資料９

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２００８年度の評価等について（案）

2009年 4月 6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２００８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 2008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】**

・本年度が現行動計画の最終年度であることに鑑み、4本の施策の柱それぞれについて、2006年度～2008年度に得られた**「進捗状況の評価」、「補完調査により得られたデータの推移」及び「補完調査による個別のIT障害等の検証の結果」をNISCが総合的に見る**こととする。**【重要インフラ対策のあるべき姿に関する評価】**

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を踏まえた事業者の内規等の見直し率（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、取り得る具体的調査方法も踏まえ、各分野における状況を把握する上で適切な調査範囲を設定。
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

※ *1. 安全基準等の整備の状況については、2007年度の評価の際の課題を踏まえて運営サイクルの調整を図り、調査時期を2009年度の前半としているため、その評価については、2009年度の評価に係る文書に内容を反映する。*

2. SJ 2008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。

- ◆ 2008年度において、計9回の重要インフラ専門委員会を開催。
- ◆ 「セプターカウンシル創設準備会」を設け、2008年7月から2009年2月まで、3回の会合及び6回のワーキンググループを開催。2009年2月にセプターカウンシルが創設され、第1回総会（設立総会）を開催。
- ◆ 「相互依存性解析及び分野横断的演習検討会」を設け、2008年7月から2009年3月まで、解析は検討会3回、作業部会2回、演習は検討会5回、作業部会3回を開催。

2008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、13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、見直し状況の把握及び検証 等
- □ 情報共有体制の強化 ・・・ セプターカウンシルの創設の検討、実施細目の見直し 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．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。）

９件　　（うち試験・訓練によるもの　１件）

Ⅱ．CEPTOARを構成する事業者等の数

全10分野　14CEPTOAR　　合計　5，608事業者等

（内訳等の詳細は、「CEPTOAR特性把握マップ」に記載。）

3．参考となるデータ　【補完調査②】

2. 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】

延べ時間　41時間

延べ参加者数　321人

延べ参加人・時間　513人・時間

（参考）

検討会　3回

作業部会　2回

個別打合せ　20回

【分野横断的演習】

延べ時間　57時間

延べ参加者数　662人

延べ参加人・時間　1，455人・時間

（参考）

検討会　5回

作業部会　3回

個別打合せ　37回

演習当日（2008年12月1日）参加者数

136人

４．実際に発生したＩＴ障害等のケースの検証　【補完調査②】

目的・スタンス

○現実のリスクとそれに対する対応状況の変化を見ることで、重要インフラ分野の情報セキュリティ対策を進めた結果、生じた変化を把握することによりプロセス評価を効果的に補完する。
○検証にあたり、所管省庁及び重要インフラ事業者等の協力（情報提供・ヒアリングの実施等）を得るに当たっては、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。

検証の観点

検証の目的・スタンスに照らして、以下の点について検証を行う。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。
・安全基準等は、被害の発生防止、拡大防止に関し、充分なものであったか。
・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。
・他の事業者等から受けた影響、あるいは他の事業者等へ与えた影響はあったか。
・その他、被害の未然防止、拡大防止、早期復旧の観点から得られた経験はあるか。

4．実際に発生したＩＴ障害等のケースの検証　【補完調査②】

検証の対象とする事例

実際に発生した「IT障害」及びIT障害の要因となり得る「脅威」について、類似事例の発生状況（可能性）や社会的影響（関心）の大きさを考慮して以下のものから選定する。

脅威	事例
意図的要因 （サイバー攻撃）	ホームページの不正アクセス及び改ざん
非意図的要因	システム障害
災害（地震）	岩手・宮城内陸地震 岩手県沿岸北部を震源とする地震

～ホームページの不正アクセス及び改ざん事例～

SQLインジェクションにより情報システムが改ざんされた事例について検証。

事例の概要

（1） 利用者からホームページの表示がおかしいとの指摘を受け、状況を確認した結果、ホームページ上に不審な文字列が表示されていることを確認した。このため、直ちにサーバをネットワークから切り離した上で、ホームページの運営管理委託事業者等に連絡するとともに利用者にサービス休止の旨を通知した。

（2） 当該サーバのログを調査した結果、某国から「SQLインジェクション」による攻撃を受け、データを改ざんされたことが判明したが、システムの特性から情報の漏えいや利用者が悪意のあるサイトに誘導されることはなかった。

（3） サービス停止の翌日には必要性の高い機能を代替サイトで提供、約2週間後に暫定対処を施して一部の機能について仮復旧を行い、3ヶ月後に全サービスの復旧を完了した。

主な修正内容は次のとおり。

- 当該サービスを提供するために作成したアプリケーションの脆弱性の修正（ユーザ入力データの妥当性チェック機能の強化、不正コード発見時におけるログの保存機能の追加）
- データベースアクセス権限の見直し（SQLサーバーの実行権限の限定、ユーザID、PWの変更）
- Webサーバの設定変更（不正コードの送信に対する返答方法の変更）

（4） 当該事業者は情報漏えい時の対応マニュアルを策定しており、報告手順と報告様式を予め定めていたため、一連の対応を迅速に行うことができた。

- 被害を受けてから発覚まで4時間
- 被害の発覚から
  - 被害を受けたシステムの切り離し判断に20分
  - 30分後にホームページにお詫びと警告を掲載
  - 4時間後に事故概要をほぼ特定
  - 5時間後には経営層に報告
  - 8時間後にはプレス発表を実施

今回の改ざんはシステム構築後のOS等のパッチ適用、バージョンアップは実施していたものの、当該サービスを提供するために作成したWebアプリケーションの脆弱性に対する検証、対策が不十分だったことが大きな原因である。

～ホームページの不正アクセス及び改ざん事例～

検証結果

◆　システム構築当初に想定していなかった不正行為による被害であったことから、社会動向の変化に伴う技術的対策の見直しを適宜に行うことが肝要であることが確認できた。

◆　最初の障害の認知は、利用者からの通報によるものであり、早期の障害認知に役立った。

◆　障害発生時における対応において、報告手順等を定めた対応マニュアルを事前に策定していたことから迅速な対応が行われており、事前の対応手順等の整備をしておくことが有効であることが確認できた。

◆　意図的攻撃により被害を被ると、復旧までに多くの時間やコストがかかる場合があることが確認できた。

課題・留意点

◎　社会動向の変化に伴う情報システムのセキュリティ要件の見直し、システム全体としてのセキュリティチェックの実施、対策の検討、対策の実施といったPDCAサイクルの考えを踏まえたセキュリティ対策の実施が必要ではないか。

◎　利用者や職員からの通報も被害による障害の発生の認識に役立つものであることから、通報があった場合の扱いをマニュアルに示すなどにより活用できるのではないか。

◎　被害を受けてから障害を認識し、適切な判断を行うまでの時間を短くするという観点から、報告手順、様式等の整備等により迅速に対応できる体制を構築するための取り組みを進めることが必要ではないか。

◎　このような事例を詳細に分析し、そこから教訓を得た上で幅広くその情報を共有していくことが重要であり、そのためには情報共有の枠組みをうまく活用していくことが必要ではないか。

～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 業務開始時より利用者に関する情報を管理するシステムに障害が発生し、当該システムの端末が使用できなくなったことから、サービスの提供に支障が生じた。

② 端末の開発メーカー等にも協力を仰いだが、原因究明に時間を要した。午前中より暫定対応によりサービスの提供を再開した。完全対応には3日程度の時間を要した。影響を受けた利用者は約7万人。

③ 障害の原因は、当初、認証機能を利用していなかったシステムに認証機能を利用する端末を追加して導入した際、認証機能の有効期限の確認を遺漏していたために有効期限が当初納入時のままであったことから、当該機能が有効期限切れとなり、当該端末が業務開始時にエラーとなったもの。

（2）① サービスの提供に必要なシステムを制御するコンピュータが故障したことから、当該システムが制御不能となったため、サービスの提供に支障が生じた。

② 復旧に4時間弱程度の時間を要した。影響を受けた利用者は約7万人。

③ 障害の原因は、当該制御コンピュータの機器故障によるものであった。当該装置は二重化され、故障時には切り替わる機能とされていたが、切り替えのためのソフトウェアにも不具合があったことから、切り替えができなかったもの。

～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必要な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できた。

◆　検証事例においては、システムの構築、増設、更新時における障害の原因の発見、除去等に関して課題があることが確認できた。

◆　利用者への影響の最小化を図るという観点からも障害が発生した場合に、早期復旧を可能とする方法、体制を整備することの重要性が確認できた。

課題・留意点

◎　障害発生を未然に防止するためには、システムの構築、保守時における障害の原因の発見、障害の要因となり得る不具合の除去等を着実に行なうことが重要であり、このために必要な対策を実施していくことが必要ではないか。

◎　費用対効果の観点も勘案しつつ、適切な早期復旧を可能とする方法、体制の整備を図っていくことが必要ではないか。

◎　このような事例を詳細に分析し、そこから教訓を得た上で幅広くその情報を共有していくことが重要であり、そのためには情報共有の枠組みをうまく活用していくことが必要ではないか。

～今年度発生した大規模地震の状況～

今年度発生した大規模地震における被害状況、IT障害等の発生状況について検証。

事例の概要

1．岩手・宮城内陸地震（発生日時：2008年6月14日8：43）

（1）地震の概要

- 震源地　岩手県内陸南部（北緯39度02分、東経140度53分）、震源の深さ8km
- 規模　マグニチュード7．2（最大震度6強：岩手県奥州市、宮城県栗原市）

（2）被害の状況（11月19日現在）

- 人的被害　岩手、宮城県を中心に、死者・行方不明者は秋田県や福島県に及ぶ（死者13名、行方不明者10名、重傷81名、軽傷370名）
- 住家被害　岩手、宮城県を中心に、一部破損は秋田県に及ぶ（全壊33棟、半壊138棟、一部破損2，181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（95回線）、通信規制の実施（1事業者）	9月17日復旧（※）
	携帯電話基地局の停波（3事業者）、通信規制の実施（3事業者）	9月17日復旧（※）
	専用線の不通（7回線）	6月25日復旧（※）
鉄道	1事業者2路線にて運転中止	6月15日運転再開
電力	最大戸数29，005戸にて供給停止	停電中の戸数：5戸 （08年11月18日現在）
ガス	5戸にて供給停止	6月15日復旧
水道	5，560戸にて断水	8月13日復旧

（※）道路等の寸断により、復旧作業ができなかったもの

今年度発生した大規模地震における被害状況、IT障害等の発生状況について検証。

事例の概要

2．岩手県沿岸北部を震源とする地震（発生日時：2008年7月24日0：26）
（1）地震の概要
- 震源地　岩手県沿岸北部（北緯39度44分、東経141度38分）、震源の深さ108km
- 規模　マグニチュード6．8（暫定値）、（最大震度6弱：岩手県野田村、青森県八戸市、五戸町、階上町）

（2）被害の状況
- 人的被害　青森、岩手県を中心に、死者、負傷者は福島、宮城県に及ぶ（死者1名、重傷35名、軽傷176名）
- 住家被害　青森、岩手県を中心に、一部破損は宮城県に及ぶ（全壊1棟、一部破損377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	通信規制の実施（2事業者）	7月24日復旧
	携帯電話基地局の停波（3事業者）、通信規制の実施（3事業者）	7月24日復旧
鉄道	2事業者3路線にて運転中止	7月25日運転再開
電力	最大戸数8，276戸にて供給停止	7月24日復旧
ガス	18戸にて供給停止	7月30日までに復旧
水道	1，364戸にて断水	8月4日までに復旧

～今年度発生した大規模地震の状況～

検証結果

◆　最大震度は大きく、ある程度の被害は発生したものの、震源地が山間部だったこともあり、重要インフラに関する被害は昨年度に発生した新潟県中越沖地震と比較すると総じて少なかった。ただし、一部地区では大規模な土砂崩壊に伴い道路、伝送路の寸断等が発生し、それに伴う障害の発生が認められた。

◆　事業者は、あらかじめ整備された災害対策規程等に基づき迅速に災害対策本部を設置し、オペレーションセンターでの設備監視などにより被災情報等の把握、共有等を行った。道路の寸断等により陸路での現地の被災状況確認や必要な資機材の搬送等には困難が伴ったが、ヘリコプターによる現地確認、資機材の搬送等は機動性が高く有効なことが確認できた。

◆　被害を被った事業者においては、過去の大規模地震発生時の教訓を踏まえた非被災地域からの広域支援が今回も実施され、有効に機能することが確認できた。

課題・留意点

◎　山間地での土砂崩壊による道路寸断等を伴うIT障害の場合、サービスの復旧には道路、伝送路といった各種インフラの同時復旧が必要となり、被害地域が限定的なものであっても、復旧には相応の時間を要する場合がある。

◎　災害への迅速な対処においては、予め災害対策規程等を整備することが有効である。

◎　非被災地域からの広域支援は有効であることから、今後とも可能な範囲で広域支援に係る取り組みを継続していくことが重要ではないか。

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障害が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、未然防止だけではなく、障害発生時の影響の最小化のための対応が重要であり、そのための事前の準備が有効である。

◎　個々の重要インフラ事業者等の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、早期復旧を可能とするための体制や規程の整備等が着実に進展しているものと考えられる。

◎　一方、他分野、他事業者の「経験」から得られた知見共有の重要性は改めて確認されたが、事業者間や分野間での情報共有について、現時点で活発に取り組まれていることは確認できなかった。

こうした経験や過去の教訓を共有していくことが重要であり、政府内の連絡体制やセプター、セプターカウンシルに期待される役割を如何に発揮していくかが今後の課題である。

6．重要インフラ対策に関する「あるべき姿」の達成に係る評価

2006～2008年度の評価及び補完調査を総括すると、以下のとおり。

◎　官民の緊密な連携の下、重要インフラの情報セキュリティ対策を強化するために2006～2008年度の間に取り組むとされた行動計画の4本の柱の38の具体的な施策は、2008年度末までにすべて実施済みである。これにより、関係主体間の連携の基礎が整うとともに、各関係主体において情報セキュリティ対策の充実に資する気付きや共通認識の醸成を進める土壌が育ちつつあるということができる。

◎　一方、これらの取組みを進める間にも、ITの利用の拡大は進んでおり、ITへの依存度は益々高まる傾向にある。IT障害が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、未然防止だけでなく、IT障害発生時の機能回復に向けた取り組みも重要であり、事前及び事後の対策をバランス良く行う必要がある。対策の着実な向上に資するため、今後も、指針及び安全基準等の適切な見直し及び浸透を図ることが引き続き課題になると考えられる。

◎　また、障害発生時の情報や他分野、他事業者の経験から得られた知見の共有の重要性が認識されており、政府内の連絡体制、セプターやセプターカウンシルなどの情報共有の枠組みの有効な活用を含め、それぞれの関係主体に期待される役割をいかに発揮していくかも今後の課題である。

◎　これらの課題への対応に当たっては、関係主体間の円滑な協力が可能となるよう、重要インフラ事業者等の取組みにおける多様性を十分に踏まえ、重要インフラ事業者等間、分野間等の相互理解を深め、共通認識の醸成に努めることが重要である。