重要インフラにおける安全基準等の策定状況の把握及び評価について

2007年4月23日

内閣官房情報セキュリティセンター（NISC）

資料３－１

安全基準等の評価実施に係る基本的スタンス

○ 重要インフラ(※1)をIT障害(※2)から防護するための全体計画として「重要インフラの情報セキュリティ対策に係る行動計画」を策定（2005年12月13日情報セキュリティ政策会議決定）。

○ また、それぞれの事業分野においてその特性に応じた必要または望ましい情報セキュリティ対策の水準を「安全基準等」という形で明示するため、「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」を策定（2006年2月2日情報セキュリティ政策会議決定）

○ 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）にて策定した本年度の具体的施策に基づき、各重要インフラ分野における「安全基準等」の策定・見直しを受け、内閣官房にて「安全基準等」の策定状況の評価を実施

（※1）重要インフラ１０分野；情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流
（※2）重要インフラの各事業において発生する障害(サービスの停止や機能の低下等)のうちITの機能不全が引き起こすものを「IT障害」という。

重要インフラの情報セキュリティ対策に係る行動計画

（2005年12月13日情報セキュリティ政策会議決定）

【4つの柱】

1．「安全基準等」の整備

2．情報共有体制の構築

3．相互依存性解析の実施

4．分野横断的演習の実施

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

（2006年2月2日情報セキュリティ政策会議決定）

- 分野横断的視点から、情報セキュリティ対策の実施にあたり、対処がなされていることが望ましい項目を列記

＜4つの柱＞

1．組織・体制及び資源の確保
2．情報についての対策
3．情報セキュリティ要件の明確化に基づく対策
4．情報システムについての対策

＜3つの重点項目＞

1．IT障害の観点から見た事業継続性確保のための対策
2．情報漏えい防止のための対策
3．外部委託における情報セキュリティ確保のための対策

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）

評価の4つのアプローチ

以下の評価の4つのアプローチのうち、現時点で対応可能な3つの観点で評価を行う（2007年3月現在）

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）

「安全基準等」の評価の方向性

- **「セキュア・ジャパン2006」に沿って、「安全基準等」が策定・見直しされたことを評価すべきではないか**
- **「指針」に記載されている対策項目が、策定・見直しがなされた「安全基準等」において適切に反映されているかを検証するべきではないか**
- **今年度試行的段階で行われている「相互依存性解析」の知見をどのように活用するべきか**
- **今般策定・見直しが行われた「安全基準等」について、各分野における活用状況等についても把握する必要があるのではないか**

（「指針」　Ⅰ目的及び位置づけ　より）

（略）　それぞれの事業分野においてその特性に応じた必要又は望ましい情報セキュリティ対策の水準を「安全基準等」という形で明示し、

（略）　本指針は、あくまで最低限の情報セキュリティ対策が講じられるよう安全基準等の策定若しくは見直しを支援するために策定されたものであることから、

（「セキュア・ジャパン2006」　第2節　重要インフラ　より）

「安全基準等」の策定状況の把握及び評価（内閣官房）

２００６年度中に「安全基準等」の策定状況を、各重要インフラ所管省庁の協力を得て把握を行い、相互依存解析の実施状況も踏まえつつ「安全基準等」の評価を実施する。

（「指針」　Ⅲフォローアップより）

（略）　重要インフラ事業者等は「安全基準等」に対する準拠状況の評価を実施していくために、情報セキュリティ対策の実施状況を自ら定期的に点検し、必要に応じ対策の改善を行う

⇒ ***重要インフラの社会的な重要性や関心の高さから、本年度末での評価対象に加え、3ヵ年計画として来年度実施すべき評価対象についても検討が必要ではないか***

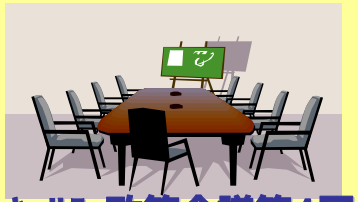
今回対応範囲

評価の4つのアプローチ

①「*安全基準等*」の策定・見直し状況	・それぞれの事業分野において「安全基準等」の策定・見直しが完了しているか
②「*指針*」との対応状況の検証	・「指針」にて示される対策が、その事業の態様等の理由から規定する必要がないと判断されない限り、「安全基準等」にて記載されているか
③「*相互依存性解析*」の結果	・各分野の「安全基準等」の見直しにおいて、分野を越えた横断的情報セキュリティ対策として今後反映することが望ましい事項はないか　*→本年度は実施に至らず*
④「*安全基準等*」の普及・活用状況 *→来年度実施に向けて検討*	・個々の事業者が自主的な取り組みのもと、「安全基準等」を満たすべく努力しているか

評価結果：①「安全基準等」の策定・見直し状況

行動計画策定時点において、安全基準等が存在しなかった分野も含め、全ての分野において安全基準等の策定・見直しが完了



情報セキュリティ政策会議第４回会合（2006年2月2日）

「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」を決定

重要インフラ

必要な又は望ましい情報セキュリティ対策の水準について「安全基準等」に明示

分野	安全基準等の名称【発行主体】	策定・見直し状況
情報通信	電気通信事業法、電気通信事業法施行規則、事業用電気通信設備規則等（関連する告示を含む） 情報通信ネットワーク安全・信頼性基準【総務省】 電気通信分野における情報セキュリティ確保に係る安全基準（第1版）【ISeCT】（※1）	実施済
	放送における情報インフラの情報セキュリティ確保に関わる「安全基準等」策定ガイドライン【日本放送協会（NHK）、（社）日本民間放送連盟】	実施済
金融	金融機関等におけるセキュリティポリシー策定のための手引書【FISC】（※2） 金融機関等コンピュータシステムの安全対策基準・解説書【FISC】 金融機関等におけるコンティンジェンシープラン策定のための手引書【FISC】	実施済
航空	航空運送事業者における情報セキュリティ確保に係る安全ガイドライン【国土交通省】 航空管制システムにおける情報セキュリティ確保に係る安全ガイドライン【国土交通省】	実施済
鉄道	鉄道分野における情報セキュリティ確保に係る安全ガイドライン【鉄道事業者等】	実施済
電力	電力制御システム等における技術的水準・運用基準に関するガイドライン【電気事業連合会】	実施済
ガス	製造・供給に係る制御系システムの情報セキュリティ対策ガイドライン【（社）日本ガス協会】	実施済
政府・行政サービス	地方公共団体における情報セキュリティポリシーに関するガイドライン【総務省】	実施済
医療	医療情報システムの安全管理に関するガイドライン【厚生労働省】	実施済
水道	水道分野における情報セキュリティガイドライン【厚生労働省】	実施済
物流	物流分野における情報セキュリティ確保に係る安全ガイドライン【国土交通省】	実施済

（※1）ISeCT:電気通信分野における情報セキュリティ対策協議会　（※2）FISC:（財）金融情報システムセンター

評価結果：②「指針」との対応状況の検証

「指針」との対応状況の検証を行った結果、以下の通り、「指針」の「4つの柱」と「3つの重点項目」が各安全基準等へ盛り込まれている（規定する必要がない場合を除く）ことを確認

分野		指針との対応状況	特徴	公開状況
情報通信	電気通信	有	事業者団体において「指針」の各項目の観点から検討しており、ISO/IEC17799を参照しながら、具体的な対策項目を明示している。また、具体的な対策チェックシートが添付されている。	公開（Web）
情報通信	放送	有	業界団体において「指針」の各項目の観点から検討しており、「表現の自由」「報道の自由」との関係から「放送内容に関わる情報」「報道に関わる情報」は対象外とし、必要と判断される項目について具体的な対策事項を明示している。	公開（個別配布）
金融		有	既存のガイドライン等を金融機関等により構成されるFISC内の専門委員会において「指針」の各項目の観点から見直しており、各項目ごとに目的、考え方、実施方法等について具体的な事例を踏まえながら解説している。	公開（有償販売）
航空		有	（航空事業者） 国土交通省及び関連機関、関連事業者の総意として「指針」の各項目の観点から取りまとめており、各項目について簡潔に記載している。 （航空管制） 国土交通省において「指針」の各項目の観点から検討しており、各項目ごとに具体的な「対策事項」を明示している。	公開（個別配布）
鉄道		有	鉄道事業者及び国土交通省をメンバーとするWGにおいて「指針」の各項目の観点から検討・合意しており、各項目ごとに「主旨目的」、「対策項目」を記載した上で、「推奨事項」として具体的な対策を明示している。	公開（個別配布）
電力		有	e-japan重点計画時に策定された既存のガイドラインを業界団体において「指針」の各項目の観点から見直しており、各項目について簡潔に記載している。	非公開（※1）
ガス		有	既存のガイドラインを業界団体において「指針」の各項目の観点から見直しており、各項目ごとに具体的な対策事項を明示している。また、CEPTOARを通じた情報提供についても言及している。	非公開（※2）
政府・行政サービス		有	既存のガイドラインを総務省において「指針」の各項目の観点から見直しており、各項目ごとに具体的な「例文」と「解説」を記載している。	公開（Web）
医療		有	厚生労働省において「指針」の各項目の観点から見直しており、各項目について技術的対策、運用的対策の観点から推奨項目も含め、具体的な対策項目と例文について記載している。	公開（Web）
水道		有	厚生労働省において「指針」の各項目の観点から検討しており、各項目ごとに具体的な対策事項を明示している。	公開（個別配布）
物流		有	国土交通省及び関連機関、関連事業者をメンバーとするWGにおいて「指針」の各項目の観点から取りまとめており、各項目ごとに「主旨・目的」「対策項目」を記載した上で、「推奨事項」として具体的な対策を明示している。情報漏洩対策については、個人情報を中心としたものとなっている。	公開（個別配布）

（※1）電気事業者外秘であり、公開によりセキュリティリスクが高まるため
（※2）ガス事業者外秘であり、公開することにより脅威の増大が想定されるため

（参考）各安全基準等に記載されている特徴的な対策項目（抜粋）

各安全基準等において、指針には具体的に例示されていないが、他分野においても参考となると考えられる事項が記載されていることが判明

（1）4つの柱

ア　組織・体制及び資源の確保

（1）自己点検の実施

（2）監査の実施

イ　情報についての対策

（3）情報の持ち出し管理
（媒体の取扱いも含む）

（4）情報の業務外目的での利用禁止

ウ　情報セキュリティ要件の明確化に基づく対策

（5）電子署名機能・暗号化機能

（6）フィルタリング機能
（ファイアウォール、ルータ等）

（7）脆弱性情報などの情報収集

（8）パッチの適用

エ　情報システムについての対策

（9）事業者の領域外に設置する場合の対策

（10）施設・コンピュータセンターの冗長化
（多重化・分散化等）

（11）外部媒体、情報機器の持込制限

（12）セキュリティ設計の実施

（13）情報システムの冗長化
（多重化・バックアップシステムの整備等）

（14）使用可能ソフトウェアの制限・
使用禁止ソフトウェアの規定

（15）システム試験の実施
（情報システム導入時、変更時等）

（16）通信回線の冗長化
（多重化・代替手段の整備）

（2）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

（17）障害発生箇所の切り分け機能

（18）演習・訓練の実施

（19）関係者等への注意喚起

イ　情報漏えい防止のための対策

（20）支給以外のシステムによる情報処理の制限・
私物機器の利用制限

（21）情報漏えい発生時の広報・報告

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

（22）外部委託に係る情報漏えい対策
（守秘義務・情報の取扱い・ペナルティの合意等）

（23）委託先選定時の国際規格認証の参照

（24）再請負に関する制約

（25）委託先に対する監査の実施