<一般利用者向け>

情報セキュリティ
テキスト

令和６年４月

室蘭工業大学
情報基盤委員会

目次

1. はじめに

情報セキュリティと私たちの生活

現代生活の中では、パソコンやスマートフォンを利用することが当たり前となっています。日々進化する情報技術を日常生活や仕事、研究活動に活用するためには、情報の扱いに注意を払うことが必須になります。

本書では、情報セキュリティの基本事項をわかりやすくまとめました。本書は情報システムを利用する為の具体的な方法を明記した解説書です。

本書に記載したルールやエチケットを守って、本学の情報システムを教育および研究に活用したり、日常生活の中で一般に提供される情報サービスを快適に利用することを望みます。

室蘭工業大学の情報セキュリティポリシー

大学の情報システムを利用するにあたり、その利用ルールとして「情報セキュリティポリシー」が決められています。教職員、学生を問わず利用者は情報セキュリティポリシーを遵守することが求められます。

情報セキュリティポリシーの対象範囲

情報セキュリティポリシーは次の範囲に適用されます。

- 情報基盤・教育システム
  - 大学の公式メール(WEB メール)
  - 大学の公式ホームページ
  - 学習支援システム(Moodle)
  - 実習室に設置してあるパソコン
  - 図書館のパソコン、国際交流室など学内に設置してあるパソコン
- 大学内のネットワークシステム（キャンパス情報ネットワークシステム）
  - 学内からのインターネットアクセス(SINET を経由したアクセス)
  - 大学で設置した無線ネットワーク(eduroam)を利用した通信
  - 研究室の有線ネットワーク、無線ネットワーク(WiFi)を利用した通信
    （私物のパソコンやスマートフォンからの利用を含む。）
- 図書館情報システムや学務情報システム（CAMPUS SQUARE)、グループウェアシステム（Garoon）などの学内の情報システム全て

補足１．私物のパソコンやスマートフォンであっても、大学のネットワークに接続し利用する場合には、情報セキュリティポリシーが適用されます。

補足２．研究室や部局などに設置した無線 LAN アクセスポイントに接続する場合にも、情報セキュリティポリシーが適用されます。本書の注意を守って利用して下さい。

2.　目的外行為の禁止と運用への協力

●大学のパソコンとネットワークを教育・研究以外の目的で利用しない

例：WiFi 経由や研究室ネットワークから違法コンテンツのダウンロード、ゲームやアダルトサイトの閲覧をしない。

●ファイル交換ソフトウェアを利用しない

目的外の利用禁止

本学のパソコンやネットワークは教育・研究目的で提供しています。教育・研究以外の目的に利用しないでください。次の例は目的外の使用になります。

(1) 学内から目的外のサイトへのアクセス

本学のネットワーク(WiFi 含む)を使った以下のサイトの閲覧。

・音楽や映画の違法ダウンロードサイト　・商用プログラムの違法ダウンロードサイト
・ゲームやアダルトサイト　・クラッキングツールのダウンロードサイト

ウイルス感染などのトラブルの原因にもなるため、アクセスしないで下さい。

(2) パソコンの教育・研究目的以外の利用

アルバイト先のチラシの作成や政治宗教活動などへの利用はしないで下さい。

(3) Winny などファイル交換ソフトの利用は禁止しています。

ファイル交換ソフトはセキュリティ上のリスクが大きいため、自宅でも利用しないことを推奨します。

運用への協力

(1) ウイルス対策をしていないパソコン・スマートフォンやウイルス感染が疑われるパソコンをネットワークに接続すると、他の人のパソコン、スマートフォンにウイルスを感染させ、迷惑をかけます。**研究室などのネットワークを停止させる原因になりますので**、ウイルス感染が疑われるパソコンやスマートフォンはネットワークに接続しないでください。

(2) ネットワークは学内で共有している有限の資源です。有効活用のため、独り占めしないような配慮をお願いします。例えば、大容量のファイルのダウンロードなどは長時間ネットワークに負荷をかけますので、ご遠慮願います。

(3) 迅速な解決のため、情報教育センター提供のパソコン故障やサービス不具合などの異常に気付いた場合には、情報教育センター技術室にご連絡願います。

お問合せ・ご相談・報告先
情報教育センター 技術室（C301）
電 話 番 号）　0143-46-5895 または 0143-46-5896
ホームページ）　https://wp.mmm.muroran-it.ac.jp/

3.　ID、パスワードの適正利用

●強固なパスワードを利用して、定期的に見直す
●学内のパスワードを学外サービスと共用しない
（使い回しの禁止）
●パスワードを他人に教えない
（付せん紙などに書いてパソコンに貼らない）

本人を認証する手段として ID 及びパスワードが使われます。これらを盗まれると、第三者が勝手にシステムを利用し、情報を盗むことが可能になります。ID 及びパスワードの管理を徹底することが必要です。

パスワードの設定

(1) 英数字、記号を組み合わせて、８文字以上のパスワードを設定してください。
(2) 辞書を使った攻撃に備えて、推測されやすい単語は使わないようにします。
(3) 利用しているパスワードは定期的に変更するようにして下さい。
(4) 大学サービスのパスワードを、学外のサービスに使い回さないでください。学外サービスのパスワードが漏えいした場合、学内サービスへ侵入される可能性が高まります。

ID、パスワードの管理

・ID、パスワードは他人から保護してください。

外部に漏れないように管理することが重要です。パスワードを他人に教えたり、付せん紙に書いてパソコンに貼ったりするような行為はしないでください。学内の掲示板など、多くの人が目にする可能性のある場所に掲示しないで下さい。

・センターの発行した通知書は教室などに放置しないでください。

初期パスワードを変更した上で、破棄して下さい。

・ID の貸し借りは禁止です。

例え、友達が許可したとしても、友達の ID、パスワードを使ってシステムにログインしたり、サービスを利用したりするなどの行為はしないで下さい。

・ID 連携に注意してください。

SNS などのサービスでは、ID を連携してログインする仕組みが提供されています。
（例：Instagram に Facebook アカウントでログイン）
連携している場合、連携元の ID やパスワードが漏えいすると複数のサービスが利用されてしまいます。ID、パスワード管理には、より注意が必要です。

4. パソコン用ソフトウェア

●サポートの切れたOS、アプリケーションは利用しない
●必ずOSとアプリケーションのアップデートを行う

パソコンのソフトウェアは“生もの”です。基本ソフト(OS)やアプリケーションソフトはソフトウェアベンダーによってサポートされる期間が決まっています。サポートの切れたソフトウェアを使い続けると、脆弱性を突かれてウイルスに感染するリスクがあります。

必ず、サポートされているソフトウェアを利用しましょう。

室蘭工業大学では、サポートの切れた OS をキャンパスネットワークに接続することを禁止しています。研究室などで古いパソコンを利用する場合には導入されている OS がサポートされているかどうかを確認して下さい。

サポートの切れた OS の使用禁止

現行サポートされている OS を使い、古い OS は使わないで下さい。
以下の OS はキャンパスネットワークに接続することが許可されていません。

- Windows8.1 以前の Windows および Windows10 Version 20H2 以前の Windows10
- macOS 10.14 Catalina 以前の MacOS

OS の自動アップデート

OS の自動アップデートを設定し、アップデートが発表された場合には必ずアップデートを実施するようにして下さい。

サポートの切れたアプリケーションの使用禁止

サポートされているアプリケーションを使い、サポート期限の切れたアプリケーションは使わないで下さい。

以下のアプリケーションは 2023/3 現在サポートが切れており、使用できません。

- アドビ製品
  - Acrobat Pro 2017/ Acrobat Standard 2017/ Acrobat Reader 2017 以前の Acrobat
  - Acrobat DC Pro / Acrobat DC Standard /Acrobat Reader DC
- Java 関連製品
  - Oracle Java 10(LTS), Oracle Java 17(LTS) 以外の製品
  - OpenJDK 11(LTS), OpenJDK 17(LTS)以外の製品

アプリケーションのアップデート

アプリケーションのアップデートを必ず実施して下さい。
可能な場合には、自動アップデートを設定して、最新版に保つようにします。

5.　ソフトウェアライセンス

●ソフトウェアはライセンスを守って利用する
（海賊版ソフトは利用しない）

パソコンのソフトウェアは著作物であり、ライセンス条件として利用できる範囲が決まっています。利用条件を守って正しく利用しましょう。**ライセンス条件に違反すると、あなたや大学が権利者から訴えられたり、法律で罰せられたりすることがあります**。

ソフトウェアライセンスの遵守

ソフトウェアはライセンス条件を守って利用して下さい。ライセンスを保有していないソフトウェアを導入してはいけません。またインターネットからダウンロードしたライセンスの不明確なソフトウェアは導入しないで下さい。

フリーソフトウェアの利用

インターネット上には、無料の（ライセンス費用のかからない）いわゆるフリーソフトウェアが公開されています。利用にあたっては、以下の点に注意が必要です。

・ライセンス条件の確認

フリーソフトウェアには様々なライセンスが設定されています。中には、商用利用の禁止のような条件もありますので、自分の利用目的で問題ないか確認が必要です。

・入手先

作成者のサイトや大手のリポジトリなど信頼できる場所から入手するようにしましょう。ウイルス感染、悪意のある改ざんをされたソフトウェアが出回っている可能性があります。

不正に改造されているソフトウェアの禁止

ライセンス認証が不要になる違法に改造された商用ソフトウェア（海賊版ソフト）をインターネットからダウンロードして利用しないで下さい。

ライセンス認証を回避するように改造されていたとしても、実行時にソフトウェアベンダーのライセンス認証サーバと通信を行うことがあります。この通信によって、商用ソフトウェアベンダーは、大学で不正にソフトウェアを使用していることを検知することが可能です。ライセンス違反として利用者や大学を訴える事例が発生しています。

大学で契約しているソフトウェアの利用

大学で契約しているソフトウェアライセンスは在学中に限り利用可能です。

- マイクロソフト(EES)
- Apex One

卒業後は継続して使えませんので、ソフトウェアをアンインストールして下さい。
卒業後も利用する場合には、改めてソフトウェアの購入が必要になります。

6.　ウイルス対策ソフト

必ず大学で提供しているソフト(Apex One)を導入すること

Windows Defender では不十分です
macOS や Linux でも導入すること

ウイルス保護(リアルタイムスキャン)をオンにし、パターンファイルの自動更新を行うこと

定期的に完全スキャンを行うこと

ウイルス対策ソフトを入れていないパソコンをインターネットにつなぐと、確実にウイルスに感染します。ウイルス対策を必ず実施して下さい。ウイルス対策を未実施のパソコンは本学のネットワークに接続することが禁止されています。

導入

パソコンを購入したら、本学で提供する Apex Onee を必ず入れてください 。

Windows の場合 WindowsDefender が付属していますが、このソフトは検知率が低くアップデートも少ない為、ウィルス対策ソフトとしては不十分です。また、macOS および Linux 向けのウイルスも多く存在しますので、Apex One を入れてください。

購入したパソコンに商用のウイルス対策ソフトが付属している場合には、そのまま利用可能です。ただし、試用期間やライセンス期限を過ぎると利用できなりますので、ライセンスが切れる前に Apex One を導入してください。

パターンファイルの更新

ウイルス対策ソフトを導入したら、リアルタイムスキャンをオンにして下さい。ファイルを保存時にウイルスが混入していないか確認（ウイルスチェック）してくれます。

また、ウイルスのパターン定義ファイルを定期的に更新するように、自動更新をオンにしておきます。

定期スキャンの実施

リアルタイム検知スキャンがオンになっていると、ファイル保存時にウイルスチェックされますが、ファイル保存後にウイルスパターンが更新され、新規にウイルスと認定されることがあります。このため、定期的に(補足１)完全スキャン（補足 2）をかけて、既存のファイルがウイルスに感染していないか、確認を行って下さい。

補足１．週一度以上が望ましい。

補足２.「完全スキャン」がない場合は、パソコンの HDD を対象にスキャンしましょう。

ウイルス感染時の対処方法

パソコンに異常な表示が出たり、動作が極端に遅かったりするなど、ウイルス感染と思われる現象を確認した場合、以下を行って下さい。

Step.1　オフラインにする

ネットワークケーブルを抜き、かつ、無線 LAN（WiFi）機能をオフにします。
（ネットワーク経由での他のパソコンへの攻撃を遮断するため）

Step.2　別のパソコンで対策ファイルを入手する

感染の疑いのない別のパソコンを使って、最新のウイルス対策ソフト(Apex One)のインストーラーをダウンロードします。

Step.3　対策ファイルを導入する

CD や USB メモリを使って、ウイルス対策ソフト（Apex One）のインストーラーを該当パソコン上に保存し、実行します。

Step.4　パターンファイルを更新する

ネットワークに接続して、ウイルス対策ソフトのパターンファイルをアップデートします。

補足１．アップデートの操作のみ行って下さい。
補足２．本来、ウイルス感染または感染の疑いがある状態で、ネットワークに接続すべきではありません。可能な場合は、Step2 で最新のパターンファイルも入手しておき、Step4 はオフライン状態で行うべきです。しかし、昨今では、オンラインでの利用を前提としたウイルス対策ソフトもあり、オンラインにしなければ更新できない場合があります。

Step.5　オフライン状態で、完全スキャンを行う

再度ネットワークから切断します（Step1 の操作を行う）。その後、ウイルス対策ソフトで完全スキャンを行い、ウイルスを除去します。

Step.6　OS をアップデートする

ネットワークに接続して、OS をアップデートします。
（Windows の場合は「WindowsUpdate」、macOS の場合は「ソフトウェア・アップデート」です。Linux の場合は OS によって呼称が異なります）

ウイルスの除去ができないなど、対処に困った場合は、
情報教育センターに相談してください。

●センターに連絡がつかない場合
当該PCはオフライン状態のまま電源をオフにして下さい。ご自身で対処する場合は、安全なPCで情報を検索し、信頼できる情報であるかに注意して下さい。偽の解決方法やツールが公開されている場合があります。

7. スマートフォンの利用

サポートされている端末および OS を使い、古い端末は使わない
アプリケーションは信頼できる場所から入手し必ずアップデートする
パスワードや生体認証でロックし、なくさない対策をとる
なくした場合に備えて、保護機能を利用する

スマートフォンは機能的にはパソコンと同等で、セキュリティ対策が必要です。友達の住所や連絡先など漏えいしては困る情報をたくさん格納しているため、悪意のあるアプリケーションから保護することが必要です。毎日持ち歩くため、なくした場合のダメージも大きく、対策が必要です。

OS

古い OS には脆弱性があり、利用しているとウイルスに感染します。OS のアップデートは必ず実施して下さい。自動アップデートの設定を行っておくと安心です。サポートされている端末および OS を使い、古い端末は使わないようにします。室蘭工業大学では、サポートの切れたスマートフォンをキャンパスネットワークに接続することを禁止しています。

アプリケーション

アプリケーションは信頼できる場所（公式のアプリストアなど）から入手して下さい。オンラインで非公式に配布されているアプリケーションは、スマートフォンの情報を流出させたり、悪意ある機能を持っていたりすることがあります。また、導入後に脆弱性が発見される場合もありますので、入手したアプリケーションにアップデートがあった場合には入替えて下さい。SNS アプリを利用する場合には、意図せずに個人情報が漏えいしない設定を行って下さい。

保護

スマートフォンを他人に利用されないように、パスワードや生体認証などでロックして下さい。そのほか、ストラップをつけるなど、なくしたり、置き忘れたりしないように対策を行って下さい。万が一なくしても、情報漏えいを防ぐ為、予め遠隔スワイプなどの設定をしておいてください。

8.　電子メールの利用

相手先メールアドレスを確認してから送信ボタンを押す
電子メールの送信時には、必ず件名をつける
SPAM メールは読まずに捨てる、リンクURLや添付ファイルは開かない
無料のメールサービスを利用する場合は情報漏えい対策をとる

メール作成の注意

- **誤送信の防止**
  一度送信すると取り消しができないため、間違えないように、送信前に必ず宛先メールアドレスを確認して下さい。送信内容のプレビュー機能や送信遅延機能（送信ボタンを押してからしばらくして送信する）の利用をお勧めします。

- **件名をつける**
  メールには、内容を表す簡潔な件名をつけて下さい。

- **添付ファイルを送信する場合は、本文でその旨を伝えます。**

- **極端に大きなファイル(数十 MB 以上)は送らないようにしましょう。**

メール受信の注意

- **疑わしいメールは開かないで捨てる**
  特に、知らない相手からのメールに注意します。SPAM メールかどうか、送信元が詐称されていないことを確認します。また、件名からも判断してください。件名のないメールは、SPAM メールの可能性があるので読まずに捨てて下さい。どうしても内容の確認が必要な場合でも、メールに含まれるリンク(URL)や添付ファイルは開かないようにして下さい。
- **HTML メールを使わない**
  メールはテキスト形式で受信するようにし、HTML 形式でメールを表示しないようにメールソフトを設定して下さい。HTML メールを開くと、リンク先の画像やファイルが自動的にダウンロードされ、相手にメールを読んだことがわかってしまいます。

本学以外のメールサービスの利用

Gmail や Yahoo!メールなど本学以外で提供されているメールサービスはメール本文が提供者に内容を確認されている（読まれている）可能性があります。
以下の点を注意して利用して下さい。

- **業務用に本学以外のメールサービスを利用しない。**
- **本学以外のメールサービスを使う必要のある場合、成績情報など秘密の内容は送らない。**
- **本学以外のメールサービスで成績情報など秘密の内容を送信する必要がある場合、送信内容をパスワードで保護、暗号化するなどして送る。**

フィッシングメールに注意

フィッシングメールは企業や団体になりすまして悪意のあるサイトへ誘導し、情報を詐取するメールです。身に覚えのないメールは、リンクをクリックしたり、添付ファイルを開いたりせずそのまま削除しましょう。

フィッシングメールの例

昨今では精巧な不審メールが増えており、公的機関や大手企業を騙る事例や、宅配業者、購入手続きの自動通知などを装った不審メールの事例があります。

【実例】楽天市場を騙ったメール

【楽天市場】注文内容ご確認（自動配信メール）

【楽天市場】
ご注文ありがとうございます

Rakuten

買い物かご 購入履歴
ヘルプ

この度は楽天市場内のショップ「*マサニ電気株式会社 楽天市場店*」をご利用いただきまして、誠にありがとうございます。

本メールは、お客様のご注文情報を受け付けた時点で送信される自動配信メールです。
ショップからの確認の連絡、または商品の発送をもってご購入についての契約が成立します。(in English <#faqEnglish>)

ご注文内容

注文番号 280052-20180509-00183503
注文日時 2018-05-09 15:25:38
お問い合わせ先

*マサニ電気株式会社 楽天市場店
問い合わせフォームから連絡

※下記内容については、上記の問い合わせ先より直接ショップにお問い合せください。
・商品やお取引に関するご不明点
・ご注文内容の変更(商品、決済・配送方法など)
・ご注文のキャンセル手続き
※ショップの情報・返品ポリシー・営業時間はこちら
※その他ご不明点がある場合は楽天市場のヘルプページ
をご確認ください。

9.　LINE の利用

LINE はリスクを理解して利用する
アドレス帳などの流失を防ぐ設定をする
直接会ったことのない相手からのメッセージや
電話は受け取らない

LINE はカジュアルな情報伝達手段として広く普及しています。大学生の間でも人気が高く、本学のほぼ全ての学生が利用しています。
以下の注意点を守って安全に利用して下さい。

アドレス帳流出防止

アドレス帳流出防止のため、プライバシー管理を厳格に行う。

例：「友だち追加設定で」以下の設定を行って下さい。
- 「友だち自動追加」をオフにする
- 「友だちへの追加を許可」をオフにする
- 「プライバシー管理」の「ID による友達追加を許可」をオフにする

上記の設定をしていないと、意図しない「友だち」が登録され、いつのまにか友だちとしてつながってしまうことがあります。

犯罪に巻き込まれないために

見知らぬ相手からの連絡で、犯罪に巻き込まれたりする危険を避けるため、以下のような対応を心掛けて下さい。
・知らない人からのメッセージや電話はブロックする。
・知らない人とインターネットを経由した ID 交換はしない。
・乗っ取られたアカウントが犯罪に利用される場合もありますので、ID やパスワードの管理を徹底する。

情報漏えいリスク

友だちとだけやり取りしているメッセージも、サービス提供者は内容を見ることができます。重要な情報は別の手段でやり取りするなどの配慮が必要です。

10. ソーシャルネットワークサービス(SNS)の利用

SNS は公の場であることを意識して発言する
個人情報や機微情報のやり取りは行わない
他人を中傷する発言を行わない

SNS の利用

Twitter、Facebook、 Instagram、 LINE などのソーシャルネットワークサービスはインフォーマルな情報交換のメディアとして人気があり、友達と情報交換を行う手段として手軽に利用されています。

しかし、便利さとは裏腹にリスクも存在するため、情報の発信には注意が必要です。

利用上の注意点

- **発信する内容に注意すること**

SNS では匿名性はないことを意識して発言してください。誰も見ていないと思っても、後にネットワーク上で検索すれば、発言があったことがわかります。例えば、違法行為を行った発言をしたり、不道徳な発言を行ったりした場合、発信者は特定され激しく非難される（ネットで炎上する）場合があります。

- **一度流出した情報は取り消せない**

一度インターネット上に発信された情報は、本人が発言を取り消しても、ネットワーク上でコピーされ、二度と取り消すことができません。

- **個人情報や機微情報を発信しない**

次のような情報は SNS でやり取りしないようにして下さい。

個人情報： 氏名、住所、生年月日、性別、電話番号、メールアドレスなど、個人を特定できる情報

機微情報： 銀行口座番号や残高情報、クレジットカード番号や借金の有無、健康保険証番号などに関する情報、病歴、持病、血液型などの医療情報、家族、親族関係や出身地などの情報、個人の趣味や嗜好などに関する情報

- **誹謗･中傷するような発言をしない**

他人を誹謗中傷する発言が、巡り巡って本人に伝わり、その人との関係を壊すこともあります。

- **画像の付加情報にも注意**

画像ファイルには、撮影した時刻や場所などの情報も同時に記録されています(EXIF)。画像共有サイトにアップロードする場合には、これらの情報が漏れないような設定にして下さい。

11. クラウドサービス

SNS、ストレージサービス、メールサービスなどの無料クラウドサービスは、リスクを理解した上で活用する。

重要データを置かない
暗号化する
別手段でバックアップをとる

インターネット上で提供されている無料アプリケーションを、本書ではクラウドサービスと呼ぶことにします。クラウドサービスには、以下のものが含まれます。

- X (旧 Twitter)や LINE、 Facebook などの SNS
- Dropbox や Google Drive、iCloud Drive などのストレージサービス
- Gmail や Yahoo!メールなどのメールサービス

クラウドサービスは無料で利用でき、便利に使うことができますが、次のようなリスクが存在します。

利用上のリスク

(1) サービス提供者によるユーザデータの利用

無料のサービス提供者は蓄積したユーザデータを利用してビジネスを行っているため、データ内容は利用されている（読まれている）と考えたほうが良いでしょう。例えば、マーケティングや広告の配信などに利用されていますが、それらに限りません。

(2) サービス提供者の管理ミスなどによるユーザデータ漏えい

サービス提供者の操作ミスなどで、ユーザデータがインターネットに漏えいするリスクがあります。

(3) ユーザデータの消失及びサービスの継続性

サービス提供者の操作ミスなどで、ユーザデータが消失するリスクがあります。また、サービス提供者の都合で、突然サービスが終了し、預けていたユーザデータを回収することができなくなるリスクがあります。

利用上の注意点

(1) 漏えい防止(預けない)

漏えいして困るような、重要なデータや業務データのやり取りや蓄積に利用しないで下さい。

(2) 漏えい防止(暗号化)

どうしても重要なデータや業務データを扱う必要がある場合には、預ける前にパソコン上で暗号化を実施して下さい。

(3) 重要データのバックアップ

サービス提供者の操作ミスや突然のサービス終了でデータを失うことに備えて、クラウドサービス以外の手段でデータのバックアップを行って下さい。

12. 情報発信に関する注意事項

情報発信を行う際には以下の注意をする。

情報発信するサーバに機密情報を置かない
定期的に発信する情報の見直しを行う
他者の権利を侵害しない

インターネットで安全に情報発信を行うため、以下の点に注意します。

情報発信するシステムの安全性の確保

(1) セキュリティの確保

OS や各種ソフトウェアなどは修正パッチなどを充て、恒常的に最新の情報を保つこと。
ページの作成を外部の業者に委託するときも同様である。

(2) CGI/SSI の利用禁止、公開掲示板（BBS）等の開設の禁止

意図しない利用をされる可能性があるため、本学の公開サーバでの使用を禁止する。

(3) 隠しディレクトリに関する注意

外部に公開しない機密情報は、たとえ隠しディレクトリであっても蔵置してはならない。

定期的に発信する情報の見直しを行う

(1) 有効期限の表示

ウェブページを公開する情報は、その有効期限を適切に明示すること。
有効期限がきた時点で当該情報をサーバから削除すること。

(2) 定期的な棚卸の実施

1 年に 1 度以上、情報の棚卸を実施し、情報発信の必要性を見直すこと。
棚卸時点で有効期限を過ぎている情報は、削除するか、その有効期限を更新すること。

(3) 組織変更時の対応

組織変更があった場合には、業務を継承する組織に引き継ぎを実施すること。
（継承する組織がない場合には、情報発信を中止すること。）

著作権等の知的財産の遵守

以下の点に注意すること

- 他人の知的財産を侵害しない
- 肖像権・パブリシティ権などを侵害しない
- 人を誹謗中傷する内容やプライバシーを侵害するような情報を掲載しない
- 企業等のロゴを利用するときは、事前に相手側と協議すること
- 写真などで顔を露出する際のリスクを十分に考慮すること

13. 情報漏えい対策

不要な情報は持ち出さない。持ち出す情報を最小限にする
持ち出す場合、パソコンの盗難防止に努める
USB メモリに重要なデータを格納して持ち歩かない
情報機器の廃棄の際には、ハードディスクを消去または破壊する

情報漏えいを防ぐためには、不必要に情報を持ち出さないことが第一です。どうしても、情報を持ち出す必要がある場合には、情報漏えいの対策が必要です。また、情報機器を廃棄する場合にも、廃棄機器から情報が漏えいしないよう配慮してください。

情報持ち出し

不要な情報は持ち出さないように心がけてください。どうしても持ち出す必要がある場合には、持ち出す情報を最小限にする工夫をして下さい。パソコンにはログインパスワードをかけておきます。盗まれたパソコンからハードディスクだけを取り出し解析されることを防ぐため、ハードディスクは暗号化しておきます。

情報機器の盗難防止対策

車で移動する場合は盗難を防ぐため、無人の車内にパソコンを放置しないで下さい。

電車で移動する場合にはパソコンをしまったカバンは網棚などに置かず、肌身離さず保持して下さい。また、出張先で懇親会に参加する場合には、会場までパソコンを持ち込まないようにして下さい。

USB メモリの利用

USB メモリは紛失しやすいため、重要なデータを格納して持ち歩かないようにします。止むを得ず利用する場合には、暗号機能付きの USB メモリを利用するなどの工夫をします。誤って不必要な情報を持ち出さないように、使い終わった USB メモリは格納する前に情報を消去しておきます。

情報機器の廃棄

パソコンを廃棄する場合には、専用ソフトを使ってハードディスク内の情報を消去します。可能なら、ハードディスクを物理的に破壊するなどの処置を行ってください。また、外部の業者などに廃棄を依頼する場合には、信頼できる業者に依頼し消去の証明書をもらって下さい。

【参考】業務用のパソコンについては、技術部で廃棄処理の代行を実施していますのでご相談下さい。

14. 情報セキュリティ事故発生時の行動

情報セキュリティ事故を起こした(発見した)ときは、慌てずに CSIRT(シーサート)に連絡する
できるだけ早期に連絡をする。

情報セキュリティ事故とは

次のような事象は、情報セキュリティ事故として扱います。

- 機密情報の入ったパソコンや USB メモリの紛失や盗難
- 機密情報（書類）の紛失や盗難
- コンピュータウイルス感染
- 機密情報のメール誤送信（送付先の誤り）
- 多量のスパムメール送信
- WEB サーバやパソコンからの情報漏洩（意図しない公開）
- 廃棄した情報機器からの情報漏洩
-

情報セキュリティインシデント対応チームとは

情報セキュリティ事故が発生した場合、被害を最小限にするため、できるだけ早期の対応が必要になります。このため、事故に対する緊急対応チーム（情報セキュリティインシデント対応チーム、CSIRT）が組織されています。

情報セキュリティ事故の際の連絡先

電子メール： m-csirt@mmm.muroran-it.ac.jp （CSIRT）
電話：0143-46-5896 （情報教育センター 技術室）

連絡の際は、具体的に詳しく状況を伝えて下さい。

2024 年 3 月　　第 9 版
2023 年 3 月　　第 8 版
2020 年 4 月　　第 7 版
2019 年 11 月　　第 6 版（電子版）
2018 年 3 月　　第 5 版
2014 年 3 月　　第 4 版
2012 年 3 月　　第 3 版
2010 年 3 月　　第 2 版
2009 年 3 月　　初版

監修･制作

室蘭工業大学　情報教育センター
https://www.icte.muroran-it.ac.jp