資料3

NISC National Information Security Center

重要インフラにおける「指針の見直し」の分析・検証に基づく指針への反映について

2009年 7月 7日

内閣官房 情報セキュリティセンター（NISC）

「指針見直し」の分析・検証におけるアプローチ

○今回の分析・検証においては、以下の5つのアプローチから検討が必要な課題を抽出し、指針への反映方法を判断する。
○今回の「指針の見直し」は、第2次行動計画策定後最初の見直しであるため、第2次行動計画の反映をアプローチに追加する。

◆指針見直しの分析・検証における5つのアプローチ

①第2次行動計画の反映：
指針（骨子案）に対して第2次行動計画の内容をどのように反映するか。

②定常的なIT障害等の発生状況の分析：
2008年度に発生したIT障害の事例から、得られた教訓をどのように指針に反映するか。

③行動計画に基づく施策の成果：
第1次行動計画に基づき、2008年度までに取り組んできた施策の成果をどのように反映するか。

④関連文書の検証：
情報セキュリティ対策に関連する文書等をどのような観点で指針に盛り込んでいくか。

⑤社会的条件（環境）の変化の検証：
技術面、経営面、法制面及びその他の社会的動向の観点から重要インフラの情報セキュリティ対策に及ぼす変化に対して、指針ではどのように反映していくか。

◆STEP1
各アプローチに基づく問題意識の抽出

状況検証：①第２次行動計画の反映

第2次行動計画の策定を踏まえ、各重要インフラ分野に共通する情報セキュリティ対策等の新たな観点の検証を実施

	概要	検証結果
（1）全体の枠組み	●第2次行動計画の全体的な枠組みについて、第1次行動計画からの変更点を検証 ・重要インフラサービスという観点の追加 ・IT障害の脅威の見直し	●**第2次行動計画において重要インフラサービスという観点を追加し、**重要インフラ事業者等が提供するサービス等のうち、特に防護すべき重要インフラサービスを重要インフラ分野毎に定め、**それを踏まえた全体的な枠組みについて見直しを実施**した。 ・重要インフラサービスの提供に必要な情報システムのうち、重要インフラ事業者等毎に**重要システム**を定めることとした。 ・重要インフラ事業者等は**サービスレベル**を定めることとした。 ・重要インフラ分野毎に**検証レベル**を定めた。 ・重要インフラサービスにおいて発生する障害（サービスレベルが維持出来ない状態等）のうち、ITの機能不全が引き起こすものを**IT障害**と定義した。 ●**IT障害の脅威の類型に他分野からの波及を追加**し、社会全体で対応が望まれる脅威と事業者による個別対応を中心とする脅威に分類した。
（2）安全基準等の整備及び浸透に関する施策	●安全基準等の整備及び浸透に関する施策について、第1次行動計画からの変更点を検証 ・指針の継続的改善 ・指針の内容の充実 ・安全基準等の継続的改善 ・安全基準等の浸透 ・事業継続計画の観点 ・対外的な説明への取組み	●**指針の継続的改善を3年に1度実施する「指針の改定に関する検討」と毎年及び必要に応じて実施する「分析・検証」に分類**した。 ●**参考事項、具体化の例示等の追加により、指針の充実**を図る。 ●対策の共有を促進するため、従来検証対象となっている安全基準等の他に**情報セキュリティに関する基準や参考文献等を改めて広く安全基準等として整理**することが望まれる。 ●**安全基準等の浸透に向けて、対策を実装するための環境整備**に努め、**「安全基準等の浸透状況等に関する調査」を定期的に実施**する。 ●**事業継続計画の策定状況等を踏まえ、指針の内容を充実**させる。 ●**情報セキュリティ監査の実施やセキュリティ報告書の作成等の自主的な取組み**を一層推奨し、**情報セキュリティ対策の対外的な説明**に努める。
（3）その他の施策	●第２次行動計画で新たに追加された施策について、第１次行動計画における記載と比較・検証 ・リスクコミュニケーション	●必要な範囲内での**リスクコミュニケーション**に努めるとともに、**公表に差し支えない範囲で情報セキュリティ対策の開示**に努める。

状況検証：②定常的なIT障害等の発生状況の分析

前回見直し以降の主要なIT障害の発生状況から、各重要インフラ分野に共通する横断的な対策課題の分析・検討を実施

	概要	検証結果
(1)サイバー攻撃等	● 不正侵入や改ざん等が昨年度に引き続き報告されており、その状況を分析 ・SQLインジェクションによる不正侵入、Webサイトの改ざんが散見される。	● **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**が望まれる。 ● **利用者や職員の通報も障害発生の認識に役立ち、通報の取り扱いをマニュアルに示した上での活用**が望まれる。 ● 障害の認識から適切な判断を行うまでの時間短縮の観点で、**報告手順、様式等の整備等により迅速に対応できる体制構築**の取り組みが望まれる。
(2)システム障害によるサービス停止、低下	● 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 ・IT化による業務の効率化で省力化などが可能となる一方、障害が発生した際には、手作業での対応限界を超え、サービスの提供に一定の支障が生じている場合がある。	● 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望まれる。 ● 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**が望まれる。
(3)情報漏えい	● 情報漏えいの発生状況を分析 ・Winny等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は引き続き発生している。	● ファイル交換ソフトを通じた情報漏えいについては、情報セキュリティの関係主体などの度重なる注意喚起にもかかわらず継続的に発生している。 ● **情報漏えいの防止に向けた実効性ある対策、被害を最小化するための継続的な取り組み**が今後も望まれる。

状況検証：③行動計画に基づく施策の成果

第１次行動計画に基づき、2008年度までに取り組んできた施策の成果を踏まえ、各重要インフラ分野に共通する情報セキュリティ対策等の新たな観点の検証を実施

	概要	検証結果
（1）指針見直しの要点の反映	●2007年度の指針見直しによって得られた成果について検証 ・水道分野と他分野との相互依存性 ・IT障害の脅威の定義、及び、重要インフラ事業者等、重要システムの範囲 ・経験やベストプラクティスの共有 ・IPv6への移行を行う場合の適切な対応	●**水道分野のサービス停止や機能の低下等により、他分野のシステムが機能不全に陥る恐れ**がある。 ●**IT障害の脅威の定義等について、第2次行動計画において見直しを実施した。**（「①第2次行動計画の反映」を参照） ●各**重要インフラ分野及び重要インフラ事業者等の取組みから得られる知見・教訓等を踏まえた指針の充実**を図る。 ●第2次行動計画別紙3のIT障害の**脅威の例示にIPv6への移行等を含める「社会全体で対応が望まれる脅威」の分類を追加**した。
（2）前回の安全基準等の浸透状況等調査の結果	●2007年度の安全基準等の浸透状況等調査における調査結果について検証 ・安全基準等の整備状況 ・安全基準等に対する準拠状況	●大半の事業者等において内規を制定済みである一方で、その見直しを予定していない事業者等が3割近く存在することが推定され、**内規見直しの推進が望まれる。**
（3）相互依存性解析で得られた成果	●2007年度における、重要インフラ分野間のサービス提供に係る相互依存性解析で得られた成果について検証 ●2008年度における、重要インフラ分野間のデータ送受信に係る相互依存性解析で得られた成果について検証	●**電力、水道分野のサービスの停止・低下時に、**時間経過に伴い**重要システムの機能不全によるサービスの停止・低下等となる**場合がある。 ●**重要インフラ分野間のデータ送受信に係る不適切な現象とその影響に関して、通信・送受信システムの正常稼働時においては、影響範囲が局所的であることが多く、非正常稼働時においては、影響範囲が広範であることが多い。**

状況検証：④関連文書の検証

前回見直し以降の関連文書から、各重要インフラ分野に共通する情報セキュリティ対策等の新たな観点の検証を実施

	概要	検証結果
(1)情報セキュリティ対策に関連する文書等	● 以下の文書を検証 ・産業構造審議会情報セキュリティ基本問題委員会 中間とりまとめ～企業における戦略的な情報セキュリティガバナンスの確立に向けて～ ・情報セキュリティ管理基準(平成20年改正版) ・政府機関の情報セキュリティ対策のための統一基準(第4版) ● 国際規格(ISO/IEC27000ファミリー)の動向について検証	● **経営層の判断の下、情報セキュリティに対する取組状況の開示の促進等を通じた戦略的CSRの推進**が望まれる ● **国際規格やISMS適合性評価制度との整合**をとって、情報セキュリティ対策を推進することが望まれる ● **技術・環境の変化等、重要インフラにおいても参考となる事項についての盛り込み**が望まれる ● ISO/IEC27000ファミリーとして整備されつつある**ISMSに関する国際規格の作成状況を踏まえ、対策項目を具体化**をすることが望まれる
(2)事業継続計画に関連する文書等	● 以下の文書を検証 ・地方公共団体におけるICT部門の業務継続計画(BCP)策定に関するガイドライン ・ITサービス継続ガイドライン ● 事業継続マネジメントシステム(BCMS)に関する国際規格の動向について検証	● **情報システム部門における事業継続計画(BCP)の構築と運用**が望まれる ● **業務プロセスの情報システムへの依存性を考慮して、組織全体の事業継続計画(BCP)と連携して事業継続マネジメントシステム(BCMS)を運用**することが望まれる
(3)暗号に関連する文書等	● 以下の文書を検証 ・政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る移行指針 ・公的個人認証サービスにおける暗号方式等の移行に関する検討会報告書 ・電子政府推奨暗号リストの改訂に関する骨子(案)	● 情報システムにおいて**暗号アルゴリズムを使用する場合は、電子政府推奨暗号リストを参考に**することが望まれる ● **暗号の危殆化が予想されている暗号アルゴリズムを使用している場合は、その移行に向けたスケジュールの策定と、より安全性の高い暗号アルゴリズムを導入**することが望まれる
(4)その他の文書等	● 以下の文書を検証 ・発注者ビューガイドライン ・情報システム調達のための技術参照モデル(TRM)平成20年度版 ・CSIRTマテリアル ・情報システムの信頼性向上に関するガイドライン(第2版) ・情報セキュリティ人財アーキテクチャ(暫定版) ・「新型インフルエンザ対策行動計画」(改定案)及び「新型インフルエンザ対策ガイドライン」(案)	● **発注者(ユーザ企業)と開発者(ベンダ企業)の十分な意思疎通と適切な役割分担**により、情報システムの運用を円滑に行うことが望まれる ● **経営層の積極的な関与の下、組織全体の視点からの情報セキュリティインシデント対応**を行う動きがある ● **知的財産としての「人財」という認識に立った情報セキュリティ人材育成や要員管理**が望まれる ● **社会全体で対応する脅威に対して、最低限の国民生活を維持するための準備と対応**について検討が望まれる

状況検証：⑤社会的条件（環境）の変化の検証

以下の社会的条件（環境）の変化より、新たな脅威の発生・新たな対策の確立についての検証を実施

	概要	検証結果
（1）社会的な側面から見た変化	●以下の動向の変化を検証 ・事業者等の合併・統合及びそれに伴う情報システムの対応 ・業務の電子化に係る動向 ・新たなサービスの動向 ・情報システムに関する社会状況と今後の見込み	● **システムの統合や更新時に**不具合が混入してIT障害に至る場合が見られるため、**十分な検証等の対応**が望まれる。 ● **災害や障害等が発生した際の情報収集のためのツールとして、様々な主体が提供するサービスを利用**することが望まれる。 ● 技術的な対策は多くの事業者等で行われており、今後は**監査等によるセキュリティ対策の評価**が望まれる。 ● IPv6への移行をはじめ、**利用されている技術が次々と移り変わることに対応するため、常にリスク分析や対策の見直しの実施**が望まれる。
（2）情報システムに関する動き	● 以下のIT動向の変化について検証 ・DNSキャッシュポイズニングに係る脆弱性 ・非機能要求の検討 ・暗号の危殆化に係る問題	● **一般に広く使われる技術、プロトコル、ソフトウェア等の脆弱性が顕在化すると、影響は社会全体に及ぶ。** ● 情報システムの要件として**情報セキュリティに関する要件は不可欠であるが、可視化が難しく、企画・設計段階から意識して検討**することが望まれる。 ● **暗号アルゴリズムについては、**時間が経過するほど解読されるリスクが高まることから、**適切なタイミングにおける見直し**が望まれる。その時に、**移行についての配慮**することが望まれる。
（3）意図的要因に関する脅威	● 以下の意図的要因に関する脅威について検証 ・SQLインジェクションによる不正アクセスの急増 ・標的型攻撃手法の進化 ・ボットに関する動向 ・最近流行したウイルスの動向	● SQLインジェクションで狙われる**Webサイトの脆弱性は、サイト毎に異なることが多く、事業者等自身が対策を実施**することが望まれる。 ● ボットやウイルスについては、減少の傾向が見られず今後も継続して対策が必要。手法の高度化、多機能化にも注意を払うことが望まれる。 ● ウイルス対策ソフトでは全てに対応することが困難であることから、**職員への教育など他の対策を併用して、対策に努める**ことが望まれる。
（4）情報セキュリティに関する動き	● 以下の情報セキュリティに関する動向について検証 ・第2次情報セキュリティ基本計画 ・制御システムに対する情報セキュリティ ・セキュリティパッチの定例化	● **未然防止のための対策と、IT障害発生後の拡大防止・早期復旧に向けた対応のバランスを取る**ことが望まれる。 ● 今後は技術的な対策に加え、**制度面、人的側面の対策**も望まれる。 ● 今後は**制御系システムについて、セキュリティ確保のための対策**が望まれる。 ● **パッチの提供が定例化されているものについては、周到な準備と迅速な対応が必要。**同時に**非定例で提供されるパッチに対する、情報収集**が望まれる。

◆STEP2
改定の方向性について

以降のページで示す「指針（第３版）」への反映の方向性については、資料4「指針（第３版）パブリックコメント案」に反映しています。

反映結果：①第２次行動計画の反映

分析・検証結果より抽出した問題意識	指針（第3版）への反映の方向性
①第2次行動計画の反映　より	
● 第２次行動計画において重要インフラサービスという観点を追加し、それを踏まえた全体的な枠組みの見直しを実施 ・重要システム、サービスレベル、検証レベル、IT障害の定義　等	● 本編：例えば、「脚注2」を「重要インフラサービスにおいて発生する障害（サービスレベルを維持できない状態等）のうち、ITの機能不全が引き起こすもの」と修正する等、指針全体について見直しを行い、必要に応じて修正。 →(1)
● IT障害の脅威の類型に他分野からの波及を追加	● 本編：「Ⅱ３．「安全基準等」の対象とする脅威」に「（４）他分野の障害からの波及」を追加し、他分野の障害からの波及の脅威の例示を記載。 →(2)
● 指針の継続的改善を3年に1度実施する「指針の改定に関する検討」と毎年及び必要に応じて実施する「分析・検証」に分類	● 本編：「Ⅲ２．本指針の継続的改善」に、指針の改定に関する検討及び分析・検証について記載。 →(3)
● 参考事項、具体化の例示等の追加により、指針の充実	● 本編：「Ⅰ５．本指針の構成」に、指針に記載する事項を「要検討事項」と「参考事項」に分類すること、及び別冊として対策編を設けて対策項目の具体化の例示等を取りまとめることを記載。 →(4)
● 情報セキュリティに関する基準や参考文献等を改めて広く安全基準等として整理	● 本編：「Ⅰ６．本指針を踏まえた安全基準等の継続的改善及び浸透への期待」に、情報セキュリティに関する基準や参考文献類を安全基準等として整理することについて記載。 →(5)
● 安全基準等の浸透に向けて、対策を実装するための環境整備	● 本編：「Ⅰ６．本指針を踏まえた安全基準等の継続的改善及び浸透への期待」及び「Ⅲ４．（１）重要インフラ所管省庁及び重要インフラ事業者等」に、対策を実装するための環境整備について記載。 →(6)
● 「安全基準等の浸透状況等に関する調査」を定期的に実施	● 本編：「Ⅲフォローアップ」に「４．安全基準等の浸透」を追加し、内閣官房が「安全基準等の浸透状況等に関する調査」を毎年行うことを記載。 →(7)

反映結果：①第２次行動計画の反映

分析・検証結果より抽出した問題意識	指針（第3版）への反映の方向性
①第2次行動計画の反映　より	
● 事業継続計画の策定状況等を踏まえ、指針の充実	● 本編：「Ⅲ2.（2）指針の分析・検証」に、事業継続計画の観点から指針の内容を充実させることについて記載。 →(8)
● 情報セキュリティ監査の実施やセキュリティ報告書の作成等の自主的な取組み	● 本編：「Ⅲ3.（1）重要インフラ所管省庁及び重要インフラ事業者等」に情報セキュリティ監査又はそれに相当するものの実施を検討することについて記載。 →(9)
● 情報セキュリティ対策の対外的な説明	● 本編：「新たな重点項目 エ　IT障害発生時の利用者の対応のための情報の提供等の対策」にサービスの停止・低下が発生した際でも利用者が安心して対応が行える情報提供の実施について記載。 ● 「重点項目 ア(イ)　事業継続計画との整合性への配慮」にリスクコミュニケーション等の連携について記載。 →(10)
● リスクコミュニケーション、公表に差し支えない範囲での情報セキュリティ対策の開示	

反映結果：②定常的なIT障害等の発生状況の分析

分析・検証結果より抽出した問題意識	指針（第3版）への反映の方向性
②定常的なIT障害等の発生状況の分析 より	
● 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	● 本編：「4つの柱　ア　組織・体制及び資源の確保」にて、反映済。 →(11)
● 利用者や職員の通報も障害発生の認識に役立ち、通報の取り扱いをマニュアルに示した上での活用	● 本編：「4つの柱　ア　組織・体制及び資源の確保」にて反映済。 →(12)
● 報告手順、様式等の整備等により迅速に対応できる体制構築	● 本編：「4つの柱　ア　組織・体制及び資源の確保」にて、「運用等に係る組織及び体制の確立及びこれを支える資源の確保」に反映済。 →(13)
● 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	● 本編：「4つの柱　エ　情報システムについての対策」に、「保守時の対応の必要性」について記載。 →(14)
● 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	● 本編：「重点項目　ア　IT障害の観点から見た事業継続性確保のための対策」に反映済。 →(15)
● 情報漏えいの防止に向けた実効性ある対策、被害を最小化するための継続的な取り組み	● 本編：「重点項目　イ　情報漏えい防止のための対策」にて、「各分野において発生防止及び再発防止の対策に取り組む必要」に反映済。 →(16)

反映結果：③行動計画に基づく施策の成果（1/2）

分析・検証結果より抽出した問題意識	指針（第3版）への反映の方向性	
③行動計画に基づく施策の成果　より		
● 水道分野のサービス停止や機能の低下等による、他分野のシステムが機能不全に陥る恐れ	本編：「Ⅱ３．「安全基準等」の対象とする脅威」に「（４）他分野の障害からの波及」を追加し、脅威の例示に水道供給の途絶について記載。 「Ⅱ６．対策項目（１）４つの柱 エ　情報システムについての対策（ア）施設と環境」に反映済。	→(17)
● IT障害の脅威の定義等について、第２次行動計画において見直し	● 本編：「脚注２」を「重要インフラサービスにおいて発生する障害（サービスレベルを維持できない状態等）のうち、ITの機能不全が引き起こすもの」と修正する等、指針全体について行動計画を踏まえた用語の見直しを行い、必要に応じて修正　（「①第２次行動計画の反映」を参照）。	→(18)
● 重要インフラ分野及び重要インフラ事業者等の取組みから得られる知見・教訓等を踏まえた指針の充実	● 本編：「Ｉ６．本指針を踏まえた安全基準等の継続的改善及び浸透への記載」に反映済み。	→(19)
● 脅威の例示にIPv6への移行等を含める「社会全体で対応が望まれる脅威」の分類をを追加	● 本編：「新たな重点項目　オ　ITに係る環境変化に伴う脅威のための対策 」に、暗号の危殆化やIPv6への移行等の対策について記載。	→(20)
● 事業者等が制定する内規見直しの推進	● 本編：「Ⅲ４．安全基準等の浸透」に重要インフラ事業者等、重要インフラ所管省庁及び内閣官房の取り組みを記載。	→(21)

反映結果：③行動計画に基づく施策の成果（2/2）

分析・検証結果より抽出した問題意識	指針（第3版）への反映の方向性
③行動計画に基づく施策の成果　より	
● 電力、水道分野のサービスの停止・低下が他分野のサービス停止・低下等に与える影響についての対応	● 本編：「Ⅱ３.「安全基準等」の対象とする脅威」に「（４）他分野の障害からの波及」を追加し、脅威の例示に電力供給の途絶、水道供給の途絶等について記載。 →(22) ● 本編：「4つの柱 エ　情報システムについての対策（ア）施設と環境」にて、停電時への対応ついては反映済。 →(23) ● 本編：「4つの柱 エ　情報システムについての対策（ア）施設と環境」に、断水時への対応について記載。 →(24)
● 重要インフラ分野間のデータ送受信に係る不適切な現象とその影響に関して、通信・送受信システムの正常稼働時においては、影響範囲が局所的であることが多く、非正常稼働時においては、影響範囲が広範であることが多い	● 本編：「4つの柱 エ　情報システムについての対策　（ウ）アプリケーションソフトウェア及び（エ）通信回線及び通信回線装置」にて、重要インフラ分野間のデータ送受信に係る対策に反映済。

反映の方向性：④関連文書の検証（1/2）

分析・検証結果より抽出した問題意識	指針（第3版）への反映の方向性	
④関連文書の検証　より		
● 経営層の判断の下、取組状況の開示の促進等を通じた戦略的CSRの推進	● 本編：新たな重点項目「エ　IT障害発生時の利用者の対応のための情報の提供等の対策」に、サービスの停止・低下が発生した際でも利用者が安心して対応が行える情報提供の実施について記載。	→(25)
● 国際規格やISMS適合性評価制度との整合 ● ISMSに関する国際規格の作成状況を踏まえ、対策項目を具体化	● 本編：「Ｉ６．本指針を踏まえた安全基準等の継続的改善及び浸透への期待」にて、反映済。	→(26)
● 技術・環境の変化等、重要インフラにおいても参考となる事項についての盛り込み	● 本編：新たな重点項目「オ　ITに係る環境変化に伴う脅威のための対策」に、記載。	→(27)
● 情報システム部門における事業継続計画（BCP）の構築と運用 ● 業務プロセスの情報システムへの依存性を考慮して、組織全体の事業継続計画（BCP）と連携して事業継続マネジメントシステム（BCMS）を運用	● 本編：「重点項目　ア　IT障害の観点から見た事業継続性確保のための対策」にて、反映済。	→(28)
● 暗号アルゴリズムを使用する場合は、電子政府推奨暗号リストを参考	● 本編：「4つの柱　ウ　情報セキュリティ要件の明確化に基づく対策」にて、反映済。	→(29)

反映の方向性：④関連文書の検証（2/2）

分析・検証結果より抽出した問題意識	指針（第3版）への反映の方向性
④関連文書の検証　より	
● 暗号の危殆化が予想されている暗号アルゴリズムを使用している場合は、その移行に向けたスケジュールの策定と、より安全性の高い暗号アルゴリズムを導入	● 本編：新たな重点項目「オ　ITに係る環境変化に伴う脅威のための対策」に、暗号の危殆化について記載。 →(30)
● 発注者（ユーザ企業）と開発者（ベンダ企業）の十分な意思疎通と適切な役割分担	● 本編：「重点項目　ウ　外部委託における情報セキュリティ確保のための対策」に、契約者双方の責任の明確化と合意形成について記載済。 →(31)
● 経営層の積極的な関与の下、組織全体の視点からの情報セキュリティインシデント対応	● 本編：「重点項目　ア　IT障害の観点から見た事業継続性確保のための対策」にて、反映済。 →(32)
● 知的財産としての「人財」という認識に立った情報セキュリティ人材育成や要員管理	● 本編：「4つの柱 ア 組織・体制及び人的資源の確保」に、情報セキュリティ人材育成等について記載。 →(33)
● 社会全体で対応する脅威に対して、最低限の国民生活を維持するための準備と対応	● 本編：「重点項目　ア　IT障害の観点から見た事業継続性確保のための対策」に新型インフルエンザ等、社会全体で対応する脅威への考慮について記載。 →(34)

反映の方向性： ⑤社会動向（環境）の変化の検証（1/2）

分析・検証結果より抽出した問題意識	指針（第3版）への反映の方向性
⑤社会動向（環境）の変化の検証　より	
● システムの統合や更新時に、十分な検証等の対応	● 本編：「4つの柱 エ 情報システムについての対策」の（イ）から（ウ）で更新時の十分な検証について追加。 →(35)
● 災害や障害等が発生した際の情報収集のためのツールとして様々な主体が提供するサービスを利用	● 本編：「重点項目 ア IT障害の観点から見た事業継続性確保のための対策」に反映済。 →(36)
● 監査等によるセキュリティ対策の評価	● 本編：「Ⅲ．フォローアップ」に記載されているが、第2次行動計画でにに具体的に盛り込まれていることを踏まえ、「4つの柱 ア 組織・体制及び資源の確保」の参考事項として外部監査について記載。 →(37)
● 利用されている技術が次々と移り変わることに対応するため、常にリスク分析や対策の見直しの実施	● 本編：継続的改善については、「Ⅲ．フォローアップ3」の（1）で安全基準等の見直しに関する検討について反映済みであるが、新たな重点項目「オ　ITに係る環境変化に伴う脅威のための対策」に脅威に対する対応を記載。 →(38)
● 一般に広く使われる技術、プロトコル、ソフトウェア等の脆弱性が顕在化すると、影響は社会全体に及ぶ	● 本編：現行指針に記載はなく、新たな重点項目「オ　ITに係る環境変化に伴う脅威のための対策」に技術等の環境変化への検討について記載。 →(39)
● 情報セキュリティに関する要件は不可欠であるが、可視化が難しく、企画・設計段階から意識して検討	● 本編：「4つの柱 ウ 情報セキュリティ要件の明確化に基づく対策」に反映済。 →(41)

反映の方向性： ⑤社会動向（環境）の変化の検証（2/2）

分析・検証結果より抽出した問題意識	指針（第3版）への反映の方向性	
⑤社会動向（環境）の変化の検証　より		
● 暗号アルゴリズムについては、適切なタイミングで見直し ● 移行についての十分な配慮	● 本編：現行指針に記載はなく、新たな重点項目「オ　ITに係る環境変化に伴う脅威のための対策」に暗号の危殆化に対応する対策項目について記載。	→(42)
● Webサイトの脆弱性は、サイト毎に異なることが多く、事業者等自身が対策を実施	● 本編：「4つの柱 ウ 情報セキュリティ要件の明確化に基づく対策」（イ）に反映済。	→(43)
● 職員への教育など他の対策を併用して、対策に努める	● 本編：「4つの柱 ア 組織・体制及び資源の確保（ア）」に記載。	→(44)
● 未然防止のための対策と、IT障害発生後の拡大防止・早期復旧に向けた対応のバランスを取ること	● 本編：「Ⅰ2「安全基準等」の必要性」に反映済。	→(45)
● 制度面、人的側面の対策	● 本編：人的側面の対策については、「4つの柱 ア 組織・体制及び資源の確保」に反映済。	→(46)
● 制御系システムについて、セキュリティ確保のための対策	● 本編：「Ⅰ4本指針の位置づけ」に、反映済。	→(47)
● パッチの提供が定例化されているものについては、周到な準備と迅速な対応 ● 非定例で提供されるパッチに対する、情報収集	● 本編：「4つの柱 ウ 情報セキュリティ要件の明確化に基づく対策（イ）情報セキュリティについての脅威」に記載済。	→(48)