第○○回　情報セキュリティ e-learning

2021年9月　IT部

IT Professor

情報セキュリティポリシーについて　①情報セキュリティポリシーとは

- 情報セキュリティポリシーとは
　会社が、どんな脅威から、どんな情報を、どのようにして守るかを明確にし、社員全員の情報セキュリティへの取り組みをルールとして定めたもの。

　IT-Professorの情報セキュリティポリシーは、2017年5月15日にIT部ポータルサイトにてリリースされました。

https://it-professor.jp/○○/security_e-learning/2017

　情報セキュリティに対して、どんなに技術的な対応が進んでも、情報管理に対するルールや社員の意識が低くては、リスクが軽減されることにはなりません。
　情報セキュリティポリシーの内容をきちんと理解し、そのルールに従った業務を行うように心がけてください。

情報セキュリティポリシーについて　②機密区分の分類

情報セキュリティポリシーには、情報の取り扱いについても記載されています。
今後、作成するドキュメントは、極秘・秘・社外秘に分類し明記しましょう。

	機密区分	ユーザーが理解すること	例
1	**極秘** **（Classified）**	秘密保全の必要性が特に高く、漏洩することにより、株主や顧客など外部利害関係者を巻き込み、企業活動に重大な損害を与えるおそれがある情報とする。	・一般公開前の建築プロジェクト情報 ・業務委託を受けた建築図面情報 ・株主情報 ・M&A等
2	**秘** **（Confidential）**	秘密保全の必要性があり、漏洩することにより、企業活動に影響を与えるおそれがある情報とする。	・重要契約書 ・財務諸表 ・人事情報 ・開発商品情報 ・コスト情報（原価） ・顧客個人情報等
3	**社外秘** **（Internal Use Only）**	「極秘」、「秘」以外の情報で、情報開示規程に基づき開示している情報以外の情報とする。	・会議の議事録 ・営業企画書 ・見積書等
4	**公開**	公開可能ドキュメント	・カタログ ・営業報告書等 ・社内報

近年増加している被害　詐欺メール（フィッシング）

有名企業をかたったメールを送信して不正なウェブサイトへ誘導し、IDやパスワード等を詐取するフィッシング詐欺が行われています。

最近では、Apple ID や Microsoftアカウント等、複数のサービスを利用できる認証情報が狙われる傾向にあり、詐取された情報を悪用され金銭的な被害が発生しています。

不自然な日本語には
気を付けましょう！

Apple IDのユーザーを尊敬する、これは非常に重要な手紙です。あなたのアカウントに異常な登録が発生し、一部の情報が失われたため、私たちはアカウント情報の更新が完了するまで、一部のアカウントをロックする権限があります。この間、appプログラムを正常に利用することができなくなります。すぐにステップに沿って、口座情報を更新していただき、ご理解いただき、まことに申し訳ありません。

リカバリアカウント　<http://0nline●●●●.com/>

3営業日以内に情報の更新がなければ、あなたの口座は完全に使用を停止します。

ご迷惑をかけまして、大変申し訳ございません。

Apple サービスセンター

例：AppleIDをかたるフィッシングメール（2019/08/20）
出典：フィッシング対策協議会

Appleのすべてのサービスで使用するアカウントです。

偽

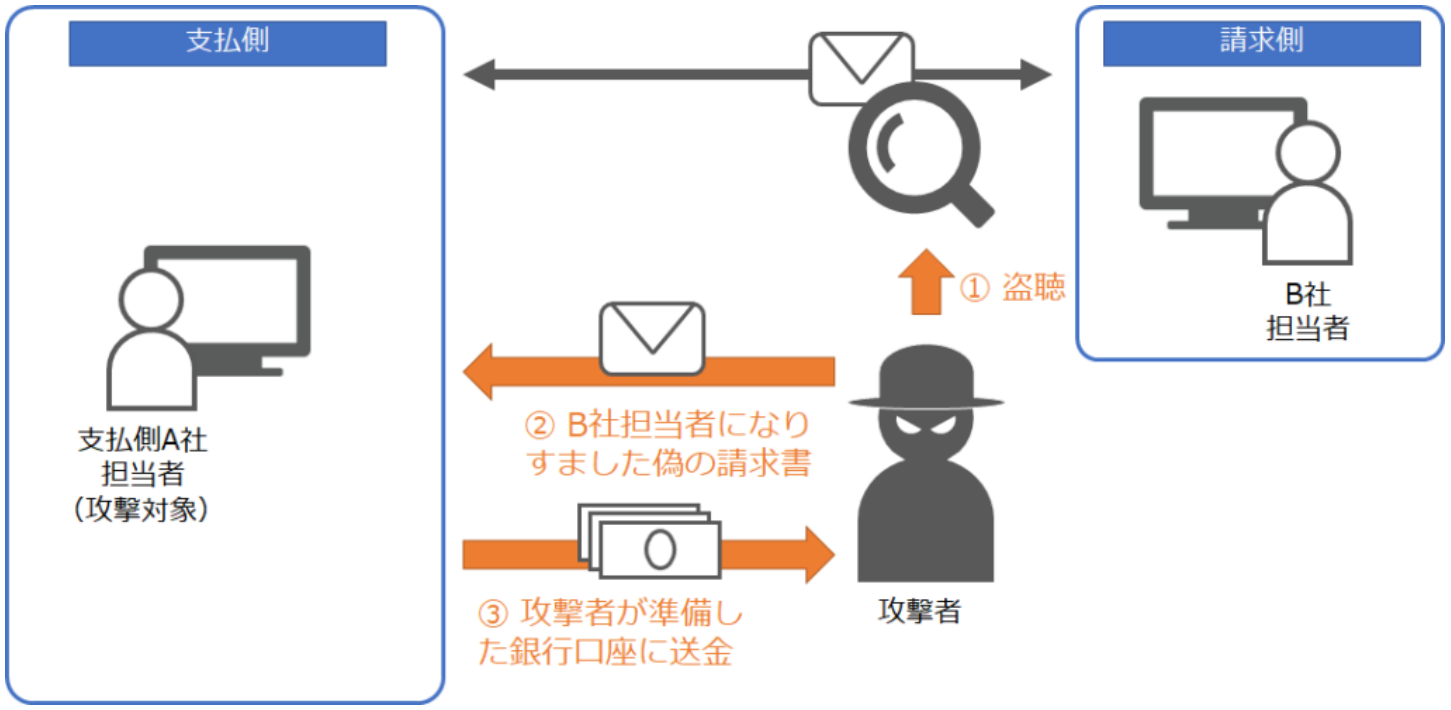
Appleのすべてのサービスで使用するアカウントです。

正

1. メール　ビジネスメール詐欺（BEC）　1/4

- **ビジネスメール詐欺とは（BEC＝Business E-mail Compromise）**

　業務用メールを盗み見して経営幹部や取引先になりすまし、従業員をだまして送金取引などに係る資金を詐取するなどの金銭的な被害をもたらすサイバー攻撃です。
実際に詐欺行為に及ぶ前に、企業内の従業員などの情報を窃取したりするために、マルウェア（ウイルス）が使われることもあります。



1. メール　ビジネスメール詐欺（BEC）　2/4

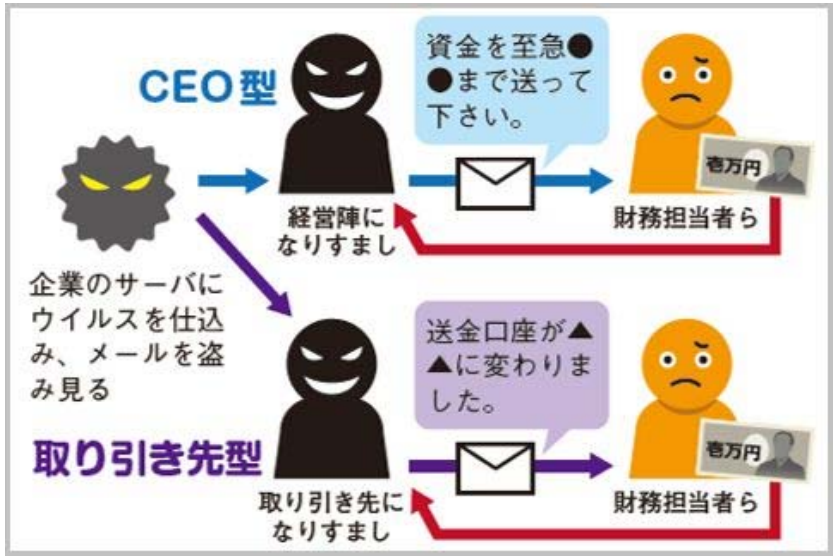
● ビジネスメール詐欺の仕組み

• 事前に標的に関する情報を盗んでおく

　業務用メールの盗み見には、偽のログインページを用意してアカウント情報を入力させる「フィッシング詐欺」を使う手口と、キーボード入力を監視する「キーロガー」を使う手口が代表的です。

• 信ぴょう性の高いメールで標的を騙す

　業務用メールを盗み見した攻撃者は、なりすましのメールを作成しターゲットの企業の従業員を巧みな方法でだまします。最近のビジネスメール詐欺では、「経営陣になりすます方法」と「取引先になりすます方法」の2つのタイプに分類されます。



1. メール　ビジネスメール詐欺（BEC）　3/4

- **事例：日本航空（JAL）が3.8億円の詐欺被害**

JALは2017年12月20日、偽の請求書メールにだまされて約3億8000億円の被害に遭ったと発表した。犯人は、JALと取引先のメールのやり取りに割り込み、取引先になりすまして、口座に金を振り込ませた。

1.　旅客機リース料　約3.6億円被害

2017年９月、旅客機のリース料について、支払先である海外の金融会社の担当者になりすました偽の請求書がJAL本社に届いた。「料金の振込先の口座が香港の銀行に変更された」などと記されており、JALの担当者は約3億6000万円を指示通りの口座に振り込んだ。数日後、全額が引き出されて回収不能になった。

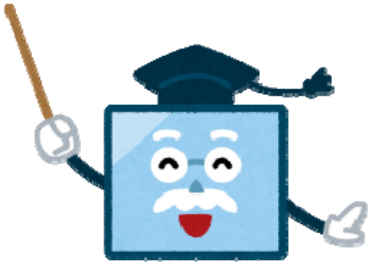
2.　地上業務委託料　約2,400万円被害

2017年８月、貨物の業務委託料について、JALの米国にある貨物事業所に支払先口座の変更を伝えるメールが届いた。JAL側の担当者は、変更された香港の銀行口座へ２回にわたり、計約2400万円を振り込んでしまった。

1. メール　ビジネスメール詐欺（BEC）　4/4

☞ユーザーがやるべきこと

- **口座変更の連絡は疑う**
  　口座変更を伝えるメールや請求書に注意し、電話などで支払先に「本当に変更なのか？」と確かめる。電話番号はメールに書いてあるものではなく、自分で調べて問い合わせる。



- **ビジネスメールのパスワードを複雑なものに**
  　メール乗っ取りを防ぐために、パスワードを独自の複雑なものにする。パスワードの使い回しは絶対にやめる。

- **ウイルス感染対策を講じる**
  　セキュリティー対策ソフトを導入する。IT-Professorでは、最新のセキュリティソフトを導入しています。ご安心ください。

- **ビジネスメール経由でのクレジットカード登録は避ける**
  　ビジネスメールのリンクをクリックした先でクレジットカードを登録しない。偽サイトへ誘導するワナかもしれない。登録を促すビジネスメールが来た場合は、自分でアドレスを調べて正規サイトを開き、本当に登録が必要なのか確かめる。

2. データの保管・保存について　1/2

最近では、大容量の機密データをサーバーやパソコン、記憶媒体に保存することが可能です。しかし、情報セキュリティ対策を怠ると、第三者によって一度に多くの機密データを持ち出される危険性があるので注意が必要です。
機密データを保管・保存する際には以下のような対策が求められます。

☞ユーザーがやるべきこと

- 機密データの保存
  - **パスワード設定や暗号化をする**
    ※データファイルへパスワード設定や暗号化する方法については、お問い合わせください。
  - **バックアップがとられているサーバ**（Nas01,rsd-rook,psd-rookなど）**に保存する**

2. データの保管・保存について　2/2

☞ユーザーがやるべきこと

- 機密データの保管
  - **データファイルやフォルダに適切なアクセス権を設定する**
    ※データファイルや保存するフォルダへのアクセス件を付与する方法については、IT部にお問い合わせください。
  - **記憶媒体は施錠可能な場所に保管する**
    ※社有フラッシュメモリーはIT部が提供します。
- 記憶媒体の保管場所
  - 施錠ができる場所（引き出しなど）
  - 高温多湿な場所を避ける
  - ホコリがつかないようにする
  - 直射日光・強い磁気に当てない
  - 結露させない、水に濡らさない

3. ソフトウェアの不正コピーの禁止　1/3

- **著作権とライセンス**

　ソフトウェア（Office系ソフト、画像処理ソフト、CADソフト、会計ソフトなど）の著作者であるソフトウェアメーカーには、ソフトウェアのインストールを許諾するかどうか、パソコン何台分までインストールを許諾するかを決める権利（著作権の一つである複製権）があります。

　従って、ユーザーがソフトウェアをインストールして使う場合には、あらかじめソフトウェアメーカーの許諾（ライセンス）が必要となります。

- **不正コピーとは？**

　ファイル共有ソフトなどを介してソフトウェアを非正規に入手してインストールした場合はもちろんですが、正規に購入した場合でも、ソフトウェアメーカーがあらかじめ許諾したインストール可能台数を超えてインストールすれば不正コピー、すなわち著作権・複製権侵害となります。

3. ソフトウェアの不正コピーの禁止　2/3

- **不正コピーが起きる背景**
  　不正コピーは意図して行われるケースとそうでないケースとがあります。「意図して」というのは論外ですが、知らずに不正コピーしてしまう場合についても注意が必要です。

  - **意図的な不正コピー**
    ソフトウェアの正規ライセンス料を節約したいという理由で、意図的な不正コピーが行われます。不正コピーが著作権法違反であることを理解し、意識を改める必要があります。

  - **意図的でない不正コピー**
    ソフトウェアのライセンス管理が不十分なため、知らないうちに不正コピーをしてしまっていたというケースも多々あります。

- **著作権法に違反したときの罰則は？**
  　不正コピーで著作権法違反が発覚した場合、刑事・民事の両面で責任を問われることになります。

3. ソフトウェアの不正コピーの禁止　3/3

- **例：Adobeソフトの場合**

IllustratorやPhotoshopといったAdobe社のソフトは、以下のような利用規約が定められています。

- **インストール**
  OSの種類に関係なく、CreativeCloud メンバーシップを所有する1人のユーザーがお使いのコンピューター複数台に CreativeCloud アプリケーションをインストールできます。

- **ライセンス認証（ログイン）**
  CreativeCloud は最大2台のコンピューターで同時にライセンス認証できます。

- **使用**
  一度に1台のコンピューターでソフトウェアを使用できます。複数人数が利用する場合は、その人数分のライセンス契約が必要になります。AdobeIDを使いまわすことは、規約上認められていません。

これで、第○○回目の情報セキュリティe-learningの学習は終了です。

このページを閉じてGoogleフォームに戻り、
チェックテストを実施してください。