

庁舎内におけるPC利用手順 ウェブブラウザ編
策定手引書

2006年2月

内閣官房情報セキュリティセンター

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

Microsoft、Windows、Internet Explorer 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。

Mozilla は、米国 Mozilla Foundation 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。

Opera は Opera Software ASA の登録商標または商標です。

1 本書の目的

本書は、府省庁においてウェブブラウザを利用してウェブサイトの閲覧等を行う際に適用する利用手順（以下「庁舎内における PC 利用手順 ウェブブラウザ編」という。）を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 ウェブブラウザ編」は、これらの実施手順の一つとして策定し、府省庁においてウェブブラウザを利用してウェブサイトの閲覧等を行う場合に適用するものである。すなわち、行政事務従事者等は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。

ウェブブラウザを利用したウェブサイトの閲覧、情報の送信、ファイルのダウンロード等を行う際には、不正プログラムの感染、情報の漏えい、誤った相手への情報の送信等の脅威だけでなく、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その他業務効率の低下や府省庁の社会的信用を失わせる脅威も想定される。このようなリスクを軽減するために、ウェブブラウザを利用する際に行政事務従事者が守るべき実施手順を整備することが府省庁に求められる。

本書は、これらの背景の下で、「庁舎内における PC 利用手順 ウェブブラウザ編」に含めるべき事項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、業務への適合性等において適切な実施手順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 ウェブブラウザ編」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 ウェブブラウザ編」に係る遵守事項

- 2.2.2 障害等の対応（1）障害等の発生に備えた事前準備
- 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
- 3.2.2 情報の利用（1）業務以外の利用の禁止
- 3.2.2 情報の利用（3）要保護情報の取扱い
- 3.2.4 情報の移送（1）情報の移送に関する許可及び届出
- 3.2.4 情報の移送（5）電磁的記録の保護対策
- 3.2.5 情報の提供（2）他者への情報の提供

- 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
- 4.1.4 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
- 4.1.4 証跡管理機能（3）取得した証跡の点検、分析及び報告
- 4.1.4 証跡管理機能（4）証跡管理に関する利用者への周知
- 4.1.6 暗号と電子署名（鍵管理を含む）（3）暗号化機能及び電子署名の付与機能の利用
- 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
- 5.2.1 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
- 5.2.2 端末（1）端末の設置時
- 5.2.2 端末（2）端末の運用時
- 5.3.1 通信回線を介して提供するアプリケーション共通対策（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（1）通信回線の構築時
- 6.3.1 府省庁外の情報セキュリティ水準の低下を招く行為の防止（2）措置の遵守

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が挙げられる。当該項目その他も各府省庁の判断で必要と思われるものは、適宜追加することができる。

- ウェブブラウザの設定変更を求めるウェブサイトの閲覧時の注意事項
- 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ファイルを開く行為の制限
- 偽ウェブサイトへの誘導及び情報搾取に係る注意事項

3 文書構成例

「庁舎内における PC 利用手順 ウェブブラウザ編」は、情報セキュリティ対策の観点以外の観点を含む一般的な利用手順書とすべきである。そのため、行政事務従事者の行為に着目した構成が有効である。文書構成の例を以下に示す。

- 1 本書の目的
- 2 本書の対象者
 - 2.1 対象者
- 3 ウェブの利用に係る全般的な注意事項
 - 3.1 私的なウェブサイト閲覧の禁止
 - 3.2 閲覧可能なウェブサイトの制限
 - 3.3 プラグイン等の導入・利用の禁止
 - 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
 - 3.5 ウェブサイト閲覧の監視
- 4 ウェブサイトの閲覧
 - 4.1 ウェブサイトを閲覧する方法
 - 4.2 府省庁内の主要なウェブサイト
 - 4.3 ウェブサイト閲覧時の一般的な注意事項
 - 4.4 SSL/TLS 通信の確認
 - 4.5 確認・警告等のダイアログへの対応
 - 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
- 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）
 - 5.1 情報送信の制限
 - 5.2 フォームに入力した情報の保護方法
 - 5.3 送信するファイルの保護方法
- 6 ファイルのダウンロード
 - 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
 - 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
 - 6.3 保存した実行ファイルの電子署名の確認
 - 6.4 不正プログラムに感染した時の対処
- 7 本手順に関する相談窓口

4 作成する上での留意事項

「庁舎内における PC 利用手順 ウェブブラウザ編」は、以下のことに留意して作成する。

- (1) 行政事務従事者がウェブブラウザを利用する場合の様々な場面を想定し、利用におけるライフサイクルによって記載事項を整理・分類する。
- (2) 注意義務規定の主語は、「行政事務従事者は」などに統一する。例えば、申請手続については申請者たる行政事務従事者とその許可者・承認者である責任者等の立場があるが、このような場合は、行政事務従事者の立場から（行政事務従事者を主語として同人の責務として）書き下す。
- (3) 図表を多用し、個々の規定ごとに具体的に説明を加える。
- (4) 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 ウェブブラウザ編」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]・・・「ウェブブラウザ」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「ウェブブラウザ」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、行政事務従事者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、これを背景として行政事務従事者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、これを行政事務従事者の立場から解釈し直す。

[別立場]・・・行政事務従事者の立場ではなく、責任者側又は管理者側の立場から記述されている遵守事項については、これを行政事務従事者の立場から解釈し直す。

[参考引用]・・・直接「ウェブブラウザ」に関連した内容ではないが、行政事務従事者の理解促進に寄与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「ウェブブラウザ」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 ウェブブラウザ編」の作成に際しては、以下のよう資料が参考となる。

5.1 政府及び政府関係機関の資料

- (1) 独立行政法人 情報処理推進機構 (IPA) の「ブラウザのセキュリティを設定をする」
<http://www.ipa.go.jp/security/ciadr/browser.html>
- (2) 独立行政法人 情報処理推進機構 (IPA) の「SOHO・家庭向けセキュリティ対策マニュアル(Ver1.20) 2.6 ブラウザとメーラのセキュリティ設定」
<http://www.ipa.go.jp/security/fy14/contents/soho/html/index.html>

5.2 政府・政府関係機関以外の資料

- (1) マイクロソフト株式会社の「ブラウジングと電子メールの安全性を強化する」
<http://www.microsoft.com/japan/security/incident/settings.msp>
- (2) 有限責任中間法人 Mozilla® Japan の「セキュリティセンター」
<http://www.mozilla-japan.org/security/>
- (3) Opera Software ASA の「Opera® セキュリティセンター」
<http://www.jp.opera.com/security/>

6 雛形の利用方法

「庁舎内における PC 利用手順 ウェブブラウザ編 (雛形)」を参考にして、「ウェブブラウザの利用手順書」を策定すると効率的である。別紙1の「ウェブブラウザの利用手順書 (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盛り込み作成したものである。

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。

- 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、既にインストールされている。
- 行政事務従事者自身はPCの管理者権限を有していない。
- 不正プログラムの感染等の障害等が発生した場合に従うべき手順が整備されている。
- 以下のソフトウェア製品を使用している。
 - OS : Microsoft® Windows® 2000 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。

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行政事務従事者とは分けて記載しており、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) 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て。
- (5) 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。
- (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。