海外及び国内重要インフラ事業者のサイバー攻撃対策の実態

佐々木　弘志
インテル セキュリティ（マカフィー株式会社）　サイバー戦略室
シニア・セキュリティ・アドバイザー　CISSP

TM

講演者 - 自己紹介

佐々木　弘志
CISSP、サイバー戦略室
インテルセキュリティ

10年以上の制御システム開発者としての経験を活かし、
重要インフラ防護（CIP）、IoTセキュリティのエバンジェリストとして活動。
講演、執筆多数。

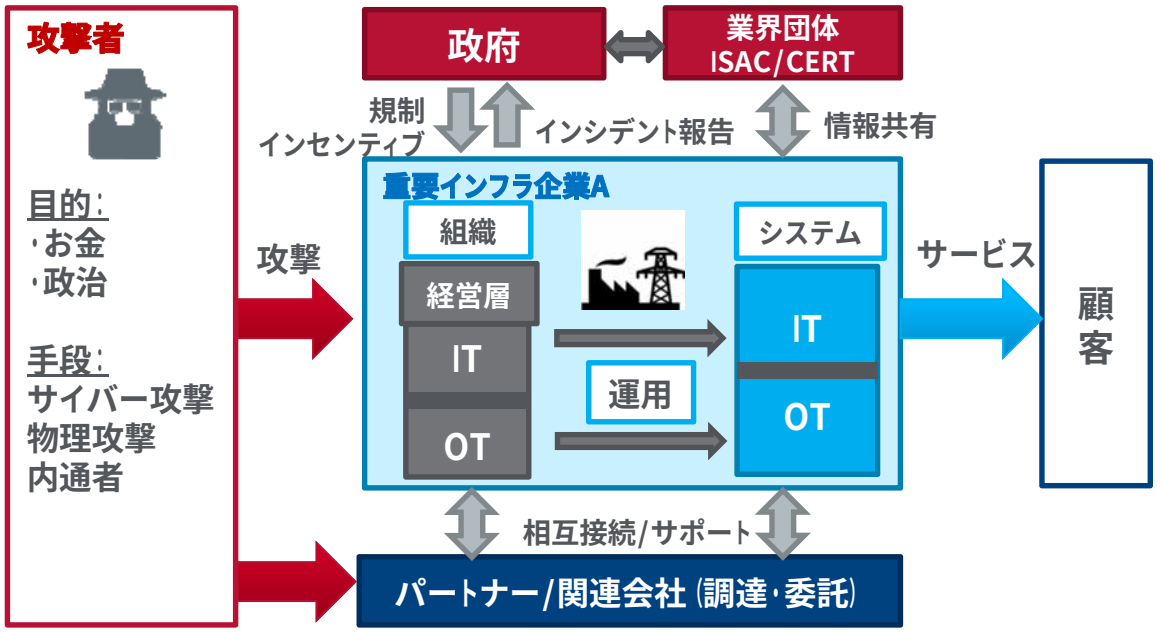
主な実績
・経済産業省　電力業界セキュリティ政策に関するヒアリング調査（米国・欧州）
-平成27年度電気施設保安制度等検討調査（電気設備技術基準国際化調査）
-平成26年度電気施設技術基準国際化調査(電気設備)
・名古屋工業大学　制御系セキュリティワークショップ共催（2015- 継続中）
・技術研究組合　制御システムセキュリティセンター（CSSC）による請負
-「制御装置におけるホワイトリスト対策の要件定義及び検査項目の開発」（2015）
-「米国における制御システムセキュリティ規格実装例の国内製制御システムにおける検証」（2013）

Agenda

0．重要インフラ事業者のサイバー攻撃対策の基本コンセプト
1．米国の電力会社の事例
2．欧州の電力会社の事例
3．日本の電力会社（東京電力パワーグリッド社様）の事例
4．まとめ

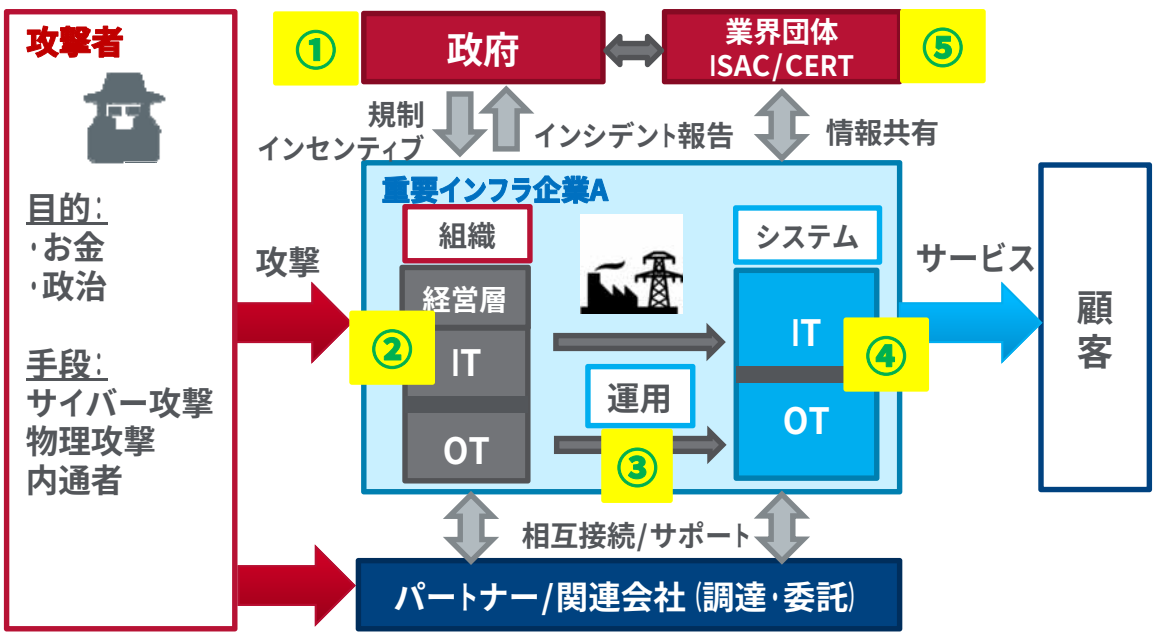
重要インフラ事業者の サイバー攻撃対策の 基本コンセプト

重要インフラ事業者を取り巻く環境



OT：Operational Technology 制御システム

重要インフラ事業者のサイバー攻撃対策の戦略



①政府の政策
- -規制
- -ガイドライン
- -インセンティブetc

②組織面の対策
- -CISOの位置付け
- -CSIRT/SOC
- -IT/OTの連携
- -関連会社への対策

③運用面の対策
- -SOC運用
- -BCP/BCM
- -外部委託

④技術面の対策
- -OT側の防護/監視

⑤情報共有
- -ISAC/CERTと協力

米国の電力会社の事例

米国電力会社の取組①

電力会社は情報系/制御系を両方見ているセキュリティ担当者がいる！

－組織体制

CISO（Chief Information Security Officer：最高情報セキュリティ責任者)が必ずいる。

概ね全体で数名～20名程度。NERC対応の部署はコンプライアンス部門に属している

IT部門が主導している。（制御系部門との壁はまだある。）

－NERC含むガイドラインの適用

NERCはコンプライアンスなので、ドキュメント作業が大変なわりに、
セキュリティレベルはフロアレベル。

対策の程度は、電力会社の規模により差がある。

大規模電力会社は対応に余裕あり。規模小さいほど負担増。

NIST Framework, NIST IR 7628, ES-C2M2の評価が高い。

－情報共有

ES-ISACを活用しているものの、地域での情報共有も有効。

米国電力会社の取組②

IT系でのセキュリティログ監視は常識。制御系の監視をしているかどうかが差。

－社内教育

フィッシングメールは全社実施。

重要サイバー資産にアクセスする外部業者に対しても教育実施。

ITと制御系チーム＋ビジネスアナリストを加えてリスク分析。

実際のアセットに対して侵入テスト実施。管理者に脅威を知らせる。

－セキュリティ対策例

レガシーOT系の対策（ネットワーク隔離＋物理セキュリティ）（2社）

状況認識の重要性が高い。IT系にはSIEM（ログ収集・解析）を導入（4社）

情報系/制御系を統合監視（Full Situational Awareness）（PG&E）

－その他

電力の安定供給が最優先。セキュリティ対策を行う根拠にもなっている。

ガスと電力の制御情報ネットワークは共通で同レベルの対策。　（PG&E）

NERC CIPの遵守状況

コンプライアンス標準のため100%遵守

- **ヒアリングした電力会社について、NERC CIP Standardの遵守状況は100%。**
- **コンプライアンス標準であるため「必ず」守らなければならない。**
- **NERCによる監査（実際の監査は地域信頼度評議会が実施する）も実施されている。**
- **NERC CIPへの対応および監査対応のために各社専門の担当者を配置している。**
- **大規模な電力会社に関しては、遵守についてそんなに負担を感じていないが、中～小規模の会社ではその膨大なドキュメント作成（関連作業の60%を占めると言われる）に不満を持っている。**

標準	概要
CIP 002-5	リスクベースのアプローチによって重要資産を特定し、これに基づき重要サイバー資産を定める。
CIP 003-5	最小限のセキュリティ管理を確立して重要サイバー資産を保護するためのセキュリティに関する行動計画を策定・実施する。
CIP 004-5	重要サイバー資産へのアクセスを電子的・物理的に許可された人員に対して、必要なトレーニングを施し、セキュリティ意識を身につけさせる。
CIP 005-5	重要サイバー資産を取り囲む電子的なセキュリティ防衛線を特定し、防衛線上の全てのアクセスポイントを特定し保護する。
CIP 006-5	重要サイバー資産を物理的に保護するための行動計画を策定・実施する。
CIP 007-5	自らが定めた重要サイバー資産のセキュリティを確保するための手法、プロセス、手続きを定義する。
CIP 008-5	重要サイバー資産に関連するセキュリティインシデントを特定、分類、対処して報告をする。
CIP 009-5	重要サイバー資産に関する復旧計画を策定し、計画手順を確立し、技法に沿った復旧計画を行う。
CIP 010-5	重要サイバー資産の構成管理プロセスを特定し、不備を特定、分類、対処して報告をする。
CIP 011-5	重要サイバー資産を廃棄や再利用する際の情報取り出しに承認を行い、情報保護を行う。

（出所）NERC CIP verion 5 Draft（2013年）

日本総合研究所:「平成25年度次世代電力システムに関する電力保安調査報告書より

電力会社における組織体制

実施体制の整備および責任・役割の明確化

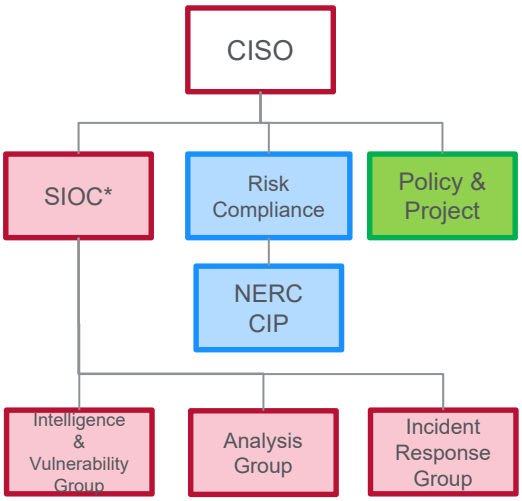
-米国の電力各社は社内に必ずCISOを配置し、責任および体制を明確化している。

-CISOのほかに、Corporate Security ManagerやCIO、CEO等と脅威のレベル等に応じて連携している。

-また、脅威のターゲット、ポテンシャル、タイムフレームなどで分類を行い、責任者の実施すべきアクションを設定している。

-なお、最近ではITシステムに対する攻撃だけではなく、制御システムに対する攻撃も含めた形で体制を構築している。

-また、社内のトレーニング（重要）、脆弱性診断、机上演習などもこの体制が中心となってしっかり行っている。



セキュリティ関係する体制図

*SIOC：Security Intelligence Operating Center

各規制・ガイドラインの活用方法

義務規定と任意のガイドラインを組み合わせて社内基準としている

マネジメント手法のガイドライン（任意）
改善のサイクルを回すためのセキュリティ成熟度モデル

ES-C2M2

業界向けガイドライン（任意）
リスクベースの対策：ベースラインの上
現実の脅威に対抗する
ためのセキュリティ対策

NIST Framework

NIST IR 7628

義務規定
指示的な対策：ベースライン（フロア）
最低限のセキュリティ対策
チェックリスト方式

NERC CIP v5

NERC CIP v3

活用

活用

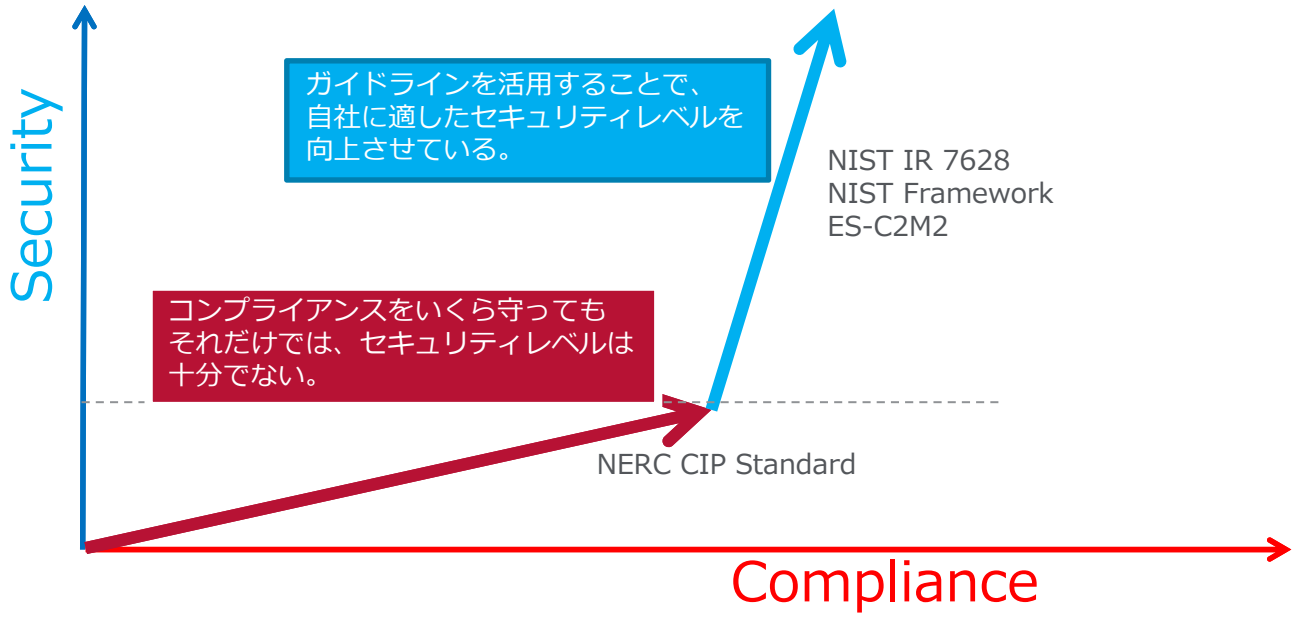
反映

電力事業者のセキュリティポリシー

様々な標準、ガイドライン、モデルを遵守・活用しつつ、現実的な脅威に対して、独自の対策を加えた形で運用している。

Security vs. Compliance

コンプライアンスを守ることはセキュリティではない



欧州の電力会社の事例

イギリス電力会社のヒアリング結果

リベラルな政策の結果、電力会社間のセキュリティレベル格差が大きい

大手電力会社では、CISOを中心とした組織の役割分担がしっかりなされており、セキュリティ対策にも力を入れていたのに対し、小さな電力会社では、情報システム部にタスクが集中しており、情報システムの監視を外部委託するなど、最小限の対策となっていた。

ヒアリング結果トピック

・ペネトレーションテストをシミュレーションで実施。（Skybox使用）**（運用/技術）**

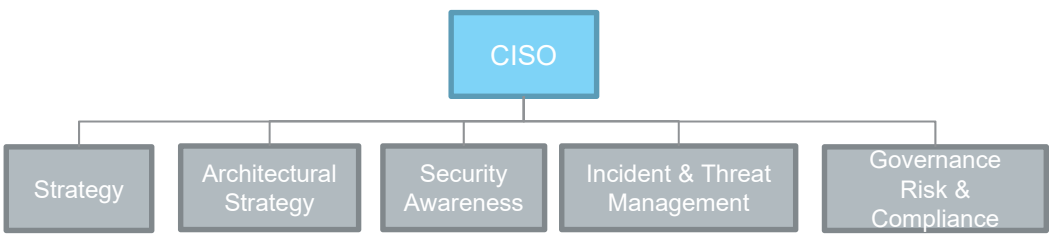
・情報共有においては、E3Cの枠組みを活用しているが、E3Cの場でインシデント情報の共有を行うときには、政府側の担当者抜きで実施する。

・セキュリティ対策を実施する動機として一番大きいのは、レピュテーション（会社の評判）であるとのこと。補助金の活用も動機のひとつとなっていた。

⇒電力自由化により、競争環境に置かれているため、たとえ地域独占的な会社であっても、サイバー攻撃を受けて停電を起こすとレピュテーションが低下し、株価に影響することが**経営問題として捉えられている**。

イギリス電力会社における組織体制例

実施体制の整備および責任・役割の明確化



National Grid における体制図

組織/役職名	英語名称	概要説明
最高情報セキュリティ責任者	CISO（Chief Information Security Officer）	自社のセキュリティ対策の総責任者であり、ボードメンバーでもある。自社のセキュリティ対策において経営リスクを考慮してコストを決定する。
戦略チーム	Strategy	今後のセキュリティ全般の対策の戦略、ポリシーを検討する。
設計戦略チーム	Architectural Strategy	電力システムの設計において、セキュリティを考慮した戦略を検討する。
セキュリティ認知向上チーム	Security Awareness	社員のセキュリティ啓発や教育・とレーニングを行う。
インシデント＆脅威管理チーム	Incident & Threat Management	インシデントや脅威情報の管理を行う。
ガバナンス、リスク、法令遵守チーム	Governance Risk & Compliance	自社を取り巻くあらゆるリスクを積極的に特定し、評価。

ドイツ電力会社のヒアリング結果

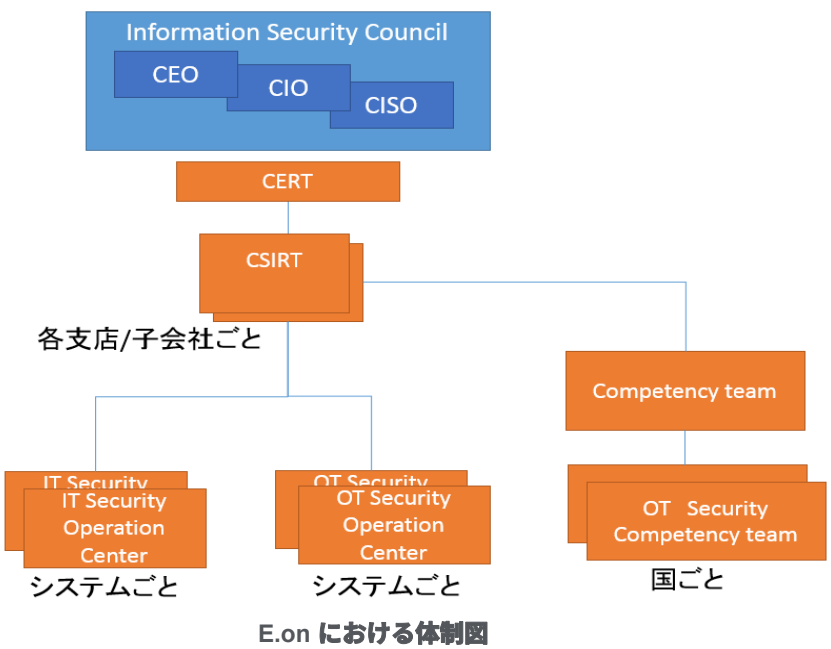
チェックリスト方式のガイドラインの活用。規制のある環境は当たり前。

ある大規模電力会社では、多国籍企業であることから、各国にある支店や子会社に対するガバナンスとマネジメントを実現する階層的な体制が構築されていた。セキュリティ対策は、BSIが規制として採用予定のISMS、 ISO27019:2013については、既に対応済。

ヒアリング結果トピック

- ペネトレーションテストは、稼働中のシステムに対してではなく、同じシステム環境を用意したテストベッド上で実施。（**運用**/**技術**）
- 情報共有においては、UP Kritisの枠組みを活用しているが、本当に重要な情報は、政府には言わず、信頼できる電力会社の担当者間で共有している。
- 規制を実現するために、組織体制はしっかりしている。ISCはボードメンバーが参加する全社的なガバナンスを効かせる組織。各子会社や組織ごとに、SOC、CSIRTなど一通りの機能は持っている。CSIRTは、子会社ごとにあり、各国の法律等などの細かい対応をする点では有利だが、多すぎてガバナンスが効きにくいところもあるので、いくつか統合する方向で検討中。（**組織**）
- セキュリティ対策を実施する動機としては、規制があるから。したがって、米国で見られたリスクベースアプローチによるガイドラインの活用は見られなかった。

ドイツ電力会社における組織体制例①



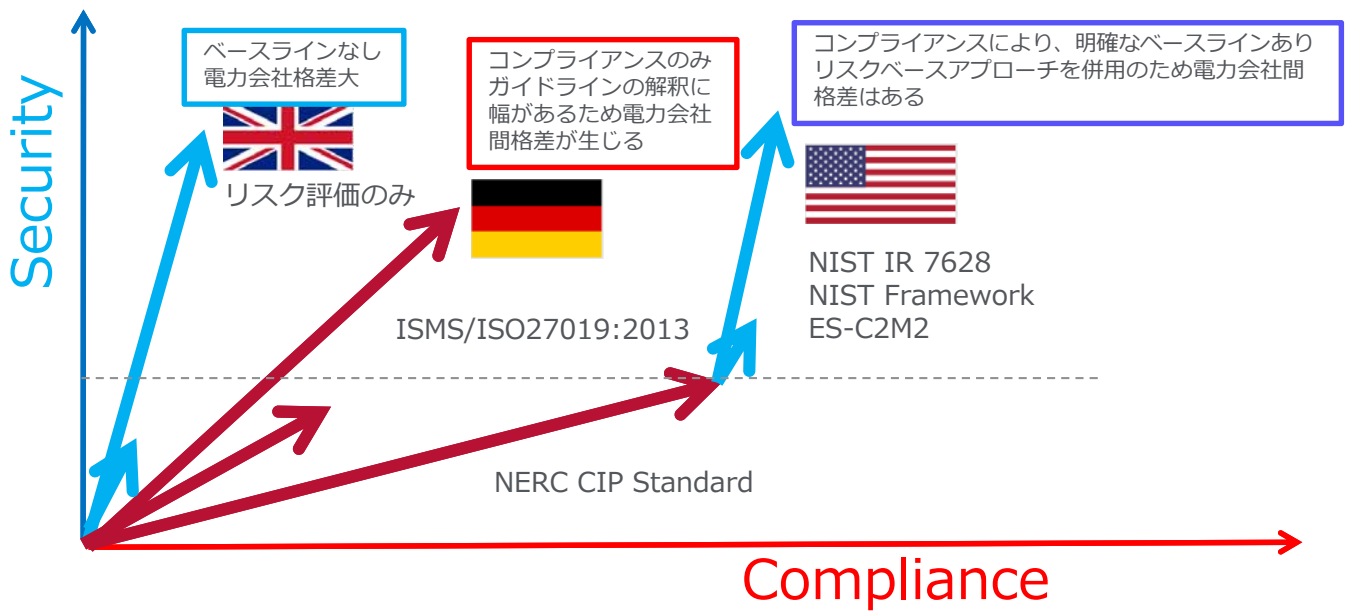
E.on における体制図

ドイツ電力会社における組織体制例②

組織/役職名	英語名称	概要説明
情報セキュリティ協議会	Information Security Council	子会社も含めた情報セキュリティ政策を決定する最高機関。CEO（最高経営責任者）、CIO（最高情報責任者）CISO（最高情報セキュリティ責任者）などボードメンバーが参加している。
緊急時対応チーム	Computer Emergency Response Team（CERT）	緊急時の対応チーム。対外的なインシデント報告の窓口。配下のCSIRTを束ねている。
セキュリティインシデント対応チーム	Computer Security Incident Response Team（CSIRT）	支店や子会社ごとに存在する。インシデント対応やガバナンスを担当する。
情報システム/制御システム用セキュリティオペレーションセンター	Information Technology（IT） / Operation Technology （OT） Security Operation Center（SOC）	情報システム（IT）、制御システム（OT）において、セキュリティオペレーションセンターがシステム（発電、送電、配電等）単位で存在する。
コンピテンシーチーム	Competency Team	ベンダー協力のもと脅威情報の管理を行う。制御システム向けのチームは各国に存在する。

Security vs. Compliance (**米国との比較**)

電力業界のセキュリティレベル向上にはさまざまなアプローチがある。



まとめ

海外及び国内重要インフラ事業者のサイバー攻撃対策の実態

・政府の**政策及び各国の文化**によって対策の考え方が異なる。
　　規制型：　　米国・ドイツ・日本
　　インセンティブ型：イギリス

・電力会社においては「組織」「運用」「技術」それぞれに対策が行われており、米国は主に組織体制を整えることにより、**キャリアパス**が確立している。
（魅力ある仕事でなければ、そもそも優秀な人は集まらない。）

・**ITとOTの壁**（組織・運用・技術）は世界中で大きな課題となっているが、今後、技術のIoT化が進む中で、組織・運用の対応が急務となると考えられる。

・日本国内でも、東京オリンピック・パラリンピックに向けて、重要インフラのセキュリティ対策が電力業界では進んでおり、他の業界への波及が望まれる。