解 説 1

サイバー・セキュリティーの現状

― サイバー攻撃の動向とその対策に向けて ―

近年、さまざまな企業や組織で「サイバー攻撃」の被害が多発しています。攻撃の多くは、既存のセキュリティー対策の弱点を狙い、さまざまな手法を組み合わせて行われており、大企業や政府機関など高度なセキュリティー対策が施されていると考えられる組織でも被害が発生したことから、多くの企業がセキュリティー対策の見直しを迫られています。本稿では、昨今の「サイバー攻撃」について手法や特徴などを紹介した後、被害が多発している標的型攻撃への対策について解説します。

❶「サイバー攻撃」とは何か

最近、「サイバー攻撃」による被害が連日のように報道されています。個人ユーザーや一般企業だけでなく、高度なセキュリティー対策が施されていると考えられる政府機関や大企業が被害に遭っている事実に驚いた方も多いのではないでしょうか。

こういった被害報道はすべて「サイバー攻撃」という言葉でひとくくりにされています。しかし、一口に「サイバー攻撃」といってもその種類は多岐にわたるため、被害状況を調査すると、それぞれ攻撃の背景や攻撃手法がまったく異なっていることが分かります。

近年の「サイバー攻撃」は、攻撃者の目的によって以下の 4 種類に分類することができます。

① 金銭目的の攻撃
② 主義・主張を表明するための示威行為
③ 産業スパイ活動
④ 国家を背景とした諜報（ちょうほう）活動

インターネット上で最も多く行われている攻撃は、「① 金銭目的の攻撃」です。インターネット上の多数のユーザーにウイルスを感染させ、クレジットカード情報など金銭につながる情報を窃取します。

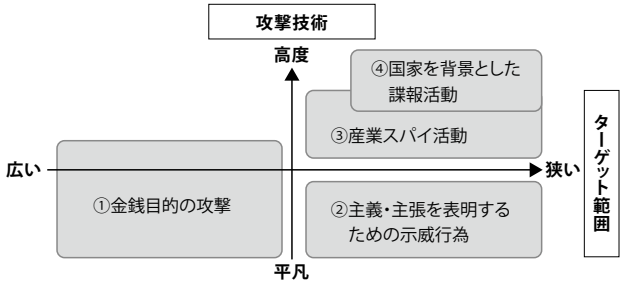

図 1.「サイバー攻撃」の目的別比較

それに対して、最近「サイバー攻撃」と呼ばれ報道されている攻撃の多くは、②～④に分類されるものです。これらの攻撃は目的や攻撃手法、技術レベル、ターゲットの範囲などが異なるため、取るべきセキュリティー対策も異なります。①～④の攻撃を、「攻撃技術」と「ターゲット範囲」の 2 点から比較すると、**図 1** のようになります。

②のタイプの攻撃は、攻撃の技術レベルが比較的低いため対策も容易ですが、③のタイプへの対策は、高度な技術を持った攻撃者によって行われる可能性が高く、対策も単一のセキュリティー機器の導入などといった容易なものではなく、企業ネットワーク全体の構成を見直しながらさまざまなポイントで対策を講じるなどの大掛かりな対策が必要になります。さらに④のタイプとなると、高度な IT 手法に手の込んだソーシャル・エンジニアリング（詐欺行為）を織り交ぜた攻撃が行われるため、侵入を完全に防ぐことは困難です。攻撃者に一部侵入されることを前提とした対策を考えなくてはなりません。

ただ漠然と「サイバー攻撃」への対策を講じるのではなく、まずはどのようなタイプの攻撃が自社の脅威となり得るのかを把握し、それに対してどこまで守る必要があるのかを明確にした上で、セキュリティー対策を検討することが重要です。

以降では、企業環境のセキュリティー対策を考えるために、まず、2 ～ 4 章にてどのような脅威が現実に発生しているのかについて幾つかの最近の事例を紹介します。その後、5、6 章では、昨今問題となっている標的型攻撃への対策方法について具体的に解説します。

❷ ハッカー集団による攻撃宣言

2011 年には、さまざまな企業や政府が LulzSec や Anonymous と名乗る集団からの攻撃を受けました。このような集団は、政府や特定の組織の方針に反対するという意思表明のために、その組織に関連する Web サイトを攻撃します。例えば、2011 年 6 月 19 日には LulzSec や

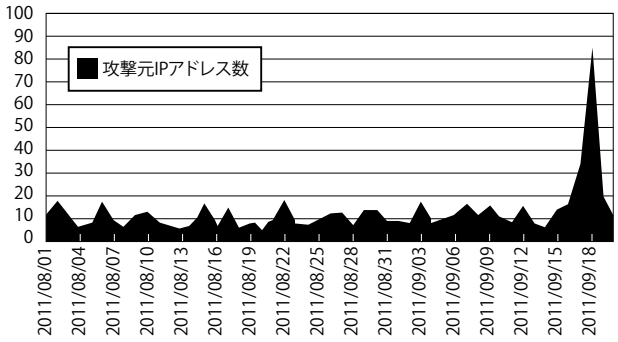

図 2. 中国からの SQL インジェクション攻撃の推移

Anonymous が「Operation Anti-Security（AntiSec）」と呼ぶ、政府や著名な組織からの情報窃取などを目的とした攻撃を表明しました。

また、2011 年 9 月には中国のインターネット・コミュニティーで、日本国内の Web サイトを攻撃する呼び掛けが行われました。中国では、満州事変の初日である 9 月 18 日に日本へ攻撃することを呼び掛ける活動が毎年行われています。

IBM の東京セキュリティー・オペレーション・センター（以下、東京 SOC）では、9 月 12 日ごろから中国を送信元とする国内の Web サイトに対する攻撃の増加を確認しました。**図 2** は中国を送信元とする SQL インジェクション攻撃の攻撃元 IP アドレス数の推移です。9 月 18 日には平常時の 8 倍程度の攻撃が行われました。

この種の攻撃は、主義・主張を表明するための示威行為として行われるため、Web サイトの改ざんやサービス妨害など、派手で分かりやすい手法が好まれる傾向にあります。また、デモ活動のように、同じ思想を持ち、このような活動に共感できる人を多く募り参加を促すため、誰でも攻撃が行える簡易な攻撃ツールの利用が呼び掛けられることがあります。東京 SOC で確認した 9 月 18 日の攻撃も自動攻撃ツールによる技術レベルの低いものばかりでした。攻撃者の数は多くても攻撃技術は高くなく、日ごろからセキュリティー対策を行っている環境では、このような攻撃の影響を受けることはありません。

しかし、サーバーやネットワークのリソースを浪費しようとする DDoS（Distributed Denial of Service：分散サービス妨害）攻撃は別です。DDoS 攻撃への参加が呼び掛けられると、それに応じた多数の送信元から大量のアクセスが発生するため、非常に大規模な DDoS 攻撃になる可能性があります。示威目的の攻撃に限らず、DDoS 攻撃の対策に関しては、十分な検討が必要です。

❸ 政府・企業の機密情報をターゲットにした攻撃

2011 年後半から、国内の防衛関連企業や政府関連機関が攻撃を受けたというニュースが立て続けに報道されました。そして、これらの攻撃は標的型攻撃であったと報告されています。標的型攻撃とは、ある特定の組織の機密情報などを狙って行われる攻撃です。最近では、特にメールを利用して標的型攻撃が行われる事例が多く、このような攻撃は標的型メール攻撃と呼ばれています。

この種の攻撃は、ターゲットの範囲が限定されているため、攻撃の実態が表面化しづらく、被害に気付きにくいという特徴があります。そして、被害が発覚した時には、すでに長期にわたり情報が漏えいした後である可能性が高いため、大きな脅威として問題になっています。

標的型メール攻撃に利用される不正なメールは、メールを受信したユーザーが不審に思わないように、差出人（From）を関係者に装ったり、件名や本文が時事ニュースを伝える内容になっていたりするものが多く確認されています。

東京 SOC でも 2011 年 3 月 11 日以降、東日本大震災の情報に見せかけた不正なメールが多数の企業や組織に送信されていることを確認しています。**図 3** は実際の震災の情報に便乗した不正なメールの例です。

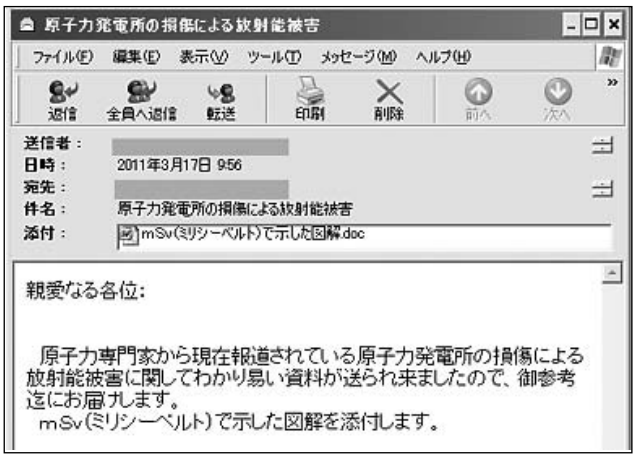

図 3. 標的型メール攻撃の例

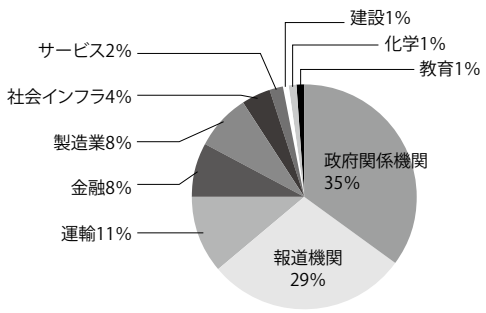

図 4. 標的型メール攻撃のターゲットとなった業種

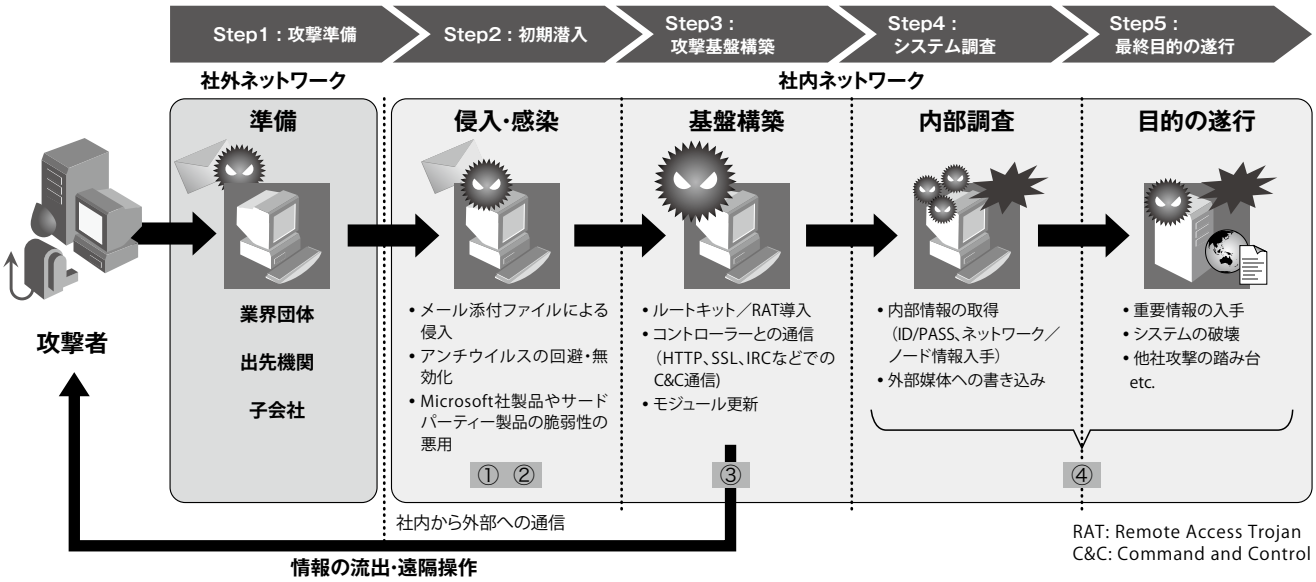

図 5. 標的型メール攻撃の攻撃パターン例［1］

不正メールにはファイルが添付され、この添付ファイルを開くことにより、開いたPCをマルウェアに感染させます。添付ファイルには主に以下の2種類が利用されます。

①Windows実行ファイル（ZIPなどで圧縮されている場合もある）
②脆弱（ぜいじゃく）性を攻撃する不正なコードが含まれたドキュメント・ファイル

特に多いのは、後者のドキュメント・ファイルによるものです。ドキュメント・ファイルには、Adobe ReaderやMicrosoft Wordの脆弱性を悪用してマルウェアに感染させようとする攻撃コードが含まれています。脆弱性のあるAdobe ReaderやMicrosoft Wordでこのような不正なコードを含むPDFファイルやWordファイルを開くと、マルウェアが起動し、システムへの侵入を許してしまいます。

図 4 は、東京SOCで確認した標的型メール攻撃の宛先となった組織の業種別検知割合を示しています。最も多く攻撃のターゲットとなっているのは政府関係機関であり、次に報道機関が多く狙われています。このことから攻撃者は国内の重要情報を狙って攻撃を仕掛けていることがうかがえます。そのほかにも、運輸業や金融、製造関係、社会インフラに関連する企業などさまざまな企業を狙って標的型メール攻撃が行われています。

❹ 近年のサイバー攻撃の特徴

多くの企業では過去何年にもわたり情報セキュリティー対策を講じてきましたが、現在もなおサイバー攻撃の脅威にさらされてしまうのはなぜでしょうか。

3章で説明した、標的型メール攻撃には以下の特徴があります（**図 5**）。

①電子メールにマルウェアを添付し、マルウェアそのものを暗号化・難読化することにより、IDS（Intrusion Detection System）やアンチウイルス・ソフトウェアによる検知を困難にする対策が行われている。

表1. 既存セキュリティー対策と回避手法の例

対策区分	セキュリティー対策	回避手法の例
入口対策	ファイアウオール	• メール添付ファイルやUSBメモリーの利用 • 内部から外部への通信（C&C通信）およびWeb（HTTP/SSL）やメール（SMTP）のポート番号の利用
	ゲートウェイ型アンチウイルス	• パッカーの利用、暗号化、難読化などのマルウェア解析対策技術の利用
	IPS/IDS	• メール添付ファイルやUSBメモリーの利用 • C&C通信の暗号化またはWeb（HTTP/SSL）やメール（SMTP）の通信プロトコルの利用
	Webフィルター	• 短期間のみ有効な攻撃サイトの設置
内部対策	ホスト型アンチウイルス／マルウェア対策ソフトウェア	• パッカーによる難読化、暗号化などの解析対策技術の利用 • システム・サービス、アプリケーション・サービスの乗っ取り
	OSを主体とした脆弱性管理	• アプリケーション／ミドルウェア脆弱性の利用 • 未公開（ゼロデイ）脆弱性の利用
	認証失敗ログの監視	• PC内部の認証情報の流用（Pass-the-Hash） • PC内に保管された文書、データに含まれる情報の利用（C&Cを通じた情報取得とリモート・コントロール） • 重要ファイル・サーバー／DBサーバーへの既存権限でのアクセス

STMP: Simple Mail Transfer Protocol
IPS: Intrusion Prevention System

② Microsoft 製品の脆弱性に加え、Adobe 社の Flash や Reader、Oracle Java SE などのサードパーティー・アプリケーションの脆弱性を悪用して不正プログラムを実行する。
③侵入された機器から Web ブラウザーと同じ通信経路で攻撃者の Web サイトにアクセスさせることにより、組織内の通常トラフィックに外部からのウイルスへの指令を隠ぺいする。
④侵入に成功した PC やサーバー上に保管されている認証情報などを用いて、近接するシステムに侵入し、最終目的となる攻撃対象に到達することで重要情報を盗み出す。

これらは、攻撃手法としては大変巧妙であり、攻撃者は一般的なセキュリティー対策の原理を熟知し、その弱点を突いたものであるといえるでしょう。**表 1** は既存のセキュリティー対策とその回避手法の例をまとめたものです。

❺ 今求められる対策とは

高度化する不正アクセスに企業が立ち向かっていくにはどうすればよいのでしょうか。IBM では、これまで導入されてきたセキュリティー対策をベースに、以下の観点から、見直しと改善を図るべきであると考えています（**図 6**）。

5.1 既存セキュリティー対策の徹底

従来行われてきた、外部からの不正アクセスを想定したセキュリティー対策（入口対策）は、今後とも継続して実施する必要があります。標的型攻撃の場合、情報詐取の第一段階としてターゲットのグループ企業や子会社が狙われる可能性があり、セキュリティー対策は本社ネットワークのみならず、各拠点、グループ企業や子会社のネットワークに対しても適用されなくてはなりません。このためには、既存のセキュリティー対策がどのようなもので、基準として何を求めているかを明確に文書化し、各拠点、グループ企業や子会社のセキュリティー担当者に理解してもらう必要があります。セキュリティー要員や運用・監視環境の確保が難しい組織については、本社側でセキュアなインターネット接続環境を提供するなどの支援策も検討すべきです。

高度化する攻撃への対応という観点からは、各システムに導入されるセキュリティー対策（内部対策）について、以下の 4 つの観点から見直しが重要であると考えます。

①OSやアプリケーションを含む脆弱性管理

昨今のサイバー攻撃のほとんどは、既知の製品の脆弱性が悪用されており、従来行われてきた脆弱性管理は現時点でも有効です[※1]。最近の攻撃ではこれまで主流であった OS の脆弱性に加え、Adobe Flash/Reader、Oracle Java SE などのアプリケーションの脆弱性を狙うケースが増えている

※1　マイクロソフト社の調査では、2011 年上半期におけるゼロデイと呼ばれる、まだ公開されていない脆弱性を利用しての攻撃は、全体の 0.12% となっています［2］。
※2　利用されている OS やアプリケーションが古く、脆弱性修正プログラムの提供が終了している場合には、最新版にアップデートする必要があります。

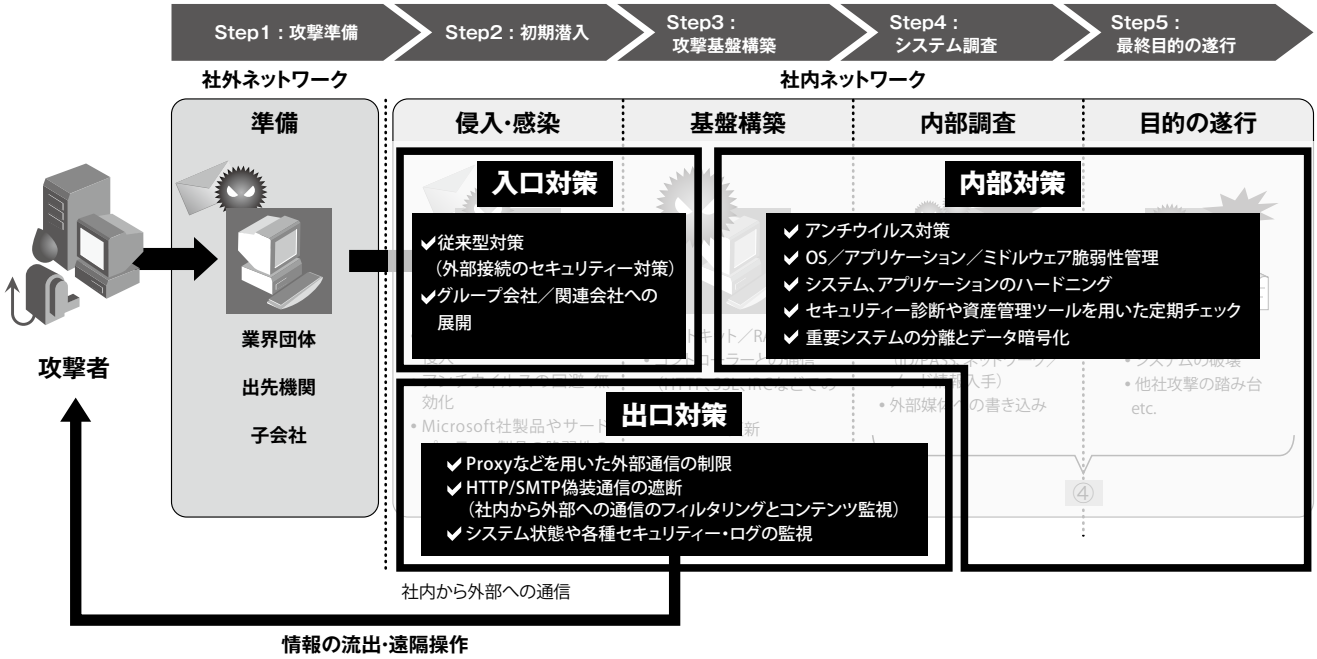

図 6. 今求められるセキュリティー対策［1］

ため、Windows Update などの Microsoft 社の OS やアプリケーションのセキュリティー脆弱性管理の仕組みに加えて、サードパーティー・アプリケーションのパッチの適用が可能なソリューションを検討する必要があります※2。

②システム／アプリケーションのハードニングと特権IDの分離

標的型攻撃で利用される攻撃手法と脆弱性の幾つかは、事前にシステムやアプリケーションのセキュリティー設定を適切にする（ハードニング）ことで、影響を抑えることができます。現在導入済みの機器に対して、ハードニングを再徹底することも有効な対策の 1 つです。

また、特に考慮すべき点として、特権 ID とユーザー ID の分離があります。通常業務のためにその PC 上の Administrator や root 権限といった特権 ID でログオンする必要はありません。通常業務を特権ユーザーから一般ユーザー権限に切り替えることにより、添付ファイルの閲覧やブラウザー経由でのマルウェア感染といった、一般ユーザーの操作が起点となる攻撃によるシステム全体の乗っ取りを抑制することができます。

③セキュリティー診断や資産管理ツールを用いた定期チェック

ハードニングやセキュリティー設定の適用状況は、インフラ・セキュリティー診断やシステム・セキュリティー・アセスメントによりチェックすることができます。マルウェアの一部には、Windows Update やアンチウイルス・ソフトウェアのシグネチャーなどのセキュリティーに関する自動更新機能を無効化させる機能を持つものがありますが、PC 資産管理ツールの持つソフトウェア・インベントリー機能を用いて、現在導入済みのソフトウェアのバーションやセキュリティー設定をチェックし、脆弱性修正やセキュリティー設定が、対象となるすべての機器に適用されているかを確認することで対応可能です。

④重要情報取り扱いシステムの分離

重要情報を取り扱うシステムやサーバーを、一般業務で使用されるネットワーク・セグメントから専用のセグメントに分離することも有効な手段です。このセグメントでは、Proxy 経由を含むインターネットへのアクセスや、通常の端末からのアクセスをプロトコル・レベルで禁止する（特に MS-RPC［Microsoft Remote Procedure Call］ や SMB［Server Message Block］ 通信なども禁止する）ことにより、セグメント内から重要情報の漏えいを難しくする効果が期待できます。また、システムの運用・保守は、メールやインターネット閲覧を行う業務用端末とは別の PC を用いて行うべきです。特に Domain Administrator や root 権限でログオンする端末は、業務端末とは別の、インターネットから隔離された環境に設置された端末を使用することが望ましいと考えます。

5.2 出口対策の導入

現在の高度化した攻撃に対して、既存の予防を前提としたセキュリティー対策だけで守ることは非常に難しいため、侵入を前提とし、侵入を速やかに検知するための対策（出口対策）が必要です。出口対策は、企業ネットワーク内部に入り込んだマルウェアや侵入者が行う諜報的な情報探索や外部との通信を検知・防護する対策全般のことです※3。出口対策で特に強化すべき点としては以下の 3 点が挙げられます。

①社内からインターネットへの通信の制限と監視

社内からインターネットへの通信を、ファイアウオールや Proxy を用いて許可されたユーザー／端末のみが特定のプロトコルでのみ許可されるよう制限する。

②HTTPやSMTP偽装通信の検知・遮断

IDS や Proxy により、HTTP や SMTP 内の通信を監視し、マルウェアによる偽装通信を検知、遮断する。

※3 IPA『「新しいタイプの攻撃」の対策に向けた設計・運用ガイド改訂第2版』では以下の8つを出口対策として挙げています［1］。
①サービス通信経路設計の実施 ②ブラウザー通信パターンを模倣するhttp通信検知機能の設計 ③RATの内部Proxy通信（CONNECT接続）の検知遮断 ④サーバー・セグメントへのhttpバックドア開設防止 ⑤重要攻撃目標サーバーの防護 ⑥マルウェアの内部拡散防止 ⑦内部拡散監視 ⑧ローカル・セグメント内感染拡大後のP2Pによる機能更新等防止

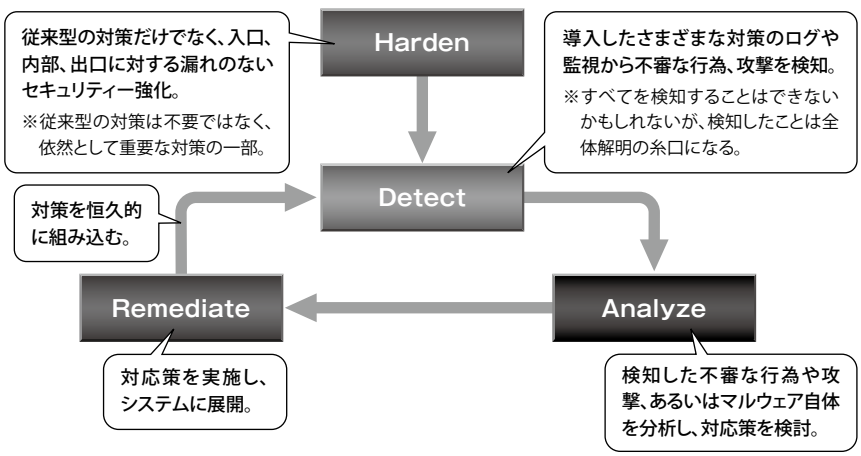

図 7. セキュリティーを維持・向上するためのプロセス

③システム状態や各種セキュリティー・ログの監視

各種セキュリティー・ログや重要システム、ネットワークの稼働状況などを監視し、許可されていない外部通信の試みや、突然のサーバー負荷情報などを検知する。

①の対策は、主にシステムの設計に関するものであり、すでに導入済みのファイアウオールやProxyサーバーの設計を見直すことでも対応できます。②、③の対策については24時間365日の監視が必要になるため、セキュリティー監視センター（SOC）などを利用することで高度の知識を有したセキュリティー専門家による常時監視体制を実現し、企業のセキュリティー運用の一部を代行してもらうことも一案となります。

5.3 セキュリティーを維持・運用するためのプロセス構築

セキュリティー対策は一過性のものではなく、維持・管理される必要があります。**図7**はIBMがセキュリティーを維持・管理する際に使用しているフレームワークです。

すべてのシステムは構築時に設定やセキュリティー・アプリケーションなどにより、基本的なセキュリティー対策と監視の仕組みを構築（Harden）し、各システムから上がってくるアラートや稼働状況の定期モニタリングを通じて不正アクセスの兆候を検知（Detect）し、詳細分析（Analyze）と、対応策を講じる（Remediate）必要があります。大変シンプルなモデルですが、この仕組みを国内のみならず、グローバルで実現できるよう、組織体制や監視環境を構築していくことが重要です。

❻ 効率的な対策を

近年のサーバー攻撃は、既存のセキュリティー対策を回避する仕組みを利用して行われるため、1つのセキュリティー・ソリューションで対応することは困難ですが、従来行われてきた対策の構成や設定を見直し、複数の対策を組み合わせて対応していくことは十分可能です。 そのためには現在自社に導入されているセキュリティー・ソリューションがどういったものであるかを分析し、弱点となる部分を補強することが必要となります。

サイバー攻撃の多くは、特定業種に属する複数の企業が同時に攻撃されることが知られています。自社のセキュリティー監視システムを外部の情報システムと連携させて分析する仕組みや、外部との情報連携を密にすることにより、自社のセキュリティー監視体制で検知することが難しい攻撃であっても、他社における攻撃情報が入手できれば、攻撃に対していち早く対応することができます。

高度化・多様化する脅威に対応できる高度なセキュリティー技術者を確保することが難しい場合には、外部のセキュリティー専門家の助言やレビューを受けることも効果的です。IBMではワークショップなどを通じて、グローバルにおけるセキュリティー管理や、標的型メール攻撃に関する課題をクイックに分析・抽出する活動も行っています。こうしたサービスや既存のIBMソリューションの活用を通じて、お客様におけるサイバー攻撃対策に役立てていただければ幸いです。

［参考文献］

［1］ 独立行政法人情報処理推進機構（IPA）セキュリティーセンター，“「新しいタイプの攻撃」の対策に向けた設計・運用ガイド 改訂第2版”，http://www.ipa.go.jp/security/vuln/documents/newattack.pdf（2011-11）.

［2］ 日本Microsoft株式会社 高橋正和，SecurityDay2012配付資料「今起きていること、今やるべきこと」，http://securityday.jp/?c=plugin;plugin=attach_download;p=materials2012;file_name=SecurityDay2012-1.pdf

日本アイ・ビー・エム株式会社
グローバル・テクノロジー・サービス事業
セキュリティー・オペレーション・センター
セキュリティー・アナリスト

朝長 秀誠 **Shusei Tomonaga**

［プロフィール］
2007年、日本IBM入社。マネージド・セキュリティー・サービスにてセキュリティー機器の導入を担当した後、セキュリティー・オペレーション・センターにてセキュリティー監視に従事。日経ITpro「今週のSecurity Check」連載や、IBMブログ「Tokyo SOC Report」から情報発信を行っている。

日本アイ・ビー・エム株式会社
グローバル・ビジネス・サービス事業
アプリケーションイノベーションサービス
セキュリティー & プライバシー
マネージング・コンサルタント

渡邉 浩一郎 **Koichiro Watanabe**

［プロフィール］
1995年、日本IBM入社。金融系を中心としたシステムのSE経験の後、セキュリティー・エンジニアとして、ペネトレーション・テストやFirewall/IDS導入、セキュリティー・インシデント対応などに従事。2004年より、コンサルタントとして現職に至る。ISO/IEC JTC1/SC27 WG4委員、CISA、CISSP、経営学修士。