DM5-04-062

別紙１

モバイルＰＣの利用手順

雛形

2005 年 12 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、府省庁外でモバイル PC を利用する場合の手順を作成する場合の雛形であり、「モバイル PC 利用手順　策定手引書」2 の実施手順に記載すべき事項を、3 の文書構成例の枠組みの中に盛り込んだものである。

本雛形の利用方法

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。

- 行政事務の遂行において、府省庁外でモバイルＰＣを利用している。
- 業務に利用する機能は、府省庁内と同様のものを利用している。
- 機器、ソフトウエア製品等は次のものを使用している。

ＣＰＵ：Intel® Pentium® 1.20ＧＨｚ
ＯＳ：Microsoft® Windows® XP Professional
メモリ：512ＭＢ
内蔵ＨＤＤ：40ＧＢ
インストールソフトウエア：

① Microsoft® Office 2003 Professional
② 一太郎®2005
③ 電子メールソフト
④ Adobe Acrobat® 6.0 Standard
⑤ ファイル暗号化ソフト
⑥ ＶＰＮクライアント
⑦ ウイルス対策ソフト

使用する環境が上記と異なる場合には、適宜、修正、追加又は削除する必要がある。

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モバイルＰＣ関連の利用手順を作成する手順には、大別して、新規で作成するものと既存の文書を修正するものとがあるが、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（利用するソフトウエア等）やその前提(利用者へ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 手順書中に明記される設定数値（パスワード文字数、容量等）については、府省庁内の定めに合わせる。
③ 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。
④ 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
2005/12/21	初版
2006/4/21	各府省庁意見に基づく修正

目次

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。
- Intel および Pentium は、アメリカ合衆国およびその他の国におけるインテルコーポレーションまたはその子会社の商標または登録商標です。
- 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 Reader 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。
- 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。

1　本書の目的及び対象者

1.1　目的

行政事務を遂行するに当たっては、府省庁外において情報処理を実施する必要が生ずる場合がある。この際、事務を遂行する環境や利用するネットワーク等、府省庁内に比較して物理的な安全対策を講じることが困難になることが多い。

また、府省庁外での事務遂行に当たっては、情報システムセキュリティ管理者等の目が行き届かないことも多いため、府省庁外でのセキュリティの維持に関しては行政事務従事者各個人の行動や意識等への依存度が高くなる。

本書は、上記の状況を考慮し、府省庁外におけるモバイル PC の利用に関する利用手順を提供することを目的とする。

なお、本書は、技術変化・進歩及び法制度の変更に対応し、常に意味あるものにするために、情報システムセキュリティ管理者の指導の下で見直しを行う必要がある。

1.2　対象者

本書は、行政事務の遂行に当たり府省庁外においてモバイル PC を利用するすべての行政事務従事者を対象とする。

＊　行政事務従事者とは、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情報及び情報システムを取り扱う者をいう。

2　利用範囲

モバイル PC を利用する際には、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よって決められた方法及び認められた方法を遵守すること。

なお、府省庁外におけるモバイル PC の接続や機能等に係る利用範囲は、安全性と利便性の双方を考慮した上で、情報システムセキュリティ管理者が設定する。

2.1　利用対象者

(1) 出張等の理由により申請した者のうち、情報システムセキュリティ責任者（又は大臣官房情報システム課）がその必要性を許可した中央合同庁舎△号館在籍の○○省職員に限る。

(2) 申請をする者は、直前 1 年以内に情報セキュリティ対策の教育を受講した職員に限る。

2.2 利用端末

(1) 原則として、貸出端末に限る。

(2) 貸出端末には以下のものを含む。

- ＰＣ本体
- ＰＣ本体用電源
- ＰＨＳカード
- ハードウエア認証キー

（例：ワンタイムパスワード生成カード）

(3) やむを得ない場合の職場端末持出しは、情報システムセキュリティ責任者（又は大臣官房情報システム課）に申請を行い、必要な機能がインストールされていること及び認められていないソフトウエアのインストールや設定がなされていないこと等、貸出端末と同等の状態を確保していることについて確認を受け、当該措置を許可された場合に限る。

2.3 利用機能

モバイル PC において利用できるのは、以下の機能のみとする。

2.3.1 ブラウザ

インターネットに接続（ただし、VPN 接続に限る。）することにより、ホームページを閲覧等する機能

2.3.2 電子メール

府省庁内外のユーザと電子メールを送受信する機能

2.3.3 省内イントラネット（電子掲示板等）

ＶＰＮ接続によりhttp://www.****.go.jpにアクセスし、情報の閲覧等を行う機能

＊ 貸出端末においては、標準ブラウザのホームページに設定されている。

2.3.4 ファイルの利用

省内イントラネットにアクセスすることにより、イントラネット上にあるファイルの利用を行う機能

＊ モバイル PC からのリモートアクセスによる省内ファイルサーバの利用はできない。

2.3.5 ファイルの作成

Microsoft® Office 2003 Professional、一太郎®2005 等によりファイルを作成する機能

2.3.6 ファイルの暗号化

貸出端末にインストールされているファイル暗号化ソフトによりファイルを暗号化する機能

2.4　接続形態

2.4.1　　インターネットへの接続

(1) 行政事務従事者は、貸与されるＰＨＳカード又は公衆電話網を利用し、許可されているアクセスポイントにダイアルアップ接続することで、インターネットへの接続を行うこと。

＊　接続するアクセスポイントは、セキュリティ確保等の観点から、情報システムセキュリティ管理者により限定され、管理されている。

2.4.2　　省内イントラネットへの接続

(1) 行政事務従事者は、貸出端末や個人端末等の種別、選択したインターネット接続の方法にかかわらず、ＶＰＮ接続により府省庁ネットワークに接続すること。

(2) VPN 接続において、行政事務従事者はモバイルＰＣからの安全なリモートアクセスを可能にするためのハードウエア認証キーを使用すること。

2.5　アクセスポイント

2.5.1　　国内

(1) 首都圏：03-****-****、**-****-****

(2) 近畿圏：**-****-****、**-****-****

(3) 北海道：**-****-****、**-****-****

(4) 東北：**-****-****、**-****-****

(5) 中国：**-****-****、**-****-****

(6) 四国：**-****-****、**-****-****

(7) 九州：**-****-****、**-****-****

2.5.2　　海外

(1) 米国：**-****-****、**-****-****

(2) 欧州：**-****-****、**-****-****

(3) アジア：**-****-****、**-****-****

2.6　利用に関する諸条件

2.6.1　　利用期間

(1) １回の利用期間は、原則として最大３０日とする。

(2) 利用期間を過ぎるとモバイルアクセス環境にアクセスできなくなるので、注意すること。

(3) 利用期間延長の必要がある場合には、期間終了時に再申請を行うこと。なお、

利用開始時に３０日を超えることがわかっている場合には、必要な期間に応じた例外措置の適用申請を利用申請と合わせて行うこと。

2.6.2　接続時間

(1) １回の連続接続時間は最大で６０分とする。６０分を経過すると自動的に切断されるので、継続して使用する場合は、再度接続を行うこと。

(2) 無通信状態が 5 分続くと自動的に切断されることになる。

3　端末の管理

3.1　借用時の端末の管理

(1) 利用申請に関しては、下記４項の「利用手続」を参照し、確実に実施すること。

(2) 貸出端末の受取に際しては、同梱されている一覧表「モバイル PC 貸出一式チェックリスト」と実際に借り受ける内容物が一致しているかを確認すること。

(3) 申請の状況については、情報システムセキュリティ責任者により、利用の許可・不許可にかかわらず記録される。

(4) 貸出しを受けるモバイル PC については、情報システムセキュリティ管理者により、セキュリティパッチ及びパターンファイルが最新の状態に保たれている。

3.2　利用中の端末の管理

(1) セキュリティパッチ及びパターンファイルの更新や利用状況等に関し、情報システムセキュリティ管理者から随時確認があるので、その場合には自らの利用状況を確認し、適切に対応すること。

(2) 行政事務従事者に対する確認結果については、情報システムセキュリティ管理者により記録される。

3.3　返却時の端末の管理

(1) 行政事務従事者は、「モバイルＰＣ貸出一式チェックリスト」を用いて、内容物がすべてそろった状態であることを確認の上、返却すること。

(2) 返却の際には、利用期間中に作成したファイルや情報、特に送受信した電子メール等を削除すること。

(3) 行政事務従事者から返却があった場合には、情報システムセキュリティ管理者により、内容物及び設定内容が確認され、返却記録が保管される。

4　利用手続

4.1　利用申請手続

利用申請に当たっては、利用する端末の種別に該当する様式により情報システムセキュリティ責任者（又は大臣官房情報システム課）に申請すること。

その際、旅行命令簿等、業務上必要な理由がわかる書類（写し）を併せて提出すること。

(1) 貸出端末の貸出許可申請

利用開始7日前までに、様式○○－1「モバイルＰＣ貸出許可申請書　兼　返却確認書」により申請すること。

(2) 職場端末の持出許可申請

利用開始7日前までに、様式○○－3「職場端末持出許可申請書　兼　返却確認書」により申請すること。

申請する際には、以下の措置を実施した後、申請書の該当項目に記述すること。

- 持出しを行う端末に保存されている全情報の確認（特に機密情報の有無とその内容の確認）
- 要機密情報の暗号化又は端末からの削除

【参考】なお、個人端末をモバイルPCとして利用する場面も想定できるが、その場合には情報システムセキュリティ責任者が実効性等を考慮し採否を判断した上で、以下のような運用をすることも考えられる。

個人端末の使用許可申請

利用開始7日前までに、様式○○－2「個人端末の業務への使用許可申請書　兼　使用終了確認書」により申請すること。

モバイルPCの使用に必要な設定及び動作確認等を行う必要があるので、利用開始3日前までに、使用する個人端末及び接続通信機器を大臣官房情報システム課に持ち込むこと。

- *個人端末使用における推奨仕様*
  モバイルアクセス環境の利用に個人端末を用いる場合、性能等利便性、セキュリティ確保の観点から以下の仕様を満たしていることを推奨する。
  - ○ *ＯＳ*
    Microsoft® Windows® XP Professional ＳＰ１以降
  - ○ *セキュリティパッチ*
    Windows® Update等により、直近までのWindows®セキュリティパッチが適用されていること。
  - ○ *ハードウエアの仕様*
    ＣＰＵ：Intel® Pentium® 1.20ＧＨｚ以上
    メモリ：256MB以上
    内蔵ＨＤＤ：１ＧＢ以上の空き容量があること
  - ○ *ネットワーク設定*
    接続通信機器（ＰＨＳカード等）によるダイアルアップ接続が可能な状態に設定されていること。
- *個人としての使用情報及びソフトウエアのバックアップ*
  個人端末を利用する場合は、大臣官房情報システム課に持ち込む前に、個人端末内の必要ファイル及び設定内容をバックアップすること。
- *貸出端末と同等の状態の確保*
  個人端末の使用に際しては、大臣官房情報システム課において以下の措置を行ったもののみ使用可能となる。
  - ○ *個人端末からの情報・ソフトウエアの消去*

○ モバイルアクセスに必要なソフトウエアのインストール及び設定

個人端末の使用終了時の措置

モバイル PC の使用が終了した個人端末は、大臣官房情報システム課にいったん持ち込み、ソフトウエアのアンインストール等を実施してもらうこと。

情報システムセキュリティ管理者により、個人端末の情報の消去、ソフトウエアのアンインストール等が実施された後、返却を受けること。

4.2 利用申請の内容

4.2.1 申請に記載されるべき内容

(1) 申請日

(2) 申請者の情報（氏名、所属、連絡先）

(3) 申請理由

旅行命令簿等、業務上必要な理由がわかる書類（写し）の添付を含む

(4) 利用する期間・持出期間

(5) 利用する場所・持出先

(6) 利用する端末等の内容（シリアル No.等を含む。）

4.2.2 申請先

情報システムセキュリティ責任者（又は大臣官房情報システム課長）

4.2.3 申請者

所属する課室長の承認を得た行政事務従事者

4.2.4 申請記録

申請の許可・不許可等にかかわらず、申請内容及び許可・不許可状況、貸出状況等は情報システムセキュリティ責任者により記録される。

4.3 利用終了時の手続

4.3.1 端末返却及び利用終了の確認

(1) 行政事務従事者は、端末の返却及び個人端末の使用終了の際には、速やかに当該様式により所属の課室長及び情報システムセキュリティ責任者（又は大臣官房情報システム課長）に報告すること。

(2) 行政事務従事者からの端末の返却及び使用終了の報告があった場合には、情報システムセキュリティ責任者によりその報告内容及び確認された実態等が記録される。

4.3.2 返却時の措置

(1) 貸出端末の場合

行政事務従事者から貸出端末が返却された場合には、情報システムセキュリティ管理者により以下の事項について確認がなされる。

- 返却された端末等と「モバイルＰＣ貸出一式チェックリスト」の員数がそろっているか
- 返却された端末のWindows®ログオン・パスワードが初期設定に戻されているか
- 返却された端末に行政事務従事者の作成したファイル、情報、電子メール等が残っていないか

なお、返却された端末は、情報システムセキュリティ管理者よる確認を経た後、次の貸出しができる状態にされた上で保管される。

(2) 職場の端末の持出しの場合

行政事務従事者は、持ち出した端末を職場において庁内ＬＡＮ等のネットワークに接続する前に、情報システムセキュリティ管理者の確認を受けること。

5　利用手順及び手順を実施する上で遵守すべき事項

利用に関する主な手順及び当該手順を実施する上で遵守すべき事項は、以下のとおりである。

5.1　起動

5.1.1　電源スイッチの押下及び BIOS パスワードの入力

【利用手順】

(1) 電源スイッチを押下し、BIOS パスワードを入力する。

(2) BIOS パスワードは、貸出時に情報システムセキュリティ管理者から伝える全貸出端末に固定の８桁の文字列を使用する。

＊ BIOS パスワードは、システムの起動に対するアクセス制御を行うためのものである。

＊ 紛失・盗難時等におけるハードディスクの抜取りによるデータ吸い上げの防止には効果がないが、ハードディスク・パスワードの設定は、機種に依存する上に、パスワードを忘れた場合の復旧方法がないことから設定していない。

5.1.2　Windows®ログオン

【利用手順】

(1) Windows®ログオンＩＤ、初期パスワードを入力する。

(2) 任意のパスワードに変更する。

【遵守すべき事項】

(3) Windows®ログオン・パスワードは、貸出時には固定の初期パスワードになっているので、利用に際しては任意の８桁以上の文字列に変更すること。

(4) 返却時には初期パスワードに再変更すること。

5.2　設定内容等の確認（府省庁外での利用開始時）

【遵守すべき事項】

(1) インストールされているソフトウエアのバージョン、前の行政事務従事者の情報が残っていないか等を確認すること。

(2) 問題があると思われる場合には、その状況を情報システムセキュリティ管理者に報告し、指示を受けること。

5.3　ネットワーク接続

5.3.1　　ダイアルアップ接続

【利用手順】

(1) リストに出るアクセスポイントの中から、最も近距離にあると思われるものを選択し、接続する。

5.3.2　　ＶＰＮ接続

【利用手順】

(1) デスクトップにある「ＶＰＮ接続」アイコンをダブルクリックする。

(2) 「ユーザ名」にモバイルアクセス用ＩＤを入力し、「パスワード」にハードウエア認証キーにより生成されたワンタイムパスワードを入力して、「接続」をクリックする。

＊　モバイルアクセス用ＩＤは、○回連続して間違えるとモバイル環境にアクセスできなくなるので、注意すること。

【遵守すべき事項】

(3) 他人によるモバイルアクセス等を防ぐため、端末とハードウエア認証キーは分離して保管すること。

5.4　ウイルスチェック

5.4.1　　パターンファイルの更新

【利用手順】

(1) アンチウイルスソフトのアイコンを右クリックし、「手動アップデートを実行する」をクリックして、パターンファイルを更新する。

【遵守すべき事項】

(2) 本ソフトは、ＶＰＮ接続中にパターンファイルを自動更新する機能を有しているが、モバイルでの利用に当たっては常に最新な状態を保つために、ＶＰＮ接続開始時に手動でアップデートすること。

5.4.2　　ウイルスチェックの実施

【遵守すべき事項】

(1) 行政事務従事者は、毎日の利用開始時及び利用終了時にウイルスチェックを実施すること。

5.5 リモートアクセスによる業務の実施

5.5.1 ホームページ等の閲覧

【遵守すべき事項】

(1) 行政事務の遂行の目的以外で、サイトにアクセスし、ホームページ等を閲覧してはならない。

5.5.2 電子メールの使用

【遵守すべき事項】

(1) 行政事務従事者は、適宜、必要な相手との電子メールの送受信を行うとともに、不要なメッセージは速やかに削除すること。

(2) 電子メールで機密性 3 情報を移送する場合には、課室情報セキュリティ責任者の許可を得ること。

(3) 電子メールで機密性 2 情報を移送する場合には、課室情報セキュリティ責任者に届け出ること。

(4) 電子メールで要機密情報を移送する場合には、ファイルの暗号化等安全確保の対策を講ずること。

(5) モバイル PC の利用においては、貸出端末でデフォルト設定されているメールソフトウエアを使用し、設定の変更（HTML 表示を可能にする設定を含む。）をしないこと。

(6) 本メールソフトでは、「サーバにメッセージを残す」設定となっているが、貸出端末において受信トレイから削除又は移動したときにはサーバ上のメッセージは削除されることになる。

(7) 個人所有のメールアドレスは使用しないこと。個人所有のメールアドレスを用いて電子メールの送受信を行う必要がある場合には、事前に情報システムセキュリティ責任者の許可を得ること。

(8) 電子メール添付用等のファイルへのアクセス制御には、以下の方法があるので、送信する相手の状態、盗聴等の危険性、送信する情報の機密性等を考慮して選択すること。【電子メール添付によるファイル送信時等における盗聴・誤送信の防止】

- ○ 事前の鍵配付による暗号化

  事前に生成した復号用の鍵を配付しておき、その鍵で暗号化することにより、盗聴や誤送信による情報の漏えいを防ぐ方法である。

  この場合、情報共有したい相手の端末に貸出端末と同じ暗号化ソフトが必要となる。○○省 PC－LAN システムの端末を利用している相手には、同じ暗号化ソフトがインストールされているため、省内での情報共有の場合にはこの方法を選択すること。

- ○ パスワード共有による自己解凍型の暗号化

パスワードを共有し、情報を移送したい相手がそのパスワードを入力することにより自己解凍されるよう暗号化する方法である。

この場合、情報共有したい相手の端末に暗号化ソフトは必要なく、○○省以外の人との情報共有に有効である。

ただし、パスワードの管理及び情報を移送する相手へのパスワードの連絡方法には十分に配慮すること。

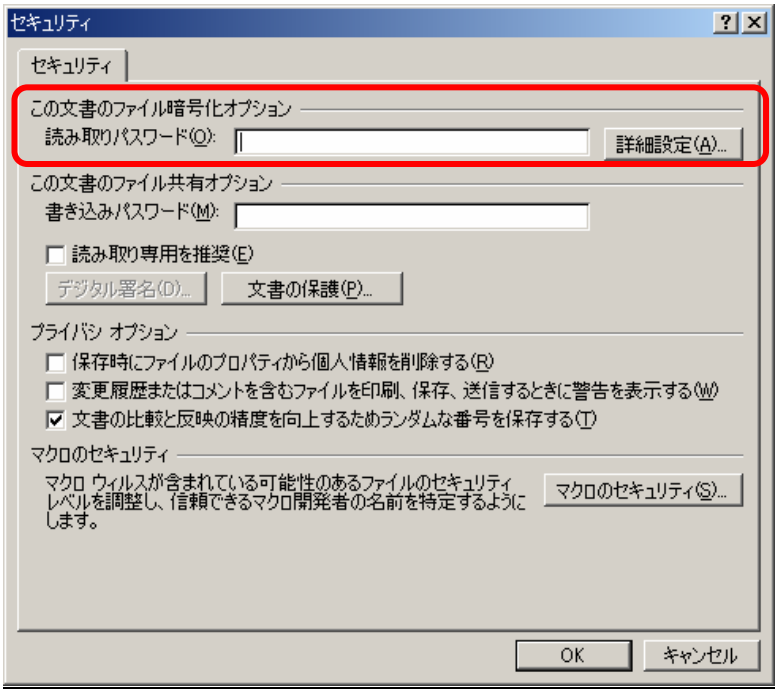
○ ファイルへのパスワード設定

Microsoft　Word 等の標準機能を使ったファイルへのアクセス制御の方法である。

読み取りパスワードについては、あらかじめ受信者と合意した文字列を用いるか、あるいは、電子メールで送信せずに、電話などの別手段を用いて伝達すること

[操作手順] 文書ファイルのパスワードの設定手順（Word の場合）

Word の[ファイル]メニューから[名前を付けて保存]を選択した後、 [ツール]から[セキュリティオプション]を選択し、[読み取りパスワード]を設定する。



あるいは、[ツール]メニューから[オプション]を選択し、[セキュリティ]タブの画面からも同様の設定が可能である。

5.5.3　庁内情報へのアクセス

【利用手順】

(1) ブラウザを起動し、http://www.****.go.jpにアクセスして、可能なサービスを利用する。

【遵守すべき事項】

(2) 省内イントラネットの情報を引用又は利用する情報は、当該情報の格付け及び取扱制限を継承すること。また、当該情報の格付け又は取扱制限を変更する必要性があると思料する場合には、作成者又は入手者に相談すること。

5.6 ファイルの作成

【遵守すべき事項】

(1) 行政事務の遂行の目的以外でファイルを作成してはならない。

(2) 作成した情報は、機密性、完全性、可用性に応じて格付け及び必要性がある場合には取扱制限を行うこと。

(3) 格付け及び取扱制限はその情報を参照する者が認識できる方法で明示すること。

5.7 ファイルの保存

【利用手順】

＊ 貸出端末においてＤドライブに保存したファイルは、シャットダウン時に自動的に暗号化される。【移動時等におけるモバイルＰＣ本体の盗難・紛失対策】

＊ 貸出端末に同梱されているリムーバブルディスクへ保存したファイルは、自動的に暗号化される。【外部記録媒体の盗難・紛失対策】

【遵守すべき事項】

(1) ファイルを保存する際には、暗号化対象フォルダであるＤドライブ又は貸与されているリムーバブルディスクに保存すること。

(2) 個人所有等、貸与されていないリムーバブルディスクの使用は禁止とする。

5.8 ネットワークの切断

【利用手順】

(1) 「ＶＰＮ接続」アイコンを右クリックして、「切断」を選択する。

(2) 「ダイアルアップ」アイコンを右クリックして、「切断」を選択してネットワーク接続を終了する。

5.9 シャットダウン

【利用手順】

(1) ネットワークの切断、各アプリケーションの終了後電源をオフにする。

6 利用時において遵守すべき事項

6.1　パスワードの設定において遵守すべき事項

行政事務従事者は、パスワードを容易に推定されないよう、設定時には以下の事項を考慮すること。

- ８文字以上とする。
- 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む。
- ４つの異なる文字を含む。
- 辞書にある言葉や一般的な言葉を単独で使用しない。
- 以前使用したパスワードを再利用しない。
- 他システムで使用しているパスワードと同一のものを使用しない。

＊　その他詳細は、パスワード運用手引を参照のこと。

6.2　盗難・紛失、情報漏えい等への対策

(1) 府省庁内での取扱いと同様、要保護情報を放置したり、必要以上に複製又は配付しないこと。

(2) モバイルＰＣを保管する場合は、必ず鍵の掛かる場所に保管すること。出張中等、鍵の掛かる場所に保管出来ない場合は、常に携帯するか、目の届くところに置いておくこと。

(3) 公共交通機関等での移動時における盗難防止、置き忘れ防止のため、網棚等に乗せないなど、置き場所に留意すること。

(4) ハードウエア認証キー等リモートアクセスに必要な機器と端末は分けて保管すること。

(5) 貸出端末のＤドライブ内のデータは、シャットダウン時に自動的に暗号化されるよう設定されている。持ち出すファイルや庁舎外で作成したファイルは『マイドキュメント』に保存すること。なお、電子メールデータも同様に自動的に暗号化される。

(6) 府省庁外での利用に際しては、周囲にどのような人がいるか分からないので、離席機会を極力少なくすること。

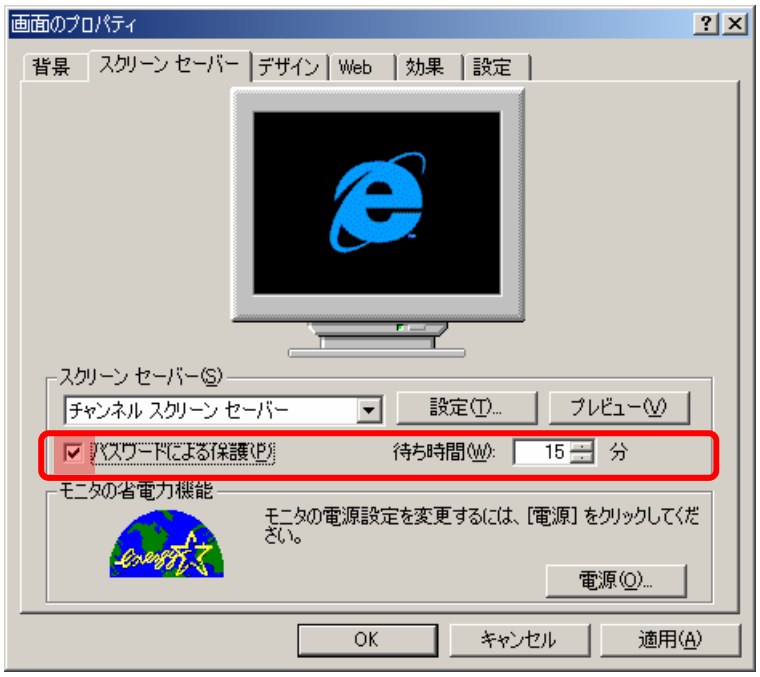
(7) 離席時には、各自が利用している端末をロックすること。また、ロックし忘れた場合に備えて、パスワード・スクリーンセーバが自動起動するように設定しておくこと。

【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]→[設定]→[コントロールパネル] を選択し、[画面]のアイコンをクリックする。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]項目をチェックし、[適用]をクリックし、[OK]をクリックする。



6.3　盗み見等防止への配慮

(1) やむを得ず離席する際には、端末をロックすること。

(2) また、ID やパスワードを入力する際には、周囲に配慮すること。

6.4　禁止事項

(1) 行政事務の遂行以外の目的での情報作成、Web サイトへのアクセス等

(2) 個人で別途契約しているプロバイダ、メールアドレス等の使用

(3) 許可されていないソフトウエア（Winny 等含む。）のインストール

(4) Web アクセス時等におけるセキュリティ設定の変更

モバイル PC の使用においては、端末のセキュリティレベルの低下を防ぐ観点から、原則として設定の変更を禁止する。

【変更を禁止する設定項目の例】

「インターネットオプション」の「セキュリティ」タブの「インターネット」及び「信頼済みサイト」の設定

「インターネットオプション」の「プライバシー」タブの設定

「インターネットオプション」の「詳細設定」タブの設定

7　緊急時の対応等

以下のような緊急時等の場合には、速やかに情報システムセキュリティ管理者に相談し、指示を受けること。

また、本書の内容についての不明な点及び質問は、情報システムセキュリティ管理者に確認すること。

7.1　端末本体又はハードウエア認証キー等を紛失した場合

行政事務従事者は、端末本体又はハードウエア認証キー等の紛失が判明した場合、直ちに情報システムセキュリティ管理者に紛失した状況等を報告の上、その後の対応に関する指示を受けること。

7.2　ウイルスに感染した場合

行政事務従事者は、ウイルスに感染したことが判明した場合、直ちに当該ＰＣの接続しているネットワーク（インターネット、ＶＰＮ等）を切断した上で、情報システムセキュリティ管理者に連絡・相談し、送信先への連絡等も含めて指示を受けること。

7.3　機器の障害等の可能性がある場合

「ホームページが閲覧できない」とか「省内イントラネットに接続できない」といった場合には、例えば以下の項目を確認した上で、ハードウエアの故障なのか、ソフトウエアの設定が間違っているのかなどを判断して対処すること。

どうしてもわからない場合には、大臣官房情報システム課内のサポートデスク（03-****-****）に相談すること。

(1) PC のモデムは正しく認識されているか。

- しっかりと接続されているか。
- モデムは正しく認識されているか。（「コントロールパネル」→「システム」→「ハードウエア」→「デバイスマネージャ」を選択し、「モデム」をダブルクリックして確認する。）
- トーンとパルスの選択は間違っていないか。

(2) ダイアルアップは正しく設定されているか。

- アクセスポイントの電話番号は正しく入力されているか。

(3) ユーザ ID とパスワードは正しく入力されているか。

(4) ブラウザソフトのプロキシ設定は正しく行われているか。

- 使用しているブラウザのバージョンに対応した設定になっているか。

【様式サンプル】

様式○○－3
年　月　日

情報システムセキュリティ責任者	
返却確認印	持出許可印

申請者所属課室長	
返却時　印	持出時　印

職場端末持出許可申請書　兼　返却確認書

1. 以下にて職場端末を庁舎外に持出ししますので、許可願います。

所属・氏名	課・室				
連絡先（内線）					
申請理由					
持出期間	年　月　日　時　～　年　月　日　時				
持出先					
持出する内容	(1)持出する端末等	シリアルNo.			
	①				
	②				
	③				
	(2)持出する情報名称**（原則、情報の持ち出し禁止）**	機密性の格付け（該当欄に○印）			
		3	2	1	
	①				
	②				
	③				
	④				
確認事項	① 持出情報の保存媒体は当省支給のものか？	Yes		No	
	② 持出情報以外の不要情報は全て消去済か？	Yes		No	
	③ 持出情報の暗号化は実施しているか？	Yes		No	
	④ PC起動時のﾊﾟｽﾜｰﾄﾞ設定は実施しているか？	Yes		No	

2. 以下のとおり職場端末を返却しましたので、確認願います。

返却日	年　月　日　時

【申請経路】申請者→所属課室長（申請許可押印）→情報システムセキュリティ責任者（持出許可押印、原紙保管）
【許可通知経路】情報システムセキュリティ責任者（許可済申請書の写し作成）→所属課室長→申請者（写し保管）
【返却確認経路】申請者（写しへの返却日記入）→所属課室長（返却確認押印）→情報システムセキュリティ責任者（押印）
（注1)職場端末とは、PC本体及び付属品及び携帯情報端末の他、FDD、CD-ROM、USB等の電子媒体を含む。
(注2)個人所有のPC等の電子媒体に機密情報等を保存し、持出すること、また持出した機密情報等を個人所有の電子媒体に保管することも厳禁。
（注3）携行時、持出先では盗難、紛失等に十分注意すること。　以 上