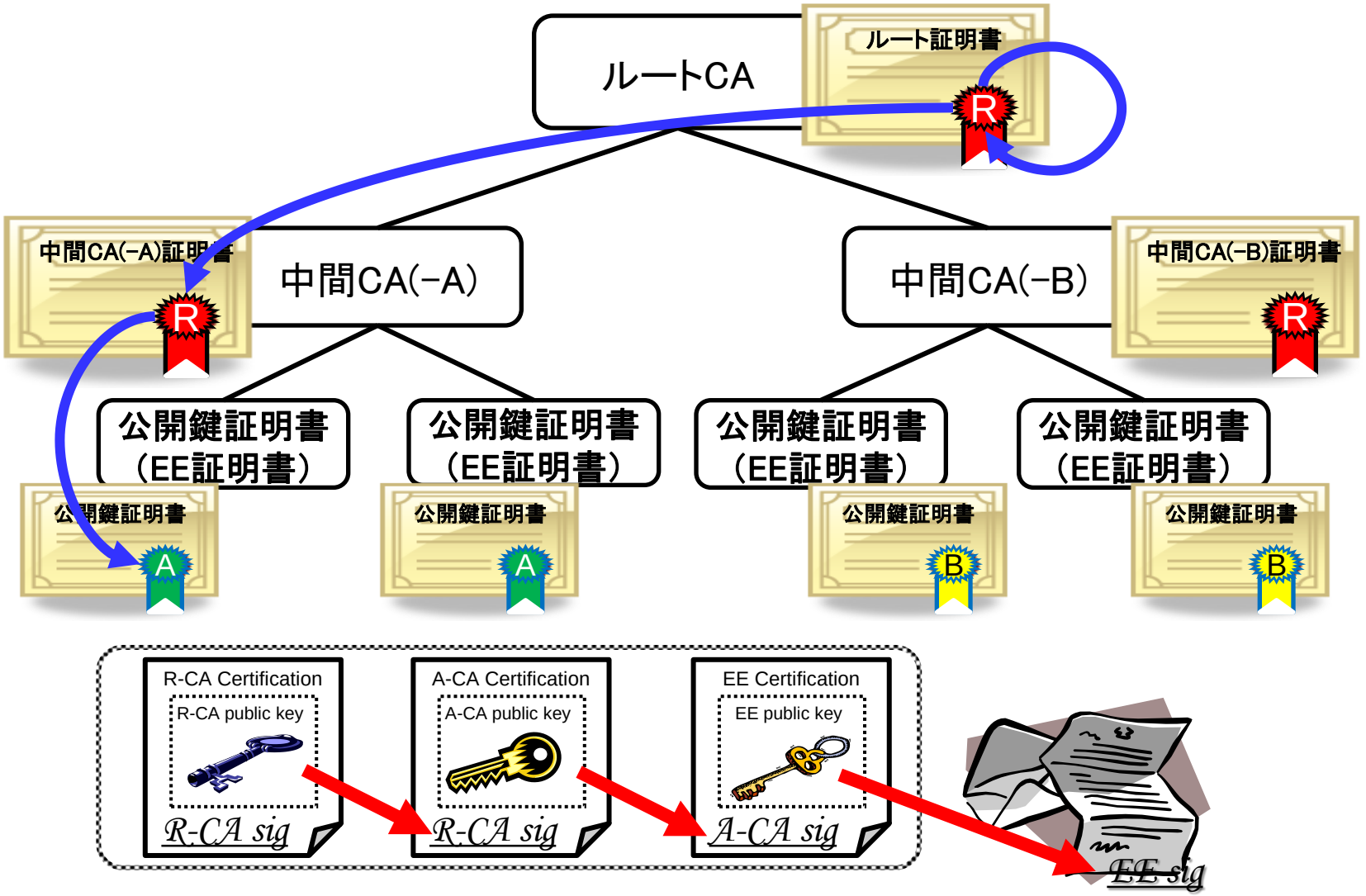
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

サイバー攻撃ツールとしての公開鍵証明書の役割

～信頼の起点にカモフラージュされた攻撃の起点～

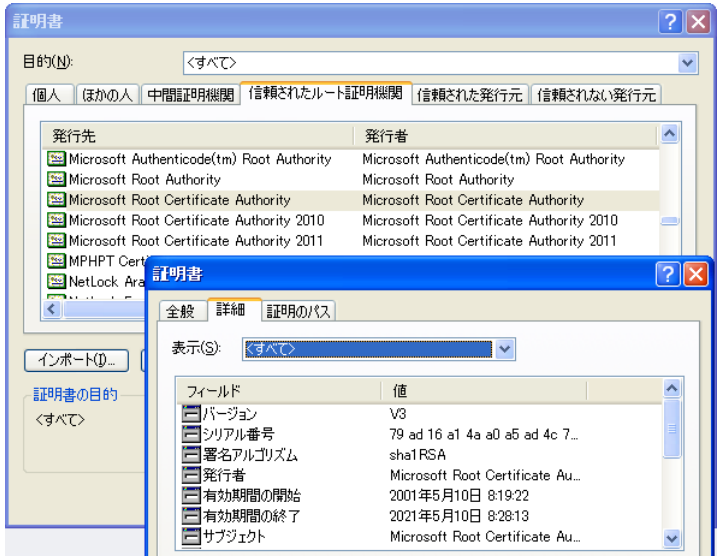
IPA　技術本部　セキュリティセンター
暗号グループ
神田 雅透

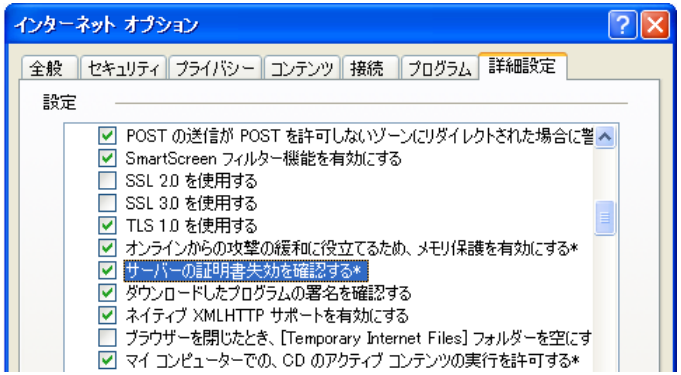
ルートCAはPKIのTrust Anchor

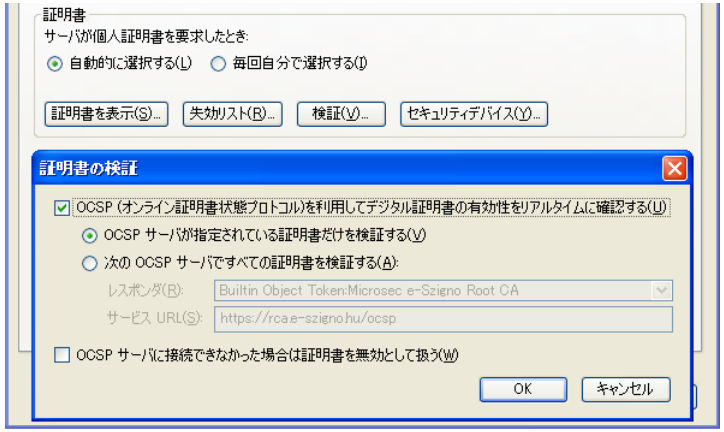


証明書を使うのを意識しないのはなぜ？

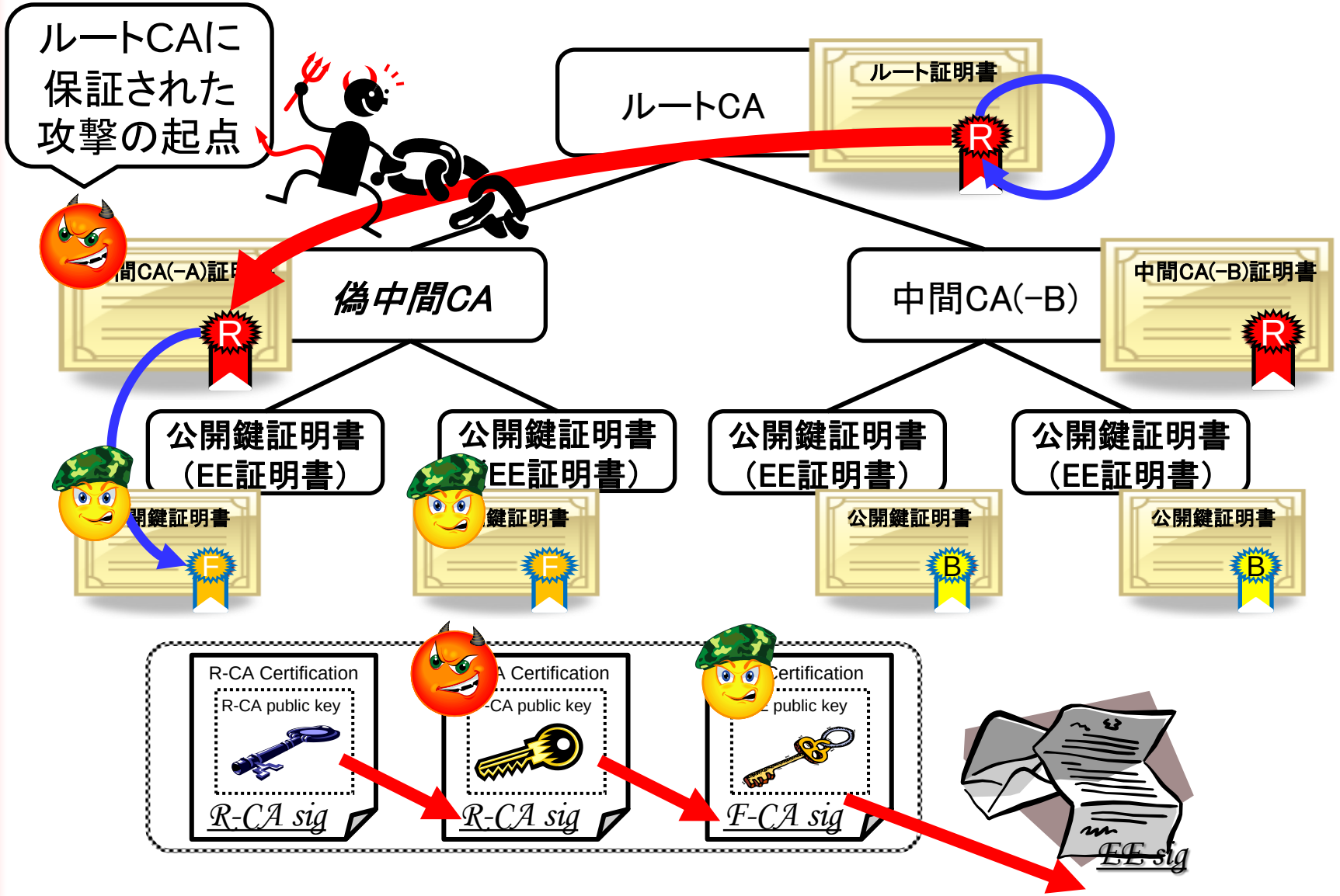
- 実際にはブラウザやアプリケーションが自動検証する
  - 登録されている「信頼できる認証局証明書」をベースに判定
  - 設定次第でリアルタイム検証も可能







秘かに入り込もうとするなら・・・



公開鍵証明書が悪用されるのはどんな時？

- ハッキングの問題
  - **登録局での検証ミス**によって不正な公開鍵証明書を認証局が誤って発行（例：Comodo事件）
  - **認証局への不正アクセス**によって不正な公開鍵証明書を発行（例：Diginotar事件）
- 暗号技術の問題
  - 力づくで公開鍵情報から**秘密鍵を割り出す**（公開鍵暗号の問題）
  - **真正な公開鍵証明書と区別ができない**不正な公開鍵証明書を計算機によって偽造（ハッシュ関数の問題）
- 運用の問題
  - 公開鍵証明書に対応する**秘密鍵が流出**（例：マレーシア政府の署名鍵流出事件）
  - 意図せず**秘密鍵を共有**。。。

この後に須賀さんから

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

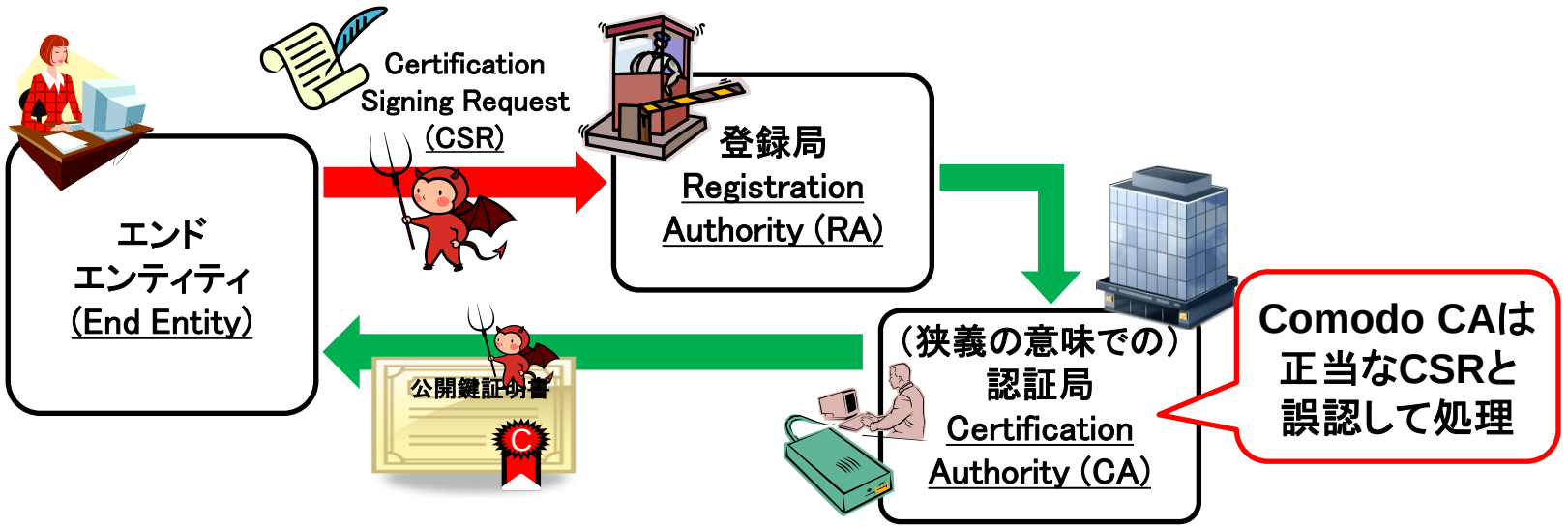
- 「イラン在住の21歳の一匹狼のクラッカー」と自称
- 「イラン政府や軍とは無関係」と主張
- 「イラン反体制派組織に恐怖を与え、イラン国民、核技術者、大統領の守護者」を自任
- 同一人物の攻撃であることの痕跡をあえて残している

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

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

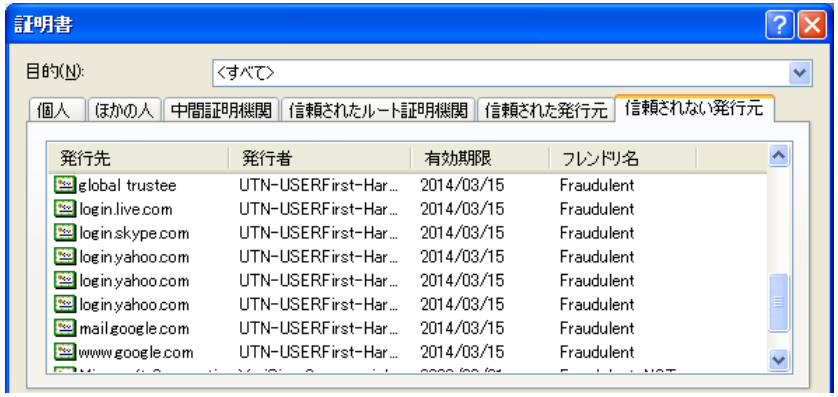
- Comodo RAを担うある再販事業者での運用ミスが主因
  - ハッキングするためにRSAを破ろうとしたが破るまでもなかった
  - CSR提出プロセスで使われるプログラムの一部に、**テキスト形式のユーザ名とパスワード**が使われていた

Comodoの対処

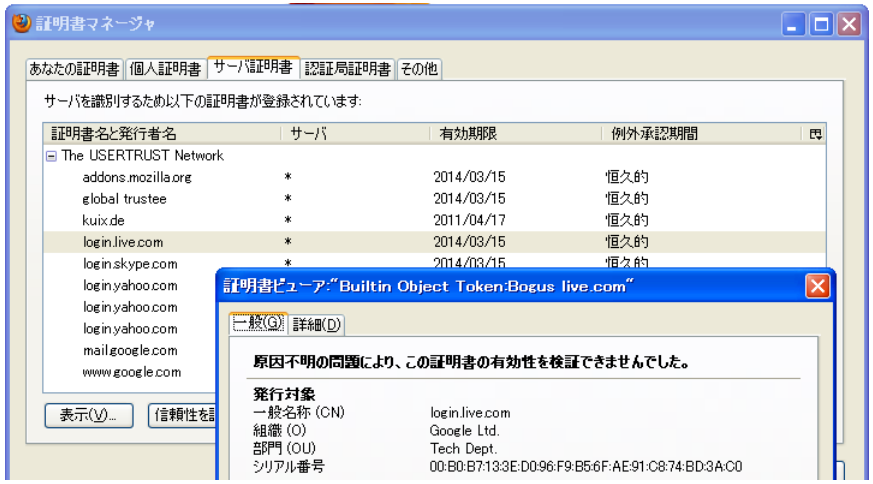
- **2011年3月15日以降**に、RAのチェックをすり抜けた偽CSRに基づいて、Comodo CAが正規に不正SSLサーバ証明書（7ドメイン・9枚）を発行
- 不正発覚後、速やかに関係者に通知
  - 当該SSLサーバ証明書を失効させ、証明書失効リストCRL (Certificate Revocation List)に登録
  - MicrosoftやMozillaをはじめとする主要なブラウザベンダに対してセキュリティアラートを通知

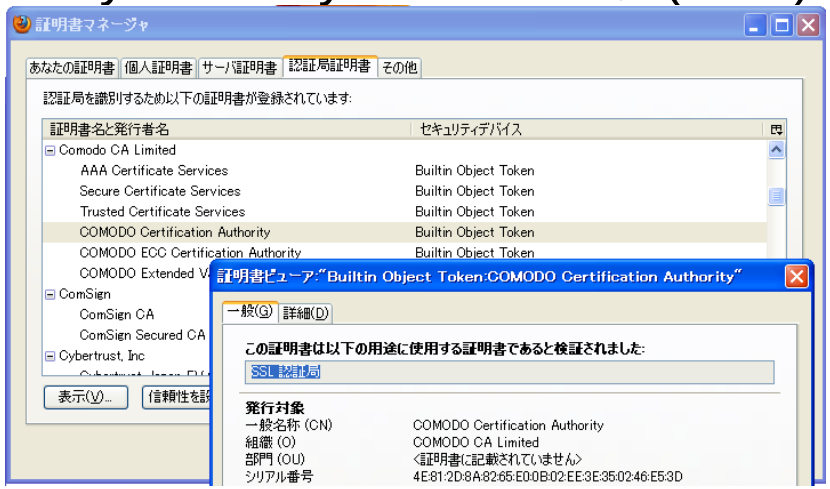
Comodoのケース

- **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）



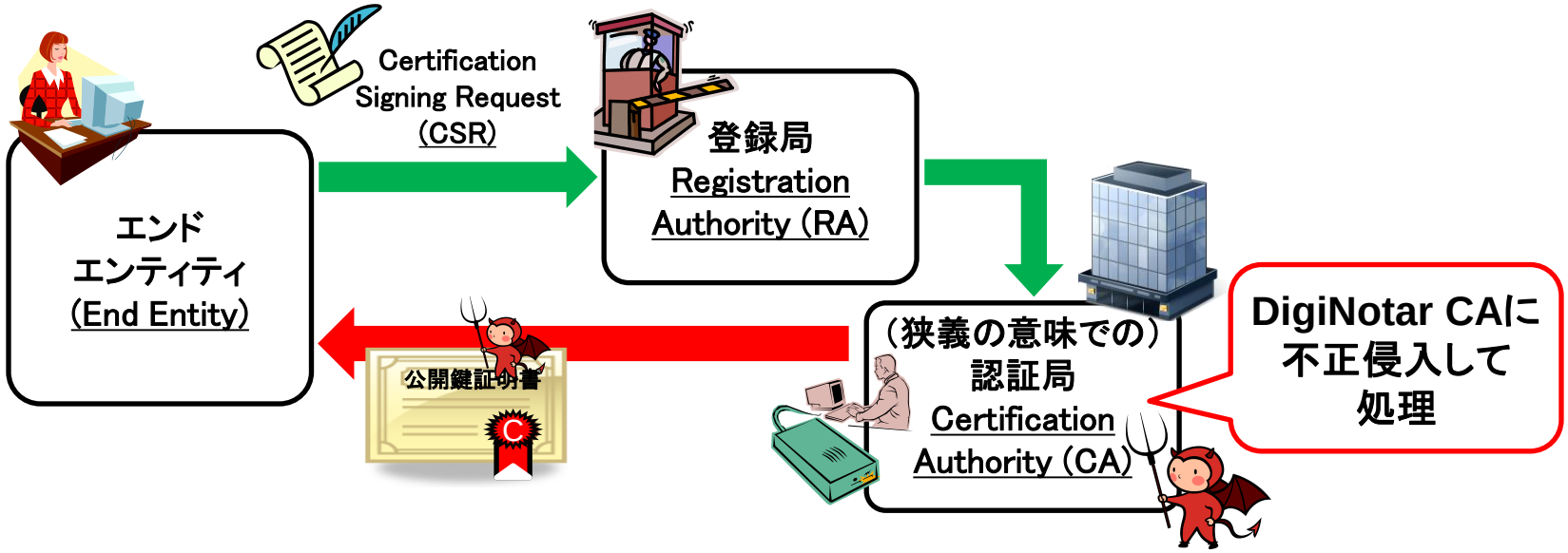
    - Mozilla：Mozilla Foundation Security Advisory 2011-11公表(22日)





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



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

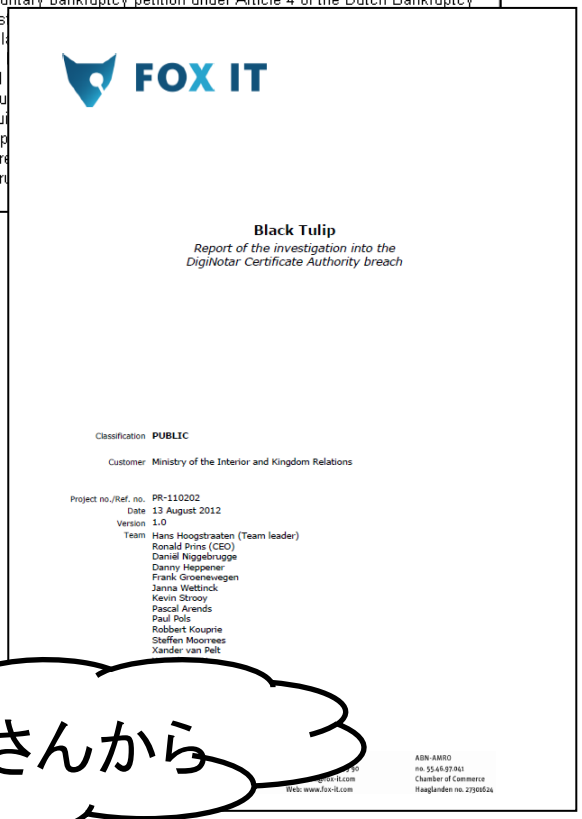
- 主要ブラウザベンダの対処
  - 事件報道後、主要ブラウザベンダは緊急の修正パッチを提供
    - 対策：**DigiNotarのルート証明書を削除**

➡ 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 Dis
19, 2011 and was decl
The Court appointed a
"Judge") to manage all
The Trustee will work u
administration and liqui
and his reports are exp
of information to the cr
business today, the Tr
activities.


FOX IT

Black Tulip
Report of the investigation into the DigiNotar Certificate Authority breach

Classification PUBLIC
Customer Ministry of the Interior and Kingdom Relations
Project no./Ref. no. PR-110202
Date 13 August 2012
Version 1.0
Team Hans Hoogstraaten (Team leader)
Ronald Prins (CEO)
Daniël Niggebrugge
Danny Heppener
Frank Groenevegen
Janna Wettinck
Kevin Strooy
Pascal Arends
Paul Pols
Robbert Kouprie
Steffen Moorrees
Xander van Pelt

ABN-AMRO
no. 55.49.97.041
Chamber of Commerce
Haaglanden no. 27301624

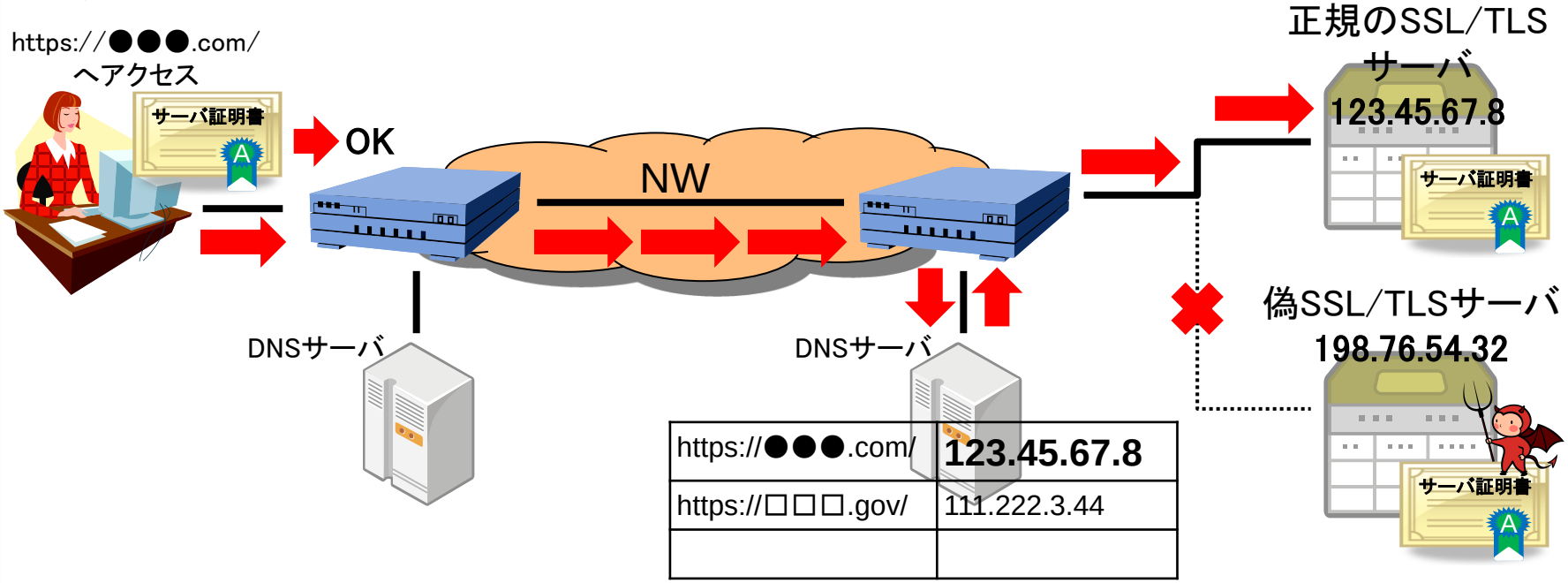
- で、実際のところ、どうだったの？
  - 中間報告では「CP/CPS違反もしくはCP/CPS自体に重過失があったことを強く疑わせる運用管理体制」を指摘・・・
  - オランダ政府承認の**最終報告書**が公表

詳しくは佐藤さんから

普段なら実害は少ない、はずなのだが・・・

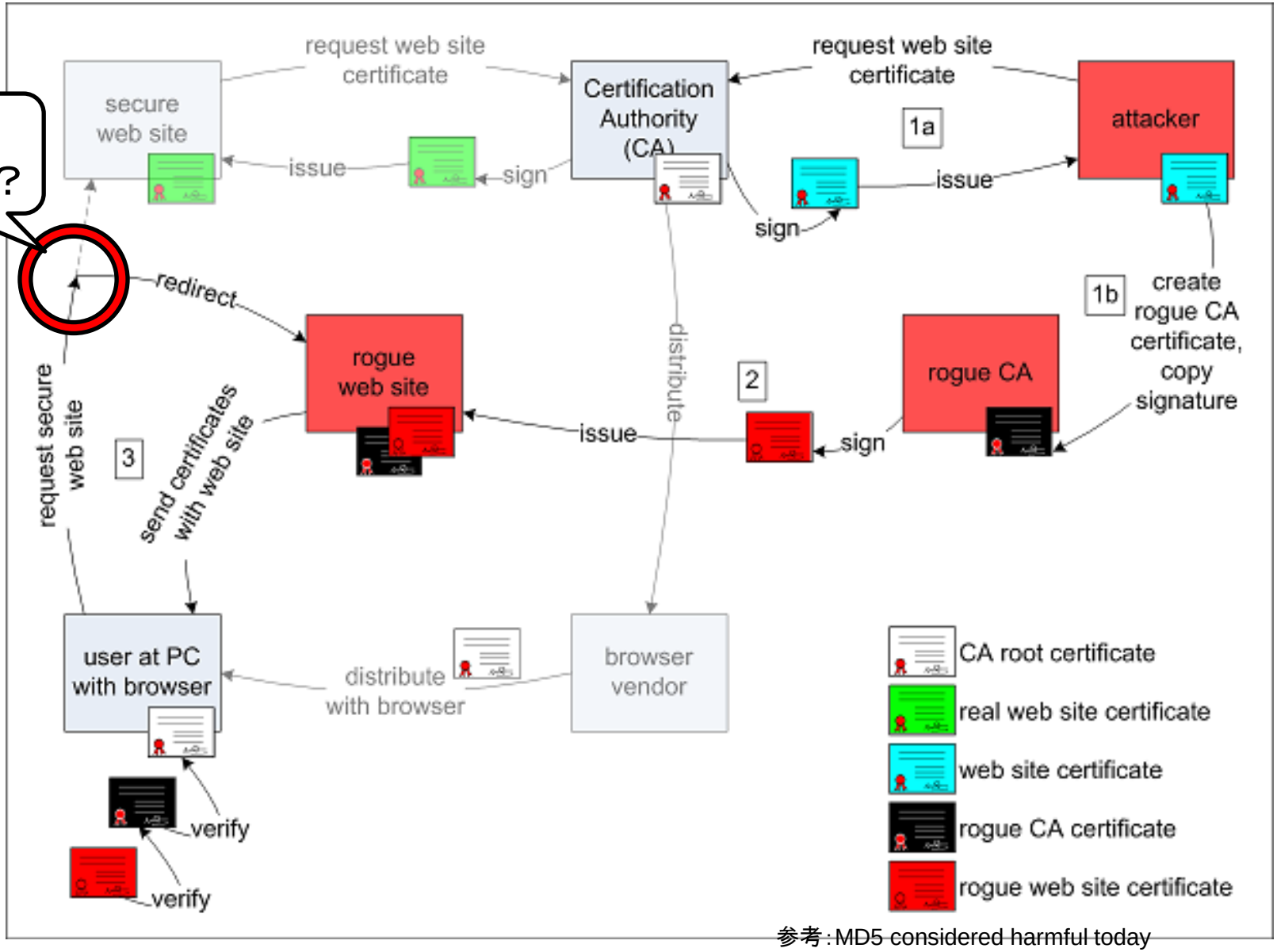
偽SSL/TLSサーバ証明書を不正発行した“だけ”なら
実害には繋がらない・・・はずだった

■ 実際の動作



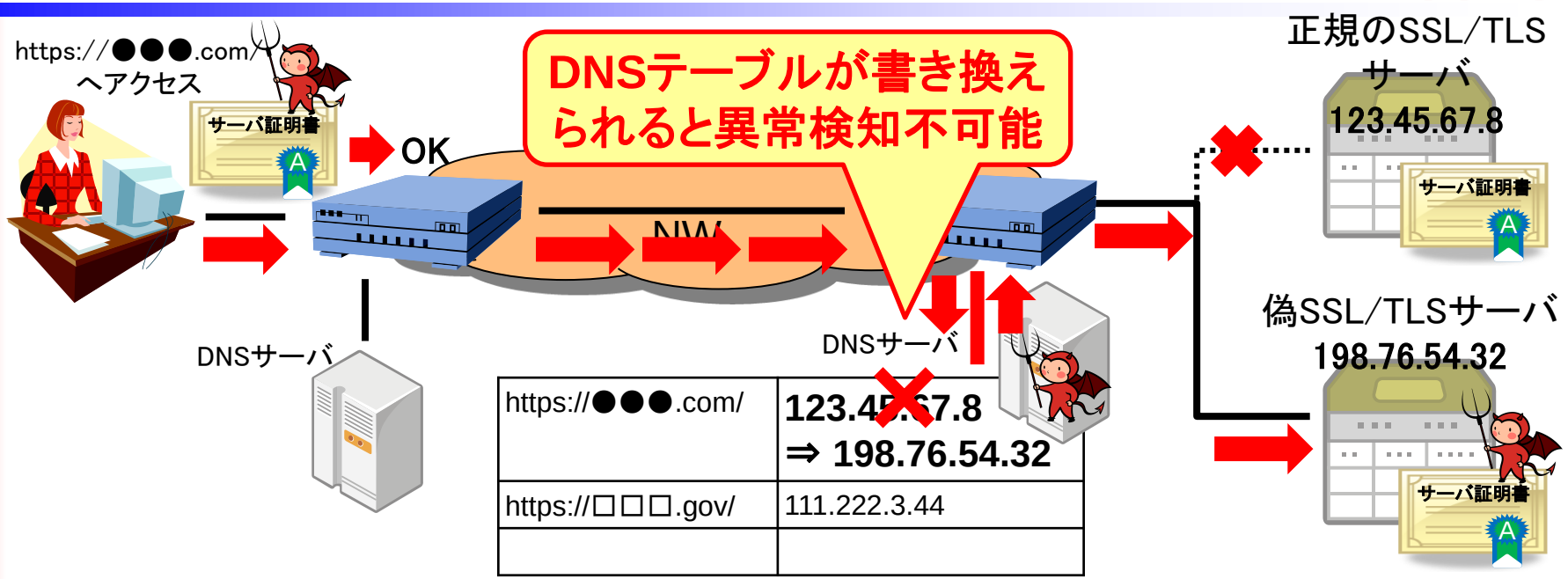
実害に結びつけるには、DNSサーバを改ざんするか、
Man-in-the-middle attackをするか

普段なら実害は少ない、はずなのだが・・・



参考：MD5 considered harmful today
http://www.win.tue.nl/hashclash/rogue-ca/

実害が発生した可能性が高い



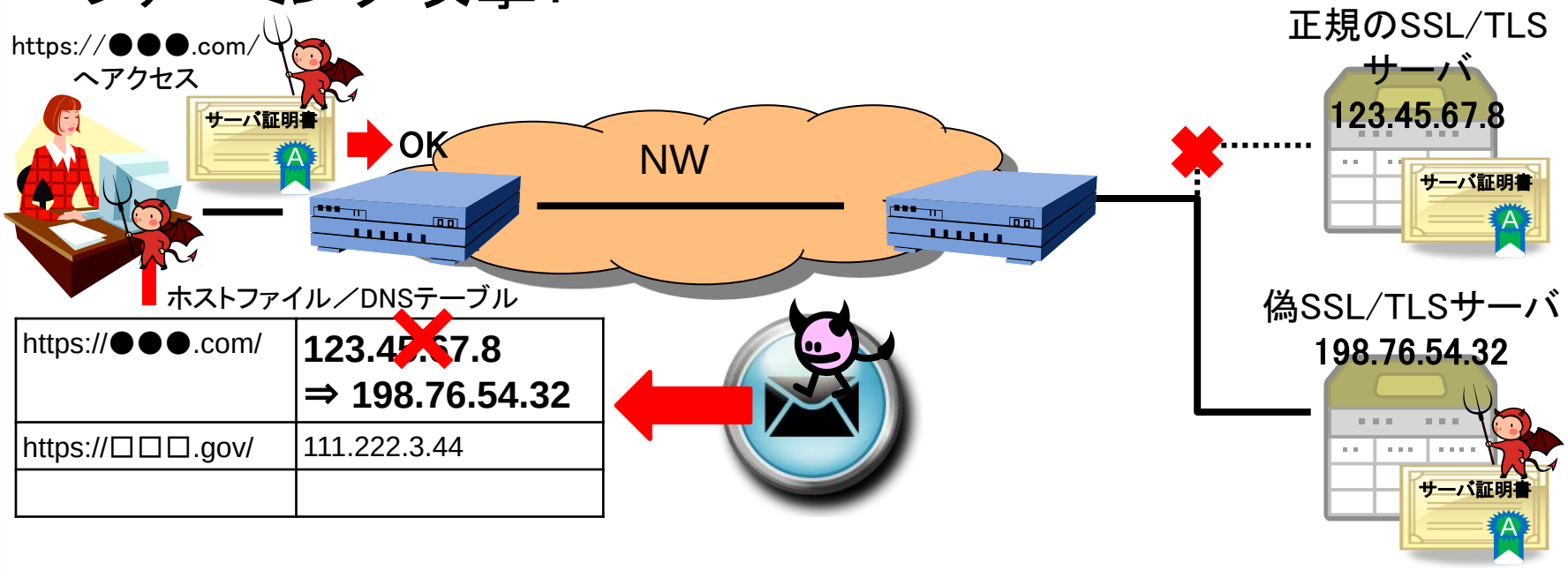
「政府機関（体制側）等による盗聴行為」が
イラン国内で実際に行われた可能性がある

- 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

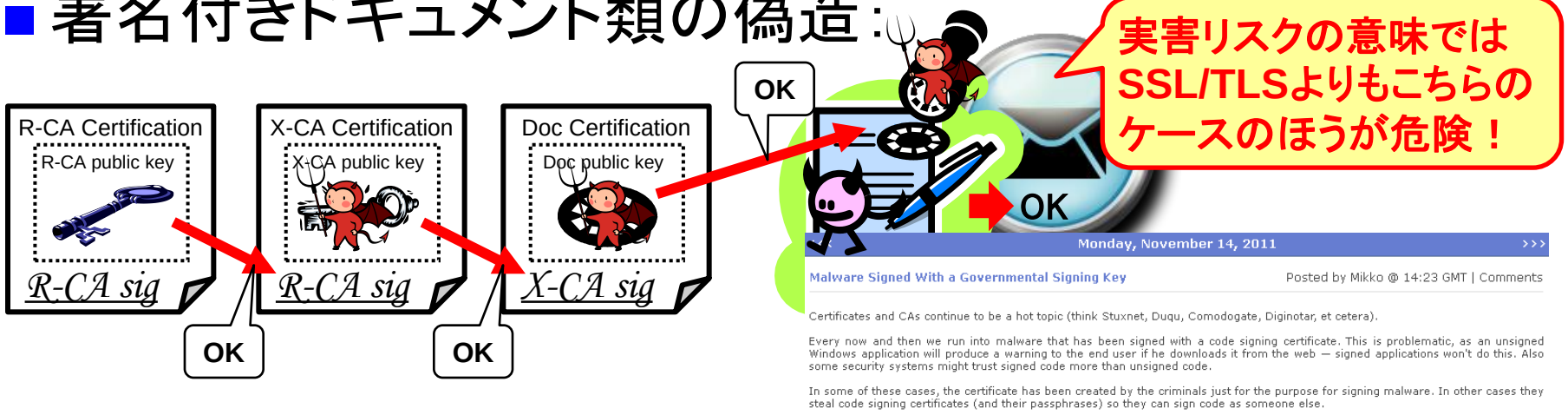
不正*.google.com証明書のOCSPリクエスト

標的型攻撃に使われるともっと危ない

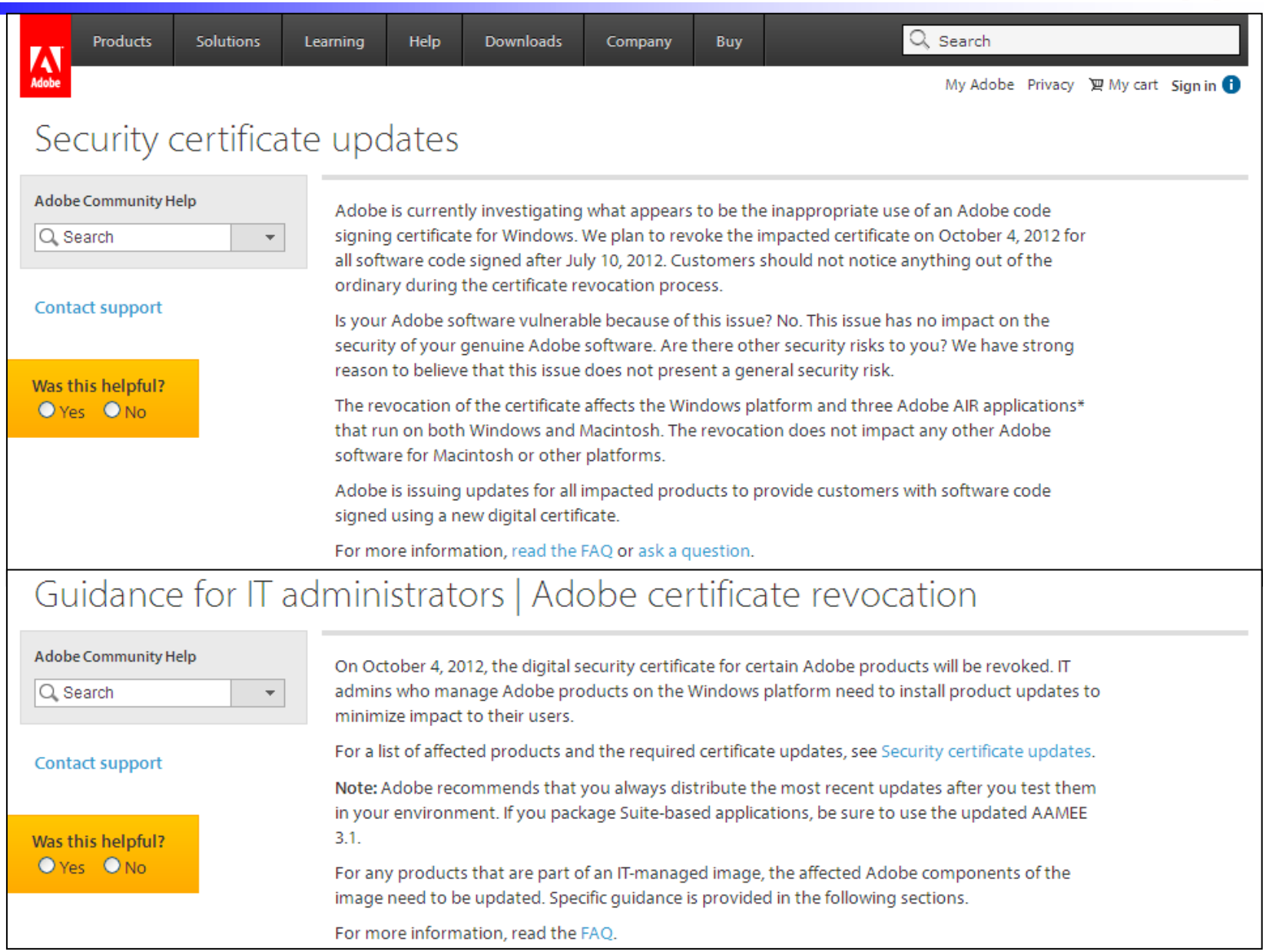
■ ファーミング攻撃：



■ 署名付きドキュメント類の偽造：

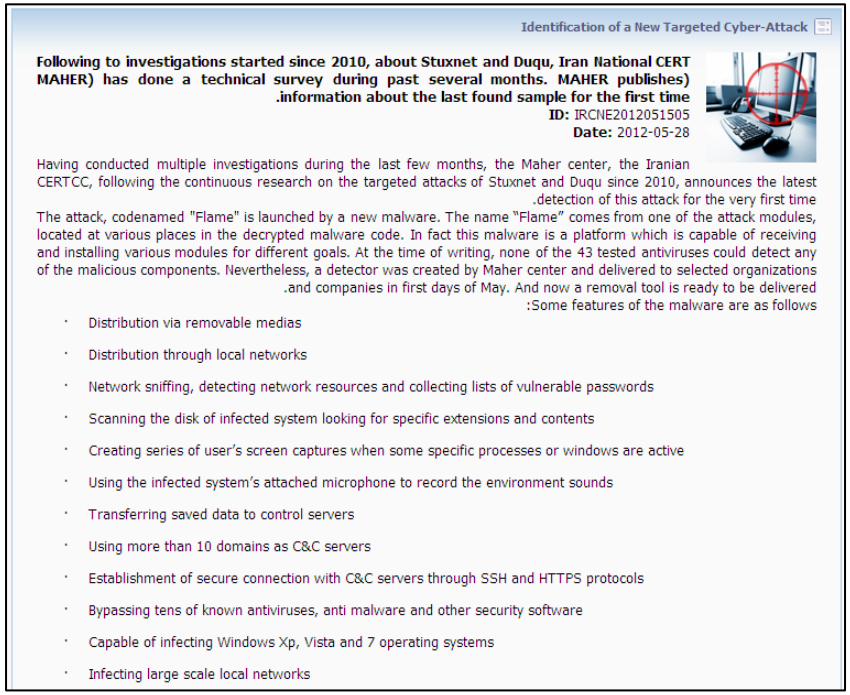


例えばAdobeの証明書失効



コード署名といえば・・・「Flame」！

- 盗聴目的に特化した完全潜伏型のマルウェア
  - 2012年5月28日　イランCERT/CCから発表
  - 約1000台感染していた
    - 少なくとも2010年2月には存在。5年前から存在していた可能性も
  - LAN/USB経由で感染・・・でも、自己増殖せず限定的な感染
    - 指示を受けての感染。自殺機能もあり



Identification of a New Targeted Cyber-Attack

Following to investigations started since 2010, about Stuxnet and Duqu, Iran National CERT MAHER) has done a technical survey during past several months. MAHER publishes) .information about the last found sample for the first time

ID: IRCNE2012051505

Date: 2012-05-28

Having conducted multiple investigations during the last few months, the Maher center, the Iranian CERTCC, following the continuous research on the targeted attacks of Stuxnet and Duqu since 2010, announces the latest .detection of this attack for the very first time

The attack, codenamed "Flame" is launched by a new malware. The name "Flame" comes from one of the attack modules, located at various places in the decrypted malware code. In fact this malware is a platform which is capable of receiving and installing various modules for different goals. At the time of writing, none of the 43 tested antiviruses could detect any of the malicious components. Nevertheless, a detector was created by Maher center and delivered to selected organizations .and companies in first days of May. And now a removal tool is ready to be delivered

:Some features of the malware are as follows

- Distribution via removable medias
- Distribution through local networks
- Network sniffing, detecting network resources and collecting lists of vulnerable passwords
- Scanning the disk of infected system looking for specific extensions and contents
- Creating series of user's screen captures when some specific processes or windows are active
- Using the infected system's attached microphone to record the environment sounds
- Transferring saved data to control servers
- Using more than 10 domains as C&C servers
- Establishment of secure connection with C&C servers through SSH and HTTPS protocols
- Bypassing tens of known antiviruses, anti malware and other security software
- Capable of infecting Windows Xp, Vista and 7 operating systems
- Infecting large scale local networks

出典: kaspersky Labs.
http://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers

そもそも「Flame」って何？

- Flameの特徴がすごい
  - マルウェアとしては非常に大きい・・・のに発見されなかった
    - 20MBもある
    - 複数のコンポーネントで構成
  - StuxnetやDuquとは兄弟的な関係
    - Stuxnetよりも20倍！も複雑 （by Kaspersky Lab.）
    - 米国とイスラエルの国家的プロジェクト（＝サイバー兵器）か？？？
  - **偽造公開鍵証明書を使ったコードサイニングがされていた**
    - **すでに知られている「MD5」に対するハッシュ衝突攻撃を利用**
    - **問題は、「MD5のハッシュ衝突探索」に対する未知の探索手法が実在し、相当ハードルが高いはずの「マイクロソフトのCA」下のPKIに入り込むことに実際に成功**
    - **偽造公開鍵証明書のトラストアンカーが「マイクロソフトのCA」**
    - **Windowsはマイクロソフトの承認を受けたコードと誤認**

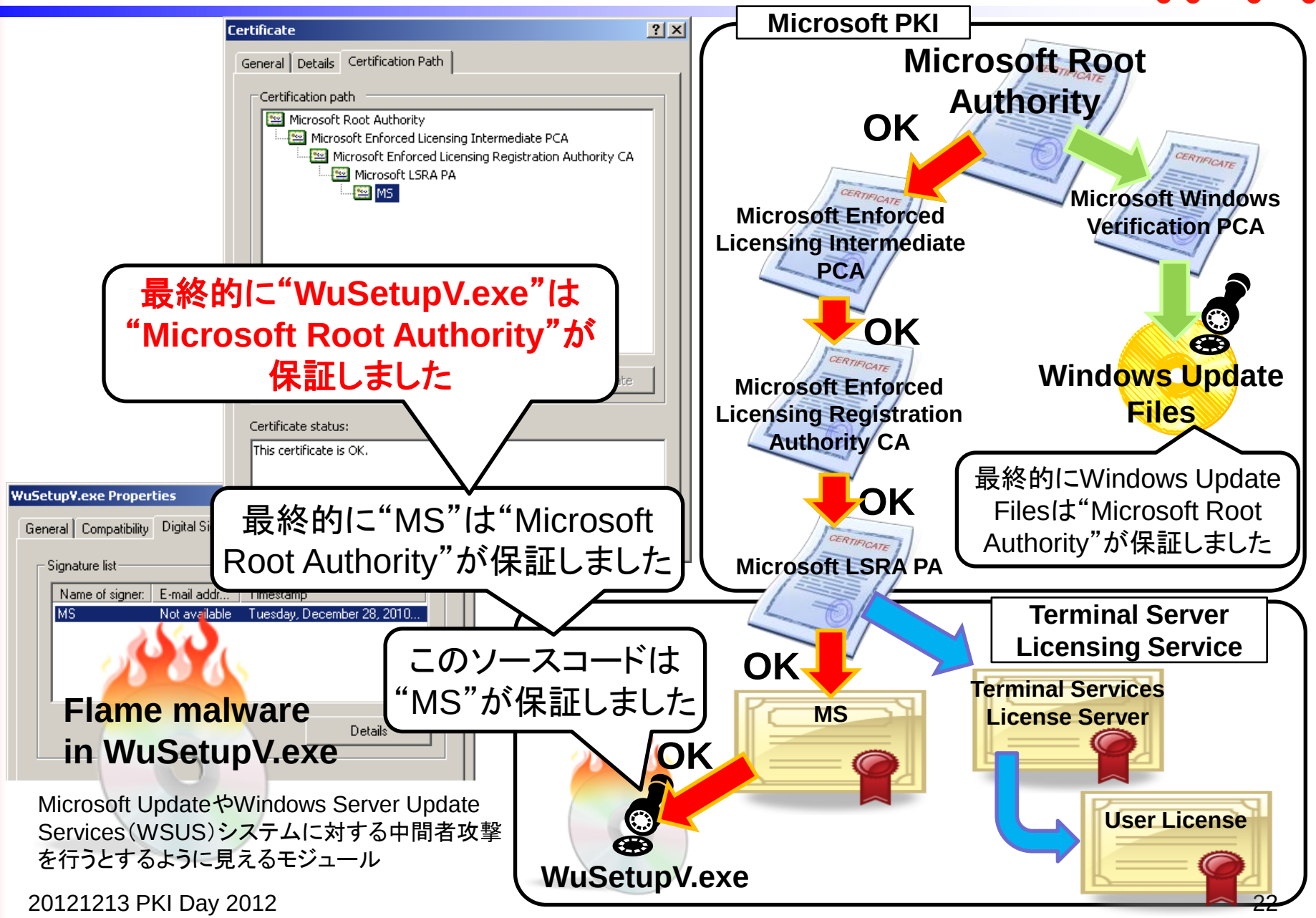
      ➡ 結果として Windows Update を利用して感染？

「Stuxnet – Olympic Games」とは異なる作戦だが、同時期のもの

「Flame」発覚後の経緯がもっとすごい・・・

- 「Flame」が見つかった。「Stuxnet」などと比べてみよう
  - 5/28 イランCERT/CCが発表
  - 5/29 “Iran Confirms Attack by Virus That Collects Information” by New York Times
  - 5/30 “Researchers Find Clues in Malware” by New York Times
- 実は（やっぱり？）アメリカからの攻撃だったんだよね
  – Olympic Games; Bush Initiativeの暴露
  - 6/1 “Obama Order Sped Up Wave of Cyberattacks Against Iran” by New York Times
  - 6/5 “FBI Probes Leaks on Iran Cyberattack” by Wall Street Journal
- **「Flame」にMSのコードサイニングが悪用されていた**
  - **6/3 “Microsoft certification authority signing certificats added to the Untrusted Certificate Store” by Microsoft**

暗号技術としてはどのように見えていたか



Microsoft UpdateやWindows Server Update Services（WSUS）システムに対する中間者攻撃を行うとするように見えるモジュール

なぜそんなことが起きたのか

- “Terminal Server Licensing Service”の本来目的は「企業管理用の下位PKI」を作るためのもの
  - 例えばリモートログイン用クライアント証明書などの発行

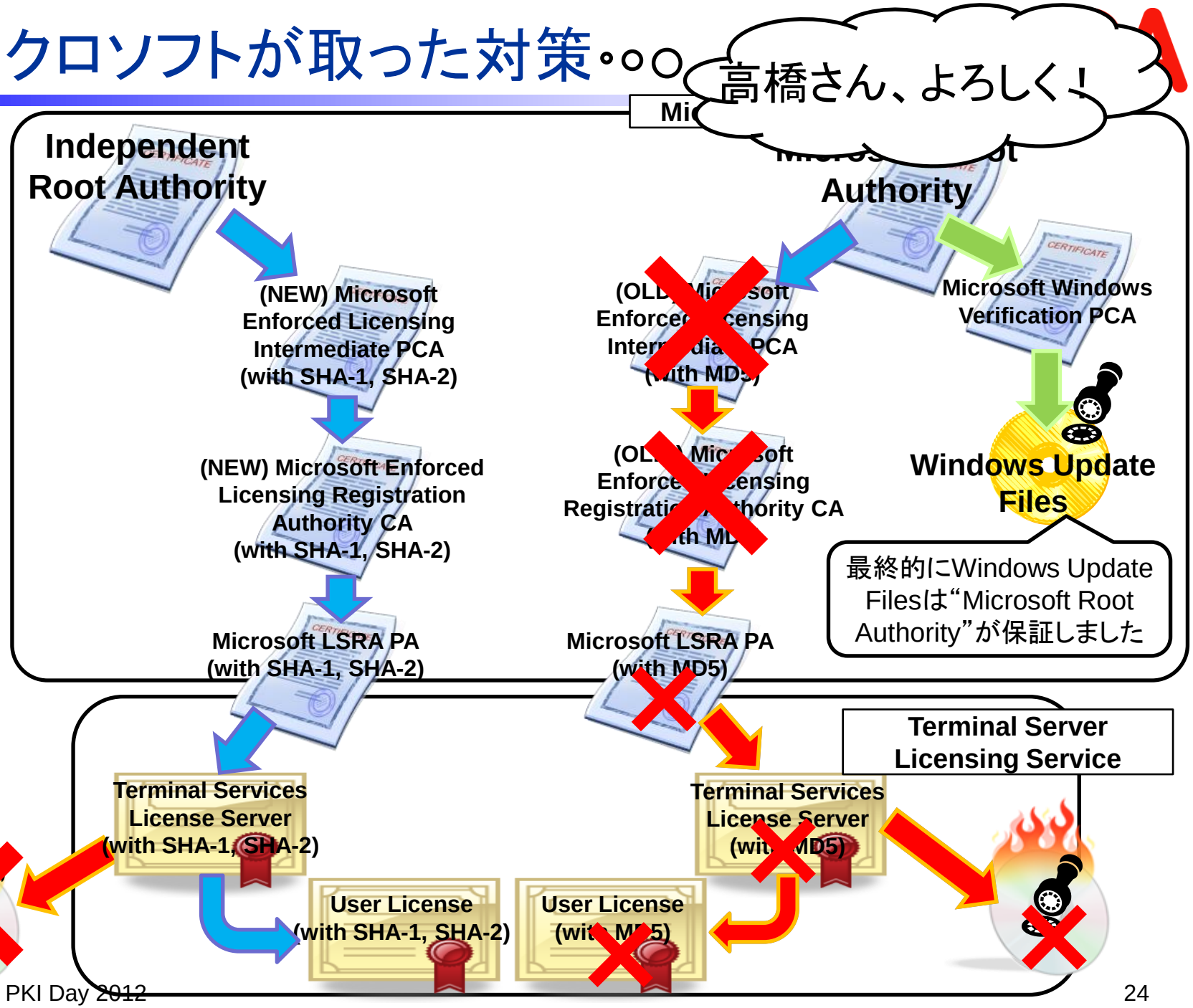
- 事件発生の3大要因
  - コードサイニングの権限がデフォルト付与
    - Microsoft LSRA PAから公開鍵証明書を発行してもらえさえすれば、（ハッシュの衝突を利用しなくても）Windows XP以前に対する不正なコードサイニングが可能
  - “MD5”を使い続けた
    - “Microsoft Hydra X.509 extension”による防御が回避される原因
  - マイクロソフトを意味する“Microsoft Root Authority”がトラストアンカーになっていた
    - どんなソースコードでも“Windows Update filesと同等の保証”を最終的にマイクロソフトが与えてしまう仕組み

コードサイニングの必要性があったのか

マイクロソフト自身、「使うのを止めろ」と警告していたのだが・・・

PKI運用上の完全なミス

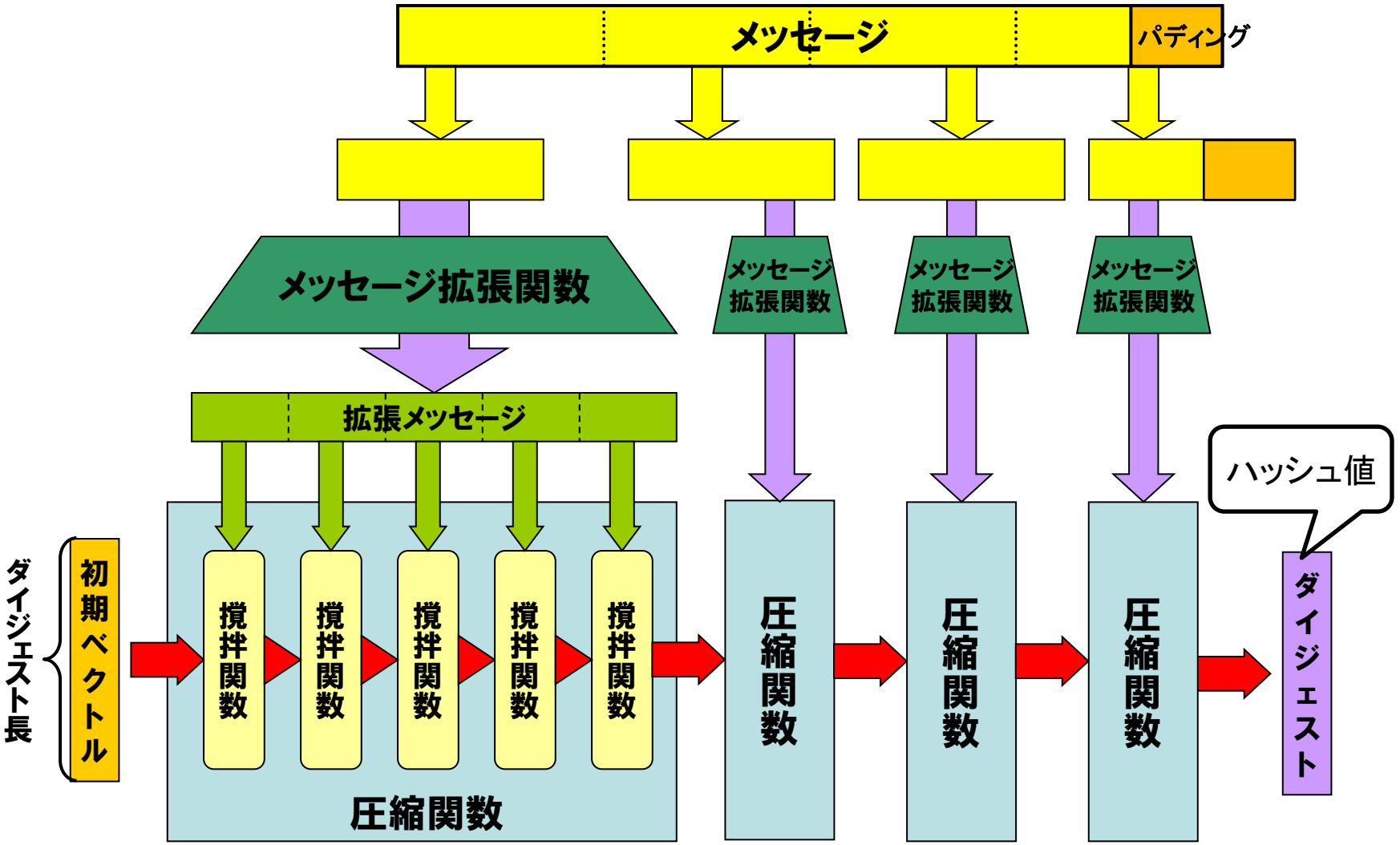
マイクロソフトが取った対策・・・



技術の具体的な話をする前に・・・
Back to the Chaos Communication Congress 2008 (CCC2008)

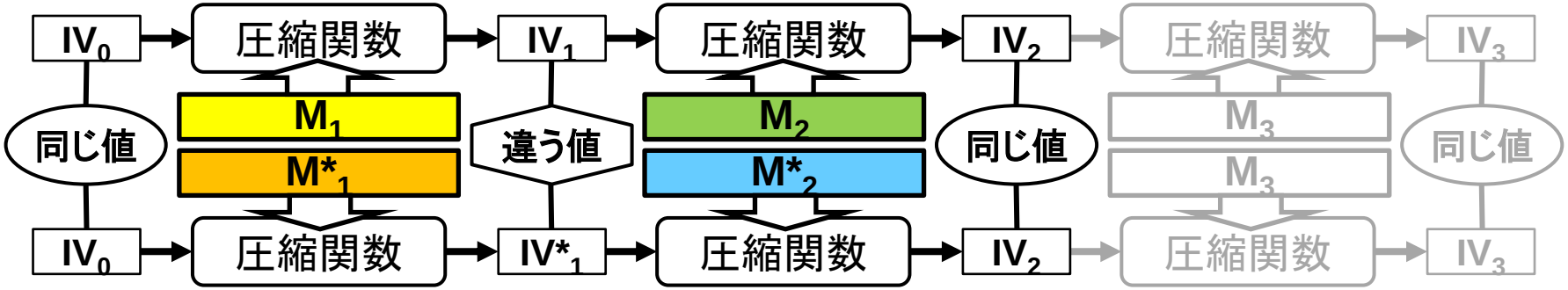
Merkle-Damgård構造　～一般的な構造～

MD4, MD5, SHA-1, SHA-2 は全てこの構造を採用



MD5（Merkle-Damgård構造）の衝突

- 2004年Wangらにより発見
  - MD5(M_1|M_2) = MD5(M^*_1|M^*_2) を見つける攻撃手法を提示

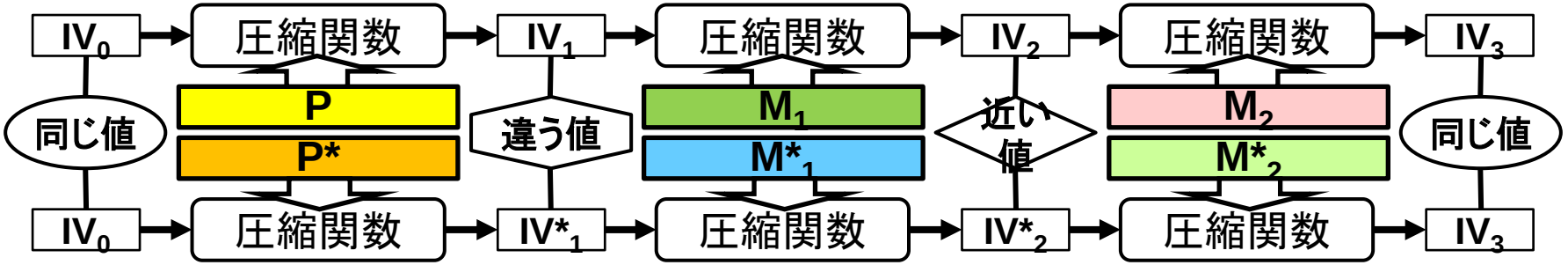


  - 2005年LenstraらによりX.509偽造証明書の作成成功
    - フォーマットが正しいだけ

	公開鍵証明書1	公開鍵証明書2
X.509 version number	0x02 (X.509 version 3)	
Serial number	0x03507449	
Signature algorithm identifier	md5withRSAEncryption	
Issuer distinguished name	CN = “Hash Collision CA”, L = “Eindhoven”, CN = “NL”	
Not valid before	Feb. 1, 2005, 00h00m01s	
Not valid after	Feb. 1, 2007, 00h00m01s	
Subject distinguished name	CN = “Hash Collision”, O = “we used a collision for MD5”, L = “Eindhoven”, C = “NL”	
Public key algorithm	rsaEncryption	
Subject public key info	**帳尻が合うような公開鍵情報#1**	**帳尻が合うような公開鍵情報#2**
Version 3 extensions	Basic constraints	
Signature info	**同一の署名**	

かな～り精錬された攻撃に変化

- 選択プレフィックス衝突：2007年Stevensらにより発見
  - 任意の(P,P*)に対しMD5(P|M_1|M_2)=MD5(P*|M^*_1|M^*_2)となる([M_1,M_2],[M^*_1,M^*_2])を見つける攻撃手法を提示
    - 制御不可のビットが存在＝衝突攻撃より制約条件が多い

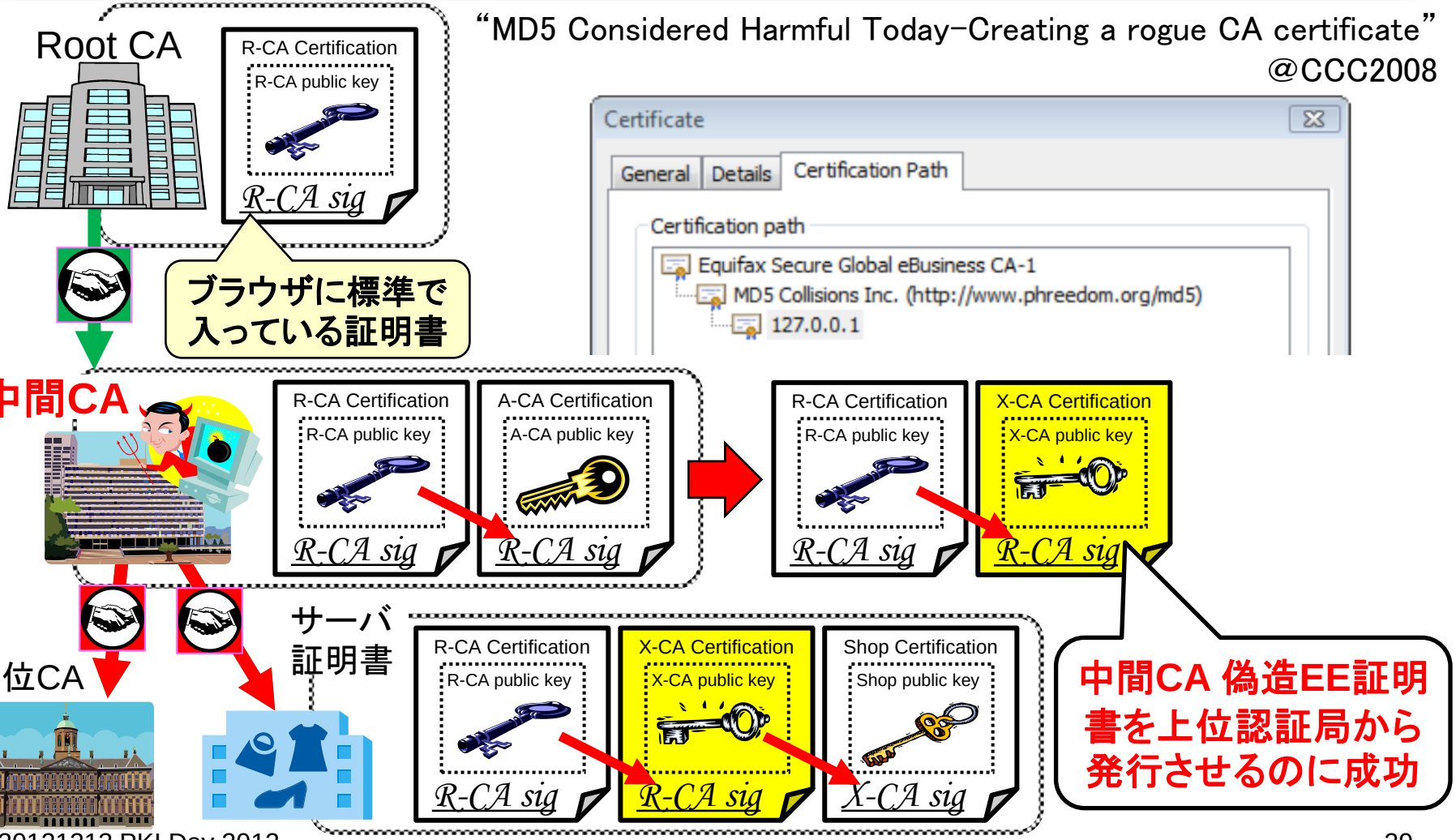


  - X.509偽造証明書の例を改良

	公開鍵証明書1	公開鍵証明書2
X.509 version number	0x02 (X.509 version 3)	
Serial number	0x010C0001	0x020C0001
Signature algorithm identifier	md5withRSAEncryption	
Issuer distinguished name	CN = “Hash Collision CA”, L = “Eindhoven”, CN = “NL”	
Not valid before	Jan. 1, 2006, 00h00m01s	
Not valid after	Dec. 31, 2007, 23h59m59s	
Subject distinguished name	CN = “Arjen K. Lenstra”, O = “Collisionaris”, L = “Eindhoven”, C = “NL”	CN = “Marc Stevens”, O = “Collision Factory”, L = “Eindhoven”, C = “NL”
Public key algorithm	rsaEncryption	
Subject public key info	帳尻が合うような公開鍵情報#1	帳尻が合うような公開鍵情報#2
Version 3 extensions	Basic constraints	
Signature info	同一の署名	

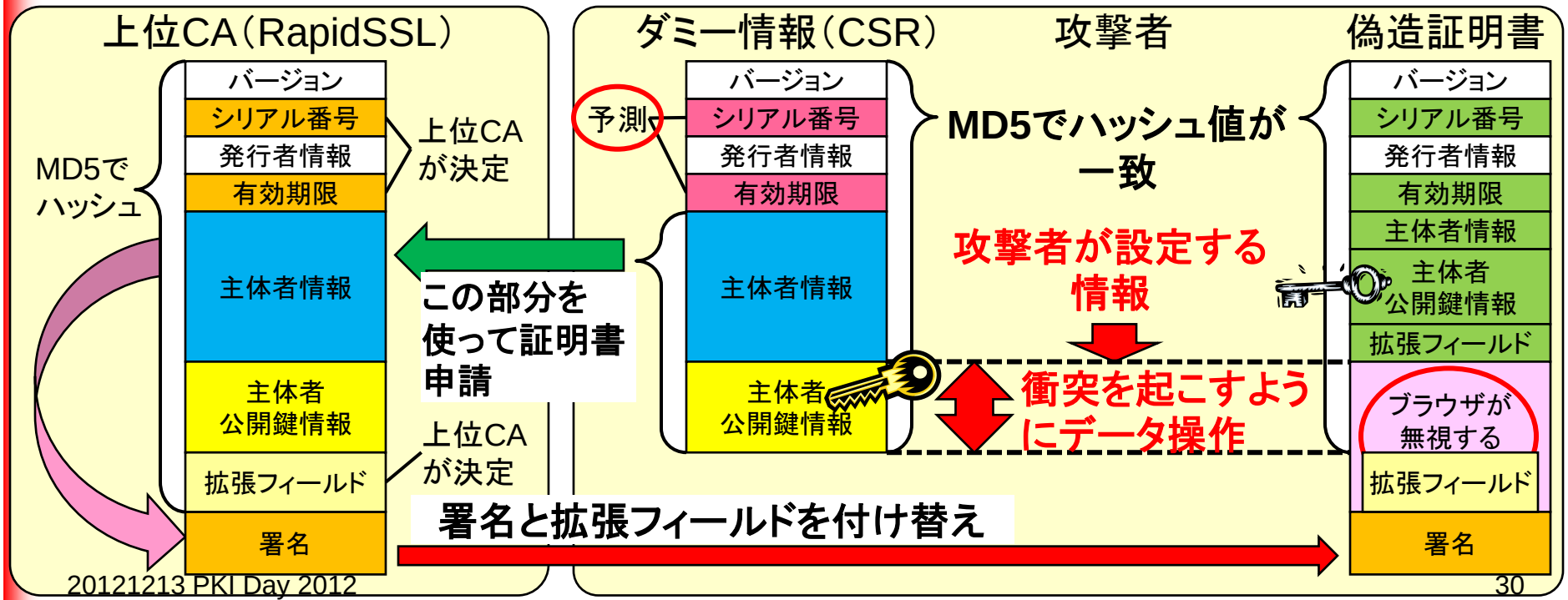
ついに本当の公開鍵証明書の偽造に成功

誘導されたら見破ることができないEE証明書が発行可能になった
⇒ MD5を利用する公開鍵証明書発行を中止する契機に



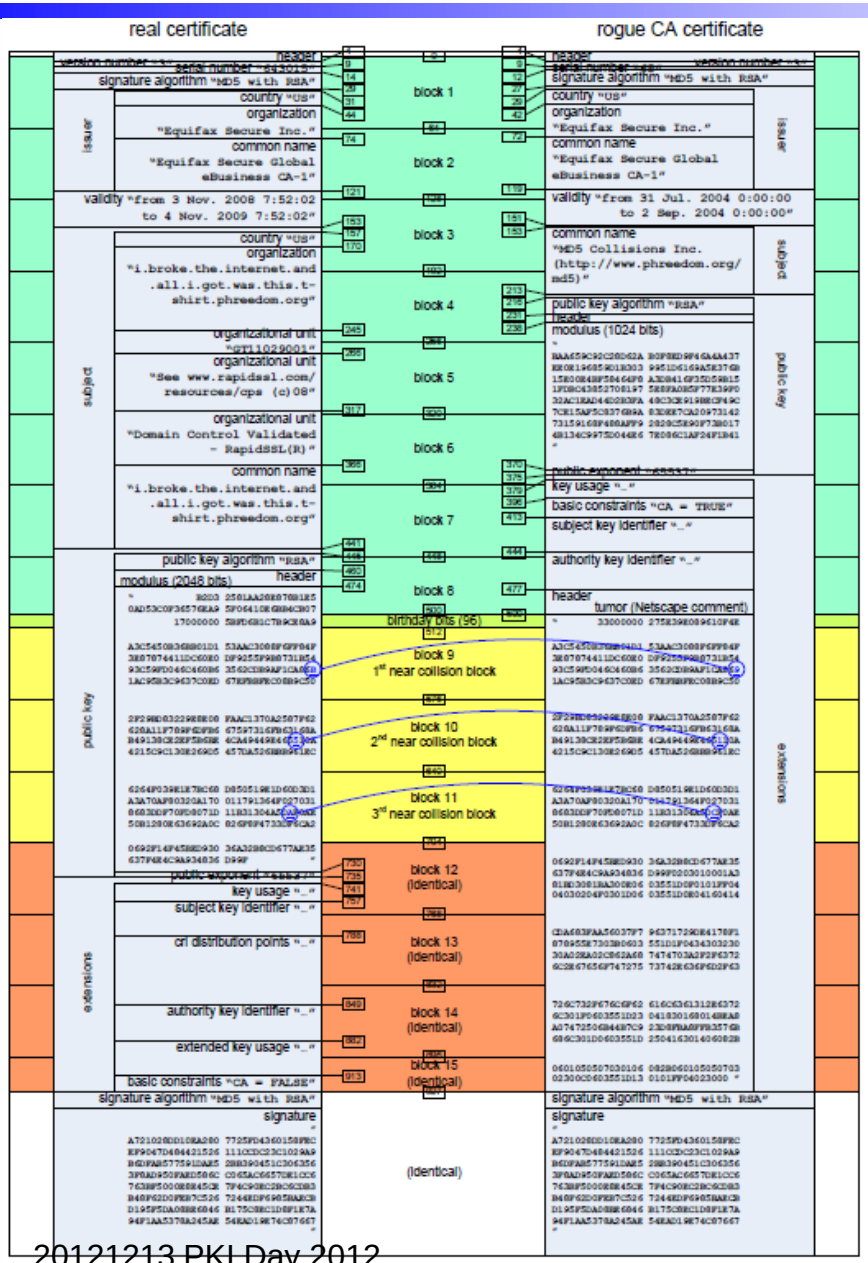
具体的にやったことは何か

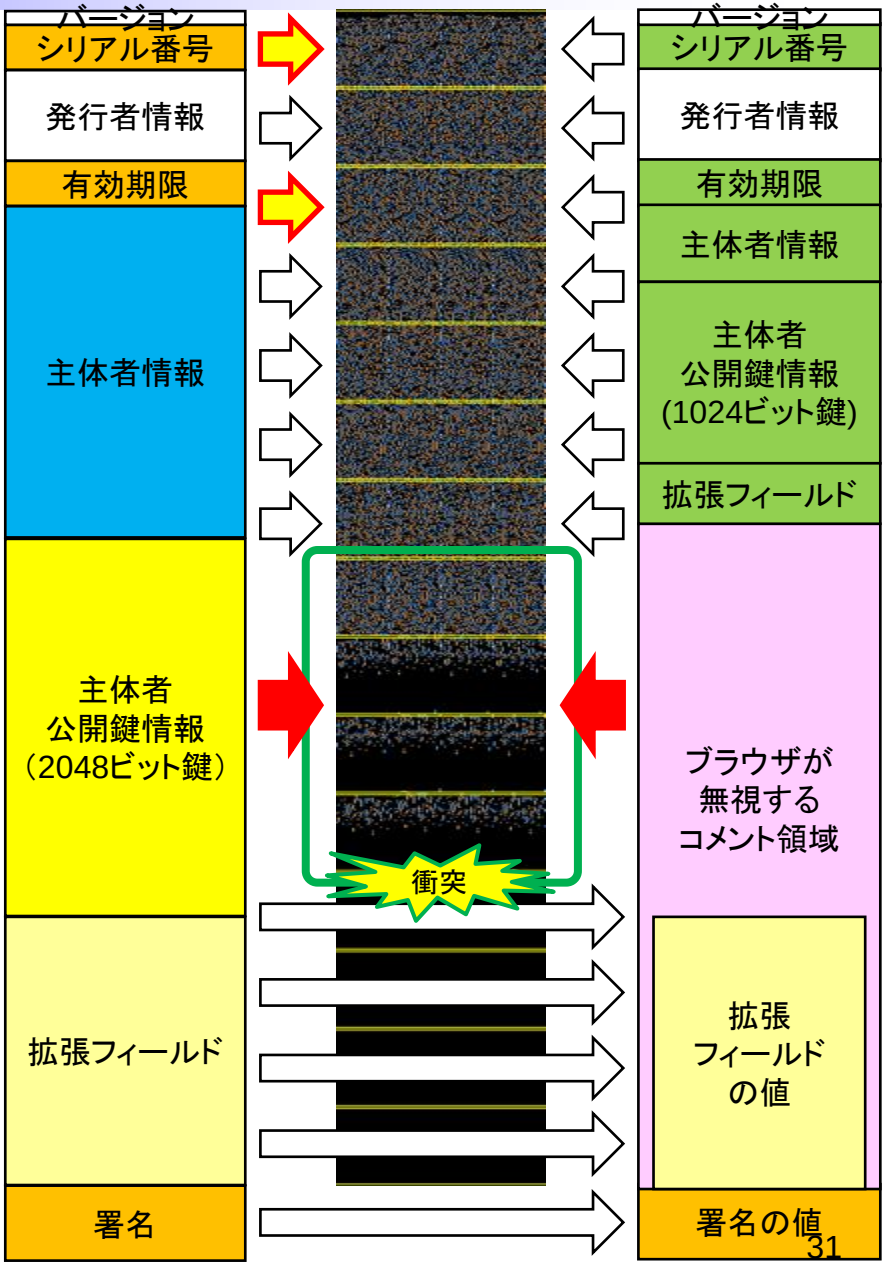
- 選択プレフィックス衝突により中間CA EE証明書偽造
  - PにRoot CAをだますためのダミー情報、P*に公開鍵を含む偽造情報を入れる
  - ルートCAが決める「シリアルナンバー」「有効期限」が予測可
  - ブラウザが無視するコメント領域を利用
  - PS3 200台で約1日



具体的にやったことは何か

出典：「MD5 considered harmful today」

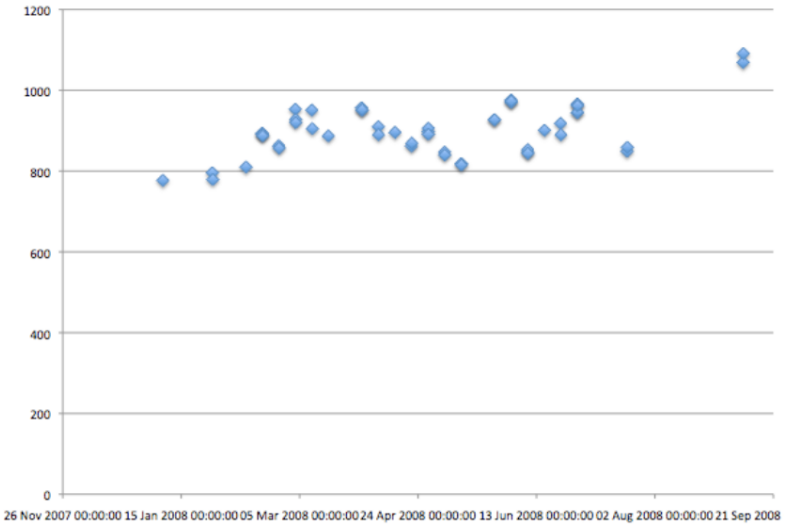




なぜうまくいったのか

- MD5を使っていた
  - 衝突を**何度も**起こすことができた
- RapidSSLではserial numberが**単調増加**
  - Serial numberの予測が可能

```
Nov  3 07:42:02 2008 GMT    643004
Nov  3 07:43:02 2008 GMT    643005
Nov  3 07:44:08 2008 GMT    643006
Nov  3 07:45:02 2008 GMT    643007
Nov  3 07:46:02 2008 GMT    643008
Nov  3 07:47:03 2008 GMT    643009
Nov  3 07:48:02 2008 GMT    643010
Nov  3 07:49:02 2008 GMT    643011
Nov  3 07:50:02 2008 GMT    643012
Nov  3 07:51:12 2008 GMT    643013
Nov  3 07:51:29 2008 GMT    643014
Nov  3 07:52:02 2008 GMT      ?
```

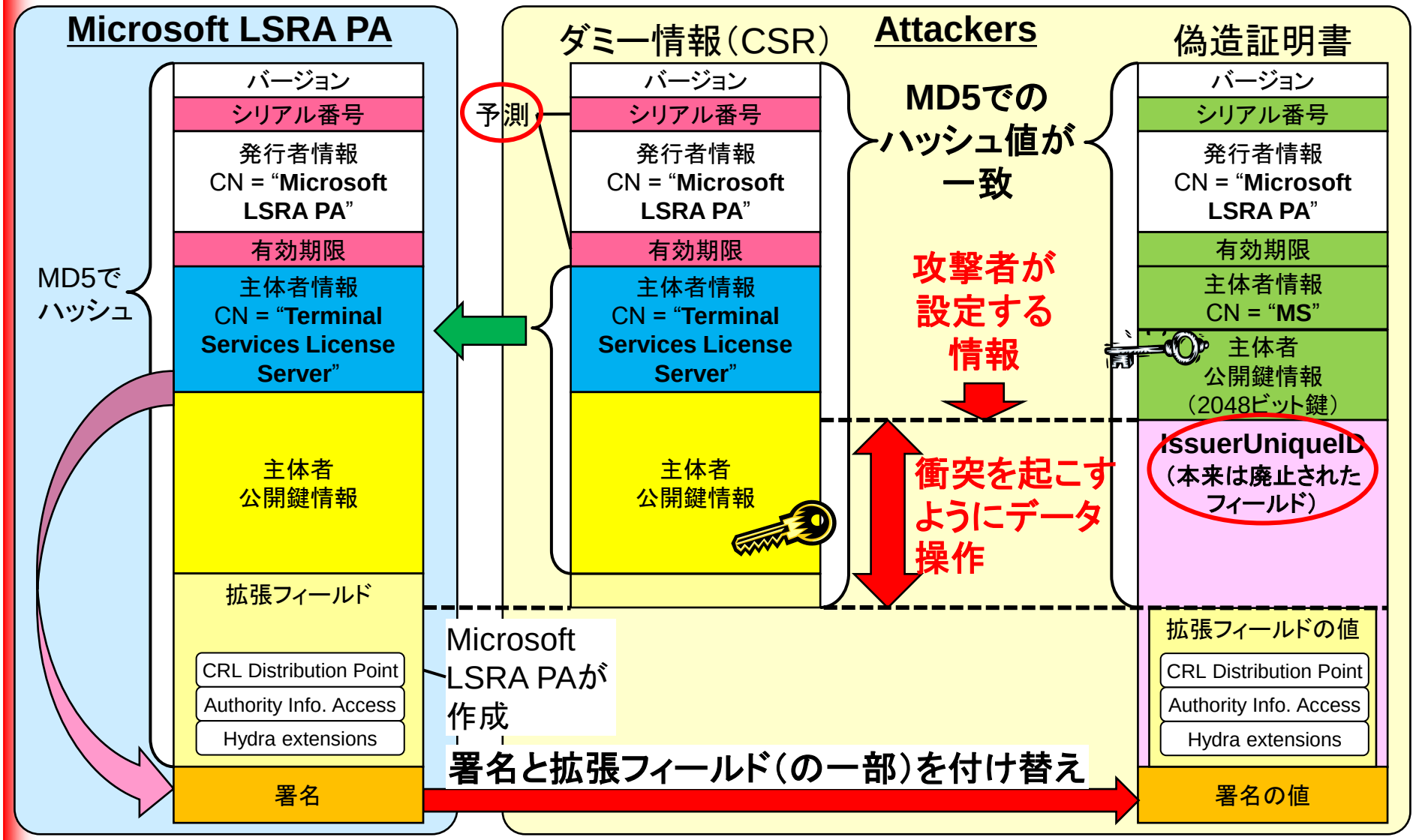


- Netscape Comment Extensionの悪用
  - **ブラウザが無視**するフィールドをハッシュの衝突に利用

では、Flameでは・・・？

具体的に起きたこと

- 考え方は「中間CA 偽造EE証明書」の作成と同様



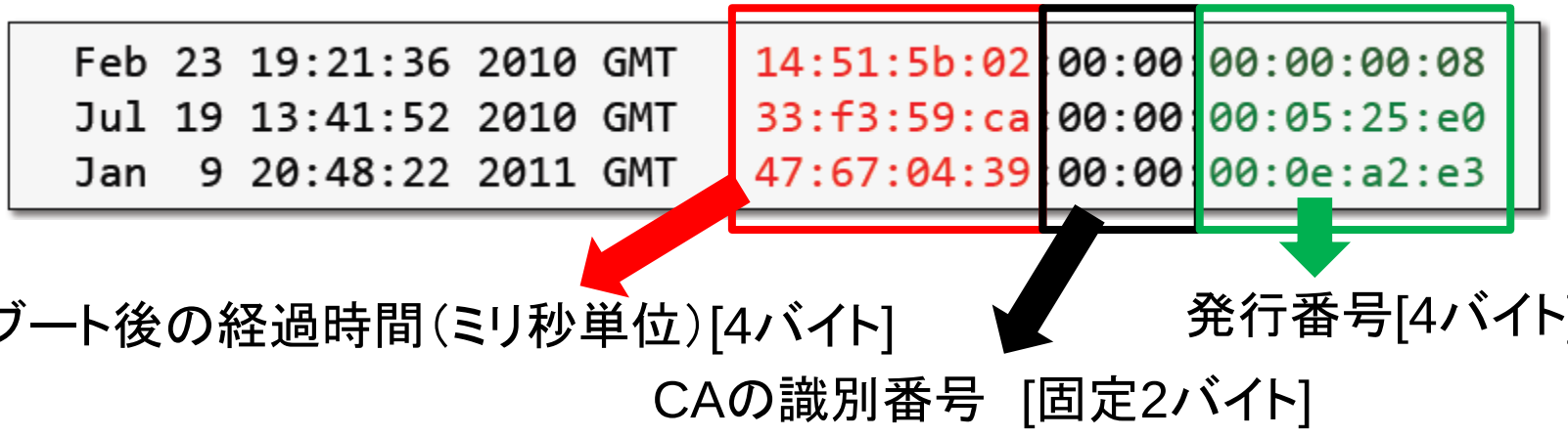
具体的に起きたこと

- MD5の悪用
  - 衝突を**何度も**起こすことができた
- issuerUniqueIDフィールドの悪用
  - **Crypto APIが無視**するフィールドをハッシュの衝突に利用
  - ハッシュの衝突を利用することで、**拡張フィールドが存在しない**形にすることができた
- 拡張フィールドでの「Hydra extension」の**チェックが機能しなかった**
  - Windows XP以前のOSについてはもともと未サポート
  - Windows Vista以降のOSでは拡張フィールドが使われる際には「Hydra extensionのチェック」が必須だが、拡張フィールド自体を使うかどうかは別問題

でも、RapidSSLのケースと同じだったのか・・・？

もっとも“普通なら”成功可能性はかなり低い

- シリアルナンバーの予測がかなり難しい（らしい）
  - Microsoft LSRA PAが作るシリアルナンバーはミリ秒単位



- 通信タイミングを合わせるのが難しい
  - ミリ秒単位で一致しないといけないので、システム負荷や通信タイミングのずれが無視できない
- 大量のハッシュの衝突データを作らないといけない
  - **現在知られている衝突探索ツールでは追いつかない**

➡ **未知の探索手法を知っている？　膨大な計算能力を持っている？**

ただ“サイバー兵器”ともなると話は別物か

- 衝突を本当に見つけられたとして・・・
  - Trail of Bits, Incによれば、RapidSSLでの証明書不正発行のときより10～100倍は難しい

- CWIによれば、少なくとも現在知られているハッシュ衝突探索手法を使ったのではない
  - Stevensらの選択プレフィックス衝突攻撃と同時期（以前）に異なる衝突探索手法が発見されたことを示唆
  - 2010年には（現在でも知られていない）探索プログラムまで実際に完成していた可能性が高い
  - Microsoft LSRA PAへの不正アクセスの可能性もありうるが・・・　その場合、LSRA PAが発行する証明書フォーマットと違うことの説明がつかない

まとめにかえて

島岡さんに
乞うご期待！

- 公開鍵証明書は基本的に自動検証されるもの
  - 監査水準が異なるルート証明書が大量に入っている
  - 信頼の起点を乗っ取られると利用者は対応のしようがない

⇨ 集中管理型にしたほうが安全性が高まるのか否か

- 公開鍵証明書“だけ”の問題ではない
  - 実害が出るときは何らかの運用ミスや他の攻撃などとセット

⇨ 公開鍵証明書の発行だけに閉じて解決できるのか

- 金銭目的よりも深刻な目的で使われそう
  - 攻撃に対する費用対効果はあまりよくなさそう
  - 金銭目的ならば公開鍵証明書がなくても攻撃可能

⇨ 本気で狙われた場合、どこまで対抗できるのか