資料３　（別紙1）

NISC National Information Security Center

2007年度　重要インフラにおける「指針の見直し」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）

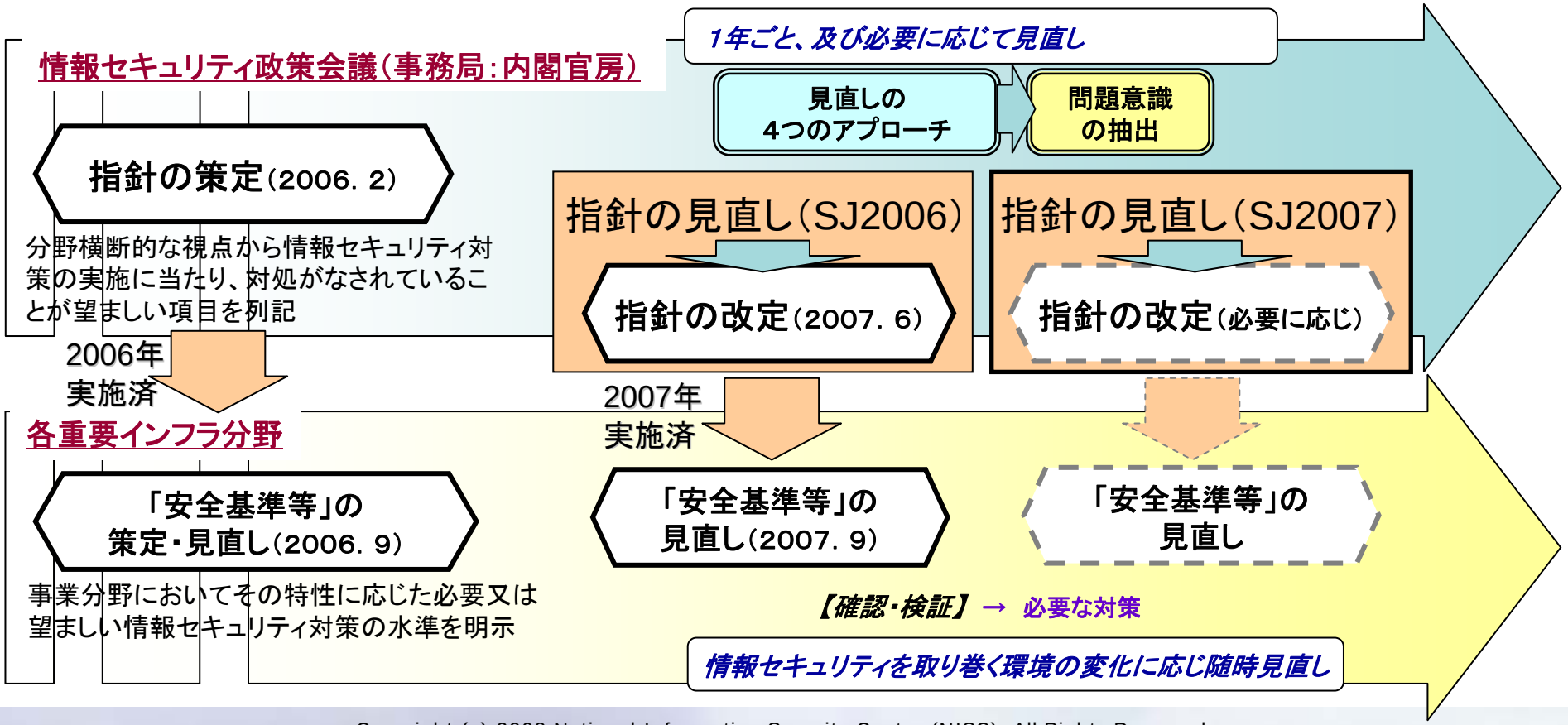
「指針の見直し」の概要

○「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」（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

○その後、定常的なIT障害の発生状況の把握等を通じて、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、指針を改定（2007年6月14日 情報セキュリティ政策会議決定）

○「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」ことから、本年度も「指針の見直し」を実施

○昨年同様の4つのアプローチより、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」を抽出し、現在の指針と照らし合わせ、必要に応じて改定を実施



「指針の見直し」の観点

「指針の見直し」の方向性

◆昨年の4つのアプローチを継承し、2007年度の見直しを実施

◆昨年度実施に至らなかった「相互依存性解析」の成果を踏まえた見直しを実施

（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2007」より）

2007年度中に相互依存性解析の成果も踏まえ、各重要インフラ所管省庁の協力を得て、指針の見直しを実施する

◆2007年度「指針の見直し」におけるアプローチ

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*」の成果	・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 ・各分野の特性や分野の関係性によって生じる、ある分野のサービスから別の分野のサービスへの波及の状況について得られた知見をどのように活用できるか
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 ・IT障害の発生を未然に防止できた例から、得られる知見や教訓はあるか

※青字部分は、2007年度に新たに追加するアプローチ

状況検証：①定常的なIT障害の発生状況の分析

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	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 ・ 新技術により構成されたシステムの障害が再発 ・ 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	● 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、**より信頼性の高い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。
(2)サイバー攻撃等	● 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 ・ 不正侵入によるWebサイト改ざんが発生 ・ 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 ・ 不審メールによる攻撃が発生	● 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。
(3)情報漏えい	● 情報漏えいの発生状況を分析 ・ 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	● 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。 ● **情報漏えいの防止に加え、発生時の被害を最小化するための継続した取り組み**が望まれる。

状況検証： ②相互依存性解析の成果

静的相互依存性解析の成果より、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」の分析・検討を実施

	概要	検証結果
（1）視点の整理	● 静的相互依存性解析の総括に必要な視点を整理した結果を検証 ・ IT障害 ・ 検討の範囲 ・ 波及 ・ 波及と関係性	● **分野における特性**として挙げられた、①他分野との関係性の有無、②IT障害の起き難さ（分野特有の対策等）**を考慮し、リスク分析の内容が適当かどうか見直す**ことが望まれる。
（2）静的相互依存性解析の検討結果	● 静的相互依存性解析の検討結果を検証	● 一般的には各分野のサービスに影響しないよう適切な対策がとられているが、各分野の主要な事業者へのヒアリングに基づき、以下の相互依存性関係が明確となった。 ・ **情報通信分野（電気通信）と他分野との相互依存性** ・ **電力分野と他分野との相互依存性** ・ **水道分野と他分野との相互依存性** ● 上記以外の分野間についても、**相互依存の可能性はあるものの、その関係性と波及が必ずしも明確にならかったケース**もあり、今後も相互依存性解析の成果**を継続的に確認**することが望まれる。

状況検証：③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の新たな観点の検証を実施

	概要	検証結果
（1）規格文書・ガイドライン等	● 国内外の規格文書・ガイドライン等から、情報セキュリティ対策の観点を検証 ・ ITSMS（ITサービスマネジメントシステム）適合性評価制度 ・ 個人情報保護法関係 ・ 分野ガイドライン ・ システム品質向上 ・ 金融商品取引法（内部統制）関連 ・ BCM（事業継続管理）関連	● ITSMS適合性評価制度として、昨年検証した国際標準が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。 ● 個人情報保護法関係では、昨年同様に法律の運用を踏まえたガイドラインの改正やQ&Aの提供が行われている。 ● 分野ガイドラインにて、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。 ● 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。 ● 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・ガイドライン及び企業向け・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。 ● BCM（事業継続管理）関連では、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。
（2）政府機関統一基準	● 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	● 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。

状況検証：④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）情報技術、情報セキュリティ動向	● 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 ・ IPアドレス枯渇問題 ・ JRE（Java Runtime Environment）問題	● 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への移行を行う場合には適切な対応**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。
（2）IT活用範囲の拡大	● 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	● 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。
（3）重要インフラ行動計画に関する動向	● 重要インフラ行動計画に関する動向を検証 ・ 情報共有体制の強化 ・ 分野横断的な演習の実施	● 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）の創設の基本的合意に関する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を実施した。
（4）大規模なIT障害に至らなかった例	● 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 ・ 自然災害	● 2007年10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。

※下線部は、第13回重要インフラ専門委員会（2008.1.31）以降の状況変化を踏まえて修正

問題意識の抽出と現行指針等での対応状況(1/3)

- 抽出した問題意識と現行指針や行動計画見直しの検討状況との照らし合わせを実施
- その結果、見直しの要点を整理(下記赤字内容)

分析・検証結果より抽出した問題意識	現行指針等との照らし合わせ結果
①定常的なIT障害の発生状況の分析　より	
● より信頼性の高いシステム設計及び検証	● 「4つの柱　エ　情報システムについての対策」にて、「システム品質確保等の対策を考慮することが重要」としている。
● 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	● 「4つの柱　エ　情報システムについての対策」にて、「IT依存の範囲拡大が進みつつある」という認識に立っている。
	● 「IT障害への脅威の例示」について、行動計画見直しにて基本的枠組みに関する事項として検討予定
● 顕在化しつつある新たな手法によるサイバー攻撃	● 「『安全基準等』の対象範囲及び対象とする脅威」にて、「サイバー攻撃によるIT障害」が対象とする脅威とされている。
● 情報漏えいの防止に加え、発生時の被害を最小化するための継続した取り組み	● 「3つの重点項目　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」について記載されている。

問題意識の抽出と現行指針等での対応状況(2/3)

分析・検証結果より抽出した問題意識	現行指針等との照らし合わせ結果
②相互依存性解析の成果　より ● 分野における特性を考慮し、リスク分析の内容が適当かどうか見直し	● 「本指針を踏まえた安全基準等策定若しくは見直しへの期待」にて「個々の安全基準等においては、より高度な情報セキュリティ水準の実現を目指し、（中略）随時検討がなされることを期待する」としている。
● 情報通信分野（通信）と他分野との相互依存性	● 「『安全基準等』の対象範囲及び対象とする脅威」にて、「通信の途絶」が対象とする脅威とされている。
● 電力分野と他分野との相互依存性	● 「4つの柱　エ　情報システムについての対策」にて、「通信回線及び通信回線装置」についての対策が明示されるべきとしている。
● 水道分野と他分野との相互依存性	● 「『安全基準等』の対象範囲及び対象とする脅威」にて、「電力供給の途絶」が対象とする脅威とされている。
● 相互依存の可能性はあるものの関係性と波及が必ずしも明確にならかったケースを継続的に確認	● 「4つの柱　エ　情報システムについての対策」にて、「停電時への対応」についての対策が明示されるべきとしている。
	● 「『安全基準等』の対象範囲及び対象とする脅威」「4つの柱　エ　情報システムについての対策」の両方にて考慮されていない
	● 「フォローアップ」にて、「相互依存性解析を実施する際には、（中略）見直しの基礎資料として提供する」としている。

問題意識の抽出と現行指針等での対応状況(3/3)

分析・検証結果より抽出した問題意識	現行指針等との照らし合わせ結果
③関連文書の検証　より	
● 要件定義、契約の変更管理の各プロセスを追加	● 「**4つの柱　エ　情報システムについての対策**」にて、「システム品質確保等の対策を考慮することが重要」としている。
● 技術・環境の変化の反映	● 「**フォローアップ**」にて、「『安全基準等』は、情報セキュリティを取り巻く環境の変化に応じ、随時見直しが行われるべきもの」としている。
④社会的条件（環境）の変化の検証　より	
● IPv6への移行を行う場合には適切な対応	● 「**4つの柱　エ　情報システムについての対策**」にて、「導入時、運用時、運用終了時」における対策が明示されるべき」としている。
● 市販ソフトウェアやフリーウェア等の運用について適切な対応	● 「**記載内容の具体性のレベル**」について、行動計画見直しにて検討予定
● 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	● 「**4つの柱　エ　情報システムについての対策**」にて、「アプリケーションソフトウェア」についての対策が明示されるべきとしている。
● 過去事例の知見や教訓を受けた対策	● 「**重要インフラ事業者等**」「**重要システム**」について、行動計画見直しにて基本的枠組みに関する事項として検討予定
	● 現行指針では考慮されていないが、「**経験やベストプラクティスの共有**」について、行動計画見直しにて情報共有体制の強化として検討予定

今後の進め方

今回は指針改定を行わず、見直しの要点を参考資料として周知

・ 今回は指針改定を行わないことについて

- 「安全基準等の浸透状況等に関する調査」の結果から、2006年9月の安全基準等の策定・見直しから1年経過した時点で、内規見直しを終えることができた事業者等は半数程度に留まることが推定
- 今回は指針改定によって、安全基準等の見直しへの新たな視点を喚起するのではなく、内規見直しを終えていない事業者等への安全基準等の着実な浸透を期することを優先
- NISCは指針の周知と安全基準等の浸透状況等の実態把握と努めるとともに、事業者等がより迅速に安全基準等を浸透する努力に期待

・ 参考資料として見直しの要点を周知することについて

- 独自の取り組みとして、安全基準等の見直しが行われている分野も存在
（「安全基準等の見直し状況の把握及び検証」（第13回重要インフラ専門委員会）より）
- 今回の検証・分析結果を参考資料として周知することで、独自の見直しを行う場合には、活用することができると期待

今回明らかになった見直しの要点は、次期行動計画との整合を図る必要があるため、行動計画見直しの状況等を踏まえ、来年度以降の指針見直しにて検討