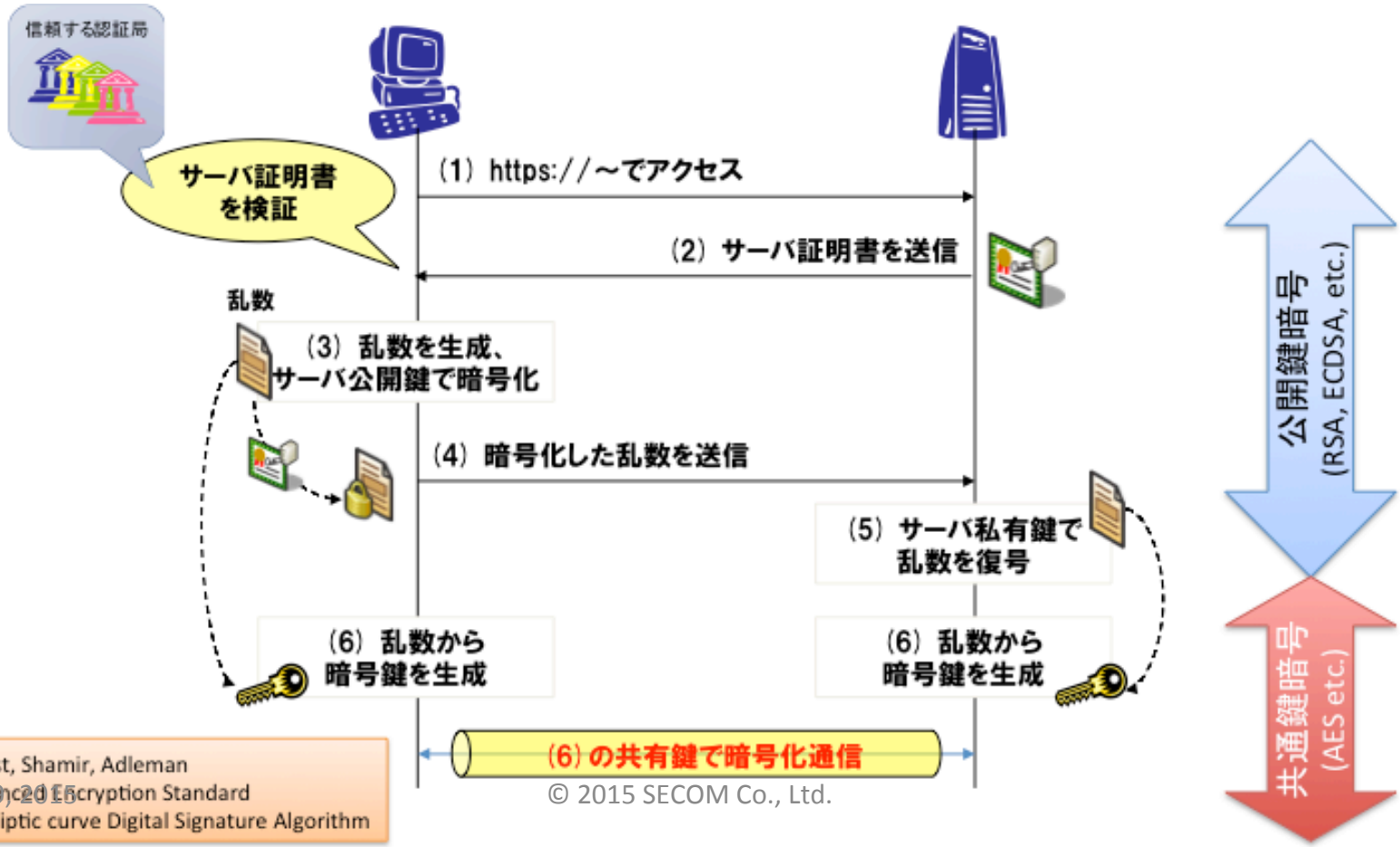
Internet Week 2015
(D1) DNS DAY

「PKIとDNS」
TLS(Web PKI)の立場から

セコム(株)IS研究所
島岡　政基

TLS(サーバ認証)の目的

- 証明書の用途
  - 認証と鍵交換(暗号化は共通鍵の仕事≠証明書)



RSA: Rivest, Shamir, Adleman
AES: Advanced Encryption Standard
ECDSA: Elliptic curve Digital Signature Algorithm

TLSの信頼モデル(1)

- 信頼の連鎖
  - (ブラウザ→ブラウザベンダ→)
    ルートCA→中間CA→サーバ証明書
- 検証方法
  - 証明パスの検証(PKI)
    - 下位証明書の署名検証←上位証明書の公開鍵
    - 各証明書の失効検証(CRLまたはOCSP)
  - サーバ認証(TLS)
    - 証明書記載のサーバFQDN↔アドレスバーのURL

これを判定するのは誰か?
→ブラウザ(アプリ)

TLSの信頼モデル(2)

- 証明書の信頼性(発行時の確認事項)
  - 申請者が私有鍵を持っていること(Proof of Possession)
  - 申請者の本人性確認(Identity Proofing)
  - 申請者の実在性確認(ドメイン名の所有権)
- トラストアンカーの信頼性
  - 証明書発行時の確認事項を公開文書(CP/CPS)で規定し、その運用について一定の準拠性監査(WebTrust for CAなど)を受けていること
  - 加えてブラウザベンダの審査が必要

これを判定するのは誰か?
→ブラウザベンダ

トラストアンカーの配布方法

- 選び方
  - 主要ブラウザ・OS等にあらかじめインストールされた「トラストリスト」
  - ブラウザ・OS等によって異なる。多いもので400件近い。
  - エンドユーザが選択(追加/削除)することも可能だが…

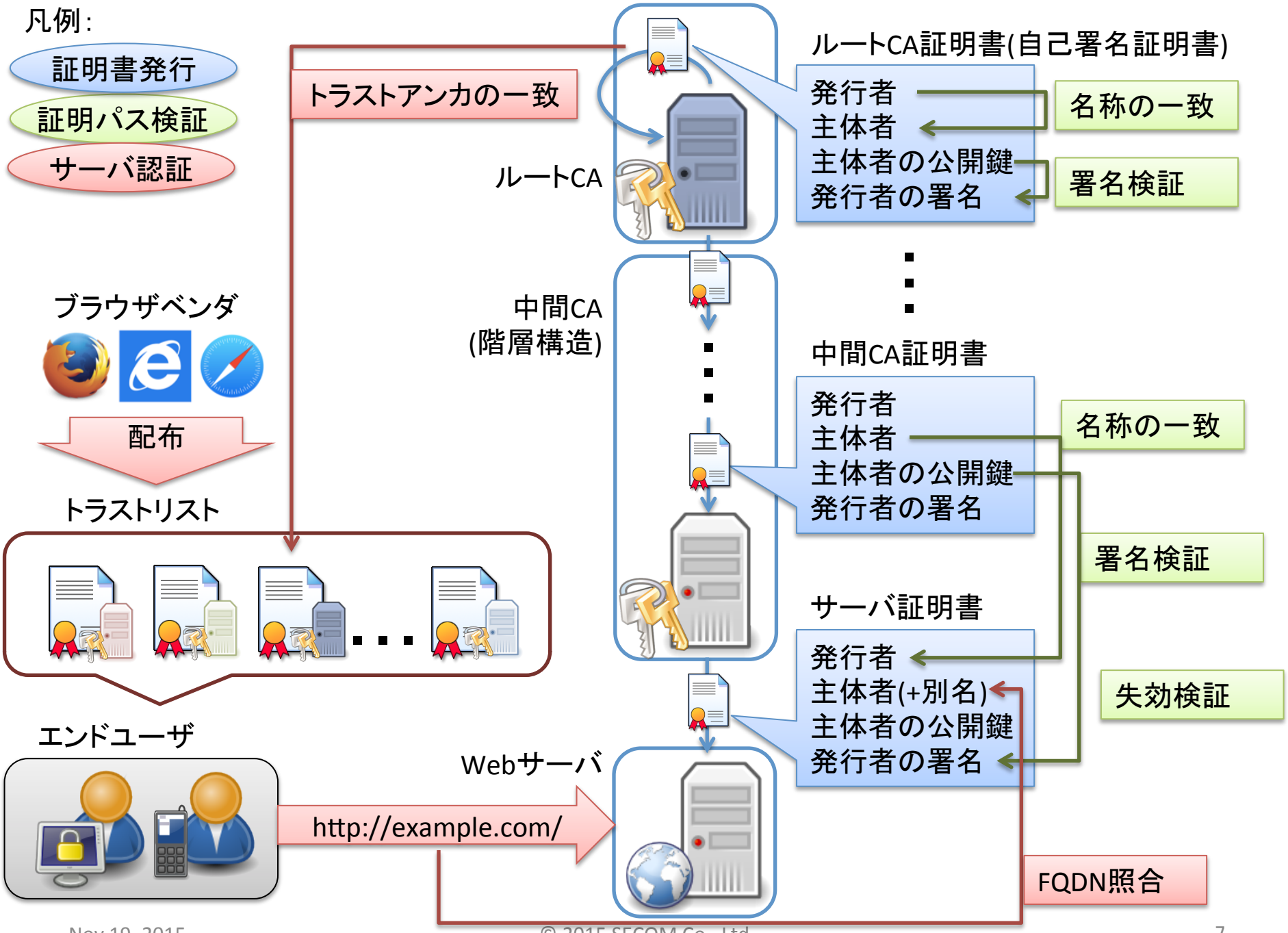
	登録件数
PCブラウザ	Windows(362) Mozilla(166) OS X(209)
スマートフォン タブレット	Android 4.4(150) iOS 7 (211)
フィーチャーフォン	ドコモ(29) au (42) ソフトバンク(31)

2014年6月調べ

- 実社会との境界線
  - エンドユーザとブラウザベンダ(実質的なトラスト)
  - 認証局とWebサーバ(発行時の確認事項)

実際の信頼モデル

- 前提
  - 認証局が証明書発行の際に何を確認するかはCP/CPSで規定され、その通りに運用していることについて定期監査を受ける義務を負う
    - 確認事項：PoP、本人性確認、実在性確認
    - 監査規準：WebTrust for CA, Baseline Requirements (CA/Browser Forum)など
    - 証明書プロファイル：暗号アルゴリズム、鍵長、鍵用途など
- トラストリスト
  - 一定の監査規準に合格した認証局のみがトラストリストに登録される(申請できる)



認証局にまつわるインシデント

- DigiNotar事件(2011)
  - オランダの半官半民ルート認証局DigiNotarに対する不正侵入と500枚超におよぶ証明書の不正発行
- CNNIC事件(2015)
  - CNNICのルート認証局下でエジプトの中間認証局自身が証明書の不正発行

我々はそもそもCNNICやDigiNotarを
信頼する必要があったのだろうか？

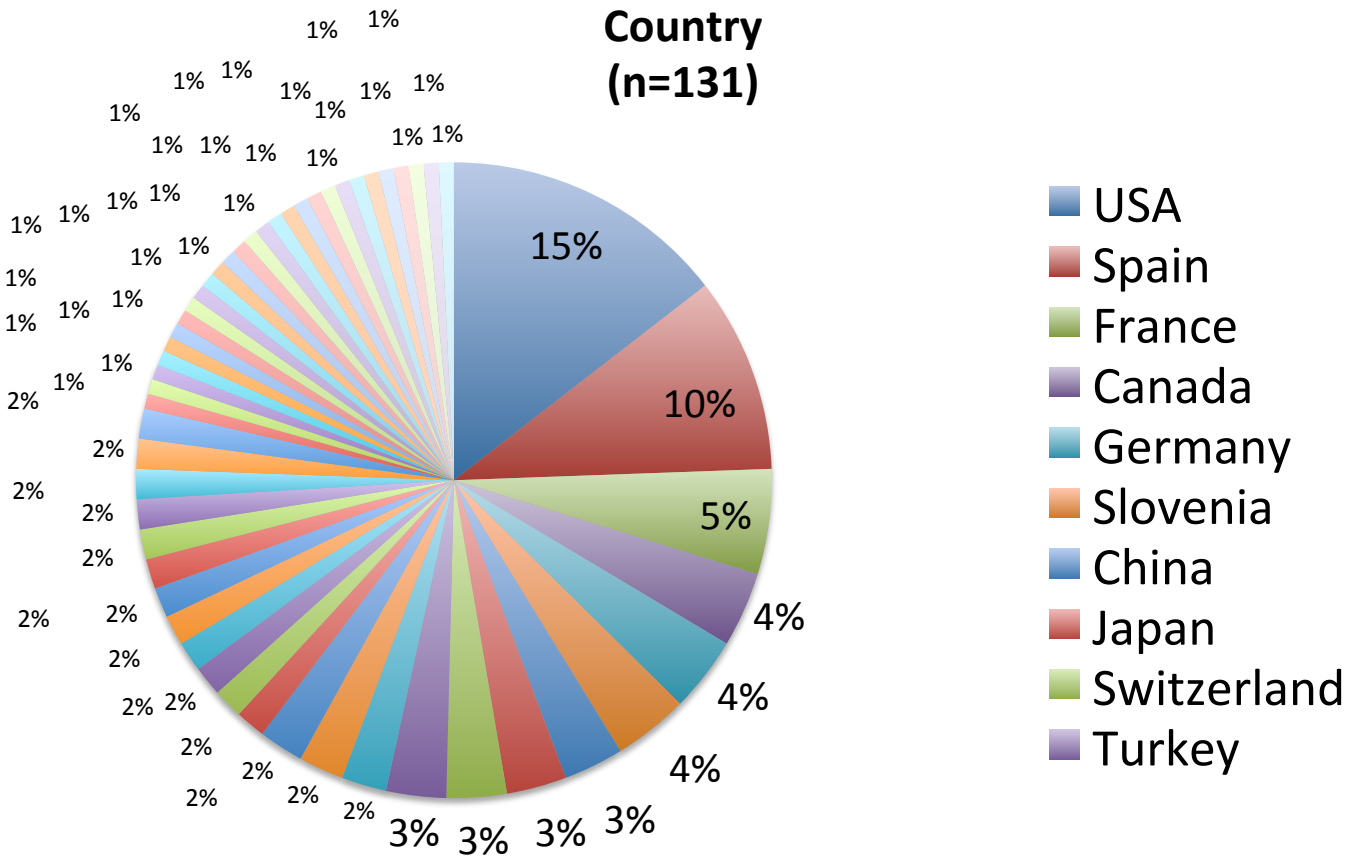
認証局のシェア Top10

CA	Count	%
GoDaddy.com, Inc.	507,342	20.99
COMODO CA Limited	358,360	14.83
GeoTrust Inc.	356,226	14.74
DigiCert	250,448	10.36
GlobalSign nv-sa	128,503	5.32
GeoTrust, Inc.	75,661	3.13
Gandi	75,551	3.13
Symantec Corporation	67,037	2.77
thawte, Inc.	55,673	2.3
Starfield Technologies, Inc.	39,638	1.64
Total	**1,914,439**	**79**

Top10でシェア79%、Top20で同90%超

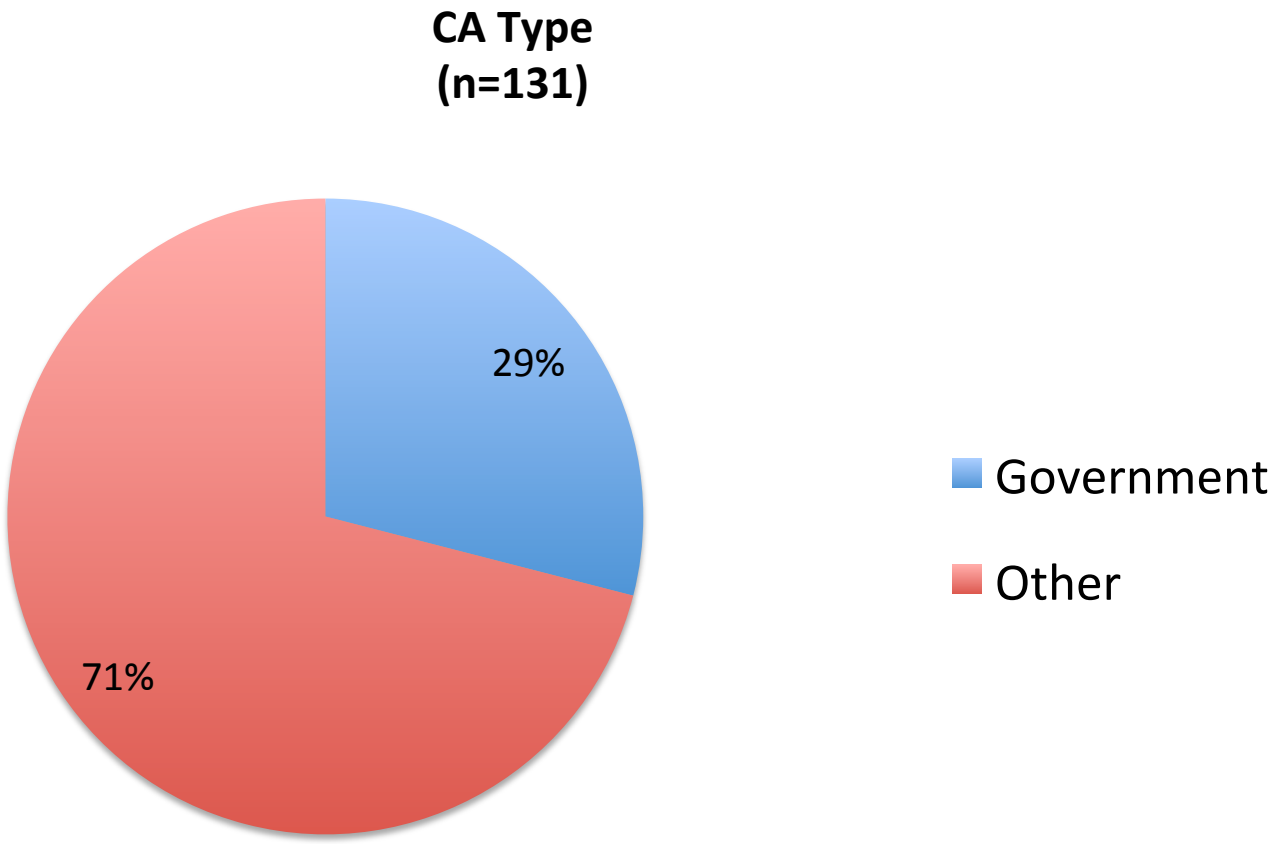
Certificate Authority Market Share Report (2015年10月時点)
http://www.securityspace.com/s_survey/data/man.201510/casurvey.html

CA Owner per Country



Microsoft Trusted Root Certificate Program: Participants (Last Revision When: 3 Nov 2015 2:09 PM)
http://social.technet.microsoft.com/wiki/contents/articles/31634.microsoft-trusted-root-certificate-program-participants.aspx

CA types



Microsoft Trusted Root Certificate Program: Participants (Last Revision When: 3 Nov 2015 2:09 PM)
http://social.technet.microsoft.com/wiki/contents/articles/31634.microsoft-trusted-root-certificate-program-participants.aspx

Web PKIの認証局のあり方

現実	ブラウザベンダから信頼を強制されている ・信頼するルート認証局、本当にそんなに必要? ・信頼する必要もなかった認証局でインシデントが…
建前	必要最小限の信頼できる認証局を 利用者自身が判断・選択
ベスト プラクティス (仮説)	主要認証局(10～20程度) 自国・地域で必要な認証局(1～5程度)

Web PKIの鍵管理

	ルートCA	Webサーバ
鍵生成	(CABFで規定) HSMでの生成 監査人立会いまたは録画	規定なし
鍵の公開	(CABFで規定) リポジトリへの公開	TLS Handshke
鍵の導入	トラストリストによる配布	Web Enrollment(SCEPなど) PKCS#12形式での配布 など
鍵の更新	(CABFで規定) 鍵生成に同様	規定なし
鍵の失効	(CABFで規定)	(CABFで規定)
鍵の期限切れ	25年以下 (Microsoftの場合)	39ヶ月以下(CABFで規定)
鍵の廃棄	N/A	N/A

DNSとの関わり

認識しておくべきこと

- 証明書の不正発行とDNS乗っ取り
  - DigiNotar事件含め2011年以降増えている
  - なんらかの方法で攻撃者の持つ鍵ペアに対して*.google.comなどの証明書を不正発行
  - DNS乗っ取りなどでクライアントに不正なDNS応答
- TLSはドメイン名によるアクセスが大前提
  - DNS応答が信頼できなければTLSは信頼できない
  - 一方でDNS over TLSなどの議論も…

DNSSEC

DANE	• オレオレ証明書を(DNS応答を使って)安全に配布できるようになる
CAA	• サーバが発行元認証局を指定できる(不正発行対策)