あなたの生活や研究を守り、
安全で充実したJAIST生活をおくるために

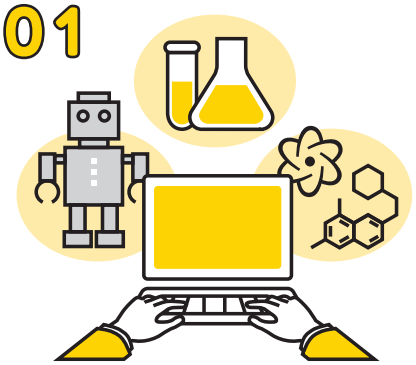
情報セキュリティパンフレット

研究活動や日常生活にとってコンピュータやインターネットは欠かすことの出来ない重要なツールとなっています。一方で、その利用にはさまざまな危険も伴い、使い方を誤ると、あなたの研究や生活が脅かされたり、人生を狂わされることにもなりかねません。本学では、あなたの生活や研究を守るために、情報セキュリティポリシーやソーシャルメディアガイドラインなどを規則/ルールとして定めています。本学の構成員であるあなたは、これらを必ず守らなくてはなりません。

本学の情報環境システムを利用する前に、本パンフレットの最終ページのチェックリストを確認し、チェックしてください。
もし、該当しないもの・よくわからないものがあればパンフレット内の説明を読み、ルールに従って情報環境を利用してください。

情報セキュリティ対策

01



JAIST の ICT 環境は教育・研究のためのものであると理解して利用します。

どのような利用が教育･研究目的と認められるかについては、各々の研究内容に強く依存するので一概な判断はできませんが、目的外利用を疑われた場合に自ら教育･研究目的の利用であると主張できるかどうかを考えてみてください。特に学生は、その主張を指導教員が認めてくれるかが判断材料となるでしょう。判断に迷う場合は、予め指導教員と相談してください。

02

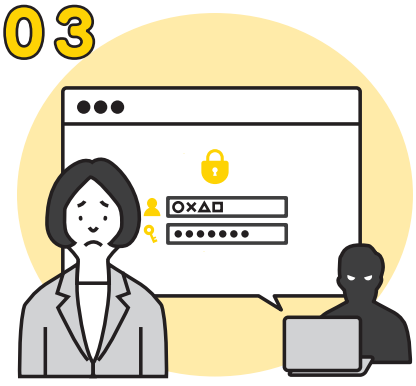
簡単なパスワードを設定しません。パスワードは他人に教えません。

パスワードは他人が推測することが難しい十分な複雑さがあるもの(※)を設定してください。また、学外サービスと同じパスワードを使い回し、そのサービスからのパスワード漏えいにより不正アクセスされた事例があります。パスワード管理ソフトなどを活用し使い回しをやめましょう。当然、あなたのユーザ名とパスワードを他人に教えてはいけません。他人に使わせた場合、何をされようがすべての責任をあなたが被ることになります。

なお、本学職員があなたにパスワードを開示するよう求めることは絶対にありません。

※10文字以上で、複数の文字種(大小文字, 記号, 数字)を組み合わせたもので、あなたが覚えやすいものがお勧めです。ユーザ名や自分の名前、誕生日や電話番号、キーボードの並びなどは容易に推測されます。
詳しくは末尾記載の「補足情報・リンク集」を参照ください。

03



他人のユーザ名 / パスワードを使うなど不正アクセスはしません。

セキュリティホールなどを利用して許されていないシステムに不正に侵入するなどといった行為だけではなく、何かしらの方法で入手した他人のユーザ名/パスワードを使って他人に成りすましてサービスを利用したり、執拗に同じページをアクセスし続けることで気づかぬうちにサービスに悪影響を生じさせてしまった場合でも、不正アクセス行為と判断され刑事･民事責任を問われる場合があります。

04

OS やアプリケーションの定期的な更新を行い、ソフトウェアを最新の状態で使います。

コンピュータウィルスは,OS(WindowsやmacOSなど)やよく利用されるソフトウェア(Office,Javaなど)の欠陥を悪用して感染します。

「Windows Update」や「ソフトウェア・アップデート」を定期的に行い、常に最新の状態に保ちましょう。その他のソフトウェアも常に最新版に更新しましょう。最新のセキュリティパッチが自動的に適用される設定で使うことをお勧めします。

また、PC以外のスマートフォンやネットワーク機器（無線LANルータ等）、IoT機器（インターネット家電など）など、ネットワークに接続するものを常に最新版に更新しましょう。

05

本学指定のアンチウィルスソフトウェアを利用します。最新のウィルスの定義ファイルに常に使用します。

PCがマルウェアに感染すると、PCのデータの破壊/漏えいといった直接的な被害が発生したりする場合以外にも、パソコン自体が遠隔操作され、迷惑メールの配信や他所への攻撃に利用されることもあります。マルウェアは、メールなどで送られてくるだけでなく、Webページ、USBメモリ等、様々な経路から感染します。不注意な操作でマルウェアに感染しないよう、本学の要件に合致するアンチウィルスソフトウェア(※)を利用し、ウィルスの定義ファイルも定期的に更新してください。

アンチウィルスソフトウェアとしては、たくさんの種類のものが販売・配布されていますが、中には性能に疑問があり十分な効果がみられないものもあります。
そこで本学では、使用すべきアンチウィルスソフトウェアの要件を定めています。
詳しくは末尾記載の「補足情報・リンク集」を参照ください。

06

フィッシングメールや不審な Web ページは開かないように注意しています。

銀行やクレジットカード会社、携帯電話会社、ポータルサイトなどを騙り個人情報等を盗もうとするフィッシングメールには注意してください。不審なメールがあった場合は、そのメールに書いてある連絡先ではなく大元の会社などに問い合わせましょう。

SNS や検索エンジンなどで見つけられる海賊版ソフトウェア、著作権上問題がある動画 / 音楽 / 漫画、違法な薬物 / 武器 / ポルノ、個人情報等を販売する Web サイトにはアクセスしないでください。不法行為で処罰されるだけでなくマルウェアに感染する可能性があります。

情報セキュリティ対策

07

個人情報や研究に関するデータの管理を徹底し、情報漏洩の対策を講じます。

大学では様々な教育研究活動が行われており、その中で個人情報や研究に関する文書やデータを取り扱う場面があります。教職員はもちろんですが、学生であっても自分自身の研究に関する研究データや講義などで個人情報を取り扱うかもしれません。

研究に関するデータや法人文書などは本学の情報格付けガイドラインに従って適切に取扱いましょう。特に研究データの中で武器や軍事転用可能なものなど安全保障に関わるものは国外への持ち出しが制限される場合があります。電子メール等で操作する場合にも宛先間違いや誤操作に注意しましょう。

08

他者の著作物を違法にコピーしたり、インターネット上で第三者が閲覧可能な状態にしたりしません。

書籍や論文、レポート、音楽、映像だけではなくWebページに掲載された文章や画像、ソフトウェア、アプリケーションも著作物です。著作権者の許諾なしに、法律で許されている範囲外で著作物を複製したり、ネットワークで第三者が閲覧可能な状態にするのは違法です。

また、著作権を侵害してアップロードされている音楽や映像などを、その事実を知りながらダウンロードすることも違法となります。

09

SNSなど、ネットへの情報発信は、本学の構成員としてモラルをもって行います。

インターネット上の発言やふるまいは、多くの人の目に触れる可能性があり、個人の安易な書込みからトラブルが引き起こされたり、本学や本学構成員の良識が疑われるなどの事態が起こりかねません。本来秘密にすべき事項や公序良俗に反する内容の書き込みなど不適切な情報発信を行わないように注意してください。本学のソーシャルメディアガイドラインを理解し、SNSにおける情報発信をする場合の基本的な心得を理解してください。

10

学外者に本学ネットワークを利用させません。

学外者に対し本学LAN(無線/有線)への接続性を提供することは、学内限定で提供されている情報やサービスへのアクセスさせることになり、大学全体を危険に晒します。
このため、ゲストの利用が許されているものを除き、許されません。

また、検閲回避などを目的にVPNや通信匿名化のアプリケーションを学内で使用すると、他人にインターネット接続性を提供することになり、世界中のユーザに学内限定情報等へのアクセスされ、非常に危険です。これらのアプリケーションを学内で不用意に利用してはいけません。

11

法に抵触したり、セキュリティを脅かすアプリケーションは使いません。

一見便利なアプリケーションでも、仕組みのよくわからないものには注意してください。
例えば、ファイル交換アプリケーション(特にP2P型と言われるようなもの)の中には、他人が共有したファイルを転送する自動公衆送信機能を持ち、結果として意図せず不法行為を行ってしまうものがあります。

アプリケーションの仕組みや評判などをきちんと調べ、法に抵触したり、セキュリティを脅かす可能性がある場合、利用前に指導教員や情報社会基盤研究センターに相談してください。

法に抵触したり、セキュリティを脅かす可能性が高いアプリケーション例

- 通信匿名化 /VPN/ 通信制限迂回アプリケーション
  VPNgate、Tor、Hotspot Shield、SpotFlux、Hola Unblocker、Mobility XE、Freenet、Hamachi 等
- 自動公衆送信機能を持つファイル共有アプリケーション
  Xunlei、LimeWire、Cabos、Winny、WinMX、Share、eMule、Perfect Dark 等

12

情報セキュリティに関する問題を発見した際の相談 / 報告窓口を把握しています。

攻撃側の技術も年々進化しており、どんなに十分注意していても、フィッシングに引っ掛かったりマルウェアに感染したりする可能性があります。このような際に、迅速に報告・相談頂くことがなにより重要です。

あなた自身がマルウエアに感染するなどトラブルが発生した場合はもちろんですが、あなたが本学の情報システム上にセキュリティ上の脆弱性や不具合を見つけた場合、著作権の侵害行為や機密情報や個人情報等が漏洩されている場合、または学外の情報システムで大学の機密情報や本学構成員の個人情報等が公開されていることを見つけた場合なども速やかにJAIST CSIRTに連絡ください。

※JAIST CSIRTへの連絡先は次のページに記載されています。

CHECK!

- 01 ☐ JAISTのICT環境は教育・研究のためのものであると理解して利用します。
- 02 ☐ 簡単なパスワードを設定しません。パスワードは他人に教えません。
- 03 ☐ 他人のユーザ名/パスワードを使うなど不正アクセスはしません。
- 04 ☐ OSやアプリケーションの定期的な更新を行い、ソフトウェアを最新の状態で使います。
- 05 ☐ 本学指定のアンチウィルスソフトウェアを利用します。
- 06 ☐ フィッシングメールや不審なWEBページは開かないように注意しています。
- 07 ☐ 個人情報や研究に関するデータの管理を徹底し、情報漏洩の対策を講じます。
- 08 ☐ 他者の著作物を違法にコピーしたり、インターネット上で第三者が閲覧可能な状態にしたりしません。
- 09 ☐ SNSなど、ネットへの情報発信は、本学の構成員としてモラルをもって行います。
- 10 ☐ 学外者に本学ネットワークを利用させません。
- 11 ☐ 法に抵触したり、セキュリティを脅かすアプリケーションは使いません。
- 12 ☐ 情報セキュリティに関する問題を発見した際の相談/報告窓口を把握しています。

ただし、これらの一部について研究目的など正当な理由がある場合には例外的に認められる場合があります。事前に本パンフレット末尾の問い合わせ先までお問い合わせください。

情報セキュリティに関する問題の相談 / 報告窓口

JAIST CSIRT

JAIST
JAPAN ADVANCED INSTITUTE OF SCIENCE AND TECHNOLOGY
1990

E-mail
sec-incident@ml.jaist.ac.jp

通報URL
https://www.jaist.ac.jp/csirt/

本パンフレットの補足情報・リンク集
https://www.jaist.ac.jp/iscenter/security/

0761-51-1300
（情報社会基盤研究センター/平日日中）

0761-51-1000
（防災センター/休日・夜間）

制作 JAIST 情報社会基盤研究センター (2021.09)