Deloitte.
デロイト トーマツ

CYBER INITIATIVE TOKYO | 2022

新時代を迎えるサイバーセキュリティの潮流と戦略の要諦

The essence of cyber security's trend and strategy in the new era

デロイト トーマツ サイバー合同会社

2022.12

本日のアジェンダ

転換期を迎えるサイバーセキュリティ動向

サイバーセキュリティ戦略の要諦（前半）

サイバーレジリエンス実現に向けて

サイバーセキュリティ戦略の要諦（後半）

本日の登壇者

岩本 高明（イワモト　タカアキ）

デロイト トーマツ サイバー合同会社
サイバー戦略担当
パートナー／執行役員

- 大手インテグレーター、戦略系コンサルファームを経て現職
- デロイト トーマツ サイバーにおいて日本の戦略チームの責任者を務める
- 戦略ファームのバックグラウンドを生かし、ビジネスと連動したサイバーセキュリティ戦略立案、リスク分析・対応方針立案等の業務を歴任
- CISO等の経営アジェンダを広くカバーし、ガバナンスからテクノロジーまでサイバー全体に広範な経験を有する
- 様々な業界・分野における経験に基づき、組織の事業・組織構造と一貫整合したサイバーセキュリティ施策の提言を多数実施

井上 健一 (イノウエ　ケンイチ)

デロイト トーマツ サイバー合同会社
サイバーレジリエンス担当
マネージングディレクター

- 2重恐喝型ランサムウェア、標的型攻撃、Webサイトへの不正アクセス、内部行為者による情報漏えい、コンピュータウイルス感染等、様々な情報セキュリティ事故に関して、調査、復旧、再発防止等を支援するプロジェクトを数多くリードしている。事故対応にて得られた知識・経験を活かし、金融機関、製薬業、商社、ECビジネスなどに対するサイバーセキュリティ管理態勢診断を提供している。

主要なプロジェクト実績

- 大手金融機関、大手製薬会社、大手メーカー、大手サービス業、大手ITベンダー等におけるサイバーインシデント調査、封じ込め・除去・回復に係る助言

グローバル品質のサイバーセキュリティファームとしてのCapabilityを最大限活用し、中長期にわたってクライアントの課題解決に向けた高度なサービスを提供

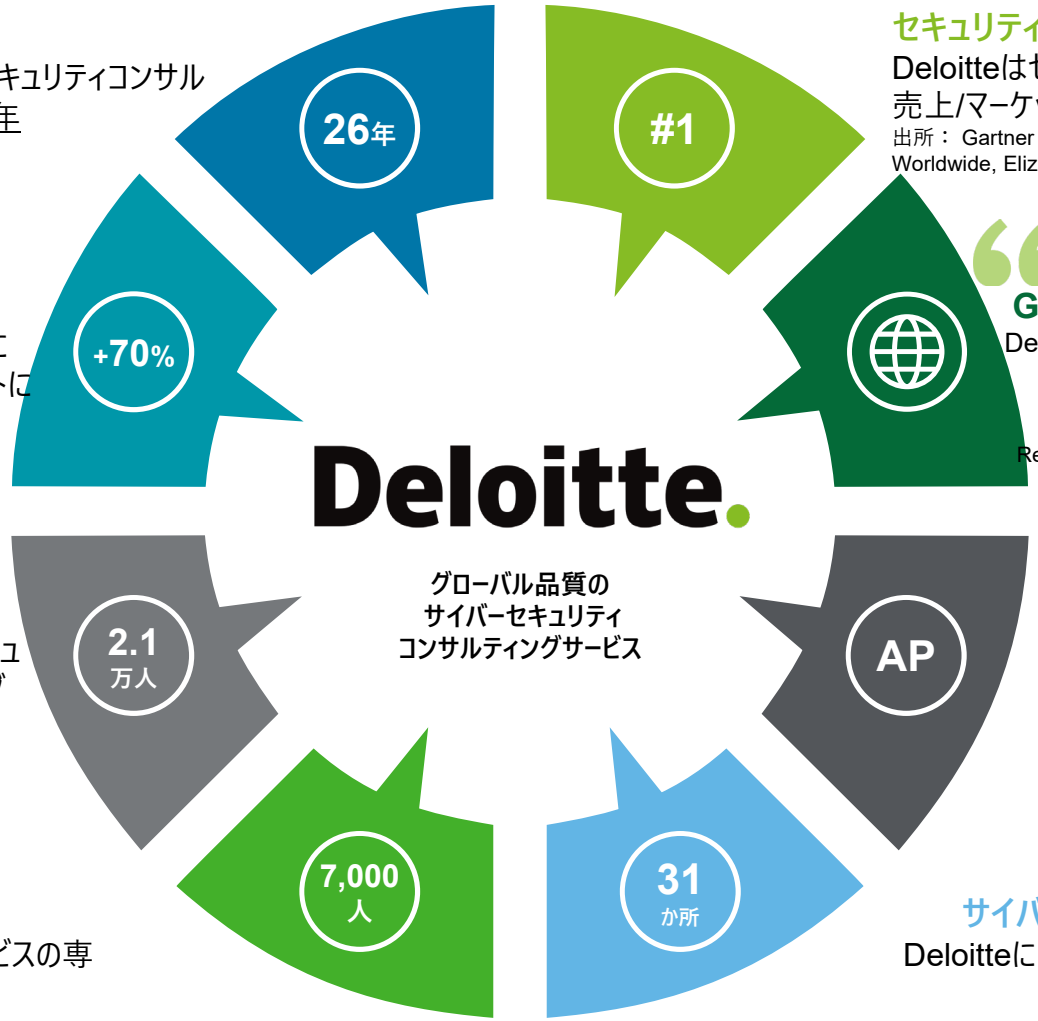
デロイトのケイパビリティと評価

サイバーサービス提供実績年数
Deloitteはクライアントにサイバーセキュリティコンサルティングサービスを提供し始めて26年

Fortune Global 500
DeloitteはFortune Global 500に選出された70%以上のクライアントに対しアドバイザリーを実施

プロフェッショナル
Deloitteはリスク管理/サイバーセキュリティに関するプロフェッショナルがグローバルで21,000人

サイバーセキュリティ専任者
Deloitteはサイバーセキュリティサービスの専任者がグローバルで7,000人



セキュリティ コンサルティング サービス
Deloitteはセキュリティ コンサルティングサービスの売上/マーケットシェアが世界No.1
出所： Gartner： Market Share ：Security Consulting Services, Worldwide, Elizabeth Kim, April 2022

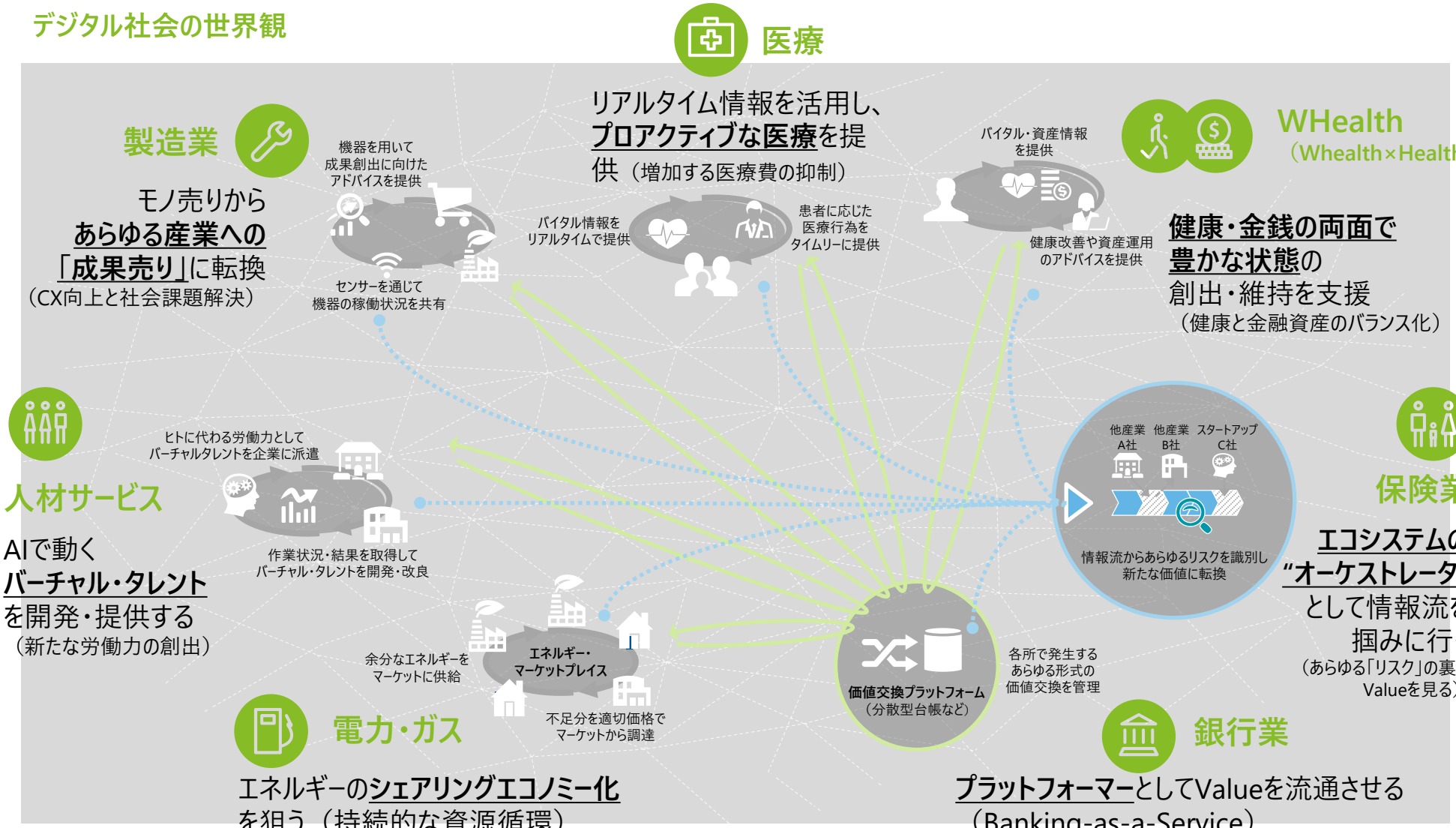
Global:インシデント対応サービス
Deloitteは世界のインシデント対応サービスのリーダーとして評価
出所: IDC MarketScape
IDC MarketScape: Worldwide Incident Readiness Services 2021 Vendor Assessment"
November 2021

Asia Pacific: クラウドセキュリティサービス
Deloitteはクラウドセキュリティサービスのリーダーとして評価
出所: IDC MarketScape
"IDC MarketScape：Asia / Pacific Cloud Security Services 2021 Vendor Assessment Study" Jun 2021

サイバーインテリジェンスセンター(CIC)
Deloitteには24/365でセキュリティ監視を行うセンターがグローバルに31か所

転換期を迎えるサイバーセキュリティ動向

デジタル化の進展に伴い情報流通が飛躍的に広がっていく世界観のもと、各産業の在り様が大きく変わる中、サイバーセキュリティがその成否を左右する最重要テーマになっている



※ 様々な産業の「Industry Vision」に関する論文・レポートをもとにデロイト トーマツ作成

サイバーセキュリティ環境は著しい変化を続けており、経営者には明確なリーダーシップの発揮が求められている

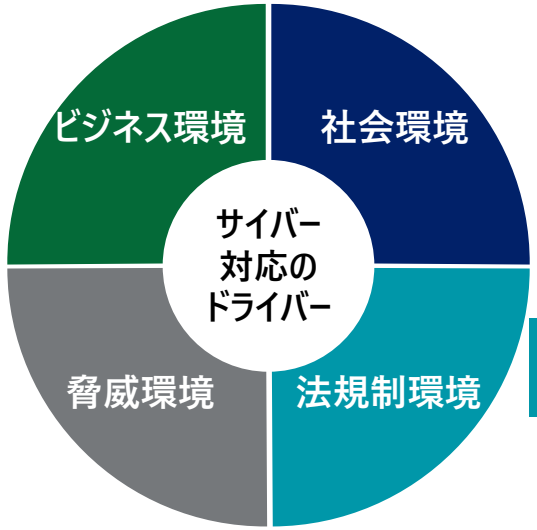
サイバー経営に求められる視点

デジタル化・働き方・生活の変化

- デジタル変革
- 繋がる社会の進展
- グローバル競争の進展・事業再編の進展
- New Normalによる環境変化

国民・資本市場からの期待値の変化

- サイバーセキュリティの社会課題化
- 電子政府・デジタル庁の設立への期待
- 投資家のサイバーセキュリティへの関心（企業価値への直接的な影響）
- ESGフレームワークへの追加



サイバー攻撃の増加・被害深刻化

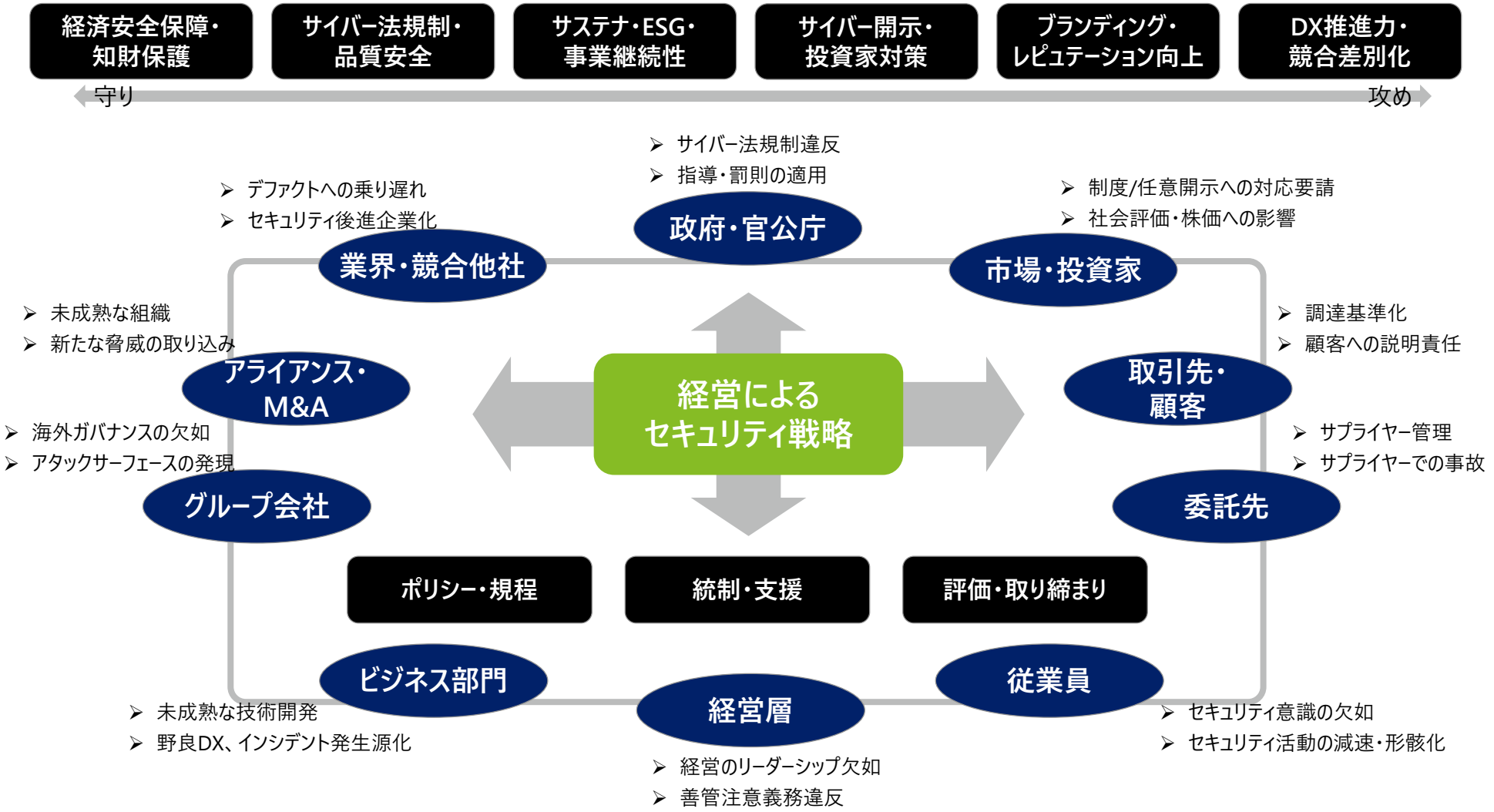
- サイバー攻撃の増大とビジネス化
- ランサムウェアによる二重恐喝、国家規模の攻撃
- 制御系、IoTシステム・サービスへの攻撃深刻化
- 攻撃による経済的損出の増大化

法規制・ガイドラインの制定・改正

- サイバー法規制・業界ルール・制度
- 企業間での情報管理の厳格化
- サプライチェーンリスクへの対応
- 経済安全保障・競争力強化のためのルール形成

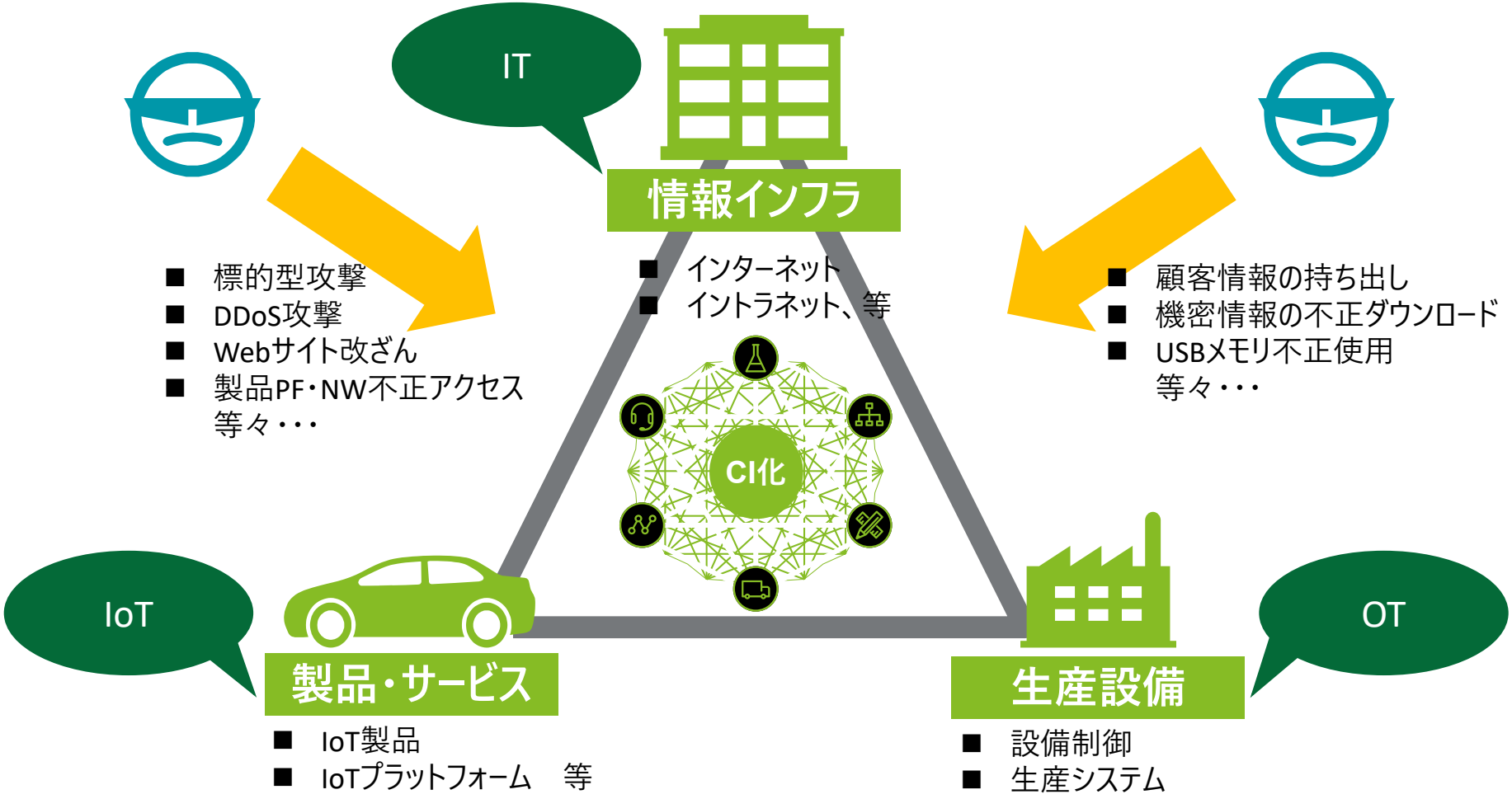
DXに先駆けた企業を中心に、経営目線から守りと攻めのサイバーアジェンダへの取り組みを推進するため、サイバーセキュリティ統括・戦略機能の強化が求められている

サイバー戦略に求められる視点



DXの進展と共にサイバーセキュリティを検討すべき領域は拡大しており、同時に考慮すべきサイバーリスクシナリオも繋がりを増している

企業におけるサイバーセキュリティ検討領域の広がり

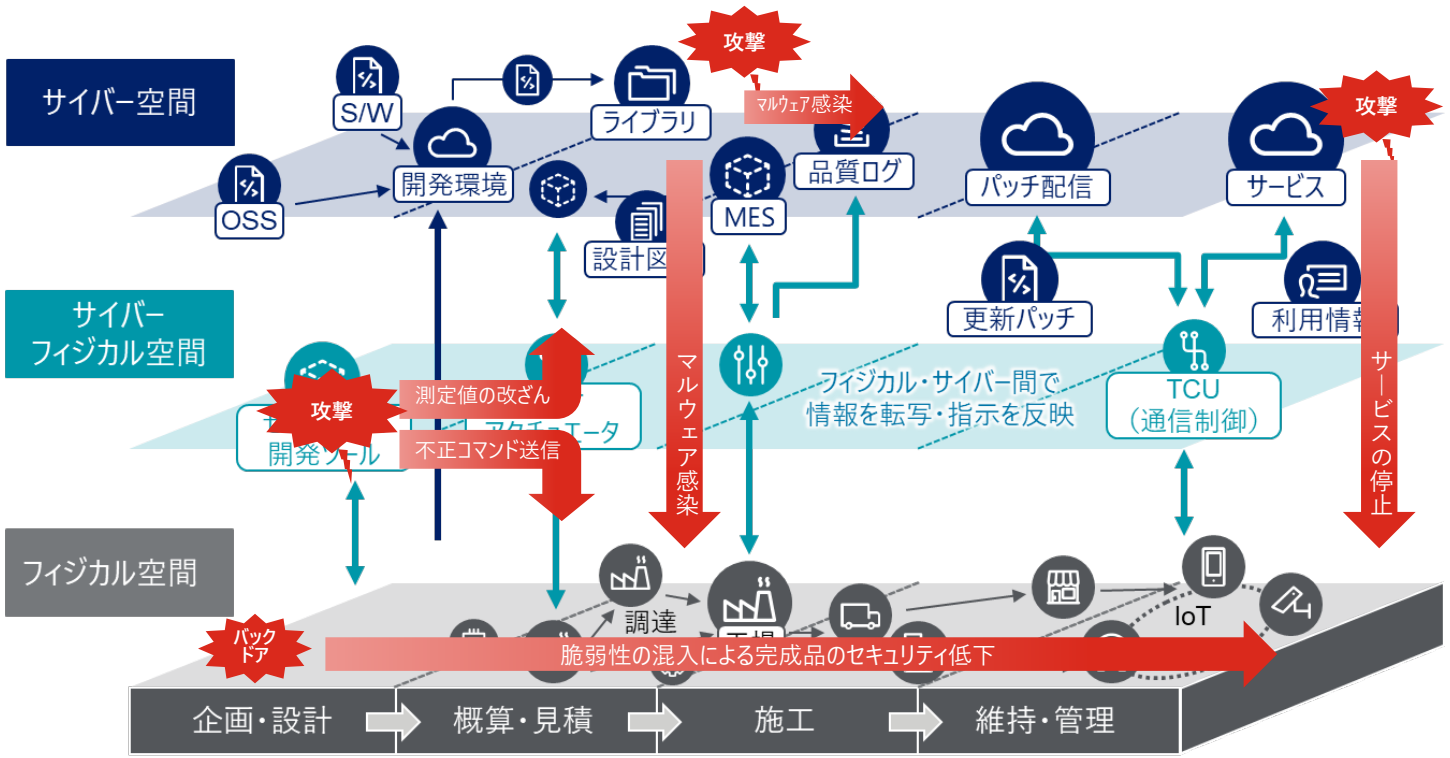


あらゆるモノとデータが繋がることにより、攻撃の起点や攻撃対象が増加するとともに攻撃の経路がより複雑化し、バリューチェーン上のあらゆる空間にサイバーリスクが存在する

サプライチェーンセキュリティに求められるグランドデザイン

- あらゆるモノとデータが繋がることによる、攻撃の起点（アタックサーフェス）の増加と守るべき範囲の急激な拡大
- サイバー攻撃による被害がフィジカル空間に及ぼす影響の増大

DX時代のサイバー脅威（イメージ）



サイバー脅威の例

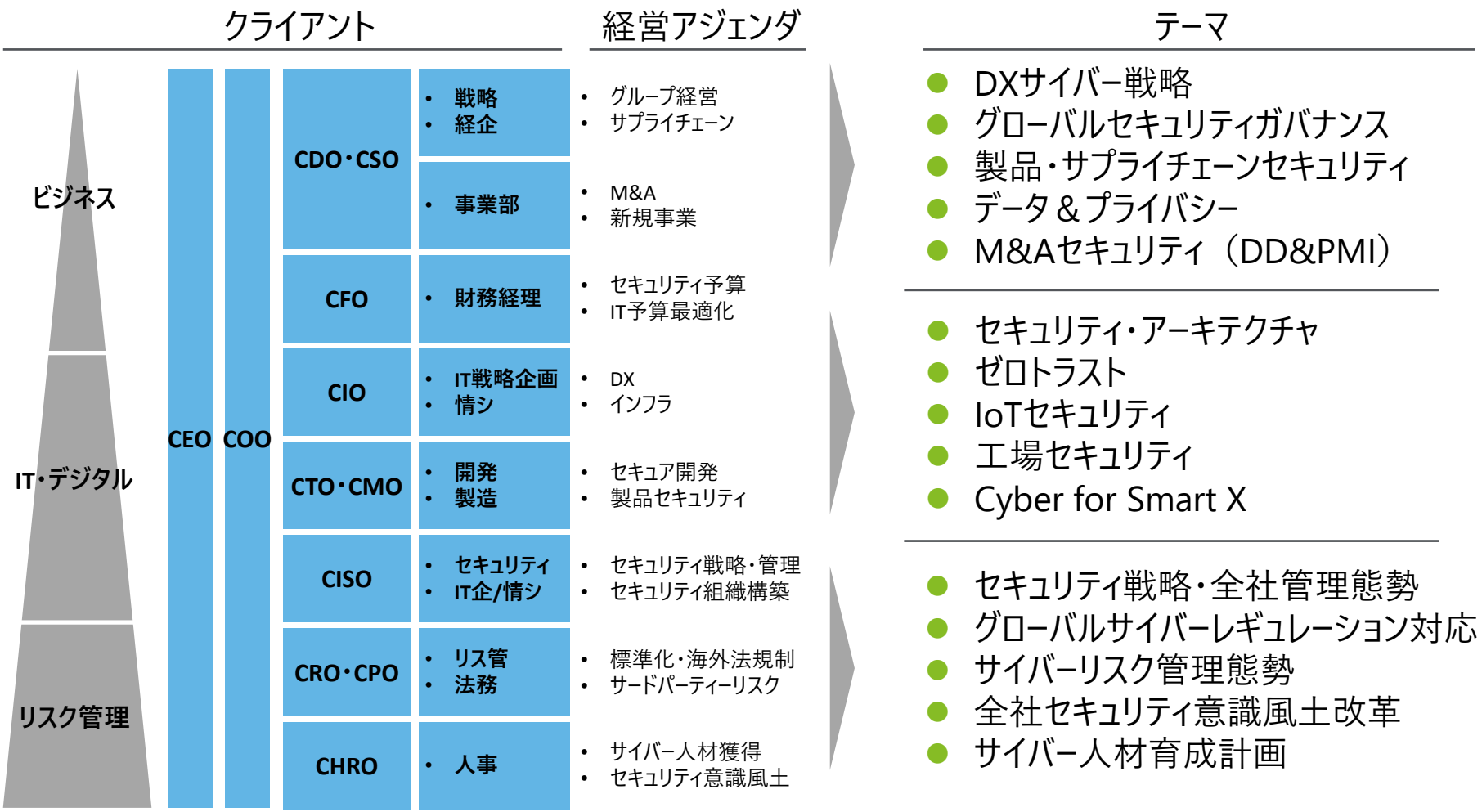
- システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染
- 窃取したID、パスワード等を利用した正規ユーザへのなりすまし
- システムを構成するサーバ等に対するサービス拒否攻撃

- IoT機器を管理するシステムからIoT機器への不正なコマンド送信
- IoTシステムを構成するIoT機器、通信機器等に対するサービス拒否攻撃
- センサーの測定値、閾値、設定の改ざん

- 品質や信頼性の低いIoT機器のネットワーク接続
- 正規の機器を模した偽造品の挿入
- 保護すべきデータの適切でない持出行為

企業のCxOが抱えるサイバーアジェンダの全体像を捉え、戦略×業務、組織×テクノロジー等、最適解を組み合わせたサイバーセキュリティ戦略を企画・実行していくことが重要である

サイバー戦略における経営アジェンダ

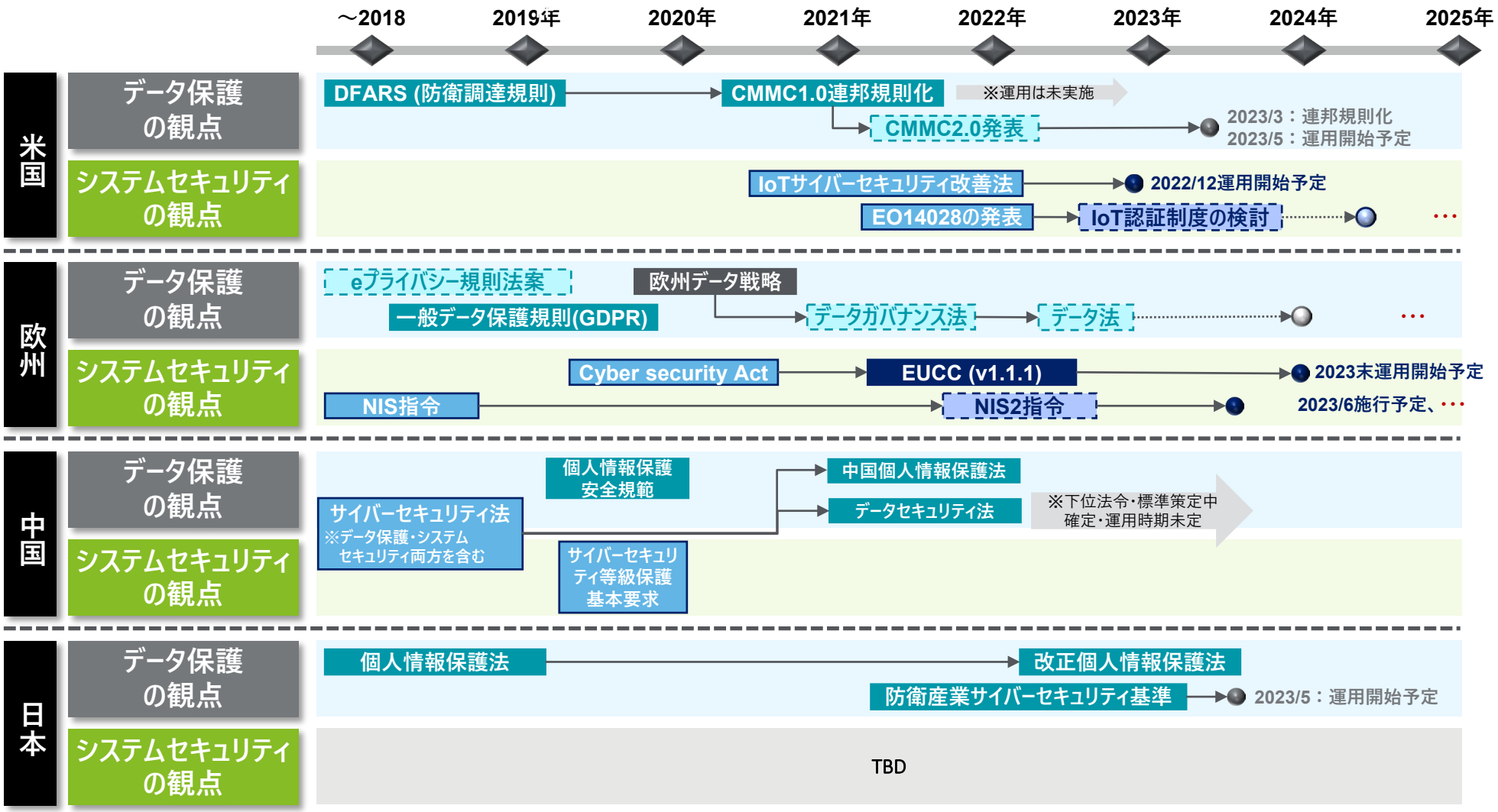


順次適用される規制・標準をギリギリ準拠すると言う姿勢ではなく、他組織に先んじて対応し競争力の源泉とすることがDX時代の勝ち方

各国のサイバー関連法規制動向サマリ

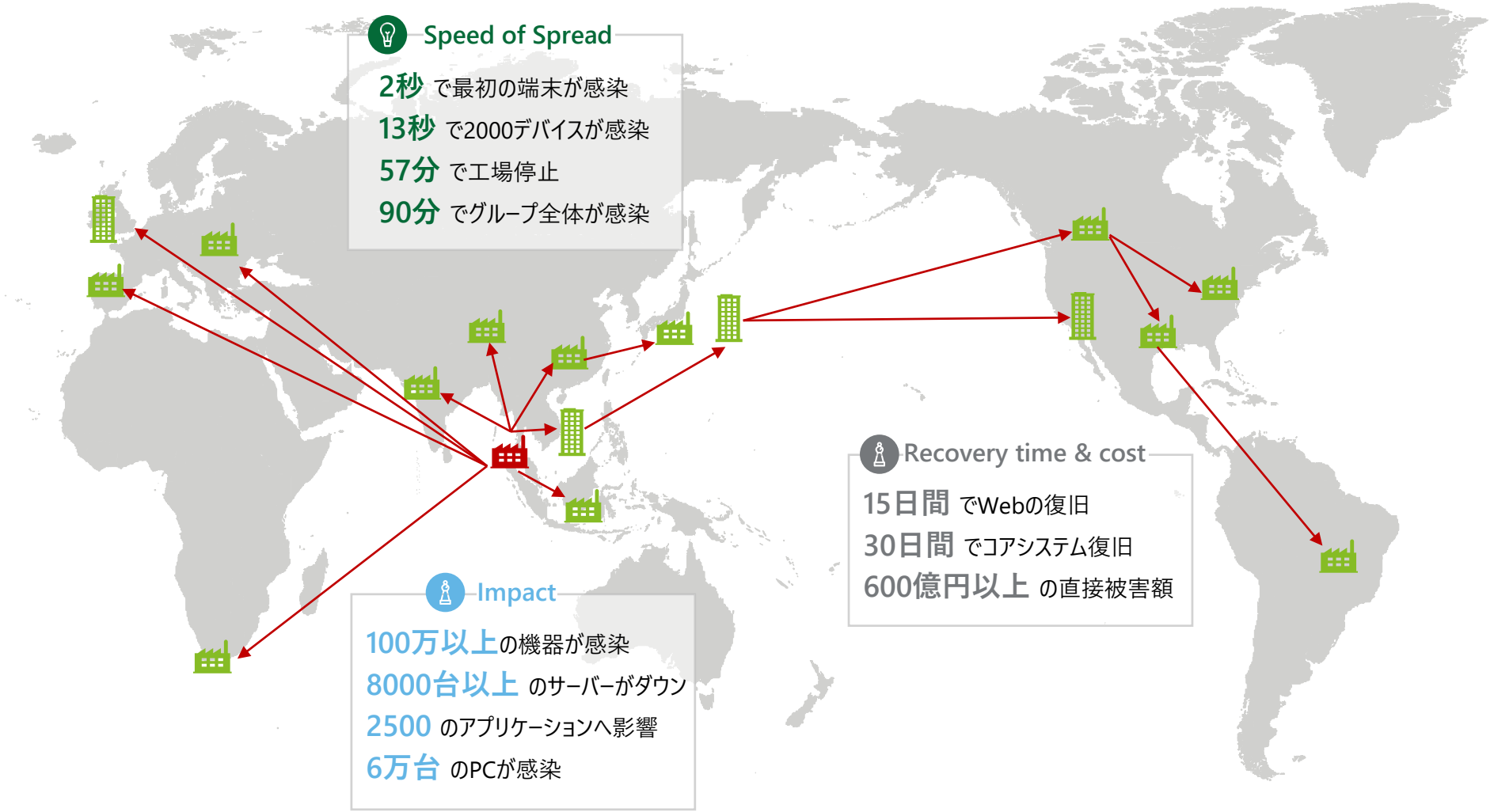
：施行済の法令・制度
：未施行の法令・制度

※2022年4月時点の情報をもとにデロイトトーマツ作成



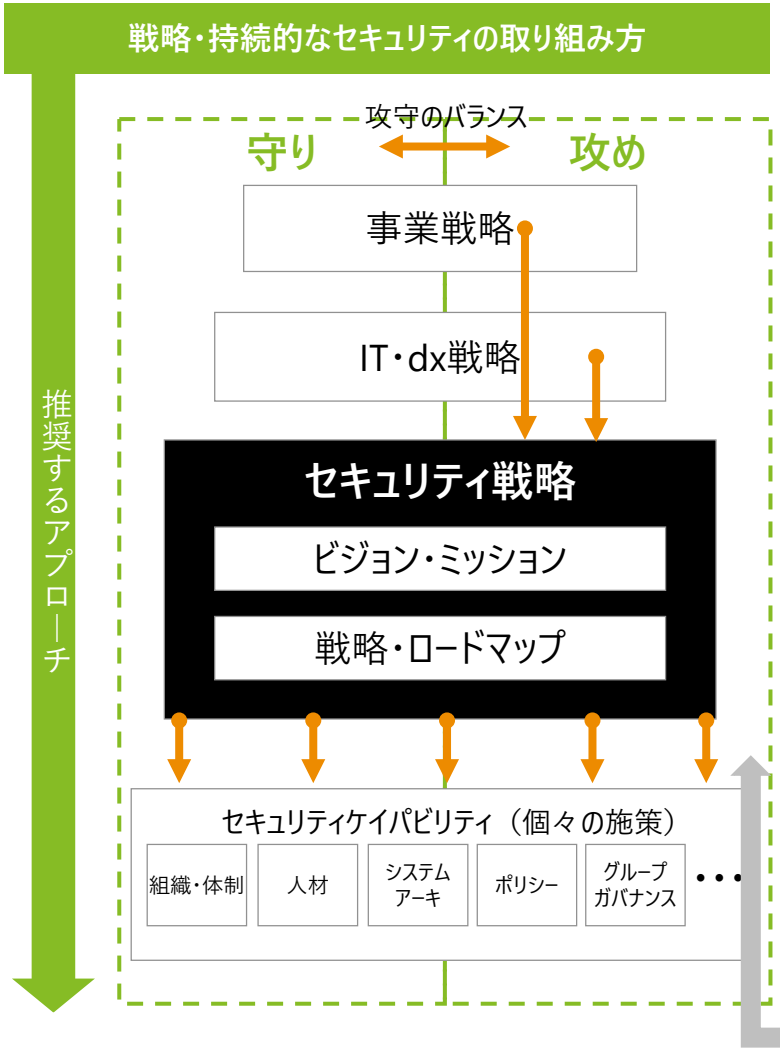
一拠点がサイバー攻撃を受けたとしてもそれがグループ全体やサプライチェーン全体へ瞬時に影響を及ぼす事例も散見される

サプライチェーン全体へのサイバー被害拡大（事例）



戦略的・持続的なサイバー能力強化の取り組みを志向することが、持続的に高度なサイバーセキュリティ能力を獲得・維持するための鍵となる

サイバーセキュリティ戦略の必要性



基本的な戦略

① 経営によるVision/Strategyの検討から着手すべき

個別テーマ毎の点としての対策ではなく、合理的な優先順位に基づく面としての対応の為、中期的な活動基準となるセキュリティVisionとその実現に向けたセキュリティStrategy策定から検討する

② 「守り」だけでなく「攻め」も志向したサイバー組織・体制の構築

単なる防衛としての情報セキュリティだけでなく、企業全体および事業として脅威と守るべきもの、防衛策を明確にし、事業への貢献や、事業における強み創出に向けた検討も含めて行う

③ アセスメントによる自社能力の見極めと経済合理的な中長期ロードマップ

自社に適したフレームワークを用いて現状をアセスメントし、戦略の実行に向けて不足しているCapabilityを洗い出し、ロードマップを策定する

戦略上の要諦

✓ 事業戦略・IT戦略との一貫整合

- 事業戦略・IT戦略をセキュアに実現するための、セキュリティ面での戦略・方針の定義
- 中長期の経営計画におけるデジタル化・ITイノベーション・技術開発等の施策をセキュリティ面から停滞させないための戦略
- 戦略に基づいた、在るべきセキュリティ管理態勢＆システム防護体制のデザイン

✓ 戦略に整合した施策の実行

- 戦略の実現に必要となる個々の施策の明確化、事業・セキュリティ両面からの優先順位の決定
- リソース（人・業務・IT）の識別、将来を見据え強化すべきポイント、方向性の決定
- 戦略実行に向けた関係者間で合意したロードマップの決定

今こそ、企業はこれまでの守り（リスク回避・軽減）の視点でだけでなく、攻め（事業への貢献）としてサプライチェーンを通じたサイバーセキュリティ強化に取り組む必要がある

（参考）攻めのサイバーセキュリティ取り組み事例

目的	直面するセキュリティ課題（弊社仮説）
DX推進のための投資	■ DXは事業変革において最も重要なドライバーとして捉えられており、日系企業の大多数がDXに着手済み、または着手予定 ■ DX推進において「サイバーセキュリティ」は「投資コスト」、「人材不足」とともに3大課題の一つとCxOには認識されている ■ 上記背景を踏まえ、サイバーセキュリティ対策を事業成長のドライバー（DX推進のための投資）と捉えだしている
製品・サービス品質の向上	■ DXにおいては、フィジカル空間、サイバー空間をより一層融合させ、製品・サービスの付加価値を向上させることが重要 ■ サイバーセキュリティ対策を製品・サービス品質の重要な要素、研究・開発投資の一部と捉え、サイバーセキュリティ対策を促進 ■ 最終製品・サービスの品質を担保するためサプライチェーン全体のセキュリティ対策を進める政府機関・企業も出てきている
既存ビジネスの差別化施策	■ サイバーセキュリティ対策を調達基準に入れる政府機関・企業が増えている ■ ISO、NIST等の標準化団体、業界団体からは、サプライチェーンセキュリティに対する要請が高まっており、法規制化の動きもみられる ■ 既存ビジネスを維持・拡大するための差別化施策としてサイバーセキュリティ対策を進める企業が増えてきている

サイバーアジェンダ

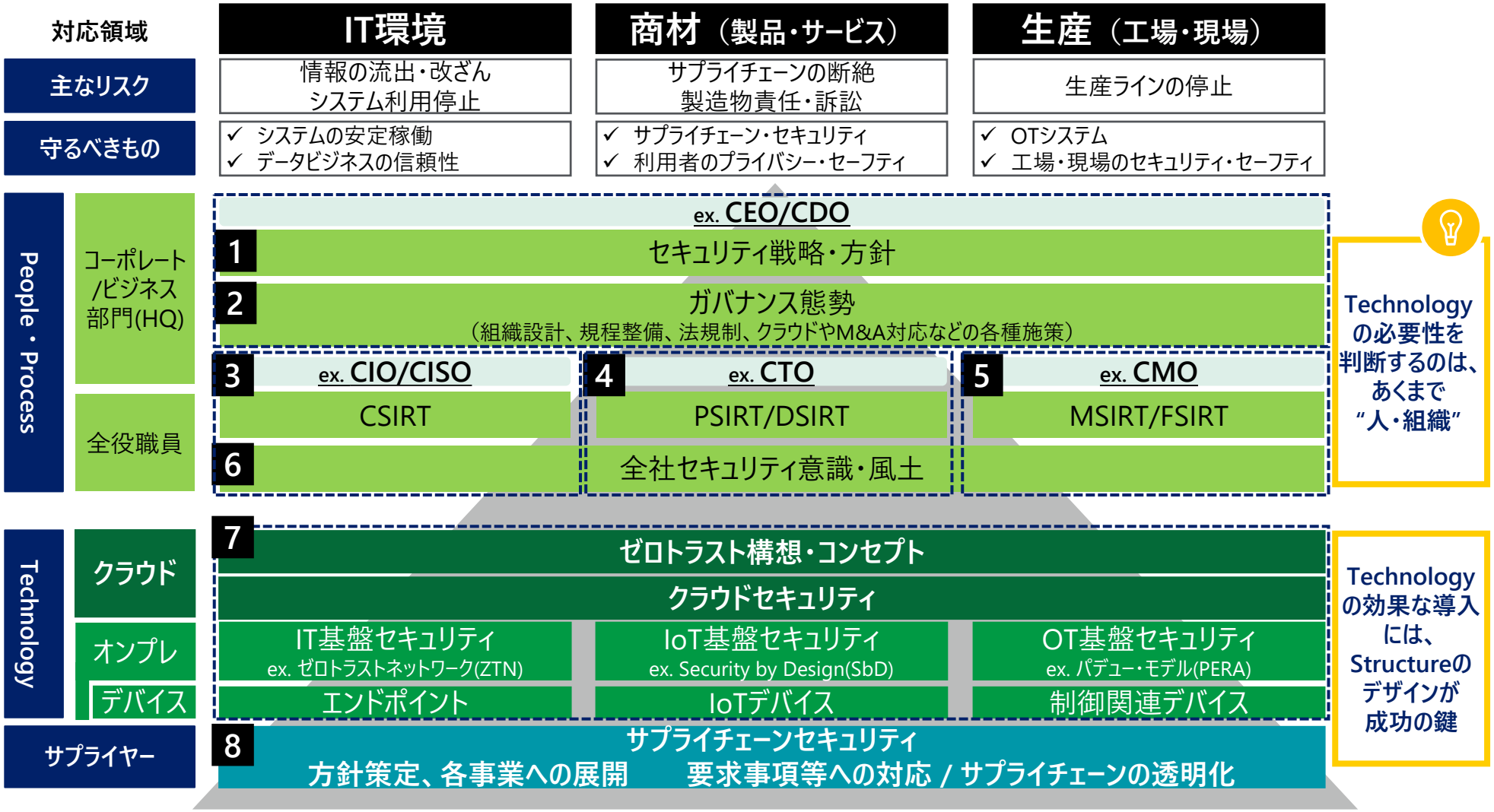
- クラウドセキュリティ戦略・ポリシー
- データ利活用と保護の全体方針
- 攻めと守りのプライバシー戦略
- 製品・サービスセキュリティ戦略
- サプライチェーンセキュリティ
- Security by Designの実現
- グローバルセキュリティガバナンス

→ DXと連動した「ビジネス適合型」のサイバーセキュリティ戦略の実現

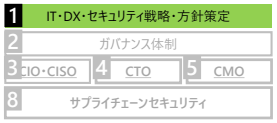
サイバーセキュリティ戦略の要諦

DX時代の企業は、自社を取り巻くサイバー脅威、守るべき領域を見極めた上で、自社のCybersecurity Structureを確立する必要がある

DXに求められるサイバーセキュリティ管理態勢の全体像

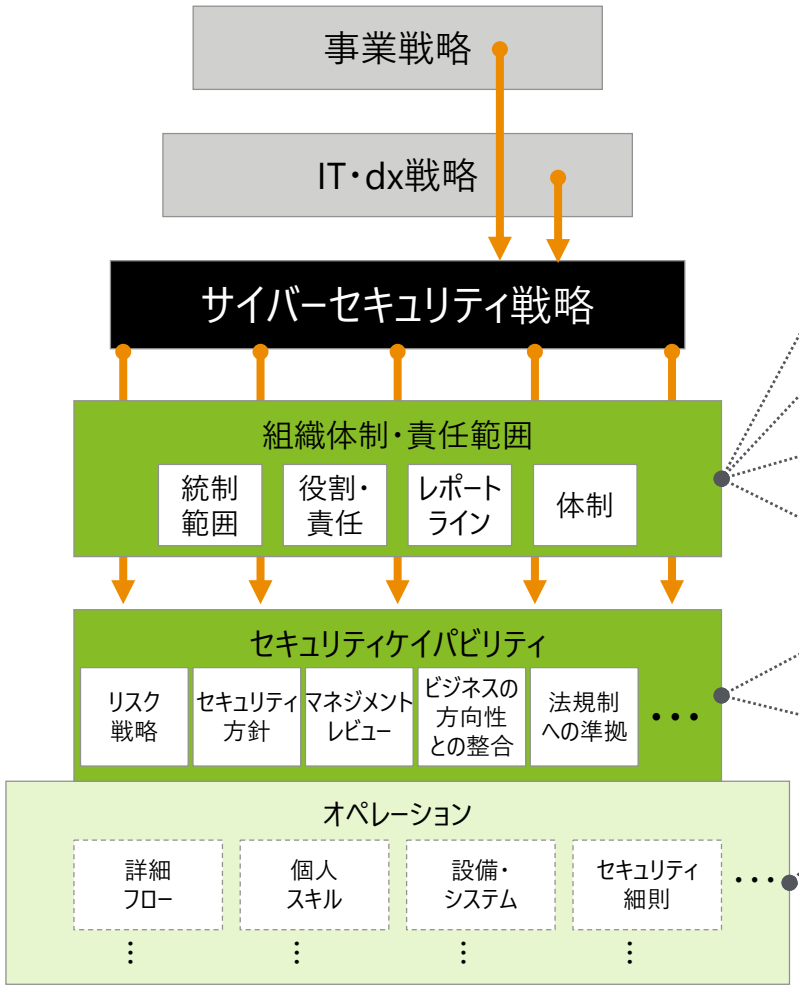


あるべき管理態勢検討にあたっては、貴社の事業・戦略といった目的達成のための次の論点を設定し、To-Beの管理態勢（機能・組織・業務等）を検討する



在るべきセキュリティ管理態勢の検討論点イメージ

検討の全体像



あるべきセキュリティ管理態勢の検討論点（例）

A セキュリティ組織の位置づけ・責任範囲・セキュリティ機能間での連携

セキュリティ戦略方向性およびセキュリティ機能配置が効果的に機能する様、セキュリティ組織の位置づけや責任範囲、セキュリティ機能（情セキ・工場・製品）間での関係を検討　※具体的には、**CISO配下に紐づく機能など**をハイレベルに整理

B コーポレート、事業側の役割

セキュリティ管理機能に係るコーポレート側と事業側の座組（役割分担）をどうするか
※具体的には、**セキュリティ推進（管理・運用）に係るそれぞれの機能の分担**の考え方など

C セキュリティのガバナンス・マネジメント・実行機能の配置

セキュリティを機能させる**3層のガバナンス・マネジメント・実行機能について、具体的にどのような配置**を考慮すべきか
特に、貴社固有の入り組んだ事業・地域の組織構造なども踏まえ、検討

D 海外含めたグループセキュリティガバナンスのあり方

事業領域・地域特性・地域事業会社の特性などを踏まえたうえで、本社機能がガバナンスを効かせる幅、深さ、そのやり方などを検討
特に、**貴社のISのガバナンスの強弱などの実態も踏まえた考え方、あり方**を検討

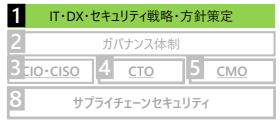
E 必要セキュリティ管理機能と配置

セキュリティ戦略方向性を踏まえた際に考慮すべき必要セキュリティ機能と、貴社における**事業戦略・IT戦略を踏まえたうえでの、セキュリティ機能のあるべき配置**を検討

F 現実的なオペレーティングモデル

セキュリティ実行機能、特に今回移行が検討されるSOCや製品選定などの機能における**現実的なオペレーティングモデル**（機能配置、組織体制、運用モデル）について検討

サイバーセキュリティ管理態勢全体を経営目線からハイレベルに分析し、リスクが高い領域を可視化すると共に、重点領域対しては詳細分析を行うアプローチが有効である



サイバーセキュリティ管理態勢の全体像（デロイトのサイバーフレームワーク）

※ ISO27002や NIST CSFに基づき体系的にセキュリティ要件が整理

CYBER STRATEGY & TRANSFORMATION(戦略)

サイバーセキュリティ管理

- 戦略と運用モデル
- ポリシー、標準、アーキテクチャ
- サイバーリスクの文化と行動
- サイバーリスクの管理、指標、報告
- クラウドセキュリティ
- 外部委託先のリスク管理

SECURE(予防)

情報保護

- 情報の分類
- データプライバシー
- 情報のライフサイクル管理
- 情報の漏洩・流出の防止
- 暗号化
- エンドユーザのデバイスセキュリティ
- 人材に関するセキュリティ対策

アプリケーション保護

- セキュアSDLC(セキュアソフトウェア開発ライフサイクル)
- 開発後のアプリケーション保護

インフラストラクチャ保護

- アセット管理
- ネットワークセキュリティ
- システムセキュリティ
- マルウェアからの保護
- パッチおよび脆弱性管理
- 物理的セキュリティ

ID&アクセス管理

- IDのライフサイクル管理
- ユーザーアクセスコントロール
- 役割ベースのアクセス制御
- 特権ユーザのアクセス制御

VIGILANT(発見)

脅威管理

- サイバー脅威インテリジェンス
- ペネトレーションテストおよび脆弱性スキャン
- ブランド保護

セキュリティアナリティクス

- サイバーアナリティクス
- セキュリティプラットフォームの管理および運用
- セキュリティイベント監視

RESILIENT(回復)

インシデント管理

- インシデントへの対応
- インシデントおよび危機への対応状況
- 事業継続管理（BCP）および回復

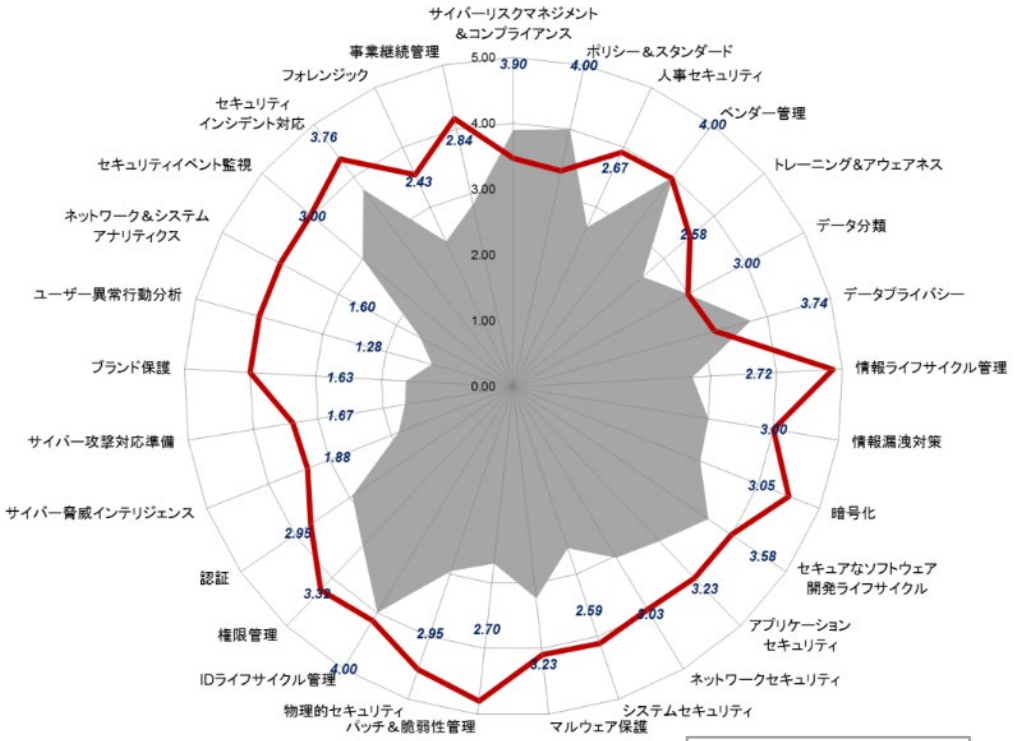
Deloitteのセキュリティアセスメントフレームワークを活用して現状のCapabilityを網羅的に可視化し、その後の改善につなげる

1 IT・DX・セキュリティ戦略・方針策定
2 ガバナンス体制
3 CIO・CISO　4 CTO　5 CMO
8 サプライチェーンセキュリティ

セキュリティアセスメント (Full Assessment)

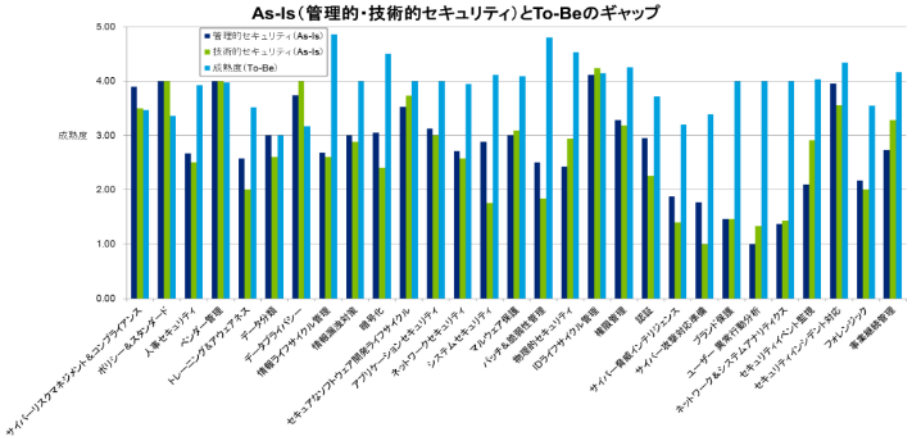
成熟度結果（As-IsとTo-Beの可視化）

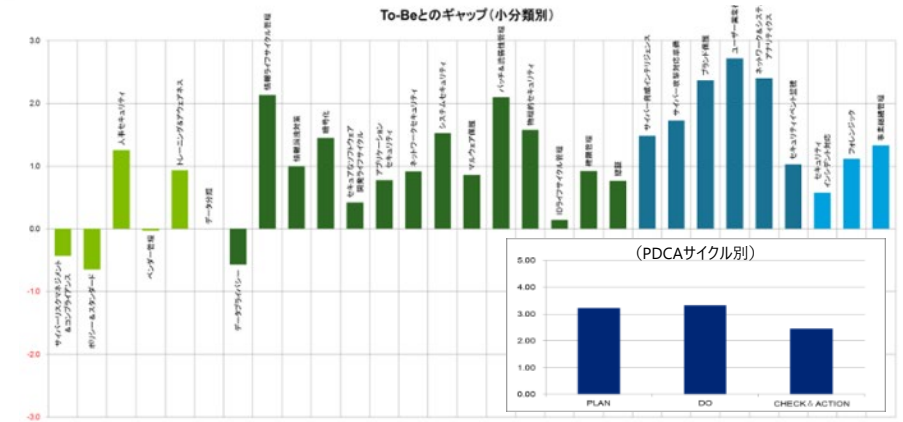
➢ 一目でわかる視認性の高いグラフ・図表等で整理



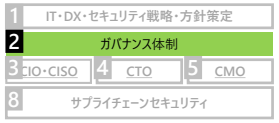
観点ごとの達成レベル

➢ 多様な視点から、分析結果を提示することが可能



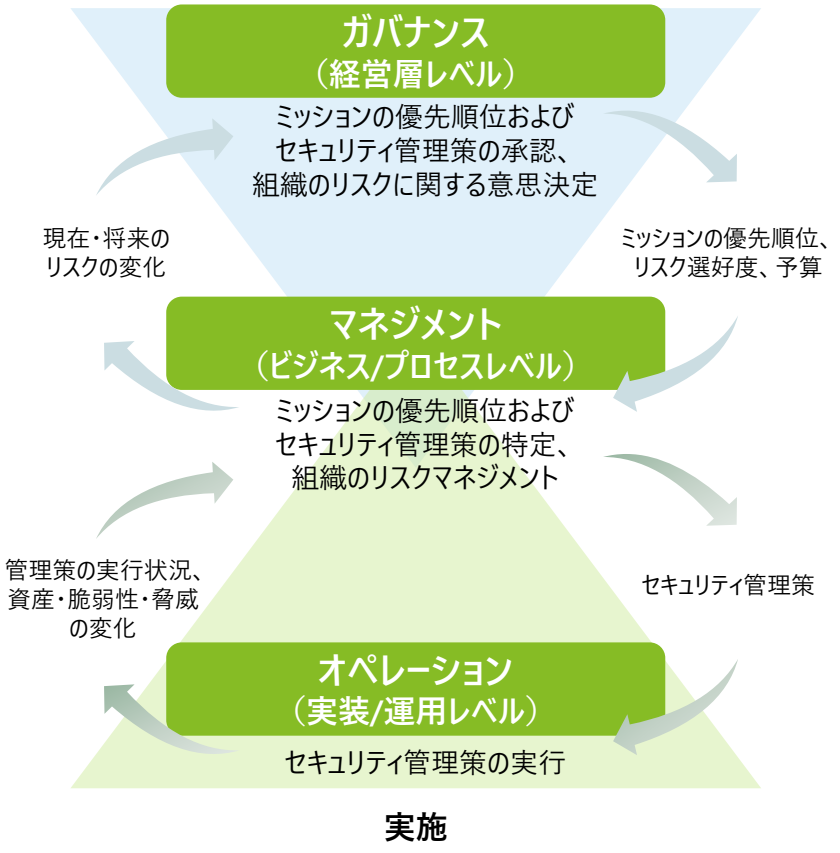


グローバルスタンダードであるNISTのサイバーセキュリティフレームワーク（CSF）に準拠したサイバー戦略・サイバーセキュリティ態勢が求められる



NIST Cybersecurity Frameworkにおける5機能の定義

必要となる組織構造



NIST CSF 1.1版よりデロイトトーマツ作成

求められる能力

サイバー攻撃

➢ 多層的なセキュリティ対策の必要性から「特定」・「防御」・「検知」・「対応」・「復旧」の5つのセキュリティ機能を定義

特定 / Identify	組織がサイバーセキュリティについての理解を深め、情報資産（情報システム・データ）、ガバナンス、ビジネス、委託先などに対するセキュリティリスクを管理
防御 / Protect	特定したリスクに対して、アクセス制御、データ保護、セキュリティトレーニングなどの防御策を導入
検知 / Detect	セキュリティイベントが発生したことを検知するためのセキュリティ機器の導入やモニタリング・検知プロセスを構築
対応 / Respond	検知したセキュリティインシデントに対して処置するために必要なプロセスを構築
復旧 / Recover	レジリエンスを担保する計画を維持し、サイバーセキュリティインシデントによる影響で障害を受けていた機能やサービスを回復するために必要なプロセスを構築

侵入前

侵入後

対策（例）

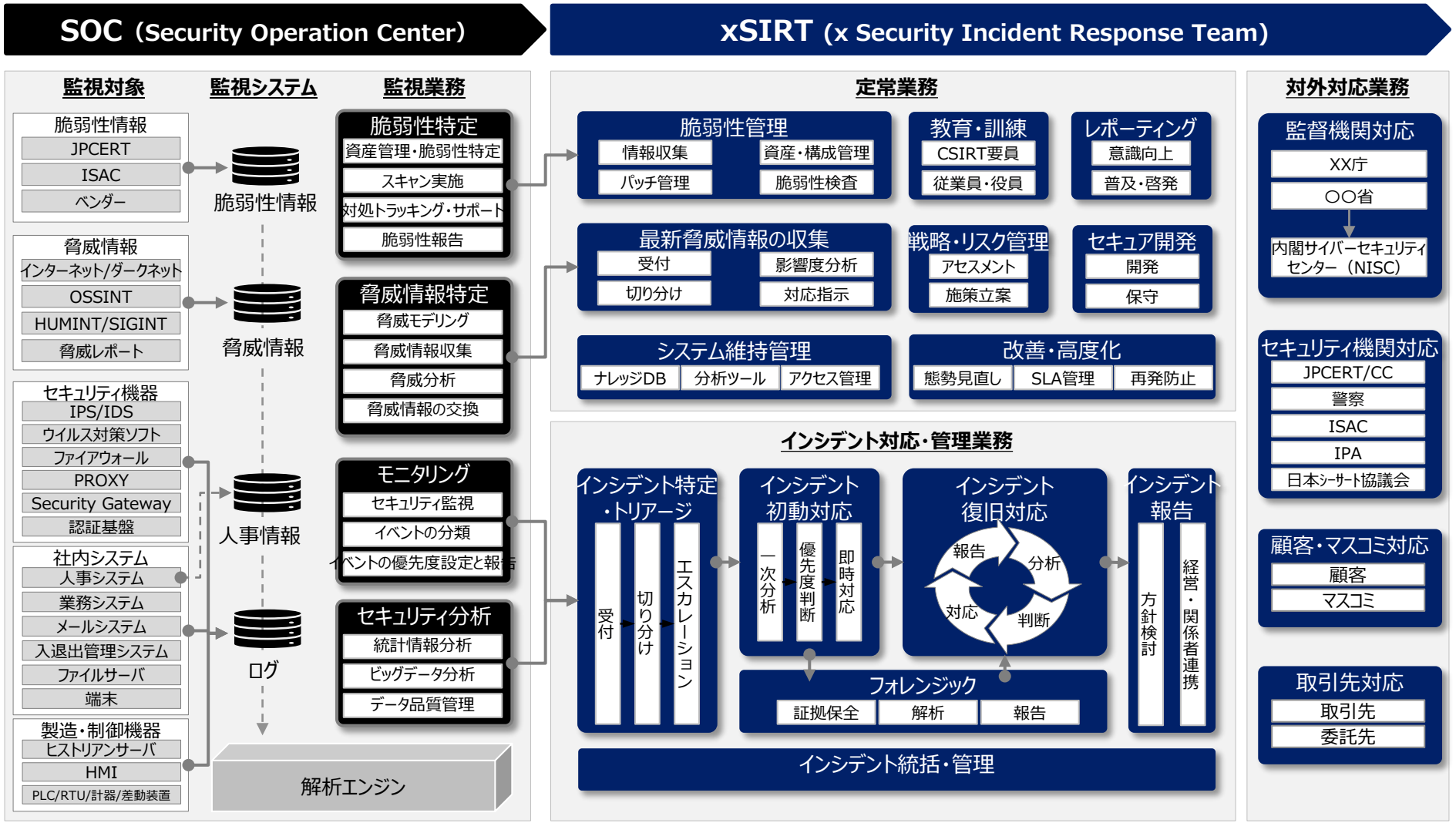
技術	管理
• アクセス制御 • 構成管理 • 識別及び認証 • メンテナンス • 物理的環境セキュリティ • システム及び通信の保護 • システム及び情報の完全性	• 意識向上及びトレーニング • 監査及び責任追跡性 • インシデントレスポンス • 記憶媒体の保護 • 人的セキュリティ • リスクアセスメント • 承認・運用認可 • セキュリティ評価

• • •

実効性あるインシデント対応態勢とは、インシデント対応に関連する一連の業務が明確化され、それぞれの有機的な連携性が維持・自律的に高度化される状態を指す

1 IT・DX・セキュリティ戦略・方針策定
2 ガバナンス体制
3 CIO・CISO　4 CTO　5 CMO
8 サプライチェーンセキュリティ

在るべきインシデント対応態勢の全体像



企業を取り巻く環境変化に伴い、サプライチェーンセキュリティの“在り方”を転換すべきタイミングを迎えており、単なるセキュリティリスクではなく「経営リスク」として捉えた組織全体での対応が求められる

サプライチェーンセキュリティの転換期

事業環境

デジタルサプライチェーンへの進化

新たな価値創出やプロセス合理化等を目的に、製品・サービスが消費者に届くまでの一連の生産・流通プロセスのデジタル化が加速

① 「ツリー型」から「メッシュ型」へ
② 流れる対象が「モノ」から「情報・データ」及び「ソフトウェア」にまで拡大

脅威環境

サプライチェーン攻撃に対する被害の深刻化

各サードパーティとのサイバー空間上での繋がりの拡大に伴うアタックサーフェスの増加、サードパーティ・ソフトウェアの脆弱性に起因する自社製品・サービスへの影響など

脅威（例）

- **脅威事例①：遠隔監視ツール攻撃(2020年)**
  マルウェアが仕込まれた遠隔監視ツールの更新機能により、約17,000社にマルウェアが侵入
- **脅威事例②：自動車メーカー攻撃(2022年)**
  受発注サーバがマルウェアに感染した影響で、自動車メーカーの工場・ラインの生産が停止

法規制環境

サプライチェーン全体の保護を目的としたサイバー法規制化が活発化

サードパーティをを含めたセキュリティ強化が“強制力”を伴う形で企業に要請されつつある
※サプライチェーン全体でのソフトウェア管理(SBOM管理)の法規制化も進んでいる

法規制（例）

- **米国：CMMC***
  国防総省とビジネス関係にある全企業に対して第三者評価機関からの認証取得を強制化
- **欧州：NIS 2 Directive (NIS2指令)**
  重要インフラ全体のセキュリティ強化を目的に、NIS指令を改正

サプライチェーンセキュリティの“在り方”を転換すべきタイミングを迎えており、単なるセキュリティリスクではなく「経営リスク」として捉えた組織全体での対応が求められる

*：CMMC (Cybersecurity Maturity Model Certification)

サイバーレジリエンスの要諦

日本企業においてもランサムウェアによる被害が深刻化している

日本におけるランサムウェア被害事例

「前例ない」大規模攻撃　大量データ暗号化　起動不能、バックアップもダメで「復旧困難」

■ 業種：製造業
■ インシデント発生時期：2021年7月
■ 概要
- グループ会社を含むサーバの大半が同時攻撃を受け、バックアップを含む大量のデータが暗号化された
- システムの起動そのものが不可能で、データ復旧の手段はなかった。外部専門家に「前例のない規模」と報告を受けた
- 財務システムも被害を受け、早期復旧が困難なため、決算を3か月延期。四半期報告書の提出も3か月延期する事態となった

ランサム攻撃で電子カルテ暗号化　病院、インフラ打撃

■ 業種：総合病院
■ インシデント発生時期：2021年10月
■ 概要
- 命を守る地域の重要インフラである病院をサイバー攻撃が襲った
- 病院のシステムに侵入し情報を暗号化し、復旧と引き換えに金銭を要求するコンピュータウィルス「ランサムウェア」に感染した
- 約8万5千人分の電子カルテが閲覧できなくなり新規患者の受け入れを停止

ランサムウエア攻撃により取引先の国内全工場停止

■ 業種：自動車部品メーカー
■ インシデント発生時期：2022年2月
■ 概要
- サーバーが1台ダウンしたこと影響範囲の特定などのため、稼働する社内サーバーをいったん全て停止した
- 取引先も国内のすべての工場の稼働を停止する事態となった

2 重恐喝型ランサムウェアへの対応は容易ではない

2 重恐喝型ランサムウェアの実例

※殆どのケースは英文で記載されている

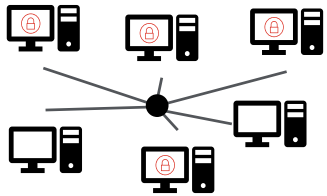
発覚

従業員

情報を窃取しデータを暗号化した
暗号化を解除したければ身代金を支払え
身代金を払わなければ窃取した情報をリークするぞ

社内調査

システム担当者



基幹系システムを含む多くの業務システムが利用不可
バックアップも暗号化され復旧も困難

ファイルサーバー等も被害を受けており
大量の個人情報・機密情報が窃取された可能性あり

危機対応

トップマネジメント

どのように被害を食い止めれば良いのか？

システム復旧のために身代金は支払うべきか？

対外公表はいつまでにどこにすれば良いのか？

業務再開時のセキュリティ強化はどこまですべきか？

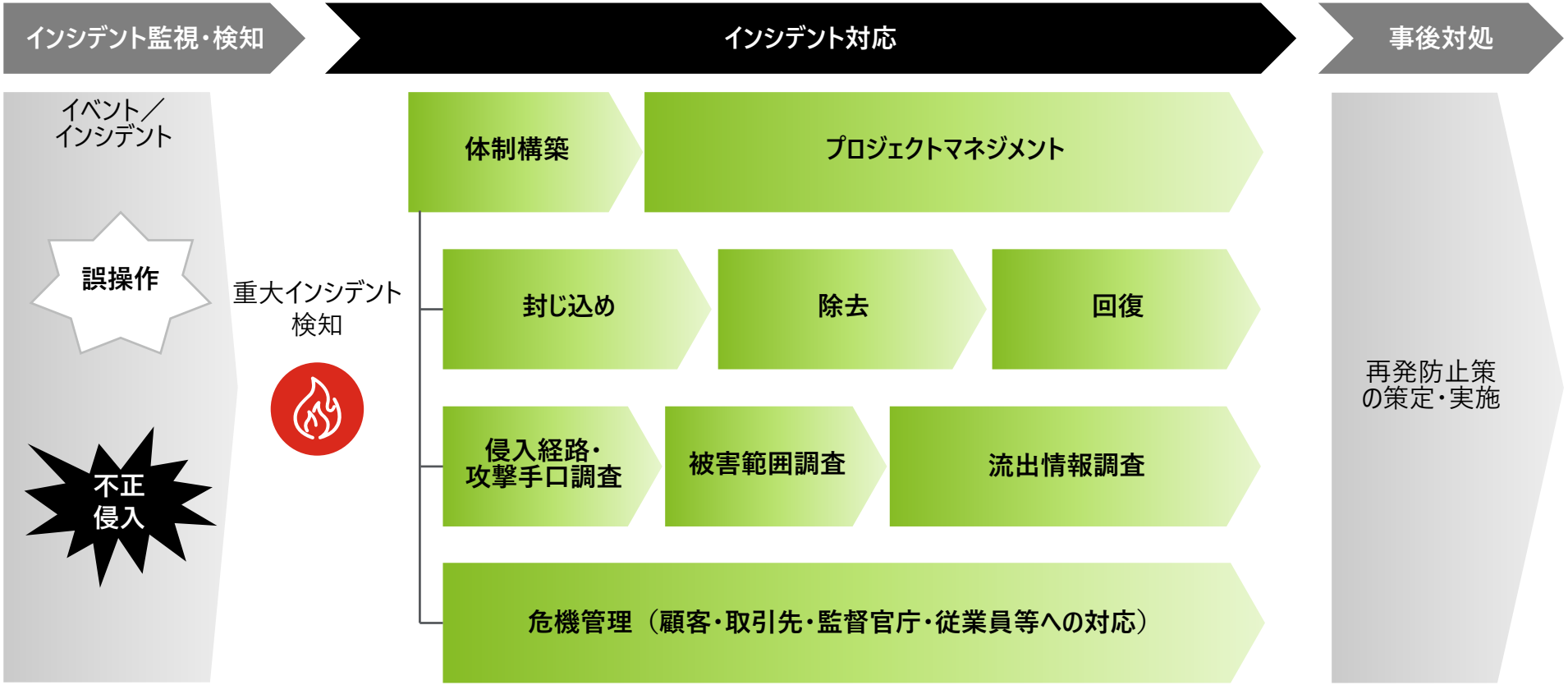
サイバーインシデント対応の現場では以下のような失敗が頻発している

インシデント対応の失敗事例

- *攻撃者が密かに潜伏している可能性への対応が不充分なままシステム利用を再開してしまう*
- *データ保全をする前にシステム回復をしてしまい調査に必要なログが消失してしまう*
- *調査により侵入経路・攻撃手口・被害範囲が特定できず、再侵入や２次被害の抑止が困難になる*
- *情報連携が上手くいっておらず、情報収集に時間がかかる、現場に指示が上手く伝わらない、取引先等への対応がバラバラになるなどの問題が多数生じる*
- *インシデント対応の全体を俯瞰した作業計画が立てられておらず、場当たり的な対応をしている*
- *外部専門家の協力は得ているもののサイバーインシデント対応が上手くいっていないなど*

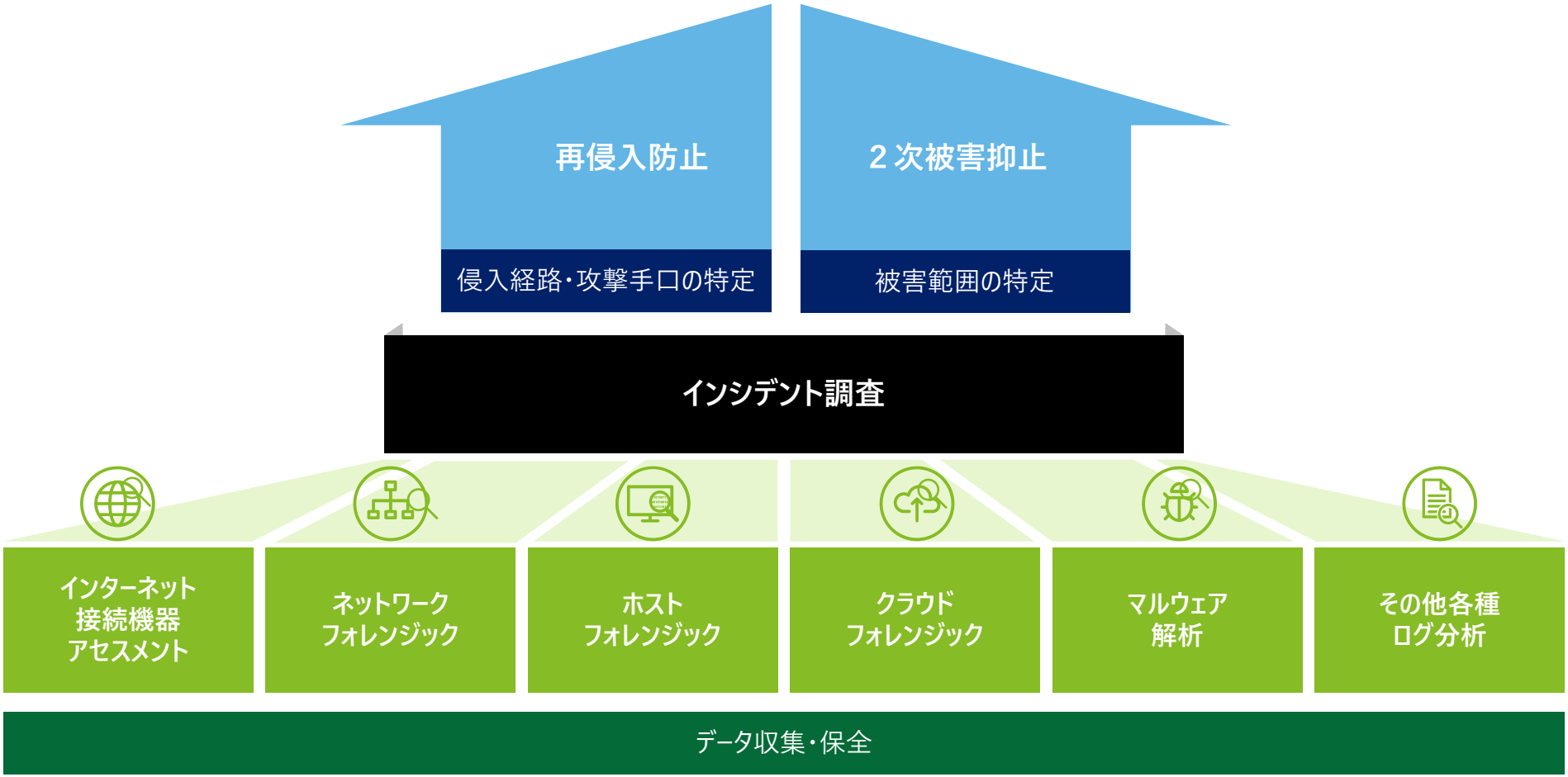
重大なサイバーインシデントは、危機対応としてトップマネジメントがリードしていくことが求められている

重大なサイバーインシデントへの対応



インシデント調査はインシデント対応の基盤である

インシデント調査の重要性



ステークホルダー対応はインシデント対応の成否に大きく影響を及ぼす

危機管理の重要性

社内

- 社内コミュニケーションプラン策定
  - 経営トップによる従業員へのメッセージ発信
  - 対外対応窓口の一本化
  - 事案公表前の従業員への伝達など

メディア

- 公表方針の検討
  - 公表レベルの検討（法定開示事項／重要度／緊急度）
  - 公表方法の検討（記者会見開催、プレスリリース、HP掲載）など
- 公表内容の特定
  - 公表すべき内容の整理
  - 公表のタイミング決定など
- 公表の準備
  - リリース
  - ポジションペーパー
  - 記者会見リハーサルなど
- メディアモニタリング
  - 報道、SNSの分析など

顧客・取引先・官公庁等

- ステークホルダーの特定
  - 影響を与え得るステークホルダーの洗い出し
- ステークホルダー対応策の検討
  - 対応の優先順位検討
  - ステークホルダー別対応の整理
  - ステークホルダーへのメッセージ作成
  - ステークホルダーの反応分析など
- 必要資料の作成
  - リリース、お詫び文、報告書等など
- インフラ整備
  - コールセンター等の運営
  - 情報のエスカレーションなど

インシデント対応の全体をコントロールするプロジェクトマネジメントがインシデント対応の成否の鍵を握る

プロジェクトマネジメントの重要性

- 膨大なタスクの計画・管理
- 関係者からの情報収集・整理
- トップマネジメントへの報告
  トップマネジメントからの指示への対応
- 社内外の情報統制
- 外部協力者との調整・管理

サイバーセキュリティ戦略の要諦（後半）

グループを取り巻く内外のセキュリティ環境の変化に伴い、画一的なグループセキュリティガバナンスは限界を迎えており、「ビジネス適合型」のセキュリティガバナンスへの転換が必要である

グループセキュリティガバナンス強化の必要性

外部環境

■ 顧客・市場等からのセキュリティ要請の複雑化

✓ 地域や事業の観点においてセキュリティ要請が多様化する中で、要請に"グループ全体"として十分に応えることが出来ない場合、今まで以上に市場からの信頼低下や事業機会の損失に影響する恐れ

■ サイバー攻撃の巧妙化・高度化

✓ 自社に関わる至る所が攻撃対象となるため、末端組織とも連携した組織大でのセキュリティの取組みが必要

内部環境

■ 新たな価値創出を目的としたビジネスの多角化

✓ ニーズの多様化・複雑化への対応として、従来のビジネスに加え、デジタルを活用した様々なビジネスを付加

✓ 専門性が高く機動力のあるスタートアップ企業の買収等の加速により、グループ各社の組織規模・事業内容・文化等の違いがより顕著に

今後のグループセキュリティガバナンスに必要となる観点

ビジネスを守る	● グループ全体で調和された合理的なサイバーリスク管理やセキュリティ対策が必要
ビジネスに貢献する	● 加速するビジネスの足枷にならず、事業のDX活性化・イノベーション創出に貢献する"ビジネス適合型"のセキュリティへの転換が必要 ● サイバーセキュリティに係るグループ全体でのインテリジェンス共有・相互活用などにより、ビジネスを支えることが必要

「事業を守る」・「事業に貢献する」という視点を踏まえ、本社が“統制役”としてグループ全体を管理・監督しつつ、グループ会社のセキュリティ推進を“支える”メカニズムを構築することが重要である

グループセキュリティガバナンス強化のポイント

①体制

本社が“統制役”としてグループ全体を管理・監督

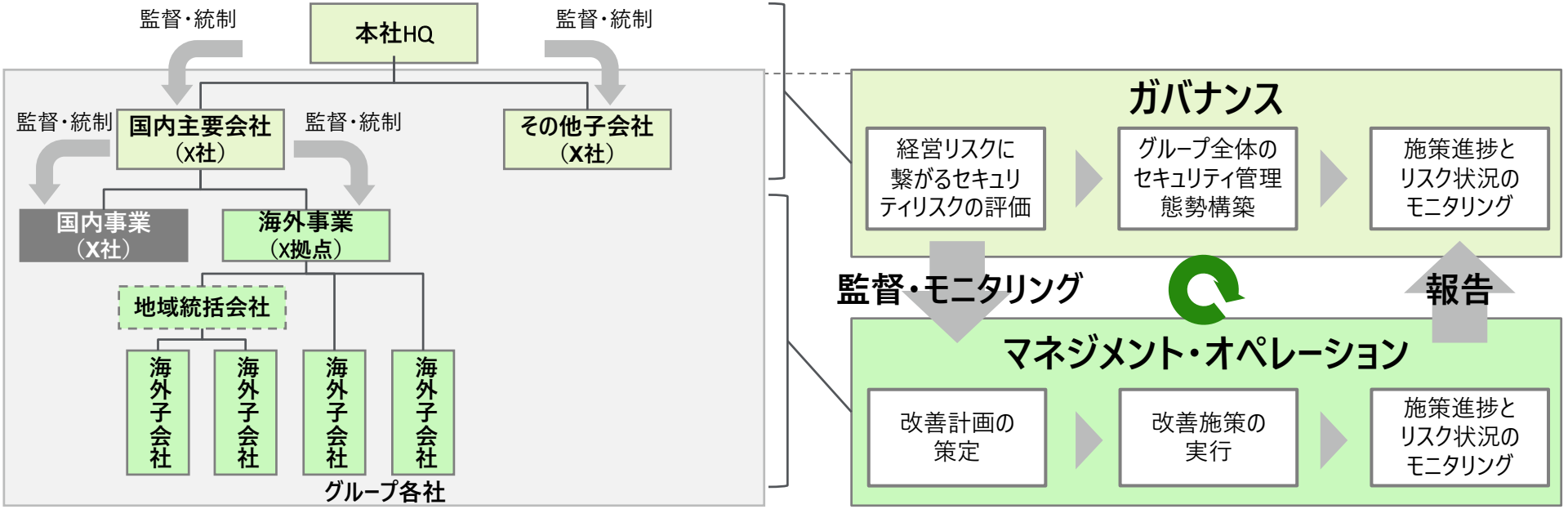
✓ グループ会社を多数抱える大企業においては、グループ**各社のリスク状況・インシデントの把握が難しくなる**ため**情報連携を確実に行える管理体制が必須**

②メカニズム

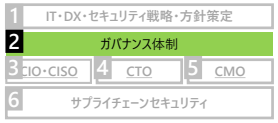
セキュリティ前線化を“支える”仕組みの構築

✓ デジタルビジネスの加速に伴い、**事業側へのセキュリティの前線化**が必要

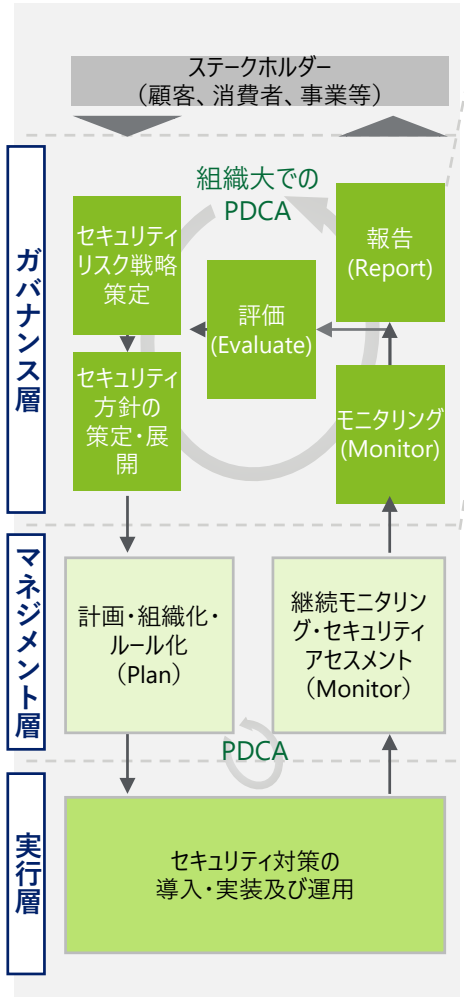
✓ 各グループ会社による**マネジメント・オペレーションを本社が支援**する仕組みが必要



大規模かつ複雑な構造の組織では、中間部分の機能を階層に分けて機能設計し、ガバナンスにグリップを効かせることが成功要因となる



セキュリティガバナンスの構造



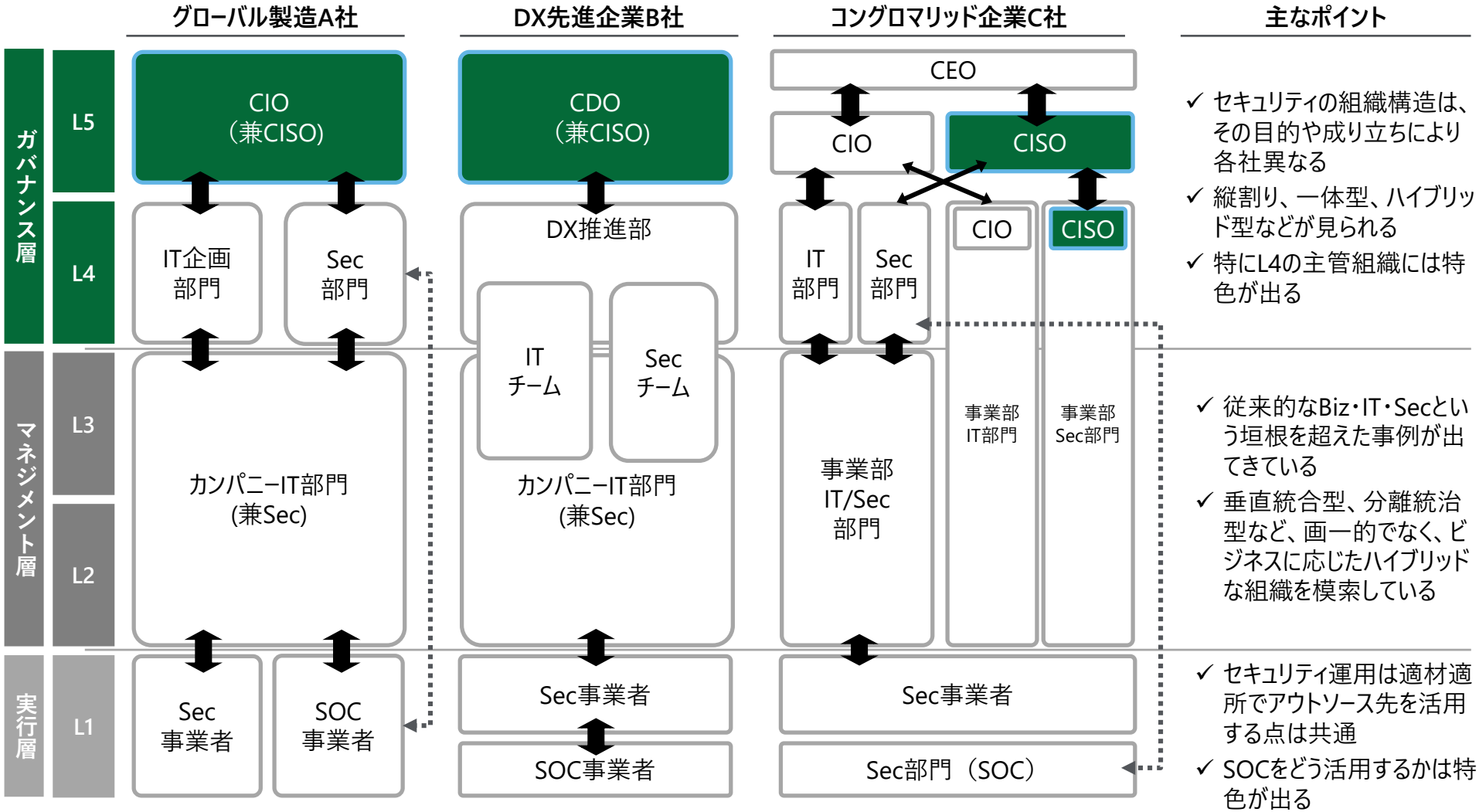
	在るべき構造	ガバナンス階層と機能配置	セキュリティ戦略実行上の課題（例）	主管組織・担当
ガバナンス層		L5 経営陣を含んだリスクコミュニケーションに基づく経営による方向付けと全社モニタリング セキュリティ戦略策定 / ビジョン・ミッション策定 / セキュリティ投資意思決定 / ステークホルダーへの報告	✓ 経営会議・取締役会等の場でセキュリティを議論する場が必要であることを経営層が管理層に求める ✓ 管理層から提言された計画の承認、結果の評価を行う	➢ CxO ➢ 経営会議・取締役会
		L4 全社セキュリティ統括組織による方向付けとモニタリング・評価 企画・ロードマップ策定 / 全社ポリシー策定 / セキュリティ投資計画 / 事業部モニタリング・評価	✓ 事業戦略に紐づくセキュリティ戦略を策定し、投資計画・ロードマップの経営層承認を得る ✓ 管理層・事業部門に戦略を伝達する ✓ 戦略に沿った施策を評価し経営層に報告する	➢ 全社IT/Sec統括組織 ➢ 全社リスク統括組織
マネジメント層		L3 事業部門別の特性に応じたルール策定およびモニタリング セキュリティ組織設計 / 部門ポリシー・ガイドライン / 管理プロセス設計 / 部門モニタリング・評価	✓ セキュリティ戦略・ロードマップを元に具体的な実行計画を策定する ✓ 事業部門への影響を検証し、対応を含めて伝達する	➢ カンパニー/事業本部 ➢ IT/リスク管理組織
		L2 事業部門管轄の個社によるマネジメント 各部ガイドライン・手順設計 / 各部モニタリング・評価 投資先によるマネジメント 各部ガイドライン・手順設計 / 各部モニタリング・評価	✓ ロードマップと実行計画の整合性を評価するための管理(進捗状況、課題による影響等の観点) ✓ 事業部門からの要望や問合せへの対応、現場への伝達・協議と事業部門を巻き込んだ解決策の検討	➢ 各事業部 ➢ IT/セキュリティ管理担当
実行層		L1 対策の導入・実装および運用 ツール導入 / 監視・対応 ・・・ ツール導入 / 監視・対応	✓ 日常の運用から想定外、対策外の脅威が生じた際の報告形態を定め、実施する ✓ 脆弱性情報や他社情報を収集し、組織のセキュリティに懸念を及ぼす情報を報告する	➢ 各事業部 IT/Sec担当 ➢ IT/Secベンダー

illustrative

役割及び責任を抜け漏れ・重複無く整理することが重要

セキュリティ管理体制は各社異なり、事業に求められる法規制や現組織が組成された経緯などを踏まえて構築している

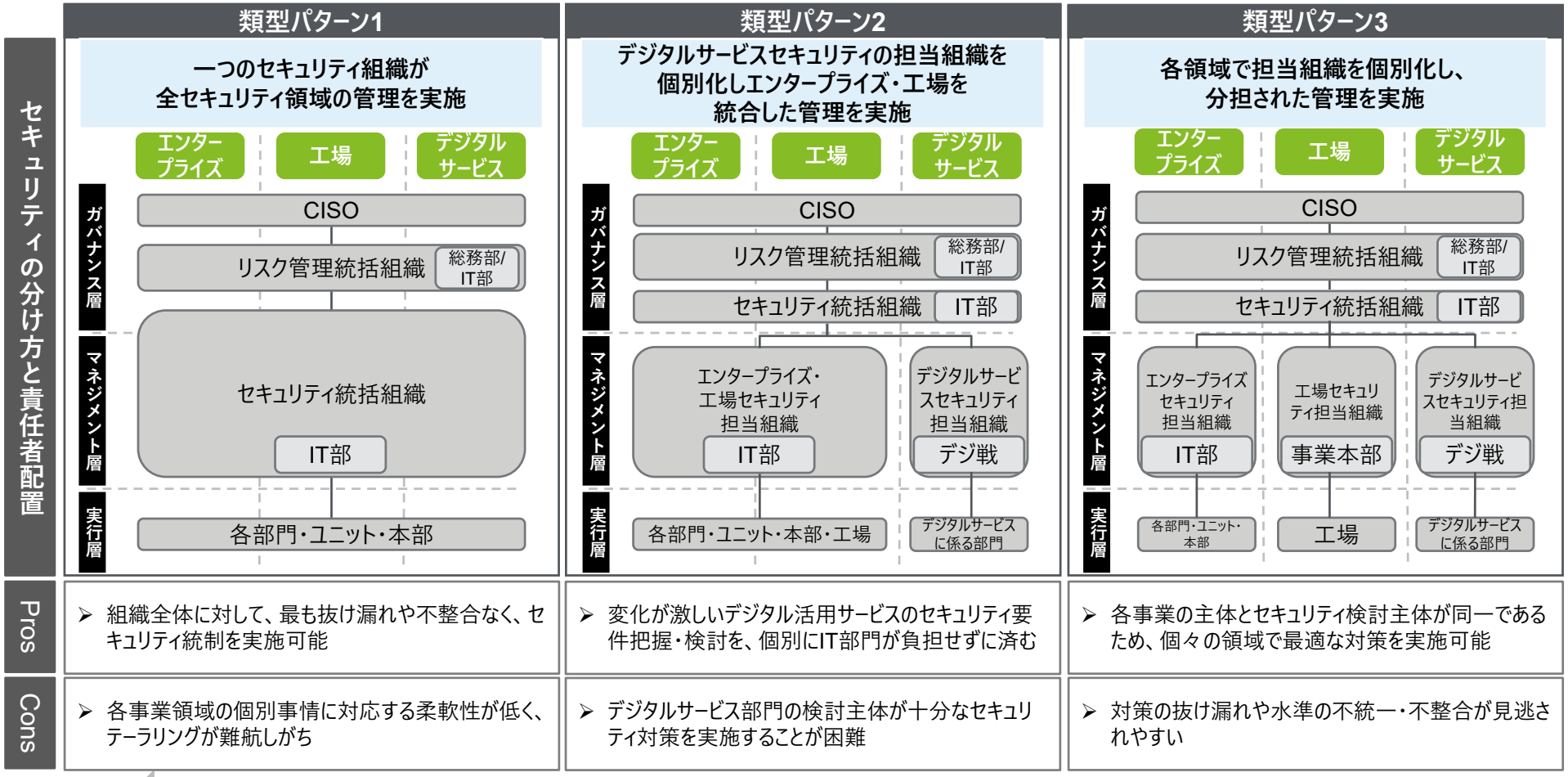
セキュリティガバナンスの構造（事例紹介）



自社のガバナンスモデルをどう定義するかについては、企業の成り立ちや文化風土、事業構造を十分に理解した上で検討する必要がある

セキュリティガバナンス構築（類型パターン）

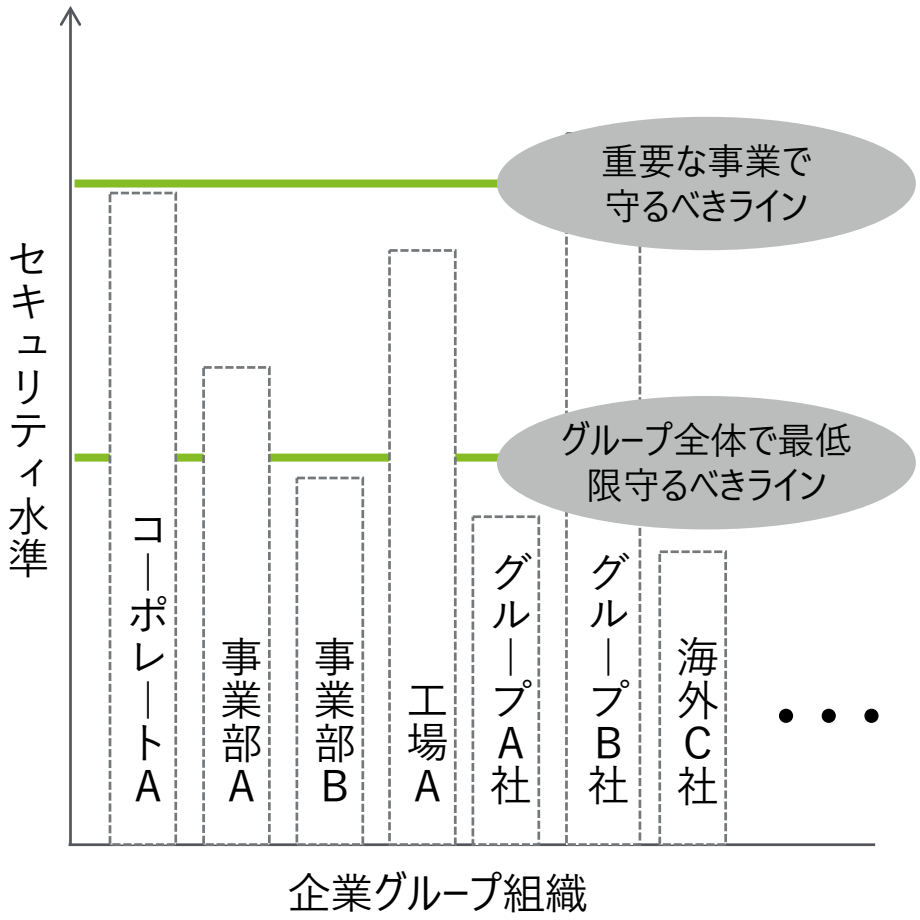
凡例　担当部署(想定)



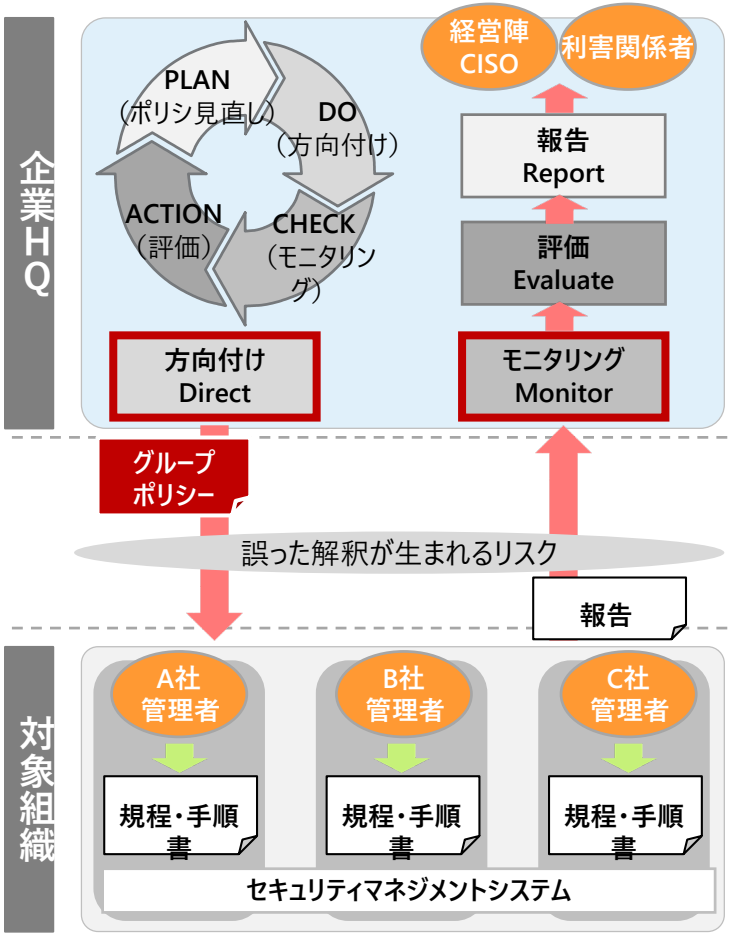
グループ全体におけるセキュリティガバナンスにあたっては、各社固有のリスク状況を踏まえ、グループ大での統制の幅と深さを検討の上、適切なガバナンスの型を適用していく事が肝要

グローバルセキュリティガバナンスの課題感

2階建ての議論



グループセキュリティガバナンスの構造



ガバナンスモデル

- ✓様々な特性を持つグループ会社に対して、一律の水準適用は困難
- ✓ポリシー運用のためのPDCAサイクルを整備し、セキュリティガバナンスを継続的に運営すること

グループポリシー

- ✓適用されたグループポリシーが、意図した目的や要件を満たして、誤解なく解釈される必要がある
- ✓展開されたグループポリシーに対して、個社に応じたセキュリティ・ルールを整備すること

ビジネス環境については、事業特性・システム特性・保有情報の3つの観点で各事業を分析し、在るべきセキュリティ態勢検討のインプットとする

Step.1 ビジネス環境の分析

Ⅰ 事業特性
- 売上・利益等の財務情報
- 事業のIT・デジタル依存性
- 事業の公益性、消費者への影響業務関与者、外部依存性
- 販売国、拠点数　等

✖

Ⅱ システム特性
- インターネットへの接続点・方法
- 保有システム数　等

✖

Ⅲ 保有情報
- 保有情報資産の性質（営業秘密、個人情報、パーソナルデータ等）
- 保有情報の量
- 保管場所（内部・クラウド）等

分析ステップ（例）

3つの観点から評価・スコアリング ▶ 2軸で評価 ▶ 各事業をパターン分け

Ⅰ 事業特性　評価項目

分類軸	評価項目	回答内容	スコア
社会的影響	事業の公益性	極めて高い	5
社会的影響	…	…	3
社会的影響	…	…	4
事業構造上の脆弱性	事業のIT依存度	極めて高い	5
事業構造上の脆弱性	…	…	5

Ⅱ システム特性　評価項目

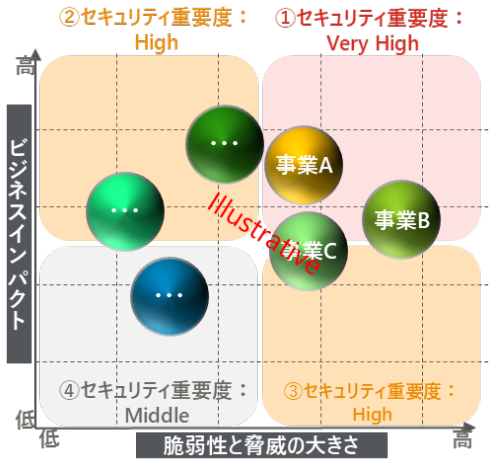
事業構造上の脆弱性	…	…	3
事業構造上の脆弱性	…	…	1

Ⅲ 情報資産　評価項目

情報資産名称	機密性	完全性	可用性	重要度スコア
xxx顧客情報	3	2	1	6
xxx情報	3	1	1	5

事業構造上の脆弱性

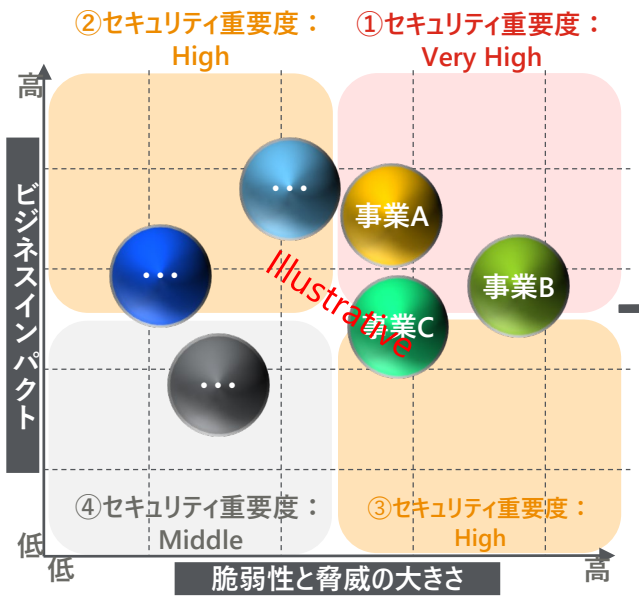
社会的インパクト



各事業のセキュリティ観点での重要度に基づき、あるべきセキュリティ管理態勢が効果的に実現できるガバナンス類型を検討する

Step2. グループ各社に対するガバナンスのモデル検討

セキュリティポートフォリオの検討



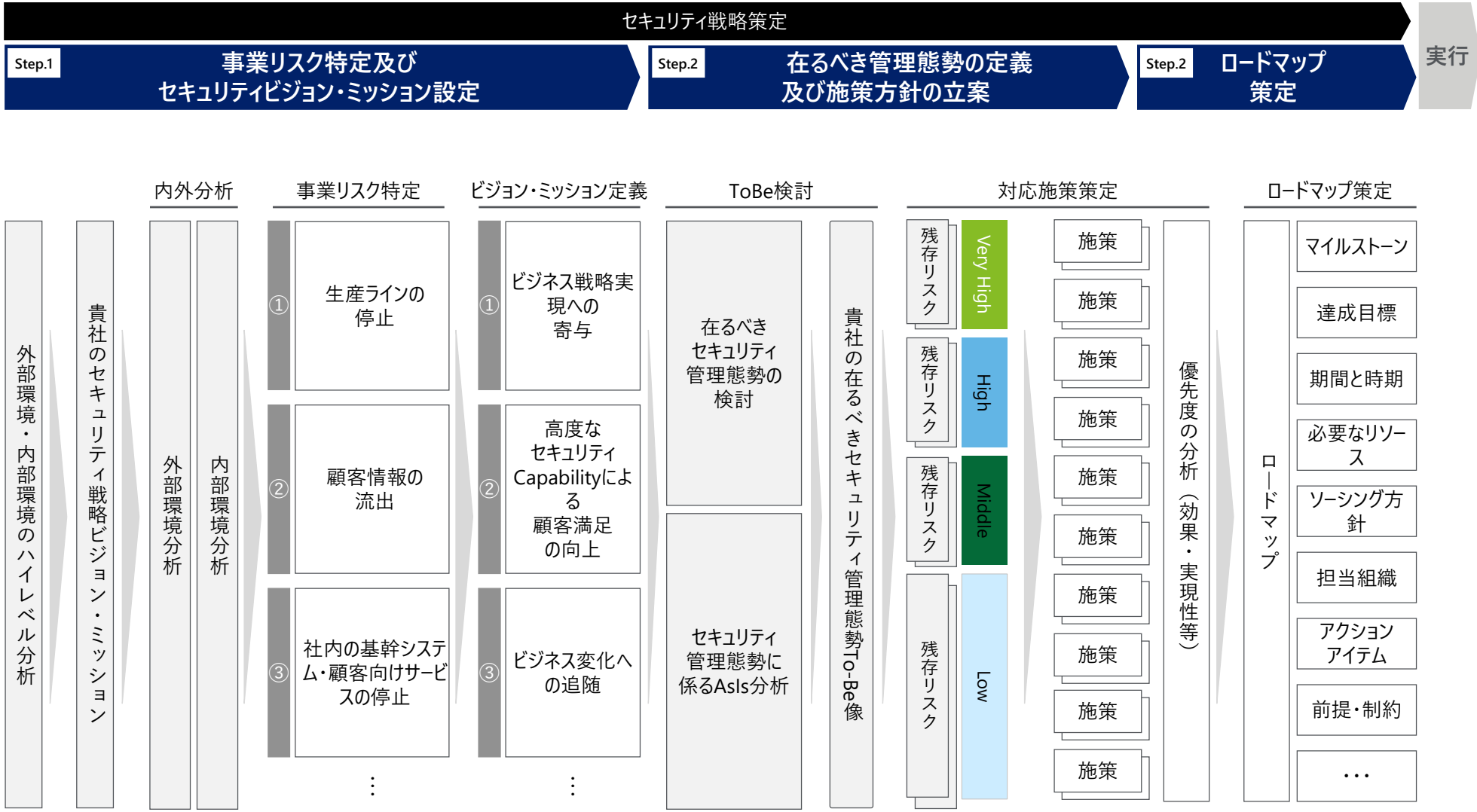
ガバナンス類型	対応方向性	該当組織のイメージ
中央集権型 全社でセキュリティ機能を共通で持つことにより、対策の効率化・セキュリティレベルの標準化・ノウハウの集約を実現	✓ 本社の統括組織が権限を持ちマネジメント・実行機能を担う ✓ 各事業会社が最低限本社と同等以上のセキュリティレベルを維持 ✓ 各事業のセキュリティレベルは、事業ポートフォリオ分析結果に準ずる	第1グループ illustrative ➢ ホールディング ➢ 本社管理のグローバルNWを利用する主要個社
自律分権型 各事業領域で自律的にセキュリティ管理機能を担い、各事業領域や各地域の特性に合わせた運用を行う	✓ 各社が自律的にセキュリティ管理機能の多くを担う ✓ 本社から組織大での方針を示したうえで、各事業会社において事業の特性に応じたセキュリティ対策を講じる	第2グループ ➢ 事業特性の強い個社 ➢ 小規模会社
ハイブリッド型 中央からの統制と自律運営を業務の中で濃淡をつけてバランスを取った運用を行う	✓ 中央からのコントロールと自律運営のバランスを取った管理を行う	第3グループ ➢ 本社管理のグローバルNWを利用する海外独法 ➢ M&Aでグループジョインしたばかりの事業会社

各事業の現状分析に基づき、適用すべきガバナンス類型を検討する

本社の中央集約により第1グループの組織群を管理するだけでなく、自律分権のスタイルにより第2、第3グループも必要な管理をすることが重要

段階的にタスク遂行と論点設定を行い、貴社の事業戦略と連動したサイバーセキュリティ戦略を策定する

（参考）サイバーセキュリティ戦略策定のアプローチ



デジタル化の進展にともなう我々のサイバー空間へ依存度の高まりにより、サイバーセキュリティの価値や位置付けは大きく変容していることを前提として理解する必要がある

デロイトからの提言「サイバーセキュリティのグレートリセット」

JAPAN'S PRACTICAL WISDOM

Incident Response

1 RESET the Mind

守り → *攻め + 守り*

- 自社を取り巻くステークホルダーに対する経営による説明責任が強く求められている
- DX時代においては**サイバー品質が事業品質、事業継続性**を決める
- **サイバーセキュリティを守りのアジェンダ**から「成長のドライバー」としての**攻めアジェンダへと**取り組みの姿勢を変えるべき
- **「ビジネス適合型」**のサイバーセキュリティ管理態勢にシフトすべき

2 RESET the Priority

ITアジェンダ → *CXOアジェンダ*

- 急激に複雑性と影響度を増すサイバーリスクは、**最重要の事業リスクになっている**
- IT部長が責任を持つ時代から**CXOが取り組む経営アジェンダ**へと優先順位を変えるべき
- DX戦略の対になる**サイバーセキュリティ戦略の実践**が経営に求められている
- **サイバーレジリエンス獲得のための危機管理・インシデント対応体制**の重要性がより増している

3 RESET the Scope

自社 → *エコシステム*

- 事業活動・事業環境の多くが**サイバー空間で繋がる時代**
- **IT／製品・サービス／生産等の事業領域全体、**更には自社のみから**サプライチェーン・エコシステム全体へと拡大すべき**
- 自社のビジネススコープに見合ったサイバーセキュリティのガバナンス・ストラクチャーを確立し、**サービス品質保証へと目標をシフトすべき**

THE GREAT RESET

Trusted Business with Trusted DX

Deloitte.
デロイト トーマツ

デロイト トーマツ グループは、日本におけるデロイト アジア パシフィック リミテッドおよびデロイトネットワークのメンバーであるデロイト トーマツ合同会社ならびにそのグループ法人（有限責任監査法人トーマツ、デロイト トーマツ コンサルティング合同会社、デロイト トーマツ ファイナンシャルアドバイザリー合同会社、デロイト トーマツ税理士法人、DT弁護士法人およびデロイト トーマツ コーポレート ソリューション合同会社を含む）の総称です。デロイト トーマツ グループは、日本で最大級のプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従い、監査・保証業務、リスクアドバイザリー、コンサルティング、ファイナンシャルアドバイザリー、税務、法務等を提供しています。また、国内約30都市以上に1万5千名を超える専門家を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツ グループWebサイト（www.deloitte.com/jp）をご覧ください。

Deloitte（デロイト）とは、デロイト トウシュ トーマツ リミテッド（“DTTL”）、そのグローバルネットワーク組織を構成するメンバーファームおよびそれらの関係法人（総称して“デロイトネットワーク”）のひとつまたは複数を指します。DTTL（または“Deloitte Global”）ならびに各メンバーファームおよび関係法人はそれぞれ法的に独立した別個の組織体であり、第三者に関して相互に義務を課しまたは拘束させることはありません。DTTLおよびDTTLの各メンバーファームならびに関係法人は、自らの作為および不作為についてのみ責任を負い、互いに他のファームまたは関係法人の作為および不作為について責任を負うものではありません。DTTLはクライアントへのサービス提供を行いません。詳細はwww.deloitte.com/jp/aboutをご覧ください。
デロイト アジア パシフィック リミテッドはDTTLのメンバーファームであり、保証有限責任会社です。デロイト アジア パシフィック リミテッドのメンバーおよびそれらの関係法人は、それぞれ法的に独立した別個の組織体であり、アジア パシフィックにおける100を超える都市（オークランド、バンコク、北京、ハノイ、香港、ジャカルタ、クアラルンプール、マニラ、メルボルン、大阪、ソウル、上海、シンガポール、シドニー、台北、東京を含む）にてサービスを提供しています。

Deloitte（デロイト）は、監査・保証業務、コンサルティング、ファイナンシャルアドバイザリー、リスクアドバイザリー、税務、法務などに関連する最先端のサービスを、Fortune Global 500®の約9割の企業や多数のプライベート（非公開）企業を含むクライアントに提供しています。デロイトは、資本市場に対する社会的な信頼を高め、クライアントの変革と繁栄を促し、より豊かな経済、公正な社会、持続可能な世界の実現に向けて自ら率先して取り組むことを通じて、計測可能で継続性のある成果をもたらすプロフェッショナルの集団です。デロイトは、創設以来175年余りの歴史を有し、150を超える国・地域にわたって活動を展開しています。“Making an impact that matters”をパーパス（存在理由）として標榜するデロイトの約345,000名のプロフェッショナルの活動の詳細については、（www.deloitte.com）をご覧ください。

IS 669126 / ISO 27001

Member of
Deloitte Touche Tohmatsu Limited