＜制御システムセキュリティ　課題と対策＞
制御システムセキュリティに関する内外の取組みと示唆

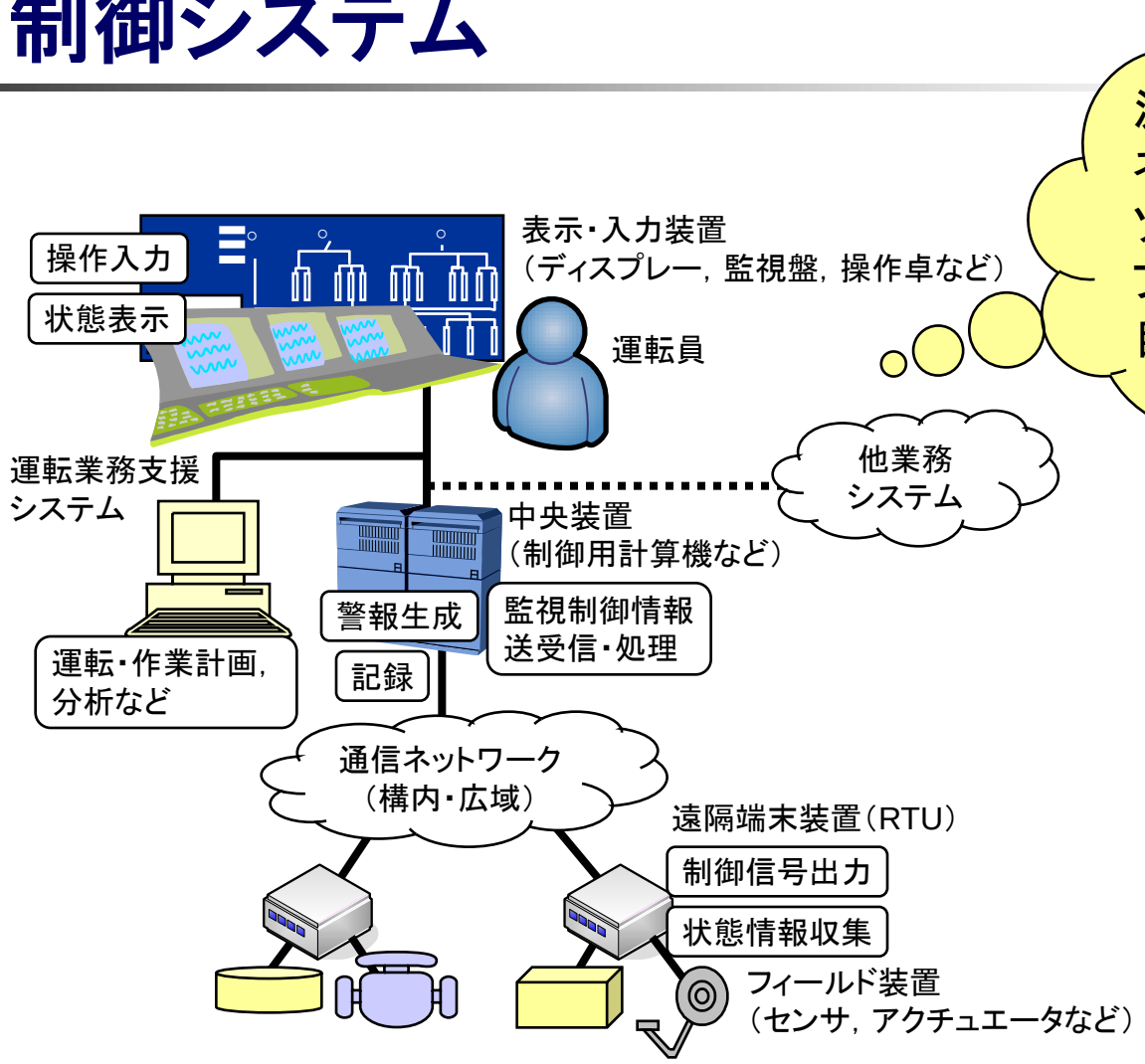
（財）電力中央研究所
システム技術研究所
芹澤 善積

2009年2月20日

発表内容

- 制御システムの概要とインシデントの傾向
- 制御システムセキュリティに関わる内外の取組み例（電力関連分野）
- セキュリティ対策の取組みに関する示唆

制御システム

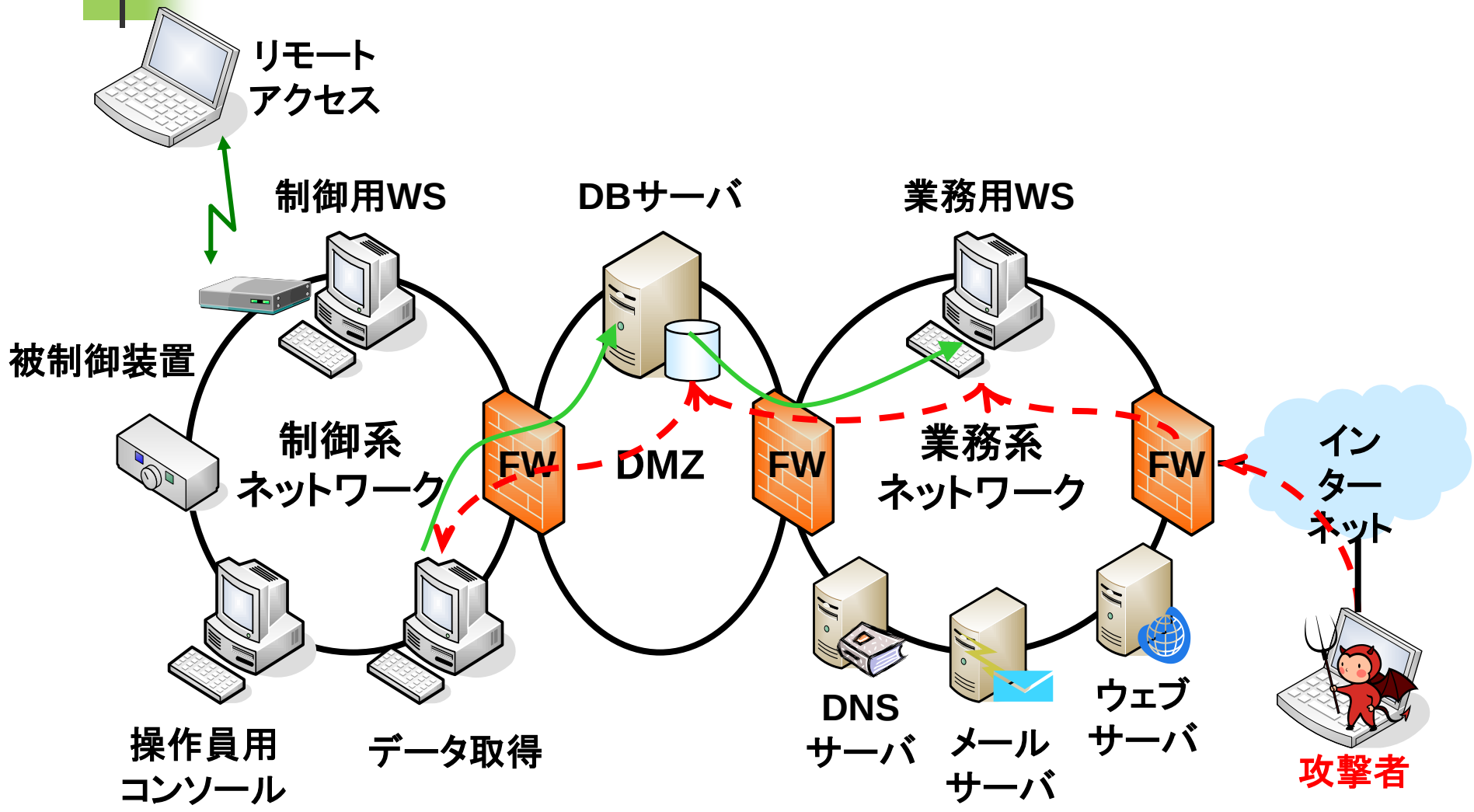


出典：芹澤・木内，「監視制御システムにおけるセキュリティ技術の動向」，電子情報通信学会誌，2009年1月号

インシデントの傾向

- 意図的インシデント事例
  - オーストラリアMaroochy市下水道監視制御システム（2000年）
    - 無線システムからの侵入
  - 米国Davis Besse原発監視制御システム（2003年）
    - Slammer Worm
  - ポーランドLodz 市Tram信号システム（2008年）
    - 改造リモートコントローラによる制御
- 非意図的インシデント事例
  - 米国ワシントン州ガソリンパイプライン破裂事故（1999年）
    - データ切替え，データ入力ミス
  - 米国テキサス州精油所爆発事故（2005年）
    - 貯留レベル設定ミス
  - 米国Browns Ferry原発（2006年），Hatch原発（2008年）
    - ブロードキャストストーム，ソフトウェアアップデートミス

侵入例(イメージ)



米国DOE（エネルギー省）NSTB プログラム

- National SCADA Test Bedプログラム
  - **DOE傘下のアイダホ国立研究所（INL），サンディア国立研究所（SNL），パシフィック・ノースウェスト国立研究所（PNNL），アルゴンヌ国立研究所（ANL）および 国立標準技術研究所（NIST）と連携したSCADAシステムの脆弱性評価と対策検討，標準化支援**
- 脆弱性評価（ベンダ製品に対して）
  - **特徴抽出とモデリング**
  - **試験計画の作成と実施**
  - **成果（対応策と電力系統の信頼性確保方策）**
    - **予防**
    - **検出**
    - **対策**
    - **復旧**
  - **ベンダ・ユーザ・評価機関の有機的な関係によるセキュリティレベルの向上**

Auroraプロジェクト

http://edition.cnn.com/2007/US/09/26/power.at.risk/index.html

NERC（北米電力信頼度協会）CIP 標準

- サイバーセキュリティ標準としてCIP (Critical Infrastructure Protection) 002～008が2006年6月に発効
- 電力システムの高信頼度運用を担保するための重要サイバー資産（コンピュータ化された機器など）の特定と，防御のためのサイバーセキュリティ対策の枠組みを示す
- 従来のITセキュリティに関する要求項目のうち，ポリシー，手続きの策定，アクセス制御，セキュリティ境界，監査，変更管理など，制御系システムにとっても有用なものを抽出
- 適用する方策が定量的であることや適合度の計測可能性を考慮
- 米国FERC（連邦エネルギー規制委員会）認定の強制標準となる（2008年1月17日）

NERC CIP標準の課題

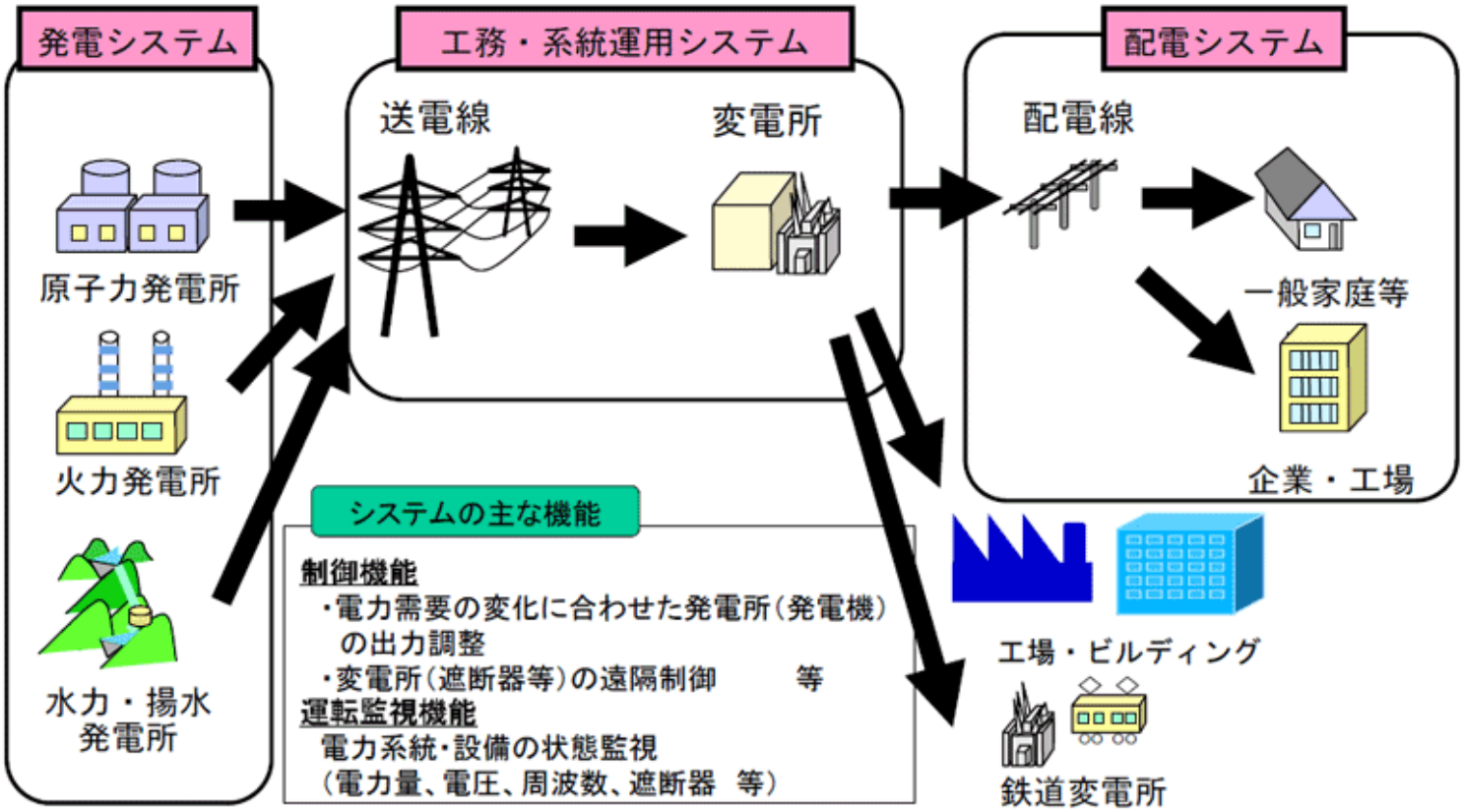
- 事業所間通信回線に関するセキュリティ対策
- ルータ以外の通信システムや無線システムに関する対策
- 基幹系統だけでなく，配電系統なども対象に加えること
- 発電所（原子力発電所を含む）におけるセキュリティ対策など
- NIST SP-800への配慮
- 第2版改訂中

米国NIST（標準技術研究所）

- FISMA（Federal Information Security Management Act of 2002）の枠組みの下，情報セキュリティに関わる標準や指針として，Federal Information Processing Standards (FIPS), NIST Guidance (Special Publication 800-Series)などを策定
- 産業用制御システム（ICS; Industrial Control System）のセキュリティに関するものを追加
  - 800-53 Recommended Security Controls for Federal Information Systems
    - Appendix I Industrial Control Systems
    - Annex 1, 2, 3 (Industrial Control System Supplements)
  - 800-82 DRAFT Guide to Industrial Control Systems (ICS) Security

わが国の電気事業における取組み

電力供給に係る制御系システム



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

電力の安定供給に向けた制御系システムの情報セキュリティ対策

- 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

電力における情報セキュリティの取り組み

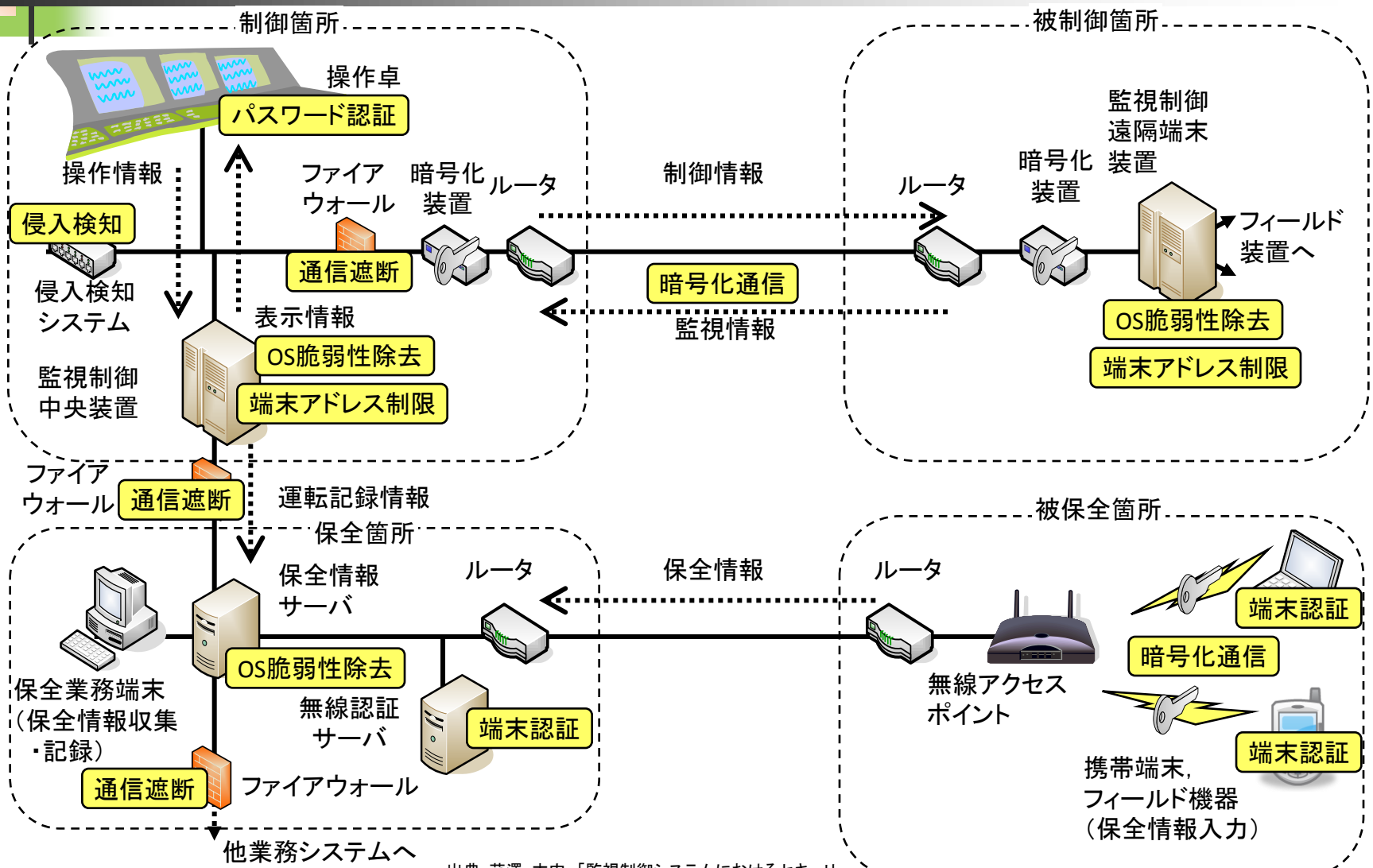
- 重要インフラとしての電力の重要性にかんがみ、各電力会社の自主的な取り組みを基本として、所管官庁との連携のもと、さまざまな対策
- 電力業界の取り組み
  - **電子会議室等による情報セキュリティに関する情報等の共有化の実施**
  - **情報セキュリティ関係会議設置による情報共有の具体的取り組み**
  - **電力業界共通の安全基準等（業界ガイドライン）の策定、見直し**
  - **官民ならびに電力業界全体の情報共有体制の整備（情報連絡共有ガイドライン策定）**
- 各電力会社の取り組み
  - **情報セキュリティに関する委員会の設置、情報セキュリティポリシー等の策定**
  - **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**

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

電力中央研究所の取組み

- 脆弱性評価（サイバー攻撃）
  - 盗聴（機密性への脅威）
    - 監視制御情報の取得
    - 系統機器構成の探索
  - 改ざん（完全性への脅威）
    - 通信（監視制御）内容の変更
    - 端末内部の情報変更
  - サービス妨害（可用性への脅威）
    - IPプロトコルを用いたDoS攻撃
- 対策提案
  - 技術的対策：認証，暗号化，通信遮断など
  - 費用対効果を考慮し，要求レベルに応じた多層的セキュリティ対策（物理的対策や人的対策も重要）
  - 対象システムや組織に応じた対策，チェックリストの作成

セキュリティ対策技術評価例



出典：芹澤・木内，「監視制御システムにおけるセキュリティ技術の動向」，電子情報通信学会誌，2009年1月号

セキュリティ対策の取組みに関する示唆

- 内外,業界，組織の違いを踏まえた対策
  - **組織としての技術レベル，組織規模**
  - **技術導入の考え方，標準化に対する考え方**
  - **従業員の意識レベル、帰属意識，流動性**
  - **ユーザ，ベンダ，（コンサルタント）との関係**
  - **官との関係**

- わが国における取組みのあり方
  - **ベンダとユーザの信頼感を持った連携強化**
  - **ベンダによるセキュリティ実装メニュー**
  - **小規模組織・業界へのサポート**
  - **ソフトウェア信頼性の向上**
  - **制御システムベンダ間のセキュリティ情報共有と技術向上**

まとめ

- 制御システムの動向
  - 汎用・標準技術の適用が拡大
  - 大きな影響は現れていないが，脅威は存在
  - 日常の継続的な確認が重要
- セキュリティ対策に関する取組み状況
  - 海外：政府系機関やユーザ，ベンダ，諸団体による多様な取組み
  - わが国：業界横断的および業界個別の取組み
- わが国における今後の取組みのあり方
  - ユーザとベンダの連携強化
  - ベンダ提供技術強化とこれに向けたベンダ間の情報共有に期待

ご清聴ありがとうございました

芹澤善積 seri@criepi.denken.or.jp