サイバー攻撃からの安全性を診断する脆弱性診断製品

システムの脆弱性を狙ったサイバー攻撃の手口が複雑化、巧妙化するにつれ、政府機関や企業の被害が深刻化しています。それに伴い、システムに対する脆弱性診断を頻繁に行うお客様が増えてきました。当社が提供する脆弱性診断製品「Tripwire IP360」は、そのようなニーズにお応えし、システムのセキュリティ強化を図りながらセキュリティ対策運用コストの低減も可能にします。また、当社が得意とする資産管理ソフトウェアやパッチ適用ソフトウェアを組み合わせたソリューションにも注力し、企業のセキュリティ対策を支援していきます。

システムの脆弱性を突いたサイバー攻撃が増加

インターネットが普及し、企業活動に不可欠なインフラとして定着する一方、政府機関や企業を狙ったサイバー攻撃による被害が深刻になっています。サイバー攻撃は、システムの脆弱性を突いて機密情報の窃取やWebサイトの改ざん、サービス停止といった攻撃を仕掛けてきます。これらの対策として、ファイアウォール、侵入検知システム、ウイルス対策ソフトの導入やセキュリティパッチ適用などを行うことが一般的です。

また、特に大きな脅威となっている標的型攻撃などの高度化・巧妙化されたサイバー攻撃に対しては、攻撃が内部に侵入することを防止する「入口対策」だけでなく、万一侵入された場合にさらなる侵入拡大の防止と監視の強化を図る「内部対策」、さらに、機密情報を窃取する通信の遮断および監視強化を行う「出口対策」を実施することが推奨されています。そして、新たな脆弱性や攻撃手法への対策が漏れなく行われているかを確認するために、システム全体に対して脆弱性診断を実施することが重要です**(図-1)**。

脆弱性診断は、サービス利用型と製品導入型の2つの方式に分けられます。サービス利用型は外部機関に診断を委託し、インターネット経由または対象システム内に機器を持ち込んで診断を実施します。製品導入型は、文字どおり脆弱性診断製品を導入し、自社内で診断を実施します。サービス利用型は、規模の小さいシステムや診断回数が少ない場合はコスト的に優位ですが、反対に規模が大きいシステムや頻繁に診断を行う場合は製品導入型の方がコスト的に優位となります。そのため、脆弱性対策に関心が高いお客様は、自社で運用ができる上にコストを気にすることなく診断回数を増やすことが可能な製品導入型を採用するケースが増えてきています。

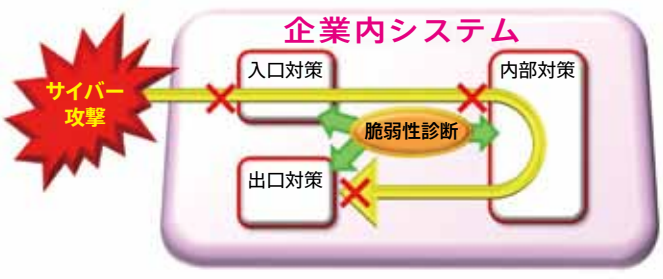

図-1 各脆弱性対策と脆弱性診断

当社ではサービス利用型及び製品導入型の両方を提供していますが、ここでは近年注目を浴びている製品導入型製品の中からTripwire IP360(以下、IP360)について紹介します。

最新のセキュリティ情報を使ってシステムの脆弱性を自社で診断

IP360は、管理機能と診断機能を合わせ持つ IP360 VnE Manager (以下、IP360 VnE)と、診断機能に特化した IP360 Device Profiler (以下、IP360 DP)で構成されます。IP360 DPは追加導入ができるため、システム構成の変更や診断対象の拡大にも柔軟に対応することができます。また、初期導入時はサービス提供型では診断が難しい内部セグメントにあるサーバ群およびネットワーク機器に対象を絞って診断し、運用に慣れてからDMZ(DeMilitarized Zone)にあるWebサーバなどについても診断対象とするなど、運用方針や予算計画に合わせて導入することができます**(図-2)**。

脆弱性診断は、複雑なシステムや大規模なシステムであっても、漏れなく脆弱性を発見することが求められます。IP360では、業界トップクラスであるTripwire社の脆弱性専門の研究チーム(VERT)が最新のセキュリティ情報に基づいて作成した診断ルールを使用するため、最新の脆弱性についても発見・特定することができます。特にマイクロソフト社が重大と警告した脆弱性については、発表から24時間以内に、対応した診断ルールが提供されます。診断ルールとはウイルス対策ソフトでいうところのパターンファイルであり、インターネット経由で最新のものを自動的にダウンロードし適用することができるため、更新漏れを気

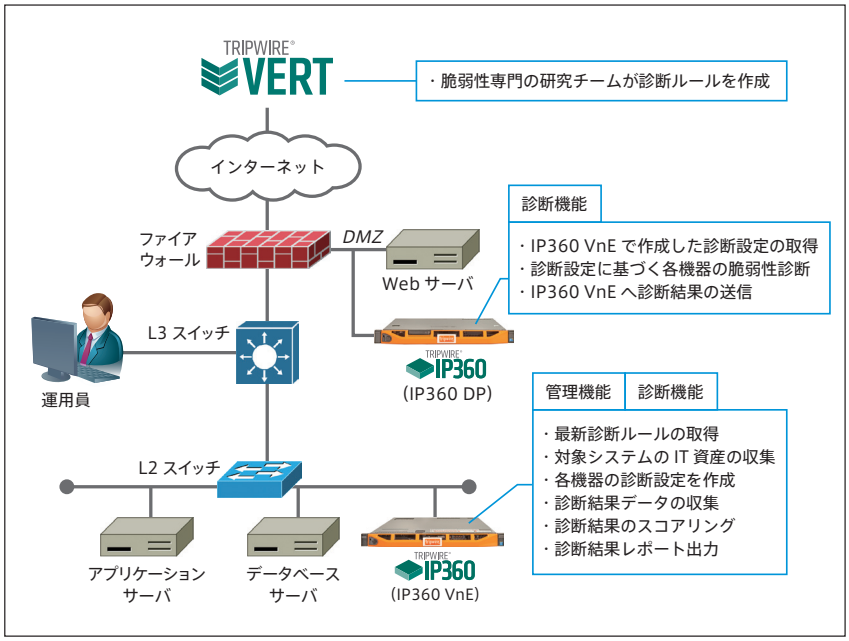

図-2　IP360の構成例

にする必要はありません。

また、エージェントレスで診断するため、OSに対してはもちろんのこと、ファイアウォールやL3スイッチなどのインストールができない機器や設定変更したくない機器に対しても診断を行うことができます。より詳細な診断を行いたい場合は、ログインアカウントとパスワードを設定することで、OSのセキュリティパッチ適用状況やWebアプリケーションの入力フォームに対する脆弱性診断なども行うことができます。

これらのIP360による診断は、ペネトレーションテスト(注1)とは異なり、診断対象への影響が最小限になるよう考慮した診断ルールで実施します。

さらに診断結果に独自のスコアリングシステムを採用しており、脆弱性が悪用された場合の影響度だけでなく、セキュリティ情報が公開されてからの日数、悪用されるリスクを考慮してスコアの算出を行います。スコアの高さは対策の優先度に比例するため、セキュリティの専門家でなくても優先的に対応すべき脆弱性を一目で判断することができます。

このスコアは、新たな脆弱性が発見されると一時的に高くなることはありますが、適切に対策を行うことで下がります。反対に対策を行わないとスコアが上がり続けるため、各機器のスコア履歴を見ることで、セキュリティマネジメントが正しく運用されていることを判断する指標として活用することができます**(図-3)**。

脆弱性診断は、一回実施すればそれで終わりではありません。OSやソフトウェアに新しい脆弱性が発見されたときやシステムを更新した後などに対策を行い、その効果を確認するために、改めて診断を実施する必要があります。このように診断を複数回実施する場合でも、自社で運用可能な脆弱性診断製品があれば、コストを気にせず必要なときに即時診断を行うことができます。そして早期に脆弱性の存在を把握し、対策を行うことで、サイバー攻撃からシステムを守ることにつながります。

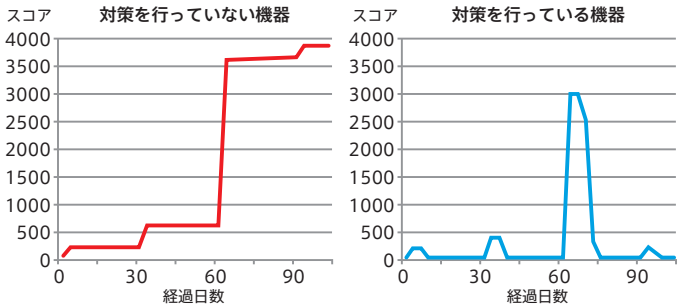

図-3　脆弱性対策の実施によるスコア遷移の違い

PCI DSS要件に対応した製品でセキュリティ強化を支援

クレジットカード会員データを安全に取り扱うことを目的として制定された、クレジットカード業界の国際的な情報セキュリティ基準に、PCI DSS(Payment Card Industry Data Security Standards)があります。IP360は、PCI DSSの要件11.2に対応しており、当社が扱っているTripwire Enterpriseを併せて導入することによって、PCI DSSの要件11.5にも対応できます。PCI DSSの認定取得を目的にされている流通業のお客様にも導入いただいております。

情報セキュリティ基準の公的な認証としてはISMS(ISO27001)がよく知られていますが、PCI DSSはISMSよりも具体的かつ定量的に要件が規定されています。そのため、クレジットカード業界だけでなく、マイナンバーなどの個人情報保護のための情報セキュリティ対策にも適用することができます。

当社では、PCI DSSの要件を複数満たすことができるIP360やTripwire Enterpriseを核として、さまざまな業界に向けてシステムのセキュリティ強化支援を行っています。今後はさらに資産管理ソフトウェアやパッチ適用ソフトウェアと組み合わせたセキュリティソリューションについても注力していきます。

(SIソリューション事業部　川﨑 守)

(注1)ペネトレーションテスト:実際のサイバー攻撃と同じ手法を使ってシステムに侵入を試みることで、そのシステムに脆弱性がないかを確認するテスト手法