2021年 Cyber IQ 調査

機先を制する
セキュリティへの転換

pwc

www.pwc.com/jp

目次

はじめに …… **3**

1. 日本企業のサイバーセキュリティを取り巻く変化の潮流 …… **4**

デジタル化されたビジネスとITのサプライチェーンのつながり …… 5

コロナをきっかけに加速したゼロトラスト …… 6

「多重恐喝型のランサムウエア」の台頭 …… 8

成熟化するサイバー攻撃ビジネス …… 9

レジリエンス志向が進むも道半ば …… 10

2. 機先を制するセキュリティへの転換 …… **12**

機先を制するセキュリティの実現に向けた具体的なアクション …… 14

先進企業インタビュー …… 18

3. 2021年 日本企業セキュリティ実態 …… **20**

おわりに …… **25**

はじめに

デジタルトランスフォーメーションの波は官民を問わず押し寄せており、ビジネスとITがさらに密接に結びついていくことは明らかです。これに伴い、サイバーセキュリティの重要性もますます高まっていくと考えられます。単に自組織の情報資産を守りビジネスを継続するためというだけでなく、社会や顧客から信頼されることで企業価値を高めていくためにサイバーセキュリティは必要不可欠なものとなっていくでしょう。

日本のセキュリティリーダー262人を対象とした2021年のCyber IQ調査では、セキュリティ戦略・計画、体制、投資、サプライチェーン、脅威インテリジェンス、プライバシーなどの分野に関して、現在と3年後の展望について実態調査を行いました。本調査の調査結果には、日本のセキュリティリーダーに対する貴重な示唆が含まれています。

これらの調査結果から得られる示唆が、日本の企業の皆さまの効果的なセキュリティ対策を講じるための一助となれば幸いです。

PwC Japanグループ　サイバーセキュリティリーダー
PwCあらた有限責任監査法人　パートナー
綾部 泰二

PwCコンサルティング合同会社　パートナー
外村 慶

2021年 Cyber IQ調査 について

日本の広範な産業セクターにおける、売上高が500億円以上の企業のセキュリティ組織のリーダー、意思決定権者を対象に調査を行い、262名の回答を得ました。
当調査は、2021年6月にPwC Japan グループが実施しました。

1. 日本企業のサイバーセキュリティを取り巻く変化の潮流

デジタル化されたビジネスとITのサプライチェーンのつながり

2021年9月、「デジタル社会形成の司令塔として、未来志向のDX（デジタル・トランスフォーメーション）を大胆に推進[*1]」することを掲げ、デジタル庁が発足した。DXはいまや国が主導する社会的関心事であり、この言葉を目にしない日はないといっても過言ではない。当然ビジネスの世界においても、DXはもはや一部の先進的大企業だけの取り組みではなく、規模や業界を問わずさまざまな企業が「デジタル技術を前提としたビジネス変革」に心血を注いでいる。

こうしたDXの進展によって、クラウド・AI・IoT・ブロックチェーンといったデジタル技術の利活用がさまざまな企業で加速するかたわら、これらの技術を安全に利活用するための対策としてセキュリティの重要性がますます高まっていることは既によく知られている。そして昨今、DXやデジタル化に取り組む企業の裾野がさらに広がったことで、「デジタルを介したつながり」におけるサイバーセキュリティの重要性も急激に高まっている。

「デジタルを介したつながり」は、ビジネスとITの2つのサプライチェーンから捉えられる。

まず、ビジネスサプライチェーンとは調達から販売に至るまでの一連の価値提供活動のことであり、製造業を例にとれば原料・部品の調達先や製造・加工の委託先、流通・販売業者といったさまざまな企業がステークホルダーとなる。また社内に目を向けても、海外拠点や子会社、工場や研究所といった多種多様なステークホルダーが存在する。DXやデジタル化が進むと、自社と他社、国内拠点と海外拠点、本社と工場といった複数の主体間でシステムが接続され、プロセスやデータの流れが有機的につながっていく。もちろん、これによってサプライチェーン全体の効率化や提供価値の向上が見込まれる一方、サプライチェーンを介したセキュリティリスクも高まっている。実際、セキュリティ対策が相対的におくれを取っている委託先企業や海外拠点を起点とし、システムやネットワークのつながりを利用してサイバー攻撃を受けたというようなインシデント事例[*2]も多く発生している。

次に、ITサプライチェーンとはITシステムやサービスに関する業務のアウトソースが連鎖するような形態[*3]を指し、システムの保守・運用の委託だけでなく、IaaS、PaaS、SaaSといったクラウドサービスもその一部と考えられる。IT関連業務のアウトソースやクラウド移行はかねてから多くの企業で進められさまざまな恩恵をもたらしているが、こうしたサービスの提供元がひとたびセキュリティ侵害を受けると、これを利用する全ての企業に被害が波及する可能性があることから、ITサプライチェーンにおけるセキュリティリスクもますます高まっているといえる。

---

*1 デジタル庁「組織情報」（https://www.digital.go.jp/about ）

*2 ENISA「Threat Landscape for Supply Chain Attacks」（https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks ）

*3 情報処理推進機構「「ITサプライチェーンにおける情報セキュリティの責任範囲に関する調査」報告書について」（https://www.ipa.go.jp/security/fy30/reports/scrm/index.html#L ）

関連リンク：PwC「【サイバーインテリジェンス】世界で広がるソフトウエアサプライチェーン攻撃の事例と対策」（https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/cyber-intelligence07.html ）

コロナ禍をきっかけに加速したゼロトラスト

今日ビジネス環境に激変をもたらしているもう一つの事象として、2020年初から続く新型コロナウイルス感染症（COVID-19）の流行による、リモートワーク化をはじめとする急激な働き方の変化が挙げられる。これに伴い、業務用端末の整備やVPNの導入・拡張といったITインフラの補強、そしてそれにひもづくセキュリティの強化に奔走した、あるいは現在進行形で対応に追われている企業も多いことだろう。コロナ禍の初期においては、VPNの導入・拡張を急遽進めたことで脆弱性対応といったセキュリティ面が後手に回った企業も少なくなかった。そのため、そうしたVPNの脆弱性を突いたサイバー攻撃が横行[*4]した。ただし、現状こうした攻撃については、企業側での脆弱性対応などにより一定程度対策が進んで来ている。一方で、かねてから進んでいたクラウド化に加えてリモートワークが急激に普及し、かつその状態がコロナ禍終息後も少なからず保持される見通しがある今、企業は「境界防御型」のセキュリティ対策からの脱却という、より大きな転換期に立たされている。

「境界防御型」とは、ファイアウォールなどによってネットワークの内と外を明確に区別し、外にある脅威からいかにネットワークの内側を守るか、というセキュリティ対策の考え方である。しかし、業務を担うシステムが次々にクラウド環境に移され、従業員も自社オフィスの他に自宅やレンタルオフィスをはじめ多様な環境からこれらにアクセスするようになったことで、このようにネットワークの内と外を分ける考え方はもはや成立しなくなりつつある。

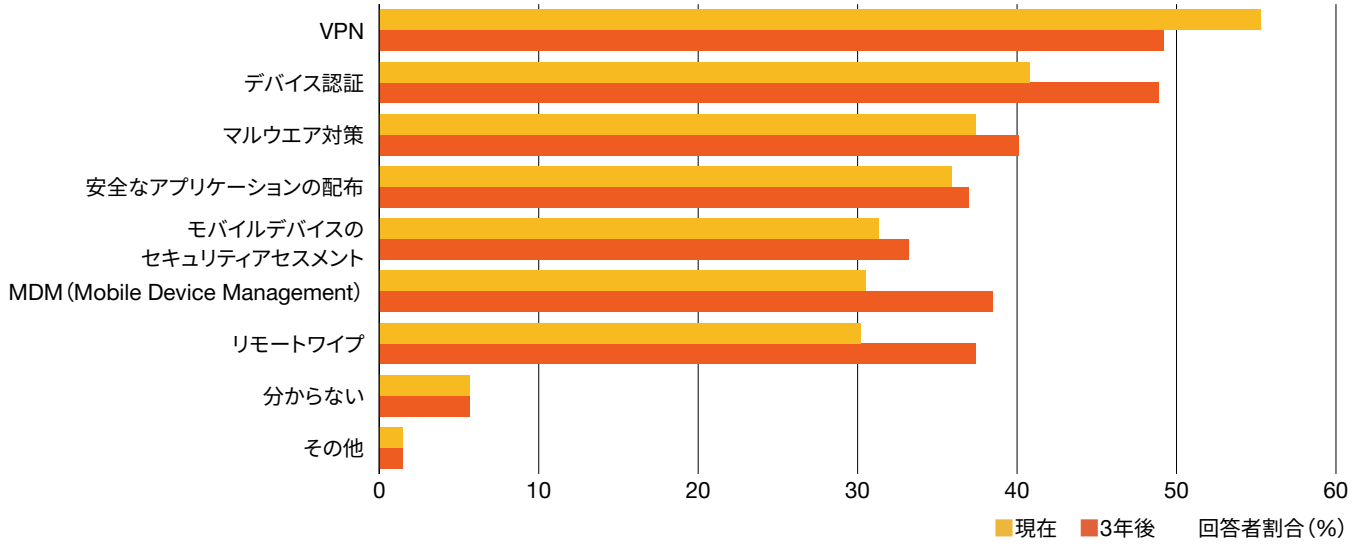
こうした中で注目されているのが、「ゼロトラスト・アーキテクチャ（ZTA）」と呼ばれる考え方である。「ゼロトラスト」とは文字通り「手放しでは何も信用しない」という思想であり、技術的には接続元ネットワークを問わずユーザーやデバイスのアイデンティティおよびそのコンテキストに基づき細かく認証・認可を行うことでこれを実現する。実はZTAそのものはコロナ禍以前から存在する考え方であるが、昨今の働き方の変化に伴い、その必要性・緊急性がますます高まっている。しかし、ZTAはあくまでアーキテクチャの概念であり、特定のセキュリティソリューションを導入すれば実現できるという性質のものではないため、先進的な企業の多くにおいても障壁や課題が多く、いまだ模索段階にあるというのが実情でもある。

Cyber IQ調査では、モバイルデバイスの対策として最も導入率が高いのは依然としてVPNのような「境界防御型」の対策であった（回答者の55.3%がモバイルデバイスに対して行っているセキュリティ対策として「VPN」を選択しており、全選択のうち最大の割合）（図表1）。

一方、現状および3年後の計画としてどのようなセキュリティ対策を講じているかについての質問では、リスクベース認証や多要素認証、シングルサインオンといったZTA関連の対策は増加に向かうことが読み取れるため、企業が考え方の転換に向けた意欲を持っていることが推察される。ただし、現実的にはZTAへの転換は短期間で達成することは難しく、関連製品市場の成熟や現有資産のマイグレーションなどを経て緩やかに進んでいくと考えられる（図表2）。

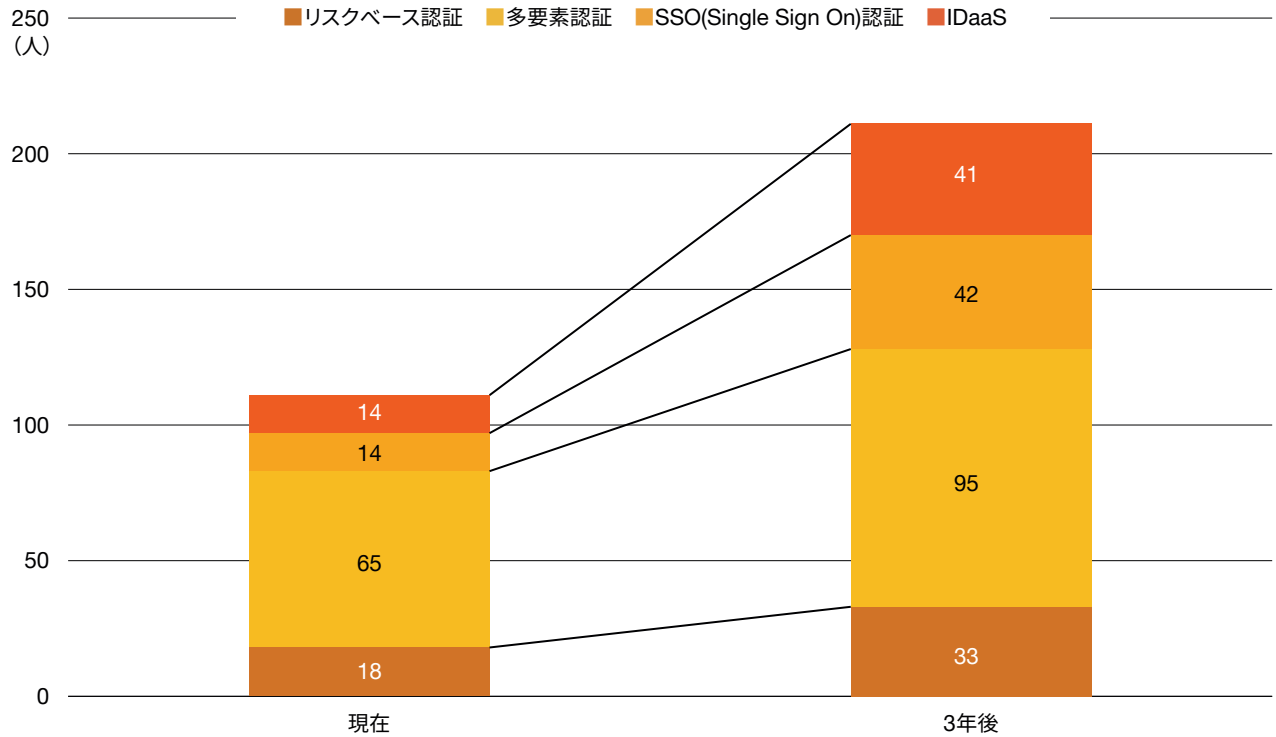
図表1：企業が導入している（3年後に導入を検討する）モバイルデバイスに対するセキュリティ対策

設問　現在、モバイルデバイスに対して行っているセキュリティ対策を選択してください。
また、3 年後に行っていると思うセキュリティ対策を選択してください（それぞれいくつでも）。



図表2：企業が導入している（3年後に導入を検討する）ZTAに関わるセキュリティ対策

設問　現在と 3 年後とを比較すると、リスクベース認証・多要素認証・SSO および IDaaS といった、ゼロトラストアーキテクチャに関連するソリューションの導入が有意に増加している



*4 CISA「Alert (AA21-209A) Top Routinely Exploited Vulnerabilities」（https://us-cert.cisa.gov/ncas/alerts/aa21-209a）

関連リンク：PwC「次世代のITインフラ － ゼロトラスト・アーキテクチャ ITインフラの役割変化とゼロトラストの適合性」（https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/zero-trust-architecture01.html）

関連リンク：PwC「国内企業における「ゼロトラスト・アーキテクチャ」の実態調査 2021」（https://www.pwc.com/jp/ja/knowledge/thoughtleadership/zero-trust-architecture-survey2021.html）

「多重恐喝型のランサムウエア」の台頭

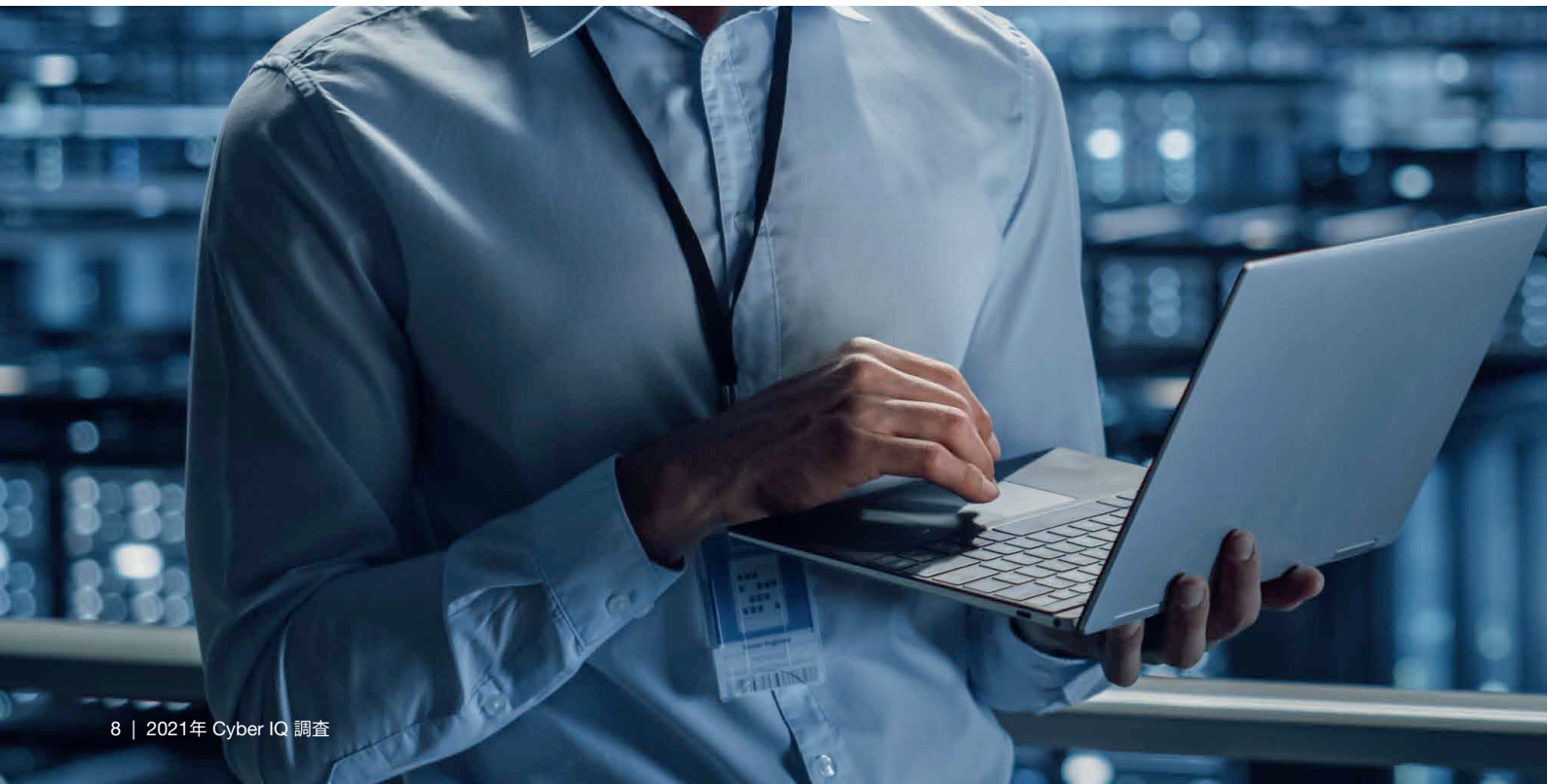
ビジネスを取り巻く環境の変化に加え、サイバー脅威も常に変化している。ここ数年、常に話題に上り続けているサイバー脅威の一つにランサムウエアが挙げられる。ランサムウエアとはマルウエアの一種であり、2017年に猛威を振るったWannaCryや、2019年から2020年にかけて流行したEmotetなどはいまだ記憶に新しいところである。独立行政法人情報処理推進機構（IPA）が毎年公開する『情報セキュリティ10大脅威 2021』でも、組織における脅威の1位として「ランサムウエアによる被害」が挙げられているなど、その趨勢はいまだ衰えるところを知らない。

ランサムウエアを用いた典型的な攻撃パターンとしては、語源である「Ransom（身代金）」からも分かるとおり、攻撃者がこれを標的システムに感染させデータを暗号化することで質にとり、「復号をしてほしければ身代金を支払え」と要求してくるというものが挙げられる。ランサムウエアに感染すると、企業はシステムやデータの可用性が侵害され、これを利用した業務、ひいては事業そのものを停止せざるを得なくなってしまう。このような事例が広く知られるようになると、多くの企業ではシステムやデータのバックアップ取得や有事の際の迅速な復旧プロセスの整備などを進めることで対策を進めて来た。

しかし近年、このような対策では対処しきれない新たな攻撃パターンとして、「二重恐喝型のランサムウエア」と呼ばれる手法が広まっている。「二重恐喝型」というのは、従来のようにデータを暗号化することで身代金を要求するという恐喝に加え、それに応じなかった場合は窃取した機密情報や個人情報を流出させる、という二段階目の恐喝をしてくるような手法を指している。より切迫した判断を迫られたシナリオとして、窃取したデータの一部をダークウェブ上で公開し72時間以内に支払いをしなければ残りのデータも流出させる、といった時限式の脅迫手法を取り入れてきた事例もある。また、それに加えて一部のランサムウエアでは、身代金の支払いに応じない場合、被害組織のWebサイトに大量の通信データを送信し、Webサイトの運営を妨害するといった三重恐喝の手口も確認されている。ランサムウエアによる身代金支払いに対する圧力は高まっており、その悪質化はとどまるところを知らない。

このように、サイバー脅威は攻撃技術もその使い方も変化し続けており、攻撃者と企業の攻防はいたちごっことなってしまっているのが実情である。こうした中で企業がサイバーリスクを少しでも低減していくためには、サイバー脅威の潮流を機敏にキャッチし、それに合わせてリスクシナリオを柔軟かつ手広く想定して対策を見直し続けることが肝要である。また、セキュリティ対策は脅威の侵入から「防御」するだけではなく、セキュリティ侵害をタイムリーに「検知」し「対応・復旧」に速やかにつなげていく「レジリエンス」が重要であることは既に広く説かれていることである。特に、このようなランサムウエアに起因するリスクシナリオにおいては、被害が業務や事業の継続性に影響する、かつ身代金を支払うべきか否かの判断が必要になってくるため、経営層や法務・広報部門などをはじめとする全社のステークホルダーを巻き込んだ「対応・復旧」プロセスを整備しておくことが特に重要となるだろう。

関連リンク：PwC「【サイバーインテリジェンス】リモートワーク導入により高まる二重恐喝型ランサムウエアの脅威」（https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/cyber-intelligence06.html）



成熟化するサイバー攻撃ビジネス

先述のようなランサムウエアの流行・脅威拡大の背景には、RaaS（ランサムウエア・アズ・ア・サービス）に代表されるようなサイバー攻撃のビジネス化・サービス化の影響が大きいと考えられている。RaaSとはその言葉のとおり、ランサムウエアによる攻撃に必要なツールやノウハウをサービスとして提供する仕組みのことである。2021年にも、DarkSideと呼ばれるRaaSによって提供されたランサムウエアが、大企業を一時操業停止に追い込んだインシデント事例があった。

RaaSのサービス形態はSaaS（ソフトウエア・アズ・ア・サービス）などと非常によく似ており、ランサムウエアの開発者は利用を希望するユーザーに対し、ライセンス形式や成果報酬形式で費用を請求することでそのサービスを提供しているといわれている。もちろん、そのような「闇のサービス」市場は通常、一般的なブラウザや検索エンジンから辿り着けるような場所ではなく、特殊なソフトウエアや経路を介してのみアクセスできるディープウェブやダークウェブの中に存在している。このようなウェブ領域は深層ウェブとも呼ばれ、本来は必ずしもサイバー攻撃やサイバー犯罪のために存在するものではないが、一般ユーザーから発見されにくいことや匿名性が高いことなどから、こうした「闇のサービス」がはびこりやすい場となってしまっている。

深層ウェブへのアクセスは特殊な方法が必要ではあるものの、攻撃のツールやノウハウを自ら作りだすことに比べればその障壁は決して高いとはいえないため、高度な知識や技術を持たない者でも比較的容易にサイバー攻撃を行えてしまう状況が生み出されているというのが現状だ。また、こうした深層ウェブでは、サイバー攻撃に必要となるサービスの提供だけでなく、攻撃に必要となるIPアドレス・認証情報などの標的情報の流通・販売、攻撃に加担する企業内部犯の募集といった活動が行われている。そして、サイバー脅威の市場は、匿名での支払いに都合が良い暗号通貨の普及などにも支えられ、ますます拡大・成熟しつつあると考えられている。

ここまでで述べたように、サイバー脅威は企業の対策の裏をかくように進化し続けているだけでなく、攻撃ツール・ノウハウの取引市場の成熟によって攻撃者になることのハードルがますます低くなっている。一方で、こうした外的脅威に加え、内部不正や不注意による情報漏洩などの内的脅威にも当然ながら引続き注意していく必要はある。企業は、残念ながらこうした脅威の拡大に直面していることを再認識し、継続的に対策を見直していくことが重要であるといえよう。

関連リンク：PwC「【サイバーインテリジェンス】リモートワーク導入により高まる二重恐喝型ランサムウエアの脅威」（https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/cyber-intelligence06.html）

レジリエンス志向が進むも道半ば

古くは情報やITの活用に始まり、デジタル化やDXといった企業のビジネスを取り巻く環境変化が進み、他方でランサムウエアに代表されるようなサイバー脅威がますます進化している中で、企業がとるべきセキュリティ対策の戦略として「サイバーレジリエンス」が提唱されて久しい（参考：PwC グローバル情報セキュリティ調査2018）。「レジリエンス」とは弾性・復元力などを意味する言葉であり、サイバー攻撃を完璧に防ぎきることが現実的に不可能となってしまった以上、ビジネスに対する影響を最小限に抑え素早く平時に戻すことにも注力する、ということがサイバーレジリエンスの趣旨である。この考え方を米国標準技術研究所（NIST）のサイバーセキュリティフレームワーク（CSF）の5機能、識別・防御・検知・対応・復旧に当てはめれば、防御一辺倒ではなく検知から復旧までの全体に注力することであると換言できよう。

では実際のところ、企業はどこまでサイバーレジリエンスを高められているのだろうか。本調査において、前述したNIST-CSFの5機能のうちどの機能でのセキュリティ対策を最も重要視しているかという質問を行ったところ、現状は「防御」が41.2%、「検知」が35.9%と突出している一方、「対応」は5.0%、「復旧」は5.3%と大きく水をあけられていることが明らかになった。また、同様の質問について3年後どのようになっているかを問うたところ、「防御」は39.7%とほぼ横ばいなものの、「検知」は21.4%と大きく減少する見込みとなった。一方で「対応」と「復旧」を最も重要視すると答えた割合は、それぞれ19.1%と10.3%であり、企業における対策の力点が徐々にシフトしていく傾向にあることがうかがえる（図表3）。

これらの調査結果から、多くの企業において、防御だけでなく検知から復旧に注力してレジリエンスを高めていきたいという意向はあるものの、特に対応や復旧までは手が回っていない現状が見て取れる。サイバーレジリエンスという概念の普及度に比して、その実現まではいまだ道半ばであると考えられる。

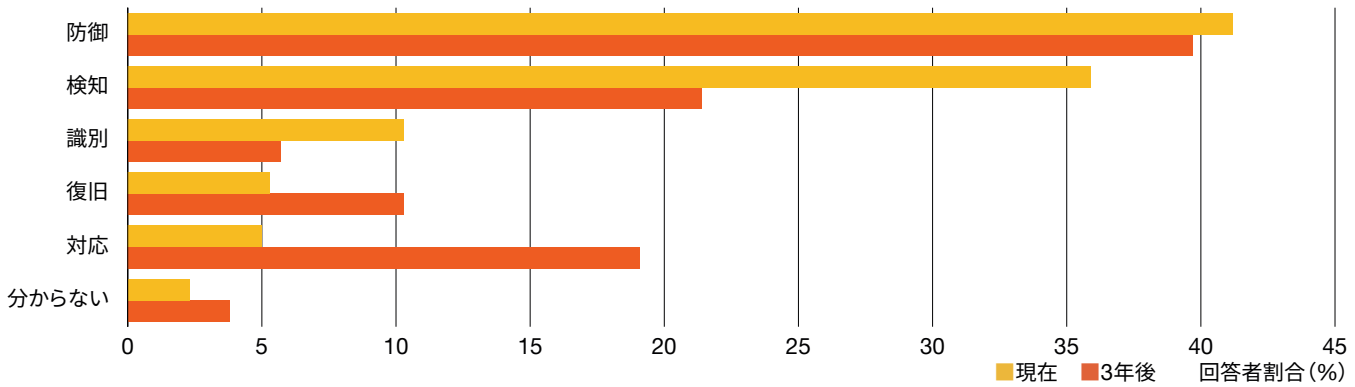
このように企業がレジリエンスの確保に腐心しつつも苦戦している現状がある一方、サイバー脅威の拡大はとどまるところを知らない。先述のようなサプライチェーンやリモートワーク先のネットワークなどを入口にランサムウエアなどが侵入しセキュリティインシデントに至るような事例も多く報道されている。そして、いわゆるオフィス環境にとどまらず工場などの生産・研究拠点の環境がデジタル化され、かつシステム同士がネットワークで接続されるようになったことで、このような脅威の侵入は事業や業務の停止に直結し得るようになり、セキュリティインシデントの被害はますます深刻なものとなってきている。

本調査においても、過去1年間で発生したセキュリティインシデントによってどのような影響を受けたかを質問したところ、「データ侵害」の21.8%と並んで「システムのダウン」「ビジネス影響」がそれぞれ22.5%、19.8%という回答結果が得られた（図表4）。

また、「ビジネス影響」の中身について掘り下げた質問では、「事業、プロセス、サービスの中断」（26.9%）や「ネットワークの逼迫」（26.9%）といった、事業や業務の継続性に直結するような影響が上位に挙げられていた（図表5）。

図表3：企業が最も重要視する（3年後に最も重要視すると考える）セキュリティ機能

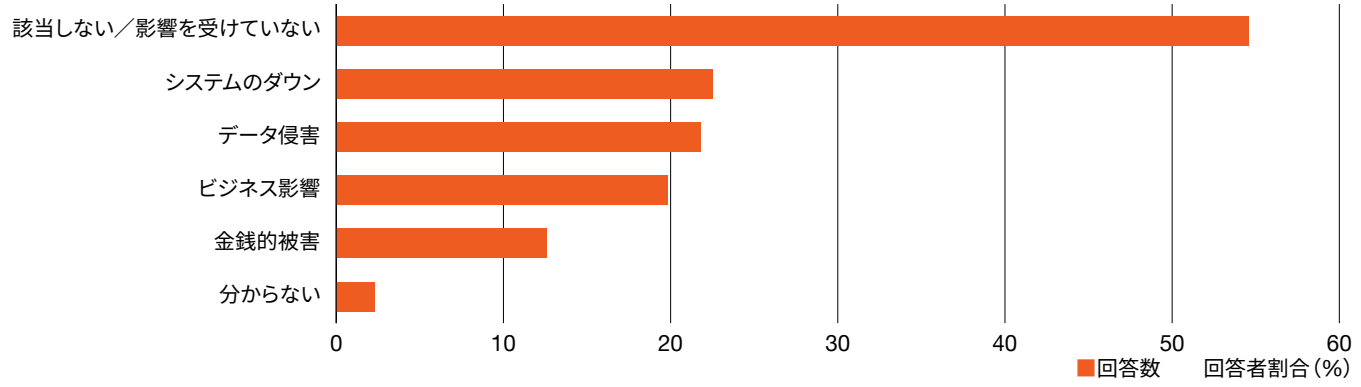
設問　現在、貴社では、「識別」「防御」「検知」「対応」「復旧」（NIST-CSFの機能）のうち、どの機能へのセキュリティ対策を最も重要視していますか。また、3年後では、最も重要視すると思いますか（それぞれひとつだけ）。



このようにサイバーセキュリティリスクは、従前の情報漏洩などと同程度に事業や業務そのものの継続性を脅かすようなものが増えてきており、経営課題としての重要度もますます高まっている。そして、ビジネスを取り巻く環境やサイバー脅威の変化を見る限り、そのような影響の深刻化は今後も加速していくことが懸念される。では、企業はどのようにしてこのリスクに立ち向かっていくべきなのか。無論、完璧に防御しきることではなくレジリエンスの向上を目指す、という戦略は引続き重要である。しかし、サイバーリスクが事業の継続性を脅かすようになり、ひとたびインシデントが発生してしまうと致命的な影響をもたらしかねなくなった以上、もはやそれだけでも不十分と言わざるを得ない。見えざる脅威に対し全方位的に守って有事に備えるという「リアクティブ」なアプローチから、脅威を積極的に理解し動的かつ柔軟に対策を変えていくという「プロアクティブ」なアプローチへの転換こそが、次世代のセキュリティ対策に求められるものであるだろう。

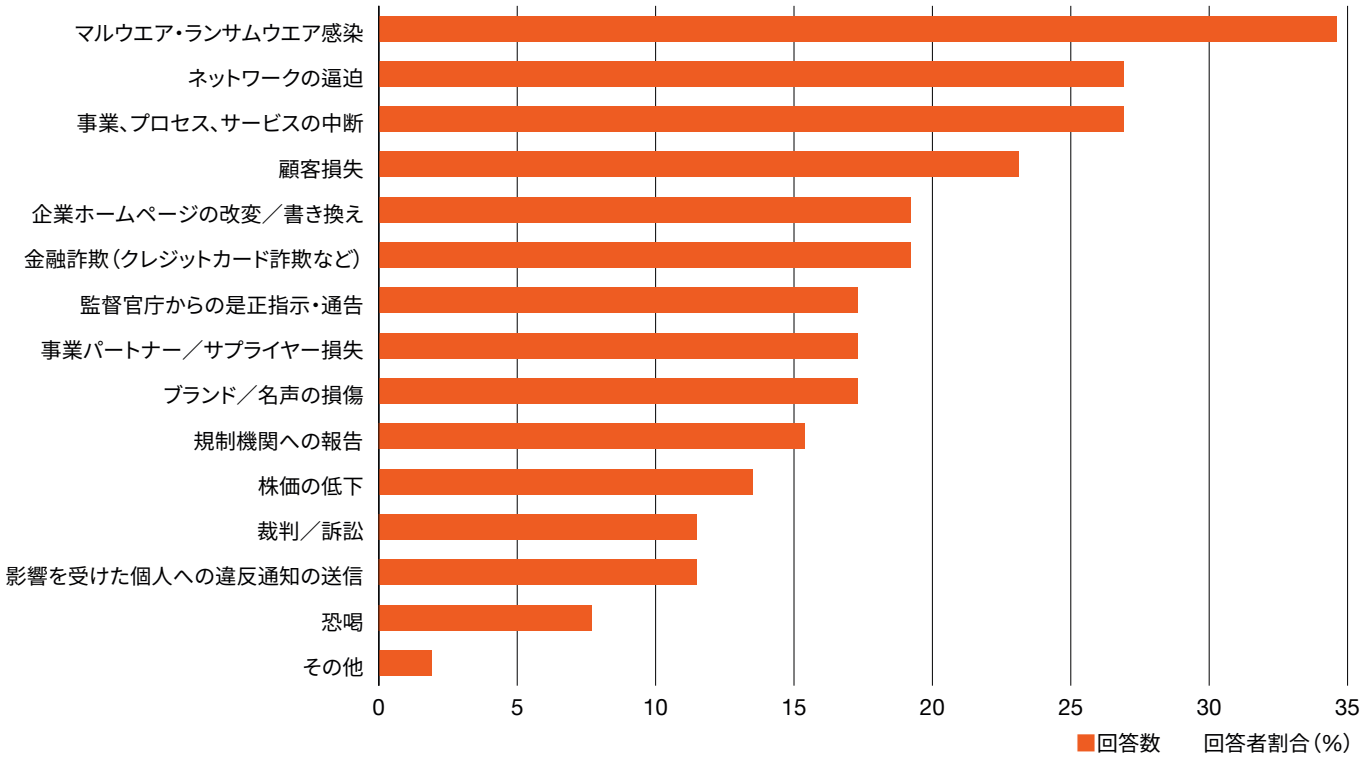
図表4：企業が被ったセキュリティインシデントによる影響

設問　あなたの組織は、セキュリティインシデントによってどのような影響を受けましたか（いくつでも）。



図表5：セキュリティインシデントによるビジネスへの影響

設問　「ビジネスの影響」を選択した方にお聞きします。具体的に、どのような影響を受けましたか（いくつでも）。



関連リンク：PwC「サイバーショックに備え、デジタル社会を強化する」（ https://www.pwc.com/jp/ja/knowledge/thoughtleadership/2018/assets/pdf/strengthening-digital-society-against-cyber-shocks.pdf ）

2. 機先を制するセキュリティへの転換

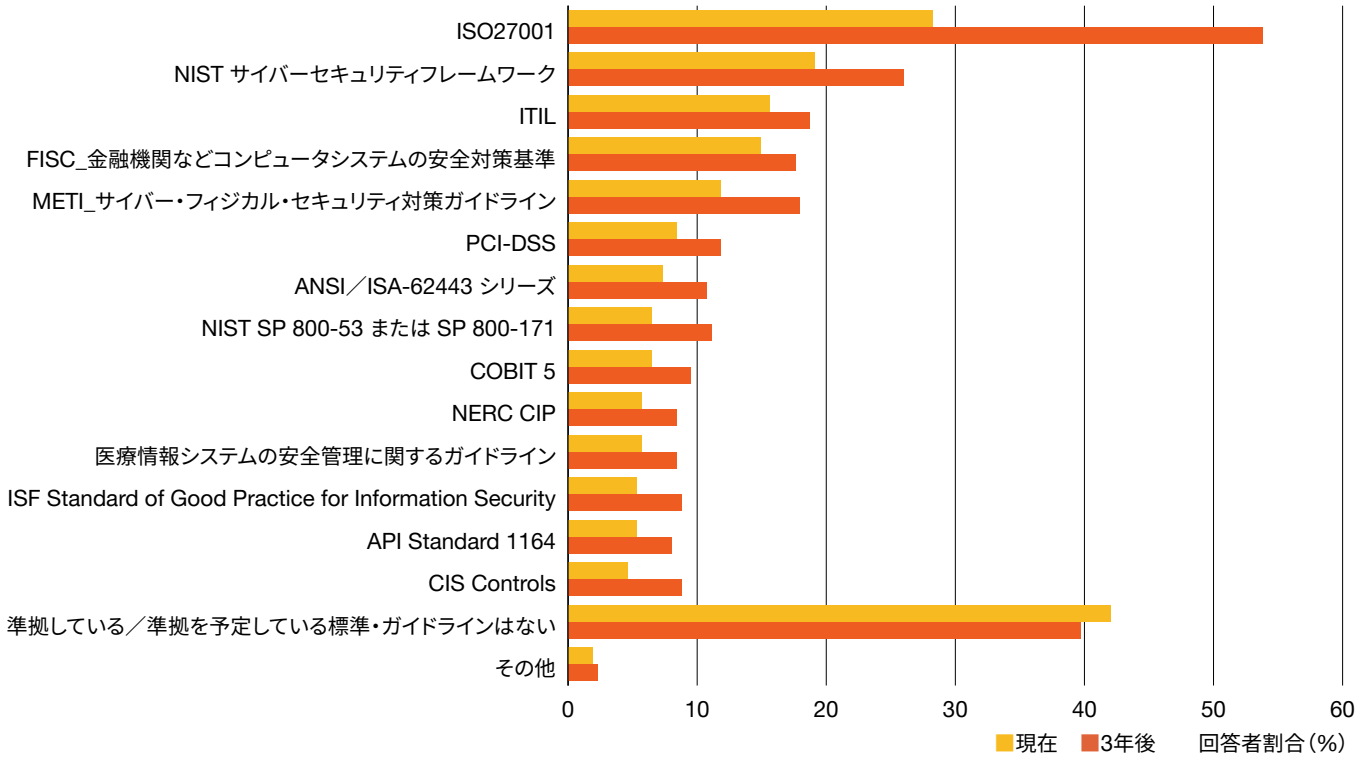
前述のようにビジネスを取り巻く環境、サイバー脅威の変化に伴い、企業は従来のアプローチでセキュリティ対策を推進するだけでは、昨今のサイバー脅威に対抗することが難しくなってきている。「従来のアプローチ」とは、セキュリティ標準・ガイドラインに基づいてアセスメントを行い、抽出・優先度付けされたギャップ・課題に基づいてセキュリティ対応計画の策定・推進を行うことを意味する。本調査でも、現在準拠している標準・ガイドラインについて質問したところ「ISO27001」が28.2%、次いで「NISTサイバーセキュリティフレームワーク」が19.1%と続き、3年後に関してもそれぞれ53.8%、26%と高い準拠率であることが確認された（図表6）。

一方、こうした標準・ガイドラインはある時点でのパラダイムに基づいて検討・策定された結果であり、公開・施行された時点から時間経過とともに最新のパラダイムとのギャップが生じることは避けることができない。また、日々新たに発生するサイバー脅威に対抗するために、企業はサイバー脅威を知得した時点でリスクを評価し、対応計画を見直すが必要がある。こうした考え方は、ベースラインアプローチ、およびリスクベースアプローチとして知られている。今日必要となっているのは、これらをさらに発展させた「機先を制するセキュリティ」である。

クラウド移行に代表されるアーキテクチャの変化やサプライチェーンリスクの台頭により企業が守るべき範囲は拡大し、また曖昧になってきている。サイバー攻撃者は、こうした新たに発生するリスクを巧みに突き、サイバー攻撃を行う。そのため「思いもよらぬポイントから攻撃を受け、気付いた時には手遅れ」という事態を免れるためには組織内部の情報だけでなく、サイバー攻撃者の意図・能力を含めた外部情報の収集・分析は必要不可欠である。これにより、自組織に起こり得る脅威を高い精度で予測して備える、こうした一連の活動をリアルタイムに近いサイクルで運営することが「機先を制するセキュリティ」である。このようなセキュリティガバナンスを、日々のリスク評価に振り回されずに実現するためには、組織の共通言語としてセキュリティ管理項目を定義し、測定・改善・報告する体制・プロセスを整備することが重要となるだろう。

図表6：企業が準拠する（3年後に準拠を検討する）標準・ガイドライン

設問　現在、貴社において、準拠している標準・ガイドラインはありますか。また、3 年後、貴社において、準拠する予定のある標準・ガイドラインはありますか（それぞれいくつでも）。



機先を制するセキュリティの実現に向けた具体的なアクション

では、「機先を制するセキュリティ」を実現するためにはどのような取り組みが必要になるのだろうか。セキュリティ対応計画を策定・推進するといった従来の取り組みに加えて、サイバーリスクに関する外的要因を収集・分析し、喫緊のリスクに対処する、計画を動的に見直す能力を獲得・強化することが基本的な考え方になるだろう。

現在、ISO/IEC27001のベストプラクティスにあたるISO27002の改訂が進められており、この中で新たな要求として「脅威インテリジェンス」が追加される見通しである。この動きは「機先を制するセキュリティ」と合致するものであり、ISO27001に基づいた情報セキュリティマネジメントシステムを運営している企業では、既存の体制・プロセスの中に当該活動を組み込むことが一つのアプローチとして考えられる。また、CSIRTを設置・運営している組織では、CSIRTの役割・機能を拡張・再定義し、当該機能を追加するといったアプローチも考えられる。こうした実現方式は、企業の組織によって異なり、さまざまな形態が考えられるだろう。

本調査でも脅威インテリジェンスに関する取り組み状況を質問したところ、自組織またはアウトソースにより情報収集を行っているという回答は約8割に上る。また、どのように活用しているのか、については「戦略策定のインプット」「インシデントレスポンスのインプット」が45.1%と同率首位である一方、「用途は定まっていないが適宜参考にしている」「あまり活用できていない」という回答が併せて37.7%に上り、利活用における課題がうかがえる結果となった（図表7）。この調査結果を踏まえると「機先を制するセキュリティ」を実現するためには。「収集した情報をいかに活用できる状態になるか」が要諦といえる。ここでは、日本企業が抱える典型的な課題を踏まえて具体的なアクションを記載する。

1. サイバーリスクの影響を受ける事業の重要成功要因を特定する

従来サイバーリスクは、ITシステムのリスクと認識されており、情報システム部門が保有、管理するものと捉えられてきた。一方、昨今のサイバーリスクは、単にITシステムに対するリスクにとどまらず、事業継続に直結する経営課題であることは前述したとおりである。特に上場企業においては有価証券報告書にサイバーセキュリティの対策状況を開示することが推奨[5]されており、こうした認識のアップデートが進んでいる。

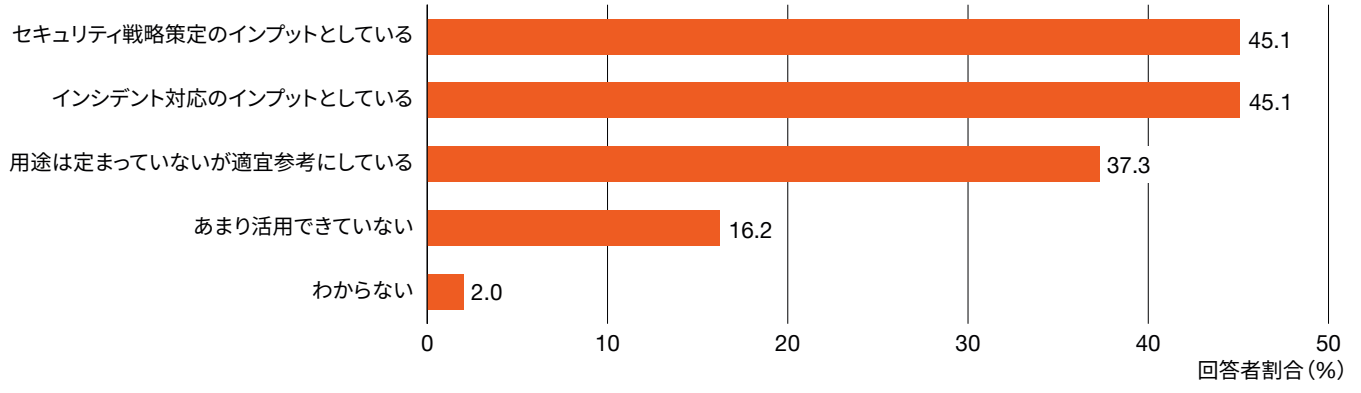
しかし、いざサイバーリスクに関する情報が収集・分析され、経営会議の場に報告されたとしても、当該リスクと事業に対するインパクトの関係性を明確に説明することができなければ実効性のある意思決定を行うことは難しいだろう。そのため、企業は事業継続上の重要成功要因を洗い出し、その中でもサイバーリスクの影響を受ける要因を事前に特定しておく必要がある。これにより、サイバーリスクが知得された際に、重要成功要因に影響を与えるか否か、どの程度の影響を与えるのか、という観点で検討・判断を行うことができる（図表8）。

例えば、ECサービスであれば、「メンテナンスを除き、常にユーザーがECサイトを利用できること」「会員情報が保護されること」などが典型的な重要成功要因として考えられる。そのため、ECサイトで利用しているソフトウエアの脆弱性が発見・報告された場合、当該脆弱性が悪用された際の重要成功要因への影響有無・程度に基づいて意思決定を行うことができる。

また、自社製品・サービスを海外で販売・展開している場合、「現地のレギュレーションに準拠すること（抵触しないこと）」が重要成功要因として考えられ、こうした情報を収集・分析し、影響を判断することが必要となる。昨今では、中国におけるサイバーセキュリティ法、各国・地域でのプライバシー法の制定・施行が進んでおり特に留意する必要がある。

図表7：企業における脅威インテリジェンスの活用

設問　貴社では、脅威インテリジェンスをどのように活用していますか（いくつでも）。



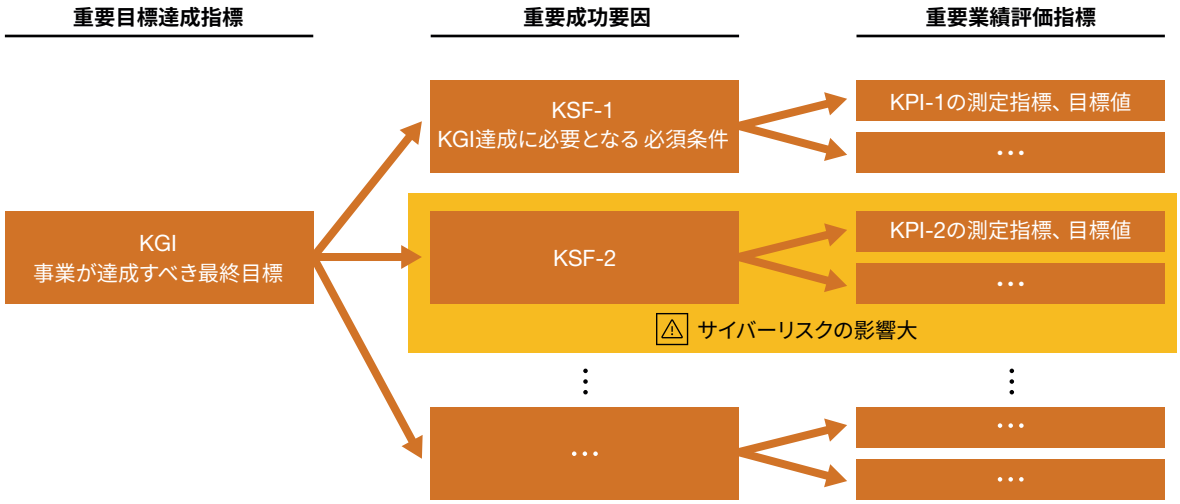
*5 経済産業省「サイバーセキュリティ経営ガイドライン Ver 2.0」（https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0.pdf）

2. 自組織に合ったサイバーインテリジェンスサイクルを整備する

昨今、脅威インテリジェンスの活動におけるOSINT（オープンソースインテリジェンス）の重要が繰り返し説かれており、政府関連機関、ISACなどの業界団体、IT・セキュリティベンダー、ニュース、SNSなどのさまざまな情報源から情報を収集することができる。先の調査でも脅威インテリジェンスの収集を行っている企業が約8割に上るものの、その活用に課題がある点を述べた。

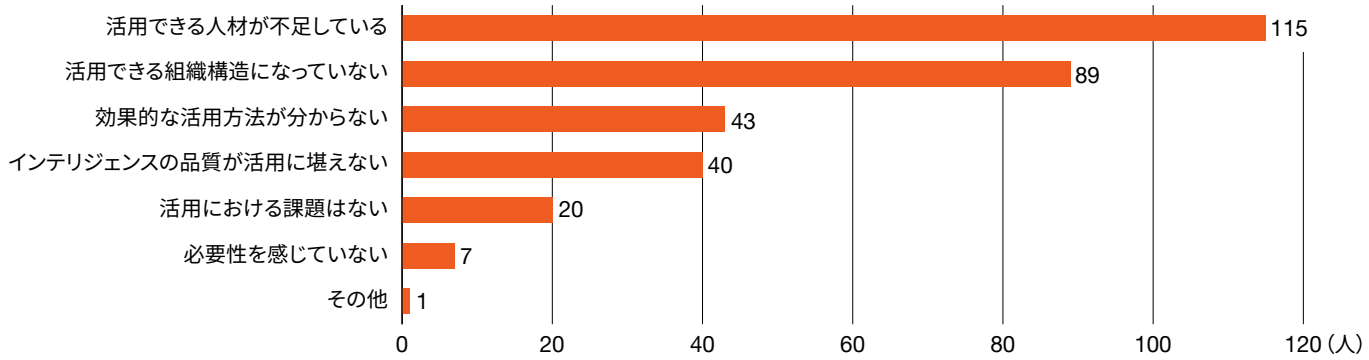
こうした課題を抱えている企業では、サイバーインテリジェンス全体の活動サイクルが十分に整備されていないことが原因の一つとして考えられる。これは特に、脅威インテリジェンスサービスを外部の専業ベンダーに委託している場合に課題になることが多い。具体的には、委託先により自社のリスク分析が代行されることを期待しており、委託先から提供された示唆・見解を自組織で評価、分析するプロセスが欠落していることが見られる。本調査でも先の利活用における課題の原因として「効果的な活用方法が分からない」「インテリジェンスの品質が活用に堪えない」という回答が確認されている（図表9）。

図表8：企業の重要成功要因へ影響を与え得るサイバーリスクの評価指標設定



図表9：脅威インテリジェンス活用における課題

設問　脅威インテリジェンスを活用するうえでの課題、または活用できない原因はなんですか（複数回答可）。



インテリジェンスの目的は、サイバーリスクが自社事業の重要成功要因に及ぼす影響を特定し、意識決定を支援することであり、完全に第三者が代行できるものではない。そのため、インテリジェンスサイクルなどの基礎的なフレームワークは参考にしつつも、自社にあったプロセスを整備することは必要不可欠である。

一般にインテリジェンス活動は、情報機関が意思決定者からの要求に基づいて行うものであり、方針策定、収集、評価、分析、配布・フィードバックといった一連の活動サイクルで実施される。これを企業活動に照らし合わせた場合、方針策定においてどのような目的を達成するために情報収集を行うかを設定し、これは先の「重要成功要因に影響を与え得るサイバーリスクを特定するため」に他ならない。また、それを実現するための情報源の洗い出し、各情報源の信頼性評価といった取り組みも必要となる。こうして策定された方針に従って以下のアクションを実施することが必要である。

1. **収集**
   情報を収集する
2. **評価**
   内容・根拠などに基づいて情報自体の信頼性を評価する
3. **分析**
   重要成功要因への影響有無・影響の程度を分析し、示唆・見解を導出する
4. **配布・フィードバック**
   示唆・見解を適切な意思決定者・会議体で諮り、意思決定を行う

3. ビジネス部門・IT部門で協働できる組織体制を構築する

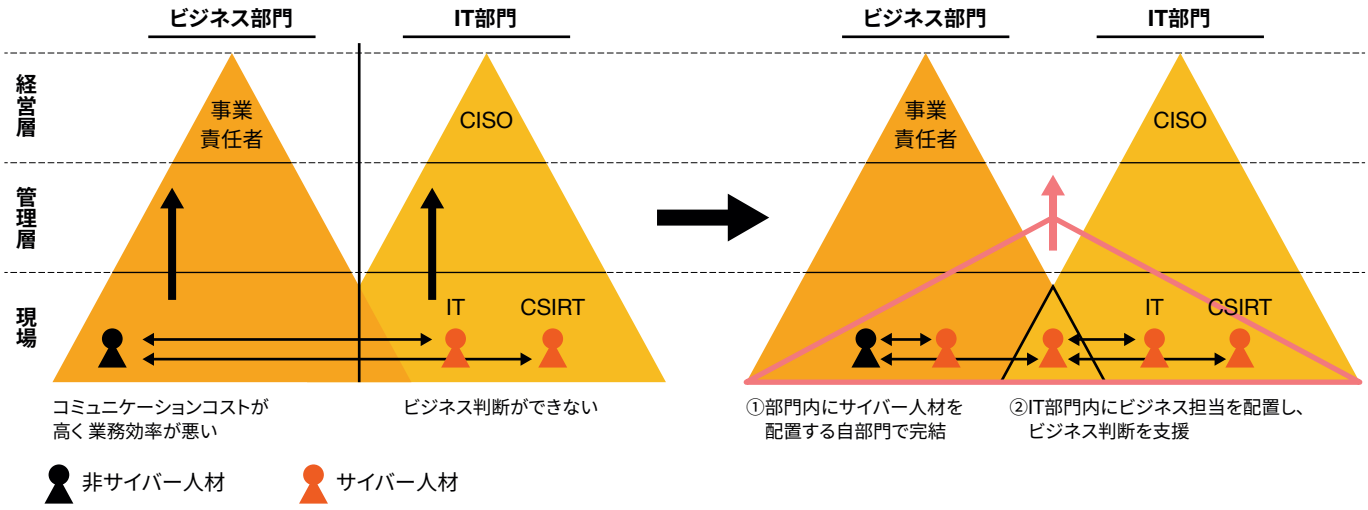
ビジネスのデジタル化によりサイバーリスクの影響を受ける重要成功要因は増加の一途をたどっており、ビジネスの意思決定においてサイバーが占める割合も大きくなっている。そのため、最高情報セキュリティ責任者（CISO）に代表される経営層が活動を牽引することはもちろん、サイバーリスクを経営アジェンダとして取り扱う必要がある点はこれまで議論されてきたとおりである。

特に、インテリジェンスに関連した活動は、技術的観点だけでなく法令・法律・規制、業界などの定めるガイドラインなどの社会・業界動向といった広範な情報を収集・分析する必要があり、求められる視座も自然と高いものとなる。そのため、現場で収集・分析された情報が取り扱い不明なままなおざりにならないように組織の共通認識としてサイバーリスクに関連した重要成功要因を特定し、総合的な判断が必要なケースにおいては適切な関連部署にエスカレーションするプロセスを整備することが重要となる。

また、近年、ビジネスに必要となるサイバーセキュリティを含んだIT機能を全社のIT部門ではなく、当該ビジネス部門内に設置する企業も存在する。こうしたケースでは、ビジネス部門は自部門内でサイバーインテリジェンスサイクルを運用することが可能となり、サイバーリスクの事業への有無・影響を迅速かつ高精度で分析することができる（図表10）。一方で、既存のCSIRT組織などにサイバーインテリジェンスの機能を拡張する場合、活動の目的が重要成功要因への有無・程度であることを考えると事業を担うビジネス部門との連携は必須となる。

最適な体制は企業によって異なるものの、ビジネス部門内にサイバー人材を配置する、IT部門内にビジネス担当のサイバー人材を配置するといった両部門が協働できる組織体制を戦略的に構築する必要があるだろう。

図表10：企業に求められるサイバー人材の配置例



経済産業省 商務情報政策局
サイバーセキュリティ課長
奥田 修司 氏

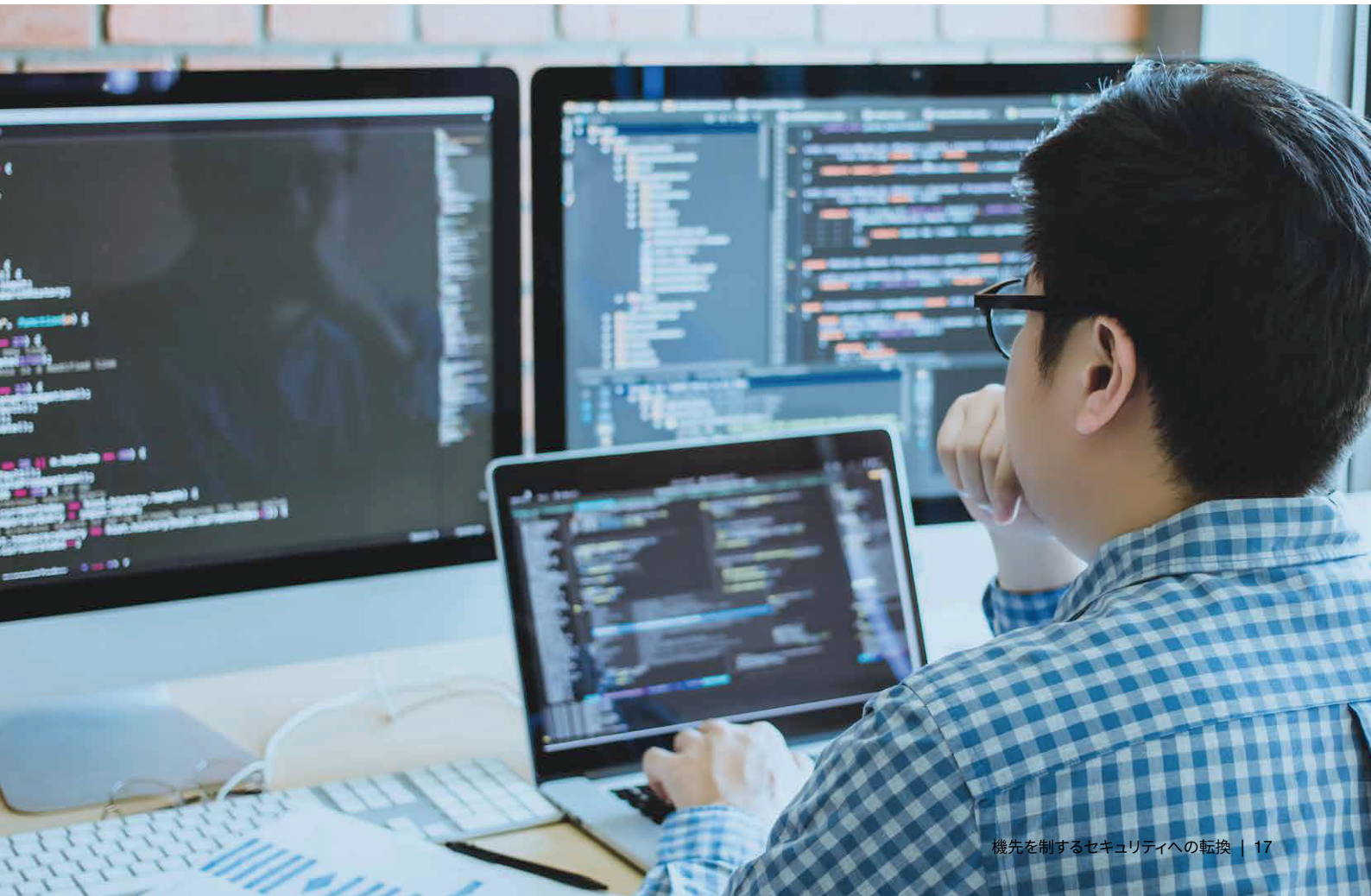
サイバー攻撃件数は年々増加しており、特に近年はランサムウエア攻撃など、直接金銭を要求する攻撃も顕著になりました。こうした攻撃への対応を一歩間違えると、企業はビジネス的な損失のみならず、社会的な信頼も一気に失います。経営者は「サイバーセキュリティリスク」を「ビジネスリスク」として認識し、サイバーセキュリティ対策を推進しなければなりません。

しかし、ここに大きな課題があります。それは「企業は収集したサイバー脅威情報を整理できず、経営層に刺さる情報として活用できていない」ことです。技術的な観点からサイバー脅威を解説し、どのような対策を講じるべきか注意喚起を促す情報は多く存在します。しかし、経営者が知りたいのは、サイバー攻撃の手法や技術的な詳細ではありません。経営者にとって重要なのは、サイバー脅威が自社のビジネス継続性や信用、知的財産に対してどの程度のダメージを与え、どう対応するかなのです。

経営者は、「今、発生しているサイバー脅威が自社のビジネスに対してどれだけのマイナスインパクトを与えるか」「狙われている知的財産は何か」を把握し、具体的な対応策を講じることが重要です。そのためには、適切な判断が下せる情報を提供する仕組みが不可欠となります。

こうした仕組み作りは、行政と産業界が連携して行わなければなりません。例えば、海外でセキュリティに関する認証制度が策定された場合、日本企業にも影響を及ぼします。しかし、日本側に認証制度に相当する仕組みがなければ、迅速な対応は難しいでしょう。サイバー攻撃がグローバル化している現在は、行政と産業界が一体となり、日本としての制度設計やガイドラインを策定することが急務です。

経済産業省は産業界と緊密にコミュニケーションし、企業の自発的な取り組みを支援することで、日本のセキュリティ対策を推進する役割を担っています。企業が活動しやすいフィールドを作り、日本のサイバーセキュリティ対応の底上げを推進していきたいと考えています。



先進企業インタビュー

NTT執行役員
Chief Information Security Officer
セキュリティ・アンド・トラスト室長
横浜 信一 氏

「Strategy under Uncertainty」という言葉があります。不確実性の中での戦略ですね。サイバーセキュリティの世界で考えると、脅威インテリジェンスの重要性がますます高まっていますが、外部環境を先読みしようとしても、そこには不確実性が伴います。しかし、まったく予見できない攻撃にさらされるケースは多くありません。例えば、欧州や米国で発生しているサイバー攻撃を注意深く分析すれば、今後、日本でどのような脅威が発生するのか、ある程度のシナリオは描けます。そのシナリオを基として情報を収集し、対策を講じることも機先を制する第一歩でしょう。とは言うものの、日々現場も含めて苦労をしながら進めているのが現状です。

テクニカルな情報には、現場の技術者が一刻一秒を争って対応しなければならない重要情報が含まれています。ソフトウエアの脆弱性情報など、日々大量に流れてくテクニカルな情報の中で、優先順位をつけ、選別をし、弊社グループ内の事業会社と連携して対応を進めていく。事業会社の業務の特性や、事業会社の担当者の対応状況を見ながら、「この脅威への対応は絶対にすべきである」「担当者にこの脅威を報告しても、今他の脅威対応で手一杯なので対応できない。であれば優先順位を下げよう」ということを考え、判断します。

現場の担当者と判断をする人間との間の相互理解や信頼感が非常に大切だと考えています。私が昨年から率いるセキュリティ・アンド・トラスト室に「トラスト（信頼）」という言葉を入れたのも、セキュリティは組織間、個人間の信頼関係なくして進めることが不可能だと考えているからです。

テクニカルな情報に加え、ノンテクニカルな情報の収集も行っています。NTTが国内企業からグローバル企業に変わるというタイミングで、グローバルレベルでサイバーセキュリティポリシーや、トレンド、規制がどうなっていくのか、理解する必要があると考えました。各国の法規制や米国連邦政府の方針、GDPR（欧州一般データ保護規則）などが、自社のビジネスにどのような影響を及ぼすのかという視点で、世界の動向を注視しています。数年前、私は定期的に渡米し、官民連携の協議会や業界団体の方と話をし、グローバルのセキュリティトレンドをモニタリングしていました。継続的に続けていくと、米国で抱えている問題は、欧州も含めた世界全体の潮流になり、日本にも来るであろうと確信を持つようになりました。また、世界を代表する先進的な通信事業者たちは、ノンテクニカルな情報をどのように捉えているのかにも注目しています。欧米の通信事業者のCISOと、現状の課題や今後の方針について情報交換し、彼らの取り組みや視座を参考にしながら、「相場観」や「これ以上はやりすぎというバウンダリー（境界線）」を見極めることも重要な活動です。

このようにグローバルのセキュリティトレンドをモニタリングし、自社へのフィードインを実施しだしてから6〜7年経過します。だんだん積み重ねていると、勘所も分かり、さまざまな施策、例えば、サプライチェーンリスクマネジメントなどの強化に役立ちます。この先どうなるのか、といった感覚やスピード感も身についてきていると感じます。

「機先を制する」ためには、テクニカル、ノンテクニカルの両方の情報をベースにし、いずれ求められることを先読みし「ready」にしておくということが求められるのではないでしょうか。レベルを一段あげるわけですから、当然投資やリソースが必要になります。経営の意思がないとできません。リーダーがどれだけ引っ張っていけるかが鍵を握るでしょう。

MS&ADインシュアランスグループホールディングス
データマネジメント部長
三井住友海上　データマネジメント部長
松澤 寿典 氏

これまで損害保険会社を狙ったサイバー攻撃の目的は、個人情報を盗取し、それらの情報を闇サイトで販売して金銭を得ることだとされていました。しかし、現在は個人情報の取引価格は暴落し、企業も情報漏洩対策を強化しています。現在、台頭しているのが、ランサムウエア攻撃です。攻撃手法は刻々と変化します。経営層は攻撃者の狙いを把握し、「自社にとっての脅威は何か」を見極め、予算の配分や対策の最終的な判断を実施しなければなりません。セキュリティ担当者は、経営層が攻撃ターゲットの違いや脅威トレンドの変化を理解し、「どこにどれだけの予算を配分するか、どのような対策を講じるか」を判断できる情報を提供する必要があると考えます。

MS&ADホールディングスのセキュリティ対策の特徴として、関連会社や100以上ある海外拠点、業務委託先や代理店といったサプライチェーンの存在が挙げられます。各代理店や拠点の業種や業態、その規模によって、直面するセキュリティリスクが異なります。そのため、サプライチェーン全体に一律のセキュリティ対策を要求することは、現実的ではありません。日本国内で考えても、関連会社には金融庁のガイドラインに基づきガバナンスを推進すればよいのですが、保険代理店は専業とは限らず他の業務を営んでいる場合も多いので、それぞれの業界に合わせたガイドラインを検討する必要があります。北米、欧州、アジアなどに存在する海外拠点には、各国の法規制や文化に合わせた対応が必要となります。クラウド事業者などの業務委託先も含めて守備範囲が非常に広く、サプライチェーンを含めた事業におけるリスクは何なのかを日々察知し、対策を展開していくところが問われています。

経営会議で「海外拠点や代理店も含めてグループガバナンスとしてはこんな状況である」ということを報告する横から、新しい攻撃が増えていく現実があります。攻撃が日常的になっているので、「過去にできている」ということを報告してもほとんど意味ないがないと考えています。そのため、我々は、現地スタッフが自分たちのサイバーリスクを把握し、自立的にセキュリティ対策を講じられる仕組み作りに取り組んでいます。「このような脅威が増えているので、我々の拠点ではこの対策が必要だと考えている。対策を実現するための計画を検討し、リソースを確保する。」と自律的に動いてもらえるところを目指しています。各拠点のベストプラクティスを共有するような仕組み作りや、グループシナジーにむけ、中央集権的なグローバルオペレーションセンターの計画も考えています。現地スタッフが各拠点のリスクレベルに合わせて対応を講じられれば、「レジリエンス」が高まり、広域防御が実現できるのです。

我々は、サイバーリスクを自社への対応という側面で考える一方、リスクを正しく認識し社会に浸透させていくことも重要なミッションとなります。企業が適切なリスクをアセスメントして、リスク対策を推進することを今後も支援していきたいと考えています。

---

3. 2021年日本企業セキュリティ実態

2021年 Cyber IQ調査から見る
サイバーセキュリティに関する企業展望

「対応」「復旧」を中心としたセキュリティ投資が増加する

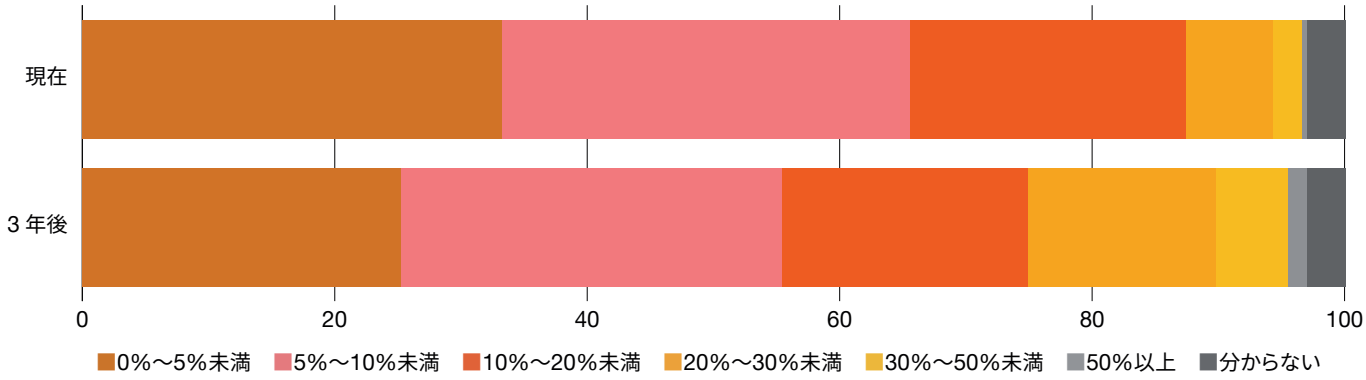
現在、情報技術関連予算のうち情報セキュリティ予算に10%以上を投資しているという回答は31.4%であるが、3年後には投資しているという回答は41.6%と増加している。回答者単位で結果を分析しても、全体のおよそ4割の回答において、情報セキュリティ予算を増額する意思があることが分かる。中でも現在「10%～20%未満」、3年後「20%～30%未満」と回答し、10%程度増額するケースが一定数存在する。具体的な領域としては、レポート本編でも述べたとおり「対応」および「復旧」に関する投資が進むと考えられる（図表11）。

インシデント対応費用の補償を後押しにサイバー保険への加入が進む

アンケートでは、現時点で加入していないという回答は75%になるが、3年後も加入していないという回答は約42%にまで減少する。今後加入を検討または補償内容の拡充を検討している企業がサイバー保険に期待する補償内容としては「危機管理」「個人情報の損失または盗難」「セキュリティ関連インシデントから発生した裁判」「インシデントへの応答」「インシデント回復」などが上位を占め、インシデント発生に関連した損失を補填したいと考えていることがうかがえる（図表12）。

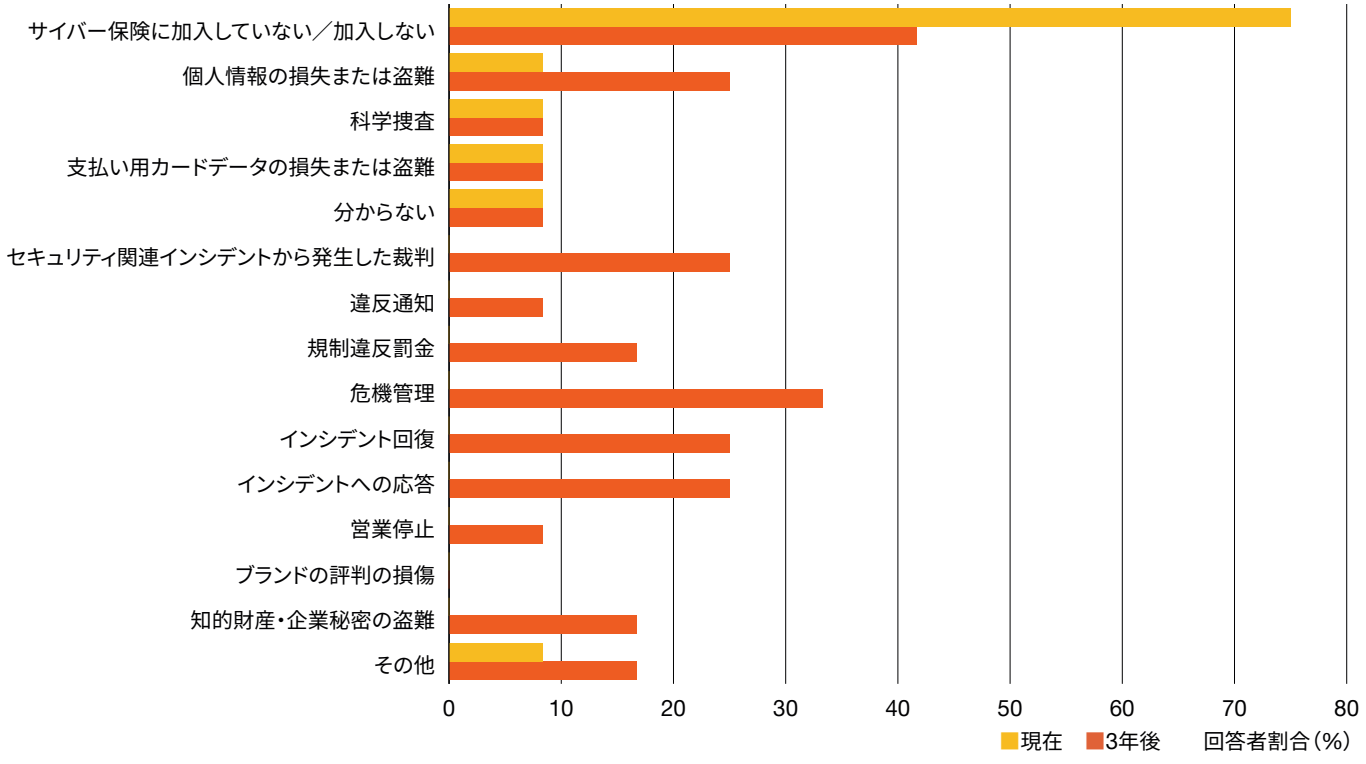
図表11：情報技術関連予算に占める情報セキュリティ予算の割合の現在と3年後（予定）の比較

設問　今年度、貴社では情報技術関連予算のうち、どの程度情報セキュリティ予算に計上しましたか。
また、3 年後はどの程度になると思いますか（それぞれひとつだけ）。



図表12：企業が加入するサイバー保険の補償内容と3年後に期待する補償内容

設問　現在、サイバー保険に加入している場合、どのような損失が補償されますか。また、3 年後、新たにサイバー保険に加入する、または、既存の補償内容の拡充を予定する場合、どのような損失の補償を期待しますか（それぞれいくつでも）。



企業は中央集権型のセキュリティガバナンスを指向している

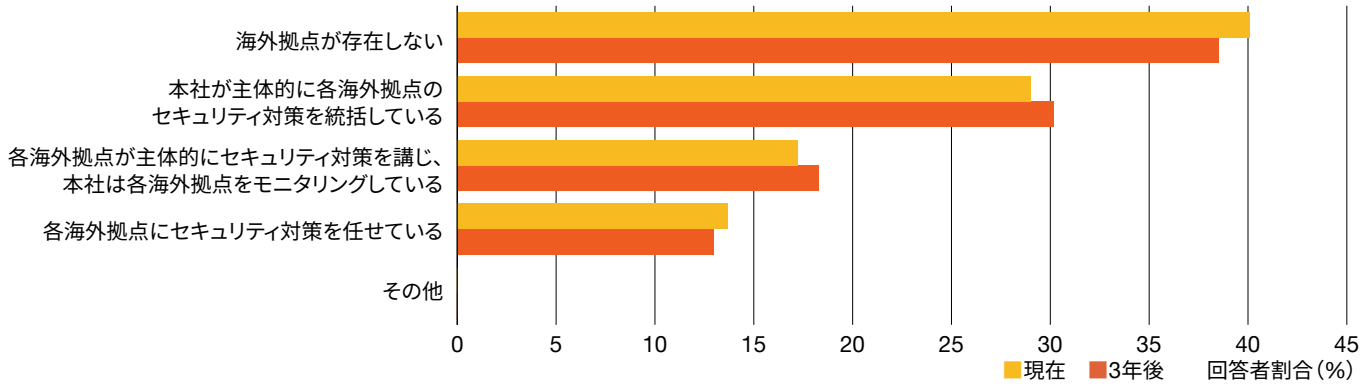
全体の約4割が「海外拠点は存在しない」と回答しており、残りの6割の半数に相当する約30%が「本社が主体的に海外拠点のセキュリティ対策を統括している」と回答している。3年後には「海外拠点にセキュリティ対策を任せている」という回答はわずかに減少し、本社がセキュリティ対策を統括あるいはモニタリングするという回答が微増している。このことから、今後海外拠点のセキュリティ統制には徐々に本社が関与していく傾向が強まる傾向があることが見て取れる（図表13）。

委託先まで含めたインシデント対応計画の整備が進む

現在多くの企業では「利害関係者とのセキュリティ規約の締結」により外部の協業先や事業委託先のセキュリティ統制を図っている。この対策により利害関係者との責任分界点は明確化されるものの、実際にインシデントが発生した場合は、委託元によるインシデント対応が求められること、市場での信頼性の低下の被害が委託元にも発生することなど、単に責任問題だけでは片づけられない課題と認識されるようになってきた。このため委託元は「利害関係者も含めたインシデント対応計画の策定」による利害関係者も含めたインシデント対応態勢の構築や、「利害関係者のリスク評価」による、より実効性のある利害関係者の管理など、利害関係者に対しより踏み込んだ統制を図る企業が増加すると予測される。一方で、現在・3年後ともに全回答の2割程度は「分からない」と回答しており、外部の協業先や事業委託先に対する有効なセキュリティ統制・対策を見いだせていない状況にある（図表14）。

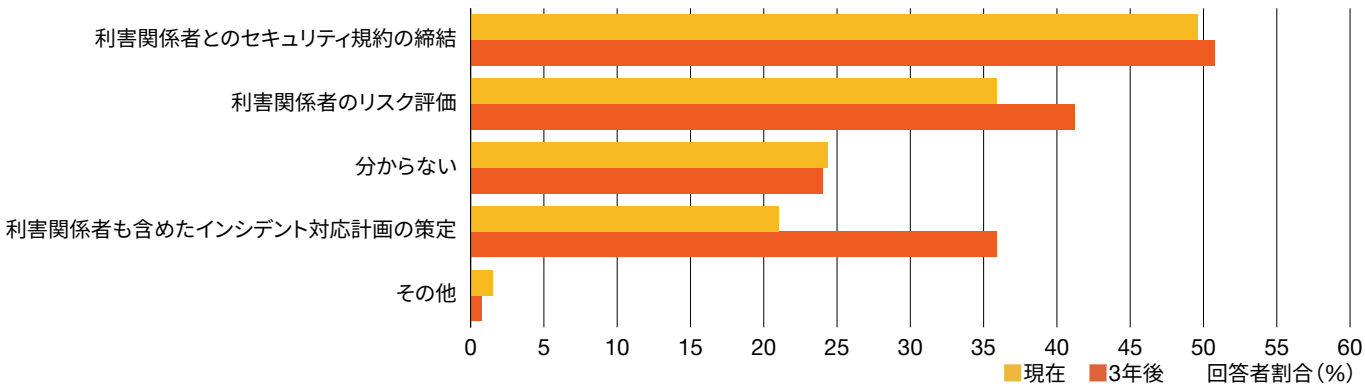
図表13：企業が実施する（3年後に実施を検討する）海外拠点のセキュリティ統制方法

設問　海外拠点が存在する場合、海外拠点のセキュリティ統制をどのように行っていますか。また、3 年後の海外拠点のセキュリティ統制をどのように行っていきたいと考えていますか（それぞれひとつだけ）。



図表14：外部の利害関係者に実施する（3年後に実施を検討する）セキュリティ対策

設問　現在、外部の利害関係者（協業先、事業委託先等）に対して行っているセキュリティ対策を選択してください。
また、3 年後に行っていると思うセキュリティ対策を選択してください（それぞれいくつでも）。



クラウド標準セキュリティ機能の利用は限定的だが、ゼロトラストを契機に利用が加速する

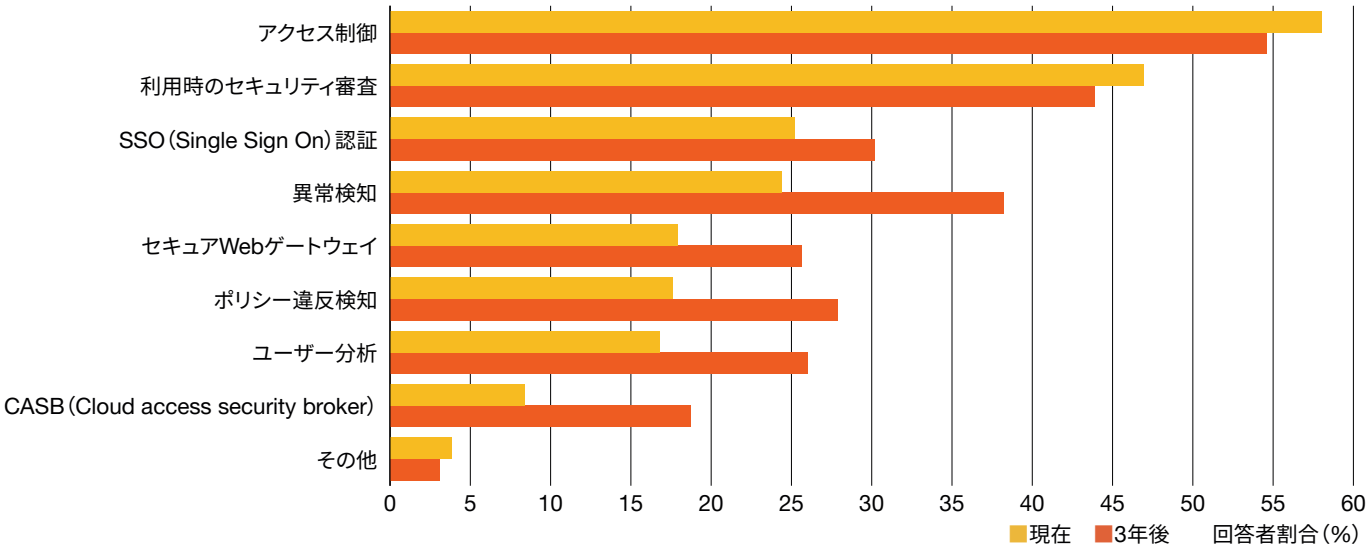
現在、クラウドサービス上に機密データを保管しているという回答は、約40%にとどまっているものの、今後、保管予定または検討中の企業を合わせると、約70%に上る。そのため、今後はオンプレミス環境ではなく、運用管理や業務効率などに大きなメリットがあるクラウド環境を中心としたビジネスやサービス提供が主流となっていくことが予想される。また、現在多く実施されているクラウドのセキュリティ対策は、「アクセス制御」や「クラウド利用時のセキュリティ審査」のみにとどまっており、クラウドのセキュリティ対策に注力できている企業は少ないことがうかがえる。ただし、3年後は「異常検知」や「ポリシー違反検知」などのセキュリティ対策を講じているという回答が顕著に増加しているため、ゼロトラスト・アーキテクチャへの移行などをきっかけに今後クラウドのセキュリティ対策が推進されるものと考えられる（図表15）。

セキュリティ人材不足と解決に向けた見通し

全回答の約8割が「セキュリティ人材が不足している」と回答しており、改めて人材不足に直面している現状が確認された。また、セキュリティ人材不足を解消するための最も良い方法については、「既存の人材育成（34.5%）」「外部委託（32.0%）」「新規雇用（25.5%）」のような「ヒトを増やす」対策であった。一方で、セキュリティ人材不足解消の最も良い方法として「自動化などによるセキュリティ業務の削減」という回答は6.5%にとどまっており、自動化がセキュリティ人材不足の解消につながると期待している企業は少ないようだ。ただし、3年後に何かしらのセキュリティ業務の自動化に取り組んでいるという回答は90%を超えているため、今後セキュリティ業務自動化の重要性は高まっていくことが考えられる（図表16）。

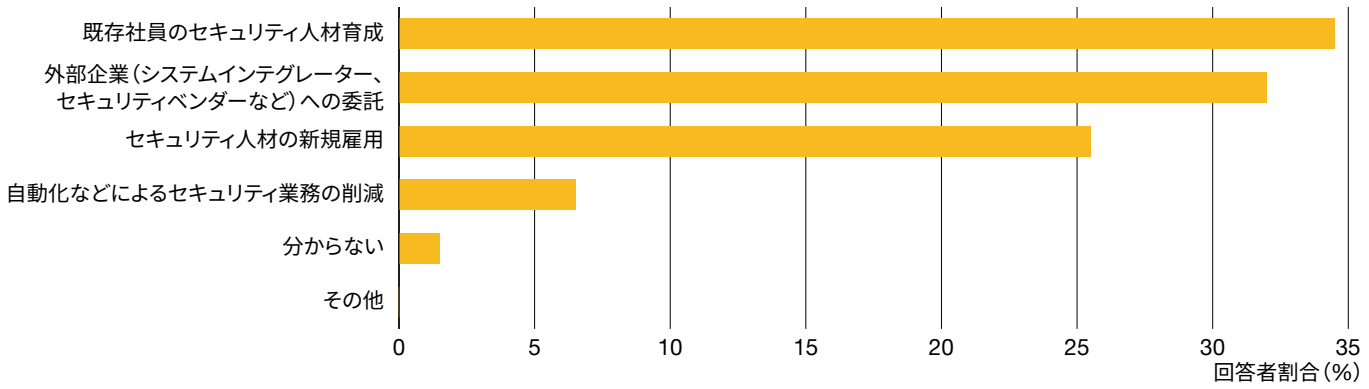
図表15：企業が実施する（3年後に実施を検討する）クラウドサービスの利用におけるセキュリティ対策

設問　現在、貴社では、クラウドサービスの利用においてどのようなセキュリティ対策を講じていますか。
また、3 年後にどのようなセキュリティ対策を講じていると思いますか（それぞれいくつでも）。



図表16：企業が考えるセキュリティ人材不足の解消方法

設問　セキュリティ人材不足をどのように解消するのが最も良いと思いますか（ひとつだけ）。

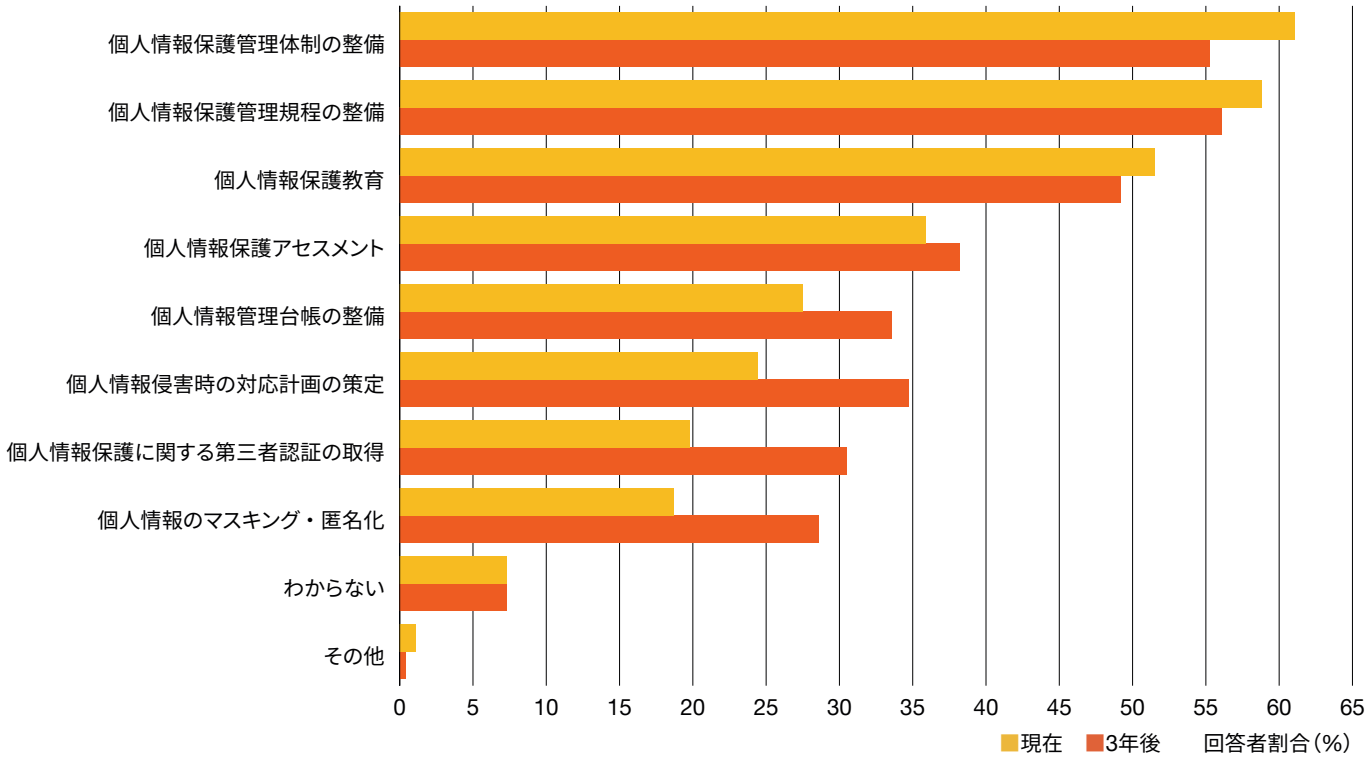


各国法令の施行／改正に伴うプライバシー保護への感度の高まり

近年、個人情報漏洩のインシデントが日常的に発生しており、消費者の個人情報漏洩の不安感が高まっている。また海外においても個人情報保護法の施行や改正が進んでおり、その対応に迫られている企業も多い状況である。そのため、自組織の個人情報保護対策の成熟度を客観的に把握する、また、自組織が提供しているサービスの安全性を消費者に示すために、「個人情報保護に関する第三者認証の取得」に取り組むという回答が増加傾向にあると考えられる。さらに、国内外における法規制の施行／改正という点において、企業に求める要件が厳格化しているといわれており、それら要件へ対応するために「個人情報管理台帳の整備」「個人情報侵害時の対応計画の策定」「個人情報保護に関する第三者認証の取得」「個人情報のマスキング・匿名化」について「3年後に取り組んでいる」という回答が大きく増加していると考えられる（図表17）。

図表17：企業が実施する（3年後に実施を検討する）個人情報保護対策

設問　現在、個人情報保護として取り組んでいるものを選択してください。また、3 年後に取り組んでいると思うものを選択してください（それぞれいくつでも）。



おわりに

新型コロナウイルス禍において、企業のクラウド利用の広がりにあわせてサイバー攻撃の手法が進化し、事業継続に影響を及ぼす事例も増えてきました。特別高度なハッキングの知識がなくてもサイバー攻撃のノウハウを売買でき、比較的容易にサイバー攻撃を実装できる、サイバー攻撃の産業化という構造も昨今の特徴ではないでしょうか。

変わりゆくサイバーセキュリティを取り巻く環境、そして高度化されたサイバー脅威により、私たちはサイバーセキュリティに対するこれまでの観念を改めなければなりません。サイバーインテリジェンスを活用し、最新の脅威動向を捉え、フォーカスすべき対策を判断し、日々動的に調整する必要があります。

本稿でご紹介した「機先を制するセキュリティへの転換」、その実現に向けた具体的なアクションをご検討いただき、セキュリティ対策の大きな変革への一歩を踏み出す時が来ています。

お問い合わせ先

PwC Japanグループ
www.pwc.com/jp/ja/contact.html

監修

林 和洋
PwCコンサルティング合同会社
パートナー

丸山 満彦
PwCコンサルティング合同会社
パートナー

執筆

村上 純一
PwCコンサルティング合同会社
ディレクター

渕 遼亮
PwCコンサルティング合同会社
マネージャー

宮内 美里
PwCコンサルティング合同会社
マネージャー

展 天承
PwCコンサルティング合同会社
シニアアソシエイト

www.pwc.com/jp

電子版はこちらからダウンロードできます。 www.pwc.com/jp/ja/knowledge/thoughtleadership.html
発刊年月：2021年12月　　管理番号：I202109-01