11
2017
Vol.6 No.11

インプレス Smart Grid ニューズレター

エネルギーとIoTの融合時代を拓くスマートグリッド専門メディア

［創刊5周年記念特集］

impress
http://sgforum.impress.co.jp/sgnl/

5 ANNIVERSARY

【創刊5周年記念】特別座談会

IoT時代のサイバーセキュリティにどう対処すべきか《前編》

― 本当の考えるべき危機はどこにあるのか ―

インプレス SmartGrid ニューズレター編集部

2020年夏に開催が予定されている、東京オリンピック・パラリンピックを間近に控え、国際的にサイバーセキュリティ攻撃が激化している。総務省やIPA（独立行政法人情報処理推進機構）の発表によれば、従来、サイバー攻撃の対象は企業の業務システムやWebサイトなどの「情報システム」が主体であったが、近年は、イランの核施設をはじめドイツの製鉄所やウクライナの電力システム（変電所）の「制御システム」に至るまで、そのターゲットを広げて攻撃されている。

さらに、IoT時代を迎える2020年には、各種センサーをはじめ、家電や自動車、医療や産業などの各種機器など、200億個とも500億個ともいわれるIoTデバイスが接続されるとあって、IoTシステムへのサイバー攻撃への対応も迫られている。

事実、2017年5月にIPAが発表した「情報セキュリティの10大脅威 2017」（後出の表2を参照）では、個人および組織におけるIoT機器への脅威が、ともに「10大脅威」にランク入りするなど、その攻撃の激しさが増大し、拡大してきている。

ここでは、IoT時代のサイバーセキュリティについて、本当に考えるべき危機と課題について議論していただいた。

【座談会出席者】＜司会＞東京大学 情報理工学系研究科 教授　江崎 浩（えさき ひろし）氏、
株式会社サイバーディフェンス研究所 専務理事・上級分析官　名和 利男（なわ としお）氏、
マカフィー株式会社 サイバー戦略室 シニア・セキュリティ・アドバイザー CISSP　佐々木 弘志（ささき ひろし）氏

1 サイバー攻撃の脅威を前提とした対策が必要とされるIoTの現場

江崎：2020年には200億～500億個のIoTデバイスが接続される時代を迎えるといわれています（図1）が、現在でも国際的にサイバーセキュリティ攻撃が激化しています（表1、表2、6ページ）。

図1　IoT時代に2020年には200億～500億個のIoTデバイスが接続されるイメージ

出所　IPA「情報セキュリティ　IoTのセキュリティ」https://www.ipa.go.jp/security/iot/index.html

IoTセキュリティ脅威の全体像として、図2（6ページ）に示すような体系的なマップが例として発表もされています。外側からCyber Warefare（サイバー戦争）、Cyber Criminals（サイバー犯罪）、Ransomeware（身代金ウィルス）が企業や組織に向かっていて、これらがIoTセキュリティの脅威を生んでいます。

また、実際に観測されたサイバー攻撃の対象についても、図3（7ページ）のように発表

されています。

最近では、総務省から、「IoT セキュリティ総合対策」[注1]が2017年10月に発表され、日本でIoTシステムのセキュリティ対策を総合的に推進するため、その取り組むべき課題が整理され、(1) 脆弱性対策に係る体制の整備、(2) 研究開発の推進、(3) 民間企業等におけるセキュリティ対策の促進、(4) 人材育成の強化、(5) 国際連携の推進、などを中心に取り組みが開始されています。

そこで、まず、IoT時代のサイバーセキュリティについて、サイバー空間（インターネット利用環境）と実空間（現場におけるIoTシステム環境）の関係について、お聞きしたいと思います。

名和：最近、企業が攻撃される内容やプレイヤー（システムの現場担当者）がかなり変わってきているという印象を受けています。

これまでのITシステムにおけるサイバー空間の利用（インターネットの利用）は、企業のビジネス効率を追求することがメインでした。ところが、IoTを使ったシステム（サイバー空間）の場合には、目的ががらりと変わってきます。

従来のITシステムの場合、コストセンターともいわれるITシステム部門の担当者が、サイバーセキュリティ対処の主人公になっています。私が、サイバー攻撃を解決するために緊急要請を受けて対処支援のためその企業に行くと、ITシステム部門の担当者にはどことなく、「システムが止まってもやむを得ない」という雰囲気が漂っています。ところが、IoTシステムに近いところでインシデント（サイバーセキュリティ攻撃）が発生し、同様に対処支援のために行くと、その現場は殺気立っているのです。売り上げが下がるということが目前に迫っている、あるいは社内横断的なプロジェクトが進んでいる場合には、周辺に迷惑がかかることに非常に敏感になっているのです。

お金（売り上げ）に直結する現場、すなわち実空間のビジネス領域においては、意識が大きく変化してきているという印象を強く受けています。

江崎：そんなに変化しているのですか。

ところで、2016～2017年にかけて、日本では、電力やガスの小売全面自由化が行われました。電力市場における競合他社に対応するため、電力業界では、ネットワーク化による事業の効率化がいっそう求められるよう

表 1　日本国内および海外の最近の大きなサイバー攻撃の事例

発生時期	サイバー攻撃被害の内容
【日本国内のサイバー攻撃の事例】	
2015年6月	日本年金機構の職員が利用する端末がマルウェアに感染し、年金加入者に関する情報約125万件が流出
2015年10月	金融庁の注意喚起を装ったフィッシングサイトを確認、国内銀行のセキュリティを向上させるためと称し、口座番号、パスワード、第二認証などの情報をだまし取られる恐れ
2015年11月	東京五輪組織委員会のホームページにサイバー攻撃、約12時間閲覧不能
2016年6月	i.JTB（JTBのグループ会社）の職員が利用する端末が、マルウェアに感染し、パスポート番号を含む個人情報が流出した可能性（標的型攻撃）
【海外のサイバー攻撃の事例】	
2010年6月	イランの核施設でウラン濃縮用の遠心分離機の制御システムがサイバー攻撃を受け機能不全に陥る
2014年12月	ドイツの製鉄所のネットワークがサイバー攻撃を受けて溶鉱炉を管理する制御システムが正常に動作しなくなった
2015年4月	フランスのテレビネットワークTV5 Monde（テヴェサンクモンド）がサイバー攻撃を受け、放送が一時中断
2015年6月	米国連邦人事管理局（OPM：Office of Personnel Management）が不正にアクセスされ、政府職員の個人情報が流出
2015年12月	ウクライナの電力会社の制御システムがサイバー攻撃を受け、停電が発生
2016年9月	インターネットサービス大手企業の米国ヤフーがサイバー攻撃を受け5億人分の顧客情報が流出
2016年10月	米国の大手DNSサービス会社Dyn社（ニューハンプシャー州）のDNSサーバが大規模なDDoS攻撃を受け、同社のDNSサービスの提供を受けていた企業のサービスにアクセスしにくくなる等の障害が発生
2016年12月	ウクライナの電力会社の制御システムがサイバー攻撃を受け、2回目の停電が発生
2017年5月	日本を含む世界150カ国以上で、ランサムウェア（身代金要求型ウィルス）のサイバー攻撃を受け、その被害件数は20万件以上に及んだ

出所　総務省「サイバーセキュリティの現状と総務省の対応について」、平成29（2017）年1月30日をもとに編集で作成、http://www.soumu.go.jp/main_content/000467154.pdf

▼注1
総務省におけるサイバーセキュリティタスクフォース：「IoTセキュリティ総合対策」、http://www.soumu.go.jp/main_content/000510701.pdf

表 2　情報セキュリティの 10 大脅威 2017（IPA 発表）

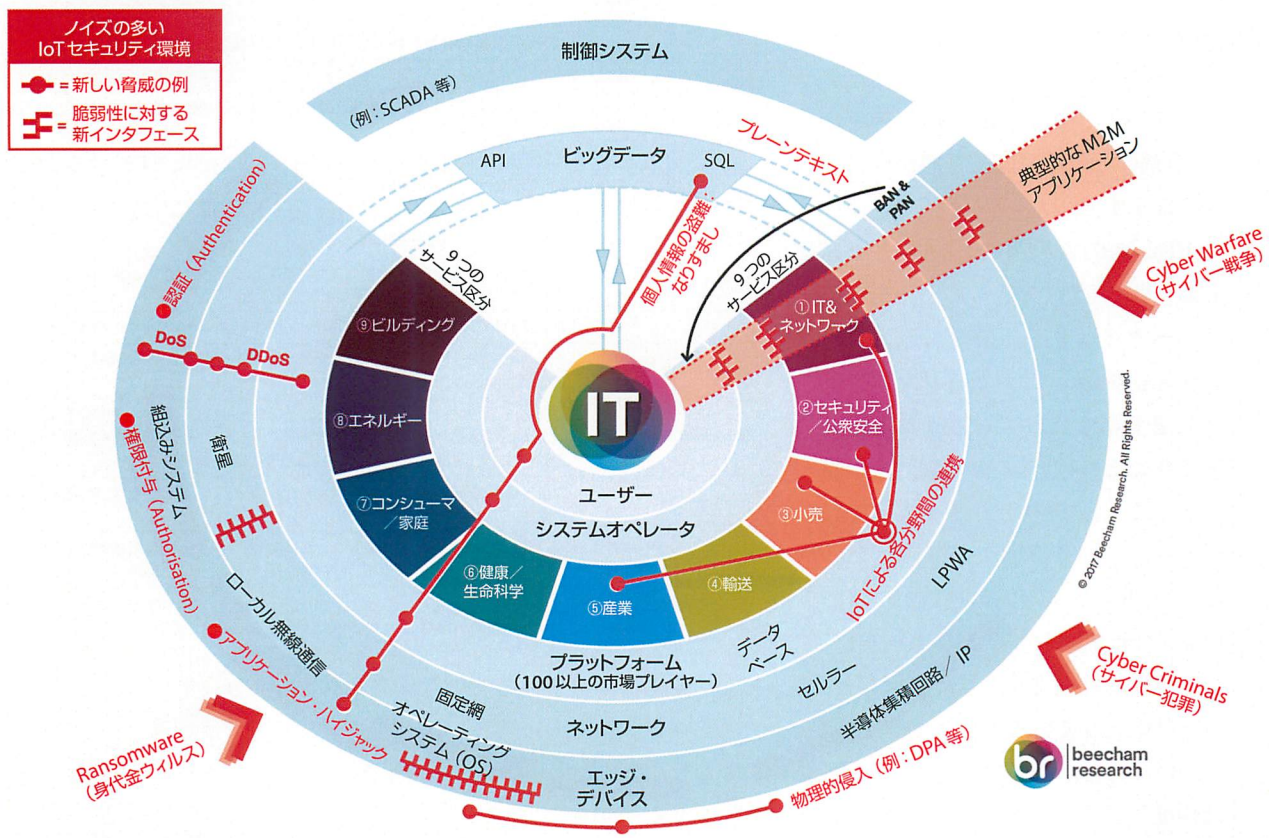
2016 順位	個人への脅威	2017 順位	組織への脅威	2016 順位
1 位	インターネットバンキングやクレジットカード情報の不正利用	1 位	標的型攻撃による情報流出	1 位
2 位	ランサムウェアによる被害	2 位	ランサムウェアによる被害	7 位
3 位	スマートフォンやスマートフォンアプリを狙った攻撃	3 位	ウェブサービスからの個人情報の窃取	3 位
5 位	ウェブサービスへの不正ログイン	4 位	サービス妨害攻撃によるサービスの停止	4 位
4 位	ワンクリック請求等の不当請求	5 位	内部不正による情報漏えいとそれに伴う業務停止	2 位
7 位	ウェブサービスからの個人情報の窃取	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（アンダーグラウンドサービス）	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

備考　①情報セキュリティ専門家を中心に構成する「10 大脅威選考会」の協力によって、2016 年に発生したセキュリティ事故や攻撃の状況等から脅威を選出し、投票によって順位付けされた。
②スマートフォンが普及し金銭をだまし取られる等の被害に遭うケースが発生しており、スマートフォンのセキュリティ対策も必須となってきている。
③ 2016 年はランサムウェア（※）による被害が拡大。個人・組織の両面において IoT 機器への脅威が登場。また、2016 年の後半には、設定が十分でない IoT 機器を狙い、IoT 機器をボット[注1]化し、DDoS 攻撃（ディードス攻撃[注2]）に悪用する、「Mirai」と呼ばれるウィルスが猛威を振るった。
※ランサムウェア（Ransomware：身代金要求型ウィルス）に感染すると、自分のパソコンだけではなく、組織内の別のサーバのファイルも暗号化されてしまうため、組織にとっては、警戒すべき脅威である。

（注 1）ボット（BOT）：コンピュータウィルスの一種（ボットウィルス）。パソコンがボットウィルスに感染すると、従来のウィルスと異なり、攻撃者が送ってくる命令を待つようになり（感染したことが分かりにくい）、命令がくると感染したパソコンから情報が盗まれたりする。攻撃者は命令によってパソコンを「ロボット（Robot）」のように操れることに由来して命名された。
（注 2）DDoS（ディードス）攻撃：Distributed Denial of Service attack、分散型サービス不能攻撃。標的とするサーバ（コンピュータ）に、複数のコンピュータから大量のパケットを送りつけ、ネットワークを輻輳（渋滞）させ、サーバのサービス機能を停止させてしまう攻撃。

出所　IPA「情報セキュリティ 10 大脅威 2017」、2017 年 5 月をもとに編集部作成、https://www.ipa.go.jp/security/vuln/10threats2017.html

図 2　IoT セキュリティ脅威のマップ：安価で普及した、高機能なエッジ・デバイスが新たな攻撃面を作り出す



ローカルネットワーク：Wi-Fi や Bluetooth、ZigBee などによるセンサーネットワーク等
DPA：Differential Power Analysis、差分電力解析。暗号を処理しているデバイスの消費電力を複数回測定して、その平均から秘密鍵を推測する攻撃のこと。消費電力を複数回測定するのは、消費電力を測定する場合に測定誤差をできるだけ小さくするため。

出所　Beecham Research（英国の調査会社、1991 年設立）、http://www.beechamresearch.com/download.aspx?id=43
〔参考〕DoD Policy Recommendations for The Internet of Things（IoT）、December 2016 http://dodcio.defense.gov/Portals/0/Documents/Announcement/DoD%20Policy%20Recommendations%20for%20Internet%20of%20Things%20-%20White%20Paper.pdf?ver=2017-01-26-152811-440

になりました。このため、情報系システム（IT）と連携する電力システムの制御系システム（OT：Operational Technology）についても、外部からのサイバー攻撃の可能性が増してきており、サイバー攻撃の脅威が存在することを前提とした対策が必要とされています（図4）。

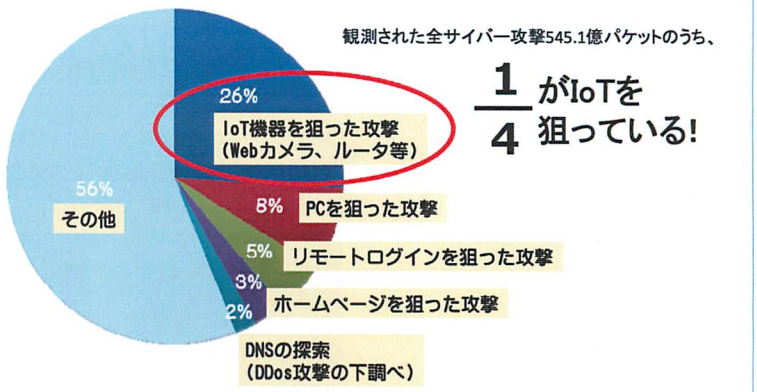
エネルギーの分野で、何かサイバーセキュリティ関連のトピックはありますか。

名和：今年（2017年）に入って、私の担当するエネルギー分野でマルウェア[注2]が発見されました。これは、システムの委託業者から感染したことが明らかでしたが、誰もその責任を負いたくなかったのか、あるいは同時に他の不具合が発見されたためか、「故障」ということにして解決させた現場が複数箇所あります。これも、IoTといってよいかどうかわかりませんが、OTにおけるインシデントです。

江崎：佐々木さんは、最近のサイバーセキュリティの実態について感じていることはありますか。

佐々木：IoTの世界では、すべてのモノ（デバイス）がネットワークにつながってきます。このためOECD[注3]の情報セキュリティのためのガイドライン[注4]では、情報システムに関するサイバーセキュリティについて、CIA（Confidentiality：機密性、Integrity：完全性、Availability：可用性）が定義されています（図5、8ページ）。

図3　NICT（情報通信研究機構）で観測されたサイバー攻撃の対象



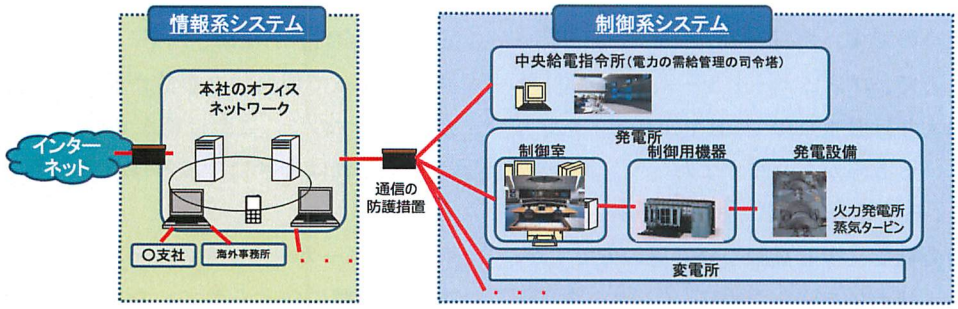
NICT：Institute of Information and Communications Technology、国立研究開発法人情報通信研究機構

出所　「サイバーセキュリティの現状と総務省の対応について」、平成29（2017）年1月30日、
http://www.soumu.go.jp/main_content/000467154.pdf

Availability、つまり、システム上に流通している情報に対してアクセス権をもっている人が、いつでもアクセスできるようになっていることについて、よく話をするのですが、現場の方はCIAがよくわからない。そのため、結局、彼らのプライオリティ（優先順位）はセーフティ（安全性）が第一であり、それがすべてなのです。

このため、話がかみ合わないところがあります。現実問題として、IoTに真剣に取り組むのでしたら、このようなCIAを必須と考えなくてはいけない。しかし、システム担当者の理解が追いついていないのです。そのうえ、社内の人同士のつながりがまだ弱いところがあります。その点が、実は現場におけるサイバー攻撃に対する一番の脆弱性なのではないかと思っています。

図4　電力分野における情報系システム・制御系システムの連携



出所　経済産業省、「電力分野におけるサイバーセキュリティ対策について」、平成28（2016）年7月1日、
http://www.meti.go.jp/committee/sougouenergy/denryoku_gas/kihonseisaku/pdf/007_06_00.pdf

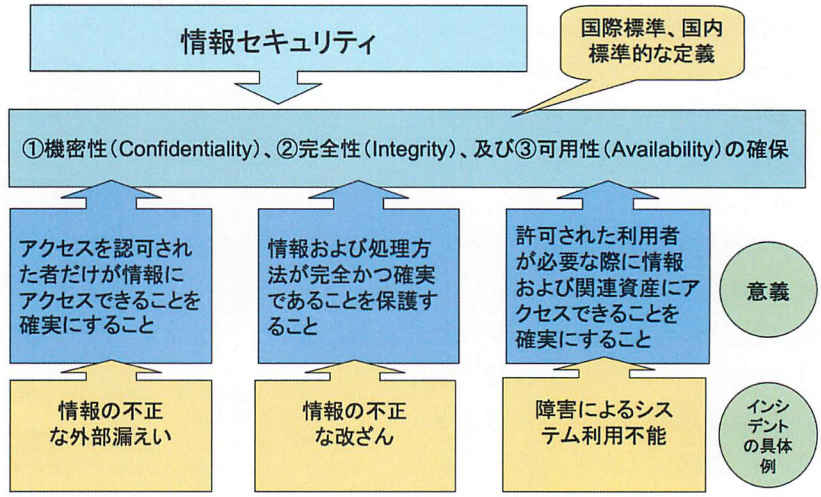
▼注2
マルウェア：Malwareは、Malicious（悪意のある）とSoftware（ソフトウェア）を組み合わせた造語。悪意のあるソフトウェアは総称して、マルウェアと呼ばれる。マルウェアには、プログラムの一部を書き換え（改ざん）て自己増殖する「ウィルス」（Virus）や、他のプログラムに関係なく単独で自己増殖する「ワーム」（Worm）などの種類がある。

▼注3
OECD：Organisation for Economic Co-operation and Development、経済協力開発機構。1948年4月発足。先進国間の自由な意見交換・情報交換を通じて、（1）経済成長、（2）貿易自由化、（3）途上国支援に貢献することを目的としている。「OECDの三大目的」といわれる。

▼注4
OECD 情報セキュリティのためのガイドライン：1992年、情報システムセキュリティガイドライン『OECD Guidelines for the Security of Information Systems』に関する理事会による勧告、およびその付属文書として発表された。5年ごとに見直される。
https://www.ipa.go.jp/security/fy14/reports/oecd/oecd-security.pdf

▼ 注5
スニーカーネット:インターネットなどを含む通信ネットワークが、まだ普及・整備されていない時代に、スニーカー（スポーツシューズ）を履いた社員がUSBやMO（Magneto-Optical disk、光磁気ディスク）などを人的に運んでデータをやり取りする、仮想的なネットワークのこと。

図5　情報セキュリティにおけるCIA（機密性、完全性、可用性）



出所　岡村久道、「情報セキュリティと法制度」、http://www.fsa.go.jp/frtc/kenkyu/event/04.pdf

2　インターネットと「つながなければ安全」か？

江崎：システムをセーフティにするために、外部のネットワークとはつなぎませんというようなことを平気でおっしゃる企業がありますが。

佐々木：現実問題として、日本の産業がグローバルに生き残っていくためには、ネットワークにつながないという選択肢はないと思います。

江崎：「外部のネットワークとつなぐ危険性」よりも、ビルを掃除する人を含めて、ビルをメンテナンスする人たちが、比較的自由に出入りできてしまうことのほうが問題です。これでは、守りようがありません。こちらのセキュリティのほうが、よほど重要ではないかと思うのです。

一方で、コンピュータルーム（EDP室）への出入りは厳重なので、セキュリティを守りやすいところがありますよね。

名和：そうですね。私の担当したある交通関係の会社で、少し高齢な経営層の方ですが、セキュリティを守るために「インターネットをすべて遮断」して、ビジネスを展開されているという例もあります。

江崎：それは逆に、危ないじゃないですか。

名和：そのとおりで、危ないことが発生すると思います。しかし、その会社の（OT領域の）現場の創意工夫で、スニーカーネット（Sneakernet[注5]）という「人間を介したデータ流通ネットワーク」がつくられていまして、USBメモリや昔ながらのMO（光磁気ディスク）などを使用して、実際にデータがやり取りされていました。

現場では異常発生時に、システム稼働の安定確保のために、あらゆる手段で解決することになっているのですが、スニーカーネットを多用したデータの授受が、“まさに”行われていました。データそのものの安全性（真正性や完全性）が確保されず、人間のデータ誤用によって偶発的な事故が発生する懸念がありますので、これは驚きでした。

江崎：それはまさに、ぼろぼろの企業ですね。

名和：スニーカーネットのことは、IT部門の方には詳細に伝えられていないネットワークなのです。事業そのものに関与していないIT部門には伝える必要がない、と認識されて

いました。会社としてデータのやり取りについてコントロール、あるいはガバナンス（統制）する必要があるはずですが、OT 領域においては、USB メモリや MO は「機械設備の一部だ」という扱いで整理されているのです。

江崎：それらを見逃しているのでしょうか。

名和：いえ、そこは正直にいいますと、互いに専門やバックグラウンドが違うので言葉が通じない、つまり意思疎通ができないのです。設備技術者がいて、機械技術者がいて、通信技術者がいて、それぞれ独自に仕事している、という具合なのです。ですから、OT 領域においてはパソコンは1つの設備なので、パソコンという設備にソフトウェアやモジュールなどが載っている。それを設備と呼んで何が悪いのですか、ということなのです。

3 あなたこそ、IoT がわかっていない！

江崎：そもそも IoT をわかっていない人が多いということですね。

名和：いや、そうではありません。その逆です。彼らからすると、私（名和）のほうこそ、まったくわかっていない人だと言われています。

江崎：しかし、ビジネスモデルの話としてみると、彼らのロジックは、「ミニマムエフォートでシステムをつくって」「つなげなくてよくて」「利益をかせぐ」というパターンではないでしょうか。

名和：いや、そこは見方の問題だと思います。彼らは、2001 年にマイクロソフトが発表した Windows XP（Windows シリーズに属する OS の1つ）についても、その当時の技術者が、しっかり検証して、安定稼働することや継続運用できることを何重にも確認してから導入しているのです。

OT 領域の現場としては、安定稼働や継続運用が一番の優先課題ですから。

江崎：かなりのエクスキューズ（言い訳）ではないかと思うのですが。

名和：現場に行くとそれが当たり前です。現場は、命をかけてシステム（設備）を守り、安定稼働を最優先しています。まさに、「ジャパニーズクオリティ」（日本品質）としてのシステムなのです。

佐々木：実際に、マルウェア感染した状態であっても、設備を動かし続けることが最優先であれば、そちらを選択する場合もあると思います。問題なのは、そのような判断が、経営への影響とのトレードオフ（交換条件）をしたうえでのトップダウンではなく、隠ぺい体質のもとに現場で行われているということです。

江崎：それは、セキュリティリスクを全然考えてないということですよね。

名和：ええ。そういうリスクについて、状況認識ができていないというところは確かにあるかもしれません。怖さを知らないのです。現状では、そのような怖さを教えてくれるベンダも少ないですし、また行政機関や警察機関も「推奨事項」を中心にアドバイスするだけなのです。

4 経営層のセキュリティへの理解はどうか

名和：現場の担当者は、ネットワークにつなげないといけないことはわかっているのです。たしかに言い訳している場面はたくさんありますが、現場担当者はその両方の立場を

使い分け、場が変わると違ったほうの言い方（反対の言い方）をする立場でもあるのです。

受託側システムは、決められた業務委託契約の中では、契約した内容以上のことはしたくないのです。また、経営層が前述したような現場の気持を認識していないので、受託者（メーカーや保守事業者）はそのようなセキュリティリスクまで解決すべきことではないということになります。仮に私が現場の担当者に強く説得しても、彼らは権限もお金もないので、とる手段としては言い訳しか返ってこないと思います。

江崎：私の経験からも、現場の方々は話をすると理解はするのですが、それを実行しようとすると上司のほうからストップがかかる、というようなことはよく聞きます。

名和：それはいつものことです。ですから、現場の味方をすると、どうしても私が一緒になって言い訳をしないといけなくなるのです。

このような実状ですから、まずはセキュリティの怖さを知らない上層部（経営側）に理解していただく、というところポイントなのです。

江崎：佐々木さん、いかがですか。

佐々木：私も同じ状況だと思います。やはり経営側の認識、さらにその会社のガバナンスも含めて、上層部がきちんと理解していることが重要なのです。つまり、IT（情報システム担当）の人とOP（制御システム運用担当）の人は、基本的に利害は異なるわけです。

OPの人は現場でモノの生産を効率化することが仕事ですが、一方、ITの人はシステムの安定運用やセキュリティを確保することが仕事だからです。それをそのまま同じレベルでぶつけてしまうと、いつまでたっても解決しません。

そこで、上層部が、「自社のビジネス目標はこうであるから、例えばIoTに取り組むのであれば、セキュリティ対策をきちんとやりなさい」と、きちんとガバナンスを効かせ両者が折り合える方針を指示しないと、いつまでたっても両者の溝は埋まらないのです。

5 米国企業におけるセキュリティの認識具合

江崎：ところで、米国企業のセキュリティの認識は、いかがでしょうか。

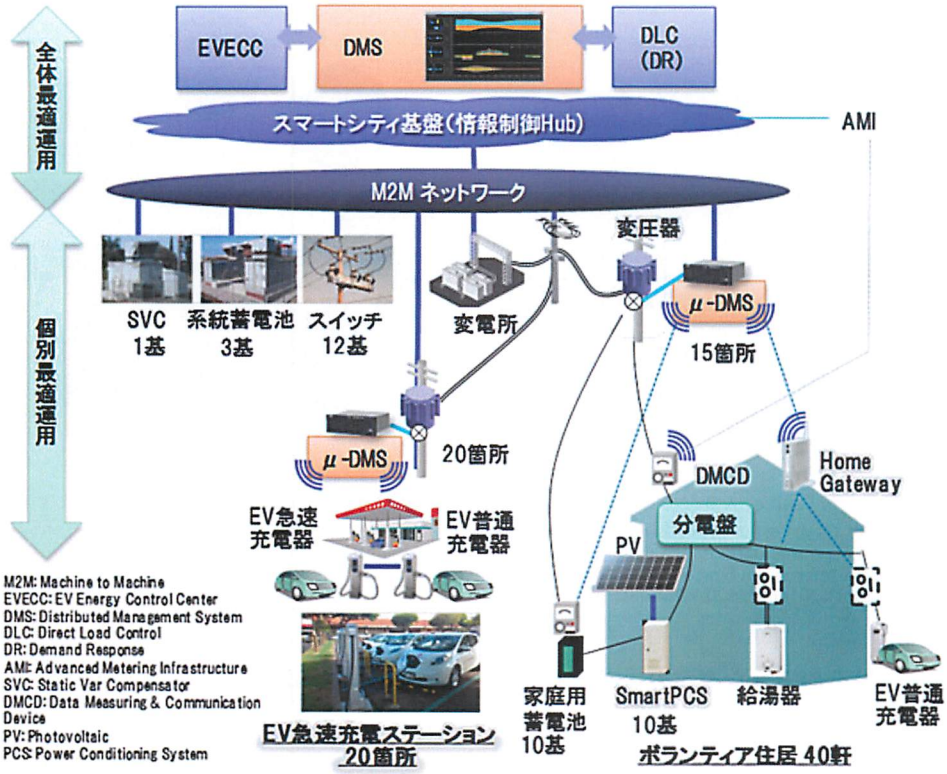
名和：私の実体験から申し上げますと、米国も、日本と同じような状況です。NEDO（新エネルギー・産業技術総合開発機構）の案件で、米国におけるスマートグリッド関連の実証事業をメキシコ州とハワイ州（図6）で行いました[注6]。この実証事業の関連で、数回にわたってさまざまな規模の電力会社やガス会社などの現場を訪問しましたが、一部においては日本よりもひどいセキュリティに対する意識が存在していることに、びっくりしました。

江崎：しかし、米国におけるIoTのセキュリティについては、DoD（国防総省）が、「IoTのための国防総省の政策提言[注7]」を2016年12月に発表するなど、頑張っていますよね

▼注6
①米国ニューメキシコ州における実証事業（事業期間：2009～2014年度）、http://www.nedo.go.jp/news/press/AA5_100277.html
②米国ハワイ州における実証事業（事業期間：2011～2015年度）、http://www.nedo.go.jp/news/press/AA5_100240.html
https://www.jstage.jst.go.jp/article/ieiej/34/8/34_541/_pdf

▼注7
Chief Information Officer U.S. Department of Defense「DoD Policy Recommendations for The Internet of Things (IoT)」、December 2016、http://DoDcio.defense.gov/Portals/0/Documents/Announcement/DoD%20Policy%20Recommendations%20for%20Internet%20of%20Things%20-%20White%20Paper.pdf?ver=2017-01-26-152811-440

図 6　米国ハワイ州マウイ島におけるスマートグリット事業のシステム構成図



出所　NEDO プレスリリース、「ハワイにおける日米スマートグリッド事業の実証サイトが始動」、2013 年 12 月 18 日、
http://www.nedo.go.jp/news/press/AA5_100240.html

（図7、図8、12ページ）。

名和：はい。当社（サイバーディフェンス研究所）は、他国政府の関係組織と連携してビジネスを展開しています。特に、国防関連の組織のミッションは国民を守ることですから、そのために必要なことに最大限取り組んでいます。現在は、エネルギー業界を守るための取り組みにシフトしています。

例えば、米軍の一部では、マイクログリッドのサイバーセキュリティに関する取り組みを強化するために、数年間にわたってSPIDERSプログラム[注8]に取り組んでいます。何かインシデントがあった場合には、軍が自らの力でエネルギー事業者を防御できる体制や準備が整いつつあります。

江崎：DoD 自身がセキュリティシステム自体を調達する、というようなことはやらないのですか。

名和：はい、やっています。DoDが電力会社と同じようなグリッドシステム（電力網）をつくって、軍が独自に運営し、そこでセキュリティのノウハウや運用技術について調査研究や実証を行っています。最終的に国のインフラを守るミッションをもっている軍が、自らの能力を向上させています。

江崎：DoDは、そもそもシステムに事故が起こらないようにする、ということまでもやっていますね。というのも、私はスマートグリッドについて米国NIST（National Institute of Standards and Technology、米国立標準技術研究所）が進めていたプロジェクト（パネル）の1つに参加して活動したことがあります。

NISTのパネル（SGIP[注9]）のなかにサイバーセキュリティグループがあって、ここが技術仕様をOKといわないと、NISTの資材調達リスト（COS[注10]）に載らないという仕組みがきちんとできています。

注8
SPIDERS：Smart Power Infrastructure Demonstration for Energy Reliability and Security、米国国防省（DoD）が推進している「エネルギーの信頼性と安全保障のためのスマートパワー・インフラストラクチャ・デモンストレーション」計画。一般の電力網の事故や攻撃という事態が発生した場合に、ミッションクリティカルな施設（例えば交通機関や金融機関等の社会的に重要なシステム）に電力を供給するために、マイクログリッドの導入が検討されている。

▼ 注9
SGIP：Smart Grid Interoperability Panel、スマートグリッド相互運用性パネル。SGIPの中に常設委員会としてSGCC（Smart Grid Cybersecurity Committee、スマートグリッド・サイバーセキュリティ委員会）がある。
http://www.sgip.org/committees-member-groups/

▼ 注10
CoS:Catalog of Standards（SGIP's SmartGrid Catalog of Standards）。スマートグリッドを構築するうえで必要と思われる規格を、NIST（関連組織はSGIP）が主導で選択し掲載したカタログのこと。
http://www.sgip.org/wp-content/uploads/SGIPs-Catalog-of-Standards-Complete-List-of-Entries_2017.pdf

図 7　DoD における他の研究分野と IoT のオーバーラップ（関連性）

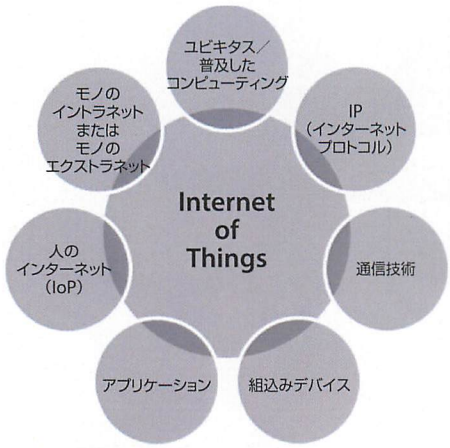
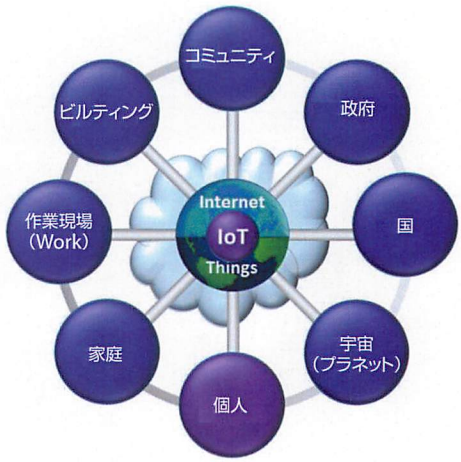


図 8　DoD における IoT アプリケーションの範囲



IoP：Internet of Peaple、人のインターネット。人をセンサーとして使う（人とデジタル技術をつなぐ）

出所　国防総省（DoD）の IoT に関する政策提言、2016 年 12 月、
DoD Policy Recommendations for The Internet of Things（IoT）, December 2016
http://dodcio.defense.gov/Portals/0/Documents/Announcement/DoD%20Policy%20Recommendations%20for%20Internet%20of%20Things%20-%20White%20Paper.pdf?ver=2017-01-26-152811-440

米国ではそのような調達の仕組みも含めて、企業などがサイバー攻撃を受けたときに、乗り込んで行って、助けてあげるというシステムをつくっていますね。

名和：その通りです。日本ではサイバー攻撃を受けてしまったら、被害組織やセキュリティ開発関連企業などに、その被害状況について官公庁から問い合わせが殺到します。

日本の場合は残念ながら、サイバー攻撃を受けた企業に対して国の組織や機関が主体的に「守る」仕組みを作ろうとする意思はもっていないようです。

佐々木：名和さんが米国の良い面を話されましたが、悪い面もあります。それは、セキュリティに関連する組織や機関が多過ぎるという問題です。例えば、DoD をはじめ、「DHS」（米国国土安全保障省[注11]）や、電力業界では民間団体「NERC」[注12]などもあります。

さらに州政府などにもセキュリティ部局があり、何かインシデント（サイバー攻撃）が起こったときに、各組織への報告義務があるため、サイバー攻撃を受けた企業や事業者などは書類の作成が多くなってしまい、それだけで疲弊してしまう面があります。

江崎：それは、制度疲労のようなものですね。

佐々木：そうです。制度ががっちりし過ぎているために、多くの関係組織や部署に、しかもそれぞれ異なるフォーマットでサイバー攻撃の報告をしなくてはならないので、現場の担当者には負担がかかり、困っています。ですから、日本がそのまま米国を真似るのはどうかな、と思います。

6　米国大統領令による ISAC（アイザック）の進展

江崎：そういう面から見ると、セキュリティに関して、日本の IT 業界はかなりうまく回っているといえますか。

名和：はい。狭い領域ではよく回っていると思います。米国では、通信をはじめ電力、金融、水道などの重要インフラに関連する各業

▼注 11
DHS：Department of Homeland Security、米国国土安全保障省。ハイジャックされた民間航空機がニューヨークの WTC（世界貿易センタービル）などに激突した同時多発テロ事件（2001 年 9 月 11 日に発生。死者は 3,025 人にものぼった）の後の 2013 年 1 月に発足した。

▼注 12
NERC：ナーク。North American Electric Reliability Corporation、北米電力信頼度協議会。北米の電力システムの信頼性向上のために作られた民間の団体。米国連邦エネルギー規制委員会（FERC：Federal Energy Regulatory Commission）から、北米唯一の電力信頼度機関（ERO：Electric Reliability Organization）として認定されている機関。電力インフラにおけるサイバーセキュリティ対策に関する重要な標準「CIP：Critical Infrastructure Protection」を策定し提供している。各電力事業者には順守が義務付けられ、違反した場合には罰則規定もある。

▼注 13
https://www.nisc.go.jp/inquiry/pdf/fy21-isac.pdf

▼注 14
ISAC：アイザック。Information Sharing and Analysis Center、重要インフラに関連する業界（分野）内でセキュリティに関する情報共有を行うための組織。分野ごとに固有の ISAC がある。米国で多く設立されているが、日本でも Telecom-ISAC Japan※1 や金融 ISAC が設立されている。
（※1）Telecom-ISAC Japan：2002 年 7 月に「インシデント情報共有・分析センター（Telecom-ISAC Japan）」として発足した非営利任意団体。2005 年 2 月に設立した「財団法人日本データ通信協会テレコム・アイザック推進会議」へ編入。表 3 参照。
https://www.telecom-isac.jp/public/soshiki.html

表 3　日本の各 ISAC と欧米の電力 ISAC（Information Sharing and Analysis Center）

名称	概要
〈金融 ISAC（日本）〉（Financials ISAC Japan）	2014 年に発足の一般社団法人。会員数は 200 社以上。主要銀行の非公式枠組みから発展。情報の共有と共通課題への対応策の検討の 2 つが活動の柱。米国の金融 ISAC（米国 FS-ISAC）とも連携（情報共有等）している。会員の位置づけ（正会員、準会員等）に応じた会費あり。
〈ICT-ISAC（日本）〉（ICT ISAC japan）	2016 年に発足の一般社団法人（従来の Telecom-ISAC Japan を発展的に継承）。会員数は約 30 社。国内主要通信事業者の自主的枠組みから発展。通信事業者に加え、放送事業者、ソフトウェアベンダが参加。当面は会員間の情報共有がメイン。会費あり。
〈電力 ISAC（日本：JE-ISAC）〉（Japan Electricity ISAC）	2017 年に発足。電気の安定供給に重要な役割を担う電気事業者間で、サイバーセキュリティに関する情報共有および分析を行う組織。会員数は約 30 社。総会で定める会費を毎年支払う（詳細は表 4 参照）。
〈米国電力 ISAC（E-ISAC）〉（Electricity ISAC）	2000 年に発足。北米電力信頼度協議会（NERC）に併設され、同協議会の会員がメンバーとなる。会員数 1,900 社以上。電力分野のサイバー攻撃情報の収集と分析、分析結果の発信が主な活動。NERC の予算で運営されており、会費なし。2015 年に ES-ISAC（Electricity Sector and ISAC）から E-ISAC に名称を変更。
〈欧州電力 ISAC（EE-ISAC）〉	2015 年に発足した自主的枠組み。会員数約 20 社。ベンダや研究機関も会員となる一方で、電力会社の参加は限定的となっている。欧州委員会の予算事業から発展。当面は会員間の情報共有がメイン。

出所　資源エネルギー庁、「電力分野におけるサイバーセキュリティ対策について」、平成 28（2016）年 7 月 1 日、
http://www.meti.go.jp/committee/sougouenergy/denryoku_gas/kihonseisaku/pdf/007_06_00.pdf

界内で、セキュリティに関する情報の共有を行うための組織として、米国の大統領令（1998 年）によって ISAC（アイザック。米国のセキュリティ情報共有組織）の設立が求められました。これを受けて米国では、例えば、通信や電力、金融、水道など、分野ごとに固有の多数の ISAC が設立されています[注13、注14]。

日本でも、すでにテレコム ISAC（Telecom-ISAC Japan、2016 年に ICT-ISAC に改組）や金融 ISAC（Financials ISAC Japan、2014 年設立）があります（表 3）。さらに電力自由化に対応し、電気事業者間のサイバーセキュリティに関する情報共有や分析を行う組織として、「電力 ISAC」（表 4）が 2017 年 3 月に設立されたばかりです。

図 9 に、電力 ISAC と他分野の ISAC と海外 ISAC の連携のイメージを、図 10（14 ページ）に、日本における電力 ISAC が果たす役割を示します。

ただし、このようなサイバーセキュリティに関する電力分野の ISAC、あるいは米国の ISAC などの内容には、技術だけでなく運用の話も含まれているため、共有すべき内容が多岐にわたっています。したがって、技術情報だけを共有している IT 業界などのサイバーセキュリティとは一線を画しています。

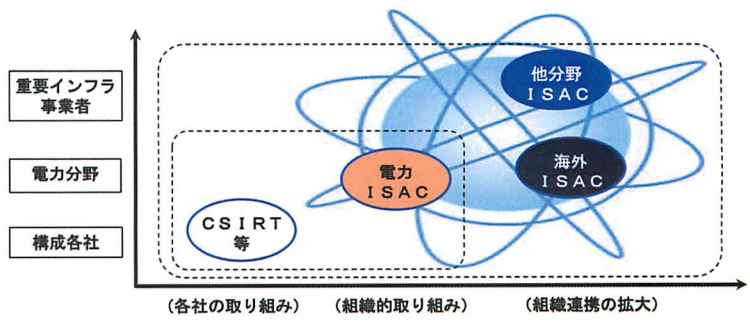
表 4　日本の「電力 ISAC」のプロフィール

項目	内容
組織名	電力 ISAC（アイザック）（Japan Electricity Information Sharing and Analysis Center、略称：JE-ISAC）
所在地	〒100-0004　東京都千代田区大手町 1 丁目 3 番 2 号
代表	代表理事：野村　武（中部電力株式会社　執行役員　情報システム部長）
設立日	2017 年 3 月 28 日
目的	電気の安定供給の役割を担う事業者間で、信頼と互助の精神に基づきサイバーセキュリティに関する情報等を交換や分析することによって、事故の未然防止、発生した事故に対する迅速な対応等を実現すること。
事業内容	サイバーセキュリティに関する情報の収集、収集した情報の内容を踏まえた情報の分析、収集・分析の結果の会員間での共有など。電力セプター※事務局。
活動内容	（1）課題検討 WG、（2）ベストプラクティス共有 WG、（3）セキュリティ教育 WG、（4）セキュリティ製品 WG、（5）セキュリティトレンド WG
正会員（50 音順）	扇島パワー、大阪ガス、沖縄電力、関西電力、九州電力、神戸製鋼所、コベルコパワー神戸、コベルコパワー真岡、JFE エンジニアリング、JFE スチール、JFE ホールディングス、四国電力、中国電力、中部電力、電源開発、東京ガス、東京ガスベイパワー、東京ガス横須賀パワー、東京電力パワーグリッド、東京電力フュエル＆パワー、東京電力ホールディングス、東北電力、日本原子力発電、日本原燃、北陸電力、北海道電力。計 26 社
特別会員	電力広域的運営推進機関

※セプター：CEPTOAR、Capability for Engineering of Protection, Technical Operation, Analysis and Response。金融や電力、通信等の重要インフラにおける IT 障害に対して、情報共有体制を強化するための情報共有・分析機能のこと。例えば金融セプター、電力セプターなどがある。

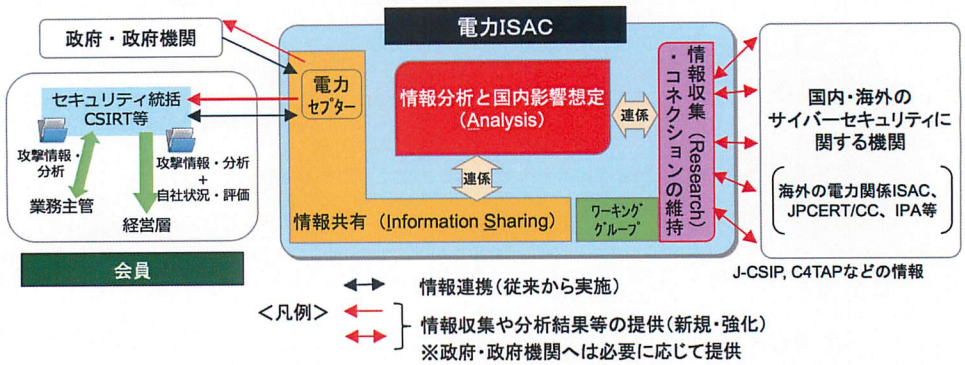
出所　https://www.je-isac.jp/news/2017/0328_01.html

図 9　電力 ISAC と他分野 ISAC および海外 ISAC の連携のイメージ



出所　「電力 ISAC の設立について」、平成 29（2017）年 7 月 7 日、電力 ISAC（JE-ISAC）、
http://www.meti.go.jp/committee/sougouenergy/denryoku_gas/denryoku_gas_kihon/pdf/004_07_02.pdf

図 10　日本における電力 ISAC が果たす役割



JPCERT/CC：Japan Computer Emergency Response Team / Coordination Center 、JPCERT コーディネーションセンター。インターネットを介して発生する侵入やサービス妨害等のインシデント について、日本国内のサイトに関する報告の受け付けや、対応の支援などを行う組織。特定の政府機関や企業からは独立した中立の組織
J-CSIP：ジェイシップ。IPA（情報処理推進機構）が運営している。Initiative for Cyber Security Information sharing Partnership of Japan、サイバーセキュリティ情報共有イニシアティブ
C4TAP：シータップ。Ceptoar Councils Capability for Cyber Targeted Attack Protection、セプターカウンシルにおける標的型攻撃に関する情報共有体制〔内閣官房情報セキュリティセンター（NISC）が事務局〕。セプターカウンシルとは各重要インフラ分野で整備されたセプター（例：電力分野、医療分野等）の代表で構成される協議会
電力セプター（事務局）：第 4 次行動計画に基づく、NISC・経産省と事業者間の情報連絡、連携の窓口
ISAC：アイザック。Information Sharing and Analysis Center、重要インフラ等の業界（分野）内でセキュリティに関する情報共有を行うための組織
CSIRT：シーサート。Computer Security Incident Response Team 、コンピュータ・セキュリティ・インシデント対応チーム。コンピュータやネットワークにおけるセキュリティ上のインシデント（事故 / 事象）に対応するために設置される専門チーム

出所　「電力 ISAC の設立について」、平成 29（2017）年 7 月 7 日、電力 ISAC（JE-ISAC）、
http://www.meti.go.jp/committee/sougouenergy/denryoku_gas/denryoku_gas_kihon/pdf/004_07_02.pdf

7　サイバーセキュリティに関して誰が責任をとるのか？

江崎：それでは、サイバーセキュリティに関して、政府などは責任を果たせないのではないですか。また、それを教育するのは誰の仕事になるのでしょうか。

名和：IT 部門のほうは、会社業務を効率化することがミッションですから、他社と連携する ISAC 的なことはしないのです。しかし、電力については安定供給というミッションがあります。つまり電力システム分野は、IT 部門とはプレイヤーが異なるため、教育するとなると、ビジネスセンスをもった責任ある人が教えることになります。

江崎：最終的には、誰が責任をとることになるのでしょう？

名和：インフラについては国家だと思います。

米国では、DHS（米国国土安全保障省）などの政府機関や公的機関が、インフラ事業者に対してサイバーセキュリティの運用上の直接的支援を段階的に始めています。そして、その組織および予算とも集約化の傾向にあります。つまり米国は、国家の意思としてインフラを守る姿勢を打ち出しており、国がその責任を担おうとしています。

しかし日本では、それぞれの省庁が独自の施策を進め、いまだに組織も予算も分散化しているため、他国に比べるとそれぞれの施策は小粒で、一部重複も見られます。

江崎：立場によって、いろいろな受け取り方がありますが、米国政府はサイバーセキュリティを理由にして、企業をコントロールしようとしているとは考えられませんか。

名和：たしかに、そういう面はあります。しかし、コントロールしないと国家としてのセキュリティは守れません。

江崎：サイバーセキュリティというのは、企業をコントロールする理由をつくりやすい面がありますが、そのような気配はありませ

んか。

名和：そのような気配は、上部機関においては感じるところもあります。ですから、国家は、多重人格者的な面を持ち合わせているように感じています。

佐々木：米国は、重要インフラ防護に関して、なるべく国家がコントロールしようとしている意図があるかと思いますが、現実問題として、規制だけで事業者のセキュリティレベルが十分になるわけではないので、民間の自主努力を促したりしています。

例えば、米国の電力会社は3,000社以上もあるので、ES-C2M2[注15]と呼ばれるセキュリティ成熟度を向上させるための自己診断ツールをDoE（米国エネルギー省）が策定して、事業者に提供しています。また、英国では、スマートメーターのプライバシーについての規制を除いて、電力システムのセキュリティ規制はなく、事業者に任せていますので、その国の文化や業界特性によるのかもしれません。

江崎：そのような状況で、国家を信用していいのでしょうか。

名和：あくまでも米国の話ですが、国家として国を守るためにサイバーセキュリティを

強化しているのですから、信用せざるを得ないという雰囲気です。国家レベルのサイバー攻撃に対して、一企業は無力に近いと認識している（米国の）経営者が多くなっています。

一企業の判断で独自で取り組みを進めて攻撃対処に失敗してしまった場合、その後は謝罪だけでは済まされない状況になってしまうと思います。この必然的に考えられる最悪の結果は、すでに十分予見可能となっています。

▼注15
ES-C2M2：Electricity Subsector Cybersecurity Capability Maturity Model、電力分野におけるサイバーセキュリティへの自己診断ツール。
https://www.ipa.go.jp/files/000053295.pdf

8 シーサート（CSIRT）とピーサート（PSIRT）の違い

江崎：国や政府レベルでほんとうに頑張っている国と、政府が機能していない国という話が出てきましたが、実際の現場の状況は、どこの国でもほぼ同じでしょうか。

名和：他国と比較すると、日本人のほうが、与えられた仕事以上のことを頑張ってくれるので非常に優秀だと思います。

IT部門の方は、サイバーセキュリティに関して、教育訓練のための予算や時間がほとんどないのに独学に近い形で勉強して、1年経って習得できるようになっている方も相当いらっしゃいます。

江崎：具体的には企業のどういう部門の人々ですか。

名和：具体的には、CSIRT（シーサート。Computer Security Incident Response Team、コンピュータ・セキュリティ・インシデント対応チーム）です。この部門の人々は、上層部から軽くいわれた程度なのに、いろいろと研究・勉強してできるようになったのです。これはすごいと思いませんか？　給料はまったく上がっていないのに、ですよ。

江崎：それはIoTのビジネスをしているところに、CSIRTが徐々に入っていって、うま

く回り出しているということですか？　また、現在の日本のレベルは小学生レベルぐらいにはなったということでしょうか。

名和：いや、すでに現場では中学生レベルくらいまで上がっています。実際に現場へ行くと、ある程度解決できるようになっていて、新たな見通しはついてきています。OTとITを結合したCSIRTも作られ、ほんとうに頑張って、解決しています。

江崎：企業の工場などで生産され、出荷される製品（セキュリティ製品ではない）のセキュリティ品質についての現状はどうでしょう？

名和：製品については、CSIRTとは別に、製品の脆弱性などを取り扱うピーサート（プロダクトサート。PSIRT：Product Security Incident Response Team）があります（表5）。PSIRTは、CSIRTとは別の取り組みをしていますので、両者を単純に比較することはできないと思います。

佐々木：CSIRTについては、一部の先進的な企業を除いて、箱だけはできてはいるが中身はまだこれからというところが多いかと思います。工場のCSIRTとなると、セキュリティの事故が起こったときに、ITとOT部門の連携を密にするための橋渡しをする必要がありますが、IT、OT両方がわかる人材が不足しているため、十分に機能するにはまだ時間がかかるという印象です。

PSIRTは、まだ設置している企業は大手に限られていますが、IoTの進展とともに広がっていくと思います。

江崎：PSIRTは、きちんと機能しているのでしょうか。

名和：表5の例1、2に示すように、パナソニック製品（例：家電製品やエアコンなど）で発見された脆弱性を解決する「Panasonic PSIRT」や、シスコシステムズの製品（例：ルータやスイッチなど）についての「Cisco PSIRT」があり、たいへん活躍しています。

パナソニックの場合は、品質管理の中にPSIRTがあります。また、横河電機グループでは、組織を横断したYOKOGAWA PSIRTを推進しています。

佐々木：IoT時代を迎え、インターネットに接続されるIoTデバイスの数が急速に増えてきています。このため、これまでセキュリティや脆弱性と関係が薄かった製品メーカーにも、サイバーセキュリティへの対応が厳しく求められるようになってきました。このような背景から、急速に各企業内においてPSIRTの設立や準備が進展し始めています。

江崎：エネルギーや電力系の企業の場合は、PSIRTのような組織はどちらかというと機能していないように見えますが。

名和：その分野については、先ほど話題になった電力ISACなどがスタートしていますので、その取り組みが期待されています。現状は、すでに機能している企業もありますが、機能していない企業も同じ数だけある、という認識です。

3年前であったら、全部だめという状況だったと思います。しかし現在は、対応できているところと、できていないところが混在していると見ています。

江崎：セキュリティの取り組みで先進的に活躍されているような部署は、会社からきちんと評価されているのですか。

名和：そこは会社の仕事としての位置づけですから、「特別な活動をしている」という評価

表5　シーサート（CSIRT）とピーサート（PSIRT）の違いとその例

項目		内容
CSIRT（シーサート）		Computer Security Incident Response Team
		コンピュータセキュリティに関するインシデント（サイバー攻撃などの出来事）に対処するための企業や行政機関等に設置される組織。インシデント関連情報、脆弱性情報等を常に収集、分析し、対応方針や手順の策定などの活動を行う。CSIRTを自社内に設置すると、他企業や他組織のCSIRTと連携しながらインシデントに効果的に対応できるようにする体制を構築できる。
PSIRT（ピーサート）		Product Security Incident Response Team
		自社で製造（あるいは販売）した製品にセキュリティの脆弱性が発見された場合に、その解決に対応する社内組織（チーム）。
	例1	パナソニックPSIRT（Panasonic PSIRT）
		パナソニック製品で発見された脆弱性を解決する組織。パナソニック製品に脆弱性が発見された場合、Panasonic PSIRTは開発部門と連携して報告された脆弱性の検証を行い、迅速に対応するチーム。
	例2	シスコPSIRT（Cisco PSIRT）
		シスコシステムズの製品とネットワークに関係するセキュリティ脆弱性情報の収集、調査、およびレポートの公開を管理する専門のグローバルチーム。

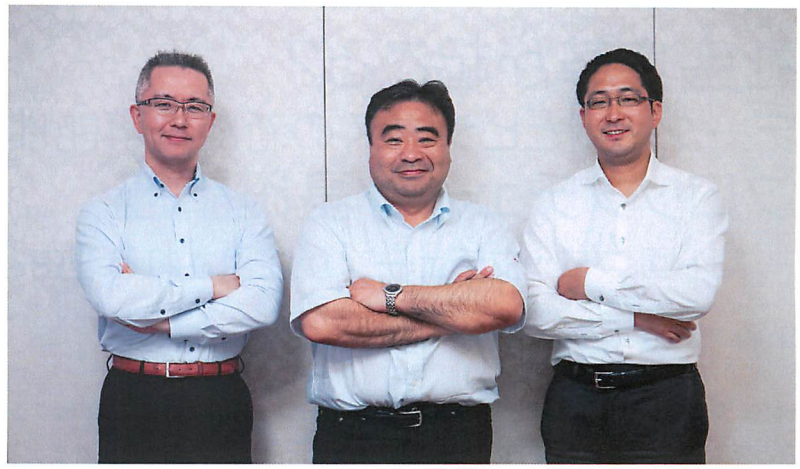
出所　各種資料をもとに編集部作成

はされていないと見ています。

江崎：そのような状況ですと、会社のなかで今後とも継続的に取り組んでいくための「ビジネスインセンティブ」（奨励金）というようなことが起こりにくいですよね。頑張ってきた人が、昇格して他部門に異動して現場を離れると、その取り組みが消失してしまうことになりませんか。

名和：そうですね。今わずかな人たちがリードして汗をかいて頑張って、それにみんな感化されて頑張っているのが現状だと思います。OTからITに歩み寄って一緒に頑張っているのですが、そのリーダーがいなくなると、もとに戻ってしまう危惧はあります。

佐々木：セキュリティの分野は、サイバー攻撃を受けるとその瞬間は話題になりますが、何も攻撃を受けない日常は、ただ粛々（しゅくしゅく）と地道にコツコツと取り組むことになります。ですから、誰かがそれをきちんと評価してあげないと、キーパーソンが会社を辞めてしまうケースもあります。



そこで、PSIRTやCSIRTなどの組織をきちんと位置付けて、経営層の理解はもとより、組織的に、持続的に対応する社内のチーム作りが重要となってきているように思います。

（後編に続く）

◎Profile（敬称略）

江崎 浩（えさき ひろし）
東京大学 情報理工学系研究科 教授

1987年 九州大学 工学部電子工学科 修士課程修了。同年4月に株式会社東芝に入社。1990年より2年間、米国ニュージャージー州ベルコア社、1994年より2年間、米国ニューヨーク市コロンビア大学にて客員研究員。
1994年 ラベルスイッチ技術のもととなるセルスイッチルータ技術をIETFに提案し、その後、セルスイッチルータの研究・開発・マーケティングに従事。1998年10月より東京大学 大型計算機センター 助教授、2001年4月より東京大学 情報理工学系研究科 助教授。2005年4月より現職。
WIDEプロジェクト代表。MPLS-JAPAN代表、IPv6普及・高度化推進協議会専務理事、JPNIC（日本ネットワークインフォメーションセンター）副理事長、ISOC（Internet Society）理事（Board of Trustee）。東大グリーンICTプロジェクト代表、日本データセンター協会 理事／運営委員会委員長。工学博士（東京大学）。

名和 利男（なわ としお）
株式会社サイバーディフェンス研究所 専務理事・上級分析官

海上自衛隊において、護衛艦のCOC（戦闘情報中枢）の業務に従事した後、航空自衛隊において、信務暗号・通信業務／在日米空軍との連絡調整業務／防空指揮システム等のセキュリティ担当（プログラム幹部）業務に従事。
その後、国内ベンチャー企業のセキュリティ担当兼教育本部マネージャ、JPCERTコーディネーションセンター早期警戒グループのリーダーを経て、サイバーディフェンス研究所に参加。専門分野であるインシデント・ハンドリングの経験と実績を生かして、CSIRT構築および、サイバー演習（机上演習、機能演習等）の国内第一人者として、支援サービスを提供。
最近では、サイバーインテリジェンスやアクティブディフェンスに関する活動を強化中。

佐々木 弘志（ささき ひろし）
マカフィー株式会社 サイバー戦略室シニア・セキュリティ・アドバイザー CISSP

PLC（Programmable Logic Controller）などの制御システム機器の開発者として14年間商品開発に従事した後、2012年マカフィー株式会社に入社。制御機器開発者としての知識を生かし、マカフィーにおける重要インフラおよびIoTセキュリティのエバンジェリストとして関連各社への啓発活動を行っている。また、2016年5月より、経済産業省 非常勤アドバイザー「情報セキュリティ対策専門官」として、経済産業省のサイバーセキュリティ政策への助言を行っている。
最近の主な活動は、内閣サイバーセキュリティセンター委託調査「EU諸国及び米国における情報共有体制」に関する調査において欧州現地ヒアリング調査実施（2016年）、独立行政法人 情報処理推進機構（IPA）産業サイバーセキュリティセンターのサイバー技術研究室リサーチフェロー、および事業者向けカリキュラムの講師担当（2017年）

12
2017
Vol.6 No.12

インプレス Smart Grid ニューズレター

エネルギーとIoTの融合時代を拓くスマートグリッド専門メディア

［創刊5周年記念特集］

［特集1］・・・04
IoT時代のサイバーセキュリティにどう対処すべきか―後編
カギとなるのは経営層の理解やガバナンス

impress
http://sgforum.impress.co.jp/sgnl/

【創刊5周年記念】特別座談会

IoT時代のサイバーセキュリティにどう対処すべきか《後編》

― カギとなるのは経営層の理解やガバナンス ―

インプレス SmartGrid ニューズレター編集部

前編（本誌2017年11月号）では、サイバー攻撃の脅威を前提とした対策が必要とされる、IoTの現場の状況を見ながら、経営層のセキュリティへの理解が重要であることや、セキュリティに関する情報共有組織「ISAC」（アイザック）の重要性、サイバーセキュリティの責任の所在などについて語っていただいた。

後編では、企業におけるCIO（最高情報責任者）とCISO（最高情報セキュリティ責任者）などの役割を整理しながら、米国のサイバーセキュリティの教育プログラムやIoT時代における経営層と現場の役割を語っていただいた。セキュリティの施策はトップダウンでなければ「部分最適」が発生してしまうこと、カギとなるのはやはり経営層の理解やガバナンスであること、セキュリティをコストと位置付けるのではなく、積極的なマインドチェンジによって、新ビジネスを拓くチャンス到来ととらえることが重要であるなど、本質に迫った議論が行われた。

【座談会出席者】＜司会＞東京大学 情報理工学系研究科 教授　江崎 浩（えさき ひろし）氏、
株式会社サイバーディフェンス研究所 専務理事・上級分析官　名和 利男（なわ としお）氏、
マカフィー株式会社 サイバー戦略室シニア・セキュリティ・アドバイザー CISSP　佐々木 弘志（ささき ひろし）氏

1 企業におけるCIOとCISOはアクセルとブレーキの関係

江崎：ここでは、企業における情報セキュリティ体制について考えていくことにしましょう。これは「情報セキュリティ・ガバナンス」ともいわれ、その企業における社内統制の体制を意味しています。図1に、最近発表された日立グループの情報セキュリティ・ガバナンスの例を示します。

一般に、企業の情報セキュリティ部門関係の責任者は、CIO、CSO、CISO（「シーゾー」あるいは「シソー」）などと呼ばれ、次のような役割を担っています。

（1）CIO：Chief Information Officer、最高情報責任者。組織全体の情報管理を行う。

（2）CSO：Chief Security Officer、最高セキュリティ責任者。組織全体のセキュリティ管理を行う。

（3）CISO：Chief Information Security Officer、最高情報セキュリティ責任者。情報システム部門とは別組織として情報セキュリティ全体を統括する。

これらは日本では、区別されていないケースが多く、1人の本部長あるいは役員が兼務しているケースも多くなっています。

名和：日本は不思議な国です。CSOは、情報セキュリティに物理セキュリティも含めた経営危機全般の管理を担当し、事業の継続性（BCP：Business Continuity Planning）

図1　日立グループの情報セキュリティ・ガバナンスの例（2017年）

出所　日立グループ「情報セキュリティ報告書2017」、2017年8月発行、http://www.hitachi.co.jp/csr/download/pdf/securityreport.pdf

が中心的な責任範囲となっています。

私の活動経験の限りで申し上げますと、CIOは情報システムをいかに活用して、営利活動、あるいはビジネスをいかに拡張するかというところに重きを置いています。これに対してCISOは、システムのリスク、あるいは脅威を見定めて、重点的に脅威に対する最適なリスクヘッジ（危険回避）をするというミッションをもっています。

双方は、CISOがブレーキでCIOがアクセルのような関係性になっていると、米国企業とのおつきあいの中で、このような表現の説明を受けることがありました。

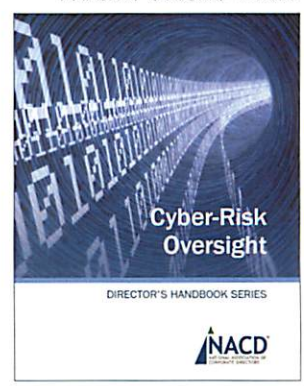
江崎：日本ではCIOとCISOを兼務していますが、ほとんどの場合、機能していないケースが多いですね。これは、会社組織でいうと、CEO（Chief Executive Officer、最高経営責任者）と監査役（取締役の業務執行を監査する人）が同じ人が兼務しているという感じです。このような現状を変えるには、その会社で生産しているプロダクト（製品）に対して「リスク管理ができていないと、会社の経営がめちゃくちゃになってしまう」というような話ができるCISOが必要なのです。

名和：そうです。CISOの担当者は名ばかりの会社が多いように感じます。

佐々木：CIOとCISOがアクセルとブレーキの関係だというのは、私も米国で聞きましたので一般的な考え方のようです。ときどき、CIOの下にCISOが設置されているケースを見かけますが、これでは、アクセル（CIO）のほうが勝ってしまいます。CIO、CISOが対等でお互いをけん制しあう関係の維持が重要だと思います。

▼注1
NACD：National Association of Corporate Director、全米取締役協会。米国では1970年代の後半に社外取締役が誕生したことに伴って、社外取締役の連携強化のため1977年にNACDが設立された。このNACDが中心となって、サイバーリスク評価指針（Directors' Handbook on Cyber-Risk Oversight）などを策定し2014年7月に発表している。2017年1月に、その最新の改訂版が発行されている。
https://www.nacdonline.org/Store/ProductDetail.cfm?ItemNumber=10687

図2　NACD発行のサイバーリスク評価指針（改訂版）の表紙



出所　https://www.nacdonline.org/Store/ProductDetail.cfm?ItemNumber=10687

2　米国のサイバーセキュリティの教育プログラム

江崎：米国には、そうした問題に関する経営者向けの教育プログラムなどがあるのでしょうか。

名和：あります。サイバーリスク評価指針（図2）などを策定している全米取締役協会（NACD[注1]）には、外部執行役員、あるいは執行役員を育成するプログラムがあります。

〔1〕ビジネス現場で必要なアクションアイテム

江崎：そのNACDの教育は、いわ

ゆるサイバーセキュリティの技術的な問題よりも、経営的な内容ですか。

名和：はい。経営目線の内容になっています。

江崎：なるほど。経営層向けの内容ですと技術的な内容に深く触れないので、前編（2017年11月号参照）でお話したような、「クローズド（つながっていない）だから安心」ということでビジネスをしていると、結局リスクが大きくなってしまうことや、そのリスクを避けるための契約の形態はどうするか、というようなことが問題になってきますね。

名和：そうですね。そういうアクションアイテム（Action Item、ビジネス現場で「すべきこと（一覧）」）を獲得する必要があると思います。今年（2017年）の10月に、スペインのバルセロナで開催された少しディープなセキュリティカンファレンスに出席しましたが、参加者は、捜査機関、セキュリティ専門家、欧米企業のCISO関係者でした。公開されていないサイバー攻撃の分析や評価に関する話がほとんどでしたが、実際に発生している事実を深く理解することで、徹底的な状況認識を共有することが目的の1つでした。

彼らとは年に3回ほど会うのですが、毎回、共有されるサイバー攻撃が深刻化している状況を肌で感じます。今、実際に何が起こっているかを整理・分析することによって、次にどのような脅威が発生するのかをディスカッションして、それぞれの場でアクションアイテムを作っていくのです。

一方、日本の企業からは、サイバー脅威はよくわからないので、すべきこと（アクションアイテム）を教えてくれといわれるのです。これは、まるで受け身の姿勢で学ぶ日本の義務教育の延長のような感じです。

〔2〕多くは名ばかりの日本のCISO

江崎：名和さん、佐々木さんのお二人の会社は、セキュリティ教育についてもビジネス領域としてお考えなのですか。

佐々木：私の会社（マカフィー）はそうです。まさにCISOの設置も含めてお手伝いをしています。実際、皆さんがおっしゃるとおりで、日本のCISOというのは多くは名ばかりであり、情報システム部長が昇格してCISOになっているケースが多いですね。

しかし、情報システム部長クラスですと、本当に企業に責任をもつ経営者の立場ではない。ですから、いくら提案してもセキュリティ自体が経営課題にならないのです。そこで、経営に責任をもつ常務取締役クラスあたりの人がCISOになってもらうことが重要なのです。

実際、海外の電力会社のCISOの方とお話していると、そのような人（CISO）の中には、自分の会社にとってどれだけリスクがあるかということを、的確に判断できるスキルの高い人も多くいます。

このようなブレーキをきちんと踏める人（すなわち、セキュリティの知識だけではなく、視野が広くバランス感覚に優れ、リスク管理ができる人）を育てるのが大事なのです。そういう人たちが会社にいれば、会社でCIOが提案したことを、CISOがそれを受けて、経営的にこのようなセキュリティ対策をする必要があると提案するわけです。結果として、会社としてセキュリティ対策にこれだけ投資すれば、これだけ儲かるよという話が経営会議でできるようになるのです。

3 IoT時代：経営層より現場のほうに可能性がある

〔1〕IoTで経営層は何をしたいのか?

江崎：それでは、IoT時代になって、経営層には具体的に何が求められているのでしょうか。

佐々木：今、日本の経営層の中にはIoT時代を迎えて、会社としてどのようなビジネスをするためにIoTを実現するのかが明確になっていないまま、現場に指示をする、というようなケースが多くなっています。結局、経営層がIoTで何をしたいのかが明確でないところが、現状での問題の根幹になっています。

ですから、その指示を受けて動いている現場の方々といくら話をしても、セキュリティの話にはなかなかならないのです。現場は一生懸命考えるのですが、(もちろん経営目線ではないので)技術指向のシーズ目線となっていて、こういう技術があるからこういうIoTができますよ、とまでは言うのですが、果たしてそれはビジネスとして儲かるのか、という疑問が出されると、そのまま止まってしまうことがよくあるのです。

江崎：そもそも経営層にお金を稼ぐというモデル自体がないところで、IoTをつくれと言われることになる。すると、ビジネスポートフォリオ[注2]をつくるところまでも、現場にふられてしまいます。

さらに、セキュリティ対策を行おうとすると、それは会社のBS(バランスシート：貸借対照表)の中では、通常はどのようなセキュリティ技術(ツール)を使っているかは書かれていないので、見えなくなってしまう。そのため、経営層は当然セキュリティに関するツールも知らない。このような現実を見ると、日本の場合は、リスクがどのように経営に対してインパクトを与えるかということを、経営層よりも現場の人たちが勉強したほうが早いのかもしれませんね。

〔2〕現場がサイバーセキュリティの知識を習得する

佐々木：そうですね。中間管理職(ミドル)の人が事業部レベルで頑張ったほうがよいのかもしれません。

江崎：結局、会社では事業部ごとに分散した採算性になっているため、その事業部が失敗すると責任を取らされる仕組みになっている。したがって、それに対抗するには、サイバーセキュリティの知識をきちんと現場の人がもっておいたほうがよいかもしれません。そういう意味では、日本の現場の人は優秀なので、勉強する気があれば、できそうな感じですね。

名和：多分できると思います。その理由は、現状では、経営層がサイバーセキュリティやOTのセキュリティを含めて、現場に丸投げしていますので、やや強制的にできてしまう環境にいるためです。

江崎：なるほど。そうすると、これは日本型と言ったら怒られるかもしれないけれども、まず経営層をきちんと教育するということが1つですが、その前に、かなり現場の賢い人たちの中から、そういうCISO的な発想がきちんとできる人を育てられそうな感じがしますが、いかがでしょうね。

〔3〕セキュリティのノウハウが継承できないという現実

名和：それは、現実には厳しいと思います。これまでは可能だったと思いますが、今は人がどんどん退職し、辞めていっている状況が目立ってきています。経験のある比較的年齢層が高い方はいらっしゃるのですが、若い方は躊躇なく離職したり、あとはキャリアを積むために他の部署に行ったりしているため、ノウハウが積み上がっていかなくなっています。

▼注2
取り組むIoT事業についての売上から利益、そして成長性などの一覧。

また、セキュリティに関する教育プログラムがないので、ノウハウを個人に代々伝えて引き継いで、他の人や部署には秘密になっているような「一子相伝」（いっしそうでん）的になっている傾向があります。

江崎：つまり、会社のローテーション（人事異動）上、異動してしまう場合があるため、セキュリティのノウハウがうまく伝達されない現象が起きていて、その部署にその財産が継承されていかないということですね。

名和：そうです。その傾向は、ここ数年特に顕著です。今年（2017年）になって強く感じていることは、フロント企業というか、ティア1[注3]の企業では、残業代を払わないといけない、給料を上げなければいけない、また長時間の残業をさせてはいけないなど、労務上の問題がクローズアップされていることです。

実は最近、IT業界では、ティア1の企業がティア2の企業に丸投げしている構図が、多くなっていますが、IoTも同じような傾向です。そのティア2の企業は超ブラック企業だったりします。そのような特定の企業（ティア2）にノウハウがたまっているのですが、その企業が倒産してしまうと、会社にノウハウが継承できないことになってしまう。今までは、ティア1の現場が強かったのですが、強い人間がティア2、さらにティア3へと流れてしまっているのです。

4 ボトムアップではなくトップダウンで「部分最適」を防ぐ

江崎：要は、丸投げしてしまっているが、その丸投げ先がどんどん変わってきているという現象が起こっているのですね。

名和：そうです。

江崎：それは、企業にとってかなり深刻な状況になってきていますね。

名和：ここ数年、特に顕著にそれを感じます。

佐々木：そのような背景から考えますと、セキュリティに関しては、ボトムアップではなかなか難しいというのが正直な感想です。いろんな事業部門がある会社で、それぞれの「現場が頑張ればいい」とよく言われるのですが、そうすると、全社的ではなく、「部分最適」が起こってしまうのです。

例えば、USBメモリの取り扱いの方法1つをとっても、社内のA部署とB部署でUSBメモリの取り扱い方が違う、ということが普通に起こってしまう。その部署が完全に独立していればいいのですが、何らかの形で各部署がみんなつながっているので、例えば、2017年5月に確認されたワナクライ（WannaCry[注4]）によるサイバー攻撃の場合、国際的にサーバへの大規模な攻撃を受けてしまい、その企業だけでなくグループ企業全体がウィルス（ワナクライ）に感染してしまったケースもありました。

このようなことが起こってしまうため、ボトムアップではなくトップダウンでないと、セキュリティに対応できない状態が発生しています。つまり、現在の日本の経営形態では対応しにくいところがあるため、いろいろな現場の方とお話していて、ここが一番苦労しているところなのです。

江崎：ということは、経営層の人は、先ほど話したように、CIOとCISOをきちんと区別して、セキュリティに関して、経営的視点からリスク管理も含めてきちんとしなさい、ということですね。

名和：そうです。多分、今の多くの経営層の方々は、ほとんどサラリーマンから上がっているので、セキュリティ対策を行う場合、具体的なコストや人手もかかるため、ミニマムのことしから行わない傾向があります。

江崎：ミニマムのことしかやっていないため、いざという時のリスク管理ができないという現象が起こりつつあるわけですね。

▼注3
ティア（Tier）：階層あるいは段階、あるいはランク付けを意味する。例えば、自動車産業の場合は、以下のような階層的なサプライチェーンとなっている。
・ティア1：第1次下請け業者（直接自動車メーカーに納入する企業）
・ティア2：ティア1の下請け業者
・ティア3：ティア2の下請け業者

▼注4
ワナクライ（WannaCry）：ワナクリプター（WannaCryptor）あるいはワナクリプト（WannaCrypt）とも呼ばれる。2017年5月に、全世界の企業や組織を攻撃したマルウェア（ウィルス）の一種。データをウィルスで暗号化して（人質にして）読めないように改ざんし、身代金を要求するランサムウェア（Ransomware）の一種。自己増殖するため、社内ネットワークに接続された各端末へ次々に感染が拡大した。
ランサムウェアとは「Ransom」（身代金）と「Software」（ソフトウェア）を組み合わせた造語で、身代金要求型ウィルスとも言われる。感染した端末内に保存されたデータをウィルスで暗号化して読めないように改ざんし（「人質」にして）、その暗号化したデータ（人質）を復号するために、脅迫文書（例：お金を払えば復号するという文書）を送り金銭を要求する攻撃方法。

5 電気・ガスのエネルギー自由化時代のセキュリティ

〔1〕自由化によるコストダウン体質で低下するセキュリティレベル

江崎：ところで、去年（2016年4月：電力自由化）と今年（2017年4月：ガス自由化）と続けて、電気・ガスなどのエネルギー市場自由化時代を迎えて、例えば具体的に電力網（グリッド）に関係するスマートグリッドやVPP（Virtual Power Plant、仮想発電所）などに関するセキュリティはどのように対応されているのでしょうか。

名和：エネルギーの小売完全自由化が始まり、エネルギー関連の大手企業ほどコスト意識が非常に高くなりました。また、エネルギー業界の統廃合[注5]も進んでいます。

このため、IT化を図りコストを切り詰めて、競争力を高めていこうとしています。そうすると、3年後の2020年まで、急激に変わっていくと見ています。さらに日本においては、2020年から送配電部門の中立性を一層確保する観点から法的分離による送配電分離が行われますので、セキュリティ対策に関する投資捻出へのモチベーションが低下していくのではないかと危惧しています。

江崎：今後、エネルギー業界は頑張っていくけれども、企業の統合化が進み、市場での競合が激しくなるため、コスト面から、セキュリティ分野にあまり人も金も投入できなくなる、ということですね。

名和：一番怖いのは、サイバー攻撃の脅威を知らない企業のリーダーがそれを進めていることです。多くの企業のリーダーは、経験上、10年前あるいは20年前の低いセキュリティレベルあるいは低い脅威（サイバー攻撃）のレベルしか、認識（あるいは体験）されていません。ですから、現在の、以前とは比べられないほど高いサイバー攻撃のレベルを理解しにくいのです。このような背景から、そのような企業ででき上がったセキュリティ対策は、未来のサイバー攻撃に対して、脆弱なものなっていくと予想されます。

江崎：佐々木さんいかがですか。

佐々木：まったく同じ意見です。今の電力・ガスなどのエネルギー業界は、自由化を背景に、各社が厳しいコストダウンを求められています。IoT（つなぐこと）を活用して、これまでよりはエネルギーをユーザーに安く提供するようになりますが、まだ発展途上ですからセキュリティレベルは下がる傾向にあると思います。

ただ、それに気づいて何とかしようとしている電力会社もありますが、そのような意識がない会社もあります。一方、電力ISAC（「前編」参照）のような動きや、ITとOTの融合をさせるようなことも認識されるようになってきており、業界でも取り組みが始まっています。

ただし、業界全体でセキュリティに関する情報共有に取り組もうとすると、今までデータを出すことにクローズだった人たちは、なかなかデータを出したがらない。これをどうやって説得し解決するかという点は、電力分

▼注5
例えば、2017年4月1日、JXホールディングスと東燃ゼネラル石油が経営統合し、JXTGホールディングスという新会社を発足させた。

野に限らず、どの業界でも課題になっています。また、これは日本だけではなくて、世界中で同じ課題となっています。

江崎：私も、政府の委員として電力のセキュリティ対策をつくるときはいろいろ取り組みましたが、最初はそもそも情報共有したくないというところから始まって、かなり抵抗されました。

名和：まさにその通りです。

〔2〕民間のセキュリティシステム向上のための業界基準

江崎：かなり抵抗が強く難しい面がありましたが、政府の審議会などで審議の結果、例えば、経産省の報告書などには、サイバーセキュリティの重要性が書かれるようになってきました。しかし、書いてもらったことを実際にできるかどうかということが勝負なのです。そこで、とりあえず民間ではどうすればよいのでしょうか。

名和：民間では権限がないので厳しいと思います。先日も早朝に、北朝鮮のミサイルに対処するために、各政府機関の局長が緊急参集チームということ召集されましたが、局長が参加する理由は、局長が法的な権限をもっているからです。各種法律について、最高レベルの権限をもつのは大臣ではなく局長クラスなのです。民間にはそういう権限が十分に与えられていないのです。

江崎：しかし、インシデントの際の実際のオペレーション（対応）は、民間の仕事になるため、政府の動き以前に民間がシステムのレベルを上げておく必要がありますね。これは、前編の最初の話に近づくわけです。つまりインシデントが起こったときに、助けてくれるのは、国の仕事になるのかもしれないけれども、それ以前に、民間のクオリティを上げておかなければいけないわけですよね。

名和：そうです。しかし、クオリティを上げるのは企業の経営層にとってコストになりますので、やはりレギュレーション（規制）をつくる公的機関や業界団体がないと、ちょっと対応が厳しいと思います。

江崎：業界の皆さんが守れるような基準などを、まず業界がつくるのが一番健全なような気がしますが。

名和：はい。商慣習（日常的な商取引の過程で形成されている慣習）に入れ込むのが一番いいのではないかと思います。

江崎：商慣習に入れ込むというのは、具体的にはどのような例がありますか。

名和：成功事例としては、国際標準としてのISMS（情報セキュリティマネジメント システム。ISO/IEC27001：2013）や国内標準としてのPマーク（Privacy Mark。プライバシーマーク）などが、多くの賛同を得て作成されました（表1）。

表1　国際標準のISMSと国内標準のPマーク

項目	ISMS	Pマーク
英語	Information Security Management System	Privacy Mark
日本語	情報セキュリティマネジメントシステム	Pマーク
標準規格	国際標準規格 ISO/IEC27001：2013 （日本語翻訳版：日本工業規格 JISQ27001：2014）	日本工業規格 JISQ15001：2006 （日本国内のみの適用）
目的	情報をCIA〔機密性、完全性、可用性〕の視点から、トータルに規定する国際規格 （Pマークより保護対象が広い）	個人情報取り扱いに関する認定制度。JIPDECが管理

JIPDEC：ジップデック。Japan Institute for Promotion of Digital Economy and Community、一般財団法人日本情報経済社会推進協会
CIA：Confidentiality（機密性）、Integrity（完全性）、Availability（可用性）
ISMS：Information Security Management System、情報セキュリティ管理システム。企業や組織が情報を管理し、機密を守るため管理システム。ITシステムのセキュリティ対策をはじめ、情報を扱う場合のセキュリティポリシー（方針）を含めた総合的なリスク管理体系のこと。国際標準規格ISO/IEC27001：2013、日本工業規格 JISQ27001：2014などで標準化されている。
Pマーク：Privacy Mark、プライバシーマーク
出所　各種資料より編集部作成

これによって、日本もセキュリティレベルがだいぶ上がっています。例えば、現在、日本は、世界におけるISMS認証取得事業者数の3分の1以上の企業が取得するなど、すごい数になっています。これらは経産省の管轄（商慣習）ですが、同じようにセキュリティ対策も商慣習として、日本でも入れ込むことができるような気がします。

6 なぜ、日本でPマークがうまくいったか

江崎：Pマーク（図3）がなぜうまくいったかというと、その仕様づくりを政府だけではなく、民間と政府の中間のところで基準をつくったからです。しかも、法律（守らないといけないというもの）ではなく、この基準でつくるとPマークを付けられますよ、というインセンティブで関心を集め、導入しやすくしたのです。

名和：政府の調達仕様書の項目に入った（加えられた）ということですね。

江崎：そうです。そういうことが、効果があるのです。そこが一番大切ではないかと思うのです。ですから私も、政府の委員会で話す時は、サイバーセキュリティは大事なのでPマークを位置づけた調達仕様書にしたほうがよいと、進言しているのです。それが米国の場合、私の認識では、GAO（会計検査院）とGSA（米国連邦政府調達庁）とNIST（米国国立標準技術研究所）の関係[注6]がうまくいっているので、そのように進むとよいと思っています。

名和：私も、そうだと思います。

江崎：CISOが、会社全体のリスク管理の視点から、自分の会社の発注形式を統一してくれればよいのです。特に大きな会社の場合、部門ごとに違うのではなく、調達仕様の面倒をみる監査機関があって、サイバーセキュリティに関するチェックをすべて行うようなガバナンスが欲しいですね。そうするとアウトソースもしやすくなる。

佐々木：その通りです。

江崎：なぜかというと、アウトソースはとても重要だからです。つまり企業の内部だけでやると、CISOというのは、会社の利益が短期間に上がるほうに引きずられてしまうので、できればサードパーティや中立性（ニュートラリティ）の高いところにアウトソースしたほうがよいと思います。

▼注6
GAO：Government Accountability Office、会計検査院
GSA：General Services Administration、米国連邦政府調達局
NIST:National Institute of Standards and Technology、米国国立標準技術研究所

図3　プライバシーマーク（Pマーク、中央※1）とそのデザイン・コンセプト

※1　プライバシーマーク制度：企業や団体など（事業者）の個人情報保護の体制や運用の状況が適切であることを、消費者に上図のような"プライバシーマーク"（Pマーク）というロゴマークを用いてわかりやすく示す制度。1998年から日本情報経済社会推進協会（JIPDEC）が運営している。プライバシーマークの使用が認められた事業者はプライバシーマーク付与事業者（2017年11月現在、約1万5,000社※）と呼ばれ、「個人情報」を大切に取り扱う事業者として、ホームページや名刺、ポスターなどにプライバシーマークを使用している。

※ https://robins.jipdec.or.jp/robins/reference_ImportSearchAction.do

出所　https://privacymark.jp/wakaru/about.html

そうすると、今後、そのような視点からサイバーセキュリティ関連のビジネスやサービスを展開するのは、結構よいビジネスになるのではないでしょうか。今後、産業構造も大きく変化しますし、リスクはますます増える方向にあります。例えば会社を買収する場合にも、そのリスクをどう減らすか、というようなことが増えてくるのではないでしょうか。

名和：その際、今後、リスクが増えていくということを、その会社のすべての関係者に認識していただかないと、私などがコンサルタントとして訪問したときに「またあの人が来て、言っている」と、迷惑そうに言われてしまうのです。

佐々木：私もよく言われますね。「あの人、また来た」というように見られています。

江崎：お話を聞いていると日本の会社では、全般的に、セキュリティに限らず、リスク管理というのはあまり熱心にやっていないようですね。

名和：やっていませんね。

江崎：サイバー攻撃関連以外にも、会社の中には、セキュリティに関連することがいっぱいありますが、会社として、そこもあまり管理できていない。そこをきちんとしていくことも重要ですね。

7 困った問題：人事配置のローテーションが早過ぎる

江崎：そういう意味でいうと、日本のセキュリティを、海外の例を参考にしながらどう着地させていくかをきちんと考えなければいけませんが、幸い日本の本格的な取り組みはこれからなので、逆に取り組みやすいかもしれませんね。しかし、日本の企業においても、国（政府）においても人事配置のローテーションが早過ぎるのは困った問題です。セキュリティに関するエキスパートが育っていないこと、担当者の業務経験のノウハウがドキュメント（文書）化されていないことも問題です。

佐々木：はい。それもこれもすべて日本の企業の場合は、経営層の理解がなく、セキュリティ担当者の社内の地位が低いためです。セキュリティの部署に配属されてそこで活躍しても、すぐ他の部署に異動になってしまう。これは、企業だけでなくて日本の政府内でも普通に起こっています。政府の場合、各省では2年おきくらいのローテーションで人事異動が通例となっていますね。理解ある人が異動してしまい、また新しくセキュリティを知らない人が配属される、というようなことを繰り返しているのです。海外の方に、この話をするとびっくりされます。

8 カギとなるのはやはり経営層の理解やガバナンス

〔1〕日本で情報共有が進まない理由

江崎：サイバー攻撃に対処するには、企業間の「情報提供と情報共有」が重要なカギになってくるということですね。

佐々木：その場合、情報共有は確かに大事なのですが、これは順番でいうと最初ではなく最後のほうかなと思っています。その理由は、まず経営層の理解やその会社の体制（ガバナンス）が重要だからです。与えられた情報（情報共有）を生かす仕組みがないと、結

局、「会社の経営にまで影響があるかもしれない脅威の情報をもらいました」「こういう事件がありますよ」と報告しても、それを社内で展開することもできず、結局、会社で使えないのです。

日本で情報共有があまり進まない理由の1つに、そもそもそれを大事なこととして扱う体制や、それを価値がある情報と思える人がまだまだ少ないということがあります。

ISAC[注7]については海外などで話を聞いていても、失敗するところと成功するところがはっきりしています。失敗するところは、そこにいる人たちの業界自体もそこまで重要視されていないのです。

例えばオランダには水のISACなどがあるのですが、あまりうまくいっていないと聞きます。なぜかというと、彼らの中でそこまで意識が高くない人たちが集まって一生懸命情報共有しても、何を共有していいかわからないし、もらった情報の利用方法もわからない。結局、そこにいる人たちのレベルが上がらないから、ISACによる本格的な情報共有も進まないのです。

江崎：そうすると、その情報共有にしても、1つには経験則的に言うと、多分あまり急に立ち上げ過ぎてもよろしくないということですね。

佐々木：そうです。だから成功しているISACの話を聞くと、結局最初はワークショップなどで、みんなで学びながら仲よくなっていくという過程をとる。その過程でみんながレベルアップし、互いに理解を深められるので、ちょっと機微な情報なども交換しやすくなる。だからISACの成長とともにその人たちも成長できるのです。頻繁に担当者が代わったらだめなのです。

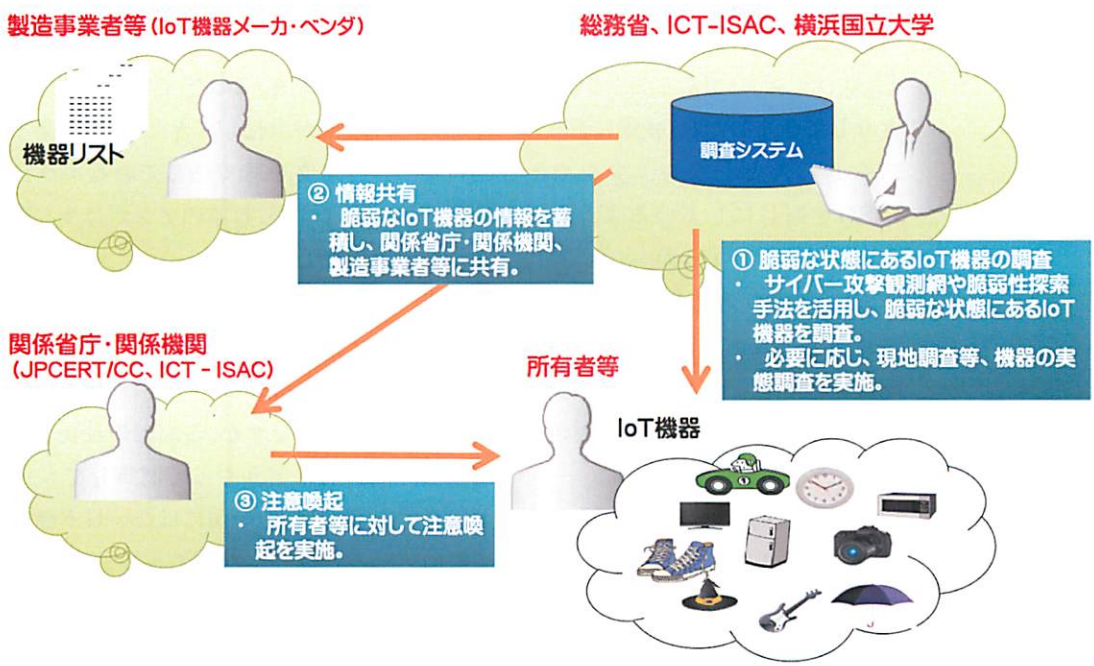
江崎：ISACでうまくいっているところは、最初にISACを立ち上げたコアのメンバーが頑張っています。業界のコアの人たちがほんとうに情報共有して、コアの部分を残しながら少しずつ共有部分を増やしていっています。

〔2〕日本のテレコムISACと米国の成功例

名和：そのようなことに留意して、うまく運営している典型が、日本の場合、テレコム

▼注7
ISAC：アイザック。Information Sharing and Analysis Center、重要インフラに関連する業界（分野）内でセキュリティに関する情報共有を行うための組織。分野ごとに固有のISACがある。米国で多く設立されているが、日本でもTelecom-ISAC Japanや金融ISACが設立されている。

図4　テレコムISACにおける脆弱なIoT機器の調査および注意喚起のイメージ



出所　http://www.soumu.go.jp/menu_news/s-news/02ryutsu03_04000088.html、http://www.soumu.go.jp/main_content/000505558.pdf

ISAC（Telecom-ISAC Japan、2016年に一般社団法人ICT-ISACに改組、「前編」参照）です。

最近、日本では、政府のサイバーセキュリティ戦略本部が、2020年およびそれ以降のサイバーセキュリティの在り方について、「サイバーセキュリティ戦略中間レビュー」を発表しました（2017年7月13日）[注8]。ここでは、今後、サイバー空間を構成するネットワークやコンピュータなどの高性能化に加え、IoT、人工知能（AI）、ブロックチェーン（分散型台帳技術）などの新しい技術革新にも適切に対応していく必要がある、という先進的な方針を出しています。

このような動きと同期して、テレコムISACは、図4（13ページ）に示すように、総務省、横浜国立大学などと連携して、重要IoT機器を中心にIoT機器の実態調査を予定しています。脆弱なIoT機器を特定した場合には、その所有者などに対して注意を喚起する方針となっています。

江崎：米国の場合はいかがですか？

名和：米国でもそのような問題意識があって、防衛領域におけるISACに相当するものとして、DoD DIB（Defense Industrial Base、国防総省 防衛産業基盤）のサイバーセキュリティ／情報保証プログラム、およびその運用管理部門としてのDC3（DoD Cyber Crime Center、国防総省サイバー犯罪センター）という組織があります。

ここでは、新しい取り組みとして数年前から、各組織の共有情報を収集し、それを分析して還元するということを行っています。アナリスト（A：Analyst）という言葉を使って、AtoAミーティングというミーティングが適時行われ、情報共有が行われています。

このミッションはISACと多少違うのですが、これが米国でうまく行われている事例です。

9 セキュリティはコストでなく新ビジネスへのチャンス

江崎：これまでのお話から、サイバー攻撃に対して、本質的に問題を解決するのは企業統治（ガバナンス）であることが、ますますはっきりしてきましたね。極端に言うとガバナンスをきちんとしない、少なくともCIOとCISOを同じにしているような会社は落第ということでしょうか。

名和：いきなり落第と言われるときつすぎますね。「きちんと現実を見て、CIOとCISOの配置を考慮しないような会社は……」というくらいにしてもいいのではないかと思います。

江崎：そういうことをやっておかないと、企業的にも生き残れないということは、国際的な流れで見ると理解され始めています。現在、CIOが強くなって、ITを使わない会社は生き残れないというのは、ほとんどの企業で理解されるようになっています。

その一方で、最近、リスク管理（CISO）の分野でも、これまで経験していないサイバー攻撃が激化してきたため、企業でも具体的なリスクを肌で感じているようになってきていますが、日本のテンポは少し遅いということでしょうか。

名和：そうですね。しかし、その痛みを感じて知っている比較的若くてIT出身の社長さんは、理解してサイバー攻撃の対策を始めているのですが、ご高齢の社長さんのなどの経営層にどうやって認識してもらうかという課題は、他の国にはない日本独特のチャレンジな課題になっています。

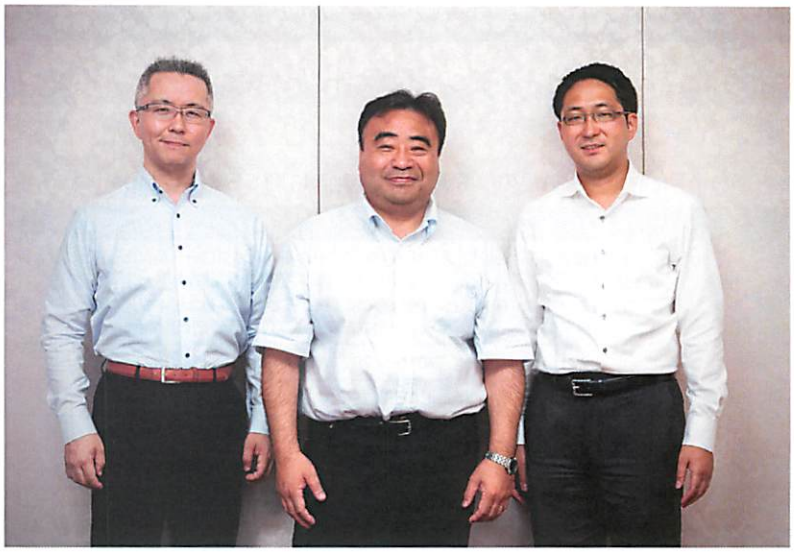
佐々木：セキュリティに関して言えば、セキュリティを単なる自分の会社を守るためのコストととらえていては、いつまでやって

▼注8
http://www.nisc.go.jp/active/kihon/pdf/csway2017.pdf

も理解が広がらない。セキュリティを、IoTを実現するために必要な投資と位置付け、これだけ投資したらこれだけ安全に利益が得られる、あるいは新しいセキュリティ・ビジネスも拓けるというように、積極的な方向にマインドチェンジをして欲しいということが、今、一番伝えたいことです。

江崎：長時間にわたり、サイバーセキュリティについて、国内外の両面からホットなお話をありがとうございました。これまで、セキュリティ対策の課題は、とかく「コストがかかる」という消極的な受け止め方がされがちでした。しかし、IoT時代を迎えて、セキュリティを、新しいビジネスを拓く投資対象として、さらにビジネスを広げるチャレンジングなテーマという積極的な視点からとらえ直すことが重要であることもわかってきました。

事実、16ページの「コラム」に示すように、IoTセキュリティ製品の市場は、2016年の500億円台から2021年には1,000億円超（1,250億円）の規模へと急速に市場を拡大すると予測されています。



今回の座談会が、読者の皆さんの新ビジネスの創造に向けて、参考としていただけるよう期待しています。

◎Profile（敬称略）

江崎 浩（えさき ひろし）
東京大学 情報理工学系研究科 教授

1987年 九州大学 工学部電子工学科 修士課程修了。同年４月に株式会社東芝に入社。1990年より２年間、米国ニュージャージー州ベルコア社、1994年より２年間、米国ニューヨーク市コロンビア大学にて客員研究員。
1994年 ラベルスイッチ技術のもととなるセルスイッチルータ技術をIETFに提案し、その後、セルスイッチルータの研究・開発・マーケティングに従事。1998年10月より東京大学 大型計算機センター 助教授、2001年４月より東京大学 情報理工学系研究科 助教授。2005年４月より現職。
WIDEプロジェクト代表。MPLS-JAPAN代表、IPv6普及・高度化推進協議会専務理事、JPNIC（日本ネットワークインフォメーションセンター）副理事長、ISOC（Internet Society）理事（Board of Trustee）。東大グリーンICTプロジェクト代表、日本データセンター協会 理事／運営委員会委員長。工学博士（東京大学）。

名和 利男（なわ としお）
株式会社サイバーディフェンス研究所 専務理事・上級分析官

海上自衛隊において、護衛艦のCOC（戦闘情報中枢）の業務に従事した後、航空自衛隊において、信務暗号・通信業務／在日米空軍との連絡調整業務／防空指揮システム等のセキュリティ担当（プログラム幹部）業務に従事。
その後、国内ベンチャー企業のセキュリティ担当兼教育本部マネージャ、JPCERTコーディネーションセンター早期警戒グループのリーダーを経て、サイバーディフェンス研究所に参加。専門分野であるインシデント・ハンドリングの経験と実績を生かして、CSIRT構築および、サイバー演習（机上演習、機能演習等）の国内第一人者として、支援サービスを提供。
最近では、サイバーインテリジェンスやアクティブディフェンスに関する活動を強化中。

佐々木 弘志（ささき ひろし）
マカフィー株式会社 サイバー戦略室シニア・セキュリティ・アドバイザー CISSP

PLC（Programmable Logic Controller）などの制御システム機器の開発者として14年間商品開発に従事した後、2012年マカフィー株式会社に入社。制御機器開発者としての知識を生かし、マカフィーにおける重要インフラおよびIoTセキュリティのエバンジェリストとして関連各社への啓発活動を行っている。また、2016年５月より、経済産業省 非常勤アドバイザー「情報セキュリティ対策専門官」として、経済産業省のサイバーセキュリティ政策への助言を行っている。
最近の主な活動は、内閣サイバーセキュリティセンター委託調査「EU諸国及び米国における情報共有体制」に関する調査において欧州現地ヒアリング調査実施（2016年）、独立行政法人 情報処理推進機構（IPA）産業サイバーセキュリティセンターのサイバー技術研究室リサーチフェロー、および事業者向けカリキュラムの講師担当（2017年）

Column

国内IoTセキュリティ製品市場が急拡大：500億円から1,000億円超の規模へ

表　国内IoTセキュリティ製品の市場予測（2017年11月6日、IDC Japan調査）

項目		内容		
IoTの定義（IDC）		(1) IP接続による通信を、人の介在なしにローカルまたはグローバルに行うことができる識別可能なエッジデバイス（IoTデバイス）で構成されたネットワークであり、 (2) 法人／政府／個人などのさまざまなユーザーが利用するユビキタスなネットワーク環境に対して、管理／監視／分析などの多様な付加価値を提供するもの。		
市場年		2016年	2016～2021年	2021年
市場規模		518億円	CAGR：19.3%	1,250億円（2016年の2.4倍）
	ハードウェア	144億円	CAGR：15.1%	291億円（2016年の2.0倍）
	ソフトウェア	374億円	CAGR：20.7%	960億円（2016年の2.6倍）
製品セグメントの内容		(1) ハードウェア製品：物理的なセキュリティ機器やセンサー／モジュールやサーバ、ストレージなどに組み込まれているセキュリティハードウェアモジュールなどが含まれる。 (2) ソフトウェア製品：IoTソリューションとネットワークのセキュリティ対策に向けたソフトである。分析ソフトウェアやアプリケーションソフト、そしてIoT向けプラットフォームなどが含まれるセキュリティソフトである（既存のセキュリティソフトも含まれる）。		
今後の市場展開	ハードウェア	(1) 現状：製造機械の稼働状況の把握や遠隔制御などを目的としたユースケースが多くを占めており、製造工場内ネットワークや遠隔制御用ネットワークなどに対するネットワークセキュリティ機器の導入が先行している。 (2) 今後：信頼性や耐久性を備え、かつ多様な機能をもったセンサー／モジュールに組み込まれたセキュリティハードウェアモジュールの導入が進む。		
	ソフトウェア	(1) あらゆる産業（次の例に示す）のさまざまなユースケースで、ニーズが加速していく。 (2) 例①：製造／資源分野では、既存のオンプレミス（企業内）で運用していたIoTの利用環境のクラウドへの移行や、新規にIoTクラウドプラットフォームを導入するケースが増加する。 (3) 例②：流通／サービス分野では、オムニチャネルオペレーション用途のIoTシステム上で、在庫管理の最適化や顧客購買行動分析を目的とした分析ソフトへの支出が加速する。 (4) 例③：個人消費者分野では、宅内のスマート家電やパーソナルロボットなどスマート機器用途のIoT機器の制御を目的としたアプリケーションソフトへの需要が高まる。		
今後の課題		(1) 現在、ランサムウェア（WannaCry）の急増によってIoT機器や制御系システムへのサイバー攻撃が現実的な脅威となり、IoTセキュリティ市場への需要が拡大している。 (2) 今後、IoTセンサーやIoTデバイスベンダ、IoTプラットホームベンダなど、セキュリティ業界を超えたパートナーエコシステムの構築が必要となっている。		

CAGR：Compound Annual Growth Rate、年間平均成長率
オムニチャネルオペレーション：Omni Channel Operation、すべて（オムニ）の販売チャネルを統合し、ユーザーがどの販売チャネルからも同じ方法で商品を購入できる環境を構築すること

出所　IDC Japan「国内IoTセキュリティ製品市場予測を発表」、2017年11月6日をもとに編集部作成、
https://www.idcjapan.co.jp/Press/Current/20171106Apr.html

IT専門の調査会社であるIDCジャパンは、2017年11月6日、「国内IoTセキュリティ市場予測、2017年～2021年」を発表した。

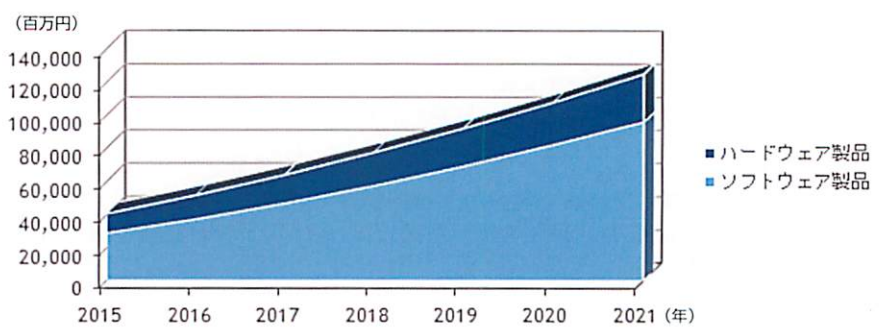
このレポートによると、2016年の国内IoTセキュリティ製品市場規模は、ハードウェア、ソフトウェアを合わせて、前年（2015年）比27.5%増の518億円で、今後2016～2021年のCAGR（年間平均成長率）は19.3%と急増し、2021年には1,250億円と1,000億を超える市場規模となると予測されている（表、図）。

この背景には、サイバー攻撃を行うランサムウェア「WannaCry」のような新型のマルウェアの登場がある[注9]。このWannaCry（ワナクライ）は、2017年5月に、マイクロソフトのWindows OSの脆弱性を利用して、パソコンなど（情報システム）ばかりでなく医療機器や、自動車工場などの産業システム（制御システム）までもサイバー攻撃対象とし、世界150カ国以上で猛威を振るったことで、話題となった。

このようなランサムウェアによってIoT環境へのサイバー攻撃が現実的な脅威ともなり、IoTセキュリティ市場が急速に拡大すると予測されている。

▼注9
IPA（情報処理推進機構）の発表によれば、今回観測されているランサムウェアはWannaCryptorと呼ばれるマルウェア（WannaCrypt, WannaCry, WannaCryptor, Wcryなどとも呼ばれる）の亜種であると考えられている。
https://www.ipa.go.jp/security/ciadr/vul/20170514-ransomware.html

図　国内IoTセキュリティ市場：製品セグメント別の売上額予測、2015年～2021年



出所　IDC Japan「国内IoTセキュリティ製品市場予測を発表」、2017年11月6日、
https://www.idcjapan.co.jp/Press/Current/20171106Apr.html