日本のサイバーセキュリティを「連携」「学び」「創造」

サイバーセキュリティ経営の再考

CISOハンドブックが提唱する
業務執行としてのセキュリティ

JNSA 社会活動部会 CISO支援ワーキンググループ
株式会社Preferred Networks 最高セキュリティ責任者

高橋　正和

CISOハンドブック

- 抽選で**5名様**に「CISOハンドブック」の**デジタル版**をプレゼントします。
- NSF2021に**ご参加登録メールアドレス**でお申し込みください。

- 当選者には、１カ月以内にJNSA事務局(mailto:office@jnsa.org)よりご案内いたします。
- ※落選された方へのご連絡はございません。ご了承ください。

キーワード
当日ご案内します

申し込みURL
https://forms.gle/o1Yb3jfbeZNmwhVH7

LINEで送る ツイート いいね！ 0

CISOハンドブック ――業務執行のための情報セキュリティ実践ガイド

￥3,740 (税込)

数量 1

カートに入れる

技術評論社　CISOハンドブックデジタル版（PDF）
https://direct.gihyo.jp/view/item/000000001358

レビューはこんな感じです

kaz

★★★★★ **とても理解しやすい**

2021年2月5日に日本でレビュー済み

Amazonで購入

CISOといえば単に情報セキュリティの専門家であり、日常の技術面、ソフト面での対策やインシデント対応を行う責任者というイメージがありますが、その役割を経営的側面から見て、自社に必要なセキュリティ対策の導き出し方などの考えについて、よくまとめられており、CISOが本来持つべき役割について解説されています。
CISOでなくても、会社のセキュリティ対策への投資の考え方に悩まれている方へ一読することをお勧めしたいです。

石川 陽一

★★★★★ **セキュリティやDXでの大事な観点が整然と詰め込まれている**

2021年2月1日に日本でレビュー済み

Amazonで購入

セキュリティやサイバー話は、とかく専門領域にディープに潜りすぎたり、流行の用語に振り回されたりします。 こちらの本では、見識のある方々により、大事な観点がしっかりと書かれています。 DX（デジタルトランスフォーメーション）に関しても要領よく触れており、ハンドブックとしてしっかりとリファレンスします。

taQra

★★★★★ **CSO/CISOが持つべき視点が網羅的に整理されている**

2021年2月10日に日本でレビュー済み

Amazonで購入

CSO/CISOの役割や業務範囲を狭く捉えている人は、とにかくリスクを回避すれば良いという対応をしてしまう。そうならないよう、幅広い分野に対して持つべき視点が網羅されている。例えば、自分がリードしない財務会計等の分野であっても、セキュリティがどのようなインパクトを持つのか理解して行動するようガイドしている。また、単にリスクを下げるのではなく、ビジネスを阻害しないようにコントロールするためのフレームワークを提供している。
最初の部分は、セキュリティに直接関係ないことが書かれているけれども、それを自分に関係ないと思ってしまう人ほどその部分を読んで欲しいと思います。

yumarse

★★★★☆ **CISOの知るべき事柄を広く浅く網羅。実践的かどうかは...**

2021年3月5日に日本でレビュー済み

Amazonで購入

CISO(Chief Information Security Officer)の担うべき役割と知っておくべき事項について、広く浅く書かれています。

印象的だったのは、書の前半では特に経営と情報セキュリティの整合性が協調され、財務諸表の読み方などが説明されていたことです。ただし内容は薄く、この程度の内容では中途半端な理解にしかなりません。会計の入門書を1冊読んだ方がずっと良いでしょう。（とはいえ、情報セキュリティは経営指標と照らして考えるべき、という考え方自体は疑いようが無く正しいと考えます）

その他にも「情報セキュリティの効果をどのような指標で計測するか。企業ITのアーキテクチャはどうあるべきか。デジタルトランスフォーメーションとの関係は。インシデント発生の際の対応は。他部門との関係性は。」など、経営幹部としてのCISOの知るべき事項が、広く浅く記載されています。ただし各事項は粒度にばらつきがあり、また複数の著者で書いているからか、文体にも差が表れていました。

情報セキュリティの担当者が、情報セキュリティと企業経営の関係性を認識するために読む本としては優秀と考えます。ただし実際にCISOなど経営陣の立場になる方が読むには、専門性が薄いないし足りないと感じました。非技術畑出身の経営者にとっては、入門本としては良いかもしれません。技術（特にITインフラ）畑出身だったり、既にセキュリティを専門的に扱ったことのある人にとっては、物足りない本となるでしょう。

だれが、CISOハンドブックを作ったのか？

JNSA CISO支援ワーキンググループ

- 2015年　現MS河野さんと当時MS高橋で活動を開始
- 2016年　CISO支援ワーキンググループを設立
- 2018年　「CISOハンドブック Ver1.0β」を公表
  - https://www.jnsa.org/result/2018/act_ciso/index.html
- 2019年　中小企業向けとして「MY CISOハンドブック」を公表
  - JNSA 全国横断サイバーセキュリティセミナー2019向け資料
  - https://www.jnsa.org/result/2019/act_ciso/
- 2021年　技術評論社より「CISOハンドブック―業務執行のための情報セキュリティ実践ガイド」を出版

執筆グループ

WGリーダー

高橋 正和	株式会社 Preferred Networks

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	株式会社東芝
岡田 良太郎	株式会社アスタリスク・リサーチ
唐沢 勇輔	Japan Digital Design 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
橘 喜胤	楽天ウォレット
田中 朗	コインチェック株式会社
西尾 秀一	株式会社ＮＴＴデータ
深谷 貴宣	ServiceNow Japan合同会社
福岡 かよ子	株式会社インテック

他、CISO支援WGメンバー

どうして、CISOハンドブックを作ったのか？

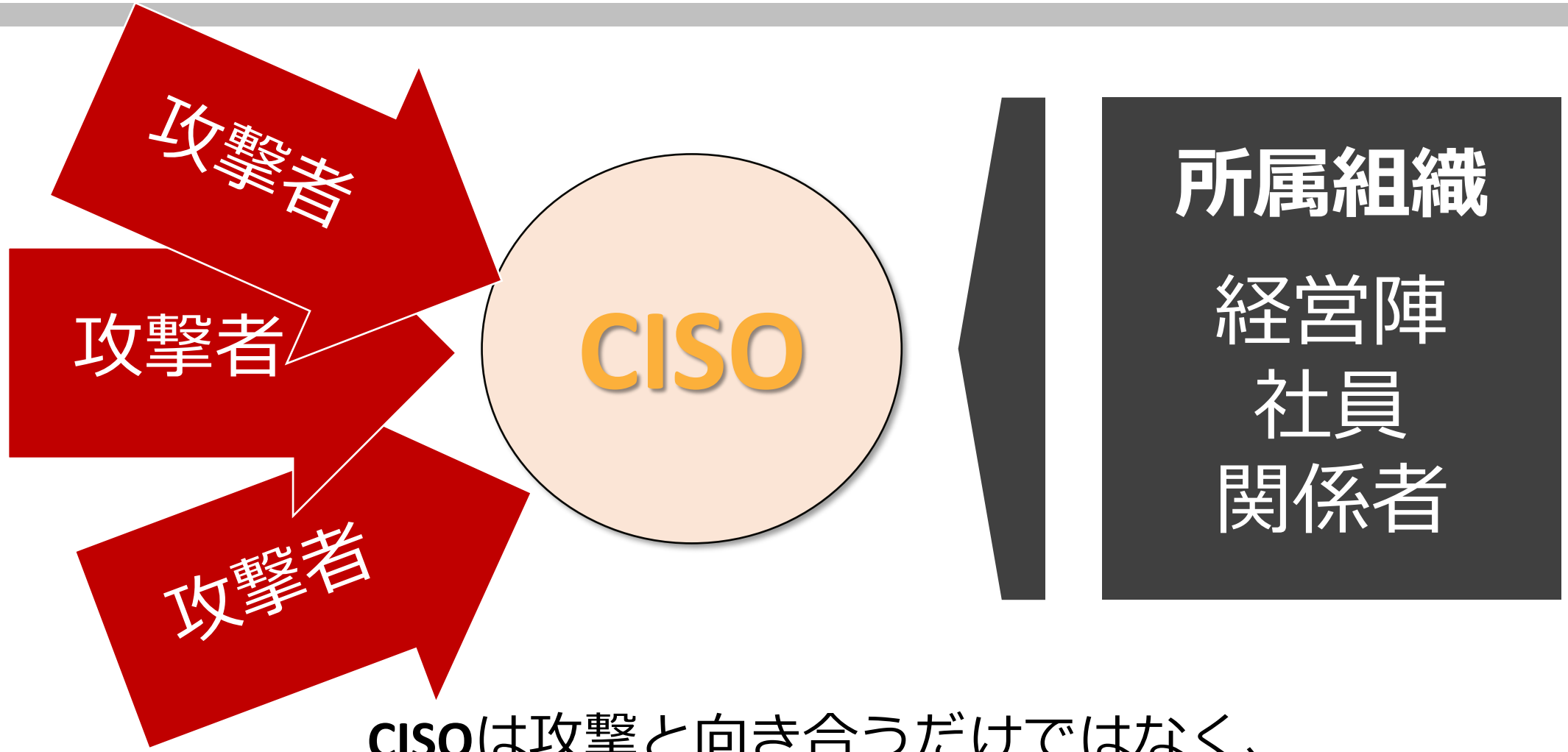
経営者はセキュリティを
理解しなければならない

というけれど…

ホントにそうなのか!?

セキュリティがわかる経営者を待つよりも
経営がわかるCISOを目指した方が良いのでは?

CISOが直面する二つの課題



CISOは攻撃と向き合うだけではなく、
組織内のステークフォルダーとも向き合う必要がある。

他の書籍と何が違うのか？

CISOハンドブックが目指すもの

- 「CISOが経営陣の一員として成すべきこと」
  - 実践するのためのガイドを提供
- 「経営陣がCISOと共に成すべきこと」
  - 経営陣がCISOを活用するための理解を促す試み
- 知識の集積ではなく「成すべきこと」を俯瞰する視点
  - CISO業務と要素の本質的な理解の足がかかり
  - 経営という意味でのマネジメント
  - 経営という視点でのセキュリティ
  - ベストプラクティスとその背景
- 特別損失対策からビジネス志向へ
  - ビジネスイネーブラとしてのセキュリティという視点

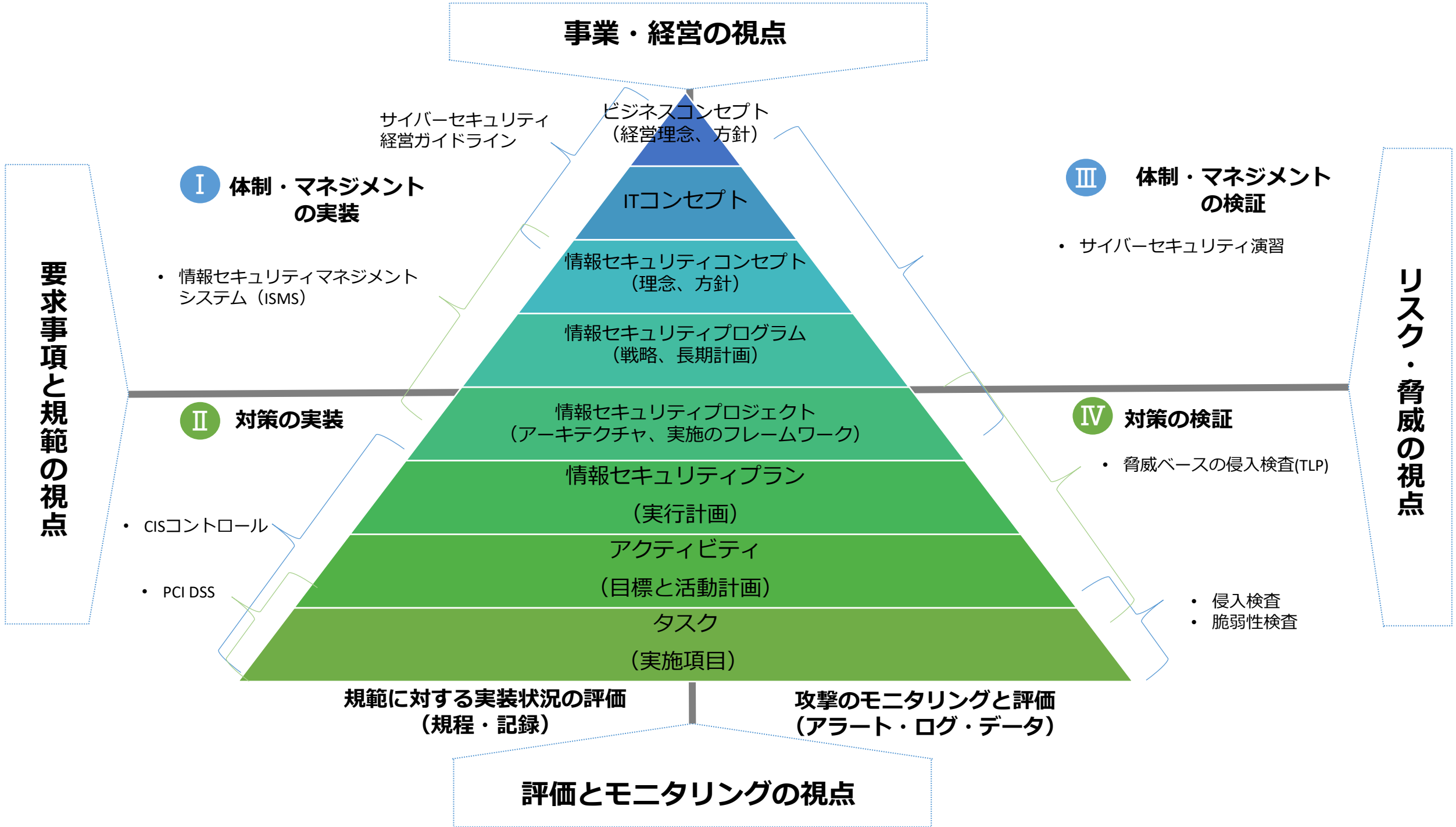
CISOハンドブックの背景とこれから

突き詰めて考えると、
CISOとして成功するってどういうこと？

内容は、当日のお楽しみ

CISOにとってどれが成功でしょう？

- 主要な標準・基準を理解し適切なセキュリティ対策を構築する
- 最新の攻撃を把握し高度な攻撃でも適切な対処を行う
- リスクに応じたコスト対効果の高い施策を行う
- 売上が伸びる
- 利益が伸びる


事業・経営の視点
サイバーセキュリティ
経営ガイドライン
ビジネスコンセプト
（経営理念、方針）
Ⅰ 体制・マネジメント
の実装
• 情報セキュリティマネジメント
システム（ISMS）
ITコンセプト
情報セキュリティコンセプト
（理念、方針）
情報セキュリティプログラム
（戦略、長期計画）
Ⅲ 体制・マネジメント
の検証
• サイバーセキュリティ演習
要求事項と規範の視点
Ⅱ 対策の実装
情報セキュリティプロジェクト
（アーキテクチャ、実施のフレームワーク）
情報セキュリティプラン
（実行計画）
アクティビティ
（目標と活動計画）
タスク
（実施項目）
Ⅳ 対策の検証
• 脅威ベースの侵入検査(TLP)
リスク・脅威の視点
• CISコントロール
• PCI DSS
• 侵入検査
• 脆弱性検査
規範に対する実装状況の評価
（規程・記録）
攻撃のモニタリングと評価
（アラート・ログ・データ）
評価とモニタリングの視点

DXとPDCA

- かみ合わない時間軸
  - そもそも、開発はプロジェクトだから、PDCAは合わない
- そうは云いながら、DevOpsは事業の側面がある
  - このため、（従来の）プロジェクト管理が馴染みにくい

- セキュリティが経営に関わるのは、究極のシフトレフトか？
  - 環境のテンプレート化など事前の仕込みが重要になる
    - リアクティブからプロアクティブ

プロジェクトと事業の違い

- 終わりの有無
  - プロジェクトには想定された終わりがあるが、事業は継続が前提
    - 継続できなくなったら終わり（目指せ永久機関！）
    - うまくいったことに伴う事業の拡大に備える必要がある
- 予算の考え方
  - プロジェクトは予算が余れば良い事だが、事業だとそうでもない
    - WG予算が余るのは、プロジェクトとしてみるとOKで、事業としてみるとNG
  - プロジェクトにBS（貸借対照表）はない
    - 事業にはお金の出所が付いて回る

CISOハンドブックをどう見てほしいか？

- 屍をさらしてみました
  - 知りたかったこと、概念としてまとめたかったことを書いています
  - いわば、自分が出来なかったこと、できたらよかった事も多いです
  - 究極のシフトレフトは、技術者が経営に入ることだと思います

  - 技術者が経営に加わる機会を得た時に、
    「成すべきこと」を行うための絵地図となることを目指しました

CISOハンドブック プレゼント

- 抽選で**5名様**に「CISOハンドブック」の**デジタル版**をプレゼントします。
- NSF2021に**ご参加登録メールアドレス**でお申し込みください。

- 当選者には、１カ月以内にJNSA事務局(mailto:office@jnsa.org)よりご案内いたします。
- ※落選された方へのご連絡はございません。ご了承ください。

キーワード

CISO

申し込みURL
https://forms.gle/o1Yb3jfbeZNmwhVH7

技術評論社　CISOハンドブックデジタル版（PDF）
https://direct.gihyo.jp/view/item/000000001358

CISO支援ワーキンググループメンバー
絶賛募集中です！

今後の予定

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。
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。

CISOs' Cyber War: How Did We Get Here? (Profile of Jack Miller ,Chief Information Security Officer of SlashNext)
https://www.darkreading.com/vulnerabilities---threats/cisos-cyber-war-how-did-we-get-here/a/d-id/1330737

今後の予定

- メンバーからのクレーム
  - 読んでるとわかった気になるが、業務で使おうと思うと使えない（T氏）
- WGの次のステップ
  - CISOハンドブックを業務に展開する資料を作ろう
    - リスク分析
    - セキュリティ計画
    - 報告書
    - その他
  - 取り上げた事例や手法を掘り下げてみる？
    - 定量リスク分析は興味深い
    - マチュリティモデルの展開も興味深い
  - 他に、面白いことはできないかな？

ここから先は、内容の抜粋

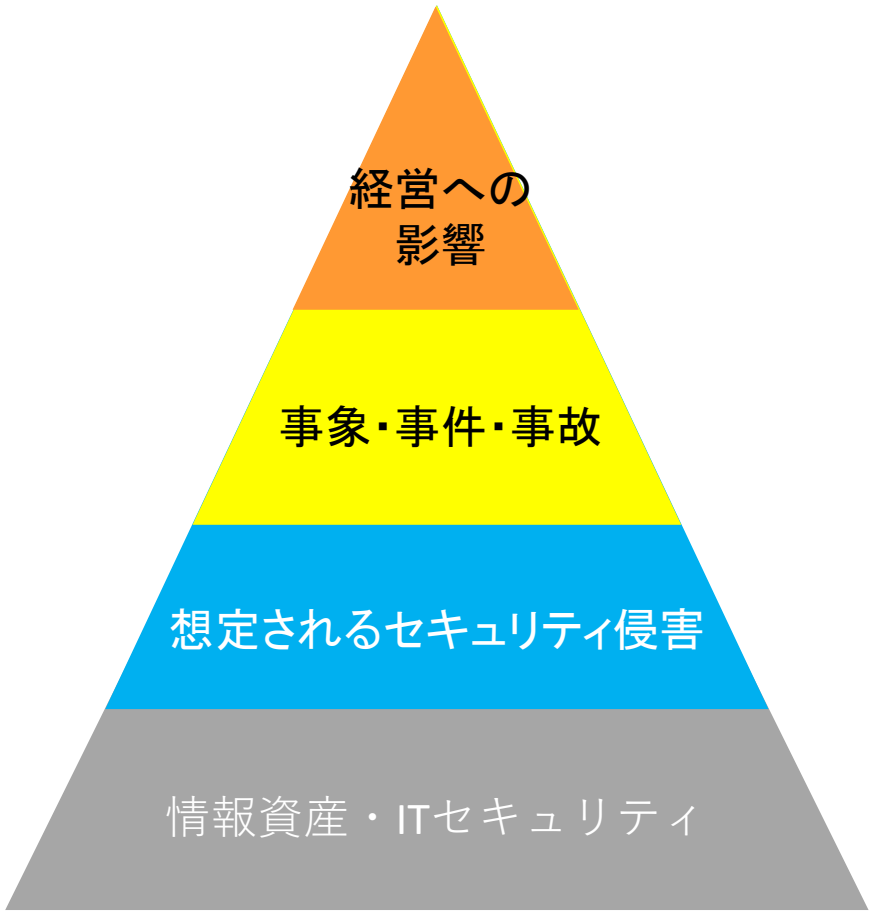
CISOハンドブックの概要（目次から）

CISOハンドブック 目次

目次　1 – 3

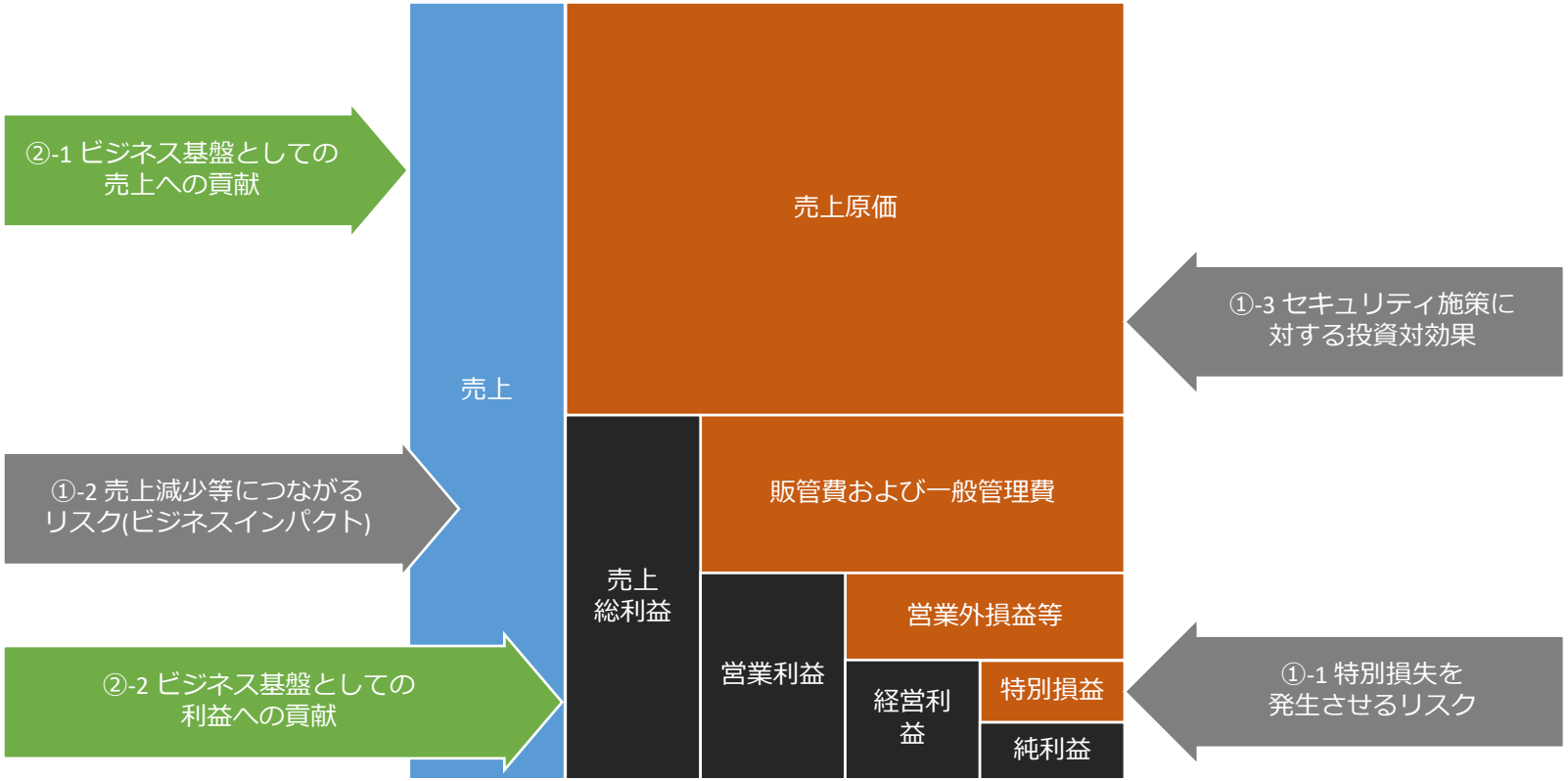
- 第1章　情報セキュリティの目的
  - ビジネス視点でセキュリティを捉えなおす
- 第2章　情報セキュリティマネジメントの基礎知識
  - リスク分析・エンタープライズリスクマネジメント
  - CISコントロールズとサイバーセキュリティフレームワーク
  - 経営サイクルと情報セキュリティマネジメントサイクル
  - マネジメントサイクルに沿った報告
- 第3章　基本となる経営指標
  - 経営における「数字」の重要性
  - 財務会計と管理会計
  - ファイナンス

CIAをビジネスリスクに展開



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	

セキュリティの二つの視点



ERM:エンタープライズリスク

ISO31000外部/内部状況とリスク項目例 (JIS Q 31000及びデロイト)

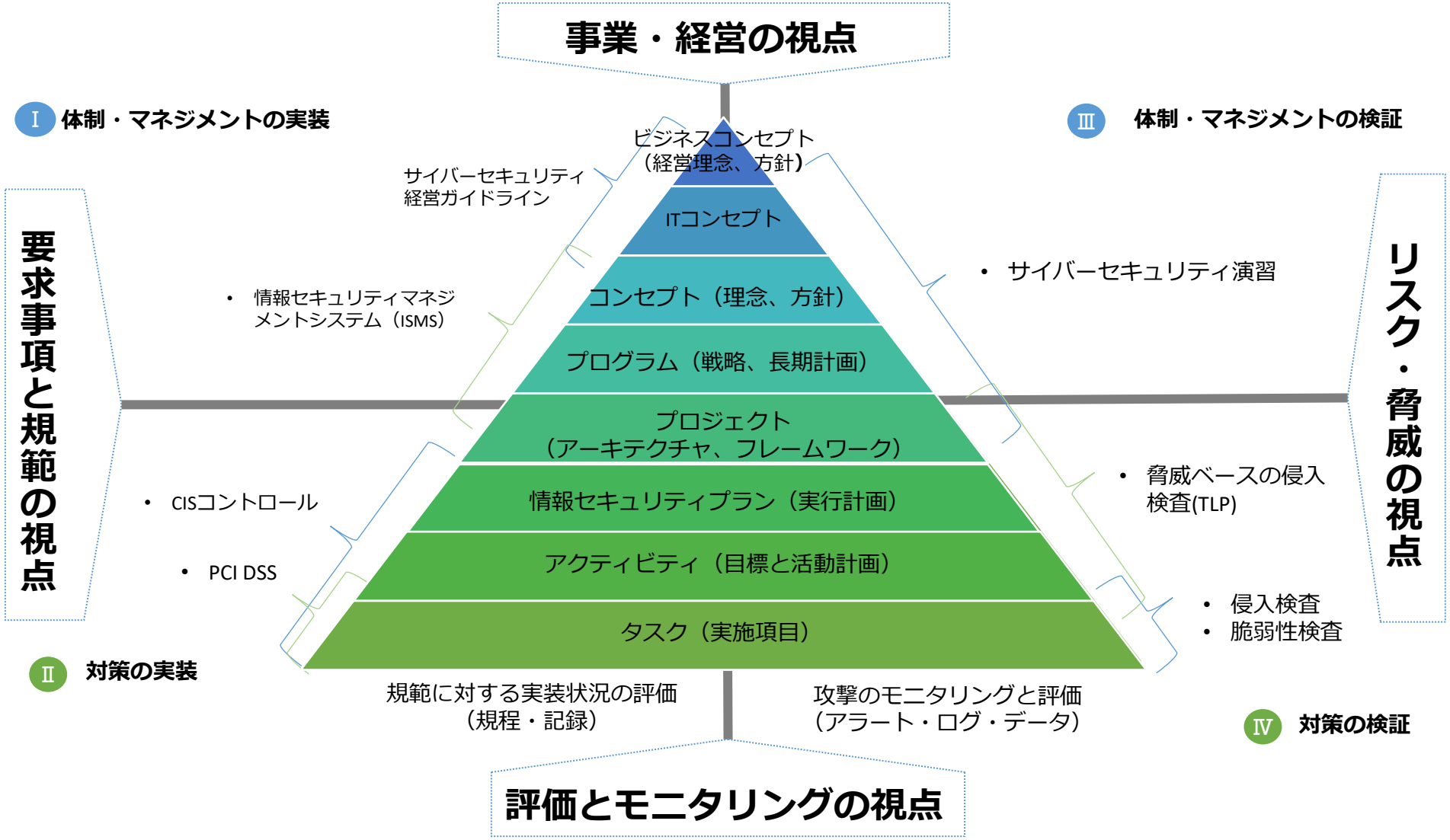
	主要な要因	分類	リスク項目の例
外部状況	国際、国内、社会または近隣地域を問わず、社会及び文化、政治、法律、規制、金融、技術経済、自然並びに競争の環境	政治	朝鮮半島情勢 / 中国・ロシアにおける政治情勢 東南・南アジアにおけるテロ等 / 中東・中近東におけるテロ、政治情勢 アフリカにおけるテロ、政治情勢
		金融	景気変動、金融危機、財政難 / 原材料並びに原油の高騰 金融犯罪
		経済	
		社会及び文化	不買運動の発生 / 流通システムの変化（小売店とAmazon）
		技術	技術・技術領域の変化・陳腐化
		法律/規制	法改正や業界基準変更時の対応の遅れ / 知的財産権侵害 公害等の環境関連法規制対応 / 法令順守違反 / 訴訟被害
		自然	地震・風水害等、災害の発生 / 疫病の蔓延（パンデミック）等の発生
		競争の環境	市場における価格競争
	組織の目的に影響を与える主要な原動力及び傾向		N/A
	外部ステークホルダとの関係並びに外部ステークホルダの認知及び価値観	株主	株主訴訟 / 風評被害などによる株価の下落 / 敵対的買収
		顧客	風評被害・不買運動等の発生
		取引先他	サプライチェーン寸断

ERM:エンタープライズリスク

ISO31000外部/内部状況とリスク項目例 (JIS Q 31000及びデロイト)

	主要な要因	分類	リスク項目の例
内部状況	統治、組織体制、役割及びアカウンタビリティ	統治	財務報告の虚偽記載 役員・従業員の不正・贈収賄等 / 経営の機能不全 子会社に対するガバナンス不全 / 買収号の事業統制不全
		体制	
		役割	
	方針、目的及びこれらを 達成するために設定された戦略	経営戦略	N/A
		事業計画	
	資源及び知識として把握される能力 （例えば、資本、時間、人員、プロセス、システム、技術）	資本	製品/サービスの品質チェック体制の不備リコール 設備事故 業務運用ミスによる多額損失発生 品質管理
		人間/時間	
	内部ステークホルダとの関係並びに 内部ステークホルダの認知及び価値観	プロセス/システム	
		技術	
	組織の文化	組織の行動原理	コンダクトリスク カルテル談合等の組織不正
		組織の思考様式	
	情報システム、情報の流れ及び意思決定プロセス （公式及び非公式の両方を含む）	情報資産	サイバー攻撃・ウイルス感染 / 情報漏洩 大規模システムダウン・情報逸出 *情報資産を取り扱う物理的範囲
		情報処理	
		物理的範囲*	
		リスク評価・分析	
	組織が選択した規格、指針及びモデル	規格/指針	N/A
		モデル	
	契約関係の形態及び範囲	従業員との契約	人材流出、人材獲得の困難による人材不足 人件費高騰 / 過労死、長時間労働問題の発生 / 労使問題
		取引先との契約	顧客対応の不備

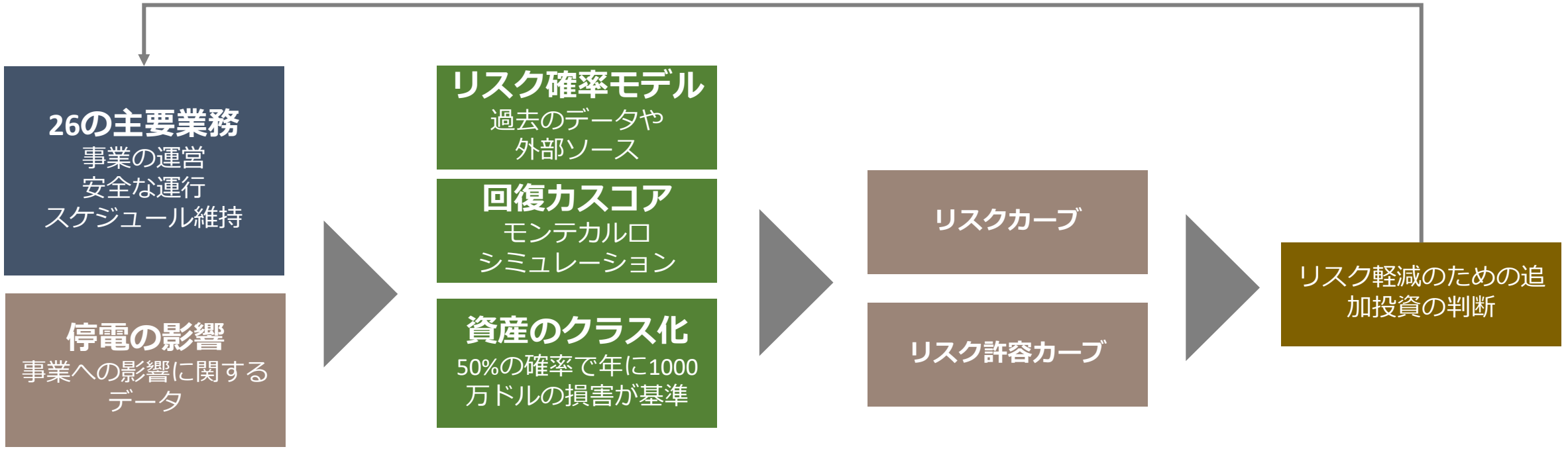
セキュリティ対策の階層化と象限



目次 4-6

- 第4章　情報セキュリティの指標化
  - コストとしての情報セキュリティ
  - 情報セキュリティ指標を経営の数字に展開（BSC）
- 第5章　モニタリングと評価手法
  - 組織情報のセキュリティ成熟度評価（C2M2）
  - 実装レベルのモニタリング（CISコントロールズの実装）
  - サイバー攻撃への対応能力評価（Red Teaming/TLPT)
- 第6章　情報セキュリティ監査
  - 情報セキュリティ監査の目的と監査の分類
  - 監査人の選び方
  - CISOは監査報告をどう活かすのか

Union Pacificの事例



サイバー攻撃の影響を理解するための参考

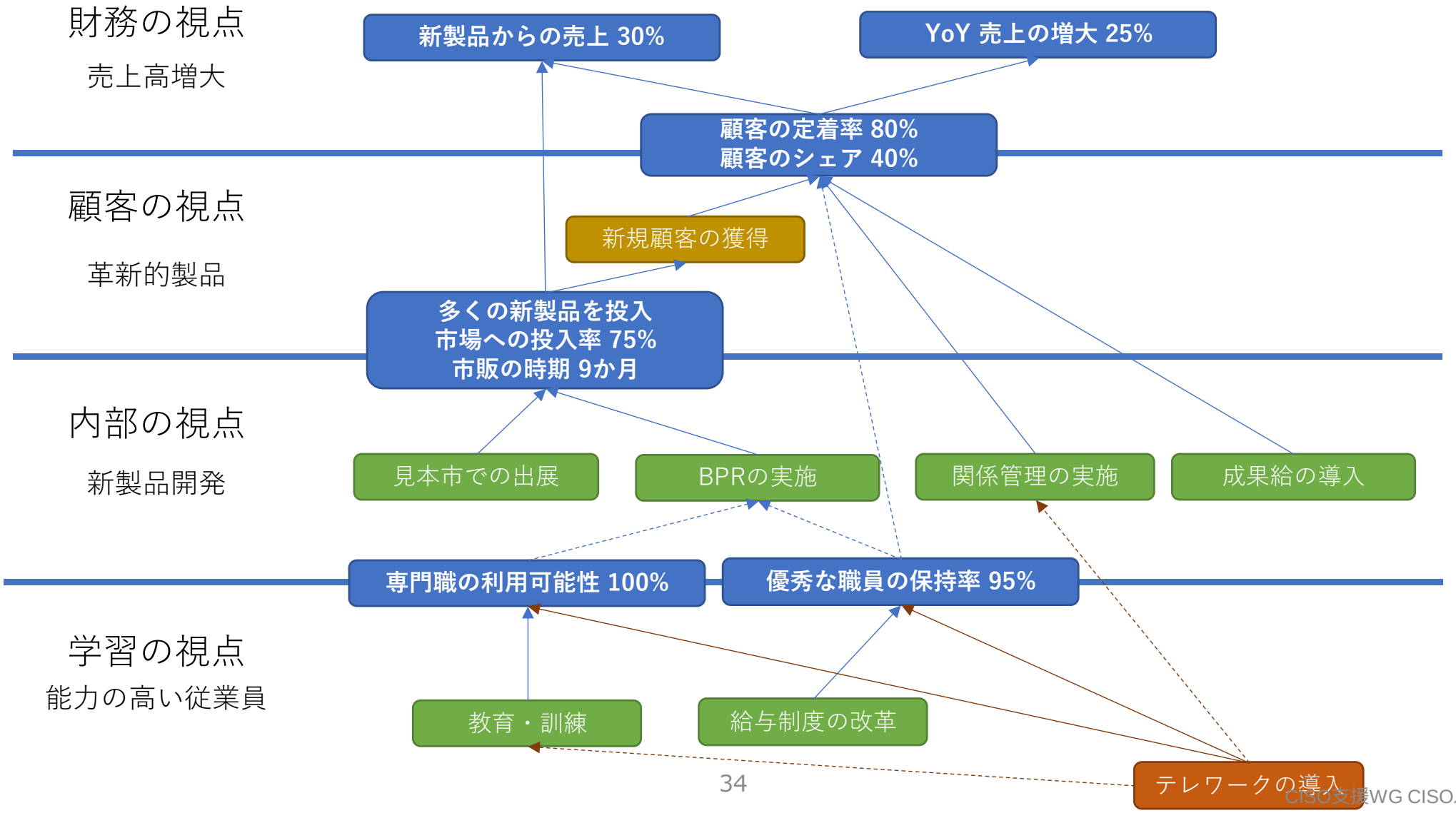
リスク評価の4つの視点
- 保険数理
- 監査人（コンプライアンス）
- 法律顧問
- サイバーリスク評価チーム

＋財務部門による費用・機会損失の算出
＋社内外ソースに基づくインシデント発生確率の算出

下記資料を基に高橋が作成

Union Pacific tracks cyber risk via its own probability modeling methodology
https://www.scmagazine.com/infosec-world-2020/union-pacific-tracks-cyber-risk-via-its-own-probability-modeling-methodology/

戦略マップ：テレワーク導入



目次 7-8

- 第7章　情報セキュリティアーキテクチャ
  - 情報セキュリティアーキテクチャの基本要素
  - エンタープライズセキュリティアーキテクチャ
    - SABASA,COBIT, TOGAF, ITIL
  - ゼロトラスト
- 第8章　DXと情報セキュリティ
  - DXとテクノロジー
  - OODA, アジャイル, DevOps
  - DXのセキュリティとPDCA
  - CISOはいかにDXに貢献できるのか

DevOpsとCISOの仕事

Ops: 実システム運用

CISO: モニタリングとオペレーションのデリバリー、情報収集、分析を監修する。
- コストとスピードがビジネスリスクに適合しているか。
- 個別のインシデントについて、どの段階を担当する者が対応にあたるべきか(DevかOpsかSREか)示唆する。
- 分析から得られたリスクの優先順位付けを評価し、改善サイクルにアウトプットしているか。

Dev:開発・改善・改修

CISO:システムに潜在するセキュリティ・リスク、ビジネス・リスクについてクリアにする活動を監修する。
- Devチームが解決に着手できるための十分な情報はスピーディに行き届いているか。
- 修正プロセスのスピードとコストはビジネスリスク対応に適合しているかどうか。

共通：CISOによるガバナンス支援
・ビジネス戦略に適合した指針が与えられているか
・適切な訓練とガイダンスが与えられている状態にあるか
・コンプライアンスの変化がDevOpsにもたらす影響は何か

PDCAとDevOps/DXのイメージ

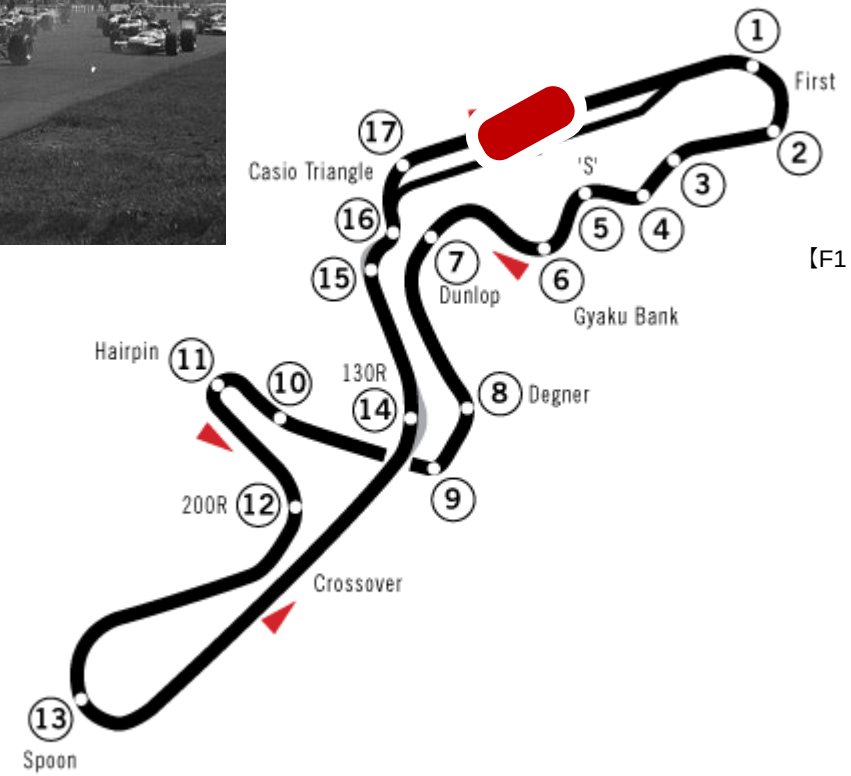
DevOps / DX

ジョン・サーティース
RA301（1968年）

©www.CliparsFree.de

【F1 2019】AI100 予選＆５LAPレース（テスト）【ロシアGP 】 https://youtu.be/VmnZaOXxzSk

PDCA



テレメトリーシステムとは？ | F1用語集 | Formula1-Data (formula1-data.com)2019年
https://formula1-data.com/glossary/car/body/telemetry-system

ホンダF1参戦の歴史 第1期
https://www.honda.co.jp/F1/spcontents2006/history/01/

目次 9-10

- 第9章　クラウドファーストの情報セキュリティ
  - クラウドサービス評価時の考慮点
  - 実践的な情報セキュリティ評価
  - セキュリティの主要な評価要素
  - 蔵度サービスをセキュアに利用するために
- 第10章　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
  - セキュリティインシデントの推移
  - 新しい領域のインシデント
  - 脆弱性評価
  - インシデントを想定したセキュリティ評価

考慮すべき法令・基準

個人情報を取り扱う際に適用される法令

名所	種類	対象	概要
個人情報の保護に関する法律（個人情報保護法）	法令	日本在住の個人の個人情報	個人情報の取り扱いについて定めた法律
General Data Protection Regulation（GDPR）一般情報保護指令	法令	EU域内在住の個人の個人情報	欧州連合（EU: European Union）によって定められたプライバシーとセキュリティに関する法律
California Consumer Privacy Act（CCPA）	法令	CA在住の個人の個人情報	カリフォルニア州（CA: California）によって定められた消費者のプライバシー保護に関する法律

データに基づき適用される基準

名所	種類	対象	概要
Payment Card Industry Data Security Standard（PCIDSS）	基準	クレジットカード情報（業界）	クレジットカード保持者データ（CHD: Cardholder Data）を安全に取り扱う事を目的として策定されたセキュリティ基準
3省3ガイドライン	基準	医療情報（日本）	厚生労働省、経済産業省、総務省が定める医療情報を委託、クラウドサービス上で安全に利用することを目的として策定されたガイドラインの総称
HIPAA	法令	医療情報（米国）	保護された医療情報のセキュリティとプライバシーの保護に関する監査

業界に適用される法令・基準

名所	種類	対象	概要
金融機関等コンピュータシステムの安全対策基準	基準	金融機関（日本）	金融情報システムセンター(FISC)が定める金融情報システムの安全対策について定めた基準
政府機関等の情報セキュリティ対策のための統一基準群	基準	政府機関（日本）	厚生労働省、経済産業省、総務省が定める医療情報を委託、クラウドサービス上で安全に利用することを目的として策定されたガイドラインの総称

主要な国際標準

規格、認証	説明
ISO/IEC27001	ISMS適合性評価制度として知られている通り、組織の情報セキュリティマネジメントをISO/IEC 27001（JIS Q 27001）に基づき評価する仕組み。
ISO/IEC27017	ISO/IEC27001に基づくISMS認証に加えて、その適用範囲に含まれるクラウドサービスの提供または利用に関して、ISO/IEC27017に規定されるクラウドサービス固有の管理策が実施されていることを認証する仕組み。
ISO/IEC27018	ISO/IEC27001に基づくISMS認証に加えて、CSPがISO/IEC27018に規定される個人情報をクラウド上で管理するにあたっての管理策が実施されていることを認証する仕組み。
SOC1 (System and Organization Controls 1)	米国公認会計士協会（AICPA）が定める、財務報告書に係る内部統制の評価を目的として、業務委託先を審査する仕組み。特定の時点における内部統制の整備状況を評価するType1レポート、運用状況を含めた評価を実施するType2レポートがある。
SOC 2	米国公認会計士協会（AICPA）が定める、情報セキュリティ、プライバシーに関する内部統制を評価する仕組み。特定の時点における内部統制の整備状況を評価するType1レポート、運用状況を含めた評価を実施するType2レポートがある。
SOC 3	SOC2と同様の評価が行われるが、内部統制の個々の評価手続き・評価結果は開示されず、総括的で定型的な評価結果と印象取得に係る意見のみを開示する。
Security Trust Assurance and Risk（STAR）	クラウドセキュリティアライアンス（CSA）によって管理、運営されているプログラム。STARプログラムは、実施した審査により3つのレベル分けをしています。
クラウドセキュリティ（CS）マーク	CSPが行う情報セキュリティマネジメントの取り組み状況に関する内部監査ついて、JASAが定めるクラウド情報セキュリティ管理基準に準拠した監査が適切に行われているかを評価する。申請により認定されるCSシルバー、外部監査が行われ、認定されるCSゴールドの２種類がある。
プライバシーマーク	一般財団法人日本情報経済社会推進協会（JIPDEC)によって管理、運営される、事業者が個人情報の取り扱いを適切に行う体制を整備していることを認定する制度。

各国の規格・認証

規格、認証	国	説明
政府情報システムのためのセキュリティ評価制度（ISMAP）（認定）	日本	日本政府機関が使用するクラウドとしての認証制度。 政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図る。
FedRAMP	米国	米国政府機関が使用するクラウドとしての認証制度。 （Federal Risk and Authorization Management Program） 連邦情報セキュリティマネジメント法（FISMA）に基づき、クラウドサービス導入の際したセキュリティ認証基準。 米国省庁が利用するには、FedRAMPの取得が必要。
Government-Cloud (G-Cloud)	イギリス	英国政府機関が運営する、政府機関向けクラウド・コンピューティング・サービスの調達フレームワーク。
Cloud Computing Compliance Criteria Catalogue（C5）	ドイツ	ドイツ政府機関とその関連団体がパブリック クラウド ソリューションを導入する際の必要最低限のクラウド セキュリティを定めた監査標準。
Information Security Registered Assessors Program （IRAP）	オーストラリア	オーストラリア政府機関が運営する、オーストラリア政府のICT（情報通信技術）システム導入におけるセキュリティ評価を提供するための仕組みであり、民間企業や公共団体のサービスは本仕組みに基づく審査、認証を取得することができる。
Multi-Tier Cloud Security Standard Singapore Standard （MTCS SS)	シンガポール	シンガポール政府機関が定めるクラウドセキュリティの認証であり、CSPは独立した MTCS 認証機関による監査を受けることにより、認証を受けることができます。

実践的CSPセキュリティ評価
ENISA: Cloud Security Guide for SMEs

ENISA: 中小企業のためのクラウドセキュリティガイド

本ガイドは、中小企業がクラウドサービスを調達する際に考慮すべき、セキュリティリスクと要件(Opportunity)を理解するための支援を目的としている。本書には、一連のセキュリティリスクとセキュリティ要件、および中小企業がプロバイダのセキュリティレベルを理解するために利用できるセキュリティに関する質問のリストが含まれています。リスクと要件は、セキュリティ上の質問とリンクしているため、最終的な結果は、ユーザのニーズや要件に応じてカスタマイズすることができる。この情報は、2つのユースケースの例と、適用されるデータ保護法と各国の関係当局の概要を示す付録によってサポートされている。

https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes　(日本語訳：CISO支援WG)

	A	B	C	D	E
1	Sample				
2	**Impact rating**	0	0		**利用回避の判断**
3	Confidentiality (3 High)	2	0		Sample Proを利用し、限られた人だけアクセス出来るProtected modeの利用義務付けることで、Confidentialを含めた、データの取り扱いを認める。
4	Integrity (3 High)	1	0		ただし、公開を前提とした論文などのドキュメントに限るものとする
5	Availability (3 High)	1	0		（2018/06/14）
6	File Share (1:no, 2: internal, 3:external)	3	0		
7	(1-3)	Rating	Assess		
8	S01: Linkによるファイル共有	3	1.0		**主要な取り扱い情報のインパクト**
9	S02: ファイル共有機能	3	2.0		申請前の特許情報など、当社にとって機密性の高い情報を取り扱う。これが漏れた場合は、公知の情報とされ、特許の取得が難しくなる可能性があり、特にLink機能を使った共有方法が問題と考えられている。
10	S03: MFA	3	2.0		取り扱う情報に顧客のCofidential情報が含まれる可能性は低い
11	S04: SSO	3	2.0		
12	O01: Geographic spread (A)	1	2.7		
13	O02: Elasticity(弾力性・柔軟性) (A)	1	3.0		
14	O03: Standard formats and interfaces	0	0		**セキュリティ評価**
15	O04: Physical security max(C,I,A)	2	3		アプリケーション開発、サーバーセキュリティ、ネットワークセキュリティについて、Web上に明確な記載がない。
16	O05: Incident response around-the-clock max(C,I,A)	2	3		取り扱うデータの性格上、データの暗号化ができないなど、セキュリティ面での課題がある。
17	O06: Software development max(C,I,A)	2	1.0		Sampleのサイトが攻撃を受けた際には、情報が流出する可能性は少なくない。
18	O07: Patching and updating max(C,I)	2	1.0		
19	O08: Backups (A)	1	1.7		
20	O09: Server-side storage (C)	2	2.0		
21	O10: Security-as-a-service and security add-ons	0	0		
22	O11: Certification and compliance max(C,I,A)	2	2.0		
23	R01: Software security vulnerabilities max(C,I,A)	2	1.0		
24	R02: Network attacks max(C,I,A)	2	1.0		
25	R03: Social engineering attacks max(C,I)	2	2.3		
26	R04: Management GUI and API compromise max(C,I)	2	2.0		
27	R05: Device theft/loss	0	0		
28	R06: Physical hazards (A)	1	2.0		
29	R07: Overloads (A)	1	2.0		
30	R08: Unexpected costs	0	0		
31	R09: Vendor lock-in	0	0		
32	R10: Administrative or legal outages (A)	1	1.0		
33	R11: Foreign jurisdiction issues (A)	1	1.0		

https://www.jnsa.org/result/2019/act_ciso/

目次 11-13

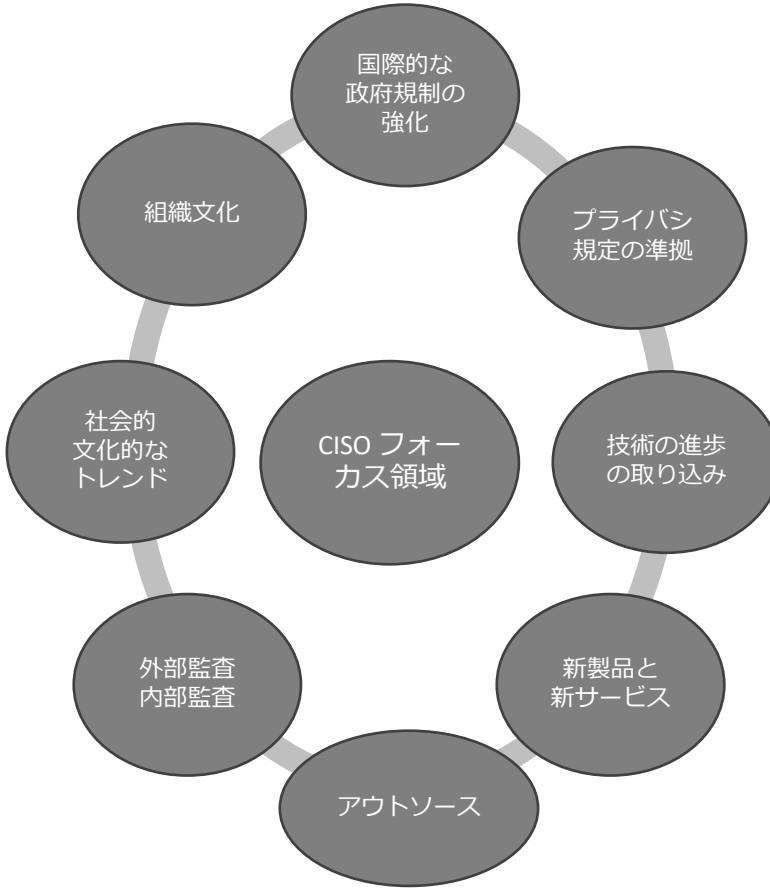
- 第11章　製品選定とベンダー選定
  - セキュリティソリューション検討時の留意点
  - ベンダー選定時の留意点
- 第12章　CISOの責務と仕事
  - CISOの役割と推移
  - サイバーセキュリティ経営ガイドライン
  - 米国におけるCISO像
- 第13章　経営陣としてのCISOへの期待

CISO COPASS: CISOの歴史

JNSA

1990s-2000	2000-2004	2004-2008	2008-2016	2016-2020s
1 限定的なセキュリティ＝ログオンとパスワード 最初のCISO 1995年	2 規制遵守の時代 CISOの採用	3 リスク指向 CISOの普及・浸透	4 脅威対応のセキュリティ ソーシャル、モバイル、クラウド CISO	5 プライバシーとデータ対応 CISO
• 情報は外部に興味深いものではない • 汎用機からPC/LAN、インターネットへ • セキュリティ＝ FW＋AV IT業務の一環としてのセキュリティ • ITの領域に留まる • 技術指向のセキュリティ • CIOの登場	代表的な規制 • HIPPA (1996) • Gramm-Leach-Bliley Act(1999) • Sarbenes-Oxley Act(2002) • California breach notification law S.B. 1386(2003) 100%の規程遵守 • 深い技術よりも、規制の理解、保護、管理、技術、運用の安全策を提供できる人	リスクレベルに応じた投資と保護 • チェックリストと委員会制度の限界 セキュリティ事故と複雑化するセキュリティ領域 • 技術スキル＋ソフトスキル(ISC)2 • NIST SP800-53* CISOの普及・浸透 • IT部門に留まる • 情報セキュリティは組織リスク（GRC**） • 法務部門（規制） • プライバシー部門	ITと社会環境の変化 • スマートフォン • SNS • BYOD • 生活形態の変化と企業での利用 • 新技術の業務活用 CISO:技術者・マーケティング・政治家 • 業務部門とのコンフリクト • 新しいアプローチが必要	プライバシーの懸念と分散するデータ • GDPR • Cloud • オフシュア • ベンダー CISO:上級管理職のパートナー • 全社リスク対策 • イニシアチブ* • 国家・犯罪攻撃への対応 • プライバシの評価 • アジャイルビジネスのサポート 第1/第3象限へ集中 **

Todays and Tomorrow

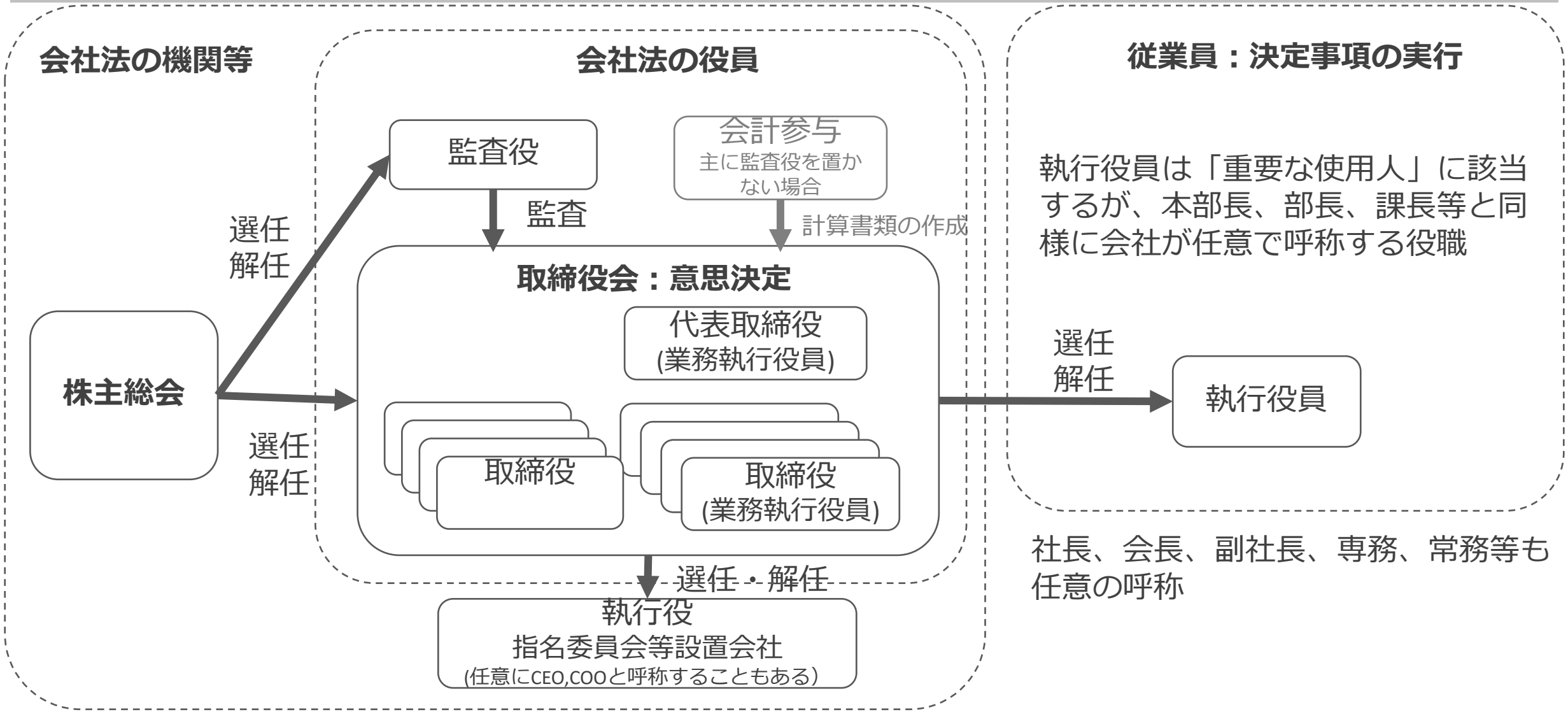


*NIST SP800-53（「米国連邦情報システムのセキュリティおよびプライバシー管理の管理策」
**GRC: Governance Risk Compliance

*イニシアティブ：重要な企業活動のことだと考えられる
**第1象限：重要で緊急
第2象限：重要ではないが緊急

出典：CISO COMPASS by TODD FITZGERALD
高橋による翻訳と構成

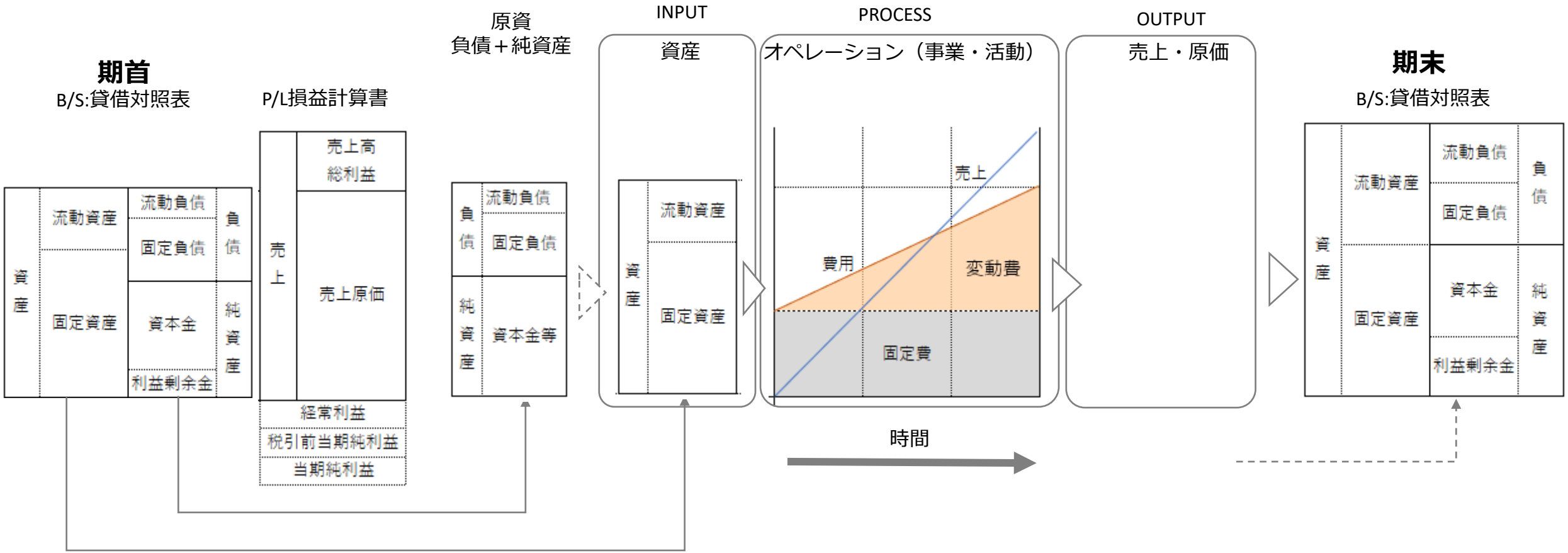
会社法と役職


会社法の機関等
会社法の役員
従業員：決定事項の実行
監査役
会計参与
主に監査役を置かない場合
監査
計算書類の作成
選任
解任
株主総会
取締役会：意思決定
代表取締役
(業務執行役員)
取締役
取締役
(業務執行役員)
選任
解任
選任・解任
執行役
指名委員会等設置会社
(任意にCEO,COOと呼称することもある)
執行役員は「重要な使用人」に該当するが、本部長、部長、課長等と同様に会社が任意で呼称する役職
選任
解任
執行役員
社長、会長、副社長、専務、常務等も任意の呼称

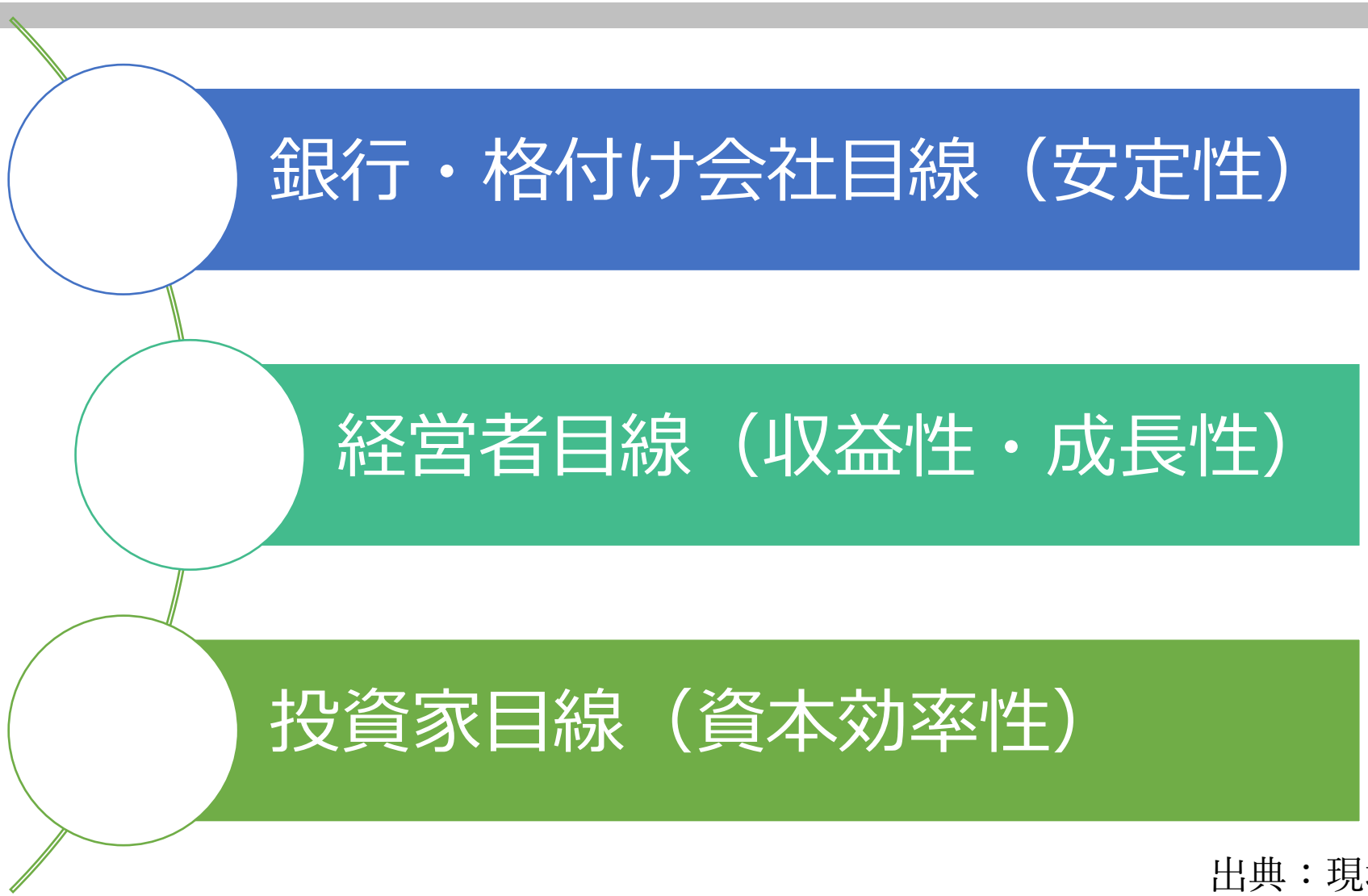
第3章　基本となる経営指標

BS, P/Lの関係

因果関係の方向が、技術系と違う点がわかりにくくしている
左から右に因果関係を記述して、HIPO的に表記してみる



財務諸表に対する3つの目線



出典：現場で使える決算書思考

B/SとP/Lの構成による財務指標の変化

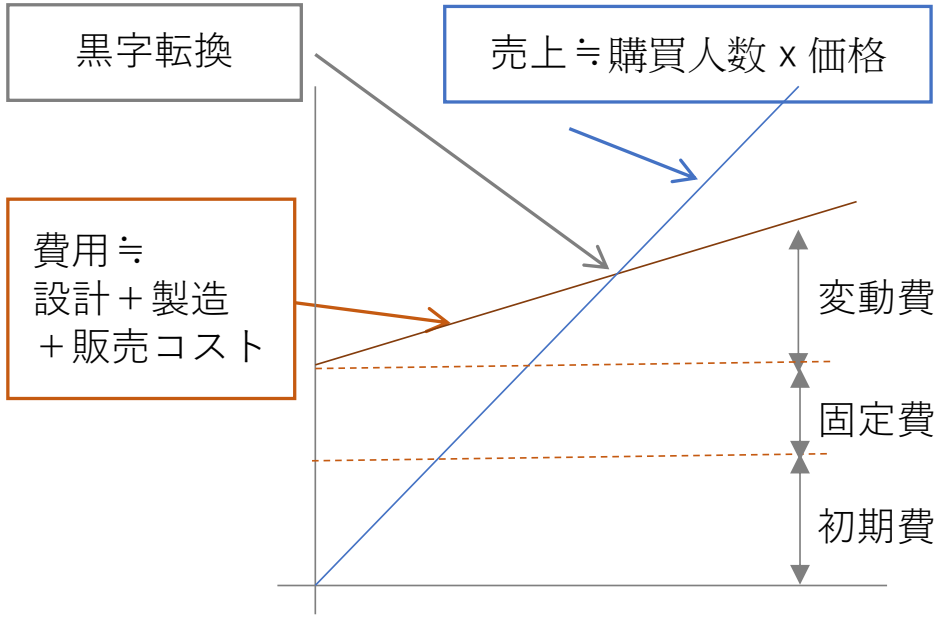
		基準	当座+100 商品-100		当座+100 固定資産-100		流動負債+100 自己資本-100		売上-100 売上原価-100		売上原価-100 販管費+100		純資産+600 負債 -600		負債100 現金を未活用		純資産100 現金を未活用	
資産	流動資産	500		500		600		500		500		500		500		600		600
	当座資産	300	100	400	100	400		300		300		300		300	100	400	100	400
	商品	200	-100	100		200		200		200		200		200		200		200
	固定資産	500		500	-100	400		500		500		500		500		500		500
	総資産	1000		1000		1000		1000		1000		1000		1000		1100		1100
負債	流動負債	400		400		400	100	500		400		400	-300	100	100	500		400
	固定負債	300		300		300		300		300		300	-300	0		300		300
	純資産	300		300		300	-100	200		300		300	600	900		300	100	400
	総負債	1000		1000		1000		1000		1000		1000		1000		1100		1100
損益	売上高	1500		1500		1500		1500	-100	1400		1500		1500		1500		1500
	売上原価	1000		1000		1000		1000	-100	900	-100	900		1000		1000		1000
	売上総利益	500		500		500		500		500		600		500		500		500
	販売管理費	400		400		400		400		400	100	500		400		400		400
健全性指標	流動比率	125	1.00	125	1.20	150	0.80	100	1.00	125	1.00	125	4.00	500	0.96	120	1.20	150
	当座比率	75	1.33	100	1.33	100	0.80	60	1.00	75	1.00	75	4.00	300	1.07	80	1.33	100
	固定比率	167	1.00	167	0.80	133	1.50	250	1.00	167	1.00	167	0.33	56	1.00	167	0.75	125
	固定長期比率	83	1.00	83	0.80	67	1.20	100	1.00	83	1.00	83	0.67	56	1.00	83	0.86	71
	自己資本率	30	1.00	30	1.00	30	0.67	20	1.00	30	1.00	30	3.00	90	0.91	27	1.21	36
資本利益率	ROI(営業利益)	0.10	1.00	0.10	1.00	0.10	1.00	0.10	1.00	0.10	1.00	0.10	1.00	0.10	0.91	0.09	0.91	0.09
	利益率	0.07	1.00	0.07	1.00	0.07	1.00	0.07	1.07	0.07	1.00	0.07	1.00	0.07	1.00	0.07	1.00	0.07
	回転率	1.50	1.00	1.50	1.00	1.50	1.00	1.50	0.93	1.40	1.00	1.50	1.00	1.50	0.91	1.36	0.91	1.36
	ROE	0.30	1.00	0.30	1.00	0.30	1.50	0.45	1.00	0.30	1.00	0.30	0.33	0.10	1.00	0.30	0.75	0.23
	売上高経常利益率	0.06	1.00	0.06	1.00	0.06	1.00	0.06	1.07	0.06	1.00	0.06	1.00	0.06	1.00	0.06	1.00	0.06
	純資産回転率	5.00	1.00	5.00	1.00	5.00	1.50	7.50	0.93	4.67	1.00	5.00	0.33	1.67	1.00	5.00	0.75	3.75

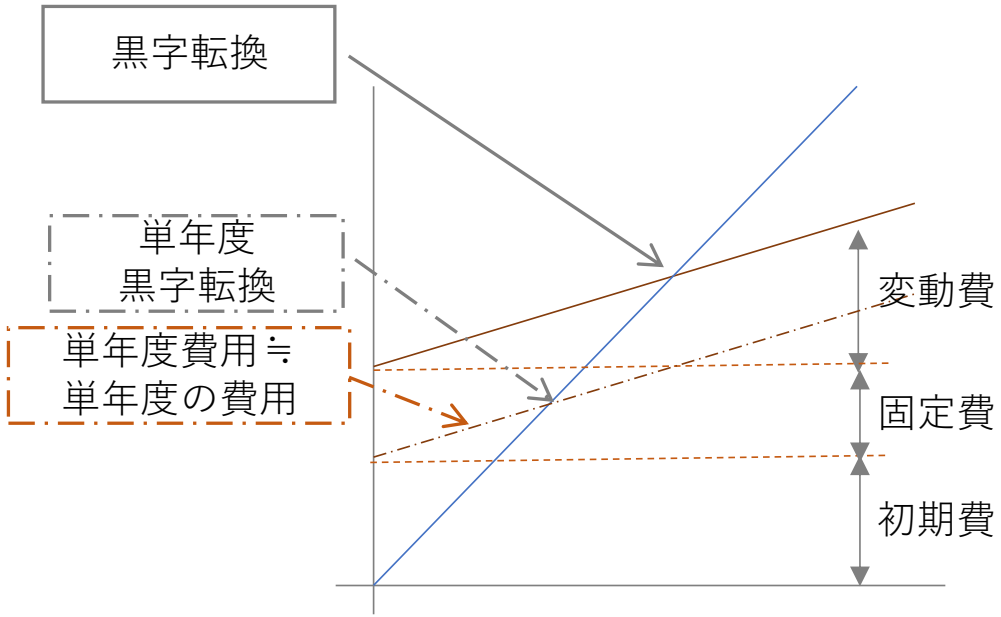
事業計画：７つの質問

1. あなたの製品は何か
2. 顧客は誰か
3. 誰が売るのか
4. どれだけの人が買うのか
5. 設計・製造のコストはいくらか
6. 価格はいくらか
7. 黒字転換はいつか

良いビジネス（儲かります）！は、どういう意味なのか

- いつになったら儲かるのか？
- 儲かる前に潰れることはないのか？
- 本当にお金になる気配があるのか？





出典：シリコンバレー流意思決定　ビジネスを成功させる7つの質問

4種類の事業計画の比較

		事業計画(1)	事業計画(2)	事業計画(3)	事業計画(4)
PL	売上高	1,020	1,034	1,587	1,527
	固定費・変動費	910	922	1,202	1,163
	減価償却	64	20	20	20
	売上原価	974	942	1,222	1,183
	売上総利益	46	92	366	343
	販売管理費	0	0	0	0
	営業利益	46	92	366	343
	営業外収益	0	0	0	0
	営業外費用	0	0	0	0
	経常利益	46	92	366	343
BS 資産	流動資産	493	493	1,121	1,286
	当座資産(現金)	426	425	1,015	1,185
	売掛金	67	68	106	101
	商品	0	0	0	0
	固定資産	760	225	225	225
	減価償却累計額	0	0	0	0
	総資産	1,253	718	1,346	1,511
BS 負債	流動負債	1,033	334	353	350
	流動負債	1,000	300	300	300
	買掛金	33	34	53	50
	固定負債	0	0	0	0
	純資産	220	384	993	1,161
	損益	-280	-116	493	661
	資本	500	500	500	500
	総負債	1,253	718	1,346	1,511
CF	営業活動CF	113	160	472	444
	投資活動CF	64	20	20	20
	財務活動CF	5	5	10	7

セキュリティトレーニング事業の計画
（3年後の期末を評価）

- 事業計画１：オンプレミス
- 事業計画２：クラウド2年で黒字化
- 事業計画３：クラウド1年で黒字化
- 事業計画４：資格認定を伴うサブスクリプション

健全性指標	流動比率	48	154	345	391
	当座比率	41	127	288	339
	固定比率	61	31	17	15
	固定長期比率	61	31	17	15
	自己資本率	18	54	74	77
ROI	ROI(営業利益)	3%	11%	43%	40%
	利益率	5%	9%	23%	22%
	回転率	67%	124%	186%	180%
ROE	ROE	9%	18%	73%	69%
	売上高経常利益率	5%	9%	23%	22%
	純資産回転率	204%	207%	317%	305%

むすび

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。
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。

CISOs' Cyber War: How Did We Get Here? (Profile of Jack Miller ,Chief Information Security Officer of SlashNext)
https://www.darkreading.com/vulnerabilities---threats/cisos-cyber-war-how-did-we-get-here/a/d-id/1330737

今後の予定

- メンバーからのクレーム
  - 読んでるとわかった気になるが、業務で使おうと思うと使えない（T氏）
- WGの次のステップ
  - CISOハンドブックを業務に展開する資料を作ろう
    - リスク分析
    - セキュリティ計画
    - 報告書
    - その他
  - 取り上げた事例や手法を掘り下げてみる？
    - 定量リスク分析は興味深い
    - マチュリティモデルの展開も興味深い
  - 他に、面白いことはできないかな？

CISO支援ワーキンググループメンバー
絶賛募集中です！

CISOハンドブック

業務執行のための情報セキュリティ実践ガイド

高橋正和、荒木敏子、池上美千代、岡田良太郎、唐沢勇輔、北瀬麻理子、武田一城、植喜風、田中昭、西尾秀一、深谷貴宣、JNSA CISO 支援ワーキンググループ 著

CISO ハンドブック

業務執行のための情報セキュリティ実践ガイド

SUMMARY

今日の企業経営において、ITは効率化の道具から、事業戦略の基盤となり、企業の命運を握る存在になっている。情報セキュリティは、高度化するサイバー攻撃に対峙し、ITをビジネスイネーブラーとして展開する上で欠かせないものとなっている。本書では、情報セキュリティ責任者であるCISO（Chief Information Security Officer）の、経営陣の一員としての任務と責務を明らかにし、事業戦略に則った情報セキュリティ業務を執行するための実践フレームワークを提案する。

CONTENTS