資料１０

NISC National Information Security Center

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年度の評価等について（案）

2008年 4月 3日

内閣官房 情報セキュリティセンター（NISC）

１．重要インフラ対策の２００７年度の評価等について

・行動計画の４本の施策の柱の取組みが着実に進んでいるか、**SJ 2007に盛り込まれた取組みの進捗度合い**を測る**【プロセス評価】**

・プロセス評価の補完として、行動計画に定める4本の施策に関して**参考となる以下のデータの推移**を捕捉しつつ、併せて**実際に発生したIT障害等のケース**を検証することで、重要インフラにおける情報セキュリティ対策向上の状況を把握。**【補完調査】**

１．安全基準等の整備の状況について

Ⅰ．各分野における安全基準等の認知率（A／α）
Ⅱ．各分野における安全基準等の見直し率（B／A ）
α：回収データ数
A：認知していると回答した事業者等の数
B：安全基準等を踏まえ見直しを行ったと回答した事業者等の数

※ なお、NISCにおいて検証する際の参考として、回収率（α／α´）を把握。
α´：調査協力を求めた事業者等の数
例：全事業者、○○加入者、任意抽出など。

２．情報共有体制の強化の状況について

Ⅰ．情報提供の件数 「実施細目」に規定する「情報提供」の件数（試験・訓練を含む。）

Ⅱ．CEPTOARを構成する事業者等の数

※ なお、NISCにおいて検証する際の参考として、構成事業者の分野における位置付けを把握。

３．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

解析及び演習に要した年間延べ時間および延べ参加者数

2. SJ 2007に盛り込まれた取組みの進捗度合いについて

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、以下の委員会等を開催し、それぞれ検討。

- 2007年度において、計7回の重要インフラ専門委員会を開催。
- 「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回のワーキンググループを開催。
- 「相互依存性解析」及び「分野横断的演習」については、2007年6月から2008年3月まで、それぞれ5回の検討会及び7回のワーキンググループを開催。

2007年度中に重要インフラにおける情報セキュリティ対策の強化のために取り組むとされていた、**12の具体的施策**は、全て3月末までに実施済み。

具体的施策

- □ 安全基準等の整備 ・・・ 安全基準等の見直し、見直し状況の把握、指針の見直し 等
- □ 情報共有体制の強化 ・・・ CEPTOAR整備の推進、「重要インフラ連絡協議会」創設の検討 等
- □ 相互依存性解析の実施 ・・・ 相互依存性解析の推進
- □ 分野横断的な演習の実施 ・・・ 重要インフラ機能演習の実施 等
- □ そ の 他 ・・・ 行動計画の見直し

3．参考となるデータ　【補完調査①】

1．安全基準等の整備の状況について

Ⅰ．各分野における安全基準等の認知率

97．9　%　「名称・内容ともに知っている」「名称のみ知っている」

Ⅱ．各分野における安全基準等の見直し率

54．8　%　「定期的に実施している」「実施したことがある」

調査依頼対象　2958事業者等
回　答　数　　2846事業者等（回収率96．2%）

※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、共通の重みづけで集計を実施。

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

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（$1\leq i\leq n$）

2. 情報共有体制の強化の状況について

Ⅰ. **情報提供の件数** 「実施細目」に規定する「情報提供」の件数（試験・訓練を含む。）

３　件　　（うち試験・訓練によるもの　２件）

Ⅱ. CEPTOARを構成する事業者等の数

全10分野　14CEPTOAR　　合計　5692事業者等

（内訳等の詳細は、「CEPTOAR特性把握マップ」に記載。）

3. 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

解析及び演習に要した年間延べ時間および延べ参加者数

【相互依存性解析】

検討会　5回

ワーキング　7回

延べ時間　92．5時間

延べ参加者数　395人

⇒計　622（人・時間）

【分野横断的演習】

検討会　5回

ワーキング　5回

延べ時間　39時間

延べ参加者数　473人

※うち、2008年2月6日実施の
演習当日参加者116名。

⇒計　1178（人・時間）

４．実際に発生したＩＴ障害等のケースの検証　【補完調査②】

重要インフラにおける情報セキュリティ対策の状況を把握し、併せて経験の共有の観点から課題等を抽出することを目的とする（個々の重要インフラ事業者等の対処の是否を問うことを目的とするものではない）。

検証は以下の視点を踏まえて行う。なお、重要インフラ事業者等が「安全基準等」により具体的に対応することが望まれる課題については、「指針」見直しの取り組みに反映させる。

- ＩＴ障害の未然防止、拡大防止、早期復旧のために実際にどのような対処が行われたか。
- 官民の情報共有体制、セプター等による事業者間での情報共有が、具体的にどのように機能したか。
- 他の事業者等からどのような影響を受け、あるいは他の事業者等へどのような影響を与えたか。
- その他、ＩＴ障害の未然防止、拡大防止、早期復旧の観点から得られた経験はあるか。

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」のほか、類似事例の発生状況（可能性）や社会的影響の大きさに着目し、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）を得ながら検証を行う。その際は、検証に協力した事業者等に不利益が生じないよう必要な配慮を行う。今年度については以下の事例を検証することとする。

- システム障害（非意図的要因）が発生した事例
- 業務システムがウイルス感染した事例
- 新潟県中越沖地震発生時の状況

～システム障害（非意図的要因）が発生した事例～

本年度重要インフラにおいて発生した、情報システム障害の発生を原因としたサービスの停止や機能の低下事例の中から、複数の事例をもとに検証。

事例の概要

（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。

（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。

（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。

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。

～業務システムがウイルス感染した事例～

インターネットを経由して業務システムがウイルス感染したため業務に支障が生じた事例について検証。

事例の概要

（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。

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、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について、完全な駆除を確認することは困難であり、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。

新潟県中越沖地震発生時（平成19年7月16日）の各重要インフラ分野における対応状況とIT障害等の発生状況について検証。

事例の概要

（1）地震の概要
- 震源地　新潟県上中越沖（北緯37度33分、東経138度37分）、震源の深さ17km
- 規模　マグニチュード6．8（最大震度6強：新潟県柏崎市、長岡市、刈羽村、及び長野県飯綱町）

（2）被害の状況
- 人的被害　新潟県を中心に、負傷者は長野県や富山県に及ぶ（死者15名、重傷329名、軽傷2,016名）
- 住家被害　新潟県を中心に、一部破損は長野県に及ぶ（全壊1,319棟、半壊5,621棟、一部破損35,070棟）

（3）重要インフラにおけるサービス停止等の状況　（IT障害に関連しないものも含む。）

分野	被害状況等	復旧状況　（複数日付ある場合は一番遅いもの）
情報通信	固定電話の不通（延べ約800回線）、発信規制の実施	7月17日　2:15までに復旧
	携帯電話基地局の停波（3事業者）、発信規制の実施（2事業者）	7月19日 19:47までに復旧
	専用線の不通（33回線）	7月16日 21:08までに復旧
	放送中継局の停波（5事業者）	7月18日 15:17までに復旧
金融	1事業者（2店舗）にて休業	7月18日営業再開
鉄道	7事業者にて運転中止	9月13日運転再開
電力	最大戸数35,344戸にて供給停止	7月18日 21:59復旧
ガス	復旧対象戸数31,179戸にて供給停止	8月27日復旧
医療	29施設にて被災（水漏れ、ひび等）	―
水道	58,961戸にて断水	8月4日復旧

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。

被害拡大の防止に効果があった対策の例

経験や教訓	対策例	重要インフラ行動計画との関係
素早い対応が必要である点を認識	災害時の参集手順等の危機管理ルールを策定	指針「事業継続性確保のための個別対策の実施」にて考慮
音声発信を中心に通信が集中	競合企業と協力し、災害用の伝言板サービスを相互に利用可能 （データ通信機能の利用が広がり、音声発信への通信集中を緩和）	電気通信分野の安全基準等において「ネットワーク輻そう」を対象とする脅威として定義し考慮
上層階は地震の揺れで検査が必要となって立入が不可	緊急時の対策本部を下層階に設置	指針「事業継続性確保のための個別対策の実施」にて考慮
店舗の自家発電機の運用・管理に不十分な点が存在	3ヵ月に一度、燃料と自家発電機の状況を点検 非常時の燃料手配の手順を明文化	指針「停電時の対応」「自己点検・監査の実施」にて考慮 相互依存性解析「電力分野と他分野との相互依存性」にて考慮
水道の供給停止により、サーバールームの加湿用水の確保が困難	貯蔵水の使用量を抑えるため、仮設トイレの手配を取り決め	相互依存性解析「水道分野と他分野との相互依存性」にて考慮

5．補完調査のまとめ

補完調査①及び補完調査②を総括すると、以下のとおり。

◎　IT障害から重要インフラを防護し、国民生活や社会経済活動に重大な影響を及ぼさないようにする観点からは、障害の未然防止だけでなく、障害発生時に影響を最小限に抑えるための機能回復に向けた対応（早期対応、応急対応など）も重要である。

◎　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、着実に向上しているものと考えられる。

◎　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なかった。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。