PC/インターネット利用ガイドライン

Guideline for PC/Internet users

～情報セキュリティを守るために、何をすべきか～

～What to do for information security～

第 1.0 版

Ver.1.0

総合情報戦略機構

Integrated Information Strategy Organization

改訂履歴

改訂年月日	改訂内容
令和　3年　3月　1日	1.0版　制定

インターネットは私たちにとってなくてはならないものですが、あらゆるサービスは善意のものばかりではありません。利用するにはそれ相応の対策や対応が必要です。

The internet is a must for us, but not all services are in good faith. To use it, you need to take appropriate measures.

インターネット技術を悪用し、迷惑メールの送信、マルウェアの送付、コンピュータへの不正侵入、詐欺行為、個人情報・重要情報の窃取、プライバシーの侵害などが発生しており、インターネットの利用は、さまざまな危険と隣り合わせです。

The use of the Internet is dangerous because Internet technology is abused to send unsolicited emails and malware, invade computers, commit fraudulent acts, steal personal and important information, and invade privacy. Danger is always just around the corner.

インターネットを正しく安心して利用するには、一人ひとりがコンピュータの情報セキュリティを守ることが大切であり、それが他の利用者の安全にもつながります。

In order to use the Internet correctly and with peace of mind, it is important for each person to protect the information security of the computer, which also leads to the safety of other users.

情報セキュリティ対策の正しい知識を身に付け、「ソフトウェアの更新」、「ウイルス対策ソフトの導入」、「ID やパスワードの適切な管理」等の適切な対策によってインターネットを活用してください。

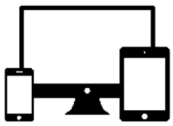
Please acquire the correct knowledge of information security measures and utilize the Internet by taking appropriate measures such as "software update", "installation of antivirus software", and "appropriate management of IDs and passwords".

以下パソコン利用者の心得を記載していますので、守るようにしてください。

The following is the guideline for PC users, so please follow it.

■PC、アプリケーション、パスワードについてすべきこと

What to do about PCs, applications and passwords



1．正規ライセンス品の使用

Use of regular licensed products

正規製品ソフトウェアを購入し、ライセンス契約に従って正しく使用してください。利用しているソフトウェアが、正規にアクティベーションしていることを確認しましょう。

Please purchase genuine product software and use it correctly according to the license agreement. Make sure that the software you are using is properly activated.

正規製品（ライセンス）でない場合は、直ちにアンインストールして、正規パッケージ製品、正規ライセンスを正しい方法で入手（購入）しましょう。

If it is not a genuine product (licensed), uninstall it immediately and obtain (purchase) a genuine packaged product and a regular license in the correct way.

過去、ライセンス違反により著作権保護団体から警告を受ける事案がありました。

In the past, there have been cases of being warned by copyright protection groups due to license violations.

2．最新の修正プログラムの適用
Apply the latest hotfix

Windows OS、Mac OS やアプリケーションは、セキュリティ対策のために日々更新され、修正プログラムが提供されます（iOS や Android OS を使ったスマートフォンやタブレットも同じです）。

Windows OS, Mac OS and applications are updated daily for security measures and hotfixes are provided. (The same applies to smartphones and tablets using iOS and Android OS.)

セキュリティリスクを回避するために、必ず Windows Update など修正プログラムを適用しましょう。修正プログラムは自動適用されるように設定しておくことを推奨します。PC は定期的に（最低一か月に一度は）起動して、更新を実行してください。

Be sure to apply a hotfix such as Windows Update to avoid security risks. We recommend that you set the hotfix to be applied automatically. Boot your PC regularly (at least once a month) to perform updates.

ソフトウェア（OS、アプリケーション）は、サポート期間内にあるものを使用してください。

Please use the software (OS, application, etc.) that is within the support period.

3.大学で使用する PC のウィルス対策
Anti-virus measures for PCs used at the University of Yamanashi

大学で使用する PC には、有償のウィルス対策ソフトウェアをインストー

ルし、有効化して使用してください。

Please install, enable, and use paid antivirus software on PCs used at the university.

山梨大学では、有償のウィルスバスターを大学が購入し、山梨大学所属の教員、研究者、学生に無料で貸与しています。積極的に利用してください。

At University of Yamanashi, the university purchased a paid virus buster and lent it to faculty members, researchers, and students belonging to University of Yamanashi free of charge. Please use it.

4．自宅で使用するPCのウィルス対策

Anti-virus measures for PCs used at home

大学の PC で扱うファイルを自宅の PC で使用したり、自宅の PC を大学に持ち込んで使用したりする場合は、自宅の PC にも有償のウィルス対策ソフトウェアをインストールし、有効化して使用しましょう。

If you want to use the files handled by the university PC on your home PC, or if you bring your home PC to the university and use it, install and activate the paid antivirus software on your home PC as well.

ウィルス対策をしていない場合は、大学の PC で扱うファイルを自宅の PC で使用したり、自宅の PC を大学で使用したりすることを禁止します。

If you do not have anti-virus measures, you are prohibited from using files handled by the university PC on your home PC or using your home PC at the university.

5．ウィルス対策ソフトの更新

Update antivirus software

ウィルス対策ソフトをインストールしたら、インターネットに接続してソフトウェア自体の更新と、「パタンファイル」の更新を頻繁に行ってください。自動更新機能があれば、それを有効化しておくようにしましょう。

After installing the antivirus software, connect to the Internet and update the software itself and the "pattern file" frequently. If you have an automatic update feature, make sure to enable it.

PC は定期的に（最低一か月に一度は）起動して、更新を実行してください。

Boot your PC regularly (at least once a month) to perform updates.

6．アカウントパスワード

Password of your account

アカウントのパスワードは、英大文字、小文字、数字、記号を各1文字以上使い、

合計８文字以上としてください。

The account password should have at least one letter using each of the following: uppercase letters, lowercase letters, numbers, and symbols, for a total of eight letters or more.

■してはいけないこと

Don't be supposed to do.

7．非正規販売されたソフトウェアのインストール禁止

Prohibition of installation of non-authorized software

正規ルートで購入したソフトウェア以外は、インストールしないこと。

Do not install any software other than the one purchased through the regular route.

極めて廉価に販売されているソフトウェアは、違法に改造され、スパイウェアとして再作成されたものがあり、使用することは非常に危険です。

Some of the software sold at extremely low prices has been illegally modified and recreated as spyware, making it extremely dangerous to use.

特に Adobe の Acrobat/Creative Suite をはじめとするソフトウェアにそのようなものが報告されています。

In particular, such software has been reported in software such as Adobe Acrobat/Creative Suite, etc.

8．研究、学習、業務等に関係ない WEB サイトの閲覧禁止

Prohibition of browsing websites not related to research, learning, business, etc.

研究、学習、業務等に関係ない WEB サイトは極力閲覧しないでください。必要であれば、自宅で閲覧するようにしてください。

Please do not browse websites that are not related to research, learning, work, etc. as much as possible. If necessary, please browse at home.

WEB サイトの閲覧、リンクのクリックで、不正なソフトウェアがダウンロード、インストールされてしまう危険があるためです。

This is because there is a risk that malicious software will be downloaded and installed by browsing the website or clicking the link.

9．WEB サイトで表示された、ポップアップやバナー広告のクリック禁止

Do not click on pop-ups and banner ads displayed on websites

WEB サイトで表示された、ポップア

ップやバナー広告をクリックしないようにしてください。不正なソフトウェアがダウンロード、インストールされてしまう危険があるためです。

Please do not click on the pop-ups or banner ads displayed on websites. This is because there is a risk that malicious software will be downloaded and installed.

１０．ファイル共有（P2P）ソフトウェア、ダウンロードマネージャの使用禁止

Prohibition of using file sharing (P2P) software and download manager

ファイル共有（P2P）ソフトウェア、ダウンロードマネージャ（「Napster」や「Winny」「BitComet」「Vuze」「Shareaza」「迅雷(xunlei)」等）の使用を禁止します。

Use of file sharing (P2P) software and download managers ("Napster", "Winny", "BitComet", "Vuze", "Shareaza", "xunlei", etc.) is prohibited.

１１．フリーウェアの自由なインストール禁止

Free installation of freeware prohibited

フリーウェアの中には、PC から集めた情報を、特定のサイトへアップロードしたりするスパイウェアと呼ばれるものが存在します。

Some freeware is called spyware, which uploads information collected from a PC to a specific site.

他国では一般的でも、日本では不正と見なすものがあるので、フリーウェアをインストールする際は、PC 管理者（講座の先生や部局情報システム管理・運用責任者）に許可を得てからインストールしてください。

Although it is common in other countries, there are things that are considered illegal in Japan, so when installing freeware, install it after obtaining permission from the PC administrator (teacher of the course or department information system administrator / operation manager).

１２．ファイルのアップロードを伴う WEB サービスの利用禁止

Prohibition of using WEB services that involve uploading files

ファイルを PDF に変換したり、PDF から Word/Excel へ変換したり、winmail.dat ファイルを元の形式に変換したりといった、WEB サービス（ブラウザから利用できるもの）は利用しないでください。

Please do not use WEB services (available from browsers) such as converting files to PDF, converting PDF to Word / Excel, and converting

winmail.dat files to their original format.

サイト側でファイルを不当に保持される危険があるためです。

This is because there is a risk that the file will be held unfairly on the site side.

１３．学外でのフリーWi-Fiの利用禁止

Prohibition of using free Wi-Fi off campus

大学の外から山梨大学の各種サービスにアクセスする際、街中、店舗等にあるフリーWi-Fiを使ってはいけません。

When accessing various services of University of Yamanashi from outside the university, do not use free Wi-Fi in the city or in stores.

通信を暗号化していないために重要な情報を盗聴される危険のあるものや、初めから利用者の重要情報を盗み取ることを目的としたWi-Fi局の可能性があるためです。

This is because there is a risk that important information will be eavesdropped on because the communication is not encrypted, or there is a possibility that the Wi-Fi station aims to steal the important information of the user from the beginning.

■注意が必要な（慎重にすべき）こと

Things that need attention (you should be careful about)

１４．USBメモリ使用上の注意

Precautions when using USB memory

USBメモリを介してコンピュータウィルス、マルウェアの感染が拡大するケースが多数あります。USBメモリはPCに挿入の都度、ウィルス対策ソフトでフルスキャンを実施してください。

There are many cases where computer viruses and malware infections spread via USB memory. Perform a full scan with antivirus software each time you insert the USB memory into your PC.

ウィルス対策ソフトが有効化されていても、フルスキャンでなければウィルスが検出されない場合があるので、徹底するようにしてください。

Even if antivirus software is enabled, the virus may not be detected unless it is a full scan, so be sure to do it thoroughly.

１５．E-Mailの使用

Using E-Mail

機密情報を、暗号化や、パスワード設

定なしにメールを使って送付しないでください。またパスワードを相手に伝えるときはできるだけメール以外の手段を使用してください。

Do not send sensitive information by email without encryption or password setting. Also, when giving the password to the other party, please use a means other than e-mail as much as possible.

どうしてもメールで送るしかない場合は、ファイルを送信したメールへの返信ではなく、別の新規メールで送付するようにしてください。

If you have no choice but to send the file by email, please send it by another new email instead of replying to the email that sent the file.

１６．SMS やメールのメッセージに記載されたリンク（URL）への対処

Dealing with links (URLs) in SMS and email messages

下記ルールに従ってください。

Please follow the rules below.

身に覚えのない送信元からの場合：絶対にクリック（またはタップ）しない。

From an unfamiliar source: Never click (or tap).

覚えのある送信元からの場合：実際に有効な URL の「ドメイン名」を確認し、正規のサイトのドメイン名と比較して、正しいことを確認してからアクセスする。

From a source you remember: Check the "domain name" of the actual valid URL, compare it with the domain name of the legitimate site, and make sure it is correct before accessing.

１７．ファイル拡張子の表示

Display file extension

ファイルの拡張子を、デフォルトで「表示する」設定にしておくようにしましょう。注意が必要なファイルかどうかを判断する明確な指標になります。

Make sure to set the file extension to "display" by default. It's a clear indicator of whether a file needs attention.

１８．メール添付ファイルの取扱い

Handling of email attachments

下記ルールに従ってください。

Please follow the rules below.

18-1.身に覚えのない送信元から送られてきた添付ファイルは決して開かず捨てる。

Never open and throw away attachments sent by unfamiliar sources.

18-2.メールに添付されたファイルは、Wクリックして開かず、PC ローカルへダウンロードし、ウィルスチェックをしてから開く。

The file attached to the email should not be opened by double-clicking, but downloaded to the local PC, checked for viruses, and then opened.

18-3.特に拡張子が「exe」「doc|docx」「xls|xlsx」(MS Office のファイル) といったものはウィルスチェックなしに決して開かない。

In particular, extensions such as "exe", "doc | docx", and "xls | xlsx" (MS Office files) should never be opened without virus checking.

１９．リンク（URL）や添付ファイルに「試しに」アクセスしない

Don't try to access links (URLs) or attachments

身に覚えのない送信元からのメッセージに記載された URL や、添付ファイルについては、興味本位で試しにアクセスしたり、ファイルを開いたりしないこと。思わぬセキュリティ事故に遭遇することがあります。

Don't try to access or open files just out of interest, if the message comes from a source you don't know. You may encounter an unexpected security accident

---

■問い合わせ先：情報システム課

Inquiry ： Information Systems Division

・甲府キャンパス：情報メディア館１F

Kofu Campus：Information Media Center 1F

E-Mail : joho@yamanashi.ac.jp

・医学部キャンパス：管理棟３F

School of Medicine Campus: Administration building 3F

E-Mail : joho-med@yamanashi.ac.jp