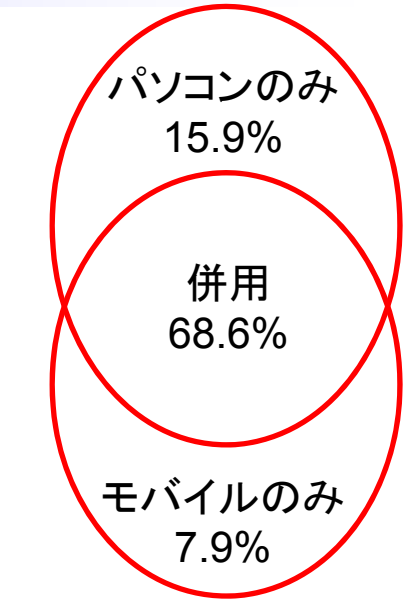
IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

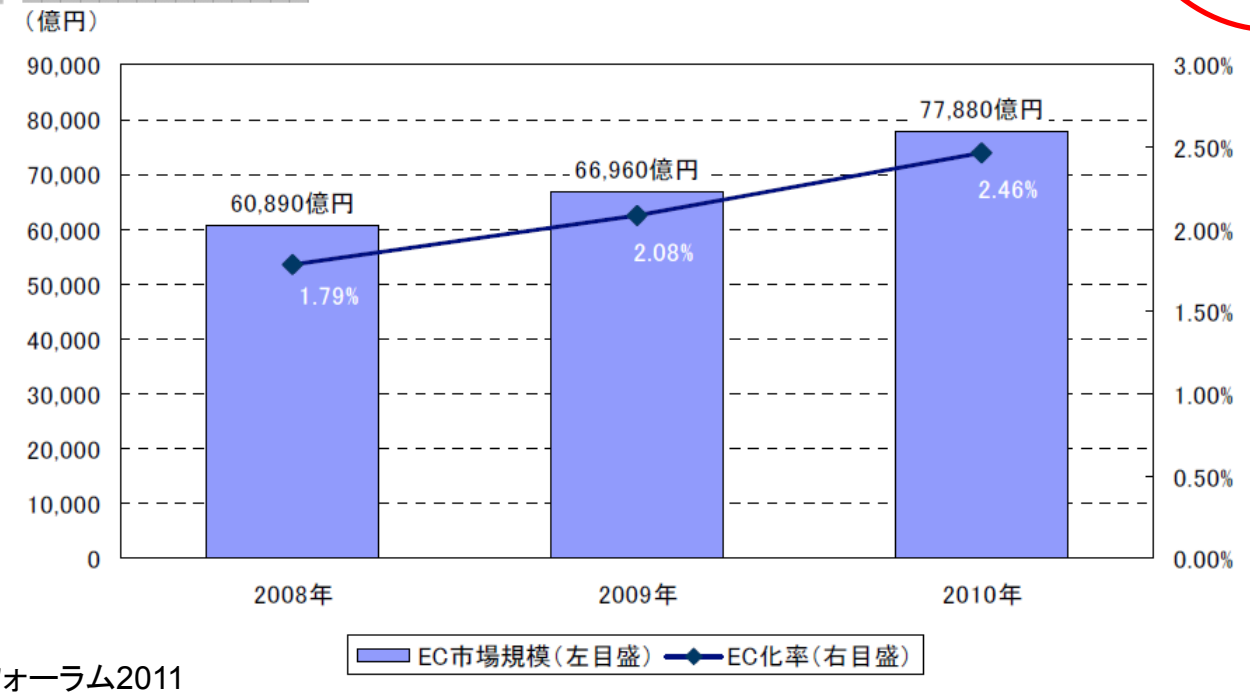
サイバー攻撃に揺らぐインターネットの信頼性
― 結局ネットの安全性を担保する根拠ってなんだろう

IPA　技術本部　セキュリティセンター
暗号グループ
神田 雅透

「平成22年度我が国情報経済社会における基盤整備」報告書

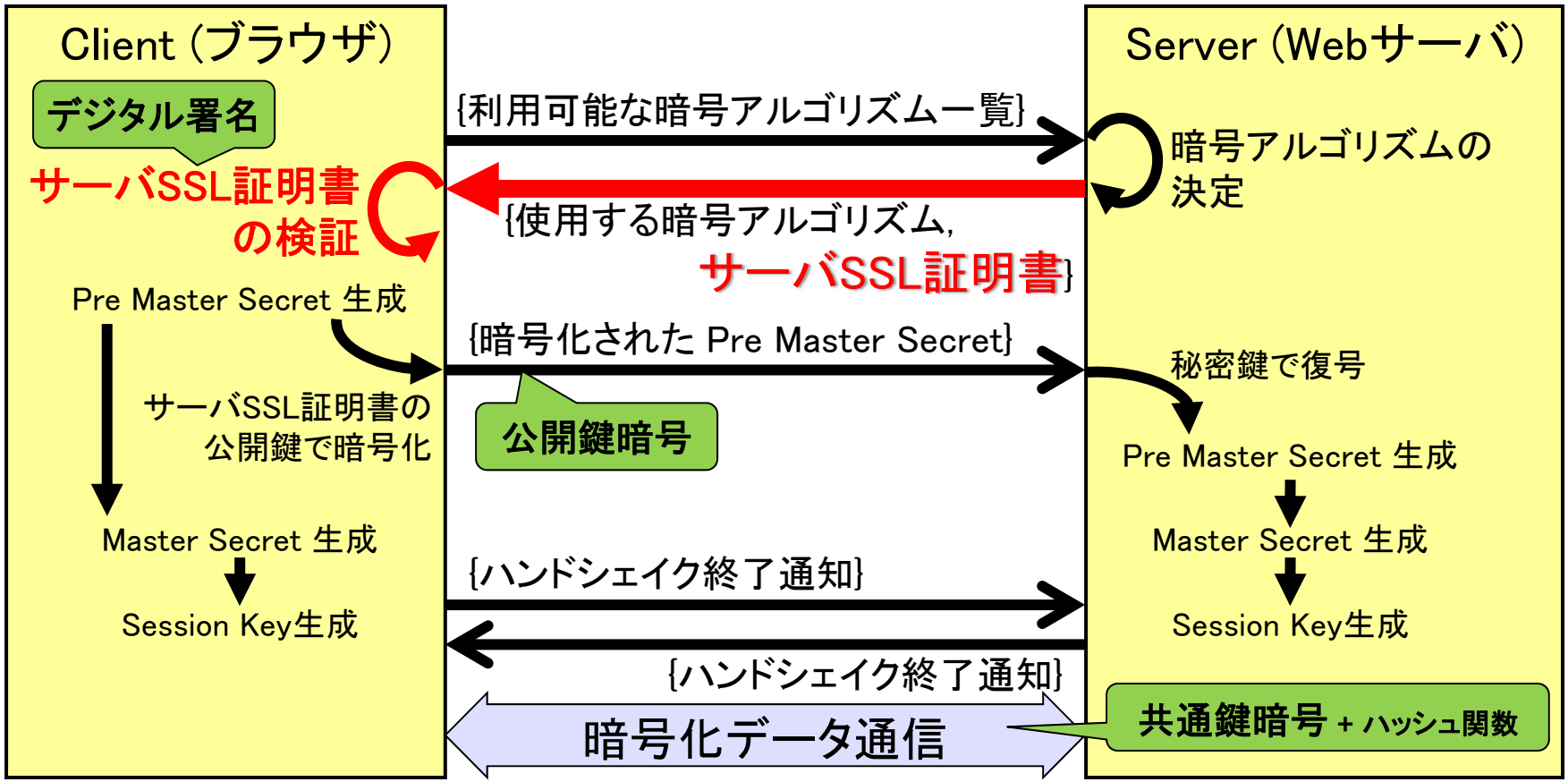
		商品・サービスの購入・取引（デジコンの購入及び金融取引を除く）	デジタルコンテンツの購入
平成20年 インターネット利用者数 9,091万人	パソコン経由でのインターネット利用者数 8,255万人	3,475万人	718万人
	携帯電話経由でのインターネット利用者数 7,506万人	743万人	1,073万人
平成21年 インターネット利用者数 9,408万人	パソコン経由でのインターネット利用者数 8,514万人	3,695万人 +220万人	1,166万人 +448万人
	携帯電話経由でのインターネット利用者数 8,010万人	1,033万人 +290万人	1,882万人 +809万人





SSL/TLS：インターネットビジネスでの必須ツール

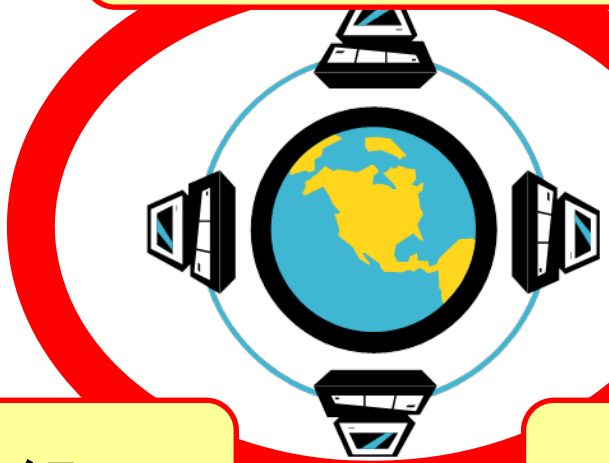
■通信の暗号化
■接続先サーバの確認



ネットの信頼性はどう担保されているの？

結局、ネットでは
どの暗号が
使われる？

技術



攻撃者

攻撃者の
目的は何？

制度・仕組み

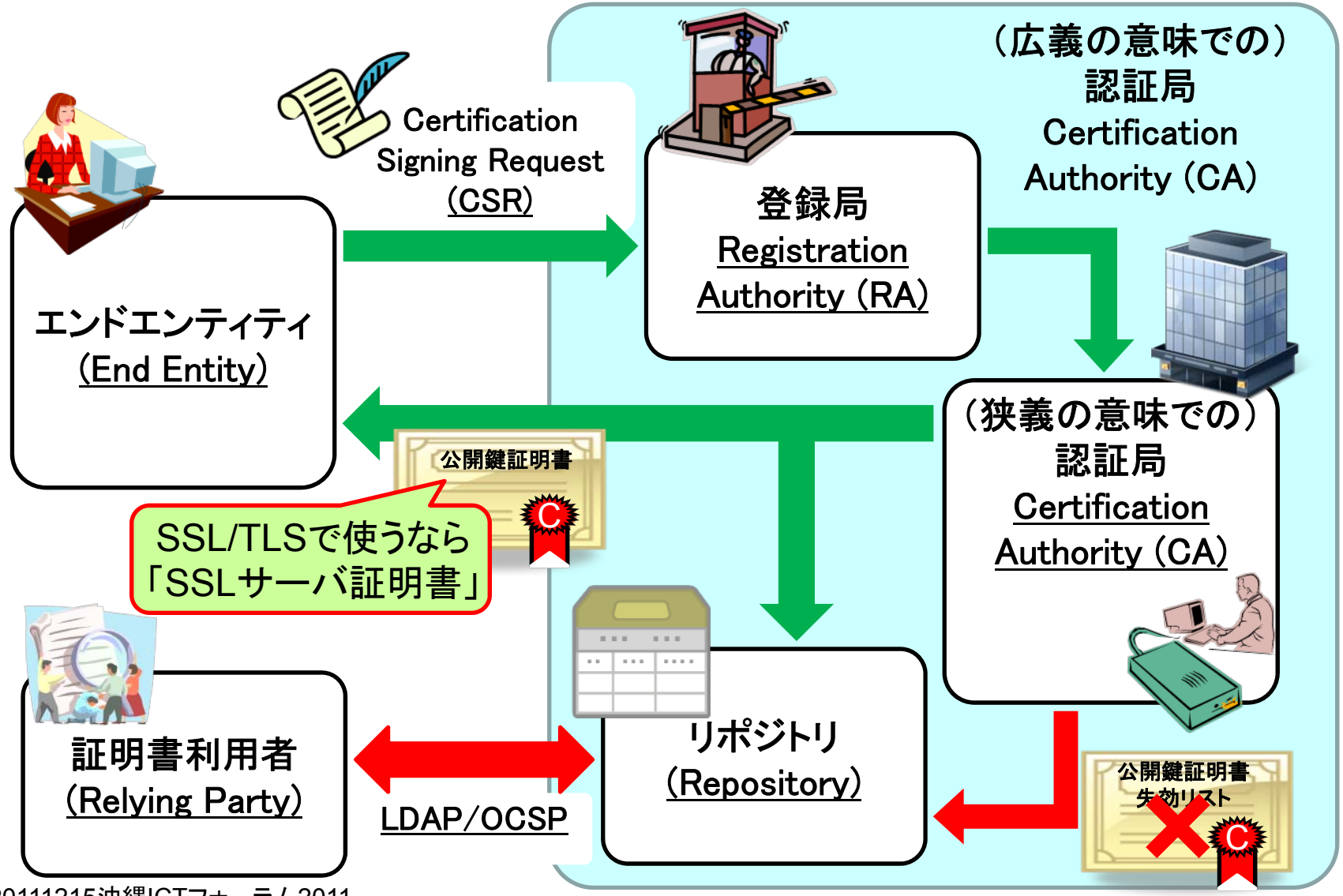
公開鍵基盤PKIの信頼性が
揺らぐと何が起きる？

運用・心がけ

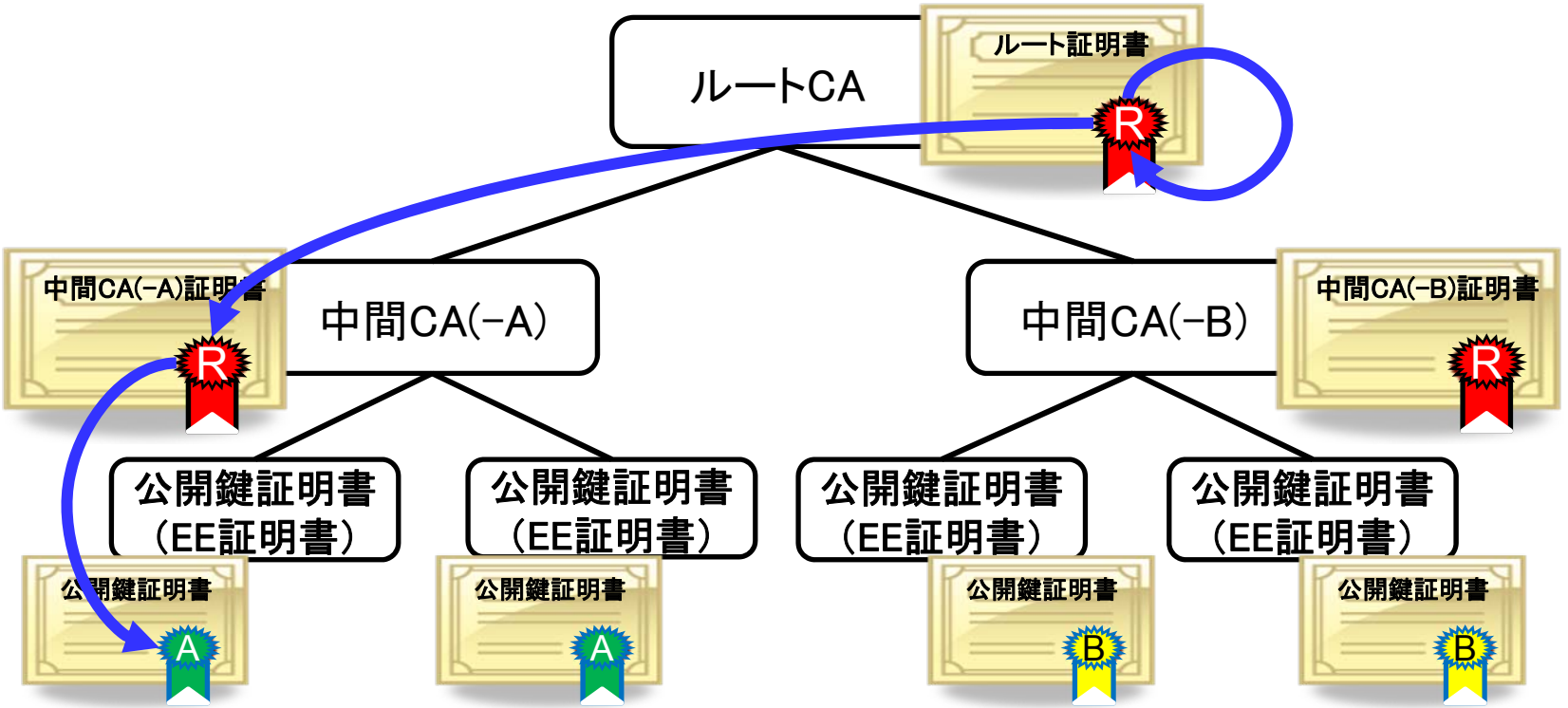
そもそもユーザのリテラシ
ってどんなもの？

公開鍵証明書は「騙されないための保険」

- 公開鍵と秘密鍵の対応関係を保証するスキーム



公開鍵基盤PKI (Public Key Infrastructure)



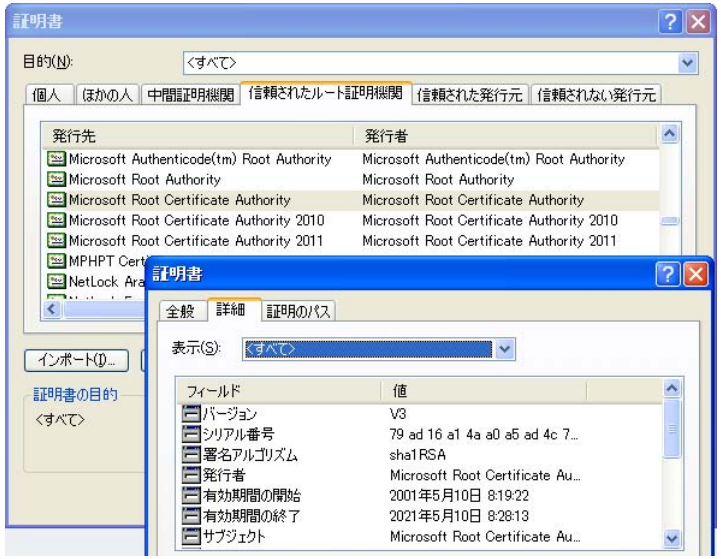
- ルートCAはPKIのTrust Anchor
  - CAはCP/CPS (Certificate Policy/Certification Practice Statement) に基づいて運営管理している（はず）
  - CP/CPSに基づいてCAが運営管理していることを監査機関は監督している（はず）

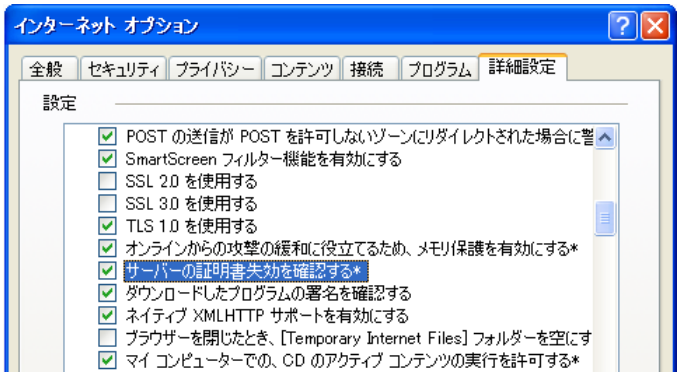
SSL/TLSを使う時に意識しないのはなぜ？

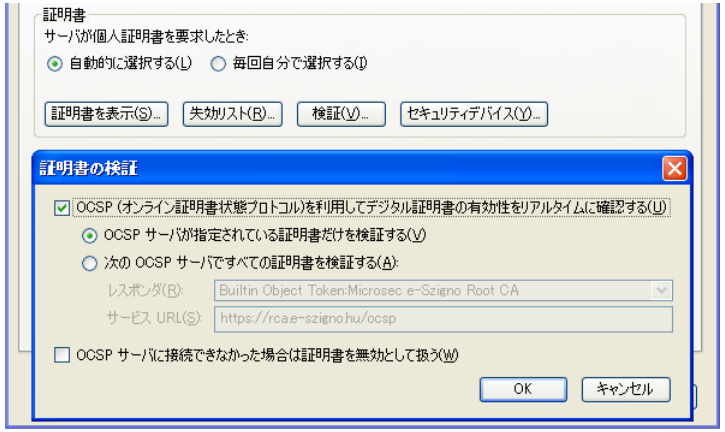
- 実際にはブラウザが自動検証する

ルート証明書のこと

  - 登録されている「信頼できる認証局証明書」をベースに判定
  - 設定次第でリアルタイム検証も可能



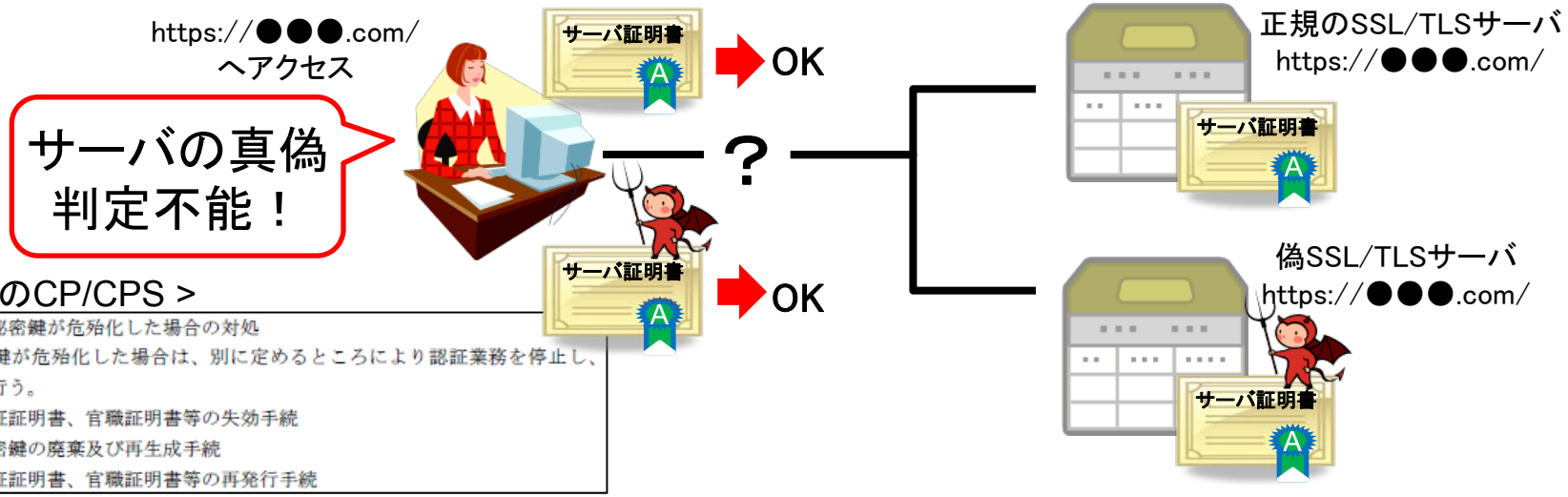




ルートCAからの不正発行は本来あってはならない

- なんらかの理由で有効期限内のSSLサーバ証明書を失効させることは“**通常業務**”の範囲内

- 認証局の管理下にないSSLサーバ証明書が不正発行される事態は業務停止にも相当する“**緊急事態**”



< GPKIのCP/CPS >

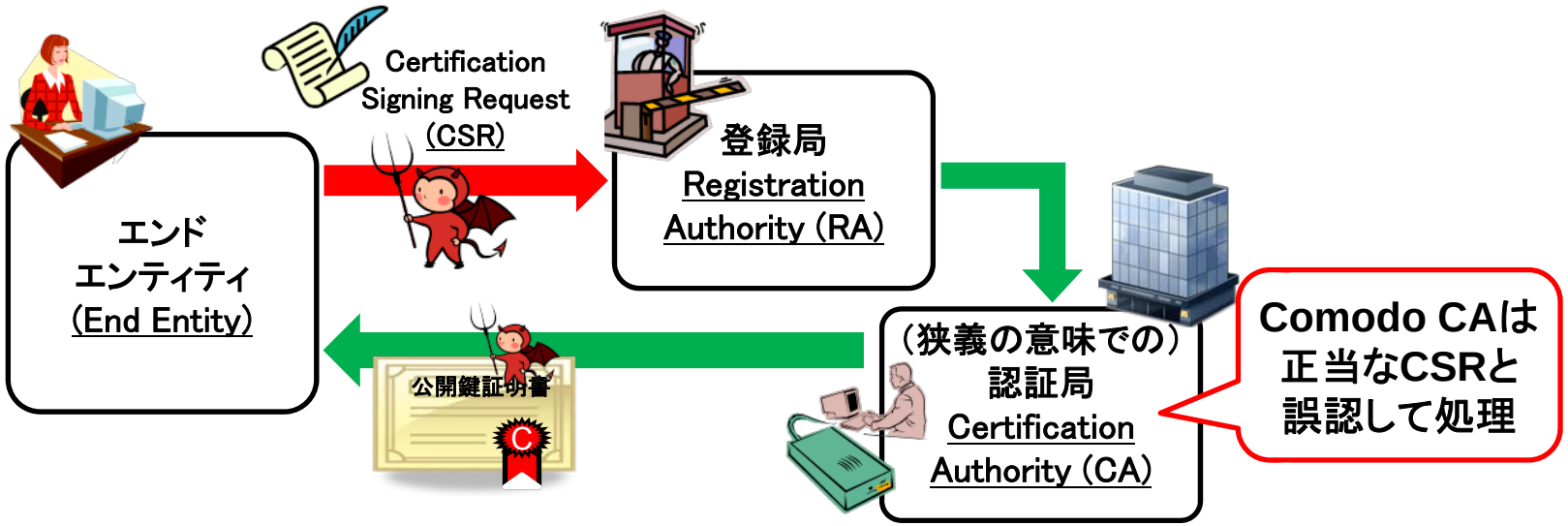
4．8．3　秘密鍵が危殆化した場合の対処

ＣＡ秘密鍵が危殆化した場合は、別に定めるところにより認証業務を停止し、次の手続を行う。

- 相互認証証明書、官職証明書等の失効手続
- ＣＡ秘密鍵の廃棄及び再生成手続
- 相互認証証明書、官職証明書等の再発行手続

Comodoのケース

- 不正SSLサーバ証明書が**通常の手続き**に則って発行
  - **Comodo RAの審査を不正にすり抜けた**結果、見掛け上正当な偽CSRに基づいて不正SSLサーバ証明書を正規発行
    - 2011年3月15日、Comodo RAに存在するユーザアカウントをクラック（主にイランに割り当てられているIPアドレスが使われた）
    - クラックされたユーザアカウント上に新たなユーザIDを作る
    - 新たなユーザIDで見掛け上正当なCSRを9つ（7ドメイン）不正に作る



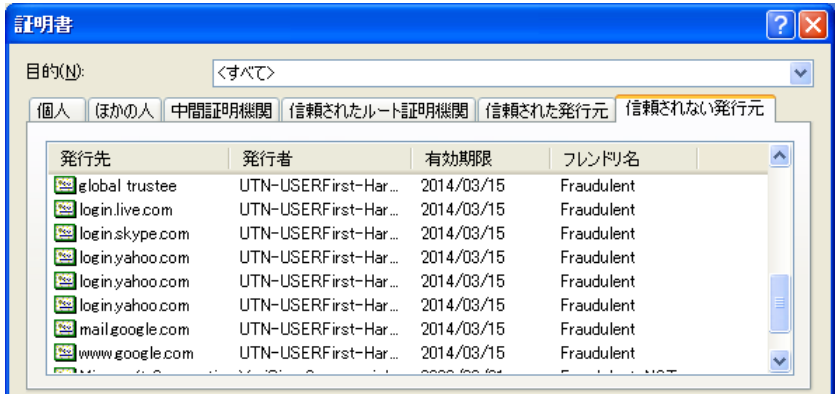
Comodoのケース

- 原因
  - Comodo RAを担うある再販事業者での運用ミスが主因
    - ハッキングするためにRSAを破ろうとしたが破るまでもなかった
    - CSR提出プロセスで使われるプログラムの一部に、テキスト形式のユーザ名とパスワードが使われていた

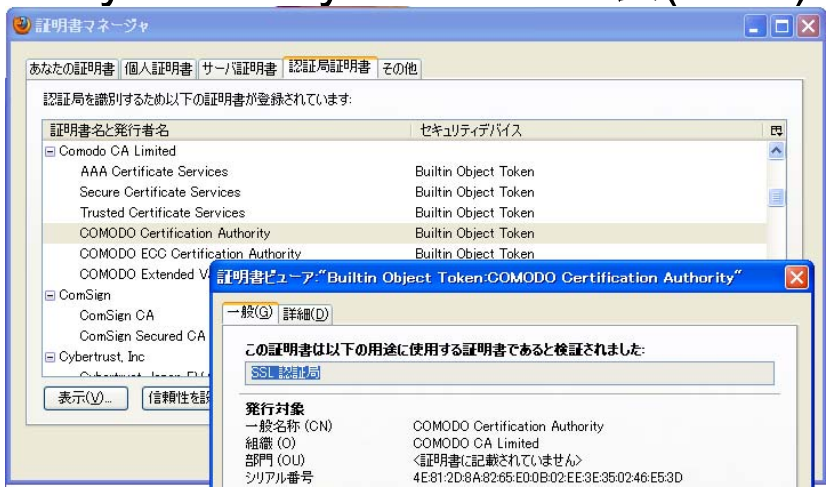
- Comodoの対処
  - 2011年3月15日以降に、RAのチェックをすり抜けた偽CSRに基づいて、Comodo CAが正規に不正SSLサーバ証明書（7ドメイン・9枚）を発行
  - 不正発覚後、速やかに関係者に通知
    - 当該SSLサーバ証明書を失効させ、証明書失効リストCRL (Certificate Revocation List)に登録
    - MicrosoftやMozillaをはじめとする主要なブラウザベンダに対してセキュリティアラートを通知

Comodoのケース

- **2011年3月22日以降**、緊急修正パッチを提供
  - **対策：当該SSLサーバ証明書の削除**
    - マイクロソフト：セキュリティアドバイザリ(2524375) 公表（24日）

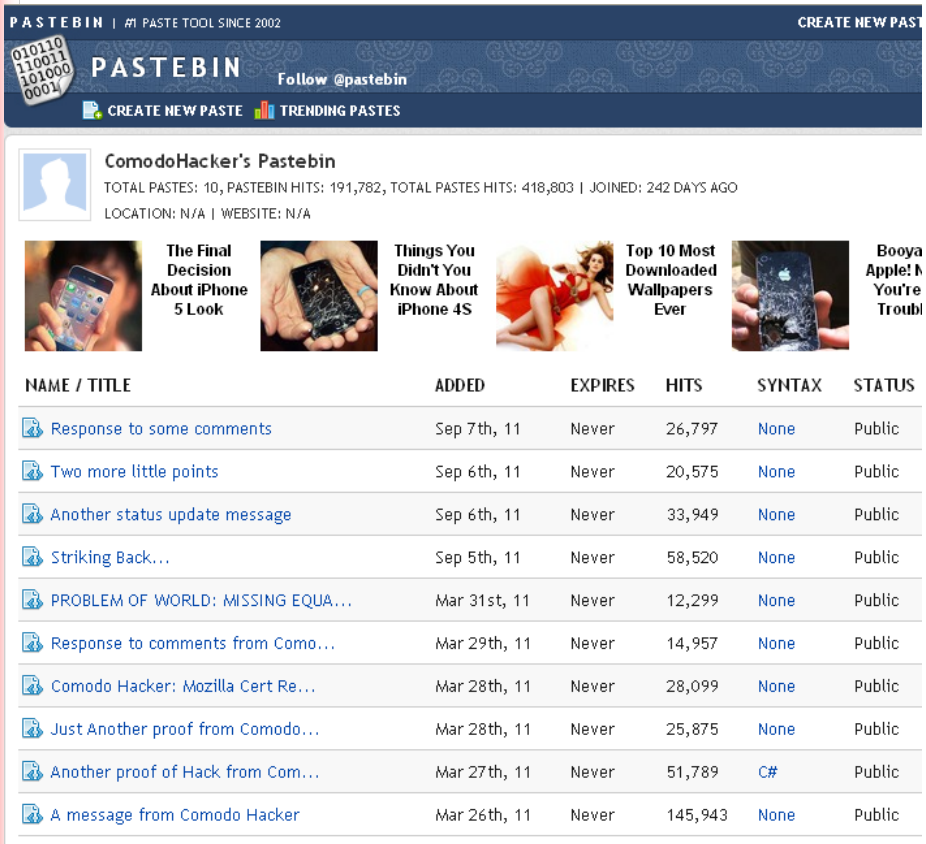


    - Mozilla：Mozilla Foundation Security Advisory 2011-11公表(22日)



Comodo Hackerって何者？

Comodo, DigiNotarを始め、複数のCAを攻撃したとの犯行声明を出したComodo Hacker



NAME / TITLE	ADDED	EXPIRES	HITS	SYNTAX	STATUS
Response to some comments	Sep 7th, 11	Never	26,797	None	Public
Two more little points	Sep 6th, 11	Never	20,575	None	Public
Another status update message	Sep 6th, 11	Never	33,949	None	Public
Striking Back...	Sep 5th, 11	Never	58,520	None	Public
PROBLEM OF WORLD: MISSING EQUA...	Mar 31st, 11	Never	12,299	None	Public
Response to comments from Como...	Mar 29th, 11	Never	14,957	None	Public
Comodo Hacker: Mozilla Cert Re...	Mar 28th, 11	Never	28,099	None	Public
Just Another proof from Comodo...	Mar 28th, 11	Never	25,875	None	Public
Another proof of Hack from Com...	Mar 27th, 11	Never	51,789	C#	Public
A message from Comodo Hacker	Mar 26th, 11	Never	145,943	None	Public

- 「イラン在住の21歳の一匹狼のクラッカー」と自称
- 「イラン政府や軍とは無関係」と主張
- 「イラン反体制派組織に恐怖を与え、イラン国民、核技術者、大統領の守護者」を自任
- 同一人物の攻撃であることの痕跡をあえて残している

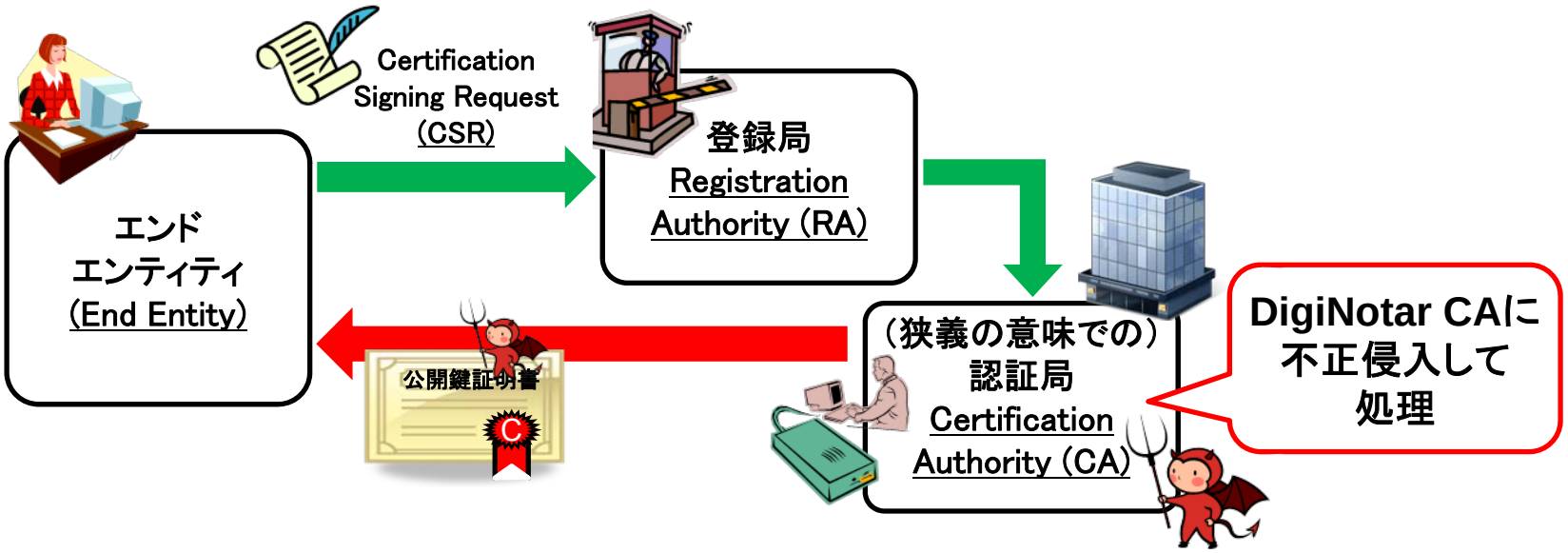
Comodo Hackerって何者？

米国などが主導するようなインターネット社会や情報化社会を否定、IT基盤に打撃を与えることが目的

- イラン核問題をはじめとする、イラン政府やイラン国民に対する米国やイスラエルの攻撃に対する報復を示唆
- DigiNotarを狙ったのはオランダへの報復と主張
  - オランダGPKIに打撃を与える目的
- 少なくともさらに3つ以上のCAに対して攻撃が成功？
  - StartCOM(本拠：イスラエル)：
    - HSM接続成功、電子メールやDBバックアップ、顧客情報などを入手
  - GlobalSign(本拠：日本)：
    - 全サーバへのアクセス成功、DBバックアップ、 ならびに米国のglobalsign.comドメインの個別鍵を入手
    - 発行業務一時停止を含む緊急対応により安全性を確認

DigiNotarのケース

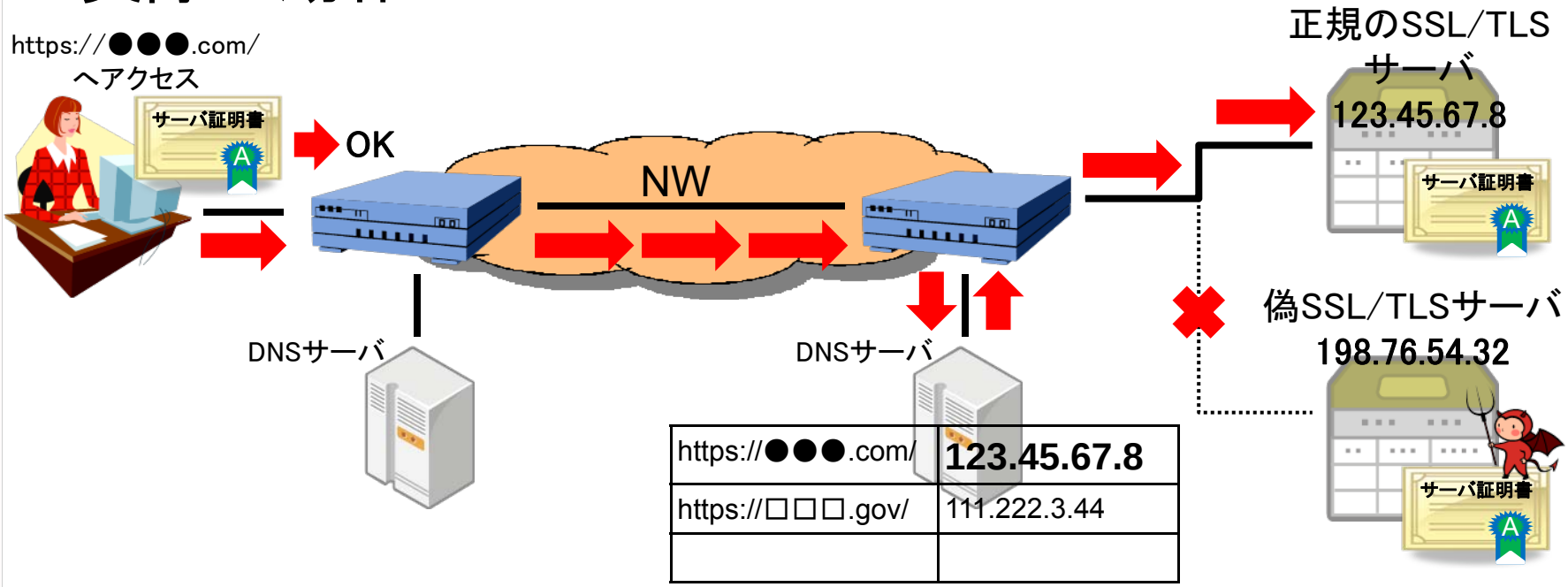
- 不正SSLサーバ証明書が**CA機能を乗っ取られて**発行
  - EV-SSLサーバ証明書発行用CAを含め、少なくとも**6つのCA（疑いを含めると30個のCA）に不正侵入**され、不正SSLサーバ証明書を発行
    - 2011年7月19日に128枚、20日に129枚発行されたのを含め、少なくとも**合計531枚**の不正SSLサーバ証明書が発行されていた
    - 2011年6月17日から今回の攻撃が始まっていたことを把握



普段なら実害は少ない、はずなのだが・・・

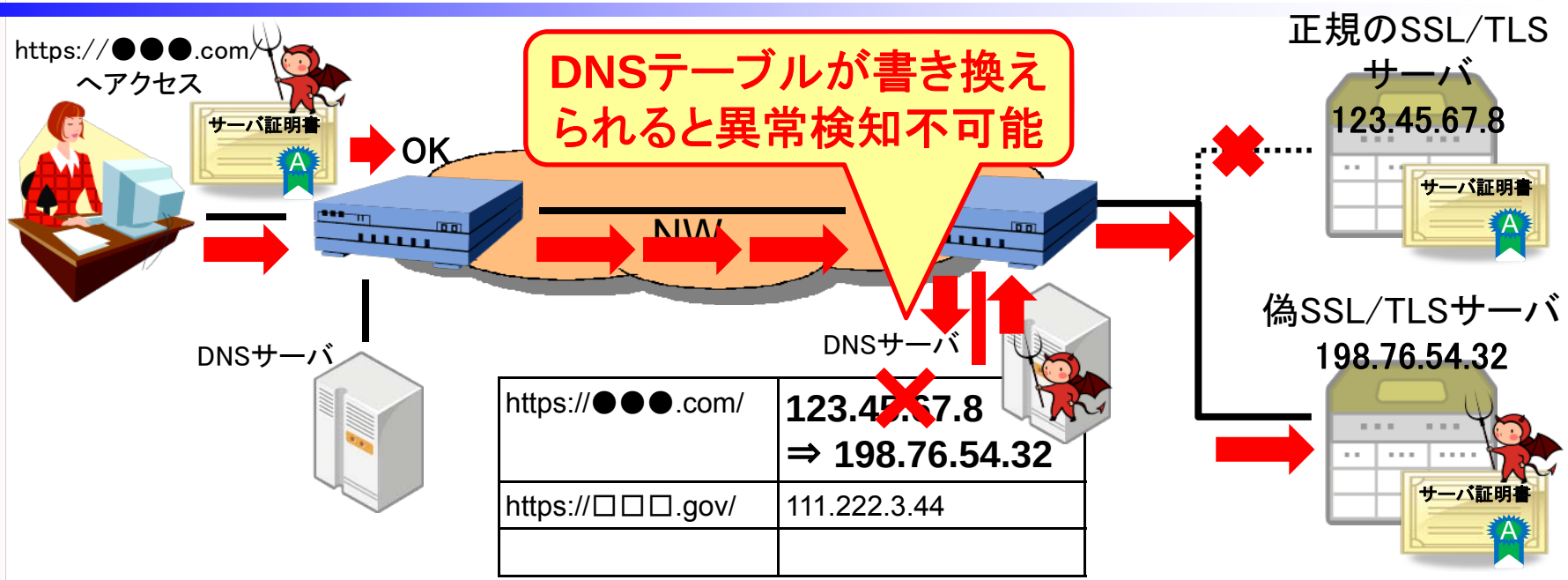
偽SSL/TLSサーバ証明書を不正発行した“だけ”なら
実害には繋がらない・・・はずだった

■ 実際の動作



実害に結びつけるには、DNSサーバを改ざんするか、
Man-in-the-middle attackをするか

実害が発生した可能性が高い



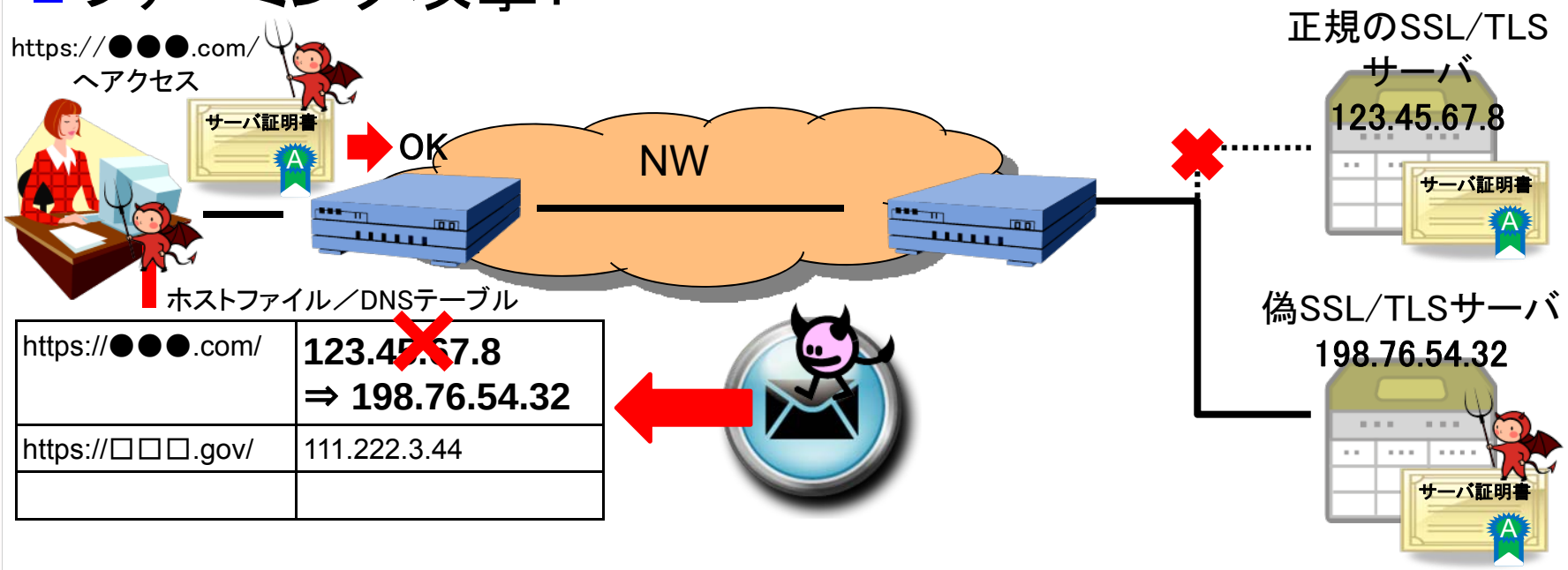
「政府機関(体制側)等による盗聴行為」が
イラン国内で実際に行われた可能性がある

- イラン周辺で不正発行されたSSLサーバ証明書に対するOCSPリクエストが多発
- 不正発行されたSSLサーバ証明書に、Googleのほか、イスラエル諜報特務局、MI6、CIA等の諜報機関が含まれた

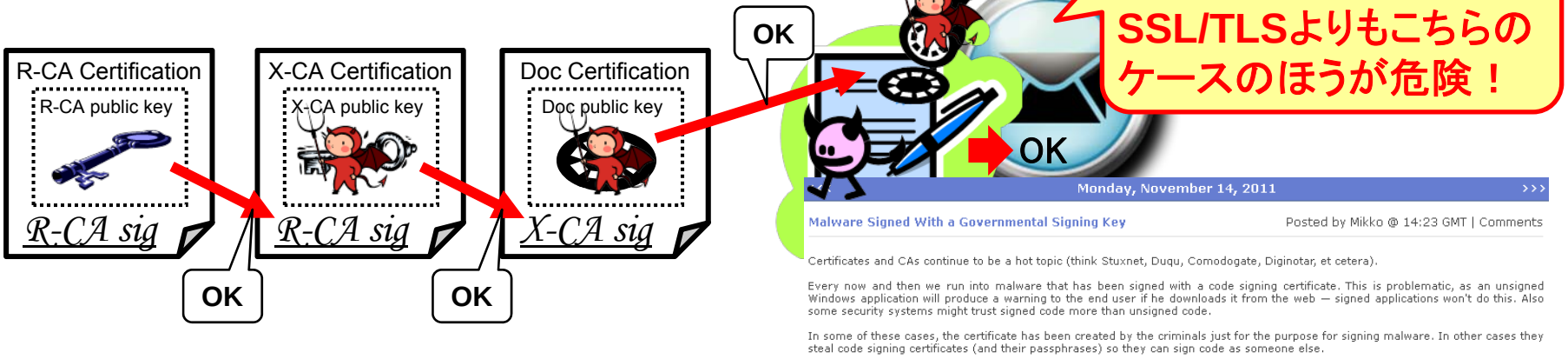
不正*.google.com証明書のOCSPリクエスト

標的型攻撃に使われるともっと危ない

■ ファーミング攻撃：



■ 署名付きドキュメント類の偽造：



PKIの危機を招いたもの

ルートCAのずさんな運営管理と見過ごした監査体制
～ ルートCAの水準と監査品質の均一性への懸念 ～

- ルートCAとしてはあまりにも重大な失態が相次ぐ
  - 事件報道されるまでの5週間、事実を隠ぺいし続けた
    - 2011年7月19日以降、短期間に不正SSLサーバ証明書の発行・失効処理が繰り返されていたにも関わらず、根本的な対策を取らなかった
    - 2011年6月17日から今回の攻撃が始まっていたことを把握
    - 7月28日イランで不正SSLサーバ証明書が悪用されていることを把握
    - OSやブラウザ等のベンダにもその事実を通知しなかった

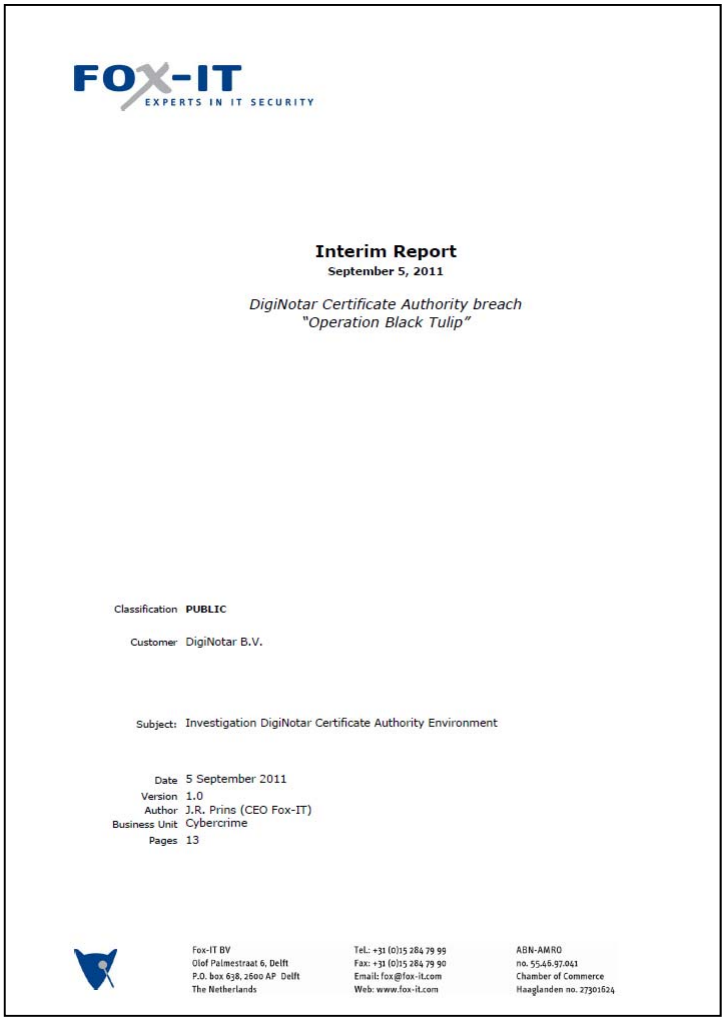
イランで在住の人がGmailにアクセスしたときに不正が発覚

when I used a vpn I didn't see any warning ! I think my ISP or my government did this attack (because I live in Iran and you may hear something about the story of Comodo hacker!)

PKIの危機を招いたもの

- CP/CPS違反もしくはCP/CPS自体に重過失があったことを強く疑わせる運用管理体制
  - ウイルス対策ソフトが機能しておらず、通常検出可能なマルウェアやウイルスが重要サーバに入り込んだまま
  - 本来は外部ネットワークから分離して設置されるはずのCAサーバに業務用LANからアクセス可能
  - 同じIDとパスワードで全CAサーバにアクセス可能なネットワーク構成
  - 強いパスワードが使われていたわけではなかった
  - 公開サーバに対してセキュリティ修正パッチが適用されていなかった
  - アクセスログが安全に所定場所に保管される仕組みではなかった

オランダ政府の承認のもとに公表された中間報告書



FOX-IT
EXPERTS IN IT SECURITY

Interim Report
September 5, 2011

DigiNotar Certificate Authority breach
"Operation Black Tulip"

Classification **PUBLIC**

Customer DigiNotar B.V.

Subject: Investigation DigiNotar Certificate Authority Environment

Date 5 September 2011
Version 1.0
Author J.R. Prins (CEO Fox-IT)
Business Unit Cybercrime
Pages 13

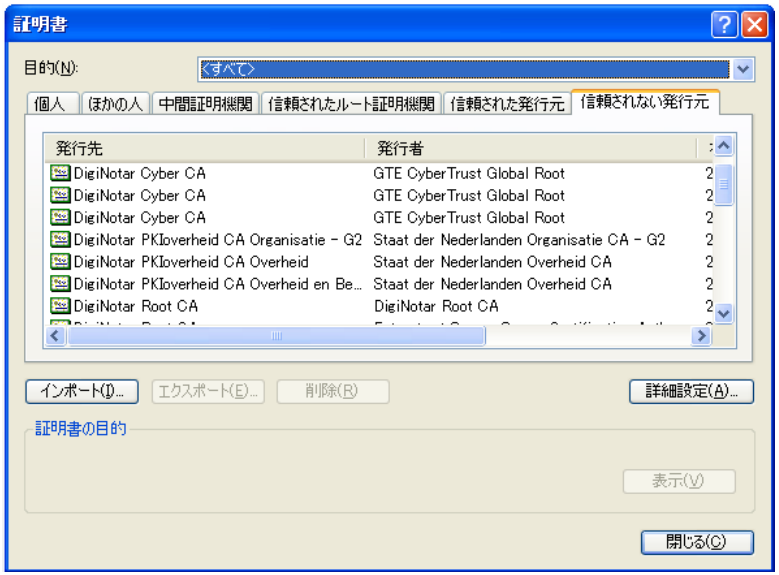
Fox-IT BV
Olof Palmestraat 6, Delft
P.O. box 638, 2600 AP Delft
The Netherlands

Tel.: +31 (0)15 284 79 99
Fax: +31 (0)15 284 79 90
Email: fox@fox-it.com
Web: www.fox-it.com

ABN-AMRO
no. 55.46.97.041
Chamber of Commerce
Haaglanden no. 27301624

PKIの危機を招いたもの

- 主要ブラウザベンダの対処
  - 事件報道後、主要ブラウザベンダは緊急の修正パッチを提供
    - 対策：**DigiNotarのルート証明書を削除**



➡ DigiNotarの業務停止
破産手続き開始

オランダGPKIのルートCAの一つが潰れた
⇒ Comodo Hackerの目的達成

VASCO Announces Bankruptcy Filing by DigiNotar B.V.

OAKBROOK TERRACE, IL, and ZURICH, Switzerland, September 20, 2011 - VASCO Data Security International, Inc. (Nasdaq: VDSI) (www.vasco.com) today announced that a subsidiary, DigiNotar B.V., a company organized and existing in The Netherlands ("DigiNotar") filed a voluntary bankruptcy petition under Article 4 of the Dutch Bankruptcy Act in the Haarlem District Court, The Netherlands (the "Court") on Monday, September 19, 2011 and was declared bankrupt by the Court today.
The Court appointed a bankruptcy trustee (the "Trustee") and a bankruptcy judge (the "Judge") to manage all affairs of DigiNotar as it proceeds through the bankruptcy process. The Trustee will work under the supervision of the Judge and be responsible for the administration and liquidation of DigiNotar. The Trustee is required to report to the Judge and his reports are expected to be made available to the public and will serve as a source of information to the creditors and other stakeholders. Effective as of the beginning of business today, the Trustee has taken over the management of DigiNotar's business activities.

PKIの危機を招いたもの

- もっと問題なのは・・・ことの真相がはっきりしないこと
  - FOX-ITレポートに書かれていることとComodo Hackerがいっていること（特にシステム構成）に食い違いがある

FOX-ITレポートが正しければ
DigiNotar特有の問題ともいえるほど
システム構成・運用が杜撰な認証局が
PKIに組み込まれていたという問題になる

Comodo Hackerが正しければ
一般的なシステム構成をもつ認証局なら
どこでも同じように攻撃される恐れがある
という問題になる

- WebTrust for CA認証制度の信頼性への問題
  - オランダ監査機関も問題を指摘できず

Dutch SSL authority KPN stops issuing certificates after hack

Published: 07 November 11, 12:56 GMT

The largest telecommunications company in the Netherlands has stopped issuing SSL certificates after finding indications that the website used for purchasing the certificates may have been hacked.

The back-end infrastructure used to generate certificates does not appear to have been affected, although an investigation is under way with results expected soon, KPN spokeswoman Simona Petescu said.

During an audit, the public-facing website showed indications that someone may have tried to prepare it for Distributed Denial-of-Service (DDoS) attacks as long as four years ago, according to a KPN press release. It does not appear that any fraudulent SSL certificates have been created, Petescu said. But as a precaution, it stopped issuing certificates and also notified the Dutch government's interior affairs ministry, she said.

Dutch SSL Certificate Provider Gemnet Investigates Website Compromise

Gemnet, a Dutch company that provides SSL certificates for the Dutch government, has closed down its website after it was compromised by a hacker who found...

By Lucian Constantin
Dec 8, 2011 7:20 AM

Gemnet, a Dutch company that provides SSL certificates for the Dutch government, has closed down its website after it was compromised by a hacker who found sensitive information on the server hosting it.

According to Webwereld, the hacker was able to break into gemnet.nl through a phpMyAdmin installation that wasn't password-protected. PhpMyAdmin is a popular software utility that facilitates the administration of MySQL databases through a Web interface.

現状ではDigiNotarほどひどいことにはなっていないが
立て続けに問題が発覚したということは・・・

対応策は？

WebTrust for CAを取得しているCAが発行した不正SSLサーバ証明書をいかに早く失効させるか

- 緊急のセキュリティ更新パッチは必ず適用
  - “定例”の修正パッチ提供まで待てない理由がある
- 携帯電話・スマートフォン向けのセキュリティ更新プログラムの提供は一般に遅れることに留意
  - 携帯電話に入っているルート証明書はもともと少ないが、スマートフォンにはそれなりに多く入っている
- 可用性は大きく損なわれるが、特に信頼できるCA以外のルート証明書を手動削除する案もあり
  - 特に政情不安な国や情報統制を行っている国では有効かも
- **結局のところ“ナショナルセキュリティ”の問題か？**

まとめにかえて

国家権力と結びついたサイバー攻撃を
エンドユーザレベルで防御するのは難しい

- 現在のインターネットの仕組みは、エンドユーザが異常検知できない状況下で攻撃することも可能
  - Trust Anchorをどこに持っていくかの課題
    - ナショナルセキュリティそのもの、かも
  - 国家権力がコントロールするネットワークは信頼性に欠ける
  - 攻撃を受けた国と被害が発生する国が違うこともある
- セキュリティ更新パッチ適用は防御のための最低条件
  - 究極的にはブラウザベンダと認証局は信用するしかない
- ウイルス対策ソフトの導入とパターンファイルの更新
  - ウイルス感染したままだと対策技術を導入しても守りきれない