KPMG

KPMG Insight

KPMG Newsletter

Vol. 41

March 2020

【経営 Topic ②】

DX化に見えるサイバーセキュリティ課題
～サーベイ結果を読み解く～

home.kpmg/jp/kpmg-insight

DX化に見えるサイバーセキュリティ課題
～サーベイ結果を読み解く～

KPMGコンサルティング株式会社
テクノロジーリスクサービス
マネジャー　新井　保廣

4回目を迎える「サイバーセキュリティサーベイ2019」では、グローバルにセキュリティソリューションを展開するEMCジャパン RSAと共同で、国内の上場企業および売上高400億円以上の未上場企業の計313社のセキュリティ責任者を対象に、アンケート形式で調査を実施しました。調査結果では、セキュリティ被害の実態として回答企業の約21%が不正侵入の痕跡を発見しており、過去４年の推移は横ばいですが、痕跡の約89%が自組織による発見でした。一方で回答企業の約63%が定期的な監査を実施しておらず、日々高まるセキュリティの脅威の発見および改善プロセスの脆弱性が浮き彫りにされました。また、例年課題の上位を占めるセキュリティ人材の不足や社員のセキュリティ意識の欠如については、デジタルトランスフォーメーション（DX）の影響を受け、セキュリティ対策の要所や費用対効果に悩みを抱える組織が増えている傾向が読み取れます。
本稿では、企業のサイバーセキュリティにおける現状課題と注視する対策領域の実態とアプローチについて解説します。
なお、本文中の意見は、筆者の私見であることをあらかじめお断りいたします。

【ポイント】

- 昨今のDXによるビジネス拡大において、デジタルリスクの中でもサイバーセキュリティはより一層複雑化を増している。
- 企業の競争力を高めるためには、利用者の信頼を得ることが以前にも増して重要となり、ビジネス戦略の初期段階からサイバーセキュリティを組み込まなければ、社会の期待に沿ったビジネスモデルが確立できず、経営層のリーダーシップが問われることとなる。
- ITのみならずOT（Operational Technology）においても、IoT、AIや5Gなどを活用したDXによる生産効率化が急速に加速する時代を迎え、経営層の関与のもとでのセキュリティガバナンスの確立が求められる。

新井　保廣
にいい　やすひろ

回答企業の属性

従業員数（連結）	
1～499人	16.3%
500～999人	24.0%
1,000～2,999人	32.1%
3,000～4,999人	9.0%
5,000～9,999人	7.1%
1万人以上	11.9%

売上高（2018年度 連結）	
500億円未満	34.9%
500～1,000億円未満	21.5%
1,000～3,000億円未満	24.0%
3,000～5,000億円未満	5.4%
5,000～1兆円未満	5.4%
1兆円以上	8.0%
無回答	1.0%

業種	
流通	20.2%
製造	33.3%
金融	10.6%
建設・不動産	12.5%
通信・IT・メディア	7.4%
旅行・レジャー・飲食	5.1%
製薬・医療	1.6%
運輸・インフラ	5.8%
その他	3.5%

I. セキュリティ被害と対策状況

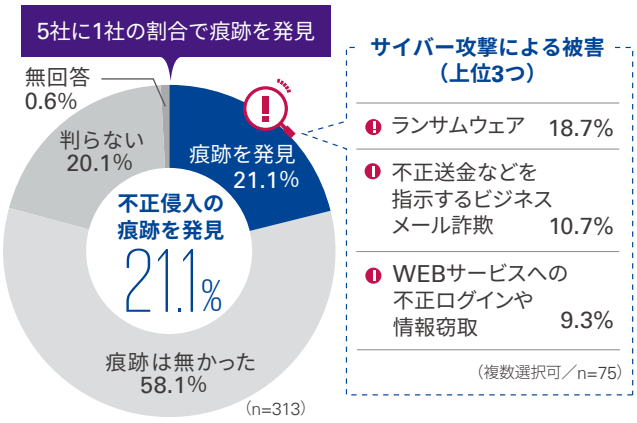
1. サイバー攻撃による被害

IPA（独立行政法人 情報処理推進機構）セキュリティセンターが毎年発行する「情報セキュリティ 10大脅威」の2019年度版では、標的型攻撃やビジネスメール詐欺、ランサムウェアによる被害が上位に挙げられており、本調査でもほぼ同様の結果が示されています。一方、セキュリティベンダーによる海外の調査では、ランサムウェアの被害が年々深刻化しており、その一因としてインターネットの闇サイトであるダークウェブ上で、ランサムウェアの開発者によるランサムウェアの提供と管理を行う攻撃者向けのサービス「RaaS」（Ransomware-as-a -Service）の立ち上げが確認されています。2017年からウクライナを中心に世界中で猛威を振るった「NotPetya」はこのサービスから入手したものと見られ、日本国内で話題となった身代金要求型の「WannaCry」よりも、システム破壊を目的とするなど一層手口がエスカレートしており、ウクライナの事案では、電力・地下鉄・銀行といった重要インフラで大混乱が発生しています。

また、従来から問題となっている標的型攻撃が巧妙化し、攻撃者が自作したマルウェアを使わず既成ソフトウェアの脆弱性を利用することでファイルレス化し、不正検出の回避や痕跡を残さない手口が増える傾向にあります（**図表1**参照）。

ランサムウェアをはじめとするサイバー攻撃による被害の深刻化は、発見された攻撃の痕跡が2割程度という調査結果からもうかがえ、攻撃手法が巧妙化した影響であることが推測されます。このようなサイバー攻撃が社会的に注目され、経営上のリスクとしての意識が高まるなか、企業が取り組むべきセキュリティ対策とその実態について、本調査結果から考察します。

図表1　サイバー攻撃による不正侵入の痕跡を発見した企業



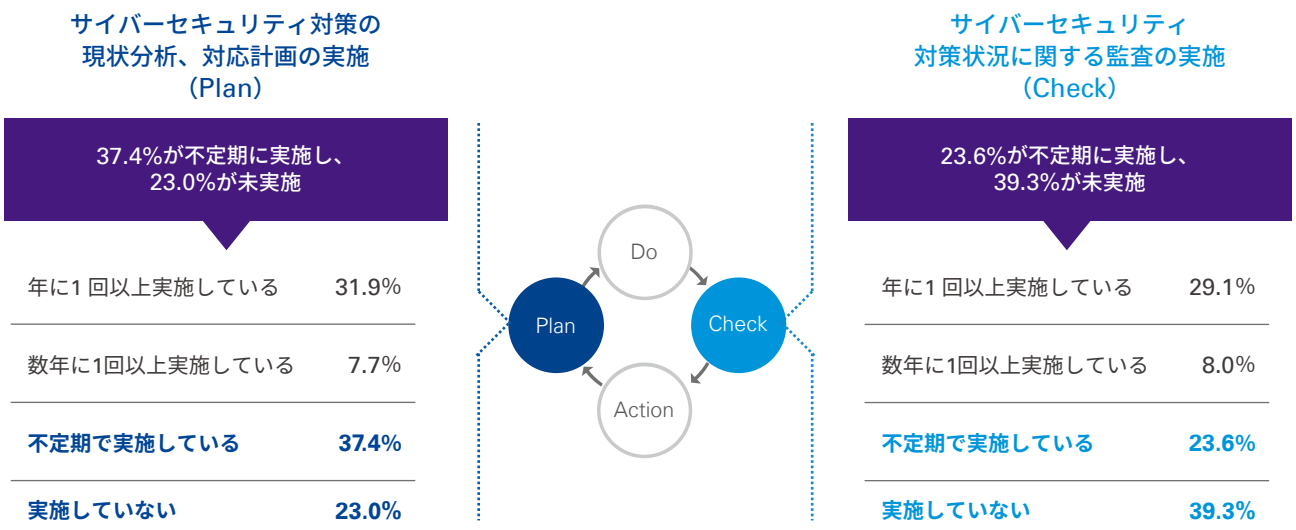
2. サイバーセキュリティ対策の現状

企業は世の中で発生するセキュリティインシデントの状況を常に鳥瞰的に捕捉し、攻撃に対抗し得る戦略を計画し実践したうえで、監視し改善しつづけなければなりません。

しかし、**図表2**が示すように、セキュリティマネジメントフレームワーク、いわゆるPDCAサイクルの観点では、サイバーセキュリティ対策の現状分析・対策計画で約6割、対策状況の監査においても約6割の企業が不定期で実施、あるいは実施していないという状況です。

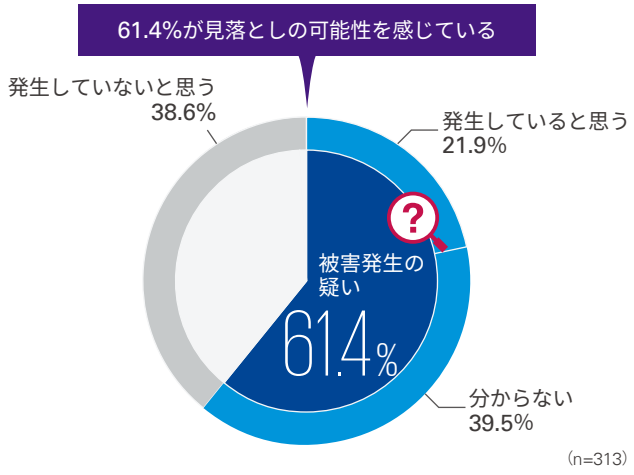
不正侵入の痕跡の発見が約2割程度という結果からも、未だサイバー攻撃を対岸の火事と捉え、自社が比較的安全であると認識しているようにも読み取れます。また、実際には攻撃を受けている可能性がある、あるいは分からないと回答した企業が約6割を占めており（**図表3**参照）、危機意識に対し行動が伴っていない傾向が見られます。

図表2　サイバーセキュリティ対策の継続



図表3　見えない攻撃への不安

自社で認識できていないサイバー攻撃による被害発生の可能性



II. 現状課題と投資を要する領域

デジタルトランスフォーメーション（DX）の浸透と連鎖して取り組むべきセキュリティ対策の課題として、前回の調査結果と同様にセキュリティの専門性を備えた人材の不足が突出しています。経済産業省は、2020年には情報セキュリティ人材が20万人程度不足すると予想しています。

この解決策として、専門性を備えた人材を新たに外部から採用するのではなく、役割に応じた人材の育成やアウトソーシングが考えられます。たとえば、セキュリティ戦略や企画、さらにリスクの評価・分析などといったマネジメントレベルに相当する人材は、自社のビジネスリスクを踏まえた対応が求められることから、業務知識を有する社内リソースから人材を選出しセキュリティ分野の訓練を積むのが有効です。一方、セキュリティ監視やインシデントの調査・分析などの実務面においては、外部サービスのMSS（マネージド・セキュリティサービス）などを活用する選択肢があります。その過程で社員が関与し、ノウハウの取得とスキルアップを図ることも考えられます。

企業のサイバーセキュリティに対する投資を前年（2018年）と比較して、横ばい、もしくは増加と答えた企業が9割強に上り、さらなる投資を要する対策領域として人材の育成が最上位となっていますが（**図表4**参照）、情報セキュリティ人材を確保するには経営層の理解が必要です。サイバーセキュリティに関するリスクを経営リスクと位置付け、危機意識を一層高めることが最優先事項と言えるでしょう。

NISC（内閣サイバーセキュリティセンター）が公開する「企業経営のためのサイバーセキュリティの考え方の策定について」にもあるように、企業の競争力を高めるために成長戦略としてAIやIoT、

図表4　今後の投資を要する対策

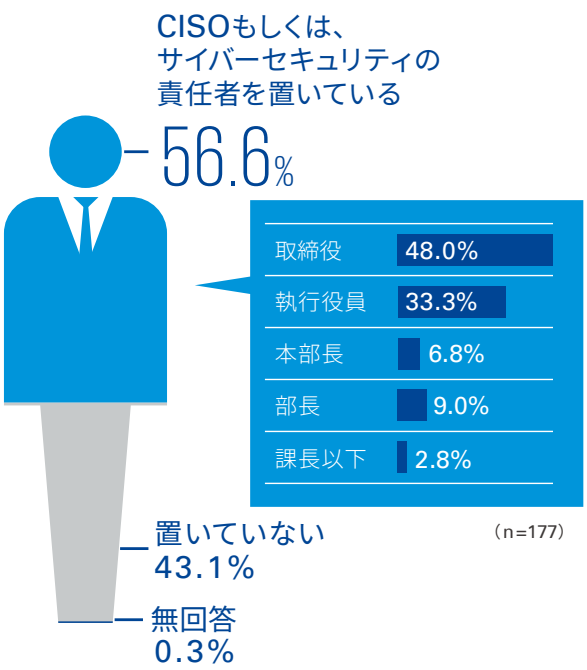
サイバーセキュリティ人材の育成が
最優先の課題となっている

サイバーセキュリティ人材の育成	**56.2%**
セキュリティ監視の強化	52.1%
内部不正対策	50.5%
IoT／クラウド環境におけるセキュリティ対策	49.5%
インシデント対応態勢（CSIRT）の強化	43.5%
モバイルデバイスの保護	43.1%
マルウェアやランサムウェア対策	40.6%
事業継続管理	39.3%
サイバーセキュリティ経営体制の構築	32.3%
脆弱性診断やペネトレーションテスト	30.0%
WEBサイトやインターネット公開システムの保護	24.9%
外部委託先管理	24.6%
制御システム環境におけるセキュリティ対策	22.0%
プライバシー情報の保護	17.9%
ブロックチェーン／仮想通貨の利用環境における セキュリティ対策	4.5%
その他	1.9%
特にない	1.3%

RPAなどの先進技術を採用するとともに、「セキュリティ品質」をより一層高めて社会的責任を果たすことが自社のブランド価値向上に繋がることを経営層に訴求する必要があります。そして、対策を講じない場合のリスクと講じた場合のメリットについて経営層がしっかりと理解することが重要です。

IPAによる「企業のCISOやCSIRTに関する実態調査2017」では、日本の経営層が情報セキュリティの意思決定にかかわる割合は6割近くに上るとされ、CISO（Chief Information Security Officer：最高情報セキュリティ責任者）の設置状況の調査でも、ほぼ類似した結果となり、役員クラスが意思決定を担うケースが大半を占めています（**図表5**参照）。しかし、欧米では約8割の企業がCISOを設置しており、専任の比率は米国の78.7%、欧州の67.1%に対し、日本は27.9%と極めて低い状況であり、明らかにセキュリティ人材不足を象徴した結果となっています。

図表5　情報セキュリティ責任者の設置状況

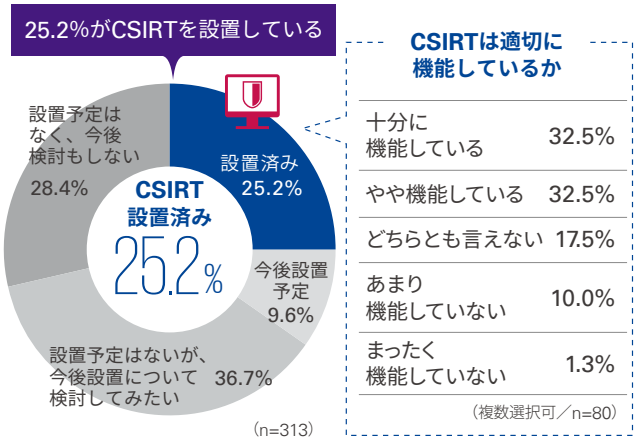


III. インシデント対応の体制

本調査で、インシデント対応の専門組織であるCSIRTの設置状況を見ると、設置済み企業の割合は25.2%と極めて低く、IPAの調査でも、米国55.6%、欧州32.9%、日本は22.6%となっています。また、IDC Japanが2019年に実施した国内ユーザ企業829社の調査では、従業員数3,000人以上の企業で50%が設置しており、従業員の規模に比例する傾向が見られます。

また、CSIRTが十分に機能していると答えた企業の割合は3割程度と、これも欧米に比べ極めて低い結果となり、人材不足の影響が影を落としているように読み取れます（**図表6**参照）。

図表6　CSIRTの設置状況



特にインシデント対応に求められるスキルはマルチレイヤーコントロールの技術的スキルや、組織のマネジメントから外部との交渉、経営層への説明といった人的スキルなど多岐に亘り、すべて揃った人材を最初から確保するのは極めて難しいと言えます。各メンバーの強みでお互いを補完し合う体制作り、あるいは前述したようなアウトソーシングの活用から徐々に社員の実務にシフトしていくといった人材育成のアプローチが効果的な打開策になります。

IV. 制御システムセキュリティへの取組み

本調査では、主に製造業や重要インフラ事業分野を中心として、制御システムを活用した事業を営む企業の割合が3割程度となっています。このなかで制御システムセキュリティの取組み状況について、対策方針の整備の観点から調べたところ、**図表7**が示すように4割程度と、組織全体のITセキュリティの取組みに対し、OT（Operational Technology）セキュリティは半分程度となっています。

一昔前の制御システムはIT系とは異なり独自のシステムや通信プロトコルを採用し、企業のOA基盤ネットワークから物理的に隔離されており、サイバーセキュリティとは無縁でした。しかし、昨今、経営効率化やコスト削減など市場の高い要請から制御系ベンダーは汎用的なIT技術を採用し、ITとOTを相互接続する時代を迎え、さらにDXの潮流によってOT環境から直接外部ネットワークに繋がるようになり、サイバーセキュリティリスクの複雑さがより一層増しています。組織全体のセキュリティ統制役を担う情報システム部門と、工場資産を管理する設備管理部門との連携が喫緊の課題であり、そのためには経営層の関与が最優先となります。工場資

図表7　サイバーセキュリティ―対策方針の整備状況

	組織全体のサイバーセキュリティ対策方針	制御システムセキュリティ対策方針
対策方針を単体で取りまとめた規程がある	42.0%	13.0%
単体で取りまとめた規程はないが、他の社内規程に対策方針を含めて記載している	40.4%	27.0%
	約80%	40%
対策方針は策定していない	17.3%	60.0%
無回答	0.3%	0.0%

産がサイバー攻撃を受けた場合には生産ラインの停止や遅延が自明であり、事業機会損失など経営に直接影響を及ぼすことを経営層に強く訴求し、ITとOTが盤石に統制されたセキュリティフレームワークの確立を進めるべきです。

V. 今後に向けて

今後はサプライチェーンにおけるDX化もさらに進むことが予想され、単一組織だけの統制から、連携する組織間の統制が課題となります。サイバーセキセキュリティにおいても、特定の組織が脆弱性を抱えている場合、連携組織一体としての脆弱性と捉える必要があり、取り組むべき対策のハードルはますます高まるでしょう。これには政府の後押しが必要であり、経済産業省は2018年よりユーザ企業、ベンダーを対象にサイバーセキュリティに対するニーズの明確化・具体化を目的とした情報交換の場として、「コラボレーション・プラットフォーム」を立ち上げています。

次回以降の調査では、企業の主要な取組み状況のトレンドを追うとともに、サプライチェーンをはじめクラウド、IoT、IIoT、AI、5Gなどの技術を活用したDX化で、予想される新たなリスクを俯瞰しつつ、有益な情報を広く社会に提供していくことも考えています。

サイバーセキュリティサーベイ2019

2019年10月発行

Japanese

本調査レポートは、ウェブリンクより閲覧、ダウンロードが可能 です。

home.kpmg/jp/cyber-survey-2019

本稿に関するご質問等は、以下の担当者までお願いいたします。

KPMGコンサルティング株式会社
テクノロジーリスクサービス
マネジャー　　新井　保廣
TEL：03-3548-5111（代表電話）
yasuhiro.niii@jp.kpmg.com

KPMGジャパン

marketing@jp.kpmg.com
home.kpmg/jp

home.kpmg/jp/socialmedia