CONTENTS

FFamily 2019 387号

表紙のことば（日本の鳥シリーズ）

中国支部

ハクチョウ（島根）

シベリアなどから越冬のため日本へ飛来する、オオハクチョウやコハクチョウなどの総称。前者は全長140cm前後で翼開長200cm超の大形の水鳥、後者は全長120cm前後で翼開長180cm程度の水鳥。純白で首の長い姿や生態はよく似ている。

コハクチョウの集団越冬地の中でも、島根県は本州の最南地として知られている。

特集
情報セキュリティ最前線 2019

近年、ネットワークを通じて企業や政府のコンピュータシステムに外部から攻撃を与える「サイバー攻撃」が世界的な規模で急増している。重要データの窃取・改ざんやシステムの停止といった被害が深刻化する中、情報セキュリティ対策をいかに強化するかが社会的な課題となっているが、日本に対しては海外諸国に比べて危機意識の低さが指摘されている。今回の特集では、私たちが直面しているセキュリティリスクや、求められる対策について、「IoT社会の発展」や「東京オリンピック・パラリンピックの開催」「テレワークをはじめとした働き方改革の進展」など、様々な社会変化とともに見ていこう。

序章
多様化しながら増加するサイバー攻撃の脅威

加速度的に増加するサイバー攻撃

Webサイトが外部からの侵入によって改ざんされた、社内のサーバに保存していた機密データが奪われた、誰かが自分になりすましてネット決済で買い物をしていた、といった事態を体験したり、見聞きしたりしたという人は少なくないはずだ。ネットワークを通じてパソコンやスマートフォン、さらには情報システム内に侵入し、情報を盗み取ったり、機能を停止させたりといった「サイバー攻撃」の世界的な急増が、社会やビジネスの安定性を大きく揺るがしている。

サイバー攻撃の脅威にさらされているのは、日本も例外ではない。情報通信分野における国立研究開発法人情報通信研究機構（NICT）の報告によれば、国内でのサイバー攻撃に関わる通信数は、2011年の約45億件から2018年には約2,121億件へと、ここ7年間で47倍という驚異的な増加を見せており、今後もさらなる拡大が予測されている。（表1）

増加の背後にあるサイバー攻撃の多様化

サイバー攻撃がこれほど増加している背景には、実施者や目的、対象、手段の多

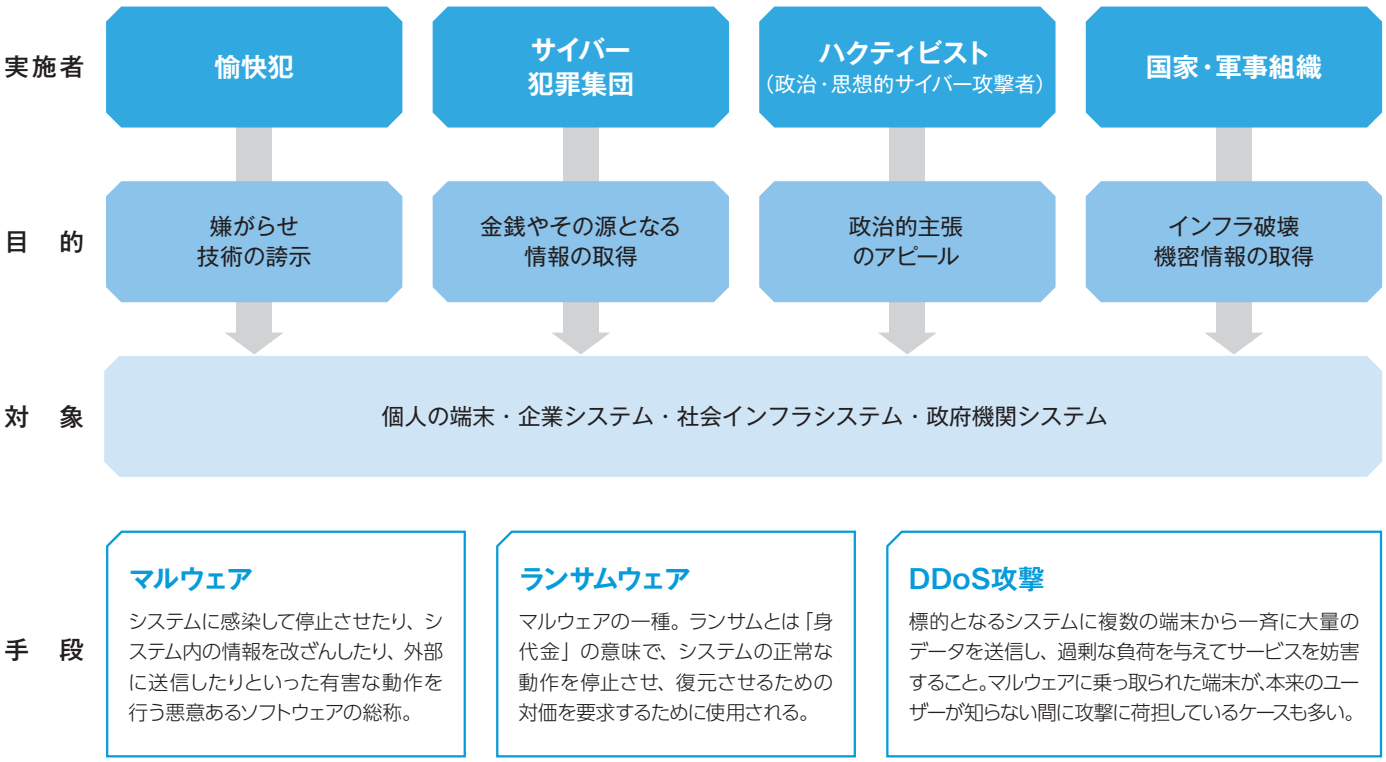
表1　国内で観測された不正なサイバー攻撃によるインターネット通信件数の推移

7年間で約47倍の増加!

2011	2012	2013	2014	2015	2016	2017	2018
45億	778億	129億	257億	545億	1,281億	1,504億	2,121億

出典：NICT（国立研究開発法人情報通信研究機構）観測レポート2018
https://www.nict.go.jp/cyber/report.html

図1　サイバー攻撃の多様化



様化がある。(図1)

一般に「サイバー犯罪」と呼ばれるのが、犯罪組織などによる金銭を目的としたサイバー攻撃だ。ネットを介して、ネットバンキングやキャッシュカードなどの口座番号、暗証番号などを盗み出し、本人になりすまして口座から現金を引き出したり、高額な買い物をしたりといった手口はよく知られている。

また、機密情報や個人情報を取得して、その情報を求める者から対価を得るというケースもある。さらに近年では、標的となるシステムを外部から停止させ、解除するための身代金を要求する「ランサムウェア」が登場するなど、手口が巧妙化している。

目的が金銭でなく、政治目的という場合もある。2010年にイランの核施設がサイバー攻撃された事件が話題となったが、これは米国とイスラエル政府によるものとの情報もあり、国家間のサイバー戦争の幕開けとも言われている。

政治目的によるサイバー攻撃は国家間だけではない。近年、社会的・政治的な主張を目的にサイバー攻撃を行う「ハクティビスト」と呼ばれる集団が急増しているが、中には「アノニマス」など高度なネットワーク技術を持つ組織もあり、政府や大手企業などの間で警戒心を強めている。

こうした集団による攻撃ではなく、個人による攻撃も無視できない。ネット上の気に入らない相手を攻撃したい、自己顕示欲を満たしたい、ネット上のゲームを有利に進めたい、といった、ごく個人的な動機によるものが多いが、結果としてシステム全体に及ぼす影響は甚大なものがあり、SNSビジネスやゲームビジネスを展開する企業にとっては深刻な脅威となっている。

攻撃手段の普及が招く誰もがサイバー犯罪者となり得る時代

サイバー攻撃の増加と多様化は、攻撃ツールの普及と低価格化を促し、攻撃するためのハードルを下げ、さらに攻撃が増加するという悪循環を生んでいる。

実際、インターネット上のアングラサイトなどでは、特別な知識・技術がなくともサイバー攻撃が可能なツールが安価に流通されている。これらを利用した、ちょっとしたイタズラ心でサイバー攻撃を行う若者たちの増加により、取り締まることが困難な状況だ。

IoT社会の発展や公衆無線LAN回線の拡充といったネットワーク社会の進化は、サイバー攻撃の機会増に直結している。「機会」と「手段」の双方が増大することで、誰もがサイバー犯罪を引き起こすことができる時代を迎えていることを、私たちは意識する必要がある。

サイバー攻撃から身を守るために私たちにできること

もはや、ネットワークにつながることを避けては生きていけない時代にあって、高まり続けるサイバー攻撃から身を守るために、何ができるだろうか。

最も大切なのは、その脅威をやみくもに恐れるのではなく、対策も含めて正しく理解することだ。

日本は情報セキュリティ上のリスク意識が低いと言われるが、それが顕著なのは一般の消費者や中堅・中小企業などであり、政府や研究機関、大企業などでは、早くから様々な対策を推進し、啓発に努めている。

自分やその家族が、あるいは所属する組織が、どのような脅威にさらされ、どのような対策を必要としているか、一人ひとりが理解し、行動することが、セキュリティ強固な社会づくりへの第一歩となるだろう。

次ページから、私たちを取り巻く様々なセキュリティリスクや、そこで求められる対策について、各方面の識者の意見を聞いていこう。

IoT×セキュリティ

IoT社会の発展がもたらすセキュリティリスク

IoT（Internet of Things）と呼ばれる技術革新が、私たちの暮らしやビジネスに大きな変化をもたらしつつある。あらゆる機器や端末がネットワーク化される社会では、新たな価値創出が期待される一方で、情報セキュリティ上のリスクが大きく高まるという懸念もある。情報セキュリティ大学院大学の後藤厚宏氏に、これからのIoT社会におけるセキュリティリスクと、その対策について聞いた。

情報セキュリティ大学院大学学長
後藤 厚宏 氏

1984年東京大学大学院工学系研究科情報工学専攻博士課程修了（工博）。NTT研究所にて並列・分散処理アーキテクチャ、インターネットセキュリティ技術、高信頼クラウドコンピューティング技術、ID管理技術の研究開発等に従事。2007年よりNTT情報流通プラットフォーム研究所長、2010年よりNTTサイバースペース研究所長。IEEE Computer SocietyのBoard of Governor、情報処理学会理事を歴任。2017年4月より情報セキュリティ大学院大学学長および同情報セキュリティ研究科長。

「つながり」が生み出す価値と「つながり」がもたらすリスク

――はじめに、そもそもIoT社会とはどのようなもので、何が期待されるかを改めて説明していただけますか？

IoT（Internet of Things）とは、PCやスマホといった情報端末だけでなく、あらゆる機器や端末がインターネットにつながることを意味しています。

インターネットを介して、社会のあらゆる情報を管理したり、あるいは集約・分析したりすることで、様々な価値創出が期待されています。

――言葉の定義としては理解していても、なかなか実態が見えづらいというのが正直なところです。

「IoT」と言われてもピンと来ない人が多いのは、その適用範囲が非常に幅広いためでしょう。

IoTが何を生み出すか、また、どんな課題を抱えているかを理解するには、全体的な印象で語るのではなく、IoTを対象別に区分して考える必要があります。

――具体的な分類としては、どのように考えればよいのでしょう？

分かりやすい分類としては、以下の3つに大別できます。

第一に、**個人の価値創造につながる「コンシューマーIoT」**です。一人ひとりの利便性や快適性の向上に寄与するもので、具体的には、ウェアラブル端末によるヘルスケア、スマート家電、Webカメラ、ゲームなどが挙げられます。

第二に、**産業の価値創造につながる「産業IoT」**です。オフィスや製造現場での効率向上や、品質・安全性の向上などにつながるもので、第四次産業革命（インダストリー4.0）と呼ばれるスマート工場をはじめ、農業や漁業のスマート化、スマートビル、業務端末の導入などが挙げられます。

そして第三に、**重要インフラの安定化・効率化につながる「インフラIoT」**です。電力やガス、水道など重要インフラの監視・制御、自動運転をはじめとした次世代交通システム、放送・通信システムなどが挙げられます。

――なるほど、そう切り分けて考えると、分かりやすいですね。

この分類は、情報セキュリティ上のリスクもイメージしやすくなっています。

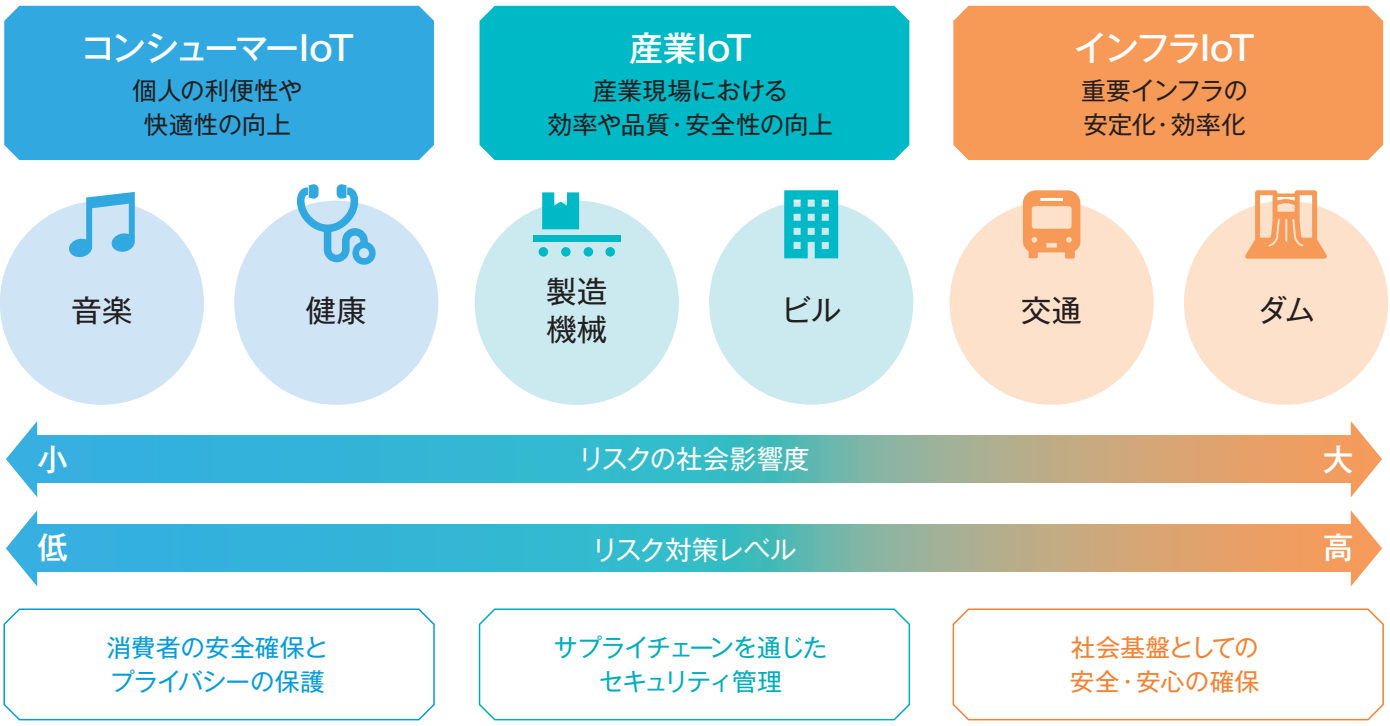
扱う情報が漏えい・改ざんされることや、外部から乗っ取られた際のリスクの社会影響レベルは、個人よりも産業、さらにはインフラの方が大きくなります。

セキュリティリスクに対する対策のレベルも個人→産業→インフラの順で高くなっていますが、これは、リスク影響の度合いだけでなく、端末の量とコストなどを考えれば、当然のことと言えます。

――IoTにおける情報セキュリティ上のリスクとは、どのようなものでしょう？

IoTの根幹は、あらゆる機器・端末がネットワークにつながることで価値を創造することにあります。しかし、これは

図1　IoTの多様性とセキュリティ課題



セキュリティの面から見れば、あらゆる機器・端末がネットワークを通じて起こる攻撃の対象となり得ることを意味しています。

加えて、ネットワークにつながる機器・端末の増加は、被害を拡大するリスクもはらんでいます。かつてはネットワーク上でやり取りされるのは情報（データ）だけでしたので、ネットワークを介して攻撃されるリスクもデータの流出や改ざんなど「情報を奪う」だけにとどまっていました。しかし、IoTによってネットワークが様々な機械や設備につながることで「実際のモノに被害を与える」ことも可能になってきます。

――モノへの被害とは、具体的にはどういったことでしょう？

これは被害ではなく、ある研究者が危険性を検証し、メーカーに警告したものですが、コネクテッドカーの車載ネットワークにぜい弱性があり、ハッキングによる遠隔操作によって交通事故を招くリスクがあることが分かりました。

また、最近では、ある国の水道管理システムがハッキングされ、大事な水処理システムが何者かによって不正に操作されていたことが判明し、大きな反響を呼びました。

どちらも日本でも起こりうることで、IoTネットワークの拡大が、セキュリティリスクの影響範囲を拡大させ、深刻度を高めていることを示す格好の教訓と言えるでしょう。

IoTでセキュリティリスクが高まる4つの理由

――IoTによる価値創造が期待される反面、大きなリスクも抱えていることが理解できました。IoTの発展が情報セキュリティリスクを高めているという指摘もありますが、その理由はどういったことが考えられるでしょう？

IoT社会でセキュリティリスクの高まりが危惧されている理由としては、大きく4つの点が挙げられます。

1つは、**ネットワークにつながる端末が多過ぎて、管理しきれない**こと。現在、大小合わせて何百億という機器・端末がネットワークにつながっており、今後もさらに増加していきます。これらすべてを厳重に管理するのは、物理的にもコスト的にも困難なため、どうしてもぜい弱性が見逃される端末が出てきます。

2つめは、**管理者不在の「野良IoT」の存在**です。かつて「ユビキタス（偏在）ネットワーク」とも呼ばれたように、IoTは社会の隅々にまで浸透し、その存在を周囲に意識されることなく、ネットにつながっている端末も少なくありません。その中には、誰が管理責任を持つのかが不明確なものもあり、セキュリティ研究者の間では「野良IoT」とも呼ばれ、サイバー攻撃の格好の標的となっています。

3つめは、**IoT機器・端末は寿命が長いため、セキュリティレベルの低い製品が利用され続けている**こと。センサーやカメラなど小規模なIoT端末は、PCやスマホに比べて寿命が長く、旧世代のセキュリティ対策しか施されていないものが現在も使われ続けています。量の多さからアップデートも難しく、これらも攻撃対象となりやすい存在です。

――なるほど、ネットワークにつながる数が多いということは、それだけ弱点も増えるというわけですね。

その通りです。ここまでの3つの理由は狙われる側でしたが、最後の1つは攻撃する側の理由です。

IoTの普及に伴うシステムの標準化によって、単一の攻撃ツールで多くのシステムを攻撃することが可能になっている、つまり、より効率的に攻撃できるようになっているのです。

Windowsがよくウイルスなどの被害に遭うのは、決してWindowsがぜい弱だからではありません。社会に広く普及しているため攻撃対象になりやすく、かつ、1つのウイルスで多くのWindows端末を攻撃できるからです。

IoTにおいても、通信・制御ソフトの標

準化が進めば、同様に1つのウイルスで多くのシステムを攻撃できるようになると懸念されています。

これら4つの理由から、IoT社会の進展は、攻撃する側にとってチャンスの拡大に直結していると言えます。

IoT社会における セキュリティリスク対策

――IoT化によって高まるセキュリティリスクに、私たちはどのように対処すべきでしょうか？

IoT社会におけるセキュリティリスクの高まりを踏まえて、すでに世界各地で国家レベルでの対策が進められています。そこで大きなポイントとなっているのが**「Security by Design（設計面からのセキュリティ）」**です。

具体的には、ネットワークにつながる製品に、開発・設計段階からセキュリティへの配慮を盛り込むこと。そのためのルールづくりが世界中で進められており、例えば、2018年10月には英国政府が「消費者向けIoT製品のセキュリティに関する行動規範」を策定し、その普及を促しています。

もちろん、日本でも産官連携での仕組みづくりが進められていて、近年、各種のガイドラインが公表されるとともに、車載器やATMなど影響度の高い機器を中心に、セキュリティに配慮した開発指針が策定されています。

IoT社会でつながる情報に国境はありませんので、これら各国の動きを参考にして、ISO/IECやITUなど国際規格でもルールづくりへの検討が進んでいます。

――心強いですね。ただ、あらゆる機器・端末に高度なセキュリティ対策を施すとなると、コストが心配になります。

確かに、あらゆる製品に万全のセキュリティ対策を施すのは現実的ではありません。セキュリティに万全を期すあまりに個々の端末が高額になっては、その普及を妨げ、かえってIoTによる価値創造を阻害しかねません。

そこで重要なのが**「セキュリティ対策と経済性の両立」**です。つまり、製品ごとに求められるセキュリティレベルを見える化し、それぞれに見合ったレベルの対策を施すという考え方です。

――具体的には、どのようなやり方があるでしょう？

自動車業界では、OTA（Over the Air）と呼ばれる、車載機器のソフトウェアなどを無線通信によって最新バージョンに更新する新たな仕組みが検討されています。

また、スマート家電なども個人が購入・所有するのでなく、メーカーがレンタルにする形にすれば、常に最新のセキュリティ対策を施すことができます。

まだアイディアの段階ですが、こうした仕組みを社会全体で考え、生み出していくことが必要でしょう。

――こうした取り組みが社会に浸透していくために、何が必要でしょうか？

ネットワークにつながる機器・端末を「作る側」「売る側」そして「使う側」、そのすべてが、セキュリティリスクを意識する必要があると考えています。

作る側や売る側は、セキュリティ対策の有無が、企業としての信頼性やブランド価値の低下、さらには補償の増大などのビジネスリスクに直結することを認識する必要があるでしょう。

また、使う側である一般消費者も、メーカー任せ、販売店任せにするのでなく、自ら「セキュリティ対策の確かな製品」を選ぶという姿勢が求められます。

――富士通も含めたメーカーの責任は、大きなものがありますね。

メーカーにお願いしたいのは、セキュリティ上のリスクや、求められる対策のレベルを、価格も含めて見える化するための評価技術や体系づくりです。

これらをもとに、商品・サービスごとにセキュリティ対策の認証制度などが整備されれば、ユーザーは用途や目的に応じた適切なセキュリティレベルの機器・端末を選ぶことができるでしょう。

あわせて、情報セキュリティリスクについて、ユーザーに積極的に発信し、啓発していくことも期待しています。

例えば自動車の場合、自動ブレーキや後部座席のエアバッグなど、法定以上の安全対策を施されたものの需要が、高額にもかかわらず拡大しています。これは消費者が「安全には対価がかかる」ということを学習した成果と言えます。

IoT機器の場合、リスクが目に見えないという難しさはありますが、メーカーの啓発によって、**「セキュリティ対策が、価格や品質に並ぶ、重要な選択基準である」**ことを広く社会に認識させていくことが、安全なIoT機器・端末の普及を促進し、IoT社会全体のリスク対策につながっていくはずだと考えています。

図2　国内におけるIoTセキュリティガイドラインの整備状況

「安全なIoTシステムのための セキュリティに関する一般的枠組み」 NISC/2016年8月	基本的な要求事項の明確化
「IoTセキュリティガイドライン」 IoT推進コンソーシアム（総務省/経済産業省）/2016年7月	IoTサービス関係者全般に向けたガイドライン
「つながる世界の開発指針」 IPA/初版 2016年3月・第2版 2017年7月	製品分野横断で活用できる開発指針
「製品分野別セキュリティガイドライン（車載器編、ATM編、IoTゲートウェイ編、オープンPOS編）」 CCDS/初版 2016年6月・Ver.2 2017年5月	製品分野別に展開した具体的な開発ガイドライン

NISC: 内閣サイバーセキュリティセンター
IPA: 独立行政法人情報処理推進機構
CCDS: 一般社団法人重要生活機器連携セキュリティ協議会

オリンピック・パラリンピック×セキュリティ

東京2020大会に潜むセキュリティリスク

2020年東京オリンピック・パラリンピック（以下、東京2020大会）を目前に控え、全国的に機運が高まる一方で、そのサイバーセキュリティ対策を世界が注視している。全世界的なスポーツイベントに潜む情報セキュリティ上のリスクや、東京2020大会に向けてさらなる増加が予想されるインバウンドに対するセキュリティについて、同大会の組織委員会でCISO（最高情報セキュリティ責任者）を務める坂明氏に聞いた。

公益財団法人
東京オリンピック・パラリンピック
競技大会組織委員会CISO
一般財団法人日本サイバー犯罪対策
センター（JC3）理事
坂 明 氏

1981年、警察庁に入庁。目黒警察署長、通商産業省通商政策局中南米室長、兵庫県警察本部長、国土交通省大臣官房審議官等を務めたほか、生活安全局セキュリティシステム対策室長、情報技術犯罪対策課長としてサイバー犯罪対策に従事。2002年にはハーバード大学国際問題研究所（WCFIA）客員研究員としてサイバーテロの研究に従事し、2008年から2年間は慶應義塾大学大学院政策・メディア研究科教授。2014年11月より日本サイバー犯罪対策センター（JC3:Japan Cybercrime Control Center）理事、2017年4月より東京オリンピック・パラリンピック競技大会組織委員会CISO。

世界的な関心の高さがサイバー攻撃の格好の標的に

――そもそも、オリンピック・パラリンピックにおいて情報セキュリティ対策が求められるのは、どういった理由からでしょう。

オリンピック・パラリンピックは地域や世代を問わず関心を集める、世界最大のスポーツイベントです。

関連して様々な経済活動も行われますので、金銭を目的とするサイバー犯罪集団にとっては、偽チケットサイトやフィッシング詐欺、さらにはランサムウェアによる身代金要求などで不当な利益を得るチャンスです。

また、こうした大きなイベントの開催には国の威信もかかっている側面から、政治・思想的なサイバー攻撃を行う「ハクティビスト」にとっては絶好のアピールの機会です。

このように、オリンピック・パラリンピックは、様々なサイバー犯罪・攻撃者の格好のターゲットとなりうるものと言えます。

――近年、開催されたオリンピック・パラリンピックでも、サイバー攻撃による被害を受けているのでしょうか？

2016年のリオデジャネイロ大会では、約1か月の開催期間中に主要なものだけでも223回ものDDoS攻撃が検知されたとの報告もあります。事前の対策などにより、大会システム自体は混乱を避けることができましたが、攻撃者が対策の薄いリオデジャネイロ州政府や銀行などにターゲットを移したため、それらのシステムがダウンするといった被害があったと言われています。

また、2018年の韓国・平昌大会でも、大会システムにサイバー攻撃があり、大会サイトが一時的にダウンするなどの被害

表1　オリンピック・パラリンピックで想定されるサイバー攻撃

金銭目的のサイバー犯罪	偽チケット販売サイト
	フィッシングサイトなどによる個人情報の窃取
	ランサムウェアによる脅迫
ハクティビストによる攻撃	大会サイトへのDDoS攻撃や改ざん
	スポンサーや開催都市など関連サイトへの攻撃
サイバーテロ	大会システムへの攻撃
	開催国の重要インフラ関連サイトへの攻撃
	開催国を訪れる要人を狙ったサイバースパイ
愉快犯	大会サイトへの攻撃・改ざん

がありました。これについては、「Olympic Destroyer」というマルウェアによるものとの報告もありますが、このマルウェアは侵入後、感染を広げるとともに、データを削除しシステム障害を起こすことによって、大会運営自体に脅威を与えるものであったと見られています。

――東京2020大会は過去の大会に比べてもリスクが高いと言われていますが、その理由を教えてください。

ICTの進化のスピードは急速で、4年間で大きく様変わりします。このため近年のオリンピックでは、開催されるごとにICT化が進んでおり、運営自体のシステム化はもちろん、情報発信メディアの拡大やSNSの活用が進んでいます。

実際、東京2020大会では、ヒトやモノの調達管理に関わる「イベントオペレーション」、競技そのものの運営を支える「スポーツオペレーション」、会場の整備や運営に関わる「ファシリティオペレーション」、電力や通信、交通インフラなどを管理する「インフラオペレーション」、チケットやライセンス商品の販売などを管理する「ビジネスオペレーション」と、幅広い領域で多岐にわたるシステムが構築されています。

これらのシステムがサイバー攻撃によって停止するようなことがあれば、東京2020大会の運営そのものが危機に瀕することになりますので、セキュリティ対策にはしっかりと取り組む必要があります。

――システム化によって大会運営が効率化されている一方で、過去に例のないほどシステムリスクが高まっているわけですね。

リオデジャネイロ大会の例でも分かるように、**近年では大会運営に関わるシステムだけでなく、警戒度の低い周辺環境もターゲット**になり得ます。

このため、スポンサーやサプライチェーンなど運営に関わる企業のシステム、さらには東京や日本社会全般のシステムがターゲットとされることも考える必要があります。

私たち組織委員会としては、自らが管轄するシステムをしっかり守り、大会の運営を確実に行っていく責務がありますが、国においても、東京2020大会に向けてサイバーセキュリティ対策を進める組織を立ち上げています。組織委員会やパートナー企業に加え、開催都市である東京都、国、そして電力・交通・通信などのインフラ運営を担う企業・組織とも連携しながら、日本社会全体を情報セキュリティ上の脅威からトータルに守っていく必要があると考えています。

インバウンドの増加がもたらすセキュリティリスク

――東京2020大会に伴い、インバウンド（訪日外国人旅行者）のさらなる増加が見込まれますが、セキュリティリスクの増加につながるとの指摘もあります。

政府や経済界も東京2020大会でインバウンドの方が多く来られることを想定した様々な歓迎策を進めていますが、セキュリティ対策についても考えていく必要があります。

その1つが**無料Wi-Fi（公衆無線LAN）の拡充によるリスクの高まり**です。海外から来日される方々がスマホなどで各種情報を取得しやすいよう、都内を中心に公衆無線LANが拡充されていますが、これが「盗聴」や「なりすまし」といったサイバー攻撃の標的となり得ることが懸念されています。

このため、通信行政を担う総務省が暗号化などのセキュリティ対策を進めており「公衆無線LANセキュリティ分科会報告書」などを公表、対策の徹底が急がれているところです。

――クレジットカードの不正利用による被害が増加していると聞きます。海外から来日された方々により多様なクレジットカードが利用されると、不正利用による被害も増加するのではないでしょうか？

確かにクレジットカードの不正利用による被害は増加していますが、その内容を見ると番号盗用による被害が大きく、また急増しています。実は海外では、クレジットカードはIC化が進んでいます。日本においても、磁気カードからICカードへの移行を進めており、対応する端末も東京2020大会までには整備されることになっています。

増加している番号盗用、つまりインターネットでの不正取引ですが、この内

図1　東京2020大会で想定すべきリスクの全体像

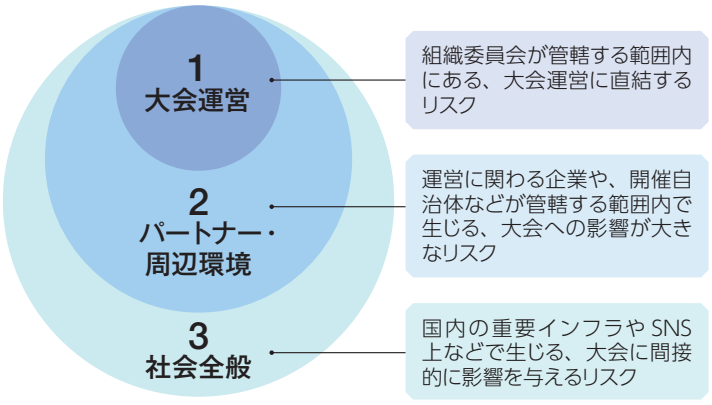


表2　訪日外国人旅行者の推移

2012	2014	2016	2018	2020
836万人	1,341万人	2,404万人	3,200万人	4,000万人

※ 2018は予測値、2020は政府目標

出典：実績＝日本政府観光局（JNTO）日本の観光統計データ
https://statistics.jnto.go.jp/graph/#graph--inbound--travelers--transition
予測＝株式会社JTB
https://www.jtbcorp.jp/jp/colors/detail/0134/

容を見ると、旅行詐欺に使われるケースがかなり多くなっています。つまり、海外から来日される方々が不利益を被るような不正が、かなりの件数発生しているということです。

これらの対策として、経済産業省やクレジットカード業界では、ICカード対応への環境整備を行うとともに、番号盗用対策についても、情報の厳格な管理や店舗においては不要な情報は持たないなど様々な取り組みを進めています。

――せっかく海外から日本を訪れてくれる方々が犯罪に巻き込まれないようにするためには、私たちカード利用者にも高いセキュリティ意識が求められますね。

その通りです。犯罪者はあらゆる手法で、クレジットカードをはじめとする様々な情報を窃取したり、利用しているコンピュータやスマートフォンを犯罪の道具として使うために乗っ取ったりしようとしています。情報セキュリティに限らず、社会的なリスクを低減するための一番の方法は、一人ひとりの危機意識を高めること。それが海外から来日される方々が日本で良い経験をしていただくためのリスク減にもつながります。

また、入管法も改正され、今後、旅行者に限らず、多くの海外の方々が来日されます。現在、例えばインターネットバンキングの不正送金事案などでは、外国人口座が使われるケースも多くあります。海外からお越しの方にも、セキュリティ意識を持っていただくことが大切だと考えています。

――最後に、東京2020大会に向けたメッセージをお願いします。

東京2020大会は、自国で世界レベルのスポーツ競技を観戦できる、おそらくは1世紀に一度の機会であり、日本の魅力を世界に発信する好機でもあります。大会運営自体にも多くの企業、ボランティアの方々等にご協力いただいていますが、さらにおもてなしなども考えれば、オリンピック・パラリンピックはまさにオールジャパンで支えていただくものと考えています。

この記念すべき大会を成功させるため、運営側だけでなく、参加・体験されるすべての人々に、セキュリティへの関心を持っていただければ幸いです。

|特集| 情報セキュリティ最前線 2019 3

働き方改革×セキュリティ

テレワーク普及の前提となるセキュリティ対策

2018年6月の「働き方改革関連法案」の成立を踏まえ、その具体策として「テレワーク」が注目されています。多くの企業で導入が検討される一方で、業務上の機密情報が漏えいするといったセキュリティリスクも懸念されています。サイバーセキュリティの専門家として、総務省が主催する「テレワークセキュリティガイドラインに関する検討会」の委員も務める吉岡克成氏に、テレワークにおけるセキュリティのあり方について聞いた。

テレワークが浸透しない原因はセキュリティリスクへの警戒心

――働き方改革関連法案の成立を機に、改めてテレワークの重要性がクローズアップされています。そのメリットや現状についてお聞かせください。

テレワークは時間と場所を選ばない働き方であり、例えば子育て中や介護中であったり、オフィスから離れた地域に居住していたりと、通常の勤務が難しい人でも働くことができるメリットがあります。**多様な働き方が選択でき、柔軟な働き方が可能になるという意味で、働き方改革のキーとなる取り組み**と言えるでしょう。

とはいえ現状では、テレワークの導入が進んでいるのは一部の業種・業態のみにとどまっています。もちろん、例えば製造オペレーションなどテレワークでの対応が困難な業務もありますが、テレワークが可能な業務であっても、まだまだ広く産業界に浸透しているとは言えない状況です。

――テレワークは働き方改革だけでなく、渋滞や通勤ラッシュの緩和、交通量の削減によるCO_2削減、災害時の事業継続性など、様々な社会課題の解決につながるものと期待されています。にもかかわらず導入が進まない背景には、何があるとお考えですか？

テレワークのメリットが分かっていて

横浜国立大学
先端科学高等研究院　准教授
吉岡 克成 氏

専門分野は情報システムセキュリティ、サイバーセキュリティ、マルウェア対策。2005年に横浜国立大学にて博士(工学)取得。2011年より横浜国立大学大学院環境情報研究院准教授。総務省テレワークセキュリティガイドラインに関する検討会委員も務め「IoTにおけるサイバーセキュリティの現状とその対策」などセキュリティ関連の講演多数。

も導入が進まない理由の1つが、セキュリティリスクへの警戒心でしょう。

セキュリティ対策の行き届いたオフィスで、同じ組織の構成員だけに囲まれて働くのとは違って、テレワークでは実施方法によっては様々な形で情報が周囲に漏れてしまうリスクがあります。

多くの企業が機密情報や個人情報を扱う現在、こうしたリスクに敏感になるのは当然と言えるでしょう。

テレワーク勤務者を取り巻くリスクとその対策

――テレワークにおけるセキュリティリスクとは、具体的にはどういったものがあるでしょう？

テレワークに関するセキュリティリスクは、大きく物理リスクとサイバーリスクとに分けられます。

物理リスクとは、「画面を盗み見られる」「PCや記録メディアを盗まれる」といった物理空間におけるリスク。サイバーリスクとは、「情報漏えい」「不正侵入」「ウイルス感染」など、ネットを介したサイバー空間におけるリスクです。

このため、**セキュリティを確保するためには物理空間とサイバー空間の両面での対策が必要**になり、それらを徹底するとなると、企業にとって大きな負担となるのは事実です。

――セキュリティ対策の煩雑さが、導入に二の足を踏む理由となっているのですね。

テレワークを行う場所は、自宅だけでなく、サテライトオフィス、あるいは移動中やカフェなどの公衆スペースなども考えられます。自宅やサテライトオフィスであれば対策を講じられますが、問題なのが公衆スペースです。

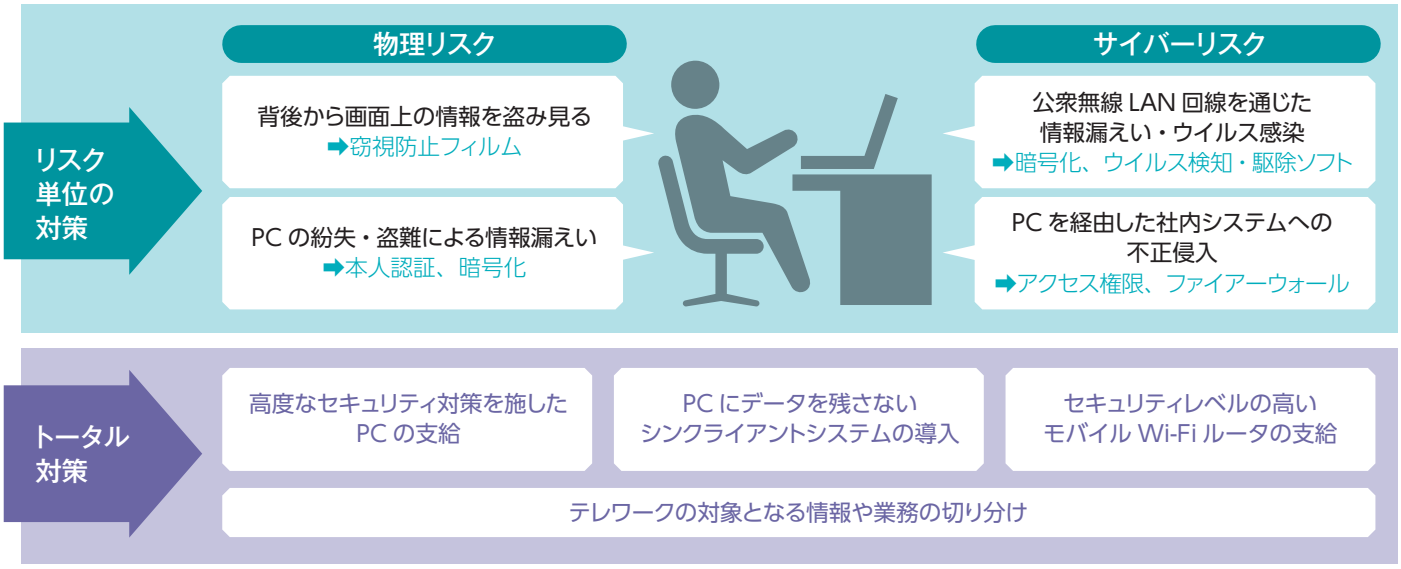
近年では、都心部を中心に無料Wi-Fiスポットなど公衆無線LANサービスが拡充されていますが、そこで問われるのは「安定してつながるかどうか」であって、高いセキュリティレベルは保証されていません。

加えて、ユーザーには使用するネットワークのリスクやセキュリティ対策のレベルが目に見えないため、気づかないうちに無防備な状態にさらされていることも少なくありません。

――公衆スペースにおけるセキュリティ対策としては、どういったことが考えられるでしょう？

まずは、セキュリティレベルが不明瞭な公衆回線には接続しないこと。とはいえ、いまや業務上でネット環境は必須ですから、あらかじめ会社側で一定のレベ

図1　テレワークにおけるセキュリティリスクとその対策



ルが確認できたモバイルWi-Fiルータを用意し、テレワーク勤務者に支給するなどの対策を講じるべきです。

同様に、業務に使用するPCなどの端末も、個人のものではなく、会社側で最新のOSや対策ソフトなどをインストールしたものを用意すべきでしょう。

――テレワーク勤務者個人に任せるのでなく、組織としての対策が必要だというわけですね。

その通りです。さらに言えば、社内システムを「シンクライアントシステム」にして、個々の端末には機密情報などを残さないようにすることも有効です。

ただ、いずれの対策も費用がかかるうえに、ある程度リスクを減らすことはできても、100%の対策にはなりません。

これらの対策に加えて、テレワークで扱える情報を制限するなど、運用面での対策も必要となるでしょう。

テレワークの普及に向けた産官連携での取り組み

――テレワークの普及を後押しすべく、政府もセキュリティ対策の啓発に努めているとのことですが、どのような内容でしょう？

代表的なものが、総務省の旗振りで策定・公表された**「テレワークセキュリティガイドライン」**です。これは、企業がテレワークを実施する際の情報セキュリティ上の不安を払拭し、安心してテレワークを導入・活用するための手引きとしてまとめられたものです。

2004年12月に初版が公表されて以降、2006年、2013年、そして2018年の第4版まで、環境変化を踏まえながら改定を重ねており、私も第3版から検討会に参加しています。

2018年の改定では、クラウドやSNSの普及や、ランサムウェアなど新たな脅威の登場、公衆無線LANのぜい弱性といった最新の状況を踏まえるとともに、より分かりやすく、使いやすい指針となるよう工夫されました。

今後はこのガイドラインをいかに広く周知させ、実際に活用してもらえるかが課題になるでしょう。

――テレワークを普及させるには、富士通を含めたICTベンダーの責任も重大だと考えています。どのような役割を期待されているのでしょうか？

サイバー攻撃は年々、高度化・巧妙化を続けていますので、個人や一般企業の対策には限度があります。

近年では、富士通をはじめ大手ICTベンダーが情報セキュリティサービスに注力しているので、自前で何とかしようとするのでなく、こうしたサービスを積極的に活用すべきだと感じています。

ベンダーへの希望としては、技術やサービスの提供だけでなく、企業やテレワーク勤務者が適切に導入し、使いこなせるよう、コンサルティングやマニュアル整備にも注力してほしいと思います。

また、難しいことかもしれませんが、サービスレベルに応じた費用対効果を明確にしてもらえれば、導入も進むのではないでしょうか。

――最後に、テレワークの普及促進に向けた提言があればお願いします。

テレワークが産業社会に浸透するためには、企業の経営者、システム管理者、そしてテレワーク勤務者、それぞれに高いセキュリティ意識が求められます。

中でも重要だと思うのが、テレワークの利用可否を判断する経営者の意識です。組織全体の情報セキュリティを確保する責任を有しているという自覚とともに、**そのための費用や労力を「余分なコスト」ではなく「必要不可欠な投資」と考えてもらいたい**と思います。そうした意識改革こそ、安全なテレワークの普及に最も必要ではないでしょうか。

図2　テレワークセキュリティガイドライン（抜粋）

経営者が実施すべき対策

- テレワークの実施を考慮した情報セキュリティポリシーを定め、定期的に監査・見直しを行う
- 情報の重要度をレベル分けし、テレワークでの利用可否や、利用可の場合の取扱方法を定める
- テレワーク勤務者への教育・啓発活動を実施させる

システム管理者が実施すべき対策

- 情報セキュリティポリシーに従い、対象となる端末にフィルタリングやウイルス対策ソフトをインストールするなどの対策を実施する
- 社内システムへのアクセス権限やファイアーウォールの設置などの対策を実施する
- 重要データのバックアップ体制を整える

テレワーク勤務者が実施すべき対策

- 情報セキュリティポリシーや社内ルールを順守する
- システム管理者の許可を受けたアプリケーションのみをインストールする
- 作業開始前に、最新のOSやウイルス対策ソフトが適用されていることを確認する
- マルウェアに感染した際は速やかに報告する
- オフィス外に情報資産を持ち出す際は、その原本を安全な場所に保存しておく
- 機密性が求められるデータを極力用いないよう業務方法を工夫し、やむを得ない場合は必ず暗号化するとともに、端末や記録媒体の盗難に注意する
- テレワークで使用するパスワードには一定以上の長さで推測されにくいものを使用し、使い回しを避ける

出典:総務省 テレワークセキュリティガイドライン（第4版）より抜粋

富士通のセキュリティ・ソリューション

“技術×人材”で産業社会全体のセキュリティレベル向上に貢献

IoT社会の発展や東京2020大会の開催、働き方改革に向けたテレワークの普及といった近年の社会動向から、情報セキュリティリスクの高まりと求められる対策について見てきた。ここからは、こうした社会の動きを踏まえて、富士通は何に注力し、どんなソリューションを提供していくのか、富士通のサイバーセキュリティを牽引する太田大州氏の話を紹介する。

富士通株式会社
サイバーセキュリティ事業
戦略本部
シニアエバンジェリスト
太田 大州 氏

「No Security, No Digital」をキーワードに、技術と人材の両面からセキュリティに挑む

――近年の社会における情報セキュリティの重要性について、富士通の認識やスタンスを教えてください。

サイバーセキュリティの重要性を社会が認識したのは、2001年の米国同時多発テロが契機と言われています。それまで、インターネットはデジタル社会を発展させる原動力というプラス面ばかりが注目されていました。しかし、テロの実行にインターネットが大きな役割を果たしたことで、その悪用されるリスクに気づき、そこから急速にサイバーセキュリティの取り組みが進展しました。

富士通では、これからのデジタル社会の信頼性や安定性を支えるうえで、セキュリティ対策が欠かせないという認識のもと、**「No Security, No Digital」をキーワードに、「技術」と「人材」の両面から、サイバーセキュリティの確保に向けたソリューションを提供**していきたいと考えています。

――技術と人材がセキュリティ・ソリューションの要ということですね。

サイバー攻撃の手口が巧妙化・高度化する中、システムや情報資産を守り抜くためのセキュリティ技術にも、さらなる進化が求められます。

先進的なセキュリティ技術を創造できる人材を育み、彼らが生み出した技術を使いこなすことで人材の底上げを図り、その中からまた新たな技術が生み出される。そうした好循環を生み出していくことが理想です。

3つの領域で先進のセキュリティ技術を創出

――具体的な技術開発のテーマとしては、どのようなものがあるでしょう？

現在、富士通が注力している技術領域は大きく3つあります。

第一に、**機密情報や個人情報を安全に利活用するための「データセキュリティ・プライバシー保護」**に関わる技術。データの暗号化や匿名化などを確実に、かつ効率的に行える技術開発を通じて、各種

表1 富士通のセキュリティ対策技術開発の成果

テーマ	技術	概要
データセキュリティ・プライバシー保護	パーソナルデータから個人の特定を防ぐk-匿名化技術	個人に紐付けられた大量の「パーソナルデータ」をビジネスに活用する際、その集団内に同じ属性を持つ人が少なくともk人以上存在するよう加工する「k-匿名化」技術によって、個人の特定を防止。自動で高速に、かつ少ないデータ量での加工を可能にした独自のソリューションとして提供しています。
認証・認可	手のひら静脈認証「Palm Secure（パームセキュア）」	手のひらの静脈を用いた個人認証は、静脈の本数が多く複雑なため識別精度が高いうえに、血管が太いため寒暖に左右されにくいといった優位性があります。すでに世界中で8,200万人が利用する「Palm Secure」を、2019年には国際標準規格FIDOに対応したソリューションとして提供する予定です。
サイバーセキュリティ	マルウェア感染の全体像を容易に把握できる高速フォレンジック技術	ネットワークの通信ログを解析することで、マルウェアを駆使した標的型サイバー攻撃の進行状況や感染経路、被害の全貌などを見える化する技術を開発。膨大なログから、サイバー攻撃に関わる情報だけを検知・集約することで、短時間での解析を可能にしており、被害が拡大する前に、迅速で包括的な対策が可能になります。

表2　セキュリティマイスターの3つの領域と人材像モデル

領域	対象組織	人材像モデル
フィールド領域 システム開発・運用の現場で高度なセキュリティ技術を適用し、お客様に安全・安心を提供するエンジニア	フィールドSE、 サービスエンジニアが属する組織	■サイバーセキュリティエンジニア ■サイバーセキュリティマスターエンジニア
エキスパート領域 お客様に最適なソリューションを提供するための、高度なセキュリティ特化技術を持つエンジニア	セキュリティビジネスや、 セキュリティ支援業務を行う組織	■セキュリティプロダクトエキスパート ■セキュアネットワークコーディネーター ■サイバーリスクアセッサー　■ペネトレーションテスター ■セキュリティアナリスト　■フォレンジックエンジニア ■サイバーリサーチャー　■レジスタードセキュリティスペシャリスト
ハイマスター領域 情報セキュリティ上の高度な脅威に対抗するための、業界最高レベルのセキュリティ技術を持つエンジニア	富士通グループ全体	■コードウィザード ■コンピュータウィザード ■グローバルホワイトハッカー ■シニアセキュリティコーディネーター

出典:富士通サイト「セキュリティマイスター認定制度」
http://www.fujitsu.com/jp/solutions/business-technology/security/secure/concept/security-meister/certification/

データの有効活用を支援していきます。

第二に、**クラウド空間を含めた様々なシステムをシームレスに、そして安全につなぐための「認証・認可」**に関わる技術。ID/パスワードに頼るのでなく、顔認証や指紋認証といった生体認証技術を確立するとともに、複数のシステムをまたいだフェデレーション(認証連携)などの技術開発に注力しています。

そして第三に、**サイバー攻撃への防御力を高める「サイバーセキュリティ」**に関わる技術。米国立標準技術研究所(NIST)が定めたフレームワークに基づき、「特定」「防御」「検知」「対応」「復旧」という5つの視点から、マルウェアの侵入などからシステムを保護するための技術開発に取り組んでいます。

セキュリティ人材の見える化が産業界全体のセキュリティ強化につながる

――もう1つの注力分野であるセキュリティ人材については、どのような取り組みが進んでいますか?

日本では、セキュリティ先進国である米国に比べて、ユーザー企業におけるセキュリティ人材の不足が懸念されています。これは、国民数というそもそもの母数の少なさに加えて、大学などでICTを学んだ人材の多くがユーザー企業ではなく富士通も含めたメーカー企業に就職するという事情もあります。

産業社会のセキュリティを維持するには、システムを提供するメーカー側だけでなく、実際に運用するユーザー側にも高いセキュリティ知識が求められます。富士通はそのギャップを埋めるために、まず、求められるセキュリティ人材の見える化に着手しました。それが2014年度に着手した「セキュリティマイスター認定制度」です。

――セキュリティ人材の見える化とは、具体的にどういうことでしょう?

一口に「セキュリティ人材」と言っても、セキュリティ技術を開発するエンジニアもいれば、システム特性を踏まえて最適なセキュリティ対策を講じるエンジニアもいるというように、求められる役割は多種多様です。

しかし、多くのユーザー企業では、セキュリティ人材に求める役割や、期待する知識・ノウハウなどが明確になっていないため、どんな人材が対応すべきかが判断しづらい状況でした。

そこで、まずは富士通グループ内に、どんな技術をもった人材が、どの組織に、どれだけいるのかを把握するために、**3つの領域、14の人材像モデルを定義して、系統的、計画的かつ継続的な育成を図る仕組み**を構築しました。

――サイバーセキュリティの担い手となる人材像を明確にすることで、その育成や、ユーザー企業のニーズへの対応がスムーズになるというわけですね。

その通りです。セキュリティ人材の育成は、富士通グループだけでなく、産業界全体の課題となっており、一般社団法人サイバーリスク情報センター(CRIC)では「産業横断サイバーセキュリティ人材育成検討会」を主催し、人材の育成や交流を図っています。

富士通もこの検討会に参加し、**セキュリティマイスター認定制度で培った経験を活かして、産業界全体におけるセキュリティ人材の育成を支援**しています。

――そうした取り組みが、新しいビジネスにつながることも期待できますね。

サイバー攻撃への脅威が高まり続ける中、ユーザー企業においてもセキュリティ人材の確保が不可欠です。

メーカー企業に偏りがちな人材構造は容易には変わらないでしょうが、サイバーセキュリティの担い手となる人材像を明確化することで、例えばアウトソーシング型のビジネスも可能になるでしょう。システムを提供する側と、活用する側の"共創(Co-creation)"によって、デジタル社会を支える強固なセキュリティを実現していきたいですね。