

第3回 日経セキュリティ会議

次世代情報セキュリティ

～企業の情報セキュリティ対策のこれからを考える～

# 重要インフラの防護と情報セキュリティ

小川和久(危機管理総合研究所所長)

2007年3月9日1300～1430

東京ビッグサイト会議棟

## 重要インフラの相互依存性

著作権上の問題により公開しません。

## ●重要インフラ防護を急ぐべき理由

- ・国民保護計画の基本
- ・日本は重要インフラ防護(CIP)で、発展途上段階
- ・重要インフラの一角が破壊されれば、国は麻痺状態
- ・重要インフラは相互に依存(弱い分野から被害が波及)
- ・例えば、通信から侵入して電力を止める
- ・電力が止まれば、緊急サービス、国防システム(自衛隊、在日米軍)、金融システムも麻痺状態になる
- ・日本の重要インフラからの侵入が米国に機能麻痺をもたらす可能性(米国の危機感)セキュリティ・ホール

## ●世界の趨勢

- ・ネットワーク・セキュリティから危機管理体制を構築

- ・ネットワーク・セキュリティに取り組めば

  - サイバー面と物理面でセキュリティが向上する

  - ソーシャルエンジニアリング的手法への対応力も向上する  
(騙し、内通者など)

  - 国民保護計画、個人情報保護のレベルも向上する

## ●情報セキュリティだけではセキュリティにならない

- ・05年11月に住民避難の実動訓練(美浜原発へのテロを想定)
- ・想定が成立しない(首相官邸と担当審議官に指摘)
- ・想定が成立するのは、原子力事故と制御不能の場合
- ・制御不能を狙うのか、電力をとめるのか
- ・制御不能(チェルノブイリ)を狙うには複合攻撃
- ・サイバー面、物理面を組み合わせる
  - ・ソーシャルエンジニアリング的手法(騙し、内通者)
- ・電力を止めるだけなら、侵入する必要はない
- ・それでも数万人の死者が出る(生命維持装置)

## アメリカのISAC構成状況

著作権上の問題により公開しません。

## ●日本の重要インフラ防護の問題点

▽重要インフラ個々のセキュリティの水準が高くない

・形式に流れる(侵入テスト、パッチ)

▽重要インフラ業界ごとの情報共有が遅れている

・ISAC(情報共有・分析センター)は通信だけ

▽政府の重要インフラ防護の取り組みの遅れ

・国家インフラ防護センター(NIPC)の不在

## ● 国家の安全を図る仕組み

国家安全保障会議（日本版NSC）

テロ対策、情報活動はNSCが統合

防衛省（自衛隊）

外敵に対処することで、国民の安全を図る

危機管理庁（日本版FEMA）（将来構想）

国内で国民の安全を図る

消防、警察、関係省庁、自治体

求められる危機管理庁に当たる企業・自治体の仕組み