情報倫理と情報セキュリティ

はじめに

■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**適切な行動規範**のことです。 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やガイドライン、さらには、罰則のある法律もありますので十分注意してください。

■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べき**危機管理対策**（リスクマネージメント）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ります。

十分な知識を身に付けて、適切な対策・対応を心がけてください。

■本マニュアルは情報の要約です。 リンクから各サイトの内容を閲覧してください。

■本学では、eラーニング【**倫倫姫のセキュリティ教室**】の受講を推奨しています。

■Contents■

▼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
- 情報センター オリエンテーション（動画※Panopto ）
- 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
- 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 SNSのための５つの合言葉

・本ガイドラインに関するお問い合わせは、広報課へ

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点

■個人情報とは、

◆出典：政府広報オンライン

◆「【個人情報保護法】をわかりやすく解説」

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。 個人情報の有用性に考慮しながら、個人の権利を守ることを目的とした法律を、**【個人情報保護法】**といいます。

■個人情報や個人データを取り扱うときの基本ルール

① **取得・利用　：勝手に使わない**

・利用目的を特定して、その範囲内で利用してください。

・利用目的を通知または公表してください。

② **保管・管理　：なくさない！漏らさない**

・パソコンやUSBメモリーに入れたデータなど、適切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。

・データを共有する人にも徹底してください。

③ **提　　供　：勝手に人に渡さない**

・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。

④ **対　　応　：要求に対応する**

・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。

顔写真/指紋/音声/虹彩など

氏名/住所/性別/生年月日など

電話番号/メールアドレス/アカウントIDなど

免許証番号/マイナンバーなど

1．情報を発信する際の注意点

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

◆出典：警視庁「サイバーセキュリティ インフォメーション」
◆「守っていますか？ルールとマナー」

- 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・社会的責任、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、思わぬところで加害者や被害者になってしまうおそれもあります。

インターネット利用　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. 他人のプライバシーを尊重する
3. 住所・氏名などの個人情報を入力する時は、十分注意する
4. ID・パスワードの管理を徹底する
5. 他人の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

◆警視庁「サイバーセキュリティ インフォメーション」より

◆参考ページ

- 政府広報オンライン
  - あなたは大丈夫？SNSでの誹謗中傷
- 総務省
  - インターネット上の違法・有害情報に関してお困りの方へ
  - 違法・有害情報相談センター
- 明治学院大学
  - 学生部

慎重な情報発信を心がけてください

2．情報を利用する際の注意点

■著作権とは、

◆出典：文化庁「著作権」

作品（コンテンツ）を創作した者が有する権利で、**知的財産権**の一種です。

2-1.著作権に注意する

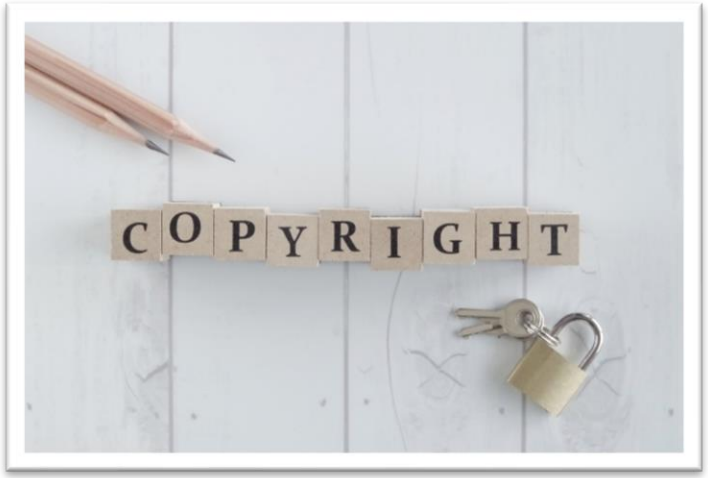
✓ 著作権を有するコンテンツとは、
- ネット上や出版されている他人の著作物（動画、写真、イラスト、文章、音楽、プログラム、本、配布物、ポスターなど）
- 授業の際に取得した授業の動画や資料、配布された教材や資料など
- ポスターなどの著作物をメインに撮影した画像など。 ※背後に映り込んだ状態には別規則 ※1（次ページ）

✓ コンテンツをコピーして自分のSNS等に投稿する、友人に譲渡するなどの再配布は、著作権法に抵触するおそれがあります。
不適切な再配布をしないよう注意してください。

✓ コンテンツを自分のレポート等に利用する際には、規定があります。
正しい引用のルールを守って利用してください。 ※2（次ページ）

✓ 映画や音楽などのコンテンツを授業で利用する際には、教育の特例ルールがあります。
規定の範囲内で利用してください。 ※3（次ページ）

✓ 違法サイトのコンテンツ（「侵害コンテンツ」いわゆる海賊版）は、自分用にダウンロードすることも違法です。 刑事罰の対象となる場合もありますので注意してください。
※ウィルス感染のリスクも伴うため、正規の配信サイトで閲覧してください。 ※1（次ページ）



2．情報を利用する際の注意点

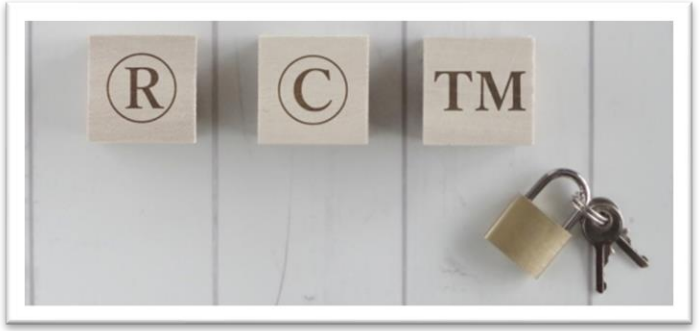
■著作権に関する情報

詳細は、下記の【各機関のホームページ】にて確認してください。

◆文化庁
- 著作権　：著作権法改正（2021年1月）
- そのダウンロード違法かも？（PDF）※1
- 著作権テキスト（PDF）
- 学校における教育活動と著作権（PDF）※3

◆政府広報オンライン
- 「侵害コンテンツ」ダウンロードの違法化について　※1

◆CRIC公益社団法人　著作権情報センター
- **著作権教室**　：著作権全般をわかりやすく解説しているサイト
- 青少年向けの著作権関連ウェブサイト：音楽やテレビ番組等の著作権に関するリンク
- 学校教育と著作権（PDF　2022年12月版 ）※3



■正しい引用のルール　※2

① 公表された著作物からの引用であること

② 引用を行う必然性があること

③ 自分の文章と引用との違いが明確に区別できる表現であること

④ 自分の文章がメインで、引用は参考程度であること

⑤ 出典を明記すること

☑ **コンテンツは、ルールを守って利用してください**

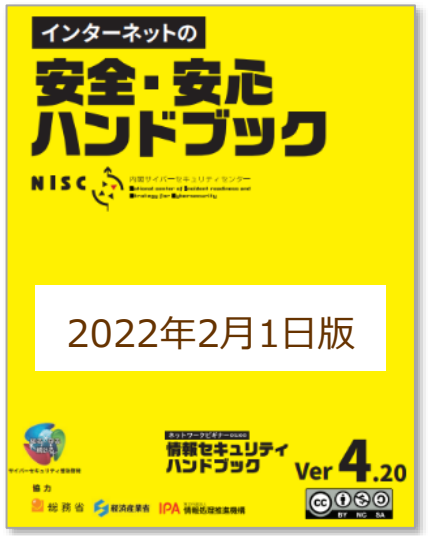
3．セキュリティ対策

■情報セキュリティとは、

パソコンやスマートフォンは単なる電子機器ではなく、大学生活に欠かせない重要なアイテムですが、保存されている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。

ネット詐欺やサイバー攻撃の手口は、時とともに変化していきます。しかし、情報セキュリティ対策の基本は、大きく変わるものではありません。 基本対策でしっかりガードして、安全にインターネットを利用しましょう。



■Contents■

◆参考ページ

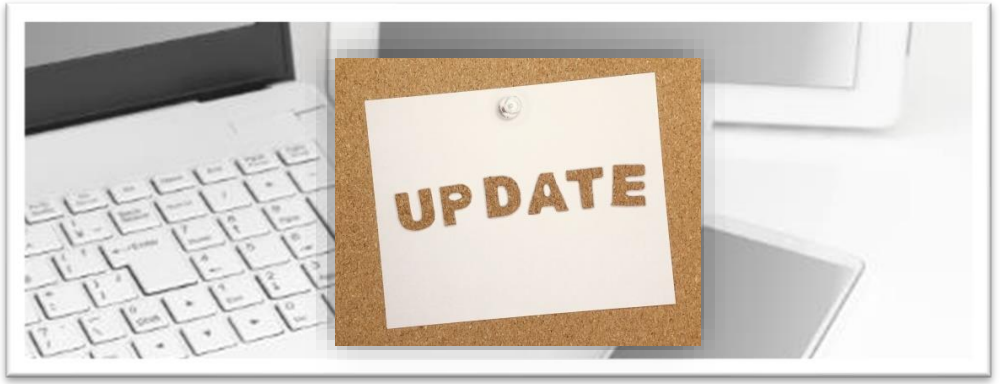
- ●内閣サイバーセキュリティセンター
  「**インターネットの安全・安心ハンドブック**」
- ●IPA 「ここからセキュリティ　対策の基本」
  「情報セキュリティ10大脅威（2023）」
- ●NISC 「サイバーセキュリティ（小冊子）」
- ●総務省「国民のためのサイバーセキュリティサイト」

3．セキュリティ対策

■情報セキュリティ対策の基本

3-1．脆弱性対策 【アップデート】

「OSやソフトウェアは、常に最新の状態に！」（動画）



- パソコンやスマートフォンのOS、ソフトウェア、アプリは、いつも最新のバージョンにしておきましょう。※1
- 古いままにしておくと、セキュリティに弱点（脆弱性）がある状態になってしまい、とても危険です。
- 最新のバージョンにアップデートをすると、脆弱性を悪用する攻撃への守りが強くなります。
- アップデートは、パソコンやスマートフォンだけではなく、ネットワークにつながるすべての機器に必要です。（ルーターやネットワークカメラ、スマートスピーカーなど、様々な機器についても忘れずに！）

◆参考ページ

- IPA 「脆弱性対策情報」
  「家庭教師が教えるネット家電セキュリティ対策！」（動画）

※1 OSのバージョンをアップグレードする際の注意！

バージョン名が変更になる大きな変更「アップグレード」をする際には、セキュリティソフトなどが対応しているかどうかを、本学のHPにて確認してから行ってください。

- 例： Windows 10 → Windows 11
  macOS Monterey → macOS Ventura
- アップグレード手順 ：Windows / Mac
- 確認は、「情報センター」(こちら)から

3．セキュリティ対策

3-2．ウイルス感染対策

「ウイルスへの対策意識を持ちましょう」（動画）

- ウイルスに感染したり、不正アプリをインストールしたりすると、大切な情報を盗まれてしまいます。 感染に気づかず、乗っ取られたままパソコンを使用すると、さらに被害が増大します。
- **パソコンやスマホなどには、必ずセキュリティソフトをインストールしましょう！**
- **ウィルス定義ファイルは、常に最新にアップデートをしましょう！**
- アプリは、原則として公式ストアから入手しましょう。
- メールの添付ファイルやリンク（URL）にウィルスが潜んでいるかもしれません。
  フィッシング情報に関する記事などを確認し、慎重に本物かどうか確かめましょう。

本学では、セキュリティソフト【**ESET**】のライセンス契約をしています。 学生・教職員は、無償で個人のパソコン、Android端末にインストールすることができます。

詳細は、情報センターのサイトを参照

ウィルス対策ソフト無償貸与サービスについて

◆参考ページ

- IPA
  「Emotet（エモテット）の感染を狙うメールについて」
  「ウイルスはのビジネスもプライベートも狙っている！」（動画）
  「あなたのスマートフォン、ウイルスが狙っている！（動画）
- Apple
  「詐欺対策と対処方のご案内」

3-3. 不正アクセス対策

1）パスワードの設定について

「パスワードは長く、複雑に、使いまわさない」（動画）

- 短いパスワードや、誕生日や名前、電話番号、辞書にある単語や、単純なパスワードでは、簡単に推測や解析をされてしまいます。
- 同じパスワードを複数のサービスで使うと、ハッキングされてしまった時に、ほかのサービスにも不正にログインされることがあります。
- パスワードは他人に教えないで大切に保管しましょう。

☑ パスワードのチェックポイント

◆チョコっとプラスパスワードより

- □ 8文字以上の文字数で構成している
- □ 数字や、記号も混在している
- □ アルファベットに大文字と小文字を混在している
- □ サービスごとに違うパスワードを設定している

2）Wi-Fi の利用について

「Wi-Fiの安全な利用について」（総務省）

- Wi-Fiを正しく理解して、安全に利用していますか？
- 接続するアクセスポイントをよく確認し、信頼性のないWi-Fiの利用は避けましょう。偽のアクセスポイントに騙されないよう、メールアドレスやID・パスワードの入力も慎重に！

◆参考ページ

- ●JCCA
  「ID・パスワード～使いまわし絶対ダメ！」（動画）
- ●サイバーセキュリティ情報局
  「自宅のWi-Fi接続のセキュリティ対策」
  「屋外でのWi-Fi接続の基礎知識」

3-4．初期設定の見直し

「スマホを買ったら画面ロックを設定しましょう」（動画）

- 新しくパソコンやスマホなどの電子機器を買ったり、ソフトウェアやアプリを入れたりしたときは、初期設定から変更してセキュリティを高めましょう。初期設定では、セキュリティが弱かったり、データ共有などの思ってもみない機能がオンになっていたりします。
- 初期パスワードを変更し、生体認証などで画面ロックを設定することで、セキュリティを強化できます。
- データ共有など、情報を渡したり連携させたりする機能の設定を確かめておくことで、予想外のトラブルを防ぐことができます。
- ルーターやネットワークカメラなどのID、パスワードは、必ず出荷時設定から変更しましょう。
- 複数の人たちと機器を共有するときは、アカウント（ログインID）をわけましょう。

◆参考ページ

●政府広報オンライン

「スマートフォンのセキュリティ対策できていますか？」（動画）

●IPA

「スマートフォンには必ず画面ロックの設定を」

●サイバーセキュリティ情報局

「スマホをなくした！というときに取るべき行動とは？」

3-5. 脅威の手口を知る

「常に最新の手口を知っておきましょう」（動画）

- ネット詐欺やサイバー攻撃などの、最新の手口を知っておきましょう。
- インターネット上の罠は、テクニックがますます巧妙に、そして多様に変化しながら、あなたの心のスキをつこうと企んでいます。 流行している手口を前もって知って、備えておけば、被害にあう可能性を低くできます。
- 端末がウィルスに感染したおそれがあると思ったら、直ちにLANケーブルを抜き、Wi-Fiをオフにしてネット接続を取りやめましょう。
- 相談できる人や相談窓口を確かめておくこともおすすめです。

◆参考ページ

●IPA 「ここからセキュリティ」「対策する」「被害に遭ったら」
「情報セキュリティ安心相談窓口」「重大なセキュリティ情報」

●フィッシング対策協議会
「緊急情報」「フィッシング対策5カ条」

●サイバーセキュリティ情報局
「スマホがウイルスに感染!?不安に思ったら試したい5つの方法」

■フィッシングサイト

ユーザーの個人情報を不正に入手するために用意されたWebサイト

■マルウェア

悪意のある（malicious）ソフトウェア（software）を合わせた造語。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。

■踏み台

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。

■DDoS攻撃

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。

マルウェアに感染させ乗っ取った多数のPCをから一斉に標的を攻撃するケースもある。 乗っ取られたままPCを放置すると、悪用され、知らぬ間にDDoS攻撃の加害者となる事例も少なくない。

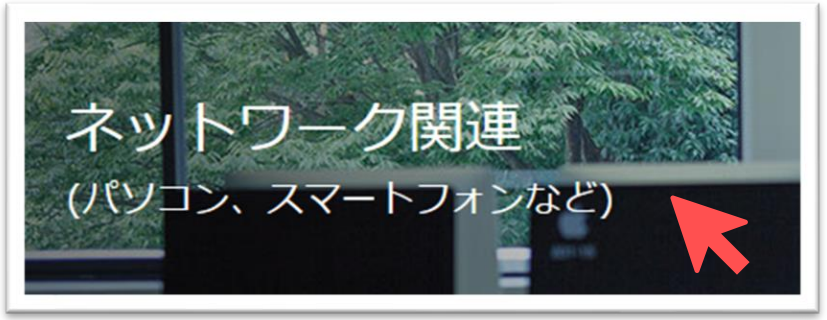
◆サイバーセキュリティ情報局「キーワード辞典」より

3．セキュリティ対策

■【情報センターからのお知らせ】を確認しましょう

✓ 本学HPに注意喚起等を掲載しています。

ネットワーク関連(パソコン、スマートフォンなど) | 明治学院大学 “Do for Others” (meijigakuin.ac.jp)



■リンクをクリックする前に検索しましょう

✓ SMSの電話番号や、メールアドレスを【Google検索】してください。

✓ 専門のサイトで、最近の詐欺の情報を確認してください。

✓ 報告されている詐欺情報に該当する場合があります。

フィッシング対策協議会

サイバーセキュリティー情報局

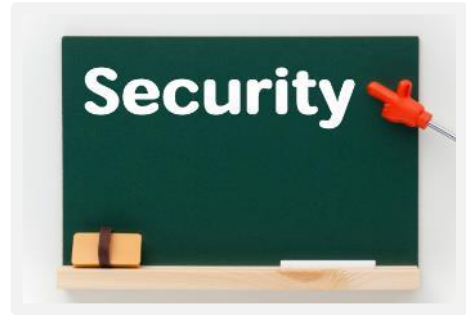
サイバー犯罪・詐欺　フィッシング

■Emotet(エモテット)

- 遠隔操作型ボットマルウェア（コンピューターウィルス）です。
- 主にメールのリンクから、偽のサイトにアクセスしたり、添付されたファイルを開いたりすることで感染します。
- こういったメールは、学校など自分が所属する組織や大手の宅配業者などになりすましたり、通販サイトの返信に見せかけるなど、警戒心を感じないように作成されていて、無意識にリンクや添付ファイルをクリックするよう仕向けています。
- リンク先の偽サイトも本物そっくりに偽装され、巧妙にパスワードを入力させたり、不正プログラムを発動させたりします。また、メールの添付ファイルでは、ありがちなタイトルのWordやExcel等を開くことにより、不正プログラムが発動したりと様々な手口があります。
- Emotetに感染すると、パスワードや個人情報などを盗まれたり、マルウェア・スパム送信などのさらなる攻撃の踏み台に利用されたり、パソコンが制御不能になる「ランサムウェア」など他のマルウェアに感染したりと、深刻な事例に陥ることが報告されています。

3．セキュリティ対策

情報セキュリティ対策のPOINT！



1．OS やソフトウェアは、常に最新の状態にしておこう

新たに広まるコンピュータウイルスに対抗するため、製造元から無料で配布される最新の更新プログラムにアップデートしましょう。

2．パスワードは貴重品のように管理しよう

パスワードは自宅の鍵と同じく大切です。パスワードは他人に知られないように、メモをするなら人目に触れない場所に保管しましょう。

3．ID・パスワードは、他人に絶対教えない

金融機関を名乗り、銀行口座番号や暗証番号、ログインIDやパスワード、クレジットカード情報の入力を促すような、身に覚えのないメールが届いた場合、入力せず無視しましょう。

4．身に覚えのない添付ファイルは開かない

身に覚えのない電子メールにはコンピュータウイルスが潜んでいる可能性があります。添付されたファイルを開いたり、URL（リンク先）をクリックしないようにしましょう。

5．ウイルス対策ソフトを導入しよう

パソコンはもちろん、スマートフォンやタブレットにもウイルス対策ソフトをインストールしましょう。ウイルス定義ファイルのアップデートも忘れずに。

6．信頼できるサイトを選ぼう

ネットショッピングやアプリのダウンロードは、詐欺や個人情報漏洩などの被害に遭わないように、信頼できるショップやサイトを選びましょう。

7．大切な情報はバックアップしておこう

思い出の写真や様々な記録など、大切な情報がパソコンの初期化や故障によって失われることのないよう、別のハードディスクなどに複製しておきましょう。

8．外出先では紛失・盗難・ネットワークに注意しよう

大切な情報を保存したパソコン、スマートフォンなどを自宅から持ち出すときは機器やファイルにパスワードを設定し、なくしたり盗まれないように注意して持ち歩きましょう。

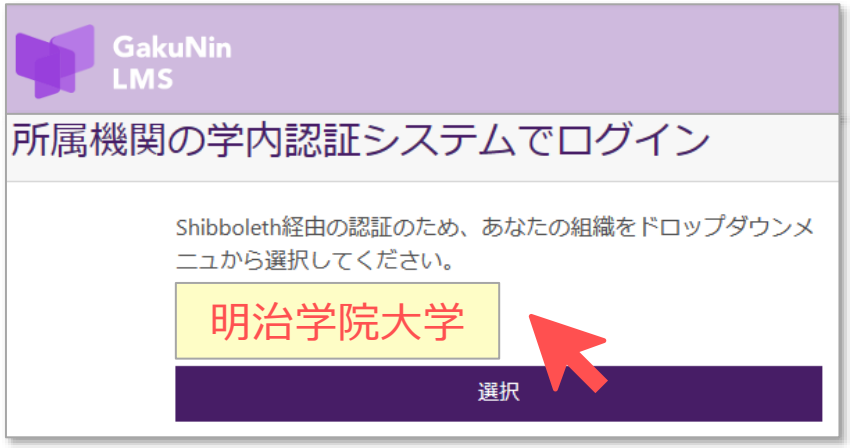
市中のFree Wi-Fiに接続するときも十分注意しましょう。

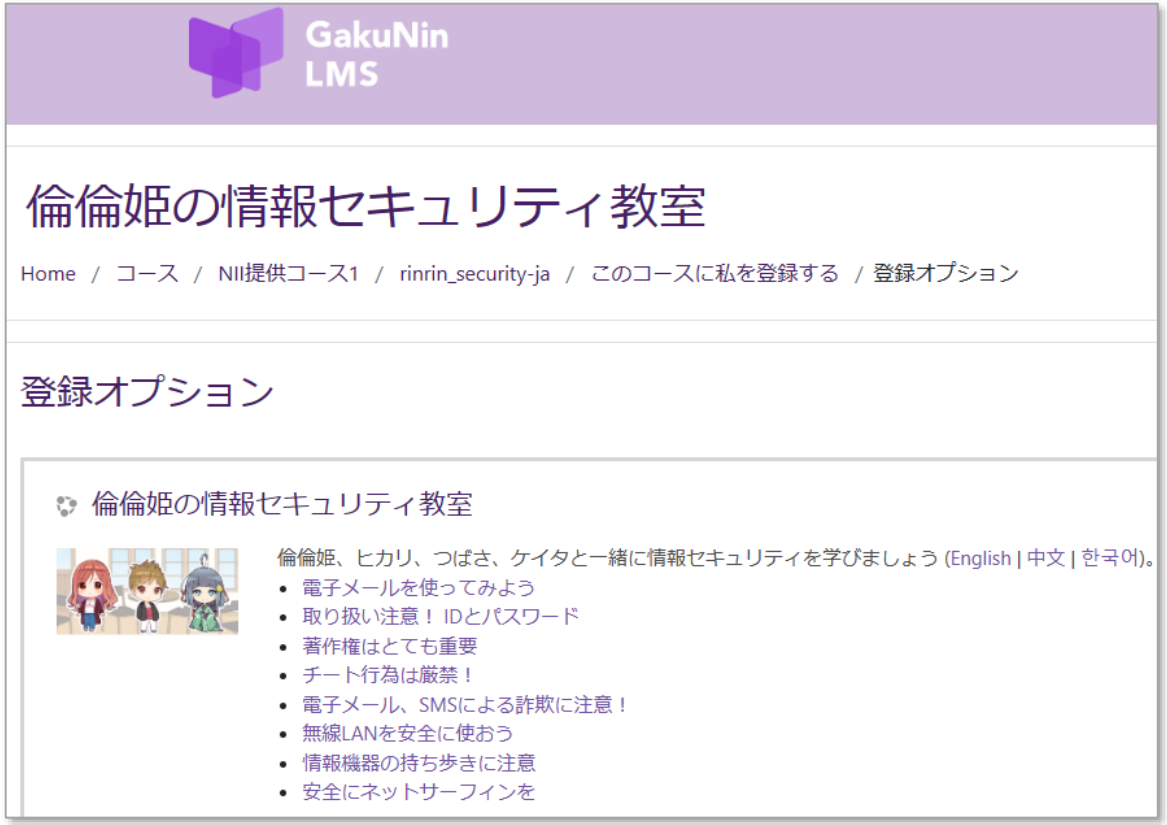
9．困ったときは、まず相談

架空請求のメールが届く。ウイルスに感染した。などの被害に遭遇したら、ひとりで悩まずに、各種相談窓口に相談しましょう。

■eラーニングで学ぶ

- 「**倫倫姫（りんりんひめ）の情報セキュリティ教室**」は、国立情報学研究所が提供する**情報倫理に関するe-Learning教材**です。
- 情報セキュリティの理解を深めて、サイバー攻撃の被害者、情報漏洩等の加害者にならないためにも、積極的に受講してください。
  - 英語・中国語・韓国語に対応しています。
  - MAINアカウントでの認証が必要です。
  - ログインは、こちら から





- NIIの紹介動画は、こちら　（YouTube）
- ログインの手順は、こちら　（動画※Stream ）

引用、出典、参考資料一覧

◆NISC【内閣サイバーセキュリティセンター】

「インターネットの安全・安心ハンドブック」

twitter: https://twitter.com/nisc_forecast

◆IPA【情報処理推進機構】

情報セキュリティポータルサイト ここからセキュリティ

情報セキュリティ

情報セキュリティ普及啓発映像コンテンツ (YouTube)

twitter: https://twitter.com/IPA_anshin

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

Canon | ESET SPECIAL SITE

◆Canon【サイバーセキュリティ情報局】

「キーワード辞典」「更新プログラム情報」

◆文化庁 著作権

◆総務省 国民生活と安心・安全 ＞ サイバーセキュリティー統括官

◆政府広報オンライン 暮らしに役立つ情報 安全・防犯

◆警視庁 安全な暮らし ＞ サイバーセキュリティー インフォメーション

相談・お悩み ＞ インターネットトラブル

◆警視庁サイバー犯罪対策プロジェクト ＞ 広報・施策

◆警察協会 ビデオライブラリー ＞ サイバー犯罪

◆フィッシング対策協議会（Council of Anti-Phishing Japan）

■NII 【国立情報学研究所】 ＞ 倫倫姫の情報セキュリティ教室

◆CRIC 【公益社団法人著作権情報センター】

◆PPC 【個人情報保護委員会】

◆JCCA 【日本クレジット協会】