標的型攻撃からの課題抽出

門林雄基
奈良先端科学技術大学院大学
情報科学研究科

アウトライン

* なぜ標的型攻撃に弱いのか
  * ７種の問いかけ
* 標的型攻撃とは何なのか
  * そのキーワードで終わらせないために

1. 専門家 vs ユーザー

* 専門家がユーザの安全性を確保するのは果たして正しかったのか
* 専門家とはいかなる能力をもった集団か

他の領域に学ぶ

* 一般市民は健康に無関心か？
* 医療従事者は一般市民の健康を確保するか？
* 自己管理が前提では？
* 専門家の常時監督下（入院）ではあらゆる活動が制限されるのでは？

他の領域に学ぶ

* 新型インフルエンザの早期警戒情報には様々な公共媒体が豊富に用いられるが

  オフィスソフトや基幹OSの早期警戒情報が同様に扱われないのはなぜか？

今おきていること

JavaScript は有効なまま

古いアクロバット

アクロバット？使わないけど
そういえば入ってるね

専門家がなんとかしてよ
専門家だろ、俺を守れ

セキュリティ？ファイア
ウォールとアンチウィルス
入れてあるよ

PDF ファイル閲覧ソフトウエア Adobe Reader 及び
PDF ファイル作成・変換ソフトウエア Adobe Acrobat には
複数の脆弱性があります。結果として、遠隔の第三者が
細工した PDF ファイル等をユーザに開かせることで
Adobe Reader や Acrobat を不正終了させたり、ユーザの
PC 上で任意のコードを実行させたりする可能性があります。

問題構造

ICT資産管理能力の欠如

JavaScript は有効なまま
脅威認識の欠如

自己責任原則の欠如

正しい技術的知識の欠如

多様でないリスクコミュニケーション

2. クリティカル vs コモディティ

* 重要インフラでコモディティ技術を使っていて大丈夫か

* 重要インフラ向けOS とは
* 重要インフラ向けファイルサーバとは
* 重要インフラ向けアプリとは

ミッションクリティカル-*

	調達	構成	保守
ハードウェア			
OS			
ミドルウェア			
アプリケーション			
ネットワーク			
ホスティング			

それぞれ
セキュリティサービスレベルをどう規定するか？

3. ID管理 vs ふるまい管理

* IDとパスワードだけでいつ何時でも使えるのは果たして正しかったのか
* 認証が終わったらノーチェックでいいのか
* 認証と権限管理を混同していないか
* 高度な認証であれば良いのか

あらゆるIDが狙われる

標的	マルウェア	ID	事象
RSA	Poison Ivy	SecurID	**偽造**
SCADA	Stuxnet	**電子証明書**	**偽造**
DoD	Sykipot	Smart Card	**偽造**
Brazil	DNSChanger	DNS	**偽造**

4. 暗号化 vs 仮想プライベート

* いちいち暗号を使わないためのVPNは果たして正しかったのか

* 多層防御を貫通している場合も

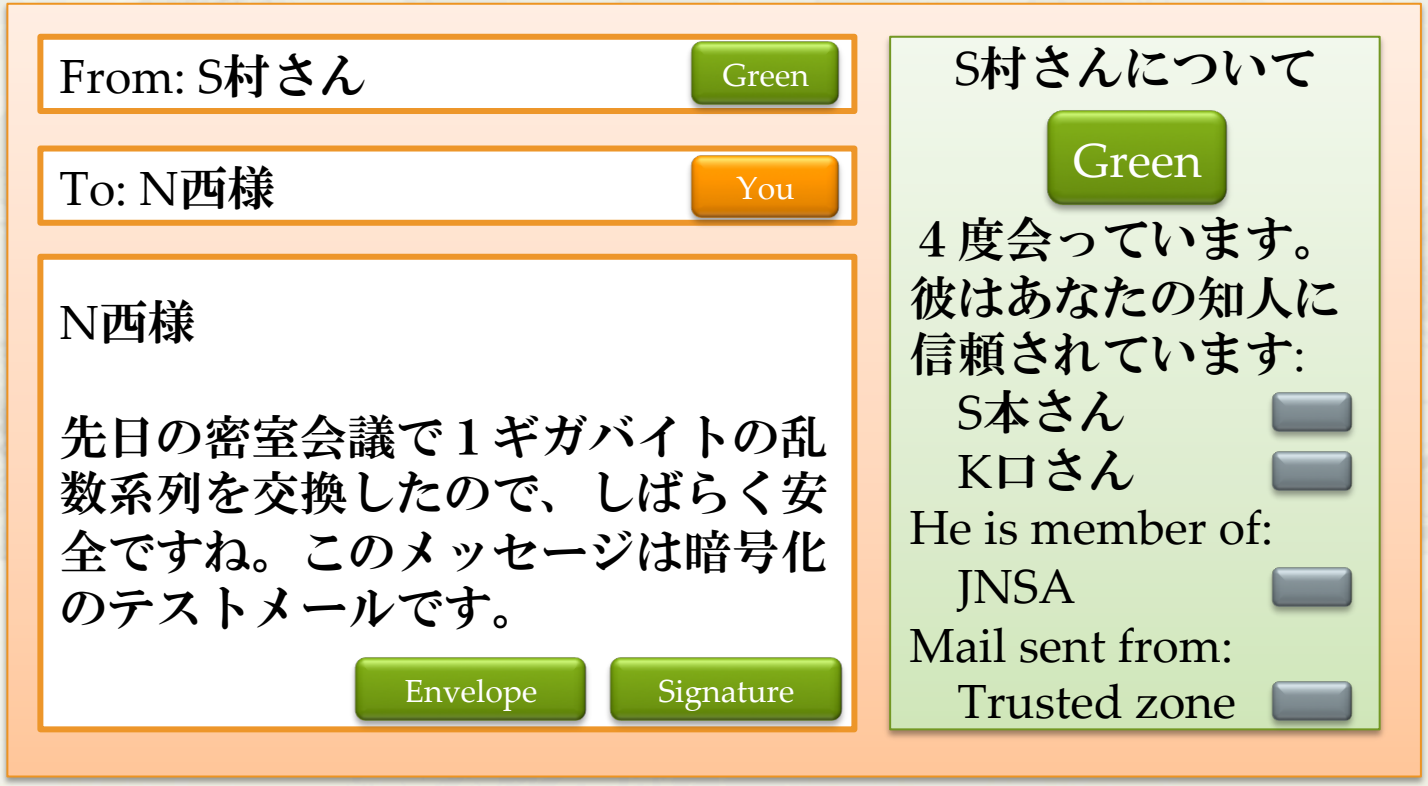
5. 物理的信頼 vs サイバー

* 鍵交換は一度だけ、というのは果たして正しかったのか
* 鍵が盗まれる・証明書が偽造される前提で即応策を考えていたのか
* 鍵交換の機会（会合等）を活かしていないのではないか

ミッションクリティカル・メーラ

(思考実験)

* フィジカルコンタクトを活かすメーラとは？



6. 技術的側面 vs 人的側面

* 技術に偏った対策だけで守れるのか
* 従業員がミスをする（クリックしてしまう）前提で何をすべきか

* クリックしてしまう従業員は誰か？
* クリックしてしまうブラウザは？
* クリックしてしまうメーラは？

* ワークフローの見直し

Extranet Security

* エクストラネット（取引企業群）でのセキュリティについて考えるべき時期

* メール添付に頼らない、企業間の安全なファイル共有とは？

7. 予防 vs 即応

* 予防措置に偏った対策は果たして正しかったのか
* 即応能力はペンテスト可能か
* 鎮圧までの時間は計測可能では？

JNSAメンバーの皆様に考えていただきたい事

* 専門家 . . . . . ユーザー
* クリティカル . . . . . コモディティ
* ID管理 . . . . . ふるまい管理
* 暗号化 . . . . . 仮想プライベート
* 物理的信頼 . . . . . サイバー
* 技術的側面 . . . . . 人的側面
* 予防 . . . . . 即応

* 二者択一ではなく、グラデーション
* SI案件において、テンプレートはないはず

「標的型攻撃」で終わらせないために

* 「標的型攻撃」は防げなかった言い訳か

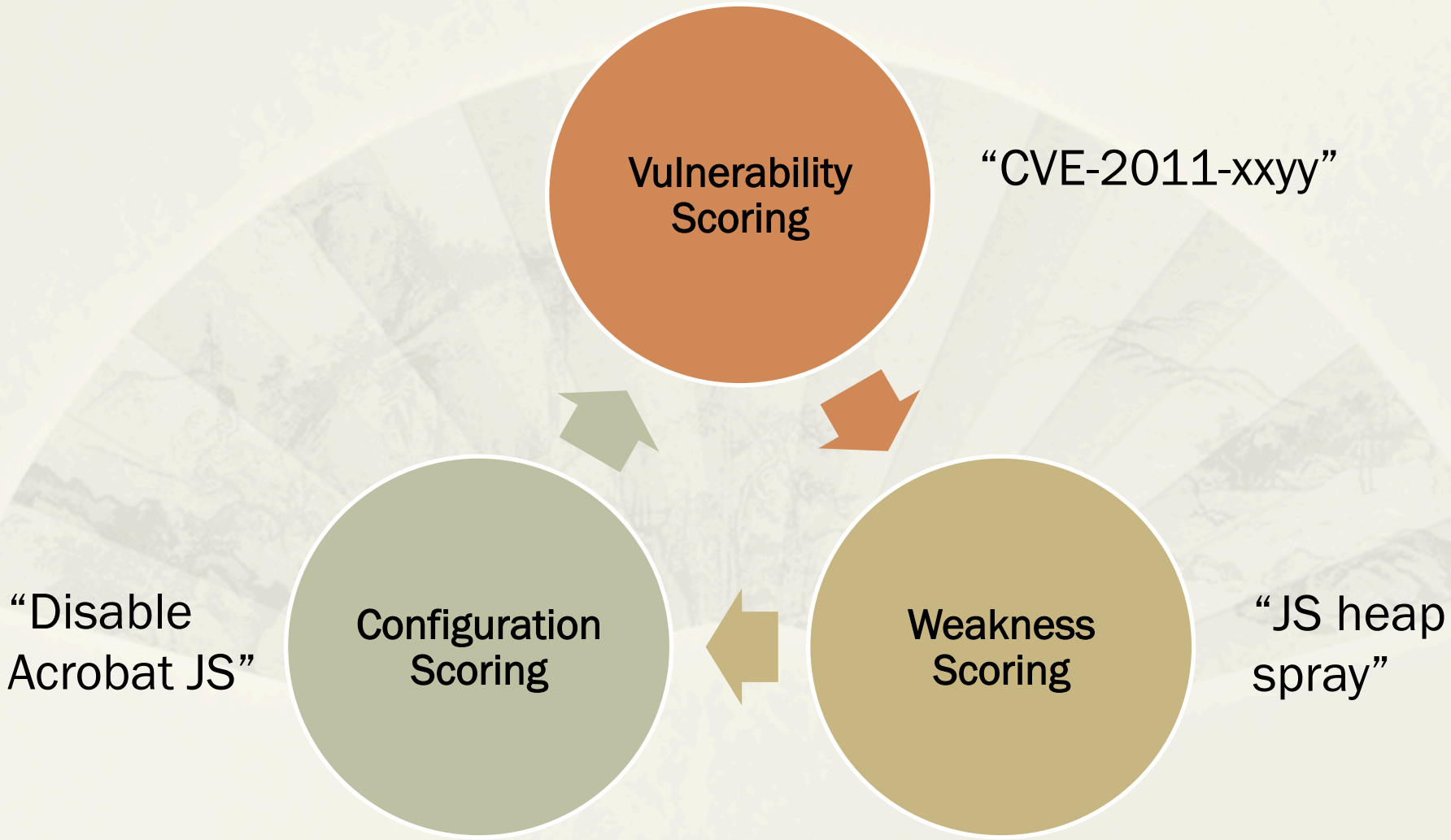
* **先月の標的型攻撃は今月の既知攻撃**
* **過去の標的型攻撃から何を学べるか**

解明が進む標的型攻撃

標的	マルウェア	トリガー	脆弱性	対策
RSA	Poison Ivy	Excel + Flash 0-day*	CVE-2011-0609	DEP
DoD	Sykipot	Acrobat 0-day*	CVE-2011-2462	Disable JS
三菱重工				
衆議院				
JAXA				

* 特定従業員を狙ったフィッシング詐欺メール

スコアリングへの反映



標的型ペンテスト

* ゼロデイそのものは模擬できなくても
  攻撃パターンは模擬できる
  * 一種の Fault injection test

* 添付ファイル着弾
* 証明書偽造
* ハードウェアトークン盗難

* 「あるはずのないこと」が起きたら…?
* 過去の事例により、パターン想定は容易に

まとめ

* なぜ標的型攻撃に弱いのか
  * 専門家 . . . . . ユーザー
  * クリティカル . . . . . コモディティ
  * ID管理 . . . . . ふるまい管理
  * 暗号化 . . . . . 仮想プライベート
  * 物理的信頼 . . . . . サイバー
  * 技術的側面 . . . . . 人的側面
  * 予防 . . . . . 即応
* 標的型攻撃とは何なのか
  * 解明
  * スコアリングへの反映
  * 標的型ペンテスト

最後に

JNSAメンバー各位の一層のご活躍を
期待しています