ウェブブラウザ利用ガイドライン

関西大学 IT センター

1　本ガイドラインの目的

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。

本ガイドラインは、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の導入を推奨する。

2　本ガイドラインの対象者

⑴ 対象者

本ガイドラインは、本学が提供するネットワークサービスを使用してウェブブラウザを利用するすべての利用者（以下、利用者と呼ぶ）を対象とする。

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。

⑴ 目的外利用の禁止

ア　利用者は研究や教育及び教育支援等、本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。営利目的でのネットワーク利用は禁止する。

イ　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。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場合や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た場合、不正請求をされることもある。

⑵ 閲覧可能なウェブサイトの制限

ア　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することがある。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。

イ　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は自己責任によるものであることに留意する。

ウ　利用者は、閲覧が制限されているウェブサイトを閲覧したい場合には、ITセンターに連絡・相談する。

⑶ プラグイン等の導入・利用時の注意

ア　利用者は、ITセンター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）等の導入、利用はセキュリティを低減する可能性があることに留意する。

イ　利用者は、ITセンター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、ITセンターに連絡・相談する。

⑷ 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

ア　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。

イ　公序良俗に反する不適切な書き込みや利用を行わない。掲示板等へのささい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

うな書き込みや、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ない。

ウ　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安全とは限らない。

⑸ ウェブサイト閲覧の監視

ア　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ことがある。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状況が記録されていることを認識する。

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。

⑴ ウェブサイト閲覧時の一般的な注意事項

ア　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。

（ア）　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。

（イ）　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、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、アクセスがブロックされて、他の利用者がオンラインジャーナルを利用できなくなることがあるので、特に注意する。

（ウ）　検索サイトの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、検索結果のリンク先を安易に閲覧しない。また、検索結果の順番は、情報の信頼度を表すものではない。

（エ）　有名で広く知られているサイトに掲載されている広告であっても、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ので、安易にクリックしない。

（オ）　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。なりすましサイトやワンクリック詐欺サイトへの誘導、詐欺の被害につながることがある。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。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。

⑵ TLS（SSL）通信の確認

ア　TLS（SSL）[1]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、URL が https://で始まっていることを確認する。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。ただし、誰でも安価に取得できる証明書があるので、証明書が正当であっても注意が必要である。

[1] 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。

⑶ 確認・警告等のダイアログへの対応

ア　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ない。

⑷ 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

ア　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。

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。

ア　重要な情報の送受信には TLS（SSL）等の安全な通信を利用する。その際、証明書の正当性を確認する。

イ　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し、入力が必要なページはポータル等を経由せずに、フォームが存在するページと同じサイトのリンクから行う。

6　ファイルのダウンロード

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。

⑴ 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

ア　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（ファイルを保存）することが望ましい。

イ　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。

ウ　利用者は、ダウンロードした実行ファイルが IT センター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、導入、利用する際には十分に注意する。

⑵ 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

ア　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、不正プログラムではないことを確認する。

イ　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、IT センターに連絡・相談する。

⑶ 保存した実行ファイルの電子署名の確認

ア　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。

⑷ 不正プログラムに感染した時の対処

ア　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、無線接続を切断する等により当該 PC をネットワークから分離し、IT センターに連絡・相談し、指示を仰ぐ。

7　本手順に関する相談窓口

⑴ 利用者は、緊急時の対応又は本ガイドラインの内容を超えた対応が必要とされる場合には、IT センターに相談する。

⑵ 利用者は、本ガイドラインの内容について不明な点又は質問がある場合には、IT センターに連絡する。

附　則

1　このガイドラインは、2019年11月６日から施行する。