上智大学
上智大学短期大学部
上智社会福祉専門学校

学生用情報セキュリティハンドブック

（ver.1.5）

ICT技術は、急速に進歩しており、教育研究分野においても、コンピュータやインターネットを活用する場面が増えています。その一方で、ICT技術を悪用してコンピュータウイルスを拡散させたり、迷惑メールや詐欺メールを大量に送信するなど、インターネット上の脅威も増大しています。本学においても、ウイルス感染、アカウントの乗っ取りなど、情報漏洩の事故に繋がりかねない、重大なセキュリティ事故も起こっています。

本ハンドブックを活用いただき、情報セキュリティ対策の必要性のご理解と、対策の実施をお願いいたします。

2019年11月1日
学校法人上智学院　情報システム室

情報セキュリティ対策　9つの取り組み

1. ソフトウェア（OS・Officeアプリケーション等）の脆弱性対策
2. パソコン等のウイルス対策
3. ソフトウェア等の適切な管理
4. Webアプリ（ファイル転送ソフト・オンラインストレージ等）の利用に関する対策
5. 無線LANのセキュリティ対策
6. パスワード管理
7. インターネット（SNS等）でのトラブル回避対策
8. オンラインサービス等での不正使用の防止
9. 不要になったパソコン等の廃棄に関する手続き

STEP

01

ソフトウェア（OS・Officeアプリケーション等）の脆弱性対策

Webブラウザや電子メールソフト、OS、Officeアプリケーションなどのソフトウェアには、時間の経過とともに、脆弱性（ぜいじゃくせい）と呼ばれる不具合が発見されることがあります。

脆弱性を放置していると、ウイルス対策ソフトを入れていても、ウイルスに感染したり、パソコンに侵入されるなどの危険性が高くなります。

ソフトウェア脆弱性の対策として、次の対応を必ず実行してください。

OS・ソフトウェア等の**更新**を確実に行う

Windowsを使用している場合は、 Windows Updateを行うことで脆弱性（ウイルスが入り込みやすいプログラム上の弱い部分）を強化することができます。（Windows10は基本的に自動更新されます）

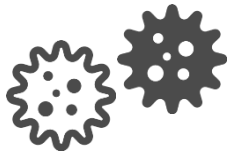
Windows以外のOSや各種ソフトウェアでも、**アップデートを実行する方法を確認**して、定期的に実行してください。

スマートフォンのアップデート情報にも注意する

- スマートフォンに通知される、OSや各種アプリのアップデート情報を確認して、適切にアップデートを行ってください。
- ただし、OSのアップデートを行ったために動かなくなるアプリなどもあります。また、アップデートが原因で不具合が起こる場合もありますので、事前に情報を集めて安全性を確認してから行うとよいでしょう。

サポートが終了しているOS・ソフトウェアは、可能な限り使用しない

- 代替手段がない場合は、ネットワークに接続しないなど、十分な対策をとってください。



STEP

02

パソコン等のウイルス対策

最近のウイルスは、電子メールを表示したり、Webブラウザでホームページを閲覧したりするだけで感染するなど、多様かつ巧妙なものになってきています。また以前に比べると、被害の内容や規模がすぐにわからないように活動するものもあります。

また、ウイルス感染はご自身の情報漏洩だけでなく、２次・３次感染により次の被害者を生み出すので、知らないうちに加害者になってしまう危険性もあります。

ウイルス対策ソフトを導入する

上智大学(短期大学部を含む)および上智社会福祉専門学校に在籍する教職員および学生は、在籍期間中、**情報システム室のWEBページからウイルス対策ソフト（Trendmicro ウイルスバスターコーポレートエディション）をダウンロードし、無料で使用**することができます。

ウイルス対策ソフトの**定義ファイルを自動更新**する

ウイルス対策ソフトを導入しただけでは、最新のウイルスに常時対応することができません。「パターンファイル」と呼ばれる定義ファイルを常に最新のものにしておく必要があります。

ウイルススキャンを**定期的に実行**する

ウイルス感染などセキュリティ関連のニュースに**常に関心を持つ**

「無料のオンラインストレージサービス」から個人情報が流出していたなど、情報セキュリティに関するニュースをよく耳にします。他人事だと思っていると、気づかずに使い続けて被害者となってしまうこともあります。常に注意を払ってIT機器を使用しましょう。

記憶媒体を差し込んだときには、フォルダやファイルを開く前に必ずウイルスチェックを実行する

USBメモリなど記憶媒体の自動実行機能を利用して、パソコンに差し込んだだけでウイルスに感染する事案が発生しています。

STEP

03

ソフトウェア等の適切な管理

ソフトウェア等は著作物のため、不正にコピー・配布することは刑事罰・損害賠償の請求対象となります。
逮捕・送検されることもあり、「知らなかった」では済まされない事態となってしまうケースもありますので、入手経路には責任を持ちましょう。
ソフトウェア等の適切な管理として、以下の対応をお願いします。

▶▶非公式なWebサイトなどから、**不正にソフトウェアを入手しない**

- 最近のアプリには追跡機能が付いています。正規品でないものを使用すると**使用者が特定され、警察に通報されたり、多額の賠償を請求されたりします**ことがあります。
- ウィルスが組み込まれているケースも多く、**多数の被害が報告**されています。

▶▶ソフトウェア**ライセンスの内容（使用権等）を確認**する

▶▶正規に購入したソフトウェアをにコピーして使用しない

▶▶契約したソフトウェアの**約款のとおりに適切に使用**する

不正なソフトｧエアやアプリを使用すると・・・

SPAMメールが頻繁に送られてきて、「便利だから」と必要以上に使用を勧められるアプリには、不正なものが多く含まれています。思わず欲しくなるような魅力的なアプリに偽装して、ユーザーにインストールさせようとします。
スマートフォンや、PCにそれらのアプリがインストールされると、外部から他人が遠隔操作できるようになります。その結果、

□知らない間に電話がかけられ盗聴される
□私生活や身の回りのものが勝手に撮影される
□位置情報を取得されて居場所を特定される
□保存されている画像やアドレス帳など個人情報が盗まれる

ということが起こります。
スマートフォンをお財布代わりに使用していれば、カード情報なども盗まれ、不正に使用されてしまうのです。

STEP

04

Webアプリ（ファイル転送ソフト・オンラインストレージ等）の利用に関する対策

ファイル転送ソフト（宅ファイル便）が不正アクセスを受け会員の個人情報が流出する事件がありました。無料のファイル転送サービスやオンラインストレージ（ファイルをWeb上に置くことで色々な端末からアクセスすることができるサービス）はとても便利ですが、管理する企業の人的なミスなどで個人情報が危険にさらされてしまうことがあります。

情報が流出した結果、損害賠償を請求され、精神的・経済的被害を受けることがあります。

ソフトウェア等の利用に関する対策として、次の対応をお願いします。

- 無料のクラウドサービスには、データを盗む目的のものもあるため、**大切な個人情報を安易に預けない。**

- 外部サービス（クラウドサービス）は**信頼できる（契約約款等が存在する）サービスを利用**する
- オンラインストレージ（iCroud、DropBox、GoogleDriveなど）を利用する際には、突然のアクセス停止やサーバーダウンなどに備えてバックアップをとっておく

オンラインストレージの利用について

Web上にアップロードしたファイルのURLを相手に送るだけで、簡単に共有できる「オンラインストレージ」はとても便利です。

ただ、フィッシングメールに掲載されているURLをクリックし、偽サイトや偽ファイルに誘導され、ウィルスに感染してしまうという被害も増えています。

共有しているフォルダに感染させてしまうと、被害は瞬く間に広がってしまいます。常に安全性を意識しながら使用するように心がけましょう。

本学ではSophiaメールを使用していますので、Office365で提供されている**OneDrive**を推奨しています。OneDriveはランサムウェア対策としてファイルの復元機能を備えています。

□ **OneDrive**の利用方法：

https://ccweb.cc.sophia.ac.jp/documents/#_217

STEP

05

無線LANのセキュリティ対策

無線LANは利便性の高さから、家庭やオフィスにおいても導入が進んでいます。最近では公衆無線LANサービスが普及し、駅や空港、カフェやレストランなどでも利用できるようになりました。しかし、無線LANは電波を利用する通信であるという性質上、**他人から通信内容を盗まれる危険性**があります。

また、自宅や研究室などに、ご自身で購入した無線LANルータを設置する場合は、セキュリティ設定に十分配慮してください。

- 情報システム室で推奨した無線LANを利用する

  本学で指定する無線LAN：**sophiawifi2019，eduroam**

- 自宅などで自前で無線LAN環境を構築する場合は、初期パスワードをそのまま使い続けるような安易な接続を行わず、WPA2パーソナル（AES)あるいはMacアドレス認証を使用する

- 公衆無線LANは安全性が保障できないのでできるだけ使わない

無線LANの危険性・・・

駅や飲食店でも公衆無線LANサービスが普及し、利用できる場所が増えました。特に、パスワード等の入力を必要としない無線LANや、共通のパスワードで利用できる無線LANの場合には、信頼できるものかどうか、よく確認してからアクセスすることを心がけましょう。

自宅や研究室などにご自身で無線LANルータを購入したり、海外への渡航の際に、持ち歩きのできるモバイルルータを借りるなど、無線LANが手軽に利用できるようになってきました。簡単に使用できますが、安全性を高めるために次の機能も利用しましょう。（参考）

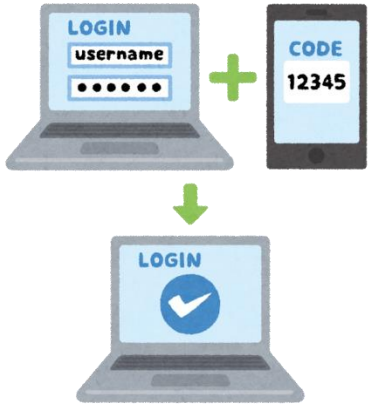
◆通信機器には、MACアドレスと呼ばれる固定の番号が付与されています。ルータの設定を行う場合に通信できるMACアドレスを登録して、接続するクライアントを制限しましょう。

◆無線LANルータには識別するための名前(SSID)が設定されていて、暗号化キー(パスワード)とセット登録されています。初期値のまま使用することも可能ですが、セキュリティ強化のために推測されやすい名前（利用者名や組織名など）は使わないようにしましょう。

STEP

06

パスワード管理



他人に自分のユーザアカウントを不正に利用されないように、推測されにくい安全なパスワードを作成し、他人の目に触れないよう適切な方法で保管することが大切です。
パスワードの管理として、以下の対応をお願いします。

- スマートフォンのパスワードもしっかりと管理をする
  - 人ごみで使用する場合には、誰かに見られていないか確認する
  - 推測されやすいパスコードは使わない
- 名前、生年月日等の**個人情報は使用しない**
- 英数字を含む**12文字以上**で設定する
  - 大文字・小文字・数字・記号の組み合わせが望ましい
  - システム制限がある場合は、可能な範囲で上記に近づける
- 他人に絶対に**教えない**
- 複数のサービスで**同じパスワードを使用しない**
- 2段階認証（ID・パスワードの他にセキュリティコードを入力）の仕組みを有するサービスの場合、**2段階認証を使用**することを推奨する。

安全なパスワードの作り方・・・

簡単な文章を作り、言葉の先頭だけを拾う、助詞の母音を抜くなどのルールを作ります。文字を記号に置き換えます。

「**s**ui**y**ou**18**ji**h**a**y**o**g**an**o**h**i**」（水曜18時はヨガの日）
→「 Sy18J!_h@Y0ganH!」

パスワードの強度チェックを行うサイトを利用する
例）カスペルスキー https://password.kaspersky.com/jp/
マイクロソフト・インテルなどでも同様のチェッカーがあります

STEP

07

インターネット（SNS等）でのトラブル回避対策

SNS等の普及により個人から情報を発信する機会が増えています。
同時に、個人の不用意な書き込み等により、他の利用者から集中的に非難を浴びるなど、SNS上のトラブルも起きています。
その結果、他の組織や個人から損害賠償を請求されてしまうことがあります。
インターネットでのトラブル回避対策として、次の対応をお願いします。

- SNS等へ書き込みする際は、**常識的かつ適切なマナーを守る**
- **書き込んだ個人を特定することは容易にできる**ことを認識し、違法な行為や反社会的な情報を書き込まない
- 不特定多数の人が閲覧するSNSに写真を投稿する場合には、撮影した位置が特定できる**ジオタグ**が埋め込まれていないか注意しましょう。
- 不用意に個人情報を書き込まない
- 一度発信したものを**完全に消去することはできない**のだということをよく理解しましょう。
  - 場合によっては損害賠償が生じるケースもあります。

SNSの利用・・・

アルバイト店員が業務中の様子を撮影した不適切動画がSNSで拡散され、企業に莫大な被害をもたらす「バイトテロ」と呼ばれる行為が頻発しています。
本人たちにとっては軽い悪ふざけくらいの気持ちでも、企業にとってはブランドイメージを汚す重大なインシデントです。
投稿者たちのその後は次のとおりです

- **匿名投稿であると甘く考えていた**
- **身元をすぐに特定されてしまい、誹謗や中傷を浴び続けている**
- **刑事事件として処罰の対象になり、損害を賠償しなくてはならない**

いくら反省しても信頼を取り戻すことはできません。結果を考えて行動しましょう。

STEP

08

オンラインサービス等での不正使用の防止

オンラインサービス（ニュースの配信・データベースの検索など）は、利用しやすくとても便利です。学内でも図書館などで、教職員や学生の皆さんが自由に閲覧できるようにオンラインサービスを提供していますが、個人が不正に利用してしまうと、大学全体に対するサービスが停止される可能性があります。
オンラインサービスでのトラブル回避対策として、次の対応をお願いします。

- SNSをはじめとするオンラインサービスを利用する際には、事前に利用規約を把握して、それを遵守する
- 電子ジャーナルやデータベース閲覧サービスにおいて、コンピュータプログラムなどを利用して一度に大量のコンテンツをダウンロードしない
  - 「自由に使用してよい」と言われているサービスでも、上智大学とサービス提供元との間で利用条件が定められています。利用規約を守らない利用者のためにサービス全体が停止される場合があるので注意してください
- 他人のアカウントを借りてサービスを利用しない、または自分のアカウントを他人に貸与しない
- オンラインサービスは、常識的かつ適切なマナーを持って利用する

上智大学オンラインサービスの一例

□ 上智大学図書館e-Resouces Access Page

電子ジャーナル・電子ブックのタイトル検索を行います。

上智大学図書館 SOPHIA UNIVERSITY LIBRARY e-Resources Access Page

□ 上智大学学術情報リポジトリ

本学の学術研究成果及び教育成果を収集・蓄積・保存し、広く公開することを目的としたシステムです。

STEP

09

不要になったパソコン等の廃棄に関する手続き

不要になったパソコン等を廃棄したり、他人へ譲渡する場合に、搭載されるハードディスク等のメディアから情報が漏洩する可能性があります。

不要になったパソコン等の廃棄に関する手続きとして、以下のいずれかの対応をお願いします。

- データ消去用のソフトウェアを利用（あるいは、データ消去の専門業者に依頼）し、**データを消去**する
- パソコン等に搭載されるハードディスク等を取り外し、**物理的に破壊**する
- 個人データが記録された媒体(CD-ROM・書類など)を廃棄するときは、シュレッダーなどで物理的に破壊する
- スマートフォンを処分する際には、個人データ（連絡先・写真など）を消去するなど**慎重に処分**する
  - 安易に回収業者に引き渡すと、そこから個人情報が流出してしまう恐れがあります。
- スマートフォンは紛失しやすいので、**落としたらすぐにロックをかける**ことができるような対策を取っておく

ソーシャルエンジニアリング・・・

ソーシャルエンジニアリングとは、人間の心理的な隙や行動のミスにつけ込んで、ネットワークに侵入するために必要となるパスワードなどの重要な情報を、情報通信技術を使用せずに盗み出す方法です。

＜手口と対策＞

■ ごみ箱漁り（トラッシング）
回収業者として目標とする企業からゴミを持ち去る

■ のぞき見（ショルダーハッキングなど）
パスワードなどの重要な情報を入力しているところを後ろから近づいて（電車の中も注意）、覗き見る。IDやパスワードが書かれた紙（付箋紙など）を瞬間的に見て暗記する。

情報セキュリティに関する情報

セキュリティ最新情報の提供
独立行政法人情報処理推進機構
（https://www.ipa.go.jp/security/personal/）

セキュリティ注意喚起情報の提供
JPCERTコーディネーションセンター
（https://www.jpcert.or.jp/）

著作権に関する情報の提供
公益社団法人著作権情報センター
（http://www.cric.or.jp/）

情報セキュリティに関する学内の規程及び資料

・上智学院情報セキュリティ基本方針
・上智学院情報システムセキュリティ規程
（https://kitei.cl.sophia.ac.jp/doc/suallstaffs/listall.html#）

各種システム等の利用ガイド
上智大学情報システム室（総合メディアセンター）利用ガイド
（https://ccweb.cc.sophia.ac.jp/userguide/）

情報セキュリティ事故等が発生した場合

「サークルの名簿が入っている媒体を紛失した」や「使用しているパソコンがコンピュータウイルスに感染した」等、情報セキュリティ事故等が発生した、あるいは発生した可能性がある場合、速やかに『学生センター』または『情報システム室（総合メディアセンター）』へご連絡ください。

事故・トラブルの相談
部署名：学生センター
連絡先：03-3238-3525

ウイルス感染などの技術的なお問い合わせ
部署名：情報システム室
連絡先：03-3238-3101

出典

◘総務省『国民のための情報セキュリティサイト』
（http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/index.html）
◘独立行政法人情報処理機構セキュリティセンター（IPA）『企業（組織）における最低限の情報セキュリティ対策のしおり＋１』
（https://www.ipa.go.jp/security/keihatsu/shiori/management/01_guidebook.pdf）