DM5-01-051

庁舎内におけるＰＣ利用手順　PC の取扱編

策定手引書

2006 年 3 月

内閣官房情報セキュリティセンター

改訂履歴

改定日	改訂箇所	改訂内容	改訂理由

商標について

Microsoft および Windows は、米国 Microsoft Corporation の、米国、日本およびその他の国における登録商標または商標です。

1　本書の目的

本書は、庁舎内における PC の取扱いに関するする規定（以下「庁舎内における PC 利用手順 PC の取扱編」という。）を情報システムセキュリティ責任者が整備するための手引書である。

府省庁においては、「政府機関の情報セキュリティ対策のための統一基準（2005 年 12 月版（全体版初版））」（NISD-K303-052、以下「政府機関統一基準」という。）に準拠する省庁基準と、省庁基準を具体化する一連の実施手順群を整備することが求められている。「庁舎内における PC 利用手順 PC の取扱編」は、これらの実施手順の一つとして策定し、庁舎内での PC の利用に対して適用するものである。すなわち、情報システムセキュリティ責任者等がこれに従うことにより、政府機関統一基準に基づく省庁基準の関係する規定を遵守することとなるものである。

情報システムセキュリティ責任者は、自身が責任者となっている情報システムに端末が含まれる場合、セキュリティを維持しながら当該端末を運用する必要があるため、運用に携わる担当者が実施すべき事項を定め、自己について定めた事項を遵守することが求められる。

本書は、これらの背景の下で、「庁舎内における PC 利用手順 PC の取扱編」に含めるべき手順及び記述例を具体的に示し、もって統一基準及び省庁基準への準拠性、業務手順への適用性等において適切な規定の整備に資することを目的とする。

2　実施手順に記載すべき事項

「庁舎内における PC 利用手順 PC の取扱編」には、以下の事項を具体化させて記載すること。

2.1　政府機関統一基準（NISD-K303-052）に定める「庁舎内における PC 利用手順 PC の取扱編」に係る遵守事項

2.1.1　組織・体制の確立（６）情報システムセキュリティ管理者の設置
2.2.2　障害等の対応（２）障害等の発生時における報告と応急措置
2.4.1　情報セキュリティ対策の見直し（１）情報セキュリティ対策の見直し
3.2.1　情報の作成と入手（１）業務以外の情報の作成又は入手の禁止
3.2.2　情報の利用（３）要保護情報の取扱い
3.2.3　情報の保存（１）格付けに応じた情報の保存
3.2.6　情報の消去（１）電磁的記録の消去方法
4.1.1　主体認証機能（１）主体認証機能の導入
4.1.1　主体認証機能（２）行政事務従事者における識別コードの管理
4.1.1　主体認証機能（３）行政事務従事者における主体認証情報の管理
4.1.2　アクセス制御機能（１）アクセス制御機能の導入

4.1.2　アクセス制御機能（２）行政事務従事者による適正なアクセス制御

4.1.3　権限管理機能（１）権限管理機能の導入

4.1.3　権限管理機能（２）識別コードと主体認証情報の付与管理

4.1.3　権限管理機能（３）識別コードと主体認証情報における代替措置の適用

4.1.4　証跡管理機能（１）証跡管理機能の導入

4.1.4　証跡管理機能（２）情報システムセキュリティ管理者による証跡の取得と保存

4.1.5　保証のための機能（１）保証のための機能の導入

4.1.6　暗号と電子署名（鍵管理を含む）（１）暗号化機能及び電子署名の付与機能の導入

4.1.6　暗号と電子署名（鍵管理を含む）（２）暗号化及び電子署名の付与に係る管理

4.2.1　セキュリティホール対策（１）情報システムの構築時

4.2.1　セキュリティホール対策（２）情報システムの運用時

4.2.2　不正プログラム対策（１）情報システムの構築時

4.2.2　不正プログラム対策（２）情報システムの運用時

5.1.1　電子計算機及び通信回線装置を設置する安全区域（３）電子計算機及び通信回線装置のセキュリティ確保

5.2.1　電子計算機共通対策（１）電子計算機の設置時

5.2.1　電子計算機共通対策（２）電子計算機の運用時

5.2.1　電子計算機共通対策（３）電子計算機の運用終了時

5.2.2　端末（１）端末の設置時

5.2.2　端末（２）端末の運用時

5.3.1　アプリケーションソフトウェア（２）アプリケーションの運用時

5.3.3　ウェブ（２）ウェブの運用時

5.4.1　通信回線共通対策（２）通信回線の運用時

2.2　セキュリティ確保に係るその他の留意事項

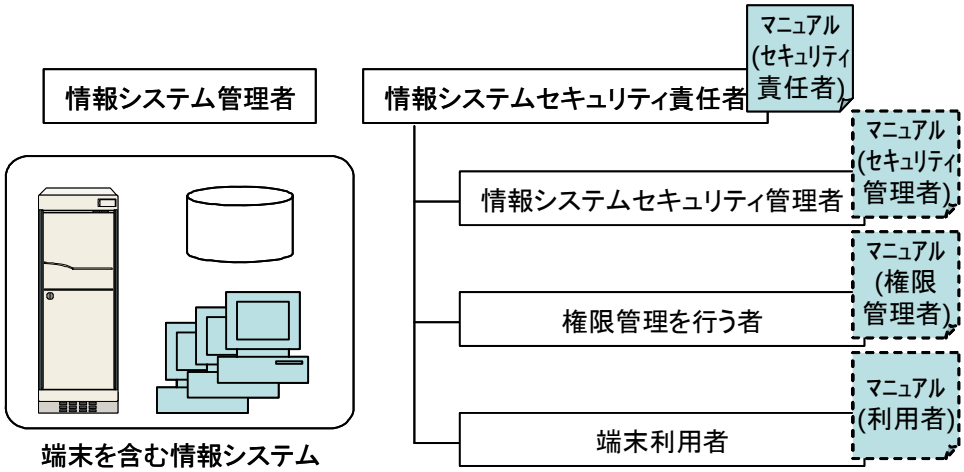
2.1 に示す遵守事項のほか、セキュリティ確保に係る留意事項として、以下の項目を考慮すべきである。

- オペレーティングシステム標準の識別コードの変更
- パスワード初期化の手順

3　文書構成例

「庁舎内における PC 利用手順 PC の取扱編」は、情報セキュリティ対策の観点以外の要素も含む一般的な利用マニュアルとすべきである。また、端末のセキュリティ対策の観点から、運用にかかわる各担当者が実施する事項を総体的に検討し、決定する必要がある。そのため、情報システムセキュリティ責任者等、担当者の行為に着目した構成が有効と考えられる。文書構成の例を以下に示す。

本構成例には、情報システムセキュリティ責任者の実施事項のほか、情報システムセキュリティ責任者が定める他の担当者の実施事項として《情報システムセキュリティ管理者パート》、《権限管理を行う者パート》及び《端末利用者パート》も含まれている。各々の担当者の関係及び実施事項を記したマニュアルは、下図のような関係を想定している。



1 本書の目的
2 本書の対象者
　2.1 対象者
3 端末管理体制の整備
　3.1 端末の運用にかかわる担当者の管理
4 端末運用にかかわる規定類の整備
　4.1 全般的な実施事項
　4.2 情報システムセキュリティ管理者にかかわる規定の整備
　4.3 権限管理を行う者にかかわる規定の整備
　4.4 行政事務従事者にかかわる規定の整備
　4.5 端末の構成の管理
5 端末機能の整備
　5.1 端末機能にかかわる検討
　5.2 端末の設置
6 端末の運用
　6.1 端末の運用に係る全般的な注意事項
　6.2 端末運用形態に係る検討
　6.3 識別コードの発行

6.4 日常の管理作業
6.5 識別コードの利用停止
6.6 端末の運用終了
《 権限管理を行う者パート 》
1 端末における権限管理手順
1.1 権限管理に係る全般的な注意事項
1.2 識別コードの発行
1.3 識別コードの利用停止
《 情報システムセキュリティ管理者パート 》
1 端末の運用について
1.1 端末の運用に係る全般的な注意事項
2 端末のセキュリティ維持にかかわる情報の整備
2.1 端末に係る情報の管理
2.2 識別コードとパスワードの代替措置の管理
3 端末機能の整備
3.1 端末の設定
4 端末のセキュリティ維持活動
4.1 端末のセキュリティ維持に係る全般的な注意事項
4.2 セキュリティホール対策の実施
4.3 不正プログラム対策の実施
4.4 識別コードの管理
4.5 障害等の対処
《 端末利用者パート 》
1 端末の取扱い
1.1 端末の運用に係る全般的な注意事項
1.2 端末の操作方法
1.3 日常の取扱い
1.4 個別機能の利用
2 識別コード及びパスワードの取扱い
2.1 識別コード及びパスワードに係る全般的な注意事項
2.2 識別コードの利用開始
2.3 識別コードの日常の取扱い
2.4 識別コードの返却
3 端末利用にかかわる手続き
3.1 主体認証情報の初期化申請
3.2 主体認証情報の露呈の報告
3.3 障害等の対処
4 本手順に関する相談窓口

4 策定する上での留意事項

「庁舎内における PC 利用手順 PC の取扱編」は、以下のことに留意して策定する。

(1) 情報システムセキュリティ責任者、情報システムセキュリティ管理者、権限管理を行う者及び端末利用者の実施する手順が整合しており、総合的に端末のセキュリティ維持を図る。

(2) 情報システムセキュリティ責任者、情報システムセキュリティ管理者、権限管理

を行う者及び端末利用者が庁舎内において端末を管理及び利用する場合の様々な場面を想定し、ライフサイクルによって記載事項を整理・分類する。

(3) マニュアルに記述する文章は、可能な限り各パートの対象として想定する読み手を主語として記述する。例えば、各パートにおいて「情報システムセキュリティ責任者」、「情報システムセキュリティ管理者」、「権限管理を行う者」、「端末利用者」を主語として書き分ける。

(4) 図表を多用し、個々の規定ごとに具体的に説明を加える。

(5) 前記 2 の実施手順に記載すべき事項を「庁舎内における PC 利用手順 PC の取扱編」に反映するに当たっては、当該事項の内容に応じて、以下のいずれかの方針で記述する。

[具体化]・・・「端末の取扱い」に限定されず一般的・抽象的に記述されており、具体化が必要と思われる遵守事項については、これを「端末の取扱い」に適用し、表現をより具体的に修正・追加する。

[転　記]・・・記述内容が具体性を持ち、変更が不要と思われる遵守事項については、これを転記する。

[詳細化]・・・記述内容が具体性を持っているが、情報システムセキュリティ責任者等の利便性を考慮して、より詳細な解説を付すべきと思われる遵守事項については、解説書等を参考に、これを詳細化する。

[背　景]・・・主にセキュリティ機能の実装に関する内容であり、これを背景として情報システムセキュリティ責任者等による注意義務が発生すると思われる遵守事項については、これを情報システムセキュリティ責任者等の立場から解釈し直す。

[参考引用]・・・直接「端末の取扱い」に関連した内容ではないが、情報システムセキュリティ責任者等の理解促進に寄与すると思われる遵守事項については、これを参考引用する。

[一　般]・・・直接「端末の取扱い」に関連した内容ではないが、一般論として手順書に記載しておくことが望ましいと思われる遵守事項については、これを周辺知識として盛り込む。

5　参考資料

「庁舎内における PC 利用手順 PC の取扱編」の策定に際しては、以下のような資料が参考となる。

5.1 政府及び政府関係機関の資料

(1) NPO 日本ネットワークセキュリティ協会(JNSA)の「情報セキュリティポリシー・サンプル 0.92a 版」
URL: http://www.jnsa.org/policy/guidance/index.html

(2) 独立行政法人 情報処理推進機構(IPA)の資料
対策のしおり- ウイルス対策、ボット対策、スパイウェア対策 -
http://www.ipa.go.jp/security/antivirus/shiori.html
SOHO・家庭向けセキュリティ対策マニュアル(Ver1.20)
http://www.ipa.go.jp/security/fy14/contents/soho/html/index.html

(3) 財団法人 インターネット協会(IA Japan)の「インターネット利用のための社内ルール整備ガイドライン」
URL: http://www.iajapan.org/rule/rule4business/

(4) 社団法人 電子情報技術産業協会(JEITA)の「パソコンの廃棄・譲渡時におけるハードディスク上のデータ消去に関するガイドライン」
URL: http://it.jeita.or.jp/perinfo/committee/pc/HDDdata/HDDdata.pdf

5.2 政府・政府関係機関以外の資料

(1) Microsoft 関連の資料

6 雛形の利用方法

別紙 1 の雛形を参考にすることにより、「庁舎内における PC 利用手順 PC の取扱編」を効果的に策定することができる。別紙 1 の雛形は、前記 2 の実施手順に記載すべき事項を、前記 3 の文書構成例の枠組みの中に記載したものであり、要求事項とその補足事項（操作手順を含む。）で構成されている。

6.1 雛形において想定する前提

本雛形は、以下を前提として記述している。そのため、使用する環境が以下と異なる場合には、適宜、修正、追加又は削除する必要がある。

- 全職員を対象とする省内LANを想定している（より限定された利用者を対象とする業務システム等にも適用可能である。）。
- 人事異動等により省内LANを利用する業務上の理由が発生又は消滅した者には、申請がなくとも端末の貸与又は返却は実施される。
- 府省庁外に接続するネットワークは構築されている（ファイアウォール等による保護がなされている。）。
- Windows®ドメインによる集中管理は実施されておらず、識別コードの管理は端末ごとに実施されている。
- Windows® Update、アンチウイルスの定義ファイル更新等は、集中的に実施されておらず、端末ごとに実施されている。
- 本システムは、セキュリティ機能として、主体認証、権限管理、アクセス管理が必要なシステムである。

- 主体認証方式として、知識による方式を採用する。
- 共有識別コードは認めないシステムである。
- 以下のソフトウェア製品を使用している。
  - オペレーティングシステム：Microsoft Windows® XP Professional Version 2002 Service Pack 2
- 障害発生時の対応の詳細は別途定められている。

6.2 手直しポイント

政府機関統一基準に基づき策定された省庁基準に準拠した「庁舎内における PC 利用手順 PC の取扱編」を策定する手順には、大別して、新規策定と既存文書の修正があるが、そのどちらの場合でも以下の事項を踏まえて作業を行う必要がある。

(1) 使用環境（利用するソフトウェア等）やその前提（行政事務従事者に管理者権限を付与しているか否か等）に応じて内容を変更する。

(2) 雛形中に、*/・・・/* 形式で明記される設定値（パスワード文字数、容量、文書名等）については、各府省庁内の定めに合わせる。

(3) 雛形中に、【・・・の場合】形式で明記される記述については、想定される複数の案を記したものであり、各府省庁の判断により適宜、選択又は修正する。

(4) 既存のマニュアル等との整合性を考慮し、適切に分割、統合、相互参照する。

(5) 雛形に情報セキュリティ対策の観点以外の一般的な記述について不足がある場合には、適宜、補う。