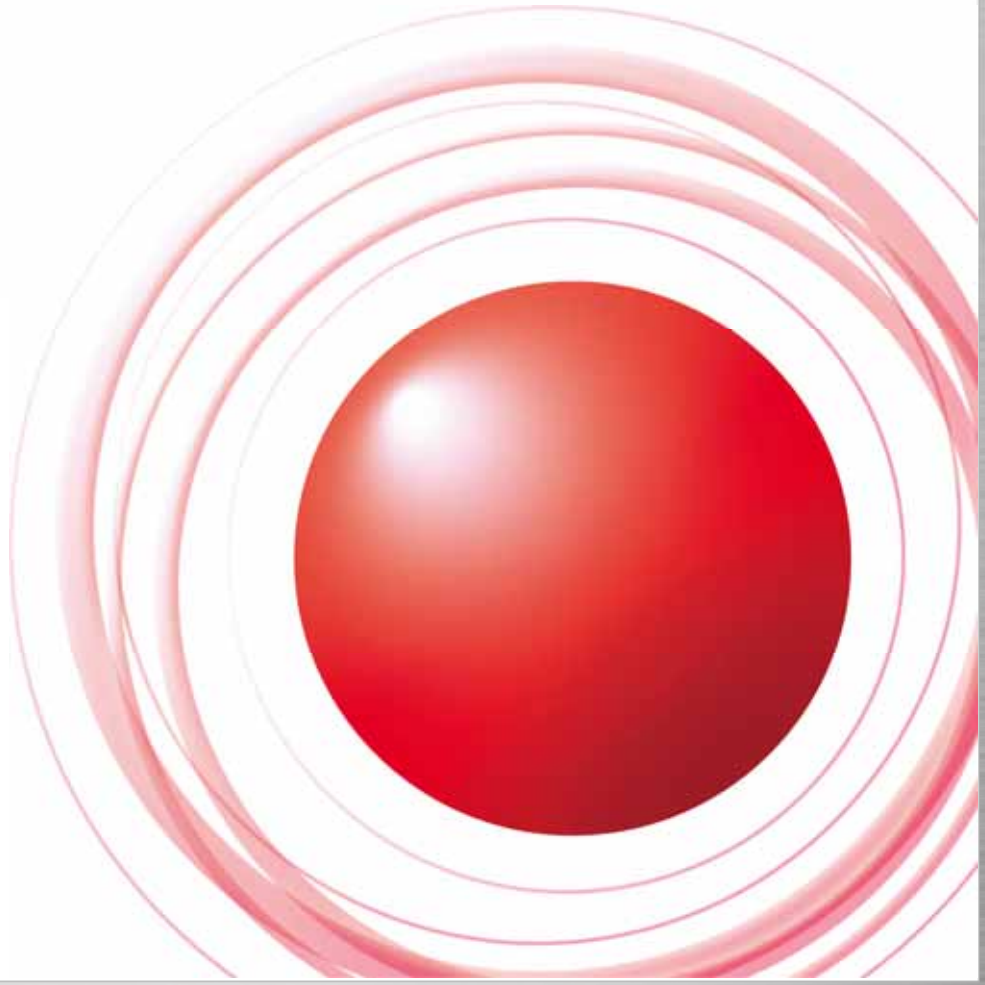
JNSA 2012年度活動報告会
June 7, 2013, UDX, Akihabara, Tokyo, Japan

「暗号技術」と「多様化するサイバー攻撃」

～「暗号技術」を用いたプロトコル・実装に多発している問題～

IIJ
Internet Initiative Japan



Yuji SUGA
June 7th, 2013

Ongoing Innovation

今回のお話のベース – IIR vol.18

Internet Infrastructure Review (IIR) Vol.18
2013年2月26日発行

RSS

今号では、2012年10月から12月までの3ヵ月間を対象として、セキュリティインシデントや迷惑メールなどの観測情報をまとめ、IIJが取り扱ったインシデントと対応について紹介しています。また、受託共同研究「アクセス網のクラウド化」についても紹介しています。

- 一括ダウンロード[PDF:5.65MB]
- エクゼクティブサマリ[PDF:3.02MB]
- インフラストラクチャセキュリティ「Torの技術」[PDF:5.03MB]

  今回は、匿名通信に利用されているTorの仕組みを紹介すると共に、昨年後半に日本の金融機関の利用者を対象に悪用されたマルウェアZeuSの亜種Citadel及び、暗号技術を用いたプロトコル・実装に多発している問題について解説します。

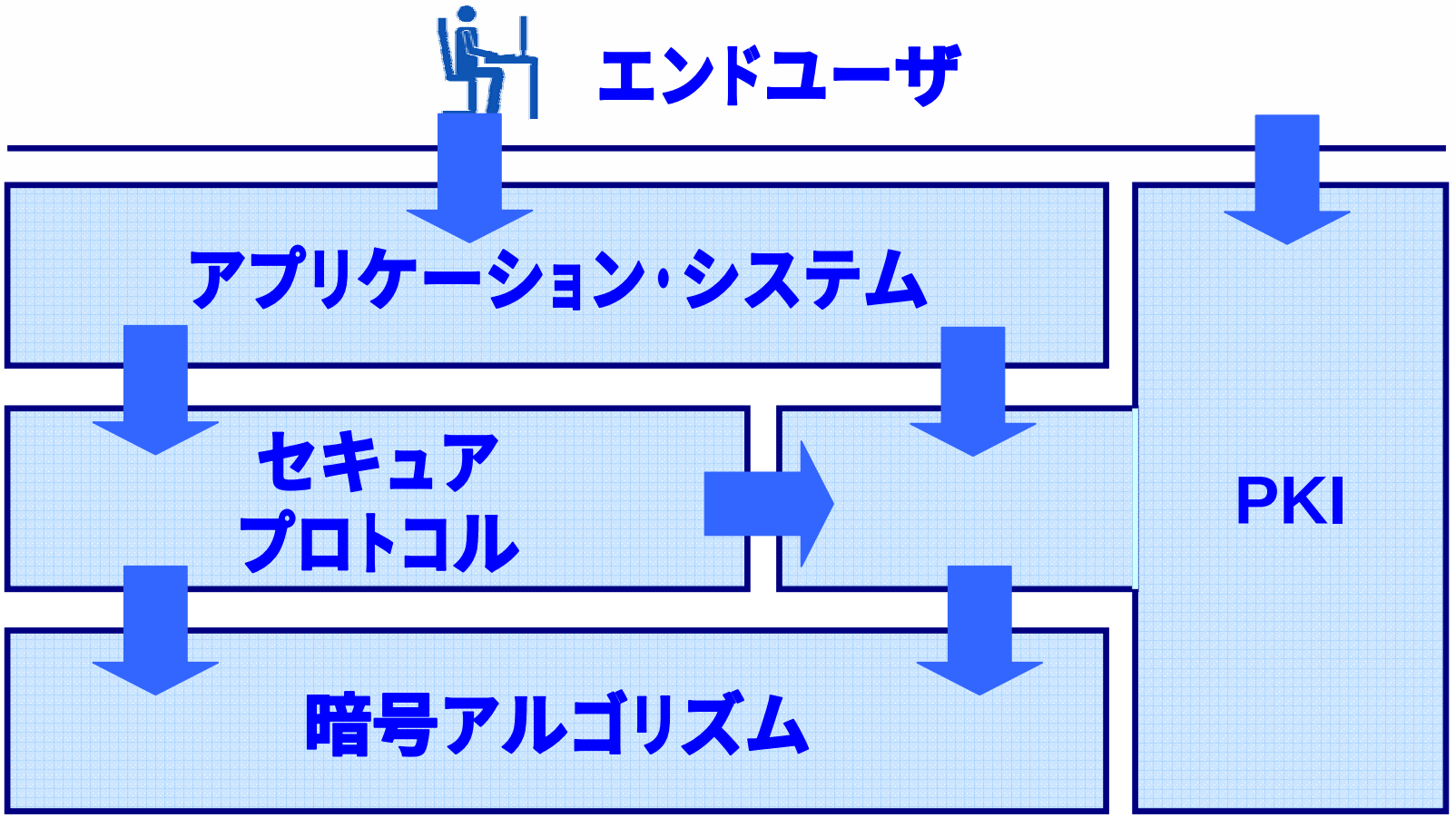
http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol18_infra.pdf

表-1暗号を用いたプロトコル・実装の脆弱性とそれに起因する事件の分類

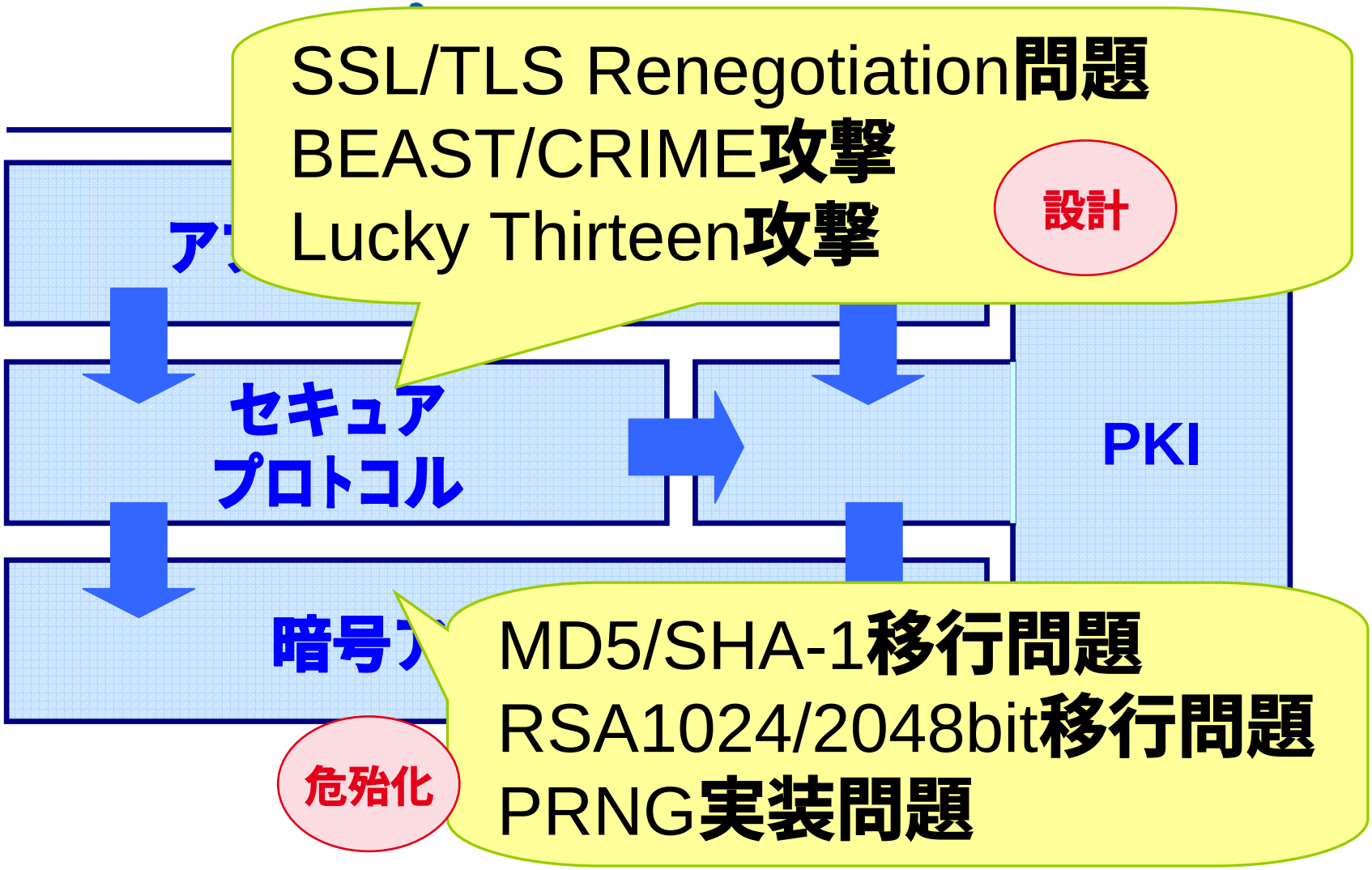
- 暗号危殆化
- 設計
- 実装
- 運用

問題の種別	年 月	脆弱性・事件 名称	詳 細
暗号危殆化による問題	2007年 3 月	APOPパスワードクラック	MD5コリジョン攻撃を用いてチャレンジを送信し、サーバになりすます攻撃が可能であることが公開された。
	2009年12月	X.509中間CA証明書偽造	MD5ダイジェストを衝突させるように、X.509v3拡張部分のうち、ブラウザが無視するエリアを調整してX.509中間CA証明書の偽造を行った。このとき、証明書のシリアル番号がインクリメントして発行されていて被署名データが推測可能であったという運用面の問題も指摘されている。
	2010年 1 月	768ビットRSA公開鍵の素因数分解	663ビットという当時の記録を更新し、80台のマシンを利用して約半年で768ビットRSA公開鍵の素因数分解に成功したとの報告があった。1024ビットRSAはまだまだ現実的な攻撃対象ではないが、2048ビットRSAへの移行を促進するきっかけの1つとなった。
	2012年 5 月	Flameマルウェア	マルウェアを悪用したコード署名機能への攻撃によるWindows Updateへの中間者攻撃が発覚した。MD5コリジョン攻撃を用いて、あたかもMicrosoft から発行されたように見える不正な証明書が発行された。
	2012年 8 月	PKCS# 1v1.5暗号に対するパディングオラクル攻撃	PKCS# 1v1.5暗号に対する既存のPadding oracle attackを改良する攻撃手法が公開された。PKCS# 11の暗号鍵インポート関数が実装されたハードウェアから暗号鍵を搾取する現実的な攻撃である。
	2012年 8 月	鍵長1024ビット未満のRSA 鍵の利用制限	Microsoftの製品群において、1024ビット未満のRSA鍵を使用した証明書の使用を制限する更新プログラムがリリースされた。
設計の問題	2008年11月	WPAに対する鍵回復攻撃	WPA (Wi-Fi Protected Access)における鍵更新アルゴリズムTKIP(Temporal Key Integrity Protocol)の問題により、MIC鍵の漏えいと改ざんパケットの生成が可能となる攻撃が公開された。
	2008年11月	SSHv2通信傍受による暗号文の一部漏えい	CBCモード利用時のSSHv2において、パケット先頭4バイトが漏えいする攻撃が公開された。パケット長チェックの仕組みを利用してトライ&エラーを行い、確率 2^{-14} で成功する。
	2009年11月	SSL/TLS Renegotiation 脆弱性	鍵情報やアルゴリズムの合意をリフレッシュするrenegotiation機構において、HTTPSフラグメントにおけるインジェクションを可能にする中間者攻撃が公開された。
	2010年10月	IPsecにおけるCBC利用時の問題	ESP trailerと呼ばれる平文データに対してブロックサイズ長になるようにパディングされたデータ構造の特徴に着目した攻撃が公開された。
	2011年 9 月	BEAST攻撃	SSL 3.0/TLS 1.0を使用しているブラウザのCBCモードに対して選択平文攻撃を行うことでブラウザ内のCookieを入手するツールが公開された。
	2011年10月	XML Encryption(CBCモード利用時)脆弱性	XML構文チェックエラーに応じて異なるエラーコードを返却するWebサービスをplaintext validity oracleとして利用した攻撃が公開された。
	2011年12月	TLS1.2におけるTruncated HMAC利用時の問題	メッセージ認証子として通常のHMACではなく、80ビットに切り詰めたデータをMACとして利用する拡張方式において、暗号化対象のアプリケーションデータが短く、暗号化データがブロックサイズを超えないケースにおいて平文の情報が漏えいする可能性が指摘された。
	2012年 7 月	MS-CHAPv2解読ツール公開	Bruce Schneierが1999年に公開したMS-CHAPv2に対する攻撃手法をクラウドから利用できるツールが公開された。
	2012年 9 月	CRIME攻撃	SSL/TLSでCompression(圧縮)機能を有効にしているケースで、Cookieを搾取するデモが公開された。たとえ同じ長さのデータを圧縮したとしても、圧縮前データに同じ文字を含むかどうかで辞書の長さが変わるという事実を用いてトライ&エラーで暗号化データを復元する手法である。
	2012年 9 月	Oracle DBにおけるパスワード搾取攻撃	Oracleデータベースのパスワードを搾取可能な攻撃が公開された。認証プロトコルの設計の問題として認識されている。
実装の問題	2008年 5 月	DebianのOpenSSLに予測可能な乱数生成の問題	Debianの特定バージョンにおけるOpenSSLを使って鍵生成を行った場合、極端に少ない鍵空間からしか秘密鍵を導出していないという問題が公開された。
	2012年 2 月	公開鍵使いまわし問題	インターネット上のIPv4アドレスを広範囲にスキャンして、SSL/TLSやSSHで利用されている公開鍵証明書、DSA署名及びPGP鍵を収集したところ、意図せず他のサイトと秘密鍵を共有していることが、独立した2グループから報告された。
	2012年10月	アンドロイド向けアプリのSSL実装の問題	SSL実装の不備により、中間者攻撃の脆弱性が可能なアンドロイド向けアプリの存在が指摘された。
	2012年11月	Huawei製Wifiプロダクトにおける実装の問題	通信中に用いられる共通鍵暗号DESにおいて、本来ランダムに選択されるはずのセッション鍵がハードコーディングされていたことが公開された。
運用の問題	2011年 3 月 ～ 11月	複数の認証機関への侵入事件と不正証明書発行事件	3月に起きたComodo事件では9件の証明書が、また8月末にはDigiNotarから500以上もの証明書が不正に発行されていることが発覚した。更に11月にはKPN社が運営するオランダの認証機関サービスにおいて、証明書発行システムへの侵入の痕跡が見つかったため証明書発行業務を停止している。
	2011年 9 月	RSA512ビット証明書発行CAの証明書失効	DigiCert Sdn. Bhd.社の発行ポリシーの問題により、中間CA証明書を無効にする方針がとられた。
	2012年 8 月	Adobeの証明書失効	Adobeで用いられていたコード署名用証明書の不正利用が発覚したため、証明書を失効処理している(事件の経緯について続報がないため現時点では運用の問題に分類している)。
	2012年10月	DKIMで利用される公開鍵にRSA512ビット鍵を利用	電子メールの送信元を認証する仕組みの1つであるDKIMにおいて、仕様上、本来1024ビット以上の鍵長を利用する必要があるが、512 ビット鍵を利用していた事例が報告された。
	2012年10月	署名されたマイクロソフトバイナリに影響を与える互換性の問題	2012年7月12日から8月14日の期間にコード署名されたバイナリのいくつかに間違った手順に基づいて署名されていたことが発覚した。CodeSign証明書にタイムスタンプに関するExtended Key Usageが含まれていなかったことが原因である。
	2012年12月	TURKTRUST認証局からの証明書不正発行	TURKTRUST認証局により、*.google.comなどに対して複数の証明書が不正発行されたことが発覚した。

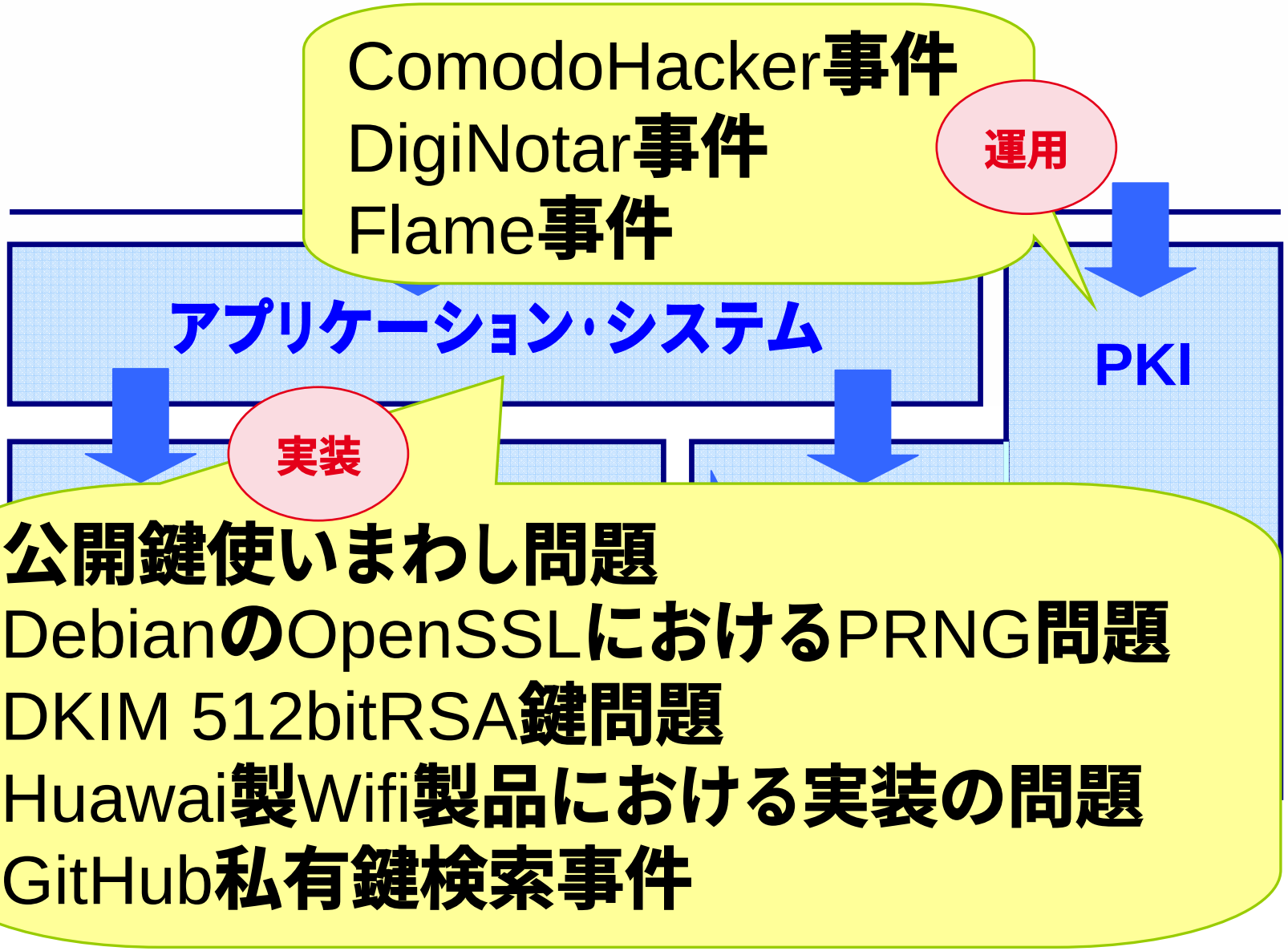
エンドユーザと「暗号技術」の距離



エンドユーザと「暗号技術」の距離



エンドユーザと「暗号技術」の距離



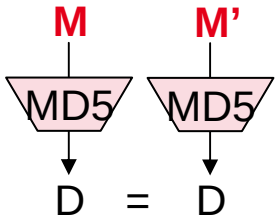
危殆化

暗号危殆化による間接的な影響

- APOP, SIP, HTTP Authentication **における**
  パスワードリカバリ攻撃
  - Yu Sasaki, Lei Wang, Kazuo Ohta and Noboru Kunihiro, "Extended Password Recovery Attacks against APOP, SIP, and Digest Authentication," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E92-A, No. 1, pp. 96-104, 2009.

- X.509**中間CA証明書偽造攻撃**
  - MD5 considered harmful today
    - http://www.win.tue.nl/hashclash/rogue-ca/

- **とも**にMD5**コリジョン攻撃を利用**



設計

2011年はCBCモードの当たり年

- 9月：BEAST攻撃 (CVE-2011-3389)
  - SSL 3.0/TLS 1.0 を使用しているブラウザの CBC モードに対して選択平文攻撃を行うことでブラウザ内の Cookie を入手するツールを公開
  - ブロックごとではなくバイトごとの全数検索だとうまくいく例を示し，実際にPayPalからのセキュアなCookieを奪取してログイン権限を不正に得るというデモを公開
- 10月：XML暗号化仕様
  - Webサービスの実装物をplaintext validity oracle として利用
  - XML Parser のエラーの意味を解釈しながらトライ＆エラー
- 12月：TLS1.2における Truncated HMAC利用時の問題
  - RFC6066で規定された拡張機能のひとつであるTruncated HMACを用いたTLS1.2通信における脆弱性が公開
  - 通常のHMACではなく、80ビットに切り詰めたデータをMAC(データの完全性を保証する認証子)として利用する拡張方式の原理的な問題

設計

CRIME攻撃 (2012年9月)

- SSL/TLSでCompression(圧縮)機能を有効にしているケースでCookie を搾取するデモが公開
- 例え同じ長さのデータを圧縮したとしても，圧縮前に同じ文字を含むかどうかで辞書の長さが変わるという事実を用いてトライ＆エラーで暗号化データを復元する

Lucky13攻撃 (2013年1月)

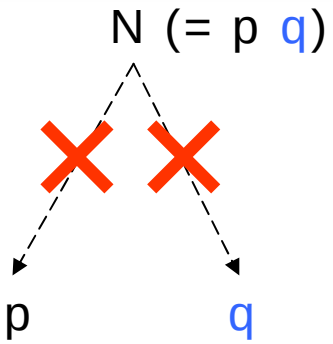
- SSL/TLSへのタイミング攻撃．演算速度の違いから情報を搾取するサイドチャネル攻撃の１種をネットを介して行う手法
- CBCモードを使わない，もしくはMACとしてHMAC-SHA1などではなくAEAD(暗号化と認証子付与を同時に行う方式)を用いる．例えば GCMモードやCCMモードなど．

- さらにRC4も死亡 (3月13日)
  - Breaking the TLS and DTLS Record Protocols

実装

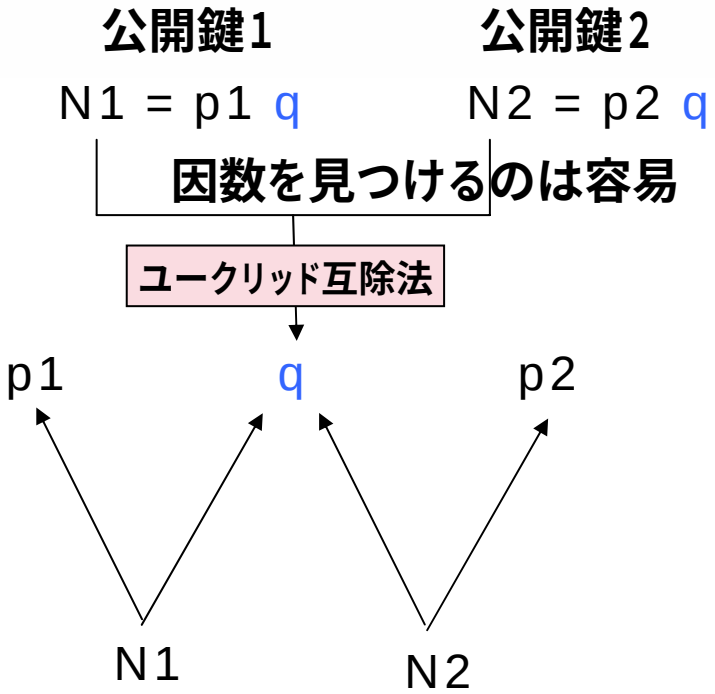
公開鍵使いまわし問題

- SSL/TLSやSSHで利用されている公開鍵証明書を収集
  → 意図せず他のサイトと秘密鍵を共有している事例
  - 機器の出荷時の鍵を利用: 5.23% (670,391ホスト)
  - 十分な鍵空間から鍵生成せず同じ秘密鍵を共有:0.34%
- RSAにて同じ秘密鍵であることが外部から同定される仕組み



素因数分解は困難

(RSAはこの困難性に
安全の根拠を置いている)



運用

PKIへの一連の攻撃

- ComodoHacker事件
  - 2011年3月 Comodo社の委託登録局(RA)のアカウントハッキングによる証明書の不正発行
  - Gmailなど著名なドメインに対するMITM攻撃
- DigiNotar認証局事件
  - 2011年8月　DigiNotar社自体への不正侵入による大量の不正な証明書発行
  - 本事件の影響により同社は翌9月に倒産
- Flame事件
  - 2012年5月 Microsoftの認証局に対するMD5選択平文攻撃による証明書の偽造
  - 未知の暗号解析手法が用いられたとの意見も
- その後も TRUKTRUSTなどPKI信頼失墜の事例が…

質問：「○○○を捨てますか？」

- **危殆化**：MD5, SHA-1
- **設計**：SSL/TLS, CBC
- **実装**：RSA
- **運用**：PKI

例：「CBCを捨てますか？」

- **単純な対策方法**：CBC→AEAD（GCM/CCM）
  - Lucky13（2**月**5**日**）**の風潮**：RC4**使おう！**
    - Lucky Thirteen: Breaking the TLS and DTLS Record Protocols
    - http://www.isg.rhul.ac.uk/tls/Lucky13.html
- **しかし**RC4**も死亡**（3**月**13**日**）
    - Breaking the TLS and DTLS Record Protocols
    - http://www.isg.rhul.ac.uk/tls
- AEAD**の普及率が課題**…

パッチの是非

- バランスが重要
  - パッチをあてたら繋がらない　(BEASTの事例)
  - パッチをあてないと危ない　MS12-006
- 互換性確保問題に帰着
  - これも移行問題の一種と考えることができる
- 結局どうすればいいのか判断基準がない…
  - 当該脆弱性に対する評価事例：CVSS

移行コストに関する評価基準が必要

- 異なる種類の暗号技術に対する同一の評価尺度を表す「等価安全性」と同様の概念
  - 80bitセキュリティ or 128bitセキュリティ
- OSやプラットフォームに依存せず一元的に扱うことができる
  - 「環境」変数を入力可能
- プロトコルやフォーマット仕様の脆弱性にも適用可能

  ＝ 暗号アルゴリズムだけに固執しない(CRYPTREC批判？)

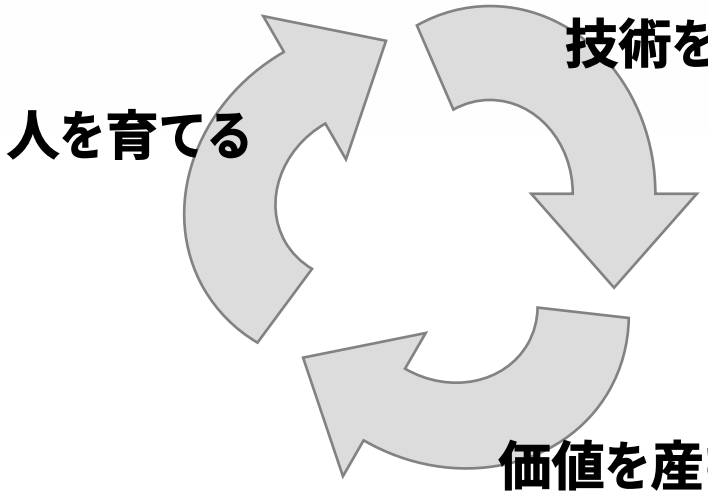
移行工学に向けて

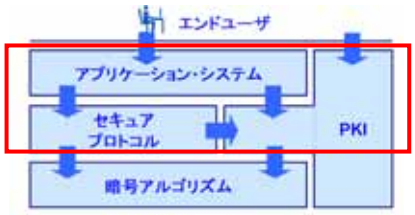
- 移行にまつわる共通的な課題･方法論の共有
- 成功･失敗事例の収集
  - 地上デジタルテレビ放送（地デジ化）
  - IPアドレス枯渇（IPv4→v6）
- ベストプラクティス→適用可能か検討したい
  - 共通課題と個別課題

2011年3月全国大会「RSA-1024はもう危険なのか？暗号2010年問題を正しく理解する」

(移行) コスト構造を変えられるか？

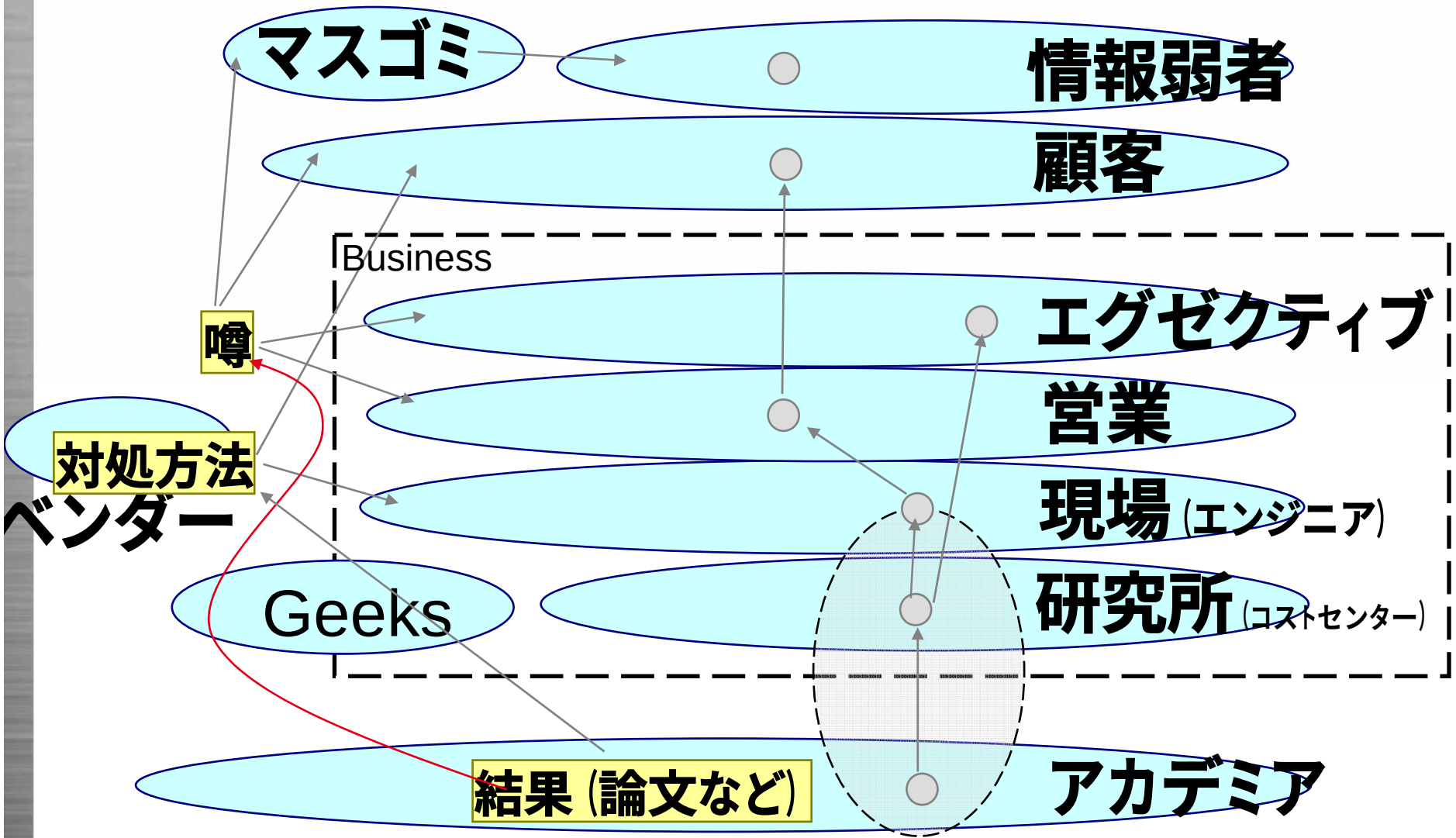
- Negativeな思考 (移行コスト負担) から
  Positiveな思考へ





個人的主張：産官学がともに嬉しい分野のひとつが
Practical Security (というロジックをうまく組み立てられるか？)

「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」

IIJ Internet Initiative Japan

インターネットの先にいます。

IIJはこれまで、日本のインターネットはどうあるべきかを考え、
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ました。
インターネットの未来を想い、イノベーションに挑戦し続けることで、世界を塗り変えていく。
それは、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/