情報倫理と情報セキュリティ

■ 情報倫理とは、

ネット社会での適正な考え方、ルールやマナーを守った適切な行動の規範のことです。

さらに、順守しなければならないインターネットに関係する規約、ガイドライン、法律もありますので注意してください。

■情報セキュリティとは、

インターネットを利用する際に注意する危機管理（リスクマネージメント）対策のことです。

自分が被害者になる場合だけでなく、犯罪者に利用されることにより、意図せず加害者になってしまうケースもあるので、適切な対策と対応が重要です。

一人ひとりがサイバーセキュリティを担うことで、
安心・安全なネット社会を作ることができます

＊サイバーとは、コンピューターやそのネットワークに関する意味の造語です。

■Contents■

主な出典

1. 情報を発信する際の注意 ：個人情報保護法
   - 1-1. 自分や知人の個人情報を安易に公開しない
   - 1-2. 相手が不快に思うような発言はしない

警視庁

2. 情報を利用する際の注意 ：著作権法
   - 2-1. 著作権・肖像権に注意する

文化庁

3. セキュリティ対策
   - 3-1. 自分の機器（PCやスマートフォン）に対する対策
   - 3-2. ネットワークに対する対策
   - 3-3. ネット情報に対する対応

総務省

はじめに　■本学における規則・注意事項など■　※必ずお読みください

▼PCとネットワークにおける規則や手引き

※情報センターHP掲載事項

- 明治学院大学情報ネットワーク規程
- 明治学院大学情報ネットワーク研究・教育利用細則
- ネットワーク説明と情報センター利用案内（動画）
- 明治学院大学コンピュータ・ネットワーク 利用の手引き

▼ソーシャルメディアに関する注意事項

※「ソーシャルメディアについて」HP掲載事項

- ソーシャルメディアの利用に関するガイドライン（勤務員・学生等）
- ソーシャルメディアアカウント利用要綱
- 明学生が考えた５つの合言葉

・本ガイドラインに関するお問い合わせ：広報課
・SNS等で、トラブルに巻き込まれたら：学生部

明学生が考えた SNSのための５つの合言葉　～再考で最高のSNSライフに～

みんな見てる、
オレのプライベート!?

友だちは、
フリー素材じゃ
ありません。

みんな！ オレの
勇姿を見てくれ！

その個性の出し方、
間違っていませんか？

騙されるわけないじゃん。
もう大学生だぜ？

デマの中継所に
ならないでっ！

起きて『既読』、お昼『なう』、
寝る前『いいね！』、
それが私の日常

昨日、SNSで
何を見たか、
思い出せますか？

ちょっと見るだけだから
だいじょうぶ！

歩きスマホは、
歩く武器。

(2014年度学生広報委員制作)

1．情報を発信する際の注意

1-1. 自分や知人の個人情報を安易に公開しない

※警視庁「情報セキュリティ広場」より

1-2. 相手が不快に思うような発言はしない

- ネット上で、円滑な活動を行うには、現実社会と同じマナーを守ることが大切です。
- ネット上に情報を公開するときに、それによって生じるリスク・法的責任を負うことは、現実社会以上に深刻になる場合があります。 安易な情報発信が、他人に不快な思いをさせたり、思わぬところで被害者や加害者になってしまうおそれがあるので、慎重な情報発信を心がけてください。

- SNS
- メッセージ
- メール
- 投稿

など

■インターネット送信の７か条

1. インターネット社会でも、実生活と同じルールとマナーを守る
2. 住所・氏名などの個人情報を入力する時は、十分注意する
3. ID・パスワードの管理を徹底する
4. 他人のプライバシーを尊重する
5. 誹謗中傷をしたり、ミスを大げさに指摘しない
6. メールを送る前に、内容をよく確認する
7. 面と向かって言えないことは書かない

１．情報を発信する際の注意

■個人情報とは、

※個人情報保護委員会HPより

氏名、顔写真、住所、生年月日、家族構成など、単一およびそれらの組み合わせにより【個人を特定できる情報】のことです。

■個人情報保護法の５つの基本チェック

① **取得** → **無断で取得しない**

・利用目的を特定して、本人にわかるように取得してください

② **利用** → **流用しない**

・取得時に特定した利用目的の範囲内でのみ利用してください

③ **保管** → **紛失しない、漏洩しない**

・USBメモリーに入れたデータなど、紛失しないように安全に管理してください

・クラウドに保管する際には、パスワードをかけ、公開条件に注意してください

④ **提供** → **他人に提供しない**

・第三者に提供する場合は、本人の了解を得てから提供してください

⑤ **対応** → **要求に対応**

・本人からの開示・訂正・利用停止等の申し出があった際は、迅速に対応してください

2．情報を利用する際の注意

※著作権相談センターHPより

2-1. 著作権、肖像権に注意し、ルールを守って使用する

●ネット上に公開されている文章や画像を、そのままコピーして自分のレポートに利用すると、【**著作権法**】に抵触するおそれがあります。※１参照

レポート等に引用する際には、出典を明記するなどのルールを守ってください。

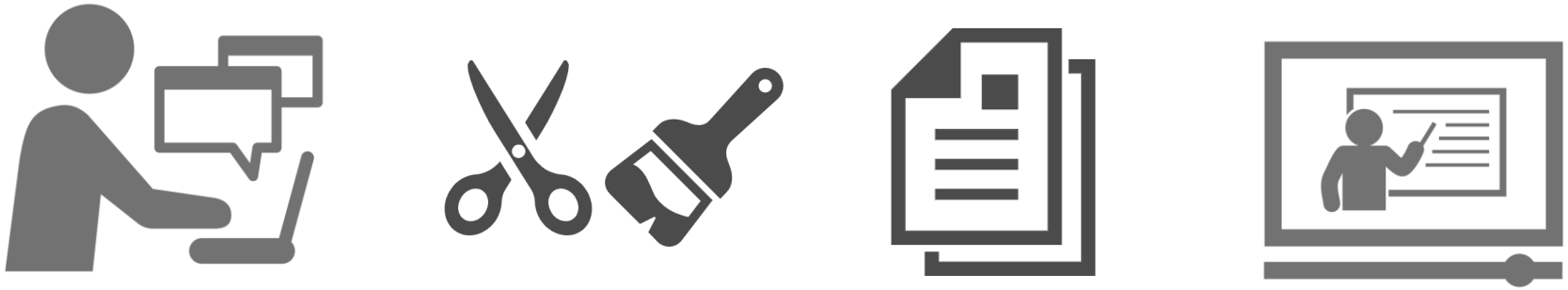
●【**違法にアップロードされたコンテンツを違法と知りながらダウンロードすること**】 も違法行為です。※２参照

●インターネット経由でコンテンツを共有する際にもルールがあります。

ただし、授業でコンテンツを利用する際には、 特例ルールがあります。 範囲内でご利用ください。 ※３参照

●出版された著作物・配布物や、インターネット経由で取得した授業の動画や資料などにも著作権があります。

Webサイトにアップする、SNSに投稿する、友人にコピーを譲渡するなど、不適切な再配布をしないよう注意してください。



2．情報を利用する際の注意

■著作権とは、

※著作権相談センターHPより

作品を創作した者が有する権利で、**知的財産権**の一種です。

■著作権に関する情報

詳細は、下記の【文化庁ホームページ】よりご確認ください。

※1「著作権」

※2 著作権法改正（2021/1/1）

インターネット上に違法に掲載された著作物のダウンロード規制の対象が、今までの「音楽・映像」から「全ての著作物（漫画、小説、写真、論文など）」に拡大されました。

※3「学校における教育活動と著作権」パンフレット

「著作権なるほど質問箱」教育機関における利用について

「著作権テキスト」

3．セキュリティ対策

■情報セキュリティとは、

※【内閣サイバーセキュリティセンター】 HPより

パソコンやスマートフォンに保存された情報が、盗まれてしまったり、勝手に変更されてしまうことで、自分や関係者が犯罪や被害にあうことがあります。

また、ウィルスに感染した自分のパソコンが犯罪者に乗っ取られ、第三者への攻撃の中継点とされて、自分が加害者になってしまうといったケースも多発しています。

知識を身に着け適切な防止措置をとることによって、パソコンやスマートフォンを快適で便利にすることができます。

【インターネットの安全・安心ハンドブック】全体版
（PDF:23MB）
英語版English version（2017）

■基本のポイント

3-1. 自分の機器に対する対策

システムを最新に保つ。 セキュリティソフトを入れて防ぐ

3-2. ネットワークに対する対策

複雑なパスワードと多要素認証で侵入されにくくする

3-3. ネット情報に対する対応

攻撃をうけつけない。 最新の情報をチェックする。

3．セキュリティ対策

3-1．自分の機器（PCやスマートフォン）に対する対策

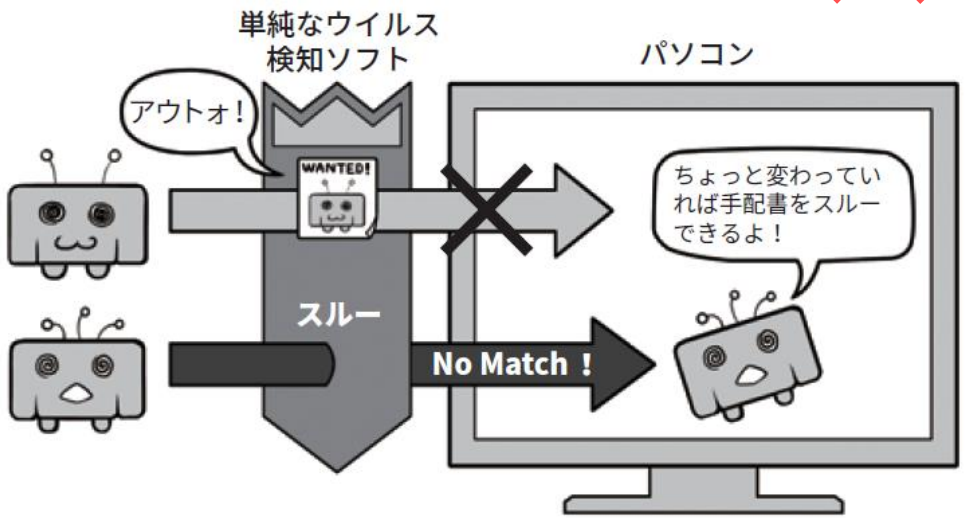
本学では、セキュリティソフト「ESET」を提供しています。　詳しくは、こちらから

3-1-1．セキュリティソフトを導入する

- ●総合セキュリティソフトをインストールする
- ●「ウィルス定義ファイル」を常に更新する

単純なウィルス検知ソフト

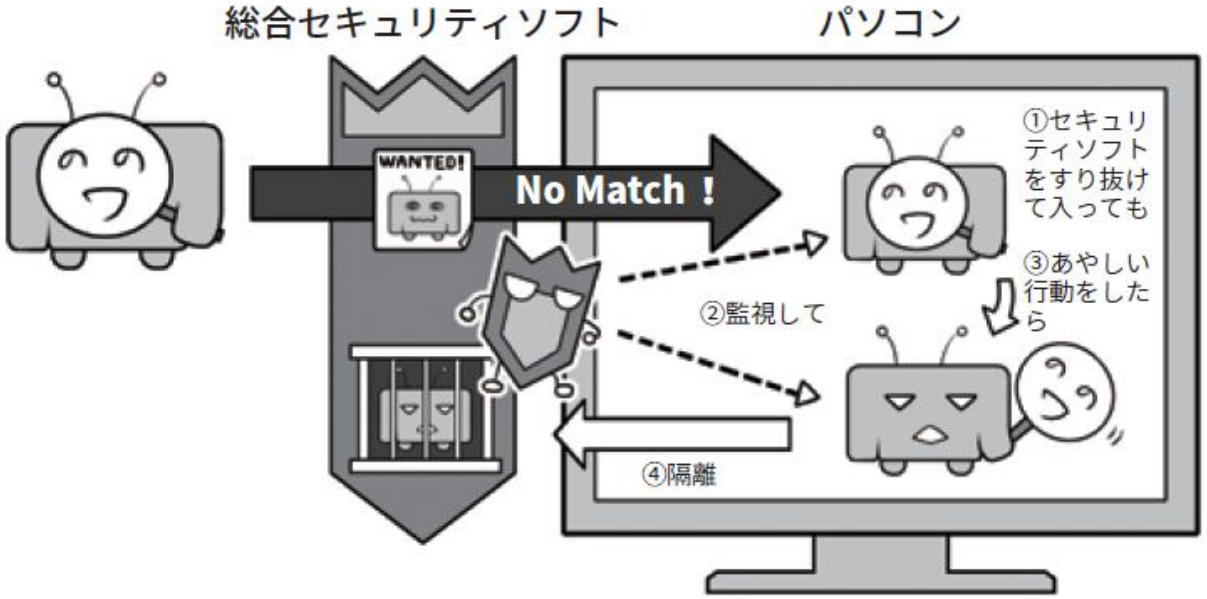
「定義ファイル」が古いとすり抜けてしまう



総合セキュリティソフト

・「定義ファイル」認識

・「ふるまい検知」、「ヒューリスティック分析」機能あり



3．セキュリティ対策

3-1-2. 環境を最新に保つ（アップデート）

●**パソコン環境**

①パソコン本体（OS、ドライバーなど）
②各種アプリ（Microsoft Office、Zoomなど）
②セキュリティソフト、ウイルス定義ファイル

●**スマホやネットワーク機器**

3-1-3. 安全なアプリを使用する

●**原則「公式ストア」からダウンロード**

●**「権限」＊に注意**

＊カメラや写真、住所録への「アクセス許可を要求」すること

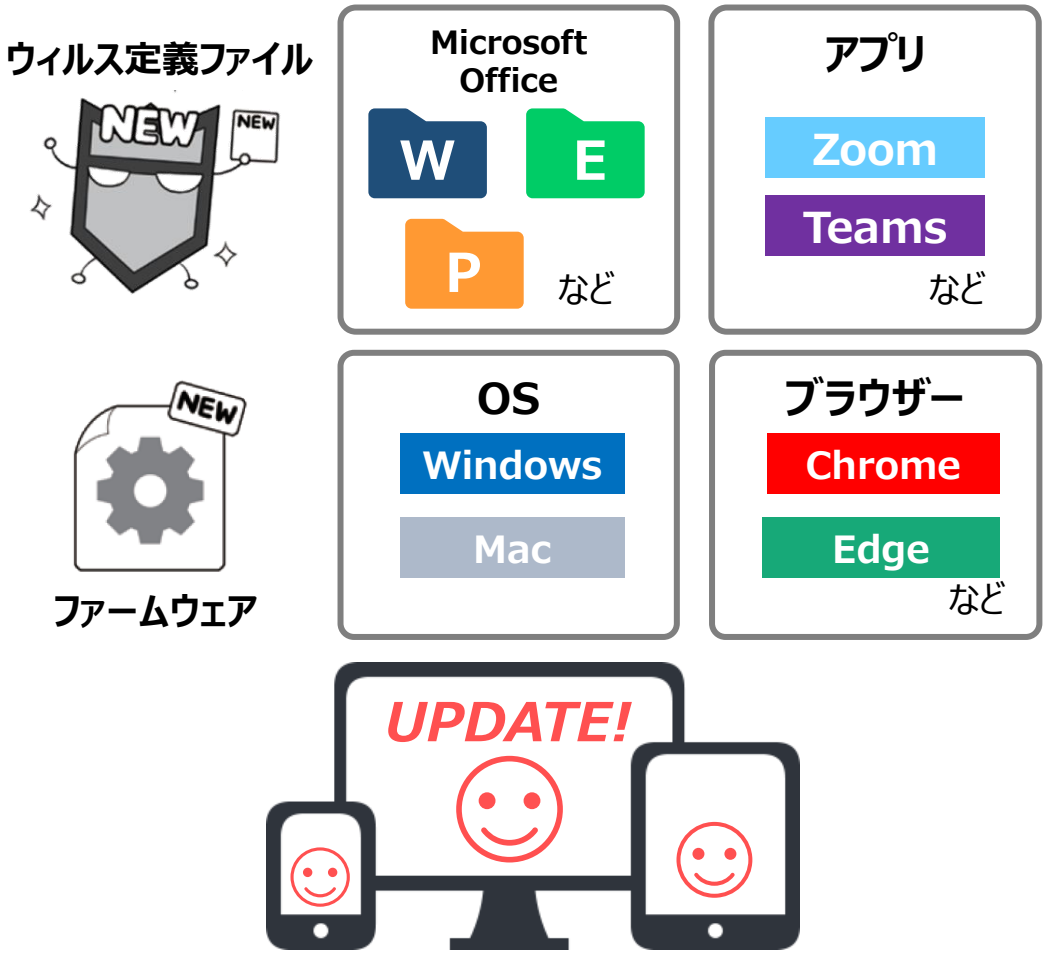
●**使わないアプリは削除**

3-1-4. ネットワーク設定を使い分ける

●**プライベートネットワーク**　：自宅または勤務先など

●**公衆ネットワーク**　：カフェの Wi-Fi など

・自分のPCは、ネットワーク上の他のデバイスには表示されません。
・PCをプリンターやファイルの共有に使用できません。



自宅外では、「**公衆ネットワーク設定**」に！
Windows10の設定方法は、Microsoftのこちらのサイトから

3-2. ネットワークに対する対策

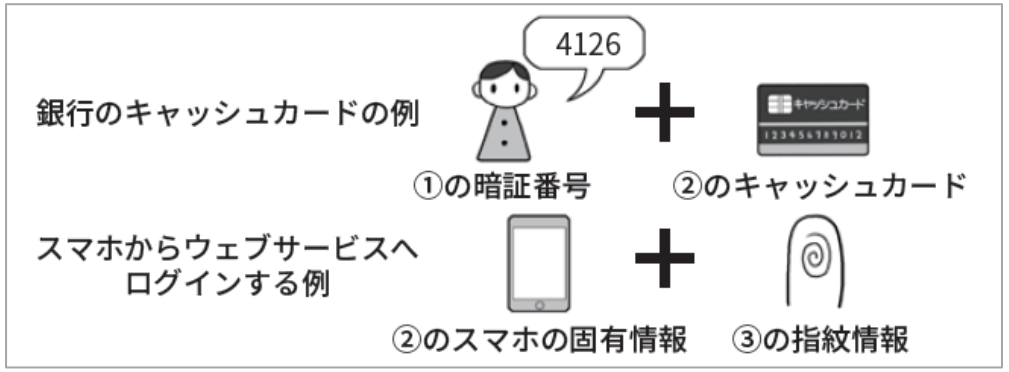
3-2-1. パスワードで侵入されにくくする

●パスワードの安全性を高める
推奨 ：英字(大文字＋小文字) ＋数字＋記号で10桁以上

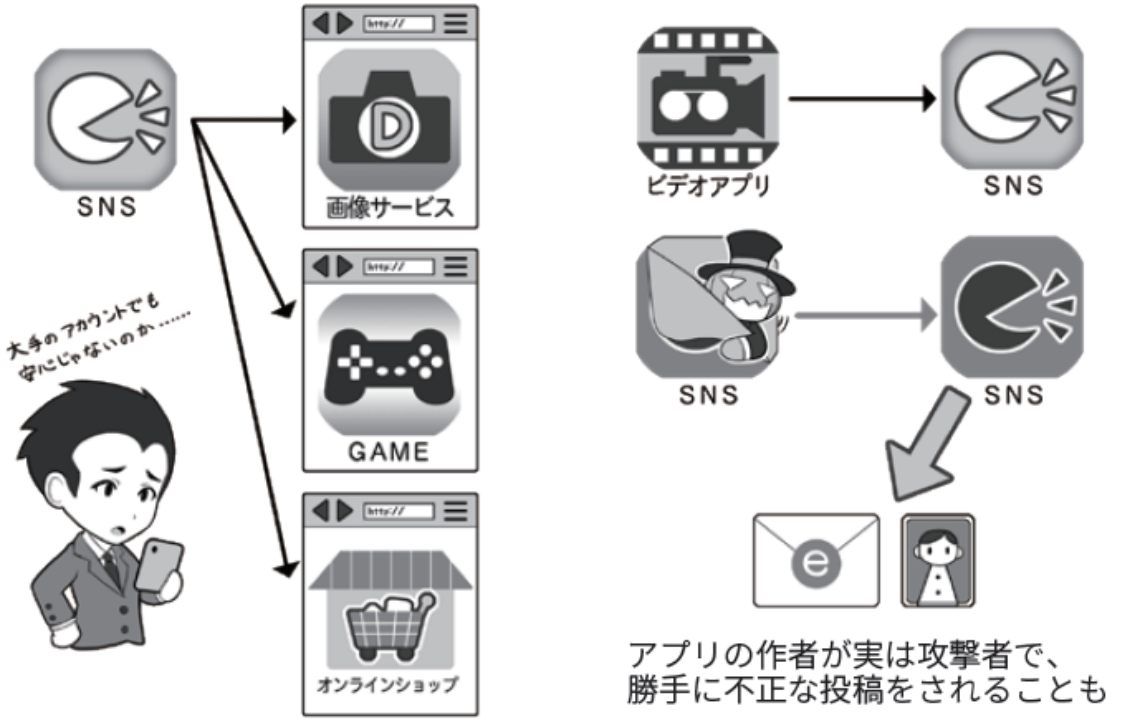
●パスワードの使い回しをしない
それぞれのサービスに別のパスワードを設定する

●適切に保管する
推奨 ：スマホ用パスワード管理アプリ、紙のノート、USBキー
NG ：クラウド上、ウェブブラウザーに保存

●多要素認証を使う
「知っていること」「持っているもの」「生体認証」の組み合わせ



ソーシャルログインとサービス・アプリ連携の違い



ソーシャルログインは、堅牢なサービスのアカウントを別のサービスの鍵に使え便利ですが、大本のアカウントの認証情報が漏れる事案が発生したため、それぞれのサービスに別々のパスワードを使用する基本対応を推奨します。

3-2-2. ネットワークを安全に使う

●通信の暗号化とは、
盗聴や漏洩により解読されないために、通信に暗号化を行います。

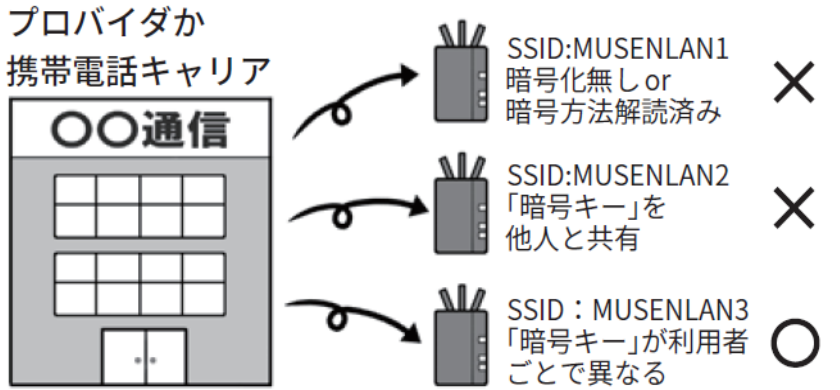
●家庭では、セキュリティの高い暗号を使う無線LANを選ぶ
暗号化を伴う無線LANの構成要素
①SSID（アクセスポイント名）
②暗号化方式
③暗号キー（パスワード）
安全な暗号化方式を選択して、「暗号キー」は非公開にして使用します。

●公衆無線LAN（Wi-Fi）の安全性を確認する
信頼している公衆無線LANが安全とは限りません。
「暗号キー」共有のWi-Fiは危険です。

●公衆無線LANサービスの例

①政府・自治体	：税金を払っている（実際には有料）
②通信会社	：契約の収益から払っている（追加料金無料）
③有料無線LAN	：料金を払っている（有料）
④善意のサービス	：無料なので責任能力なし

公衆無線LANが安全とは限らない



「暗号キー」共有は接続しない

●暗号化方式が安全でも、「暗号キー」を他人と共用するものは、すべて危険です。

●接続するときは、暗号化されたサイトやアプリのみの使用をお勧めします。

・インターネット ：「https://」で始まるサイトのみ
・メール ：「SSL/TLS」を使った通信設定
・スマホアプリ ：Letter Sealing機能でのトークなど

3．セキュリティ対策

暗号化方式の比較

接続	Android	iOS、mac OS	Windows
×（暗号化無し）			
△（暗号化有り）			 ＊1

●各種類の端末における「無線LANアクセスポイント」の表示例

かぎマークの意味は、暗号化の「あり/なし」を区別するだけで、「信頼できるアクセスポイント」という意味ではありません。

＊1：Windowsでは、「セキュリティ保護あり」と表示されるバージョンもあります。

●SIM認証（端末個別）の例

SSID名が、0001docomo、au_Wi-Fi2、0002softbankなど各携帯電話キャリア提供のものは、WPA2-EAPを採用しています。

暗号化の強度	暗号化の種類	特　徴
弱い	WEP	脆弱性で改ざんを検知できないため、利用は不可
やや強い	WPA	解読が難しい暗号化方式（AES）を使用したものの利用は可
強い	**WPA2**	認証、改ざんの検出などが強化されている 現在、主流
さらに強い	WPA3	今後普及 より強固なセキュリティ

安全性が確保されていないと思われるアクセスポイントに接続されている場合は、Wi-Fiの接続を切ることが推奨されます。

3-3. ネット情報に対する対応

3-3-1. 情報漏れを防ぐ

●ソーシャルエンジニアリング（心の隙をつく攻撃）に注意

カフェなどのテーブルにパソコンやスマホを開いたまま席を離れたりしないよう、また画面を背後から覗かれないような注意も必要です。

●写真に情報を付加しない

写真に位置情報を付加したり、個人情報が推測できる背景の「映り込み」などに注意が必要です。

3-3-2. 怪しいメールに注意する

●フィッシング詐欺メール

偽装サイトのリンクをクリックさせ、情報を入力させて個人情報を盗む詐欺のことです。本物のサイトに酷似している場合もあり、注意が必要です。

●ウィルス添付メール

ありがちなメールに偽装してウィルス付きのファイルが添付されてきた場合、ファイルをクリックするとウィルスに感染してしまう危険があります。不審な添付ファイルはクリックしないでください。

「**マルウェア**」（ウィルス）にパソコンが感染すると、「**DDoS攻撃**」をする「**踏み台**」とされる恐れがあります！　※用語は次ページ参照

怪しいメールとはなにか

①仕事のメールを装う

サイバー攻撃に使われる怪しいメールとは、まず「見ただけでは完結しない」メールです。リンクをクリックさせたり、添付ファイルを開かせたり、なにかをインストールさせようとしたりします。

②銀行、カード会社、オンラインショッピングサイト、プロバイダ関係を装うメール

また、自分が利用しているウェブサービスの名称で、緊急にどこかのウェブサイトを見させようとするのも、よく使われる手口です。

3．セキュリティ対策

3-3-3.　最新の情報をチェックする

Canon | ESET SPECIAL SITE　出典：サイバーセキュリティ情報局（キヤノンMJ）

キヤノンMJがお届けする安全なデジタル活用のためのセキュリティ情報
サイバーセキュリティ情報局

【サイバーセキュリティ情報局】

サイバーセキュリティに関するニュースや用語が、わかりやすく掲載されている
Canon社の情報サイトです。

※出典：「キーワード辞典」より

■マルウェア（malware）とは■

悪意のある（malicious）ソフトウェア（software）を合わせた造語であり、感染対象に対して有害な作用をもたらすことを目的に作成されたソフトウェアの総称である。 コンピューターウイルスはマルウェアの一種であり、マルウェアのほうがウイルスより広い概念である。

■踏み台とは■

サイバー攻撃者が、関係のない第三者のコンピューターやサーバーを乗っ取り、攻撃の拠点として利用すること。もしくは利用された拠点そのもの

■DDoS攻撃とは■

複数の端末から標的となる通信機器や端末に対して大量の通信を行い、サービスを妨害する攻撃の一種

マルウェアに感染して乗っ取られたコンピューターを「踏み台」として利用し、それら多数の端末から一斉に標的を攻撃するケースも増えている。その場合、踏み台にされた機器は、所有者の知らぬ間に攻撃に悪用され、結果的にDDoS攻撃に加担してしまうケースも少なくない

CHECK！

【内閣サイバーセキュリティセンター】

Twitter
https://twitter.com/nisc_forecast

NISC 内閣サイバーセキュリティセンター 注意警戒情報

【情報処理推進機構】

Twitter
https://twitter.com/IPA_anshin

IPA 情報セキュリティ安心相談窓口

個人のパソコン・スマートフォンには、必ずセキュリティ対策を！

本学は、セキュリティソフトESETのライセンス契約をしています。無償でご利用できます。 詳しくは、こちらから

【情報倫理と情報セキュリティ】 明治学院大学情報センター
2021年３月　Ver. 1.00作成