資料2

2007年度の情報セキュリティ政策の評価等

－「真の情報セキュリティ先進国」を目指す取組みの2年目の評価－

（重要インフラ関係部分抜粋）

内閣官房情報セキュリティセンター（NISC）

2008年4月22日

第3章　重要インフラにおける現状の評価等

第１節　重要インフラにおける情報セキュリティに関する2007年度の取組み

１．2007年度の取組みの背景

重要インフラにおいては、そのサービスの安定的供給が最優先課題であるという面から、各事業において発生するIT障害が国民生活・社会経済活動に重大な影響を及ぼさないよう対策を実施することが必要である。このような安全対策は、一義的には各重要インフラ事業者等が担うべきものであるが、社会全体のITへの依存が進む中で、日増しに増大していく各種脅威への対策が個々の取組みだけでは限界に達しつつあるのが現実である。

そこで、中・長期的な取組み課題は山積するものの、先ずは実施可能なものから取組みを開始し、継続的な見直しと改善を通じて、情報セキュリティ対策の向上を図っていくというアプローチが妥当との判断に立ち、「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）（以下「行動計画」という。）を定め、「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」（基本計画）を目指して取組みを進めているところである。

重要インフラにおける2007年度の取組みは、この行動計画の下で情報セキュリティ対策を推進するため、2006年度の成果を踏まえ、引き続き取り組まれたものである。

２．2007年度の取組み

行動計画においては、重要インフラ関係の4本の施策の柱（①安全基準等の整備　②情報共有体制の強化　③相互依存性解析の実施　④分野横断的な演習の実施）と、各主体における取組み項目を示し、各項目ごとにアクションプランとして具体化を図ることにより、重要インフラの情報セキュリティ対策の向上につなげていくことにしている。また、行動計画は、3年ごと又は必要に応じ、見直しを行うこととなっている。

これを踏まえ、SJ2007において、具体的取組みを定め、実施したところである（具体的には「第2節2」において後述）。

【参考：　4本の施策の柱】

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

2006年2月2日に情報セキュリティ政策会議において決定された「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」（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。

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・適切に提供する。

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。

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。

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。

第2節 2007年度の取組み及び取組みを受けた重要インフラにおける現状の評価等（2007年度の評価等）

1. 2007年度の評価等に関する基本的考え方（評価等の視点）

第1節に述べたとおり、重要インフラの情報セキュリティ対策については、行動計画に従って、官民の緊密な連携の下で、情報セキュリティ対策の強化を目指しているところである。行動計画に定める取組みは、IT障害の発生を可能な限り未然に防止するために必要な対策及びIT障害が発生した際の影響を可能な限り極小化するために必要な具体的対策（すなわち、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ための対策）であり、これらの取組みの進捗度合いをみることで、重要インフラにおけるサービスの安定的供給機能の維持とリスクへの適切な対応の実現度合いを把握することができる。このことを踏まえ、2007年度の重要インフラにおける情報セキュリティ対策の評価等は、2006年度同様、対策向上を目的に行動計画で定めた4本の施策の柱それぞれについて、各年度ごとの目標（具体的取組み）に対する実施状況を把握し、その進捗度合いがどの程度の状態であるかということを確認するという視点に立って行うこととする。

2. 評価等について（評価指標等）

（1）2007年度の評価等について

2007年度における重要インフラにおける情報セキュリティ対策の評価等を行うに当たり、進捗度合いを把握する対象となる「具体的取組み」（すなわち目標）は、SJ2007に記載されているそれぞれの取組みである（別表1）。そして、これらの取組みの進捗度合いそのものが、2007年度の進捗度合いを把握するための指標である。

（2）2008年度の評価等について

2008年度についても年度計画に盛り込む取組みの進捗度合いが指標となる。目標とする取組みの設定については、重要インフラ専門委員会において、報告された2007年度の実施状況や実際のIT障害の発生状況なども踏まえながら、また2007年12月よ

り開始している行動計画見直しの検討状況も考慮し、重要インフラにおける情報セキュリティ対策の着実な向上を確保することに留意しつつ、行うこととする。

3. 評価等の結果と総評

(1)施策の取組み結果に関する評価等

重要インフラにおける情報セキュリティ対策向上の取組みに関しては、2007年度においては、表-1のとおり、計7回(2006年度・3回)の重要インフラ専門委員会会合を開催し、それぞれ検討を重ねたところである。

また、「「重要インフラ連絡協議会(CEPTOAR－Council)(仮称)」創設に向けた検討の場」を設け、2007年5月から2008年3月まで、8回の会合及び5回のワーキングを開催したほか、「分野横断的演習」及び「相互依存性解析」についても、2007年6月から2008年3月まで、それぞれ5回の検討会と解析7回、演習5回のワーキングを開催し、具体的な検討、取組みを進めたところである。

表-1 重要インフラ専門委員会会合

	主な議題
第9回専門委員会 (2007年4月12日)	・CEPTOAR の整備状況 ・2006年度の進捗状況、及び2007年度の取組目標について
第10回専門委員会 (2007年6月19日)	・2007年度の相互依存性解析及び分野横断的演習の枠組みと進め方
第11回専門委員会 (2007年9月28日)	・2007年度「安全基準等の見直し状況等の把握及び検証」(実施案) ・2007年度「安全基準等の浸透状況等に関する調査」(実施案) ・重要インフラにおける補完調査
第12回専門委員会 (2007年12月3日)	・2007年度「安全基準等の見直し状況等の把握及び検証」(中間報告) ・2007年度「指針」の見直し(実施案) ・「重要インフラ連絡協議会」(仮称)の創設促進に関する報告 ・静的相互依存性解析の総括 ・2007年度における分野横断的演習 ・行動計画見直しの検討スケジュール
第13回専門委員会 (2008年1月31日)	・2007年度「安全基準等の見直し状況等の把握及び検証」(報告) ・2007年度「指針」の見直し(中間報告) ・情報共有・分析機能の整備状況 ・「重要インフラ連絡協議会」(仮称)創設に向けた検討状況 ・2007年度分野横断的演習の実施(具体的シナリオ等) ・行動計画の見直し(論点のたたき台)
第14回専門委員会 (2008年3月4日)	・2007年度「安全基準等の浸透状況等に関する調査」(報告) ・2007年度「指針」の見直し(報告) ・行動計画の見直し(論点整理骨子案)
第15回専門委員会 (2008年3月28日)	・行動計画の見直し(論点整理に関する集中討議)

その結果、行動計画に定める4つの施策の柱それぞれについて、本年度は以下のとおりの取組みの成果が得られた。

(ア)安全基準等の整備

①「安全基準等」の見直し

2007年6月に行われた指針の改定を踏まえ、重要インフラ10分野すべてにおいて9月末までに「安全基準等」の見直しが実施された。

②「安全基準等」の見直し状況の把握及び検証

第11回重要インフラ専門委員会にて了承された「2007年度重要インフラにおける「安全基準等の見直し状況の把握及び検証」について」に基づき、

ⅰ)「安全基準等」の見直し状況等の把握

ⅱ)「指針」との対応状況の検証

ⅲ)「相互依存性解析」の成果を踏まえ各分野の「安全基準等」において今後反映することが望ましい事項の洗い出し

を行い、第13回重要インフラ専門委員会で報告を行った。

③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

第11回重要インフラ専門委員会にて了承された「2007年度重要インフラにおける「安全基準等の浸透状況等に関する調査」について」に基づき、重要インフラ10分野について、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が事業者等にどの程度浸透しているか、また事業者等が安全基準等に対して準拠しているかを把握するための調査を実施し、第14回重要インフラ専門委員会で報告を行った。

④指針の見直し

第12回重要インフラ専門委員会にて了承された「2007年度「指針」の見直し」に基づき、

ⅰ)定常的なIT障害の発生状況の分析

ⅱ)「相互依存性解析」の成果

ⅲ)関連文書の検証

ⅳ)社会的条件や環境の変化の検証

の4つのアプローチからの分析・検証により、情報セキュリティ対策に関する「問題意識」を抽出して現在の指針と照らし合わせを実施した。その結果を第14回重要インフラ専門委員会に報告し、見直しの要点を重要インフラ10分野に周知する参考資料としてとりまとめた。

（イ）情報共有体制の強化

①情報共有体制整備と機能強化のための取組み

CEPTOAR 特性把握マップのとりまとめ、情報共有訓練及び CEPTOARも参加した官民連携による分野横断的演習を実施した。

②各重要インフラ分野における CEPTOAR 整備の推進

新規追加3分野（水道、医療、及び物流）において、2007年度までに整備が完了した。これにより重要インフラ10分野すべてにおいて整備が完了した。

③CEPTOAR 特性把握マップ

重要インフラ所管省庁等の協力を得て、2007年度末現在の各 CEPTOAR の特性を把握するとともに、整備状況とあわせて CEPTOAR 特性把握マップ(ver2)をとりまとめた。

④CEPTOAR－Council（仮称）設置に向けた検討

CEPTOAR 代表者等から構成される「重要インフラ連絡協議会（CEPTOAR－Council）（仮称）創設に向けた検討の場」を設け、8回の会合を開催した。同「検討の場」において、来年度以降の検討方針を「「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な考え方」としてとりまとめた。

（ウ）相互依存性解析の実施

有識者、各重要インフラ分野の分野委員及び重要インフラ所管省庁からなる相互依存性解析検討会を設置し、検討会5回・WG7回を実施し、「相互依存性解析における視点（考え方のポイント）」を整理しつつ、「動的相互依存性解析」を実施した。併せて2006年度と2007年度に実施した解析結果を整理し「相互依存性解析報告書」としてとりまとめた。

（エ）分野横断的演習の実施

有識者、各重要インフラ分野の分野委員及び重要インフラ所管省庁からなる分野横断的演習検討会を設置し、検討会5回・WG5回を通じてシナリオ等についての議論を経て、約120名の参加を得て分野横断的な機能演習を実施した。

（2）施策の取組みによる社会的変化に関する評価等

以上のような、行動計画に基づく具体的取組みを進めたこと等により、重要インフラにおけるサービスの安定的供給機能を維持しつつリスクに適切に対応する社会の実現に向け、本年度においては、次に掲げるような社会的変化が認められた。

（ア）安全基準等の整備

重要インフラ10分野で安全基準等の見直しが実施されており、重要インフラにお

ける情報セキュリティ対策が着実に前進していることが確認できた。具体的には、各分野毎の安全基準等のPDCAサイクルにおいて、各分野毎の独自の観点に加え政府の指針の観点を盛り込んだ見直しが進展するとともに、同一指針に基づく分野横断的な検証によって各分野毎の安全基準等の特徴等が明らかになることで、分野間でのノウハウの共有のための環境整備が進展した。

また、各分野毎の安全基準等に基づき重要インフラ事業者の内規の見直しが進んでおり、事業者毎の内規のPDCAサイクルにおいても政府指針の観点が反映されつつある事が確認できた。ただし、全事業者への浸透にはなお時間を要することも推定されている。

また、指針の見直しを通じ、安全基準等の適用対象とならないシステムも含めて、我が国の国民生活や社会経済活動に多大なる影響を及ぼすおそれが生じる障害が発生していることや、水道分野と他分野との相互依存性を踏まえた対応の必要性、過去の事例の知見や教訓を受けた対策の重要性などの問題意識が改めて認識された。

（イ）情報共有体制の強化

重要インフラ10分野すべてにおける CEPTOAR の整備完了や、「重要インフラ連絡協議会（CEPTOAR－Council）」（仮称）の創設についての来年度以降の検討方針の取りまとめ、官民連携による分野横断的演習の実施、情報共有訓練などを通じ、重要インフラにおける官民の各主体間での情報共有、連絡・連携のための枠組みの構築が一層進展した。

（ウ）相互依存性解析及び分野横断的演習

2006年度における静的相互依存性解析に基づき、2007年度においては、相互依存性に関わる「視点の整理（定義化）」を実施し、重要インフラ分野間における相互依存性に対する認識の共有・共通化が図られた。さらに、動的相互依存性解析の実施を通じて重要インフラ事業者間には相互依存関係はあるものの、それぞれに適切な対策が施されていることが判明した。しかしながら、その対策が時間的経過や状況の変化により対策の想定状況を越えた場合には、サービスの停止や機能の低下に至る可能性があることを確認した。

また、分野横断的演習については、NISC、重要インフラ所管省庁、重要インフラ事業者等、さらにはCEPTOARがそれぞれプレイヤーとして参加し、緊急時における情報共有・情報連絡について、具体的事象を想定したシナリオによる演習を実施した。これらの活動を通じて、IT障害発生時における情報共有・情報連絡手法等の確認と検証を実施した。

（3）補完調査の結果について

（ア）補完調査の目的及び方法

重要インフラにおける情報セキュリティ対策に関する2007年度の補完調査は、「情報セキュリティ政策2007年度の評価等に向けた「作業方針」」（2007年10月3日）に

基づき、(イ)に示す各項目についてのデータを捕捉するとともに、実際に発生した事例について個別に検証を行うことにより、重要インフラにおける情報セキュリティ対策に関する変化の状況を把握し、上記(2)の評価等を補完するために行う。

(イ)補完調査①～参考となるデータの捕捉～

ｉ)安全基準等の整備の状況について

安全基準等の整備状況を示すデータとして、本年度実施した「安全基準等の浸透状況等に関する調査」(※1)で得られたデータをもとに、「安全基準等の認知率」及び「安全基準等の見直し率」の捕捉を行った結果、以下のとおりであった。

なお、算出に当たっては、単純集計では回収数の多い分野の全体集計への影響が大きくなることから、重要インフラ全体の状況把握をより適切に行うため、共通の重みづけ(※2)で集計を実施した。

調査依頼対象	２９５８事業者等
回答数	２８４６事業者等 （回収率９６．２％）
認知率	９７．９　％ 「名称・内容ともに知っている」「名称のみ知っている」を合算
見直し率	５４．８　％ 「定期的に実施している」 「実施したことがある」を合算

※1「安全基準等の浸透状況等に関する調査」

各重要インフラ分野の事業者等を対象に、各重要インフラ分野のおける安全基準等がどの程度浸透しているか、また事業者等が安全基準等に対して準拠しているかを把握するために行ったアンケート方式による調査。

※2

$$A=\frac{\left(a_1/\alpha_1\right)+\left(a_2/\alpha_2\right)+\cdots+\left(a_n/\alpha_n\right)}{n}$$

A:回答Ａに対する全体集計（%）

a_i:分野iにおける回答Ａの数（$1 \leq i \leq n$）

α_i:分野iにおける回収数（$1 \leq i \leq n$）

ⅱ）情報共有体制の強化の状況について

情報共有体制の強化の状況を示すデータとしては、「2007年度における「情報提供」の件数」及び「CEPTOARを構成する事業者等の数」の捕捉を行った。

「情報提供」とは、注意喚起等、各重要インフラ事業者等の対策に資する情報について、内閣官房から重要インフラ所管省庁を通じ各重要インフラ事業者等に対し行うものとして行動計画に規定しているものであるが、2007年度においては、3件（うち情報共有訓練のために実施したもの2件）であった。

また、「CEPTOAR を構成する事業者等の数」については、全10分野、14 CEPTOAR の合計で5,692事業者等であった。各重要インフラ分野ごとの事業者数等については、「CEPTOAR 特性把握マップ」のとおりである。

ⅲ）相互依存性解析の実施、分野横断的な演習の実施の状況について

相互依存性解析及び分野横断的演習の実施状況を示すデータとしては、それぞれに要した「年間延べ時間」及び「延べ参加者数」を捕捉した。

先述のとおり、2007年度においては、「相互依存性解析」及び「分野横断的演習」について、2007年6月から2008年3月まで、それぞれ5回の検討会と解析7回、演習5回のワーキングに有識者、各重要インフラの分野委員及び所管省庁といった巾広い参画が得られたところである。その結果、相互依存性解析には年間延べ92．5時間、参加者数延べ395人、計622（人・時間）を費やし、分野横断的演習には年間延べ39時間、参加者数延べ473人、計1178（人・時間）を費やした。

なお、2008年2月6日に実施した本年の分野横断的演習当日参加者は、116名であった。

（ウ）補完調査②～具体的事例の検証～

具体的事例の検証として、2007年度において実際に発生した「IT障害」及びIT障害の要因となり得る「リスク」について、類似事例の発生状況（可能性）や社会的影響の大きさにも着目し、内閣官房において事例を選択し、各重要インフラ分野の協力（情報提供・ヒアリングの実施等）を得ながら、ⅰ）システム障害（非意図的要因）が発生した事例、ⅱ）業務システムがウイルス感染した事例、ⅲ）新潟県中越沖地震発生時の状況　について、それぞれ以下のとおり検証を行った（なお、ⅰ）及びⅱ）において検証の対象とした事例の概要は、別紙のとおり）。

ⅰ）システム障害（非意図的要因）が発生した事例

（検証結果）

○　利用者がサービスの提供を受ける際に使用する情報システムの障害は、利用者への影響が大きく現れやすいことが確認された。

○　障害発生時においては、原因究明よりも応急復旧対応が優先されること、また、復旧のためのシステムの利用制限のタイミングなど、事業継続と障害復旧の両立のための判断が重要でありかつ困難であることが確認された。

○　同一のシステムを多数の事業者が同時に利用している場合には、当該事業者間での連携が特に重要であり、またシステムを構築・納入する業者（複数であれば尚更）との連携・意思疎通も同様に重要であることが確認された。

○　障害の発生原因は多様であることや、業務や情報システムの複雑化が進んでいることなどから、未然防止の対策で対応できる範囲には限界があることが改めて確認された。

（課題・留意点）

○　情報システムを利用したサービス提供の基盤化が進む中、障害の未然防止だけでなく、障害が発生した際の応急対応をより充実したものにすることも効果的。その際は、各事業分野の特性に応じて、以下の事項について留意が必要。

・　個々の事業者としての応急復旧対応と、他の事業者への情報提供との優先度も踏まえて、情報共有等の事業者間連携について検討すること。

・　システムを構築する事業者だけでなく、システムを利用してサービスを提供する事業者としての役割や責任も踏まえ、適切な対応と連携について検討すること。

・　システム復旧後にも、利用者への影響は残存する場合があることを踏まえた対応を検討すること。

○　発生した障害の分析を行い、事後の再発防止に活用することは効果的。

ⅱ）業務システムがウイルス感染した事例

（検証結果）

○　ウイルス対策ソフトは導入されていたが、当該ウイルスに対応していなかったため検出できなかったことから、新種のウイルスの場合、未然防止の対策で対応できる範囲には限界があることが改めて認識された。ウイルス等のサイバー攻撃に対しては未然防止の対策も重要であるが、攻撃手法が日々変化していることから事前に準備可能な対策では防ぎきれない場合もある。

○　障害発生後は、原因究明や利用者等への周知よりも、システム復旧等の応急対応をとることの方が、事業者にとっての優先的関心事であることが確認された。

○　一度システム内部に侵入したウイルスを完全な駆除を確認するのは困難であり、復旧のための対応に多くの時間やコストがかかる場合があることが確認された。

（課題・留意点）

○　インターネットを経由してのウイルス感染については、特定の分野等に特化したものではなく、何らかの形でインターネットと直接的・間接的に接続関係があるシステムを使用している事業者にとっては、共通的な脅威である。

○　未知のウイルス等の新たな脅威や事例に関する情報は、幅広く共有することで他の事業者等での未然防止や応急対応に資するのではないか。関係

機関の既存制度を効果的に活用するなど、情報共有体制の充実について考えることが必要。

○　一方、コスト等の実効性も含めると、未然防止だけでなく、感染時に柔軟かつ適切に対応できるように準備することも必要。

ⅲ）新潟県中越沖地震発生時の状況

（検証結果）

○　複数の重要インフラ分野においてサービスが停止したものの、2004 年新潟県中越地震での経験や教訓を活かした対策が立てられていたことから、IT 障害については被害を最小限に抑えることができたものと考えられる。各分野にて整備された安全基準等に基づく対策や、分野間の依存性を考慮した対策が有効であったと考えられる。

○　マシンルームの床全体が免震構造であったためオンラインシステムの通常通り稼動が可能であった例や、本社だけでなく子会社のシステムもデータセンターに収容する等のサプライチェーン全体を見据えた情報システム整備やバックアップの構築が有効であった例などが確認された。

○　商用電源の停電を原因とする金融分野事業者の一部店舗の休業や、通信回線の輻そうによる原子力発電所の地震計データの一部伝送停止など、重要インフラ分野間での影響の波及が確認された。

○　災害応急体制のもとでの情報共有、被災状況の把握、各省庁の対応状況等の確認が行われたものの、重要インフラ行動計画に基づく官民の情報連絡は、機能する場面とはならなかった。

（課題・留意点）

○　首都圏直下地震等では、より大規模な人的被害・物的被害が想定されるとともに、その地理的条件から重要インフラの基幹となるシステムにおいても、大規模なシステム障害の発生のおそれがある。

○　自然災害発生時の対応について定める既存の法令や防災計画等の枠組み等との整合を図りつつ、情報セキュリティの観点からの官民の情報連絡や総合調整について検討することが必要。

（エ）補完調査のまとめ

以上のとおり補完調査を行った結果、重要インフラにおける情報セキュリティ対策の状況については、個々の重要インフラ事業者等による情報セキュリティ対策については、過去の経験の蓄積や、安全基準等の整備、「指針」の浸透等の効果により、向上が進んでいることが確認できた。

一方で、障害リスクの発生時における情報や、他分野、他事業者の「経験」から得られた知見の共有の重要性は改めて確認できたものの、重要インフラ事業者等間及び重要インフラ分野間において、これらの情報共有については、現時点において活発に進んでいるものとは確認できておらず、政府内の連絡体制や CEPTOAR に期待される役割を如何に発揮していけるかが今後の課題であると考えられる。

（4）総評

以上のことより、2007年度における取組みは、別表2のとおり、2006年度に引き続き、当初の目標に沿った成果をあげており、個々の重要インフラ事象者等による情報セキュリティ対策の向上が進んでいるものと理解できる。

一方で、構築された情報共有体制の活発な運用までには、なお時間を要するものと考えられることや、国民生活、社会経済活動におけるITの利用は引き続き進展や拡大が予想されること、加えてIT障害を発生させる要因や脅威は常に変化し続けるものであることから、重要インフラにおける情報セキュリティ対策については、引き続き継続的にその向上に取り組んでいくことが必要である。

第3節　2008年度に向けた課題

重要インフラにおける情報セキュリティ対策の向上のためには、行動計画に掲げた取組みの着実な進捗が必要不可欠である。現在の行動計画の最終年度にあたる2008年度においては、これまでの取組みを通じて認識した以下のような課題を踏まえた取組みを行うことが重要である。

（ア）安全基準等の整備

各重要インフラ分野における安全基準等については、2007年6月に改定された指針の内容を踏まえ全分野で見直しが行われ、指針をトリガーとした分野横断的なPDCAサイクルが動き出したことが確認できた。今後は、このサイクルがセキュリティレベルの底上げのツールとして有効に機能するよう定着させていくことが必要である。

一方で、安全基準等について「見直し状況等の把握」「浸透状況等調査」「指針の見直し」の各施策を進める中で、その運営サイクルについて、各分野において安全基準等の大規模な改定や検討会等を行う場合に要する期間や、事業者等による内規の見直し期間との重複による混乱の発生などの課題が顕在化しており、実態を踏まえた望ましい形にすることが必要である。

また、「安全基準等の浸透状況等に関する調査」の結果から、2006年9月の安全基準等の策定・見直しから 1 年経過した時点で内規見直しを終えることができた事業者等は半数程度にとどまることが推定されるため、2007年度は、指針改定によって安全基準等の見直しへの新たな視点を喚起するのではなく、内規見直しを終えていない事業者等への安全基準等の着実な浸透を期することを優先したところである。見直しの過程で明らかになった見直しの要点については、現在検討中の行動計画見直しの状況等も踏まえ、来年度以降の指針見直しにて検討する必要がある。

（イ）情報共有体制の強化

①情報共有体制整備と機能強化

2006年度に構築された、重要インフラにおける官民の各主体間での情報共有、連

絡・連携のための枠組みは、2007年度の取組みによって一層充実進展をした。

しかしながら、重要インフラ事業者等間及び重要インフラ分野間における、障害リスクの発生時の情報や他の分野・事業者の「経験」から得られた知見の共有については、現時点において現実に活発に進んでいるものとは確認できていない。今後は、これらの情報の共有がいかにすればスムーズに進むか、阻害要因の研究とその解決に向けた対策の検討が課題である。

②「CEPTOAR 特性把握マップ」のフォローアップ

「CEPTOAR 特性把握マップ」とは、各重要インフラ分野ごとに設けられる CEPTOAR について、事業特性から反映された機能特色等について業種ごとに把握し、特徴把握が容易かつ可視性を工夫したものであり、今後の CEPTOAR のあり方を考える上で参考となるものである。

2007年度末で重要インフラ10分野すべてにおいて、CEPTOAR の整備が完了したところであるが、整備の過程において、整備目的の共有、既存の連絡体制との整合性、必要となるコストなど、様々な課題の中で整備が進められており、分野によっては、今後具体的な運用等を通じて機能の充実がなされる可能性もある。

③「CEPTOAR－Council」（仮称）創設の検討

「CEPTOAR－Council」（仮称）は、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の、各 CEPTOAR 間での横断的な情報共有の場として想定しているものである。

2007年度においては、「CEPTOAR－Council」（仮称）創設に向けた検討の場」を8回及びワーキングを5回開催し、創設に向けての基本的考え方を取りまとめたところであり、今後はこの考え方に基づき創設準備会を設置し、2008年度内の「重要インフラ連絡協議会（CEPTOAR－Council）」（仮称）の創設を目指し、より具体的な検討を進める必要がある。

（ウ）相互依存性解析の推進

官民の連絡・連携体制と、IT障害発生時の対応能力の向上を図るため、2006年度及び2007年度における相互依存性解析のとりまとめを踏まえ、「分野間のシステムにおける繋がり」等の課題についてその実施方法も含め検討することにより、相互依存性解析の深化を図る必要がある。

（エ）分野横断的演習の推進

官民の連絡・連携体制と、IT障害発生時の対応能力の向上を図るため、2007年度に引き続き、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考慮しつつ、想定される具体的な脅威シナリオ等、諸条件を基にテーマを設定し、テーマに応じた最適な演習手法（机上演習、機能演習など）による分野横横断な演習を実施し、その深化を図る必要がある。

（別表1）

4本の施策の柱	2007 具体的取組み目標	
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	安全基準等の見直し	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。
	「安全基準等」の見直し状況等の把握及び検証	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。
	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	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。
	指針の見直し	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。
②情報共有体制の強化	情報共有体制整備と機能強化	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。
	各重要インフラ分野におけるCEPTOAR整備の推進	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。
	「CEPTOAR 特性把握マップ」のフォローアップ	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。
	「重要インフラ連絡協議会（CEPTOAR－Council）」（仮称）創設の検討	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	重要インフラ分野間の相互依存性解析の推進	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	重要インフラ機能演習の実施	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。
	各分野サイバー演習との連携	2007 年度に分野ごとに実施される「情報通信」等のサイバー演習と、内閣官房の実施する演習について、実施形態及びその目的の整合性を考慮しつつ、連携を図る。

（別表2）

2007年度における取組みの進捗状況

4本の施策の柱	2007 具体的取組み目標		2007成果
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	安全基準等の見直し	・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。	2007年6月に行われた指針の改定を踏まえ、**重要インフラ10分野について9月末までに実施**。
	「安全基準等」の見直し状況等の把握及び検証	**・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 ・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。	・第11回重要インフラ専門委員会にて提示された「2007年度重要インフラにおける「安全基準等の見直し状況の把握及び検証」について」に基づき**実施**。
	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	・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。	・第11回重要インフラ専門委員会にて提示された「2007年度重要インフラにおける「安全基準等の浸透状況等に関する調査」について」に基づき**実施**。
	指針の見直し	・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**。	・第12回重要インフラ専門委員会にて提示された「2007年度重要インフラにおける「指針の見直し」について」に基づき検討を**実施**。
②情報共有体制の強化	情報共有体制整備と機能強化	・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・要件等を検討**。	**・CEPTOAR特性把握マップのとりまとめ**、**情報共有訓練**及びCEPTOARも参加した官民連携による**分野横断的演習**を実施。
	各重要インフラ分野における CEPTOAR 整備の推進	・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。	・新規追加3分野（水道、医療、及び物流）において、2007年度までに**整備を完了**。
	「CEPTOAR 特性把握マップ」のフォローアップ	・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**。 ・2007年度末を目処に、**CEPTOAR特性把握マップをフォローアップ**。	・重要インフラ所管省庁等の協力を得て、2007年度末現在の**各 CEPTOAR の特性を把握**するとともに、整備状況とあわせて**CEPTOAR 特性把握マップ(ver2)をとりまとめ**。
	「重要インフラ連絡協議会（CEPTOAR－Council）」（仮称）創設の検討	・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。	・CEPTOAR 代表者等から構成される「重要インフラ連絡協議会（CEPTOAR-Council）（仮称）創設に向けた検討の場」を設け、**8回の会合を開催**。 ・「検討の場」において、来年度以降の検討方針を**「「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な考え方」**としてとりまとめ。

③相互依存性解析の実施	重要インフラ分野間の相互依存性解析の推進	・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**検討の深化及び演習シナリオへの反映**、 ・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**。	・検討会を設置し、**検討会5回・WG7回**を実施。 ・「相互依存性解析における視点（考え方のポイント）」を整理しつつ、「**動的依存性解析」**を実施。 ・2006年度と2007年度に実施した解析結果を整理し「**相互依存性解析報告書**」としてとりまとめた。
④分野横断的な演習の実施	重要インフラ機能演習の実施	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、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、**分野横断的な機能演習を実施**。	・有識者、各重要インフラ分野の分野委員及び重要インフラ所管省庁からなる分野横断的演習検討会を設置し、検討会5回・WG5回を通じてシナリオ等についての議論を経て、約120名の参加を得て分野横断的な**機能演習を実施**した。
	各分野サイバー演習との連携	**分野ごとに実施される**「情報通信」等のサイバー**演習**と、内閣官房の実施する演習について、実施形態及びその目的の整合性を考慮しつつ**連携**。	・**情報通信分野及び航空分野**における机上演習に**NISCが参加**し、演習の実施手法等の知見を受けた。

（別紙）

～検証した具体的事例の概要～

ｉ）システム障害（非意図的要因）が発生した事例

（その１）

① 未明から6時間にわたって、利用者に関する情報を管理するシステムに障害が発生。当初は職員が手作業での処理により対応したが、午前 8 時ごろから対応が追い付かなくなり、サービスの停止や遅延が発生。

② システムを復旧させるため、待機系への切り替え等を行い、午後0時頃にシステム復旧。その間、当該事業者のサービス停止や遅延が発生。システム復旧後も、影響は翌日まで残存。影響を受けた利用者は約7万人。

③ 当該事業者からは後日、所管官庁に原因の報告がなされた。原因は、ハードウェア障害、高負荷状態による通信滞留、プログラムの設定ミスの3種類の障害が、ほぼ同時間帯に発生したことによるものと判明。また、再発防止策として、上記原因に対する技術的対策に加え、監視・運用体制の見直しや利用者への情報提供方法の改善等の管理的側面の対策についても報告。

（その２）

① 早朝、特定分野の16事業者において4378台の業務端末（利用料金清算等に関する端末）が起動しない不具合が発生。不具合の発生は午前4時過ぎに事業者が認知。その後、技術的分析を行いつつ、事態の重大性を判断し、午前5時に対策本部を設置。

② 仮復旧のための方法が確認できたため、当該措置を順次実施し、午前 11 時にはすべての措置を完了。また、一部の事業者においては、利用者の混乱回避のため、当該システム端末を使用せずに利用者へのサービス提供を行う措置を実施。

③ 当日中に原因をほぼ解明。翌日以降、改修ソフトを対象となる全端末にインストールする作業を実施。修正作業が完了するまでの間は、手動による対応を並行して実施。また、HP などにより、事業者から経過や原因など具体的な内容について公表。

④ 3日後に、同様の原因から別の情報処理端末にも不具合が発生。当該端末の製造業者側のチェック漏れにより、不具合発生の可能性についての報告はなかったため、事業者として事前の対応が取れなかったもの。

（その３）

① 特定分野の複数の事業者による特定のサービスにおいて、障害事例が複数回発生。利用者がサービスを利用できないなどの影響が発生。

② それぞれの障害の原因は、サーバ不具合、設備故障、ソフトウェア不具合、保守作業のミス等様々であり、特定の原因によるものではなかった。

③ 障害の発生以降、随時 HP により、復旧状況や原因、再発防止策などに関する情報が公表。

ⅱ）業務システムがウイルス感染した事例

① ホームページの閲覧で職員の端末にコンピュータウイルス（以下、ウイルス）が侵入。侵入したウイルスの感染活動により内部システムの広範にわたり感染が拡大した結果、業務システムに障害が発生し、サービスの継続に一部影響が発生。

② システム障害発覚後、解析により原因がウイルスによるものであることが判明したが、既に多くの端末やシステムへ感染が拡大。

③ ウイルス感染判明後、以下の応急的な措置を実施。翌日には通常体制で業務ができる状態に復旧。

・ネットワークシステムをインターネットから遮断

・業務システムの復旧を最優先し、その後にウイルス駆除を実施

復旧までの間は、未感染端末と手動による運用で対応したが、一部サービスに影響が発生。当該事業者のホームページで情報を掲載し、利用者等への周知等、混乱拡大の防止のための措置を講じた。なお、他の事業者への影響の拡大は確認されていない。

④ ウイルスの特定と駆除方法の特定に数日を要し、対応がほぼ収束するまでには 1 ヶ月以上要した。また、当該事業者においてはウイルス対策ソフトが導入されていたものの、当該ウイルスに対応していなかったため検出できなかったことが判明。