

日本のサイバーセキュリティを「連携」「学び」「創造」

業務執行として再考する 情報セキュリティ

～CISOハンドブック Ver2.0のご紹介～

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



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

著作：JNSA CISO支援ワーキンググループ

出版社：技術評論社（2021/1/20）

発売日：2021/1/20

単行本（ソフトカバー）：400ページ

ISBN-10：4297118351

ISBN-13：978-4297118358

どうして、CISOハンドブックを作ったのか？

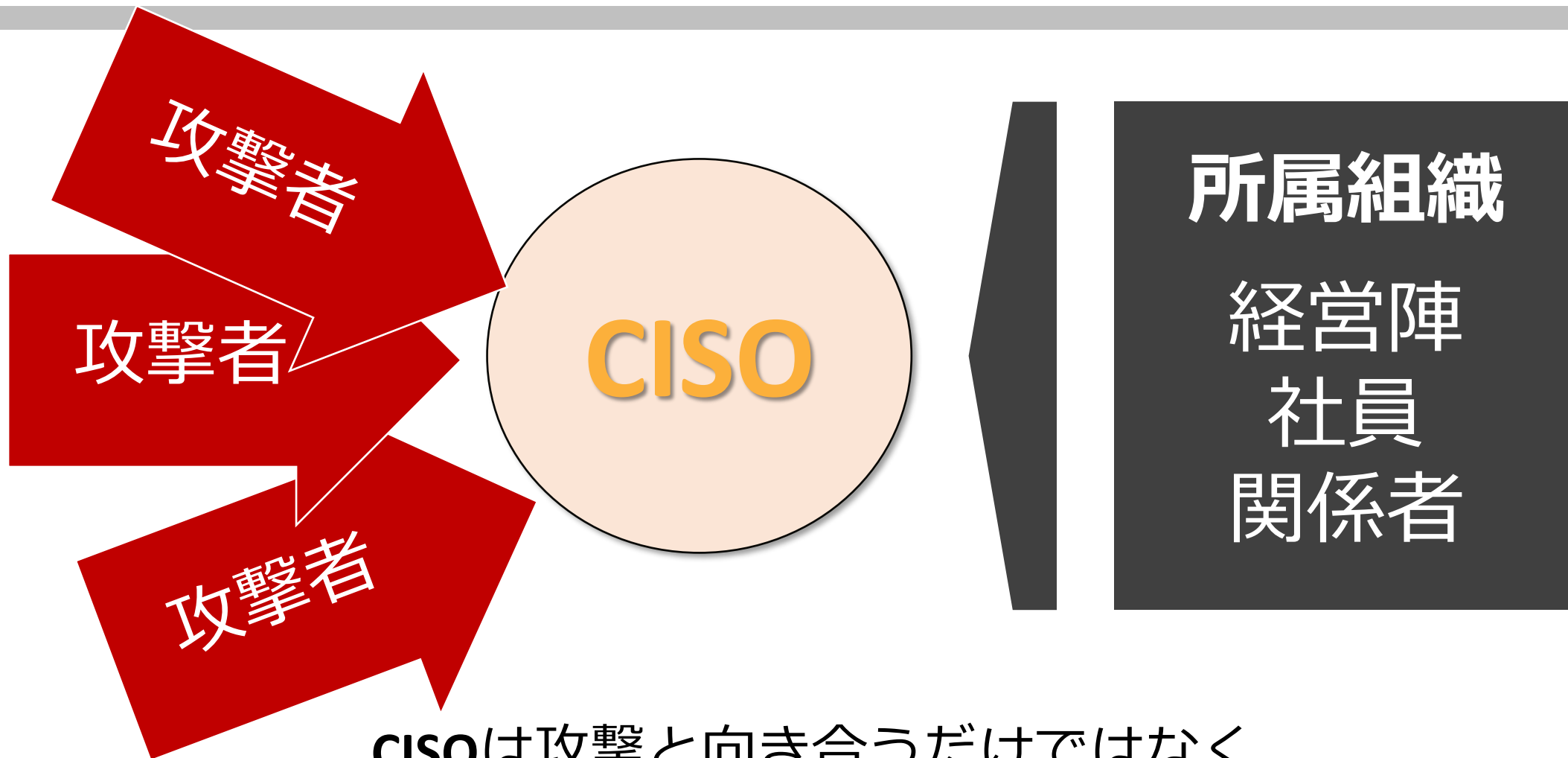
**経営者はセキュリティを
理解しなければならない**

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ハンドブックの中心となる視点

CISOが直面する二つの課題



**CISOは攻撃と向き合うだけでなく、
組織内のステークホルダーとも向き合う必要がある。**

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ハンドブックの概要（目次から）

CISOハンドブック 目次



- 第1章 情報セキュリティの目的
- 第2章 情報セキュリティマネジメントの基礎知識
- 第3章 基本となる経営指標
- 第4章 情報セキュリティの指標化
- 第5章 モニタリングと評価手法
- 第6章 情報セキュリティ監査
- 第7章 情報セキュリティアーキテクチャ
- 第8章 DXと情報セキュリティ
- 第9章 クラウドファーストの情報セキュリティ
- 第10章 情報セキュリティインシデント対応と報告
- 第11章 製品選定とベンダー選定
- 第12章 CISOの責務と仕事
- 第13章 経営陣としてのCISOへの期待

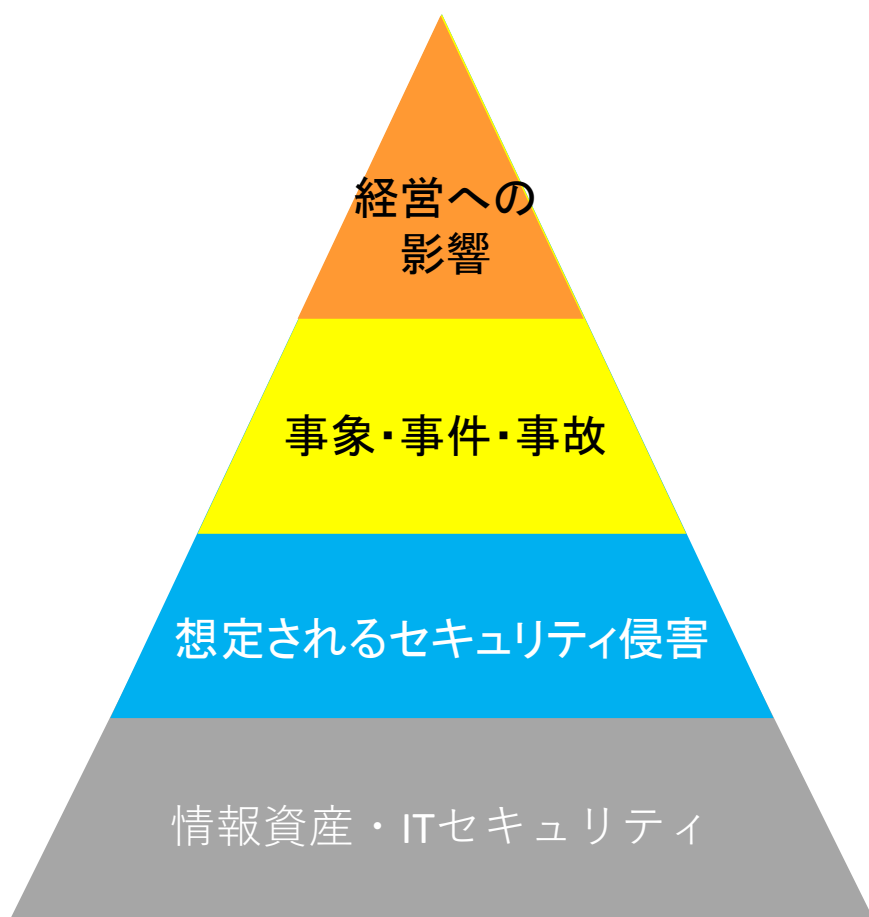
- Annex A 事業計画策定例
- Annex B CISOダッシュボード
- Annex C 情報セキュリティ対策
の標準化と自動化の流れ
- Annex D EDC 手法を使った
セキュリティ対策効果の試算
- Annex E Need to Know 再考
- Annex F 新型コロナウイルス後の
セキュリティ
- Annex G セキュリティインシデントの推移
- Annex H 情報格付け

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		
ストッキング 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

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	
		金融	
		経済	
		社会及び文化	
		技術	
		法律/規制	
		自然	
	組織の目的に影響を与える主要な原動力及び傾向	競争の環境	
		株主	
	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	顧客	
		取引先他	

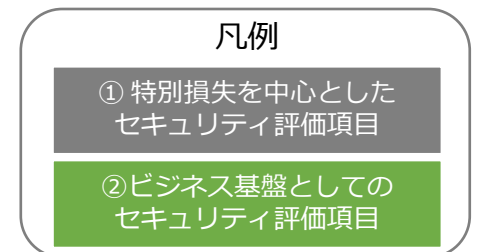
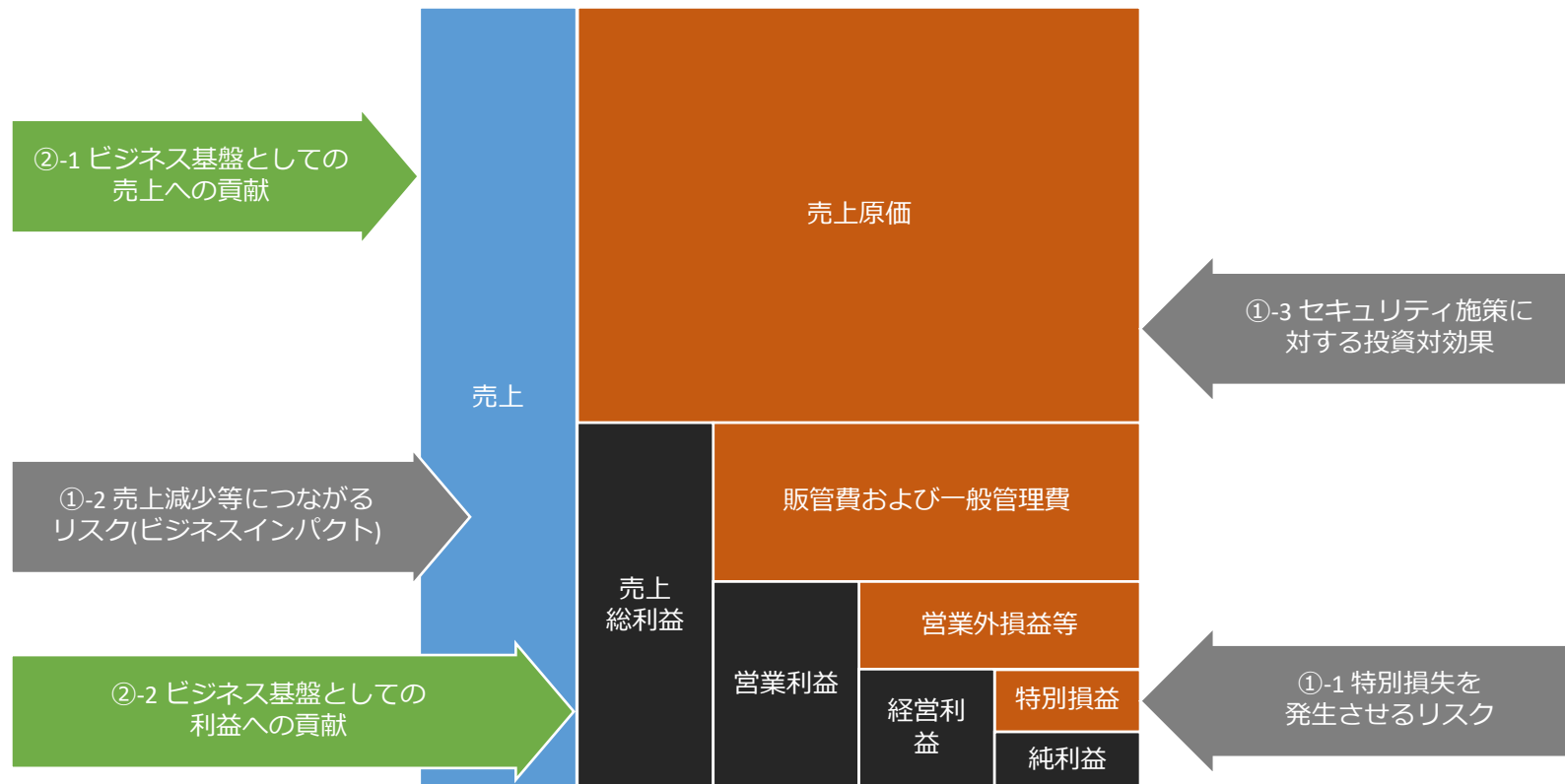
ERM:エンタープライズリスク

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 事業計画	N/A
	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	コンダクトリスク カルテル談合等の組織不正
		技術	
	組織の文化	組織の行動原理	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
		組織の思考様式	
		情報資産	
		情報処理	
	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)	物理的範囲*	*情報資産を取り扱う物理的範囲
		リスク評価・分析	
		規格/指針	
	組織が選択した規格、指針及びモデル	モデル	N/A
		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
	契約関係の形態及び範囲	取引先との契約	顧客対応の不備

セキュリティの二つの視点



要求事項と規範の視点

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)

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)

III 体制・マネジメントの検証

- ・ サイバーセキュリティ演習

II 対策の実装

- ・ CISコントロール
- ・ PCI DSS

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)
- ・ 侵入検査
- ・ 脆弱性検査

リスク・脅威の視点

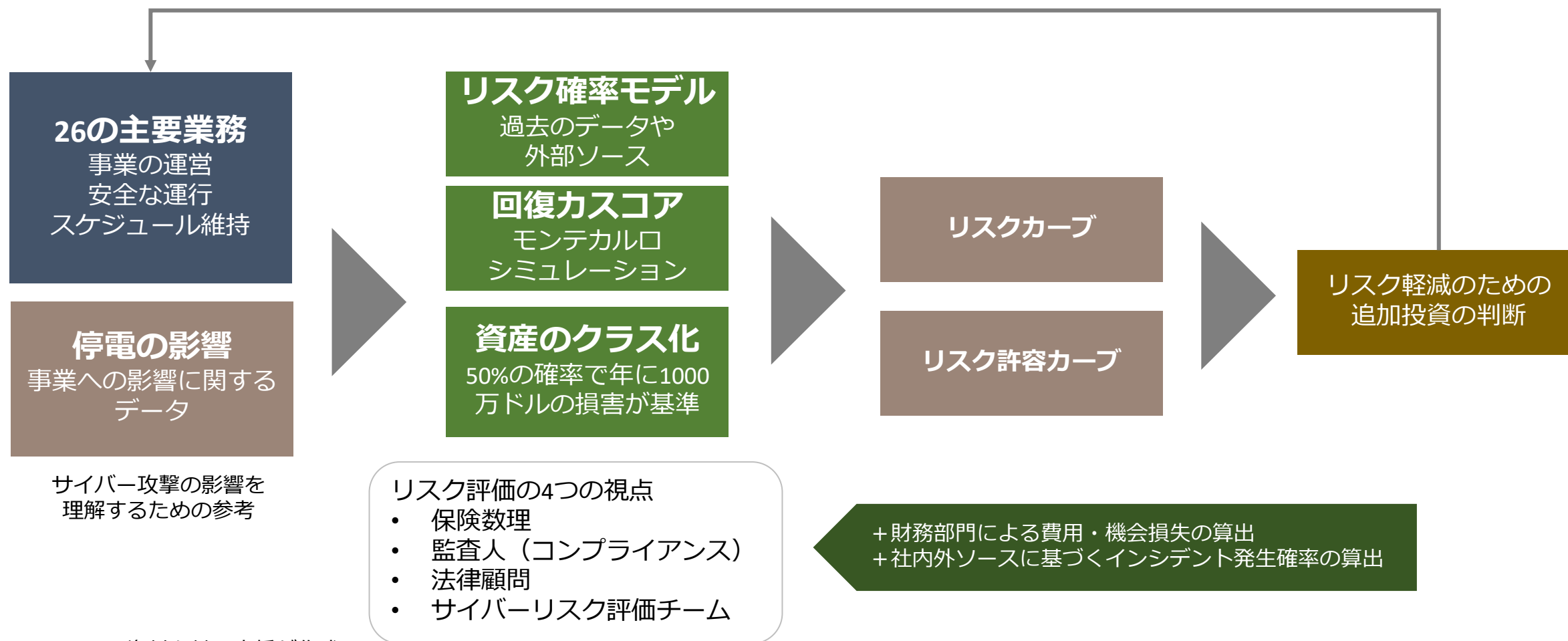
規範に対する実装状況の評価
(規程・記録)

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

- 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

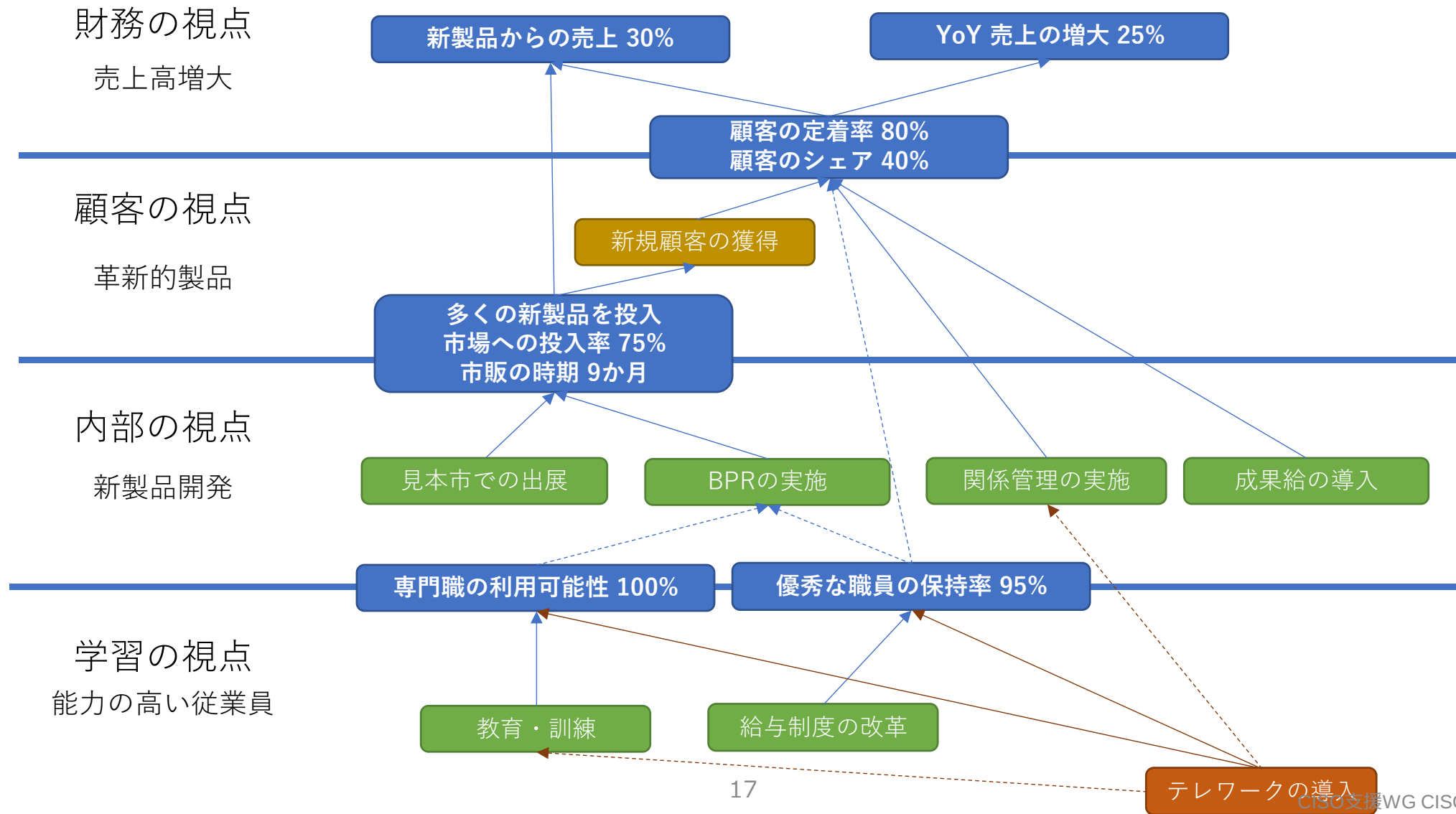


下記資料を基に高橋が作成

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



- 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

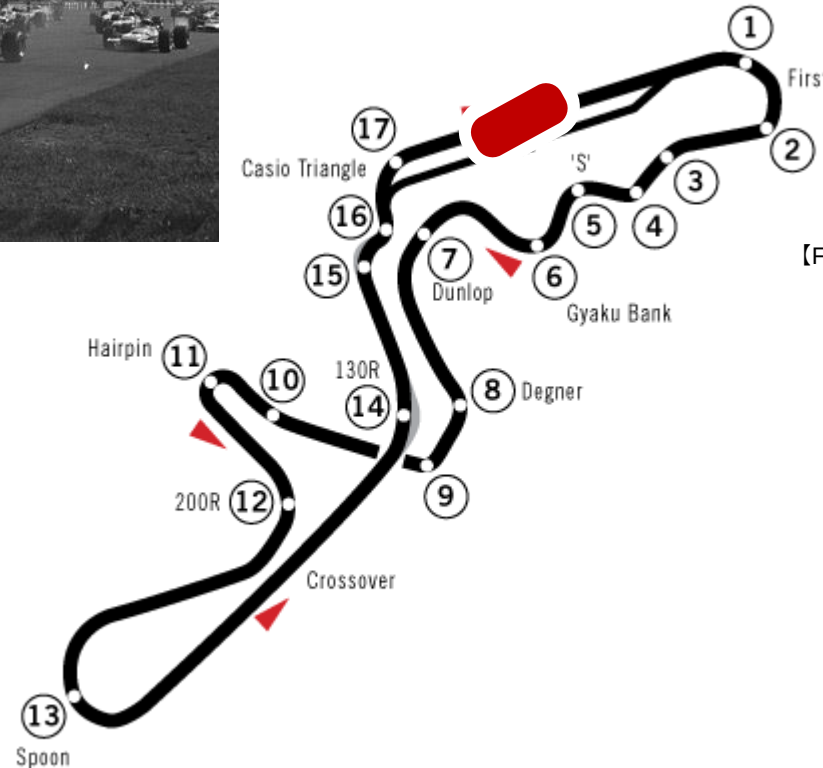


ジョン・サーティース
RA301 (1968年)

PDCA



©www.ClipartsFree.de



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



テレメトリーシステム

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>

- 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
 - クラウド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の評価する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の評価する仕組み。特定の時点における内部統制の整備状況の評価する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について、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
4	Integrity (3 High)	1	0		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。
5	Availability (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
6	File Share (1:no, 2: internal, 3:external)	3	0		(2018/06/14)
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
10	S03: MFA	3	2.0		Link機能を使った共有方法が問題と考えられている。
11	S04: SSO	3	2.0		取り扱う情報に顧客のConfidential情報が含まれる可能性は低い
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/

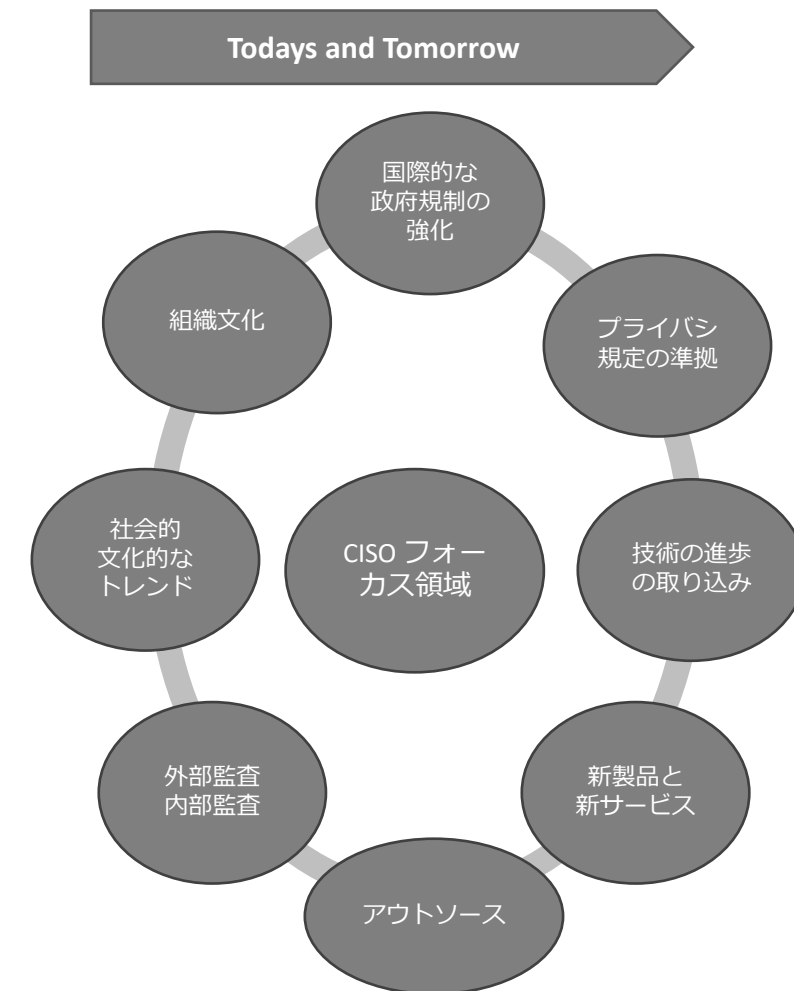
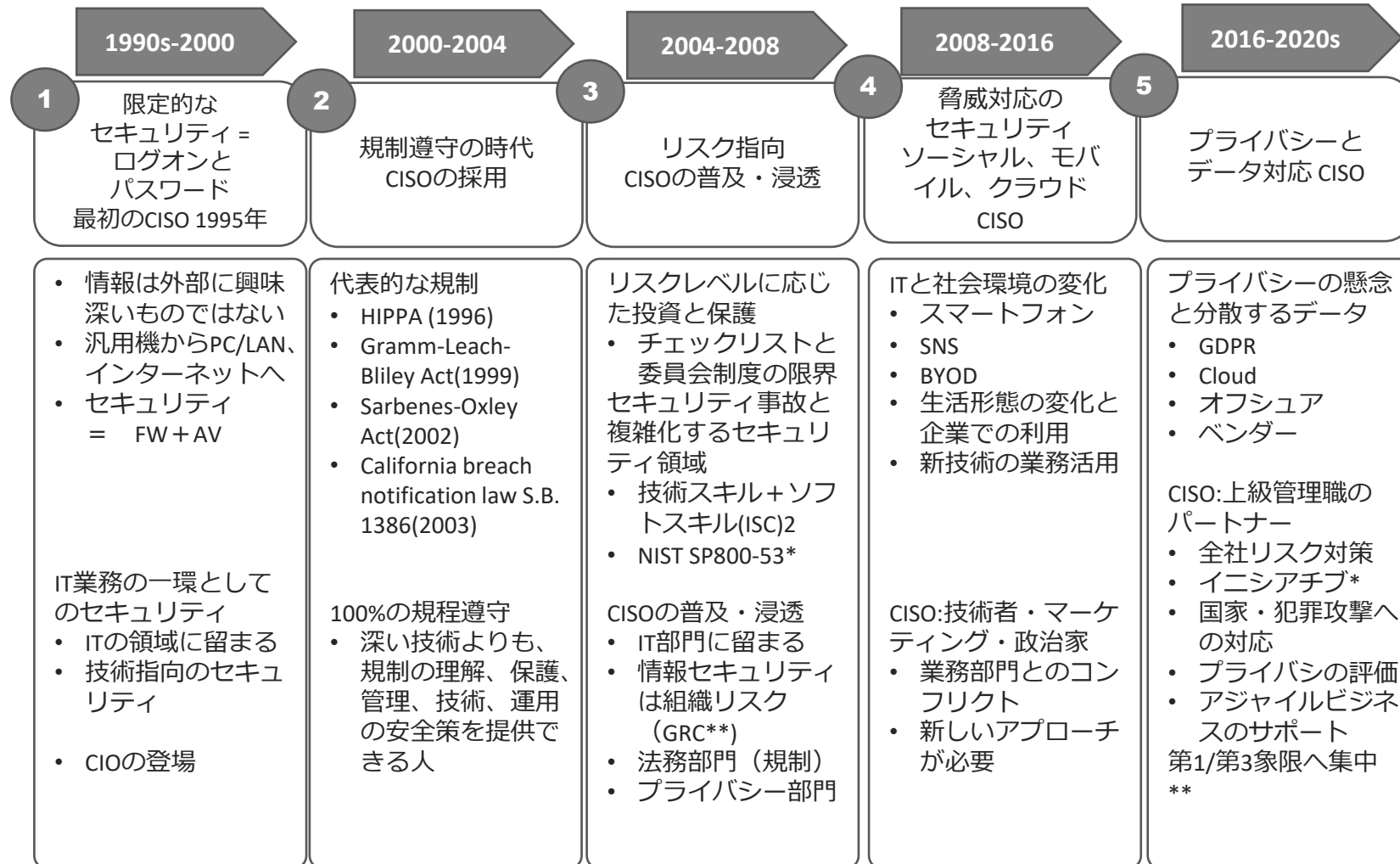
CISO支援WG CISOハンドブックV2.0

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



*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

*イニシアチブ: 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

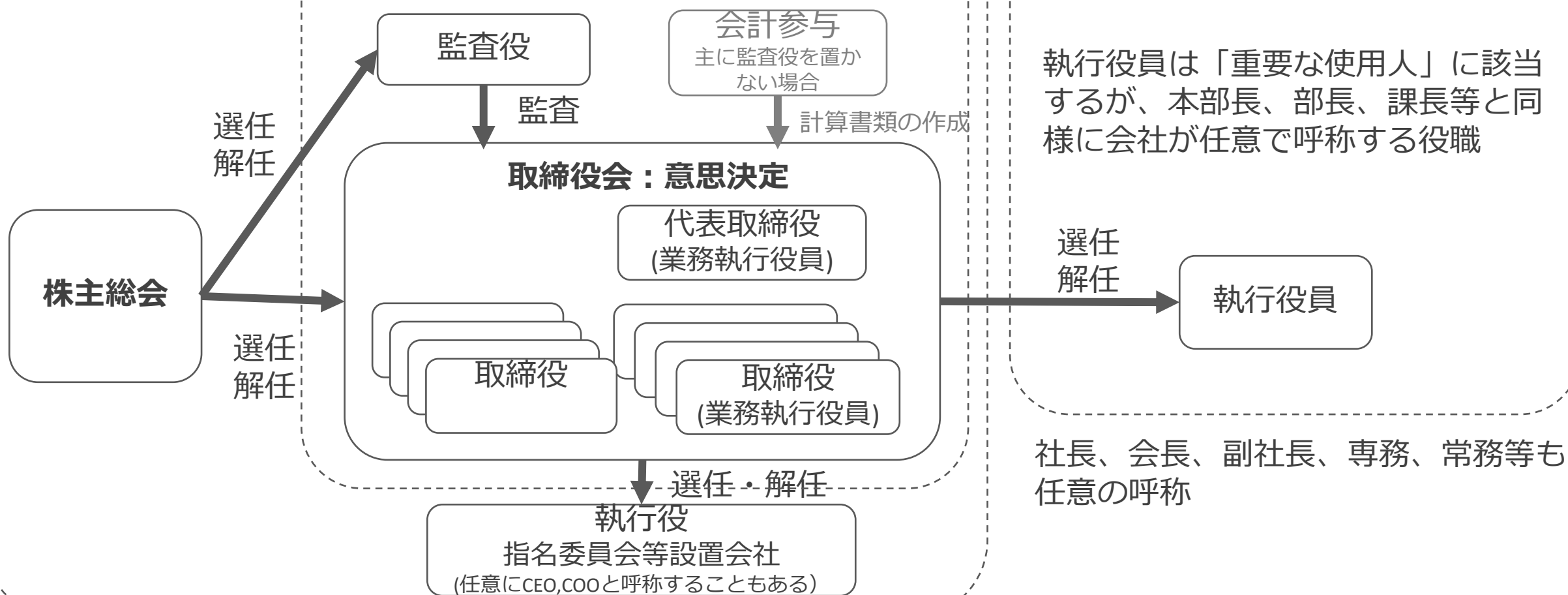
会社法と役職



会社法の機関等

会社法の役員

従業員：決定事項の実行



株主の権利



経営権：議決権のある株式1/2超

- 取締役・監査役の選任
- 役員の報酬などの決定
- 剰余金の配当
- 準備金の減少
- 剰余金についてのその他の処分
(利益準備金、繰越利益剰余金、別途積立金など)

支配権：議決権のある株式の2/3以上

- 定款の変更
- 合併・会社分割・株式交換・株式移転の承認
- 合意による特定の株主からの自己株式取得
- 相続人など（特定株主）に対する売渡請求
- 株式の合併
- 資本金の減少
- 全部取得条項付種類株式の取得

拒否権

- 議決権のある株式の1/3超

単独株主権

- 違法行為差止請求権など

少数株主権

- 会計帳簿閲覧請求権は3%以上

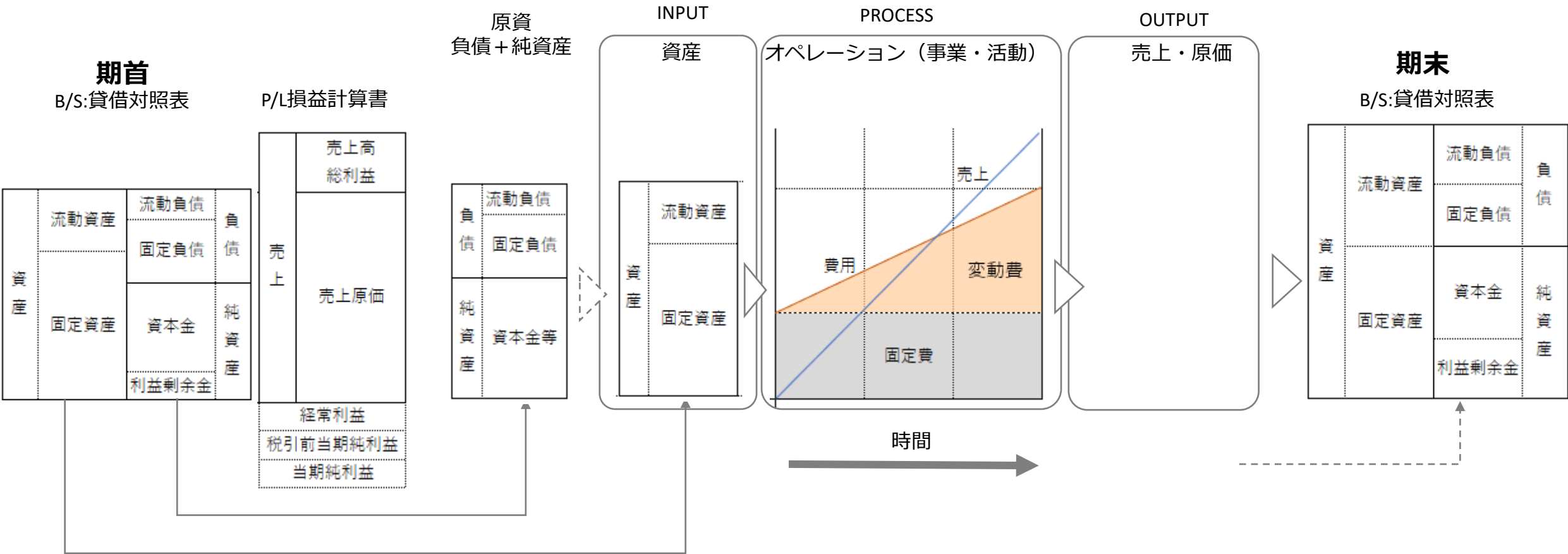
完全経営支配権

- 100%の株式を所有。

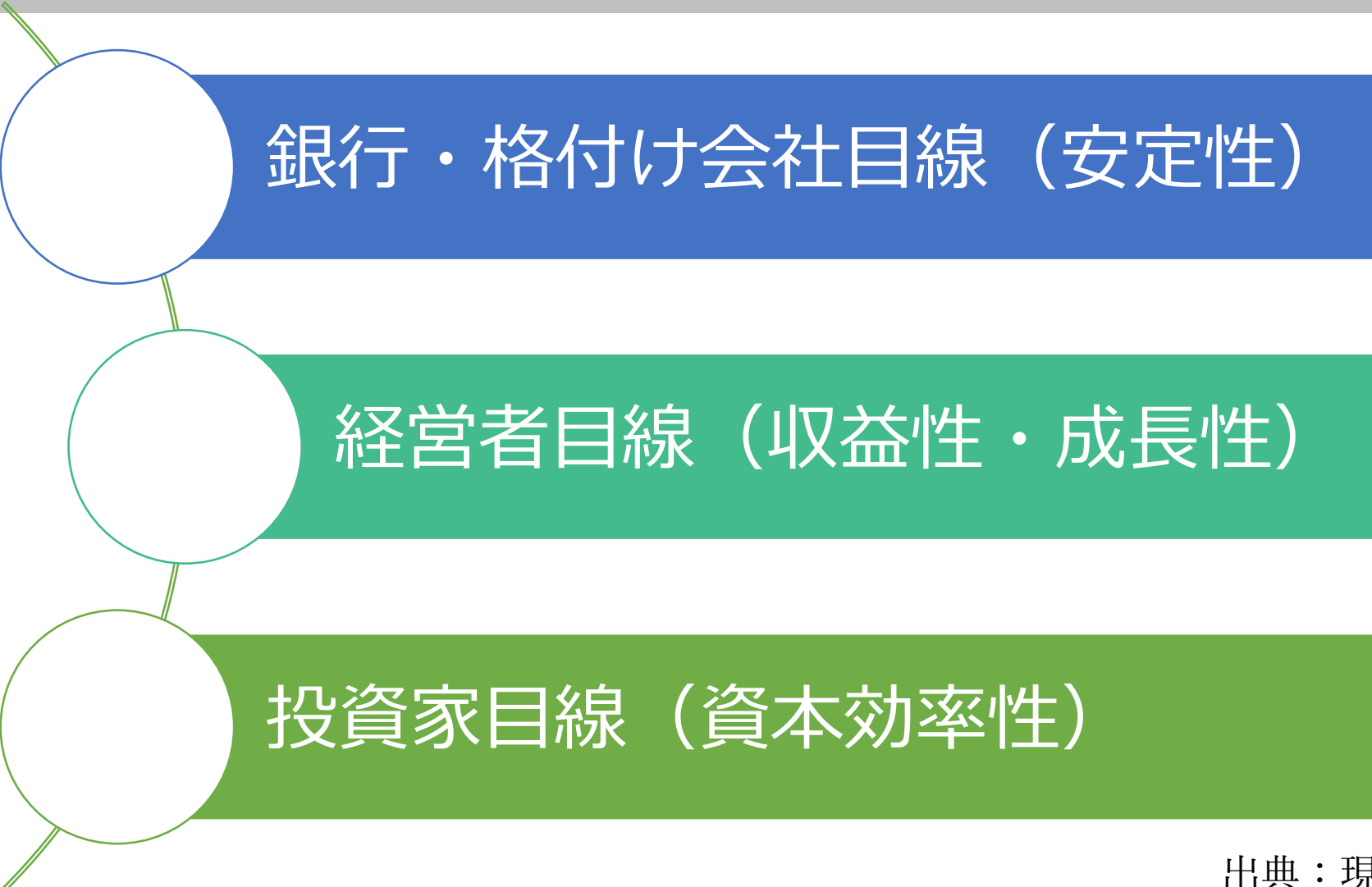
第3章 基本となる経営指標

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



銀行・格付け会社目線（安定性）

経営者目線（収益性・成長性）

投資家目線（資本効率性）

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

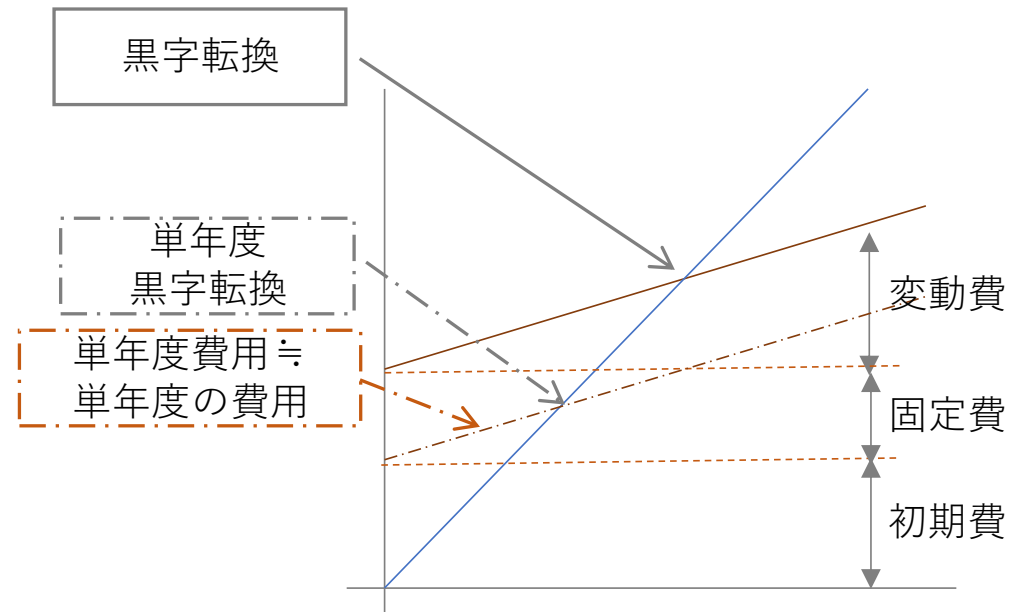
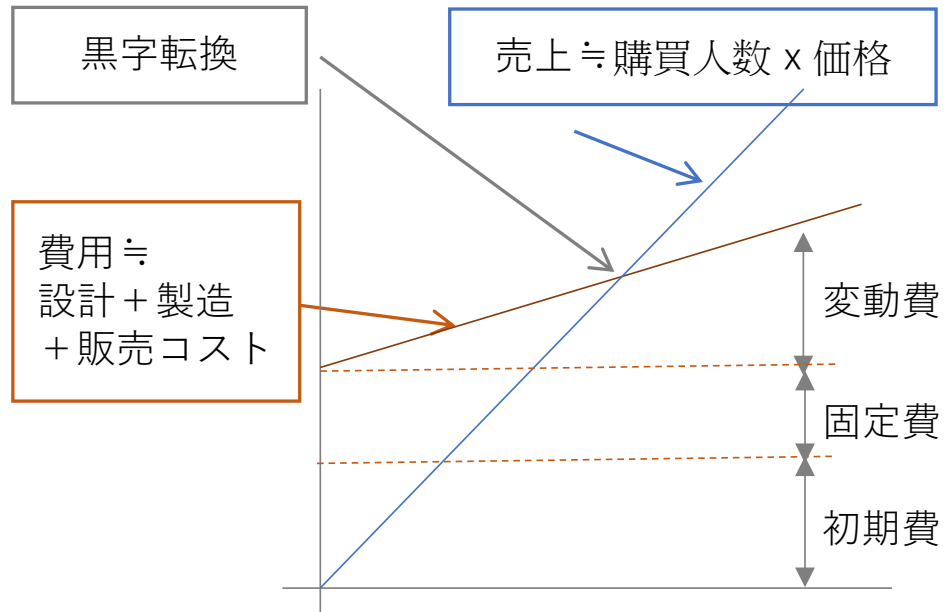
		基準	当座+100 商品-100	当座+100 固定資産-100	流動負債+100 自己資本-100	売上-100 売上原価-100	売上原価-100 販管費+100	純資産+600 負債-600	負債100 現金を未活用	純資産100 現金を未活用
資 産	流動資産	500	500	600	500	500	500	500	600	600
	当座資産	300	100 400	100 400	300	300	300	300	100 400	100 400
	商品	200	-100 100	200	200	200	200	200	200	200
	固定資産	500	500	-100 400	500	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
	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
健 全 性 指 標	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. 誰が売するのか
4. どれだけの人を買うのか
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？



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
	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

		事業計画(1)	事業計画(2)	事業計画(3)	事業計画(4)
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？

- JNSA CISO支援WGは参加者を募集しています
 - ぜひご参加ください！
- ISACAをはじめとした皆様ともディスカッションを進めていきたいと考えています。
 - まだ、具体的なアイディアはありませんが…

Chief Information Security Officer

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

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、荒木絃子、池上美千代、岡田良太郎、
唐沢勇輔、北澤麻理子、武田一成、橋本風、
田中皓、西尾秀一、森谷真直、
JNSA CISO 支援ワーキンググループ ※

技術評論社



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對峙し、ITをビジネスインフラ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、事業戦略に即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

- 第1章 情報セキュリティの目的
- 第2章 情報セキュリティマネジメントの基礎知識
- 第3章 基本となる経営指針
- 第4章 情報セキュリティの指標化
- 第5章 モニタリングと評価手法
- 第6章 情報セキュリティ監査
- 第7章 情報セキュリティアーキテクチャ
- 第8章 DXと情報セキュリティ
- 第9章 クラウドファーストの情報セキュリティ
- 第10章 情報セキュリティインシデント対応と報告
- 第11章 製品選定とベンダー選定
- 第12章 CISOの責務と仕事
- 第13章 経営陣としてのCISOへの期待

Annex

- A 事業計画策定例
- B CISOダッシュボード
- C 情報セキュリティ対策の標準化と自動化の流れ
- D EDC手法を使ったセキュリティ対策効果の試算
- E Need to Know再考
- F 新型コロナウイルス後のセキュリティと業務形態
- G セキュリティインシデントの推移
- H 情報格付け

良い会社？

正しい（会社 | 仕事 | 考え）？