経済産業省

資料６－１

電力分野における
サイバーセキュリティ対策について

平成28年６月15日

経済産業省 商務流通保安グループ

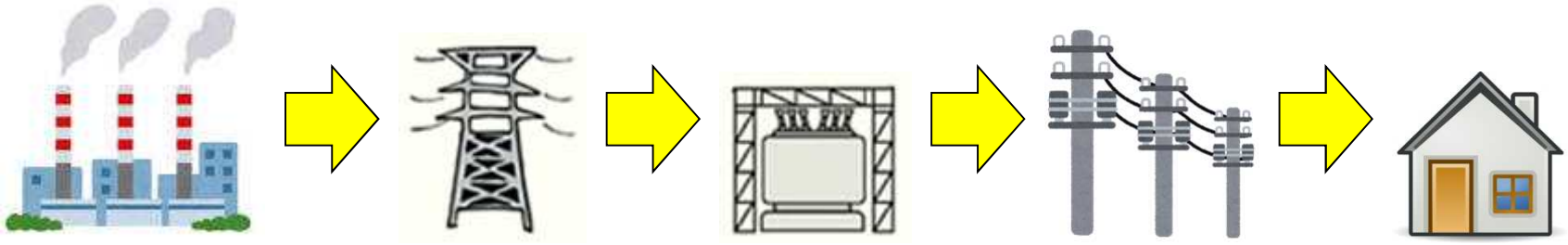
電力安全課

1．電力制御システムの概要

- 適時適切な電力の安定供給のためには、発電所や送電/配電のネットワークとは別に、それらを発電所、中央給電指令所（中給）、制御所等において、監視・制御等を行う制御システムが不可欠。
- それぞれの電力制御システムは、外部との接続点を限定したクローズドなネットワーク構成となっている。

発電 → **流通（送電系統／配電系統）** → **需要家**

電気の流れ



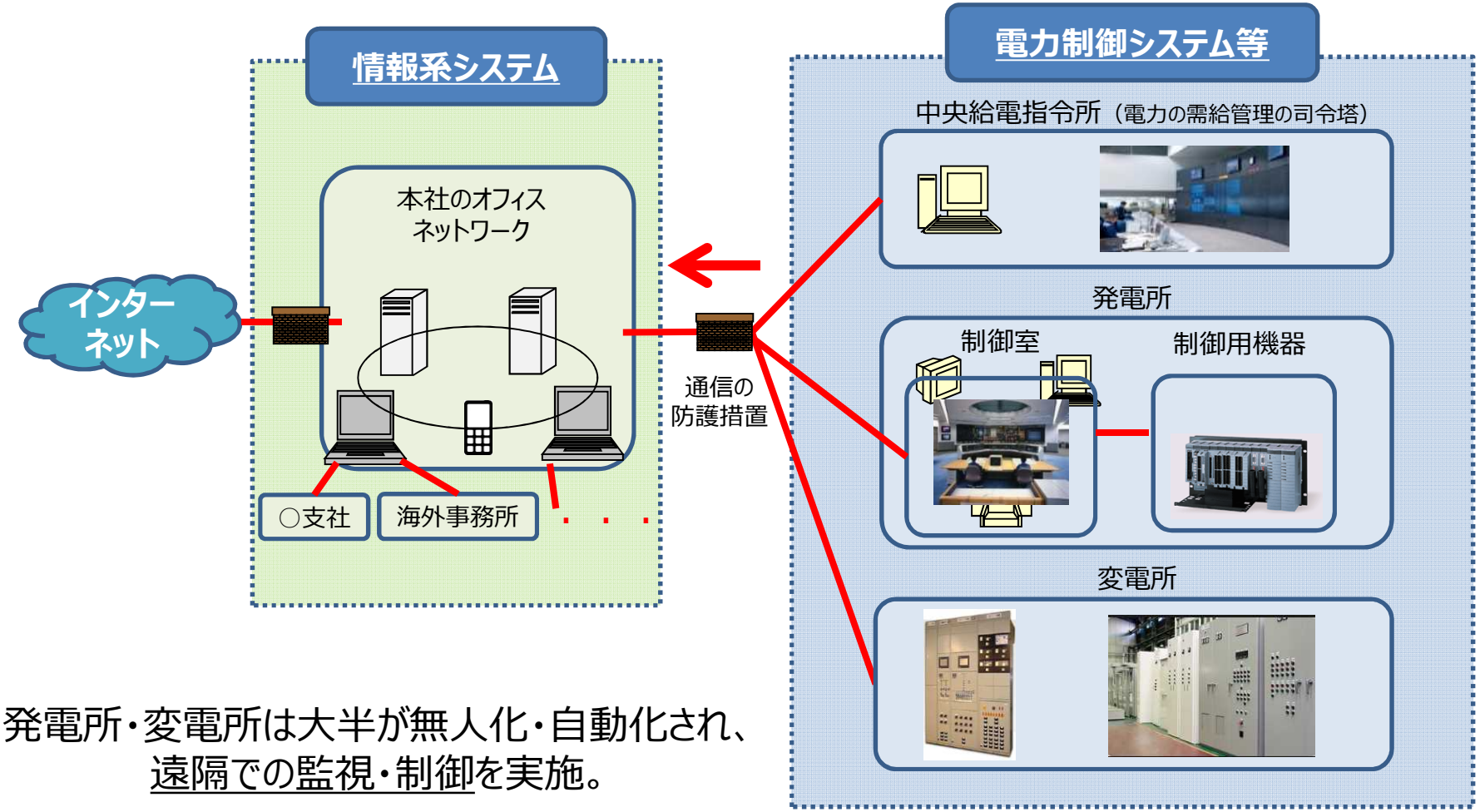
主な電力制御システム

発電所制御システム	需給制御システム	系統制御システム	配電自動化システム	スマートメーターシステム

発電所	中央給電指令所	制御所／電力センターなど

（参考）電力分野における情報システムの模式図

- 電力分野における情報ネットワークは、インターネットとも繋がり、顧客データ等をやりとりする「情報系システム」と、発変電設備等をコントロールする「電力制御システム等」に大別される。
- 両システム間は、基本的に電力制御システム等から情報系システムへ一方向に情報が流れるシステムとなっており、インターネットを介した不特定多数が電力制御システム等にアクセスできないこととなっている。



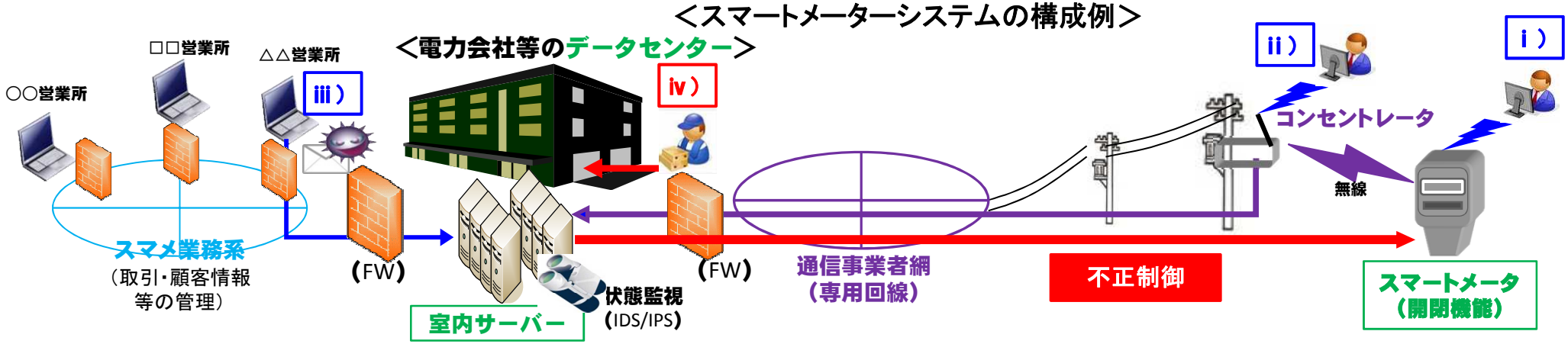
発電所・変電所は大半が無人化・自動化され、
遠隔での監視・制御を実施。

（参考）スマートメーターシステムのセキュリティの脅威と対策について

＜スマートメーターシステムの特徴＞

- スマートメータシステムは、電力設備の制御系ネットワークからは独立したもの。
- 大多数のスマートメーターには、電力供給の開始・停止等を遠隔で行うための**開閉機能を具備**。
- このため、サイバー攻撃等を通じた開閉機能の不正操作により、大規模停電のおそれが指摘。

＜スマートメーターシステムの構成例＞



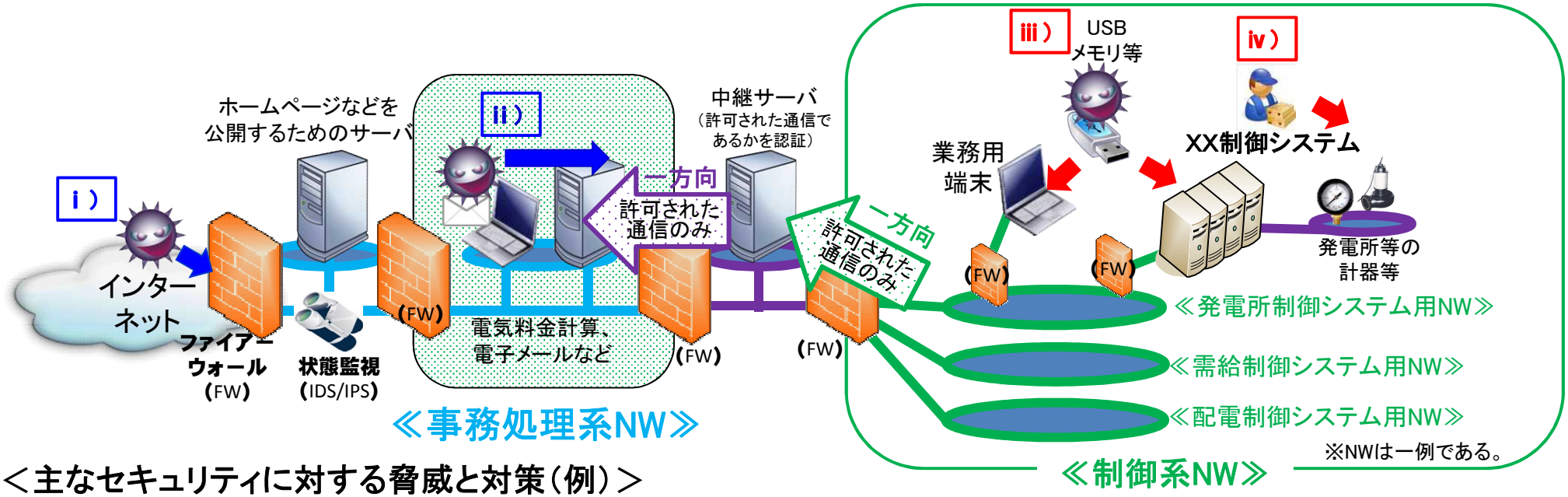
＜主なセキュリティに対する脅威と対策（例）＞

脅威		対策例
・不正アクセス	i）**メーター通信部**に**無線通信により直接不正侵入**して開閉機能を不正制御	・**各種認証**（許可された機器や制御信号のみ接続・受理） ・**データの暗号化等** ・ログ管理による**状態監視**
	ii）**コンセントレータから不正侵入**して開閉機能を不正制御（無線通信による侵入）	・同上 ・上記に加え、**データーセンター**（室内サーバー）**との接続点に多層防御**（ファイアウォールの多段構成、侵入検知等の設置）
	iii）**スマメ業務系**（取引情報・顧客等の管理）**システムからの不正侵入**（マルウェアに感染したメール等による侵入）	・**業務系システムとの接続点は多層防御**（ファイアウォールの多段構成、侵入検知等の設置） ・**開閉機能操作に複数人での操作**（管理者の確認）が必要。 ・ログ管理による**状態監視**
・物理的侵入	iv）**データセンター等の建物へ侵入**して機器を不正操作（物理的に侵入）	・データセンターへの**入退出管理**（カード認証・生体認証等） ・**許可されたUSBのみ接続、　・アクセス認証**（権限の限定化）

（参考）電力制御システムのセキュリティの脅威と対策について

＜電力制御システムの特徴＞

- 制御システム及び制御システム用ネットワークは、インターネットとの直接的な接続点が存在しないため、万が一ウィルスが侵入してもインターネットと直接通信ができないなど、**攻撃の成功が困難**な構成。



＜主なセキュリティに対する脅威と対策（例）＞

	脅威	対策例
・不正アクセス	ⅰ）**インターネットから**（事務処理系ネットワークを経由した）**制御システム用NWへの攻撃**（ネットから侵入）	・インターネットと制御システム用NWとの**直接的な接続・通信の禁止**（事務処理系NWを介した場合は、ⅱ）と同様） ・ログ管理による**状態監視**
	ⅱ）**事務処理系ネットワークから制御システム用ネットワーク**へのウイルスの侵入（マルウェアに感染したメール等による侵入）	・**直接通信の禁止、通信方向の限定、通信許可機器の限定**（中継サーバを経由した一方向かつ特定の機器同士の通信のみ許可） ・ログ管理による**状態監視**
・物理的侵入	ⅲ）USBメモリ等**外部記憶媒体経由でのウイルス侵入**（物理的な侵入）	・**不要なUSBポートを閉塞** ・接続する**USBメモリを限定** ・接続前に**USBメモリのウイルスチェックを実施**
	ⅳ）中央給電指令所、発電所中央制御所等の**建物へ侵入して不正操作**（物理的に侵入）	・中給等の**入退出管理**（カード認証・生体認証等）、・**許可されたUSBのみ持ち込み・接続**、 ・**システムへのアクセス認証**（権限の限定化）

2．経済産業省の取り組み①（電力制御システムの耐性評価）

- 経済産業省は、**電力制御システム**について委託事業を活用して、**耐性調査を実施**。
- その結果、現在の事業環境における**セキュリティ対策**については、**一定の評価を確認**。

＜H25年度経済産業省『電力セキュリティ保安調査』＞

事業名：平成25年度次世代電力システムに関する電力保安調査
委託先　：　株式会社日本総合研究所
委員長　：　新　誠一（電気通信大学）
事業期間：平成25年10月～平成26年2月（委員会は5回開催）

○アンケート（10社）及びヒアリング（3社）を通じて、現状の電力の取組を評価。
・**セキュリティポリシー**は、**電気事業連合会ガイドライン**※に則って、会社全体及び部門ごとに策定・構築。
（※政府の「重要インフラの情報セキュリティ対策に係る行動計画」に基づき、電事連で自主ガイドラインを作成。
一般電気事業者各社が、外部接続の限定等、自主的に取組を実施。）
・**対策や思想**は、外部接続点を限定した**クローズドなネットワーク構成、物理的隔離と入退所管理、記録媒体の持込制限、下請等の要員管理**などを実施。
・**接続管理**（侵入防御）は、**ファイアーウォール**等による**通信経路・方向の限定**、リモートメンテナンス回線の極小化、接続先の認証かつ必要時のみ外部接続などを実施。
・**教育**は、**サイバーセキュリティ演習**（主催：CSSC、電中研）等を通じた対処練度の向上、社員に対する**定期的な意識啓発**を実施。

⇒　これらの取組により、これまで運転制御に影響のあるセキュリティインシデントは発生しておらず、
“現状のセキュリティ対策としては一定の評価ができる”

○今後の事業環境変化を踏まえた“**提言事項**“
①マネジメントシステムの確立　②外部接続点の対策徹底
③業界横断的な情報共有　④セキュリティ人材の訓練・育成
⑤電力自由化を見据えたサイバーセキュリティガイドラインの策定等

3．経済産業省の取り組み②（欧米の電力システム調査）

- 平成26、27年度、欧米の電力システムにおけるサイバーセキュリティーに係る制度や対策の実態を調査。
- そのアプローチ(規制のみ（独）、電力会社の自主性の尊重（英）、それらの組み合わせ（米））に違いあり。
- 日本としては、米国型アプローチをベースに、規制により一定のセキュリティを確保した上で、事業者の自主的な更なる取り組みを促していく方向か。

□ 調査対象

【平成26年度：アメリカ】
サイバーセキュリティガイドライン作成・運用機関、政府関連機関、監督官庁、電力会社
【平成27年度：EU、イギリス、ドイツ】
EU関係機関、政府関係機関、電力会社、電気工作物のベンダー

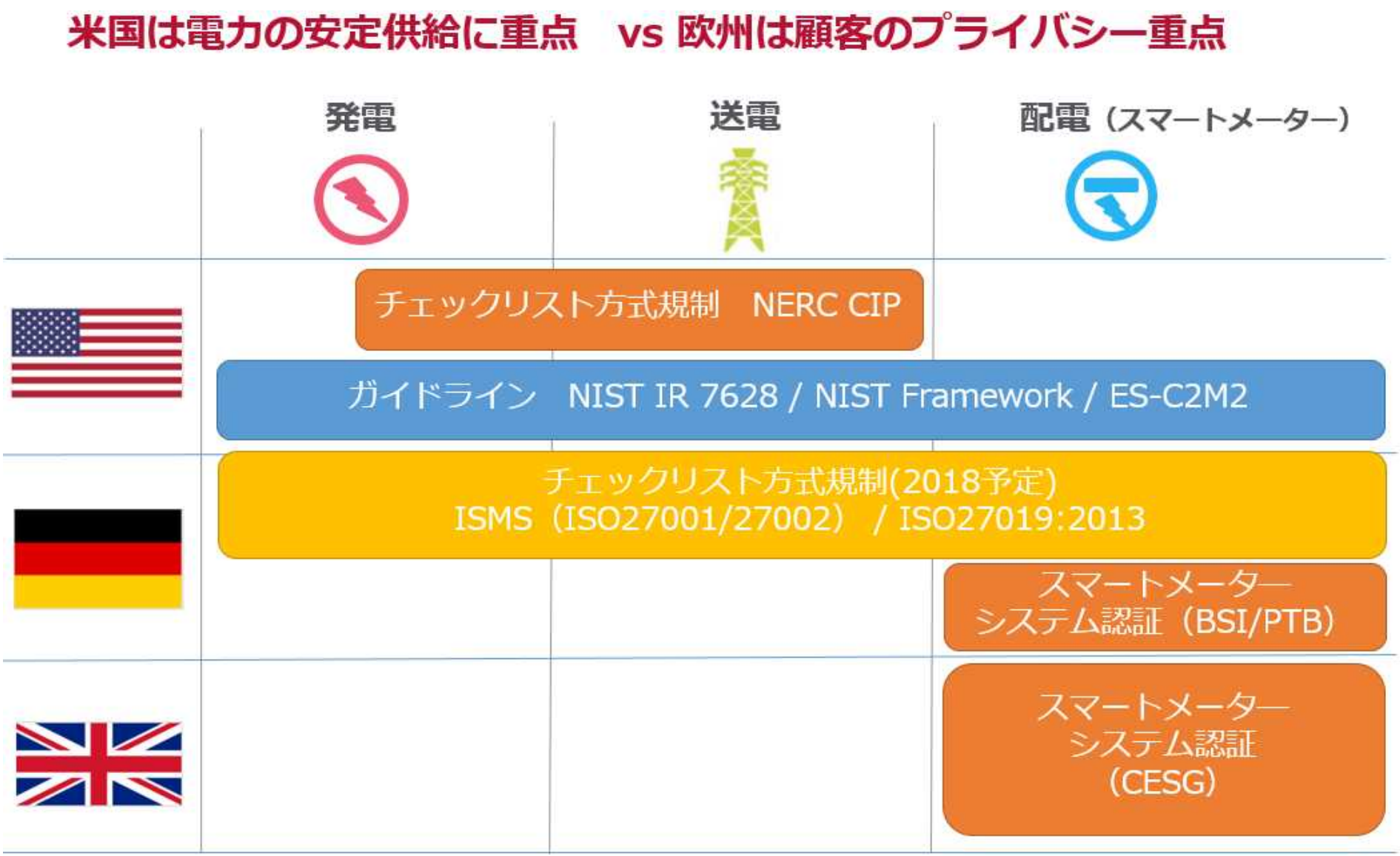
□ 調査結果

【アメリカ】
・セキュリティ対策は、電力の安定供給の確保が主目的。
・「遵守義務のある規制」＋「経営リスクに応じたリスクベースアプローチ」の併用。
【イギリス、ドイツ】
・セキュリティ対策は、プライバシー保護が主目的。スマートメーターシステムへの適用が先行。
・イギリスは、「リスクベースアプローチ」のみ。ドイツは、「規制」のみ（2018年適用予定）。

□ 調査結果を踏まえ日本がとるべきアプローチ

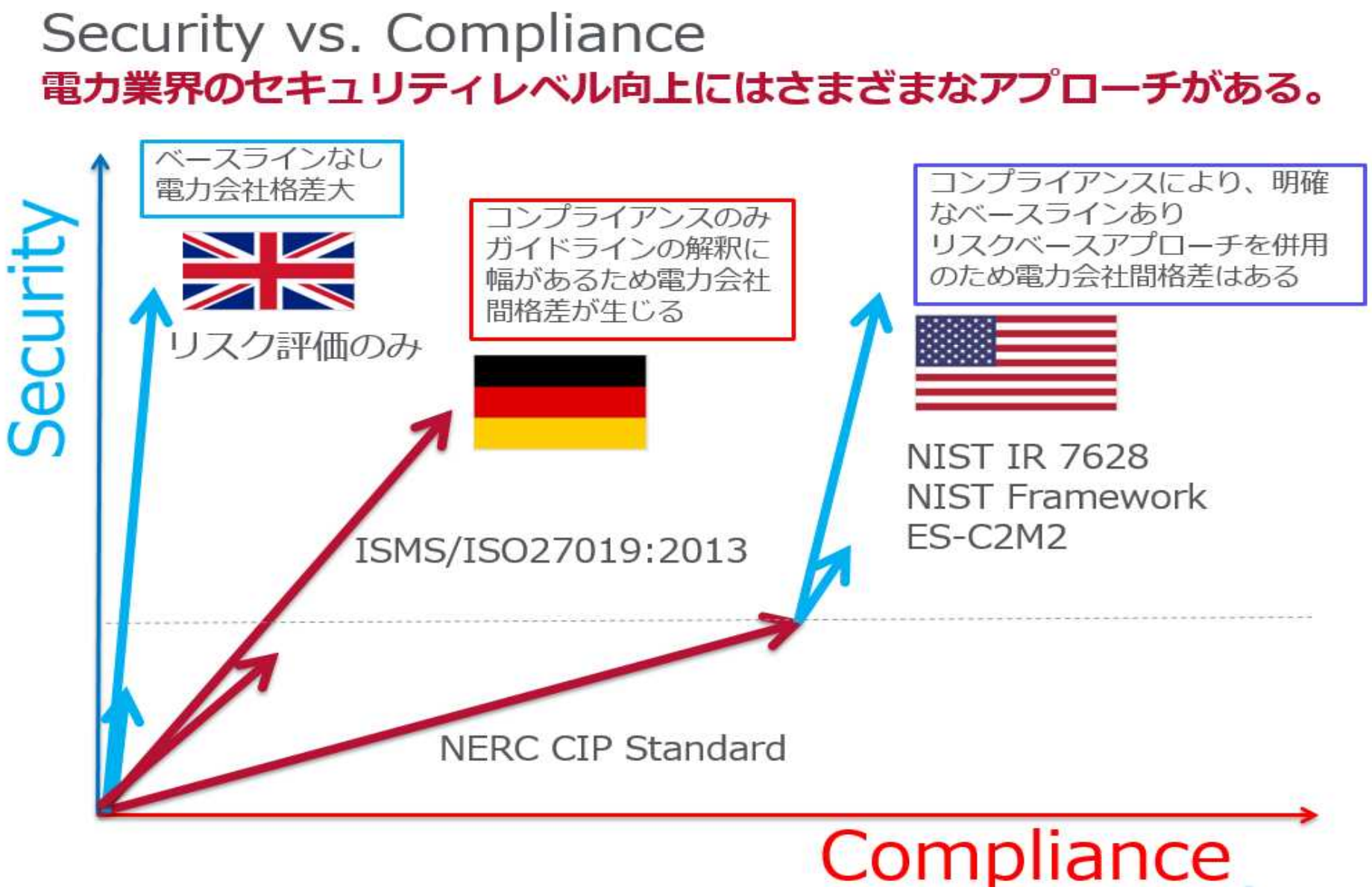
①アメリカのアプローチを参考にして、規制によりベースラインを確保しつつ、インセンティブ等により企業のセキュリティ文化を形成。
②「自主保安」の思想の下、電力会社が、自ら第三者によるガイドライン適合に関する監査を定期的に実施。
③官民が協力し、インシデント、ベストプラクティス等の情報共有や分析機能を強化。

（参考）米英独の規制・ガイドラインのマッピング



（出典）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）報告書

（参考）米英独のアプローチの違い



（出典）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）報告書

４．経済産業省の取り組み③（民間ガイドラインの法令への位置づけ）

○第10回電力安全小委員会（平成27年6月26日）での審議を踏まえ、民間団体において策定されたサイバーセキュリティ対策に関する２つのガイドライン（スマートメータ、制御系）を、技術基準（ハード対策）及び保安規程（マネジメント等ソフト対策）に位置付け（電気事業法の省令に根拠規定を追加した上で、当該ガイドラインをエンドース）。（平成28年8月頃に措置予定）

＜スマートメータシステム　セキュリティガイドライン＞

・平成27年2月　資源エネルギー庁を中心としたスマートメーター制度検討会セキュリティ検討WGにて、ガイドライン策定要件等をとりまとめ。

・平成28年3月　第85回JESC委員会にてガイドライン策定。

＜電力システム（制御系）セキュリティガイドライン＞

・平成26年9月　日本電気技術規格委員会（JESC）で検討開始。

・平成27年6月　同委員会情報専門部会を新たに設置。

・平成28年5月　第86回JESC委員会にてガイドライン策定。

（共通事項）

■ 事業者が実施すべき「勧告的事項」と、実施の要否を個別に判断すべき「推奨的事項」に分類。

■ セキュリティ管理組織の設置及びマネジメントシステムの構築、教育の実施等を「勧告的事項」として記載。

機器	・セキュリティ仕様 ・ファームウェアアップデート
通信	・通信プロトコル ・暗号 ・ネットワーク分離
システム	・コマンド管理 ・外部記憶媒体利用制限
運用	・管理者権限管理 ・ログ取得 ・データ管理
物理	・セキュリティ区画保護 ・アクセス管理

設備・システム	・ネットワーク分離 ・通信データ保護 ・不正処理防止 ・アクセス制御
運用・管理	・セキュリティ仕様 ・データ管理 ・管理者権限割当 ・セキュリティパッチ

＋

安定供給等の観点から、システムの重要度を定義

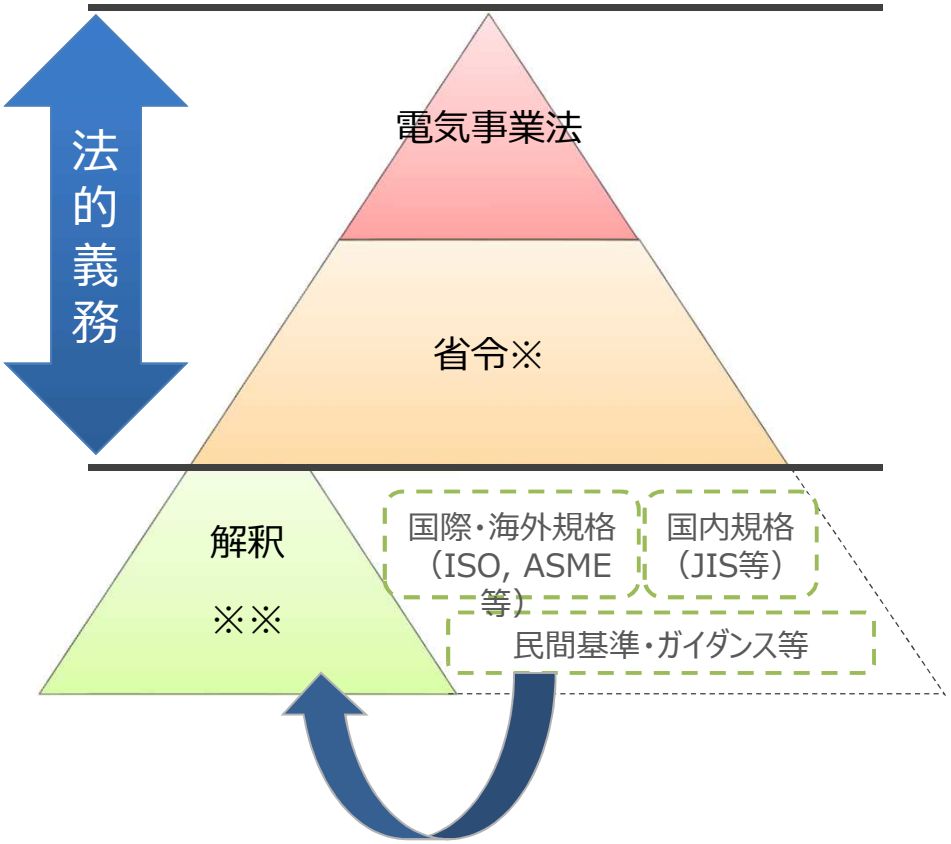
↓

重要度に応じた追加的セキュリティ対策を提示

・ログの取得　・入退管理

（参考）技術基準への位置づけのイメージ

○ 電気事業法第３９条により、事業者に省令で定める技術基準への適合維持を義務づけ。
○ 技術基準省令へサイバーセキュリティの確保を要求。
○ 技術基準省令に適合する基本的な仕様規定である解釈にＪＥＳＣガイドラインを位置づけ。
(十分な保安水準の確保が達成できる技術的根拠があれば、解釈の記載内容に限定されるものではない)



ＪＥＳＣ規格を解釈で引用。
（省令に適合するものであることの明確化）

※条文のイメージ
（サイバーセキュリティ対策）
第○条　電気工作物を制御する電子計算機は人体に危害等を及ぼさないよう、又は電気の供給に著しい支障を及ぼすおそれがないようサイバーセキュリティを確保しなければならない

※※条文のイメージ
【サイバーセキュリティ対策】（省令第○条）
第△条　省令第○条に規定するサイバーセキュリティの確保は次の各号によること。
一　スマートメーターシステムにおいては、日本電気技術規格委員会規格　ＪＥＳＣ　○○○（２０１６）「スマートメーターシステムセキュリティガイドライン」によること。
二　電力制御システムにおいては、日本電気技術規格委員会規格　ＪＥＳＣ　○○○（２０１６）「電力制御システムセキュリティガイドライン」によること。