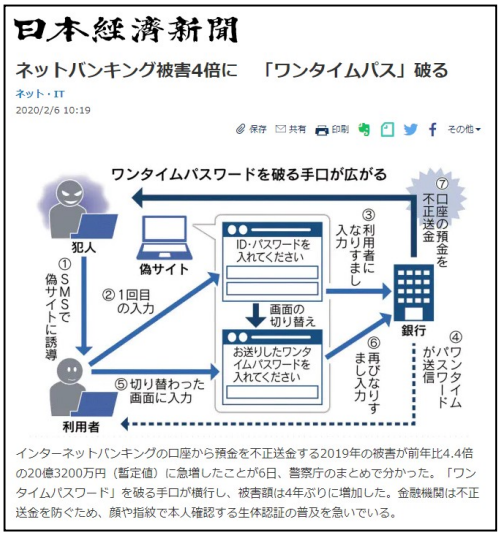
情報セキュリティの本質と対策

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を提供する

一般社団法人情報セキュリティ研究所
代表理事　中村宇利

2017 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。しかし、官公庁関係の情報漏洩はそれだけではない。住基ネット、年金情報、マイナンバー、衆議院、図書館利用情報など、多くの事例が報告されている。十分なセキュリティ対策をとっていると考えられてきた企業も例外ではない。NTT やヤフー、東芝、三菱重工、三菱東京 UFJ 銀行に続いて、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。その後も自社技術を使って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。2020 年には、防衛関係企業からの情報漏洩が相次いで報告された。高い暗号技術を誇る三菱電機や防衛関連の暗号技術を提供する NEC から防衛情報を含む情報漏洩があったというのである。また、東京オリンピックを見据え、様々なサイバーセキュリティ対策を大掛かりに行ってきた DOCOMO の口座が不正使用されたと報じられた。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。ある官公庁のセキュリティ担当者は、どれだけ対策を施しても万全という気になれない。一体これ以上どうすれば良いのかと困惑している。



2009 年 1 月 31 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 兆ドルであることを発表したと報じている。現在までに、ワンタイムパスワードの利用など様々な対策が施されているが、残念ながら被害額は倍増していると言われている。日本でも 2019 年には警察庁が、フィッシングによるものとみられるインターネットバンキングに関わる不正送金被害の急増について、全銀協等と連携して注意喚起を行っている。翌年日経新聞が、ワンタイムパスワードを破る手口が広がっていると報じたが、実はワンタイムパスワードをインターネットを介して送信することは危険である。

近年、国の施策もあって電子決済が急増し、認証にクレジット決済に見られるような ID とパスワードのみを要求する方式が普及しているが、情報セキュリティ的には論外といってよい。あくまで千円程度までの少額決済専用と考えるべきである。公的な認

証基盤では、これらに加えて公開鍵認証を行うが、中間者攻撃（man-in-the-middle-attack）を考慮するならば、決して安全な認証とは言えない。前述のインターネットバンキングは、ワンタイムパスワードを用いるので固定の ID とパスワードよりはるかに安全といえるが、中間者攻撃の前には無力である。
やや毛色の異なる問題ではあるが、2020 年米国大統領選挙では、不正投票が話題になった。一方わが国の選挙システムも極めて大きな問題を抱えている。通常、選挙の公示（告示）後、選挙管理委員会から選挙人名簿に登録されている人に、「入場整理券」が郵送され、投票日当日に投票所へ持参して投票する。投票所では、選挙人名簿と対照されるだけで印鑑や身分証明書は不要であり、本人認証は行わない。つまり、「入場整理券」を持参すれば誰でも投票できる。民主主義の根幹にかかわる問題が放置されているのである。

＜産業競争力と国家戦略＞

最近は、日本でもサイバー犯罪に関する報道が多くなり、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、サイバー犯罪対策を含む情報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。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十分な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。この結果、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。最近でも、多くの国民が先進国の１つとしてどこよりも早く新型コロナワクチンを開発できると信じていたが、期待通りの結果が出せなかった事実は日本の現在を表している。最早日本は技術的には先進国ではないのかもしれない。

今では、「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が数倍高いこともあり、製造コストについて調べると日本の競争力が逆転しているケースが少なくない。もしこれに加えて、開発コストを適切に製品に上乗せできるのであれば、日本は再び競争力を取り戻せる可能性が存在する。これが最後の機会と覚悟し、産業情報の漏洩を防止する情報セキュリティ対策を抜本的に見直すことが望まれる。

＜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の盗難・改竄などの脅威・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信じられている。ネットワーク管理者は、ネットワークそのものの防御だけでも手いっぱいで、不正アクセス対策やマルウエア対策などのシステムを導入し、多重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、セキュリティの要と考えている。多くの現場ではシステム全体の防御まではとても考慮できず､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、技術者はただその時の最善を尽くすのみである。抜本的解決など考えることもできない。一例を挙げると、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避けて専用線を利用する。銀行の ATM が銀行外に設置してある場合、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、専用線を狙われた場合には、期待効果とは逆に､情報盗難はより容易くなる｡単に専用線を用いる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に見え、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といえるのかと途方に暮れているようだ。

実は、情報セキュリティ上の脅威・攻撃は、人的要因を除けば、①情報の盗難、②情報の改竄、③認証情報の不正使用によるなりすまし、④コンピュータ及びネットワークの破壊・かく乱の４つに絞られる。このことに注目することで適切な対策を見出すことができる。

＜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＞

④コンピュータ及びネットワークのかく乱に関する脅威・攻撃はサイバー攻撃と呼ばれることが多い。このサイバー攻撃を防御する技術をサイバーセキュリティといい、情報セキュリティの１つで、システム自体の冗長性を高めること、ネットワークの接点での防御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、強固にすれば、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、①情報盗難、②情報改竄に対しては暗号技術を正しく用いて対応する。情報の生成直後に完全暗号で全暗号化し使用直前に全復号化すればそのほぼ全てを防御できる。残る③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が多い。この攻撃の防御はこれまで極めて困難だったが、最近は特殊な認証の仕組を用いることで、中間者攻撃を防御できることが判明している。

情報を送信する装置内で生成直後に全暗号化し､その情報を受信する装置内で使用直前に全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、E2E Protection」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、使用されるとき以外の情報は常に暗号化されており、脅威・攻撃のうち①情報盗難、②情報改竄、③なりすましを防ぐことができる。エンドにおける④コンピュータ及び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、通信途中のネ

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、セキュリティ上の問題は極小化される。

このエンド・トゥ・エンドプロテクションに必要なのは、ⓐ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、ⓑ通信する両者間で用いる完全暗号（Complete Cipher）であり、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。

尚、完全暗号（Complete Cipher）は、1949 年にクロード・シャノン博士が著した「秘匿系の通信理論（Communication Theory of Secrecy Systems", Bell System Technical Journal, vol. 28, pp. 656–715, 1949)」に端を発する情報理論的安全性を担保する暗号技術であり、Remote Synchronization と合わせて実装する。「完全暗号」は理論的に解読できない秘匿保管、秘匿通信を可能とする、超高速演算を行う量子コンピュータ時代における唯一の暗号ソリューションである。

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 2020」である。この表に掲載されている脅威を分析すると、表右側の 10 位の「サービス妨害攻撃によるサービスの停止」だけが純粋なサイバー攻撃であり、そのほかの脅威は、人的被害や IT 基盤の予期せぬ障害を除けば、すべて①情報の盗難、②情報の改竄、③なりすましのいずれかまたは複数に関係しており、暗号技術を軸にした対策で防御可能である。「サービス妨害攻撃によるサービスの停止」は 2016 年の 4 位から徐々に順位を下げて、表から分かる通り 2019 年の 6 位から 2020 年では 10 位となっており、多くの組織にとって対策済みであり、最早大きな脅威とはなっていない状況である。以上より、情報セキュリティの対策が、4 つのうちで最も露見しやすい脅威に対するサイバーセキュリティに偏っており、より直接的な脅威である①情報の盗難、②情報の改竄、③なりすましの 3 つについて、対策そのものがほとんど行われていないことが分かる。実際、官公庁や企業の現場でも、情報セキュリティとサイバーセキュリティを同じものと考える人さえいて、サイバーセキュリティ対策を行っただけで、情報セキュリティ対策を全く行っていないことに気付きさえしないケースが多くみられる。

昨年順位	個人	順位	組織	昨年順位
NEW	スマホ決済の不正利用	1位	標的型攻撃による機密情報の窃取	1位
2位	フィッシングによる個人情報の詐取	2位	内部不正による情報漏えい	5位
1位	クレジットカード情報の不正利用	3位	ビジネスメール詐欺による金銭被害	2位
7位	インターネットバンキングの不正利用	4位	サプライチェーンの弱点を悪用した攻撃	4位
4位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	5位	ランサムウェアによる被害	3位
3位	不正アプリによるスマートフォン利用者への被害	6位	予期せぬIT基盤の障害に伴う業務停止	16位
5位	ネット上の誹謗・中傷・デマ	7位	不注意による情報漏えい（規則は遵守）	10位
8位	インターネット上のサービスへの不正ログイン	8位	インターネット上のサービスからの個人情報の窃取	7位
6位	偽警告によるインターネット詐欺	9位	IoT機器の不正利用	8位
12位	インターネット上のサービスからの個人情報の窃取	10位	サービス妨害攻撃によるサービスの停止	6位

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 2020」
（https://www.ipa.go.jp/security/vuln/10threats2020.html）

＜基本的な情報セキュリティソリューションとは＞

当研究所では、情報そのものの防御と認証の 2 つを情報セキュリティの基本としてソリューションを提供している。

全ての情報セキュリティの前提として、まず以下のガイドラインに則ったセキュリティポリシーを策定、実行することを推奨している。

a) 必要な情報だけを選別する
b) 必要最小限の人だけがアクセスできるようにする
c) 大規模データベース（DB）は業務に支障がない範囲で小規模 DB に分割する
d) 必ずバックアップを取る

その上で情報セキュリティ上の防御の基本として、前述の通り、①情報の盗難、②情報の改竄、③認証情報の不正使用によるなりすましについては、完全暗号を、④コンピュータ及びネットワークの破壊・かく乱には、従来のサイバーセキュリティ技術を用いて防御するソリューションを提案している。

また、情報セキュリティ上の認証の基本として、複数要素認証（第一要素は必ず可変）と複数経路認証、そして複数の認証者の 3 つを適切に組み合わせて実施する。

複数要素認証は固定型よりも可変型を優先する。認証の問題に対してよく語られる 2 段階認証もパスワードを 2 回同じ経路で送ったのでは、長いパスワードを使ったのと同じであり 2 要素認証とは言えないので注意が必要である。この基本を考慮すれば、電子決済で多用される ID とパスワードのみの認証は論外であることが容易に理解されるであろう。

現在でも大きな問題とされる特殊詐欺も複数認証者の考え方を導入すればそのほとんどを防御できる。高齢者が銀行の ATM を使用する際、振込又は出金実行ボタンを押しただけでは実行されないようにしつつ、予め決められた 2 番目の認証者である子供や配偶者などのスマホのアプリを自動的に立ち上げて、2 人目以上の認証がなされるまで実行されないようにすればよい。

また、現在使用されている「マイナンバーカード」は複数要素認証を行う際に、サービス提供の経路とは異なる経路を使用するよう推奨しており安全性は低くはないが、固定の認証情報を使用する点で可変の認証情報を用いる場合に劣る。パスワードは変更されない以上可変型とは言えない。固定のマイナンバーが、インターネットバンキング等で使用されるワンタイムパスワードのような、国民誰でもが利用できる可変型認証要素として利用可能な、可変型の「ダイナミックマイナンバー」のようなものに、近い将来改良されることを期待したい。

＜情報セキュリティを基礎に据えた製品/サービスの開発＞

最後に前述の完全暗号を用いることで実現できる製品およびサービスについて考察する。

当研究所では、情報通信産業分野において、通信、AI、IoT、クラウドコンピューティング、量子コンピュータ、VR/AR（スマートコントラクト、メタバース）、フィンテックの 7 つを重要分野とし、その中の AI と量子コンピュータを除く 5 つの分野では完全暗号が決定的な役割を果たすと考えている。

以下に、これら 5 つの重要分野の応用具体例を示す。

応用分野	暗号モジュール	具体例
通信	Crypt Comm （秘匿通信用ソフト/ハード）	・秘匿通信 ・次世代通信網（RSP/TCP/IP）
IoT	Ubiquitous MK （CryptoSyncKeyを用いるスマートキー）	・スマートキー ・スマートグリッド ・自動運転
Cloud Computing	Crypto Cloud Base （Secure Cloud Platform）	・クラウドインテリジェンス ・データ信託
VR/AR	Crypto Print （暗号紋＆遠隔認証）	・暗号紋（著作権保護/管理） ・スマートコントラクト ・デジタル印鑑　・証明写真 ・ダイナミックマイナンバー
Fintech	Crypto Cash （FinTech関係の応用ソフトウエア）	・CBDC ・暗号資産　・暗号保険 ・暗号証券/暗号債権 ・投票券

① 次世代通信

現在無線通信の分野では、5G など高速大容量通信において米中がしのぎを削る。しかし通信にとって重要なのは、高速大容量だけではなく、内容を守る「秘匿通信」である。無線有線を問わず情報の搬送方法（搬送経路）がどのように変化しようとも、今後インターネットの強大化、高密化に拍車がかかり、より重要なインフラとなることは間違いない。将来インターネットは、現在特定用途向け通信インフラで提供されている特別な通信網や専用線を取り込み、シンプルで安価で安全な最重要ネットワークに進化する。インターネット技術を取り込んだ次世代通信インフラが生まれつつある。

② IoT

様々なモノがインターネットに接続され、情報を交換しまた相互に制御する仕組みを IoT と呼ぶ。通信技術に加えて、「遠隔認証」と「秘匿通信」が必須とされ、センサーネットワークやビッグデータ、スマートキー、そして、自動車分野の将来図である自動運転（Connected Car）や、エネルギーを相互供給するスマートグリッドに不可欠の技術である。独国が進めるインダストリー4.0 や我が国の Connected Industries においても中心的役割を果たし、近未来の工場／製造設備（ロボット等）の要となる。IoT をリードするものが世界の製造をリードする。

③ クラウドコンピューティング

アプリケーションとデータをインターネット上に配し、計算もデータ保存／転送もすべてインターネット上で行う技術である。個人情報や産業情報を扱うので、通信技術に加えて、「遠隔認証」と「秘匿通信」「秘匿保管」が必須とされる。現在、マイクロソフトとアマゾンのクラウドサービスが群を抜いており、日本企業は大きく後れを取っているが、医療や自動運転（Connected Car）などの特定目的クラウドではまだまだ挽回の余地がある。

完全暗号を適切に用いれば、スマートコントラクトやデータ信託も可能である。

④ VR/AR（スマートコントラクト、メタバース）

専用機を中心に日本が世界を席巻してきたゲームの分野においても、VR/AR を使って新しい 3D コ

ンテンツを利用する時代になった。VR/AR 専用機の分野では米国企業の後塵を拝しているがまだまだ今後の応用分野では日本企業がリードできる分野である。3D コンテンツは 2D に比べてコストがかかるので、ゲームでも映像でも繰り返し利用がコスト的に有利で著作権管理も重要である。 かつて音楽や映画の著作権管理はレコード/CD 単位での管理を行っていたが、デジタルコンテンツに変わった現在、ファイル単位の管理に暗号技術が用いられている。3D コンテンツについてもファイル単位で真正性を保証するための「暗号紋」を使えば、盗難や改ざんを防ぐだけでなく確実な著作権管理が実現できる。新たな著作権管理団体が組成されることも考えられる。また、デジタル印鑑や証明写真、可変型マイナンバー（ダイナミックマイナンバー）も重要な応用製品/サービスとなる。

⑤ フィンテック

各国で自国の法定通貨をデジタル化する試みが始まった。これを可能にするのが「完全暗号」を利用する「クリプトキャッシュ」である。クリプトキャッシュはもともと従来の紙幣の偽造、不正使用を防止する目的で開発されてきた技術であり、21 世紀に入ってようやく完成した。クリプトキャッシュは法定通貨だけでなく、株券や社債券、保険証券等の証券一般までをデジタル化することができる。一方で、ブロックチェーンという未熟な技術で始められた暗号資産という新しい台帳型資産は、交換価値があることを認められ新たな産業に育ちつつある。ブロックチェーンを使ううちは偽造、不正使用が絶えないため、これもクリプトキャッシュで作り直せば、安全な暗号資産を作ることができる。尚、民主主義の根幹である不正のできない投票システムもクリプトキャッシュによって実現できる。