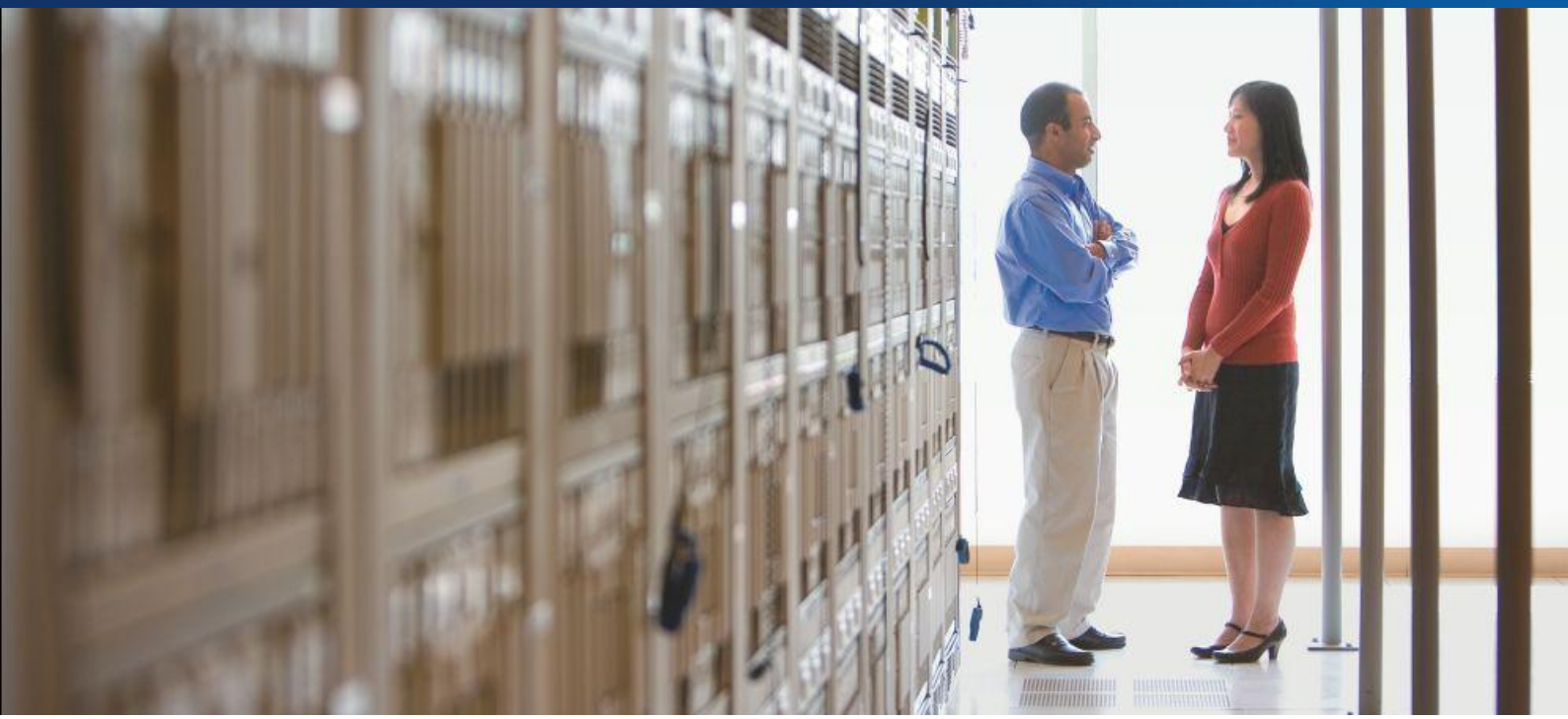
Microsoft

Trustworthy Computing



マイクロソフト セキュリティ更新プログラム ガイド

IT プロフェッショナルの皆様が、マイクロソフトのセキュリティ更新プログラムのリリース情報、プロセス、コミュニケーションおよびツールをより深く理解し、最大限に活用するのをお手伝いします。

2009 年 7 月

目次

セキュリティ更新プログラム管理に関するビジネス ケース

George Stathakopoulos (Trustworthy Computing Security General Manager) からのメッセージ

コンピューティングの脅威のランドスケープは変異を続けており、IT のインフラストラクチャも依然として危険にさらされています。業界のセキュリティ技術および防御策はますます洗練されてきているにも関わらず、懸念は続き、テクノロジー、それに付随する。

その結果、マイクロソフトおよび業界のその他の企業は、真摯な努力を重ねて、サイバー犯罪および不正な目的でテクノロジーを悪用しようとする攻撃者に対抗する必要があります。セキュリティの脅威を低減することは、より安全で、信頼性の高いインターネットのための Microsoft® End to End Trust (エンド ツー エンドの信頼性) 構想の重要な要素です。長期にわたり取り組んできた信頼できるコンピューティングの取り組み、および End to End Trust の進化は、皆様がオンラインで誰を、何を信用するかに関する制御およびより効果的な選択を行うのに役立ちます[1]。

セキュリティは、End to End Trust 構想における重要な要素です。マイクロソフトの強化されたセキュリティに対する戦略的なアプローチには以下のものが含まれています。

- **最善策の共有** – マイクロソフトのセキュリティ開発ライフサイクル (SDL)[2] はソフトウェア業界を率いるセキュリティの保証プロセスで、製品に基礎からセキュリティを構築します。マイクロソフトは、SDL および別のリソースを共有して、IT プロフェッショナルおよびサードパーティが可能な限り最も安全なソフトウェアを開発するために支援しています。
- **世界規模のセキュリティ レスポンスの実施** - マイクロソフトは積極的なレスポンス、ツールおよびプログラムの提供により、継続的にセキュリティを向上させ、出現中の脅威の防御および管理を支援しています。
- **ガイダンスおよび啓発活動の提供** - マイクロソフトは、Web サイト、ブログおよびその他のリソースを含むコンテンツおよびツールのホストにより、IT プロフェッショナルにセキュリティ レスポンス ガイダンスおよび啓発活動を提供しています。

業界内のその他の企業も製品やサービスをサポートするために、リソースや資料を提供しています。この大量の資料により、限られた時間で必要なものを正しく見つけることが困難です。お客様が効果的にすべての重要なセキュリティの更新プロセスに取り組むことを支援するため、マイクロソフトは本セキュリテ

---

[1] End to End Trust およびこの構想に関する詳細情報は、www.microsoft.com/japan/mscorp/twc/endtoendtrust/default.mspx をご覧ください。

[2] www.microsoft.com/sdl

ィ更新ガイドを作成しました。本ガイドの目的は、マイクロソフトのプログラム、サービス、情報および通信を最大限に利用し、組織の IT 環境をより安全にすることです。

本ガイドが皆様にとって、皆様の IT インフラストラクチャを守り、より安全で、安心できるコンピューティングおよびインターネット環境を構築するために役立つ詳細情報およびツールを含む、価値あるリソースであると判断されることを希望しています。

George Stathakopoulos

General Manager, Trustworthy Computing Security

Trustworthy Computing Group

マイクロソフト セキュリティ更新プログラム ガイドの使用方法

マイクロソフト セキュリティ更新プログラム ガイドへようこそ

本ガイドは、IT プロフェッショナルがマイクロソフトのセキュリティのリリース情報、プロセス、コミュニケーションおよびツールを深く理解し使用できるように設計されました。マイクロソフトの目標は、IT プロフェッショナルが組織的なリスクを管理し、反復可能で効果的なセキュリティ更新プログラムの展開メカニズムを開発することを支援することです。

本ガイドでは、便利な用語集、マイクロソフト セキュリティ情報のプロセスの概要、およびマイクロソフト セキュリティ更新プログラムの段階ごとの情報をご覧になれます。

本ガイドは、セキュリティ更新プログラムのプロセスについて、次の各ステージでまとめられています。

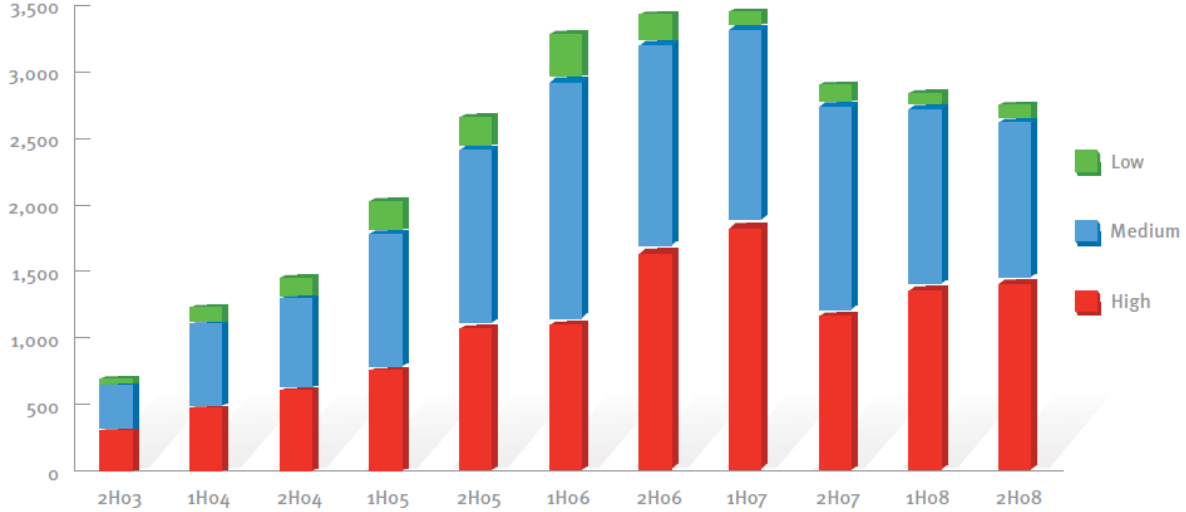
- **ステージ 1： マイクロソフトのセキュリティ リリースの通知を受けとる**
- **ステージ 2： リスクを評価する**
- **ステージ 3： 緩和策を評価する**
- **ステージ 4： 標準または緊急の更新プログラム展開のタイムライン**
- **ステージ 5： システムを監視する**
- **進行中のステージ: 監視する**

各セクションでは、ステージの完了後に想定される結果と同様に、ステージの目的と意図に関する概要を説明しています。

本ガイドが、皆様の IT インフラストラクチャの保護に役立ち、業務における価値のあるリソースになることを願っています。さらに、21 世紀に向けてより安全で、信頼性の高いコンピューティングの枠組みを構築することを模索する中で、本ガイドが幅広い協力においてさらなるステップとなるように望んでいます。

はじめに

脆弱性とは、攻撃者がそのソフトウェアの整合性、可用性および機密性を悪用可能な、ソフトウェアの弱点です。最悪の脆弱性の場合、攻撃者が、影響を受けるシステムで任意のコードを実行する可能性があります。脆弱性を開示することにより、脆弱性の存在が一般に広く明らかになります。開示は、多様なソースから行われ、ソフトウェア ベンダー、セキュリティ ソフトウェア ベンダー、独立系セキュリティ 研究者、さらには悪意のあるソフトウェア (マルウェア) の作成者からさえも行われます。セキュリティ イン



テリジェンス レポート (SIR) では、2003 年から 2008 年 12 月 31 日まで、ソフトウェア業界全体における数千ものさまざまな深刻度の脆弱性の開示について毎年報告しています (図 1 参照)。

図 1 業界全体における脆弱性の開示 (2H03–2H08[3]、半年毎)

すべての脆弱性は同等ではありません。Common Vulnerability Scoring System (CVSS) version 2.0 は 3 種類の複雑度を示しています: 低い程度、中程度および高程度

これらの表示は、攻撃者が該当の脆弱性をどの程度容易に悪用できるか、その程度を定義しています。図 2 が示しているのは、2003 年下半期から 2008 年下半期における半期ごとに開示された脆弱性の複雑性を示しています。複雑性の組み合わせは、2008 年上半期以降、相対的な時期でおおまかに見ると一定しており、高い複雑性の脆弱性の割合は (一般的に悪用が最も困難ですが) 若干上昇しているものの、非常に低い数字を維持しています。過去の期間のように、2008 年下半期に公開された大部分の脆弱性が低複雑性のもので、攻撃者がこれらの脆弱性について確実な悪用コードを容易に作成可能であることがわかります。

[3] nHYY は期間を示しています。nH はその年の上半期 (1) または下半期 (2) のどちらかを示し、YY は念を表しています。たとえば、1H06 は 2006 年上半期 (1 月 1 日から 6 月 30 日まで)、2H08 は 2008 年下半期 (7 月 1 日から 12 月 31 日まで) を指します。

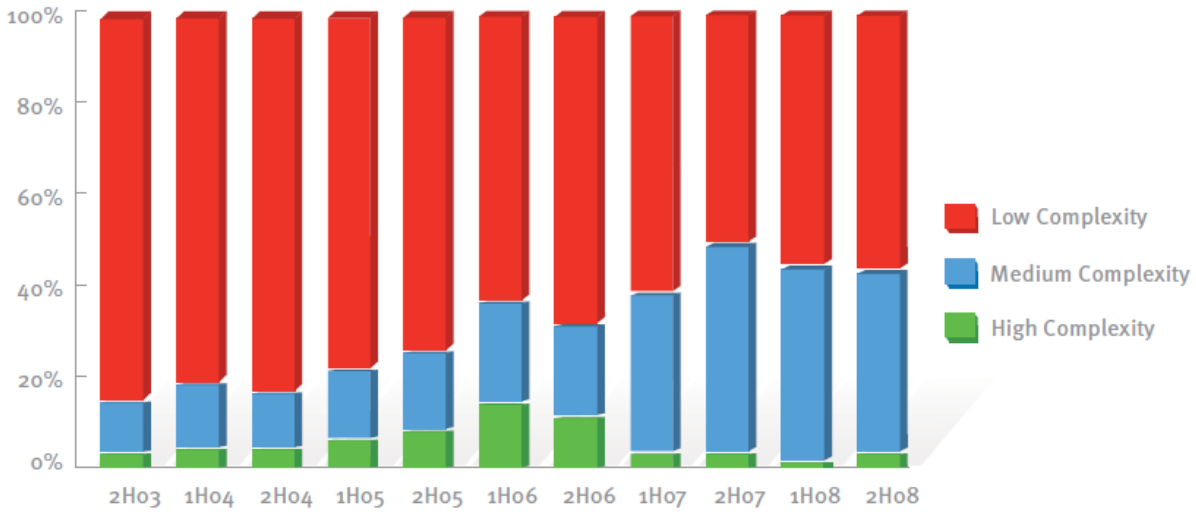
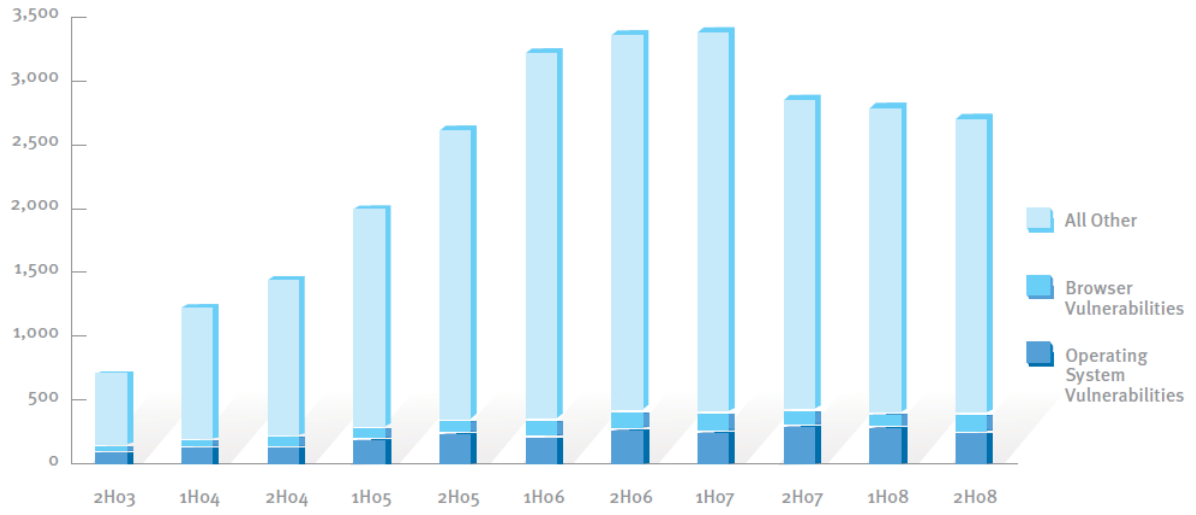


図 2: 業界内の脆弱性の開示 (アクセスの複雑性毎、2H03–2H08)

脆弱性は業界全体の問題です。業界では、毎年数千もの脆弱性が公開されます。そして、公開された大部分がオペレーティング システムや Web ブラウザーではなく、アプリケーションのものです。図 3 が示しているのは、2003 年下半期以来の、オペレーティング システム、ブラウザーおよびその他のコンポーネントの脆弱性です。一般的に、マイクロソフトの脆弱性公開の傾向は、規模はかなり小さいものの、業界



全体を反映しています。

図 3: 業界内のオペレーティング システム、ブラウザーおよびその他の脆弱性 (2H03–2H08)

セキュリティ更新プログラム管理が極めて重要です。悪用コードは、ソフトウェアの脆弱性を悪用します。SIR の調査では、更新プログラムをたまにしかインストールしない、または全くインストールしないユーザーがいるため、脆弱性用のセキュリティ更新プログラムが利用可能になってからも長期間、悪用が有効であり続けることが示されています。2003 年に修正された脆弱性の悪用コードが現在でも存在しています。これが示しているのは、攻撃者がある脆弱性を悪用する方法を理解した場合、対象のセキュリティ更

新プログラムが存在したとしても、攻撃者はその先の何年間も、さまざまな攻撃方法により、定期的にその悪用コードを利用して、「未修正」のシステムを攻撃しようとすることです。さらに、最新版の SIR で、マイクロソフトは特定の期間中の、成功した攻撃に使用された数百ものファイル サンプルを解析しました。新しいセキュリティ更新プログラムを早期に一定して適用することにより、すべてのサポートされているバージョンのソフトウェア アプリケーションに対するこれらのすべての攻撃を防ぐことができます。

これは、エンタープライズの IT 管理者およびセキュリティ専門家が、今日直面する状況です。組織のデスクトップ コンピューター、サーバー、仮想マシンおよびモバイル機器を、オペレーティング システムおよびアプリケーション用の最新のセキュリティ更新プログラムで維持するプロセスは、すべてのインターネット接続環境におけるリスク管理の方法論の中心を占めるようになりました。

本ガイドと脆弱性の管理の目的

本セクションの内容*:*

- 本ガイドの目的
- マイクロソフトが、自社製品の脆弱性を管理する方法

本セクションを終了すると、*IT* プロフェッショナルは次の項目について理解します*:*

- 組織の IT 環境におけるセキュリティの脆弱性管理に役立つようマイクロソフトがリリースしているすべてのコミュニケーション、ガイダンス、プログラムおよびサービスを IT プロフェショナルが最大限に活用できるよう支援するという、本ガイドの目的を理解します。

本ガイドの目的

オンラインの犯罪活動がビジネスに与える脅威を緩和する取り組みの中で、IT プロフェショナルはマイクロソフトのセキュリティ更新プログラムのリリース プロセスおよびマイクロソフトのすべてのサポートリソースを理解する必要があります。IT 環境のサポートおよび維持に加え、IT プロフェショナルはソフトウェア ベンダーのセキュリティのコミュニケーションおよびセキュリティ更新プログラムのリリースプロセスの実施方法を理解する必要があります。本ガイドは、IT プロフェショナルが 2 種類のマイクロソフトのセキュリティ リリース (1. セキュリティ更新プログラムおよび 2. セキュリティ アドバイザリ)、およびすべてのマイクロソフトのコミュニケーション、ガイダンス、プログラムおよびサービスの間で、計画および管理するために役立つものです。マイクロソフトのセキュリティ リリースに含まれている、すべてのコンポーネントおよびコミュニケーションを理解することにより、IT プロフェショナルはセキュリティ ガイダンスを強化し、常に最新の情報を入手できます。IT プロフェショナルが組織のオペレーティング システムおよびアプリケーション ソフトウェアで、信頼のレベルを判断したり、維持できない場合、組織がリスクにさらされ、いくつかのセキュリティの脆弱性を持つことになります。さらに、セキュリティが悪用され、収益の損失、クリーン アップ費用および IT 環境の再構築、知的所有権、訴訟、またはそれ以上の悪い結果を引き起こす可能性があります。この脅威を最小限にするには、組織がシステムを正しく構成し、最新のソフトウェアを使用して、推奨されているセキュリティ更新プログラムをインストールすることが必要です。すべての組織向けにドキュメント化されたセキュリティ リリースおよび更新プログラムのポリシーを作成して、コミュニケートすることは、多くの企業のリスク管理プロセスで重要な部分です。

本ガイドは、IT プロフェショナルがマイクロソフトのセキュリティ リリース情報、プロセス、コミュニケーションおよびツールを深く理解するために役立ちます。マイクロソフトのゴールは、IT プロフェショナルが組織的なリスクを管理し、セキュ

リティ更新プログラムについて反復可能で、効果的な展開メカニズムを開発することです。

背景にあるリスク管理のフレームワーク さまざまなセキュリティ更新プログラム リリースのコミュニケーション、ガイダンス、プログラムおよびサービスがどのように組織のリスク管理に役立つか、IT プロフェショナルに理解していただくため、本ガイドは一般のお客様のリスク管理の枠組みに従っています。これは図 4 に示され、後ほど詳細を説明します。この枠組みは一般的で、IT プロフェショナルが従うためのベースラインの役割を果たすように意図されています。また、同時にリスク管理の枠組みでマイクロソフトの特定のリソースを使用する場合、関連性およびその伝達を支援するのに、必要な情報も含まれています。

図 4: お客様のリスク管理の枠組み

脆弱性の管理

ソフトウェアの脆弱性は紛れもない事実です。ソフトウェア製品の構想からリリース、展開そしてその後までのライフ サイクルを通し、すべての脆弱性を防ぐのは不可能です。SDL は、残存している脆弱性の深刻度および影響を低減すると共に、マイクロソフトのソフトウェアにおける脆弱性の数を減少させることを目的としています。しかし、ソフトウェアを開発しているのは人間であるため、脆弱性は残存します。お客様の保護をより強化するために、マイクロソフトの信頼できるコンピューティング (TwC) グループには、マイクロソフト セキュリティ レスポンス センター (MSRC) が含まれています。このグループでは、マイクロソフトのソフトウェアの脆弱性およびその可能性があるものを調査します。

マイクロソフトの脆弱性管理。マイクロソフトおよび MSRC が製品の脆弱性を解決する一般的な方法は、セキュリティ更新プログラムを公開することです。製品の脆弱性を効果的に解決するセキュリティ更新プログラムの作成は、広範なプロセスで、一連の連続したステップが含まれています。脆弱性の発見からセキュリティ更新プログラムの公開までの時間の長さには多くの要素が影響します。すべての脆弱性にはそれぞれ、固有の問題があります。しかし、一般的には、マイクロソフトに脆弱性の可能性があるものが報告された際に、指定のセキュリティ エンジニアが、影響を受ける製品に対する脅威の程度および影響を調査します。MSRC が、その脆弱性の程度および深刻度を確認すると、適切なマイクロソフトの製品チームと協力して、影響を受けるすべてのサポートされているバージョン用のセキュリティ更新プログラムを開発します。最終的に、このチームでセキュリティ更新プログラムが作成された後、サポートされている

様々なオペレーティング システム、アプリケーションおよび世界中の影響する言語について、多数の組み合わせと順列で検証を行う必要があります。

セキュリティ更新プログラムは、すべての状況に該当するわけではないため、マイクロソフトは、マイクロソフトからの組織のセキュリティに必要な情報に関する通知として、セキュリティ アドバイザリも公開しています。

マイクロソフト セキュリティ更新プログラム用語

本セクションの内容*:*

- マイクロソフトのソフトウェア更新プログラムの用語
- セキュリティ以外、またはシステム ソフトウェアの更新プログラム管理
- Windows® Update の利点 vs Microsoft® Update の利点
- 非正規のマイクロソフト ソフトウェアに対するセキュリティ更新プログラムのポリシー

本セクションを終了すると、*IT* プロフェッショナルは次の項目について理解します*:*

- 異なる種類のマイクロソフトのソフトウェア更新プログラム
- Windows Update と Microsoft Update の違い、および、それぞれを構成するためのリソース
- 非正規のマイクロソフト ソフトウェアに対するマイクロソフト セキュリティ更新プログラム ポリシー

本セクションにおけるマイクロソフトの参照リソース*:*

- **システム ソフトウェアの更新プログラムの管理。** For IT プロフェショナルが組織のサーバー、デスクトップ コンピューターおよびモバイル コンピューターに適用が必要なソフトウェア更新プログラムの管理についての情報は、technet.microsoft.com/updatemanagement/ をご覧ください。
- **Windows Server Update Services (WSUS) および更新プログラム** このページでは、WSUS がマイクロソフトの更新プログラムを保存および管理する方法を説明するために役立ちます。technet.microsoft.com/updatemanagement/bb245780.aspx (英語情報) をご覧ください。
- マイクロソフト **Windows 悪意のあるソフトウェアの削除ツール (MSRT)。** MSRT はサポートされている Windows のオペレーティング システムを実行しているコンピューターを確認します。www.microsoft.com/japan/security/malwareremove/ をご覧ください。
- **Office Update.** 2009 年 8 月 1 日以降、Office Update にアクセスを試行して、更新プログラムをダウンロードしようとする場合、そのユーザーは、Microsoft Update の Web サイトにリダイレクトされます。
- **Windows Update.** これは、無償のビルトイン サービスで、コンピューターをより安全で、信頼性を高く保ち、また、デバイスとの互換性も保つために役立ちます。Windows Update は新たな機能を提供して、Windows のエクスペリエンスを強化できます。www.microsoft.com/ja-jp/windows/downloads/windowsupdate/ をご覧ください。
- **Microsoft Update** これは、Windows に含まれている無償のビルトイン サービスです。単一の場所から更新プログラムの入手と自動更新のスケジューリングが行えます。さらに、お客様は、Microsoft Office システムおよびインターネット サービスである Windows Live™ ネットワーク

のようなマイクロソフトのソフトウェア向けのセキュリティおよびセキュリティ以外の更新プログラムを入手可能です。update.microsoft.com/microsoftupdate をご覧ください。

- **Microsoft Update Solution Center (マイクロソフト サポート オンライン)。**これには、Windows Update の使用に関する最も一般的な問題や一般的なエラー メッセージの説明などのソリューションを含む、ヘルプおよびサポートが含まれます。support.microsoft.com/ph/6527#tab3 をご覧ください。

マイクロソフト ソフトウェア更新プログラム

マイクロソフト セキュリティ更新プログラムとマイクロソフト ソフトウェア更新プログラムには明確な違いがあります。後者は、例えば新しいバージョンのデバイス ドライバーや、アプリケーションまたは Windows コンポーネントを向上させるもので、前者は、例えばセキュリティの専門家から報告されたセキュリティ脆弱性を修正するものです。

次は、Windows Update の一環として、または Windows Server Update Services (WSUS) に配布されるマイクロソフトの更新プログラムの種類です。

- **セキュリティ更新プログラム**製品特有のセキュリティ関連の脆弱性に対応する、幅広く公開される修正プログラムです。セキュリティの脆弱性は MSRC によって深刻度を基に評価され、緊急、重要、警告、注意 (深刻度の評価についての詳細は後ほど説明します) で示されます。
    - 本ガイドはこれらの種類の更新プログラムのみに焦点を絞ります。
    - WSUS および Microsoft updates の使用に関する詳細情報は、次の Web サイトをご覧ください: technet.microsoft.com/ja-jp/updatemanagement
- **緊急の更新プログラム**緊急のセキュリティ以外の不具合を解決する、幅広く公開される特定の問題用の修正プログラムです。緊急の更新プログラムの例として、マイクロソフト Windows 悪意のあるソフトウェアの削除ツール (後述) の更新プログラムがあります。
- **定義ファイルの更新プログラム**幅広く頻繁に公開されるソフトウェアの更新プログラムで、製品の定義のデータベースに追加されます。定義のデータベースは、悪質なコード、フィッシング Web サイトまたは迷惑メールなど、特定の属性を持つオブジェクトの検出に頻繁に使用されます。
- **更新プログラム ロールアップ**検証済みの、累積的な修正プログラムのセット、セキュリティ更新プログラム、緊急の更新プログラム、およびその他の更新プログラムが、容易な展開のためにパッケージ化されたものです。通常、ロールアップはセキュリティ、または製品コンポーネントのような特別な分野を対象にしています。その他、更新プログラム ロールアップの一例にはサービス パックがあります。
- **サービス パック:** 検証済みの、累積的な修正プログラムのセット、セキュリティ更新プログラム、緊急の更新プログラムおよび更新プログラム、そして製品リリース後に社内で検出された問題に対する追加の修正プログラムです。サービス パックにも、お客様からご要望のあった限定数のデザイン変更または機能が含まれる場合があります。
- **Feature pack:** 一般的に、次の完全な製品のリリースに含まれる製品の新機能です。Feature pack には、新たなセキュリティ機能や改善が含まれる場合があります。

種類分けに関係なく、クライアント側のオペレーティング システムから見ると、すべてのマイクロソフトの更新プログラムは「重要」「推奨」および「オプション」と指定されています。

- **重要** (Windows® XP では、優先度の高い) の更新プログラムは、改善されたセキュリティ、プライバシーおよび信頼性などの重要な利点を提供します。これらは利用可能になると、インストールされます。
- **推奨** (Windows XP ではオプション) の更新プログラムは、緊急以外の問題の解決や、お客様のコンピューティング エクスペリエンスを強化します。これらの更新プログラムはシステムの基本的な問題を解決しませんが、アプリケーションの互換性の向上、機能の向上など、重要な向上を提供します。
- **オプション**の更新プログラムには、更新プログラム、ドライバーまたはマイクロソフトあるいはそのパートナーによる、お客様のコンピューティング エクスペリエンスを強化するための新たなアプリケーションが含まれます。これらの更新プログラムは手動でインストールする必要があります。つまり、オプションの更新プログラムは自動でダウンロードまたはインストールされませんが、レビューのために Windows Update で表示されます。

特に、重要および推奨される更新プログラムなど、最新のソフトウェア更新プログラムを素早く、継続的に各自のコンピューターにダウンロードおよびインストールすることは、セキュリティおよび適切な機能性を維持するために重要なことです。IT プロフェショナルにとっては、組織のコンピューターに更新プログラムを適用することは、サイズに関わらず、システムを安全に保ち、正しく実行するために重要なことです。Windows Update (Microsoft Windows に含まれる無償の組み込みサービス) は、組織のコンピューターが安全性および信頼性をより高く保ち、デバイスやアプリケーションと互換性を保つために役立てられます。単一の場所で提供され、更新プログラムの取得および自動更新のスケジュール設定が可能です。

Windows Update (Windows XP では自動更新) クライアントは、既定で Windows Update のみを確認します。Windows およびその他のマイクロソフト ソフトウェアの更新プログラムを入手するために、IT プロフェショナルは Microsoft Update サービスを利用して更新プログラムを確認するよう、Windows Update を構成する必要があります。Microsoft Update は、Windows オペレーティング システムを実行しているすべてのコンピューターが、マイクロソフトから利用可能なセキュリティおよびソフトウェアの更新プログラムについて必ず通知されるために、推奨されます。Microsoft Update をご使用になるには、update.microsoft.com/microsoftupdate をご覧ください。

Windows Update は Windows Vista®、Windows 7 および Windows XP のオペレーティング システムで若干異なる構成を持っています。Windows Update およびその機能に関する詳細情報は、www.microsoft.com/ja-jp/windows/downloads/windowsupdate/ をご覧ください。

Office Update、Microsoft Update それとも Windows Update?

Office Update または Windows Update の代わりに Microsoft Update を使用するようコンピューターを構成します。これにより、コンピューターが Windows オペレーティング システム用のセキュリティ更新プログラムに加え、Microsoft Office システムおよびその他のマイクロソフトのアプリケーションのセキュリティ更新プログラムを確実に受け取ることができます。Microsoft Update および Windows Update の違いに関する説明は、windows.microsoft.com/ja-jp/windows/help/windows-update をご覧ください。

2009 年 8 月 1 日以降、Office Update にアクセスを試行して、Office Updates を使用して更新プログラムをダウンロードする場合、ユーザーは自動的に Microsoft Update の Web サイトにリダイレクトされます。

Windows Update プロセスに関する詳細情報は、download.microsoft.com/download/a/9/4/a94af289-a798-4143-a3f8-77004f7c2fd3/Windows%20Update%20Explained.docx で利用可能な、ホワイト ペーパー “Windows Update Explained,”(英語情報) をご覧ください。

Windows Update をご利用の際に最もよく起きる問題に対する解決策などのヘルプおよびサポート、エラー メッセージの説明については、マイクロソフト サポート オンライン (support.microsoft.com/ph/6527#tab3) をご覧ください。

本ガイドで説明しているサービスやプロセスの中には、セキュリティ以外の更新プログラムをインストールするために使用可能なものもありますが、通常これらの更新プログラムは、セキュリティの目的で必要ではないため、重点を置きません。

他のすべての種類の更新プログラムによるシステムの維持に関する情報は、technet.microsoft.com/updatemanagement/ をご覧ください。

非正規ソフトウェアに対するセキュリティ更新プログラム ポリシー

Windows Update (Windows XP の自動更新) は、正規および非正規の Windows コンピューターに、Windows および
その他のマイクロソフトのソフトウェア向けのセキュリティ更新プログラムを提供します。非正規の Windows システムも、Windows およびその他のマイクロソフトのソフトウェア向けのサービス パック、更新プログラム ロールアップ、および重要な信頼性およびアプリケーションの互換性のための更新プログラムをインストール可能です。システムの正規、非正規に関わらず、より多くのシステムが保護されるため、このアプローチはコンピューター エコシステム全体をより安全に保つために役立ちます。しかし、マイクロソフトの判断により、その他の付加価値のある更新プログラムおよびソフトウェアは、非正規のシステムに対してブロックされる場合があります。

Windows 7 および Windows Vista では、非正規の Windows システムは、Windows Update コントロール パネルを介して利用可能な更新プログラムにアクセス可能です。Windows XP では、非正規の Windows システムは、自動更新でのみセキュリティ更新プログラムにアクセスできます。

マイクロソフトのソリューションを使用して、セキュリティ更新プログラムを管理する

本セクションの内容:

- マイクロソフト製品を使用して、セキュリティ更新プログラムを管理するための 3 種類のアプローチには、それぞれ独自の利点および考慮点があります。
    1. Microsoft Update および自動更新に依存する更新プロセス
    2. Windows Server Update Services (WSUS) に依存する更新プロセス
    3. Microsoft System Center の構成マネージャーに依存する更新プロセス

本セクションを終了すると、*IT* プロフェショナルは次を理解します:

- セキュリティ更新プログラムを管理するために Microsoft Update および自動更新を使用する必要性および考慮点
    - *Microsoft Update* および自動更新を使用した管理されたセキュリティ更新プログラムのプロセスが必要な *IT* プロフェショナルおよび組織が読む必要があるのは、このセクションのみです。
- セキュリティ更新プログラムを管理するために、WSUS を使用する必要性および考慮点
    - WSUS はマイクロソフト以外の更新プログラムの展開をサポートしません。
- セキュリティ更新プログラムを管理するために、Microsoft System Center Configuration Manager を使用する必要性および考慮点
    - その他の多くの機能の中で、Configuration Manager はマイクロソフトの更新プログラムおよびマイクロソフト以外の更新プログラムをサポートします。

本セクションにおけるマイクロソフトの参照リソース:

- **Microsoft Update。** これは、Windows に含まれている無償のビルトイン サービスです。単一の場所で更新プログラムの入手と自動更新のスケジューリングができます。さらに、お客様は、Microsoft Office システムおよび Windows Live のようなマイクロソフトのソフトウェア向けのセキュリティおよびセキュリティ以外の更新プログラムを入手可能です。update.microsoft.com/microsoftupdate をご覧ください。
- **Windows Server® Update Services**. これを使用して、更新プログラムの設定を完全に管理し、お客様のネットワーク上のコンピューターへの更新プログラムの配布を制御します。technet.microsoft.com/wsus/ をご覧ください。
- **Microsoft System Center の構成マネージャー** これは、大規模で複雑、また異種システムが混在する IT インフラストラクチャで使用し、物理的、仮想的、分散した、およびモバイルの環境のサーバー、クライアントおよびデバイスを包括的に査定、導入、および更新します。microsoft.com/systemcenter/configurationmanager をご覧ください。

- コンプライアンス評価に対して更新をカスタマイズするには、technet.microsoft.com/library/bb633119.aspx をご覧ください。

マイクロソフトのソリューションを使用した、セキュリティ更新プログラムへの 3 種類のアプローチ。マイクロソフトが開発した、ソフトウェア更新ツールの包括的なスイートは、コンピューターを自動的に更新し、悪意のあるソフトウェアの攻撃からコンピューターを保護するために役立てられます。しかし、さまざまな理由で、個人あるいは組織は、マイクロソフトのソフトウェアを更新するための他の方法を検討する場合があります。この点を考慮して、マイクロソフトは多様なソリューションを開発し、独自の特定の環境で可能な限り最新であるために異なるニーズを持つ IT プロフェショナルを支援します。セキュリティ更新プログラムの管理には、多くのアプローチがありますが、このセクションでは、マイクロソフトのソフトウェア更新ソリューションを使用する 3 種類のアプローチにまとめ、Windows のお客様のセキュリティ更新に対するニーズを解決します。その 3 種類は次の通りです。

1. Microsoft Update および自動更新に依存する更新プロセス
2. Windows Server Update Services (WSUS) に依存する更新プロセス
3. Microsoft System Center Configuration Manager に依存する更新プロセス

Microsoft Update および自動更新による更新プロセス

対象とするお客様	個人ユーザーおよび小規模企業 (通常、50 台未満のコンピューターを所有)
ニーズ	すべてのシステムが最新のマイクロソフトのセキュリティ更新プログラムで常に最新に保たれるようにします。
利点および考慮点	• セキュリティ更新プログラムは、最小限のユーザーの操作またはユーザーの操作がなくてもインストール可能で、セキュリティ更新プログラムの技術的な詳細を理解するは必要ありません。 • 各組織で、マイクロソフト セキュリティ更新プログラムにより影響を受ける可能性がある基幹業務 (LOB) のアプリケーションまたはその他のカスタム アプリケーションを持たないようにしてください。
価格	すべての IT プロフェショナルが無償で利用可能です。

自動更新の機能やお客様が Microsoft Update でオプトインしている場合、Windows はすべてのマイクロソフト製品について最新のセキュリティ更新プログラムで自動的にコンピューターを最新に保ちます。ユーザーは、更新プログラムおよび情報を検索する必要がありません。Windows はコンピューターにそれらを直接配信します。

Windows はシステムがオンラインであるのを確認し、インターネット接続を使用して Microsoft Update Web サイトからダウンロードを検索します。

ユーザーは Windows がコンピューターを更新する方法および日時を指定できます。例えば、図 5 に示されているように、推奨される構成として、ユーザーは指定したスケジュールで自動的に更新プログラムをダウンロードおよびインストールするよう Windows を設定できます。

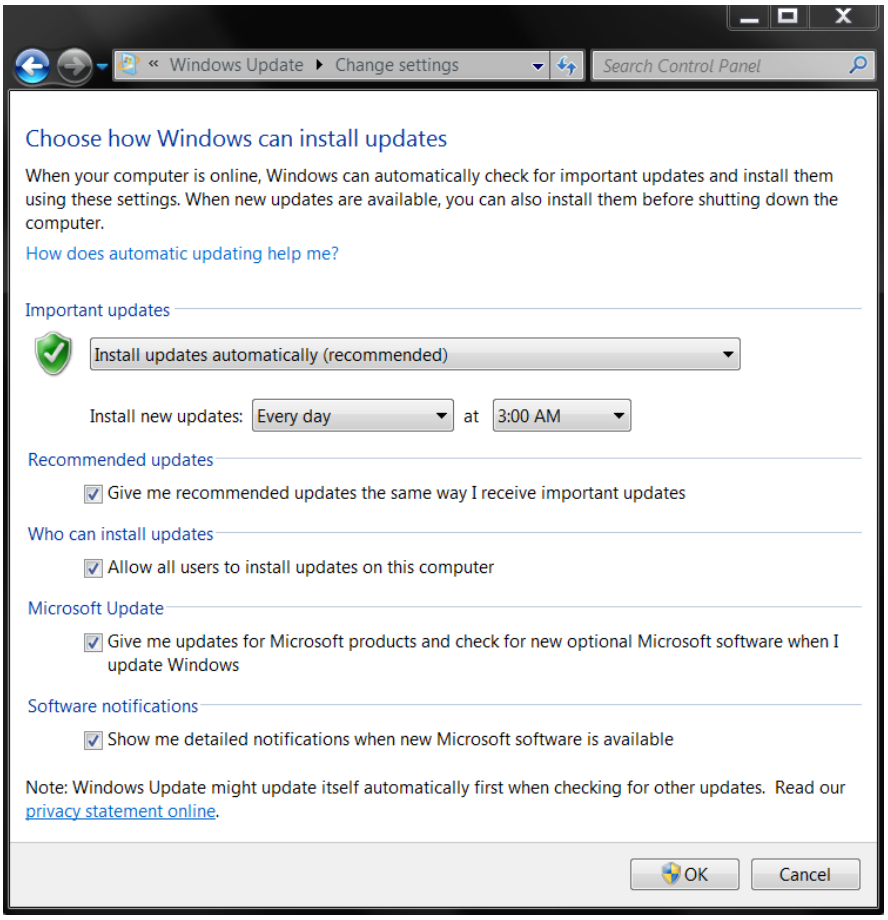


図 5: Windows 7 の自動更新の設定

これは、専門の IT ヘルプデスクなどの機能を持たない個人ユーザーまたは小企業環境のユーザーに推奨されるアプローチです。このアプローチを使用することで、最小限の技術的な専門知識およびコンピューター使用時の中断を最小限に抑えて、コンピューターを最新に保つことができます。

皆さんの組織がこの自動管理プロセスだけを必要とする場合、本ガイドラインで提供している残りの情報は、参考程度にご覧ください。大部分が、このセキュリティ更新プログラムのアプローチに対しては適用外です。

現在の構成を検証して、最新の更新プログラムを確認するには、update.microsoft.com/microsoftupdate をご覧ください。

Windows Server Update Services (WSUS) による更新プロセス

対象とするお客様	中規模企業および大規模企業 (通常 50 台以上のコンピューターを所有)
ニーズ	お客様のネットワークのコンピューターに対し、更新プログラムの設定を完全に管理し、更新プログラムの配布を制御します。
利点および考慮点	• WSUS はマイクロソフト以外の更新プログラムの展開はサポートしません。 • 構成可能なオプションにより、IT プロフェショナルは管理されたデバイスのインベントリ レポートを集め、どの更新プログラムをコンピューターまたはコンピューター グループに適用するかを判断し、必要な更新プログラムの作業を指定し、柔軟性のあるスケジュールで、ほとんどもしくは全くユーザー操作なしに更新プログラムをインストール可能です。 • このプロセスは、社員の生産性およびネットワークの機能性に対し、変化が感じられる程度の影響を低減します。 • 特定のコンピューターに必要とされるセキュリティ更新プログラム、というようなカスタム レポートを作成し、セキュリティ更新プログラムの通知および自動配布をスケジュールします。 • 特定のノードをセキュリティ更新プログラムの対象とします。 • 多層のサーバーの階層を持つ複雑なネットワーク上の複数のサーバーを単独のコンソールから管理します。
価格	サポートされているバージョンの Windows Server® のライセンス ユーザーは、無償で利用可能です。

専門の IT ヘルプデスクなどの機能を持たない組織で、高度なレベルで組織の Windows クライアントおよび Windows サーバーにセキュリティ更新プログラムを配布する日時と方法を管理したい場合、有効な Windows サーバー ライセンス所有ユーザーには、無償で WSUS (technet.microsoft.com/wsus/ をご覧ください) がご利用になれます。WSUS により、管理者はサポートされているバージョンの Windows サーバーまたはクライアント製品を実行しているコンピューターに対し、マイクロソフト製品のセキュリティ更新プログラムの展開を管理できます。WSUS を使用すると、管理者はネットワークのコンピューターに、Microsoft Update を介して公開された更新プログラムの配布をより良く管理できます。

セキュリティ更新プログラムの管理に WSUS を使用するアプローチで特筆すべき特徴としては、次のものがあります。

- WSUS はマイクロソフトの更新プログラムの展開のみをサポートしています。
- 更新プログラムは、次の種類で特定します:
  - 製品または製品ファミリ (例: Windows Server® 2003 または Microsoft Office system)
  - 更新プログラムの分類 (例: 緊急の更新プログラム、ドライバーなど)
  - 言語 (例: 英語および日本語のみ)
- 自動的に同期を開始するように設定する、締め切りを強制する、特定の日時を設定して更新プログラムをインストールまたはアンインストールします。管理者は締め切りを過去の時間に対して設定することで、ダウンロードを即時に実行するよう強制できます。
- 電子メールによる新たな更新プログラムの通知、および、更新プログラムの状態、コンピューターの状態、コンピューターのコンプラインスの状態、更新プログラムのコンプライアンスの状態を基にしたレポーティング機能を設定します。
- 管理者は次のような狙ったタスクを実行可能です。
  - テスト コンピューター グループに新しい更新プログラムを適用して、運用環境に配布する前に更新プログラムを評価します。
  - 特定のアプリケーションを実行しているコンピューターを保護します。例えば、緊急の更新プログラムが特定のコンピューターで使用しているアプリケーションと互換性がない場合、管理者は更新プログラムがそれらのコンピューターに配布されていないことを確認できます。
- パフォーマンスの向上、および帯域幅の最適化を達成できます。

Microsoft System Center Configuration Manager による更新プロセス

対象とするお客様	先進組織、または大規模組織 (通常、複数拠点の組織、または特定の管理やコンプライアンス要件を持つ組織)
ニーズ	物理的、仮想的、分散した、およびモバイル環境のサーバー、クライアント、およびデバイスを包括的に評価、展開および更新します。Windows に最適化されており、さらに拡張可能であるため、大規模、複雑および異機種環境の IT インフラストラクチャを持つ組織の IT システムへの考察を強化し、制御を得るために最良の選択です。
利点および考慮点	• このプロセスはマイクロソフトおよびマイクロソフト以外のソフトウェアの更新プログラムおよびアプリケーションの管理および配布をサポートします。 • このプロセスは、組織の IT システムが望ましい構成状態にあるようにし、ネットワーク全体におけるシステムの可用性、セキュリティおよびパフォーマンスを改善しま

	す。 • このプロセスは、WSUS に含まれない高度な管理者制御と情報を提供します (例えば、マイクロソフト製品、サード パーティのアプリケーション、カスタム、社内、LOB アプリケーション、ハードウェア ドライバーなどの更新プログラムの配布)。 • メンテナンス ウィンドウを使用して予め指定した回数および日付で、サーバーおよびクライアントにシステム変更を適用します。 • カスタマイズ可能なユーザー インターフェイスを表示して、より優れたユーザー エクスペリエンスの管理を行い、再起動およびインストールなどの実施構成について詳細な制御を維持します。
	www.microsoft.com/japan/systemcenter/configmgr/howtobuy/pricing-licensing.mspx をご覧になるか、または米国以外の場合、現地のマイクロソフト代表またはパートナーにご連絡ください。

セキュリティ更新プログラムのプロセスに別のレベルの機能性および制御を望んでいる組織について、このアプローチは Microsoft System Center Configuration Manager を使用して WSUS 環境を管理し、追加の更新プログラムの管理および適用方法を実現します。

WSUS が無償なのに、どうしてこのアプローチは有償なのですか?

このソリューションは、WSUS に含まれていない高度な管理者制御および認知の領域で、いくつかの機能性を提供します。特に、IT プロフェショナルはマイクロソフト製品、サードパーティのアプリケーション、カスタム、社内、LOB アプリケーション、ハードウェア ドライバーおよび基本入力/出力システム (BIOS) などの更新プログラムをデスクトップ コンピューター、ポータブル コンピューター、サーバーおよびモバイル機器などの、さまざまなデバイスに配布可能です。IT プロフェショナルは、ネットワーク アクセス保護 (NAP) を使用して検疫サポートを有効にしたり、コンピューターのインベントリの特徴を基にコレクションを作成可能です。これにより、管理者は、次のような機能を実行する一方で、より上手く更新プログラムに焦点を絞れます。

- マイクロソフトおよびマイクロソフト以外の更新プログラムを管理します。従って、更新の管理に異なるツールを使用するのではなく、ひとつの製品ですべての管理タスクを実行できます。
- サービス ウィンドウ (通知) をベースに更新プログラムを展開します。
- カスタマイズ可能なユーザー インターフェイスを表示してより優れたユーザー エクスペリエンスの管理を行い、再起動やインストールなどの実施構成について詳細な制御を維持します。
- インベントリ情報により環境への対応を完全に理解し、更新プログラムについて、システム状態の詳細な状況を入手します。

IT プロフェショナルは、必要な構成管理 (DCM)、ネイティブのソフトウェア開発キット (SDK) および独立したソフトウェア ベンダー (ISV) パートナーの協力により、構成マネージャーを拡張できます。DCM

を使用して、IT プロフェショナルは、マイクロソフトおよびサード パーティの最善策の構成知識を利用して、構成定義およびメンテナンスを改善できます。

Microsoft System Center の構成マネージャーの詳細情報は、www.microsoft.com/japan/systemcenter/configmgr/ をご覧ください。

Microsoft System Center の構成マネージャーを使用して強化された更新プログラムの機能を提供する方法に関する詳細情報は、technet.microsoft.com/library/bb633119.aspx の「ソフトウェアの更新の構成」をご覧ください。

本ガイドの後半では、WSUS による更新プログラム プロセスを使用します。それは、このアプローチが、マイクロソフトのセキュリティ更新プログラムに対する構成可能で移植可能なリスク管理フレームワークの確かなベースラインを提供するからです。

マイクロソフト セキュリティ更新プログラムのリリース プロセス

本セクションの内容:

- 初めに、マイクロソフトからの通知で始まる、マイクロソフトのセキュリティ更新プログラムのリリース プロセス
- さまざまなマイクロソフトのセキュリティ リリースの通知およびセキュリティ更新プログラム
  - セキュリティ情報の事前通知サービス
  - セキュリティ情報のサマリー
  - セキュリティ情報
  - セキュリティ更新プログラム
  - サポート技術情報
  - セキュリティ アドバイザリ
- セキュリティ更新プログラムを標的にした電子メール メッセージ詐欺
- マイクロソフト セキュリティ リリース受信後に開始する、お客様のリスク管理のフレームワーク
  1. ステージ 1: マイクロソフト セキュリティ リリースの通知を受け取る
  2. ステージ 2: リスクを評価する
  3. ステージ 3: 緩和策を評価する
  4. ステージ 4: 標準および緊急の更新プログラム展開のタイムライン
  5. ステージ 5: システムを監視する

本セクションを終了すると、*IT* プロフェショナルは次を理解します:

- マイクロソフト セキュリティ更新プログラムに付随するガイダンスおよび多様なリソースを理解します。
- マイクロソフトのセキュリティ更新プログラムに関するリソースおよびガイダンスにマップ可能な、お客様のリスク管理の枠組みを確認します。
- マイクロソフトが電子メールの添付でセキュリティ更新プログラムを配布しないことを理解します。マイクロソフトは IT プロフェショナルが、本ガイド、セキュリティ情報のリンク先、または Microsoft Update、Windows Update、WSUS または Microsoft System Center Configuration Manager などの展開ツールを利用して、マイクロソフトのセキュリティ更新プログラムを入手することを推奨します。

本セクションで紹介されているマイクロソフトのリソース

- **セキュリティ情報の事前通知サービス:** www.microsoft.com/japan/technet/security/bulletin/advance.mspx をご覧ください。

- **セキュリティ情報のサマリー:** www.microsoft.com/japan/security/bulletins/secinfo.mspx をご覧ください。
- **セキュリティ情報:** www.microsoft.com/japan/technet/security/current.aspx をご覧ください。
- **セキュリティ アドバイザリ:** www.microsoft.com/technet/security/advisory/ をご覧ください。
- **セキュリティ通知:** technet.microsoft.com/ja-jp/security/dd252948 をご覧ください。
- **サポート技術情報の記事**: サポート技術情報番号で検索してください。www.microsoft.com/japan/technet/security/current.aspx をご覧ください。
- **MSRT:** www.microsoft.com/japan/security/malwareremove/ をご覧ください。

マイクロソフト セキュリティ リリースに関するコミュニケーション

製品のセキュリティを脅かす脆弱性に関する情報がある場合、マイクロソフトはお客さまに次のような通知を送信します。

セキュリティ情報の事前通知

セキュリティ情報の事前通知には、新たに公開されるセキュリティ情報の数、影響を受ける製品、総合的な最大深刻度、および更新プログラム関連の検出ツールについての情報が含まれます。含まれる情報の詳細の度合いは、攻撃が構築される可能性のある情報は公開せず、セキュリティ更新プログラムが公開されるまで組織を保護する必要性とバランスが保たれています。予告なしの提供を避けるため、また、混乱の可能性を最小限に抑えるため、セキュリティ情報の事前通知はセキュリティ情報に関連しない同日公開の別の更新プログラムの情報も提供します。特に MSRT 向けの更新プログラムに加えて、Microsoft Update および Windows Update で公開されるセキュリティ以外の更新プログラムの件数を説明します。

可能であれば、マイクロソフトは、セキュリティ情報を公開する 3 営業日前に通知を行います。この事前通知は、IT プロフェショナルが、差し迫るセキュリティ更新プログラムのリリースに備え、適切なリソースを計画するのに役立つものです。詳細情報については、www.microsoft.com/japan/technet/security/bulletin/advance.mspx のマイクロソフト セキュリティ情報の事前通知をご覧ください。

時折、サマリーセキュリティ情報の事前通知に記載されていても、セキュリティ情報サマリーがセキュリティ情報の事前通知を置き替える際にリリースされないセキュリティ情報があります。これは、マイクロソフトがセキュリティ更新プログラムを公開するまで、品質をテストするからです。マイクロソフトで、セキュリティ情報の事前通知のリリースから、セキュリティ情報および該当のセキュリティ更新プログラムの公開までの間に品質問題を検出した場合、マイクロソフトはセキュリティ情報およびセキュリティ更新プログラムの公開を延期する場合があります。時として、組織のセキュリティ更新プログラム計画への影響具合によっては、マイクロソフトは、これを反映するセキュリティ情報の事前通知を再公開する場合があります。

セキュリティ情報サマリー

セキュリティ情報およびセキュリティ更新プログラムが公開される場合、セキュリティ情報の事前通知がセキュリティ情報サマリーに置き替わります。これは、リリースに含まれるセキュリティ情報に関して最も信頼のおける情報のリソースです。事前通知の情報に加え、セキュリティ情報サマリーには各脆弱性の悪用の可能性の評価が含まれています (これは「Exploitability Index」という名称で、後ほど説明します)。マイクロソフト セキュリティ情報サマリーの詳細情報については、www.microsoft.com/japan/technet/security/bulletin/summary.mspx をご覧ください。

セキュリティ情報

セキュリティ情報サマリーには、IT プロフェショナルがリスク評価をする際に役立つ特別な技術情報を提供するすべての関連サポート技術情報と共に、サマリーリリースに含まれる各セキュリティ情報へのリンク先が含まれています。各セキュリティ情報には、セキュリティ更新プログラムおよび脆弱性に関する詳細なガイダンスと情報が含まれています。セキュリティ情報は、19 言語にローカライズされ、「よく寄せられる質問」「脆弱性情報」「緩和策および回避策」およびその他の関連のセキュリティ更新プログラムの情報が含まれています。詳細情報については、www.microsoft.com/japan/technet/security/current.aspx の「Microsoft セキュリティ情報検索」ページをご覧ください。

セキュリティ更新プログラム

セキュリティ更新プログラムは、セキュリティ情報で説明しているセキュリティの脆弱性を解決するファイルを含む、ダウンロードです。これらのファイルは、更新プログラムを適用するために必要で、検証、および組織で必要なコンピューターへの適用ができます。本ガイドの後半に、セキュリティ更新プログラムの入手、検証および展開に関する情報が掲載されています。

ひとつのセキュリティ更新プログラムが、Common Vulnerabilities and Exposures (CVE) のデータベース [4] の複数の脆弱性を解決することがよくあります。それぞれが、その他の関連の問題と共に、該当のマイクロソフト セキュリティ情報の一覧に掲載されています。可能な場合はいつでも、MSRC は、ひとつのバイナリまたはコンポーネントに影響を与える複数の脆弱性を統合し、1 件のセキュリティ更新プログラムでそれら脆弱性を解決します。これにより、MSRC は、IT プロフェショナルが個々のセキュリティ更新プログラムをテストおよび各自のコンピューター環境に統合する際に直面する混乱の可能性を最小限にする一方で、各更新プログラムの効果を最大にすることができます。

サポート技術情報 (KB)

Microsoft Customer Service and Support (CSS) は、セキュリティ情報とすべての情報を重複させずに、該当のセキュリティ情報に関連するサポート技術情報 (KB) を書きます。サポート技術情報は、セキュリティ更新プログラムの既知の警告や現象を明らかにするためにリリースされ、セキュリティ更新プログラムを提供するセキュリティ情報に継続して掲載されます。

[4] cve.mitre.org/

セキュリティ アドバイザリ

マイクロソフト セキュリティ アドバイザリは、19 言語にローカライズされ、脆弱性の可能性があるものや、IT プロフェショナルの全体的なセキュリティの資料となるその他のセキュリティ情報について、マイクロソフトが通知するものです。これらの通知は、必ずしもセキュリティ情報またはセキュリティ更新プログラムを必要としないものの、お客様の全体的なセキュリティに影響を与えるものがあります。セキュリティ アドバイザリの中には、セキュリティ更新プログラムの公開に至るもの、引き起こされた脅威を緩和するために、IT プロフェショナルに役立つガイダンスが含まれるものがあります。各セキュリティ アドバイザリは追加情報を説明する独自のサポート技術情報 (KB) 番号を伴います。セキュリティ アドバイザリが説明する可能性があるトピックの例は次の通りです:

- 一般で公開された脆弱性に適用可能なガイダンスおよび緩和策
- 一般で公開された脅威の可能性のあるものに関する情報

予測可能なセキュリティ更新プログラムのリリース プロセス

セキュリティ更新プログラムのリリースを予測しやすいようにし、リソース計画について IT プロフェショナルおよび組織を支援するために、マイクロソフトは標準化したセキュリティ更新プログラムのリリース プロセスを備えています。このプロセスは、常にセキュリティ情報の事前通知から始まり、IT プロフェショナルに間もなくセキュリティ更新プログラムを公開することを通知します。公開されると、セキュリティ情報では、付随するセキュリティ更新プログラムの技術的詳細および必要な変更を提供します。セキュリティ アドバイザリは、予測可能ではないものの、マイクロソフトのセキュリティ リリースの別の形です。セキュリティ情報の事前通知と同様に、マイクロソフトは IT プロフェショナルにセキュリティ アドバイザリが公開されたことを通知します (この通知に関する情報は後半にあります)。マイクロソフトのセキュリティ リリースが、セキュリティ情報および付随するセキュリティ更新プログラムの事前通知なのか、セキュリティ アドバイザリであるかどうかに関わらず、IT プロフェショナルは通知を受信後に、措置を講じてリスク管理プロセスを開始することが重要です。

マイクロソフトのセキュリティ リリース

本ガイドの目的に関して、「マイクロソフト セキュリティ リリース」は、お客様が措置を講じ、セキュリティ リスクを管理する必要がある、マイクロソフトからのセキュリティの通知を指します。繰り返しになりますが、この特定の通知は常にセキュリティ情報の事前通知またはセキュリティ アドバイザリのいずれかから始まり、IT プロフェショナルは独自の管理プロセスを開始する必要があります。一般的に、マイクロソフトが利用可能にするその他のリソースは、マイクロソフトのセキュリティ リリースと結び付けられています。本ガイドでは、これらのリソースがお客様のリスク管理のフレームワークに適用されるため、その詳細を説明します。

広範なリソースおよびガイダンス

マイクロソフトのセキュリティ リリースには通常、別の支援リソース、ガイダンス、ツールなどが含まれます。本ガイドは、リスク管理プロセスで利用可能な、さまざまなマイクロソフトのリソースを検証します。図 6 では、マイクロソフトのセキュリティ リリースおよび付随の信頼できるガイダンスを説明しています。マイクロソフトのセキュリティ リリースで利用可能なその他のさまざまなリソースについては、後に情報を提供します。

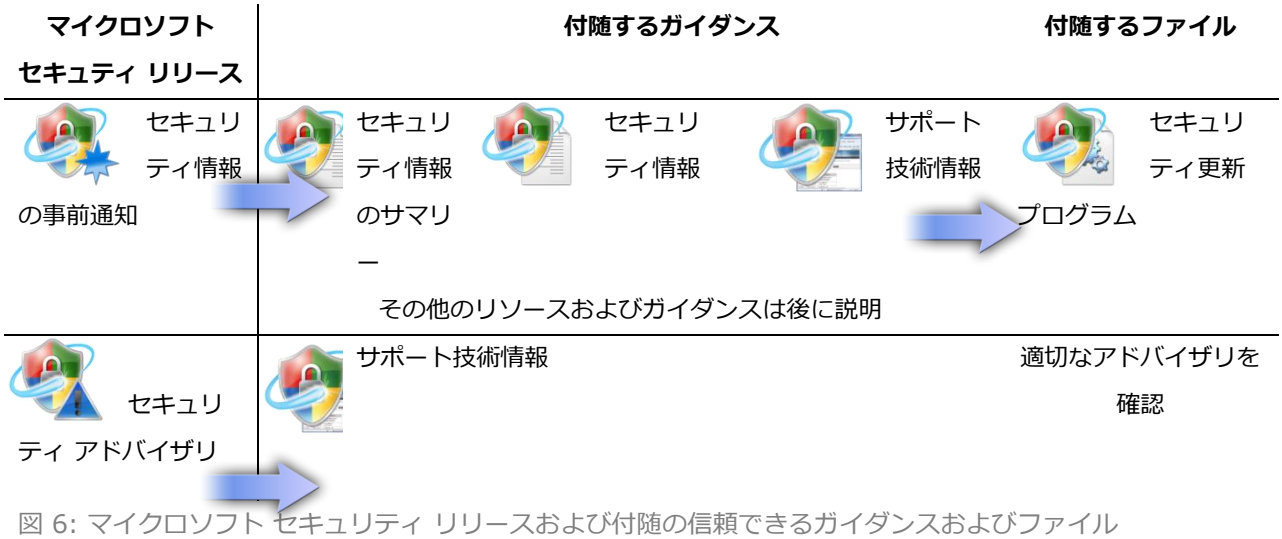


図 6: マイクロソフト セキュリティ リリースおよび付随の信頼できるガイダンスおよびファイル

マイクロソフト セキュリティ更新プログラムを標的にする不正な通知

マイクロソフトからのセキュリティ電子メール メッセージと称する電子メール メッセージで、実行可能ファイルが添付されているものは、決して正式なものではありません。このような電子メール メッセージは偽り、またはなりすましで、添付ファイルには悪意のあるソフトウェアが含まれる可能性があります。マイクロソフト セキュリティ更新プログラムの配布と称する電子メール メッセージを受信した IT プロフェショナルは、メッセージを削除し、添付ファイルを開かないことを推奨します。

マイクロソフトは、電子メールを利用してセキュリティ更新プログラムを配布しません。

マイクロソフトによるセキュリティの通知に関する電子メール メッセージは、IT プロフェッショナルが、このドキュメントのリンク、セキュリティ情報、または Microsoft Update、Windows Update、WSUS、Microsoft System Center Configuration Manager などの展開ツールを使用して、マイクロソフトのセキュリティ更新プログラムを入手することを常に推奨しています (セキュリティ更新プログラムの入手に関する追加情報は後ほど説明します)。

これらの悪質な電子メール メッセージの添付ファイルが開かれた場合、マイクロソフトは IT プロフェショナルに早急に完全なウイルス対策スキャンを実行し、悪意のあるソフトウェアがインストールされていないことを確実にすることを推奨します。さらに、IT プロフェショナルは無償のオンライン コンピューター セーフティー スキャンも実行可能です。実行するには safety.live.com をご覧ください。

マイクロソフトのお客様に対する、悪意のある電子メール メッセージの認識および回避に関する詳細情報は、www.microsoft.com/japan/protect/yourself/phishing/msemail.mspx をご覧ください。

お客様のリスク管理のフレームワーク

各セキュリティ リリースで利用可能なマイクロソフトのガイダンス、リソースおよびツールを説明するために、本ガイドでは、一般的なお客様のリスク管理のフレームワークを背景として採用しています。本ガイドにおいて、「お客様のリスク管理のフレームワーク」とは、マイクロソフトで利用可能なセキュリティ リリースのリソースを理解し活用するために IT プロフェショナルが従うことができる、一般的なリスク管理のフレームワークまたはタイムラインを指しています。図 7 は、お客様のリスク管理のフレームワークの主要な段階を特定しています (より詳細なバージョンは付録で利用可能です)。このフレームワークは最もまとまっており、タイムラインとして用いられます。

本ガイドで使用されているリスク管理のフレームワークは、主要な 5 段階に分かれています。各段階では様々なマイクロソフトのリソースおよび役立つヒントを説明しているので、IT プロフェショナルはリスクの管理のために詳しく情報を得られます。

1. マイクロソフトのセキュリティ リリースの通知を受け取る
2. リスクを評価する
3. すべての緩和策または回避策を評価する
4. 標準またはより緊急のタイムラインで、セキュリティ更新プログラムを作成、テスト、展開する
5. システムを監視する

図 7: お客様のリスク管理のフレームワーク

図 7 で特定されている段階は単純なものですが、実際には組織は、多様なレベルのセキュリティ リスクと、異なるレベルの管理およびサポートを含む複雑なインフラストラクチャを所有しています。例えば、上の図 7 の「標準の更新プログラムのタイムライン」および「緊急の更新プログラムのタイムライン」に示されているように、ひとつの展開タイムラインしか持たない組織がある一方、ふたつ以上の展開のタイムラインを持つ組織があります。このフレームワークの主な意図は、IT プロフェショナルがより情報を把握し、包括的な参考ドキュメントを所有できるよう、マイクロソフトのセキュリティ リソースとガイダンスがリスク管理のフレーム ワーク全体のどこに当てはまるのかを明確にすることです。

上記に関連して、IT プロフェショナルがいくつかの重要なポイントを理解することが重要です。

1. **セキュリティ更新プログラムのプロセスは複雑な場合があります。**多くのビジネス アプリケーションおよびカスタムの LOB アプリケーションをサポートしている組織では、特にそうです。しかし、優れたセキュリティ更新プログラムのプロセスを達成可能にするソリューションがいくつかあります。
2. **セキュリティ更新プログラムのアプローチは、極めて重要です。**お客様の必要性に応じて、本ガイドのひとつまたはそれ以上のアプローチを適用できます。IT プロフェショナルは、組織の全アプリケーション (サードパーティの更新プログラムや LOB アプリケーションを含む) のサポートに必要な、最適のアプローチを選択する必要があります。
3. **IT プロフェショナルは、ビジネス リスクと実装費用のバランスを取る必要があります。**これは難しいプロセスです。本ガイドが意図しているのは、IT プロフェショナルが、リスク管理プロセスを支援するためにマイクロソフトから利用可能なツール、サービスおよび情報を理解するのをお手伝いすることです。
4. **各自の組織に適するように、すべてのフレームワークおよびプロセスをカスタマイズする必要があります。**各組織の要件は異なるため、適宜これらの要件に合わせて計画し、カスタマイズしてください。

本ガイドは、マイクロソフトのセキュリティ リリースのフレームワークの段階をさらに検証するため、IT プロフェショナルは、各自の組織に最善の判断を下すためにマイクロソフトが提供した情報をどのように使用できるのかを確認できます。

組織でリスク管理のアプローチを導入していない場合、本ガイドの「ステージ 2: リスク評価」で、オプションを提供しています。

ステージ 1: マイクロソフトのセキュリティ リリースの通知を受け取る

本セクションの内容*:*

- IT プロフェッショナルが、すべての関係するマイクロソフトのセキュリティの通知を受け取っていることを確認する方法

本セクションを終了すると、*IT* プロフェッショナルは次の項目について理解します*:*

- すべてのマイクロソフトのセキュリティ リリースの通知を受け取っていること

本セクションにおけるマイクロソフトの参照リソース*:*

- **セキュリティ通知:** technet.microsoft.com/security/dd252948.aspx をご覧ください。
- **MSRC ブログ:** blogs.technet.com/msrc/ をご覧ください。
- **セキュリティ情報の事前通知サービス:** http://www.microsoft.com/japan/technet/security/bulletin/advance.mspx をご覧ください。
- **セキュリティ情報サマリー:** http://www.microsoft.com/japan/technet/security/bulletin/summary.mspx をご覧ください。
- **セキュリティ情報:** http://www.microsoft.com/japan/technet/security/current.aspx をご覧ください。
- **セキュリティ アドバイザリ:** http://www.microsoft.com/japan/technet/security/advisory/ をご覧ください。
- **TwC Security and Privacy Blogs:** www.microsoft.com/twc/blogs をご覧ください。

マイクロソフト セキュリティ リリースの通知

マイクロソフトは、お客様のセキュリティに影響する具体的な情報がある場合、通知を送信します。セキュリティの変更が必要な場合、マイクロソフトはサポートしている関連のセキュリティ情報、技術情報などと共に、セキュリティ更新プログラムをリリースします。そうでない場合でも、お客様のセキュリティに影響を及ぼす事柄について、マイクロソフトはいくつかの手段を利用して通知し (例: セキュリティ アドバイザリやブログの掲載)、それに沿ってガイダンスを提供します。

通常、マイクロソフトは毎月第 2 火曜日 10:00 AM (太平洋標準時) に、セキュリティ更新プログラムおよびセキュリティ情報を公開します。各組織が稼働するタイム ゾーンに応じて、IT プロフェショナルは、この公開スケジュールを地域の状況に合うよう調節する必要があります。セキュリティの問題があまりに深刻で、Windows ベースのコンピューターが重大なリスクに直面し、マイクロソフトが通常の月例リリ

ースのサイクル以外でセキュリティの変更が直ちに必要であると判断した場合、定例外でセキュリティ リリースを行います。

セキュリティ リリースが、セキュリティ アドバイザリ、標準的な月例のセキュリティ更新プログラム、または定例外の公開であるかに関わらず、マイクロソフトは特定の通知を利用します。組織のセキュリティ チームは、マイクロソフトのセキュリティ通知を受け取った後、どのセキュリティの問題と更新プログラムが組織に関係するかを判断し、組織が講じる必要のあるステップを計画できます。

マイクロソフトのセキュリティ リリースの通知を受信する

タイミング良く、確実に IT プロフェショナルがマイクロソフトのセキュリティの通知またはお知らせを受信するために、マイクロソフトは適切な IT サポート スタッフが少なくとも図 1 に示されているアラートに登録することを推奨します。

	通知	詳細
	包括的なセキュリティ アラート	無償の包括的なアラートは、公開予定のセキュリティ情報 (および関連のセキュリティ更新プログラム) の事前通知、セキュリティ アドバイザリ、および以前に公開されたマイクロソフトのセキュリティ情報またはセキュリティ アドバイザリに変更があった場合に、適時に通知を提供します。これらの通知は IT プロフェショナルのために作成され、詳細な技術情報が含まれており、電子メール メッセージは Pretty Good Privacy (PGP) でデジタル署名[5]されています。 • **電子メール:** マイクロソフト プロダクト セキュリティ警告サービス • **RSS:** セキュリティ情報 RSS • **Web サイト:** セキュリティ情報検索 http://www.microsoft.com/japan/technet/security/current.aspx 前述のリソースへアクセスする場合は、こちらをご覧ください: technet.microsoft.com/ja-jp/security/dd252948.aspx
	Microsoft Security Response Center (MSRC) ブログ アラート	MSRC ブログは MSRC が IT プロフェッショナルとコミュニケーションを取るためのリアルタイムの手段を提供します。MSRC は、IT プロフェショナルがマイクロソフトのセキュリティ レスポンスへの取り組み、セキュリティ インシデントの初期段階での更新プログラム、およびセキュリティ情報の公開サイクルにおける定例の投稿を理解するために役立てていただくため、このブログを利用して重要かつ実質的なセキュリティのコミュニケーションを広めています。 • **RSS:** MSRC Blog • **Windows Live Alert:** MSRC Blog • **Web サイト:** blogs.technet.com/msrc (英語情報)

[5] デジタル署名は英語版のみ行われています。

Trustworthy Computing Security and Privacy ブログ	このページは、マイクロソフトの信頼できるコンピューティング (TwC) グループによるブログを動的にまとめ、掲載しています。このチームは、より安全性が高く、プライバシーの確保された、信頼できるコンピューティング エクスペリエンスを提供するために取り組んでいます。マイクロソフトのコンピューティングのプライバシーおよびセキュリティに関する長期的な展望および戦略をご覧ください。 Trustworthy Computing Security and Privacy のブログの冒頭ページは次をご覧ください: www.microsoft.com/twc/blogs (英語情報)

表 1: セキュリティ アラートの登録

マイクロソフトにより、新たなセキュリティ リリースが利用可能になった場合、IT プロフェショナルが通知されたセキュリティの現象および脆弱性、各組織が受けるリスクを直ちに判断できることが重要です。本ガイドは、お客様のリスク管理のフレームワークに適用する、IT プロフェショナルに必要なプロセスおよび判断に関する詳細を提供します。

本ガイドのこのステージでは、マイクロソフトのセキュリティ更新プログラムおよびアドバザリのみに焦点を置いています。組織がいくつかの推奨策を、サービス パック、ドライバーの更新プログラムおよびその他の更新の種類向けの、メンテナンス更新プロセスに組み込むことも可能だと思います。

ステージ 2: リスクを評価する

本セクションの内容*:*

- マイクロソフトのリソースを、次の事項を決定するお客様のリスク管理フレームワークに適用します。
  - セキュリティ リリースで取り上げられた脆弱性が組織に該当するかどうか。
  - リスクがある場合、このセキュリティ リリースで取り上げた脆弱性は組織に影響を及ぼすかどうか。
- 脆弱性の適用およびリスクの判断に利用可能なマイクロソフトのリソース
- マイクロソフトのリソースを利用したリスク評価の例
- セキュリティ更新プログラムの適用前の追加の考慮点

本セクションの終わりに、*IT* プロフェショナルは次を理解できます。

- 主要なマイクロソフトのリソースを理解すると、各組織への脆弱性の適用性を判断できます。情報を収集するために使用されるマイクロソフトのリソースには次が含まれます。
  - マイクロソフト プロダクト サポート ライフ サイクル
  - セキュリティ情報、セキュリティ アドバイザリ、MSRC ブログ、Microsoft Security Research & Defense ブログ、および TechNet セキュリティ情報 Web キャスト
- 主要なマイクロソフトのリソースを理解すると、組織のリスク レベルを判断できます。これらには、次が含まれています。
  - セキュリティ情報およびセキュリティ アドバイザリ
  - セキュリティ情報およびマイクロソフト深刻度の評価システムおよびその他の脆弱性の影響に関する情報
  - 悪用可能性指数は、セキュリティ情報を適用しなかった場合の脆弱性のリスクを明記していします
- 次のような、現時点での組織のリスク管理のフレームワークに関連している、その他の重要な考慮点を理解します。
  - サポート技術情報の内容を確認する
  - セキュリティ更新プログラムのアンインストールの容易性および強制的な再起動が必要であるかどうかを評価する

本セクションにおけるマイクロソフトの参照リソース*:*

- **マイクロソフト セキュリティ リスク管理ガイド**
- 技術にとらわれないソリューションで、リスク管理に 4 段階のアプローチを提供します。このガイドは、セキュリティ リスクの管理について業界で認められた多くの標準を紹介しており、マイ

クロソフト IT の実体験を組み込み、さらにマイクロソフトのお客様およびパートナーからの情報が盛り込まれています。セキュリティ リスク管理ガイドをご覧ください。

-
- **マイクロソフト セキュリティ情報検索ページ**
- このページはセキュリティ情報に関する中心となるポータル サイトです。最新のマイクロソフト セキュリティ情報およびアドバイザリ、以前のセキュリティ情報の提供、セキュリティ情報およびサポート技術情報などの検索機能を提供しています。www.microsoft.com/japan/technet/security/current.aspx をご覧ください。
- **マイクロソフト プロダクト サポート ライフサイクル検索ページ** support.microsoft.com/lifecycle/search/ をご覧ください。
- **MSRC ブログ** blogs.technet.com/msrc/ (英語情報) をご覧ください。
- **Microsoft Security Research & Defense ブログ** blogs.technet.com/srd/ (英語情報) をご覧ください。
- **Microsoft Exploitability Index （悪用可能性指標）**

この指標は、IT プロフェショナルがセキュリティ更新プログラムの展開の優先順位を決定するのに役立ちます (technet.microsoft.com/ja-jp/security/cc998259.aspx をご覧ください)。悪用可能性指標は、各月のセキュリティ情報のサマリーに含まれています。www.microsoft.com/technet/security/bulletin/summary.mspx をご覧ください。

- **サポート技術情報** http://www.microsoft.com/japan/technet/security/current.aspx または support.microsoft.com/ で検索してください。

リスク管理のフレームワークにおける判断

紛れもなく、IT プロフェショナルがリスク管理のフレームワークで下す最も重大な判断のひとつは、新たに特定された脆弱性が組織にとってどのようなリスクであるかです。セキュリティ更新プログラムの展開は、テストや導入時の費用および発生する問題のサポート費用の両方について、固有の費用がかかります。IT プロフェショナルが下す必要のある判断は、この費用が、更新プログラム未適用のシステムから引き起こされる可能性のある攻撃により組織が直面するリスクを上回るかどうかです。図 8 では、リスクの段階を評価するために適切な情報およびそれに続く判断の詳細を説明しています。

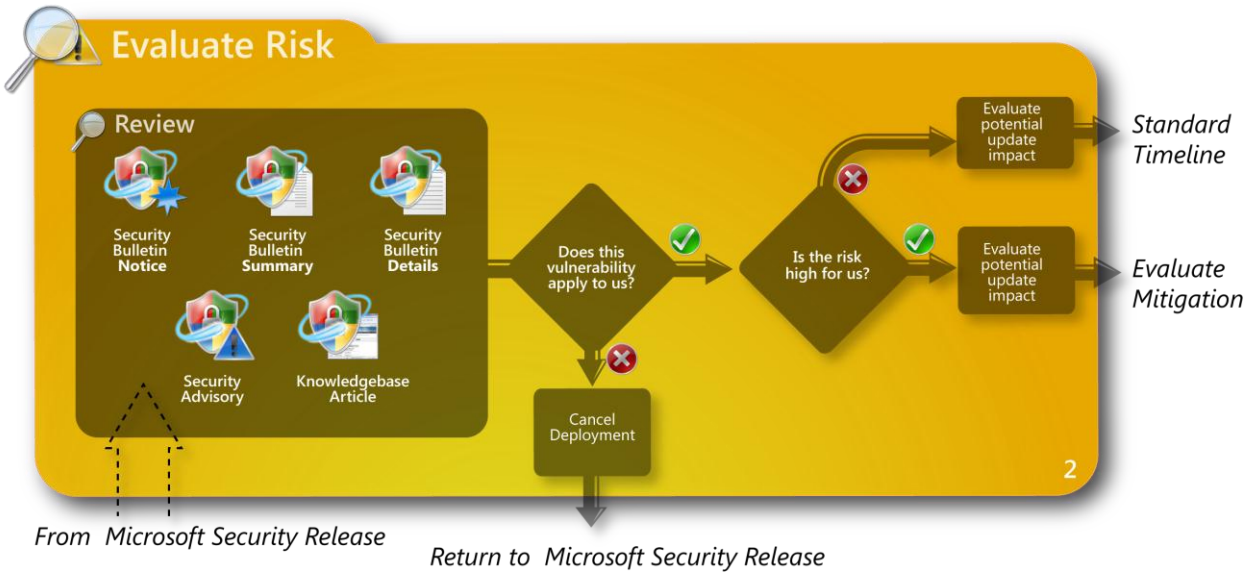


図 8 リスクの段階を評価する

みなさんの組織の既存のリスク管理プロセスは十分でしょうか? リスク管理のアプローチに関するガイダンスが必要な組織は、技術にとらわれないソリューションで、リスク管理に対して 4 段階のアプローチを提供しているマイクロソフトのセキュリティリスク管理ガイドを参照可能です。

このガイドは、あらゆるタイプの組織が、優れたセキュリティ リスク管理プログラムを計画、構築および維持するのに役立ちます。セキュリティ リスク管理ガイドは、セキュリティ リスクを評価し、許容可能なレベルにするため、リスク管理プログラムの各段階の処理方法および進行中のプロセスを構築する方法を説明しています。これは、セキュリティの権威である専門家チームが開発、確認して、認めたものです。このセキュリティ リスク管理ガイドと本ガイドを組み合わせることにより、IT プロフェショナルは、マイクロソフトがより優れたセキュリティ リスクの管理のために提供している多くのリソースについて、より理解を深めることができます。

マイクロソフト セキュリティ リスク管理ガイドについては、こちらをご覧ください: technet.microsoft.com/library/cc163143.aspx. technet.microsoft.com/ja-jp/library/cc163143.aspx

このステージにおける判断 図 8 に示されているように、IT プロフェショナルはこの段階で 2 つのことを特定する必要があります。

1. 脆弱性は組織に該当しますか? 別の言い方をすると、マイクロソフトのセキュリティ リリースで言及している脆弱性は、組織に該当しますか?
2. この脆弱性のリスクは組織にとって高いものですか? 別の言い方をすると、マイクロソフトのセキュリティ リリースで解決された脆弱性が組織に与えるリスクはどのようなものですか?

このステージでは、更新プログラムの展開前に適した、他の重要な考慮点を説明しています。

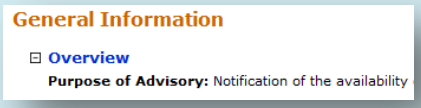
脆弱性が該当するかどうかを特定する

マイクロソフトのセキュリティ リリースの通知を受信後、お客様のリスク管理のフレームワークでリスクの段階を評価する際に最初に判断することは、脆弱性が組織に該当するかどうかです。詳細な情報を得た上で判断できるよう、本セクションでは、より詳細な情報を得た上で判断を下すために必要なセキュリティの情報を収集するためのマイクロソフトのリソースを紹介します。

セキュリティの脆弱性情報を収集する

IT プロフェショナルは、いくつかの重要な情報を収集、評価し、セキュリティ制御またはセキュリティ更新プログラムを適用する前に、組織がどのようなリスクにさらされるかを確実に判断することが必要です。マイクロソフトは、確実に組織が、IT のインフラストラクチャおよび組織全体のセキュリティにもたらす脆弱性のリスクを理解するため、いくつかの重要なコミュニケーションを利用します。図 2 では、その脆弱性が組織に該当するかどうかを正しく特定するために必要なセキュリティの情報を収集するために、従うことが推奨されているマイクロソフトのリソースに焦点を当てています。

判断	詳細
製品が影響を受けているか確認します。	マイクロソフトは、IT プロフェショナルに脆弱性の影響を受ける製品について、次のように通知します。 • **セキュリティ情報サマリー**の、「概要」のセクションでは、IT プロフェショナルに影響を受ける製品またはソフトウェアのファミリを通知します。例えば、Windows が「影響を受けるソフトウェア」のセクションの一覧にある場合、現在サポートされているすべての Windows のオペレーティング システムが影響を受けるということです。 ○ セキュリティ情報サマリーにより、IT プロフェショナルはセキュリティ情報および関連のセキュリティ更新プログラムを各組織に適用するかどうかを素早く評価できます。たとえば、IT プロフェショナルが Internet Explorer を**使用していない**場合には、、セキュリティ情報サマリーに Internet Explorer が「影響を受けるソフトウェア」として記載されていればサマリー、関連のセキュリティ情報およびセキュリティ更新プログラムを確認する必要はないのです。 • **セキュリティ情報**および**セキュリティ アドバイザリ**は、セキュリティ情報サマリーよりも「影響を受けるソフトウェアまたはソフトウェア」を具体的に特定します (例えば Windows の場合、その他のバージョンの Windows として、Windows XP Service Pack 3 が「影響を受けるソフトウェア」に記載されている可能性があります)。 **影響を受ける製品を確認するための情報源** • セキュリティ情報サマリーは、http://www.microsoft.com/japan/technet/security/bulletin/su

判断	詳細
	mmary.mspx をご覧ください。 • セキュリティ情報を確認にするには、http://www.microsoft.com/japan/technet/security/current.aspx をご覧ください。 • セキュリティ アドバイザリを確認するには、http://www.microsoft.com/japan/technet/security/advisory/ をご覧ください。 **影響を受ける製品およびコンポーネントを確認する。**セキュリティ情報またはセキュリティ アドバイザリの「影響を受けるソフトウェア」セクションで、より具体的な影響を受ける製品情報をご覧ください。 • 各セキュリティ情報では、影響を受けるソフトウェアの詳細を説明しています。影響を受けるソフトウェアおよび影響を受けないソフトウェア (例: 影響を受けるオペレーティング システム: Windows XP Service Pack 3, 影響を受けないソフトウェア: Windows Vista Service Pack 1)が含まれています。 • セキュリティ アドバイザリでは、「概要」のセクションに影響を受けるソフトウェアおよび影響を受けないソフトウェアの詳細を説明  しています (次のセキュリティ アドバイザリのサンプルを参照のこと) セキュリティ情報で、「緩和する要素」を特定するために役立つその他の情報源は、「脆弱性の詳細」セクションです。「脆弱性の詳細」セクションで、セキュリティ情報で解決している CVE 番号を展開し、「緩和する要素」を展開します。ここに追加情報が含まれています。 「影響を受けるソフトウェア」または「概要」セクションに製品が掲載されていない場合、この脆弱性は該当しておらず、セキュリティ更新プログラムまたは追加の対策は必要ありません。

判断	詳細
お使いのアプリケーションとオペレーティング システムのマイクロソフト サポート ライフサイクルを確認します。	組織では、マイクロソフトがすでにサポートを終了したソフトウェアのバージョンを実行している可能性があります。組織のリスク管理プロセスの一環として、IT プロフェショナルは IT 環境の製品がすでにサポートを終了しているかどうかを把握しておく必要があります。なぜなら、このような製品には組織のリスクを低減するために緩和する必要のある脆弱性が含まれている場合があるためです。 古いリリースのソフトウェアを所有している組織が、サポートされているリリースに移行して、脆弱性にさらされる可能性を防ぐことは、最優先であるべきです。これらのソフトウェア バージョンまたはエディションに関するセキュリティ更新プログラムのサポート期間の詳細情報は、support.microsoft.com/lifecycle/search/ をご覧いただき、マイクロソフトが製品をサポート中であるかどうかを確認してください。 マイクロソフトのセキュリティ情報に掲載されている「影響を受けるソフトウェア」は、互換性を確保するためにセキュリティ更新プログラムを検証しています。しかし、サポート ライフ サイクルが終了した古いソフトウェアのリリースは検証されていません。 追加情報は、support.microsoft.com/gp/LifeWinFAQ の Windows オペレーティング システム ライフサイクル FAQ をご覧ください。 古いマイクロソフト製品のカスタム サポートが必要な場合、各地域のマイクロソフトまでご連絡ください。あるいは、組織がアライアンス、プレミアまたは認定を受けた契約をお持ちの場合、各マイクロソフトのアカウント チームの代表、テクニカル アカウント マネージャーまたは担当のマイクロソフト パートナーの代表までカスタム サポート オプションについてお問い合わせください。地域のマイクロソフトのオフィスを確認するには、次のような方法があります。 1. www.microsoft.com/worldwide/ の Microsoft Worldwide に移動します。 2. 「連絡先の情報」の一覧は、各主要な業務地の近隣のオフィスを選択し、[Go] ボタンをクリックします。Web サイト、オフィスの住所および電話番号が表示されます。 3. 連絡をとる際には、地域のプレミア サポートのセールス マネージャーとお話ください

判断	詳細
MSRC ブログを確認します。	blogs.technet.com/msrc/ で、MSRC ブログを確認します。 The Microsoft Security Response Center (MSRC) Working to help protect customers from vulnerabilities in Microsoft software MSRC Microsoft Security Response Center 数ある中でも、MSRC が特に提供しているのは次の通りです。 • セキュリティ情報に含まれていない追加リソースおよびガイダンス • すべてのセキュリティ リリースに関連の重要な情報 • セキュリティ リリースに伴うすべての問題に関する情報 (例: 互換性の問題) • マイクロソフト製品に影響するインシデントまたは脆弱性に関する情報

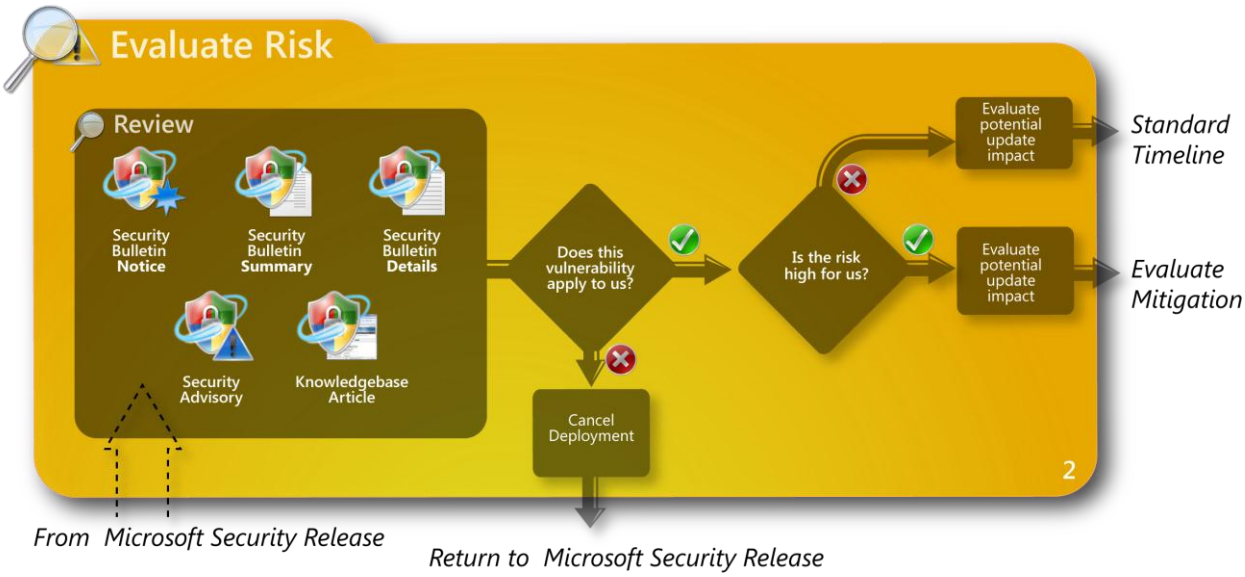
図 2 マイクロソフトのセキュリティ リリースの情報ソース

IT プロフェショナルはこの情報を収集および確認後、セキュリティの脆弱性が組織に該当するかどうかを確認する必要があります。

脆弱性リスクの判断

脆弱性が組織に該当すると IT プロフェショナルが確認後、下の図に示されているように、リスクを評価するのステージの次のステップで、組織の受けるリスクを特定する必要があります。

マイクロソフトのセキュリティの通知が、複数のセキュリティ問題に関する情報がある場合には、*IT* プロフェショナルは組織が受ける可能性のあるリスクについて、個々に各問題を確認する必要があります。



ハイリスクとは何でしょう？

常に、組織によって脆弱性のリスクが異なります。そして各組織は一般的に「ハイリスク」および「ローリスク」と考える限界点があり、その間に別の多くのリスク評価が含まれています。前述のとおり、マイクロソフトのセキュリティ リスク管理ガイドにより、IT プロフェショナルが組織内のリスク レベルを適切に判断できます。そのため、本ガイドの目的のために、お客様のリスク管理のフレームワークは 2 種類のリスクのレベル (ハイリスクおよびローリスク) を採用しています。さらに、各組織における分類の仕方は情報量 (その多くを下で説明しています) によります。重要な点は、IT プロフェショナルが最も深刻な脆弱性 (本ガイドでは”ハイリスク”として示しています) を最初に緩和することに焦点を置く必要があります。

マイクロソフトの深刻度評価システム

脆弱性の深刻度評価から生じるリスク評価の考慮にいれる最初の情報のひとつです。マイクロソフトは、マイクロソフト深刻度評価システムを使用して、脆弱性の深刻度を伝えます http://www.microsoft.com/japan/technet/security/bulletin/rating.mspx をご覧ください)。

マイクロソフトの深刻度評価システムの説明

マイクロソフトは、数種類の深刻度評価システムを確認しています。例えば、Common Vulnerability Scoring System (CVSS) の最新のバージョンである CVSSv2 は、2007 年に採用され、業界の全製品の脆弱性を評価します。深刻度の評価は、お客様の層で分類される複雑なプロセスです。従って、ひとつの評価ですべてのシナリオのお客様全員に対する脆弱性の本当のリスクを示すのは困難です。その結果、効果的な脆弱性の深刻度評価システムは脆弱性を過大評価も過小評価もしないものであるべきです。それは、大多数のお客様が正しくリスクを測定する手助けとなり、お客様に通知されたリスク評価を独自に評価可能なものです。

マイクロソフトは、脆弱性の深刻度の情報について主要なソースはお客様の必要性から生まれ、特に、ベンダーが製品を一番良く知っており、最も確かな情報に基づくガイダンスを提供可能なため製品のベンダーに提供されるべきものであると信じています。マイクロソフトはお客様に、緩和策、回避策のような信頼できるガイダンス、および予想される攻撃方法の説明を提供し、お客様独自のリスク分析や管理の実施を手助けします。マイクロソフト セキュリティ レスポンス センターは、お客様から、深刻度評価システムがお客様のリスク レベルの評価に役立てる中で、価値のあるものであるという報告が来ています。また、お客様はマイクロソフトに対し、マイクロソフト セキュリティ情報、アドバイザリおよびマイクロソフトの深刻度評価システムは、お客様のリスクレベルを評価するために価値があると話されています。マイクロソフトは、最悪のケースのシナリオを警戒して、脆弱性の深刻度の評価を、最大の深刻度を持つ「緊急」、「重要」、「警告」および「注意」のように評価しています。評価が境界線にある状況に対しては、マイクロソフトの経験では「最悪のケース」シナリオ側で警戒します。

深刻度評価の意味。簡単に言うと、マイクロソフトの深刻度評価は最も深刻な起こりうる攻撃の影響であると解釈されます。マイクロソフトは、各問題を評価し、問題の影響を既定の構成の技術的なレベルで客観的に計ります。この分析および最も深刻なセキュリティによる影響を基に、マイクロソフトはセキュリティ情報で深刻度評価を提供します。表 3 では、4 種類の深刻度評価および関連の影響について説明します。

評価	定義
緊急	この脆弱性が悪用された場合、インターネット ワームがユーザーの操作なしで蔓延する可能性があります。
重要	の脆弱性が悪用された場合、ユーザーのデータの機密性、完全性またはアベイラビリティが侵害される可能性があります。または、処理中のリソースの完全性またはアベイラビリティが侵害される可能性があります。
警告	この脆弱性が悪用された場合、既定の構成、監査または悪用が困難であることなどの要素により、悪用される可能性は大幅に緩和されます。
注意	この脆弱性の悪用は非常に困難です。または影響はわずかです。

表 3 マイクロソフト セキュリティ評価システム

この基準についての追加情報は、
http://www.microsoft.com/japan/technet/security/bulletin/rating.mspx をご覧ください。

最も深刻および総合的な深刻度の評価。注目すべき点は、セキュリティ情報はより詳細を提供する一方、セキュリティ情報サマリーは影響を受ける製品ファミリの最も深刻なセキュリティの深刻度をリストしているということです。例えば、Windows が影響を受けるソフトウェアの一覧にある場合、Windows XP Service Pack 2 が「緊急」、Windows Vista が「重要」の評価を受けます。セキュリティ情報サマリー

は、各セキュリティ情報の最大深刻度の評価は「緊急」で、 Windows に最大深刻度を適用します。このセキュリティ情報は、サポートされているバージョンの影響を受けるソフトウェア毎に、最大のセキュリティの影響および総合的な深刻度の評価を説明しています。例は、図 9 および 図 10 をご覧ください。

下の図 9 に示されているように、各マイクロソフト セキュリティ情報の「概説」のセクションには表が含まれ、セキュリティ情報が解決する各製品およびコンポーネント、最も深刻なセキュリティの影響、総合的な深刻度および更新プログラムによって置き替えられるセキュリティ情報が一覧になっています。

Affected and Non-Affected Software

The following software have been tested to determine which versions or editions are affected. Other versions or editions are either past their support life cycle or are not affected. To determine the support life cycle for your software version or edition, visit Microsoft Support Lifecycle.

Affected Software

Windows Operating System and Components

Operating System	Component	Maximum Security Impact	Aggregate Severity Rating	Bulletins Replaced by this Update
Microsoft Windows 2000 Service Pack 4 (KB923561)	Not applicable	Remote Code Execution	Important	None
Windows XP Service Pack 2 and Windows XP Service Pack 3 (KB923561)	Not applicable	Remote Code Execution	Important	None

図 9 マイクロソフト セキュリティ情報の総合的な深刻度

図 4 (下を参照) の別のリソースと共に、この深刻度評価は、より優れたリスク管理に使用可能なツールの情報を IT プロフェショナルに提供するために役立てられます。IT プロフェショナルの中には、セキュリティ更新プログラムが解決する脆弱性に関して、より詳細な技術情報が必要な場合があるため、各セキュリティ情報には、図 10 に示されているような「脆弱性の情報」というセクションに、脆弱性に関する詳細情報が含まれています。他の説明のうち、このセクションは (CVE 番号で特定した) 脆弱性、個々の脆弱性の深刻度評価および影響を受けるソフトウェアに対する最も深刻なセキュリティの影響を説明しています。

Vulnerability Information

Severity Ratings and Vulnerability Identifiers

The following severity ratings assume the potential maximum impact of the vulnerability. For information regarding the likelihood, within 30 days of this security bulletin's release, of the exploitability of the vulnerability in relation to its severity rating and security impact, please see the Exploitability Index in the April bulletin summary. For more information, see Microsoft Exploitability Index.

Vulnerability Severity Rating and Maximum Security Impact by Affected Software					
Affected Software	**WordPad and Office Text Converter Memory Corruption Vulnerability - CVE-2009-0087**	**WordPad Word 97 Text Converter Stack Overflow Vulnerability - CVE-2008-4841**	**Word 2000 WordPerfect 6.x Converter Stack Corruption Vulnerability - CVE-2009-0088**	**WordPad Word 97 Text Converter Stack Overflow Vulnerability - CVE-2009-0235**	**Aggregate Severity Rating**
Operating System and Components					
Microsoft Windows 2000 Service Pack 4	**Important** Remote Code Execution	**Important** Remote Code Execution	Not applicable	**Important** Remote Code Execution	**Important**

図 10 マイクロソフト セキュリティ情報の「脆弱性の詳細」

組織により異なるリスク。リスク管理のフレームワーク次の段階に移る前に、組織に関連しているリスクを明確に特定する方法でリスクを文書化しておくことが重要です。次のセクションでは、各組織に適用されるリスクを特定するためにカスタマイズされたリスク評価を作成するために IT プロフェショナルが使用可能なソースおよび情報を提供します。

リスク評価のリソース

表 4 は、IT プロフェショナルが、組織のリスク レベルを判断する際に役立つリスク管理のフレームワークの一環として考慮すべき、ステップとマイクロソフトのリソースを特定しています。

	リスク評価のステップ	詳細
	**マイクロソフトのセキュリティ リリースの一覧の「影響を受けるソフトウェア」が「リスクの高い」もので、解□決のために更新プログラムが作成されている脆弱性であるかどうかを判断します。**	すべての脆弱性がすべての IT 環境で同じ危険性になるということではありません。いくつかの脆弱性は構成や使用状況のシナリオに依存します。このステップでは、IT プロフェッショナルが実装されている脆弱性の発生する可能性がある組織内の製品またはサービスのインスタンスを特定する必要があります。 *例えば、あるセキュリティ更新プログラムは Active Server Pages (ASP) が有効にされたインターネット インフォメーション サービス (IIS) を実行しているすべての Windows Server のオペレーティング システム向けに設計されたとします。組織には、Windows Server オペレーティング システムがいくつかあり*

	リスク評価のステップ	詳細
		ますが、組織がすべての *IIS* サーバーで *ASP* を有効にしていない場合、このセキュリティ更新プログラムは該当しません。 IT プロフェショナルは、セキュリティ情報の「影響を受けるソフトウェア」および「影響を受けないソフトウェア」のセクションを確認する必要があります。その後、脆弱性の悪用の深刻度を低減する「緩和する要素」および関連のコンテンツが含まれている「脆弱性の情報」の CVE 番号のエントリを読みます。
	該当するセキュリティ情報の追加の技術情報については、Microsoft Security Research & Defense ブログを確認します。	Review the Microsoft Security Research & Defense ブログはこちらをご覧ください: blogs.technet.com/srd/ (英語情報)  Microsoft Security Research & Defense ブログには、特定のセキュリティ情報、セキュリティ更新プログラムおよびセキュリティ アドバイザリに関する情報が含まれています。これには、セキュリティ情報またはアドバイザリに含まれていない脆弱性に関する追加の技術情報または活発な攻撃、追加の緩和策および回避策、そして IT プロのリスク管理を支援するためにその他の注意が含まれる場合があります。 Security Research & Defense blog のブロガーはマイクロソフトの社員で、マイクロソフトの脆弱性の報告に関する詳細な技術分析、新たな脆弱性の調査および研究、セキュリティ情報に技術的なガイダンスを提供し、セキュリティ更新プログラムが確実に効果的にソフトウェアの脆弱性を排除させます。
	インタラクティブな TechNet セキュリティ情報の Web キャストに参加、閲覧します。	近日公開、または以前の TechNet セキュリティ情報の Webcast はこちらをご覧ください: www.microsoft.com/technet/security/bulletin/summary.mspx (英語情報) セキュリティ情報の公開と共に、マイクロソフトは、セキュリティ更新プログラムの公開から 25 時間後に開始する 1 時間のセキュリティ情報の Web キャストをホストします。このセッションは、マイクロソフトのセキュリティ問題の専門家がホストし、最新のセキュリティ情報に関する技術的な概要から始まります。対話的な質疑応答オンライン フォーラムで、お客様の質問や懸念を解決するため、多くの時間を費やします。

リスク評価のステップ	詳細
	IT プロフェショナルで、これらのライブの Web キャストに参加できない場合、または後で資料を確認したい場合は、マイクロソフトが定期的に掲載している blogs.technet.com/msrc/archive/tags/Security+Update+Webcast+Q_2600_amp_3B00_A/default.aspx の MSRC ブログのセキュリティ情報の Web キャストの質疑応答のスクリプトをご確認ください。
に更新プログラムを適用する前に、脆弱性の影響を受けた場合の組織の負担費用を確認します。	セキュリティ更新プログラムを適用しないことに関してリスクがあることを理解することが重要です。特定された脆弱性がセキュリティの悪用または IT プロフェショナルがセキュリティ更新プログラム (標準的な更新プログラムのプロセスの一環として) をインストールする前にシステムの不安定を引き起こす場合、業務上にどのような影響があるか、その可能性を理解する必要があります。IT プロフェショナルは「更新プログラムを適用していない」システムに対する攻撃の影響の可能性を基に、リクエストの変更に優先順位をつける必要があります。 脆弱性によるセキュリティ上の最大の影響を説明している、セキュリティ情報の「脆弱性の詳細」のセクションを確認します。 Microsoft Security Bulletin MS09-010 - Critical Vulnerabilities in WordPad and Office Text Converters Could Allow Remote Code Execution (960477) Published: April 14, 2009 | Updated: April 16, 2009 **Version:** 1.1 **Vulnerability Information** **Severity Ratings and Vulnerability Identifiers** The following severity ratings assume the potential maximum impact of the vulnerability. For information regarding the li days of this security bulletin's release, of the exploitability of the vulnerability in relation to its severity rating and securit the Exploitability Index in the April bulletin summary. For more information, see Microsoft Exploitability Index. **Vulnerability Severity Rating and Maximum Security Impact by Affected Software** Affected Software | WordPad and Office Text Converter Memory Corruption Vulnerability - CVE-2009-0087 | WordPad Word 97 Text Converter Stack Overflow Vulnerability - CVE-2008-4841 | Word 2000 WordPerfect 6.x Converter Stack Corruption Vulnerability - CVE-2009-0088 | WordPad Word 97 Text Converter Stack Overflow Vulnerability - CVE-2009-0235 | Aggregate Severity Rating その後、「脆弱性の詳細」の下のセクションの、セキュリティ情報で説明されている各脆弱性に関する「よく寄せられる質問」を読んでください。通常、MSRC は最も深刻なセキュリティの影響について、最初に FAQ 「どのようなことが起こる可能性がありますか?」で解決します。

	リスク評価のステップ	詳細
	脆弱性に対して作成された悪用コードの機能する可能性を考慮します。	悪用コードは、ソフトウェア プログラムまたはサンプル コードで、影響を受けるシステムに対して実行された場合、脆弱性を悪用して攻撃者の身元のなりすまし、ユーザーまたはシステム情報の改ざん、攻撃者の実行への関与の否定、ユーザーまたはシステム情報の漏えい、正規ユーザーへのサービス拒否または攻撃者に特権の昇格を行います。 悪用コードを機能させると、悪用コードが脆弱性に対して最大のセキュリティの影響を起こす可能性あります。例えば、リモートでコードが実行されるセキュリティの影響が脆弱性にある場合、悪用コードを実行すると標的のシステムに対して実行された際に、リモートでコードが実行可能です。 Microsoft Exploitability Index (悪用可能性指標) は追加情報を提供して、IT プロフェショナルがマイクロソフトのセキュリティ更新プログラムの展開の優先順位を効果的につける手助けをします。このインデックスは、IT プロフェショナルに公開から 30 日以内でマイクロソフトのセキュリティ更新プログラムで解決した脆弱性を標的にして、作成した悪用コードが実行される可能性に関して、ガイダンスを提供します。 作成された悪用コード実行の可能性が高い脆弱性は、優先的に展開する必要があります。「注意事項」のセクションでは、マイクロソフトはセキュリティ情報の脆弱性が現在インターネット上で悪用されているかの有無について説明しています。 Exploitability Index (悪用可能性指標) は、"Exploitability Index" セクションの下のセキュリティ情報サマリーにあります。 Exploitability Index (悪用可能性指標) の詳細情報は、technet.microsoft.com/security/cc998259.aspx をご覧ください。
	これは定例外のセキュリティ更新プログラムですか?	危機的な状況によっては、お客様が重大なリスクに直面すると想定され、高品質な更新プログラムを直ちに開発および公開可能である場合、マイクロソフトは定例外のセキュリティ更新プログラム (標準的なマイクロソフトのセキュリティ更新プログラムのリリース サイクルに固執しないセキュリティ更新プログラムの公開) を公開します。 定例外のセキュリティ更新プログラムは、まれなことで予定されたものではな

	リスク評価のステップ	詳細
		いため、ハイリスクの可能性として特別な配慮および注意が必要です。 IT プロフェショナルが確実に定例外のマイクロソフトのセキュリティ更新プログラムについて通知を受けるため、前のセクション「ステージ 1: マイクロソフトのセキュリティ リリースを受け取る」をご覧ください。さらに、IT プロフェショナルがマイクロソフトのセキュリティ更新プログラムが定例外または月例のセキュリティ更新プログラムのプロセスで定期的に配布されるものであるかどうか確実でない場合、MSRC ブログ (blogs.technet.com/msrc/) または、日本のセキュリティチームのブログ (blogs.technet.com/b/jpsecurity/) で、リアルタイムの情報を確認できます。
	「推奨するアクション」のセクションを検討します。	セキュリティ アドバイザリは多くの場合、製品にセキュリティの変更を強制するバイナリを含んでいないため、これは主にセキュリティ アドバイザリに関連します。この結果、IT プロフェッショナルがマイクロソフト セキュリティ アドバイザリを受け取った際、マイクロソフトは IT プロフェッショナルに「推奨するアクション」のセクションを検討し、適切なアクションを行うことを推奨します。

表 4: リスク評価のステップ

上記の表からのすべてのセキュリティに関する情報を組み合わせると、IT プロフェッショナルがリスクのスナップショットを組み立てるのに役立ちます。これは下記のようなものになると考えられます。

CVE 識別子	マイクロソフトの深刻度	Exploitability Index	コメント	備考
CVE-20YY-XXXX	緊急	1	安定した悪用コードの可能性。リモートでコードが実行される可能性 (RCE)	イン ザ ワイルドでの現在の悪用
CVE-20YY-XXXX	緊急	1	安定した悪用コードの可能性。RCE の可能性	責任ある態度での公開
CVE-20YY-XXXX	緊急	1	安定した悪用コードの可能性。RCE の可能性	責任ある態度での公開
影響を受ける製品	Windows XP SP2、Windows SP3、Windows Server 2003 SP2			
影響を受けるコンポーネント	DirectX® 7、DirectX 8.1、DirectX 9.0/9.0a/9.0b/9.0c			
考えられる攻撃の方法	• 特別な細工がされた Quick Time ファイルを開く、または特別な細工がされたストリーミング コンテンツ、または Web コンテンツを配信するアプリケーションを Web サイトから受け取る • コンテンツは電子メールで送信されるか、または Web サイトでホストされている可能性があります。 • ネットワーク共有でホストされているコンテンツ。ファイルにマウスポインターをのせるだけでクラッシュが発生する可能性があります。			
攻撃の影響	攻撃者はログオン ユーザーと同じ権限を取得する可能性があります。攻撃者は次にプログラムのインストール、データの表示、変更、削除、または完全なユーザー権限を持つ新規アカウントの作成を行う可能性があります。			
問題を緩和する要素	• 攻撃者がユーザーに強制的に特別な細工がされた Web サイトを訪問させる、または特別な細工がされたファイルを開かせる方法はないと考えられます。 • すべてのサポートされているバージョンの Windows Vista および Windows Server 2008 は影響を受けません。			
追加情報	このセキュリティ更新プログラムは、マイクロソフト セキュリティ アドバイザリ XXXXXX の問題を解決します。			

表 5: リスク評価のサンプル

その他のアプローチは?

もちろん、セキュリティ上の脆弱性によるリスクを評価するためのアプローチはたくさんあります。例として、脆弱性によるリスクを確認するために必要な分析を上記のレベルで行うことは骨が折れ、非生産的であると感じ、このため、これらのステップすべてを飛ばし、すべての更新プログラムを同等な扱いにする方が価値があると考える企業もあります。組織は次の段階、またはセキュリティ更新プログラム パッケージの作成、テスト、適用にまで進む可能性もあります。。

例: マイクロソフトのガイダンスを適用してリスクを評価する

次のセクションは、(マイクロソフト セキュリティ アドバイザリではなく) マイクロソフトのセキュリティ更新プログラムにのみ該当します。(アドバイザリにはこの情報が含まれていません。) 次のステップは IT プロフェッショナルが対策やセキュリティ更新プログラムの適用を実施する前に組織が直面する可能性のあるリスクに影響を及ぼす可能性のある要素を確認する手助けとなります。この例で、ある月に MSRC が 5 つの新しいセキュリティ情報 (それぞれの深刻度は表 6 に記載しています) を公開したとします。

セキュリティ情報	脆弱性識別子	マイクロソフトの深刻度	リスク評価
MSYY-001	CVE-20YY-AAAA	緊急	…
MSYY-002	CVE-20YY-BBBB	緊急	…
MSYY-003	CVE-20YY-CCCC	重要	…
MSYY-004	CVE-20YY-DDDD	警告	…
MSYY-005	CVE-20YY-EEEE	緊急	…

表 6: 深刻度評価システムの例

マイクロソフト セキュリティ情報の深刻度評価は最悪の場合の攻撃のシナリオを前提としています。この情報に基づき、このように IT プロフェッショナルはこれらのセキュリティ更新プログラムに優先度をつけることができます。

- 緊急の更新タイムライン: MSYY-001、MSYY-002、MSYY-005
- 標準の更新タイムライン: MSYY-003,MSYY-004

例: 情報を使用してリスク評価を確認する

表 7 は Exploitability Index (悪用指標表) の評価を適用した結果を示しています。

セキュリティ情報	脆弱性識別子	Exploitability Index	マイクロソフトの深刻度評価	リスク評価
MSYY-001	CVE-20YY-AAAA	1 - 安定した悪用コードの可能性	緊急	…
MSYY-002	CVE-20YY-BBBB	1 - 安定した悪用コードの可能性	緊急	…
MSYY-003	CVE-20YY-CCCC	1 - 安定した悪用コードの可能性	重要	…
MSYY-004	CVE-20YY-DDDD	2 - 不安定な悪用コードの可能性	警告	…
MSYY-005	CVE-20YY-EEEE	3 - 機能する見込みのない悪用コード	注意	…

表 7: Exploitability Index (悪用指標表) の例

さらに、上記の表 4 に記載しているその他の考慮点はここでも該当する場合があります。たとえば、MSYY-001 が Microsoft Office Visio® (2002 SP2、2003 SP3 および 2007 SP1) で「リモートでコードが実行される」脆弱性についてで、この組織はこのセキュリティ情報では「影響を受けないソフトウェア」とされている Microsoft Office Visio Viewer のみを使用しているとします。この場合、セキュリティ更新プログラム MSYY-001 は該当しないため、IT プロフェッショナルはこのセキュリティ更新プログラムを適用しません。(表 8 参照のこと) このため、IT プロフェッショナルはこの追加情報をリスク評価の際に考慮し、リスク評価に異なる優先度を選択する可能性があります。

セキュリティ情報	脆弱性識別子	Exploitability Index	マイクロソフトの深刻度評価	リスク評価
~~MSYY-001~~	~~CVE-20YY-AAAA~~	~~1 - 安定した悪用コードの可能性~~	~~緊急~~	~~高~~
MSYY-002	CVE-20YY-BBBB	1 - 安定した悪用コードの可能性	緊急	高
MSYY-003	CVE-20YY-CCCC	1 - 安定した悪用コードの可能性	重要	高
MSYY-004	CVE-20YY-DDDD	2 - 不安定な悪用コードの可能性	警告	低
MSYY-005	CVE-20YY-EEEE	3 - 機能する見込みのない悪用コード	緊急	低

表 8: リスク評価システムの例

お客様が影響を受けるソフトウェアを所有していないため、MSYY-001 が評価から削除されていることが変更点です。また、MSYY-005 は深刻度が「緊急」であったため、最初に優先度「高」と評価されました

が、現在ではその優先度が下げられています。逆に、MSYY-003 は以前は優先度「低」でしたが、現在ではその優先度が上げられています。これらのケースで、変更は表 4 のステップで提供されている追加情報を反映しています。ここで、Exploitability Index が役に立ちます。MSYY-003 は MSYY-005 よりも深刻度が低い (緊急に対し重要) のですが、実際は MSYY-003 には安定した悪用コードがあると考えられるため、その全体の優先度は高くなります。逆に、MSYY-005 には安定した悪用コードはないと考えられるため、全体の優先度は低くなります。

このレビューの結果により、セキュリティの公開が組織にとってリスクが低い場合、更新プログラムを標準の更新プロセスに渡し、必要なテストおよび変更のリクエスト プロセスの完了時に適用することができます。このガイドで、後ほどこれらの段階を詳しく説明します。

更新プログラム適用に関する考慮点

IT プロフェッショナルのリスク管理のフレームワークの「リスクを評価する」段階にいくつかの最終的な考慮点があります。セキュリティ更新プログラムが適用について最終的な許可を受ける前に、そのセキュリティ更新プログラムが既存のインフラストラクチャに問題を導入する可能性がないことを確認するためのその他の考慮点があります。これらの要素はセキュリティ更新プログラムの割り当てられたリスク評価には影響を及ぼしません。しかし、IT プロフェッショナルは運用環境でコンピューターやサービスでの影響の可能性を検討する際、これらの要素を考慮することが重要です。変更のリクエストのカテゴリを確立するために、IT プロフェッショナルは、表 9 に記載されているいくつかの追加の考慮点を検討する必要があります。

セキュリティ更新プログラムの展開の考慮点	詳細
展開を遅らせる、または複雑にする可能性のある更新プログラムに関する既知の問題や悪影響があるかどうかを確認します。	マイクロソフトはすべてのセキュリティ更新プログラムを広範なリサーチ、開発およびテスト プロセスの対象としています。セキュリティ更新プログラムは適切な品質のレベルに達した場合のみ、公開されます。しかし、リスク評価プロセスの一部として、多くの場合管理者は既知の問題の確認を望みます。 セキュリティ情報の上部にある「概説」の「既存の問題」のセクションを確認してください。通常、問題がある場合、support.microsoft.com で、そのセキュリティ情報に関連するサポート技術情報を紹介しています。 IT プロフェッショナルは www.microsoft.com/japan/technet/security/current.aspx で「サポート技術情報 (KB) から検索」を使用してサポート技術情報を検索することもできます。 サポート技術情報はすべてのセキュリティ情報およびアドバイザリに付随しています。これらのセキュリティ情報では、セキュリティ更新プログラムに関する警告または問題が記載されており、また、サポート エンジニアがお客様からの一般的な懸念をあげています。
セキュリティ更新プログラムが必要なコンピューターの台数とそれらのコンピューターが持つロール (つまり、企業にとっての重要度) を確認します。	ここでの重要な要素は、影響を受けているコンピューターの台数ではなく、企業にとってこれらのコンピューターがどの程度重要であるかです。主な資産がセキュリティ更新プログラムを最初に受け取るようにする必要があります。 その他の考慮点の中で特にこの質問に答えることにより、特定の重要なビジネス システムのユーザーが知覚できる影響を少なくし、更新サーバーに負荷を与える可能性に加え、ネットワーク帯域への影響の可能性を確認する手助けとなります。
更新プログラムのサイズがネットワークのインフラストラクチャに影響を及ぼす可能性があるかどうかを確認します。	大規模なソフトウェアの更新を同時に多数のコンピューターに適用すると、ネットワークのパフォーマンスが低下し、ネットワークの適切な操作に悪影響を及ぼす可能性があります。IT プロフェッショナルはすべての更新プログラムの説明を綿密に検討し、常にセキュリティ更新プログラムのサイズおよびその更新プログラムを受け取るコンピューターの台数を確認している必要があります。この情報もまた適切なリリースのス

	セキュリティ更新プログラムの展開の考慮点	詳細
		ケジュールを支援します。 IT プロフェッショナルはセキュリティ更新プログラムのファイルのサイズを catalog.update.microsoft.com の Microsoft Update カタログ サービスを使用して確認することができます。
	更新プログラム展開の妨げとなる可能性のある企業の祝日や行事があるかどうかを確認します。	悪意のあるソフトウェアの開発者は、悪用の前にコンピューターに更新プログラムが適用されていない可能性を最大限にするために、主な祝日の前のリリースを標的とし始めていることが調査で確認されています。この理由から、IT プロフェッショナルは通常は祝日である期間でも、リスクの高い適用をエスカレートできる必要があります。
	更新プログラムを展開するための、またはユーザーに展開中に発生する可能性のある問題に対応するための十分なリソースを確保します。	IT プロフェッショナルは展開チームの最新の状況をチェックし、必要なスタッフが招集でき、更新プログラムの展開が必要とされるタイムライン内で確実に完了できるようにする必要があります。
	すべての対象となるコンピューターに更新プログラムを展開するために必要となる適用方法を確認します。	更新プログラムの範囲により、IT プロフェッショナルは組織のすべてのコンピューターに更新プログラムを展開するために様々な方法が必要になる場合があります。たとえば、ある IT プロフェッショナルはサービスの混乱を最小限に抑えるようにするために、ミッション クリティカルなサーバーは手動のプロセスで更新することに決定するかもしれません。その他の IT プロフェッショナルはクライアント コンピューターは WSUS を使用する自動化された展開プロセスにより更新しようと決定するかもしれません。すべての必要な方法をこの段階で決定し、確実に更新プロセスの実際の影響を評価することが重要です。 **注:** 組織の包括的なセキュリティ更新プログラムへのアプローチは既にこの決定の多くを網羅している必要があります。しかし、展開前にこのステップを再度検討することは依然として有益です。
	更新プログラムの適用をサポートするためにその他の変更が必要と	たとえば、セキュリティ更新プログラムが適用できるのは最新のサービス パックにのみで、そのサービス パックが特定の運用システムにインストールされていない場合、特定のセキュリティ上の脆弱性に対し、この

	セキュリティ更新プログラムの展開の考慮点	詳細
	なるか?	ようなコンピューターを保護できない可能性があります。この場合、サービス パックとソフトウェアの更新プログラムの両方とも適用する必要があるため、変更のリクエストの影響とカテゴリはさらに重要になります。
	更新プログラムのインストール後に、その更新プログラムをアンインストールできるか?	これは後ほどさらに詳しく説明しますが、更新プログラムを評価する際に、その更新プログラムにテスト中に確認されなかった問題が存在した場合、容易にアンインストールできるかどうかを確認してください。更新プログラムをアンインストールする機能は、完全に自動化されたアンインストールのサポートから手動のアンインストールの手順、アンインストール不可に至るまで様々です。更新プログラムがアンインストールできない場合、最新のバックアップからコンピューターを復元することが唯一のオプションとなる場合があります。更新プログラムに必要なアンインストールの方法に関わらず、IT プロフェッショナルは、展開がテスト環境で得られた結果と一致しない場合、明確なロールバック プランを用意しておく必要があります。 IT プロフェッショナルは更新されるすべてのコンピューターの最新のバックアップがあること、また更新プログラムの削除が正常に行われない場合に、これらのコンピューターが復元できることを確認することを望むでしょう。更新プログラムが原因で、コンピューターが完全にエラーとなり、コンピューターをバックアップから復元する必要がある状態となることはほとんど考えられませんが、これは IT プロフェッショナルが対応の準備をする必要のある状況です。

セキュリティ更新プログラムの展開の考慮点	詳細
	マイクロソフトは各セキュリティ情報でセキュリティ更新プログラムの削除に関する情報を提供しています。セキュリティ情報の「展開に関する情報」のセクションで、関連するソフトウェアの表の「更新プログラムの削除」の欄を確認してください。 www.microsoft.com/japan/technet/security/current.aspx をご覧ください。
コンピューターまたはサービスの稼働時間にはどのような影響がありますか?	更新プログラムのインストール中、特定のサービスを停止、一時停止または終了する必要はありますか? コンピューターは更新の後に再起動する必要はありますか? 再起動の必要がある場合、組織の重要なサービスは影響を受けますか? またはインストール中にエンド ユーザーはコンピューターで作業できなくなりますか?

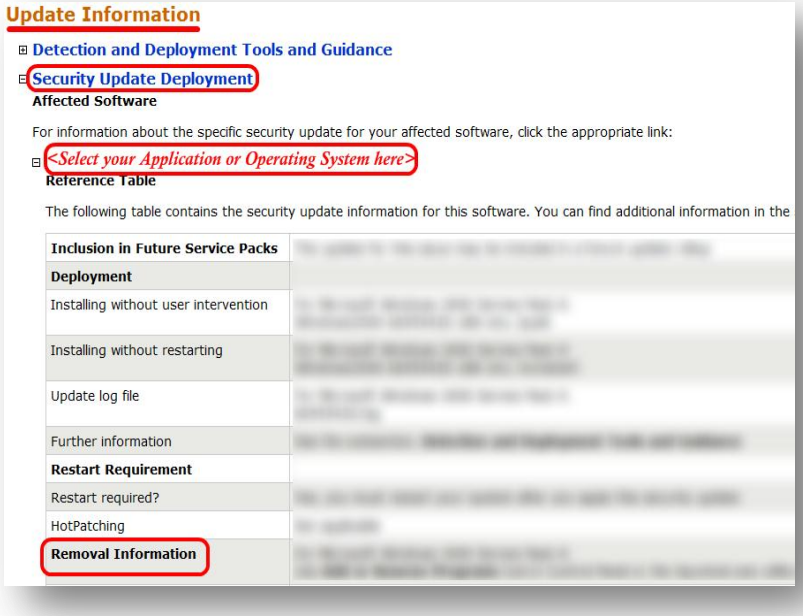


表 9: セキュリティ更新プログラムの展開についての考慮点

IT プロフェッショナルが脆弱性の技術的な詳細を明確に定義することも重要です。具体的には、IT プロフェッショナルは影響を受けるオペレーティング システム、サーバーの役割、機能、サービスおよびアプ

リケーションを明らかにする必要があります。システム管理チームはこの情報を使用して、組織での正確な展開プランを決定することができます。

IT プロフェッショナルはこれらのステップすべてをしっかりと考慮した後、リリースされた更新プログラムを展開する必要があるかどうかを決定することができます。この時点で、IT プロフェッショナルはすべてのコンピューターについて標準の更新タイムラインに従うべきかどうか、または組織にとってその展開を緊急の更新タイムラインにエスカレートするほど深刻なものであるかどうかを決定できるはずです。(これらのタイムラインは両方ともこのガイドのステージ 4 で説明しています。) 展開のステージはしばらく時間を要する可能性があるため、マイクロソフトは IT プロフェッショナルに短期的な緩和策のオプションを検討することを推奨します。これは次のステージのお客様のリスク管理のフレームワークで説明しています。

ステージ 3: 緩和策を評価する

本セクションの内容*:*

- 短期的な防御に適している緩和策および回避策
- このプログラムはセキュリティ更新プログラム展開中に高度な防御を提供します。

本セクションを終了すると、*IT* プロフェッショナルは次の項目について理解します*:*

- 緩和策と回避策の相違点を理解する
    - このガイドの目的に関して、緩和策とは脆弱性による危険を低減するためネットワークまたはコンピューターのレベルで行われるステップです。回避策とは、ユーザー レベルでの動作における変更です
    - マイクロソフト セキュリティ情報およびセキュリティ アドバイザリは緩和策を、脆弱性の悪用の深刻度を低減する可能性のある (既定の状態で存在する) 設定、一般的な構成または一般的な最善策としています。
    - マイクロソフト セキュリティ情報およびセキュリティ アドバイザリは回避策を根本的な脆弱性を修正するものではありませんが、更新プログラムを展開するまで、既知の攻撃の方法を阻止する手助けとなるものとしています。
- 短期的な緩和策を実施するかどうかを決定する手助けとなるマイクロソフトのリソースを見つけます。
- 緩和策および回避策が短期的な防御であり、これらはセキュリティ更新プログラムの展開の代わりになるものではないことを理解します。
- マイクロソフトのセキュリティ更新プログラムを展開する一方で、MAPP パートナーの Web ページをチェックし、MAPP メンバーが更新版の保護を提供しているかどうかを確認します。
- マイクロソフトのセキュリティ更新プログラムを展開した後、これらの短期的な緩和策を削除する必要がある場合があることに留意します。

本セクションにおけるマイクロソフトの参照リソース*:*

- **マイクロソフト セキュリティ情報 (緩和策および回避策):** 緩和策および回避策に関する情報は、www.microsoft.com/japan/technet/security/current.aspx をご覧ください。緩和策および回避策の情報は各セキュリティ情報の「脆弱性の詳細」のセクションをご覧ください。
- **マイクロソフト セキュリティ アドバイザリ: 緩和策および回避策に関する情報は、セキュリティ アドバイザリ** www.microsoft.com/japan/technet/security/advisory/default.mspx をご覧ください。
- **Microsoft Active Protections Program (MAPP) パートナーに関する Web ページ :** www.microsoft.com/security/msrc/collaboration/mapppartners.aspx (英語情報) でセキュ

リティ ソフトウェア ベンダーから有効な保護が利用可能となっているかどうかを確認してください。

- **Microsoft Security Research & Defense ブログ:** このブログは緩和策および回避策に関する追加情報を紹介している場合もあります。blogs.technet.com/srd/（英語情報）**をご覧ください。**

実行可能な短期的なセキュリティ制御

このガイドの目的に関して、緩和策とは脆弱性によるリスクを低減するためにネットワークまたはコンピューターのレベルで行われるステップです。回避策とは、ユーザー レベルでの動作の変更です。

短期的な防御を実装する: IT プロフェッショナルがセキュリティに関する通知をマイクロソフトから受け取り、リスク分析を行っている間、彼らの多くが攻撃を防ぐ手助けとなる防御を実装することを選択します。リスク評価と緊急性により、緊急の更新プロセスを介し影響を受けるコンピューターにセキュリティ更新プログラムを展開する組織もあるでしょう。(これは後ほど説明します。) しかし、多くの場合、実行可能な短期的なソリューションを実装することが考えられます。これにより、標準の更新プロセスを介し詳細なリスク分析を行い、セキュリティ更新プログラムを展開する時間が IT プロフェッショナルにさらに提供されます。たとえば、(組織でのコンピューターの運用にとって重要でない) 特定のポート番号を使用するサービスで脆弱性が確認された場合、短期的なコンピューターのファイアウォールのポリシーに変更を行うことが容易な場合があります。この緩和策は IT プロフェッショナルを短期的に保護するソリューションを提供し、彼らがセキュリティ更新プログラムを十分に展開する前に、さらに徹底的にリスク管理を行う時間を提供することができます。

マイクロソフト セキュリティ アドバイザリなどのその他のケースでは、セキュリティ更新プログラムが利用可能でない場合が多くあります。このため、適切な短期的な防御は、マイクロソフト セキュリティ アドバイザリで説明されている推奨される回避策に従うことです。

緩和策および回避策がセキュリティ更新プログラムの代わりとなることは決してない: セキュリティ情報で特定の脆弱性についての問題を緩和する要素や回避策を提供することの目的は、IT プロフェッショナルに直ちに、つまり、広範囲に展開される前に、セキュリティ更新プログラムが適切なテストを受けている間、環境を保護するために使用できるオプションを提供することです。問題を緩和する要素の情報がセキュリティ更新プログラムを適用しないことを正当化するものではないのと同様に、回避策の情報は適切なセキュリティ更新プログラムが適用される前の暫定的な対策として提供されています。このため、問題を緩和する要素はリスク評価と適用プロセスおよび手順の両方に密接に関連しているものとみる必要があります。

マイクロソフトは問題を緩和する要素と回避策を提供している: 脆弱性の調査報告のプロセスの一部として、マイクロソフトはセキュリティ更新プログラムが対応する脆弱性が悪用されることを防ぐ手助けとなる問題を緩和する要素と回避策の両方を確認しています。マイクロソフトは特定の脆弱性について実行可能な問題を緩和する要素や回避策を確認している場合、これらの情報をセキュリティ情報の「脆弱性の詳細」のセクションに記載しています。マイクロソフトが実行可能な問題を緩和する要素や回避策を確認できなかった場合、その旨を記載しています。同様に、回避策の情報はセキュリティ アドバイザリの「推奨されるアクション」に記載しています。

IT プロフェッショナルは、環境に対し高いリスクがあると特定された問題について、直ちに緩和策および回避策を実装することを検討し、セキュリティ更新プログラムが適用されている間によりよい保護が提供できるようにする必要があります。緩和策や回避策が利用可能でない問題については、更新プログラムの展開の優先順位が高くなる場合があります。図 11 は、組織における短期的な緩和策 (または回避策) の評価および展開を行うために使用できるステップの概要を示しています。

図 *11:* 緩和策のステージを評価する

緩和策を評価する段階での唯一の考慮点は、セキュリティ更新プログラムの展開よりも迅速に、効果のある短期的な緩和策を実装することができるかどうかです。使用できる短期的な緩和策が存在する場合、可能な限り迅速にそれを文書化し実装する必要があります。緩和策の使用ができるかどうかを確認するために、IT プロフェッショナルは表 10 に記載されているリソースを使用することができます。

	緩和策の評価のリソース	**詳細**
	セキュリティ情報またはアドバイザリを検討し、組織で短期的なリスクを緩和する緩和策または回避策があるかどうかを確認します。	**セキュリティ情報で**、問題を緩和する要素および回避策の詳細は「脆弱性の詳細」の各脆弱性のセクションに記載されています。IT プロフェッショナルは特に 2 つのエリアを参照してください。 1. 問題を緩和する要素とは、既定の状態で存在する、一般的な構成または全般的な最善策で、脆弱性の悪用の深刻度を低減する可能性のあるものを指します。 2. 回避策とは、根本となる脆弱性は修正しませんが、更新プログラムの適用前に既知の攻撃の方法を阻止する手助けとなる設定または構成上の変更を指します。マイクロソフトは記載している回避策をテストしており、その回避策が機能を低下させるかどうかを通常説明

	緩和策の評価のリソース	詳細
		している ます。 **セキュリティ アドバイザリ**で、多くの場合「推奨されるアクション」を説明していますが、このセクションにも「回避策」のセクションがあります。これらの回避策も、マイクロソフトがテストしたものです。これらの回避策は根本的な脆弱性は修正しませんが、既知の攻撃の方法を阻止する手助けとなります。回避策が機能を低下させる場合、このセクションにその旨を記載しています。
	脆弱性の影響を緩和するために使用できる有効なソフトウェア セキュリティ保護があるかどうかを確認します。	多くの IT プロフェッショナルがマイクロソフトのセキュリティ更新プログラムを展開している間に利用できる保護が存在するだろうかと考えています。 Microsoft Active Protections Program (MAPP) はセキュリティ ソフトウェア プロバイダーのためのプログラムです。MAPP のメンバーはウイルス対策ソフトウェア、ネットワーク ベースの侵入検出システム、ホスト ベースの侵入防止システムなどの各自のセキュリティ ソフトウェアやデバイスにより IT プロフェッショナルに最新の保護を提供できるよう脆弱性に関する情報を早期に受け取ります。 マイクロソフト セキュリティ情報の概要を受け取った時、またはリスク分析を行っている間、IT プロフェッショナルは www.microsoft.com/security/msrc/mapp/partners.mspx で最新の有効な保護について MAPP パートナーの Web ページをチェックすることを推奨します。 MAPP プログラムは多くのグローバルなサードパーティの組織で構成されており、このような組織の業務は多数のセキュリティ セグメントにまで広がっています。(たとえば、侵入検出、侵入防止、ウイルス対策ソフトウェアなどです。) MAPP パートナーの Web ページにはリスク管理プロセス中に適用する必要のある有効な保護へのリンクが含まれています。IT プロフェッショナルおよび組織への結果は、マイクロソフトのセキュリティ更新プログラムを適用している間の強化された保護です。 有効なソフトウェアのセキュリティ保護に関する詳細情報は、www.microsoft.com/security/msrc/collaboration/mappfaq.aspx (英語情報) または付録をご覧ください。

	緩和策の評価のリソース	詳細
	Microsoft Security Research & Defense のブログをチェックし、脆弱性の影響を緩和する手助けとなる追加情報があるかどうかを確認します。	このガイドの「ステージ 2: リスクを評価する」のセクションで説明しているように、Security Research & Defense のブログにはセキュリティ情報やアドバイザリに記載されていないその他の緩和策や回避策に関する技術的な情報が含まれています。このブログは blogs.technet.com/srd/ (英語情報)でご覧いただけます。 MSRC ブログは重要なマイクロソフトのセキュリティ リソースですが、IT プロフェッショナルに緩和策または回避策を提供することに焦点をあててはいません。これに対し、Security Research & Defense ブログのブロガーは、マイクロソフトのスタッフで、彼らはそれぞれ、脆弱性の報告についての綿密で技術的な分析、新しい脆弱性に関する調査とリサーチ、セキュリティ情報に技術的なガイダンス (セキュリティ情報で説明される緩和策や回避策に関する情報を含む) の提供、ソフトウェアの脆弱性を排除するにあたり更新プログラムが効果的であることの確認などを行っています。

表 10: 緩和策の評価のリソース

高リスク、緩和策なし: セキュリティ更新プログラムが高リスクであり、また効果的な緩和策が確認されていない場合、最善の方策は組織内のすべての影響を受けるシステムに緊急の更新を開始することです。このプロセスは “緊急のパッケージ適用プロセス” のセクションで後ほど説明します。

短期的な緩和策を削除する: 短期的な緩和策が十分に行われている場合、IT プロフェッショナルは標準の更新プロセスを使用して更新プログラムを展開することができます。展開が監視プロセスの一部として確認されている場合、通常の組織の通常の運営に戻すにあたり望ましいのであれば、短期的な緩和策 (もちろん、これが MAPP による有効な保護である場合を除く) を削除することができます。

ステージ 4: 標準または緊急の更新プログラム展開のタイムライン

本セクションの内容*:*

- 「*Deploying Microsoft Windows Server Update Services*」ガイド
- 2 つのセキュリティ更新プログラム パッケージのタイムライン – 標準および緊急
    - 標準の更新タイムラインの目標は 1 か月を超えない
    - 緊急の更新タイムラインは組織によりさまざまで、関連するリスクにより異なる
- セキュリティ更新プログラムの公開までの 6 つのステップ
    1. 展開のプランを立てる
    2. セキュリティ更新プログラムがダウンロードで利用可能かどうかを確認する
    3. 必要な更新プログラムのファイルを取得する
    4. 更新プログラム パッケージを作成する
    5. パッケージをテストする
    6. パッケージを必要としているコンピューターにそのパッケージを展開する

本セクションを終了すると、*IT* プロフェッショナルは次の項目について理解します*:*

- 「*Deploying Microsoft Windows Server Update Services*」 ガイドを読み、組織のネットワーク トポロジーに WSUS を構成するためのオプションを理解する。これは非常に重要です。
- セキュリティ更新プログラムの適用についての 6 つのステップと様々なリソースを理解する。
- さらに徹底的なテストの実行とセキュリティ更新プログラムの迅速な適用の必要性とのバランスをとるための考慮点を理解する。
- セキュリティ更新プログラムのファイルを取得する場所と方法を理解する。
- 次を示すために最低限のレベルのテストが実行される必要性を理解する。
    - インストールの完了時にコンピューターは設計された通りに再起動する。
    - セキュリティ更新プログラムが遅い、または信頼できないネットワークに接続されているコンピューターを対象としている場合、これらのリンクでダウンロードできる。ダウンロード完了時に、セキュリティ更新プログラムが正常にインストールされている。
    - セキュリティ更新プログラムがアンインストールのルーチンで提供される。このルーチンは必要であれば更新プログラムを正常に削除するために使用できる。
    - 業務に不可欠なシステムおよびサービスがセキュリティ更新プログラムのインストール後に引き続き実行される。

本セクションにおけるマイクロソフトの参照リソース*:*

- **Windows Server Update Services (WSUS) および更新プログラム:** このページは WSUS がどのようにマイクロソフトの更新プログラムを保存、管理しているかを説明しています。technet.microsoft.com/ja-jp/updatemanagement/bb245780.aspx をご覧ください。

- **Windows Update Server Services (WSUS) technet.microsoft.com/ja-jp/wsus/default.aspx をご覧ください。さらに具体的な情報は、次の Web ページをご覧ください。**
    - ***Deploying Microsoft Windows Server Update Services* ガイド** technet.microsoft.com/library/cc720507(WS.10).aspx (英語情報) をご覧ください。
    - **Windows Update エージェント (WUA) アプリケーション プログラミング インターフェイス (API)** セキュリティ更新プログラムをさらにカスタマイズするために使用できるスクリプトについては、MSDN Web サイトの “Searching, Downloading, and Installing Updates” および “Searching, Downloading, and Installing Specific Updates” をご覧ください。ウィンドウを作成、変更、サーバー ファームでの複雑な更新のワークフローを調整、または新しく準備されたコンピューターを自動的に更新します。
        - **WUA API:** msdn.microsoft.com/library/aa387099(VS.85).aspx (英語情報) をご覧ください。
        - **“Searching, Downloading, and Installing Updates.”** msdn.microsoft.com/library/aa387102(VS.85).aspx (英語情報) をご覧ください
        - **“Searching, Downloading, and Installing Specific Updates.”** msdn.microsoft.com/library/aa387101(VS.85).aspx (英語情報) をご覧ください。
- **ローカル公開:** WSUS API により、IT プロフェッショナルは各自の組織向けのカスタム更新プログラム、アプリケーションおよびデバイス ドライバーをローカル公開と呼ばれるプロセスを介し作成し、公開することができます。ローカル公開は、カスタム更新プログラムの計画、実装、テストおよび適用は複雑で時間のかかるプロセスであるため、開発およびテスト リソースに専念している組織により実行されるのが最善です。
    - **注:** WSUS API はプロフェッショナルな開発者以外には使用が非常に複雑です。さらに、WSUS はマイクロソフト以外の更新プログラムをサポートしないことを理解することが重要で、このニーズのため、マイクロソフトは IT プロフェッショナルに Microsoft System Center の構成マネージャーを使用するか、プロフェッショナルの開発者による公共の WSUS API に同等の機能の開発を推奨します。
    - ローカル公開のプロセスは 7 つの個別のステップに分割されます。(下記をご覧ください。) msdn.microsoft.com/library/bb902470(VS.85).aspx (英語情報) をご覧ください。
- **Microsoft ダウンロード センター** http://www.microsoft.com/downloads/search.aspx?displaylang=ja をご覧ください。

- **Microsoft Update カタログ** catalog.update.microsoft.com/v7/site/Home.aspx をご覧ください。
- **Microsoft Baseline Security Analyzer (MBSA)**[6]. このツールは小中規模の企業が、マイクロソフトのセキュリティの推奨策に従ってそれぞれのセキュリティ状態を確認し、特定の改善策のガイダンスを提供する手助けとなります。MBSA を使用してコンピューター システムで一般的な管理上の脆弱性や不足しているセキュリティ更新プログラムを検出します。MBSA は更新プログラムのインストールを実行しません。MBSA は更新プログラムをスキャンするのみで、更新プログラム管理のために Microsoft Update を使用してコンピューターを構成する機能があります。technet.microsoft.com/ja-jp/security/cc184924.aspx をご覧ください。
- **Microsoft System Center の構成マネージャー:** MBSA、WSUS およびその他が提供しない追加機能を提供するマイクロソフトからのソリューションです。www.microsoft.com/systemcenter/configurationmanager/ (英語情報) をご覧ください。
- **Microsoft Customer Service & Support (CSS)**. 皆さんの組織の既存のマイクロソフトのサポート連絡先を通じて、または (1) (866) PC-SAFETY [米国およびカナダ (1) (866) 727-2338] で CSS に連絡してください。米国外では、IT プロフェッショナルは各国のマイクロソフトの支社に連絡してください。support.microsoft.com/common/international.aspx をご覧ください。

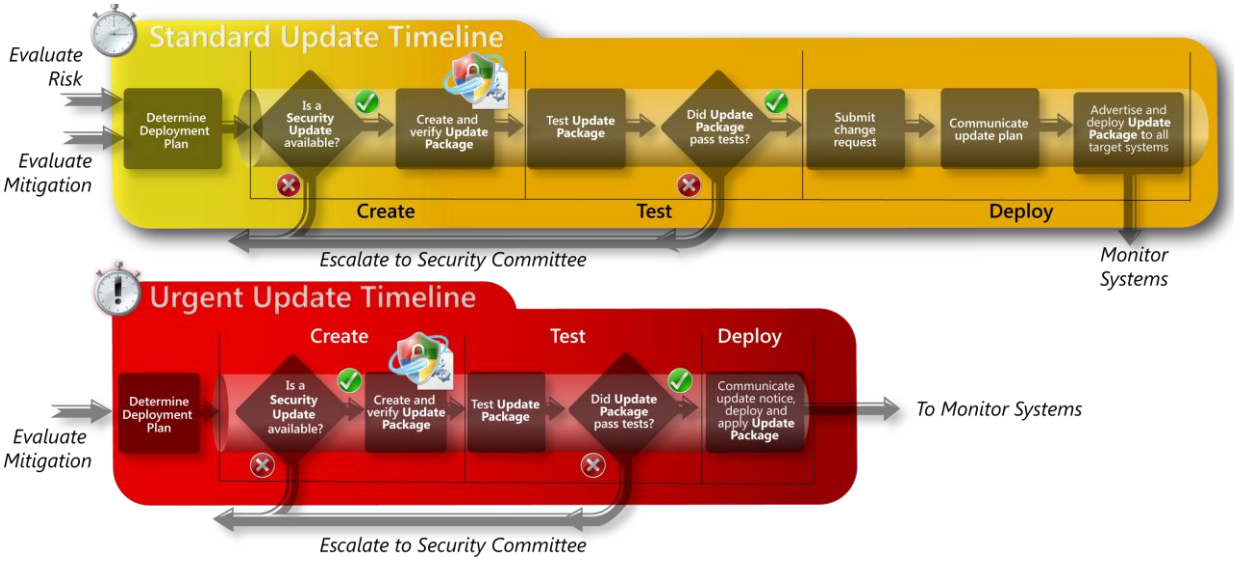
[6] MBSA は、英語、ドイツ語、フランス語、日本語の 4 つの言語にローカライズされていますが、基本となる検出は Microsoft Update および WSUS がサポートするすべての言語の対象となるコンピューターを正確にスキャンします。

Deploying Microsoft Windows Server Update Services ガイド

この段階の一番最初のステップは、Deploying Microsoft Windows Server Update Services ガイドを読み、十分に理解することです。このガイドは WSUS の展開方法を説明しており、WSUS の機能方法について包括的に説明しています。また、WSUS のスケーラビリティおよび帯域管理機能についても説明しています。さらに、このガイドは IT プロフェッショナルに WSUS サーバーをインストールし、構成するためのステップ バイ ステップの手順を提供しています。WSUS が更新するクライアント ワークステーションおよびサーバー上の自動更新の更新や構成方法も説明しています。詳細情報は technet.microsoft.com/library/cc720507(WS.10).aspx (英語情報) をご覧ください。

2 つの適用のタイムライン

このガイドで前述しているように、組織はインストールのインフラストラクチャや更新プログラムの緊急性により、常に 1 つまたは複数の展開プロセスに従うことができます。マイクロソフトは、セキュリティ更新プログラムに対応するために、組織のリスク評価に基づいて IT プロフェッショナルに少なくとも 2 つのタイムラインを確立することを推奨します。危険度の低いセキュリティ更新プログラムについては、IT プロフェッショナルは標準の更新タイムラインに従い、更新プログラムが組織にとってコストや中断を最小限にする方法で展開することができます。しかし、危険度の高いセキュリティ更新プログラムについては、IT プロフェッショナルはその他の考慮点よりも迅速な展開に焦点を置く緊急の更新タイムラインを



使用する必要があります。図 12 はこの段階を示しており、2 つのタイムラインの例をあげています。

図 12: セキュリティ更新プログラム パッケージのプロセス - 作成、テストおよび展開

このステージでの各段階: 前述のタイムラインのステップとその時間的な長さは、組織のスタッフの配属と様々な分類のコンピューターや使用されている展開プロセスのサービス レベル契約 (SLA) により異なります。しかし、これらの適用プロセスの 3 つの基本的な段階は常に同じです。

- **作成:** セキュリティ更新プログラムのバイナリを入手し、それらをパッケージして組織の対象となるコンピューターに展開する準備をととのえるために必要なプロセス。
- **テスト:** 組織のサーバーまたはクライアント システムの範囲をエミュレートするテスト システムへのセキュリティ更新プログラム パッケージの影響をテストするプロセス。
- **展開:** 必要なコンピューター システムにセキュリティ更新プログラム パッケージをインストールするプロセス。このプロセスにはシステムの状態が展開の広がりを追跡できるようにするための報告または段階も含まれています。

標準のパッケージの適用プロセス

1 か月の最大限のエンド ツー エンド プロセスのタイムライン: 標準のパッケージの適用プロセスの目標は、セキュリティ更新プログラムを組織のユーザーおよびサービスへの中断を最小限にするような方法で運用環境に提供することです。同時に、優先順位の低いセキュリティ更新プログラムを、次回のセキュリティ更新プログラムの公開前に確実に展開する必要があります。これは通常最大限のエンド ツー エンドのプロセスのタイムラインである 1 ヵ月となります。(通常の標準のマイクロソフトのセキュリティ更新プログラムのリリース サイクルの期間。) 図 13 は標準の更新プログラムのタイムラインに伴うステップの概要を示しています。

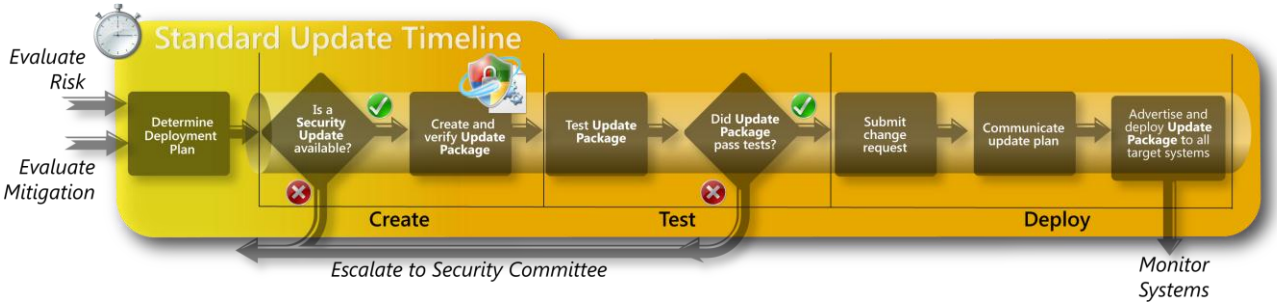


図 *13:* 標準の更新プログラムのタイムライン

更新プログラムを展開するための 6 つのステップ: IT プロフェッショナルは新しいセキュリティ更新プログラムの展開を計画する際、6 つのステップを行う必要があります。

1. 展開のプランを立てる
2. セキュリティ更新プログラムがダウンロードで利用可能かどうかを確認する
3. 必要な更新プログラム ファイルを入手する
4. 更新プログラム パッケージを作成する
5. パッケージをテストする

6. パッケージを必要としているコンピューターにそのパッケージを展開する

展開のプランを立てる

展開とは、セキュリティ更新プログラムにより提供される保護を実装するプロセスです。展開はプロセスの究極の目標であるため、利用可能な展開方法を理解し、それらの方法を評価に組み込むことはセキュリティのリスク評価と同じくらい重要です。

このステップで、IT プロフェッショナルは可能な展開方法を理解し、セキュリティ更新プログラムの展開についてのプランを立てる必要があります。可能な展開方法がスケジュールにどのような影響を及ぼす可能性があるかを理解し、必要な変更を行うことが重要です。たとえば、WSUS が主な適用方法であるにもかかわらず、セキュリティ更新プログラムをサポートしない場合、更新プログラムの適用が最初のプランよりも 2 日長くかかることが確認されるかもしれません。次に、IT プロフェッショナルは回避策を実装し、この展開期間中に必要な保護を提供する場合もあります。

セキュリティ情報を確認する: 展開方法に関する追加情報がセキュリティ情報の「セキュリティ更新プログラムに関する情報 - 検出および展開ツールとガイダンス」のセクションに記載されています。このステージで、WSUS に組み込まれているレポート機能を使用して、コンピューターにセキュリティ更新プログラムが必要であるかどうかを確認するとよいでしょう。

その他のステップと並行して展開のプランを立てる: 「展開のプランを立てるステップ」では、複雑に関連している工程もあり、必ずしも直線状ではありません。ある組織では、ステップは同時に起こり、また順次起こる企業もあります。IT プロフェッショナルは組織のポリシー、ニーズおよびリソースに基づき、これらのステップの実装を決定する必要があります。これらのステップにとって最も重要なことは、特定の構造や順序ではなく、これらの異なる段階が互いに通知し、応答しあうことができることです。あらゆる実装についてのカギとなる点は、フレキシブルで順応性のある状態を保つことで、更新プログラムの必要条件および IT インフラストラクチャの制限を考慮している達成可能な適用プラン (例を下の表 11 にあげています) を決定することです。リスク評価の段階で提供された情報を使用して、適用チームは更新の必要があるコンピューターとその更新の順序を迅速に決定する必要があります。

迅速な展開対徹底的なテスト: IT プロフェッショナルには、緊急の更新タイムラインまたは標準の更新タイムラインに必要とされている更新プログラムのリストがある場合があります。または、その境目を不明瞭にする更新プログラムやコンピューターがあり、IT プロフェッショナルを不安にさせる場合もあります。IT プロフェッショナルはセキュリティ更新プログラムの影響を受けるコンピューターの正確な台数を確認し、各コンピューターについての組織の SLA を満たす更新タイムラインを設定する必要があります。組織はこの問題に対応する手助けとなるポリシーを持つことを推奨します。

この問題を解決するために、IT プロフェッショナルはセキュリティ更新プログラムの展開を迅速に進める必要性対環境で更新プログラムのテストを行う必要性に関する組織のポリシーに基づき、セキュリティ更

新プログラムを展開する必要があります。IT プロフェッショナルがセキュリティ更新プログラムを展開したい方法に基づき、対象となるグループにコンピューターを分類する組織もあります。多くの組織はデスクトップ コンピューターおよびサーバーについて別のグループを使用しています。また、新しいセキュリティ更新プログラムの早期展開を実行するために、「テスト」コンピューターのグループを作成しています。WSUS で、構造のグループ化はかなりフレキシブルです。(コンピューターはデスクトップやテストなど、複数のグループに属すことができます。)

これでプランを立てるステージは終了です。この時点で、IT プロフェッショナルはセキュリティ更新プログラムのリスク評価、緩和策および回避策などのセキュリティ リスク、テスト、展開に関する評価およびプランのすべての要素を反映したスケジュールができているはずです。

例: セキュリティ更新プログラムの展開のプランを立てる

更新の範囲は 1 台のコンピューターから組織内のすべてのコンピューターまで及ぶため、展開のプランを立てることは複雑なプロセスである場合もあります。組織内のすべてのコンピューターを同時に更新できる更新システムを IT プロフェッショナルが所有している可能性は低いため、展開チームはサポートできるコンピューターの台数、また時刻を確認する必要があります。

たとえば、組織に 1 度に 500 台のコンピューターをサポートできる更新システムがあり、指定された高リスクの更新プログラムが 5,000 台のコンピューターに必要である場合、組織は更新サーバーのオーバーロードを避けるため展開の間隔を開ける必要があります。ほとんどの組織は、組織内のコンピューターに既に特定された優先順位があるはずです。通常、少なくとも 2 つの優先順位のレベルがあります。これらは「高価値 (HV)」および「標準」または「一般」のコンピューターと呼ばれることもあります。次にこれらの優先順位がサーバーおよびクライアント コンピューターの両方に適用され、全部で 4 つのコンピューターの分類ができます。これらの定義を使用して、適用システムの制限までこれらのグループ分けの 1 つまたは複数を選択することにより、展開を段階分けすることができます。この例で、展開チームは表 11 で示されているようにコンピューターを分類することに決定しました。

	システムの分類	システムの総数	リスクの総数	説明
	HV サーバー	50	20	運用または収益を生み出すコンピューターなど、組織にとってミッション クリティカルなサービスを提供するサーバー コンピューター。
	一般的なサーバー	200	180	インフラストラクチャ サービスおよびサポート機能を提供するサーバー コンピューター。これらのデバイスは重要ですが、組織の収入源には直接寄与しません。
	HV クライアント	2,000 (1,500 リモート*)	1,000 (800 リモート*)	組織にとって重要であるとされている機能に使用される組織内のコンピューター。コンピューター ユーザーの役割、またはコンピューターに保存されているデータやアプリケーションの機密性のため、このように考えられます。
	一般的なクライアント	4,500 (2,000 リモート*)	1,400 (600 リモート*)	組織にさまざまなサービスを提供していますが、機密情報は保存していないコンピューター。

* ここで「リモート」とはリモートのポータブル コンピューターを指します

表 11: セキュリティ更新プログラムの展開プランの例

表 11 で、クライアント コンピューターは含まれているリモートのポータブル コンピューターの台数によっても特定されていることに注意してください。リモート コンピューターは組織のネットワーク エッジ (例: ネットワーク ファイアウォール) の保護 (および可能な緩和策) 外での攻撃の危険にさらされる可能性があるため、この情報が重要となる脆弱性もあります。このようなケースで、このさらに危険にさらされる可能性により、攻撃のリスクが非常に高まる場合、展開のプランにおいて、その他の修正されたコンピューターよりも、リモートの一般的なクライアントに高い優先順位をつけることが必要となる場合があります。

この情報を使用して、展開のインフラストラクチャの現実的な能力を考慮に入れる展開プラン例を作成することができます。この組織の例で、すべてのコンピューターでの緊急の更新プログラムの展開についての SLA は、表 12 で示されているように、更新プログラムが 24 時間以内に提供されます。

段階	時間	システムの分類	総数	説明
1	08:00–12:00	HV サーバー、一般的なサーバー、および HV クライアント (第一段階)	500	20 台の HV サーバー、180 台の一般的なサーバー、300 台の HV リモート クライアント
2	12:00–16:00	HV クライアント	500	500 台の HV リモート クライアント
3	16:00–20:00	HV クライアントおよび一般的なクライアント (第一段階)	500	200 台の残りの HV クライアント、300 台の一般的なリモート クライアント
4	20:00–00:00	一般的なクライアント	500	300 台の一般的なリモート クライアント、200 台の残りの一般的なクライアント
5	00:00–04:00	一般的なクライアント	500	500 台の一般的なクライアント
6	04:00–08:00	一般的なクライアント	100	100 台の一般的なクライアント

表 12: 展開の段階

この例で、展開のプロセスはこのサポートされているコンピューターの台数についてその最大限に非常に近い台数で実行されています。その他の 500 台のコンピューターがセキュリティ更新プログラムを必要としている場合、組織はこれらのコンピューターのすべてに緊急の SLA を満たすことができていなかったことになります。現行のコンピューター管理プロセスの一部として、展開チームはその展開システムの最大の更新能力を評価し、最悪の場合のシナリオで、組織の SLA が各コンピューターの分類に見合っているようにすることが重要です。

セキュリティ更新プログラムをダウンロードできるか?

標準の更新タイムラインにおける次のステップは、必要なセキュリティ更新プログラム ファイルを入手することです。ほとんどのマイクロソフトのセキュリティ更新プログラムのリリース サイクルで、セキュリティ更新プログラムのファイルはセキュリティ情報の概要のリリースと同時に利用可能となります。セキュリティ更新プログラムのファイルは、マイクロソフトのサービスにより公開されるのに多少の時間を要する場合もあります。IT プロフェッショナルがマイクロソフトのセキュリティ更新プログラムの公開後にその更新プログラムにアクセスできない場合、組織の既存のマイクロソフトのサポートの連絡先を通じて、または (1) (866) PC-SAFETY [(1) (866) 727-2338 米国およびカナダ] に電話連絡により、マイクロソフト CSS に連絡する必要があります。米国およびカナダ以外の国については、IT プロフェッショナルは各国のマイクロソフト支社に連絡する必要があります。
support.microsoft.com/common/international.aspx をご覧ください。

セキュリティ アドバイザリの場合、必要な場合のみ、セキュリティ更新プログラムが含まれます。このため IT プロフェッショナルは、アドバイザリを参照し、ダウンロードおよび展開する必要のあるセキュリティ更新プログラムが提供されているかどうかを確認する必要があります。アドバイザリがファイルを提供していない場合、該当する調査の完了時に、マイクロソフトは IT プロフェッショナルが組織のコンピューター システムを保護するために行うべき適切なアクションをお知らせします。

信頼されるソースから必要なセキュリティ更新プログラム ファイルを入手する

ファイルのリリース時に関わらず、IT プロフェッショナルは次のようないくつかのソースからセキュリティ更新プログラムを入手することができます。

- マイクロソフト セキュリティ情報
- Microsoft Update、Windows Update、WSUS または Microsoft System Center の構成マネージャーなどのマイクロソフトの展開ツール
  注: 多くの場合、IT プロフェッショナルはマイクロソフトの検出および展開ツールを使用してセキュリティ更新プログラムを入手しますが、それでもセキュリティ更新プログラムが見つからない場合もあります。これは、新しいソフトウェアが最近追加され、各ツールが新しいソフトウェアをまだ反映していないという可能性があります。
- マイクロソフト ダウンロード センター www.microsoft.com/download/ をご覧ください。
- Microsoft Update カタログ サービス catalog.update.microsoft.com をご覧ください。

このセクションでは、このガイドは Microsoft Update カタログ サービスについて説明します。これは、企業ネットワークで配布できる更新プログラムのリストを提供するマイクロソフトのサービスです。Microsoft Update は更新プログラムを MSI (MSP または MSU を含む)、実行可能な update.exe、およ

びその他のファイル形式としてサポートします。ほとんどのセキュリティ更新プログラムは CAB ファイルに統合されています。また、IT プロフェッショナルはその他のマイクロソフトのソフトウェアの更新プログラム、ドライバーおよび修正プログラムを一度に見つけられる場所として Microsoft Update カタログ サービスを使用することもできます。

Microsoft Update カタログ サービスを使用して更新プログラムをダウンロードするためには、次のステップに従ってください。

- **ステップ 1:** Microsoft Update カタログ サービス catalog.update.microsoft.com にアクセスします。Microsoft Update カタログに関するよく寄せられる質問は catalog.update.microsoft.com/v7/site/Faq.aspx をご覧ください。
- **ステップ 2:** Microsoft Update カタログで更新プログラムを検索する
  - たとえば、**Windows Vista セキュリティ** のように [検索] ボックスに検索ワードを入力します。
  - [検索] をクリックし、ENTER を押します。
  - 表示されている一覧を参照し、ダウンロードする更新プログラムを選択します。
  - [追加] を各選択ごとにクリックし、更新プログラムをバスケットにダウンロードします。
  - ダウンロードしたいその他の更新プログラムを検索するには、上記のステップを繰り返してください。
- **ステップ 3:** Microsoft Update カタログから更新プログラムをダウンロードする
  - [検索] ボックスの下の [バスケットの表示] をクリックし、ダウンロード バスケットを表示します。
  - 更新プログラムのリストを確認し、[ダウンロード] をクリックします。
    注: メッセージが表示された場合、使用許諾契約書を読み、*[同意する]* をクリックして同意します。
  - [ダウンロード オプション] ウィンドウの [フォルダー] ボックスで、更新プログラムを保存したい場所を選択します。フォルダーのフル パスを入力するか、[参照] をクリックしてフォルダーの場所を指定します。
  - [続行する] をクリックし、ダウンロードを開始します。
  - ダウンロードが完了したら、[閉じる] をクリックし、ダウンロード結果のウィンドウを閉じます。
  - Microsoft Update カタログのウィンドウを閉じます。
  - このステップの前半で指定されたフォルダーの場所を見つけます。
  - 各更新プログラムをダブルクリックし、次に更新プログラムをインストールするための説明に従います。

注: 更新プログラムが別のコンピューター用であった場合、そのコンピューターに更新プログラムをコピーし、その更新プログラムをダブルクリックし、インストールします。

- ダウンロード バスケットに追加されたすべてのアイテムが正常にインストールされたら、このステップは完了です。

このサイトを使用して、IT プロフェッショナルは更新プログラムを検索し、更新プログラムがサポートする必要のある各オペレーティング システムに必要な更新プログラムのリストを作成することができます。IT プロフェッショナルは次に必要なファイルをダウンロードし、それらを使用して適用プロセスのための適用パッケージを作成することができます。

更新プログラム パッケージを作成する

組織のための更新プログラム パッケージを作成するにあたり、いくつかのアプローチが選択できます。組織の管理インフラストラクチャにより、更新プログラム パッケージの種類および更新プログラムを必要とするオペレーティング システムまたはアプリケーション、複数の更新プログラム パッケージを作成する必要がある場合もあります。

WUA API: WUA API はコンポーネント オブジェクト モデル (COM) インターフェイスのセットで、これによりシステム管理者およびプログラマーは Windows Update および WSUS にアクセスすることができます。スクリプトやプログラムを記述して、コンピューターに現在利用可能な更新プログラムを調べ、更新プログラムのインストールまたはアンインストールができます。システム管理者は WUA を使用してプログラム的にコンピューターに適用すべき更新プログラムを確認し、それらの更新プログラムをダウンロードし、ほとんど、またはまったくユーザーの介入なしでインストールすることができます。ISV およびエンド ユーザーの開発者は WUA 機能をコンピューター管理または更新プログラム管理ソフトウェアに統合し、シームレスな運用環境を提供することができます。

WUA API の使用に関する詳細情報は msdn.microsoft.com/library/aa387287(VS.85).aspx (英語情報) をご覧ください。

ローカル公開: WSUS API により、IT プロフェッショナルはローカル公開と呼ばれるプロセスを介し、各組織向けのカスタム更新プログラム、アプリケーションおよびデバイス ドライバーを作成できます。ローカル公開は、カスタム更新プログラムのプラン、実装、テストおよび適用は複雑で時間を要するプロセスであるため、専用の開発およびテスト リソースを持つ組織が最もうまく実行することができます。

注: WSUS API はプロフェッショナルな開発者以外の人物には使用が複雑で、マイクロソフト以外の更新プログラムはサポートしません。この必要条件について、マイクロソフトは IT プロフェッショナルは Microsoft System Center の構成マネージャーを使用するか、プロフェッショナルな開発者を雇用し、公共の WSUS API に同等の機能を開発することを推奨します。

ローカル公開に関する詳細情報は、msdn.microsoft.com/library/bb902470(VS.85).aspx (英語情報) をご覧ください。ローカル公開のプロセスは 7 つのステップにより構成されています。

1. ローカルで公開された更新プログラムを信頼するよう更新サーバーおよびクライアントをセット アップします。
2. 更新プログラムのバイナリ (MSI または MSP パッケージ、または実行可能ファイル) を作成します。
3. 更新プログラムのメタデータを作成し、更新プログラムをインストールする時期と方法を指定します。
4. 更新プログラムを更新サーバーに公開します。
5. 更新プログラムをテスト クライアントのセットに展開することにより、更新プログラムをテストします。
6. 更新プログラムをすべてのクライアントに適用します。
7. 更新プログラムを改定し、バージョン付けをします。

このプロセスに関する詳細情報は、次をご覧ください。

- msdn.microsoft.com/library/bb902479(VS.85).aspx の “Setting Up the Trust Relationship” (英語情報)
- msdn.microsoft.com/library/bb902477(VS.85).aspx の “Authoring Updates” (英語情報)
- msdn.microsoft.com/library/bb902478(VS.85).aspx の “Publishing Updates” (英語情報)
- msdn.microsoft.com/library/bb902483(VS.85).aspx の “Testing Updates” (英語情報)
- msdn.microsoft.com/library/bb902492(VS.85).aspx の “Revising and Versioning Updates” (英語情報)

サンプル スクリプト: マイクロソフトは WSUS サンプル スクリプトも提供しています。WSUS サンプル スクリプトのレポジトリについては、www.microsoft.com/technet/scriptcenter/scripts/sus/default.mspx?mfr=true (英語情報) をご覧ください。

Microsoft System Center の構成マネージャーを使用してアドバタイズする: IT プロフェッショナルがパッケージおよびパッケージのデータが 1 つまたは複数の配布ポイントに送信されたことを定義した後、構成マネージャーを使用して適用プロセスを管理している IT プロフェッショナルは指定されたコレクションでこれらのプログラムをクライアントに利用可能にするアドバタイズを作成することができます。アドバタイズに関する詳細情報は、「提供情報について」technet.microsoft.com/ja-jp/library/bb694110.aspx をご覧ください。

更新プログラム パッケージをテストする

パッケージが作成された後、IT プロフェッショナルはいくつかの承認テストによりそれらを実行し、その更新プログラムが運用を綿密に反映している環境で機能すること、また、ビジネス クリティカルなシステムがセキュリティ更新プログラム展開後でも正常に動作し続けることを確認します。企業の代表者とともに管理者はセキュリティ更新プログラムの深刻度に関わらず、実行すべきテストのセットを作成する必要があります。IT プロフェッショナルは次を示すために最低限のレベルのテストを常に実行する必要があります。

- インストールの完了時に、コンピューターは設計されたように再起動します。
- セキュリティ更新プログラムが遅い、または信頼できないネットワーク接続に接続されているコンピューターを対象としている場合、これらのリンクでダウンロードできます。ダウンロードが完了すると、セキュリティ更新プログラムは正常にインストールされます。
- ビジネス クリティカルなコンピューターおよびサービスがセキュリティ更新プログラムのインストール後にも引き続き動作します。
- セキュリティ更新プログラムを運用環境に適用する前に、トラブルシューティングのステップ、手順およびテスト中に使用されるツールに関する情報に関する情報が収集され、サービス デスクのサポート スタッフと運営チームが利用できるようになります。

テストがどのくらい行われたかに関係なく、セキュリティ更新プログラムを運用環境に展開すると、予測されない、またはラボ環境で再現されない可能性のある影響が起こることがあります。更新プログラムまたは更新プログラムのグループをテスト コンピューターに適用した後、すべてのアプリケーションおよび機能をテストしてください。IT プロフェッショナルが更新プログラムのテストに専念する時間と費用は、問題のある更新プログラムを展開した場合に起こる可能性のある損害に応じて、決定する必要があります。

IT プロフェッショナルは更新プログラムを 2 通りでテストすることができます。

1. テスト環境でテストする
2. 試験的な展開でテストする

テスト環境

テスト環境はテスト ラボで構成され、テストすべき事項や各コンポーネントのテスト方法を説明するケースを詳述するプランが含まれています。テスト環境で更新プログラムをテストするためのリソースがある組織は、更新プログラムのアプリケーションとの非互換性が原因となる問題の件数を削減できるため、常にテスト環境で更新プログラムをテストする必要があります。組織にセキュリティ更新プログラムをテストするためのリソースがない場合でも、IT プロフェッショナルはサービスパックを運用コンピューターに展開する前に、常にそれらをテストする必要があります。

テスト環境の利益: テスト ラボは 1 つのラボまたは複数のラボにより構成されており、複数のラボの場合、各々が製造環境にリスクを与えずにテストをサポートします。テスト ラボ環境で、テスト チームのメンバーは展開の設計仮定を確認し、展開の問題点を発見し、また特定の更新プログラムが実装する変更を理解することを促進することができます。このような作業により、展開中に起こるエラーのリスクを削減し、テスト チームのメンバーが更新プログラムの展開中、または適用後に起こる可能性のある問題を迅速に解決することができます。

多くの組織が各自のテスト スタッフを 2 つの機能上のグループに分けています。そのグループとは、設計チームと展開チームです。設計チームは展開プロセスに不可欠な情報を収集し、即時のおよび長期的なテストのニーズを特定し、テスト ラボの設計を提案 (または既存のテスト ラボへの改善を推奨) します。展開チームは設計チームの決定を実装し、継続的に新しい更新プログラムをテストすることにより、プロセスを完了します。

更新プログラムのテスト環境の有効期間の最初で、展開チームは更新プログラムの展開プロセスをテストし、設計が機能することを確認します。その後、IT プロフェッショナルが展開する更新プログラムを確認した後、展開チームは個々の更新プログラムをテストし、すべての更新プログラムが組織が使用するアプリケーションと互換性があることを確認します。

同等の構成内容: 更新プログラムの環境では、デスクトップ コンピューター、モバイル コンピューター、サーバーなど組織の主なコンピューターのそれぞれの役割を果たすコンピューターが存在する必要があります。各役割を果たすコンピューターに異なるオペレーティング システムがインストールされている場合、各オペレーティング システムは専用コンピューター、マルチ ブート構成の単一のコンピューターまたは仮想デスクトップ環境で利用可能である必要があります。

組織のコンピューターの各種類を代表するコンピューターのセットがある場合、それらをプライベート ネットワークに接続します。また、IT プロフェッショナルは更新プログラムのインフラストラクチャのコンピューターのテスト バージョンに接続する必要があります。たとえば、IT プロフェッショナルは WSUS を使用することにより更新プログラムを展開するプランを立てる場合、WSUS サーバーをラボのネットワークに接続します。

IT プロフェッショナルがラボのコンピューターで使用されているすべてのアプリケーションを読み込み、各アプリケーションの機能をテストするための手順を開発する必要があります。たとえば、Internet Explorer の機能をテストするためには、IT プロフェッショナルはマイクロソフトの Web サイトとイントラネットの Web サイトの両方を訪問する場合があります。後に、IT プロフェッショナルが更新プログラムをテストする時に、このテストを繰り返し行う場合があります。アプリケーションの 1 つがテストに合格しない場合、テスト中の更新プログラムが問題を引き起こした可能性があります。(このガイドの後のセクションに更新プログラムのテストについての詳細情報があります。)

IT プロフェッショナルが多数のアプリケーションをテストする場合、スクリプトを特定し、更新プログラムのテストを自動化することができます。

試験的な展開

更新プログラムの実装をテストするとともに、試験的な展開を行うことにより、組織の展開プランや展開プロセスをテストする機会がもたらされます。IT プロフェッショナルが更新プログラムをインストールするために必要となる時間、人員およびツールを確認するにあたり役立ちます。また、サポート スタッフのトレーニングや更新プログラム展開のプロセスに対するユーザーの反応を評価する機会にもなります。たとえば、ダイヤルアップ ユーザーが特定の更新プログラムをダウンロードするのに 1 時間かかる場合、IT プロフェッショナルはそのユーザーに更新プログラムを配信する別の方法を検討する可能性があります。

テスト プロセスのステップ

試験的な展開を行った後の次のステップは、テストで使用したケースのセット全体を調べ、更新プログラムがオペレーティング システムまたはそのオペレーティング システムで実行されているアプリケーションの必要な機能を変更していないかどうかを確認することです。表 13 は IT プロフェッショナルが行う必要のあるテスト プロセスのステップを詳細に説明しています。

	テスト プロセスのステップ	詳細
	すべての影響を受けるソフトウェアの更新プログラムについて、セキュリティ更新プログラムのインストールをテストします。	これらのテストは、対象となるシステムにセキュリティ更新プログラム パッケージが正常に展開、インストールされるようにします。
	クライアントおよびサーバーの更新プログラムについて、更新プログラム適用後の機能をテストします。	これらのテストは、更新プログラムの適用後でも、システムで必要とされるローカル サービスが引き続き利用可能であり、正しいレベルで実行されるようにします。
	クライアントおよびサーバーの更新プログラムについて、ネットワーク インターフェイスをテストします。	これらのテストは、更新プログラムの適用後でも、特定のインターフェイス システムを介しネットワークに提供される必要なリモート サービスが引き続き利用可能であり、必要とされるレベルで実行されるようにします。
	その他のセキュリティ更新プログラムについて (たとえば、Microsoft Office system、Internet Explorer 用の更新プログラム) ユーザー アプリケーションをテストします。	クライアント システムで、必要なビジネス アプリケーションの機能をテストすることが重要です。これらのテストのケースはすべてのサポートされているユーザー アプリケーションについての機能のセットを実行するために使用されます。

	その後、Microsoft Office システムおよび Internet Explorer についてユーザー アプリケーション テストの 2 つの例があります。IT プロフェッショナルは組織の重要な各ビジネス ユーザー アプリケーションについての繰り返し可能なテストを特定し、開発する必要があります。

表 *13:* テスト プロセスのステップ

このガイドの次のいくつかのセクションで、表 13 のテスト プロセスのステップの機能をテストするために適用できるユーザーのテスト ケースの例をいくつかあげます。**これらのステップは単にテスト プロセスを開始するベースラインです。IT プロフェッショナルはこれらを組織の特定の必要条件向けに変更することを推奨します。**

セキュリティ更新プログラムのインストールをテストする

表 14 はすべての影響を受ける製品用のセキュリティ更新プログラムのインストールとアンインストールをテストするための推奨されるステップをいくつか説明しています。

	詳細
インストール前	更新プログラムがシステム、オペレーティング システムまたはアプリケーションのバージョンに適用されることを確認します。詳細情報はこのガイドの「ステージ 2: リスクを評価する」をご覧ください。 「警告」がないことを確認します。
インストール	インストール プロセスが実行され、正常に完了したことを確認し、このプロセス中でエラーが発生しなかったことを確認します。 コンピューターおよび更新プロセスのログを確認し (%systemroot%¥KB[XXXXXX].log の KB[XXXXXX] は、特定の KB の番号を指します。例: KB973346) エラーが記録されていないことを確認します。 更新プログラムのインストールが正常に報告されることを確認します。更新プログラムにより、これには次が含まれる場合があります。 • レジストリで更新プログラムのインストール キーを確認し、適切に作成されたことを確認します。 • 更新プログラムのインストールが監視システムにより正しく報告されたことを確認します。 • 更新プログラムが [コントロール パネル] の [プログラムの追加と削除]

	詳細
	フォルダーに表示されていることを確認します。 • アンインストール ディレクトリが存在し、変更されたバイナリ ファイルが含まれていることを確認します。 • システムが通常とは異なる、または異常な動作をしないことをテストします。
インストールの再起動の後	指定された変更が逆になっていたり、変更されていないことを確認します。 システムが通常とは異なる、または異常な動作をしないことを確認します。必要であれば、手動でシステムを再起動します。
更新プログラムの再インストールを試行する	更新プログラムのインストールが以前に失敗したり (インストールされない部分があった) 再インストールの試行が失敗しないかを確認します。 アンインストール パラメーターまたはバイナリへの変更がないことを確認します。
アンインストール	アンインストール プロセスが実行され、正常に完了することを確認します。 レジストリ キー、バイナリ、構成ファイルなどを確認することにより、すべての変更が元の構成に戻っていることを確認します。 システムまたは更新プロセス ログ (例: %systemroot%¥KB[XXXXXX].log) にエラーがないことを確認します。 更新プログラムのインストールが削除されたことを確認します。これが正常に行われたことを示すめやすには次があります。 • レジストリ キーが削除されています。 • 監視ツールが更新プログラムが不足していることを正しく報告しています。 • 更新プログラムが [コントロール パネル] の [プログラムの追加と削除] に表示されていません。 • アンインストール ディレクトリが削除されています。 更新プログラムのアンインストールに関する追加情報は、後ほど「セキュリティ更新プログラムのアンインストール」のセクションをご覧ください。
アンインストールの再起動の後	指定された変更が逆になっていたり、変更されていないことを確認します。 システムが通常とは異なる、または異常な動作をしないことを確認します。

表 *14:* セキュリティ更新プログラムのインストール テストのステップ

必要なオプション スイッチおよびパラメーターでインストールおよびアンインストールのテストを繰り返してください。たとえば、再起動なしのオプション、無人のオプションなどでテストを行います。

更新後のシステムの機能をテストする

表 15 および 16 は、サーバーおよびクライアントにそれぞれセキュリティ更新プログラムをインストールした後、システムの機能のテストに関するいくつかの推奨を詳しく説明しています。これらのステップは単にテスト プロセスを開始するためのベースラインです。IT プロフェッショナルは組織の特定の必要条件向けにこれらを変更することを推奨します。

サーバーのユーザビリティのテスト *(注: 各テストの終わりに、操作に関連するエラーについて、イベント ログを確認してください。)*
システムが起動 (コールド ブート) および再起動 (ウォーム ブート) を正常に完了させることをテストします。
ローカル管理者としてログオンし、ログオンが正常に完了することをテストします。
すべての必要なサービスが正しく開始することを確認します。
ネットワークが適切に初期化されるか
必要なポートが依然として有効であることを確認します。
IP アドレス、ネットワーク マスクおよびその他のネットワーク パラメーター (例: デフォルト ゲートウェイ、DNS および WINS) が正しく割り当てられていることを確認します。
Localhost、ローカル ネットワーク (例: デフォルト ゲートウェイ) 上のホストおよびリモート ネットワーク セグメント上のホストに PING できることを確認します。
プロキシーが必要な場合、プロキシーを使用することにより、アクセスおよび外部のホストを確認します。
ドメイン コントローラー
ドメイン コントローラーがすべての DCDIAG.EXE テストに合格することを確認します。
クライアントがドメイン コントローラーを検出できることを確認します。(たとえば、**ipconfig flushdns** コマンドの後にクライアントがホストを PING し、“nslookup” を実行することができる。)
分散ファイル システム (DFS) の複製およびファイル レプリケーション サービス (FRS) (該当する場合) が正しく機能することを確認します。
DNS サーバー
DNS サービスが起動し、単純なクエリと再帰テストの種類の両方を正常に完了することを確認します。
ネーム サービスが名前を適切に解決していることを確認します。(たとえば、**ping servername** コマンドがサーバー名および IP アドレスを返すなど。)

WINS サーバー
WINS サービスが起動され、正常な状態であることを確認します。
WINS データベースの整合性の確認が正常に完了することをテストします。
WINS クライアントが名前を解決し、更新できることを確認します。
サーバーのイベント ログを確認し、WINS の操作に関連するエラーが含まれていないことを確認します。
動的ホスト構成プロトコル (DHCP) サーバー
DHCP サービスが適切に起動すること、Microsoft 管理コンソール (MMC) DHCP スナップ イン サーバーの統計が適切な操作を示しており、アドレス データベースがリースされているアドレスを示していることをテストします。
DHCP クライアントが IP アドレスを取得できることを確認します。
DHCP データベースの整合性確認を実行し、エラーが発生せずに完了することを確認します。
IIS Server
IIS サービスが実行されていることを確認し、WWW 公開サービスが適切に開始されていることを確認するためにサービスを確認し、INETINFO.EXE プロセスが実行されていることを確認するためにプロセスを確認します。
IIS サービスが再起動後に起動することを確認します。
Web サーバー上の認証と暗号化のレベルが適切に動作することを確認します。(つまり、ユーザーがアクセスを認証されている Web コンテンツにアクセスできるかを確認します。)
IIS 管理の IP アドレスおよびドメイン名が適切に設定されていることを確認します。
ルート フォルダーおよびすべての必要な Web ファイルが存在していることを確認します。
クライアントがサーバー上の静的な Web ページと有効な Web ページの両方にアクセスできることをテストします。
ファイルおよびプリント サーバー
管理者が新しいファイル共有を作成できることをテストします。
管理者がファイル共有へのドメイン ユーザーのアクセスを正常に変更できることを確認します。
クライアント システムが、ファイル共有が Active Directory® が公開された後にそれを見つけることができることを確認します。
管理者としてログオンし、新しいプリンターを正常に追加できることを確認します。
クライアント システムが、プリンターが Active Directory に公開された後に、そのプリンターにアクセスできることを確認します。
クライアント システムから、文書を正常に印刷できることを確認します。

表 15: サーバーについての更新後のシステムの機能のテスト

クライアントのユーザビリティのテスト (注: 各テストの終わりで、操作に関連するエラーがあるかどうか、イベント ログを確認します。)
管理者のテスト
ドメイン管理者ユーザーがワークステーションを子ドメインに追加できることを確認します。
ドメイン管理者ユーザーがログオンし、パスワードの変更、印刷、印刷キューの表示や管理、リモート共有のファイルへのアクセス、IP アドレスのリリースおよび更新ができることを確認します。
ユーザーのテスト
ドメイン ユーザーがログオンし、パスワードの変更、印刷、印刷キューの表示、リモート共有のファイルへのアクセスができることを確認します。

表 16: クライアントについての更新後のシステムの機能のテスト

アプリケーション インターフェイスをテストする

テストの段階での次のステップは、更新プログラムの適用後、特定のインターフェイス システムを介しネットワークに提供された必要なリモート サービスおよびアプリケーションが引き続き利用可能であり、必要とされるレベルで実行されることを確認することです。表 17 および 18 では IT プロフェッショナルがセキュリティ更新プログラムのインストールの後に、システムの機能が正しいことを確認するために使用できるいくつかの推奨されるテストをあげています。これらのステップは単にテスト プロセスを開始するためのベースラインであるため、IT プロフェッショナルは各自の組織の特定の必要条件に応じてこれらを変更することを推奨します。

ローカル アプリケーション インターフェイス
IIS Server
ローカル IIS サービスに認証できることを確認します。
管理者アカウントとしてログオンし、次のテストを実行できることを確認します。 • ローカル IIS サービスを管理する。 • ローカル IIS サービスから静的なページを取得する。 • ローカル IIS サービスから ASP ページを取得する。
SQL Server
ローカル SQL Server サービスに認証できることを確認します。
管理者アカウントとしてログオンし、次のテストを実行できることを確認します。 • ローカル SQL Server サービスを管理する。 • SQL Server テーブルをクエリする。 • ストアド プロシージャーを実行する。

表 *17:* ローカル アプリケーション テスト

リモート アプリケーション インターフェイス	
	各アプリケーションがバック エンド サーバーまたはサービスに必要に応じて接続を持つことを確認します。
	システムが必要となるバックエンド サーバーに認証できることを確認します。
ターミナル サーバー	
	リモート デスクトップ プロトコル (RDP) セッションをクライアント コンピューターから開始を試行します。
	ローカル管理者として RDP セッションを介しログオンできることを確認します。
	ローカル管理者アカウントが必要な管理コンソールにアクセスできることをテストします。
	RDP セッションが必要な暗号化のレベルに対し安全で、サーバー認証が正常に行われたことをテストします。
	ドメイン管理者ユーザーとして RDP セッションを介しログオンできることを確認します。
	ドメイン管理者アカウントが必要な管理者コンソールにアクセスできることをテストします。
	標準のターミナル サーバー ユーザー アカウントが RDP セッションを終了できることをテストします。
	ユーザー アカウントが切断されたセッションを復旧できることを確認します。
IIS Server	
	ネットワークで IIS サービスに認証できることを確認します。
	ローカル管理者アカウントとして認証を行い、リモート IIS サービスを管理できることを確認します。
	管理者アカウントがリモート IIS サービスから静的なページと有効なページ (例: ASP) の両方を取得できることを確認します。
	標準ユーザー アカウントがリモート IIS サービスに認証できることを確認します。
	標準ユーザー アカウントがリモート IIS サービスから静的なページと有効なページ (例: ASP) の両方を取得できることを確認します。
SQL Server	
	管理者アカウントが SQL Server サービスにログオンできることを確認します。
	管理者アカウントが次のタスクを実行できることを確認します。 • テーブルのクエリ • ローカル (SQL Server) ユーザーの追加と構成 • ドメイン ユーザーの追加と構成 • ストアド プロシージャーの実行

	• テーブルの作成と更新 • テーブルの削除
	標準ユーザー アカウントが次のタスクを実行できることを確認します。 • SQL Server サービスへの認証 • テーブルのクエリ • ストアド プロシージャーの実行 • テーブルの更新
注意	基本的な機能のテスト (つまり、接続、認証、管理、機能の読み取りおよび書き込み) は Message Queuing (MSMQ とも呼ばれています)、SNA Gateway、ネットワーク ファイル システム (NFS) などのようなその他のバックエンド接続に対しても同様に適用されます。

表 18: リモート アプリケーションのテスト

ユーザー アプリケーションをテストする

表 19 および 20 は Microsoft Office system および Internet Explorer 用のセキュリティ更新プログラムをテストするためのいくつかの推奨されるプロセスをあげています。テスト プロセスのこの部分では、組織のすべてのサポートされているビジネス アプリケーション向けのテストのセットを必要とします。Internet Explorer について、IT プロフェッショナルは更新プログラムのインストールの前または後でページのレンダリングが正しく行われ、アプリケーションが機能していることを確認するためのテストを行う必要があります。これらのステップは単にテスト プロセスを開始するためのベースラインであるため、IT プロフェッショナルは各自の組織の特定の必要条件に応じてこれらを変更することを推奨します。

Microsoft Office System のテスト
Microsoft Office system 用のサポートされているサービス パックがシステムにインストールされていることを確認します。
ファイルを開く、保存する、編集する、閉じるなど、Microsoft Office system のアプリケーションの通常の操作を実行します。
文書、スプレッドシート、プレゼンテーション ファイルをさまざまな形式で保存できることを確認します。たとえば、Microsoft Office Word で .docx、.doc、.html、.dot および .rtf、Microsoft Office Excel® で .xlsx、.xls、.html、.xml およびさまざまなテキスト形式などです。
異なるセキュリティ レベル (低、中、高) で文書 (ワークブックおよびプレゼンテーションを含む) を実行します。
Microsoft Visual Basic® for Applications のアプリケーションを利用する Microsoft Office system の社

内およびサードパーティのアプリケーションを実行します。
ファイルに埋め込まれた ActiveX® コントロールが問題なく読み込みを行い、新しい ActiveX コントロールの追加が正しく機能することをテストします。
デジタル著作権管理 (DRM) でも上記のテストを実行してください。DRM でもファイルを開く、編集する、保存するが機能することを確認してください。

表 19: Microsoft Office System のユーザーについてのアプリケーションのテスト

サーバーおよびワークステーション上の Internet Explorer のテスト
社内で開発された LOB Web アプリケーションをテストします。
該当するエンタープライズ リソース プラニング (ERP) およびカスタマー リレーションシップ マネジメント (CRM) アプリケーションをテストします。
たとえば Microsoft Visual Studio® などの .css ファイルを使用するアプリケーションをテストします。
Internet Explorer コンポーネントを使用するアプリケーションを実行し、ファイル転送プロトコル (FTP) の操作を実行します。
Dynamic Hypertext Markup Language (DHTML) を使用する Web アプリケーションが引き続き使用できることを確認します。 • ポップアップ オブジェクト • **window.location** オブジェクト • **window.opener** オブジェクト • イベント • <object> タグ • **window.self** オブジェクト • ActiveX コントロール • .NET コントロール
Web アプリケーションがカスケード スタイル シート (CSS) を使用し、正しく表示できることを確認します。
バイナリ ビヘイビアーを使用する HTML ページが引き続き予期された動作を行うかを HTML ページを使用して、Web アプリケーションをテストします。
外部のスクリプトを使用する HTML ページが予期されたように引き続き実行されることを確認します。
<script> タグを使用する HTML ページを使用して Web アプリケーションの機能をテストします。
.mht ファイルを開くテストをします。
ファイルのダウンロードに urlmon.dll を利用するすべてのアプリケーションを確認します。
Web ページを保存するテストをします。

CSS を使用する HTML ページをテストします。
Microsoft Office 2003 System (Web ツールバー搭載) または Microsoft Money など、Internet Explorer をブラウザーとしてホストするすべてのアプリケーションが引き続きページを正しく表示することを確認します。

表 20: Internet Explorer のユーザーについてのアプリケーションのテスト

必要な更新プログラム パッケージがテスト プロセスに合格した後、次のステップはそれらを展開方法に渡し、組織に展開することです。

更新プログラム パッケージを展開する

組織で、多種多様なコンピューターがセキュリティ更新プログラムを必要とする場合があります。このセクションでは、IT プロフェッショナルが組織内のシステムの大多数への展開をサポートするために使用できる (中断と労力を最小限にし、かつ展開の推奨されるタイムフレーム内である) 方法について説明します。

パッケージの展開を開始する前に、必要な更新ウィンドウ中、更新が必要なシステムおよび環境内のシステムの最新の図式を得ることが重要です。理想的には、組織は監視およびレポートのソリューションを使用し、すべての管理されているコンピューターの現在の状態に関するレポートを作成できることです。展開が対象となるシステムで更新されているもの、また、更新されていないものを追跡するために開始された時、展開の基礎としてこのレポートを使用し、システムの監視の段階 (後に説明します) に渡すことができます。

これらのレポートをサポートする監視ソリューションを使用していない組織では、IT プロフェッショナルは対象となるシステムとその現在の状態を確認するための別の方法を見つける必要があります。

その他の管理ソリューションが利用可能でない場合、IT プロフェッショナルは無償の MBSA ツールを使用してネットワークで現在有効なシステムをスキャンすることができます。MBSA は小中規模の企業が各自のセキュリティの状態がマイクロソフトのセキュリティの推奨策に従っているかを確認することを支援し、特定の改善策のガイダンスを提供ツールです。MBSA を使用してシステムで一般的な管理上の脆弱性や不足しているセキュリティ更新プログラムを検出してください。http://technet.microsoft.com/ja-jp/security/cc184924.aspx をご覧ください。

MBSA は更新プログラムをインストールしません。更新プログラムのスキャンを行い、システムを更新プログラム管理のために Microsoft Update を使用するように構成するのみです。MBSA は完全なシステム管理インベントリ ツールの代わりとなるものではありませんが、インベントリ ソリューションが存在しない環境で使用することができます。

より大規模な企業の組織は MBSA が提供しない追加機能を必要とする可能性があります。このため、Microsoft System Center の構成マネージャーが MBSA および WSUS が提供しない追加機能を提供する別のソリューションとなります。www.microsoft.com/systemcenter/configurationmanager/ (英語情報) をご覧ください。

いくつかの潜在的な問題や制限が、セキュリティ更新プログラムを十分に運用環境に適用するために必要なステップに影響を及ぼす可能性があります。IT プロフェッショナルはセキュリティ更新プログラム適用の任務を負う時、表 21 の情報を検討する必要があります。

適用の考慮点	コメント
タイムラインの必要条件に対し例外をどのように処理するかを検討します。	リスク評価のプロセスとして、対象となるシステムが更新されるまでの時間が決定されている必要があります。 しかし、これらのタイムラインに合わないシステムもある場合があります。このため、このようなシステムが更新プログラム未適用の状態のままでないようにするための文書化されたプロセスを用意することが重要です。システムの可用性、ユーザーの役割および責任、システムの不安定さの性質または更新プログラムにより解決されるとされているセキュリティ上の脆弱性の性質など、いくつかの要素がこの状況につながる可能性があります。
システムが最小限のインストールの必要条件を満たしていることを確認します。	更新プログラムがインストールのための特定の量のディスク領域を必要とする場合、またはインストール前に更新プログラムをキャッシュしたい場合、各クライアント コンピューター上の空きのディスク領域の量を確認する必要があります。 さらに、リモート クライアントがサイズの大きい更新プログラムをダウンロードするのに時間を要する場合があります。更新プログラムが「必須」であると分類されていない場合、このようなクライアントがネットワークに物理的に接続されるまで、インストールを延期することが適切である場合もあります。しかし、更新プログラムが必須となった後、対象となるクライアントがリモートであったとしても更新プログラムの適用は強制となります。
更新の時間枠とタイムゾーンについてのプランを立てます。	ビジネスに不可欠なコンピューターには変更およびコンピューターの再起動が許可される時間 (休止時間) がある場合があります。セキュリティ更新プログラムの展開やこれらの休止時間のため必要となるシステムの再起動のスケジュールを立てる必要があります。また、クライアントが異なる時間に更新されるよう更新プログラムの展開を段階分けするのもよいでしょう。タイムゾーンの使用がこれらの適用の管理に役立つ場合があります。 WSUS を使用する IT プロフェッショナルは定期的にスケジュールされたメンテナンス時間の前にグループ ポリシー設定を使用してクライアントに強制的に更新プログラムをイ

適用の考慮点	コメント
	ンストールさせることができます。これを行う前に、子 WSUS サーバーに強制レプリケーションがあることを確認してください。これらは通常 WSUS サーバーの管理ページの [今すぐ同期] オプションを使用して、ネットワークの平穏時に更新プログラムを同期するようスケジュールされています。 詳細情報は technet.microsoft.com/library/cc720507(WS.10).aspx (英語情報) の Deploying Microsoft Windows Server Update Services ガイド (英語情報) をご覧ください。
グループ ポリシーの制限はどのような状態ですか?	クライアント コンピューターが特定のグループ ポリシー設定の使用によりロック ダウンされている場合、セキュリティ更新プログラムの正常なインストールに影響が及ぶ場合があります。
更新プログラムが元のインストール ファイルへのアクセスを必要とするかどうかを確認します。	更新すべき製品が Windows インストーラーを使用して展開された場合、Windows インストーラーは元のインストール ファイルへのアクセスが必要となる場合があります。セキュリティ更新プログラムの無人インストールが実行される場合、これらのファイルは製品が最初にインストールされた時と同じ場所に配置される必要があります。製品が最初にインストールされたのが物理的なメディア (例: CD ドライブ) からである場合、Windows インストーラーは現在挿入されている CD 上で元のファイルを見つけようとします。
ユーザー アプリケーションがユーザーごとにインストールされているかどうかを確認します。	すべてのユーザーについて、アプリケーションがコンピューターごとではなく、ユーザーごとにインストールされている場合、IT プロフェッショナルはコンピューターごとにアプリケーションを再インストールし、セキュリティ更新プログラムを新しいインストールに適用する必要があります。
ネットワーク帯域の制限についてのプランを立てます。	セキュリティ上の脆弱性による危険にさらされているコンピューター、または不安定な状態になる可能性のあるコンピューターにセキュリティ更新プログラムを適用しなければならないやむを得ない理由がある場合、このようなコンピューターが更新された後に、その他のコンピューターへの適用を継続してください。 たとえば、セキュリティ更新プログラムをリモート サイトに展開することはネットワー

適用の考慮点	コメント
	ク帯域の制限のため、ローカル サイトへの展開よりも時間が長くかかる可能性があります。このような場合、最短の時間で最大数のシステムが更新されるように、まずローカルでの展開を検討するのが最適です。ローカルでの展開時間が完了した後、セキュリティ更新プログラムをリモート サイトに展開することができます。

表 *21:* パッケージ展開の考慮点

これらの考慮点には、IT プロフェッショナルが最初の展開プランに変更を行う必要のあるものもある場合があります。このような場合、SLA を確認することが重要です。適用が SLA の必要条件を満たさない場合、組織がさらされる危険を評価できるよう、これを適切な個人に伝達する必要があります。

変更要求を提出する

次のステップは IT プロフェッショナルが標準の変更制御プロセスを介し管理される生産システムへの変更要求を提出することです。

IT プロフェッショナルが必要な変更要求を提出した後、深刻度、影響、適用するために必要なステップなどの更新プログラムに関する情報をユーザー、企業およびサービス デスクに伝達する方法と日時を決定する必要があります。

これは上記で説明している展開プランに含まれている必要があります。

組織に展開スケジュールを伝える

エンド ユーザーおよび管理者に保留中の更新プログラムのリリースに関する情報を伝えることが重要です。IT プロフェッショナルは明確で容易に識別できる電子メール メッセージをユーザーおよび管理者に送信する必要があります。これにより、更新プログラムについて通知され、またそのインストール方法に関する情報が提供されます。可能であれば、行う必要のあるアクションについて念を押すために、ユーザーおよび管理者にフォローアップのためのフラグを設定した電子メールを送信してください。

共通のイントラネット ホーム ページ: 組織にユーザー向けの共通のイントラネット ホーム ページがある場合、そのサイトに更新の期間についての通知を投稿することを検討してください。

Wake-on-LAN 機能: 更新プログラムを業務の中心となる時間外にデスクトップ コンピューターに展開する場合、これをユーザーに通知し、組織が Wake-on-LAN 機能をこれらのコンピューターで有効にしていない特定の日付にコンピューターの電源を入れたままにしておくよう指示する必要があります。

WSUS ポリシー オプションを使用する: WSUS を使用して、IT プロフェッショナルは更新プログラムの通知を使用することにより直接ユーザーに通知することもできます。これらは展開パッケージの準備完了時に直接ユーザーのコンピューターに配信されるポップアップ メッセージです。これが該当する場合、IT プロフェッショナルはこのパッケージを提供する方法についていくつかの追加オプションを検討する必要がある場合もあります。表 22 でこのオプションについて説明しています。

WSUS ポリシーのオプション	コメント
ダウンロードとインストールを通知	「新しい更新プログラムがダウンロードできるようになった」ことを示す通知がタスクバーに表示される時には常に、ローカル管理者権限でログオンしているユーザーは更新プログラムをダウンロードするオプションを選択する必要があります。このインストールを完了させるためには、ユーザーは「新しい更新プログラムがダウンロードできるようになった」ことを示す通知が表示された時に、ソフトウェアの更新プログラムをインストールする必要があります。

自動ダウンロードしインストールを通知	自動更新クライアントはクライアント コンピューターに適用される新しく許可された更新プログラムを自動的にダウンロードします。更新プログラムをインストールするためには、ローカル管理者権限でログオンしているユーザーは「新しい更新プログラムがダウンロードできるようになった」ことを示す通知が表示された場合、ソフトウェアの更新プログラムをインストールするオプションを選択する必要があります。
自動ダウンロードしインストール日時を指定	ローカル管理者権限でログオンしているユーザーはスケジュールされたインストールの時間よりも前に更新プログラムをインストールすることができます。またはインストールの完了後、再起動 (必要である場合) を延期することができます。ローカル管理者権限がないユーザーについては、更新プログラムはスケジュールされた時間にバックグラウンドでインストールされます。このようなユーザーは [スケジュールされた自動更新のインストールに対しては自動再起動しない] のポリシー設定が有効である場合、コンピューターの再起動を延期することのみができます。

表 22: WSUS ポリシーのオプション

適用段階での WSUS の使用に関する詳細情報は、technet.microsoft.com/library/cc706995(WS.10).aspx (英語情報) の WSUS Technical Library (英語情報) をご覧ください。

更新プログラムをインストールする

リリース プランが立てられ、通知された後、展開プロセスにおける次の段階は必要な更新プログラムをシステムにインストールすることです。ここで実行する必要のあるタスクと操作は主に組織の展開方法の必要条件により異なります。このステップはすべてのコンピューターにおよぶためにさまざまな方法を必要とする場合があります。たとえば、クライアント システムに標準の更新プログラムの展開タイムラインのプロセスを使用することができます。しかし、HV サーバーについては、サーバーを綿密に監視し、可能な限り迅速に完全な動作状態に戻すことができるため、システム管理者はおそらく手動で更新プログラムを適用するでしょう。

より大規模な組織には、IT プロフェッショナルが複数の更新サーバーでの更新作業の負荷の均衡をとり、組織のサーバーで更新プログラムを段階分けし、クライアントの更新件数がどのサーバーにも負荷をかけ過ぎないようにする必要があるため、さらに複雑な面があるでしょう。理想的には、IT プロフェッショナルはこのステージの初期で説明した段階的な展開でセキュリティ更新プログラムをリリースすることです。これにより、セキュリティ更新プログラムの初期のの配布中に発生する可能性のあるエラーによる影響や悪影響が最小限となります。

このプロセスのステップは IT プロフェッショナルが更新プログラムを展開するために使用するインフラストラクチャ管理製品により異なります。しかし、ツールは別にして、次のような特定の段階が通常必要になります。

- **展開サーバーで必要な更新プログラムをステージングする:** 必要な更新プログラムを更新クライアントにアドバタイズする準備のできている展開サーバーにそれらの更新プログラムをコピーします。
- **更新プログラム パッケージを必要なクライアントに配布する:** IT プロフェッショナルがこの段階を管理する方法は更新プロセスに含まれているクライアント数と組織の更新サービスの機能により異なります。IT プロフェッショナルが多数のクライアントをサポートしている場合、配布プロセスは複数のサーバーで更新プログラム パッケージをステージングし、負荷を分散させるか、ある期間にわたってクライアント ベースを更新するロール更新を実行し、受け入れ可能な最大の制限が更新サーバーで保持されているようにする可能性があります。
- **更新プログラム パッケージを実行する:** パッケージの実行方法は管理ツールにより異なりますが、IT プロフェッショナルには 2 つの基本的なオプションがあります。それは自動化と手動です。

WSUS で更新プログラムを許可する: 段階的なロールアウトが必要な場合、IT プロフェッショナルは WSUS 親サーバー上の更新プログラムのみをクライアントに利用可能にすることを許可する必要があります。次に WSUS クライアントは次の検出サイクルか、ローカル管理者により指示された時に新しく許可された更新プログラムをダウンロードし始めます。(自動更新クライアントが、新しい更新プログラムが利用可能となった時にローカル管理者に通知するよう構成されている場合)

しかし、段階的なロールアウトがある場合、IT プロフェッショナルはまず親 WSUS サーバーのみで更新プログラムを許可する必要があります。次に、IT プロフェッショナルがそのサーバーによりサポートされているクライアントに更新プログラムを正常に展開した後、ロールアウトの次の段階でクライアントをサポートする WSUS 子サーバーでの許可リストの同期を有効にする必要があります。

緊急のパッケージの展開プロセス

セキュリティ更新プログラムが緊急の更新プログラムとしての優先順位がつけられた場合、更新プログラムを可能な限り最短期間で展開するために、パッケージの展開プロセスは通常、迅速に進める必要があります。図 14 は緊急の更新プログラム パッケージの適用段階に必要となるステップを示しています。

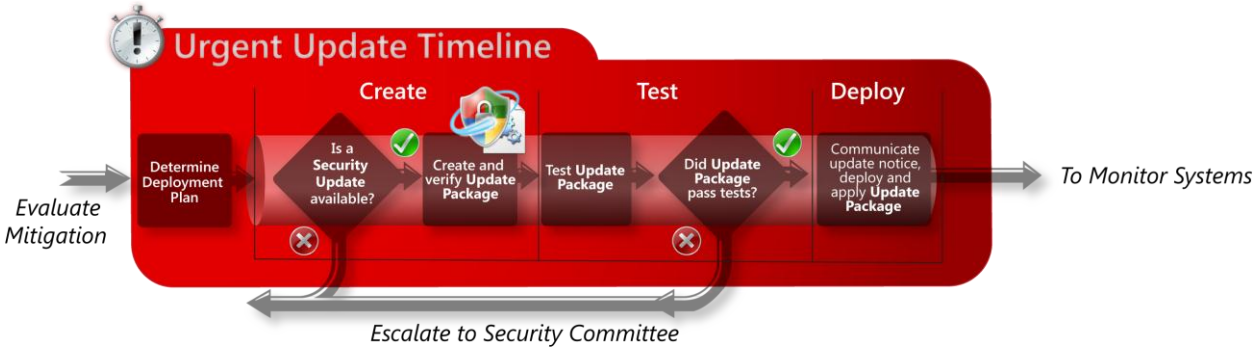


図 14: 緊急のパッケージの展開プロセス

セキュリティ更新プログラムの適用を迅速に進める: セキュリティ更新プログラムの展開は次の 2 つの方法のうち 1 つを使用して迅速に進めることができます。

1. 標準の更新タイムラインと同じ基本プロセスを使用しますが、プロセスの速度を上げるために追加のスタッフを必要とします。
2. 更新プログラムを送信するために必要な労力を最小限にする、より単純なプロセスを使用します。

いずれのアプローチでも、目標は「更新プログラムが適用されていない」システムが組織のネットワークに接続できる状態である時間を最小限にすることです。つまり、IT プロフェッショナルに既に更新プログラムを受け取っているデバイスに対し、更新プログラムが必要なデバイスを特定し、確認するために必要な記録があることが必要不可欠です。自動化された信頼できる方法でこれを行うことができることは、標準の更新タイムラインにとって有益であり、一方でこれは緊急の更新タイムラインにとっては極めて重要です。

更新プログラム パッケージを作成する

パッケージを作成するためのプロセスは緊急の更新プログラム展開のタイムラインと標準の更新プログラム展開のタイムラインのリリース プロセスの両方について基本的に同じです。しかし、評価の一部として更新プログラムが高リスクと特定された場合、展開チームに更新プログラムの準備のために可能な限り多くの通知をすることが重要です。

パッケージをテストする

更新プログラムの完全なテスト プロセスには、すべてのサポートされているシステム構成が確実にテストされるようにするためにかなりの投資が必要になります。組織によっては、この完全なテスト サイクルが

更新プログラムの展開プロセスにおいて受け入れ難い遅れになることもあります。このような場合、限定的なフィールド テストのオプションがより迅速な展開プロセスを提供する手助けとなることがあります。たとえば、ラボ環境を使用するのではなく、ベータ テスト環境として選ばれたグループの運用システムで緊急の更新プログラムを直接テストする組織もあります。この最初のインストールが正常に行われる限り、完全な展開が義務付けられ、または最新でないコンピューターが組織のネットワークに接続を試行するとすぐに自動的に完全な展開が行われることもあります。

サーバーの更新については、このプロセスは運用サーバー以外で開始し、更新プログラムがこれらの優先度の低いサーバーで確認された後にのみ、運用サーバーに適用します。

パッケージを展開する

緊急の更新タイムラインについて、更新プログラムが最初に提供された時点から、その更新プログラムがオプションから強制的なものとなるまでの時間はおそらく標準の更新タイムラインよりもはるかに短時間であると考えられます。更新プログラムを展開するにあたり数日、または数週間を費やすのではなく、システムのユーザーおよび管理者は更新プログラムが必要となる前のほんの数時間を費やすことになります。これにより、この時期にシステムがオンラインでない状況が発生し、それらのシステムが次に接続する時に、直ちに更新される必要があります。

この状況に対応するためには、IT プロフェッショナルは展開プロセスを監視し、依然として更新プログラムが必要であるクライアントの状態を追跡することが重要です。これはお客様のリスク管理フレームワークにおける最終段階のポイントです。

ステージ 5: システムを監視する

本セクションの内容*:*

- 正常に更新プログラムが適用されたことを確認する
- セキュリティ更新プログラムをアンインストールする
- 実装後のレビュー
- 短期的な緩和策の削除に関するリマインダー

本セクションを終了すると、*IT* プロフェッショナルは次の項目について理解します*:*

- 正常な更新プログラムのインストールを確認する、または拒否する方法
  - スクリプトの使用
  - Microsoft Baseline Security Analyzer (MBSA) の使用
  - ファイル バージョンの確認の使用
  - Microsoft System Center の構成マネージャー
- セキュリティ更新プログラムのアンインストールについてのリソースと方法
- 実装後のレビューについての一般的なステップを理解する

本セクションにおけるマイクロソフトの参照リソース*:*

- マイクロソフト スクリプト センター: technet.microsoft.com/ja-jp/scriptcenter/ee817145.aspx をご覧ください。
- **Microsoft Baseline Security Analyzer (MBSA)**[7] これは小中規模の企業が各自のセキュリティの状態がマイクロソフトのセキュリティの推奨策に準じていることを確認し、特定の改善策のガイダンスを提供する手助けとなるツールです。MBSA は一般的な管理上の脆弱性やコンピューターで不足している更新プログラムを検出する手助けとなります。MBSA は更新プログラムのインストールは実行せず、更新プログラムをスキャンするのみで、更新プログラム管理に Microsoft Update を使用するようコンピューターを構成する機能を持ちます。technet.microsoft.com/ja-jp/security/cc184924.aspx をご覧ください。
- **Configuration Manager in Microsoft System Center:** www.microsoft.com/systemcenter/configurationmanager/ (英語情報) をご覧ください。
- **Microsoft Customer Service & Support (CSS)**: 組織の既存のマイクロソフトのサポート連絡先か、または (1) (866) PC-SAFETY [(1) (866) 727-2338 (米国およびカナダ) で CSS に連絡してください。その他の国については、IT プロフェッショナルは各国のマイクロソフトのオフ

[7] MBSA は、英語、ドイツ語、フランス語、日本語の 4 つの言語にローカライズされていますが、基本となる検出は Microsoft Update および WSUS がサポートしているすべての言語の対象となるコンピューターを正しくスキャンします。

ィスに連絡してください。support.microsoft.com/common/international.aspx をご覧ください。

システムを監視するステージは最新のセキュリティ更新プログラムが正常に展開されているようにし、今後の更新サイクルがスムーズに継続されるようにすることを支援します。図 15 はこの段階で必要となるステップの概要を示しています。

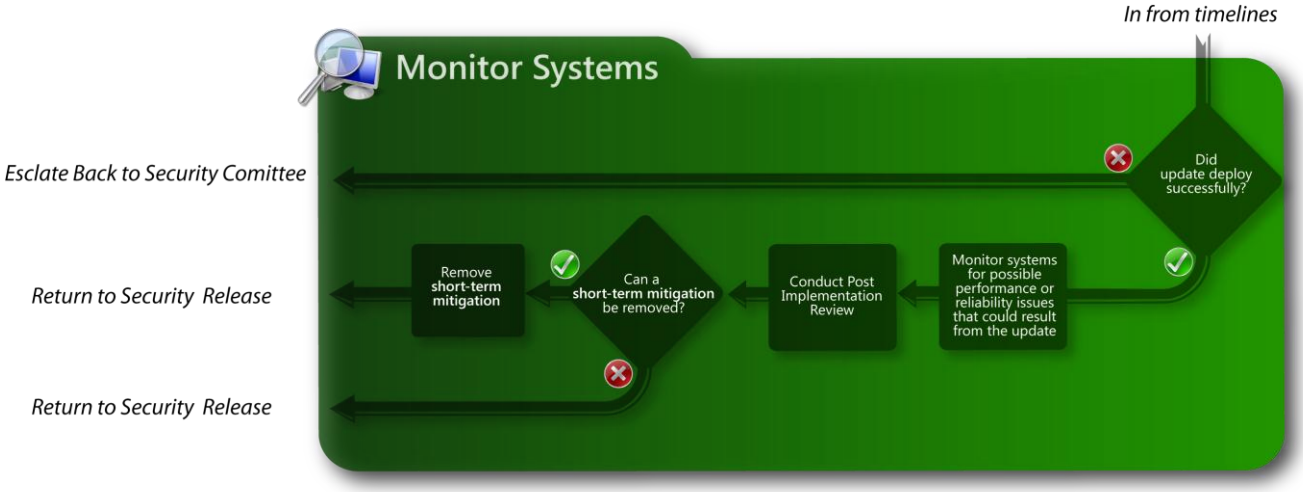


図 15: システムを監視するプロセス

正常な更新プログラムの展開

システムを監視するステージでの最初のタスクは、更新プログラムが正常に展開されたシステムとそうでないシステムを迅速に確認することです。更新プログラムのインストールが次のような理由 (これだけに限りませんが) のため、失敗する可能性があります。

- コンピューターがオフライン
- コンピューターが再構築中、またはイメージ再作成中
- コンピューターに十分なディスク領域がない
- コンピューターが更新サーバーと通信していない
- 必要とされている更新クライアント ソフトウェアがコンピューターで実行されていない
- コンピューターにいくつかの依存するソフトウェアが不足している

理由が何であれ、展開のサポート チームがその他のシステムのトラブルシューティングを支援するために必要とされる可能性があるのはこの時点です。このプロセスによりシステムが更新ウィンドウ外になる場合、組織がさらされるリスクを確認できるように、適切な管理者に情報を提供することが重要です。リス

クが高い状況については、これは正常に更新プログラムが適用されていないシステムがオフラインで手動で更新されるまで、このようなシステムが組織のネットワークから削除される場合もあります。

更新プログラムのインストールを確認する

更新プログラムがシステムに正常にインストールされたかどうかを確認するために、次のようないくつかの方法が使用されます。

コンピューターの管理のレポート: コンピューターの管理システムがセキュリティ更新プログラムのバージョンをレポートする機能をサポートする場合、このオプションは更新プログラムのインストールを確認する通常最も迅速で容易な方法です。

リモート スクリプトのクエリ: 組織のオペレーティング システムの種類によって、IT プロフェッショナルは Windows スクリプト ホスト (WSH) または Windows PowerShell などのスクリプト環境を使用してその状態についてコンピューターをクエリできる場合があります。この方法が正しく機能するためには、確認されるすべてのシステムがスクリプト環境とリモートでのクエリの機能の両方をサポートしていることが重要です。

WSH および Windows PowerShell に関する詳細情報はスクリプト センター technet.microsoft.com/ja-jp/scriptcenter/default.aspx をご覧ください。

IT プロフェッショナルが使用できる Windows PowerShell スクリプトについては www.microsoft.com/technet/scriptcenter/scripts/msh/srvpacks/spms01.mspx (英語情報) をご覧ください。

Microsoft Baseline Security Analyzer (MBSA)[8]: セキュリティ更新プログラムが正常にインストールされたかどうかを確認するための別の優れた方法は、MBSA を使用することです。このツールを構成して、リモートでコンピューターをクエリし、セキュリティ更新プログラムの状態を確認することができます。

最新バージョンの MBSA のダウンロードおよび詳細情報は technet.microsoft.com/ja-jp/security/cc184923.aspx **をご覧ください。**

MBSA はスキャンされた各コンピューターが割り当てられる Update Services サーバーに対し、セキュリティ更新プログラムのスキャンの部分の実行のサポートを提供します。さらに、Update Services サーバーを所有していない組織にスタンドアロンのスキャンを実行します。管理者は Update Services サーバー上の更新プログラムの許可されたリストを無視するか、またはそのリストをもっぱら順守するかについて MBSA のオプションを選択することができます。しかし、既定で、セキュリティ スキャンは

[8] MBSA は、英語、ドイツ語、フランス語、日本語の 4 つの言語にローカライズされていますが、基本となる検出は Microsoft Update および WSUS がサポートしているすべての言語の対象となるコンピューターを正しくスキャンします。

Update Services サーバー上の許可されたセキュリティ更新プログラムのリストに対して、また Microsoft Update カタログで利用可能なセキュリティ更新プログラムの完全なリストに対してのみ行われます。スキャンされたコンピューターについて、Update Services サーバーで許可されていないアイテムは情報スコアのみが提供され、累積的なセキュリティ評価のスコアには考慮に入れられません。許可されてはいますが、対象となるコンピューターにインストールされていないアイテムには適切な警告が出され、セキュリティ上の危険が考慮されます。MBSA は詳細な Update Services オプションを提供し、割り当てられた Update Services サーバーを持たない対象となるコンピューターがヘルプデスクが明確にエラーを特定できるようにエラーを方向できるようにします。コマンド プロンプトで、これは /wa (WSUS により許可されている) オプションにより提供されます。

ファイル バージョンの確認: MBSA または別のツールが IT プロフェッショナルにとってのオプションでない場合、マイクロソフトはサポート技術情報およびセキュリティ情報の「ファイル バージョンの確認」のセクションでそれぞれのパッケージについての情報も提供します。Windows にはいくつかのバージョンやエディションがあるため、次のステップは異なる場合があります。そのような場合、これらのステップを完了するために製品の説明書をご覧ください。しかし、一般的にファイル バージョンの確認は次のステップに従ってください。

1. [スタート] をクリックし (Windows Vista および Windows 7 については、[スタート] は下のアイコンにより表示されます)

   [検索の開始] をクリックし、更新プログラムのファイル名を入力します。
2. **[**プログラム] の下で、ファイル名を右クリックし、次に [プロパティ] をクリックします。
3. [全般] タブで、セキュリティ情報のサポート技術情報で提供しているファイル情報の表とファイルのサイズを比較します。
4. [詳細] タブをクリックし、ファイル バージョンおよび変更された日付などの情報をセキュリティ情報のサポート技術情報で提供しているファイル情報の表と比較することもできます。
5. 最後に、[以前のバージョン] タブをクリックし、新しいまたは更新バージョンのファイルについてのファイル情報と以前のバージョンのファイルについてのファイル情報を比較します。

サポートされているツールのないアプリケーションもあります。このため、ファイル バージョンの確認は正常にインストールが行われたことを確認する唯一の方法となります。

Microsoft System Center の構成マネージャー: 前述のように、より大規模なエンタープライズ組織は MBSA が提供していない追加機能が必要となる可能性があります。このため、Microsoft System Center

の構成マネージャーが MBSA や WSUS が提供していない追加機能を提供する別のソリューションとなります。www.microsoft.com/systemcenter/configurationmanager/ (英語情報) をご覧ください。

コンピューターが正常に更新プログラムのインストールを完了した後でも、時間をとって、更新プログラム適用後の問題で、機能の損失やパフォーマンスの低下の原因になる可能性があるものがないかを監視することを推奨します。

このような問題が受け入れテストが滞りなく行われた後に発生することはまれですが、特に、標準ではないコンピューターの構成またはアプリケーションを実行している可能性のあるクライアント コンピューターでは発生する可能性があります。

セキュリティ更新プログラムをアンインストールする

理由が何であれ、IT プロフェッショナルは迅速にセキュリティ更新プログラムをアンインストールする必要がある場合があります。明らかに、セキュリティ更新プログラムをアンインストールすると、システムやネットワークは脆弱性の影響を受ける可能性のある状態となります。さらに、影響を受けるソフトウェア用のセキュリティ更新プログラムがインストールされていない場合、Microsoft Update で更新プログラムが表示され続けます。それにもかかわらず、表 23 から 25 はさまざまな製品でセキュリティ更新プログラムのアンインストール方法についてのクイック リファレンスの説明を提供しています。

Windows 2000、Windows XP および Windows Server 2003 (すべてのエディション)	Windows Vista、Windows Server 2008 および Windows 7 (すべてのエディション)
[コントロール パネル] の [プログラムの追加と削除] または %Windir%¥$NTUninstallKB[XXXXXX]$¥Spuninst フォルダーの Spuninst.exe ユーティリティを使用します。	WUSA.exe は更新プログラムのアンインストールをサポートしていません。WUSA.exe でインストールした更新プログラムをアンインストールするには、[コントロール パネル] をクリックし、次に [セキュリティ センター] をクリックします。 Windows Update の下で [インストールされている更新プログラムの表示] をクリックし、次に表示されている一覧から削除する必要のある更新プログラムを選択します。

表 23: オペレーティング システムから更新プログラムを削除する手順

Office XP および 2003 Office System (すべてのエディション)	2007 Office System (すべてのエディション)
[コントロール パネル] の[プログラムの追加と削除] を使用します。 **注:** この更新プログラムを削除する場合、Microsoft Office XP の CD を挿入するようメッセージが表示される場合があります。さらに、[コントロール パネル] の [アプリケーションの追加と削除] から更新プログラムをアンインストールするオプションがない場合もあります。この問題について、いくつかの考えられる原因があります。詳細情報は、サポート技術情報 828451 (support.microsoft.com/kb/828451) をご覧ください。	[コントロール パネル] の [プログラムの追加と削除] を使用します。

表 *24: Microsoft Office System* から更新プログラムを削除する手順

Windows 2000 上の Internet Explorer 5.01 SP4 および Internet Explorer 6 SP1	Windows XP および Windows Server 2003 上の Internet Explorer 6、Internet Explorer 7、Internet Explorer 8	Windows Vista および Windows Server 2008 上の Internet Explorer
すべてのサポートされているエディションの Windows 2000 Service Pack 4 上の Internet Explorer 5.01 Service Pack 4 については、HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Updates¥Internet Explorer 5.01¥SP4¥KB[XXXXXX]-IE501SP4-20090303.120000¥Filelist を使用します。	Internet Explorer 6 については、[コントロール パネル] の [プログラムの追加と削除] または %Windir%¥$NTUninstallKB[XXXXXX]$¥Spuninst フォルダーの Spuninst.exe ユーティリティを使用します。 Internet Explorer 7 については、[コントロール パネル] の	WUSA.exe は更新プログラムのアンインストールをサポートしていません。WUSA.exe によりインストールされた更新プログラムをアンインストールするには、[コントロール パネル] をクリックし、次に [セキュリティ センター] をクリックします。[Windows Update] の下の [更新履歴の表示] をクリックし、[インストールされた更新プログラム] をクリックして、更新プロ

すべてのサポートされているエディションの Windows 2000 Service Pack 4 については、HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Updates¥Internet Explorer 6¥SP1¥KB[XXXXXX]-IE6SP1-20090303.120000¥Filelist を使用します。	[プログラムの追加と削除] か %Windir%¥ie7updates¥KB[XXXXXX]-IE7¥spuninst の Spuninst.exe ユーティリティを使用します。 Internet Explorer 8 については [コントロール パネル] の [プログラムの追加と削除] または %Windir%¥ie8updates¥KB[XXXXXX-IE8¥spuninst フォルダーの Spuninst.exe ユーティリティを使用します。	グラムの一覧から選択します。 Wusa.exe に関する詳細情報は support.microsoft.com/kb/934307 をご覧ください。

表 25: Interent Explorer から更新プログラムを削除する手順

IT プロフェッショナルがセキュリティ情報および関連するサポート技術情報を参照しても、なおセキュリティ更新プログラムがアンインストールできない場合、組織の既存のマイクロソフトのサポートへの連絡先か、または (1) (866) PC-SAFETY [(1) (866) 727-2338 米国およびカナダ] に電話連絡し、CSS に連絡をとってください。それ以外の国については、IT プロフェッショナルは各国のマイクロソフトのオフィスに連絡してください。support.microsoft.com/common/international.aspx をご覧ください。

チームはケースに特定の情報を収集し、問題の評価や解決策の特定を支援することができます。

実装後のレビューを行う

実装後のレビューは更新プログラム管理プロセスに行う必要のある改善を確認するため、通常、リリースされた更新プログラムの展開から 1 週間から 4 週間以内に行う必要があります。通常、セキュリティ更新プログラム展開の重要なメンバーおよびサポート チームがこのレビューを行います。レビューに推奨される議題となるトピックには次があります。

- 脆弱性が脆弱性のスキャン レポートおよびセキュリティ ポリシーの標準に追加されたことを確認します。
- ビルド イメージおよびオフラインの仮想マシンのドライブ ファイルが更新され、展開後に最新のセキュリティ更新プログラムを含んでいることを確認します。
- 計画された結果と実際の結果について討議します。
- リリースに関連するリスクについて話し合います。
- インシデント全体の組織のパフォーマンスをレビューします。これを組織のレスポンス プランを向上させ体験から学んだものを含む機会とします。
- サービス ウィンドウへの変更について討議します。

- 更新システムが組織の必要条件に現在でも合っているかどうかを確認します。
- ダウンタイムや復旧の費用など、インシデントによる損害やコストを評価します。
- 環境について、別のベースラインを作成するか、または既存のベースラインを更新します。

このミーティングの全体の目標は、更新プロセス中に得た教訓を伝え、今後の更新プロセスに統合することです。

短期的な緩和策を削除する

次のリリースのために全体のプロセスをリセットする前の最終ステップは、不要になった短期的な緩和策の削除です。通常、短期的な緩和策は組織の通常の運用にいくらかの影響があります。組織のシステムが危険にさらされている間、この影響は容認できます。しかし、更新プログラムが正常に適用された後は、緩和策を削除して組織を通常の運用に戻す必要があります。

進行中のステージ: 監視する

本セクションの内容*:*

- マイクロソフト セキュリティ情報およびアドバイザリへのメジャーな改定とマイナーな改定
- 悪意のあるソフトウェア (マルウェア) の脅威と戦うことを支援するマイクロソフトのリソース

本セクションを終了すると、*IT* プロフェッショナルは次の項目について理解します*:*

- セキュリティ情報およびアドバイザリのメジャーおよびマイナーな改訂を理解しています。
  - これらは何を意味するか
  - IT プロフェッショナルがどのように改訂の最新情報を常に受けることができるか
  - 改訂された場合、セキュリティ情報およびアドバイザリのどの個所を見るか
- Microsoft Malware Protection Center (MMPC) とは、マイクロソフトの権威筋で、Windows プラットフォームのマルウェア対策のリサーチ、保護、ガイダンスについてのグローバルな意見です。MMPC には次のような多くのリソースおよびソリューションがあります。
  - マイクロソフト セキュリティ インテリジェンス レポート
  - Microsoft Malware Protection Center Blog およびセキュリティ ポータル
  - Microsoft Windows 悪意のあるソフトウェアの削除ツール
  - Windows Defender.
- その他のマイクロソフトのセキュリティ リソース

本セクションにおけるマイクロソフトの参照リソース*:*

- **マイクロソフト セキュリティ インテリジェンス レポート:** 何億もの Windows ユーザーから得られたデータを活用する半年に 1 度の報告で、ソフトウェアの脆弱性の公開、悪用コード、悪意のあるソフトウェア、迷惑ソフトウェアである可能性のあるものなど、変化する脅威の展望に関する綿密な見解を提供します。www.microsoft.com/japan/sir をご覧ください。
- **Microsoft Malware Protection Center (MMPC) セキュリティ ポータル:** この Web サイトには、脅威に関する詳細、悪意のあるソフトウェアのエンサイクロペディア、悪意のあるソフトウェアのツールおよびリソース、悪意のあるソフトウェアの送信メカニズムのサンプルなどが含まれています。www.microsoft.com/security/portal/ (英語情報) をご覧ください。
- **Microsoft Malware Protection Center (MMPC) ブログ:** このブログには MMPC のトピックの専門家からのリアル タイムのコミュニケーションが含まれており、新たに現れる目につく悪意のあるソフトウェアの脅威やコンピューター セキュリティの分野におけるその他のリサーチ トピックを取り扱っています。blogs.technet.com/mmpc/ (英語情報) をご覧ください。
- **Microsoft Windows 悪意のあるソフトウェアの削除ツール (MSRT):** MSRT はサポートされている Windows オペレーティング システムを実行するコンピューターについて、特定の蔓延している悪意のあるソフトウェアによる感染を確認し、感染が確認された場合それを駆除することを

支援します。http://www.microsoft.com/japan/security/malwareremove/default.mspx をご覧ください。

- **Windows Defender:** このソフトウェアはポップアップ ウィンドウ、遅いパフォーマンス、スパイウェアやその他の望ましくない可能性のあるソフトウェアが原因となるセキュリティ上の脅威に対しコンピューターを保護する手助けとなります。
- **Trustworthy Computing (TwC) Security and Privacy Blog の集合ページ:** このページは動的にセキュリティおよびプライバシーのブログを統合し、取り上げます。www.microsoft.com/twc/blogs （英語情報） をご覧ください。
- **セキュリティ Solution Accelerator:** IT プロフェッショナルがプロアクティブにセキュリティインフラストラクチャを計画し、統合し、運用する手助けとなるツールやガイダンスを無償で提供しています。technet.microsoft.com/ja-jp/solutionaccelerators/cc835245.aspx をご覧ください。
- **セキュリティ リスク管理ガイド:** リスク管理に 4 段階のアプローチを提供する技術にとらわれないソリューションです。このガイドはセキュリティ上のリスクについての多くの業界が受け入れている標準を参照し、マイクロソフトの IT およびパートナーによる実際の経験を統合しています。technet.microsoft.com/ja-jp/library/cc163143.aspx をご覧ください。
- **IT Infrastructure Threat Modeling Guide:** IT インフラストラクチャのセキュリティにおける投資の優先順位を決定する手助けとなる脅威のモデルを作成するための方法です。このガイドは SDL の脅威のモデルについて存在している広範な方法論を説明し、検討しています。またその方法論を使用して IT インフラストラクチャ向けの脅威のモデルのプロセスを確立します。go.microsoft.com/fwlink/?LinkId=154010 (英語情報) をご覧ください。

残念ながら、セキュリティ更新プログラムが正常に展開されても、セキュリティ管理の職務が終わるわけではありません。今日の進化する脅威の動向では、常に警戒している状態にあることはやむをえません。このガイドの前半の「ステージ 1 マイクロソフトのセキュリティ リリースの通知を受け取る」で説明したように、Microsoft Technical Security の通知と MSRC ブログの警告は、皆さんの組織のセキュリティに対する姿勢に関連するマイクロソフトからのニュースやコミュニケーションの最新情報を提供します。

メジャー、またはマイナーな小さなセキュリティ情報およびアドバイザリの改訂

マイクロソフトのセキュリティに関する通知を受け取るようサインアップしている場合、セキュリティ情報またはセキュリティ アドバイザリの公開後に改定された場合、マイクロソフトからその旨を通知する電子メール メッセージを受け取ることができます。

メジャーな改定はより顕著で、リリース バイナリに影響する場合もあります。このような場合、通常 IT プロフェッショナルがセキュリティ更新プログラムを再インストールする必要があります。多くの場合、セキュリティ情報の影響を受けるソフトウェアや影響を受けないソフトウェアのセクションに製品が追加された場合、または削除された場合にメジャーな改定が行われます。また特定の製品についての深刻度が改定された場合にも行われます。このため、セキュリティ情報またはアドバイザリのメジャーな改定の通知を受けた場合、注意深くその通知を読み、必要なアクションを行うことが重要となります。

マイナーな改定は多くの場合、セキュリティ情報本文の文脈が変更された場合に行われるため、組織のセキュリティを妨げることはありませんが、IT プロフェッショナルはその改定内容に注意を向ける必要があります。さらに、マイクロソフトは事実に影響のない改定やスペル ミスの修正については IT プロフェッショナルに通知することはありません。

セキュリティ情報およびセキュリティ アドバイザリの改訂を確認する別の方法は、文書そのものを確認することです。改訂については 2 箇所に記載されています。

1. セキュリティ情報またはアドバイザリのヘッダー （図 16 をご覧ください。）

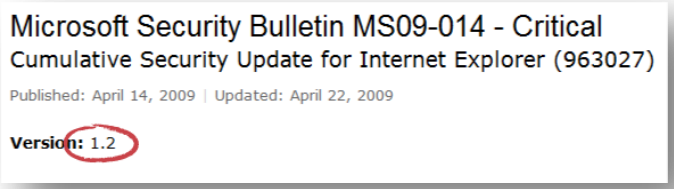


図 *16:* セキュリティ情報のヘッダー

2. セキュリティ情報のフッター。こちらには変更履歴の詳細を記載しています。(図 17 をご覧ください。)

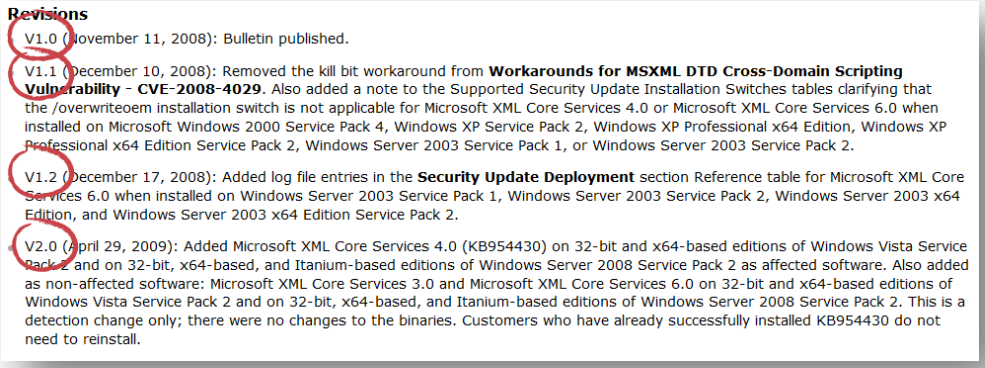


図 17: セキュリティ情報のフッター

すべてのセキュリティ情報およびアドバイザリは最初に 1.0 として公開されます。マイナーな改定が行われるごとに X.1 が増え、メジャーな改定が行われると 1.X が増えます。このため、2.3 と記されたセキュリティ情報およびアドバイザリは 1 回のメジャーな改定と 3 回のマイナーな改定が行われたことになります。

悪意のあるソフトウェアによる恒常的な脅威

犯罪者は多くの言語および多くの異なる国々のユーザーやコンピューターを標的にしたソフトウェアを作成しているため、悪意のあるソフトウェアおよび望ましくない可能性のあるソフトウェアはますます世界的な現象となっています。これらの脅威が悪用し続けるものは、Web ブラウザーやオペレーティング システムに存在する問題よりもはるかに人間の本質やソフトウェア アプリケーションの方が多いです。マイクロソフトはそのオペレーティング システムおよびアプリケーションを SDL により安全にすることを進めているため、犯罪者は自身のソフトウェアを標的となるコンピューターに侵入させようという目的で、焦点をサードパーティのアプリケーション、ブラウザーのアドオン、人間の感情に移しています。

犯罪者がこの傾向を悪用する方法で特に際立ったものは、ユーザーに悪意のある偽のウイルス対策やスパイウェア対策のソフトウェアをダウンロードさせ、インストールさせることです。犯罪者が標的となるユーザーにこの詐欺的なセキュリティ ソフトウェアをインストールするよう誘導した後、犯罪者はそのユーザーのクレジット カードの詳細を取得したり、感染したコンピューターにさらに悪意のあるソフトウェアをダウンロードするための道筋を確立する可能性があります。マイクロソフトのセキュリティ製品およびサービスは 2008 年下半期に1,000 万台もの世界中のコンピューターから詐欺的なセキュリティ ソフトウェアを削除しました。また今後もこれらの脅威に対応し続けていきます。

マイクロソフト マルウェア対応センター (MMPC) はWindows プラットフォームにおけるマルウェア対策のリサーチ、保護およびガイダンスについての信頼できるグローバルな意見です。特に、このグループはマイクロソフト セキュリティ インテリジェンス レポート (SIR) (www.microsoft.com/japan/sir をご覧ください。SIR は変化する脅威の動向に関する綿密な見解を提供しています。) の主要な貢献者です。SIR にはソフトウェアの脆弱性の公開と悪用の傾向、セキュリティおよびプライバシーの侵害、悪意のあるソフトウェアおよび望ましくない可能性のあるソフトウェア、電子メール、スパム、フィッシングの傾向を詳細に分析しています。各レポートは各カレンダー月の前半および後半で確認されたデータと傾向に焦点を当てており、履歴データを使用してコンテキストを提供しています。SIR の目的は IT プロフェッショナルに脅威の動向における主な傾向に関する最新情報を提供し続け、IT プロフェッショナルがこれらの脅威に直面した場合のセキュリティに対する姿勢を強化する手助けとなる価値ある洞察とセキュリティ ガイダンスを提供することです。

組織が通常の運営を行っている間、脆弱性を悪用する新しい悪意のあるソフトウェアについて常に最新情報を得ているようにするためのステップを行う必要があります。サポートが必要な場合、次の悪意のあるソフトウェアに関するリソースが役に立ちますのでご覧ください。

- **MMPC セキュリティ ポータル:** これは包括的な Web サイトで上位を占める脅威の詳細、詳細な悪意のあるソフトウェアのエンサイクロペディア、悪意のあるソフトウェアに関するツールおよびリソース、悪意のあるソフトウェアの送信メカニズムのサンプルが含まれています。www.microsoft.com/security/portal (英語情報) をご覧ください。
- **MMPC ブログ:** これは MMPC の内容についての専門家にお客様とのコミュニケーションを図るためのリアル タイムの方法を提供します。トピックには、コンピューター セキュリティの分野におけるその他のリサーチ トピックとともに、新しく出現する、目につく悪意のあるソフトウェアの脅威に関する「背景となる」情報も含まれています。blogs.technet.com/mmpc/ (英語情報) をご覧ください。
- **Microsoft Windows 悪意のあるソフトウェアの削除ツール (MSRT):** これは、お客様のコンピューターから蔓延する悪意のあるソフトウェアのファミリを特定し、駆除することを支援する無償のツールです。MSRT は「重要」な更新プログラムとして Windows Update、Microsoft Update、自動更新から公開されます。ツールのバージョンも、マイクロソフト ダウンロード センターから利用可能です。MSRT は Windows Vista、Windows XP、Windows Server 2008、Windows Server 2003 および Windows 2000 を実行するコンピューターから特定の蔓延する悪意のあるソフトウェアを削除する手助けとなります。2008 年 18 日以来、このツールは 119 種類の悪意のあるソフトウェアのファミリを検出、削除しています。これらのほとんどが現在蔓延しているか、または追加された時点で蔓延していたものです。検出および削除のプロセスが完了すると、ツールは悪意のあるソフトウェアが検出、削除されたかを含む結果を説明する報告を表示します。www.microsoft.com/japan/security/malwareremove/default.mspx をご覧ください。

  注: MSRT にはリアルタイムの保護はなく、具体的に選択されている蔓延している悪意のあるソフトウェアを対象にできるマイクロソフトのウイルス対策の定義データベースの部分のみを使用するため、MSRT は最新のウイルス対策ソリューションの代わりとなるものではありません。
- **Windows Defender:** このソフトウェアは、ポップアップ ウィンドウ、遅いパフォーマンス、スパイウェアやその他の望ましくない可能性のあるソフトウェアが原因となるセキュリティ上の脅威からコンピューターを保護します。既知のスパイウェアをコンピューターで検出し、削除することにより、これを行います。Windows Defender にはリアルタイム保護という機能があり、これはスパイウェアが検出された場合、推奨されるアクションを提示し、中断を最小限にし、ユ

ーザーの生産性を保つことを支援する監視システムです。
www.microsoft.com/windows/products/winfamily/defender (英語情報) をご覧ください。

その他のセキュリティ リソース

Microsoft Trustworthy Computing (TwC) Group Security and Privacy Blog の集合ページ: このページはマイクロソフトの信頼できるコンピューティング (TwC) グループ (さらに安全で、プライバシーが保たれ、信頼できるコンピューティング エクスペリエンスを提供すべく取り組んでいるチームです) によるブログを動的に統合し、掲載しています。マイクロソフトのコンピューティングのプライバシーとセキュリティに関する長期的な展望および戦略についてご覧ください。

Trustworthy Computing (TwC) Security and Privacy Blog の集合ページは
www.microsoft.com/twc/blogs （英語情報） をご覧ください。

セキュリティ Solution Accelerator はツールとガイダンスの集まりです。これらは無償の権威あるリソースで、IT プロフェッショナルがプロアクティブにセキュリティ インフラストラクチャのプランを立て、統合し、運用する手助けとなります。http://technet.microsoft.com/ja-jp/solutionaccelerators/cc835245.aspx をご覧ください。

以前に説明した **Security Risk Management Guide** は、技術にとらわれないソリューションで、リスク管理に 4 段階のアプローチを提供しています。このガイドはセキュリティ上のリスク管理について多くの業界が受け入れている標準を参照し、マイクロソフト IT による実際の経験を統合しており、またマイクロソフトの IT プロフェッショナルやパートナーからのインプットも含まれています。
http://technet.microsoft.com/ja-jp/library/cc163143.aspx をご覧ください。

IT Infrastructure Threat Modeling Guide は、IT インフラストラクチャ セキュリティにおいて、投資の優先順位を決定する手助けとなる脅威のモデルを作成するための、容易に理解できる方法を提供します。このガイドは SDL の脅威のモデルについて存在する広範な方法論を説明し、検討しています。またその方法論を使用して IT インフラストラクチャ向けの脅威のモデルのプロセスを確立します。
go.microsoft.com/fwlink/?LinkId=154010 (英語情報) をご覧ください。

概要

セキュリティ更新プログラムの展開プロセスは、インターネットに接続しているすべての環境において、システム管理の日常業務に必要な部分となりました。犯罪者は今やマイクロソフトばかりでなく、さまざまなベンダーによるオペレーティング システムやアプリケーションを、その悪意のあるソフトウェアの標的としています。このため、組織のシステムとアプリケーションを更新された状態に保たないと、ユーザーが犯罪者や犯罪者が開発した悪意のあるソフトウェアによる攻撃の深刻な危険にさらされることになる可能性があります。

完全なマイクロソフトのセキュリティ更新プログラム公開および適用のプロセスの図はこのガイドの付録をご覧ください。

マイクロソフトのソフトウェアに存在する脆弱性に対し、マイクロソフトは効果的でタイムリーな対応を提供することをお約束しています。マイクロソフトは多くの業界のパートナーと協力し、お客様が業界を先導するレベルの保護を受け取り、お客様のコンピューターを攻撃しようとする犯罪者に対抗できるようにします。

このガイドでマイクロソフトが提供している情報は、皆さんのリスク管理での決定をサポートすることを意図しています。このガイドは IT プロフェッショナルが、生産性に対する最小限の中断でセキュリティ更新プログラムを組織全体に迅速に適用するにあたり役立つ、マイクロソフトが提供するすべてのコミュニケーション、ガイダンス、プログラムおよびサービスを理解し、活用し、最大限にすることを支援するよう作成されています。

このトピックおよびその他のセキュリティ関連のトピックに関する最新の情報については http://www.microsoft.com/japan/security/msrc/default.mspx または http://technet.microsoft.com/ja-jp/security/default.aspx をご覧ください。

フィードバック

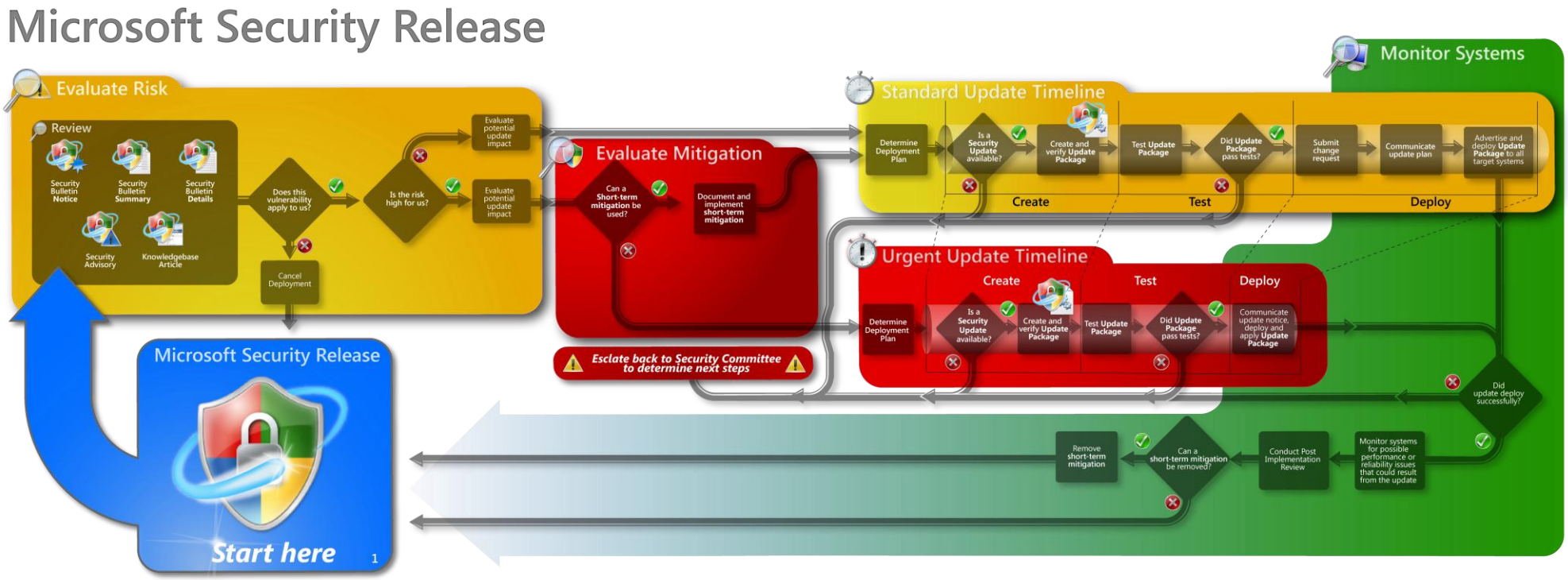
このガイドをご覧いただきましてありがとうございます。このガイドの著者は、皆さんのニーズにさらによく応えるにはどのようにしたら良いかフィードバックやご意見をお待ちしています。マイクロソフトがこのコンテンツをどのように改善できるかに関するフィードバックやご意見をご自由にお寄せください。

Trustworthy Computing Security Update Guide チーム twcsecfb@microsoft.com までフィードバックをお寄せください。

付録

このページは意図的に空白にしています。

マイクロソフトのセキュリティ更新プログラムの公開および展開のプロセスの図



用語集および一般的に使用される用語

この用語集はマイクロソフトのセキュリティ更新プログラムの公開と展開のプロセスに関し、中核となる概念および技術を説明しています。悪意のあるソフトウェアの用語に関する詳細情報は、Microsoft Malware Protection Center (MMPC) のポータルをご覧ください。
www.microsoft.com/security/portal/encyclopedia.aspx (英語情報) をご覧ください。

有効なソフトウェアのセキュリティ保護

有効なソフトウェアのセキュリティ保護は、マイクロソフトのシステムへの侵入を検出または保留にすることができます。また、悪用されている問題に対しマイクロソフトのセキュリティ更新プログラムが利用可能でない場合 (例: 悪意のある動作を引き起こしているウイルス対策の定義や悪用の試行を阻止する IDS 署名など) にマイクロソフトのシステムを悪用の試行から保護することができます。

バイナリ

更新プログラムの 2 つの基本的なコンポーネントは、更新プログラムのバイナリと更新プログラムのメタデータ ファイルです。バイナリは更新プログラムの実行可能ファイルで、特定の更新プログラムには 1 つ、または複数の更新プログラムのバイナリが含まれています。更新プログラムのメタデータ ファイルは、更新プログラムをインストールする日時や方法とともに、更新プログラムに関する基本的な情報が含まれている XML 形式の文書です。

制御

組織的な、手順上の、または技術的なリスク管理の方法で、保護や対策の同義語です。

対策

コンピューター環境におけるリスクを削減するソフトウェアの構成、ハードウェア、手順です。保護や緩和策とも呼ばれています。

重要な更新プログラム

特定の問題に対し広範囲に公開された修正プログラムで、Microsoft Windows 悪意のあるソフトウェアの削除ツール (MSRT) 用の更新など、重要かつセキュリティ関連以外の問題に対応します。

注: 「重要な更新プログラム」と深刻度「緊急」と評価されている (マイクロソフト セキュリティ情報にて) セキュリティ更新プログラムがあります。これら 2 つはマイクロソフトの異なる更新プログラムです。その差異に関する詳細情報は、上記の「マイクロソフトのソフトウェアの更新プログラムの用語」をご覧ください。

多層防御

1 つのセキュリティ コンポーネントがエラーとなった場合でも保護できるよう、複数の層のセキュリティを使用するアプローチです。

サービス拒否

正当なユーザーによるサービスまたはコンピューターの使用を妨げようとする、明白な試みです。

特権の昇格

特権を持たないユーザーが特権のあるアクセスを取得する状況です。特権の昇格の例として、特権を持たないユーザーが管理者グループに追加される方法を企てることがあります。

悪用コード

ソフトウェア プログラムまたはサンプル コードで、これが脆弱性の影響を受けるコンピューターに対し実行された場合、脆弱性を悪用して攻撃者の ID のなりすまし、ユーザーまたはコンピューターの情報の改ざん、攻撃者の操作の拒否、ユーザーまたはコンピューターの情報の公開、有効なユーザーへのサービスの拒否、攻撃者の特権の昇格を行います。

Feature Pack

新しい製品の機能で通常次の完全な製品のリリースに含まれます。Feature Pack には新しいセキュリティ機能や改善点が含まれる場合があります。

機能する悪用コード

脆弱性の最も深刻なセキュリティ上の影響を実行可能にする悪用コードです。たとえば、脆弱性の影響がリモートでのコードの実行である場合、機能する悪用コードは、標的となるコンピューターで実行された場合、リモートでコードを実行できます。

ホットフィックス

1 つまたは複数のファイルで構成されている単一のパッケージで、製品に存在する問題を解決するために使用されます。ホットフィックスは特定のお客様の状況に対応するもので、マイクロソフトとのサポート関係を通してのみご利用いただけます。また、マイクロソフトからの書面での法的な同意なしに、お客様の組織外に配布できない場合もあります。QFE (Quick Fix Engineering の更新プログラム)、パッチ、および更新プログラムという用語は、ホットフィックスと同義語として過去に使用されていました。

影響

資産に対して、脅威が脆弱性を悪用した場合に予測される企業全体の損失。

セキュリティ以外の更新プログラム

セキュリティに関連しないすべてのソフトウェアの更新プログラムです。マイクロソフトは特に、定例のセキュリティ更新プログラムのリリース サイクル中にセキュリティ以外の更新プログラムを公開しています。これは、Microsoft Outlook 迷惑メール フィルターの更新プログラムなど、いくつかのセキュリティ以外の更新プログラムは Microsoft Update によりセキュリティ更新プログラムと同時に公開されるためです。

オプションの更新プログラム

オプションの更新プログラムには、お客様のコンピューティング エクスペリエンスを向上させる更新プログラム、ドライバー、またはマイクロソフトやそのパートナーからの新しいアプリケーションが含まれています。これらの更新プログラムは手動でインストールする必要があります。つまり、オプションの更新プログラムは自動でダウンロードまたはインストールされませんが、Windows Update でこれらはレビューのために表示されます。

セキュリティ更新プログラム

製品に固有のセキュリティ関連の脆弱性に対し広範に公開された修正プログラムです。セキュリティ上の脆弱性はその深刻度に基づき評価されます。この深刻度は MSRC により割り当てられ、マイクロソフト セキュリティ情報に、「緊急」、「重要」、「警告」、「注意」として記載されます。(深刻度の詳細はこのガイドで前述しています。)

サービス パック

製品のリリース以降に社内で確認された問題に対する追加の修正プログラムとともに、テストされた累積的な修正プログラム、セキュリティ更新プログラム、重要な更新プログラムおよび更新プログラムを含みます。また、サービス パックはお客様からリクエストされた設計の変更や機能が、限定された数で含まれている場合もあります。

ソフトウェアの更新プログラム

ソフトウェアの更新プログラムとは、マイクロソフト コーポレーションがリリースするソフトウェア製品を改善または修正するために使用されるすべての更新プログラム、更新プログラムのロールアップ、サービス パック、Feature Pack、重要な更新プログラム、セキュリティ更新プログラム、ホットフィックスです。

置き換え

この用語は、セキュリティ情報で提供している新しいセキュリティ更新プログラムが古いセキュリティ情報の別のセキュリティ更新プログラムを置き換えることを指しています。置き換わる場合、新しいセキュ

リティ更新プログラムのバイナリは最新のセキュリティ上の脆弱性に対する修正プログラムに加え、古いセキュリティ更新プログラムの修正も含んでいます。過去に、必要であるものは新しい更新プログラムのみである場合でも、新しいセキュリティ更新プログラムと過去に公開されたセキュリティ更新プログラム (ともに同じ修正を含んでいる) の両方とも「必要である」とされていることがありました。

更新プログラムのロールアップ

テストされた累積的なホットフィックスのセット、セキュリティ更新プログラム、重要な更新プログラム、および更新プログラムが、適用が容易になるよう一緒にパッケージされたものです。ロールアップは通常、セキュリティまたは製品のコンポーネントなどの特定のエリアを対象にしています。特に、更新プログラムのロールアップのよい例としては、サービス パックがあります。

アップグレード

アップグレードとは、インストールされている製品のバージョンを、同じ製品のより新しいバージョンに置き換えるソフトウェアのパッケージを指します。アップグレードのプロセスは通常、既存のお客様のデータと設定をそのままにしながら、既存のソフトウェアを新しいバージョンと置き換えます。

Windows Update エージェント (WUA)

Windows Update エージェント (WUA) API は COM インターフェイスのセットで、システム管理者およびプログラマーが Windows Update や Windows Server Update Services (WSUS) にアクセスできるようにします。コンピューターに現在利用可能な更新プログラムを確認したり、更新プログラムをインストール、またはアンインストールするためのスクリプトやプログラムを書くことができます。

回避策

回避策のセクションには、皆さんが環境に更新プログラムを適用するまで脅威を緩和する手助けとなるよう、マイクロソフトがテストした回避策に関する情報が含まれています。このセクションをリスク評価の一部としてご覧いただく必要があります。