Solaris パッチ管理:
推奨手法

ホワイトペーパー

日本語版発行
August 2005
Part No.817-0575-12

英語版 ORG
Part No. 817-0574-12
Revision 3, August 2004

目次

はじめに

パッチの適用やソフトウェアリリースから次のソフトウェアリリースへのシステムの更新は、複雑で時間を要するプロセスへと変化しています。新しいパッチが適用されるたびにソフトウェアの層が増えるため、ソフトウェアを更新するための手法には、再検討と明確化が必要となります。また IT プロフェッショナルは、使用可能な中で最適のソフトウェアがインストールされているように、システムを管理する必要もあります。

さらに近年、問題を悪用するプログラムの出現から CERT 勧告までの平均時間が短くなっていると同時に、ハッカーによるセキュリティー問題の悪用の数は驚異的に増大しています。使用すべきソフトウェア更新とパッチ、およびそれらを適用すべきタイミングを知っておくことは、IT プロフェッショナルにとって重大な課題となっています。

そのため、パッチの選択と適用に関してベンダーに支援を依頼するカスタマの数はますます増えています。すべてのパッチに関して最新の状態を維持しようとするポリシーを実践している IT 管理者がいる一方、適用するパッチの数を最小限にすることを推奨する業界のエキスパートもいます。

このホワイトペーパーは Sun のカスタマを対象としており、パッチおよびソフトウェア更新を管理するための Sun の推奨手法を説明しています。また、このホワイトペーパーでは、適切にパッチが適用され、更新されたソフトウェアを維持するための推奨手法とプロセスについても説明しています。ソフトウェア更新のリスク、コスト、タイミングに関する説明や、Sun のパッチ関連のツールへのリファレンスもあります。

注: 一般にパッチは、ソフトウェアの機能、性能、信頼性、データの完全性、セキュリティーなどの既知の問題に対するバグ修正に関連するものです。パッチには、特定のソフトウェアリリースに対する新機能や機能拡張が含まれていることがあります。ソフトウェア更新にはバグ修正に対するパッチだけでなく、新機能、機能拡張、新しいハードウェアのサポート、およびそのほかのパッチを適用できるようにするパッチが含まれています。 このホワイトペーパーの情報の大部分は、パッチとソフトウェア更新の両方に適用できます。

ソフトウェア更新の推奨手法

ソフトウェアを更新するための Sun の推奨手法には、次の手法が含まれます。

- リスク、コスト、可用性、およびタイミングに基づいて、パッチ適用またはソフトウェア更新の必要性を分析する
- 可能な限り環境への変更を最小限にする
- 可能な限り迅速に SunSM Alert Notification などの重大な問題に対処する
- 環境へのそのほかの変更は、既知の問題に対処するためにとどめる
- 業務とアプリケーションのニーズに適合するよう、環境を最新の状態に維持する

リスクとコストを最小限にし、システム全体の可用性の最高レベルを維持するため、Sun は、可能な限り環境に導入する変更の量を最小限にすることを推奨します。また Sun は可能な限り迅速に、重大なセキュリティー、データ損失、および可用性の問題に対処することも推奨します。この目的のため、Sun は推奨パッチクラスタおよび Sun Alert パッチクラスタの使用をサポートしています。ただし、Sun による可用性とパッチ管理データの分析では、重大な問題への対処以外のパッチの追加適用は、システム全体の可用性を低下させ、計画されたダウンタイムおよび計画外のダウンタイムを増やすことが明らかになっています。

推奨パッチクラスタは、すべての Sun Alert 問題への対処に必要なすべてのパッチの最新のバージョンを反映しています。最新の推奨パッチクラスタをシステムに定期的に適用する方針を採用しているカスタマもあります。この手法はすべての Sun Alert の問題に対処しているものの、必要よりも多くの変更をシステムに導入しています。同様に、最新の推奨パッチクラスタを定期的に再適用する必要もありません。

Sun Alert パッチクラスタは、すべての Sun Alert の問題への対処に必要な全パッチの中の最低限のリビジョンと、システムに適用可能な最低限の変更を反映したものです。

つまり、重大な問題に確実に対処するだけでなく、特定の問題やニーズに対応するためにのみパッチを適用すべきである、というのが Sun の見解です。単に最新の状態を維持するためにパッチを適用すべきではありません。パッチに何らかの価値があるかどうかを理解せずに最新リビジョンのパッチを適用しても利益はありません。

新規インストールの場合、環境内で動作する Solaris™ オペレーティングシステム (Solaris OS) の最新リリースを使用して、アプリケーションと業務のニーズをサポートすることを Sun は推奨します。この作業が完了すれば、必要に応じてソフトウェアを更新し、パッチを適用するだけで済みます。Sun のカスタマにはインストールチェックリストと最新の Recommended Patch Set を結び付ける、Enterprise Installation Standards (EIS) Methodology にアクセスできるカスタマもいます。

次の節では推奨事項について説明し、各推奨事項の実装方法を説明します。

推奨手法

ソフトウェアを更新する必要性の分析

たとえわずかなものであっても、環境に変更を導入することには、ある程度のリスクを伴います。リスクにさらされる危険性、受容可能な保守コスト、必要な可用性、更新のタイミングに関連してシステムの環境を分析します。それぞれの適用環境、システム、またはアプリケーションには固有の要件が存在する場合があります。

環境への変更を最小限にする

特定された固有の環境のそれぞれに対して方針が確立されたならば、これらの各環境内での変更を最小限にします。ある変更を実装することに関連するリスクに加え、Sun のデータでは、パッチを適用するためにシステムがオフラインになるため、可用性が低下することが示されています。ただし、ダウンタイムと保守コストを犠牲にしても、たとえばインターネットに直結している Web サーバーに最新のセキュリティーパッチを適用しなければならないことが頻繁にあります「変更を最小限にする」ことは、適用環境が基準になります 。

Sun Alert Notification に対処する

Sun Alert Notification は契約カスタマが利用でき、セキュリティー問題に関して学ぶ 1 つの手段となります。

Sun Alert Notification は特定のハードウェアおよび製品ソフトウェアの問題について説明したもので、ご使用のコンピューティング環境と生産性に対するリスクを提示する場合もあります。Sun Alert Notification は、データ損失、セキュリティー、および可用性の 3 つの領域における潜在的な問題に関する情報を提供します。Sun は、警告がカスタマベースに広範囲に適用されると考えられる場合、Sun Alert Notification を作成します。

Sun Alert Notification によって提示された該当パッチは、可能な限り迅速に適用してください。場合によっては、あるポートへのアクセスを無効にするなど、Sun Alert にはパッチ以外の解決方法が存在する場合があります。このような解決策は、パッチ適用よりもシステム変更の程度が低く、低コストである場合があります。

通常、Sun Alert Notification は定期的にスケジュールされたパッチ管理プロセスから外れたものであり、独自のパッチ管理プロセスを適用する必要があります。このプロセスは、使用している環境とカスタマイズされたプロセスに依存します。次のパッチメンテナンスサイクルまでにパッチを適用するかどうかを決定する前に、潜在的なリスクを慎重に考慮してください。

Sun Alert Notification で提示された問題を解決するすべてのオペレーティング環境関連のパッチは、依存するパッチとともに、推奨パッチクラスタおよび Sun Alert パッチクラスタに含まれています。Sun Alert Notification に詳細が記載されている問題を解決する、オペレーティング環境関連以外のパッチは、使用しているシステム環境に適用可能であるなら、SunSolve Online℠ Web サイトからダウンロードし、適用する必要があります。

定期的に SunSolve℠ サイトを確認し、新しくリリースされた Sun Alert Notification やパッチに関連する情報がないかを調べてください
URL は http://www.sun.com/sunsolve です。

関係する技術担当者は加入手続きを行って、定期的に Sun Alert サマリーレポートを受け取る必要があります。加入手続きを行って、サマリーレポートを受け取るには、http://sunsolve.sun.com/pub-cgi/show.pl?target=salert-notice にアクセスしてください。

既知の問題に対処する

Sun Alert の問題を解決するパッチは多くのカスタマにとって重要ですが、Sun のパッチの大部分は、固有のアプリケーションスイートや環境を持つカスタマなど、少数のカスタマが関心を持つような問題に対処するだけです。

問題が発生し、解決策にパッチの適用が必要である場合、業務環境におけるシステムの現在の状態を慎重に考慮します。以下の質問に対して答えを出してください。

- システムが現在ダウンしていて稼働不能であるか
- システムは稼働しているが、問題となるエラーが発生や障害が発生しているか
- メンテナンスサイクルが十分早く、パッチ適用を待つリスクを受けることができるか

業務のニーズに応じて環境を最新の状態に維持する

環境の維持を開始する最善の方法は、業務とハードウェアの要件に合致する最新のオペレーティングシステムをインストールすることです。これには次のようなメリットがあります。

- システム全般の安定性の向上
- バグ修正を含むソフトウェア開発における最新の改善
- システムのセキュリティーの向上
- システムの性能の向上
- 管理すべきパッチの削減

Solaris OS の最新バージョンを使用していない場合は、業務のニーズを満たす限りにおいて、使用する Solaris OS の最新リリースを実行することが重要になります。たとえば、Solaris 9 OS を使用している場合、(このホワイトペーパーの執筆時点では) 最新リリースは Solaris 9 4/04 です。このリリースには、更新が作成された時点で Solaris 9 OS に使用可能なすべてのパッチが含まれています。Solaris OS の旧バージョンの場合、そのオペレーティングシステムのバージョンに対して存在する最新リリースを使用します。

注: Solaris OS の最新バージョンに対してのみ、ソフトウェア更新が定期的にリリースされます。古い Solaris OS の最新リリースは、購入元から入手できます。

パッチ

この節では、次のパッチ関連のトピックについて説明します。

- パッチの定義
- パッチの種類
- パッチの相互関係
- パッチ配備のメカニズム

パッチの定義

パッチとは、オペレーティングシステムまたはそのほかのサポート対象ソフトウェア内の、既知の問題または潜在的な問題に対する修正をまとめたものです。パッチは、特定のソフトウェアリリースに対して新機能や機能拡張を提供することもできます。パッチは、既存のファイルやディレクトリを置換または更新するファイルとディレクトリから構成されています。

Solaris のパッチの大部分は、スパースパッケージパッチとして配布されます。スパースパッケージパッチは、パッケージが最初にカスタマに配布されてから変更されたオブジェクトのみを含みます。スパースパッケージの配布は、Linux の Red Hat Package Manager (RPM) とは対照的です。たとえば、RPM はオペレーティング環境のコンポーネント全体を置き換えます。スパースパッケージを使用することで、Sun は環境の変更を最小限にするパッチを提供できます。

各パッチは、パッチ ID 番号 (`patch_id`) により識別されます。パッチ ID は、xxxxxx-yy という形式の 6 桁の基本識別子と 2 桁のリビジョン番号から構成されます。

パッチは累積的でもあります。新しいリビジョンには、以前のリビジョンで配布された機能がすべて含まれています。たとえば、パッチ 123456-02 には、パッチ 123456-01 のすべての機能と、パッチの README ファイルに記載されているリビジョン 02 で追加された新しいバグ修正や機能が含まれています。

パッチの種類

パッチには、標準パッチと非標準パッチの 2 つの一般的な種類があります。

標準パッチ

標準パッチは、必要に応じて自動バックアウトをサポートし、またこの節で説明されている種類のパッチが含まれます。

汎用パッチ

汎用パッチにはバグ修正や新機能が含まれます。汎用パッチにはパッチ ID に特別な ID がありませんが、たとえば次のように、パッチ `README.patch_id` ファイルの Keywords フィールドにある特別なキーワードで識別されます。

- `security` – セキュリティーパッチクラスタに追加されたパッチを識別します。
- `y2000` – Y2K パッチクラスタに追加されたパッチを識別します。
- `encryption` – 現在の輸出法令に基づいて SunSolve Web サイトからの配布を限定するパッチを識別します。
- `point_patch` – SunSolve サイトの特別なディレクトリを使用して、特定のカスタマに配布を限定するパッチを識別します。
- `kernel` - 当該パッチ、およびそのパッチが依存するすべてのパッチが常に推奨パッチクラスタに追加されるようにするパッチを識別します。

カーネル更新パッチ (KU パッチ)

KU パッチは、Solaris のカーネルとそのほかの Solaris の中核機能を更新します。このパッチは、新しい修正が導入されるたびにリリースされるのではなく、定期的なスケジュールに基づいてリリースされます。

制限パッチ (R パッチ)

制限パッチは、頭文字「R」によって示されます。R パッチを使用すると、そのほかのパッチによるパッケージの以降の変更を防止するため、R パッチが変更するすべてのパッケージがロックされます。

ポイントパッチ

ポイントパッチは一般的な使用を意図していません。この種類のパッチにアクセスできるのは、特定のポイントパッチ ID が提供されたカスタマのみです。

ポイントパッチには、特定のカスタマ用の修正や、場合によっては特定のシステム用の修正が含まれている場合があります。これらの修正はソースコードツリーのブランチ上に作成され、メインソースコードツリーには含まれません。通常、ポイントパッチは、修正が配布されたカスタマにのみ適合するものと Sun は考えています。ポイントパッチは Sun のサポート担当者と相談したあとにのみインストールし、可能な限り早く削除する必要があります。

非標準パッチ

非標準パッチは、スパースパッケージパッチの形式では配布されません。

一般的な非標準パッチ

多くの非標準パッチは、次の種類になります。

- ディスケットイメージとしてリリースされる必要がある、x86 ベースシステム用のドライバ更新パッチ
- OBP、コントローラ、ディスクファームウェアを含むファームウェア/ハードウェアパッチ
- システムファームウェアを更新するためのバイナリファイルを含む Flash PROM 更新パッチ
- オペレーティングシステムソフトウェアには含まれないそのほかのパッチ
- パッケージ形式では配布されない場合がある一部の製品パッチ
  パッチの README ファイルには、必要なインストール手順が記載されています。

一時パッチ (T パッチ)

一時パッチとは、テスト用に構築されテストの準備ができていますが、まだそのプロセスを完了していないパッチです。T パッチは、そのパッチがカスタマの問題を修正することを確認するために「Active Escalation」に加入しているカスタマに対して利用可能になる場合があります。

一時パッチは「T108528-14」のように、パッチ ID の先頭の「T」により識別できます。パッチの README ファイルの最初の行には、パッチ ID のあとに「(Preliminary Patch - Not Yet Released)」という文があります。

パッチが確認され、Sun 内部でのパッチテストが完了すれば、T パッチの記号表示はパッチ ID とパッチの README ファイルから削除され、パッチは SunSolve サイトでリリースされます。

パッチの相互関係

パッチで提供される機能は、バグ修正と新機能のどちらであれ、そのほかのパッチで提供される機能と相互関係を持つ場合があります。このような相互関係は、パッケージの pkginfo ファイルにある次の 3 つのフィールドにより決定されます。

- パッチの依存関係 (SUNW_REQUIRES)
- パッチの累積と旧式化 (SUNW_OBSOLETES)
- パッチの非互換性 (SUNW_INCOMPAT)

パッチの依存関係 (SUNW_REQUIRES)

あるパッチで実現される機能が、少なくともほかの 1 つのパッチで実現される機能に対してコードの依存関係を持つ場合があります。つまり、パッチが正しく機能するために、他のパッチが必要となります。

そのほかの点でパッチに関連性がない場合、依存関係は、別のパッチにより必要とされるあるパッチとして記述することができます。あるパッチが 1 つまたは複数のパッチに依存している場合、パッチのスパースパッケージの pkginfo ファイルにある SUNW_REQUIRES フィールドで、どのパッチを必要とするかを指定します。

依存関係の必要条件は、一方向でのみ機能します。パッチ A がパッチ B を必要とする場合、パッチ B がパッチ A を必要とすることはありません。

パッチは累積的なものであるため、パッチ A がパッチ B のリビジョン xx を必要とする場合、リビジョン xx 以降またはそれと等しいパッチ B のすべてのリビジョンも要件を満たします。つまり、指定されるすべての必要なパッチリビジョンと関連付けられる、暗黙的な新リビジョンが存在します。

SUNW_REQUIRES フィールドは、パッチ間のハードコーディングされた直接の依存関係を指定するのに使用されます。そのほかの種類の依存関係がある場合、そのような依存関係はパッチの README ファイルに指定され、次の要素を含む可能性があります。

- **条件付き依存関係:** たとえばターゲットシステムに CDE 1.3 がインストールされている場合のみなど、ハードコーディングされたパッチの依存関係が特定の条件下でのみ発生する場合
- **弱い依存関係:** ある特定のバグを完全に修正するには別のパッチが必要であるが、その別のパッチがなくてもそのほかの点ではパッチは正しく動作する場合

パッチの累積と統合 (SUNW_OBSOLETES)

時として、バグ修正や新機能により、2 つ以上の既存のパッチが緊密に絡み合うようになります。そのため、パッチの依存関係を指定するのではなく、複数のパッチの機能を 1 つのパッチに統合した方がよい場合があります。この場合、統合されたパッチは旧式になります。

統合された方のパッチは、パッチのスパースパッケージの pkginfo ファイルにある SUNW_OBSOLETES フィールドに、不要になった 1 つまたは複数のパッチとして記述されます。このような宣言は明示的旧式化と呼ばれます。

パッチの累積は、一方向でのみ機能します。つまり、パッチ A がパッチ B をまとめる場合、パッチ A にはパッチ B のすべての機能が含まれています。この時点でパッチ B は旧式になります。パッチ B の新しいリビジョンは生成されません。

パッチの新しいバージョンにより、同じパッチの古いリビジョンは自動的に旧式化されます。自動的に旧式化されたパッチは、SUNW_OBSOLETES フィールドではフラグが設定されていません。つまり、パッチ A のリビジョン xx は、スパースパッケージの pkginfo ファイルにある SUNW_OBSOLETES エントリで、パッチ A のリビジョン x-1 を明示的に旧式化しておりません。

パッチの非互換性 (SUNW_INCOMPAT)

ごくまれに、2 つのパッチに互換性がない場合があります。たとえば、パッチの一方がポイントパッチである場合に非互換性が生じる場合があります。非互換性は、一方または両方のパッチのスパースパッケージの pkginfo ファイルにある SUNW_INCOMPAT で指定されています。

パッチの非互換性は双方向です。パッチ A またはパッチ B が他方のパッチとの非互換性を指定している場合、ターゲットシステムには一方のパッチしかインストールできません。たとえば、ターゲットシステムにパッチ A がすでにインストールされ、パッチ B がパッチ A と互換性がない場合、パッチインストールユーティリティー patchadd はパッチ B のインストールを許可しません。パッチ B をインストールする必要がある場合は、まずパッチ A を削除する必要があります。

パッチ配布コレクション

多くの場合パッチは、次の節で説明されているように、セットの一部です。パッチは、SunSolve Patch Support Portal http://www.sun.com/sunsolve/patches にあります。

推奨パッチクラスタ

SunSolve サイトの推奨パッチクラスタセクションには、さまざまな OS/アーキテクチャーの組み合わせ用のパッチのセットがあります。Sun は、ニーズに適した推奨パッチクラスタを使用することをお勧めします。

推奨パッチクラスタの各パッチは、次の条件の 1 つ以上を満たしています。

- **Sun Alert の問題への対処:** パッチは可用性、セキュリティー、またはデータ損失の問題に対処しています。
- **パッチユーティリティーの正しい動作に必要である:** パッチおよびパッケージユーティリティー自体に対するパッチ、またはパッチにより使用されるユーティリティー、および `ksh`、`sh`、`csh`、`nawk`、`fgrep`、`installf`、`removef` などのパッケージユーティリティーに対するパッチが含まれています。
- **以前のパッチのいずれかにより必要とされる:** そのパッチは推奨パッチクラスタのほかのパッチの `pkginfo` ファイルにある `SUNW_REQUIRES` フィールドに指定されています。

推奨パッチクラスタは頻繁に更新されるため、SunSolve サイトを定期的にチェックして更新がないかを調べてください。

Sun Alert パッチクラスタ

特定のオペレーティングシステム用の推奨パッチクラスタは、すべてのパッチ関連の Sun Alert Notification に対処するために必要なすべてのパッチの最新リビジョンを統合しています。ただし、特定のオペレーティングシステム用の Sun Alert パッチクラスタには、Sun Alert のすべての問題に対処するために必要なすべてのパッチの中の最低限のリビジョンしか含まれていません。

Sun Alert パッチクラスタの基準は、基本的には推奨パッチクラスタの基準と同じです。各パッチは、次の条件の 1 つ以上を満たしています。

- **Sun Alert の問題への対処:** パッチは可用性、セキュリティー、またはデータ損失の問題に対処しています。
- **パッチユーティリティーの正しい動作に必要である:** パッチおよびパッケージユーティリティー自体に対するパッチ、またはパッチにより使用されるユーティリティー、および `ksh`、`sh`、`csh`、`nawk`、`fgrep`、`installf`、`removef` などのパッケージユーティリティーに対するパッチが含まれています。

- **以前のパッチのいずれかにより必要とされる:** そのパッチは Sun Alert パッチクラスタのほかのパッチの `pkginfo` ファイルにある `SUNW_REQUIRES` フィールドに指定されています。

Sun Alert パッチクラスタは必要に応じて更新されるため、SunSolve サイトを定期的にチェックして更新がないかを調べてください。

Security T-Patches

SunSolve サイトの Security T-Patches セクションでは、セキュリティー問題に対処するパッチへのアーリーアクセスが提供されています。パッチはまだ T パッチの段階です。つまり検証とパッチテストのプロセスを完了していません。Security T-patches のインストールは、ユーザー自身の判断とリスクによります。

Security T-patches により対処される問題に関する情報と、可能な回避策は、Security T-Patches セクション http://www.sun.com/sunsolve/patches からアクセスできる Free Security Sun Alert データコレクションを通じて利用できます。

ソフトウェア更新

Solaris アップデートは、Solaris OS (執筆時点では Solaris 9) の最新リリース (ほかのリリースには適合しない) の完全に新しいリリースイメージです。Solaris アップデートには、Solaris アップデートが作成された時点で Solaris OS の最新リリースに使用可能な新しい機能パッケージと最新の統合パッチが含まれています。Solaris システムのインストールまたはアップグレードは、Solaris OS の初回インストールに似ています。

Solaris アップデートでパッチは、Solaris OS イメージに新しく組み込まれています。つまり、パッチはイメージに事前に適用され、元に戻すことはできません。

注: Solaris アップデートには、パッチ組み込みプロセスにおける制限を解決するために使用されるいくつかの特別なスクリプトパッチが含まれています。このようなスクリプトパッチは Solaris アップデート以外では意味がないため、SunSolve サイトから独立したパッチとしてダウンロードすることはできません。

注: SunSolve サイトの推奨パッチクラスタセクションおよび Sun Alert パッチクラスタセクションを確認して、Solaris アップデートの内容が確定されてからリリースされたパッチがないかを調べてください。内容が確定した日付とリリースの日付との間には、テストと運用ができるよう、時間差があります。

パッチおよびソフトウェア更新の考慮事項

もっとも適切なソフトウェアがインストールされるよう、パッチとソフトウェア更新を管理する必要があります。効果的な管理テクニックに従うことにより、次のようなシステム上の利点が得られます。

- 可用性の向上
- 性能の向上
- セキュリティーの向上
- 安定性の向上

ソフトウェアを更新するかどうかを決定する際には、コスト、リスク、可用性、およびタイミングを考慮する必要があります。更新の継続を決定する前に、問題のシステムとソフトウェアに関してこれらの要因のバランスをとる必要があります。

これらの要因に関するしきい値を確立するには、ユーザーと環境の要件を慎重に考慮し、計画する必要があります。各要因はシステムやネットワークごとに異なる場合があります。

- **コスト:** 業務が負担できるもの
- **リスク:** サービス拒否などにさらされること、およびその結果
- **可用性:** ダウンタイムのスケジューリング、ダウンタイムの長さ、および計画外のダウンタイムの結果
- **タイミング:** 実行するリリースの決定、およびパッチを適用する時期の決定

この節では、情報に基づいて決定を下せるよう、上記の要因に関して可能な限り多くの情報を提供します。

コスト

ソフトウェアの更新には、人手に関するコスト、業務に対するコスト、および計画外のダウンタイムに関するコストなど、数種類のコストが関連します。Sun のパッチの大部分にはバックアウト機能があり、Sun 製品ではパッチを取り消す可能性が比較的低いため、取り消されるパッチに関するバックアウトと再作業に関連するコストは比較的低くなっています。

コスト問題のもう一方の面は、パッチを適用しないことに関連するコストです。通常これらのコストには、システムを回復するための調査と修正の作業、および業務に関する計画外のダウンタイムが含まれます。

ソフトウェアを更新するコストは、ソフトウェアを更新しないコストと比較でき、また「継続か中止か」の決定が可能な場合にはコストしきい値が存在するように思われる場合があります。しかしながら、コストは 1 つの要因にすぎません。リスクも考慮する必要があります。

計画外のダウンタイムのリスクが高くても、コストがそれほど高くない場合は、ソフトウェアは更新すべきです。低リスク、高コスト、またはその両方が成り立つ場合は、ソフトウェア

は更新すべきではありません。固有のしきい値は、各ケースにおいて評価する必要があります。

リスク

パッチの適用にはリスクがあり、またパッチを適用しないことへのリスクもあります。パッチを適用するリスクとしては、変更の結果として予期せぬ結果が生じる可能性があります。パッチを適用しないリスクとしては、パッチの修正対象であるアプリケーションを使用できなくなる可能性があります。ソフトウェアを更新する決定は、検討中のソフトウェアインストールに固有の十分なデータと要件に基づいて行う必要があります。

セキュリティーの問題に対処しないと、セキュリティーの問題が環境に最大のリスクをもたらす可能性があります「汎用」パッチとは異なり、セキュリティーの脆弱性は Sun Alert Notification を通じてアナウンスされます。このような脆弱性を防止するためのパッチは、より重要に扱い、可能な限り迅速に適用する必要があります。

さまざまな企業が、セキュリティー固有のパッチを適用するためのさまざまな方針を採用しています。企業は、新しいパッチではあるが、潜在的な問題がある可能性があるパッチを性急に適用することにより発生しうる問題を回避する必要性と、パッチが安定する (エージング) のを待っている間にセキュリティーの欠陥にさらされるリスクとの間でバランスを取ろうとしています。セキュリティーの脆弱性のアナウンスメントと、ハッカーによる脆弱性の悪用との間の平均タイムラグは短くなってきているため[i]、高度に制御された環境であっても、配備の迅速さに対する圧力が強まってきています。

『Timing the Application of Security Patches for Optimal Uptime』[ii] において、著者は、一般に利用可能なパッチ情報に基づいて、システムにパッチを適用する理想的な時間を見つけるための数学モデルを構築しています。著者の結論では、パッチのリリースから 10 日後と 30 日後が、パッチ適用の 2 つの最適の時期です。この研究は Sun のパッチに固有のものではない点に注意してください。

可用性

IT 業界には、ソフトウェアを更新することで計画外のダウンタイムを防止できるという認識があります。Sun は、この結論に対して意見を述べるための、統計的に有意なデータを持っていません。ただし、パッチの適用頻度とともに、(計画済みおよび計画外を合わせた) 全般的なダウンタイムが高くなることを示すデータはあります。事前にパッチを適用して、潜在的なバグによる機能停止を削減が目標である場合、Sun の分析では、ソフトウェアの更新では多くの場合再起動が必要になるため、実際にダウンタイムが長くなることが示されています。

変更を最小限にするという方針に従えば、理想的なシステムとは、ソフトウェアを更新する必要が全くなく、永続的に可用性を維持するシステムになります。この「理想」は、次の図では直線で表されています。各タイムサイクルには、対応する可用性のサイクルが存在します。

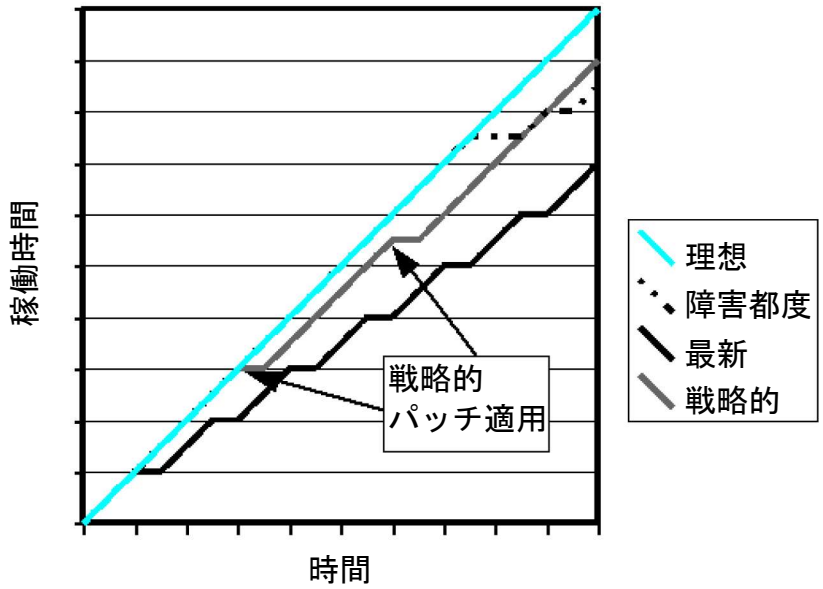

図 1.1 この図は、パッチの適用と、それによる可用性の影響を表しています。

既知の問題によりシステムの機能停止が発生した場合、短い点線で示されているように、機能停止の時点で稼動時間は停止します。通常、システムの稼働を回復することが第一の優先順位であり、修正措置を適用することはあとになります。そのため、問題を解決するために、2 つ目の計画済みの機能停止が必要になります。システム回復にある程度の時間が必要であるため、計画外の機能停止は、計画済みの機能停止よりも通常は長くなります。

バグを修正するパッチを事前に適用することで計画外の機能停止を完全に回避し、計画済みの機能停止を 1 回だけにすることは有用です。ただし問題は、どのバグが発生する可能性が高いかを事前に知ることです。

Sun がパッチを提供する対象のバグの多くは、特定のシステムで実際にエラーを発生させる可能性は極めて低いものです。一部のバグは、アプリケーションスタック、システムの構成、システムが動作する環境 (コードを介したデータパスを含む) により、発生することはありません。発生し得るすべてのバグに対してシステムの予防措置をとろうとすると、パッチが公開されるたびにすべてのパッチで最新の状態にしなければならなくなります。そのため、仮定に基づく「パッチ適用による最新」のアプローチ (図の長いギザギザの線) は、計画外の機能停止を回避するために、数多くの計画済みの機能停止を引き起こすことになってしまいます。これにより、システムは、単にバグに対処するだけで失われる可用性よりも多くの可用性を失う結果になります。

セキュリティー問題が出現した時点でセキュリティー問題に対処し、定期的にニーズを評価する新しいアプローチ (「戦略的パッチ適用」すると呼ばれる) を採用することで、パッチ 適用による最新」のアプローチ (場合によっては「問題発生時に対処」するアプローチ) よりもダウンタイムを短くすることが可能になる場合があります。

重大な機能停止を引き起こす特定のバグのリスクにさらされていると判断できる場合は、事前にパッチを適用する必要があります。このシナリオでは、機能停止が発生する前に、バグを対象とする事前解決が実施され、失われる可能性のある可用性の一部を回復します。

どの問題でも、数多くの決定を行わなければなりません。たとえば、特定のバグには相当なリスクがあり、そのバグにより引き起こされる機能停止はコスト上回避を試みるのに十分である場合などです。ある種の機能停止は、可用性の損失によるコストを上回るコストを含む場合があります。そのため、このグラフは判断要因の 1 つの軸にすぎず、さまざまな要因を考慮しなければなりません。

タイミング

タイミングが特に重要になるのは、どのソフトウェアリリースを実行すべきであるかを決定する時点、およびシステムにパッチを適用する時点です。Solaris OS の新しいリリースは、継続的により高い品質を提供しています。業務のニーズが満たされている場合、初期適用環境には最新のソフトウェアをインストールする必要があります。

取り消されるパッチへの対処は、考慮すべき別の要因となります。すでに説明したように、『Timing the Application of Security Patches for Optimal Uptime』では、パッチを適用する最善の時期はパッチのリリースから 10 日後と 30 日後であることが述べられています。取り消される Solaris のパッチはごく少数であるため (現時点では Solaris 8 では 2 パーセント、Solaris 9 では 3 パーセント)、公開時にこれらのパッチを適用するリスクは極めて低くなっています。

ワークフロープロセス

この節では、ソフトウェアを更新するための推奨方針を実施する方法について説明します。次の図に、ソフトウェア更新サイクルの高レベルでの概要を示します。

このサイクルにはエンドポイントが定義されていないことに注意してください。マシンが環境に導入された時点から、マシンがその役割を終える時点まで、ポリシーに応じて、確実にプロセスに従います。Sun は、環境を変更する前にインベントリを完成することを推奨しているため、少なくとも最初のサイクルでは、ある意味で「検出」がサイクルの開始になります。各サイクルのステップは、次の節で説明されています。

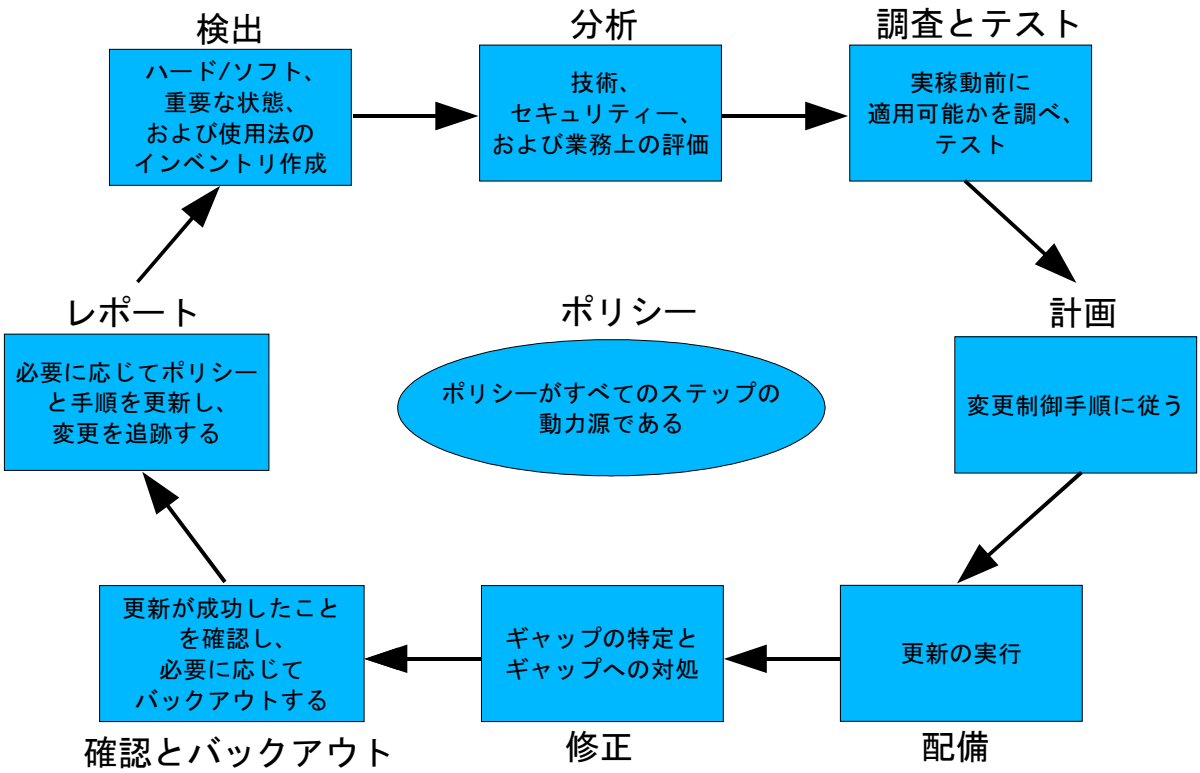

図 1.2 この図は、ソフトウェア更新サイクルの高レベルな概要を示しています。

1) 検出

新しいパッチ管理およびソフトウェア更新プロセスの確立における最初のステップは、環境の完全なインベントリを完成することです。少なくともこのインベントリには、システムのハードウェア (ファームウェアを含む)、オペレーティングシステム (すべてのバージョン、すべての更新、および適用されたすべてのパッチ)、アプリケーションソフトウェア (すべてのバージョンと適用されたすべてのパッチ)、および記憶装置デバイスの記述が含まれる必要があります。

このインベントリは、システム、ネットワーク機器、ルーターなどのネットワークインフラストラクチャーを反映する必要があります。システムの重要な段階 (テスト、開発、運用など) および配備の種類 (ファイアウォールや Web サーバーなど) も追跡する必要があります。

特定のアプリケーションの位置を含め、このインベントリを最新の状態に維持する必要があります。

2) 分析

このステップでは、以下の質問に対する回答を用いてリスクを評価します。

- 戦略的にパッチ適用を行う場合、費用対効果が適切かどうか
- 環境に対する影響を判別するための一連のテスト環境は用意できているか

このステップには次の事項の実行が含まれます。

- **技術的評価:** 更新されたソフトウェアが、企業で使用するアプリケーションのサービスと機能に関する問題を修正しているかどうかを評価します。
- **業務への影響の評価:** ソフトウェアを更新するか、更新しないかにより、業務プロセスへの影響があるかどうかの判断をします。またこの評価は、ソフトウェアを更新するための適切な時点、たとえば至急、週末、四半期の終わりなども決定します。
- **セキュリティーの評価:** 技術評価中にセキュリティーの問題も解決されているかどうかを判断します。パッチ適用に性能上のメリットがない場合であっても、セキュリティー上のメリットが存在する場合があります。

また、独自の内部コンピュータネットワークを維持し、ベンダーが供給するアプリケーションを活用している企業は、特定のオペレーティングシステムのパッチまたは更新が自社のソフトウェアに干渉しないことをアプリケーションベンダーが保証するまで、オペレーティングシステムへのパッチ適用やソフトウェアの更新を躊躇する場合があります。そのため、新しいパッチが可能な限り早く評価されるように、企業はベンダーと緊密に連携する必要があります。Sun は、ベンダーによる新しいソフトウェアリリースの認証が早く行われるよう、多数のベンダープログラムを実行します。

3) 調査とテスト

各パッチを適用する前に、パッチが予定通り機能し、環境と互換性があることを確認するために、パッチをテストします。実稼動環境でパッチを適用する前に、システムレベルだけでなく完全な品質保証環境でも各パッチをテストします。統合テストは、パッチのシステムとの互換性と、環境内のそのほかのコンポーネントとの互換性を確保するのに役立ちます。

評価とテストにより、パッチの適用やソフトウェアの更新が、以前修正された脆弱性を復活させないことや、新しい脆弱性を生み出さないことを確認する必要があります。Sun は、このような種類の問題の再発を回避するために、Solaris のパッチを累積することを選択しています。実稼動環境におけるパッチの適用は、パッチの適用による混乱のリスクを最小限にするため、通常の変更管理手順に従います。

また、ソフトウェアの更新後、実稼動環境でもテストを実行します。少なくとも、アプリケーションソフトウェアを含んだ統合テストを実施する必要があります。

4) 計画

通常の変更管理手順とともに計画を行います。特定のステップ、必要な時間、関係者への適切な通知、および何らかの要素が意図通りに進行しなかった場合の緊急対策ステップを計画します。

このステップはテストと開発システムにはあまり重要でない場合がありますが、運用システムには間違いなく関連しています。変更制御が実行される度合いは、経験と既存の企業のポリシーによって定まります。

詳細な計画を用意することで、パッチ適用の労力全体を効率化し、緊急対策計画が万が一必要になった場合も、可能な緊急対策計画を準備することができます。

5) 適用

テストを十分に完了したあと、残りのシステムに変更を適用します。テストが代理システムで行われた場合、ほかの場所で変更を適用する際のトラブルの可能性は低くなりますが、残念なことに、運用システムは多くの場合、規模、セキュリティー構成、トラフィックボリュームなど、テスト時にすぐには複製できない固有の特性を持っています。Sun は、適用のステップのあとでは、テストと実稼動環境が異なる領域での動作を最も詳しく監視することをお勧めします。

ほかのシステムで正しく動作しない場合、そのギャップを調査し、対処する必要があります。

6) 修正

パッチは、手作業、またはプロセスを自動化するツールを使用して適用できます。自動化は、大規模配備におけるコストの削減、特定のメンテナンスに対する配備のスケジューリング、および人的ミスの可能性の削減において特に便利です。

パッチの配備に対する 1 つの問題としては、配備の時点でリモートユーザーが接続していない場合が挙げられます。これにより、リモートユーザーのシステムにパッチが未適用のままだと、リモートユーザーのシステムによってネットワークが脆弱になります。例としては、ほかのソースからの脆弱性にさらされたラップトップを、リモートユーザーがネットワークに接続した場合: Federal General Accounting Office のネットワークが Microsoft Remote Procedure Call (RPC) の脆弱性の影響を受けたケースが挙げられます。[iii]

7) 確認とバックアウト

以前に行った分析とテストプロセスにより環境に対するリスクは最小限になっていますが、予見できない競合、逆行、またはエラーが発生した場合に、以前の状態に戻す準備をすることも必要です。Linux や Microsoft のパッチなどでは使用できないバックアウト機能を装備しているため、Solaris のパッチには利点があります。

この操作はプロセスにおける実際の「ステップ」ではない場合がありますが、セーフティーネットを用意しないと、システムの機能停止に対する企業の脆弱性が大幅に高まり、パッチ管理コストが高くなる可能性があります。

8) レポート

Sun とそのカスタマにより、ソフトウェア更新サイクルに関連する幅広いレポートが作成されています。多くのケースでは、レポートは問題の検出に関連したデータを提供するのに役立っています。ただし、サイクルのすべてのステップに関連するデータが必要な場合もあります。このため「レポート」はプロセスでは独立したステップになっています。レポート には次の要素が含まれます。

- **パッチ管理プログラムを文書化するポリシーと手順:**これらは、情報セキュリティーポリシーやシステム開発および実装ポリシーなどです。多くの場合は既存のポリシーと手順に組み込まれています。
- **機能レベルでのパッチ管理に対する責任の明確な定義と割り当て:**これには、システム管理と保守を担当するすべての個人に関する連絡先情報が含まれます。
- **実装されたパッチと却下されたパッチ両方の追跡:**これには、過去、現在、未来において、どのような違いがあるのかが含まれます。
- **企業全体でのパッチ適用の進行状況、コンプライアンス、またはファイル破損:**上記の要因すべてが含まれる可能性があります。

9) ポリシー

上記の 8 つの各ステップの中心にあるのがポリシーで、ソフトウェア更新サイクルのすべての段階の動因となります。一般的なポリシーには、ダウンタイムのスケジュールやシステムに対するスケジュール済みメンテナンスに関する規則、セキュリティー関連のパッチの (異なる可能性のある) 取扱い、および異なるシステム上の特定のバージョンのソフトウェアを決定する責任の委任が含まれます。

企業がその独自の環境に対して、コスト、リスク、可用性、およびタイミングの間の関係、およびそれらのしきい値を明示的に作成するのはポリシーにおいてです。これらの関係としきい値の動因となるのは、その企業の可用性、監査、および業務サポートの要件と基準です。ポリシーは企業のサービス管理プロセスに完全に統合され、業務上の要件における将来の変更に対応できるよう十分な柔軟性を備えている必要があります。

すべてのパッチ管理ポリシーの重要なコンポーネントは、パッチプロセスを開始する「トリガー」イベントの明示的なリストです。一般的なトリガーには、CERT 勧告の頻繁な監視、ベンダーからの通知 (Sun Alert プログラムなど)、企業の業務サイクルに一致する定期的な (四半期ごとまたは半年ごと) スケジュールに基づくレビューが含まれます。

ツールに関する推奨事項

この節では、Sun の多数のパッチ関連ツール、それらのツールに最も適したアプリケーション、およびそれらの使用方法について説明します。一部のツールはサービス契約が必要であり、そのことが明記されています。Sun は以下のツールを使用することをお勧めします。

- Sun Patch Manager 2.0 または PatchPro プラグインが付属する Solaris Patch Manager 1.0
- Sun Explorer ソフトウェア - インストール環境の把握用
- 複数のマシンにパッチを適用するため 『Solaris Patch Manager Base Version 1.0 Strategy White Paper』で説明されているワークフロー。
  URL は http://www.sun.com/bigadmin/content/patchpro/ です。

オンサイトサポートを受ける資格があるカスタマは、次のソフトウェアを使用できます。

- 分析モジュールとして Sun Checkup が付属する Traffic Light Patchtool (TLP)
- Sun Explorer ソフトウェアが付属する TLP

次の 2 つの節「パッチ管理ツール」と「パッチ適用支援」には、ソフトウェアを更新するために Sun がサポートするツールとサービスが一覧表示されています。また、それぞれの短い説明、詳細情報を参照するための URL (またはその両方) が付属します。

パッチ管理ツール

- Sun Patch Manager 2.0
- Solaris Patch Manager 1.0
- PatchPro
- Traffic Light Patchtool
- パッチユーティリティー

Sun Patch Manager 2.0

Sun は、Solaris 10 リリースに Sun Patch Manager 2.0 を含めることを計画しています。バージョン 2.0 には、`smpatch` コマンド行インタフェースだけでなく、Sun Patch Manager ブラウザインタフェースも用意されています。ブラウザインタフェースを使用して基本的なパッチ管理作業を実行することもできますが、`smpatch` コマンドを使用して基本的なパッチ管理作業以外に多くの作業を実行することもできます。`smpatch` コマンドは、ローカルモードとリモートモードの 2 つのモードでも使用可能です。

Solaris 10 版の Sun Patch Manager 2.0 は、パッチ管理プロセスを自動化するため、PatchPro の機能を組み込んでいます。このプロセスには、システム上でのパッチ分析の実行と、結果として作成されるパッチのダウンロードおよび適用が含まれています。使用可能なパッチは、依存関係が自動的に選択された状態で個別に選択したり、ユーザーが指定したアクション (ダウンロード、またはダウンロードとシステムへのパッチの適用) 用の完全なセットとして選択できます。

Solaris 10 版の Sun Patch Manager 2.0 を使用すると、Sun のパッチサーバーから HTTPS を介した直接ダウンロードの代替策として、パッチのローカルコレクション、またはイントラネット上のローカルパッチサーバーを指定できます。

Sun Patch Manager 2.0 は Solaris 8 および Solaris 9 でもダウンロードして使用できます。URL は http://www.sun.com/software/download/products/40c8c2ad.html です。ただし、Solaris 10 版の Sun Patch Manager 2.0 の機能のすべてが、Patch Manager 製品の Solaris 8 および Solaris 9 バージョンに含まれているわけではありません。すべてのバージョンに固有の機能については、http://www.sun.com で Solaris の製品マニュアルを参照してください。

Sun Patch Manager 2.0 の詳細については、http://www.sun.com/service/support/sw_only/patchmanager.html にアクセスしてください。

Solaris Patch Manager 1.0

Solaris Patch Manager 1.0 は Solaris 9 リリースに含まれ、グラフィカルユーザーインタフェースと、`patchadd`(1M) および `patchrm`(1M) ユーティリティー用のコマンド行インタフェースの両方が用意されています。完全なソフトウェア分析と自動ダウンロード機能を

実現するために、PatchPro との統合が提供されています (別途ダウンロードする必要あり)。

Solaris Patch Manager 1.0 は Solaris Management Console の機能を利用して、マルチシステムリモートパス管理機能、スケジューリング、およびロギングを実現します。バージョン 1.0 の詳細については、
http://www.sun.com/service/support/sw_only/patchmanager.html を参照してください。

Patch Manager ツールに関する追加情報

Sun は、パッチ管理プロセス中の再起動とソフトウェアの再構成により発生する可能性のあるダウンタイムの削減に積極的に取り組んでいます。ただし一部のツールを安全にインストールするためには、シングルユーザーモードでのインストールや、ユーザーの操作が必要です。Patch Manager は、ユーザーによる対話型インストールを行うために、これらのパッチ、およびそれらに依存するパッチを特定するダイアログボックスを表示します。特別なインストールの指示については、これらのパッチの README ファイルを参照してください。

PatchPro

PatchPro は、Patch Manager 用に分析、ダウンロード、およびインストール機能を実行し、次の形態で提供されています。

- Solaris 10 での Sun Patch Manager 2.0 用の分析エンジンとして完全に統合
- Solaris 9 の Solaris Patch Manager 1.0 に対するダウンロード可能なアドオン分析モジュール
- Solaris 2.6、Solaris 7、および Solaris 8 用の Solaris Patch Manager Base Version 1.0 として独立して使用可能

PatchPro は、システム上に現在インストールされているソフトウェアとパッチの詳細な分析を実行し、その特定のシステムに適切なすべてのパッチを特定します。ソフトまたはハード依存を含むデジタル署名されたパッチがダウンロードされ、セキュリティーが検証され、正しい順序でインストールされます。ダウンロードの完全な制御と自動インストールの程度は、構成ファイルにより実現されます。スケジューリングは cron デーモンにより実現されます。

PatchPro によりダウンロードされたパッチの中で、ユーザーにより設定されたポリシーの結果として、または自動化に適していないパッチの種類により、自動的にインストールしてはならないパッチは、ユーザーがあとで操作するよう隔離されます。

デフォルトでは、PatchPro からのメッセージは `syslogd` により `/var/adm/messages` ファイルに記録されます。ただし、特定の PatchPro のログは必要に応じて構成可能で、電子メールを通じて管理者に通知するよう構成を設定できます。URL は http://patchpro.sun.com/ です。

PatchPro Interactive

Patch Manager 製品とともに使用される PatchPro テクノロジに加えて、PatchPro のバリエーションである PatchPro Interactive を http://www.sun.com/sunsolve/patches から入手できます。

PatchPro Interactive を使用すると、システム情報を対話形式で入力できます。PatchPro Interactive は、システム情報に基づくカスタムパッチリストを生成します。この実装を使用して、SunSolve サイトに直接アクセスできないシステム用のパッチリストを生成します。

Traffic Light Patchtool

Traffic Light Patchtool (TLP) はマルチシステムパッチ管理ツールで、多くの場合 Sun Checkup ツールの出力および Enterprise Installation Service (EIS) CD とともに実行されます。eRAS サービスは推奨事項のみを提供するのに対し、TLP はパッチの問題を修正するのに役立ちます。TLP には次の機能があります。

- パッチ適用を簡単にするいくつかの小さなスクリプトとファイル
- ファームウェアおよび Flash PROM パッチが付属する追加ディレクトリ
- README ファイルの概要
- システムの再起動や構成ファイルの変更を必要とするパッチなど、特別な処理を必要とするパッチのリスト

TLP は次の 2 つの方法で使用できます。

- **オフサイト:** Sun Explorer ファイルが Sun に転送され、TLP が実行され、FTP または CD-ROM を使用することで結果がカスタマに送信されます。
- **オンサイト:** TLP がカスタマシステムにインストールされ、そのシステム上で Sun Explorer ファイルが収集および分析されます。結果は同じシステム上で使用可能になります。カスタマは、このシステムからパッチクラスタを直接インストールできます。

オンサイト TLP を使用すると、カスタマは、(どのパッチが適用されているかに依存した) 各システムの実装状態の概要も把握できます。カスタマは、システムのセットに定義すべきパッチクラスタのセットを定義できます。またこれらのクラスタは、最後に成功したクラスタインストールにより追跡できます。状態は、GREEN、AMBER、または RED (Traffic Light) に設定 (および報告) することができます。

パッチクラスタインストールは `/var/sun/EIS-CD.log` ファイルに記録されます。このファイルが監査ログになります。

TLP は有料、またはある種の Sun Services 契約の一部として利用できます。TLP、EIS、およびそのほかの関連する Sun Preventive Services については、http://www.sun.com/service/preventive/index.html にアクセスしてください。

パッチユーティリティー

パッチユーティリティーの詳細については、次のマニュアルページを参照してください。

- `patchadd`(1M)
- `patchinfo`(1M)
- `patchrm`(1M)
- `pkgchk`(1M)
- `smpatch`(1M)
- `showrev`(1M)

パッチ適用支援

Sun Explorer

Sun Explorer ソフトウェアは、あるシステムに関する情報の収集に使用される大規模なスクリプトのセットで、ほかのプログラムによる分析または Sun への送信準備が完了した tar ファイルの形式で結果を保存します。Sun Explorer は (ユーザーの同意を得て) 出力をオンラインデータベース `ConfigDB` に電子メールで送信するように設定できます。続いてユーザーはシステムを選択し、データベースから大量のレポートを生成することができます。これらのレポートは Sun Alert の問題、パニック、クラスタエラー、ディスクエラー、電源の問題、OS メッセージ、および実行時情報をカバーしています。このデータから、システム管理者は事前にシステムを望ましいパッチレベルに維持したり、生成されたシステムメッセージを検出することができます。エンジニアはこの情報を使用して、カスタマが経験している可能性がある問題に対処することもできます。
Sun Explorer ソフトウェアの詳細については、
http://sunsolve.sun.com/pub-cgi/show.pl?target=explorer/explorer&nav=patchpage にアクセスしてください。

Sun Checkup

Sun Checkup は eRAS Services システム構成分析ツールで、Sun のサポートエンジニアがダウンロードして携帯して使用できます。このツールを使用すると、エンジニアは、特定のカスタマの環境に対する eRAS Services 製品の「軽量」バージョンの情報を提供することができます。このツールにはルールに基づいたチェックリストが含まれています。

そのほかのツールおよびサービス

パッチ管理またはソフトウェア更新の際にさらなる支援になるものとして、以下を参照してください。

- 特別注文の SunPS℠ プログラム (プロフェッショナルサービス向け)
  http://www.sun.com/service/consulting/index.html
- N1™ Grid Service Provisioning System
  http://wwws.sun.com/software/products/service_provisioning/index.html
- Solaris Live Upgrade ソフトウェア
  http://wwws.sun.com/software/solaris/liveupgrade/
- JumpStart™ ソフトウェア
  http://www.sun.com/bigadmin/content/jet/
- Solaris Flash ソフトウェア
  http://wwws.sun.com/software/solaris/webstartflash/
- Sun Control Station ソフトウェア
  http://wwws.sun.com/software/controlstation/
- Configuration and Service Tracker
  http://www.sun.com/service/support/cst/index.html
- Sun Alert Notification
  http://sunsolve.sun.com/pub-cgi/show.pl?target=sunalert_patches
- Patch Club Report
  http://sunsolve.sun.com/pub-cgi/show.pl?target=patchpage
  または https://subscriptions.sun.com/subscription_center/ecomm.jsp
- パッチとアップデート
  http://sunsolve.sun.com/pub-cgi/show.pl?target=patchpage
- 最新の Solaris アップデート
  http://www.sun.com/software/download/products/40c8c2ad.html

ユースケース

この節では、いくつかのシナリオと、この文書で説明した方針と推奨手法を使用してどのようにこれらのシナリオに取り組むかを説明します。

ケース 1: 変更の最小化

最新の Solaris アップデートを使用してシステムが構築されています。このアップデートは、近隣システムと一貫性を保っています。少しして、2 つのパッチが適用されました。パッチ 111111-01 はセキュリティーの問題に対処し、パッチ 222222-01 は搭載された新しいカードをサポートしています。初期パッチベースラインが適用されてから 6 か月後、最新の推奨パッチクラスタから適用すべき新しいパッチがあるかどうかを確認するため、システムを評価しました。パッチ 111111-03 および 222222-05 が新しいパッチです。これらを適用すべきでしょうか。

このケースでは、いずれのパッチも適用しません。セキュリティーパッチに関しては、6 か月前の -01 リビジョンでセキュリティー問題が解決されていれば、セキュリティーの修正を含んでいない -03 を適用する必要はありません。2 つ目のパッチに関しては、新しいカードはすでに -01 パッチでサポートされています。新しいリビジョンが現在発生している何らかの問題に対処したり、必要な機能拡張を提供するのでない限り、それらは適用しないでください。

ケース 2: 古いパッチの置換

パッチ 111111-01 および 222222-01 が、新しいパッチ 333333-01 に統合されていて、旧式になっています。この旧式化は、これらオリジナルのパッチが今後新しいパッチおよびクラスタリリースに出現しないことを意味します。この場合、新しい修正は統合した新しいパッチに含まれていくので、オリジナルの 2 つのパッチを新しいパッチに置き換えるべきでしょうか。

いいえ、システムを変更してもメリットはありません。2 つのパッチが存在することで、将来の変更に悪影響を及ぼすことはありません。パッチを置き換えないことにより、システムに影響を与えることなく変更を最小限にするという規則が守られます。

ケース 3: 一貫性

Solaris 9 4/04 リリースを使用して複数のシステムが構築されており、その後、複数のパッチを使用して更新しています。1 年後、新しい装置がデータセンターに追加され、オリジナルのシステムとの一貫性を確保する必要があります。4/04 リリースを使用して新しいシステムを構築すべきでしょうか。 それともすべてのシステムを 4/05 リリースを使用して構築すべきでしょうか。

4/04 ベースラインに対して新しいシステムを構築すると、既存のシステムは変更する必要がないため、変更を最小化するという方針を満たしています。環境内でベースラインを確立することにはメリットがあります。ただし、業務環境が変わり、既存のシステムが新しい要件を満たすために機能拡張の一部を必要とする場合は、既存のシステムと新しいシステムを含め、すべてのシステムを 4/05 ベースラインに更新することを検討しても構いません。そのような変更が保証されている場合、より新しいソフトウェアを使用することで、最高の品質の確保に役立ち、また業務のニーズに対して最新のソフトウェアを使用するという方針も満たされます。

ケース 4: システムを起動するタイミング

セキュリティーパッチの多くは、適用後再起動する必要があります。これらのパッチはさまざまな時期にリリースされるため、各パッチが直ちに有効になるためにはシステムを毎回起動する必要があります。起動することなくパッチをインストールし、(起動の頻度を下げることにより全般的なダウンタイムを減少させる) すべてのパッチが同時に適用されるように 1 回だけ起動するのを待つ方が優れているのでしょうか。

適用できるかどうか、および問題が発生する可能性があるかどうかを判断するには、サイトの環境と各パッチを分析する必要があります。可能であれば、パッチを適用してからシステムを起動するのを待ち、次の計画済みダウンタイムまで回避策を使用するのが好ましい場合があります。

i http://www.cert.org/stats/cert_stats.html を参照
ii Beattie, Arnold, Cowan, Wagle, Wright, and Shostack, Timing the Application of Security Patches for Optimal Uptime, 2002 LISA XVI, Philadelphia, PA
iii Dacey, Robert F., Director, Information Security Issues, Effective Patch Management is Critical to Mitigating Software Vulnerabilities, Testimony Before the Subcommittee on Technology Information Policy, Intergovernmental Relations, and the Census, House Committee on Government Reform, General Accounting Office, September 10, 2003