今理解しておくべき Web PKIを支えるトラストの動向

セコム株式会社IS研究所
島岡　政基

自己紹介

- 認証局サービスの設計・構築(2000～)
- 運用視点からのPKIに関する調査研究(2001～)
  - 各種PKI相互運用プロジェクト(JNSA, Asia PKI Forumなど)
  - IETFでの標準化活動(RFC 5217)
  - 認証業務における本人確認コストのモデル化
- 数少ない国内ルートCAの設計・構築・運用(2004～)
  - 各ブラウザベンダへのルートCA登録など
  - 国内初のWebTrus for CA認定取得
- 最近はトラストの研究がメイン
  - トラスト勉強会はじめました(次回12/18)
  - https://sites.google.com/view/trust-study

今日お話しすること

- Web PKIを支えるトラストの歴史
- CTをはじめとする技術的取り組み
- CA/ブラウザフォーラムを中心とする運用的取り組み
- CA安全神話崩壊がもたらした変化

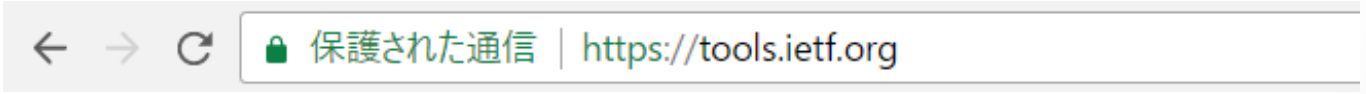
まずは
ウォーミングアップ

サーバ証明書の種類

種類	説明
DV証明書 (Domain Validation)	ドメイン名に関する身元確認 WHOISデータベースなどを参照
OV証明書 (Organization Validation)	ドメイン名および組織の身元確認 上記に加えて企業信用情報データベースなどを参照
EV証明書 (Extended Validation)	ドメイン名および組織(**法人格**)の身元確認 上記に加えて(商業)登記簿などを参照 DV/OVと異なりグリーンバーによる視認性を確保

HTTP

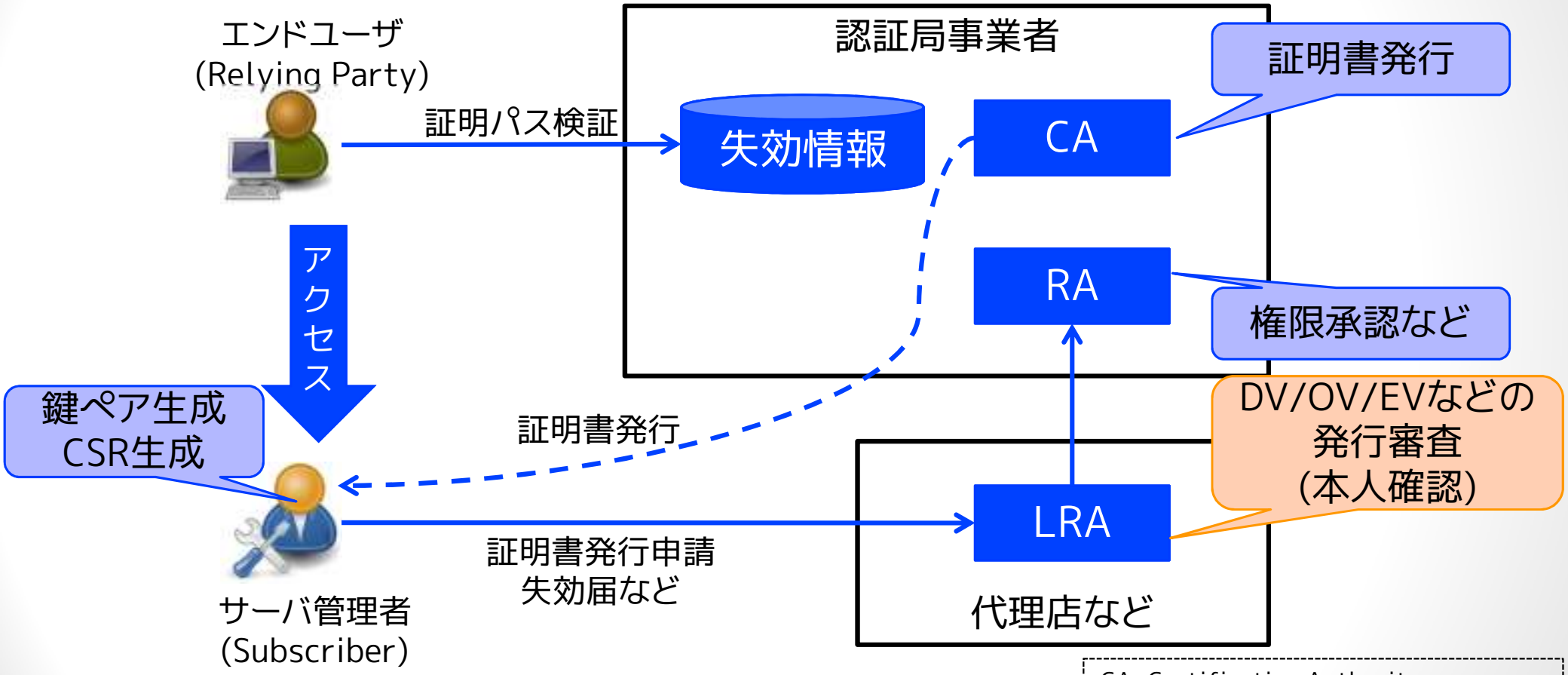
DV



OV

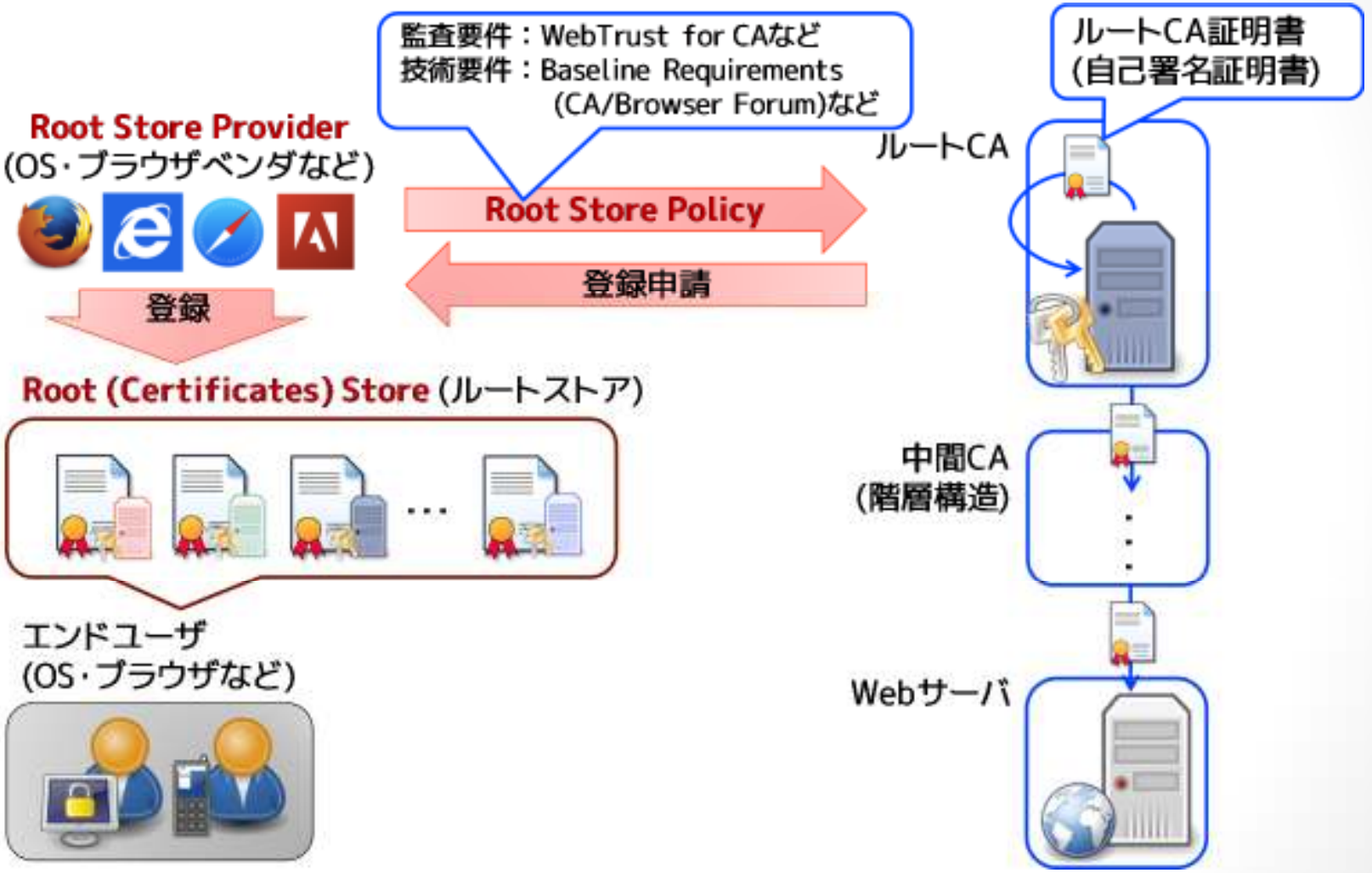
EV

CA/RAの役割



CA: Certification Authority
(L)RA: (Local) Registration Authority
CSR: Certificate Signing Request

Web PKIのトラストモデル



用語の説明

- WebTrust for CA(WTCA)
  - 認証局運用監査規準のデファクトスタンダード
  - AICPA/CICA(米・加公認会計士協会)が2000年に策定
  - CABF設立後はCABFの各種要件・ガイドラインを参照
  - 毎年の外部監査を必須要件としている
- CA/Browser Forum(CABF)
  - CA事業者とブラウザベンダの業界団体として2006年に設立
  - WG活動をもとに認証局の各種要件・ガイドラインを策定
  - 動議・投票による合意形成

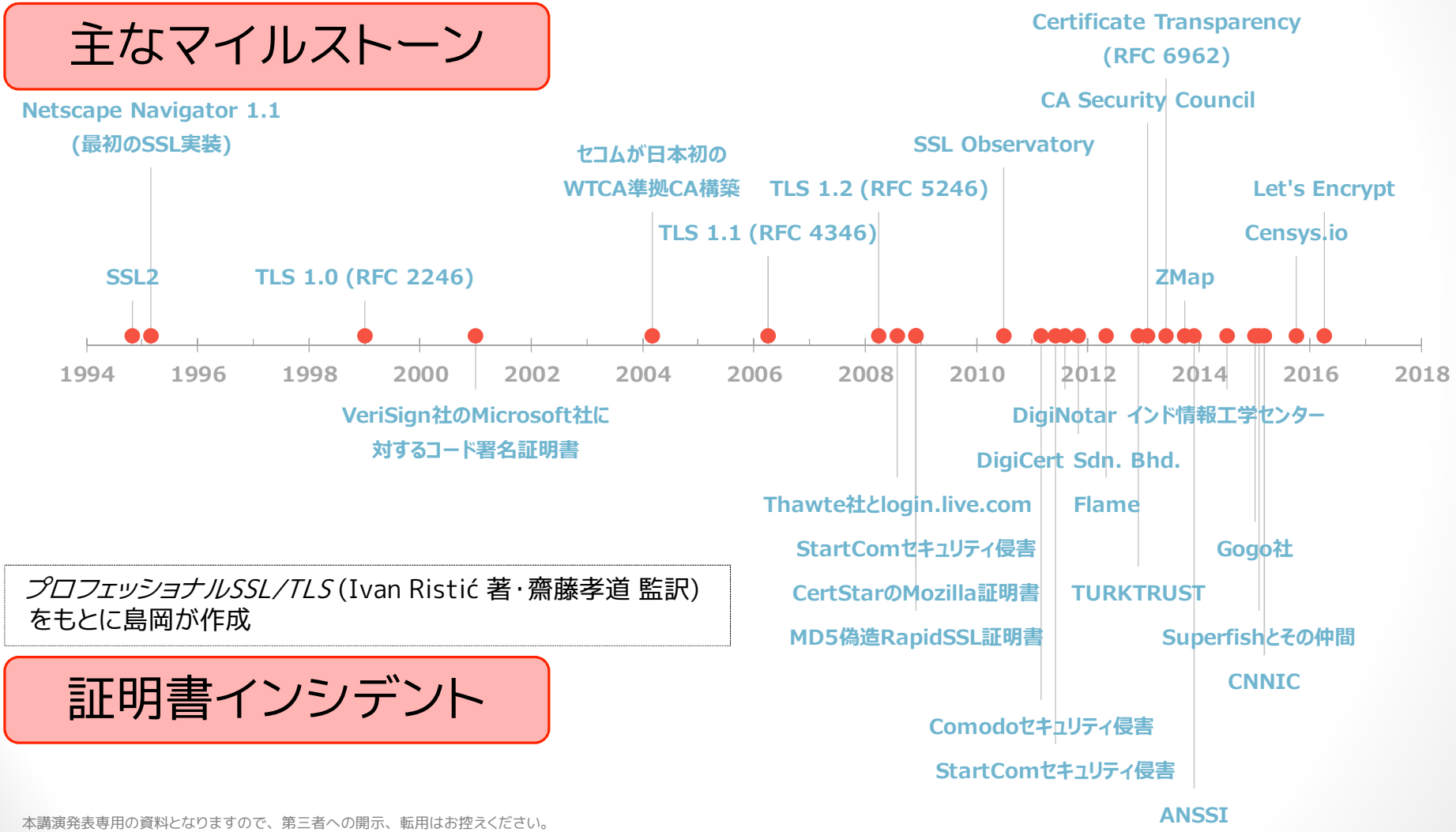
Root Store Policy, Root Program

- Apple
  - https://www.apple.com/certificateauthority/ca_program.html
- Google Chrome
  - https://www.chromium.org/Home/chromium-security/root-ca-policy
- Microsoft
  - https://aka.ms/rootcert/
- Mozilla
  - https://www.mozilla.org/projects/security/certs/policy/
- Opera
  - https://www.opera.com/docs/ca/

WebPKIに
何が起きているのか

Web PKIのトラストの歴史

主なマイルストーン

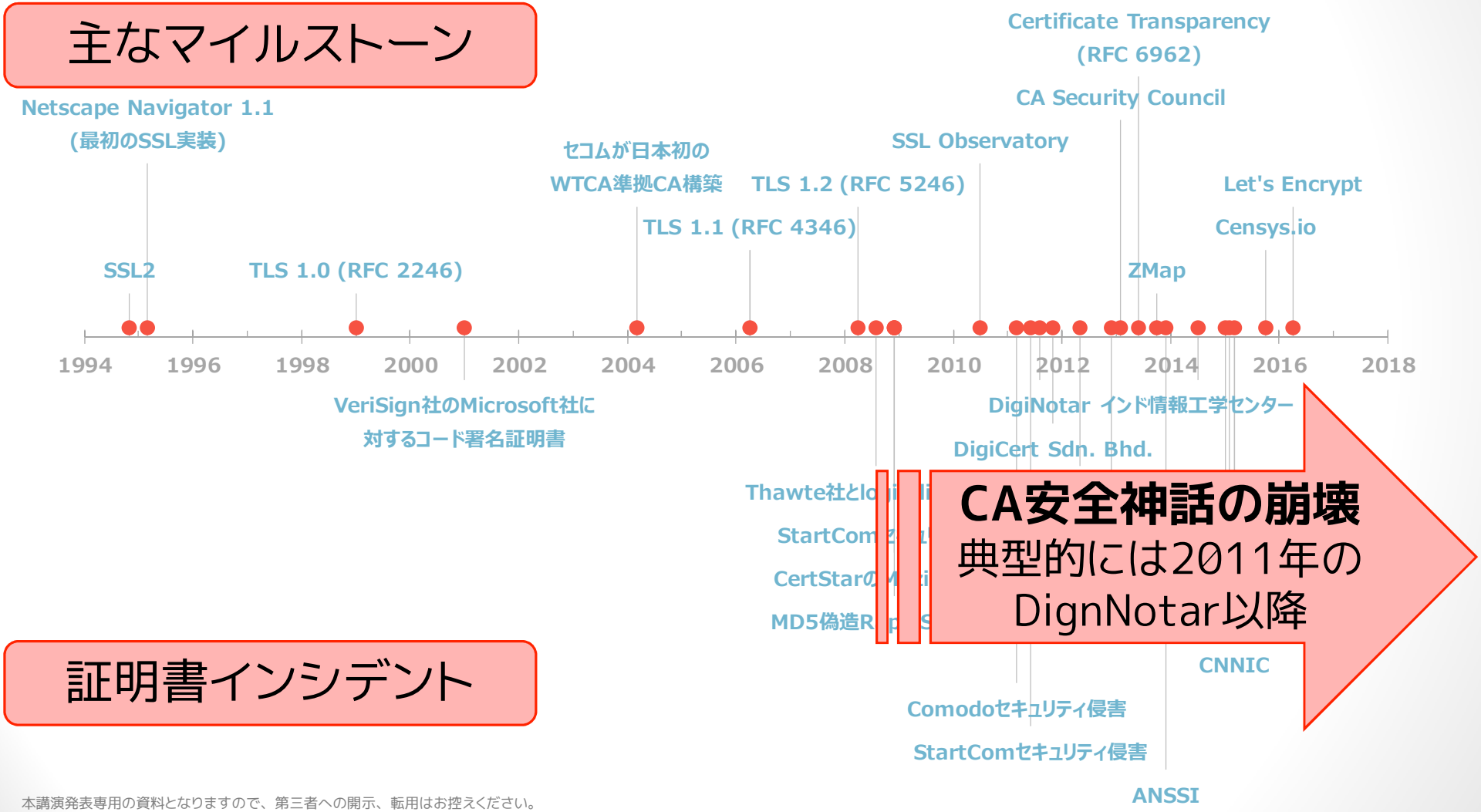


プロフェッショナルSSL/TLS (Ivan Ristić 著・齋藤孝道 監訳)
をもとに島岡が作成

証明書インシデント

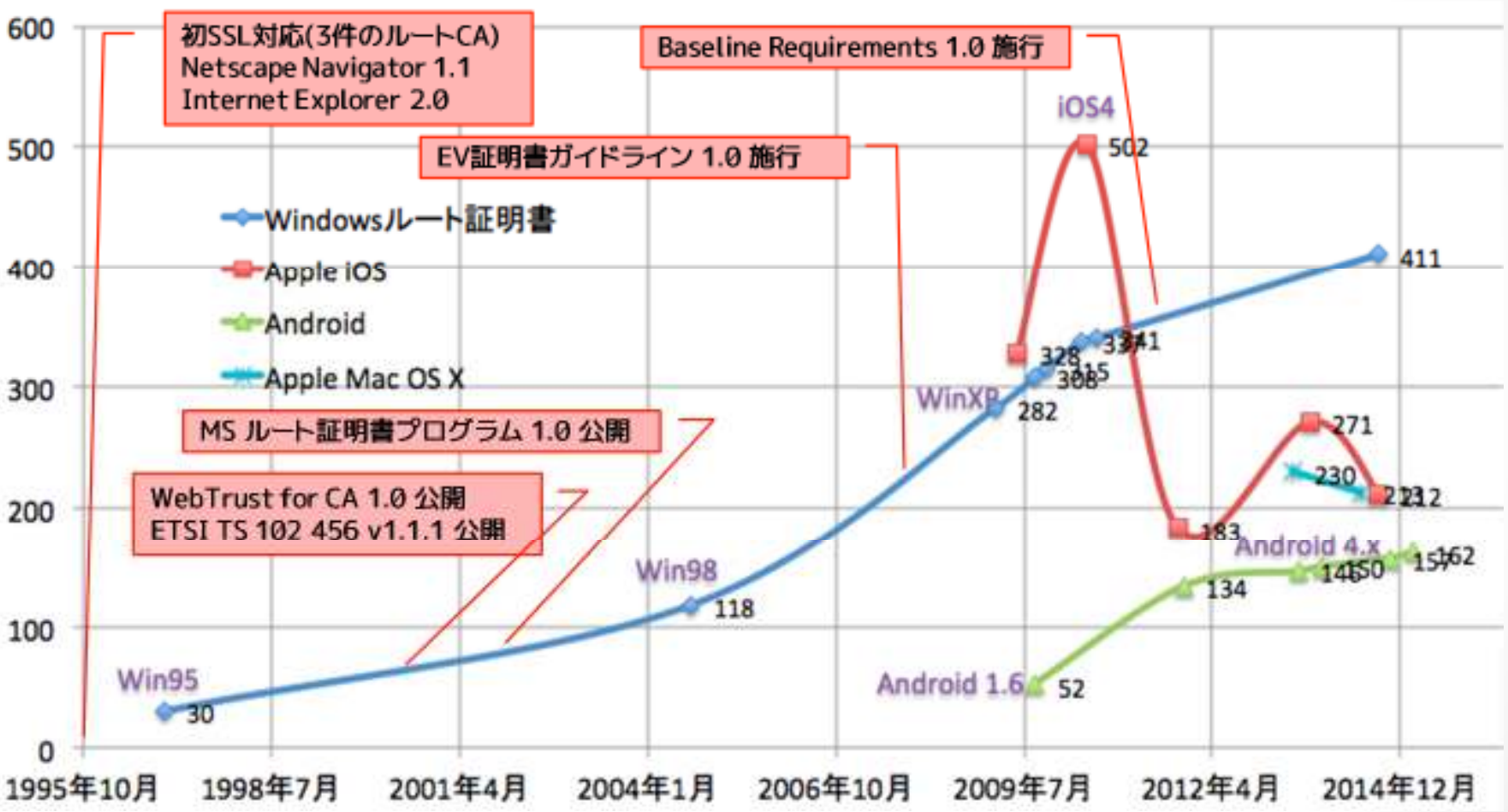
Web PKIのトラストの歴史

主なマイルストーン



証明書インシデント

ルートストアの変遷



自堕落な技術者の日記 - Windowsルート証明書の更新プログラム(2014.09)と戯言など
http://blog.livedoor.jp/k_urushima/archives/1767480.html

いまWeb PKIに起きていること

- CA安全神話の崩壊
  - 2008年以降証明書の不正発行・偽造などが本格化
    - 2011年のオランダのルート認証局DigiNotarへの不正侵入による不正発行が典型的なターニングポイント
  - 数の膨張による人^H質的運用の限界
- NSAをはじめとするPervasive Surveillanceの顕在化
  - 従来の想像を超える攻撃技術・資源の投入 (stuxnet, flame, etc.)
  - より高度な暗号技術の開発競争へ (TLS 1.3, 耐量子暗号など)
- 暗号技術(標準・実装)に対する攻撃の本格化
  - BEAST, Lucky13, Heartbleed, POODLEなど
  - MD5証明書偽造、RC4解読など

認証局を盲目的に
信頼できる時代は終わった

より強固な暗号化通信のニーズ
信頼基盤・暗号技術の安全性回復

今のインターネットに必要なこと

- より強固な暗号化通信のニーズ
  - 中長期的にも確実に必要
  - プロトコルアーキテクチャなどにも Security by Designが求められる時代に

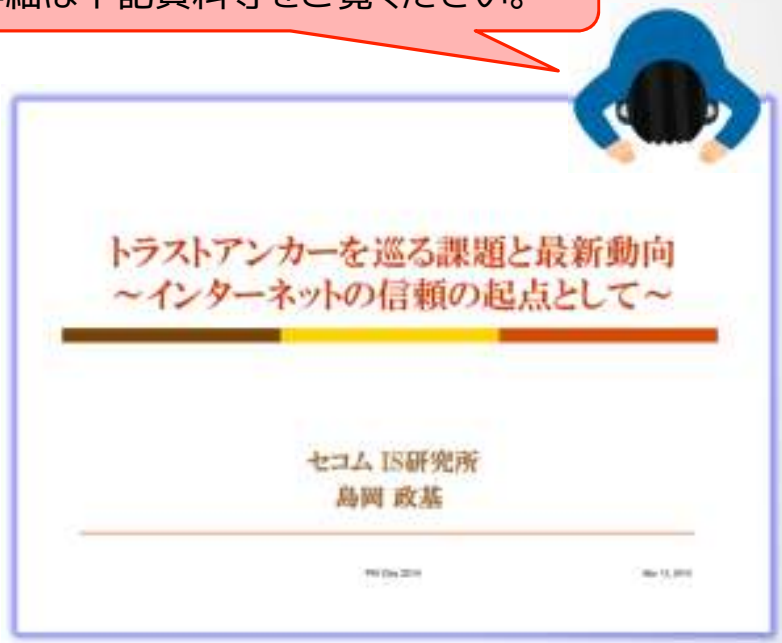
- 信頼基盤・暗号技術の安全性回復
  - 今すぐ乗り換えられる代替手段・選択肢はない
    - 実装の洗練と普及、エコシステムの確立、スイッチングコスト
    - 中長期的な観点はまた別に必要
  - 質から量のアプローチへ
    - 定量的・システマチックな運用管理(Operation Technology)へ

Web PKIのチャレンジ
～技術と運用の両面～

技術的取組み

- 証明書の不正発行・誤発行対策
  - HPKP(廃止), CT, CAA
- 常時HTTPS化
  - HSTS
- Web PKIに代わるトラスト基盤の期待
  - DANE
- 証明書の有効性を制限
  - Tech-constrained Approach
  - Short-Lived Certificate

本日は時間の都合で赤枠のみ解説します。
他の詳細は下記資料等をご覧ください。



島岡政基,「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～」,
PKI Day 2014, NPO日本ネットワークセキュリティ協会, 2014.
http://www.jnsa.org/seminar/pki-day/2014/data/AM03_shimaoka.pdf

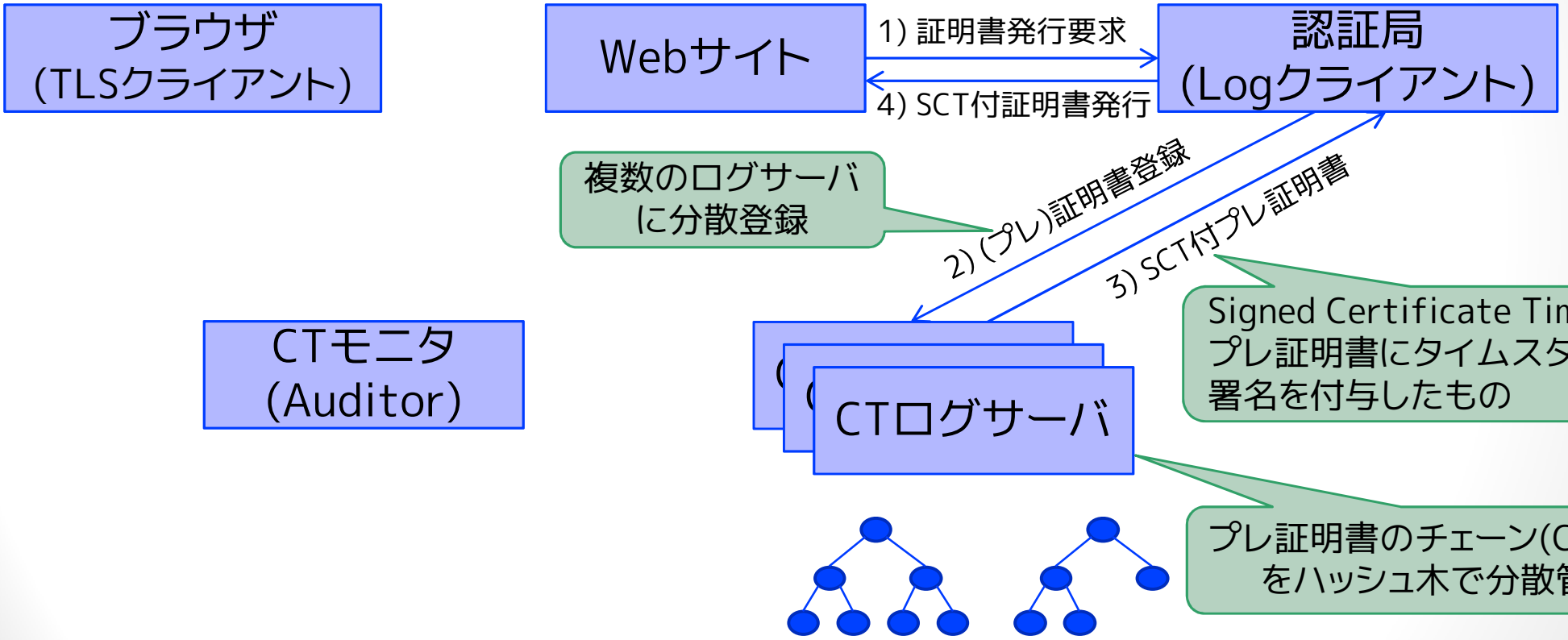
Certificate Transparency

- 自分の証明書が勝手に発行されないための技術
  - 勝手に ＝ 他の認証局から or 他の誰かに
  - DigiNotar事件を受けてGoogleが提案(2011)、2013年にRFC 6962
- すべての認証局の発行ログを衆人環視するための技術
  - 拙速が故に功罪両面あり
    →ただちに6962bisがWG itemに

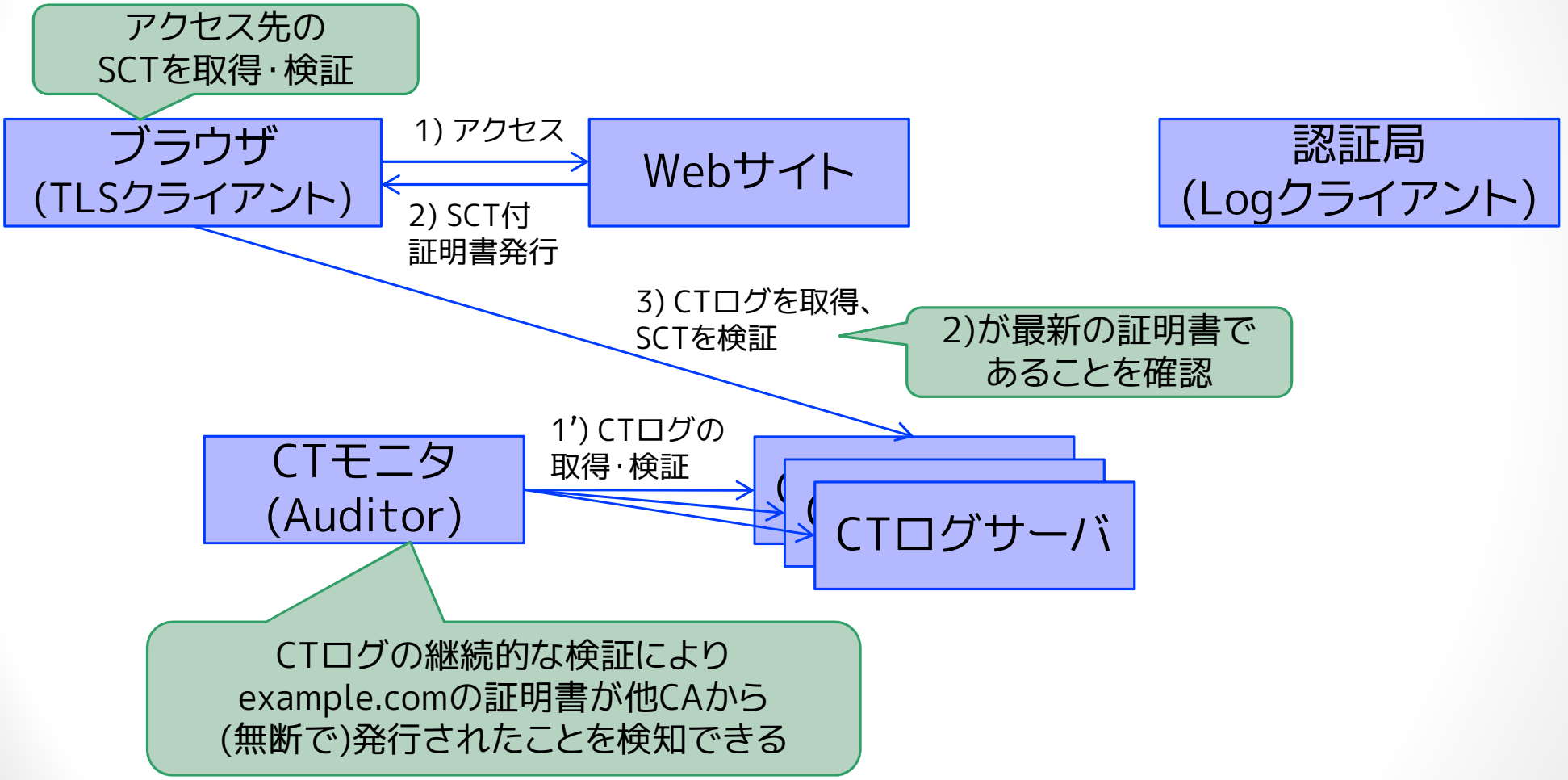
本日は時間の都合で概説のみ説明します。
詳しくは下記資料をご覧ください。

大角祐介,「Certificate Transparencyを知ろう ～証明書の透明性とは何か」,
PKI Day 2016, NPO日本ネットワークセキュリティ協会, 2016.
http://www.jnsa.org/seminar/pki-day/2016/data/1-2_oosumi.pdf

CTの仕組み(1)



CTの仕組み(2)



主なCTログサーバ

Name	Operator	Size	Status
Pilot	Google	164,039,310	Available
Rocketeer	Google	158,805,020	Available
Icarus	Google	136,315,966	Available
~~Aviator~~	~~Google~~	46,466,471	*Frozen*
WoSign log	**WoSign**	6,717,011	Available
Symantec	**Symantec**	6,067,807	Available
Skydiver	Google	6,064,152	Available
DigiCert log	**DigiCert**	3,224,377	Available
StartCom log	**StartCom**	334,643	Available
VEGA log	**Symantec**	323,970	Available
Venafi log	**Venafi**	99,824	Available

各ログサーバの保有している
証明書ログ件数

(HTTP) 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 (RFC 7469)
- 実装
  - Chrome46以降, Firefox35以降, 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
```

HPKPからCTへ？

(前略)Chromeのセキュリティ担当チームは、「Chrome 67」でHPKPのサポートを取りやめる**計画を明らかにした**。Chrome 67の安定版がリリースされるのは、2018年5月29日頃の見込みだ。

　HPKPをめぐっては、これまで複数のセキュリティ研究者がさまざまな問題を指摘してきた。たとえば、サイト運営者が誤ってサイト訪問者をブロックしてしまったりする可能性があるという。

　Chromeのチームは開発者に対し、ピンではなく、Certificate Transparency（CT：証明書の透明性）と比較的新しいExpect-CTヘッダーと呼ばれる仕組みの利用を推奨している。

出典：https://japan.cnet.com/article/35109624/

DNS CAA レコード (RFC 6844)

- Certification Authority Authorization
  - 当該FQDNに証明書を発行するCAをCAAレコードで指定する

```
example.com.  CAA 0 issue "example.net"
example.com.  CAA 0 iodef "mailto:example@example.net"
```

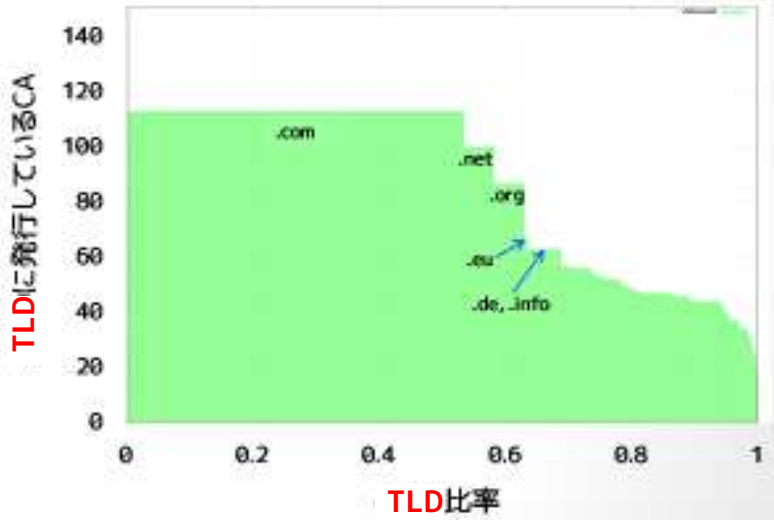
- CABF BRでCA検証が必須化(2017年9月以降)
  - CAは、発行申請されたFQDNにCAAレコードが設定されていた場合には、これに従わなければならない(MUST)
    - 一部例外規定あり
  - Webサイトが必ずCAAレコードを設定しないといけないわけではない

Tech-constrained Approach

- 認証局が発行する証明書の名前空間と拡張鍵用途を技術的に制限することによってリスクを縮減させるアプローチ
- 課題
  - すべてのルートCAにすべてのgTLDの証明書を発行できる権限を与えている (cf. *.google.com)
  - 多くのルートCAがコード署名証明書を発行する権限を持っている
- 実態
  - 多くのルートCAは発行先TLDが偏っている
    - gTLD + 自国のccTLD
  - .comに証明書を発行していないルートCAも3割近く存在する
- アプローチ
  - 認証局が発行する証明書の名前空間を技術的に制限する
    - 証明書ベース：X.509 nameConstraints拡張
    - 実装ベース：ブラウザ依存
  - 認証局が発行する証明書の拡張鍵用途を(CA単位で)技術的に制限する
    - 実装ベース：ブラウザ依存(X.509のextendedKeyUsage拡張とは別)

名前制約の効果の分析と試算

- MozillaのRichard Barnesによるレポート(2015年3月)
- 過去1年間の実績では
  - 60%のルートは、発行する証明書のTLDが11以下である
  - 28%のルートは.comに証明書を発行していない
- 各ルートが発行可能なTLDを適切に制御できたら？→試算してみた
  - 仮に実績ベースで発行可能なTLDを制限すると、attack surfaceは42%に削減される



Mozilla, Empirical measurement of the DNS scope of Mozilla root CAs, Fig. 2(a), 2015.
https://docs.google.com/document/d/1nHcqeuWlgM9a1jZ6MjoOyJX7OL2p3GzAR9AJeNaxTV4/

名前制約の一例

- ANSSI(フランス政府認証局)
  - フランス管轄下のccTLDのみ(.fr, .gp, .gf, .mq, etc.)に限定
- Kamu SM(トルコ政府認証局)
  - トルコのccTLDの一部に限定
- Technical Constrained CAはWebTrust for BRの監査要件が一部緩和される

Short-Lived Certificate

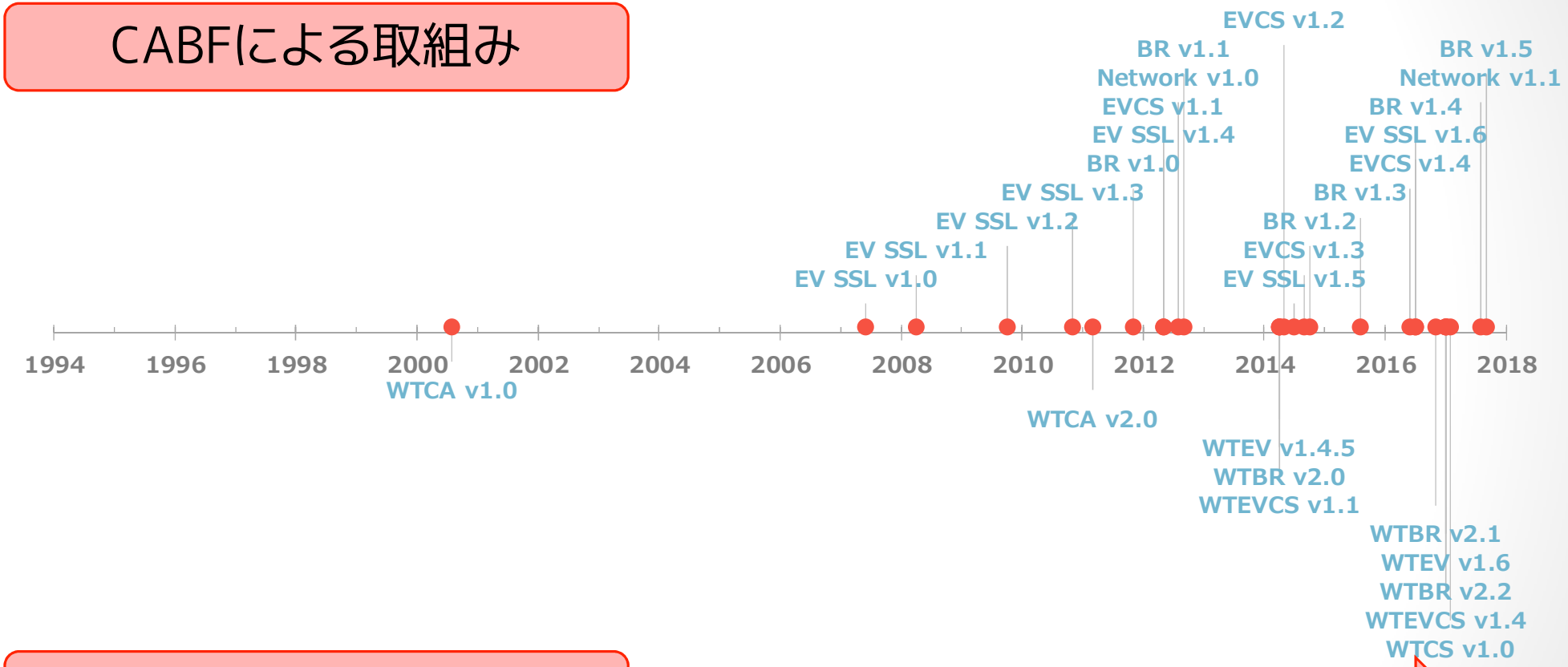
- 証明書の有効期間を短期間化することで失効メカニズムを不要とするなどしてリスクを縮減するアプローチ
  - Let's Encryptは控えめに90日とした
  - Grid Computing分野では約10日間の運用事例あり[1]
- CABFでの議論 (Ballot 140, 153)
  - 有効期間96h(4日間！)を発行可とする動議→却下された
  - あくまでもオプショナルという位置づけ(強制ではない)
- IETFでの議論 (draft-ietf-acme-star [2])
  - Short-Term, Automatically-Renewed (STAR)
  - Short-termについても若干議論あり
    - 1～2週間程度 vs. 24～72h程度

ブラウザベンダは4/5が賛成
CAベンダの賛同はわずか4/21

[1] https://gridka-school.scc.kit.edu/2011/downloads/AAI_SLCS_20110909_Andres_Aeschlimann.pdf
[2] https://tools.ietf.org/html/draft-ietf-acme-star

運用的取組み

CABFによる取組み



WebTrustによる取組み

CA安全神話の崩壊

CABFによる取組み

- EV SSL Guideline (2007～)
  - EV SSL証明書のガイドライン (法人組織の確認規準)
- Baseline Requirements (BR) (2011～)
  - WebTrust for CAの技術曖昧性を解消
  - DV/OV/EV認証局すべてを対象とする規準
- Network Security (2012～)
  - DigiNotar事件を受けて不正侵入対策などを規定

WebTrustによる取組み

- WebTrust for CA 2.0 (2011)
  - すべてのパブリック証明書を発行する認証局の認定規準
  - Baseline Requirementsに合わせて11年ぶりに改訂
- WebTrust for EV (2014～)
  - EV証明書を発行する認証局の認定規準
- WebTrust for BR (2014)
  - BR + Network Securityにもとづく認定規準
- WebTrust for CS/EVCS (2017～)
  - コード署名証明書を発行する認証局の認定規準

HTTPS Telemetry

古典的Telemetry

- マーケットリサーチ分野
  - ~~NetCraft、~~SecuritySpace[1]、W3Techs[2]など
- Alexa上位サイトを中心とした分析
  - 一般的なトレンドを知るには十分
- SSL Observatory[3]
  - 世界でおそらく初めて全IPv4空間のHTTTPSノードを調査した
  - 調査に2～3カ月を要した

[1] http://www.securityspace.com/s_survey/sdata/201710/certca.html
[2] https://w3techs.com/technologies/overview/ssl_certificate/all
[3] Eckersley, Peter, and Jesse Burns. "An observatory for the SSLiverse." *Talk at Defcon* 18 (2010).

SSL Pulse

- TLSサーバの定点観測サイト
  - https://www.ssllabs.com/ssl-pulse/
  - Qualys社SSL Labsが提供
- **Alexa上位の15万件**のHTTPSサイトを、2012年4月から毎月定点観測している
  - Let's Encryptの影響はあまり見られない
  - 過去の月次スナップショットも取得できる
- 証明書以外にもHSTSやCAAレコードなど関連技術の普及状況、TLS関連の主要な脆弱性対応状況を調査している
  - Heartbleed, CCS Injectionなど

ZMapとCTモニタの登場

- ZMap (2013) [1]
  - ミシガン大学が開発した超高速インターネットスキャナ
  - 45分間で全IPv4空間をスキャン可能(ただしミシガン大並の環境が必要)
  - 定期的な観測の頻度を向上させただけでなく、インシデントなどでスナップショットをとることが可能に
  - 従来の大手Webサイトの観測による標本調査から全数調査へ
    - 中小Webサイトの状況を正確に把握できるようになった
- CTモニタ (2015～)
  - 現在の証明書のCT対応率は約96.8%(Censys調べ)
    - CT非対応証明書は2.35M枚 (EVも何故か44K枚ある)
  - Chrome特有の要件
    - 2015年以降、全EV証明書のログ提供が必須化
    - 2018年4月以降、OV/DVを含む全証明書のログ提供が必須化
  - CTログにより外部から観測困難な情報も取得可能になった

EVは93.2%

ZMapとCTモニタの登場によって
世界規模の証明書データセットが構築された

[1] Durumeric, Zakir, Eric Wustrow, and J. Alex Halderman. "ZMap: Fast Internet-wide Scanning and Its Security Applications." *USENIX Security Symposium*. Vol. 8. 2013.

ZMap Project (https://zmap.io/)

censys (https://censys.io)

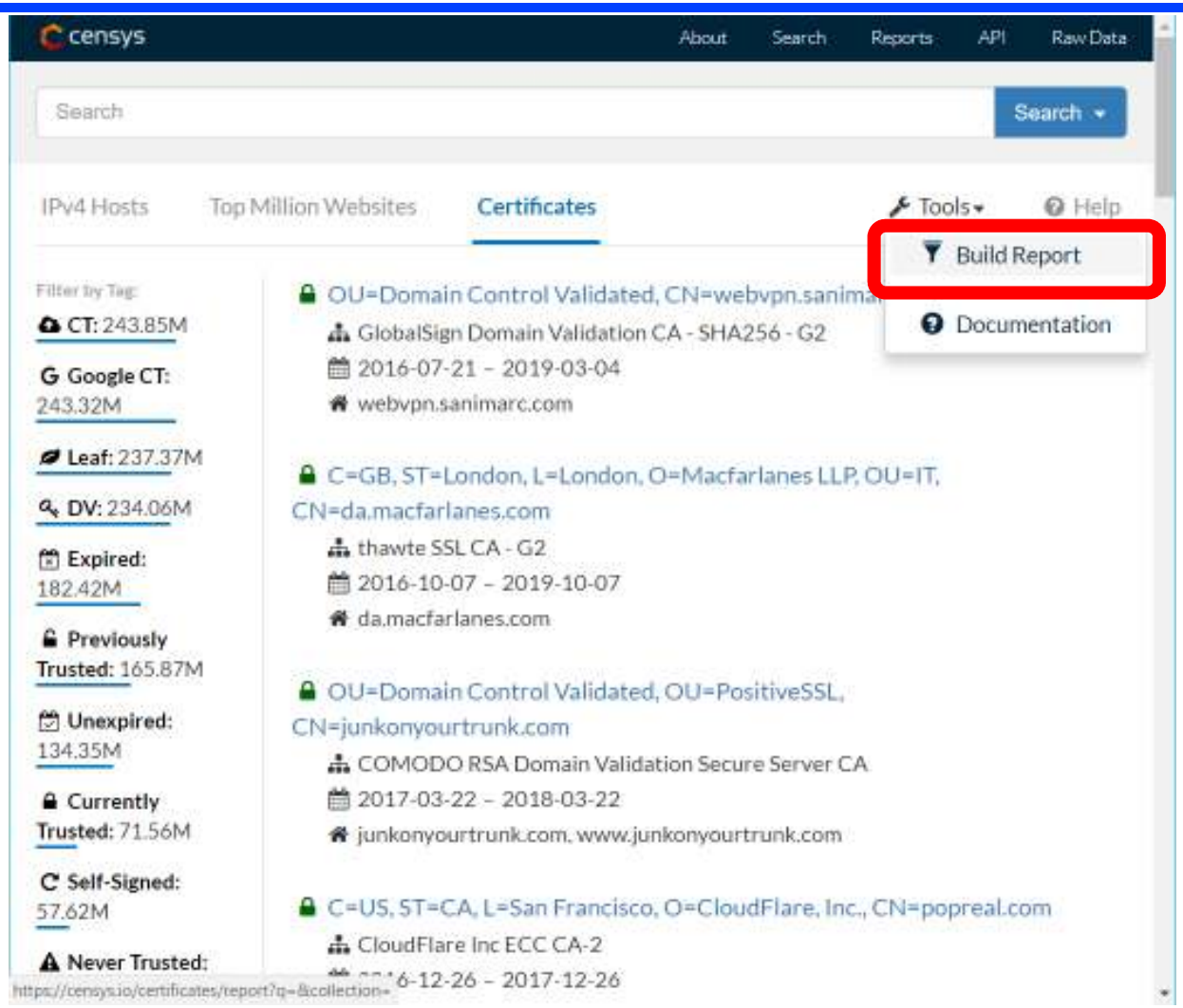
- ZMapが定期的に収集するインターネットデータセットの検索ポータルとして2015年から公開[1]
  - 定期的にIPv4空間をスキャン、データセットを収集している
  - 検索性能、使い勝手ともに飽くことなく進化中でオススメ
  - 2017年12月から有償化の予定
    - 商利用可、学術用途の無償提供は継続
- データセットの種類
  - IPv4 Hosts (110Mノード)
  - Websites (970K件)
  - Certificates (244M件)
    - CTログサーバとも連携して大規模化の一途

[1] Durumeric, Zakir, et al. "A search engine backed by Internet-wide scanning." *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2015.

Censysで証明書データセットを検索

絞り込み

クロス分析も可能



検索例

parsed.issuer.organization.raw: “Let’s Encrypt” AND paypal.com
(Let’s Encryptから発行された”paypal.com”を含む証明書)

Let’s Encryptから発行されたものは全6,980枚
現在も有効なものは1,010枚

crt.sh (http://crt.sh/)

- COMODOが提供するCTモニタ
  - CTログ検索エンジン
  - APIやAtomフィードも提供
- 各種準拠性チェッカが充実
  - cablint, x509lint, zlint
  - Mozilla CA Certificate Disclosures

cablint (1-week Summary)

crt.sh CA/B Forum lint: Summary

Group by "Issuer O"

For certificates with notBefore >= 2017-10-31:

Issuer O	Issuer CN, OU or O	# Certs Issued	FATAL # Certs	FATAL %	ERROR # Certs	ERROR %	WARNING # Certs	WARNING %	ALL # Certs	ALL %
AC Camerfirma S.A.	Camerfirma AAPP II - 2014	1	0	0	0	0	0	0	0	0
AC Camerfirma S.A.	Camerfirma Corporate Server II - 2015	36	0	0	0	0	3	8.33	3	8.33
ACCV	ACCVCA-120	3	0	0	1	33.33	0	0	1	33.33
Actalis S.p.A./03358520967	Actalis Authentication CA G3	1	0	0	0	0	0	0	0	0
Actalis S.p.A./03358520967	Actalis Domain Validation Server CA G1	621	0	0	0	0	0	0	0	0
Aetna Inc	Aetna Inc. Secure CA2	1	0	0	0	0	0	0	0	0
AffirmTrust	AffirmTrust Certificate Authority - OV1	15	0	0	0	0	0	0	0	0
AffirmTrust	AffirmTrust Extended Validation CA - EV1	75	0	0	0	0	0	0	0	0
AlphaSSL	AlphaSSL CA - G2	1	0	0	1	100	0	0	1	100
Amazon	Amazon	2616	0	0	0	0	0	0	0	0
Beame.io Ltd	Beame.io CA 1	1	0	0	0	0	0	0	0	0
Buypass AS-983163327	Buypass Class 2 CA 2	8	0	0	0	0	0	0	0	0
Buypass AS-983163327	Buypass Class 3 CA 2	14	0	0	0	0	0	0	0	0
CertCenter AG	AlwaysOnSSL CA - G1	141	0	0	0	0	0	0	0	0
Certplus	KEYNECTIS Extended Validation CA	1	0	0	0	0	1	100	1	100
Česká pošta, s.p. [IČ 47114983]	PostSignum Public CA 3	2	0	0	1	50	2	100	2	100
China Financial Certification Authority	CFCA DV OCA	2	0	0	0	0	2	100	2	100
Chunghwa Telecom Co., Ltd.	Public Certification Authority - G2	22	0	0	0	0	0	0	0	0
CloudFlare, Inc.	CloudFlare Inc Compatibility CA-3	8042	0	0	6782	84.33	0	0	6773	84.22
CloudFlare, Inc.	CloudFlare Inc ECC CA-2	8033	0	0	0	0	0	0	0	0
CloudFlare, Inc.	CloudFlare Inc RSA CA-1	8026	0	0	0	0	0	0	0	0
COMODO CA Limited	COMODO Domain Validation Legacy Server CA 2	2885	0	0	2490	86.31	0	0	2484	86.10
COMODO CA Limited	COMODO ECC Domain Validation Secure Server CA	30	0	0	0	0	0	0	0	0
COMODO CA Limited	COMODO ECC Domain Validation Secure Server CA 2	266034	0	0	0	0	0	0	0	0
cPanel, Inc.	cPanel, Inc. Certification Authority	165080	0	0	0	0	0	0	0	0
CrossCert	CrossCert Class 2 Server CA - V2	6	0	0	4	66.67	4	66.67	4	66.67
CrossTrust	CrossTrust DV CA3	1	0	0	0	0	1	100	1	100
CrossTrust	CrossTrust OV CA3	1	0	0	0	0	2	200	2	200
Cybertrust Japan Co., Ltd.	Cybertrust Japan EV CA G2	208	0	0	0	0	0	0	0	0
Cybertrust Japan Co., Ltd.	Cybertrust Japan Extended Validation Server CA	11	0	0	0	0	0	0	0	0
Cybertrust Japan Co., Ltd.	Cybertrust Japan Public CA G3	335	0	0	0	0	0	0	0	0
Cybertrust Japan Co., Ltd.	Cybertrust Japan Secure Server CA	33	0	0	0	0	0	0	0	0
DarkMatter LLC	DarkMatter Secure CA	4	0	0	0	0	0	0	0	0

規準から逸脱した証明書を
各CAが何件発行しているか

cablint (Issues)


crt.sh CA/B Forum lint: Issues

For certificates with notBefore >= 2017-10-31:

Severity	Issue	# Affected Certs
ERROR	BR certificates must have subject alternative names extension	1
ERROR	BR certificates must include an HTTP URL of the OCSP responder	4
ERROR	BR certificates must include certificatePolicies	1
ERROR	BR certificates must not contain directoryName type alternative name	1
ERROR	BR certificates must not contain rfc822Name type alternative name	1
ERROR	BR certificates with CRL Distribution Point must include HTTP URL	5
ERROR	BR certificates with organizationName must include either localityName or stateOrProvinceName	84
ERROR	commonNames in BR certificates must be from SAN entries	1
ERROR	Constraint failure in X520countryName: ASN.1 constraint check failed: X520countryName: constraint failed (X520countryName.c:57)	3
ERROR	Constraint failure in X520OrganizationName: ASN.1 constraint check failed: UTF8String: constraint failed (X520OrganizationName.c:174)	3
ERROR	Constraint failure in X520SerialNumber: ASN.1 constraint check failed: X520SerialNumber: constraint failed (X520SerialNumber.c:57)	5
ERROR	DNSName is not FQDN	287
ERROR	EV certificates must include localityName in subject	1
ERROR	Invalid country in jurisdictionCountryName	3
ERROR	SHA-1 not allowed for signing certificates	9477
ERROR	Unallowed key usage for RSA public key (Key Agreement)	13
WARNING	BR certificates should include an HTTP URL of the issuing CA's certificate	274
WARNING	CA certificates should not include subject alternative names	1
WARNING	Certificate does not include authorityInformationAccess. BRs require OCSP stapling for this certificate	1
WARNING	Certificate Policies should not contain notice references	634
WARNING	commonNames in BR certificate contains U-labels	842
WARNING	Deprecated Netscape extension 2.16.840.1.113730.1.1 located as critical extension	656
WARNING	TLS Server auth certificates should not contain IPSec End System usage	1
WARNING	TLS Server auth certificates should not contain IPSec Tunnel usage	1
WARNING	TLS Server auth certificates should not contain IPSec User usage	1
WARNING	Trailing whitespace in organizationName	1
WARNING	Underscore should not appear in DNS names	29
WARNING	Unicode organizationalUnitName is using deprecated BMPString	1
WARNING	Unicode organizationName is using deprecated BMPString	3
WARNING	Unknown Extension: 2.23.140.1.31	7

規準から逸脱した証明書の
種類と枚数

Mozilla CA Certificate Disclosures

crt.sh **Mozilla CA Certificate Disclosures**

Generated at 2017-11-07 01:13:02 UTC

Category	Disclosure Required?	# of CA certs
Disclosure Incomplete	**Yes!**	2 + 7 Summary
Unconstrained Trust	**Yes!**	3 + 246 Summary
Unconstrained, but all unexpired observed paths Revoked	Unknown	333
Unconstrained, but zero unexpired observed paths	Unknown	1484
Expired	No	4112
Technically Constrained (Trusted)	Maybe soon?	63
Technically Constrained (Other)	No	55
Disclosed as Revoked, but Expired	Already disclosed	47
Disclosed as Revoked and in OneCRL	Already disclosed	346
Disclosed as Revoked (but not in OneCRL)	Already disclosed	30
Disclosed as Parent Revoked (so not in OneCRL)	Already disclosed	89
Disclosed	Already disclosed	2816
Unknown to crt.sh or Incorrectly Encoded	Already disclosed	19

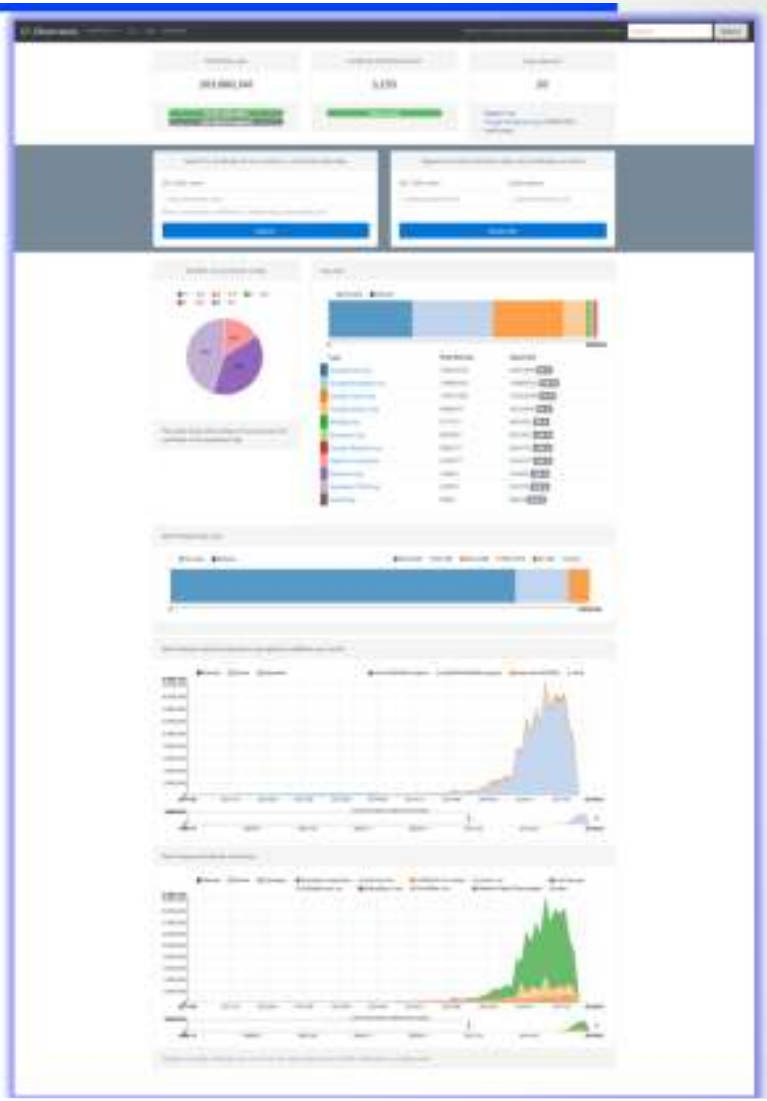
Mozilla Root Certificate Policyと
整合しない認証局証明書
(ただちに違反なわけではない)

ct-observatory

https://www.ct-observatory.org/

- ボン大学のUSECAPグループが2016年5月に立ち上げ
- 言わば”*CTダッシュボード*”
  - 扱う情報はcrt.shとほぼ同等
  - 可視化に注力
- 理想的なCTモニタ
  - 指定したFQDNのCTログが投稿されるとアラートを送信してくれる

第三者が勝手に個別監視できることに対するもやもや感もあり



HTTPS Telemetryがもたらした変化

- 新たなデータセットの誕生
  →OTの加速
  - 証明書のリスクや課題を、定量的･多面的に
    分析･検証できるようになった

- 認証局のPDCAサイクルが実質的に短縮化
  - CTモニタによって異常･不正の検知サイクルが短期化
  - 一方でブラウザベンダによる審査は長期化
  - 機械的な検知ルールによるセキュリティ疲れ??

Let’s Encrypt (LE)

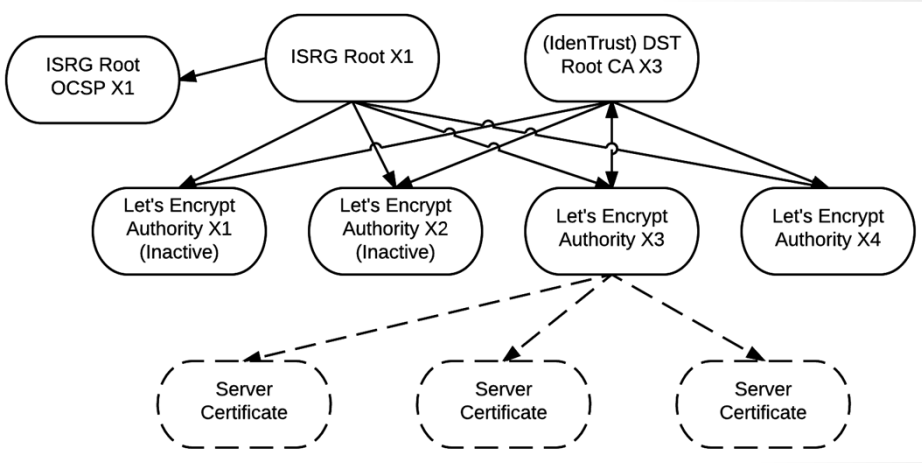
Let's Encrypt (https://letsencrypt.org)

- Internet Security Research Groupが2015年10月に開始した証明書無償発行サービス
  - Technical Advisory Boardには有名どころが大勢
  - Mozilla, Akamai, Cisco, EFF, Chrome, OVHなどが出資
- 証明書を自動発行・更新するACMEプロトコルを策定中
  - draft-ietf-acme-acme-08
  - DV証明書のみがスコープ
  - HTTP/JSONベースのプロトコル、署名フォーマットはJWS
  - CertbotなどOSS実装多数あり
- 統計値など
  - 有効証明書枚数：約60M枚
  - 有効ドメイン数：約20M件
  - のべ発行枚数：約165M枚(約2年間)

現在のCTログにある証明書枚数がのべ250M枚…

証明書と証明書チェーン

- 証明書プロファイル
  - 有効期間は90日間
  - サーバ証明書はECDSAでもOK
    - ECDSAルートは2018年3月予定
  - CT、CAAレコード、IDNに対応済
  - ワイルドカード証明書は2018年1月予定
- 証明書チェーン
  - 独自ルートCA(ISRG Root X1)を運用しつつIdenTrustからもクロスルート
  - Mozilla, Appleには独自ルートを搭載
  - MicrosoftはIdenTrustからのクロスルートで対応

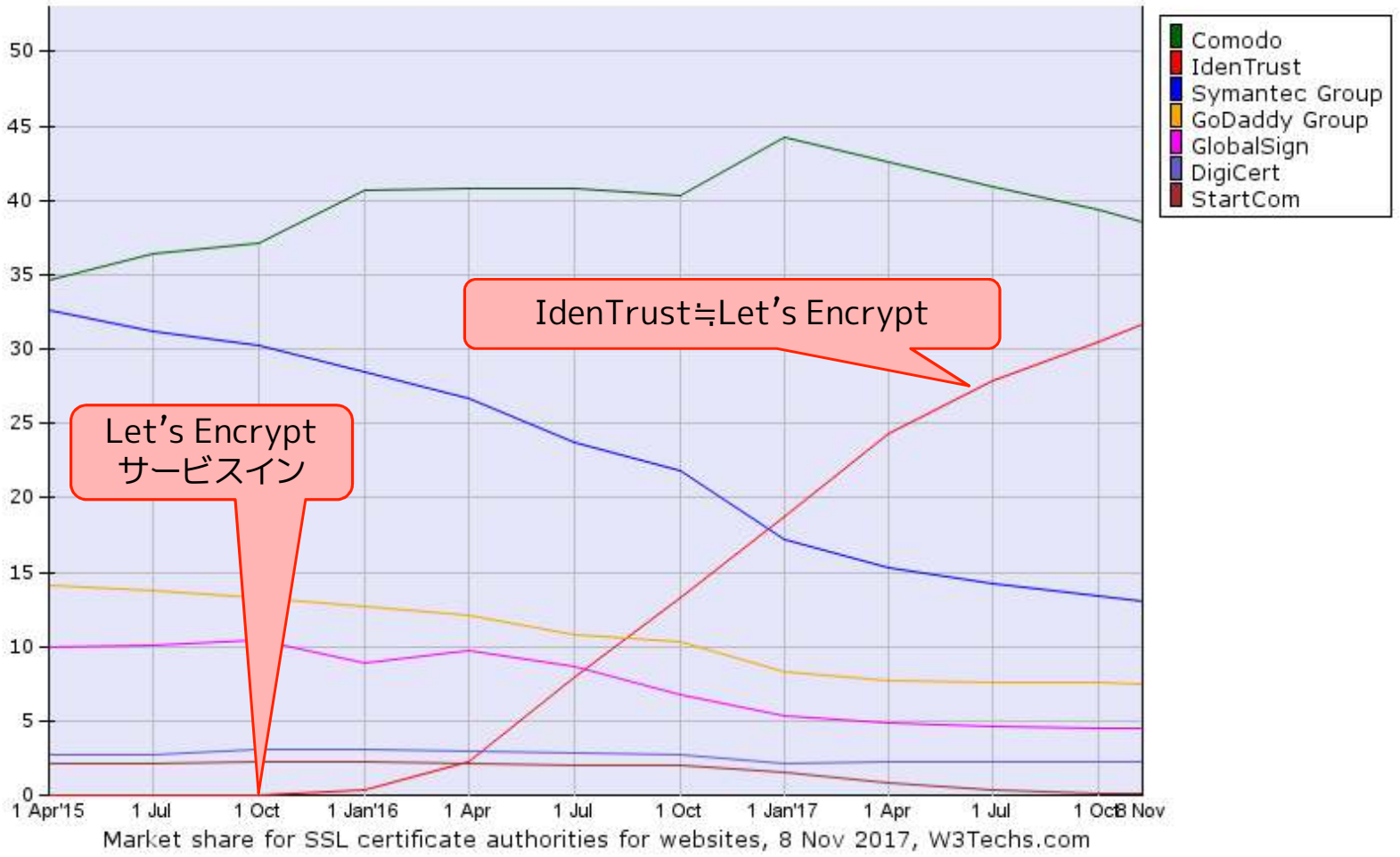


出典：https://letsencrypt.org/certificates/

Let’s Encryptの成長ぶり？

出典：https://ct.tacticalsecret.com/

マーケットシェアへの影響



出典：https://w3techs.com/technologies/history_overview/ssl_certificate/ms/q

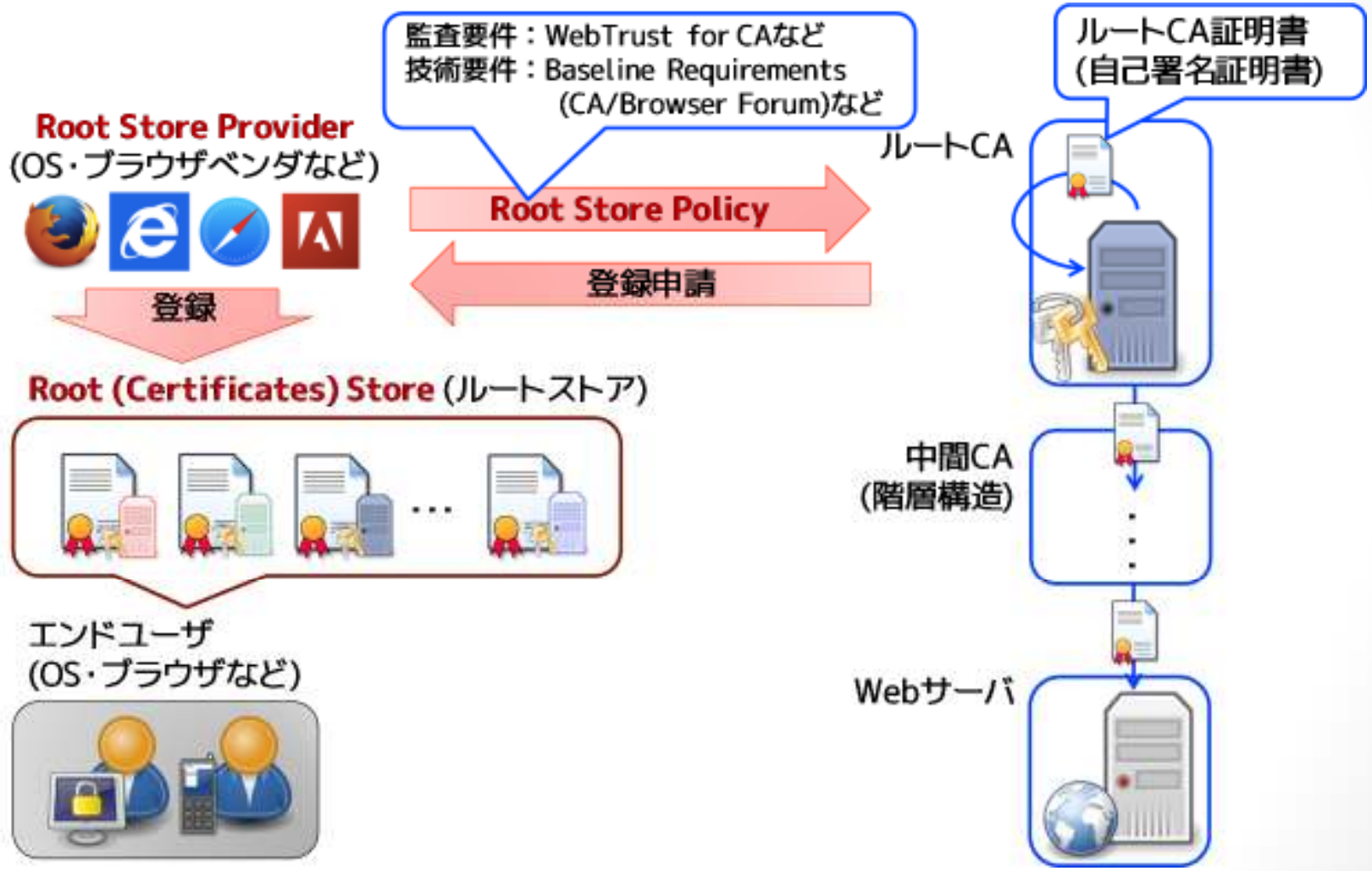
LEの功罪

- 証明書の無償化と普及
  - DVのホワイトナイトとしての期待
- 証明書管理の自動化・OTの加速
  - ACMEによるOTの徹底→他CA事業者へのプレッシャー
- 証明書有効期間の短縮→証明書アジリティの改善
  - 自動発行・更新により、有効期間を意識しなくてよくなった(24カ月→3カ月)

- フィッシングサイトのTLS化
  - ACMEプロトコルに則っている限りは機械的に発行される
  - Human-readabilityのないドメイン名 (Machine Generated Domain Name)
- CTへの負担？
  - CTログの約2/3がLet's Encrypt (164M/248M件)

Root Store Providerの迷走？苦闘？

Web PKIのトラストモデル



トラストアンカーとしてのブラウザベンダ

- 形式上のトラストアンカーはルートCAだが…
- ルートCAを入れる審査をするのはブラウザベンダ
  - 実質的なトラストアンカと言える
- ブラウザベンダ>>ルートCA
  - ルートCAは証明書の信頼の基点になる強い存在だが、そのルートCAに対して更に強い権限を持っているのは実はブラウザベンダである

CABFにおけるパワーバランス

- 可決票数に関する規定 (In section 2.3 (f), Bylaws, v.1.7)
  - 認証局事業者(50)の2/3以上 (最大：50 * 2/3 ≒ 34)
    および
  - ブラウザベンダ(6)の過半数 (最大：6 * ½ + 1 = 4)

- 事例：Adopt Code Signing BRs (Ballot158)
  - コード署名用ガイドライン策定の動議
  - 認証局事業者 賛成17, 反対1, 棄権3 (94%支持)
  - ブラウザベンダ 賛成2, 反対3 (40%支持)
    - 賛成：Microsoft, Qihoo360
    - 反対：Google, Mozilla, Opera

- ブラウザベンダ3社が反対に回ると絶対に可決されない
  - OSベンダとブラウザベンダでも微妙に立ち位置が変わる

Chromeグリーンバー問題

- Chrome53→55 (2016/08/21～12/01)
  - ChromeのCT検証機能の不具合によりSymantecの一部のEV証明書が正しくグリーンバー表示されなくなる
  - GoogleからSymantecへ再三の是正勧告を行っていた最中でのGoogle側の粗相…
- Chrome57→58(2017/03/09～05/18)
  - ChromeのEV証明書判定機能の不具合により、Symantecの一部のEV証明書が正しくグリーンバー表示されなくなる
  - GoogleによるSymantecへの制裁措置が騒がれた直後だけに色々な憶測が飛び交った

Microsoft “Reinforce trust”事件 (2015/12/17)

- 同社Root Policy改訂(2015年6月)に合わせてルートCAの審査見直しを行い、2016年1月から複数のルートCAを無効化するとのアナウンス[1]
- ダメだった点：
  - 無効化予定とされたルートCAの件数は二転三転し、関係者は翻弄されることに。
    - 当初20件→14件に修正→最終的には6件[2]
  - 公式チャネル[3] より先に別筋のブログ[4]で公表された
    - [3] Microsoft Trusted Root Certificate Program Updates
    - [4] Microsoft Malware Protection Center (現Windows Security blog)
- 原因：Microsoft担当者とCA事業者側のコミュニケーションミス・不足

[1]https://web.archive.org/web/20151218085547/https:/blogs.technet.microsoft.com/mmpc/2015/12/17/microsoft-updates-trusted-root-certificate-program-to-reinforce-trust-in-the-internet/
[2] http://aka.ms/rootupdates#JAN16_B
[3] http://aka.ms/rootupdates
[4] https://blogs.technet.microsoft.com/mmpc/2015/12/17/microsoft-updates-trusted-root-certificate-program-to-reinforce-trust-in-the-internet/
[5] http://aka.ms/rootupdates#JAN16_C

One more incident for Symantec [5]
Root Updatesでは、一部のSymantecルートについてEKUメタ情報が誤編集され、一時的に同ルートが検証できなくなるというインシデントもあった(2016/01/20～28)

CNNICの無効化

- 2015年3月、CNNICの下位CAであるMCS HoldingsがGoogleの所有ドメインに不正に証明書を発行していたことが発覚
  - CNNIC曰く、MCSは特定のドメインにしか発行できない契約だった
  - 下位CAであるMCSの私有鍵は、HSMで管理されていないどころかMITMプロキシに格納されていた
  - 組織のF/Wなどに配備されることで中間者攻撃が可能に
- 2015年3月、MCS Holdingsを各ブラウザが失効
- CNNIC自体も塩漬け状態に
  - CNNICが過去に発行した証明書は検証可能
  - 以降に発行する証明書は検証できなくなる

WoSign/SmartComの無効化

- 期限を越えたSHA-1証明書の発行(2015/01～03)
  - BRによるとSHA-1証明書の有効期間は2016年末までとすべき(SHOULD NOT)
- 証明書の二重発行(2015/03～04)
  - シリアル番号の重複
- 規定外の公開鍵暗号アルゴリズムの使用(SM2)
- StartComの買収(2015/11)
- SHA-1証明書のバックデート発行
- 証明書自動発行サービスの脆弱性

- Mozilla, Google, Apple, Microsoftが相次いで両ルートを失効

Symantec問題(1)これまでの流れ

- SymantecはこれまでGoogleやMozillaから再三にわたり証明書誤発行・規準違反などの指摘を受けてきた[1]-[4]
  - 不正なテスト証明書発行(O=TESTやgoogle所有ドメインなど)
  - 期限超過のSHA-1証明書発行　など
- 2017年3月、Googleは改善の見込みがないと判断し、Chromeにおいて同社のルートCAを段階的に無効化していくことを提案[5]
- 2017年8月、SymantecはPKI事業をDigiCertに売却することを発表[6]
- 2017年9月、ChromeにおけるSymantecルートの段階的な無効化計画を発表[7][8]

Symantec問題(2) ロードマップ

- 新インフラ：
  - DigiCertが新設する、Symantecの既存PKIサービスを収容するためのManaged Partner Infrastructure[9]
  - Chrome70以降でも引き続き利用可能な証明書を発行できる
  - 証明書有効期間は13カ月に制限される(他CAは39カ月)
- 旧インフラ：
  - Symantecの既存PKIサービス: Thawte, VeriSign, Equifax, GeoTrust, RapidSSL
  - Chrome70以降では信頼されなくなる
- 2017.12.01
  - GoogleとSymantecの合意にもとづき、この期日までに新インフラを利用可能にしなければならない
  - Symantecによれば実際の移行開始は2018年の予定[10]
- 2018.03.15 Chrome 66ベータ公開→04.17 同安定版公開
  - 旧インフラで2016-06-01より前に発行された証明書は無効となる
- 2018.09.13 Chrome70ベータ公開→10.23 同安定版公開
  - 旧インフラのすべての証明書が無効となる

ただし2018年3月以降は
他CAも825日未満に制限

Symantec問題(3)参考URL

[1] CA:Symantec Issues, https://wiki.mozilla.org/CA:Symantec_Issues

[2] Sustaining Digital Certificate Security (2015-10-28), https://security.googleblog.com/2015/10/sustaining-digital-certificate-security.html

[3] Improved Digital Certificate Security (2015-09-18), https://security.googleblog.com/2015/09/improved-digital-certificate-security.html

[4] Misissued/Suspicious Symantec Certificates (2017-01-20), https://groups.google.com/d/msg/mozilla.dev.security.policy/fyJ3EK2YOP8/yvjS5leYCAAJ

[5] Intent to Deprecate and Remove: Trust in existing Symantec-issued Certificates (2017-03-24), https://groups.google.com/a/chromium.org/d/msg/blink-dev/eUAKwjihhBs/rpxMXjZHCQAJ

[6] DigiCert to Acquire Symantec's Website Security and Related PKI Solutions (2017-08-02), https://www.symantec.com/about/newsroom/press-releases/2017/symantec_0802_01

[7] Chrome's Plan to Distrust Symantec Certificates (2017-09-11), https://security.googleblog.com/2017/09/chromes-plan-to-distrust-symantec.html

[8] Chrome が Symantec の証明書に対する信頼を破棄する予定について (2017-09-28), https://developers-jp.googleblog.com/2017/09/chromes-plan-to-distrust-symantec.html

[9] PUBLIC: Symantec Managed Partner Infrastructure (2017-07-27), https://docs.google.com/document/d/1Yd079EsKQ-QawTvWgjIfrCV6d0NNlwoS1ftB0MaJkBc/edit#heading=h.48fu6bs40er0

[10] SymantecからDigiCertへの売却にあたってのFAQ, https://www.websecurity.symantec.com/ja/jp/digicert-and-symantec-faq/faqs#a1

オランダ政府への牽制

- オランダで2018年1月から情報セキュリティサービス法が施行される
- Mozillaの開発者は、これによりインターネット監視が合法的に行われるようになることを懸念
- Mozillaのトラストリストからオランダ政府のルート認証局を取り消す提案が行われ、議論が続いている(？)

Root Store Providerの悩み

- 数が膨れ上がった認証局の安全性をどうコントロールするか
  - ルートCAだけで400件超
  - 中間CAまで含めれば5,000件超
  - 質から量への転換
- ブラウザベンダという本業からすればあまりにも重い!?
  - Web以外の責任まで負いたくない (cf. CodeSigning, S/MIME)
- 既にOTを持つブラウザベンダと、
  OTの進みが遅いCA事業者のギャップ (私見)
  - グローバルなCA事業者：代理店を抱えすぎてコントロールが難しい
  - ドメステックなCA事業者：規模が小さくてOTの障壁が高い
  - OTによってCA事業者の淘汰が進むと、
    結果的に量から質への回帰が進む可能性もあり得る??

まとめ

- Web PKIに起きていること
  - CA安全神話の崩壊
  - Pervasive Surveillanceへの懸念
  - 暗号技術に対する攻撃の本格化
- 今のWeb PKIに必要なこと
  - やっぱり暗号化通信は欠かせない
  - 信頼基盤と暗号技術の安全性の回復
- 運用的・技術的取組み
  - Certificate TransparencyとHTTPS Telemetry
  - 定量的・技術的な管理(OT)へのシフト
- ブラウザベンダの迷走と苦闘
  - ルートストアプロバイダとしての責任と焦り
  - OTの適用が難しい？世界とのギャップ
  - CA事業者に対する新しいガバナンスの模索

推薦書籍

- プロフェッショナルSSL/TLS (Bulletproof SSL and TLS)
  - Ivan Ristić 著、齋藤孝道 監訳
  - 紙書籍+電子書籍(PDF)：税込¥5,339
  - 電子書籍(PDF)のみ：税込¥4,860
- SSL Pulseを立ち上げたIvan Ristićの力作
- 紙書籍+電子書籍(PDF)がお買い得
- 暗号技術やプロトコルの解説だけでなく、認証局も含めて過去のインシデントが概観できます
- もちろん典型的な暗号設定の解説もあります
- 大津さんもレビュアーです！