情報セキュリティの本質と対策

情報セキュリティ上の脅威・攻撃に対する実用的ソリューション

情報セキュリティ研究所　所長　中村宇利

平成 29 年 12 月 3 日、日本経済新聞の一面に「中央省庁サイト、8 割にリスク　改ざん・なりすまし・盗み見・・・暗号化、人手や予算乏しく」という見出しの記事が掲載された。8 割の中央省庁サイトで、暗号化の遅れや人手不足のためセキュリティ・リスクを抱えているというのである。情報漏洩（盗み見）一つとっても、1 月にコインチェック社から 580 億円分の仮想通貨が盗まれたという事件があった。セキュリティ対策の杜撰さが指摘されているが、十分なセキュリティ対策をしている企業でも情報漏洩事件を起こしている。2011 年の 4 月から 6 月にかけて、ソニーグループ全体で 1 億 261 万 3000 件の情報漏洩事件があった。その前年に、筆者等は同社の法務関係者に完全な技術の採用を提案したが、自社技術で十分との回答であった。しかし漏洩事件後、自社技術により様々な対策を施したにもかかわらず、2014 年 11 月に、グループ会社のソニー・ピクチャーズから再び 4 万 7,000 人分合計 100TB 超の可能性のある個人情報漏洩が発生した。この他にも、2015 年 5 月の日本年金機構における 125 万件の個人情報漏洩事件や、2015 年 11 月三菱東京 UFJ 銀行の出会い系サイトの運営事業者の振込情報約 1 万 4,000 件の外部流出事件など、セキュリティ対策を万全に行っているはずの事業者の漏洩事件は世間に衝撃を与えた。これらはすべて不正アクセスによるものである。

2014 年 7 月のベネッセにおける 2,900 万件の子供や保護者の住所や氏名、電話番号、子供の性別や生年月日などの漏洩事件は、委託先従業員による外部持ち出しという人的漏洩なので別の問題に聞こえるかも知れないが、正しい技術による正しい対策さえあれば、このような大量流出はあり得なかったのである。

このような情報漏洩事件が頻発する理由は、情報漏洩を容易にできる未熟な技術を使っているからである。前述の日経の記事にも「ログイン画面など一部ではなく、サイト全体で徹底すれば利用者を守れる。この対策を『常時 SSL 化』と呼ぶ。」と書かれているが、完全な暗号技術をサイト全体で徹底すれば確かに守れるが、SSL 自体古い不完全な技術でありほとんど役に立たないことには触れられていない。

情報漏洩ができる環境であれば、漏洩よりは多少難しいが、情報改竄も可能である。一方、なりすましは最も容易で、対策は最も難しい。例えば、セキュリティレベルの高い最新のビルでは、来館者の 1 人 1 人に電子的な 1 回限りの入館証が発行され、来館者は記号やバーコードをプリントアウトして持参し、ゲートの読取機にかざして許可が出ればゲートが開く仕組となっている。空港における電子航空券とゲートを使った認証と同じ仕組である。一見するとセキュリティが厳重な気がするが、バーコードを入手すれば誰でも入館できる点は見逃されている。バーコードを落とす人もいれば、盗まれる人もいる。現行技術を用いた環境であれば電子的に盗むことはさらに容易である。これをネット上ですべて行う遠隔認証ではその何倍も易しいという事実を見逃してはならない。

その結果、膨大な損失が生じている。2009 年 1 月 9 日の BBC ニュースによれば、スイスダボス会議で世界有数のセキュリティ関係会社の代表が「Online Theft」が世界で 1 兆ドルあることを発表している。その金額は年々増加しており、未だ有効な対策が施されていない。

最近は、日本でもサイバー犯罪が報道されることが多くなり、事の重大さが認識されてきた。警察庁においてもサイバー対策を重視し、各都道府県警ではサイバー対策課を設けて対策にあたるなど、サイバー犯罪へ

の対策が緊急課題となっている。サイバー犯罪とは、主にコンピュータネットワーク上で行われる犯罪の総称であり、ネットワーク上の不法取引やデータの大量配布による著作権侵害、法律に違反するデータの公開などを主として指す。米国をはじめとする諸外国では陸・海・空の三軍に加えて、サイバー軍の設立を開始している。サイバー空間での攻防はすでに国家安全保障上の問題と認識されているのである。一方、我が国では、サイバーセキュリティを包括的に扱う動きがようやく出てきたばかりだ。サイバー空間の攻防は極めて重要だが、他国に先駆けて情報セキュリティ全般を扱い、二度と膨大な損失を被ることの無い有効な対策を打つことを期待したい。なぜなら、国防以前の問題として、産業情報の漏洩は、直接的に国力低下の原因につながる国家安全保障上の重要問題だからだ。一つの工業製品を発売するため日本を含む先進国では、基礎研究から始まり、その応用研究、これらを利用した製品開発（設計図を含む）、製造技術開発（金型や製造ラインなど）に膨大な費用をかけている。これらの費用は、原則としてすべて新製品の付加価値を構成し、最終製品の発売にあたっては、その製品本来の製造コストに加えて、この研究開発に要するコストを上乗せして、新製品の価格が決定されている。そして従来はこの新製品が有する新規性、独自性、利便性ゆえに、類似の従来製品と比較して高価格であっても価格競争力を維持してきた。ところが近年、新製品と同じ付加価値を持つほぼ同等の製品が、発売日までほぼ同じ日に市場に出てくるという不可解な事態が発生するようになっている。そのため我が国の製造業者は、研究開発にかけた膨大なコストを乗せた分だけ価格が高い新製品を市場に供給することを余儀なくされ、いつの間にか日本の経済力は、世界第二位の地位までも奪われるに至ってしまった。その結果、①競争力の低下とシェアの縮小、②技術力が高価格につながらないことによる研究開発費の圧縮、③日本人技術者の減少および技術力の低下、と負の連鎖さえ見られる。
「世界の工場」と称される国々と比べても、日本のほうが製造効率は数倍高いので、製造コストについて日本の競争力が勝っているケースは少なくない。それに加えて、開発コストを適切に上乗せできるのであれば、日本の競争力は以前よりも高くなり得ると言っても良い。そのためそこでは産業情報の漏洩を防止する情報セキュリティ対策が不可欠である。

＜情報セキュリティ上の脅威・攻撃＞
コンピュータが単独で使用される場合、コンピュータそのものの破壊を狙った攻撃や不正利用、コンピュータの中の重要データを盗難改竄するなどの脅威・攻撃が知られている。コンピュータ同士がネットワークでつながると、コンピュータそのものに加えて、ネットワーク機器自体に対する脅威・攻撃やネットワーク上での重要データの盗難・改竄などの脅威・攻撃についても対処しなければならない。防御すべき場所がコンピュータ単体からネットワーク全体に広がったことで、途方もないコストをかけてあらゆる脅威・攻撃に備えなければならないという心理的圧力をコンピュータ管理者に与えている。その結果、ネットワークそのものの防御だけでも手いっぱいで、様々な対策システムが組み込まれ、多重にモニタリングを行い、新たなインシデントに対してできるだけ早い対処を行う事が、情報セキュリティの要のごとく考えられ、コンピュータ自体を含む全体の防御まではとても考慮できない状況となっている。次から次へと引き起こされる新たなインシデントに振り回され、情報セキュリティ対策に終わりはなく、技術者はただ最善を尽くすのみである。抜本的解決など最早夢物語と考え最初から諦めてしまうこともある。例えば、多くのサービスではネットワークセキュリティの抜本的解決のため公衆回線であるインターネットを利用せず専用線を利用する。銀行のＡＴＭが銀行外に設置してある場合があるが、銀行の建物から延びる通信線は当然のことながらほとんどが専用線である。しかしこのＡＴＭの為の専用線の多くは暗号化されておらず、また仮にされていても専用線

の中にはＡＴＭに関係する情報だけが流れるので、期待効果とは逆に、情報盗難はより容易くなるという残念な結果となっている。専用線を使うだけではセキュリティは確保できないのである。このように情報セキュリティのソリューションは極めて複雑であり、多くの技術者が、どれだけの脅威があるのか、どこまでの対策を行ったら十分なのかと途方に暮れている。
ところが、ＪＳＳＣ情報セキュリティ研究部会において解析した結果、情報セキュリティ上の脅威・攻撃は、人的要因を除けば、①コンピュータ及びネットワークの破壊・かく乱、②情報の盗難、③情報の改竄、④認証情報の偽使用によるなりすましの４つに絞られるという意外な結論を得た。

＜情報セキュリティ上の脅威・攻撃に対するソリューションは存在するか＞
①コンピュータ及びネットワークのかく乱脅威・攻撃はシステム自体の冗長性を高めることで実質的被害を避けられる。コンピュータ及びネットワークを多重化し、ネットワークとの接続点を被害想定数より多くすれば、一部のシステムに障害が引き起こされても、全体としてみれば被害は最小限に抑えられる。
一方、②情報盗難、③情報改竄、④なりすましは、広義の中間者攻撃と考えられ、ネットワーク上だけでなく、コンピュータに不正に入れられたマルウエアや標的型メールによって、中間者に強制誘導されて引き起こされるものも多い。ネットワークのセキュリティを完璧にまで高めても、全体としては脆弱なままということである。このうち④については最近、特殊な認証情報を使うことで、中間者攻撃を防御できることが判明した。またそもそもネットワーク上を流れる情報のうちどの部分が認証情報か分からなければなりすましは難しい。認証以外のデータと混ぜたり、認証データをバラバラにして別のパケット内に混在させたりすることで、どこに認証データが存在するか分からなくすることができる。さらに認証情報を含めた全情報を暗号化して通信すれば（全情報暗号通信）、認証情報だけを取り出すことは不可能である。
残る②と③であるが、実は、情報の生成直後に完全暗号化し使用直前に復号化すればそのほぼ全てを防御できる。前述の通り、個人情報やクレジットカード情報が漏洩したという事件が絶えないが、完璧にこの対策を行えば、最早これらの問題は過去のものになる。この対策方法に必要なのは、①ネットワークを介して情報の送受信を行う情報生成者と使用者とでデータの送受信を行うために用いられるデータ（典型的には、暗号化、復号化に用いる変化する鍵）をシンクロさせること（Remote Synchronization）と、②両者間で用いる完全暗号（Complete Cipher）技術とを確立することである。それら技術は、高速に処理できることが実際の対策には必要であるが、すでに開発済みでありいつでも使用できる状態にある。

＜エンド・トゥ・エンドプロテクション＞
上記のように、情報を送信する装置内で生成直後に完全暗号化し、その情報を受信する装置内で使用直前に復号化するソリューションを「エンド・トゥ・エンドプロテクション」と呼ぶ。このソリューションを構築できれば、送受信を行う装置内を含めて、使用されないときの情報はすべて暗号化されており、脅威・攻撃のうち②情報盗難、③情報改竄、④なりすましを防ぐことができる。①ネットワークのかく乱脅威・攻撃への対策を十分に行っていることを前提に考えるならば、ネットワーク機器やインフラなどはそれほどセキュリティを高めた製品でなくても、例えばダムルーターやダムスイッチでも、セキュリティ上問題はなくなる。
完全な情報セキュリティ対策に必要なのは、①適切な情報生成者と使用者をシンクロさせること（遠隔同期、Remote Synchronization）と、②両者間で用いる完全暗号（Complete Cipher）であり、その結果、エンド・トゥ・エンドプロテクションが可能になり、情報処理プロセスを透明化し、マルウエアを受け付けないコン

ピュータアーキテクチャを採用する機器と併せて使用すれば、現在の情報セキュリティ上のほとんどの問題を解決できる。

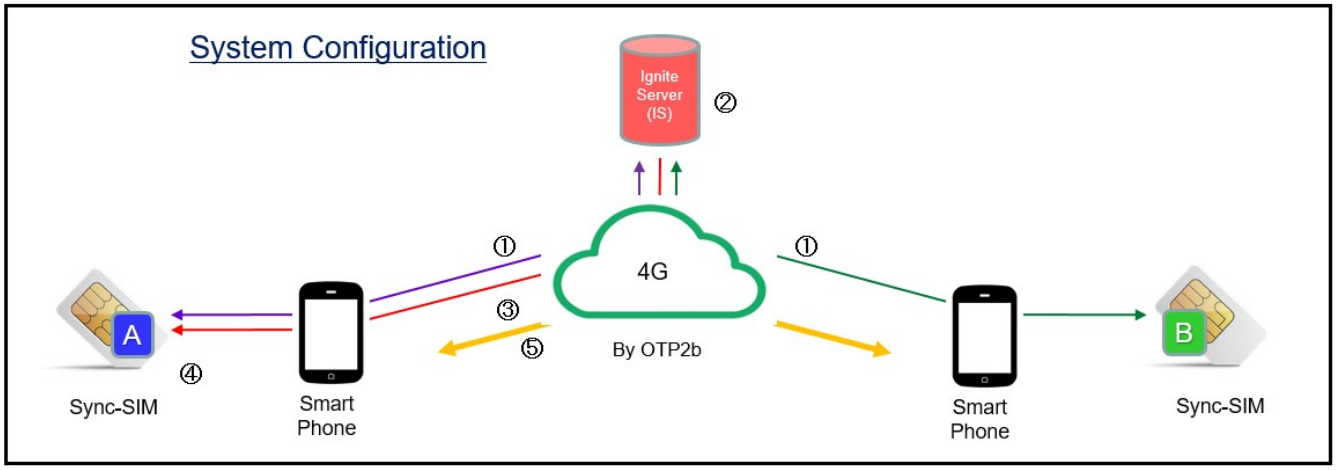
次表は情報処理推進機構（IPA）が発表した「情報セキュリティ 10 大脅威 2017」である。この表に掲載されている脅威に対しても実際、個人に対するものとしてあげられている脅威のうち、インターネットバンキングやクレジットカード情報の不正利用（1 位）、ウェブサービスへの不正ログイン（4 位）、ウェブサービスからの個人情報の窃取（6 位）、IoT 機器の不適切な管理（10 位）は直接的に、ランサムウェアによる被害（2 位）、スマートフォンやスマートフォンアプリを狙った攻撃（3 位）、ワンクリック請求等の不当請求（5 位）、インターネット上のサービスを悪用した攻撃（9 位）は組合せで防ぐことができる。また、組織に対するものとしてあげられている脅威のうち、ウェブサービスからの個人情報の窃取（3 位）、内部不正による情報漏洩とそれに伴う業務停止（5 位）、ウェブサイトの改ざん（6 位）、ウェブサービスへの不正ログイン（7 位）、IoT 機器の脆弱性の顕在化（8 位）、インターネットバンキングやクレジットカード情報の不正利用（10 位）は直接的に、標的型攻撃による情報流出（1 位）、ランサムウェアによる被害（2 位）は組合せで防御できる。尚、サービス妨害攻撃によるサービスの停止（4 位）は従来技術で解決でき、また残りの、組織の攻撃のビジネス化（アンダーグラウンドサービス）（9 位）と個人のネット上の誹謗・中傷（7 位）及び情報モラル欠如に伴う犯罪の低年齢化（8 位）は人的問題である。

昨年順位	個人	順位	組織	昨年順位
1位	インターネットバンキングやクレジットカード情報の不正利用	1位	標的型攻撃による情報流出	1位
2位	ランサムウェアによる被害	2位	ランサムウェアによる被害	7位
3位	スマートフォンやスマートフォンアプリを狙った攻撃	3位	ウェブサービスからの個人情報の窃取	3位
5位	ウェブサービスへの不正ログイン	4位	サービス妨害攻撃によるサービスの停止	4位
4位	ワンクリック請求等の不当請求	5位	内部不正による情報漏えいとそれに伴う業務停止	2位
7位	ウェブサービスからの個人情報の窃取	6位	ウェブサイトの改ざん	5位
6位	ネット上の誹謗・中傷	7位	ウェブサービスへの不正ログイン	9位
8位	情報モラル欠如に伴う犯罪の低年齢化	8位	IoT機器の脆弱性の顕在化	ランク外
10位	インターネット上のサービスを悪用した攻撃	9位	攻撃のビジネス化	ランク外
ランク外	IoT機器の不適切な管理	10位	インターネットバンキングやクレジットカード情報の不正利用	8位

＜具体的なソリューション＞

前述の通り、エンド・トゥ・エンドプロテクションを実現するためには、①適切な情報生成者と使用者をシンクロさせること（遠隔同期、Remote Synchronization）と、②両者間で用いる完全暗号（Complete Cipher）が必要である。②については別の機会に譲り、以下、①について説明する。

遠隔関係にある A、B の 2 地点において、それぞれが独立に遠隔同期させた新開発の同期サーバー（イグナイトサーバーと端末（スマートフォンやタブレットなど）に搭載する新型 SIM（Sync-SIM）の関係を利用して、同期の取れていない A、B 2 つの端末に搭載された新型 SIM 同士の遠隔同期を以下の手順で可能ならしめ、これら端末間での P to P 暗号通信を行う。



① イグナイトサーバ（IS）とタブレット A（Sync-SIM-A）およびタブレット B（Sync-SIM-B）との間に遠隔同期のための NTI-OTP ソフトウエアをインストールし、環境条件をプリセットする。
② IS と Sync-SIM-A、IS と Sync-SIM-B の間の同期キーOTP2a、OTP2b を用いて同期キー（Sync-Key）を生成する。
③ IS は、②の Sync-Key を、スマートフォンを通じて Sync-SIM-A に送信する。この際暗号通信する必要はない。
④ Sync-SIM-A は、入手した Sync-Key から自身の持つ OTP2a を用いてセッションキーを取り出す。
⑤ これをセッションキー（AES キー）として暗号通信を行う。

この結果、遠隔関係にある A、B の 2 地点の Sync-SIM がイグナイトサーバーを介していつでも同期がとれるようになり、安全なネットワークインフラが完成する。最早、②情報盗難、③情報改竄、④なりすましを心配しないで済む。
ネットワーク上で計算処理を行い、データを保管し、送受信するクラウドコンピューティングや、ネットワークでつながる巨大データセンターには不可欠な基盤となるであろう。また、様々な IoT（Internet of Things）や巨大双方向送電網であるスマートグリッド、自動運転に不可欠のコネクティドカーや医療情報や個人情報を共有する高度ネットワーク医療などに対しても実用インフラを提供する。
このインフラがインターネット全体に広まれば、必要な時に任意の 2 地点において遠隔同期が達成され、インターネットそのものが安全なインフラになるであろう。

＜おわりに＞
情報セキュリティについて考えるとき、まず共通の土台の上に立って、何を目的にどんな対策を講じるかを考えなければならない。現在はこの議論の土台が必ずしも明確ではなく、その結果、十分な開発が行われず、適切な対策を取ることができない状況である。様々な攻撃に対して場当たり的に対処しているだけでは、包括的（排他的&網羅的）な対応はできない上に、膨大なコストがかかる。包括的な対策は、現在のコンピュータネットワーク全体で費やされているコストに比べても、むしろ少ない費用で実現可能である。
本論文にて、本当の脅威を洗い出し、絞り込み、現時点で実施できる最新の暗号技術を用いれば十分な対策が可能であることを論じた。提示させていただいた土台の上で、専門家の間で十分な議論をし、必要な研究開発を行い、対策を講じる必要がある。国家安全保障のためにも一刻も早い対応が望まれる。

日本が世界に先駆けて究極の情報セキュリティ対策を実施し、世界を導く立場を確立できれば、その先にある、インターネット第２フェーズ（必ずしも常時繋がっていると限らないインターネット）や IoT（あらゆるものが繋げたいときに繋がるインターネット）の世界が作り出す巨大市場において、失われた３０年を超えて、世界の中の確かな位置を取り戻せるであろう。第３の矢は日本人自らの手で作り出せるのである。