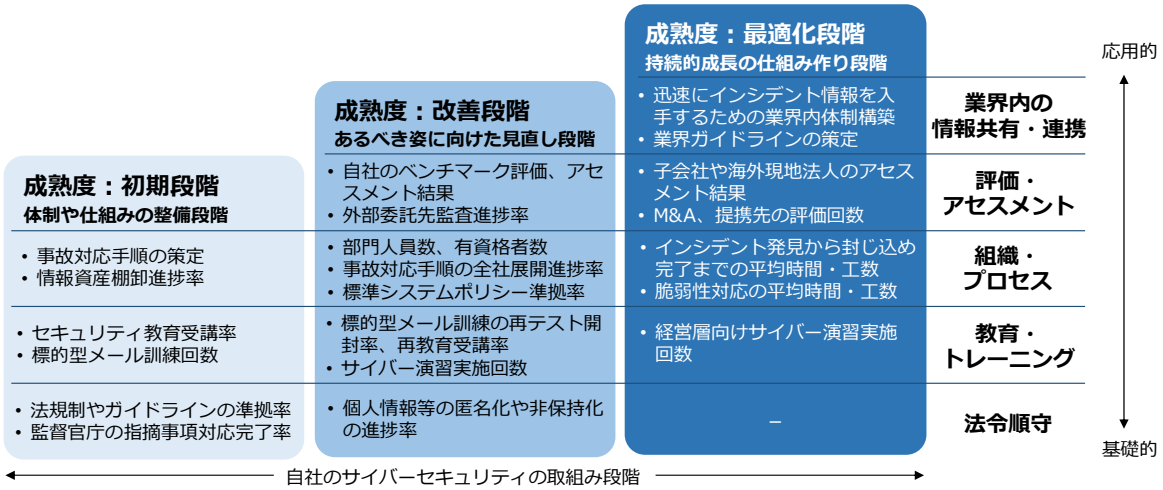
2019 年 4 月

損失額を減らすための「サイバーセキュリティの KPI モデル」（試論）

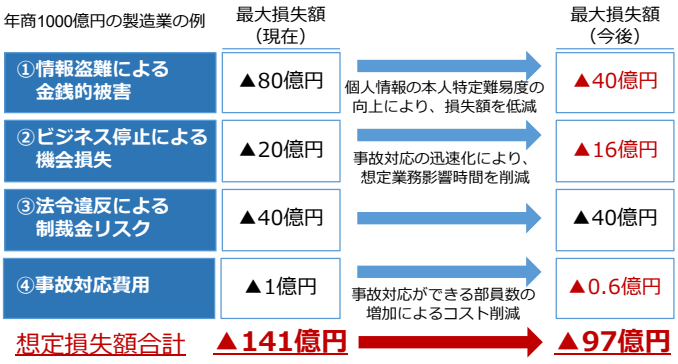
【要旨】

- ビジネスのデジタル技術への依存度が高まるほど、セキュリティ事故が発生した場合の経営への影響は増大する。サイバー攻撃は、悪意のある相手がおり、日々攻撃を変化させているため、発生確率を下げることは難しい。しかし、経営層と現場部門の取り組みにより、セキュリティ事故が発生した場合の損失額は軽減できる。
- 企業のセキュリティ事故による損失額を軽減し、デジタル技術を活用したイノベーションを推進するため、JCIC は「サイバーセキュリティの KPI モデル（図表 1）」をオリジナルモデルとして策定した。このモデルでは、セキュリティ責任者が自組織の取組み段階（以下、「成熟度」という）に応じた KPI[1]をモデルから選択し、目標設定やパフォーマンス評価に活用することを提案している。KPI による目標管理の見える化が社内に浸透し、経営層の理解が深まることで、予算や人員などのリソースが獲得しやすくなる。この流れを社会全体に普及させ、社会全体のセキュリティのレベル向上やイノベーション推進につなげる必要がある。
- また、KPI を設定する際は、数字だけを一人歩きさせないために、「自社のサイバーセキュリティの目的は何か」という基本部分を押さえることが重要である。本レポートでは、ビジネス視点でサイバーセキュリティに取り組むためのアプローチも紹介する。

図表 1 サイバーセキュリティの KPI モデル



図表 2　最大損失額の軽減効果（例）



上図（図表 1）の KPI モデルから、自組織の成熟度に応じた KPI を選択し、当期の目標とする。左図（図表 2）の例では、①本人特定の難化、②事故対応の迅速化などの KPI 達成により、セキュリティ事故が発生した場合の想定損失額を 97 億円まで軽減できることを示している。

このモデルは、あくまでもガイドという位置づけであり、組織の状況に応じて自由にカスタマイズ可能である。今後、様々な企業規模や業種などで活用してもらい、フィードバックを得ながら随時アップデートする予定であることから、本レポートは試論と位置づけた。

[1] KPI: Key Performance Indicators（重要パフォーマンス指標）の略。企業目標（売上や利益など）の達成度を定量的に評価する指標を意味し、多くの企業で用いられている。

1. はじめに

JCIC が 2018 年 9 月に公開したレポート「取締役会で議論するためのサイバーリスクの数値化モデル」では、取締役や経営層がサイバーセキュリティを自分事として捉えてもらうためには、経営の共通言語である「金額」を用いて議論すべきであると提言した。本レポートでは、セキュリティ事故（インシデント）による損失額を軽減し、デジタル技術を活用したイノベーションを推進するための「サイバーセキュリティの KPI モデル」を紹介する。また、ビジネス視点でサイバーセキュリティに取り組むためのアプローチも紹介する。

本レポートの対象読者は、主にセキュリティ責任者（CISO、部門長など）を想定しているが、取締役/監査役/経営層/経営企画/総務/リスク管理/人事/財務/情報システムなどのマネジメント層も読んでいただきたい内容になっている。また、民間企業の他、公共機関や非営利団体にも参考になる情報であると考える。ぜひ、このレポートを日頃のセキュリティ活動のヒントとして活用していただきたい。

2. 社会全体のセキュリティレベル向上のために

経済産業省が 2018 年 9 月に発表した「デジタルトランスフォーメーション（DX）レポート[2]」によると、デジタル技術を活用したビジネスモデルの創出をスピーディーに進めることで、2030 年に我が国の実質 GDP を 130 兆円超も押し上げる効果がある。一方、ビジネスのデジタル技術への依存度が高まるほど、セキュリティ事故が発生した場合の経営への影響は増大する。また、セキュリティ対策が後回しにされた場合、過度なリスク懸念またはリスク認識不足からデジタルトランスフォーメーションが思うように進まずに、ビジネスが停滞してしまう懸念もある。もはや、サイバーセキュリティは IT 部門だけの問題ではなく、企業経営の持続的成長を揺るがす経営課題であると言える。

サイバー攻撃は、悪意のある相手がおり、日々攻撃を変化させているため、一企業の努力だけでサイバー攻撃の発生確率を下げることは非常に難しい。しかし、取締役・経営層がサイバーセキュリティの重要性を自分事として理解し、またセキュリティ部門や関連部門が部門の垣根なく事故対応の態勢を築くことによって、セキュリティ事故が発生した場合の損失額は必ず軽減できる。

そこで、JCIC は「サイバーセキュリティの KPI モデル」を策定した。この KPI モデルの作成の目的は、企業の損失額を軽減させることだけではなく、積極的なデジタルトランスフォーメーションやイノベーションの推進に繋げることである。KPI による目標管理の見える化を社内に浸透させ、取締役・経営層に対してサイバーセキュリティの活動を定期的に報告し、議論することで、企業全体にセキュリティを重視する企業文化を築くことができる。このような取り組みによって、適切な予算や人員などのリソースも獲得しやすくなり、積極的なデジタルトランスフォーメーション推進にも繋がるはずだ。

このセキュリティの見える化の流れを、企業や業界の限られた領域だけではなく、社会全体に普及させることにより、社会全体のセキュリティのレベル向上につなげる必要がある。安心安全なデジタル社会を確立できれば、デジタル技術により様々な社会課題が解決され、経済も発展する社会を目指す「Society 5.0」の実現に近づくことができる。

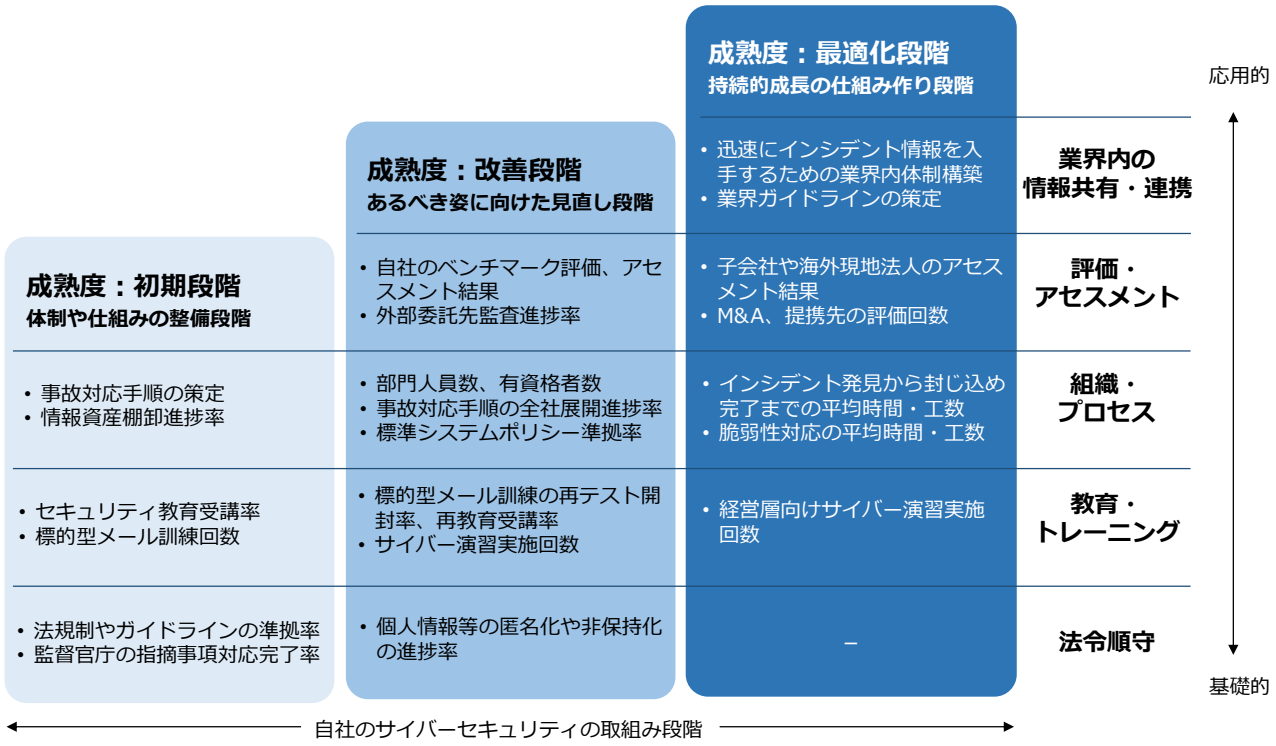
[2] 経済産業省「デジタルトランスフォーメーション（DX）レポート」http://www.meti.go.jp/press/2018/09/20180907010/20180907010.html
デジタルトランスフォーメーションとは、「新たなデジタル技術を活用して、新たなビジネスモデルを創出・柔軟に改変する概念」と説明されている。

3. サイバーセキュリティの KPI モデル

■ KPI モデルの策定手法

国内企業や海外企業がどのような KPI を設定しているかについて、インタビューや文献調査を行った（主な KPI の例を次ページ図表 3 に示す）。業種や企業規模による傾向は確認できなかったが[4]、サイバーセキュリティの成熟度[5]によって設定する KPI が変わる傾向があった。そこで、各社からヒアリングした 47 種類[6]の KPI を、3 段階の成熟度に割り振った（横軸の「初期段階」、「改善段階」、「最適化段階」）。次に、5 つの施策の種類（縦軸の「法令順守」、「教育・トレーニング」、「組織・プロセス」、「評価・アセスメント」、「業界内の情報共有・連携」）に分類し、基礎的な内容から徐々に応用的な内容になるよう並べた。47 個の KPI は、各社共通で利用できるものと、企業規模や業界特有のものに分けられるため、共通で利用できる KPI を抽出し、モデルに採用した。

（再掲）図表 1 サイバーセキュリティの KPI モデル



（セキュリティ責任者が自組織の成熟度に応じた KPI を上図から選択し、半期や通期の目標とする）

[4] 金融機関では、サイバーリスクの指標として「KRI （Key Risk Indicators；企業のリスク度合いを測るリスク指標）」を用いているケースが複数社あった。

[5] サイバーセキュリティの成熟度に関しては、現時点で企業横断的に判断できる基準などが確立されたものはなく、国内で議論を進めている段階である。

[6] KPI の詳細は「【別紙】サイバーセキュリティに関する KPI の例」を参照

図表 3　主な企業の KPI の例[7]

対象企業	セキュリティ部門のKPI	企業の状況
国内化粧品業	• 海外現地法人の経営層との打合せ回数 • 外部のセキュリティレベル評価　　など	海外ガバナンス強化のため、現地法人のマネジメントとの対話を重視。また、外部インテリジェンスを活用した自社のセキュリティレベルの評価を実施。
国内メディア業	• 第三者ベンチマーク評価 • 子会社や委託先のセキュリティ監査進捗率 • 事故対応手順の策定、グループ展開進捗率	特にグループ会社や主要委託先のセキュリティレベルを向上させることが課題となっている。
国内公共機関	• 職員セキュリティ教育受講率 • サイバー演習実施回数 • SOCシステム導入プロジェクト進捗率 （SOC：セキュリティオペレーションセンター）	人的・技術的なセキュリティ対策により、属人的な対応から、定期異動を考慮した組織力の底上げを目指す。
米国自動車製造業	• 製品セキュリティレビュー回数 • 脆弱性の公開から着手までの平均日数 • 業界ガイドラインの策定	脆弱性通報プログラムに報奨金制度を追加した他、自動車業界の情報共有組織である米国AUTO-ISACの主要メンバーとしても活躍している。
（参考） 米国政府機関	• 管理されているハードウェア資産の割合 • 管理されているソフトウェア資産の割合 • 重要度の高・中のシステムに関するセキュリティ認定取得率 • 管理されているモバイル機器の割合	米国政府は、省庁横断優先目標を掲げており、その1つとして「サイバーセキュリティ」を測定し、四半期毎に測定結果が公開されている。 （詳細は、参考資料①を参照）

■ KPI モデルの活用方法

サイバーセキュリティの KPI モデルは、期初にセキュリティ責任者がパフォーマンスの見える化に取り組む際のガイドとして活用することを想定している。特に、成熟度が初期段階の企業の場合、このモデルに採用した共通で利用できる KPI から始めることを推奨する。このモデルに厳格に従う必要はなく、企業独自の KPI を加えることや、組織の状況に応じて自由にカスタマイズすることも可能である。

なお、KPI の項目が多すぎると、KPI のデータ集めや数値調整だけで疲弊し、自社のビジネスにとって何のための KPI なのかを見失う懸念がある。KPI の数は、初期段階では 2～3 個からはじめて、徐々に 5～6 個程度に増やすことを検討すべきである。

図表 4 KPI モデルの活用方法

項目	内容
対象者	主に CISO、セキュリティ部門の責任者やマネージャーが対象
活用するタイミング	期初の目標設定時
KPI の設定方法	まず、自組織の成熟度（横軸）を設定する。次に、縦軸の KPI 項目から、重点的に取り組む KPI を選択し、経営層の合意を得る。その後、KPI を達成するための施策を立案し、各メンバーやグループ企業などに展開する。
KPI モデル活用のメリット	・ 成熟度に応じた KPI を設定でき、客観的にパフォーマンスを評価できる ・ セキュリティ事故による損失を軽減できる
留意事項	・ KPI 達成を目的化させないこと。あくまでもセキュリティの目的は経営への影響を軽減することであり、KPI は目標達成のための手段や指標であることを関係者全員に意識させる必要がある ・ 各メンバーが KPI に直接関係のない業務をしなくなる恐れがある。セキュリティ責任者は、追加で発生した業務を遂行した者をプラス評価する仕組み、KPI を状況の変化に応じて変更できる仕組みなどをあらかじめ定める必要がある

[7] 公開情報やインタビューを通じて JCIC が作成。内容の一部は推定。

KPI の目標値の目安、算出方法などの詳細情報は、「【別紙】サイバーセキュリティに関する KPI の例（PDF ファイル）」に記載した。別紙のイメージを以下に示す。

図表 5【別紙】サイバーセキュリティに関する KPI の例（抜粋）

管理番号	大項目	中項目	小項目	KPIの目安	対象組織	分類	KPI算出方法
1.1.1	セキュリティ部門の施策	情報資産棚卸進捗率	ハードウェア資産棚卸進捗率	95%以上	成熟度「低」（初期段階）	組織・プロセス	棚卸を実施した情報資産数 ÷ 対象とする情報資産数
1.1.2			ソフトウェア資産棚卸進捗率	95%以上	成熟度「低」（初期段階）	組織・プロセス	
1.1.3			モバイル機器棚卸進捗率	95%以上	成熟度「低」（初期段階）	組織・プロセス	
1.1.4			利用しているクラウドサービス棚卸進捗率	90%以上	成熟度「中」（改善段階）	組織・プロセス	
1.2.1		法規制やガイドラインの準拠率	法規制準拠率	100%	成熟度「低」（初期段階）	法令順守	現在の実績値 ÷ 計画値
1.2.2			個人情報の匿名化、非保持化	100%	成熟度「中」（改善段階）	法令順守	現在の実績値 ÷ 計画値
1.3.1		監督官庁の指摘事項対応完了率	監督官庁の指摘事項対応完了率	100%	成熟度「低」（初期段階）	法令順守	対応完了数 ÷ 指摘事項数
1.4.1		セキュリティ部門人員数	セキュリティ部門人員数	対IT人員の5%以上 対全社員数の0.25%以上	成熟度「中」（改善段階）	組織・プロセス	セキュリティ人員 ÷ IT人員 セキュリティ人員 ÷ 全社員数
1.4.2			資格取得者数	自社の現状に合わせて設定	成熟度「中」（改善段階）	組織・プロセス	資格取得者数
1.5.1		セキュリティ予算	対IT予算比率	対IT予算の7%以上	成熟度「中」（改善段階）	組織・プロセス	セキュリティ予算 ÷ IT予算
1.5.2			予算消化率	95%以上	成熟度「中」（改善段階）	組織・プロセス	使用額 ÷ 予算額
1.6.1		新規システム開発の評価回数、合格率	新規システム開発の評価回数	自社の現状に合わせて設定	成熟度「中」（改善段階）	組織・プロセス	システム評価回数
1.6.2			新規システム開発の評価合格率	90%以上	成熟度「中」（改善段階）	組織・プロセス	合格数 ÷ システム評価回数
1.7.1		ベンチマーク評価	ベンチマーク評価	自社の現状に合わせて設定	成熟度「中」（改善段階）	評価・アセスメント	ベンチマーク評価結果
1.8.1		アセスメント結果	自社のアセスメント結果		成熟度「中」（改善段階）	評価・アセスメント	アセスメント・監査結果
1.8.2			子会社や海外現地法人のアセスメント結果		成熟度「高」（最適化段階）	評価・アセスメント	アセスメント・監査結果
1.9.1		海外現地法人のガバナンス構築進捗率	全社ポリシー準拠率		成熟度「中」（改善段階）	組織・プロセス	現在の実績値 ÷ 計画値
1.9.2			監視システム導入率		成熟度「中」（改善段階）	組織・プロセス	
1.10.1		サイバー演習実施回数	経営層向けサイバー演習実施回数		成熟度「高」（最適化段階）	教育・トレーニング	現在の実績値 ÷ 計画値
1.10.2			CSIRT向けサイバー演習実施回数		成熟度「中」（改善段階）	教育・トレーニング	
1.10.3			グループ会社向けサイバー演習実施回数		成熟度「中」（改善段階）	教育・トレーニング	
1.11.1		インシデント対応完了	インシデント発見までの平均時間		成熟度「高」（最適化段階）	組織・プロセス	不正侵入から検知までの平均時間
1.11.2			インシデント対応完了平均時間・工数		成熟度「高」（最適化段階）	組織・プロセス	検知から封じ込めまでの平均時間
1.12.1		脆弱性対応	脆弱性対応着手までの平均時間		成熟度「高」（最適化段階）	組織・プロセス	緊急な脆弱性の公開から着手までの平均時間
1.12.2			脆弱性対応完了までの平均時間・工数		成熟度「高」（最適化段階）	組織・プロセス	着手から対応完了までの平均時間
1.13.1		業界内の情報共有体制構築	迅速にインシデント情報を入手するための業界内体制構築	業界の現状に合わせて設定	成熟度「高」（最適化段階）	業界内の情報共有・連携	現在の実績値 ÷ 計画値
1.13.2			業界ガイドラインの策定		成熟度「高」（最適化段階）	業界内の情報共有・連携	現在の実績値 ÷ 計画値

■ 更なる調査の必要性

この KPI モデルは、様々な企業規模や業種で活用してもらい、フィードバックを得ながら随時アップデートする予定である。また、組織のデジタルトランスフォーメーションの取組みと KPI の関係性、KPI に関わる項目を自動的に収集している事例収集、自社製品・サービスのセキュリティをどのように KPI として取り組むか、組織のセキュリティ姿勢やマインドをどう KPI で測るかなどについても今後調査する必要がある。

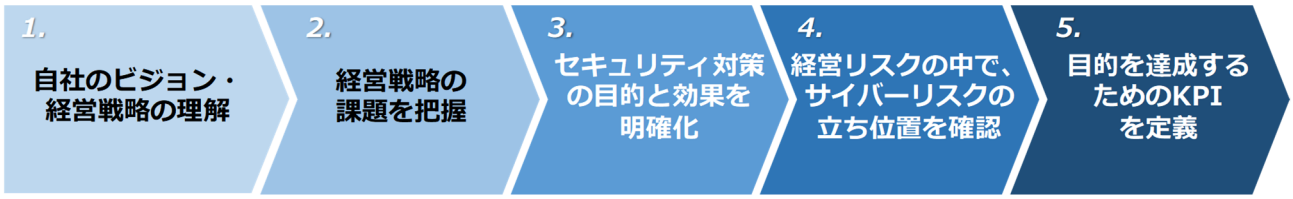
なお、インタビューの中で、サイバーリスクの可視化指標として「KRI（Key Risk Indicators；企業のリスク度合いを測るリスク指標）」を用いているケースが複数社あった。サイバーリスクの管理指標である KRI に関しては、今後のレポートで紹介する。

4. ビジネス視点でサイバーセキュリティに取り組むためのアプローチ（KPI の設定方法）

KPI を設定する際は、数字を一人歩きさせないために、「自社のサイバーセキュリティの目的は何か」という基本部分を押さえることが重要である。JCIC が各企業のセキュリティ責任者らと議論を重ねたところ、「自社の存続やブランドを守るために、サイバーセキュリティは不可欠」、「人命や社会責任を守るために、サイバーセキュリティが必須になってきている」といった意見が出ている。まずは、自社のビジョンや経営戦略が何で、その障壁となるものは何かという議論を社内で重ねることが重要である。

「自社のサイバーセキュリティの目的は何か」、「どのような KPI を設定すべきか」を検討するアプローチ方法について、以下にまとめた（図表 6）。まず、セキュリティ責任者は、自社のビジョン・経営戦略を理解し、経営戦略を妨げる阻害要因を把握する必要がある。そして、サイバーセキュリティの目的を明確にし、セキュリティ対策を強化することで期待できる効果を明確にする。その後、他の経営リスクと比較し、サイバーリスクの立ち位置（重要度合い）を確認する。最後に、サイバーセキュリティの目的を達成するための KPI を設定する。こうして導き出された KPI は、必ず経営層の関心を引くはずである。

図表 6 ビジネス視点でサイバーセキュリティに取り組むためのアプローチ



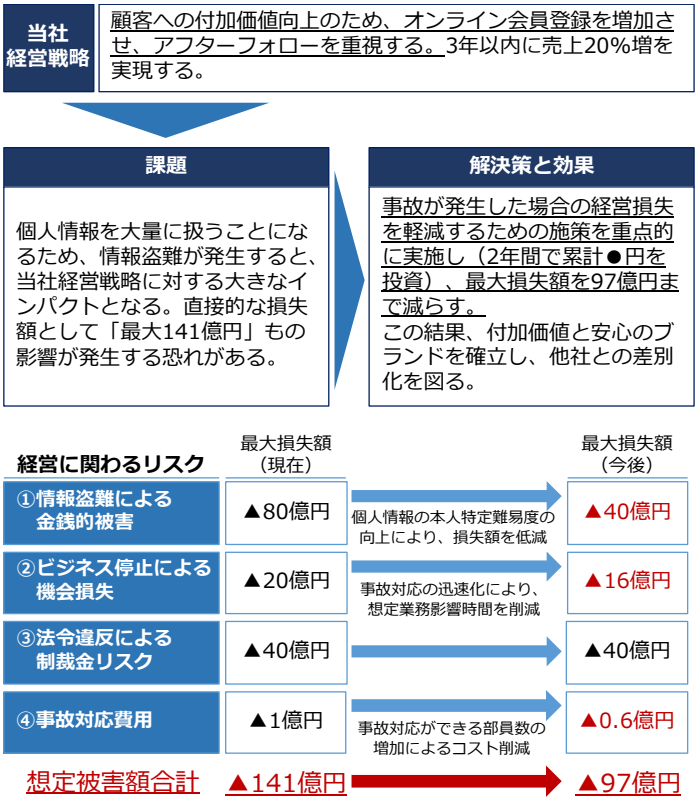
項番	項目	内容	チェック欄
1	**自社のビジョン・経営戦略の理解**	経営層の考えを社員向け通達や社内の掲示板などで確認する。直接、経営層の考えを聞く機会を設ける。	□
2	**経営戦略の課題を把握**	経営層が考える経営課題を社員向け通達や株主向け資料（有価証券報告書の事業等のリスク）などで確認し、可能であれば直接考えを聞く。	□
3	**セキュリティ対策の目的と効果を明確化**	サイバーセキュリティによって自社が何を実現したいのか、自社が実現したいことをセキュリティ責任者はどうサポートできるのかを明確にする。次に、サイバーリスクの想定被害額を算出し、リスク対応の優先度を決める。また、目的と期待するビジネス視点での効果を文書として明文化する。	□
4	**経営リスクの中でサイバーリスクの立ち位置（重要度合い）を確認**	自社を取り巻くリスクの中で、サイバーリスクの立ち位置を確認する。経営企画、リスク管理などの部門と議論を交わし、各部門と認識を合わせる。	□
5	**目的を達成するための KPI を設定**	半期・通期に重点的に取り組む KPI を設定し、経営層などの合意を得る。また、達成状況をモニタリングする仕組みを作る。	□

5. 経営層へのビジネス視点での報告例

セキュリティ責任者が経営層に報告する際の KPI の利用シーンを具体的にイメージしやすいように例示する。以下は、業務用・家庭用の空調設備を取り扱う年商 1000 億円の製造業の例である。空調設備は成熟した市場であり、海外メーカーとの競合が厳しい状況になっている。そこで、中期経営計画として「顧客の声を重視した付加価値向上」を掲げ、製品購入時のオンライン会員登録を必須にし、消耗品の交換時期の通知などのアフターフォローを重視する戦略とした。以下の資料は、経営層を積極的に巻き込むためにセキュリティ責任者が作成したものという位置づけである。

■ 経営戦略の課題とセキュリティ対策の効果を説明

図表 7 期待する効果

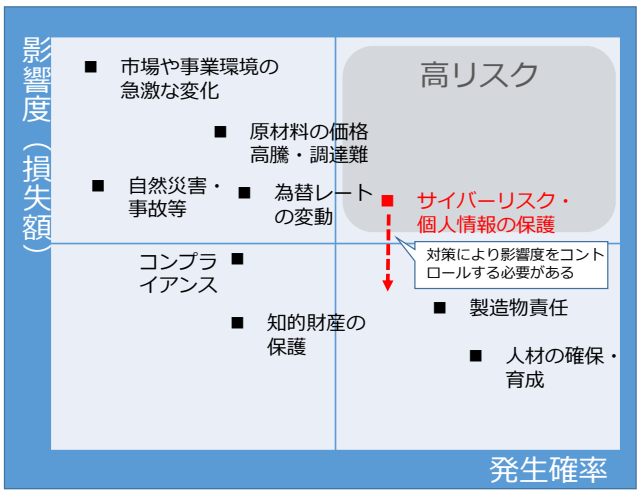


まず、自社の経営戦略におけるサイバーセキュリティの目的や重要性をストーリーで説明する（図表 7）。同社では、「付加価値向上のためオンライン会員を増加させる」という経営戦略を掲げているが、情報盗難が発生すると経営戦略に対する大きな影響となり、会員数増加という戦略実現の障壁になる。

事故が発生した場合の損失額を軽減するためのセキュリティ施策を重点的に実施することで、最大損失額を「141 億円」から「97 億円」までに減らす効果があることをセキュリティ責任者が経営層に示している。また、最大損失額は、JCIC の「サイバーリスクの数値化モデル」を用いて金額換算した。

■ 経営リスクの中で、サイバーリスクの立ち位置を説明

図表 8 事業リスク評価



次に、経営リスクの中でサイバーリスクの立ち位置を経営層に理解してもらうために、他のリスクと影響度・発生確率を比較する（図表 8）。同社の場合、会員登録数を拡大させる戦略によって「サイバーリスク・個人情報の保護」が高リスク（右上）に位置付けられており、影響度と発生確率が相対的に大きいことを示している。この表を用いて、今後セキュリティ対策により、影響度（損失額）を下げる効果があり、リスクが許容できるレベルになると伝えることができる。

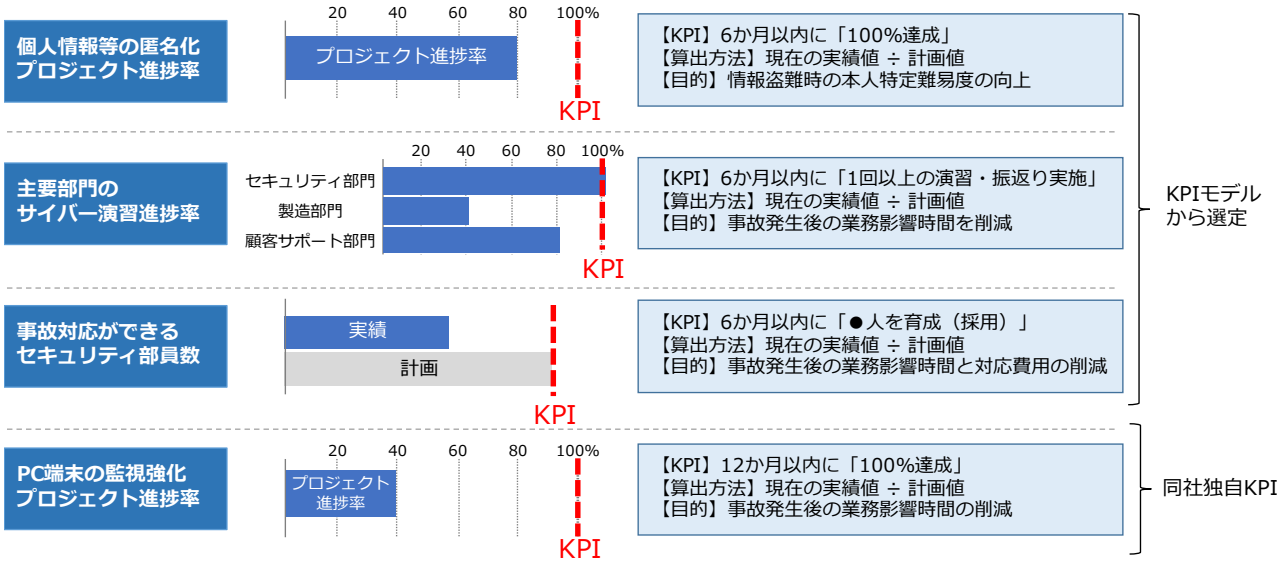
■　目的を達成するための KPI を説明

そして、セキュリティ事故による影響度（損失額）を下げるための KPI を「サイバーセキュリティの KPI モデル」の「成熟度：改善段階」から 3 つ設定し、更に同社独自の KPI として 1 つを設定した。

まず、1 つ目の KPI として、情報盗難時の金銭的被害を軽減するための「個人情報等の匿名化プロジェクト進捗率」を設定した。次に、事故発生後の業務影響や機会損失を減らすための「主要部門のサイバー演習進捗率」や、事故対応ができる「セキュリティ部員数」を KPI として設定した。また、同社独自の KPI として、セキュリティ事故後の技術調査を迅速にするための「PC 端末の監視強化プロジェクト進捗率」を設定した。

その後、KPI を達成するための詳細な計画を策定し、各メンバーやグループ企業などに展開し、達成状況をモニタリングする仕組みを作る必要がある。また、経営戦略で掲げたオンライン会員増加や売上 20%増などにサイバーセキュリティの取組みが貢献できているかという点について、定期的に経営層や関連部門と議論を重ねることも求められる。

図表 9　サイバーセキュリティの KPI と目的

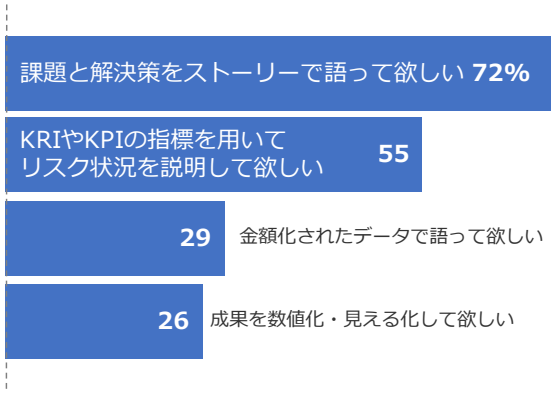


【参考】米国の取締役・経営層がサイバーリスクの報告時に求めるポイント

米国民間企業の調査によると、取締役・経営層は、サイバーリスク報告に求めるポイントとして、「課題と解決策をストーリーで語って欲しい」という回答が最も多く、次いで「KRI*や KPI を用いてリスク状況を説明して欲しい」という回答があった（図表 10）。米国企業においてもサイバーセキュリティに精通した取締役・経営層の数は限られるため、見える化を重視していることが分かる。

* KRI（Key Risk Indicators；企業のリスク度合いを測るリスク指標）

図表 10 米国の取締役・経営層がサイバーリスクの報告時に求めるポイント（Cyentia Institute 調査[8]、n=85）



[8] Cyentia Institute「Cyber Balance Sheet 2017 Report」 https://www.cyentia.com/library-item/cyber-balance-sheet-the-2017-report/

6. まとめ

本レポートでは、セキュリティ事故による損失額を軽減し、デジタル技術を活用したイノベーションを推進するための「サイバーセキュリティの KPI モデル」を紹介した。また、ビジネス視点でサイバーセキュリティに取り組むためアプローチも紹介した。

セキュリティ責任者がどのような KPI を設定すべきか選定に悩むような場合、「自社のサイバーセキュリティの目的は何か」という基本部分に立ち戻って欲しい。自社のビジョンや経営戦略が何で、その障壁となるものは何かという議論を社内で重ねることで、サイバーセキュリティにおいて設定すべき指標が見えてくるはずである。また、KPI による目標管理の見える化が社内に浸透し、取締役・経営層に対してサイバーセキュリティの活動を定期的に報告し、議論することで、企業全体にセキュリティを重視する企業文化を築くことができる。このような取り組みによって、適切な予算や人員などのリソースも獲得しやすくなり、積極的なデジタルトランスフォーメーション推進に繋げることができる。

安心安全なデジタル化社会を実現するためには、社会全体のセキュリティレベル向上が求められる。そのためには、セキュリティの見える化の流れを、企業や業界の限られた領域だけではなく、社会全体に普及させる必要がある。JCIC は、サイバーセキュリティの推進活動を通じ、Society 5.0 の実現、イノベーションの加速、そして安心安全な社会の実現に取り組んでいく。

以 上

参考文献

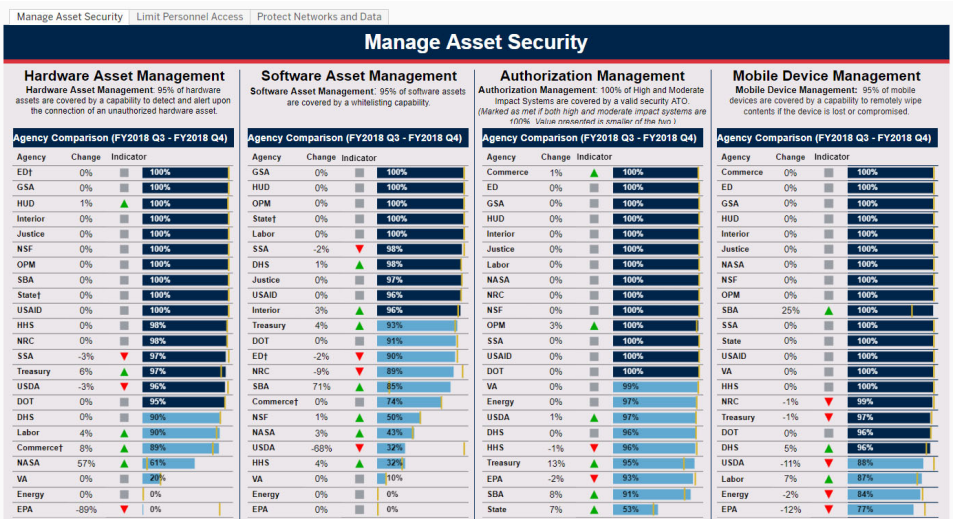
- 経済産業省「デジタルトランスフォーメーション（DX）レポート」, http://www.meti.go.jp/press/2018/09/20180907010/20180907010.html
- 財務省「KPI についての論点の整理」, https://www.mof.go.jp/pri/research/discussion_paper/ron276.pdf
- IPA「CISO 等セキュリティ推進者の経営・事業に関する役割調査」, https://www.ipa.go.jp/security/fy29/reports/ciso/index.html
- Cyentia Institute「Cyber Balance Sheet 2017 Report」, https://www.cyentia.com/library-item/cyber-balance-sheet-the-2017-report/
- NIST「情報セキュリティパフォーマンス測定ガイド」, https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-55r1.pdf
- COSO「Developing Key Risk Indicators to Strengthen Enterprise Risk Management」, https://www.coso.org/Documents/COSO-KRI-Paper-Full-FINAL-for-Web-Posting-Dec110-000.pdf
- GM 投資家向け情報, https://investor.gm.com/sec-filings
- DESTINATION XL GROUP 投資家向け情報, http://investor.destinationxl.com/
- Nature's Sunshine Products 投資家向け情報, https://www.naturessunshine.com/us/company/c1/filings/
- NIST SP 800-64「システム開発ライフサイクルにおけるセキュリティの考慮事項」, https://csrc.nist.gov/publications/detail/sp/800-64/rev-2/final
- セキュア開発ライフサイクル（SDLC ：Secure Development Life Cycle）, https://www.pwc.com/jp/ja/services/cyber-security/product-cs/sdlc.html
- 米国政府におけるサイバーセキュリティの KPI, https://d2d.gsa.gov/tableau-report-for-embed/7861
- オーストラリア政府サイバーセキュリティ戦略, https://cybersecuritystrategy.homeaffairs.gov.au/sites/all/themes/cybersecurity/img/cyber-security-strategy-first-annual-update-2017.pdf
- 全米取締役協会「サイバーリスクハンドブック」, https://www.nacdonline.org/insights/publications.cfm?ItemNumber=10687
- JCIC「第 1 回年次会合レポート」, https://www.j-cic.com/news/event20181128.html

参考資料①　米国政府におけるサイバーセキュリティの KPI

2010 年に、米国政府は「政府業績成果現代化法（GPRAMA）」を導入し、目標の達成度合いの見える化を行っている。行政管理予算局（OMB）は、省庁横断優先目標（Cross-Agency Priority Goals、CAPGs）を掲げており、その 1 つとして「サイバーセキュリティ」を省庁横断的に測定している。例えば、サイバーセキュリティというカテゴリの中に情報資産管理の KPI があり、以下 4 項目について四半期毎に達成度合いが公開されている。

- 管理されているハードウェア資産の割合：　95%以上
- 管理されているソフトウェア資産の割合：　95%以上
- 重要度の高・中のシステムに関するセキュリティ認定取得率：　100%
- 管理されているモバイル機器の割合：　95%

図表 11　米国政府におけるサイバーセキュリティの KPI 進捗状況[9]

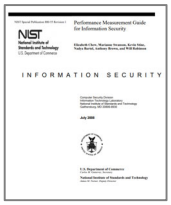


参考資料②　米国国立標準技術研究所（NIST）の「情報セキュリティパフォーマンス測定ガイド」

国内外でサイバーセキュリティの KPI に関する研究調査は、ほとんど確認できなかった。最も参考になる資料として、NIST の「情報セキュリティパフォーマンス測定ガイド[10]（SP 800-55 rev.1）」があるが、2008 年以降の更新はされていない。KPI の研究調査が進んでいない理由は、組織毎に様々な KPI が存在しており、脅威と対策が日々変化する状況では、標準化が難しいためと考えられる。

なお、このガイドでは、部署単位ではなく、各関係者が担当するパフォーマンス測定指標の数について言及している。一人につき、優先度が高い測定指標を 2～3 個選択し、セキュリティ対策の成熟度に伴い KPI の数を徐々に増やすべきとしている。また、測定指標の設定において、以下の 4 点を考慮する必要があるとしている。

- 定量化可能な情報（割合、平均、数値）を用いること
- 測定指標の根拠となるデータが容易に入手できること
- 繰り返し可能な施策を対象とすること
- パフォーマンスの追跡やリソースの割り当てに役立つものであること

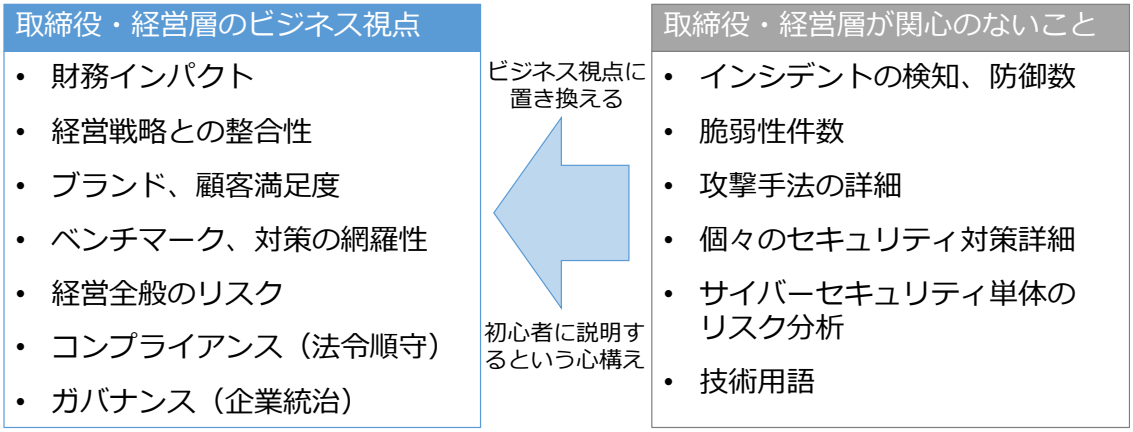


[9] https://www.performance.gov/CAP/key_performance_indicators.html , https://d2d.gsa.gov/tableau-report-for-embed/7861 （2019 年 4 月閲覧）

[10] NIST「情報セキュリティパフォーマンス測定ガイド」https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-55r1.pdf

参考資料③　取締役や経営層に説明する際の留意事項

セキュリティ責任者が取締役会や経営会議で報告する際、若しくは他部門と議論をする際は、「サイバーセキュリティの初心者に説明する」という心構えを持ち、必ずビジネス視点に置き換えて説明する必要がある。例えば、「新たな攻撃手法によって、セキュリティ事故件数が増加している」という内容では状況報告としてしか受け取れないため、「最大80 億円の財務損失の恐れがある」、「当社の経営戦略である新製品投入に影響が出る恐れがある」といったビジネスへの影響にまで言及する必要がある。



NPO 法人の全米取締役協会（17,000 人以上の取締役が参加する団体）が発行した取締役が認識しておくべき事項をまとめた「サイバーリスクハンドブック[11]」では、取締役会でサイバーリスクを報告する頻度は、3 か月に 1 回を推奨とし、少なくとも半年に 1 回は議論すべきとしている。報告の内容としては、全社のサイバーセキュリティ管理状況、新規ビジネス・新規マーケット参入のリスク、M&A・投資計画に関するリスクなどとしている。また、取締役・経営層に対してサイバーリスクを説明する際のポイントも以下の通りまとめられている。

- 取締役・経営層にどう関与して欲しいか明確にすること
- わかりやすい報告に心がけること（例：サマリーを書く、図表を使いビジュアル化する、技術用語は避ける）
- 単なる報告だけで済まさず、示唆的な情報を伝えること（例：トレンド変化、他社との差異、ビジネス影響）
- 情報過多にならないこと
- 議論と対話に注力できること

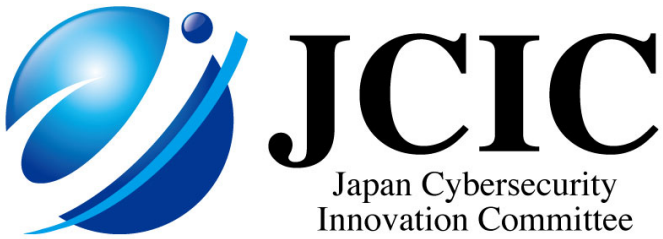
また、JCIC が 2018 年 11 月に行ったパネルディスカッション「取締役から見たサイバーリスク[12]」の議論は、日本企業のセキュリティ責任者にとって非常に参考になる情報であった。このディスカッションでは、現役の取締役・経営層が登壇し、以下の発言があった。

- 取締役・経営層に説明する際は「素人に説明する」つもりでわかりやすく説明する必要がある
- 経営リスク全体の中の 1 つとしてサイバーリスクを議論する必要がある
- 他社と比較して当社はどのレベルなのかを説明する必要がある
- セキュリティ事故の事例を理解し、当社で発生した時の意思決定プロセスを整備する必要がある

上記は、日本のセキュリティ責任者にとって役立つポイントであるため、今後、取締役・経営層とのコミュニケーションを取る際に参考にしていただきたい。

[11] https://www.nacdonline.org/insights/publications.cfm?ItemNumber=10687

[12] https://www.j-cic.com/news/event20181128.html



[本調査に関する照会先]

主任研究員　上杉謙二　uesugi@j-cic.com

主任研究員　平山敏弘　hirayama@j-cic.com

－ ご利用に際して －

■ 本資料は、JCIC の会員の協力により、作成しております。本資料は、作成時点での信頼できると思われる各種データに基づいて作成されていますが、JCIC はその正確性、完全性を保証するものではありません。

■ 本資料は著作権法により保護されており、これに係る一切の権利は特に記載のない限り JCIC に帰属します。引用する際は、必ず「出典：一般社団法人日本サイバーセキュリティ・イノベーション委員会（JCIC）」と明記してください。

■ [お問い合わせ先] info@j-cic.com