Oracle® Solaris Cluster 4.4 セキュリティーガイドライン

Part No: E75683-01
2018 年 8 月

Part No: E75683-01

Copyright © 2000, 2018, Oracle and/or its affiliates. All rights reserved.

このソフトウェアおよび関連ドキュメントの使用と開示は、ライセンス契約の制約条件に従うものとし、知的財産に関する法律により保護されています。ライセンス契約で明示的に許諾されている場合もしくは法律によって認められている場合を除き、形式、手段に関係なく、いかなる部分も使用、複写、複製、翻訳、放送、修正、ライセンス供与、送信、配布、発表、実行、公開または表示することはできません。このソフトウェアのリバース・エンジニアリング、逆アセンブル、逆コンパイルは互換性のために法律によって規定されている場合を除き、禁止されています。

ここに記載された情報は予告なしに変更される場合があります。また、誤りが無いことの保証はいたしかねます。誤りを見つけた場合は、オラクルまでご連絡ください。

このソフトウェアまたは関連ドキュメントを、米国政府機関もしくは米国政府機関に代わってこのソフトウェアまたは関連ドキュメントをライセンスされた者に提供する場合は、次の通知が適用されます。

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

このソフトウェアまたはハードウェアは様々な情報管理アプリケーションでの一般的な使用のために開発されたものです。このソフトウェアまたはハードウェアは、危険が伴うアプリケーション(人的傷害を発生させる可能性があるアプリケーションを含む)への用途を目的として開発されていません。このソフトウェアまたはハードウェアを危険が伴うアプリケーションで使用する際、安全に使用するために、適切な安全装置、バックアップ、冗長性(redundancy)、その他の対策を講じることは使用者の責任となります。このソフトウェアまたはハードウェアを危険が伴うアプリケーションで使用したことに起因して損害が発生しても、Oracle Corporationおよびその関連会社は一切の責任を負いかねます。

OracleおよびJavaはオラクル およびその関連会社の登録商標です。その他の社名、商品名等は各社の商標または登録商標である場合があります。

Intel、Intel Xeonは、Intel Corporationの商標または登録商標です。すべてのSPARCの商標はライセンスをもとに使用し、SPARC International, Inc.の商標または登録商標です。AMD、Opteron、AMDロゴ、AMD Opteronロゴは、Advanced Micro Devices, Inc.の商標または登録商標です。UNIXは、The Open Groupの登録商標です。

このソフトウェアまたはハードウェア、そしてドキュメントは、第三者のコンテンツ、製品、サービスへのアクセス、あるいはそれらに関する情報を提供することがあります。適用されるお客様とOracle Corporationとの間の契約に別段の定めがある場合を除いて、Oracle Corporationおよびその関連会社は、第三者のコンテンツ、製品、サービスに関して一切の責任を負わず、いかなる保証もいたしません。適用されるお客様とOracle Corporationとの間の契約に定めがある場合を除いて、Oracle Corporationおよびその関連会社は、第三者のコンテンツ、製品、サービスへのアクセスまたは使用によって損失、費用、あるいは損害が発生しても一切の責任を負いかねます。

ドキュメントのアクセシビリティについて

オラクルのアクセシビリティについての詳細情報は、Oracle Accessibility ProgramのWeb サイト(`http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`)を参照してください。

Oracle Supportへのアクセス

サポートをご契約のお客様には、My Oracle Supportを通して電子支援サービスを提供しています。詳細情報は(`http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info`) か、聴覚に障害のあるお客様は (`http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs`)を参照してください。

目次

このドキュメントの使用法 7

1 Oracle Solaris Cluster セキュリティーの概要 9
Oracle Solaris Cluster とセキュリティーの概要 10
障害回復フレームワークとセキュリティーの概要 10
一般的なセキュリティーの原則 11
Oracle Solaris Cluster のセキュアなインストールおよび構成 11
Geographic Edition のセキュアなインストールおよび構成 12
Oracle Solaris Cluster のセキュリティー機能 13
障害回復フレームワークのセキュリティー機能 15
開発者向けのセキュリティーの考慮事項 16

索引 19

このドキュメントの使用法

- **概要** – Oracle Solaris Cluster 製品をセキュアにインストール、構成、および使用する方法について説明します。
- **対象読者** – 技術者、システム管理者、および認定サービスプロバイダ
- **前提知識** – ハードウェアのトラブルシューティングや交換に関する豊富な経験

製品ドキュメントライブラリ

この製品および関連製品のドキュメントとリソースは `http://www.oracle.com/pls/topic/lookup?ctx=E75635-01` で入手可能です。

フィードバック

このドキュメントに関するフィードバックを `http://www.oracle.com/goto/docfeedback` からお聞かせください。

第 1 章

Oracle Solaris Cluster セキュリティーの概要

Oracle Solaris Cluster 製品は、高可用性サービスおよびスケーラブルなサービスの作成に使用できる統合されたハードウェアおよびソフトウェアソリューションです。このガイドでは、Oracle Solaris Cluster のセキュリティーの概要、セキュアなインストールと構成に関する情報、セキュリティー機能、および開発者向けのセキュリティーの考慮事項について説明します。このガイドと Oracle Solaris Cluster のマニュアルセット全体を使用して、Oracle Solaris Cluster ソフトウェアの全体像が提供されます。

障害回復フレームワークは、Oracle Solaris Cluster ソフトウェアの階層化された拡張です。障害回復フレームワークは、地理的に長距離を隔てられた複数のクラスタを使用することによる予期しない障害からアプリケーションを保護します。これらのクラスタは、クラスタ間でレプリケートされたデータを管理する障害回復フレームワークのコピーを格納します。

この章で説明する内容は次のとおりです。

- 10 ページの「Oracle Solaris Cluster とセキュリティーの概要」
- 10 ページの「障害回復フレームワークとセキュリティーの概要」
- 11 ページの「一般的なセキュリティーの原則」
- 11 ページの「Oracle Solaris Cluster のセキュアなインストールおよび構成」
- 12 ページの「Geographic Edition のセキュアなインストールおよび構成」
- 13 ページの「Oracle Solaris Cluster のセキュリティー機能」
- 15 ページの「障害回復フレームワークのセキュリティー機能」
- 16 ページの「開発者向けのセキュリティーの考慮事項」

Oracle Solaris オペレーティングシステム (OS) のセキュリティーの詳細は、『Oracle Solaris 12 セキュリティーと強化ガイドライン』および『Oracle Solaris 11.4 でのシステムおよび接続されたデバイスのセキュリティー保護』を参照してください。

Oracle Solaris Cluster とセキュリティーの概要

Oracle Solaris Cluster 環境は、Oracle Solaris オペレーティングシステムをクラスタオペレーティングシステムに拡張します。クラスタは 1 つ以上のノードのコレクションで、各ノードはこのコレクションに排他的に属しています。

Oracle Solaris Cluster ソフトウェアを使用すると、次のような利点があります。

- ソフトウェアやハードウェアの障害によるシステムの停止時間が削減される
- 通常はシングルサーバーシステムが停止してしまうような障害が発生しても、エンドユーザーがデータやアプリケーションを使用できる
- クラスタにノードを追加して負荷を分散することで、追加のプロセッサに合わせてサービスを拡張できるため、アプリケーションのスループットが向上する
- クラスタ全体を停止しなくても保守を行うことができるため、システムの可用性が向上する

クラスタは従来のシングルサーバーシステムと比較して複数のメリットを提供します。これらのメリットには、フェイルオーバーとスケーラブルサービスのサポート、モジュール化成長機能、ノードに対する負荷制限の設定機能、従来のハードウェア耐障害性システムに比べて低いエントリ価格などが含まれます。

Oracle Solaris OS で実行されるクラスタのタイプには、グローバルクラスタとゾーンクラスタがあります。クラスタはグローバルクラスタ、ゾーンクラスタ、または両方の組み合わせに指定できます。ゾーンクラスタの構成による利点の詳細は、『Concepts for Oracle Solaris Cluster 4.4』を参照してください。

障害回復フレームワークとセキュリティーの概要

Oracle Solaris Cluster 障害回復フレームワークは、Oracle Solaris Cluster ソフトウェアの階層化された拡張です。データレプリケーションソフトウェアを使用すると、障害回復パートナークラスタで実行されているアプリケーションは、地理的に離れたセカンダリクラスタにサービスを移行することで障害に対応できます。地震、火災、暴雨などの災害によって、プライマリサイトのクラスタが無効になることがあります。

障害が発生した場合、パートナークラスタは、次のレベルの冗長性を使用することでサービスを引き続き提供できます。

- セカンダリクラスタ
- セカンダリクラスタに複製されたアプリケーション構成
- セカンダリクラスタにレプリケートされたデータ

障害回復フレームワークは、地理的に離れているクラスタをサイト間のサービスの移行によって管理および構成する一連のツールを提供します。クラスタはグローバルクラスタ、ゾーンクラスタ、または両方の組み合わせに指定できます。障害回復フレームワークは、堅牢なセキュリティー、アプリケーションサービスの移行、およびデータレプリケーションによってエンタープライズシステム全体の障害に対応することで、複数の物理的な場所で可用性を管理できます。

一般的なセキュリティーの原則

Oracle Solaris Cluster のアプリケーションをセキュアに使うために、次の原則が重要になります。

- ソフトウェアを最新の状態に維持します
- 重要なサービスへのネットワークアクセスを制限します
- 最少特権の原則に従います
- システムの動作状態をモニターします
- Oracle の最新のセキュリティー情報を入手します

Oracle Solaris Cluster のセキュアなインストールおよび構成

このセクションでは、Oracle Solaris Cluster ソフトウェアのセキュアなインストールと構成を計画して実行するためのリンクを示します。

- **インストール** – Oracle Solaris Automated Installer (AI) を使用すると Oracle Solaris Cluster ソフトウェアをインストールできます。詳細は、『安装和配置 Oracle Solaris Cluster 4.4 环境』 の 「ソフトウェアのインストール」を参照してください。
- **クラスタパッケージ** – Oracle Solaris Cluster パッケージでは Oracle Solaris Image Packaging System (IPS) のパッケージ名を使用します。

  Oracle Solaris Cluster コア、データサービス、および障害回復フレームワークパッケージのリストを確認するには、『Package Group Lists for Oracle Solaris Cluster 4.4』を参照してください。
- **構成** – グローバルクラスタとゾーンクラスタを構成して管理できます。詳細は、『安装和配置 Oracle Solaris Cluster 4.4 环境』 の 第 3 章,「グローバルクラスタの確立」、『安装和配置 Oracle Solaris Cluster 4.4 环境』 の 第 6 章,「ゾーンクラスタの作成」、および『管理 Oracle Solaris Cluster 4.4 配置』 の 第 1 章,「Oracle Solaris Cluster の管理の概要」を参照してください。

  `clinstall` インストール方法およびグローバルクラスタノードを確立するためのすべての方法について、1 つの指定制御ノードの事前の承認が必要です。それにより、指定されたシステムのみが構成するノードへのアクセスを許可されま

す。必要に応じて、よりセキュアな構成には DES 暗号化を使用できます。詳細は、`clauth(8CL)` のマニュアルページを参照してください。

- **共通エージェントコンテナの脆弱性** – 共通エージェントコンテナといくつかの古い Java バージョンの組み合わせでは、Oracle Solaris Cluster ソフトウェアにセキュリティーの脆弱性が生じます。使用しているシステムにこの脆弱性があるかどうかを識別する方法、およびの修正方法の詳細は、My Oracle Support の参照ドキュメント 『CVE-2014-3566 Oracle Solaris Cluster で SSL v3.0 の脆弱性 (別名「プードル攻撃」) を軽減するための手順 (Doc ID 1999997.1)』 (`https://support.oracle.com/epmos/faces/DocumentDisplay?id=1999997.1&displayIndex=1`) を参照してください。このドキュメントには My Oracle Support のログインが必要です。
- **Kerberos V5 でセキュリティー保護された HA for NFS** – HA for NFS データサービスで管理されている NFS サービスへのアクセスをセキュリティー保護する必要がある場合は、HA for NFS データサービスをセキュリティー保護するように Kerberos V5 クライアントを構成できます。これには、すべてのクラスタノード上の論理ホスト名における NFS のための Kerberos 主体の追加が含まれます。詳細は、『Oracle Solaris Cluster Data Service for NFS Guide』 の 「Securing HA for NFS With Kerberos V5」を参照してください。

Geographic Edition のセキュアなインストールおよび構成

このセクションでは、障害回復フレームワークのセキュアなインストールおよび構成を計画および実行するためのリンクを提供します。

- **インストール** – 障害回復フレームワークソフトウェアは、Oracle Solaris オペレーティングシステムおよび Oracle Solaris Cluster ソフトウェアを実行しているクラスタにインストールする必要があります。Oracle Solaris Automated Installer (AI) を使用して、Oracle Solaris Cluster ソフトウェアのインストールと同時に、またはあとから任意の時点で障害回復フレームワークソフトウェアをインストールします。障害回復フレームワーク構成は Oracle Solaris Cluster ソフトウェア構成と同一です。『Installing and Configuring the Disaster Recovery Framework for Oracle Solaris Cluster 4.4』 の 第 2 章, 「Installing and Configuring the Disaster Recovery Framework Software」を参照してください。
- **障害回復フレームワークパッケージ** – 障害回復フレームワークパッケージは Oracle Solaris Image Packaging System (IPS) パッケージ名を使用します。パッケージのリストを確認するには、『Package Group Lists for Oracle Solaris Cluster 4.4』を参照してください。
- **構成** – どのノードやクラスタでも障害を発生させずに、障害回復フレームワークを実行しているクラスタですべての管理タスクを実行できます。動作クラスタ上の障害回復フレームワークをインストール、構成、開始、使用、停止、およびアンインストールできます。『Administering the Disaster Recovery Framework for Oracle Solaris Cluster 4.4』 の 第 4 章, 「Administering Rights Profiles」を参照してください。

Oracle Solaris Cluster のセキュリティー機能

このセクションでは、Oracle Solaris Cluster ソフトウェアが提供する具体的なセキュリティーメカニズムについて説明します。

セキュアなインストールを行うには、次のクリティカルなセキュリティー機能を使用します。

- **セキュリティーコンプライアンス** – Oracle Solaris Cluster が構成されて実行されているとき、デフォルトのコンプライアンスプロファイル Solaris `Recommended` は内部および外部のセキュリティー要件に対するコンプライアンスを満たしているか Oracle Solaris Cluster をテストします。Oracle Solaris Cluster のみに関連したチェックのカスタマイズされたリストについては、`compliance tailor` コマンドを使用します。コンプライアンスプロファイルおよびプロファイルのカスタマイズの詳細は、『Oracle Solaris 12 セキュリティーコンプライアンスガイド』を参照してください。
- **クラスタに対する承認** – クラスタにアクセスするには、`solaris.cluster.modify`、`solaris.cluster.admin`、および `solaris.cluster.read` の役割に基づくアクセス制御 (RBAC) 承認を使用します。役割のほとんどのセキュリティー属性を変更するには、User Security 権利プロファイルが割り当てられている管理者になる必要があります。詳細は、『Oracle Solaris 11.4 でのユーザーとプロセスのセキュリティー保護』 の 「権利使用の管理」および『管理 Oracle Solaris Cluster 4.4 配置』 の 「Oracle Solaris Cluster の承認」を参照してください。
- **IP Security Architecture (IPsec)** – `clprivnetinterface` に対して IPsec を構成して、クラスタインターコネクト上のセキュアな TCP/IP 通信を提供します。

  詳細は、『安装和配置 Oracle Solaris Cluster 4.4 环境』 の 「Oracle Solaris Cluster インターコネクトの IPsec によるセキュリティー保護」を参照してください。
- **新しいノード** – クラスタにノードを追加するには、権限のある `claccess` コマンドまたは `clsetup` ユーティリティーを使用します。詳細は、『管理 Oracle Solaris Cluster 4.4 配置』 の 第 8 章, 「クラスタノードの管理」を参照してください。

  アクセスステータスのデフォルト設定は `claccess deny-all` です。この設定を変更するのは、新しいノードの追加など、特権付きの操作を実行する場合のみです。操作を終了したら `deny-all` ステータスを元に戻す必要があります。クラスタ構成を頻繁に変更することが予想される場合は、`/usr/cluster/bin/claccess -p protocol=authentication-protocol` コマンドを使用してよりセキュアな認証プロトコルを選択することで、新しいシステムの信頼を最大限に確保できます。詳細は、`claccess(8CL)` マニュアルページおよび『Managing Authentication in Oracle Solaris 11.4』 の 第 5 章, 「Using Secure RPC on Oracle Solaris」を参照してください。
- **Trusted Extensions** – Oracle Solaris Trusted Extensions 機能はゾーンクラスタで使用するように設定できます。詳細は、『安装和配置 Oracle Solaris Cluster 4.4 环境』 の 「ゾーンクラスタにおける Trusted Extensions のガイドライン」および『安装和

配置 Oracle Solaris Cluster 4.4 環境』 の 「Trusted Extensions をインストールおよび構成する方法」を参照してください。

- **ゾーンクラスタ** – ゾーンクラスタは、`cluster` 属性が設定された `solaris` ブランド、`solaris10` ブランド、または `labeled` ブランドの 1 つ以上の非大域ゾーンで構成されます。A `labeled` ブランドゾーンクラスタは、Oracle Solaris ソフトウェアの Trusted Extensions でのみ使用します。

  `clzonecluster` コマンドまたは `clsetup` ユーティリティーを使用して、ゾーンクラスタを作成します。Oracle Solaris ゾーンで提供される分離を含めて、グローバルクラスタと同様にゾーンクラスタでサポートされるサービスを実行できます。詳細は、『安装和配置 Oracle Solaris Cluster 4.4 环境』 の 「ゾーンクラスタの作成および構成」および『管理 Oracle Solaris Cluster 4.4 配置』 の 「ゾーンクラスタに関する作業」を参照してください。

- **クラスタコンソールへのセキュア接続** – クラスタノードのコンソールにはセキュアシェル接続を確立する必要があります。`pconsole` ユーティリティーの詳細は、『管理 Oracle Solaris Cluster 4.4 配置』 の 「クラスタコンソールに安全に接続する方法」を参照してください。

- **共通エージェントコンテナ** – Oracle Solaris Cluster Manager ブラウザインタフェースは強力な暗号化技術を使用して、各クラスタノード上にある Oracle Solaris Cluster 管理スタック間の通信をセキュリティー保護します。詳細は、『管理 Oracle Solaris Cluster 4.4 配置』 の 「Oracle Solaris Cluster Manager の管理とトラブルシューティング」を参照してください。

- **ロギング** – Oracle Solaris Cluster ソフトウェアでは、`syslogd` コマンドを使用して、エラーメッセージおよびステータスメッセージを記録します。メッセージの格納場所を制御する `/etc/syslog.conf` ファイルを必ず設定してください。また、`/var/adm/messages` ファイルなどのログファイルのセキュリティー保護も必要です。詳細は、『管理 Oracle Solaris Cluster 4.4 配置』 の 「クラスタの管理」を参照してください。

- **Auditing** – Oracle Solaris Cluster 監査は Oracle Solaris オペレーティングシステム内に存在するため、デフォルトで有効になっています。監査により、実行されたすべてのコマンドは `/var/cluster/logs/commandlog` ファイルに保管されます。

  このファイルは `root` の役割によってのみ読み込みおよび書き込み可能です。Oracle Solaris Cluster Management の権利プロファイルを割り当てた root 以外の役割に対してクラスタ管理の側面を委任したとき、これらのユーザーに、保護されたこれらのクラスタログファイルを読み取る権限を付与する場合もあります。この操作はユーザーに対するアクセス制御リスト (ACL) を `commandlog` ファイルに追加することによって行うことができます。

  `commandlog` ファイルの表示の詳細は、『管理 Oracle Solaris Cluster 4.4 配置』 の 「Oracle Solaris Cluster のコマンドログの内容を表示する方法」を参照してください。Oracle Solaris ACL モードの詳細は、the `chmod(1)` マニュアルページおよび『Securing Files and Verifying File Integrity in Oracle Solaris 11.4』 の 第 2 章, 「Using ACLs and Attributes to Protect Oracle Solaris ZFS Files」を参照してください。

- **Oracle Solaris オペレーティングシステムの強化** – Oracle Solaris Cluster ソフトウェアはセキュリティー強化技術を使用して Oracle Solaris オペレーティングシステムを強化された状態に再構成します。さらに、Oracle Solaris システムの監査をアクティブ化できます。

障害回復フレームワークのセキュリティー機能

このセクションでは、Oracle Solaris Cluster 障害回復フレームワーク (以前の Geographic Edition) が提供する具体的なセキュリティーメカニズムについて説明します。

セキュアなインストールを行うには、次のクリティカルなセキュリティー機能を使用します。

- **障害回復フレームワーク承認** – 障害回復フレームワークの権利プロファイルは、コアの Oracle Solaris Cluster ソフトウェアによって使用される権利プロファイルに基づいています。役割のほとんどのセキュリティー属性を変更するには、User Security 権利プロファイルが割り当てられている管理者になる必要があります。`root` 役割を担い、`solaris.cluster.geo.modify`、`solaris.cluster.geo.admin`、および `solaris.cluster.geo.read` 承認を持つ役割を使用してクラスタ内の障害回復フレームワークにアクセスします。詳細は、『Oracle Solaris 11.4 でのユーザーとプロセスのセキュリティー保護』および『Administering the Disaster Recovery Framework for Oracle Solaris Cluster 4.4』の「Modifying a User's Rights」を参照してください。
- **セキュリティー証明書** – インストール中に、セキュリティー証明書を使用してセキュアなクラスタ通信のためにクラスタが構成されます (同じクラスタ内のノードは同じセキュリティー証明書を共有する必要があります)。Geographic Edition パートナーシップでのクラスタ間の通信は、セキュリティー証明書を使用して、Secure Sockets Layer (SSL) で Java Management Extensions (JMX) ポートを経由することでセキュリティー保護されます。詳細は、『Installing and Configuring the Disaster Recovery Framework for Oracle Solaris Cluster 4.4』の「Configuring Trust Between Partner Clusters」を参照してください。
- **共通エージェントコンテナ** – ゾーンクラスタが障害回復フレームワークパートナーシップのメンバーとして機能できるには、共通エージェントコンテナをゾーンクラスタ内で手動で構成する必要があります。詳細は、『Installing and Configuring the Disaster Recovery Framework for Oracle Solaris Cluster 4.4』の「Preparing a Zone Cluster for Partner Membership」を参照してください。
- **IP Security Architecture (IPsec)** – IPsec を使用して、パートナークラスタ間のセキュアな TCP/UDP ハートビート通信を構成します。詳細は、『Installing and Configuring the Disaster Recovery Framework for Oracle Solaris Cluster 4.4』の「Securing Inter-Cluster Communication」を参照してください。

開発者向けのセキュリティーの考慮事項

このセクションでは、Oracle Solaris Cluster ソフトウェアを使用してアプリケーションを作成する開発者にとって役立つ情報を提供します。開発者は V API を使用します。詳細は、『Concepts for Oracle Solaris Cluster 4.4』 の 第 3 章,「Key Concepts for System Administrators and Application Developers」を参照してください。

開発者が作成するエージェントアプリケーションは、製品のセキュリティーフレームワーク内で動作し、次のセキュリティー機能を考慮する必要があります。

- **エージェントコールバックメソッド** – Oracle Solaris Cluster ソフトウェアは広範囲のアプリケーションエージェントをサポートしています。これらは一連のコールバックメソッドとして実装され、アプリケーションの起動、停止、プローブ、検証を制御します。`Start`、`Stop`、`Validate` などのコールバックメソッドは常に root として実行されます。これらの実行可能メソッドファイルに root ユーザー以外が書き込み可能な場合には脆弱性が発生し、非 root ユーザーがコールバックメソッドにコードを挿入することで、不正に権限を引き上げることが可能になってしまいます。Oracle Solaris Cluster ソフトウェアはそのようなコールバックメソッド実行可能ファイルの所有権およびアクセス権を調べます。このチェックは `resource_security` クラスタプロパティー設定によって制御されます。`resource_security` が `SECURE` に設定されており、メソッドコードに非 root ユーザーが書き込み可能であることが判明した場合、メソッドの実行は失敗します。

  一方、エージェントメソッドは、アプリケーション固有の管理コマンドなどの外部プログラムをしばしば実行します。エージェントメソッドはこうした外部プログラムをすべてラッパーを使用して実行することで、外部プログラムが可能なかぎり最小限の権限で実行されるようにする必要があります。Oracle Solaris Cluster ソフトウェアでは `application_user` および `resource_security` プロパティーと `scha_check_app_user` API が提供されており、アプリケーションがセキュアに実行されていることをデータサービスで確認できるようになっています。`scha_check_app_user` コマンドをスクリプトで呼び出すことで、構成済みの `Application_user` および `Resource_security` 設定に対してユーザー名を検証できます。詳細は、`scha_check_app_user(8HA)`、`r_properties(7)`、および `cluster(8CL)` のマニュアルページを参照してください。
- **アプリケーションへのセキュアなアクセス** – 管理コマンドまたは構成コマンドを発行する場合、アプリケーションへのセキュアなアクセスが必要になることがあります。このセキュアなアクセスは、Oracle Wallet Manager などの資格証明に基づくメソッドで実行する必要があります。パスワードを指定する必要がある場合、パスワードは不明瞭化されたフォームでセキュアに使用して格納する必要があります。たとえば、`ps` コマンドを使用してユーザーが表示できるコマンド行に渡すことはできません。Oracle Solaris Cluster ソフトウェアでは、プライベート文字列を作成するための `clpstring` コマンドが提供されています。このプライベート文字列は、エンコードされたパスワードをクラスタ内にセキュアに保存するために使用でき、管理タスクを実行するためにパスワードの使用が必要な場合に取得できま

す。このコマンドについては、clpstring(8CL) のマニュアルページを参照してください。

データサービスを開発するときのこれらのセキュリティー機能の使用方法の詳細は、『Developing Data Services』を参照してください。

索引

あ

アプリケーションへのセキュアなアクセス, 16
インストール, 11
オペレーティングシステムの強化, 15

か

開発者
　セキュリティーの考慮事項, 16
概要
　Oracle Solaris Cluster, 10
　Oracle Solaris Cluster 障害回復フレームワーク, 10
共通エージェントコンテナ, 15
クラスタ
　インストール, 11
　構成, 11
　セキュリティー機能, 13
クラスタコンソールへのセキュア接続, 14
グローバルクラスタ, 10
構成, 11, 12
コンプライアンス, 13

さ

障害回復, 10
障害回復フレームワーク
　概要, 10
　セキュリティー機能, 15
　利点, 10
承認
　クラスタ, 13
　障害回復フレームワーク, 15
セキュリティー
　一般原理, 10
　開発者向けの考慮事項, 16
　障害回復フレームワークのインストール, 12
　証明書, 15
セキュリティー機能
　障害回復フレームワーク, 15
ゾーンクラスタ, 10
　labeled ブランド, 14
　Trusted Extensions, 13

た

データレプリケーション, 10

な

ノードの追加, 13

は

パッケージ
　Oracle Solaris Cluster, 11
　Oracle Solaris Cluster 障害回復フレームワーク, 12

ら

ロギング, 14

A

auditing, 14

Automated Installer, 11, 12
disaster recovery framework, 11

C
`claccess` コマンド, 13
`clauth` コマンド, 11
`clsetup` ユーティリティー, 13

G
Geographic Edition 参照 障害回復フレームワーク
global cluster, 11

I
IP Security Architecture (IPsec), 13
IPsec, 13, 15

L
labeled ブランドゾーンクラスタ, 14

O
Oracle Solaris Cluster
　概要, 10
　セキュリティー, 10
Oracle Solaris Cluster 障害回復フレームワーク
　インストール, 12
　構成, 12

P
`pconsole` ユーティリティー, 14

T
Trusted Extensions, 13

Z
zone clusters