DM5-02-061

別紙１：雛形

庁舎内におけるクライアントＰＣ利用手順　電子メール編

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、庁舎内で PC を利用する場合の手順書を作成する場合の雛形であり、「庁舎内における PC 利用手順 電子メール編」２の実施手順に記載すべき事項を、同 3 の文書構成例の枠組みの中に盛り込み作成したものである。

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。

- 電子メールの使用については、既に許可されている。
- 使用する電子メールアドレスについては、既に取得している。
- 電子メールソフトについては、既にインストールしている。
- 行政事務従事者自身がクライアントＰＣの管理者権限を所有している。
- 行政事務従事者自身が電子メールソフトの各種の設定を行っている。
- 以下のソフトウェア製品を使用している。

  OS：Microsoft® Windows® 2000
  電子メールソフト：Microsoft® Outlook® Express 6 (6.00.2800.1123)
  文書作成ソフト：Microsoft® Word® 2002 (10.6764.6735) SP3
  表計算ソフト：Microsoft® Excel® 2002 (10.6501.6735) SP3

そのため、使用する環境が上記の前提と異なる場合には、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電子メール関連の利用手順書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。例えば、行政事務従事者に電子メールソフトのインストールや各種の設定権限が付与されておらず、行政事務従事者による変更が不能である場合には、これらに関する記述を省略する。
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 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
2005/12/21	初版
2006/4/21	各府省庁意見に基づく修正
2006/8/1	表記の統一

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。

目次

1　本書の目的

電子メールは日々の業務において必要不可欠なものになっている。そのため、電子メールは、ルールやマナーを守った安全な方法で使用しなければ、多くの利用者に迷惑をかけることになる。その上、誤った方法による使用は業務の停止や社会的信用を失わせる要因となる可能性もある。

本書は、このようなリスクを軽減し、情報資産を保護し、電子メールの利用に関する基準を提供することを目的とする。

2　本書の対象者

本書は、電子メール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。

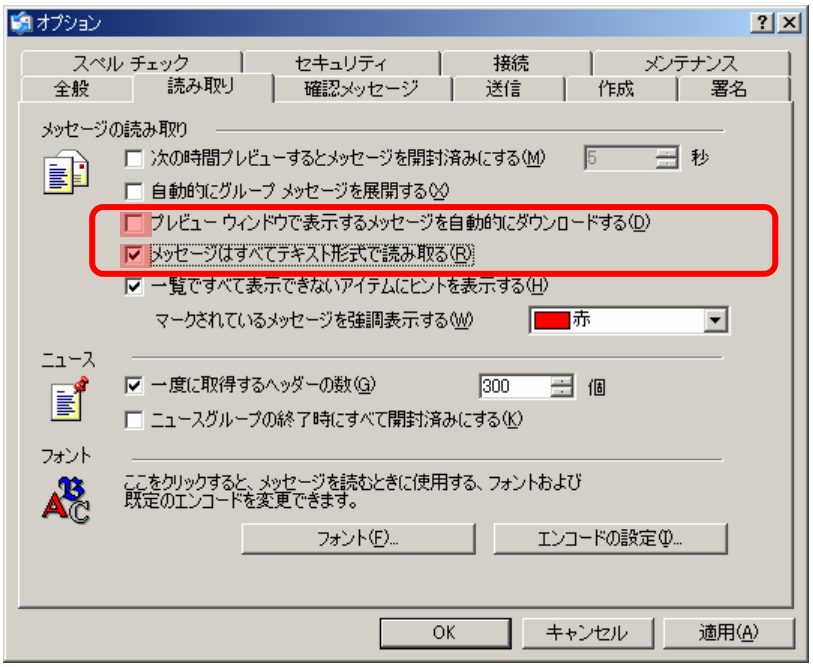
3　電子メールソフトの設定

3.1　電子メール受信に係る設定

(1) 行政事務従事者は、受信した電子メールをテキスト（リッチテキストを含む。）として表示することとし、HTML メールなどの表示による偽のホームページへの誘導や不正なスクリプトの実行を未然に防ぐこと。

［操作手順］ 受信した電子メールをテキスト表示するための設定手順

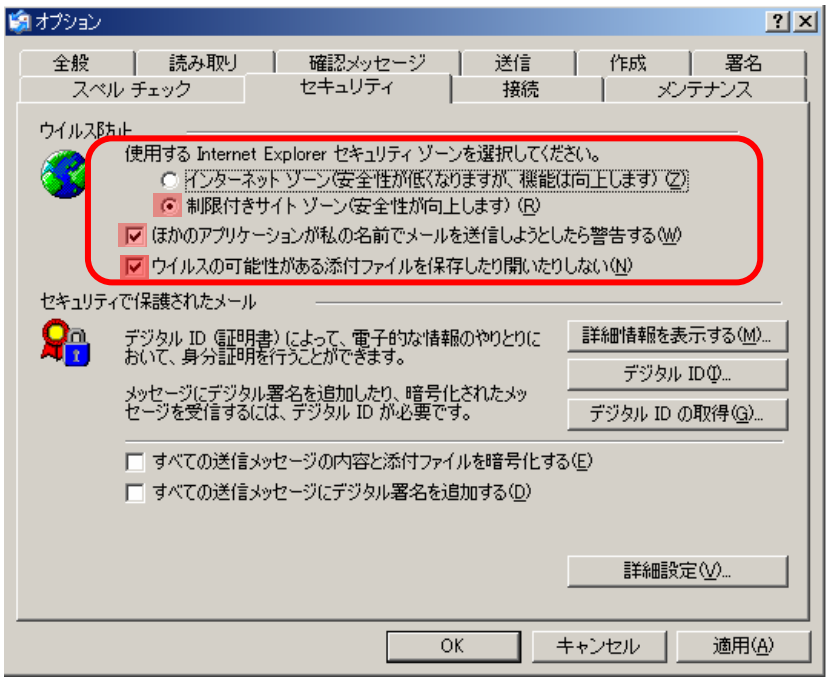
Outlook® Express の[ツール]メニューから [オプション]を選択し、[読み取り]タブの画面において「プレビューウィンドウで表示するメッセージを自動的にダウンロードする」のチェックを外す。また、「メッセージはすべてテキスト形式で読み取る」をチェックする。



(2) 行政事務従事者は、アンチウイルスソフトに加えて、電子メールソフト側においてもウイルス対策が設定可能であれば、これを実施すること。

[操作手順] Outlook® Express 側でのウイルス防止対策の設定手順

Outlook® Express の[ツール]メニューから [オプション]を選択し、[セキュリティ]タブの画面において「使用する Internet Explorer セキュリティゾーン」として「制限付きサイトゾーン(安全性が向上します)」を選択する。また「ほかのアプリケーションが私の名前でメールを送信しようとしたら警告する」及び「ウイルスの可能性がある添付ファイルを保存したり開いたりしない」をチェックする。

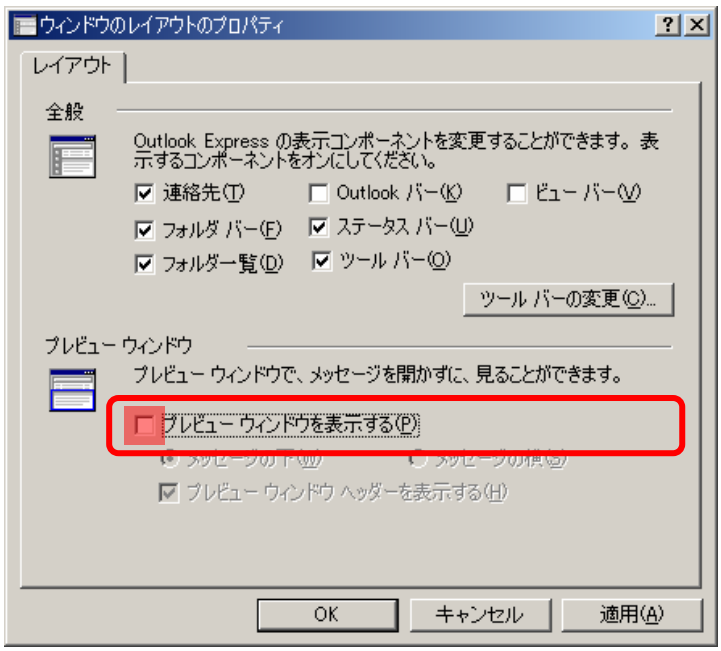


【参考：プレビュー機能を停止することを求める場合】

(3) 行政事務従事者は、プレビュー機能を停止すること。

[操作手順] プレビュー機能停止の設定手順

Outlook® Express の[表示]メニューから [レイアウト]を選択し、以下の画面において「プレビューウィンドウを表示する」のチェックを外す。

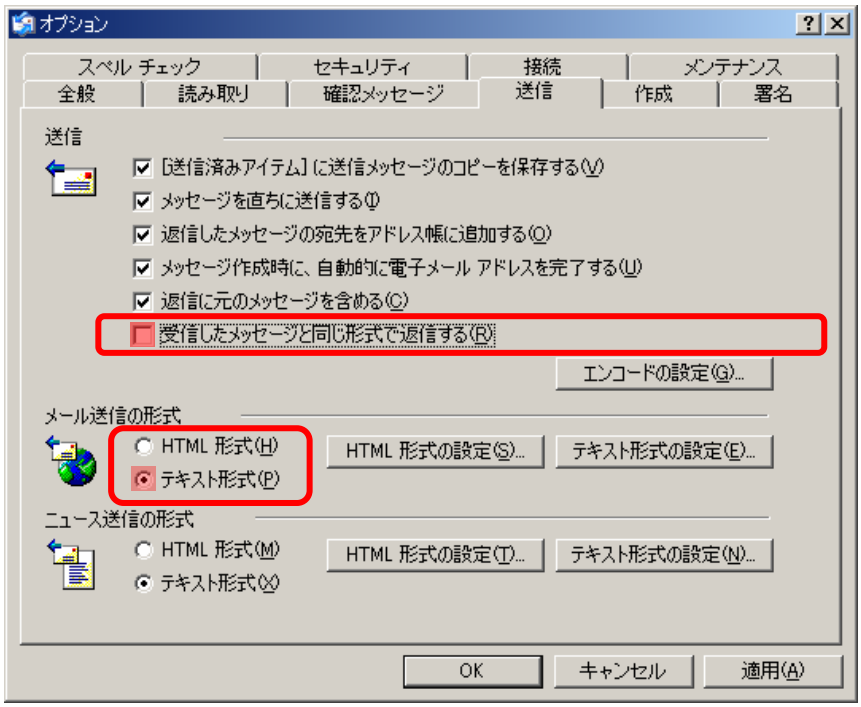


3.2 電子メール送信に係る設定

(1) 行政事務従事者は、原則として、HTML 形式の電子メールを送信しないこと。これは、当方より HTML 形式の電子メールを送信した場合、それを受信した側の情報セキュリティ水準の低下を招くおそれがあるからである。

[操作手順] HTML メールを送信禁止するための設定手順

Outlook® Express の[ツール]メニューから [オプション]を選択し、[送信]タブの画面において「受信したメッセージと同じ形式で返信する」のチェックを外す。また、「メール送信の形式」として「テキスト形式」を選択する。


オプション
スペル チェック
セキュリティ
接続
メンテナンス
全般
読み取り
確認メッセージ
送信
作成
署名
送信
[送信済みアイテム] に送信メッセージのコピーを保存する(V)
メッセージを直ちに送信する(I)
返信したメッセージの宛先をアドレス帳に追加する(O)
メッセージ作成時に、自動的に電子メール アドレスを完了する(U)
返信に元のメッセージを含める(C)
受信したメッセージと同じ形式で返信する(R)
エンコードの設定(G)...
メール送信の形式
HTML 形式(H)
テキスト形式(P)
HTML 形式の設定(S)...
テキスト形式の設定(E)...
ニュース送信の形式
HTML 形式(M)
テキスト形式(X)
HTML 形式の設定(T)...
テキスト形式の設定(N)...
OK
キャンセル
適用(A)

4　電子メールに係る全般的な注意事項

4.1　電子メールの私的利用の禁止

(1) 行政事務従事者は、電子メールシステムを、業務を遂行する上で必要な場合のみ使用することとし、私的目的のために使用しないこと。

4.2　電子メールの自動転送の禁止

(1) 行政事務従事者は、要保護情報を含む電子メールを府省庁外へ自動転送する場合には、情報システムセキュリティ責任者又は課室情報セキュリティ責任者の許可を得ること。

(2) 行政事務従事者は、要保護情報を含む電子メールを府省庁外へ自動転送する必要がある場合には、別途定められた安全管理措置を講ずること。

(3) 行政事務従事者は、要保護情報を含む電子メールを府省庁外へ自動転送する必要性がなくなった場合には、その旨を報告すること。

4.3　府省庁支給以外の情報システム利用の禁止

(1) 行政事務従事者は、業務遂行にかかわる情報を含む電子メールを送受信する場合には、本電子メールシステムを利用することとし、府省庁支給以外の情報システム（個人所有の電子メールアドレス等）を利用しないこと。

(2) 行政事務従事者は、府省庁支給以外の情報システム（個人所有の電子メールアドレス等）を用いて電子メールを送受信する必要がある場合には、情報セキュリティ責任者又は課室情報セキュリティ責任者の許可を得ること。

(3) 行政事務従事者は、府省庁支給以外の情報システム（個人所有の電子メールアドレス等）を用いて電子メールを送受信する必要がある場合には、別途定められた安全管理措置を講ずること。

(4) 行政事務従事者は、府省庁支給以外の情報システム（個人所有の電子メールアドレス等）を用いて電子メールを送受信する必要性がなくなった場合には、その旨を報告すること。

4.4　電子メールの監視

(1) 電子メールシステムの適正な利用のため、その利用状況（あて先、内容、添付ファイル等）について証跡の取得、保存、点検及び分析が行われる可能性がある。行政事務従事者は、その趣旨を理解の上、電子メールの内容に関するモニタリング及び監査を実施していることを認識すること。

4.5　電子メール ID 及び電子メールアドレスの管理

(1) 行政事務従事者は、他人の電子メール ID（メールサーバへのログイン ID。以下同じ。）及び電子メールアドレスを使用しないこと。

(2) 行政事務従事者は、電子メール ID 及び電子メールアドレスを他人と共用しない

こと。

(3) 行政事務従事者は、自己に付与された電子メール ID を、それを知る必要のない者に知られるような状態で放置しないこと。

(4) 行政事務従事者は、行政事務のために電子メールを利用する必要がなくなった場合は、情報システムセキュリティ管理者へ届け出ること。

(5) 特定のサービス、職位、部門単位に付与される電子メール ID 及び電子メールアドレスのように、電子メール ID 及び電子メールアドレスを複数の関係者で共用する、あるいは担当者が引き継いで使用する必要がある場合には、その許可及び設定について情報システムセキュリティ責任者に相談すること。

4.6 ニュースグループ、メーリングリスト等の発信機関への ID 登録の禁止・制限

【例：原則禁止とし、業務上必要なものに限定して許可される場合】

(1) 行政事務従事者は、原則として、ニュースグループ、メーリングリスト等(例えばメールマガジン、Web マガジン、フリーメール等)へのＩＤ登録を行わないこと。

(2) 行政事務従事者は、ニュースグループやメーリングリスト等へのＩＤ登録が業務上必要な場合、情報システムセキュリティ管理者と相談の上、所属部課単位又は代表者名で登録すること。

【例：行政事務従事者の判断にゆだねる場合】

(1) 行政事務従事者は、ニュースグループ、メーリングリスト等(メールマガジン、Web マガジン、フリーメール)へのＩＤ登録は、情報セキュリティ情報のメール配信サービスなど、業務上必要なものに限定すること。

5　パスワードの管理

5.1　クライアントＰＣのログイン管理・電源管理

(1) 行政事務従事者は、クライアントＰＣのログインパスワードを設定すること。

(2) 行政事務従事者は、退勤時・出張時にはクライアントＰＣの電源を切ること。

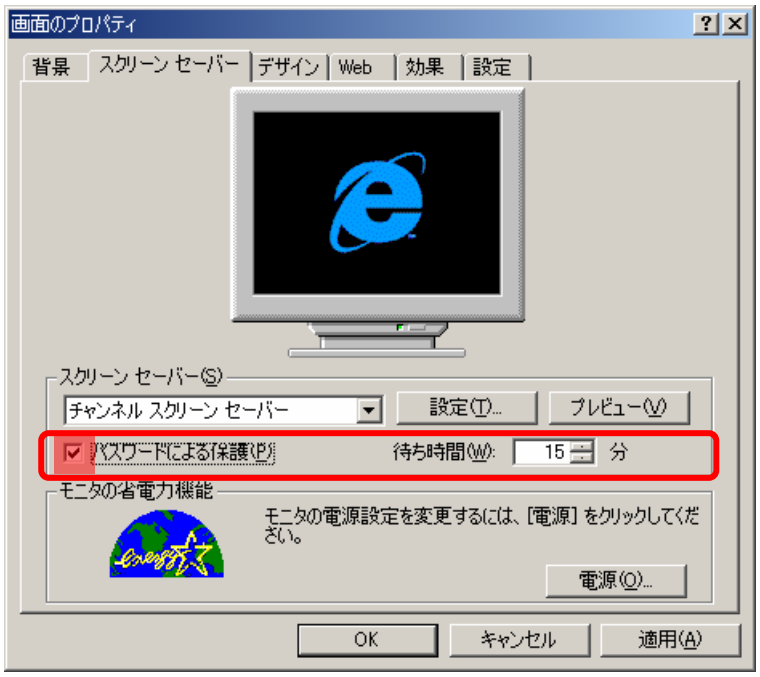
(3) 行政事務従事者は、離席時には、各自が利用しているクライアントＰＣをロックすること。また、ロックし忘れた場合に備えて、パスワード・スクリーンセーバが自動起動するように設定すること。

【操作手順】 クライアントPC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]をチェックし、[適用]をクリックし、[OK]をクリックする。



5.2　電子メールパスワードの管理

(1) 行政事務従事者は、パスワードを設定すること。

(2) 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に、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むこと。

- ４つの異なる文字を含むこと。
- 辞書にある言葉や一般的な言葉を単独で使用しないこと。

その他詳細は、『パスワード運用手引』を参照のこと。

(3) 行政事務従事者は、パスワードを他人に知られないように管理すること。

- 内容が分かる状態で付箋に記入して貼付しないこと。
- パスワード入力時には周囲からの盗み見に注意すること。
- 管理者を名乗ってパスワードを聞き出す等の行為に注意すること。
- 付与された初期パスワードは速やかに変更すること。

(4) 行政事務従事者は、代行処理などのためにパスワードを他人に教えないこと。

(5) 行政事務従事者は、パスワードを忘却しないように努めること。

- 他者が容易に閲覧することができないような措置(施錠して保存する等)をとること。
- 他者が見ても分からないような措置（独自の暗号方式、変換ルール等）をとること。

(6) 行政事務従事者は、定期的に（■か月に１回）パスワードを変更すること。

(7) 行政事務従事者は、パスワードが漏えいしたり、電子メールを他者に使用された場合（その危険性がある場合を含む。）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連絡すること。

(8) 行政事務従事者は、パスワードを忘れた場合には、情報システムセキュリティ管理者に相談すること。

(9) 行政事務従事者は、パスワードを電子メールソフトに永続的に保存しないこと。ただし、電子メールの受信のたびにパスワード入力を行うことが過度に煩雑である場合には、電子メールソフトに一時保存し、クライアント PC 起動後のみパスワード入力とする仕組みを利用してもよい。

(10)行政事務従事者は、パスワードを電子メールソフトに一時保存する場合には、当該パスワードを一時保存するクライアントＰＣを「主体認証情報格納装置」とみなして、以下の点に配慮して安全に取り扱うこと。

- パスワードを保存しクライアントＰＣを本人が意図せずに使用されることのないように安全措置を講じること。
- パスワードを保存しクライアントＰＣを他者に付与及び貸与しないこと。
- パスワードを保存しクライアントＰＣを紛失しないように管理すること。紛失した場合には、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。

6　電子メールの受信

6.1　電子メールの受信確認

(1) 行政事務従事者は、定期的に、電子メールの受信確認を行うこと。

6.2　電子メール添付ファイルのウイルスチェック

(1) 行政事務従事者は、アンチウイルスソフトによる自動ウイルスチェックを実施すること。

(2) 行政事務従事者は、情報システムセキュリティ管理者が自動的にウイルスチェックを実施するように設定している場合又は自動的にウイルスチェック最新データを更新するように設定している場合は、当該設定を変更しないこと。

(3) 行政事務従事者は、受信した電子メールの添付ファイルに対して、随時、ウイルスチェックを行うこと。これは、新種のウイルスに対応したパターンファイルの提供が間に合わず、ファイル受信時のウイルスチェックにおいてウイルスが発見されなかった場合を考慮し、最新のパターンファイルを用いて過去に受信した電子メールの添付ファイルに対してもウイルスの有無を確認するための対策である。

(4) 行政事務従事者は、緊急時対応が必要な時には、情報システムセキュリティ管理者からの指示に従うこと。

6.3　あて先間違いの電子メールを受信したときの対処

(1) 行政事務従事者は、あて先間違いの電子メールを受信し、送信者から正しい受信者へ再度送信する必要がある場合には、可能な範囲で送信者へあて先が間違っていたことを通知すること。

(2) 行政事務従事者は、あて先間違いの電子メールを受信した場合には、これを削除すること。

6.4　不審な電子メールを受信したときの対処

(1) 行政事務従事者は、不審な電子メールを受信した場合には、電子メールを開かず、情報システムセキュリティ管理者に連絡・相談し、指示を仰ぐこと。

(2) 行政事務従事者は、電子メールに不審なファイルが添付されていた場合には、情報システムセキュリティ管理者に連絡・相談し、指示を仰ぐこと。

6.5　ウイルスに感染したときの対処

(1) 行政事務従事者は、クライアントＰＣがウイルスに感染した場合には、直ちに当クライアントＰＣをネットワークから分離し、情報システムセキュリティ責任者に連絡・相談し、指示を仰ぐこと。

6.6　迷惑メールの対処

(1) 行政事務従事者は、必要以上に電子メールアドレスを公表し又は通知しないこと。

(2) 行政事務従事者は、ネットワークを経由して電子メールアドレスを開示し又は通知する場合には、アドレスを自動収集されないように、工夫を施すことが望ましい。(画像情報で貼付する、意図的に全角文字で表示する、無駄な文字列を前後に接続する等)

(3) 行政事務従事者は、送信される迷惑メールに対しては、これを無視することが望ましい。送信者へ停止要求を出した場合、その電子メールアドレスが使用されている事実を伝えてしまう結果となり、かえって迷惑メールが増加してしまう可能性もあるからである。

7 電子メールの作成

7.1 To, Cc 及び Bcc の制限

(1) 行政事務従事者は、To（あて先)、Cc（カーボンコピー）及び Bcc（ブラインドカーボンコピー）の総あて先件数は必要最低限とすること。

- 使用するネットワークリソースは、電子メール１件の使用リソース×総あて先件数である。

(2) 行政事務従事者は、同時に多数の人へ電子メールを送信する場合、Bcc を利用するか、あるいは各自に個別送信する等配慮すること。これは、その場合に電子メールアドレスを To、Cc に列記してしまうと、当該電子メールを受信した者に、他の者の電子メールアドレスが露呈することになるからである。

7.2 電子メール１件当たりのファイル容量の制限

(1) 行政事務従事者は、電子メール本体と添付するファイルを含めた総容量が■■Mbyte を超えないこと。

- 本電子メールシステムでは、送信の際の容量制限を■■MByteとしている。

(2) 行政事務従事者は、電子メール本体と添付するファイルを含めた総容量が■■Mbyte を超える場合、別手段による情報提供や分割送信などについて検討の上、情報システムセキュリティ管理者に相談し、指示を仰ぐこと。

7.3 電子メールの形式の制限

(1) 行政事務従事者は、原則として、HTML 形式の電子メールを送信しないこと。これは、当方より HTML 形式の電子メールを送信した場合、それを受信した側の情報セキュリティ水準の低下を招くおそれがあるからである。

7.4 電子メールの内容

(1) 行政事務従事者は、要機密情報を電子メールで送信する場合は別途定められた安全措置を講ずること。

- 行政事務従事者は、機密性3情報を電子メールで送信する場合には、課室情報セキュリティ責任者の許可を得ること。
- 行政事務従事者は、機密性2情報を電子メールで送信する場合には、課室情報セキュリティ責任者に届け出ること。

- 行政事務従事者は、要機密情報を電子メールで送信する場合には、安全確保に留意して送信手段を決定すること。例えば以下の手段が挙げられる。
    - ○ 外部を経由しないネットワーク(専用線等)
    - ○ 暗号化された通信路(VPN等)
    - ○ 暗号メール(S/MIME等)
- 行政事務従事者は、検討の上決定された送信手段について課室情報セキュリティ責任者へ届け出ること。
- 行政事務従事者は、要機密情報を含む添付ファイルを電子メールで送信する場合には、以下の保護対策の必要性を検討し、必要があると認めたときには、これを実施すること。
    - ○ 添付ファイルに対するパスワード保護
    - ○ 添付ファイルの暗号化(暗号化ソフトの使用等)

(2) 行政事務従事者は、要保全情報を電子メールで送信する場合には、電子署名の付与を行う必要性の有無を検討し、必要があると認めたときには、情報に電子署名を付与すること。

(3) 行政事務従事者は、電子署名の付与に用いた鍵を適切に管理すること。

(4) 行政事務従事者は、他人になりすまして電子メールを作成しないこと。

(5) 行政事務従事者は、電子メールを転送する際に、作成者の許可なく内容の変更をしないこと。

(6) 行政事務従事者は、個人情報やプライバシーの保護を考慮すること。

(7) 行政事務従事者は、次の事項に該当する電子メールの送信を行わないこと。

- 機密保護違反（■■方針・規程を遵守）
- 権利違反（知的財産権、著作権、商標権、肖像権、ライセンス権利等）
- セクシャルハラスメント及び人種問題に関わる内容
- 無礼及び誹謗中傷
- ねずみ講に相当する内容
- 脅迫、個人的な儲け話や勧誘に相当する内容

7.5 ネチケット

(1) 行政事務従事者は、チェーンメール（同じ内容の電子メールを別の人に転送するように要請するもの等）の送信・転送を行わないこと。

(2) 行政事務従事者は、スパムメール（ダイレクトメール等営利目的を主とした無差別に発信された電子メール)、ジャンクメール（役に立たない情報が書かれている電子メール）等を送信しないこと。

(3) 行政事務従事者は、電子メールに題名を付けること。また、題名は電子メールの内容が分かるように具体的かつ簡潔に書くこと。

(4) 行政事務従事者は、俗語的表現やあらかじめ定められていない省略語を使用しないこと。

(5) 行政事務従事者は、機種依存文字コードを使用しないこと。

- 行政事務従事者が判断できない場合には、情報システムセキュリティ管理

者に相談し、指示を仰ぐこと。

(6) 行政事務従事者は、電子メールを作成する際、全角 30 文字以内に改行を入れること。

(7) 行政事務従事者は、To と CC との使い分けを意識し、送信する電子メールに対する返事を要求する時には、To（あて先）を使用すること。

(8) 行政事務従事者は、その他の一般的事項（ネチケット）を考慮すること。

8 電子メールの送信

8.1 送信時の注意

(1) 行政事務従事者は、To（受信者）の記述に誤りがないかを確認してから送信すること。

(2) 行政事務従事者は、電子メールにファイルを添付し送信する際に、ファイルのウイルスチェックを行うこと。

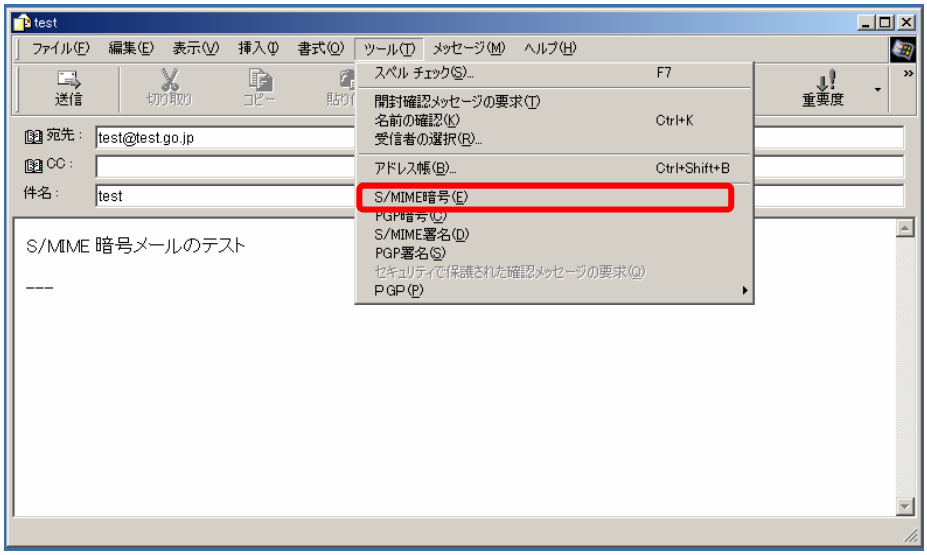
8.2 電子メールの暗号化

(1) 行政事務従事者は、要機密情報を電子メールで送信する場合には、暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化すること。

- 暗号メール(S/MIME等)
- 添付ファイルの暗号化(暗号化ソフトの使用等)

[操作手順] 電子メール（S/MIME）の暗号化手順

Outlook® Express の新規メール作成画面の[ツール]メニューから [S/MIME 暗号]を選択の上、送信する。 なお、送信に先立ち、送り先相手の電子証明書の取得は完了しているものとする。



(2) 行政事務従事者は、暗号化された情報の復号に用いる鍵を適切に管理すること。

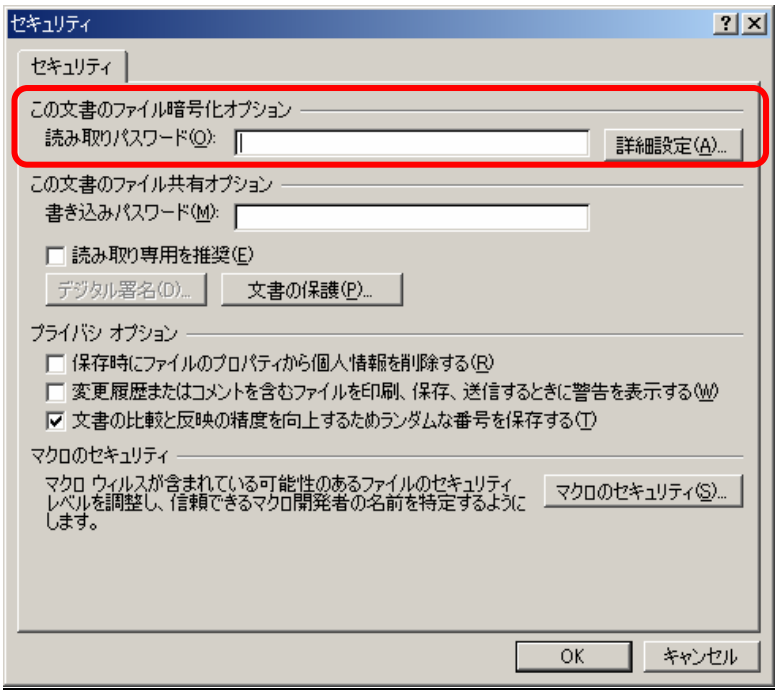
(3) 行政事務従事者は、暗号化された情報の復号に用いる鍵のバックアップを取得しておくこと。

8.3 添付ファイルのパスワード保護

(1) 行政事務従事者は、要機密情報を含む添付ファイルを電子メールで送信する場合には、パスワードを用いて保護する必要性の有無を検討し、必要があると認めたときは、添付ファイルにパスワードを設定すること。

[操作手順] 文書ファイルのパスワードのかけ方(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。

(2) 行政事務従事者は、保護に用いた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。

8.4 電子メール送信時における情報漏えい防止の確認事項

(1) 行政事務従事者は、添付ファイルを電子メールで送信する場合には、当該電子ファイルの付加情報等から不用意に情報が漏えいすることがないか確認すること。

- 「プロパティ」に作成者や修正者等の個人情報が残っていないか
- 一見すると表示されていない部分（「非表示」の設定箇所、非表示とした

コメント、裏に隠れたシート等）に要機密情報が含まれていないか

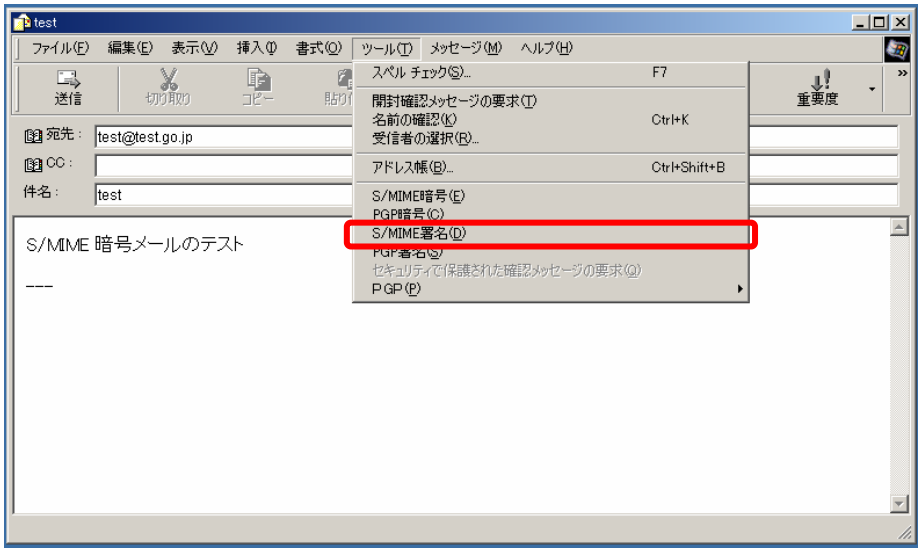
- 変更履歴が必要以上に保存されていないか

8.5　電子メールへの署名付与

(2) 行政事務従事者は、要保全情報を電子メールで送信する場合には、電子署名の付与を行う必要性の有無を検討し、必要があると認めたときには、情報に電子署名を付与すること。

[操作手順] 電子メール（S/MIME）の暗号化手順

Outlook® Express の新規メール作成画面の[ツール]メニューから [S/MIME 暗号]を選択の上、送信する。 なお、送信に先立ち、送り先相手の電子証明書の取得は完了しているものとする。



(3) 行政事務従事者は、電子署名の付与に用いた鍵を適切に管理すること。

8.6　電子メール送信時の受信確認機能の使用制限

(1) 行政事務従事者は、トラフィック増を防止するため、電子メール送信時の受信確認は必要最低限の使用とすること。

8.7　電子メールを誤って送信したときの対処

(1) 行政事務従事者は、電子メールを誤って送信した場合、相手先（受信者）へのフォローは発信者責任で実施すること。

8.8　ウイルスを送信したときの対処

(1) 行政事務従事者は、誤ってウイルスを送信したことが判明した場合、直ちに情報システムセキュリティ責任者に連絡・相談し、相手先（受信者）への連絡等も含めて指示を仰ぐこと。

9　電子メールの保存・削除

9.1　メールボックス（サーバ側）における電子メールの保存・削除

(1) 行政事務従事者は、サーバの個人別メールボックスに格納される電子メールの保存期限や最大容量、バックアップ状況等を考慮の上、適宜、メールボックスから不要な電子メールを削除すること。

- サーバ側の個人別メールボックスに格納される電子メールの最大容量は、■■Mbytesに設定されている。

(2) 行政事務従事者は、サーバの個人別メールボックスに格納される電子メールの保存期限や最大容量、バックアップ状況等を考慮の上、適宜、クライアントＰＣへの保存を行うこと。

- サーバ側の個人別メールボックスに格納される電子メールの保存期限は、■か月に設定されている。

9.2　メールボックス（クライアントＰＣ側）における電子メールの保存・削除

(1) 行政事務従事者は、本文や添付ファイルに要機密情報が含まれている電子メールを保存する場合には、暗号化等の措置を講じた上で保存することが望ましい。

(2) 行政事務従事者は、本文や添付ファイルに要保全情報が含まれている電子メールについては、適宜バックアップすること。

(3) 行政事務従事者は、不要なメッセージは速やかにクライアントＰＣから削除すること。

(4) 行政事務従事者は、本文や添付ファイルに要機密情報が含まれている電子メールを削除する場合には、その機密性に配慮し、復元が困難な状態にすること。

10 本手順に関する相談窓口

(1) 行政事務従事者は、緊急時の対応及び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) 行政事務従事者は、本書の内容について不明な点及び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。