資料３

重要インフラにおける安全基準等の策定・見直しについて（案）

2006年11月

内閣官房情報セキュリティセンター（NISC）

重要インフラにおける安全基準等の意義・位置づけ

○ 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、セキュア・ジャパン2006にて本年度の具体的施策を策定（2006年6月15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）

○ これらを受け、各重要インフラ分野において、「安全基準等」の策定・見直しを実施（2006年9月を目処に）

（※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

イ）「安全基準等」の策定状況の把握及び評価

ウ）指針の見直し

各重要インフラ分野において、「安全基準等」の策定・見直しを実施（2006年9月を目処に）

重要インフラにおける安全基準等の策定・見直し状況

重要インフラ所管省庁の協力を得て、「安全基準等」策定・見直し状況の調査を行った結果、以下の通り、策定・見直しがなされつつあることを確認（2006年11月現在）

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等【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基準・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】	見直し中（※3）
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
（※3）今年度中に見直し完了予定

重要インフラにおける安全基準等の特徴

現時点で策定・見直しが完了した「安全基準等」を分野横断的に概観したところ、IT障害が国民生活・社会経済活動に重要な影響を及ぼさないようにするため、「自らが何をすべきか」が全ての関係者にとって理解可能な状況となりつつあることを確認

① 「行動計画」にて、対象とする脅威及び対象分野が拡張されたのに対応し、「安全基準等」を策定・見直ししている

- 「サイバー攻撃によるIT障害」に加え、「行動計画」にて新たに脅威とされた「非意図的要因によるIT障害」、「災害によるIT障害」を対象とする脅威としている
- 既存7分野（情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス）に加え、新規3分野（医療、水道、物流）についても、今年度中に見直し完了予定である医療分野を除き、安全基準等の策定・見直しが完了している

② 「指針」にて掲げる4つの柱と3つの重点項目をふまえ、各分野において必要と考えられる項目を記載している

- 4つの柱と3つの重点項目について、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
- また、当該事業分野の特質及び当該事業者等の特質（法令等の要求事項、業務内容、事業者等の規模等）をふまえ、情報セキュリティ対策項目を記載している
- 加えて、情報セキュリティを取り巻く環境の変化に応じ、安全基準そのものを随時見直すこととしている

③ 国内外のベストプラクティスを参考にしている

- ISO/IEC17799等の情報セキュリティに関する国際標準を参考にしている
- 「指針」に加えて、「政府機関の情報セキュリティ対策のための統一基準」、先行的に整備された他分野の「安全基準等」をベストプラクティスとして参考にしている

④ 事業者等において具体的な情報セキュリティ対策を行うことが予定されている

- 「安全基準等」は一部を除き法的拘束力を持たない「推奨基準」や「ガイドライン」の位置づけであるため、情報セキュリティ対策の具体的内容は事業者等の自主的な取り組みに委ねられている
- 事業者等において、具体的な情報セキュリティ対策を定めた内規の策定・見直しが期待されている
- 事業者等において、PDCAサイクルを回す中で自主的な点検を行い、継続的改善を行うことが期待されている