

第2回

脆弱性検査 [後編]

本連載では、セキュアなシステム / ネットワークを構築するうえで必要不可欠な各種セキュリティ対策について解説する。今回は、システム / ネットワークのセキュリティ・ホールを調査する「脆弱性検査」を取り上げ、具体的な検査の種類 / 項目 / 方法などについて説明した。今回は、その後編として、脆弱性検査を実施する際の留意点と同検査の最新動向を紹介する。

小川 孝
ネットワンシステムズ



脆弱性検査前のポイント

脆弱性検査の実施によって、システム / ネットワークにおける脆弱性の有無を調べることができるが、それと併せて、既存のセキュリティ対策が有効かどうかも明らかにできる。つまり、適切なセキュリティ対策を講じ、その効果を評価するためにも、脆弱性検査は必要不可欠な取り組みだと言えるのである。

今回は、脆弱性検査と情報セキュリティ監査制度の関連性、脆弱性検査のタイプ / 検査項目 / 方法について解説した。今回は、これらを踏まえたうえで、脆弱性検査の実施にあたって押さえておくべきポイントと、同検査の最新動向を紹介する。

なお、2003年の4月から経済産業省が実施している情報セキュリティ監査制度では、監査を実施する際の検討事項、外部委託を行う際の注意事項、監査の仕様例などが定められている。そして、脆弱性検査は、同制度の基準である「情報セキュリティ監査基準」の構成要素の1つでもある。したがって、脆弱性検査を実施する際の参考のためにも、同制度に一度は目を通しておくことをお勧めする。

以下では、脆弱性検査の実施前、実施時、実施後の3つの段階に分けて、脆弱性検査のポイントを説明する。まず、脆弱性検査を実施する前にやるべきことはプランニングである。システムやネットワークにおける脆弱性はウイルスと同様なくなることがない。したがって、セキュアなシステム / ネットワークを維持するには、脆弱性への対策を継続的に行う必

要がある。それに伴い、脆弱性検査もできるかぎり短い周期で、かつ定期的に行うのが理想である。

そこで、脆弱性検査を検討する際は、中長期的にわたって継続的に実施するという前提の下、項目別に検査を計画していく。その際にポイントとなるのが検査の分類、実施体制、検査を依頼する業者の選び方である。以下、これらについて見ていこう。

検査の分類

検査は簡易的なものと本格的なものに分けるとよい。簡易的な検査は、ツールを用いて短い周期で繰り返し実施する。この検査では、ホストやネットワークに過大な負荷を与える検査項目を除外したほうがよい。一方、本格的な検査はある一定期間を置いて集中的かつ定期的に検査ツールと手作業によって行う。簡易的な検査と本格的な検査の運用例を表1に示した。ただし、これらはあくまでも一例にすぎない。実際には、セキュリティポリシー、検査作業にかかる負荷、検査対象となるホストの持つ情報価値などを基に検査項目、頻度、検査対象を見直す必要がある。

検査には、ひとつおりの検査項目を備えるオールインワン型のツールを利用するとよい。このようなツールは通常、バージョンアップすることで新しく発見された脆弱性を対象に加えて、検査を行えるようになっている。また、検査ツールの中にはスケジュール機能を備えているものが多いので、この機能を有効にして、定期的な検査を自動的に行うと作業が軽減できる。

なお、検査によっては、実行する時間帯を考慮

表1：簡易的な検査と本格的な検査の運用例

	簡易的な検査	本格的な検査
方法	ネットワーク型検査ツールを利用する 検査項目の多いオールインワン型のツールを使用	オールインワン型検査ツール、特定の検査専用ツール、手作業を組み合わせて行う
作業者	社内のIT/IS部門	専門業者
対象	定期的に行う検査：ネットワーク上の重要なホスト 随時に行う検査：新規で導入したホスト	すべてのホスト
方針	一般的なOSおよびアプリケーションの既知の脆弱性や設定の不備を中心に検査する 稼働しているシステムへの影響が特に懸念されるような検査は除外する 大量のトラフィックやサービスによって故意に負荷をかけるDoS(サービス不能攻撃)検査など実際に攻撃や侵入を行う検査を実施	オールインワン型検査ツールでは対応しきれない検査を行う 独自のアプリケーションや環境に依存したシステム設定に関する検査を重点的に行う <検査例> Webアプリケーションの脆弱性検査、リモート・アクセス環境の調査、簡易的な検査よりも詳細な検査 稼働しているシステムへの影響が特に懸念される検査も実施する DoS検査など実際に攻撃や侵入を行うような検査を実施

する必要がある。例えば、実際に攻撃や妨害行為を試す検査では、対象のネットワークや機器に障害が発生する可能性があるため、業務への影響が少ない時間帯や休日に行うようにするべきである。

ただし、通常の検査でも回線速度や機器の動作状態により、まれに障害が発生する。したがって、発生が予測される障害への対応手順を確認し、検査作業中の各管理者への連絡手段を確保しておくことが、最低限の準備として必要になる。そのほか、検査によって発生する大量のログの格納場所を確保し、外部から検査を行う場合にはISPへ事前に連絡しておくことも忘れないようにしたい。

実施体制

検査の分類に伴い、だれが検査を行うのかということを決める必要がある。一般に、脆弱性検査は外部の専門業者に依頼するケースが多い。これは、脆弱性検査には専門的な知識が必要だということに加えて、第三者機関による公正性や客観性が求められるためである。なお、脆弱性検査にかかわる知識は、専門業者だけでなく、ネットワーク/サーバを構築する技術者も理解しておくべきだろう。

ただし、外部に検査を委託すると、事前に調整や準備を行うための時間や費用の負担が大きく、定期的な検査や小規模な構成変更時の検査を行う

余裕がなくなることがある。それでは、脆弱性検査の継続性が維持されず、精度も低くなってしまふ。

こうした場合の対処法はいくつかある。1つは、検査ツールは自社で用意し、検査だけを業者に依頼する方法である。この方法では、検査内容やライセンス料など検査ツールにまつわる部分を自社でコントロールすることが可能になる。また、上述した「簡易的な検査」を自社の技術者によって実施するという選択肢もある。ただし、その場合でも、検査結果の公正性や客観性を確保する目的から、本格的な検査は専門業者に依頼することが望ましい。

自社で簡易的な検査を行う際は、表1に示したように検査ツールを用いる。前編で述べたとおり、検査ツールにはフリー・ソフトウェアと市販製品があるが、自社で行う検査には市販製品を用いるほうが無難である。ネットワーク・セキュリティに詳しい技術者が社内にいればフリーの検査ツールを利用することも可能だが、サポートや動作保証がないことに留意する必要がある。以下、ツールによる検査の説明は、断りのないかぎり、市販製品を前提にしていることをご了承いただきたい。

ツールの設定と実行は、マニュアルどおりに行えば特に難しいことはない。手作業による検査と違い、セキュリティに関する知識がそれほどなくても、常に同質の検査が行える。ただし、ツールを用いた検査では、



結果を正しく読み取ることが難しい場合もある点に留意されたい。例えば、検査結果を基に出力されるレポートには、実際の運用に見合った対策が表示されているとは限らない。そのため、発見された脆弱性に対して確実に対処できるように、国内外のセキュリティ関連のサイトや脆弱性に関する情報提供サービスを利用して、情報を収集しておく必要がある。

なお、作業管理の一本化を目的に、ネットワークやシステムを構築したベンダーが脆弱性検査を行うケースもある。そのような場合は、外部の業者といえども、自社で行う場合と同様にあくまでも簡易的な検査として扱うべきである。そして、検査の公正性や客観性を確保するためには、第三者機関による定期的な検査を別途行う必要がある。

さて、上記のケースを整理すると、脆弱性検査の実施体制は以下の3段階に分けることができる。

- 段階1：準備から作業までの一連の検査業務を専門業者に委託する
- 段階2：自社で市販の検査ツールを購入し、検査は専門業者に委託する
- 段階3：市販の検査ツールを用いて、比較的短い周期の定期検査や小規模なシステム/ネットワークの変更に伴う検査は簡易検査として自社で行い、それとは別に第三者機関である専門業者による詳細な検査を定期的実施する

専門業者による検査においては、検査ツールの

ライセンス料が検査料金に含まれていることが多い。そのため、段階2に移行すれば、中長期的に見てツールのライセンス料を削減することができる。さらに、社内に検査ツールの利用体制を整えることで、費用面での効果が大きい段階3へステップアップすることが可能になる。

検査の専門業者を選ぶ

先に述べたように、自社で簡易検査を行う場合にも、本格的な検査は第三者である外部の業者に依頼するべきである。しかし、その際にどの業者に頼むべきかは迷うところであろう。

基本的なことから言えば、検査作業者の技術力だけを基準にして業者を絞り込むのは適切ではない。周到な検査計画、作業時の報告体制、検査対象へ影響を及ぼさないための保護策などをきちんと準備したうえで検査全体を確実に遂行し、検査後に検査環境に応じたわかりやすい報告書を作成することができる業者であるかどうかを見極める必要がある。それには、提供している検査サービスの詳細について、業者から明確な説明や回答が得られるかどうかを確認してみるとよいだろう。表2に確認すべき項目をまとめた。

そのほか、業者自体の情報セキュリティ管理体制を確認するのも有効である。

なお、セキュリティに関する技術力を評価するための基準や資格といったものも存在しているが、国内では認知度も低く、あまり活用されていないのが実情である。

表2：業者の質を判断するための確認事項

- ツールによる検査のほか、手動による検査サービスを提供できるか
- ツールによる検査の欠点や検査できない項目を明確に説明できるか
- ツールによる検査を行う際、環境に応じてどのようにツールの調整を行うかわかりやすい報告書を提出できるか、またそのサンプルを見せてもらえるか
- 発見された脆弱性にセキュリティ修正パッチが適用できない場合などに適切な回避方法を提示できるか

国際的に有名なセキュリティ関連の認定資格としては、米国の非営利団体であるISC²(International Information Systems Security Certifications Consortium)が主催するCISSP(Certified Information Systems Security Professional)のほか、SANS InstituteのGIAC(Global Information Assurance Certification)、CompTIAのSecurity+などがある。日本国内でこれらの資格を持っている技術者はまだ少ないと思われるが、国内でも受験可能な環境が整いつつあるため、今後は有資格者が増えていくだろう。

また、国内のセキュリティ関連の資格としては、情報セキュリティアミニストラータやシステム監査技術者が有名である。しかし、前者はその名のとおり、セキュリティ管理者としての資質を問うものであり、専門技術者としてのスキルは問われない。一方、後者は監査作業全体を遂行する能力を評価するための判断材料にはなるが、脆弱性検査の技術力までは評価できない。そのほか、セキュリティ製品やOS、ネットワーク製品などのベンダーが認定するセキュリティ関連の資格もあるが、それらも脆弱性検査に必要な知識をすべてカバーしているわけではない。

よって、こうしたセキュリティ関連の資格は、総合的な技術力評価の一要素として参考にする程度にとどめておいたほうがよいだろう。

ところで、情報セキュリティ監査制度の柱の1つである「情報セキュリティ監査企業台帳」(注1)には、情報セキュリティ監査を実施する業者/組織(監査主体)が7つのテーマに沿って登録されている(表3)。ただし、その登録は上述したようなセキュリティ監査に関する技術指標が明確ではない状況で実施された。また、現時点でも監査を行う人物に関する資格などには何も制限が設けられていない。そうした点からすると、情報セキュリティ監査企業台帳は、業者選定の材料とするには情報不足の感が否めないが、数少ない貴重な情報源であるには違いない。

表3：情報セキュリティ監査企業台帳の監査主体の分類テーマ

IT関連業務内容
セキュリティ関連業務
参加するIT関連機関
得意とする監査対象の分野・業種
得意とする監査形態
監査従事者が持つ取得済監査関連資格
取得している監査関連の認証



検査実施時のポイント

次に、実際に検査を行う際に考慮すべきポイントを見ていこう。前述したように、脆弱性検査には手作業で行う場合とツールを用いる場合とがある。以下、それぞれの場合に分けて解説する。

手作業による検査実施時のポイント

手作業で行う検査のメリットの1つは、実際の攻撃者の手法をシミュレートできることである。ただし、実際に攻撃や妨害を行う検査は、他の検査と異なり、システムに影響を及ぼすというリスクを有する。したがって、この種の検査を行う際は、必要性を十分見極めたうえで、あらかじめ準備を行ってから実施していただきたい。

例えば、外部ネットワークからの検査しか行わない場合や独自のOSやアプリケーションに対して検査を行う場合は、実際に攻撃を試してみなければ脆弱性の有無を正確に判断することは難しい。しかし、一般的なOSやアプリケーションに関する既知の脆弱性を調べる場合は、サーバやネットワーク機器に直接ログインして内部の設定を検査するホスト型検査でバージョン情報やセキュリティ・パッチの適用状況を調べれば、高い精度で脆弱性の有無を

注1：現在、特例による業者の登録を受け付けており、今回の登録に申し込んだ業者の情報を反映したバージョンが2004年1月下旬に公開される予定である。詳細は、以下のWebページで確認されたい。
[情報セキュリティ監査企業台帳のWebサイト]
<http://www.meti.go.jp/policy/netsecurity/is-kansa/>



判断することができる。

なお、手作業による検査は、侵入に要する時間を計りたい、未知の脆弱性を調べたいという目的から行うこともあるが、調査結果は検査を行う技術者のスキルに依存する部分が大いなので、注意が必要だ。

ツールによる検査実施時のポイント

ツールによる検査を行う際のポイントは、以下の3点に集約することができる。

検査ツールの限界

検査ツールは、あらかじめ決められた確認手順で脆弱性の有無を判断する。そのため、高度な専門技術者による手作業の検査と比べると、検査精度が低下することは避けられず、脆弱性の誤検出や見逃しが発生する可能性が増えてしまう。したがって、検査ツールを利用する際には、そうした事情を踏まえて、簡易的な検査にのみ用いるか、または手作業による検査で補完するといったかたちで対処する必要がある。

設定のカスタマイズ

検査ツールを使用する際は、検査対象のネットワークやサーバ固有の環境に合わせて、設定をカスタマイズする必要がある。以下、その目的をまとめた。

検査精度の向上

検査に具体性を持たせるために、検査項目の中には、検査するネットワーク上に固有の情報(メール・アドレス、ドメイン名、サーバやネットワークのIPアドレス、管理者のユーザー名やパスワードに関する情報など)を設定しなければならないものがある。

また、パスワードの検査には、あらかじめ自分の組織で使われそうなIDやパスワード(会社名、部署名など)を集めて作成した辞書ファイルを加える。これにより、検査ツールに付属している辞書や一般的

な辞書のみを使った検査よりも、不適切なパスワードが発見される可能性が高くなる。

検査時間の短縮

検査対象の機器数が多い場合は、検査にかかる時間も無視できない。そこで、脆弱性が存在しないことが明白な検査項目を外したり、通信に関する設定値を調整したりすることで、検査時間の短縮を図ることができる。ただし、検査時間の短縮は検査精度とのトレードオフになる場合が多く、不要な検査項目の見極めやツールの通信設定値の調整には、セキュリティ技術とツールに関する知識が求められるので、注意が必要だ。

レポートの出力機能

レポートには、すべてのOSや環境に応じた対策が出力されるわけではない。また、記述されている対策が自社の環境に最適な解決策であるとも限らない。特に、最新の脆弱性については、対策が記述されていなかったり、情報が不完全だったりするケースがある。そうした場合に備えて、ベンダーのWebサイトやセキュリティ関連の情報サイトから、最新の脆弱性に関する情報を入手しておく必要がある。



検査後のポイント

検査前、検査時のポイントを説明したところで、検査後のポイントについての説明に移ろう。脆弱性検査の性質からすると、検査後の対処こそ最も重要であるとも言えるので、以下のポイントはしっかりと押さえておきたい。

最新情報を集める

アプリケーションやネットワーク製品の脆弱性は毎日のように発見されており、検査の終了直後に危険度の高いものが新たに見つかることも少なくない。したがって、検査を行って脆弱性への対処を

終了後も、システムの安全性を保つために、何らかの対策を講じる必要がある。それには、定期的に脆弱性検査を行う一方で、常日ごろから脆弱性に関する最新情報の収集と対策を行うようなセキュリティの運用体制を敷いておくのがよいだろう。

対策後に再検査を行う

業者による検査では、発見された脆弱性に対して検査結果のレポートを基に検査担当者が設定変更を行い、その作業報告をもって対策の完了とするケースが多い。しかし、それでは検査の公平性と客観性が保たれないので、検査対象を絞るなど、何らかのかたちで再検査を行うべきである。例えば、検査期間を複数日設けている場合は、危険度の高い脆弱性を見つけた時点で速報として口頭で報告する一方で、即座に検査と並行して対策を施し、最終日にその再検査を実施するケースもある。

検査結果を生かす

検査後は、発見された脆弱性に対策を施すとともに、脆弱性を生み出した原因を調べて、それを基に運用体制を改善していくことが重要である。これにより、「計画(Plan)、実施(Do)、確認(Check)、見直し(Action)」という情報セキュリティ管理の運用サイクルが滑らかに回るようになる。

だが、実際には、社内システムを構築したベンダーに脆弱性検査/対策を丸投げしているといったケースをよく見かける。こうしたケースでは、検査結果を生かした運用体制の改善が行われなため、時間の経過とともに対策が陳腐化し、同様の脆弱性が再発する可能性が高い。システム/ネットワーク上に脆弱性を生み出す要因を表4に例示した。

表4：システム/ネットワーク上に脆弱性を生み出す要因の例

ネットワークやシステム設計時のセキュリティに関する検討不足
新たに発見したOSやアプリケーションの脆弱性に対する対応方針や手順が決まっていなかった
運用や設定手順書の対策項目に抜けがあった
機器導入時や運用時の設定ミス
一時設定の戻し忘れなど、運用手順の不徹底

ューティング・モデルに沿うかたちで進化を続けている。以下、その最新動向を紹介しよう。

Webアプリケーションの脆弱性検査

Webアプリケーションは、外部ネットワークに公開されることが多いWebサーバ上で動作するという性質上、セキュリティの確保に特に注意を払う必要がある。もちろん、脆弱性検査はWebアプリケーションの安全性を高めるためにも有効である。

そもそも、Webサーバにおける脆弱性検査は、対象をWebサーバとWebアプリケーションなどWebサーバ上で動作するコンテンツやアプリケーションに分けて行われる(次ページの図1)。Webサーバ自体の検査は、これまで説明してきた一般的な脆弱性検査に含まれる。一方、Webサーバ上で動作するアプリケーションやコンテンツに対する検査は、以下のような理由により、一般的な脆弱性検査とは別に単独で実施されることが少なくない。

検査で用いられる技術や手法がWebサーバ自体の検査とは異なる

コンテンツの内容・規模がWebサイトにより異なる
コンテンツの変更が頻繁に行われる

他の検査に比べて作業量が多くなる傾向がある

本来、アプリケーション開発においては、セキュリティ設計に際して、暗号化のほか、入力値のチェック、改竄防止、なりすましなどを考慮しなければな

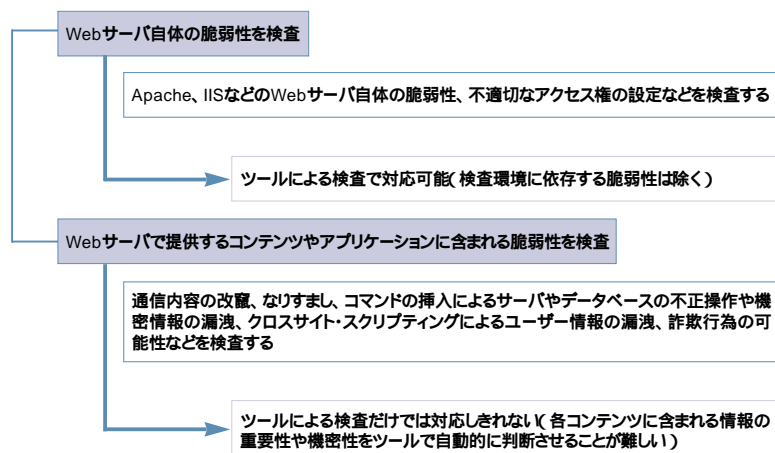


脆弱性検査の最新動向

脆弱性検査の手法は、その時点で主流のコンピ



図1：Webサーバにおける脆弱性検査



らない。Webアプリケーションでは、こうしたセキュリティ対策はサーバ側で行われるのが基本だが、実際には、正しく設計／実装されていないものがままある。こうしたこともあって、Webアプリケーションを運用するには脆弱性検査が大切なのである。

なお、Webアプリケーションにおけるセキュリティリスクには、セッション・ハイジャック(注2)によるなりすまし、クロスサイト・スクリプティング(注3)による情報窃取や詐欺行為、コマンド・インジェクション(注4)によるデータベースやサーバへの不正アクセスから生じる機密情報の漏洩などがあり、これらの脆弱性は、企業経営に対して致命的なダメージを与えかねない危険性を有している。実のところ、定期的に脆弱性検査を行っていないWebサイトでこの検査を行うと、必ずといってよいほど何らかの脆弱性が発見される。

また、独自に開発したアプリケーションでは、ソース・コードの中にセキュリティ上問題となる動作を引き起こす処理や関数が含まれていないかどうかを調査する必要がある。そのため、大規模なWebアプリケーションでは、ソース・コードの検査も同時に行ったほうが検査の精度や作業効率が高まる。

技術面以外の最新動向

通常、脆弱性検査は機器やネットワークにおける技術的なセキュリティ・リスクを対象としており、運用体制や物理的なセキュリティ・リスクといったシステム／ネットワークを取り巻く環境に関するリスクまではカバーしていない。しかし最近では、技術面以外のセキュリティ・リスクに対する対策の重要性も認知されつつあり、脆弱性検査と併せてこれらのリスクについても検査を実施するケースが多い。以下、技術面以外のセキュリティ・リスクを対象とした検査について紹介する。

運用状況の検査

システム管理者やエンドユーザーインタビューなどを行うことにより、現在の運用状況がセキュリティ・ポリシーや手順書に沿っているか、またセキュリテ

注2：第三者に通信が乗っ取られること

注3：ユーザーが入力した文字列などにより動的に生成されるWebページにおいて、本来は許可されていない不正な操作を行うことを可能にするセキュリティ・ホール。あるサイトに書かれているスクリプトが別のサイトへとまたがって(クロスして)実行されることから、クロスサイト・スクリプティングと呼ばれる

注4：外部コマンド呼び出し時に適切なフィルタ処理を行っていないため、任意のコマンドを実行されてしまうこと

ィ上妥当であるかどうかを検査する。本来は、システム監査や運用監査のような本格的な監査を実施するのが理想だが、簡易的な検査でも、システム運用の基盤における脆弱性を調べることが可能である。

本格的に検査を行う場合は、ソーシャル・エンジニアリングにより、システム管理者やエンドユーザーに対して、いわゆる抜き打ち検査を行うこともあるが、そこまで徹底的な運用状況の検査を実施するケースはまだ少ない。

物理的な環境の調査

運用にも関連するが、入退室管理、サーバの設置状況、ネットワーク配線といった物理的な安全性の検査も重要である。サーバやネットワークへの不正アクセスや妨害は、ネットワーク経由で行われるとは限らない。例えば、ネットワーク経由での不正アクセスが困難な環境でも、現地に出向いてLANの中に入り込むことで、ローカルのサーバやクライアントから簡単に不正アクセスが行えることがある。そのため、物理的な環境の安全性も、脆弱性検査の際に調べておくとうい。

検査ツールの今後

検査ツールの今後の展開として、検査性能の向上が図られるのは当然だが、本稿ではそれ以外の目新しい動きを紹介しよう。

リスク統合分析ツールとの関係 / 統合

ネットワーク型およびホスト型の検査ツールの結果を統合したり、ウイルス対策ソフトや他のセキュリティ製品のログ、資産管理ツール、運用管理ツールなど、さまざまな分野の情報を集約したりすることによって、リスク管理や分析を行う製品が出始めている。今後、脆弱性検査用のツールは、組織のリスク分析を行うツールの一要素として統合されていくのではないと思われる。

IDSとの関係 / 統合

ネットワーク型の脆弱性検査ツールとIDS(Intrusion Detection System:不正侵入検知システム)を関係させた製品も登場している。この製品では、検査ツールが最新の脆弱性情報を基に検査を実施し、その検査結果から脆弱性が存在する項目のみがIDSの監視対象として自動的に絞り込まれる。つまり、IDSの侵入検知の精度を高めると同時に、脆弱性の発見もリアルタイムに近いかたちで実現しようという考え方が具現化されているのだ。

以上、前編と後編の2回にわたり、脆弱性検査に関する解説を行ってきた。前述したように、今回取り上げた脆弱性検査は、情報セキュリティ管理の運用サイクルの一部であり、情報セキュリティ管理において、技術的な対策や改善を行うために必要なセキュリティ・リスクを洗い出すものである。しかし、組織全体の情報セキュリティの向上を図るためには、技術面以外のセキュリティ・リスクの検証と対策も重要である。例えば、サーバやネットワークの物理的な環境や運用管理体制、セキュリティ・ポリシーなどについても監査が必要となる。

また通常、脆弱性検査は定期的実施されるため、最新の脆弱性に対して、即時に対応できるとは限らない。そこで、IDSやIDP(Intrusion Detection and Prevention System:不正侵入検知 / 防御システム)などのアプライアンスを導入したり、インシデント(事件・事故)発生時の対応手順をあらかじめ決めておいたりすることで、万が一、脆弱性を利用した不正アクセスや侵害行為が発生しても、即座に異常を認識して被害を最小限に食い止めることができる仕組みを用意しておく必要がある。

脆弱性検査には当然コストがかかる。コストをかける以上、できるかぎり精度の高い検査を行えるよう、事前の検討はもちろんのこと、検査結果を積極的に有効活用していきたいものである。 **CW**