



# IPSの活用による Patch Tuesday問題の克服

# Contents

本書の内容

|                               |   |
|-------------------------------|---|
| はじめに .....                    | 3 |
| Patch Tuesdaysという慣行の始まり ..... | 3 |
| Patch Tuesdayモデルの問題点 .....    | 3 |
| 適時性の欠如 .....                  | 4 |
| パッチ公開スケジュールが予測可能 .....        | 4 |
| 日々のシステム運用への影響 .....           | 5 |
| より効果的なアプローチ .....             | 5 |

## はじめに

今日、セキュリティ・パッチと「Patch Tuesday」の問題は、システム管理者にとって、最もストレスを感じる大きな課題の1つとなっています。

Microsoftなどのベンダー各社がソフトウェアのパッチを公開する毎月第2火曜日（日本時間では水曜日）は、IT技術者の間で「Patch Tuesday」（パッチの火曜日）と呼ばれています。Patch Tuesdayのようなパッチの提供方法は、少なくともいくつかの点においてはセキュリティの向上に役立っています。その一方、システム管理者にとってはさまざまな混乱の原因になっていることから、Patch Tuesdayは一部で「報いを受けるとき」などとも呼ばれています。

しかしセキュリティ・パッチは、脆弱性の問題に対処する唯一の方法というわけではありません。最近では、パッチよりも効果的に脆弱性を保護できる手段として、侵入防御（IPS）技術が注目を集めています。IPSは、ネットワーク環境に影響を与えることなく、脆弱性に対する攻撃をリアルタイムで防御します。この技術白書では、Patch Tuesdayが抱える本質的な問題点と、IPSが提供する事前対応型の防御技術の重要性について解説します。

## Patch Tuesdaysという慣行の始まり

Patch Tuesdaysという仕組みは突然誕生したわけではありません。Microsoftは、Windows 98以降から、Windowsやそのコンポーネントに対するパッチが提供されているかどうかを自動チェックする「Windows Update」機能をオペレーティング・システムに搭載しています。

この仕組みは、対照的なユーザ層に影響する2つの問題を抱えていました。1つは、初心者ユーザはWindows Updateの存在を知らず、アップデートを実行しないということ。もう1つは、大規模企業などでWindowsを管理している上級ユーザにとって、Windows Updateを使用してネットワーク上に存在するすべてのシステムを最新の状態に保つのは容易ではないということです。

その後が始まったPatch Tuesdaysでは、1か月の間セキュリティ・パッチを公開せずに累積させておき、毎月第2火曜日にまとめて公開するという方法が採用されました。これによりシステム管理者は、パッチをテストおよび導入するための準備を前もって行えるようになりました。

他のいくつかのベンダーもMicrosoftに追随し、同様の方法でパッチを公開しています。先ごろ確認したところでは、毎月第2火曜日に何らかのパッチを公開しているベンダーは、主要なところだけで20数社に上っていました。このパッチ提供方法は、大局的に見ればネットワークのセキュリティを向上させるのに役立っているといえます。しかしそれと同時に、セキュリティを低下させるおそれのあるいくつかの重要な問題を内包しているのです。

## Patch Tuesdayモデルの問題点

セキュリティ業界では、「システム管理者が我を忘れて熱弁をふるう姿を見なければ、Patch Tuesdayにどう対処しているか尋ねてみればいい」などという冗談がささやかれています。また一部では、Patch Tuesdayは「Black Tuesday」（黒い火曜日）などとも呼ばれています。Patch Tuesdayがどのように何かと物議を醸しているのはなぜでしょうか。なぜ否定的な見方をされることが多いのでしょうか。構想自体に問題はないにもかかわらず、最も基本的な脅威すら防御できないことがあるのはなぜなのでしょう。

3つ目の疑問は、とりわけ重い問いかけです。Verizon Businessが先ごろ発表したレポートによると、ほとんどのセキュリティ侵害は被害が発覚するまでに数か月を要しており、その間、問題は修正されないままとなっています<sup>1</sup>。これはつまり、数年とは言わないまでも数か月の間、攻撃を受け続ける可能性があるということを意味します。

## チェック・ポイントが提供するIPS技術

- IPS-1：IPSに特化したスタンドアロン型のソリューション
- SmartDefense：チェック・ポイントの主要セキュリティ・ゲートウェイ製品に統合されたIPS技術
- SmartDefenseサービス：防御機能のアップデートを提供

1：2008 Data Breach Investigation Report, Verizon Business.

これらの問いに対する答えは、パッチを定期公開することに付随する本質的な弱点に隠されています。Patch Tuesdayは、「適時性に欠ける」、「ハッカーが攻撃の計画を立てやすくなる」、「日々のシステム運用に影響を与える」という3つの大きな問題を抱えています。総合的に見てパッチは、脆弱性によってもたらされる問題への完全な解決策にはなっていないのです。

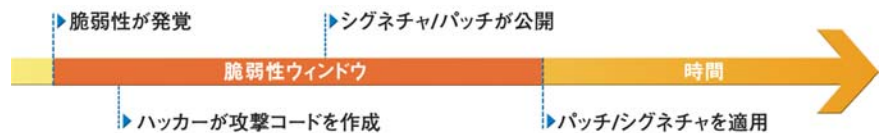
### 適時性の欠如

Patch Tuesdayの1つ目の大きな問題は、適時性に欠けることです。パッチは一定のスケジュールに従ってリリースされるため、Microsoftをはじめとするベンダー各社は、次のPatch Tuesdayに間に合うようにパッチを開発します。もし脆弱性が発見されたのがPatch Tuesdayの直前であった場合、パッチの開発が直近のPatch Tuesdayに間に合わず、次回に持ち越されてしまうかもしれません。この場合、パッチの公開は1か月、もしくはそれ以上遅れることになります。厄介な脆弱性であれば、数年にわたってパッチが提供されないままということもあり得ます。

ベンダー各社は、脆弱性の内容が深刻である場合には定例外のパッチを緊急リリースすることで、この問題に対処しようとしています。しかし、定例外のパッチは管理者にとって混乱の元以外の何ものでもなく、もし定例外のパッチが日常的にリリースされることになれば、突然公開されるパッチに慌てて対応するというPatch Tuesday以前の状態に逆戻りすることになります。

### パッチ公開スケジュールが予測可能

2つ目の問題は、パッチを定期公開するという仕組みの性質上、そのリリース・スケジュールが予測可能であることです。ハッカーは、毎月第2火曜日にパッチが公開されることを認識しており、この情報を利用して「脆弱性ウィンドウ」の間に攻撃を仕掛けようとしています。脆弱性ウィンドウとは、「脆弱性が発見されてからその修正パッチが組織全体に適用されるまでの期間」のことをいいます。注意が必要なのは、「修正パッチが公開されるまでの期間」ではないことです。企業などでは、パッチが公開されたからといってすぐに適用されるとは限らず、また適用されたとしても一部に適用漏れが生じる可能性があるからです。Verizon Businessの最近のレポートによると、調査対象となったセキュリティ侵害事件の71パーセントは既知の脆弱性が狙われたものであり、その脆弱性を修正するパッチは1年以上前に公開されています<sup>2</sup>。



ハッカーの立場からすると、この脆弱性ウィンドウが最も成功率の高い時期とすることになる。

2: 前掲書の1 2008 Data Breach Investigation Report, Verizon Business.

一部のハッカーは、ほとんどの組織はすべてのパッチをすぐに適用したりはしないということを認識したうえで、Patch Tuesday直後に攻撃コードを作成し始めます。このことから、翌日の水曜日は「Exploit Wednesday」(攻撃の水曜日)などと呼ばれています。Patch Tuesday直後にパッチ未公開の脆弱性を突く攻撃を開始すれば、ベンダーがその修正パッチを公開するまでの間、ハッカーは29日間という時間を稼ぐことができます。

ハッカーの中には、Patch Tuesdayの直後を狙って脆弱性を攻撃し始める者もいます。Microsoftは基本的に、次回のPatch Tuesdayまでその脆弱性を修正するパッチを公開しないからです。これにより脆弱性ウィンドウはさらに長くなり、場合によっては、脆弱性のあるシステムを攻撃する時間が1か月以上もハッカーに与えられることになります。

## 日々のシステム運用への影響

3つ目の大きな問題は、システムの運用に大きな影響を与える場合があることです。組織のすべてのシステムにパッチを適用するまで、脆弱性対策は万全になりません。1つのマシンに1つのパッチを適用し忘れるだけで、組織全体が危険にさらされる可能性があります。サーバの数が数十台、エンドポイント・コンピュータの数が数百台にもなる大規模組織では、管理者が重要なマシンにパッチを適用し忘れるといったことは十分に起こり得ます。

パッチと既存プログラムとの相性問題が発生することも少なくありません。これは、ソフトウェア導入ポリシーが厳しく、パッチを適用する前に厳格なテストを実施しなければならない大規模企業において、大きな頭痛の種となっています。また、再起動を必要とするパッチがシステム運用に影響を及ぼす場合もあります。

例えばSkypeでは2007年、Patch Tuesdayの後にサービスが2日間にわたって停止するという障害が発生しました。同社の発表では、この障害は、膨大な数のクライアント・マシンが一斉に再起動したことによって顕在化した未知のソフトウェア・バグが原因であるとされています。

まとめると、パッチは必要不可欠な存在であるものの、その適用にはさまざまな問題が付きまとうために導入が遅れ、攻撃に対して脆弱な時間が長くなる場合があるということです。

## より効果的なアプローチ

パッチを定期的に公開する手法と不定期に公開する手法にはそれぞれ長所と短所がありますが、脆弱性に対するセキュリティを最大化する方法は、パッチ適用が唯一というわけではありません。適切に管理された賢明なパッチ戦略は引き続き欠かせませんが、その弱点は、強力な侵入防御システム (IPS) を導入することによって補うことができます。IPSは、ネットワークへの侵入を試みる脅威を検出してブロックし、それらがサーバやエンドポイント・コンピュータにアクセスすることを防ぎます。

IPSを導入すると、公開されたパッチを大慌てで複雑なシステムに適用するのではなく、よりプロアクティブ(事前対応的)なアプローチで脆弱性に対処できるようになります。IPSでは、組織全体に対する保護が直ちに提供されるため、管理者は余裕を持って各サーバやエンドポイント・コンピュータにパッチを適用することができます。

優れたIPSは、脆弱性対策をシグネチャだけに依存するのではなく、より幅広い防御機能を提供します。個々の攻撃をシグネチャに基づいてブロックするだけでなく、攻撃の種類を見分け、プロトコルの挙動が仕様に沿った正しいものであるかどうかを監視することによって、ハッカーよりも常に一步先んじることを可能にします。

IPSでは、パッチが公開される前の脆弱性のみならず、発見・公開される前の脆弱性さえも保護できる場合があります。パッチ適用は引き続き強く推奨されるものの、事前対応型のIPSを導入すると、脆弱性ウィンドウをゼロにし、システム運用への影響を最小限に抑えつつパッチのテストや配布を行うことが可能になります。

さらに、集中管理機能を備えたIPSでは、簡単なマウス操作だけで組織全体のセキュリティを最新の状態にし、システムのあらゆる脆弱性を保護することができます。

強力なIPS技術と確固たるパッチ戦略を組み合わせた包括的なアプローチを採用することで、システム管理者は、毎月のPatch Tuesdayを乗り切り、パッチ未公開の脆弱性を突く攻撃にも対処できるようになります。チェック・ポイントは、IPS専用アプライアンスや包括的なIPS機能を搭載した統合セキュリティ・ゲートウェイなど、ネットワーク・インフラストラクチャとデータを保護するさまざまなソリューションを提供しています。パッチの適用前でもネットワークを保護できる、容易に導入可能な事前対応型IPS機能の詳細については、<http://www.checkpoint.co.jp/defense/advisories/public/index.html>をご覧ください。



## Check Point Software Technologies Ltd.について

チェック・ポイント・ソフトウェア・テクノロジーズ・リミテッド ([www.checkpoint.com](http://www.checkpoint.com)) は、インターネット・セキュリティにおけるトップ企業として、世界の企業向けファイアウォール、パーソナル・ファイアウォール、データ・セキュリティ、およびVPN市場をリードしています。チェック・ポイントは、情報セキュリティの分野に注力するセキュリティの専門企業であり、ネットワーク・セキュリティからデータ・セキュリティ、セキュリティ管理ソリューションに至る広範な製品を提供しています。チェック・ポイントは、NGXプラットフォームを通じて、企業ネットワークおよびアプリケーション、リモート・ユーザ、支店・支社環境、およびパートナー各社のエクストラネットのビジネス通信およびリソースを保護する幅広いセキュリティ・ソリューションのための統一されたセキュリティ・アーキテクチャを提供しています。また、業界をリードするデータ・セキュリティ・ソリューションであるCheck Point Endpoint Security製品ラインナップを通じ、PCやモバイル端末に保存されている各種企業データや重要なデータの暗号化と保護を提供します。数々の受賞歴のあるチェック・ポイントのZoneAlarm Internet Security Suiteをはじめとするコンシューマ向けセキュリティ・ソリューションは、世界中で何百万にも及ぶお客様のPCをハッカー、スパイウェア、およびデータ窃盗から未然に保護しています。またチェック・ポイントは、何百社もの各分野のトップベンダーが提供する最高のソリューションとの統合および相互運用性を実現するフレームワークであるOPSEC (Open Platform for Security) により、自社ソリューションの能力をさらに拡大します。現在、チェック・ポイント・ソリューションは、世界中のパートナー・ネットワークを通じて販売、導入、サービス提供されています。チェック・ポイントの顧客には、Fortune 100社の全社と何万ものあらゆる規模の企業や組織が含まれています。

©2003-2009 Check Point Software Technologies Ltd. All rights reserved.

Check Point, AlertAdvisor, Application Intelligence, Check Point Endpoint Security, Check Point Endpoint Security On Demand, Check Point Express, Check Point Express Cl, Check Pointのロゴ, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoreXL, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, Hybrid Detection Engine, IMsecure, INSPECT, INSPECT XL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpect, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management, Provider-1, PureAdvantage, PURE Security, puresecurityの logo, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Security Management Portal, Sentivist, SiteManager-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SMP, SMP On-Demand, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, UTM-1, UTM-1 Edge, UTM-1 Edge Industrial, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express Cl, VPN-1 Power, VPN-1 Power Multi-core, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 VSX, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone Labs, Zone Labsのロゴは、Check Point Software Technologies Ltd. あるいはその関連会社の商標または登録商標です。ZoneAlarm is a Check Point Software Technologies, Inc. Company. その他の企業、製品名は各企業が所有する商標または登録商標です。本書で記載された製品は米国の特許No.5,606,668、5,835,726、5,987,611、6,496,935、6,873,988、6,850,943、および7,165,076により保護されています。その他の米国における特許や他の国における特許で保護されているか、出願中の可能性があります。

Leverage IPS to Make Patch Tuesday Just Another Day

P/N:502830-J 2009.02

※記載された製品仕様は予告無く変更される場合があります。

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社  
〒160-0022 東京都新宿区新宿5-5-3 建成新宿ビル6F  
<http://www.checkpoint.co.jp/> E-mail : [info\\_jp@checkpoint.com](mailto:info_jp@checkpoint.com) Tel : 03 (5367) 2500