テレワーク＆セキュリティセミナー in 滋賀

意外と身近な！ コツコツセキュリティ

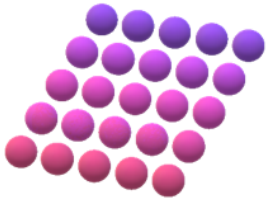
立命館大学 情報理工学部
教授　毛利 公一

RITSUMEIKAN

自己紹介

- 立命館大学 情報理工学部
  教授 毛利 公一
  博士(工学)
- 専門分野
  - オペレーティングシステム
  - 仮想化技術
  - ソフトウェアセキュリティ
- 担当授業
  - オペレーティングシステム
  - ネットワークセキュリティ 他
- https://www.asl.cs.ritsumei.ac.jp/

ちょっとだけ宣伝させてください！



Ritsumeikan University

IoT Security Research Center

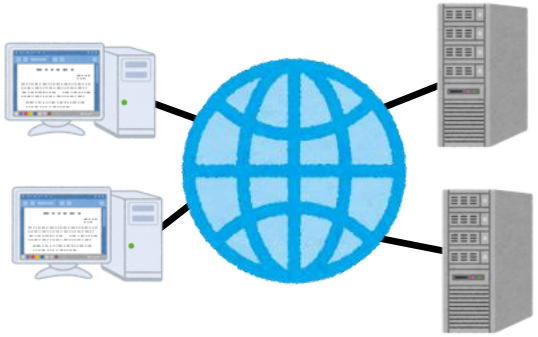
- 2020年8月1日設立しました！
- IoTと情報セキュリティ全般を扱います
  - ハード，ソフト，ネットワーク，暗号・ブロックチェーン
  - 組込み機器，クラウド，情報システム・ビジネスシステム
  - セキュリティマネジメント，法制度，標準化，人材育成
- 共同研究，受託研究，技術指導，企業間連携のハブとしても
- https://iot-security-center.jp

- ご興味がありましたらまずはBKCリサーチオフィスまで！
  - http://www.ritsumei.ac.jp/research/collaboration/about/

なかなか複雑な時代・状況になりました

- かねてからの情報化社会（古い響き・・・）
- オンライン化
- インターネット　←　ここのあたりから怪しくなりますよね
  - ソフトウェアが複雑になってきた
  - ハードウェアも高性能になってきたが単純じゃなくなってきた
  - ネットワークも繋ぐだけならいけるがそれ以上は

あれ？
  - 気付かないうちにECとかeGovとか当たり前になってきた
  - 管理できる範囲が絞れ，統制が容易
  - ただし，企業を越える（サプライチェーン）影響はあり



そして・・・
  - テレワーク・在宅ワーク，オンライン授業，BYOD
  - 管理・統制しづらい環境が加わってくると

これから何が起こるんでしょう・・・

Bring Your Own Device
自分のデバイスを持ってきて使う

RITSUMEIKAN

家でわかるセキュリティ

- 家を守りたいですか？なぜ？

セキュリティのポイント(1)

- 守りたいもの(大切なもの)は何か？
  - 情報資産

では，どう守りますか？

- ここでは「家族や家財を守りたい」として考えてみましょう

本当に守れますか？

それで本当に守れますか？

これでも本当に守れますか？

セキュリティのポイント(2)

- 守りたいもの(大切なもの)は何か？
  - 情報資産
- 弱みはどこか？
  - 脆弱性(必ずしも全ての弱みはわからない)
- 何から守りたいのか？
  - 脅威(攻撃手法)

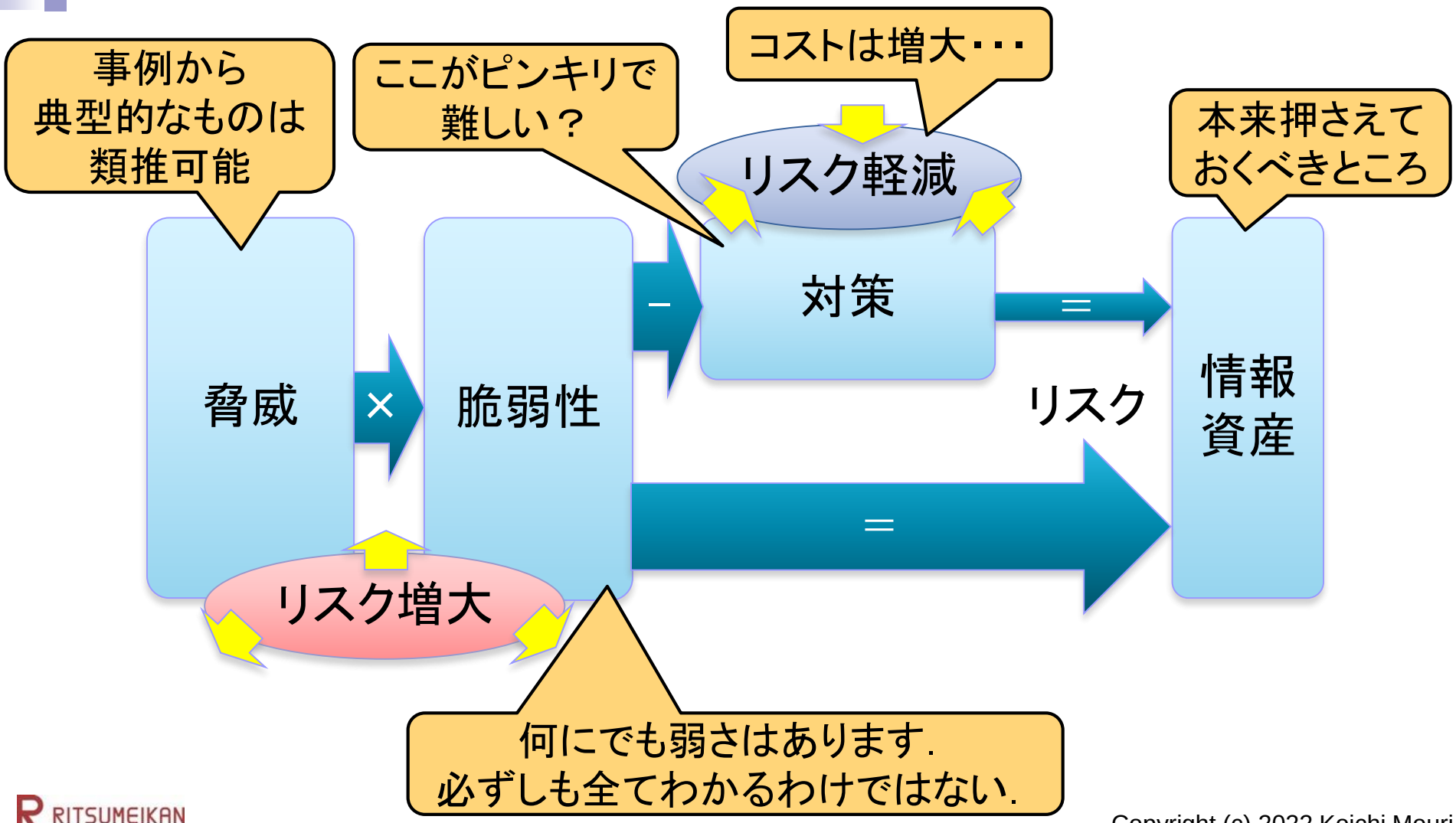
典型的な対策はこんなのでしょうか

セキュリティのポイント(3)

- 守りたいもの(大切なもの)は何か？
  - 情報資産
- 弱みはどこか？
  - 脆弱性(必ずしも全ての弱みはわからない)
- 何から守りたいのか？
  - 脅威(攻撃手法)

- どうやれば守れるか？
  - 対策

それらの関係は・・・



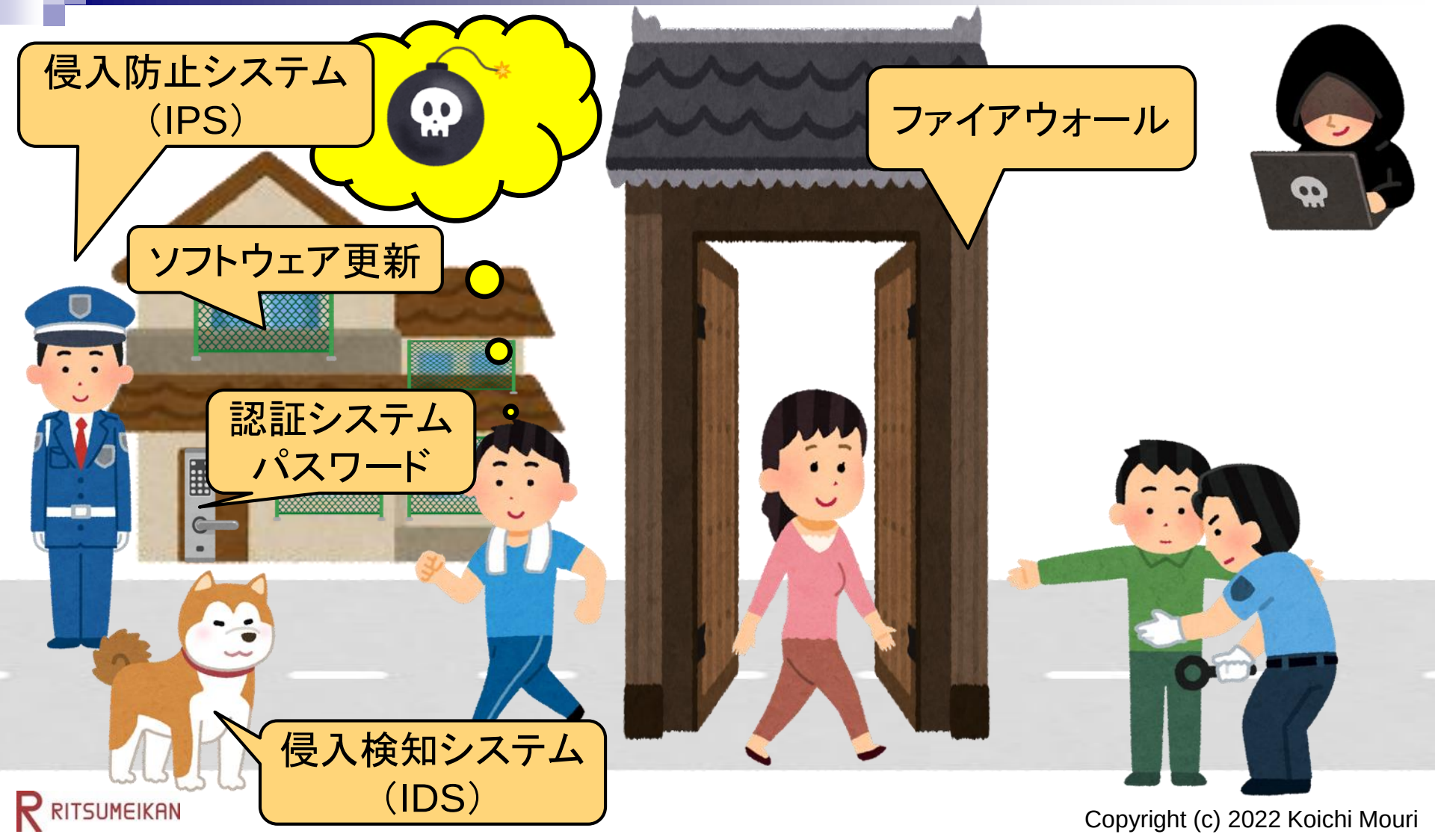
情報資産

- たまに聞きませんか？こんなの

情報資産の大切さ

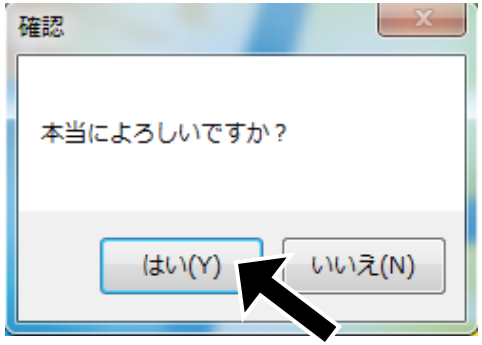
- 情報セキュリティの3要素
  - 機密性・・・秘密が漏れては困る
    - 暗号化，アクセス制御（読み書きできる人の制限）
  - 完全性・・・改ざんされては困る
    - 署名（改ざんが検出できる）
  - 可用性・・・使えなくなると困る
    - 冗長構成（二重化等），バックアップ
- 脅威は情報資産の持つこれらの性質を破ろうとする
  - 本当にありませんか？
  - 日頃から扱っているデータ等の位置づけの整理がオススメ
- これができるのは誰でしょうか？

典型的な対策



最近の脅威と対策を見ていきましょう

攻撃のパターンは実は2パターン



- 利用者が招き入れて動かしてしまう
  - 鍵をかけ忘れていたり
  - どこかでダウンロードしたり
  - 「はい」のボタンを押したり

  してます．「何もしていないのに」というのは・・・

- ソフトウェアの誤動作を誘う
  - セキュリティホール（脆弱性）

- いずれにしても
  - ソフトウェアが悪いことのために動き出します

鍵，開いてますよ！

内閣府、メールを乗っ取られる　不正送信２万件
ＮＰＯ情報照会用

2015/8/3付

内閣府は３日、「内閣府ＮＰＯホームページ」で利用しているメールアカウントが乗っ取られ、不特定多数のアドレスに約２万件の不正なメールが送信されたと発表した。大量発信されたのは７月30日午前０時すぎで、どういった内容のメールが送信されたのかなどは判明しておらず詳細を調査している。

乗っ取られたのは、ＮＰＯ法人の設立状況などを公開している内閣府ＮＰＯホームページの「サポートデスク」のメール。内閣府はサポートデスクの利用者のメール情報などが流出していないか確認している。

サポートデスクはシステム上、内閣府のホームページから切り離されており、内閣府の内部情報の流出はないという。

管理先の民間業者が短くて推測しやすいパスワードを使用していたことが原因とみられる。乗っ取られたアカウントを使用停止するとともに、乗っ取り防止策を検討している。

nikkei.comの記事より

教訓：パスワード

- パスワードは最後の砦
  - パスワードは英数字・大文字小文字・記号を使う
  - 長いほど良い．私は16文字以上にしています
  - Webサービスではサイト毎・サービス毎に変える
  - パスワードは覚えません．ブラウザに覚えさせます
- 古い常識は更新を
  - パスワードを紙に書いて貼るな
    - どうしても手入力しないといけないもの
    - メモくらい良いじゃん．ただ，人目は気にしましょう
  - パスワードは定期的に変更せよ
    - 事実上，あまり意味は無い
    - ただし，人事異動等があればやるべき

ある日のメール（本物）

三井住友カード　迷惑メ…- frigg mail　2021年2月24日 20:24

『【重要】三井住友カード株式会社からの緊急のご連絡』

宛先: 毛利公一

SMBC　SMBCグループ

三井住友カード

いつも弊社カードをご利用いただきありがとうございます。
昨今「三井住友銀行」や「SMBC」「三井住友カード」などを装った電子メールを送り、お客さまの個人情報等を
入力させる詐欺が発生しています。メール記載のＵＲＬをクリックせずにメールの削除をお願いいたします。
つきましては、以下へアクセスの上、カードのご利用確認にご協力をお願い致します。
予めご了承下さい。

▪ ご利用確認はこちら

https://smbc-card.sekef.com

▪ 注意事項

※本メールはご登録いただいたメールアドレス宛に自動的に送信されています。
※本メールは送信専用です。ご返信いただきましてもお答えできませんのでご了承ください。
※変更後、48時間以内に発効する必要があり、期間中は使用できません。
※カードの個人情報によっては電話で連絡する場合もございます。
※正確な情報は必ず記入してください。

▪発行者

三井住友カード株式会社
https://www.smbc-card.com
〒105-8011 東京都港区海岸1丁目2番20号 汐留ビルディング

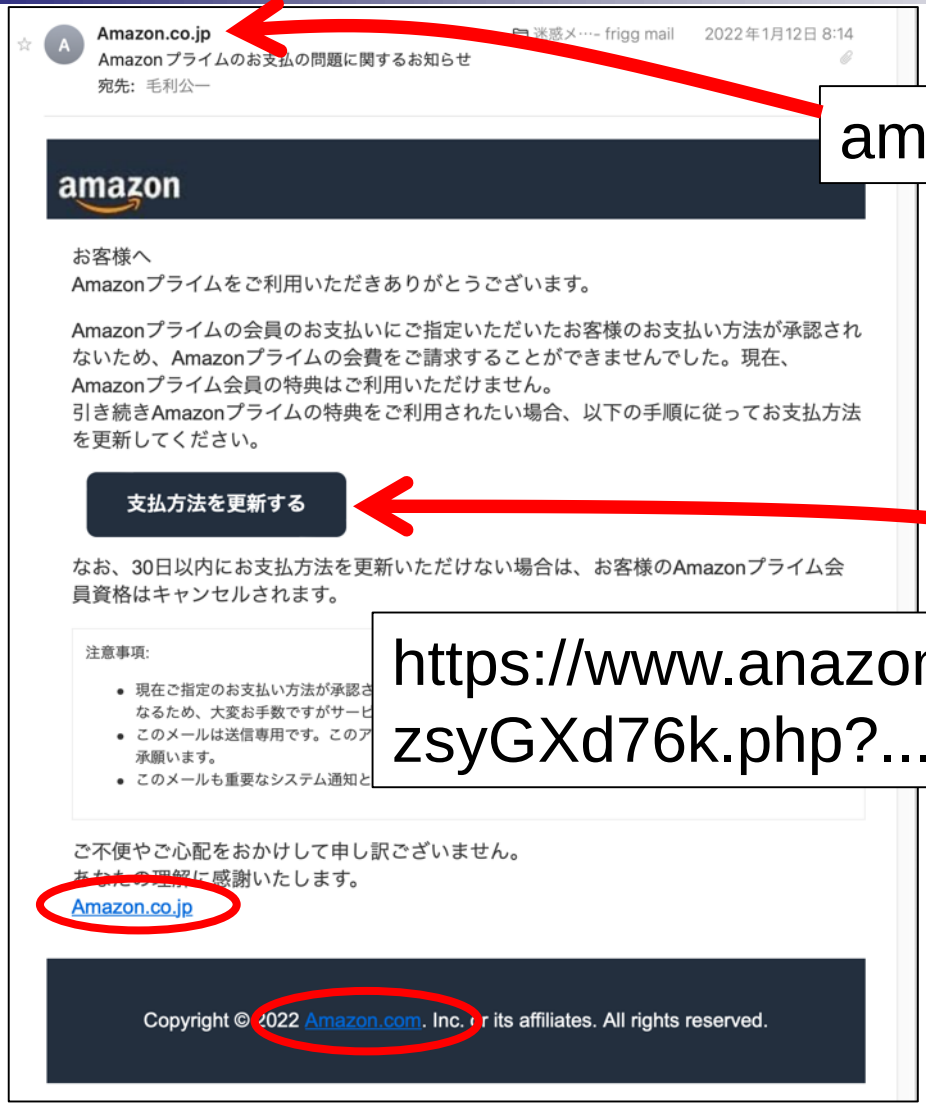
Copyright (C) 2021 Sumitomo Mitsui Card Co., Ltd.

詰めが甘い

▪ ご利用確認はこちら

https://smbc-card.sekef.com

ある日のメール（本物）その2



amazon-co-jp@qqjcgnp.cn

やっぱ甘い

さっきよりマシ

https://www.anazom.co.ip.barborium.shop/zsyGXd76k.php?...

Amazon.co.jpか
Amazon.comか
甘い

ある日のメール(本物)その3

ここ！

Apple 迷惑メール - frigg mail 2018年11月20日 17:22

{spam} アラート:あなたのアカウントは閉鎖されます。

宛先: 毛利公一

Appleをご利用いただき あり がと うございますが、ア カウント管理チームは最近Appleアカウントの異常な操作を検出しました。アカウントを安全に保ち、盗難などのリスクを防ぐため、アカウン ト管理チームによってアカウントが停止されています。次のアドレスでアカウントのブロックを解除することができ ます。

注:アカウントを再開するときは、情報を正確に記入してください。3つのエラーが発生すると、アカウントは永久 に禁止されます。 このアドレスでアカウントを復元してください:

リカバリアカウン ト

すぐに復元してください！盗難に よるアカウントの紛失を防ぐため、アカウント情報が時間内に確認されない場合、アかウント管理チームはアカウ ントを完全に凍結します。アカウントを再開する前に、アカウントを再登録しないでください。でなければ、アカウ ント管理チームはアカウントを 凍結することになっております。

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. Apple Distribution International, Hollyhill Industrial Estate, Hollyhill, Cork, Ireland. すべての権利を保有しております。

RITSUMEIKAN

こんなの出ました

あれ？
似たサイト
知ってます

双子？

そもそもクリックしないで！

https://u2378520.ct.sendgrid.net/wf/click?
upn=9xvkd0i977MJD7aGFt1lbd93Vhk9Vh-2BFalMe2i4-
3rML70dDaV4n1V27NuGJif5aCnKtBHxBRWyECQw4rSjGmvNnHYOkFW2szbiA2i
GbxB7hU-2BWvgqj9xKA82MBGzbr
2FSLxmZx7RLm-2FHXjJ0um85zRV
2FmHpDrQmD2Fbm0BL9ya8kJ5G3

こういう，
長いやつは
特に危ない

Webサイトにアクセスするだけで

表示だけでウイルス感染、正規サイトに不正広告の「手口」

2015年09月04日 15時09分 ツイート G+ B!

７月以降、ウェブサイトの広告を表示するだけでウイルス感染する事例が多発している。国内から９００万件以上のアクセスがあると推測され、オンライン銀行詐欺ツールやランサムウェアが忍び込んでいる可能性が高い。（ＩＴジャーナリスト・三上洋）

ウェブサイトのバナー広告表示→自動転送されて脆弱性攻撃サイトへ→ウイルス感染

一般ユーザーが被害にあう、厄介なウイルス感染の手法が広まっている。ウェブサイトのバナー広告を使ったもので、最悪の場合は表示するだけでウイルス感染し、ネットバンキングからお金を盗みとられるなどの被害が出てしまう。

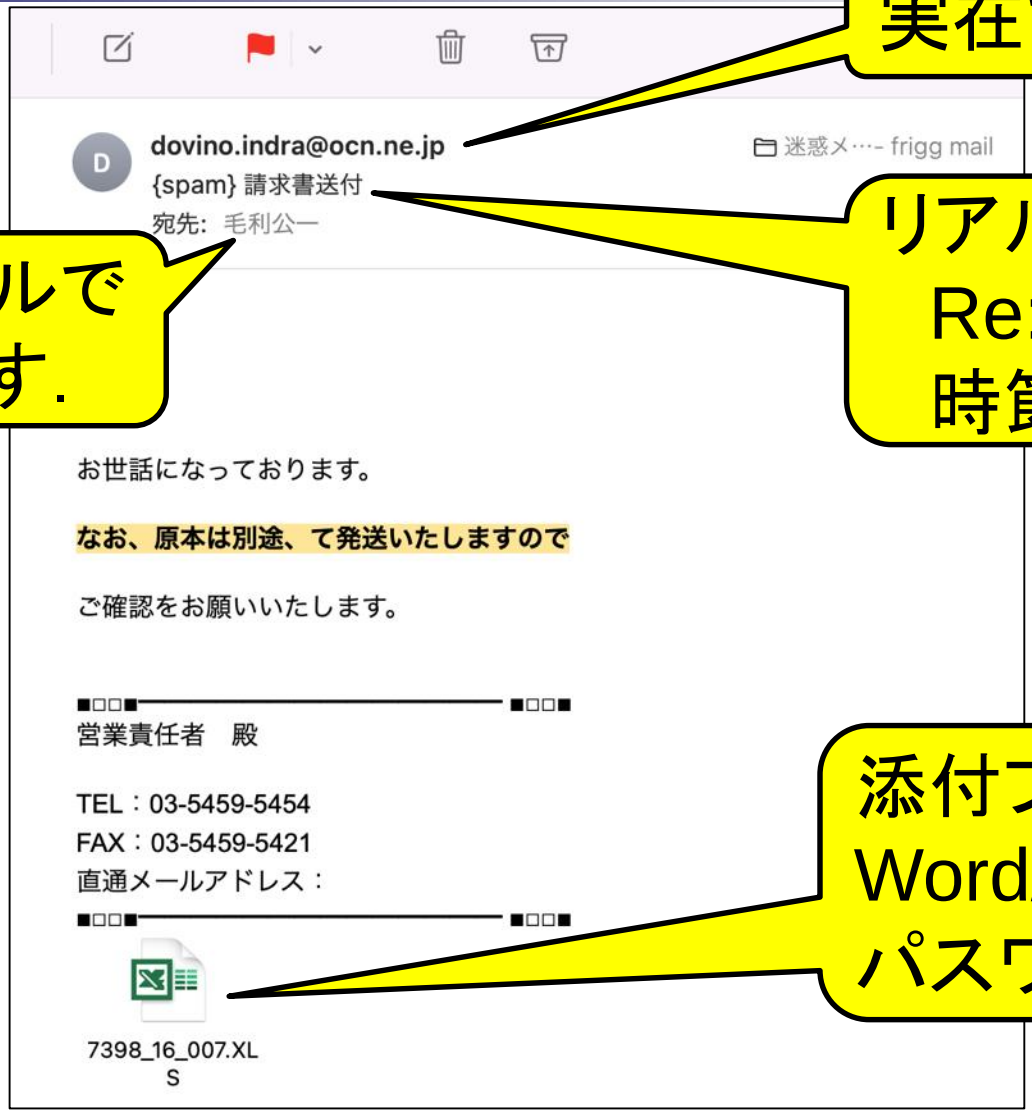
yomiuri.co.jpの記事より

RITSUMEIKAN

教訓：フィッシング

- メールのリンクはクリックするな！強く疑え！！
  - URLのドメイン名を意識すると少し強くなれる！
    - https://www.amazon.co.jp/deal/1234...
    - メールの送信者とリンク先は，表面上と実体が一致しているか
    - さらに，それらが仕事関係であるかどうかを想像
    - その人は普段からそんなメールを送ってくるか？
  - 文章には厳しく
    - 日本語がおかしいぞ
    - 文章先頭の名前が一般的な「お客様」，メアドの@の左側
  - 親切心は不要．基本は無視で良い
- 無視しきれない．判断できない．確認したい
  - 別の手段で確認（電話）
  - リプライではなく，メールを新規作成
  - リンクを多用することがわかっていれば，事前にルール作成も

最近の流行はEmotet



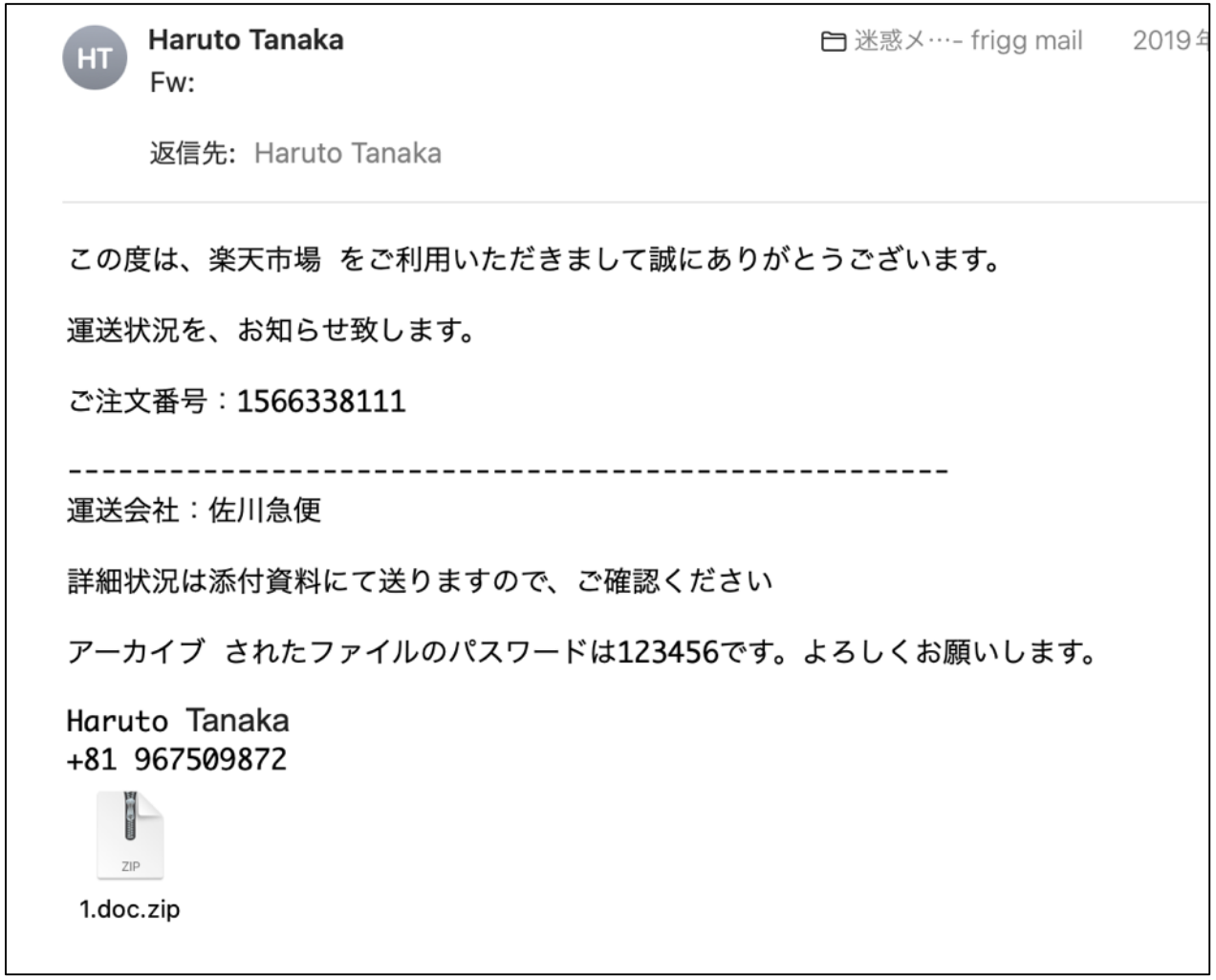
実在するアドレス

リアルなタイトル
Re: なんたら
時節ネタも

最初はメールで
やって来ます.

添付ファイル
Word/Excel
パスワード付きzip

もうーつ



HT **Haruto Tanaka** 迷惑メ…- frigg mail 2019年

Fw:

返信先: Haruto Tanaka

この度は、楽天市場 をご利用いただきまして誠にありがとうございます。

運送状況を、お知らせ致します。

ご注文番号：1566338111

運送会社：佐川急便

詳細状況は添付資料にて送りますので、ご確認ください

アーカイブ されたファイルのパスワードは123456です。よろしくお願いします。

Haruto Tanaka
+81 967509872

ZIP
1.doc.zip

Emotetの概要

- ファイルをオープンするとマクロが動き，
  ユーザにEmotetをダウンロード・実行させるように
  巧みに誘導
  - マクロを有効に（コンテンツの有効化）しない！
- Emotet感染後
  - 重要なファイルを盗み，外部サーバに送信
    - メール関連情報，認証情報などの情報
  - 別のマルウェア（ランサムウェア等）のダウンロード等
  - 内部PCへのEmotet伝染
  - 外部へのEmotetメールばらまき
    - 取引先を巻き込んでしまう可能性がある
- 詳しくは IPAやJPCERT/CCの情報を
  - https://www.ipa.go.jp/security/announce/20191202.html

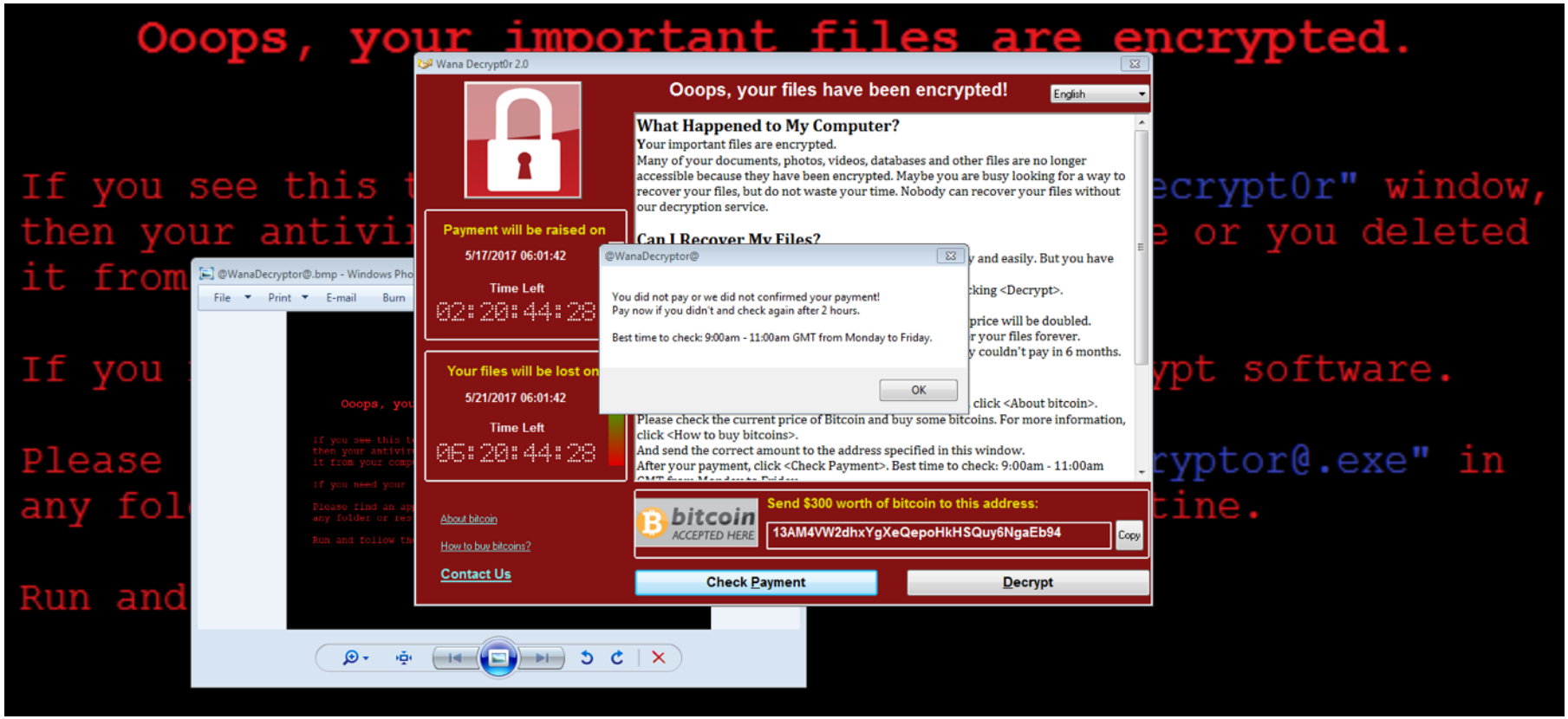
教訓：添付ファイルも危険

添付ファイルは開くな！！添付ファイル撲滅！

- 添付ファイルで重要なファイルを送受信は止めましょう
  - 機密性のあるものをメールするのは良くない風習．
    パスワード付き添付ファイルに意味は無いし，不便なだけ．
  - 機密性不要のものは絶対悪とまでは言えないのですが，
    添付ファイルを容易にクリックする土壌に．
    - 特にWord/Excelはやめたい．せめてPDF
- OneDrive等オンラインストレージの活用がよい
  - 取引先毎にフォルダを作成して共有
  - フォルダにファイルを格納
  - メール等でそれを案内

ランサムウェアも困りますよ･･･

checkpoint.co.jp



騒ぎになりました

nikkei.comの記事より

サイバー攻撃、日立でシステム障害　企業・官公庁が警戒

2017/5/15 10:58 (2017/5/15 13:08更新)

共有　保存　印刷　その他

世界中を襲う大規模なサイバー攻撃が発覚してから最初の平日を迎えた日本では、日立製作所の社内システムに障害が発生したことが分かった。企業や官公庁は警戒を強めており、出社した従業員に対し不審な電子メールを開かないよう注意喚起するなど対策を急ぐ。15日朝時点で公共交

今回のサイバー攻撃は「ワナクライ（ＷａｎｎａＣｒｙ＝泣き出したい）」の名で急速に広まった。パソコンやサーバー内のデータを勝手に使えなくし、元に戻す見返りにビットコインでの金銭を要求する「ランサム（身代金）ウエア」と呼ばれるウイルスが使用された。日本時間の12日（金）深夜～13日（土）未明に発生した。欧州警察機関（ユーロポール）のウェインライト長官は14日、英民放ＩＴＶに対し、被害が少なくとも150カ国で20万件以上に上ると述べた。

今回のサイバー攻撃で基本ソフト（ＯＳ）「ウィンドウズ」の欠陥を突かれた米マイクロソフト（ＭＳ）は、ブラッド・スミス社長兼最高法務責任者が14日、声明を発表。「技術部門、利用者、政府が手を携え、サイバー攻撃への対策を講じるべきだ」として、官民や部門を超えた協力を呼びかけた。同社は欠陥を修正するソフトを無償公開しており、未対応のパソコンへの適用を強く推奨している。

もひとつ教訓：ランサムウェア

- ランサムウェアの怖さ
  - 接続された機器すべてがやられる可能性が含む，バックアップ！
  - 暗号化されたデータを元に戻すにはお金がかかるたぶん払えちゃう
  - お金を払ったらデータは元に戻るかも？しかし，データを消すとは言っていない．流出も
- 繋がないという原始的な手段も有効
  - 定期的なバックアップはとってますよね・・・？
  - バックアップのメディアは入れっぱなしじゃないですよね・・・？

さて，いろいろ見てきましたが・・・

コンピュータは怖い？面倒？金食い虫？

- いえ，今こそ正面から切り込んでいくタイミングなのです
  - コンピュータは身の回りに
  - 何でもネットワークに繋がって
  - 産官学，子供さん＆お孫さん
- コンピュータは便利ですのでぜひ活用を！
  - 企業の発展のために情報資産の活用を！
  - 情報資産の活用と安全確保は第一義的には自社の責任！
    - 定型のものはパッケージ・外注でも良い
    - 自社の宝は自社で

上手なお付き合いを！

- セキュリティについては現実世界と同様に
  - 情報資産の価値，脆弱性，脅威の分析
  - 対策の選択とコストのトレードオフ
- 日常的には
  - 常に怪しい人に狙われているという「心がけ」が大切
    - パスワードの運用は大丈夫？
    - Webやメールなど外に触れるところ，リンクとファイルは鬼門
  - 技術的側面では基本的な対策を怠らず，
    - ソフトウェアの更新は自動化（PC，スマホ，ルータ等すべて）
    - やっぱりバックアップが大切
    - 高度なセキュリティ装置の導入は十分検討して適切なレベルで
  - 継続は力なり
    - 定期的な再分析，保守切れの機器やソフトウェアの置き換え
    - 勉強会・研修の実施，（実施可能な）ルール作り