KPMG

KPMG Insight

KPMG Newsletter

Vol.18

May 2016

経営トピック④

サイバー イン ザ ボードルーム

kpmg.com/jp

サイバー イン ザ ボードルーム

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

昨今、標的型攻撃に代表されるサイバー攻撃の発生が急増するなか、実際に攻撃を受けた企業もますます増加しており、経営者はサイバーリスク対応に関する意思決定を迫られると同時に、ステークホルダーに対する説明責任も求められています。
攻撃発生の予測が難しく、攻撃側が圧倒的に有利とされるサイバーセキュリティ領域において、限られた経営資源を効果的に投入してリスク低減を図るためには、経営者とボードメンバーが自社におけるサイバーリスクとその対策状況について、的確かつタイムリーに把握する必要があります。
本稿では、経営層によるサイバーリスクにかかわる意思決定とステークホルダー対応を支援する、インテリジェントツールとしての「サイバーセキュリティ経営ダッシュボード」の構築と、その活用による効果的なサイバーセキュリティマネジメント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年における標的型攻撃の警察への報告件数は過去最高を記録したが、経営会議でサイバーセキュリティについて議論している企業は未だ3割程度にとどまっている。
- 常に変化するサイバーリスク環境において迅速かつ適切な意思決定を行うためには、経営者が自社におけるサイバーセキュリティ対策状況をタイムリーに把握するための仕組みが必要である。
- 「サイバーセキュリティ経営ダッシュボード」は、自社を取り巻く最新のサイバー脅威に対する現在の対策状況について、KPIを通じて簡潔かつ直感的に理解し、投資対効果の評価と、次なる打ち手に関する意思決定を支援する強力なインテリジェントツールとして活用が期待される。

I. サイバー脅威の現状と転換

2016年3月30日、衆議院第一会館にて「サイバーセキュリティ×経営 シンポジウム」が開催されました。このシンポジウムのサブタイトルは、「サーバールームから役員室への転換」とされており、まさにサイバーセキュリティが情報システム部門だけの課題ではなく、経営者とボードメンバーがイニシアチブを執って推進すべき「ボードアジェンダ」としての取組みへと、その転換期を迎えていることがうかがえます。

1. 標的型攻撃の猛威

2016年3月17日に警察庁が発表した資料[1]によると、平成27年（2015年）中に警察が報告を受けた標的型メール攻撃は3,828件と過去最多を記録しました（**図表1**参照）。この件数は、昨年の2倍以上、一昨年の7倍以上となっており、標的型攻撃が急増しています。

数年前までは日本語の標的型メールの文面が不自然であったり、リンクをクリックした際に接続される指令サーバーが海外であったりするなど、その攻撃手法は比較的見破りやすく、検知も容易でした。しかし、昨年に起きたある行政機関における標的型攻撃被害にも代表されるように、日本の組織や企業を狙った、標的型メールが巧妙に作り込まれるようになり、指令サーバーも国内に配置することで怪しまれないように周到に準備されるなど、単純な攻撃件数の増加というだけではすまないほどに、その脅威は増しています。

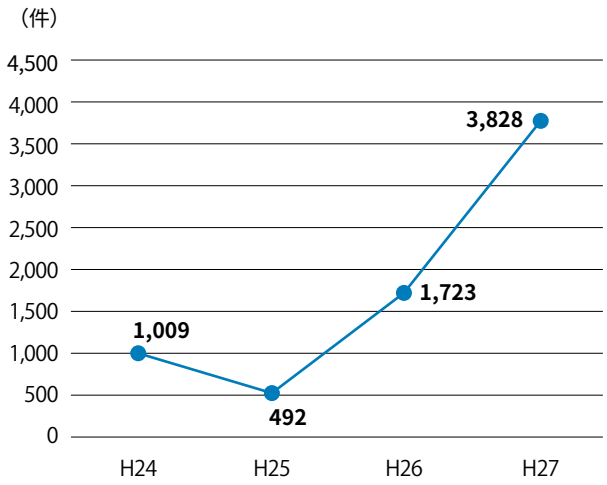
また、偶然にも警察庁と同日にJIPDECとITRが発表した共同調査結果[2]によると、2015年中に標的型サイバー攻撃を経験した企業は9.5%であり（**図表2**参照）、およそ10社に1社の割合で標的型攻撃を実際に受けたことになります。この割合も一昨年の6.7%から年を追うごとに増加しており、サイバーリスクの拡大を実感し始めている企業経営者も増えていると考えられます。

2. ボードメンバーによるサイバーセキュリティ討議

一方、2016年3月24日に日本情報システム・ユーザー協会が発表した資料[3]によると、ボードメンバーが経営会議でセキュリティについて審議・報告している企業は約3割程度にとどまっており、標的型攻撃の猛威とは裏腹に企業経営者のイニシアチブによる対策推進が十分に行われているとは言い難い状況にあります（**図表3**参照）。

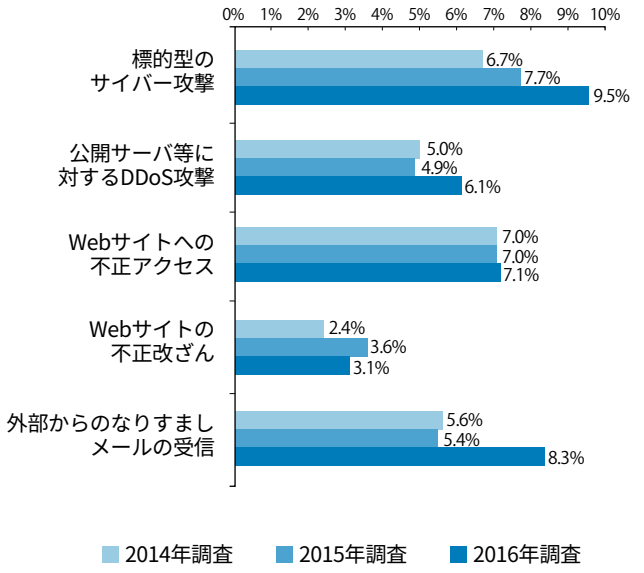
こうした状況も鑑みて、経済産業省は昨年12月に経営者向け

【図表1　警察庁が報告を受けた標的型攻撃件数の推移】



出典：警察庁「平成27年におけるサイバー空間をめぐる脅威の情勢について」

【図表2　過去１年間に経験した外部攻撃に関わるセキュリティ・インシデントの経年比較】



出典：JIPDEC ／ ITR「企業 IT 利活用動向調査 2016」

1 「平成27年におけるサイバー空間をめぐる脅威の情勢について」（警察庁　2016年3月17日）
https://www.npa.go.jp/kanbou/cybersecurity/H27_jousei.pdf
2 「サイバー攻撃の認知率とリスク重視度が上昇　マイナンバー制度対応は前進するも、多くの企業は道半ば― JIPDECとITRが「企業IT利活用動向調査2016」の速報結果を発表 ―」（一般財団法人日本情報経済社会推進協会（JIPDEC）、株式会社アイ・ティ・アール　2016年3月17日）
http://www.jipdec.or.jp/topics/news/u71kba0000004gf8-att/20160317.pdf
3 プレスリリース「『企業 IT 動向調査2016』（情報セキュリティ）の速報値を発表」（一般社団法人 日本情報システム・ユーザー協会　2016年3月24日）
http://www.juas.or.jp/servey/it16/it16_security.pdf

の「サイバーセキュリティ経営ガイドライン」[4]を発行し、策定に携わった関係者が各所でこれをテーマとした講演や解説セミナーを実施するなど、まさに国策として企業経営者によるサイバーセキュリティ対策への積極的取組みを促しており、今後徐々に意識付けが図られていくものと期待されます。

3. ステークホルダーに対する説明責任

サイバーリスクは経営者や企業だけの関心事ではありません。企業がサイバー攻撃を受けた際に直接または間接的に影響を受ける株主、顧客、ビジネスパートナー、サプライヤー、関係当局、社会等においても昨今のサイバーリスク増大に対する危機意識は高まっており、こうしたステークホルダーに対する説明責任を果たすことも、企業や経営者にとって重要なミッションとなっています。

そのため、サイバー攻撃による事件や事故が発生する度に、たとえ自社に一切影響がないとしても、「御社では、今回○○社で発生したようなサイバー攻撃への対策は採られていますか？」というステークホルダーからの質問が投げかけられることとなり、このような問いかけに即座に回答できるように、日常的に自社を取り巻くサイバーリスク環境とその対策状況について、経営者は理解しておく必要があります。

Ⅱ. サイバーリスクの把握とダッシュボードの活用

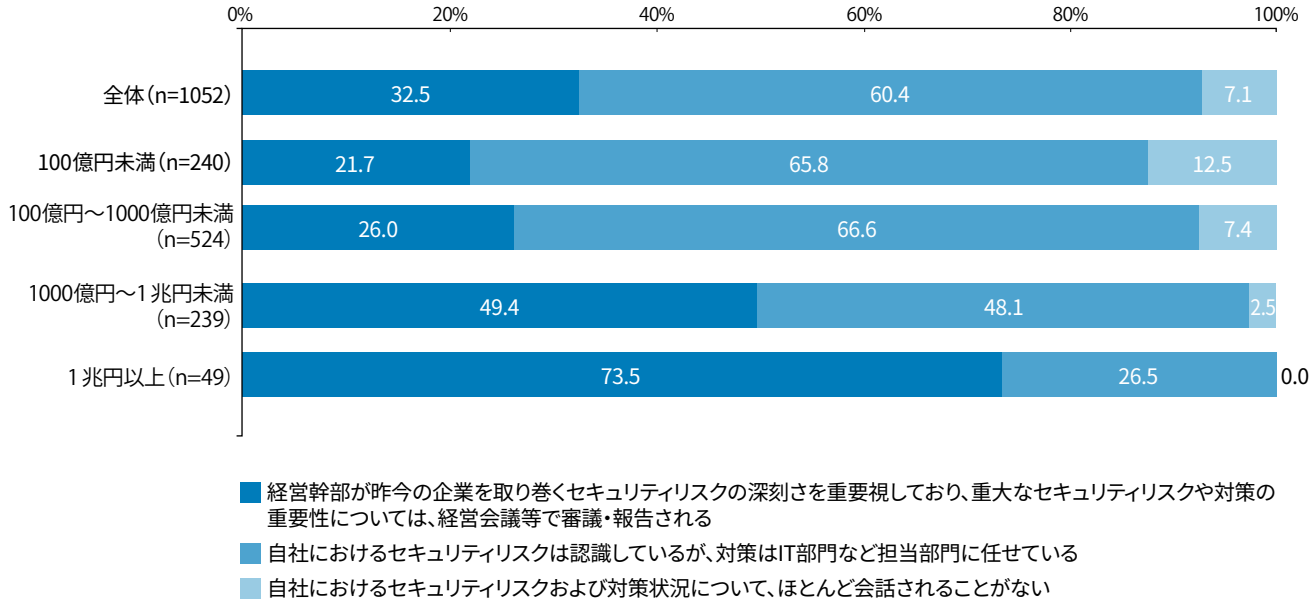
企業の基幹インフラとしてITシステムの活用が進むにつれ、2005年頃からは経営者を支援するBI（Business Intelligence：ビジネスインテリジェンス）ツールによる「見える化」ブームが起き、企業の経営者が意思決定や経営判断を行う際に必要な経営指標について、あたかも自動車のダッシュボードのように数値やグラフなどで視覚的に整理された「経営ダッシュボード」が耳目を集めるようになりました。

本章では、当時から10年以上が経過した今、テーマを「サイバーセキュリティ」に変えて、再びこの「経営ダッシュボード」を活用することの意義と方法論について解説します。

1. サイバーリスクの把握と意思決定

ステークホルダーへの説明責任という対外的コミュニケーションに加え、企業の経営者およびボードメンバーは刻々と変化するサイバーリスクへの対策を推進するための意思決定が求められます。的確かつ迅速な意思決定を行うためにも、自社におけるサイバーリスク環境とその対策状況を、経営者やボードメンバーが理解できるような仕組みづくりが不可欠です。

【図表3　経営幹部のセキュリティリスクに対する関わり方】



出典：一般社団法人 日本情報システム・ユーザー協会「企業 IT 動向調査 2016」プレスリリース

4 「サイバーセキュリティ経営ガイドラインver.1.0」（経済産業省、独立行政法人 情報処理推進機構）
http://www.meti.go.jp/press/2015/12/20151228002/20151228002-2.pdf

一口にサイバーリスクを把握すると言っても、ウイルス対策やファイアウォールなどを実装していれば、ほとんどの攻撃を防ぐことができていた十数年前とは違い、今は、一見何の変哲もないコミュニケーションを通じて心理的な弱点を突く標的型メールのような攻撃や、自社ネットワークにアクセスできるサードパーティベンダーによる不正な情報の持ち出しなどは、もはや単純にテクノロジーだけで解決できるリスクではなくなっています。

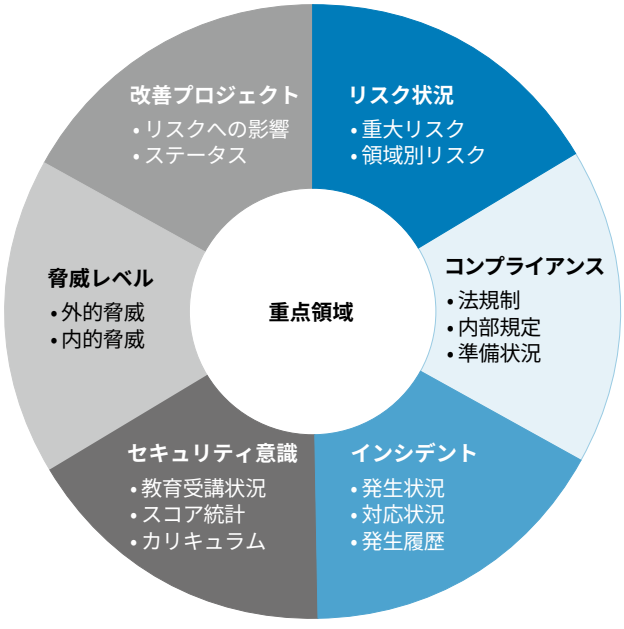
実際にサイバーリスクへ対応するには、従来からその中心的役割を果たしてきた情報システム部門だけではなく、人事、法務、広報、営業等、サイバーセキュリティ対策の管轄範囲やステークホルダーとの関係性によって関与する事業部が多岐にわたることに加え、国内外の営業拠点や生産設備等も考慮に入れ、組織にとってのリスクを網羅的かつ効率的に把握しなければなりません。

さらに、いまやサイバーセキュリティ対策は様々な領域において専門的かつ高度なものとなっているため、各担当部門から経営者が報告を受けたとしても、それが組織のビジネスにとってどれほどのリスクであるのか、対策は十分なのか、追加の打ち手は必要か、といった意思決定を行うための明確な判断材料とはならない場合があります。

2. サイバーセキュリティ経営ダッシュボード

こうした課題を踏まえ、経営者およびボードメンバーが専門的かつ多岐にわたるサイバーリスクを効果的に把握するために

【図表4　サイバーセキュリティ経営における6つの重点領域】



は、KPI（Key Performance Indicator）などの明確な指標を用い、サイバーセキュリティ対策領域ごとにその実装および管理状況を直感的に捉えることが有効な手段の1つであると考えられます。

（1）サイバーセキュリティ経営の重点領域

経営手法に決まった型式がないのと同様に、経営者やボードメンバーが抱くサイバーリスクに対する意識は千差万別であり、その管理における重点領域もまた多様であることは想像に難くありません。

そこでKPMGでは、経営者やボードメンバーとのディスカッションを通じ、多くの組織において共通する課題や重視すべき事項を、6つのサイバーセキュリティ管理領域から構成されるフレームワークで整理しました（**図表4**参照）。

① リスク状況

経営者は、今、組織にとってどのようなサイバーリスクがあるか、深刻度の高いものを優先的に認識するとともに、全体的な対応状況についても把握する必要があります。経営戦略とリスクマネジメントは密接に関係するものであり、サイバーリスクに対して適切な戦略方針を打ち出すことは経営者の責任でもあ

【図表5　リスク状況に関するダッシュボードの例】

リスク概要	深刻度	トレンド	詳細／対応状況
R1: 知的財産の喪失	Very High	New	既存システムでは管理者権限に対するアクセス制御が十分ではない。 システム改修のための分析を実行中。
R2: 顧客情報の不正開示	Medium	↓	顧客情報インベントリが現状80%。 インベントリ済みのレポジトリについてはコンプライアンスに準拠している。
R3: オンラインセールスチャネルの停止	High	→	ペネトレーションテストの結果、環境設定において深刻な脆弱性が発見された。 改修計画を検討中。
R8: 機密情報の漏えい	Very High	↑	新規ビジネス企画プロジェクトが発足。 IT環境の整備とセキュリティ意識向上トレーニングを実施中。
R7: 会計不正	Medium	→	監査指摘事項として、会計システム管理プロセス上の不備が発見された。 手順の改定準備中。

ります。

経営者にとって効果的にリスク状況を把握するためには、網羅的なリスクの洗い出しと、明確な指標に基づく深刻度の割り当てが不可欠であり、サイバーリスクを適切に評価するためのアセスメントフレームワークと、評価の実施体制をあらかじめ確立しておく必要があることは言うまでもありません（**図表5**参照）。

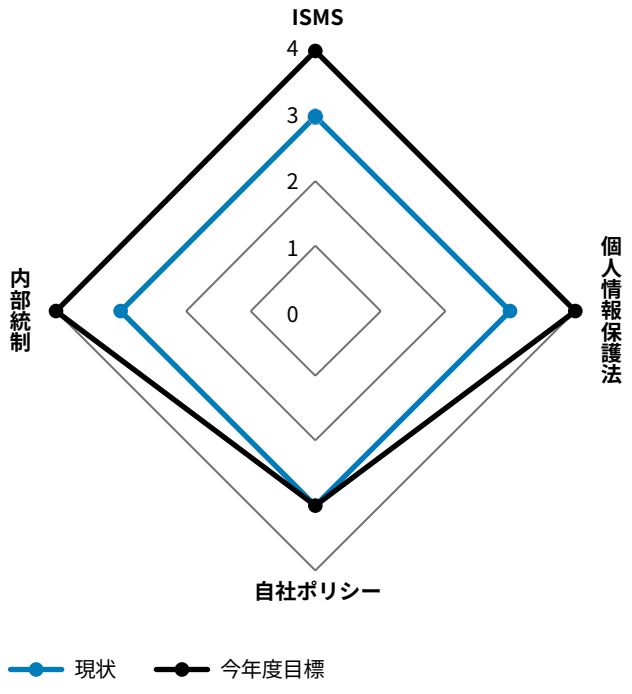
② コンプライアンス

経営者の関心事の1つとして、自社の事業活動がサイバーセキュリティに関する法律や業界規制に準拠しているか、および内部で規定されたフレームワークに即しているかという点があります。

実際に、コンプライアンスが契機となってサイバーセキュリティ対策を加速させた企業も少なからずあり、特に当局や取引先、顧客等の要請からこうした取組みを推進することは事業戦略の一環でもあると言えます。裏を返せば、法規制や顧客からの契約上の要求に違反することは、罰金、契約の打ち切り、信頼関係の破たんなどに繋がり、経営戦略上の重大な問題となります。

法規制や顧客からの要請は、政治、経済、市場環境の変化に伴い、新たなコンプライアンスが必要になるケースや、コンプライアンス要件が変化することもあるため、経営者は自社の状況を常に把握しておかなければなりません（**図表6**参照）。

【図表6　コンプライアンスに関するダッシュボードの例】



③ インシデント

セキュリティ・インシデントの発生状況とその原因、対応状況やビジネスへの影響は経営者とステークホルダーにとっての重大な関心事です。

インシデントの発生数、影響度合い、発生源等に関する統計や、同業他社のベンチマーク、インシデント検知や対応に要した時間といったインシデント管理プロセスの効果が、観察すべき主な指標と言えます（**図表7**参照）。

【図表7　インシデントに関するダッシュボードの例】

分類	発生数	想定インパクト	発生源	トレンド
ハッキング	2	10－20億	外部	↑
マルウェア	3	100 - 1,000万	サードパーティ	↓
ソーシャル	-	-	-	→
不正	1	1－2億	内部	↑
物理	-	-	-	→
エラー	-	-	-	↓

④ セキュリティ意識

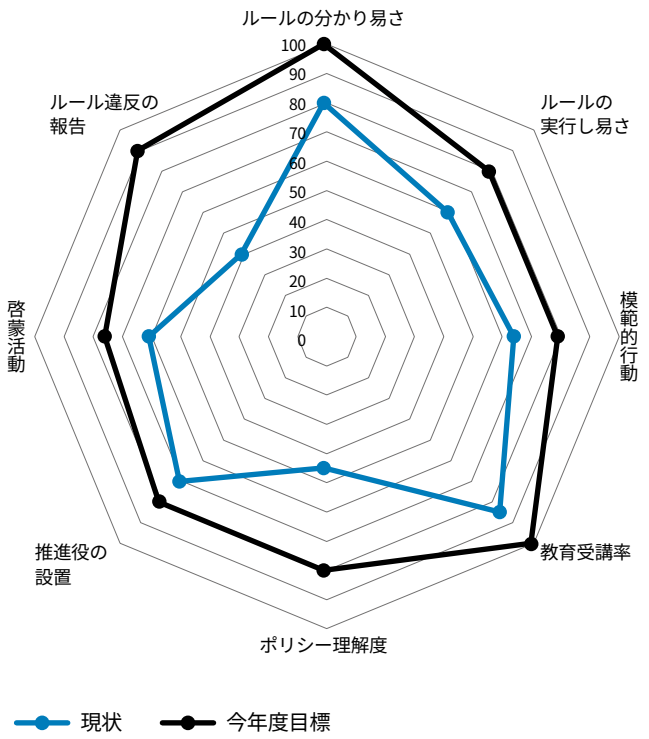
人の心理的な弱点や盲点を悪用する標的型攻撃の成否は、従業員一人ひとりのセキュリティ意識に懸かっていると言っても過言ではありません。サイバーセキュリティに関する意識向上の目的は、組織の情報資産を取り扱う従業員、取引先、その他関係者が意識的にその保護に取り組むようにすることであり、それによってヒューマンエラーを防止し、インシデントの発見に繋げることができます。

人の意識的水準や理解度、サイバーセキュリティにかかわる事象が発生した際に期待される行動について、正確かつ明確に測る簡便な指標はないため、KPMGでは8つの観点を多面的に組み合わせてセキュリティ意識を評価する方法を推奨しています（**図表8**参照）。

⑤ 脅威レベル

組織を取り巻くサイバー脅威を把握することは、今後生じ得るサイバーリスクを予見し、先行して対策を採るために不可欠です。この領域はサイバーインテリジェンスと呼ばれ、この活

【図表8　セキュリティ意識に関するダッシュボードの例】



動が充実しているほど、組織はより早く的確なサイバーセキュリティ対策が推進できる環境にあると言えます。

サイバーインテリジェンスとは、国家間の情勢、活動家や犯罪組織の動向、同業他社の状況、内部不正の兆候等、様々な情報を内外の情報源から集積し、解析することで、サイバーセキュリティ上の示唆を得る活動を指します（**図表9**参照）。

⑥ セキュリティ改善プロジェクト

経営者は、現在進行中の主要なサイバーセキュリティ関連プロジェクトの進捗や概況を把握し、ステークホルダーに最新の取組みについて説明できなければなりません。

さらに、経営者をはじめとしたボードメンバーは、これらのプロジェクトが管轄するビジネスに及ぼす影響を理解し、意思

【図表9　脅威レベルに関するダッシュボードの例】

分類	脅威レベル	ゲージ
ハクティビスト	3	
ハッカー集団	2	
犯罪組織	4	
国家間紛争	1	
産業スパイ	3	
サードパーティ	5	
内部不正	2	

決定を行う際に所与の条件として考慮する必要があります（**図表10**参照）。

（2）ダッシュボード構築プロセス

実際にダッシュボードを構築するためには、大きく分けて2つのステージで構成されるプロセスを経る必要があります。1つ目は、ダッシュボードで報告すべき要素とその内容を定義することであり、2つ目は、それを実現するための仕組みの実装と組織の活動への組み込みです。各ステージは、さらに細分化されたフェーズに分解することができます（**図表11**参照）。

① 初期設計

初めに、ダッシュボードを利用するステークホルダーを特定し、そのステークホルダーによる組織のサイバーセキュリティ環境に対する関心事を洗い出します。

その結果、自ずとダッシュボードでどのような領域の活動状況を示すべきかというラフスケッチが上がり、大まかなKPIをリストアップすることができます。通常、こうした洗い出しは、ステークホルダーの意向を可能な限り正確に把握するためにも、ワークショップ形式でのインタラクティブなディスカッショ

【図表10　セキュリティ改善プロジェクトに関するダッシュボードの例】

プロジェクト	リージョン	予算	進捗	ビジネスインパクト	完了予定	備考
最新OSへの入れ替え	Global	1B JPY	!	Critical	17年1月	アプリケーションとの互換性の問題が発生。検証中。
外部委託先監査	APAC	30M JPY	✔	High	16年8月	30社中21社完了。
ISMS認証取得	Japan	50M JPY	!	Low	15年12月	軽微な指摘事項への対応中。
SOC構築	US/EMEA	500M JPY	✕	Medium	17年3月	リソース不足による大幅遅延。完了予定を延期。

ンを通じて実行することが、最も効率的かつ効果的であると言えます。

ダッシュボードの情報源となるKPIは、雲をつかむような非現実的または抽象的な指標を設定してしまうと、いつまで経っても目標に到達しない、進捗状況が具体的にわからないといった事態に陥るため、実際に組織が実行可能な範囲を指標として設定する必要があります。

サイバーセキュリティ経営ダッシュボードは、組織やビジネスユニットの戦略方針と整合した優先度の高い必要最低限のコンテンツで構成されますが、ステークホルダーが多くなればなるほど、あれもこれもと膨大なKPIを盛り込みがちであり、結果的に複雑で見づらく形骸化してしまい、本来知るべき重要な事象を見逃してしまうリスクがあることに注意しなければなりません。

② プロトタイプ

次に、初期設計で洗い出されたダッシュボードの主要なコンテンツを実際にどのようなフォーマットで、どのように表示するかという、ダッシュボード作成のための技術的な仕組みやレイアウト、表示項目の定義を行います。

各コンポーネントは、大まかなステータスを表示するフォーマットから、ドリルダウンでより詳細を表示するような形式が理想的であり、たとえばレーダーチャートやヒートマップのような全体像のうち、特定項目をクリックすることで、実際にその表示の根拠となったリスクの詳細を確認できるという仕組みが求められます。

レイアウトや表示項目は、ダッシュボードを参照するステークホルダーの嗜好に強く依存するため、このフェーズでは試作とフィードバックを繰り返し行うことで、理想的な構成に近づけていくことになります。その過程では、初期設計フェーズで検討されなかった新たな要件が発生する可能性があることも、考慮に入れておかなければなりません。

③ 詳細設計

ダッシュボードに必要なすべてのKPI、評価の閾値、データの取得方法、表示項目、レイアウト、ドリルダウン構成、フォーマット、リフレッシュの頻度、認証機構等を決定し、ダッシュボードを完成させるまでの開発ステップをロードマップとして整理します。

最終的にはダッシュボードをすべて自動化することが理想的ですが、これには多大な労力と投資、組織横断的な取組みが必要になる可能性が極めて高く、まずはステークホルダーが最優先するステータスを自動か手動かにかかわらず、既存の報告方式よりもわかりやすく、直感的に理解できるように整理し表示することを最初の目標とすべきです。

④ プルーフ・オブ・コンセプト

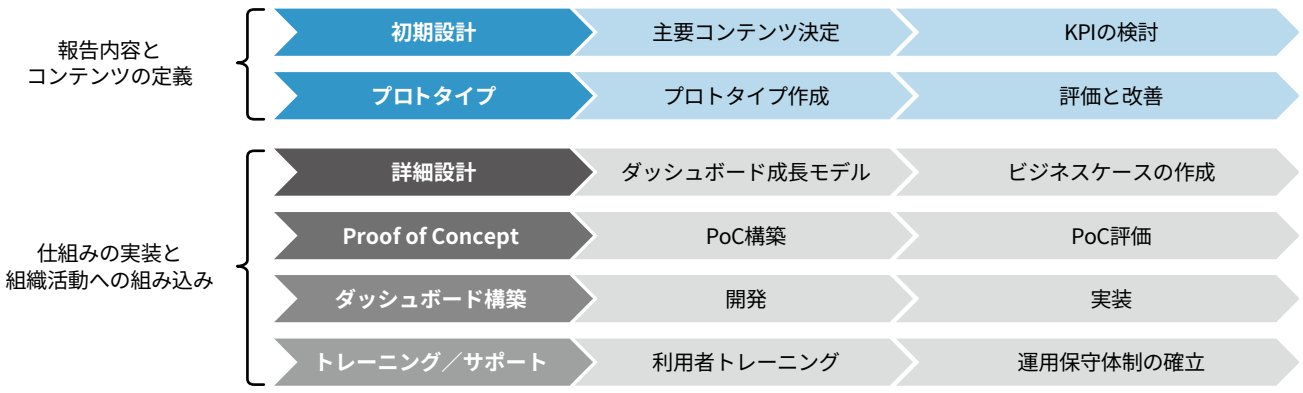
詳細設計した機能の一部を実際に構築することで、それが意図したとおりに効果を発揮するか実証します。

特定のKPI算出に必要なデータを実環境から収集し、それを集計して設計フェーズで定義したフォーマットで表示してみることで、ステークホルダーが期待した水準のインテリジェンスが得られるか、実際に確認する一連のプロセスを行います。その過程では、プロトタイプフェーズ同様に、先行する設計フェーズでは検討されなかった新たな要件の発生可能性についても考慮が必要であり、その結果ロードマップに変更が生じる場合もあります。

⑤ ダッシュボード構築

ダッシュボードの開発では、個別の機能を1つずつ開発して追加実装していくアジャイル開発プロセスが有効であり、これにより少機能の状態からでも早期に利用を開始することが可能です。同時に、ステークホルダーからのフィードバックによってすべての機能を一から開発し直さなければならなくなるような事態も回避できます。

【図表11　ダッシュボード構築プロセスの全体像】



⑥ トレーニング＆サポート

ダッシュボードが最初に利用可能状態になったタイミング、または機能が追加されるつど、利用者である各ステークホルダーに対するトレーニングを実施します。

ダッシュボードの機能が追加され、参照するステークホルダーも増えていくにつれ、当初予期できなかったような動作上の不具合や利用者による問い合わせが増加するため、サポート体制を確立しておくことも求められます。

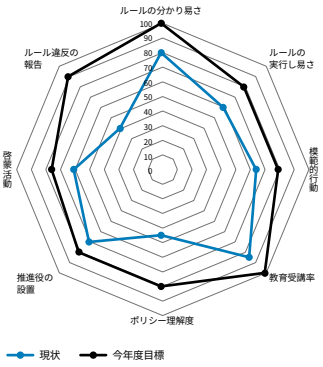
日々変化するサイバーリスクに対し、多種多様かつ専門的な対策を組織全体にわたって講じる必要があるサイバーセキュリティ領域において、経営者やボードメンバーが的確に最新のサイバーリスクとその対策状況を把握するとともに、ステークホルダーへの説明責任を果たすためのインテリジェントツールとして、本稿で解説したメソドロジーを参考に、「サイバーセキュリティ経営ダッシュボード」を構築し、活用することをお勧めします（**図表12**参照）。

【図表12　サイバーセキュリティ経営ダッシュボードのサンプル】

インシデント発生状況サマリー

分類	発生数	想定インパクト	発生源	トレンド
ハッキング	2	10 – 20億	外部	↑
マルウェア	3	100 - 1,000万	サードパーティ	↓
ソーシャル	-	-	-	→
不正	1	1 – 2億	内部	↑
物理	-	-	-	→
エラー	-	-	-	↓

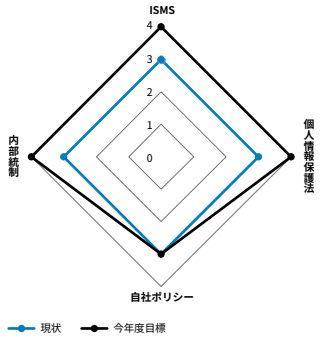
セキュリティ意識レベル



リスクステータス

リスク概要	深刻度	トレンド	詳細／対応状況
R1: 知的財産の喪失	Very High	New	既存システムでは管理者権限に対するアクセス制御が十分ではない。システム改修のための分析を実行中。
R2: 顧客情報の不正開示	Medium	↓	顧客情報インベントリが現状80%。インベントリ済みのレポジトリについてはコンプライアンス準拠している。
R3: オンラインセールスチャネルの停止	High	→	ペネトレーションテストの結果、環境設定において深刻な脆弱性が発見された。改修計画を検討中。
R8: 機密情報の漏えい	Very High	↑	新規ビジネス企画プロジェクトが発足。IT環境の整備とセキュリティ意識向上トレーニングを実施中。
R7: 会計不正	Medium	→	監査指摘事項として、会計システム管理プロセス上の不備が発見された。手順の改定準備中。

各種コンプライアンスへの準拠ステータス



脅威レベル

分類	脅威レベル	ゲージ
ハクティビスト	3	
ハッカー集団	2	
犯罪組織	4	
国家間紛争	1	
産業スパイ	3	
サードパーティ	5	
内部不正	2	

セキュリティ改善プロジェクト

プロジェクト	リージョン	予算	進捗	ビジネスインパクト	完了予定	備考
最新OSへの入れ替え	Global	1B JPY	!	Critical	17年1月	アプリケーションとの互換性の問題が発生。検証中。
外部委託先監査	APAC	30M JPY	✓	High	16年8月	30社中21社完了。
ISMS認証取得	Japan	50M JPY	!	Low	15年12月	軽微な指摘事項への対応中。
SOC構築	US/EMEA	500M JPY	×	Medium	17年3月	リソース不足による大幅遅延。完了予定を延期。

【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）

サイバーインシデント対応戦略
（KPMG Insight Vol.17/Mar.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