サイバーセキュリティ経営実践ガイダンス

サイバーインテリジェントプラットフォームの活用

2017年6月

2020年の東京オリンピック・パラリンピックに向け、政府は民間企業に対してサイバーセキュリティの強化を求め、情報共有を推進しています。その一方で、情報漏えい事故などは後を絶たず、中には経営に大きなインパクトを与えているケースも少なくありません。そうした中、2015年12月に経済産業省から「サイバーセキュリティ経営ガイドライン」が公開されました（2016年12月改訂）。

本ホワイトペーパーでは、あらためて「サイバーセキュリティ経営」とは何かを考えるとともに、経営目線での実効的なセキュリティへの取組みを考察しています。

1. はじめに

今年も世界経済フォーラム（ダボス会議）で「グローバル・リスク報告書2017年版」が公表されました。グローバル・リスクは5つのカテゴリー（経済、環境、地政学、社会、技術）から構成されており、注目すべきリスクとして、異常気象、自然災害、大規模な移民、テロ、水資源危機、気候変動対応と並び、「サイバー攻撃」が上位リスクに位置付けられています。

つまり、サイバー攻撃は経営にとって無視できないリスクとなっています。しかし、現実には日々発生するセキュリティインシデントへの対応に追われ、本来推進すべき計画に従った対策の実行が思うように進まないことも多くあります。

多くの企業では毎年、サイバー攻撃への対策を含むセキュリティ施策に関する予算と活動計画が議論されますが、そのインプット情報として、前年度の振り返り、具体的には、実施したセキュリティ施策の成功要因や失敗要因を評価・分析した結果を用いることが極めて重要です。

しかし、こうしたフィードバックが適切に行われているケースは多くなく、それは、明確なKPI（Key Performance Indicator、重要業績評価指標）を設けていないことが理由の1つとして挙げられます。

各セキュリティ施策について、具体的な目標を達成するために、どのような効果を期待し、それを実現できたと判断するための定量的な指標（KPI）を定め、それぞれの施策の相関関係を含めた活動計画を策定することが肝要です。

このように、サイバーセキュリティ経営を実践していく上で、セキュリティに対する考え方、進め方を改めて見直す必要があると考えられます。

2. サイバーセキュリティ経営の理解

経営者は、世界各地で大きなセキュリティインシデントが発生し、その被害がメディアなどで報道されると、自社で同様のインシデントが発生していないか、あるいはその可能性が無いか、速やかに把握したいと考えます。しかし、社内にそういった対応を行う組織が存在しないケースや、存在する場合でも、情報がその組織内で閉じられ、経営者がそれを把握する手段が無いケースも多く見られます。

自社でセキュリティインシデントが起きてしまってからでは遅いため、組織内におけるサイバーリスクとサイバーセキュリティ対策状況を経営者が常時把握できる状態とし、トップダウンで迅速に動ける仕組みを作ることが重要です。またその仕組みは、社会の情勢や、セキュリティ脅威の変化、つまりはリスクの変化に合わせて強化・改善していく必要があります。

2-1 サイバーセキュリティ経営とは

会社法上、経営者は内部統制の構築義務があり、そのうちの1つが「情報セキュリティ管理義務」です。情報セキュリティの重要性が叫ばれ、「サイバーセキュリティ経営ガイドライン」が公開されている中で、セキュリティリスクを把握していながら適切なコントロールを怠った場合、あるいは自社のセキュリティリスクそのものを把握していない場合は、経営者としての過失が問われる可能性があります。

そのため「サイバーセキュリティ経営ガイドライン」では、“セキュリティはコストではなく投資である”ことが明確に打ち出され、実施にあたり、「サイバーセキュリティ経営の3原則」［表1］と「サイバーセキュリティ経営の重要10項目」［表2］が定義されています。

［表1］　サイバーセキュリティ経営の3原則

サイバーセキュリティ経営の3原則
(1)　経営者がリーダーシップをとって推進すること
(2)　自社のみならず、系列企業やサプライチェーン等を含めたセキュリティ対策が必要であること
(3)　関係者との適切なコミュニケーションが必要であること

出所：経済産業省「サイバーセキュリティ経営ガイドライン」

［表2］　サイバーセキュリティ経営の重要10項目

サイバーセキュリティ経営の重要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
■ サイバー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
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

出所：経済産業省「サイバーセキュリティ経営ガイドライン」

2-2 サイバーセキュリティ経営の意義

「サイバーセキュリティ経営ガイドライン」では、サイバーセキュリティ経営についての重要施策が網羅されています。新たな仕組みを要求しているわけではなく、これまでの取組みを体系的に見直し、経営の理解と参画を得るためのガイドラインであり、これを企業が遵守すべきベースラインと捉え、自発的にセキュリティ対応を行うことが期待されています。

さらに「サイバーセキュリティ経営ガイドライン」には、「サイバーセキュリティ対策の状況について、サイバーセキュリティへの取組みを踏まえたリスクの性質・度合いに応じて、情報セキュリティ報告書モデル、CSR報告書、サステナビリティレポートや有価証券報告書等への記載を通じて開示を検討する」とも明記されています。すなわち、企業が情報セキュリティの取組みを開示することにより、当該企業の取組みが顧客や投資家などのステークホルダーから適正に評価されることを目指すものであり、経営者に対して、市場に評価される仕組みをつくることを推奨しています。

これがサイバーセキュリティ経営の最大の意義であると考えられ、自社の事業形態に適合した管理と運用の判断を行うことが重要です。

2-3 サイバーセキュリティ経営における課題

セキュリティ対策は、経営者が積極的に参画し、決断し、推進することにより、実装レベルや運用管理レベルの向上に確実に拍車がかかります。しかし一方で、セキュリティ対策は専門的、技術的な要素を含むため、一部の組織や担当者で属人的に行われていることも少なくありません。

「サイバーセキュリティ経営ガイドライン」においても、経営者が考えること、指示すべきことは整理されているものの、要求事項に対し“誰が”、“何をするのか”までは言及されていません。そのため、重要10項目の要求事項に対し、各々を具体的なタスクに落とし込む必要があります。

また、セキュリティ対策への投資に対する成果を測定し評価するためには、タスク毎にKPIを定義し、必要な情報を定量的に把握できるようにする必要があります。[表3]では「インシデントレスポンス（事故対応）」での必要なタスクを示しています。

［表3］ インシデントレスポンスに対するタスクとKPI

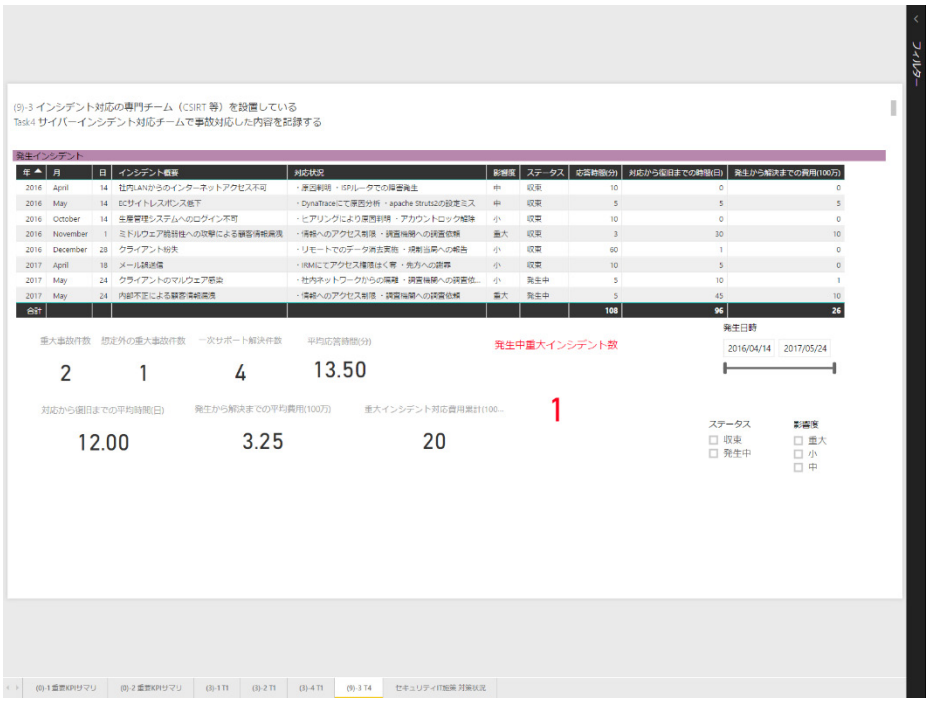
必要タスク
■ インシデントの定義
■ インシデント対応フローの作成と運営
■ インシデントのモニタリング（監視、検知）
■ 発生したインシデントのビジネスへの影響判断
■ インシデント対応を行うサービスデスクの設置
■ 情報セキュリティ委員会への報告、など
KPI
■ インシデントの発生件数（重大／軽微／ヒヤリハット）
■ 想定外の要因で発生した重大インシデントの件数
■ インシデント件数の削減率
■ インシデント対応から復旧までに要した平均時間
■ インシデント対応から復旧までに要した平均費用
■ インシデント対応に対する従業員の満足度

出所：経済産業省「サイバーセキュリティ経営ガイドライン」

単にインシデントの発生件数だけを捉えるのではなく、想定内／想定外の分析、インシデント対応に要した時間や費用、従業員満足度などを指標に加えれば、より現実的な評価（＝リターンの測定）が行えます。

このようなKPIは、内部の評価指標だけでなく、対外的に説明責任を果たすための具体的なエビデンスにもなり得ます。経営が求める実施状況（進捗状況）やリスク評価指標を可視化することができ、経営ダッシュボードによってセキュリティに対する投資効果（ROI）を把握することができます。

［図1］ 可視化したKPI例



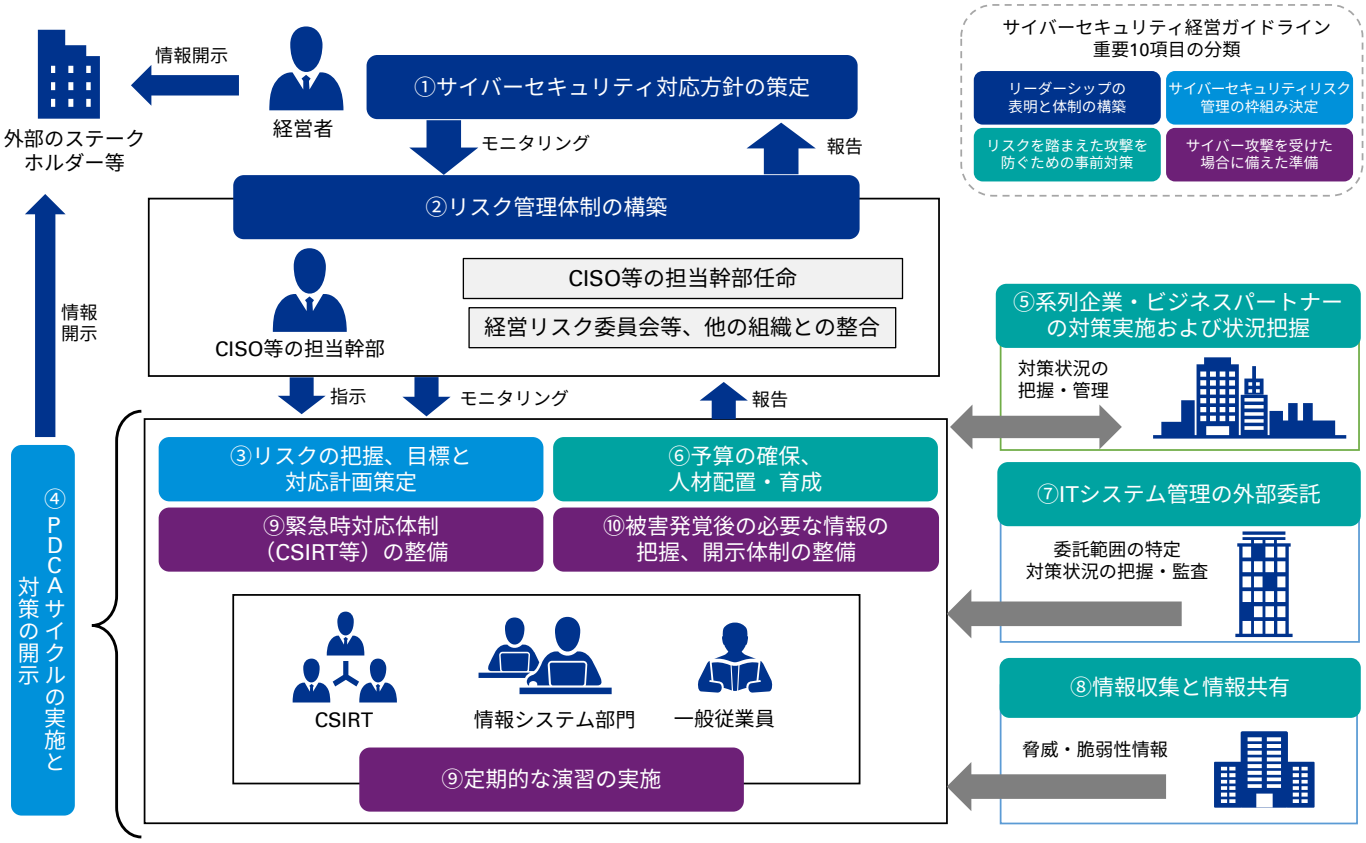
3 サイバーインテリジェントプラットフォーム概要

3-1 全体像

サイバーセキュリティ経営の実践における課題を克服し、効果的かつ効率的に継続管理を行うためには、さまざまな項目について有機的に連携させるための基盤が必要です。

たとえば、サイバーセキュリティ経営の重要10項目を企業が対応しなければならない活動プロセスと照らし合わすと、[図2]に示すような相関図になります。

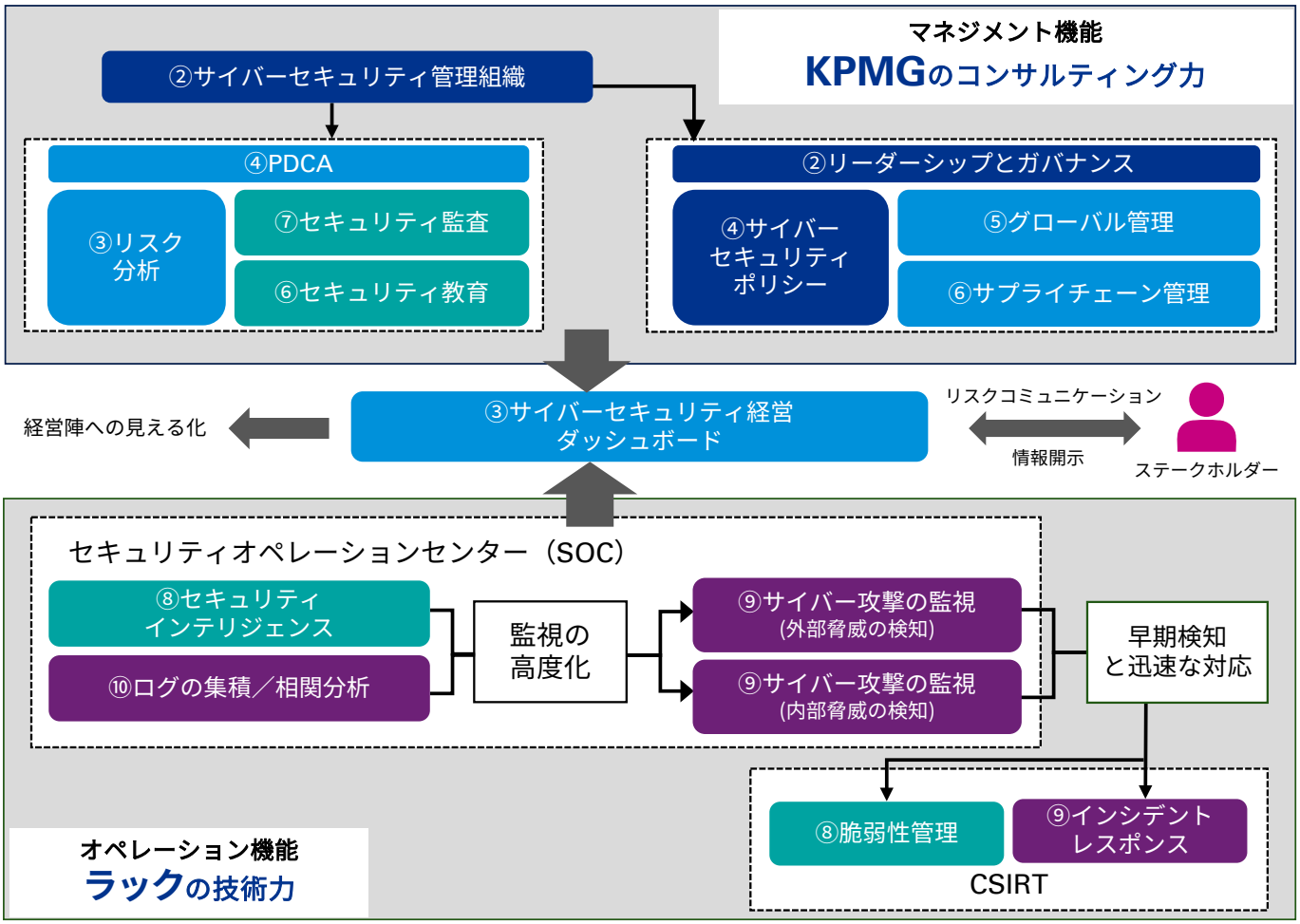
［図2］重要10項目への対応



このように、サイバーセキュリティ経営を実現するために不可欠な各種の活動は各独立した取組みではなく、すべてがお互いに影響し合い、つながり合った一連のプロセスです。

ラックとKPMGが、サイバーセキュリティ経営の実現を支援するための基盤として、サイバーセキュリティ経営の重要10項目をベースに共同開発したものが「サイバーインテリジェントプラットフォーム」です。

［図3］サイバーインテリジェントプラットフォームの概念図



「サイバーインテリジェントプラットフォーム」は、『マネジメント』と『オペレーション』の2つの機能から構成され、これらの機能に包含されるすべての活動は『ダッシュボード』を通じて可視化され、経営によるモニタリングを可能にします。

3-2 『マネジメント』機能

「サイバーインテリジェントプラットフォーム」の2大構成要素の1つである『マネジメント』機能は、サイバーセキュリティ管理組織を主体として、企業のサイバーセキュリティポリシーに基づく組織全体に対するリーダーシップと、サプライチェーンやグローバル組織への対応を含めた、網羅的なガバナンスの実現を支援するものです。

さらに、定期的なリスク分析に基づく改善策の実行、従業員の教育、サイバーセキュリティの計画・実行状況に対する客観的な監査といった、PDCAサイクルによる効果的なサイバーセキュリティ管理活動の実践を支援します。

3-3 『オペレーション』機能

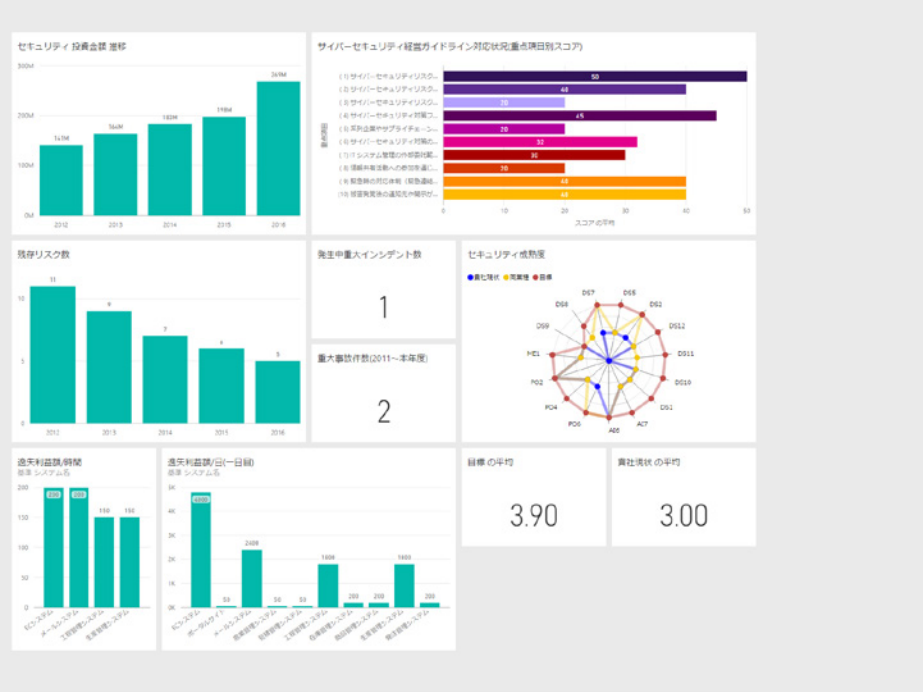
一方、『オペレーション』機能は、サイバー攻撃を未然に防ぎ、またサイバー攻撃を受けた際に迅速に検知することで被害の拡大を防止するセキュリティオペレーションセンター（SOC）の構築や運用の高度化を支援するものです。

さらに、インシデントが発生した場合に迅速かつ的確に対応するためのセキュリティインシデント対応体制（CSIRT）の構築や体制の強化を支援するものです。

3-4 『ダッシュボード』

「サイバーインテリジェントプラットフォーム」では、前述の2大機能によって実現されるべき各種のサイバーセキュリティ管理活動が効果的に機能していることを経営者やセキュリティ担当責任者（CISO）、現場の管理責任者がそれぞれの責任範囲に応じてモニタリングするための『ダッシュボード』を提供します（[図4]［図5]）。

［図4］経営者向けダッシュボード（例）

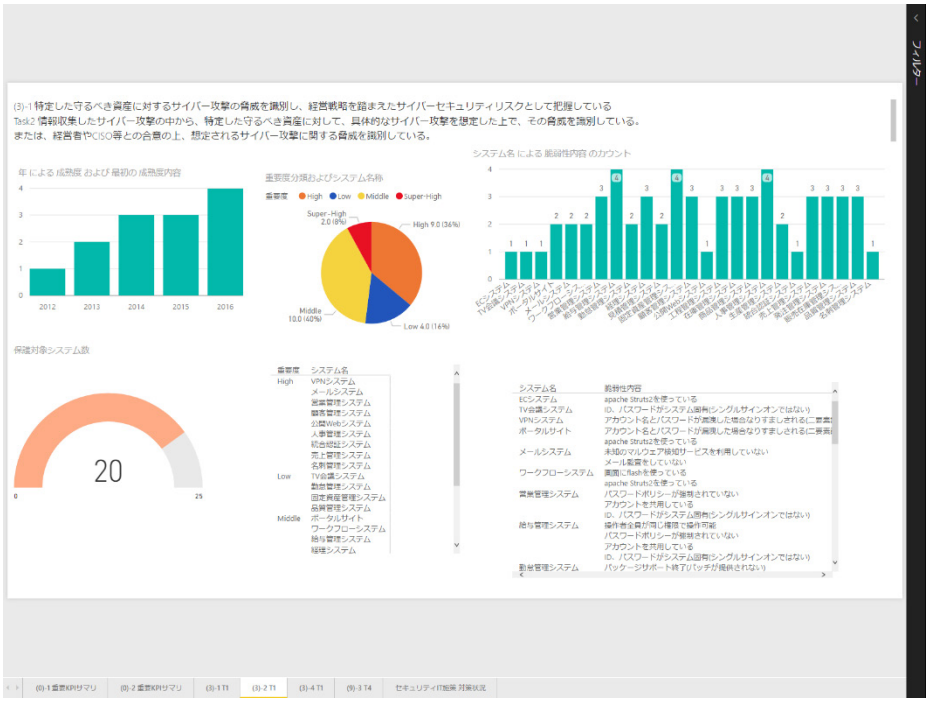


［図5］CISO向けダッシュボード（例）

「サイバーインテリジェントプラットフォーム」の『ダッシュボード』によりサイバーセキュリティ管理活動を可視化し、経営者は、定量的または定性的にモニタリングすることで、サイバーセキュリティへの投資や推進活動が効果を発揮しているかどうかを評価することが可能です。加えて、経営者やCISOが意思決定を行うために必要な情報を迅速に提供することで、サイバーセキュリティ経営の推進を支援し、さらには対外的な説明責任を果たすことを強力に支援するツールになり得ます。

『ダッシュボード』は、経営者やCISOが必要な情報をサマリーし、提供するとともに、そのサマリー情報からさらに詳しい詳細レポートを確認することができます（[図6]）。

［図6］ダッシュボードからリンクされる詳細レポート（例）



4. サイバーインテリジェントプラットフォームの活用方法

4-1 マネジメント基盤

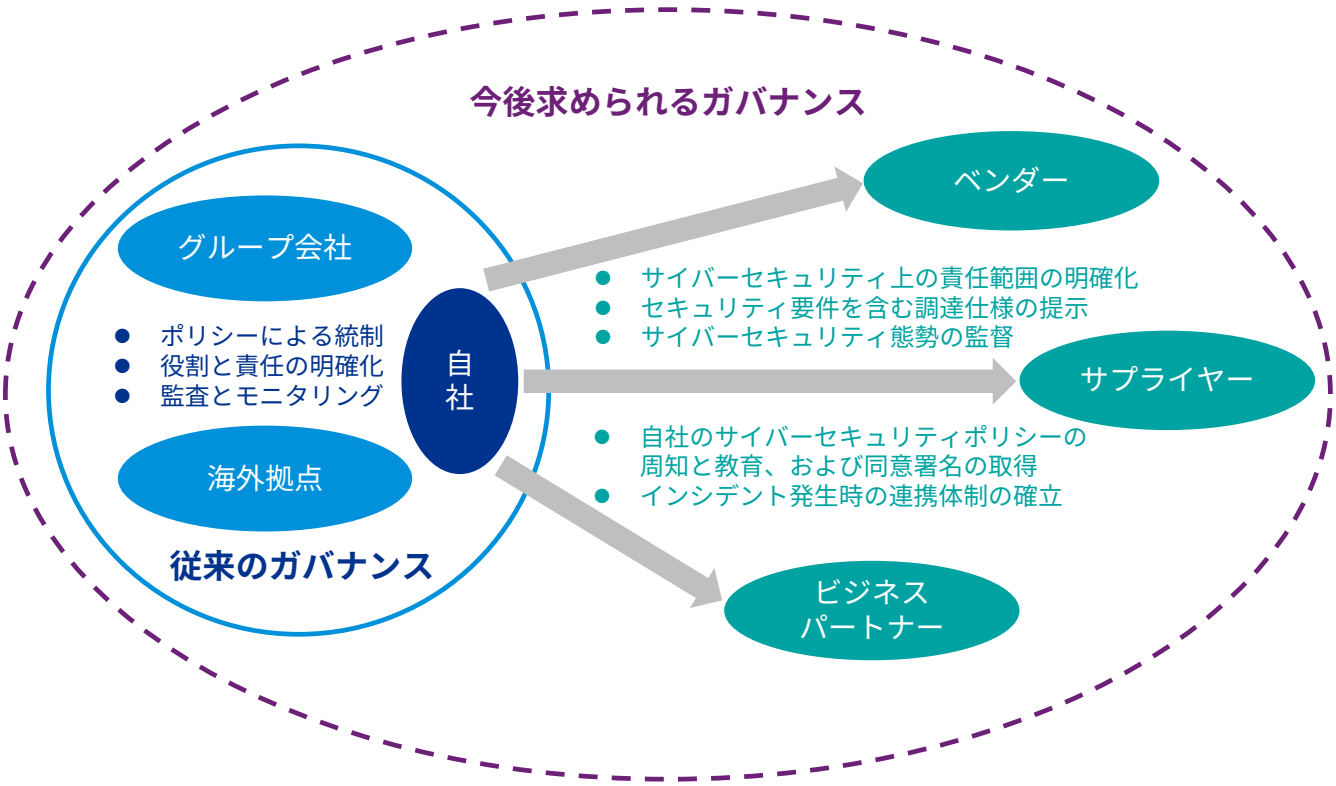
4-1-1 リーダーシップとガバナンス

サイバーセキュリティポリシーは、組織におけるサイバーセキュリティ対策と管理において、“誰が”、“何を”、“どこまで”すべきかという判断や意思決定を行う上での拠り所となり、従業員の行動指針ともなり得るものです。

経営者は、ビジネス戦略と整合するサイバーセキュリティポリシーを定め、CISOを任命し、自社のサイバーセキュリティ態勢の維持強化のために適切な投資を行うことでリーダーシップを発揮する必要があります。

今日、インターネットのみならず、ビッグデータ、AI（人工知能）、IoT（モノのインターネット）といった技術革新や、ビジネスの多様化・国際化によって、子会社や海外拠点だけでなく、サプライヤー、ビジネスパートナー、顧客、消費者など、さまざまな事業体や個人が組織のネットワークと繋がり、さまざまなデータを授受しています。組織内部の取組みだけでは、セキュリティリスクへの対応が充分であるとは言えません。ある企業では業務委託先の従業員がイントラネットワークに接続して不正にデータをダウンロードし、外部に持ち出して漏洩するという事件が発生しました。企業は、組織を取り巻くサプライチェーン全体のセキュリティリスクを考慮し、適切に統制していくことが求められていると言えます。

［図7］必要なガバナンス



「サイバーインテリジェントプラットフォーム」は、経営者が求められるリーダーシップとガバナンスを推進するために、サイバーセキュリティポリシーの策定からグローバル組織統制、サプライチェーン管理支援、CISOの活動補佐などを提供します。

これらの管理活動が期待通りに実行されていることを確認するためのKPIとしては、一定の頻度で経営会議においてサイバーセキュリティリスクや対応方針に関する議論が行われているか、サイバーセキュリティポリシーを浸透させるための教育を定期的に実施しているか、組織が関係を持っているビジネスパートナーを把握しそのうち深刻なサイバーリスクにつながる可能性のある事業者に対して定期的なサイバーセキュリティ監査を実行できているか、などが挙げられます。

4-1-2 PDCAサイクル

ビジネス環境は常に変化し、経営者が企業の持続的成長に必要な戦略の立案と実行を半永久的に求められるのと同様に、サイバーリスク環境も常に変化し続けています。組織にとってサイバーセキュリティとは終わりのない取組みであり、PDCAサイクルを通じて改善を続けていくべきものです。

有限な経営資源の中から必要最小限の投資で効率的にサイバーセキュリティ施策を推進していくためには、経営者が組織にとってのサイバーリスクを的確に把握し、事業への影響に基づいて優先度に応じた投資の意思決定をする必要があります。経営資源を投下し、サイバーセキュリティ施策を策定したが、その効果を最大限に発揮されるために、サイバーセキュリティポリシーに沿った適切な運用が行われていることを客観的に監査することも、対策の形骸化を防ぐためには不可欠です。

ITシステムにおけるサイバーセキュリティ対策への投資にも限界がある中、技術的な対策だけで従業員の故意や過失による不正を防止することは困難です。組織が効率的にサイバーセキュリティの対応水準を高めるためには、従業員が日常的にサイバーリスクを意識して業務にあたるなど、人的なレベルの向上が求められます。経営者は組織のサステナビリティという観点でもサイバーセキュリティ対策が欠かせない取組みであり、従業員に対するサイバーセキュリティポリシーの遵守と浸透を促し意識を向上させるために、組織のサイバーセキュリティ成熟度を高めるための教育を推進すべきです。

「サイバーインテリジェントプラットフォーム」は、経営者がサイバーリスクを的確に把握して意思決定を行うための判断材料となるアセスメントの実施、ビジネスインパクトに応じた施策の優先度付けと実行ロードマップの策定、施策実行後の運用状況に対する監査、従業員のサイバーセキュリティ意識向上のための教育といった一連のサイバーセキュリティ管理活動に関するPDCAサイクルの導入と実践を支援します。

経営者は、こうしたPDCAサイクルを適切に機能させるためのモニタリングを行うにあたり、サイバーリスクアセスメントによって洗い出されたリスクの数と深刻度具合、またそれらが前回の確認時と比較してどの程度低減されているか、そのためにどの程度の経営資源が投入されたか、またサイバーセキュリティ監査による指摘事項の数がどのように推移しているか、従業員によるサイバーセキュリティ教育の受講率や内容の理解度はどの程度か、などについてKPIを使用したダッシュボードを通じてモニタリングすることが可能です。

4-2 オペレーション基盤

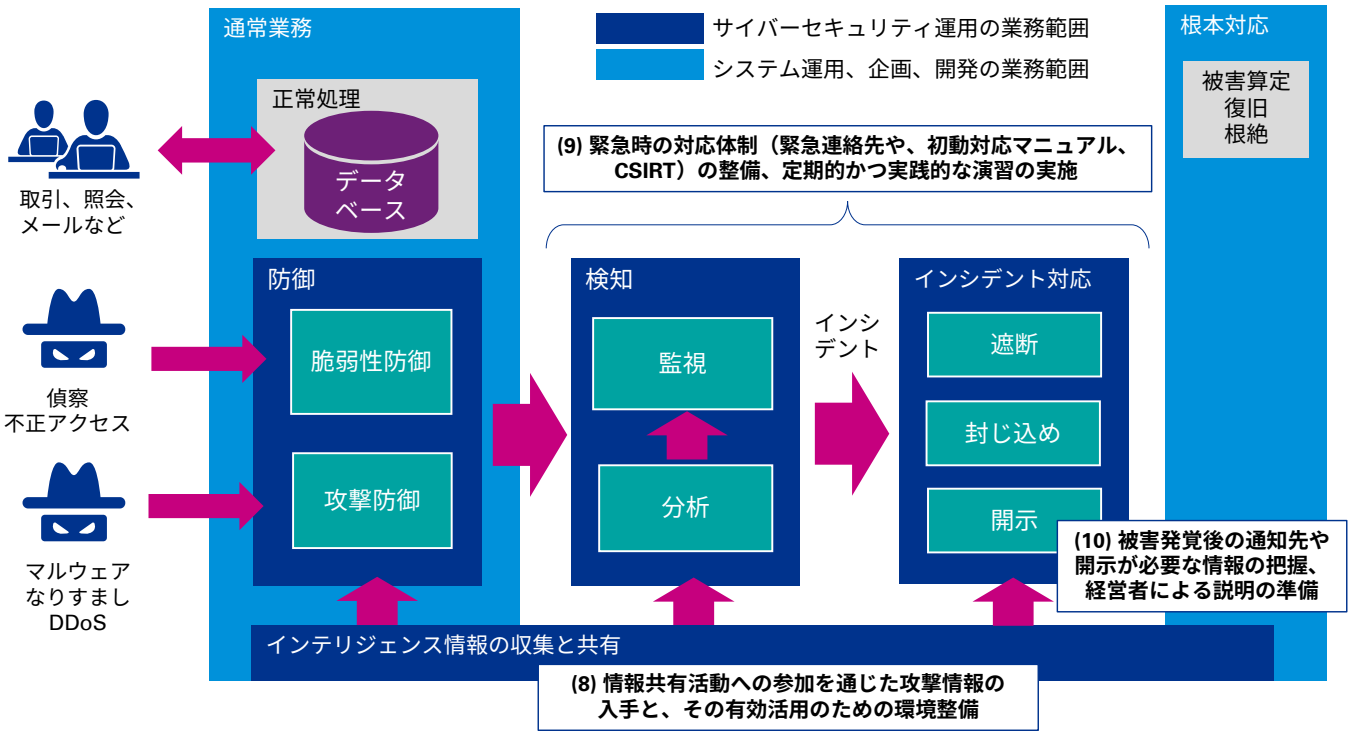
サイバーセキュリティ経営の重要10項目における⑧～⑩項目は、サイバーセキュリティ対策の企画、開発段階からみて、想定外に進化した手口の攻撃や、許容したリスクへの攻撃の監視、およびインシデント対応を求めています。

オペレーション基盤とは、このような「サイバーセキュリティ経営ガイドライン」の要求事項を充たす、セキュリティインシデント対応の業務や組織、システムなどを指します。

オペレーション基盤の主たる業務は、通常業務の攻撃防御の状況管理と、セキュリティインシデントの判別、封じ込めたサイバーセキュリティインシデントに対する抜本的な対応を企画し、開発部門へ引継ぐことです。

正常通信を処理する通常業務と、SOCおよびCSIRT業務間の一連のつながりは［図8］に概要を示します。

［図8］業務関連図



［表4］業務関連図補足

業務	内容
脆弱性防御	システム毎の脆弱性の深刻度別に管理する
攻撃防御	サイバー攻撃のブロック件数などを管理する
監視	セキュリティ機器のログを一元管理して、通信の状況を監視する
分析	過去ログなどを利用した遡及分析を行う
遮断	セキュリティインシデントが発生した当該機器の即時遮断
封じ込め	セキュリティインシデントの暫定対策による防御力の強化
開示	観測したセキュリティインシデント情報の外部公表
インテリジェンス情報の収集と共有	外部の脅威情報、自社への攻撃情報などを把握し、防御力や検知力の強化に活用する

「サイバーインテリジェントプラットフォーム」は、防御、検知、インシデント対応など個々の業務の状況を可視化します。

4-2-1 通常業務

サイバー攻撃には、不正アクセスなど脆弱性を突いて侵入を試みるものやDDoS（分散型サービス拒否攻撃）など、システム環境の特徴を攻撃するものなどがあります。本ホワイトペーパーではサイバー攻撃を以下の5種類に分類しています。

［表5］サイバー攻撃の分類

分類	内容
偵察	スキャンなどによる攻撃対象候補への調査用通信など
不正アクセス	公開ウェブサービスなどの脆弱性を利用した侵入や任意のコード実行など。大部分が情報窃取を目的としている
マルウェア	悪意あるコードを何らかの方法で送付する攻撃。目的は情報窃取、業務妨害、遠隔操作など
なりすまし	公開ウェブサービスの認証突破による侵入など
DDoS	通信や処理の過負荷を狙った大量通信による、業務妨害を目的とした攻撃

これらのサイバー攻撃は常時、ファイアウォール、IPS、プロキシ、マルウェア対策ソフトなどの攻撃防御の対策によって抑止されており、防御状況はログなどで管理することができます。セキュリティインシデントの発生有無を判定するためには、まず初めにこれらの機器が発するアラートを管理する必要があります。

また、システムの本番リリース後に判明した脆弱性に対する対応も、通常業務のサイクルの中に組み込んで実施しなければなりません。本番リリース後に判明した脆弱性情報を収集し、IT資産管理台帳に基づいた脆弱性評価と適切なパッチ適用によって、サイバー攻撃へのセキュリティ強度を維持します。

「サイバーインテリジェントプラットフォーム」は、通常時のセキュリティ運用の位置付けで、システム毎の攻撃推移の統計や、システム毎の脆弱性の管理状況を可視化します。

4-2-2 SOC／CSIRT業務

経営者がセキュリティ運用に対してまず初めに関心を持つのが、自社でセキュリティインシデントが起きているのか？です。

SOCやCSIRTは、経営者への報告においてサイバーセキュリティ経営の重要10項目の⑨に記載された「インシデントの検知」、「インシデント対応」や、「セキュリティ運用の状況把握」、「インテリジェンス情報の集約」などを行います。

「インシデントの検知」は、SIEM（Security Information and Event Management）ツールなどが発するアラートをさらに深堀りする「監視」や、影響範囲を特定する「ログの分析」によって、インシデントの全体像を明確化します。

「監視」は、セキュリティインシデントの発生有無を判定する業務であり、セキュリティ機器が発する複数の警告の相関関係やインテリジェンス情報との組み合せを分析し、単体のセキュリティ機器をすり抜けたサイバー攻撃を識別します。また、関係各部との情報共有などによって、システム障害とセキュリティインシデントの切り分けを行います。

「ログの分析」とは、発生したインシデントの影響範囲を特定する遡及分析を指します。

SOCやCSIRTは、経営者と緊密に連絡をとりながら、警察などの要請で実施する数ヵ月間に跨る過去日付のアクセス履歴の調査や、マルウェアを検知したPCが所属する部門全体の影響範囲調査などを実施します。

サイバーセキュリティ」経営の重要10項目の⑧にもある通り、このような監視、ログ分析業務を実施するためには、社内で検知したサイバー攻撃や、公的機関や業界団体などから提供される各種インジケータの管理が重要です。SOCやCSIRTは、情報収集、台帳管理、予防を含む情報の有効活用などを実施し、かつ、経営者からの問合せに、情報管理者の立場から最新の状況を迅速に回答する必要があります。

「監視」と「ログ分析」を実施するためには、集積した膨大なログデータベースに対するリアルタイム処理が必須となりますので、手動でのログ管理は困難です。エンタープライズ環境では、SIEMツールによるログ管理とMSS（Managed Security Service）など外部リソースの有効活用を検討することになります。

経営者のセキュリティ運用に対する2つ目の関心事は、発生したセキュリティインシデントの被害内容と外部公表の必要性判断です。

「インシデント対応」は、この関心事に応える業務で、判定されたセキュリティインシデントの「遮断」や「封じ込め」、「開示」などを行います。

「遮断」は、被害規模を極小化する封じ込めの一種で、セキュリティインシデントを起こしたPCの抜線や通信の遮断などを指します。

「封じ込め」は、当該のサイバー攻撃を抑止する攻撃防御の強化を指し、パッチやシグネチャの適用など、攻撃防御力を強化するさまざまな対応を実施します。

また、サイバーセキュリティ経営の重要10項目の⑩に則り、検知から封じ込めまでの間に、事前に設定した基準に基づく「開示」可否の判断が最低限必要となります。

「インシデントの検知」、「インシデント対応」は、さまざまな立場の関係者の深い知見を迅速に有する業務です。円滑なインシデント対応には、インシデント初動対応マニュアルの整理、緊急連絡先体制図の整理、手順に基づいた事前訓練の実施など、周到な事前準備が重要となります。訓練には、経営陣による開示などを含みます。

「サイバーインテリジェントプラットフォーム」は、SOCやCSIRT業務におけるインシデント管理状況を可視化します。インシデント初動対応マニュアルや緊急連絡先体制図、SIEMやMSSの導入、訓練、インテリジェンス情報の管理などは個別コンサルティングで対応します。

5. サイバーインテリジェントプラットフォームの高度な活用

第4章までサイバーセキュリティ経営を実現するための課題に対して、サイバーインテリジェントプラットフォームの有効性、活用方法について述べてきました。本章では将来実現させることを検討している、「サイバーインテリジェントプラットフォーム」のさらなる活用について説明します。

さらなる活用とは端的に言うと、“リスク可視化情報を業務可視化へ活用する”という「戦略投資」です。

5-1 生産性向上

セキュリティと並んで今の日本において、経営者の責任で推進すべき重要事項がもう1つあります。それは“自社の生産性向上”です。

日本の今後の生産年齢人口を考えると“労働力の維持”は必要です。しかし、それは日本の労働総量の低下緩和のためであり、個人や企業の生産性を高めることには繋がりません。今、企業にとって本当に必要なのは、短時間で質の高いアウトプットを生み出すことができる“働き方の質の改善”です。

それでは、生産性を向上させるためにはどうすればよいのでしょうか。

$$\text{生産性} = \frac{\text{仕事の質} \times \text{量}}{\text{時間}}$$

生産性は労働時間当たりの付加価値であり、上記の方程式で表現されます。よって生産性を高めるには分母（時間）を小さくするか、分子（質と量）を大きくすることが求められます。

5-2 ワークスタイル変革

前述の通り、生産性を向上させるためのアプローチとして、分子である「仕事の質」と「量」、つまりは“付加価値”を高める方法があります。

ここでいうワークスタイル変革とは、自分自身の働き方を変えることであり、たとえば、生産性が高い他者の働き方を見習い、取り入れることなどが考えられます。

統合ログ管理製品を販売する日本のメーカーが実施した行動分析では、メール処理や資料作成時間などのPC操作ログ、会議や顧客訪問などのスケジュールからの動線などをインプットしたところ、ほとんどの行動が1：9の割合程度でグルーピングされ、また、少数派に分類される1のグループは他者とは異なったアクションで結果を出すケースもある、という結果となりました。

高い付加価値を生み出す従業員の行動パターンを分析および社内で共有することで、組織的・個人的な活動を変えることで生産性の向上に寄与すると考えられます。

サイバーインテリジェントプラットフォームにおいても、収集したIT活用状況のビッグデータと業務プロセス情報、社内満足度といった事業や経営のスコアカードを相関分析することで、業務効率性向上について繋げられると考えています。

5-3 モチベーションの向上

PC操作ログによる作業の可視化や動線の明確化などを進める場合、「必要以上に監視されている」と感じる従業員が出てくることもあります。

しかし、セキュリティ面で考えると『あなたを守るための証跡である（インシデントがあったときに潔白を証明する）』こと、そして、『あなたの働き方を可視化することで、効率的にワークスタイル変革ができ、そのことが個人の幸せと会社での成果を両立することにつながる』ことを社員に対して啓蒙することで、社員のモチベーション向上につなげることができるのではないかと考えます。

KPMGコンサルティング株式会社

小川 真毅
ディレクター

稲村 大介
マネジャー

株式会社ラック

内田 昌宏
常務理事

槻山 幸司
理事

岩城 裕嗣
コンサルタント

KPMGコンサルティング株式会社

〒100-0004
東京都千代田区大手町1丁目9番5号
大手町フィナンシャルシティ　ノースタワー
TEL ：03-3548-5111
FAX : 03-3548-5114

kc-cybersecurity@jp.kpmg.com

kpmg.com/jp/kc

株式会社ラック

〒102-0093
東京都千代田区平河町2丁目16番1号
平河町森タワー
TEL ：03-6757-0100

cip@lac.co.jp

www.lac.co.jp