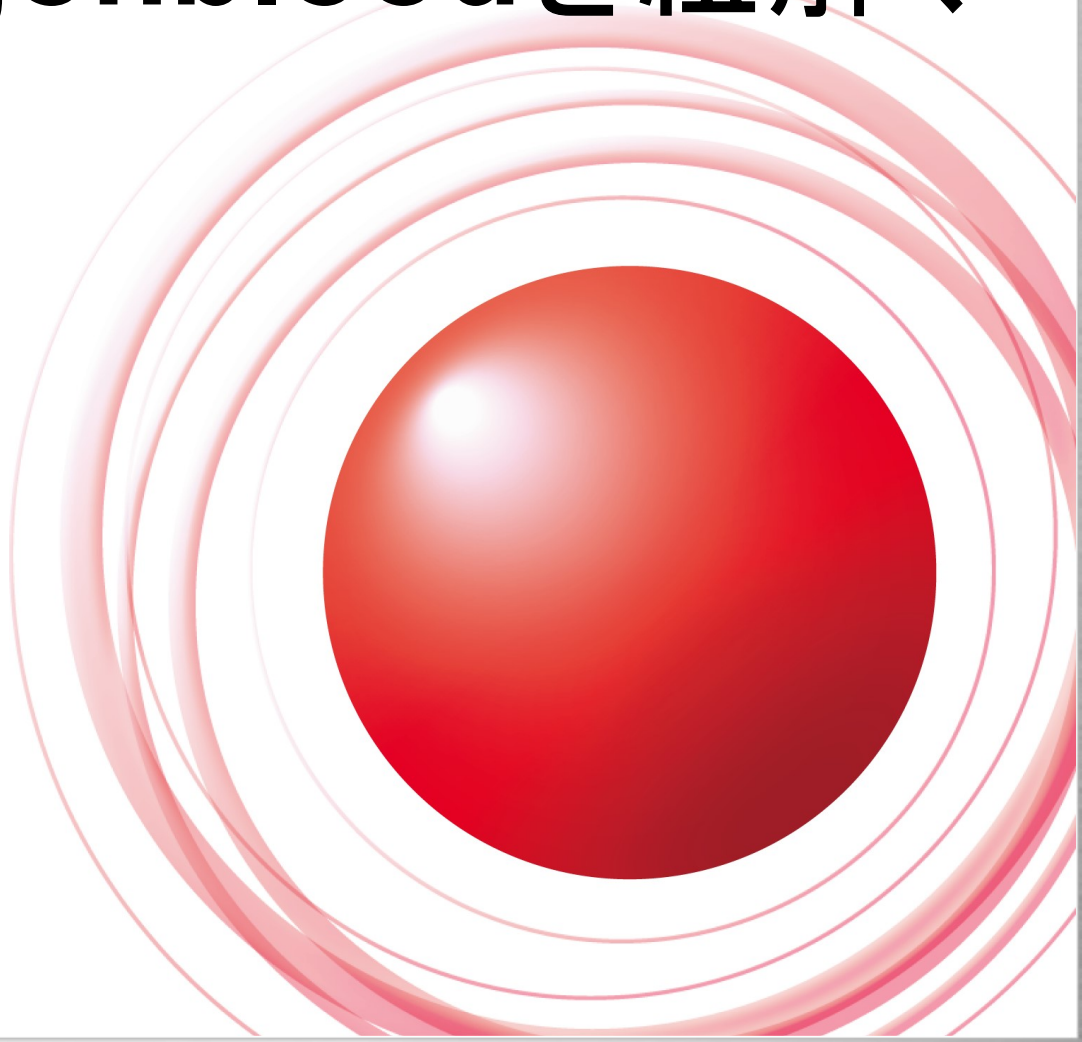
Janog44 meeting, Kobe, Japan

www.iij.ad.jp
安全な接続

WPA2/WPA3への攻撃 KRACKsとDragonbloodを紐解く



Internet Initiative Japan

wizSafe

セキュリティ本部セキュリティ情報統括室
須賀祐治
2019-07-26

毎度毎度最初のスライドは…

- 今回はまだ頑張った方だと思う
  - 前回J41@広島は朝4時にお好み焼き食べながら作業して事前資料を出していないはず

自己紹介

- CRYPTREC 暗号技術活用委員会 委員
- CRYPTREC TLS暗号設定ガイドラインWG 主査
  - 7/12 CRYPTRECシンポジウム 招待講演
- 暗号プロトコル評価技術コンソーシアム 幹事
- 情報処理学会 CSEC研究会 幹事
  - CSS2017 プログラム委員長
- 電子情報通信学会 ISEC研究会 幹事補佐
- CyberSciTech2019 Program co-chair
- Cryptoassets Governance Task Force SecWG member
  - 「仮想通貨交換所のセキュリティ対策についての考え方」
- SCAIS2015-2020実行委員
  - アカデミアとインダストリの架け橋となるワークショップ

本発表のバックグラウンドとモチベーション

JANOG44の資料から(1/3)

JANOG 41 meeting, Hiroshima, Japan

配信大丈夫か知らんが 愛を叫ぶ

KRACKs攻撃の裏で愛(RSA influences)を叫ぶ

須賀祐治
2018-01-26

Ongoing Innovation

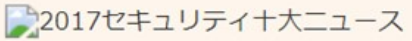
JANOG44の資料から(2/3)

KRACKsをざっくりと

セキュリティのプロが選ぶ！

JNSA 2017 セキュリティ十大ニュース

～ 特異な年2017、停滞が始まったのか ～



【第１位】10月4日　総務省が「IoTセキュリティ総合対策」を発表

～　攻撃者が嬉々とするIoT機器の危機的な状況　～

【第２位】5月14日　IPAがランサムウェア「WannaCry」に関する注意喚起を発表

～　侮るなかれ、セキュリティ対策の基本の基本　～

【第３位】8月25日　米国の一私企業のミスで日本の通信インフラが混乱

～　巨人の咳一つでゆらぐインターネット　～

【第４位】10月16日　世界が狂騒したWPA2の脆弱性は狂想だった

～　SNSでの不確かな憶測情報が不安を助長した　～

http://www.jnsa.org/active/news10/

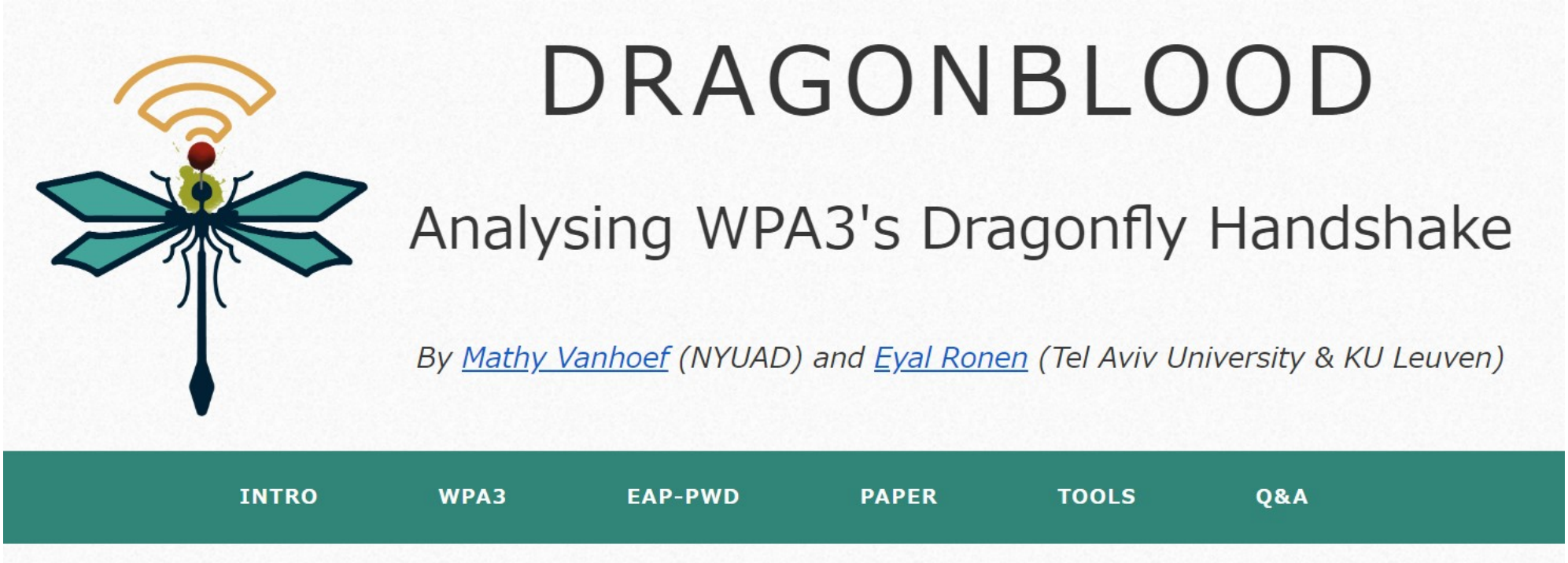
JANOG44の資料から(3/3)

KRACKsをざっくりと

- M. Vanhoef and F. Piessens, Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2, ACM CCS'17
  - https://papers.mathyvanhoef.com/ccs2017.pdf
- WPA1/WPA2のプロトコル仕様の問題
  - 製品バグではない点でヤバそうな雰囲気を醸し出してた
- クライアント(Supplicant)側へのMiTM攻撃
  - パスワード復元攻撃ではなく暗号化データを解読する攻撃
  - パスワード変更しても意味はない
- Supplicant はWPA2はダダ漏れの土管と考えて使え
  - 特にSSL証明書を検証しないAndroidアプリの利用はやばいだろう
- 802.1X認証は改めてEAP-TLSなどで張り直すので大丈夫(のはず)

DragonBlood

- KRACKs攻撃と同じ発見者
- 皮肉なことにKRACK攻撃に対抗するために設計されたWPA3の脆弱性を発表



https://wpa3.mathyvanhoef.com/

DragonBlood をざっくりと

https://wlan1nde.wordpress.com/2018/09/14/wpa3-improving-your-wlan-security/

- 初動時の理解：Wifi AllianceとしてはWPA3対応製品はまだあまり出荷されていないし
  リファレンスコードを修正したので，各社もソフトウエアにパッチすればOKと考えている？
- 問題箇所の特定：
  SAE(Simultaneous Authentication of Equals)
  - IEEE 802.11 Section 12.4.1で規定の「パスワードで認証する」鍵交換プロトコル
  - SAE は WPA3-Personal でのみ利用.
    なので今回の攻撃はWPA3-Enterpriseは影響なし

ちょっときな臭さを感じなくもない

- Dragonfly Handshake/Dragonfly Key Exchange
- RFC7664で規定の「パスワードで認証する」鍵交換プロトコル
  - CFRG主導で2015年に策定.
  - 某社主導で辞書攻撃に対抗するためdragonflyを開発しSAEという名前でIEEE 802.11標準になったという記載も.

https://irtf.org/cfrg

※HeartBleed-hertbeat

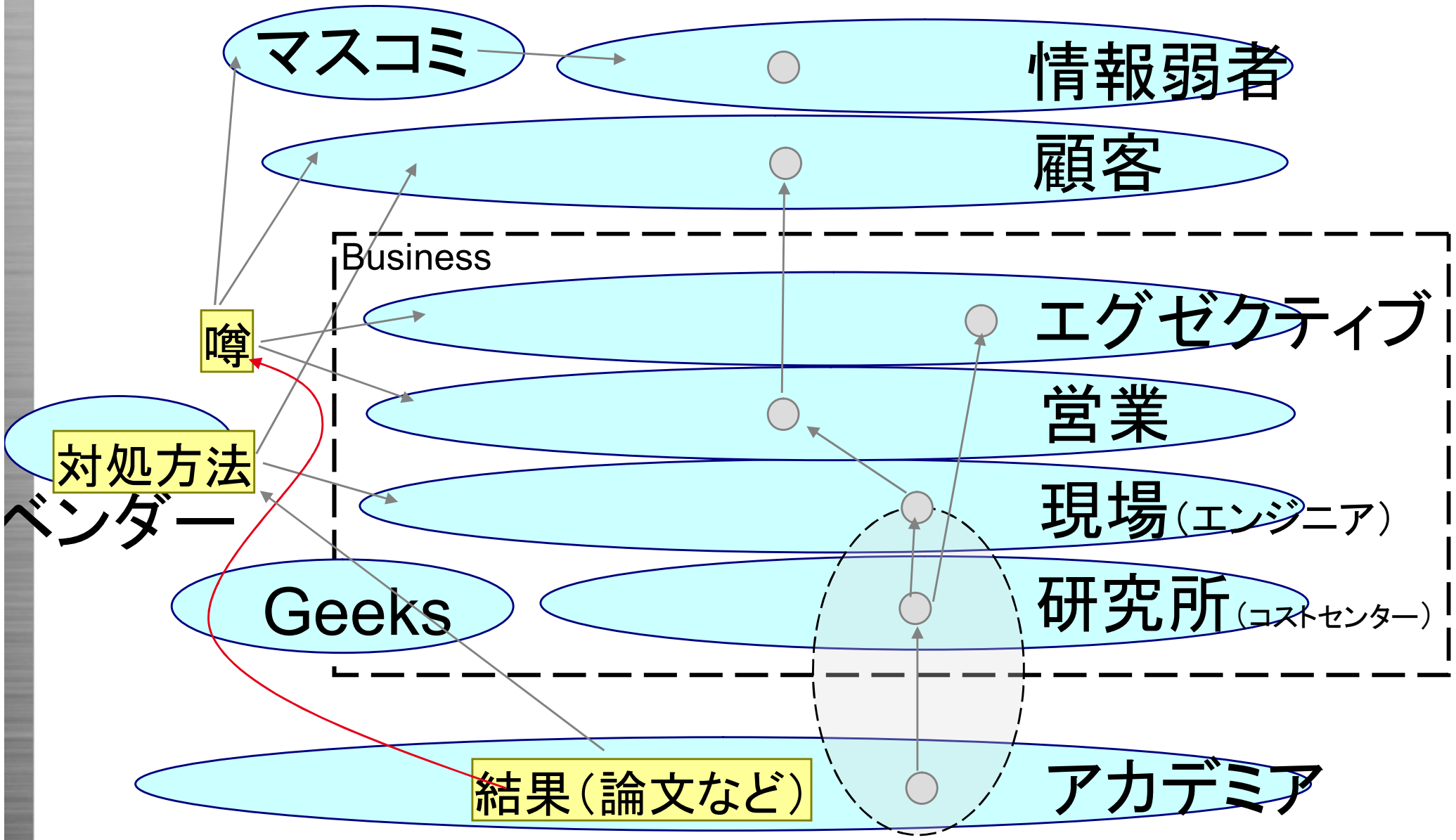
著者もちゃんとした分類を放棄

- どちらも Wi-Fiパスワードの搾取が可能になる.
- (1) ダウングレード攻撃
  - (1.a) WPA2にダウングレードする→結果的にbrute-force attackにつながる
  - (1.b) 弱い楕円曲線暗号アルゴリズムを使わせる
- (2) サイドチャネル攻撃（Dragonflyプロトコルに対して）
  - (2.a) cache-based 攻撃：hash-to-curveアルゴリズムがダメだ
  - (2.b) timing-based 攻撃：hash-to-groupアルゴリズムがダメだ
  - → (2.a)(2.b)は辞書攻撃に似たパスワード分割攻撃（password partitioning attack）につながる
- 影響度：Dragonflyの40以下のハンドシェイクを（観測ではなく）能動的に攻撃して得られた情報をAmazon EC2 instancesでぶっこ回せば125ドルでパスワードが取れる

2つの脆弱性を紐解くにあたり…

- 2011-12年に「そういう人材」の必要性を訴えていたことを思い出す（次・次々ページ参照）.
- 今回はTechnicalな解説だけにフォーカスするのではなく，複数のエンジニアが実際にどのように議論しながら，バランスのよい「技術翻訳」をしていったのかを紹介.
- そこから方法論とかベストプラクティスが得られればいいなという思考実験.

「技術翻訳者」連携の必要性



2012年3月総合大会「セキュリティプロトコル仕様の脆弱性事例と世代交代困難性」

「技術翻訳者」の役割

- 正しい情報をわかりやすく「上」に伝える
  - 落としてよい情報と肝の情報
- 誤りがあればそれを正す
  - 噂が広まるのは早い
- どう解釈しているのか「横」に伝える

2012年3月総合大会「セキュリティプロトコル仕様の脆弱性事例と世代交代困難性」

「似たような」3つの概念との違い

- （1）Technical translator
  - 技術文書の翻訳専門家
- （2）脆弱性ハンドリング
  - 脆弱性発見者・報告者とベンダとの調整
  - 対策方法が開示されてちゃんと世の中に浸透していくまでをコーディネート
- （3）組織内CSIRT
  - Computer Security Incident Response Team
  - コンピュータセキュリティにかかるインシデントに対処．監視作業を含むケースも．

具体的な実例紹介に移る前に…
2010年と2015年の分類方針

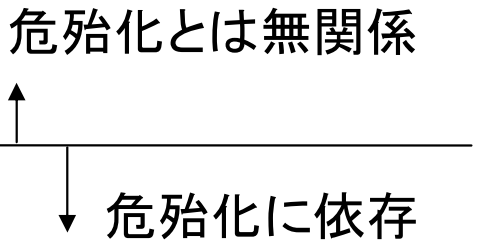
暗号アルゴリズムの危殆化

- アルゴリズム自体に欠陥が生じる問題
  - 設計当時は安全と思われていた
  - しかしアルゴリズムに内在していた欠陥が近年の暗号解析研究によって明らかになった「設計ミス」
- 対処方法：暗号アルゴリズムを差し替える
  - 移行コスト，社会的インパクトが大きい
    - 1976年に策定されたDESはTDESとして現在も使われており**2030年まで**利用を容認→2023年に前倒し
  - 既に現役引退したアルゴリズム
    - 共通鍵暗号：DES,(TDES: “DES sunset” という用語あり)
    - ハッシュ関数：MD2/4/5, SHA-1

危殆化による波及する影響範囲

- 暗号アルゴリズムや(利用法)の脆弱性を用いて通信プロトコルやデータフォーマットへの攻撃を試みる事例が多発している.

- 脆弱性分類の一方式
  - (1)実装の脆弱性
  - (2)通信プロトコルそのものの問題
  - (3)利用法・しくみの脆弱性
  - (4)危殆化の事実そのもの



危殆化による波及する影響範囲(2/2)

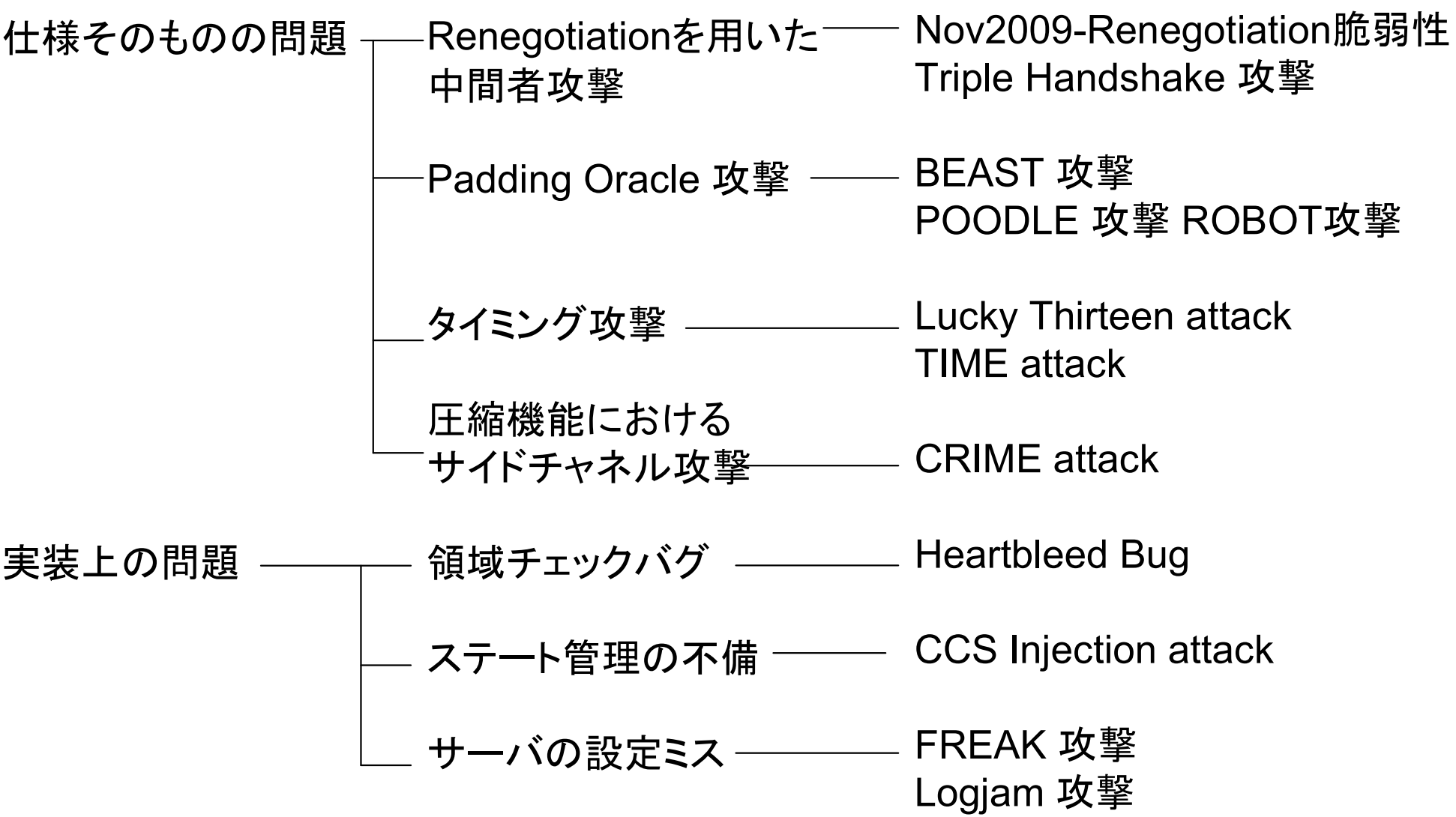
- 脆弱性に対する対策
  - (1)実装の脆弱性
    - パッチを当てる / 脆弱性のないプロダクトに差し替える
  - (2)通信プロトコルそのものの問題
    - 抜本的な対策は仕様を更新すること
      - それまでに配布されるパッチは一時的な回避策に過ぎない
  - (3)利用法・しくみの脆弱性
    - 代替案があれば差し替える
      - 例:CBC → CTRモード, TKIP → CCMP

危殆化とは無関係

危殆化に依存

  - (4)危殆化の事実そのもの
    - 暗号アルゴリズムの変更
      - 例:DES → AES

2015年の分類例：SSL/TLSに対する攻撃



ここでちょっとだけ脱線予定

- BEAST-likeな攻撃に脆弱なサーバへの風当たりが強い
  - CBCという暗号モードの使い方が元凶
  - 決してCBC単体が危殆化しているわけではない
- TLS1.3ではAEADに完全移行
  - CBCを早めに捨てたのはよかった事例…

TLSの事例から学ぶことはできるのか

CELLOSからのアウトプット

https://www.cellos-consortium.org/jp/index.php?KRACKs_20171019J

CELLOS

Cryptographic protocol Evaluation toward Long-Lived Outstanding Security

HOME
What's New!
CELLOSとは
概要
活動内容
発起人
体制
構成
規約
役員
会員
公開情報
速報

KRACKs_20171019J

[2017/10/19] WPA/WPA2プロトコルの脆弱性KRACKsについて

2017年10月16日、無線LANにおける認証と暗号化のプロトコルであるWPA、WPA2における脆弱性KRACKsについて、ACMCCSで発表予定の論文[1]とその詳細が公開されました。今回の脆弱性は、WPA/WPA2のプロトコル仕様に原因があります。そのため、根本的にはより安全なプロトコルを利用する必要がありますが、現時点においてWPA/WPA2の代替となるプロトコルは存在しません。一方で、後方互換性を保つことができるパッチが用意されており、このパッチを適用することにより、この脆弱性を利用した攻撃を防ぐことができます。

脆弱性・攻撃の概要と影響

今回の脆弱性は、無線LANにおける認証プロトコルが達成しようとしてるセキュリティの性質

KRACKs対応タイムライン（2017年10月）

- 10/16 11:47 BlackHat EU'17でWPA2攻撃論文出てる！
- 10/16 11:48 "TheRegister"-ed 確認

- （現在集計中です．出さないかもしれない）

- 10/20 08:19 CELLOSサーバで報告書公開

技術翻訳に求められる素養はなんだろうか

TLSの事例から学ぶことはできるのか

マーケティング用語？

必要となる素養（完全な私見）

- 技術的バックグラウンド
- アンテナを立てておく
- 英語いる？
- 積極的に発信する・ヒトに教えてみる

いくつかの方法論

https://www.ipa.go.jp/security/vuln/CWE.html

- [難しさ] とにかく早く判断しないといけない
- CWE（Common Weakness Enumeration; 共通脆弱性タイプ）による分類であたりをつけられればいいんだけど…
  - CVEも（発番されてはいるけれど）出ていないことも

参考：CWE分類の観点での2つの脆弱性の比較

- KRACKs:10個のCVEだけどJust one CWE
  - Vulnerability Note VU#228519

CWE-323: Reusing a Nonce, Key Pair in Encryption

- Dragonblood：6個のCVEで5種類のCWE

CVE-2019-9494: SAE cache attack a
attacks) - CWE-208 and CWE-524

CVE-2019-9495: EAP-PWD cache
side-channel attack) - CWE-524

CVE-2019-9497: EAP-PWD reflection
validation) - CWE-301

CVE-2019-9498: EAP-PWD server missing
scalar/element - CWE-346

CVE-2019-9499: EAP-PWD p
scalar/element - CWE-346

confirm missing state validation - CWE-642

https://www.kb.cert.org/vuls/id/228519/
https://www.kb.cert.org/vuls/id/871675/

ツールでサポートできるか？

- 特に今回の攻撃想定環境では無線デバイスが含まれるため構築が難しい

- 実際どうされていますか？
- 良いツールはありませんか？

次に備えるために

- 予兆できるか？トップカンファレンスのプログラムが出そうな時期に公開されることが多い
  - ただこれは使えなくなりつつある
  - 投稿は毎月・2ヶ月に一度→一年にまとめてカンファレンスを開催するジャーナルモデル
- 正直ノーアイデア．かといって枯れた技術は安全神話を持ってはいけないだろう

倫理に関する観点

- 脆弱性公開に関する議論
- アカデミアにおける研究倫理の取り組み
  - 例えば街角でアクセスポイントをクロールする
  - 攻撃としないまでも統計的な処理をすれば許されるのか

CSS2018・2019での取り組み

- CSS2018：相談窓口の設置

https://www.iwsec.org/css/2018/ethics.html

研究倫理相談窓口

CSS2018研究倫理委員会とCSS2018研究倫理相談窓口について

セキュリティ研究においては、被検者や他人に危害が及ぶことを完全に防止することが困難な実験(例：インターネット接続した実行環境による実マルウェア解析実験など)が必要な場合や、実在するシステムや製品の脆弱性が発見される場合があり、研究方法や研究により得られた情報の開示方法について、特に研究者の倫理観が求められています．

CSS2018では，セキュリティ分野の研究倫理の重要性の高まりを受け，CSS2018研究倫理委員会を設置致します．また、研究倫理委員会の活動としてCSS2018研究倫理相談窓口(以降，相談窓口)を開設致します．相談窓口では，CSS2018および併設ワークショップにて発表

- CSS2019：投稿時にセルフチェックリスト

https://www.iwsec.org/css/2019/ethics.html

研究倫理相談窓口

CSS2019研究倫理委員会とCSS2019研究倫理相談窓口について

セキュリティ研究においては，実験参加者や他人に危害が及ぶことを完全に防止することが困難な実験(例：インターネット接続した実行環境による実マルウェア解析実験など)が必要な場合や，実在するシステムや製品の脆弱性が発見される場合があり，研究方法や研究により得られた情報の開示方法について，特に研究者の倫理観が求められています．

CSS2019では，セキュリティ分野の研究倫理の重要性の高まりを受け，**サイバーセキュリティ研究における倫理的配慮のためのチェックリスト（以降，チェックリスト）**の活用，および昨年に引き続きCSS2019研究倫理委員会を設置します．研究倫理の観点で懸念がある場合はまずチェックリストを活用し，セルフチェックを実施してください．

業界へのフィードバック事例

https://conferences.ncl.ac.uk/ssr2019/

SSR conference, 11 Nov 2019, London, UK

Security Standardisation Research Conference 2019 (ACM CCS Workshop)

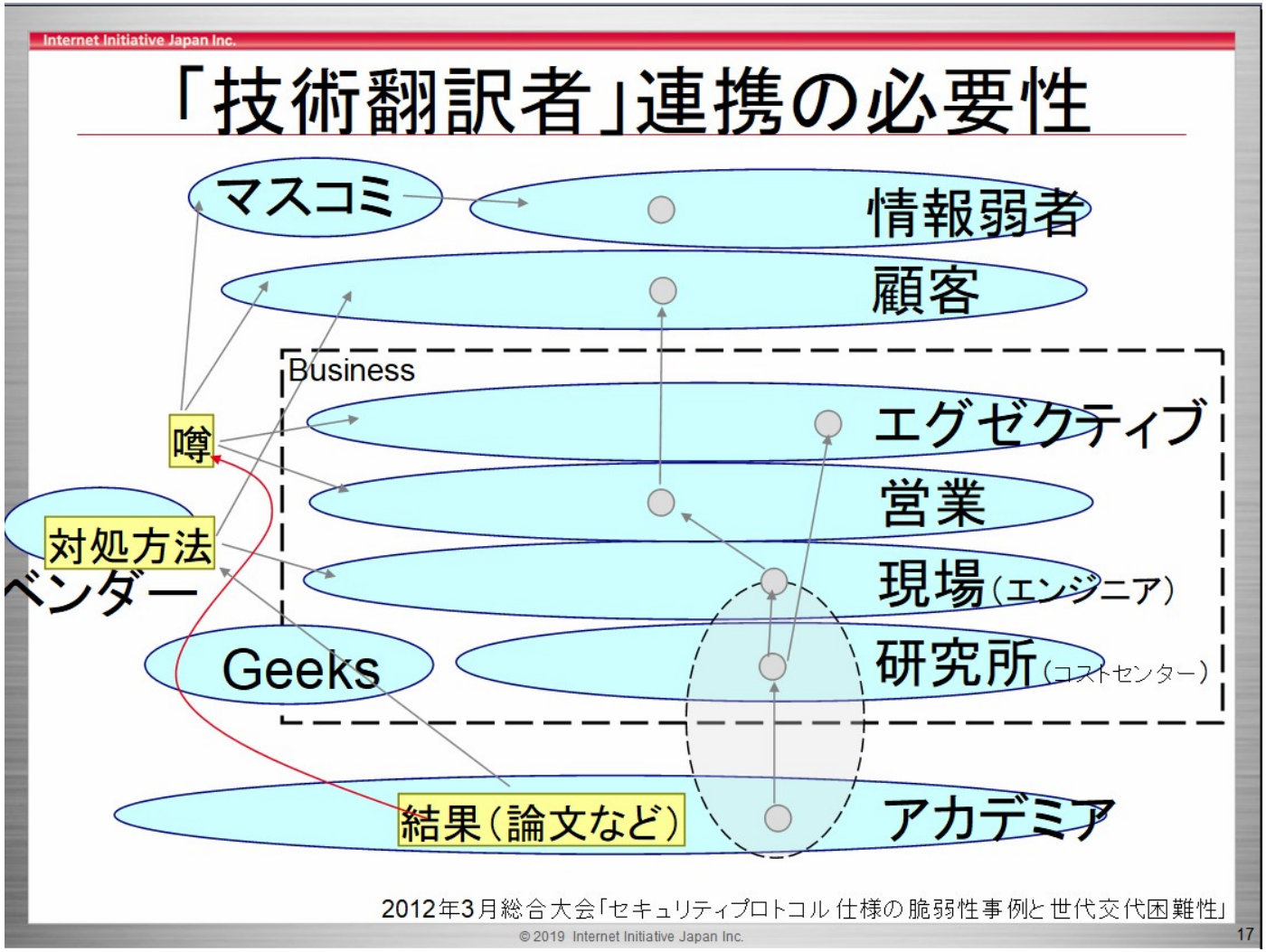
The 5th Conference on Security Standards Research will be held in London, UK, 11 Nov 2019. Please note that SSR is an ACM CCS workshop this year.

- セキュリティ標準化に関わる国際会議
  - 形式証明系もあればポリティカルな分析も
  - TLS1.3策定時期のコントリビューション
- 実は2015年に第2回をIIJ@飯田橋で開催済

自戒を込めて

そもそも

- Janogなコミュニティにこういう境界領域人材は必要か?



IIJ Internet Initiative Japan

Lead Initiative

日本のインターネットは1992年、IIJとともにはじまりました。以来、IIJグループはネットワーク社会の基盤をつくり、技術力でその発展を支えてきました。インターネットの未来を想い、新たなイノベーションに挑戦し続けていく。それは、つねに先駆者としてインターネットの可能性を切り拓いてきたIIJの、これからも変わることのない姿勢です。IIJの真ん中のIはイニシアティブ――IIJはいつもはじまりであり、未来です。

Ongoing Innovation

お問い合わせ先 IIJインフォメーションセンター
TEL:03-5205-4466（9:30～17:30 土/日/祝日除く）
info@iij.ad.jp
http://www.iij.ad.jp/