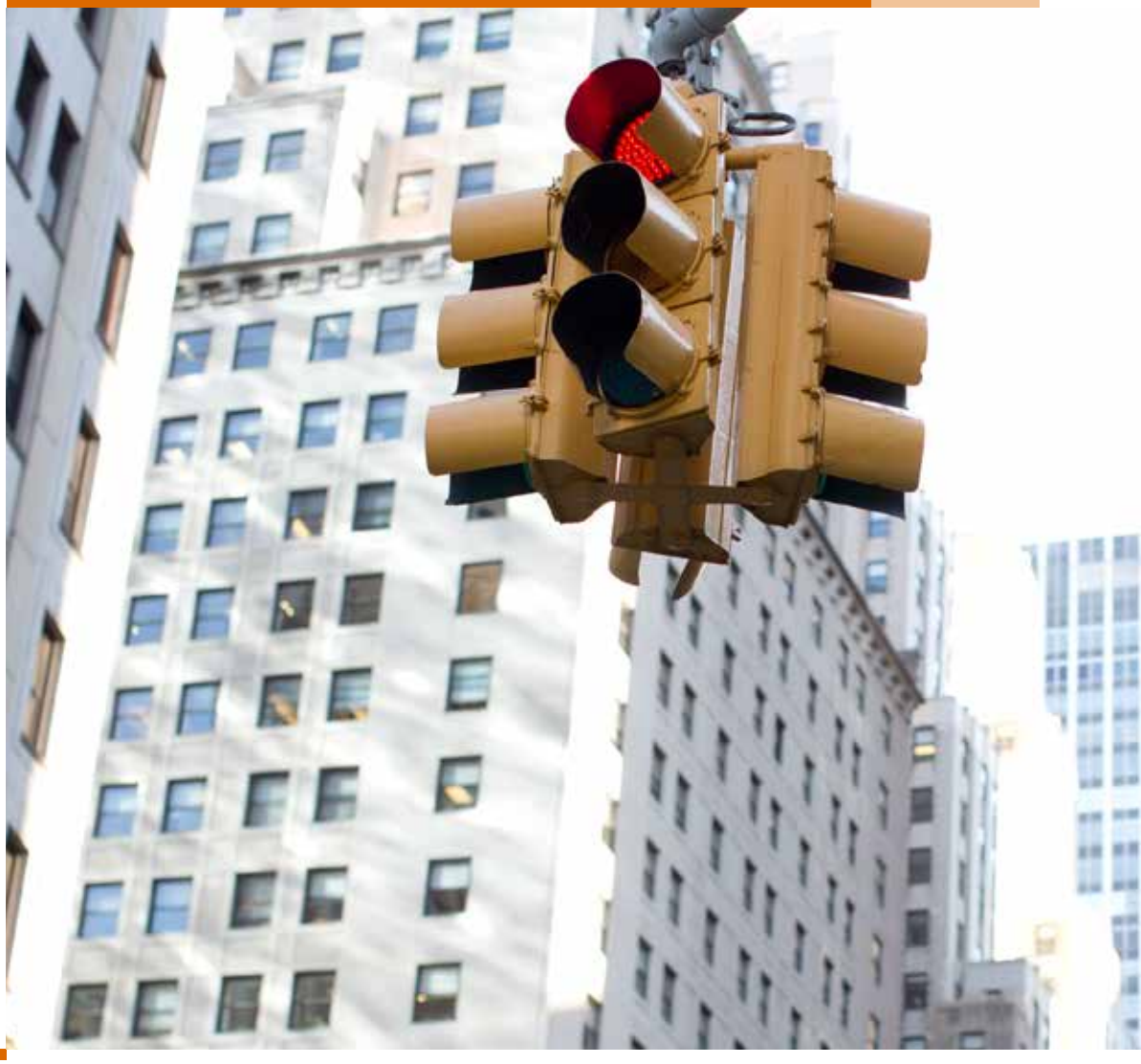
www.pwc.com/jp

米国サイバーセキュリティ：停滞するセキュリティ対策

2015年米国サイバー犯罪調査における主な発見事項



pwc

米国サイバー犯罪調査2015

米国サイバー犯罪調査2015は、PwC、CSOマガジン、カーネギーメロン大学ソフトウエアエンジニアリング研究所CERT®プログラムおよび米国シークレットサービスが共同で実施したものである。

500を超える米国の組織や政府関係機関から調査回答を、各組織のサイバーセキュリティリーダーが結集し評価した。そして、官民におけるサイバー犯罪インシデントの頻度と影響、サイバーセキュリティ脅威、情報セキュリティ支出、サードパーティービジネスパートナーのリスクのトレンドを分析した。また、情報セキュリティ機能や取締役会への高まる期待に企業がどの程度適応しているかも探った。

今日のサイバーセキュリティの状況をより深く洞察し、よりバランスの取れた分析結果を得るために、この調査では、PwCの「第18回世界CEO意識調査」、「グローバル情報セキュリティ調査® 2015」、「2015 Digital IQ調査」を引用した。

サイバー犯罪の新たな局面

サイバー犯罪が世間を騒がせ、
企業にとって頭痛の種に

76%

2015年にサイバー脅威に対する懸念を強めていると述べた回答の割合

サイバーセキュリティインシデントに関して懸念すべきことは、発生件数の増加だけではない。徐々に破壊力が強まり、標的となる情報および攻撃手法が多岐にわたっていることも忘れてはならない。攻撃者が脅威や手法、標的を常に進化させていることは明らかだ。テクノロジーへの投資、情報の共有、人員のトレーニングに余念がなく、目的と能力を持って攻撃を仕掛けてくる。

米国の官民のエグゼクティブ、セキュリティエキスパートなど500人を対象として実施した2015年米国サイバー犯罪調査において、懸念の高まりが見られたのも当然だろう。事実、回答者の76%（前年比59%増）が過去12カ月と比べてサイバーセキュリティ脅威に対する懸念が高まったと回答している。他の調査でも同様の上昇がみられる。例えば、PwCの「第18回世界CEO意識調査」では、米国のCEOの87%（前年は69%）が、サイバー脅威が成長に及ぼす影響に懸念を示した[1]。

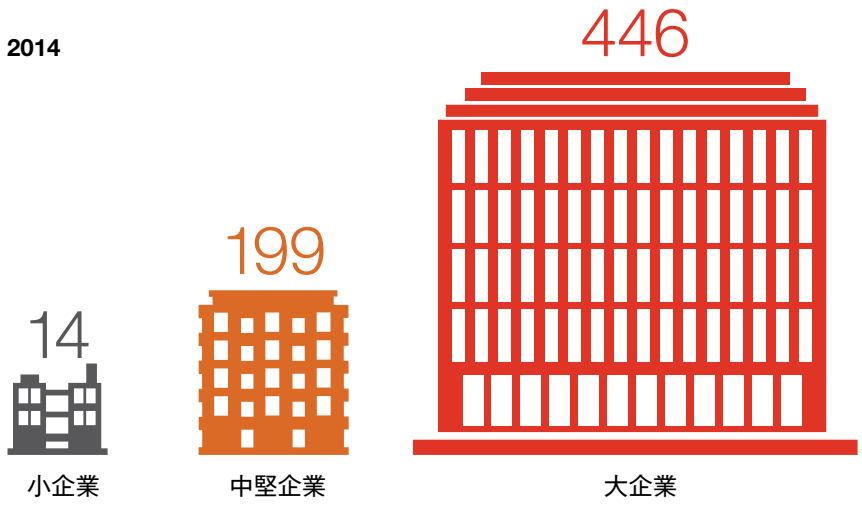
認識と危惧がともに高まったことは確かだ。過去12カ月にセキュリティインシデントを検知した回答者は過去最高の79%に達した。未検知のまま潜むインシデントも多いため、総数はこれを大きく上回ると考えられる。

企業規模とサイバーセキュリティ検知能力には強い相関が見られた。概して、大企業ほど年を追ってインシデント検知能力が強化される傾向がある。事実、大企業の回答者が検知したインシデント数は小企業の回答者31倍に上る。これは前回の調査結果と同様だ。PwCの「グローバル情報セキュリティ調査® 2015」では、2014年のインシデント検知数が大企業では28%増加していたのに対し、小規模では5%減少していた[2]。

大企業ほどセキュリティ技術、プロセス、リソースが成熟している傾向があることから、当然の結果と言えるだろう。

セキュリティ侵害のタイプとして最も多く挙げられているのが、ネットワークやデータに対して正規のアクセス権を持つ従業員やサードパーティーベンダーではなく、外部の脅威主体による犯罪であることは想定内だろう。特に危惧されるのはフィッシング攻撃であり、実行が比較的容易な上に組織内で広がるスピードも速く、役職を問わずあらゆる個人が標的になる。2014年にフィッシング攻撃を受けたと述べた回答者は3分の1以上（31%）に上り、発生頻度の高いインシデントタイプとなった。

検知されたインシデント数（企業規模別）*



従業員数1,000名未満を小企業、1,000名～9,999名を中堅企業、10,000名以上を大企業とした。

1 PwC, 18th Annual Global CEO Survey, January 2015

2 PwC, *CSO, CIO* magazine, The Global State of Information Security® Survey 2015, September 2014

国家、政治的ハッカー、犯罪組織の区別は消えつつある

破壊力を増すサイバー攻撃

2014年に何らかの攻撃の対象となったデータレコードは初の10億件に達した（セキュリティ会社Gemalto調べ）[3]。これらのセキュリティインシデントの多くは非常に広い範囲から報告されている。2014年になって「データ侵害」という言葉が一般にも広まり、『The New York Times』ではデータ侵害に関する記事が前年の125件から大幅増となる700件以上に上った[4]。

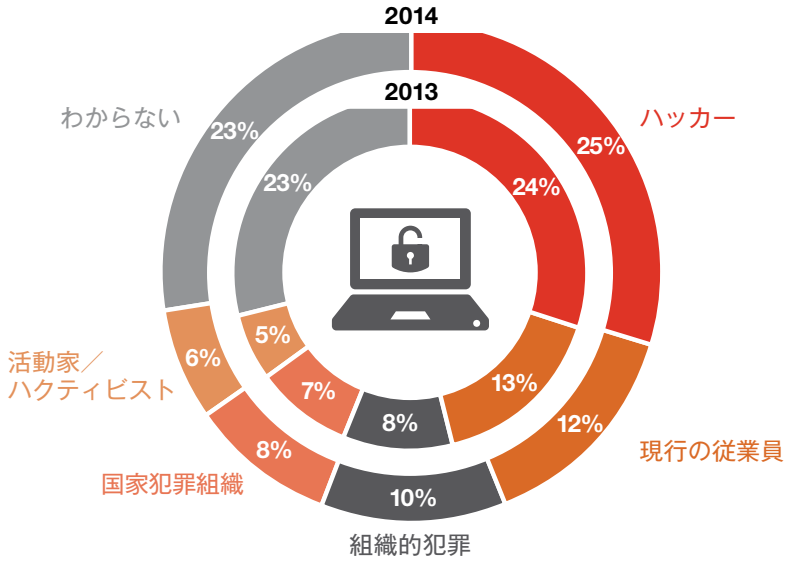
問題はインシデント件数の増加やその検知の可否だけではない。最近は派手な手口が注目を集め、世間に知れ渡るようになっている。

これまで、サイバー犯罪が公になるのは、発表を義務付けられているインシデントに限られていた。つまり、見えていたのは氷山の一角にすぎなかった。今は水面下に潜んでいたリスク（と攻撃）が巨大な姿を現し、Webサイト、ソーシャルメディア、新聞を毎日のように騒がせている。脅威主体の行動が勢いを増し、日々破壊力が強まっていることも、騒動に拍車をかけている。

昨年後半にグローバルなエンターテインメント企業が受けた派手な攻撃は脅威主体の動機や手段の多様性を示すものであり、国家、政治的ハッカー、犯罪組織、悪意を持った個人の区別は消えつつある。政治的な動機を持つ国家などのハッキング加害者は、個人データや従業員間のやりとり、社内の機密文書、給与情報などを公開して企業に損害を与えた。また、攻撃によって企業の電子メールや電話システムが中断され、個人への暴力など、これまでにはないレベルの脅威も現れた。

動機や手段のみならず、攻撃手法も進化している。分散型サービス拒否（DDoS）攻撃はますます増加しており、本年は発生頻度の高いサイバーセキュリティインシデントのタイプとして回答者の18%に挙げられている。DDoS攻撃を受けた場合、多くの場合は評判が低下するほか、Eコマースなどの業務プロセスが滞る恐れもある。

企業を脅かす主なサイバー脅威



3 Gemalto, Gemalto Releases Findings of 2014 Breach Level Index, February 12, 2015

4 Verizon, 2015 Data Breach Investigations Report, April 15, 2015

この2年間で攻撃が目立った小売りおよび消費財業界では、情報セキュリティ支出が大幅に増加している

比較的新しいタイプのマルウェアであるランサムウエアの巧妙化が進み、広く見られるようになっている。企業が身代金（ランサム）を払うまで、データは攻撃者の支配下に置かれる。米連邦捜査局（FBI）は先頃、この種の攻撃の増加を警戒するよう呼び掛けている[5]。2014年には、サイバー犯罪調査の回答者の13%がランサムウエアの被害を受けたと述べている。ランサムウエアの報告は今後ますます増え続けると思われる。

サイバー犯罪の中には、数十年前から存在するがメディアに取り上げられることはほとんどないものもある。例えば、スパムメールがそうだ。この種のサイバー犯罪は広く報告されていないものの、発生件数が増加し被害も大きくなっている。FBIとインターネット犯罪苦情センターの発表によれば、グローバルのスパムメールによる被害額は過去14カ月で2億1500万米ドルに上っており、財務的損失の84%は米国企業が被っている[6]。今回の調査では、法執行機関に属する回答者の21%が取扱件数の上位5つに挙げている。この種の犯罪は、上層部を狙ったフィッシング攻撃から始まることが多い。

大企業と小売業者のセキュリティ支出が増加

肯定的な見方をすれば、近年のセキュリティインシデントの急増は、企業がサイバーセキュリティへの投資の拡大に踏み切るきっかけとなったと言える。

この調査では回答者の平均セキュリティ予算を測定していないが、グローバル情報セキュリティ調査® 2015では、この2年間で米国の情報セキュリティ予算がIT予算の2倍近いレートで増加したことが判明している[7]。

サイバー犯罪調査により、大規模なサイバー攻撃を受けた業界は情報セキュリティ投資を大幅に増やす傾向があることが明らかになった。事実、この2年で度重なる攻撃を受けた小売りおよび消費財業界では、38%の企業がセキュリティ支出を前年度比で20%以上増やした。他の業界を大幅に上回る増加率だ。それとは対照的に、セキュリティ予算を20%増やしたと述べた回答者は、銀行および金融では17%、医療では15%にとどまっている。

サイバーセキュリティ投資の適切なレベルが業種や脅威環境によって異なるのは言うまでもない。もともとセキュリティに力を入れている銀行および金融業界では、さらに20%を超える増強は不要かもしれない。しかし、サイバーセキュリティの支出がまだ少ない医療業界は、さまざまな攻撃主体から新しいタイプの攻撃を受けている。PwC Health Research Instituteでは、近年のデータ侵害によって医療業界の企業が機密性の高い個人情報の保護に乗り出し、情報セキュリティ投資を拡大すると予測している[8]。サイバー犯罪調査では2015年の情報セキュリティ予算について質問を設けなかったが、グローバル情報セキュリティ調査® によると、医療の支払いと提供に携わる企業の51%が2015年のセキュリティ支出を増やす予定であることが判明している[9]。

サイバー犯罪調査では、大企業の情報セキュリティ支出が大幅に上回っている傾向が明らかになった。2014年にセキュリティ投資を20%以上増やした企業は、従業員数1万名以上の企業では20%であるのに対し、小規模企業では12%にすぎなかった。

このような積極的な投資は、大企業の成熟したセキュリティの慣習として表れている。大企業は長年一貫して投資を増やしてきた。

規模にかかわらず、セキュリティ予算を増やした企業の幹部はサイバーセキュリティの費用対効果を重視する。これは、支出を増やしたことでセキュリティ態勢が目に見えて改善されることを確認するためだ。

5 Federal Bureau of Investigation, Ransomware on the Rise, January 20, 2015

6 eWeek, Spam Campaign Business E-mail Compromise Pilfers $215 Million, January 23, 2015

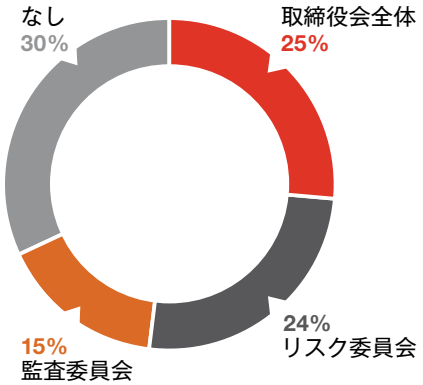
7 PwC, *CSO, CIO* magazine, The Global State of Information Security® Survey 2015, September 2014

8 PwC Health Research Institute, Medical Cost Trend: Behind the Numbers 2016, June 2015

9 PwC, *CSO, CIO* magazine, The Global State of Information Security® Survey 2015, September 2014

取締役会のほぼ半数はいまだ、サイバーセキュリティを企業全体のリスクではなくITの問題ととらえている

サイバーリスクに対する取締役会の関与



取締役会は懸念を示しているものの、関与しているとは限らない

昨年の集中砲火をきっかけに、多くの取締役会はサイバーセキュリティへの関心を強めた。そして、現時点と今後のリスク、セキュリティ準備態勢と対応計画を把握しようとしている。そこで、セキュリティリーダーがサイバーリスクの状況説明をどのくらいの頻度で行うかを尋ねた。

回答者の4人に1人（26%）は、取締役会に対するセキュリティのプレゼンテーションを最高情報セキュリティ責任者（CISO）または最高セキュリティ責任者（CSO）が1年に1回しか行わないと述べた。30%は上級セキュリティ担当者が四半期に一度行うと回答した。しかし、セキュリティリーダーによるプレゼンテーションは行われていないという回答は28%を占めた。

サイバーセキュリティに関する他のベストプラクティスと同様に、CISOやCSOが四半期に一度の取締役向けプレゼンテーションを実施している傾向は大企業に強く見られ、小企業では弱い。事実、セキュリティリーダーがセキュリティリスクに関する説明を行ったことがないという回答は小企業では3人に1人（33%）と、大企業の18%と比べて多い。

取締役会がサイバーリスク管理にどのように参加するかはそれぞれ異なるが、全米取締役協会（NACD）の総合ガイドラインでは、取締役会全体がリスク管理に関与することが推奨されている。NACDでは、戦略とリスクは深く関係しているため、取締役会全体がサイバーセキュリティリスクの責任を負う必要があるとされている[10]。取締役会がサイバーリスク管理に関与していないという回答が30%にも及んでいることはやや気掛かりだ。反対に、取締役会全体がサイバーリスク管理に関与しているという回答は25%だった。

興味深いのは、監査委員会がサイバーリスク管理に関与しているという回答がわずか15%である点だ。この数年間、サイバーセキュリティなどの内部情報に関する問題は往々にして監査委員会に寄せられていた。監査委員会の出番が比較的減ったのは、サイバーセキュリティ管理の責任が取締役会に移ったためとも考えられる。

10 National Association of Corporate Directors, Cyber-Risk Oversight: Directors Handbook Series, 2014

上級幹部は取締役会からサイバーリスクおよびサイバーセキュリティ準備態勢に関する質問を待つべきではない

侵害が発生した場合に問われる責任を考えれば、これらの統計は企業の姿勢の甘さを露呈するものだ。取締役会が運用上のサイバーリスクを実質的に考慮していないことから、監督機関や原告弁護人は、経営陣が実施し取締役会が監視すべき運用上のリスクに対する備えを怠ったと結論付ける可能性がある。

また、取締役会が、サイバーセキュリティは単なるITリスクではなく企業全体が抱えているリスクであるという認識を持つことも重要だ。しかし、このような認識を持つ企業はまだ少ない。取締役会のほぼ半分（49%）は、サイバーセキュリティをITリスクととらえている。コーポレートガバナンスの問題としてとらえているのは42%にすぎない。

サイバーセキュリティを企業全体のリスクとして認識している企業は、サイバーセキュリティ活動や関連する義務を理解し適切に管理していること、そして社会の一員としての責任を果たす姿勢を外部の利害関係者に示すことができる。企業がそのような社会的責任を果たし、適切な認識を持つには、多くの場合、コーポレートガバナンスの実績ある方法論や基準に基づく緻密な監督プログラムが必要だ。監督プログラムの下で、取締役会での報告を合理化し、複数の部門にまたがって運用上のサイバーリスクを低減する活動を統合し、適切なセキュリティ規程類および手順を整備していることを実証できる

エンタープライズリスクの理解を深めるために、いち早くサイバーリスクやその発生確率を正式に定量的に推計しようとする動きも見られる。サイバーセキュリティのバリュー・アット・リスク（想定最大損失額）と呼ばれる手法だ。これは、昔から金融サービスで使用されてきたバリュー・アット・リスク（VaR）というリスク分析手法をもとにしている。CEO、CRO、取締役会は、リスクにさらされているデジタル資産やプロジェクトの潜在的損失、代替セキュリティモデルや投資、サイバーセキュリティ保険によってリスクを低減する方法を把握できるようになる。

確実に言えるのは、上級幹部は取締役会からサイバーリスクおよびサイバーセキュリティ準備態勢に関する質問を待つべきではないということだ。CISOおよびCSOは少なくとも半年に一度、サイバーセキュリティに関するリスクを取締役会に積極的に報告すべきである。

取締役会がサイバーセキュリティを監督すべき7つの理由

いまやサイバーリスクは企業が直面している重大なビジネスリスクの一つであり、その責任は取締役会が負う。役員はサイバーセキュリティを、戦略、部門横断、経済の観点から対応すべき企業全体のリスクとしてとらえる必要がある。ここでは、取締役会がサイバー脅威とサイバーセキュリティ機能を真剣に問うべき7つの理由を挙げる。

1. サイバーセキュリティの影響は全社に及ぶ。たとえリスク発生点が数千マイル離れた場所であっても、インシデントが発生すれば企業運営全体が影響を受ける。
2. 財務的影響が大きく、集団訴訟が起こされれば高いコストが生じる。取締役会は企業の経済的価値を守る受託者責任を問われることになる。
3. 規制が進むにつれ、その遵守は困難で高コストになる。例えば、EUのデータ保護指令には、企業の世界収益の最大5％が罰金として科せられる提案がある[11]。これは民事訴訟にも関連する。
4. IoT（Internet of Things）は新たな脅威をもたらす。制御システムやスマートビルディングシステムに障害が起これば、甚大なリスクと物理的損害が生じる。
5. サイバーリスクに対する防衛手段として、サイバーセキュリティ保険を検討するとよいだろう。リスク委員会は役員や責任者の法的責任、企業総合賠償責任、旧職在籍責任、損害保険について確かめておく必要がある。
6. 国家や犯罪組織などの攻撃者は、経済的妨害、営業秘密の窃取、マネーロンダリング、テロリズム、軍事および諜報活動などを目的とし、連携して活動する。
7. サイバー攻撃を受けた場合、大きな経済的損失を被るほか、合併や新製品の発表、潜在的顧客との成約などの戦略的目標が遠ざかることでブランドの評判も傷つく。

11 European Commission, Stronger data protection rules for Europe, June 15, 2015

新設されるISAOを通じて、企業は個々の業界、課題、地域、脅威ごとの情報を柔軟に共有できるようになる

情報共有を第一に

情報共有は待ったなしの段階にまできている。バラク・オバマ大統領が2015年2月に発した大統領命令では、新しい情報共有分析機関（ISAO）の新設が指示されており、議論が進むのは間違いないだろう。

信頼性と具体性、適時性を兼ね備えた情報共有が可能になれば、脅威状況の認識、防衛における機敏性、情報に基づく意思決定、影響を受ける顧客や企業、監督機関への迅速な通知に向けて整備が進む。また、企業を取り巻く脅威の全体像を把握することも比較的低コストでできるようになる。

このような利点があるにもかかわらず、業界ごとの情報共有分析センター（ISAC）への参加は芳しくない。2014年にISACに参加した回答者は25%と前年からほぼ横ばいだ。参加率が高いのは、電力、水道、銀行、金融、政府機関である。

多くの業界観測筋は、大統領命令によって情報共有の取り組みへの参加者が増加すると見ている。新設されるISAOは現在の業界ごとのISACにはない柔軟性を備えており、個々の業界や地域、課題、事象、脅威に関する情報を官民で共有できるようにする。

ISAOにより、業界の壁を越えた情報共有も実現されるかもしれない。例えば、重大な課題は、金融サービス、製薬といった分野ではなく、企業の規模や顧客層によって異なる。ウォール街の大手銀行ならば、共通点が多いのは地方銀行よりも大手製薬会社だろう。実際、中間市場の企業と大手企業の課題は異なることが多い。

ISAOはこのような問題の突破口となる可能性があるが、まずは基礎となる目標を定めなければならない。情報共有モデルを成功させるには、使命と重点の明確化、会員による規則の決定と厳密な適用、価値の明示、信頼関係の構築と維持が必要だ。

情報共有の実現を阻んでいる最大の原因は、統一された枠組みや基盤、データ基準の欠如である。自動化された統合インフラストラクチャーがなければ、脅威情報と対応策をリアルタイムで配信することはできない。米国では、その実現を目指し、国土安全保障省などがTAXII、STIX、CybOXなどの具体的な標準メッセージおよび通信フォーマットを推進している。導入率についてははっきりしたデータがまだなく、フォーマットが最適なものかどうかも不明だ。

確かなのは、スピードが重要だということだ。サイバー脅威分析を専門とするRiskAnalytics社の調査では、2014年に発生した攻撃の75%は、はじめの一社で攻撃が成功するまでの時間は1日（24時間）以内だった。このうち40%は、1時間以内に次の標的、すなわち二社目への攻撃を成功させたということだ[12]。

情報共有モデルを成功させるためには、消費者データのプライバシーに関する明確な指針を定め、テクノロジー企業による暗号化の使用をめぐる官民の争いを解決する必要もある。現在、米国議会では情報共有の規制法案が検討されている。成立すれば、情報共有の実現を阻んでいる問題の一部が解決されることになるだろう。

12 Verizon, 2015 Data Breach Investigations Report, April 15, 2015

テクノロジー投資の偏り

サイバーセキュリティ予算が増加する中、サイバー犯罪に対する警戒の高まりから、テクノロジーソリューションに頼って攻撃を回避しリスクを管理する傾向が強まっている。

PwCが実施した第18回世界CEO意識調査では、米国のCEOの75%がサイバーセキュリティソリューションを「非常に重要なビジネス戦略」と位置付けた[13]。2015 Digital IQ Surveyでも同様にテクノロジーへの依存が見られた。回答者の69%は、最大の支出カテゴリとしてサイバーセキュリティテクノロジーへの投資を挙げた[14]。

米国サイバー犯罪調査での回答がテクノロジーについて楽観的だったのもうなずける。ほぼ半数（47%）が、新しいテクノロジーの追加が最優先の支出であると回答とした。注目すべきは、プロセスの再設計を最優先とした回答が15%のみという点だ。新しい技能の獲得を挙げた回答者は33%だった。

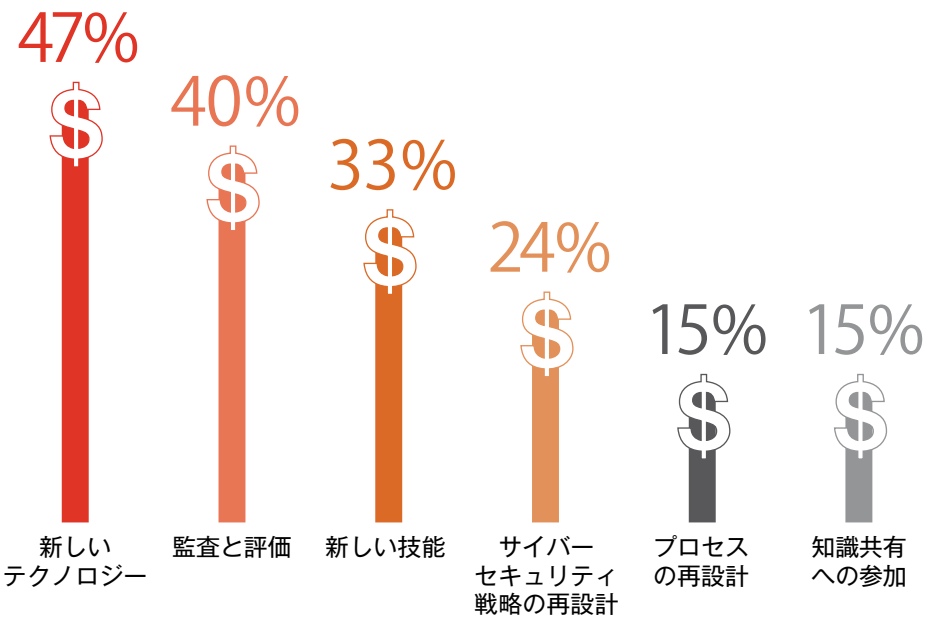
新しいテクノロジーの導入に関連するサイバーリスクに対応する専門知識の有無を尋ねた質問では、適切な人材がいると答えた回答者は26%にすぎなかった。ほとんどは、内外の専門知識を駆使して新しいソリューションのサイバーリスクに対応していた。

プロセスの更新と従業員トレーニングを実施せずに新しいテクノロジーを導入した企業は、投資に見合う価値を最大限に引き出せない可能性が高い。真の効果を得るには、サイバーセキュリティプログラムにおいて、テクノロジーによって実現される機能、再設計されたプロセス、従業員の技能トレーニングのバランスをとる必要がある。

従業員のトレーニングと認識はサイバーセキュリティの重要要素であるにもかかわらず、軽視されがちだ。セキュリティ認識およびトレーニングプログラムを定期的に実施していると述べた回答者は全体の半分（50%）のみだった。新人向けにセキュリティトレーニングを行っている回答者の割合も同じだ。

従業員向けのセキュリティ認識プログラムを徹底することに加え、インシデント対応および危機管理マニュアルを定期的にテストして更新することも重要だ。計画には、セキュリティおよび業務関係者向けに高頻度で実施する机上訓練、従業員および幹部向けの継続的なトレーニングを含める。今日のサイバー犯罪環境においては、焦点は攻撃を受けるかどうかではなく、被害をいかに軽くするかということだ。準備態勢が整っていれば、影響を抑えることができる。セキュリティ担当者は準備態勢を整えることで、経営陣や取締役会に確実に管理していると報告できる。

サイバーリスクに伴う支出の優先順位



13 PwC, 18th Annual Global CEO Survey, January 2015

14 PwC, Three surprising digital bets for 2015, January 2015

金融サービス業界では監督機関が先頭に立ってサードパーティーサプライヤーの適正評価を呼び掛けている

サードパーティーリスクへの対応は不十分

昨年は、サードパーティーのセキュリティ機能の適正評価への関心が高まった。ビジネスパートナーのシステムが攻撃を受け、大きな損害を被ったことが大きい。

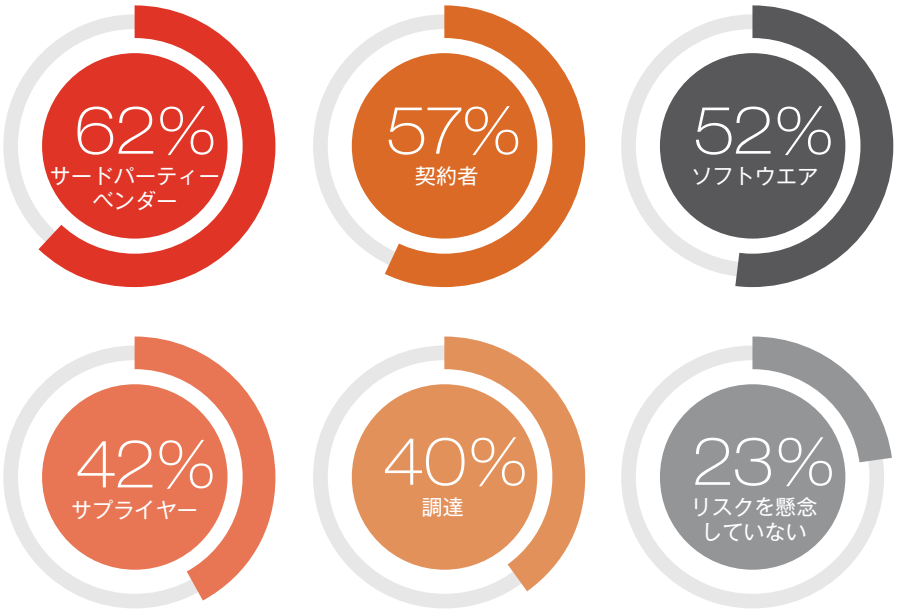
サードパーティーのサイバーセキュリティ評価の必要性は今に始まったことではない。新しいことといえば、監督機関がサードパーティーのリスク管理に本腰を入れ、企業が継続的な監督と統治、適正評価を行うことを期待するようになった点だ。

金融サービス業界では、監督機関が陣頭指揮を執っている。米連邦金融機関検査協議会（FFIEC）は、企業がリスクを識別し、サイバーセキュリティの成熟度を判断できるよう、サイバーセキュリティ評価ツールを開発した。このツールでは、テクノロジーや接続タイプ、配信チャネル、オンラインおよびモバイル製品およびテクノロジーサービス、組織的特徴、外部の脅威に基づき、内在するリスクプロファイルを評価できる[15]。

ニューヨーク州金融サービス局は、サードパーティープロバイダーのセキュリティ評価に力を入れている。同局は2014年10月、規制対象となる40の金融機関に対し、適正評価、ポリシー、手順、機密データの保護策、サードパーティーの情報セキュリティの不備による損失に対する保護策について聞き取り調査を行った[16]。

このような監督機関による厳しい監視が他の業界にも波及する可能性が高まる中、サプライチェーンやビジネスエコシステムに関連するリスクを評価している回答者の数に多少の増加が見られることは朗報だ。本年は回答者の62%がサードパーティーパートナーのセキュリティリスクを評価していると答えた。また、57%が契約業者のセキュリティリスクを、さらに42%がサプライヤーのセキュリティリスクを評価していると答えた。

対象別リスク評価実施状況



15 Federal Financial Institutions Examination Council, Cybersecurity Assessment Tool, June 2015

16 New York State Department of Financial Services, Update on Cyber Security in the Banking Sector: Third Party Service Providers, April 2015

経営陣のほぼ5人に1人（19%）が、サードパーティーおよびサプライチェーンパートナーに関連するサイバーセキュリティリスクを懸念していないと回答

気掛かりなのは、CEO、CFO、COOのほぼ5人に1人（19%）は、サプライチェーンリスクを懸念していないと回答していることだ。このような幹部の多くは、サードパーティーの脅威にはIT部門が対応すべきと考えているのかもしれない。そうだとすると、困った事態になりそうだ。CIOも19%がサプライチェーンリスクに対する懸念を示していないからだ。

現状では、ビジネスパートナーの適正評価が十分というには程遠いことは明らかである。また、サードパーティーのサイバーセキュリティ評価を1年に1回以上行っているという回答は16%にすぎない。サードパーティーの評価をまったく行っていないという回答も23%ある。ほとんどの企業は協業するサードパーティーパートナーのサイバーセキュリティ機能を評価するプロセスを整備しておらず、外部パートナーに対するインシデント対応計画も作成していない。

パートナーのセキュリティ機能を評価する権利を契約書に明記することが重要だ。M&A取引の契約履行や準備の段階で、合法的に適正評価を実施する計画がないと、後で十分な評価を行うことができない恐れがある。また、セキュリティ支出の増大は、クラウドコンピューティングのようなITサービス機能以外の部分で発生していることも考慮すべきだ。IT以外の契約では適正評価を実施できず、重要な情報セキュリティおよびプライバシー保護策が必要である可能性もある。

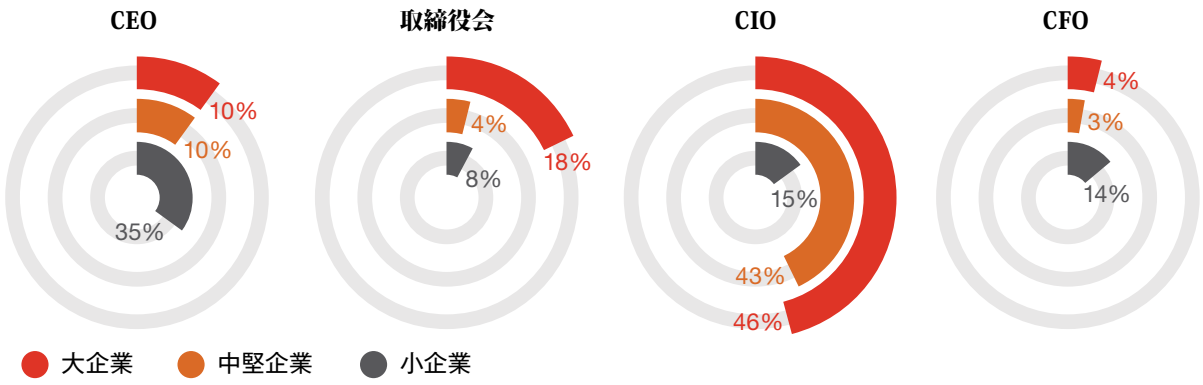
同時に、サードパーティーのセキュリティ侵害への対応計画を整備し、定期的にテストすることも忘れてはならない。インシデント対応計画があっても、十分なテストと継続的な更新を行っていなければ、宝の持ち腐れとなってしまう。

CISOの戦略的役割

サイバー犯罪が企業全体のリスクとして注目を集めるに伴い、CISO（最高情報セキュリティ責任者）の役割と責任はますます重要になっている。そのため、組織構造にセキュリティ機能をいかに組み込み、CISOの所属先／報告先をどこにすべきかについての議論が盛んだ。

調査によると、CISOおよびCSOの所属はCIO直下が最多であり、続いてCEO、CFO、COO、取締役会の順になっている。組織構造は業界や企業規模によって異なるものの、CIOが統括する組織構造はほぼ全てに共通している。

CISO／CSOの所属先（企業規模別）*



従業員数1,000名未満を小企業、1,000名～9,999名を中堅企業、10,000名以上を大企業とした。

本年のサイバーセキュリティ調査では、小企業ではCEOの直下に上級セキュリティ担当者が属し、中堅企業ではCIOの直下にCISOまたはCSOが属していることがわかった。大企業では、セキュリティリーダーがCIOまたは取締役会の直属になっているのが一般的だ。

セキュリティリーダーがCIOの直属であることが最も多いということは、IT部門の下にセキュリティ機能を置く構造が最も効果的なのだろうか。答えは否だ。適切な組織構造は個々の要因によって異なり、CIOの役割は企業や業界によってさまざまであるため、一般化することはできない。例えば、金融サービスでは、銀行の監督機関がCISOに説明責任の拡大を求め、セキュリティリーダーの所属をCIO直下としないようにする措置を取っている。現在はCISOにリスク対応とセキュリティ技術の両方が求められるようになり、IT部門の上下関係と、リスク責任者と法務責任者で別の指揮命令系統が複雑に絡んでいることもある。サイバーセキュリティのリスクが高まるとともに、CISOの役割はこれからも進化していくだろう。

正式な組織構造がどうであれ、CISOの責任と能力はこの数年間で決定的に深まった。CISOが担う役割はこれまでにないほど困難になり、明らかだ。CISOには、リスクの説明責任を負い、企業全体で最小限の情報セキュリティ態勢を実現することが期待されている。

今日のCISOは経営陣と同等の経験を持つ統括者である必要がある。求められているのは、セキュリティだけではなく、リスク管理、コーポレートガバナンス、コミュニケーションの専門知識だ。セキュリティリーダーは幹部にビジネスリスクを知らせる手段を持ち、リスクベースのセキュリティ課題を経営陣、取締役会のほか、監査、法務、コンプライアンスのような監督グループに対して十分に詳しく説明できなければならない。つまり、情報セキュリティリーダーには、他の上級幹部と同じくらい変革を起こす力が必要なのだ。

いまこそが正念場

脅威、そして攻撃の手法と標的が急速かつ着実に進化していることは明らかだ。サイバー犯罪者は、テクノロジーへの投資と情報の共有をいとわず、目的を持ってしぶとく攻撃を仕掛けてくる。

企業は技能を磨き、敵に立ち向かわなければならない。ただし、そのためには、単にサイバーセキュリティ支出を増やせばよいというわけではない。脅威を敏感に察知できるよう、限られたリソースを最大の効果が見込める活動に割り当てる必要がある。例えば、脅威分析力の向上、重要資産のセキュリティの強化、対応力を高めるための社内全体のシミュレーションの実施、セキュリティ認識向上のための活動などが考えられる。サイバーセキュリティの脅威と対応策について情報を積極的に共有する準備も進めるべきだ。これから長い時間をかけて、取締役会から個々の従業員の隅々まで持続的な取り組みが必要になる。

企業にとって、いまが正念場である。ビジョン、決意、技能、リソースを結集して、絶え間なく変化し続ける脅威の迅速な検知、対応、低減を可能にするリスクベースのサイバーセキュリティプログラムを構築しなければならない。これ以上遅れをとれば、ニュース第1面に載るリスクを冒すことになるだろう。

お問い合わせ先

プライスウォーターハウスクーパース株式会社
〒104-0061　東京都中央区銀座8-21-1　住友不動産汐留浜離宮ビル
03-3546-8480（代表）

松崎 真樹
パートナー
maki.matsuzaki@jp.pwc.com

山本 直樹
パートナー
naoki.n.yamamoto@jp.pwc.com

星澤 裕二
パートナー
yuji.hoshizawa@jp.pwc.com

www.pwc.com/jp

PwC Japan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あらた監査法人、京都監査法人、プライスウォーターハウスクーパース株式会社、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、ディールアドバイザリー、コンサルティング、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、世界157カ国に及ぶグローバルネットワークに195,000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の提供を通じて、企業・団体や個人の価値創造を支援しています。詳細は www.pwc.com/jp をご覧ください。

本報告書は、PwC メンバーファームが 2015 年 7 月に発行した『US cybersecurity: Progress stalled』を翻訳したものです。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/ja/japan-knowledge/report.jhtml
オリジナル（英語版）はこちらからダウンロードできます。http://www.pwc.com/us/en/increasing-it-effectiveness/publications/us-cybercrime-survey-2015.jhtml
日本語版発刊月：2015 年 9 月　管理番号：I201507-4

© 2015 PwC. All rights reserved.
PwC refers to the PwC Network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.
This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.