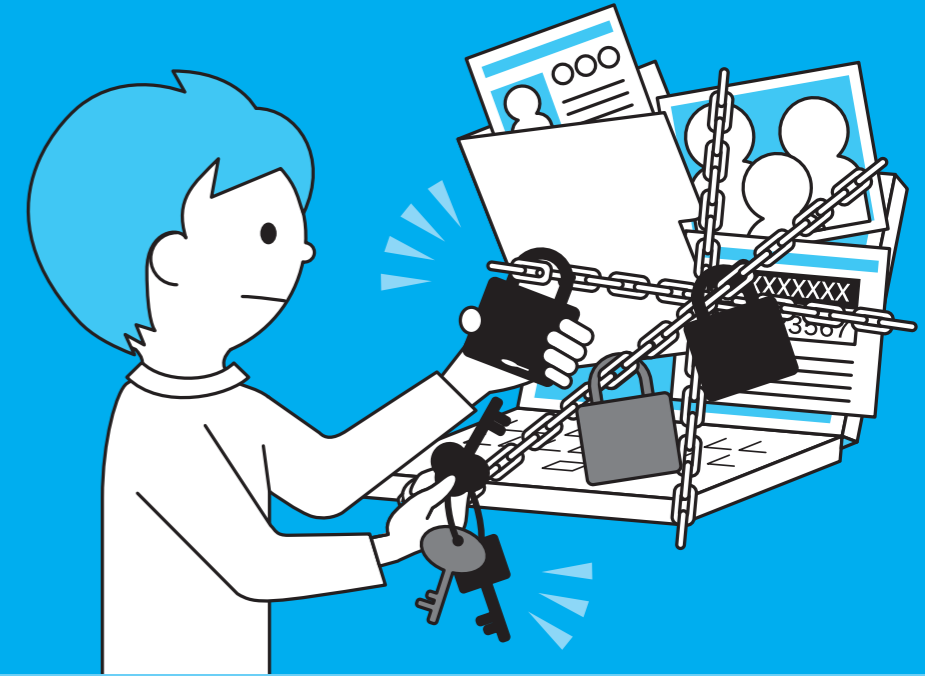


学生・生徒のみなさんへ To All Students

「自分の個人情報自分で守る」
「他人の個人情報、著作権は侵害しない」
という意識が大切です。

The key principles are: "Protect your personal information by yourself" and "Do not infringe on personal information and copyright of others."



Case 1

Webサイト上で見つけた
他人の著作物を
自分のレポートとして
出所を明示しないで提出した。

I submitted someone else's copyrighted material I found on a web site as my report and I didn't indicate the source.



他人の著作物を自分の書いたものとして提出すると剽窃(盗用)にあたり、著作権法に抵触します。引用は認められますが、引用部分を区別する、出典を明らかにするなど引用の要件を厳格に満たす必要があります。それ以外は剽窃として不正行為とみなされます。不正行為が発覚した場合、所属学部において、その時点で履修しているすべての科目の無効、停学を含む厳しい処罰が下されますので、十分に注意してレポートを提出してください。次のような行為は明白に剽窃(盗用)に該当します。

- Web、書籍、他人のレポートなどに掲載されている他人の文章の語句を一部変更した、あるいは語順を変更しただけで自分のレポートとして提出する。
- レポート(論文)共有サイト(サービス)から入手したレポート(論文)を自分のものとして提出する。

To quote someone else's work and to submit it as your own is a violation of the Copyright Act and considered "plagiarism (theft)." Citation is permitted as long as it strictly meets the requirements for citation, such as separating the quoted part from the main text and indicating the source of the citation. If you fail to do so, it is regarded as an illicit act called plagiarism. Any student who is found to be engaged in such illicit act is subject to severe punitive measures by the University, such as, disqualification of enrollment in all courses in the semester and suspension from the University.

All students must be aware of the rules of quoting someone else's work when submitting reports. The following acts, for example, will be regarded as plagiarism:

- To obtain someone else's work from a Web site, a book or a report, and submit it as your own after modifying the words partially or changing the order of the words.
- To submit a report (essay) obtained from a report (essay)-sharing web site (service) as your own writings.

Case 2

出所不明のメールの
添付ファイルやURLを
開いてしまった。

I opened an attached file or clicked a link with an email that comes from an unknown sender.



添付ファイルにウイルス等が隠されていたり、本物のウェブサイトを装った危険なウェブサイトのURLをクリックさせて、PC内の情報を抜き取ったり、他のPCにウイルス等をばらまくなど、重大な問題を引き起こす危険性があります。有線LANを利用している場合はネットワークケーブルを抜き、無線LANを利用している場合は接続を遮断してください。そのあとすぐにヘルプデスクに連絡し、指示を仰いでください。

There is a risk that a computer virus is attached to the file or that an email contains a link to a fake website. These viruses and fake websites would steal confidential information, corrupt data and even attack on other PCs. When it happens, please remove LAN cable from the network or disconnect the network connection if you are using Wi-Fi. Please contact Helpdesk immediately and ask directions.

Case 3

Twitter, facebook, LINE
などのソーシャルメディアや
MyPortfolioなど大学の
システムで不適切な情報を
公開してしまった。

I posted inappropriate information on social media such as Twitter, Facebook, LINE and the university page such as My Portfolio.



個人アカウントによる私的利用であっても、インターネット上に公開された情報には不特定多数の利用者がアクセスでき、一旦発信した情報は完全に削除することができません(公開先を限定していたとしても転載される可能性があります)。インターネットでは匿名性は保証されないことを十分に理解し、責任と良識ある利用に留意しなければなりません。有名人の目撃情報や友人のプライベートな情報を無断で発言すること、自分自身の違法行為や迷惑行為などを暴露するといった事例も数多く存在します。カンニングや飲酒運転等の違法行為、不正行為そのものが許されないことは当然ですが、ソーシャルメディアで発言することにより、想像以上にインターネット上で情報が拡散し、時には大学全体を巻き込んで大きなトラブルに発展する恐れがあります。学生によるソーシャルメディアの不適切な利用が大問題となり、その結果、企業の内定取り消しへとつながった事例も発生しています。また、公開機能を持つ“MyPortfolio”システムでも同様で、公開の際には、自身の責任の元で、利用してください。万が一問題に巻き込まれた場合は所属事務所に相談してください。

Please keep in mind that information you post on the Internet is not only accessible to the general public of various backgrounds and locations, but also it is impossible to delete completely from the internet. This holds true regardless of whether you are logging on to your business or to your private account. (Note that information may be reproduced even if it is designated to be accessible only by a selected few.) Remember that there is no complete assurance of anonymity on the Internet and that even information imparted by an individual could provide the basis for the evaluation of the organization. Be fully responsible for your conduct and do not let your guard down when using social media and social networking sites. There have been many cases of inappropriate posts, such as unauthorized disclosure of information on encounter with famous people or friends' private information, illegal or inappropriate behavior by the person making the post, and so forth. It is needless to say that there is no excuse for illegal or dishonest behavior itself, including cheating, driving under the influence of alcohol, etc., but the negative effects may be exacerbated greatly when these behaviors are exposed on the Internet, and the information may prevail in society much more deeply than the individual expects. Inappropriate use of social media by students has caused enormous problems in the past and in some cases resulted in corporate enterprise canceling offers of employment to the students involved. The same applies to the "MyPortfolio" system, so please exercise caution when publishing information on your portfolio as you are responsible for keeping your information safe. Should you find yourself in any trouble, please consult the administration office of the University.

早稲田大学 情報企画部 IT Strategies Division, Waseda University

相談窓口・連絡先 Contact Information for consultation/inquiries

個人情報保護に関する窓口(総務部法務課)
Consultation about personal information protection (Legal Affairs Section)

E-mail : kojinjoho@list.waseda.jp

早稲田ポータルオフィス
Academic Advising Office

E-mail : itc-support@list.waseda.jp

ヘルプデスク お問い合わせ窓口一覧表
<http://www.waseda.jp/navi/inquiry.html>

Inquiries and IT Desks
<http://www.waseda.jp/navi/e/inquiry.html>

「あなたと情報セキュリティ」ウェブサイト Web site for "Information Security for You"
<https://www.waseda.jp/wits/data/info-sec/index.html>

あなたと 情報セキュリティ Information Security for You





情報セキュリティに関する社会的動向

Trends Related to Information Security

個人情報保護

個人情報とは、当該情報に含まれる内容によって、個人が誰かを識別することができる情報のことを指します。個人情報保護法では、①個人情報の利用目的の明確化および目的外利用の制限、②個人情報の適正な取得と利用目的の通知、③個人情報のデータ内容の正確性の確保と安全管理措置、④従業者、委託先の監督および第三者提供の制限、⑤本人からの求めに応じた個人情報の開示・訂正・利用停止等、について定められています。

著作権

授業内の利用であれば著作権者の許諾なしで著作物を利用可能と思われがちですが、利用可能な範囲には制限があり、著作権者の利益を不当に害するような利用は認められていません。特に、インターネット経由でコンテンツを配信する場合は、たとえ授業内であっても、特別な条件を満たさない限り、著作権者の許諾なしに著作物を利用することはできません。

2010年1月1日施行の改正著作権法において、**違法にアップロードされた音楽・映像といったコンテンツを、それと知りながらダウンロードする行為自体も違法となりました**。また2012年の改正では、違法ダウンロードに対する刑事罰が規定され、2年以下の懲役若しくは200万円以下の罰金、あるいはこの両方が科されることとなりました（2012年10月1日施行）。違法なインターネットサイトから音楽や映像などの著作物をダウンロードすることは絶対にははいけません。

Protection of Personal Information

The term “personal information,” used here, refers to any information that may be used to identify an individual. The main stipulations of the Act on Protection of Personal Information are: (1) clarity about the purposes to which personal information is to be put and restrictions on the use of personal information for purposes other than that for which it has been collected for; (2) the fair collection of personal information and notification of the purposes for which personal information is processed; (3) assurance of the accuracy of personal information and security measures; (4) supervision over workers and contractors and restrictions on the disclosure of personal information to third parties; and (5) disclosure, revision, cease of use, etc. of personal information at the request of the individual concerned.

Copyright

It is often taken for granted to use copyrighted contents in class without obtaining permission from the copyright owners. However, there is restriction to use the copyright and it is not allowed to infringe the copyrighter’s right unrighteously. It is not permitted to distribute the copyrighted contents via Internet without prior permission from the copyright owner, even if the contents are used only for the class puposes.

The revised Japanese Copyright Law, which came into force on January 1, 2010, **also prohibits any knowing downloading of music or video contents that are illegally uploaded to the Internet**. Furthermore, a substantial revision was made in 2012, imposing criminal punishment against illegal downloading. The penalty ranges from a fine of not more than two million yen, up to two years’ imprisonment, or both. (Effective October 1, 2012). It is strictly prohibited to download copyrighted music or video contents from illegal Internet sites.



早稲田大学の取り組み

Initiatives at Waseda University

個人情報保護に関する取り組み 👉 関連 URL 1

早稲田大学では、個人情報保護の重要性を深く認識し、1995年5月26日に「個人情報の保護に関する規則」を設けました。早稲田大学では、その規則や関連法令等を踏まえ、個人情報を適切に保護、管理しております。

情報セキュリティに関する取り組み 👉 関連 URL 1

2002年9月、本学の管理するコンピュータ、ネットワークなどを利用し、情報を取り扱うにあたり、守らなければならない最低限の事項として「早稲田大学情報セキュリティポリシー（以下、ポリシー）」を定めました。ここでは、大学の提供するサービスを利用する者は、このポリシーを遵守する責任があり、意図の有無を問わず、学内外の情報資産に対する権限のないアクセス・改ざん・複写・破壊・漏洩等をしてはならないと定めています。

なお、2012年1月に「情報セキュリティ対策に関する規程」を制定し、情報セキュリティに対する大学の体制を整備し、そのもとでさまざまな対策を行っています。

著作権に関する取り組み 👉 関連 URL 2 3

2003年11月に「WIND（早稲田大学インターネットドメイン）におけるWWW用コンテンツ作成に関するガイドライン」を定め、WINDを利用する上で法規・社会慣行に沿った情報ネットワークの適正な運用を図っています。また2004年3月には「教育・研究を目的とするWebコンテンツにおける著作物の扱いについて」にて注意を喚起しています。

Initiatives for Protection of Personal Information 👉 Reference URL 4

With the aim of promoting protection of personal information, Waseda University established the “Personal Information Security Rules” on May 26 , 1995 . Waseda University protects and manages the personal information based on the the rule and related law and regulations.

Initiatives for Information Security

In September 2002, the University established the “Waseda University’s Information Security Policy” (hereinafter referred to as “the Policy”) which specified minimum rules to be complied with when information is handled via the computers and network systems at the University. The Policy provides that all users of the services offered by the University have the responsibility to observe the Policy and must not engage in any unauthorized access, alteration, reproduction, destruction, leakage, etc. of information assets both within and outside the University, even if it is unintentionally.

Furthermore, the University established "Regulations on Information Security measures" on January 2012, and is taking some measures to meet security requirements.

Initiatives for Protection of Copyright

In addition, the University released the “Guidelines for Creating Contents Used on the World Wide Web by WIND (Waseda’s Internet Domain)” in November 2003, with the aim of promoting proper use of the information network among WIND users in accordance with legislation and social norms. Moreover, in order to raise awareness of this issue, the University issued the announcement on the “Handling Written Materials in a Web Context for Education and Research Purposes” in March 2004 .



各種注意事項

Cautions

個人情報保護に関する注意事項

2015年6月、早稲田大学において標的型攻撃により個人情報の流出が確認されました。他にも、個人情報を保管しているノートPC、USBメモリや紙媒体の名簿等の盗難・紛失事故が発生しています。

学外でも個人情報流出事件・事故が多発しています。例えば、ノートPCやUSBメモリの入った鞆を電車内で盗難されたケース、個人情報を含むデータを自宅に持ち帰り、ウィルス感染したPCからファイル交換ソフトウェアを介して個人情報が流出したケースなどがあります。これらの事件・事故に共通することとして、安易に個人情報を含む文書（紙・データ）や記憶媒体を持ち出していることが挙げられます。

また、**最近**は電子メールの宛先を誤って送信するケースも増えていきます。特に個人情報等機微な情報が含まれていると思われぬところに流出してしまう可能性があるので注意してください。パスワードは他人に安易に解析されないよう大小英字・数字混在8文字以上とし、複数のPCやシステムで使い回さないようにしてください。 👉 関連 URL 5 6

個人情報が記録された文書（紙・データ）や、記憶媒体等を取り扱う際は、次の点に注意してください。

- むやみに持ち出さない。
- 第三者がアクセスできない場所に保存・管理する。
- ノートPC、USBメモリ、外付ハードディスク等はセキュリティ対策機能（暗号化・認証等）がついた製品を使用し、データは暗号化して保管する。また、Winny、WinMx、Shareなどのファイル交換ソフトウェアは、その性質上、コンピュータウィルスへの感染、情報流出の原因となります。ファイル交換ソフトウェアは利用しないでください。

マイナンバーはきわめて重要な個人情報です。大学でアルバイトをしたときなど大学から支払いがあった場合は、大学（委託先業者）からマイナンバーの提供をお願いします。マイナンバーを不正に取得しようとする詐欺が発生する恐れがありますので、**マイナンバーの提供方法はMyWasedaなどで必ずご確認ください**。また、友人など他人のマイナンバーを預かったり控えたりしてはいけません。

コンピュータウィルスに関する注意事項 👉 関連 URL 7 8

コンピュータウィルス（以下、ウィルス）感染を防ぐために、ウィルス対策ソフトウェアを導入することが重要です。しかしそれだけではセキュリティ対策は不十分です。新種のウィルスに対応できるようにウィルス定義ファイルを常に最新の状態にアップデートするように心がけてください。また、Windows/MacなどのOSに限らず、使用しているソフトウェアの脆弱性（セキュリティホール）の有無をインターネットなどでチェックし、定期的に情報収集を行ってください。セキュリティパッチが配付されている場合には、早期にプログラムの修正を行うことが大切です。関連URLに記載している独立行政法人情報推進機構セキュリティセンターのWebサイトでは、緊急対策が必要な脆弱性の報告を参照することができます。

また、早稲田大学では、学内ネットワークでのみ無制限に利用できるウィルス対策ソフトウェアの提供サービスを実施しています。ウィルス対策ソフトウェアを導入されていない方、もしくは更新期限が切れたままのウィルス対策ソフトウェアを使い続けている方は関連URLを参考に導入してください。

ライセンスの適切な運用に関する注意事項

ソフトウェアの不正利用は絶対にしないでください。ソフトウェアの不正利用は「懲役10年以下、罰金1000万円以下」と非常に重い刑罰が法律により定められています。これは、研究・教育活動を目的とする大学組織においても例外ではなく、最近では2010年度末にある国立大学法人がソフトウェアの著作権侵害について多額の和解金を支払う事例もありました。

また、以下の例のように、本人が無意識にソフトウェアの不正利用を行っている危険性もあります。

ソフトウェア不正利用の例

- 研究室、サークル内で他人が購入したソフトウェアを借りて、自分のPCにインストールした
 - 不正コピーされた媒体を購入し、利用している
 - 不正コピーされたソフトウェアをファイル交換ソフトウェアでダウンロードして使っている
 - 疑わしいウェブサイトからダウンロードしたソフトウェアを使っている
- 特に、研究室やサークルなどのグループでソフトウェアを購入、利用する場合には適切な管理体制、手順を設けることが必要になります。以下に、簡単なライセンス管理に関する方法を紹介します。

ライセンス管理方法（例） 👉 関連 URL 9 10

- ソフトウェア管理に関する責任者を定める
- ソフトウェア購入時のライセンス証書、契約書などを大切に保管する
- 以下の内容を含んだライセンス管理台帳を作成する
-購入ソフトウェア名
-利用可能台数
-購入時期、ソフトウェア利用期間
- 以下の内容を含んだ、ソフトウェアをインストールした機器の台帳を作成する（ソフトウェア管理台帳）
-ソフトウェア名
-利用者名、導入機器
-インストール日/アンインストール日
-購入時期、ソフトウェア利用期間
- ライセンス管理台帳、ソフトウェア管理台帳を比較し、定められた数量以上のソフトウェアを利用していないか確認する

Cautions Concerning Protection of Personal Information

In June 2015, highly sensitive personal information in the possession of the University was found to have been unintentionally released. Loss or theft of laptop computers and USB flash memory devices containing personal data has also been reported.

Many other accidents involving leakage of personal information have occurred. For example, a computer storing

personal information was stolen from the owner’s house by a burglar, and a bag for carrying a laptop computer and a USB flash memory device was stolen while the owner moving on a train. It has been also reported that while a person working on some data containing personal information at home, the computer leaked the personal information through file sharing software, and it turned out that the computer had been infected by virus. Common to these cases is that documents (paper-based / data) and storage media containing personal information are taken out of the campus without taking appropriate care.

There have been increasing cases of e-mails being sent to the wrong recipients. Extra caution is advised in order to avoid unexpected abuse of potentially sensitive personal information released unintentionally.

In order to prevent for someone from cracking your password, set yourpassword with more than 8 characters and mix of upper and lower casealphabetical and numeric characters. Do not use the same password in multiple PCs and the systems. 👉 Reference URL 11 12

Please observe the following points when handling documents (paper-based / data), storage media, etc. containing personal information:

- Do not take any documents (paper-based/data), storage media, etc. containing personal information out of the University incautiously without appropriate care.
- Store documents (paper-based data), storage media, etc. containing personal information in places not accessible to a third person.
- Use laptop computers, USB flash memory devices, external hard disk drives, etc. with security features (encryption, user authentication, etc.) and complete the encryption process when storing the data. Do not use file-sharing software such as Winny, WinMX, and Share, as they can cause virus infection and information leakage.

Social security number "My Number" is extremely sensitive personal information. If the payment was made to you by the University, for instance if you did a part time job for the University, the third party vendor may ask you to provide them with your social security number (My number). There may be a risk someone would try to gain access to your social security number (My Number) fraudulently. Please refer to" My Waseda" for how to provide your social security number to others. Do not keep/ notate someone elses' / Friends' social security number (My Number) information.

Cautions Concerning Computer Virus Infections 👉 Reference URL 13

It is important to install anti-virus software to prevent computer virus (hereinafter “virus”) infection. But installing anti-virus software alone is not enough. Please keep your virus definition file updated to the latest version in order to protect your data from new virus. In addition, please collect information regularly via the Internet, etc. to check vulnerabilities (security holes) of all software you use, including OS such as Windows and Macintosh. If security patches are released, please install them and update the software programs as soon as possible. Reports on vulnerabilities that require immediate actions are issued by the Information-technology Promotion Agency (IPA), IT Security Center Section. For more details, please refer to the reference URLs below.

Waseda University also provides an anti-virus software service for free available solely on its campus network. If you have not installed any anti-virus software, or if you are using expired anti-virus software, please consider using this service.

Cautions Concerning Appropriate Use of Licenses

Abuse of software is strictly prohibited. The abuser is subject to extremely serious punishment decreed by law, defined as “up to ten years in prison and up to 10 million yen in fines.” No exception applies to university organizations for research and education. As recently as the end of fiscal 2010, a national university corporation paid an enomous amount of money to settle a software copyright infringement claim made against it.

In addition, as in the examples below, there is a risk that some users may be unintentionally committing abuse of software.

Examples of software abuse

- To borrow software bought by someone else in your laboratory/faculty room or student club, and install it on your own computer
- To buy and use an illegally-copied media
- To download and use illegally-copied software from the Internet or P2P software
- To download software from an suspicious website or an unauthorized website and use it

In particular, software bought for groups such as laboratories/faculty rooms and student clubs must be used under appropriate management methods and procedures. The following is an example of simple method for license management.

License Management Method (example)

- Choose a person who will be responsible for software management.
- Store the license certificate and the contract obtained at the time of software purchase in a safe place.
- Create a License Management Register with the following categories.
 - Name of the purchased software
・ The number of installations allowed
 - Date of purchase and duration of software use
- Create a register of the devices in which the software has been installed. Include the following categories in this register (as a Software Management Register).
 - Name of the software
・ Name of users and name of devices in which the software has been installed
 - Date of installation/uninstallation
・ Date of purchase and duration of software use
- Compare the License Management Register with the Software Management Register and confirm that the number of computers/devices using the same software does not exceed the number of the purchased software licenses.

👉 関連 URL /Reference URL

- 早稲田大学「個人情報の保護に関する規則」[情報セキュリティポリシー] https://www.waseda.jp/top/privacy-policy
- 早稲田大学「WINDにおけるWWW用コンテンツ作成に関するガイドライン」 http://www.waseda.jp/wits/RULES/rule_guideline.html
- 早稲田大学「教育・研究を目的とするWebコンテンツにおける著作物の扱いについて」 http://www.waseda.jp/mnc/kamoku/COPYRIGHT/warning.html
- Waseda University “Privacy Policy” https://www.waseda.jp/top/en/privacy-policy
- Waseda ID 取得・変更 http://www.waseda.jp/navi/mywaseda/wasedaid.html
- パスワード変更 http://www.waseda.jp/navi/mywaseda/passwd.html
- 独立行政法人情報処理推進機構セキュリティセンター「重要なセキュリティ情報一覧」 http://www.ipa.go.jp/security/announce/alert.html
- 早稲田大学「Sophos Anti-Virusの利用」 http://www.waseda.jp/navi/rental/soft/sophos.html
- ビジネス ソフトウェア アライアンス（BSA） http://www.bsa.or.jp/
- SAM（Software Asset Management）ポータル ※各種テンプレートがダウンロードできます。 http://www.bsa.or.jp/psamportal/
- Create or Change Waseda ID http://www.waseda.jp/navi/e/mywaseda/wasedaid.html
- Changing your Password http://www.waseda.jp/navi/e/mywaseda/passwd.html
- IT Security Center, IPA “Security Alerts” http://www.ipa.go.jp/security/english/securityalerts.html