電気エネルギーシステムにおける サイバーセキュリティ

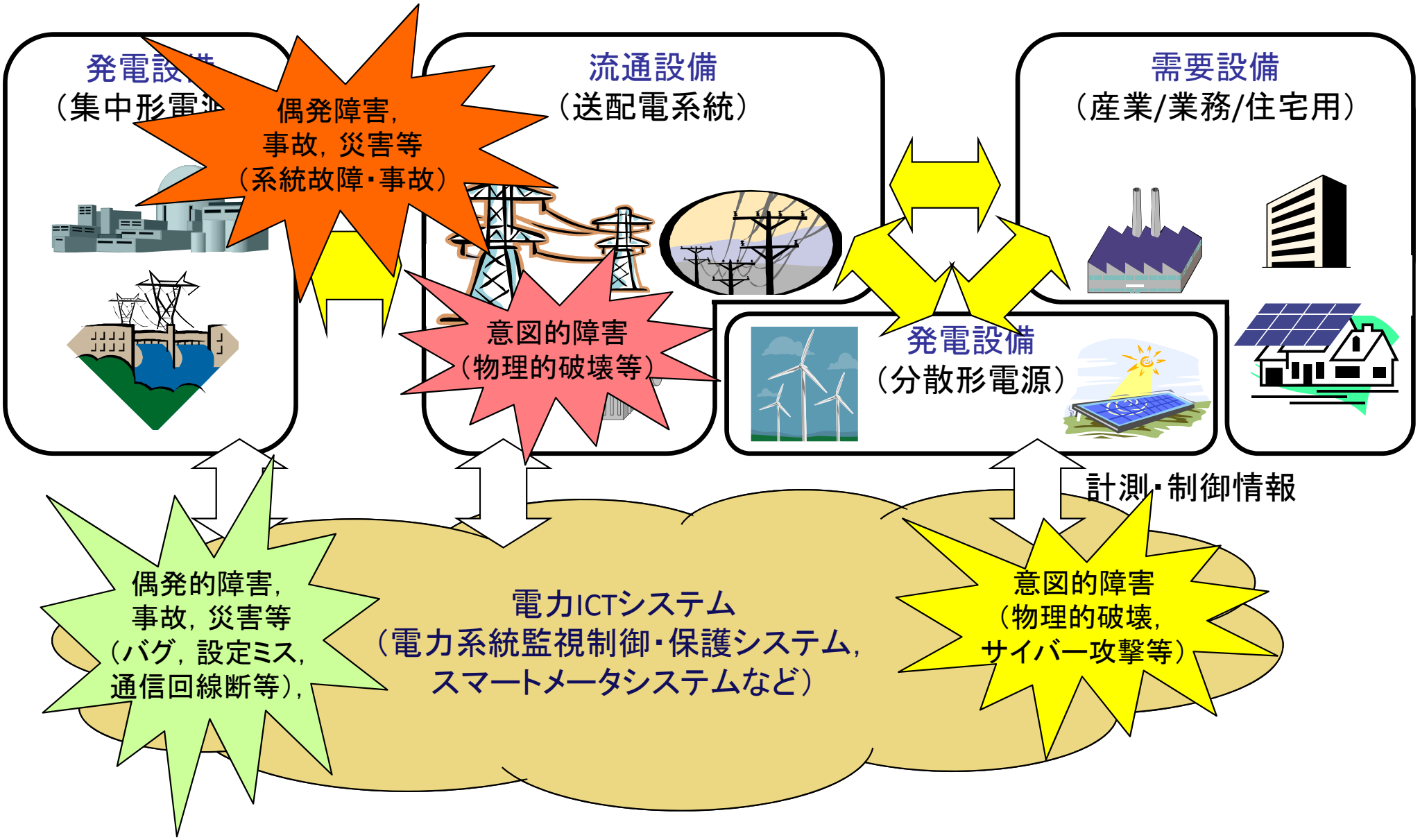
電力中央研究所　システム技術研究所

芹澤　善積

電気学会　公開シンポジウム
「電気エネルギーの未来を考える」
2016年2月24日

電力中央研究所

電気エネルギーシステムへの脅威



偶発的／意図的障害とセーフティ／セキュリティ

<table>
<tr><th colspan="2">脅威</th><th colspan="2">保護資産</th></tr>
<tr><th>分類</th><th>内容</th><th>物質的資産
（設備，人身など）</th><th>非物質的資産（情報，サービス，社会的イメージなど）</th></tr>
<tr><td rowspan="3">偶発的</td><td>天災（地震，火災，水害，落雷など）</td><td colspan="2" rowspan="3">セーフティ（機能安全）
（信頼性，可用性，保守性）</td></tr>
<tr><td>故障（ハードウェア／ソフトウェア障害，回線故障，過負荷など）</td></tr>
<tr><td>過失（データ入力ミス，運用ミス，ソフトウェアバグ，誤接続など）</td></tr>
<tr><td rowspan="2">意図的</td><td>第3者の不正行為（システムへの不正アクセス・操作，破壊行為など）</td><td colspan="2" rowspan="2">セキュリティ（サイバーセキュリティ）
（機密性，完全性，可用性，真正性，
責任追跡性，否認防止，信頼性）</td></tr>
<tr><td>当事者の不正行為（情報窃取・漏えい，罷業など）</td></tr>
</table>

- ✓ 機能安全：監視装置や防護装置などの付加機能によりリスクを低減すること
- ✓ リスクは資産価値，脆弱性，脅威（発生確率）の関数
- ✓ システムの拡大・高度化などにより脆弱性や脅威も多様化

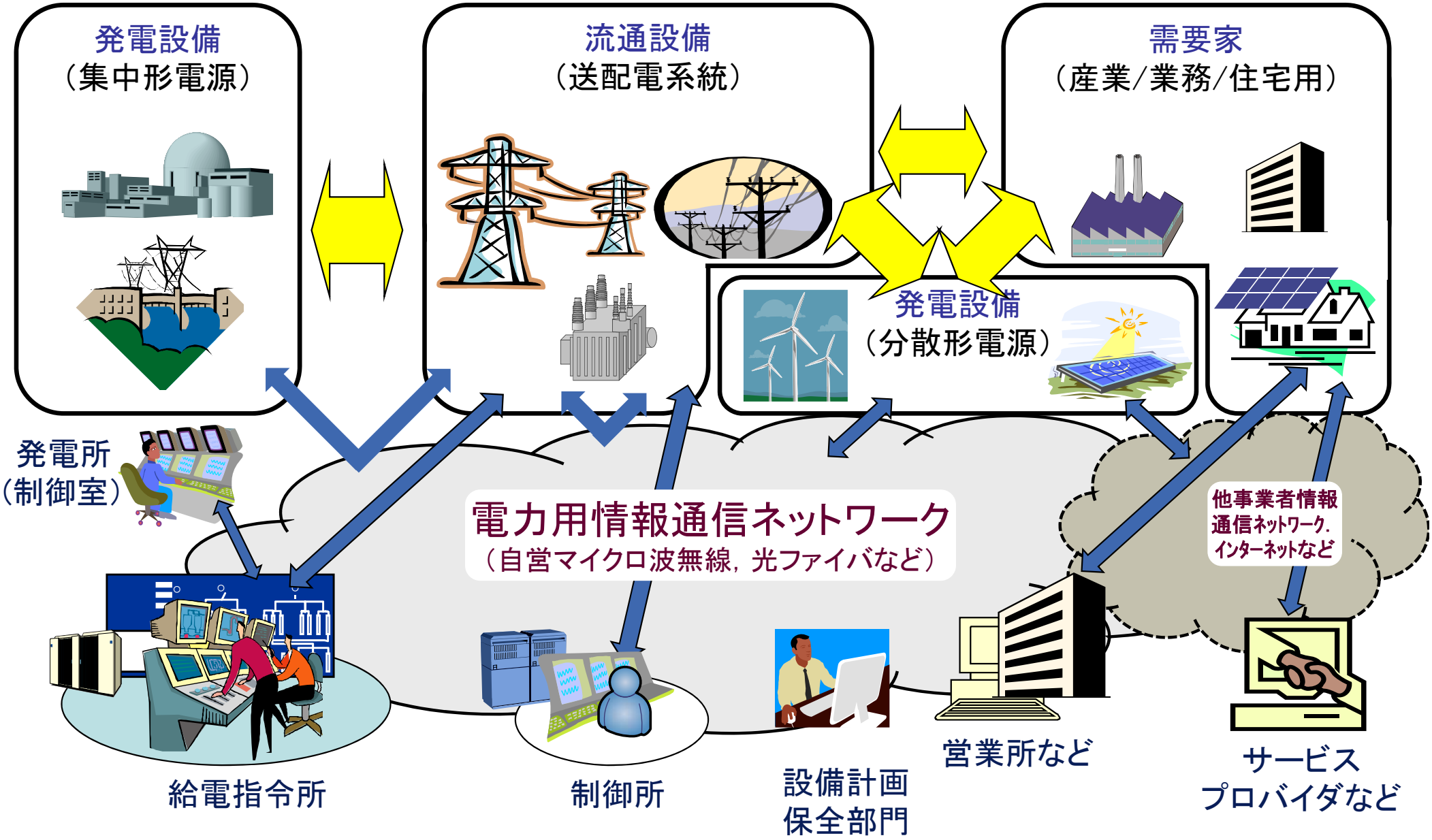
参考：福澤ほか，「Cyber Physical Systemのリスク管理技術と情報セキュリティ心理学によるアプローチ」，電学論C, Vol. 134, No. 6, pp. 756-759, 2014/6

目次

- 電気エネルギーシステムにおけるICTシステム（電力ICTシステム）の概要
- 電力ICTシステムの偶発的障害に対するセーフティ確保の取組み
- 電力ICTシステムのセキュリティ確保の取組み

電力ICTシステムの概要

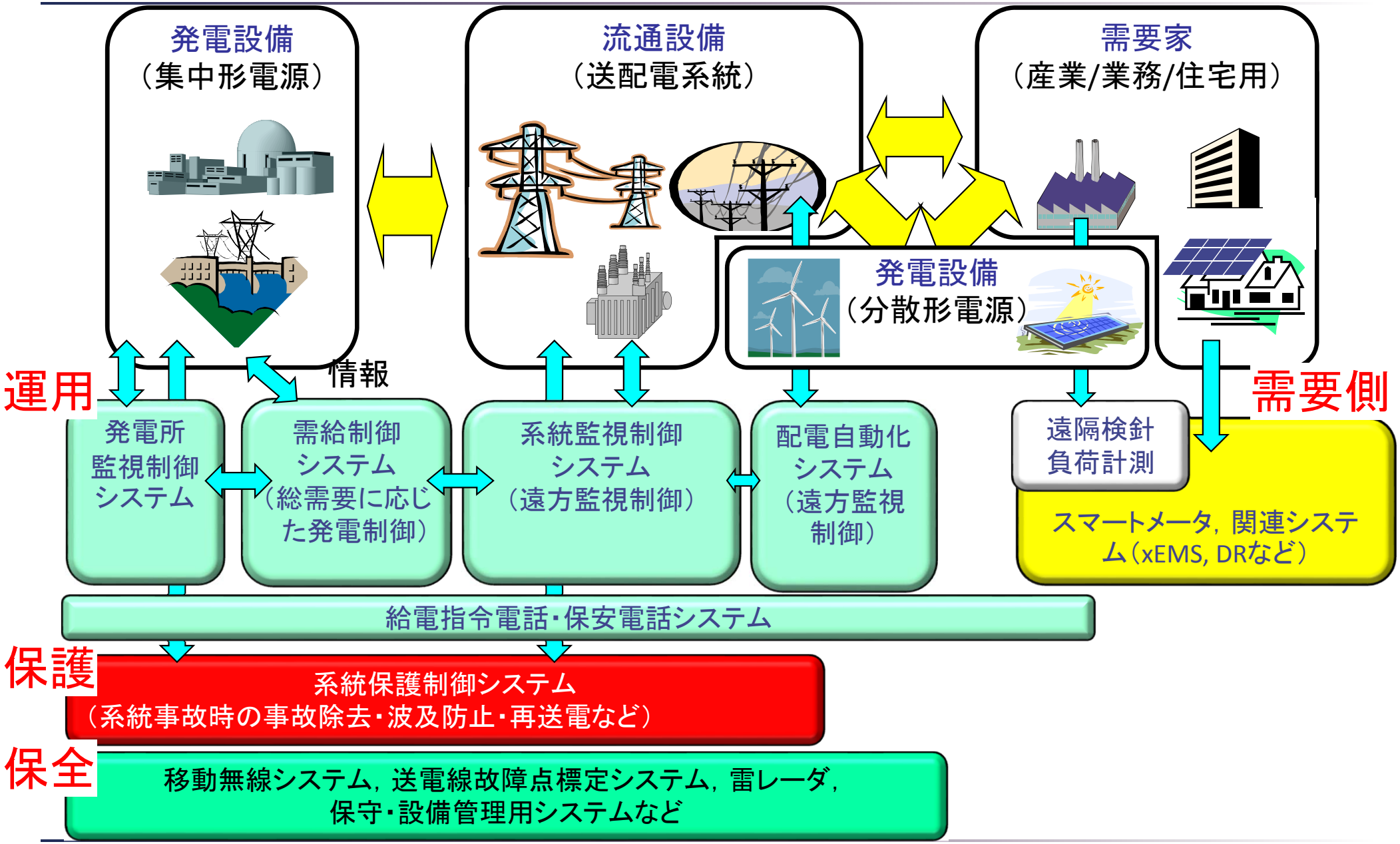
電力系統とICTネットワーク



電力ICTシステムの適用先

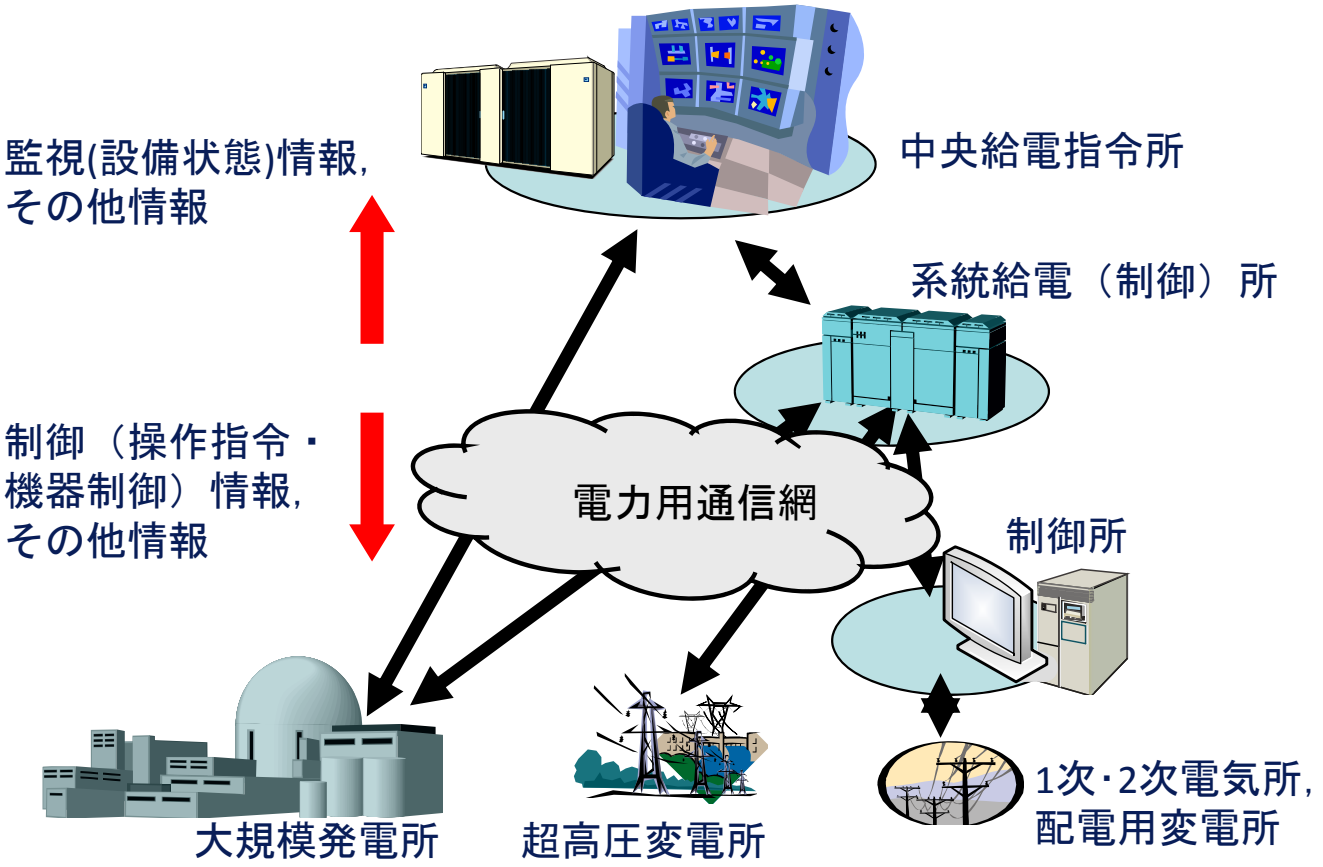
- 系統運用（平常時の電力品質と経済性の維持）
  - 電力系統の状態計測，遠隔監視制御（操作）
  - 自動給電（周波数調整，経済的発電量配分指令，潮流・電圧制御）
  - 給電指令電話
- 系統保護（緊急時の供給信頼性維持）
  - 送電線・母線・変圧器などの事故時遮断（切り離し；事故除去）
  - 過負荷や周波数・電圧異常，不安定化の未然防止・制御（負荷・発電機遮断，系統分離など）（事故波及防止）
- 設備保全（設備の健全性の維持）
  - 電力設備の状態監視（画像など），雷監視，故障点標定，保守・点検用現場支援通信など
- 需要家通信
  - 負荷計測，遠隔検針・制御（スマートメータ），需要家サービス情報提供など
- 一般業務用通信

電力系統とICT適用システム



系統運用(給電・設備監視制御の自動化)

- 系統運用者
- 計算機制御システム，HMI，データベース，エンジニアリング支援
- 通信ネットワーク(広域/ローカルネットワーク)



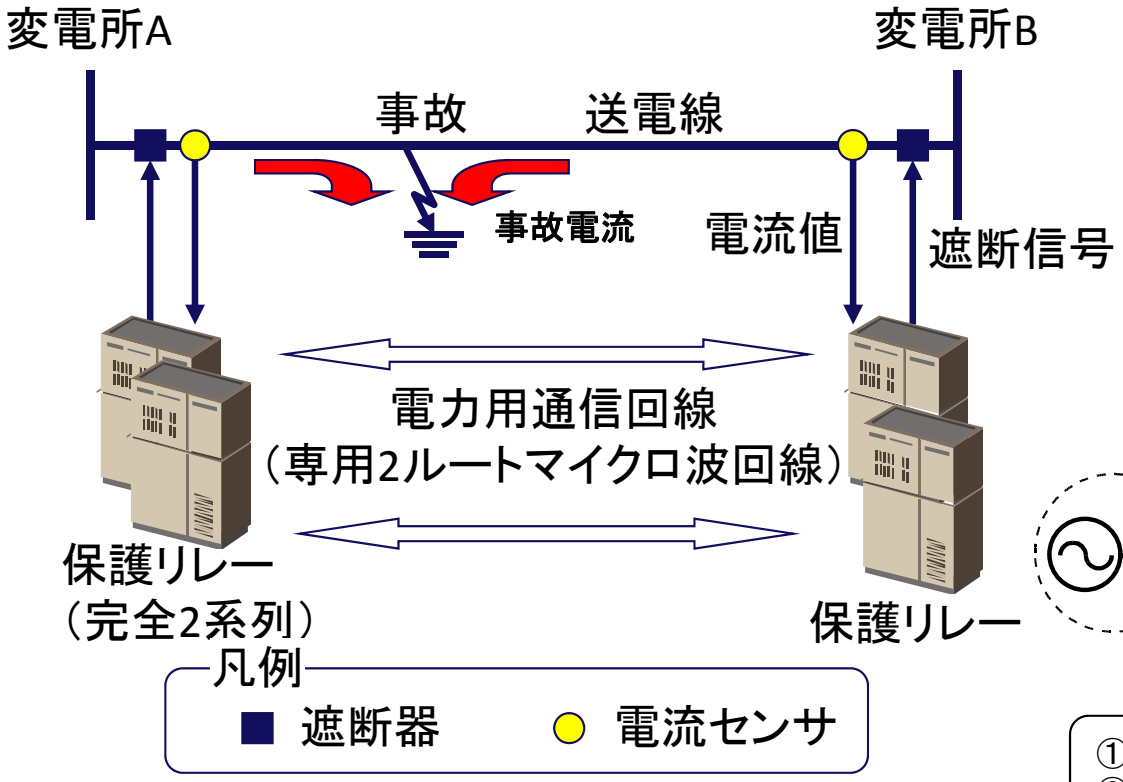
系統運用システムの現状と今後

- 大規模発電所の監視制御・保護・保全
  - 計算機制御システム（プラント毎のベンダ依存）
- 給電・送変電設備監視制御（自動化）
  - 計算機制御システムのオープン（汎用・標準技術適用）・分散化
  - 広域・構内通信ネットワークはサイクリック・シリアル通信方式から IP（インターネットプロトコル）方式へ
  - 上位通信プロトコル，データ定義は独自（一部共通仕様あり）

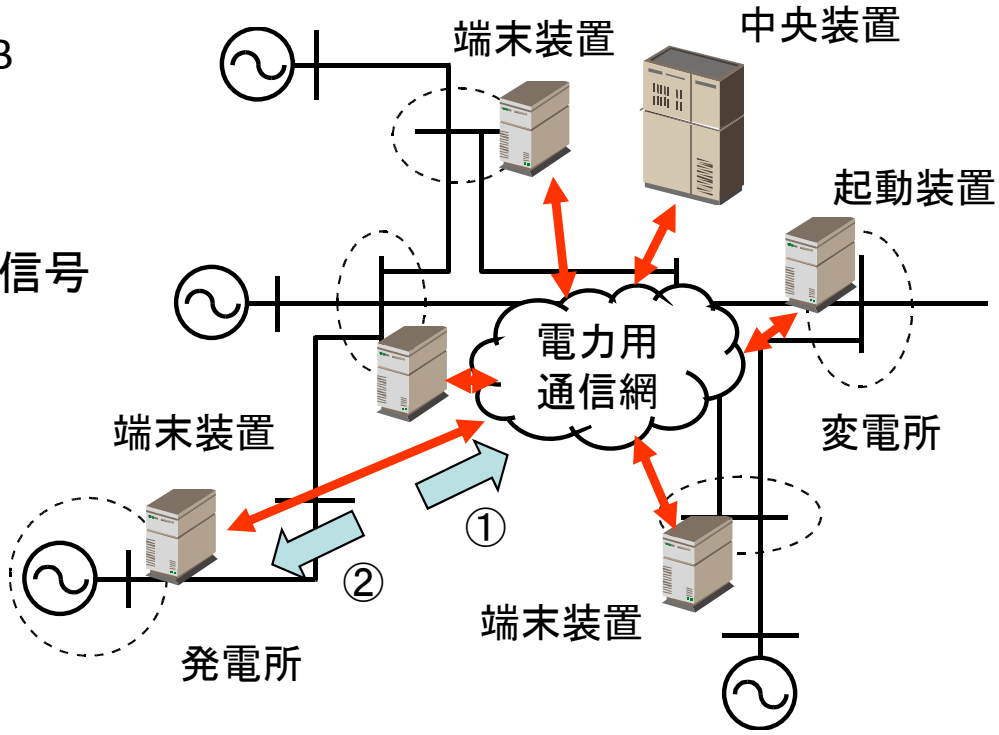
  - 国際標準通信プロトコルへの対応，国内共通化・標準化
  - 再生可能エネルギー電源（太陽光，風力など）の大量導入や電力システム改革に伴う
    系統状態監視の詳細化

系統保護システム

事故除去システム（電流差動型送電線保護リレー）



事故波及防止システム・系統安定化制御システム



①上り情報：系統情報（事故前後），起動情報（事故検出）
②下り情報：指令（発電機抑制・遮断，負荷遮断，系統分離）

電力系統事故の約7割は雷撃が原因

系統保護システムの現状と今後

- 事故除去，自動再閉路，事故波及防止・系統安定化など
- 送電系統のシステムはほぼ完備（対象系統毎に最適化）
- 極めて高い信頼性やリアルタイム性が必要
- 配電系統は通信に依存しない局所的保護と故障区間分離主体
- 復旧制御は運用者による系統状況の把握と操作
- 個別システム毎に専用化（システム間のデータ連携や動作連携はほとんどなし）

- 再生可能エネルギー電源大量導入などに伴う送配電系統の保護制御機能の強化，広域化
- 保護系通信システムのレガシー機器対策としてIP化を指向（通信ネットワークの独立性は維持）

需要側システムの現状と今後

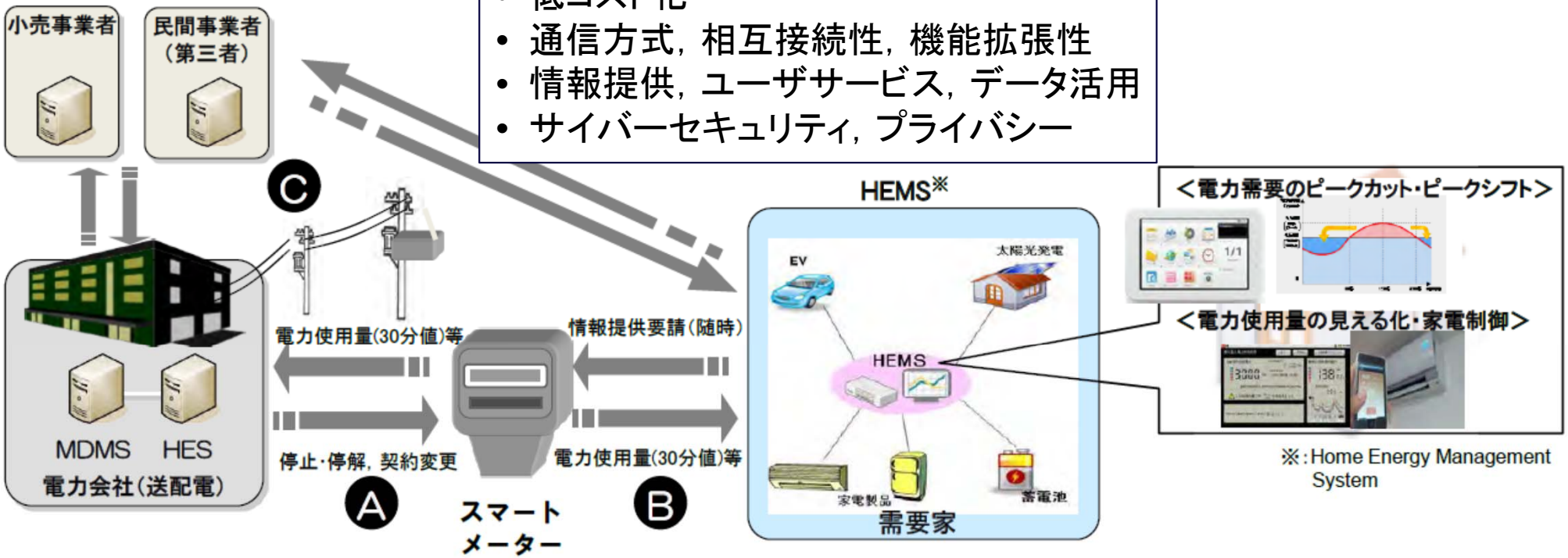
- 特別高圧需要家は専用通信線にて監視・保護・検針・ロードサーベイ・需要調整，高圧需要家も検針可，自営エネルギー管理システム
- 低圧需要家向け計量・各種作業は人手中心，遠隔自動検針・停止/停解操作（スマートメータ）の導入開始（柱上集線装置まで光ファイバ通信＋ラストkm無線/PLC，携帯電話）
- 通信事業者ネットワークは需要家まで到達，広帯域化，宅内ネットワークは通信・放送系のみ

- スマートメータの効率的導入（コスト，期間，自営/事業者通信ネットワーク）と運用，データ活用
- エネルギー利用の見える化と需要調整（デマンドレスポンス；DR）
- 分散形エネルギー電源（DER）大量導入時の動作監視・出力制御（中央給電所からの制御?）
- 需要家内のエネルギー機器（HP，EVなど）の最適管理および管理用ネットワークシステム

スマートメータに関わる情報の授受

- Aルート：スマートメータ⇔HES⇔MDMS；AMI
- Bルート：スマートメータ⇔ HEMS（ECHONET Lite）
- Cルート：電力会社⇔小売事業者/サービスプロバイダ⇔xEMS；関連システム（DR，アグリゲータ，再エネ出力制御等）

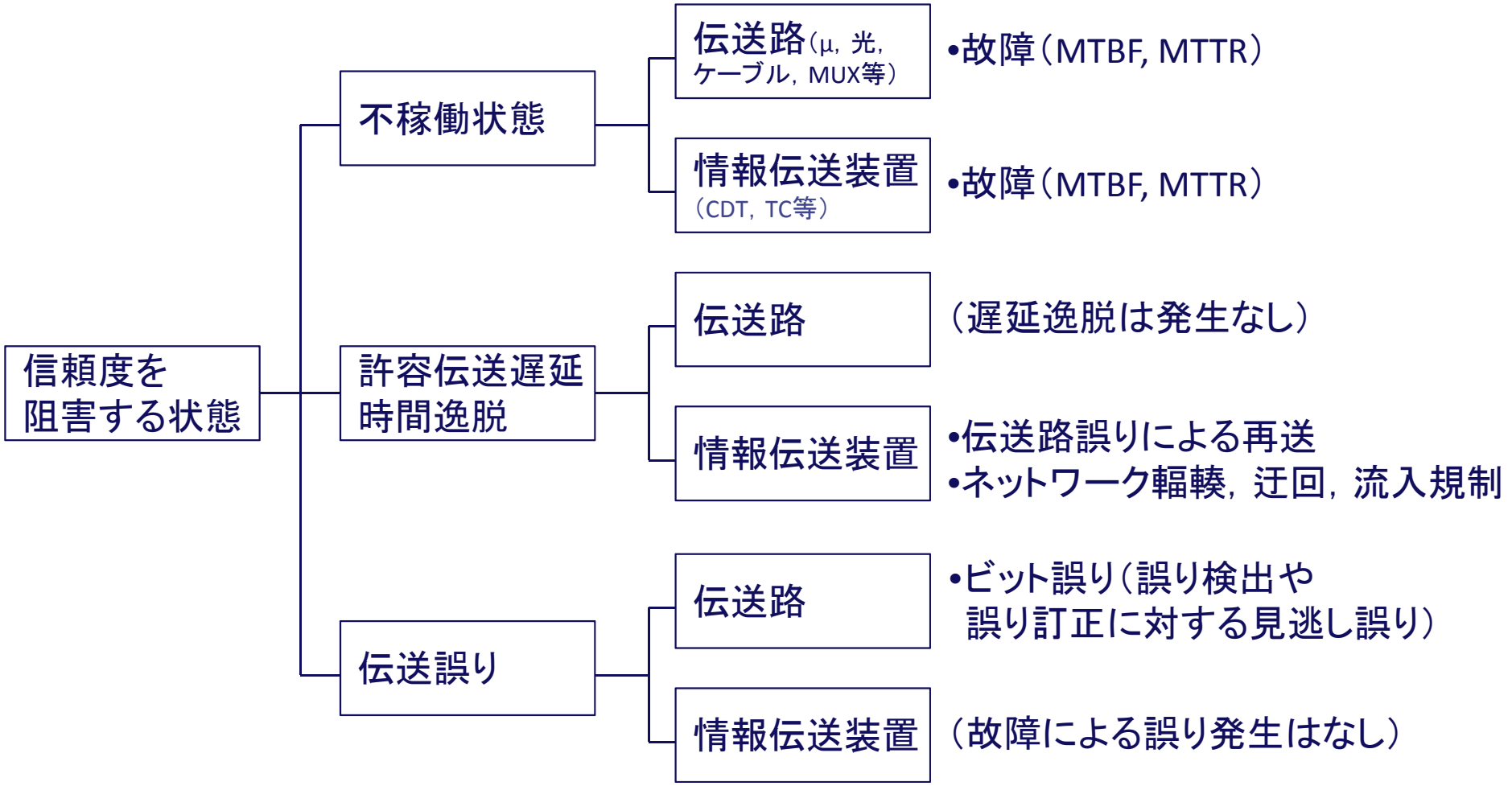
＜課題＞
- 低コスト化
- 通信方式，相互接続性，機能拡張性
- 情報提供，ユーザサービス，データ活用
- サイバーセキュリティ，プライバシー



参考：経済産業省「スマートメーター制度検討会（第15回）-配布資料」

電力ICTシステムの偶発的障害に対するセーフティ確保の取組み

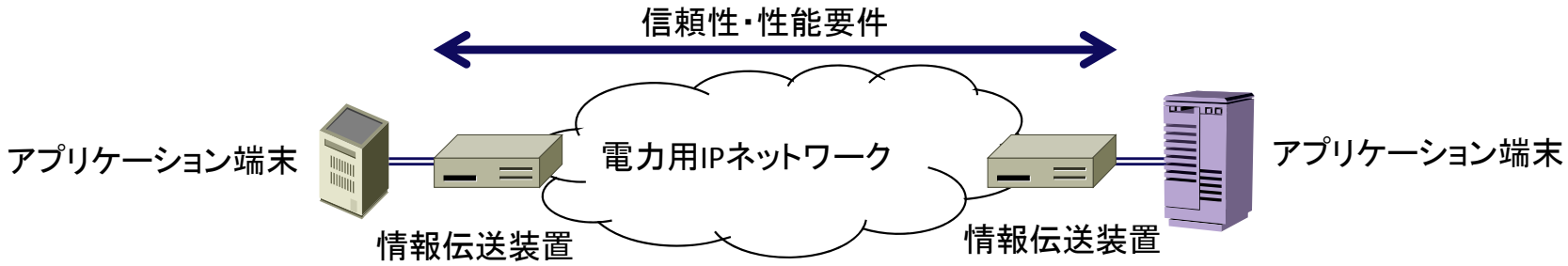
給電情報伝送システムの信頼度阻害要因



出典：電気協同研究55巻1号「給電情報伝送システムの信頼度評価とシステム設計」（1999年）

監視制御システムの信頼性・性能要件

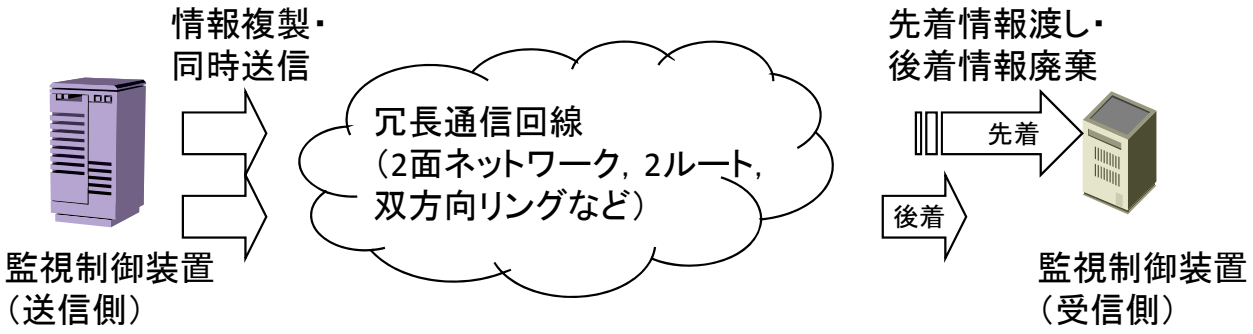
アプリケーション		通信区間	不稼働率	伝送遅延時間	情報途絶猶予時間
給電運用（需給調整）	電力系統監視	給電指令所 ⇔ 発変電所	$< 7 \times 10^{-5}$	< 3 to 10 s	監視: < 18 s 制御: < 2 s
	自動給電	給電指令所 ⇔ 発電所	$< 2 \times 10^{-5}$	< 2 to 5 s	
監視制御	遠隔監視制御 ダム監視制御	制御所 ⇔ 発変電所・ダム	$< 7 \times 10^{-5}$	監視: < 2 to 4 s 制御: < 0.5 s	
	配電自動化	制御所 ⇔ 配電線フィーダ	$< 7 \times 10^{-5}$	< 0.5 to 3 s	
設備管理	通信運用監視	通信ネットワーク管理センタ ⇔ 通信局・中継局	$< 7 \times 10^{-5}$	< 7 to 33 s	–
	映像遠隔監視	監視箇所 ⇔ 被監視箇所（現場）	–	< 2 to 3 s	–
給電指令	給電用電話	給電指令所・制御所 ⇔ 発変電所	$< 7 \times 10^{-5}$	< 150 or 250 ms	–



出典：電気協同研究58巻4号「電力用通信網へのIPネットワークの適用性評価・システム設計技術」（2002年）

監視制御システム用冗長伝送方式

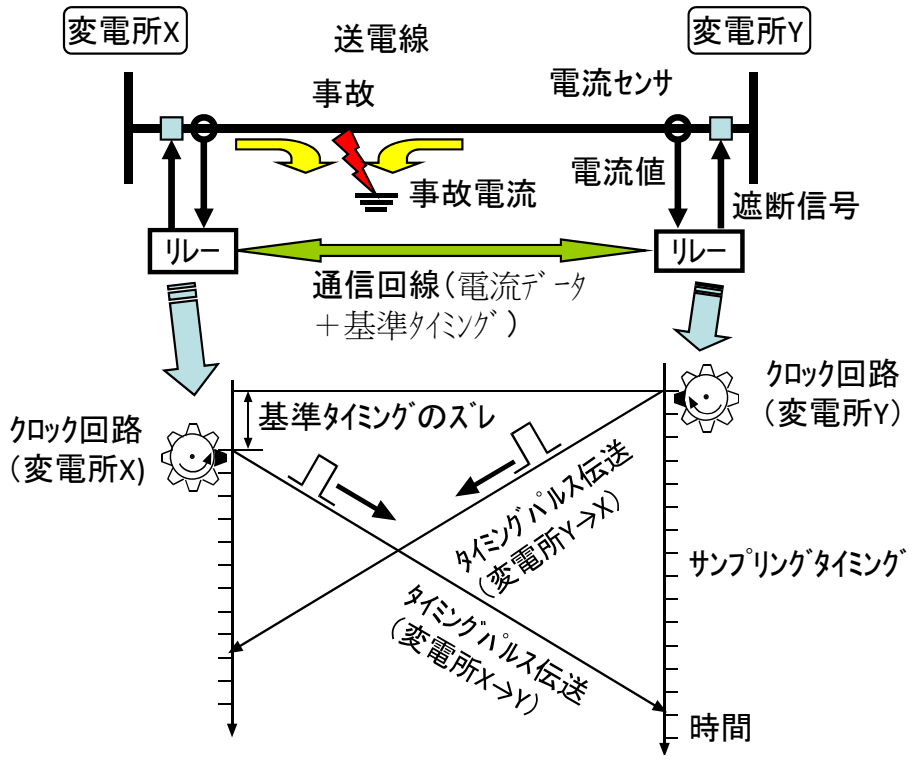
機能	動作内容
2ルート送信・後着廃棄	• 情報をコピーし2系列同時送信し，受信側で先着情報を渡す • 後着情報は廃棄
送達確認・再送	• 情報のシーケンス番号を管理し，順序と連続性を確認 • 確認できない場合には要求により再送
連送・後着廃棄	• 同一情報を連続送信 • 後着情報は廃棄



送電線保護システムの性能・信頼性要件

PCM電流差動リレーシステム

項　　目	要　求　条　件
絶対伝送遅延	2.5～5 ms以下
伝送遅延変動	±20 μs以内
上り下り遅延差	160～200 μs以下
ビット誤り率	1×10^{-7}以下
回線瞬断率	5×10^{-5}以下
システム不稼動率	1×10^{-7}以下



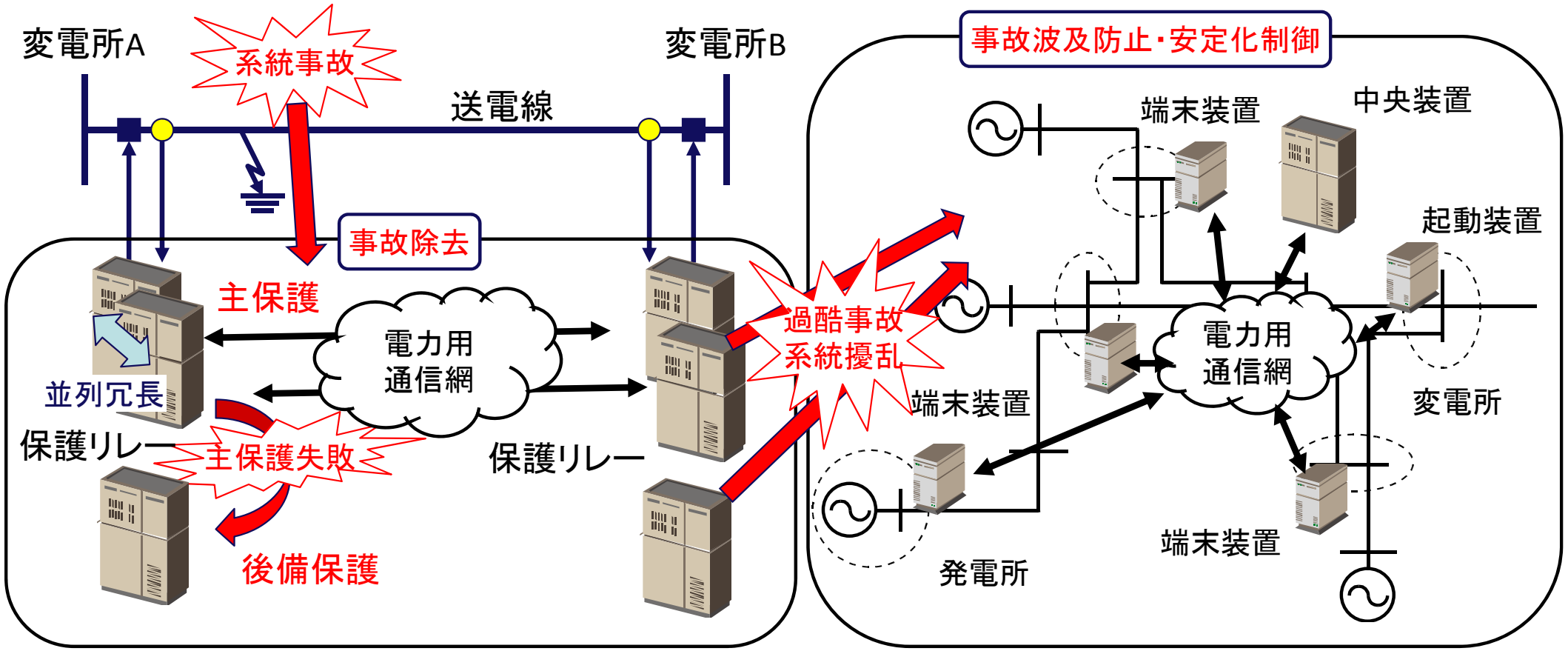
保護リレー装置信頼度向上の考え方

信頼度向上策	ねらい	具体例
固有信頼度の向上	•壊れないものを作る •ソフトウェアバグのないものを作る •系統の要求に合致したものを作る	•ハードウェア信頼度の向上（ファンレス等） •ソフトウェア信頼度の向上* •電力系統解析技術の向上
不良発生の防止	•壊す要因を排除し壊れにくいものとする	•サージ対策
直列多重化	•壊れても直ちに誤動作につながらない構成とする	•事故検出リレーによるフェイルセイフ
自動監視の適用	•稼働信頼度の向上（壊れたらすぐに発見・修復し，系統事故との同時発生を避ける）	•常時監視の適用 •自動監視の適用
多系列化	•装置不良と系統事故との同時発生に備え，保護の確実化を図る	•2系列化

＊）高位言語によるソフトウェアのビジュアル化，シーケンス図からのソフトウェア製作の自動化，ソフトウェアのモジュール化による再利用など

出典：大浦監修：「保護リレーシステム工学」，電気学会

系統事故に対する多重防護



電力ICTシステムのセキュリティ確保の取組み

諸外国での電力システムに関連するインシデント事例

対象	発生国	発生時期	被害内容	原因
ウラン濃縮施設	イラン	2010年	ウラン濃縮施設における約8,400台の遠心分離機がすべて停止	マルウェア（Stuxnet）のコンピューター感染
スマートメーター	米国	2009年	電力消費量記録の改竄	インターネット上で調達可能なソフトウェアによるハッキング
業務システム	米国	2009年	重要データの社外漏洩 / 需給予測システムへの攻撃（未遂）	アクセス権限抹消に要するタイムラグを不正に利用された
SCADAシステム	米国	2007年	SCADAシステムにアクセス可能なPCのアクセス権限が不正に取得された。	フィッシングメール+Windows DNSの脆弱性
系統監視制御システム（アリゾナ州）	米国	2007年	141の分配回路ブレーカーが開き、98,700人の顧客を巻き込む停電が発生	SCADAシステムのベンダがアプリケーションを自動更新し、それを電力施設に伝えなかった。
原子力発電所（ブラウンズ・フェリー）	米国	2006年	発電所の再循環水ポンプが制御不能	発電所統合ネットワーク上の過度の情報量による制御装置の不調
送電システム	米国・カナダ	2003年	米国北東部とカナダでの電源障害	ハッカーがグリッドのセキュリティを侵害するために一日で約100回攻撃
発電所監視システム	米国	2003年	265の発電所で、508ユニット分の発電機が停止（61,800MW相当）	SCADAシステムのアラームプロセッサー障害により、オペレーターが適切に運用できず
原子力発電所（Davis Besse）	米国	2003年	SCADAシステムが5時間、プロセスコンピュータを6時間停止	Slammerとして知られているワームがVPN接続を介して侵入・感染
変電所	米国	不明	変電所の通信障害	Slammerのトラフィックによる通信障害
配電所	欧州	不明	3日間、変電所の半分と通信障害	パッチ不適用のルータにワームが感染

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」
http://www.meti.go.jp/meti_lib/report/2015fy/E003791.pdf

わが国の電気事業における取組み

制御系システムのセキュリティ対策

◆システム構成面の対策

- 制御系システムの多重化（同一システムの重複設置），バックアップ化（設置箇所被災時の代替場所での対応等）
- 電力会社専用の通信ネットワーク（電力保安通信網）の利用
- インターネット等外部ネットワークとは，直接接続しない　等

◆運用・体制面の対策

- 24時間365日でシステムの稼働状況を監視
- システム障害発生時，現地技術員による監視・操作の実施
- 厳格な入退管理，システム利用権限付与等によるシステム利用者の制限
- 訓練，教育の実施　等

出典：電気事業連合会HP 「情報セキュリティの取組み」
http://www.fepc.or.jp/present/supply/security/index.html

元々は機能安全に向けた対策がセキュリティに対しても一定の効果

わが国の電気事業における取組み（続）

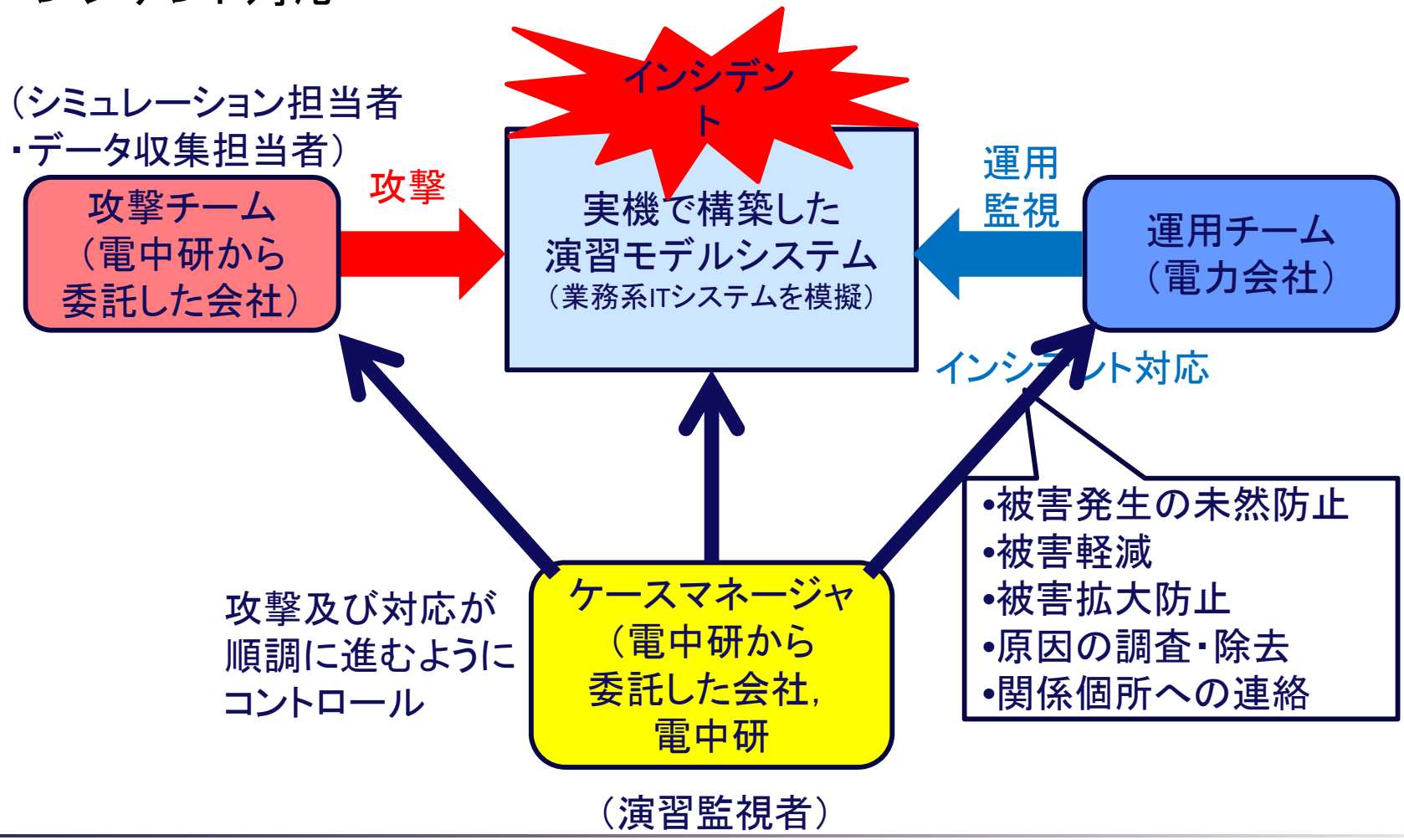
情報セキュリティマネジメント

- 電力業界全体の取り組み
  - 電子会議室等による情報セキュリティに関する情報等の共有化の実施
  - 情報セキュリティ関係会議設置による情報共有の具体的取り組み
  - 電力業界共通の安全基準等（業界ガイドライン）の策定，見直し
  - 官民ならびに電力業界全体の情報共有体制の整備（情報連絡共有ガイドライン策定）
- 各電力会社の取り組み
  - 情報セキュリティに関する委員会の設置，情報セキュリティポリシー等の策定
  - 防災対策等における危機管理体制等を活用した緊急時対応計画等の策定
  - 情報セキュリティ教育等各種情報セキュリティ施策の実施
  - セキュリティ演習への参加*)：電中研（サイバー攻撃対応演習），CSSC（制御システムセキュリティセンター）

出典：電気事業連合会HP 「情報セキュリティの取組み」，http://www.fepc.or.jp/present/supply/security/index.html
＊) 報告者が追記

電力分野でのサイバー攻撃対応演習

- 電力各社を対象に電力中央研究所（電中研）で実施（2005年度～）
- 一般業務系システムを模した実機モデルシステムを攻撃し，参加者がインシデント対応



制御系システムと情報系システムの違い

	制御系システム	情報系システム
セキュリティ確保の対象	モノ（設備，製品，人身）	サービス（連続稼動） 情報
システム更新	10～20 年	3～5 年
稼働時間	24 時間365 日連続	通常業務時間内
運用管理	現場技術部門	情報システム部門
セキュリティ対策の優先順位 • C：機密性（Confidentiality） • I：完全性（Integrity） • A：可用性（Availability）	A，I，C（可用性重視）	C，I，A（機密性重視）

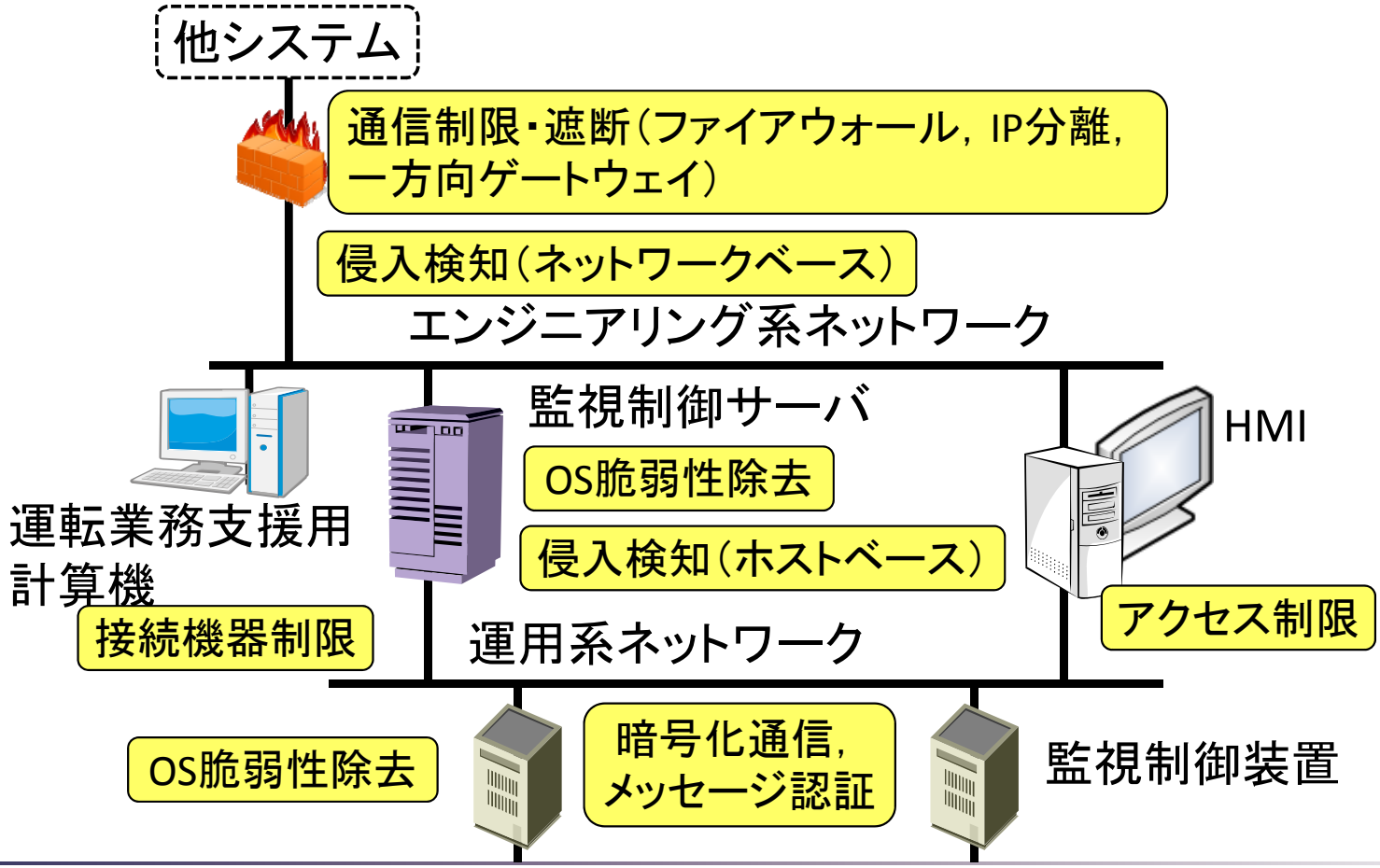
監視制御・保護システムでの対策の考え方

◆ 可用性(A)や完全性(I)の確保

- 動作信頼性や関連通信の要件(動作時間，誤動作・誤不動作，伝送遅延，伝送誤り，時刻同期など)が極めて厳しい
- 対象とするネットワーク構成と情報処理・交換機構に対し影響を及ぼす脅威とリスクを詳細に分析した上で，必要な対策について，上記要件を満足できること(リアルタイム性や動作性能への影響)を確認
- 組込み機器である保護リレーや監視制御装置自体に対策を施すことは計算機資源の観点から困難な場合も考えられるため，対策の優先順位を考慮
  1. 境界防護(物理的隔離，ネットワーク分離，ネットワーク侵入検知など)
  2. ネットワーク機器の管理と対策
  3. 監視制御・保護装置への対策(物理的なタンパ対策とともに，データ通信の完全性確保のため，簡易な鍵管理によるメッセージ認証など)
- 保守用端末などの外部接続機器の認証，中央演算用サーバ等への不正接続などに対するホワイトリスト化(怪しい者を排除するのでなく，信用できる者のみ許可)，アクセス制御強化なども有用

監視制御システムのセキュリティ対策例

- 脅威，リスク（発生確率とレベル），対策の適用可能性やコストなどを総合的に判断して対策
- 境界防護，ネットワーク機器での対策，監視制御装置での対策



現状のセキュリティ対策と将来におけるリスク

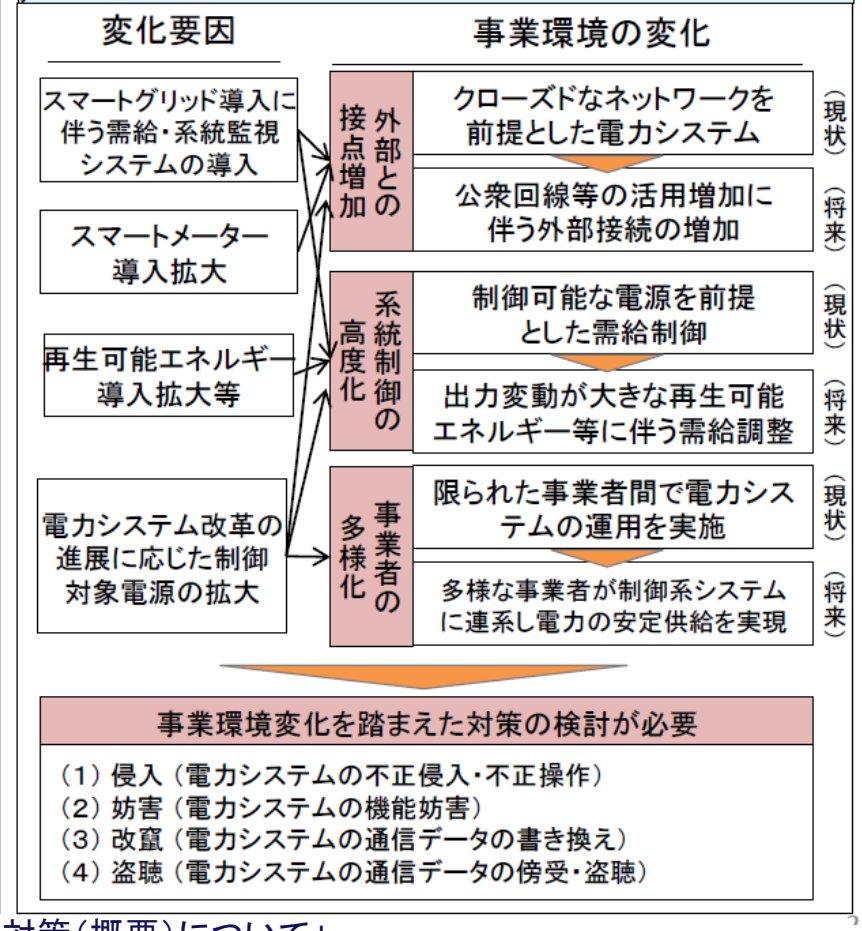
○現状の事業環境におけるサイバーセキュリティ対策について、一般電気事業者各社へのヒアリング及びアンケートによる詳細調査を実施。調査結果の分析によると、現状の対策は一定の評価ができる。
○ただし、今後の事業環境変化を踏まえた対策の検討が必要。

現状の一般電気事業者のセキュリティ対策（概要）

ポリシー	● 電気事業連合会のガイドラインに則って、各社が社内ポリシー又は部門ポリシーを策定・運用 ● スマートメーター等についてはNIST（米国国立技術研究所）等のガイドラインを参考に対策を実施・検討
対策/思想	● 原則、外部との接続点を限定したクローズドなネットワークを構成
物理(人)的対策	● 物理的隔離と侵入防御（守衛等による入退所管理も含む。） ● 記録媒体の持ち込み制限 ● 点検や修理に関わる事業者の要員の管理
接続管理	● ファイア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 ● 接続先を認証して必要時のみ外部接続する運用
教育/演習	● 電力中央研究所や制御システムセキュリティセンターが主催するサイバーセキュリティ演習への参加 ● サイバーセキュリティに対する定期的な意識啓発を実施

これまでのところ、電力の安定供給に影響を与えたサイバーセキュリティインシデントは発生しておらず、現状の事業環境におけるサイバーセキュリティ対策として、一定の評価ができる。

今後の事業環境の変化



経済産業省：「（報告）電力システムへのサイバー セキュリティ対策（概要）について」
http://www.meti.go.jp/committee/sankoushin/hoan/denryoku_anzen/pdf/005_12_00.pdf

サイバーセキュリティ対策の在り方

電力システムにおける現状と課題	米国の対策例	他産業の対策例
・これまで電力の安定供給に影響を与えたサイバーセキュリティインシデントは発生しておらず、現状の事業環境における対策としては一定の評価ができる。 ・今後は事業環境変化を踏まえた対策の検討が必要。	・事業者はセキュリティ対策に関するガイドライン（CIP※）の遵守状況をFERC（連邦エネルギー規制委員会）に提出。	・（通信）業界横断的な対策 ・（金融）内部・出口対策の強化 ・（プラント）外部からの侵入を前提とした対策の強化。マネジメントシステムの第三者認証。

提言（概要）

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
○リスクを考慮したマネジメントシステムの確立 ・リスクアナリシス ・電力設備・機器（スマートメーター含む）の調達・廃棄における対策　等	○外部ネットワークとの接続点における対策 ・不正な通信の監視・検知 ・侵入防御の多段構成等の対策　等	○他分野（情報通信事業者等）の情報セキュリティ関係者との情報共有の強化（共通脅威の分析等）	○経営課題としてのサイバーセキュリティ対策の重要性の啓発 ○導入、運用及びインシデント発生時、適切に対応できるセキュリティ人材の訓練・育成等

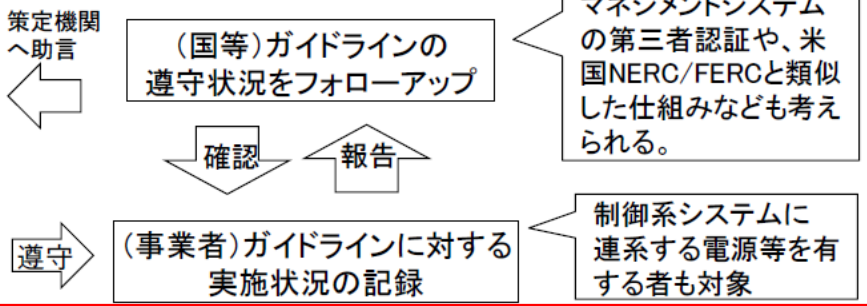
⑤電力分野のサイバーセキュリティガイドラインの策定等

○事業環境の変化も踏まえたガイドライン（日本版CIP※）の策定

■ガイドラインで規定する項目（案）（①～④を考慮して策定）

項目	概要
行動計画	セキュリティに関する行動計画を策定・実施
リスクアナリシス	リスクアナリシスを通じた重要資産の特定
対策立案	資産の重要度に応じたセキュリティ対策の立案
個別対策	電力システムの物理的保護
	電子的な接続点の保護
	サプライチェーンリスクの留意
人材育成	セキュリティ対策に資する人材育成・教育計画
危機管理	サイバーインシデントへの対応手順

○セキュリティ対策の実効性を高めるための検討



経済産業省：「（報告）電力システムへのサイバー セキュリティ対策（概要）について」
http://www.meti.go.jp/committee/sankoushin/hoan/denryoku_anzen/pdf/005_12_00.pdf

NERC CIP Ver.5の構成

- CIP-002（大規模電力系統（BES）サイバーシステムの分類）
  - BESサイバーシステムおよび関連するBESサイバー資産の特定と分類
- CIP-003（セキュリティ管理統制）
  - 責任と説明義務を果たし，一貫性と維持可能性を持ったセキュリティ管理統制の枠組み
- CIP-004（要員と教育）
  - リスクを最小化するための要員の訓練と教育，セキュリティ意識の具備に関する要件
- CIP-005（電子的セキュリティ境界）
  - BESサイバーシステムへの電子的なアクセスを管理するための制御された電子的セキュリティ境界の要件
- CIP-006（BESサイバーシステムの物理的セキュリティ）
  - 重要サイバー資産を物理的に保護するための行動計画の策定・実施に関する要件
- CIP-007（システムセキュリティ管理）
  - BESの誤動作や不安定性につながる攻撃に対処するための最良のセキュリティ技術，運用，手続きの要件
- CIP-008（インシデント報告と対応計画）
  - インシデント発生後のBES高信頼運用リスクを緩和するためのインシデント対応要件仕様
- CIP-009（BESサイバーシステムの復旧計画）
  - BESサイバーシステムに関する信頼性機能回復のための復旧計画の要件
- CIP-010（構成変更管理と脆弱性評価）
  - BESサイバーシステムの許可されていない変更の防止・検知のためのシステム構成管理と脆弱性評価の要件
- CIP-011（情報の保護）
  - BESサイバーシステム情報への許可されないアクセスを防止するための情報保護の要件

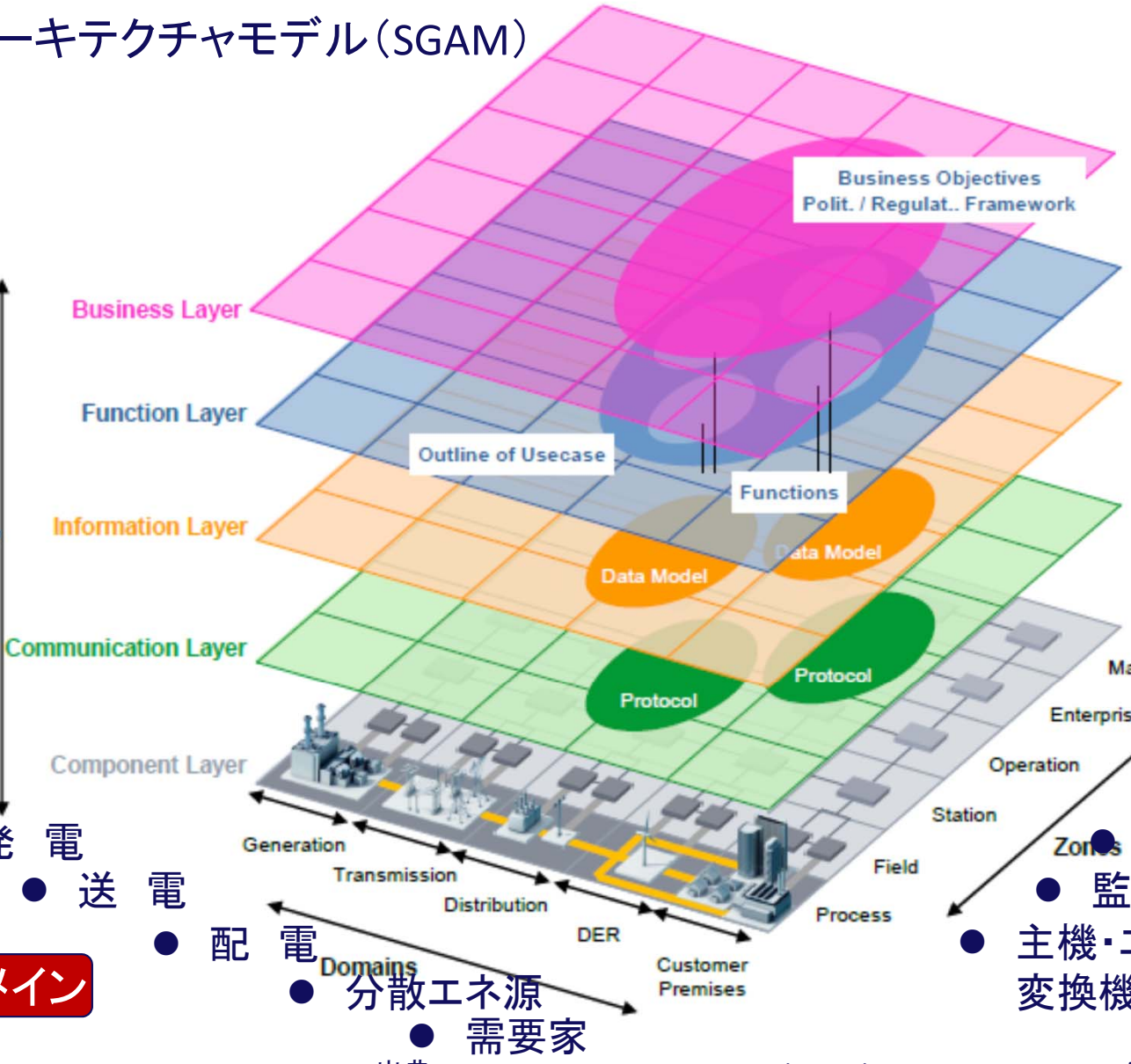
NERC：北米電力信頼度協議会，CIP：重要インフラ保護

スマートグリッドのICT構造

- スマートグリッドアーキテクチャモデル（SGAM）
- System of systems

相互運用性レイヤ

- ビジネスケース
- 機能・ユースケース
- 情報オブジェクト
- 通信プロトコル
- 物理的ICT要素



ゾーン

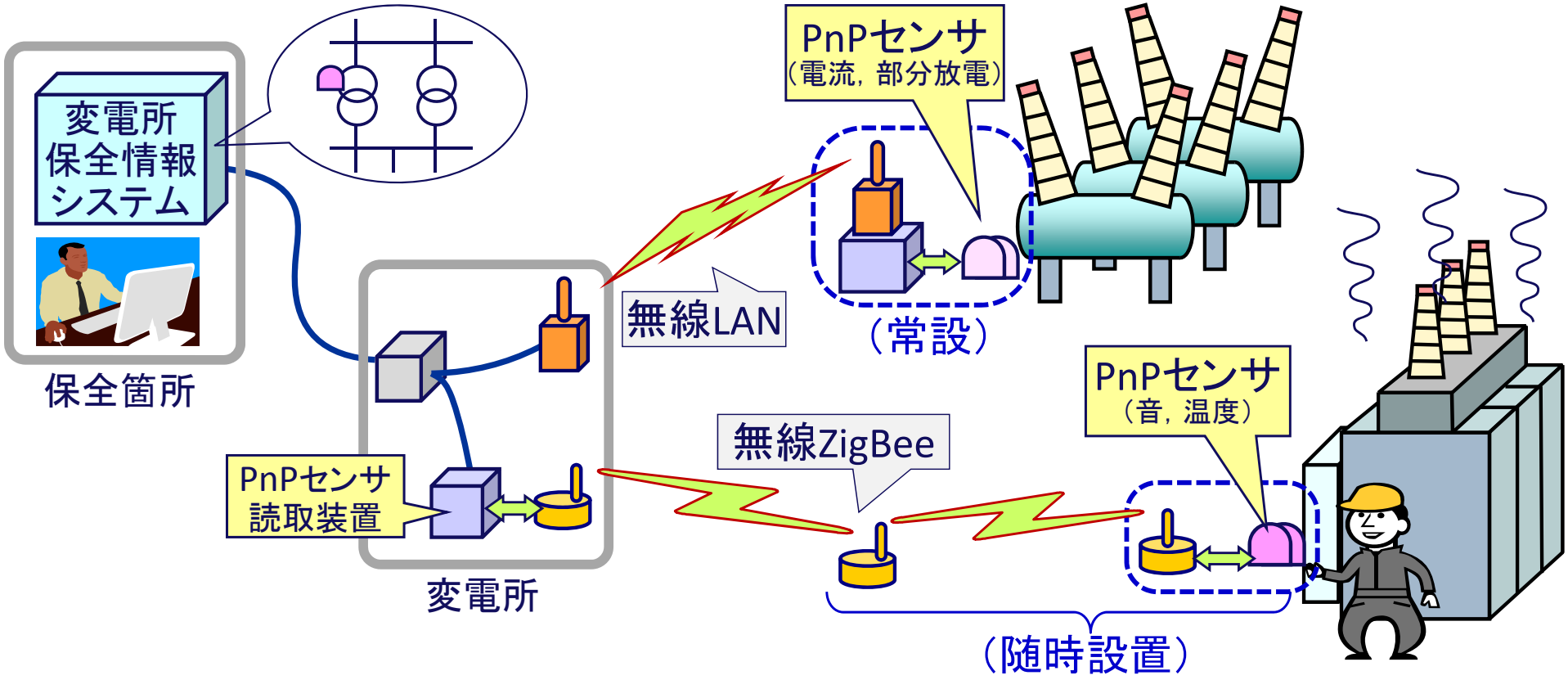
- 市　場
- 企　業
- 運　用
- 電気所・事業所
- 監視制御機器
- 主機・エネルギー変換機器

ドメイン

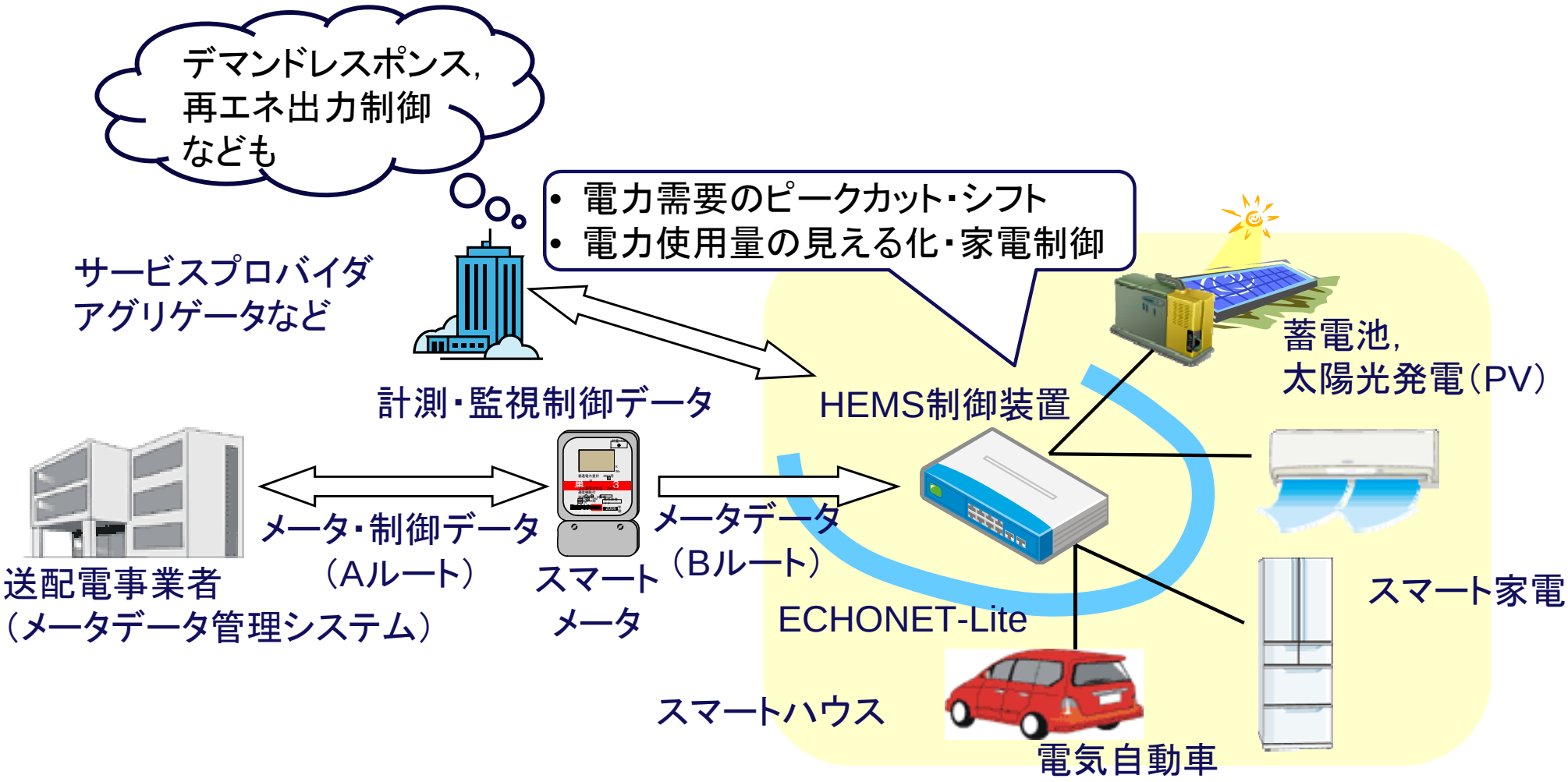
- 発　電
- 送　電
- 配　電
- 分散エネ源
- 需要家

出典：CEN-CENELEC-ETSI Smart Grid Coordination Group: SG-CG/M490/H_ Smart Grid

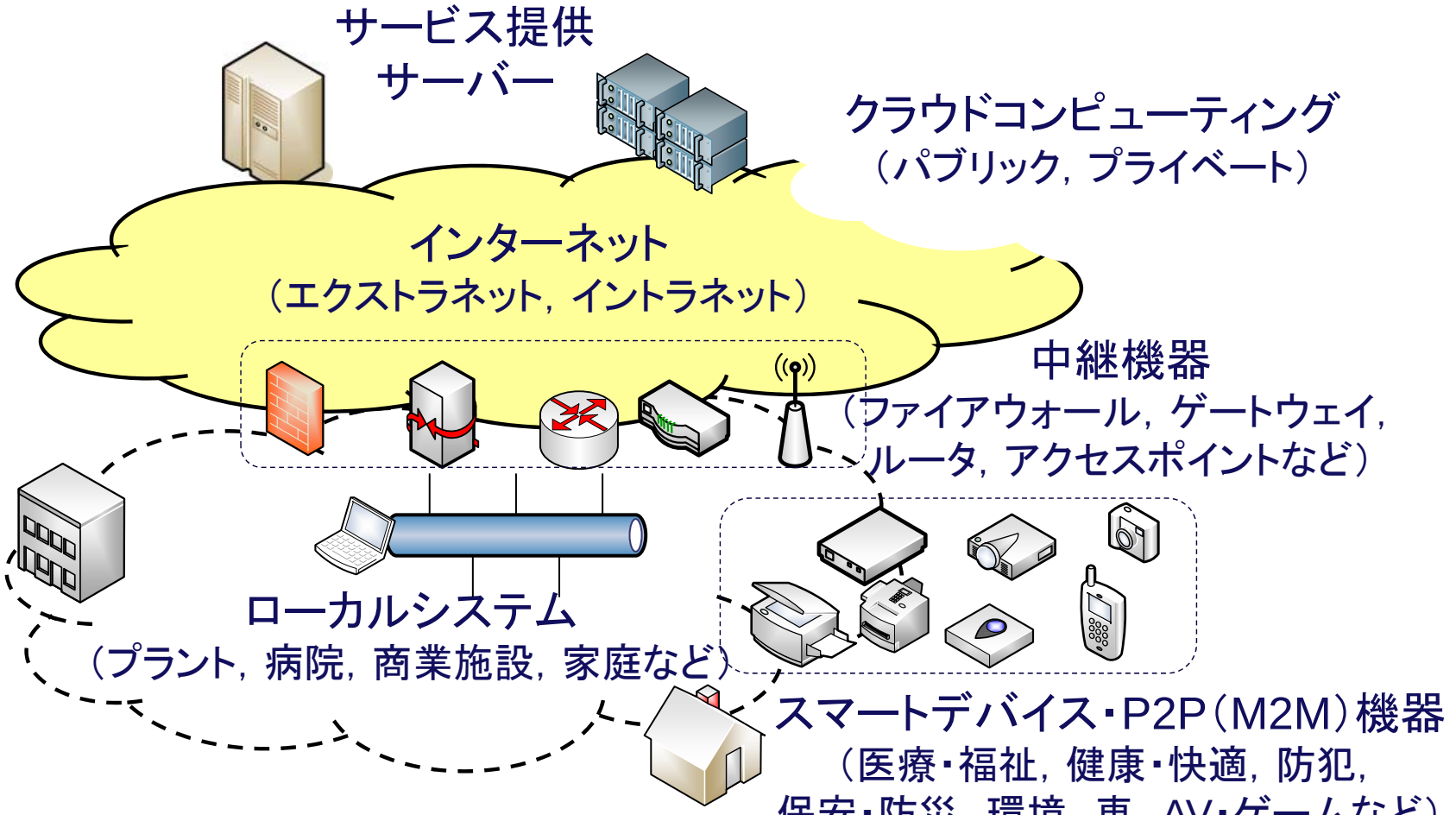
電力設備の状態監視保全用センサネットワーク



スマートメータ，xEMSシステム



IoTとサイバーセキュリティ



参考：中野学，「IoTセキュリティの全体像とその整理」，IoT Security Forum 2015

- IoTデバイスへのサイバー攻撃
  - IoTデバイス（ディジタルビデオレコーダ，Webカメラ，無線ルータなど）がTelnet経由で侵入され，踏み台攻撃に利用されている（Yin Minn Pa Pa, et al., “IoTPOT: Analysing the Rise of IoT Compromises,” 24th USENIX Security Symposium, 2015）

スマートメータのセキュリティ脅威と対策

■スマートメーターは、電力使用量などお客さまのプライバシーに係る情報を扱うことから、不正アクセスや情報の漏洩・改ざん等の脅威に対し、確実なセキュリティ対策を施す。

■脅威と対策

脅威種別	具体的事象例	対策
通信傍受	●公衆空間における通信の傍受	●暗号化 ●暗号鍵の定期的更新
なりすまし	●不正侵入	●不正通信の検出 ●接続認証
改ざん	●公衆空間における改ざん	●パケットの改ざん検出
妨害	●妨害信号の送出	●妨害信号の監視

東京電力:「RFCを踏まえたスマートメーター仕様に関する基本的な考え方」,
www.tepco.co.jp/cc/press/betu12_j/images/120712j0101.pdf

スマートメータ制度検討会
セキュリティ検討WG報告書

- 統一的なガイドラインの策定
  - 標準対策要件（公開）
    - ① スマートメーターシステムのセキュリティ対策に取り組むに際しての基本的な考え方
    - ② セキュリティマネジメント要求事項（組織，文書化，セキュリティ管理等）
    - ③ 各セキュリティマネジメント要求事項を実施する目的・考え方等
    - ④ 安定供給の確保に関するサービスレベルを維持するために事業者が実施すべき最低限のセキュリティ対策の具体的要求事項
  - 詳細対策要件（非公開）
    - ① スマートメーターシステムの構成要素毎に想定される脅威
    - ② 当該脅威と事業リスクとの相関関係
    - ③（ⅰ）抑止，（ⅱ）内部防御／情報保護，（ⅲ）侵攻検知，（ⅳ）被害把握／事業継続の各フェーズにおける当該脅威に対する対策例
    - ④ 標的型攻撃への対策や内部不正への対策，サイバー攻撃と物理攻撃の組合せによる攻撃への対策など
- 各事業者におけるセキュリティ対策
- 脆弱性関連情報の共有・管理体制

まとめ

まとめ

- 電力系統の監視制御・保護システムは電力安定供給に直結するため，信頼度や性能に関する厳しい基準を定め，障害・事故・災害に対処できる設計や構成
- 給電情報システムや監視制御システムなどの平常時運用制御システムは，汎用・標準技術の導入やIP化などが進みつつあるが，物理的隔離やID・パスワードなどによる認証，独立した専用の通信ネットワーク化などにより，関係者以外がシステムに容易にアクセスできない仕組み
- 保護制御システム（電力系統の障害・事故・災害等に対応し，高速に事故区間の除去や発電機・負荷遮断などによる安定化制御を行うシステム）は，所要の信頼性を確保するため，システム全体での多層化（主・後備保護システム，事故波及防止制御システム），各システムでの冗長構成（主保護システムや保護リレーの二重化，通信回線の2ルート化など）やフェイルセーフ機構などの組込み　⇒セキュリティ対策効果の確認要
- 電気事業者の現状のサイバーセキュリティ対策は一定の評価がなされているが，今後の事業環境変化を踏まえた対策の検討が必要　⇒　制御系とスマートメータのセキュリティ対策の規格が策定される見込み

ご清聴ありがとうございました

芹澤 善積
seri@criepi.denken.or.jp