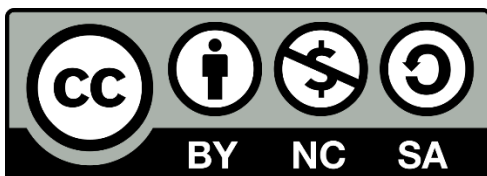


CISOの視点から サイバーセキュリティ経営を俯瞰する

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

Copyright and License



著作権 © 2023-2024 JNSA CISO支援ワーキンググループ. 本著作物は、Creative Commons Attribution Share-Alike 4.0 ライセンスの下で公開されています。再利用や配布を行う場合は、この作品のライセンス条項を明らかにする必要があります。営利目的の利用をご検討される場合は、JNSA(sec@jnsa.org)までご相談ください。

Copyright © 2023-2024 The JNSA CISO support working group. This document is released under the Creative Commons Attribution Share-Alike 4.0 license. For any reuse or distribution, you must make it clear to others the license terms of this work.

Please contact the JNSA(sec@jnsa.org) when considering commercial use.

このドキュメントについて

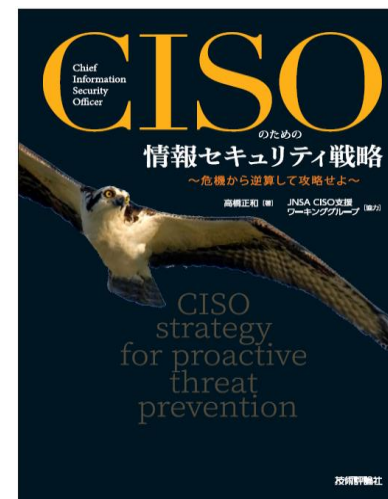
- CISO支援WGでは、CISOの業務に役立つガイダンスやツールを提供するため、「CISOハンドブック」と「CISOのためのセキュリティ戦略」の2冊を出版しました。
- 「CISOハンドブック」は、CISOが経営陣の一員として何をすべきかに焦点を当て、実践的なガイドを提供しています。さらに、経営陣がCISOをどのように活用すべきかを理解し、経営陣がCISOとともに何を達成すべきかを示す試みでもあります。
本ドキュメントは「CISOハンドブック」に記載されている基本的な内容をご紹介します。
- 「CISOのためのセキュリティ戦略」は、セキュリティ対策のデバッグ（システムテスト）を目的とし、イベントをインプット、開示すべき情報をアウトプット、セキュリティ対策をプロセスと位置づけたもので、CISOハンドブックで述べている内容を、具体的なシナリオに落とし込む試みでもあります。
- 「CISOのためのセキュリティ戦略」の内容については、「20 ワークショップ進行用資料」をご参照ください。

CISO支援WG関連書籍



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
発売日：2021/1/20
単行本（ソフトカバー）：400ページ
ISBN-13：978-4297118358



CISOのための情報セキュリティ戦略
～危機から逆算して攻略せよ～
高橋 正和（著）
JNSA CISO支援ワーキンググループ（協力）

出版社：技術評論社
発売日：2023/1/21
単行本（ソフトカバー）：200ページ
ISBN978-4-297-13294-1 C3055

事業責任者の立場になってみると
業務執行に関する資料が見つからない

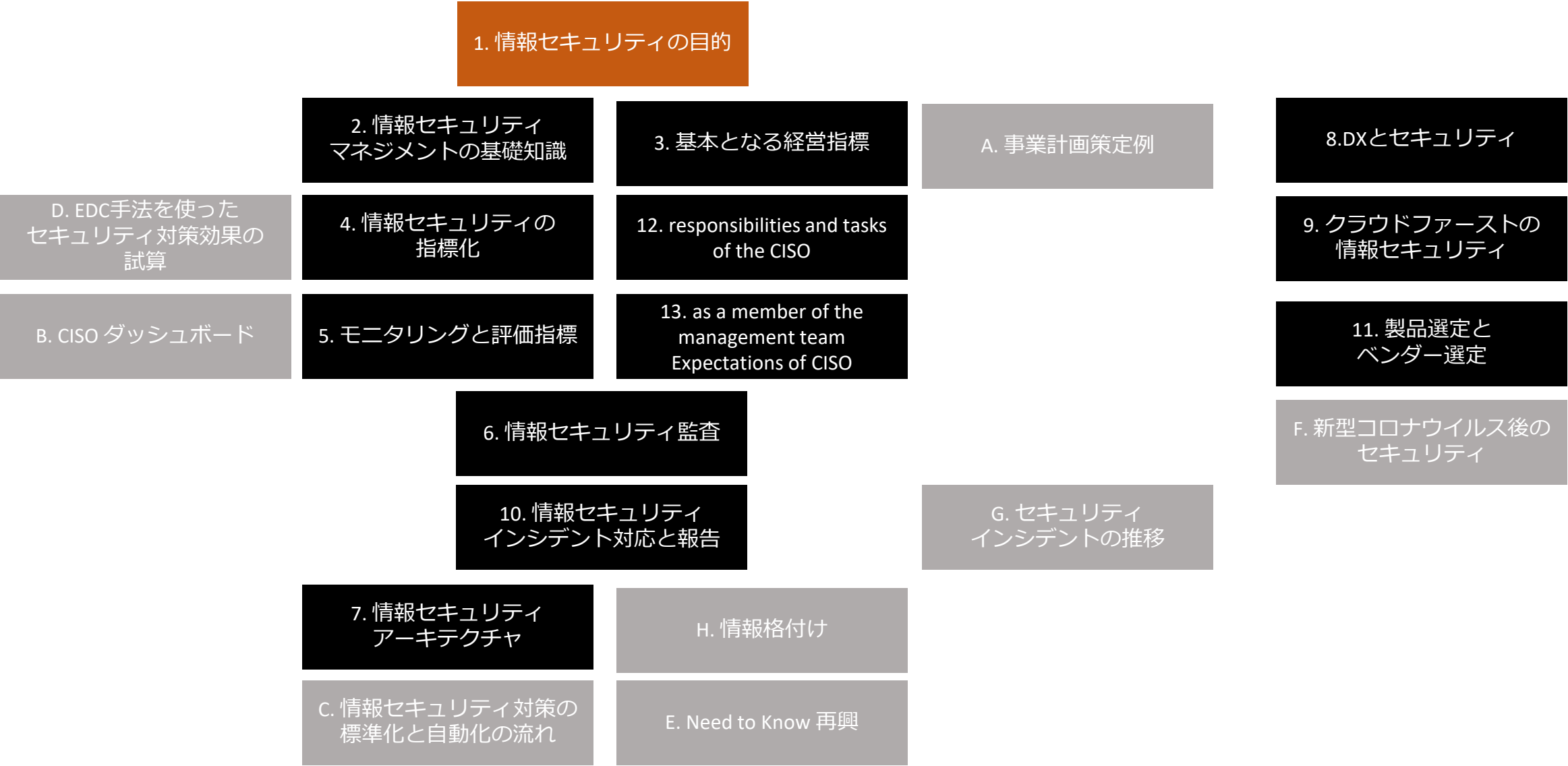
- 経営の書籍≡経営者の成功物語かMethod（手法）
- マネジメントの書籍≡庶務管理
- 業務を執行する当事者目線の資料がない

ハンドブックは悪くないが実務への展開が難しい
by WGメンバー

ハンドブックを補完する内容として目指したこと

- 網羅性から、具体的なシナリオへ
- 計画の策定から、計画の検証とコミュニケーションへ
- わかるから、出来るへ

CISO ハンドブックの構成



業務執行としての 情報セキュリティ

料理で考える本講演の論点

料理人としてのシェフ
担当責任者としてのシェフ
経営者としてのシェフ

ソリューションのスキーム

Research
素材と鮮度の探求



Best of breed (最高の材料)
セキュリティ製品・サービス



ここにフォーカスしすぎてないか？



Research
器具と調理法の探求

Best Practice (最高の方法論)
セキュリティ規範・規準



Skilled Operation

熟練の料理人

良い素材x良いレシピ = 良い料理



素材とレシピがあれば出来る？

専門家のスキーム

最高！



オーダーは、この料理なのか？

Unskilled Operation

非熟練者

良い素材x良いレシピ ≠ 良い料理



こいつをどうにかしないと
ダメなんじゃないか？

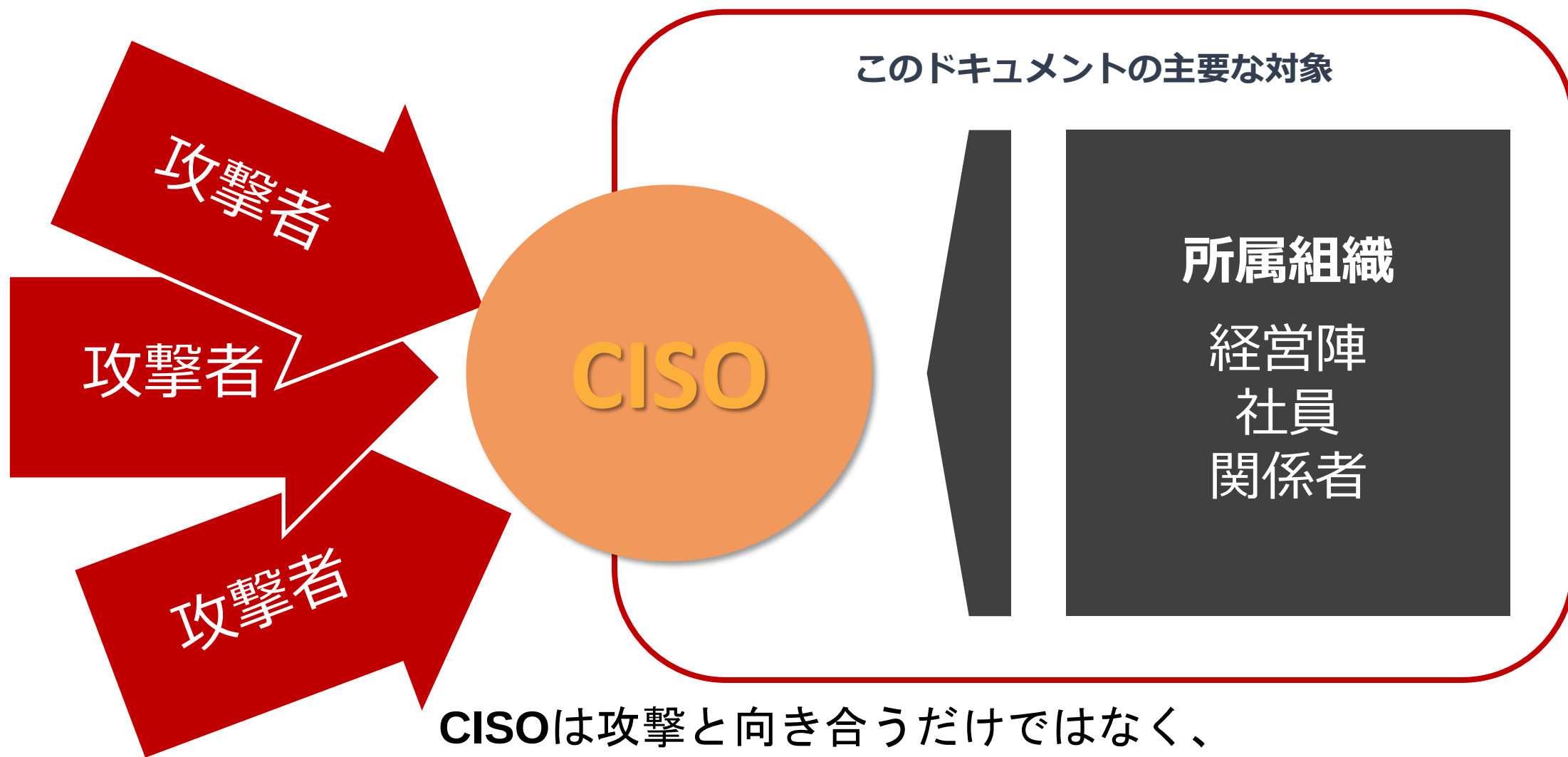
事業（ユーザー企業）のスキーム

ひどい・・・



結果から考えないとダメ？

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。**

典型的な対立関係

事業推進の視点

すぐやりたい・試したい

走りながら考えたい

今期の売上を考えたい

事故が起きたことはない

情報セキュリティの視点

評価と検証が不可欠

実施手順が不可欠

リスク対応が不可欠

世界中で事故が起きている
事故前提の対応が不可欠

でも...
「責任を取る」
ことはない

No Incidentを
担保できない

事業リスクの文脈

「攻め」のセキュリティ
自社ビジネスの基盤としてのIT
(スタビライザーとしてのセキュリティ)

情報セキュリティリスクの文脈

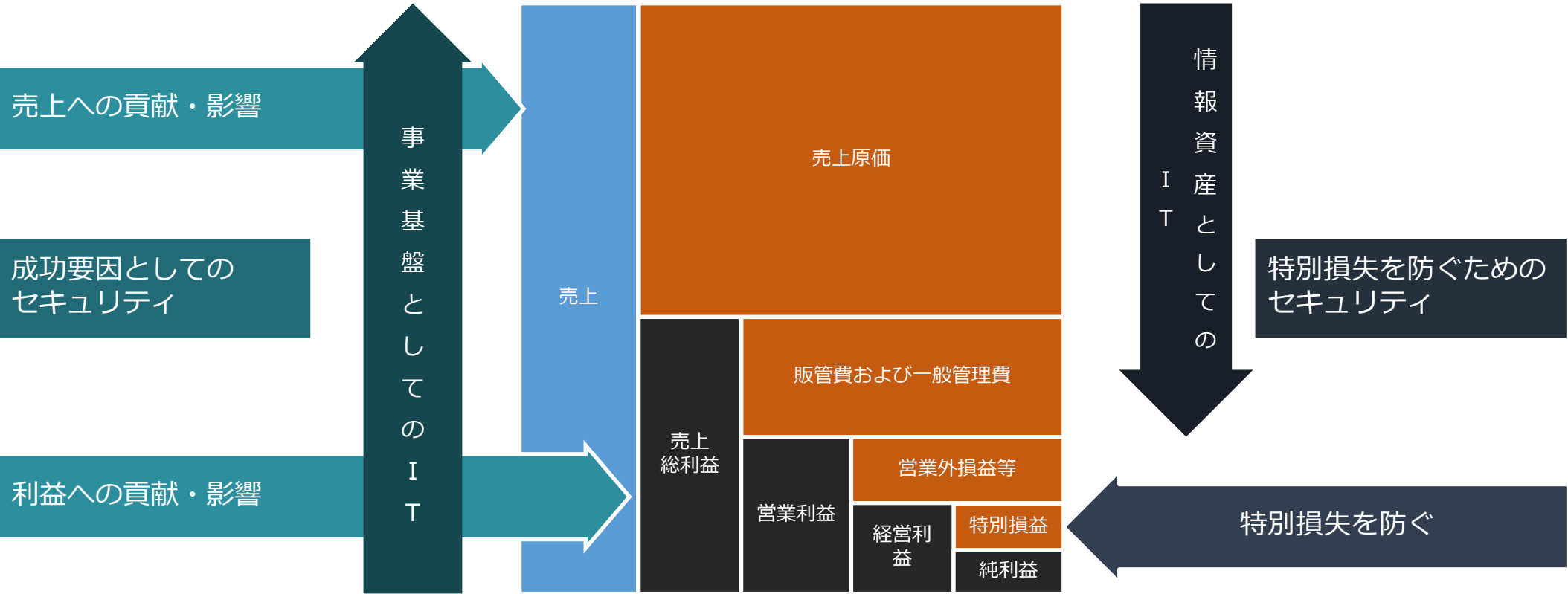
「守り」のセキュリティ
一般化されたセキュリティ対策
(ブレーキとしてのセキュリティ)

CISOハンドブック 中心となる論点

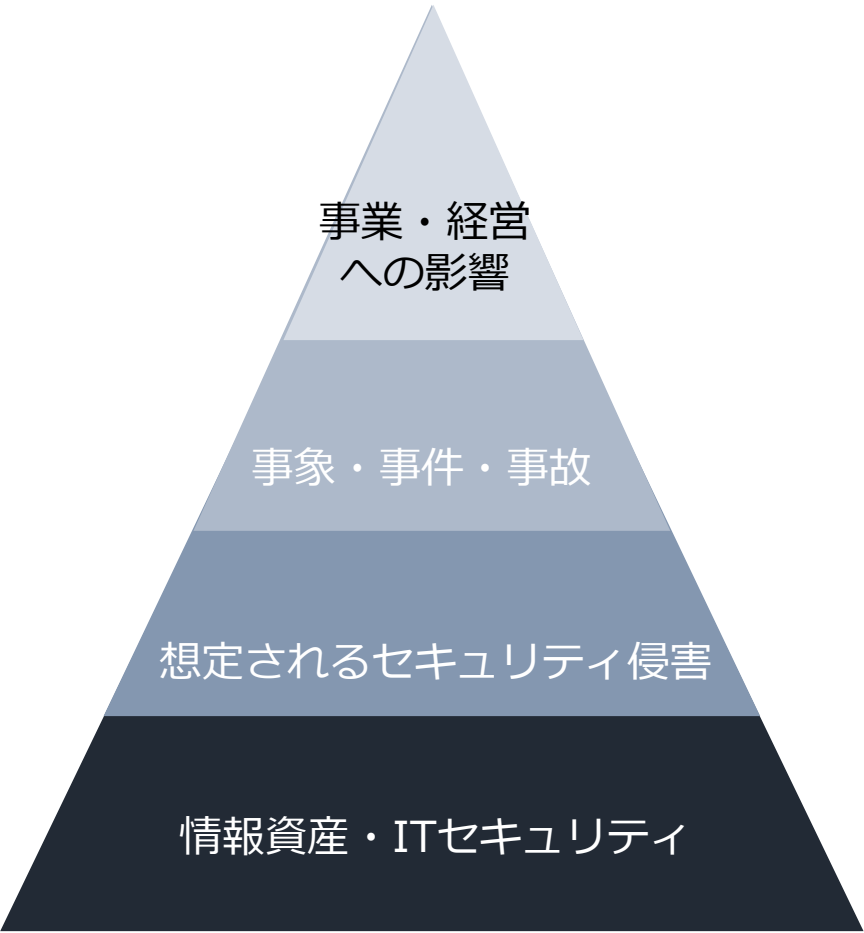
セキュリティリスク・ビジネスリスク

ビジネス/ビジネスリスクの文脈

ITセキュリティリスクの文脈

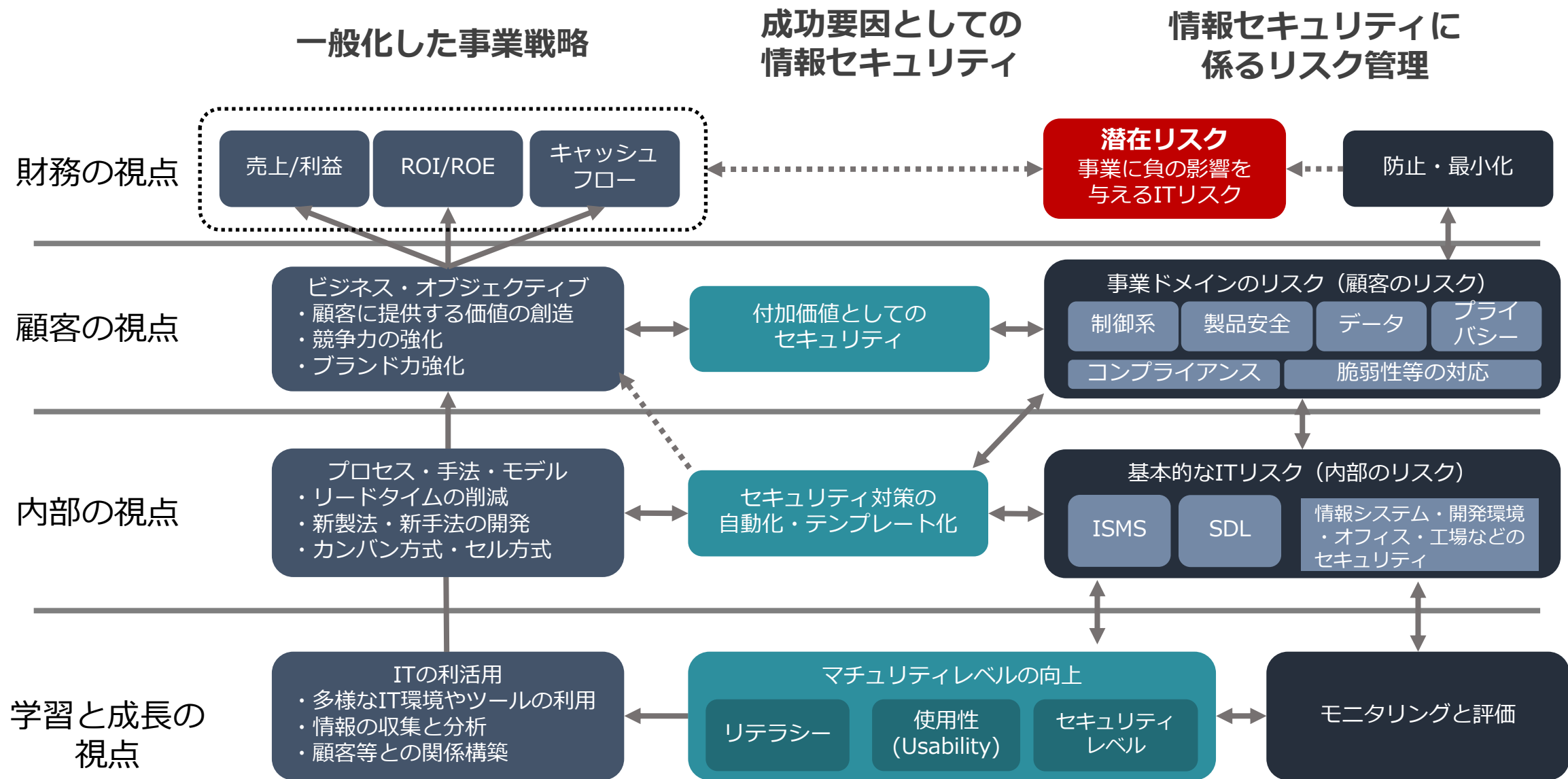


専門用語を共通言語化する

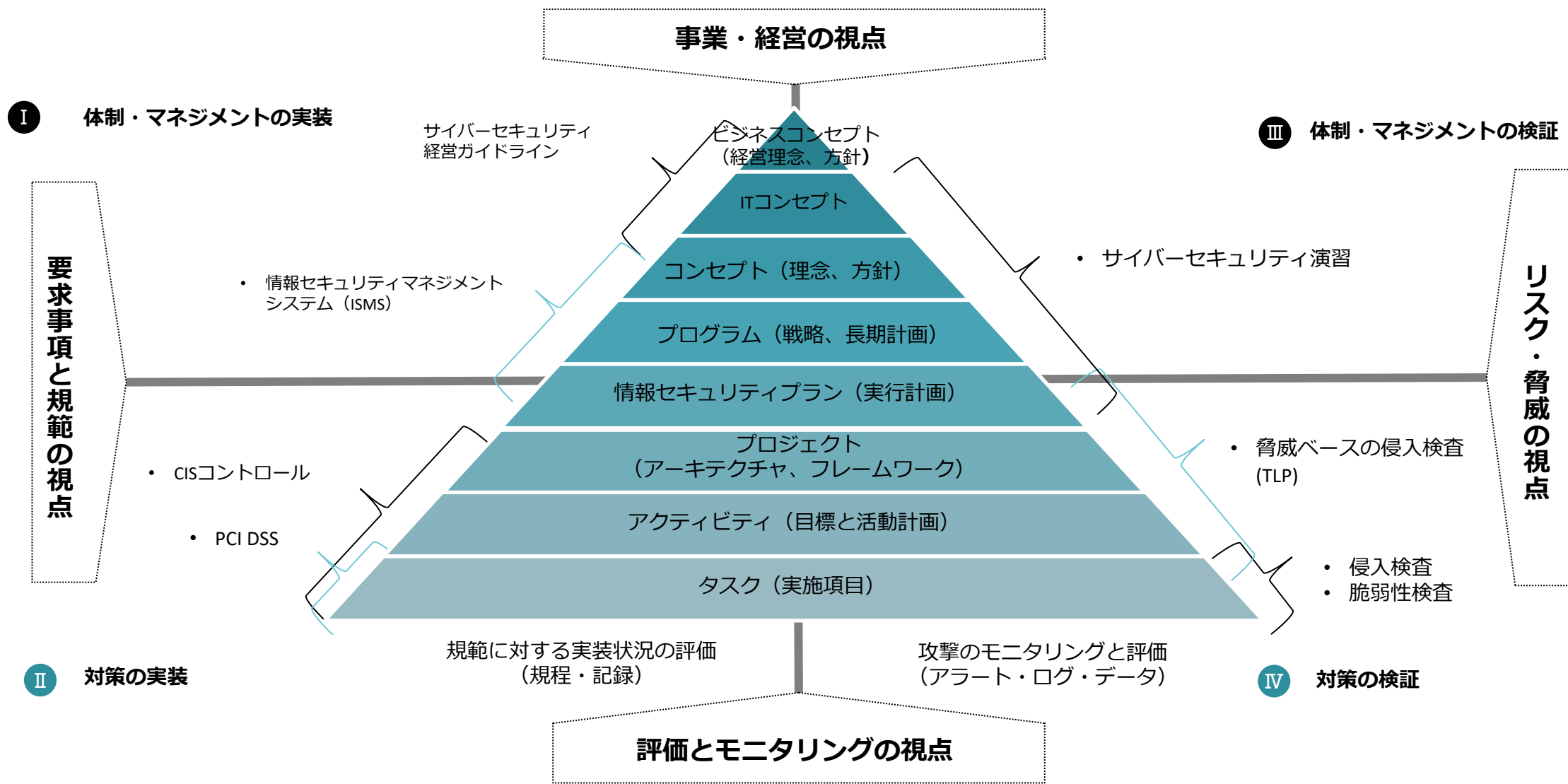


Confidentiality (機密性)	Integrity (完全性)	Availability (可用性)
競合優位性の低下：競合の躍進、評判の低下 費用的な損失：損害賠償、営業機会損失 事業への影響：営業停止		
ストーキング 秘密の暴露 スパイ行為	システム誤作動 偽の発注・契約 紛争の誘発	システムの停止 社員間の連絡できない 社外との連絡できない 売上が立たない
利用状況の漏洩 画像・音声の漏洩 踏み台による漏洩	プログラム等の改ざん データの改ざん	プログラム等の改ざん 制御データの改ざん 通信経路の遮断
ソフトウェアの脆弱性 設定の不備 プロトコルや暗号の不備 ネットワークや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

セキュリティを成功要因として位置づける



チェックリストと構造化アプローチ



プロスポーツで考える構造化

計測する対象は、立ち位置によって違ってくる

選手の視点（試合の視点：OODA的）

- 自身の成績、ゲームに勝つ、年棒を上げる
ポジションや役割によってゴールが違うものになる
- 個人成績（得点・アシスト・打率等）

監督の視点（シーズンの視点：OODA, DevOps的）

- シーズンで成績をあげるためにゲームに取り組む
- 課題は次のゲームまでに改善に努める
- 選手を評価する（個人成績、サイバーメトリックス）
- チームの成績（順位、試合数）

オーナーの視点（中長期的な視点：PDCA的）

- チームが存続する価値と収益があること
- コンセプト・経営計画・投資計画・財務状況（経費と収益）
- チームの成績・選手の評価・スタッフの評価
- チームの価値

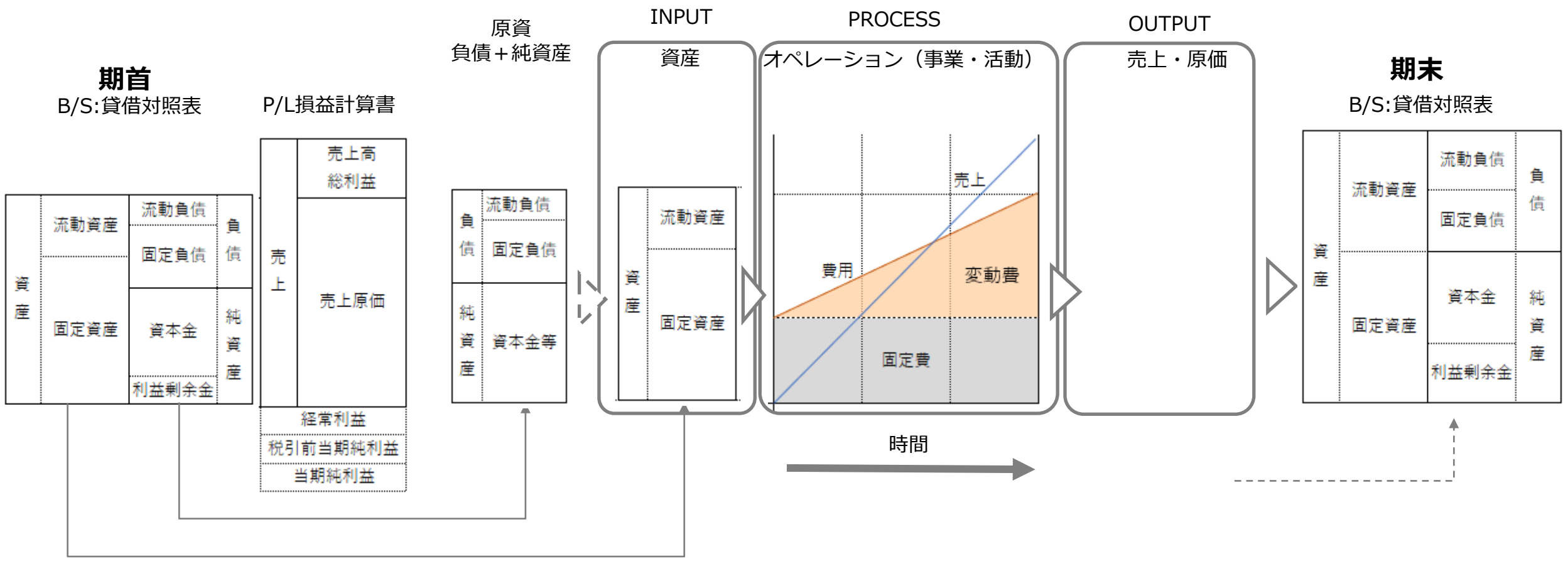
参考：今こそスポーツチーム経営を考えよう | 橋本 貴智 <https://note.com/takatomoh/n/n92441835b7dd>



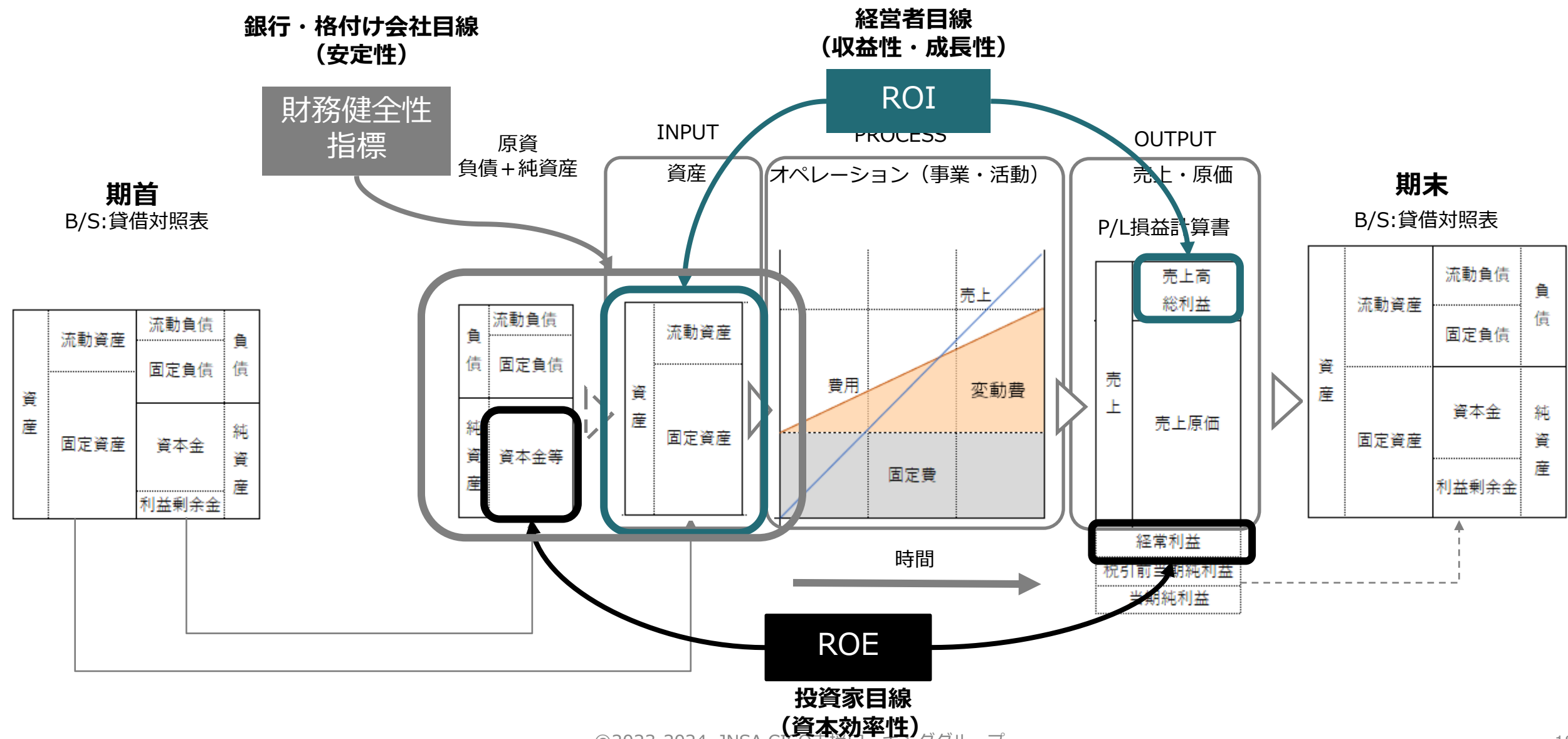
財務諸表を読み取る (理解を試みる)

財務諸表を理解する（ことを試みる）

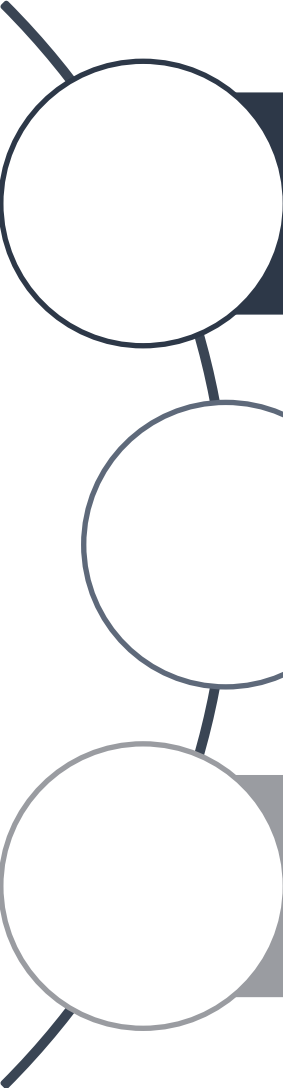
因果関係の方向が、技術系と違う点がわかりにくい
左から右に因果関係を記述して、HIPO的に表記してみる



財務諸表に対する3つの目線



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）

財務健全性指標
流動比率・固定比率など

経営者目線（収益性・成長性）

ROI
Return on Investment

投資家目線（資本効率性）

ROE
Return on Equity

BSとPLの構成による財務指標の変化

仕訳を変えると、財務指標により、影響が違って見える。

		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									
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



むすび

CISOハンドブックが目指すもの

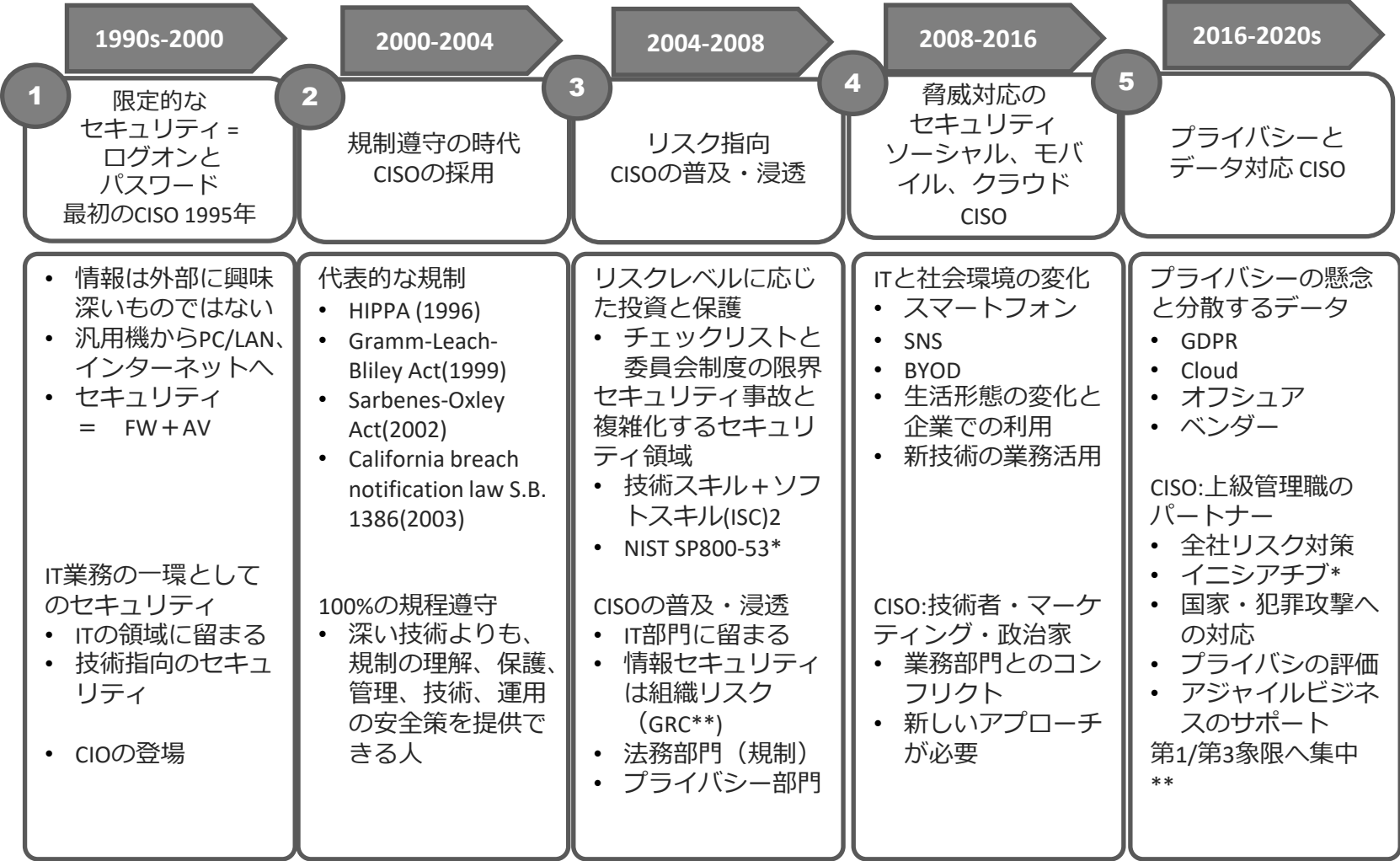
- 「CISOが経営陣の一員として成すべきこと」
 - 実践するためのガイドを提供
- 「経営陣がCISOと共に成すべきこと」
 - 経営陣がCISOを活用するための理解を促す試み
- 知識の集積ではなく「成すべきこと」を俯瞰する視点
 - CISO業務と要素の本質的な理解の足がかり
 - 経営という意味でのマネジメント
 - 経営という視点でのセキュリティ
 - ベストプラクティスとその背景
- 特別損失対策からビジネス志向へ
 - ビジネスイネーブラとしてのセキュリティという視点

本ドキュメントや「CISOハンドブック」が業務執行としての情報セキュリティに取り組むうえで、参考にしていただければ幸いです。

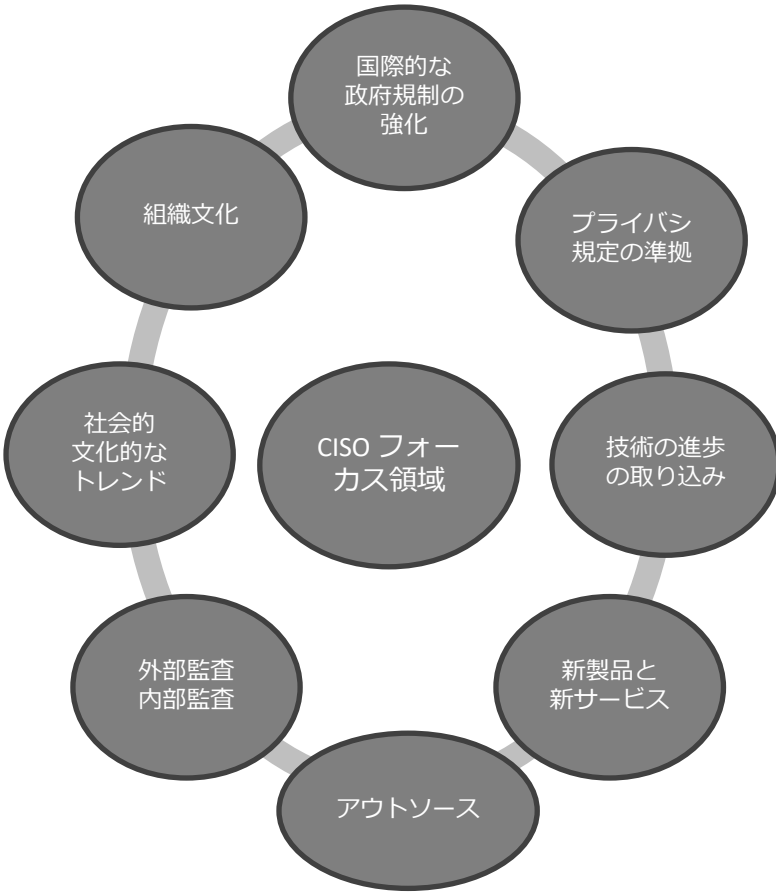
参考

CISOハンドブックで取り上げている内容の一部を、参考として以下に抜粋します。

CISO COPASS: CISOの歴史



Today's and Tomorrow

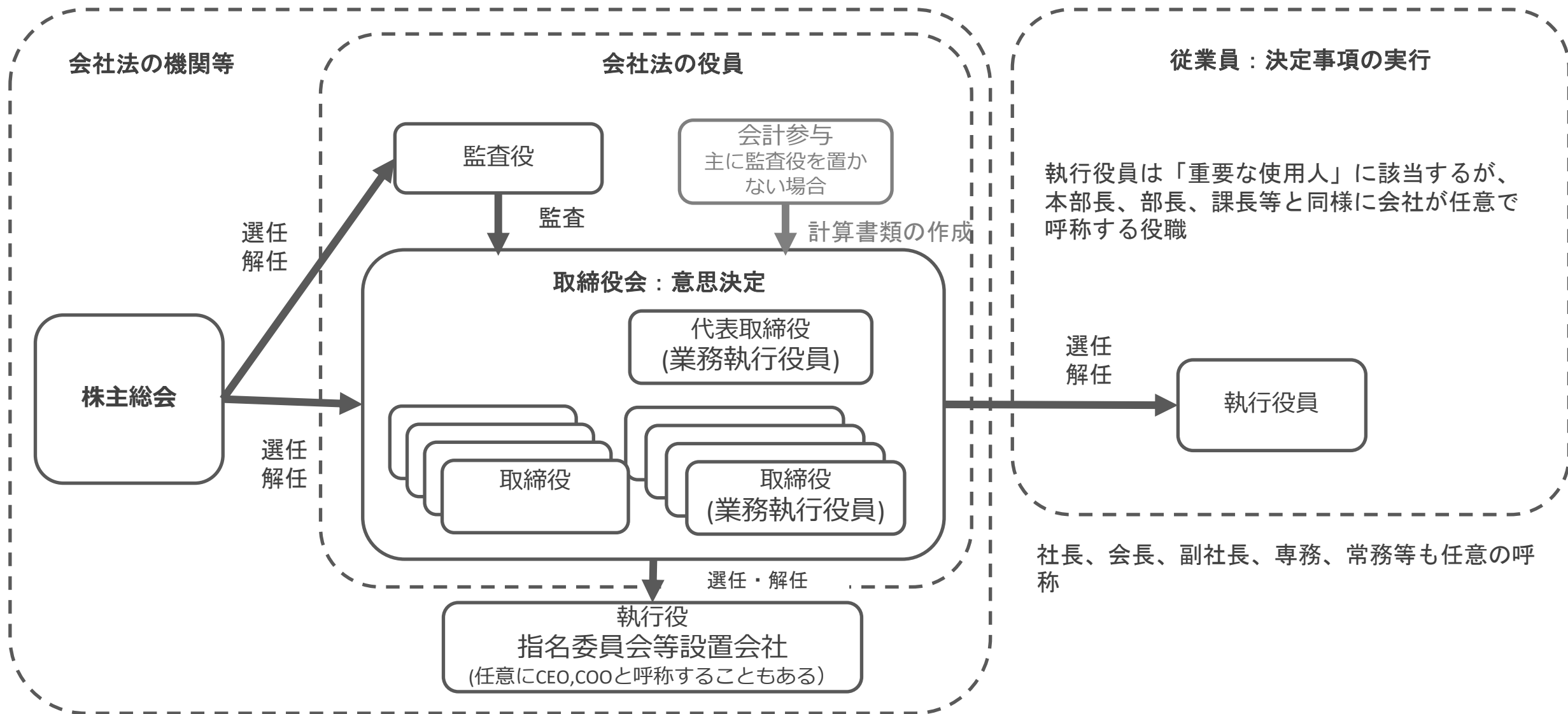


出典 : CISO COMPASS, TODD FITZGERALD
ISBN-10 : 0367486024
CISO WGによる翻訳と構成

*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

会社法と役職



考慮すべき法令・基準（クラウド）

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（クラウド）

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（クラウド）

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 (2018/06/14)
5	Availability (3 High)	1	0		
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Confidential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

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

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、武田一城、橋宮風、
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

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、武田一城、橋宮風、
田中皓、西尾秀一、森谷真直、
JNSA CISO 支援ワーキンググループ ※



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

An aerial photograph of a dense city skyline, likely New York City, with the Empire State Building prominently visible in the center. The image is overlaid with a semi-transparent blue filter. The text "Thank you" is centered in a large, white, sans-serif font.

Thank you