つながる社会を支える富士通のサイバーセキュリティへの取り組み

Fujitsu's Engagement on Cyber Security in Supporting Connected Society

向井　健太郎

あらまし

クラウド，ビッグデータ，AI（人工知能），IoTといった革新的なデジタルテクノロジーが今や身近なものとなり，社会のデジタル化が加速している。人やモノといったあらゆるものがデータとつながることで形成される「つながる社会」は，社会・経済システムの構造とその在り方にまで影響を及ぼし，我々の日常を劇的に変えている。デジタル革新が紡ぎ出すつながる社会によって，お客様のビジネス環境やビジネスそのもののデジタル化がとどまるところなく進展している。これらにより，利便性が高まる一方で，我々の生活を脅かすような新たな脅威が生まれ，身近に迫っており，システムやデータを守るサイバーセキュリティは欠かせない状況になっている。こうした状況を踏まえて，サイバーセキュリティは富士通の事業の根幹を支える生命線であり，お客様から信頼される能力を保有し続けることは富士通の使命であると認識している。

本稿では，我々を取り巻く環境と，つながる社会を支える富士通のサイバーセキュリティへの取り組みについて述べる。

Abstract

Innovative digital technologies, such as cloud, big data, AI, and the IoT have now become familiar, and the digitalization of society is accelerating. A connected society, formed by connecting everything—including humans and things—with data is affecting the structure of social and economic systems and the fundamental ways in which they work, which is in turn dramatically changing our daily lives. This connected society created by digital innovation, is advancing the digitalization of customers' business environments and businesses themselves in an unstoppable manner. As these changes bring improved convenience, at the same time, we are confronted by emerging new threats, which makes cyber security for protecting systems and data indispensable. In view of this situation, Fujitsu is aware that cyber security is the lifeline which supports the basis of its business, and it is recognized that it is the mission of Fujitsu to keep the ability trusted by the customer. This paper describes Fujitsu's engagement on cyber security to support a connected society.

1. まえがき

日本での普及率が3～5％程度にとどまっているスマートスピーカーについて，筆者の場合は得体の知れないデジタルアシスタントを家に招き入れる事に不安を感じ，躊躇してきた。そんな中，米国での普及率が4割を超えたというニュース[(1)]がきっかけとなり，我が家でも導入に踏み切った。新たな生活は思いの外快適で，未来が身近になってきた感覚を何となく醸し出してくれている。

20世紀に我々が思い描いてきた未来は，AI（人工知能），IoT，クラウド，ビッグデータ，ブロックチェーン，モビリティ，ロボティクス，そしていよいよ到来する5G（第5世代移動通信システム）といった，革新的なデジタルテクノロジーによって現実のものとなりつつある。

日本政府は，デジタル化する社会を背景に，テクノロジーとデータを活用して目指すべき未来社会である「Society 5.0」を提唱したが,[(2)] その実現にはサイバーセキュリティが欠かせない。あらゆるものがデータとつながって形成される「つながる社会」によって，デジタル革新が加速し利便性が高まっている。一方で，経済活動や日常生活を脅かすような新たな脅威が生まれている。

富士通ではサイバーセキュリティを事業の根幹を支えるものと捉えており，デジタル社会の変遷に身を置くお客様を将来にわたって支えるために，取り組みを加速している。

本稿では，つながる社会を支える富士通のサイバーセキュリティへの取り組みについて述べる。

2. 世界の潮流とサイバー攻撃の現状

本章では，世界の潮流，およびサイバー攻撃の現状と対策を意識した政府の動きなどについて述べる。

2.1 世界の潮流

2018年以降の世界の潮流を俯瞰すると，自国第一主義が台頭し，大国間における貿易戦争は激化している。また，世界規模で排他的な風潮が高まっているとともに，国際秩序が揺らぐような様相を見せており，地政学的リスクが高まってきている。これらの情勢を踏まえたのか，国際通貨基金（IMF）は2018年10月に数年ぶりとなる世界経済の成長の鈍化とインフレの加速を発表するなど，経済面でも不安要素が出てきている。

技術面の潮流とデジタル革新の波は，国際協調体制にも大きく波及し始めている。既にデータ保護については，特定データの域外移転の制限などを含め，世界レベルで盛んに議論が交わされている。また，AIがもたらすシンギュラリティ，通信速度が100倍にもなる5G，そして量子コンピューティングなどのデジタルテクノロジーは，新たなイノベーションを呼び起こし，我々の日常のみならず，戦場や戦争そのものを確実に劇的に変えて行く。デジタルテクノロジー分野での覇権は長期的には世界の覇権に直結するため，大国間の利害関係は対立し続けるであろう。

地政学的リスク分析で定評のあるユーラシア・グループは「Top Risks 2019」において，今後西側諸国がサイバー攻撃に対して反撃を開始する可能性などを挙げ,「熾烈化するサイバー戦争」を世界の十大リスクの三番目に挙げており,[(3)] 懸念が高まっている。地政学，経済，そして技術といった潮流は複雑に絡み合い，国家間の軋轢（あつれき）が生まれ，今後より一層，国際社会や世界経済の先行きの不透明感が増していくことが危惧される。

2.2 激化するサイバー攻撃

サイバー攻撃の主体は，個人から国家組織まで多岐にわたる。国内のサイバー総攻撃数は，2013年から2018年の間に，12.4倍に急増している。[(4)] また，全世界のサイバー攻撃による経済被害は2017年には約63兆円に上り,[(5)] 全企業活動の純利益420兆円[(6)]の約15％という規模にまで達している。

社会がデジタル化していく中で，我々の社会は「新たな脅威」にさらされている。2017年に，ランサムウェア[(注1)]のWannaCryが，わずか24時間で全世界に拡散し，病院や工場，そして鉄道の券売機など，現実空間に実被害をもたらした。ほかの注視す

（注1） データやシステムを人質にして身代金を要求するマルウェア。マルウェアは悪意が込められたソフトウェア。

べきサイバー攻撃の事例としては，2015年にウクライナで発生した大規模停電（社会インフラへの攻撃），2017年の仮想通貨の窃取（金融システムへの攻撃），そして2016年の米大統領選における情報操作疑惑（民主主義への挑戦）などが挙げられる。

今後，先進国をはじめとした様々な国が標的となり，金融や電力などの重要な社会インフラが長期にわたって停止した場合，人命は危機にさらされ，2008年の金融危機がもたらしたような，システミックリスクを引き起こす可能性があると懸念されている。

2.3 攻撃手法の進化

攻撃の激化とともに，攻撃の手法も急激な進化を遂げている。WannaCry以降も，わずか数年のうちにNotPetyaやSamSam，およびそれぞれの進化型の亜種が発生し続けている。中には，ランサムウェアのコードを利用し，仮想通貨の採掘を行うものもある。また最近では，既存のウイルス対策ソフトでは検知できないファイルレスマルウェアが出てきている。これは，メモリ領域を活用したり，Windows端末に搭載されている純正ツール（PowerShellやWMI-Windows Management Instrumentationなど）を活用したりする攻撃である。

標的型攻撃においては，メールやWebサイト，USBメモリを用いる手法にとどまらず，チャットボットやWi-Fiハッキングなどを用いるケースも現れている。また，サプライチェーン上の製造過程にあるソフトウェアやハードウェアにバックドアを埋め込んだ攻撃や，正規のソフトウェアアップデート機能を悪用してマルウェアを配信するなど，攻撃手法も巧妙化している。

マルウェアを中心とした攻撃や標的型攻撃への対処に目が行きがちではあるが，不正に入手したユーザー認証情報を活用して本人になりすました不正なアクセスや，Webアプリケーションの脆弱性を突いた攻撃，そしてEC（Electronic Commerce）サイトからの情報窃取なども盛んである。

デジタル革新によって生み出され続けているテクノロジーの数々は，攻撃対象領域を広げており，スマートフォン，IoT，およびOT（Operational Technology）に加え，AIも狙われ始めている。例えば，AIに学習させるデータを汚染することによって，判断ミスを誘発するような攻撃も懸念されている。2011年にロッキードマーチン社が提唱した，サイバー攻撃のプロセスを七つのステップに分けてモデル化したサイバーキルチェーンがあるが，現在では約9割の攻撃が最初の五つのステップを一括した形で実行されており，[7] 攻撃側の手法が高度化していることが伺える。

これらの状況を受けて，米MITREのATT&CK[8]や米国政府のCTF（Cyber Threat Framework）[9]など，テクノロジー領域において新たな対応フレームワークが開発されている。

2.4 脅威に関する認識と対策

脅威が拡大し続ける中，2018年1月に行われたダボス会議[注2]では，サイバー攻撃が経営者にとっての三大重要リスクの一つとして初めて認知された。翌年の同会議においても，引き続き発生可能性の高いリスクのトップ5としてランクインしている。[10] 最重要経営課題としてサイバー脅威が認知された背景を，以下に示す。

・サイバー攻撃が多くの企業に被害を与え，経営を脅かし続けている事実
・グローバルガバナンスや対策の難しさ
・各国・地域で乱立しているサイバーセキュリティに関わる法規制（データ，サプライチェーン，クラウド，IoTなど）への対応の難しさ

また，サイバー攻撃には以下に示す特有の性質があるため，対応が難しい。

・防御側が圧倒的に不利な構造であること
・抑止が成立しにくいこと
・内部脅威への対応が難しいこと
・外国の国家機関による関与があること
・ビジネスとしての対策は防衛しかないこと
・対応できる人材が限られること
・相手が海外にいる場合が多いこと
・相手の特定が困難であること

米国ではICT製品のサプライチェーンを狙ったサ

（注2） 毎年1月スイスのダボスで開かれる世界経済フォーラムの年次総会。世界各国の政財界のリーダーや学者らが参加し，賢人会議とも言われる。

イバー攻撃に対する危機意識が定着しており，政府や重要インフラの調達においては潜在リスクのあるハイテク製品が排除されている。安全保障の観点から，日本も相応の対応が迫られている。米国国立標準技術研究所（NIST）は，既存のセキュリティ規格やガイドライン類にサプライチェーンリスクマネジメント（SCRM）の要件を盛り込んで，対策の普及に努めている。これらのセキュリティ要件が市場への入場券となるのは確実であり，製品やサービスを提供したり活用したりする側もこれらへの対応が遅れるようであれば市場からの退場を余儀なくされるであろう。米国では，国土安全保障省が官民連携タスクフォースの立ち上げを2018年11月に発表し，官民連携強化に邁進している。[11]

3. つながる社会を支えるソリューション

これらの状況を鑑み，富士通ではサイバーセキュリティ事業における戦略として，お客様のマイナスの極小化（サイバー攻撃による経営リスクの極小化）とプラスの拡大（お客様の攻めの投資であるデジタル化のサポートなど）に注力することで，お客様の成長に必要なデジタル革新を支え続けることを目指している（図-1）。

本章では，富士通が提供するソリューション群，および注力領域や差異化要素などについて述べる。

3.1 ライフサイクルに即したソリューション

富士通では，図-2に示すサイバーセキュリティのライフサイクル全体を包括したソリューションを，ワンストップで提供している。以下に，ソリューションの各機能の概要を述べる。

(1) アセスメント・コンサルティング

お客様のシステムや業務設計におけるセキュリティコンサルティング。脆弱性分析や事業インパクト分析といったアセスメント，業務継続を意識したプロセス，システムの脆弱性改善・耐性強化など。

(2) ツール導入

セキュリティ要件を実装し，セキュアなシステムを構築するセキュア・システムインテグレーション（SI）。

(3) 監視・運用

お客様のパソコンやネットワークなど，システム環境全体のサイバーセキュリティを24時間365日リアルタイムで監視・運用するマネージドセキュリティサービス（MSS：Managed Security Service）。防御から検知，プロアクティブ対応までのライフサイクルに即した対応，運用強化支援およびインシデントへのレスポンスなど。

(4) 人材教育サービス

高度セキュリティ専門人材の育成・訓練サービス。

これらの機能をもつソリューションによって，富士通は以下に示す四つの要素をグローバルにワンストップのサービスとして提供している。これらを掛け合わせたものが富士通の総合力と優位性であると認識している。

①差別化の源泉

セキュリティに関わる様々なインテリジェンス，

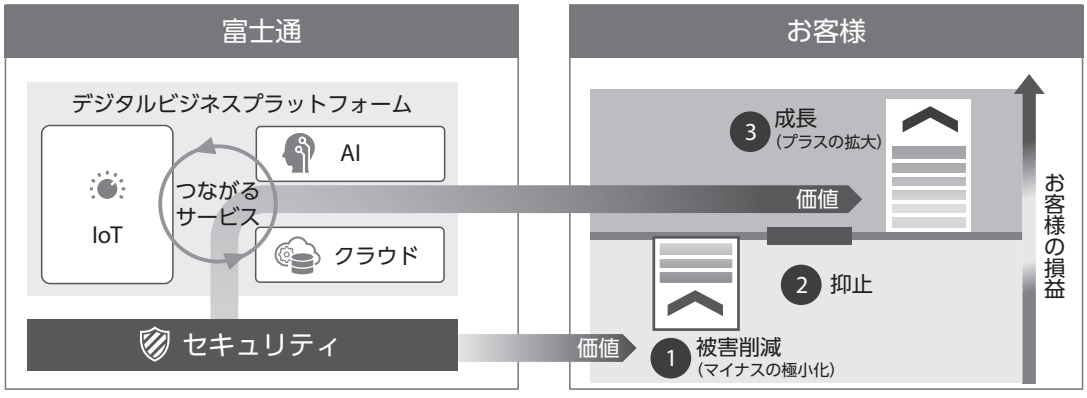

図-1　富士通のサイバーセキュリティ事業モデル

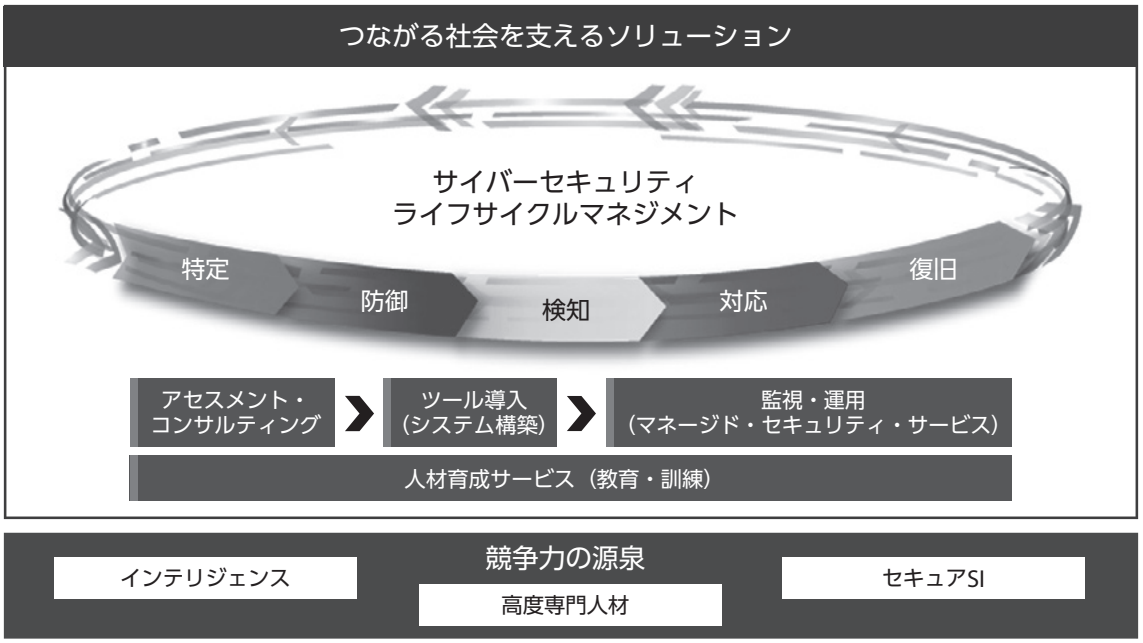

図-2　ライフサイクルに即したソリューションと競争力の源泉

高度セキュリティ専門人材，最先端技術・サービス，事業インフラ（SOC：Security Operation Center）

②お客様環境や業種の理解

長年にわたりシステム運用の現場で培ってきたナレッジを活用

③セキュリティ要件のシステムへの適用（セキュアSI）

システムの企画段階からセキュリティ要件を盛り込むセキュリティデザインに裏付けされたインテグレーション力を適用

④グローバルカバレッジ

東京およびロンドンの2ヘッドクォーター体制によるグローバルサポート

3.2 必要とされるインテリジェンス

2章で述べたとおり，世界の地政学・経済・技術の潮流は，サイバー空間にも大きな影響を及ぼすと考えている。富士通ではこれらに加えて，セキュリティに関する法制度・標準規格，サイバー攻撃に関する脅威情報などのインテリジェンスをグローバルに収集・分析し，サービスに活かしている。

サイバー攻撃を受けない組織や侵入を100％防げる組織は存在しないため，攻撃への対応は，常にインシデントが発生してから対処する後追い型である。このため，侵入を検知するまでは攻撃が続いてしまう。ある調査によると，世界でサイバーセキュリティ侵害の発生から検知までに要した日数は平均101日で，アジア太平洋地域に限定するとこの値は498日にまで跳ね上がると示されている。[12] このことから，「検知」と「検知後の対処」の迅速化が求められている。

富士通では，被害の極小化に直結する施策として，侵害から検知までの期間を短縮するために，従来のインシデント・ドリブン型アプローチに加えて，インテリジェンスを活用して攻撃者などを想定して先手を打つインテリジェンス・ドリブン型アプローチを導入している。このアプローチによって，脅威の兆候などを先読みし，タイムリーな防御力の向上と早期検知，更に関係部門へ対策を促すことで，被害の極小化に努めている。これらは，お客様の業務継続性を意識した，プロアクティブな防御と早急な対応による復旧を実現する上でも貢献している（図-3）。

サイバー脅威情報については，富士通社内に設置したA3L（Advanced Artifact Analysis Laboratory）がインターネットやダークウェブなどから最新情報を収集・分析し，マルウェア解析，デジタルフォレンジック分析，インシデント分析を

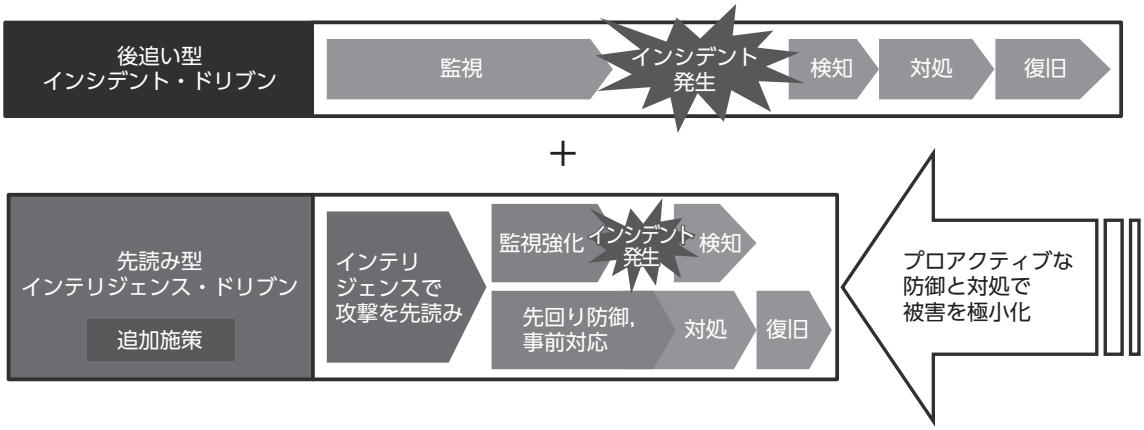

図-3　インテリジェンス・ドリブンセキュリティ

行っている。また，脅威情報をデータベース化し共有することで，セキュリティサービスの強化につなげている。

グローバルに高まるサイバーセキュリティへの懸念を背景に，各国・地域においてセキュリティに関わる規制や規格が乱立している。このような状況に対して，規制や規格の具体的な内容に加えて，それらを突き動かしている背景などをタイムリーに捕捉し，富士通の事業に迅速に反映させることを意識して取り組んでいる。

変遷し続けるデジタルビジネスを支える，多様なシステムをサポートするためには，まだ顕在化していない将来の脅威に立ち向かうとともにインテリジェンスを磨き続ける必要がある。富士通は，長年にわたってシステム運用の現場で培ってきたナレッジを，このインテリジェンスと掛け合わせることで，お客様をより強力にサポートすることに注力している。

3.3　セキュアSI

システムのサイバーセキュリティ対策において，セキュリティ・バイデザインは欠かせない。富士通はこれを徹底させるために，企業内における情報セキュリティ対策の技術的な基本方針であるESA（Enterprise Security Architecture）を2006年に確立している。

富士通はESAにおいて，ソリューションのアーキテクチャー（構成するフレームワーク，運用手法，テクノロジー，プロダクトを標準化したもの）を明確に定義し，理想とするSMF（Security Management Framework）をリリースした。セキュアSI事業を通して，富士通の顧客提供価値をお客様に認識していただけるようになると考えている。

デジタル革新に伴って，守るべき対象が人やデータ，IoTから，あらゆる設備まで爆発的に拡大しており，サイバーセキュリティの境界線が曖昧になっている。そのような環境の変化に対応するために，現在ESAの改版に着手している。NISC（内閣官房情報セキュリティセンター）が2011年に，情報セキュリティを企画・設計段階から確保するための方策[13]としてセキュリティバイデザインを提唱している。こうした動きを受けて，富士通では社内の高度サイバーセキュリティ専門人材であるセキュリティマイスターを通じて，セキュリティ・バイデザインの普及を目指している。

3.4　高度専門人材

富士通では，恒久的にサイバー脅威と対峙して行く上で必要な能力を培う仕組みとして，セキュリティマイスター制度を確立している。これを通じて，2021年度末までに1.1万人規模の高度専門人材を社内で育成する予定である。

富士通では，インシデントに適切に初動対応できる実践力を備え，セキュリティ専門家と連携できる人材や，お客様が必要とするソリューションを素早くお届けすることを目的として，各業種のお客様の課題解決をリードする専門知識と経験値の高い営業

人材である専門営業を育成している。

富士通では社内の人材育成に加えて，産学官連携を通じてセキュリティ技術者育成にも取り組んでいる。

4. つながる社会を支える先端技術

データ，システム，人，AI，IoTによってつながる社会が形成されるが，これからの社会を守るためには，それぞれの信頼性を担保するサイバーセキュリティ技術が欠かせない。

例えば，データ保護の観点から必要な技術として，データのライフサイクルにおいて，データをいかにセキュアな形で複数の組織間で流通させるかがポイントとなる。以下に必要な技術を挙げる。

・データにセキュアにアクセスする技術
・データが漏えいしてもリスクを最小限に抑えるためのデータの匿名化や暗号化などの保護技術
・データの改ざんを防ぐデータ管理技術であるブロックチェーン技術

また，AIに提供するデータが汚染されないようにするなど，多様なリスクに対応する対策も必要となってくる。

デジタル革新は攻撃側にもメリットがあり，AIの高度化などに伴って，今後人間が介在せず高度に自動化・高速化された攻撃も出てくるであろう。したがって，防衛側も革新的であり続けないと対抗できない。複雑なセキュリティ運用の高速化と高度化を実現するためのオートメーションやオーケストレーションについて，取り組みを始めている。

更に，富士通は，独自技術を核とした新サービスの開発を目指し，以下の新たな取り組みにも挑戦し続けている。

(1) MSS高度化技術

・脅威検知関連：EDR（Endpoint Detection & Response），MDR（Managed Detection & Response），Threat Hunting
・アイデンティティ＆アクセス管理：IAM（Identity Access Management），IGA（Identity Governance & Administration）
・プラットフォーム関連：TIP（脅威インテリジェンスプラットフォーム），オートメーション＆オーケストレーション技術
・上記へのAI適用

(2) データの信頼性担保技術

富士通独自の技術「コネクションチェーン」

(3) 品質強化（テスト技術）

システムやIoT製品における未知の脆弱性検出技術（ファジングツール）

(4) 認証（生体認証技術）

(5) IoT/OTセキュリティ

(6) データ保護技術，暗号化など

5. 富士通の目指すセキュリティの姿

富士通ではMSSをはじめとするセキュリティサービスの更なる強化に向けて，東京およびロンドンの2ヘッドクォーター体制を2018年に敷いた。これによって，先進技術の自社サービスへの取り込みを加速させる。ほかにも，マルチリージョン対応，SOCなどのビジネスインフラの高度化，セキュリティインテリジェンス活用などによって，サービスを強化し続けている。これらの事業を支える上で最も重要な人材育成手法についても，グローバルな体制を最大限に活かしながら強化していく。

富士通は，今後もお客様，パートナー様，業界をはじめとした産官学連携を通じて，サイバーセキュリティのエコシステム強化にグローバルに取り組んでいく。

6. むすび

本稿では，デジタル革新を背景とした新たな脅威と，つながる社会を支える富士通のサイバーセキュリティの取り組みについて述べた。

サイバー攻撃は，サイバー空間が人類の活動と価値創造のプラットフォームである限り，止むことはない。安全で安心できる社会の発展にサイバーセキュリティは不可欠である。今後も，脅威と対峙する力を保有し続け，お客様から信頼される存在となるために挑戦を続けていく。

参考文献

(1) RBC Capital Markets Report：Tech Crunch

(2018).
https://techcrunch.com/2018/12/28/smart-speakers-hit-critical-mass-in-2018/
(2) 内閣府：第5期科学技術基本計画 (H28～H32).
https://www8.cao.go.jp/cstp/kihonkeikaku/5honbun.pdf
(3) Eurasia Group："Top Risks 2019" (2019).
https://www.eurasiagroup.net/siteFiles/Media/files/2019_Eurasia_Group_Top_Risks_Report_Japanese.pdf
(4) NICT (国立研究開発法人情報通信研究機構)：NICTER観測レポート2018.
http://www.nict.go.jp/press/2019/02/06-1.html
(5) McAfee & CSIS："Economic Impact of Cybercrime—No Slowing Down" (2018).
https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf
(6) 日経：「純利益 世界で3割増　17年度、トップ10に中国4社」.
https://www.nikkei.com/article/DGXMZO29489060X10C18A4MM8000/
(7) Alert Logic：The State of Threat Detection 2018.
https://www.alertlogic.com/resources/industry-reports/2018-critical-watch-report/
(8) MITRE：ATT&CK.
https://attack.mitre.org/
(9) ODNI：CTF.
https://www.dni.gov/index.php/cyber-threat-framework
(10) WEF：The Global Risks Report 2019.
http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf
(11) DHS：広報リリース (2018).
https://www.dhs.gov/news/2018/11/15/dhs-announces-ict-supply-chain-risk-management-task-force-members
(12) FireEye：M-Trends 2018.
https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html
(13) NISC：情報セキュリティ企画・設計段階から確保するための方策.
https://www.nisc.go.jp/active/general/pdf/SBD_overview.pdf

著者紹介

向井　健太郎 (むかい　けんたろう)
富士通 (株)
グローバルサイバーセキュリティビジネスグループ
グローバルビジネスの開発に従事。