NISC National Information Security Center

「政府機関の情報セキュリティ対策のための統一基準(第4版)」改訂の概要について

2009年2月

内閣官房情報セキュリティセンター

目次

1. 統一基準第4版見直しの考え方

基準外要因の確認 （リスク分析をする。必要なら、対応として許容リスクも見直す。）

- A. 政府内要件の変化への対応
  - 情報セキュリティ対策に関係する行政事務要件について、その目標達成のために統一基準改訂の必要があれば、改訂方法を決定する
  - 第二次基本計画の検討内容について、その目標達成のために統一基準改訂の必要性があれば、改訂方法を決定する
- B. 政府外環境の変化への対応
  - 世の中で起きた事件事故についての検証 （政府機関内で発生したと仮定して以下の検証をする）
    - 原因が基準違反とならなければ改訂必要
    - 原因が基準違反となるならば改訂不要 （ただし、「遵守事項や解説見直し」の検討材料とする。）
  - 周知された注意喚起についての検証
    - 基準で対応していない潜在的脅威について、顕在化の可能性が高まっていればリスク対応する

基準のすべての遵守事項の内容確認 （改訂で許容リスクを変化させないことを原則とする。）

- C. 実務に則した遵守事項の見直し
  - 運用の障害又は困難（冗長な対策、難解な文章など）の可能性があれば、それを解消・軽減するための修正をする
    - 遵守事項の達成目標を変えずに表現（主体・客体・実施策、条件等）を変更する
    - 遵守事項の達成目標を変える（環境などの変化により許容リスクを保つために達成目標を変える）
- D. 運用改善のための解説の見直し
    - 誤解のない表現、理解度の増す表現の追加・修正
- E. 文言の改善
    - 表現漏れの改善、誤字脱字の修正

2. 統一基準第4版見直し結果

基準外要因

- A. 政府内要件の変化への対応
  - 最高情報セキュリティアドバイザーの設置の義務化　→A1
- B. 政府外環境の変化への対応
  - ウェブの閲覧・情報送信時の危険性　→B1、B2
  - 電子メールのボット被害　→B3
  - 無線LANの暗号方式の脆弱性　→B4

遵守事項の見直し

- C. 実務に則した遵守事項の見直し
  - 基準見直し時の観点の明確化（基本編と情報システム編への分割）　→C1
  - 情報の格付け及び取扱制限に関する規程の取り込み（DM3-01の取り込み）　→C2
  - チェックリスト随時記入による運用改善（重複事項の統合）　→C3～C8
  - 文書整備計画の簡便化（文書整備事項の集約）　→C9～C15
  - 対策内容の明確化（表現（主語・述語・客体、条件等）を変更）　→C16～C20
- D. 運用改善のための解説の見直し
- E. 文言の改善

遵守事項の見直しにより、遵守事項数は　第3版471項→第4版426項（▲45）となった。

3. 統一基準第4版改訂

A. 政府内要件の変化への対応
B. 政府外環境の変化への対応
C. 実務に則した遵守事項の見直し
D. 運用改善のための解説の見直し
E. 文言の改善

A. 政府内要件の変化への対応

修正・追加

■ 各府省庁における最高情報セキュリティアドバイザーの設置の義務化

経緯

・現在検討中の第2次基本計画検討委員会において、構成委員から指摘されているとおり、政府機関の情報セキュリティ対策におけるPDCAサイクルの実効性を強化するため、

－「情報セキュリティに係る年次報告書」の客観性を確保する観点から、最高情報セキュリティアドバイザーが本報告書の作成に実質的に関与する

－各政府機関の最高情報セキュリティアドバイザーが集まる会議体を設置し、本報告書の比較・評価等を行うとともに、得られた知見の共有やフィードバックを積極的に図ることとする

等、最高情報セキュリティアドバイザーの積極的な活用を行うこととしている。

・これを受けて、各府省庁においてこれまで任意であった最高情報セキュリティアドバイザーの設置を義務化するものである。

A1 **■最高情報セキュリティアドバイザーの設置**

・最高情報セキュリティ責任者は、情報セキュリティに関する専門的な知識及び経験を有した専門家を最高情報セキュリティアドバイザーとして置くこと。 1.2.1.1組織・体制の整備(8)(a)【2.1.1(1)(c)】 **修正**

・最高情報セキュリティ責任者、情報セキュリティ対策等の実施において最高情報セキュリティアドバイザーが行う業務の内容について定めること。 1.2.1.1組織・体制の整備(8)(b) **追加**

本書における遵守事項項番の表記方法：

【 】内は第3版の項番です。

以後のスライドで同じ。

B. 政府外環境の変化への対応

追加

■ ウェブクライアントのセキュリティ設定を求める基本遵守事項の追加

経緯

・ホームページへの攻撃が急増しており、閲覧により電子計算機に意図せず悪意のあるソフトウェアが実行される等、ウェブクライアントを介した情報漏えい等の被害が増加しつつある。

B1

■ウェブクライアントの安全な設定

・行政事務従事者は、情報セキュリティの確保がなされるよう適切にウェブクライアントのセキュリティ設定をすることを基本遵守事項に追加。 2.2.3.2ウェブ(2)(a)

■ ウェブサイトへの情報送信時の安全確認を求める基本遵守事項の追加

経緯

・ウェブメールを利用する際に個人の識別コード等を入力する等、閲覧しているウェブサイトで表示されるフォームに重要な情報を入力し、送信する機会が増加しつつある。

・このような現状を踏まえると、行政事務従事者が業務上の必要性から、閲覧しているウェブサイトに表示されるフォームに、要機密情報を入力・送信する機会が増加していることが想定されるが、その際に必要な対策を行わなければ、要機密情報の漏えい等の情報セキュリティ事故の発生の恐れがある。

・このため、ウェブサイトに表示されるフォームに要機密情報を入力・送信する場合の情報セキュリティ対策について、新たに遵守事項として定めるものである。

B2

■ウェブサイトに表示されるフォームに要機密情報を入力・送信する場合の安全確認

・行政事務従事者は、閲覧しているウェブサイトに表示されるフォームに要機密情報を入力して送信する場合には、以下の事項を確認することを基本遵守事項に追加。 2.2.3.2ウェブ(2)(c)

（ア）送信内容が暗号化されること。

（イ）当該ウェブサイトが送信先として想定している組織のものであること。

B. 政府外環境の変化への対応

修正

■ 電子メールサーバに関する脅威の増加による強化遵守事項の見直し

経緯

・脅威の増加と対策の実現可能性を考慮した上で、強化遵守事項のうち、基本遵守事項とすることが相当である遵守事項を見直す。

B3 **■電子メールの送信時認証を基本遵守事項に変更する**

・ボットによる電子メールの送信対策として 2.2.3.1電子メール(1)(b)【5.3.2(1)(b)】を強化遵守事項から基本遵守事項に変更。

■ 無線LAN環境を構築する場合の基本遵守事項の明確化

経緯

・無線LAN通信における暗号方式の脆弱性の顕在化。

B4 **■無線LAN環境における通信内容の暗号化について、遵守事項及び解説の修正**

・2.2.4.2府省庁内通信回線の管理(3)(b)【5.4.2(3)(b)】要機密情報を取り扱う無線LAN環境については、通信内容の暗号化を行う必要があることを遵守事項に追記。

・WEP（Wired Equivalent Privacy ）は、比較的容易に解読できるという脆弱性が報告されており、適当な暗号方式ではない（電子政府推奨暗号リストにおいても推奨していない）ため、選択しない事を解説に追記。

C. 実務に則した遵守事項の見直し

分割

■ 編による構成分割

経緯

・教育や自己点検、監査、見直し時の確認や検討観点として、各遵守事項について技術的なことを主眼とするのかそれ以外かが容易にわからない場合がある。

・統一基準を「基本編」と「情報システム編」に分割明示することで、教育や自己点検、監査、見直し時の確認や検討観点を明確にする。

・省庁対策基準の見直しについて、決裁者のレベルを分けることを容易にすることもできる。
＜例：基本編はCISO（官房長レベル）以上、情報システム編は課長レベルなど。＞

C1

統一基準（第3版）

第1部　総則
第2部　組織と体制の整備
第3部　情報についての対策
第4部　情報セキュリティ要件の明確化に基づく対策
第5部　情報システムの構成要素についての対策
第6部　個別事項についての対策
（A.1　解説書別添資料）

・体系は基本的な考え方であり、節・遵守事項レベルで見ると異なる編で分類しているものもある。

・統一基準第4版の詳細な構成は項番対応表参照のこと。

※情報システム編相当を課長レベルの決裁とする場合は、委任規定等が必要。

統一基準（第4版）

第1編　基本編
第1.1部　総則（第3版・第1部）
第1.2部　組織と体制の整備（第3版・第2部）
第1.3部　情報についての対策（第3版・第3部）
第1.4部　情報処理についての対策（第3版・第6部）
第1.5部　情報システムについての基本的な対策（第3版・第4部）

第2編　情報システム編
第2.1部　情報セキュリティ要件の明確化に基づく対策（第3版・第4部）
第2.2部　情報システムの構成要素についての対策（第3版・第5部）
第2.3部　個別事項についての対策（第3版・第6部）

A.1　解説書別添資料

C. 実務に則した遵守事項の見直し

修正

■ 情報の格付け及び取扱制限に関する解釈の明確化

経緯

・情報の格付け及び取扱制限の遵守事項に対して、実務上の解釈については、これまで省庁の個別質問に回答する他は、別途示していた「情報の格付け及び取扱制限に関する規程　策定手引書（以下、DM3-01）」にだけ反映していた。

・省庁の個別質問に回答した解釈内容は、省庁対策基準に記載されるべき事項と思料しており、統一基準により各省庁間での解釈に差異がないようにする。

C2

■統一基準第4版に解釈の明記

・これまでの解釈について統一基準第4版では次のとおり明確にすることとする。

ー情報の格付けの区分及び取扱制限の種類　1.1.1.3(1)、(2)、(3)	←集約：定義や解説に分散記載していたものを集約
ー情報の作成又は入手時における格付けと取扱制限の決定　1.3.1.1(2)	←統合：情報作成時と入手時、変更時を統合
ー格付けと取扱制限の明示等　1.3.1.1(3)	←修正：明示の解釈を明記
ー格付けと取扱制限の加工時における継承　1.3.1.1(4)	←分割：継承を情報加工時と複製時を分けて明記
ー格付け及び取扱制限の複製時における継承　1.3.1.2(3)	←分割：継承を情報加工時と複製時を分けて明記
ー格付け及び取扱制限の見直し　1.3.1.2(4)	←分割：情報加工時の変更を情報作成に統合
ー取扱制限の種類に係る付表例　A.1.2	←移動：DM3-01の例示を解説として記載

C. 実務に則した遵守事項の見直し

統合

■ 運用改善に伴う重複する遵守事項の統合

経緯

・第3版『4.1情報セキュリティについての機能』の行政事務従事者による対策実施に係る遵守事項の中で、第3版『3.2情報の取扱い』と重複しているものを見直す。

・遵守事項を削除することにより、遵守事項の本来意味が失われることがないように集約先の遵守事項解説を見直し、必要な修正を行う。

C3 ■『アクセス制御機能』の中で『情報の取扱い』と重複する項目の統合

第3版

・「3.2情報の取扱い」の関連項目
（3.2.3(1)(a)）

・「4.1.2アクセス制御機能」の関連項目
（4.1.2(2)(a)）

解説を修正
行政事務従事者によるアクセス制御の実施

内容の分割
情報システムセキュリティ責任者によるアクセス制御の実施（共有ファイルサーバ等）

第4版

・「1.3.1.3情報の保存(1)(a)」

・「2.1.1.2アクセス制御機能」

2.1.1.2(2)(a) 情報システムセキュリティ責任者は、**行政事務従事者自らがアクセス制御を行うことができない情報システムについて**、当該情報システムに保存されることとなる情報の格付け及び取扱制限に従って、アクセス制御を行うこと。

C4 ■『暗号と電子署名（鍵管理を含む）』の中で『情報の取扱い』と重複する項目の統合

第3版

・「3.2情報の取扱い」の関連項目
（3.2.3(1)(d), 3.2.3(1)(e), 3.2.4(5)(b), 3.2.4(5)(c)）

・「4.1.6暗号と電子署名（鍵管理を含む）」の関連項目
（4.1.6(4)(a), 4.1.6(4)(b)）

解説を修正
情報を暗号化（電子署名を付与）すること

内容の分割
定められた方法・アルゴリズムの遵守

第4版

・「1.3.1情報の取扱い」

1.3.1.3(1)(d) 行政事務従事者は、パスワードを用いた保護が必要な場合、その設定をすることを追加。 **追加**

・「1.5.2.4暗号と電子署名の標準手順」

1.5.2.4(2)(a) 行政事務従事者は、情報を暗号化する場合及び情報に電子署名を付与する場合には、**定められたアルゴリズム及び方法に従うこと。**

例示:『アクセス制御機能』の中で『情報の取扱い』と重複する項目の統合

第3版

3．2．3情報の保存

(1)格付けに応じた情報の保存

【基本遵守事項】

(a)行政事務従事者は、電磁的記録媒体に保存された要保護情報について、適切なアクセス制御を行うこと。

解説:電磁的記録媒体に保存された情報に関して、機密性、完全性及び可用性の格付け及び取扱制限に応じ、必要のない者に情報へアクセスさせないためのアクセス制御を可能な範囲で実施することを求める事項である。

電磁的記録媒体に保存された情報には電子計算機等を利用してアクセスすることになるため、アクセス制御は、電子計算機、オペレーティングシステム、アプリケーション及びファイル等を単位として行うことができ、これらを選択し組み合わせて、適切なアクセス制御を実現する。

＋

第4版

＜行政事務従事者によるアクセス制御の実施＞

1．3．1．3(1)(a)　**解説に以下を追加**

情報システムに行政事務従事者自らがアクセス制御設定を行う機能が装備されている場合には、行政事務従事者は、当該情報の格付け及び取扱制限の指示内容に従って、必要なアクセス制御の設定を行うこと。例えば、要機密情報であれば、不適当な者から参照されないよう、読取制限の属性を付与し、完全性2情報であれば、不適当な者から変更されないよう、上書き禁止の属性を付与することがこれに当たる。

ただし、複製禁止の取扱制限がされていたとしても、情報システムに複製禁止とする機能がなければ、そのアクセス制御の設定をすることはできない。その場合には、情報システムが備えていない機能については、行政事務従事者が取扱上注意することで、その指示を遵守することになる。

解説移動

4．1．2アクセス制御機能

(2)適正なアクセス制御

【基本遵守事項】

(a)行政事務従事者は、情報システムに装備された機能を用いて、当該情報システムに保存される情報の格付けと取扱制限の指示内容に従って、必要なアクセス制御の設定をすること。

解説:情報システムに行政事務従事者自らがアクセス制御設定を行う機能が装備されている場合には、行政事務従事者は、当該情報の格付けと取扱制限の指示内容に従って、必要なアクセス制御の設定を行うことを求める事項である。例えば、要機密情報であれば、不適当な者から参照されないよう、読取制限の属性を付与し、完全性2情報であれば、不適当な者から変更されないよう、上書き禁止の属性を付与することがこれに当たる。

ただし、複製禁止の取扱制限がされていたとしても、情報システムに複製禁止とする機能がなければ、そのアクセス制御の設定をすることはできない。その場合には、情報システムが備えていない機能については、行政事務従事者が取扱上注意することで、その指示を遵守することになる。

修正

＜情報システムセキュリティ責任者によるアクセス制御の実施＞

遵守事項と解説の修正

2．1．1．2

(2)適正なアクセス制御

【基本遵守事項】

(a)情報システムセキュリティ責任者は、行政事務従事者自らがアクセス制御を行うことができない情報システムについて、当該情報システムに保存されることとなる情報の格付け及び取扱制限に従って、アクセス制御を行うこと。

解説:共有ファイルサーバのアクセス制御のように、情報システムを行政事務従事者が利用する際に、自らがアクセス制御を行うことができない場合、情報システムの導入時及び運用時にアクセス制御を行うことを求めた事項である。例えば、要機密情報であれば、不適当な者から参照されないよう、読み取り制限の属性を付与し、完全性2情報であれば、不適当な者から変更されないよう、上書き禁止の属性を付与することがこれに当たる。

また、行政事務従事者自らがアクセス制御を行うことが出来る場合、1.3.1.3(1)(a)の規程に基づき対策を行うこと。

C. 実務に則した遵守事項の見直し

統合

■ 運用改善に伴う重複する遵守事項の統合

経緯

・第3版の情報システムに係る遵守事項において、自己点検において重複する点検になってしまう部分が存在。

・第3版『第5部　情報システムの構成要素についての対策』の遵守事項の中で、第3版『4.1情報セキュリティについての機能』及び『4.2 情報セキュリティについての脅威』と重複しているものを削除する。

C5 ■『情報システムの構成要素についての対策』の中で『情報セキュリティについての機能』と重複する項目の削除

第3版

・「4.1情報セキュリティについての機能」

・「5.2電子計算機」、「5.4通信回線」の関連項目
（5.2.1(1)(d), 5.2.1(1)(e), 5.2.3(2)(d), 5.4.1(1)(o)）

本集約による変更無し →

第4版

・「2.1.1情報セキュリティについての機能」

C6 ■『情報システムの構成要素についての対策』の中で『情報セキュリティについての脅威』と重複する項目の削除

第3版

・「4.2情報セキュリティについての脅威」

・「5.2電子計算機」、「5.4通信回線」の関連項目
（5.2.1(1)(f), 5.2.1(1)(g), 5.2.1(2)(e), 5.2.1(2)(f), 5.4.1(1)(l), 5.4.1(2)(i)）

本集約による変更無し →

第4版

・「2.1.2情報セキュリティについての脅威」

C. 実務に則した遵守事項の見直し

統合

■ 運用改善に伴う重複する遵守事項の統合

経緯

・第3版『4.2情報セキュリティについての脅威』に属する各部構成の平仄をあわせることを目的として、重複している遵守事項を削除する。
・遵守事項を削除することにより、遵守事項の本来意味が失われることがないように統合先の遵守事項解説を見直し、必要な修正を行う。

C7

■遵守事項を削除し、統合先の遵守事項の解説に削除した遵守事項の趣旨を加えた修正

・削除した遵守事項：第3版4.2.2不正プログラム対策 (2)(i)
・統合先の遵守事項：1.5.2.1情報システムに係る文書及び台帳整備 (1)(a)(エ)障害・事故等が発生した際の対処手順

■ その他重複する遵守事項の統合

経緯

・その他重複している遵守事項を削除する。
・遵守事項を削除することにより、遵守事項の本来意味が失われることがないように統合先の遵守事項解説を見直し、必要な修正を行う。

C8

■遵守事項を削除し、統合先の遵守事項の解説に削除した遵守事項の趣旨を加えた修正

・削除した遵守事項：第3版5.3.1通信回線を介して提供するアプリケーション共通対策(2)(b)
・統合先の遵守事項：2.2.2.1電子計算機共通対策(2)(a)【5.2.1(2)(c)】

C. 実務に則した遵守事項の見直し

集約

■ 情報システムに係る文書整備に関わる遵守事項の集約

経緯

・文書整備計画の対象となる遵守事項が散在しており、それらの抽出作業が冗長となる。

・第3版において、情報システムに係る文書整備に関する遵守事項が第4部、第5部の各所に散在。

・第3版『4.2.1セキュリティホール対策』及び『第5部　情報システムの構成要素についての対策』の中の文書整備に関わる遵守事項を、一つの遵守事項にまとめ、分かりやすさの向上を図る。

C9 **■情報システムに係る文書整備に関わる遵守事項を『1.5.2.1 情報システムに係る文書及び台帳整備』に集約する**

第3版

・「4.2.1セキュリティホール対策」の関連項目
(4.2.1(1)(a), 4.2.1(2)(a))

・「5.2電子計算機」の関連項目
(5.2.1(1)(a), 5.2.1(1)(b), 5.2.1(1)(h), 5.2.1(2)(a), 5.2.1(2)(b),5.2.1(2)(d), 5.2.1(2)(g))

・「5.3アプリケーションソフトウェア」の関連項目
(5.3.1(1)(a), 5.3.1(2)(a))

・「5.4通信回線」の関連項目
(5.4.1(1)(a), 5.4.1(1)(d), 5.4.1(1)(e), 5.4.1(2)(a), 5.4.1(2)(b), 5.4.1(2)(c), 5.4.1(2)(f))

第4版

1.5.2.1(1)(a) 情報システムセキュリティ責任者は、所管する情報システムについて**以下の事項を記載した文書を整備すること**。

文書の整備

(ア)当該情報システムを構成する電子計算機関連事項

(イ)当該情報システムを構成する通信回線及び通信回線装置関連事項

(ウ)情報システムの構成要素のセキュリティ維持に関する手順

(エ)障害・事故等が発生した際の対処手順 追加

文書の利用

1.5.2.1(1)(b) 情報システムセキュリティ管理者は、所管する情報システムについて**整備した文書に基づいて、情報システムの運用管理において情報セキュリティ対策を行うこと**。 追加

C. 実務に則した遵守事項の見直し

集約

■ 規定の整備と遵守に関する遵守事項の集約

経緯

・文書整備計画の対象となる遵守事項が散在しており、それらの抽出作業が冗長となる。
・第3版の第4部から第6部の情報システム関係の節のうち、府省庁での規定の整備・遵守に関わるものを基本編にまとめる。
・規定の整備を求める遵守事項については主語を「統括情報セキュリティ責任者」に統一する。
・強化遵守事項を基本遵守事項にする場合には、「必要に応じて」を付す。

C10

■『1.5.2.2【6.1.1】機器等の購入』の集約

(1)規定の整備：1.5.2.2(1)(a), 1.5.2.2(1)(c) →変更なし　1.5.2.2(1)(b)→文言修正
(2)規定の遵守：1.5.2.2(2)(a)→変更なし　1.5.2.2(2)(b)→文言修正
（項目の削除）　第3版6.1.1(2)(c)→「1.2.5.1外部委託」で内容を読み取れることから、削除。

C11

■『1.5.2.3【6.1.3】ソフトウェア開発』の集約

第３版6.1.3(1)(a)～6.1.3(5)(b) ：主語は全て情報システムセキュリティ責任者。

↓

(1)規定の整備：1.5.2.3(1)(a)：**統括情報セキュリティ責任者**は、ソフトウェア開発について規定を整備すること。

〇規定で定めるべき事項については（ア）～（セ）に列挙。

〇**（強化→基本）**　第３版6.1.3(4)(c)ソースコードレビュー→「必要に応じて」を加えて強化遵守事項から基本遵守事項に変更。

(2)規定の遵守：1.5.2.3(2)(a)：情報システムセキュリティ責任者は規定を遵守すること。

（次のスライドにつづく）

集約

■ 規定の整備と遵守に関する遵守事項の集約 （つづき）

C12 **■『1.5.2.4【4.1.6】暗号と電子署名の標準手順』の集約**

(1)規定の整備（1.5.2.4(1)【4.1.6(1)】）： 第3版4.1.6(1)(a)→1.5.2.4(1)(a)文言修正、 第3版4.1.6(1)(b), 4.1.6(1)(c)→1.5.2.4(1)(b)に集約
第3版4.1.6(1)(d)→1.5.2.4(1)(c)文言修正

(2)規定の遵守（1.5.2.4(2)【4.1.6(4)】）： 第3版4.1.6(4)(a),4.1.6(4)(b)→1.5.2.4(2)(a)に集約、 第3版4.1.6(4)(c)→1.5.2.4(2)(b)文言修正
第3版4.1.6(4)(d)→1.5.2.4(2)(c)文言修正

C13 **■『1.5.2.5【6.3.1】府省庁外の情報セキュリティ水準の低下を招く行為の防止』の集約**

(1)規定の整備：1.5.2.5(1)(a)→変更なし

(2)規定の遵守：1.5.2.5(2)(a)→文言修正

C14 **■『1.5.2.6【6.3.3】ドメイン名の使用についての対策』の集約**

(1)規定の整備：1.5.2.6(1)(a) →文言修正

(2)規定の遵守：1.5.2.6(2)(a)→新規（行政事務従事者は規定を遵守すること） **追加**

C15 **■『1.5.2.7【4.2.2】不正プログラム感染防止のための日常的実施事項』の集約**

第3版4.2.2(1)(a) ：**情報セキュリティ責任者**は不正プログラム感染防止のための日常的実施事項を定めること。

第3版4.2.2(2)(b)～(2)(g)：行政事務従事者の遵守事項

↓

(1)規定の整備：1.5.2.7(1)(a)：**統括情報セキュリティ責任者**は不正プログラム対策について規定を整備すること。

〇規定で定めるべき事項については（ア）～（キ）に列挙。 （キ）：**追加**

(2)規定の遵守：1.5.2.7(2)(a)：行政事務従事者は規定を遵守すること。

C. 実務に則した遵守事項の見直し

修正

■ 情報システムセキュリティ責任者の権限見直し

経緯

・情報システム編における主語を実務に即して見直し、情報セキュリティ責任者と情報システムセキュリティ責任者の権限を明確にする。

C16 **■主語を情報システムセキュリティ責任者に変更**

・2.1.1.4証跡管理機能(3)(a)【4.1.4(3)(a)】

・2.1.1.4証跡管理機能(4)(a)【4.1.4(4)(a)】

・2.1.2.2不正プログラム対策(2)(b)【4.2.2(2)(h)】

■ 許可及び届出の取得の明確化

経緯

・許可及び届出の取得にあたり、遵守事項及び解説にて許可及び届出先を明確にするとともに、許可又は届出を要しない場合について明確にするための見直しを行う。

C17 **■許可及び届出の取得を明確にするため、遵守事項及び解説の修正**

・『又は』を見直し『及び』に修正。

・許可又は届出を要しないと認められた場合を追記。

・対応遵守項目：1.4.1.1府省庁外での情報処理の制限【6.2.1】

1.4.1.2府省庁支給以外の情報システムによる情報処理の制限【6.2.2】

C. 実務に則した遵守事項の見直し

修正

■ サーバ装置の可用性維持に関する対策実施段階の見直し

経緯

・設計段階にて対策を考慮することができるように遵守事項の位置の見直しを行う。

C18 **■設計段階にて対策を実施するため、遵守事項の位置を移動**

・ 2.2.2.3サーバ装置(1)(e)【5.2.3(2)(h)】 (2)サーバ装置の運用時から(1)サーバ装置の設置時に移動。

■ サーバ装置の可用性維持に関する対策方法の見直し

経緯

・可用性維持のための手段として適切になるように遵守事項の見直しを行う。

C19 **■可用性維持のための手段を明確にするため、遵守事項及び解説の修正**

・ 2.2.2.3サーバ装置(1)(e)【5.2.3(2)(h)】可用性維持の手段としてサーバ装置の冗長構成を追記。

C. 実務に則した遵守事項の見直し

修正

■ 情報システムに係る台帳整備の内容見直し

経緯

・第3版の情報システム台帳に関する遵守事項では、台帳に記載すべき内容について解説には記載しているものの、遵守事項自体の記載が不十分。

・情報セキュリティ対策の観点から、最小限、台帳に記載するべき内容を明確化する記述を遵守事項に加えるとともに、併せて、台帳の運用方法を整理する。

C20 **■台帳整備に関する遵守事項の内容を明確化のため見直す**

第3版

4.3.1(5) 情報システムの台帳整備

4.3.1(5)(a) **情報システムセキュリティ責任者**は、情報システムを新規に構築し、又は更改する際には、**当該情報システムで取り扱う情報及び当該情報の格付けを含む事項**を統括情報セキュリティ責任者に報告すること

4.3.1(5)(b) **統括情報セキュリティ責任者**は、すべての情報システムに対して、(中略)事項を記載した台帳を整備すること。

第4版

(2)(a) **統括情報セキュリティ責任者**は、すべての情報システムに対して、当該情報システムに係る**以下の事項を記載した台帳を整備すること**。

(ア)情報システム名、管理課室及び管理責任者の氏名・連絡先

(イ)システム構成

(ウ)接続する府省庁外通信回線の種別

(エ)取り扱う情報の格付け及び取扱制限に関する事項

(オ)当該情報システムの設計・開発、運用、保守に関する事項

(2)(b) **情報システムセキュリティ責任者**は、情報システムを新規に構築し、又は更改する際には、当該情報システムの台帳の記載事項について統括情報セキュリティ責任者に報告すること。

D. 運用改善のための解説の見直し

修正

■ **解説の明確化**

D1

■ **情報システムセキュリティ責任者の設置時期の明確化** 1.2.1.1組織・体制の整備(5)(a)【2.1.1(5)(a)】

D2

■ **中央省庁業務継続ガイドラインの反映** 1.2.5.2業務継続計画との整合的運用の確保(1)(c)(ア)【6.3.2(2)(c)(ア)】

D3

■ **暗号化及び電子署名の標準手順に従うことを明記** 1.3.1.3情報の保存(1)(e)【3.2.3(1)(d)】
1.3.1.3情報の保存(1)(f)【3.2.3(1)(e)】
1.3.1.4情報の移送(5)(b)【3.2.4(5)(b)】
1.3.1.4情報の移送(5)(c)【3.2.4(5)(c)】

D4

■ **情報システムのセキュリティ要件決定時における情報システム編の遵守を明記**
1.5.1.1情報システムのセキュリティ要件(1)(c)【4.3.1(1)(c)】

D5

■ **施設全体を安全区域として対策を実施することの明確化**
2.2.1.1電子計算機及び通信回線装置を設置する安全区域(1)(a)【5.1.1(1)(a)】

等

E. 文言の改善

修正

■ 電子署名の機能に関する明確化

経緯

・電子署名の機能として、発行する文書に関しては署名の付与、受領する文書に関しては署名の検証が挙げられる。これまでの遵守事項では署名の付与に重点を置き、相対する署名の検証について明確にされていなかったため、該当する遵守事項の見直しを行う。

E1 **■電子署名の検証機能について明確にするため、遵守事項及び解説の修正を行う**

・2.1.1.6暗号と電子署名（鍵管理を含む）【4.1.6】『電子署名の付与』→『電子署名の付与及び検証』、『電子署名の付与又は検証』。

■ 受信した電子メールの表示に関する遵守事項の見直し

経緯

・対策を明確にするために遵守事項及び解説の見直しを行う。

E2 **■受信した電子メールの表示に関して、遵守事項及び解説の修正を行う**

・2.2.3.1電子メール(2)(b)【5.3.2(2)(b)】スクリプトを実行しない形式での表示とすることに修正。

■ 用語の整理等

E3

■ 情報セキュリティを脅かすものをより明確化するため「障害等」→「障害・事故等」にする（ 1.2.2.2【2.2.2】 等）。

■ 2.2.2.2(1)(d)【5.2.2(1)(d)】「機能を付加すること」→「機能を設けること」への平仄合わせ等。