８．安全管理措置（ガイドライン第１１条）

８－１．技術的保護措置

［ガイドライン］

第11条　電気通信事業者は、個人情報へのアクセスの管理、個人情報の持出し手段の制限、外部からの不正なアクセスの防止のための措置その他の個人情報の漏えい、滅失又はき損（以下「漏えい等」という。）の防止その他の個人情報の安全管理のために必要かつ適切な措置（以下「安全管理措置」という。）を講ずるものとする。

第2項　電気通信事業者は、安全管理措置を講ずるに当たっては、情報通信ネットワーク安全・信頼性基準（昭和62年郵政省告示第73号）等の基準を活用するものとする。

（第11条の解説）

(1) 本条は、電気通信事業者が、個人情報を取り扱うに当たり、個人情報を安全に管理するための措置を講ずるものとすることを規定したものである。

安全管理措置は、技術的保護措置及び組織的保護措置に大きく分類され、その双方を適切に実施することが必要である。

その際には、本人の個人情報が漏えい等した場合に本人に与える影響等を考慮し、通信の秘密に該当するもの等、より重大な影響を及ぼす可能性がある個人情報については、より厳格に取り扱うこととする等の措置をとることが適当である。

なお、例えば、不特定多数者が書店で随時に購入可能な名簿で、電気通信事業者において全く加工をしていないものについては、個人の権利利益を侵害するおそれは低いと考えられることから、それらを処分するために文書裁断機等による処理を行わずに廃棄し、又は廃品回収に出したとしても、電気通信事業者の安全管理措置の義務違反にはならない。

電気通信事業者は、不特定多数の者が書店で随時に購入可能な電話番号簿で、当該事業者が全く加工していないものを、処分するために溶解や文書裁断機等による処理を行わず破棄し、又は廃品回収に出しても差支えない。

しかし、電話番号簿の発行に関わる電気通信事業者にとって、当該電話番号簿は、自己が保有する個人情報を用いたものであり、その事業者が廃棄処分する場合には、文書裁断や溶解等の処理を行った上で処分すべきである。

電話番号簿自体に個人に関する書き込みをしている場合には、加工したものとみなすべきである。電話をかけた先にチェックを付けたような場合も同様に加工したものとみなすべきである。

８－１－１．アクセスの管理

（第11条の解説）
(2) 技術的保護措置とは、・・・
① 個人情報へのアクセスの管理（アクセス権限者の限定（異動・退職した社員のアカウントを直ちに無効にする等の措置を含む。）、アクセス状況の監視体制（アクセスログの長期保存等）、パスワードの定期的変更、入退室管理等）

個人情報へのアクセスの管理として、具体的には次のような措置をとることとする。

ア．アクセス権限者の限定

電気通信事業者は、個人情報の漏えい及び不正使用を防止するために、個人情報へのアクセス権限を必要最小限とすることとする。

また、従業者(注)が異動・退職等によりアクセス権限が失われたときは、直ちにアカウントを無効にするとともに、長期にアクセス権限が放置されることを防止するために有効期間を設定する等定期的に有効確認を行うこととする。

さらに、委託先の従業者や再委託先等の従業者に対し、アクセスを認める場合にも、従業者と同様に、アクセス権限の限定や有効確認等を行う必要がある。

（注）「従業者」とは、電気通信事業者の組織内にあって直接間接に事業者の業務に従事している者をいい、電気通信事業者との間の雇用関係の有無は問わないので、雇用関係にある従業員（正社員、契約社員、嘱託社員、パートタイマー、アルバイト等）及び役員（取締役、執行役、監査役、理事、監事等）のほか派遣労働者も含まれる。

＜措置の例＞

- 従業者の情報とアカウントを一元的に管理し、人事異動や組織変更等がタイムリーに反映されるシステムの導入（アカウントの重複や削除漏れを防止）
- アクセスのためのＩＣカード等の認証デバイスシステムの導入

イ．アクセス状況の監視体制

電気通信事業者は、個人情報の漏えい及び不正使用を防止するために、個人情報へのアクセス者が特定できるアクセス履歴（使用者、使用・エラー履歴、不規則利用等）を残し、これを監視するとともに、必要な範囲内でアクセスログの保存期間を定めて、保存することとする。

＜措置の例＞

- アクセス時ステータスが確認可能なＩＣカード等の認証システムの導入
- アクセス記録の長期（又は無期限）保存
- 不正アクセスを遮断可能な監視ツール等の導入

- 不正アクセスへの防御性を高めるためのネットワークのシステムの脆弱性の定期的な調査の実施
- 不正侵入検知装置（ＩＤＳ）等の導入
- 個人情報を取り扱うシステムへのインターネット経由のアクセスの制限（セキュリティーを確保のためのシステムの導入やアクセスの規制等）

ウ. パスワードの定期的変更

電気通信事業者は、個人情報の漏えい及び不正使用を防止するために、個人情報へのアクセスが可能なシステム又は端末に対するパスワードについて有効期間を設定する等により定期的に有効確認を行うこととする。

＜措置の例＞

- パスワードの有効期間（１～３ヶ月）を定め、期限までに変更を促し、必ず変更させるようなシステムの導入

エ. 入退室管理

電気通信事業者は、個人情報の漏えい及び不正使用を防止するために、個人情報を取り扱う敷地、ビル、事務室、設備等の設置環境に関して、その取り扱う個人情報の内容、形態、規模に応じて区分毎の入退室権限を設定するとともに各種管理システム等を通じて入退室管理を行うこととする。

＜措置の例＞

- ビルや部屋、端末、ネットワーク、ファイル等、個人情報に対するあらゆるレベルのアクセスについて、ＩＣカード等の認証デバイスを用いて管理し、すべての証跡が個人を特定できる形式で必要な期間保存されるシステムの導入

○（好ましい事例）

事例８－１　社員の情報とアカウントを一元的に管理し、人事異動や組織変更等がタイムリーに反映される仕組みを導入する等して、アカウントの重複や削除漏れを防止するよう対処している。

事例８－２　パスワードの有効期間（１～３ヶ月）を定め、システム上期限までに変更を促して必ず変更させるような仕組みを導入している。

事例８－３　ビルや部屋、端末、ネットワーク、ファイル等、個人情報に対するあらゆるレベルのアクセスについて、ＩＣカード等の認証デバイスを用いて管理し、すべての証

跡が個人を特定できる形式で必要な期間保存される仕組みを導入している。

事例８－４　不正なアクセスに対し、監視ツール等を利用して監視するとともにそうした疑いのある不正なアクセスを遮断している。

事例８－５　不正なアクセスを防ぐため、ネットワークやシステムの脆弱性を定期的に調査して、防御性を高めるように対処している。

事例８－６　不正侵入検知装置（ＩＤＳ）等を活用することにより、不正パケットを常時監視し、内部からの情報漏えいを防止している。

事例８－７　コンピューターウィルス・ワームのチェックツール及びそのパターンファイルを常に最新に保ち、感染状況等を常時監視して迅速に対策を講じることができる体制を構築する等して、個人情報が漏えいしないよう対処している。

事例８－８　インターネット経由で個人情報を取り扱うシステムにアクセスすることについて、セキュリティーを確保するとともにそのアクセスを適切に管理している。

×（好ましくない事例）

事例８－９　個人情報へのアクセスログを保存しない、又は、保存したとしても数日で削除されてしまう。

８－１－２．持出し手段の制限

（第11条の解説）
⑵ 技術的保護措置とは、・・・
② 個人情報の持出し手段の制限（みだりに外部記録媒体へ記録することの禁止、社内と社外との間の電子メールの監視を社内規則等に規定した上で行うこと等）

個人情報の持出し手段の制限として、具体的には次のような措置をとることとする。

ア．みだりに外部記録媒体へ記録することの禁止

電気通信事業者は、従業者が業務に必要な範囲を超えて個人情報をパソコンや外部記録媒体（従業者が持ち込んだ媒体を含む。）に記録することを禁止することとする。

＜措置の例＞

- 個人情報を外部記録媒体へ記録するパソコン上の操作（個人情報データベースからのダウンロードやファイルサーバ等からのコピー及び印刷等。）について常時監視システムを導入する。
- 個人情報へのアクセスが可能なシステム又はパソコンに、ＵＳＢメモリ、ＦＤドライブ等の外部記録媒体の使用を限定するソフトウェアを導入する。
- 個人情報へのアクセスが可能なシステム又はパソコンに、ＵＳＢメモリ、ＦＤドライブ等の外部記録媒体の接続装置を装着しない。
- 業務上の必要性からやむをえず個人情報を外部記録媒体に記録する場合は、個人情報を分割し組み合わせないと復元できず、かつ、その分割したそれぞれのデータ単独では元の情報を全く復元できない仕組み等外部記録媒体の紛失等に対して適切な対処を施す。
- サーバに格納した個人情報に、パソコンや携帯電話等の端末からアクセスしても、それらの端末には個人情報が残らないシステムを導入する。

イ．パソコンの持出し制限

電気通信事業者は、個人情報を記録したパソコンの持出しに関する社内規則（持出しの許されるパソコンの特定、起動時のパスワード設定等）を定め、適正に管理することとする。

ウ．私物パソコン等の使用の制限

従業者の私物のパソコンや外部記録を業務に使用することを原則として禁止することとし、やむを得ず私物パソコン等の使用を認める場合には、会社の業

務用のパソコン等と同様の安全管理措置が講じられていることを厳重に確認することとする。

エ．電子メール使用ルール

個人情報を外部に漏えい等する危険を避けるための電子メールの使用ルールを定めるとともに、メールフィルタリングや送信メールのログの記録化等、これを担保するシステムを導入するなどの対策を講じることとする。

＜電子メールの使用ルールの例＞

- 私用メールは一切禁止する。
- 社外への複数配信の禁止（複数配信する必要がある場合には、適切な取扱いを図るよう十分注意しつつＢＣＣやメール配信システムを使用）
- 携帯電話や他のパソコンへの自動転送禁止
- 個人アドレスへの業務メールの転送禁止
- 個人情報を含む電子メールの送信時の、暗号化やパスワードの設定の必須化
- 社外メール配信時の複数従業者によるチェック

オ．社内と社外の間の電子メール監視

電気通信事業者は、必要に応じ、あらかじめ社内規則等に規定した上で、従業者の社内と社外との間の電子メールを監視するなどの措置を講じることとする。

ただし、その場合は従業者のプライバシー保護に十分留意するものとする。また、雇用管理に関する個人情報の取扱いに関する重要事項を定めるときは、あらかじめ労働組合等に通知し、必要に応じて、協議を行うことが望ましい。また、その規定を定めたときは、従業者に周知することが望ましい。

カ．消去の徹底

電気通信事業者は、個人情報を記録した媒体（パソコン、外部記録媒体、紙等）を廃棄する場合は、個人情報の消去を徹底することとする。

○（好ましい事例）

事例８－１０　個人情報を外部記録媒体へ記録するパソコン上の操作（個人情報データベースからのダウンロードやファイルサーバ等からのコピー及び印刷等。）について常時監視することで、個人情報が漏えいすることを防止している。

事例８－１１　業務上の必要性からやむをえず個人情報を外部記録媒体に記録する場合は、個人情報を分割し組み合わせないと復元できず、かつ、その分割したそれぞれのデ

ータ単独では元の情報を全く復元できない仕組みを採用するなど外部記録媒体の紛失等に対して適切な対処を施している。

事例８－１２　サーバに格納した個人情報に、パソコンや携帯電話等の端末からアクセスしても、それらの端末には個人情報が残らない仕組みを導入することで、故意の場合のみならず、本人が意図しないにもかかわらず自己の端末に情報が蓄積される形態も含め、個人情報の外部持出しを防止している。

事例８－１３　不正侵入検知装置（ＩＤＳ）等を設置することにより、情報漏えいに繋がる通信（社内で監視しているメールサーバを経由しない通信等(注)）を適切に検知し、対処を行える仕組みを設けている。

(注)社内で監視しているメールサーバを経由しない通信等

インターネット上のWebメールを利用したメール通信、外部とのチャットやメッセンジャ通信、ウイルスやスパイウェアの通信等をいう。

事例８－１４　個人情報へのアクセスが可能なシステム又はパソコンに、ＵＳＢメモリ、ＦＤドライブ等の外部記録媒体の使用を限定するソフトウェアを導入している。

×（好ましくない事例）

事例８－１５　個人情報が含まれたデータベースについて、外部記憶装置(端末も含む)にダウンロードすることなく参照できるにもかかわらず、データを外部記録装置に記録する。

事例８－１６　個人情報が含まれたデータベースから必要な情報のみを抽出する機能があるにもかかわらず、すべてのデータを外部記憶装置に記録する。

事例８－１７　個人情報が含まれたデータについて、必要以上の部数をプリントアウトする。

８－１－３．外部からの不正アクセスの防止

（第11条の解説）
⑵ 技術的保護措置とは、･･･
③ 外部からの不正アクセスの防止のための措置（ファイアウォールの設置等）

外部からの不正アクセスの防止のための措置として、具体的には次のような措置をとることとする。

ア．ファイアウォールの設置

電気通信事業者は、不正アクセスを防止するために、ネットワークに接続する情報システムには、ファイアウォール、不正侵入検知装置（ＩＤＳ）等の不正アクセス防止機器を設置するなどの対策を講じることとする。

イ．Ｗｉｎｎｙ等ファイル交換ソフト等の使用制限

Ｗｉｎｎｙ等ファイル交換ソフトや、会社が安全性を確認したソフトウェア以外のソフトを、業務用パソコンにインストールすることや使用することを禁止することとし、定期的又は恒常的に監視を行うこととする。

○（好ましい事例）

事例８－１８　インターネットに接続する情報システムに対し、最新のセキュリティー情報に基づいてファイアウォール、不正侵入検知装置（ＩＤＳ）等の設定を常に適正に保ち、常時監視できるような仕組みを導入することにより個人情報の漏えい等を防止している。

８－１－４．情報セキュリティーに関する基準の活用

（第11条の解説）
⑵ 技術的保護措置とは、・・・
（①～③）などの内部からの情報漏えい及び外部からの不正アクセスの双方を防止するための物理的・技術的措置を指すが、上記①～③のほか、情報通信ネットワーク安全・信頼性基準その他の国内・国際の公表されている情報セキュリティーに関する基準を活用して、各電気通信事業者が個人情報の取扱状況に応じた適切な内部規程・マニュアルを策定し、実施することが必要である。

各電気通信事業者が適切な内部規程・マニュアルを策定し、実施することとは、具体的には、電気通信事業者は、必要に応じ、国内外の工業標準化の促進を活動目的とした団体等から発行されている情報セキュリティーに関する基準を活用して、適切な内部規程・マニュアルを策定し、実施することとする。

８－１－５．技術基準の適合維持義務

（第11条の解説）
⑵ 技術的保護措置とは、・・・
なお、事業用電気通信設備（電気通信回線設備及び基礎的電気通信役務を提供する電気通信事業の用に供する電気通信設備）に関する技術的保護措置については、事業用電気通信設備を設置する電気通信事業者に対し、事業用電気通信設備規則（昭和60年郵政省令第30号）に定める技術基準の適合維持義務が課されている（電気通信事業法第41条）ことにも留意する必要がある。

電気通信事業者の保有する個人情報を格納する装置が、電気通信事業法第４１条に定める事業用電気通信設備に該当する場合は、当該装置が事業用電気通信設備規則（昭和６０年郵政省令第３０号）の定める技術基準を満たさないことによって損傷又は破壊されることのないようにすることとする。

８－２．組織的保護措置

８－２－１．従業者・委託先の責任と権限の明確化

（第11条の解説）
⑶ 組織的保護措置とは、
① 安全管理に関する従業者･委託先の責任と権限を明確に定めること
（･･･などの人的･組織的な措置を指すが、これらの事項については、次条及び第13条に詳細な規定がおかれているので、それらの規定を参照されたい。）

安全管理に関する従業者・委託先の責任と権限を明確に定めることとは、具体的には、次のような措置をとることとする。

ア．従業者の責任と権限の明確化

電気通信事業者は、その雇用する従業者に対しては就業規則において、雇用関係にない従業者に対してはその雇用者との契約において、従業者の責任を明確にすることとする。また、内部規程中に個人情報を取り扱うことができる従業者を決める権限者を明らかにすることとする。

イ．委託先の責任と権限の明確化

電気通信事業者は、委託先に業務を委託する契約中に、個人情報の保護・秘密保持に関する規定を置くこととする。

８－２－２．内部規程・マニュアルの策定と監査

（第11条の解説）
(3) 組織的保護措置とは、･･･
② 安全管理に関する内部規程･マニュアルを定め、それらを従業者に遵守させるとととともに、その遵守の状況について適切な監査を行うこと
（･･･などの人的･組織的な措置を指すが、これらの事項については、次条及び第13条に詳細な規定がおかれているので、それらの規定を参照されたい。）

安全管理に関する内部規程・マニュアルを定め、それらを従業者に遵守させるととともに、その遵守の状況について適切な監査を行うこととは、具体的には、次のような措置をとることとする。

ア．安全管理に関する内部規程・マニュアルの策定

電気通信事業者は、事業内容、その取り扱う個人情報の内容、形態、規模に応じて安全管理に関する内部規程・マニュアルを策定することとする。

なお内部規程・マニュアルには、個人情報の適正な取扱いの確保に必要な体制に関する規定、物理環境に関する規定、情報システムに関する規定、インシデントに関する規定、監査に関する規定等を置くこととする。

イ．安全管理に関する適切な監査

電気通信事業者は、安全管理に関して定めた内部規程・マニュアルの遵守状況を、自己診断、内部監査、外部監査等のいずれか又は各種監査方法を組み合わせ、定期的かつ効率的に監査することとする。

８－２－３．従業者・委託先との秘密保持契約締結

（第11条の解説）
⑶ 組織的保護措置とは、･･･
③ 従業者･委託先と秘密保持契約を締結すること等により安全管理について従業者･委託先を適切に監督すること
（･･･などの人的･組織的な措置を指すが、これらの事項については、次条及び第13条に詳細な規定がおかれているので、それらの規定を参照されたい。）

従業者･委託先と秘密保持契約を締結すること等により安全管理について従業者・委託先を適切に監督することとは、具体的には、次のような措置をとることとする。

ア．従業者との内部規程・マニュアル遵守の誓約

電気通信事業者は、従業者に対し、その就労の開始時において、安全管理に関する従業者の責任と権限を明確にした内部規程・マニュアルについて十分な説明又は教育・訓練を施したうえで、その遵守を誓約させることとする。

イ．委託先との秘密保持契約の締結

電気通信事業者は、委託先に業務を委託する契約中に、委託先に委ねる個人情報の内容、形態、規模に応じて、個人情報の保護・秘密保持に関する規定を置くこととする。

８－２－４．教育研修

（第11条の解説）
(3) 組織的安全管理措置とは、･･･
④ 安全管理について従業者に対し必要な教育研修を行うこと
などの人的･組織的な措置を指すが、これらの事項については、次条及び第13条に詳細な規定がおかれているので、それらの規定を参照されたい。

安全管理について従業者に対し必要な教育研修を行うこととは、具体的には、次のような措置をとることとする。

ア．就労の開始時における個人情報保護に関する教育研修

電気通信事業者は、従業者に対し、就労の開始時に個人情報保護に関する教育研修を実施するものとし、当該教育研修の実施にあたっては、教育研修の実施効果及び監査等の目的を考慮して、教育研修の体系、実施計画を立案するものとする。

イ．年１回程度の教育研修

電気通信事業者は、すべての従業者に対し、少なくとも年１回程度の個人情報の保護に関する教育研修を実施するものとする。（９－１－２．従業者への教育研修参照のこと）

８－３．持出時の安全管理措置を講じる際の考え方等

（第11条の解説）

(4) 個人情報をパーソナルコンピュータ、外部記録媒体等で社外に持ち出す場合には、パーソナルコンピュータ等が紛失、盗難することによって個人情報が漏えいするリスクが問題になる。そのため、リスクに備え、持ち出した個人情報の安全性が確保されるよう措置を講じる必要がある。

持ち出した個人情報の安全性を確保するためには、リスクの評価、リスクに対応するために必要とされる措置の検討・決定、決定した措置の適切な運用という手順で対策を行うことが必要である。

まず、リスクの評価に当たっては、個人情報の持出し時に想定される具体的なリスクを網羅的に評価することが必要である。

次に、措置の検討・決定に当たっては、技術的保護措置と組織的保護措置との双方についての検討が必要である。技術的保護措置については、個々の技術的保護措置の特性を把握しリスクに適切に対応できる具体的な措置を選択することが必要である。その際には、複数の措置（パーソナルコンピュータの起動時等での個人認証、外部媒体の接続制限、ウイルス侵入による情報漏えいに備えた最新のセキュリティ一水準維持、高度な暗号化措置及び適切な復号鍵の管理、通信経路の暗号化、社内サーバにおける端末認証等）を適切に組み合わせることが重要である。また、講じようとする技術的保護措置の技術的に最も弱い部分を確認すること、利便性、安全性及び導入コストを勘案することが重要である。組織的保護措置については、技術的保護措置が適切に運用されるよう、安全管理措置に関する内部規程の整備や従業員への周知等を行うことが必要である。

さらに、決定した措置の適切な運用に当たっては、定期的な監査や従業員に対する定期的な研修の実施等に努めるとともに、リスクの状況について適宜に見直しを行うことが必要である。

なお、技術的保護措置を講じていたとしても、業務上必要な分量や種類を超えた個人情報を持ち出すことは避け、必要最低限の範囲にするべきである。また、漏えいした場合に本人の権利利益の侵害の程度が大きい個人情報については、安易に外部に持ち出さないこととするとともに、持ち出す必要がある場合は、より高い安全性が確保されるような技術的保護措置を講ずることが必要である。

個人情報の入ったパーソナルコンピュータや外部記録媒体等を社外へ持ち出す場合には、パーソナルコンピュータ等が紛失、盗難することにより個人情報が漏えいするリスクがあることから、次のような点に留意して、持ち出した個人情報の安全性が確保されるよう措置を講じる必要がある。

① リスクの評価では、持ち出す個人情報の種類、内容やその分量、持ち出す従業者の範囲や持ち出す方法、社内での管理状況等の関連する状況を踏まえ、ど

のようなリスクがどこで生じるのか等、個人情報を社外へ持ち出した場合に想定される具体的なリスクを網羅的に整理し評価することが必要である。

② 「講じようとする技術的保護措置の技術的に最も弱い部分を確認すること」とは、導入コストをかけて部分的にセキュリティー強度を強固にしても、相対的にセキュリティー強度の弱い部分があれば、その部分から問題が生ずるおそれがあるため、技術的にセキュリティー強度の最も弱い部分を把握し、その部分に対応する措置が十分なものなのかを検討することが必要であるとの趣旨である。

③ 「利便性、安全性及び導入コストを勘案することが重要である」とは、措置を講ずることによる利便性への影響及び導入コストと、持ち出された個人情報の安全性の双方を勘案することが重要であり、一般に、利便性や導入コストと安全性とはトレードオフの関係にあるため、評価したリスクについて、利便性や導入コストと安全性の双方のバランスを判断して適切な措置を決定することが必要であるとの趣旨である。

④ 決定した措置が適切に運用されることを確実にするために、内部規程等が遵守されているかどうかの定期的な監査や、従業員に対する定期的な研修の実施等に努めることが必要である。また、リスク評価や必要とされる措置について適宜に見直しを行うことが必要である。

⑤ 個人情報を持ち出す場合には、適切な技術的保護措置を講じているかどうかには拘らず、紛失や盗難に遭わないように、パーソナルコンピュータ等が適切に管理されるようにすることや、持ち出す個人情報は、業務上必要最低限の範囲にすることが必要である。

⑥ 「漏えいした場合に本人の権利利益の侵害の程度が大きい個人情報」については、安易に外部に持ち出さないことが必要であるが、これらの個人情報の例には、通信の秘密に該当する情報や銀行口座番号、クレジットカード情報等のほか、ガイドライン第４条第２項で取得を制限しているいわゆるセンシティブ情報が含まれる。

ワイヤレスブロードバンド環境の進展や持ち出した情報資産の安全性を確保可能とするサービスの登場により、個人情報をパーソナルコンピュータや外部記憶媒体等で社外に持ち出す場合に、漏えいが発生した場合でも本人への二次被害が生じないよう適切な技術的保護措置を講じることも可能になってきている。

なお、パーソナルコンピュータや外部記憶媒体等の紛失等に際し、漏えい等の発生した個人情報に対して適切な技術的保護措置が講じられていた場合には、本人への通知、公表、総務省への報告に関する手続を簡略化することが可能と

されている。（ガイドライン２２条参照）

個人情報をパーソナルコンピュータや外部記録媒体等で社外に持ち出す場合に想定されるリスクと技術的対応策、求められる安全管理措置については、総務省「利用者視点を踏まえたＩＣＴサービスに係る諸問題に関する研究会」で検討され第二次提言として公表されている。（平成２２年５月）

具体的な安全管理措置の取組については、参考資料３－２総務省「利用者視点を踏まえたＩＣＴサービスに係る諸問題に関する研究会」第二次提言の抜粋(注)を参照されたい。

（注）参考資料３－２は総務省「利用者視点を踏まえたICTサービスに係る諸問題に関する研究会」第二次提言から次の部分を抜粋している。

Ⅲ　安全管理措置に関する検討について

2. 想定されるリスクと技術的対応策

3. 求められる安全管理措置