2006年度における分野横断的演習と相互依存性解析の取組みについて

2007年4月23日

内閣官房情報セキュリティセンター（NISC）

資料3-3

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。

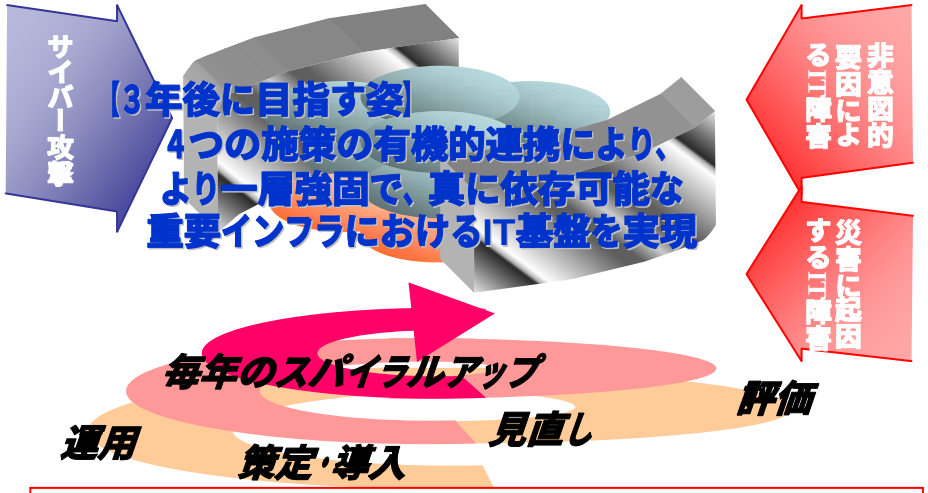
○　1)サイバー攻撃のみならず 2)非意図的要因、3)災害に起因する、「ITの機能不全が引き起こすサービスの停止や機能の低下等」（IT障害）から重要インフラを防護。官民で緊密に連携をとりつつ、4つの施策の有機的連携により推進。

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



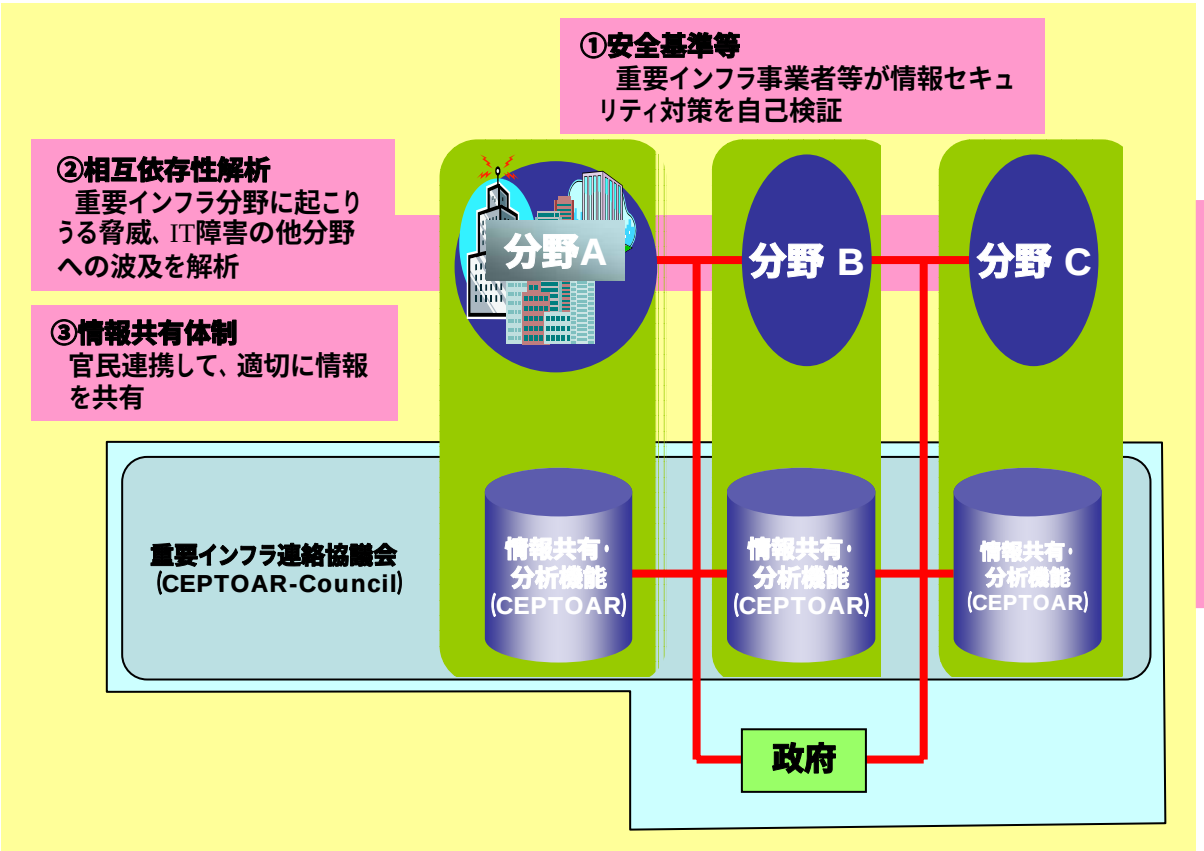
【現状認識】

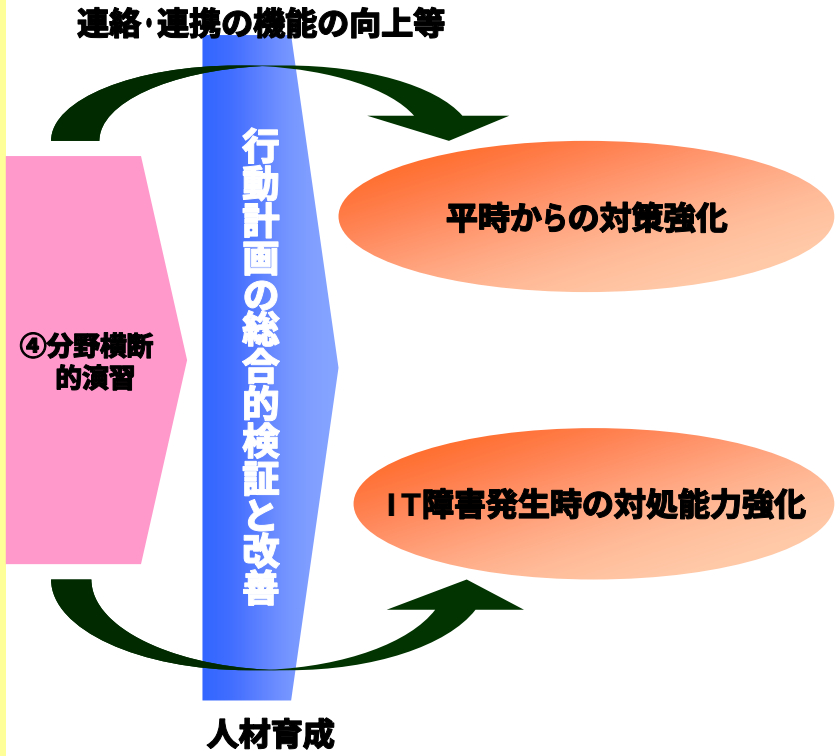
- IT障害に係る脅威の特性等を踏まえ、重要インフラ対策の基本理念、求められる対策に関する共通認識を醸成するアプローチの重要性
- 想定脅威の拡大、大規模かつ広範な領域に大きな影響を与える可能性のある事象への対応強化の必要性
- 連絡・連携や情報共有の枠組みで、分野横断的な情報セキュリティ対策強化の必要性

【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

分野横断的演習及び相互依存性解析の概要

○ 「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。
○ 演習については、2006年度においては「研究的演習」及び「机上演習」を実施し、2007年度からは「機能演習」を実施。相互依存性解析の結果等を踏まえ、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。





分野横断的演習及び相互依存性解析の背景と必要性

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 アウトソーシングなど連携の多様化、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

④ IT技術・運用方法の多様化やビジネス環境の変化等により、基本設計時と現在の潜在リスクとの乖離の可能性

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）進行等による脆弱性連鎖の可能性

⑥ IT技術の発展に伴う複合的な脆弱性増加の可能性

IT障害の特徴等

① 地域あるいは分野を超えた連鎖的・広範囲な障害波及の可能性増大の中、障害発生のメカニズムや分野間での接続関係が未解明。

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し、被害規模が短時間に拡大する可能性。

③ 事案発生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い。

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。

⑤IT技術の発展など状況は常に変化しており、想定外の事態発生等の可能性。

○ 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、分野横断的演習及び相互依存解析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

＜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。

＜机上演習の実施＞

- 研究的演習を踏まえ、2007年2月7日（水）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。

- 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。

2006年度における机上演習の概要

我が国におけるIT障害に関する分野横断的な初めての演習として、官民の連絡・連携の仕組みづくりとその実効性の向上を目指し、「机上演習」（具体的なシナリオの下に、会議形式で課題討議をする演習）を実施

1．日時　2007年2月7日（水）　13:30～17:30

2．場所　三田共用会議所

3．参加者

・政府：内閣官房情報セキュリティセンター、
重要インフラ所管省庁（金融庁、総務省、
厚生労働省、経済産業省、国土交通省）

・重要インフラ分野（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

・分野横断的演習関係有識者

等、約90名が参加

鈴木内閣官房副長官の冒頭挨拶

演習風景

2006年度における分野横断的演習から得られた知見と課題

1．障害発生時等の分野間及び分野内のコミュニケーションと連携のあり方

- 障害発生時に、障害の状況や全体像、原因や復旧見通しなどについて、分野を超えて情報を把握できる仕組みの構築。
- 防災や国民保護などの既存の仕組みへのIT障害対応の視点の盛り込みや防災訓練などとの連携。
- 情報連絡や共有に関し、リソース供給者やサービス利用者などの関係者間で、効果的かつ現実的なコラボレーションが図られる環境や仕組みづくり。

2．官民での情報共有・連携のあり方

- 官民ともに参画し、共有の幅を広げた情報発信・共有についての分野を超えた仕組みの構築。

3．IT障害発生時における迅速な対策等実施のための平時からの対応

- 情報共有の重要性に関する共通認識の醸成のための継続的取組み。
- 緊急体制への速やかな移行と対応など、事象発生時を想定した訓練の実施。
- システム稼動に必要なリソース（例えば、冷却水や加湿用水などの必要量や備蓄量など）の再確認。
- 防災など、幅広い危機管理の中でのIT障害対策の位置づけと的確な運用。

4．今後の演習や解析などの取組み

- サイバー攻撃や自然災害など、多様な脅威や状況を想定した演習の実施。
- IT関係の連絡・連携を含めた防災訓練等との連携。
- 情報共有の意義を実感する演習など、目的を明確にした演習の実施。

2006年度における相互依存性解析の取組み

(相互依存性の把握による対応の重要性)
- 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、障害発生のメカニズムや分野間での接続関係が未解明。
- 情報システムは、高度化・複雑化していることに加え、想定外の事態の発生も見込まれ、分野間の関係の把握を通じた効果的な対策への要請が増大。

(IT障害のメカニズムの構造化・可視化)
- 重要インフラ10分野間での定性的な接続関係の全体像の概要の把握の中で、ITシステムの運用に電力、通信、水が重要なリソースであることが判明した。

(「求められる対策」に関する共通認識の醸成)
- 「自助」の取り組みは進んでいるが、「共助」の重要性への認識が高まった。また、「依存する分野」と「依存される分野」では、認識に違いがあるものもあり、他分野の状況を把握することにより、認識の共有に寄与した。
- 他分野から期待される事項の把握の中で、IT障害時における情報共有に対する期待が大きいことが判明した。

(演習への知見の提供等)
- 演習シナリオに知見提供を行った。また、ベストプラクティスなど、事例分析からの知見を共有することができた。

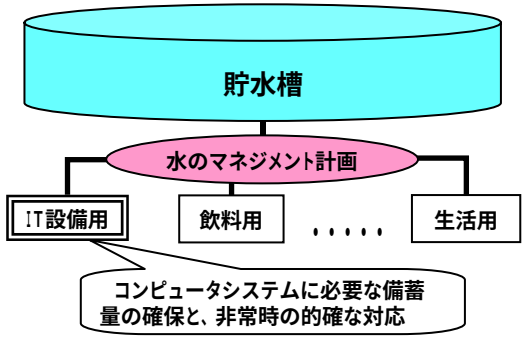
(レベルアップに向けた対応への示唆)
- 官民や分野間での情報共有の仕組み作りに向けた示唆が得られ、情報セキュリティ対策の強化に向けた知見が得られた。
- 情報システムの高度化・複雑化の中で、障害発生のメカニズムや事象間の因果関係の解明に関する認識の向上に寄与した。

情報セキュリティレベル向上等に関する取組み（効果的事例）

1．障害発生時における情報システム運用の水確保に係る金融分野での効果的対応の事例

金融分野では、情報システムを安全に運用継続するための仕組みを、具体的にかつ判り易く、分野内に広く周知し徹底させるという努力を継続的に実施。

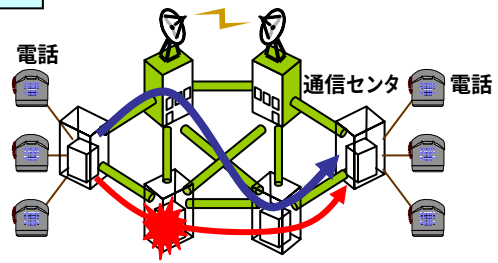
この一環として、平時からコンピュータシステムにおける水の重要性を認識し、貯水量を管理していたことから、新潟中越地震では、応援人員の急増等により想定以上の水使用に対して、節水対策に取り組み、障害を防止できた。



2．通信ネットワークの信頼性向上や災害時サービス確保の電気通信事業者の取組み事例

○ 過去の災害等を教訓に、通信ネットワークや通信設備の信頼性確保に向けた対策を実施している。また、万一の災害発生等に備え、24時間体制で通信ネットワークの監視を行うとともに、復旧用の設備・機材を全国に配備し、重要機関等の通信確保および迅速なサービスの復旧に努めている。

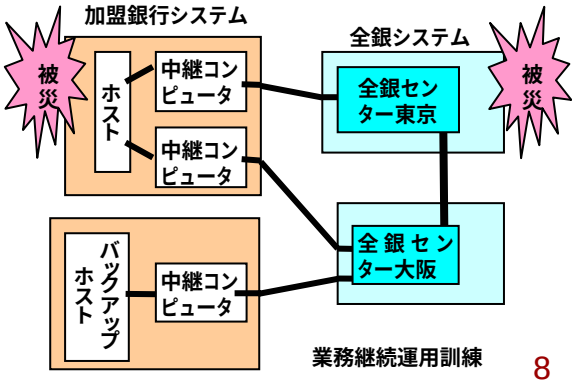
○ IT障害を含めた災害対策を実施し、その内容を利用者に分かり易い形でホームページにて公開している。災害時のため、安否確認等に使われる伝言サービス、携帯電話各社での伝言サービスの相互リンク設定、ニュース配信サービスを実施している。



通信センタの分散・中継回線の多ルート化による通信の確保

3．首都直下地震を想定した全銀システムでの事業継続運用訓練の事例

我が国の決済システムの中核となっている全銀システムは、様々な災害・障害等を想定し、地域的に隔離されたシステムの接続構成となっている。これにより、首都直下型地震で被災した場合でも業務継続を可能としている。さらに、首都直下型地震を想定した大阪のセンターでの業務継続運用訓練を定期的に実施することで、被災時の運用習熟を行っている。



業務継続運用訓練

2006年度における分野横断的演習と相互依存性解析を踏まえた今後の取組みのポイント

- 2006年度は、官民の連絡・連携の仕組みづくりとその実効性の向上を目指し、分野横断的演習と相互依存性解析を実施。
- 2007年2月には、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、机上演習を実施。
- 以下のような、演習と解析により得られた知見を活用し、官民で緊密に連携をとりつつ、情報セキュリティ政策の向上を一層推進。

（コミュニケーションの強化による緊急時対応能力の向上）

1．分野を超えたIT障害に関する情報連絡・共有プラットフォーム機能の基盤づくりの検討・取組み

- 「IT障害発生や復旧に関する状況」等につき、情報連絡・共有が有効に機能する基盤づくりの検討・取組みと、防災などの既存の仕組みとの整合のとれた対応
- タイムリーな情報共有の観点から、オープンな情報共有のあり方の検討・工夫

（IT障害に対する総合力の強化）

2．「安全基準等の指針」の見直し、安全基準等や事業継続計画などへの知見の提供

- 安全基準等の指針、安全基準等、事業継続計画、関連規定のより効果的な運用や見直し等への知見の提供
- ITシステムの運用に電力、通信、水が重要なリソースであることを踏まえ、より効果的な対応への知見の提供

（IT障害対応に関する平時からの対応強化）

3．情報共有の重要性等に関する共通認識醸成、効果的事例など知見の共有や演習の継続的実施

- 情報共有の重要性に関する共通認識醸成、平時からのコミュニケーションづくりや効果的事例などの知見の共有
- 多様な脅威や状況を想定した分野横断的演習の実施や防災訓練等との連携

分野横断的演習と相互依存性解析を踏まえた今後の取組みの方向性（1）

重要インフラを巡る状況

・IT技術の進展、ネットワーク型オペレーションの進行、運用方法の多様化などの中、国民生活・社会経済活動の基盤となる重要インフラへの想定脅威が拡大。また想定外の脅威、複合的リスクの出現の可能性
・重要インフラ間の相互依存性の増大により、連携・協力すべき主体の範囲は飛躍的に拡大。

連絡・協力すべき主体拡大の中、分野を超えた情報共有や連絡・連携体制構築の必要性

IT障害の未然防止、発生時の拡大防止・迅速な復旧、再発防止という各側面における等の対応の必要性

情報システムの高度化・複雑化の中、波及のメカニズム等を解析しつつ、重要インフラのサービス提供の安定供給に資することの必要性

（取組み）

・IT障害の波及メカニズムの解明（相互依存性解析）や具体的脅威シナリオをもとにした演習（分野横断的演習）の実施

・2006年度から段階的に実施し、2007年度からは本格稼働レベルで情報セキュリティ対策を推進

（今後の取組みのポイント）

（緊急対応能力の向上）
「分野を超えたIT障害に関する情報連絡・共有プラットフォーム機能の基盤づくり」の検討・取組み

（障害対応への総合力の向上）
「安全基準等の指針」の見直し、安全基準等や事業継続計画などへの知見の提供

（平時からの対応力の向上）
情報共有の重要性等に関する共通認識醸成、効果的事例など知見の共有や演習の継続的実施

（目指す方向性）

国民生活や社会経済活動を支える重要インフラ基盤確立に向けたスパイラルアップ

・サプライチェーンの進展などの中、関係者間でのリスクに関するコミュニケーションの向上

・「自助」のみならず「共助」の考え方を進めることによる、社会のリジリエンシーの向上

IT障害の特徴等

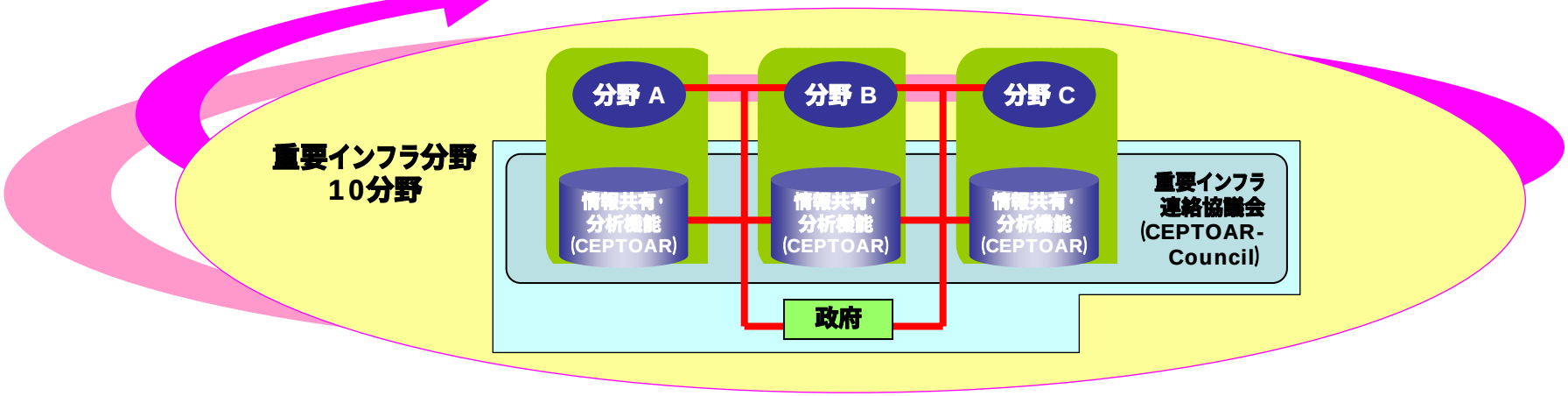
・IT障害の被害波及の高速化、空間や分野を超えた波及の可能性などの特徴を踏まえた分野横断的な対応が重要
・初動段階では原因究明が困難で、原因究明に時間を要することが多い。他方、他分野の対応状況を把握する機会が乏しい状況にあり、情報共有が重要な要素

分野横断的演習と相互依存性解析を踏まえた今後の取組みの方向性（2）

平時からの対策強化

IT障害発生時の対処能力強化

PDCAサイクルによる毎年度のスパイラルアップ



2006年度の分野横断的演習と相互依存性解析から得られた今後の取組みのポイント

1 「分野を超えたIT障害に関する情報連絡・共有プラットフォーム機能の基盤づくり」の検討・取組み

2 「安全基準等の指針」の見直し、安全基準等や事業継続計画などへの知見の提供

3 情報共有の重要性等に関する共通認識醸成、効果的事例など知見の共有や演習の継続的実施

2006年度における行動計画の総合的検証と改善

分野横断的演習
官民連携しての初めての取組みとなる机上演習の実施

依存関係、想定課題の検証

想定脅威、シナリオ設定のための知見提供

相互依存性解析
分野間の定性的な依存関係の把握

2007年度以降の演習と解析の取組み

1．相互依存性解析

- 時間と空間を超えて波及する等のIT障害の特徴を踏まえ、時間と空間の要素を取り入れた動的解析の実施方法についての検討等。
- 脅威の変化･多様化、想定外の脅威の発生などを踏まえ、脅威の類型や、脅威と障害の因果関係についての検討の深化。
- 一定の想定障害ケースについて、検討を深め、演習シナリオにも反映し、実際の対応能力の向上に寄与しうるアプローチの実施。

2．分野横断的演習

- 本年度の知見等を踏まえ、セプターやセプターカウンシル等を活用した情報連絡や共有のあり方についての機能の検証。
- 障害発生時に、より効果的に対応するため、より実践的な演習の実施。
- 想定障害のパターンや状況設定を検討し、相互依存性解析の結果をも踏まえた演習の実施。
- 組織運営上及び技術上の課題事項を検証し、官民連絡･連携体制の機能向上への寄与。

3．本年度の演習と解析の課題への検討と対応

- 情報連絡･共有プラットホーム機能の基盤づくりの検討･取組み。その際、セプターやセプターカウンシル、官民連絡･連携体制、災害などの既存の仕組みとの整合･連携のとれた対応を図る。
- ノウハウの蓄積や事例分析などを通じた、対応力の向上などの、総合力アップのための方策の検討。