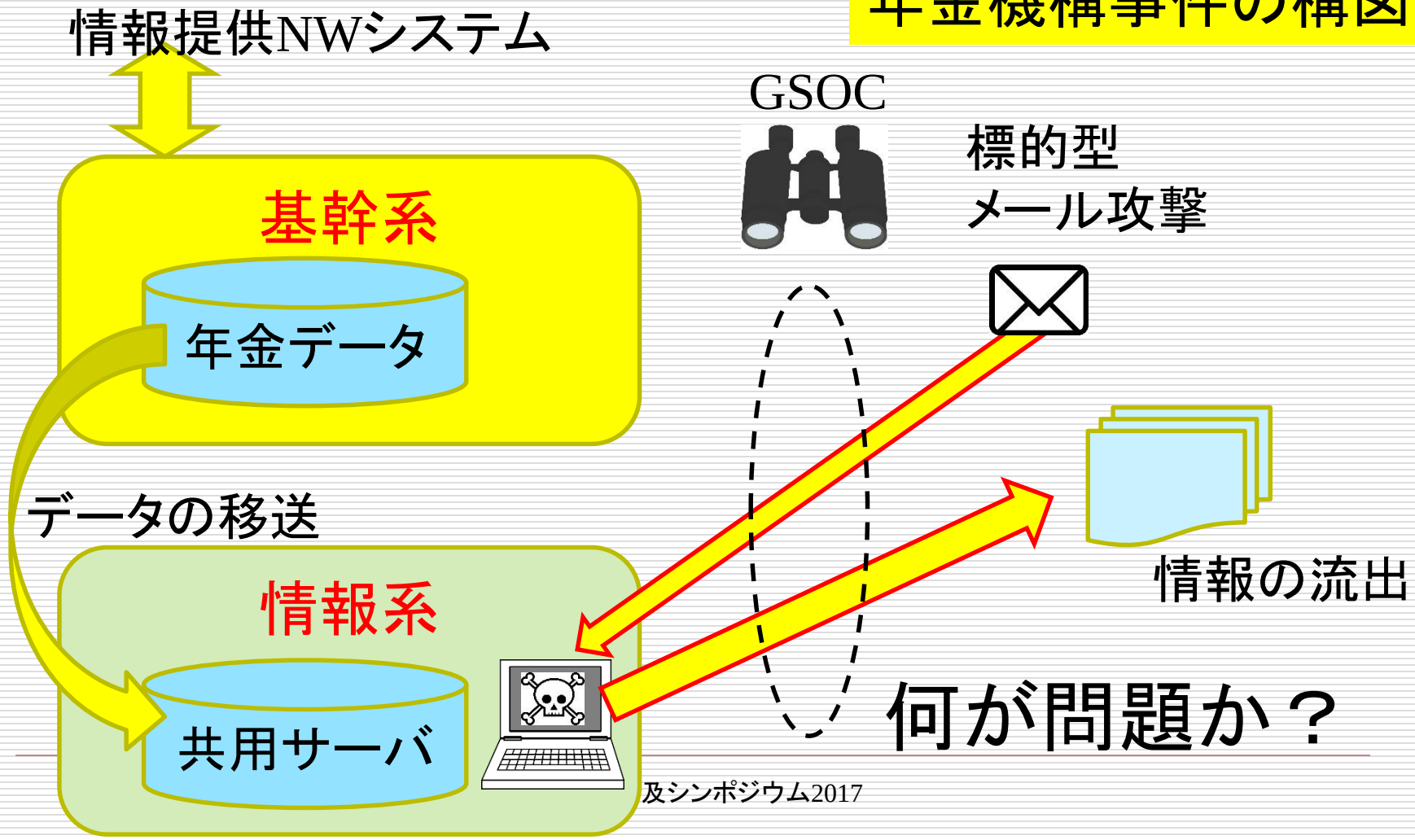
メールなりすまし対策の普及のために

立命館大学
情報理工学部
上原哲太郎

標的型メール攻撃が止まらない

年金機構事件の構図



フィッシング事案も相変わらず

- 昨年8月以降大学を狙ったフィッシングが頻発
  - 山梨大学、立教大学、上智大学、関西学院大学、九州産業大学、中央大学、筑波大学…
- この中で関西学院大学に大きな被害
  - Office365を配付、教職員も利用
  - OneDriveも有効にしていた模様？
  - 職員のアカウントから名簿流出

標的型メール攻撃対策訓練大流行
しかし開封率は？

- NISCによる政府職員6万人向け訓練（H.23）
  - 1回目　添付ファイル　開封率　10.1%
  - 2回目　リンク型　開封率　3.1%
- LAC社「ITセキュリティ予防接種」訓練
  24社・団体アンケート（H.24）
  - 1回目平均　36.1%
  - 2回目平均　16.4%　ただし1社はむしろ上昇
- NRIセキュア社「標的型メール攻撃シミュレーション」集計（H.23~25）
  - 従業員の開封率は16～22%
  - 役員の開封率は28～31%　約1.5倍

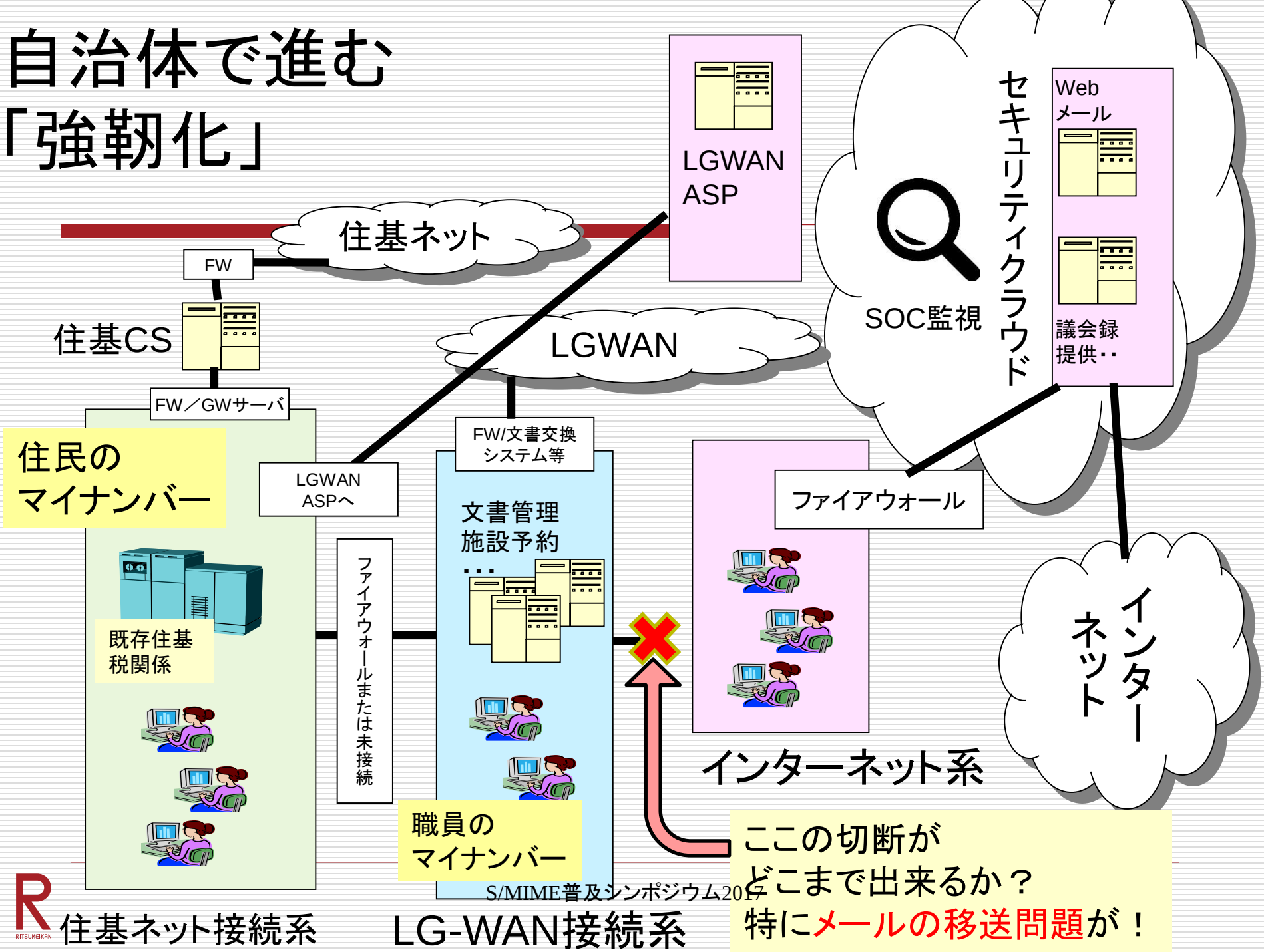
開封率を問うことの意味は？！

- どうせ0%にはならないしできない
  - 人のアノマリ解析力は高くない（正常バイアス）
  - 敵は成功するまで繰り返すので
    次第に見分けはつかなくなる
- 組織内で1人でも開封すれば攻撃は成功
- 標的型メール開封を責任問題にすれば
  業務効率低下は明らか
- 「開封後の初動」を訓練するために行うもの
  - 「ばらまき型メール」では効果あるが
    相手を絞った標的型メールでは効果は疑問
- メールの危うさに気づいてもらうためのもの？

事故の原因は何なのか

- 重要なデータを
  インターネット直接接続環境で扱う
  - リスクポイントが多すぎて完全な対応は困難
- メールを送信者確認せずに扱う
  - 目視による確認の無意味
- エンドユーザが実行ファイルを直接扱う
  - 「実行形式による暗号化」の愚

自治体で進む「強靭化」


LGWAN
ASP
住基ネット
FW
住基CS
LGWAN
セキュリティクラウド
Web
メール
SOC監視
議会録
提供・・
FW／GWサーバ
住民の
マイナンバー
LGWAN
ASPへ
FW/文書交換
システム等
文書管理
施設予約
・・・
ファイアウォール
既存住基
税関係
ファイアウォールまたは未接続
インター
ネット
インターネット系
職員の
マイナンバー
ここの切断が
どこまで出来るか？
特にメールの移送問題が！
住基ネット接続系
LG-WAN接続系

広がる「メール無害化」だが…

- 本来の意図は「テキストメールのみの利用」

- 添付ファイルを使用したいという声に押されて「添付ファイル中のウィルスになりうるデータの削除」という方向に
  - マクロの除去、PDF/docxの「冗長部分」の除去など
- しかし弊害も少なからず
  - 電子署名が無効になるetc.

H25.3「標的型攻撃に対抗するための通信規格の標準化動向に関する調査」

- いくつかの規格に関し動向調査
  - HTTP周辺（HTTP Authなど）
  - メール周辺（S/MIME, DKIMなど）
    - メールについては
      なりすまし防止の規格は複数成立
      →普及状況やその問題点を整理
    - いくつかの事業者にヒアリング
      ISP，証明書事業者，学術有識者と討議
- 調査結果はこちら
  http://www.soumu.go.jp/main_sosiki/joho_tsusin/hyojun/02tsushin04_03000122.html または上記タイトルで検索

この辺の
状況は
進展してない


総務省｜標的型攻撃に対抗するための通...
www.soumu.go.jp/main_sosiki/joho_tsusin/hyojun/02tsushin04_03000
よく見るページ
Firefox を使いこなそう
Web スライス ギャラリー
おすすめサイト
総務省
MIC
Ministry of Internal Affairs and Communications
ご意見・ご提案
English
Google™カスタム検索
サイト内
関連サイト
ここに検索語句を入力
検索
アクセシビリティ閲覧支援ツール
総務省トップ > 政策 > 情報通信(ICT政策) > 研究開発・標準化の推進 > 標的型攻撃に対抗するための通信規格の標準化動向に関する調査結果
標準化の推進
ITUへの寄与について
用語解説
各種申請・届出の受付
リンク集
このホームページに関する問い合わせ先
標的型攻撃に対抗するための通信規格の標準化動向に関する調査結果
近年、特定の組織を標的にしたサイバー攻撃(標的型攻撃)による被害が問題となっています。標的型攻撃には、初期の段階で関係者になりすましたメールに付随したマルウェアや、フィッシング的手法を用いて、組織内にあるICT機器自体の制御を奪うケースがあります。このため、メールのなりすまし防止に使われる技術の標準化は、このような標的型攻撃に対する耐性を高めるものとして期待されています。　このような背景から、このたび、なりすまし防止に向けた取組の一助となることを期待して、これらの標的型攻撃に対抗するための要素技術の導入と運用方法を含めた標準化動向を調査し、以下のとおり調査結果を取りまとめました。
標的型攻撃に対抗するための通信規格の標準化動向に関する調査結果
お問い合わせ先
情報通信国際戦略局　通信規格課
TEL：03-5253-5763
ページトップへ戻る
サイトマップ
プライバシーポリシー
当省ホームページについて
総務省
Copyright © 2009 Ministry of Internal Affairs and Communications All Rights Reserved.

調査の概要

- S/MIMEを中心に運用にかかる問題点を整理
  - なりすまし防止に力点　暗号化を主眼にしていない
  - DKIMやSPFとの住み分けを意識
    - ドメイン認証　vs　アドレス認証
    - S/MIMEは「認証だけなら」スモールスタート可能
- 狙いは「運用のベストプラクティス」の抽出
  - 意外と「ありそうでない」
  - 出口として国際標準規格での補助的文書を目指す

S/MIME普及阻害要因とその緩和

- 電子証明書のコスト
  - 個人の私用なら無料の時代（Comodo他）
  - しかしStartCom問題で後退…
- 受信側の非対応
  - かつてより改善された
    - ケータイ　Android WebMail
  - 受け取っても「これ何ですか？」→サポートコスト
- 署名付きメールを受け取らない環境（さすがに減った）
- アプリケーション上でのわかりにくさ
  - SSL/TLSのような統一UIの不在
- 「過去の証明書で署名/暗号化されたメール」の扱い
  - mbox内のメールは復号しておくべきか否か？

S/MIME環境は確かに改善している

- WebMail系
  - Office365のOutlook Web Appはサポート
    - Exchange Online 2010以降でサポート
    - ただし要ActiveX controlなので
      Internet Explorerのみ（！）
  - Gsuites for EnterpriseのGmailがサポート
- アプリケーション系
  - Windows8当時S/MIME未サポートだった
    WUP版の標準Mailクライアントが、
    Windows10世代になってS/MIMEサポート復活

まずは到達したい目標

- 通常の業務において受け取るメールの
  ほとんどを送信者が確認可能なものにして
  かつ分かりやすく利用者に伝える
  - そうすれば送信者認証がないメールは
    「不審なメール」になる
- さらに送信者評価＝レピュテーションを加える
  - レピュテーションに基づいて攻撃を機械的検知
- これで「相手が既にマルウェア支配下にない限り」
  大丈夫

次はこのような世界を目指したい

- メールを思い切って業務システムから切り離しては?
  - 自治体で行った例に倣う
  - ワークフロー見直しの良い機会
- その上で「なりすまし防止」が確実なメールのみ業務システム上に取り込む
  - マルウェアリスクは送信者認証と実行ファイルの排除で十分に下げられる
  - 相手が乗っ取られていないことが前提
- これをお互いに行うことで送信者認証メールを普及させることが出来るのでは
  - 送信者は最後はヒトが確認しないとセキュリティは保てない
  - DKIMなら導入コストは低い
  - S/MIME普及でさらに暗号化メール普及を狙える

今足りないものは？

- 「ユーザインターフェース」のコンセンサス
  - S/MIME署名結果の見せ方や壊れた署名の扱い
  - DKIM/SPFなどドメイン認証の結果の扱い
- レピュテーション基盤の確立
  - ドメインによる評価、アカウント別の評価
- S/MIMEの証明書運用のベストプラクティス
  - 企業等の組織では証明書は一元管理が現実的
- DMARC運用経験の蓄積