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。

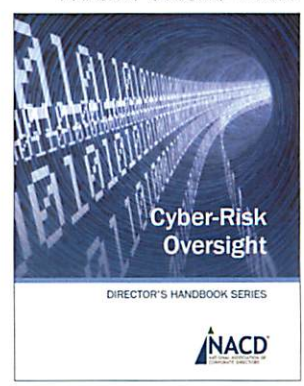
江崎：日本ではCIOとCISOを兼務していますが、ほとんどの場合、機能していないケースが多いですね。これは、会社組織でいうと、CEO（Chief Executive Officer、最高経営責任者）と監査役（取締役の業務執行を監査する人）が同じ人が兼務しているという感じです。このような現状を変えるには、その会社で生産しているプロダクト（製品）に対して「リスク管理ができていないと、会社の経営がめちゃくちゃになってしまう」というような話ができるCISOが必要なのです。

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<br>（日本語翻訳版：日本工業規格 JISQ27001：2014） | 日本工業規格 JISQ15001：2006<br>（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<br>（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。

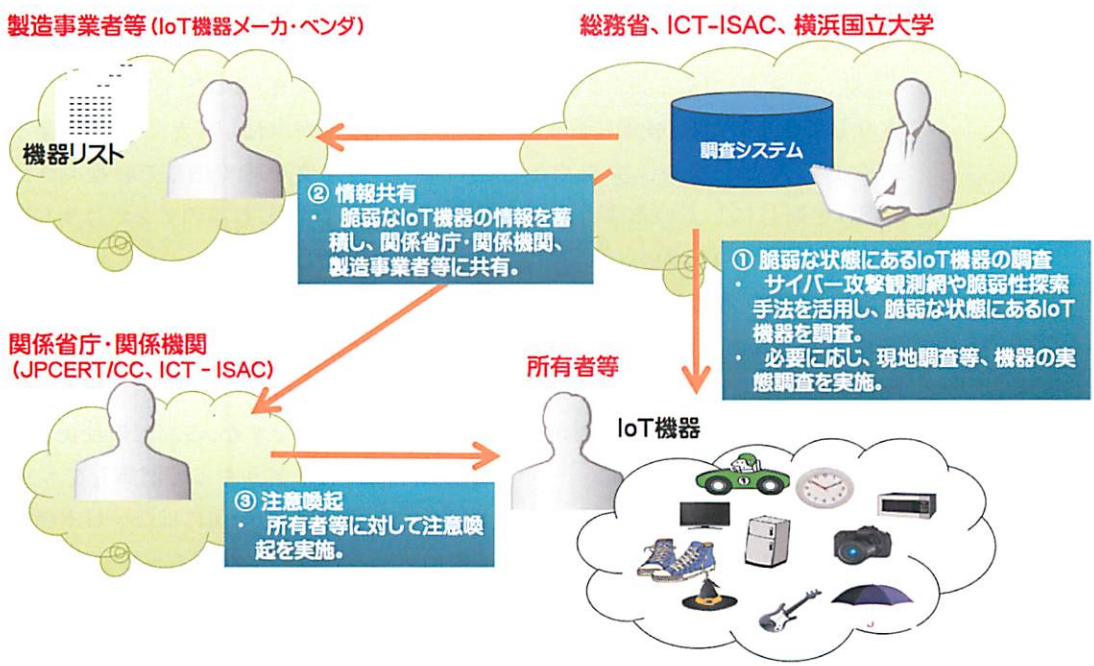
江崎：ISACでうまくいっているところは、最初にISACを立ち上げたコアのメンバーが頑張っています。業界のコアの人たちがほんとうに情報共有して、コアの部分を残しながら少しずつ共有部分を増やしていっています。

### 〔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。

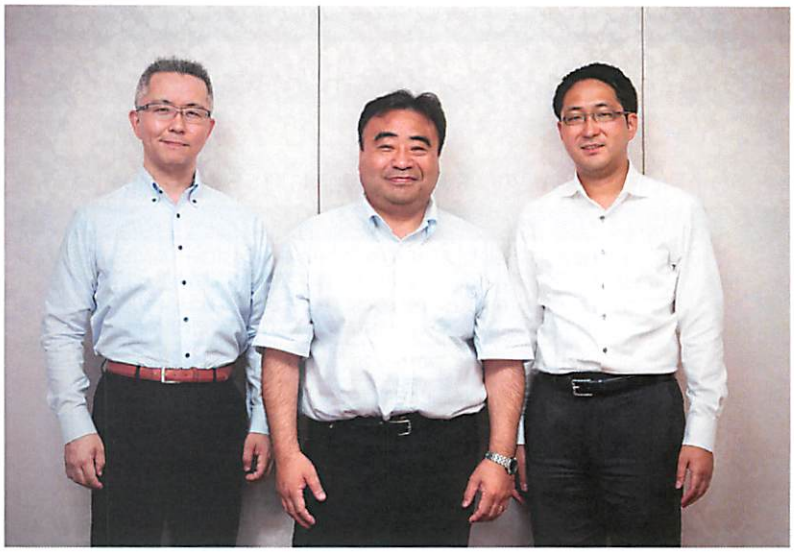
佐々木：セキュリティに関して言えば、セキュリティを単なる自分の会社を守るためのコストととらえていては、いつまでやって

▼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、<br>(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。<br>(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。<br>(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。<br>(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。<br>(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。<br>(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。<br>(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。

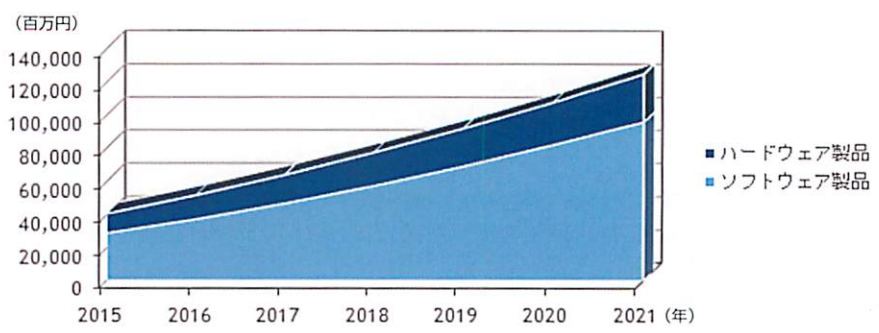
このレポートによると、2016年の国内IoTセキュリティ製品市場規模は、ハードウェア、ソフトウェアを合わせて、前年（2015年）比27.5%増の518億円で、今後2016～2021年のCAGR（年間平均成長率）は19.3%と急増し、2021年には1,250億円と1,000億を超える市場規模となると予測されている（表、図）。

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