ソフトウェアパッチの適用およびアップデート

IT セキュリティのシートベルト

自動車には、乗用車・商用車のほぼ全てにシートベルトが備わっています。そして、膨大な数に上る調査結果によると、シートベルトによって命が救われ、衝突の際の負傷リスクが軽減されることを示しています。例えば、米国疾病管理予防センター（CDC）によると、「シートベルトは、衝突に起因する重傷と死亡の確率を半減させる。」という報告がされています。

更に CDC によると、「2012 年には、220 万人以上の成人が、自動車事故により緊急治療室へ搬送」「致命的でない負傷であっても、医療費や業務に就けないことによる総支出は、500 億ドルに上る」ことが想定されています。

それでも、毎年、残念ながら多くの人々がシートベルトを着用していなかったために交通事故で死亡、または瀕死の重傷を負っています。

もし、シートベルトが標準装備でなく、自分で選ばなければならないとしたら、死亡率や負傷率がどれ程になるか想像してみて下さい。このようなリスクがあることが分かっているにも関わらず、コストや手間を気にして、シートベルトを着用せずに運転するでしょうか？シートベルトを着用せずに運転した場合のリスクが広く知られていることを考慮すると、その可能性は非常に低くなります。

しかし、コストや導入するまでの手間など様々な理由から、ほとんどの企業がパッチ配布の自動化とそのプロセスに投資していません。多くの企業のトップは、セキュリティ上、十分に保護されていないシステムを利用した状態で事業を継続することの方が、システムに対して適切にセキュリティ対策を行うことよりも、負担が掛からず、かつコストが安いと考えています。これは、リスクの影響を熟知し、また同業他社が大規模な被害を受けたとしても、その考えは変わらないようです。

パッチの適用における課題

効果的な IT セキュリティについて検討する際、予防的なパッチの適用プロセス（および、それらをサポートするツール）の効果を、効果の高いように伝えることは簡単ではありませ ん。米国の国家安全保障局に該当するオーストラリア局は、以下の 4 つの簡単なステップで標的型攻撃の 85%を防止できると推定しています。

- アプリケーションホワイトリスティング
- アプリケーションのパッチ適用
- OS システムのパッチ適用
- 管理者権限の制限

そして、パッチ適用の価値は、セキュリティ専門家の間では幅広く知られていることは明らかです。2015 年 6 月、Google は 231 名のサイバーセキュリティ専門家と 294 名の一般のインターネットユーザーに対する、重要なデータの保護方法に関する調査結果を公表しました。専門家の間では、ソフトウェアの更新プログラムのインストールは、強力なパスワードの設定と、2 段階認証手段以上に重要だと答えました。回答した専門家の約 35% は、ソフトウェアの更新プログラムのインストールは重要だと回答した一方で、一般ユーザーの間では、わずか 2%が同様に回答しました。

一般ユーザーは、ウイルス対策ソフトウェアと、強力なパスワードが最も重要と考えていました。

多くの場合、効果的なパッチの適用は、事業を行う上でも不可欠です。2015 年 6 月に開催された HP のイベント内にて行われた、「The hidden dangers of inadequate patching（不適切なパッチ適用に隠れた危険性）」というタイトルのセキュリティブリーフィングで、「様々な政府による規制と同様に、業界標準のコンプライアンス基準についても、堅実なサービス提供とパッチ適用戦略が必要だ。」と指摘されています。パッチ管理を要する規制の例としては、PCI データセキュリティスタンダード(PCI DSS) および、欧州ネットワーク情報セキュリティ (NIS)条例などがあります。

しかし、セキュリティ対策への取り組みの価値が明らかになっているにも関わらず、パッチ適用に関する課題の多くは、依然として未解決のままです。2015 年の Verizon のデータ侵害調査レポート（DBIR）では、「セキュリティ侵害行為が見られた脆弱性の 99.9% は、共通の脆弱性（CVE）が公表された 1 年以上経過後に不正侵入されていた」ということが明らかにされています。

より厄介なのは、このレポートにある、「主に長期間に渡って提供されているセキュリティパッチが適用されていないために、多数の脆弱性が未対応のままである。事実、これらの脆弱性の多くは

ほぼ 8 年間前の 2007 年にまで遡るものである」ということです。

2015 年 4 月に米国コンピューター緊急事態対応チーム（US-CERT）が公開した警告では、「高リスクの脆弱性トップ 30」と特定したものが記載されています。 これらのトップ 30 となる脆弱性のうち、最も古い CVE とセキュリティ情報は、2006 年に公開されたものです。

なぜパッチの適用に失敗するのか? 要因と改善策

前述の Google の調査では次の内容が述べられています。「ソフトウェアの更新プログラムは、安全性を高めるオンラインセキュリティのシートベルトです。しかし、一般ユーザーの多くは、セキュリティ対策のベストプラクティスとして認識していないばかりか、ソフトウェアの更新プログラムそのものがセキュリティリスクだという誤解をしています。」

誤解かどうかは別として、この懸念は一部の専門家の間でも語られています。HP の調査では、セキュリティ意識の高いビジネスパーソンがパッチを適用しない、またはパッチを信用しない理由のいくつかを取り上げています。

- パッチ適用により OS が壊れる
- パッチ適用によりセキュリティ問題が引き起こされる
- パッチが予定通りに動作しない
- パッチには文書化されていない、若しくは不要な「機能」が含まれている
- 「サイレント（自動）」での パッチ配布は、ユーザーの作業を妨害したり、トラブルシューティング作業を混乱させることが多い

これらの懸念以上に、パッチの適用が必要な可能性のあるすべてのシステムの発見と優先順位付けは困難な場合があります。これらの問題は、モバイルやリモート、外出の多いユーザーにとっては必要なパッチの発見を遅らせます。

幸いなことに、今日のパッチ管理ソリューションは、上記に挙げた問題の全てに対応しています。例えば、企業に提供される前に徹底的に検証されたパッチは、OS を壊したり、セキュリティ問題の元になったり、予定通りに動作しない、または不要な機能が含まれているということはほぼありません。

しっかりと設計されたパッチ管理ソリューションは、ユーザーの作業を妨げたり、業務を中断させることなくパッチを配布することができます。また、現在のソリューション は、社内で最も重要な OS と、サードパーティーアプリケーションの全てにパッチを展開し、また管理することができます。

より大規模でより複雑な環境向けのセキュリティ対策をお探しの方は、ビジネス主導でパッチ適用の優先度を設定する、一貫した方法が役立つ場合があります。その方法の開発と実行は、特定の事業用件とゴールに基づいたものでなくてはなりません。しかし、これをゼロから作成する必要はありません。Forrester Research 社は、例えば、「優先パッチプロセス」（「P3」）と呼ばれるものをそのクライアントに提供しています。

情報通信技術専門家の国際的団体である ISACA の 2014 年 2 月のニュースレターでは、「4 Considerations During the Patch Management Process.（パッチ管理プロセスにおける 4 つの検討事項）」という記事でこのプロセスの概要を紹介しています。

1. 脅威予測を使用して、もっとも脆弱な資産を特定し、それらへの不正侵入の難易度を予測することで、攻撃の難易度を評価します。
2. 一部、対象の資産に既に存在し、またその資産がアクセスするデータのタイプと機密度に基づき、各資産へのセキュリティ侵害行為による潜在的な影響を計測します。
3. その脆弱性の悪用するツールが既に存在するかどうか、およびその悪用行為の悪質性などの要因に基づいて、各脆弱性の「固有リスク」を計測します。
4. 上記 3 つの推奨推定値と測定結果のガイドに基づき、リスク分類と評価に基づくパッチ優先度を割り当てます。

この全てが効果的なパッチ管理の重要な部分ですが、これは全体プロセスのほんの一部です。HP の調査は、その他の必要な手順を、以下のように特定しています。

1. すべての資産の正確かつ完全な検知
2. どの資産がセキュリティ対策を必要としており、かつそれぞれの資産を守るためにどのようなプロセスを取るべきかを決定する
3. 信頼できるパッチの提供者の特定、および常にアクセスできるようにしておく（メールや SNS 上で情報をキャッチできるなど）
4. 人的リソースや自動化ソリューションによるコスト、パッチ適用に失敗する確率、適用までに係る時間などの情報に基づいた、必要なパッチをインストールし管理するための方法の決定

その他のパッチの優先付けを行うための戦略及び実行プランについては、調査会社やパッチ管理ソリューションベン ダ、インテグレータなど様々なリソース等で紹介されています。しかしながら、そのような情報がなくとも、パッチ管理方法は十分に改善できます。より質の高いパッチ管理を実

現するためには、現状の問題を特定し、評価、展開し、また管理することにより、さらにクリティカルなシステムやアプリケーションを安全に管理することができます。

Ivanti Patch for Endpoint Manager による解決策

シートベルトを装備することにより、欲しいものにアクセスできる利便性を保ちながら、安全な環境を維持することができます。Ivanti Patch for Endpoint Manager は、一貫して統合された、パッチ管理の自動化を全社横断的に実現できるツールです。Windows や Linux、 Mac OS 等異なるプラットフォームの脆弱性対策を全て検知・実施します。また、Oracle や Java、その他のウェブブラウザなどのサードパーティー製のアプリケーションへのパッチ配布を自動的に行うことにより、脆弱性対策を実施することができます。

更に、社内ネットワークに接続している全てのデバイスへのパッチ配布も可能であり、ローディング中やリモート接続、休止状態であっても配布が可能です。特長としては、ネットワークへの最低限の負荷で、数分間で数千台のマシンへの適用を可能とする点にあります。パッチ管理の可視化においては、脆弱性に関するダッシュボード及びレポートを通じて、全てのデバイスのパッチ状態を可視化します。

Ivanti Patch for Endpoint Manager は、パッチ管理を自動化し、かつ効率的にすることでコスト削減を実現します。Ivanti Patch for Endpoint Manager をご導入頂いたアメリカの地方銀行においては、年間で 20 万ドルのコスト削減に成功した報告があります。

より詳細な情報については、**www.ivanti.co.jp** をご覧ください。

www.ivanti.co.jp

03-5226-5960

Contact-Japan@ivanti.com