外部からの脅威に対するセキュリティ技術の動向

日本電信電話㈱
第三部門　プロデュース担当
主幹研究員　舘 剛司

情報セキュリティリスクの分類

近年のICTの進展とブロードバンドの普及に伴って、企業や組織におけるセキュリティ対策（ここでは特に情報セキュリティに関するものを対象とする）は、ますます重要かつ複雑なものとなっている。

例えば、企業で扱う情報の所在だけでも、ネットワーク（インターネットを含む）、サーバ、PC端末、大容量記憶媒体など多岐に渡り、大量の情報を簡単に扱えるようになったため、それに伴う情報漏洩のリスクやインシデント発生時の影響も増加してきている。

企業における情報セキュリティのリスクを、要因の所在の観点から分類・整理した結果を表1および図1に示す。

最近は、企業におけるコンプライアンス強化の必要性が強く認識され、内部要因に着目したセキュリティリスクが取り上げられる機会が増えている。一方で、外部要因によるセキュリティリスクも、ますます多様化しており、それに応じた対策技術も機能面・運用面において日々進化している。

今回は、図1の左上の領域、つまり情報へのアクセス権限を持たない部外者（と言っても社員や契約社員も対象になる）による不正行為に伴う情報セキュリティリスクのうち、特にシステム的リスクとその対策技術の動向について紹介していく。

情報セキュリティ対策技術

(1)　不正アクセス・なりすましへの対策技術

不正アクセスとなりすましは、いずれも本来情報へのアクセス権限を持たない者による不正行為だが、対策としては「ネットワークレベルでのアクセス監視・遮断」、「システム自体の脆弱性対策」、「アカウント管理・認証の強化」の大きく3つに分類される。

「ネットワークレベルでのアクセス監視・遮断」としては、ファイアウォールや侵入検知システム（IDS）・防御システム（IPS）を導

[a]不正アクセス	情報へのアクセス権限を持たない者が、制限を不正に回避してアクセスして、情報の漏洩・改ざん・破壊などを行う。
[b]なりすまし	情報へのアクセス権限を持たない者が、正規権限者を装ってアクセスする。
[c]盗聴	正規権限者による情報へのアクセスを、アクセス権限を持たない者が盗み見る。
[d]不法侵入	敷地内や建物、部屋に入る許可を受けていない者が内部に侵入し、情報に不法にアクセスする。
[e]盗難	情報を格納した機器やメディアを所持する許可を受けていない者が、不正な持ち出し、正規権限者からの物理的な奪取を行う。
[f]不正プログラム実行	不正アクセス、盗聴、なりすまし、不正操作などの不正な振る舞いをするプログラム（ウイルス、ワーム、スパイウエア、許可されていないP2Pソフトなど）が実行される。
[g]不正操作	情報へのアクセス権限を持った正規権限者が、故意に許可されない行為（情報の漏洩・改ざん・破壊など）を行う。
[h]誤操作・誤設定	情報へのアクセス権限を持った正規権限者が、過失で許可されない行為（情報の漏洩・改ざん・破壊、システム誤設定など）を行う。
[i]紛失	情報を格納した機器やメディアを所持する許可を受けている者が、過失で紛失する。
[j]災害・事故	自然災害・事故などが原因で、不作為的に情報が漏洩・破壊される。
[k]システム障害	システムの障害が原因で、不作為的に情報が漏洩・破壊される。
[l]サイバー攻撃	不正プログラムなどを利用した大規模・組織的な攻撃で、情報の漏洩・改ざん・破壊やシステム停止などをもたらす。
[m]証拠の非保全	万が一、情報が漏洩・紛失・破壊された場合に、対象情報・漏洩ルート・行為者などが特定できず、迅速な対処が出来ない。

表1　企業・組織における情報セキュリティのリスク

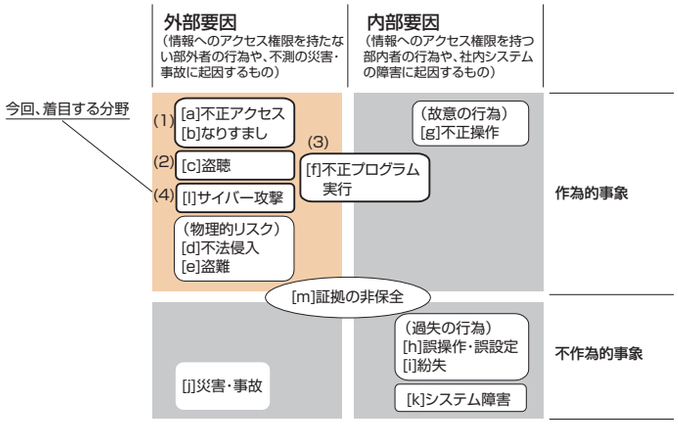

図1　情報セキュリティリスクの分類

入し、社内サーバへの外部からのアクセスや特定のIPアドレス以外からのアクセスを監視・制限することが基本的な対策である。最近では、不正アクセスがあったこと（逆に不正アクセスされていないこと）を証明するために、監視結果のログを改ざんできない形で残す仕組みなども、ネットワークフォレンジックとして注目されている。

「システム自体の脆弱性対策」としては、サーバのセキュリティホールを突いて不正アクセスされることを防ぐために、インベントリ管理システムでパッチあて管理を自動化することが効果的だ。さらに、サーバが仮に乗っ取られても、管理者権限自体を制限できるセキュアOSの採用が、オープンソース普及の動向とともに注目されている。また、SQLインジェクションやクロスサイトスクリプティングなど、Webアプリケーションの脆弱性を突いてくる攻撃に対しては、Webサーバとのやり取りをアプリケーションレベルで監視・制御するアプリケーションファイアウォールなどもある。

「アカウント管理・認証の強化」としては、生体認証やワンタイムパスワード、電子認証局などの導入によりユーザー認証や機器認証のセキュリティ強度を上げることが効果的である。またこれらの対策は同時に、一時的なアカウントの貸し借りや、管理者によるアクセス権限の設定ミス・変更漏れなど（一義的には部内者による不正行為や過失だが）への対策としても有効であり、シングルサインオンも含めていわゆるアカウント統合管理ソリューションとして全社・全組織的に導入する動きが活発である。

(2) 盗聴対策技術

インターネット時代の盗聴対策としては、「ネットワーク上でのパケット盗聴対策」、「(特に) 無線LAN上でのパケット盗聴対策」、「スパイウエアなどによる端末入力の傍受対策」、「電磁波漏洩対策」などが新しい課題である。

「ネットワーク上でのパケット盗聴対策」としては、例えばイーサネット上であれば盗聴ノード監視ソフトウエアなどの対策ツールもあるが、運用に稼動もかかり、かなり専門的な対策といえるだろう。一方で、社内LANへの不正な端末の接続を制限する認証VLANやインベントリ管理システムの端末認証機能を使う方が、社員の過失でウイルス感染端末を接続させることも防げるため、より一般的な対策である。

ただし、これらの対策は対処療法的な側面もあるため、併せて実施すべき対策として、重要情報については通信や電子ファイルを暗号化して保護することが、部内者の誤操作による情報漏洩を防ぐためにも必要と考えられている。

通信路の暗号化として、拠点間でVPNルータを導入したり、Webサーバへのアクセスを SSL暗号化したりといった対策に加え、最近ではコミュニケーションインフラとして定着した電子メールに対する暗号化対策（暗号メール）の必要性への認識が高まっている。

電子ファイルの暗号化は、PC端末のOSやオフィスアプリケーションの機能としても提供されているが、対策を徹底するためには、ファイルサーバ上に保管されるファイルを自動的に暗号化し、アクセス権限を管理するファイル管理システムが有効である。

「(特に) 無線LAN上でのパケット盗聴対策」としては、無線LANの普及初期の頃に比べればかなり企業側の意識が高まってきたようだが、最近ではWEPキー設定などの一般的なアクセスポイントのセキュリティ対策だけでなく、ユーザー認証や暗号鍵交換のセキュリティを強化した方式（WPA、IEEE802.11iなど）を採用した製品もリリースされており、今後一層の普及が予測される。

「スパイウエアなどによる端末入力の傍受対策」は、ネットカフェなどでインターネットバンキングなどを利用する際のキーロガー対策という印象が強いが、最近ではコンピュータウイルスのようにリモートから感染させられるものもあり、今後、企業でも（3）でご紹介する不正プログラム対策として認知度が高まるものと予想される。

「電磁波漏洩対策」も、まだ企業における対策の必要性の認知度が低いセキュリティ対策であるが、専用のアンテナや測定器を使えば技術的に盗聴が可能なことが分かっており、防衛関連など重要機密情報を扱っている現場では、PC端末のケーブルや

モニタから電磁波を漏れにくくするシールドや、わざとかく乱信号を発する装置などに対するニーズがある。

(3) 不正プログラム対策技術

企業において発生しているセキュリティインシデントの中で、端末やサーバのウイルス感染に伴うものは、いぜんとして上位を占めている。ウイルス対策ソフトの普及率はすでにかなり高いようだが、最近ではSoftEtherやWinnyなどのP2Pソフトの普及に伴う情報漏洩リスクも顕在化しており、必要とされる対策はより複雑化している。ここでは、「端末・サーバ側での対策」と「ネットワーク側での対策」に大別して紹介する。

「端末・サーバ側の対策」としてはウイルス対策ソフトがまず基本だが、さらにOSのアップデート状況やユーザーによるアプリケーション追加などを監視・制御するデスクトップ管理システム・インベントリ管理システムも、最近の情報漏洩事件の増加に伴って採用する企業が増えてきている。ただし、ネットワーク上のすべての端末・サーバへシステムのインストールを徹底することは、運用的にかなりの負担となり、各部門で自由にPC端末を購入するようなやり方では対策の徹底自体が難しくなっている。

そういう意味では、PC端末自体を廃止して、ウイルス対策や端末管理に伴う手間を大幅に改善してくれるシンクライアントを、業務専用端末として導入する企業も徐々に増えている。

一方で、「ネットワーク側での対策」は、端末やサーバ側での対策を補完するもの、というのが一般的な認識である。まず、IDS、IPSやファイアウォールでトラフィック上の特定パターン（シグニチャ）を監視することで、感染ファイルやP2Pソフトのパケットを遮断することができる。また、外部から持ち込まれた端末の接続を制御する検疫システムや認証VLANも、水際で感染を防ぐ対策だ。

ただ、攻撃手段も年々巧妙化してきており、Zero Dayアタックのように必ずしもウイルス対策ソフトやシグニチャ監視で防げないインシデントも、すでに発生している。またIDS、IPSで誤検知も含めて検知アラームが多くあがり過ぎるなど、運用上の課題も指摘されている。そこで最近では、トラフィック監視技術を応用して端末やサーバごとに発生するトラフィックの統計情報を解析し、異常トラフィックや異常通信の発生を検知する技術（NBAD; Network Behavior Anomaly Detection）を応用した製品が出始めている。従来のIDS、IPS機能と組合せることで、より高精度かつ少ない運用稼働で対策を実施できると期待されている。

(4) サイバー攻撃対策技術

サイバー攻撃の手口としては、単純に企業のサーバに不正アクセスするものや、ウイルスやワームを使って踏み台とする大量の端末から企業のサイトへのアクセスを集中させてサービスダウンに追い込むDDoS（Distributed Denial of Service）攻撃などがある。

前者は、企業が不正アクセス対策を徹底することで、インシデントの発生を防止することができると考えられる。また、データ破壊や改ざんが目的のケースも多いので、万が一に備えて、データバックアップシステムや改ざん検知の仕組みを導入することも重要である。

一方、後者（DDoS攻撃）は攻撃元が広域に分散しているため、企業側だけでできる対策は、サーバの負荷分散や予備サイトへの誘導など限定的なものしかない。そこで最近は、ISP側で攻撃トラフィックを特定し、迂回・廃棄することで、正常トラフィックを救済するDDoS攻撃検出・防御サービスを提供するところもある。

また、現時点ではサイバー攻撃というよりは、迷惑着信の部類に入るだろうが、スパムメールやスパム電話（SPIT; Spam over IP Telephony）なども、企業の生産性にダメージを与えるセキュリティ脅威である。スパムメールについては、対策ソフトなどにより、メールサーバやメーラである程度ふるい分けることができるが、スパム電話は取ってみないことには、それと分らないことも多く、まだ対策技術が間に合っていない新しい課題である。DDoS攻撃対策と同様、今後はISPや通信事業者側での対策が期待される分野といえる。

そのほかの動向

(1) 運用アウトソーシング

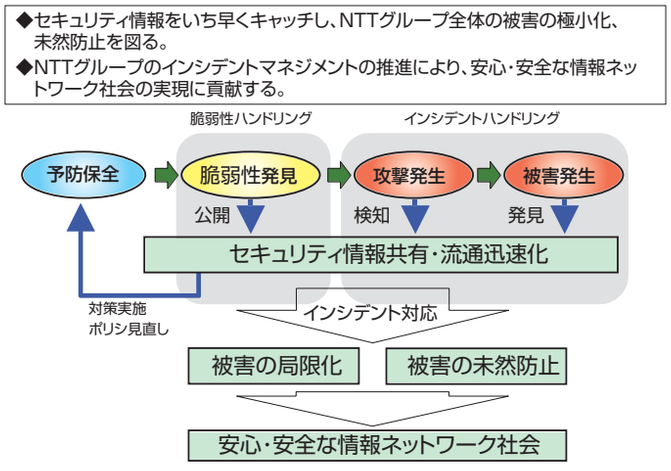

図２　NTT-CERTの活動

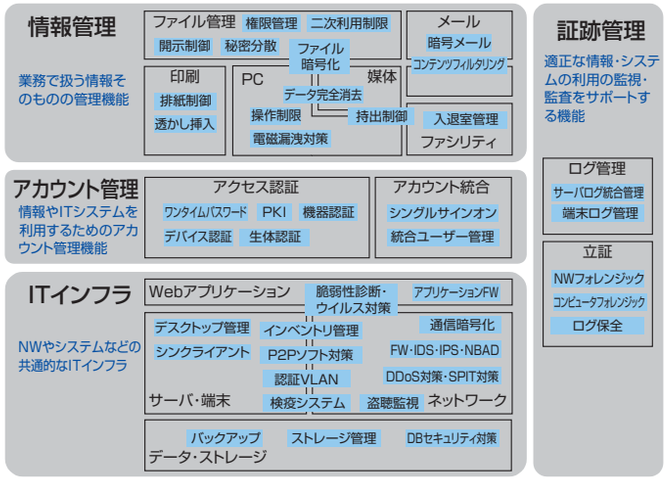

図３　情報セキュリティリスクへの主な対策技術

特に近年、セキュリティリスクが多様化・複雑化しており、ここで紹介した個々の対策を矛盾なく導入・運用するためには、かなりの知識・ノウハウや運用体制が必要とされる。そこで、情報セキュリティ対策のコンサルティングからシステムの保守・運用までを専門のサービス事業者にアウトソーシングする企業が増えている。

ITアウトソーシング市場の中でも、特にサーバやストレージのホスティングサービス、ネットワーク環境やデスクトップ環境の保守運用サービス（SOC; Security Operation Centerを含む）、などが高い伸びを見せている。これは、ハードウエア（サーバ、ストレージ、ネットワーク機器、端末など）のコモディティ化が進む一方で、さまざまなセキュリティ対策のニーズが顕在化し、システム全体を安定運用するためにますます専門的な知識・ノウハウが求められているという背景によるものと考えられる。

(2) CSIRTの活動

企業におけるセキュリティ対策はいたちごっこの側面があり、完全なセキュリティ対策システムというものは存在せず、システムの運用を通して対策の見直しやフィードバックを繰り返していく必要がある。また仮にインシデントが発生した際に、素早く状況を把握し、対策立案・実施するためにはある程度組織だって動けるような体制がどうしても必要になってくる。

このような企業・組織における組織的なセキュリティ活動を行う専門チームとして注目されている形態が、CSIRT（Computer Security Incident Response Team）である。CSIRTは各企業・組織レベルで活動するチームだけでなく、各国レベルで公共的な活動を行うチーム（米国のCERT/CC、日本のJPCERT/CCなど）もいる。また、これらのCSIRTどうしで情報交換する場（世界中の170以上のCSIRTが加盟するFIRSTなど）も用意されている。NTTグループでも、持株会社の情報流通プラットフォーム研究所の中にNTT-CERTを立ち上げており（図2参照）、グループ内でのセキュリティ情報の交換やFIRSTを介した情報交換を行っている。

まとめ

図３に情報セキュリティリスクへの主な対策技術を、大きく４つの分野に分けて示す。

今回紹介した外部からの脅威に対するセキュリティ技術としては、従来からセキュリティ対策として比較的認知度の高い、「ITインフラ」の分野を主に取り上げた。

一方で、最近は個人情報保護法や日本版SOX法への対応について企業の関心が高く、「情報管理」、「アカウント統合管理」、「証跡管理」の対策製品が、まだ市場全体は「ITインフラ」に比べかなり小さいものの、高い伸びを示している。同分野での動向は本誌11月号で紹介させて頂く予定である。