北摂SITA 2018-9-16 勉強会

情報セキュリティ対策

ひっかかった実例をもとに

MO_ibaraki

情報セキュリティ10大脅威 2018

IPA

● 順位

「個人」向け脅威	順位	「組織」向け脅威
インターネットバンキングや クレジットカード情報等の不正利用	1	標的型攻撃による被害
ランサムウェアによる被害	2	ランサムウェアによる被害
ネット上の誹謗・中傷	3	ビジネスメール詐欺による被害
スマートフォンやスマートフォンアプリを 狙った攻撃	4	脆弱性対策情報の公開に伴う 悪用増加
ウェブサービスへの不正ログイン	5	脅威に対応するための セキュリティ人材の不足
ウェブサービスからの個人情報の窃取	6	ウェブサービスからの個人情報の窃取
情報モラル欠如に伴う犯罪の低年齢化	7	IoT機器の脆弱性の顕在化
ワンクリック請求等の不当請求	8	内部不正による情報漏えい
IoT機器の不適切な管理	9	サービス妨害攻撃によるサービスの停止
偽警告による インターネット詐欺	10	犯罪のビジネス化 （アンダーグラウンドサービス）

出典元：情報処理推進機構「情報セキュリティ10大脅威 2018 個人編」
https://www.ipa.go.jp/security/vuln/10threats2018.html

【1位】インターネットバンキングやクレジットカード情報等の不正利用

～被害は継続して発生、仮想通貨に関する被害も～

- **攻撃手口**
  - **ウイルス感染による認証情報の窃取**
    - 悪意あるファイルをメールに添付して送信し、ファイルを開かせる
    - 悪意あるウェブサイトが表示されるリンクをクリックさせる
  - **フィッシング詐欺による認証情報の窃取**
    - 実在する企業を模した偽のウェブサイトやURLを作成し、メールに記載されたリンクからアクセスさせる
    - メールの件名や本文に読まなければならないと思わせるような細工を施し、クリックを促す

出典元：情報処理推進機構「情報セキュリティ10大脅威 2018 個人編」
https://www.ipa.go.jp/security/vuln/10threats2018.html

【1位】インターネットバンキングやクレジットカード情報等の不正利用

～被害は継続して発生、仮想通貨に関する被害も～

- **対策一覧**
  - **利用者**
    - 被害の予防
      - メールやウェブサイトの十分な確認
      - 添付ファイルやリンクを安易にクリックしない
      - 普段表示されない画面に個人情報等を入力しない
      - 事例や手口の情報収集
      - OS・ソフトウェアの更新
      - セキュリティソフトの導入
      - ファイルの拡張子を表示させる設定
      - パスワードの適切な管理と運用
      - 銀行が推奨する認証方式の利用
      - 仮想通貨の安全な利用（ウォレットの適切な管理等）
    - 被害の早期検知
      - 不審なログイン履歴の確認
      - 口座やクレジットカードの利用履歴を確認
      - 利用時のメール連絡機能等の活用
    - 被害を受けた後の対応
      - コールセンターへ連絡
      - クレジットカードの停止
      - システムの復元・初期化
      - パスワードの再設定

出典元：情報処理推進機構「情報セキュリティ10大脅威 2018 個人編」
https://www.ipa.go.jp/security/vuln/10threats2018.html

フィッシングメールの実例

差出人 Apple(チーム) <Ug2C7Hx5Wx82awTHV2SS@Ug2C7Hx5Wx82awTHV2SS.com> ☆

件名 **Apple IDは、デバイスの追加を承認するのを待っています。[デバイスID: #ZATkQrYZHo]**

宛先

Apple ID は未知のデバイスでサインインされています。

望ましくない行動を防ぐために、最後のアクティビティを確認する必要があります。

起動ログの詳細を以下に示します。

ロケーション : JL. Mangkubumi、メダン、北スマトラ

IP : 32.12.5.129

国 : インドネシア

最新のApple ID 操作を確認してください。

デバイスを自分のApple ID に追加し、 ここをクリック>

デバイスを永久に削除し、 ここをクリック>

Apple ID に使用するデータが必要であることを確認してください。

あなたからの返信が届かない場合は、 私たちは Apple ID を 3 ヶ月以内に無効にします。

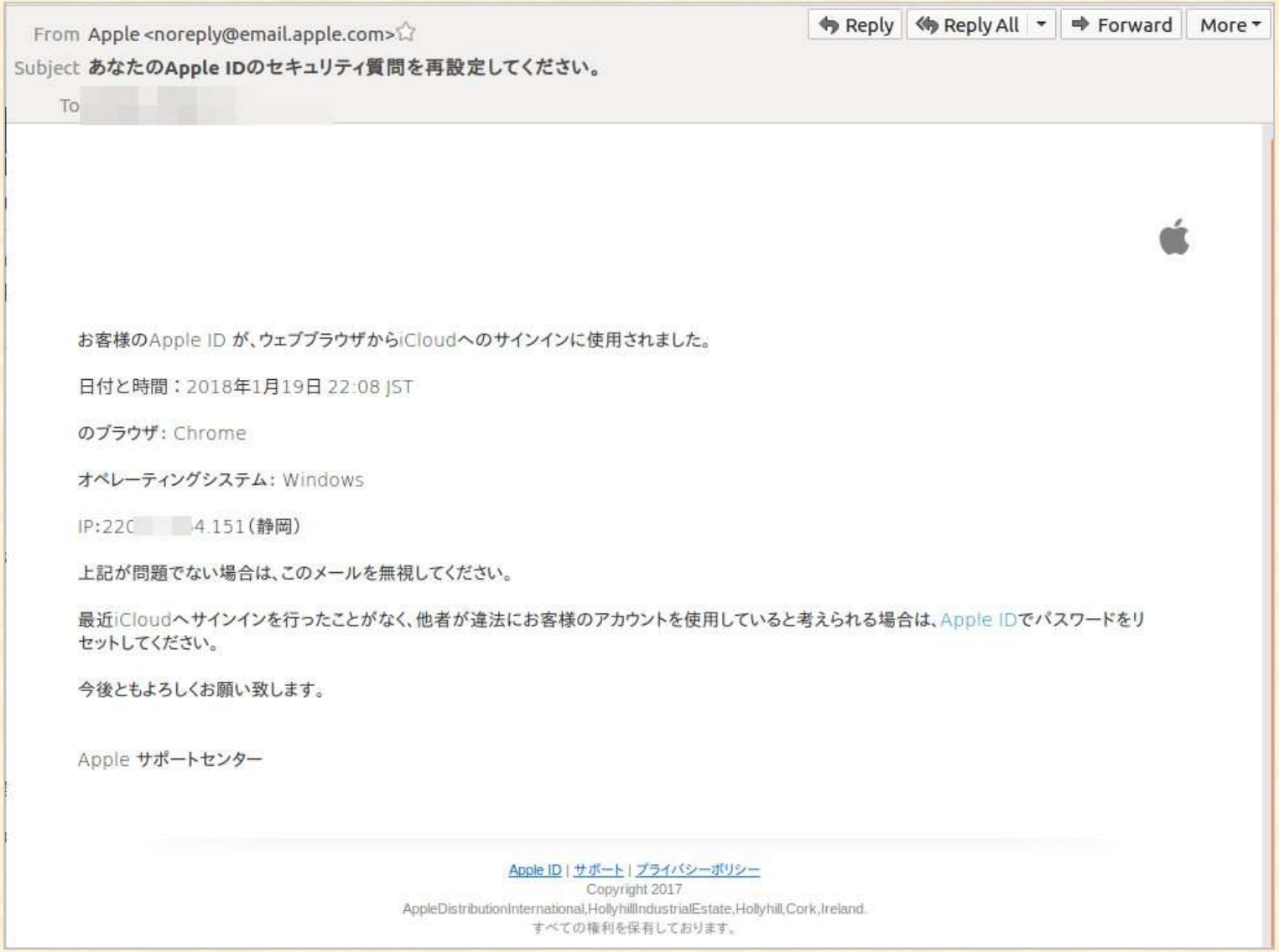
利便性と顧客のセキュリティが最優先事項です。

敬具

Apple

2018.9.12受信

フィッシングメールの実例



From Apple <noreply@email.apple.com>
Subject あなたのApple IDのセキュリティ質問を再設定してください。
To

Reply | Reply All | Forward | More

お客様のApple ID が、ウェブブラウザからiCloudへのサインインに使用されました。

日付と時間：2018年1月19日 22:08 JST

のブラウザ: Chrome

オペレーティングシステム: Windows

IP:220 4.151(静岡)

上記が問題でない場合は、このメールを無視してください。

最近iCloudへサインインを行ったことがなく、他者が違法にお客様のアカウントを使用していると考えられる場合は、Apple IDでパスワードをリセットしてください。

今後ともよろしくお願い致します。

Apple サポートセンター

Apple ID | サポート | プライバシーポリシー
Copyright 2017
AppleDistributionInternational,HollyhillIndustrialEstate,Hollyhill,Cork,Ireland.
すべての権利を保有しております。

フィッシングメールの実例

最近LINEアカウントの盗用が多発しており、ご不便をもたらして、申し訳ありません。あなたのアカウントが盗まれないよう、システムは2段階パスワードに更新いたしました。なるべく早く設定をお願いします。

こんにちは、このメールはLINEで自動送信されています。
以下のURLをクリックし、二級パスワード設定手続きにお進みください。

https://line.me/R/au/email/vjbfynvrjotpd4dzs53hel0r5swm0zci/5373
<http://www.line●●.cn/>

LINE
http://line.me

LINE Corporation

メール文面例

思わずひっかかったフィッシングメール

・偽「Apple」より、iPhoneに、
「2段階認証がまだ設定されていないので、下記より、設定してください」

ちょうど設定しようと考えていた頃で、思わずリンクをクリックしてしまった
リンク先のサイト（Appleみたい）で、Apple ID, パスワードの入力！

・反応なし → やってしまった！！！

ひっかかった後にとった行動

元の偽メールをみると、下段のリンク先等も、青文字だがリンクなし

慌てて、正規のAppleサイトで、PWは変更

Appleサポートに電話連絡

不正ログインはその時点で確認されなかったが、現Apple IDは破棄し、新たなIDに移行を強く勧められた

Apple IDの移行

iCloudで写真共有等があり、新規ではなく移行が必要 → **この移行が大変**

すべてのデバイス(iPhone、iPad、Mac）からサービスごとに（FaceTime、iPhoneを探す、iCloud等）サインアウトが必要・・・、手元にない端末も…

さらに、
同じ「ID（メールアドレス）」と「PW」の組み合わせは、すべて変更した。（多くのサイトで使用…）

フィッシングメールの特徴例

１．挨拶文
　「カスタマー様」や「ユーザー各位」といった一般的な挨拶文になっている。(正規の会社の多くは、ユーザー個人宛のメッセージにはユーザー本人の名前を記載)

２．登録していないメールアドレスに着信

３．文法誤りやスペルミス

４．リンク先が、HTTPSを使用していない

５．クレジットカードや、アカウントのパスワードなどの個人情報を要求される

最近のセキュリティ対策

１．２段階認証の導入

インターネット上の各種サービス（ウェブサービス）を利用する際に、通常の ID とパスワードに加えて、もうひとつ本人確認の要素を増やす（セキュリティコードの入力や、スマホ上でのログイン可否選択）ことによって安全性を高める。

・Apple、amazon、Google、DropBox、…

最近のセキュリティ対策

２．VPN接続

・誰でも“つながり放題”の公衆無線LAN(フリーWiFi)
・無防備(暗号化なし)で “のぞき放題”(傍受可能)

VPN（Virtual Private Network：仮想プライベートネットワーク）で、データを暗号化して、安全な通信ルートを確保する。デバイスとアクセスポイントの間の通信を暗号化するので、たとえ傍受されたとしても、解読できない

VPNアプリ(有料版）の利用、SSL(https)サイトの使用

最近のセキュリティ対策

3．PW認証（I/O 2018/6月号、8月号より）

「パスワードの定期変更は必要なし」
（総務省「情報セキュリティハンドブックVer.3.00」）

・安全なパスワードは、
「複雑さ」より「長さ」

例）大小英文字＋数字＋記号　（96文字）
8桁の場合、96の8乗＞7千兆通り
英小文字（26文字）
12桁の場合、26の12乗＞9京通り

・欧米では、「複数の単語からなるパスワード」が主流

以上

ありがとうございました