DM5-01-051

別紙１：雛形

庁舎内におけるＰＣ利用手順　　ＰＣの取扱編

雛形

2006 年 3 月

内閣官房情報セキュリティセンター

本書の位置付け

本書は、「庁舎内で PC を利用する場合の手順書」を策定する場合の雛形であり、「庁舎内における PC 利用手順 PC の取扱編策定手引書」の２に示す実施手順に記載すべき事項を、同 3 に示す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。

本書の利用方法

本書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。

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「PC の取扱マニュアル」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策定する必要がある。

① 使用環境（利用するソフトウェア等）やその前提(端末利用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必要がある。
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 既存のガイドライン等との整合性を考慮し、適切に分割、統合、相互参照する。
⑤ 本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。

改訂履歴

改訂日	改訂理由
2005/3/31	初版
2006/4/21	各府省庁意見に基づく修正

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。

Microsoft Corporationのガイドラインに従って画面写真を使用しています。

『一太郎』は、株式会社ジャストシステムの登録商標（商標）です。

Acrobatは、Adobe Systems Incorporated(アドビシステムズ社)の登録商標または商標です。

Norton AntiVirusは、Symantec Corporationの登録商標です。

ウイルスバスターは、トレンドマイクロ株式会社の登録商標です。

目次

1　本書の目的

行政事務を遂行するに当たっては電子計算機の利用が不可欠となっており、庁舎内においても端末利用者が端末を利用し様々な情報の作成、利用、保存等を実施している。これらの情報及び端末を適切に保護するためには、日常から端末の取扱いについて実施すべき事項を定め、これを適切に遵守する必要がある。

本書は、これらの事項について、情報システムセキュリティ責任者が実施すべき手順及び方法、並びに情報システムセキュリティ責任者が策定する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それぞれの役割に応じて実施すべき手順等を具体的に定めるための参考情報を提供することを目的とする。

2　本書の対象者

2.1　対象者

本書では、端末の運用にかかわる情報システムセキュリティ責任者が実施すべき対策等について記述するとともに、情報システムセキュリティ責任者が作成すべき端末の運用にかかわる手順についても、情報システムセキュリティ管理者、権限管理にかかわる者及び端末利用者の対象者ごとに分けて記述している。

なお、端末利用者とは、政府職員及びそれぞれの府省庁の指揮命令に服している者のうち、それぞれの府省庁の管理対象である端末を取り扱う者をいう。

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

(1) 情報システムセキュリティ責任者は、当該情報システムの管理において必要な単位ごとに情報システムセキュリティ管理者を定めること。また、情報システムセキュリティ管理者として定めた者を統括情報セキュリティ責任者に報告すること。

(2) 情報システムセキュリティ責任者は、端末の権限管理を行う者を定めること。

(3) 情報システムセキュリティ責任者は、端末ごとに当該端末を管理及び利用する端末利用者を特定する文書を作成し、当該端末利用者に変更があった場合には速やかに反映すること。

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

(1) 情報システムセキュリティ責任者は、端末のセキュリティ維持に関する手続を含む規定を整備すること。
*［本マニュアルの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、端末利用者パートのように、］*対象者ごとに実施すべき事項を手順も含め作成し、対象者に通知すること。

(2) 情報システムセキュリティ責任者は、自らが整備した情報セキュリティ関係規程の見直しの必要性を適時検討し、必要があると認めた場合にはその見直しを行うこと。

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

(1) 情報システムセキュリティ責任者は、端末におけるセキュリティホール対策の実施計画を立て、情報システムセキュリティ管理者に実施させることについてもあらかじめ定めること。実施計画は、端末の導入時及び運用時の実施手順として、詳細に定めることが望ましい。

補足
　セキュリティホール対策として端末にインストールされているソフトウェアにパッチを適用する場合、特殊なアプリケーションを利用しているなど、特段の理由がない限り、パッチが提供されてから適用されるまでの時間を短くすることなどを目的として、パッチの提供の検知から適用までを自動的に実施可能なソフトウェアでは、これを利用することが多い。
　例えば、Windows® の場合は、Windows® Update 又は Microsoft® Update を利用することにより、端末の導入時等に過去に提供されたすべてのパッチを適用すること、端末運用時にパッチ適用を自動化することが可能である。
一方、パッチの提供の検知から適用までを自動化できないソフトウェアの場合は、パッチの提供有無の確認方法、パッチの入手方法及び可能な場合には入手したパッチの検証方法、パッチ適用方法等を、セキュリティホール対策の実施計画に含めておく必要がある。

4.3　権限管理を行う者にかかわる規定の整備

(1) 情報システムセキュリティ責任者は、初期パスワード及びパスワードの変更管理にかかわる事項について定め、権限管理を行う者に通知すること。
初期パスワードについては、生成及び通知方法、初回ログイン時の初期パスワードの強制変更の有無等、変更管理については Windows® においてパスワードにかかわる設定が可能な有効期間、長さ、変更禁止期間等を定めること。

- 初期パスワードについて定める事項
  - 生成方法：生成ツールにより*[8]*桁のパスワードを生成
  - 通知方法:*[初期パスワードを印刷した紙を封筒に入れ、封筒に氏名、識別コードを記入し、当事者に手交]*
  - 初期パスワード強制変更：*[あり]*
- パスワードの変更管理について定める事項
  - パスワードの長さ：*[8]*桁以上
  - パスワード変更禁止期間：*[2]*日
  - パスワードの有効期間：*[40]*日
  - 同一パスワードの利用禁止回数：*[2]*回

(2) 情報システムセキュリティ責任者は、パスワードの忘却等により識別コードが利用できなくなった利用者からパスワード初期化の許可申請を受けた場合に、正当な利用者であることを確認した上でパスワードを初期化する手続を定め、権限管理を行う者に通知すること。手続には、以下のような項目を含めることが望ましい。

- パスワード初期化の申請書
- 職員証の目視その他正当な利用者を確認する方法及びその記録方法

(3) 情報システムセキュリティ責任者は、暗号化された情報（以下「暗号文」という。）を復号するための復号鍵の生成手順、有効期限、当該鍵の保存媒体及び暗号鍵の保存場所を定めること。

> 補足
> 　Windows® XP においては、ファイル又はフォルダを暗号化する操作を行うと自動的に暗号鍵及び復号鍵が生成され、内蔵記録媒体の標準的なフォルダに保存される。この Windows® XP の動作を生成手順等としてそのまま採用することも可能である。
> 　暗号化に係る運用については、端末利用者が個別に必要性を判断し実施する手法と、ファイルを保存する場合に標準的に実施する手法があるが、後者の方が、暗号化が必要なファイルの暗号化漏れを少なくできるという利点がある。このため、標準的に暗号化を実施する場合は、これを手順書に含めておくことが望ましい。例えば、権限管理を行う者が識別コードを端末に登録する際に、標準的に暗号化を実施するように設定する方法を明記する。

(4) 情報システムセキュリティ責任者は、復号鍵が露呈した場合の対応手順を定めること。
当該手順を定める場合には、以下の項目を含めることが望ましい。

- 復号鍵が露呈した事実の報告先（情報システムセキュリティ責任者又は情報システムセキュリティ管理者等）
- 露呈した復号鍵の使用停止の手順
- 露呈した復号鍵によって復号される情報を他の暗号鍵を用いて再暗号化する手順

【復号鍵のバックアップを定める場合（強化遵守事項）】

(5) 情報システムセキュリティ責任者は、復号鍵のバックアップ又は預託の方法を定めること。
当該手順を定める場合には、以下の項目を含めることが望ましい。

【バックアップの場合】

- 復号鍵のバックアップを実施する者及び手順

【預託の場合】

- 復号鍵の預託者
- 預託者が復号鍵を保管する手順及び場所
- 預託者から復号鍵の正当な利用者への返却手順

補足
復号鍵を紛失すると、当該復号鍵と対になる暗号鍵を用いて作成された暗号文は復号できなくなる。例えば Windows® XP では、復号鍵は、暗号文と同一の内部記録媒体に保存されていることがある。この場合は、内蔵記録媒体が故障等により使用できなったときに、復号鍵をバックアップしていなければ、暗号文自体のバックアップを取得していたとしてもバックアップしてある暗号文を復号することができなくなる。

4.4 端末利用者にかかわる規定の整備

(1) 情報システムセキュリティ責任者は、端末で利用可能なソフトウェア（オペレーティングシステム、アプリケーションのほか、周辺機器を使用するためのドライバソフトウェア等も含む。）を定め、端末を利用する端末利用者に通知すること。
端末で利用可能なソフトウェアは、以下のとおり。

- *［オペレーティングシステム： Windows® XP Professional Version 2002 Service Pack 2］*
- *［ブラウザ：Internet Explorer®］*
- *［アンチウイルスソフトウェア：Norton AntiVirus®，ウイルスバスター®］*
- *［文書作成：Microsoft® Office、一太郎®、Acrobat®］*

補足
上述の端末で利用可能なソフトウェアはあくまで例示であるが、利用可能と定めたソフトウェアについては、セキュリティホール情報を継続的に収集し、これが公開された場合には適切に対処する必要がある。したがって、利用可能と定めるに当たっては、情報システムごとにその必要性を検討し、利用可能なソフトウェアの種類をむやみに増やさないことが望ましい。

また、利用可能と定めたソフトウェアについては、当該ソフトウェアの開発を行った会社等によるセキュリティパッチの提供等のサポートが継続されていることを適宜確認し、継続されていないことが確認できた場合は、サポートが継続されている同種の製品に切り替えることが望ましい。
なお、オペレーティングシステムの機能により利用可能なソフトウェアを制限できる場合は、併せて設定することにより、ソフトウェアの利用を機械的に制限することができるため、これを実施することが望ましい。

(2) 情報システムセキュリティ責任者は、端末の接続を許可する通信回線を定め、端末を利用する端末利用者にこれを通知すること。
端末の接続を許可する通信回線は、以下のとおり。

- *[府省庁LAN]*

補足
通信回線を構成する通信回線装置（ルータ、ファイアウォール等）のセキュリティ機能及び端末のセキュリティ機能が相補的に機能していることにより端末を保護している場合、接続先の通信回線を変更すると通信回線装置のセキュリティ機能と端末のセキュリティ機能にそごが生じ、端末の保護が有効に働かなるおそれがある。このような危険性の発生を防止するため、接続可能な通信回線を定めておく必要がある。またこのとき、通信回線で実施されていないセキュリティ対策が端末で実施されていることを確認する必要がある。

4.5 端末の構成の管理

(1) 情報システムセキュリティ責任者は、端末の周辺機器を含む構成図及びインストール済みのソフトウェア等を記した電子計算機関連文書を整備し、機器の構成等に変更が生じた場合には速やかに当該文書の更新を行うこと。
当該文書には、以下の情報を含めることが望ましい。

- ハードウェア要素
  - 端末の型番
  - 外部記録装置の種別
  - 外部記録装置の接続インターフェイスの種別
- ソフトウェア要素
  - インストールされているソフトウェアの一覧（名称、種別、バージョン）
  - アンチウイルスソフトウェアによる定期検査のスケジュール

5 端末機能の整備

5.1 端末機能にかかわる検討

(1) 情報システムセキュリティ責任者は、端末で要安定情報を扱う場合には、当該端末に求められるシステム性能を将来の見通しも含めて検討し確保すること。

補足
　システム性能とは、CPU 性能、メモリ容量、ハードディスク容量などのハードウェアに関連する性能に関する事項のほか、オペレーティングシステムのサポートの継続に関して開発会社から公表されている予定期間等、端末の利用を継続することに関連する様々な事項を指す。
　例えば、端末のオペレーティングシステムに Windows® を選択する場合、想定される利用期間にわたりセキュリティパッチの提供が行われるか否かが１つの重要な判断要素となる。

(2) 情報システムセキュリティ責任者は、以下の項目についてその必要性を検討し、必要と認められる機能を端末に導入すること。

- 主体認証
  - 利用者がパスワードを定期的に変更しなければ情報システムの利用を継続させない機能
  - 利用者が自らパスワードを設定する機能
  - パスワードの暗号化保存機能
  - パスワード漏洩時の対処（主体認証情報又は識別コードの停止）機能
- アクセス制御（端末利用者に詳細に行わせるか否かの検討も含む。）
- 権限管理
- 証跡管理
- 保証のための対策
- 暗号化機能（暗号化アルゴリズムの検討も含む。）
- 電子署名の付与機能

端末のオペレーティングシステムの機能を利用する方法もあるが、Windows® XP を選択した場合は、「保証のための機能」、「電子署名の付与機能」は標準では装備していないため、いずれかの機能を必要と判断したときは、それらの機能を別途追加する必要がある。

【端末からの盗み見を防止する措置を実施する場合（強化遵守事項）】

(3) 情報システムセキュリティ責任者は、端末を操作中に画面を盗み見られることを防ぐために、盗み見防止のフィルタを装備すること。当該フィルタは、画面の視認角度を狭くする効果が得られる。

【電磁波の漏えいを防止する措置を実施する場合（強化遵守事項）】

(4) 情報システムセキュリティ責任者は、電磁波の漏えいにより情報が盗み取られることを防ぐために、電磁波対策フィルタをディスプレイケーブル等に装備すること。

5.2　端末の設置

(1) 情報システムセキュリティ責任者は、端末の設置場所を安全区域内に定めること。

【端末を移動できない措置を実施する場合（強化遵守事項）】

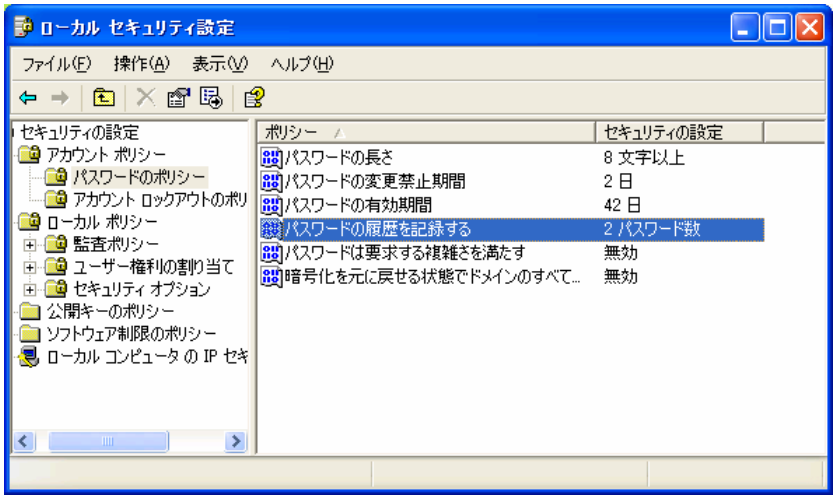
(2) 情報システムセキュリティ責任者は、容易に搬出可能な端末については、ノート

型 PC、デスクトップ型 PC など形状にかかわらず、セキュリティワイヤーによる固定を行うこと。
当該ワイヤーは、切断、破損等が困難な固定物に接続することにより盗難防止の効果が高まる。

(3) 情報システムセキュリティ責任者は、パスワードの変更管理について定めた事項については端末にインストールしたソフトウェアを利用して遵守させることが望ましい。
これにより、権限管理を行う者はパスワードの変更管理について作業を実施する必要がなくなる。

【操作手順】 パスワードの変更管理について Windows® XP に設定する方法

[スタート]→[コントロールパネル]→「パフォーマンスとメンテナンス」→「管理ツール」を選択し、「ローカルセキュリティポリシー」をクリックする。「ローカルセキュリティ設定」のウィンドウにおいて、メニューから「セキュリティ設定」→「アカウント ポリシー」→「パスワードのポリシー」を選択する。パスワードの長さ、有効期間等のポリシーの中で、設定する項目を選択して数値等を設定する。



(4) 情報システムセキュリティ責任者は、端末の内蔵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。
Windows® XP の場合、端末の使用を開始する前から要保護情報の保存が想定されるのであれば、権限管理を行う者が識別コードを発行する際に、端末に作成される「マイドキュメント」フォルダが他の識別コードの端末利用者から読み取られないように、アクセス制御の設定を実施しておくことが望ましい。

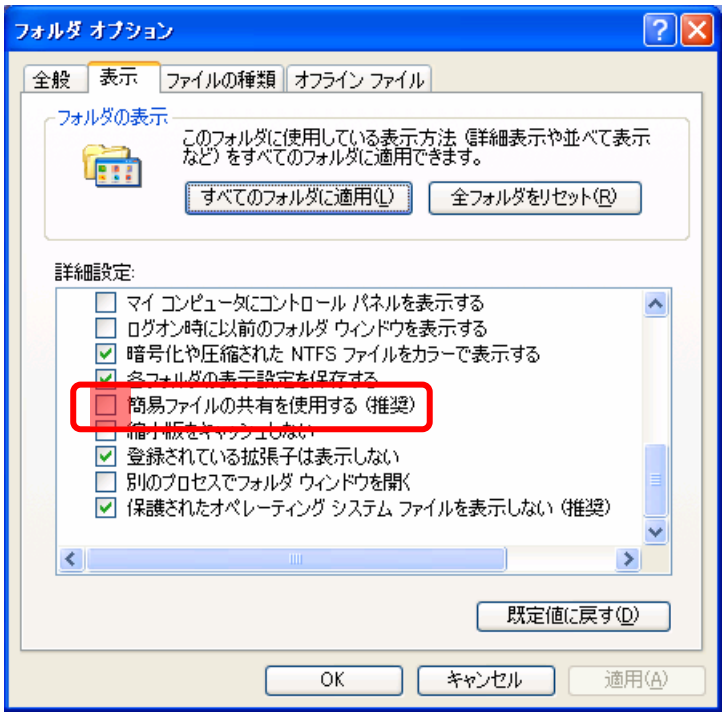
【端末利用者にファイルの詳細なアクセス制御を実施させる場合】

(5) 情報システムセキュリティ責任者は、端末利用者にファイルのアクセス制御を実施させる必要があると思料する場合には、その実施可能な状態に端末を設定すること。

【操作手順】 ファイルの詳細なアクセス制御を可能にさせる設定を行う手順

[スタート]→[コンピュータ]を選択し、表示されたウィンドウにおいて[ツール]→[フォルダオプション]を選択する。さらに表示されたウィンドウにおいて「表示」タブをクリックし、「詳細設定」の中か

ら「簡易ファイルの共有を使用する（推奨）」のチェックを外し、「OK」をクリックする。



(6) 情報システムセキュリティ責任者は、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に付与する識別コードに権限管理を実施すること。

> 補足
> 例えば、利用可能なソフトウェアの実行、セキュリティパッチの適用等に支障がない場合は、管理者権限を付与しない、リモートコンピュータからのアクセスを許可しない等、識別コードに付与する権限を制限しておくことにより、セキュリティインシデントが発生するおそれ又は発生した場合の被害を軽減することができる。
> 権限管理を実施するに当たっては、原則として、識別コードごとに業務又は業務上の責務に即して、その遂行に必要となるアクセス権限を付与することになる。ただし、Windows® XP の場合には、「ユーザーグループ」を構成することで、当該グループ内の「ユーザー」（識別コード）をまとめて管理することが可能となることから、情報システムセキュリティ責任者が「ユーザーグループ」ごとにアクセス権限を定め、権限管理を行う者が識別コードを発行する際に、当該識別コードがどの「ユーザーグループ」に属するかを決定する方法を用いることも可能である。

(7) 情報システムセキュリティ責任者は、「Guest」等不要な識別コードは、削除又はオペレーティングシステムの制限により削除できない識別コードについては利用停止にしておくことが望ましい。
また、オペレーティングシステムで標準的に管理者権限が付与されている識別コード（「Administrator」）や管理者権限を持つと類推される識別コード（「root」、「Admin」等）は、外部からの攻撃で狙われやすいため、それ以外の識別コード

に変更しておくことが望ましい。

【操作手順】 識別コードを変更する方法

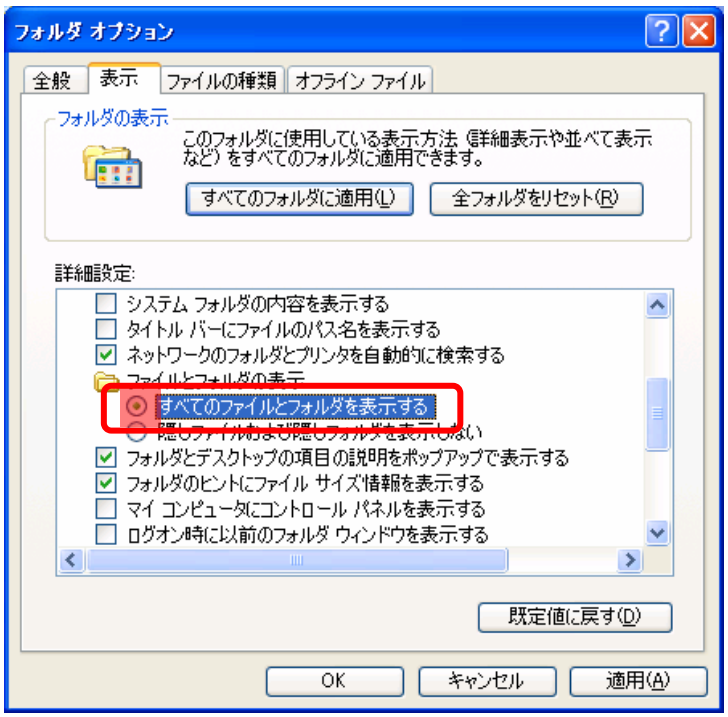
[スタート]→[コントロールパネル]→[パフォーマンスとメンテナンス]→[管理ツール]を選択し、「ローカルセキュリティポリシー」をクリックする。「ローカルセキュリティ設定」のウィンドウにおいて、メニューから[セキュリティ設定]→[ローカルポリシー]→「アカウント: Administrator アカウント名の変更」を選択する。ダイアログに新たに設定する管理者権限を持つ識別コードを入力し「OK」をクリックする。

(8) 情報システムセキュリティ責任者は、アンチウイルスソフトウェアを端末にインストールすること。インストールしたアンチウイルスソフトウェアについては、不正プログラム感染の回避のための日常的実施事項と整合性を保つように、不正プログラム定義ファイルの自動アップデート、不正プログラムの自動検査機能及び不正プログラムの定期的検査についての設定を行うこと。
また、誤操作等により不用意に設定が変更されないように、管理者権限を持つ識別コードにより端末を操作する場合を除き、これらの設定の変更が不可能な状態にすることが望ましい。

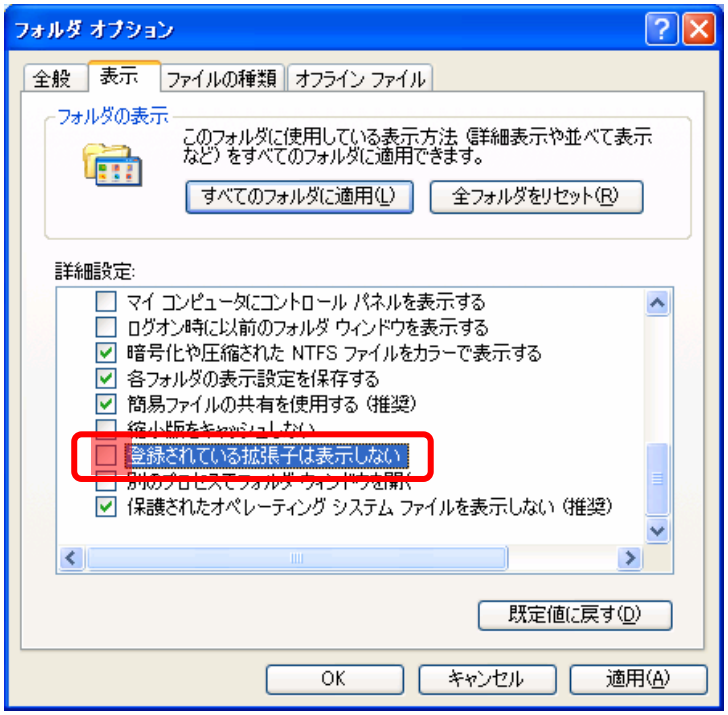
(9) 情報システムセキュリティ責任者は、不正なプログラム、ファイル等の発見を容易にするために、以下のような設定を行うことが望ましい。

【操作手順】 記録媒体に保存されているファイル及びフォルダをすべて表示させる方法

[フォルダオプション]→[ファイルとフォルダの表示]→[すべてのファイルとフォルダを表示する]にチェックを付ける。



[フォルダオプション]→[登録されている拡張子は表示しない]のチェックを外す。



【端末のパスワード・スクリーンセーバの設定を実施する場合（強化遵守事項）】

(10)情報システムセキュリティ責任者は、他者に端末を不正に操作されること及び画面上に表示されている情報を見られることを防ぐために、パスワード・スクリーンセーバが自動起動するように設定すること。
離席してからパスワード・スクリーンセーバが自動起動するまでの時間は、端末に対する不正を防ぐことはできないため、端末の操作を行わなくなってから、*[30]*分以内にすることが望ましい。

【操作手順】パスワード･スクリーンセーバの自動起動の設定手順

Windows® の[スタート]→[コントロールパネル]→[デスクトップの表示とテーマ]→[画面] を選択する。その後、[スクリーンセーバー]のタブをクリックし、「パスワードによる保護」をチェックし、「OK」をクリックする。

【端末の時刻同期を実施する場合（強化遵守事項）】

(11)情報システムセキュリティ責任者は、端末の時刻を他の端末等と同期する必要がある場合には、これを行うこと。

補足 端末の時刻を同期することにより、端末から送信するメールの時刻、証跡を取得した場合に当該証跡の時刻等が統一され、セキュリティインシデント発生時の証跡の解析等が容易になるという効果が得られる。 Windows® XP の端末は、Windows® ドメインに参加している場合は、自動的に同期される。その他の方法としては、端末に NTP(Network Time Protocol)サーバを登録しておくことにより定期的かつ自動的に時刻を同期することが可能になる。

【公開されていないセキュリティホールの対策を実施する場合（強化遵守事項）】

(12)情報システムセキュリティ責任者は、公開されていないセキュリティホール、パッチが提供されていないセキュリティホールについて、これを実施する判断を行った場合には、情報システムセキュリティ管理者に通知し実施させること。

補足 Windows® XP SP2 の場合には、DEP (Data Execution Prevention)というデータ実行防止技術があり、当該技術では、端末のメモリ上のプログラムの実行を制限することにより、バッファオーバーフロー攻撃による不正なプログラムの実行を阻止することが可能になる。ただし、端末の CPU の種別

によって得られる効果が異なることや、端末で利用するアプリケーションソフトウェア等に不具合が発生する場合があるので、CPU の種別や利用するアプリケーションソフトウェア等に応じて、具体的に設定する必要がある。

【閲覧可能なホームページの制限を端末で実施する場合（強化遵守事項）】

(13)情報システムセキュリティ責任者は、閲覧可能なホームページの制限を端末で実施する場合には、コンテンツフィルタソフトウェアをインストールし、閲覧制限にかかわる設定を実施すること。
また、当該制限を端末利用者が変更不可能な状態にすることが可能なコンテンツフィルタソフトウェアを利用している場合は、端末利用者が変更不可能な状態にしておくことが望ましい。

6　端末の運用

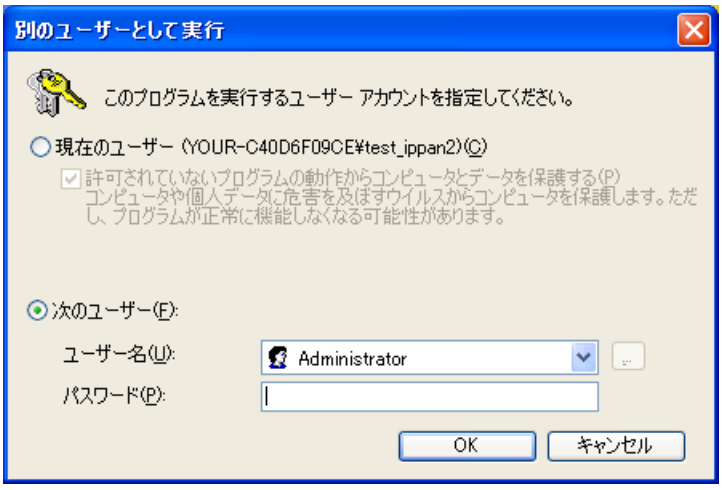
6.1　端末の運用に係る全般的な注意事項

【管理者権限の利用について制限を実施する場合】

(1) 情報システムセキュリティ責任者は、セキュリティ維持のための端末操作その他管理者権限を必要とする場合に限って、当該権限を利用すること。

【操作手順】 利用者権限の識別コードでログインしている最中に管理者権限を必要とする操作を行う方法

コントロールパネルを管理者権限で実行しようとする場合、[スタート]→[コントロールパネル]→[パフォーマンスとメンテナンス]を選択し、[Shift]キーを押しながら[システム]を右クリックしてプルダウンメニューを表示させる。プルダウンメニューから[別のユーザーとして実行]を選択し、表示されたダイアログの「次のユーザー」を選び適切なユーザー名とパスワードを入力して「OK」をクリックする。



6.2　端末運用形態に係る検討

【識別コードの再利用を禁止する場合（強化遵守事項）】

(1) 情報システムセキュリティ責任者は、識別コードの再利用について必要性を判断

し、その結果について権限管理を行う者に通知すること。

6.3　識別コードの発行

(1) 情報システムセキュリティ責任者は、権限管理を行う者にその職務遂行に用いる識別コード及び初期パスワードを発行すること。

6.4　日常の管理作業

(1) 情報システムセキュリティ責任者は、セキュリティホールにかかわる情報について、必要に応じて、他の情報システムセキュリティ責任者と共有すること。

(2) 情報システムセキュリティ責任者は、端末利用者からの報告等によりパスワードが他者に使用され又はその危険が発生したことを認識した場合には、直ちに当該パスワードによる主体認証又はこれに対応する識別コードによる端末の使用を停止させること。

【暗号アルゴリズムの危殆化に関する情報を収集する場合（強化遵守事項）】

(3) 情報システムセキュリティ責任者は、暗号機能を端末で利用する場合、当該機能で使われている暗号アルゴリズムの危殆化に関する情報を適宜収集すること。

> 補足
> 情報の収集は、ソフトウェアの開発会社のホームページのほか、以下のサイトが参考になる。
> CRYPTREC：http://www.cryptrec.jp/

【端末のソフトウェアの状態を定期的に検査する場合（強化遵守事項）】

(4) 情報システムセキュリティ責任者は、端末のソフトウェアの状態を定期的に検査し、利用してはならないソフトウェアがインストールされている、パッチが適用されていないなどの状態を検出した場合には、これを改善すること。

6.5　識別コードの利用停止

(1) 情報システムセキュリティ責任者は、権限管理を行う者が有する管理者権限について、人事異動等により当該権限を行使する必要がなくなった場合には、当該権限を持つ識別コードを無効にすること、又は当該識別コードに付与された管理者権限を行使できなくすること。

6.6　端末の運用終了

(1) 情報システムセキュリティ責任者は、端末の使用を終了する際には、当該端末に保存された情報を復元困難な状態にする必要性の有無を検討し、必要と認めたときは、データ消去ソフトウェア又はデータ消去装置を用いて、当該情報を復元が困難な状態にすること。

《 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

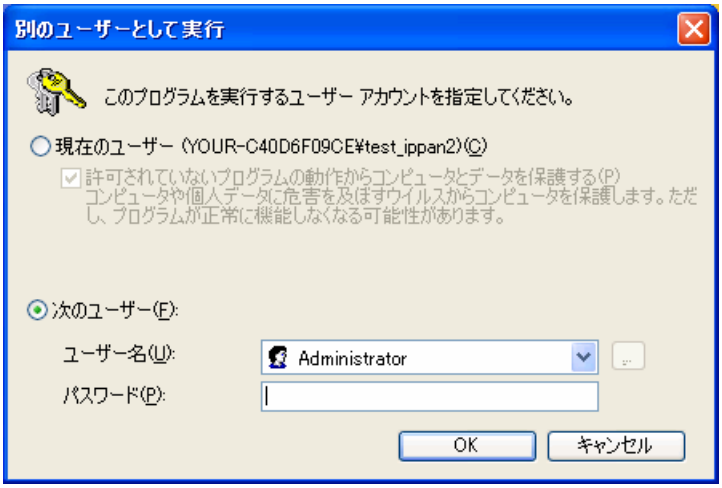
(1) 権限管理を行う者は、権限管理にかかわる規定に基づき、端末の権限管理を実施すること。規定に定められていないことを自己の判断で実施しないこと。
セキュリティ維持等の観点から、規定に定められていない事項を実施する場合は、規定を定めた情報システムセキュリティ責任者に報告、相談等の上これを実施し、規定の改善に努めることが望ましい。

【管理者権限の利用について制限を実施する場合】

(2) 権限管理を行う者は、セキュリティ維持のための端末操作その他管理者権限を必要とする場合に限って、当該権限を利用すること。

【操作手順】 利用者権限の識別コードでログインしている最中に管理者権限を必要とする操作を行う方法

コントロールパネルを管理者権限で実行しようとする場合、[スタート]→[コントロールパネル]→[パフォーマンスとメンテナンス]を選択し、[Shift]キーを押しながら[システム]を右クリックしてプルダウンメニューを表示させる。プルダウンメニューから[別のユーザーとして実行]を選択し、表示されたダイアログの[次のユーザー]を選び適切なユーザー名とパスワードを入力して「OK」をクリックする。



1.2　識別コードの発行

(1) 権限管理を行う者は、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した者に対して識別コード及びパスワードを発行する場合には、初期パスワードについて定められた以下の事項に従い、情報システムセキュリティ管理者に管理者権限のものを、端末利用者に利用者権限のものを発行すること。共用識別コードの利用が許可されている情報システムの場合は、識別コード及び初期パスワードの発行に際して、共用識別コードの必要性の有無を検討し、共用識別コードを発行するか、識別コードを発行するかの決定を行うこと。この場合、特段の理由がない限り、識別コードを個別に発行することが望ましい。また、発行する識

別コードが共用識別コードである場合は、当該識別コード等の発行と併せ、その旨を通知すること。

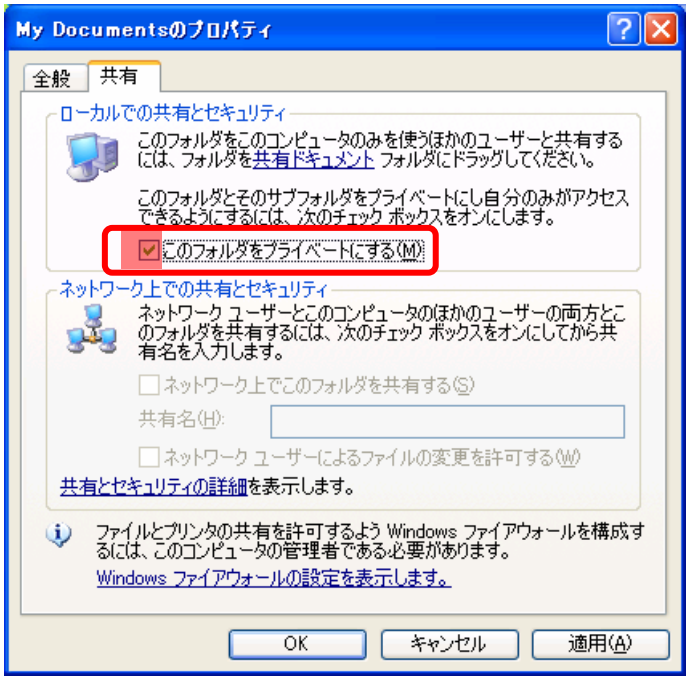
- 初期パスワードについて定められた事項
  - 生成方法：生成ツールにより*[8]*桁のパスワードを生成
  - 通知方法：*[初期パスワードを印刷した紙を封筒に入れ、封筒に氏名、識別コードを記入し、当事者に手渡しする]*
  - 初期パスワード強制変更：*[あり]*

(2) 権限管理を行う者は、端末に識別コードを登録する際にアクセス制御の設定を求められている場合は、当該識別コードが利用する「マイドキュメント」フォルダにアクセス制御の設定を実施すること。

【情報システムセキュリティ責任者が端末利用者にファイルの詳細なアクセス制御を実施させないと判断した場合】

【操作手順】「マイドキュメント」にアクセス制御を実施する方法

登録した識別コードでログインした後、「スタート」→[マイコンピュータ]を選択し、表示されたウィンドウにおいて、[マイドキュメント（又は「"識別コード"のドキュメント」と表示）]を右クリックする。表示されたプルダウンメニューにおいて[共有とセキュリティ]を選択し、開かれたウィンドウにおいて「このフォルダをプライベートにする」にチェックを付け「OK」をクリックする。

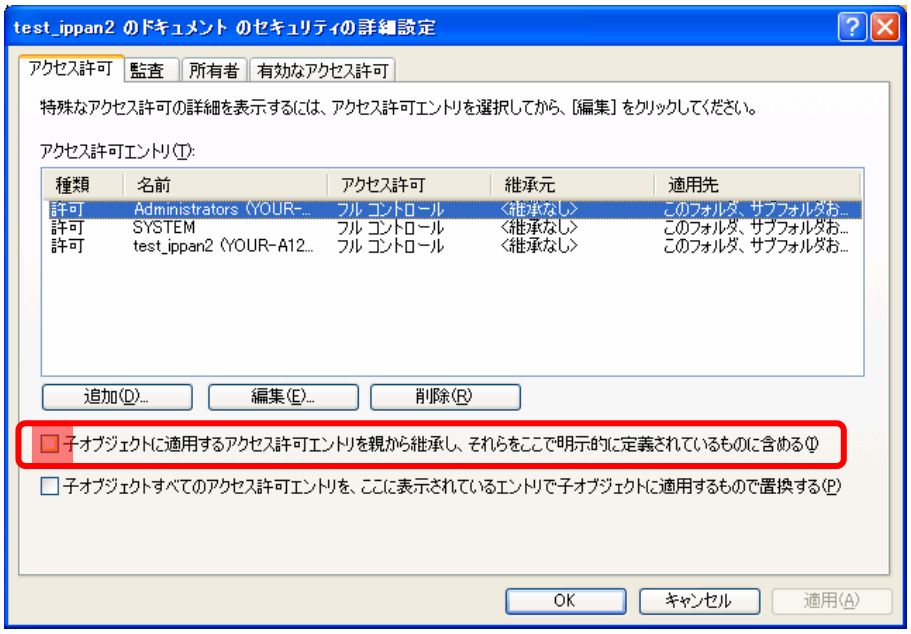


【情報システムセキュリティ責任者が端末利用者にファイルの詳細なアクセス制御を実施させると判断した場合】

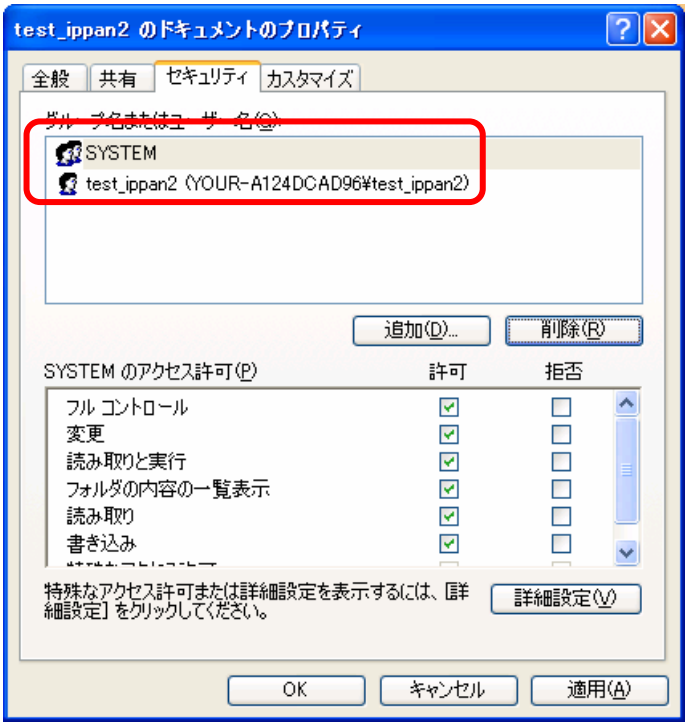
【操作手順】「マイドキュメント」にアクセス制御を実施する方法

[スタート]→[マイコンピュータ]→[ローカル ディスク]→[Documents and Settings]を選択し、表示されているフォルダの中から、設定しようとする識別コードと同じ名称のフォルダを開き、その中から[My Documents]を右クリックし、表示されたプルダウンメニューから[プロパティ]を選択する。表示されたウィンドウにおいて、[セキュリティ]タブを選択した上で[詳細設定]をクリックし、表示されたウィンドウにおいて「子オブジェクトに適用するアクセス許可エントリを親から継承し、それらをこ

こで明示的に定義されているものに含める」のチェックを外す。このとき、「このオプションを選択すると、子オブジェクトに・・・」という旨の警告ダイアログが表示される場合は、[コピー]を選択する。その後「OK」をクリックする。



次に、[グループ名またはユーザー名]から「SYSTEM」及び端末利用者に付与した識別コードを除き、クリックして選択した後に「削除」ボタンをクリックする。

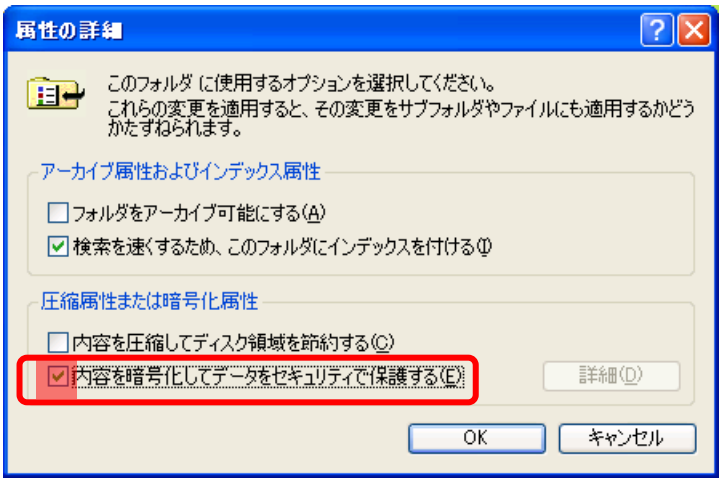


(3) 権限管理を行う者は、ファイルを保存する際に標準的に暗号化が実施される設定とするよう求められている場合には、当該識別コードが利用する「マイドキュメ

ント」フォルダに暗号化の設定を実施すること。

【操作手順】「マイドキュメント」を暗号化する方法

登録した識別コードでログインした後、「スタート」→[マイコンピュータ]を選択し、表示されたウィンドウにおいて、「マイドキュメント（又は「"識別コード"のドキュメント」と表示）」を右クリックする。表示されたプルダウンメニューにおいて「プロパティ」を選択し、開かれたウィンドウにおいて「属性」の「詳細設定」をクリックする。表示されたウィンドウにおいて「内容を暗号化してデータをセキュリティで保護する」にチェックを付け「OK」をクリックする。



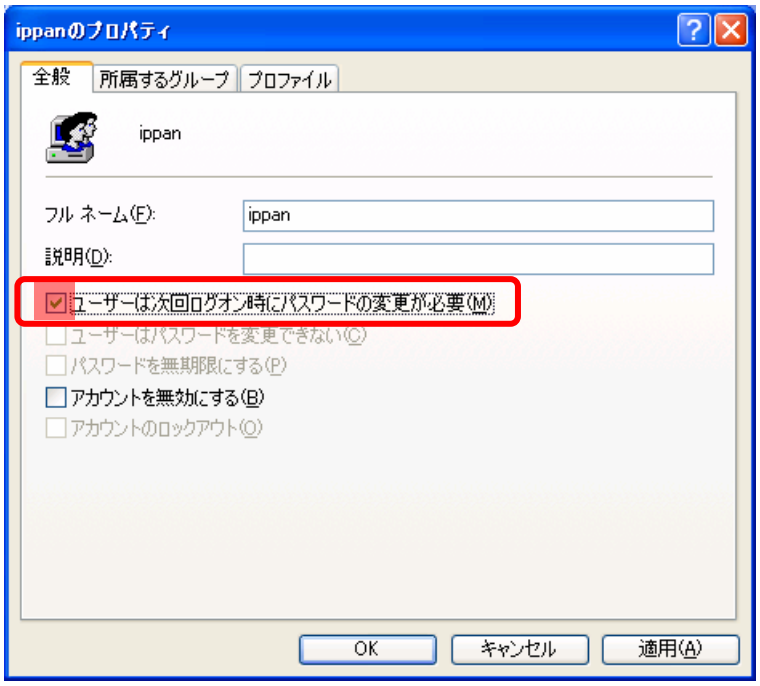
(4) 権限管理を行う者は、パスワードの忘却等により識別コードを使用できなくなった利用者からパスワード初期化の許可申請を受けた場合には、パスワードの初期化の手続及び初期パスワードについて定められた事項に従い、初期パスワードを再発行すること。

<u>【情報システムセキュリティ責任者が、初回ログイン時に初期パスワードを強制的に変更させると判断した場合】</u>

(5) 権限管理を行う者は、識別コードで初回ログインを行った場合に任意のパスワードに変更させるように設定すること。
また、初期パスワードの配布にかかわり初期パスワードを知り得る者が端末を不正に利用することを防ぐため、当該設定及び初期パスワードを使用者だけに通知する方法を併用することが望ましい。

【操作手順】 初回ログイン時にパスワードを変更させるための設定方法

「スタート」→[コントロールパネル]→[パフォーマンスとメンテナンス]→「管理ツール」→「コンピュータの管理」を選択し、表示されたウィンドウの左側に表示されている「コントロールツリー」において「コンピュータの管理（ローカル）」→「ローカルユーザとグループ」→「ユーザー」をクリックする。表示されている識別コードから目的の識別コードを選択し、表示されたウィンドウにおいて「ユーザーは次回ログオン時にパスワードの変更が必要」にチェックを付け、「OK」をクリックする。



【識別コードの発行について記録を保存する場合（強化遵守事項）】

(6) 権限管理を行う者は、端末利用者と付与した識別コードとの対応について、記録を保存すること。当該記録を消去する場合には、情報セキュリティ責任者から消去について承諾を事前に得ること。

【識別コードの再利用を禁止する場合（強化遵守事項）】

(7) 権限管理を行う者は、端末利用者に付与したことがある識別コードを、他の端末利用者に付与しないこと。

> 補足
> 職位等に対応する識別コードが存在し、それを担当者が引き継いで使用する場合など、やむを得ず端末利用者に付与したことのある識別コードをその後他の端末利用者に付与する場合には、識別コードを再利用する場合もあると想定される。ただし、その場合は、パスワードを初期化し、以前に使用していた端末利用者による使用を禁ずるとともに、任意の時点で識別コードを利用していた端末利用者を特定できるように、履歴を管理すること。

(8) 権限管理を行う者は、業務上の責務と必要性を勘案し、必要最小限の権限を付与するよう権限管理を実施すること。

> 補足
> Windows® の場合は、「ユーザーグループ」ごとに権限管理を行うことが可能であり、識別コードの権限管理をより厳しくする制限する必要がある場合には「ユーザーグループ」に割り当てられている権限を制限することにな

る。
例えば、ネットワーク経由でファイル等を他の電子計算機からアクセス可能とする場合、識別コードごとに読み込み、書き込み、実行等の権限を付与することなどが挙げられる。

(9) 権限管理を行う者は、人事異動等に伴って識別コードの追加又は削除を行う際に、不適切なアクセス制御設定の有無を点検すること。

1.3 識別コードの利用停止

(1) 権限管理を行う者は、人事異動等により端末利用者が情報システムを利用する必要がなくなった場合には、当該端末利用者が利用していた識別コードを無効にすること。情報システムセキュリティ管理者が有する管理者権限についても同様に当該権限を持つ識別コードを無効にすること、又は当該識別コードに付与された管理者権限を行使できなくすること。
また、これらの識別コードの無効化を行う場合、同時に不必要な識別コードの有無を点検すること。

《 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

(1) 情報システムセキュリティ管理者は、端末のセキュリティ維持等にかかわる規定に基づき、端末の運用管理を実施すること。規定に定められていないことを自己の判断で実施しないこと。
セキュリティ維持等の観点から、規定に定められていない事項を実施する場合は、規定を定めた情報システムセキュリティ責任者に報告、相談等の上これを実施し、規定の改善に努めることが望ましい。

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

(1) 情報システムセキュリティ管理者は、端末で利用可能として定められたソフトウェアについて、セキュリティホール対策に必要となる機器情報の文書を整備すること。また、機器情報に変更があった場合は、当該文書に反映すること。
文書に記録すべき情報としては、以下の項目が想定される。

- セキュリティホール対策情報の収集対象となるソフトウェアの一覧（名称、種別、バージョン）

(2) 情報システムセキュリティ管理者は、通信回線に接続する端末の識別コードとして*[IP アドレス及び MAC(Media Access Control)アドレス]*、端末の利用者と当該利用者の識別コードとの対応を管理すること。

2.2　識別コードとパスワードの代替措置の管理

(1) 情報システムセキュリティ管理者は、識別コードを付与されている端末利用者から代替手段の使用に関する許可申請を受けた場合は、正当な利用者であることを確認した上で、代替手段を使用することの必要性の有無を検討し、必要があると認めた場合には代替手段を提供すること。代替手段を提供した場合は、その記録を残すこと。

> 補足
> 代替手段としては、当日限り有効とした暫定的な識別コード及びパスワードの提供等がある。

(2) 情報システムセキュリティ管理者は、他者の識別コードを代理利用する旨の申請を受けた場合は、識別コードの割り当てられた本人の事前の了解を得ていることを確認した上で、識別コードの代理利用により実施する業務の継続の重要性を検討し、代理利用の許可を与えること。当該許可を与えた場合は、その理由と利用期間を記録に残すこと。これにより、事後に当該識別コードを実際に使用していた者を特定できるように備えることができる。

3　端末機能の整備

3.1　端末の設定

(1) 情報システムセキュリティ管理者は、端末に保存されるパスワードを容易に知られないように暗号化すること。
暗号化に当たっては、パスワード漏えいの危険性を低減させるため、複数の暗号化手法が選択可能な場合には、より強固な方法を用いることが望ましい。

> 補足
> Windows® XP の場合、パスワードは不可逆の暗号化が行われ電磁的記録媒体に保存されるが、この際利用される不可逆の暗号化は 2 種類ある。このうち、LAN Manager ハッシュ(LM ハッシュ）と呼ばれる方式は、攻撃による破られる危険性が高いため、Windows® 95 又は Windows® 98 のサーバがディレクトリサービスを提供しているネットワーク等、当該方針を用いることにより端末の運用に問題が生ずる場合を除き、停止することが望ましい。

【操作手順】 Windows® XP において LAN Manager ハッシュ（LM ハッシュ)を無効にする手順

「スタート」→「ファイル名を指定して実行」を選択し、「regedit」と入力し「OK」をクリックする。以下のレジストリ キーを見付けクリックする。
レジストリーキー: HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥Lsa
[編集]→[新規]→[DWORD 値] をクリックする。「新しい値#1」と表示された欄に「NoLMHash」と入力し、Enter キーを押す。既に「NoLMHash」が既に存在する場合は、この作業は省略し、「NoLMHash」をクリックする。
[編集]→[修正] を選択し、「値のデータ」欄に「1」と入力して[OK] をクリックする。この変更を有効にするために、コンピュータを再起動し、パスワードを変更する。

4　端末のセキュリティ維持活動

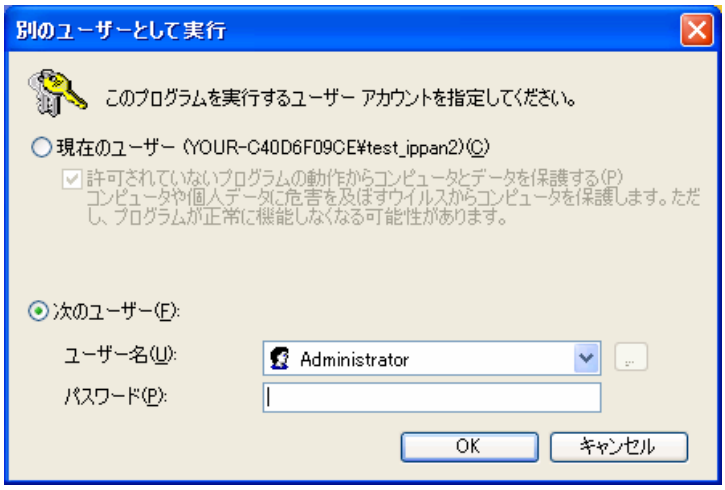
4.1　端末のセキュリティ維持に係る全般的な注意事項

【管理者権限の利用について制限を実施する場合】

(1) 情報システムセキュリティ管理者は、セキュリティ維持のための端末の操作その他管理者権限を必要とする場合に限って、当該権限を利用すること。

【操作手順】 利用者権限の識別コードでログインしている最中に管理者権限を必要とする操作を行う方法

[システム]コントロールパネルを管理者権限で実行しようとする場合、[スタート]→[コントロールパネル]→「パフォーマンスとメンテナンス」を選択し、「Shift」キーを押しながら「システム」を右クリックしてプルダウンメニューを表示させる。プルダウンメニューから「別のユーザとして実行」を選択し、表示されたダイアログの「次のユーザ」を選び適切なユーザ名とパスワードを入力して「OK」をクリックする。



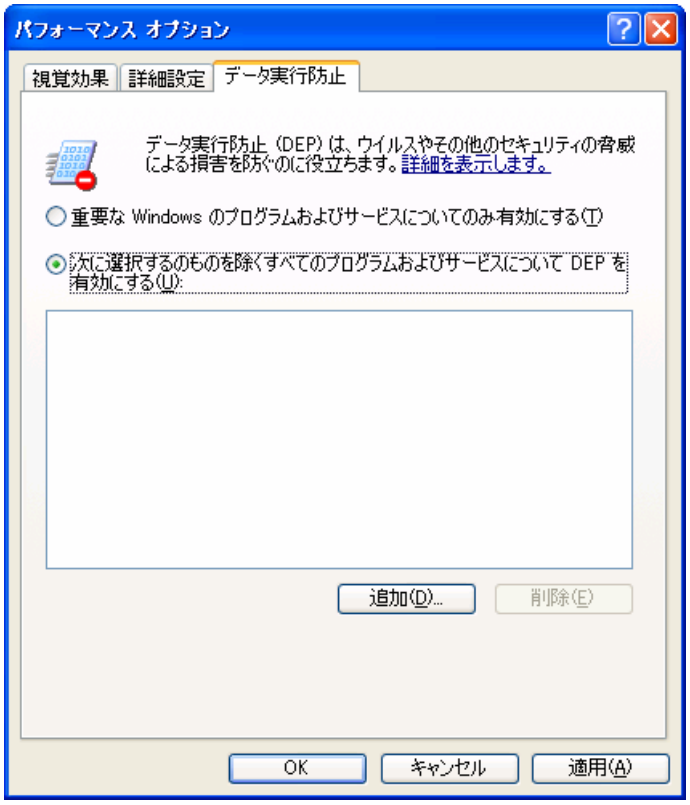
4.2　セキュリティホール対策の実施

【公開されていないセキュリティホールの対策を実施する場合（強化遵守事項）】

(1) 情報システムセキュリティ管理者は、公開されていないセキュリティホール、パッチが提供されていないセキュリティホールについて、情報システムセキュリティ責任者から対策を実施する旨の通知を受けた場合は、これを実施すること。

【操作手順】 ソフトウェア DEP の適用をすべてのプログラムに拡張する方法

[スタート]→[コントロールパネル]→[パフォーマンスとメンテナンス]→[システム]を選択し、表示されたウィンドウの[詳細設定]タブをクリックする。[パフォーマンス]についての[設定]を選択すると、さらにウィンドウが表示される。この中から[データ実行防止]タブを選択し、「次に選択するものを除くすべてのプログラムおよびサービスについて DEP を有効にする」をチェックし「OK」をクリックする。



(2) 情報システムセキュリティ管理者は、端末で利用しているソフトウェアについて、公開されたセキュリティホール情報を収集すること。

補足
情報の収集においては、ソフトウェアを開発した会社のホームページのほか、以下のサイトが参考になる。

- JP Vendor Status Notes：http://jvn.jp/
  経済産業省告示「ソフトウェア等脆弱性関連情報取扱基準」を受けて、日本国内の製品開発者の脆弱性対応状況を公開するサイトとして、有限責任中間法人 JPCERT コーディネーションセンター（JPCERT/CC）と独立行政法人 情報処理推進機構（IPA）が共同で運営しているホームページ
- JPCERT コーディネーションセンター：http://www.jpcert.or.jp/
  インターネットを介して発生する侵入やサービス妨害等のコンピュータセキュリティインシデントについて、日本国内のサイトに関する報告の受け付け、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言などを、技術的な立場から行なっている同法人が運用しているホームページ

(3) 情報システムセキュリティ管理者は、端末におけるセキュリティホール対策の計画に基づき、対策を実施すること。

補足
　ソフトウェアによっては、新しいパッチ提供の有無を自動的に調査し、パッチが提供された場合は自動的にダウンロードした上で適用を行うといった機能が利用可能な場合がある。このような機能は、パッチの適用をもれなく実施可能になる利点がある一方で、適用されたパッチにより不具合が発生する可能性があることから、情報システムの特性に応じて、活用することが望ましい。

【操作手順】 Windows® の「自動更新」によりセキュリティホール対策を設定又は確認する手順

Windows® の[スタート]→[コントロールパネル]→「セキュリティセンター」→[自動更新]を選択し、「自動（推奨）」を選択した上で「OK」をクリックする。又は「自動（推奨）」が選択されている場合は、それを確認し「OK」をクリックする。

(4) 情報システムセキュリティ管理者は、定期的にセキュリティホール対策の実施状況を確認すること。
端末で利用可能なソフトウェアについて、セキュリティホール情報及びパッチ提供の状況の情報を収集し、これに基づいて端末のパッチ適用等の対策状況を調べ、不適切な状態にある端末が発見された場合には是正措置を行うこと。

4.3 不正プログラム対策の実施

(1) 情報システムセキュリティ管理者は、不正プログラムの情報の収集に努め、端末において実施しているセキュリティホール対策、不正プログラム対策等で対処が不足していると判断される場合には、端末利用者に対処について指示や注意喚起を行うこと。

補足
　パッチが提供されていないセキュリティホールを攻撃する不正プログラムが出現した場合であって、利用しているアンチウイルスソフトウェアに定義ファイルが提供されていないときは、当該不正プログラムの感染経路になり得るネットワークの利用を制限すること、セキュリティホールが存在するソフトウェアの利用を制限することなどを実施する。

4.4 識別コードの管理

(1) 情報システムセキュリティ管理者は、端末利用者からの報告等によりパスワードが他者に使用され又はその危険が発生したことを認識した場合には、直ちに当該識別コードの利用を停止すること。

4.5 障害等の対処

(1) 情報システムセキュリティ管理者は、障害等の発生を知ったときには、統括情報セキュリティ責任者が定めた報告手順により、情報セキュリティ責任者にその旨を報告すること。

(2) 情報システムセキュリティ管理者は、障害等が発生した場合、対応手順の有無を

確認しそれを実施できる場合にはその手順に従い、確認できないときには被害の拡大防止に努めること。また、指示があった場合には、その指示に従うこと。

補足 端末が不正プログラムに感染したか又は感染の疑いがある場合には、例えば、直ちに LAN ケーブルを抜くこと等により接続している通信回線から端末を切り離し、通信回線を経由した感染の拡大を防ぐことが必要となる。

《 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) 端末利用者は、端末の運用にかかわる規定に基づき、端末の運用を実施すること。規定に定められていないことを自己の判断で実施しないこと。
セキュリティ維持等の観点から、規定に定められていない事項を実施すると場合は、規定を定めた情報システムセキュリティ責任者に報告、相談等の上これを実施し、規定の改善に努めることが望ましい。

(2) 端末利用者は、行政事務の遂行以外の目的で端末を利用しないこと。

> 補足
> 目的外利用の事例として、以下のような利用が想定される。
>
> - ファイル交換ソフトウェアの利用
> - 娯楽ホームページの閲覧
> - ショッピング、バンキング、オークション等のサービスの利用
> - メールマガジンの受信

(3) 端末利用者は、端末におけるソフトウェアの利用については、許可されているソフトウェアの利用に限ること。利用可能なソフトウェアが定められている場合は、それ以外のソフトウェアを利用せず、利用してはならないソフトウェアが定められている場合は、当該ソフトウェアを利用しないこと。
なお、ソフトウェアの利用には、インストールしてあるソフトウェアを実行することに限らず、フロッピーディスク等の外部記録媒体上にあるソフトウェアを直接実行することも含まれる。

- *情報システムセキュリティ責任者が定めた利用可能なソフトウェア*
  - *［オペレーティングシステム： Windows® XP Professional Version 2002 Service Pack 2］*
  - *［ブラウザ：Internet Explorer®］*
  - *［アンチウイルスソフトウェア：Norton AntiVirus®, ウイルスバスター®］*
  - *［文書作成：Microsoft® Office、一太郎®、Acrobat®］*

(4) 端末利用者は、端末にインストールされているアンチウイルスソフトウェアにより不正プログラムを検知した場合は、アンチウイルスソフトウェアの指示に基づき当該不正プログラムを除去することが望ましい。合理的な理由により当該不正プログラムを除去しない場合、又は不正プログラムが除去できない場合、不正プログラムとして検知される実行ファイルを実行せず、データファイルをアプリケーション等で読み込まないこと。

(5) 端末利用者は、接続許可が与られた通信回線以外に当該端末を接続しないこと。

- 情報システムセキュリティ責任者が定めた接続可能な通信回線
  - *［府省庁LAN］*

補足
　通信回線を構成する通信回線装置（ファイアウォール等）のセキュリティ機能と端末のセキュリティ機能が一体的に機能していることにより端末を保護している場合、接続先の通信回線を変更すると、通信回線装置のセキュリティ機能と端末のセキュリティ機能にそごが生じ、端末の保護が有効に働かなるおそれがあることに留意しなければならない。

(6) 端末利用者は、通信回線への接続許可を受けていない端末を通信回線装置に接続しないこと。

1.2　端末の操作方法

(1) 起動（府省庁で適宜作成されたい。）

(2) ログイン（府省庁で適宜作成されたい。）

(3) ログアウト（府省庁で適宜作成されたい。）

(4) 終了（府省庁で適宜作成されたい。）

(5) バックアップ（府省庁で適宜作成されたい。）

1.3　日常の取扱い

(1) 端末利用者は、退勤時・出張時には端末の電源を切ることが望ましい。
端末の稼働時間を減らすことにより、起動時にのみに実行されるソフトウェアがインストールされている場合に当該ソフトウェアを遅滞なく実行させること等の情報セキュリティを確保するための効果のほか、端末の劣化を防止することも期待できる

(2) 端末利用者は、離席時には、各自が利用している端末をロックすること。
これにより、他者に端末を不正に操作されること及び画面上に表示されている情報を見られることを防ぐことができる。
また、パスワード・スクリーンセーバが自動起動するよう設定になっていない場合は、ロックし忘れた場合に備えて当該設定を実施することが望ましい。離席してからパスワード・スクリーンセーバが自動起動するまでの時間は、端末に対する不正を防ぐことはできないため、端末の操作を行わなくなってから、*[30]*分以内にすることが望ましい。

【操作手順】 端末のロックの設定及び解除手順

設定するときは、Ctrlキーと Altキーを押したまま、Deleteキーを押して、Enterキーを押す。
解除するときは、Ctrlキーと Altキーを押したまま、Deleteキーを押し、パスワードを入力する。

【操作手順】 パスワード･スクリーンセーバの自動起動の設定手順

Windows® の[スタート]→[コントロールパネル]→「デスクトップの表示とテーマ」→[画面] を選択する。その後、[スクリーンセーバー]のタブをクリックし、[パスワードによる保護]をチェックし、[OK]をクリックする。

(3) 端末利用者は、アンチウイルスソフトウェアにおける不正プログラム定義ファイル等を最新に保つこと。
端末の利用を開始した時点から自動的に不正プログラム定義ファイル等を最新化する設定になっている場合はその設定を変更せず、不正プログラム定義ファイル等の最新化が自動的に実施される設定になっていない場合は当該設定を有効にすることが望ましい。

(4) 端末利用者は、アンチウイルスソフトウェアにおいて、不正プログラムの自動検査を行うよう設定すること。

(5) 端末利用者は、アンチウイルスソフトウェアを用いて、端末に対し不正プログラムを *[毎週１回]* は検査するよう設定すること。

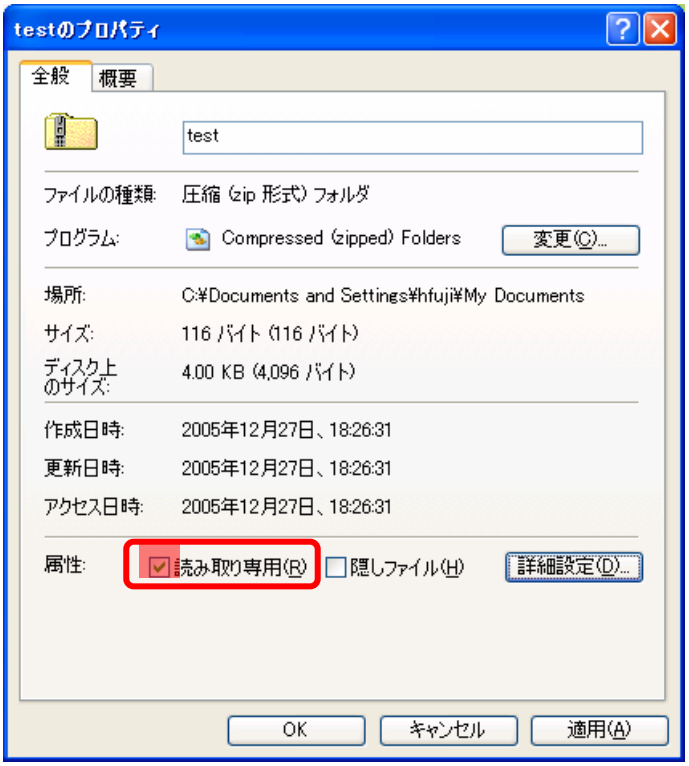
(6) 端末利用者は、利用可能と定められたソフトウェアについては、当該ソフトウェアのセキュリティ機能を活用し、不正プログラム感染等のセキュリティインシデントの予防に努めること。特に、ブラウザ、電子メール等、府省庁外と情報の授受を行うソフトウェアについては重要である。

(7) 端末利用者は、電子ファイルを作成又は入手した場合は、情報の格付け及び取扱制限に従って、当該電子ファイルに対して必要なアクセス制御の設定を行うこと。
Windows® XP を利用している場合、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、Windows® XP では複製禁止とする機能がないため、そのアクセス制御の設定をすることはできない。このように情報システムが備えていない機能については、端末利用者が取扱上注意することで、情報の格付け及び取扱制限の指示を遵守することになる。

【情報システムセキュリティ責任者が端末利用者にファイルの詳細なアクセス制御を実施させないと判断した場合】

【操作手順】 読み取り制限の手順

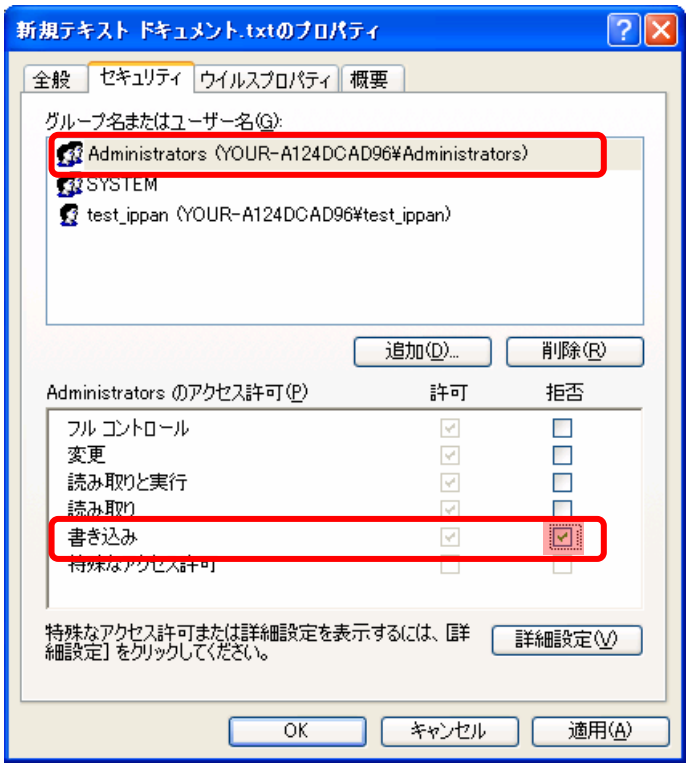
読み取り制限を付与したい対象のファイルを選択し、右クリックでプルダウンメニューを表示させる。この中から「プロパティ」を選択し、属性の「読み取り専用」にチェックを付け、「OK」をクリックする。



【情報システムセキュリティ責任者が端末利用者にファイルの詳細なアクセス制御を実施させると判断した場合】

【操作手順】 書き込み制限の属性の付与の手順

書き込み制限を付与したい対象のファイルを選択し、右クリックでプルダウンメニューを表示させる。この中から「プロパティ」を選択し、表示されたウィンドウの中から「セキュリティ」タブをクリックする。「グループ名またはユーザー名」から制限を実施した識別コードを選択し、その識別コードに対して実施したい項目にチェックを付け、許可したい事項のチェックを外し、「OK」をクリックする。下記の例では、「Administrators」というグループに対して、「書き込み」を制限している。



(8) 端末利用者は、外部記録媒体を他者に提供する場合には、保存されたことがある情報を復元が困難な状態にすることの必要性の有無を検討し、必要と認められるときは、データ消去ソフトウェア等により、残留する要機密情報を最小限に保つこと。

> 補足
> 要機密情報を保存したことがある外部記録媒体を、府省庁外の者に提供する場合には、提供時点において要機密情報が電子ファイルに保存されていない場合であっても、データ消去ソフトウェアにより残留する要機密情報を最小限に保つ必要がある。機密性１情報の情報しか保存したことがない外部記録媒体を他者に提供する場合には、要機密情報の復元を困難にする必要性はない。
> ただし、他者に提供しようとする外部記録媒体が、機密にすべき情報の電子ファイルを保存したことがあるかどうかを区別することが困難な場合には、データ消去ソフトウェアを利用し残留する要機密情報を最小限に保つ必要がある。

(9) 端末利用者は、外部記録媒体を廃棄する場合には、データ消去ソフトウェア若しくはデータ消去装置の利用又は物理的な破壊若しくは電磁的な破壊などの方法を用いて、当該媒体に記録されたすべての情報が復元困難な状態にすること。

> 補足
> 例えば、CD-R 等の光学式の外部記録媒体については物理的な破壊を行

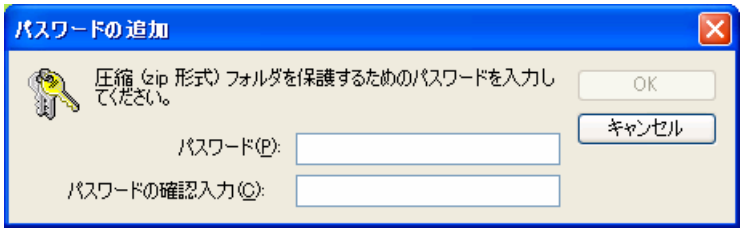
い、USB メモリ等のフラッシュメモリによる外部記録媒体については、当該外部記録媒体が使用可能な状態の場合はデータ消去ソフトウェアによる消去、又は当該外部記録媒体が使用不可能な状態の場合は物理的な破壊を行うなど、適切な方法を選び実施することになる。

1.4 個別機能の利用

(1) 端末利用者は、電子ファイルにパスワードを設定する必要がある場合（要機密情報である電磁的記録を移送する場合等）には、これを実施すること。

【操作手順】 Windows® XP の機能により電子ファイルにパスワードを設定する手順

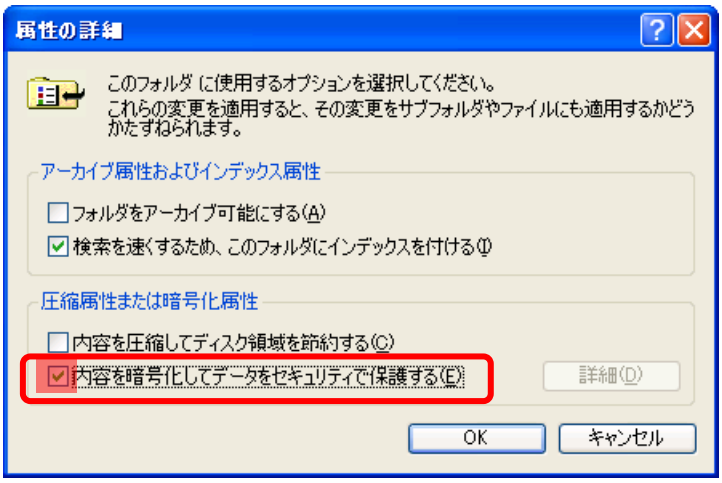
対象のファイルを選択し、右クリックによりプルダウンメニューを表示させる。この中から「送る」→「圧縮（zip 形式）フォルダ」を選択し、ZIP と呼ばれる形式に対象ファイルを圧縮する。その後、できあがった zip 圧縮ファイルをダブルクリックして開き、「ファイル」メニューから「パスワードの追加」を選択し、パスワードを入力し「OK」をクリックする。



(2) 端末利用者は、電子ファイルを暗号化する必要がある場合（要機密情報である電磁的記録を移送する場合、保存する場合等）には、これを実施すること。

【操作手順】 Windows® XP の機能により電子ファイルを暗号化して保存する手順

対象のファイル又はフォルダを選択し、右クリックによりプルダウンメニューを表示させる。この中から「プロパティ」を選択し表示されたダイアログから「属性」の「詳細設定」をクリックする。表示されたダイアログにおいて「内容を暗号化してデータをセキュリティで保護する」にチェックを付け、「OK」をクリックする。



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

(1) 端末利用者は、端末を使用する場合、当該端末で利用可能な他者の識別コードがあったとしても、それを利用しないこと。
自己に付与された識別コード以外の識別コードを使って、情報システムを利用することは、なりすまし行為であることを認識する必要がある。仮に、悪意がない行為であっても、他者の識別コードを使って情報システムを利用することを、独自の判断で行わないこと。

(2) 端末利用者は、自己の識別コードを他者に付与及び貸与しないこと。共用する識別コードについても情報システムセキュリティ管理者から各本人に個別に付与されるものであり、それを他者に付与及び貸与しないこと。

(3) 端末利用者は、自己の識別コードを不必要に知られるような状態で放置しないこと。例えば、付箋に書きディスプレイに張ること等を行わないこと。

2.2　識別コードの利用開始

【情報システムセキュリティ責任者が、初回ログイン時に初期パスワードを強制的に変更させると判断した場合】

(1) 端末利用者は、端末の初回ログイン時に、パスワードの変更を求めるメッセージが表示された場合は、メッセージに従いパスワードを変更すること。

【情報システムセキュリティ責任者が、初回ログイン時に初期パスワードの強制的な変更を行わないと判断した場合】

(2) 端末利用者は、識別コードの利用を新たに開始する場合は、自己に付与されている識別コードについての初期パスワードを変更すべきである。

> 補足
> 初期パスワードは端末の設定を実施した者が知っており、その他にも初期パスワードが端末利用者に配布される作業の途中において誰かに知られている可能性があることから、識別コードを付与された者になりすまして端末を利用するおそれがあり、これを防止するために変更すべきである。

【操作手順】パスワードを変更する手順

Windows® XP の画面において、Ctrlキーと Altキーを押したまま、Deleteキーを押し、「パスワードの変更」をクリックする。

2.3　識別コードの日常の取扱い

(1) 端末利用者は、定期的にパスワードの変更を行うこと。
パスワードの有効期限が設定されている場合、設定した期間が過ぎるとパスワードの変更を求めるメッセージが表示される。この場合は、メッセージに従いパスワードを変更する。

【操作手順】パスワードの変更手順

*Ctrl*キーと*Alt*キーを押したまま、*Delete*キーを押して、*パスワードの変更*キーをクリックする。その後、「古いパスワード」にその時点で設定されているパスワードを入力し、「新しいパスワード」及び「新しいパスワードの確認入力」に変更したいパスワードを入力し「OK」をクリックする。

(2) 端末利用者は、パスワードについては、以下の管理を徹底すること。

- パスワードの長さ：*[8]*桁以上
- パスワード変更禁止期間：*[2]*日
- パスワードの有効期間：*[40]*日
- 同一パスワードの利用禁止回数：*[2]*回

(3) 端末利用者は、設定するパスワードについて、他者から容易に推測されることがないように、以下の点に留意すること。

- ２つ以上のアルファベットと１つ以上の非アルファベットを含める。
- ４つの異なる文字を含める。
- 辞書にある言葉や一般的な言葉を単独で使用しない。

【識別コードの利用停止を届けさせる場合】

2.4　識別コードの返却

(1) 端末利用者は、自己に付与された識別コードを利用する必要がなくなった場合には、情報システムセキュリティ管理者に届け出ること。

3　端末利用にかかわる手続

3.1　パスワードの初期化申請

(1) 端末利用者は、パスワードを忘却したこと等により識別コードによるログインができない場合には、権限管理を行う者にパスワードの初期化を依頼することができる。

3.2　パスワードの露呈の報告

(1) 端末利用者は、パスワードが他者に使用され又はその危険が発生した場合には、直ちに情報システムセキュリティ責任者又は情報システムセキュリティ管理者にその旨を報告すること。

3.3　障害等の対処

(1) 端末利用者は、障害等の発生を知ったときには、統括情報セキュリティ責任者が定めた報告手順により、責任者等にその旨を報告すること。

(2) 端末利用者は、障害等が発生した場合、対応手順の有無を確認しそれを実施できる場合にはその手順に従い、確認できないときには被害の拡大防止に努めること。また、指示があった場合には、その指示に従うこと。

補足

例えば、端末が不正プログラムに感染したか又は感染の疑いがある場合には、直ちにLANケーブルを抜くこと等により接続している通信回線から端末を切り離し、通信回線を経由した感染の拡大を防ぐことが必要となる。

4　本手順に関する相談窓口

(1) 端末利用者は、緊急時の対応又は本書の内容を超えた対応が必要とされる場合には、情報システムセキュリティ責任者に相談し、指示を受けること。

(2) 端末利用者は、本書の内容について不明な点又は質問がある場合には、情報システムセキュリティ管理者に連絡し、回答を得ること。