業務執行として考える CISO業務

高橋　正和

CSO, Preferred Networks

質問

- セキュリティ専門家であるあなたは、日ごろの実績が認められたのかどうか、ある日、CISO（執行役員）として、毎月行われる経営会議に参加することになりました。
- 経営会議は会社の経営方針を決定する重要な会議で、各執行役は、持ち時間１０分で報告を行うことになっています。

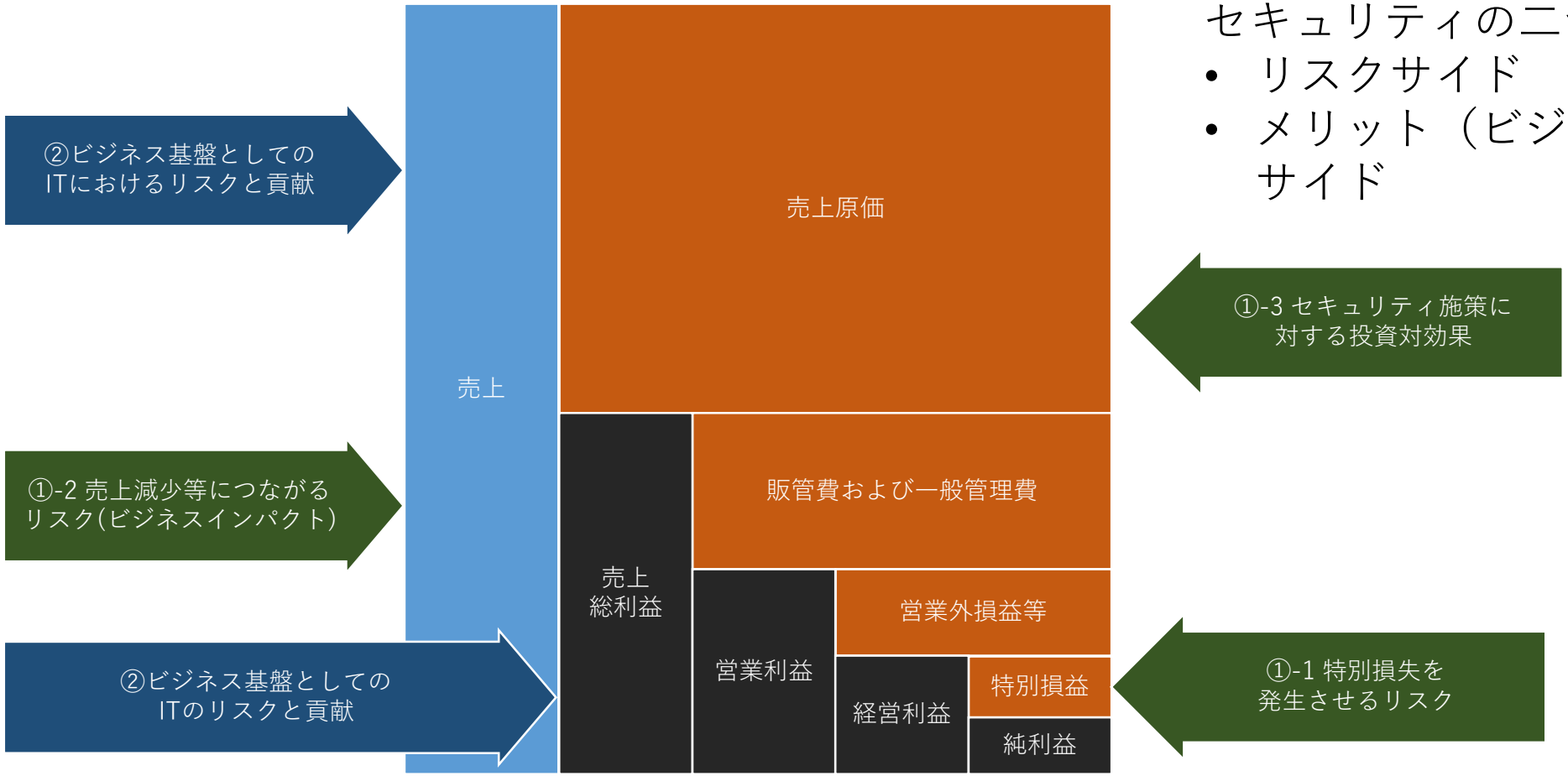
- あなたは何を報告しますか？

背景と前提

CISO等の役割 (出典 IPA)

- セキュリティポリシーを策定する.
- サイバーセキュリティリスク管理体制を構築する.
- 自社のサイバーセキュリティリスクを把握し，リスク対応計画を策定する.
- 対策実施に掛かる費用について経営層の承認を得る.
- 構築した体制を維持，改善するための PDCA サイクルを統括，監督する.
- インシデント対応の陣頭指揮を執る.
- 新規 IT 導入時等，事業部門に対するセキュリティの技術的観点からのアドバイスをする.

BSにみるセキュリティの変化
（ITが情報系からビジネス基盤に変化）



セキュリティの二つの側面
- リスクサイド
- メリット（ビジネス推進）サイド

CISOはなにを報告するか？

ISMSに基づいた報告

- ISMS構築に関する報告書はあるが、毎月経営陣に報告することはあまり想定されていない
  あえて、報告するとすれば以下の項目か？

  - ポリシー順守率（ヒアリング形式では無理がある？）
  - インシデント（ありませんでした、の報告か？）

  経営会議で聞きたい内容だろか？
  経営計画に影響はあるだろうか？
  しっかりやれ！、以上にいえることはあるだろうか？
  当たり前ではあるが、ISMSは経営ではない。

情報セキュリティ報告書モデル（経産省）

表 1　情報セキュリティ報告書モデルの基本構成

①基礎情報
報告書の発行目的、利用上の注意、対象期間、責任部署等

②経営者の情報セキュリティに関する考え方
情報セキュリティに関する取組方針、対象範囲、報告書におけるステークホルダーの位置付け、ステークホルダーに対するメッセージ等

③情報セキュリティガバナンス
情報セキュリティマネジメント体制（責任の所在、組織体制、コンプライアンス等）、情報セキュリティに関わるリスク、情報セキュリティ戦略等

④情報セキュリティ対策の計画、目標
アクションプラン、数値目標等

⑤情報セキュリティ対策の実績、評価
実績、評価、情報セキュリティの品質改善活動、海外拠点の統制、外部委託、情報セキュリティに関する社会貢献活動、事故報告等

⑥情報セキュリティに係る主要注力テーマ
内部統制や個人情報保護、事業継続計画など特に強調したい取組、テーマの紹介、工夫した点等

⑦（取得している場合の）第三者評価・認証等
ISMS 適合性評価制度、情報セキュリティ監査、プライバシーマーク制度、情報セキュリティ関連資格者数、格付け／ランキング等

- 例 1
  - 個人情報保護
    - 顧客情報管理を前提とした業務プロセスと情報システムの設計と見直し
    - 個人情報保護に関する教育の徹底
  - 事業継続
    - 情報システムのバックアップ体制に関する見直し
    - 事業継続計画訓練の実施
  - 基幹システムのダウンに係る影響の縮小化
- 例 2
  - ISMSの認証取得
  - 情報資産の洗い出し
  - 社員教育の徹底
  - ビジネスパートナーとの情報共有ルールの明確化
- 例 3
  - 機密情報・重要情報管理方針およびルールの策定
  - 雇用契約の見直しと教育・研修の実施
  - 物理セキュリティの改善
  - 情報セキュリティの品質改善活動
  - 外部委託ルールの見直し

http://www.meti.go.jp/policy/netsecurity/docs/secgov/2007_JohoSecurityReportModelRevised.pdf

サイバーセキュリティ経営ガイドライン解説書

- フレームワーク（PDCA）のサイクル / 対策状況の把握
  - 事業への影響度や情報の重要度 に合わせて、どのようなリスクをどの程度低減できているかという視点
    - 顧客情報管理リスクの状況等
  - 環境変化や新たな脅威の発生と対応という視点
    - インシデントに至らなかったヒヤリハットなどの内容や件数

- リスク低減の視点（例）
  - 新システムが稼働し、顧客情報が1万人分増えました
- 環境の変化・新たな脅威（例）
  - 従業員から 報告された様々な内容について、事業への影響度で分類、集計し、件数をまとめた結果

https://www.ipa.go.jp/files/000056148.pdf

そもそも、経営会議で
なにを報告すべき？

ドラッカー（経営会議で議論すべきこと）

- 1.現在のお客様を創り出すための目標について
- 2.未来のお客様を創り出すための目標について
- 3.ヒト （人材の採用、配置、育成など）
- 4.モノ （情報、知識、技術、設備、お取引先、パートナーなどに関すること）
- 5.カネ （予算、資金繰りに関すること）
- 6.生産性向上の目標について
- 7.社会貢献の目標について
- 8.売上と利益（目標ではなく条件）

…難しすぎる…

GE幹部を「ウン」と言わせる資料の作り方

XX事業部:2016年1月月報

主要KPI

KPI	Actual	Target	%
売上			
利益			
離職率			
HC			

MAIN DEALS LOST (15年第3四半期)

Deal (理由)	<value>K
Deal (Reason)	<value>K

主要案件(15年第4四半期)

Deal	status	<value>K
Deal	status	<value>K
Deal	status	<value>K
Deal	status	<value>K

主要プロジェクト

顧客名	金額	スコープ	RISK	Prof%
Cust <Project>	xxx M	xxx	M	x%
Cust <Project>	xxx M	xxx	L	x%
Cust <Project>	xxx M	xxx	H	x%

部門の課題とアクション

- Unsigned contracts
- Watch projects

サマリー

- …

経営陣への要望

- …

マネジメントリポートの例。最も伝えたいことを左上に書くのが鉄則

マネジメントリポートを作成するときに私がいつも押さえているポイントが3つあります。
（1）現状が一目で分かるものにすること、
（2）必ず3つの視点を入れること、
（3）経営陣にしてほしいことを明確にすること、
です。

3つの視点を入れる
GE時代、リーダーにとって大切なことは、
（1）変化をドライブし、
（2）パフォーマンスを出し、
（3）インテグリティを守る、
の3つだと学びました。

GE幹部を「ウン」と言わせる資料の作り方
https://business.nikkei.com/atcl/report/15/260984/012700005/?P=1

意外なくらいに資料がない

わかったような気にはなるのだが…

- 経営戦略の資料はある
- 経営企画の資料もある
- 人事管理・チームマネジメント等の庶務管理もある

- しかし
  業務執行や経営会議はほとんど見つからない

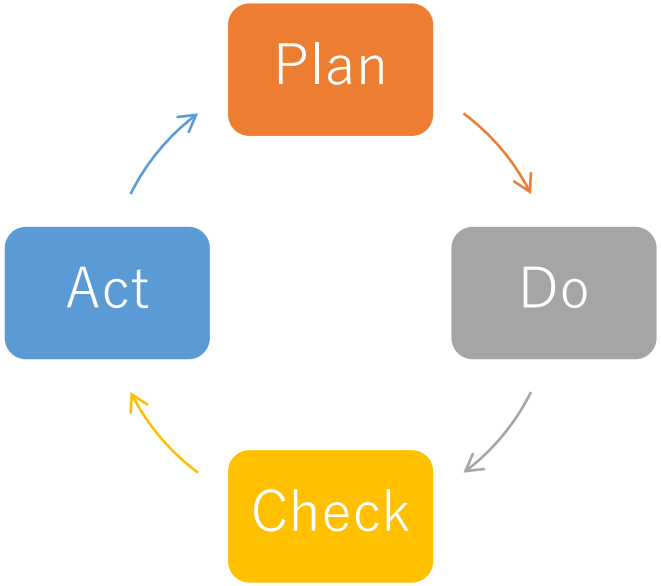
- 「はじめての経営会議」が必要？

セキュリティ対策の
リスクサイドについての考察

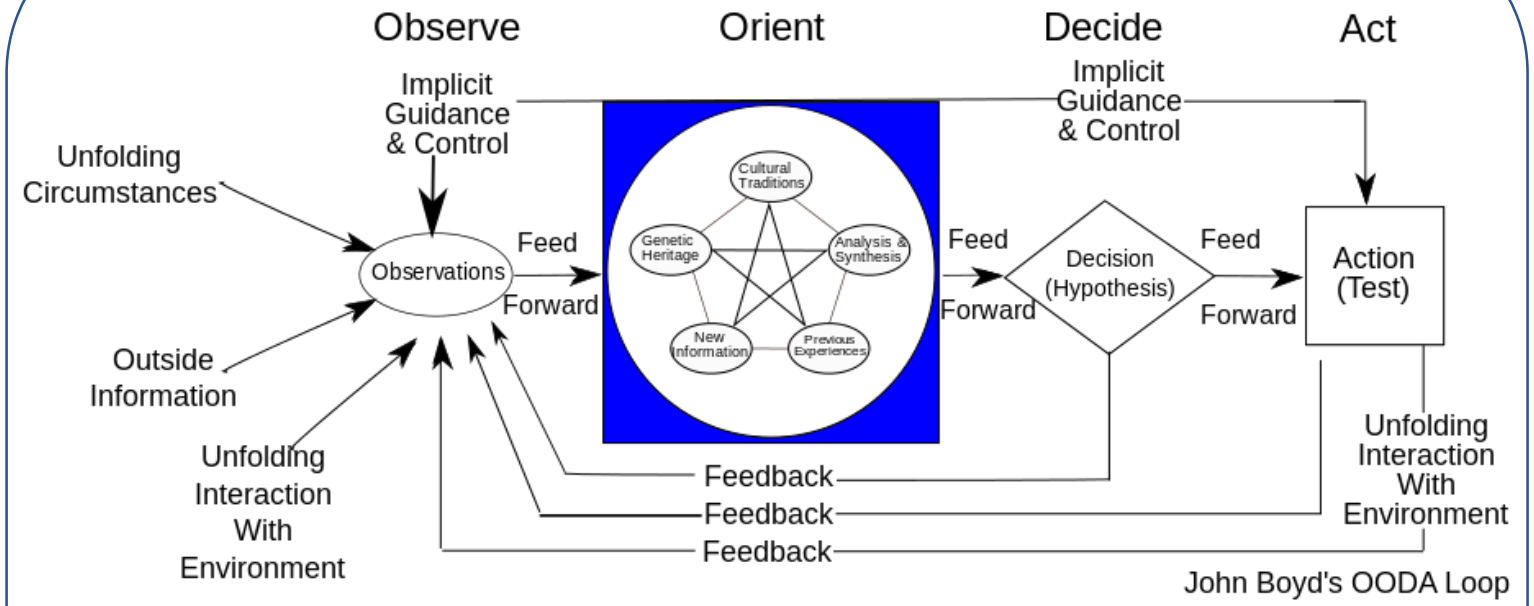
攻撃への注目：サイバーセキュリティフレームワーク

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。	

二つのマネジメントサイクル



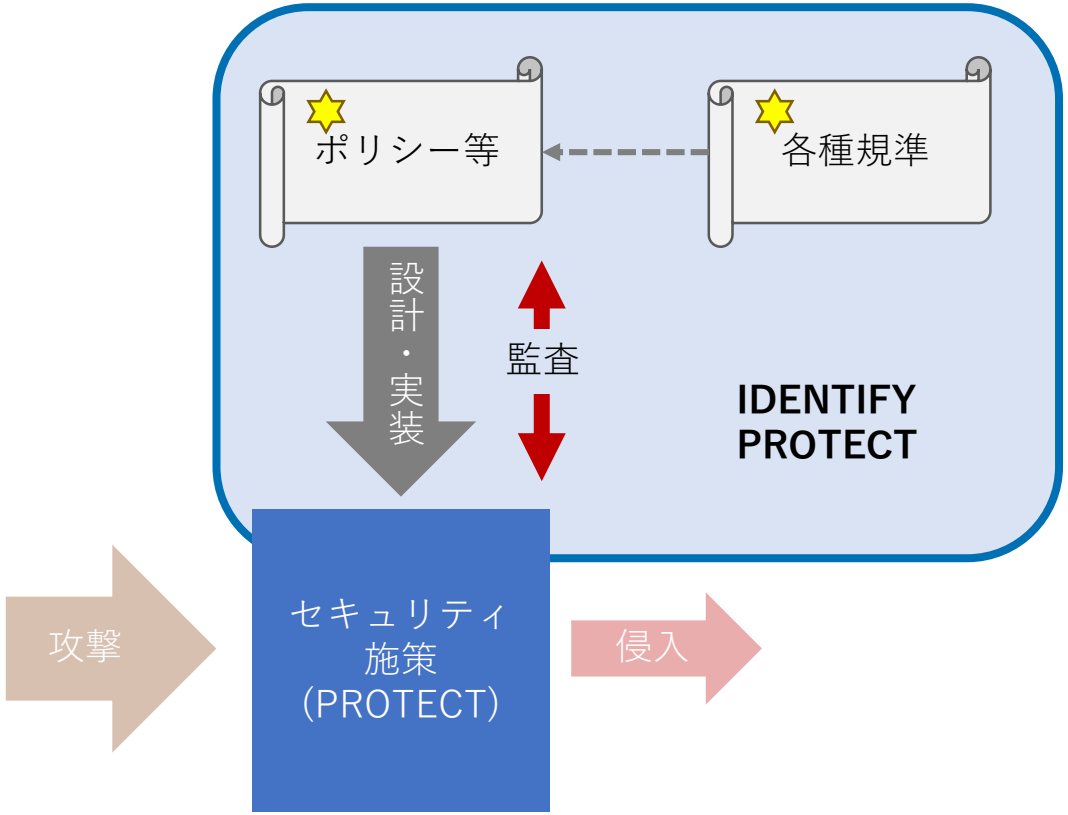
PDCA



OODA

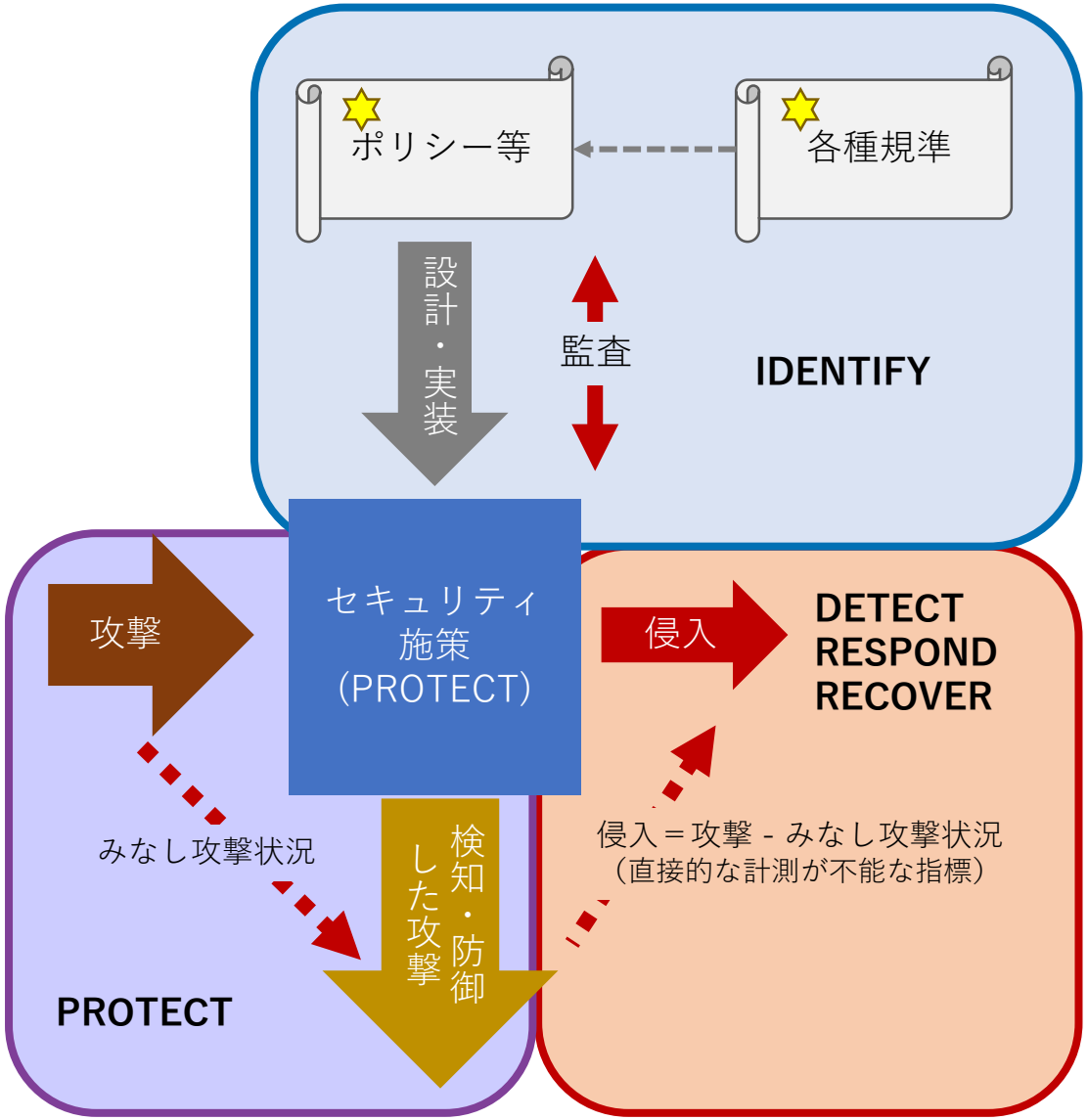
ウィキペディアの執筆者，2018，「OODAループ」『ウィキペディア日本語版』，（2018年4月19日取得，https://ja.wikipedia.org/w/index.php?title=OODA%E3%83%AB%E3%83%BC%E3%83%97&oldid=68251854）

報告内容：一般的なPROTECT=ポリシー遵守状況



攻撃を前提としていない？

報告内容：CISOダッシュボードの指標



Governance	CISOが果たすべきガバナンス ＝経営会議で報告すべき、業務執行にかかわる事項
Risk	Risk = Security and Risk condition ≒ *f(Attack condition, Protect condition, suspicious activity, Indirect activity)*

Security and Risk condition

① Attack condition
攻撃検出状況に関するKPI

AV/IDS等による検出
セキュリティ製品の
アラート等
攻撃などに関する情報

② Protect condition
対策状況に関するKPI

ウィルス対策, システムバージョン、パッチ、コンフィグレーション等、セキュリティ対策として実施すべき項目の適用率等
脆弱性情報

③ Suspicious activity
侵入が疑われる状況のKPI

SIEM/ATA/WDATP等による検出や、その他の侵入が疑われるもの
内部犯行を含んだ、疑わしいイベント

④Indirect activity
人事的、物理的等、直接ITとは関係しない状況のKPI

退職者、PCやデバイスの紛失・盗難
外部からのインテリジェンス

リスクサイドの報告例

			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，協力をお願いしたい．
	概況的	1	ネットワークデバイスへの深刻な脆弱性が報告されているが，弊社では使用していないことが確認されている(別紙 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．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． 分析を速め，より効果的な防御を行うためには，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 3)．
	概況的	2	問い合わせ窓口に，アカウントロックアウト対応依頼が立て続けに 3 件入った．攻撃とは考えにくい件数だが，念のためアクセス状況を精査し，リスト型攻撃等の監視を強めている．
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． 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た．プロシージャに沿ってアカウントなどの停止を実施済み．
	概況的	1	情報セキュリティトレーニングが終了していない社員が残っている．今月中に全社員の受講を予定している．

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)．
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	情報セキュリティトレーニングを見受講の社員が 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をお願いしたい．

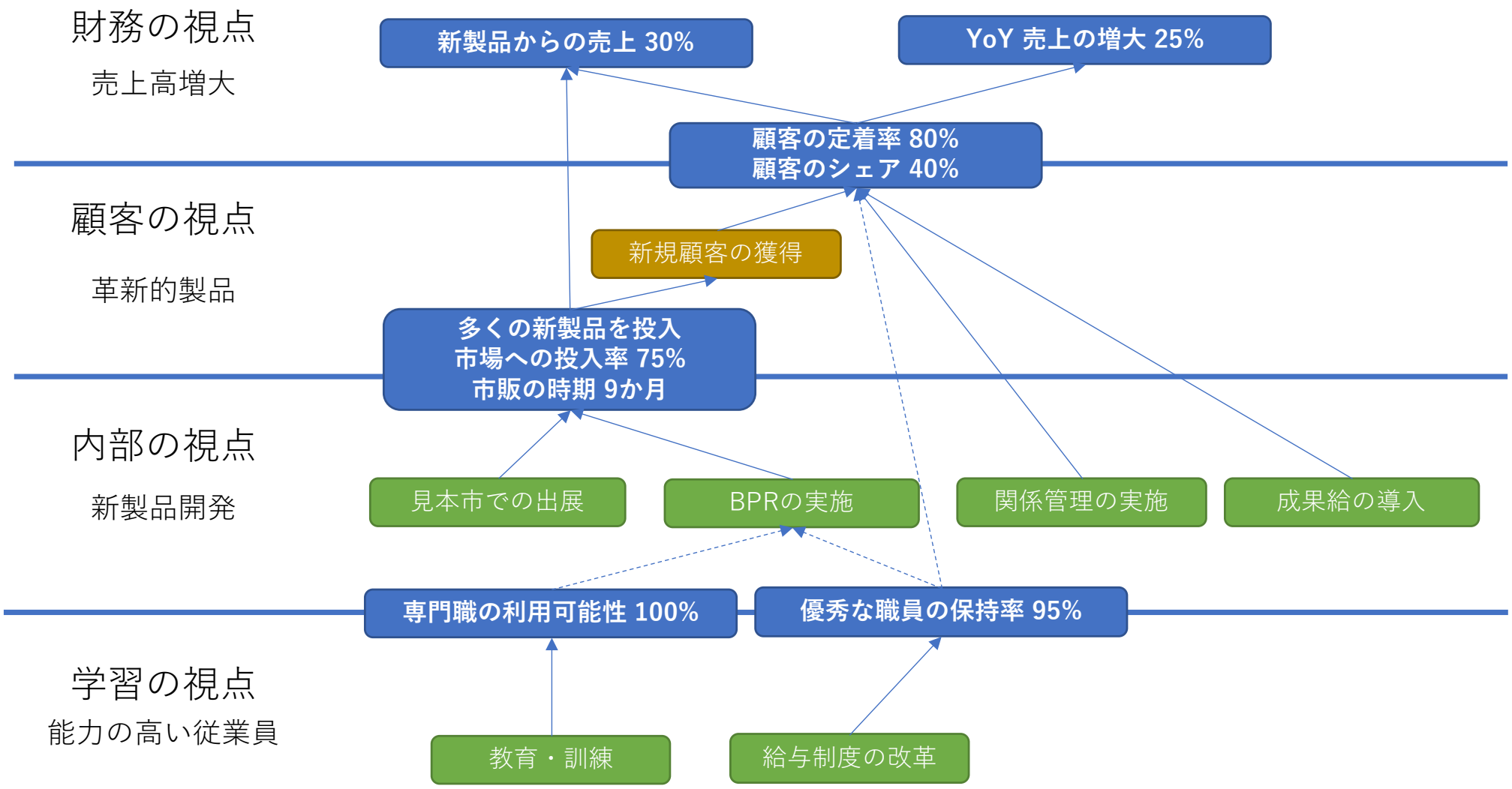
メリットサイド
情報セキュリティの指標化

戦略テーマ、戦略目標、目標値、実施項目

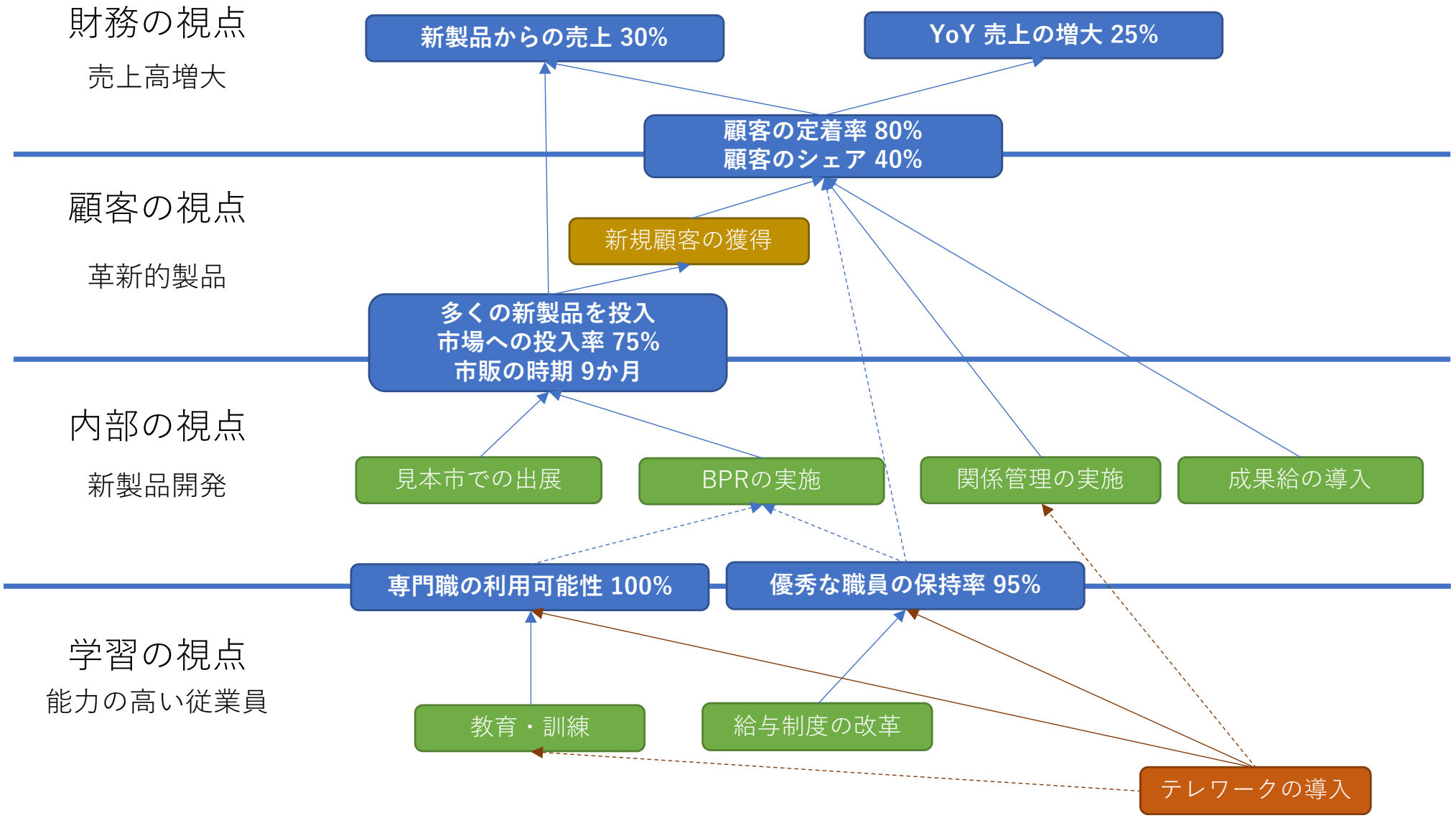
視点	戦略テーマ	戦略目標	目標値	実施項目
財務の視点	売上高増大	年々の売上伸び率	＋25%	×
		新製品からの売上	30%	×
顧客の視点	革新的製品	顧客の定着率	80%	関係管理の実施
		顧客のシェア	40%	成果給の導入
内部の視点	新製品開発	市場への投入率	75%	見本市での出展
		市販の時期	9ヶ月	BPRの実施
学習の視点	能力の高い従業員	専門職の利用可能性	100%	教育・訓練
		優秀な職員の保持率	95%	給与制度の改革

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

戦略マップ


財務の視点
売上高増大
新製品からの売上 30%
YoY 売上の増大 25%
顧客の定着率 80%
顧客のシェア 40%
顧客の視点
革新的製品
新規顧客の獲得
多くの新製品を投入
市場への投入率 75%
市販の時期 9か月
内部の視点
新製品開発
見本市での出展
BPRの実施
関係管理の実施
成果給の導入
専門職の利用可能性 100%
優秀な職員の保持率 95%
学習の視点
能力の高い従業員
教育・訓練
給与制度の改革

戦略マップ：テレワーク導入



テレワーク導入の数値目標化

	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

このような指標化を行うことで、メリットサイドの指標化ができるのではないか。

むすび

サイバーセキュリティ経営とは？

- ISMSはサイバーセキュリティ経営ではない

- 経営という言葉は曖昧さがある
- CISOにとっての経営は「業務執行」を中心に考えることが適切
- セキュリティ計画の策定・導入等も重要な業務執行であるが、以下の観点が必要
  - 実施した施策の成果
  - これから実施する施策
  - それぞれの根拠

- 経営会議を想定することで、CISOが執行すべき業務を逆引きすることができるのではないか。

CISO ハンドブック

（CISO支援ワーキンググループ）

2018.5.11

※引用のご連絡及び内容に関するお問い合わせは、
「各種公開資料の引用及び、内容に関するお問合せ」をご確認下さい

CISO ハンドブックについて

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）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

https://www.jnsa.org/result/2018/act_ciso/

Thank you !