MIZUHO

みずほ銀行

One MIZUHO

mizuho global news

みずほグローバルニュース

日本:
姫路城

2018
AUG&SEP
vol.98

特集

サイバーセキュリティ戦略を考える

海外事例から学ぶ企業のサイバーセキュリティ対策

アクセンチュア株式会社
セキュリティコンサルティング本部 マネジング・ディレクター 大茂 幸子氏
Ms. Sachiko Ohshige, Managing Director, Accenture Security in Japan

日本のサイバーセキュリティ関連予算は、平成30年度は概算要求ベースで730億円と、過去数年で増額の一途をたどった。しかしながら、その規模が海外の大手企業1～2社分の予算にすぎないことを考えると、我が国のサイバーセキュリティ対応の遅れは、まだ社会的に十分認知されていないようにも感じる[*1]。

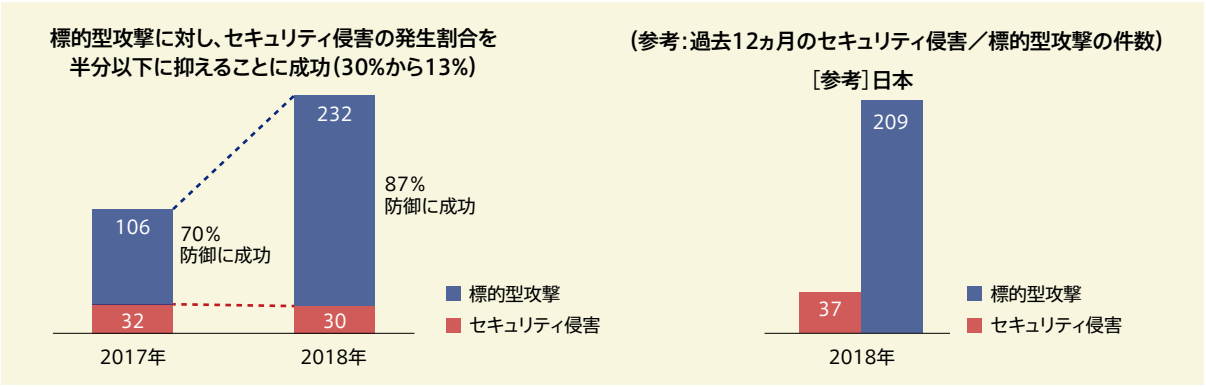
国境を越えたサイバー攻撃の手法が巧妙化する一方で、セキュリティ担当者の数は世界的にも不足し、GDPR（EU一般データ保護規則）を含む海外法規制は厳しさを増している。データの保護やプライバシーの問題が大きな注目を集めるデジタル社会において、信頼に足るサイバーセキュリティ対策を講じ、適切な情報管理を行うことは、あらゆる企業にとって経営課題となり、サイバーセキュリティ対策へ投資しないことが、むしろリスクになり得る時代となった。

大企業はサイバーレジリエンスを向上

大企業においては、サイバーセキュリティ対策の取り組みが着実に効果をあげているとの調査結果もある。アクセンチュアが2018年に世界15ヵ国の企業幹部、約4,600人を対象に実施したサイバーレジリエンス調査[*2]によると、WannaCryを含むランサムウェア（身代金要求型ウイルス）による事件が多発した過去2年間において、企業に対する標的型攻撃は、前年比で倍以上に増えた一方で（106件から232件）、事故発生率については半分以下に低下したとの回答が得られた（30%から13%）（図表1）。

ただし、調査対象企業では月平均で2～3件のセキュリティ侵害事故の発生が認められており、態勢整備には一層の改善や継続的な対策の実施が必要とされている。

図表1. 標的型攻撃への防御力向上



【年間売上高10億ドル（約1,100億円）以上の企業4,600社を対象に調査（うち日本企業は400社）】
（出典）Accenture Security, 2018 State of Cyber Resilience調査

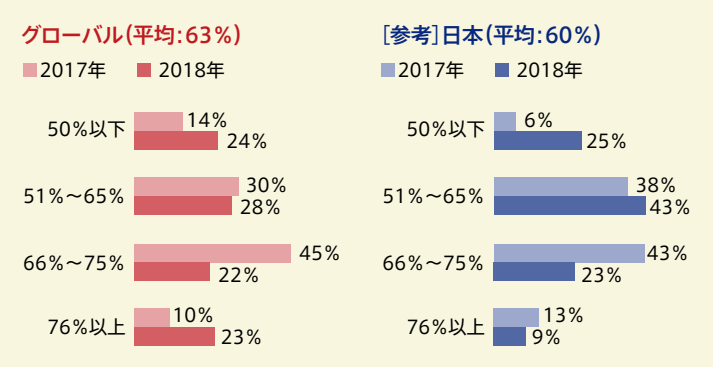
大企業の検知能力の向上

多発する攻撃の背景には、攻撃ツールや開発キットなどが流通し、盗んだデータを売買可能なブラックマー

ケットの存在がある。不正サイトであるダークウェブでは、ランサムウェアサービス(RaaS: Ransomware-as-a-Service)や、DDoS攻撃サービス(DDoS-for-Hire)など、コモディティ化された製品・サービスが購入可能で、盗んだデータは仮想通貨を介して収益化するなど、高いスキルや多額の投資を必要としない、サイバー犯罪市場のエコシステムが形成されている。攻撃の商業化が進み、また組織化された犯罪グループの関与で、サイバー攻撃のオペレーション規模は飛躍的に拡大した。

同調査によると、事件多発で緊張感が増した状況下でも、対象の大企業のセキュリティチームの63%が侵害未遂を検知していた。ただし「76%以上の高い検知率」を確保した企業が約2倍に増えた一方で(2017年10%から2018年23%)、「50%以下の検知率」にとどまった企業も増加していた(2017年14%から24%)。攻撃防御に成功する企業が増える一方で、対応に苦戦する企業も増えるという、二極化が進行していることがうかがえる(図表2)。

図表2. セキュリティチームが検知したサイバー攻撃の割合

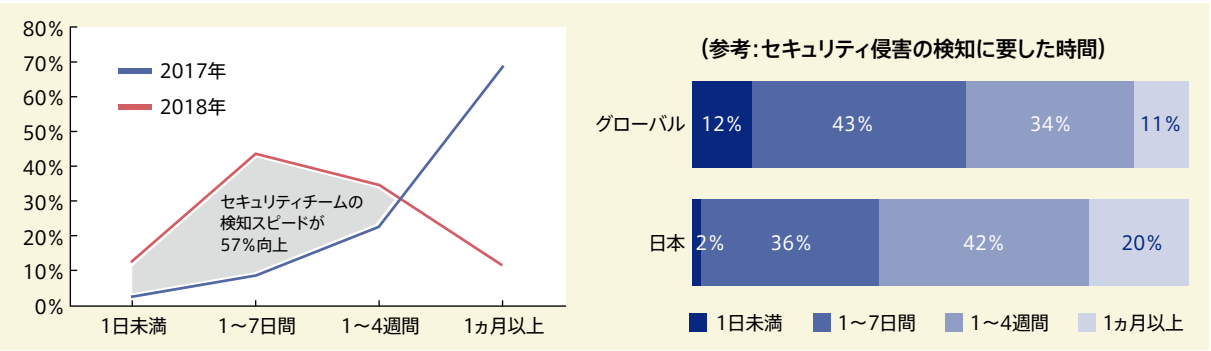


【年間売上高10億ドル(約1,100億円)以上の企業4,600社を対象に調査(うち日本企業は400社)】
(出典)Accenture Security, 2018 State of Cyber Resilience調査

より速い検知

同調査では、「1ヵ月以内」の検知が9割(89%)に達した(2017年は約3割)。うち「1週間以内」の検知が過半数(55%)であり(同約1割)、検知スピードの向上が確認された(図表3)。

図表3. セキュリティ侵害の検知スピード向上



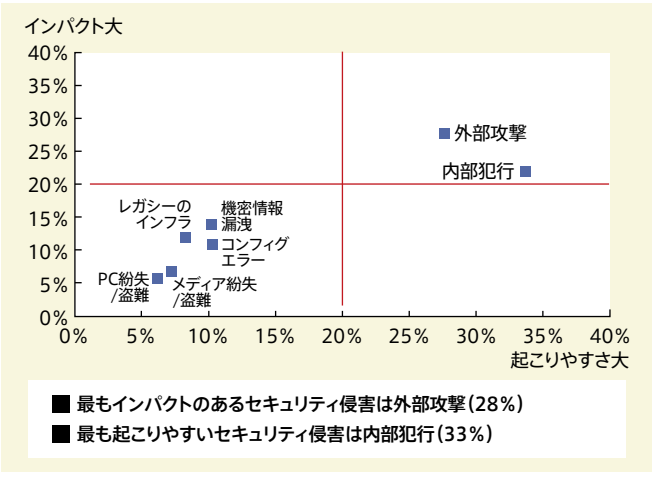
【年間売上高10億ドル(約1,100億円)以上の企業4,600社を対象に調査(うち日本企業は400社)】
(出典)Accenture Security, 2018 State of Cyber Resilience調査

外部攻撃と並ぶ、内部犯行の多さも要注意

改善を検討する際に外部攻撃に目を向けがちであるが、内部犯行者も軽視すべきではない。同調査によるとダメージの大きな攻撃のトップ2は、ハッカーなどによる「外部攻撃」と並んで、悪意のある者による「内部犯行」であった。

同調査では、外部攻撃は2017年以降9%増加し(2017年19%から2018年28%)、内部犯行は昨年より約半分に減少していた(2017年43%から2018年22%)。なお、セキュリティ侵害の問題は、インパクトだけでなく、攻撃の相対数も重

図表4. 最もダメージのあるセキュリティ侵害のトップ2



【年間売上高10億ドル(約1,100億円)以上の企業4,600社を対象に調査(うち日本企業は400社)】
(出典)Accenture Security, 2018 State of Cyber Resilience調査

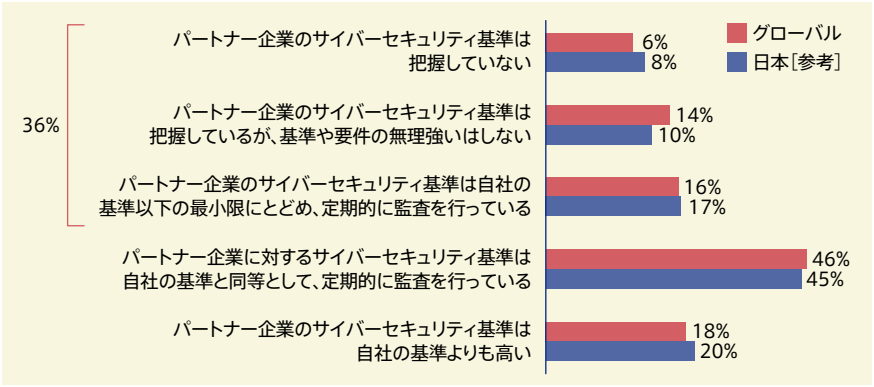
要視すべきである。起こりやすさの比率について、外部攻撃（28%）よりも、内部犯行（33%）が高いことを踏まえると、外部のみならず内部脅威からも組織を守る対策が不可欠である（図表4）。

サプライチェーンを保護する

グループ会社やパートナー企業のセキュリティレベルが低ければ、自社のサイバーセキュリティ対策をどれほど強化しても十分な効果をあげることは難しい。サイバー脅威においてはセキュリティレベルの最も低い部分が狙われるため、子会社やパートナー企業のサイバーセキュリティ対策もおろそかにはできず、最優先で取り組むべきである。図表5に示されるように、グローバルでは1/3以上（36%）が“パートナー企業に対し、自社と同レベルのサイバーセキュリティ基準を適用していない”状況を回答しており、自社を超えたサプライチェーンにおけるセキュリティ保護の遅れが浮き彫りとなっている。

あらゆる脅威への備えを盤石なものとするため、大企業は内部・外部のバリューチェーンを横断して、サイバーセキュリティプログラムの基本配備を推し進めていくべきである。

図表5. パートナー企業のサイバーセキュリティ基準の遵守状況



【年間売上高10億ドル（約1,100億円）以上の企業4,600社を対象に調査（うち日本企業は400社）】
（出典）Accenture Security, 2018 State of Cyber Resilience調査

企業規模を問わないサイバー攻撃

デジタル時代の到来により、ここ数年でインターネットに多種多様なモノが接続されるIoT（Internet of Things：モノのインターネット）関連の技術がさらに発展し、ヒトやプロセスまでもが接続されるIoE（Internet of Everything：すべてのモノのインターネット）の世界がますます現実味を帯びてきた。一方、これによりネットワーク、ソフトウェア、人員の各レベルで膨大なデータが生成されることになるため、増え続けるデータに応じてアタックサーフェス（攻撃されるポイント）が拡大し、かつてないほどに情報のセキュリティとプライバシーの確保が迫られる時代に入った。

それゆえにサイバー攻撃のターゲットは、大企業のみならず、確実に中小企業にも拡大している。大規模企業から機密情報（先端技術、特許、入札価格など）の入手を目的に中小企業を踏み台とする、犯罪グループによる標的型攻撃が想定される。さらに、セキュリティ人材の不足や社内研修の未実施が組織の脆弱性につながり、攻撃発生時に被害を拡大させる可能性もある。

人員の限られた組織では、大企業以上にサイバー対策コストの捻出が難しく、攻撃によるインパクトは深刻である。サイバー空間にどのような種類の脅威が存在し、自社に対してどのようなサイバー攻撃のリスクがあるのかなど、検討すべき担当者が社内に不在であれば、実際に攻撃された時にどう対処するか、どうやって復旧するか、皆目見当がつかないといった事態が想定される。米国土安全保障省傘下のNational Cyber Security Alliance（NCSA）によると、小規模な企業がハッキング被害を被った場合、対応がわからないために、半年以内に60%が事業中止に至ることが報告されている[*3]。大企業の場合、仮にセキュリティ侵害に遭い、データ漏洩を生じさせた場合でも、経営陣や法務、広報などから構成される危機対応チームが機能し、批判的な報道への対策や関係当局による重い罰金などに対応することが可能であっても、一般的に経営基盤が脆弱な中小企業にとっては対応困難なケースが大半であろう。

海外の中小企業の状況

中小企業のサイバー対策状況の調査報告の数は少ないが、いくつかの調査結果をもとに、海外の中小企業を取り巻く現状について確認しておきたい。

大手通信事業者のVerizon社が2018年に公表した「データ漏洩/侵害調査報告書」によると、世界65ヵ国で1年間に発生したインシデント53,000件およびデータ漏洩2,216件のうち、被害を受けた58%が中小企業であったという[*4]。

セキュリティソフトウェア企業のWebroot社が2017年に発表した「中小企業のサイバー脅威調査」[*5]では、米国、英国、オーストラリアの中小企業(従業員数100～500人未満)のITシステムの意思決定者の96%が「自社が近い将来サイバー攻撃を受けるのではないか」と回答し、うち71%が「まだ万全な対策を取れているとはいえない」との懸念を示している。また、同調査では、ITシステムの意思決定者の最大の懸念事項として、「新種のマルウエア感染」(56%)、「モバイル攻撃」(48%)、「フィッシング攻撃」(47%)が上位に挙がった。このほか、ITシステムの意思決定者の2/3は、「社員間の信頼とモラルの修復よりも、会社の公的イメージの修復のほうが困難」との見方を示したが、「ITセキュリティの専門家を設置している」と回答したのは23%、「外部のITセキュリティ専門家の支援を受けている」と回答したのは37%にとどまり、サイバー攻撃に対する懸念に対して十分な対策ができていない現状が浮き彫りになっている。

米調査機関のPonemon Instituteによる2016年の「中小企業のサイバーセキュリティの状況」[*6]では、「自社がサイバーリスクや攻撃を"極めて効果的に"軽減している」と回答した中小企業は、わずか14%にすぎなかった。また、デバイス管理の最低限のルールであるパスワード管理を徹底しなければ、容易にハッカーに乗っ取られリモートで自社内ネットワークへ侵入されてしまう危険は明白であるものの、「自社にパスワードポリシーはあるが運用されていない」と回答した中小企業が65%にも上るなど、セキュリティ対策の基本中の基本ができていないことが指摘されている。

アクセンチュアではフィッシングの脅威に関する調査も展開している

英国のNational Cyber Security Centre(NCSC)の2018年の「サイバーセキュリティ漏洩/侵害調査」[*7]によると、過去1年間に全企業のうち4割(43%)がサイバーセキュリティ侵害に遭っていた。内訳として零細企業の40%、小規模企業の47%、中規模企業の64%が含まれていた。

NCSCは英国の国家サイバーセキュリティセンターとして、複数の省庁にまたがっていたサイバーセキュリティ機能を統合し2016年に新設された。サイバー脅威評価を横断的に実施し、官民におけるサイバー空間上の脅威情報共有を推進している。大企業から中小企業、政府、官公庁の対応窓口として、サイバーセキュリティガイダンスを提供し、サイバーセキュリティの啓発活動を行っている。

さらに英国では、スタートアップ、マイクロを含む小規模事業者および中小企業を対象とした、Cyber Essentials制度およびCyber Security Innovation Voucher制度が2014年より開始した。

Cyber Essentials制度は、審査に合格した組織がマークを表示することで、ステークホルダーへのサイバー対策への取り組みのアピールと、政府入札案件への一要件を満たすメリットをインセンティブとして、英国のサイバーセキュリティレベルの底上げに寄与している。Cyber Security Innovation Voucher制度は、上限5,000ポンド(約75万円)を、外部のサイバーセキュリティ専門家からの支援やマーク取得の費用として提供しており、400以上の組織が恩恵を受けた。

なお、我が国も、2017年より、IPAの「SECURITY ACTION」(中小企業が自己宣言する形でセキュリティへ取り組みをアピールするマーク)、および一般社団法人サービスデザイン推進協議会の「IT導入補助金」(上限50万円)や、最近では経済産業省の「コネクテッド・インダストリーズ税制(IoT税制)」がスタートしている。

米NCSAは、小規模会社に対するサイバー攻撃は全体の70%以上で、小規模会社の50%がサイバー攻撃を経験し、ハッキングを受けた小規模会社の60%が6ヵ月以内の事業停止に至ったと報告し、中小企業にとってもサイ

バー攻撃が実在する脅威であることを示した[*3]。

米国では、中小企業へのサイバーセキュリティに関するガイダンスとして、国土安全保障省が、中小企業に対するサイバーセキュリティの基礎教育ツールとして、NIST (National Institute of Standards and Technology) のサイバーセキュリティフレームワークの使用をリリース時(2014年)から奨励した。同時期には、連邦通信委員会による小規模会社向けのサイバー対策計画サイト(Small Biz Cyber Planner)や、アメリカ連邦中小企業庁によるWebラーニングサイト(Cybersecurity for Small Business training course)が提供された。

グローバルレベルでは中小企業のサイバーセキュリティの対策強化も求められている(写真はイメージ)

IBM、Mastercard、Microsoftの元CEOなどがボードメンバーを務めるThe Cyber Readiness Institute (CRI) のレポートによると、大規模組織が技術的管理から従業者教育に至るまで、一定の人員や対策費用をサイバー対策に割り当てるのに対し、中小企業の場合はITシステム部門の専門人員も持たない場合があり、サイバーリスクへの対処は非常に困難である点が指摘されている[*8]。

さらに、中小企業が大規模組織のシステムへ侵入するための手段として狙われるケースが増えており、中小企業であっても、かつてない緊張感をもとに取り組む必要があると警告している。

中小企業では、サイバーハイジーン(サイバー衛生:サイバー対策の基本原則)であるパッチ管理、最小特権、暗号化、正規のダウンロードなどの不適切な運用で脆弱性を生じさせているケースが多い。トレーニングを受けていない従業者や、バージョンが旧型のシステムなども、サイバーリスク管理上の課題に含まれる。

中小企業とサイバーセキュリティ

経営者は、サイバーセキュリティ対策を経営課題として認識し、自らの責任で取り組むことが重要である。具体的な課題には、方針策定、社内外の体制構築・対策実施、被害からの早期回復を含む復旧計画の策定などが含まれる。万一事故が生じた際に、経営者が利害関係者へ謝罪説明を行う場合、実行済みの対策いかんで免責の範囲も変わってくるだろう。また、取引先や業務委託先、海外などを含むサプライチェーンにおいて、機密情報・顧客情報など、最も価値のある資産を保護するために、どのようなIT資産があり、攻撃対象は何か、どのようなセキュリティホールがあるかなどを把握したうえで、適した対策をとる必要がある。

内閣サイバーセキュリティセンター、情報処理推進機構などより提供されているガイドラインやアセットの活用、都道府県下の警察・商工会議所・学術機関・地方自治体などからのサポートを受けることも重要である。サイバーセキュリティの脅威がゼロになることはない。セキュリティ対策は通常業務の一部という認識で推進する必要がある。

この先のサイバーセキュリティ対策
～すべてがデジタルになる時、すべてがリスクにさらされる～

本記事の冒頭で、大企業のサイバーセキュリティ対策が強化されている調査結果をご紹介した。素晴らしい進歩ではあるが、従来型インシデントへ対応した成果であるため、それだけでは将来のサイバーリスクへの対応が間に合わない。企業はより速く、賢く、無駄なくリーンに、そしてより敏感に、新しいテクノロジーがもたらすオペレーティングモデルやビジネスモデルの導入に取り組んでいる。IoTやクラウドコンピューティング、人工知能(AI)や機械学習(Machine Learning)、ロボティクス、オープンAPIなどによりデータの連携や利活用が進むにつれ、セキュリティリスクは増大していく。デジタル時代へ移行を進める企業は未知のサイバーリスクに対処していく必要がある。

未来をどう防護すべきか

将来のサイバーセキュリティ対策には、新しいビジネスモデルや、AI・機械学習などのインテリジェント・テクノロジーの活用に対するリスクの備えが必要である。機械が機械を攻撃する時代であり、企業はビジネスにセキュリティ対策を結びつけるだけではなく、ハッカー側が用いるインテリジェント・テクノロジー（AIや機械学習など）を採用する必要がある。2018年のアクセンチュアのサイバーレジリエンス調査[*2]によると、経営層の3/4が、新たな技術によるサイバーセキュリティリスクの大幅な削減を期待していると回答したが、新技術だけでは十分とはいえない。デジタル化社会において、将来の事業を安全に成長させるためには、サイバーレジリエンス（有事の場合の復旧力・回復力）の向上が必要であり、企業すべての活動にセキュリティの組み込みが求められる。

組織は、セキュリティを全従業者の重要な任務として、“セキュリティ・ファースト”の意識を醸成し、企業の防護範囲を拡張し続けていく必要がある。その一歩として、データの保護とガバナンスにフォーカスしたサイバーセキュリティ戦略および投資計画の策定から着手することが望ましい。さらにセキュリティの専門技術の配備や、説明責任を果たせるような組織への構造改革、従業員や顧客への理解浸透や外部の戦略的パートナー企業との連携も欠かせない。

未来のビジネスは信頼とともに成長させる

将来のサイバーセキュリティのリスク対応には新たな戦略が要る。トップリーダーは組織を挙げてセキュリティをコア・コンピテンシー（企業の中核となる能力）に置き、サイバーレジリエンスを浸透させるべきである。それが達成できれば、信頼に足る業務プロセス、顧客およびパートナー企業との強固な信頼関係、そして市場ポジショニングの確立を基に、未来の事業成長を安心して推進できると考えられる。

＊1 2016年のサイバーセキュリティ予算はJ.P. Morgan Chase & Co.（US$500M: 約550億円）、Bank of America（推定US$450M: 約495億円）、Citibank（US$300M: 約330億円）、およびWells Fargo（US$250M: 約275億円）の4社でUS$1.5B（約1,650億円相当）。
https://www.forbes.com/sites/stevemorgan/2015/12/13/j-p-morgan-boa-citi-and-wells-spending-1-5-billion-to-battle-cyber-crime/#2ec988f8116d
＊2 https://www.accenture.com/us-en/insights/security/2018-state-of-cyber-resilience-index
＊3 www.staysafeonline.org/stay-safe-online/resources/small-business-online-security-infographic
＊4 https://www.templarbit.com/blog/jp/2018/04/11/highlights-of-the-verizon-2018-data-breach-investigations-report
＊5 https://www-cdn.webroot.com/7515/2935/7252/SMB_Cybersecurity_Survey_F.pdf
＊6 http://www.triscal.com.br/shared/docs/seguranca-state_cybersecurity_small_medium_businesses-2016.pdf
＊7 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf
＊8 https://www.cyberreadinessinstitute.org/news-and-resources/2017/small-and-mid-sized-businesses-cyber-threats-by-the-numbers

育む場作りと人材育成

富士通株式会社 サイバーセキュリティ事業戦略本部 サイバーディフェンスセンター
シニアセキュリティコーディネーター　佳山 こうせつ氏

第一章：つながる時代に必要な人が育まれる場作り

IoT時代の到来でデジタルデータが価値を生む一方、日本では多くの企業がエンジニアの不足に悩んでいます。

そうした状況下、富士通では2014年からセキュリティマイスター認定制度を立ち上げ、人材育成に取り組んできました。700名を目標に制度設計して4年が経過した2018年4月現在、3,000名を超えるセキュリティマイスターが育まれました。本稿では、4年の実践から感じた人材育成の意味について私の考えを説明したいと思います。

IoT時代の到来で情報の利活用がさらに進む

IoT時代の到来で、さまざまなセンサーや機器がインターネットにつながり、膨大な量のデジタルデータが集まり、「新たな価値」を生むようになった。

たとえば、全国各地に設置したセンサーなどを通じて気温や湿度を測定したり、リアルタイムに雨雲の状況を把握したりすることで、それらの情報をもとにコンビニエンスストアの店頭に並べる商品を随時変えていくこともできる。消費者ニーズにさらに細かく対応し、在庫を持たない店舗運営もさらに加速するだろう。

こうした情報の利活用は今後も進み、点在化された情報をいかに安全・確実に結びつけるかといったネットワークの重要性がさらに高まっていくと考えられる。

「つながる時代」に高まるセキュリティの重要性

IoT時代とは、点在していた情報が「つながり」、新しいイノベーションを起こす時代とも考えられる。情報が「つながる」時代だけに、ひとたびサイバー脅威が顕在化すると、その被害が連鎖反応的に拡大していくことが懸念される。事実、ランサムウェア「WannaCry」というサイバー脅威は、つながったコンピュータが次々に被害に遭うことで、その被害規模が拡大していった。

こうした「つながる時代」に、セキュリティは継続的な価値を生む土台となる。安心してイノベーションに投資できるようにし、若者が新しいアイデアを安心して実践できるような環境を作ることがセキュリティの役割である。情報と情報とがネットワークを通じて安全・確実につながるように「事業の継続を担保」することこそが、今後のイノベーションの鍵を握っている。

人材育成とは"つなげる"もの

このような状況下、多くの企業では、セキュリティもデザインできるエンジニアの育成が求められている。「つながる時代」のセキュリティもデザインできるエンジニアとは、単純にセキュリティに関する知識やスキルが豊富というだけの人材ではない。

「つながる時代」には、企業のビジネスでも決して自社だけで完結するものではなくなる。協業や共創、エコシステムの構築においては、企業同士が協力しあい、大きなイノベーションの実現に向かってともに歩むことも必要である。

サイバーセキュリティ研修風景

富士通のサイバーレンジ（仮想演習場）CYBERIUM

企業同士の連携が今まで以上に密接になるなか、イノベーションの実現も1社だけではなく、連携・協業する複数の企業間でセキュリティを共通の言語で語り、共通の問題意識を持ち、そしてエコシステムの全体像の中でセキュリティを俯瞰することが大切である。そのための人的ネットワークを構築することのできる人材が求められている。

人と人がつながれば組織がつながる。普段それぞれのミッションで縦割りになりがちな組織が、人のつながりにより情報を巡らせるようになる。人と人、組織と組織、企業と企業へと広がったネットワークは、産官学の連携にもつながっていくだろう。さらに世代をまたがって次世代につなげることも人材育成の役割といえる。

そして、情報が巡れば相互理解が芽生える。セキュリティを理解し、セキュリティ現場がイノベーションを理解することで、セキュリティが付加価値となる競争力を作ることができると信じている。たとえば、セキュリティの人と生産管理現場の人、プラント設備管理現場の人などがつながると、よりセキュアなIoTの利活用が可能になると考えられる。

学ぶ、体験する、考える、そして仲間を作る「CYBERIUM」

「つなげる人材育成」をお客さまや地域、若者たちと実現するために、国産のサイバーレンジ「CYBERIUM」を開発。「CYBERIUM」では、疑似的なサイバー攻撃シミュレーションを体験しながら、攻撃の手口や防御方法を実践的に学ぶことができる。

セキュリティを学び、体験し、考える場、そして先人の成功や失敗を共有する場、さらに仲間を作りコミュニケーションする場を継続的に提供し、皆さまとともに、セキュリティ人材を育んでいきたいと考えている。

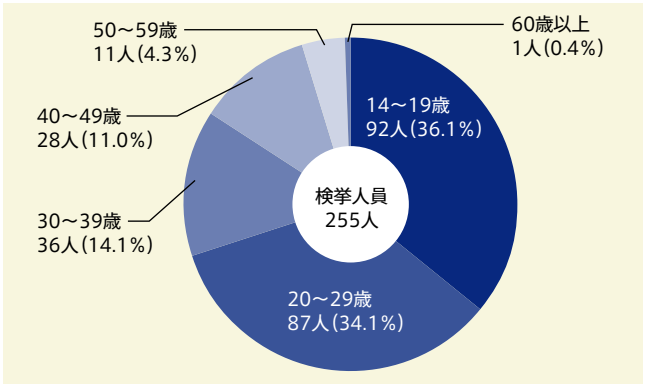
第二章：若者を明るく育む地域の産官学連携による場作り

2018年5月24日より3日間南紀白浜にて「サイバー犯罪に関する白浜シンポジウム（以降、白浜シンポジウム）」が開催されました。テーマは「若者とサイバー犯罪：被害者・加害者・傍観者」。近年サイバー犯罪に占める若者の割合が増加しているというトピックが大きな議題となりました。第二章では、この事態に対し、企業として何ができるのかを考えます。

進むサイバー犯罪加害者の若年化

2018年3月22日に公表された「不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究

図表1. 平成29年における年代別被疑者数



（出典）国家公安委員会、総務大臣、経済産業大臣「不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況」、平成30年3月22日
http://www.meti.go.jp/press/2017/03/20180322004/20180322004.html

図表2. 過去5年の年代別被疑者数の推移

区分＼年次	平成25年	平成26年	平成27年	平成28年	平成29年
14～19歳	44	49	53	62	92
20～29歳	30	43	43	56	87
30～39歳	37	45	41	48	36
40～49歳	27	25	29	29	28
50～59歳	8	5	5	3	11
60歳以上	1	3	2	2	1
計（人）	147	170	173	200	255

（出典）国家公安委員会、総務大臣、経済産業大臣「不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況」、平成30年3月22日

開発の状況」によると、不正アクセス禁止法違反の検挙者数が増えており、特に14～19歳のレンジが増加傾向であるという事実が白浜シンポジウムでも、大きな話題となった。

必要とされたい気持ちが犯罪へと誘う

特に印象的だったのは、朝日新聞社の須藤記者が6年間密着取材を通して感じられた、加害者に関する次の見解である。「陽の当たらない世界に潜む若い子たちはたくさんいる」、「必要とされている感がすごいらしく、いい方向へグリップしてあげる存在が重要」。記者目線のこのコメントから、理解されたい、必要とされたいという気持ちがサイバー犯罪の動機となりうるということを知り、改めて考えさせられた。

ネット独学に潜む危険性

サイバー犯罪者となった若者が、その知識を「独学」で得たという事実からも、独学に潜む危険性に関しても考える必要があると感じた。

［参考ニュース記事］
「佐賀県教育委員会の情報システム「SEI-Net」などに侵入したなどとして、不正アクセス禁止法容疑で佐賀市の17歳の無職少年が再逮捕された事件。少年は独自開発した攻撃用プログラムでシステムの脆弱性をつくなどして個人情報を入手していたという」

(出典) 17歳が教育システムに不正アクセス　攻撃用プログラムで脆弱性つく　「能力にちょっと驚く」と馳文科相(ITmedia)
http://www.itmedia.co.jp/news/articles/1606/30/news092.html

上記ニュースについて、好奇心にかられ独学で技術を身につけることの危険性について、活発な議論がなされた。

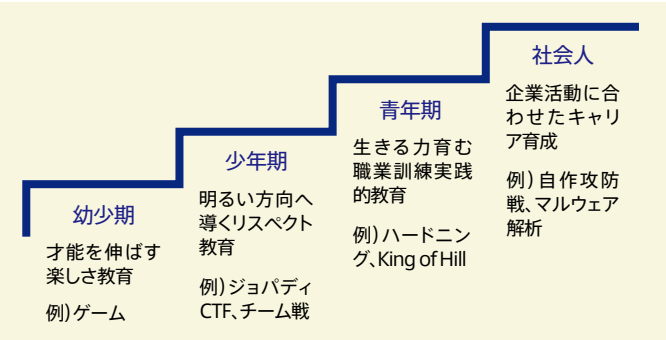
ネットの情報から独学で技術のみを習得し、法規制に関する知識や、モラルを備えることなく、技術に対するリスペクトもないまま技術者となってはいないか？結果としてサイバー犯罪予備軍になってはいないだろうか？この課題の解決に貢献しうる取り組みの1つが「明るい地域の場作り」である。

若年層犯罪を減らしたい　明るい地域の場作り

①育む場作り ～生涯学習モデル～

富士通は、愛媛県警・愛媛大学と共同でハンズオンセミナー(主催：サイバーセキュリティシンポジウム道後実行委員会、以降道後ハンズオンセミナー)を2017年から始動。また、セキュリティマイスター道場など、地域の場づくりに役立つ場作りに協力している。
https://www.youtube.com/watch?v=bEqNFz7WdxE

図表3. 生涯学習モデル



力のありあまった子供たちが警察署の柔道・剣道で汗を流し力と心を研鑽し成長するように、コンピュータ技術のありあまった若者がその年代に合わせ、地域の道場でコンピュータで汗を流し技術と心を研鑽し成長できるような場が必要。

そこでは、学校でマイノリティになっている子供が仲間づくりをする、困ったことを相談するといった機会もあるだろう。このような場が楽しいと感じる成功体験を重ねることで、技術に対するリスペクトを持てるようになれば、若者たちを犯罪から遠ざけることができるのではないだろうか。

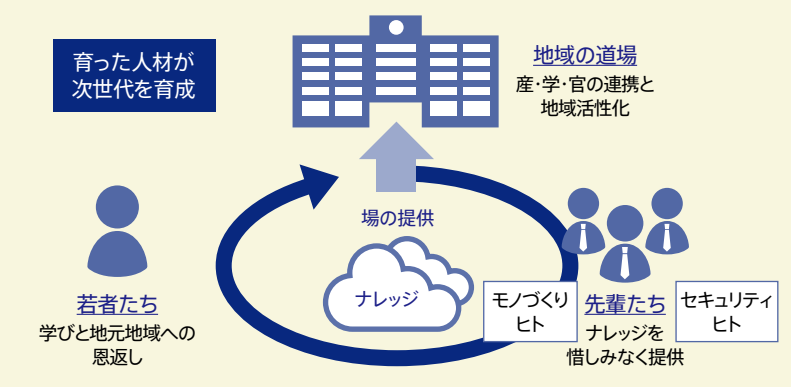
②育むエコサイクル ～つなげるモデル～

場作りが一時的にうまくいったとしても、継続的な活動でないと意味が薄れる。地域で継続する活動にするためには、お金を極力かけず、育った人が次の世代を育てるサイクルを作ることが重要である。

地域が次の世代を育てる機会を与え、さらに何かに貢献する機会を与え、技術がつながり、何かに貢献するというサイクルが、つなげるモデルである。

このような活動で承認欲求を満たしながら、たとえば地域の警察に就職したいといった夢を持てるような若者が生まれるようになれば嬉しいと考えている。

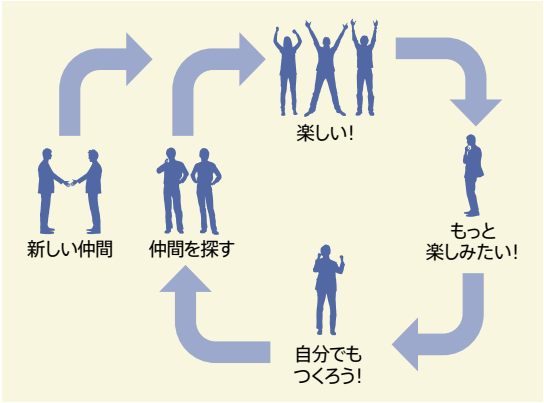
図表4. つなげるモデル



若手セキュリティマイスターである当社の堀も、白浜シンポジウムで以下の写真のような発表を行った。

「楽しい、またやりたい、自分が作りたい、場をつなげたい、広げたいと、自身を振り返って、若い世代の目線で考え実践しながら彼ら自身が次世代につなげていきます」。

図表5. 明るい場の連鎖

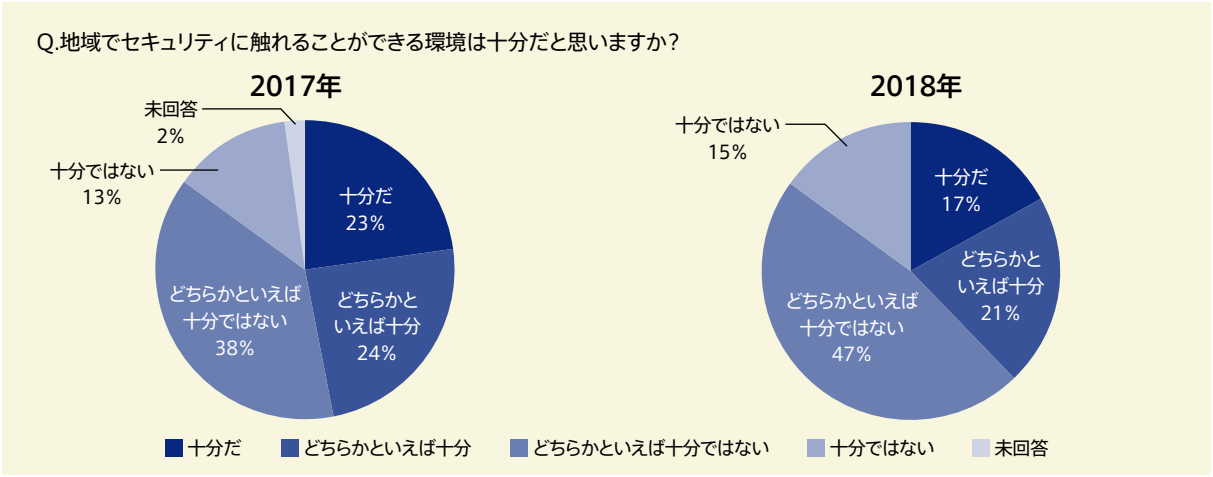


出所：当社講演資料「若い力と技術と情報が集う明るい“場”の提供 ～20代エンジニアの視点～」

最後に

図表6のように、2017年から始めた道後ハンズオンセミナーでのアンケートの結果からも、地域の場作りを求める声が少しだけ垣間みえる。

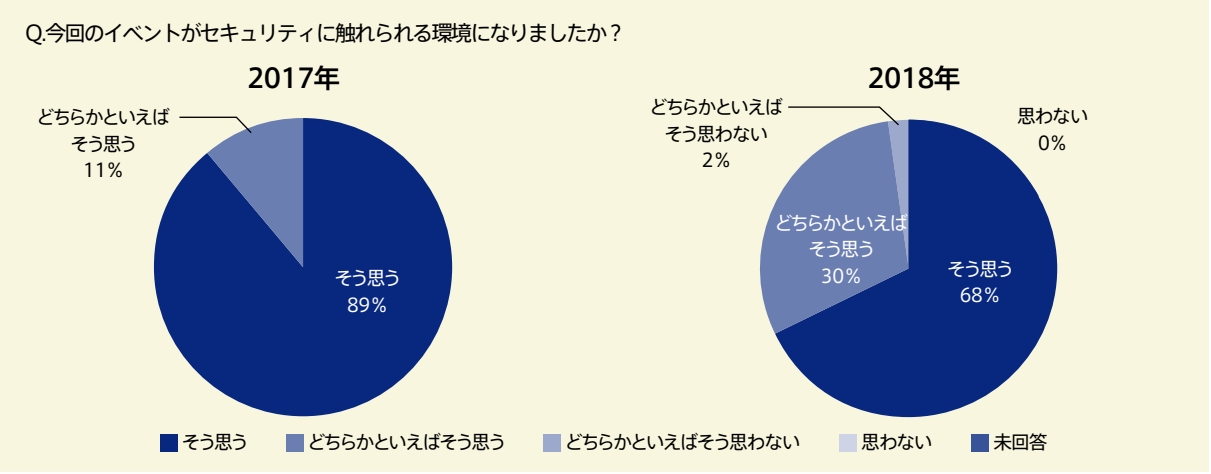
図表6. 道後ハンズオンセミナーアンケート結果



出所：セミナーアンケート結果より当社作成

図表7のように、セキュリティに触れられる場を求める声に対して、場作りが一定の効果を出していることも読み取れる。また、2018年からは、2017年の修了生が教えるというサイクルにも初チャレンジした。

図表7. 道後ハンズオンセミナーアンケート結果



出所：セミナーアンケート結果より当社作成

技術で社会に貢献することを目指す企業として、地域の場作りを通して、若者たちにも技術で社会に貢献できることを伝えたい。この活動によって、若年層がテクノロジーを悪用し加害者になるというケースの減少につなげるべく、我々企業が貢献できることを増やしていきたいと考えている。

地域の教育と地域の安心安全にこれまで貢献されてきた多くの方々の目線を大切にしながら、さまざまな方と協力し推進していきたい。

佳山こうせつ氏 プロフィール

富士通独自のセキュリティ技術者育成プログラムであるセキュリティマイスター認定制度を2014年に設立し、全社で推進。セキュリティ専門家の育成だけでなく、開発・運用現場の技術者のセキュリティスキル底上げを盛り込んだ育成プログラムの開発と実施、技術者発掘のためのセキュリティコンテストの主催や富士通製のサイバーレンジ（仮想演習場）であるCYBERIUMの開発にも力を注いでいる。
独立行政法人 情報処理推進機構 セキュリティセンター研究員、SecHack365トレーナー、SECCON実行委員、セキュリティキャンプ講師育成WG主査。
「『高度標的型攻撃』対策に向けたシステム設計ガイド」、「IPA テクニカルウォッチ：『攻撃者に狙われる設計・運用上の弱点についてのレポート』」を執筆。
(ISC)2 2016年アジア・パシフィック 情報セキュリティ・リーダーシップ・アチーブメント（ISLA）受賞。

中小企業におけるサイバーセキュリティ対策 ～官民連携における情報共有～

みずほ銀行 データマネジメント部　小山 昌樹

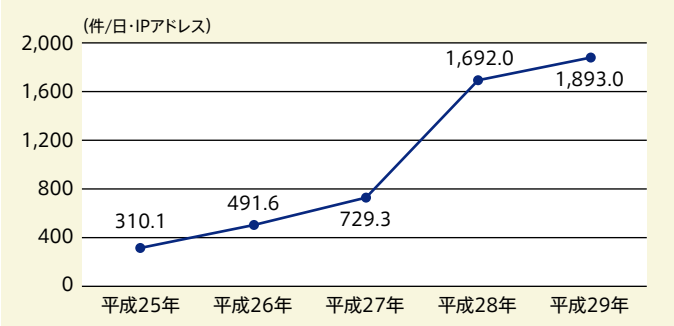
サイバー攻撃、大企業だけでなく中小企業も狙われている現状

情報通信ネットワークが社会広範に普及し、それにともないサイバー攻撃の対象となる企業・システムも増加し、連日のようにサイバー攻撃による情報漏洩、不正送金、BEC（ビジネスメール詐欺）[*1]の被害が報道され、その被害額も甚大となっている。米国では2013年10月から2016年12月までの約3年間のBECの被害額は約53億ドル、1件あたりの平均被害額は約13万ドルにも上り[*2]、日本国内においても2016年中の個人情報漏洩の発生件数は468件、1件あたりの平均想定損害賠償額は6億2,811万円に上っている[*3]。また別の調査においても日本企業のサイバー攻撃による平均損害額は2016年839万ドル、2017年は1,045万ドルと増加しており[*4]、サイバー攻撃によるリスクは年々高まっている。

サイバー攻撃の標的として狙われるのは大企業に限られず、むしろサプライチェーンに組み込まれ、大企業と連携し情報資産を扱う中小企業もまた、サイバーセキュリティ対策に大企業ほど注力できない分、格好の標的となっている可能性が高い[*5]。

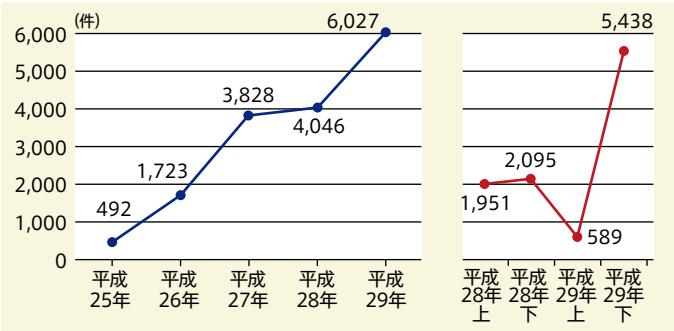
IPA（情報処理推進機構）が中小企業に対して実施したサイバーセキュリティに関するアンケートでは従業員100人以上300人未満の企業では19％、従業員100人未満の企業では7％がサイバー攻撃を受けたと回答しており[*6]、企業の規模が小さくなるほどに攻撃を受けたと回答している割合が少なくなっている。しかしながら警察庁の発表では2017年中、サイバー空間における探索行為は1日1IPアドレス1,893件に増加、サイバーインテリジェンス情報共有ネットワーク[*7]により情報共有された標的型メールも増加し、その手口については「ばらまき型」攻撃が全体の97％でそのうちおよそ90％の攻撃がインターネットでは非公開のメールアドレスに対する攻撃である[*8]という状況を考慮すれば、業種別の程度の差はあるにせよ中小企業の保有するIPアドレスに対する探索行為、非公開のメールアドレスに対する標的型メール等いわゆるサイバー攻撃が実際に行われている割合はさらに高く、攻撃を受けていないのではなく、受けていても把握できていない可能性が高いと考えられる。それを裏付けるように日本の企業では諸外国に比べてサイバー攻撃の被害経験は少ないものの、IT管理者自身が被害を把握できていないと認識している割合が世界平均に比べ約2倍も高くなっている[*9]。

図表1. センサーに対するアクセス件数の推移



（出典）警視庁「平成29年中におけるサイバー空間をめぐる脅威の情勢等について」

図表2. 標的型メール攻撃の件数の推移



（出典）警視庁「平成29年中におけるサイバー空間をめぐる脅威の情勢等について」

ではどのようにしたら自社がサイバー攻撃を受けていることを把握し、攻撃被害を未然に防げるのか。サイバー攻撃の手口は日々複雑化、巧妙化が進んでおり、それを防ぐための情報も膨大で多岐にわたり、一企業、一

組織だけで対抗し得るものではない。サイバー攻撃を行う犯罪者はダークウェブ等で情報交換や攻撃ツールを売買する等情報の共有化が進んでいるなか、サイバー攻撃を防ぐ側も企業間、同業種間、さらには業種の垣根を越えて連携し、情報共有体制を築いていかなければならない。次にそのために重要な役割を果たす情報共有の仕組みである官民連携の取り組みを、日本とサイバーセキュリティ分野でトップレベルである米国を中心にみていきたい。

日本におけるサイバーセキュリティの中小企業向け対策と官民連携による情報共有の取り組み

日本においてもサプライチェーンが標的となり、対策が追いついていない中小企業が狙われるリスクが高まっているとして、経済産業省が中小企業のトラブル対応支援を目的として行動計画を策定し、中小企業のサイバーセキュリティ対策支援に動き出している。また、多くの企業が集積しその99%が中小企業である東京都では、東京都・警視庁・中小企業支援機関、研究機関、セキュリティ企業等が連携し「東京中小企業サイバーセキュリティ支援ネットワーク（略称 Tcyss：ティーサイス）」が設立され、(1)サイバーセキュリティ意識の啓発活動、(2)サイバーセキュリティに関する情報共有、(3)サイバーセキュリティに関する相談への対応、(4)サイバーセキュリティ事案発生時の相互連携等を行っている。警視庁では区市町村、警察署、商工会等が相互に連携して事業者に対し、草の根レベルまできめ細かな支援を推進するために、市区町村との協定を締結しており、これまで31（5月31日時点）の協定を締結するなど、中小企業におけるサイバーセキュリティ対策のさらなる向上が期待されている。

また全国都道府県警察を中心にサイバー攻撃の標的となる重要インフラ事業者等との間で「サイバーテロ対策協議会」が設置されサイバー攻撃の脅威や情報セキュリティに関する情報共有等が行われているほか、先端技術を有する全国約7,700の事業者との間で情報窃取を企図したとみられるサイバー攻撃に関する情報共有を行う「サイバーインテリジェンス情報共有ネットワーク」が設置され、情報共有を行っている。

この他にも同じ業界の民間事業者同士でサイバーセキュリティに関する情報を共有するISAC（Information Sharing and Analysis Center：情報共有分析センター）が金融、情報通信、電力の3セクターで設置、情報共有が図られ、金融ISACでは専用のポータルサイトを通じ、日々のインシデントや脆弱性情報等をリアルタイムに共有し、また重要課題についてワーキンググループを設け協助の精神で取り組み、その知見や成果をアニュアルカンファレンスや地方のワークショップにおいて共有する等活発に活動を行っている。また官民連携を目的として重要インフラ分野における政府主導の情報共有の枠組みも構築されてはいるものの、米国のISAC（Information Sharing and Analysis Center：情報共有分析センター）が24セクター、さらにはそれを補完するISAO（Information Sharing and Analysis Organization：情報共有分析機関）が27セクター[*10]と比較するとカバーしている範囲も、情報共有の枠組みとしても日本はまだまだ十分とはいえない。調査においても日本で情報共有をしている企業の割合は約36%と世界の約54%と比べて低く、その理由としても情報共有の枠組みの整備、標準化ができていない、技術的な基盤が整備されていないという点があげられていることから[*11]情報共有する組織・枠組みの構築が遅れていることがわかるのではないだろうか。

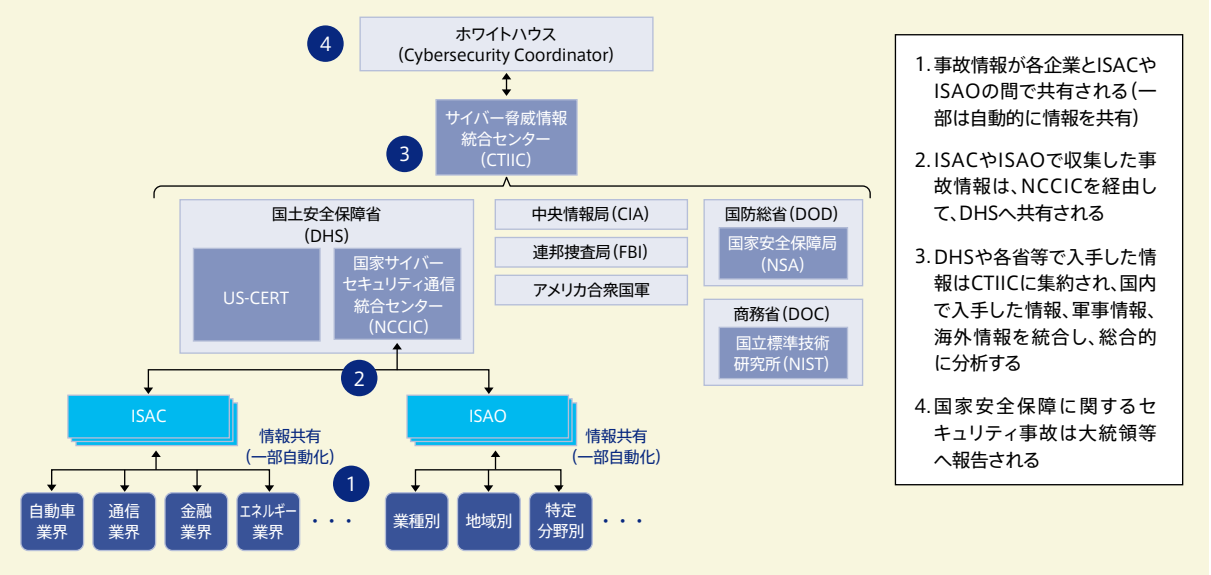
米国および諸外国における官民連携による情報共有の取り組み

米国においては情報共有の枠組みはさらに進んでおり、ここではその主要な組織であるDHS（Department of Homeland Security：国土安全保障省）を中心に官民連携の情報共有の取り組みについてみていきたい。

米国ではISACが金融・通信・電力等の重要インフラ事業者ごとに設置され情報共有が行われるとともに、重要インフラに限らずさらに広い範囲での情報共有を行うためにISAOが地域・分野ごとに設置され、これらの組織で収集された情報が国家サイバーセキュリティ通信統合センター（NCCIC）を経由しDHSへ共有する仕組みの構築を目指しており情報のペーパレス・自動化が進んでいる[*12]。そしてDHSで集約された情報とCIAやFBI、国防総省（DOD）等の他省庁で集約された情報はサイバー脅威情報統合センター（CTIIC）に一元的に集約され分析する体制が整備されている（図表3参照）。

また司法機関であるFBIでもサイバー攻撃に関連した情報共有の枠組みが作られておりFBI、DHS、民間企業

図表3. 米国の情報共有の仕組み



(出典)一般社団法人サイバーセキュリティ・イノベーション委員会(JCIC)「諸外国におけるサイバーセキュリティの情報共有に関する調査」

が情報共有・連携を図るための組織としてDSAC(Domestic Security Alliance Council:国内安全保障協議会)、またFBIが民間企業等との情報共有を行うためのパートナーシップとしてInfra Gardが整備されており、各種サイバー攻撃に関する情報共有を行う等して関係構築を図っており、いずれも官民連携の情報共有の組織として重要な役割を果たしている[*13]。

そして上記のような組織構築の大きな原動力の1つとなっているのが情報提供に関する法整備である。2015年に「サイバーセキュリティ情報共有法」が可決され、情報共有に関する違法性リスク等の懸念が払拭され、その後米国食品医薬品局(FDA)では医療機器の脆弱性を発見した場合60日以内に修正し利用者への通知を求め、ニューヨーク州金融サービス局ではセキュリティ事故検知72時間以内に監査当局に通知義務を課す等[*14]、情報共有に関する法整備が急速に進められている。

この流れは米国以外でも顕著であり、英国においても2018年1月英国政府が重要インフラ事業者に対し、インシデント時には適切なセキュリティ対策の有無の報告を求め、効果的なサイバーセキュリティ対策を怠っていた場合、最大1,700万ポンド(約26億円)以下の制裁金を科すことがあると発表している。また、英国では官民連携の情報共有プラットフォームとして、サイバーの脅威情報を国家サイバーセキュリティセンター(NCSC)に集約する「サイバーセキュリティ情報共有ネットワーク(CiSP)」を構築しており、7,000超の組織に属する1万2,000人のメンバーからリアルタイムで情報の提供可能な産業セクター・省庁を横断した情報シェアシステムとなっている[*15]。

またシンガポールにおいても2017年11月に通貨当局が米国のFS-ISACとアジア太平洋地域でのサイバー攻撃に対する情報共有の強化に向けて地域分析センターを設立したほか、2018年2月に、「サイバーセキュリティ法」が可決され、重要インフラ事業者がサイバー攻撃を受けた際は直ちにサイバーセキュリティ庁への報告を義務付け、違反した企業には10万シンガポールドル(約820万円)の罰金、2年以内の懲役が科せられる等の法規制が進んでいる。

社会参加の要件となっていく情報共有

これまで述べてきたように、米国を始めとするサイバーセキュリティ対策先進国では急速にサイバーセキュリティの情報共有に関する法整備が進められている現状があり、EUにおいてもGDPR(General Data Protection Regulation:EU一般データ保護規制)が2018年5月に施行されて、個人情報漏洩の検知後72時間以内に当局への通知が義務化され違反企業には高額の制裁金が科される等、世界的にもサイバーセキュリティの情報共有に関する法規制が進んでいる。

あらゆる企業がサイバー攻撃の標的となる得る現状において、適切な情報共有を推し進めていくことは、社会全体のサイバーセキュリティの強化となり、それがサイバー攻撃の被害の減少、社会全体の利益へとつながる。サイバーセキュリティの脅威に関する情報共有は今やサイバー攻撃を行う犯罪者に社会全体で打ち勝つために求められる必須条件であるだけでなく、サイバーセキュリティなくして成り立たない現在の社会への参加要件となりつつあるのである*16。

最後に、いくつか日本国内におけるサイバー攻撃の脅威情報に関しての情報共有組織、相談窓口等について紹介していきたい。

日本シーサート協議会は各企業のシーサート(CSIRT: Computer Security Incident Response Team)*17同士の連携、情報共有を行うと同時に、また新規にシーサートを構築する組織を支援する活動、各種ワークショップ等も行っている協議会であり、自社にシーサートがある企業、または構築を考えている企業にとっては有用な情報共有の場になると考えられる。

IPAのJ-CSIP(サイバー情報共有イニシアティブ)*18はサイバー攻撃に関する情報共有を行っている組織であり現在11の類似産業分野から228の組織(業界団体含む)が参加する情報共有体制が確立されている。また同じIPAのJ-CRAT(標的型サイバー攻撃特別相談窓口)*19は標的型攻撃に関する相談・情報提供を行う窓口となっており、標的型攻撃の被害に遭った際に、ケースによってはウィルス検体解析、攻撃・被害把握等のレスキュー活動も行っている。

JPCERT/CC*20はインシデント対応の相談を受け付けておりWebサイト改ざん、不正アクセス、マルウェア感染等の相談を受け付けているほか、これらのインシデント発生時にフィッシングサイトの閉鎖依頼、マルウェアを公開しているサイトへの対応依頼等も行っている。

また情報収集の面では、フィッシング対策協議会*21がフィッシング詐欺に関する事例情報の提供を行っており、現在観測されているフィッシングメールの情報が提供されているほか、JC3(日本サイバー犯罪対策センター)*22においてもサイバー犯罪の手口やマルウェア感染につながるメールの特徴等の情報提供を行っている。

社内の人材育成としては先にあげたIPAが中小企業の経営者、IT、情報セキュリティ担当者向けにセミナーを開催している*23ほか、警視庁のサイバーセキュリティ対策本部でも東京都内の中小企業や商工会等に向けたセミナーを行っているので活用し、社内のサイバーセキュリティの向上に役立てていくことができる。

ここで紹介させていただいたのはあくまで一部の組織や取り組みであり、この他にも有用なものが多数あると思うがまずはこれらを活用することから始め、サイバーセキュリティ対策の向上に役立てていただければ幸いである。

＊1 代表的な手口としては、攻撃者が企業の最高経営責任者等の電子メールアカウントをハッキング、またはそれになりすまし、偽の電子メールを職員に送信して不正な送金を行わせるものがある。
＊2 FBI　Public Service Announcement (May 04,2017)
＊3 JNSA　2016情報セキュリティに関する調査報告書
＊4 Ponemon Institute社とAccenture社によるCOST OF CYBER CRIME STUDY 2017
＊5 IPA　サイバー攻撃はサプライチェーンを狙う～サプライチェーンの情報セキュリティ対策～
＊6 IPA　2016年度中小企業における情報セキュリティ対策の実態調査～調査報告書～
＊7 警察と情報窃取の標的となるおそれの高い先端技術を有する全国の事業者との間で情報共有を行っている枠組み
＊8 警察庁　平成29年中におけるサイバー空間をめぐる脅威の情勢等について
＊9 A10 Networks Inc APPLICATION INTELLIGENCE REPORT
＊10 JETRO　米国サイバーセキュリティ対策の行方 2017.11.14
＊11 PwC　グローバル情報セキュリティ調査2017
＊12 JCIC　諸外国におけるサイバーセキュリティの情報共有に関する調査
＊13 www.dsac.gov / www.infragardmenbers.org
＊14 JCIC　諸外国におけるサイバーセキュリティの情報共有に関する調査
＊15 日本貿易振興機構　英国のサイバーセキュリティ体制の現状と課題
＊16 米食品医薬品局(FDA)は医療機器業界内のすべての利害関係者がISAOに参加し脅威情報の共有をすることを強く推進している。
Postmarket Management of Cybersecurity in Medical Devices　Dec,28,2016 14p(FDA)
＊17 シーサートとは、コンピュータセキュリティにかかるインシデントに対処するための組織の総称
＊18 https://www.ipa.go.jp/security/J-CSIP/index.html
＊19 https://www.ipa.go.jp/security/J-CRAT/index.html
＊20 https://www.jpcert.or.jp/
＊21 http://www.antiphishing.jp/
＊22 https://www.jc3.or.jp/
＊23 https://www.ipa.go.jp/security/seminar/seminar.html

今日から始める3つのセキュリティ対策

みずほ情報総研
銀行システムグループ決済・チャネル系システム事業部第3部 内野 充晃

企業が個人情報漏洩のインシデントを1回でも発生させてしまった場合、どの程度の損害賠償を請求されるかご存じでしょうか。JNSA（日本ネットワークセキュリティ協会）の報告によると約5億5千万円となっており、経営に与える損失は甚大です（図表1）。また、それらの事実はインターネット上に半永久的に残り続けるなど、まさにサイバーセキュリティが経営のトップリスクの1つとなっていることは周知のとおりです。

そのような環境下、自社WEBサイトの運営費に月額100万円の費用をかけられる企業と月額2～3万円の企業では、セキュリティ対策に投資できる規模が全く異なります。また、CISOと呼ばれる最高情報セキュリティ責任者をアサインし全社的なセキュリティガバナンス体制を構築できているような企業と、従業員の個人情報を扱う機会が多いという理由で総務の係長がセキュリティ担当を兼務したり、少しITに詳しいという理由でセキュリティ担当をアサインしているような企業では、セキュリティ対策に投下できる人的体力も大きく異なります。

本稿では、費用・体力に限界がある企業で、何から始めればよいか困っているセキュリティ担当の方に向け、今日から行動に移せる3つのセキュリティ対策をご紹介します。

図表1. JNSAの報告書に記載されている
セキュリティインシデントに関わる具体的な情報

漏洩人数	519万8,142人
インシデント件数	386件
想定損害賠償総額	1,914億2,742万円
1件あたりの平均漏洩人数	1万4,894人
1件あたり平均損害賠償額	5億4,850万円
1人あたり平均損害賠償額	2万3,601円

出所：特定非営利活動法人日本ネットワークセキュリティ協会（参考）
https://www.jnsa.org/result/incident/

1. 基本的な対策ができているか確認する

まずは、自社が基本的な対策ができているかチェックしよう。何が基本的な対策なのか自信がない場合は、独立行政法人情報処理推進機構（IPA）が公開している「中小企業の情報セキュリティ対策ガイドライン[*1]」のなかの「5分でできる！情報セキュリティ自社診断」（図表2）をおすすめする。25の設問に答えるだけで自社のセキュリティレベルを確認できる。

次に、自社のIT資産状況（OSやソフトウェアが最新状態か）はもちろんのこと、社員が保有しているIT機器（スマホやタブレット）の業務での使用状況をチェックしたほうがよい。

特に、昨今のコスト削減や業務効率化、働き方改革などにともない、業務データをクラウドで保管したり、コピー機・複合機がインターネットに接続され業者がリモートで保守していたり、業務連絡のため社員同士が個人所有のスマートフォンでSNSを利用していることも考えられる。また従業員1人ひとりが気をつけていたとしても、アルバイトや委託先業者の不注意や対策の怠りが大きな事故を招きかねず、従来からIT機器として認識してきたものだけではなく日常業務もふまえて洗い出そう。

2. 世の中で何が起きているのか情報収集する

次に、最新の攻撃手法や他社のセキュリティインシデントなどを情報収集し自社にとって脅威になりうるものがないか確認する。

攻撃手法については、IPAの「情報セキュリティ10大脅威」を一読してほしい（図表3）。2018年の10大脅威には、3位の「ビジネスメール詐欺による被害」や、4位の「脆弱性対策情報の公開にともなう悪用増加」など、昨年ランク外だった脅威が3つもある。このように脅威の大きなトレンドは担当者として把握しておきたい。

図表2. 付録「5分でできる!情報セキュリティ自社診断」

診断項目	No	診断内容	チェック				自社診断 パンフレットと対応しています
			実施している	一部実施している	実施していない	わからない	
Part1 基本的対策	1	Windows Updateを行うなどのように、常にOSやソフトウェアを安全な状態にしていますか?	4	2	0	0	P3 No1「脆弱性対策」を参照
	2	パソコンにはウイルス対策ソフトを入れてウイルス定義ファイルを自動更新するなどのように、パソコンをウイルスから守るための対策を行っていますか?	4	2	0	0	P3 No2「ウイルス対策」を参照
	3	パスワードは自分の名前、電話番号、誕生日など推測されやすいものを避けて複数のウエブサービスで使い回しをしないなどのように、強固なパスワードを設定していますか?	4	2	0	0	P3 No.3「パスワード管理」を参照
	4	ネットワーク接続の複合機やハードディスクの共有設定を必要な人だけに限定するなどのように、重要情報に対する適切なアクセス制限を行っていますか?	4	2	0	0	P3 No4「機器の設定」を参照
	5	利用中のウェブサービスや製品メーカーが発信するセキュリティ注意喚起を確認して社内共有するなどのように、新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか?	4	2	0	0	P3 No5「情報収集」を参照
Part2 従業員としての対策	6	受信した不審な電子メールの添付ファイルを安易に開いたり本文中のリンクを安易に参照したりしないようにするなど、電子メールを介したウイルス感染に気をつけていますか?	4	2	0	0	P4 No.6「電子メールのルール」を参照
	7	電子メールを送る前に目視にて送信アドレスを確認するなどのように、宛先の送信ミスを防ぐ仕組みを徹底していますか?	4	2	0	0	P4 No.7「電子メールのルール」を参照
	8	重要情報をメールで送る時は重要情報を添付ファイルにて書いてパスワード保護するなどのように、重要情報の保護をしていますか?	4	2	0	0	P4 No.8「電子メールのルール」を参照
	9	無線LANを利用する時は強固な暗号化を必ず利用するなどのように、無線LANを安全に使うための対策をしていますか?	4	2	0	0	P4 No.9「無線LANのルール」を参照
	10	業務端末でのウェブサイトの閲覧やSNSへの書き込みに関するルールを決めておくなどのように、インターネットを介したトラブルへの対策をしていますか?	4	2	0	0	P4 No.10「ウェブ利用のルール」を参照
	11	重要情報のバックアップを定期的に行うなどのように、故障や誤操作などに備えて重要情報が消失しないような対策をしていますか?	4	2	0	0	P4 No.11「バックアップのルール」を参照
	12	重要情報を机の上に放置せず書庫に保管し施錠するなどのように、重要情報の紛失や漏洩を防止する対策をしていますか?	4	2	0	0	P5 No.12「保管のルール」を参照
	13	重要情報を社外へ持ち出す時はパスワード保護や暗号化して肌身離さないなどのように、盗難や紛失の対策をしていますか?	4	2	0	0	P5 No.13「持ち出しのルール」を参照
	14	離席時にコンピュータのロック機能を利用するなどのように、他人に使われないようにしていますか?	4	2	0	0	P5 No.14「事務所の安全管理」を参照
	15	事務所で見知らぬ人を見かけたら声をかけるなどのように、無許可の人の立ち入りがないようにしていますか?	4	2	0	0	P5 No.15「事務所の安全管理」を参照

出所:独立行政法人情報処理推進機構(一部作図)　https://www.ipa.go.jp/files/000055517.pdf

ビジネスメール詐欺は、2017年12月に大手航空会社への振り込め詐欺がニュースに大きく取り上げられたのでご記憶されている方も多いだろう。このようなTVや新聞で扱われるセキュリティインシデントは、最初のうちはセンセーショナルに報道されるが、ほとぼりが冷めるにつれ徐々に沈静化し、原因究明が発表される頃にはすっかり世間の関心が薄くなり報道の頻度も下がる。しかし、まさにその原因や再発防止策こそが、自社の対策に役立つものであるため、全容が公表されるまでフォローしてほしい。またTVや新聞報道に至らずインターネットニュースでしか取り上げられないインシデントについても、冒頭に紹介した「情報セキュリティインシデントに関する調査報告書」などにまとめられている。

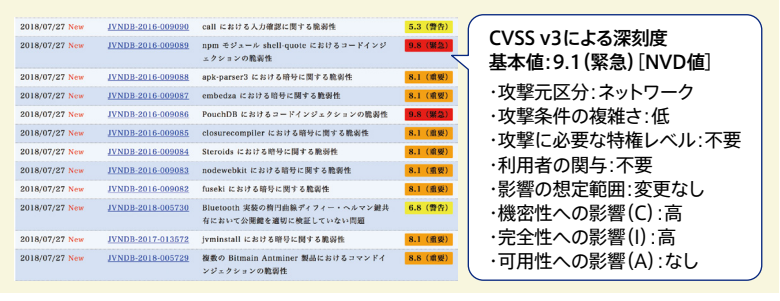
図表3. 2018年情報セキュリティ10大脅威について 前年との比較

順位	組織	昨年順位
1位	標的型攻撃による被害	1位
2位	ランサムウェアによる被害	2位
3位	ビジネスメール詐欺による被害	ランク外
4位	脆弱性対策情報の公開に伴う悪用増加	ランク外
5位	脅威に対応するためのセキュリティ人材の不足	ランク外
6位	ウェブサービスからの個人情報の摂取	3位
7位	IoT 機器の脆弱性の顕在化	8位
8位	内部不正による情報漏洩	5位
9位	サービス妨害攻撃によるサービスの停止	4位
10位	犯罪のビジネス化（アンダーグラウンドサービス）	9位

出所:独立行政法人情報処理推進機構(一部作図)
https://www.ipa.go.jp/security/vuln/10threats2018.html

さらに、少々手間はかかるが、「JVN iPedia(脆弱性対策情報のデータベース)」(図表4)は毎日国内外の数十件の脆弱性情報が更新されており、最新情報が入手できる。数十件と聞くと敬遠したくなるが、攻撃条件の複雑さなどから脆弱性の深刻度を「緊急」、「重要」、「警告」等で分類し、影響を受ける製品名やバージョンも明記されており、

図表4. JVN iPediaの脆弱性情報



出所:Japan Vulnerability Notes(一部作図)
https://jvndb.jvn.jp/

自社システムへの影響を迅速に確認できる。さきほど紹介した「情報セキュリティ10大脅威」の4位に「脆弱性情報の公開にともなう悪用増加」があがっているとおり、公開された脆弱性は即座に悪用される危険があるため、緊急度の高いものだけでも速やかに確認しておきたい。

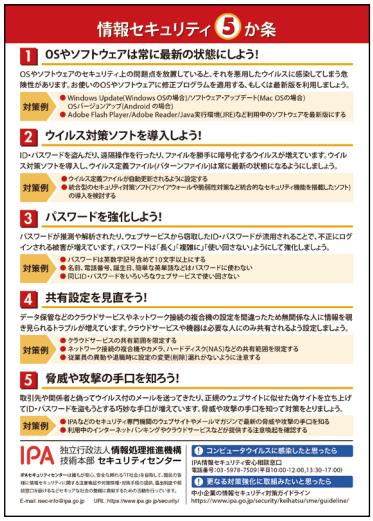
3. 自社にあった対応策を考える

3点目は、自社の弱みや攻撃のトレンドをふまえた対応策を立てることである。

検討するうえで有用なガイドラインとして、前述の「中小企業の情報セキュリティ対策ガイドライン」をすすめたい。そのなかの「情報セキュリティ5か条」(図表5)は、企業や個人などに最低限求められるセキュリティ対策が簡潔にまとめられている。

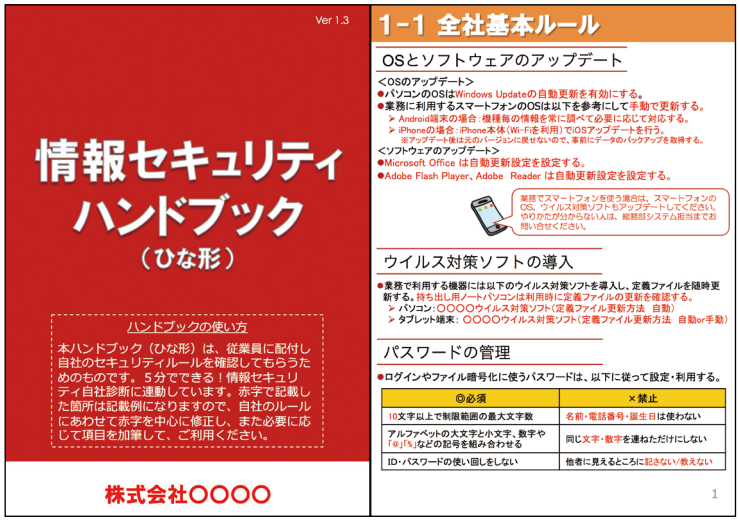
さらに従業員に対し、自社のセキュリティルールを周知徹底するための「情報セキュリティハンドブック(ひな形)」も提供されている(図表6)。ただし、ここで注意したいのは、ひな型の表紙の名前を自社の社名に変えるだけにしないことだ。自社の社員が読んで理解・実践できるものなのか確認し、無理であれば代替策への差し替えや、補足説明を追加しよう。

図表5. 情報セキュリティ5か条



出所:独立行政法人情報処理推進機構
https://www.ipa.go.jp/files/000055516.pdf

図表6. 情報セキュリティハンドブック(ひな形)



出所:独立行政法人情報処理推進機構
https://www.ipa.go.jp/files/000055529.pptx

たとえば、パスワードにつき「10文字以上英数字記号を組み合わせ名前や誕生日などは使わない」、「同じものは使い回さない」等をルールに定めたところで、実際に守らせることはなかなか難しい。そのような場合は図表7のように、記憶もできて、他人に推測されない強固なパスワードの作成手順を追加してはどうだろうか。

そして、万が一インシデントが発生した場合に被害を最小限にとどめられるよう、ぜひインシデント対応マニュアルも作っておくとよい。ただし、最初から細いフローを準備しておくというより、まずは問題が起きたときにスムーズに動けるように、社内で以下のような会話はしておこう。

たとえば、「どんなインシデントが起こりうるのか」、「誰に迷惑がかかるのか。お客さまか。取引先か。従業員か」、「どんな時には即刻、上司にエスカレーションしなければならないのか」、「インシデント調査を依頼でき

図表7. 強固なパスワード作成の例

~自分の好きな歌をパスワードにしてみよう!~

STEP 1 歌の歌詞を決める

どんぐり　ころころ　どんぶりこ
おいけに　はまって　さあ　たいへん
どじょうが　でてきて　こんにちは
ぼっちゃん　いっしょに　あそびましょ

STEP 2 頭文字を抜き出す

dkdohstddkbia

STEP 3 1文字おきに大文字にする

DkDoHsTdDkBiA

STEP 4 文字の一部を記号や数字に置き換える

例:o→0、s→$、i→1
DkD0H$TdDkB1A

STEP 5 使うサイトによって、頭か末尾にサイトの略称を変える

例)
保険組合の場合
「HK」+「DkD0H$TdDkB1A」=「HKDkD0H$TdDkB1A」
ニュースサイトの場合
「NS」+「DkD0H$TdDkB1A」=「NSDkD0H$TdDkB1A」

(作成)みずほ情報総研

る会社はどこか。費用はどれくらいか」、「弁護士への相談費用はどれくらいか」、「社外・社内とのやり取りは誰が窓口になるのか」などである。

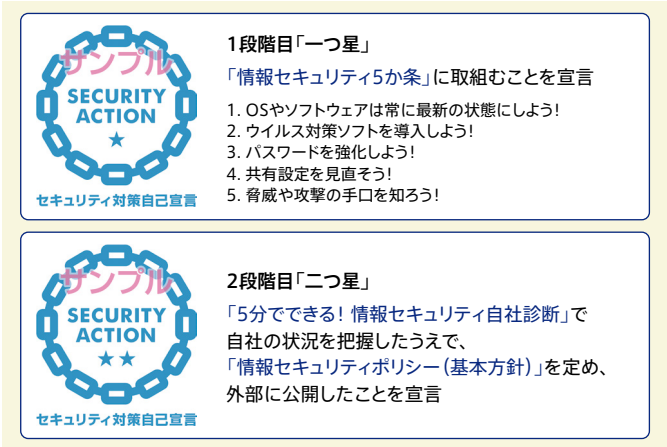
そして大切なのは、これらガイドラインやマニュアルは一度作成して終わりではなく、内容を陳腐化させないよう定期的に見直しを行わなければならない。3月18日は「サイバーの日」となっている。たとえば、そのようなタイミングを利用するのも一案である。

最後に

自社の特性に則した課題の確認や対策立案ができた後は、せっかくなので、IPAが推進するセキュリティアクションを宣言してはいかがだろうか（図表8）。セキュリティアクションとは、企業自らの情報セキュリティ対策への取り組みを自己宣言する制度である[*2]。宣言することでセキュリティアクションのロゴを自社のホームページや名刺に記載できる。それにより自社のセキュリティへの取り組み姿勢のアピールにつながり、また保険会社が提供するサイバー保険の保険料割引やサービスデザイン推進協議会が推進するIT導入補助金制度[*3]の申請要件のひとつにもなっている。

本稿では今日から始めるセキュリティ対策について紹介した。これらをヒントに具体的な行動に移してもらえれば幸いである。

図表8. IPAが推進するSECURITY ACTION



出所：独立行政法人情報処理推進機構
https://www.ipa.go.jp/security/security-action/it-hojo.html

＊1 https://www.ipa.go.jp/security/keihatsu/sme/guideline/index.html
＊2 https://www.ipa.go.jp/security/security-action/sa/index.html
＊3 https://www.it-hojo.jp/overview/

ケニアビジネスに有効なアプローチ
～経済実態を捉えた新たなビジネスモデル～

みずほ銀行 国際戦略情報部　調査役 芹澤 暢宏

進出地としてのケニア共和国

“ケニア”と聞いて、多くの日本人が最初に思い浮かべるものは、広大なサバンナに暮らす野生動物や色鮮やかな民族衣装を纏ったマサイの戦士など、豊かな自然や観光のイメージが中心となるであろう。一方、アフリカビジネスに関わるものが聞くと、思い浮かべるイメージは大きく異なる。

ケニアは人口約4,700万人（国連は2030年に6,700万人、2045年に8,800万人になると予想）、国内総生産（GDP）795億米ドル（サブサハラ・アフリカで5番目の経済規模）と地域経済を牽引する国である。インド洋に面し、天然の良港であるモンバサ港を擁することから、東アフリカの内陸国にとっては重要な物流ハブ国にもなっている。

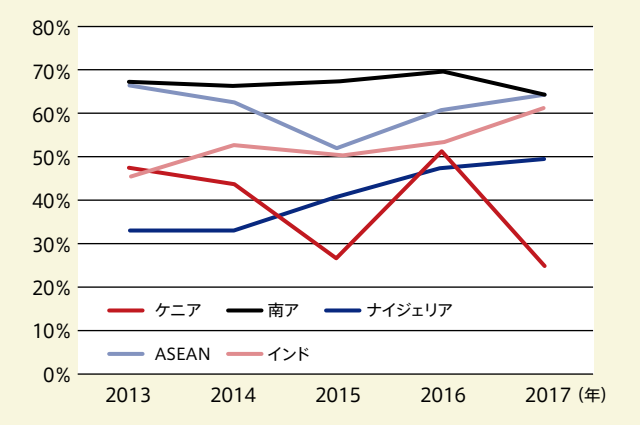
また、公用語として英語が広く通じ、世界銀行の「Doing Business 2018」でも80位にランクされており、事業環境は良好といえないまでも他の新興国と比較して劣後するものではない（例：インドネシア72位、南アフリカ82位、インド100位、ナイジェリア145位、ミャンマー171位）。

なお、ケニアはサブサハラ・アフリカにおける我が国最大のODA受益国であり、初めてのアフリカ開催となったTICAD VI[*1]が首都ナイロビで行われるなど、日本・ケニア政府は良好な関係を築いている。

成長著しい東アフリカ地域のハブ国としてのポテンシャル、良好な二国間関係などから、アフリカビジネスを展望する日本企業にとって、ケニアは有望な進出候補地となっている。外務省の「2018年海外在留邦人数調査統計」（2017年10月時点）によると、サブサハラ・アフリカでは南アフリカに次いで2番目に多い、54の日系企業が進出している。また、日本貿易振興機構（JETRO）がアフリカの日系企業を対象に毎年実施する「今後の注目国」アンケートでも、2015年度調査から3年連続の第1位となっている。

近年は経済成長にともない中間層の台頭が注目されており、日本企業においても、港湾整備・地熱発電といったインフラビジネスのみならず、BtoCの市場を狙った進出も増えてきている。しかしながら、年間5～6％の順調な経済成長とは裏腹に、多くの日系企業がケニアでの事業に苦戦をしている。図表1はJETROが各国の日系企業に対し実施した業績に関するアンケート結果を比較したものである。これによると、ケニアに進出する日系企業の半数以上が赤字であり、他地域と比較しても、利益水準が大きく劣後している。中間層の台頭が叫ばれるなか、高付加価値製品・サービスを得意とする日本企業がケニアビジネスに苦戦しているのはなぜか。そこには、経済主体が統計上捕捉困難なインフォーマルセクターに存在するというケニアの経済実態が大きく関係している。ケニアでは、インフォーマルセクターが経済活動の大半を占め、フォーマルセクターの市場規模は想定されているよりも小さく、中間層をビジネスの対象とするだけでは赤字に陥りやすくなる。本稿ではその理由に関する仮説とビジネスチャンス発掘のヒントを示してみたい。

図表1．現地日系企業における黒字企業（営業利益）の割合



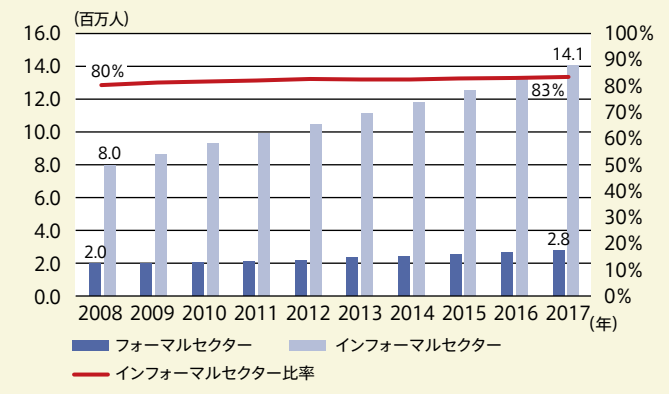
（出典）JETROアフリカ進出日系企業実態調査およびアジア・オセアニア進出日系企業実態調査より、みずほ銀行国際戦略情報部作成

ケニアの経済実態

インフォーマルセクターとは経済学用語で、経済活動が行政の指導下で行われておらず、国家統計などの正式な記録に表れにくいものをいう。職業としては、例えば、小規模農家、個人商店主（法人格のない企業）、季節・日雇い労働者などが該当する。消費活動もスーパーマーケットやショッピングモールといったモダントレードではなく、市場やKioskと呼ばれる小規模商店といったトラディッショナルトレードで食料品や生活用品などを購入する。多くが低所得層であり、銀行口座も持っていない。インフォーマルセクターの経済比率が高いことは発展途上国の経済構造の特徴であるが、ケニアも同様の状況となっている。

図表2はケニアにおけるフォーマル／インフォーマルセクター別の就労人口の推移を表したものである。統計によると、ケニアでは就労人口の8割以上がインフォーマルセクターの仕事に従事していることがわかる。また、一般的には、国家の経済成長にともない、インフォーマルセクターの比率は下がっていく傾向にあるものだが、ケニアではむしろ、インフォーマルセクターの比率が漸増している。ケニアは過去10年、おおむね年率5%前後の順調な経済成長を遂げてきており、1人あたりGDPも2倍弱まで拡大（970米ドルから1,700米ドル）したものの、現状、フォーマルセクターへの移行局面にはないことがわかる。ケニアでは生産年齢人口が年平均成長率3.4%の水準で増加（2010～2015年）しているが、この増加分をフォーマルセクターが吸収できるほどの労働集約型産業が育っておらず、インフォーマル経済が主体となる経済構造は今後も継続すると考えられる。

図表2. ケニアにおけるフォーマル/インフォーマルセクター就労人口推移

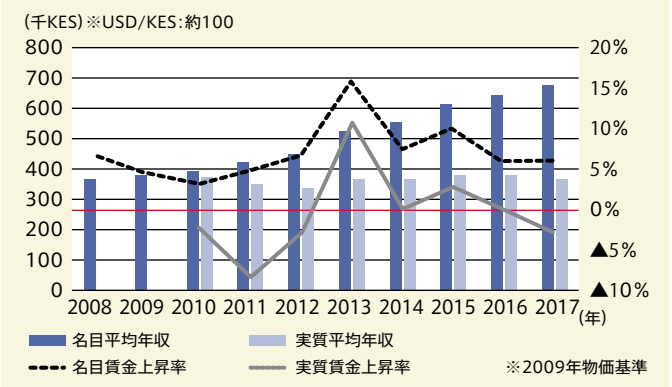


（出典）KNBS Economic Surveyより、みずほ銀行国際戦略情報部作成

図表3は、ケニアにおけるフォーマルセクターの賃金水準の推移を表したものである。これによると名目賃金は2009年から2017年までの9年間で約1.8倍に増加しているものの、実質賃金は約4%のマイナスとなっている。すなわち、物価の上昇に賃金の上昇が追いついておらず、これまで中間層が台頭しているといわれてきたものの、実際には購買力が拡大しているとはいいがたい状況がわかる。

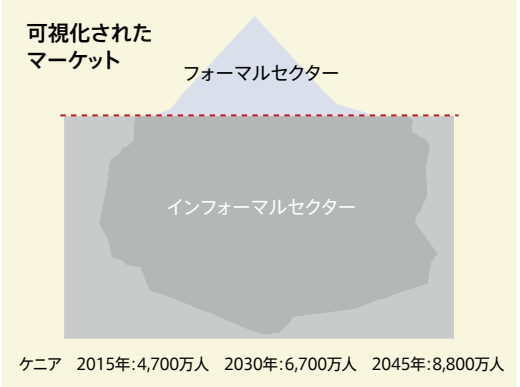
これまで、ケニアビジネスに携わる企業は、可視化された市場であるフォーマルセクター向けのビジネスを対象としてきた。しかしながら、2つの統計データが示すように、フォーマルセクターはボリュームゾーンになりえず、中間層の存在もいまだ限定的であるなか、フォーマルセクターを狙ったビジネスはパイの取り合いとなり、激しい競争にさらされていることがうかがえる。例えば、中間層の増加を見込み、多店舗展開を進めてきた地場大手スーパーマーケット業界では経営破綻する企業も出てくるなど、軒並み不調に陥っている。また、ケニアだけの事例ではないが、Nestléは2015年に、「アフリカは次のアジアではなかった（中間層の規模は小さく、

図表3. ケニアにおけるフォーマルセクターの賃金水準



（出典）KNBS Economic Surveyより、みずほ銀行 国際戦略情報部作成

図表4. ケニアの経済実態イメージ



（出典）UN World Population Prospectより、
みずほ銀行国際戦略情報部作成

想定よりも育っていなかった)」として、中間層向けに注力していた戦略を低所得層向けに方針転換している。なお、当社の2017年度決算報告には、サブサハラ・アフリカ地域の売上が2桁成長していると記されており、戦略転換以降、事業が好調であることがうかがえる。中間層の拡大を見込みケニアに進出した日本企業も、想定よりもフォーマルセクターの市場は小さく、前述のJETROのアンケート結果にあるように採算確保が困難な状況にあると考えられる。

中間層の成長が限定的であるなか、ケニア市場で十分な売上規模を確保するためには、ボリュームゾーンであるインフォーマルセクターをビジネス対象とする必要があるが、統計にも表れず、銀行口座すら持っていない低所得者層が大半であり、企業にとってはマーケティングや与信が困難であったことから、従来ビジネスの対象として捉えることが難しかった。

ケニアにおける新たなビジネスモデル

こうした市場環境へのアクセスを切り開いたのが、ICT、IoT、AIなどテクノロジーの進展とともに、ケニアに広く普及するモバイルプラットフォームを活用したビジネスモデルである。

図表5. 携帯電話・モバイルマネーサービスの普及率

	2015年	2016年	2017年	備考
携帯電話加入件数(百万)	37.72	38.98	42.82	人口比約85%
モバイルマネー利用者数(百万)	28.64	34.96	37.39	人口比約75%
モバイルマネー取引額(B KES)	2,816	3,355	3,638	GDPの約半分
モバイルマネー代理店数(千)	144	166	182	日本のコンビニ数5.5万

(出典)ケニア中央銀行ウェブサイト、ケニア通信局「SECOND QUARTER SECTOR STATISTICS REPORT」より、みずほ銀行国際戦略情報部作成

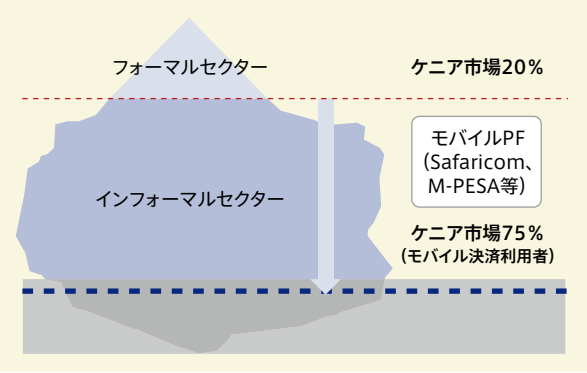
図表5のとおり、ケニアでは携帯電話が広く普及しており、インフォーマルセクターに属する低所得者も多くが所有している。また、銀行口座を持たないインフォーマルセクターの人々にとって、M-PESA[*2]に代表されるモバイルマネーサービスは重要な決済手段であり、これも広く利用されている。すなわち、国内に広く普及する携帯電話やモバイルマネーのプラットフォームの活用が、インフォーマルセクターへアクセスする鍵となっている。図表6のイメージ図のとおり、これまで可視化されたケニア市場はわずかであったが、モバイルプラットフォームを活用することで、ビジネスの対象が大きく拡大する可能性を秘めているのである。

実際、近年ケニアではモバイルプラットフォームを活用した新たなビジネスが生まれてきている。そして、この新たなビジネスモデルの担い手は、ケニアの経済実態を理解し、それに沿ったアイデアを持つ地場のスタートアップ企業である。図表7はケニアのスタートアップビジネスの一例をまとめたものであるが、いずれの企業も、モバイルプラットフォームを活用し、これまでアクセスの難しかったインフォーマルセクターに属する消費者や事業主を相手としている。一部の企業はモバイル決済の支払い履歴を与信判断に活用するなどして低所得者層の信用リスクを低減している。この潮流は多様なビジネス分野に広がりつつある。

地場のスタートアップが興るなかで、インフォーマルセクターへの市場アクセスを狙い、これら企業との提携を始める外国企業も現れてきている。例えば、Kioskなどのインフォーマルリテイラー向けに日用品のEコマース・配送サービスを提供するSokowatch社は創業4年で5,000以上の小売店に商品を配送するまでに成長したが、現在UniliverやP&Gなどのグローバルプレイヤーが当社のサービスを活用し、Kioskに自社製品を販売している(メーカーが一定の手数料をSokowatch社に支払う)。

また、日本企業からも注目を集め始めており、2017年11月に豊田通商がSendy社(客待ち中のバイクタクシーや空荷のトラックを活用した配送サービス事業)に、2018年5月には三井物産がM-Kopa Solar社(未電化地域の家庭向け太陽光発電システムの割賦販売事業)にそれぞれ出資するなど、わずかで

図表6. モバイルプラットフォームを活用したビジネスアクセスのイメージ



(出典)みずほ銀行国際戦略情報部作成

図表7. ケニア発スタートアップ企業の事例

分野	企業	事業内容
卸売	Sokowatch	Informal Retailer（キオスク等）向けFMCGのEコマース（SMS/アプリ）を開発・運営。配送は地場Agentに委託し、24時間以内に配送。Uniliver、P&G、Nestlé、GSKなどのFMCGグローバル大手が当社を通じて販売。購入履歴から今後の仕入れ予測もでき、消費動向をメーカーに提案しマーケティングに役立てることも可能。現在タンザニアでも展開
卸売	Twiga Foods	農家とInformal Retailerをつなぐマッチングアプリケーション・配送・信用販売を提供。決済はモバイルマネー。IBMと協力して、支払いデータをもとにしたキオスク向けのマイクロファイナンス事業を開始
小口配送	Sendy	客待ち中のバイクタクシーや空荷のトラックを活用した配送サービスを提供。利用者は専用のアプリで集荷場所と配達先を指定し、近隣のドライバーが集荷。2017年11月、豊田通商は子会社の仏CFAOを通じて出資
家庭用電力	M-Kopa Solar	未電化地域の家庭向けに太陽光発電システムの割賦販売を行う。支払いはモバイルマネーで、利用者は日払い可能。入金が確認できない場合、遠隔操作でシステムを停止する。テレビも販売。ウガンダ、タンザニア、ガーナに拡大し、60万家庭に普及。2018年5月、三井物産は当社への出資を発表
家庭用ガス	Paygo Energy	Pay-As-You-GOガスボンベデリバリー。利用者はオンラインで必要なガスの量を選択、支払うと、ガスボンベが配送される。スマートメータで遠隔ロック可。また、ガスの残量を自動で管理。一定残量になると、当社に通知が行き、次のボンベが配送される
医療保険	M-TIBA	M-PESAによる少額医療積立サービス。Safaricomがパートナーと開発。怪我・病気の際は提携病院で受診。支払いはM-Tibaのモバイルアカウントから。病院も確実に費用請求できる
教育	Kytabu	出版社と提携し既存の教科書をデジタル化し販売。利用者は必要なページ/期間を選択し、購入することができる
農業	ACRE Africa	干ばつなどの天災にあった小規模農家向けモバイル保険サービス。同社の気象観測所と農学アルゴリズムに基づき、農家へ保険金を支払う。農家は種や農薬を購入する際に商品に貼り付けられたカード番号をSMS送信し保険登録。SMS送信された情報から位置が特定され衛星ピクセルが割り当て。シンジェンタ財団が出資

（出典）JETRO、各社ホームページなどより、みずほ銀行国際戦略情報部作成

はあるが一部の日本企業も地場スタートアップ企業との提携を行っている。

テクノロジーとモバイルプラットフォームを活用しインフォーマルセクターにアクセスする地場スタートアップ企業が現れ、日本を含む一部のグローバル企業が提携を始めているなか、有望なスタートアップ企業を選定し、パートナーとして活用することが、今後のケニアビジネスに有効なアプローチの1つとなると筆者は考える。一般的にスタートアップ企業との提携は事業化に至らないリスクもあり、多くの企業にとってためらいがちとなる手段であるが、仮に短期的なマネタイズが困難であったとしても、インフォーマル市場参入に必要な情報・ノウハウを習得することに意義あると考えられる。

最後に

現在約12億人のアフリカの人口は2050年には約30億人にまで増加するといわれており、中・長期的に視野に入れるべき巨大市場である。一方、総じて人件費が高いため工業化のハードルが高く、先進国やアジア諸国が経験してきた既存の経済成長モデルが当てはまらないことから、グローバル企業にとって、アフリカ市場の攻略は手探りの状況である。これまでケニアの経済実態と市場参入に対する新たなアプローチ方法を紹介してきたが、経済の大部分をインフォーマルセクターが占める構造は、ケニアのみならず、南アフリカやモーリシャスなど一部の国を例外として、サブサハラ・アフリカ市場全体の傾向となっている。

ケニアは世界的に見ても、いち早くモバイルマネーの普及が進んだ国であり、現在ではそのプラットフォームを活用したスタートアップビジネスが台頭している。これらの新たなサービスは、近隣国にも波及しており、ケニアはまさにアフリカのイノベーションセンターとしての地位を確立している。このようななか、“先進国のロジックが通用しない” アフリカ市場攻略の実験場という観点でも、ケニアは大きく注目されている。例えば、Google、Microsoft、Oracleなどといった名だたるテック企業がケニアで人材開発やインキュベーション支援を行っている。IBMは地場スタートアップとともにマイクロファイナンス事業に参入している。また、Facebookのマーク・ザッカーバーグ氏やAlibabaのジャック・マー氏などの著名IT起業家も相次いでケニアを訪問している。

ケニアビジネスでスタートアップを活用することは、ケニアのインフォーマルセクターのみならず、アフリカ市場攻略の鍵となる可能性を秘めているのである。

＊1 Tokyo International Conference on African Developmentの略。アフリカの開発をテーマとする国際会議。1993年以降、日本政府が主導し、国連、国連開発計画、アフリカ連合委員会、世界銀行と共同開催。TICAD Vまではすべて日本開催であったが、2016年のTICAD VIから3年ごとにアフリカ・日本の相互開催となった。2019年8月28～30日にかけて、第7回であるTICAD VIIが横浜で開催予定

＊2 ケニアの通信キャリア最大手Safaricom（Vodafoneグループ傘下）が2007年から提供するモバイルマネーサービス。M-PESAのシェアは78%であり、ケニアのモバイルマネー市場で圧倒的な存在感を持つ。利用者はM-PESAの代理店で開設した口座に現金をチャージし、モバイル端末（所謂“ガラケー”も対応）から、送金金額と暗証番号を送金相手にSMSで送る。SMSを受信した相手は当該画面と暗証番号を代理店で提示することによって現金を受け取ることができる。2008年から隣国タンザニアでもサービスを開始しており（Vodafoneグループの南アフリカに本社を置くVodacomが提供）、同国でも40%超のトップシェアを持つ

政権交代後のマレーシアにおける当面の注目点

みずほ総合研究所 アジア調査部　主任研究員 稲垣 博史

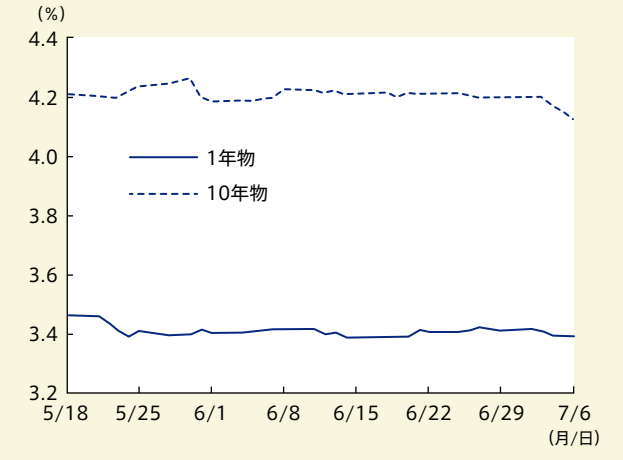
2018年5月9日の総選挙で、1957年のマレーシア独立以来政権を担ってきた国民戦線が敗北し、希望連盟が歴史的勝利をおさめた。希望連盟を率いるのは、1981年から2003年まで国民戦線の代表として首相を務めたマハティール氏で、このたび首相として再登板した。市場経済を基本とする経済政策は維持されることから、今後の経済について大きく見方を変える必要はないが、いくつか不透明な要素があることも事実だ。以下、3つの重要問題に注目してみた。

隠し債務問題：過度な心配は不要

マレーシア連邦政府の債務は、2017年時点で6,868億リンギ（GDP比50.7％）とされてきた。ところが、マハティール首相は5月21日に、実際には1兆リンギを上回ると主張。リム財務相は5月24日に、正確には1兆873億リンギ（GDP比80.3％）であると発表した。差し引き4,005億リンギもの隠し債務があったということで、このニュースは一時マスコミを大いににぎわせたが、債券市場は驚くほど無反応で、その後の国債金利はほぼ横ばいで推移した（図表1）。この隠し債務問題は、いったいどのように理解すればいいだろうか。

まず債務の増加額のうち、1,991億リンギ（GDP比14.7％）は公営企業等に対する保証債務だという。しかし、連邦政府だけでなく公営企業などを含む公的債務の内訳として、保証債務はかねてから開示されていた。2016年時点で1,772.5億リンギ（GDP比14.4％）と発表されていたから、2017年になってひどく大幅に増えたわけでもない。つまり、保証債務を公的債務から連邦政府債務に括り直したというだけの話で、これはまったく隠し債務ではない。

図表1. 国債金利（2018年）



（資料）CEIC Dataより、みずほ総合研究所作成

次に残りの2,014億リンギ（GDP比14.9％）は、PPP*プロジェクトへのリース料支払いだという。これについては、政府が詳細を明らかにしていないので実態がよくわからないが、ある財政問題の専門家は「将来にわたるリース料の支払い額を、債務として認識したということだろう。リース料の支払い自体は隠されていたわけではないと思われる」との見方であった。そうだとすれば、これも隠し債務とまで呼べるかは疑問だ。

まとめると、隠し債務問題のうちリース料部分の真相ははっきりしないが、現時点で隠し債務があったと決めつけるのは行き過ぎだろう。

では、政府はなぜ債務問題が深刻といい始めたのだろうか。希望連盟が選挙公約としていた、物品・サービス税（GST）廃止や燃油補助金復活といったばらまき政策実現のためには財源が必要だ。前政権下で進んでいた各種インフラ投資プロジェクトの見直しが有力な財源だが、「ばらまきのために見直す」と説明すれば、インフラ投資プロジェクトに関わる国内の利害関係者や、中国（東海岸鉄道の建設を受注）・シンガポール（クアラルンプールとシンガポールを結ぶ高速鉄道を計画）といった関係国政府から批判を浴び、場合によっては

違約金が発生する。「債務問題が深刻なために見直す」と説明した方が、理解を得られやすいと判断したのではないか。あるいは、すべての公約を実行できなくとも、債務問題を理由にすれば大きな批判を浴びずに済むと考えたのかもしれない。

汚職問題：捜査は順調だが結審まで時間を要する

国民戦線が国民の支持を失った直接の原因は、ナジブ前首相に、国営投資会社の1MDB（1Malaysia Development Berhad）にまつわる汚職疑惑が生じたことであった。ナジブ氏サイドにわたった金額は26億リンギ（ないし7億米ドル）としばしば報じられるが、1MDBから失われた金額は45億米ドルとの報道もある。この問題は、今後の火種となりうる要素をはらんでいる。例えば、疑惑解明がうまく進まなければ、政府は有権者の支持を失う恐れがある。また、疑惑を突きつけられたナジブ氏の支持派が反発し、大規模デモ等が発生すれば政治的に混乱するかもしれない。

政府は、5月12日にナジブ夫妻に対して出国禁止命令を出し、5月16日にナジブ氏宅などの家宅捜索を行った。そして、先述の26億リンギと比べればわずかな金額ではあるが、4,200万リンギを不正に受け取ったとして7月3日にナジブ氏は逮捕され、翌4日に起訴された。懸念されたナジブ派の反発については、7月4日に高裁前で抗議活動があったと報じられているものの、参加人数は「100人以上」と報じられており、さほど大規模なものではない。

このように現時点では、大きな混乱を招くことなく、捜査は順調に進んでいると評価できるのではないか。もっとも、資金の流れは複雑で全容解明は容易ではないもようで、結審までは数年を要するとの見方が多い。

後継者問題：現時点では評価が難しい

マハティール首相は、かねてからアンワル元副首相に首相職を禅譲するとしてきた。首相が93歳と高齢なだけに、長く首相を続けることはそもそも難しい。アンワル氏は、5月の総選挙時点で収監されていたため立候補できなかったが、国王の恩赦により選挙後に釈放された（図表2）。今後いずれかの段階で、予備選挙を経て国会議員に復帰するとみられる。

ただし、アンワル氏へのバトンタッチがいつになるか、現時点でははっきりしない。それどころか、そもそも、本当に禅譲されるか疑問視する向きすらある。アンワル氏はかつて副首相職をマハティール氏に解任されたことがあり、両者は長らく政敵の関係にあったからだ。市場経済を重視するとされるアンワル氏に対し、マハティール氏は首相再任後に新しい国民車構想を語ったりするなど政府の役割を重視する傾向にあり、政策的にも対立する可能性がある。

図表2. アンワル氏に関するこれまでの経緯

1993年12月	マハティール政権の副首相に就任
1998年9月	マハティール首相により解任、逮捕
2004年9月	罪状のうち「同性愛行為」は最高裁が無罪、職権乱用罪では有罪判決
2013年5月	野党連合を率いて総選挙に臨む
2015年2月	2008年の同性愛行為で有罪確定、収監
2017年7月	野党連合が将来の首相候補に指名
2018年5月	国王の恩赦で釈放

（資料）「釈放「アンワル氏が次期首相」マハティール氏、約束通り譲るか」（『日本経済新聞』2018年5月17日）など各種報道より、みずほ総合研究所作成

マハティール氏は「自分は、今後1～2年は首相の座にとどまる」、アンワル氏も「マハティール氏は目先の目標を達成するまで首相の座にとどまるべきだ。1年、あるいはもう少しかかるかもしれない」とそれぞれ発言している。このため、禅譲問題はしばらく注目されないだろうが、来年後半頃から大きな問題となるかもしれない。もし禅譲がうまくいかなければ、希望連盟は分裂し、政権が崩壊する可能性がある。

これらの問題を乗り切れば堅調な経済成長

マハティール政権に関する3つの問題に焦点を当てたが、やはり最大の注目点は後継者問題だ。実際に動きが出るのはまだ先だろうが、この問題に関連するアンワル氏の動向や、マハティール首相の発言をよくみていくべきだろう。次に注目されるのが汚職問題である。隠し債務問題については、新情報が出てこない限り、あまり気にする必要はなさそうだ。

マレーシアには、半導体、化学、資源など強力な輸出基盤があることに加え、インドネシアやタイなどの周辺国対比で高度なインフラや経済制度が備わっている。このため、これら3つの問題をうまく乗り切れば、マレーシア経済は当面、堅調な成長を続けることができるとみている。

＊ Public Private Partnership、官民共同でインフラ事業を行うこと

作成：みずほ銀行　国際戦略情報部

お問い合わせ先

くわしくはお取引店または下記まで（今号よりメールアドレスが変わりました）

e-mail: **globalnews.mizuho@mizuho-bk.co.jp**

（2018年8月13日現在）