電気通信事業における
情報セキュリティ確保に係る安全基準（第２版）について

２０１２年９月１２日

電気通信事業者協会

電気通信事業における情報セキュリティ確保に係る安全基準

「安全基準等」の策定のねらい

国民生活や社会経済活動の基盤である重要インフラ事業におけるIT化の進展や相互の依存関係の増大にともない、重要インフラのIT障害に対して適切な情報セキュリティ対策を強化していくことが喫緊の課題となっている。それには、事業者自らがIT障害に対して十分な対策をなしているのか自己検証しつつ、IT障害から重要インフラを防護する対策を進めることが重要である。しかし、対策の実施にあたっては、「何をすべきか」、「どの程度すべきか」の判断が困難な状況にある。

そこで、**電気通信事業分野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」という形で明示し、個々の事業者が自主的な取り組みのもと、「安全基準等」を満たす努力をし、自己検証を行える基準を策定する。**

「安全基準等」とは

以下の4種類のいずれかの形で各事業者がさまざまな判断、行為を行うにあたり、基準又は参考にするものとして策定された文書類を「安全基準等」と呼ぶ。

政府指針(※)による「安全基準等」の定義		電気通信分野の安全基準等（NISCに登録されているもの）
①	業法に基づき国が定める「強制基準」	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 【総務省】
②	業法に準じて国が定める「推奨基準」及び「ガイドライン」	情報通信ネットワーク　安全・信頼性基準 【総務省】
③	業法や国民からの期待に準じて事業者団体等が定める業界横断的な「業界標準」及び「ガイドライン」	**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【TCA　安全・信頼性協議会】**
④	業法や国民及び契約者等からの期待に応えるべく事業者自らが定める「内規」	

【※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 第3版（情報セキュリティ政策会議 H22.5.11）による定義
http://www.nisc.go.jp/active/infra/pdf/infra_pl09.pdf】

重要インフラの情報セキュリティ対策推進体制（国および電気通信分野）

国

内閣官房

情報セキュリティセンター（NISC）

情報セキュリティ政策会議の事務局として関係省庁との連携を図る

情報セキュリティ政策会議

国の情報セキュリティ政策に関する基本戦略を決定

重要インフラ専門委員会

・国の重要インフラ防護のための情報セキュリティ対策を検討

・情報セキュリティ政策会議で策定した年度計画（情報セキュリティ20XX）の推進

- **共通脅威分析検討会**　「5つの柱」の③
- **分野横断的演習検討会**　「5つの柱」の④

政府機関評価指標専門委員会

企業・個人評価指標専門委員会

情報セキュリティ政策会議が決定した基本戦略

国民を守る情報セキュリティ戦略　2010.5

「第2次情報セキュリティ基本計画※」（2009.2）を包含する、
今後4年間（2010年度～2013年度）を対象とした包括的な戦略

※2009年2月に決定された重要インフラ、政府機関、企業、個人の情報セキュリティ問題全般に関する3カ年計画

第2次重要インフラの情報セキュリティ対策に係る行動計画　2009.2

◆重要インフラについては、**10分野**で**「5つの柱」**の施策を推進

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

「5つの柱」：

①「安全基準等」の整備および浸透	安全基準作成にあたっての指針の改善、浸透度調査
②情報共有体制の強化	分野毎のセプター、セプターカウンシルの活動の充実・強化
③共通脅威分析	分野間相互依存性解析の継続、分野共通の脅威の検討
④分野横断的演習	重要インフラ分野横断的な演習の実施
⑤環境変化への対応	国民に対する広報公聴活動、国際連携の推進等

情報セキュリティ2010　2010.7

2010年度及び2011年度に実施する具体的な取組

セプターカウンシル　「5つの柱」の②　各分野のセプター間の情報共有

- サイバー攻撃対応力向上WG
- 暗号の2010年問題ｽﾀﾃﾞｨWG
- …

電気通信分野

総務省

- **情報流通行政局 情報セキュリティ対策室**
- **総合通信基盤局 データ通信課 電気通信技術システム課**

- **電気通信事業者協会（TCA）**
  - **安全・信頼性協議会**
    - **安全基準等検討WG【参考】**　「5つの柱」の①
  - **Telecom-ISAC Japan（データ通信協会）**

・電気通信分野の「情報共有・分析機能（CEPTOAR: Capability for Engineering of Protection, Technical Operation, Analysis and Response）」

ティーセプター　「5つの柱」の②

重要インフラ10分野

…

「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」の見直しの経緯

内閣官房情報セキュリティセンター（NISC）

＜情報セキュリティ政策会議＞

第一次情報セキュリティ基本計画　H18.2

セキュアジャパン2006
H18.6

セキュアジャパン2007
H19.6

セキュアジャパン2008
H20.6

第二次情報セキュリティ基本計画　H21.2

セキュアジャパン2009
H21.6

＜重要インフラ専門委員会＞

重要インフラの情報セキュリティ対策に係る「安全基準等」策定にあたっての指針　（H18.2制定）

重要インフラの情報セキュリティ対策に係る「安全基準等」策定にあたっての指針　第2版　（H19.6改定）

指針の改定はせず、見直し検討時に得られた知見を「参考事項」として周知　（H20.3）

重要インフラの情報セキュリティ対策に係る「安全基準等」策定にあたっての指針　第3版　（H22.5改定）

電気通信業界

＜ISeCT：電気通信分野における情報セキュリティ対策協議会＞

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）策定（H18.9）

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）見直し検討（H19.9）

自主点検・監査、冗長化、負荷分散等の規定状況を検証（⇒改訂不要と判断）

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1.1版）改訂（H21.3）

水道分野との相互依存性、関連規定類の変更に伴う改訂を実施

＜TCA：安全・信頼性協議会＞ ※ 平成21年度より移管

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1.1版）（H21.4）

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2版）（H22.12）

政府行動計画に基づく見直し、脅威や環境変化（IPv6、暗号危殆化等）への対応等のための改訂を実施（⇒P.6）

「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２版）」の構成の考え方

「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」では、「６つの観点」及び「４つの脅威等」に基づき、以下のとおりセキュリティ対策の基準を規定している。（※）

凡例　“○”：セキュリティ対策の記述あり　“－”：セキュリティ対策の記述なし

６つの観点 ／ ４つの脅威等	１章 組織・体制の整備及び資源の確保	２章 情報についての対策	３章 情報セキュリティ要件の明確化に基づく対策	４章 情報システムについての対策	５章 IT障害の観点から見た事業継続性確保のための対策	６章 外部委託における情報セキュリティ確保のための対策
サイバー攻撃（DDoS攻撃等）	○	○	○	－	○	－
ネットワーク輻そう（企画型輻そう、災害型輻そう）	○	－	－	○	○	－
故障、災害等	○	－	－	○	○	－
重要情報漏えい（設備情報等）	○	○	○	－	○	○
共通（一般的対策）	○	○	○	○	○	○

【※ 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2版（安全・信頼性協議会 平成22年12月10日）「Ⅲ. 具体的な対策」より
http://www.tca.or.jp/information/pdf/networksecurity/anzenkijun2.pdf】

「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2版）」の改訂のポイント

- 政府は『「安全基準等」策定にあたっての指針（以下　政府指針）』の改訂を決定　（情報セキュリティ政策会議2010.5.11）
- 政府指針の改訂を受け、電気通信業界の安全基準である『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1.1版）』に対する見直し作業を、安全・信頼性協議会下の安全基準検討WGにて実施し、「第2版」として2010年12月10日に策定
- 改訂にあたっては、特に、安全基準の内容に深く関わる以下の「＃1」「＃2」を中心に検討

○政府指針第2版⇒第3版の主な変更点（全48項目）※

#	主な変更ポイント	内容
1	政府の第2次行動計画との整合性確保	●重要インフラサービス、重要システム、検証レベル、サービスレベルといった新たな観点を追加 ●IT障害を引き起こす脅威の例示を充実（新型インフル、他分野の障害からの波及等）
2	重点項目の追加	●重点項目を2つ追加（対策項目が「4つの柱と3つの重点項目」から「4つの柱と5つの重点項目」へ） ＜追加された重点項目＞： （1）IT障害発生時の利用者の対応のための情報の提供等の対策 重要インフラサービスの停止状況・復旧等の情報の適時の提供の方策の明示、重要インフラ事業者の情報セキュリティ対策に関する取組みについての対外的な説明 （2）ITに係る環境変化に伴う脅威のための対策 暗号の危殆化や、IPv6への移行等、情報システムの基盤を支える技術等の環境変化について、IT障害発生の未然防止のための適切な対策の検討
3	内容の具体化	●事業者等の自主的な取組みに資する項目を充実化 （1）指針の記載事項を「要検討事項」と「参考事項」に分類 ＜追加された参考事項＞：「情報セキュリティ人材の育成等」、「外部監査等による情報セキュリティ対策の評価」 （2）指針本編とは別に「対策編」（平成22年7月30日重要インフラ専門委員会決定）を作成し、対策項目の具体化を例示
4	指針見直しサイクルの変更	●指針の改訂と、事業者のPDCAサイクルとの整合性確保 （1）指針の改訂は、原則として3年に1度（従来は毎年見直し） （2）1年毎、及び必要に応じて適時に、指針の分析・検証を行い、その結果を必要に応じて指針の追補版として周知

【※ 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 第3版（情報セキュリティ政策会議 H22.5.11）より
http://www.nisc.go.jp/active/infra/pdf/infra_pl09.pdf】

【参考】 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2版）目次構成

目次

【参考】TCA 安全・信頼性協議会 安全基準検討WG

情報セキュリティ政策会議において決定する「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」に基づいて、「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」の見直しを行うための専門的な検討を行う。

参加企業一覧(※)

日本電信電話株式会社（主査）
KDDI株式会社（副主査）
ソフトバンクテレコム株式会社
スカパーJSAT株式会社
株式会社ケイ・オプティコム
東京テレメッセージ株式会社
中部テレコミュニケーション株式会社
ソフトバンクモバイル株式会社
株式会社NTTドコモ
株式会社ウィルコム
近鉄ケーブルネットワーク株式会社
株式会社ジュピターテレコム
東日本電信電話株式会社
西日本電信電話株式会社
NTTコミュニケーションズ株式会社
フュージョン・コミュニケーションズ株式会社
イー・アクセス株式会社

【※ TCA 安全・信頼性協議会 http://www.tca.or.jp/information/anshinkyou.html 】