McAfee MPOWER
講演資料
無断転載禁止

NTT DATA
Trusted Global Innovator

経営リスク管理から考える Security by Design

2018年11月8日

ＮＴＴデータ先端技術株式会社
相談役・最高技術顧問
工学博士、CISSP, PCI DSS QSA
三宅功

経営リスク管理とSecurity by Design

☆ 経営リスク管理は経営陣の責務の１つ　コーポレートガバナンス･コード

【基本原則３】上場会社は、会社の財政状態･経営成績等の財務情報や、経営戦略･経営課題、リスクやガバナンスに係る情報等の非財務情報について、法令に基づく開示を適切に行うとともに、法令に基づく開示以外の情報提供にも主体的に取り組むべきである。

【基本原則４】、、、、会社の持続的成長と中長期的な企業価値の向上を促し、収益力･資本効率等の改善を図るべく、

－－－－－－－－－－－－－－－－－－－－－－－－

(2) 経営陣幹部による適切なリスクテイクを支える環境整備を行うこと

－－－－－－－－－－－－－－－－－－－－－－－－

☆ とは言え、事業運営には様々なリスクが存在する。情報セキュリティに関するリスクはOne of Them。さらにはITが密接にからむとともに環境変化が激しいため、理解･認識が難しい。

☆ 本日お伝えしたい“Security by Design”とは事業システムそのものへ情報セキュリティ対策を作りこむこと。これによりAdd onでなくBuilt inによる企業の包括的･持続可能な情報セキュリティマネジメントを実現したい。

経営陣に求められるサイバーリスク対応

1. Directors should understand and approach cybersecurity as an enterprise-wide risk management issues, not just an IT issue.
2. Directors should understand the legal implications of cyber risk as they relate to their company's specific circumstances.
3. Boards should have adequate access to cybersecurity expertise, and discussion about cyber-risk management should be given regular and adequate time or board meeting agendas.
4. Directors should set the expectation that management will establish an enterprise-wide cyber-risk management framework with adequate staffing and budget.
5. Board-management discussions about cyber-risk should include identification of which risks to avoid, which to accept, and which to mitigate or transfer through insurance, as well as specific plans associated with each approach.

"Cyber-Risk Oversight - Director's Handbook Series", NACD (National Association of Corporate Directors) 2017

経営陣に求められるサイバーリスク対応

1. 経営陣はサイバーセキュリティ対策を、**ITに限定されたものではなく、全社をあげてのリスク対策と認識し**取り組む必要がある。

2. 経営陣は自社が置かれた環境に関連して、サイバーリスクの法的意味を十分に理解しておく必要がある。

3. 経営陣は、サイバーセキュリティの専門家に適宜アクセス可能であり、サイバーセキュリティリスク管理に関する議論を**定常的に適切なタイミングで実施する、或いは取締役会の議題**とすること。

4. 経営陣は、**適切な要員と予算配分の元での組織全体としてのサイバーリスク管理の枠組み（フレームワーク）を確立しておくこと**を求める必要がある。

5. **サイバーリスクに関する経営陣内での議論は**、どのリスクが除かれ、どのリスクが受容され、どのリスクが軽減あるいは保険による転嫁がなされたか、それぞれの事象に関する**個別の計画に基づいて行われる必要がある。**

“Cyber-Risk Oversight - Director’s Handbook Series”,
NACD(National Association of Corporate Directors) 2017

どうすれば良いのか？

☆ 大前提は、あくまで個々の組織の特性に合わせた情報セキュリティ対策を実施すること。

☆ そのためには、

① 自組織の組織目的、これに対応した組織構成とビジネスプロセス、サポートシステム（ITシステムを含む）、人材、サプライチェーン、物理施設等を棚卸し（**事業システムの把握**）

② これらの事業環境で扱われる重要情報（営業秘密、個人情報等）を処理、蓄積、転送レベルで把握するとともに、それが**失われた場合の組織目的に対する影響度（リスク）を評価**し

③ 重要情報及びこれを扱うシステムに対する費用対効果を考慮したリスク対策（管理策の適用）を行う⇒**世の中のベストプラクティスを活用**

☆ 標準化された**情報セキュリティマネジメントシステム**(ex. ISMS, NIST SP800等）は③実現のための**ベストプラクティス・リスト**であり、**自組織が情報セキュリティリスク管理を実施していることを対外的に表明するためのツール**でもある

リスク評価　Step-1

事業システムを特定し、情報資産・情報の流れを把握する

リスク評価　Step-2　リスクの特定

特定された情報資産・情報が侵害された場合の影響度からその重要度を決定する。

情報資産		オーナー/組織	処理・蓄積転送フロー	重要度評価			脅威			リスク評価	対策の現状評価
				C	I	A	O	I	M		
営業秘密				高	中	低	大	中	小	高	
	-----									中 低	
個人情報											

情報システム											

物理施設											

外部関係 (ｻﾌﾟﾗｲﾁｪｰﾝ)											

C: 機密性　O: 外部
A: 可用性　I：内部
I：完全性　M: 意図しないミス

重要度は経済的インパクトだけでなく法規制上から見た要求も含まれる

セキュリティ管理策をどう決めて行くか

☆ リスクの特定結果から、これを低減する管理策を**費用対効果の観点で優先度付け**して決める。

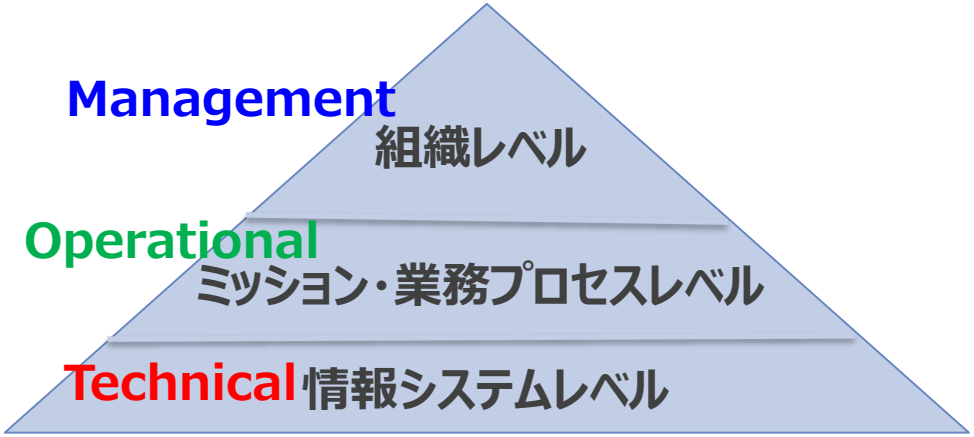
☆ 管理策は、**①組織的・人的対策、技術的対策、物理的対策の視点、②マネジメント、プロセス、システムの階層的視点**、で考える。

ISO 27001より

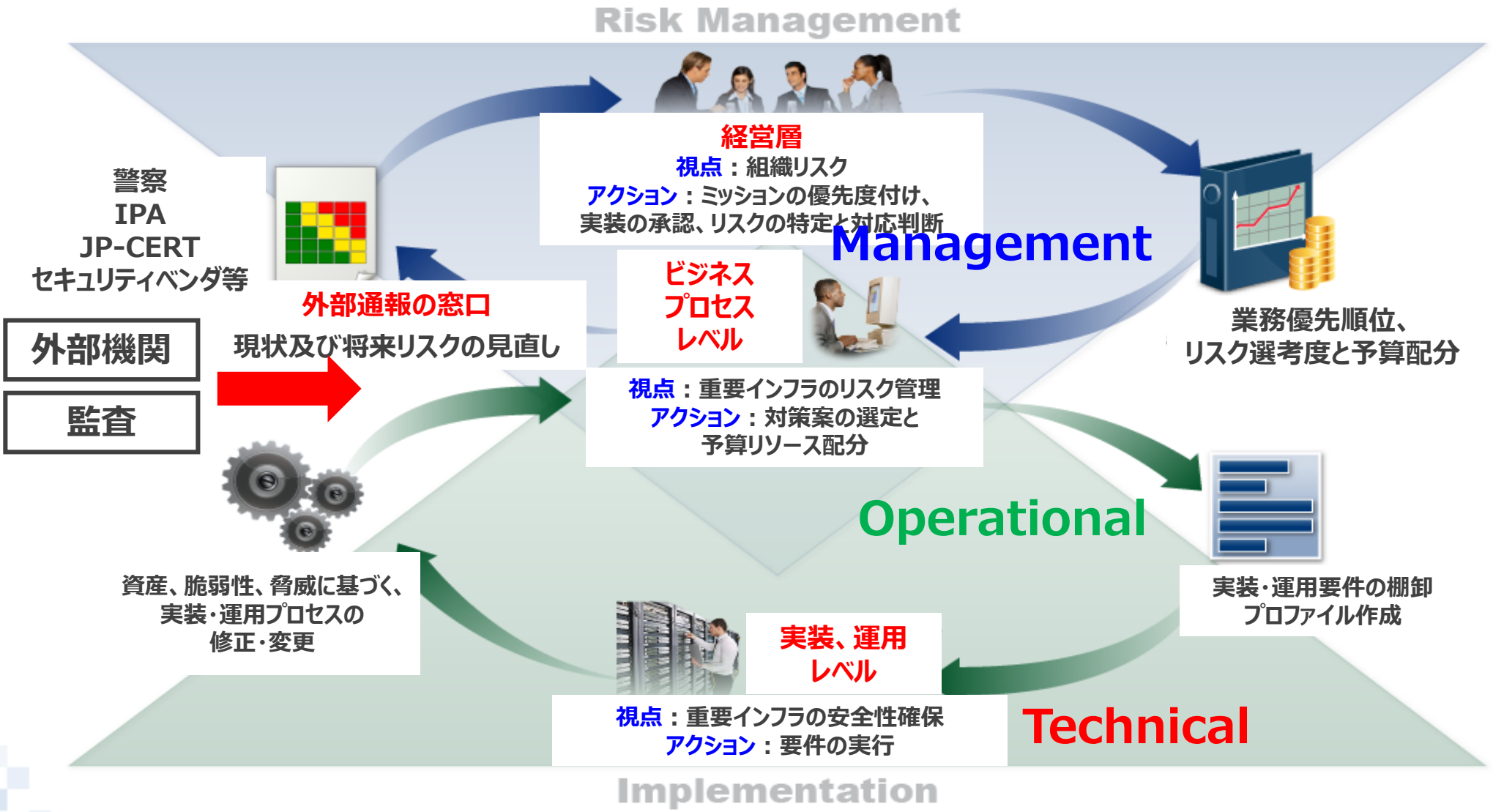
附属書A（規定）管理目的及び管理策

A.5 情報セキュリティのための方針群 A.6 情報セキュリティのための組織 A.7 人的資源のセキュリティ A.8 資産の管理	人的・組織的対策
A.9 アクセス制御 A.10 暗号	技術的対策
A.11 物理的及び環境的セキュリティ	物理的対策
A.12 運用のセキュリティ	技術的対策
A.13 通信のセキュリティ A.14 システムの取得、開発及び保守	技術的対策
A.15 供給者関係 A.16 情報セキュリティインシデント管理 A.17 事業継続マネジメントにおける情報セキュリティの側面 A.18 順守	人的・組織的対策

NIST SP800-53より



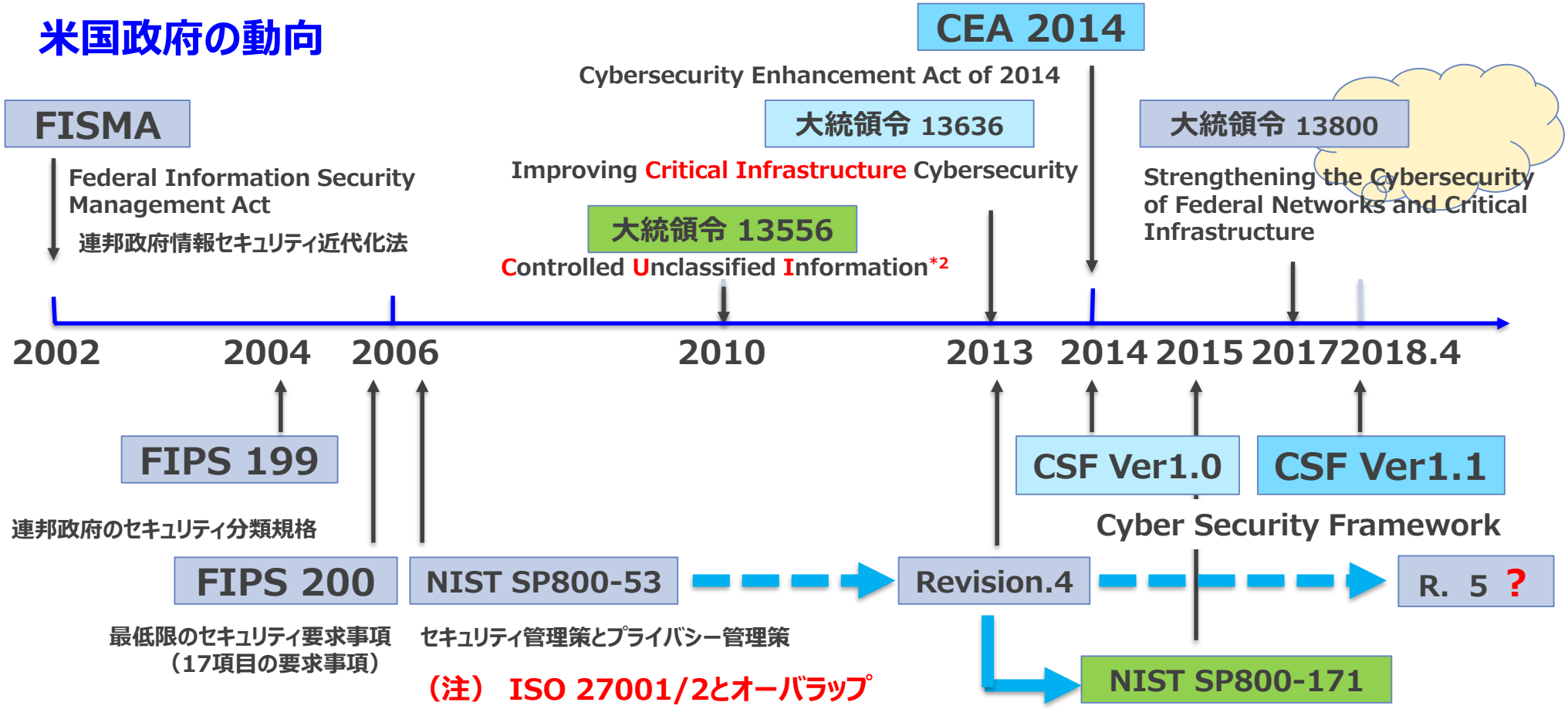
セキュリティ管理策をどう回していくか？



NIST Framework for Improving Critical Infrastructure Cybersecurity Ver1.1より

NIST SP800-53とCyber Security Frameworkについて

米国政府の動向



NIST*1の対応状況

*1 National Institute of Standard and Technology

*2 National Archives and Records Administrationで管理

NIST SP800-53 Re.4　管理策ファミリ

☆ ISO 27001/2の管理策とかなり重複するが、より詳細に規定

ID	管理策ファミリー	項目数＆レベル
AC	アクセス制御	25, Technical
AT	意識向上及びトレーニング	5, Operational
AU	監査及び責任追跡性	16, Technical
CA	セキュリティ評価及び運用認可	9, Management
CM	構成管理	11, Operational
CP	緊急時対応計画	13, Operational
IA	識別及び認証	11, Technical
IR	インシデント対応	10, Operational
MA	保守	6, Operational

ID	管理策ファミリー	管理レベル
MP	メディア保護	8, Operational
PE	物理的及び環境的な保護	19, Operational
PL	計画作成	7,Management
PS	人的セキュリティ	8, Operational
RA	リスク評価	5, Management
SA	システム及びサービス調達	20, Management
SC	システム及び通信の保護	41, Technical
SI	システム及び情報の完全性	16, Operational
PM	情報セキュリティプログラム管理	16. Management

１８ファミリ、Technical　93 Operational 96 Management 57, Total 246項目

NIST SP800-53 Re.4　管理策の構造

	順序	アクション
P1	最初	最初の実装として実装する。
P2	次	P1管理策後に実装する
P3	最後	P1,P2管理策後に実装する
P0	指定なし	ベースライン管理策対象外

FIPS 199で規定

影響度	組織活動、組織資産、個人に対して
低	限定的な悪影響
中	重大な悪影響
高	致命的または破滅的悪影響

管理策番号	管理策名	優先順位	当初のベースライン管理策		
			低	中	高
アクセス制御					
AC-1	アクセス制御ポリシーおよびアクセス制御手順	P1	AC-1	AC-1	AC-1
AC-2	アカウント管理	P1	AC-2	AC-2(1)(2)(3)(4)	AC-2(1)(2)(3)(4)(5)(11)(12)(13)
AC-3	アクセス強制	P1	AC-3	AC-3	AC-3
AC-4	情報フローの強制	P1	選択されていない	AC-4	AC-4
AC-5	職務の分離	P1	選択されていない	AC-5	AC-5
AC-6	最小権限の原則	P1	選択されていない	AC-6(1)(2)(5)(9)(10)	AC-6(1)(2)(3)(5)(9)(10)
AC-7	不正ログイン試行	P2	AC-7	AC-7	AC-7

NIST SP800-171とISO 27001/2

☆ NIST SP800-171はCUI（管理された非格付け情報）の管理をSP800-53で規定される中程度の管理策で守ることが対象。

☆ ISO 27001/2でカバーされていない部分は、

NIST SP800-171　付属書Dに記述 → 以下のような差分あり

- 特権管理の詳細化
- 非アクティブなセッションの制御
- リモートアクセス管理の詳細化
- モバイルディバイス、可搬ストレージ等の管理の詳細化
- 監査プロセスの詳細化、ログの関連付け
- 情報システムコンポーネントのセキュリティ強化
- アプリケーション、サービス、プロトコル等の機能の最小化
- ネットワークアクセスにおけるユーザ識別・認証の詳細化
- パスワード管理の詳細化
- インシデント対応能力の試験
- システムメンテナンス要件の詳細化
- 持ち出しメディアの保護
- 物理アクセスの監視
- 脆弱性スキャンの詳細化
- システム及び通信の保護の強化
- 通信及びシステムの不正使用の兆候把握

（１）JASA,“管理された非格付け情報の保護対策マネジメントガイドライン”, 2018.2

NIST Cyber Security Framework Ver1.1, 2018.4版

☆ 重要インフラのサイバーセキュリティを向上させるためのフレームワーク

☆ 2014.2にVer1.0が出された後、官民連携して継続的にバージョンアップ

最新版では、サプライチェーンリスクマネジメント、内部監査への活用等が追加

☆ 基本的には次の３つの要素で構成される

１）フレームワークコア(Framework Core)

サイバーセキュリティの脅威に対応するための一般的プロセスとこれに対応した要求条件をリスト化
これに基づいて、自組織に必要な管理策選定のガイドラインを与える

２）フレームワークインプレメンテーションティア(Framework Implementation Tier)

１）のアクションに対応した管理策を選定するとともに、選定した管理策がどこまで有効かを評価
→選定はあくまで組織の特性に対応したリスク低減に対する有効性vs.コストで実施

３）フレームワークプロファイル(Framework Profile)

リスクベース

各要求条件に対応したリスク低減のために本来必要な管理策と、現在状況のギャップを分析しリスクが受容可能なレベルに向けてのロードマップを作製する

☆ さらに、最新版ではサプライチェーン及び内部監査について言及

Framework Coreの構成

想定されるセキュリティ侵害のプロセスに合わせ、要件を整理

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

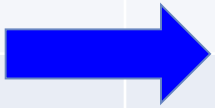
NIST SP800-53等の
ベストプラクティス
ミッションに合わせた管理策を選定する

Framework Tierの構成

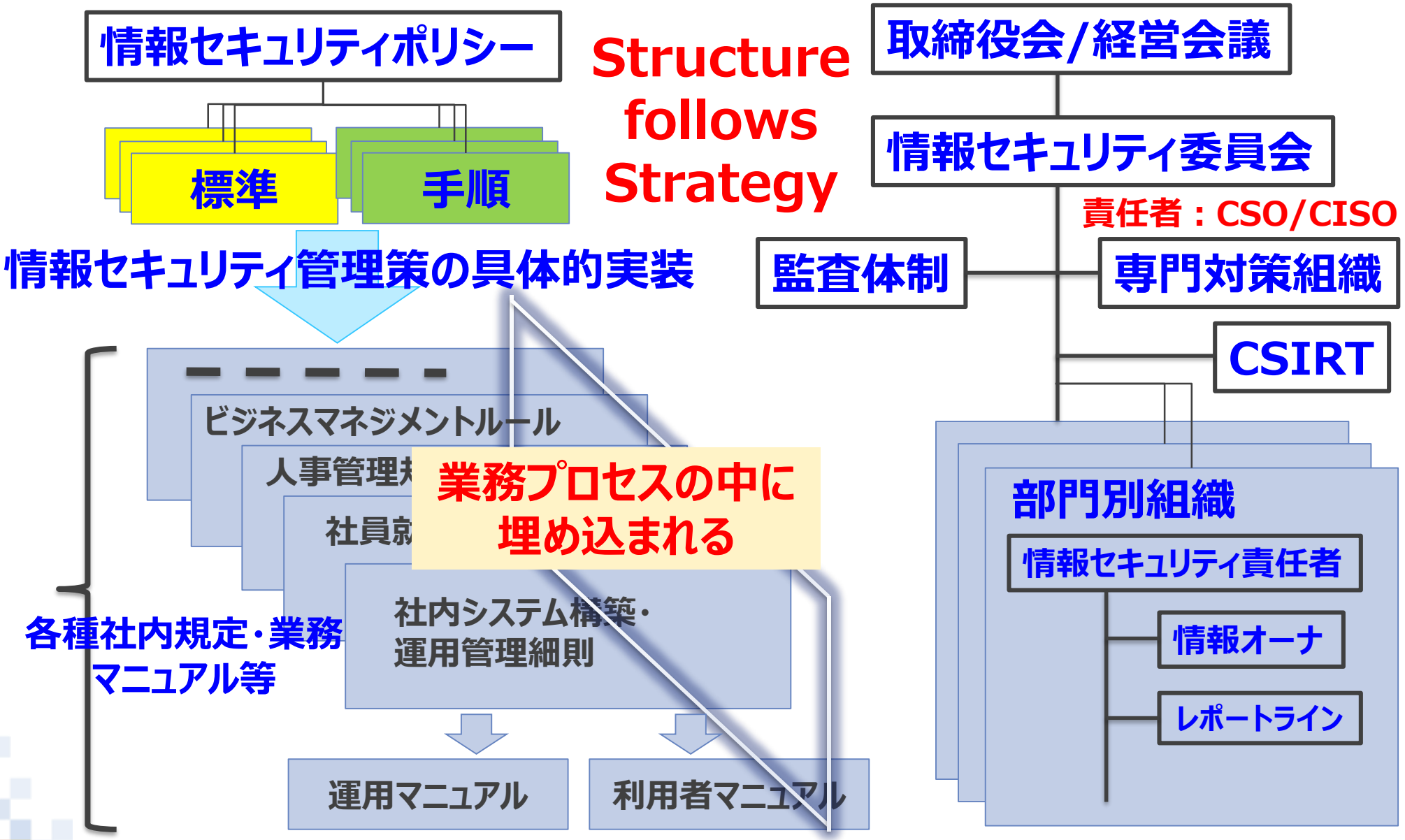
対策の完成度を４つのTierで評価

	リスク管理プロセス	リスク管理の統合化	外部関係
ティア1 Partial	リスク対策は確立されていない	組織全体にわたるリスク対策が行われていない	プロセスが不十分
ティア2 Risk Informed	リスク対策は部分的に存在。ポリシーとして不十分。	組織全体としての取り組みは行われていない	関係性は理解されているがリスクを共有する仕組みはない
ティア3 Repeatable	リスク対策はポリシーとして明確になっている	組織全体にわたる取り組みが確立されている	イベント発生時の対応連携が確立されている
ティア4 Adaptive	予測的な対応、継続的な改善のプロセスができている	想定されるリスク情報に基づいた組織全体にわたる取り組みができている	事前情報の共有、活用が行われている

Framework Profile

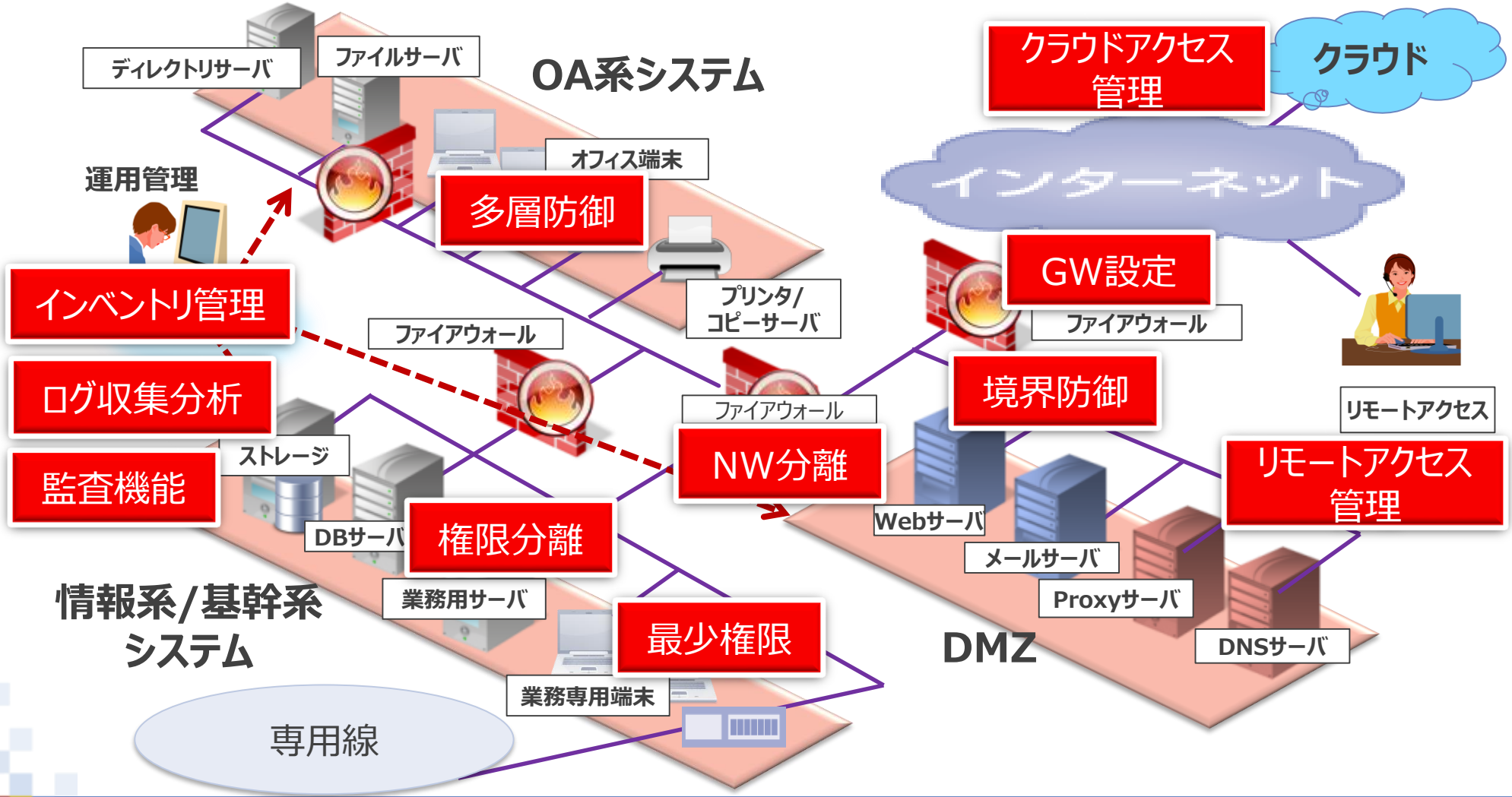
	現状の管理策リスト	目指すべき管理策リスト
特定		
防御	Tier： X 	Tier： X＋１
検知		
対応		
復旧		

ポイントはドキュメント化と組織実装



技術的対策としての管理策のマッピング

情報システムに対して、基本的な技術的管理策をBuilt-in（設計・導入段階からの実装）する→機能重複回避、オペレーションの簡易化



NTT DATA

まとめ

☆ 情報セキュリティ対策はまず事業システムから考える

→ ITだけの対応ではない

☆ どの管理策を採用するかはリスクベースの判断で行う

→ 経営陣のコミットメントが必要

☆ ポリシーをベースとした情報セキュリティマネジメント方針に対応した組織を作る

→Stricture follows Strategy

☆技術的管理策は情報システムにBuilt-inされる

→機能重複の回避、オペレーションの簡易化

NTT DATA

Trusted Global Innovator