名古屋大学情報セキュリティガイドライン

平成 23 年 6 月 23 日改定
平成 24 年 6 月 28 日改定
平成 24 年 8 月 8 日改定
平成 24 年 10 月 25 日改定
平成 25 年 10 月 24 日改定
平成 27 年 1 月 15 日改定
平成 27 年 12 月 24 日改定
平成 28 年 2 月 23 日改定
平成 28 年 12 月 22 日改正
平成 30 年 2 月 22 日改正
平成 31 年 2 月 28 日改正
令和 2 年 7 月 2 日改正
令和 3 年 2 月 24 日改正
令和 4 年 2 月 24 日改正
令和 5 年 2 月 16 日改正
令和 5 年 7 月 4 日改定
令和 7 年 2 月 27 日改定
令和 7 年 10 月 23 日改定

名古屋大学

－ 目　　次 －

名古屋大学情報セキュリティガイドライン

はじめに

この名古屋大学情報セキュリティガイドライン（以下、「本ガイドライン」と略称）は、「名古屋大学情報セキュリティポリシー」（平成 14 年 3 月 19 日 評議会決定、平成 23 年 6 月 21 日 改定、平成 28 年 4 月 1 日 改定）に基づいて定められたものです。

本ガイドラインは、名古屋大学（以下、「本学」と略称）の全ての情報設備機器（以下、「情報機器」と略称）や情報ネットワークを利用するものに適用されます。したがって、全学的に運営される名古屋大学キャンパス情報ネットワーク（Nagoya University Integrated Communication Environment、以下「NICE」と略称）に接続するすべての情報機器に適用されます。パーソナルコンピュータやスマートフォン・タブレット端末など、特定の個人専用となる情報機器の場合でも、NICE に接続していれば、本ガイドラインが適用されます。

本学のすべての部局と構成員は、本ガイドラインを遵守することが求められます。そのため、各部局の責任者は、構成員に本ガイドラインの内容を周知せねばなりません。本学構成員でない場合であっても、本学の図書館等における情報機器の利用者（図書館の外来利用者、各種学会等でのネットワーク設備の利用者等）は、本ガイドラインを遵守せねばなりません。各部局は、本ガイドラインで述べられていない事項で部局において必要な項目を、独自に定めることができます。

本ガイドラインは、

第 1 章 情報システム利用ガイドライン（利用者心得）
第 2 章 危機管理ガイドライン
第 3 章 セキュリティ技術ガイドライン（管理者心得）
第 4 章 クラウドサービス利用ガイドライン
第 5 章 情報セキュリティ研修・啓発ガイドライン

の 5 章から構成されており、それぞれは独立した内容となっています。特に、サーバやパソコンなどを管理されている方は第 3 章を詳細にお読みください。

本ガイドラインは、今後、運用を続けていく中で、情報通信技術環境の変化に合わせて、随時、追加及び修正を行っています。また、現時点で想定されない事項や変化に対しても、随時対応します。ガイドライン違反や広報に関するガイドラインに関する事項も、本ガイドラインで規定することは避け、関係する委員会等での所轄としました。

第 1 章　情報システム利用ガイドライン（利用者心得）

1.1 概要

この利用者心得は、本学が研究や教育目的で提供するコンピュータ（研究室等で導入したパーソナルコンピュータも含む）などの情報機器やデータベースなどの情報資源の利用について、利用者に留意していただきたい具体的な情報を指針として提供しようとするものです。提供されるのは、次のような項目に関する指針です。

1. セキュリティ意識の向上
2. 利用の開始
3. 情報機器の利用
4. 情報の受信と生成
5. 情報の管理
6. 情報発信
7. ウェブ会議システム
8. テレワーク
9. 危機管理
10. 相談窓口

なお、パーソナルコンピュータやワークステーション等の機器を導入しようとする人は、機器管理者にもなりますので、この章とともに「第 3 章　セキュリティ技術ガイドライン（管理者心得）」も読んでください。

1.2 セキュリティ意識の向上

1.2.1 認証情報の管理

コンピュータやネットワークにアクセスするための認証情報は、本人だけのものです。他人に使用させたり、貸与したり、公開することは認められません。例えば、認証情報としては、名古屋大学 ID、機構アカウント、部局・講座が発行するアカウント（部局、講座のメールアカウント等）、個人管理のアカウント（各自のパソコンのアカウント等）のパスワードなどがあります。

認証の方法としては、利用者の知識を用いた認証（例えば、ID とパスワード）、利用者が所有しているものを用いた認証（例えば、IC カード）、利用者の生体情報を用いた認証（例えば、指紋認証）などがあります。複数の認証方法を組み合わせた多要素認証が利用できる場合は、これを用いることを推奨します。学外からアクセス可能なサーバにおいて要保護情報を取り扱う場合は、多要素認証を必ず利用してください。

パスワード認証においては、パスワードを適切に管理することが必要です。簡単に推測可能なパスワードは使用しないでください。パスワードの長さは、10 文字以上とし、英大文字、英小文字、数字、記号の 4 種類を使用するようにしてください。また、パスワードは、サービスや情報システム毎に異なるパスワードを使用するようにしてください。情報連携推進本部や機器管理者からパスワード変更の指示を受けた場合、あるいはパスワード情報が漏洩した疑いがある場合は、速やかにパスワードを

変更してください。変更後のパスワードは変更前のパスワードと類似しないようにしてください。

注意事例

- 利用者の氏名、ユーザ名から容易に推測できる文字列、辞書の見出し語、あるいはその一部を数字で置き換えたパスワードは簡単に推測可能なため、パスワードには使用しないでください。例えば、「123456」、「asdfgh」、「password」、「passw0rd」のようなパスワードは不適切です。
- パスワードを使いまわすと、いずれかのサービスでパスワードが漏えいしたときに、その他のサービスまでも不正アクセスの被害にあう危険性が高まります。
- 教育補助業務を依頼している学生に教員が自分のパスワードを教えてはいけません。教員は、学生の不適正な行為の責任を引き受けることになります。補助業務依頼の際は、別途パスワードを付与するなどの対応をとってください。
- ネットカフェの PC のような不特定の人が使用する機器上では、名古屋大学のアカウントは使用しないようにしてください。
- フィッシングによるパスワード窃取を避けるために、パスワード変更方法を常日頃から確認する、あるいはパスワード変更のウェブページをブックマークに保存しておくなどしてください。
- パスワードをメモとして残す場合は、鍵のかけられる場所に保管するようにしてください。
- 自分がログインしていないにもかかわらず多要素認証アプリが「承認」を求めてきた場合は、必ず「拒否」してください。また、第三者にパスワードが窃取されている疑いがあるので、速やかにパスワードを変更してください。

1.2.2 コンピュータウイルス

利用者がインターネットその他で情報を受信する場合、情報の提供者・発信者が良心的であるとは限りません。利用者には、コンピュータウイルスなど多くの危険の存在を意識し、怪しい情報にはアクセスしないなどの慎重な行動をとることが求められます。

コンピュータウイルスは、主に電子メールにより感染します。その感染方法は、年々巧妙になっています。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ず、必要であれば送信元に別途確認するなどといった自衛が必要です。

また、Web サイトの閲覧を通じたウイルス感染も起こり得ます。怪しいサイトへはアクセスしないなどの対策が必要です。

なお、ウイルス対策ソフトウェアの導入も、添付ファイルに紛れたウイルス検出、Web サイトアクセスを通じたウイルス感染の検出に一定の効果を示します。

意図的に、コンピュータウイルスを作成し、配布することは当然許されません。

注意事例

- 電子メールや Web 閲覧を媒介にする悪質なウイルスがあります。これらに感染すると、システムの破壊といったトラブルだけでなく、情報の漏洩に至る場合もあります。これらの

感染からの復旧には、多大の労力が必要です。

- コンピュータウイルスには亜種が多く、ウイルス対策ソフトウェアを導入していたとしても、検知できないことがあります。
- ウイルスパターンファイルの対応前に、ウイルスに感染する場合があります。
- 犯罪者がコンピュータを乗っ取るために Bot と呼ばれるコンピュータウイルスを広めています。こういったウイルスに感染しても、見かけ上は全く変わらないために、感染していることに気がつきません。これらの感染からの復旧には、多大の労力が必要です。
- 感染したウイルスによっては、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、感染したウイ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。
- 不適切な Web ページにアクセスすると、ユーザが知らない間にセキュリティ上危険なソフトウェアを実行させられたり、自動認証等に利用する情報(一般にクッキーと呼ばれます。)が漏れたりする可能性があります。
- 無償のソフトウェアには、個人の Web アクセス傾向を勝手に収集・分析するスパイウェアと呼ばれるソフトウェアがあります。このような機能を持ったソフトウェアを利用すると知らないうちに、利用者の趣味や嗜好が分析され、外部に漏えいします。
- 有用なソフトウェアを装って、盗聴や不正侵入のための裏口を仕掛ける「トロイの木馬」というプログラムがあります。
- 金融機関等からの電子メールと装って、オンラインバンキングのユーザ情報、クレジットカード番号、暗証番号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といった注意が必要です。ウイルスやワームの感染、秘密にしているはずの情報の漏えいといった危険があります。

1.2.3 著作権、知的財産権侵害

ソフトウェアなど多くのものが知的財産として法的に保護されています。 権利者の許可なく、他人が作成したものを P2P ソフトで交換したり、Web ページで公開・配布してはいけません。
ソフトウェアの不正取得（海賊版の購入など）やライセンス条項を無視した利用は、個人の責任に留まらず、大学全体の責任になります。
参考：公益社団法人 著作権情報センターホームページ http://www.cric.or.jp/

注意事例

- 私的使用目的であっても、違法配信であることを知りながら著作物（音楽・映像・漫画・書籍・論文・コンピュータプログラムなど）をダウンロードすると、刑罰（2 年以下の懲役、200 万円以下の罰金、あるいはその両方）や損害賠償の対象となる可能性があります。
- 違法ソフトウェアのダウンロード、使用は、著作権法 119 条 1 項　権利侵害罪に当たります。刑罰（懲役 10 年以下、1,000 万円以下の罰金、あるいはその両方）の対象となる可能

性があります。また、著作権者から侵害行為の差止請求、損害賠償請求がなされる可能性があります。

- ネットオークションなどにおいて、違法ソフトウェアが正規のソフトウェアと偽って販売されている場合があります。ソフトウェアの購入は、信用できる販売ルートで行ってください。
- 名古屋大学が管理する経費（外部資金を含む）でハードウェア、ソフトウェアを購入したときや、そのようなソフトウェアをインストールしたときには、その経費の責任者はハードウェア、ソフトウェア、インストールに関する情報をソフトウェア管理システム（SAM）に登録し、ソフトウェアを適切に管理する必要があります。
- 名古屋大学における P2P ソフトウェアの利用制限については、名古屋大学情報連携推進本部 Web ページにある P2P 型ファイル交換ソフトウェアの使用制限についてを適宜参考にしてください。

1.2.4 情報漏えい

本学構成員は、要機密情報を慎重に管理し、情報の漏えいを防ぐ必要があります。個人情報については、「東海国立大学機構個人情報保護規程」
（http://www.nagoya-u.ac.jp/extra/kisoku/act/frame/frame110000102.htm）を遵守してください。また、Web を介して情報を公開する場合にも十分な注意が必要です。

参考：パソコン等の盗難・紛失に伴う情報漏洩の防止対策
http://www.icts.nagoya-u.ac.jp/ja/security/pc-security.html

注意事例

- 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、重要な情報の漏えい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・漏えい対策をする機器（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、保護管理者の指示に従う必要がありますが（「東海国立大学機構個人情報保護規程」33 条）、原則として禁止されています。要機密情報を入れたノートパソコン・タブレット端末・スマートフォンを持ち歩く場合には、紛失や置忘れ等により情報が漏えいしないように細心の注意が必要です。
- 航空機や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ますが、情報の種類によっては問題になることも考えられます。
- スマートフォンなど高性能化する携帯電話の撮影機能などが情報漏えいの原因になる可能性もあるので細心の注意が必要です。
- 機密性 3 の情報を含む電子メールを送信することは非推奨です。
- 機密性 4 の情報を含む電子メールの送信は認められません。機密性 4 の情報を受信した場合は、速やかにメールサーバから削除してください。
- 機密性 2、3 の情報を含む電子メールを送信する場合には、名古屋大学、もしくは東海国立大学機構の電子メールサービスを利用し、東海国立大学機構情報格付け取扱手順にしたが

ってください。受信メールに要機密情報が含まれていた場合は、そのメールはメールサーバには残さないようにしてください。

- クラウドサービスを利用する場合には、その機密性によらずクラウドサービス利用ガイドラインに従って、クラウドサービスの内容を確認してください。

1.2.5 年次情報セキュリティ研修

名古屋大学では、構成員の情報セキュリティに対する意識の向上と情報セキュリティ対策が実体の伴うものとなることを期待して、構成員に対し年次情報セキュリティ研修を実施しています。構成員は年次情報セキュリティ研修を実施する必要があります。

1.3 利用の開始

1.3.1 情報機器・情報資源

本学の情報基盤としては、全学的に運営される NICE があります。コンピュータなどの情報機器は、図書館など全学的に運用されるものと、学部や研究室などが提供しているものがあります。情報資源には、図書館が提供している各種のデータベースのほか、各部局が Web を介して提供する各種情報、インターネット経由で学外に対して公開している情報などがあります。

NICE は名古屋大学キャンパスで利用されているネットワークです。大学内での情報アクセス、ならびに、インターネットアクセスには NICE が利用されます。詳しくは、情報連携推進本部の NICE の解説ページ（https://icts.nagoya-u.ac.jp/ja/services/nice/）を参照してください。

1.3.2 利用登録

本学の情報機器・情報資源を利用するためには、それらが全学のものであるか、部局のものであるかを問わず、利用登録が必要です。名古屋大学情報メディア教育システムのように学生は入学と同時に自動で利用登録されるものもあります。

本学は、構成員のために共同利用目的の情報機器・情報資源を提供しているため、利用者の不適正な行為について責任を問われる立場にあります。利用者には、このことを理解した上での適切な行動が期待されます。

本学の情報機器・情報資源の例としては、名古屋大学 NUWNET、情報メディア教育システム、学科単位での計算機システムがこれに該当します。

1.3.3 情報機器の NICE への接続

利用者が情報機器を NICE に接続しようとする場合には、原則として IP アドレス発行責任者あるいは IP アドレス発行の権限を委譲された者（以下、IP アドレスサブ管理者）へ接続許可申請することが必要です（IP アドレス発行責任者及び IP アドレスサブ管理者は「名古屋大学キャンパス情報ネットワーク接続機器 IP アドレス管理内規」に従って登録情報の追加・変更・削除を行う必要があります。）未登録のグローバル IP アドレスによる通信が発見された場合、その通信は遮断します。通信の再開には、部局長経由での始末書（割り当てられた IP アドレスを登録せずに使用した場合）あるいは

被害届（第三者により不正に使用された場合）の提出が必要となります。部局や研究室独自のネットワークへ接続する場合も、そのネットワーク管理者への接続許可申請することが必要です。名古屋大学NUWNETを通じて情報機器をNICEに接続する場合には､接続認証により接続許可申請がなされます。なお、持ち込みの情報機器に関しては、NICE に接続する時点でウイルスに感染していないことを確認してから接続してください。

1.4 情報機器の利用

1.4.1 適切な使用

本学の情報機器は、ほとんどのものが本学構成員の共用する設備です。そのため、多くの人が情報機器を快適に利用できるようにするため、利用者は、情報機器を良好な状態に保つための配慮と協力を心がけなくてはなりません。

注意事例

- 図書館等の共用端末を混雑する時間帯に個人で長時間独占使用することは、望ましくありません。
- 個人の Web ページを学外の広告付きの無料サイト上に作成し、学内の Web ページから直接たどれるようにすると、Web ページの広告が名古屋大学の公認であるかのような印象を与えます。このような紛らわしい行為は望ましくありません。

1.4.2 不正なアクセス

不正アクセス行為の禁止等に関する法律（以下「不正アクセス禁止法」という。）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認証情報などを不正に入手してコンピュータを利用すること、またはその未遂を禁止しており、違反者に刑事罰に科せられる場合もあります。

注意事例

- 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は、不正アクセス禁止法に違反します。

1.4.3 無権限のハードウェアの導入、改変、持ち出し、破壊

コンピュータ、プリンタ、ネットワーク機器などのハードウェアは、情報機器の重要な構成部分です。これらの情報機器を管理者に無断で導入、改変、あるいは、追加したり、持ち出すことはできません。意図的損傷や破壊が許されないのはもちろんです。

注意事例

- ネットワークケーブル等のケーブル類、コンピュータ機器等および電源等の設備を破壊す

る行為は、器物損壊であり、処分の対象になります。
- ネットワーク機器やコンピュータ類などの大学の情報機器を破壊したり持ち去ったりする行為は、大学の財産権を侵害するものであり、刑事処分・学内の懲戒処分の対象になります。
- 適切な理由もなく、マウスボールやキーボードの特定の文字のキートップを外して集めることは、機器の意図的損傷です。
- IP アドレスが発行されていないコンピュータ等の NICE への接続を禁止します。無許可接続はネットワークトラブルの原因になります。

1.4.4 無権限のソフトウェアの導入、改変

名古屋大学情報メディア教育システムのコンピュータなど共用の情報機器にインストールされている基本ソフトウェア（以下、「OS」という。）や応用ソフトウェア（アプリケーションソフト）をシステム管理者の許可なく改変することはできません。インストール権限のない情報機器にソフトウェアをインストールすることも認められません。

注意事例
- たとえば、情報メディアセンターの端末にゲーム等を無許可でインストールする、OS やアプリケーションソフトウェア等の一部でも許可なく書きかえることは、重大なルール違反です。

1.4.5 情報機器の持ち出し

学外へ本学管理の情報機器を持ち出す場合には、機器設置責任者の許可が必要です。持ち出す場合には、保存されている情報に注意し、要機密情報を保持している場合には、パスワードの設定、暗号化など十分な情報管理をしてください。

1.4.6 ハラスメント

共有プリンタに不快な画像を印刷出力する、壁紙（ディスプレイの背景の画像）に不快画像を使うなどの行為は、不適切な行為です。

1.5 情報の受信と生成

1.5.1 他人の作成した情報への配慮

利用者は、情報機器と情報資源をネットワーク化したコンピュータシステムを活用してレポートや Web ページなどさまざまな資料・情報を容易に作成することができます。情報の生成にあたっては、利用者は他人が作成した図・写真・文章・ロゴ・音源・プログラムなどの適切な利用に配慮し、著作権その他第三者の権利利益を尊重しなければなりません。

注意事例

- ソフトウェア等の海賊版の利用や不正コピーの利用は、著作権法違反です。
- 音楽 CD やソフトウェア媒体では、コピーの許容範囲が厳格に規定されています。不適切なコピーの作成や配布は許されません。
- 電子ジャーナル等では、「公正利用 (Fair Use)」という考えがあります。大量に内容を印刷するとか、多数のタイトルを一度にダウンロードするといった行為は、電子ジャーナル等の「公正利用の注意 (https://www.nul.nagoya-u.ac.jp/ej/ej_atten.html)」の範囲を超えます。

1.5.2 目的外利用

本学の情報機器は、もっぱら教育・研究の推進と職務・支援業務遂行のために提供されています。そのため、利用者には、公用と私用の区別を意識して、設置目的にそぐわない利用（目的外利用）をしないように注意しなければなりません。

目的外利用の典型としては、本学の情報機器を使って外部からデータ入力やプログラム開発業務を受注し、もっぱら利益を上げる商業目的で利用するというような場合です。しかし、目的外の利用の形態や態様はさまざまなので、この心得では、利用者を学生と教職員に分けて、目的外利用と考えられる事例についての注意情報を提供しています。

注意事例

- 私的なアルバイトのために掲示板等を利用することは、適切ではありません。
- 本学の情報機器を用いて、外部の計算機やデータの保守を、利益をあげる目的で行うことは原則として認められません。
- 研究目的でやむを得ない場合を除き、本学の情報機器や電子メールアドレス、ドメイン名等を利用しネットオークションをしてはいけません。なお、研究目的でやむを得ず利用する場合は、事前の許可が必要です。
- 自分の書物を宣伝・販売するために本学の情報機器を利用することは不適切です。ただし、著作リストの掲示や講義を受講する本学の学生へのテキスト販売に必要な情報の提示はこの限りではありません。

1.6 情報の管理

1.6.1 問題発生の予防

ネットワークの急速な普及で、さまざまな問題が発生するようになっています。ちょっとしたミスから紛争になったり、不要なダイレクトメールを送りつけられたり、予想外の金銭を請求されることがあります。以下の 1.6.2 と 1.6.3 に挙げるような適切な情報管理は、問題発生防止の有効な手段です。

1.6.2 個人情報

自分の個人情報は厳重に管理してください。わずかな謝礼目当てでアンケートに回答した結果、提供

した個人情報が勝手に利用されてトラブルに巻き込まれることもあります。

注意事例

- 適切な個人情報保護ポリシーが明示された企業以外の Web アンケートや懸賞に対して、安易に回答しないようにしてください。
- ソフトウェアの認証やユーザ登録については、認証又は登録をしないと利用ができない、ソフトウェアの更新ができない等の不利益を被る可能性があります。この場合には、入力必須の項目についてだけ記入することで対処して下さい。

1.6.3 他人のプライバシー

他人から提供される情報には、プライバシー情報が含まれていることが稀ではありません。たとえば、友人からの電子メールの内容についても、通常の封書同様、慎重な取り扱いをするなど、常識的な判断に基づいて行動することが必要です。

注意事例

- たとえ親しい人からの問い合わせであっても、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ことは避けるべきです。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。
- 他人に自分のプライバシーに関する情報を電子メールで提供する場合は、読んだ後に消去をお願いするなどの文言を入れるなど、慎重な行動をとることが求められます。

1.6.4 退職時における秘密情報の取り扱い

利用者が名古屋大学を退職する場合には、職務上知り得た秘密情報及びこれを含む情報機器等を持ち出してはいけません。

参考：

「国立大学法人法」第 18 条
(https://hourei.net/law/415AC0000000112)、
「東海国立大学機構職員就業規則」第 28 条第 1 項第 3 号
(https://education.joureikun.jp/thers_ac/act/frame/frame110010928.htm)、
「東海国立大学機構個人情報保護規程」第 10 条、第 33 条、第 42 条
(https://education.joureikun.jp/thers_ac/act/frame/frame110011384.htm)

1.6.5 情報の共有

情報を共有する際に、適切な手段を用いなければ情報漏洩に繋がる恐れがあります。以下では、情報共有の方法をいくつか例示します。

- 名古屋大学の教職員の間でファイルを共有する方法として、NUSS 教育研究ファイルサービスシステム（機密性 1～3）や NSSS セキュア教育研究ファイルサービスシステム（機密性 1～4）によるファイルの共有があります。

- NSSS において機密性 4 の情報を扱う場合は、名古屋大学情報連携推進本部セキュア教育研究ファイルサービス利用内規に従ってデータを暗号化する必要があります。
- NUSS や NSSS を用いて教職員間でファイルを共有する方法として、名大 ID を用いたファイル共有の機能があります。
- 学外の人からファイルを受け取る方法として、NUSS のアップロード専用フォルダがあります。
- NUSS には、URL でフォルダを共有する機能があります。URL 共有の機能は、教職員間でファイルを共有する方法としては非推奨です。（名大 ID によるファイル共有を利用してください。）URL 共有の機能を利用する際、公開を意図していないフォルダについては必ずパスワードを設定してください。

1.7 情報発信

1.7.1 情報発信者の責任

情報発信には、大きな社会的メリットがありますが、その一方で様々なリスクが伴います。利用者には、情報発信の意義とリスクについて十分な認識が求められます。

1.7.2 チェーンメール・メッセージ

チェーンメール・メッセージ（メールや SNS で他の人に拡散するように呼び掛けるメッセージ）を発信したり、転送したりしてはいけません。チェーンメール・メッセージは、情報システムへ負担をかけます。また、デマの拡散に繋がる危険性があります。善意からのメッセージであっても、社会的に悪影響を及ぼす可能性があることに留意する必要があります。

1.7.3 プライバシー侵害・情報漏えい

Web ページは、原理的には世界中の人が閲覧することのできるものです。そのため、他人のプライバシーに関する情報や個人情報を Web ページなどに掲載する場合には、適切な判断が求められます。SNS や電子メールによる情報発信についても同様の配慮が必要です。

注意事例

- 職員名簿や学生名簿等を発行者に無断で部外者に配布する行為は、不適切です。
- アクセスが制限された Web ページにある他人の個人情報を本人の同意を得ずに引用し、又は公開することはできません。
- 職務上知り得た秘密を SNS 等に掲載する行為は、不適切です。
- メーリングリスト（ML）の返信先は、多くの場合、ML 自体になっています。ML への投稿者に返信する場合は注意が必要です。
- メール送信時に To と Cc に記載したメールアドレスは、そのメールの受信者全員に知られるため注意が必要です。
- 情報発信の方法を適切に選択することで、情報の誤発信を防ぐことができます。例えば、

TACT により講義の連絡事項をアナウンスすれば、講義の受講者のみに簡単にアナウンスできます。

また、ウェブサービスの性質によっては、意図せざる情報漏洩が発生する危険性があります。

注意事例

- NUSS で機密性 2、3 の情報を URL 共有するときには、パスワード保護を実施してください。
- 様々なサービスを提供する Web サイトがありますが、その中にはアップロードしたファイル、入力した情報などをサービス提供者が保存したり、サービス提供者が第三者に提供するものがあります。そのため、Web サイトに不用意に機密性が高い情報をアップロードしたり、入力したりすると情報漏洩に繋がる恐れがあります。Web サイト上で機密性の高い情報を扱う場合は、その Web サイトの性質を把握し、問題がないことを確認した上で利用してください。

1.7.4 著作権・肖像権・パブリシティ権

情報発信する際は、著作権、肖像権、パブリシティ権等を侵害しないように注意してください。

1.7.5 誹謗中傷

SNS などを用いて他人を誹謗中傷してはいけません。

注意事例

- SNS などでは、言葉の行き違いから感情的な論争になりがちです。また、匿名の SNS や参加者が限定された SNS であっても誹謗中傷を行ってはいけません。
- 自分とは異なる立場を表明する他人の Web ページに対して意見を述べたり、コメントしたりする場合には、節度を持った誠実な行動が必要です。

1.7.6 目的外利用

物や情報の販売を目的として、大学の情報機器を用いて情報発信することは、原則として認められません。

注意事例

- 本学の情報機器や情報資源を物品や情報の販売に利用することは認められません。
- 商品やサービスを販売する目的で、本学の情報機器を使って広告等を掲示・発信することは認められません。
- 本学の情報機器や情報資源を使って、商取引の仲介をすることは認められません。
- もっぱら政治活動や宗教活動に本学の情報機器を利用することは認められません。

1.7.7 ソーシャルメディアサービスによる情報発信

ソーシャルメディアサービスを活用して情報発信する場合には、以下の事項に注意してください。

1. 本学からの情報発信であることを閲覧者に明らかにするために、本学のドメイン名（nagoya-u.ac.jp で終わるドメイン名）を用いて管理しているウェブサイトにおいて、ソーシャルメディアサービスのアカウント名、あるいはアカウントページの URL を明記してください。
2. ソーシャルメディアの提供事業者が認証アカウントを発行している場合には、可能な限りこれを取得するようにしてください。
3. ソーシャルメディアサービスの認証情報についても、本学の認証情報と同様に適切に管理してください。（「1.2.1 認証情報の管理」に準じてください。）

1.7.8 外部委託・クラウドサービス等を利用した学外向けウェブサイト

学外向けに提供するウェブサイトの作成を外部委託する場合や、クラウドサービスを利用して構築する場合には、本学のドメイン名（nagoya-u.ac.jp で終わるドメイン名）を使用するようにしてください。本学のドメイン名を使用することにより、本学が提供した情報であることをウェブサイトの閲覧者が確認できます。

注意事例

- 外部の独自ドメイン名を使用してウェブサイトを構築すると、閲覧者からは本学からの情報発信か、なりすましによるものかの判断が難しくなります。
- 外部の独自ドメイン名を使用した場合、その利用権を放棄した際に別の用途（風俗的、反社会的な用途もあり得る）に転用される可能性があります。
- クラウドサービスを使用したウェブサイトに本学のドメイン名を使用する場合は、「名古屋大学クラウドサービス利用ガイドライン チェックリスト」を情報連携推進本部に提出することが必要です。

1.7.9 その他

その他、公序良俗に反する情報を発信してはいけません。

注意事例

- 自殺の方法や爆弾の製造方法に関する情報の表示と配布をしてはいけません。
- 猥褻図画を特定の相手に繰り返し送付することは、ハラスメント行為に該当すると考えます。(参考：ハラスメント相談センター)
- 拒否されているにもかかわらず、何度もメールや SNS メッセージを送る行為は不適切です。

1.8 ウェブ会議システム

遠隔講義やオンライン会議などでウェブ会議システムを使用するとき、第三者によって遠隔講義やオンライン会議を妨害されないようにセキュリティに注意を払う必要があります。

1.8.1 会議の参加者による対策

1. ウェブ会議システムのクライアントソフトウェアも通常のソフトウェアと同様に随時アップデートが提供されています。ソフトウェアを最新の状態に更新して会議に参加するようにしてください。
2. 第三者による会議への参加を防ぐために､会議のURLを他人に教えないようにしてください。

1.8.2 会議の開催者（講師）による対策

第三者が、会議や講義に無断で参加し、不適切な画像や音声の共有によって会議や講義を妨害する行為を防ぐために、ウェブ会議システムを適切に設定して使用してください。

1. 会議にパスワードを設定できる場合は、必ずパスワードを設定してください。
2. 会議のURLは、会議の参加者や講義の受講者以外には公開しないようにしてください。
3. 画面共有の機能などを参加者ごとに制限できる場合は、必要最小限の機能を参加者に割り当てるように設定してください。

1.9 テレワーク

テレワークにおいては、本学の情報機器を学外に持ち出したり、個人所有の情報機器を使用したりするため､学内における情報セキュリティ対策とは異なる対策が必要となります。また､テレワークを実施する環境についても注意する必要があります。

1.9.1 本学の情報機器を用いたテレワーク

本学の情報機器を用いてテレワークを実施する場合は、以下の対策を実施してください。

1. 本学から情報機器を持ち出す前に、情報機器のソフトウェアやウイルス対策ソフトを最新の状態に更新してください。
2. 情報機器に情報（文書等）を保存する場合は、その情報が学外の情報機器に保存可能なものかを確認し、暗号化をして保存してください。
3. 業務外の用途（例えば、業務と関係ないウェブサイトの閲覧）に本学の情報機器を使用することは認められません。
4. テレワークが長期にわたる場合は、情報機器が最新の状態に更新されているかを定期的に確認し、最新の状態を維持するようにしてください。
5. テレワークに使用した情報機器を本学に返却しNICEに接続するときは､最新の状態に更新し、ウイルス対策ソフトによるフルスキャンを実施してください。また無許可のソフトウェアがインストールされていないかを確認してください。

1.9.2 個人所有の情報機器を用いたテレワーク

1. 個人所有の情報機器を用いたテレワークでは、原則としてその情報機器に本学所有の情報を保存することは認められません。ただし、公開を前提とした情報など、情報の責任者が本学所有でない情報機器での保存を認めている場合は保存してもかまいません。
2. テレワークを開始する前に、情報機器を最新の状態に更新し、ウイルス対策ソフトによるフル

スキャンを実施してください。

3. 本学所有の情報を、個人所有の情報機器に誤って保存していないかを定期的に確認してください。
4. テレワークを終了する場合は、情報機器に対してウイルス対策ソフトによるフルスキャンを実施してください。マルウェアが検出された場合は、検出結果を保存し、「第 2 章危機管理ガイドライン」に従って、情報セキュリティインシデントとして報告してください。

1.9.3 テレワークの環境について

1. テレワークは周りに人がいない環境で実施してください。画面の盗み見や、テレビ会議時の音声による情報漏洩が起こらないように気を付ける必要があります。
2. テレワークに使用する情報機器をインターネットに接続する場合は、自宅のネットワークなどの信頼できるネットワークを使用してください。カフェなどに設置された公衆無線 LAN の使用は避けてください。
3. 離席するときは、画面をロックして第三者に操作されないようにしてください。

1.10 危機管理

情報機器に何らかの重大な問題が発生した場合には、利用者は応急措置、対応措置を順にとることになります。ここで、応急措置とは問題に対する対処的な措置、対応措置とは問題に対する根本的な解決をとることを意味します。なお、危機発生時の対応については、第 2 章も参考にしてください。

1.10.1 応急措置

利用者は、自分の利用する情報機器にウイルス感染など重大な問題を発見した場合には、ただちにその機器のネットワーク接続ケーブルを外す、無線 LAN をオフにするなどの措置を求められます。

1.10.2 対応処置

システム管理者あるいは情報連携推進本部（https://www.icts.nagoya-u.ac.jp）の指示に従い、利用者は、応急処置が行われた情報機器に対して対応処置を行います。

1.10.3 状況報告

利用者は、本学または自分の利用する情報機器・情報資源について不正アクセスやウイルス感染などの情報セキュリティインシデント（以下、「インシデント」と略称）が発生したことを発見した場合には、すみやかに情報連携推進本部に状況報告をしてください。また、可能な限り、当該情報機器の管理者への報告もあわせて行ってください。

情報セキュリティインシデント発生時の連絡先

TEL 052-789-4393(内線 4393)

E-mail: security@icts.nagoya-u.ac.jp

Web: https://qa.icts.nagoya-u.ac.jp/

1.11 相談窓口

本学の情報機器・情報資源の利用について、相談窓口を設けています。まず、情報連携推進本部の Web ページや質疑応答集の情報を確認して下さい。適切な情報が見つからない場合に、相談窓口にお尋ね下さい。

総合窓口：IT ヘルプデスク（TEL　052-747-6389（内線 6389））

第 2 章 危機管理ガイドライン

2.1 概要

本危機管理ガイドラインは、本学が教育研究利用目的で提供する NICE、コンピュータなどの情報機器、データベースなどの情報資源の利用について、インシデントが発生した場合に、状況を一元的に把握して適切な措置を講じるための関係者の対処方法について具体的な情報を提供しようとするものです。

2.2 情報セキュリティホットラインの設置

情報連携推進本部は、インシデントの発生を複数の方法（電話・ファックス・電子メール・Web など）で情報連携推進本部情報セキュリティ室（以下、情報セキュリティ室と略称）に報告するための体制（情報セキュリティホットライン、IT ヘルプデスク）を整備し、Web、パンフレット、掲示を介してその存在をさまざまな場所に掲示することで周知を図ります。

2.3 インシデントの報告

インシデントを発見、インシデントとなる可能性を発見した第１発見者は、情報セキュリティホットラインを通じて、速やかに情報セキュリティ室に状況を報告してください。また、可能な限り、当該情報機器の管理者へも報告してください。

2.4 インシデントへの対応

2.4.1 初期対応

情報セキュリティ室は、初期対応として、情報機器の管理者への連絡、情報機器のネットワークからの切断といった対応を実施します。この対応は、通常時は、３時間以内、休日等は、8 時間以内に行うことを目標とします。

2.4.2 情報セキュリティ室による緊急措置

情報セキュリティ室は、インシデントの報告を受けた場合、当該情報機器の管理者と協力して問題処理を行うが、被害拡大防止のために緊急の必要がある場合には、当該情報機器の管理者の了解がなくても、情報機器の設置場所に立ち入り、特定のサービスの停止、特定の情報機器から外部へのアクセスの遮断、特定の情報機器から内部へのアクセスの遮断などを行います。

2.4.3 情報設備機器の管理者への通知

情報セキュリティ室は、インシデントの連絡が当該情報機器の管理者になされていない場合には、ただちにインシデントの通知を行います。

重大なインシデント（不正アクセス、不正コマンド実行、情報改竄、情報窃取など、そのおそれがある場合も含む）の場合は、情報機器を保有する部局の長にもインシデントの通知を行います。

情報セキュリティ室が当該情報機器の管理者の了解なしに緊急措置をとった場合には、当該情報機器の管理者に状況と緊急措置の内容について事後的に説明を行います。

2.4.4　情報機器の管理者による対応

情報機器の管理者は、必要な措置を講じた後、インシデントの状況、および対応について情報連携推進本部に報告を行います。重大なインシデントの場合、管理者は部局の情報セキュリティ単位組織、および部局長にも状況・対応を報告します。

注意事例

- 重大なインシデントが発生した場合は、情報連携推進本部の助言に従って、情報機器の証拠保全を実施してください。マルウェア感染が疑われる情報機器を証拠保全する場合は、情報機器に対して何も操作を行わず、まず、ネットワークから切り離してください。ネットワークから切り離した後の作業については、情報連携推進本部の助言に従うようにしてください。
- 証拠保全したハードディスクには、アクセスしないようにしてください。アクセスする場合は、書き込み防止の措置（リードオンリーでマウント、書き込み防止機能を持った機器の使用）をする必要がありますので、IT ヘルプデスク（e-mail: it-helpdesk@icts.nagoya-u.ac.jp、Tel: 052-747-6389）に相談してください。証拠保全したハードディスクは、部局長の監督下で保管してください。

2.5　情報連携推進本部への報告

情報セキュリティ室は、インシデントの状況に応じた措置を行いますが、そのうち重大なインシデントについては情報連携推進本部に適宜対応状況の報告を行います。

2.6　学外への連絡

情報連携推進本部は、大学が必要だと判断した場合、文部科学省等の学外組織にインシデントの状況、および対応状況について連絡を行います。

2.7　インシデント情報の有効活用

情報連携推進本部は、インシデント情報のデータベースを作成し、情報推進部、情報セキュリティ単位組織などで有効活用して、情報セキュリティの向上に役立てる作業を行います。

2.8　部局における連絡体制の整備

各部局は、インシデント発生時における連絡体制を整備することが必要です。

2.9　個人情報の漏えいが疑われる場合の対応

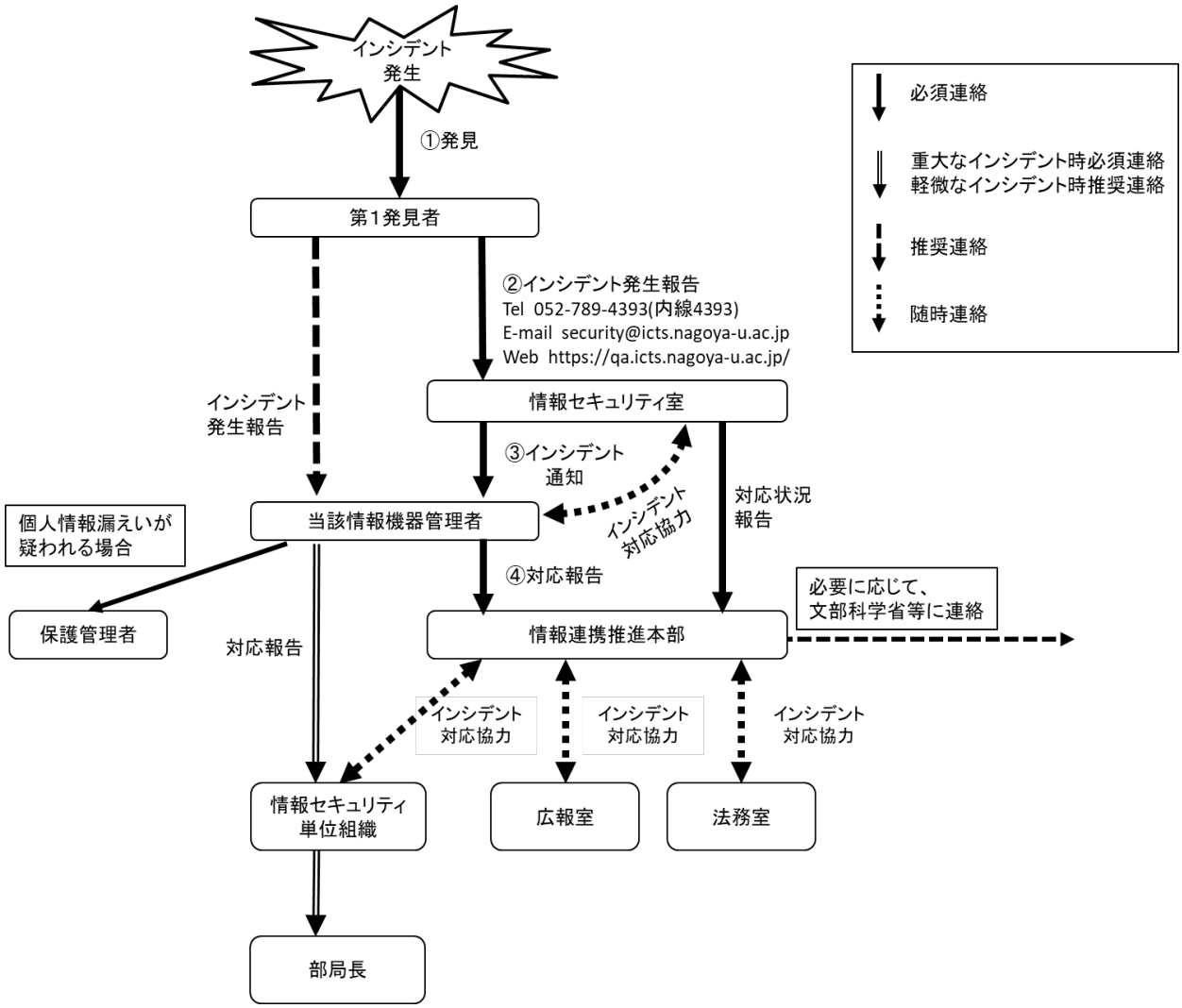
個人情報の漏えいが疑われる場合は、東海国立大学機構個人情報保護規程に従って、保護管理者に報告してください。

2.10　情報セキュリティホットラインの定期点検

情報セキュリティ室と情報セキュリティ単位組織の管理者は、情報セキュリティホットラインが問題なく動作することの確認を月 1 回以上確認します。

2.11　危機管理に関する周知ならびに啓発活動

情報セキュリティ研修を通じて、インシデントが発生した場合における対処法と対処の重要性などを利用者や管理者に周知するとともに、対処法が正しく理解されているかどうかを確認します。


インシデント
発生
①発見
第1発見者
②インシデント発生報告
Tel 052-789-4393(内線4393)
E-mail security@icts.nagoya-u.ac.jp
Web https://qa.icts.nagoya-u.ac.jp/
情報セキュリティ室
インシデント
発生報告
③インシデント
通知
インシデント
対応協力
対応状況
報告
当該情報機器管理者
個人情報漏えいが
疑われる場合
④対応報告
保護管理者
対応報告
情報連携推進本部
必要に応じて、
文部科学省等に連絡
インシデント
対応協力
インシデント
対応協力
インシデント
対応協力
情報セキュリティ
単位組織
広報室
法務室
部局長
必須連絡
重大なインシデント時必須連絡
軽微なインシデント時推奨連絡
推奨連絡
随時連絡

第 3 章　セキュリティ技術ガイドライン（管理者心得）

3.1 概要

このセキュリティ技術ガイドライン（管理者心得）は、情報機器を NICE に接続あるいは接続しようとするすべての本学構成員を対象として、情報機器・情報資源のセキュリティを守るために必要な管理の指針を述べています。ここで注意すべきことは、パソコンやスマートフォン・タブレット端末など特定の個人専用となる情報機器の場合でも（個人が大学に持ち込むパソコンも含む)、NICE に接続していれば、個々の利用者自身が管理者になるということです。

大学内には、NICE 以外のネットワークも敷設されているため、情報機器を接続する際には、接続先のネットワークを確認しなければなりません。NICE 以外のネットワークと NICE を接続すると、通信障害が発生し、ネットワーク全体が利用できなくなります。

本セキュリティ技術ガイドラインに沿った適切な管理がなされないために被害や障害が発生し、情報機器が利用できなくなり、教育研究や業務などの活動に影響が出るおそれがあります。不適切な管理のために本学の情報機器がネットワーク攻撃の踏み台にされ、外部のネットワークに被害を与えるような場合には、本学のネットワーク全体がインターネットから排除されることもあり得ます。このように、ネットワークに接続されている情報機器の管理は、単に本学構成員個人の問題であるだけでなく、本学全体の問題であることを認識してください。

3.2 管理対象となる情報機器

本セキュリティ技術ガイドラインでは、対象とする情報機器を次の５つのカテゴリに分け、それぞれセキュリティを守るための情報機器管理の方法について説明します。

1. ネットワーク設備機器
   ルータ、HUB、NAT、無線 LAN 用設備機器、リモートアクセスサーバ、 DNS サーバ、DHCP サーバ、VPN サーバ
2. サーバ
   Web サーバ、メールサーバ、ネームサーバ、ファイルサーバ、計算サーバ、 データベースサーバ
3. 個人向けコンピュータ
   パーソナルコンピュータ（以下、パソコンと略称)、クライアント WS、タブレット端末、スマートフォン
4. 特殊機器
   制御機器、医療機器など
5. その他
   プリンタ、スキャナ、複合機、テレビ会議システム、NAS（ネットワーク接続ストレージ)、計測設備機器など

3.3 情報機器管理の基本的な考え方

3.3.1 機器設置責任者および運用管理責任者の選任

名古屋大学情報セキュリティポリシーと情報連携推進本部の定めにより、情報セキュリティ単位組織（以下、単位組織と略称）は、NICE に接続するすべての情報機器について、機器設置責任者および運用管理責任者（以下、「管理者」と 略称）を選任してください。

1）機器設置責任者

機器設置責任者は、情報機器の NICE への接続に関する最終的な責任を負う人です。機器設置責任者は、その責任を果たすために運用管理責任者を任命することができます。

パソコンなどもっぱら特定の個人専用となる情報機器の場合は、利用者自身が機器設置責任者及び運用管理責任者となります。

2）運用管理責任者

運用管理責任者は、情報機器の設定や日常的な運用管理を行い、情報機器が適正に機能するよう管理する責任を負います。

運用管理責任者は、本人の備忘録として、また、運用管理責任者の交替に備え、情報機器の設定変更、セキュリティパッチ適用などの運用管理作業記録を作成・保存する義務を負います。

運用管理責任者は、自分が運用管理する情報機器が原因でネットワーク障害が発生した場合には、速やかに調査し対処することが求められます。対処が困難な場合には、運用管理責任者には、機器設置責任者の了解を得て、速やかに当該情報機器をネットワークから切り離す等の応急処置が求められます。

注意事例

- 教職員の異動や学生の卒業による運用管理責任者の交替において、引継ぎ等がうまく行われず、運用管理がなされないまま使用されている情報機器があります。運用管理責任者が運用管理責任を果たせない場合、機器設置責任者と相談の上、NICE 全体の安定運用のために管理できない情報機器を NICE から撤去してください。

3.3.2 情報機器の設置と管理の基本的な考え方

管理者は情報機器管理のために以下の２項目について適切な措置をとる義務があります。

1）物理セキュリティ：情報機器の設置場所、情報機器への物理アクセス

2）ネットワークセキュリティ：情報機器へのネットワークアクセス

サーバについては、上記２項目に加えてさらに次の２項目のセキュリティについて適切な措置をとる義務があります。

1）アカウントセキュリティ：利用者管理

2）ファイルシステムセキュリティ：データの保全

ここでは物理セキュリティとネットワークセキュリティの基本的な考え方について述べ、サーバ固有の事項は 3.5 サーバで述べます。

1）物理セキュリティの基準

情報機器を設置する場所としては、盗難、破壊などの被害を受けにくい安全な設置環境を選んでく

ださい。特に基幹ネットワークの情報機器やサーバ類など重要な情報機器については、立ち入りが制限できる環境に設置し、無停電電源装置をつけることにより瞬間的な停電の影響を受けないようにする、といった管理が要求されます。

個人利用のパソコンについては、盗難被害がしばしば報告されています。ノートパソコンを安易に放置しない、研究室でも夜間は施錠する、など常識的な管理が必要です。

共用スペースに設置される情報機器の管理については、外部の者による盗難や破壊に加えて、利用者が行う盗難や破壊に備えた予防策を講じてください。

2) ネットワークセキュリティの基準

NICE は全世界と繋がったネットワークであり、NICE に接続された情報機器は、世界中からアクセスできる情報機器になります。したがって、インターネットサーバとして機能する情報機器では、不必要なサービスが起動しないように設定するとともに、インターネットからのアクセスが可能なアドレスを限定するなどのアクセス制御を設定してください。

3.4 ネットワーク設備機器

管理者が管理すべきネットワーク設備機器には、NICE で設置したルータや HUB に加えて、部局や研究室で独自に設置しているルータ、HUB、NAT、無線 LAN 装置、リモートアクセスサーバ、DNS サーバ、DHCP サーバ、VPN サーバなどがあります。

3.4.1 設置の基準

ネットワーク設備機器の設置に関しては以下の点に注意してください。

(1) 関係者以外の立ち入りを制限できる環境に設置する（特に基幹ネットワーク設備機器)。
(2) 無停電電源装置を設置する（特に基幹ネットワーク設備機器)。
(3) 専用のノード室に設置することが望ましい。
(4) 不特定利用者が自由に利用できるような情報コンセントは設置しない。
(5) 高性能なネットワーク設備機器は、コンピュータと同様に故障防止のために空調設備がある部屋に設置することが望ましい。
(6) ネットワーク設備機器は、小型化するにつれて冷却ファンの騒音が無視できなくなるので、できればネットワーク設備機器専用のノード室を設けることが望ましい。
(7) 施錠されていない教室など不特定利用者が自由に出入りできる場所に情報コンセントを設置する場合には、無許可利用を防止するために、情報コンセントに蓋をつけて施錠するなどの対策をとることが望ましい。

3.4.2 管理者の義務

ネットワーク設備機器の運用に当たっては、ネットワーク設定を誤ると影響が大きいので十分注意してください。特にプライベートアドレスで運営している私設 LAN を NAT などで NICE に接続する場合には、プライベートアドレスのパケットが NICE に流出しないようにしてください。

基本的なネットワーク設定の他にも以下の点に注意が必要です。

(1) 設備機器設定用のパスワードを変更する。

(2) SNMP の設定を変更する。
(3) MAC アドレスによるアクセス制限を設ける (DHCP)。
(4) 暗号化通信を利用する。
(5) 利用者認証を設ける (リモートアクセス)。

設備機器設定のためのパスワードを初期設定のままにしておくと、その設備機器について詳しい人、あるいは、Web 上に公開されているマニュアルに記載された初期パスワードなどにより勝手に設定を変更されてしまう危険があります。

SNMP の設定を初期設定のままにしておくと、ネットワーク情報を読み取られたり、ネットワーク設定を変更されてしまったりする危険があります。

無線 LAN 環境や DHCP サーバを設置する場合には、利用を許可されていない人が利用できないようにするために情報連携推進本部が示す無線 LAN セキュリティ基準(https://icts.nagoya-u.ac.jp/nu-only/ja/security/wireless-lan.html) に記された方法に従ってください。各部局は、無線アクセスポイントに関わるインシデント発生時に緊急に対応する最小組織単位を定める必要があります。最小組織単位は、講座や研究グループとし、各最小組織単位には、無線アクセスポイントの停止などの操作を実施できる責任者が必要です。ファイアウォールを設けてサブネット内の他の利用者と隔離した環境で利用するとより安全です。また、NICE に直接的、あるいは、間接的に接続されている無線 LAN アクセスポイントは、他の機器と同様に名古屋大学 IP アドレスデータベースに登録してください。

リモートアクセスサーバを設置する場合には、必ず認証機構を設け、特定の利用者だけが利用できるようにして運用してください。リモートアクセスサーバ経由で接続できる範囲も研究室内に限定するなど、必要最低限にすることが望まれます。

無線 LAN や DHCP サーバなどの設置については、各単位部局 (サブネット) で設置に関する方針を定め、サブネット内で競合しないように運用する必要があります。設備機器の設置にあたっては、単位部局の運用方針に基づいた 「無線 LAN 装置設定チェックリスト」などを用意し、それにしたがって設定されていることを確認する手続きをとってください。設定を業者に依頼する場合にも、チェックリストのとおり設定されていることを記録しておく必要があります。

学外からのアクセスを必要とする機器については、「IP アドレス管理システム・ポート公開申請システム操作マニュアル」に従って、ポート公開を申請してください。学外からの通信、および学外への通信を必要としない IP アドレスについては、遮断申請をすることにより、外から内、内から外の両方向の通信を遮断することができます。

ポート公開した機器は不正アクセスされるリスクが高いため、情報セキュリティ室が定期的にセキュリティ管理状況を確認します。ポート公開した場合は、「IP アドレス管理システム」において「セキュリティ管理状況」が入力できるようになりますので、必ず入力してください。「セキュリティ管理状況」が未入力の場合は、当該機器の通信を遮断します。

3.4.3 保守

NICE で設置したネットワーク設備機器については、常に状態をチェックし、ネットワーク設備機器が故障しないように予備的な保守が行われています。ネットワーク設備機器の故障は影響が大きいので、部局や研究室で用意したネットワーク設備機器についても予備のネットワーク設備機器を用意し

ておくなど同様の対策をとっておくべきでしょう。

3.4.4 稼働記録の管理

稼働記録（ログ）は最低1年保存してください。

3.5 サーバ

サーバとは、複数の利用者がネットワークを介して利用する情報機器であり、Web サーバ、メールサーバ、ファイルサーバ、データベースサーバなどがあります。管理者は、サーバについて、その管理に加えて利用者管理をする義務があります。

3.5.1 設置の基準

サーバは、できるだけ立ち入りが制限できる環境に設置してください。また、無停電電源装置を設置して瞬間的な停電に対処できるようにしておくことも有効です。

3.5.2 管理者の義務

管理者は、以下の事項を守ってサーバを運用してください。

(1) 最新のセキュリティパッチを当てておく。
(2) 不必要なインターネットサービスは起動しない。
(3) アクセス制御を設定する。
(4) 定期的にデータのバックアップをとる。
(5) データの正当性をチェックする。(特に Web サーバ)
(6) 情報漏えい防止に留意する。
(7) 利用者のプライバシー保護に留意する。

1) 最新のセキュリティパッチ

どのようなサーバであっても、OS 自身やインターネットサービスの機能を実現するソフトウェアにバグやセキュリティホール（不正な侵入に利用されるシステムの不備）が発見されると、OS のパッチが提供されたり、ソフトウェアのバージョンアップが行われたりしています。定期的に（たとえば、1ヶ月に1回）OS のパッチ情報をチェックし、最新のセキュリティパッチが当ててあるようにしてください。特に、重要なセキュリティ情報を入手した場合には、後回しにせず、速やかに対処してください。また、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をオンとするのも有効な方法です。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。

2) 不必要なインターネットサービスの終了

不必要なインターネットサービスが正しく設定されないまま起動していると、セキュリティホールになってしまいます。サーバを設定する場合には、必要なインターネットサービスだけが起動されるように設定してください。

3) アクセス制御

複数の利用者で共同利用するサーバにおいても、計算サーバやファイルサーバのように、ある程度サービスを提供する範囲が限定できる場合にはアクセス制限してください。UNIX の場合は tcp_wrapper などのツールが有用です。

また、Web サーバを介して情報を公開する場合には、情報の重要度に応じて適切なアクセス制御を設定することが必要です。

4) 定期的バックアップ

ディスクの故障に備えるためにも、サーバのデータは定期的にバックアップをとってください。

5) データの正当性チェック

サーバに格納される情報は、改竄等がないようにデータの正当性を常にチェックすることが求められます。Web サーバにおいては、単にデータを保存するだけでなく、tripwire などのツールを利用してデータが改竄されていないか常に注意しておく必要があります。また、動的な Web ページの場合には、クロスサイトスクリプティングを防止するように、入力されるデータの正当性をチェックすることが望まれます。

6) 情報漏えい防止

サーバに格納される情報が不必要に流出することのないよう、適切な措置をとることが望まれます。サーバプログラムの適切なアップデート、適切な設定、ユーザ認証等において細心の注意が求められます。

7) 利用者のプライバシー保護

サーバの管理者は、利用者が行った行為でネットワークに被害が出た場合には、管理者の権限で速やかに対処しなければなりませんが、その際、利用者のプライバシーを侵害しないようにする必要があります。例えば、権限のないファイルにアクセスしない、電子メールなどの個人情報に関わるデータを解析する必要が発生した場合は問題解明に必要な情報に解析を限定する、などの対応が求められます。

8) アクセス制限

サーバを安全に運用するためには、サーバへのアクセス制限が有効です。アクセス可能な IP アドレスを制限する、不正アクセスの検知・ブロックを行う Fail2ban 等のツールを導入する、ポート番号を変更するなどの措置が有効です。

9) 脆弱性検査

定期的に脆弱性検査ツールを用いて、サーバの脆弱性の検査を実施するなどの措置が必要です。

10) ウェブサーバの管理

ウェブアプリケーションを使用している場合は、そのアップデートを定期的に実施してください。またウェブアプリケーションを独自に開発する場合は、脆弱性を作りこまないように注意が必要です。業者にウェブアプリケーションの開発を委託する場合は、典型的な脆弱性（SQL インジェクション、コマンドインジェクションなど）についてはその対策を契約に含めるようにしてください。

3.5.3 利用者認証機能

管理者は、サーバやサーバ上の情報へのアクセスにおいて、利用者を特定し、それが正当な利用者であることを検証する必要がある場合、利用者の識別、及び利用者認証を行う機能を設ける必要があ

ります。

管理者は、利用者認証機能を設けるにあたり、利用者がアクセスできる情報の格付けに応じて、十分な強度をもった認証方式を用いる必要があります。

注意事例

- 利用者が要保護情報にアクセスできる場合は、多要素認証による利用者認証機能を提供してください。

3.5.4 保守

サーバに障害が発生すると、多くの利用者に影響が出るため、速やかに回復させる必要があります。したがって、重要なサーバについては二重化しておくことが望まれます。

3.5.5 利用者の管理

利用者の管理には、ID (利用登録)の管理と利用者管理・教育が含まれます。

1) 不必要な ID の速やかな抹消

ID の管理においては、卒業生など不要な ID は速やかに登録抹消することが重要です。

2) 一時的な ID の管理

サーバのセットアップ、仮想マシンを利用して多くのサーバをセットアップする、業者が設定を行う場合、など、一時的に必要となる ID の管理は、以下の点に注意してください。

(1) 一時的な ID は必要な時にのみ利用できるようにしてください。一時的な ID は、用件が完了次第、速やかに抹消してください。

(2) guest などの明らかにそれとわかるユーザ名は使用しないでください。

3) 利用者教育

管理者がサーバの管理をきちんと行っていても、利用者の行為でセキュリティが危うくなる場合があります。管理者は、利用者管理・教育をサーバ管理の一部として認識するべきでしょう。特に、以下の行為はサーバのセキュリティレベルを下げることになりますので慎むよう、利用者に徹底させる必要があります。

(1) 容易に見破られるパスワードを付けない。

(2) パスワードを書き留めない。

(3) ユーザ名とパスワードを他人に教えない。

(4) 自分が利用できる環境を家族や友人に使わせない。

(5) 可能な範囲で、crack、 John the Ripper などのパスワードチェックツールを利用して定期的に利用者のパスワードが適正であることを確認してください。

3.5.6 稼働記録の管理

一旦サーバのセキュリティが破られると、管理者は状況を把握し、原因を調査する必要があります。そのためには、稼働記録が必要になります。

(1) システムログ、メール配送記録、Web へのアクセスログなどの稼働状況は必ず記録するよ

うに設定してください。

(2) 稼働記録は、最低 1 年保存してください。

(3) ログに異常がないか日常的にチェックすることが望ましいです。

(4) 初期設定では、システムログの保存期間が短期間となっている場合があります。サーバ構築時に保存期間を確認してください。

(5) システムの構成変更、利用者追加・変更、バックアップ、パッチ適用等の運用に関する作業記録を残すようにしてください。

3.5.7 Web サーバの管理

Web サーバの情報の漏えいやコンテンツの改ざんを防ぐために、以下の対策を実施してください。

1) アップデートの実施

Web サーバに脆弱性が混入しないようにするために、以下のものについて、継続的にメンテナンスされていて、かつ情報漏洩・改竄に繋がる脆弱性の存在が確認されていないバージョンを使用するようにしてください。

(1) Web サーバプログラム（apache など）

(2) Web アプリケーション（WordPress, Joomla など，プラグインも含む）

(3) Web アプリケーションが利用するデータベース（MySQL, PostgreSQL など）

(4) Web アプリケーションが利用するプログラム（PHP, Perl など）

注意事例

- Web アプリケーションのプラグインの中には、継続的にメンテナンスされていないものがあります。そのため、使用しているプラグインの情報を定期的に確認し、メンテナンスがなされているかを確認することが必要です。

2) Web サーバの設定

(1) CMS(Contents Management System)を利用する場合は、その管理画面のページに対して IP アドレスによるアクセス制限を実施し、CMS 管理者以外の者がアクセスできないようにしてください。パスワードについても初期設定のままにせず、十分に複雑なパスワードを使用してください。

(2) ディレクトリリスティングの機能は、必要がない限り無効にしてください。

3) Web アプリケーションの作成

Web アプリケーションを自作する場合は、SQL インジェクションなどの Web アプリケーションの脆弱性に注意して設計してください。

3.5.8 メールサーバ

NICE 内に設置されたメールサーバへの学外のユーザからの通信（メールソフトやウェブメールの通信）は、原則として、全学ファイアウォールにより遮断されます。多要素認証を導入した場合は遮断を

解除することができます。また、情報連携推進本部長が特例として認めたメールサーバについても遮断を解除することができます。

3.6 個人向けコンピュータ

ここで対象とするのは、パソコン、クライアントとして利用するワークステーション、タブレット端末、スマートフォンです。個人で利用するパソコンなどは利用者本人が管理者であることに十分留意してください。

3.6.1 管理者の義務と責任範囲

1) パスワードの設定

パスワードが設定できるものについては必ずパスワードを設定してください。 個人利用だからといって、パスワードなしで利用することのないようにしてください。指紋認証などの生体認証、TPM の利用なども有効です。

2) 共同利用のパソコンの管理

共同利用する業務用などのパソコンについては、その設置にあたって運用方針や運用管理責任者を定める必要があります。個々のパソコンの利用者は定められた運用方針に従って利用しなければなりません。

3) サーバ機能を有するパソコンの管理

個人向けコンピュータであっても、サーバ機能を持っている場合は、「3.5 サーバ」と同等に管理してください。特に、予期していない UNIX / Linux のインターネットサービスや Windows IIS、ファイル共有、DLNA が起動することのないように十分注意してください。

4) セキュリティパッチの適用

使用している情報機器の OS 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。管理者は、定期的に各ベンダー等の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、必要な対応をとることが求められます。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。また、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をオンとするのも有効な方法です。

5) マイクロソフト Windows の管理

パソコンの OS として多く利用されている Windows は、多く流通しているが故にセキュリティホールを突いたウイルスが作成され、NICE 内でもしばしば感染の被害が出ています。Windows パソコンの管理者は以下の点に注意してください。

a) Windows Update の自動更新を有効にする

Windows OS のセキュリティホールを解決する Update 情報は頻繁に提供されています。Windows Update はスタートメニューから起動できるようになっていますし、実行も簡単にできますので、毎月１日に実行するなど、定期的に実行するようにしてください。

Windows には自動更新の機能が組み込まれています。この機能を有効にしておけば、更新情報

を自動的に検出して通知してくれるので、更新し忘れが防止できます。

b) ウイルス検出ソフトを機能させておく

Windows パソコンの管理者は、ウイルス防止対策をとる義務があります。ネットワークに接続するパソコンには、必ず、コンピュータウイルス対策ソフトウェアをインストールするとともに、最新のウイルス定義ファイルを使用するように設定を行ってください。ウイルス定義ファイルの自動更新機能をオンにするのもよいでしょう。多くのウイルス対策ソフトでは、ウイルス定義ファイルの自動更新機能がオンになっています。

6) アップル Mac OS の管理

Mac OS もウイルスに感染する危険性があります。ウイルス対策ソフトを導入してください。名古屋大学では、Mac OS 用のウイルス対策ソフトを配布しています。

a) ソフトウェアアップデートの自動適用を有効にする

MacOS X でも Windows と同様、ネットワークを介したソフトウェアアップデートが提供されており、この機能は標準ではオンになっています。ソフトウェアアップデートを利用して、ソフトウェアを最新の情報に保ってください。

7) タブレット端末、スマートフォンの管理

タブレット端末やスマートフォンもパソコンと同様のセキュリティ対策が必要です。OS やアプリケーションソフトウェアのセキュリティパッチを適宜適用してください。ウイルスに感染する危険性がありますので、ウイルス対策ソフトの導入などを検討してください。

8) アプリケーションソフトの管理

OS と並んで、最近ではアプリケーションソフトのアップデートもネットワークを通じて配布されています。自動的にアップデートする設定を有効にしておくとよいでしょう。

3.7 特殊機器

ここで対象とするのは、事故、災害、健康被害等を引き起こす危険性を有する機器、およびそれを制御する機器です。例えば、以下のような機器です。

1. レーザー機器
2. エックス線装置
3. 産業用ロボット
4. 強磁場発生装置
5. 医療機器

1) 特殊機器の接続

特殊機器は、原則としてインターネットにアクセスできないようにしてください。これらの機器が外部からの攻撃により正常に動作しなくなった場合、事故や災害につながる恐れがあります。メンテナンス等の安全上の理由によりやむを得ず、特殊機器をインターネットにアクセスできるようにする場合でも、プライベートネットワーク内に機器を設置し、VPN 接続を利用するなど、外部から直接アクセスできないような環境で使用してください。

2) 接続申請

安全上やむを得ず、特殊機器を NICE に接続する場合は、特殊機器が正常に動作しなくなった場合に生じうるリスクとその対策について検討し、部局長の承認を得た上で、情報連携推進本部に事前に接続申請書を提出する必要があります。

3) 汎用 OS をベースとした特殊機器の管理

Windows/Linux 等の OS をベースにした特殊機器はサーバ機能が利用できるため、「3.5 サーバ」としての管理も必要です。

3.8 情報機器の持ち出しおよび持ち込みについて

1) 持ち出しについての許可

ノートパソコンやスマートフォン・タブレット端末はいろいろな場所で利用できるため、セキュリティの面からは注意が必要です。学外へ本学が所有する情報機器（レンタルも含む）を持ち出す場合には、機器設置責任者の許可を取るとともに、機器上に保存しているデータに応じて、その取扱いを定めるルール（例えば「東海国立大学機構個人情報保護規程」、「東海国立大学機構情報格付け基準」）に従うようにしてください。

2) 情報機器の持ち込み

学外へ持ち出した情報機器、あるいは個人所有の情報機器を NICE に接続する場合、事前にマルウェアに感染していないかを確認してください。個人所有の情報機器であっても、それを NICE に接続する場合は、本学の情報機器と同程度のセキュリティ対策を実施する必要があります。

3.9 その他の情報機器

ここで対象とするのは、ネットワーク設備機器、サーバ、および個人向けコンピュータ、特殊機器以外の情報機器です。プリンタ、スキャナ、複合機、テレビ会議システム、NAS（ネットワーク接続ストレージ）、計測設備機器などが該当します。

1) パスワードの設定

パスワードが設定できるものについては必ずパスワードを設定してください。 個人利用だからといって、パスワードなしで利用することのないようにしてください。また、一見パスワードには縁がなさそうなネットワークプリンタのような装置でも、設定用のパスワードがある場合があります。このようなパスワードは初期設定のままにせず、管理に適切なパスワードを設定してください。

2) その他の情報機器の管理

これらの機器には Linux 等の OS が使用されている場合があります。そのため、ファームウェアの定期的な更新が必要です。ファームウェアが公開されず、第三者が被害を受けるような脆弱性が修正できない場合は、機器をネットワークに接続しないなどの対応をとるようにしてください。

注意事例

- 情報漏えいを防ぐために、プリンタ、スキャナ、複合機、NAS は、プライベートネットワークに接続してください。プライベートネットワークを構築するサービスとして、情報連携推進本部は Secure NICE（http://www.icts.nagoya-u.ac.jp/ja/network/secure-nice.html）

を提供しています。

- テレビ会議システムなどのグローバルネットワークに接続することを前提とした機器以外のその他の情報機器は、グローバルネットワークへの接続は原則として認められません。

3.10 暗号化手法について

ネットワークを利用した通信内容やコンピュータ上に保存された情報は、本人の意思にかかわらず、内容が漏えいしてしまう可能性があります。漏えいを避ける一つの手段として、情報の暗号化が挙げられます。具体的には、以下の項目があります。

1) Web サイトの暗号化

Web サイト全体を常時 SSL 化することにより、なりすましや盗聴の防止などのセキュリティリスクの低減が期待できます。また、主要な Web ブラウザは、常時 SSL 化されていない Web サイトに対してアドレスバーに警告を表示することがあります。Web サイトの URL が https:// から始まること、および正しい証明書を使っていることを確認してください。サーバ証明書には、名古屋大学サーバ証明書発行サービス（https://upki.icts.nagoya-u.ac.jp/csi_server_cert/）を利用することができます。

2) 電子メールの暗号化

電子メールで重要な内容をやりとりする場合は、内容を暗号化してください。暗号化の機能を持ったメールクライアントやツールを利用するようにしてください。具体的には PGP などが挙げられます。

3) データファイルの暗号化

コンピュータ上のデータファイルを暗号化するツールが多数存在します。

4) 通信の暗号化

通信を暗号化するプロトコルは、「CRYPTREC 暗号運用ガイドライン」を参照し、十分に安全性が確認されているものを採用してください

URL: https://www.cryptrec.go.jp/op_guidelines.html

注意事例

- TLS1.1 以前のプロトコルは十分な安全性が確保できないため、利用不可に設定にして使用しないようにしてください。

3.11 リモートアクセス環境について

VPN (Virtual Private Network) サーバやリモートデスクトップなどのリモートアクセス環境は、学外から学内への侵入経路となりうるため注意が必要です。学内に設置する VPN サーバやリモートデスクトップを有効にしている機器については、「IP アドレス管理システム」においてポート公開の申請をしてください。公開の目的や状況によっては、利用が認められない場合があります。VPN については、段階的に情報連携推進本部が提供する VPN サービスに集約することを予定しています。

1) 利用開始、および利用停止の手順の整備

リモートアクセス環境について利用開始の手順を定め、リモートアクセスを必要とするユーザのみが利用できるようにしてください。また、不要になったユーザアカウントを無効にできるように

利用停止の手順を定め、定期的に（少なくとも年 1 回程度は）アクセス可能なユーザの見直しを実施してください。

2）利用者の認証

利用者の認証に使用するパスワードは、その他のシステムのパスワードを使いまわさないようにしてください。

3）情報へのアクセス

要機密情報を、リモートアクセス環境を構成するシステムに置くことは認められません。また、リモートアクセス環境からアクセスする学内システムは、IP アドレスで制限するなどして最小限にとどめてください。

注意事例

- 電子ジャーナルやサイトライセンスソフトウェアには、リモートアクセス環境を経由した利用が禁じられているものがあります。ライセンス違反とならないように注意してください。

4）認証ログ

認証に関するログは、少なくとも 1 年間は保管してください。また、定期的にログを確認して、不正アクセスがないかを調査してください。

5）SSH の認証方法

グローバル IP アドレスを持つ SSH サーバは、公開鍵認証または多要素認証による利用者認証を必須とし、パスワード認証は無効にしてください。プライベート IP アドレスしか持たない SSH サーバは、公開鍵認証または多要素認証の使用は任意とします。

第 4 章　クラウドサービス利用ガイドライン

4.1 概要

本章では、クラウドサービスを利用しようとするすべての本学構成員を対象として、クラウドサービスを安全に利用するための指針を提供します。一般に、クラウドサービスは「クラウド事業者の管理の下」、「他の利用者とコンピュータ資源を共有」して運用されています。そのため、クラウドサービスで取り扱う情報については、このような運用形態を意識する必要があります。本ガイドラインでは、クラウドサービス選定時に留意すべき事項について説明しています。なお、機微な情報をクラウドサービスで扱う場合は、事前に情報連携推進本部に相談してください。

4.2 クラウドサービスの選定

クラウドサービスを利用する際には、そのクラウドサービスがどのように運用されているかを事前に把握することが重要です。以下に、クラウドサービス選定の際に留意すべき事項について挙げます。

4.2.1 クラウドサービスとの接続

クラウドサービスを利用する場合、名古屋大学の外部のサーバを利用することになります。そのため、クラウドサービスを構成するシステムとそれを利用する端末間の通信の安全性を確保するために、以下の事項が満たされるかを確認してください。

1) 通信の暗号化

利用者の端末からシステムまでの通信が暗号化できるかを確認してください。

2) アクセス制限

システムへのアクセスに関して、IP アドレスによるアクセス制限をかけることが可能かどうかを確認してください。また、アクセス制限により学内の特定の端末からのみアクセス可能にするような運用にしてください。（ウェブサイトなどの外部への公開を意図している部分についてはアクセス制限の対象には含まれませんが、サイトの管理画面等はアクセス制限の対象です。）

4.2.2 クラウドサービス上のセキュリティ対策

クラウドサービスにおいても、セキュリティについて意識することが必要です。クラウドサービス選定時には以下の事項について確認してください。

1) セキュリティポリシー

クラウドサービスがどのようなセキュリティポリシーで運用されているかを確認してください。

2) マルウェア対策

マルウェア検知・防御が可能かどうかを確認してください。

3) セキュリティインシデント発生時の対応

セキュリティインシデント発生時にクラウド事業者がどのように対応するかについて確認してください。

4) システムのログ

クラウドサービスのシステムに関するログが閲覧できるか確認してください。

4.2.3 契約条件

1) 責任範囲の明確化

クラウド事業者と本学との責任範囲や損害補償について、契約時に書面を交付するなどして明確にしてください。

2) 準拠法

係争時にどこの法に準拠するかを確認してください。

4.2.4 データの取扱い

1) データの所有権・利用権

クラウドサービス上のデータについて、その所有権、および利用権を、クラウド事業者が提供する文書を確認する、あるいは契約時に書面を交付するなどして明確にしてください。

2) 契約終了時のデータの扱い

クラウドサービス契約終了時に、クラウドサービス上のデータ、およびユーザのデータが適切に削除されるかを確認してください。

4.2.5 サービスの品質の確認

長期的にクラウドサービスを利用する場合は、その事業者が長期的にサービスを提供可能であるかについて検討してください。また、サービスの稼働率や応答時間など、十分な性能が提供されるかについても事前に確認してください。

4.3 クラウドサービスの利用

4.3.1 ユーザ情報の管理

通常の情報機器と同様に、パスワードは簡単に推測できないものとし、他のサービスと同じパスワードは使いまわさないようにしてください。

第５章　情報セキュリティ研修・啓発ガイドライン

5.1 概要

名古屋大学情報セキュリティポリシーは、情報機器・情報資源の公開性・利便性に伴う危険と責任の自覚の必要性を指摘し、「研修制度の導入と啓発活動」の実施を定めています。この情報セキュリティ研修・啓発ガイドライン（以下、研修ガイドラインと略称）は、研修と啓発活動の実施に関する具体的な指針を提供するものです。

5.2 情報セキュリティ研修・啓発体制

情報セキュリティ室と情報セキュリティ単位組織が協力して、情報セキュリティに関する研修・啓発を実施します。

5.3 情報セキュリティ研修の基本的な考え方

本学の構成員が、(1) NICE に接続された情報機器やサブネットワークの利用資格を取得しようとする場合、(2) 情報機器を NICE に接続中あるいは接続しようとする場合、(3) NICE の管理運用に関与する場合には、研修を実施することを原則とします。

情報セキュリティ研修には、初期研修、定期研修、臨時研修の３種類があり、ネットワーク利用者、情報機器の管理者を対象に実施します。

5.3.1　初期研修

初期研修は、本学の各種ネットワークの利用資格を初めて取得する者（例えば新入生、新任教員、新任研究員、新任職員）と、情報機器の管理者に初めて任命された者を対象にして実施します。

1) ネットワーク利用者の初期研修

ネットワーク利用者に行う研修は、情報システムガイドライン（利用者心得）その他を教材として使用し、次の４項目に重点をおいてガイダンス、e-Learning 等を通じて実施します。

(1) 情報セキュリティの目的と重要性。
(2) 利用者は、何ができて何ができないか。
(3) 利用者は、問題が起きたときにどのように対処すべきか。
(4) 利用者自身の情報セキュリティに関する心構えの必要性。

2) 情報機器を NICE に接続しようとする者の初期研修

管理者に対して行う研修は、別に作成するセキュリティ技術ガイドライン、情報システム利用ガイドラインその他を教材として使用し、次の 4 項目に重点をおいて実施します。

(1) 情報セキュリティの目的と重要性。
(2) 管理者自身の情報セキュリティに関する心構えの必要性。
(3) 管理者が持つべき情報セキュリティ技術。
(4) 管理者は、問題が起きたときにどのように対処すべきか。

3) NICE の管理運営にあたる者の初期研修

NICE の管理運営にあたる者の初期研修については、情報連携推進本部で計画を策定します。

4) 初期研修実施の基本的な考え方

(1) 効率的な研修実施計画の策定

情報セキュリティ室は、初期研修実施の方法について、情報セキュリティ単位組織と十分な連絡調整を行ったうえ、情報セキュリティ単位組織ごとの初期研修計画が重複なく、効率的に実施されるように配慮することが望まれます。

初期研修実施にあたっては、オンライン学習の導入など省力化に努めるとともに、学習者に負担をかけないよう定められた期間内であればいつでも受講可能な方式の導入が必要です。

(2) 初期研修受講記録の保存

情報連携推進本部または情報セキュリティ単位組織は、初期研修を受講した人の記録を適切な期間保存するものとします。

(3) 初期研修の省略

初期研修は、情報機器の利用資格を新たに与えるたびに実施することを原則としますが、他で受講した初期研修が内容的に十分であると判断できる場合には、その利用申請者が実際に初期研修を受講していたことを確認した上で、省略することができます。

5.3.2 定期研修

情報セキュリティ室は、情報セキュリティ単位組織と協力し定期研修を実施します。情報セキュリティ単位組織は、必要に応じて独自定期研修を実施します。

5.3.3 臨時研修

情報セキュリティ室は、情報セキュリティ単位組織と協力し臨時研修を必要に応じて実施するものとします。情報セキュリティ単位組織は、必要に応じて独自の判断で臨時研修を実施することができます。

5.4 啓発

情報セキュリティ室は、情報セキュリティ単位組織と協力して、情報セキュリティに関する情報を収集し、本学の構成員に対して提供します。啓発活動は、メーリングリスト、Web を通じた周知、パンフレット、ポスターを通じた周知など、さまざまな媒体を利用します。情報セキュリティ室は、情報セキュリティに関する情報を名古屋大学情報連携推進本部のホームページに一元的に集約します。