資料３－１

「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』策定にあたっての指針」の見直しについて（案）

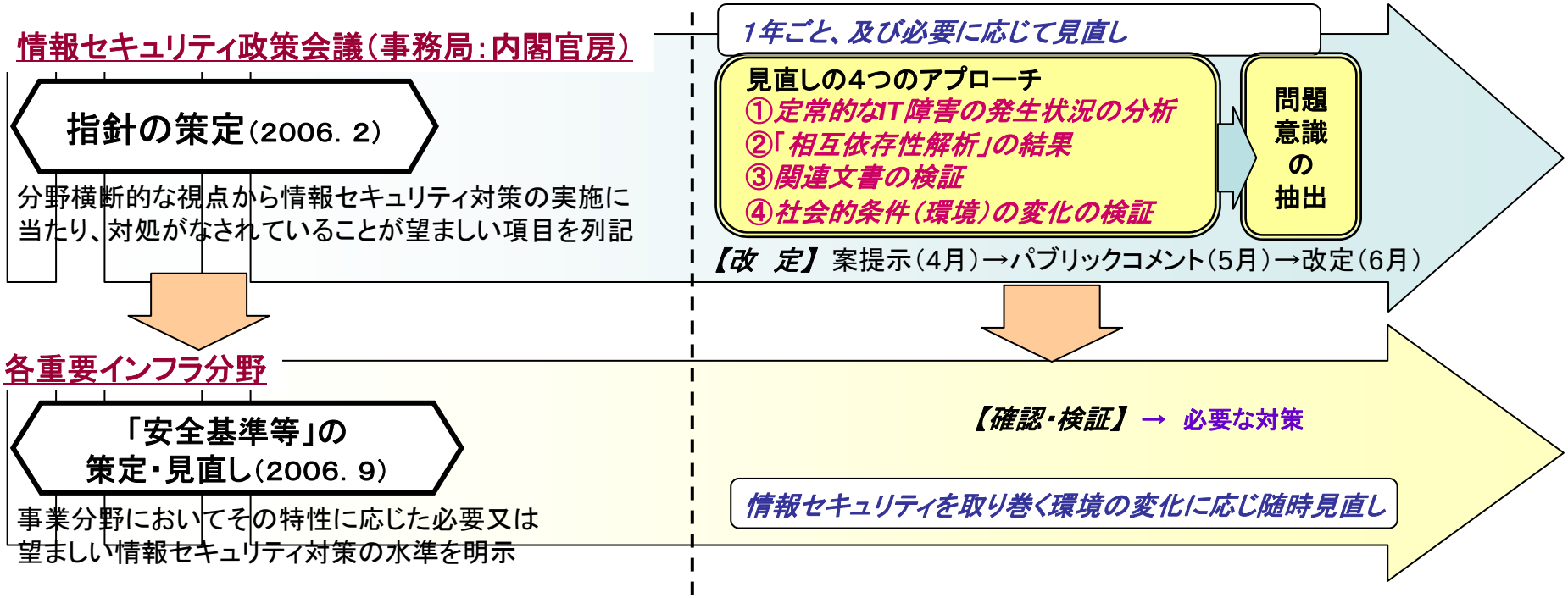
2007年3月

内閣官房情報セキュリティセンター（NISC）

指針の見直しの基本的スタンス

指針の目的・位置づけ等をふまえ、4つのアプローチより抽出された論点から問題意識を整理し、改定を検討

- 「安全基準等」策定にあたっての指針（以下「指針」）は、重要インフラ分野における安全基準等の策定・改定を支援することを目的として2006年2月に策定。
- 「指針」の策定に当たっては、各重要インフラ分野において、2006年9月を目処に「安全基準等」の策定・見直しがなされることを前提に、「安全基準等」において何らかの対処がなされていることが望ましい項目を列記。
- 今回フォローアップとして「指針」の見直しを行うにあたっては、まず以下の4つのアプローチにより分析・検証を行い、情報セキュリティ対策に関する「問題意識」を抽出。
- 抽出した「問題意識」について、現在の「指針」と照らし合わせ必要な改定を行い、各重要インフラ分野の「安全基準等」における対策の状況や今後の方針を確認・検証。



見直しの4つのアプローチ

指針見直しの観点として、以下4つのアプローチにて状況検証を実施

セキュア・ジャパン2006

（2006年6月15日情報セキュリティ政策会議決定）

【具体的施策】

ア）各重要インフラ分野の安全基準等の策定・見直し（重要インフラ所管省庁）

イ）「安全基準等」の策定状況の把握及び評価（内閣官房）

ウ）指針の見直し（内閣官房）

「指針」の見直しの方向性

- ◆「安全基準等」の把握等を通じて、重要インフラ分野に共通的な要検討事項が新たに導き出されるのではないか
- ◆「相互依存性解析」の知見をふまえ、「指針」の見直しにどのように活用するか
- ◆「指針」や「セキュア・ジャパン2006」の記載内容から導き出される方策以外に「指針」の見直しに資する事項はないか

（指針より）

・内閣官房は、1年ごと、及び必要に応じて適時に、本指針の見直しを推進する

・内閣官房は定常的なIT障害の発生状況の把握を通じ、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・検討を行い、本指針改定のための基礎資料として整備する

・（前略）内閣官房が各重要インフラ所管省庁及び重要インフラ事業者等の協力を得て相互依存性解析を実施する際には、その結果を本指針や各重要インフラ分野における「安全基準等」の見直しの基礎資料として提供する

（「セキュア・ジャパン2006」より）

政府機関統一基準、その他関連文書を参照しつつ、各重要インフラ所管省庁の協力を得て、2006年度中を目処に指針の見直しを実施する

⇒ ***「指針」の目的である「安全基準等の策定・改定を支援」に資するため、各分野に共通する横断的な対策課題の分析・検討を行うことが必要ではないか***

見直しの4つのアプローチ

①*定常的なIT障害の発生状況の分析*	・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・検討の結果、情報セキュリティ対策の新たな観点が発見されたか
②「*相互依存性解析*」の結果	・相互依存性解析の結果を基礎資料にして、新たな「何らかの対処がなされていることが望ましい項目」をどのように活用できるか → *本年度は見直しに至らず*
③*関連文書の検証*	・情報セキュリティ対策の新たな観点が追加されたか。それは、重要インフラ分野に共通的な要検討事項といえるか
④*社会的条件（環境）の変化の検証*	・技術の進歩があったか（新たな脅威の発生・新たな対策の確立） ・社会的重要性に変化があったか

状況検証： 定常的なIT障害の発生状況の分析

指針策定後の主要な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	分析結果
(1)システム障害によるサービス停止、低下	● システム運用時にソフトウェア、ハードウェア等の誤処理、停止が原因で障害が発生 ● サービスの要求が急激に増加することにより、サービス要求の処理能力を超過し、処理の停止、遅延(輻輳)が発生	● 情報システムの冗長化、負荷分散等のサービス停止の防止策及び処理性能確保のための対策を検討する必要があるのではないか ● 運用開始前に、システム品質確保策として負荷試験、試運転の実施や、特に新規技術を導入する場合の技術の成熟度や運用実績の確認等性能面の検証を十分に行う必要があるのではないか
(2)首都圏広域停電によるIT障害	● クレーン船により送電線が2回線とも損傷。首都圏広域にわたる停電が発生	● 停電により他の分野の事業者にも影響が波及したが、重要インフラで維持すべき重要システムにおいては、停電時への対応として電源供給の多重化、予備設備等による対応がなされた
(3)台湾沖地震による通信の途絶	● 台湾沖で地震が発生。地震の影響により海底ケーブルが破損し、通信障害が発生	● IT障害の発生源となる脅威は海外にも存在する場合もあり、必ずしも国内に限らない
(4)ファイル交換ソフトウェアによる情報漏えい	● 自宅に持ち帰った業務データが格納されたPCがコンピュータウイルスに感染、ファイル交換ソフトウェア経由でインターネットに流出	● 情報取扱いの誤りが原因で発生している情報漏えいとして、脅威の顕在化後も続発 ● 対策を実施しても再発していることから、情報の取扱いの見直し、情報漏えい予防の対策及び対策に対する周知・教育等の情報漏えい防止のための取り組みが必要ではないか ● 外部委託先でとるべき情報漏えい防止策としても同様の対策が必要なのではないか

問題意識の抽出： 定常的なIT障害の発生状況の分析

指針策定後の主要なIT障害の発生状況の分析結果より、5箇所（下線部分）について指針の改定が必要と考えられる

	分析結果より抽出した問題意識（案）	指針改定に向けた検討（案）
（1）システム障害によるサービス停止、低下	● 冗長化、負荷分散	● 「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」にて可用性確保のために導入すべきセキュリティ要件として負荷分散、冗長化を反映する必要があると考えられる
	● 処理性能確保、システム品質確保	● 「4つの柱　エ　情報システムについての対策」にて対策の例示として処理性能確保やシステム品質確保を反映する必要があると考えられる
（2）首都圏広域停電によるIT障害	● 停電時への対応	● 「4つの柱　エ　情報システムについての対策」にて、施設と環境の対策として、既に考慮されている
（3）台湾沖地震による通信の途絶	● IT障害の発生源となる脅威は国内に限らない	● 「4つの柱　エ　情報システムについての対策」にて、IT障害の発生源となる脅威は国内に限らない点を反映する必要があると考えられる
（4）ファイル交換ソフトウェアによる情報漏えい	● 対策を実施しても再発	● 「3つの重点項目　イ　情報漏えい防止のための対策」にて、発生防止及び再発防止を明示する必要があると考えられる
	● 外部委託先でとるべき情報漏えい防止策	● 「3つの重点項目　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」にて、外部委託先でとるべき情報漏えい防止策を明示する必要があると考えられる

状況検証：　関連文書の検証

指針策定後の関連文書から、各重要インフラ分野に共通する情報セキュリティ対策の新たな観点の検証を実施

	概要	検証結果
（1）国内外の規格文書	● 以下の規格文書を検証 • JIS Q 27001:2006　2006年5月 • JIS Q 27002:2006　2006年5月 • JIS Q 15001:2006　2006年5月 • ISO/IEC 20000-1:2005 (2007年JIS化予定) • ISO/IEC 20000-2:2005 (2007年JIS化予定)	● JIS Q 27001及びJIS Q 27002：ISO/IEC 17799の改訂にて対応された「リスクアセスメント及びリスク対応」及び「**情報セキュリティインシデント管理**」のカテゴリの新設等を反映。 ● JIS Q 15001：**個人情報保護法との整合性**が図られるとともに、マネジメントシステムを運用するための要件の追加 ● ISO/IEC 20000-1及びISO/IEC20000-2：**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。
（2）省庁ガイドライン	● 各省庁にて策定されたガイドライン類について、情報セキュリティ対策の新たな観点が追加されたかを検証	● 個人情報の保護に関するガイドライン：指針制定以降は、Q&Aの内容反映等や法令改正に伴う所要の改正等のみ ● 情報システムの信頼性向上に関するガイドライン：**情報システムの企画・開発から保守・運用**にわたり関係者が遵守すべき又は遵守することが望ましい事項を規定
（3）各重要インフラ分野の安全基準等	● 「安全基準等」の策定状況の把握から得られた状況を検証 ● 「安全基準等」の評価の一環として、各分野の安全基準等における対策項目の具体的な記載内容を検証	● 指針の表現上の問題として、**強制基準以外の場合は「遵守が必要である旨を規定する」のは適切でない**点判明 ● 情報セキュリティ対策の新たな観点：**自己点検・監査の実施**
（4）政府機関統一基準（及び個別マニュアル群）	● 政府機関統一基準（2005年12月情報セキュリティ政策会議決定）の改定状況を検証 ● 政府機関統一基準適用個別マニュアル群（22文書：2006年2月以降順次作成）について検証	● 政府機関統一基準の見直し課題を参考にすると、重要インフラにおいても、**「踏み台」対策に対する検討、想定するリスクについて見直しを実施**する必要があるのではないか ● 政府機関統一基準適用個別マニュアル群は、政府機関統一基準を更に具体化したレベルとして事業者が安全基準等から内規を作成する際の関連文書として参照することが望ましい

問題意識の抽出：　関連文書の検証

指針策定後の関連文書の検証結果より、2箇所（下線部分）について指針の改定が必要と考えられる

	検証結果より抽出した問題意識（案）	指針改定に向けた検討（案）
（1）国内外の規格文書	● 情報セキュリティインシデント管理	● 「3つの重点項目　ア　IT障害の観点から見た事業継続性確保のための対策」にて既に考慮されている
	● 個人情報保護法との整合性	● 「3つの重点項目　イ　情報漏えい防止のための対策」にて既に考慮されている
	● ITサービスマネジメントについてPDCAサイクルを運用	● 「4つの柱　エ　情報システムについての対策」にて既に考慮されている
（2）省庁ガイドライン	● 情報システムの企画・開発から保守・運用	● 「4つの柱　エ　情報システムについての対策」にて既に考慮されている
（3）各重要インフラ分野の安全基準等	● 強制基準以外の場合は「遵守が必要である旨を規定する」のは適切でない	● 「『安全基準等』策定の目的」にて強制基準以外の場合は「遵守が必要である旨を規定する」のは適切でない点を反映する必要があると考えられる
	● 自己点検・監査の実施	● 「4つの柱　ア　組織・体制及び資源の確保」にて自己点検・監査の実施を反映する必要があると考えられる
（4）政府機関統一基準（及び個別マニュアル群）	● 「踏み台」対策に対する検討	● 「『安全基準等』の対象範囲及び対象とする脅威」にて既に考慮されている ● 「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」にて既に考慮されている
	● 想定するリスクについて見直しを実施	● 「『安全基準等』の継続的検証 ①『安全基準等』の見直し」にて既に考慮されている

状況検証：　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）リスクマネジメント関連の動き	● リスクマネジメントの観点から、情報セキュリティに関する新たな脅威の発生や新たな対策の確立などの動きを検証（以下文書例） • 事業継続管理（BCM）に関する利用ガイド（JIPDEC） • サーベインズ・オクスリー法（企業改革法）遵守のためのIT統制目標 第2版（ITGI） • 事業継続ガイドライン 第一版 解説書（案）（内閣府　防災担当） • システム管理基準 追補版（財務報告に係るITガイダンス）（案）（経済産業省）	● 企業改革法（米国）の施行や金融商品取引法の制定を受け、財務報告に係る内部統制の構築で求められている「ITへの対応」を解説したガイドライン類の策定が進んでいる ● 事業継続計画（BCP）について、国内外でガイドライン等の策定がなされる中、2008年の規格化を目標とした国際標準化の動きがある ● いずれの側面においても、マネジメントシステムの基本的な枠組みであるPDCAサイクルの適用を前提として、具体的な個別の対策を実施することとなっている
（2）重要インフラ全般の動き	● 重要インフラにおける情報セキュリティ対策の観点から、社会的条件（環境）の変化として考えられる最近の状況を検証	● IT化の進展により、情報システムへの依存度がより高くなっている一方で、そもそもIT依存が見えにくくなってきている点、及びIT依存が明らかであっても技術やノウハウの理解が十分でなく適切な対応が困難になってきている点から、IT依存のブラックボックス化が進みつつある ● 制御系システムをはじめとして、かつて機械的でより単純な原理にて動作するものに対しても、より一層の信頼性確保やコスト低減等を目的に、ITの適用範囲の拡大・高度化がなされつつある
（3）重要インフラ行動計画に基づく取組み	● IT障害の未然防止、発生時の被害拡大防止・迅速な復旧及び再発防止のため、各重要インフラ分野における「情報共有・分析機能」（CEPTOAR）の整備を実施中	● 2006年度末にCEPTOAR整備（新規追加分野は基本的合意の完了）を目指す中、各重要インフラ分野においてCEPTOAR整備についての合意が得られつつある

問題意識の抽出：　社会的条件（環境）の変化の検証

社会的条件（環境）の変化の検証結果より、3箇所（下線部分）について指針の改定が必要と考えられる

	検証結果より抽出した問題意識（案）	指針改定に向けた検討（案）
（1）リスクマネジメント関連の動き	● 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」）	● 「4つの柱　ア　組織・体制及び資源の確保」にて既に考慮されている
	● PDCAサイクルの適用（事業継続計画）	● 「3つの重点項目　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PDCAサイクルの適用を反映する必要があると考えられる（事業継続計画）
（2）重要インフラ全般の動き	● IT依存のブラックボックス化 ● ITの適用範囲の拡大・高度化	● 「4つの柱　エ　情報システムについての対策」にてIT依存のブラックボックス化やITの適用範囲の拡大・高度化が進みつつある点を反映する必要があると考えられる
（3）重要インフラ行動計画に基づく取組み	● CEPTOAR整備についての合意	● 「フォローアップ」にてCEPTOAR整備についての合意を反映する必要があると考えられる