CISO ハンドブック

業務執行として考える情報セキュリティ

Ver. 1.1 β

特定非営利活動法人　日本ネットワークセキュリティ協会
社会活動部会　CISO 支援ワーキンググループ

2018 年 6 月 22 日（1.1 β）
2018 年 4 月 27 日(1.0 β）

目次

1. はじめに

本書の目的

情報セキュリティ事故が数多く報道され、またGDPR（EU一般データ保護規則）[(1)]などの国際的な規制の対応が求められるなど、セキュリティへの関心が高まり、組織のセキュリティ対策を所轄するCISO（Chief Information Security Officer）が注目されています。一方で、情報セキュリティ対策は、危険性や損失といったマイナス面が主要なテーマとなり、ビジネスに対してどのように貢献するのか、という視点で議論される事は殆どありません。しかし、CISOが経営陣の一員として、セキュリティに取り組むためには、想定される危険性や損失に取り組むだけではなく、ビジネスの視点を持って業務を執行することが求められます。

セキュリティを経営に取り込むための試みとして、経済産業省が発行した「サイバーセキュリティ経営ガイドライン[(2)]」が注目されています。重要な取り組みのひとつですが、ポリシー順守を目的としたPDCAフレームワークとCSIRT(Computer Security Incident Response Team)が主要な内容で、CISO業務の執行に必要なビジネスの視点は取り上げられていないように思います。

本書では、この点を踏まえ、CISOが経営陣の一員としてセキュリティ業務を執行する上で前提となる、ビジネス（経営）の基本的な枠組みを整理し、明確にすべき目標と指標、そして施策を評価する判断基準を提供することを目的としています。

本書の使い方

- 経営会議で資料を作る際のひな型として
- 技術担当からCISOになった人がビジネスを理解するための参考として
- セキュリティ経験の少ないCISOがセキュリティ業務を理解するための参考として
- 経営会議で話される業務執行（CISOの役割と責任、業務）の概要を理解する参考として
- ビジネスに関連付けた計測項目と判断基準の例として
- ビジネスに沿ったセキュリティ計画や、事業継続計画の策定の資料として

2. 情報セキュリティの目的

情報セキュリティの課題

現在の情報セキュリティには、多くの課題がありますが、ここでは三つの課題に注目します。

まずは、経営に結びついた現実的なセキュリティ対策の構築です。セキュリティ対策は、ニュースで取り上げられるなど、情緒的な要因で場当たり的に導入される傾向があります。しかし、効果的な投資を行うためには、経営計画に基づいたセキュリティ戦略を構築し、日々変化する脅威や技術動向に対応した施策を実施することが求められます。

二番目の課題は、セキュリティ対策の実効性の担保です。これまで、セキュリティ対策の柱としてセキュリティポリシーの策定が重要視されてきました。しかし、セキュリティポリシーが普及した現在でも、セキュリティ侵害は後を絶ちません。このため、世界的な傾向として、緊急対応を行う CSIRT 活動や、セキュリティ侵害を前提としたサイバーセキュリティフレームワーク（米国 NIST）[(3)]が注目されています。

三番目の課題は、CISO が経営陣の一員として、これらの課題を担うことにあります。しかし、CISO に要求される領域は多岐に渡り、技術系の CISO は経営に関する知識とスキルが不足し、非 IT 系の CISO は技術的・具体的な知識とスキルが不足する傾向があります。

本章では、三番目の課題に注目し、ビジネス視点を意識した情報セキュリティと、リスク分析について取り上げます。

ビジネス視点の情報セキュリティ

情報セキュリティの目的は「情報資産の保護」と言われますが、ビジネスの視点では、「情報資産の保護」は目的ではなく手段に相当します。例えば、ビジネス上の損害とならないように「情報資産を保護」する、競合優位性を高めるために「情報資産を保護」する、といった考え方が必要で、情報資産の洗い出しを行う場合も、個々の情報資産の価値をビジネスの視点で評価し、それぞれの資産ごとに対策を策定していく必要があります。

つまり、情報セキュリティの責任者は、自社ビジネスをよく理解する必要があります。脅威による直接的な損害だけではなく、ビジネス施策をセキュリティ上の判断で見合わせた場合の事業リスクについても取り組み、事業部門や関連部門、そして経営陣といったステークホルダーとの連携が不可欠です。

セキュリティを専門としない経営陣や他部門の人たちとコミュニケーションをとっていくためには、セキュリティ上の重要な用語と概念を伝えるとともに、CISO がビジネスの一般的な用語や概念を身につける必要があります。

ビジネスにおけるリスク項目

セキュリティ侵害が発生した場合、何らかの情報資産の CIA（Confidentiality, Integrity, Availability）が侵害されたことになります。そして、顧客情報や機密情報の漏洩、システムの停止、不正送金、さらには業務の停止、評判・評価（レピュテーション）に影響し、株価の低下にもつながります。

情報セキュリティでは、このようなビジネス上の影響を事前に明らかにするリスク分析が重要とされています。しかし、リスク項目の洗い出しはヒアリングを中心とする場合が多く、洗い出したリスク項目の網羅性や合理性の判断は困難です。

表 1 は、企業が直面する一般的なリスクの例で、表 2 は IT 企業において想定される包括的なビジネスリスク項目の例です。想定すべきビジネスリスクは多岐に及んでおり、これらの理解を欠いては、情報セキュリティリスクの評価ができません。リスク項目の洗い出しを行うに当たっては、ビジネス全体のリスク項目に基づき、他の経営陣と共に網羅性と合理性を検討する必要があります。

表 1　企業が直面する一般的なリスク（出典：J-Net21 起業マニュアル　リスクマネジメントの基礎[4]）

財産損失のリスク	火災・爆発・地震・風災害（台風など）・盗難などによって、企業が所有している財産が損なわれるリスクのこと
収入減少のリスク	企業の売り上げや利益が減少するリスクのこと。たとえば、取引先の倒産など
賠償責任のリスク	企業が株主、従業員、消費者から賠償責任を問われるリスクのこと。たとえば、製造物責任や役員賠償責任を問われての訴訟など
人的損失のリスク	経営者、重役、あるいはその他の従業員の死亡・事故・疾病・不健康・信用損失などのリスクのこと
ビジネスリスク	新製品開発や海外進出などの営業戦略上のリスク、および株式投資・商品取引・為替相場・他社への融資などの資産運用上のリスクのこと

表 2　IT 企業において想定されるビジネスリスク一覧（出典：CxO(経営層)のための情報セキュリティ[5]）

災害リスク	自然災害、パンデミックス、テロなどの外部からの攻撃、火災
事業環境リスク	社外からの風評被害、政府調達制度の変更、環境汚染による損害
戦略リスク	人材確保の困難さ、デリバティブ取引による経済的損失、企業の合併・分割
財務リスク	問題プロジェクト、社内システムトラブル
事故・故障リスク	社内サービス停止、お客様・社員情報の漏洩、機密情報の持出し
情報セキュリティリスク	サイバー攻撃、お客様・社員情報の漏洩、機密情報の持出し
犯罪リスク	電磁的記録不正作出、供用、私的非道行為、現金・預金の着服・窃取
労務リスク	労働災害、長時間労働にかかる法令等違反、社員のメンタル不調、差別行為
事業運営上のリスク	営業契約における規定違反に起因する損失、

	購買契約における規定違反に起因する損失

リスク分析では、リスク項目の優先度についても考察する必要があります。経営者が優先すべきと考えているリスク項目（**表 3**）では、「⑩情報漏洩」だけが直接情報セキュリティに関わる項目となっています。しかし、「⑰子会社のガバナンスに係るリスク」、「①財務報告の虚偽記載」、「④役員・従業員の不正」は、SOA（Sarbanes-Oxley Act Section 404）[6]や内部統制と深くかかわる項目であり、「⑲海外拠点の運営に係るリスク」も、IT ガバナンスと不可分の項目といえます。ビジネスに IT が不可欠となった現在では、情報セキュリティに直接的にかかわるリスクばかりではなく、間接的に IT や情報セキュリティが関わるべきリスク項目が多いことを理解する必要があります。

表 3　優先すべきリスク（出展：デロイトトーマツ　企業のリスクマネジメント調査（2015 年版）[7]）

分析資料6:優先すべきリスク　企業規模別

※いずれも母集団は全回答企業（N=237社）
1社につき最大3項目まで選択

図6:優先して着手が必要と思われるリスク　企業規模別傾向

優先すべきリスク	全体			従業員数1,000名以上			従業員数1,000名未満		
	2013年	2014年	2015年	2013年	2014年	2015年	2013年	2014年	2015年
⑲海外拠点の運営に係るリスク	1位	3位	1位	1位	1位	2位	4位	5位	1位
	29%	28%	46%	39%	34%	47%	16%	19%	45%
⑰子会社ガバナンスに係るリスク	4位	2位	2位	2位	2位	1位	3位	2位	2位
	26%	29%	44%	32%	32%	50%	17%	24%	36%
⑩情報漏えい	2位	1位	3位	4位	3位	3位	1位	1位	3位
	28%	31%	25%	28%	29%	25%	27%	33%	25%
②海外企業買収後の事業統合リスク ※2014年より項目追加		9位	4位		6位	3位		17位	10位
		9%	19%		12%	25%		4%	11%
⑱海外取引に係るリスク（現地との調整）	7位	9位	5位	7位	8位	5位	11位	11位	6位
	13%	9%	18%	16%	10%	20%	9%	8%	14%
⑥人材流出、人材獲得の困難による人材不足	8位	6位	6位	9位	5位	6位	7位	7位	4位
	13%	13%	16%	14%	13%	13%	12%	13%	19%
⑨製品、サービスの品質チェック体制の不備	11位	5位	7位	9位	6位	7位	13位	3位	5位
	12%	16%	13%	14%	12%	12%	8%	23%	15%
①財務報告の虚偽記載	9位	9位	8位	8位	11位	9位	11位	11位	8位
	13%		11%	15%	8%	11%	9%	8%	12%
③地震・風水害等、災害対策の不備	3位	4位	9位	3位	4位	7位	2位	4位	11位
	26%	21%	10%	30%	21%	12%	21%	22%	7%
④役員・従業員の不正	6位	9位	9位	6位	8位	9位	5位	14位	11位
	16%	9%	10%	19%	10%	11%	13%	6%	7%

CISO は、長期間変化のないポリシーに基づいたルール順守のセキュリティ対策ばかりではなく、事故や攻撃、対応する脆弱性に目を向け、技術的な側面だけではなく、ビジネスへの影響を考慮し、対症療法ではなく、将来を見据えた取り組みを行うことが望ましい。

コラム：脅威、脆弱性、リスク

セキュリティ侵害（アクシデント）は、「脅威」と「脆弱性」と「リスク」がそろっているときに生じます。

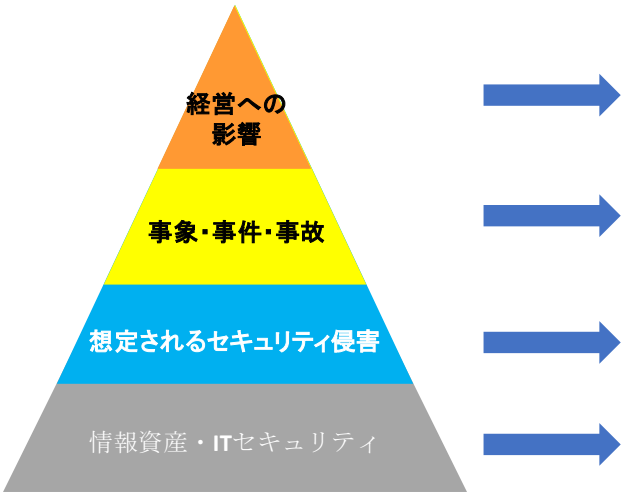
脅威は、システムあるいは組織に危害を与える要因のことです。情報セキュリティでは、情報資産の機密性・完全性・可用性（CIA)を阻害する要因を指します。脅威には、故意に行われるもの（不正侵入やマルウェアを感染させる行為、DoS 攻撃、ソーシャルエンジニアリングなど)、過失によるもの（紛失、操作・設定ミスなど)、故障・誤動作（部品の劣化など)、自然災害（地震や火災など）があります。
脆弱性は、システムあるいは組織に存在する、設備機器や関係者、運用上の欠陥、不備などのことで、セキュリティ・ホールとも呼ばれます。例えば、OS・ソフトウェアのバグ、共通パスワードの利用、初期設定のままセキュリティ強化をしていない状態、重要な資産を適切に保護せずに保持している状態、入退室管理の不備などがあげられます。悪気のない人の行為そのものが、脆弱性になることもあります。
脆弱性に合致する脅威が行われると、インシデントが発生します。
リスクとは、脅威によって脆弱性が利用されインシデントが発生したときに、システムあるいは組織に損害や何らかの影響を与える可能性のことです。リスクの大きさは、攻撃が実際に行われる可能性や、攻撃対象（情報資産）の価値、システムあるいは組織に与える被害の大きさなどによって、算出されます。

セキュリティ侵害による被害の軽減を組織的に図ることを「リスク・マネジメント」と呼びます。リスク・マネジメントでは、まずリスクを特定し、分析・評価したのち、そのリスクの対策方針を決定、方針に基づいて対策を選択し実行します。
リスク対策には、リスクそのものを制御する対策と、リスクには手を付けない対応の 2 種類があり、一般に、発生確率の高いリスクには、前者のリスク制御対策を講じます。
発生確率の高いリスクに対する制御対策のうち、ビジネスへの影響が大きいものは、インシデント自体が発生しないようにする「リスク回避」対策を、影響が少ない場合は「リスク低減（最適化)」対策を選択します。
「リスク低減」対策には、データの暗号化や、アクセス制御などがあります。
「リスク回避」には、脅威あるいは脆弱性の発生元である機器やサービスを使わない、停止するといった思い切った対策を含みます。
発生確率の低いリスクに対し、ビジネスへの影響が大きいものは「リスク移転」を、ビジネスに与える被害が小規模だと判断できるものは、対策を講じず放置する「リスク受容」を選びます。この 2 つの対応はどちらも、リスク自体の発生可能性を変化させません。「リスク移転」では、実際に被害が発生したときに備えて、代替手段の計画や保険、事前の予算確保を行っておきます。
このように、特定されたすべてのリスクへの対策の計画が立案され、対策が実施された後は、運用状況の監視を継続し、必要に応じて計画の見直しやリスクの再分析を行います。

ビジネスリスクと情報セキュリティの関係

情報セキュリティ計画を立案する際に、リスク分析は欠かせない作業ですが、ビジネスの視点が欠けた、IT 技術レベルのリスク分析に終わることも少なくありません。

「ビジネスにおけるリスク項目」でも述べたように、考慮すべきリスク項目は多岐にわたります。また、企業や組織ごとに脅威は違っており、必要とされる対策も異なります。このため、エンタープライズ・リスク・マネジメント（ERM）などのフレームワークに基づいたリスク分析が重要になります。情報セキュリティリスクと、企業レベルのリスクとの関連性を明らかにすることにより、経営全体の課題として、情報セキュリティ対策を捉えることができるようになります。なお、ERM に取り組む第一歩として、「ビジネスにおけるリスク項目」の表 2 と関連付けて分析することも効果的です。



Confidentiality（機密性）	Integrity（完全性）	Availability（可用性）
競合優位性の低下：競合の躍進、評判の低下 費用的な損失：損害賠償、営業機会損失 事業への影響：営業停止		
ストーキング 秘密の暴露 スパイ行為	システム誤作動 偽の発注・契約 紛争の誘発	システムの停止 社員間の連絡できない 社外との連絡できない 売上が立たない
利用状況の漏洩 画像・音声の漏洩 踏み台による漏洩	プログラム等の改ざん データの改ざん	プログラム等の改ざん 制御データの改ざん 通信経路の遮断
ソフトウェアの脆弱性 設定の不備 プロトコルや暗号の不備 ネットワークや通信の不備	運用上の不備 利用者による改造 認証の不備 ワーム・ウィルス	

図 1　ビジネスリスクとセキュリティリスクの関係（コミュニケーションシステム）

CISO は、組織全体のリスクを俯瞰して理解し、ビジネス目標に応じた内容となるように対応を行うことが望ましい。ガバナンスの一環として、組織全体の目標に従うようにセキュリティ対策を実施することが望ましい。

情報セキュリティ計画フェーズの実施モデル

セキュリティ計画を策定する際には、セキュリティから考え始めるのではなく、ビジネスコンセプトから始まる階層構造で考えることが必要です（図 2）。ビジネスコンセプトに従った、IT コンセプトを策定

し、その上でリスク分析に基づいた情報セキュリティコンセプトを策定することで、経営計画や他の事業計画との整合性のあるコンセプトを担保します。例えば、セキュリティコンセプトを実現するためのアーキテクチャや、計画を明確にするセキュリティプログラム、これを実施していくためのフレームワークとしてのセキュリティプロジェクトを計画し、より具体化していくために、セキュリティプラン、アクティビティ、タスクを計画します。

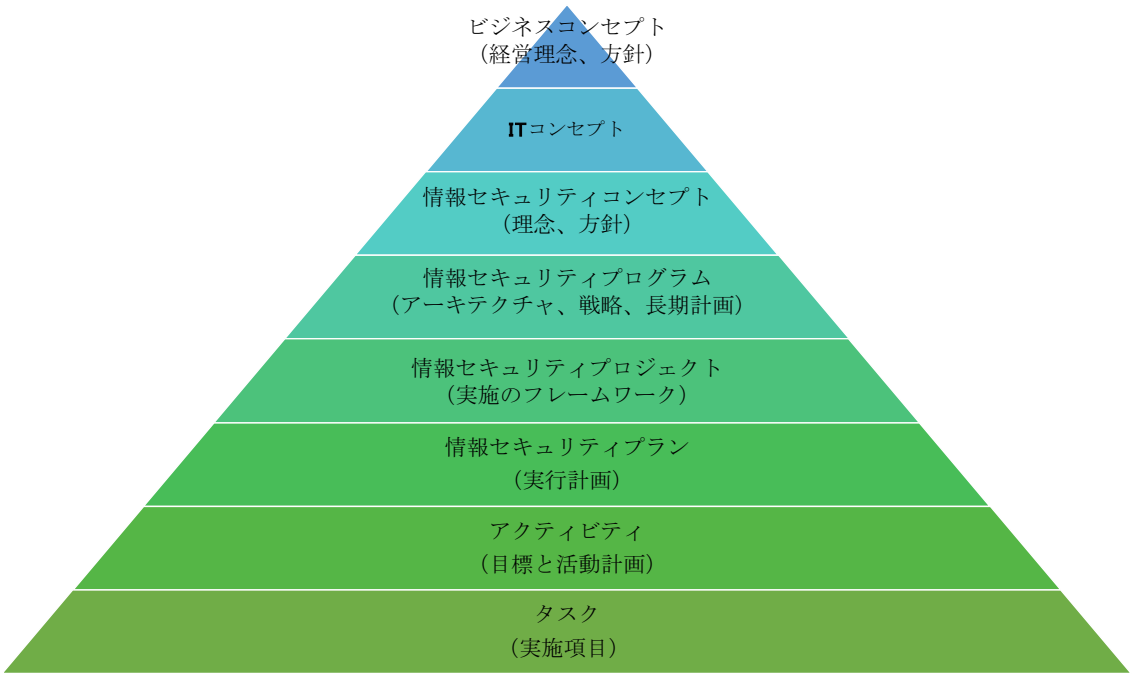


図 2 情報セキュリティ計画フェーズの実施モデル

実際にセキュリティ対策を策定する際には、必ずしもこのモデルを踏襲する必要はありませんが、階層モデルを利用することで、個々の計画が対象とする領域（階層）や粒度感を明確にし、それぞれの目標、KPI、計測手法の設定といった、マネジメントサイクルに沿った構造的な計画策定の一助となります。

CISO は、ビジネスコンセプトに沿った IT コンセプトとセキュリティコンセプトを CIO や他の経営陣と協力して構築することが望まれます。そのうえで、セキュリティコンセプトに基づいたプログラムを計画し、より具体化した上で実施することが望ましい。

情報セキュリティのフェーズ

多くの場合、セキュリティ対策はセキュリティ侵害（侵入）を防止することを中心としてきましたが、相次ぐセキュリティ事件の分析から、セキュリティ侵害を完全に防ぐことはできないと考えられるようになり、米国 NIST が提唱するサイバーセキュリティフレームワーク（図 3）に代表されるように、侵害

の防止（Pre-breach）だけではなく、侵害後の対応（Post-breach）が重要視されるようになりました。

サイバーセキュリティフレームワークのフレームワークコアは、「特定」、「防御」、「検知」、「対応」、「復旧」の５つのフェーズで構成されます。従来のセキュリティ対策は、「特定」（リスク分析・脅威分析）、「防御」（基本的なセキュリティ対策）に相当します。CSIRT（Computer Security Incident Response Team）業務は「検知」と「対応」、危機管理業務は「対応」と「復旧」に相当することが一般的です。CSIRT はより広い範囲で捉えている場合もありますが、本書では「対応」と「復旧」を主に CSIRT が扱うフレームワークコアとしています。

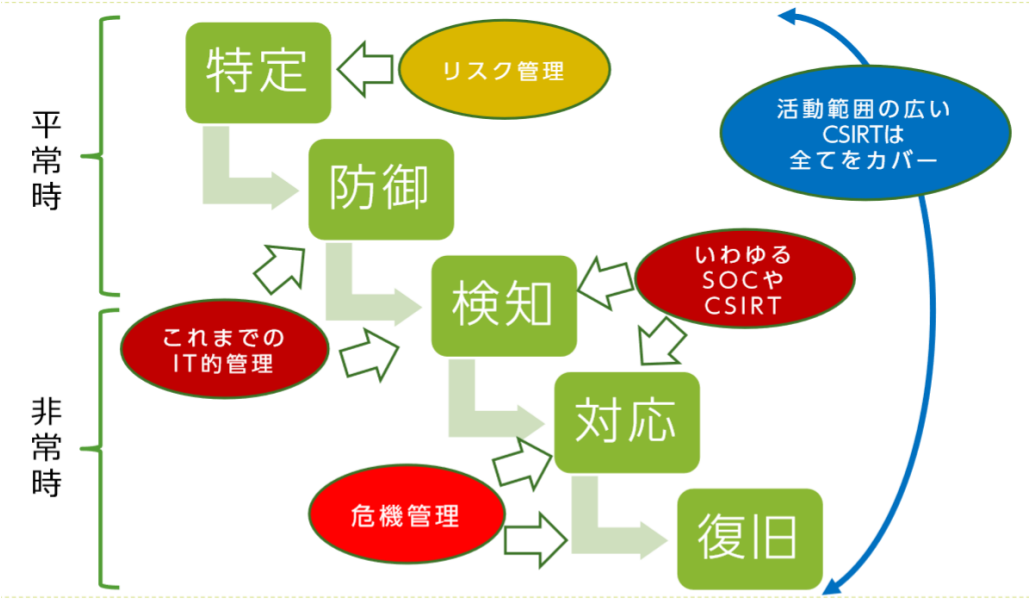


図 3 情報セキュリティのフェーズ（サイバーセキュリティマネジメント入門 [8]）

表 4　機能の一意の識別子とカテゴリーの一意の識別子（サイバーセキュリティフレームワーク[9]）

機能の一意の識別子	機能	カテゴリーの一意の識別子	カテゴリー
ID	特定	ID.AM	資産管理
		ID.BE	ビジネス環境
		ID.GV	ガバナンス
		ID.RA	リスクアセスメント
		ID.RM	リスク管理戦略
PR	防御	PR.AC	アクセス制御
		PR.AT	意識向上およびトレーニング
		PR.DS	データセキュリティ
		PR.IP	情報を保護するためのプロセスおよび手順
		PR.MA	保守
		PR.PT	保護技術
DE	検知	DE.AE	異常とイベント
		DE.CM	セキュリティの継続的なモニタリング
		DE.DP	検知プロセス
RS	対応	RS.RP	対応計画の作成
		RS.CO	伝達
		RS.AN	分析
		RS.MI	低減
		RS.IM	改善
RC	復旧	RC.RP	復旧計画の作成
		RC.IM	改善
		RC.CO	伝達

サイバーセキュリティフレームワークは、各フェーズのマチュリティ（習熟度）への着目と、Post-breachの重要性を明確に示した点に特徴があります。しかし、“既存のプロセスに取って代わるものとして作成されたわけではありません。企業は現行のプロセスをそのまま使用して、そのプロセスを本フレームワークにオーバーレイし、サイバーセキュリティリスクに対する現行の取り組みとのギャップを特定して、改善のためのロードマップを作成することができます。”（サイバーセキュリティフレームワークから抜粋）とされています。サイバーセキュリティフレームワークの各フェーズを構成する既存のベストプラクティス・規準などを表 5 で確認できます。

情報セキュリティ計画の策定においては、Pre-breach フェーズの対策だけではなく、Post-breach フェーズも計画に組み入れる必要があります。

表 5　フレームワークコアの一部（サイバーセキュリティフレームワーク[9]）

機能	カテゴリー	サブカテゴリー	参考情報
特定（ID）	資産管理（ID.AM）：組織が事業目的を達成することを可能にするデータ、職員、デバイス、システム、施設を特定し、事業目標と自組織のリスク戦略との相対的重要性に応じて管理している。	ID.AM-1：企業内の物理デバイスとシステムの一覧を作成している。	• CCS CSC 1 • COBIT 5 BAI09.01, BAI09.02 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8
		ID.AM-2：企業内のソフトウェアプラットフォームとアプリケーションの一覧を作成している。	• CCS CSC 2 • COBIT 5 BAI09.01, BAI09.02, BAI09.05 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8
		ID.AM-3：企業内の通信とデータの流れの図を用意している。	• CCS CSC 1 • COBIT 5 DSS05.02 • ISA 62443-2-1:2009 4.2.3.4 • ISO/IEC 27001:2013 A.13.2.1 • NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.AM-4：外部情報システムの一覧を作成している。	• COBIT 5 APO02.02 • ISO/IEC 27001:2013 A.11.2.6 • NIST SP 800-53 Rev. 4 AC-20, SA-9
		ID.AM-5：リソース（例：ハードウェア、デバイス、データ、ソフトウェア）を、分類、重要度、ビジネス上の価値に基づいて優先順位付けしている。	• COBIT 5 APO03.03, APO03.04, BAI09.02 • ISA 62443-2-1:2009 4.2.3.6 • ISO/IEC 27001:2013 A.8.2.1 • NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14
		ID.AM-6：すべての従業員と第三者である利害関係者（例：供給業者、顧客、パートナー）に対して、サイバーセキュリティ上の役割と責任を定めている。	• COBIT 5 APO01.02, DSS06.03 • ISA 62443-2-1:2009 4.3.2.3.3 • ISO/IEC 27001:2013 A.6.1.1

CISO は、ビジネスを前提としたセキュリティ対策を実施できるようにすることが望ましい。また、セキュリティのフェーズに応じた対応を計画および実施できるように体制づくりを行うこと。その際には、ベストプラクティスやフレームワークなどを参考にして、効率的に実施することが望ましい。

コラム：サイバー・キル・チェーン

サイバーセキュリティフレームワークと関連性の高い考え方に、サイバー・キル・チェーンという考え方があります。サイバー・キル・チェーンとは、Lockheed Martin 社が、情報システムへの攻撃シークエンスを 7 つのフェーズに分けてモデル化したものです[10]。

1. Reconnaissance（偵察）
2. Weaponization（武器化）
3. Delivery（配送）
4. Exploitation（攻撃）

5. Installation（インストール）
6. Command & Control（遠隔操作）
7. Action（目的の実行）

このサイバー・キル・チェーンの各フェーズで各々有効なセキュリティ対策を実施し、攻撃者が最終フェーズである Action（目的の実行）に到達する確率を下げようとする防御を、多層防御といいます。
早い段階でセキュリティ・イベントを検出できれば早期対応が可能になりますが、サイバー・キル・チェーンの初期のフェーズで観測されるイベントは、無害な一般イベントとほとんど変わらないため、セキュリティ・インシデントに結び付けるのは非常に困難です。
最近では、様々なイベントや情報を収集・分析し、こうした攻撃の予兆を探る脅威インテリジェンス・サービスが増えています。

情報セキュリティアーキテクチャ

多くの場合、セキュリティ対策は IT システムと独立して実装されています。例えば、IT システムに大きな変更を加えずに実装可能な、アンチウイルス、ファイアウォール、IDS/IPS、といったセキュリティ機能を中心とした実装です。このようなアプローチでは、セキュリティアーキテクチャ（設計思想、設計方法）は重要視されませんが、現在の複雑化した IT システムのセキュリティを効果的に構築・維持するためには、長期に利用できるセキュリティアーキテクチャが不可欠です。

セキュリティアーキテクチャが構築されないと、モグラたたきのような場当たり的な対策を積み重ねることになり、導入費用やメンテナンス費用の増加、運用の複雑化、さらに、これらを緩和するための追加投資が必要になるなど、高価で投資対効果の低いセキュリティ対策に終始する傾向があります。

具体的なセキュリティアーキテクチャについては、「情報セキュリティアーキテクチャと共通プラットフォーム」で述べていきます。

CISO は長期的に利用できる、セキュリティアーキテクチャを構築し、ライフサイクルを意識した情報セキュリティ計画を構築すること。計画が目的どおりに実行されていることを確認するための指標も策定することが望ましい。

経営サイクルと情報セキュリティ・マネジメントサイクル

情報セキュリティはいわゆるプロジェクトのような終わりがありません。組織が継続する限り情報セキュリティも継続する必要があります。このため情報セキュリティでは、PDCA を主要なマネジメント

サイクルとして活用することが一般的です。PDCA サイクルは Plan、Do、Check、Act の頭文字をとったもので、国内では計画、実行、評価、改善と訳して利用しています。

経営サイクルに沿って PDCA を考えると、当初の年度経営計画が Plan に相当し、これが逐次執行(Do)されます。そして、四半期毎の評価（Check)を経て、経営計画の修正などの Act が行われることで、合理的な業務執行が担保されます。中・長期の計画についても同様です。しかし、情報セキュリティにおける PDCA では、Check のフェーズがアンケートやヒアリングに終始することが多く、データなどの事実に基づいた評価が行われません。適切なセキュリティマネジメントを行うためには、データや事実に基づいた Check を行うこと、そして Plan そのものの合理性を評価することが重要です。

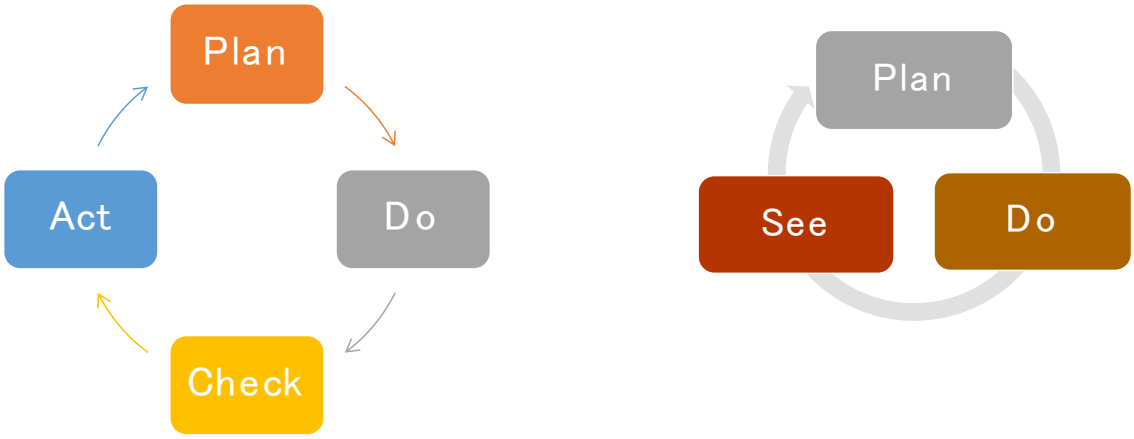


図 4 PDCA サイクルと PDS サイクル

また、PDCA は万能ではありません。例えば、プロジェクトマネジメントに PDCA を適用しても、うまく行かないことが多いようです。PDCA と似た考え方に、PDS(Plan、Do、See）があります。PDCA は年間計画などのマネジメントに向いた手法ですが、PDS は具体的な活動のマネジメントに向いたサイクルで、プロジェクト管理のように流動性が高い場合は PDS サイクルの方が適用しやすいと考えられます。

元々は航空戦の洞察に基づいた、指揮官の意思決定プロセスとして構築された OODA ループは、Observe（監視）, Orient（情勢判断）, Decide（意思決定）, Act（行動）の 4 つのフェーズで構成され、想定外の事態や緊急性の高い事態への対応を中心としたサイクルという特性があります。

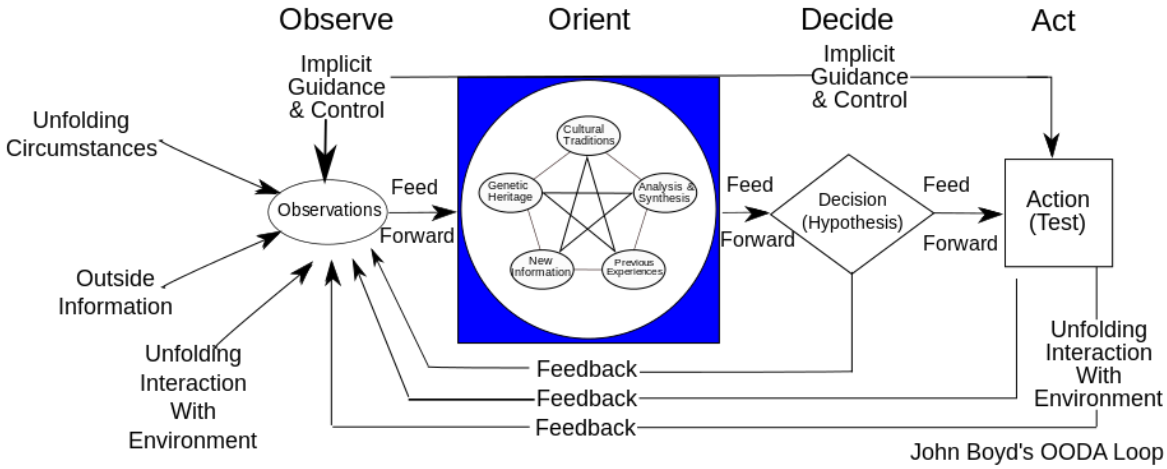


図 5 OODA Loop[11]

一方で、先に述べた米国 NIST サイバーセキュリティフレームワーク(図 3)では、Framework Core (フレームワークコア) として、Identify (特定)、Protect (防御)、Detect(検知)、Respond (対応)、Recovery(復旧)で構成するフレームワークを提唱しています。PDCA, PDS, OODA は汎用的なフレームワークですが、サイバーセキュリティフレームワークは、その名称の通りに、サイバーセキュリティに特化したフレームワークになっています。

情報セキュリティの分野では、一般に PDCA が基本とされますが、ひとつのフレームワークに固執せず、目的に沿ったフレームワークを選択することが必要です。

CISO は、これらのマネジメントサイクルを単なる改善だけではなく、企業としての学習と成長につなげていくこと。そのためにも情報セキュリティ計画を丹念に検討し、その評価を通じて事業部門、他部門、経営陣といったステークホルダーと協力を得ることが望ましい。

監査による執行状況の評価

情報セキュリティを経営リスクと捉えるならば、CISO が適切なタイミングに適切な情報を収集することは重要です。情報のなかでもシステムセキュリティに関する監査報告は、社内のセキュリティ実装状況を分析するための、最も有用な情報の 1 つです。

システムセキュリティ監査報告の重要性を例にとって述べてみます。

外部からの攻撃対策は優先順位を高くする必要がありますが、近年増加している標的型攻撃は、IPA から発表された「情報セキュリティ 10 大脅威 2018」[12]の「組織」区分 1 位にもなっており、多くの CISO が警戒している事象でしょう。

この標的型攻撃への重要対策として特権 ID の管理があります。特権管理者の権限が奪取されてしまうと、特権管理配下の権限はすべて掌握されてしまい、攻撃者の意のままに情報を外部に流出させられる危険が増すからです。特権 ID を守るための対策は、①特権 ID の付与を最小限にするなど 厳格なアクセス制御、そして、②特権を奪取されたら早く知るためのアクセスログの取得と突合せ監査が有効です。この 2 つの対策は、平常時からルール通りに運用されていることが重要であり、第三者の目で運用管理状況を確認する監査が機能することで形骸化を防止できます。

また、監査の報告が高品質であれば、組織の情報セキュリティ対策として経営層が重要と位置づけた施策が期待通りに運用されているかの正しい評価ができます。そのため、監査人が有効であると判断した場合、重要施策が適切であり有効である確証を CISO に与えることができます。

特に、連結決算対象の子会社も含めたグループ全体のセキュリティリスクを正しく理解するためには、IT の現業部門同士の情報連携だけに期待することは禁物です。なぜならば、個社の情報システムは個社ごとに特徴があるため、システムのレイヤーで詳細なリスクを連携するには限界があるからです。そのため、CISO 自らが積極的に個社それぞれから監査報告を求め、グループ全体のセキュリティリスクへの対応力を正しく理解する必要があります。

CISO には、組織全体を俯瞰し、限られた予算をどこに投じてリスクを低減すべきかの判断が求められます。もしも、優先度の高いシステムの改善や効果的な投資によるリスク低減ができることで、IT 投資の選択と集中やセキュリティ事件・事故の抑止が可能になれば、セキュリティを「本業にはならない、頑張っても収益につながらないコスト」ではなく、「競争優位性を獲得するための戦略の 1 つ」とすることができます。

経営サイクルの加速（ウォーターフォールから DevSecOps へ）

IT システム開発の世界では、長い間、製品リリースを主要なゴールとするウォーターフォールモデルが標準的な手法でしたが、計画から完成までに時間がかかり、ビジネス環境の変化への追従が難しい側面がありました。近年では、クラウドシステムに代表されるように技術・サービスの構築や提供方法が変化し、より速いサイクルでの開発や更新が可能になっています。

ビジネス機会を逃さないためには、リリース時だけでなく、運用後もユーザ・ニーズに迅速に応え、対応し続けることが必要です。このような経営目標に沿った IT システム開発手法として、多くの先進的な企業では、運用と開発を一体化した手法である DevOps を採用しています。また市場のセキュリティ要件が厳しくなればなるほど、セキュリティ対策の項目数・試験項目数が増加しますが、こうした要求に対して、DevOps 手法の全工程にセキュリティを組み込んだ DevSecOps 手法が、スピードアップとコスト削減の点から注目され始めています。

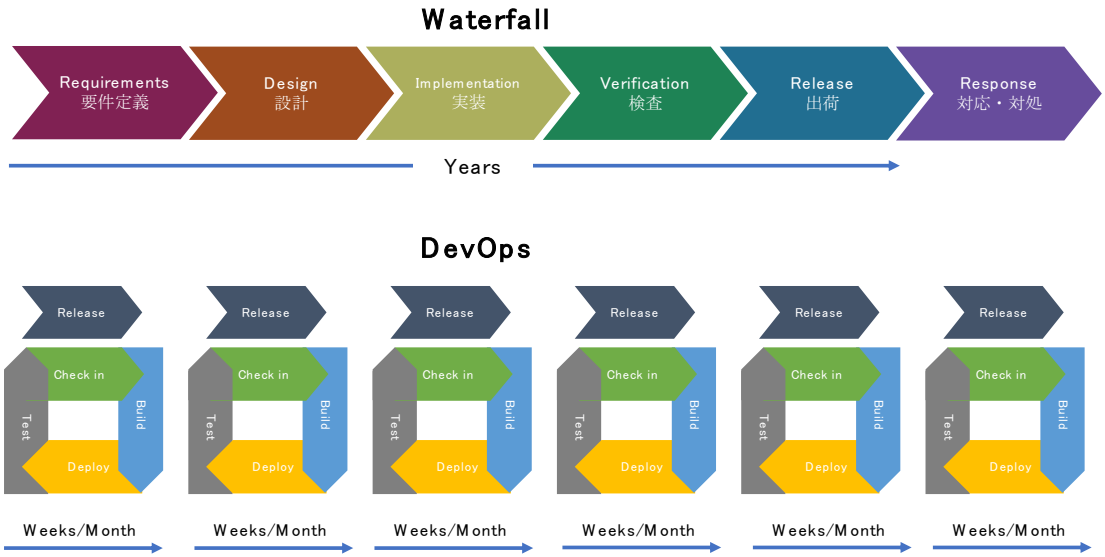


図 6 ウォーターフォールモデルと DevOps モデル

例えば、セキュリティ・パッチの適用は重要なセキュリティ対策のひとつであり、早期の実行が望ましい対策ですが、検証に時間を要するため、特に運用中のシステムへの適用は難しくなります。DevSecOps 手法では、テストの自動化によってパッチ適用の問題点を把握するまでの時間が短縮され、さらに仮想化技術やクラウドサービスを利用することで、パッチの段階的な適用や迅速な切り戻しを行えるようになります。こうして、パッチ適用の最大の課題である、システム安全性の担保を目指すことができます。

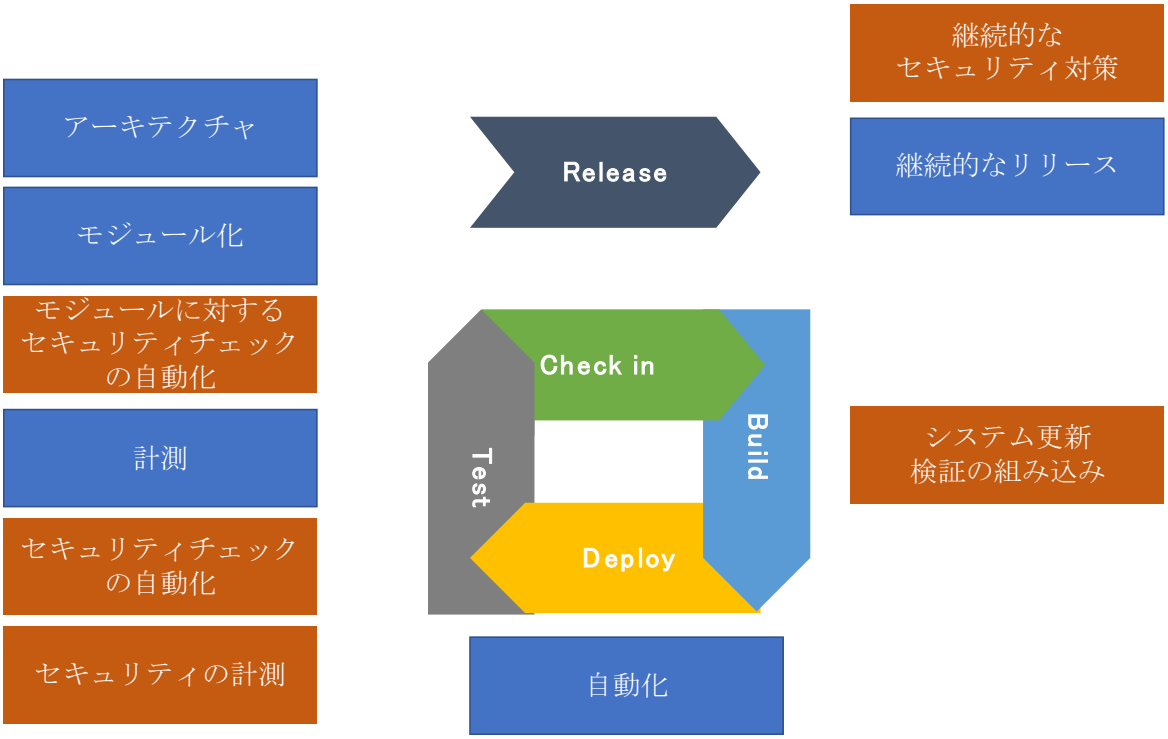


図 7　DevSecOps モデル

4. 基本となる経営指標

経営幹部への典型的な悪口に「数字しか見ていない」といったものがあります。技術の本質がわからず、表面的な数字を追うことで、必要な対策が実施できないと感じることもあると思います。しかし、経営における数字は共通言語とまで言われています。つまり、数字で計画し、数字で結果を評価することが、経営の本質と言っても良いのかもしれません。

経営における「数字」の重要性

経営者は情報セキュリティに対する理解が足りないと言われますが、経営者に情報セキュリティの詳しい知識が必要なわけではありません。経営者の役割はもちろん経営で、これを司っているのが売上や利益などの経営に関する数字です。外部のステークホルダーとのやり取りも経営に関する数字で行われます。つまり、経営者に情報セキュリティを理解してもらうには、数字に基づいたコミュニケーションが不可欠です。

CISO が経営陣の一員として業務を執行するためには、これらの数字を理解しなければなりません。良い仕事をしても、指標として数字に展開されなければ他の経営陣の理解は得られません。

財務会計

一般的に経営に関する数字というのは、財務会計における数字とされています。これらは、外部向けに提示するものであり、これまでのやり取り、つまり過去の数字と将来の目論見（計画）を示すもので、決算書や財務諸表に掲示されている数字がこれにあたります。主に株主が企業を評価する際に利用される数字として、半期、四半期を含む決算に関わる時期に公表されます。公表された内容によって株価が変動し、企業の時価総額などにも反映されます。

株価と経営

株価の上下は企業評価や資金調達の問題だけではなく、企業買収などの危機に関する指標にもなります。時価総額が極端に下がった場合、買収リスクが増大し、敵対的買収の可能性も高まります。敵対的買収が実施されると、経営権や事業に対する主導権を失い、事業の停止や解雇など、従業員に対しても大きな影響を与えることにつながります。また、敵対的買収の対策のために新たな対応と費用が必要となり、更に経営状態が悪化する要因となります。

このように、株価の変動は株主や経営者だけの問題ではなく、従業員を含めた全てのステークホルダーに影響を与えるものとなります。

管理会計

一方で、企業運営状況を表す内部向けの数字が管理会計の数字です。内部における様々な取り組みを評価し、見直しを行っていく際の指標となります。近年、管理会計は週次・日次など非常に短期間で管理され、ビジネスのスピードを速めるための一つのサイクルとして活用されています。

管理会計のサイクルが短縮された要員のひとつに、ERP（Enterprise Resource Planning）の普及を挙げることができます。ERP の普及により、実績評価を迅速に行い、速やかに予実のギャップを把握し、補正することができるようになりました。管理会計が適切に行われないと、大きな予実ギャップが突然明らかになり予想外の下方修正に至るなど、経営への信頼を失うことにつながります。

管理会計を適切に行うことで、事業の見直しと、財務会計における報告の修正などを適宜行い、経営への信頼が低下するリスクを低減することが期待されています。

数字と情報セキュリティ

これまでの情報セキュリティでは、主に情報系の IT システムが対象であることから、特別損失に関する数字が中心で、事業計画に対しては、想定されるマイナスの影響（BI：Business Impact）が指標とされてきました。

しかし、IoT や Fintech では、IT は情報系システムではなく、ビジネス基盤となる基幹系システムであり、情報セキュリティも同様に、ビジネス基盤という視点で捉える必要があります。つまり、特別損失などの負のインパクトだけではなく、売上や経常利益といった主要な経営指標を考慮することが求められます。情報セキュリティの対象が、企業の業績そのものとることで、情報セキュリティに関する数字は、管理会計、財務会計に関わることになります。

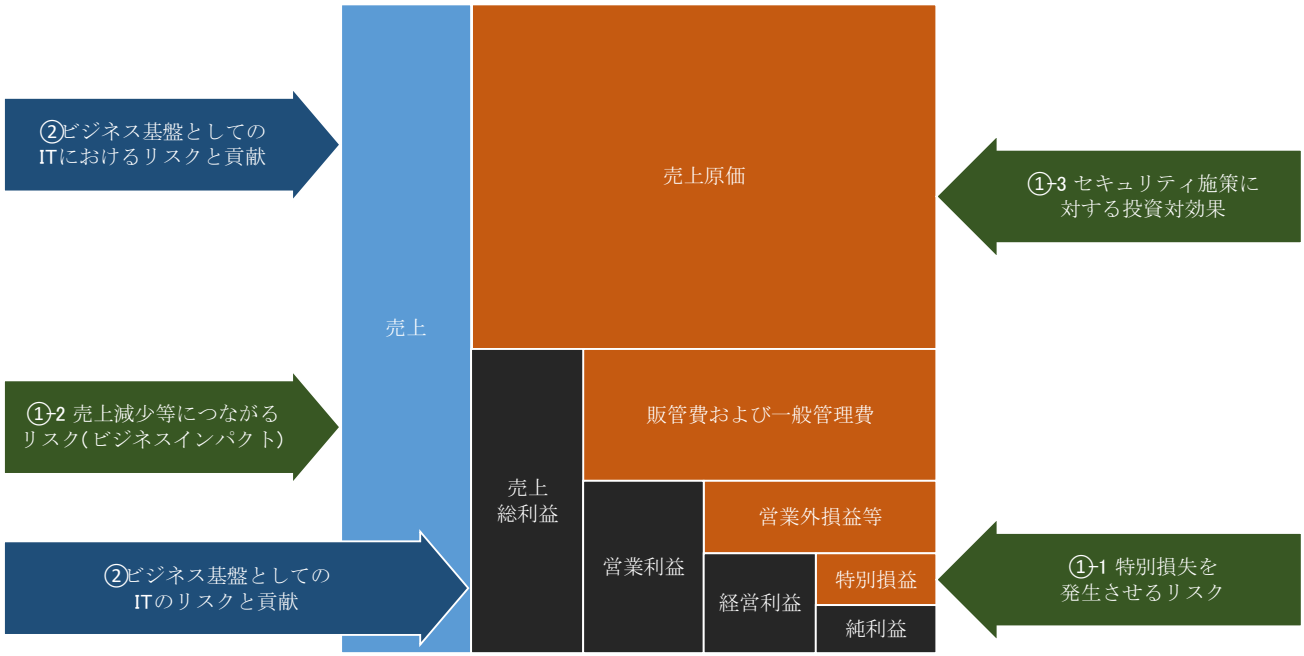


図 8 経営の数字

CISO は、経営の基盤となる会計についての基本的な理解を通じ、経営へのかかわりを深めること。損失への対策だけではなく、セキュリティを通じて、売上や利益に貢献する視点でも取り組むことが望ましい。

5. 情報セキュリティの指標化

情報セキュリティは特別損失を未然に防ぐもの、という視点で考えた場合、情報セキュリティの投資対効果を経営の数字とすることは難しいかもしれません。損失を主題とした考え方は、実際には発生していない事故を想定し、想定事故のリスク（想定損害額×発生確率）と対策に必要な費用などを比較します。しかし、実際には発生していない事故なので、施策が事故を未然に防いだのか、そもそも事故が発生しなかったのかを評価することは難しい面があります。

一方で、事業計画に沿ったセキュリティという考え方では、事業計画を実現し、業務の効率化や競争力を獲得するためのセキュリティとしての見方で、事業目的に沿った数字として指標化することが可能です。以下に働き方改革としてテレワークを導入するケースを例に、セキュリティの指標化について考察します。

情報セキュリティ指標を経営の数字に展開

働き方改革でテレワークサービスを提供する場合、損失を中心とする考え方では、テレワークを提供することで生じる新たなリスクに応じた対策を実装すると考えます。これに対して、事業計画に沿う考え方では、テレワークを導入することで実現しようとしている目標や成果を考えます。そして、求められる成果と必要とされるセキュリティ対策を明らかにしていきます。

一般に、対策の効果を計測するために KPI(Key Performance Indicator)が利用されますが、KPI の関係性、重要度、優先順位が不明瞭となる傾向があり、本来のビジネスゴールではなく、KPI そのものが目標になりがちです。このよう状況を回避し、ビジネスゴールと KPI の関連性を明らかにし、構造的なフレームワークを構築する手法のひとつとして、バランスト・スコアカード（BSC）[13]を挙げることができます。

バランスト・スコアカードでは、目的を達成するために「戦略目標」を決め、「重要成功要因」を決定し、「重要評価指標」を設定します。具体的な目標を「ターゲット」として設定しつつ、どのような行動を取ればよいかを「アクションプラン」として策定していきます。これらの 5 つの要素をさらに、財務、顧客、業務プロセス、学習と成長という 4 つの視点で整理し、関係性を明確にすることで、目標達成のための要因管理ができるようになります。

図 9 では、売上高を増大させるという財務視点の戦略テーマを、革新的な製品を顧客に提供するという顧客視点の戦略テーマで実現しようとしています。革新的な製品は、新製品の市場への投入サイクルを高めることで維持し、そのために能力の高い従業員を維持するという戦略です。

視点	戦略テーマ	戦略目標	目標値	実施項目
財務の視点	売上高増大	年々の売上伸び率	＋25%	×
		新製品からの売上	30%	×
顧客の視点	革新的製品	顧客の定着率	80%	関係管理の実施
		顧客のシェア	40%	成果給の導入
内部の視点	新製品開発	市場への投入率	75%	見本市での出展
		市販の時期	9ヶ月	BPRの実施
学習の視点	能力の高い従業員	専門職の利用可能性	100%	教育・訓練
		優秀な職員の保持率	95%	給与制度の改革

図 9　戦略テーマ、戦略目標、目標値、実施項目（出典：わが国の公的機関における効率性と有効性の必要[14]）

これを、戦略マップと呼ばれるダイアグラムとして、本書が書き起こしたものが図 10 です。表として整理する場合と比較して、各項目の関係性をよりダイナミックに記載することができます。

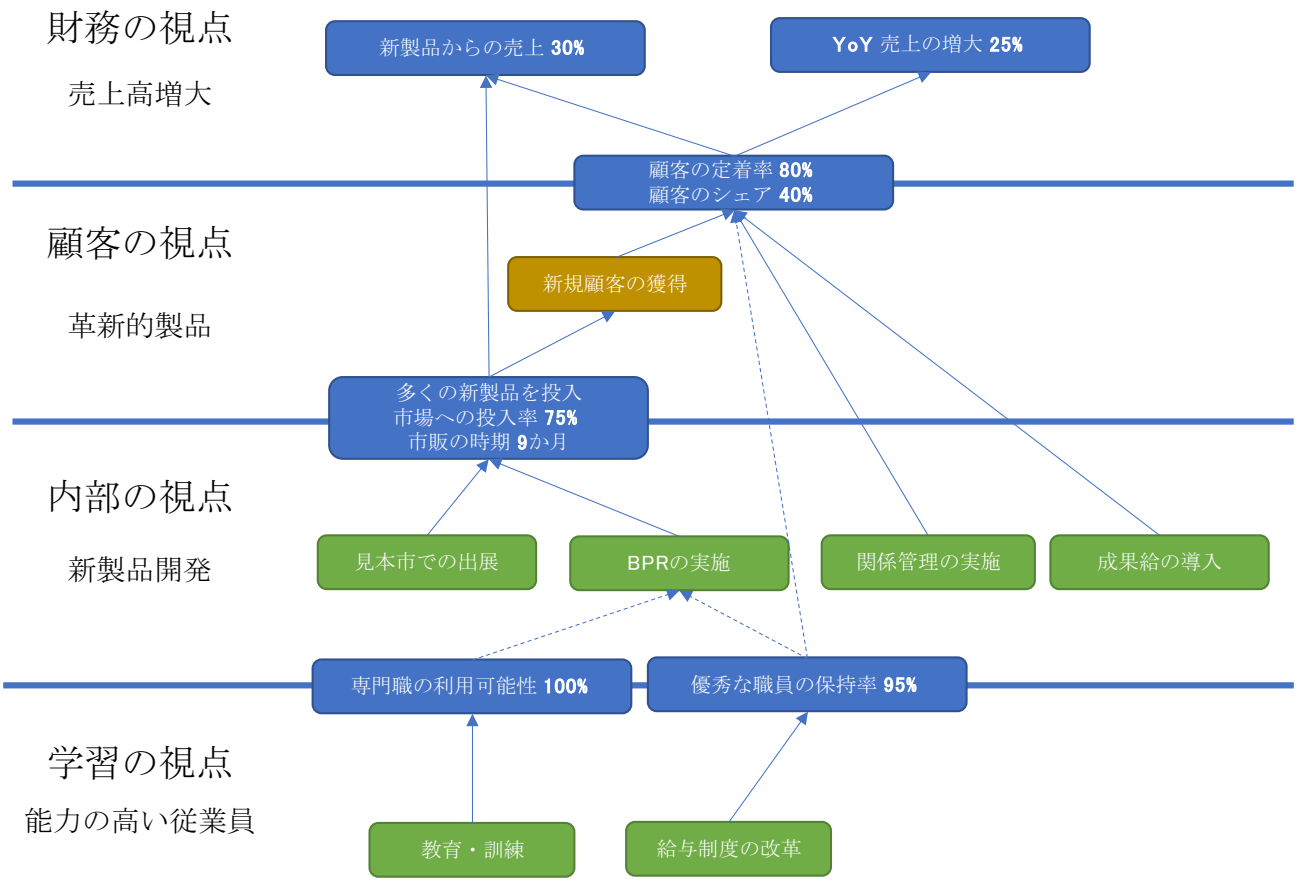


図 10　バランスト・スコアカード　戦略マップ

ケーススタディ:テレワークを題材としたバランスト・スコアカードの利用例

ケーススタディとして、図 10 の戦略マップに、テレワークの導入を加えたものが図 11 です。この図では、テレワークを導入することで、経営戦略に以下の貢献ができることを示しています。

- 介護や育児などで定時勤務が難しい従業員が無理せずに働けることで、「優秀な社員の保持率 95%」と、「専門職の利用可能性 100%」に貢献する。
- 教育の機会を広げることにより、「専門職の利用可能性 100%」に貢献する
- 場所と時間を問わないことで「関係管理」を効果的に実施する。

これにより、テレワークの経営戦略上の位置づけが明らかになります。それぞれに、具体的な数値目標を設定すると、計画をより明確なものにすることができます。

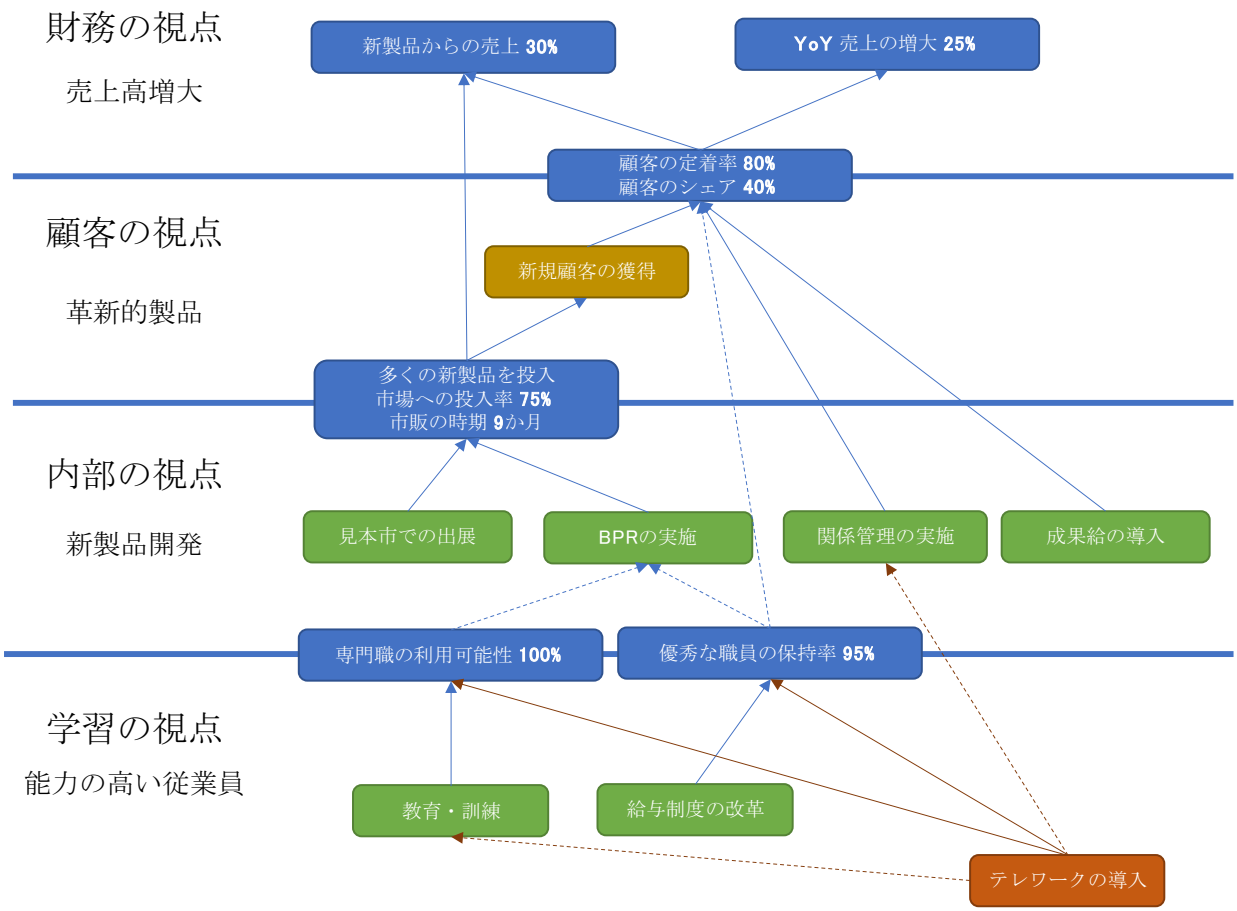


図 11　バランスト・スコアカード　戦略マップ-テレワークの導入

次に、テレワークを実施する上での考慮すべき脅威について分析します。

- 端末などの紛失・盗難など
- 通信経路や作業環境からの盗聴・情報搾取
- 作業端末への不正アクセス・マルウエア感染
- サーバなどへの不正アクセス・マルウエア感染

これらの脅威に対する対策が実施されていない場合、追加のセキュリティ対策を実施します。原則として、IT アーキテクチャ、セキュリティアーキテクチャに則った対策を行うようにします。

この作業を通じて、テレワークに期待する効果、想定されるリスク、対策コストが明らかになり、セキュリティ対策のコストを、事業計画と結びつけることができるようになります。

表 6　バランスト・スコアカードにテレワークを組み込んだ例

	戦略目標	重要成功要因 重要評価指標	ターゲット	アクション
財務	売上高増大	年々の売上伸び率 新製品からの売上	+25% 30%	
顧客 (従業員)	革新的製品	顧客の定着率 顧客シェア	80% 40%	関係管理の実施 成果給の導入
業務 プロセス	新製品開発	市場への投入率 市販の時期	75% 9 ヶ月	見本市での出展 BPR の実施
学習	能力の高い従業員	専門職の利用可能性 優秀な社員の保持率 テレワーク環境の構築	100% 95% -50% (平均処理時間)	教育・訓練 給与制度の改革

（参考）

会計監査院：　テレワークや在宅勤務における情報セキュリティ対策の現状と論点[15]

総務省：　テレワークセキュリティガイドライン[16]

CISO は、事業計画を理解し、情報セキュリティ対策の有効性について会計上の数字との関連を明確にすること。その際には、財務会計と管理会計の指標を明確にすることが望ましい。

経営的な目標に沿ってセキュリティ施策を位置付け、施策を計画するにあたっては、計測可能な指標化を行い、各経営指標との関連付けを明確にすることが望ましい。

経営陣の一員としてセキュリティを考える場合、コーポレートガバナンスについても取り組む必要があります。COSO（トレッドウェイ委員会組織委員会：Committee of Sponsoring Organizations of the Treadway Commission）が発行した、内部統制フレームワークでは、セキュリティガバナンスは 3 つの目的カテゴリー（業務活動、財務報告、法令順守）と、5 つの構成要素（統制環境、リスク評価、統制活動、情報および伝達、モニタリング）でモデル化されています。

セキュリティは法令順守を中心に考えられることが多いと思いますが、COSO モデルは、業務活動および財務報告といった目的設定も重要であることを示しています。

セキュリティ計画策定の最も上流にあたるリスク分析においても、3 つの目的カテゴリーが重要です。法令順守のリスクばかりではなく、業務活動のリスク、財務報告のリスクについて、分析と評価を行う必要があります。

コーポレートガバナンスにおけるセキュリティガバナンスの位置

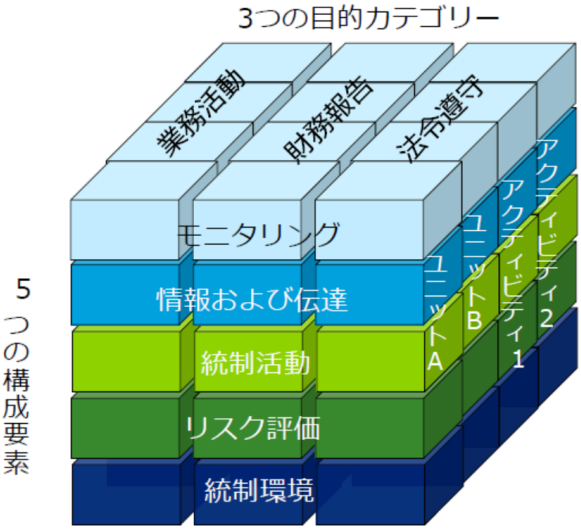


図 12　COSO の活用

経営における情報セキュリティの役割

コーポレートガバナンスについても、経営レベルの数字としてみていきます。先に述べたバランスト・スコアカードの考え方は、IT セキュリティをコーポレートガバナンスに関連付け、財務的な数字とするための有用な視点を提供します。

図 13 は、セキュリティとコーポレートガバナンスをバランスト・スコアカードに展開した例です。現状で実施ができている項目は赤色で示されており、他の部分については十分に検討ができていない項目

として記載しています。バランスト・スコアカードへの展開を通じて、関係部門と具体的な項目についてコミュニケーションを図ることは、コーポレートガバナンスに沿った包括的なセキュリティ計画と実装に寄与します。

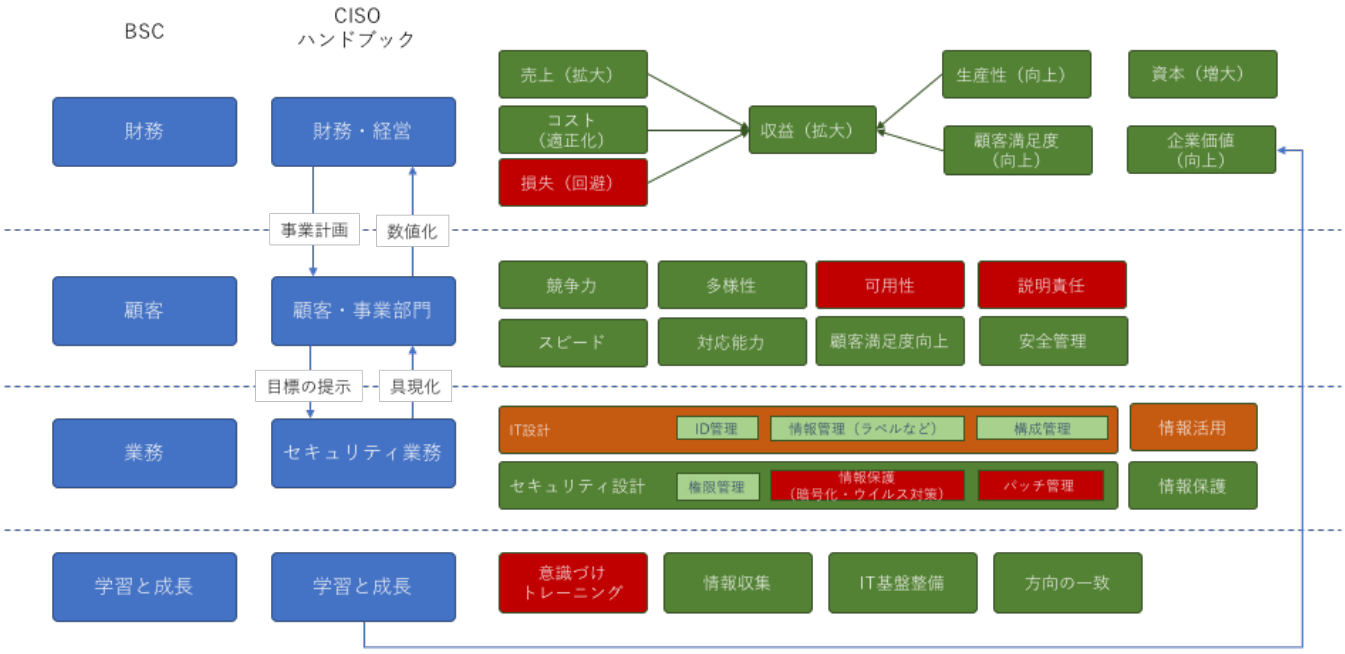


図 13 バランスト・スコアカードを参考にした指標と業務づくりの例

CISO は、経営における情報セキュリティの役割を理解し、業務執行を行うこと。業務における各員の役割と責任を明確にすること。情報セキュリティ対策をビジネスと業務に組み込み、他部門とのコミュニケーションや包括的な情報交換を日常的な活動とすることが望ましい。

情報セキュリティに対する役割と責任

ビジネス目標に対して、セキュリティが貢献するための考え方について述べてきましたが、ここでは各人の役割と責任について取り上げます。

経営陣は、コーポレートガバナンスや ERM という立場から、他のリスクと同様にセキュリティに対する最終的な責任を負うことになりますが、経営陣が直接施策を実施するわけではありません。担当部門へ指示し、報告を得ることで施策を実施します。CISO は、経営陣の一員として、セキュリティに対する業務執行を担当し、自らの部下やスタッフ、また関係する他部門に対して、施策を指示し報告を得る必要があります。

一般に、スタッフレベルでは、コーポレートレベルで想定しているリスクが伝わらず、ネットワークのアクセスコントロールなどの具体的・技術的な内容に偏り、目的と手段が混同することも少なくありません。効果的なセキュリティ施策を実施するためには、経営目標の実現に向けた差配が必要です。

セキュリティに関わる組織構成・組織運営については、IPA「サイバーセキュリティ経営ガイドライン解説書[17]」に詳しく述べられています。

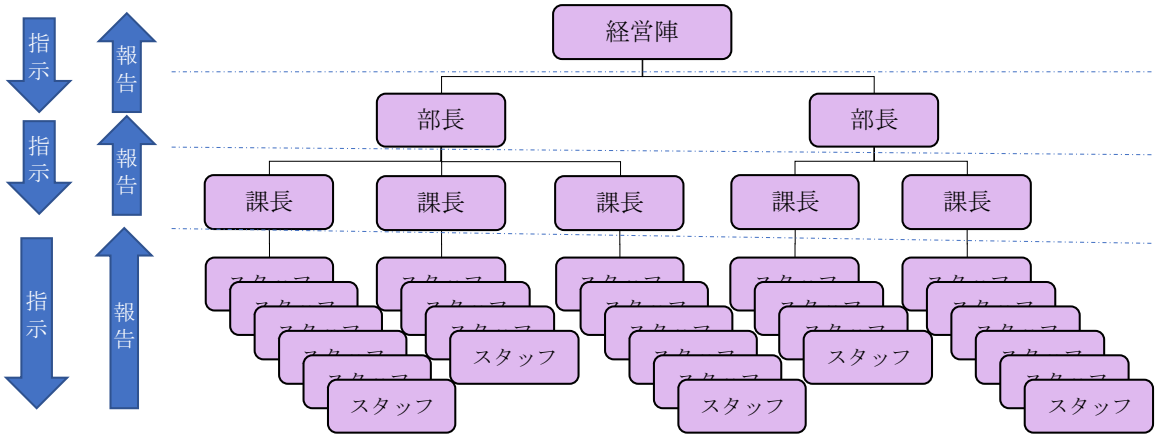


図 14 報告と責任の関係

CISO は、情報セキュリティにおける各人の役割を理解し、それを実行できるような環境構築を行うこと。情報セキュリティポリシーの策定と見直しを繰り返し行い、情報セキュリティ対策が実行可能かつ有効な状態を維持することが望ましい。

6. 情報セキュリティの評価とモニタリング

平常時の評価と指標

CISO を業務執行という視点でとらえた場合、経営会議で何を報告するかを考える必要があります。多くの場合、セキュリティポリシーに対する順守率（Protection condition）が指標とされますが、この視点では、自組織がどのような脅威に直面しているかを把握することができません。例えば、セキュリティ更新の適用率とマルウェア対策の利用率が 100%だとしても、いわゆる APT(Advanced Persistent Threat)などの執拗な攻撃に直面していれば安全な状況にあるとは言えません。このため、Protection condition だけではなく、自組織がどのような攻撃に直面しているかを Attack Condition として把握する必要があります。

Protect condition, Attack Condition に加えて、侵入を許した兆候(Suspicious activity）と、脅威を誘発する可能性(Indirect activity)を指標としてまとめたものを、本稿執筆グループでは CISO ダッシュボードとして提案しています（別紙：CISO ダッシュボード)。

CISO ダッシュボードの主要な報告要素

- Attack condition
  どの程度の攻撃に直面しているのか（＝検出しているのか）
- Protection condition
  対策の状況は計画通りか（Assurance の領域）
- Suspicious activity
  侵入を許したか、その可能性はあるか（内部犯行の可能性を含む）
- Indirect activity
  PC の紛失、建屋への侵入、人事上のトラブルなどの状況（間接的な懸念事項）

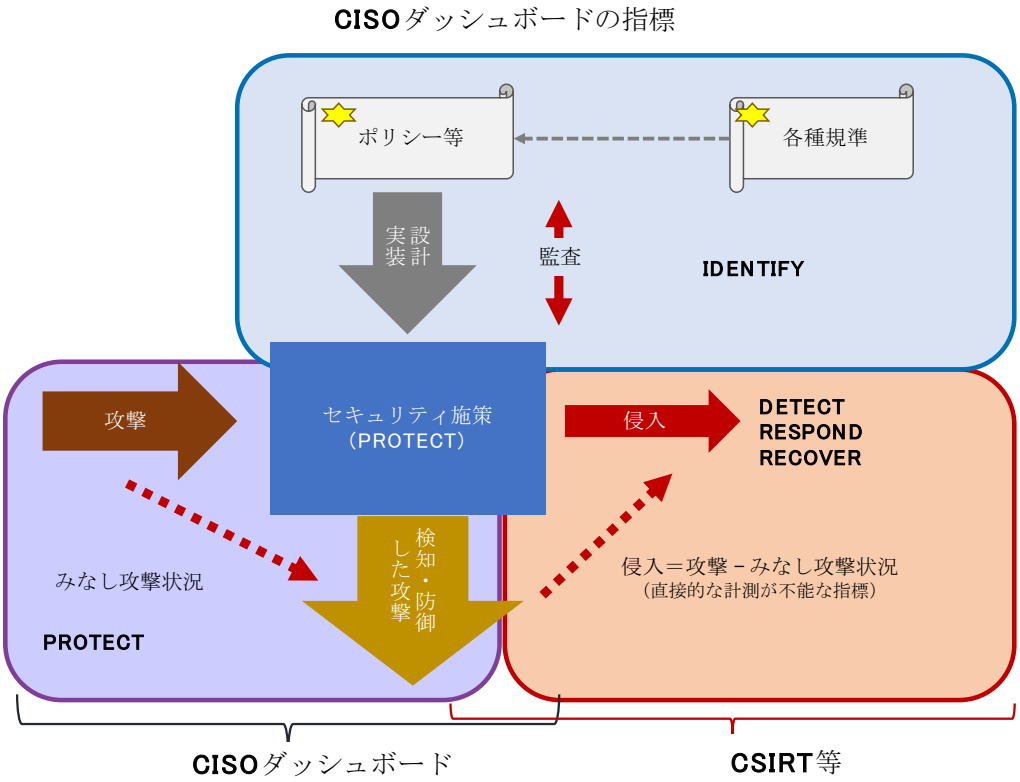


図 15　CISO ダッシュボード

表 7　CISO ダッシュボードに基づいたセキュリティ報告書のイメージ

セキュリティ報告書（XX 年度 XX 月　経営会議向け）

項目	備考		
Attack condition	技術的	2	弊社を狙ったと思われる攻撃メールが、XX 月 XX 日-XX 月 XX 日にかけて、SPAM フィルターと AV で検知された。総数は、23 件で、開発の特定部門に集中している。現段階では、全てブロックできたと判断しているが、警戒を続ける必要がある。
	概況的	1	海外で大規模なインシデントが報道されているが、報道を見る限り対策済みの手法と判断される（別紙１）。
Protect condition	技術的	2	先月から配布された PC のキッティングに問題のある事が判明。既に回収をしているが、まだ最終確認がとれていない。XX 月 XX 日までに終了予定。一部業務に影響が出るが、協力いただきたい。
	概況的	1	ネットワークデバイスへの深刻な脆弱性 xxx が報告されているが、弊社では該当するデバイスを使用していないことが確認されている（参考資料 2）。
Suspicious activity	技術的	3	外向けの通信に、不審な接続先との通信が記録されている。詳細を分析中だが、大規模な調査が必要となる可能性がある。上記攻撃メールとの関連も疑われるため、早急な調査が必要。分析を早め、より効果的な防御を行うため精度の高いブラックリストの入手が効果的と考えている(別紙 2：決済申請)。
	概況的	2	大規模なアカウント情報の漏洩が続いている。標準システムでは二要素認証を強制しているが、IT 基板側に脆弱なアカウントがないかを確認している。
Indirect activity	技術的	2	1 台の PC と、2 台の会社貸与スマホが紛失。リモートワイプで対策済み。
	概況的	2	データベース保守を担当するベンダーが懲戒解雇となっている。プロシージャに沿ってアカウントなどの停止を実施した。

決済事項	疑わしい通信が観測されているが、対処の必要性を判断するにあたり、十分な精度とスピードが確保できない。この課題を解決するために、精度の高いブラックリストの購入を申請する（別紙 2：決済申請）
報告事項	XX 年度 YY 月で決済を受けた分析システムは、XX 月の中旬から試験稼働を始めている。ZZ 月までには試験稼働と評価を終了し、本格的な稼働を始める予定。
その他	セキュリティトレーニングを未受講の社員が２０名ほど残っている。上司にあたる役員を CC した上でリマインドを行うので、部下のトレーニング受講に協力頂きたい。 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」が公表され、注目されている。当ミーティングでコピーを配布する。

情報セキュリティにおける説明責任

CISO は、経営における説明責任を理解し、それに応じたセキュリティに関する報告を行うことが望まれます。報告のタイミングは、「経営会議」、「決算発表」、「事故発生時」などが想定されます。特に事故が発生した場合や事故の前兆がある場合は、その影響や原因、再発の有無についても説明できるように事前の準備が必要です。このためには、他社の事故を自社に置き換えて分析し、適切な対応ができるかを検証することも効果的です。なお、事故発生時の対応については、「8 情報セキュリティ・インシデント対応と報告」で詳しく取り上げます。

表 8　事故発生時に想定される発表内容と担当などの確認

想定される発表内容	担当などの確認
事故の概要	責任者（CEO, CIO, CTO, CSO, CISO 等）
影響を受ける顧客数と特徴	報道対応
想定される二次被害	事故調査、まとめ
顧客などに推奨する対策	法的な検討
事故の原因・要因	顧客対応
事業への影響の有無	その他
再発防止策	

CISO は、企業の IT 活用の目的や効果について理解し、セキュリティがこれを大きく侵害することがないように、セキュリティ計画を策定すること。また、セキュリティの指標を決定し、計測する際には、同時に IT における指標についても計測し、侵害がないことを確認することが望ましい。

7. セキュリティのための IT 基盤設計

情報セキュリティアーキテクチャと共通プラットフォーム

これまでに述べたように、経営とセキュリティの関わりを理解し、企業全体の IT 設計・実装にセキュリティを組み込むためには、基本となるアーキテクチャ（設計、設計方針）が不可欠です。基本となるアーキテクチャは、一般にエンタープライズ・セキュリティ・アーキテクチャ（ESA）と呼ばれ、多くの機能が利用する共通プラットフォームを構築します。ESA では、GRC（Governance, Risk, Compliance）とオペレーション全般にわたる広い範囲を扱うことになり、共通プラットフォームとアプリケーション・システムを組み合わせて実装を行うことになります。

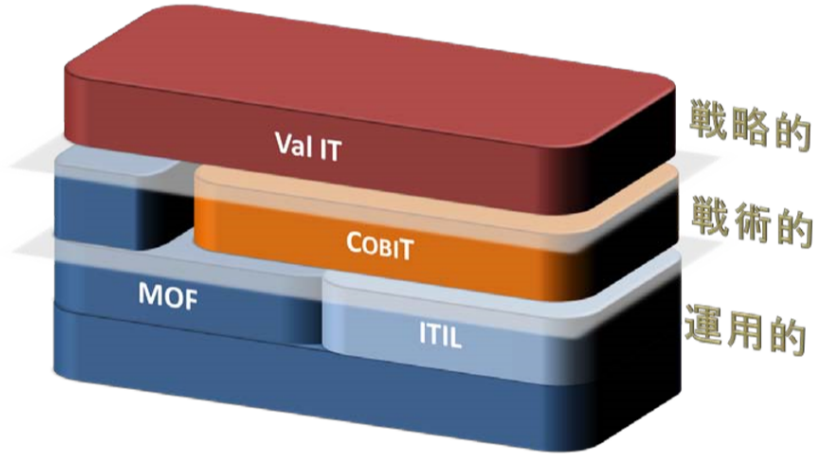
表 9　共通プラットフォームの例（IT とセキュリティのアーキテクチャ）

- インベントリ管理/構成管理
- Id マネジメントとアクセス制御（権限管理）
- 監査（ログ）とモニタリング
- 暗号サービス
- システム統制

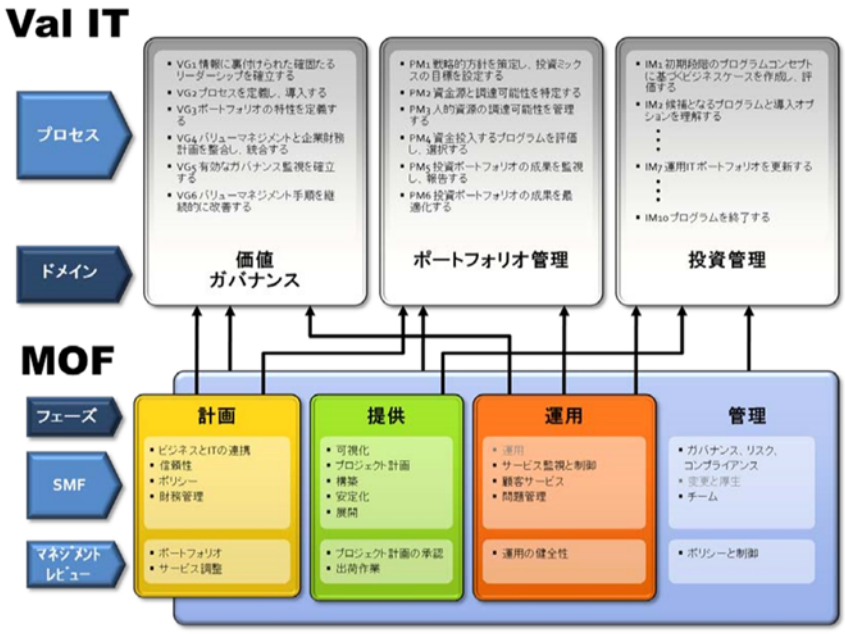
GRC とオペレーションを一貫したアーキテクチャとして構築する試みとして、マイクロソフト社では、戦略的なフレームワークとして Val IT、戦術的なフレームワークとして COBIT、運用的なフレームワークとして ITIL と、IT 運用の具体的な技術指針 Microsoft® Operations Framework（MOF）と呼ばれるフレームワークで構成される ESA として開発・運用しています。

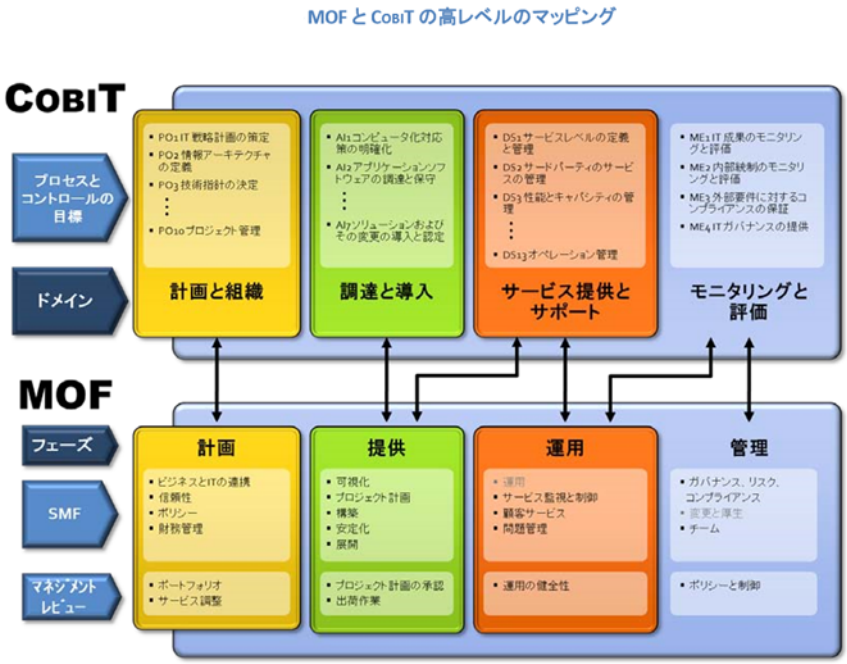
ケーススタディ：Microsoft® Operations Framework（MOF）

IT の運用は、このような多くの要件への準拠を証明しながら、サービスを管理しなければならないという課題に常に直面しています。これらの要件は、本質的にガバナンス、リスク、コンプライアンス（GRC）に分類されますが、多くの組織では COBIT および Val IT ガバナンス フレーム ワークを採用して GRC のニーズに対処しています。しかしこれらのフレームワークは、一般的な企業や IT のガバナンスの指針を示すように設計されているため、IT の運用に必要な具体的な運用上および技術上の指針は示していません。MOF が品質と信頼性の高いサービスの提供という日常的な IT 運用に GRC の機能を統合する重要な役割を果たせるのが、このような分野です。つまり、MOF によって、全体的なサービス管理ライフサイクルに GRC 機能を組み込むための要素が IT 運用にもたらされます。



MOF と Val IT の高レベルのインターフェイス





出典：MOF と COBIT/Val IT の比較および クロスインプリメンテーション ガイド[18]

CISO は個々の情報セキュリティ対策が機能していることを評価する軸を策定し、それを計測するための基盤や環境を構築することが望ましい。

セキュリティを内包したIT基盤設計の方針

CISOは、経営戦略、事業戦略を適切に展開するため、セキュリティアーキテクチャに基づいたIT基盤の構築を、CIOなどと協力をしながら進める事が望まれます。IT基盤において基本的なセキュリティを担保するための主要なIT要素として、リスク分析とリスク把握、IAAAに基づいたアクセス制御、情報分類（データクラシフィケーション)、権限管理、ネットワークアクセス制御、統制基盤、モニタ（総合ログ管理）について考察します。

リスク分析

IT基盤にセキュリティを組み込むためには、リスク分析に基づいたセキュリティエンジニアリングを構築する必要があります。「ビジネスにおけるリスク項目」でも記載していますが、情報セキュリティリスクが、事業運営や経営に与える影響を十分に理解してリスク分析を行う必要があります。

IAAAに基づいたアクセス制御

セキュリティ対策の主要な取り組みとしてアンチウイルス対策やファイアウォールの設置などが挙げられますが、セキュリティ対策の基盤となるのはIAAA(Identification, Authentication, Authorization, and Auditing)に基づくアクセス制御の概念と実装です。

IAAAを実装するには、部門単位の調整だけではなく、組織全体にわたる調整が必要になります。つまり、経営陣としての方針策定と調整が必要です。

往々にして、利用者は必要以上に高い権限を求めます。しかし、不用意な権限の付与はIAAAによるアクセス制御の実効性を低下させます。最小権限の原則を維持するためには、経営陣としての判断や調整が求められるとともに、IAAAに基づいたコントロールを容易にするITアーキテクチャ設計が必要です。例えば、権限を各IDに割り振るのではなく、IDにロール（職務、役割）を紐づけ、ロールに基づいた権限を付与することで、権限付与の根拠を明確にし、人事異動などの変化に対して柔軟で自動的な対応ができることが望まれます。

また、近年のクラウドサービスなどの普及により、外部サービスの利用機会が増えていますが、外部サービスの利用においては、統一的なId管理とアクセス制御を適用が、より重要なセキュリティ施策となります。

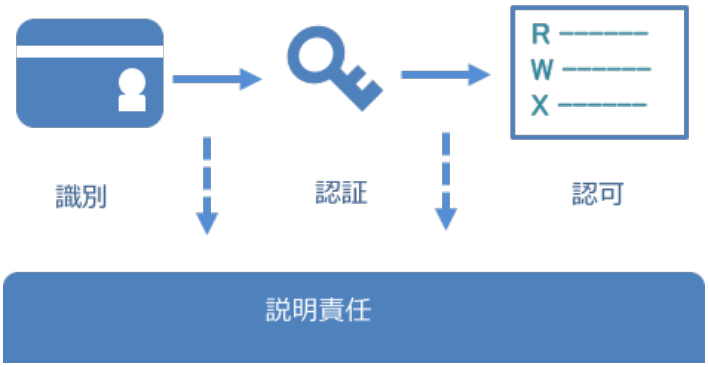


図 16　IAAA の概念

CISO は、IAAA がセキュリティの本質であることを理解すること。権限管理を適切に反映できる ID 基盤を設計、構築することが望ましい。

情報分類（データクラシフィケーション）

情報の保護はセキュリティ施策の主要な目的の一つですが、保護レベルを上げるに従い、使い難く、利用コストが高いものになります。例えば、重要な機密ファイルへのアクセスや、Active Directory などのディレクトリシステムの操作を、社内の特定の端末に限定することは現実的ですが、日常的に利用される全てのデータへの同様の制限は現実的ではありません。また、過度の制限を実施すると、従業員が独自の IT 環境を利用するシャドーIT を誘発する可能性が高まります。適切な保護策を実施するためには、情報の重要度や機密性などに基づいて情報を分類し、そのレベルに応じた保護策を策定する必要があります。

CISO は、組織内または組織に関わる人員が、情報資産を正しく理解できるように分類指針を構築すること。また、情報資産を利用する人員についても分類し、情報管理における権限設定が円滑に行われるようにすることが望ましい。
参考：NIST　SP800-60　「第 I 巻：情報および情報システムのタイプとセキュリティ分類のマッピングガイド」[19]

権限管理

経営陣や役職者に対して、ドメイン・アドミニストレータなどの管理者権限（特権）が付与されているケースがありますが、権限は職位ではなくロール（職務）に基づいて付与します。特権アカウントは、操作ミスの影響が大きいだけではなく、マルウェアに感染した際には、全社に深刻な影響を与える可能性が高まります。特権には、大きな責任が伴うことを理解する必要があります。

バックアップなどの特定のオペレーションに対して、管理者権限を付与する場合もみられますが、これ

も同様の理由から望ましくありません。バックアップに必要な権限だけを付与するようにします。また、特権を常時付与するのではなく、作業が必要な時に付与し、規定の時間後に自動的に特権を消すことも効果的な対策で、特にシステムメンテナンスを外部の業者に委託している場合に有効な対策です。

CISO は、役職（職位）に基づいた権限付与ではなく、ロール（職務）に基づいた権限付与をすることで、人員の異動など役割の変更に一貫性を持った対応ができる仕組みづくりを構築すること。最小権限を原則とし、必要に応じて権限の分離なども検討すること。そのために CIO や HR（人事）とのコミュニケーション図り、時宜を得た、または定期的な棚卸しを行うことが望ましい。

物理的・ネットワーク的なアクセス制御

物理的な分離を基盤としたネットワークアクセス制御は、信頼できるネットワーク（セキュリティドメイン）を、比較的容易に構築できることから、中心的なセキュリティモデルとして利用されてきました。

一方で、通信環境の進展に伴い、自宅や外出先からの社内ネットワークへの接続が一般化し、クラウドサービスの利用により、社内ネットワークで利用していたサービスを社外ネットワークに移行するなど、閉じたネットワークの維持が難しくなっています。加えて、社員の WiFi ルーターやティザリングによる想定外のインターネット接続、標的型攻撃におけるマルウエア（RAT）のセキュリティドメインを越えた通信にも配慮する必要があり、物理的・ネットワーク的なセキュリティドメインに頼った対策だけでは対処できないケースが増えています。

例えば、近年では利用が一般化しているクラウドサービスを利用する場合は、ネットワークによるセキュリティドメインの構築や、IP アドレスに基づいたアクセスコントロールが利用できない場合も少なくありません。このため、多要素認証を含んだリスクベースの IAAA がより重要視されるようになっています。

CISO は、IT 環境の変化に応じた対策を計画、立案、実施できるような仕組みづくりを常に考慮することが望ましい。

統制基盤

PC やスマートフォンなどの多数のデバイスを、個別に管理することは現実的ではなく、一貫したセキュリティ対策を担保することは出来ません。企業レベルでセキュリティ対策を実施するためには、ハードウェアやソフトウェアのセキュアな設定、セキュリティ・パッチの適用、マルウェア対策ソフトウェアの更新などを実施するための、統制基盤を構築する必要があります。

また、近年、インベントリ（棚卸、状況の把握）の重要性が改めて指摘されており、SANS「The CIS Critical Security Controls for Effective Cyber Defense」[20]や、「サイバーセキュリティフレームワーク[3]」

においても、最重要項目としてデバイスとソフトウェアのインベントリが取り上げられています。インベントリ管理を行う上では、統制基盤を利用した自動化されたインベントリ管理が重要となります。

SANS CIS

- CSC1:　許可されたデバイスと無許可のデバイスのインベントリ
- CSC2:　許可されたソフトウェアと無許可のソフトウェアのインベントリ

サイバーセキュリティフレームワーク

- 資産管理（ID.AM）：組織が事業目的を達成することを可能にするデータ、職員、デバイス、システム、施設を特定し、事業目標と自組織のリスク戦略との相対的重要性に応じて管理している。

CISO はセキュリティ施策を展開し維持するために、セキュリティ施策が自動的に適用され、計測が行える統制基盤を構築することが望ましい。

統合ログ管理

ログを収集することは重要ですが、各機器や PC などのデバイスログを個別に収集をしていたのでは、効果的なモニタリングを実施することは困難です。SIEM(Security Information Event Management)のように、イベントの収集分析に特化したソリューションを導入することも効果がありますが、統制基盤に基づいたログやイベントの収集をログ管理の基盤とすることが望まれます。

CISO は個々のシステムのログを単独で扱うのではなく、統合的に収集管理ができる統合ログ管理基盤を構築することが望ましい。

継続的な技術動向の把握

常に変化する IT 環境、ビジネス環境でセキュリティレベルを維持するためには、最新の技術動向や、脅威状況を把握する必要があります。日々のニュースを収集するだけではなく、例えば CISSP などの評価の高い包括的な資格の取得や、日本シーサート協議会（NCA）に参加し、他社のセキュリティ担当者との情報交換を行うことも有益です。

コラム：CISO が考慮すべきログ対策

いざインシデントが発生したら、CISO は情報セキュリティを統括する責任者として、経営層やステークホルダー（お客様や株主など）に説明をすることになります。そのとき、ステークホルダーを納得させるだけの情報を提示できるかどうかは、インシデント対応の中でも重要なポイントとなり、CISO の腕の見せ所ともいえます。

高度化・巧妙化するサイバー攻撃を検知するため、様々な対策手法が研究・開発されていますが、それでも 100%検知できるわけではありません。攻撃者に侵入され、長期にわたって情報窃取されていても気づけない組織が多い中、外部からインシデントの通報があった際に、事実関係を調べ、影響範囲を把握し、説明責任を果たすことができるだけの備えとしてログ対策の重要が注目されています。事実関係を特定するための情報が足りないと、説明責任を果たすことが難しくなるだけではなく、ビジネスインパクトを過大評価・過小評価することにもつながりかねないことにも注意が必要です。

また、サイバー攻撃だけではなく、内部不正も忘れてはなりません。組織内にある情報の価値を理解し、正規の権限を持って行われる内部不正については、適切なアクセス制御や ID 管理などの対策も重要ですが、無用な犯人探しや冤罪を避けるためにも、事実関係を記録し、発覚した時点で確認できる備えが必要となります。

このほか、法規制要件の変化、クラウドサービスのログ取得（従来のオンプレミスシステムと同じ手法ではログ取得ができないケース）など、環境の変化に合わせて柔軟なログ対策が求められるようになってきています。

場合によっては機密情報が含まれるかもしれないログをどこまで取得し、どれぐらいの期間保管するのかなどの運用設計が必要となるログ対策は、決して簡単なことではないものの、ログの重要性を再認識し、本格的に対策に取り組む組織も増えています。

本ハンドブックでは、具体的にどういった内容を説明すべきかのサンプルをご紹介していますが、あなたの組織では、いざという時に、報告すべき情報を提示できるだけのログ対策を行っているでしょうか？

サイバー攻撃対策におけるログの活用については、JPCERT/CC から提供されている「高度サイバー攻撃への対処におけるログの活用と分析方法」、ログ管理全般の実態については、IPA による「企業における情報システムのログ管理に関する実態調査」に詳しく記載されていますのでご参照ください。

（参考）

JPCERT/CC 高度サイバー攻撃への対処におけるログの活用と分析方法[21]

IPA 「企業における情報システムのログ管理に関する実態調査」報告書について[22]

8. 情報セキュリティ・インシデント対応と報告

情報セキュリティ・インシデントと CSIRT の設置

近年、セキュリティ侵害（アクシデント）はビジネスそのものに大きな影響を与えるようになっています。セキュリティ対策の主要な目的は、アクシデントや、アクシデントにつながるインシデントの抑制にありますが、適切な対策を実施したとしても、これを無くすことは出来ません。

このため、サイバーセキュリティフレームワークでも述べられているように、インシデントの発生を前提とした、インシデント検出と対応を行う体制の構築が求められます。このようなインシデントをハンドリングする社内組織は、CSIRT（Computer Security Incident Response Team）と呼ばれ、その重要性が増しています。CSIRT の活動は、必ずしも事後的なものに限らず、インシデントの防止・被害の低減を行うための活動も含まれます。

インシデント対応においては、CSIRT が具体的なインシデントハンドリングを担当し、CISO はビジネスへの影響を考慮した、経営陣、顧客、関連省庁などの内外のステークホルダーとの調整と対応が主な役割となります。

具体的なインシデントハンドリングについては、NIST SP800-61 「コンピュータセキュリティ インシデント対応ガイド 」[23]、JPCERT/CC「高度サイバー攻撃（APT）への備えと対応ガイド ～企業や組織に薦める一連のプロセスについて」[24]などを参考にしてください。

CISO は、CSIRT を設置し、これを監督すること。CSIRT の規模は組織の規模によって異なるため、グループごとにリーダーを設置するなどして、円滑な情報交換ができる様な組織とすることが望ましい。

コラム：イベントとインシデント、アクシデント

JISQ27000[25]では、インシデントとは、ある「事態」を示す言葉とされています。事業運営や情報セキュリティに影響を与えたり脅かしたりする可能性のあるインシデントのことを「セキュリティ・インシデント」と呼びます。

インシデントは、1 つ以上の事象で構成されています。この事象のことは「イベント」といいますが、その中でも特にセキュリティ・インシデントと関係のあるイベントを「セキュリティ・イベント」と呼びます。

被害をもたらしたインシデントのことを「アクシデント」といいます。

例えば「メールを受信し、添付ファイルを開いたら、ウイルスに感染した」というという一連のイベントがもたらす事態はセキュリティ・インシデントですが、その結果、データが破壊されるなど業務に支障をきたす被害を引き起こしたインシデントは、アクシデントに分類されます。

1つのアクシデントの前にはアクシデントに至らなかったインシデントが29件発生している（ハインリッヒの法則）と言われます。こうしたインシデントをいち早く検出して対応することが、アクシデントを防ぐことにつながります。そして、インシデントを早期に検出するためには、イベントの監視が欠かせません。

インシデントを想定した施策の事前評価

インシデント対応を遅滞なく行うためには、対応手順を事前に用意することが不可欠です。緊急時にひとつひとつ対応を検討していては、迅速な対応ができず状況を悪化させることになります。一方で、対応手順が策定されていても、事前に確認作業や訓練を行っていないと、インシデント対応手順が現実的ではない場合が多く、また、担当者や経営者の役割と作業の実効性は期待できません。

対応手順の合理性を検証し、それぞれの役割と対応手順の確認するためには、インシデント発生を想定した机上演習が効果的です。机上演習は、対応手順の検証だけではなく、セキュリティ施策そのものの評価を行い、経営陣を含めたステークホルダーの役割を確認することができます。

演習では、具体的なインシデント/アクシデント（表 11）が発生した場合に、想定される発表内容が適切に用意できるか、対応はそれぞれ誰が行うのかを確認します（表 10）。

より具体的な内容については、Annex C インシデントを題材にしたトレーニングとして記載しています。

なお、初めてこのような取り組みを行う場合は、IPA の「情報漏えい発生時の対応ポイント集[26]」などが参考になります。

表 10　想定される発表内容と担当などの確認（再掲）

想定される発表内容	担当などの確認
事故の概要 影響を受ける顧客数と特徴 想定される二次被害 顧客などに推奨する対策 事故の原因・要因 事業への影響の有無 再発防止策	責任者（CEO, CIO, CTO, CSO, CISO 等） 報道対応 事故調査、まとめ 法的な検討 顧客対応 その他

表 11　想定インシデントの例

	インシデント	情報元/受付部門
1	標的型攻撃で機密情報が漏れた可能性があることが、外部からの連絡で判明した	JPCERT/CC
		CSIRT
2	ハッカーの侵入を受けて、すべてのメールがインターネットに公開されたと連絡が入った	メディア
		広報
3	WEB ページから顧客情報が閲覧可能な状態にあると連絡	個人（匿名）
		広報
4	自社にしか登録をしていない「メールアドレスに広告が入った」とのクレームが、今日になって入った	顧客
		ユーザサポート
5	顧客から、弊社にしか登録をしていない「クレジットカードが勝手に使われた」とのクレームが入った	顧客
		ユーザサポート
6	インターネット上の掲示板に弊社の顧客情報を含むドキュメントが掲載されている	取引先
		担当営業
7	自社が所有する IP アドレスから攻撃を受けているとのクレームが入った	取引のない海外企業
		ユーザサポート
8	自社のメールアカウントを使った、標的メールが取引先に送信された	官公庁
		大代表→広報
9	業務システムから、機密情報が社外に持ち出された	官公庁
		大代表→広報

10	サービスで提供をしている Web サーバが、ミドルウエアの脆弱性を悪用され、改ざんをされた	官公庁 大代表→広報

CISO は、時宜を得た情報収集を行うことを心がけ、判断が明確にできるような環境を構築すること。インシデントなどの概要を経営会議で報告するだけではなく、これらの情報から得られたビジネスに与える影響を、経営陣が判断の根拠となる数字や事実として明らかにし、必要に応じて取組みの改善などを提案することが望ましい。
それぞれの組織において、セキュリティの実務を担当するものには教育やトレーニングの機会を提供し、外部の情報だけではなく、内部の情報を利用したセキュリティ計画を構築できる環境を構築することが望ましい。

コラム： 脆弱性診断、ペネトレーションテスト、レッドチーミング

脆弱性診断（Vulnerabilities Assessment）は、診断対象システムの、既知の脆弱性の有無を調査します。
ペネトレーションテスト（Penetration Testing）は、脆弱性診断で見つかった脆弱性に対して、実際に攻撃（Exploit）を試行します。

レッドチーミングは運用中のシステムに対して、企業・組織の特徴や特性を考慮し、独自手法や最新から古典的な手法まで、有効と考えられるあらゆる攻撃手法を用いて、実戦さながらに計画・準備された一連の攻撃が、通告なしに実行されます。
ペネトレーションテストは剣を振り回しながら派手に襲いかかる海賊、レッドチーミングは闇に紛れてこっそり行動する忍者に例えられたりします。

ペネトレーションテストがシステムに着目するのに対し、レッドチーミングは、組織内のセキュリティ・リスクを能動的に洗い出す演習です。対象システムの技術的な対策の不備だけでなく、計画、体制、設備、関係者の動きなど、組織の総合的なセキュリティ耐性と攻撃検知力・対応力のレベルと課題とを明らかにする実効性の高い手段であり、組織のセキュリティ総合評価であるともいえます。
企業は、定期的にレッドチーミングのようなセキュリティ演習を行い、その評価結果を組織のセキュリティ強化や人材育成計画の検討に活用することができます。最近では、自社内にレッド・チームを設置し、日常的に自社システムを攻撃し、製品やサービスのセキュリティ品質の維持と向上につなげている企業が増えています。
（参考）Penetration Test vs. Red Team Assessment: The Age Old Debate of Pirates vs. Ninjas Continues[27]

レッドチーミングの例として、イギリスの中央銀行（Bank of England）が主導している CBEST という取り組みがあります(CBEST Intelligence-Led Testing CBEST Implementation Guide[28])。CBEST は金融当局主導で金融機関にレッドチームテスト的な内容を実施するもので、同等の考え方がイギリス外への展開や、金融業界以外の業種への派生が議論され始めています。レッドチーミングとして珍しくドキュメントも公開されています。

9. 経営陣としての CISO への期待

これまで見てきたように CISO は経営視点で業務を執行することが求められており、経営陣としての責任と権限を有しています。経済産業省の「サイバーセキュリティ経営ガイドライン」[(2)]では、経営者が認識すべき 3 原則と CISO などに指示すべき 10 の重要事項を示しています。CISO は多岐にわたる情報セキュリティ全般の責任者であることが期待される立場であり、自社のセキュリティ状態を把握するための体制、仕組みを作り、他の経営陣に対して適切な提案や報告を行い、運用フェーズにおいては計画した施策の進捗状況や、自社のセキュリティ状況の報告が必要です。またリスク項目の定期的な見直しと、その結果に応じた計画の修正も行う必要があります。

セキュリティ施策の推進には、経営層、ビジネス推進部門、管理部門などを中心に、社内のあらゆる部門との連携が必要です。各部門にはそれぞれの目標が、目標とその計画に対して事前にセキュリティプログラムが組み込まれることが望まれます。各部門と日頃よりコミュニケーションをとり、各部門の状況を理解するとともに、セキュリティプログラムの重要性を啓蒙する必要があります。

コミュニケーションにおける注意事項 相手の立場を理解すること、セキュリティ中心に技術的な用語は極力避けること。特にセキュリティは IT や事業推進の効率化などの阻害要因と取られる場合もあり、その必要性、目的を丁寧に説明すること。 リズム・オブ・ビジネス（Rhythm of Business）や事業計画や目標の理解、数字、評価指標などを織り交ぜることにより共通言語での相互理解が望ましい。

経営会議での報告

経営会議での定期的な報告は CISO に求められる重要な責務であり、経営陣を啓蒙する最大の機会でもあります。経営会議では数字に基づいた報告が一般的であり、セキュリティダッシュボードのような数字をベースとした報告フォーマットを策定し、ビジネス的視点から、自社の現状、世の中の脅威状況、自社への影響についての評価をまとめ、必要に応じて技術的な補足をすることが望まれます。推進しているセキュリティプログラムの進捗状況についても、単に進捗状況を伝えるのではなく、ビジネス的視点から影響を判断し、課題と対応策を提示するようにします。フォーマットや報告内容は、他の経営陣とのコミュニケーションを通じて充実を図るようにします。

経営陣はセキュリティや IT の素養が不足している場合も少なくありません。経営会議への参加を通じて、経営陣に対するセキュリティの啓蒙を行い、セキュリティを企業の文化としていくことも CISO の重要な役割です。また、CISO は、他の経営陣の報告から各部門の状況を読み取り、ビジネス状況を理解するとともに、自らにかかわる課題を理解し、速やかに対応することも重要です。

CISO は経営陣の一員として経営会議で、セキュリティダッシュボードなどを使い、自社のセキュリティの現状と今後の計画について、他の経営陣がわかりやすいように報告を行うこと。また、経営会議を経営陣の啓蒙の機会とし、セキュリティを企業文化として根付かせる努力をすることが望ましい。

財務会計部門との連携（CFO）

CFO は、リスク分析とセキュリティにかかわるビジネスインパクト評価、セキュリティ施策予算と評価など、CISO の業務に深くかかわります。CISO は CFO と組織が保有するエンタープライズ・リスクとセキュリティ投資のバランスを共有するなど、密接な連携をとることが必要です。加えて、セキュリティ侵害が発生した場合の予算執行や、保険によるリスクの転嫁なども事前に協議してください。

一方で、エンロン事件を受けて制定された SOA（Sarbanes-Oxley Act Section 404）[(6)]に見るように、会計業務は、企業の最も重要なオペレーションであり、外部からの侵害ばかりではなく、社内からの不適切な行為に対しても対策を行う必要があります。CISO は CFO と連携し、予算の計画や執行にかかわる業務フローを明確し、適切で適法な会計処理を担保する必要があります。

財務会計システムは企業にとって極めて重要なシステムで、法律やガイドラインに従う必要がある。CISO は CFO と連携を取り適切な会計処理を担保し、エンタープライズ・リスク、緊急時の対応予算などについても、CFO と連携をとって進めることが望ましい。

業務部門との連携（COO）

ビジネスを推進している事業部門との協力関係、支援体制の構築は、ビジネスに貢献するセキュリティを推進する上で不可欠な取り組みです。ビジネスリスクについては、COO とセキュリティ事故事例に基づいた自社ビジネスへの影響を議論することで、共通認識を醸成することも重要です。

事業部門が持つ課題や、将来の展開を理解することで、よりセキュアなオペレーションの提案や、セキュリティプログラム、セキュリティアーキテクチャの見直しを通じて、競合優位性などのビジネスメリットを提供するセキュリティ施策の検討を進めます。

また、医療関係や金融関係など、業種によっては高いレベルのコンプライアンスが求められる場合があります。CISO はこのようなビジネス特有の環境と動向に配慮し、COO と連携をすることで、ビジネスが競争力を保つための取り組みが必要です。

セキュリティはビジネスの足かせと考えられることが少ない。COO とのコミュケーションを通じて、セキュリティ対策によるリスクの軽減だけではなく、ビジネスに対する貢献について、共通の理解を構築することが望ましい。

IT 部門との連携（CIO）

情報セキュリティ対策、運用はその多くが IT システム上に実装されることになります。合理的な IT 環境を構築し、効果的なセキュリティ対策を実装するためには、「情報セキュリティ計画フェーズの実施モデル」で述べたように、ビジネスコンセプト、IT コンセプトに基づいた、情報セキュリティコンセプトの構築が必要です。加えて、「セキュリティのための IT 基盤設計」で述べた情報セキュリティアーキテクチャを構築するためには、IT 部門の代表である CIO の理解が不可欠です。システムの構築、既存システムの改版、新規システムの導入の際にも、CIO と協力をしながら、セキュリティアーキテクチャに基づいたセキュリティ要件を組み込むようにします。セキュリティの要件の実装は IT 部門が実施するケースも多いことから、予算や作業の分担についても十分な連携が必要です。

運用フェーズでは、セキュリティ対策が IT パフォーマンス低下や、システム停止など、IT 運用と相反する事態も発生します。また、セキュリティ・インシデント対応時には、IT 部門とセキュリティ部門の協力が不可欠です。CISO と CIO は、IT システム構築時にこれらの懸念事項を共有し、あらかじめ緊急対応手順書の作成などを通じて懸念事項と対応手順を明らかにし、緊急対応体制を構築することが望まれます。

IT システムおよびセキュリティシステムが、ビジネスの展開を支えることで、事業部門と協力をしながら、お互いの成果となるように連携することが望ましい。

リスク管理部門との連携（CRO）

「ビジネスにおけるリスク項目」で述べたように、情報セキュリティリスクは、エンタープライズ・リスクの一要素として捉える必要があります。エンタープライズ・リスクの多くは、直接的・関節的に情報セキュリティと関連があります。CISO は CRO とエンタープライズ・リスクについて協議し、リスクの洗い出し、リスクの回避、低減、受容、移転について協議します。一見、IT に関係のないリスクにも、情報セキュリティによる対策が効果的なこともあれば、物理的な対策が IT リスクへの効果的な対策となることも想定されます。

IT システム、企業の状況、社会情勢などにより、リスクは常に変化します。定期的にリスクの考え方、枠組みの見直しを行い、リスク環境の変化についてリスク管理部門と連携して対応することが望ましい。

総務・人事部門との連携

情報セキュリティは、IT システムだけで構築されるわけではなく、建屋などの物理的なセキュリティ、入退出のセキュリティ、入退社や人事移動といった人員管理など、総務・人事部門との連携が不可欠で

す。加えて、セキュリティポリシーなどセキュリティに関する社内規定についても、総務・人事部門が所轄となるケースもあります。総務・人事部門は、様々な法令や通達などに対するコンプライアンスが求められる業務領域であることにも注意を払う必要があります。

緊急対応時において、アカウントの停止、証拠物件の確保、PC や操作履歴の調査などの一連の作業も、総務・人事部門との連携が不可欠で、事前に緊急対応マニュアルなどに組み込む必要があります。

CISO は、IT セキュリティだけではなく、物理セキュリティを含めた幅広い判断が求められますが、総務・人事部門と連携しながら、業務を進めることが求められます。

総務・人事部門は情報セキュリティの計画と実装、緊急対応のなど、セキュリティ対策全般において連携が必要な部門となる。それぞれの業務ドメインが違うため、同じ課題に対して異なる常識を持つことも考えられるため、目的と手段を明確にしながら、協力関係を構築することが望ましい。

法務部門との連携

日本では、2003 年に「個人情報の保護に関する法律」が施行され、産業分野のガイドラインが設定されるなど、ビジネスを進めるうえで CISO と法務部門の協力は不可欠になっています。加えて、2018 年 5 月に施行される GDPR[(1)]が注目されており、日本の企業でも対応が必要とされることから、より法務部門と CISO の連携が求められています。

また、セキュリティ侵害や事故が発生をした場合には、法務部門との協力は不可欠です。緊急対応の状況では、特に迅速な判断が求められるため、緊急対応マニュアルの作成などを通じて、事前に対応をまとめておくことが望まれます。

一方で、法務部門は遵守すべき規程（法令やガイドラインなど）がないものについては、あまり関心を持たない傾向があります。例えば個人情報は法律があるので重要視しますが、営業機密にはあまり関心を持たないかもしれません。また、ルールを破った場合の罰則を決めることでセキュリティを担保できると考え、技術的・運用的な予防策や軽減策に関心を示さないこともあります。法務部門と連携をとるうえでは、これらの特性を踏まえて連携を進める必要があります。

法務部門は、GRC(ガバナンス、リスク、コンプライアンス)のコンプライアンス対応に不可欠な部門で、法令やガイドラインを相互に理解する必要がある。またセキュリティ侵害や事故が発生した際に対応を進める際にも、法務部門の協力が不可欠である。事前に緊急対応マニュアルを作成し、必要な対応を明確にしておくことが望ましい。

監査部門との連携

「監査による執行状況の評価」でも取り上げたように、CISO と監査部門との連携が重要であり、コン

プライアンスの確立において、監査部門との連携は欠かせません。

また、近年は、自社のセキュリティ対策を顧客などの外部に対して明らかにするため、ISMS(ISO/IEC 27001)、プライバシーマーク、PCI DSS など、第三者機関による認証が重要視されています。監査部門は、これらの認証に基づく内部監査の実施と、第三者機関による監査の窓口としての重要な役割を果たします。

監査部門と CISO は対立的な関係ではなく、セキュリティダッシュボードで述べたような日常的な計測（モニタリング）の延長線上に監査がある。セキュリティ計画、実施状況、計測項目についても、監査部門と連携し、より良いものとしていくことが望ましい。

広報部門との連携

平常時には、広報部門と連携はないかもしれません。しかし、セキュリティ侵害が起きた場合には、外部への窓口である広報との連携が欠かせません。緊急時には、状況が不確定な段階で事件を公表せざるを得ないなど、外部との難しいコミュケーションが想定されます。このため、あらかじめコミュケーションの方針を定め、社員や役員が果たすべき役割、コミュケーションが必要なステークホルダーなどを明らかにすることが望まれます。

緊急時の対応については、「インシデントを想定した施策の事前評価」、「Annex C インシデントを題材にしたトレーニング」でも記載しています。これらを参考に、あらかじめ必要な対応を明らかにし、トレーニングを通じて、対応の適切さを確認するとともに、それぞれの役割を遅滞なく果たせるようにしてください。

広報部門とは緊急時だけではなく、定期的にコミュケーションを図り、緊急対応が必要なセキュリティ侵害や事故が発生した場合に、遅滞なく連携が取れることが望ましい。

社外との連携

CISO は現在の社内セキュリティに責任を持つとともに、他社の取り組み、技術動向、脅威動向を学ぶことで、新たな脅威に備え、より合理的なセキュリティ対策を実装していく必要があります。将来に備えた活動を行うためには、社内外のトレーニングやイベントへの参加だけではなく、業界や業種を超えたセキュリティ担当者との交流も重要視されています。ベンダーからの情報だけに頼るのではなく、情報収集ルートを複数持つことが重要です。日本でも様々な情報交換の場ができており、国際的な組織の日本窓口を通じた海外との交流も増えています。加えて、SNS などのインターネットをベースとしたコミュニケーションも活発に行われており、個人が国内外の活動に参加することも難しくありません。

JNSA もセキュリティに関係する方々の交流の場を提供する団体の一つであり、多くの部会やワーキン

ググループが活動を通じて、多数の成果物を公表しています。

CISO は現在のセキュリティへの対応だけではなく、社外の専門家などとの交流を通じて、将来のセキュリティ対策をより合理的なものとすることが望ましい。

10. むすび　執行責任者としての CISO

ある調査（APAC CISO 調査[29]）では、新しい技術の導入を阻害する主要な要因として、予算（81%）に続いて、セキュリティ上の懸念（78%）が挙げられており、予算が確保できてもセキュリティが担保できなければ、新たな投資が難しい状況にあること、つまり、現代の企業経営における CISO の重要性を示しています。

このように、CISO は、単にセキュリティ侵害による損害を防ぐばかりではなく、企業経営に貢献することが求められますが、これまでのセキュリティ施策は、規準や標準への遵守が重要視され、セキュリティ施策の有効性やビジネスへの貢献を示すことができていません。加えて、一般的な日本企業では、管理職研修はいわゆる庶務研修だけで企業経営を学ぶ機会がなく、技術者や技術管理職が CISO、CIO、CTO などの経営陣に加わる機会を得ても、経営陣としての基本や素養に恵まれず、適切な業務執行が難しいといった実情があります。

CISO が経営陣の一員として、この課題に取組むためには、広範囲な領域の知見が必要とされ、いわゆる情報セキュリティ以外についても理解と対応が求められます。JNSA CISO 支援ワーキンググループは、CISO の立場を支援し、CISO が企業や社会の期待に応えていくためのエールを送っていきたいと考えています。

最後になりましたが、当ワーキンググループ立ち上げ時に多大な貢献をいただいた根津研介氏（故人 NTT データ先端技術株式会社）に謝意を表したいと思います。

コラム：CISO の孤独

インシデント（アクシデント）によって経営上重大な被害が生じたときに、CISO が任命されることがあります。インシデント（アクシデント）によって経営上重大な被害が生じたときは、CISO が罷免・解雇されるときでもあります。

1994 年に初めての CISO が米 Citigroup で任命され、セキュリティが経営課題の 1 つであるという認識が広まってから十数年になりますが、セキュリティを経営戦略的にとらえ、CISO に何を求めるのか責任範囲を明確にしたうえで、適切な人材を任命するというプロセスはまだ一般的とはいえません。

いきなり抜擢され、セキュリティ強化を頑張ろうとすれば、現場からは余計な仕事を増やしたと冷ややかな目で見られ、経営層・株主からはセキュリティ・コストの妥当性を追求され、問題が起きれば、メディアの激しいフラッシュに目をしばたたかせながら、インシデントは絶対起きないはずではなかったのかとステークホルダーに詰め寄られる、かくのごとく、CISO は社内外で孤独な立場に陥りやすい役職です。

とある CISO は 20 年のキャリアを振り返って「よく頑張ったし、いくつかの戦闘では勝利もしたが、戦争には負けた。一人きりで感謝されることもない、終わりの見えない辛い仕事だった」という言葉を残しています(30)

こうした満身創痍・四面楚歌の CISO にしか分からない孤独と苦悩をわかち合い、解決のヒントと心の平安を求めて、業界を超えた CISO 同士のラウンド・テーブルでの情報交換、ネットワーキングが、世界中で活発に行われています。

本書もこうした CISO 業務に取り組む方々の手助けとなることを願っています。

11. Annex A 執筆メンバー

ワーキンググループリーダー

河野 省二	株式会社ディアイティ（在籍時：2016 年 5 月-2017 年 10 月）
高橋 正和	株式会社 Preferred Networks（2017 年 11 月からリーダー代行）

執筆メンバー

荒木 粧子	株式会社ソリトンシステムズ
池上 美千代	東芝デジタルソリューションズ株式会社
北澤 麻理子	ドコモ・システムズ株式会社
武田 一城	株式会社ラック
田中 朗	三菱電機インフォメーションネットワーク株式会社
西尾 秀一	独立行政法人情報処理推進機構（株式会社 NTT データ）
福岡 かよ子	株式会社インテック

他、CISO 支援ワーキンググループメンバー

レビューアー

岡田 良太郎	日本 CISO 協会（株式会社アスタリスク・リサーチ）
蔵本 雄一	日本 CISO 協会（合同会社 WHITE MOTION）
鎌田 敬介	一般社団法人 金融 ISAC

協力

日本 CISO 協会

日本 ISMS ユーザーグループ

12. Annex B 参考資料

本文中ではご紹介できませんでしたが、WG のディスカッションや、レビューアーからコメントとしてご紹介をいただいた興味深い資料をご紹介いたします。その他の資料は、文末の脚注をご参照ください。

CISO Jobs Mind Map

http://rafeeqrehman.com/wp-content/uploads/2016/10/CISO_Job_v8.png

The CIS Critical Security Controls for Effective Cyber Defense

Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains

https://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

CISOs' Cyber War: How Did We Get Here?

https://www.darkreading.com/vulnerabilities---threats/cisos-cyber-war-how-did-we-get-here/a/d-id/1330737

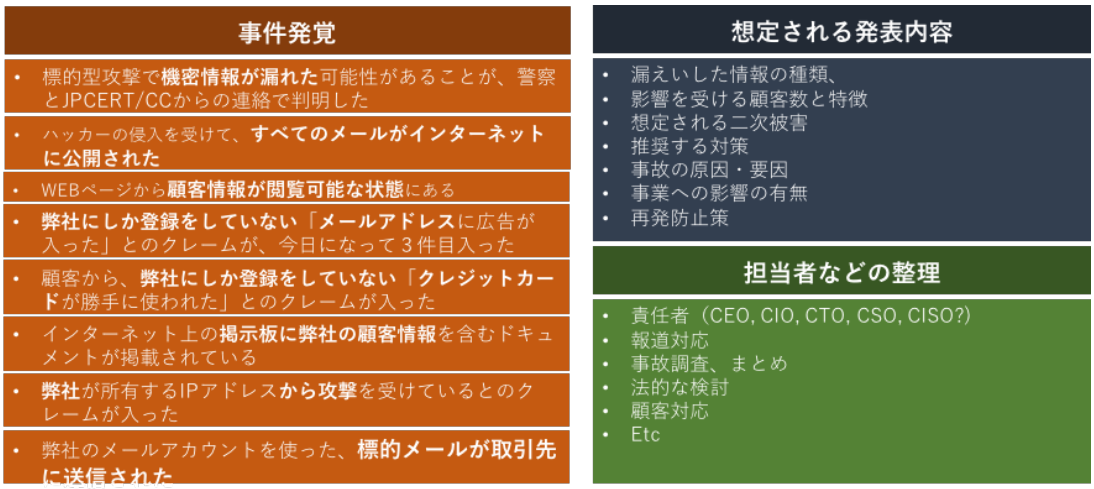
FS-ISAC Unveils 2018 Cybersecurity Trends According to Top Financial CISOs

https://www.fsisac.com/article/fs-isac-unveils-2018-cybersecurity-trends-according-top-financial-cisos

13. Annex C インシデントを題材にしたトレーニング

セキュリティ事故が社会的な問題として報道されるようになり、データ侵害の影響は、平均で 4 億円を超えると言われている。しかし、セキュリティ対策は進んでいない。この要因として、「経営レベルでのセキュリティを捉える」ことが出来ていない点があり、事故が起きたときに、はじめて企業の経営陣が、ビジネスにおけるセキュリティの役割と影響を理解するといった事態も少なくない。

このワークショップでは、セキュリティ事故の机上シミュレーションを通じて、セキュリティポリシーや事故対応ポリシーなどに則って、対応・対処を進め、社外への報告をするまでを実施する。これにより、事故対応における組織面での課題を検証するとともに、報告書の作成や、状況の判断のために、必要な情報（ログなど）が入手できることを検証する。また、再発防止策の策定を通じて、現在のセキュリティ対策の問題点を明らかにし、今強化すべき事項を明らかにするものである。



詳細は、別紙「インシデント対応ワークショップ」に記載

14. Annex D CISO ダッシュボード

別紙として記載

15. 脚注

[1] EU 一般データ保護規則（仮訳）について
https://www.jipdec.or.jp/library/archives/gdpr.html
[2] サイバーセキュリティ経営ガイドライン
http://www.meti.go.jp/policy/netsecurity/mng_guide.html
[3] 重要インフラのサイバーセキュリティを 向上させるためのフレームワーク
https://www.ipa.go.jp/files/000038957.pdf
[4] J-Net21 起業マニュアル　リスクマネジメントの基礎
http://j-net21.smrj.go.jp/establish/manual/list4/step5/manual106-1.html
[5] CxO(経営層)のための情報セキュリティ―経営判断に必要な知識と心得 三宅功著　ダイヤモンド社
ISBN-10: 4478083908, ISBN-13: 978-4478083901
[6] Public Law 107 - 204 - Sarbanes-Oxley Act of 2002
https://www.gpo.gov/fdsys/pkg/PLAW-107publ204/content-detail.html
[7] デロイトトーマツ　企業のリスクマネジメント調査（2015 年版）
https://www2.deloitte.com/jp/ja/pages/about-deloitte/articles/news-releases/nr20160107.html
[8]「サイバーセキュリティマネジメント入門」鎌田敬介　一般社団法人金融財政事情研究所
ISBN-10: 4322132154,　ISBN-13: 978-4322132151
[9] 重要インフラのサイバーセキュリティを 向上させるためのフレームワーク
https://www.ipa.go.jp/files/000038957.pdf
[10] Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains
https://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf
[11] ウィキペディアの執筆者，2018,「OODA ループ」『ウィキペディア日本語版』,（2018 年 4 月 19 日取得,
https://ja.wikipedia.org/w/index.php?title=OODA%E3%83%AB%E3%83%BC%E3%83%97&oldid=68251854）
[12] 情報セキュリティ 10 大脅威 2018
https://www.ipa.go.jp/security/vuln/10threats2018.html
[13] キャプランとノートンの戦略バランスト・スコアカード　ロバート・S・キャプラン ，デビッド・P・ノートン
東洋経済新報社 ISBN-10: 4492554327, ISBN-13: 978-4492554326
[14] わが国の公的機関における効率性と有効性の必要：会計検査研究 No.36（2007.9）
www.jbaudit.go.jp/koryu/study/mag/pdf/j36d02.pdf
[15] テレワークや在宅勤務における情報セキュリティ対策の現状と論点
https://www.mizuho-ir.co.jp/publication/report/2013/mhir06_telework.html
[16] テレワークセキュリティガイドライン
www.soumu.go.jp/main_content/000199491.pdf
[17] IPA サイバーセキュリティ経営ガイドライン解説書
https://www.ipa.go.jp/security/economics/csmgl-kaisetsusho.html
[18] MOF と COBIT/Val IT の比較および クロスインプリメンテーション ガイド
http://www.itgi.jp/pdfdata/MOF%20to%20COVIT,Val%20IT.pdf
[19] NIST　SP800-60　「第 I 巻：情報および情報システムのタイプとセキュリティ分類のマッピングガイド」
https://www.ipa.go.jp/files/000025339.pdf
[20] 効果的なサイバー防御のための CIS クリティカルセキュリティコントロール
https://www.cisecurity.org/wp-content/uploads/2017/03/CIS-CSC_v6.1_Japanese_Final_r1.pdf
[21] JPCERT/CC 高度サイバー攻撃への対処におけるログの活用と分析方法
https://www.jpcert.or.jp/research/apt-loganalysis.html
[22]「企業における情報システムのログ管理に関する実態調査」報告書について
https://www.ipa.go.jp/security/fy28/reports/log_kanri/index.html
[23] コンピュータセキュリティ インシデント対応ガイド
https://www.ipa.go.jp/files/000025341.pdf
[24] 高度サイバー攻撃（APT）への備えと対応ガイド ～企業や組織に薦める一連のプロセスについて
https://www.jpcert.or.jp/research/apt-guide.html
[25] JISQ27000 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語
https://webdesk.jsa.or.jp/books/W11M0090/index/?bunsyo_id=JIS%20Q%2027000:2014
[26] 情報漏えい発生時の対応ポイント集
https://www.ipa.go.jp/security/awareness/johorouei/index.html
[27] Penetration Test vs. Red Team Assessment: The Age Old Debate of Pirates vs. Ninjas Continues
https://blog.rapid7.com/2016/06/23/penetration-testing-vs-red-teaming-the-age-old-debate-of-pirates-vs-ninja-continues/

[28] CBEST Intelligence-Led Testing CBEST Implementation Guide (Version 2.0)
https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/cbest-implementation-guide.pdf?la=en&hash=1BFF85C8F9E6C0E8BE478BB22B422EDDA5E00DC0

[29] Microsoft survey shows 62% of IT leaders in Asia Pacific expect to increase spending on new technologies in 2015
https://news.microsoft.com/apac/2014/10/27/microsoftciosurvey/

[30] CISOs' Cyber War: How Did We Get Here?
https://www.darkreading.com/vulnerabilities---threats/cisos-cyber-war-how-did-we-get-here/a/d-id/1330737