参考資料4

セキュア・ジャパン2007

ーITを安心・安全に利用できる環境づくりのための情報セキュリティ対策の底上げー

【抜粋版】

情報セキュリティ政策会議

2007年　6月14日

第3章　対策実施4領域における情報セキュリティ対策の強化

本セキュア・ジャパン2007においては、セキュア・ジャパン2006に引き続き、情報セキュリティ対策を実際に適用し実施する主体の領域を、政府機関・地方公共団体、重要インフラ、企業、個人の4領域に分け、それぞれの特性に応じた具体的施策を定めることとする。

第2節　重要インフラ

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することを目指し、政府は、重要インフラの情報セキュリティ対策について、「重要インフラの情報セキュリティ対策に係る行動計画」（2005年12月13日情報セキュリティ政策会議決定）を別途定めているところであるが、2007年度には以下の施策を重点的に推進する。

①重要インフラにおける情報セキュリティ確保に係る「安全基準等」の整備

「重要インフラにおける情報セキュリティ確保に係る『安全基準等』[1]策定にあたっての指針」[2]（以下、「指針」という。）を踏まえ、それぞれの重要インフラ事業分野ごとに、必要な又は望ましい情報セキュリティ対策の水準について、「安全基準等」に明示することを目標とする。さらに、指針については1年ごと及び必要に応じて適時見直すこととし、「安全基準等」については、情報セキュリティを取り巻く環境の変化に応じ、随時見直しを行う。

【具体的施策】

ア）各重要インフラ分野の安全基準等の策定・見直し

a)安全基準等の見直し（重要インフラ所管省庁[3]）

2007年6月を目処に行われる指針の改定を踏まえ、2007年9月を目処に、各重要インフラ分野において、安全基準等の確認・検証を行い、必要に応じ改定等の対策を実施する。

b)「安全基準等」の見直し状況等の把握及び検証（内閣官房）

---

1 「安全基準等」とは、重要インフラ事業者等が、様々な判断、行為を行うに当たり、基準又は参考にするものとして策定された文書類を指す。

2 「重要インフラにおける情報セキュリティ確保に係る『安全基準等』策定にあたっての指針」（2006年2月2日情報セキュリティ政策会議決定）

3 「重要インフラ所管省庁」とは、重要インフラ事業者等（「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）中「1　目的と範囲」に示す定義による。以下同じ。）と法令に従って直接に接する省庁を指す。以下同じ。

各重要インフラ分野における「安全基準等」について、各重要インフラ所管省庁の協力を得つつ見直しの状況を2007年中に把握するとともに、相互依存性解析の成果も踏まえた検証を2007年度中に実施する。

イ）各重要インフラ分野における安全基準等の浸透状況等に関する調査の実施（内閣官房及び重要インフラ所管省庁）

2007年度中に、内閣官房は、重要インフラ所管省庁の協力を得つつ、2006年度に策定・見直しを行った各重要インフラ分野における安全基準等の浸透状況についての調査を実施する。

ウ）指針の見直し（内閣官房）

2007年度中に相互依存性解析の成果も踏まえ、各重要インフラ所管省庁の協力を得て、指針の見直しを実施する。

エ）ネットワークのIP化に対応した電気通信システムの安全・信頼性確保（総務省）

ネットワークの IP 化の進展に対応して、ICT サービスの安定的な提供を確保するため、2007年度中に、ネットワークの設備面や運用・管理面について、制度改正など必要な安全・信頼性対策を講じる。

②情報共有体制の強化

IT障害に関する情報について、1）IT障害の未然防止、2）IT障害の拡大防止・迅速な復旧、3）IT障害の要因等の分析・検証による再発防止の3つの側面から、政府等は重要インフラ事業者等に対し適宜・適切に提供し、また重要インフラ事業者等間並びに相互依存性のある重要インフラ分野間においてはこれら情報を共有する体制を強化する。

（ア）官民の情報提供・連絡のための環境整備

関係機関と連携し、注意喚起等、各重要インフラ事業者等の対策に資するものとして、重要インフラ事業者等に提供する情報の収集を行い、CEPTOAR（後述）等を通じて、情報を提供する。

また、重要インフラ事業者等が、法令等で報告が義務づけられている事故、障害、業務遅延等のほか、特異重大なものとして重要インフラ事業者等が連絡を要すると判断した情報を政府に連絡するための環境の整備を促進する。

【具体的施策】

ア）情報共有体制整備と機能強化（内閣官房）

各分野におけるCEPTOARの整備及びCEPTOAR-Council（仮称）の整備等の状況変化を踏まえ、2006年度に整備された官民の情報共有体制に対して追加すべき機能・要件等の検討を行う。

（イ）各重要インフラ分野における情報共有・分析機能（CEPTOAR）の整備

IT障害の未然防止、発生時の被害拡大防止・迅速な復旧及び再発防止のため、政府等から提供される情報について、適切に重要インフラ事業者等に提供し、関係重要インフラ事業者等間で共有することにより、各重要インフラ事業者等のサービスの維持・復旧能力の向上に資するため、各重要インフラ分野内に「情報共有・分析機能」（CEPTOAR：Capability for Engineering of Protection, Technical Operation, Analysis and Response）の整備を促進する。

【具体的施策】

ア）各重要インフラ分野におけるCEPTOAR整備の推進（重要インフラ所管省庁）

２００７年度末までに、新規追加分野（水道、医療及び物流）においてCEPTOARが整備されるよう取組みを進める。

イ）「CEPTOAR特性把握マップ」のフォローアップ（内閣官房）

2007年度中に、各分野におけるCEPTOARの機能・要件の検討状況及び整備状況（新規追加分野については整備状況）の把握を行う。また、2007年度末を目処に、CEPTOAR特性把握マップのフォローアップを行う。

（ウ）「重要インフラ連絡協議会（CEPTOAR－Council）」（仮称）の創設促進

重要インフラ事業者等において、分野横断的な情報共有の推進を図り、多様な知見をサービスの維持・復旧に活かしていくため、各CEPTOAR間での横断的な情報共有の場として「重要インフラ連絡協議会（CEPTOAR－Council）」（仮称）の創設を促進する。

【具体的施策】

ア）「重要インフラ連絡協議会（CEPTOAR－Council）」（仮称）創設の検討（内閣官房及び重要インフラ所管省庁）

2007年度中に重要インフラ連絡協議会（CEPTOAR－Council）（仮称）の創設についての基本的合意を得るべく、検討の場を開催し課題についての検討を進める。

③相互依存性解析の実施

我が国全体としての重要インフラ対策の向上に向けた、分野横断的な状況の把握のため、それぞれの重要インフラに起こりうる脅威が何であるかを把握するとともに、ある重要インフラにIT障害が生じた場合に、他の重要インフラに、いかなる影響が波及するかという相互依存性の把握を行う。

【具体的施策】

ア）重要インフラ分野間の相互依存性解析の推進（内閣官房）

重要インフラ分野における IT 化の一層の進展と分野間の関連性の高まりを踏まえ、官民の連絡・連携体制の機能と、事業継続を含むIT障害発生時の対応能力の向上等を図るため、2007 年度は、国内外の脅威の類型や脅威と障害の因果関係、障害と事業継続との関係などについての検討の深化や演習シナリオへの反映を行うとともに、重要インフラにおける障害発生から波及・拡大という連鎖的な伝播プロセスを動的に把握する動的依存性解析を推進する。なお、実施にあたっては、実施方法について十分に検討を行う。

④分野横断的な演習の実施

想定される具体的な脅威シナリオの類型をもとに、各重要インフラ所管省庁、各重要インフラ事業者等、各重要インフラ分野のCEPTOAR等の協力の下に、重要インフラ横断的な演習を行う。演習を通じ、安全基準等、情報共有体制、情報共有・分析機能、相互依存性解析等の各施策の実効性・妥当性を定期的に、かつ、段階的に、検証する。また、この演習やその他の訓練、セミナー等を通じて、重要インフラ所管省庁及び重要インフラ事業者等を中心に、高度なITスキルを有する人材を育成し、確保する。

【具体的施策】

ア）重要インフラ機能演習[4]の実施（内閣官房及び重要インフラ所管省庁）

官民の連絡・連携体制の機能と、IT 障害発生時の対応能力の向上等を図るため、2007 年度は、重要インフラ所管省庁、各重要インフラ事業者等及び各重要インフラ分野の CEPTOAR 等の協力を得て、相互依存性解析の知見を踏まえつつ、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、分野横断的な機能演習を実施する。

イ）電気通信事業分野におけるサイバー攻撃への対応強化（総務省）

2008年度までに、緊急時における、関係事業者間及び事業者・政府間の連携

4　実際の組織の指示判断系統機能を用いて模擬的に検証するための演習

体制の強化や調整力を発揮できる高度な ICT スキルを有する人材の育成を図るため、2007年度も、2006年度に引き続き、電気通信事業者を中心に、各重要インフラに跨るインターネット上で発生するサイバー攻撃を想定したサイバー攻撃対応演習を実施する。

ウ）各分野サイバー演習との連携（内閣官房及び重要インフラ所管省庁）

2007年度に内閣官房の実施する演習において、「情報通信」等の分野ごとに実施されるサイバー演習の実施形態及びその目的との整合性を考慮しつつ、連携を図る。

⑤「重要インフラの情報セキュリティ対策に係る行動計画」の見直し

【具体的施策】

ア）「重要インフラの情報セキュリティ対策に係る行動計画」の見直し（内閣官房）

2007年中に、各重要インフラ所管省庁の協力を得て、「重要インフラの情報セキュリティ対策に係る行動計画」の見直しに向けて、重要インフラ分野における情報セキュリティ対策向上の状況についての調査・把握に着手する。その際、災害発生時における対応等、他の関連する省庁横断的な取組みとの整合性の確保、連携についても検討を行う。また、官民の連携の在り方についても継続的に検討を行う。

第5章　政策の推進体制と持続的改善の構造

第3節　持続的改善構造の構築

情報セキュリティを巡る問題は、新たなリスク要因が次々と発生し、また想定し得なかった事故、災害や攻撃が発生する等、その状況変化が早いことから、政策の効果を常に評価し、改善を行うことが必要である。このため、政府は、以下のような持続的改善のための構造を構築することが必要である。

（1）「年度計画」の策定とその評価等

政府は、基本計画の実現を図るため、毎年度、より具体的な施策の実施プログラムを「年度計画」として策定するとともに、その実施状況を評価し、その結果を可能な限り公表する。

なお、政府以外の関係機関における対応が不可欠である等、施策を円滑に進捗させる観点から、中長期的な計画を定めることが必要なものについては、単年度にこだわらず、複数年度のマイルストーン設定も検討する。

【具体的施策】

ウ)「重要インフラの情報セキュリティ対策に係る行動計画」の見直し(内閣官房)【再掲】

2007年中に、各重要インフラ所管省庁の協力を得て、「重要インフラの情報セキュリティ対策に係る行動計画」の見直しに向けて、重要インフラ分野における情報セキュリティ対策向上の状況についての調査・把握に着手する。その際、災害発生時における対応等、他の関連する省庁横断的な取組みとの整合性の確保、連携についても検討を行う。また、官民の連携の在り方についても継続的に検討を行う。