上智学院
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

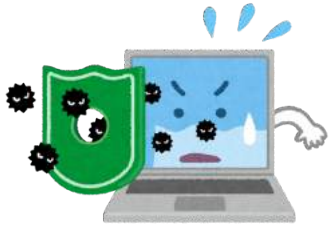
情報セキュリティ対策　18の取り組み

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. 無線LANのセキュリティ対策
4. ソフトウェア等（ファイル共有ソフト等）の利用に関する対策
5. パスワード管理
6. 重要情報へのアクセス管理
7. 標的型攻撃メールへの対策
8. 電子メールの誤送信対策
9. 電子メールからの情報漏洩対策
10. インターネット（SNS等）でのトラブル回避対策
11. オンラインサービス等での不正使用の防止
12. 重要情報のバックアップ対策
13. 重要機器の管理
14. 重要情報の物理的管理
15. 重要情報の持ち出し管理
16. 不要になったパソコン等の廃棄に関する手続き
17. ソフトウェア等の適正な管理
18. サーバ室の管理

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。

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。
- Windows7のサポートは、2020年1月までです。

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。

それ以外の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。

PC等に標準で**ファイアウォールの機能**が実装されている場合は、適切な設定をする

ファイアウォール（防火壁）とは、お使いのPC側のネットワークとインターネットの間で通信を制御する機能です。

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

  （情報システム室にて配布しています：
  https://ccweb.cc.sophia.ac.jp/userguide/service/sv_01/）

- 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

- ウイルス感染による、学内外の被害**事例を確認**する

- **セキュリティ講習会**を定期的に受講する

  どのようなウイルスが流行しているのか、どのような経路で感染するのか、情報システム室の担当者がご説明します。

- 許可されていない、または持ち主の分からない記憶媒体を使用しない

- 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

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：**Sophia Wi-Fi，eduroam**

- 研究室内などに自前で無線LAN環境を構築する場合は、WPA2パーソナル (AES)あるいはMacアドレス認証を使用してください。

- 公衆無線LANは安全性が保障できないので業務や研究では使わない

無線LANの危険性・・・

ホテル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

04

ソフトウェア等（ファイル共有ソフト等）の利用に関する対策

ファイル共有ソフト等の利用により、ウイルスに感染する危険性があります。また、ウイルスの感染により、パソコン等に保存していた研究・授業等の情報や個人情報がネットワーク上に流出する危険性があります。

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。

- **不特定多数の人に配信することが目的のファイル共有ソフト**は使用しない
- **正規のルートで購入**したソフトウェアのみを利用する
- 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

ファイル共有ソフトとは・・・

ファイル共有ソフトとは、インターネット上で不特定多数の利用者とファイルを共有するためのソフトウェアのことです。日本では『Winny』に代表される多くのファイル共有ソフトが存在しましたが、そこで共有されるデータは、著作権違反のデータ（音楽、映画、テレビ番組、ゲームソフトなど）が多く、社会問題となりました。現在ではファイル共有ソフトをターゲットにしたウイルスにより、企業や組織の機密情報がインターネット上に漏洩してしまうという事件が数多く発生しています。ファイル共有ソフトは可能な限り使わないことが望ましいです。

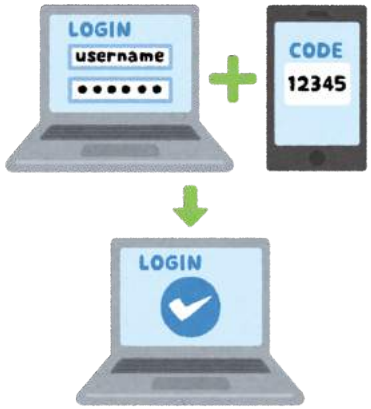
本学ではSophiaメールを使用していますので、Office365で提供されている**OneDrive**を推奨しています。

□ **OneDrive**の利用方法：
https://ccweb.cc.sophia.ac.jp/documents/#_217

STEP

05

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。

- 名前、生年月日等の個人情報は使用しない
- 英数字を含む8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
- パスワードを紙に記載して、ディスプレイ等に貼らない
- 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・・・

1.数字などの入った適当な言葉を考えます

例）「水曜18時はヨガの日」

2.すべてアルファベットにします

「suiyou18jihayoganohi」

3.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

「sy18jihyoganhi」

4.大文字小文字、i＝!・O＝０・a=@などの記号に置き換えたりします

「Sy18J!_h@Y0ganH!」　完成！

STEP

06

重要情報へのアクセス管理

ネットワークを介して接続された機器に保存される情報が、インターネット（学外）から閲覧できてしまう状況が問題となっています。
インターネットを介して情報漏洩を起こしたり、接続機器の不正利用によるサイバー攻撃に加担してしまう場合もあります。
重要情報へのアクセス管理として、次の対応をお願いします。

- 研究室内等で共有機器を使用する場合、必要な人のみアクセスできるようにする
- 同じID・パスワード等を共有しない
- 初期パスワード・設定のまま使用しない

セキュリティ対策を怠ると・・・

＜踏み台＞

他人のコンピュータに侵入するときに、直接自分のコンピュータから接続すると、接続元のIPアドレスによって、犯人が特定されてしまう可能性があります。そこで、犯人が自分のコンピュータを探しにくくするために、目的のコンピュータに接続するまでに、いくつかのコンピュータを経由させようとします。これら中継地点としてのみ利用されるコンピュータのことを踏み台と言い、自分でも気付かないうちに加害者にされてしまうことがあります。

＜ネットワーク上のプリンタ複合機＞

業務用のプリンタ複合機では、機器内にプリントアウトされた情報やスキャンされた情報、FAXのデータなどが残されています。送信者やファイルの場所など、データの送受信情報が全て確認できるようになっています。複合機のパスワードを初期値で使い続けたり、ファームウェアを古いままにしておいたりすると、それらの情報がインターネット上から閲覧されてしまう危険性があります。

STEP

07

標的型攻撃メールへの対策

特定の企業や組織を狙った標的型攻撃メールにより、重要な情報が盗まれる事件が頻繁に発生しています。
標的型攻撃メールとは、組織の担当者が業務に関係する電子メールだと信じて開封してしまうように巧妙に作り込まれたウイルス付きの電子メールのことです。
標的型攻撃メールへの対策として、次の対応をお願いします。

- 電子メールの添付ファイルを安易に開封したり、電子メール本文中のURLを不用意にクリックしたりしない
- 標的型攻撃メールに関連する被害事例を確認する
- セキュリティ講習会を定期的に受講する

標的型攻撃メールに注意

不審なメールに注意しましょう！

- ☐ 予定や約束がないのに、会議や請求書などのタイトルでファイルが添付されてくる
- ☐ 本文が公的な内容であるのに、差出人がフリーメール
- ☐ 添付ファイルがexe形式、あるいはZIP（圧縮）内にあるexe形式であるにもかかわらず、ファイルアイコンがWordやExcel、PDFなどである
- ☐ 文章中にリンクがあり、別のサイトに誘導される

不審な電子メールの添付ファイルの開封、電子メール本文中のURLをクリックしてしまった場合、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。

連絡先：内線＜3101＞or＜4473＞

STEP

08

電子メールの誤送信対策

電子メール送信する際に、宛先アドレスの間違いやメールアドレスの表示方法（「To」「Cc」「Bcc」）の誤操作等による情報漏洩が頻繁に発生しています。
電子メールの誤送信対策として、以下の対応をお願いします。

- メールを送信する前にメールアドレスの再確認を行う
- 「To」「Cc」「Bcc」の使い分けに注意する
- 多くの宛先に電子メール送信する際は、本学が用意するML（メーリングリスト）などを使用すること（宛先、間違えによる誤送信を予防するため）
- 電子メールソフト（Outlook等）の機能でメール送信前に確認を促す「確認ダイアログ」を利用する

一斉メールを送信する時には・・・

同じ内容のメールをたくさんの人に送りたいときには、
宛先を自分のアドレスにし、送り先のアドレスは「Bcc」に記載して送るようにしましょう。
宛先（To）に記載されたアドレスは、各宛先の全員に見えてしまいます。全員が知り合いならばよいのですが、見知らぬ人のアドレスを安易に知ることができてしまうので危険です。送信先の全てのアドレスを「To」に入力することは避けましょう。

宛先:	taro_jochi@sophia.ac.jp,
Cc:	
Bcc:	jiro_kioi@gmail.com, hanako_sophia@yahoo.co.jp,
件名:	一斉メール：懇親会について

STEP

09

電子メールからの情報漏洩対策

個人情報等を含んだ添付ファイル付きの電子メールの誤送信等により、情報漏洩等の事故が発生しています。
電子メールからの情報漏洩対策として、以下の対応をお願いします。

- あるいは、**本学が推奨するファイル転送サービス**を利用する
- 添付ファイルを送付する際は、**ファイルを暗号化（パスワード付き）**する
- 暗号化に使用した**パスワードは、ファイルを添付した電子メールに記載しない**（電話等でパスワードを伝達する）

ファイル転送サービス・・・

メールでファイルを添付する場合には、その容量に制限があります（学内ではメール自体も含めて10MB以内）。大容量または大量のデータやファイルを送信・受信する際に、一般的には「ファイル転送サービス」を利用します。
アップロードやダウンロード時に特別な操作がいらないWebブラウザベースが特徴で、無料のもの(広告が入る)と、企業向けにセキュリティなどを強化した有料サービスがあります。
学内で利用する際には、**無料サービスの「宅ファイル便」や「データ便」などで機密ファイルを送付するのは、極力避けて**ください。
暗号化対応のUSBメモリなどで直接的なやり取りを行うか、**ソフィアメール(Office365)のOneDrive**を使用し、公開範囲を厳密に設定した上で、リンクのみを先方に送信する方法をお勧めします。

STEP

10

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。
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な非難を浴びる現状が起きています。
その結果、他の組織や個人から損害賠償を請求されることもあります。
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
- 不用意に個人情報を書き込まない

SNSの利用・・・

業務でSNSを使用した情報発信を行う場合には、組織の情報セキュリティポリシーに従い、以下のようなことに注意をしましょう。

- ☐ 企業や組織のブランドイメージを損なう発言をしない。
- ☐ 第三者にアカウントを乗っ取られないよう、アカウント情報(IDやパスワードなど)の適切な管理を行う。
- ☐ 利用するサービスの規約を遵守する。
- ☐ メンテナンスなどで、サービスが利用できない場合の運用を決めておく。

STEP

11

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 12

重要情報のバックアップ対策

パソコンや記憶媒体等の故障や誤操作、ウイルス感染等により保存した情報（データ）が消失する可能性があります。
重要情報のバックアップ対策として、以下の対応をお願いします。

▶▶ 重要情報をファイルサーバ、外付けハードディスク等に定期的にバックアップする

ランサムウェアの脅威・・・

ランサムウェアは、ユーザーのPCに侵入することでPCをロック、またはデータを暗号化し、秘密裏に目的を遂行すると姿を現し「解除鍵が欲しければ」と金銭を要求する身代金要求型の不正プログラムです。主に、標的型攻撃メールや不正サイトへのアクセスで感染しますが、いざというときのために、最新のバックアップをとっておくようにしましょう。

STEP 13

重要機器の管理

研究等で使用するパソコン（タブレット等を含む）等には、研究に関する情報や個人情報が記録されている場合があります。それらのパソコン等の盗難は情報漏洩につながります。
重要機器の管理として、以下の対応をお願いします。

▶▶ 研究終了後は、パソコン等を鍵のかかるロッカー等に保管する

▶▶ パソコン等の**本体**にデータを保管しない

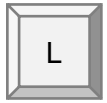
- 重要なデータをパソコン本体に保存しなければ、被害も最小限に抑えられます。

STEP

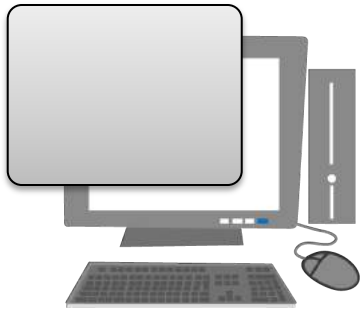
14

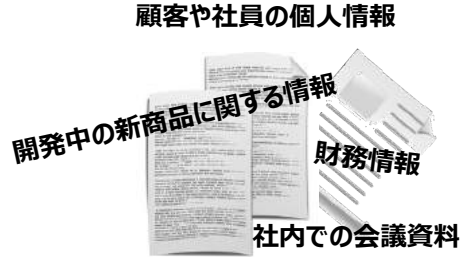
重要情報の物理的管理

パソコン（タブレット等を含む）が盗まれることにより、格納された重要情報（学生の個人情報等）が漏洩する可能性があります。
また、パソコン等の画面を開いた状態で離席すると画面上に表示される情報が第三者に閲覧できる状態となるため、情報漏洩につながります。
重要情報の物理的管理として、以下の対応をお願いします。

- パソコン（タブレット等）・記憶媒体（USB等）及び重要情報の記載がある書類等を自席や教室等に放置しない
- 離席時にはパソコン等に鍵（画面ロック等）をかける
  - 画面ロック：【Windows】キー  ＋【L】 
  - デスクトップ表示：【Windows】キー  ＋【D】 
- 個人情報・機密情報が記載されたドキュメントを、人目につく場所に置いたまま帰らない。（特に重要なものについては、キャビネットで施錠管理する）

覗き見防止用のフィルムを貼るという手段もあります！





STEP

15

重要情報の持ち出し管理

学内からの安易な情報の持ち出しは、情報漏洩事故を引き起こす大きな要因となります。
情報を持ち出すことで、学外で置き忘れ（紛失）、盗難等により情報漏洩につながります。
重要情報の持ち出し管理として、以下の対応をお願いします。

個人情報の持ち出しは原則禁止とする

万が一の盗難・紛失に備えて、重要な情報は持ち出さないようにしましょう。
やむを得ず持ち出した場合は、**【媒体からは絶対に目を離さない】【網棚などに置かない】【飲み会などの酒宴に参加しない】**を厳守してください。

持ち出しをする場合、暗号化対応のUSBメモリ等を使用する

持ち運びに便利なUSBメモリですが情報漏洩のリスクとは隣り合わせです。
セキュリティ対応のUSBメモリは次の様な機能があり安全です。
・パスワードを入力しないと使用できないのでデータを見られることがない
・自動でウイルスチェックが実行されるのでウイルス感染を防ぐことができる

本学が承認するクラウドサービスの利用により物理的な持ち出しを回避する

本学では、学内のサーバ上でOSやソフトウェア、データを集中管理し、職員側は入力・表示などの最低限の機能に絞った**シンクライアント端末**を利用しています。このような業務形態は、**端末内に重要な情報が保存されず**、外出先での端末利用に関する情報セキュリティ対策としても有効です。

PCやUSBメモリ等に、過去に持ち出した不要な個人情報が入っていないか定期的に確認する

※個人情報の持ち出しとは以下のような行為です
「個人情報を収めたパソコン等の機器又はUSB等のメディアを持ち出す。」
「個人情報が記載された紙媒体を学外に持ち出す。」

STEP

16

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
  - 情報システム室で貸し出していますので、ご活用ください
- 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

情報システム室では、情報機器（PC, サーバなど）の安全な廃棄のサービスを始めました。
学生個人情報などの重要なデータを記録した機器を廃棄する場合は、情報システム室でお預かりして一括廃棄いたしますのでご相談ください。

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。
たとえばこんな手口があります

■ 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
対策：オフィスへの入退管理を強化して、正当な用件のない部外者を社内へ不正に侵入させない。資料の廃棄を徹底する。

STEP

17

ソフトウェア等の適正な管理

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。
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。

- ソフトウェアライセンスの内容（使用権等）を確認する
- ソフトウェアを不正にコピーしない
- 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

無料版Officeの利用について・・・

上智大学、上智大学短期大学部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、マイクロソフトからOfficeをダウンロードして、無料で使用することができます。

- ソフィアメールのアカウントを持つ、上智大学／上智社会福祉専門学校の教職員および学生が対象です。
- 卒業、退学、離籍と同時に使用できなくなります。
- 自宅のPCを含め、ひとり5台までインストールすることができます。

※ 詳細は：URL
https://ccweb.cc.sophia.ac.jp/userguide/service/sv_11/

STEP

18

サーバ室の管理

研究等で使用するサーバ等を設置する際は、情報セキュリティ上（部屋の施錠ができる）の問題がない場所であるかどうか確認する必要があります。
多くの人が出入りする場所では、盗難や直接サーバを操作される恐れが高まり、情報を盗み取られる可能性があります。
サーバ室の管理として、以下の対応をお願いします。

- サーバ等を設置する部屋は施錠管理を行う
- サーバ等を設置する部屋の入退室を入退室管理票等で管理する

入退室管理によるセキュリティ対策

- オフィスの施錠管理を行う
- 入退室の履歴を記録に残す（台帳記入など）
- 身分証を発行し、従業員に携帯させる
- 出入りが激しい場所については、不審者がいないかどうかを常に留意する

- セキュリティカードなどで出入り口の制限を行う
- 出入り口に守衛を配置したり、監視カメラを設置したりする
- バイオメトリクス（生体認証）など、より強固なシステムを導入する

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

「パソコンやUSBメモリ等の媒体を紛失した」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『総務局総務グループ』・『学術情報局情報システム室（総合メディアセンター）』へご連絡ください。

パソコンやUSBメモリなどの紛失
部署名：総務グループ
連絡先：03-3238-3172　内線：3172

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　内線　3101 or 4473

個人情報が記録されたパソコンを廃棄される場合

情報システム室では、情報機器（PC，サーバなど）の安全な廃棄のサービスを始めました。
学生個人情報などの重要なデータを記録した機器を廃棄する場合は、情報システム室でお預かりして一括廃棄いたしますのでご相談ください。

部署名：情報システム室
連絡先：03-3238-3101　内線　3101 or 4473

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）