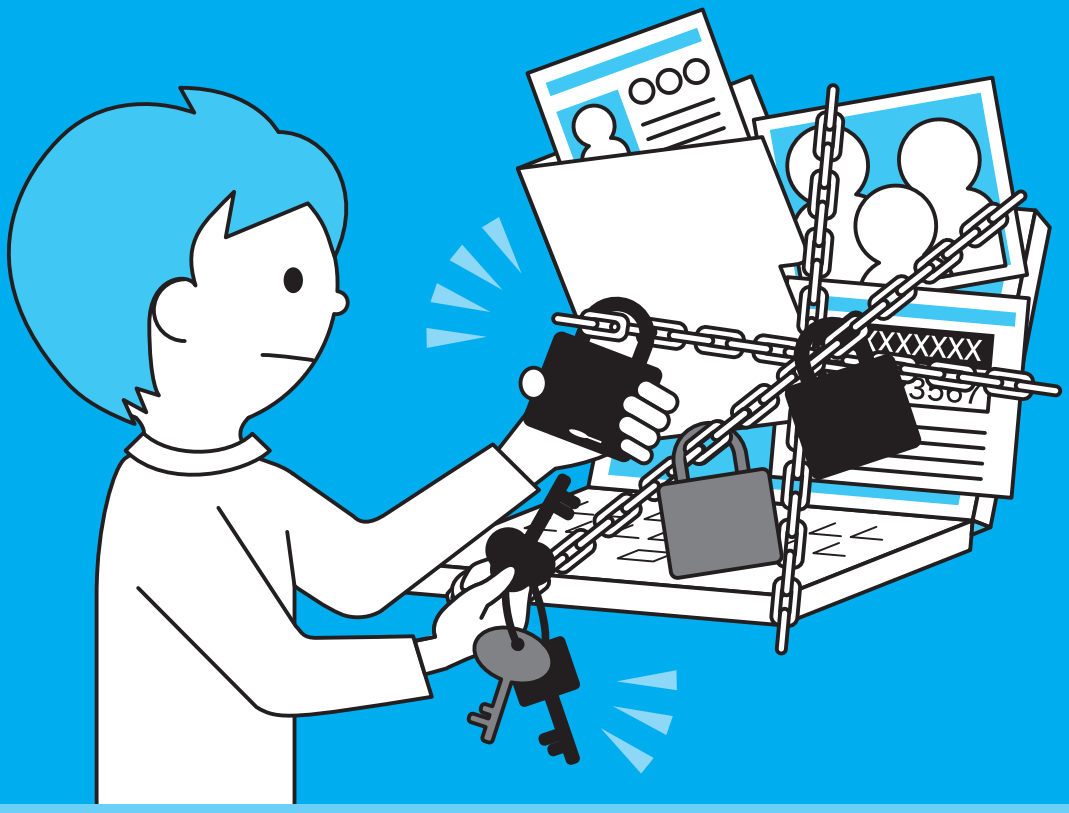
学生・生徒のみなさんへ

「自分の個人情報は自分で守る」
「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。



あなたと情報セキュリティ

Information Security for You

WASEDA University
早稲田大学

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。

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、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。

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。

添付ファイルにウィ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にウィ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。

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。

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。

早稲田大学 情報企画部

相談窓口・連絡先

- 個人情報保護に関する窓口（総務部法務課） E-mail : kojinjoho@list.waseda.jp
- 早稲田ポータルオフィス E-mail : itc-support@list.waseda.jp
- ヘルプデスク お問い合わせ窓口一覧表 https://www.waseda.jp/navi/inquiry.html

「あなたと情報セキュリティ」ウェブサイト

https://www.waseda.jp/wits/data/info-sec/index.html

Last Updated: 2021/4/1

情報セキュリティに関する社会的動向

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

2020年4月28日施行の改正著作権法により、第三者著作物の利用について、授業内の利用であれば、インターネット経由でコンテンツを配信する場合においても許諾なく利用可能となりました。ただし、「必要と認められる限度であること」、「著作権者の利益を不当に害しないこと」が前提となるので、適切な利用を心掛けてください。

2021年1月1日施行の改正著作権法において、**違法にインターネット上に掲載された著作物（侵害コンテンツ）のダウンロード規制の対象が、音楽・映像から全ての著作物（漫画、雑誌、小説、写真、論文、コンピュータープログラムなど含む）に拡大されました。**正規版が有料で提供されている著作物に係る侵害コンテンツを反復・継続してダウンロードした場合には、刑事罰（2年以下の懲役または200万円以下の罰金（またはその両方））の対象にもなります。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してはいけません。文化庁のホームページ等を参照して正しい知識を身につけましょう。 **関連URL 1**

早稲田大学の取り組み

個人情報保護に関する取り組み **関連URL 2**

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 2**

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。

研究情報を守るための取り組み **関連URL 3**

「研究情報を守るためのセキュリティガイドライン 」では、重要な研究情報を「漏えい」「改ざん」「消失」等の脅威から守るうえで参考となる「セキュリティ対策の考え方」や「セキュリティ対策の具体的な実施例」等を紹介しており、セキュリティ対策に役立てられるようにしています。

著作権に関する取り組み **関連URL 4 5**

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。

各種注意事項

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メモリの入った鞄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ます。特に個人情報等機微な情報が含まれていると思わぬところに流出してしまう可能性があります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 6 7**

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。

(1)むやみに持ち出さない。
(2)第三者がアクセスできない場所に保存・管理する。
(3)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することがあります。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 8 9**

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 10**

(1)ソフトウェア管理に関する責任者を定める
(2)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
(3)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
(4)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
(5)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

関連URL /Reference URL

1 文化庁「著作権」 https://www.bunka.go.jp/seisaku/chosakuken/
2 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
3 早稲田大学「研究情報を守るためのセキュリティガイドライン」 https://www.waseda.jp/wits/RULES/ResearchInformationSecurity.pdf
4 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」 https://www.waseda.jp/wits/RULES/rule_guideline.html
5 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」 https://www.waseda.jp/mnc/kamoku/COPYRIGHT/warning.html
6 Waseda ID 取得・変更 https://www.waseda.jp/navi/mywaseda/wasedaid.html
7 パスワード変更 https://www.waseda.jp/navi/mywaseda/passwd.html
8 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」 https://www.ipa.go.jp/security/announce/alert.html
9 早稲田大学「Sophos Anti-Virusの利用」 https://www.waseda.jp/navi/rental/soft/sophos.html
10 ビジネス ソフトウェア アライアンス（BSA） https://bsa.or.jp/