DM5-03-051

別紙１：雛形

庁舎内における PC 利用手順　　ウェブブラウザ編

雛形

2006 年 2 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 ブラウザ編」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盛り込み作成したものである。

本雛形の利用方法

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。

- ウェブブラウザの使用については、既に許可されている。
- ウェブブラウザについては、既にインストールしている。
- 行政事務従事者自身が PC の管理者権限を有していない。
- 以下のソフトウェア製品を使用している。

  OS：Microsoft® Windows® 2000　SP4

  ウェブブラウザ：Microsoft® Internet Explorer® 6 SP1 (6.00.2800.1106)

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ウェブブラウザ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 情報システムセキュリティ責任者及び情報システムセキュリティ管理者のウェブブラウザの利用に関連する実施手順を付録に記載しており、情報システムセキュリティ責任者及び情報システムセキュリティ管理者が対象となっている他の実施手順等との整合性を考慮して分割、統合する。

② 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、行政事務従事者にウェブブラウザのインストールや各種の設定権限が付与されており、行政事務従事者による変更が可能である場合には、情報システムセキュリティ管理者の実施手順の記述を修正し、行政事務従事者の実施手順に追加する。

③ 雛形中に明記される設定値（ウェブブラウザの設定等）については、各府省庁内の方針等に合わせる。

④ 手順書中に、*[・・・]* 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。

⑤ 手順書中に、**【・・・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。

⑥ 既存の実施手順等との整合性を考慮し、適切に雛形を分割、統合、相互参照する。
⑦ 雛形はセキュリティ対策のみを記述したセキュリティの実施手順ではなく、ウェブブラウザの利用手順にセキュリティ対策の要素が含まれている構成を想定して記述されている。ただし、利用マニュアルとしての項目を網羅的に記述しているわけではないため、不足がある場合には、適宜追加する。

改訂履歴

改訂日	改訂理由
2006/2/17	初版
2006/4/21	各府省庁意見に基づく修正

商標について

目次

《 対象：行政事務従事者 》

1　本書の目的

ウェブは、府省庁内における業務システムの利用、情報の伝達や共有だけでなく、府省庁外のニュースサイトや検索サイトの活用等業務の円滑な遂行に必要不可欠なツールとなっている。一方で、業務時間中における私的目的でのウェブの閲覧、掲示板への無断書き込み等、業務効率の低下や府省庁の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、行政事務従事者がウェブを安心・安全に利用するために必要な事項を定めることを目的とする。

2　本書の対象者

2.1　対象者

本書は、ウェブブラウザを利用するすべての行政事務従者を対象とする。

なお、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　ウェブの利用に係る全般的な注意事項

ウェブブラウザを利用した府省庁外のウェブサイトの閲覧、府省庁内の情報システムの利用等、ウェブの利用において、行政事務従事者の安全性を確保し、業務効率を向上させるために、ウェブの利用に係る全般的な注意事項を記述する。

3.1　私的なウェブサイト閲覧の禁止

(1) 行政事務従事者は、業務を遂行する上で必要な範囲でウェブサイトを閲覧するものとし、それ以外で閲覧しないこと。

(2) 行政事務従事者は、府省庁外のウェブサイトを閲覧することにより、府省庁が管理するドメイン名及び IP アドレスから閲覧された記録が閲覧先のウェブサーバに残る点に留意し、業務を遂行する上でのウェブサイト閲覧であっても、慎重に閲覧すること。

【閲覧可能なウェブサイトをコンテンツフィルタリング等により制限する場合（強化遵守事項）】

3.2　閲覧可能なウェブサイトの制限

(1) 適正なウェブ利用を維持するため、コンテンツフィルタリング等により閲覧可能なウェブサイトを制限している。行政事務従事者は、閲覧したいウェブサイトが閲覧制限されている可能性に留意すること。

(2) 行政事務従事者は、コンテンツフィルタリング等による閲覧制限がなされていないウェブサイトであっても、当該ウェブサイトの閲覧が許可されているわけではない点に留意し、業務を遂行する上で必要な範囲でウェブサイトを閲覧すること。

(3) 行政事務従事者は、業務を遂行する上で、制限されているウェブサイトの閲覧が必要な場合には、情報システムセキュリティ管理者に連絡・相談すること。

3.3　プラグイン等の導入・利用の禁止

(1) 行政事務従事者は、情報システムセキュリティ責任者が端末で利用可能と定めていないプラグイン（ウェブブラウザの機能を拡張するためのソフトウェア）等の、端末への導入、利用を行わないこと。

(2) 行政事務従事者は、業務を遂行する上で、情報システムセキュリティ責任者が端末で利用可能と定めていないプラグイン等の導入、利用が必要な場合には、情報システムセキュリティ管理者に連絡・相談すること。

3.4　府省庁外のウェブサイトで提供されているサービスの利用等の制限

(1) 行政事務従事者は、業務を遂行する上で必要のある場合を除き、原則として、掲示板、ブログ等への書き込み、ウェブメールの利用等を行わないこと。

3.5　ウェブサイト閲覧の監視

(1) 適正なウェブ利用を維持するため、その利用状況（いつ、誰が、どのウェブサイトを閲覧したか等）について監査証跡の取得、保存、点検及び分析を行う可能性がある。行政事務従事者は、その趣旨を理解の上、自身のウェブサイトの閲覧がモニタリング及び監査されていることを認識すること。

コラム：政府機関を狙ったフィッシングの注意

2005 年度に、政府職員を装った電子メールに不正プログラムが添付されていた事件、特定の組織を狙ったフィッシング（本物に似せた偽のウェブサイトへ誘導し、入力情報を詐取する手法）や不正プログラム（スパイウェア、ウイルス、トロイの木馬等）の感染が頻発したことから、今後政府職員を攻撃の対象にした同様の攻撃が行われる可能性が高いと考えられる。

政府職員が府省庁外のウェブサイトに情報を送信する機会は多くないため、フィッシングの被害に遭う可能性は低いと考えられるが、個人情報、行政情報等の入力やソフトウェアのインストール等を求める電子メールを受信した場合であって、文面、内容等が不自然なときは、フィッシングや不正プログラムの感染の可能性について留意する必要がある。

4　ウェブサイトの閲覧

ウェブサイトの閲覧に使用するウェブブラウザの利用方法、ウェブサイトを閲覧する場合に想定される脅威を回避するための注意事項等について記述する。

4.1　ウェブサイトを閲覧する方法

（省略）ウェブブラウザの基本的な利用方法を記述

4.2　府省庁内の主要なウェブサイト

（省略）業務の遂行上閲覧する府省庁内外の情報システムの URL と概要を記述

4.3　ウェブサイト閲覧時の一般的な注意事項

(1) 行政事務従事者は、府省庁外のウェブサイトを閲覧する場合には、以下の事項に留意すること。

- ウェブサイトの情報（特に個人が作成しているウェブサイト）には、正しい情報だけでなく偽情報や誤情報が含まれている可能性があるので、ウェブサイトの情報を検討せずそのまま採り入れないこと。
- ウェブページの再読み込みを短時間に繰り返す（「F5」キーを連打する。）と、サービス不能攻撃と見なされる可能性があるので、注意すること。
- 検索サイトでは検索に利用するキーワードによっては、検索結果に有害なウェブサイトへのリンクが含まれている可能性があるので、安易に検索結果のリンク先を閲覧しないこと。

(2) 行政事務従事者は、府省庁内のウェブサイトを閲覧する場合には、以下の事項に留意すること。

（省略）府省庁内のウェブサイトを閲覧する場合の注意事項を記述

4.4　SSL/TLS 通信の確認

(1) SSL/TLS通信とは、通信内容の暗号化及び通信相手のなりすまし対策がなされた安全な通信であり、重要な情報等を送受信するウェブサイトで標準的に利用されている技術である。行政事務従事者は、閲覧している府省庁外のウェブサイトと個人情報、重要な情報等を送受信する可能性がある場合には、SSL/TLS通信が利用されていることを確認すること。確認方法は、「5.2フォームに入力した情報の保護方法」を参照すること。

【ウェブブラウザの設定によりダイアログを表示する設定にしている場合】

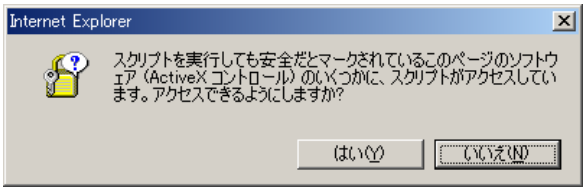
4.5　確認・警告等のダイアログへの対応

(1) セキュリティ機能に係る設定等により確認のためのダイアログ等が表示される可能性がある。当該ダイアログに関して安易に ActiveX®、Java®等のスクリプトの実行を許可すると、不正プログラムの感染、情報漏えい等の危険性があるため、

行政事務従事者は、確認のためのダイアログが表示された場合には、以下のように対処すること。

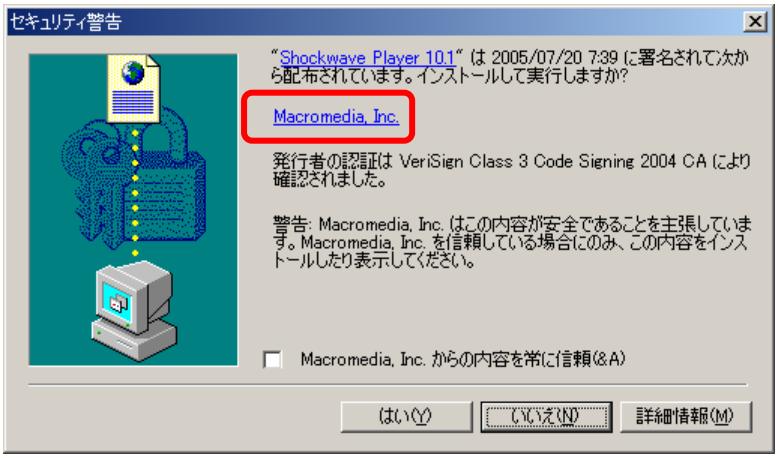
- [スクリプトを実行しても安全だとマークされているActiveX®コントロールのスクリプトの実行]の確認ダイアログの場合には、信頼できるウェブサイト（府省庁内のウェブサイト、著名な検索サイト、著名なニュースサイト等）に限り、許可すること。

[確認ダイアログ] _[スクリプトを実行しても安全だとマークされている ActiveX®コントロールのスクリプトの実行]の確認ダイアログ



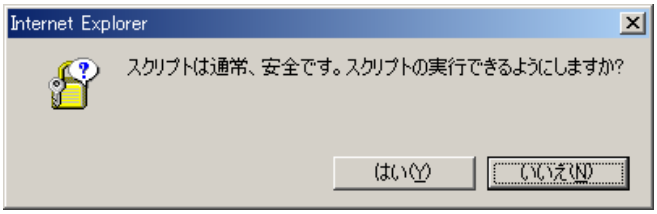
- [署名済みActiveX®コントロールのダウンロード]の確認ダイアログの場合には、表示された発行者の組織名がActiveX®の提供元と同一である場合に限り、インストールして実行を許可すること。なお、当該ActiveX®の利用が許可されていない場合には、インストールして実行しないこと。

[確認ダイアログ] _[署名済み ActiveX®コントロールのダウンロード]の確認ダイアログ



- [Java®アプレットのスクリプト]又は[アクティブスクリプト]の確認ダイアログの場合には、信頼できるウェブサイト（府省庁内のウェブサイト、著名な検索サイト、著名なニュースサイト等）に限り、許可すること。

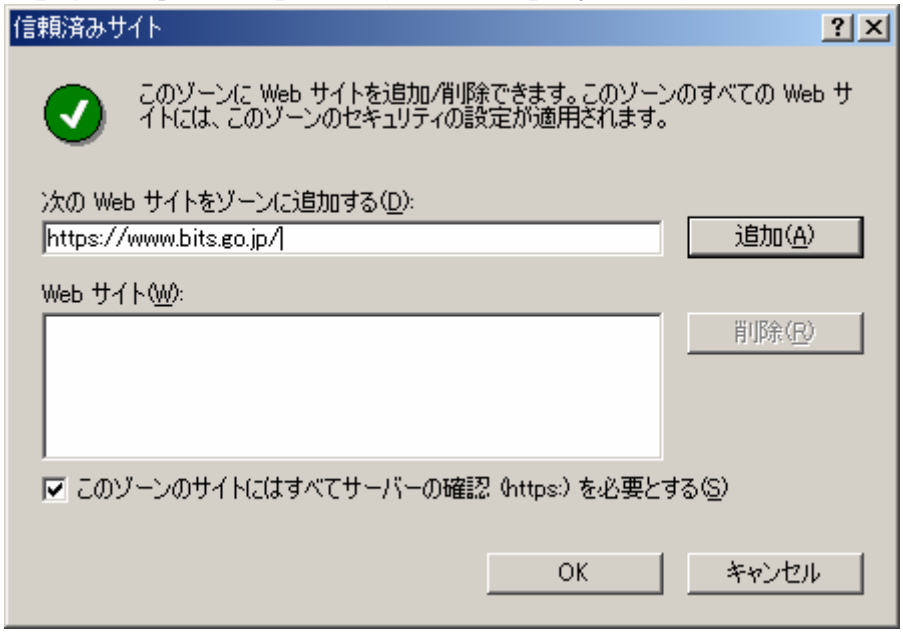
[確認ダイアログ] _[アクティブスクリプト]の確認ダイアログ



(2) 行政事務従事者は、信頼できるウェブサイトに限り、確認用ダイアログの表示を回避することができる。

［操作手順］ダウンロードしたプログラムの署名を確認するための設定手順

Internet Explorer®の[ツール]メニューから[インターネットオプション]を選択し、[セキュリティ]タブを選択する。［イントラネット］又は［信頼済みサイト]を選択し[サイト]ボタンを押下する。
[次の Web サイトをゾーンに追加する]の項目に URL を記述し、[追加]ボタンを押下する。
[このゾーンのサイトにはすべてサーバーの確認(https:)を必要とする]のチェックを外さないこと。ただし、SSL/TLS を利用しない(http:)のウェブサイトを登録したい場合には、当該ウェブサイトのドメイン名が適正な組織の有するものであることを確認し、サイト証明書を利用したウェブサイトの認証ができないリスクを認識した上で、[このゾーンのサイトにはすべてサーバーの確認(https:)を必要とする]のチェックを外して当該ウェブサイトを登録した上で、利用することができる。



4.6　ウェブブラウザの設定変更を要求するウェブサイトの閲覧

(1) 行政事務従事者は、ウェブサイトから閲覧のためにプラグイン、スクリプト等の実行に関するウェブブラウザの設定変更を要求された場合であっても、ウェブブラウザのセキュリティレベルが低下し不正プログラムに感染する危険性等があるため、当該要求に従ってウェブブラウザの設定を変更しないこと。

(2) 行政事務従事者は、ウェブブラウザの規定の設定で閲覧できないウェブサイトを閲覧する場合には、*[庁内 LAN の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。

5　ウェブサイトへの情報送信（フォームへ入力した情報の送信、ファイルのアップロード等）

送信する情報の盗聴、なりすましによる誤った通信相手への情報送信その他ウェブサイトに情報を送信する場合に想定される脅威を回避するための注意事項等について記述する。

5.1　情報送信の制限

(1) 行政事務従事者は、ウェブサイトへの情報の送信については、業務を遂行する上で必要な場合に限ること。

(2) 行政事務従事者は、ウェブサイトに情報を送信する場合は、当該情報の格付けに応じて以下のとおり処理すること。

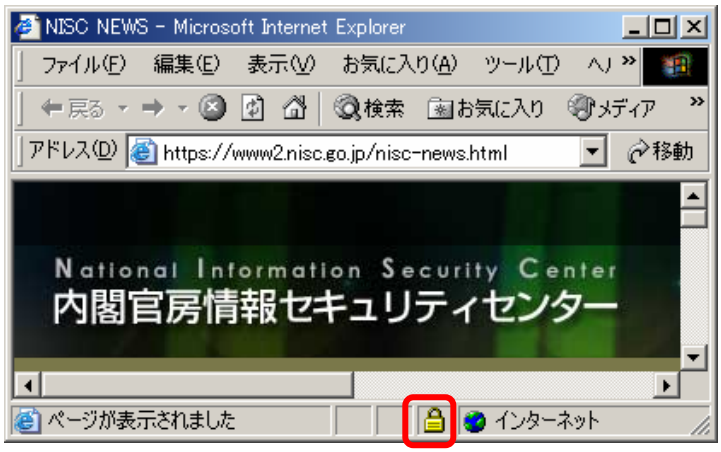
- 機密性３情報の場合には、情報の送信に関して課室情報セキュリティ責任者の許可を得ること。また、必要以上に配付しないこと。
- 機密性２情報の場合には、情報の送信に関して課室情報セキュリティ責任者に届け出ること。
- 機密性１情報の場合には、当該情報が機密性１情報であることを自身で確認すること。

5.2　フォームに入力した情報の保護方法

(1) 行政事務従事者は、閲覧しているページに表示されているフォームに機密性の高い情報（パスワード、要機密情報等）を入力してウェブサイトに送信する場合には、情報漏えいを防止するため、SSL/TLS 通信が利用されていることを確認すること。

[操作手順] SSL/TLS 通信の確認手順

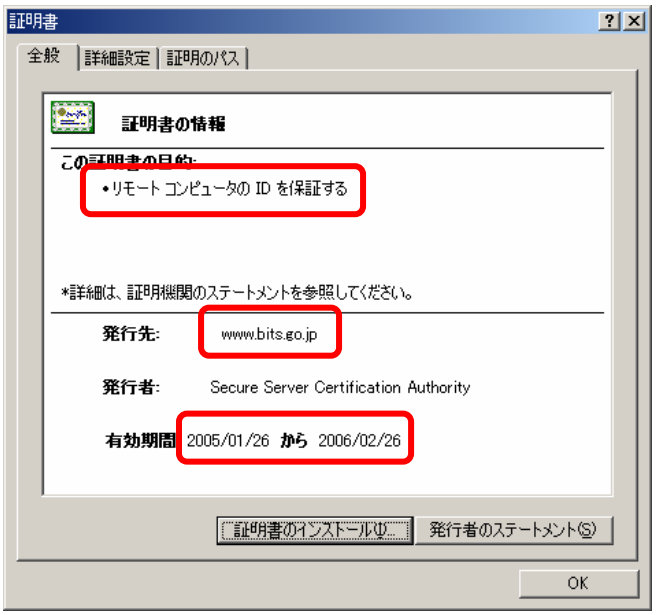
Internet Explorer®の場合、情報を送信するページを表示しているウェブブラウザのウィンドウ右下に、[鍵]マークが表示されていることを確認する（暗号化されていない場合は、[鍵]マークが表示されていない）。



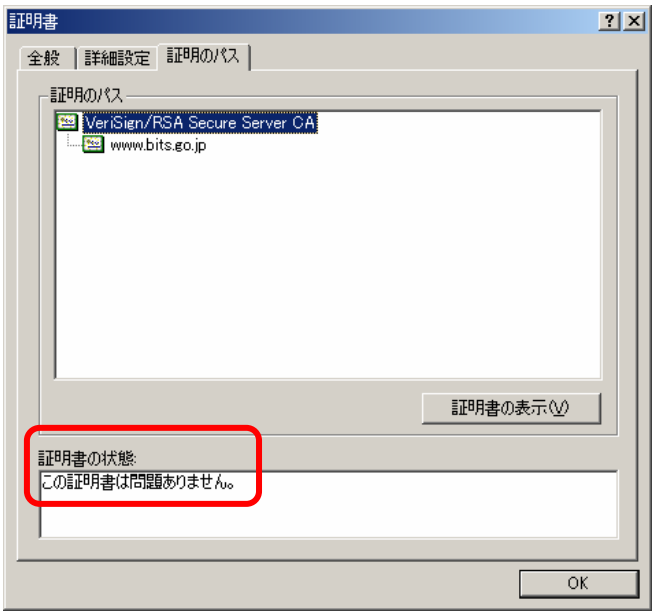
(2) 行政事務従事者は、SSL/TLS 通信を利用しているウェブサイトの初回閲覧時に、サイト証明書の内容から、表示されているウェブサイトが閲覧を想定している組織のウェブサイトであることを確認し、不適切な場合にはウェブサイトの閲覧を中止すること。

［操作手順］ サイト証明書の確認手順

情報を送信するページを表示している Internet Explorer®のウィンドウ右下に表示された[鍵]マークをダブルクリックし、表示されたサイト証明書の情報において、証明書の目的が[リモートコンピュータの ID を保証する]であること、発行先の名称が閲覧しているウェブサーバの名称と同じであること、当該名称が閲覧を想定している組織のウェブサーバの名称であること、及びサイト証明書が有効期間内にあることを確認する。



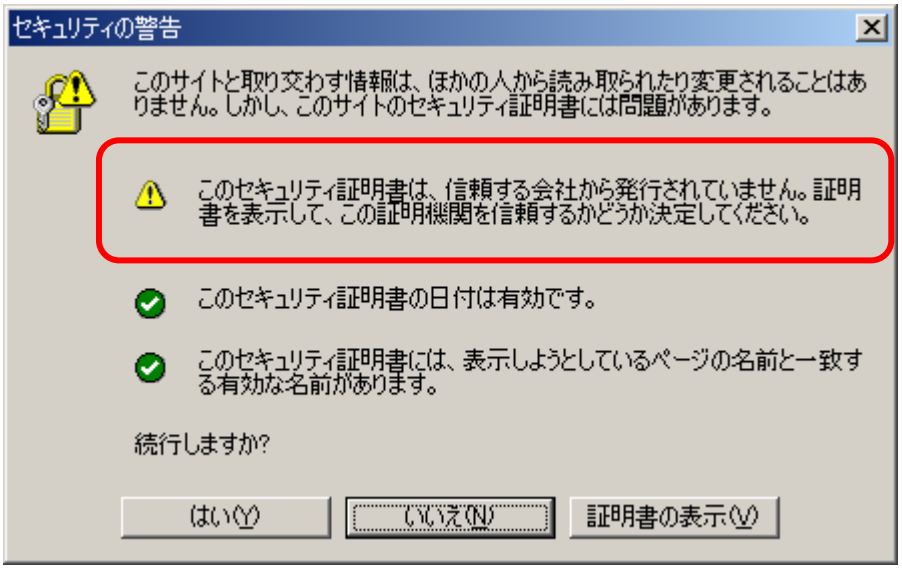
また、[証明のパス]タブに移動し、サイト証明書の発行者を選択し、[証明書の状態]に[この証明書は問題ありません。]と表示されていることを確認する。



(3) 行政事務従事者は、サイト証明書が適切でない旨の警告ダイアログが表示された場合には、当該ウェブサイトがなりすましに利用されている可能性があるため、警告の内容を確認しウェブサイトの閲覧を中止すること。

［警告ダイアログ］サイト証明書が適切でない場合の警告ダイアログ

黄色の注意マークが表示されている点に問題があり、不適切と判断されている。下の例では、サイト証明書の発行機関が信頼されていないため、警告されている。その他に、「サイト証明書の有効期間が終了している」、「サイト証明書が証明しようとしているウェブサイトと異なるウェブサイトを閲覧している」という問題がある。
以下のような警告ダイアログが表示された場合には、[いいえ]を押下し、ウェブサイトの閲覧を中止する。



5.3　送信するファイルの保護方法

(1) 行政事務従事者は、要機密情報に格付けされているファイルを府省庁外のウェブサイトに送信する場合には、情報漏えいを防止するため、以下にあげる方法を１つ以上用いて当該情報を保護すること。ただし、機密性２情報の場合には、パスワードを用いた保護で代替することができる。

- 通信路の暗号化
- 情報の暗号化

【秘密分散を利用する場合（強化遵守事項）】

- 秘密分散

(2) 行政事務従事者は、要機密情報に格付けされているファイルを府省庁内のウェブサイトに送信する場合には、府省庁外のウェブサイトに送信する場合の措置に準じて保護することが望ましい。

(3) 行政事務従事者は、府省庁外のウェブサイトに情報を送信する場合は、当該情報の付加情報（ファイルのプロパティ情報等）の内容に間違った情報又は不要な情報が含まれていないかを確認すること。

コラム：文書ファイル等に付加されている情報の取扱い

Microsoft® Office 製品、一太郎®等の文書ファイルを作成するソフトウェアにおいては、文書ファイルに様々な付加情報が含まれており、付加情報の代表的なものとして、作成者の氏名や所属、最終更新者や最終更新時間、総編集時間等の文書情報がある。文書情報は、他者の作成したファイルをコピーして編集したり、テンプレート等を利用してファイルを作成したりする際に、引き継がれている場合がある。このため、文書情報の内容を確認しないまま、当該ファイルを他者に提供すると、元ファイルの作成者の氏名や所属が提供先に漏えいすることになることから、文書ファイル等の文書情報に不適切な情報が含まれていないか確認する必要がある。

また、これらのソフトウェアでは、変更履歴等を残したり、コメントを挿入したりする機能が備わっている場合があり、当該変更履歴やコメントも付加情報に含まれる。変更履歴機能は、削除、追加等の変更した箇所が容易に分かり、コメント機能は文中に含めることができない注意事項等を記述することができる等、便利な機能である。しかし、変更履歴、コメント等を残したまま、当該ファイルを他者に提供すると、本来提供されるべきでない情報が提供先に漏えいすることになるため、文書情報と同様に注意する必要がある。

6　ファイルのダウンロード

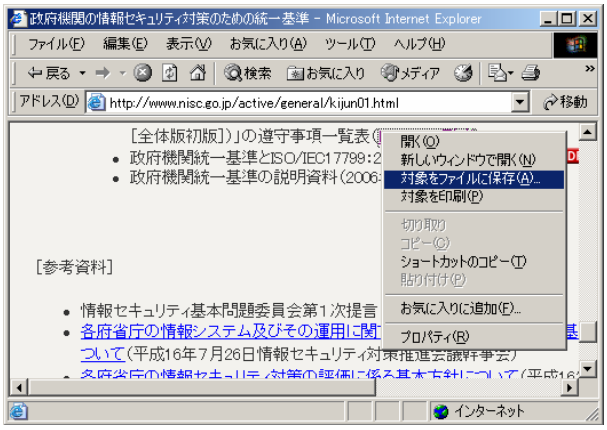
不正プログラムの感染その他ウェブサイトからダウンロードしたファイルを実行又は開く場合に想定される脅威を回避するための注意事項等について記述する。

6.1　ウェブブラウザから直接的に、実行ファイルを実行する行為及び文書ファイル等を開く行為の制限

(1) ウェブブラウザから実行ファイルを直接的に実行した場合でもアンチウイルスソフトウェア等の自動検査機能によりウイルスを検出することが可能であるが、行政事務従事者は、実行ファイルをダウンロードする場合には、電子署名及び不正プログラムの有無を確認し、また問題が生じた場合に原因となったファイルの特定を容易にするため、ウェブブラウザから直接実行するのではなく、端末上に一旦ダウンロードすることが望ましい。

［操作手順］ファイルのダウンロード

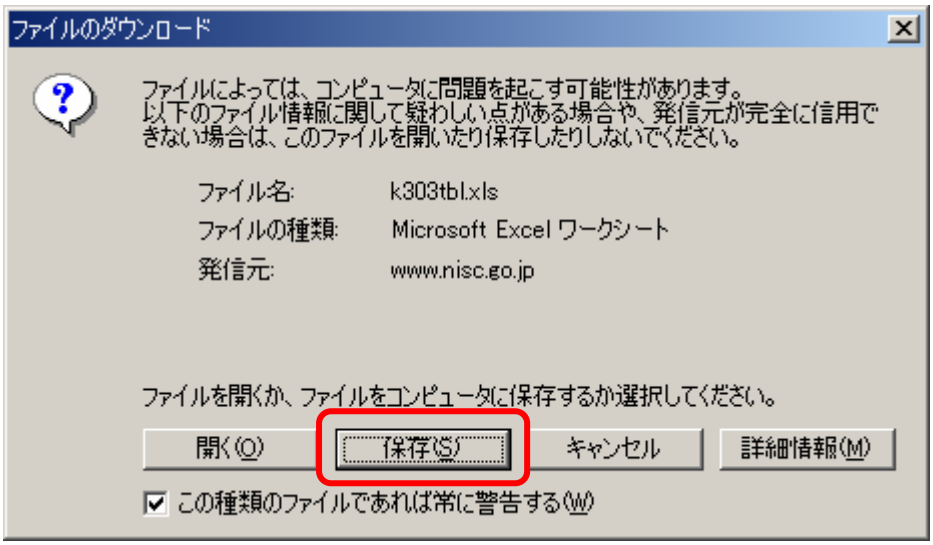
Internet Explorer®に表示されているページ上で、ダウンロードしたいファイルへのリンクを右クリックし、[対象をファイルに保存]を選択する。表示されるダイアログに従って、任意のディレクトリにファイルを保存する。
また、ダウンロードする際に、ファイルの保存又は実行を確認するダイアログが表示された場合には、保存を選択する。



(2) ウェブブラウザから文書ファイルを直接的に開いた場合でもアンチウイルスソフトウェア等の自動検査機能によりウイルスを検出することが可能であるが、行政事務従事者は、ウェブサイト上にある文書ファイル等を開こうとする（利用しようとする）場合には、不正プログラムの有無を確認し、また問題が生じた場合に原因となったファイルの特定を容易にするため、ウェブブラウザから直接開くのではなく、端末上に一旦ダウンロードすることが望ましい。ただし、信頼できるウェブサイト上にある文書ファイル等を開こうとする（利用しようとする）場合、この限りではない。

［操作手順］ファイルの[開く]又は[保存]の選択

ダウンロードするファイルへのリンクをクリックすると、[開く]又は[保存]を選択するダイアログが表示される。
[保存]を選択し、任意のフォルダに１度保存する。



(3) 行政事務従事者は、ダウンロードした実行ファイルが情報システムセキュリティ責任者により定められた利用可能なソフトウェアに含まれていない場合には、導入、利用しないこと。

6.2 保存したファイルに対する不正プログラムの有無の確認

(1) 行政事務従事者は、保存したファイルを実行又は特定のソフトウェアにより開く前に、不正プログラムの有無の確認を行うこと。

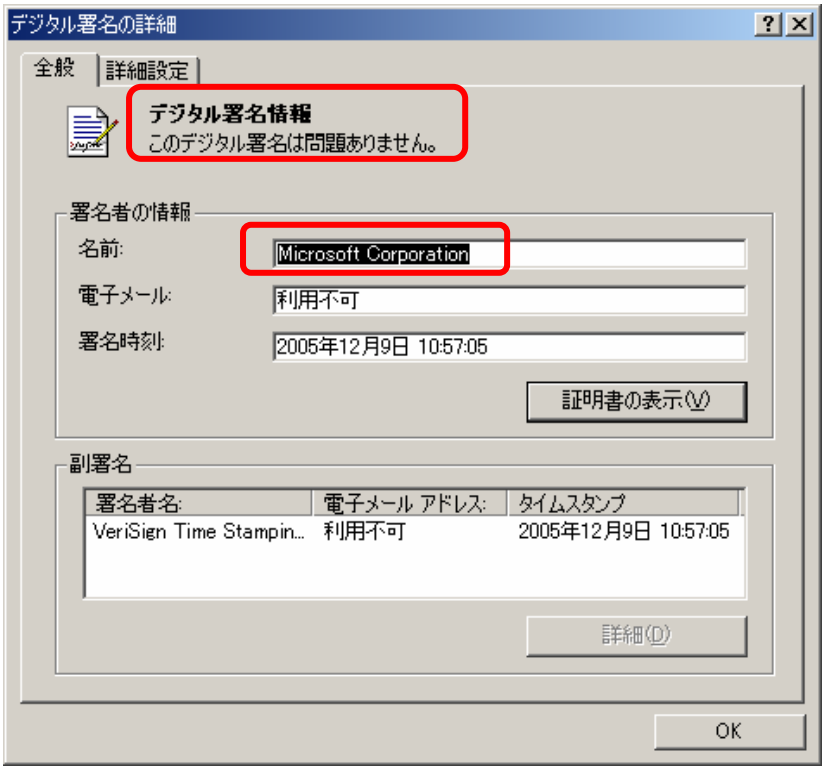
(2) 行政事務従事者は、保存したファイルに不正プログラムが含まれていることが判明した場合には、当該ファイルを実行せずに又は特定のソフトウェアにより開かずに、情報システムセキュリティ管理者に連絡・相談し、指示を仰ぐこと。

6.3 保存した実行ファイルの電子署名の確認

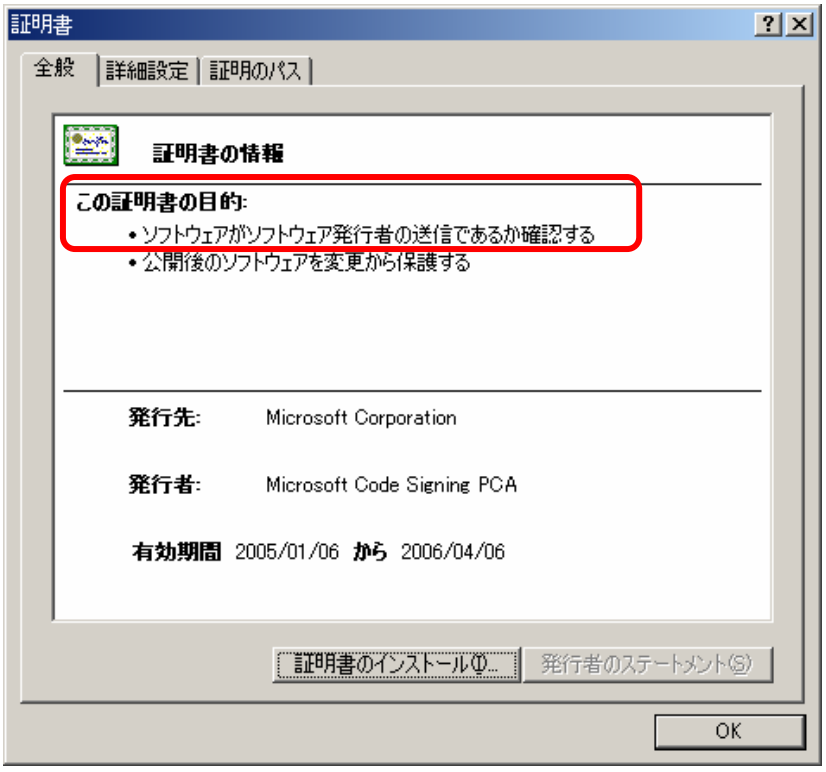
(1) 行政事務従事者は、保存した実行ファイルについて電子署名により配布元が確認できる場合には、配布元が適切な組織であることを確認すること。

[操作手順] 実行ファイルの電子署名の確認手順

エクスプローラ上で、ダウンロードした実行ファイルを選択し、右クリックから[プロパティ]を選択する。電子署名がなされている場合には、プロパティのウィンドウに[デジタル署名]タブが存在するので、当該タブを選択し、[詳細]ボタンを押下する。
表示された[デジタル署名の詳細]ウィンドウにおいて、[デジタル署名情報]が[このデジタル署名は問題ありません]となっていること、[署名者の情報]の[名前]が、実行ファイルの提供元の組織であることを確認する。



また、[証明書の表示]ボタンを押下し、表示されたウィンドウの[この証明書の目的]が[ソフトウェアがソフトウェア発行者の送信であるか確認する]となっていることを確認する。



6.4　不正プログラムに感染した時の対処

⑴ 行政事務従事者は、ダウンロードしたファイルを実行し又は開いたことにより、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により当該 PC をネットワークから分離し、*[庁内 LAN の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。

7　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) 行政事務従事者は、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。

《 対象：情報システムセキュリティ責任者 》

1　本書の目的

ウェブは、府省庁内における業務システムの利用、情報の伝達や共有だけでなく、府省庁外のニュースサイトや検索サイトの活用等業務の円滑な遂行に必要不可欠なツールとなっている。一方で、業務時間中における私的目的でのウェブの閲覧、掲示板への無断書き込み等、業務効率の低下や府省庁の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、行政事務従事者による安心・安全なウェブの利用を実現するために、情報システムセキュリティ責任者に求められる事項を定めることを目的とする。

2　本書の対象者

2.1　対象者

本書は、ウェブブラウザを利用する情報システムに関する情報システムセキュリティ責任者を対象とする。

3　ウェブブラウザのセキュリティに係る事項の決定

3.1　ウェブブラウザのセキュリティホール対策

(1) 情報システムセキュリティ責任者は、ウェブブラウザのセキュリティホールに関連する情報から、当該セキュリティホールが情報システムにもたらすリスクを分析した上で、セキュリティホール対策計画を作成すること。

3.2　ウェブブラウザのセキュリティ設定

(1) 情報システムセキュリティ責任者は、行政事務従事者が利用する端末上で動作するウェブブラウザにおけるスクリプト等の実行、パスワードの保存等のセキュリティに関連する設定を定めること。

(2) 情報システムセキュリティ責任者は、行政事務従事者が利用する端末上で動作するウェブブラウザで利用可能なプラグイン（ウェブブラウザの機能を拡張するためのソフトウェア）等を定めること。

(3) 情報システムセキュリティ責任者は、定められた設定及びウェブブラウザで利用可能なプラグインを*[○ヶ月に1度]*見直すこと。

4　ウェブの利用に係る事項の決定

【閲覧可能なウェブサイトをコンテンツフィルタリング等により制限する場合】

4.1　閲覧可能なウェブサイトの制限

(1) 情報システムセキュリティ責任者は、行政事務従事者が閲覧可能な府省庁外のウェブサイトを定め、コンテンツフィルタリング等により制限すること。

(2) 情報システムセキュリティ責任者は、定めた閲覧可能なウェブサイトを*[○ヶ月に1度]*見直すこと。

5　ウェブ利用に関する証跡管理

5.1　証跡の点検及び分析

(1) 情報システムセキュリティ責任者は、取得した証跡を以下の観点から、*[○ヶ月に1度]*点検及び分析すること。

- 閲覧が禁止されているウェブサイトの閲覧
- 私的なウェブサイトの閲覧

(2) 情報システムセキュリティ責任者は、点検及び分析の結果を統括情報セキュリティ責任者又は情報セキュリティ責任者に報告すること。

《 対象：情報システムセキュリティ管理者 》

1　本書の目的

ウェブは、府省庁内における業務システムの利用、情報の伝達や共有だけでなく、府省庁外のニュースサイトや検索サイトの活用等業務の円滑な遂行に必要不可欠なツールとなっている。一方で、業務時間中における私的目的でのウェブの閲覧、掲示板への無断書き込み等、業務効率の低下や府省庁の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、行政事務従事者による安心・安全なウェブの利用を実現するために、情報システムセキュリティ管理者に求められる事項を定めることを目的とする。

2　本書の対象者

2.1　対象者

本書は、ウェブブラウザを利用する情報システムに関する情報システムセキュリティ管理者を対象とする。

3　ウェブの利用に係る全般的な管理作業

3.1　ウェブサイト閲覧の証跡管理

(1) 情報システムセキュリティ管理者は、行政事務従事者が府省庁外のウェブサイトを閲覧した証跡を、ファイアウォール、プロキシサーバ等で取得すること。

3.2　行政事務従事者からの報告・連絡・相談への対応

(1) 情報システムセキュリティ管理者は、行政事務従事者からコンテンツフィルタリングの制限解除、ウェブブラウザの設定変更等の相談を受けた場合には、その事由が業務の遂行上必要であることを確認し、セキュリティを著しく低下させない範囲で一時的に制限の解除等に応ずること。

(2) 情報システムセキュリティ管理者は、制限の解除等の事由となった業務が完了した場合には、速やかに本来の設定に戻すこと。

(3) 情報システムセキュリティ管理者は、行政事務従事者から不正プログラムの感染等の障害等の報告を受けた場合には、規定の手順に従って対応すること。

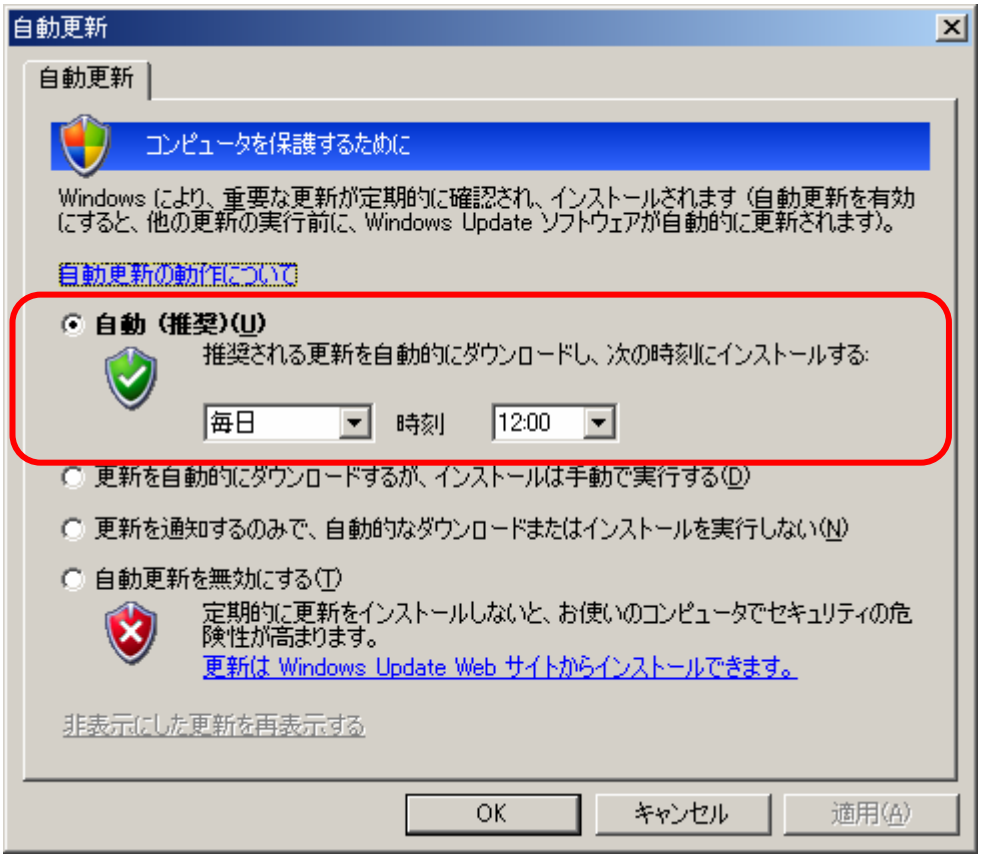
4　ウェブブラウザの設定

4.1　ウェブブラウザのセキュリティホール対策

(1) 情報システムセキュリティ管理者は、発見・報告されたウェブブラウザのセキュリティホールについて対策を実施し、行政事務従事者が利用するウェブブラウザを常に最新の状態に維持すること。

［操作手順］自動更新の設定手順

Internet Explorer®は、Windows® OS のアップデート機能である Microsoft® Update 又は Windows® Update を利用して、OS 等と同時に行うことができる。
[スタート]ボタンから[設定]を選択し、[コントロールパネル]を開く。[コントロールパネル]内の[自動更新]を開き、自動更新の設定を[自動(推奨)]にする。更新の確認頻度は、毎日 12:00 に行うようにする。



4.2 ウェブブラウザの基本設定

(省略)「お気に入り」、「ホームページ」等に関する設定

4.3 セキュリティ機能に係る設定

(1) 情報システムセキュリティ管理者は、行政事務従事者が利用するウェブブラウザのプラグイン等のインストール又は実行に係る設定について、無効な状態、又はインストール若しくは実行の可否を確認できる状態にすること。

[操作手順] プラグイン等のインストール及び実行に関する設定手順

Internet Explorer®の[ツール]メニューから[インターネットオプション]を選択し、[セキュリティ]タブに移動し [インターネット]ゾーンを選択し、 [レベルのカスタマイズ]ボタンを押下する。
[ActiveX®コントロールとプラグインの実行]を、[有効にする]に設定する。
[スクリプトを実行しても安全だとマークされていない ActiveX®コントロールの初期化とスクリプトの実行]を、[無効にする]に設定する。
[スクリプトを実行しても安全だとマークされている ActiveX®コントロールのスクリプトの実行]を、[ダイアログを表示する]に設定する。
[署名済み ActiveX®コントロールのダウンロード]を、[ダイアログを表示する]に設定する。
[未署名の ActiveX®コントロールのダウンロード]を、[無効にする]に設定する。

(2) 情報システムセキュリティ管理者は、行政事務従事者が利用するウェブブラウザのスクリプト等の実行に係る設定について、無効な状態又は実行の可否を確認できる状態にすること。

[操作手順] スクリプト等の実行に関する設定手順

Internet Explorer®の[ツール]メニューから[インターネットオプション]を選択し、[セキュリティ]タブに移動し [インターネット]ゾーンを選択し、 [レベルのカスタマイズ]ボタンを押下する。
[Java®アプレットのスクリプト]を、[ダイアログを表示する]に設定する。

【アクティブスクリプトの実行を有効にしない場合】

[アクティブスクリプト]を、[ダイアログを表示する]に設定する。

【アクティブスクリプトの実行を有効にする場合】

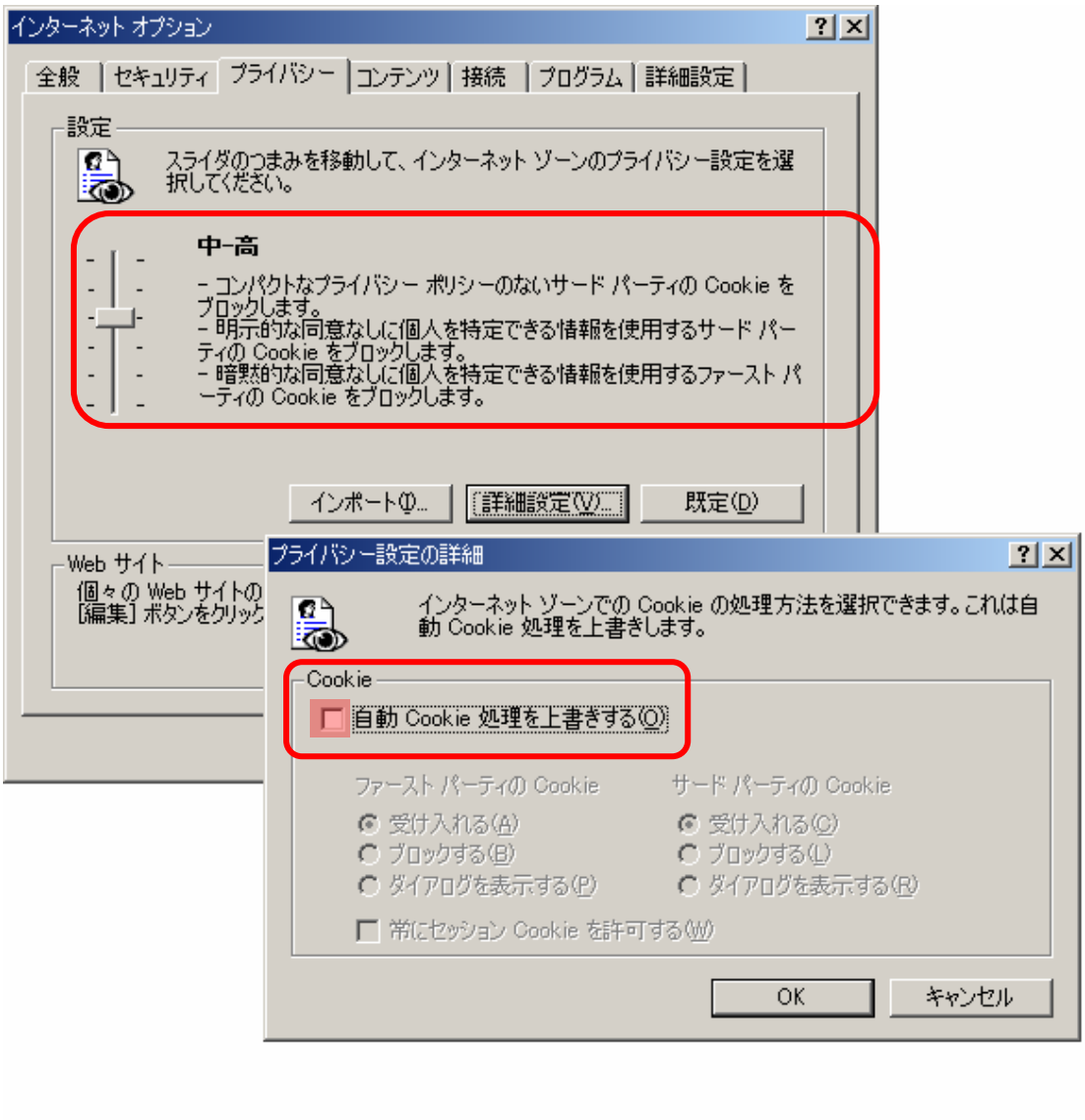
[アクティブスクリプト]を、[有効にする]に設定する。

[スクリプトによる貼り付け処理の許可]を、[無効にする]に設定する。

(3) 情報システムセキュリティ管理者は、行政事務従事者の利用するウェブブラウザのクッキーに係る設定について、安全な状態にすること。

[操作手順] クッキーを安全に利用するための設定手順

Internet Explorer®の[ツール]メニューから[インターネットオプション]を選択し、[プライバシー]タブに移動し [設定]を [中-高]に設定する。
さらに、[詳細設定]ボタンを押下し、[自動 Cookie 処理を上書きする]がチェックされていないことを確認する。チェックされている場合には、チェックを外す。



(4) 情報システムセキュリティ管理者は、行政事務従事者が利用するウェブブラウザの SSL/TLS 通信について、脆弱な暗号化通信機能を利用しないように設定すること。

[操作手順] SSL2.0 を利用しないための設定手順

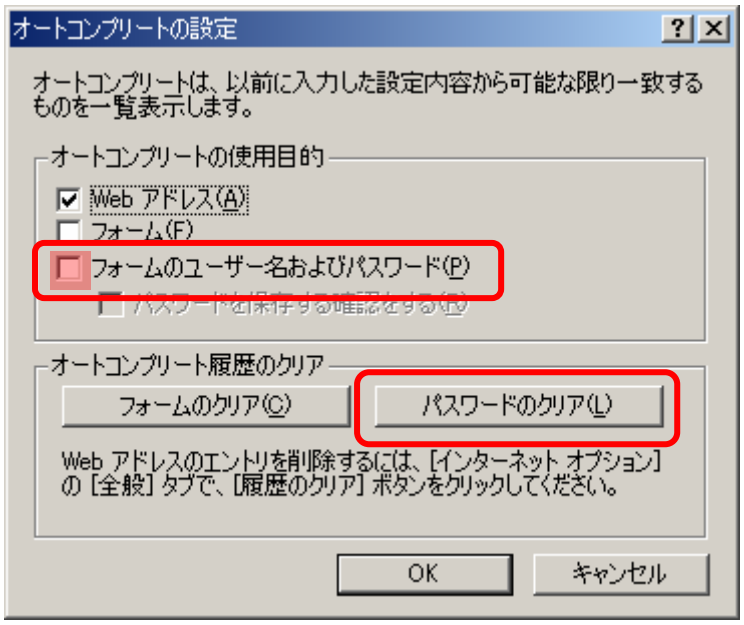
Internet Explorer®の[ツール]メニューから[インターネットオプション]を選択し、[詳細設定]タブを選択する。
[セキュリティ]の項目にある、[SSL2.0 を使用する]のチェックを外す。[SSL3.0 を使用する]、[TLS1.0 を利用する]のチェックを付ける。

(5) 情報システムセキュリティ管理者は、行政事務従事者が利用するウェブブラウザのパスワードを自動補完する機能を停止すること。

[操作手順] パスワードの自動補完を停止するための設定手順

Internet Explorer®の[ツール]メニューから[インターネットオプション]を選択し、[コンテンツ]タブにある[個人情報]の枠内の[オートコンプリート]ボタンを押下する。表示された[オートコンプリートの

設定]ウィンドウの、[オートコンプリートの使用目的]の枠内にある[フォームのユーザー名およびパスワード]のチェックを外す。
既に自動補完されるパスワードが存在している場合には、[オートコンプリート履歴のクリア]の枠内にある[パスワードのクリア]ボタンを押下する。



(6) 情報システムセキュリティ管理者は、行政事務従事者が利用するウェブブラウザにおいて、ダウンロードしたプログラムの署名を確認する機能を有効にすること。

[操作手順] ダウンロードしたプログラムの署名を確認するための設定手順

Internet Explorer®の[ツール]メニューから[インターネットオプション]を選択し、[詳細設定]タブを選択する。
[セキュリティ]の項目にある、[ダウンロードしたプログラムの署名を確認する]のチェックを付ける。

(7) 情報システムセキュリティ管理者は、行政事務従事者が利用するウェブブラウザにおいて、サイト証明書が無効な場合に警告を挙げる機能を有効にすること。

[操作手順] ダウンロードしたプログラムの署名を確認するための設定手順

Internet Explorer®の[ツール]メニューから[インターネットオプション]を選択し、[詳細設定]タブを選択する。
[セキュリティ]の項目にある、[無効なサイト証明書について警告する]のチェックを付ける。

(8) 情報システムセキュリティ管理者は、行政事務従事者が利用するウェブブラウザにおいて、無用なポップアップウィンドウをブロックする機能を有効にすること。