産技研技術セミナー・BMB第36回勉強会
「中小企業のための情報セキュリティ対策」
対策事例（1）
知っておきたいサイバーセキュリティ

石島　悌（いしじま　だい）
ishijima <at-mark> tri-osaka.jp
※ <at-mark> は @ に修正してください
地方独立行政法人 大阪府立産業技術総合研究所
http://tri-osaka.jp/
製品信頼性科（電気計測・情報通信・セキュリティ担当）

@マイドームおおさか　４階研修室
2017-03-09（木）16:10〜16:40ごろ

自己紹介（何をしている人か）

製品信頼性科所属（電気計測・情報通信担当）

安心して使える安全な電気製品・電子回路設計のお手伝い

・

信頼できる（dependableな）

ネットワーク・情報システムの運用

情報セキュリティの確保

・

情報処理学会・インターネットと運用技術研究会 幹事

製品評価技術基盤機構（NITE）電気技術解析WG 委員

関西オープンフォーラム実行委員

・

情報処理技術者※・電気主任技術者・エネルギー管理士、他

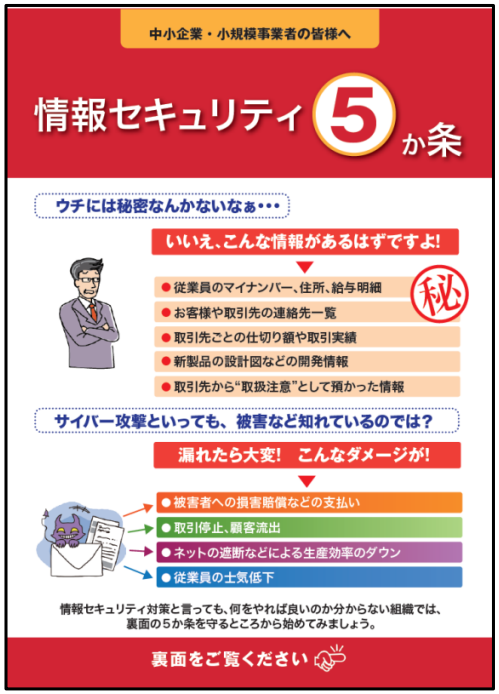
※テクニカルエンジニア（情報セキュリティ）・マイコン応用、他（SV, SU, ME,...）

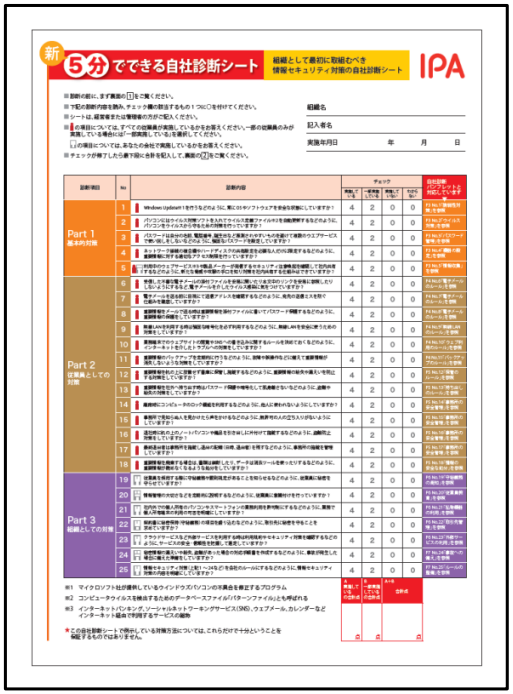
（申請手続き中）国家資格「情報処理安全確保支援士」

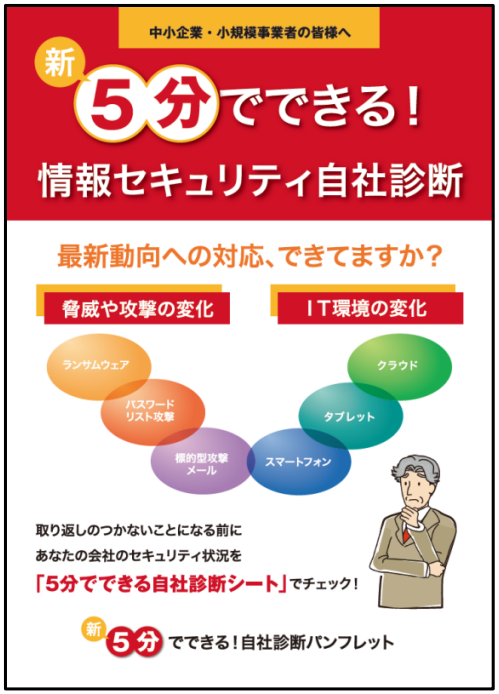
・

IPAセキュリティプレゼンター／講習能力養成セミナー受講者

追加配布資料について（IPAの資料）







「情報セキュリティ啓発中小企業の情報セキュリティ対策ガイドライン」
https://www.ipa.go.jp/security/keihatsu/sme/guideline/ などから
IPAの許諾を得て配布しています。対象としているのは次のような組織です。

- ●情報システム責任者を置けない、または兼任となる
- ●経営資源が限られるため、対策経費はあまりかけられない

本日の話題

- 府警本部さん、近畿管区警察局さんの「脅威」の話こわかったですね（…聴講前に資料を見ずに書きました）
- 「こわいこと」にあわないためにはどうすれば？
  - 職場で気をつけること
    - 攻撃から守る、情報の管理、メールや記憶媒体の取り扱い
  - 自宅に帰ってから（あるいは通勤途上で）の注意点
    - 偽サイトなど最近の注意すべきトピックス
    - スマートフォン・携帯電話で気をつけること
  - 違和感を覚えたらクリック・タップしない、開かない
  - 自分の操作を過信しない
    - タイプミス・勘違いによる誤操作に要注意

「こわいこと」にあわないために

- 大事なことなので結論を最初に書いておきます

「ヨソよりはマシ」ポリシーを徹底する

- パソコンやスマホなど
  情報機器の利用に限らない
- サーバ管理なども同様
- もっといえば
  「一般的な犯罪」にも
  遭遇しないツボ

攻撃者の心理（狙うならどちら？）

- 攻撃者に
  「あなたやあなたの組織は相手にしても無駄」
  と思わせることが大事

2月1日～3月18日は「サイバーセキュリティ月間」です。

#サイバーセキュリティは全員参加！

毎年2月はセキュリティ月間

毎年2月になったら担当者はチェック

内閣サイバーセキュリティセンター・今年のキャッチフレーズ
www.nisc.go.jp/security-site/month/catchphrase.html

何を知り、どう守れば？

- 何を知ればいいの？→ここに情報があります！
  - 内閣サイバーセキュリティセンター
    http://www.nisc.go.jp/security-site/index.html
  - 情報処理推進機構（IPA）のセキュリティのページ
    https://www.ipa.go.jp/security/
  - 組織の担当者さんは、かみ砕いて説明してください
  - これらの情報で不明な点があれば産技研にご相談を
- どんなことから守るの？
  →たとえば「情報セキュリティ10大脅威」
- どうすれば守れるの？→たとえば「対策９か条」

情報セキュリティ10大脅威 2017

1位に
金銭被害

以下、ランサムウェア、
不正アプリ、
不正ログイン、
ワンクリ詐欺、
個人情報の
窃取、
誹謗中傷、
…

昨年順位	個人	順位	組織	昨年順位
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の不正利用	1位	標的型攻撃による情報流出	1位
2位	ランサムウェアによる被害	2位	ランサムウェアによる被害	7位
3位	スマートフォンやスマートフォンアプリを狙った攻撃	3位	ウェブサービスからの個人情報の窃取	3位
5位	ウェブサービスへの不正ログイン	4位	サービス妨害攻撃によるサービスの停止	4位
4位	ワンクリック請求などの不当請求	5位	内部不正による情報漏えいとそれに伴う業務停止	2位
7位	ウェブサービスからの個人情報の窃取	6位	ウェブサイトの改ざん	5位
6位	匿名によるネット上の誹謗・中傷	7位	ウェブサービスへの不正ログイン	9位
8位	情報モラル不足に伴う犯罪の低年齢化	8位	IoT機器の脆弱性の顕在化	ランク外
10位	インターネット上のサービスを悪用した攻撃	9位	攻撃のビジネス化（アンダーグラウンドサービス）	ランク外
ランク外	IoT機器の不適切管理	10位	インターネットバンキングやクレジットカード情報の不正利用	8位

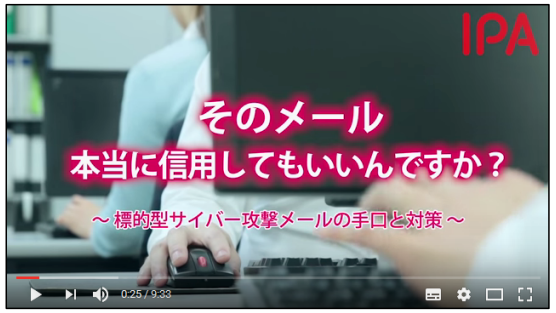
1位に
標的形攻撃

以下、ランサムウェア、
個人情報の
窃取、
妨害攻撃、
内部不正、
サイト改ざん、
不正ログイン、
IoT脆弱性、
…

https://www.ipa.go.jp/security/vuln/10threats2017.html

標的型攻撃から身を守る

- よい教材があります（オチが秀逸です）
  - そのメール本当に信用してもいいんですか？
    ～標的型サイバー攻撃メールの手口と対策～
    https://youtu.be/duGNXcEEToU



  - 組織の情報資産を守れ！
    ～標的型サイバー攻撃に備えたマネジメント～
    https://youtu.be/qlcIBHlUKd0

前のスライド、本当に信用してもいい（以下ry

- 一応「IPAのビデオ教材」を周知しているようだ
- 短縮URLを使っているけど大丈夫？
  - 「youtu.be」なので、YouTubeの動画っぽい
  - でも、関係のない動画が出てくるかもしれない!?

いきなり二次元コード
貼られてもなぁ…

- 気になる人は「『動画タイトル』 IPA」で検索
  - https://www.youtube.com/user/ipajp （IPA Channel）
- 少しだけ慎重になることが、あなたと組織を守る

メールによる攻撃の例

リンクをクリックすると
ウイルスに感染する
らしいです。
でも何か違和感
ありませんか？

「授権」って何よ？

ツッコミを入れて情報を見る

- なんでマイクロソフトは（職場の）アドレスを知っているのか？
- 送信元のアドレス、何かおかしくない？
- わざわざリンクを開かないといけないのか？

- 怪しいメールやウェブページの傾向
  - 日本語が不自由（「授権が終了」？）
  - やたらとクリックさせたがる
    （怪しげなウェブページへのリンクがある）
  - 経緯を追いかけると不自然なやりとり（巧妙な標的型）

巧妙な標的型攻撃の事例

- 文科省装い慶大にウイルス送信　過去の実在メール悪用か（産経新聞の報道）
  http://www.sankei.com/affairs/news/160526/afr1605260025-n1.html
- メールには実在する担当者の名前
- 「文科省（ご連絡）」と記した上で「新学術領域研究の中間・事後評価について」との見出し
- もれなくウイルス付き
- メンテされなくなったサーバが踏み台
  →送信者アドレスが不自然で発覚、被害なし

話題のランサムウェア

「ランサム」とは
「身代金」のこと
（ransom）

余談：
ウイルスの「イ」は
小さい「ィ」では
ありません

誤：ウィルス
↓
正：ウイルス

https://www.nhk.or.jp/gendai/articles/3946/index.html

～ではどうすれば脅威から自身や組織を守ることができるか～

情報セキュリティ対策９か条

1 OSやソフトウェアは常に最新の状態にしておこう

新たにひろ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改良プログラムにアップデートしましょう。

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。

7 大切な情報は失う前に複製しよう

家族や友人との思い出の写真など、大切な情報がパソコンの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保管しておきましょう。

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。

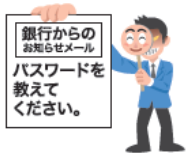
5 ウイルス対策ソフトを導入しよう

ウイルスに感染しないように、コンピュータにウイルス対策ソフトを導入しましょう。(家電量販店などで購入できます)

8 外出先では紛失・盗難に注意しよう

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。

3 ログインID・パスワード絶対教えない用心深さ



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。

6 ネットショッピングでは信頼できるお店を選ぼう

品物や映画や音楽も購入できるネットショッピング。詐欺などの被害に遭わないように信頼できるお店を選びましょう。身近な人からお勧めのお店を教わるのも安心です。

9 困ったときはひとりで悩まず まず相談

詐欺や架空請求の電子メールが届く、ウイルスにより開いているウェブページが閉じないなどの被害に遭遇したら、一人で悩まず各種相談窓口に相談しましょう。(下記参照)

http://www.nisc.go.jp/security-site/files/poster_20150201.pdf

9か条は多い？ では5か条で！

1 OSやソフトウェアは常に最新の状態にしよう！

OSやソフトウェアのセキュリティ上の問題点を放置していると、それを悪用したウイルスに感染してしまう危険性があります。お使いのOSやソフトウェアに修正プログラムを適用する、もしくは最新版を利用しましょう。

2 ウイルス対策ソフトを導入しよう！

ID・パスワードを盗んだり、遠隔操作を行ったり、ファイルを勝手に暗号化するウイルスが増えています。ウイルス対策ソフトを導入し、ウイルス定義ファイル(パターンファイル)は常に最新の状態になるようにしましょう。

3 パスワードを強化しよう！

パスワードが推測や解析されたり、ウェブサービスから窃取したID・パスワードが流用されることで、不正にログインされる被害が増えています。パスワードは「長く」「複雑に」「使いまわさない」ようにして強化しましょう。

4 共有設定を見直そう！

データ保管などのクラウドサービスやネットワーク接続の複合機の設定を間違ったため無関係な人に情報を覗き見られるトラブルが増えています。クラウドサービスや機器は必要な人にのみ共有されるよう設定しましょう。

5 脅威や攻撃の手口を知ろう！

取引先や関係者と偽ってウイルス付のメールを送ってきたり、正規のウェブサイトに似せた偽サイトを立ち上げてID・パスワードを盗もうとする巧妙な手口が増えています。脅威や攻撃の手口を知って対策をとりましょう。

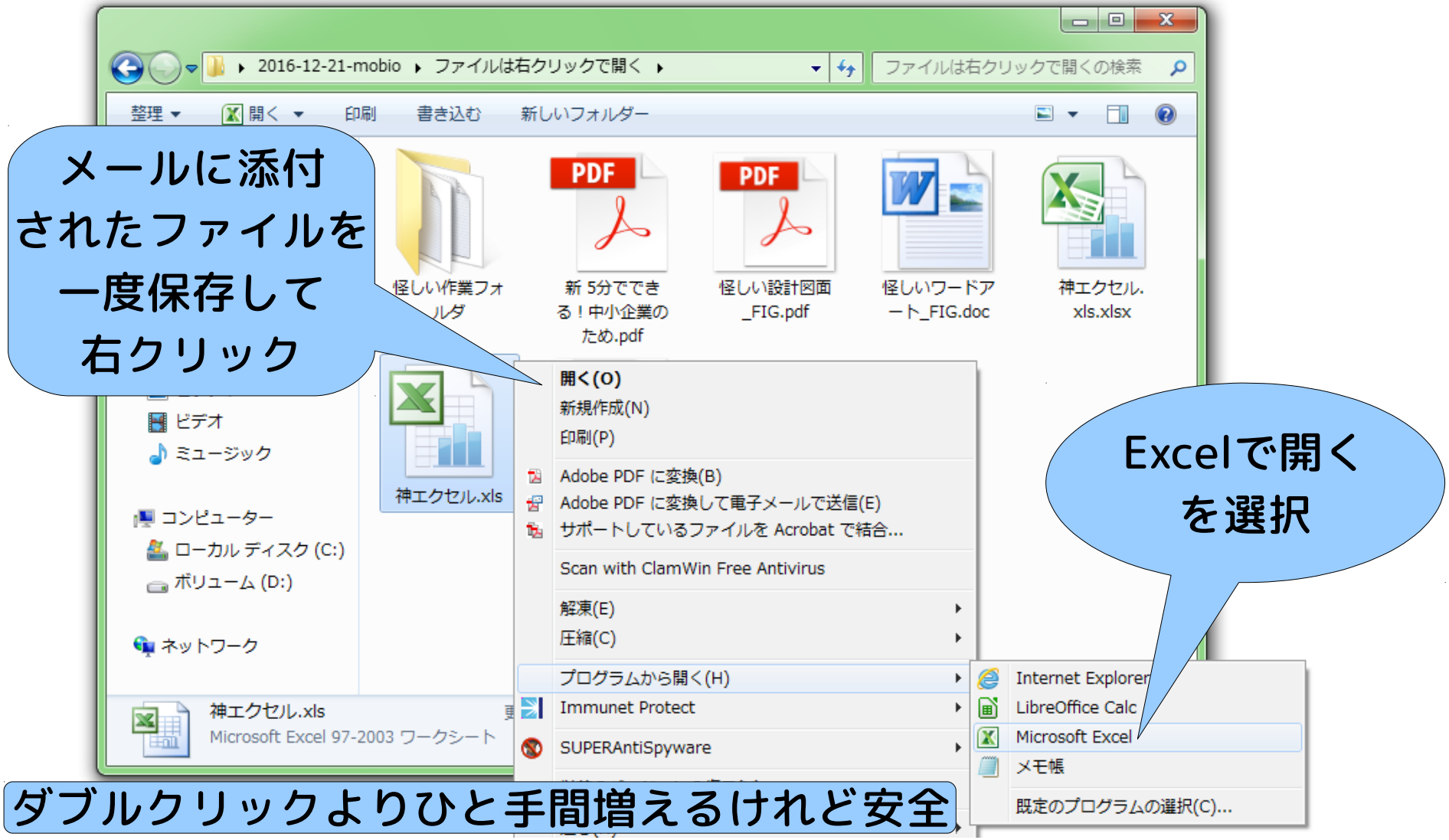
中小企業の情報セキュリティ対策ガイドライン 情報セキュリティ5か条

https://www.ipa.go.jp/security/keihatsu/sme/guideline/

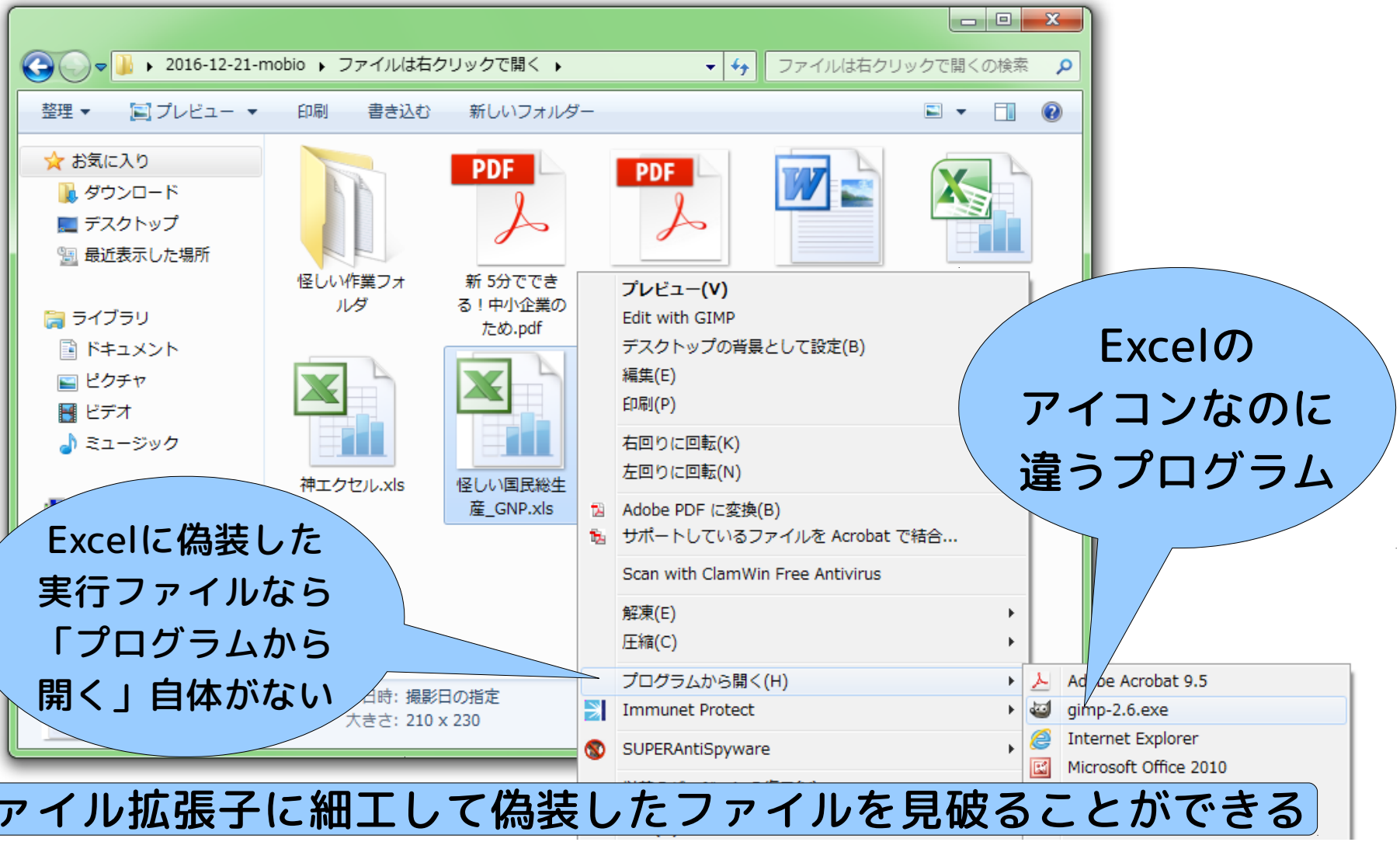
あなたと組織を守る方法とは

- 「9か条」や「5か条」に従えば守れるのでは
- OSやソフトウェアは最新に（第1条）
  - Windows UpdateやAdobeなんとか、Javaなど
    - MyJVN バージョンチェッカでチェック
      http://jvndb.jvn.jp/apis/myjvn/vccheck.html
- ウイルス対策ソフトウェアを導入（第5条）
  - ウイルスのデータも最新に
- 身に覚えのない添付ファイルやリンクを開かない（第4条）
  - OSのアップデートやウイルス対策ソフトで防げない攻撃はこういう経路（ランサムウェアなど）

ファイルを開くときの小ネタ



エクセルに偽装したファイルだと



ファイル拡張子に細工して偽装したファイルを見破ることができる

IDとパスワードの管理

- サービスごとに（可能であればIDも）別々に
  - サービス提供者が攻撃したときの備え
  - 具体例：アマゾンと楽天で別々のパスワードを使う
- 第7位の「ウェブサービスへの不正な…」を防ぐ
  - 組織の第7位、個人の第4位
- 安易なパスワードを使わない
  - 123456、password、qazwsxなど
  - 覚えられない場合は物理的にメモして厳重保管

ミスによる漏洩・紛失

- 宛先を間違えてメール送信
  - 宛先に限らず読み直す習慣、出す前にプチ気分転換
- 情報の紛失
  - 物理的に記憶媒体を紛失してしまう
  - バックアップをとっていなかったので情報が消える
    →第7条「大切な情報は失う前に複製しよう」
  - 「明日学会で発表するパワポを入れたUSBが壊れた！」
    （実話・年に1度ぐらいは耳にする）

紛失・盗難に対する備え

- ノートパソコンやスマートフォンの持ち出し時
- USBメモリなどの持ち出し時

- 対策
  - パスワード・パスコード設定をする
  - 暗号化して記録しておく
  - 情報機器やメディアの入ったかばんを網棚に置かない
    - ひざの上に置く
    - 席に置いてよい状態なら出口に近い側に置く

大切な情報は失う前に複製を

- バックアップを必ず作成する
- 記憶媒体（ハードディスク、USBメモリ、光学メディア）などはいずれ読めなくなる
- 可能であれば遠隔地に置く（できれば近畿以外）
- USBメモリなどにコピーするときは暗号化を
- ランサムウェア（身代金ウイルス）対策にもなる

職場を離れての対策・注意点は？

- 「9か条」や「5か条」に従えば守れるのでは
- OSやソフトウェアは最新に（第1条）
  - スマホも最新に！
- IDとパスワードを適切に管理（第2条・第3条）
- 身に覚えのないファイルやリンクに注意（第4条）
- ウイルス対策ソフトウェアを導入（第5条）
  - スマホにも導入しましょう！
- 信頼できるネットショップを使う（第6条）

不審なリンク vs 試される直感

- SMSで偽のサイトへ
  - Smishingとも呼ばれる（SMS＋phishing）
- アマゾンを騙るサイト
  - 本物ソックリ！
- 個人情報やクレカ情報を要求される
- 見分けかた
  - アドレス・鍵マーク

引用元：
https://twitter.com/nami07889597/status/760019896990175233

信頼できるネットショップの利用

- 詐欺などの被害に遭わないように信頼できるネットショップを利用する
- 本物そっくりのサイト（偽サイト）に注意
  - 購入者に代金を振り込ませて商品を届けない詐欺
    - 振り込み先が個人名義や海外は注意
    - 『「ブランド名」＋激安』の組み合わせ検索で出てくることも
- 偽サイトについては警察も注意喚起しています

職場でも職場以外でも

- 自分はミスしないと思わない
  - 操作ミス、特にタイプミスは誰でもする
  - できるだけコピペですませる
    - 特にメールアドレスなど
  - 操作の完了のクリックやタップは一呼吸おいてから
    - メールを送信するとき
    - 添付ファイルを開くとき
    - ネットショッピングで注文を確定するとき
    - ファイルを消すとき
- ミスしてもリカバーできる（取り返せる）状態に

現実世界もサイバーも区別なく

- 便利な環境があれば攻撃者はそれを利用する
  - 標的型攻撃
  - 偽サイト
- 便利な環境で自分自身と他者を守る
  - セキュリティに気を配る
  - マナーやエチケットみたいなもの
- できることをできるようにやる
  - 他の企業・組織よりマシ
  - ご近所よりマシ

おわりに

- セキュリティについては日々新たな話題が出ます
  - しっかりした情報源を参照して注意と対策を
    - 内閣サイバーセキュリティセンター
      http://www.nisc.go.jp/about/index.html
    - 情報処理推進機構（IPA）セキュリティセンター
      https://www.ipa.go.jp/security/outline/isecabst.html
- システム管理者や経営企画層は職員に啓発を
  - わかりやすくタイムリーに
  - ポイントを絞って情報共有
  - セキュリティは「経費や負担」ではなく「投資・責任」

http://headlines.yahoo.co.jp/hl?a=20160804-00000000-scan-prod

- 困ったことがあれば産技研にご相談ください

付録

経営陣のみなさまへ

「情報セキュリティ対策は、事業の継続を確保し
企業経営の健全な発展をもたらす投資」（内閣府）
http://www.nisc.go.jp/security-site/month/files/shiryou03_katou.pdf

「企業にとって最も重要な資産は信頼」
情報セキュリティ対策は、あなたの会社の重要な情報を
悪意のある者から保護するのにとても重要です。
あなたが外出時に鍵をかけるのと同様に、情報システムにも
予防策を講じる必要があります。あなたの会社を守るため、
情報セキュリティの取り組みについてあなた自身が学び、
従業員を教育しなければなりません。
http://www.nisc.go.jp/security-site/office/manager.html

最後に、もう一つだけ。

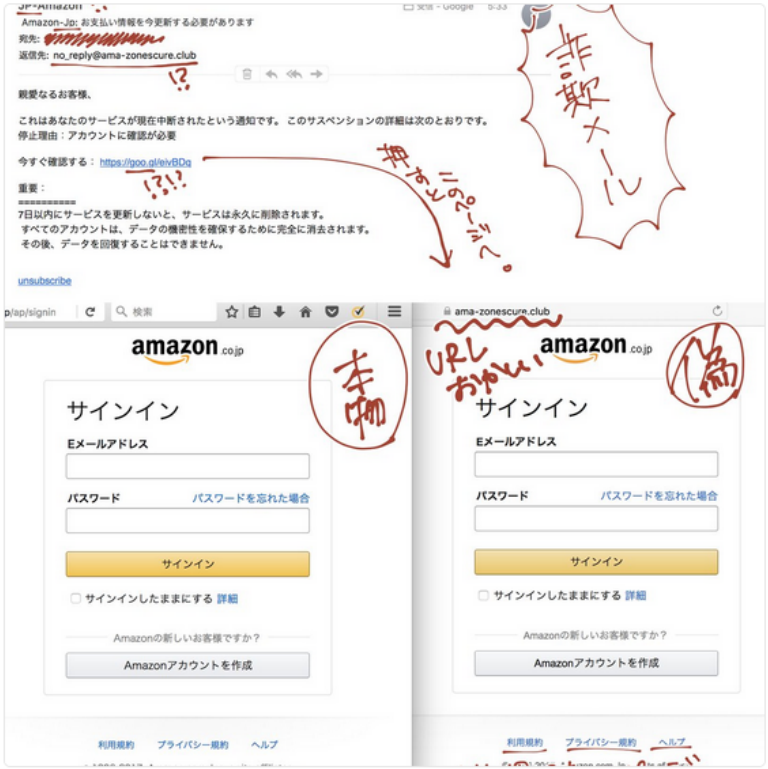
経営者に向けた300ページのサイバーセキュリティ指南書、
パロアルトが無償配布（2016年12月21日 06:00）
http://internet.watch.impress.co.jp/docs/news/1036145.html

「企業経営のためのサイバーセキュリティの考え方の策定について」
…この際、これまでの経営判断の基準に加えて、
リスクの一項目としてサイバーセキュリティの視点を
忘れてはならない。これは経営の根幹にかかわることであるため、
情報システム担当任せにするのでなく、
新たな脅威への対処を先取りする真の「リスクマネジメント」として
経営者がリーダーシップをとって取り組む必要がある。
http://www.nisc.go.jp/active/kihon/pdf/keiei.pdf （H28年8月2日）

おまけ

偽サイト（アマゾン）

朝っぱらからびっくりした！一瞬引っかかりかけた詐欺メールが来たので注意喚起！
おそらく個人情報抜き取り用と思われる偽amazon…！！メアドとURLがおかしかったのと、ノートンが反応してくれたので気付けたけど、サインインページほんとそっくりなので皆さんも気をつけて！



引用元：

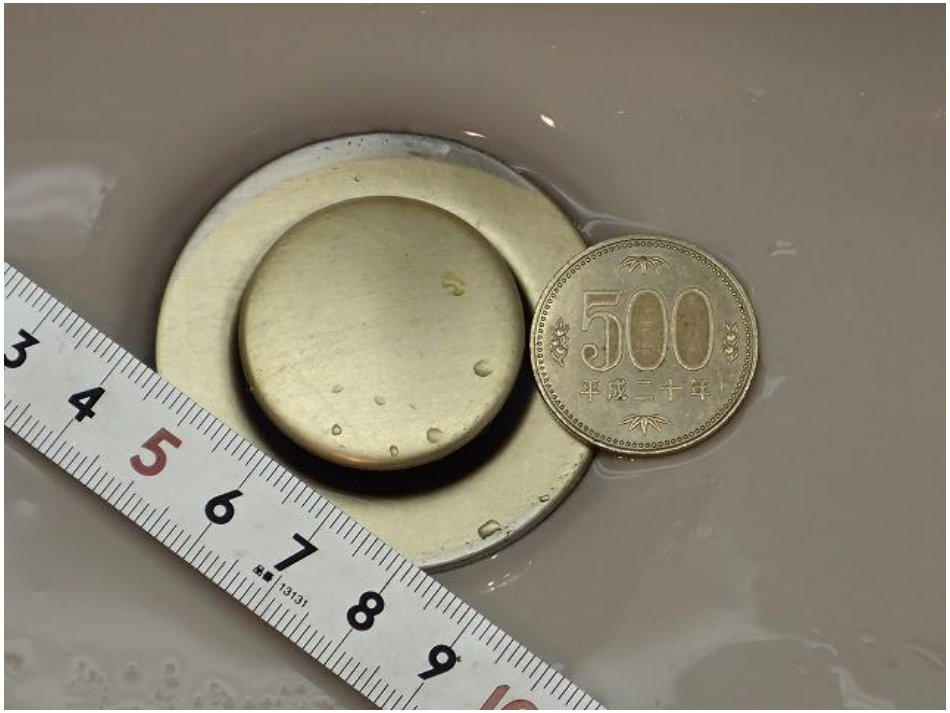
https://twitter.com/yaaaa_0816/status/832693751684354050

話題のゲームにも偽アプリ

http://nlab.itmedia.co.jp/nl/articles/1607/21/news132.html

歩きスマホ・ながらケータイ

物理的に紛失しやすい例



500円玉より小さいものは
紛失するとまず見つからない
（個人の見解です）

違和感を覚えたらタップしない

さすがにバッテリに
ウイルスは感染しない

しかもSony製ではなく
iPhoneである

まさに
「犯罪は社会を映す鏡」

MyJVN バージョンチェッカ

http://jvndb.jvn.jp/apis/myjvn/vccheck.html