KPMG

制御システムにおける サイバーリスクマネジメント態勢の確立と 事例紹介

KPMGコンサルティング株式会社
サイバーセキュリティアドバイザリー
マネージャー
保坂　範和

目次

01
制御システムの現状と課題

重要インフラへのサイバー攻撃

攻撃事例１

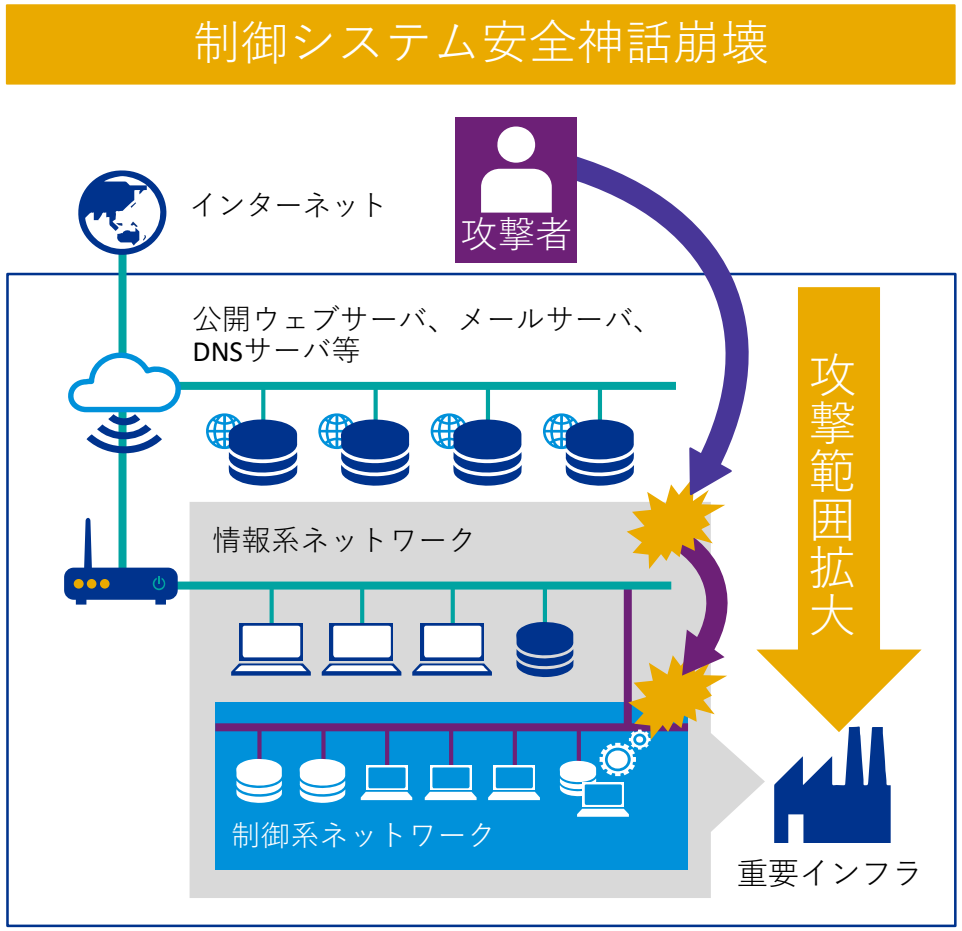
サイバー攻撃による大規模停電
2016年　ウクライナ

攻撃事例２

ランサムウェアによる工場の操業停止
2017年　日本

攻撃事例３

サプライチェーンを狙ったサイバー攻撃
2017年　日本



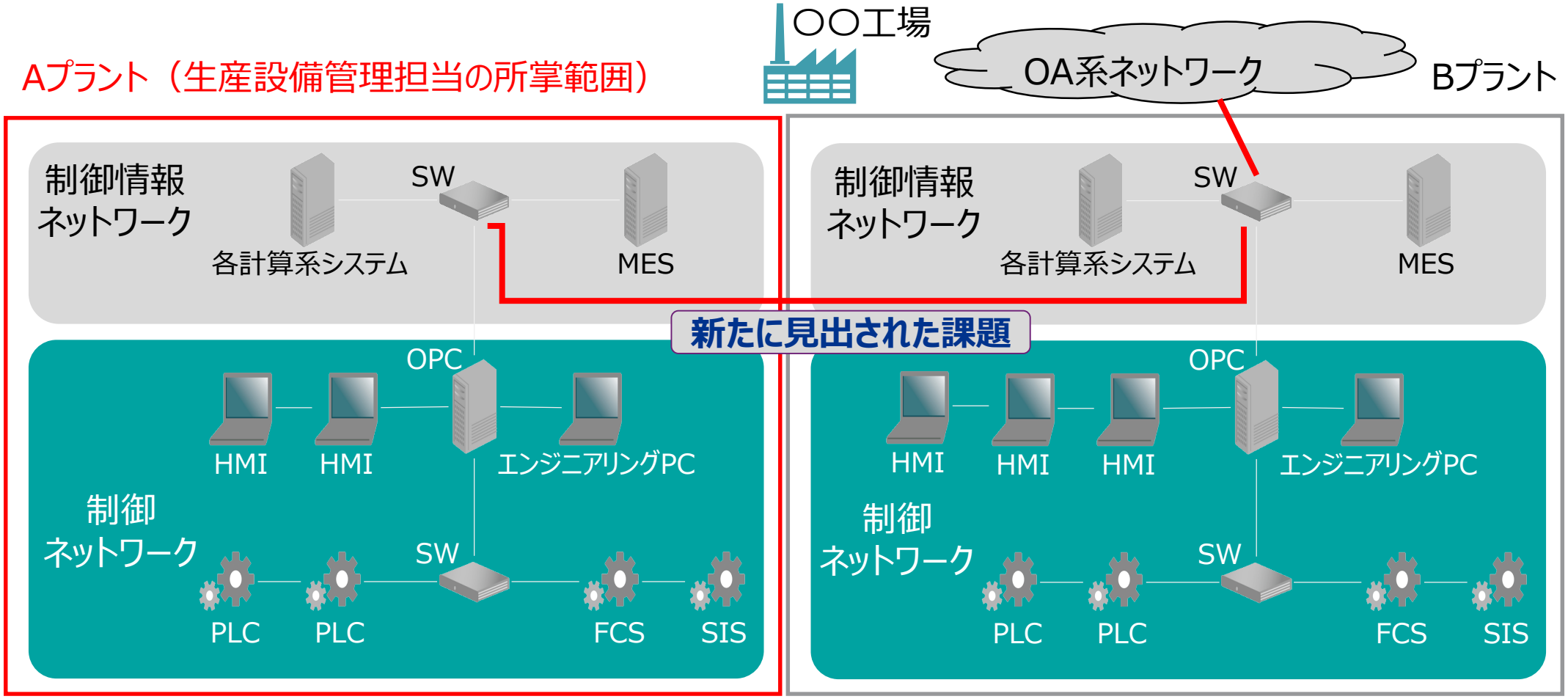
前提として押さえるべきOTとITの違い

優先すべき目的・論点や、対策実装の前提条件や制約、推進主体が情報系システムと異なる。

	制御系システム	情報系システム
セキュリティの優先順位	**継続的な安定稼働（可用性）や安全確保**	機密情報の漏えい防止（機密性）
セキュリティの対象	モノ（設備・製品） サービス（連続稼働）	情報
システム更新のライフサイクル	**10～20年**	3～5年
システム稼働時間	**24時間365日（再起動は原則許容されない）**	サービス提供時間外
システム運用管理	計装部門 設備管理部門	情報システム部門

と言われているが、実態は・・・？

生産現場担当者の認識（現実とのギャップ）



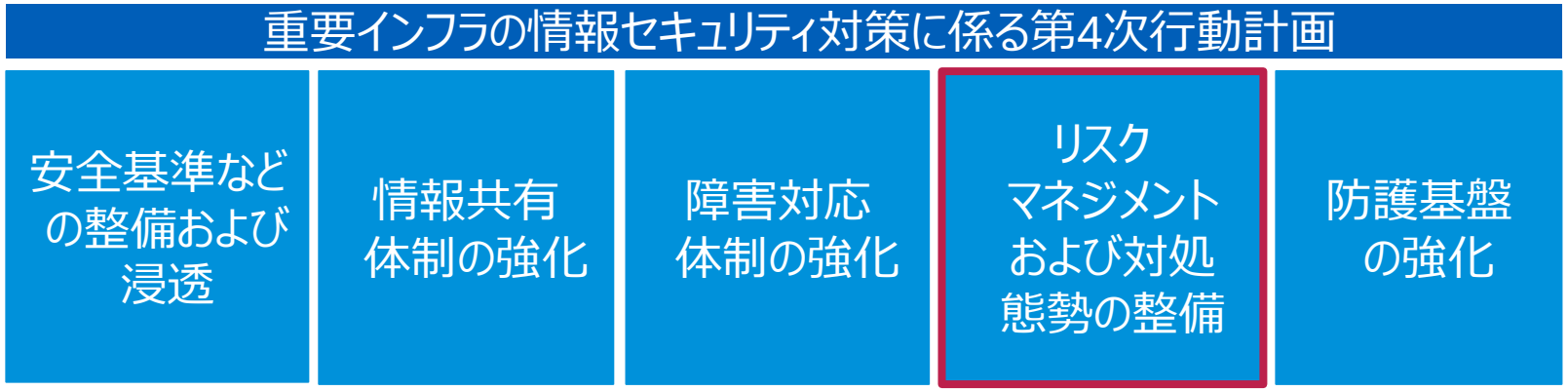
政府による重要インフラ業界への働きかけ

IPA

- 制御システムのサイバーセキュリティ人材育成と中心とした事業を推進する「産業サイバーセキュリティセンター」を発足（2017.4.1）
- 経済産業省による事業の一環として「制御システムのセキュリティリスク分析ガイド」を公開（2017.10.2）

NISC

- 「重要インフラの情報セキュリティ対策に係る第4次行動計画」を公表（2017.4.18）



電力業界の変化に伴うサイバーセキュリティ動向

＜業界個別の取組例＞

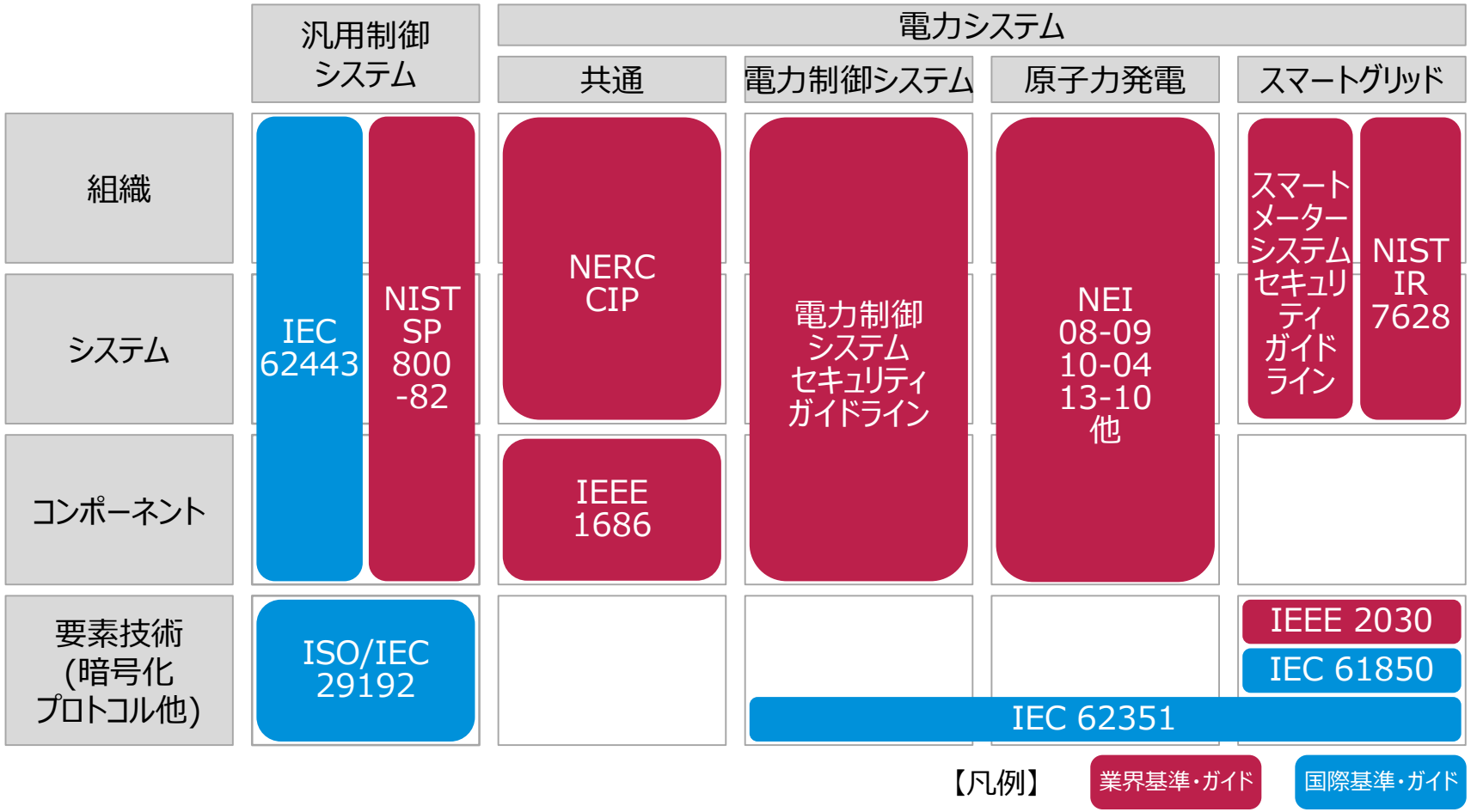
事業環境の変化に伴うサイバーリスクの高まりと、政府・業界における取り組みが進む

電力自由化	■ 多様なプレーヤーが電力システムに接続 ■ コスト低減のためのシステムオープン化	従来のセキュリティ水準の維持が困難であり、電力安定供給への支障や情報漏えい等のリスクが顕在化
スマートグリッドの進展	■ 2018年度末までに全国約8000万台の電力量計の半数以上がスマートメーター化	海外では電力システムのオープン化に伴うサイバー攻撃の被害が増加
2020年東京オリンピック	■ 2012年ロンドンオリンピックでは開会式の停電を狙うサイバー攻撃が発生	2020年の東京オリンピックではより高度かつ大規模なサイバー攻撃に備える必要性

2016年に国内発の
ガイドラインとして立て続けに策定

- スマートメーターシステム セキュリティガイドライン
- 電力制御システム セキュリティガイドライン

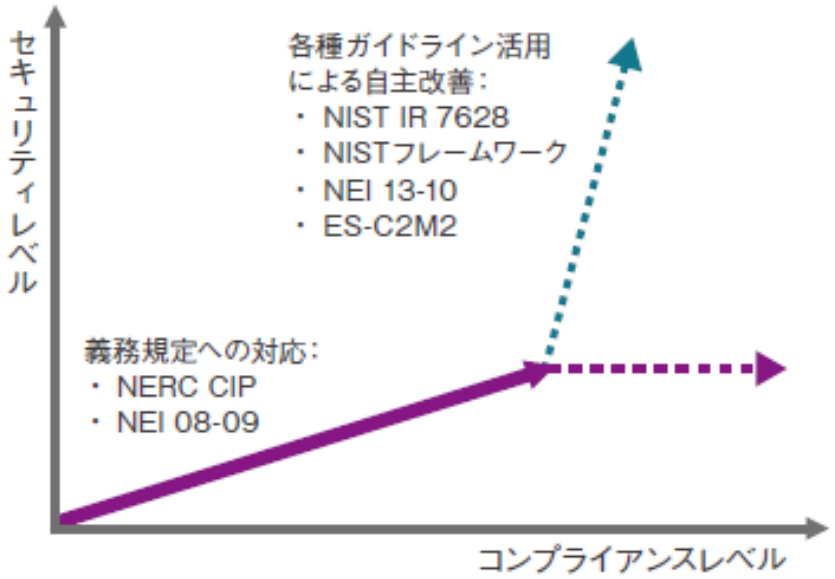
電力システムに係るサイバーセキュリティ関連基準・ガイド
＜業界個別の取組例＞



電力事業者における関連規制・スタンダードの適用例
＜業界個別の取組例＞

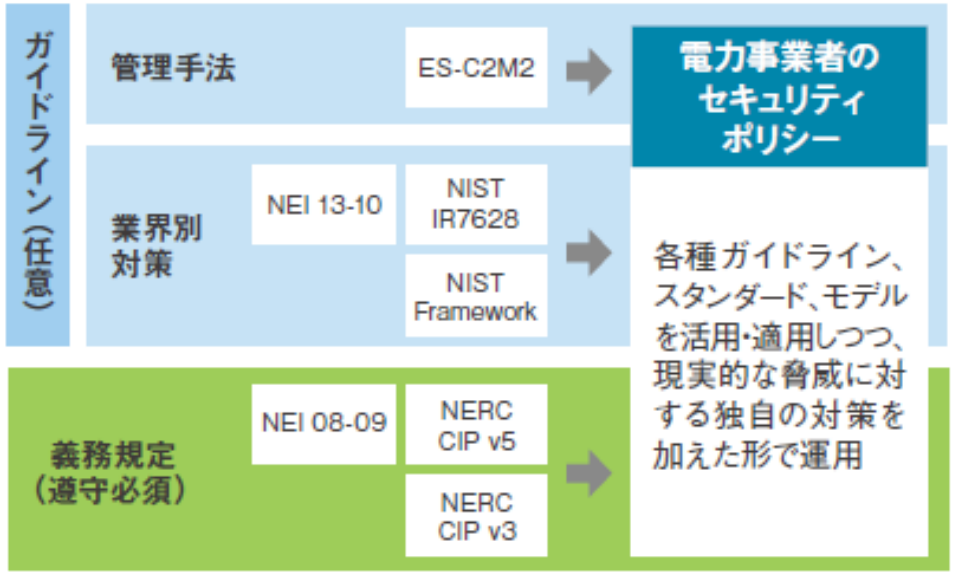
コンプライアンスvsセキュリティ

コンプライアンスのみに注力し続けても、セキュリティレベルは一定水準までしか高まらない



自社のポリシー／スタンダードの策定

義務規定と任意ガイドラインから必要なものを選定し、組み合わせ、自社のポリシー、スタンダードを策定している



出所：「平成26年度電気施設技術基準国際化調査（電気設備）サイバーセキュリティ対策に関する調査報告」の掲載内容に基づき、KPMGが加筆・編集

KPMG

02
制御システムにおける
サイバーリスクマネジメント態勢

重要インフラ事業者にとっての課題

社会的責任の観点

サイバーセキュリティに関する説明能力の向上

✓サイバーセキュリティに関する責任所在の明確化

✓CIOや情報セキュリティ責任者に限定しない全社的な意識向上

✓全社的に自社の事業アセットとサイバー攻撃に対する脆弱性・リスクの的確な認識

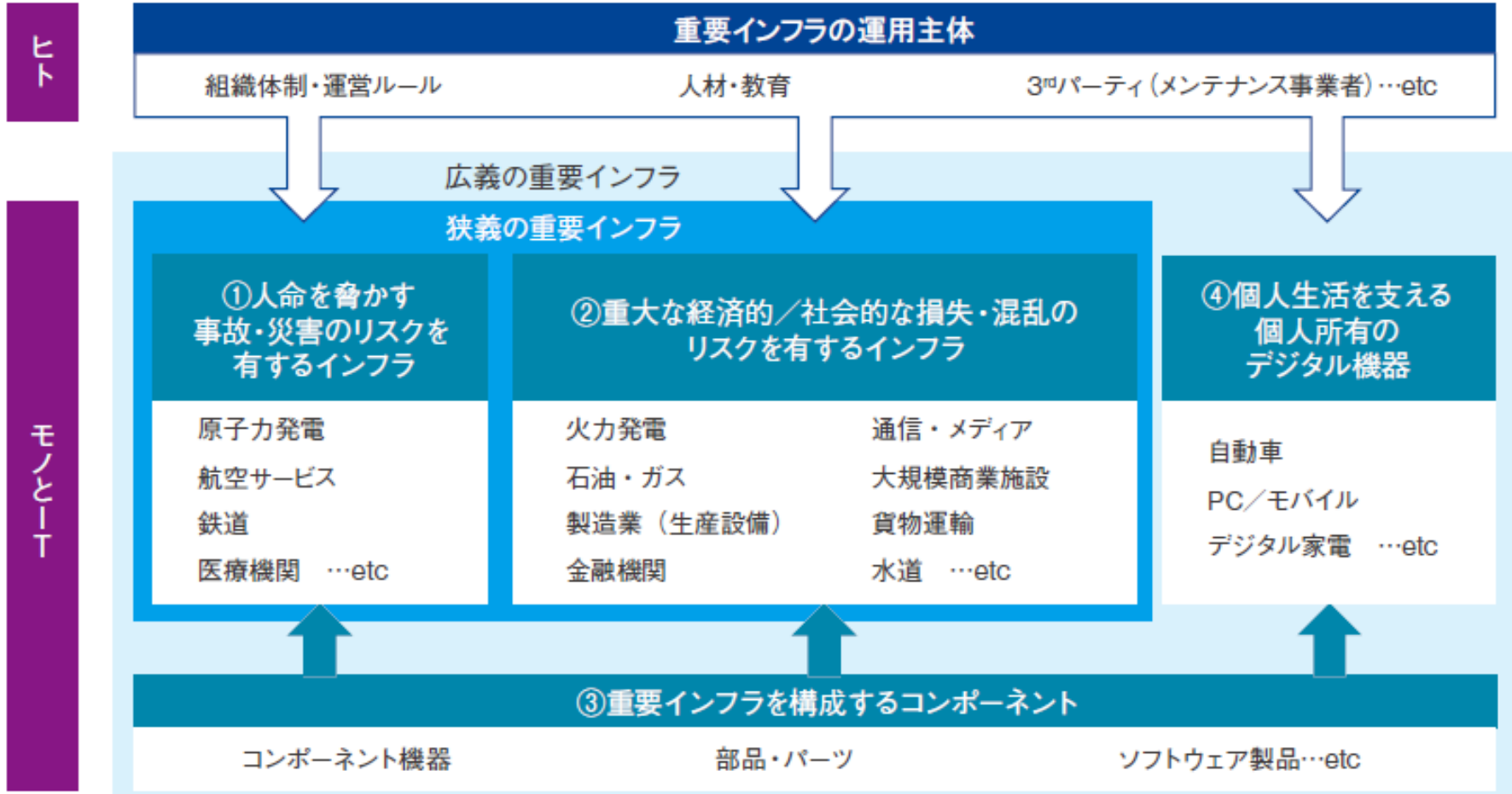
事業競争力の観点

効果的かつ効率的なサイバーセキュリティ対策の推進

✓今後整備が進む関連規制・スタンダードへの迅速なキャッチアップと積極的姿勢での活用

✓老朽化が進むレガシーアセットへの対応も含めた、アセットへの投資管理、ライフサイクル管理の態勢構築

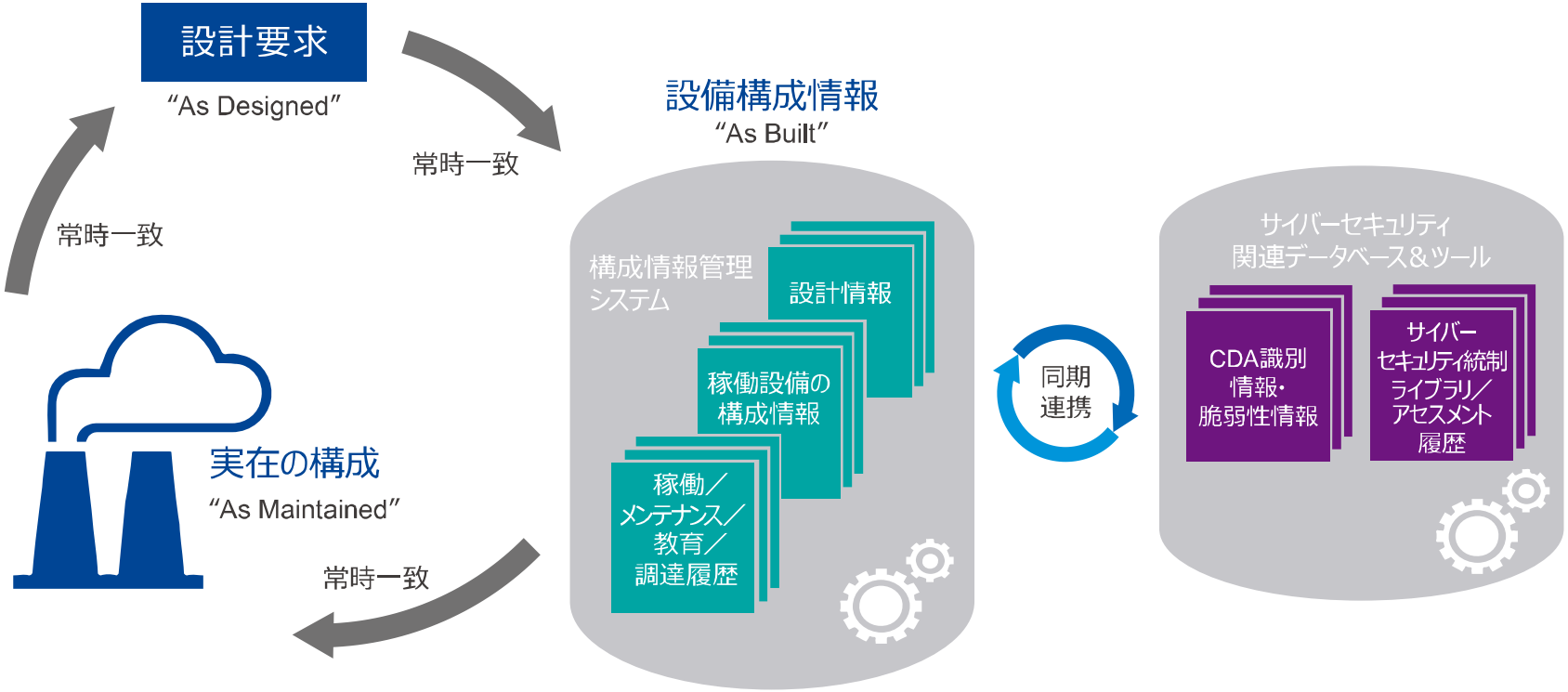
重要インフラ事業者にとってのセキュリティリスク



出展：重要インフラ産業におけるサイバーセキュリティ対策の要諦と方向性，KPMGジャパン
<https://assets.kpmg.com/content/dam/kpmg/pdf/2016/03/jp-cyber-security-infrastructure.pdf>

セキュリティ対策で重要性を増す構成管理

米国における原子力発電プラントの構成情報管理とサイバーセキュリティ対策

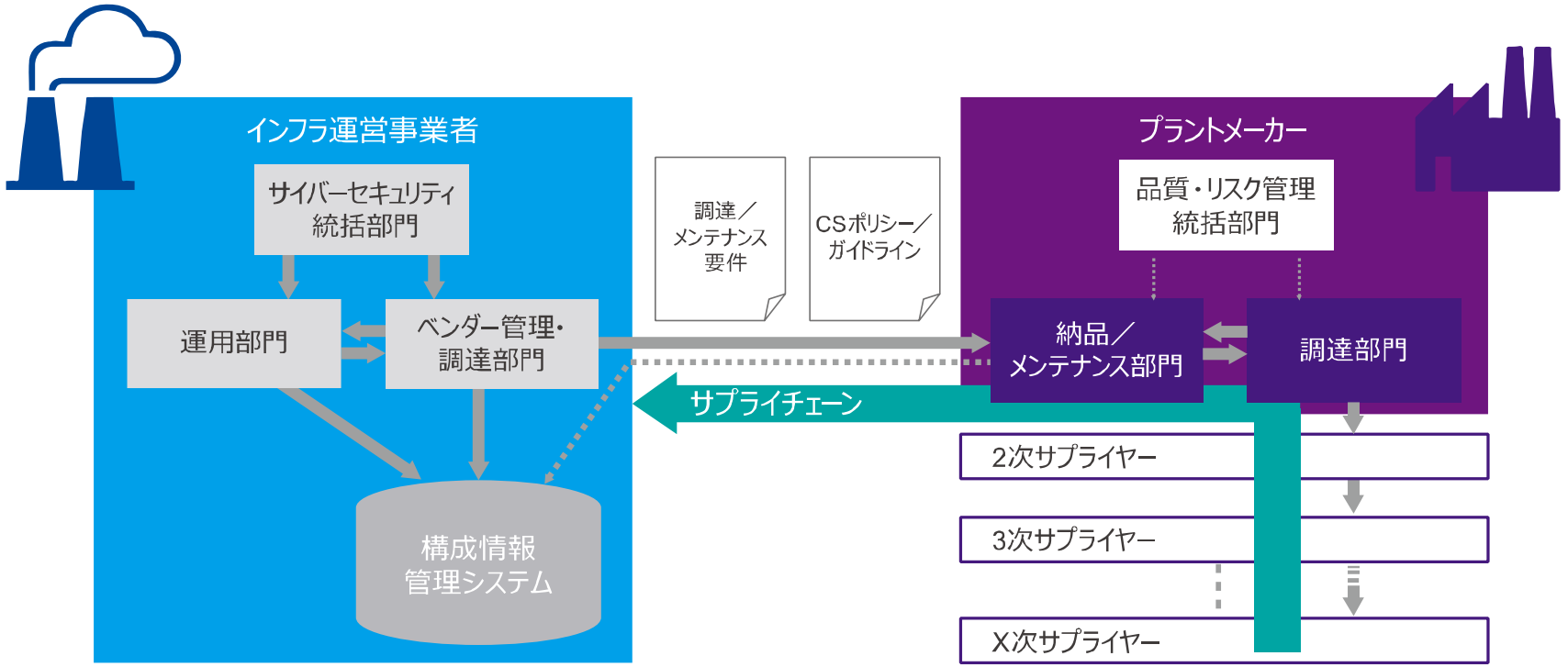


出所：「重要インフラ産業におけるサイバーセキュリティ対策の要諦と方向性」（KPMGジャパン）

セキュリティ対策の網羅性と効率性を担保するためには、構成情報を自社で管理できる態勢の構築が不可欠

企業間連携が求められるサプライチェーン攻撃への備え

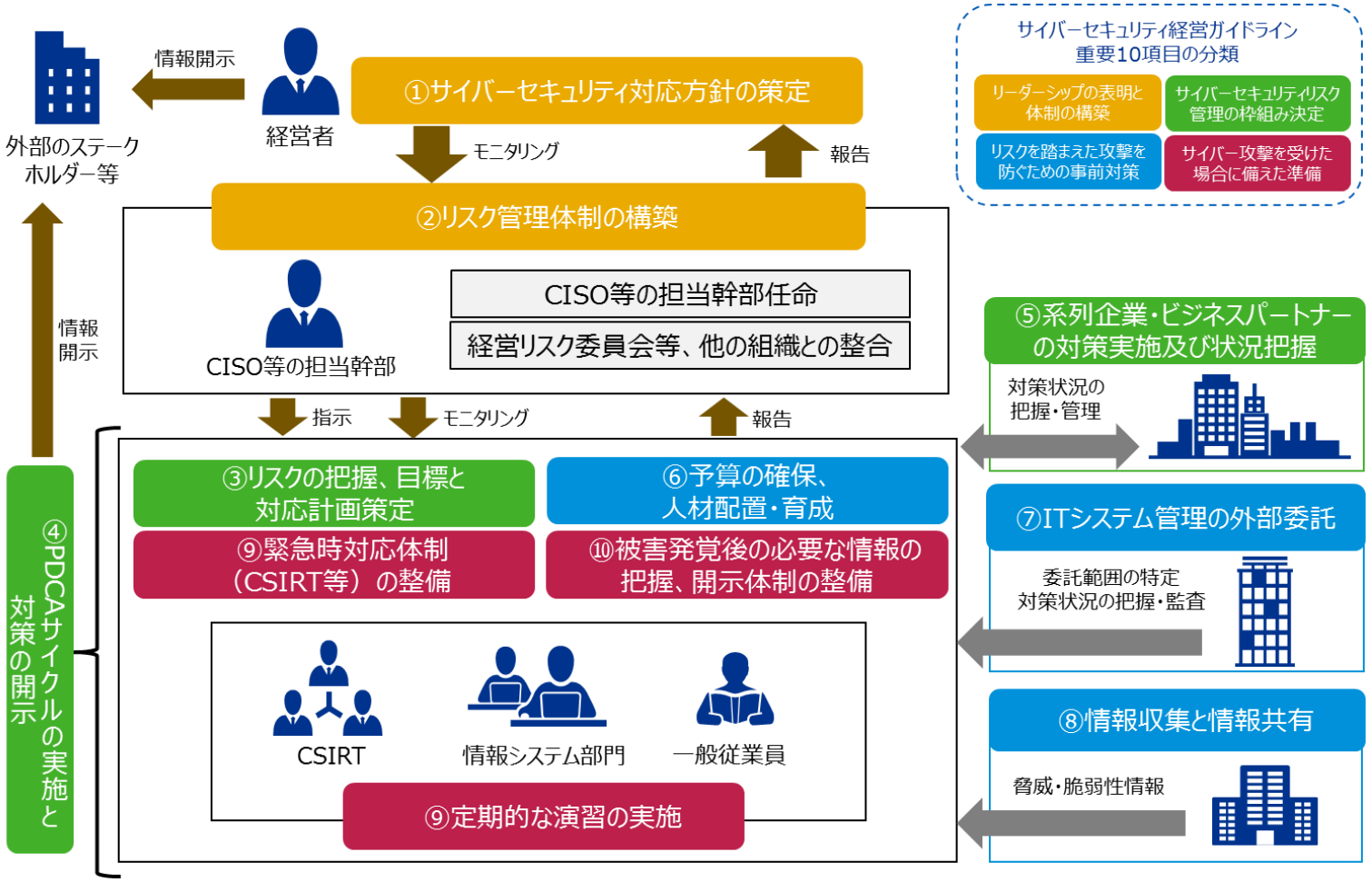
ユーザ企業とベンダー企業を横断したサプライチェーンのガバナンス



出所：「重要インフラ産業におけるサイバーセキュリティ対策の要諦と方向性」（KPMGジャパン）

USB攻撃の実例も存在する中、保守や更改などベンダーとの接点においてもセキュリティ対策が必要

サイバーセキュリティ経営で求められるリスク管理

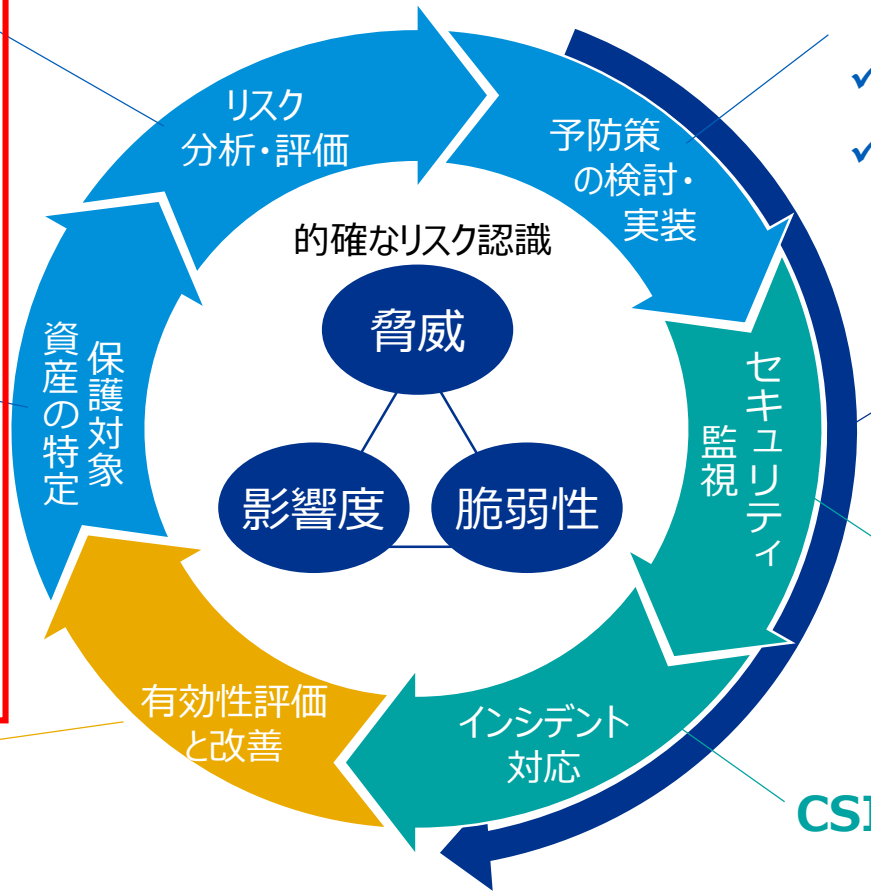


制御系サイバーセキュリティの高度化ライフサイクル

- ✓ 脅威シナリオ分析
- ✓ リスクアセスメント実施
  （第三者による客観的評価）

- ✓ 資産の棚卸調査
- ✓ 資産情報台帳管理

- ✓ KPI モニタリング
- ✓ インシデント対応訓練
- ✓ サイバーセキュリティ教育



- ✓ セキュリティポリシー策定
  （基本方針・対策基準 など）
- ✓ 対策設計・教育計画策定
- ✓ 対策導入・教育展開

**体制構築と
人材教育**

SOC体制の確立

CSIRT体制の確立

サイバーセキュリティへの対策状況を把握するフレームワーク
CMA(Cyber Maturity Assessment) for ICS

法令とコンプライアンス

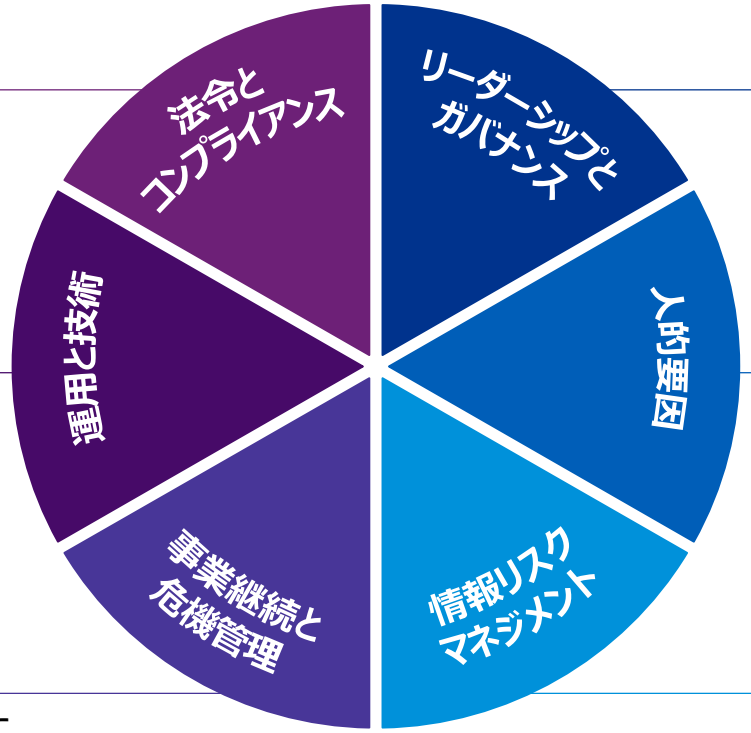
関連法令や国際認証基準への準拠度合い

運用と技術

特定されたリスクを低減させるために導入されている対策のレベル

事業継続と危機管理

セキュリティインシデントに対する組織の準備状況およびその対応能力



リーダーシップとガバナンス

経営者がセキュリティリスクを理解し、責任を負っているか

人的要因

セキュリティに対する従業員の意識、スキル、知識といった組織風土

情報リスクマネジメント

情報資産に対するリスク管理手法が定義され、それに則って情報資産が管理されているか

制御システム向けセキュリティリスク分析

モニタリングと課題抽出によるセキュリティ戦略見直し

①モニタリング

サイバーセキュリティ経営ダッシュボードにより、各セキュリティ施策の実施状況・効果をモニタリングする。

サイバーセキュリティ経営ダッシュボード

②課題抽出・方針検討

モニタリング結果に基づき、強化すべきセキュリティ領域を特定する。

抽出された課題（例）

・セキュリティ上の脅威が適切に検出できていない（ログ監視の不備）

・CSIRTが機能していない（要員不足・手順の不備）

具体的なセキュリティ施策（例）

・SIEM導入、監視ルールの策定
・SIEM運用の人員・教育計画の策定
・外部SOCの選定・導入
・インシデント報告・対処手順の整備
・SOC/CSIRTの要員確保・教育計画の策定
・インシデント報告・対処手順の整備

サイバーセキュリティ経営ガイドライン重要10項目の分類

- リーダーシップの表明と体制の構築
- サイバーセキュリティリスク管理の枠組み決定
- サイバー攻撃を受けた場合に備えた準備
- リスクを踏まえた攻撃を防ぐための事前対策

③方針見直し・高度化

新たな戦略と方針に基づき施策を実施する。

サイバーセキュリティ戦略と方針の見直し

- リスク分析
- セキュリティ監査
- サプライチェーン管理
- グローバル管理
- SOCの構築・強化
- ログ監視の高度化
- CSIRTの構築・強化
- セキュリティ教育
- 脆弱性管理
- ペネトレーションテスト
- ITセキュリティツール導入

03
海外・国内の事例紹介

＜投影のみ＞

04
まとめ

まとめ

重要インフラに迫るサイバー脅威

- ✓サイバー攻撃の件数増加、手法高度化のトレンドの中で、重要インフラ産業においても脆弱性と脅威が高まっている
- ✓重要インフラ産業におけるサイバーセキュリティ事故は、大規模な社会的混乱や人身事故など甚大な被害に帰結する危険性をはらむ

重要インフラ事業者の課題

- ✓重要インフラ事業者は、社会的責任の一翼を担う立場として説明能力を高める必要があり、経営層がサイバーセキュリティへの理解を深めることが急務となっている
- ✓サイバーセキュリティをリスク管理の一領域として捉え、インフラ設備の投資判断、ライフサイクル管理を推進が求められる

サイバーセキュリティ対策の要諦

- ✓現状把握として、資産の棚卸調査、事業リスクの把握、システムリスク評価が急務
- ✓情報システムと制御システム、本社とプラント間などにおけるサイバーセキュリティ上の役割と責任範囲を明確にする
- ✓サイバー人材の育成と外部専門家との連携態勢の確立が急務
- ✓インフラ設備のみならず、サプライチェーンで関与するベンダーや、運用オペレーションで関与する組織・人も含めた俯瞰が必要

お問合せ先

KPMGコンサルティング株式会社

サイバーセキュリティアドバイザリー

kc-cybersecurity@jp.kpmg.com

TEL：03-3548-5111（代表）

kpmg.com/jp/kc