資料3

NISC National Information Security Center

2008年度重要インフラにおける「安全基準等の見直し状況等の把握及び検証」について

【最終報告（参考資料）】

2009年 1月 23日

内閣官房 情報セキュリティセンター（NISC）

目次

◆2008年度「安全基準等」の見直し状況等の把握及び検証におけるアプローチ

①「安全基準等」の見直し状況等

①安全基準等の見直し概要（情報通信分野（電気通信））

名称	①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） ②情報通信ネットワーク安全・信頼性基準 ③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）
発行主体	①、②総務省 ③電気通信分野における情報セキュリティ対策協議会（ISeCT）
08年度 見直しの概要	1．見直し（確認・検証）の状況・理由 ①及び②ともに、ネットワークのIP化に伴う電気通信サービスの事故の多発等を踏まえ確認・検証を実施した。 2．見直し（確認・検証）のプロセス 2005年10月から2007年5月に実施した情報通信審議会 情報通信技術分科会での審議・答申を踏まえ、①については、2007年8月にパブリックコメントを実施した。 同様に、②についても分科会の答申を踏まえ、情報通信審議会IPネットワーク設備委員会で2007年9月から12月まで審議を行い、2007年12月にパブリックコメントを実施した。 3．見直し（確認・検証）の結果 ①については電気通信事業法施行規則 第29条にネットワークの安全・信頼性確保のため管理規程の記載事項を追加し、2007年11月に公布・施行した。 ②については、ネットワークのIP化に対応した安全・信頼性対策として基準の項目及び対策の追加を行い、2008年3月公布、2008年4月施行した。 4．備考 ③については、定期的な見直しとして、電気通信事業の動向の変化、並びに情報セキュリティを取り巻く環境の変化に応じ、随時検討を行ない、必要に応じて確認・検証することがガイドライン上に明記されている。なお、ISeCTにおいて、2009年3月までに確認・検証を実施する予定である。

① 安全基準等の見直し状況等（情報通信分野（放送））

名称	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
発行主体	日本放送協会（NHK）、社団法人 日本民間放送連盟
状況	１．見直し（確認・検証）の状況・理由 指針見直しの要点（※）を踏まえ、確認・検証を実施した。 ２．見直し（確認・検証）のプロセス 日本放送協会及び社団法人日本民間放送連盟において、確認・検証を実施した。 ３．見直し（確認・検証）の結果 現行のガイドラインで問題がないことが確認できたため、改定不要と判断した。

※1：2007年度「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」見直しを通じて得られた重要インフラの情報セキュリティ確保に係る参考事項（要点）（2008年4月3日 重要インフラ専門委員会）

①安全基準等の見直し概要（金融分野）

名称	①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 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 ③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
発行主体	財団法人金融情報システムセンター（FISC）
08年度 見直しの概要	1．見直し（確認・検証）の状況・理由 ①については、1999年以来見直しを行っていないため、金融機関を取り巻く環境の変化に対応するため確認・検証を実施した。 2．見直し（確認・検証）のプロセス ①については、2007年11月から2008年5月にFISC監査安全部が事務局を務める「安全対策基準改訂に関する検討部会（以下、「部会」という）」で、確認・検証を実施した。具体的には、金融機関へのヒアリング実施による実態把握及び1999年以降に公表された主要なガイドラインとのギャップ分析の結果を踏まえ、改訂案の策定を行った。 3．見直し（確認・検証）の結果 ①については、策定した改訂案について、2008年5月に部会の上部組織である「安全対策専門委員会」の承認を受け、6月に改訂版を発刊した。 4．今後の予定 ②については、定期的な見直しの一環として、部会で検討作業を実施中であり、次回開催予定の「安全対策専門委員会」に付議する予定である。

① 安全基準等の見直し状況等（航空分野（航空管制、航空運送））

名称	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
発行主体	国土交通省
状況	**1．見直し（確認・検証）の状況・理由** 指針見直しの要点（※1）、政府機関統一基準（※2）に準拠する国土交通省情報セキュリティポリシーの改定等を踏まえ、確認・検証を実施した。 **2．見直し（確認・検証）のプロセス** 2008年8月から9月に国土交通省航空局で、確認・検証を実施した。 **3．見直し（確認・検証）の結果** 現行のガイドラインで問題がないことが確認できたため、改定不要と判断した。 **4．指針見直しの要点の取扱い** 航空管制システムに関係するシステムベンダーに周知を行った。

名称	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
発行主体	国土交通省
状況	**1．見直し（確認・検証）の状況・理由** 指針見直しの要点（※1）や定期航空協会内の各事業者が策定しているセキュリティポリシー等を踏まえ、確認・検証を実施した。 **2．見直し（確認・検証）のプロセス** 2008年8月から9月に国土交通省航空局で確認・検証を実施し、検証結果を、航空事業者、定期航空協会が確認した。 **3．見直し（確認・検証）の結果** 現行のガイドラインで問題がないことが確認できたため、改定不要と判断した。 **4．指針見直しの要点の取扱い** 航空事業者等に対して周知を行った。

※1：2007年度「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」見直しを通じて得られた重要インフラの情報セキュリティ確保に係る参考事項（要点）（2008年4月3日 重要インフラ専門委員会）
※2：政府機関の情報セキュリティ対策のための統一基準（第3版：平成20年2月4日情報セキュリティ政策会議決定）

① 安全基準等の見直し状況等（鉄道分野、電力分野）

名称	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
発行主体	鉄道事業者等
状況	1．見直し（確認・検証）の状況・理由 指針見直しの要点（※）、毎年度定められる年度計画（セキュア・ジャパン）を踏まえ、確認・検証を実施した。 2．見直し（確認・検証）のプロセス 2008年7月から9月に安全基準等の策定主体の一つである国土交通省鉄道局を中心に確認・検証を実施し、検証結果について鉄道事業者等に確認した。 3．見直し（確認・検証）の結果 現行のガイドラインで問題がないことが確認できたため、改定不要と判断した。 4．指針見直しの要点の取扱い 鉄道CEPTOARに周知した。

名称	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
発行主体	電気事業連合会
状況	1．見直し（確認・検証）の状況・理由 指針見直しの要点（※）を踏まえ、確認・検証を実施した。指針見直しの要点を踏まえた確認・検証にあたっては、要点に示された全ての項目を検討の対象とした。 2．見直し（確認・検証）のプロセス 2008年4月から5月に安全基準等の策定主体である電気事業連合会において、確認・検証を実施した。 3．見直し（確認・検証）の結果 指針見直しの要点に示された項目を個々に検証したところ、現行のガイドラインに問題がなかったため、改定不要と判断した。 4．指針見直しの要点（※）の取扱い 各電力事業者の内規見直し時の参考になるよう、電力事業者に周知した。

※2007年度「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」見直しを通じて得られた重要インフラの情報セキュリティ確保に係る参考事項（要点）（2008年4月3日 重要インフラ専門委員会）

① 安全基準等の見直し状況等（ガス分野、政府・行政サービス分野）

名称	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
発行主体	社団法人 日本ガス協会
状況	1．見直し（確認・検証）の状況・理由 指針見直しの要点（※）、一般的なITの先端技術動向、事業者の情報システムや運用の改善に伴う内規の見直しを踏まえ、確認・検証を実施した。指針見直しの要点を踏まえた確認・検証にあたっては、要点に示された全ての項目を検討の対象とした。 2．見直し（確認・検証）のプロセス 2008年4月から10月に日本ガス協会に設置されている分野内WGにおいて、ガイドラインの章ごとにWGの委員で分担し、確認・検証を実施した。 3．見直し（確認・検証）の結果 個々の観点について個々に確認・検証したところ、現行のガイドラインに問題ないことが確認できたため、改定不要と判断した。

名称	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
発行主体	総務省
状況	1．見直し（確認・検証）の状況・理由 他省庁が策定している個人情報の取り扱いに関するガイドラインについての調査を踏まえ、確認・検証を実施した。 2．見直し（確認・検証）のプロセス 2008年1月から4月に総務省自治行政局で他分野のガイドラインとの項目の差分及び記述レベルのギャップについて分析した。 具体的には地方公共団体の業務を利用主体及び個人情報の機密性に応じて４つに分類した上で、比較対象とする業務及び項目を選定し、それぞれについて、物理的、技術的セキュリティ、外部委託の観点から検討を行った。 3．見直し（確認・検証）の結果 致命的な不足項目は認められず、現行の安全基準等の記載で必要な記載事項が盛り込まれていること及び短期間での改定による各自治体での混乱を避けるため、改定は不要と判断した。

※2007年度「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」見直しを通じて得られた重要インフラの情報セキュリティ確保に係る参考事項（要点）（2008年4月3日 重要インフラ専門委員会）

① 安全基準等の見直し状況等（医療分野、水道分野）

名称	医療情報システムの安全管理に関するガイドライン第３版
発行主体	厚生労働省
状況	**１．見直し（確認・検証）の状況・理由** 無線LANやモバイルネットワークの利用といった業務体系の多様化への対応状況等について、確認・検証を実施した。 **２．見直し（確認・検証）のプロセス** 2007年10月から2008年3月に厚生労働省医政局に設置されている「医療情報ネットワーク基盤検討会」において、ネットワークの接続形態毎の脅威の分析等により、確認・検証を実施。 **３．見直し（確認・検証）の結果** 無線・モバイルを利用する際の技術的要件に関する事項、紛失や盗難等のリスクに関する事項の追記といった改定を2008年3月に実施した。 また、指針見直しの要点については、現行のガイドラインに問題ないことが確認できたため、改定不要と判断した。

名称	水道分野における情報セキュリティガイドライン
発行主体	厚生労働省
状況	**１．見直し（確認・検証）の状況・理由** 水道CEPTOARの整備、指針見直しの要点（※）を踏まえ、確認・検証を実施した。指針見直しの要点を踏まえた確認・検証にあたっては、要点に示された全ての項目を検討の対象とした。 **２．見直し（確認・検証）のプロセス** 水道CEPTOARの整備への対応については、2007年度中に厚生労働省健康局水道課が日本水道協会と連携しつつ、確認・検証を実施した。 また、指針見直しの要点を踏まえた確認・検証については、2008年9月に確認・検証を実施した。 **３．見直し（確認・検証）の結果** 2008年3月に水道CEPTOARに関する記載の追加等について改定を実施した。 また、指針見直しの要点については、現行のガイドラインに問題ないことが確認できたため、改定不要と判断した。 **４．備考** 情報システム障害について水道事業者等から報告があった場合、障害の内容を踏まえつつ、必要に応じてガイドラインの見直しを行うこととしている。なお、これまでの報告件数は０件である。

※2007年度「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」見直しを通じて得られた重要インフラの情報セキュリティ確保に係る参考事項（要点）（2008年4月3日 重要インフラ専門委員会）

① 安全基準等の見直し状況等（物流分野）

名称	物流分野における情報セキュリティ確保に係るガイドライン
発行主体	国土交通省
状況	１．見直し（確認・検証）の状況・理由 指針見直しの要点（※）を踏まえた確認・検証を実施した。 ２．見直し（確認・検証）のプロセス 2008年8月から9月に国土交通省政策統括参事官付（物流参事官室）で、確認・検証を実施した。その際、物流CEPTOAR等の関係者からの意見も併せて確認した。 ３．見直し（確認・検証）の結果 現行ガイドラインに問題ないことが確認できたため、改定不要と判断した。 ４．指針見直しの要点の取扱い 物流CEPTOAR及び事業者等に周知した。

※2007年度「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」見直しを通じて得られた重要インフラの情報セキュリティ確保に係る参考事項（要点）（2008年4月3日 重要インフラ専門委員会）

②各分野の安全基準等の特徴等

②各分野の安全基準等の特徴等

４つの柱　「ア　組織・体制及び資源の確保」

各重要インフラ事業者等における情報セキュリティ対策のPDCAサイクル を機能させるために、その運用等に係る**組織及び体制の確立**及びこれを支える資源の確保が重要である。
情報セキュリティ対策は、それに係るすべての職員が、職制及び職務に応じて与えられている権限と責務を理解した上で、準備された資源によって、負うべき責務を履行することで実現される。
このため、情報セキュリティ対策を実施する組織・体制及び資源の確保について明示されることが必要である。
なお、組織・体制及び資源の確保には、例えば、**セキュリティに関わる人材育成や教育**といった基礎的・長期的な取り組みから、情報セキュリティ対策の実効性を確保する上で兼務を禁止する役割の設定や違反への対応、例外措置の規定、**自己点検・監査の実施**等具体的な対策項目が含まれる。

○組織・体制の確立
・情報セキュリティに関する体制の整備（責任者の設置、専門部門、委員会）
・資源確保（雇用条件、懲戒手続）
・担当者の限定
・要員管理
・役割、責任分担の分離
・社内規定の整備（違反に関する規程、例外措置に関する規程）
・障害に対応する体制・手順の整備
・情報セキュリティ基本方針の策定
・守秘契約

○セキュリティに係わる人材育成や教育
・社員に対する教育の実施
・マニュアルの整備
・訓練の実施

○自己点検・監査の実施
・自己点検の実施
・監査の実施（内部監査・外部監査）
・対策の見直し

②各分野の安全基準等の特徴等

４つの柱　「イ　情報についての対策」

(ア)情報の格付け

取扱う情報について、その**重要性に応じた適切な措置**を講じるため、機密性、完全性、可用性の観点から情報の格付け（ランク）や、取扱制限（例：複製禁止、持出禁止、再配布禁止）が明示されるべきである。

○重要性に応じた適切な措置

・資産の洗出し方法（体制、洗出し項目、洗出し基準）

・情報のライフサイクルと情報の格付けに応じたセキュリティ対策

②各分野の安全基準等の特徴等

４つの柱　「イ　情報についての対策」

(イ)情報の取扱い

情報の作成、入手、利用、保存、移送、提供及び消去等、情報のライフサイクルに着目し、各段階におけるセキュリティ対策が明示されるべきである。

取扱う情報について、その重要性に応じた適切な措置を講じるため、機密性、完全性、可用性の観点から情報の格付け(ランク)や、取扱制限(例:複製禁止、持出禁止、再配布禁止)が明示されるべきである。

○情報の利用
- 目的外利用の禁止
- アクセス履歴の保存
- アクセス制御・出力制御
- 離席時の対策
- 入退室管理
- 長時間画面表示の制限
- 配布、複製の制限

○情報の作成、入手
- 情報の作成・入手時に格付け、取り扱い制限の設定、表示
- 入手時点の情報の格付けの継承
- 格付けの変更手続き
- 作成者の識別・認証(権限管理・認証)

○情報の保存
- 格付けに応じた情報の保存期間の決定
- 格付けに応じたアクセス制御
- 電子署名、暗号化による保護
- バックアップ
- 記録媒体の保存場所(災害対策)
- 長期間保存時の書き込み禁止措置
- 記録の確定手順の確立、作成責任者の識別情報の記録
- 更新履歴の保存
- 情報の持ち出し、所在管理

○情報の移送
- メールによる送信の制限
- 届出、許可制度、手続き
- 暗号化、パスワードの設定

○情報の提供
- 情報漏えい対策(付加情報の削除)
- 届出、許可制度、手続き

○情報の消去
- 情報漏えいの事象と対策例
- 復元困難な消去の実施
- 消去の確認
- 消去作業の記録
- 廃棄の許可制度
- 破棄手順の確立

②各分野の安全基準等の特徴等

４つの柱　「ウ　情報セキュリティ要件の明確化についての対策」

(ア)情報セキュリティ確保のために求められる機能

主体認証（利用者及び機器等の認証）、**アクセス制御**、**権限管理**、**証跡管理**、**負荷分散**、**冗長化**など基本的なセキュリティ機能の観点から、当該情報システムへ導入すべきセキュリティ要件が明示されるべきである。

○主体認証
- ・主体認証を行う必要性の検討（情報の格付け、情報システムの重要性）
- ・主体認証技術の選択（ID・パスワード認証、IDカード、生体認証、及び多要素認証）
- ・主体認証情報の保護（暗号化、パスワードの定期変更・文字数制限）
- ・不正使用検知時における主体認証の利用停止措置
- ・不正使用防止のための利用者の責任（ID・パスワードの貸与禁止、離席時の端末ロック）

○アクセス制御
- ・アクセス制御を行う必要性の検討（情報の重要度、取扱制限）
- ・利用者アクセスの管理（利用者登録、特権管理、パスワードの管理、アクセス権のレビュー）
- ・ネットワークのアクセス制御（利用方針、外部接続時の認証）
- ・アクセス制御の設定と管理（利用時間による制御、端末設定による制御、強制アクセス制御、ファイアウォール）

○権限管理
- ・権限管理の必要性の検討
- ・識別コードと主体認証情報の付与手続きの明示と管理

○証跡管理
- ・証跡管理の必要性の検討
- ・証跡データの取得と管理
- ・証跡データの点検、分析及び報告

○負荷分散
- ・トラフィックの分散処理、予備機の設置
- ・負荷状態の監視制御機能の充実

○冗長化
- ・ネットワークの適切な管理・制御、通信経路の迂回措置
- ・ハードウェアの予備

○その他
- ・自ら提供するサービスのセキュリティレベルを加入者に表明
- ・暗号と電子署名（鍵管理を含む）
- ・無線LANを利用する場合の留意点

②各分野の安全基準等の特徴等

４つの柱　「ウ　情報セキュリティ要件の明確化についての対策」
(イ)情報セキュリティについての脅威
セキュリティホール、**不正プログラム**及び**サービス不能攻撃**など様々な脅威に対して、当該情報システムへ導入すべきセキュリティ要件が明示されるべきである。

○セキュリティホール
- ・情報収集
- ・対応計画
- ・対応記録
- ・事前検証の実施
- ・定期チェック
- ・不正アクセスの監視・検出（IDSの使用）
- ・通信フィルタリング（ファイアウォール）
- ・外部ネットワークからの遮断等
- ・アンチウイルスソフトウェア使用（端末、ゲートウェイ）、メンテナンス、定期検査、セキュリティパッチ適用
- ・利用していない通信ポート等の非活性化、マクロ実行の抑制
- ・早期発見・早期回復対策（監視、障害の検出、障害箇所の切り分け、障害時の縮退・再構成、取引制限、リカバリ機能）

○不正プログラム
- ・情報収集
- ・注意喚起
- ・監視、記録の保存
- ・専門家との協力体制の構築
- ・アンチウイルスソフトウェア使用（自動検査、定期検査、メンテナンス）

○サービス不能攻撃
- ・帯域制限、ネットワーク輻そう検出・規制機能（重要通信の識別）
- ・通信フィルタリング
- ・通信回線の冗長化、通信事業者との連携

②各分野の安全基準等の特徴等

４つの柱　「エ　情報システムについての対策」
(ア)施設と環境、(イ)電子計算機、(ウ)アプリケーションソフトウェア、(エ)通信回線及び通信回線装置 共通

○導入時
・文書(仕様書、規程、マニュアル、利用者管理)の整備、見直し、変更管理、周知
・冗長化、予備設備(電子計算機、通信機器、コンピュータセンタ)
・試験(機能試験、回帰試験、負荷試験、障害試験、本番環境に影響を与えない試験)の実施
・責任分界点の明確化(相互接続時)・契約への盛り込み
・安全区域への設置(遠隔地でのバックアップ媒体保管、水害を受けにくい場所)
・防災対策(免震・耐震構造、耐火措置、落雷対策、水害対策、防災設備、監視設備、警報装置、非常口及び非常灯)
・自家発電装置、無停電電源装置、予備電源
・防犯対策(侵入防止装置、赤外線検知装置、トラップセンサー)の設置、記録用機器の使用制限、盗難防止装置)
・システム設計時の性能見積もり(将来の見込み含む)
・供給元及び更新情報、保守期間等が明確な機器の利用
・守秘義務契約の締結
・再委託先に対する同等の水準の制限
・保険への加入
・受け入れ基準の確立

○運用時
・入退室管理(障壁、施錠、主体認証、記録、継続的に立ち入る者の承認、侵入監視装置の設置、施設の最小限表示)
・データバックアップ、バックアップ媒体の安全管理
・目的外利用の禁止(閲覧可能なWebの制限、私的目的による使用の禁止)
・証跡管理
・不正検知、異常検知
・稼働監視(通常時、繁忙時の性能、トラブル時の復旧時間、再発防止策の実施状況、システム容量・能力管理)
・情報収集(利用ソフトウェア)
・無許可ネットワーク、外部ネットワーク接続の禁止
・運用管理記録、障害記録、作業記録の作成・管理(外部作業員管理等)
・主体認証(ネットワーク接続時も含む)
・時刻同期
・セキュリティホール対策(検査、対応)
・無線LAN使用時の対策(暗号化、主体認証、機器識別、証跡管理、アクセス制限、他ネットワークの利用制限、機密性確保、接続可能な機器の管理)
・ネットワークの分離(制御系と無線ネットワーク)
・構成管理(機器管理、外部接続管理)

○運用終了時
・情報の復元困難な状態にする(データ消去ソフトウェア、物理的破壊、磁気的な破壊)

※(ア)施設と環境～(エ)通信回線及び通信回線装置の間で、異なる節に同じ対策が書かれている対策について、共通のものとして取り出したもの

②各分野の安全基準等の特徴等

４つの柱　「エ　情報システムについての対策」

(ア)施設と環境

入退出の管理や**安全区域の確保**、**停電時への対応**等情報システムの設置・運用に係る施設や環境面での対策が明示されるべきである。

○入退出の管理

・訪問者及び受け渡し業者の管理（身分の記録、審査手順、立ち入り制限区域の設定、職員等の立ち会い・付き添い、ストラップ・ID カード、情報システムに接触できない場所での受け渡し）

・安全区域内のセキュリティ管理（身分証明書の携帯・常時視認、物品等の持ち込み・持ち出しの情報セキュリティ責任者の承認・記録、コンピュータ・外部記録媒体等の持ち込み制限、作業の監視）

○安全区域の確保

・設置場所の配慮（コンピュータセンターの２重化、遠隔地でのバックアップ媒体保管、水害を受けにくい場所への設置）

・電子計算機及び通信回線装置のセキュリティ確保（不正操作・盗み見・ケーブルからの盗聴・電磁波による漏えい等の防止対策）

○停電時への対応

・自家発電装置、無停電電源装置　・自家発電設備の冷却水等の定期点検項目

※(イ)電子計算機～(エ)通信回線及び通信回線装置で、異なる節に同じ対策が書かれている対策については、共通項目としてP16に記載している。

②各分野の安全基準等の特徴等

４つの柱　「エ　情報システムについての対策」

(イ)電子計算機

電子計算機の**設置時**、**運用時**、**運用終了時**における対策が明示されるべきである。

○設置時

・利用者の管理
・利用可能なソフトウェアの制限、利用不可のソフトウェアの制限、不要なアプリケーションの利用禁止、無効化、削除
・モバイル端末に対する対策（暗号化）
・情報漏えいに対する措置
・権限管理
・記録媒体を持たない端末の利用
・遠隔保守時の暗号化通信
・出荷時初期設定からの変更
・障害時、緊急時の対応手順の策定

○運用時

・不正プログラムへの対応（ウイルス対策ソフトの導入）
・定期点検の実施
・定期的な使用ソフトウェアの把握
・暗号化
・利用可能な通信回線、通信方法の制限
・負荷分散
・変更管理
・設置時と運用時のパスワードの変更
・障害時、緊急時を想定した訓練
・リモートアクセスの原則禁止
・人員交代等におけるアカウント管理
・敷地外に機器を設置する場合の対応
・権限管理、利用者制限
・外部委託作業者の作業の監視

※(ア)施設と環境、(ウ)アプリケーションソフトウェア、(エ)通信回線及び通信回線装置の間で、異なる節に同じ対策が書かれている対策については、共通項目としてP16に記載している。

②各分野の安全基準等の特徴等

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
アプリケーションソフトウェアの**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である。

○導入時
・世代管理の実施
・セキュリティ要件の検討、仕様化
・電子メールの不適切な中継設定の禁止
・主体認証
・ウェブにおける特殊文字使用の禁止、無効化
・ウェブサーバから攻撃に資する情報の送信を防ぐ対策
・公開するサーバ上に保存する情報の制限
・電子証明書による正当性証明
・通信データの暗号化
・運用体制（管理者、障害時の連絡体制、委託先窓口等連絡先、通常時以外の特別体制）の整備及び周知
・保険への加入
・開発環境と運用環境の分離
・移行手順の明確化

○運用時
・アクセス制御、ルーティングの整合性確認
・事業者自身が運用もしくは委託先が運用する電子メールサーバの利用
・HTMLメール使用時の注意
・電子署名による配布元の確認
・閲覧可能なWebサイトの制限
・電子メールの対策・制限（添付ファイルの保護、不正中継禁止、送受信容量の制限、自動転送、業務外利用、送信先アドレス漏洩の防止、電子署名、暗号化）
・不正監視
・セキュリティ管理
・利用ソフトウェア管理、バージョン管理
・外部ネットワークとの接続制限

※(ア)施設と環境、(イ)電子計算機、(エ)通信回線及び通信回線装置の間で、異なる節に同じ対策が書かれている対策については、共通項目としてP16に記載している。

②各分野の安全基準等の特徴等

４つの柱　「エ　情報システムについての対策」

(エ)通信回線及び通信回線装置

通信回線及び通信回線装置の**構築**から**運用**、**運用終了又は停止**に至るまでの対策が明示されるべきである。

○構築時

・未承認機器からの通信の遮断、
・通信の暗号化
・物理的セキュリティ
・SLAの締結
・通信性能の確保
・遠隔地からの保守時の対策
・外部からの侵入が困難な回線の選択
・原則公衆回線からの接続の禁止（例外時はコールバックやユーザの限定）
・移動、転倒防止措置
・不特定多数が接続するネットワークとの接続禁止
・改ざん防止対策
・盗聴防止対策
・ISO15408などの安全性が確認された機器の採用

○運用時

・変更管理
・運用管理記録の作成
・稼働監視
・不正検知
・異常（非日常状態の）検知
・利用する機器、利用者及び識別コードの管理
・リモートアクセス時の対策（主体認証、証跡管理、アクセス制限、機密性確保、利用可能な端末の管理）
・不要なポートの閉塞
・制御系ネットワークと無線ネットワークのセグメントの分離
・ルータによるDoS攻撃対策

※(ア)施設と環境、(イ)電子計算機、(ウ)アプリケーションソフトウェアの間で、異なる節に同じ対策が書かれている対策については、共通項目としてP16に記載している。

②各分野の安全基準等の特徴等

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」
（ア）事業継続性確保のための個別対策の実施
IT障害を未然に防止するための措置、**IT障害の発生を早期発見するための措置**、及びIT障害が発生した場合の**拡大防止や迅速復旧のための措置**が明示されるべきである。

○未然防止措置
・指揮命令系統の明確化
・権限委譲、代行順位の決定
・重要拠点（指揮拠点）の確保
・復旧計画、手順書の策定（連絡先、報告事項、対応措置、再発防止措置の策定）
・事業継続計画の試験
・教育・訓練・演習の実施（メーカとの協調）
・システムの多重化、代替手段の整備
・信頼性設計
・試験の実施
・物理的な不正侵入の防止
・他システムとの独立、接続点の最小化
・定期点検、システム更新
・非常時用の機能の整備、管理、監査及び管理手順の整備
・監督省庁への連絡
・重要業務の洗い出し、重要要素の抽出
・連絡体制の構築、連絡手段の確保
・障害管理
・設備管理

○早期発見のための措置
・システムの稼働監視
・不正アクセス、不正トラフィックの監視

○拡大防止・早期復旧のための措置
・対外的な情報発信、情報共有
・バックアップシステムの整備、代替手段の準備
・バックアップ稼働計画、復帰計画の策定
・データバックアップ、遠隔地への保管
・広報、顧客からの問い合わせの対応

②各分野の安全基準等の特徴等

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」

（イ）事業継続計画との整合性への配慮

事業継続計画が策定される場合には、顕在化する可能性が高いIT障害として様々なケースを想定して**事業継続計画に組み入れる**とともに、適宜点検し、必要に応じ対策の改善を行うべきである。

○事業継続計画との整合性の確保

・事業継続計画の把握体制の構築
・参考文献の提示（事業継続計画ガイドライン（内閣府）、企業に於ける情報セキュリティガバナンスのあり方に関する研究会報告書 参考資料事業継続計画策定ガイドライン（経済産業省））
・関係者間での事業継続計画の整合

②各分野の安全基準等の特徴等

３つの重点項目「イ　情報漏えい防止のための対策」
(ア)保護すべき情報の類型化
漏えい対策の対象となる**保護すべき情報を類型化**し、明示されるべきである。

○保護すべき情報を類型化
・情報分類の指針、情報のラベル付け及び取扱い、重要情報の格付け（ランク）
・資産の洗出し方法（体制、洗出し項目、洗出し基準）、情報、情報システムについてランク付け
・情報資産について、機密性、完全性、可用性ごとの分類
・安全管理上の重要度に応じて分類（安全性が損なわれた場合の影響の大きさに応じた重要度に応じた分類）
・個人データ取扱台帳の整備、リスクアセスメント結果に応じた分類

②各分野の安全基準等の特徴等

３つの重点項目「イ　情報漏えい防止のための対策」

(イ)保護すべき情報の管理

保護すべき情報及び当該情報が記録された**媒体を安全に取扱う(作成、入手、利用、保存、移送、提供及び消去等)ための措置**が明示されるべきである。

○作成、入手

・作業責任者・手続きの明確化
・作業担当者の識別、認証、権限付与(権限管理、電子証明書)
・業務以外の情報作成・入手の禁止
・情報作成・入手における格付け・分類と取扱制限

○利用

・格付けと取扱制限に沿った利用(業務外利用の禁止)
・要保護情報の利用にあたっての措置(情報交換の方針及び手順、取外し可能な媒体の管理、重要情報の内部漏えい、盗難、紛失、流出への対策)
・紙資料や電子媒体の持ち出し管理(紙資料等の保管ルール、端末への資料の保管、持出しに関するルールや制限)

○保存

・格付けに応じた情報の保存
・保存期間に応じた措置(長期保管の際の書込禁止の措置)
・安全な場所への保管(自然災害を被る可能性が低い地域への保管、外部記録媒体の耐火、耐熱、耐水及び耐湿を講じた施設への保管)
・内容表示の記号化
・バックアップの分散、隔地保管

○移送

・作業責任者・手続きの明確化
・作業担当者の識別、認証、権限付与
・情報の移送に関する許可及び届出に係る措置
・移送手段の選択
・電磁的記録の保護対策(相互認証、暗号化、パスワードの設定)

○提供

・情報を公表・外部提供する際の措置(完全性の確保)

○消去

・電磁的記録や書面の消去方法・廃棄方法(記録媒体の初期化等復元できない処置の実施)
・日時・担当者・処理内容の記録
・担当者の識別、管理者の許可、外部委託先を含めた処理確認

②各分野の安全基準等の特徴等

３つの重点項目「イ　情報漏えい防止のための対策」

(ウ)不正アクセスによる脅威への対策

保護すべき情報が保存された**PCや外部記録媒体の盗難、紛失**及び当該**PCや外部記録媒体からの情報漏えいを防止するための措置**や、保護すべき情報を処理するウェブやメール等の**アプリケーションからの情報の漏えいを防止するための措置**が明示されるべきである。

○PCや外部記録媒体の盗難、紛失を防止するための措置

・入退管理
・PC・外部媒体の原則外部持ち出し禁止
・移動可能な機器の盗難防止策、情報盗難の防止等の措置の実施

○PCや外部記録媒体からの情報漏えいを防止するための措置

・安全管理措置を講ずるための組織体制の整備、規定整備とそれに従った運用
・個人データの取扱状況を一覧できる手段の整備
・雇用契約時及び委託契約時における非開示契約の締結
・従業員に対する教育・訓練の実施
・保存の際のパスワード、暗号化等の対策の実施
・電子メールで送信する場合の相手先を限定し宛先を十分に確認すること

○アプリケーションからの情報の漏えいを防止するための措置

・取扱者の責任と権限の明確化
・取扱手順の規定と実施状況の確認
・主体認証機能、アクセス制御機能、権限管理機能
・データ保漏洩防止（暗証番号等の漏洩防止、相手端末確認機能）
・破壊・改ざん防止（排他制限機能、不良データ検出機能、ファイル突合機能）
・予防策（取引制限機能、事故時の取引禁止機能、電子的価値の保護機能、暗号鍵の保護機能、電子メール、ホームページ閲覧等の不正使用防止機能）
・ネットワーク上からの不正アクセス対策（ファイアウォール、ウイルス対策ソフト、IDS）、不正侵入防止機能（使用されていないポートの閉鎖、データの書き換えを検出する設定、定期的な改ざんの有無の検査）
・攻撃の予告に対する措置
・攻撃の記録の保存と関係機関との連携
・検知策（アクセスログの取得・保管、不正アクセスの監視機能、不正な取引の検知機能、異例取引の監視機能）
・早期発見対策（監視機能、障害の検出および障害箇所の切り分け機能）
・早期回復対策（障害時の縮退・再構成機能、取引制限機能、リカバリ機能）

②各分野の安全基準等の特徴等

３つの重点項目「イ　情報漏えい防止のための対策」
(エ)内部関係者による脅威への対策
内部関係者による情報漏えいを抑止するための措置、**情報漏えいの追跡性確保のための措置**の他、**情報セキュリティに関するリテラシーを向上させるための措置**や**取扱いミスを低減させるための措置**が明示されるべきである。

○内部関係者による情報漏えいを抑止するための措置
- 個人データ管理責任者の選定（閲覧等の利用時の管理者の許可）
- 外部での情報処理に関する規定の整備（事業社外での情報処理の制限）
- 個人データを取り扱う従業員及び権限の明確化
- 守秘・非開示契約の締結（不当な目的での使用等の禁止）
- 紙資料等の保管ルール（施錠可能なキャビネットへの保管、鍵の管理）
- 端末への資料の保管、持出しに関するルールや制限
- 入退管理や常時監視（カメラ）等の導入
- 役割の分離
- 破壊・改ざん防止（排他制限機能、アクセス制限機能、不良データ検出機能、ファイル突合機能、IDアクセスの不正使用防止機能）
- 会社支給以外のシステムによる情報処理
- 異常発見時の対応（管理者への連絡と適切な処置の実施）
- 退職後の個人情報保護規程
- 内部からの攻撃の監視（従業員の監督とモニタリング）

○情報漏えいの追跡性確保のための措置
- 証跡管理
- 検知策（不正アクセスの監視機能、不正な取引の検知機能、異例取引の監視機能）
- 早期発見（監視機能、障害の検出および障害箇所の切り分け機能）
- 早期回復対策（障害時の縮退・再構成機能、取引制限機能、リカバリ機能）

○リテラシーを向上させるための措置
- 情報セキュリティ対策の教育・研修・訓練

○取扱いミスを低減させるための措置
- 取引制限機能、事故時の取引禁止機能
- 電子的価値の保護機能、暗号鍵の保護機能、電子メール、ホームページ閲覧等の不正使用防止機能
- 外部ネットワークからのアクセス制限、不正侵入防止機能

②各分野の安全基準等の特徴等

３つの重点項目「イ　情報漏えい防止のための対策」
(オ)情報漏えい発生時の対応策の整備
　情報漏えいの発生に備えて、当該事象へ対応するための**体制**及び**対処手順**等が明示されるべきである。

○体制
- ・責任・権限を有する担当者の選任
- ・連絡体制の整備
- ・報告事項、対応措置、代替手段などの規定

○対処手順
- ・事実関係の把握・整理・対応検討（漏えいした情報の範囲の特定）
- ・漏えい経路の特定（システム・端末の調査等）
- ・漏えい継続の阻止、被害の最小化（対象通信の遮断や対象サーバ等をネットワークから隔離するための運用フロー等の整備）
- ・記録の保全
- ・本人への通知、事実関係の公表、広報
- ・所管省庁への報告
- ・関係機関への周知（セプターを活用した情報共有）
- ・漏えいに至った経緯・原因等の解析
- ・再発防止策の検討と対策の実施

②各分野の安全基準等の特徴等

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」
(ア)委託先管理の仕組み
外部委託可能な範囲の明確化や**委託先の選定基準**、**委託先に求める情報セキュリティ対策項目**や**事業者としての管理方法等**が明示される事が必要である。この場合、**国際規格を踏まえた既存の取り組み**等を参考に検討するべきである。

○外部委託可能な範囲の明確化や委託先の選定基準や委託先の選定基準
- 委託目的の明確化
- 選定手続、選定基準の明確化
- 委託先が具備する要件の整理（技術水準、経営状況、管理体制、教育）
- 委託可能なシステムの範囲の明確化
- サービス変更時の再審査
- 脅威の想定
- 委託範囲外への影響の想定

○委託先に求める情報セキュリティ対策項目
- 情報セキュリティ対策の遵守方法
- 同等以上の情報セキュリティ対策
- 委託先に求める情報セキュリティ対策の周知
- 機密保持（機密保持契約）、目的外利用の禁止（確認書の提出）
- 個人情報を扱う場合の要件の明確化
- 委託先作業時の申請
- 作業報告書の提出

○事業者としての管理方法
- 提供する情報の最小化
- 委託先がアクセス可能な資産の制限
- 委託先のセキュリティ対策の実施に関する保証
- 納品検査時のセキュリティ対策の確認
- 委託先が再委託するときの対応策の整備
- 監視
- レビュー
- 監査
- 保守用専用アカウントの設定

○国際規格を踏まえた既存の取り組み
- 各種公的認証の取得状況（JIS X 5080）

②各分野の安全基準等の特徴等

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」
(イ)外部委託実施における情報セキュリティ確保策の徹底
基本契約の締結や委託内容・取扱い情報の重要性に応じたとるべき情報漏えい防止策等の強化**対策事項の契約への盛り込み等**、**契約者双方の責任の明確化と合意形成**が明示されるべきである。

○基本契約の締結
・委託先の情報セキュリティ対策（セキュリティポリシーの準用、教育）
・機密保持（機密保持契約）、目的外利用の禁止（確認書の提出）
・情報セキュリティ侵害発生時の対処手順
・情報セキュリティ対策不履行時の対処手順（損害賠償請求）
・情報管理責任者の設置
・再請負の制限
・責任者、委託内容、作業者、作業内容の特定
・サービスレベルの保証
・契約終了時の情報の扱い

○情報の重要性に応じた対策事項の契約への盛り込み
・扱う情報に応じた対策の選定
・委託先における同等以上のセキュリティ対策の実施

○契約者双方の責任の明確化と合意形成
・遵守方法及び管理体制に関する管理（確認書の提出、管理記録の提出）
・委託先要因の各種ルールの遵守
・施設全体の運転業務全般にわたる取り決め
・障害発生時の罰則規定の合意
・監査
・入退室管理
・選定手続き、選定基準、要件に基づく委託先選定

②各分野の安全基準等の特徴等

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」
(ウ)ＩＴ障害発生時の対応策の整備
IT障害発生時における委託先の措置や**重要インフラ事業者等としての対処方法（委託先及び委託元との間の連絡体制や委託先と委託元が一体となったトラブル対処方法等）**が明示されるべきである。

○IT障害発生時における委託先の措置
・対処手順を含んだ契約の締結
・対処手順の事前の周知
・異常検知ツールの活用
・異常状態の記録・保存
・連絡体制の整備
・障害箇所の切り離し
・原因の特定
・修正プログラムの適用
・緊急事態の洗い出し

○重要インフラ事業者等としての対処方法（委託先及び委託元との間の連絡体制や委託先と委託元が一体となったトラブル対処方法等）
・問題発生時の対処の合意
・利用者への説明責任の認識
・行動基準の規定
・責任分界点の明示
・体制の整備（連絡体制）
・事実関係の確認
・外部要因による障害の防止
・波及の恐れがある場合のセプターへの連絡
・委託先との情報共有
・他システムへの影響調査
・IT障害対応の訓練、演習の計画・実施

②各分野の安全基準等の特徴等

◆安全基準等の継続的改善
　各分野ごとの安全基準等の運用を把握する観点から、現状の各分野の安全基準等の見直しや浸透に関するPDCAサイクルがどのようになっているか

分野		各分野ごとの対応状況
情報通信	電気通信	電気通信事業法等（※）及び情報通信ネットワーク安全・信頼性基準については、情報通信審議会 情報通信技術分科会の答申を踏まえ、確認・検証を実施している。また、改定においてはパブリックコメントを実施している。 また、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）については事業者や情報セキュリティマネジメントの知見を有する事業者・団体を構成員とする協議会において確認・検証を実施している。
	放送	日本放送協会（NHK）、社団法人日本民間放送連盟において、確認・検証を実施している。
金融		FISC内に常設されている安全対策基準改訂に関する検討部会において、確認・検証を実施している。
航空	航空運送	本文に、国土交通省航空局、航空運送事業者間で合意することが明記されており、国土交通省航空局で確認・検証を実施し、検証結果について、航空事業者、定期航空協会が確認している。
	航空管制	国土交通省航空局が確認・検証を実施している。
鉄道		本文に、国土交通省鉄道局と鉄道事業者等が協力して確認・検証を行うことが明示されており、国土交通省鉄道局を中心に鉄道CEPTOAR内において確認・検証を実施している。
電力		電気事業連合会において確認・検証を実施しており、必要に応じて各電力会社の社長で構成される電気事業連合会総合政策委員会で決定している。
ガス		日本ガス協会に設置されている分野内WGにおいて、ガイドラインの章ごとにWGの委員で分担し、確認・検証を実施している。
政府・行政		総務省自治行政局において確認・検証を実施している。また、改定においてはパブリックコメントを実施している。
医療		厚生労働省医政局に設置されている医療情報ネットワーク基盤検討会において、確認・検証を実施している。また、改定においてはパブリックコメントを実施している。
水道		厚生労働省健康局水道課において、日本水道協会と連携しつつ、確認・検証を実施している。
物流		国土交通省政策統括参事官付（物流参事官室）において確認・検証を実施しており、必要に応じて物流CEPTOARの関係者と連携している。

※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）

③ 安全基準等に係る３年間の取り組みについての総括

③安全基準等に係る３年間の取り組みについての総括（情報通信（電気通信）分野）1/2

名称		①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） ②情報通信ネットワーク安全・信頼性基準 ③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）
発行主体		①、②総務省、③電気通信分野における情報セキュリティ対策協議会（ISeCT）
策定・見直し状況	2006年度	①②については、2006年2月に策定された指針を踏まえ、2006年9月を安全基準等として位置付けるとともに、③については、業界横断的なガイドラインとして備えるべき対策項目及び水準を示すものとして新たに策定した。
	2007年度	③については、2007年6月の指針の改定を踏まえ、電気通信分野における情報セキュリティ対策協議会で議論を実施した。指針での改定項目が現行安全基準等にて既に記載されているため、改定は不要という判断を電気通信分野における情報セキュリティ対策協議会で議決した。 ①、②ともに、ネットワークのIP化に伴う電気通信サービスの事故の多発等を踏まえ、情報通信審議会 情報通信技術分科会の答申を踏まえ、確認・検証を実施した。 ①については、電気通信事業法施行規則 第29条に管理規程の記載事項を追加し、新たな記載項目の詳細について告示に定めることとし、2007年8月にパブリックコメントを実施した。2007年11月21日に公布・施行した。 ②についても、情報通信審議会IPネットワーク設備委員会で2007年9月～12月まで審議し、ネットワークのIP化に対応した安全・信頼性対策として基準の項目及び対策の追加を行った。
	2008年度	②については、2008年4月1日に施行した。 ③については、2009年3月までに定期的な確認・検証を実施する予定である。

③安全基準等に係る３年間の取り組みについての総括（情報通信分野（電気通信））2/2

名称	①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） ②情報通信ネットワーク安全・信頼性基準 ③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）
概要	**①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）** １．電気通信事業の公共性にかんがみ、その運営を適正かつ合理的なものとするとともに、その公正な競争を促進することにより、電気通信役務の円滑な提供を確保するとともにその利用者の利益を保護し、もつて電気通信の健全な発達及び国民の利便の確保を図り、公共の福祉を増進することを目的して制定した。 ２．安全基準等に関わる代表的な条項。 ・第8条：重要通信の確保　・第41条～第51条：第１款 電気通信事業の用に供する電気通信設備　等 ３．ＩＴ障害の原因となる事故・災害等に関する技術基準・管理規定、重要通信確保義務等、電気通信事業者等が設備、管理面で遵守しなければならない事項を規定。 **②情報通信ネットワーク安全・信頼性基準** １．電気通信事業者全般及び自営系ネットワークを対象とし、情報通信ネットワークにおける安全・信頼性対策の指標となるガイドライン（国が法令等に準じて定めた推奨基準）として告示。 通信の安定的な提供、通信の疎通の確保、通信の不正使用の防止等を目的として、情報通信ネットワーク全体から見た対策項目について網羅的に整理、検討を行い、ハードウェア及びソフトウェアに備えるべき機能やシステムの維持と運用までを総合的に取り入れたもの。 ２．２つの安全・信頼性基準と２つの配慮すべき事項から構成。 〔安全・信頼性基準〕　設備等基準　管理基準 〔配慮すべき事項〕情報セキュリティポリシー策定のための指針、危機管理計画策定のための指針 **③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）** １．次の７つの観点を記述。 ・組織・体制の整備及び資源の確保　・情報についての対策　・情報セキュリティ要件の明確化に基づく対策 ・情報システムについての対策　・IT障害の観点から見た事業継続性確保のための対策 ・情報漏えい防止のための対策　・外部委託における情報セキュリティ確保のための対策 ２．対象脅威を（１）サイバー攻撃によるIT障害、（２）ネットワーク輻そう、（３）その他のIT障害（故障、災害等）（４）重要情報漏えいの4つとし、一般的対策（共通項目）と、対象脅威毎に固有の情報セキュリティ対策とを区分して記述。 ◎安全基準等の公開状況：公開 ①は電子政府の総合窓口等で公開されている。　http://www.e-gov.go.jp/index.html ②は総務省ホームページで公開されている。　http://www.soumu.go.jp/menu_02/ictseisaku/net_anzen/ ③はISeCTのホームページで公開されている。　http://www.fmmc.or.jp/ISeCT/index.html

③安全基準等に係る３年間の取り組みについての総括（情報通信分野（放送））

名称		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
発行主体		日本放送協会（NHK）、社団法人 日本民間放送連盟
策定・見直し状況	2006年度	国民生活に極めて密着し、社会経済活動の基盤として位置づけられる基幹情報メディアである放送事業を支える放送設備や回線設備等の情報インフラに対するセキュリティ対策を主体的に進めていくための留意点をまとめたものとして、2006年9月に制定した。
	2007年度	NHK及び民放連において指針の改定を踏まえ、反映されているかどうかについて検討を実施した。見直しの結果、指針の改訂項目については、現行安全基準において規定されており、改定の必要はないと判断した。加えて、2008年1月にNHK、民放連において、対応すべき障害の具体化の観点から、情報システムのセキュリティ要件の見直しを実施した。
	2008年度	指針見直しの要点を踏まえ、確認・検証を実施した。現行のガイドラインに問題がないことが確認できたため、改定不要と判断した。
概要		１．ガイドラインの構成 ・策定の目的 ・対象範囲と想定する脅威 ・放送事業者が担うべき役割 ・組織・体制等の確保 ・情報インフラにおける情報の取扱いについての対策 ・情報セキュリティ要件の明確化に基づく対策 ・情報システムについての対策 ・外部委託における情報セキュリティ確保のための対策 ２．情報の対象範囲 放送サービスを提供するに当たり構築されている情報システム ※「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（各放送事業者がガイドラインの策定を検討） ３．安全基準等の公開状況：公開

③安全基準等に係る３年間の取り組みについての総括（金融分野）

名称		①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 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 ③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
発行主体		財団法人金融情報システムセンター（FISC）
策定・見直し状況	2006年度	①②③については、2006年2月に策定された指針を踏まえ、2006年9月に安全基準等として位置付けた。また、定常的な見直しの一環として、金融機関等のセキュリティ動向を踏まえ2007年3月に②の第7版追補版を発刊した。
	2007年度	常設している「安全対策基準改訂に関する検討部会」で継続的に見直しを行っており、2007年6月に改定された指針について見直しを実施した。既に対応済みであり、改訂不要と判断した。
	2008年度	①については、金融機関を取り巻く環境の変化に対応するため確認・検証を実施した。具体的には、金融機関へのヒアリング実施による実態把握及び、1999年以降に公表された主要なガイドラインとのギャップ分析の結果を踏まえ、改訂案の策定を、FISCが事務局を務める「安全対策基準改訂に関する検討部会」で行い、部会の上部組織である「安全対策専門委員会」で承認を受け、2008年6月に改訂版を発刊した。 ②については、定期的な見直しの一環として、部会で検討作業を実施中であり、次回開催予定の「安全対策専門委員会」に付議する予定である。
概要		①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 １．安全対策の趣旨徹底と遺漏のない履行のために、明確な施策によって、全社的な意思統一を図る必要性が高まってきたことから策定。金融機関等自身がビジネスにおいて何を脅威として認識し、何を保護するかを決定すると同時に、金融機関等自身の言葉で表現することが重要であり、各金融機関においては、本書を参考にして、自機関のオリジナルなセキュリティポリシーを策定することが必要としている。 ２．セキュリティポリシーを策定するに当たって必要な作業とその考え方 ①解説編 基本的な視点、アプローチ方法、有効に機能するために望ましい組織、体制の在り方 ②策定手順編 セキュリティポリシーとセキュリティスタンダード策定に対する考え方と手順 ③参考編 安全対策の実施・運用へのセキュリティポリシーの係わりを整理

③安全基準等に係る３年間の取り組みについての総括（金融分野）

名称	①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 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 ③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
概要	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 １．金融機関等のコンピュータシステムの安全対策の管理体制の確立等を目的に策定 ２．具体的な安全対策基準 ①設備基準138小項目：自然災害、不正行為等に対する設備面の対策 ②運用基準113小項目：開発・運用管理体制等についての対策 ③技術基準53小項目：ハードウェア、ソフトウェア等技術面の対策 ３．各金融機関等は、本基準を参考に以下の手順で適切な安全対策を実施することを期待 ①セキュリティポリシー（基本方針）の策定 ②セキュリティスタンダード（自社の安全対策基準）の策定と実施 ③安全対策の改善（PDCAサイクルの実施） ④コンティンジェンシープランの策定 ③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 １．金融機関等の業務の公共性に鑑み、緊急事態においても「ある一定水準の業務の継続性の確保」という社会的要請に応えるために策定 ２．策定の流れは以下の通り（PDCAサイクル） 第1工程：必要性の認識と推進 第2工程：予備調査と基本方針の決定 第3工程：具体的なコンティンジェンシープランの立案 第4工程：コンティンジェンシープランの決定 第5工程：コンティンジェンシープランの維持管理 ３．以下自然災害以外のリスクも考慮 ①大規模システム障害リスク（コンピューターシステム停止） ②風評リスク ③情報漏洩リスク（情報漏洩事故） ④サイバー攻撃リスク（破壊（サイバーテロ）） ◎安全基準等の公開状況：公開 ①、②、③はFISCのホームページ等を通じて有償販売されている。

③安全基準等に係る３年間の取り組みについての総括（航空分野（航空管制））

名称		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
発行主体		国土交通省
策定・見直し状況	2006年度	指針に加え、政府機関統一基準、国土交通省セキュリティポリシー及び航空局内規をベースとし、重点課題であるIT障害の対象脅威に対して、情報セキュリティ対策の項目及び内容を明示するものとして2006年9月に策定した。
	2007年度	2007年6月に改定された指針を踏まえ、安全ガイドラインの見直し要領に従い、国土交通省航空局の関係者にて現行ガイドラインとの整合状況の確認を実施した。見直しの結果、「負荷分散・冗長化を検討すること」を追記した。
	2008年度	指針見直しの要点や政府機関統一基準に準拠する国土交通省情報セキュリティポリシーの改定等を踏まえ、確認・検証を実施した。現行ガイドラインに問題がないことが確認できたため、改定不要と判断した。
概要		１．安全基準等として盛り込む具体的な対策が網羅的なものになるよう、本ガイドラインは、次の７つの観点毎に必要となる情報セキュリティ対策の項目及び内容を記述 ・組織・体制及び資源の確保 ・情報についての対策 ・情報セキュリティ要件の明確化に基づく対策 ・情報システムについての対策 ・IT障害の観点から見た事業継続性確保のための対策 ・情報漏えい防止のための対策 ・外部委託における情報セキュリティ確保のための対策 ２．対象脅威を以下の３つとし、脅威に対応すべき対策項目を記述 ・サイバー攻撃によるIT障害 ・非意図的要因によるIT障害 ・災害によるIT障害 ３．安全基準等の公開状況：公開

③安全基準等に係る３年間の取り組みについての総括（航空分野（航空運送））

名称		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
発行主体		国土交通省
策定・見直し状況	2006年度	指針に加え、政府機関統一基準及び情報セキュリティ管理基準等の基準をベースとし、重点課題であるIT障害の対象脅威に対して、情報セキュリティ対策の項目及び内容を明示するものとして2006年9月に策定した。
	2007年度	2007年6月に改定された指針を踏まえ、ガイドラインに示された見直し要領に従い、国土交通省航空局及び航空運送事業者等にて整合状況の確認を実施した。見直しの結果、「負荷分散・冗長化を検討すること」を追記した。
	2008年度	指針見直しの要点や定期航空協会内の各事業者が策定しているセキュリティポリシー等を踏まえ、国土交通省航空局で確認・検証を実施し、検証結果を航空事業者、定期航空協会が確認した。現行のガイドラインに問題がないことが確認できたため、改定不要と判断した。
概要		１．安全基準等として盛り込む具体的な対策が網羅的なものになるよう、本ガイドラインは、次の７つの観点毎に必要となる情報セキュリティ対策の項目及び内容を記述 ・組織・体制及び資源の確保 ・情報についての対策 ・情報セキュリティ要件の明確化に基づく対策 ・情報システムについての対策 ・IT障害の観点から見た事業継続性確保のための対策 ・情報漏えい防止のための対策 ・外部委託における情報セキュリティ確保のための対策 ２．対象脅威を以下の３つとし、脅威に対応すべき対策項目を記述 ・サイバー攻撃によるIT障害 ・非意図的要因によるIT障害 ・災害によるIT障害 ３．安全基準等の公開状況：公開

③安全基準等に係る３年間の取り組みについての総括（鉄道分野）

名称		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
発行主体		鉄道事業者等
策定・見直し状況	2006年度	指針に加え、政府統一基準及び情報セキュリティ管理基準等の基準をベースとし、重点課題であるIT障害の対象脅威に対して、情報セキュリティ対策の項目及び内容を明示するものとして平成2006年9月に策定した。
	2007年度	2007年6月に改定された指針を踏まえ、所要の見直し作業を国土交通省 鉄道局を含めた鉄道セプター内において実施した。見直しの結果、指針での改定項目が既に記載されているため、改定は不要と判断した。
	2008年度	指針見直しの要点、毎年度定められる年度計画（セキュア・ジャパン）を踏まえ、策定主体の一つである国土交通省鉄道局を中心に確認・検証を実施し、検証結果について鉄道事業者等に確認した。現行のガイドラインに問題がないことが確認できたため、改定不要と判断した。
概要		１．安全基準等として盛り込む具体的な対策が網羅的なものになるよう、本ガイドラインは、次の７つの観点毎に必要となる情報セキュリティ対策の項目及び内容を記述 ・組織・体制及び資源の確保 ・情報についての対策 ・情報セキュリティ要件の明確化に基づく対策 ・情報システムについての対策 ・IT障害の観点から見た事業継続性確保のための対策 ・情報漏えい防止のための対策 ・外部委託における情報セキュリティ確保のための対策 ２．対象脅威を以下の３つとし、脅威に対応すべき対策項目を記述 ・サイバー攻撃によるIT障害 ・非意図的要因によるIT障害 ・災害によるIT障害 ３．安全基準等の公開状況：公開

③安全基準等に係る３年間の取り組みについての総括（電力分野）

名称		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
発行主体		電気事業連合会
策定・見直し状況	2006年度	自主的な取り組みのもと、2005年６月にe-Japan戦略Ⅱ加速化パッケージを先取り策定されたガイドラインについて、2006年2月に策定された指針を踏まえ、確認・検証を実施した。同年9月に従来の想定脅威に「非意図的要因」などを加えるなどの改定を2006年9月に実施した。
	2007年度	2007年6月に改定された指針の改訂を踏まえるとともに、全体的な見直しを実施した。2007年9月までにPDCAサイクルの規定等対応が必要と判断した箇所について改定を実施した。
	2008年度	指針見直しの要点を踏まえて確認・検証を実施した。現行のガイドラインに問題がないことが確認できたため、改定不要と判断した。
概要		１．本ガイドラインは、電力１２社で十分なリスク分析等を行ったうえで、それぞれの想定脅威に対し、電力制御システム等において事前に具備すべき対策を示した「技術的水準」と、運用時や障害発生時等の対策を示した「運用基準」とに整理しながら、網羅的に取り纏めた。 ・総則（目的・リスク・用語の定義等を記載） ・災害に対する技術的水準 ・災害に対する運用基準 ・サイバー攻撃や非意図的要因による障害に対する技術的水準 ・サイバー攻撃や非意図的要因による障害に対する運用基準 ２．本ガイドラインは、指針が対象とする範囲を含めて、「電力制御に係るネットワークは独立性を高め公衆網とは分離させる」など、効果が期待できる各種対策を取り纏めている。 ３．安全基準等の公開状況：非公開 電力分野の安全基準等は非公開であるが、情報セキュリティに関する取り組みが電気事業連合会のホームページで紹介されている。 http://www.fepc.or.jp/present/supply/security/index.html

③安全基準等に係る３年間の取り組みについての総括（ガス分野）

名称		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
発行主体		社団法人 日本ガス協会
策定・見直し状況	2006年度	情報セキュリティに関する都市ガス業界標準として、2006年2月に策定された指針を踏まえ、事業者自ら定める内規の策定を促進・支援するためのガイドラインとして平成2006年9月に策定した。
	2007年度	2007年6月に改定された指針を踏まえた見直しを実施した。見直しの結果、2007年8月に指針で改定された箇所のうち、対応が必要と判断した箇所について改定を実施した。
	2008年度	指針見直しの要点、一般的なITの先端技術動向、事業者の情報システムや運用の改善に伴う内規の見直しを踏まえ、確認・検証を実施した。現行のガイドラインに問題がないことが確認できたため、改定不要と判断した。
概要		１．ガイドラインには安全基準として求められる7つの観点毎に必要となる対策項目を網羅するために、以下の構成にて策定。 ・ガイドライン策定の目的　・対象範囲と想定する脅威 ・重要インフラ事業者の担う役割 ・対策項目 〇4つの柱 ◇組織・体制及び資源の確保　◇情報についての対策 ◇情報セキュリティ要件明確化に基づく対策　◇情報システムについての対策 〇3つの重点項目 ◇事業継続性確保のための対策　◇情報漏えい防止のための対策 ◇外部委託先における情報セキュリティ確保の対策 ・フォローアップ ２．都市ガス業界では「ＩＴ障害」をＩＴの機能不全による「ガスの供給支障」と捉え、製造・供給に係る制御系システムを対象に、指針に沿って非意図的要因・災害対応も含めてセキュリティ対策を規定した。 ３．安全基準等の公開状況：非公開 ガス分野における安全基準等は非公開であるが、情報セキュリティの取り組みが日本ガス協会のHPで紹介されている。 http://www.gas.or.jp/security_taisaku.pdf

③安全基準等に係る３年間の取り組みについての総括（政府・行政サービス分野）

名称		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
発行主体		総務省
策定・見直し状況	2006年度	情報セキュリティ侵害事案の発生、新たな対策技術の動向等を踏まえ、地方公共団体の情報セキュリティ水準の向上を推進するため2001年に策定し、2003年に一部改定したガイドラインについて、2006年の指針策定や様々な事案の発生、政策動向等を踏まえて2006年9月に全部改定を実施した。
	2007年度	2007年6月に改定された指針を踏まえた総務省 自治行政局において、見直しを実施した。見直しの結果、2006年9月全面改定時に既に盛り込み済みであったため、改定不要と判断した。
	2008年度	他省庁が策定している個人情報の取り扱いに関するガイドラインについての調査を踏まえ、確認・検証を実施した。致命的な不足項目は認められず、改定は不要と判断した。
概要		１．ガイドラインの主な特徴 ・全体を「総則」、「情報セキュリティ基本方針」、「情報セキュリティ対策基準」の三章構成に整理。 ・対策基準の構成を、PDCAサイクルを踏まえて変更。また、各対策の説明を、趣旨、例文、解説の順に統一。 ・情報漏えい防止等のため取るべき対策や生体認証等新たな対策技術の動向を踏まえた規定を追加。 ・各地方公共団体において取り扱う情報資産の重要性や取り巻く脅威の大きさが異なることから、各地方公共団体の実情に応じて実施することが望まれる事項を推奨事項と明記。 ・地域における広報啓発や注意喚起、官民の連携・協力等に積極的に貢献することが望まれる旨記述。 ・責任主体を明記し、権限と責任を明確化。 ２．指針への対応 ・指針において列記された項目に対応 ・情報のライフサイクルに着目した対策の明示 ・機密性、完全性、可用性の観点からの情報の分類や取扱制限の明示　等 ３．安全基準等の公開状況：公開 当該ガイドラインは総務省のホームページに公開されている http://www.soumu.go.jp/s-news/2006/pdf/060929_8_1.pdf

③安全基準等に係る３年間の取り組みについての総括（医療分野）

名称		医療情報システムの安全管理に関するガイドライン第３版
発行主体		厚生労働省
策定・見直し状況	2006年度	法令に保存義務が規定されている診療録及び診療諸記録の電子媒体による保存に関するガイドライン及び医療機関等における個人情報保護のための情報システム運用管理ガイドラインを含んだガイドラインとして2005年３月に作成。 その後、医療が「重要インフラ」に位置付けられたことに伴い、指針への対応等サイバー攻撃や災害等への対応を明確化することが求められたことを踏まえ、2007年３月にネットワーク要件や災害等の非常時の対応等を新設・改正等所要の改定を行った。
	2007年度	厚生労働省医政局において、2007年3月時点の指針の改定案の改定内容に対して、改定要否を検討した。また、パブコメ後に正式に決定された指針についても見直し要否について再度確認を実施した。結果、対応していることが確認されたため、改定不要と判断した。また、厚生労働省医政局に設置されている「医療情報ネットワーク基盤検討会」において、ネットワークの接続形態毎の脅威の分析等により、見直しを実施した。無線・モバイルを利用する際の技術的要件に関する事項、紛失や盗難等のリスクに関する事項の追記といった改定を実施した。
	2008年度	指針見直しの要点を踏まえ、確認・検証を実施した。現行ガイドラインに問題がないことが確認できたため、改定不要と判断した。
概要		１．必要となる情報セキュリティ対策の項目及び内容を記述 ①個人情報を含むデータを扱う医療機関等で参照されるべき内容 ・医療情報を扱う医療機関等における責任のあり方 ・情報システムの基本的な安全管理等 ②保存義務のある診療録等を電子的に保存する場合の指針等 ③運用管理規定の作成について ２．対象脅威を大きく以下の４つとし、考え方、最低限のガイドライン及び推奨されるガイドラインとして記述 ①サイバー攻撃によるＩＴ障害　②災害によるＩＴ障害 ③意図的要因によるＩＴ障害　④非意図的要因によるＩＴ障害 ３．安全基準等の公開状況：公開 当該ガイドラインは厚生労働省等のホームページに公開されている http://www.mhlw.go.jp/shingi/2008/03/s0301-2.html

③安全基準等に係る３年間の取り組みについての総括（水道分野）

名称		水道分野における情報セキュリティガイドライン
発行主体		厚生労働省 健康局 水道課
策定・見直し状況	2006年度	水道分野が重要インフラ分野にされたことを受けて、2006年2月に策定された指針を踏まえ、水道事業者が適切な情報セキュリティ対策を実施するための参考として、国が定める「ガイドライン」として2006年度に策定した。
	2007年度	厚生労働省が（社）日本水道協会と連携しつつ、指針の改定内容を踏まえた検討を実施。水道セプターの位置付け等の記載について改定を実施した。なお、水道セプターの設置は2008年3月を予定していたことを踏まえ、ガイドライン改訂版の通知は同月に実施した。
	2008年度	指針見直しの要点を踏まえ、確認・検証を実施した。現行のガイドラインに問題がないことが確認できたため、改定不要と判断した。
概要		１．安全基準等として盛り込む具体的な対策が網羅的なものになるよう、本安全基準は、次の７つの観点毎に必要となる情報セキュリティ対策の項目を記述 ・組織と体制の構築 ・情報についての対策 ・情報セキュリティ要件の明確化に基づく対策 ・情報システムの構成要素についての対策 ・事業継続性確保対策 ・情報漏えい防止のための対策 ・外部委託における情報セキュリティ確保のための対策 ２．対象脅威を以下の３つとし、各脅威に応じた対策を記述 ・サイバー攻撃によるIT障害 ・非意図的要因によるIT障害 ・災害によるIT障害 ３．安全基準等の公開状況：公開. 当該ガイドラインは厚生労働省の窓口で個別配布されている。

③安全基準等に係る３年間の取り組みについての総括（物流分野）

名称		物流分野における情報セキュリティ確保に係るガイドライン
発行主体		国土交通省
策定・見直し状況	2006年度	指針に加え，政府統一基準及び情報セキュリティ管理基準等の基準をベースとし、重点課題であるIT障害の対象脅威に対して、情報セキュリティ対策の項目及び水準を明示するものとして2006年9月に策定した。
	2007年度	2007年6月に改定された指針を踏まえ、物流分野における関係者との間で所定の見直しを実施した。指針での改定項目が現行安全基準等にて既に記載されているため、改定は不要と判断した。
	2008年度	2008年8月から9月に国土交通省政策統括参事官付（物流参事官室）で、確認・検証を実施した。現行のガイドラインに問題がないことが確認できたため、改定不要と判断した。その際、物流CEPTOAR等の関係者からの意見も併せて確認した。
概要		１．安全基準等として盛り込む具体的な対策が網羅的なものになるよう、本安全基準は、次の７つの観点毎に必要となる情報セキュリティ対策の項目及び水準を記述 ・組織・体制の整備及び資源の確保 ・情報についての対策 ・情報セキュリティ要件の明確化に基づく対策 ・情報システムについての対策 ・IT障害の観点から見た事業継続性確保のための対策 ・情報漏えい防止のための対策 ・外部委託における情報セキュリティ確保のための対策 ２．対象脅威を以下の３つとし、脅威に対応すべき対策項目を記述 ・サイバー攻撃によるIT障害 ・非意図的要因によるIT障害 ・災害によるIT障害 ３．安全基準等の公開状況：公開