KPMG

KPMG Insight

KPMG Newsletter

Vol.17

March 2016

経営トピック③

サイバーインシデント対応戦略

kpmg.com/jp

サイバーインシデント対応戦略

KPMG コンサルティング株式会社

サイバーセキュリティアドバイザリー
ディレクター　小川　真毅

小川　真毅
おがわ　まさき

ウイルス感染やウェブサイトの改ざん、コンピューターデバイスの紛失・盗難、メールの誤送信といった従来のセキュリティインシデントは、攻撃手法やその影響範囲が単純または限定的であり、原因究明や復旧にさほど時間を要しませんでした。
これに対し、標的型攻撃に代表される昨今のサイバー攻撃は、その名のとおり特定の組織や従業員を標的として対象を絞って巧妙にカスタマイズされており、痕跡を残さないように様々な手法を駆使して実行されるため、被害が拡大するまで表面化することなく攻撃が進行してしまう傾向にあります。
本稿では、こうしたサイバーインシデントを早期に検知するとともに、発生したインシデントの被害を最小限に抑えるために必要な体制と仕組みの構築、運用といった、サイバー脅威全盛時代に組織に求められる復旧対応力（＝レジリエンシー）について解説します。
なお、本文中の意見に関する部分については、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】

- 2015年12月に経済産業省が公開した「サイバーセキュリティ経営ガイドライン」では、企業の経営者はサイバーセキュリティに関するリーダーシップ、積極的な投資への関与、ステークホルダーへの説明責任を果たすことが「3原則」として求められている。
- 企業がサイバーレジリエンシーの維持向上を実現するためには、サイバーインシデントの検知や対応に必要な体制の構築、専門的スキルと人的リソースの確保、サプライチェーン環境の考慮など、様々な課題を理解し、解決する必要がある。
- 企業の経営者は、CISO（Chief Information Security Officer）の設置をはじめとしたリーダーシップの確立、サプライチェーンを含めたサイバーセキュリティ統制、インシデント検知と対応オペレーションの最適化を通じて、サイバーインシデント対応能力を高めていかなければならない。

I. サイバーセキュリティ経営ガイドライン

2015年12月28日、経済産業省商務情報政策局情報セキュリティ政策室が推進し、企業経営者向けにサイバーセキュリティ対策の原則や重要項目をまとめた「サイバーセキュリティ経営ガイドライン」が正式に公開されました[1]。本章では、このガイドラインの概要紹介を通じてサイバーインシデント対応の重要性について解説します。

1. サイバーセキュリティ経営の3原則

企業に対するサイバー攻撃が大規模化、巧妙化する一方、サイバーセキュリティリスクや対策の必要性に関する経営層の理解が不十分であったり、その対策の推進において十分なリーダーシップが発揮されていなかったりすることで、深刻な被害に発展しているケースが散見されています。

たとえば、ガートナー社が実施した、日本企業に対する情報セキュリティ調査[2]において、自社の情報セキュリティ人材がどのような肩書きや資格を保有しているかを尋ねた結果、「肩書きはない（兼務など）」が最も多く（43.1%）、次に「情報セキュリティ委員長」が36.6%、「プライバシーマーク委員長」が19.7%となりました。自社に最高情報セキュリティ責任者（CISO）がいると答えた企業の割合は、18.9%でした。

※2015年3月にガートナーが日本国内の企業に実施した本調査は、ユーザー企業のIT部門のマネージャーを対象にしたものです。対象企業の業種は全般にわたり、有効回答企業数は515件でした。

これを端的に捉えれば、8割以上の企業において、サイバーセキュリティに関する経営上の明示的な責任を有する専任者が存在しないことを意味しており、予算の確保や組織全体に渡る対策の推進、ステークホルダーへの説明責任などが十分に実行されないリスクを抱えていることになります。

したがってこのガイドラインは、こうした経営者によるサイバーセキュリティリスクに対する認識とリーダーシップの欠如を改善することを企図しており、「サイバーセキュリティ投資への積極的関与」、「グループ企業、サプライチェーン、ビジネスパートナーを含めた対策」、「サイバーセキュリティ対策に関するステークホルダーへの情報開示とコミュニケーション」という3つの事項を挙げ、経営者が認識すべき「3原則」としています（**図表1**参照）。

【図表1　サイバーセキュリティ経営の3原則】

原則1	原則2	原則3
経営者は、IT活用を推進する中で、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要	自社は勿論のこと、系列企業やサプライチェーンのビジネスパートナー、ITシステム管理の委託先を含めたセキュリティ対策が必要	平時及び緊急時のいずれにおいても、サイバーセキュリティリスクや対策、対応に係る情報の開示など、関係者との適切なコミュニケーションが必要

出典：経済産業省「サイバーセキュリティ経営ガイドライン」（2015年12月）を基にKPMGが作成

2. サイバーセキュリティ経営の重要10項目

このガイドラインでは、3原則に加えて、経営者がCISOまたは相応の責任者に対して要請すべき「重要10項目」を「リーダーシップ」、「リスク管理」、「事前対策」、「事後対応」という4つのカテゴリに分類して示しています（**図表2**参照）。

【図表2　サイバーセキュリティ経営の重要10項目】

カテゴリ		重要10項目
リーダーシップの表明と体制の構築	1	サイバーセキュリティリスクの認識、組織全体での対応の策定
	2	サイバーセキュリティリスク管理体制の構築
サイバーセキュリティ**リスク管理**の枠組み決定	3	サイバーセキュリティリスクの把握と実現するセキュリティレベルを踏まえた目標と計画の策定
	4	サイバーセキュリティ対策フレームワーク構築（PDCA）と対策の開示
	5	系列企業や、サプライチェーンのビジネスパートナーを含めたサイバーセキュリティ対策の実施及び状況把握
リスクを踏まえた攻撃を防ぐための**事前対策**	6	サイバーセキュリティ対策のための資源（予算、人材等）確保
	7	ITシステム管理の外部委託範囲の特定と当該委託先のサイバーセキュリティ確保
	8	情報共有活動への参加を通じた攻撃情報の入手とその有効活用のための環境整備
サイバー攻撃を受けた場合に備えた準備（**事後対応**）	9	緊急時の対応体制（緊急連絡先や初動対応マニュアル、CSIRT）の整備、定期的かつ実践的な演習の実施
	10	被害発覚後の通知先や開示が必要な情報の把握、経営者による説明のための準備

出典：経済産業省「サイバーセキュリティ経営ガイドライン」（2015年12月）を基にKPMGが作成

1　経済産業省、独立行政法人 情報処理推進機構「サイバーセキュリティ経営ガイドライン Ver 1.0」（2015年12月）
http://www.meti.go.jp/press/2015/12/20151228002/20151228002.html

2　ガートナープレスリリース「ガートナー、情報セキュリティに関する調査結果を発表　デジタル・ビジネスにおける情報セキュリティの取り組みには「人材」が重要となるものの、約半数の日本企業にはセキュリティ人材の採用計画がないという結果に」（2015年7月1日）
https://www.gartner.co.jp/press/html/pr20150701-01.html

これら4つのカテゴリはいずれも企業経営者がサイバーセキュリティ対策を推進するために不可欠な要素ですが、どれだけ「リーダーシップ」、「リスク管理」、「事前対策」を徹底しても、次から次へと新たな手段を講じてサイバー攻撃が仕掛けられてくる昨今のサイバーセキュリティ分野においては、残念ながら完全にサイバーセキュリティリスクを排除することはできません。

したがって、企業の事業継続性を確保するための最後の砦である「事後対応」の重要性がますます高まっており、サイバー攻撃によるインシデント発生時における復旧対応力（＝サイバーレジリエンシー）の向上がまさに求められていると言えます。

Ⅱ. サイバーレジリエンシーにおける課題

1. サイバーインシデントの検知

企業がサイバーレジリエンシーを高めるために、インシデント発生時の対応体制を確立する必要があるのは言うまでもないことですが、自社がサイバー攻撃による侵入や被害を受けていると気付くことができない限りはこのインシデント対応体制は発動されず、無用の長物と化してしまいます。また、たとえサイバー攻撃に気付くことができたとしても、その発見に時間がかかりすぎてしまえば手遅れとなり、被害の拡大を阻止することは極めて困難になります。

（1）サイバー攻撃発見までの時間

ベライゾン社のセキュリティインシデント調査レポート[3]によると、サイバー攻撃の発生後、数日以内に検知することができた割合は、数日以内にサイバー攻撃が成功した割合を大幅に下回っており、多くの場合サイバー攻撃による侵入や被害がある程度進行してからようやく検知に至っていることがわかります（**図表3**参照）。

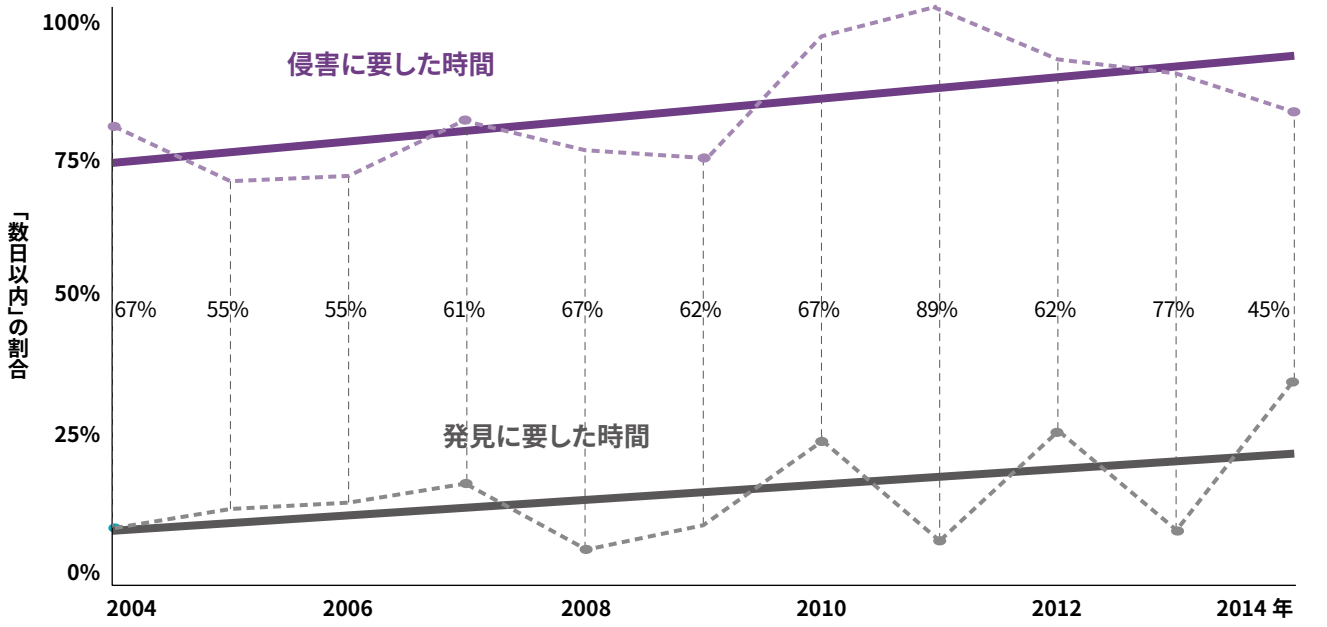
同レポートでは、調査対象となったサイバーインシデントの約60%が、サイバー攻撃の開始から数分以内に企業への侵入に成功していたと報告しており、サイバーインシデントの検知機能が十分整備されていない企業がまだまだ多いことを、如実に物語っています。

（2）セキュリティ監視体制の構築

近年多くの企業がこうした課題を解決するために、サイバー攻撃の兆候や被害を早期に検知するためのセキュリティ監視センター（SOC:Security Operation Center）の構築を進めていますが、経営層によるスポンサーシップが十分でない場合、監視オペレーターの人員不足やスキル不足などが生じて効果的に機能していないケースもよく見受けられます。

人員やスキルの不足、コスト的な問題を解消するという観点

【図表3　サイバー攻撃の発見と侵害の時間的差異】



出典：ベライゾンジャパン合同会社「2015年度データ漏洩／侵害調査報告書」

3　ベライゾンジャパン合同会社「2015年度データ漏洩／侵害調査報告書」
https://www.verizonenterprise.com/jp/DBIR/2015/

から、自社設備としてこうした監視センターを構築するプライベート型SOC（PSOC:Private Security Operation Center）ではなく、セキュリティ監視業務を外部の専門業者に委託するマネージド型SOCを導入する企業も増加しています。

マネージド型SOCは、一般にマネージドセキュリティサービスプロバイダー（MSSP:Managed Security Services Providers）と呼ばれる事業者によって提供されており、VPNや専用線などのセキュアなネットワーク経由でリモートから自社へのサイバー攻撃の発生状況を監視するサービスです。こうしたサービスは、自社でセキュリティ監視のための人材確保や育成、大規模なシステム導入の必要がなく、比較的容易にセキュリティ監視を開始し、効率的に運用できるというメリットがある一方、自社固有のアプリケーションやシステムの監視には対応していない、各システムの事業上の重要性や情報資産価値を考慮したリスクレベルの割り当てが難しいなどのデメリットもあります。

そのため、委託元の企業側でも一部固有のアプリケーションやシステムを監視したり、外部委託業者から受け取ったセキュリティアラートの自社事業への影響度を判断する必要が生じるなど、セキュリティ監視の網羅性や精度の面では完全に外部委託だけに依存することはできません。

（3）サプライチェーンの注視

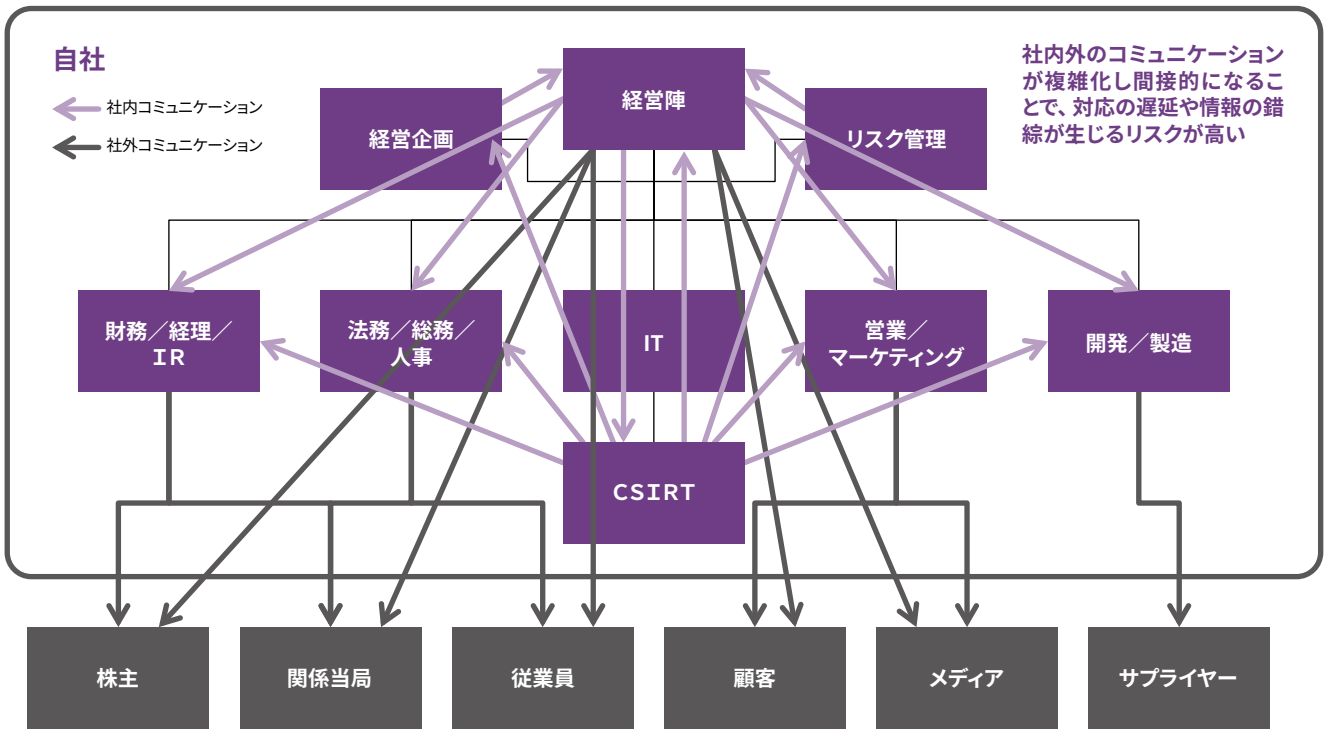
一昨年に国内で発生した大規模情報漏えいインシデントでは、委託先従業員が不正に個人情報を取得して第三者へ提供していたことが問題でした。

ビジネスの拡大において多様なベンダー、サプライヤー、ビジネスパートナーとの関係を構築し、情報のやり取りやネットワークの相互接続をすることは必要不可欠になっています。しかし一方で、事業環境、事業規模、ITインフラが異なれば、サイバーセキュリティに対する意識や対策方針も当然異なり、サプライチェーンで繋がっている外部の組織が必ずしも自社と同等のセキュリティレベルを有しているとは限りません。サプライチェーンを通じて自社の情報資産や顧客情報を取り扱う事業体が増加すればするほど、サイバーリスクも増加するということに注意を払う必要があります。

2. サイバーインシデントへの対応

サイバーインシデントを検知するためのセキュリティ監視体制と両輪の関係にあるのが、サイバーインシデント対応体制です。言うまでもなく、サイバーインシデントが検知された場合には、迅速に初動対応にあたり、被害拡大の防止から原因究明、内外に向けたコミュニケーションを主導的に執り行うための体制とプロセスの確立が不可欠です。

【図表4　複雑化したインシデント対応コミュニケーション例】



このための体制は、一般にコンピューター(またはサイバー)セキュリティインシデントレスポンス体制、もしくはCSIRT(Computer／Cyber Security Incident Response Team)と呼ばれ、前章で紹介した「サイバーセキュリティ経営ガイドライン」でもその設置が重要項目の1つとして挙げられているだけでなく、サイバーセキュリティ基本法に基づく重要インフラ事業者向けのガイドラインなど様々な業界規制やガイドラインにおいて推奨事項とされています。

(1) 平時と緊急時の切り分け

多くの場合、サイバーインシデント対応体制の確立においても、セキュリティ監視体制と同様の課題が生じます。一般に、CSIRTのようなインシデント対応チームは、インシデントが発生した緊急時に本格的に稼働しますが、インシデントが発生していない平時においては、インシデント対応計画の改善や訓練などは必要になるものの、常時すべての要員をこの活動に割り当てることは経営効率上困難な場合が多いため、いざという時に効果的に機能しなかったり、他業務とのリソース衝突によって十分な要員を確保できなかったりするケースがあります。

(2) 体制の位置付け

サイバーセキュリティ対策はIT部門の管轄であると認識している経営者も未だ少なくないため、インシデント対応体制を含め、すべてIT部門の担当として割り当てている場合があります。

実際に、図らずもサイバーインシデントを経験してしまった企業の経営者であれば身をもって経験しているはずですが、インシデント発生時には技術的な対処だけではなく、関係当局や規制団体への報告、顧客やメディアとのコミュニケーション、責任者の処遇など、組織内の様々な部門に影響が及ぶため、IT部門だけで判断できない対応事項が多く発生し、社内外とのコミュニケーション経路が複雑化します(前頁**図表4**参照)。

さらに、サプライチェーンに関わる外部組織が関係するサイバーインシデントが発生した際には、各事業体がどのような責任範囲でどのように連携するのかあらかじめ共通理解が行われていないと、その調整に手間取ることで対応が後手に回ってしまう可能性が高く、こうした観点も含めた体制の整備が必要となります。

(3) 専門的知識の習得

たとえCSIRTのリソースを十全に確保し、組織横断的な活動体として定義したとしても、最新のサイバー攻撃やテクノロジーに対する専門知識の不足により対応を誤ると、原因究明が極めて困難になり、被害の拡大を招いてしまう可能性もあります。

たとえば、標的型攻撃などで使われるカスタマイズされたマルウェアは、自身のプログラムをメモリー上でのみ稼働させ、ハードディスク上には痕跡を残しません。そのため、システムの動作がおかしい、または情報漏えいの懸念などが生じた際に、疑わしい端末を安易に再起動してしまうと、メモリーは揮発性記憶媒体であるため、そこで稼働していたマルウェアの情報は跡形もなく消えてしまい、再起動後には何の痕跡も残らず原因究明が極めて困難になります。

Ⅲ. サイバーインシデント対応戦略

1. 経営層のリーダーシップ

ここまで見てきた課題を踏まえ、何よりもまず経営層は、サイバーインシデントへの対応体制の確立が組織における最優先事項の1つであることを、組織内外のステークホルダーに対して明示的に表明する必要があります。

そのための具体策としてCISOの任命が挙げられます。CISOはサイバーセキュリティに関する専門的な知見を有し、サイバーリスクが組織の経営に与える影響を分析したうえでステークホルダーに対する説明責任を果たすとともに、適切な意思決定に基づく経営資源の割り当てを行うことができる人材です(**図表5**参照)。これまで多くの企業はこうした人材の育成には力を注いでこなかったため、前述の統計が示すようにCISOは非常に希有な存在となっています。

自社でこうした素養を持つ人材がいる場合は今後積極的に育成していく必要がありますが、サイバー攻撃が熾烈化している現状ではそのような中長期的アプローチだけでは組織のレジリエンシーを早期に改善することはできません。そのため、外部からCISOを招聘したり、CISOの役割を部分的に専門家に委

【図表5　CISOに求められる人材像と主な役割】

人材像	✓ サイバーセキュリティ専門家としての豊富な経験と知識 ✓ サイバーセキュリティ業界における幅広いネットワーク ✓ 組織のビジネスに関する深い理解 ✓ 経営幹部としてのマネジメントスキル
主な役割	✓ 組織のサイバーリスクを一元的に把握し、組織経営と事業継続に対するインパクトを分析・評価する ✓ CEO／CIO／CROなど他の経営幹部と密接に連携し、経営資源の投入に関する意思決定を行う ✓ 組織とサプライチェーン全体に渡るサイバーセキュリティガバナンスを推進するための方針を提示し、統制状況を監督する

託したりするなど、内部育成以外の短期的アプローチも検討する必要があります。

2. サプライチェーンの統制

経営層がリーダーシップを発揮すべき範囲は自社組織内にとどまりません。サプライチェーンを通じたサイバーリスクの増長を理解し、サプライチェーン全体に渡るサイバーセキュリティ上の統制活動を推進しなければなりません（**図表6**参照）。

具体的には、ベンダー、サプライヤー、ビジネスパートナーとの間でサイバーセキュリティ上の責任範囲の切り分けや自社と同等のサイバーセキュリティ対策の要請などを行ったうえで、定常的にサイバー攻撃に対する監視状況を共有し、必要に応じて委託先を監査できるような連携体制の確立を、CISOや最高リスク管理責任者（CRO：Chief Risk Officer）、および各事業責任者を通じて徹底する必要があります。

3. インシデント検知・対応オペレーションの最適化

限られた経営資源を有効に活用してサイバーインシデントの検知・対応体制を確立するためには、組織、プロセス、テクノロジーそれぞれの観点で自社の組織環境に最適なオペレーション体制を選択する必要があります（**図表7**参照）。

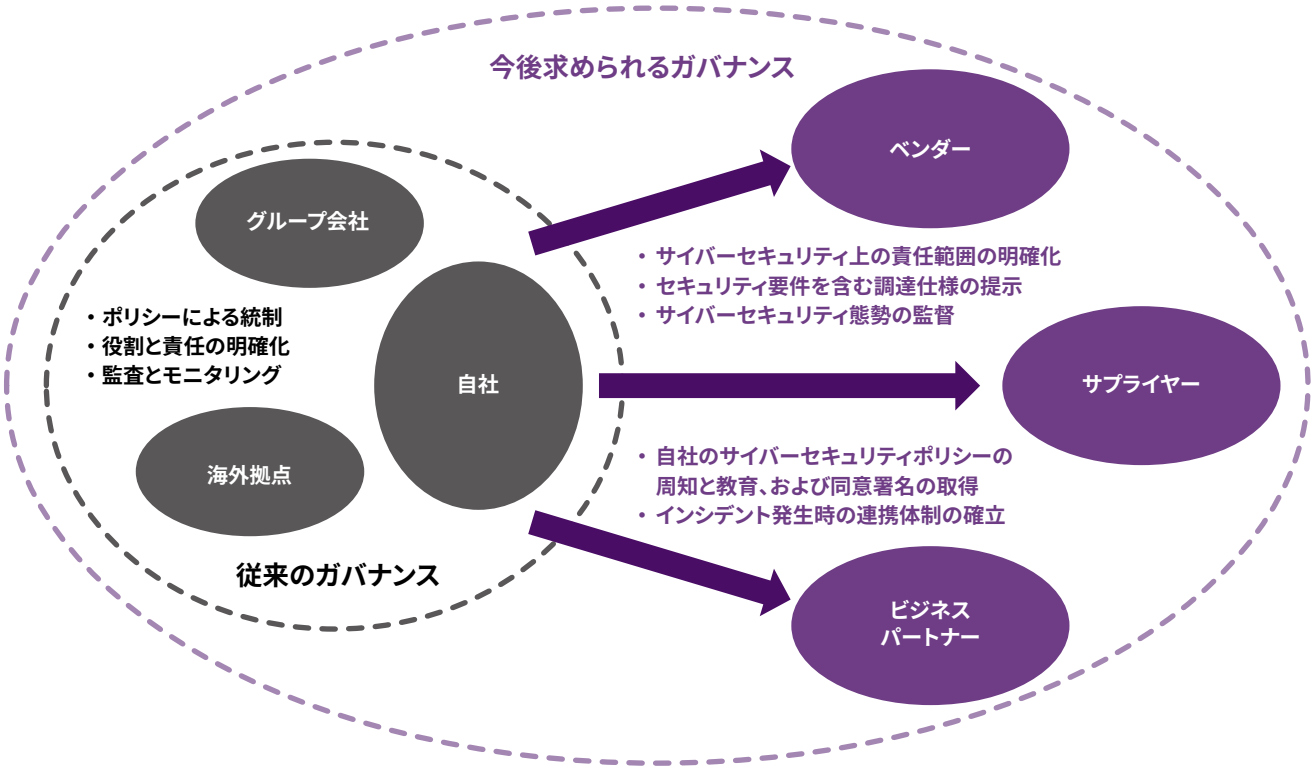
まず組織の観点では、平時と緊急時それぞれの人的リソース配分やCSIRTの位置付けと要員構成、内部要員のスキルで対応可能な範囲と外部の専門家に依存すべき範囲の切り分けなどについて、分析したうえで方針を決定する必要があります。

次にプロセスの観点では、セキュリティ監視対象の選定、資産価値と脅威の深刻度に応じたリスクレベルの定義、インシデント対応計画の策定と訓練などを実施する必要があります。

【図表7　インシデント検知・対応体制の最適化ポイント】

組織	✓ 平時と緊急時の人的リソース配分 ✓ 迅速な対応と円滑なコミュニケーションを実現するためのCSIRTの組織的位置付け（経営直轄か、組織横断的かなど） ✓ 内部リソースとスキルに基づく外部リソースの積極的活用
プロセス	✓ 優先度に応じたセキュリティ監視対象範囲やデバイスの選別 ✓ 資産価値と脅威の深刻度に応じたリスクレベルの定義と割り当て ✓ インシデント対応計画の策定と定期的訓練に基づく見直し
テクノロジー	✓ セキュリティ監視センターの構築形態（プライベート型／マネージド型／ハイブリッド型） ✓ 自社環境に整合したソリューションやツールの採用 ✓ グローバル展開・グループ展開を見据えたインフラ構築

【図表6　サプライチェーン全体のサイバーセキュリティ統制】



さらにテクノロジーの観点において、セキュリティ監視センターをプライベート型とマネージド型どちらで構築するか、どのようなソリューションやツールを採用するか、グローバル展開を見据えた場合にも展開可能か、といった点を考慮しながら導入を図っていく必要があります。

企業の経営者とCISO（または同等の責任者）は、こうした一連の取組みを通じて組織のレジリエンシーの維持向上に努めるとともに、組織全体のサイバーセキュリティ態勢とリスクを一元的に掌握し、次なる打ち手とそれを実行するための経営資源の投入に関して適切な意思決定を下すことで、セキュリティリスクを効果的かつ効率的に低減していくことが求められています。

IoTエコシステムとセキュリティ

【目次】

1. サイバーセキュリティは「必需品」になる
2. 業界標準の模索
3. セキュリティ、プライバシー、信頼性への取組み
4. エコシステム全体でセキュリティ、プライバシー、信頼性を追求する

IoT（モノのインターネット）に関しては、世の中で言われていることがすべて大げさであるとは言い切れません。実際、IoTは大半の人が考えているよりも大きな存在になる可能性さえあります。ただし、IoT分野で成功するには、単に洗練されたアプリケーションやネットワークに接続されたデバイス、高度な分析だけでなく、セキュリティやプライバシー、信頼性に対する確固たるアプローチが必要です。本レポートでは、世界中の100のIoT「ユーザー組織」に対する最新調査と、業界のリーダーや学会およびKPMGのIoT専門家への1対1のインタビュー取材に基づいて、IoTのセキュリティ、プライバシー、信頼性に焦点を合わせ、誕生しつつあるエコシステムのすべてのプレーヤーにとって実用的で実行可能な助言を提供します。

レポートはKPMGジャパンのウェブサイトからダウンロードいただけます。

http://www.kpmg.com/Jp/ja/knowledge/article/risk-advisory-thoughtleadership/Pages/iot-ecosystem-security.aspx

【バックナンバー】

サイバーリスク最新トレンドと対応戦略
（KPMG Insight Vol.15/Nov.2015）

サイバーインテリジェンス活用戦略
（KPMG Insight Vol.16/Jan.2016）

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
ディレクター　小川　真毅
masaki.ogawa@jp.kpmg.com

サイバーセキュリティアドバイザリー
kc-cybersecurity@jp.kpmg.com

KPMGジャパン

marketing@jp.kpmg.com
www.kpmg.com/jp