Fiscal year **2023**

NAGOYA UNIVERSITY INFORMATION SECURITY

名古屋大学情報セキュリティ

情報セキュリティインシデント発生時の連絡先

052-747-6389 (内線：6389)

security@icts.nagoya-u.ac.jp

情報セキュリティガイドラインをよく読みましょう。

本学では情報セキュリティポリシーに基づき、情報セキュリティガイドラインを定めました。
名古屋大学キャンパス情報ネットワーク（NICE）に接続する情報機器の利用にあたっては、
セキュリティポリシーおよびガイドラインをよく理解してから利用してください。

認証情報（ユーザ名とパスワード）の管理

あなたがパスワードを友達に漏らした場合、その友達はあなたになりすますことができます。その友達がネットワーク犯罪等を行った場合、あなたの責任を問われることがあります。パスワードは、絶対に他人に漏らさないようにしてください。パスワードを紙にメモしておく場合には、鍵のかかる場所に保管するなど管理を厳重にしてください。また、利用するサービスごとに、異なるパスワードを使ってください。
世の中にはパスワードを解読するツールも存在します。辞書に載っている単語やその組み合わせ、文字数の少ないものなどは簡単に解読できてしまいます。英数字だけでなく記号を含めてランダムに生成した10文字以上のものを使用することが望ましいです。

セキュリティパッチの適用

使用している情報機器の基本ソフトウェアやアプリケーションソフトウェアにセキュリティ上問題となる不具合が発見された場合には、ソフトウェアの製造元から修正プログラム（セキュリティパッチ）が配布されます。利用者は、定期的にウェブページ等に掲載される注意情報・更新情報を確認し、必要な対応をとる必要があります。
また、古いソフトウェアの中にはサポートが終了して修正プログラムが配布されないものがあります。このようなソフトウェアは使用せず、最新のものにアップグレードしてください。
情報連携推進本部のホームページには、OSやアプリケーションソフトウェアの脆弱性情報が掲載されていますので、適宜参照してください。
Windows Update、Microsoft Updateなどセキュリティパッチを自動的にインストールする機能は極力オンとしておきましょう。

コンピュータウイルス

コンピュータウィルスは、主に電子メールによって感染します。その感染のさせ方は、年々巧妙になっています。例えば、クレジットカード会社を装ったメールが大量に送信されており、メールに記載されたリンクにアクセスするとウイルスをダウンロードさせられます。多くの場合、差出人は詐称されていますので、たとえ親しい人からの電子メールであっても怪しい添付ファイルは開かないように注意してください。
感染したウィルスによっては、ネットワークにつながった大量のコンピュータを自動的に攻撃することがあります。また、感染したウィルスによって不正アクセス用の侵入口が作られ、これを通じて知らないうちに、他を攻撃する加害者になっていることもあります。
ウィルスに感染したと思われる場合には、ネットワークから機器を切り離し（LANケーブルを抜く、Wi-Fiをoffにして）情報セキュリティインシデント発生時の連絡先に連絡してください。

フィッシング・スミッシング

金融機関やスマートフォンメーカからの電子メールと装って、クレジットカード番号や暗証番号、パスワード等を盗み出すサイトに誘導し、入力させるフィッシング詐欺が広がっています。不審な電子メールは開かない。怪しいWebページにアクセスしない、疑わしいサイトからはアプリやプログラムのダウンロードを行わないといった注意が必要です。スマートフォンなどのSMS（ショートメッセージサービス）を利用し、認証情報や暗証番号等を盗み出すスミッシング被害も増加しています。
万が一、怪しいWebページなどにアクセスした場合は、ネットワークから機器を切り離し（LANケーブルを抜く、Wi-Fiをoffにして）情報セキュリティインシデント発生時の連絡先に連絡してください。

著作権、知的所有権

音楽CDやソフトウェアを著作権者に無断でコピーし、配布することは著作権法違反です。このような目的でP2Pソフトウェアを利用することもいけません。他人が作成した図、写真、ロゴなどを著作権者に無断でWebページの作成材料に使ったり、ネットワーク等を介して配布、交換してはいけません。ソフトウェアの不正取得（海賊版の購入やWinny等での入手）および使用をしてはいけません。不正利用を防ぐため、Winny等のP2Pソフトウェアの利用については、名古屋大学および他の複数の組織が著作権違反の有無について監視をしています。ファイル交換ソフトウェアのうち、Winny、WinMX、Share、Gnutella、Xunlei、BitTorrentは原則使用禁止です。違法配信されている音楽・映像をその事実を知りながらダウンロードする行為は違法です。

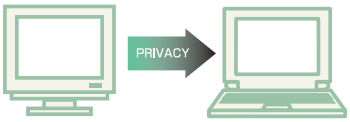
情報漏洩

試験問題や成績情報をコンピュータのハードディスクにそのまま保存することは、重要な情報の漏洩につながる可能性があるのでしてはいけません。情報管理・漏洩対策をする機器（ハードウェアキーなど）を導入して暗号化するなどの対策をとってください。
個人情報の持ち出しについては、東海国立大学機構個人情報保護規程の指示に従ってください。重要な情報を入れたノートブック型コンピュータを持ち歩く場合には、紛失や置忘れ等により情報が漏洩しないように細心の注意が必要です。列車の席等での作業では、隣席から内容が見えることがあり、情報の種類によっては問題になることも考えられます。

不正アクセス

不正アクセス禁止法（正式には、「不正アクセス行為の禁止等に関する法律」）は、認証情報を貸与されていない人、つまり利用する資格のない人がコンピュータを利用しようとすることを禁止しています。違反した場合には刑事罰（3年以下の懲役又は100万円以下の罰金）に科せられることがあります。
他人の認証情報を利用する行為、またその行為を助ける行為は、不正アクセス禁止法に違反します。書き換え権限のない情報を改ざんしたり、破壊したりする行為も、不正アクセス禁止法に違反します。

プライバシー



他人のプライバシーに関する情報を本人の同意なしに電子メールや掲示板等で発信することは避けるべきです。また、SNSなどに掲載することも避けるべきです。
たとえ親しい人からの問合せであっても、他人のメールアドレス等プライバシーに関わる情報をむやみに教える事は避けるべきです。本人の同意を得てから回答するなど、適切な配慮を心がけましょう。

新入生情報セキュリティ研修

情報セキュリティのレベルを適切に維持するためには、利用者一人一人の自覚と情報セキュリティに関する知識の習得が重要になります。情報連携推進本部では、新入生に新入生情報セキュリティ研修を実施しています。必ず受講してください。新入生情報セキュリティ研修に合格することで学内のサービスが利用できるようになります。

►https://icts.nagoya-u.ac.jp/ja/security/training.html

年次情報セキュリティチェック

名古屋大学に所属するすべての人が、情報セキュリティガイドラインを遵守することにより名古屋大学のセキュリティレベルが適切な水準に保たれていることを確認し、さらに、情報セキュリティ対策が妥当であるかどうかを確認するため、毎年度、年次情報セキュリティチェックを実施しています。必ず実施してください。年次情報セキュリティチェックを受講していないと、アカウントロックのペナルティを受け、学内のサービスが利用できなくなります。

►https://icts.nagoya-u.ac.jp/ja/security/annual-check.html

新入生は、“新入生情報セキュリティ研修”と“年次情報セキュリティチェック”の両方を実施する必要があります。

Link集

名古屋大学 情報連携推進本部 ・・・・・・・ https://www.icts.nagoya-u.ac.jp/
JPCERT コーディネーションセンター ・・・・・ https://www.jpcert.or.jp/
情報処理推進機構 セキュリティセンター ・・・ https://www.ipa.go.jp/security/
警視庁サイバーセキュリティインフォメーション ・・ https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/
内閣サイバーセキュリティセンター ・・・ https://www.nisc.go.jp/
@police ・・・・・・・・・・・・・・・・ https://www.npa.go.jp/cyberpolice/

名古屋大学情報連携推進本部

Information & Communications

名古屋大学情報連携推進本部

名古屋大学の情報関連施策全般について、各部局等を総合的に調整し、情報サービス及び情報の高次利活用を推進することを目的に平成18年4月1日に情報連携統括本部として発足し、令和2年4月1日より情報連携推進本部に名称変更されました。

セキュリティインシデント対応

サイバーテロ、ネットワーク犯罪を含むさまざまなセキュリティインシデントが発生した場合、責任者、担当者に連絡を取り、インシデントの調査を行います。重大なインシデントの場合は、ネットワークやシステムの遮断や停止を行い、要因を特定し、復旧を支援します。その後、再発防止策を検討します。

セキュリティ情報の収集、提供

情報技術は日々進歩しており、事前に予測できないような新たな問題が発生することがあります。情報連携推進本部は、最新のセキュリティに関する技術情報を収集し、学内の情報セキュリティレベルを最新の状態に保つように努力します。また、新たなコンピュータウィルス、セキュリティホール等の情報を電子メール、ウェブ等を通じてみなさまに提供します。ITヘルプデスクでは、皆様からの情報を受け付けております。

▶ITヘルプデスク
TEL:052-747-6389
Mail:security@icts.nagoya-u.ac.jp

セキュリティの啓発活動

名古屋大学のすべての構成員の情報セキュリティ意識を向上し、高いレベルのセキュリティを維持することを目的として、新入生に対するセキュリティ研修、システム管理者に対するセキュリティ技術の講習会などを企画し、実施します。