NRI 未来創発
Dream up the future.

ITソリューションフロンティア
IT Solutions Frontier

特集「これからの情報セキュリティ」

07 | 2014 Vol.31 No.7
(通巻367号)

www.nri.com/jp

野村総合研究所
Nomura Research Institute

Adobe Readerのメニューバーで「表示(V)→ページ表示(P)」にある「見開きページ(U)」と「見開きページモードで表紙をレイアウト(V)」の2か所にチェックすると紙面のイメージでご覧いただけます。また、両面プリンターをご使用の場合、印刷時に「ページの拡大／縮小(S)」で「小冊子の印刷」を選択すると紙面に近い状態を再現できます。

ITソリューション フロンティア
IT Solutions Frontier
07／2014

視　点

特　集　「これからの情報セキュリティ」

NRI Web Site

日本社会の安全・安心のために

NRIセキュアテクノロジーズは、2014年5月に野村総合研究所（NRI）の情報セキュリティ関連事業を承継し、ID管理に関する6つの事業を統合した。当社は2000年8月の創業以来、NRIグループにおける情報セキュリティサービスの中核を担ってきたが、今回の事業統合は、高度化・複雑化する脅威に対する備えとして、お客さまの多様なセキュリティニーズにお応えする体制を構築し、サービスラインナップを拡充することを目的としたものである。

これにより、世界最高レベルのサービス品質を提供できる唯一無二の情報セキュリティ専門企業として、お客さまに今まで以上に安全・安心をお届けできるようになったと自負している。また、情報セキュリティを取り巻く環境がますます厳しくなるなかで、事業規模、従業員数ともに業界最大となったことにより、今後は業界全体をけん引していく役割も求められると考えている。

冒頭に記したように当社の設立は2000年8月だが、サービスの開始は1995年にさかのぼる。インターネットの商用利用が始まったのはそれよりさらに前の1990年代初頭である。それ以後、企業・組織は、時間的・場所的な無限定性、高速性という利点を持つインターネットを、国境を越えて事業活動を効率化しながらビジネスを加速させるためのアクセルとして利用してきた。一方で、そのインターネットが持つ匿名性、無痕跡性という特徴を業務においてどのようにカバーするかにも多くのリソースが割かれた。

お客さまのシステムおよびネットワークとインターネットとの境界において24時間・365日の監視を行う「マネージドセキュリティサービス」と、情報セキュリティに関するポリシー策定などのコンサルティングサービスの提供に端を発する当社も、この20年の間にお客さまのさまざまなご要望を受け、各サービスを進化させてきた。また、情報セキュリティ関連のソフトウェアの開発といった分野にも事業を拡大してきた。

今後もこれらの事業を発展させることは不可欠であるが、最近、情報セキュリティの質的な転換が迫られていることを強く感じる。その要因は、サイバー攻撃の内容やそれを行う犯罪組織の性格がこれまでとは異なったものになってきていることである。

例えば、「Stuxnet（スタックスネット）」という特殊なマルウェア（コンピュータウイルスなどの悪意あるプログラム）によってイランのウラン濃縮施設が稼働不能に陥るという事件が2010年に起きた。PCが感染しても何も影響が出ないという特殊なマルウェアの出現もさることながら、国家機関のように膨大な資金と人的リソースを持つ組織が背後にあることをうかがわせる事件であったことも衝撃的だった。この事件を契機として、重要

NRIセキュアテクノロジーズ
代表取締役社長
増谷　洋（ますたにひろし）

インフラや制御システムのセキュリティ対策の重要性が認識されるようになった。しかし、長きにわたりインターネットとは一線を画していると思われてきたシステムに、短期間で抜本的な対策を施すことは困難である。そのため当社では、政府機関と連携して、これらに携わる方々の意識改革を含め各種の施策を推進していく取り組みを始めている。

また、標的型攻撃（特定の企業・組織を対象に機密情報の詐取をねらう）の存在が広く知られるようになった2011年ころから、サイバー攻撃とその被害が連日のように報じられている。標的型攻撃はステルス性が高い（探知されにくい）という特徴から、攻撃を受けたことに気付かないことがある。そのため、報じられた以上に被害が発生していることもあり得る。被害に遭わないためには、ネットワークの監視を高度化し、不審な通信を一刻も早く発見して対応することが重要となる。当社では、日頃からのマルウェア感染防止などの標的型攻撃対策、情報および情報システムの保全・保護、有事の際のインシデント対応の迅速化などにおいてお客さまをサポートしていく所存である。

インターネットバンキング利用者の預金を不正に送金するなどの被害も多発している。最近は「Zeus（ゼウス）」と呼ばれるマルウェアとその亜種によるものが多く、2014年は過去最高の被害額になることが確実といわれている。標的型攻撃への対策も含め、金融機関は情報セキュリティを強固にすることを他の業界以上に求められる。そのため、当社では金融機関が相互に情報の連携・共有ができる枠組みの構築を図っていきたい。各社の情報を集約し、同じ課題を持つ者が集まって問題を解決することで、各社は少ないコストで今まで以上の対策を推進できる。

最後に、2020年の東京オリンピックに向けた対策について触れておきたい。2012年に開催されたロンドンオリンピックでは、期間中にサイバー攻撃が２億回以上もあったという（www.v3.co.uk/v3-uk/news/2279265/bt-reveals-over-200-million-hack-attempts-on-london-olympics-2012-website）。

今から６年後の東京オリンピックの開催時にネットワークの状況がどのようになっているかを正確に予測することは困難だが、ロンドンとは比較にならない備えが求められることは間違いない。それには官と民の連携、グローバルな連携が不可欠である。２万２千人が不足している（独立行政法人情報処理推進機構による2012年４月27日発表の報告書）といわれる情報セキュリティ人材の育成も急務である。

ネットワーク社会の健全な発展に対して責任ある企業として、本稿で述べた課題の解決に向け、当社がその原動力となることを目指していきたい。 ■

情報セキュリティの現状と課題
―企業実態調査の結果から―

NRIセキュアテクノロジーズでは、広く社会の情報セキュリティ意識向上を目的として、毎年国内３千社あまりを対象に情報セキュリティに関する実態調査を行っている。本稿では、2013年の調査から明らかになった情報セキュリティをめぐる現状や課題、最近の動向などを紹介し、本稿以降の特集論文の導入としたい。

情報セキュリティをめぐる状況

NRIセキュアテクノロジーズは、2002年から毎年、「企業における情報セキュリティ実態調査」を行い、結果を公表している。直近の2013年の調査（以下、「実態調査」）からは、注目すべき動向や課題として次の４つが浮き彫りになった。

①標的型攻撃が増加している
②サイバー攻撃に対応する専門組織を設置する企業が増えている
③情報セキュリティ人材が不足している
④グローバルに事業を展開している企業で、国内外のセキュリティレベルに差がある

(1) 増加する標的型攻撃

標的型攻撃というのは、広く不特定の相手にコンピュータウイルスなどを送りつけるのではなく、特定の企業や企業グループ、官公庁、特定の業界など、対象を絞って攻撃を仕掛けるものである。

代表的な攻撃手法として、コンピュータウイルスなどを特定の相手に送りつけるもの、Webサイトを構築している企業のWebサーバーソフトウェアのぜい弱性（セキュリティ上の欠陥）を利用して攻撃を仕掛けるものなどがある。

「実態調査」では、17.2%の企業が「この１年の間に標的型攻撃を受けた」と回答している。さらに、標的型攻撃を受けた企業の30.7%が「被害が発生した」としている。標的型攻撃は、以前は“愉快犯”的なものが多かったが、ここ数年は個人情報やクレジットカード情報など金銭に結び付く情報の詐取を目的としたものが多くなっている。

(2) 目立つ専門対応組織設置の動き

Webサーバーをねらった標的型攻撃への対応策として、そのぜい弱性の解消はもちろん重要だが、攻撃が巧妙化していることからこれらに組織的に対応する必要性が高まっている。そこで、攻撃を予防しつつ、もし攻撃を受けても被害を最小にとどめるための対応を行うCSIRT（Computer Security Incident Response Team。「シーサート」と読む）と呼ばれる専門チームを社内に設置する企業が増えている。

「実態調査」ではCSIRTを「構築済み」あるいは「１年以内に構築予定」とする企業が、１年前の調査に比べて2.7倍の伸びとなっている。これは、標的型攻撃への対策としては比較的安価に実施できる「従業員教育」を

NRIセキュアテクノロジーズ
取締役
コンサルティング事業本部長
菅谷光啓（すがやみつよし）

専門は情報セキュリティに関する
調査・コンサルティング

抑えていちばん大きい伸び率である。

(3)不足する情報セキュリティ人材

CSIRTは、従来のような対症療法的な一時的な活動ではなく、組織的で継続的な活動を行うものであり、また情報セキュリティに関する高度な知識を持つ人材が求められる。しかし「実態調査」では、多くの企業でこうした人材が不足しており、担当者のセキュリティのスキルは不十分と感じられていることが分かった。人材の調達に関しては、社外から調達するのではなく、社員を育成する方針の企業が多いことも明らかになっている。有効に機能するCSIRTを一朝一夕に作るのは難しいので、チームを支える人材の育成を少しずつでも進めることが必要だろう。

(4)不十分なグローバルセキュリティ統制

「実態調査」でもう1つはっきりしたのは、グローバルに展開している企業の国内外のセキュリティレベルの差である。国内の支社および支店ではセキュリティ統制（セキュリティレベルの均一化）を実現しているとする企業が90%以上だが、海外の支社および支店では50%前後にとどまっている。その要因を聞くと、最も多いのが「現地のセキュリティ意識が低い」であった。こうした意識の問題や、「セキュリティ専門の担当者を置けない」という現地事情のなかで、いかにして国内と同水準までセキュリティのレベルを引き上げるかが、グローバル展開している企業の多くが抱えている課題である。

社会インフラへのサイバー攻撃の脅威

日本でまだ大きな被害は発生していないが、社会インフラを支える制御システムへのサイバー攻撃の可能性が無視できなくなっている。金銭目的のサイバー攻撃と違って、社会インフラへの攻撃は国を標的としたサイバーテロである。日本では日常的に意識することは少ないが、海外では実際にサイバーテロと思われる攻撃が発生している。そのため2012年にCSSC（制御システムセキュリティセンター）が設立されるなど、日本でも徐々に対策の必要性が認識され始めている。

Windows XPのサポート終了の影響

2014年4月9日にWindows XPのサポートが終了し、今後はぜい弱性が発見されても修正プログラムは配布されない。しかし「実態調査」によると約3割の企業が「サポート終了後もWindows XPを継続して利用する」としており、IDC Japanの予測でも、2014年6月末で法人241万台、家庭向け351万台が残るとしている（www.idcjapan.co.jp/Press/Current/20140407Apr.html）。攻撃者にとって、Windows XP搭載PCは格好の標的となり、一般消費者をねらったID・パスワードの詐取による金銭被害はもちろん、企業への標的型攻撃が増えることが予想される。企業はますますインシデント対応を強化する必要に迫られるであろう。 ■

Webサイトへの攻撃の傾向と対策
―Webアプリケーションのリスク TOP 10―

Webサイトへの攻撃の主流は、ネットワークやOS（基本ソフト）レベルのぜい弱性（セキュリティ上の弱点）を突くものから、Webアプリケーションのぜい弱性を悪用するものへとシフトしている。本稿では、Webアプリケーションの代表的なリスクを概説し、最近の事件や攻撃の傾向を踏まえながら、有効な対策について解説する。

Webサイトへの攻撃の変化

2000年の１月から２月にかけて、中央省庁のホームページのコンテンツが改ざんされる事件が立て続けに発生し、Webサイトへのサイバー攻撃が大きな社会問題として認識されるようになった。またその頃から、Webサーバーを感染させてコンテンツを改ざんする「ワーム」と呼ばれる自己増殖型のウイルスが猛威を振るうようになった。

当時のWebサイトの改ざんやワームは、ファイアウオールやOSの設定不備を悪用したWebサーバーへの不正ログインや、Microsoft社のIIS（Internet Information Services）のようなWebサーバーソフトウェアのぜい弱性を悪用したものがほとんどであった。しかし、情報セキュリティの重要性が認識されてソフトウェアベンダーもぜい弱性が発見されると修正プログラムを迅速に提供するようになった結果、ネットワークやOS、Webサーバーソフトウェアのぜい弱性を突く攻撃は効力を失いつつある。

それに代わって数が増え威力を増しているのが、Webサイト向けに独自開発したWebアプリケーションや、Webアプリケーション開発のフレームワーク、CMS（コンテンツマネジメントシステム。Webサイトのコンテンツを編集・配布するためのソフトウェア）のぜい弱性を突く攻撃である。

Webアプリケーションの主なリスク

表１は、Webアプリケーションのリスクを、リスクの大きい順に10項目示したものである。これはWebアプリケーションのセキュリティ向上を図る非営利組織「OWASP（Open Web Application Security Project）」が作成したもので「OWASP Top 10」と呼ばれている。OWASPは良質なツールやガイドラインを無償で配布しており、業界内における評価も高い。「OWASP Top 10」は2004年から３年おきに改訂され、2013年には最新の改訂版が刊行された。

(1) 認証とセッション管理の不備

最近数多く報道されているセキュリティ事件や、NRIセキュアテクノロジーズのセキュリティ運用サービス「MSS（マネージドセキュリティサービス）」で見られる傾向と合致するリスク項目としては、まず2010年版の３位から2013年版の２位に上昇した「認証とセッション管理の不備」が挙げられる。

NRIセキュアテクノロジーズ
MSS事業本部長
小田島　潤（おだしまじゅん）

専門はPKI（公開鍵暗号基盤）、認証、
Webアプリケーションセキュリティ

表1　「OWASP TOP 10」(2013年版)に挙げられたリスクとその概要

順位	項目	概要
1	インジェクション	データベースなどに格納された重要情報を不正に参照・更新するコマンドを注入・実行される
2	認証とセッション管理の不備	パスワードの総当たり攻撃や、ログイン状態の情報を不正に入手されることで、他人に成りすまされる
3	クロスサイトスクリプティング	他人のブラウザ上でスクリプト言語が不正に実行され、ログイン状態等の重要情報が詐取される
4	安全でないオブジェクトの直接参照	WebアプリケーションがWebサーバー上のファイルやデータベース内のレコードを参照する際に、ユーザーからの入力値をそのままキー情報として用いるために、本来はアクセス権のない情報を攻撃者が参照できてしまう
5	セキュリティ設定のミス	一般には公開すべきでないコンテンツや機能を意図せず公開してしまうなど
6	機密データの露出	強度の弱い暗号アルゴリズムが許可されているなど
7	機能レベルアクセス制御の欠落	本来は権限のない機能を利用できてしまう(部長でない者が部員の人事評価を更新できるなど)
8	クロスサイトリクエストフォージェリ	正当なユーザーが、意図しない操作を不正に実行させられる(攻撃者の口座に不正に入金させられるなど)
9	既知のぜい弱性を持つコンポーネントの使用	使用する暗号化ライブラリー、フレームワーク、CMSなどのコンポーネント(部品)に既知のぜい弱性がある
10	未検証のリダイレクトとフォワード	他のWebサイトに移動する機能がある場合、ユーザーにより入力された宛先の検証が十分でないと、悪意のあるサイトへ誘導される

つい最近も、大手航空会社のマイレージポイントを管理するWebサイトがアカウントハッキング攻撃（別のWebサイトから不正に入手したID・パスワードの一覧を使って機械的に不正ログインを試みること）を受け、ユーザーのマイレージポイントが不正にギフト券などに換金されるという事件が大きく報道された。

根本的な対策としては、IDとパスワードに加えてワンタイムパスワード（ランダムに発生させた1回限り短時間だけ有効なパスワード）を導入するなど、認証を強化することが挙げられる。しかし、利便性やコストとの兼ね合いもあり、全てのWebサイトで導入することは難しい。従って、現実的な対策としては、一定時間内に一定回数以上の認証失敗を検知した場合にそのアカウントを使用停止にする方法、IDを変えて何回もログインを試みる動作を検知した場合に当該送信元からのアクセスをブロックする方法が考えられるが、不正と判断する適切なしきい値を設定するには高度な運用ノウハウが求められる。

(2) OpenSSLのぜい弱性

次に、6位の「機密データの露出」と9位の「既知のぜい弱性を持つコンポーネントの使用」に関連するリスクに触れておきたい。本稿の執筆時点で、Heartbleed（心臓出血）と呼ばれるOpenSSLのぜい弱性を突いた攻撃がホットな話題となっている。OpenSSLは、暗号化通信の標準的なプロトコルであ

るSSL（Secure Socket Layer）およびその後継のTLS（Transport Layer Security）の機能をオープンソースで実装したライブラリー（プログラム部品）である。比較的最近のOpenSSLのバージョンから実装されたHeartbeat（鼓動）機能にバグ（プログラムのミス）があり、Webサーバーのメモリー上に一時的に格納されたパスワードなどの機密情報が抜き取られる危険性がある。

抜本的な対策は、ぜい弱性が修正されたバージョンのOpenSSLに更新するか、またはHeartbeat機能を無効にすることである。

(3)既知のぜい弱性を持つコンポーネントの使用

2013年版の9位に挙げられた「既知のぜい弱性を持つコンポーネントの使用」は、初めて他の項目から独立して取り上げられたものである。これは、2011年に発生したSONYグループのWebサイトにおける大規模な個人情報の漏えいが、「Struts2」というWebアプリケーション開発フレームワークのぜい弱性を突いた攻撃によるものとされていることや、アプリケーション開発言語兼フレームワークの「Ruby On Rails」やCMSの「WordPress」のぜい弱性を突いた攻撃などが多数発生したためと推測される。

スマートデバイスやクラウドコンピューティングの隆盛により、Webアプリケーション開発のニーズはますます高まっており、開発生産性を向上させるためには、これらのフレームワークやCMSを積極的に活用せざるを得ない。そのため、Webサイトを構成する全てのソフトウェア部品のバージョンとそのぜい弱性を、独自開発したWebアプリケーションと同等に管理することが求められる。

Webアプリケーションのリスク対策

Webアプリケーションのリスク対策の王道は、設計段階からセキュリティを考慮し、その後の開発・テストの工程で“セキュリティを作り込む”ことである。すなわち、基本設計の段階で、各機能要件において想定されるセキュリティリスクとその対策を、「セキュリティ概要設計書」として記述し、その後の各工程においても、他の機能要件と同様に詳細化および実装し、テストを進めることである。しかし、本番稼働中のWebアプリケーションに対してこの対策をそのまま実施することは難しい。そこで、Webアプリケーションを改修することなくセキュリティを強化する製品が登場している。表2は、前述した「OWASP Top 10」のリスクに対して、どのタイプの製品が向いているかを示したものである。

①WAF（Webアプリケーションファイアウオール）

WAFはWebアプリケーションへの攻撃対策に特化したファイアウオールで、Webアプリケーションの通信のやり取りを把握して不正侵入を防御する。濃淡はあるものの各リ

表２ 「OWASP TOP 10」(2013年版)のリスクに対する対策製品の得意・不得意

順位	項目	WAF	IDS/IPS	DB FW
1	インジェクション	○	△	○
2	認証とセッション管理の不備	○	△	×
3	クロスサイトスクリプティング	○	△	×
4	安全でないオブジェクトの直接参照	△	×	○
5	セキュリティ設定のミス	○	○	×
6	機密データの露出	△	×	×
7	機能レベルアクセス制御の欠落	△	×	×
8	クロスサイトリクエストフォージェリ	○	×	×
9	既知のぜい弱性を持つコンポーネントの使用	○	○	×
10	未検証のリダイレクトとフォワード	○	×	×

※機能の詳細は製品によって異なるため、NRIセキュアテクノロジーズのセキュリティ運用サービス「マネージドセキュリティサービス」における採用製品を前提に比較した。

スクに満遍なく対応できる。

②IDS(侵入検知システム)/IPS(侵入防御システム)

IDSは、攻撃パケットに含まれる特徴的なパターンを事前に定義しておき、観測された通信をこれと比較・照合して、攻撃と判断された場合に管理者に通知するシステムである。IPSはこれに自動遮断機能を加えたものである。比較的古くからある製品で、Webアプリケーション以外の通信プロトコルにも適用できるが、「OWASP Top 10」のリスクに関してはWAFと比較してカバー範囲は狭い。しかし、前述したHeartbleedは、Webアプリケーションの通信が始まる前の暗号化処理の段階で成立する攻撃であったため、WAFでは検知できなかったがIDS/IPSでは検知できた。また、リスクによっては監視設定と運用を工夫することでWAFと同等の導入効果を発揮させることもできる。

③DB FW(データベースファイアウオール)

DB FWは、企業の基幹システムにデータベースが普及している現状を踏まえ、内部からか外部からかを問わず、データベースへの不正アクセスや情報漏えいの防止に特化した新しいタイプのファイアウオールである。「OWASP Top 10」の1位に挙げられている「インジェクション」は、主にデータベースに対する問い合わせ言語であるSQLを不正に操作する攻撃であるため、特にDB FWによる抑止効果が期待できる。

以上、主にWebアプリケーションに対する攻撃について、その概要や対策を述べてきた。NRIセキュアテクノロジーズは、Webアプリケーションのぜい弱性診断と対策の助言、上記対策製品の運用監視サービスを通じて安全・安心なインターネット社会の実現に貢献したいと考えている。 ■

組織内CSIRTへの期待
―インシデント対応力を向上させるために―

事業の継続的な成長のためにはシステムの安全・安心は必須であり、情報セキュリティ対策は必然である。特に、企業にとって今後より重要になってくるのはインシデント（セキュリティの脅威となる出来事）への対応力である。本稿では、組織としてインシデント対応力を高めるために企業はどう取り組むべきか考察する。

浮き彫りにされたぜい弱性マネジメントの難しさ

(1)頻発する重大インシデント

近年、情報セキュリティ事故のニュースが後を絶たず、各企業はその都度、自社への影響やその範囲を確認する作業に追われる。2014年に入って早々に、通常は年に10回あるかどうかという「すぐに対応しなければならないぜい弱性（セキュリティ上の欠陥）」に関する注意喚起が続けて出された。いわゆるOpenSSL/Struts騒動である。「OpenSSL」は暗号化通信の標準的なプロトコルSSLをオープンソースで実装したプログラム部品、「Struts」はWebアプリケーション開発のフレームワークで、ともに重大なぜい弱性が発見された。監督官庁からも即時かつ過去にさかのぼって調査することが求められ、対応に追われた関係者は少なくなかったであろう。

システムを構成するOS（基本ソフト）やアプリケーションなど、さまざまなソフトウェアにはたびたび重大なぜい弱性が発見・公表され、修正プログラムや新バージョンがリリースされる。システム担当者は現有システムに関するぜい弱性情報を収集し、システムへの影響を考慮して修正の適用可否を判断する必要がある。影響が極めて大きい（個人情報の漏えいやシステムの乗っ取りにつながる）と判断されれば、業務やシステムへの影響を緩和する策を即座に講じるとともに、修正プログラムの適用やバージョンアップの準備に取り掛からなければならない。これらをぜい弱性マネジメントと呼ぶ。当たり前で地味な作業だが、最近はぜい弱性の公表からそのぜい弱性を突いた攻撃が発生するまでの時間は極端に短くなってきており、対処が難しくなっている。今回の騒動はそのことをあらためて浮き彫りにした。

(2)緊急対応の要否判断の難しさ

まず、緊急対応を行うべきか否かの判断自体が難しい。OpenSSLの場合、SSLプロセス上のメモリー情報が外部から読み取られるぜい弱性が公表された４月７日から数日の間は、影響範囲として「秘密鍵が漏えいする可能性がある」といった点に焦点が当てられていた。そのため、フィッシングサイトを立てられる、過去の電文を解読されるといった攻撃が想定された一方、秘密鍵が漏えいしたからといって誰でも簡単に攻撃できるわけではないという意見も多かった。このように、攻

NRIセキュアテクノロジーズ
コンサルティング事業本部
テクニカルコンサルティング部長
観堂剛太郎（かんどうこうたろう）

専門はサイバーセキュリティに関するコンサルティング

撃の発生可能性を含めた影響範囲の判断に迷うという状況があったのではないだろうか。

しかし、十分な知識を有するセキュリティの専門家の助けがあれば、即座に流通した攻撃コードを検証して、取得され得るメモリー情報に何が含まれるのかを知ることができただろう。それによってユーザーが直前に送信したログインIDやパスワードなどが読み取られる危険があり、それが再送されるだけで成りすましが行われ得ることが理解できていれば、緊急対応が必要なことは一目瞭然だったはずだ。

(3) 対応の適切さを確かめることの難しさ

対策が決まり実施した後は、対策が“全体で”適切に実施されたかを追跡する必要がある。しかし、日頃からインベントリー管理（ハードウエアおよびソフトウェアのスペックやバージョンなどの情報管理）ができていない場合は容易ではない。

重要な基幹システムならばともかく、クラウドで構築された消費者向けの期間限定のWebサイトや、M&Aで子会社化した企業のシステム、グローバル企業の海外システムなど、インターネット公開システムの全体を普段から把握しておくことは難しい。たとえ把握できていたとしても、それらシステムが利用している製品をバージョン単位で確認しなければならない。ヒアリングベースでそれを行うことは、相応に時間と手間がかかる。

今回の「Struts」のぜい弱性の場合、数年前からたびたび重大な問題が発生していたため「Struts」を利用するシステムは把握できていたかもしれない。しかし、グローバル企業のシステムのライフサイクルを考えれば、情報が古いということは十分にあり得る。

対策面でも、個別のシステムはそれぞれ事情を抱えており、一律の対策方針にそぐわないことがままある。修正プログラムを適用すれば済むケースは、テストの負荷はあるものの対応は比較的楽である。しかし、公式サポートが終了している製品を使っているシステムや、修正プログラムが公開される前からぜい弱性が明らかになる場合（「Struts」のケース）は、暫定的な回避策を検討しなければならない。IDS（侵入検知システム）で検知する、WAF（Webアプリケーションファイアウオール）で止めるなど、個別のシステムの事情を考慮して採用される回避策が本当に妥当であるかまで見ていかなければ“全体”の追跡にはならない。

(4) 求められる一元的な対応

企業はこの難しいぜい弱性マネジメントに正面から向き合わなければならない。今後も同様に、即座に対応しなければならない危険度の高いぜい弱性は確実に報告され、対処が遅れれば遅れるほど、被害に遭う可能性が高まる。その中で、上述したとおり、システム担当者が個別に対応するには限界があり、企業として統制された状態で一元的に対応していくことが求められる。

リスト型アカウントハッキングへの対応

2013年以来、企業はリスト型アカウントハッキングに悩まされ続けている。攻撃者は、どこかで入手した大量のID・パスワードのリストを用いて、標的とするシステムにログインを試行し続ける。そのシステムに同じID・パスワードが登録されていればログインが成功し成りすましが行われるといった攻撃手法である。この攻撃は、今もどこかのシステムからアカウント情報（ID・パスワード）が漏えいしており、また複数のシステムに同じIDとパスワードが登録されることが多いために有効になりやすいのである。

オンラインゲーム業界では数年前から発生していた問題だが、2013年の５月ごろから他の業種でも攻撃を受ける事件が断続的に発生した。今でこそ脅威の認識が広まったが、有効な暫定措置を取ることも難しく、システムを停止せざるを得ないこともあったのではないかと思われる。

システムの側では、２要素認証や端末識別の導入といった根本的な対策は存在するが、ユーザーの利便性への影響、導入に要するコストや時間を考えると簡単に導入できるものではない。攻撃を受けている場合の暫定的な措置にはパスワードリセット、CAPTCHA（画面に表示される文字を入力させる）や追加認証（ID・パスワード以外に生年月日などを要求する）の実装などがある。

攻撃元アドレスからのアクセスをブロックするという方法もあるが、最近は国内のプロバイダーのIPアドレスを順次変更しながら攻撃するケースが目立ち、大量の攻撃元IPアドレスを前に手の打ちようがないというケースもある。これは、攻撃者が家庭用ブロードバンドルーターのぜい弱性を突き、家庭で利用されているプロバイダーのアカウント情報を大量に詐取して攻撃に悪用しているためである。プロバイダーや通信事業者は、これを根絶するために利用者環境の調査や注意喚起などを行っているが、時間がかかるのはやむを得ない。またプロバイダーは「通信の秘密」を守る義務もあり、被害側の同意や協力がなければ調査や対策が困難である。攻撃を受けた企業がこうした事情を理解してプロバイダーと連携することにより、現に起きている攻撃の状況が改善される可能性がある。

このように対策は見えなくはないが、何をするにも一定の時間がかかり、少なくとも数日の間システムをどうするか、少ない材料で決断しなければならないことがある。また、業務やシステムの安全のためにあらゆる手段を検討する必要があるために、１つの組織だけでは解決できないこともある。プロバイダーやセキュリティベンダー、時には製品メーカーとも連携し、協調して解決策を模索することも必要であろう。緊急の場合には、同種の攻撃を受けた経験を共有する者は、この上ない相談先となるのではないだろうか。対策

の選択肢を検討し決定するために貴重な情報の交換ができることだろう。

インシデント対応力を高めるための組織内CSIRT

ぜい弱性マネジメントでもリスト型アカウントハッキングへの対応でも、一元的な対応と組織間の連携が重要であることは上述のとおりである。その認識から、企業の間で注目され実際に取り組みが進むようになっているのが、インシデントの予防や緊急対応を担う専門の組織、CSIRT（Computer Security Incident Response Team。「シーサート」と読む）である。CSIRTを設置していない企業はもちろん、取り組みを始めている企業でも、CSIRTとは何か、既存の枠組みと何が異なるのか、緊急対応体制として必要な機能は何か、自社に不足している要素は何かといった検討・検証を進めることを勧めたい。CSIRTについてはJPCERTコーディネーションセンター（JPCERT/CC）が「CSIRTマテリアル」（www.jpcert.or.jp/csirt_material）を公表しているので、ぜひ参照していただきたい。

筆者は、CSIRTの利点の１つは組織間の連携をスムーズにすることだと考えている。サイバー攻撃が巧妙かつ複雑になっていく状況で、自社だけで判断したり対応したりすることが困難な局面が増え、他の組織との情報交換や連携が有効となるケースが非常に多くなっている。自社のCSIRTの存在や連絡先が公表されていれば他組織のCSIRTとの連携が容易で、情報提供も受けやすくなる。

2013年12月に米国小売大手のTarget社で大量のクレジットカード情報が漏えいする事件が起きたことを受け、全米小売業協会（NRF）は情報セキュリティの脅威に対して情報共有・分析を行う組織（Information Sharing and Analysis Center：ISAC）を設立すると発表した。日本でも多くの業界団体で同様の枠組みがつくられている。

自社への攻撃発生状況やそれを受けての対処方針などについては、外部に対して閉じた枠組みの中であっても情報提供がためらわれることもあろう。競合となる同業他社に手の内を明かす行為ともいえるからだ。しかし、もはやそのような懸念を抱いている場合ではないかもしれない。他社でインシデントが発生すれば、同種の脅威に対する見解や対策状況の報告を求められ得るし、同業種が同時に攻撃の対象となるケースもあり、決して人ごとで済まされる話ではない。協調して脅威に立ち向かうことが、結果として業界全体の安全と、ひいては自社の利益になると考えたい。その土台となるのが、各企業における組織内CSIRTなのである。

今後、一層複雑で検出しにくいサイバー攻撃が、より重大なインシデントを発生させ得る。インシデント対応力の向上は、企業の継続的な事業発展の礎となるであろう。 ■

不足する情報セキュリティ人材
―巧妙化する攻撃に備えるための人材育成方策とは―

サイバー攻撃がますます巧妙化している今、情報セキュリティ対策も高度化を余儀なくされているが、それに伴って多くの企業で人材不足が顕在化している。本稿では、人材育成の課題にどう取り組むか、また、情報セキュリティ人材に求められるスキルとはどういうものか、どのようにしてそのスキルを習得すべきかを解説する。

巧妙化するサイバー攻撃

大手重工系企業への標的型攻撃が報じられた2011年ころから、システムへの不正侵入やその被害に関するニュースが連日のように報じられている。手口も巧妙化し、痕跡を残さずに企業内の重要情報を盗み取ることも可能になっている。

不正侵入の方法としては、ソフトウェアの既知のバグ（プログラムのミス）やぜい弱性（セキュリティ上の欠陥）を悪用するケースが多いが、ぜい弱性が公表されると同時に、またはそれよりも早く攻撃が始まることもある。これは、公表から攻撃まで全く時間が経っていないことから「ゼロデイのぜい弱性」と呼ばれる。2014年４月にも、広く利用されているソフトウェアのぜい弱性が公表され、企業も対応に追われたことは記憶に新しい。

従来は、ソフトウェアにぜい弱性が発見されるとそれを修正するプログラムが公表されるので、担当者が計画的に対応することで攻撃を防ぐことは比較的容易だった。しかし最近はぜい弱性の公表と攻撃に時間差がなくなってきているため、事故発生時のインシデント対応と同じ素早い対応が求められており、情報収集を含めて企業が単独で対応することは困難になっている。

このような状況から、サイバー攻撃に対しては事故を前提に対策を考えることが主流になっている。不正侵入を完全に食い止めることは不可能であり、侵入をいかに早く発見して損害を最小限にとどめるか、またいかに手口を詳細に分析して再発防止策を講じられるかが重要だという考え方である。

情報セキュリティ人材不足の深刻化

サイバー攻撃の巧妙化とともに情報セキュリティがITインフラの必須要件と考えられるようになってきた一方で、情報セキュリティに関する人材不足も深刻化してきている。これについては国も認識しており、政府の情報セキュリティ政策会議が2013年に発表した「サイバーセキュリティ戦略」のほか、内閣官房セキュリティセンター（NISC）の「サイバーセキュリティ 2013」や「情報セキュリティ人材育成プログラム」でも人材育成の重要性とその基本方針が示されている。

独立行政法人情報処理推進機構（IPA）の「情報セキュリティ人材の育成に関する基礎調査」（2012年４月）によると、従業員100人

NRIセキュアテクノロジーズ
事業開発部長
関取嘉浩（せきとりよしひろ）
専門は情報セキュリティ関連の事業企画

以上の企業の情報セキュリティ技術者は現在約23万人いるが、そのうち何らかの教育やトレーニングを受ける必要がある人は約14万人おり、また技術者も約2万2千人が不足しているという。

企業も認識する人材不足

NRIセキュアテクノロジーズが毎年実施している「企業における情報セキュリティ実態調査」の2013年度の調査（2014年2月公表）によると、セキュリティ人材が不足していると感じている企業は85%に上り、重視する情報セキュリティ対策に「社内人材の育成や従業員教育」を挙げた企業が前年の28%（3位）から44%（1位）に急増している。

情報セキュリティ人材が不足していると感じる理由として多かったのは、「セキュリティ担当者のスキル不足」（47%）と「セキュリティ関連業務の大幅増加」（40%）であった。これは、たとえ担当者がいても、セキュリティ関連業務が広範になってきており、担当する要員やチームがそれをカバーする十分な知識やスキルを習得できていないことを反映していると思われる。

しかし、人材不足の状況を認識しているにもかかわらず、「今後3年間に担当者を増やす予定」と回答した企業は、2012年度には21.6%であったのに対して2013年度は15.1%という結果であった。その背景にあるのは、個人のスキル不足に対して、人員の増加を抑制しつつ、ある程度の時間をかけて補おうという考えであろう。

また、社外人材の活用も抑制する傾向にあり、少数の担当者の育成に主眼を置くという方針がはっきりと出ている。その育成に関して、IPAが主催している情報処理技術者試験の中でも、情報セキュリティスペシャリスト試験やネットワークスペシャリスト試験などのハイレベルな資格を奨励する企業が多い。その理由として「国家資格であること」「認知度が高いこと」を挙げる企業が多く、国内での実力を示す資格と考えられていることがうかがえる。

これらの資格ももちろん重要であるが、グローバル化が進んでいる状況と、それに伴って多様な人材が必要になっていることを考えると、今後はグローバルに通用する海外の認定資格にも目を向けるべきである。よく知られた海外の資格認定制度としては、SANS Instituteが主催しているGIAC（Global Information Assurance Certification）のほか、（ISC）²のCISSP（Certified Information Systems Security Professional）、ISACAのCISA（Certified Information Systems Auditor）などがある。

求められる情報セキュリティ人材とは

(1) 必要となるスキル

数年前までは、セキュリティポリシーの策定、PDCAサイクルの実行、コンプライアン

ス（法令順守）のような手続き指向のセキュリティ対策に予算や人的リソースが多く投入される傾向にあった。しかし今では、ネットワークのモニタリングやログ解析、インシデント対応、フォレンジック（事故の原因究明に必要なデータの収集・分析と、それを法的に証明するための手段や技術）、マルウェア（コンピュータウイルスなどの悪意あるプログラム）解析などの分野に投資をシフトしないと効果的な対策が望めなくなってきている。また、ぜい弱性診断やセキュアプログラミング（ぜい弱性をつくらないプログラミング）といった分野も重要である。従って、今求められている情報セキュリティ人材とは具体的には以下のような技術者である。

①ネットワークセキュリティアナリスト（システムやネットワークの運用・管理を攻撃検知の視点から行い、インシデント発生時の初期対応も行える）

②ペネトレーションテスター（最新の攻撃手法を熟知し、システムやネットワークにぜい弱性がないかを、疑似的な侵入を実行することによって検査し、対策を提案することができる）

③インシデントハンドラー（インシデント発生時に素早く対応し、システム・ネットワーク運用者および管理者と連携して対策を行い安全に復旧を行える）

④フォレンジックアナリスト（インシデント発生時にシステムやネットワーク上の証拠を発見し適切に保全できる）

⑤マルウェアアナリスト（侵入に使われたコードやマルウェアを解析し、攻撃手法の解明や対策手法を検討できる。また、システムやネットワーク上に残された痕跡から未知のマルウェアの検出も行える）

⑥サイバーインテリジェンスアナリスト（攻撃者の戦略を調査し、攻撃手法を分析するとともに、分析結果に基づいて防御施策を策定できる。「インテリジェンス」はここでは「諜報活動」の意）

⑦セキュアプログラマー（システム開発、アプリケーション開発において、ぜい弱性をつくらないプログラミングを実践できる）

(2) 研修カリキュラムの整備と人材の組織的活用

前述のとおり、最近の情報セキュリティへの脅威に対抗するためには、実践的な業務スキルを習得した人材が不可欠である。このような人材を育成するためには、システムに精通するだけでなく、攻撃者の考え方と侵入の手口を知り、常に攻撃者に先んじて対処できるスキルと経験が必要であり、これらを段階的に習得できる研修カリキュラムを整備することが重要である。

研修カリキュラムは、以下のような経験を積めるものであることが必要である。

①ぜい弱なシステムに対して実際に攻撃を仕掛ける

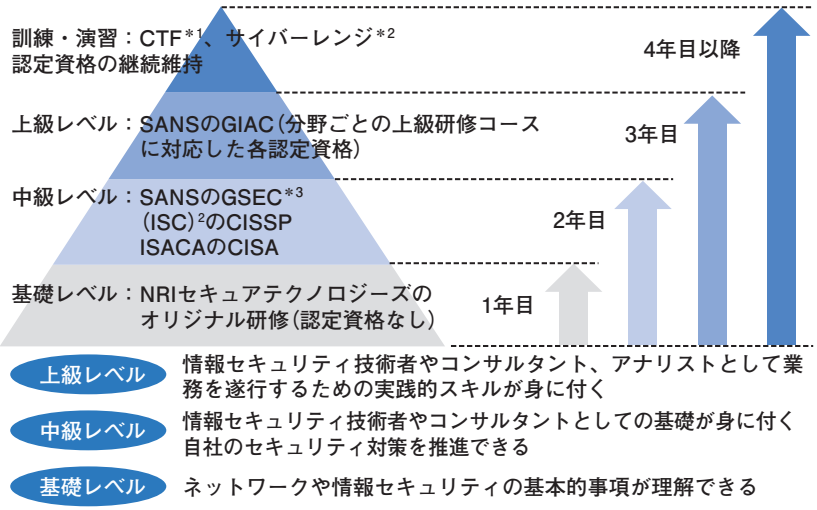
②攻撃を成功させるための技術的背景やツー

ルなどを理解する

③上の①および②の経験に基づいて防御手法を検討しシステムに実装する

また、習得したスキルが陳腐化することを防ぐための再履修機会の確保、セキュリティ担当者のキャリアパスの明確化など、育成した人材を組織としてどのように活用するかの検討も必要である。

図1　グローバル認定資格・研修のレベルとスキル習得の目安



*1：Capture The Flagの略で、情報セキュリティ技術者が競技形式で知識と技能を競う催し
*2：サイバー攻撃を防御するための演習環境　*3：GIAC Security Essentials Certification

外部とも連携した人材育成を

ひと口に情報セキュリティ人材といっても、業務や役割は多岐にわたり、1人の担当者ですべてをカバーすることは不可能である。かといって、個々の分野のスキルを習得した人材でチームを構成するなどして、セキュリティ関連業務をすべて社内で行おうとすることも実際には難しい。自社で無理のない範囲の業務を行い、それ以外を専門ベンダーにアウトソーシングすることは、現実的というだけでなく、育成すべき人材像を絞り込めるという意味でも有効であろう。

最近は、対策の立案・推進、社内の啓発、インシデントを含めたさまざまな局面における初動対応や意思決定に関わる業務は社内のセキュリティ担当者が行い、それ以外の運用監視、分析、検査などの専門的で高度なスキルが必要な分野は専門のサービス提供事業者の協力を得るというやり方になってきているようだ。図1に、ここまでで述べたことを踏まえた人材育成の枠組みを示す。社内担当者のスキルレベルは中級以上で、情報セキュリティ全般を理解し、インシデント対応のスキルを持った人材ということになろう。言うまでもなく、セキュリティサービス提供事業者は上級以上のスキルを持った技術者を育成する必要がある。

ますます巧妙化するサイバー攻撃に対抗するために、外部とも連携しつつ企業活動の安全・安心を確保する実践的なスキルを持った人材をいかに育成するか、そこに企業の将来がかかっていると言えよう。■

セキュリティ基準「PCI DSS」の有用性
―他業種へ適用する際のポイント―

クレジットカードのセキュリティを定めた国際基準「PCI DSS（Payment Card Industry Data Security Standard）」は、個人情報と金銭情報を扱うがゆえに厳格なルールとなっている。そのため、クレジットカードを扱わない業種のセキュリティ基準としても有効である。本稿では、PCI DSSの概要と普及状況、これを他業種へ適用する際のポイントを解説する。

国際セキュリティ基準「PCI DSS」

PCI DSSは、国際カードブランド５社で構成されるPCI SSC（Payment Card Industry Security Standard Council）が、クレジットカード情報を取り扱う事業者に求められる要件についてまとめた国際セキュリティ基準である。2004年12月に策定され、改訂を経て現在はバージョン3.0（2013年11月）に至っている。

表１に示すように、PCI DSSでは12の要件が規定されている。表には示していないが、いずれの要件も具体的に定められている点が特徴であり、ISMS（情報セキュリティマネジメントシステム）など他の広く知られた基準との大きな違いである。例えばパスワードについては「英文字と数字の組み合わせで７文字以上」「90日ごとに変更」「直近の４回と同じパスワードを利用禁止」などとしている。

なおPCI SSCの構成メンバーはAmerican Express、Discover、JCB、MasterCard、Visaである。

PCI DSSの普及状況

PCI SSCは、クレジットカードを取り扱う事業者をカード取引件数によってレベル分けし、レベルごとにPCI DSSへの準拠期限やその確認方法を定め、全ての加盟店とサービスプロバイダー（決済代行会社、会員を募集するカード会社、データ処理会社など）に対して準拠を求めている。最もPCI DSSへの準拠が進んでいる米国においては、PCI DSSに準拠すれば事故発生時に金融機関への損害賠償を免れることができるという州法や、PCI DSSに準拠しない場合は刑事罰もあるという州法があるなど、準拠が進む環境がある。

一方、日本ではまだまだ準拠が進んでいないというのが実情である。日本では改正割賦販売法（2010年12月施行）がクレジットカード情報の安全管理について定めているものの、PCI DSSに準拠しない法人に対する罰則規定は存在しない。このため、多くの企業では、多額の投資を行ってまでPCI DSSに準拠する明確な理由がなく、米国と比べると準拠への取り組みがあまり行われてこなかった。

このような状況下で、一般社団法人日本クレジット協会は経済産業省と連携し、2011年３月に「日本におけるクレジットカード情報管理強化に向けた実行計画」（www.j-credit.or.jp/info_management.html）を策定した。

NRIセキュアテクノロジーズ
マネジメントコンサルティング部
主任セキュリティコンサルタント
板田俊一（いただしゅんいち）

専門は情報セキュリティ全般に関するコンサルティング

表1　PCI DSSセキュリティ基準

項目	内容
安全なネットワークとシステムの構築と維持	1. カード会員データを保護するために、ファイアウオールをインストールして維持する 2. システムパスワードおよび他のセキュリティパラメーターにベンダー提供のデフォルト値を使用しない
カード会員データの保護	3. 保存されたカード会員データを保護する 4. オープンな公共ネットワーク経由でカード会員データを伝送する場合、暗号化する
ぜい弱性管理プログラムの維持	5. 全てのシステムをマルウェアから保護し、ウイルス対策ソフトウェアを定期的に更新する 6. 安全性の高いシステムとアプリケーションを開発し、保守する
強力なアクセス制御手法の導入	7. カード会員データへのアクセスを、業務上必要な範囲内に制限する 8. システムコンポーネントへのアクセスを識別・認証する 9. カード会員データへの物理アクセスを制限する
ネットワークの定期的な監視およびテスト	10. ネットワークリソースおよびカード会員データへの全てのアクセスを追跡および監視する 11. セキュリティシステムおよびプロセスを定期的にテストする
情報セキュリティポリシーの維持	12. 全ての担当者の情報セキュリティに対応するポリシーを維持する

この計画でも罰則規定はないが、準拠に向けた対応期限が定められていることから、現状を調査して部分的に対応を始める企業が徐々に増えている。

幅広い業種のセキュリティ基準として

PCI DSSは、クレジットカードの情報を扱わない企業にとっても、セキュリティ基準として非常に参考になる。これは、PCI DSSがクレジットカード情報という機微な情報の保護に関するグローバル基準であり、その内容が具体的という特徴があるからである。実際に、アカウント管理のルールについてPCI DSSの要件8を参考にしたり、システムのリスク評価に際して、PCI DSSに規定された評価項目を参考にしたりする企業がある。

ただし、PCI DSSをそのまま適用すればいいわけではない。例えば、PCI DSSは非常に高い水準のセキュリティ対策を求めているため、機微な情報を扱わない企業やシステムでは、費用対効果が釣り合わない過剰投資を招く恐れがある。PCI DSSではネットワークとサーバーに対して定期的なぜい弱性スキャン（検査）を外部（インターネット）と内部（社内ネットワーク）の両方のネットワークから実施することを求めているが、クレジットカード情報を扱わないのであれば、インターネットからの不特定多数の不正アクセスのリスクを考慮して、外部ネットワークからのスキャンを優先するという考え方もある。

このようにPCI DSSは、その要件を十分に理解した上で自社の事情に合わせて適切に取捨選択すれば、幅広い業種の企業で有効なセキュリティ基準として適用可能であろう。■

グローバルセキュリティ統制の勘所
―絵に描いた餅で終わらせないために―

NRIセキュアテクノロジーズが毎年実施している「企業における情報セキュリティ実態調査」（以下、「実態調査」）で、セキュリティレベルの国内外の格差が明らかになった。本稿では、日本をベースにした完璧なはずのセキュリティ統制計画がグローバル展開に失敗する現状を紹介し、異文化理解を踏まえた施策展開の大切さについて筆者の経験を基に考察する。

セキュリティレベルにグローバル格差

本稿では、グローバルセキュリティ統制を「日本企業が自社・自グループの海外拠点向けに情報セキュリティ対策を計画し、これを展開・浸透させること」と定義する。多くの日本企業がグローバル化を進める一方で、事業の成長スピードにグローバルセキュリティ統制が追い付かず、国内外のセキュリティレベルに差があることが指摘されてきた。

2013年に実施した「実態調査」で、その格差の実態がはっきり確かめられた。海外拠点に対するセキュリティ統制ができていると回答した企業は、支店で46.8%、連結子会社で43.4%と半分以下にとどまり、国内拠点との違いが明らかである（図１参照）。

グローバルセキュリティ統制を阻む要因

ここで、グローバルセキュリティ統制の具体的な課題に着目してみよう（表１参照）。

海外拠点におけるセキュリティ統制上の重要課題は、意識の低さや担当者の兼務など、要員の確保やリテラシーに関するものであり、体制面の強化が必要という結論に落ち着く。しかしながら、これは一筋縄ではいかない問題である。筆者の経験に照らすと、グローバルセキュリティ統制に悩みを持つ企業には次のような共通点がある。

①国内拠点のベストプラクティスをベースに高度な統制計画を策定しがち

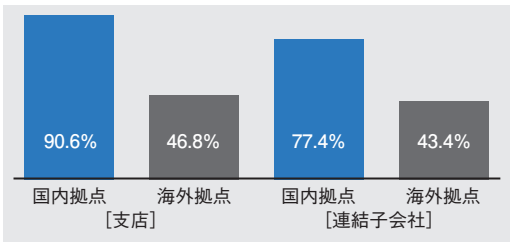
②展開対象となる地域・国の文化的な特性とその差異を考慮することを忘れがち

すなわち、日本人の特性といわれる勤勉さや究める精神によって策定された完璧なはずの統制計画が、海外のさまざまな地域特性に阻まれて現地に浸透せず、役に立たない計画（絵に描いた餅）となってしまうのである。

ASEANに見られる地域特性

地域特性について、早くから日本企業の進出先となったASEAN（東南アジア諸国連合）を例に考えてみよう。ASEAN全体では、次の３つの特性が挙げられる。

図１　セキュリティ統制が取れていると感じる企業



NRIセキュアテクノロジーズ
コンサルティング事業本部
ストラテジーコンサルティング部長
足立道拡（あだちみちひろ）

専門は情報セキュリティ対策に関するコンサルティング全般

①人材流動性の高さ

人材流動性の高さはASEANの顕著な傾向で、さまざまな背景を持つ人が次々とやって来る。新たに入ってきた人へのセキュリティ教育はもちろん大切だが、筆者は、一律のルールで縛るのは逆効果と考えている。どうしてもルールにせざるを得ないものは必要最低限の項目に絞り、禁止事項だけでなく順守事項を明確にすることが大切である。

表1　海外拠点の課題トップ5（複数回答）

順位	課題	割合	国内での順位
1	現地のセキュリティ意識が低い	60.0%	2位
2	拠点担当者が兼務のため、セキュリティ業務がおろそかになりがち	54.7%	1位
3	IT機器・サービスの調達・仕様の全体最適化が困難	50.4%	5位
3	セキュリティルール類の整備が困難	50.4%	6位
5	IT利活用のモニタリング・資産管理が困難	50.1%	4位

②セキュリティリテラシーの不足傾向

現地の人員のリテラシーが必ずしも高くないことを前提に対策を考えたい。欧米では「悪意のある人」が脅威の前提だが、ASEANでは「リテラシー不足の人」を脅威の前提とすべきである。例えば、ASEANの一部ではマルウェアの混入などセキュリティリスクが高いはずの違法コピーが会社への貢献（コスト削減）と認識されることがある。こうした認識を改めるべく、現地の日本人従業員が日本らしい工夫をしている例を目にした。江戸時代の高札（法令を記した立札）を模したイラストで現地従業員に「違法コピーの禁止」を訴えたのである。見た人の記憶に残りやすく、日本の文化に興味や関心を持つ現地従業員に大変に好評だったという。

③国と文化の多様性

国によって経済的な格差があり、シンガポールではPCやソフトウェアなどの調達は問題ないが、それ以外の国では現地では調達が難しい場合がある。セキュリティもカスタマイズが必要である。例えば、中国系の社会では、夕食を自宅で家族と食べ、その後で自宅で仕事をするという文化がある。会社貸与のPCを持ち出すニーズが高いため、それに応じたセキュリティ対策が重要になる。

海外拠点の現状を出発点に

ある大手グローバル企業でセキュリティ統制を担当されている方が「海外拠点の現状を肯定するところから始める姿勢こそが大事」と話されていた。まさに金言であり、この姿勢こそ事業のグローバル展開の大前提に据えられるべきである。最後に、グローバルセキュリティ統制の手順である「計画、展開、浸透」に沿って心構えを整理しよう。

①最低限のベースライン定義（計画）
②現状肯定とスモールスタート（展開）
③システム化と伝え方の工夫（浸透）

本稿がグローバルセキュリティ統制検討の一助となれば幸いである。 ■

社会インフラのセキュリティ対策
―増大する制御システムのセキュリティリスク―

海外では、電気、ガス、水道などの社会インフラに対するサイバー攻撃により、一部機能の停止などの被害が発生している。幸い日本ではそのような被害は報告されていないが、監視端末がコンピュータウイルスに感染するなどの被害は発生している。本稿では、脅威が高まりつつある制御システムのセキュリティの状況と対策について解説する。

脅威にさらされる制御システム

従来は人の手によって行われていた電気、ガス、水道などの社会インフラの運転・管理は、今日では制御システムと呼ばれる自動化装置を使って行われるようになっている。この制御システムがサイバー攻撃の対象になり得ること、それが深刻な脅威であることが日本でも注目されるようになったきっかけは、2010年にイランの核施設を標的としたサイバー攻撃が発生したことである。これ以後、世界では社会インフラに対するサイバー攻撃が増え続けている。

1990年代まで、制御システムは独自に開発された技術に基づいて、クローズドな（外部から遮断された）環境の中で動作していた。しかし1990年代後半に入ってインターネットが普及するとともに、標準的なネットワーク規格であるEthernet（イーサネット）をベースとした通信機器が大量に生産され、価格も大きく下落していった。そのため、ベンダー独自のプロトコルが主流であった制御システムの通信環境も、Ethernetをベースとしたものに置き換えられていった。

また、従来は独自に回路設計を行って製造していた制御装置も、大幅なコストダウンを図るために主要なロジックをソフトウェアで記述するようになり、そのベースとなるOS（基本ソフト）も、それまでのベンダー独自のものから、一般にもなじみの深いWindowsやUNIXが採用されるようになった。さらに、従来はエンジニアが現場に出向いて行っていた作業が、インターネットと接続することによりリモート端末を使って行うことができるようになり、広大なプラント（大型の設備）の情報の伝達・管理を省力化することも可能になった。

こうした変化は、制御システムを維持管理する側にコストダウンや利便性の向上という大きな恩恵をもたらしたが、それと同時に、制御システムが企業や家庭におけるPCやネットワーク環境と同様のセキュリティの脅威にさらされることにもなった。

制御システムのネットワークは、プラント操業上の問題がない限り、そこで使われているハードウェアの入れ替えやソフトウェアの変更が行われることはあまりない。そのため、制御端末で使われるソフトウェアやOSが古いままで、パッチ（セキュリティ上の欠陥を修正するプログラム）の適用などの対策

NRIセキュアテクノロジーズ
事業開発部
マネージャー
鈴木　伸（すずきしん）

専門はセキュリティに関するコンサルティング

NRIセキュアテクノロジーズ
事業開発部
上級セキュリティコンサルタント
新谷敏文（しんがいとしふみ）

専門は制御セキュリティに関するコンサルティング

が施されないまま放置されている状況が見受けられる。コストダウンや利便性の向上が実現した一方で、セキュリティリスクが徐々に増大していったのである。

制御システムのセキュリティ対策

では、制御システムのセキュリティリスクを低減するにはどうすればよいのか。制御システムでもオフィス環境と同じセキュリティ対策を行えばよいのだろうか。答えは否である。オフィスでPCのセキュリティを維持するには、頻繁なパッチの適用や、新しいコンピュータウイルスなどに対応するためのパターンファイル更新といった作業が必要である。オフィスのPCであれば、一時的にアプリケーションが使えなくなったり再起動が必要となったりしても対処が可能であるが、大規模な制御システムでは現実的ではない。また、パターンファイルを利用するセキュリティ対策製品は、パフォーマンスに影響を与える場合があることや、インターネット接続が制限される環境も多く定期的なファイル更新が困難であることなどから、制御システムにそのまま適用することは難しい。こうした状況を踏まえ、制御システム向けに考えられたセキュリティ対策製品が登場してきている。

①ホワイトリスト型セキュリティ対策製品

先にも述べたように、制御システムは大きな変更が少ない。また、比較的少数のアプリケーションが定型的な動作をするといった特性を持っている。そこで、定常状態を事前に記録しておき、それとは異なる動作を検知した場合に異常が発生したと判断する、ホワイトリスト型のセキュリティ対策製品が登場し普及し始めている。

ホワイトリスト型のセキュリティ対策製品の利点として、パターンファイルの更新といった煩雑なメンテナンスが不要であることが大きい。ホワイトリスト型のセキュリティ対策製品は今後も増えていくと思われ、制御システムのセキュリティ向上に貢献すると考えられる。

②データダイオード

ホワイトリスト型のセキュリティ対策製品は制御システムに特に有効と考えられるのに対して、金融システムなども含めて、サイバー攻撃により甚大な損害が発生する可能性のあるシステム全般に有効な、データダイオードと呼ばれる製品も登場している。これは、簡単に言うとネットワークの通信に関して一方向の通信しか許可しないファイアウオールである（ダイオードは電流を一方向にしか流さない電子素子）。

一方向のみの通信しか使わないことにより、オフィス環境のようにセキュリティの脅威にさらされやすいネットワークから、重要なシステムをモニターはできるが変更は一切できないことが論理的に保証される。そのため、たとえウイルスに感染したネットワークと制御システムのネットワークがつながれて

いても、制御システムは物理的に切り離されているのと同様に安全性を維持できる。

セキュリティ演習から見えた課題

セキュリティ製品の導入以外に、2013年ごろから目立つようになったのが、インフラ事業者を対象としたセキュリティインシデント演習である。演習を主催しているのは業界団体やCSSC（制御システムセキュリティセンター）などである。CSSCとは、重要インフラの制御システムのセキュリティを確保するために設立された技術研究組合であり、制御装置のベンダーやセキュリティベンダーが多く参加している。NRIセキュアテクノロジーズもCSSCが設立された2012年から参加しており、実際の制御装置を使ったセキュリティの検証や、セキュリティに関わる認証制度の研究、制御デバイスのセキュリティ認証機関の設立支援などを行ってきた。

またNRIセキュアテクノロジーズはこれらの演習のいくつかに参加する機会を得た。セキュリティインシデント演習はこれまで行われてこなかったものであり、演習に参加することで、制御システムを運用する現場のセキュリティに関する課題を見ることができた。

社会インフラのプラントは、安全操業を実現するためにさまざまな対策が施されており、運転要員や保守要員によって安全が守られてきた。安全操業の根幹には、故障や誤操作が発生しても重大な被害は発生させないようにするという考え方がある。この考え方は、プラント全体の設計から、末端の制御装置や機械の設計に至るまで徹底されている。そのため、プラント内で特定の機器が故障しても、２重化や３重化されている装置の残りの系列が動作することでプラントを稼働し続けることができる。

しかし、セキュリティインシデントはこの考え方では対処できないことが多い。例えば、監視端末がコンピュータウイルスに感染し、そこから制御装置に対して何らかの攻撃が行われ、攻撃対象となった制御装置が正常に動作しなくなった状況を考えてみよう。この場合、プラントの監視ルームでは、攻撃された制御装置が制御する対象に設置されたセンサーか、または攻撃された制御装置そのものが検知した異常が監視端末上にアラームとして通知される。運転要員は制御装置の動作がおかしいと判断して保守要員に連絡し、保守要員は当該の制御装置を故障と判断し、別の系統の制御装置を作動させる。しかし、監視端末がウイルスに感染しているため、別系統の制御装置でも同じ障害が発生する。こうして対策が遅れ、被害が拡大していく。

故障による停止を想定した並列処理では、ウイルスによる攻撃も並列で行われてしまうため、セキュリティインシデントにはこの仕組みは無意味である。ただし、複数のプラントが独立して同じ処理をしている場合は、セキュリティインシデントに対する有効な回避

策になる。

もう1つ、より根本的な問題点がある。何らかの異常が発生した場合に、それがセキュリティインシデントによるものか故障や誤操作によるものかという切り分けができないことである。

インシデントを正しく検知するために

セキュリティインシデントを検知する方法として、制御装置や監視端末などの個々の装置にウイルス検査機能を入れることが考えられる。しかしこの方法は、ソフトウェアのインストールや更新などの運用の手間や、システムへの影響（パフォーマンスの低下など）を考えると現実には難しいと思われる。また、ウイルス感染が1つの装置内部にとどまるのであれば、ウイルスが原因で装置の動作に異常が見られた場合も装置の故障と同じ扱いで対処できるので、セキュリティに特化した監視を行う必要性は低い。

制御システムは複数のネットワークに分けられており、ウイルスによる攻撃が行われた場合には、それらをまたがる通信が発生することが想定される。そこで、このような通信が検知されれば攻撃の発生が確認できるため、ネットワーク上を流れるパケット（データの小さなまとまり）の異常を検知することが重要であり、IDS（Intrusion Detection System）と呼ばれる仕組みが一般的に利用される。IDSは主にインターネットと社内ネットワークの通信を監視して、外部からの不正な侵入がないかを検知する目的で利用されることが多いが、制御システムのネットワークを監視する目的にも利用できる。

ネットワークを監視するためにはシグネチャーと呼ばれるデータ（不正アクセスや攻撃の特徴をパターンとして記録したデータ）が必要である。シグネチャーは、もともとインターネットからの攻撃を想定したものが中心であり、さまざまなプロトコルが存在することに加えてインターネットやオフィス環境とは異なる特徴を持っている制御ネットワークに適用しても精度の高い検知ができない。

最近では、SCADA（Supervisory Control And Data Acquisition：監視制御システム）や制御ネットワーク用のプロトコルを対象としたシグネチャーも登場しているが、その場合でも、制御の現場でこのような通信の監視を行うためには、既存のプラント監視の運用とうまく連携できるように考えることも必要である。

今後、さまざまなデバイスがネットワークに接続され、制御の自動化も進んでいくと考えられる。NRIセキュアテクノロジーズは、セキュリティの専門企業として、ITに関わるものだけでなく社会インフラを支える制御システムについても日々研究を重ね、利便性を支える安全・安心のために今後も貢献していきたい。■

米国のインフラセキュリティの動向
―日本も参考にすべき新たなフレームワーク―

2013年２月12日にオバマ大統領が重要インフラへのサイバー攻撃に対するセキュリティ強化を推進する大統領令に署名したことを受けて、米国の国立標準技術研究所（NIST）が策定したセキュリティフレームワークが１年後の同日に公開された。本稿では、このフレームワークの概略を紹介し、その意義について考察する。

大規模な情報漏えい事故が発生

米国小売業大手のTarget社で大規模な情報漏えいが2013年末から起きていたという報道は衝撃的だった。メンテナンス業者のID・パスワードを盗用し、ネットワーク経由で多数の店舗のレジにコンピュータウイルスを仕込み、買い物客のカード情報を盗む手口はさほど新しくはないが、驚くべきは流出した情報の量である。約４千万枚のクレジットおよびデビットカードの情報のほか、約７千万人の個人情報が流出したという、過去最大級の情報漏えい事故である。Target社は全米に店舗を構える大手ディスカウントスーパーだが、この事故で売り上げが低下したことに加え、事故対応や損害賠償のコスト増もあって業績が著しく悪化しているという。

新しい情報セキュリティの枠組み

この例に見られるように、サイバー攻撃は一瞬にして企業の経営を危うくするほどの大きな脅威となっている。サイバー攻撃に国境はなく、日本でも銀行口座からの不正送金や、アカウント詐取などの被害が深刻になってきている。米国で2014年２月12日に公開された「Cybersecurity Framework」（以下、「フレームワーク」）は、NISTが官民の専門家の意見をまとめて作成したセキュリティガイドラインである。「フレームワーク」は３つのパートから構成されている。

①Framework Core

サイバー攻撃への対策を３つの階層で整理し、文字どおり「枠組み」となっている。サブカテゴリーとして細分化された具体的な対策は、既存の情報セキュリティ基準を参照している。

②Framework Tiers

インフラ事業者に、対策状況を４段階でスコアリングすることを求めている。最も高い評価のレベル４は、リスクが把握され、対応プロセスが定義・実行され、リスクの変化にも追随できる状態とされている。

③Framework Profile

インフラ事業者に、現状の対策状況を可視化し、あるべき姿とのギャップを埋める改善活動を実施することを求めている。

経営目線で活用できる「フレームワーク」

「フレームワーク」は、新しい対策基準を作ることを目的としたものではなく、以前か

NRIセキュアテクノロジーズ
取締役
北米支社長
松下　直（まつしたなおし）

専門はサイバー攻撃対策ソリューション

らあるいくつかのセキュリティ基準やベストプラクティスを横串で結び付けて体系化したものである。

筆者は、この「フレームワーク」の意義は、企業のサイバー攻撃への対策の状況を経営者の目線で可視化できるところにあると考えている。従来の「NIST SP 800-53（連邦政府情報システムにおける推奨セキュリティ管理策）」のような細かな対策基準を自社が達成できているかをチェックしようという経営者がいるとは思えない。しかし、この「フレームワーク」を用いて、例えばインシデント対応だけが遅れていることを1枚の表で表現されれば、経営者は現状を容易に把握することができるのではないだろうか。

報道によると、Target社はサイバー攻撃を検知する最先端の製品を以前から導入し、レジに仕込まれたコンピュータウイルスは検知されていたという。情報漏えいの発生が分かると直ちに侵入経路を遮断したし、消費者の被害を未然に防ぐためにカード利用のモニタリングサービスを無償で提供している。「フレームワーク」でいうならば、認識、防御、攻撃検知、復旧の4つは高いレベルにあった。ただ1カ所、インシデント対応が十分でなく被害が拡大したという見方ができる。

NRIセキュアテクノロジーズも米国でセキュリティモニタリングサービスを提供しており、毎日、何百万件と送られて来るアラートからインシデントを見つけ出すことの難しさは身に染みて感じている。大規模なインシデントが起きれば対策の必要性に気付きもするが、地道なセキュリティ対策に費用を投じ続けることは、経営の目線からは効果が見えにくく優先順位が下がりがちだ。Target社の場合も、ウイルスらしい挙動を示すアラートを解析してインシデントと判断できていたら、被害はずっと軽減できたのではないかと惜しまれてならない。

サイバー攻撃への耐性の向上のために

NISTは「フレームワーク」普及のためのロードマップを作成しており、その中で「フレームワーク」の改善と、ワークショップの継続的な開催を宣言している。米国の国土安全保障省（DHS）も、「フレームワーク」を重要インフラ事業者に普及させていくプログラムを発表している。日本では、内閣官房情報セキュリティセンターと各省庁が連携して、重要インフラのセキュリティ対策に関わる第3次行動計画の検討を進めている。その中で打ち出された「重要インフラ事業者等が自らの状況を正しく認識し、活動目標を主体的に定めるに当たって必要となるリスクマネジメントの訴求」という方針は、米国の「フレームワーク」の方向性と共通する。

サイバー攻撃に対する企業のセキュリティの状況が経営の目線で可視化され、対策が進み、サイバー攻撃への耐性が向上することを願ってやまない。■

NRI Web Site

NRI公式ホームページ　www.nri.com/jp

会社情報

NRIグループのCSR活動	www.nri.com/jp/csr	IR情報	www.nri.com/jp/ir

事業・ソリューション別のポータルサイト

コンサルティング	www.nri.com/jp/products/consulting	日本における先駆者として社会や産業、企業の発展に貢献してきたコンサルティングサービスを紹介
未来創発センター	www.nri.com/jp/souhatsu	アジア・日本の新しい成長戦略に関わるNRIの取り組み、研究成果の情報発信、政策提言などを紹介
金融ITソリューション	www.nri.com/jp/products/kinyu	金融・資本市場でのビジネスを戦略的にサポートするITソリューションの実績、ビジョンを紹介
NRI Financial Solution	fis.nri.co.jp	金融・資本市場に関わるNRIの取り組みについての情報発信、政策提言、ITソリューションを紹介
産業ITソリューション	www.nri.com/jp/products/sangyo	流通業やサービス業、製造業などさまざまな産業分野のお客さまに提供するソリューションを紹介
IT基盤サービス	www.nri.com/jp/products/kiban	産業分野や社会インフラを支えるシステム、システムを安全・確実に運用するためのソリューションを紹介
情報技術本部	www.nri-aitd.com	先端的な基盤技術への挑戦と知的資産創造、技術をベースにした新事業の創造の実践を紹介
BizMart	www.bizmart.jp	企業間業務や生・配・販を中心とするさまざまな業種の業務効率化を支援するソリューションを紹介
GranArch	granarch.nri.co.jp/main.html	システムインテグレーション事業において培った基盤構築のノウハウを結集させたソリューション群を紹介

サービス・ソリューション別のWebサイト

INSIGHT SIGNAL	www.is.nri.co.jp	マーケティング戦略の効果を科学的に“見える化”し、効果を最大化することを目的とした総合支援サービス
TrueNavi	truenavi.net	コンサルティング業務を通じて独自に開発したインターネットリサーチサービス
TRUE TELLER	www.trueteller.net	コールセンターからマーケティング部門までさまざまなビジネスシーンで活用可能なテキストマイニングツール
てぷらぱ	teplapa.nri.co.jp	テスト工程の効率化を実現するテスト自動実行支援ツール
OpenStandia	openstandia.jp	オープンソースソフトウェアにより高品質な業務システムを構築するワンストップサービス
Senju Family	senjufamily.nri.co.jp	ITサービスの品質向上とコスト最適化を実現するシステム運用管理ソフトウェア

グループ企業・関連団体のWebサイト

NRIネットコム	www.nri-net.com	インターネットシステムの企画・開発・設計・運用などのソリューションを提供
NRIセキュアテクノロジーズ	www.nri-secure.co.jp	情報セキュリティに関するコンサルティング、ソリューション導入、教育、運用などのワンストップサービスを提供
NRIサイバーパテント	www.patent.ne.jp	「NRIサイバーパテントデスク」など、特許の取得・活用のためのソリューションを提供
NRIデータiテック	www.n-itech.com	IT基盤の設計・構築・展開と稼働後のきめ細かな維持・管理サービスを提供
NRI社会情報システム	www.nri-social.co.jp	全国のシルバー人材センターの事業を支援する総合情報処理システム「エイジレス80」を提供
NRIシステムテクノ	www.nri-st.co.jp	味の素グループに情報システムの企画・開発・運用サービスを提供
だいこう証券ビジネス	www.daiko-sb.co.jp	証券業務に関わるさまざまなミドル・バックサービスをワンストップで提供
野村マネジメント・スクール	www.nsam.or.jp	日本の経済社会の健全な発展および国民生活の向上のために重要な経営幹部の育成を支援する各種講座を開催

Worldwide

NRIグループ（グローバル）	www.nri.com	NRIアジア・パシフィック	www.nrisg.com
NRI Financial Solutions（英語）	fis.nri.co.jp/en	野村総合研究所（香港）有限公司	www.nrihk.com
野村総合研究所（北京）有限公司	www.nri.com.cn/beijing	野村総合研究所（台湾）有限公司	www.nri.com.tw
上海支店	shanghai.nri.com.cn	野村総合研究所ソウル	www.nri-seoul.co.kr
野村総合研究所（上海）有限公司	consulting.nri.com.cn		

『ITソリューション フロンティア』について

本誌の各論文およびバックナンバーはNRI公式ホームページで閲覧できます。
本誌に関するご意見、ご要望などは、it-solution@nri.co.jp宛てにお送りください。

ITソリューションフロンティア

2014年 7 月号　Vol.31 No.7（通巻367号）
2014年 6 月20日　発行

発行人　嶋本　正
発行所　株式会社野村総合研究所　コーポレートコミュニケーション部
〒100－0005　東京都千代田区丸の内1－6－5　丸の内北口ビル
ホームページ　www.nri.com/jp

発　送　NRIワークプレイス株式会社 ビジネスサービスグループ
〒240－0005　横浜市保土ケ谷区神戸町134
電話（045）336－7331／直通　Fax.（045）336－1408