

北海道情報大学ウェブブラウザ利用ガイドライン

1. 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、北海道情報大学（以下「本学」）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、そ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かつ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. 本ガイドラインの対象者

本ガイドラインは、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及び学生（以下「利用者」）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等は、次のとおりとする。

3. 1 目的外利用の禁止

- 1) 利用者は、研究や教育及び教育支援等、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こと。私的目的での利用は、禁止する。

3. 2 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、SNS、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当たっては、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、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し、たとえ有名なサイトであっても決して安全とは言い切れないため、不用意にリンクをクリックしないこと。

3. 3 ウェブサイト閲覧の監視

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）について監査証拠の取得、保存、点検及び分析を行う可能性がある。利用者は、この趣旨を理解の上、自身のウェブサイトの閲覧がログとして記録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は、次のとおりとする。

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、次の事項に留意すること。

- 2) ウェブサイトの情報には、正しい情報だけではなく、偽情報や誤情報が含まれている可能性があるため、ウェブサイトの情報を鵜呑みにしないこと。
- 3) 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ことを理解すること。また、認証を求められるページへ入った後で、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こと。
- 4) 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り、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こと。また、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こと。
- 5) 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ため、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、重要度や参照頻度といった特別な意味があるわけではなく、先頭に表示されるからといって、正しいということではないこと。
- 6) 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こと。
- 7) 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。なりすましサイトやワンクリック詐欺サイトへの誘導、フィッシング被害に繋がる可能性があること。画面上で URL 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繋がるリンクになっている場合があること。
- 8) 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こと。

4. 2 暗号化通信の確認

URL が「https://」ではじまるものであること。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発行元などから確認すること。なお、サーバ証明書の内容は、鍵マークをクリックし、確認すること。ただし、ウェブのサーバ証明書は、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。

4. 3 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

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、安易に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。

5. 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は、次のとおりとする。

5. 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。

5. 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ウイルススキャン等を実行し、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、情報センター事務室に報告し、指示を仰ぐこと。

5. 3 保存した実行ファイルの電子署名の確認

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。

5. 4 不正プログラムに感染した時の対処

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若しく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、情報センター事務室に報告し、指示を仰ぐこと。

6. 本ガイドラインに関する相談窓口

- (1) 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、情報センター事務室に相談し、指示を受けること。
- (2) 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、情報センター事務室に連絡し、回答を得ること。