トラストアンカーを巡る課題と最新動向
～インターネットの信頼の起点として～

セコム IS研究所
島岡 政基

相次ぐ認証局関連のインシデント

- DNS Spoofingと中間者攻撃のコンボ
  - DigiNotar, Comodo
- 証明書偽造攻撃
  - (脆弱な暗号アルゴリズムに対する攻撃)
  - MD5証明書へのchosen prefix attack (Flame)
- 認証局等へのハッキング
  - DigiNotar, Comodo
  - Adobeのコード署名システム
- 認証局の運用ミス
  - TURKTRUST 中間CA証明書の誤発行
  - 512bitの中間CA証明書(マレーシアDigiCert)
- (TLSの脆弱性に対する攻撃手法の高度化)

PKI Day 2012を振り返って

【午後の部】「PKIへの攻撃とその対応」

- 認証局へのハッキング
  - Comodo, DigiNotar
- 暗号技術に対する攻撃
  - Flame, (BEAST, CRIME, Lucky13)
- 実装の脆弱性や運用の問題
  - 公開鍵の安易な使いまわし問題
  - (トルコTURKTRUST，マレーシアDigiCert)

PKI Day 2012公開資料
http://www.jnsa.org/seminar/pki-day/2012/index.html

被害が本格化する要素

- 潤沢な予算
  - 国家規模の不正など
- 攻撃方法の高度化・組織化・巧妙化
  - 暗号技術，圧縮技術，DNSハイジャック，標的型攻撃など
- 潤沢な計算資源
  - クラウドコンピューティングの普及

- 特定の暗号技術，セキュリティプロトコルに大きく依存
  - MD5, SHA1, RC4, RSA, TLS
- 認証局に大きく依存した信頼基盤
  - 代替技術，回避手段の確立困難

どんなリスクが増えるのか？

- Webサイトおよび利用者
  - HTTPS通信に対する中間者攻撃による盗聴・改ざんなど
  - **不正なサーバ証明書を検知する手段**を講じる必要がある
- 認証局
  - 認証局に対する攻撃(主に侵入)の高度化
  - 不正侵入からの不正発行，不正失効
  - 不正侵入・鍵の危殆化の**疑い**による
    - 顧客対応コスト増，損害賠償
    - 臨時監査，システム改修
    - 風評被害，他事業・関連組織への影響　などなど
  - 不正侵入に対する検知・防止策
  - 不正発行・失効に対する検知・防止策

社会基盤化したPKIは捨てられない

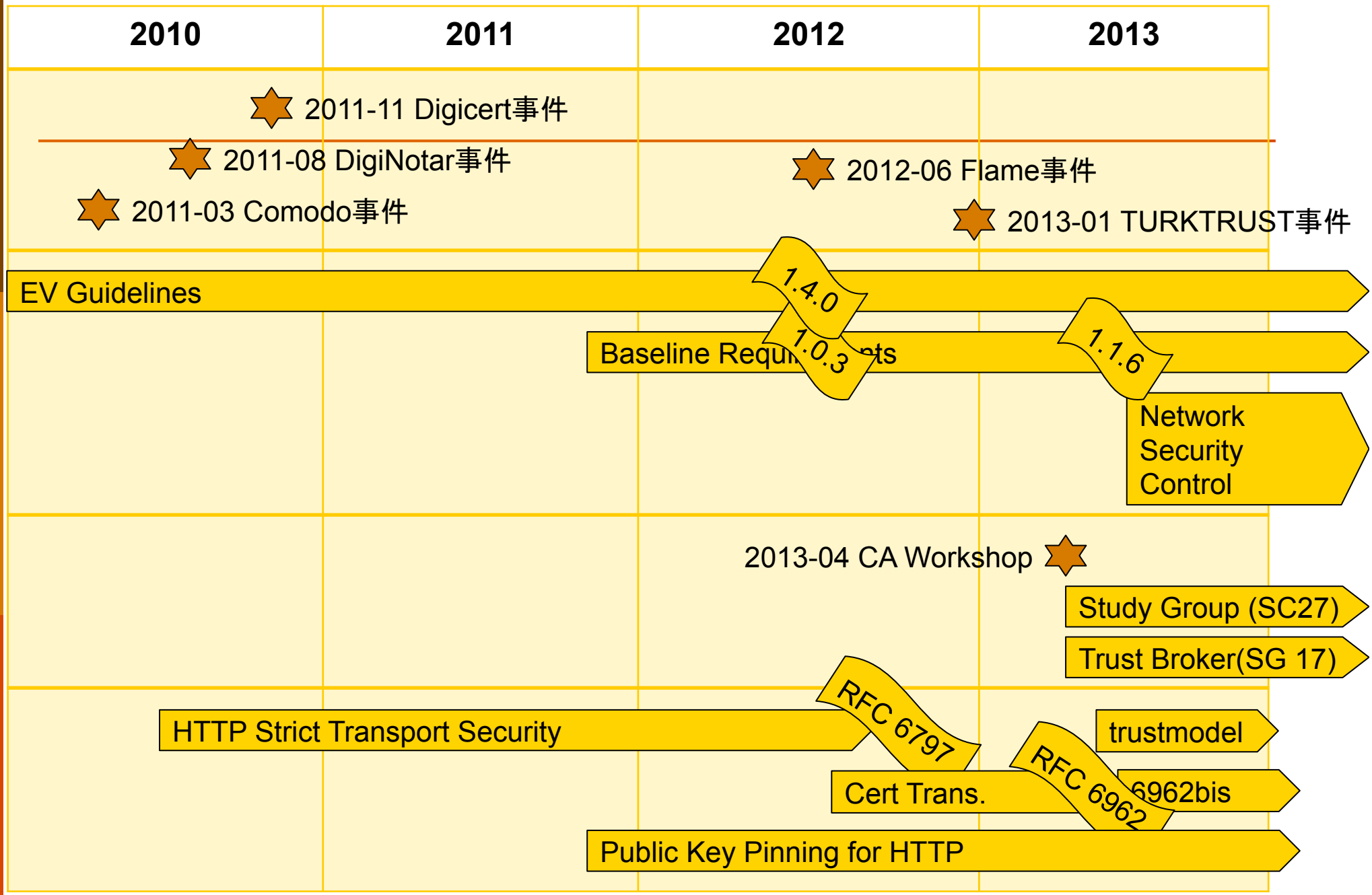
- 世界中のブラウザの実装を入れ替える必要がある
  - スマホ，組込み機器，レガシー機器，などなど
- PKI Alternativesへの道は長い
  - 新しい技術の開発・普及
  - ビジネスプレイヤーの充実

PKIはこの危機にどう立ち向かうのか?

- 業界団体による運用・技術の見直し
  - Work around(短・中期)[運用・技術]
  - Alternatives(長期)[技術]
- 各プレイヤーの取り得る対策(短・中期)
  - ブラウザ利用者
  - サーバ(証明書)管理者
  - 認証局

各組織の動向概観

- CA/Browser Forum
  - 認証局運用規準の改訂
- IETF
  - 対策技術の標準化
- ISO/IEC JT 1/SC 27
  - 認証局運用監査のStudy Group設置
- ITU-T SG17 (X.509)
  - Trusted Brokerを含む新しい?トラストモデルの提案
- その他
  - NIST CA Workshop, CA Security Council


2010
2011
2012
2013
2011-11 Digicert事件
2011-08 DigiNotar事件
2011-03 Comodo事件
2012-06 Flame事件
2013-01 TURKTRUST事件
EV Guidelines
1.4.0
Baseline Requirements
1.0.3
1.1.6
Network Security Control
2013-04 CA Workshop
Study Group (SC27)
Trust Broker(SG 17)
HTTP Strict Transport Security
RFC 6797
trustmodel
Cert Trans.
RFC 6962
6962bis
Public Key Pinning for HTTP

IETFの対応

- App Area – websec WG (Web Security)
  - HSTS(RFC 6797)
  - draft-ietf-websec-key-pinning
- Ops Area – wpkops WG (WebPKI Ops)
  - draft-ietf-wpkops-trustmodel
- Sec Area – trans WG (Public Notary Transparency)
  - 6962bis(Certificate Transparency)

RFC 6797 - HTTP Strict Transport Security
http://tools.ietf.org/html/rfc6797
draft-ietf-websec-key-pinning-11
http://tools.ietf.org/html/draft-ietf-websec-key-pinning
draft-ietf-wpkops-trustmodel
http://tools.ietf.org/html/draft-ietf-wpkops-trustmodel
RFC 6962 – Certificate Transparency
http://tools.ietf.org/html/rfc6962
draft-ietf-trans-rfc6962-bis
http://tools.ietf.org/html/draft-ietf-trans-rfc6962-bis

CA/Browser Forumの対応 (1)

- CABFの策定した規程類
  - EV Guideline v1.4.5 (2014年1月策定・施行)
    - いわゆるEV証明書の発行ガイドライン
  - Baseline Requirements v1.1.6 (2013年7月策定・施行)
    - WebTrust for CAの後継で，いわゆるDV/OV証明書の発行要件
  - Network Security Control v1.0 (2013年1月策定・施行)
    - 認証事業者が遵守する(SHALL)ネットワークセキュリティ要件

Guidelines For The Issuance And Management Of Extended Validation Certificates, v.1.4.5
https://cabforum.org/extended-validation/
Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.1.6
https://cabforum.org/baseline-requirements-documents/
Network and Certificate System Security Requirements, v. 1.0
https://cabforum.org/network-security/

CA/Browser Forumの対応 (2)

- EV Guideline
  - 特段の対応なし(下記BRで対応しているため)
- Baseline Requirements (BR)
  - 2013-07 中間CAのプロファイル要件を改訂したv1.1.6を策定・施行
    - extendedKeyUsage必須: serverAuthまたはclientAuth
    - serverAuthの場合はnameConstraintsも必須
    - ただし具体的な名前空間に関する記述はなし
- Network Security Control
  - 2013-01 DigiNotar事件を受け，策定・施行
    - CAのネットワークセグメントの隔離徹底，権限分離，パッチ管理など
    - ~~ただし，すべてSHALLなので強制力はない??~~

ドメスティックな認証局とグローバルな認証局に整理できるといいかも!?

SHALLはMUST相当なので強制でした(_o_)

nameConstraintsについて (1)

- CABFで2013年前半に主に議論されてきた
- BR 1.1.6 で追加されたばかり

- ***9.7 Technical Constraints in Subordinate CA Certificates via Name Constraints and EKU***
  - For a Subordinate CA Certificate to be considered Technically Constrained, the certificate MUST include an Extended Key Usage (EKU) extension specifying all extended key usages that the Subordinate CA Certificate is authorized to issue certificates for. The anyExtendedKeyUsage KeyPurposeId MUST NOT appear within this extension.
  - If the Subordinate CA Certificate includes the id-kp-serverAuth extended key usage, then the Subordinate CA Certificate MUST include the Name Constraints X.509v3 extension with constraints on dNSName, iPAddress and DirectoryName as follows:-

nameConstraintsについて (2)

- 現在300以上あるルートCAの大半はおそらくローカルマーケット
  - 政府系か，商用認証局であっても半官半民の国内向け認証局
  - トップ10でグローバルシェアの7割以上

CA	Feb-13 Count (%)	Jan-13 Count (%)	Growth (%)
GoDaddy.com, Inc.	274,253 (21.57)	269,354 (21.63)	-0.28
GeoTrust, Inc.	197,872 (15.57)	191,211 (15.36)	1.35
COMODO CA Limited	98,238 (7.73)	91,434 (7.34)	5.23
Verisign	92,742 (7.30)	92,492 (7.43)	-1.8
Thawte, Inc.	67,040 (5.27)	66,098 (5.31)	-0.66
DigiCert	60,124 (4.73)	58,347 (4.69)	0.92
GeoTrust Inc.	48,300 (3.80)	47,708 (3.83)	-0.85
GlobalSign nv-sa	45,569 (3.58)	44,311 (3.56)	0.72
Unknown	33,372 (2.63)	33,016 (2.65)	-1
Network Solutions L.L.C.	25,638 (2.02)	25,099 (2.02)	0.04
Total	**943,148 (74.20)**	**919,070 (73.82)**	**4**

Certificate Authority Market Share Report
http://www.securityspace.com/s_survey/data/man.201302/casurvey.html

nameConstraintsについて (3)

- 国内だけを発行対象とするのであれば名前空間を制限してしまえばよいのでは?
  - nameConstraintsを正しく処理できる実装は?
- CAにとって名前空間を制限するインセンティブは?
  - ドメインの実在性確認はWHOISに大きく依存
  - 信頼性の低いレジストリが運営するTLDはリスクが高い

nameConstraintsについて (4)

- gTLD増加問題
  - .my vs. .rny
  - IDNベースのgTLDなどもあり，無節操に発行申請を受け付けるとスクリーニングコストが大変なことに…
  - 信頼できるレジストラのTLDのみ発行対応する，という宣言もありかも
- IDN-TLDを審査する難しさ
  - 審査体制の維持コスト vs 申請機会の少なさ
  - キリル文字などを使ったフィッシング

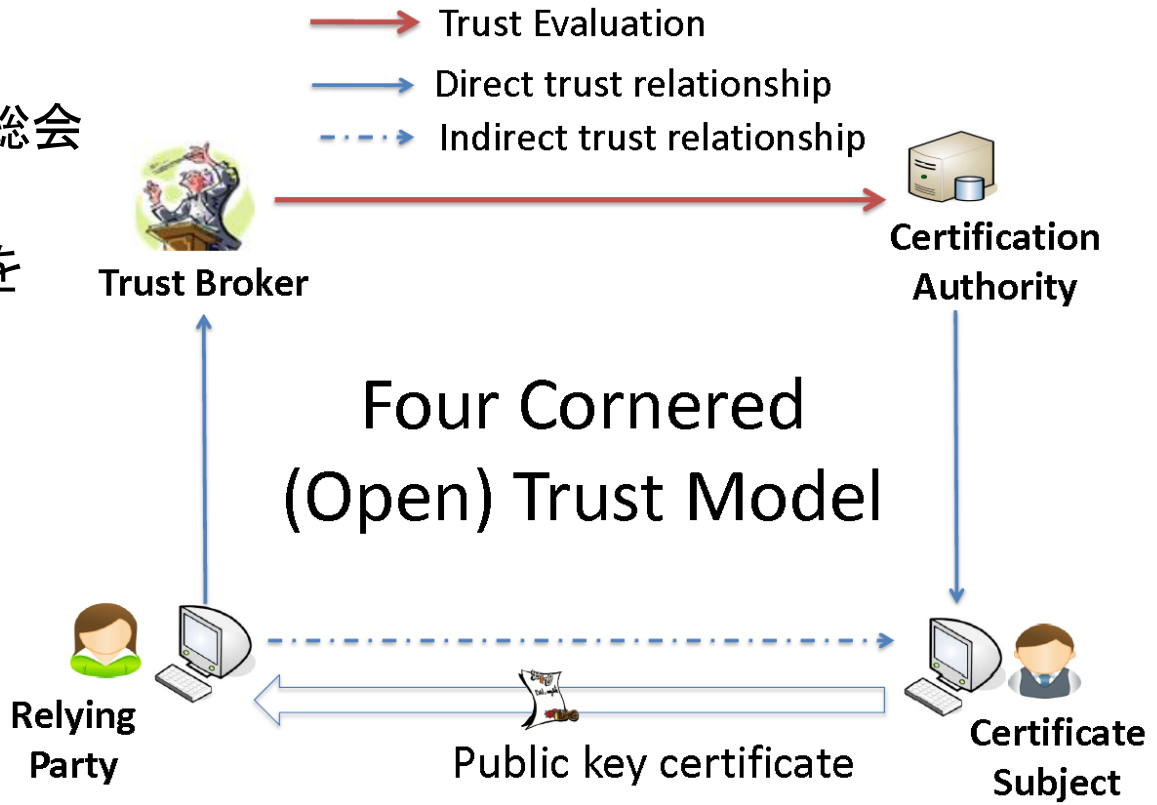
[告知] 新gTLD大量導入に伴う リスク検討・対策提言専門家チーム

- これまで勝手にgTLDをプライベートな名前空間として利用してきた組織によって生じる，名前衝突問題の一種
  - 証明書の発行対象にも重複が発生する場合がある
- SAC057: SSAC Advisory on Internal Name Certificates (15-Mar-2013)
  - ICANNによる名前衝突問題と証明書に関する調査報告書
- 国内への問題周知や対策・提言などをまとめる専門家チームをJPNICが設立
- 3月末を目処に国内向け報告書を作成中

ITU-T SG17 X.509

- Trust Brokerの提案
  - David ChadwickらがSG17総会@Geneveで提案(2013-04)
  - CAを評価するTrust Brokerを加えた4コーナーモデル
- まだ検討を開始した段階

•ブラウザベンダやEUのTrusted Service Providerなどの概念を明確化したもの
•まったく新しいモデルなわけではない
•デファクトのデジュール化



Proposition summary to X.509 committee:
Adding the Role of technical and juridical expert to the X.509 trust model
http://www.x500standard.com/index.php?n=Ig.X509ext
PKI: State of the art and future trends
http://www.ietf.org/proceedings/88/slides/slides-88-wpkops-0.pdf

その他の組織の対応

- NIST CA Workshop
  - 様々な対策技術の議論
- IAB Security Program
  - 対策技術のサーベイ
- ISO/IEC JTC 1/SC 27
  - New Study Group: Framework for PKI Policy / Practices / Audit (2013-04～)
  - ITU-T SG17同様にTSPを対象とした議論?
- CA Security Council
  - 2013-02 設立
  - Comodo, DigiCert, Entrust, GlobalSign, Go Daddy, Symantec, and Trend Micro

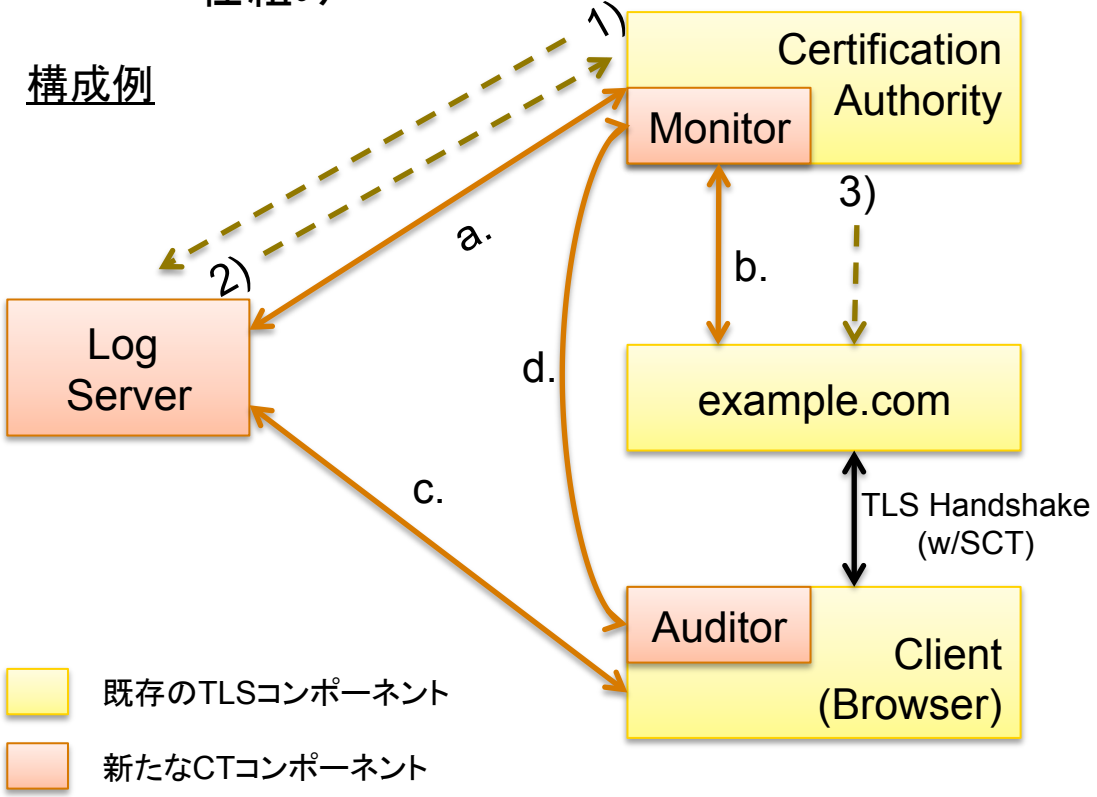
主な対策技術

- Certificate Transparency系
  - Sovereign Keys
- Perspectives系
  - Convergence
  - MECAI
  - DetecTor
- Public Key Pinning系
  - Trust Assertions for Certificate Keys (TACK)
  - DNS-Based Authentication of Named Entities (DANE)

Certificate Transparency (1)

- 概要
  - 証明書発行内容の事前チェック
  - 他の認証局で発行済の証明書を，別の認証局で再発行しようとした際に検知する仕組み

構成例



0) 証明書発行申請の受付
1) Precertificateの生成・送信
2) SCT (Signed Certificate Timestamp)の発行
3) 証明書を発行，SCTと共に配付

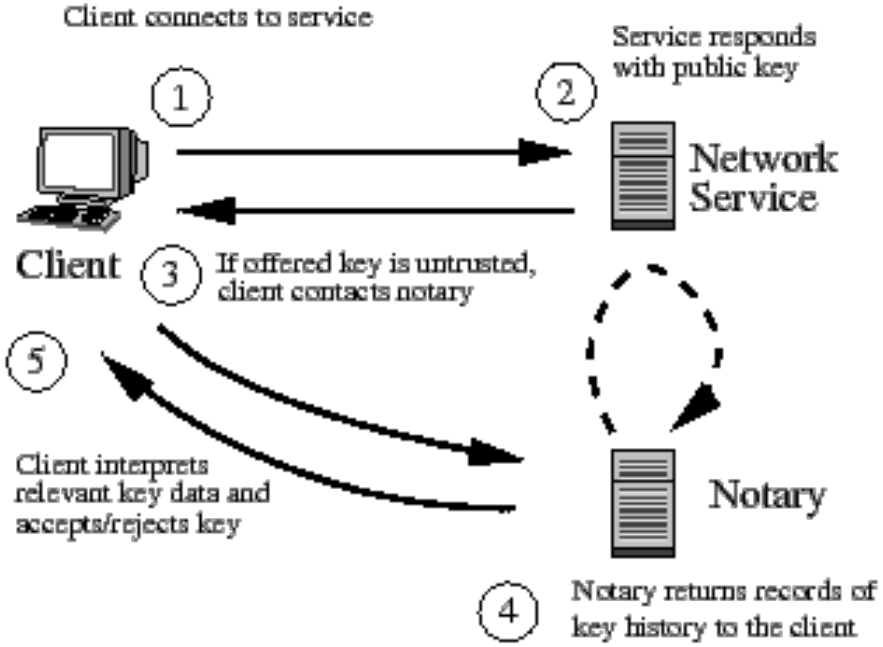
a. 不審な証明書の監視
b. example.comに対して不正な証明書発行がなかったことを照会
c. ログの監査，特定の証明書のログ
d. ログの分岐検知などのためにログ情報の交換

Certificate Transparency (2)

- 実装
  - GoogleがNotary(Log Server)を提供
  - 米DigiCertがいち早く対応を表明
  - 現在trans WGで6962bisとしてCA以外への拡張が議論されている
    →汎用的なNotaryサーバとしての期待
- 課題
  - 発行情報を収集するNotaryサーバが必要
  - 参加した認証局間での不正発行しか検知できない
- 類似技術
  - Sovereign Keys (Timeline Serverが各サイトの公開鍵を把握する)

Perspectives (1)

- 概要
  - 初めてアクセスするサイトの鍵の信頼性を第三者検証に委ねる
    - SSL/TLSが抱えるTOFU (Trust on first-use) リスク
  - 理想的には，複数のNotaryと，アクセス先の鍵情報を提供するクライアント群によって，分散型データベースを構築する
  - 利用者は，複数のNotaryに検証を依頼することでTOFUリスクを回避する



Perspective (2)

- 課題
  - 複数のNotaryとできるだけ大勢の誠実なクライアントが必要
  - Notaryに対するTOFU問題
- 派生技術
  - Convergence
  - Mutually Endorsing CA Infrastructure (MECAI)

Public Key Pinning

- 概要
  - アクセス先のサーバ鍵を事前共有しておくことで，中間者攻撃を検知する
  - 狭義のPKP(ブラウザにハードコーディング)と，広義のPKP for HTTPがある
    - 前者はブラウザにハードコーディング
    - 後者は初回HTTPヘッダを使ってサーバからブラウザにPublic KeyをPinする
- 実装
  - Chrome, Cert Patrol (Firefox add-on), Android 4.2以降
- 課題
  - ハードコーディングだとスケールしない→PKP for HTTPで解決
  - TOFU問題 → 後述のpreloaded HSTSと組み合わせて解決する
- 類似技術
  - Trust Assertions for Certificate Keys (TACK)
  - DNS-Based Authentication of Named Entities (DANE)

```
Public-Key-Pins:
pin-sha1=”4n972HfV354KP560yw4uqe/baXc=”;
pin-sha1=”qvTGHdzF6KLavt4PO0gs2a6pQ00=”;
pin-sha256=”LPJNul+wow4m6DsqxbninhsWHlwfp0JecwQzYpOLmCQ=”;
max-age=10000; includeSubDomains
```

HTTP Strict Transport Security

- 概要
  - サーバ接続を強制的にHTTPSにする
    - 単なるリダイレクトだと中間者攻撃リスクがある
- 実装
  - ブラウザ：IE以外はほぼ対応済
  - サーバ：ヘッダだけなのでほぼ全実装が対応
- 課題
  - TOFU問題 → preloaded HSTSで回避
    - TOFU: Trust on First Use
    - トラストアンカー配布問題もTOFUの一種

```
<VirtualHost example.com:443>
    # Use HTTP Strict Transport Security to force client to use secure connections only
    Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"
</VirtualHost>
```

User:Dotdotike/Trust Upon First Use - Wikipedia, the free encyclopedia
http://en.wikipedia.org/wiki/User:Dotdotike/Trust_Upon_First_Use

各方式の比較分析資料

- NIST CA Workshop **Session 3: Analysis Frameworks**
  - **SEARCH for Trust** ***SSL/TLS Enhancement or Alternatives for Realizing CA Homogeneity (SEARCH) for Trust***
    - 主要方式をいくつかの評価軸で定性的に採点，比較している
    - HSTS + Pinningが最高点，次点でCAA(DNSSEC)
  - **Deployment Models for Backup Certificate Systems**
    - 全部ばっさりとダメ出しされている・・・
- IAB Security Program
  - **Evolving the Web Public Key Infrastructure**
    - 淡々と技術解説，長短分析しているのみ
    - 長短分析は実は前出*”Deployment～”*のEric Rescorlaが書いている

スライド20の各技術の概要はこれらによくまとまっています

Workshop on Improving Trust in the Online Marketplace
http://www.nist.gov/itl/csd/ct/ca_workshop.cfm
Alexandra C. Grant, *"Search for Trust: An Analysis and Comparison of CA System Alternatives and Enhancements."* Dartmouth Computer Science Technical Report TR2012-716, June 2012.
http://www.cs.dartmouth.edu/reports/abstracts/TR2012-716/
Evolving the Web Public Key Infrastructure
http://tools.ietf.org/html/draft-tschofenig-iab-webpki-evolution

まとめ

- 利用者
  - 機微情報を盗聴・搾取されないようにするために・・・
  - HSTSやPublic Key Pinningに対応したブラウザの利用
    - Chrome, Firefoxなど
  - 同技術未対応サイトでの機微情報の送受信を控える
    - とは言え判別は難しい…
- サイト管理者
  - 不正サイトを立てられないようにするために・・・
  - HSTSおよびPinningのサポート
  - 金融機関などはpreloaded HSTS listに追加してもらう
- 認証局
  - 不正侵入の防止・検知
    - CABF Network Security Controlの遵守
  - 不正発行・失効の防止・検知
    - 名前制約による被害範囲の最小化
    - Certificate Transparency?