資料5

NISC National Information Security Center

2007年度　重要インフラにおける「指針の見直し」（中間報告）について【参考資料】

2008年 1月 31日

内閣官房 情報セキュリティセンター（NISC）

①定常的なIT障害の発生状況の分析

IT障害の発生状況の分析 （１）システム障害によるサービス停止、低下

分析内容：

- システムの仕様やプログラム上の欠陥（バグ）等、非意図的要因によるシステム障害（※）の発生状況を分析

※行動計画上の重要インフラのIT障害に該当しない事例も含めて分析

分析結果：

① 新技術により構成されたシステムの障害が再発

時期	概要
2007年 （複数回発生）	さまざまな原因及び影響範囲にて、IP電話のサービス障害が発生

② IT化により利便性が向上する一方で、障害時には手作業で対応できる限界を超えてしまう事象が発生

時期	概要
2007年5月	予約システム障害により、全国の空港の予約･発券業務の処理能力が低下
2007年10月	首都圏にて特定の自動改札機がプログラムミスにより、660駅で4400台が停止

- IT障害の影響が想定範囲を超える事例や検証フェーズでプログラムミスが見つけられていないと想定される事例が散見される。
- 新しいシステムを構築する際には、**よりきめ細かなシステム設計及び検証**や不適切な入力を排除する工夫が望まれる。
- IT依存の一層の深化に伴い、**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。

IT障害の発生状況の分析（2）サイバー攻撃等

分析内容：
- 不正侵入、改ざん、ウイルス攻撃等、サイバー攻撃によるIT障害の発生状況を分析

分析結果：

① **不正侵入によるWebサイト改ざんが発生**

時期	概要
2007年10月	Webサイトが21回にわたり改ざんされ、閲覧でウイルス感染の可能性
2007年11月	Webサイトへの不正アクセス被害により、フィッシングサイトが設置 Webサイトへの不正アクセス被害により、全ページにウイルスが埋め込まれた

② **ウイルスが埋め込まれたWebサイトへのアクセスによるウイルス感染が発生**

時期	概要
2007年9月	パソコンがインターネット経由でウィルス感染し、各部署の業務用ソフトが停止

③ **不審メールによる攻撃が発生**

時期	概要
2007年9月	新首相を騙るウィルスメールが出現
2007年12月	パスワードなどを聞き出す不審メールが発生

- **フィッシングサイトの設置による営利目的の攻撃の発生に加え、Web閲覧のみでのウイルス感染等より巧妙な手法に変化してきている。**
- **経済的利得や政治的背景等から特定の個人や組織を対象とするスピア型（標的型）攻撃が発生している。**
- **顕在化しつつある新たな手法によるサイバー攻撃について注意を払い続けることが望まれる。**

IT障害の発生状況の分析　（3）情報漏えい

分析内容：
- 情報漏えいの発生状況を分析

分析結果：
- **Winnyを介して感染するコンピュータウィルスによる情報流出についての注意喚起を行ってきたが、その後もファイル交換ソフトを通じた情報漏えいが発生**

時期	概要
前回見直し以降も継続して発生	重要インフラ分野においてもファイル交換ソフトによるネットワークを介した情報漏えいが報道された。Winnyの使用による情報漏えい以外にも、Share等を使用することによる情報漏えいが散見される。

＜参考＞「Winnyを介して感染するコンピュータウイルスによる情報流出対策について」（2006年3月15日内閣官房情報セキュリティセンター）より抜粋

3. 重要インフラ事業者等への注意喚起

国民生活や社会経済活動の基盤である重要インフラ事業者等における機密情報や重要情報等の漏えいは、その機能の停止・低下等につながるおそれがあることから、重要インフラ事業者等に対して、対策を徹底すべく、注意喚起を行うよう、本日付で所管省庁に要請します。

- **ファイル交換ソフトを通じた情報漏えいが、継続的に発生し続けている。**
- **情報漏えいを防止するための継続した取り組みが望まれる。**

③関連文書の検証

関連文書の検証　（1）規格文書・ガイドライン等

検証内容：
- 前回見直し以降に制定/改正された国内外の規格文書・ガイドラインから、情報セキュリティ対策の観点を検証

検証結果：
- 規格文書・ガイドライン等を以下の6つに分類して検証（文書名は次頁）

	分類	概要
1	**ITSMS（ITサービスマネジメントシステム）適合性評価制度**	**昨年検証した国際標準**（ ISO/IEC 20000-1:2005, ISO/IEC 20000-2:2005 ）**がJIS化され、ITサービスマネジメントシステムの認証制度が開始されている。** ※昨年は「ITサービスマネジメントについてのPDCAサイクルの運用を規定」を検証結果として導出
2	**個人情報保護法関係**	**昨年同様に法律の運用**（過剰反応に対する見直し、委託先に対する監督義務に対する見直し等）**を踏まえたガイドラインの改正や**行政の透明性向上の観点から**Q&Aの提供が行われている。** ※昨年は「Q&Aの内容反映や法令改正に伴う所要の改正」を検証結果として導出
3	**分野ガイドライン**	先進的な取組みとして、一部の重要インフラ分野においては、ITガバナンスの構築に向けてのガイドや、**PDCAサイクルのC（評価）の中心となる監査実務の際に参照する文書が提供されている。**
4	**システム品質向上**	情報システムの信頼性向上を図るためのガイダンスや指標等が提供され、**目に見えないソフトウェア開発の品質を確保するための共通の物差しである「共通フレーム2007」において、新たに要件定義、契約の変更管理の各プロセスを追加している。**
5	**金融商品取引法（内部統制）関連**	いわゆる日本版SOX法と呼ばれる**金融商品取引法の内部統制報告制度の施行に関連して、昨年の検証以降、内閣府令・ガイドライン及び**IT統制を構築する**企業向け・**内部統制監査を行う**監査人向けのガイダンス等、多数の文書が提供されている。** ※昨年は「PDCAサイクルの適用（内部統制の構築で求められている「ITへの対応」）を検証結果として導出
6	**BCM（事業継続管理）関連**	**昨年検証した国際標準化に向けた各国の動きに加え、国内外で標準・ガイドラインの制定が行われている。** ※昨年は「PDCAサイクルの適用（事業継続計画）」を検証結果として導出

＜参考＞規格文書・ガイドライン一覧　（2007年以降に策定/改正されたもの）

	分類	名称	発行年月	備考
1	ITSMS適合性評価制度	日本規格協会「JIS Q 20000-1:2007 情報技術－サービスマネジメント－第1部：仕様」「JIS Q 20000-2:2007 情報技術－サービスマネジメント－第2部：実践のための規範」	2007年4月	ISO段階の文書について昨年検証済
2	個人情報保護法関係	経済産業省「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」	2007年3月	2007年12月再見直しを行い、パブコメ実施
		金融庁「金融機関における個人情報保護に関するQ＆A」	2007年10月	
3	分野ガイドライン	FISC「金融機関等のシステム監査指針（第3版）」	2007年3月	
		総務省「地方公共団体における情報セキュリティ監査に関するガイドライン」	2007年6月	
		総務省「地方公共団体におけるITガバナンスの強化ガイド」	2007年7月	
4	システム品質向上	経済産業省「情報システムの信頼性向上に関する評価指標（試行版）」	2007年4月	
		経済産業省「情報システム・モデル取引・契約書」	2007年4月	
		経済産業省「情報システムに係る相互運用性フレームワーク」	2007年6月	
		IPA「共通フレーム2007」	2007年9月	
5	金融商品取引法（内部統制）関連	金融庁「金融商品取引法制に関する政令・内閣府令」	2007年7月	
		金融庁「証券取引法等の一部を改正する法律の施行等に伴う関係ガイドライン」	2007年10月	
		日本公認会計士協会　監査・保証実務委員会報告「財務報告にかかる内部統制の監査に関する実務上の取り扱い」	2007年10月	
		経済産業省「システム管理基準　追補版（財務報告に係るIT統制ガイダンス）」	2007年3月	案段階の文書について昨年検証済
		経済産業省「システム管理基準　追補版（財務報告に係るIT統制ガイダンス）　追加付録」	2007年12月	
		ITGI/ISACA「COBIT4.1」	2007年5月	
6	事業継続管理関連	内閣府（防災担当）「中央省庁業務継続ガイドライン」	2007年6月	
		英国規格協会「BS25999-2（Business continuity management-Part2:Specification）」	2007年11月	
7	その他	総務省「ASP・SaaSにおける情報セキュリティ対策ガイドライン」	2008年1月	
		経済産業省「SaaS 向けSLA ガイドライン」	2008年1月	

関連文書の検証　（2）政府機関統一基準

検証内容：

- 政府機関の情報セキュリティ対策のための統一基準（第2版）（2007年6月14日情報セキュリティ政策会議）の改訂に向けた検討状況を検証

検証結果：

・ **政府機関の情報セキュリティ対策のための統一基準（第3版改訂案）**（2007年12月12日情報セキュリティ政策会議）

Ⅰ 技術・環境の変化の反映

〇ドメインネームシステム（DNS）に関する対策、監視機能 、政府機関サイトへの成りすまし対策

→重要インフラ分野ごとに分野の特性・態様等を踏まえ、これらの対策についても検討する必要があると考えられる。

Ⅱ 実務に即した見直し

〇遵守事項の明確化、用語の整理

Ⅲ 参考：政府統一基準解説書の記述の明確化

〇国民等がPCにダウンロードするソフトウェアの安全性確保についての解説を充実

- **重要インフラ分野ごとに分野の特性・態様等を踏まえ、技術・環境の変化の反映について検討する必要があると考えられる。**

④社会的条件（環境）の変化の検証

社会的条件の変化の検証 （１）情報技術、情報セキュリティ動向

検証内容：
- 社会一般における情報技術や情報セキュリティ動向を踏まえた新たな脅威の発生・新たな対策の確立の動向を検証

検証結果：

① **IPアドレスの枯渇**
- APNICの予測によると3～5年後には現在IPネットワークで利用されているIPv4アドレスが枯渇する。
- 根本的な対策はIPv6への移行であるが、IPv4とIPv6は互換性がないため大掛かりな対応が必要であり、他のネットワークやシステムの利用者の環境も含め中長期的な対応することが必要。
- インターネットやLANを利用する場合は、IPv4とIPv6の並行稼動期間を置いてた上で、IPv4の並行が不要になる段階でIPv6に完全移行することが想定される。
- 重要インフラ事業者においても、IPv6への移行を検討し、システムの整備計画と整合を図ることが望まれる。
- IPv6に移行する場合は、IPv4の時と同等以上のセキュリティ対策を確保することが望まれる。

② **JRE（Java Runtime Environment）問題**
- 政府機関等の電子申請・届出システムを利用するには、申請者の端末に脆弱性が顕在化しているJRE（Java Runtime Environment）をインストールしなければならないという問題が発生
- 提供されたアップデートに対する検証等の必要な対応が遅れることにより、問題が大規模化した。
- JREに限らず、一般に提供される市販ソフトウェアやフリーウェア等の脆弱性は、ゼロデイ攻撃の対象となることがある。また、脆弱性に対するアップデートは公表ベースになることが多く、適切に対応することが望まれる。

- **インターネットの普及により、IPv4プロトコルでのIPアドレス不足が予測されているため、IPv6への移行に向けての適切な対応が望まれる。**
- **市販ソフトウェアやフリーウェア等の脆弱性に対してベンダー等から修正プログラムが提供される際の運用について適切な対応が望まれる。**

社会的条件の変化の検証 （2） IT活用範囲の拡大

検証内容：
- 重要インフラ事業者等におけるITを活用したサービス拡大の状況を検証

検証結果：

・ 重要インフラ事業者等におけるITを活用したサービス拡大の状況として、以下の事例がある。

概要
電力事業者における携帯電話による利用料金の支払いサービス
航空運送事業者による航空券の電子化
鉄道乗車券のICカード化と鉄道事業者間の相互運用
共通カードにて、航空券の電子化と鉄道乗車券のICカード化を予定

・ IT化により利便性が向上する一方で、障害時には手作業で対応できる限界を超えてしまう事象が発生している（「①定常的なIT障害の発生状況の分析」より）

- **IT活用範囲の拡大により、既に安全基準等の対象となっている場合もあるが、必ずしも現在の安全基準等の対象とならないサービスが開始・拡大されており検討が望まれる。**

社会的条件の変化の検証 （3）重要インフラ行動計画に関する動向

検証内容：
- 重要インフラ行動計画に関する動向を検証

検証結果：

① 情報共有体制の強化
- 2007年度末までに、新規追加分野（医療、水道及び物流）において情報共有・分析機能（CEPTOAR）が整備されるよう取組みが進められている。
- 2007年度中に重要インフラ連絡協議会（CEPTOAR-Council）（仮称）の創設についての検討の場を開催し、課題についての検討が進められている。
- なお、政府・行政サービス分野（地方公共団体）においては、2006年度に自治体ISAC（仮称）実証実験として、IT事故を想定した演習が行われた。また、電気通信事業分野においても、2006年度と2007年度にサイバー攻撃対応演習が行われた。

② 分野横断的な演習の実施
- 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、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の実施に向けた検討が進められている。
- 各分野サイバー演習との連携として、電気通信事業分野におけるサイバー攻撃対応演習との連携を図っている。
- 関係機関（IPA、JPCERT/CC）は、重要インフラに対して特に影響が大きいと推察される脆弱性関連情報について、政府や重要インフラ事業者等への一般公表前の情報提供が行えるよう「早期警戒パートナーシップガイドライン」を改訂した。

- **追加3分野（医療、水道、物流）の情報共有・分析機能（CEPTOAR）整備に向けての検討がなされている。**
- **重要インフラ連絡協議会（CEPTOAR-Council）（仮称）の創設についての検討がなされている。**
- **政府、重要インフラ分野、CEPTOAR、関係機関等の協力を得て、分野横断的な機能演習の実施に向けた検討がなされている。**

社会的条件の変化の検証 （4） 大規模なIT障害に至らなかった例

検証内容：
- 大規模なIT障害の発生が懸念されたが、それに至らなかった事例における知見や教訓を検証

検証結果：

・ 自然災害

時期	概要
2007年7月	新潟県中越沖地震（最大震度6強）により、停電・断水・通信の輻輳・ガス供給の停止等が発生したが、いずれも小規模・比較的短時間で復旧。 • 情報通信分野では、危機管理ルールの徹底や競合企業との協力等、2004年10月新潟県中越地震での教訓を受けた対応により、速やかな復旧を行うことが可能であった。 • 金融分野でも、初動体制の見直しや定期的な燃料と自家発電機の状況の点検等、2004年10月新潟県中越地震での教訓を受けた対応により、サービス継続が可能であった。 • 電力分野では、ITの機能不全によるサービス停止はなかった。なお、原発の地震計全97台中63台の本震データが、通信回線輻輳のため伝送完了前に次々に発生した余震の揺れにより上書されたが、2004年10月中越地震の知見を元に設置した30台の新設地震計は、データ喪失を免れた。

- **2007年7月の新潟県中越沖地震において、一部重要インフラのサービス停止はあったものの、過去事例の知見や教訓を受けた対策もあり、情報システムでは比較的軽微な障害にとどまった。**