C3253 ウェブブラウザ利用ガイドライン

国立情報学研究所 学術情報ネットワーク運営・連携本部  
高等教育機関における情報セキュリティポリシー推進部会

**改定履歴**

|  |  |  |
| --- | --- | --- |
| 日付・文書番号 | 改定内容 | 担当 |
| 2007年2月15日  A3203 | 新規作成（ウェブブラウザ手順） | 国立大学法人等における情報セキュリティポリシー策定作業部会 |
| 2007年10月31日  A3203 | 「ウェブブラウザ利用ガイドライン」として、全体的な内容を見直し | 国立大学法人等における情報セキュリティポリシー策定作業部会 |
| 2015年10月9日  C3253 | 文書番号の変更のみ | － |

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。

sp-comment[at]nii.ac.jp　（[at]を＠に置き換えてください）

担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

解説：本ガイドラインの対象者は、事務従事者を除く一般利用者である。

**1. 本書の目的**

　ウェブは、情報の伝達や共有に必要不可欠なツールとなっている。一方で、私的目的でのウェブの閲覧、掲示板への無断書き込み等は、大学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、利用者がウェブを安心・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。なお、ウェブブラウザを利用するPC端末にはウイルス対策ソフトウェアが導入されているものとする。ウイルス対策ソフトウェアが導入されていないPC端末でのウェブ閲覧は原則として禁止する。

**2. 本書の対象者**

2.1 対象者

　本書は、ウェブブラウザを教育や研究目的で利用するすべての教員学生（以下利用者と呼ぶ。）を対象とする。 行政事務従事者は、事務手順書のブラウザ手順に従うものとする。

**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ウェブサイトの閲覧、各種情報システムの利用等、ウェブの利用において、利用者の安全性を確保するために、ウェブの利用に係る全般的な注意事項を記述する。

3.1 目的外利用の禁止

(1) 利用者は研究や教育および教育支援等、大学で活動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。営利目的でのネットワーク利用は禁止する。

(2) 利用者は学内から任意のウェブサイトを閲覧することにより、閲覧先のサーバに本学のドメイン名及びIPアドレス等が記録されることに留意すること。記録された情報をもとに、サーバ管理者により本学に対して不当な要求が行われるとか、閲覧者の個人情報の開示をサーバ管理者が要求する場合がある。また、掲示板等に名前やメールアドレスを記入して場合、不正請求をされることもある。

【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。利用者は、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) 利用者は、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すること。

(3) 利用者は、制限されているウェブサイトの閲覧が必要な場合には、部局技術管理者に連絡・相談すること。

3.3 プラグイン等の導入・利用の禁止

(1) 利用者は、部局技術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) 利用者は、部局技術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、部局技術管理者に連絡・相談すること。

3.4 外部のウェブサイトで提供されているサービスの利用等の注意事項

(1) 利用者は、学外の掲示板、ブログ等への書き込み、ウェブメールの利用等にあたっては、情報漏えいの可能性に十分に注意すること。

(2) 公序良俗に反する不適切な書き込みや利用を行わないこと。掲示板等への単純な書き込みであっても、内容によっては本学や本学構成員の良識が疑われる場合がある。特に、他人への誹謗中傷と誤解されるような記事やプライバシーや著作権等の侵害と疑われかねない書き込みをしてはならない。

(3) 不正なサイトへの誘導を狙ったリンクやウイルス等の不正なソフトウェアをダウンロードさせることを目的としたリンクはインターネット上に多数存在する。有名なサイトであっても決して安全ではないので、不用意にリンクをクリックしないこと。

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。利用者は、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。

**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 ウェブサイト閲覧時の一般的な注意事項

(1) 利用者は、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。
* 目的とするウェブサイトの閲覧には、URIを直接入力すること。データ入力に中継サイトを利用するとデータの詐取やクロスサイトスクリプティングの危険性がある。また、認証を求められるページへ入って後で、そのページから張られたページへのリンクの参照は、認証情報が不正利用されることがあるので注意が必要である。
* ウェブページの再読み込みを短時間に繰り返すと、サービス不能攻撃（DoS攻撃、サービスに不要な通信をおこさせて、サービスの質の低下を狙った攻撃）と見なされる可能性があるので注意すること。 サイトによっては、当該ドメインや当該IPアドレスからのアクセスがブロックされる可能性がある。オンラインジャーナルの大量一時ダウンロードによっても、アクセスブロック等の問題が発生することがある。
* 検索サイトでは、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。また、検索結果リストの表示の順番は重要度とか参照頻度といった特別な意味があるわけではない。先頭に表示されるからといって、正しいということはない。
* 有名で広く知られているサイトであっても、バナー広告等を安易にクリックしないこと。有害なサイトやウイルスダウンロードサイトがリンクされていることがある。
* 電子メールで送られてきたHTMLメール内のリンクを安易にクリックしないこと。成りすましサイトやワンクリック詐欺サイトへの誘導、phishing被害につながることがある。次ページにphishingサイトの例を示す。画面上でURIに見える部分は見せかけのテキストで、IDとパスワードを詐取するためのサイトへのリンクになっている。
* ウェブページ閲覧時に、見かけないセキュリティ警告表示とともにソフトウェアのダウンロードを求められてもダウンロードしないこと。ウイルスや不正なソフトウェアをインストールさせられる可能性がある。

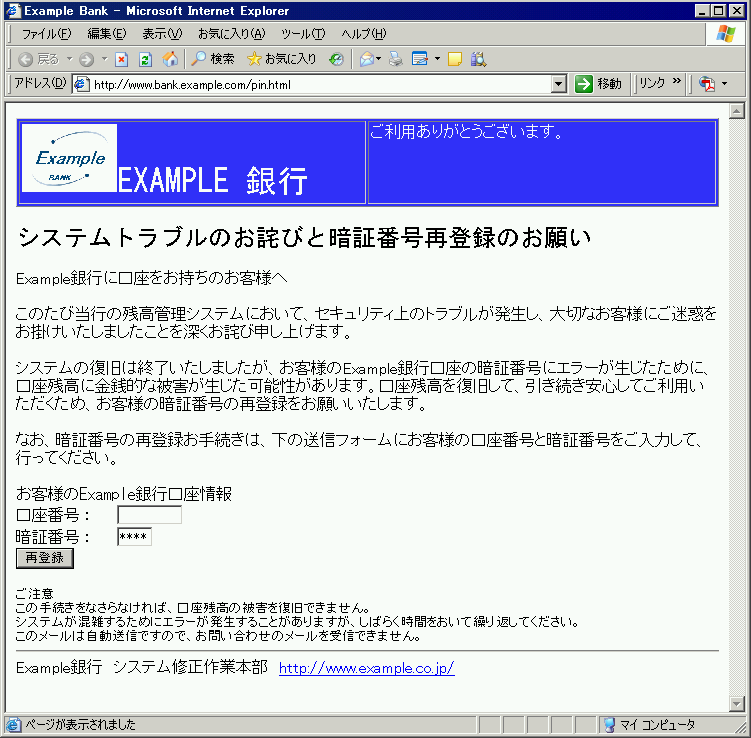


図１　金融機関からの連絡を装って暗証番号を盗み出そうとするサイトの例（説明用に作成）[[1]](#footnote-1)

4.2 TLS（SSL）通信の確認

(1) TLS（SSL）[[2]](#footnote-2)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。利用者は、閲覧している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、TLS（SSL）通信が利用されていることを確認すること。また、その際提示される証明書が正当なものであることを確認すること。証明書によっては、次ページの図のような画面が表示される。このような場合には注意が必要である。

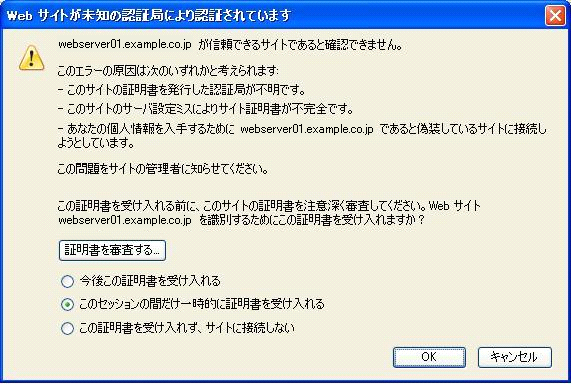


図２　注意を要する証明書への警告表示の例（１）

また、以下のような警告が表示されることもある。

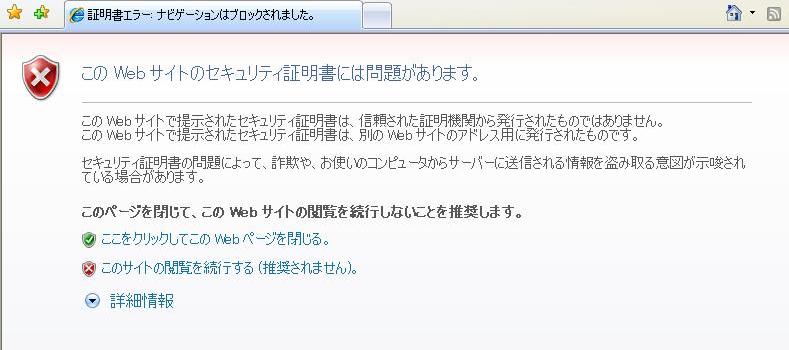


図３　注意を要する証明書への警告表示の例（２）

TLSを利用している場合には、下図のような錠前が表示されることが多い。



図４　TLSを利用していることを示す表示

ただしウェブサーバ証明書は誰でも取得できるものであることを 理解しておかなければならない。

【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】

4.3 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、利用者は、確認のためのダイアログが表示された場合には、中身を確認せずに安易に実行を許可してはいけない。

4.4 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) 利用者は、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安易に変更しないこと。

**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。

(1) 重要な情報のやりとりにはTLS（SSL）等の安全な通信を利用すること。その際、証明書の正当性を確認すること。

(2) 情報の書き込みにあたっては、クロスサイトスクリプティング等の危険性に留意するこ  
と。入力の必要なページは、ポータル等を経由せずに参照すること。

**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、利用者は、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。

(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、利用者は、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。

(3) 利用者は、ダウンロードした実行ファイルが部局技術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) 利用者は、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) 利用者は、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、部局技術管理者に連絡・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) 利用者は、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。

6.4 不正プログラムに感染した時の対処

(1) 利用者は、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、部局技術管理者に連絡・相談し、指示を仰ぐこと。

**7. 本手順に関する相談窓口**

(1) 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、部局技術責任者に相談し、指示を受けること。

(2) 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、部局技術管理者に連絡し、回答を得ること。

1. 図１～図４では、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。

   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。 [↑](#footnote-ref-1)
2. SSL（Secure Sockets Layer）には重大な脆弱性が発見されたため、2015年時点で一般的に使われているのはSSLの後継プロトコルのTLS（Transport Layer Security）であるが、ウェブサイトとの通信内容を暗号化することは依然として「SSLで接続する」などと表現されることがある。 [↑](#footnote-ref-2)