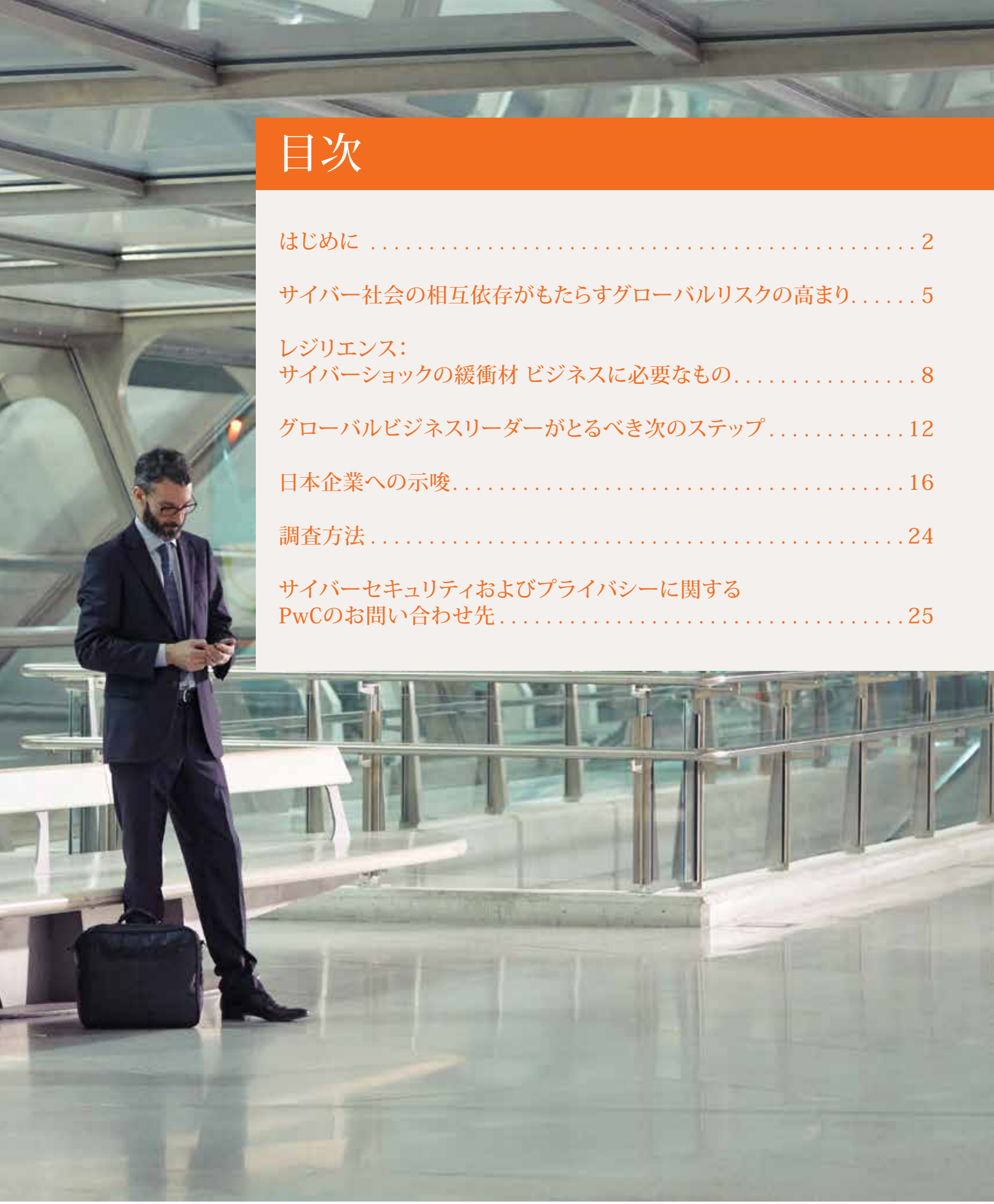
www.pwc.com/jp

サイバーセキュリティおよびプライバシー

サイバーショックに備え、デジタル社会を強化する

グローバル情報セキュリティ調査2018 Vol.1

pwc



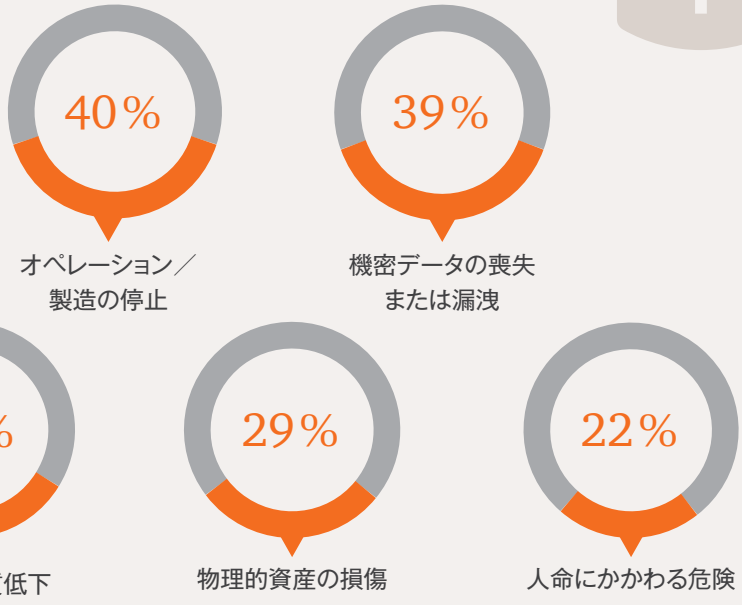
目次

はじめに

大規模なサイバーセキュリティ侵害は、ほぼ毎日メディアに取り上げられ、消費者や経営陣に警鐘を鳴らすとともに、それが日常的なこととなりつつある。このようなインシデントが注目を集めているにもかかわらず、世界中の多くの企業は、ますます複雑化するデジタル社会において、新たなサイバーリスクの把握と管理に悪戦苦闘しているのが現状だ。データや相互接続性への依存度が高まる中、サイバーショックに対するレジリエンス、つまり連鎖的な破壊をもたらす大規模な障害にも耐え得る回復力を備えておくことが、かつてないほど重要性を増している。

これまでのところ、サイバー攻撃による死亡事故は報じられたことはなく、物理的破壊に至った例も比較的少ない[1]。しかし、サイバー攻撃の破壊力はますます明らかになってきており、特に地政学的脅威において顕著である。例えば、2015年12月にトルコで発生したサイバー攻撃は、同国の銀行、メディア、政府で使用されているネットワークに被害を及ぼした[2]。その後、同月内に、送電網のダウンを狙った最初の事例となるサイバー攻撃が、ウクライナの送電網システムを標的として行われ、23万人もの住民が影響を受ける大停電が引き起こされた[3]。この攻撃では同国の電話システムも標的とされ、停電を報告する手段が遮断されたため、復旧にも支障が出ることとなった[4]。さらに2017年7月には、ウクライナのコンピューターを標的としたPetyaによるサイバー攻撃が行われ、世界中のビジネスオペレーションが混乱に追い込まれた。このように、大規模な影響があるインシデントリスクの高まりによって、サイバー攻撃の破壊力が世界経済に影響を及ぼす懸念が高まってきている[5]。

オートメーションおよびロボティクスシステムに対するサイバー攻撃が成功した場合に予想される結果



出典：PwC、CIOおよびCSO、グローバル情報セキュリティ調査2018、2017年10月18日
回答者数：9,500人

1 The Cipher Brief, Cyber Deterrence Is Working – So Far, July 23, 2017
2 Harvard University Belfer Center for Science and International Affairs, Too Connected To Fail, May 2017
3 Wired, Inside the cunning, unprecedented hack on Ukraine's power grid, March 3, 2016
4 US Homeland Security Advisory Council, Final Report of the Cybersecurity Subcommittee: Part I - Incident Response, June 2016
5 The Wall Street Journal, The Morning Download, Sept. 11, 2017

サイバー空間の危険性が増してきていることは、世界中の経営者が認めている。私たちが行ったグローバル情報セキュリティ調査2018（GSISS）では、オートメーションやロボティクスを利用する企業のトップが、サイバー攻撃による潜在的で重大な影響を認識していることが示されている。回答者の40％がサイバー攻撃の最大の潜在的影響としてオペレーションの停止を挙げ、39％が機密データの漏洩、32％が製品の品質低下、29％が物理的資産の損傷、22％が人命にかかわる危険を挙げた。

「多くの企業は、デジタルリスクの評価を行い、不可避の事象に対するレジリエンスの構築に重点を置く必要がある」
– Sean Joyce, US Cybersecurity and Privacy Leader, PwC

このような認識があるにもかかわらず、サイバー攻撃のリスクにさらされている多くの企業では、リスクに対処する準備が行われていない。GSISS2018の調査で対象となった122カ国、9,500人の回答者のうち、44％は包括的な情報セキュリティ戦略を策定していないと回答している。また48％が従業員に対するセキュリティ意識啓発のトレーニングプログラムを用意していないと答え、インシデントレスポンスにかかわるプロセスが未策定という回答は54％に上る。「多くの企業は、デジタルリスクの評価を行い、不可避の事象に対するレジリエンスの構築に重点を置く必要がある」とPwCのUS Cybersecurity and Privacy Leader、Sean Joyceは述べている。

「サイバーハルマゲドン」が勃発するという誇張表現も、これとは逆に、サイバー攻撃の脅威は平凡なものにすぎないという見方も、経営陣にはうまく届いていない。しっかりとした議論をグローバルで行い、サイバーショックに対するレジリエンス構築に役立つ具体的な助言を得る方がずっと生産的だ。GSISS2018のシリーズ第一弾である本書では、そこに着目して結果をまとめている。

サイバー社会の相互依存がもたらすグローバルリスクの高まり

世界経済フォーラム（WEF）によると、インフラネットワークにおけるサイバー相互依存の高まりはトップレベルの世界的なリスク要因の一つであるとされている。WEFのグローバルリスク報告書2017年版では、サイバー攻撃、ソフトウエアの欠陥、その他の要因により、「ネットワーク全体に連鎖し、社会に予期しない影響を及ぼす」システム障害が発生する恐れがあることが指摘された[6]。

また、米国家情報会議が最近発表したグローバルトレンド報告書でも同様に、重要インフラの脆弱性によってサイバーディスラプション（「致命的な結果」を伴う潜在的に大規模な破壊）が起きる「差し迫った」リスクに、社会が直面していることが警告されている[7]。サイバー以外の災害のケーススタディを見てみると、後続の事象の引き金となっているのは、電源喪失であることが多い。多くのシステムは瞬時に、あるいはその日のうちに影響を受ける。つまり一般的に、問題が連鎖する前の段階で初期の問題に対応する時間は、ほとんどないに等しい[8]。重要ネットワークと非重要ネットワークの間の相互依存関係は、時として問題が発生するまで認識されずに放置されていることすらある[9]。

世界各国の多くの人々、特に日本や米国、ドイツ、英国、韓国は、他国からのサイバー攻撃を危惧している[10]。サイバー攻撃を仕掛ける各種ツールは世界のそこかしこに散らばっている。また、小国も大国に引けを取らない能力を獲得しようとしている。米国家安全保障局（NSA）のハッキングツールが流出したことで、悪意あるハッカーがより高度な能力を手に入れてしまうこととなった[11]。サイバー攻撃が発生した際、標的となった企業の大半は、犯人をはっきりと特定できないという。GSISS2018によると、攻撃元を特定する能力に強い自信を持っているという回答は、わずか39％にすぎない。

---

6 World Economic Forum, 2017 Global Risks Report, January 2017
7 US National Intelligence Council, Global Trends: Paradox of Progress, January 2017
8 CascEff, Cascading effects: What are they and how do they affect society? July 31, 2017
9 2001年9月11日テロ攻撃以降のインターネットの機能停止は、イベントの連鎖によって起きた:大規模データセンターが燃料式の補助発電機を使用するために必要な電力の不足、都市部の空気の質の悪化によるデータセンターの冷却の困難、燃料消費の加速、緊急時の車両制限による燃料供給の滞りを経て、最終的に燃料の枯渇による発電機能の停止に至った。Harvard University Belfer Center for Science and International Affairs, Too Connected To Fail, May 2017を参照
10 The Pew Research Center, Spring 2017 Global Attitudes Survey, August 2017
11 PwC, Bold Steps to Manage Geopolitical Cyber Threats, 2017

攻撃元を特定する能力に強い自信を持っているという回答は、わずか39%にすぎない

出典：PwC、CIOおよびCSO、
グローバル情報セキュリティ調査2018、2017年10月18日

セキュリティ対策が十分ではないIoT（Internet of Things：モノのインターネット）デバイスの生産量増加に伴い、サイバーセキュリティの脆弱性も広範囲に及ぶようになった[12]。データの完全性に対する脅威が高まった結果、システムの信頼性が損なわれ、重要インフラの損傷を通じて人命が危険にさらされる恐れさえ出てきた[13]。

G7の指導者らは、2017年5月に採択した声明の中で、サイバー攻撃に対抗し、重要インフラや社会への影響を低減するために協力していくことを宣言した。2カ月後のG20では、指導者らはデジタルテクノロジーにおけるサイバーセキュリティと信頼の必要性を改めて確認した。これから待ち受けている課題は大きい。国際連合の専門機関の一つ、国際電気通信連合は2017年版世界サイバーセキュリティ指標報告書の中で、グローバルな相互接続が「ありとあらゆるもの」をサイバーリスクにさらし、「国の重要インフラから基本的人権までの全てが侵害される恐れがある」と述べた[14]。

国連の2017年版「Global Cybersecurity Index」によれば、サイバーセキュリティの準備状況には国によって（「地域間でも、地域内でも」）大きな差があるという[15]。国連の中でも、サイバーセキュリティに関する戦略を発表済みの加盟国は38%、独立したサイバーセキュリティ戦略を策定済みの加盟国は11%にすぎないことが分かっている。サイバーセキュリティ戦略を現在策定中であるとする加盟国も12%のみだ。加盟国の61%が、国直轄の緊急時対応チームを構築したと回答したが、サイバーセキュリティインシデントの評価指標を公開している加盟国はわずか21%にとどまっている。

12 PwC、『IoTの可能性を探る』、2017
13 当時の国家情報長官James Clapper氏は2016年に議会に対し、次のように述べた。「今後のサイバー攻撃は、意志決定に影響を及ぼし、システムの信頼性を低下させ、物理的悪影響を引き起こすために、完全性（正確性および信頼性）を損なうデータ改変または操作に重点が置かれることはほぼ確実だ。公共施設やヘルスケアなどの環境でIoTデバイスや人工知能（AI）がさらに広く採用されれば、これらの潜在的影響は一層深刻になるだろう」
14 United Nations International Telecommunication Union, Global Cybersecurity Index report, 2017
15 The report ranked Singapore, the United States, Malaysia, Oman, Estonia, Mauritius, Australia, France, Georgia, and Canada as the most committed member states

GSISS2018の結果、企業における包括的なサイバーセキュリティ戦略の見直し頻度が特に高い国は日本（72％）で、サイバー攻撃が国の最大のセキュリティ脅威となっていることが分かった[16]。また、マレーシア（74％）も国連の「Global Cybersecurity Index」で非常に高い評価を得ている国である。それぞれ東アジアおよび太平洋地域に属しており、世界経済フォーラムによると、サイバー攻撃がビジネスリスクの上位5位以内に入る地域とされている[17]。

攻撃に対する準備態勢が整っていても、必ずしもリスクが低いとは限らない。国連の2017年度版の「Global Cybersecurity Index」では、加盟国の中で最も熱心にサイバーセキュリティ対策に取り組んでいる国として、米国がシンガポールに次いで第2位とランク付けされている。しかし米国のインフラは、世界経済フォーラムが北米の最大のビジネスリスクと見なす「大きな経済的損害、地政学的緊張、インターネットに対する広範な信頼の失墜をもたらす、大規模なサイバー攻撃やマルウェア」[18]に対し、今も脆弱なままである。米国土安全保障省によると、国内の重要インフラのうち1件のサイバーセキュリティインシデントによって、500億米ドルの経済的損害、2,500人の即時の人的被害、国防の重大な低下を招く可能性があるものが、60以上もあるとされている[19]。

多くの人々にとって、サイバー攻撃のリスクは現実問題だ。ピュー研究所の調査によると、米国民の圧倒的多数が、今後5年以内に米国の公共インフラ、銀行、金融システムに大規模なサイバー攻撃が仕掛けられるだろうと考えている。一方で、ほとんどの情報セキュリティ専門家は、米国の重要インフラがサイバー攻撃を受けるのは、2年以内であろうと予測している[20]。

16 The Pew Research Center, Spring 2017 Global Attitudes Survey, August 2017
17 World Economic Forum, 2017 Global Risks Report shareable infographics, January 2017
18 World Economic Forum, 2017 Global Risks Report, January 2017
19 "Additional views" statement by Sen. Susan Collins (R-ME) in US Senate Report 114-32, April 15, 2015
20 Black Hat, The 2017 Black Hat Attendee Survey: Portrait of an Imminent Cyberthreat, July 2017

このことが示すように、どれほど準備が整えられているかにはかかわらず、全ての企業が戦略的なサイバーセキュリティ目標の実行状況を検証することは不可欠であると言える。ホワイトハウスの国家インフラ評議会は、2017年8月の報告書で、効果的なツールや実務があるにもかかわらず、多くの米インフラ企業が基本的なサイバー対策を実践していない現状を示した[21]。事実、同報告書の著者によると、多くの企業は連邦政府によって提供されているサイバー脅威のスキャン、検知、低減、防御のためのツールが利用できることにすら気付いていないという。

レジリエンス：サイバーショックの緩衝材
ビジネスに必要なもの

米国家情報会議は2017年、「将来成功する国家は、経済、環境、社会、そしてサイバー攻撃に対してレジリエントなインフラ、知識、対外的な関係に投資する国家であろう」と述べた。「同じことは今後成功を収める企業にも言える。レジリエントな企業は、オペレーションの継続、顧客との信頼構築、好業績達成のためのベストな地位を築くだろう」。では、組織はどのようにしてサイバー攻撃の影響を吸収できるだけの強さを獲得できるようになるのだろうか？その答えは、GSISS2018の結果から読み取ることができる。

経営陣はサイバーレジリエンスの構築に対し、より重い責任を想定しなければならない。民間部門では、経営陣が事業運営に伴うリスクについても説明責任を負わなければならない。取締役会に求められるのは、実効性のある監督と積極的なリスク管理だ。事業継続、後継者育成計画、戦略的連携、データアナリティクスのための戦略がカギとなる。しかし、GSISS2018では、大半の企業の取締役会が自社のセキュリティ戦略や投資計画に積極的に関与していない実態が浮き彫りになった。

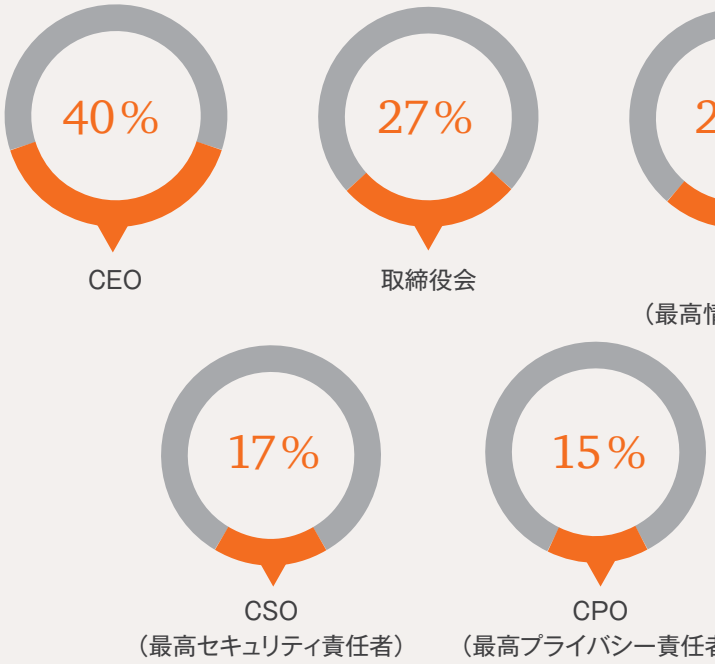
21 National Infrastructure Advisory Council, Securing Cyber Assets, August 2017

GSISSでは、自社の取締役会が包括的なセキュリティ戦略に積極的に参加しているという回答は44％にすぎなかった。「多くの取締役会が、サイバーセキュリティをいまだにITの問題と捉えている」とMatt Olsen氏（IronNet Cybersecurity共同設立者、事業開発および戦略責任者。元米国家テロ対策センター所長）は指摘する。全米取締役協会（National Association of Corporate Director）が2016年から2017年にかけて上場企業および非上場企業を対象として実施した調査によると、サイバー攻撃に対する防御が適切に行われていることに自信を持つ役員はほとんどいない[22]。取締役会がセキュリティ対策に関与しない以上、不安があるのも当然だ。全GSISSの回答者のうちほぼ半数が、リスクのみでもセキュリティ支出に影響する根拠となると回答し、約30％がそうは思わないとの回答、残りは分からないとの回答であった。

GSISSの回答者の大多数（66％）は、セキュリティ支出が各事業の収益と連動していると答えている。ただし、どちらとも言えないという回答も相当数（34％）ある。最高情報セキュリティ責任者（CISO）の存在が徐々に重要となってきている。GSISS2018によれば、企業のCISOやCSO（Chief Security Officer）が、CIOではなく、CEOまたは取締役会の直属であることが一般的になってきている。「自社のサイバーセキュリティネットワークに関する取り組み状況を、取締役会が理解できるようにするのはCISOの責務だ」とKeith Alexander氏（IronNet Cybersecurity創設者兼CEO。元米サイバー軍大将、国家安全保障局長官）は語る。「発生した全てのサイバー攻撃の他、サイバー領域におけるトレーニングや設備、ツールが不足しているという情報も提供すべきだ。取締役会が自社の直面しているリスクを理解し、対応する責任を果たせるように、CISOは不足しているものが何かを強調しなければならない」。

22 「非常に自信がある」と回答したのは、上場企業の役員の5%、非上場企業の役員の4%にすぎなかった。最多の回答は「まあまあ自信がある」（上場企業の役員の42%、非上場企業の役員の39%）であった（National Association of Corporate Directors、2017 Cyber-Risk Oversight Handbookの調査データより）

CISO、CSO、または情報セキュリティ統括責任者は、どの組織／役職の直属となっていますか？



出典：PwC、CIOおよびCSO、グローバル情報セキュリティ調査2018、2017年10月18日
回答者数：9,500人

組織はリスクを明らかにするために、さらに深く堀り下げなければならない。社会において、また社内においてもより強固なサイバーレジリエンスを実現するためには、新しいテクノロジーにつきものの新たなリスクを見つけ出し管理する、協調的な取り組みが求められる。企業がデジタルの発展に必要なセキュリティ対策をとるには、適切なリーダーシップとプロセスを備えておかなければならない。多くの企業はまだこの取り組みに着手したばかりだ。

例えば、ビジネスエコシステム全体のIoTのリスクを評価する計画があるという答えは、比較的少数の回答者からしか得られていない。IoTのセキュリティの責任の所在は企業によってさまざまで、29％がCISO、20％がエンジニアリングスタッフ、17％がCRO（最高リスク責任者）であるとしている。サイバーセキュリティ責任者にいたっては、いまだに多くの企業で不在のままだ。約半数（52％）の回答者がCISOを、45％がCSOを、47％が社内業務支援のための専任セキュリティ担当者を設置していると答えている。多くの企業では、サイバーリスクをより積極的に管理する余地が残されている。バックグラウンドチェックを行っていると答えた回答者は半数にとどまる。侵入テスト、脅

ビジネスエコシステム全体のIoTリスクを評価する計画があると答えた回答者は34%のみ

出典：PwC、CIOおよびCSO、グローバル情報セキュリティ調査2018、2017年10月18日

威分析、情報セキュリティの能動的監視、インテリジェンスと脆弱性の評価など、ビジネスシステムにおいてサイバーリスクを検知するための主要プロセスを採用しているという回答は半数に満たない。

ステークホルダー間でのより一層の情報共有および協力も求められている。セキュリティレベルを上げて将来的なリスクの可能性を低減するために、競合を含む同業他社と正式に協力しているとした回答は、58%にとどまった。信頼でき、タイムリーで、かつ実用的なサイバー脅威情報は、レジリエンスを支える迅速な対応能力のための重要な成功要因だ。組織、分野、国、地域間の壁を超え、サイバーショックに耐え得る能力を構築できるかどうかは、チームとしての努力にかかっており、より深く重要な関与なくして十分な効果を得ることは難しいであろう。

共有される情報が実用的なものであるかどうかも重要である。活動によって同業他社との間でより実用的な情報を共有し、受け取ることができるようになったとの回答は、他社との協力にかかわっているGSISSの回答者のうち半数にとどまった。

バックグラウンドチェックを行っているという回答は半数にとどまる

出典：PwC、CIOおよびCSO、グローバル情報セキュリティ調査2018、2017年10月18日

グローバルビジネスリーダーがとるべき次のステップ

最高責任者らが先頭に立つこと、そして取締役会が関与することは必須だ。ビジネスをけん引する幹部層こそがサイバーレジリエンスの構築責任を負わなければならない。企業全体のサイバーリスクおよびプライバシーリスクを横断的に管理する、トップダウンの戦略を策定することが不可欠だ。レジリエンスは、業務オペレーションと一体化されるべきである。企業のリスク管理戦略は、自社が直面しているサイバー脅威情報の正確な理解と、どの資産が最も厳格な保護を必要とするかの認識とともに伝えられなければならない。加えて、これと矛盾しないリスク選好フレームワークも必要である。経営陣は組織のあらゆるレベルにおいて、サイバーリスク管理の文化醸成に努めなければならない。

リスク回避のみを目的とするのではなく、利益を得る手段としてレジリエンスを追求すべきである。リスクに対するより強力なレジリエンスの獲得は、長期的な業績の向上にも繋がる。例えば日本では、2011年に津波が起こる前にエンタープライズリスクマネジメント（ERM）の取り組みに事業継続管理を組み込んでいた企業は、競合他社よりも早く業務を再開でき、また災害後の市場シェアを伸ばすことができた[23]。世界各国の政府は、主要業界のレジリエンス強化のために有用なプラクティスやテクノロジーを開発し、広めることで、長期的な経済・国家安全保障上の利益を得ている。

23 PwC, Building a Risk Resilient Organisation, 2012

目的を持って協力し、得られた教訓を生かす。官民のトップは、レジリエンスおよびリスク管理の強化のみならず、サイバー依存性および相互接続のリスクを識別し、マッピングし、テストするためにも、国、分野、組織の境界を超えて協力しなければならない。説明責任、法的義務、責務、結果管理、ノルマといった厄介な問題に対しても同様である。そのためにも、組織はこれまでに得た知見を活用するべきである。

- 災害対応時におけるケーススタディを見てみよう。例えば2016年、ハリケーン・サンディの後に非常に効果的に電力復旧ができたことの主たる要因を調査した結果、サイバーセキュリティの領域においては当該要因が欠如していることが分かった。この調査結果には、サイバー攻撃に関連する個々の課題を解決するための、オールハザード対応システムが構築できる可能性が示されている[24]。
- 全米取締役協会の『2017年度版サイバーリスク管理ハンドブック（2017 Cyber-Risk Oversight Handbook）』では、役員が「組織のシステムが経済的に可能な範囲で最大限レジリエントであるために、経営陣が十分関与しているかを確認する必要がある」と強調されている[25]。世界経済フォーラムが2017年1月に発表したサイバーレジリエンスの原則も、入手可能なツールの一つである。
- 重要なシステムの開発者は、新アメリカ安全保障センターの2014年の報告書で提唱されているように、システムが「可能な限り予測可能で、かつ正常に」停止するように設計するべきである[26]。
- 情報共有分析機関（ISAO：Information Sharing and Analysis Organization）から新たに発行されたガイドラインは、ステークホルダー間でのサイバー脅威情報や過去の教訓をより効果的に共有するために役立つであろう。

24 The Johns Hopkins University Applied Physics Laboratory LLC, Superstorm Sandy: Implications for Designing A Post-Cyber Attack Power Restoration System, March 2016
25 National Association of Corporate Directors' 2017 Cyber-Risk Oversight Handbook
26 Center for a New American Security, Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies, 2014

- ニューヨーク・サイバー・タスク・フォースが2017年9月に公開した報告書では、最小のコストで最大の効果を得るさまざまなサイバーセキュリティのアプローチが提唱されている。同タスクフォースのエグゼクティブディレクター、Jason Healey氏によれば、クラウドベースのテクノロジー[27]は、デザイン段階でセキュリティを組み込んだアーキテクチャおよび基盤を提供できるため、サイバーセキュリティを向上させる大きな可能性を秘めている。「効果が見えてくるのはこれからだ」(Healey氏)。
- 新たな研究がチャンスを生み出すかもしれない。一例として、米エネルギー省(DOE)は2017年9月、同省の国立研究所およびパートナーに対して、送電網および石油・ガスインフラのレジリエンスとリスク管理強化のためのサイバーセキュリティツール開発に、賞金2,000万米ドル以上を拠出すると発表した[28]。

相互依存に対するストレステストを実施する。世界の全主要産業界で、リスク管理のための情報取得を目的としたサイバー攻撃シナリオのシミュレーションを行い、相互依存に対するストレステストを実施するとよいだろう。In-Q-TelのCISOであるDan Geer氏は、次の質問に対する答えが得られるように、サイバーセキュリティのストレステスト用シナリオを作成することを提唱している。「依存先に障害が発生したとしたら、自社は耐えられるだろうか?」[29]。この考え方はハーバード大学ベルファー科学・国際問題センターが2017年5月に公開した調査でも支持されており、重要インフラセクターのスポンサーに規制機関を設置することや、当該テストを検証することの潜在的価値が強調されている[30]。

金融分野では近年、FS-ISAC(Financial Services Information Sharing and Analysis Center)がFSARC(Financial Systemic Analysis & Resilience Center)やGlobal Resilience Federationの確立を目指すなど、自発的な取り組みが行われている。このような取り組みにより、他分野でも利用可能なサイバーセキュリティモデルが生み出されるだろう。同理事長兼CEOを務めるBill Nelson氏によると、FS-ISACでは、組織がサンドボックス内でサイバー攻

27 クラウドの詳細については、PwC、『先進的サイバーセキュリティおよびプライバシーの実現』、2017およびNew York Cyber Task Force, Building a Defensible Cyberspace, Sept. 28, 2017を参照
28 US Department of Energy, press release, September 2017
29 Dan Geer, For Good Measure: Stress Analysis, login: Volume 39, Number 6, USENIX, December 2014
30 Harvard University Belfer Center for Science and International Affairs, Too Connected To Fail, May 2017

撃をシミュレーションすることでレジリエンスをテストできるように、仮想サイバー領域の構築に向けた概念実証アプローチを模索しているという。エネルギー分野では、北米の送電網およびその他の重要インフラに対するサイバー攻撃および物理的攻撃をシミュレーションするGridEx演習を、2年に一度実施している。「実戦さながらの演習。これに代わる手段は他にない」とIronNet CybersecurityのMatt Olsen氏は語る。

データの操作や破損に繋がるリスクに一層集中する。Dan Geer氏は2017年4月のインタビューで、今後は機密性に代わって、完全性が民間部門におけるサイバーセキュリティの最も重要なゴールになるだろうと予言した。さらに軍事分野では、「完全性を攻撃する武器は、既に機密性を攻撃する武器をしのぐ、はるかに強力なものとなっている」と付け加えた[31]。金融分野のSheltered Harborイニシアチブでは、他分野でのこうした新たなリスクへの対応に役立つモデルや教訓を提供できる可能性がある。こうした取り組みにより、銀行が大規模なサイバー攻撃を受けた際に口座データを復元・復旧するのに役立つ標準が策定されている、とNelson氏は説明する。米国立標準技術研究所（NIST）が2017年9月にドラフトを公開した新しい実践ガイド“Data Integrity：Recovering from Ransomware and Other Destructive Events”[32]では、データ破損からの効果的な復旧のためのガイダンスが提供されている。国家安全保障通信諮問委員会が本年初めに作成した報告書ドラフトでは、ブロックチェーンの利用が「トランザクションやデータの完全性が非常に重要な場合に特に関連性が高い」であろうとされている[33]。

組織の回復力を強化し、破壊的なサイバー脅威に耐え、セキュアなデジタル社会を実現する。そのためにリーダーが意味ある行動を起こせるチャンスは、今まさに目の前にある。GSISS2018第二弾では、関連するテーマとして、デジタル社会におけるプライバシーおよび信頼について取り上げる。

31 Dan Geer, closing keynote at SOURCE, Boston, April 27, 2017
32 US National Institute of Standards and Technology, Data Integrity: Recovering from Ransomware and Other Destructive Events, issued in draft in September 2017
33 US National Security Telecommunications Advisory Committee, Draft Report to the President on Emerging Technologies Strategic Vision, 2017

日本企業への示唆

本セクションは、The Global State of Information Security® Survey2018にご協力いただいた日本企業257社のデータを、PwC Japanグループが独自に分析し、グローバルとの比較を通じて、日本企業が今後取り組むべきサイバーセキュリティのポイントをまとめたものである。

示唆1：ビジネスの「可用性」を脅かすサイバー攻撃への対策

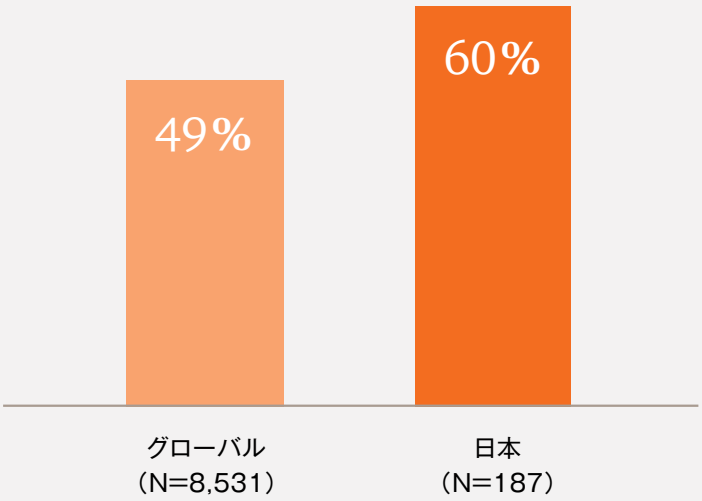
～「可用性」を脅かすサイバー攻撃～

サイバー攻撃は、従来、大規模データ漏洩など、情報資産の機密性を脅かすリスクだと考えられてきた。しかし、2017年5月に世界規模で発生したWannaCryというランサムウェアは、工場の操業停止など、事業の継続を困難に陥れた。この事例から、サイバー攻撃は、機密性の問題を引き起こす以外に、可用性を脅かすリスクでもあると認識されるようになった。ビジネスに与える影響は、可用性の侵害の方が深刻な場合もある。

現代の事業環境を見てみると、業務で利用されるITは企業単体の中で納まることなく、外部の組織とさまざまなネットワークで密接に結び付いており、企業間の相互依存性は非常に高い。この複雑に絡み合うネットワークの中で、どこか1社でも業務が停止すると、エコシステム全体に影響が及ぶ。

多くの日本企業は既にこの重要性を認識しているようだ。GSISS2018の調査では、サプライチェーンへのセキュリティ基準の定着を重視している日本企業の割合がグローバルと比較しても高かった（図1）。

図1：直近の重要なサイバー対策として「サプライチェーンへのセキュリティ基準の定着」を挙げた企業割合



しかし、「言うは易し行うは難し」ということだろうか。2018年3月に情報処理推進機構（IPA）が公表した「ITサプライチェーンの業務委託におけるセキュリティインシデント及びマネジメントに関する調査報告書」[34]において、委託先が実施すべき具体的な情報セキュリティ対策を仕様書などに明記していないと回答した企業は69.1％もあり、委託先で実施する具体的なセキュリティ対策を事前に合意することは容易ではないことがうかがえる。また、委託先のインシデントの発生について、分からないと回答した企業は10％であったが、再委託先より先になると24.4％と増えており、委託先の階層が増えるにつれ、状況把握がより困難になることが分かる。

今後は、製造・物流のサプライチェーン、企業や学術組織横断の共同研究・開発、クラウドサービスをプラットフォームとした企業間データ連携など、さまざまな形態のエコシステムの中で、連携する企業同士が、共通ルールとしてのセキュリティポリシーを定義したり、サイバー攻撃を想定した合同訓練・演習を実施したりすることが求められる。

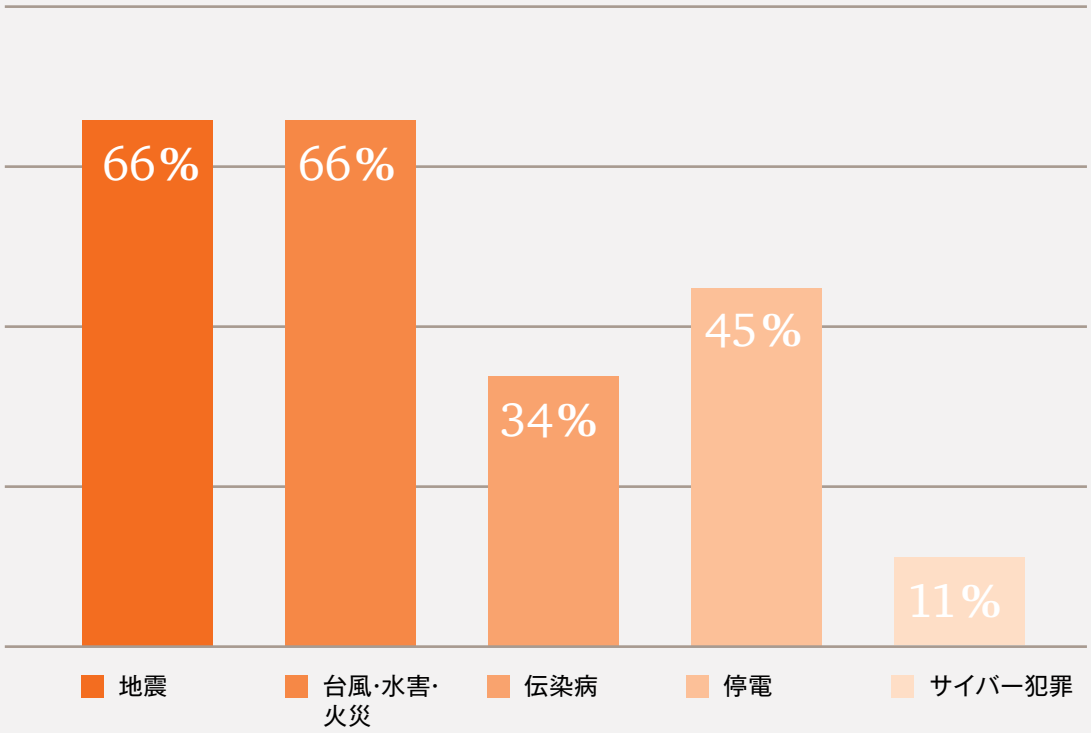
34 ITサプライチェーンの業務委託におけるセキュリティインシデント及びマネジメントに関する調査報告書（独立行政法人情報処理推進機構）2018年3月
https://www.ipa.go.jp/security/fy29/reports/scrm/index.html

～日本におけるBCPのナレッジ～

元来、自然災害の多いわが国では、以前から多くの企業がBCP（事業継続計画）を策定し、運用してきた。東日本大震災の3年後にPwCが実施した「IT-BCPサーベイ」の調査結果を振り返ってみると、情報システムの中断・停止時における対応体制・手順（IT-BCP）の策定率は、58％と半数を超えていた[35]。

ただし、2014年当時、多くの企業が想定していたリスクは、地震や台風・水害・火災などの自然災害であった。WannaCryのようなランサムウェアが猛威を振るう前の世の中においては、サイバー犯罪をリスクとして挙げた企業は約1割にとどまっていた（図2）。

図2：IT-BCPが想定するリスクの割合



出典：PwC、「IT-BCPサーベイ報告書」（2014）

35 IT-BCPサーベイ2014（PwC）2013年12月
https://www.pwc.com/jp/ja/knowledge/thoughtleadership/it-bcp-survey2014.html

～自然災害向けのBCPをサイバー攻撃向けのBCPへ転用する～

悪意ある第三者からのサイバー攻撃は、想定外に発生するという点で、自然災害に似ている。想定するリスクこそ異なるが、日本企業が長年培ってきた、自然災害を対象とするBCPの延長線上でサイバー攻撃に対するBCPを検討すべきである。では、サイバー攻撃を想定したBCPはどのように策定すればよいのだろうか。

図3は、サプライチェーンの一部が「大規模地震に被災することを想定したBCP」と、同じく「サイバー攻撃を受けることを想定したBCP」を比較したものだ。地震向けBCPの常套手段である「拠点の地理的な分散」は、サイバー攻撃に対しては無力だが、それ以外の点で、共通項は多い。

自動車や精密機器などの業界では、これまで中越沖地震（2007年）、東日本大震災（2011年）、熊本地震（2016年）など、大きな地震が発生するたびに、サプライチェーンで結ばれた仲間たちが、被災した企業に集結して復旧の手助けをしてきた。サイバー攻撃への対策において、これらの企業が相互に協力できない理由があるとは考えにくい。

図3：自然災害に対するBCP／サイバー攻撃に対するBCPの異同ポイント例

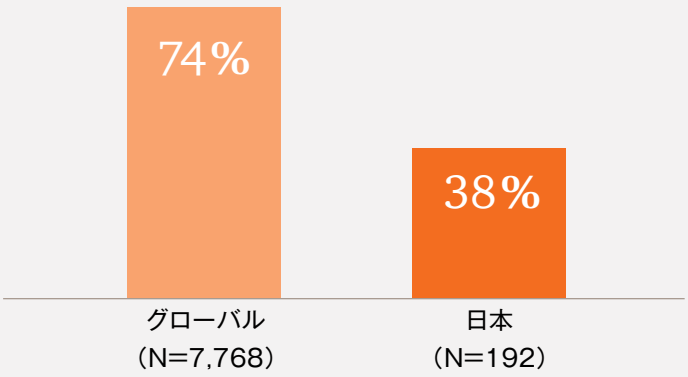
	ポイント	ベストプラクティス	共通点	相違点
1	サプライヤーの管理態勢確認	サプライヤーにおける管理体制や社内規程・手続きの内容を確認する。	セキュリティポリシーやインシデントレスポンス体制を確認し、インシデント発生時に適切な対応を取る準備ができていることを確認する。	—
2	サプライヤーの冗長化	平時から同一業務を複数のサプライヤーに発注する。災害時にどちらかが被災した際には、他方への発注量を増やす調整を行う。	一社だけがランサムウェアに感染する場合には、他社への発注量調整でしのぐことができる。	ネットワークを通じて感染が拡大するリスクがある。ネットワークのセグメンテーションや監視設計が重要。
3	地理的な分散	複数の拠点が同時に被災しないように重要拠点を地理的に分散させる。	—	物理的な場所は意味を持たない。
4	合同BCP訓練	サプライチェーン全体で一気通貫のBCP訓練を行う。	合同BCP訓練は、ランサムウェア対策においても意義のある重要な活動である。	対応部署や役割が異なる。サプライチェーンの中で、ITやサイバーセキュリティ部門同士が連携を取ることが重要。
5	対外的なコミュニケーション	被災時には、社外の利害関係者に対してタイムリーにコミュニケーションを行う。	監督官庁、取引先、顧客、株主・投資家、従業員など、自社のインシデントがどの利害関係者にどのように影響するのか事前に分析する必要がある。	—

示唆２：経営者が自らサイバーセキュリティに関する経営判断を下せるようになるには

～サイバーセキュリティ対策に自信のない日本企業～

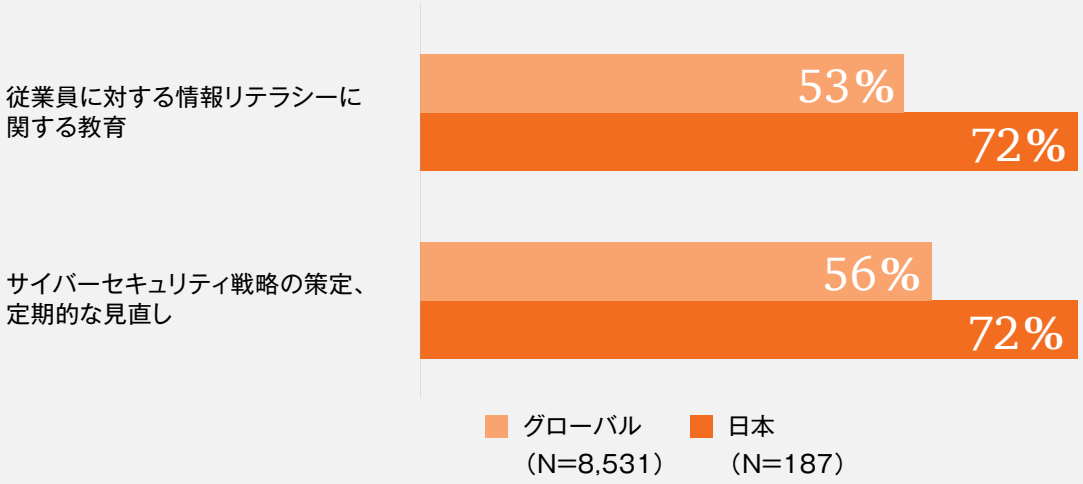
GSISS2018の結果を見ると、日本企業の経営陣は、海外企業の経営陣に比べて、自社のサイバーセキュリティ対策についてまったく自信を持っていないことが分かる（図4）。

図4：サイバーセキュリティ対策に自信があると回答する企業の割合



ただし、日本企業は、必ずしも世界の企業に後塵を拝しているわけではない。個々のセキュリティ対策の実施状況を見ると、むしろ、日本企業の方が積極的に対策を進めているものもある。「従業員に対する情報リテラシー教育の取り組み」や「サイバーセキュリティ戦略の策定・見直し」といった対策は、グローバル全体の平均よりも相当高い数値を示している（図5）。

図5：あなたの組織・企業では、どのようなセキュリティ対策を実施していますか（複数回答）

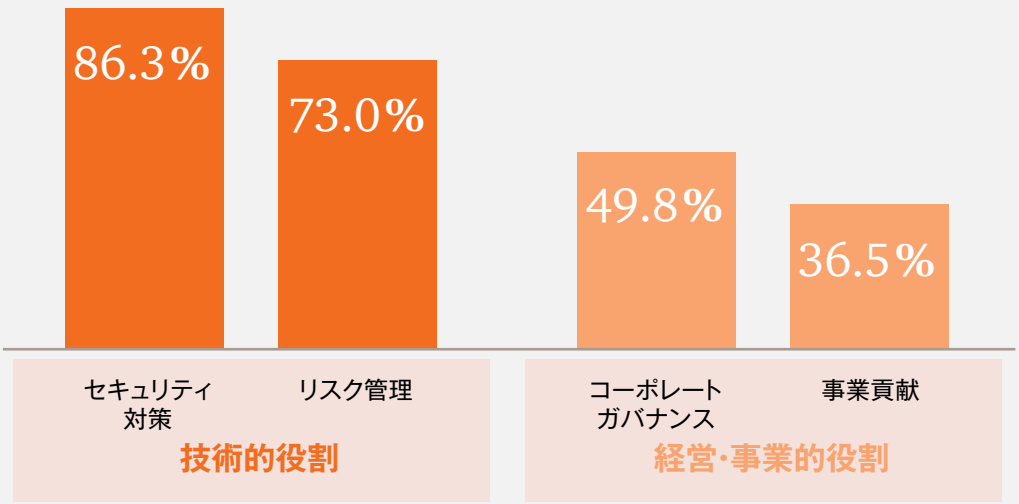


～経営陣がサイバーセキュリティに自信を持てない理由～

日本企業の経営陣が自社のサイバーセキュリティ対策に自信を持てないのはなぜだろうか。

2018年3月に公表された情報処理推進機構（IPA）による「CISOなどセキュリティ推進者の経営・事業に関する役割調査」は、この疑問を紐解くヒントとなる[36]。本報告書では、日本企業の経営層の75.3％がCISOなどのセキュリティ推進者に経営へのコミットメントが求めているにもかかわらず、半数はその役割を有していないことが分かっている（図6）。また、その理由として、「マネジメントに関する訓練が不足していること」、「事業戦略とセキュリティリスクの紐付けができていないこと」、「マネジメント人材や経営と現場を繋ぐ人材が不足していること」を指摘している。

図6：CISOが実際に有する役割



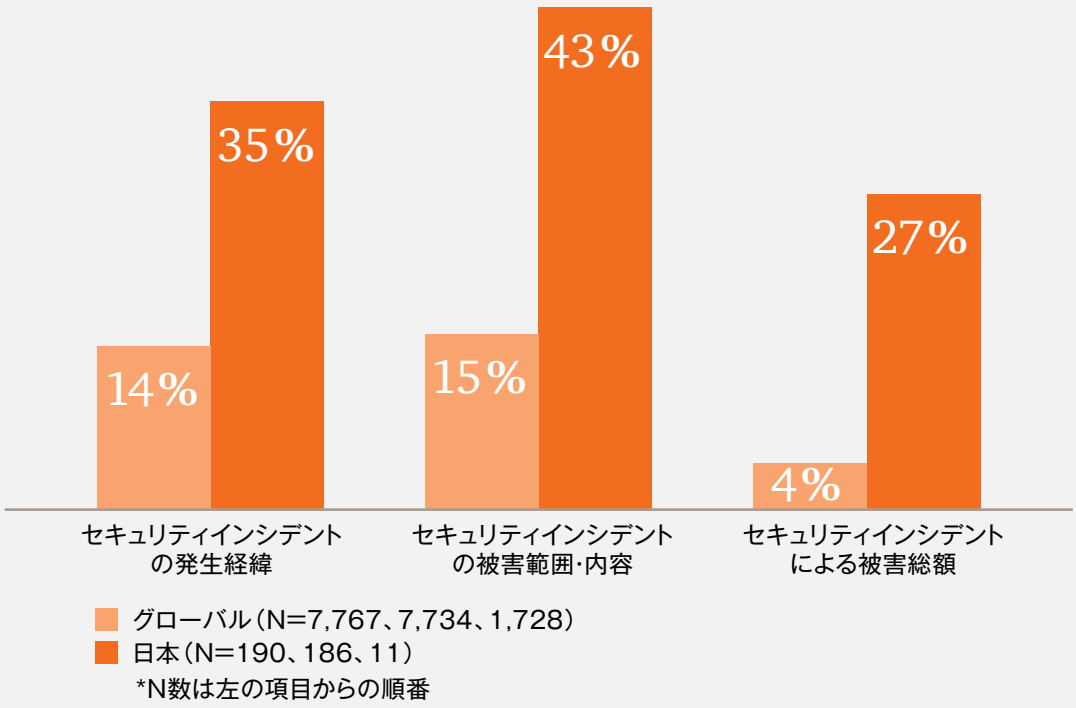
出典：情報処理推進機構（IPA）、CISO等セキュリティ推進者の経営事業に関する役割調査（2018）のデータをもとにPwC作成

36 CISO等セキュリティ推進者の経営・事業に関する役割調査（独立行政法人情報処理推進機構）2018年3月
https://www.ipa.go.jp/security/fy29/reports/ciso/index.html

GSISS2018の調査結果から、この問題へもう一歩踏み込んで考えてみたい。

サイバーインシデントの発生経緯からその範囲や内容、さらには被害額について、経営陣が「把握していない」と回答する日本企業の割合がグローバルに比して多いことが示されている（図7）。

図7：「把握していない」と回答した企業の割合



この結果を踏まえると、経営陣は、現場におけるインシデント対応状況やセキュリティ対策の推進状況などを正確には把握しておらず、セキュリティ投資の効果を実感できていないのではないだろうか。そうだとすると、経営陣がサイバーセキュリティ対策に自信を持てないのは当然である。

経営陣にセキュリティ投資の効果を伝えるには、どのようなコミュニケーション方法が考えられるだろうか。

～経営陣が内容を正しく理解できる報告～

セキュリティ投資に関する報告は、サイバーセキュリティの技術用語を多用するのではなく、経営陣が常日頃接している指標や用語を用いて行うことが効果的である。サイバーインシデントが発生した際、一部の経営陣は、新種のマルウェアの特徴や自社システムの脆弱性に興味を持つかもしれない。しかし、大多数は、どの程度の損失・復旧コストが生じたのか、株価がどの程度影響を受けたのか、メディアの報道やSNSの投稿がどのような論調で語られているのかなどを気にかけている。

もちろん、これはインシデント発生時だけではない。平時から、こまめにコミュニケーションすることが重要である。サイバー空間で起きている攻撃の傾向、他社におけるサイバーセキュリティの取り組み、関連する法規制の動向などと合わせて、自社の取り組みの進捗状況や効果を、月に一度もしくは四半期に一度程度の頻度で報告してはどうだろうか（図8）。経営陣が実感として理解できる報告を行うことによって、セキュリティ投資の金額やセキュリティ担当者の人数が十分なのか、CISOの権限が合理的であるのかなどについて、経営陣が自信を持って判断することができるはずだ。

図8：経営陣への報告例

2018年度 セキュリティ投資額	計画	実績	昨年比
	¥200M	¥195M	18%↑

施策導入状況

セキュリティ施策		KPI	実績
リスク管理体制	サイバーセキュリティ関連人員の増員	CSIRT 7名→10名	社員 +1名
			外注 +2名
		SOC 3名→5名	外注 +2名
SCM	系列企業・ビジネスパートナーの対策実施状況確認	完了（68%→82%）	4社へ実施（76%）
業界内情報共有	情報提供の仕組み構築	完了	完了
	情報取得の仕組み構築	完了	遅延 19年度3月予定

運用状況

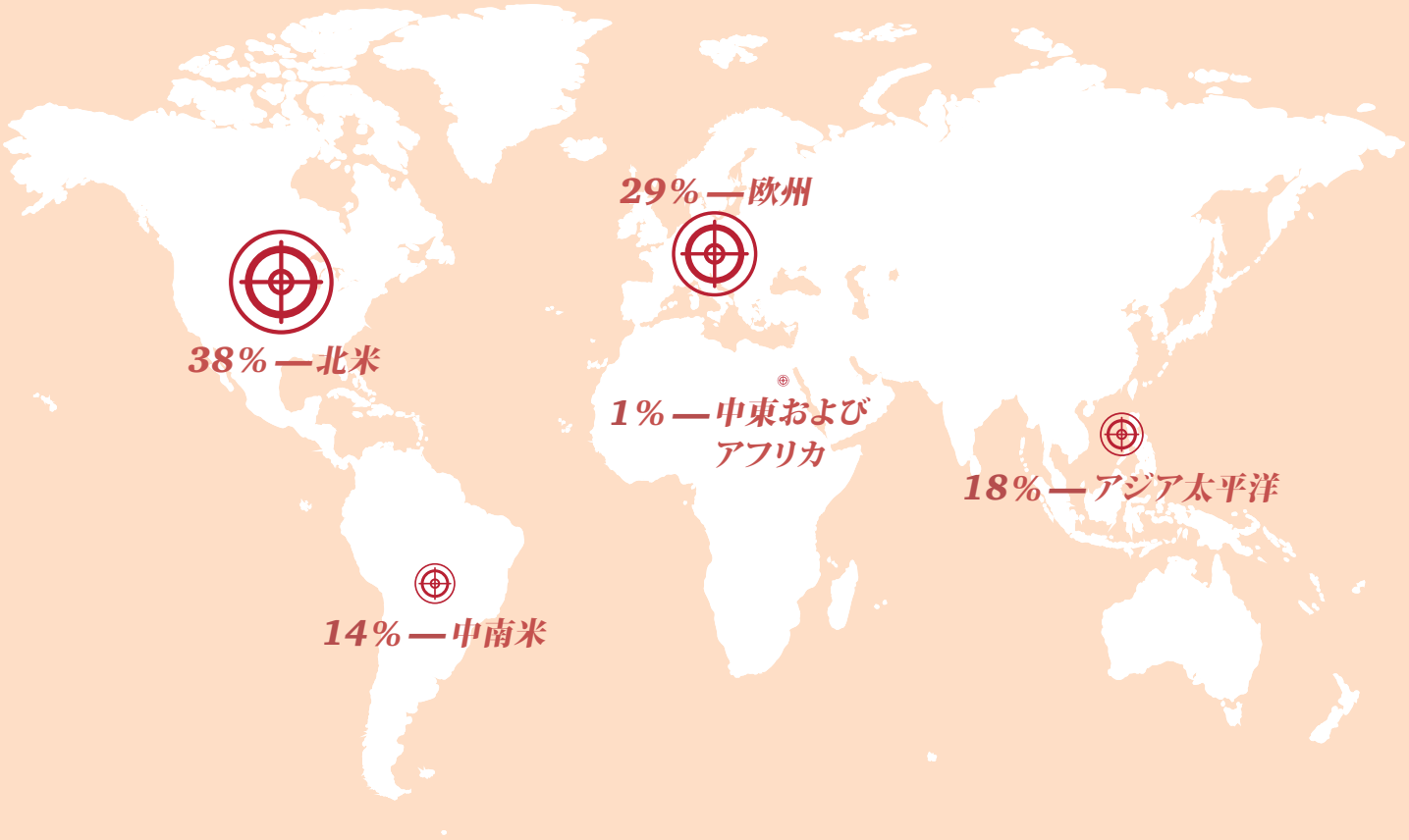
管理項目		実績	昨年比
インシデント	インシデント発生件数	124件	−5%
	インシデント想定損失	¥20M	−6%
	インシデント復旧費用	¥1M	+5%
リスク特定	リスク分析対象システム	231	+1%
	指摘事項数 High	53	+2%
	指摘事項数 Medium	230	−3%
	指摘事項数 Low	78	−4%
	対応進捗率	43%	+6%
教育	セキュリティ教育対象者	4,936名	+1%
	セキュリティ教育実施回数	36回	+0%
	教育受講率	85%	+2%

調査方法

グローバル情報セキュリティ調査2018（以下、「本調査」という）は、PwC、『CIO magazine』、および『CSO magazine』が実施した情報セキュリティに関する世界的な調査です。2017年4月24日から5月26日までの期間において、『CIO magazine』および『CSO magazine』の読者および全世界のPwCクライアントに対して、電子メールによって調査への協力を依頼し、オンライン調査を実施しました。

本報告書で解説する調査結果は、122カ国、9,500人以上の最高経営責任者（CEO）、最高財務責任者（CFO）、最高情報責任者（CIO）、最高情報セキュリティ責任者（CISO）、最高セキュリティ責任者（CSO）、副社長、ITおよび情報セキュリティ役員からの回答に基づいています。

回答者の地域別では、北米が38％、欧州が29％、アジア太平洋が18％、中南米が14％、中東およびアフリカが1％です。



誤差は1％未満です。ここでは四捨五入した数値を使用しているため、数値の合計が100％にならない場合があります。
本報告書の全ての図および図形は、調査結果に基づき作成したものです。

サイバーセキュリティおよびプライバシーに関するPwCのお問い合わせ先（国別）

オーストラリア

Richard Bergman
Partner
richard.bergman@au.pwc.com

Steve Ingram
Partner
steve.ingram@au.pwc.com

Andrew Gordon
Partner
andrew.n.gordon@pwc.com

Megan Haas
Partner
megan.haas@pwc.com

Robert Martin
Partner
robert.w.martin@pwc.com

オーストリア

Christian Kurz
Senior Manager
christian.kurz@pwc.com

ベルギー

Filip De Wolf
Partner
filip.de.wolf@be.pwc.com

ブラジル

Edgar D'Andrea
Partner
edgar.dandrea@br.pwc.com

カナダ

Sajith (Saj) Nair
Partner
s.nair@ca.pwc.com

David Craig
Partner
david.craig@pwc.com

Richard Wilson
Partner
richard.m.wilson@pwc.com

Justin Abel
Partner
justin.abel@pwc.com

Kartik Kannan
Partner
kartik.kannan@pwc.com

中国

Ramesh Moosa
Partner
ramesh.moosa@cn.pwc.com

Kenneth Wong
Partner
kenneth.ks.wong@hk.pwc.com

Kok Tin Gan
Partner
kok.t.gan@hk.pwc.com

Marin Ivezic
Partner
marin.ivezic@hk.pwc.com

Chun Yin Cheung
Partner
chun.yin.cheung@cn.pwc.com

Lisa Li
Partner
lisa.ra.li@cn.pwc.com

Samuel Sinn
Partner
samuel.sinn@cn.pwc.com

デンマーク

Christian Kjær
Partner
christian.x.kjaer@dk.pwc.com

Mads Nørgaard Madsen
Partner
mads.norgaard.madsen@dk.pwc.com

フランス

Philippe Trouchaud
Partner
philippe.trouchaud@fr.pwc.com

ドイツ

Derk Fischer
Partner
derk.fischer@pwc.com

インド

Sivarama Krishnan
Partner
sivarama.krishnan@in.pwc.com

インドネシア

Subianto Subianto
Partner
subianto.subianto@id.pwc.com

イスラエル

Rafael Maman
Partner
rafael.maman@il.pwc.com

イタリア

Fabio Merello
Partner
fabio.merello@it.pwc.com

日本

Yuji Hoshizawa
Partner
yuji.hoshizawa@pwc.com

Sean King
Partner
sean.c.king@pwc.com

Naoki Yamamoto
Partner
naoki.n.yamamoto@pwc.com

韓国

Soyoung Park
Partner
s.park@kr.pwc.com

ルクセンブルク

Vincent Villers
Partner
vincent.villers@lu.pwc.com

メキシコ

Fernando Román Sandoval
Partner
fernando.roman@mx.pwc.com

Yonathan Parada
Partner
yonathan.parada@mx.pwc.com

Juan Carlos Carrillo
Director
carlos.carrillo@mx.pwc.com

中東

Mike Maddison
Partner
mike.maddison@ae.pwc.com

オランダ

Gerwin Naber
Partner
gerwin.naber@nl.pwc.com

Otto Vermeulen
Partner
otto.vermeulen@nl.pwc.com

Bram van Tiel
Director
bram.van.tiel@nl.pwc.com

ニュージーランド

Adrian van Hest
Partner
adrian.p.van.hest@nz.pwc.com

ノルウェー

Lars Fjørtoft
Partner
lars.fjortoft@pwc.com

Eldar Lorezntzen Lillevik
Director
eldar.lillevik@pwc.com

ポーランド

Rafal Jaczynski
Director
rafal.jaczynski@pl.pwc.com

Jacek Sygutowski
Director
jacek.sygutowski@pl.pwc.com

Piotr Urban
Partner
piotr.urban@pl.pwc.com

シンガポール

Tan Shong Ye
Partner
shong.ye.tan@sg.pwc.com

Jimmy Sng
Partner
jimmy.sng@sg.pwc.com

Paul O'Rourke
Partner
paul.m.orourke@sg.pwc.com

南アフリカ

Sidriaan de Villiers
Partner
sidriaan.de.villiers@za.pwc.com

Elmo Hildebrand
Director/Partner
elmo.hildebrand@za.pwc.com

Busisiwe Mathe
Partner/Director
busisiwe.mathe@za.pwc.com

スペイン

Javier Urtiaga Baonza
Partner
javier.urtiaga@es.pwc.com

Jesus Manuel Romero Bartolomé
Partner
jesus.romero.bartolome@es.pwc.com

Israel Hernández Ortiz
Partner
israel.hernandez.ortiz@es.pwc.com

スウェーデン

Martin Allen
Director
martin.allen@se.pwc.com

Rolf Rosenvinge
Partner
rolf.rosenvinge@se.pwc.com

スイス

Reto Haeni
Partner
reto.haeni@ch.pwc.com

トルコ

Burak Sadic
Director
burak.sadic@tr.pwc.com

英国

Zubin Randeria
Partner
zubin.randeria@pwc.com

Richard Horne
Partner
richard.horne@uk.pwc.com

Alex Petsopoulos
Partner
alex.petsopoulos@uk.pwc.com

米国

Sean Joyce
Principal
sean.joyce@pwc.com

David Burg
Principal
david.b.burg@pwc.com

Grant Waterfall
Partner
grant.waterfall@pwc.com

www.pwc.com/gsiss
www.pwc.com/cybersecurityandprivacy

Contributing authors

Christopher Castelli, Barbara Gabriel, Jon Yates,
and Philip Booth

お問い合わせ先(日本)

PwCコンサルティング合同会社
〒100-6921 東京都千代田区丸の内2-6-1
丸の内パークビルディング
03-6250-1200(代表)

山本 直樹
パートナー
naoki.n.yamamoto@pwc.com

PwCサイバーサービス合同会社
〒100-0004 東京都千代田区大手町1-1-1
大手町パークビルディング
03-6212-9080(代表)

星澤 裕二
パートナー
yuji.hoshizawa@pwc.com

PwCあらた有限責任監査法人
〒100-0004 東京都千代田区大手町1-1-1
大手町パークビルディング
Tel: 03-6212-6800(代表)

岸 泰弘
パートナー
yasuhiro.kishi@pwc.com

グローバル情報セキュリティ調査2018
日本版レポート執筆委員

PwCコンサルティング合同会社
道輪 和也
本川 友理
前田 享志

PwCあらた有限責任監査法人
綾部 泰二
三澤 伴暁
江原 悠介
米山 善章
武谷 遼太
森澤 佳子
前川 初美
中山 洋輔

www.pwc.com/jp

PwC Japanグループは、日本におけるPwCグローバルネットワークのメンバーファームおよびそれらの関連会社（PwCあらた有限責任監査法人、PwC京都監査法人、PwCコンサルティング合同会社、PwCアドバイザリー合同会社、PwC税理士法人、PwC弁護士法人を含む）の総称です。各法人は独立して事業を行い、相互に連携をとりながら、監査およびアシュアランス、コンサルティング、ディールアドバイザリー、税務、法務のサービスをクライアントに提供しています。
PwCは、社会における信頼を築き、重要な課題を解決することをPurpose（存在意義）としています。私たちは、世界158カ国に及ぶグローバルネットワークに236,000人以上のスタッフを有し、高品質な監査、税務、アドバイザリーサービスを提供しています。詳細はwww.pwc.comをご覧ください。
本報告書は、PwCメンバーファームが2018年2月に発行した『Strengthening digital society against cyber shocks』を翻訳し、日本企業への示唆を追加したものです。翻訳には正確を期しておりますが、英語版と解釈の相違がある場合は、英語版に依拠してください。

電子版はこちらからダウンロードできます。 www.pwc.com/jp/gsiss
オリジナル（英語版）はこちらからダウンロードできます。 www.pwc.com/us/en/cybersecurity/information-security-survey/strengthening-digital-society-against-cyber-shocks.html
日本語版発刊年月： 2018年6月　　管理番号： I201803-7