正常な構成のすべてのドメインを稼働させる処理からなる。
自動診断 (AD)	エラー発生時に起動され、FRU のコンポーネント健全性ステータス (CHS) の一部として診断情報を記録するソフトウェアエンジン。この情報は、各コンポーネントの FRUID 内に保存される。場合によっては、自動回復プロセスが開始され、POST の再実行が行なわれる。
自動診断エンジン	プラットフォームおよびそのドメインの利用度に影響を与える、ハードウェアエラーを特定するソフトウェア機能。
自動フェイルオーバー	SMS デーモン fcmd による処理。メイン SC でハードウェアまたはソフトウェア障害が発生したときに、SC の制御をメイン SC からスペア SC へ自動的に切り替える。
シャーシのシリアル番号	Sun Fire ハイエンドシステムの特定に使用されるシリアル番号。シャーシのシリアル番号は、システムシャーシ正面の下部中央付近に貼付されているラベルに印刷されています。この番号は、サービスプロバイダがハードウェアイベントと保守アクションを該当するシステムに関連付けるときに使用される。
シャーシのホスト ID	センタープレーンのシリアル番号。この番号は、COD ライセンスを取得するために、COD 機能でプラットフォームを特定する際にのみ使用される。

使用可能構成要素リスト	ドメイン管理者または構成者の特権を持つユーザーによりドメインに割り当てることができるコンポーネントのリスト。pcd(1M) デーモンがこのリストの状態を保持する。setupplatform(1M) がこのリストを更新する。
スタティック RAM (SRAM)	電源が提供されている間だけ内容を保持するメモリーチップ。
双頭状態	メイン、スベアの両方の SC が、自分はメイン SC であると認識している状態。

た

ダイナミック RAM (DRAM)	ハードウェアメモリーチップで、内容を保持するために定期的な再書き込みが必要なもの。この処理は「リフレッシュ」と呼ばれる。Sun Fire ハイエンドシステムでは、DRAM は主記憶の SIMM および制御ボードにのみ使用されている。
チェックポイントデータ	特定の実行ポイントでの SC クライアントの状態のコピー。チェックポイントデータは定期的にディスクに保存される。
ディスクアレイ	ハードウェア周辺機器内にある複数のディスクのまとまり。ディスクアレイでは、収容されている各ディスクへ 1 ～ 2 本のファイバチャネルモジュールを通じてアクセスできる。
ディスクアレイコントローラ	ホストシステムに装着されるコントローラで、ファイバチャネルモジュールを 1 ～ 2 本持つ。
ディスクアレイポート	ディスクアレイコントローラへ接続できるファイバチャネルモジュールで、ドライバのペアにより保守される。たとえば、SSA では soc/pln である。
デュアルインラインメモリーモジュール (DIMM)	複数のメモリーチップとサポート回路を載せた小さな回路基板。
電源投入時自己診断 (POST)	hpost(1M) が実行するテスト。hpost は、初期化されていない Sun Fire ハイエンドシステムハードウェアについて、そのコンポーネントを調査およびテストし、矛盾なく初期化されたシステムにするために必要な構成を行って OpenBoot PROM に渡すプログラムである。Sun Fire ハイエンドシステムの POST は、lpost、spost、および hpost というコンポーネントにより階層的に実装されている。
動的再構成 (DR)	コンピュータを停止させなくとも、オペレーティングシステムからシステムボードを論理的に脱着できる機能。DR はホットスワップと関連して使用できる。ホットスワップは、システムボードを物理的に脱着する作業である。Sun Fire システムでは、新しいシステムボードの追加、修理されたシステムボードの再装着、あるいはドメイン構成の変更の際に DR を使用できる。

**動的再構成の自動化
(ADR)**

システムボードの動的再構成は、ボードを自動的に `assign/unassign` (割り当てまたは割り当て解除)、`connect/disconnect` (接続または切断)、および `configure/unconfigure` (構成または構成解除) する処理や、ボードの状態情報を取得する処理に関する各種のコマンドにより実行される。これらのコマンドは、対話的に実行したり、シェルスクリプトで実行したりできる。

**特定用途集積回路
(ASIC)**

Sun Fire ハイエンドシステムでは、回路にある大きなメインチップならばどれも ASIC という。UltraSPARC プロセッサおよびデータバッファチップも含まれる。

ドメイン

1 つまたは複数のシステムボードのセットで、個別のシステムとして動作する。OS を起動できるので、他のドメインに依存せずに稼働できる。自身の OS を実行できるコンピュータ環境である。Sun Fire ハイエンドシステムでは、18 個までのドメインを利用できる。システムを共有する複数のドメインも、その性質上お互いに独立している。

**ドメイン構成ユニット
(DCU)**

単一のドメインへ割り当てることができるハードウェアのユニット。ドメインは、DCU で構成される。CPU またはメモリー、PCI I/O、hsPCI I/O、および hsPCI+ I/O は DCU である。csb ボード、exb ボード、および SC は DCU ではない。

ドメイン停止

修正不能なハードウェアエラーで、影響を受けるドメインを即座に終了させる。

ドメイン無し

どのドメインにも割り当てられていないボード (DCU) の状態を表す用語。

ドリフトファイル

xntpd により計算されたドリフト (周波数エラー) の値を記録するために使用されるファイル。最も一般的な名前は `ntp.drift` である。

トンネルスイッチ

SC またはドメインの通信トンネルを、ドメイン内のある I/O ボードから別の I/O ボードへ移す処理のこと。通常は、トンネルの設定されている I/O ボードが動的再構成で取り外された場合に発生する。

な

**ネットワークインタ
フェースカード (NIC)**

IP リンクへのインタフェースとして動作する、内蔵または別個のカードの形をとるネットワークアダプタ。

**時間情報プロトコル
(NTP)**

Network Time Protocol の略。Solaris の時刻を遠隔ホストの時刻と同期する。

は

- ハートビート割り込み** SC から読み出せる、通常の Solaris OS インジケータへの割り込み。実行中の Solaris システムのハートビートがない場合、通常は Solaris がハングアップしている。
- パスグループ** 同一の装置または 1 セットの装置へのアクセスを提供する、2 通りのパスのセット。
- ファイバチャネル
モジュール** ディスクアレイポートに接続できるディスクアレイコントローラ上にある、光通信接続 (OLC) モジュール。
- 物理パス** ホストからディスクまたはネットワークへの電氣的なパス。
- ブラックリスト** hpost(1M) が起動時に読み込むテキストファイル。ブラックリストファイルでは、システムで使用または構成されない Sun Fire ハイエンドシステムのコンポーネントを指定する。プラットフォームまたはドメインのブラックリストファイルは、enablecomponent および disablecomponent コマンドを使用して編集できる。ASR ブラックリストは、esmd で作成および編集される。

ま

- メールボックス** 「Mbox」を参照してください。
- メタディスク** ディスクを抽象化して、物理的には 2 本のパスにあるグループへのアクセスを 1 つのディスクにすること。
- メタネットワーク** ネットワークを抽象化して、物理的には 2 本のパスにあるグループへのアクセスを 1 つのネットワークにすること。

わ

- 割り当てられている
ボードのリスト** ドメイン管理者または構成者の特権を持つユーザーによりドメインに割り当てられているコンポーネントのリスト。pcd(1M) デーモンがこのリストの状態を保持する。

索引

A

ACL の設定, 89
addboard, 92, 107
addcodlicense, 152
addtag, 91

C

cancelcmdsync, 236
Capacity on Demand (COD), 148
 RTU (right-to-use) ライセンス, 148
 キー, 151, 153
 取得, 151
 証明書, 148
 割り当て, 149
 インスタントアクセス CPU (ヘッドルーム), 150
 資源
 CPU のステータス, 162, 164
 監視, 150, 158, 160
 設定, 155
 シャーシのホスト ID, 75, 157, 165
 必要事項, 151
codd, 56
console, 12

D

dca, 57

DCU, 3, 4, 86, 87
 割り当て, 87
deleteboard, 94, 109
deletecodlicense, 153
disablecomponent, 175
dsmd, 58
dxs, 59

E

efhd, 60
elad, 61
enablecomponent, 178
erd, 62
esmd, 62

F

fomd, 63
frad, 64

H

hwad, 65

I

initcmdsync, 235, 237

K

kmd, 67

M

man, 71

mld, 72

moveboard, 95, 111

N

NIC, 188

ntpd

構成, 103

NVRAM, 119

O

OpenBoot PROM (OBP), 117

osd, 73

P

pcd, 74

POST

ハードウェア障害, 133

poweroff, 169

poweron, 169

R

reset, 172

resetsc, 183

runcmdsync, 236

S

savecmdsync, 236

setbus, 124

setcsn, 76

setdate, 102

setdefaults, 96, 113

setfailover, 230

setkeyswitch, 116, 119, 123, 164

setobpparams, 119

setupplatform, 89, 155

showboards, 97, 114, 198

showbus, 125

showcmdsync, 236, 237

showcodlicense, 153

showcodusage, 159

showdate, 102

showdevices, 115, 198

showenvironment, 198

showfailover, 232

showkeyswitch, 203

showlogs, 130, 145, 165, 208

showobpparams, 119, 199

showplatform, 99, 114, 165, 199

showxirstate, 202

SMS

機能, 3, 4

デーモン, 52

SMS デーモン, 52

smsbackup, 247

smsconfig, 252

smsconnectsc, 14

SMSETC, 83

SMSLOGGER, 83

SMSOPT, 83

smsrestore, 248

SMSVAR, 83

smsversion, 249

Solaris オペレーティング環境, 132

Solaris のハートビート, 202

SRS Net Connect, 129

ssd, 77

Sun Management Center, 129

T

testemail, 142
tmd, 81

W

wcapp, 56

X

xntpd
構成, 103

い

イベント
イベントのリスト, 145
エラーレポート, 145
クラス, 136
コード, 136, 145
ログ, 145

か

環境変数
SMSETC, 83
SMSLOGGER, 83
SMSOPT, 83
SMSVAR, 83

き

機能が低下した構成の設定の変更, 124

く

グローバル自動 DR, 88

こ

コマンド

addboard, 92, 107
addcodlicense, 152
addtag, 91
cancelcmdsync, 236
console, 12, 193
deleteboard, 94, 109
deletecodlicense, 153
disablecomponent, 175
enablecomponent, 178
flashupdate, 106
initcmdsync, 235, 237
moveboard, 95, 111
poweroff, 169
poweron, 169
reset, 172
resetsc, 183
runcmdsync, 236
savecmdsync, 236
setbus, 124
setcsn, 76
setdate, 102
setdefaults, 96, 113
setfailover, 230
setkeyswitch, 116, 119, 123, 164
setobpparams, 119, 120
setupplatform, 89, 155
showboards, 97, 114, 198
showbus, 125
showcmdsync, 236, 237
showcodlicense, 153
showcodusage, 159
showdate, 102
showdevices, 115, 198
showenvironment, 198
showfailover, 232
showkeyswitch, 203
showlogs, 130, 145, 165, 208
showobpparams, 119, 199
showplatform, 99, 114, 165, 199
showxirstate, 202
smsbackup, 247
smsconfig, 252
smsconnectsc, 14
smsrestore, 248

- smsversion, 249
- testemail, 142
 - コンソール, 11
- コンソール, 11
- コントローラボード, 6
- コンポーネントの健全性ステータス, 130, 132

し

- システムコントローラ, 1
- 自動診断および自動回復, 127
 - イベントログ, 130
 - エラーと障害イベントの報告, 129, 132
 - コンポーネントの健全性ステータス, 130, 132
 - 診断エンジン、種類, 129, 132, 133
 - 電子メールイベント通知, 129, 133
- domains
 - ハードウェアエラー, 127
 - ドメインの回復, 130
 - ハードウェアエラーの検出, 128, 131, 133
 - リソースの構成解除, 132
- シャーシのシリアル番号, 75, 137, 145
- シャーシのホスト ID, 75, 157, 165
- 使用可能構成要素リスト, 89
- 診断エンジン, 127, 136

せ

- 静的および動的なドメイン構成, 87

て

- デーモン, 52
 - codd, 56
 - dca, 57
 - dsmd, 58
 - dxs, 59
 - efhd, 60
 - elad, 61
 - erd, 62
 - esmd, 62
 - fomd, 63

- frad, 64
- hwad, 65
- kmd, 67
- man, 71
- mld, 72
- osd, 73
- pcd, 74
- ssd, 77
- tmd, 81
- wcapp, 56

- デュアルコントローラボード, 6
- 電子メールイベント通知, 129, 133
 - テスト, 142
 - 電子メール制御ファイル, 134, 138
 - 電子メールテンプレート, 134, 135

と

- 動的再構成
 - グローバル自動, 88
 - サポート, 195
- 動的システムドメイン, 1
- ドメイン, 1
 - addtag, 91
 - コンソール, 193
 - 自動回復, 130
 - ハードウェアエラー, 128, 131
- ドメイン構成ユニット, 86, 87
 - DCU, 3, 4
- ドメインコンソール, 193
- ドメインの削除
 - コマンド行, 94, 95, 109, 111
- ドメインのステータス
 - ドメインステータス, 99, 114
- ドメインの追加, 92, 107
- ドメインの命名
 - コマンド行, 91

ね

- ネットワークインタフェースカード, 188
- ネットワークタイムプロトコルデーモン

構成, 103

ふ

ファイル

ntp.conf, 103

ブラックリスト

プラットフォームおよびドメイン, 174, 180

ほ

ホットスペア, 150

め

メッセージ

イベント, 144

ロギング, 207

ログ, 195

ろ

ログ

イベント, 130, 145

情報の種類, 209

ファイルの保守, 208

メッセージ, 195, 207

ログファイルの管理, 212

