CISO ダッシュボード

～サイバーセキュリティを経営に組み込むための考察～

日本での 2011 年に発覚した中央官庁や防衛産業に対するサイバー攻撃以来、数多くのセサイバー攻撃やセキュリティ事故が報道されている。これまで、セキュリティは技術的な側面で捉えられることが多かったが、2013 年に米国で相次いだ流通業界の POS システムへの攻撃を契機に、セキュリティが経営レベルの問題であると認識されるようになった。日本においても、昨年（2016 年）には経済産業省から「サイバーセキュリティ経営ガイドライン」が公表されるなど、経営レベルにおけるセキュリティ対策の重要性が認識されるようになったことで、改めて CISO （Chief Information Security Officer）の役割が注目されるようになっている。

一方で、「経営」は幅広い概念で「経営戦略」「経営計画」「管理会計」「財務分析」「経営指標」等の様々な領域を包括しており、「サイバーセキュリティ経営」を考察する際には、「経営」として取り上げる領域を明確にする必要がある。CISO は執行責任者としてサイバー（情報）セキュリティに関する領域の「業務を執行（オペレーション）する」役割を担っている。そして、他の執行責任者と共に、それぞれが統括する業務について、経営会議等において報告し了承を得ることで、組織全体の業務が執行される。つまり、他の経営陣の視点から CISO の役割を考察すると、「経営会議において情報セキュリティに関する状況を適切に報告し、必要な施策に関する経営会議での了解を得ること」と定義することができる。

本稿では、このような観点から、CISO が経営会議で報告し了承を得るための内容を「CISO ダッシュボード」と呼称し考察する。

経営視点におえるセキュリティ

経営における IT セキュリティの役割を考えるにあたって、企業経営のための代表的な財務諸表である P/L（Profit / Loss：損益計算書）を使って考察をする。セキュリティ対策の狙いを P/L の科目に当てはめると、①-1 特別損失を発生させるリスク、①-2 売上の減少につながるリスク（ビジネスインパクト）、そして、①-3 セキュリティ施策に対する投資対効果を、それぞれコントロールすることだと位置付けることができる。

一方で、近年注目を浴びている Industry 4.0, Smart Factory 等の IoT とも呼ばれる領域や、Fin Tech と呼ばれる領域においては、IT は業務効率化を目的としたものではなく、ビジネス基盤して位置付けられる傾向が顕著である。つまり、これまでのセキュリティで考察

されてきた情報系としての IT リスクに限らず、②ビジネス基盤としての IT におけるリスクのコントロール、という視点も必要になってくる。

本稿では、「②ビジネス基盤としての IT リスクのコントロール」は、企業や事業により大きく異なるため、主に①-1,2,3 を対象に「CISO ダッシュボード」の考察を進める。

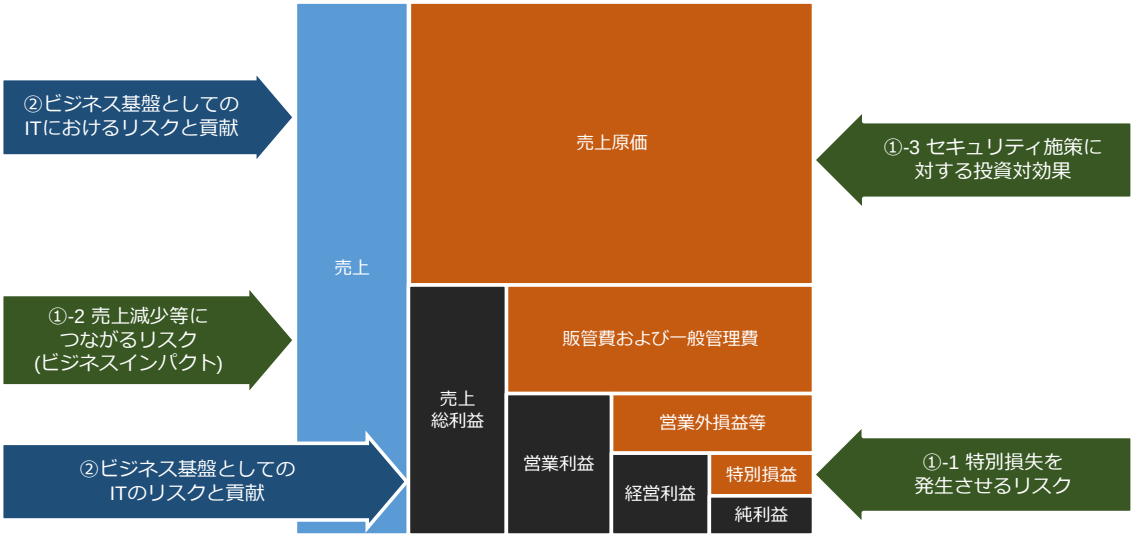


図 1 セキュリティ対策の P/L での考察

サイバーセキュリティフレームワークのアプローチ

これまで、組織におけるセキュリティ対策は、ISO/IEC27001, 27002 や PCIDSS 等のセキュリティ標準やセキュリティ基準を満たすことだと考えられてきた。しかし、これらの基準や標準を満たした組織においも、サイバー攻撃の被害が数多く発生している。つまり、標準や基準に従うだけでは、十分なセキュリティ対策ではないことが明らかになってきた。

「米国の重要インフラのセキュリティとレジリエンスを高める」ための大統領令第 13636 号を受けて、米国国立標準技術研究所（National Institute of Standards and Technology）が 2014 年 2 月に公表した、「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[1]（Framework for Improving Critical Infrastructure Cybersecurity）」では、“*サイバーセキュリティへの取組を企業にとってのビジネス上のモチベーションにつながるものにすることと、サイバーセキュリティリスクを企業のリスク管理プロセスの一環としてとらえることに重きを置いている。*”もので、“*フレームワークコア(Framework Core)、フレームワークプロファイル(Framework Profile)、およびフレームワークインプレメンテーションティア(Framework Implementation Tier)。*”の三つの要素で構成されており、フレームワークコアでは、”*同時的・連続的に実行される 5 つの機能「特定（Identify）」、「防御（Protect）」、「検知（Detect）」、「対応（Respond）」、「復旧（Recover）」*”の要素で構成されている。

表 1　サイバーセキュリティフレームワーク：フレームワークコア

Functions（機能）	Definition（定義）	Phase(フェーズ)
IDENTIFY（特定）	システム、資産、データ、機能に対するサイバーセキュリティリスクの管理に必要な理解を深める。 「特定」機能における対策は、本フレームワークを効果的に使用する上で基本となる。 企業はビジネスを取り巻く状況、重要な事業をサポートするリソース、および関連するサバーセキュリティリスクを理解することで、自組織のリスク管理戦略とビジネスニーズに適合するように取り組みの対象を絞って、優先順位付けを行うことが可能になる。 「特定」機能の成果カテゴリーには、たとえば以下がある：資産管理; ビジネス環境; ガバナンス、リスクアセスメント; リスク管理戦略。	Pre Breach（Plan/Design）
PROTECT（防御）	重要インフラサービスの提供を確実にするための適切な保護対策を検討し、実施する。 「防御」機能は、発生する可能性のあるサイバーセキュリティイベントがもたらす影響を抑えるのを支援する。「防御」機能の成果カテゴリーには、たとえば以下がある：アクセス制御; 意識向上およびトレーニング; データセキュリティ; 情報を保護するためのプロセスおよび手順; 保守; 保護技術。	Pre Breach（Deploy）
DETECT（検知）	サイバーセキュリティイベントの発生を検知するための適切な対策を検討し、実施する。 「検知」機能はサイバーセキュリティイベントのタイムリーな発見を可能にする。「検知」機能の成果カテゴリーには、たとえば以下がある： 異常とイベント; セキュリティの継続的なモニタリング; 検知プロセス。	Post Breach
RESPOND（対応）	検知されたサイバーセキュリティイベントに対処するための適切な対策を検討し、実施する。 「対応」機能は、発生する可能性のあるサイバーセキュリティイベントがもたらす影響を封じ込めるのを支援する。「対応」機能の成果カテゴリーには、たとえば以下がある： 対応計画の作成; 伝達; 分析; 低減; 改善。	
RECOVER（復旧）	レジリエンスを実現するための計画を策定・維持し、サイバーセキュリティイベントによって阻害されたあらゆる機能やサービスを復旧するための適切な対策を検討し、実施する。 「復旧」機能は、サイバーセキュリティイベントがもたらす影響を軽減するための、通常の運用状態へのタイムリーな復旧を支援する。「復旧」機能の成果カテゴリーには、たとえば以下がある： 復旧計画の作成; 改善; 伝達。	

1　IPA: 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　http://www.ipa.go.jp/files/000038957.pdf

「特定（Identify)」は分析や計画で、プロジェクト計画や年初の実施計画に相当し、「防御（Protect)」は狭義のセキュリティ対策であり、セキュリティ関連の主要な業務に相当する。「検知（Detect)」「対応（Respond)」、「復旧（Recover)」は、いわゆる Post Breach、つまり、侵入の発見と対処に関するもので、主に CSIRT(Computer Security Incident Response Team)が対応するフェーズといえる。サイバーセキュリティフレームワークでは、Resilience （回復力：レジリアンス）が重要な目的とされていることから、Post Breach への取り組みが重視されている。

本稿では、先に述べたような CISO の業務執行という視点から、経営会議などの定期的な場で報告すべき主要な内容を、このフレームワークコアを参考にしながら CISO ダッシュボードの考察を進める。

CISO ダッシュボードの主要計測項目についての考察

セキュリティマネジメントの基本は PDCA（Plan, Do, Check, Act）サークルといわれている。多くの場合、何らかのセキュリティ基準/標準に基づいてキュリティポリシーやセキュリティ施策が“Plan”され、Do(実施)される。そして、Check においては、Plan と Do の比較が行われ、必要に応じて Act(対策実施)される。Check の対象となるのは、主として、セキュリティポリシーなどで定義された「あるべきセキュリティ対策状」と「実際の対策の実施状況」の差に相当する。CISO ダッシュボードでは、この差分を、「Protection condition：コンプライアンス率（ポリシー遵守率)」として計測する。コンプライン率は、フレームワークコアの「防御（Protect)」の計測に相当する。

一方で、コンプライアンス率は、組織が受けている攻撃や侵入については考慮していない。防御（Protect）状況を把握するためには、コンプライアンス率に加えて攻撃の状況を把握する必要がある。このため、CISO ダッシュボードでは、コンプライアンス率に加えて「Attack condition：検知・対処された攻撃」を主要な要素として取り上げる。この要素は、「特定（Identify)」の基礎情報としてフィードバックをすることになる。

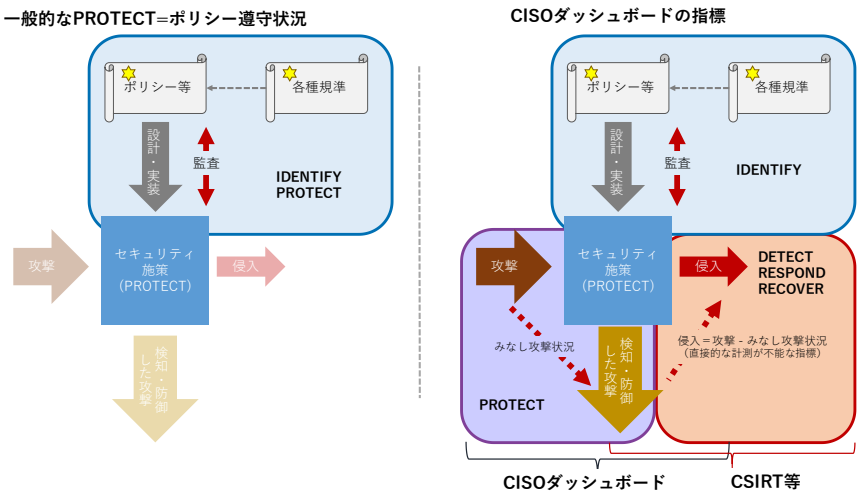


図 2　セキュリティ施策の考察

成功した侵入を「検知・防御ができなかった攻撃」と定義した場合、「検知・対処された攻撃」には、成功した侵入は含まれていないため、成功した侵入を直接的に計測することはできない。このため、侵入の可能性を評価するにあたっては、なんらかの間接的な指標を利用する必要がある。具体的には、認証やアクセスの失敗、通常とは異なる認証の成功（Pass the Hash 等）、権限の昇格、大量のデータ通信、ブラックリストに掲載されたサイトへのアクセス等の「典型的な侵入活動を示す指標」を計測することで、侵入の可能性を評価することができるものと考えられる。なお、「Suspicious activity：典型的な侵入活動を示す指標」は外部からの侵入ばかりではなく、内部犯行についても検出をするものと考えられる。

これらの要素に加えて、情報流出につながる可能性のある事象として PC の紛失や盗難や物理的な侵入にかかわる情報、内部犯行につながる可能性のある事象として、人事上のトラブル等、「Indirect activity 間接的な指標」も考慮する必要がある。

ここに挙げた 4 つの要素を中心に CISO ダッシュボードの考察を進めていく。

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）

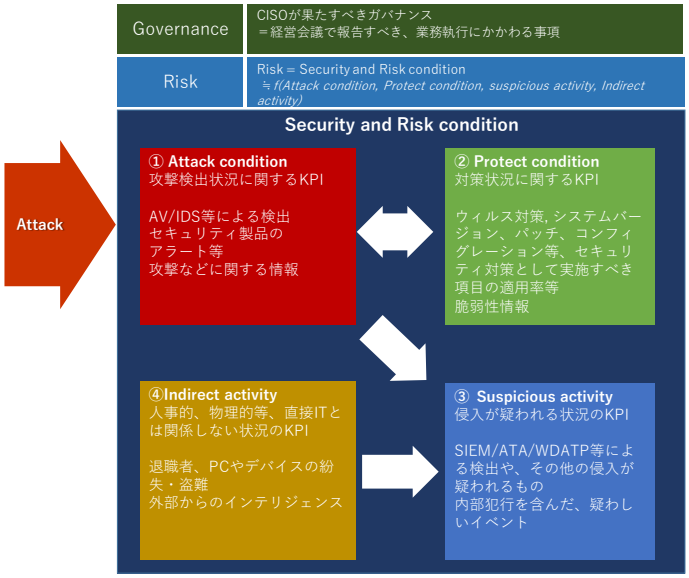


図 3　CISO ダッシュボード主要項目

CISO ダッシュボードの構成要素

CISO ダッシュボードの構成要素として、Attack condition, Protection condition, Suspicious activity, Indirect activity の 4 項目を挙げたが、それぞれの項目について、技術的な要素と、概況的な要素に着目する必要がある。技術的な要素は、ログ等から計測が可能な項目であり、概況的な要素は、新たな脆弱性の公表や被害が発生している攻撃要素などである。それぞれの項目と考えられる代表的な指標を以下に記載する。

- 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）
  - 技術的な項目
    受信メール総数、SPAM 受信数、マルウエア検知数、IDS 検知数等
  - 概況的な項目
    セキュリティ事故情報、新たに公表された攻撃手法やツール
- Protection condition
  対策の状況は計画通りか（Assurance の領域）
  - 技術的な項目
    インベントリ（PC 等の総数、ポリシー適用状況）、特権アカウント
  - 概況的な項目
    新たに公表された脆弱性、ゼロディ攻撃
- 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）

- 技術的な項目
  認証の成功・失敗、アクセスの失敗、ブラックリストに含まれるサイトへのアクセス
- 概況的な項目
  システムトラブル、ネットワークトラブル、ヘルプデスクへの問い合わせ

- Indirect activity
  - 技術的な項目
    PC の紛失、盗難
  - 概況的な項目
    建屋への侵入、人事上のトラブル、顧客からのクレーム、不審電話、不審者
    トレーニングなどの状況

表 2　CISO ダッシュボード主要項目（候補）

	技術的		概況的
	計測項目	計測要素	
Attack condition	メール総数（送信、受信）	メール数と転送量の偏差値	事故情報
	SPAM受信数（可能なら分析）	スパム数とスパム割合の偏差値	ツール情報
	AV検知数（GW, End Point, etc）	検出数の偏差値、GW-EPの偏差値	その他
	IDS検知	Highの偏差値、全体の偏差値	
	公開サーバ、ネットワーク境界	探査状況、SSHなどの試み	
	ブラックリスト	ブロック数、偏差値	
Protection condition	インベントリ		脆弱性状況
	総数（ドメイン参加、非ドメイン）	ドメイン参加台数	・ゼロディ
	ポリシーのコンプライアンス状況	NGの台数と割合(Config, パッチ、AV、etc)	・脆弱性の利用状況
		暗号化状況(Volume)	
	ネットワークインベントリ	非ドメイン参加の台数、未登録のPC	
	ホストベースインベントリ	アプリケーションの利用状況、コンプライアンス違反のアプリ	
	特権アカウント（管理済み、未管理）	重要特権アカウント保持数	
		Build in Adminの管理状況	
Suspicious activity	検知ツール・手法の状況		システムトラブル
	SIEM, ATA, WDATP		ネットワークトラブル
	認証関係		人的なトラブル
	ログインの失敗、異常		
	ロックアウト（?）		
	トラフィック		
	異常なトラフィック		
	疑わしい接続先		
	Proxyの認証エラー		
	イントラネットハニーポット		
	サーバー、アカウント、PC		
Indirect activity	PCなどの紛失、盗難		社内トラブル
	ロックアウト		社内クレーム
	ーー		顧客からのクレーム
	新規PCの導入・入れ替え		不審電話
	サーバーやネットワークの更新		不審者
	新規サービスのスタート		
	ソフトウェアの更新		

CISO ダッシュボードを使った報告イメージ

CISO ダッシュボードを使った、経営会議で報告すべき内容を考察する。ここまでに述べた CISO ダッシュボードの要素をそのまま報告したのでは、他の執行責任者に対する十分な説明にはなっていないと考えられる。CISO ダッシュボードは、CISO が状況を判断するための材料であり、これに基いた報告書を作成する必要がある。

想定される報告書のイメージは次の通り。

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)。
Attack condition	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。現在詳細を分析中だが、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。
Attack condition	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。

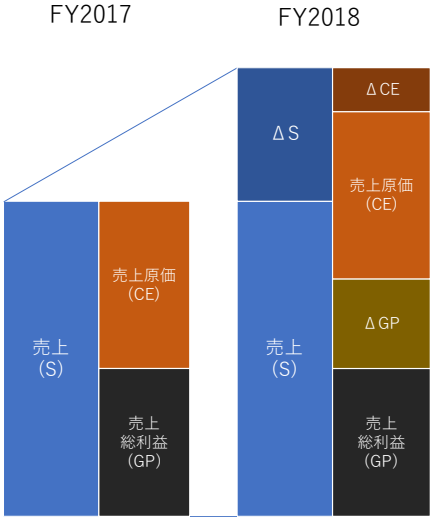
決済事項	疑わしい通信が観測されているが、対処の必要性を判断するにあたり、十分な精度とスピードが確保できない。この課題を解決するために、精度の高いブラックリストの購入を申請する（別紙２：決済申請）
報告事項	XX 年度 YY 月で決済を受けた分析システムは、XX 月の中旬から試験稼働を始めている。ZZ 月までには試験稼働と評価を終了し、本格的な稼働を始める予定。
その他	セキュリティトレーニングを未受講の社員が２０名ほど残っている。上司にあたる役員を CC した上でリマインドを行うので、部下のトレーニング受講に協力頂きたい。 経済産業省から、「サイバーセキュリティ経営ガイドライン」が公表され、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

ビジネス基盤としてのセキュリティについて

Smart Factory や Fin Tech のように、セキュリティをビジネス基盤として活用する場合、IT 利用の目的は、P/L における売上および利益額の増加に対する貢献にある。これらの科目を増加させる手段を単純化すると、マーケット規模かマーケットシェアのいずれか、または両方を伸ばすことが必要である。

このような視点でセキュリティを考える場合、特別損失や（負の）ビジネスインパクトといった視点ではなく、IT による競争優位性を確保するための品質の一つとしてセキュリティをとらえる必要がある。

これも、CISO ダッシュボードに組み込むべき指標ではあるが、個別の経営戦略や経営計画に深く結びついた内容となるため、本稿での考察は行わない。



考慮すべき対象領域への考察

- *ΔS* :売上の差分
- *ΔCE* :売上原価の目標との差分
- *ΔGP* : *ΔS* - *ΔCE*

考慮すべき対象領域への考察

- S = MS x Share
- S + ***ΔS*** = (MarketSize+ ***ΔMS***)x(Share+ ***ΔShare***)

***ΔS*を増やすためには、マーケットサイズの拡大 or / and シェアの拡大が必要**

図 4　IT をビジネス基盤とする場合についての考察

むすび

本稿では、CISO が経営陣の一員として業務を執行するにあたって、経営会議等で報告すべき内容についての考察を行い、Attack condition, Protection condition, Suspicious activity, Indirect activity の 4 つの項目による CISO ダッシュボードを提案した。これの項目については、実際の環境での計測などを通じた評価が必要だと考えられるが、CISO が果たすべき役割について議論を進めるための、提案ができたと考えている。

また、自動的に CISO ダッシュボードを作成するためのツールの開発や、CSIRT 等の緊急対応への連携、年初やアドホックなセキュリティ計画の立案へのフィードバックの検討など、これから考慮すべき事柄が多数残っている。

これらの内容について、逐次進めていきたいと考えている。