NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

CISOハンドブック

業務執行として考える情報セキュリティ

JNSA 社会活動部会 CISO支援ワーキンググループ
リーダー / JNSA 副会長　高橋 正和

CISOハンドブックの構成

- CISOハンドブック v1.0β [4.70MB]

- CISOダッシュボードv09 [1.94MB]

  ※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」と呼称し考察しました。

- インシデント対応ワークショップVer01 [1.58MB]

  ※「インシデント対応手順」の策定を通じて、組織のセキュリティ在り方やステークホルダーを明らかにし、事故が発生した際には、手順に従ったインシデント対応を適切かつ遅滞なく実施できることを目指すものです。

- インシデント対応ワークショップ-表v02 [47KB]

※上記ワークショップを行う場合に使う表です。

CISOハンドブック作成の背景

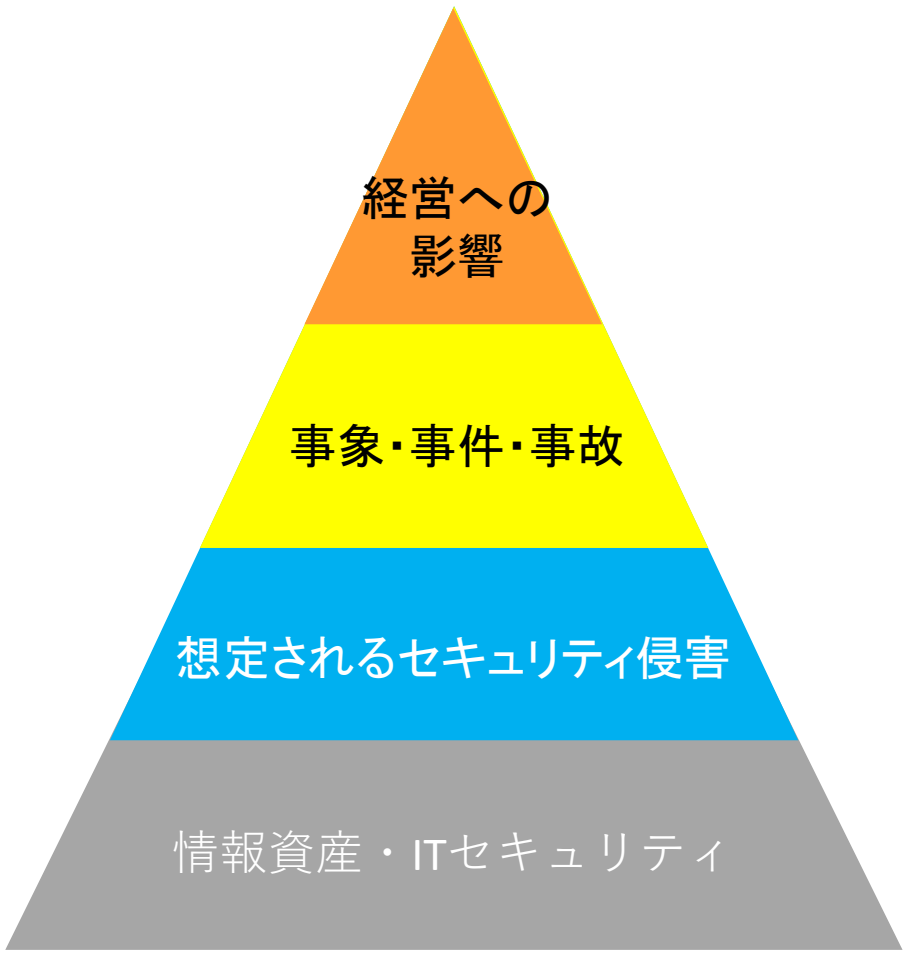
業務執行にフォーカスした CISOハンドブックの使い方

CISOハンドブックの使い方

- 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

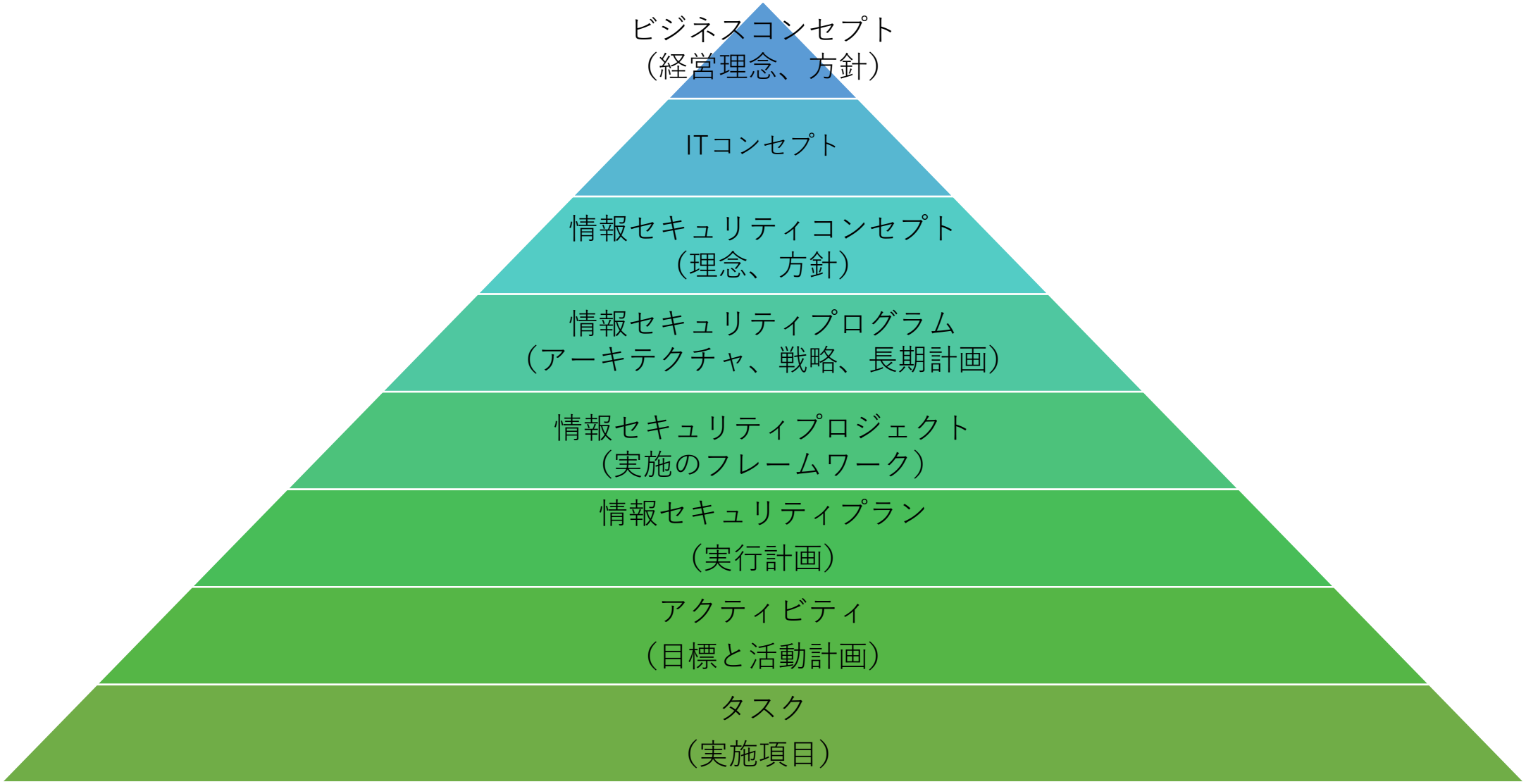
情報セキュリティ
マネジメントの基礎知識

ビジネスリスクとセキュリティリスクの関係

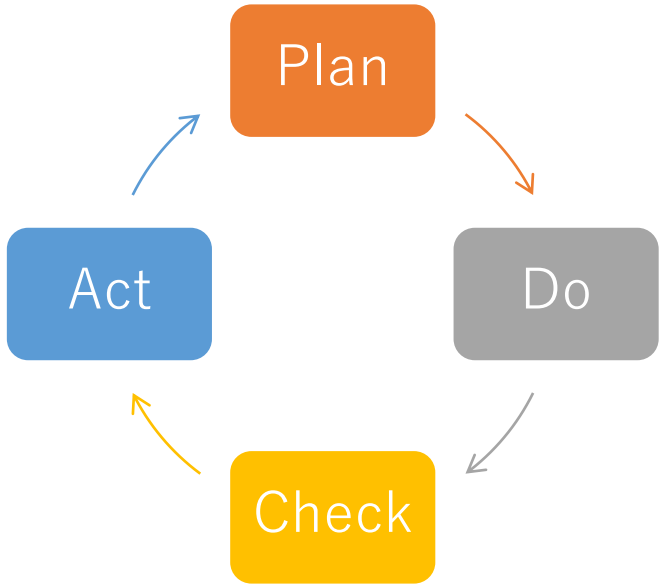


Confidentiality（機密性）	Integrity（完全性）	Availability（可用性）
競合優位性の低下：競合の躍進、評判の低下 費用的な損失：損害賠償、営業機会損失 事業への影響：営業停止		
ストーキング 秘密の暴露 スパイ行為	システム誤作動 偽の発注・契約 紛争の誘発	システムの停止 社員間の連絡できない 社外との連絡できない 売上が立たない
利用状況の漏洩 画像・音声の漏洩 踏み台による漏洩	プログラム等の改ざん データの改ざん	プログラム等の改ざん 制御データの改ざん 通信経路の遮断
ソフトウェアの脆弱性 設定の不備 プロトコルや暗号の不備 ネットワークや通信の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

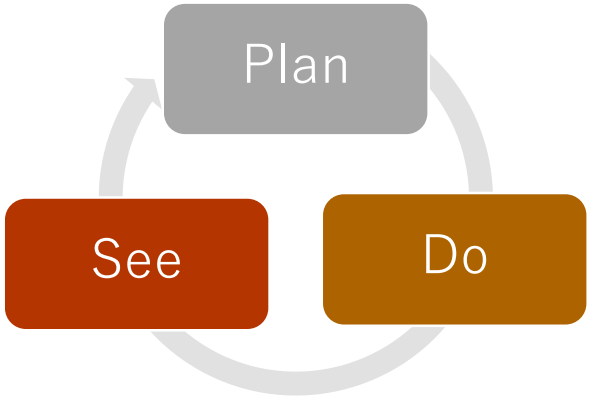
情報セキュリティ計画フェーズの実施モデル



情報セキュリティ・マネジメントサイクル

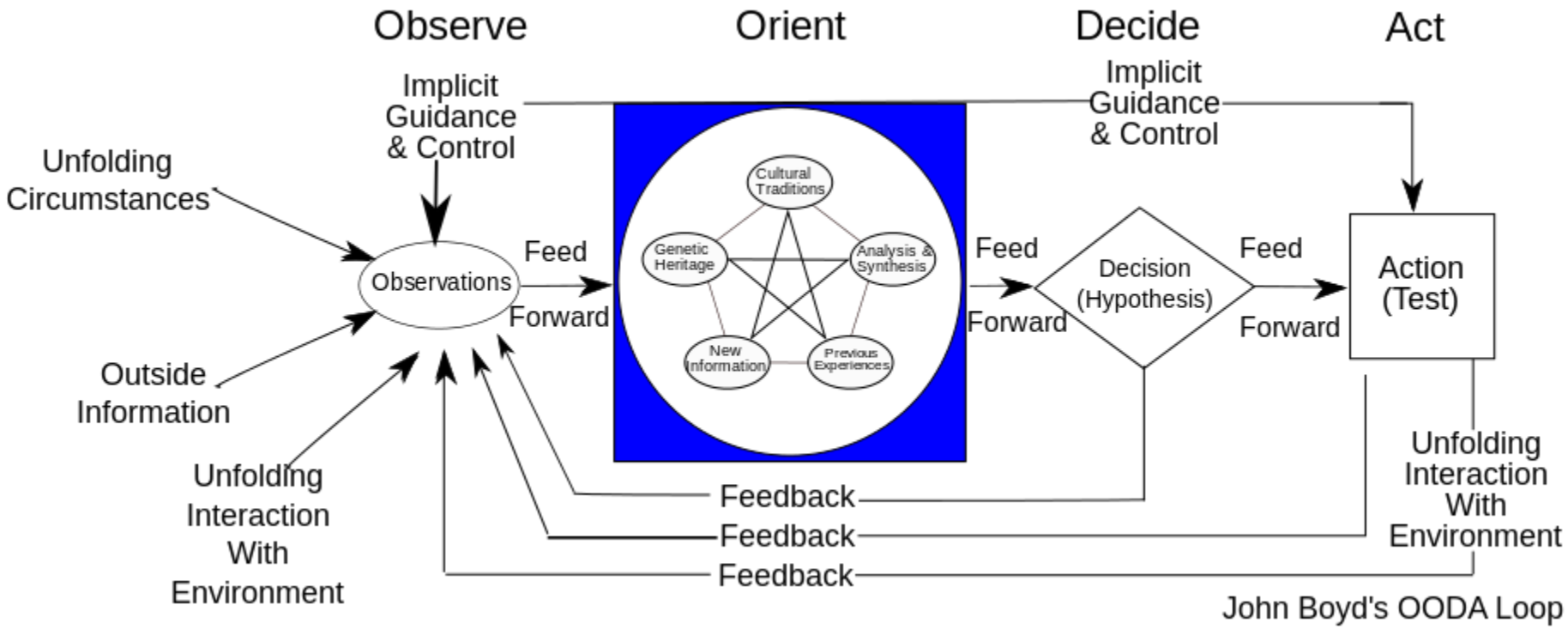


プログラム・プロジェクト指向
定期的：決算発表などに近い



タスク・アクティビティ指向
逐次的：仮説・実験・検証に近い

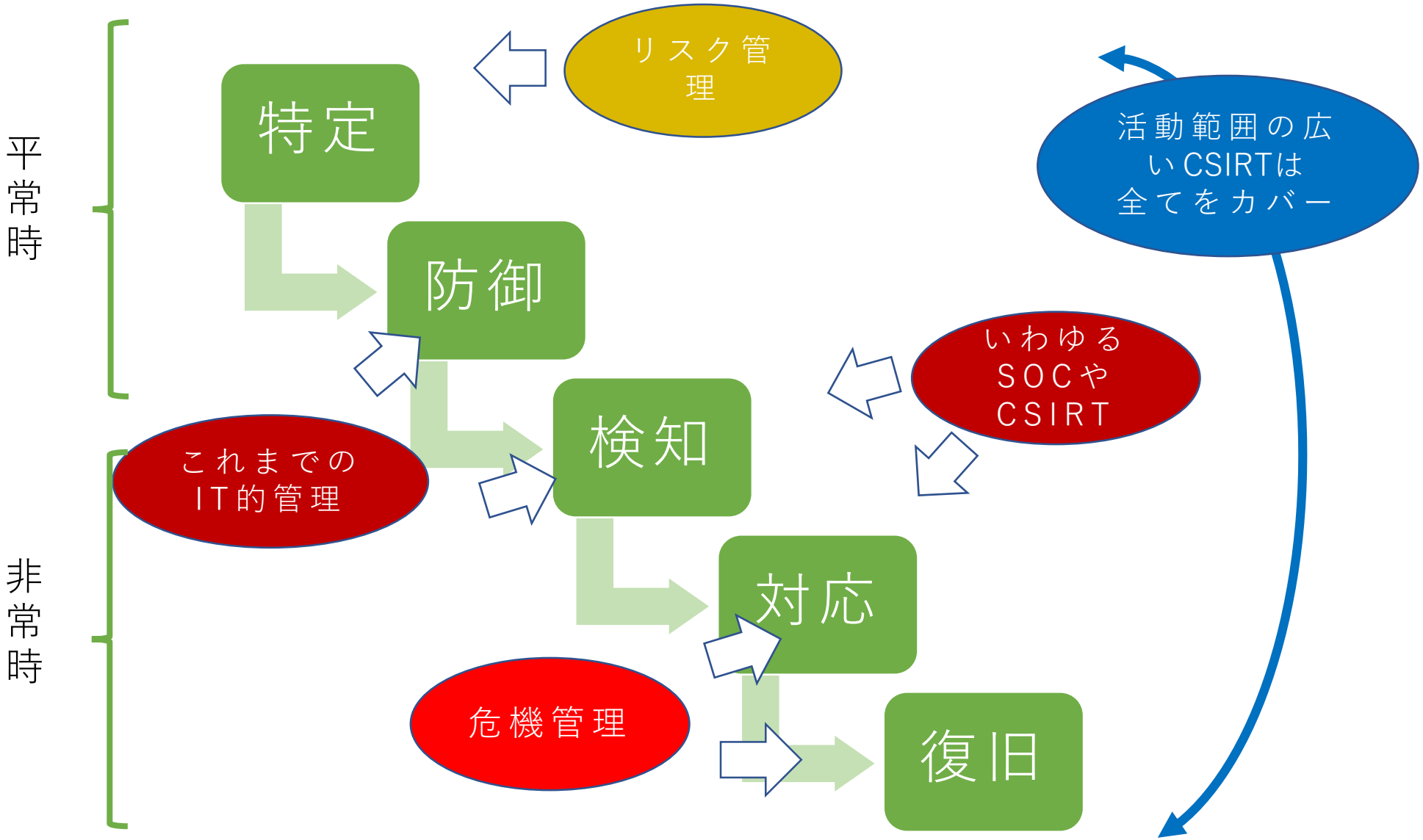
OODA Loop



航空戦の洞察に基づいた、指揮官の意思決定プロセスとして構築
Observe（監視）, Orient（情勢判断）, Decide（意思決定）, Act（行動）の４つのフェーズで構成

出典：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）

サイバーセキュリティフレームワーク-1



出典: 鎌田敬介
「サイバーセキュリティマネジメント入門」

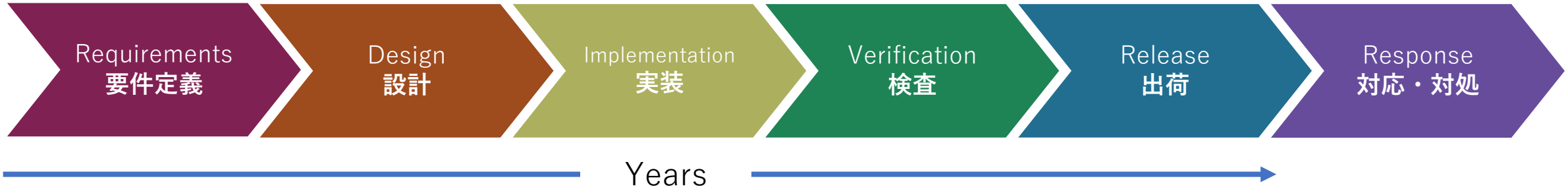
サイバーセキュリティフレームワーク-2

機能の一意の識別子	機能	カテゴリーの一意の識別子	カテゴリー
ID	特定	ID.AM	資産管理
		ID.BE	ビジネス環境
		ID.GV	ガバナンス
		ID.RA	リスクアセスメント
		ID.RM	リスク管理戦略
PR	防御	PR.AC	アクセス制御
		PR.AT	意識向上およびトレーニング
		PR.DS	データセキュリティ
		PR.IP	情報を保護するためのプロセスおよび手順
		PR.MA	保守
		PR.PT	保護技術
DE	検知	DE.AE	異常とイベント
		DE.CM	セキュリティの継続的なモニタリング
		DE.DP	検知プロセス
RS	対応	RS.RP	対応計画の作成
		RS.CO	伝達
		RS.AN	分析
		RS.MI	低減
		RS.IM	改善
RC	復旧	RC.RP	復旧計画の作成
		RC.IM	改善
		RC.CO	伝達

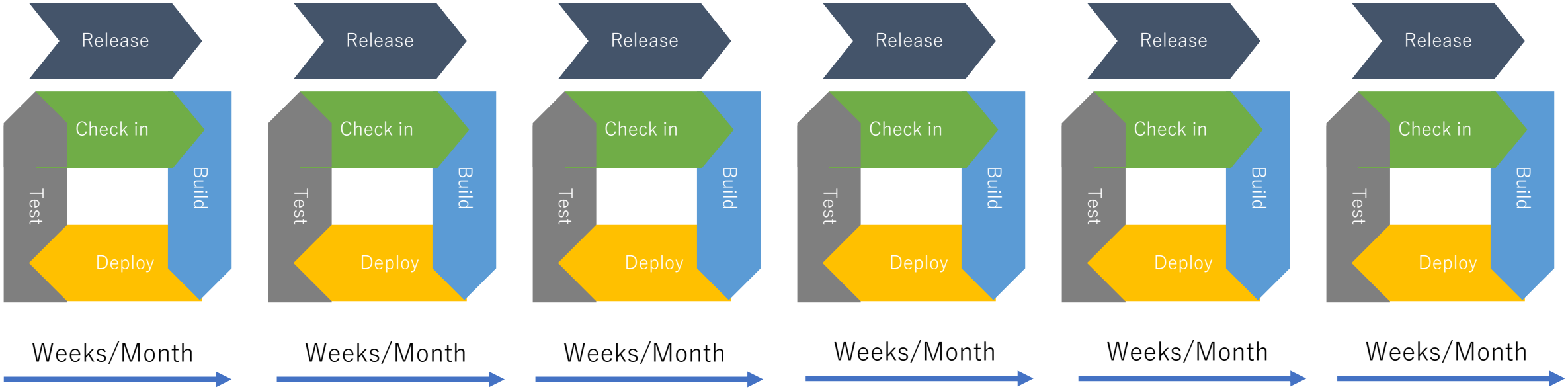
機能	カテゴリー	サブカテゴリー	参考情報
特定 (ID)	**資産管理(ID.AM)**: 組織が事業目的を達成することを可能にするデータ、職員、デバイス、システム、施設を特定し、事業目標と自組織のリスク戦略との相対的重要性に応じて管理している。	**ID.AM-1**: 企業内の物理デバイスとシステムの一覧を作成している。	• **CCS CSC** 1 • **COBIT 5** BAI09.01, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-2: 企業内のソフトウェアプラットフォームとアプリケーションの一覧を作成している。	• **CCS CSC** 2 • **COBIT 5** BAI09.01, BAI09.02, BAI09.05 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-3: 企業内の通信とデータの流れの図を用意している。	• **CCS CSC** 1 • **COBIT 5** DSS05.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISO/IEC 27001:2013** A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: 外部情報システムの一覧を作成している。	• **COBIT 5** APO02.02 • **ISO/IEC 27001:2013** A.11.2.6 • **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: リソース(例:ハードウェア、デバイス、データ、ソフトウェア)を、分類、重要度、ビジネス上の価値に基づいて優先順位付けしている。	• **COBIT 5** APO03.03, APO03.04, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.6 • **ISO/IEC 27001:2013** A.8.2.1 • **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14
		ID.AM-6: すべての従業員と第三者である利害関係者(例:供給業者、顧客、パートナー)に対して、サイバーセキュリティ上の役割と責任を定めている。	• **COBIT 5** APO01.02, DSS06.03 • **ISA 62443-2-1:2009** 4.3.2.3.3 • **ISO/IEC 27001:2013** A.6.1.1

経営サイクルの加速

Waterfall



DevOps

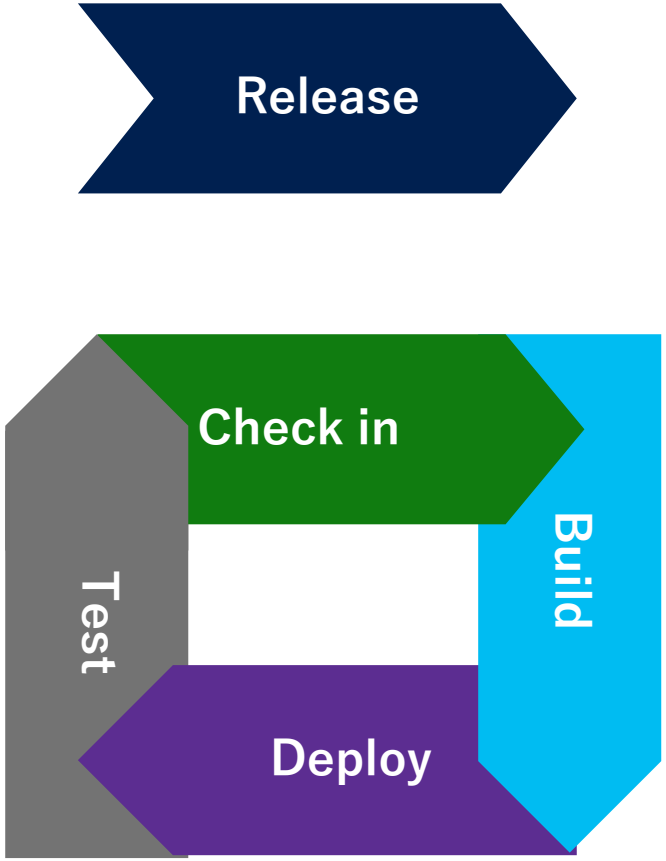


DevOpsの要素

アーキテクチャ

モジュール化

計測



継続的なリリース

自動化

基本となる経営指標

基本となる経営指標

平成29年12月期　決算短信〔日本基準〕(連結)

平成30年２月15日

上場会社名	トレンドマイクロ株式会社	上場取引所	東
コード番号	4704	URL	http://www.trendmicro.co.jp
代表者	(役職名) 代表取締役社長	(氏名)	エバ・チェン
問合せ先責任者	(役職名) 代表取締役副社長	(氏名)	マヘンドラ・ネギ　(TEL) 03-5334-3600
定時株主総会開催予定日	平成30年３月27日	配当支払開始予定日	平成30年３月28日
有価証券報告書提出予定日	平成30年３月27日		

決算補足説明資料作成の有無　：　有
決算説明会開催の有無　：　有　(　機関投資家・アナリスト向け　)

(百万円未満切捨て)

１．平成29年12月期の連結業績（平成29年１月１日～平成29年12月31日）

（１）連結経営成績　(%表示は対前期増減率)

	売上高		営業利益		経常利益		親会社株主に帰属する当期純利益	
	百万円	%	百万円	%	百万円	%	百万円	%
29年12月期	148,811	12.8	36,441	6.1	37,035	5.4	25,691	4.2
28年12月期	131,936	6.1	34,360	10.9	35,138	3.1	24,651	15.0

(注) 包括利益　29年12月期　27,694百万円(　27.2%)　28年12月期　21,773百万円(　36.8%)

	１株当たり当期純利益	潜在株式調整後１株当たり当期純利益	自己資本当期純利益率	総資産経常利益率	売上高営業利益率
	円 銭	円 銭	%	%	%
29年12月期	187.01	185.24	15.1	11.6	24.5
28年12月期	179.63	178.80	15.3	11.7	26.0

(参考) 持分法投資損益　29年12月期　586百万円　28年12月期　390百万円

（２）連結財政状態

	総資産	純資産	自己資本比率	１株当たり純資産
	百万円	百万円	%	円 銭
29年12月期	331,157	177,077	53.0	1,274.45
28年12月期	308,537	166,471	53.4	1,202.12

(参考) 自己資本　29年12月期　175,409百万円　28年12月期　164,861百万円

（３）連結キャッシュ・フローの状況

	営業活動によるキャッシュ・フロー	投資活動によるキャッシュ・フロー	財務活動によるキャッシュ・フロー	現金及び現金同等物期末残高
	百万円	百万円	百万円	百万円
29年12月期	46,915	△33,817	△16,908	98,440
28年12月期	33,510	12,925	△15,050	102,375

２．配当の状況

四半期報告書

第一部【企業情報】

第１【企業の概況】

１【主要な経営指標等の推移】

回次		第18期第３四半期連結累計期間	第19期第３四半期連結累計期間	第18期
会計期間		自　平成28年４月１日 至　平成28年12月31日	自　平成29年４月１日 至　平成29年12月31日	自　平成28年４月１日 至　平成29年３月31日
売上高	(千円)	16,043,574	16,606,326	22,092,016
経常利益	(千円)	1,328,676	1,432,911	2,109,341
親会社株主に帰属する四半期（当期）純利益	(千円)	797,991	934,587	1,383,036
四半期包括利益又は包括利益	(千円)	810,620	942,667	1,401,786
純資産額	(千円)	6,476,264	7,790,733	7,067,922
総資産額	(千円)	11,620,313	12,435,286	12,347,679
１株当たり四半期（当期）純利益金額	(円)	42.84	48.73	73.83
潜在株式調整後１株当たり四半期（当期）純利益金額	(円)	42.36	―	72.82
自己資本比率	(%)	55.7	62.7	57.2

回次		第18期第３四半期連結会計期間	第19期第３四半期連結会計期間
会計期間		自　平成28年10月１日 至　平成28年12月31日	自　平成29年10月１日 至　平成29年12月31日
１株当たり四半期純利益金額	(円)	17.89	18.41

(注) １　当社は四半期連結財務諸表を作成しているため、提出会社の主要な経営指標等の推移については記載しておりません。
２　売上高には、消費税等は含まれておりません。
３　第19期第３四半期連結累計期間の潜在株式調整後１株当たり四半期純利益金額については、潜在株式が存在しないため記載しておりません。

財務会計と管理会計（飛行機のメタファー）

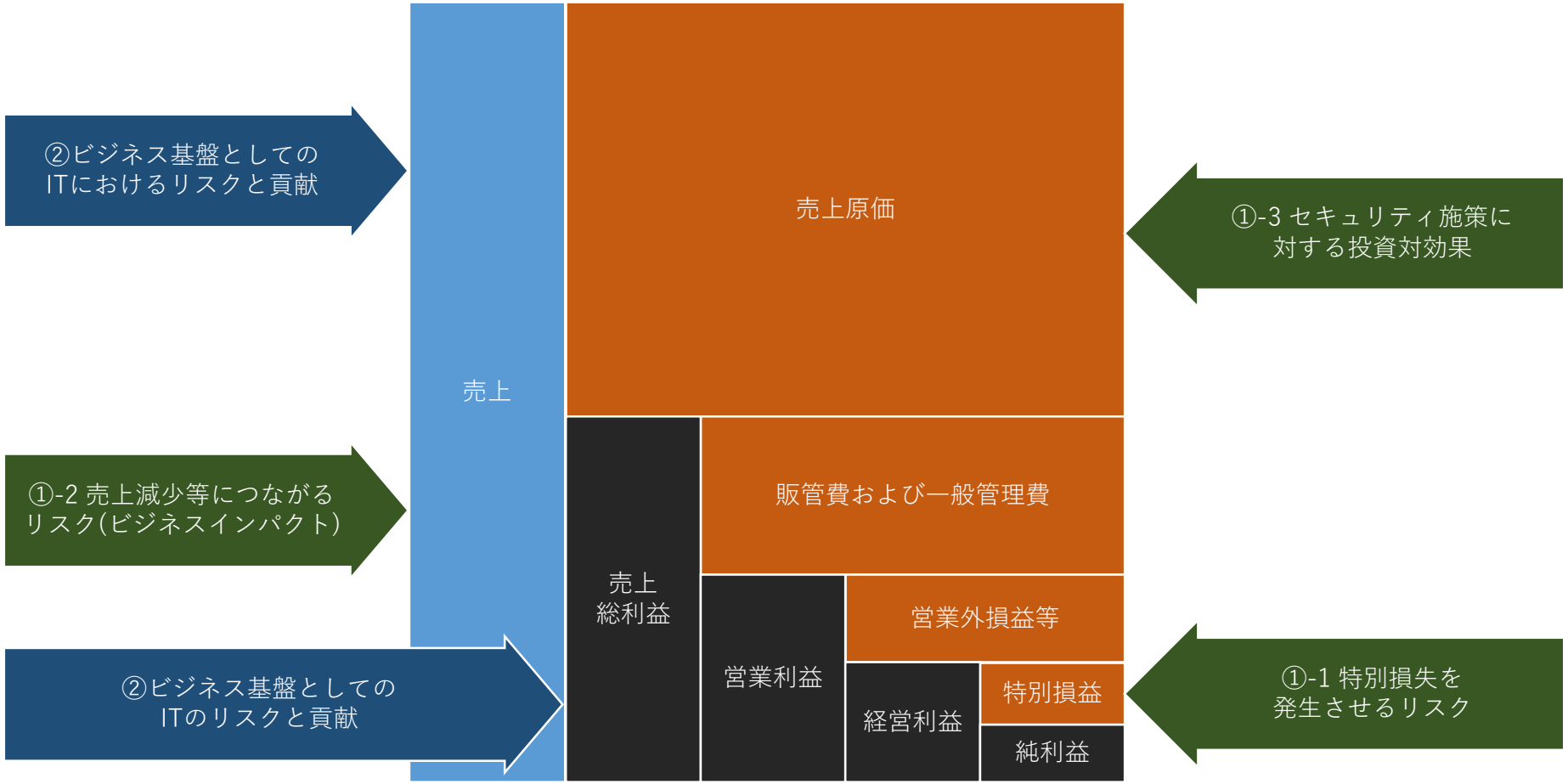
財務会計

HANEDA | フライト情報 | 交通アクセス | 空港マップ | サービス施設 | ショップ&レストラン | 空港を楽しもう | よくあるご質問

17:30	17:44	佐賀	ANA	ANA0456	第2	5・6	出口5・6
17:35	17:44	徳島	ANA	ANA0284	第2		到着済み
17:35	17:40	札幌（新千歳）	JAL	JAL0516	第1	4・5／6	出口4・5／6
17:40	17:45	長崎	SKY	SKY0446	第1		到着済み
17:40	17:45	神戸	SKY	SKY0446	第1		到着済み
17:40	17:45	神戸	SKY	SKY0112	第1		到着済み
17:40	17:46	札幌（新千歳）	ANA	ANA4728	第2		到着済み
17:40	17:46	札幌（新千歳）	AIR DO	ADO0028	第2		到着済み
17:40	17:58	福岡	JAL	JAL0320	第1	4・5／6	出口4・5／6
17:40	17:46	大阪（伊丹）	JAL	JAL0126	第1	8・9／7	出口8・9／7
17:40	17:42	沖縄（那覇）	ANA	ANA0470	第2	1・2	出口1・2
17:45	18:39	岡山	JAL	JAL0240	第1		遅れ
17:45	17:55	福岡	ANA	ANA3850	第1	2・3／1	出口2・3／1
17:45	17:55	福岡	SFJ	SFJ0050	第1	2・3／1	出口2・3／1
17:45	17:52	高知	JAL	JAL0496	第1	4・5／1	出口4・5／1
17:50	17:55	小松	ANA	ANA0756	第2	2・3	出口2・3
17:50	17:48	能登	ANA	ANA0750	第2	2・3	出口2・3
17:55	18:26	福岡	SKY	SKY0018	第1		遅れ
17:55	18:11	鹿児島	JAL	JAL0650	第1	8・9／12	出口8・9／12
17:55	18:00	札幌（新千歳）	SKY	SKY0720	第1	10・11／12	出口10・11／12
18:05	---	熊本	SNJ	SNJ0018	第2		欠航
18:05	---	熊本	ANA	ANA3718	第2		欠航

管理会計

BSにみるセキュリティの変化



情報セキュリティの指標化

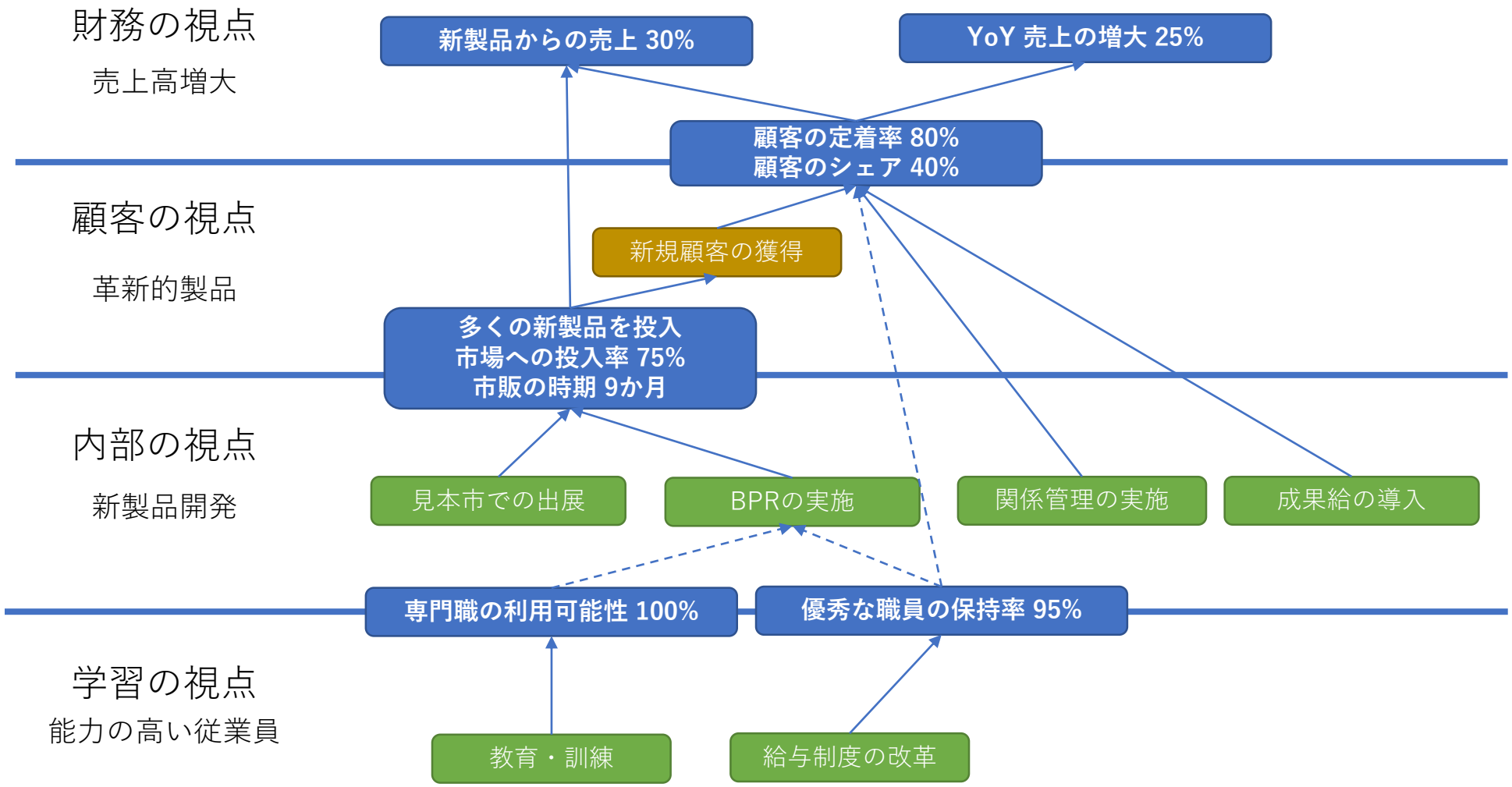
～バランス・スコアカードの活用～

戦略テーマ、戦略目標、目標値、実施項目

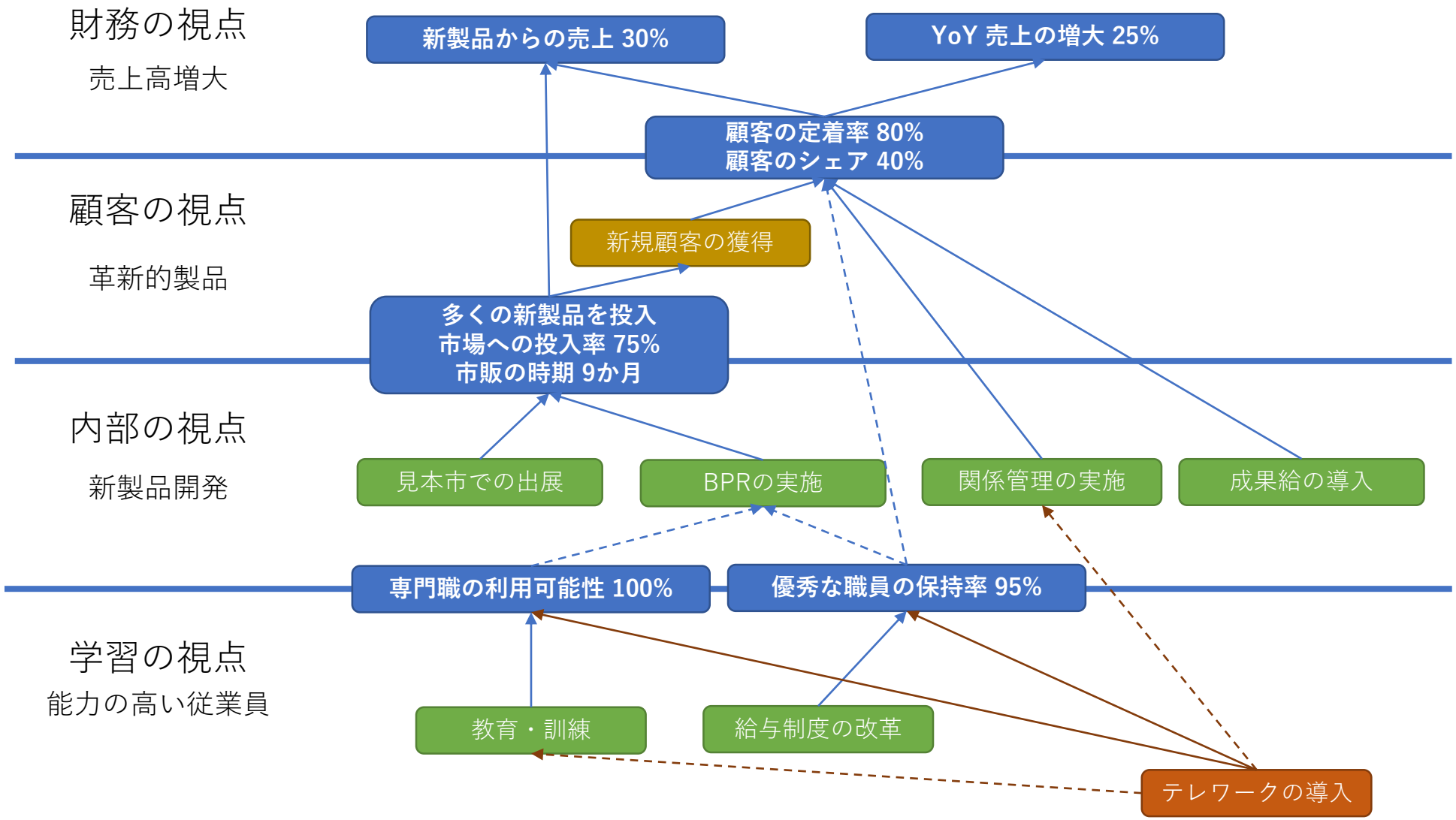
視点	戦略テーマ	戦略目標	目標値	実施項目
財務の視点	売上高増大	年々の売上伸び率	＋25%	×
		新製品からの売上	30%	×
顧客の視点	革新的製品	顧客の定着率	80%	関係管理の実施
		顧客のシェア	40%	成果給の導入
内部の視点	新製品開発	市場への投入率	75%	見本市での出展
		市販の時期	9ヶ月	BPRの実施
学習の視点	能力の高い従業員	専門職の利用可能性	100%	教育・訓練
		優秀な職員の保持率	95%	給与制度の改革

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



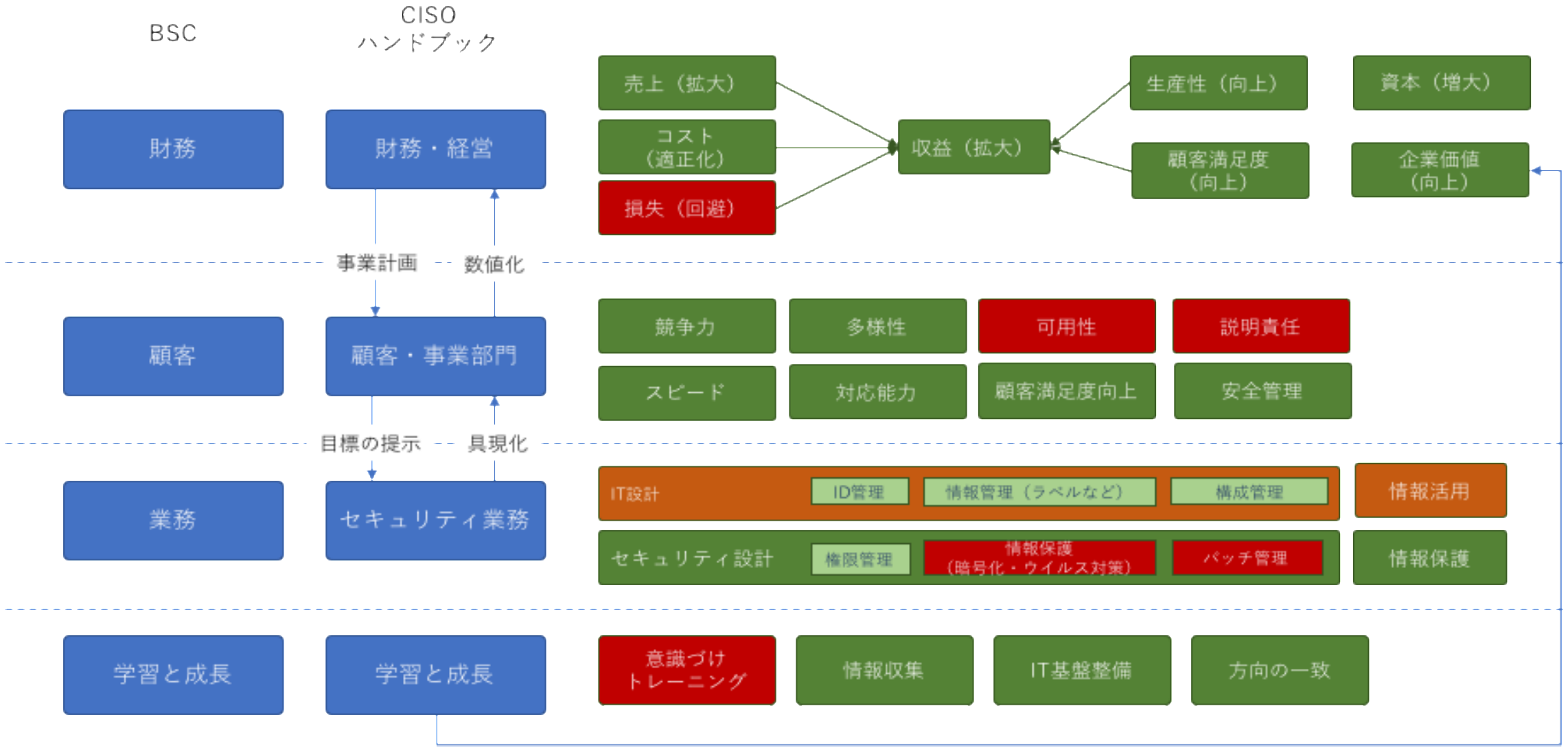
戦略マップ：テレワーク導入



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

バランスト・スコアカードを参考にした指標と業務づくりの例

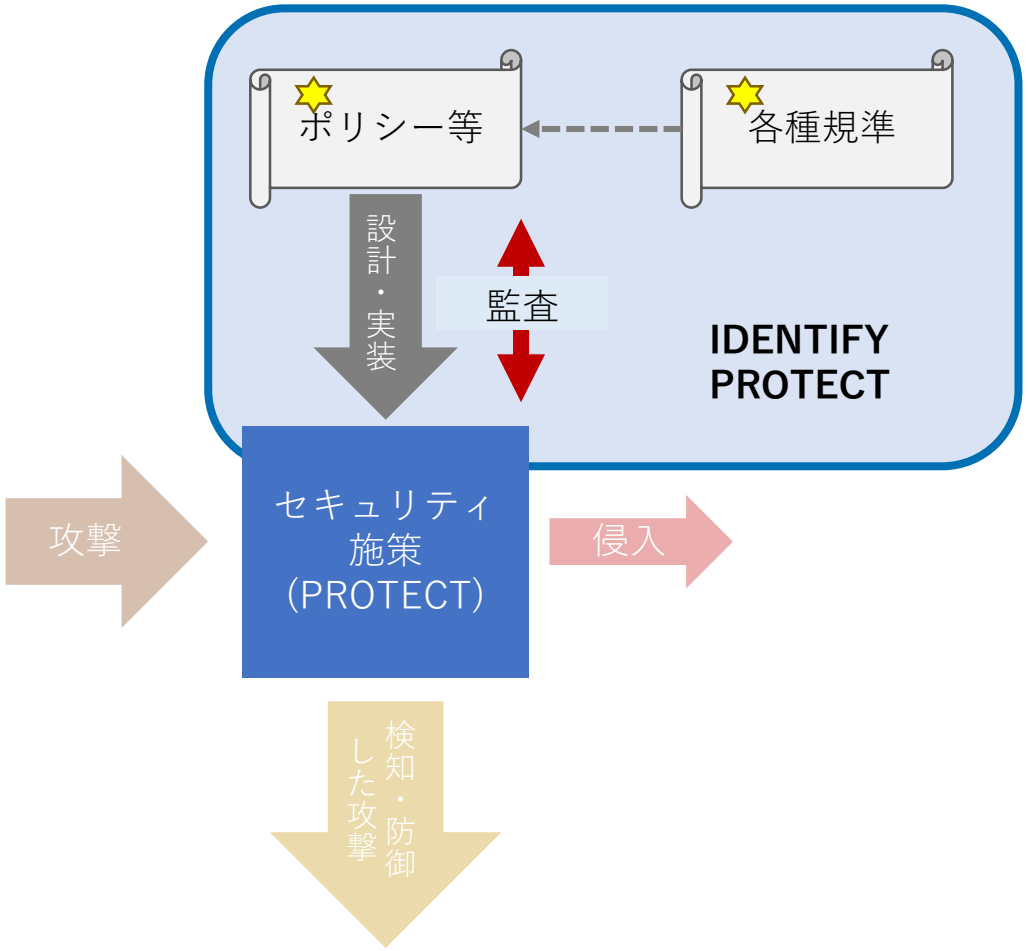


情報セキュリティの評価とモニタリング

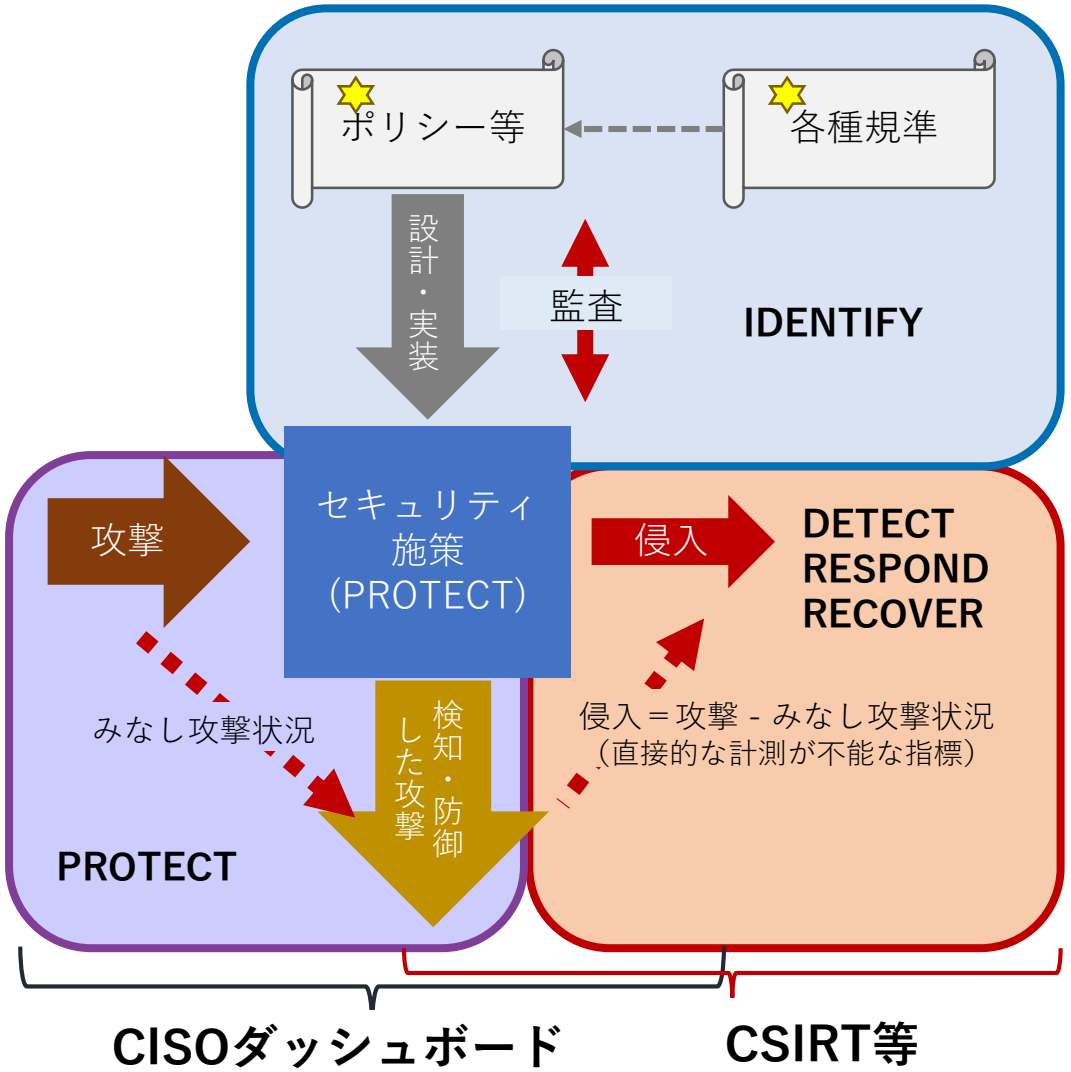
ディスカッションテーマ

計測項目の考察：CISOダッシュボード

一般的なPROTECT＝ポリシー遵守状況



CISOダッシュボードの指標



CISO ダッシュボード：業務執行としてのセキュリティ

CSIRTではなく、業務執行としてのセキュリティ

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

Attack

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

経営会議で何を報告すべきなのか
どのように決済を仰ぐべきなのか

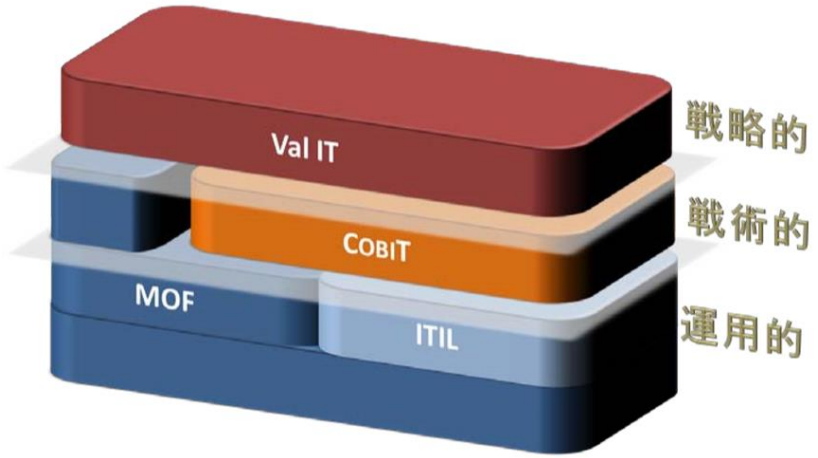
セキュリティ報告書（XX年度XX月　経営会議向け）

			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日までに狩猟予定。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*xxx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（参考資料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。 分析を早め、より効果的な防御を行うためには、より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	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。
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
	概況的	1	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。IT/セキュリティ部門では展開済み。 当ミーティングでコピーを配布します

セキュリティのための IT基盤設計

ディスカッションテーマ

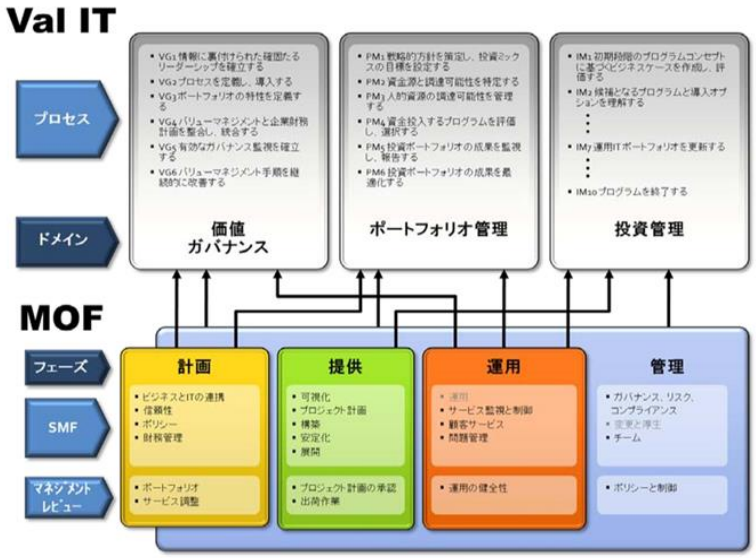
MOF と COBIT/Val IT の 比較および クロスインプリメンテーション



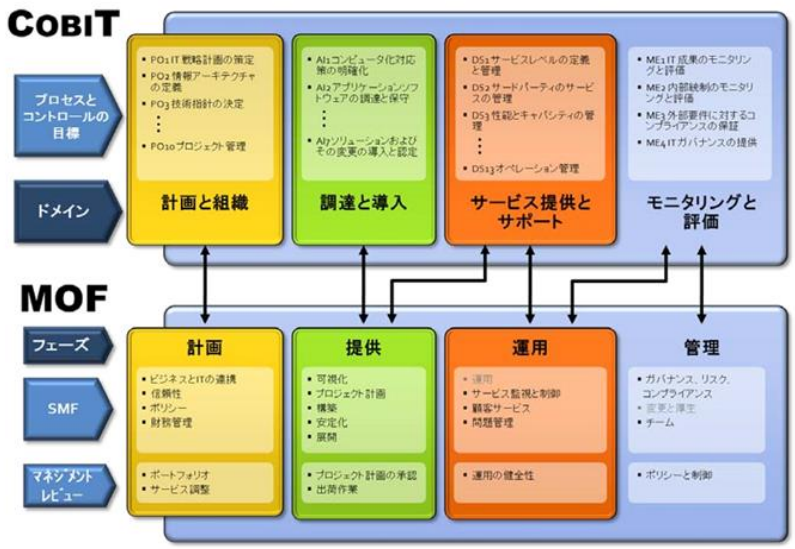
MOF:Microsoft® Operations Framework

http://www.itgi.jp/pdfdata/MOF%20to%20COVIT,Val%20IT.pdf

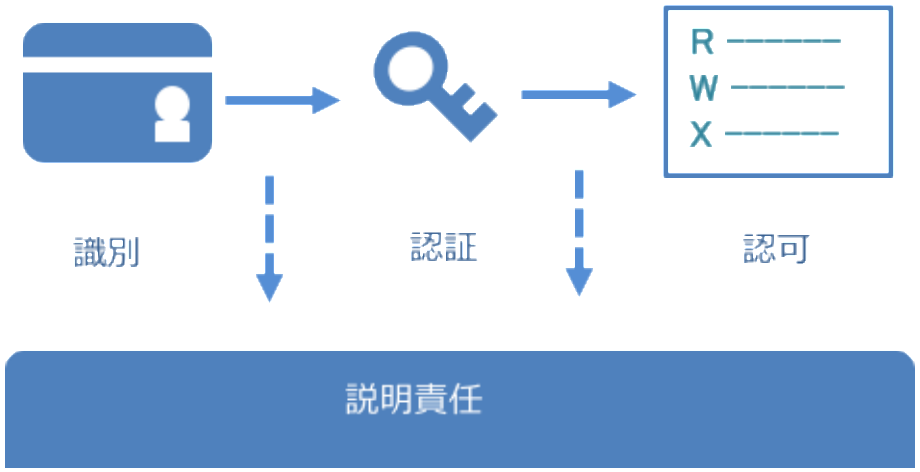
MOF と Val IT の高レベルのインターフェイス



MOF と COBIT の高レベルのマッピング



セキュリティを内包したIT基盤設計の方針



- リスク分析
- アクセス制御
- 情報分類
- 権限管理
- ネットワークアクセス制御
- 統制基盤
- 統合ログ管理

経営陣としてのCISOへの期待

ディスカッションテーマ

主要な社内のステークフォルダー

想定されるインシデント

想定される発表内容	担当などの確認
事故の概要 影響を受ける顧客数と特徴 想定される二次被害 顧客などに推奨する対策 事故の原因・要因 事業への影響の有無 再発防止策	責任者 （CEO, CIO, CTO, CSO, CISO等） 報道対応 事故調査、まとめ 法的な検討 顧客対応 その他

	インシデント	情報元/受付部門
1	標的型攻撃で機密情報が漏れた可能性があることが、外部からの連絡で判明した	JPCERT/CC CSIRT
2	ハッカーの侵入を受けて、すべてのメールがインターネットに公開されたと連絡が入った	メディア 広報
3	WEBページから顧客情報が閲覧可能な状態にあると連絡	個人（匿名） 広報
4	自社にしか登録をしていない「メールアドレスに広告が入った」とのクレームが、今日になって入った	顧客 ユーザサポート
5	顧客から、弊社にしか登録をしていない「クレジットカードが勝手に使われた」とのクレームが入った	顧客 ユーザサポート
6	インターネット上の掲示板に弊社の顧客情報を含むドキュメントが掲載されている	取引先 担当営業
7	自社が所有するIPアドレスから攻撃を受けているとのクレームが入った	取引のない 海外企業 ユーザサポート
8	自社のメールアカウントを使った、標的メールが取引先に送信された	官公庁 大代表→広報
9	業務システムから、機密情報が社外に持ち出された	官公庁 大代表→広報
10	サービスで提供をしているWebサーバが、ミドルウエアの脆弱性を悪用され、改ざんをされた	官公庁 大代表→広報

インシデント・シミュレーション

ある日、「事件発覚」の中のひとつの項目が報告された。事件を公表するかどうかを、至急判断しなくてはならない。
公表するものとして、「想定される発表内容」をまとめる事は可能か、また、どの程度の時間が必要か。

事件発覚

- 標的型攻撃で**機密情報が漏れた**可能性があることが、警察とJPCERT/CCからの連絡で判明した
- ハッカーの侵入を受けて、**すべてのメールがインターネットに公開された**
- WEBページから**顧客情報が閲覧可能な状態**にある
- **弊社にしか登録をしていない「メールアドレス**に広告が入った」とのクレームが、今日になって３件目入った
- 顧客から、**弊社にしか登録をしていない「クレジットカード**が勝手に使われた」とのクレームが入った
- インターネット上の**掲示板に弊社の顧客情報**を含むドキュメントが掲載されている
- **弊社**が所有するIPアドレス**から攻撃**を受けているとのクレームが入った
- 弊社のメールアカウントを使った、**標的メールが取引先に送信された**

想定される発表内容

- 漏えいした情報の種類、
- 影響を受ける顧客数と特徴
- 想定される二次被害
- 推奨する対策
- 事故の原因・要因
- 事業への影響の有無
- 再発防止策

担当者などの整理

- 責任者（CEO, CIO, CTO, CSO, CISO?）
- 報道対応
- 事故調査、まとめ
- 法的な検討
- 顧客対応
- その他

むすび

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?
https://www.darkreading.com/vulnerabilities---threats/cisos-cyber-war-how-did-we-get-here/a/d-id/1330737

CISOハンドブックの構成

- CISOハンドブック v1.0β [4.70MB]

- CISOダッシュボードv09 [1.94MB]

  ※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」と呼称し考察しました。

- インシデント対応ワークショップVer01 [1.58MB]

  ※「インシデント対応手順」の策定を通じて、組織のセキュリティ在り方やステークホルダーを明らかにし、事故が発生した際には、手順に従ったインシデント対応を適切かつ遅滞なく実施できることを目指すものです。

- インシデント対応ワークショップ-表v02 [47KB]

※上記ワークショップを行う場合に使う表です。

社会活動部会
CISO支援ワーキンググループ