


重要インフラにおける分野横断的演習の取組みについて(案)

2006年11月
内閣官房情報セキュリティセンター

重要インフラ対策の枠組み ～4つの施策の有機的連携による推進～

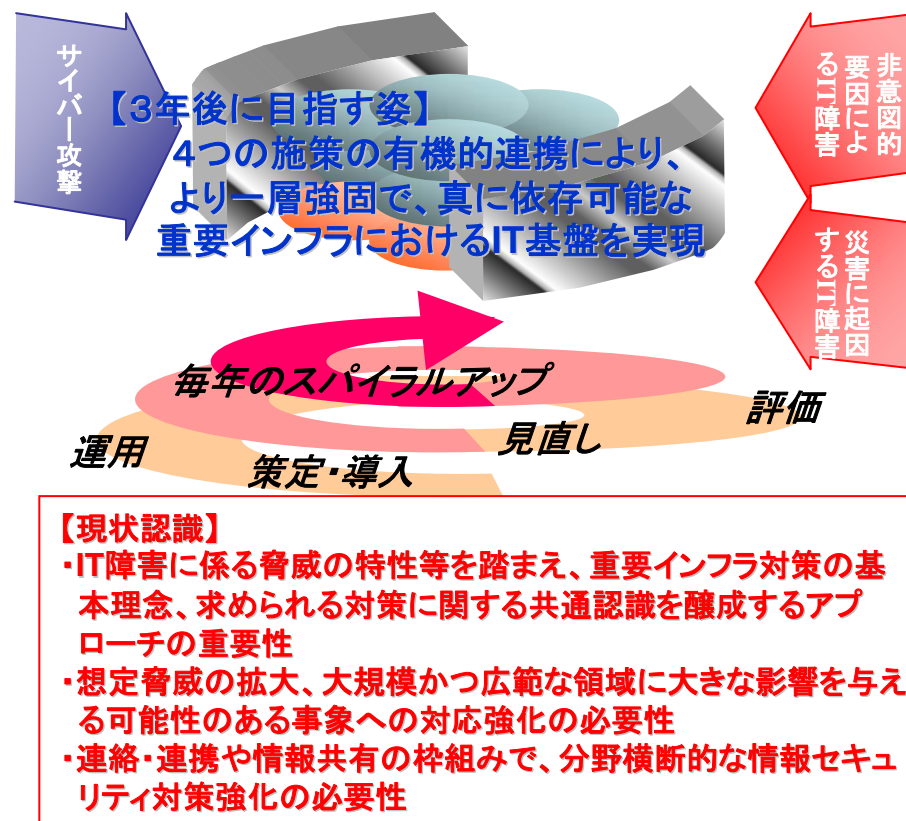
- 我が国の重要インフラ(10分野: 情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流)横断的な情報セキュリティ水準の向上を図るための「個別設計図」として、「重要インフラの情報セキュリティ対策に係る行動計画」を策定。
- 1)サイバー攻撃のみならず 2)非意図的要因、3)災害に起因する、「ITの機能不全が引き起こすサービスの停止や機能の低下等」(IT障害)から重要インフラを防護。官民で緊密に連携をとりつつ、4つの施策の有機的連携により推進。



重要インフラの情報セキュリティ対策に係る行動計画
(2005年12月13日情報セキュリティ政策会議決定)

【4つの柱】

1. 「安全基準等」の整備
2. 情報共有体制の構築
3. 分野横断的演習の実施
4. 相互依存性解析の実施



【目標】 2009年度初めには、重要インフラにおけるIT障害の発生を限りなくゼロに

2006年度以降における重要インフラ施策の進め方

2006年度 官民連携の枠組みづくりによる新しい重要インフラ防護体制づくり				
	1Q	2Q	3Q	4Q
「安全基準等」の整備	2006年9月を目途に各分野にて安全基準等の策定・見直しに努力		安全基準等に基づく対策強化等	
情報共有体制の構築	2006年度末までに、各分野にて情報共有・分析機能を整備（医療、水道、物流は整備に関する基本的合意を2006年度末までに完了することを目指す。）			
分野横断的演習の実施	研究的演習の実施		「机上演習」の実施	
相互依存性解析の実施	相互依存性解析の試行的実施			

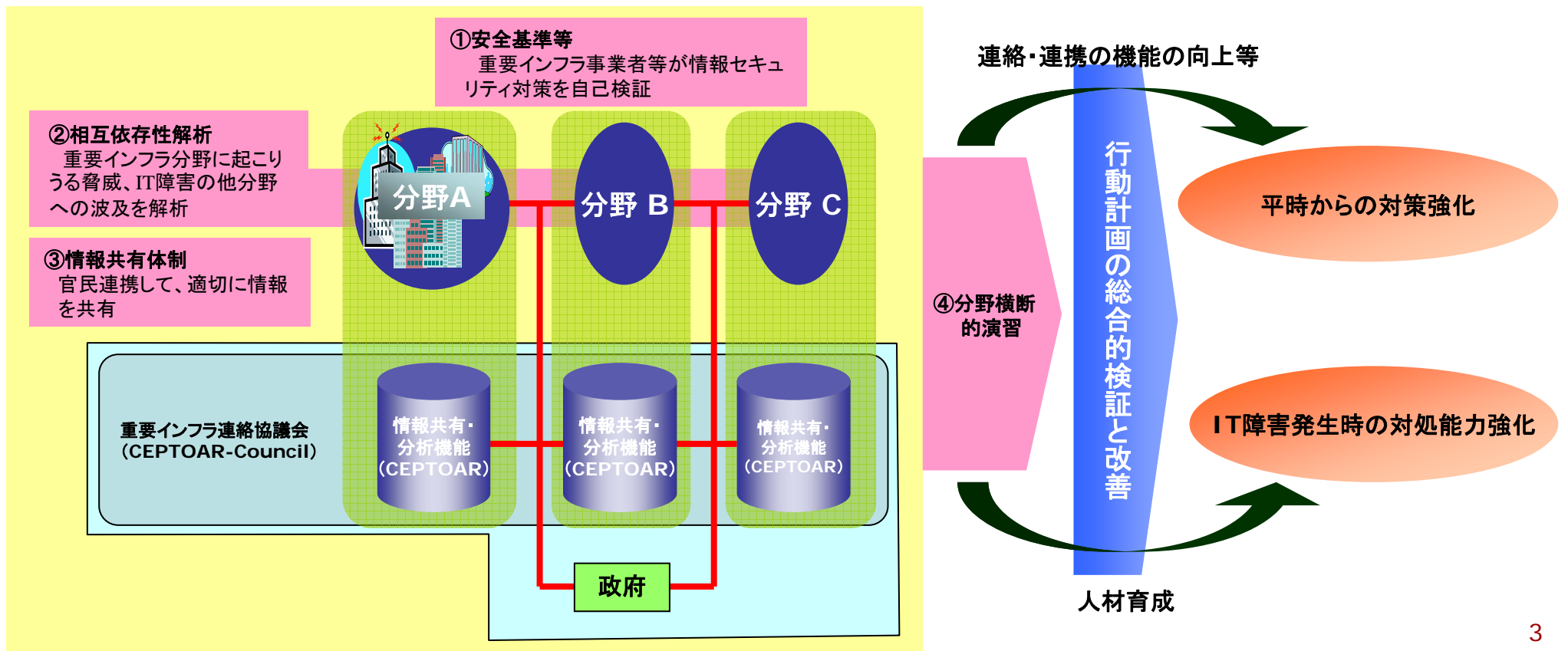
2007年度 行動計画の本格的稼働段階
安全基準等と指針の継続的見直し
情報共有体制の本格的稼働
機能面での実効性の検証
動的依存性解析の推進

2008年度 計画期間を通じた検証と行動計画の見直しに向けた検討
次期計画に向けた指針の検討
情報共有体制の一層の強化に向けた対応検討
連絡・連携の枠組みや施策の実効性の検証
分野間の連携基盤強化のための知見の提供

行動計画の実施により、官民が連携した、新しい重要インフラ防護体制の整備

分野横断的演習の概要

- 「重要インフラの情報セキュリティ対策に係る行動計画(2005年12月13日情報セキュリティ政策会議決定)」を踏まえ、段階的に実施。2006年度においては「研究的演習」及び「机上演習」を実施し、CEPTOARの整備等に資するとともに、2007年度からは「機能演習」を実施。
- 想定される具体的な脅威シナリオの類型をもとに、テーマを設定し、分野横断的に実施。
- 重要インフラ事業者におけるIT障害に対する官民の情報共有、連絡・連携のための仕組みの実効性を検証し、緊急時の対応力の強化に資するとともに、高度なITスキルを有する人材育成など、情報セキュリティ基盤の強化に資する。



分野横断的演習の背景と必要性

ITを巡る状況の変化

- ① 重要インフラの業務・オペレーションの多様化とIT依存の増加
- ② 重要インフラ分野における社会的に影響が大きいIT障害の発生
- ③ アウトソーシングや外部委託など連携の多様化の進展、自動化・リモートコントロール化・ブラックボックス化などのシステムの多様化・複雑化と障害発生時の復旧の長時間化
- ④ 重要インフラによるサービス提供構造において、多様なIT技術や運用方法の活用の進展やビジネス環境の変化等により、基本設計時の想定と、現在の実際の運用上の潜在リスクとの乖離の可能性（技術構成、パッケージ化、自動化等）
- ⑤ ネットワーク型オペレーション（電子ネットワークや重要インフラ間サプライチェーン）の進行等による他の重要インフラ分野への脆弱性の連鎖の可能性
- ⑥ IT技術そのものの発展や、運用方法の多様化に伴う複合的な脆弱性増加の可能性

IT障害の特徴等

- ① ITの利活用の進展や依存関係の増大の中で、自分野のみならず他分野への障害波及の可能性が増大。一方、障害発生メカニズムや分野間での接続関係が未解明であり、相互依存関係の解析が必要。また、他分野の対応状況が不明の面あり。
- ② データの高速・リアルタイム処理の進展により、被害の波及スピードが高速化するとともに、分野や地域を越えて広範囲に波及し、被害規模が短時間に拡大する可能性。
- ③ 事案発生時の初動段階で原因究明が困難。かつ、時間を要することが多く、その中で、状況に応じた的確な対応が重要。
- ④ コンピュータウイルスやDoS攻撃など、攻撃が低コストかつ容易化。また、共通製品の不具合の広範囲に渡る影響波及など、これまでは考えられなかった障害の発生や波及が想定。
- ⑤ これまで分野横断的な演習や相互依存性解析の経験が乏しい一方、IT技術の発展やIT利活用の進展など状況は常に変化しており、想定外の事態の発生等も想定されるので、的確な対応が必要。

- 実効性の高い対策を講じていくためには、重要インフラ事業者等におけるサービスの維持・復旧が、より容易になるよう、官民の関係主体が協力することが重要。
- IT障害を想定し、分野横断的演習の実施による組織間連絡・連携の検証等を通じ、情報セキュリティ対策の強化を図ることが必要。

2006年度における分野横断的演習の取組み(1)

< 研究的演習の実施 >

- 2006年度前半期に実施
- 我が国におけるIT障害に関する分野横断的な初めての取組みとして、演習実施の概念及び演習手法の理解、机上演習に向けた課題設定やシナリオづくり等を実施。
- 関係主体間で「連携」した情報セキュリティ対策について、共通認識の醸成・向上を図ることにより、官民連携の体制づくりに寄与。

- 情報共有や連絡・連携におけるポイント

- ・IT障害の特質を踏まえ、初動段階での状況に応じ、状況を捉えた内容とタイミングでコミュニケーションをとることが重要。
- ・緊急時に、他の分野ではどういった対応をとるのか、など、他分野のコンタクトポイントを明らかにし、円滑なコミュニケーションができるようにすることが大切。等

- 事業継続等に関するポイント

- ・アプリケーション、ハードウェア、OSなど異なるバージョンが混在し、またバージョンアップされ、複雑化していることから、迅速復旧・対応の観点から、演習・訓練が重要。
- ・オペレーションの多様化、リモートコントロールなどが進む中、想定リスク等も変化するので、将来を見通した対応が必要。等

- 演習の実施にあたってのポイント

- ・演習において「何を目的とし、何を目指すのか」を明確化して、関係者間で意識共有し、実施することが重要。
- ・演習の結果を、次のステップやプロセスにフィードバックして、レベルアップにつなげることが重要。等

研究的演習を踏まえ、机上演習の実施へ

2006年度における分野横断的演習の取組み(2)

< 机上演習の実施 >

- 研究的演習を踏まえ、2007年2月上旬を目途に実施。
- 初めての分野横断的演習として、ITを巡る状況の変化やIT障害の特徴等を踏まえ、官民の連絡・連携、情報共有の体制づくり、官民連携の実効性向上等を目的として、具体的な演習テーマの下、演習参加者が会議形式で課題討議を実施。

想定シナリオ(案)

首都圏の重要IT関係施設でITサービスの停止等が発生し、決済機能やオンライン・ネットワーク機能の低下等、短時間に複数分野に波及・影響したという想定で、官民における連絡・連携、情報共有の枠組み等を検証。

- 2007年度以降は、各CEPTOARの整備後、官民の連絡・連携体制のファンクションの検証・向上のため、「機能演習」を実施。これにより、組織運営上及び技術上の課題事項を検証し、官民連絡体制の機能向上へ寄与。