

Certificate Transparencyを知ろう

～証明書の透明性とは何か～

NTTデータ先端技術株式会社

セキュリティ事業部 セキュリティ診断担当

大角 祐介 (おおすみ・ゆうすけ)

Facebook - フェイスブック - ×

→ <https://www.facebook.com>

www.facebook.com
このサイトへの接続はプライベート接続です。
[詳細](#)

権限 接続

Chrome で DigiCert SHA2 High Assurance Server CA がこのウェブサイトの証明書を発行したことを確認しました。証明書の透明性に関する有効な情報がサーバーから提供されました。
[証明書情報](#)

www.facebook.com への接続は新しい暗号スイートにより暗号化されています。

この接続には TLS 1.2 を使用しています。

接続は AES_128_GCM を使用して暗号化および認証されており、ECDHE_ECDSA が鍵交換メカニズムとして使用されています。

[ヘルプ](#)

メールアドレスまたは携帯番号
パスワード

ログインしたままにする

アカウント

級生、

画像 : facebook (<https://www.facebook.com/>) トップページ

生年月日

A row of clear wine glasses is shown on a shelf. The glasses are arranged in a line, with the one in the foreground being the most prominent. The background is slightly blurred, showing more glasses and a warm, golden light. The text "Transparency(透明性)?" is overlaid on the image in a bold, black font with a white outline.

Transparency(透明性)?

- Certificate Transparency (CT), RFC 6962
 - 証明書の透明性とは何か、その仕組み
- CTのメリット、デメリット
- CTで遊ぼう
 - CTを用いた攻撃シナリオを考える
- 最近の動向
 - RFC 6962-bis で何が変わるか
 - CTが役に立った(のか)? Thawte事件
 - Let's encryptの対応状況

- Certificate Transparency (CT), RFC 6962
 - 証明書の透明性とは何か、その仕組みとねらい
- CTのメリット、デメリット
- CTで遊ぼう
 - CTを用いた攻撃シナリオを考える
- 最近の動向
 - RFC 6962-bis で何が変わるか
 - CTが役に立った(のか)? Thawte事件
 - Let's encryptの対応状況



Certificate: 證明書
Transparency: 透明性

<https://www.certificate-transparency.org/>

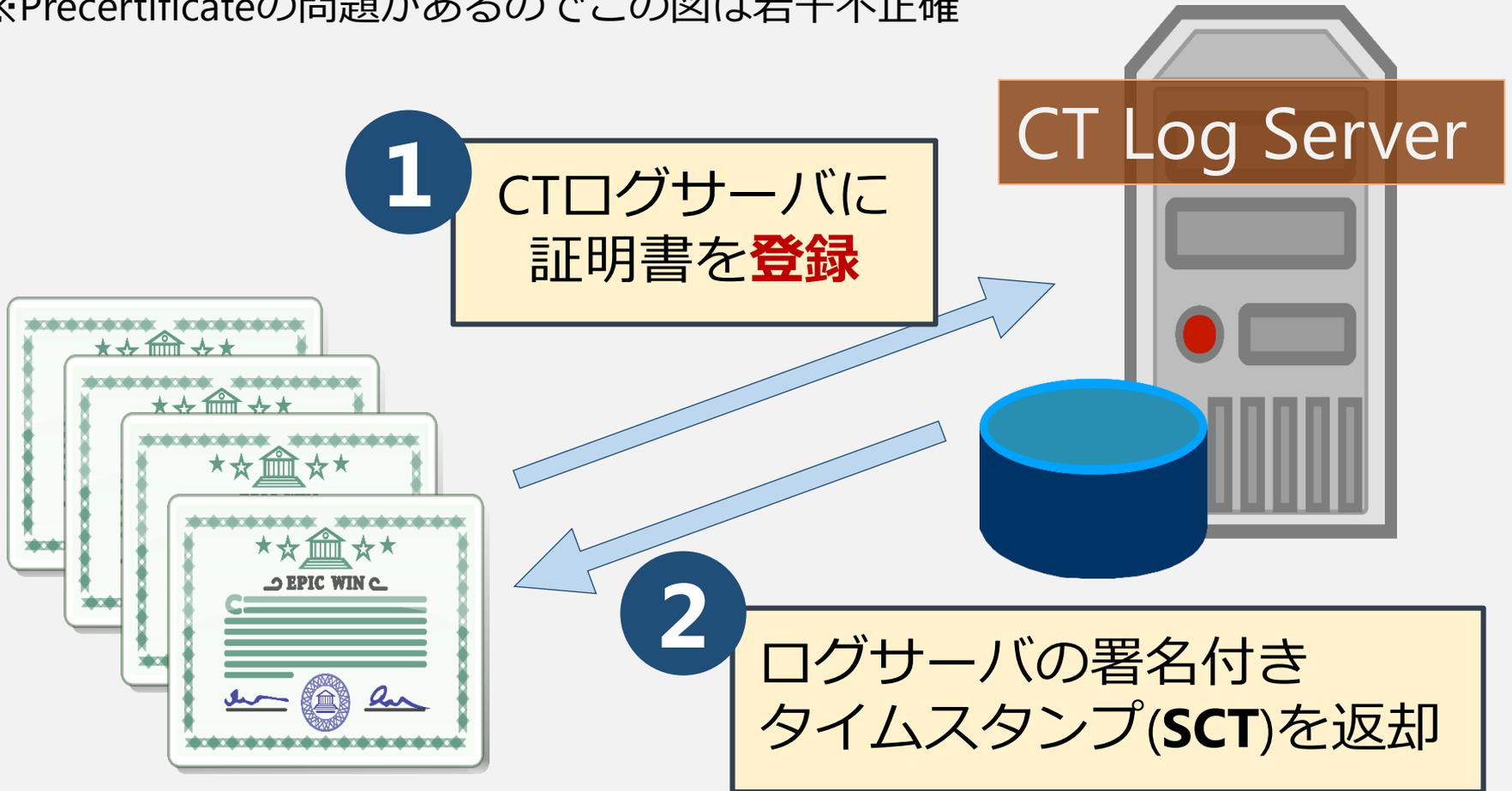
Googleが提唱している、 証明書発行の監視・監査の仕組み

(RFC 6962)

※まだExperimentalなRFC

画像 : Certificate Transparency公式ページ
<https://www.certificate-transparency.org/>

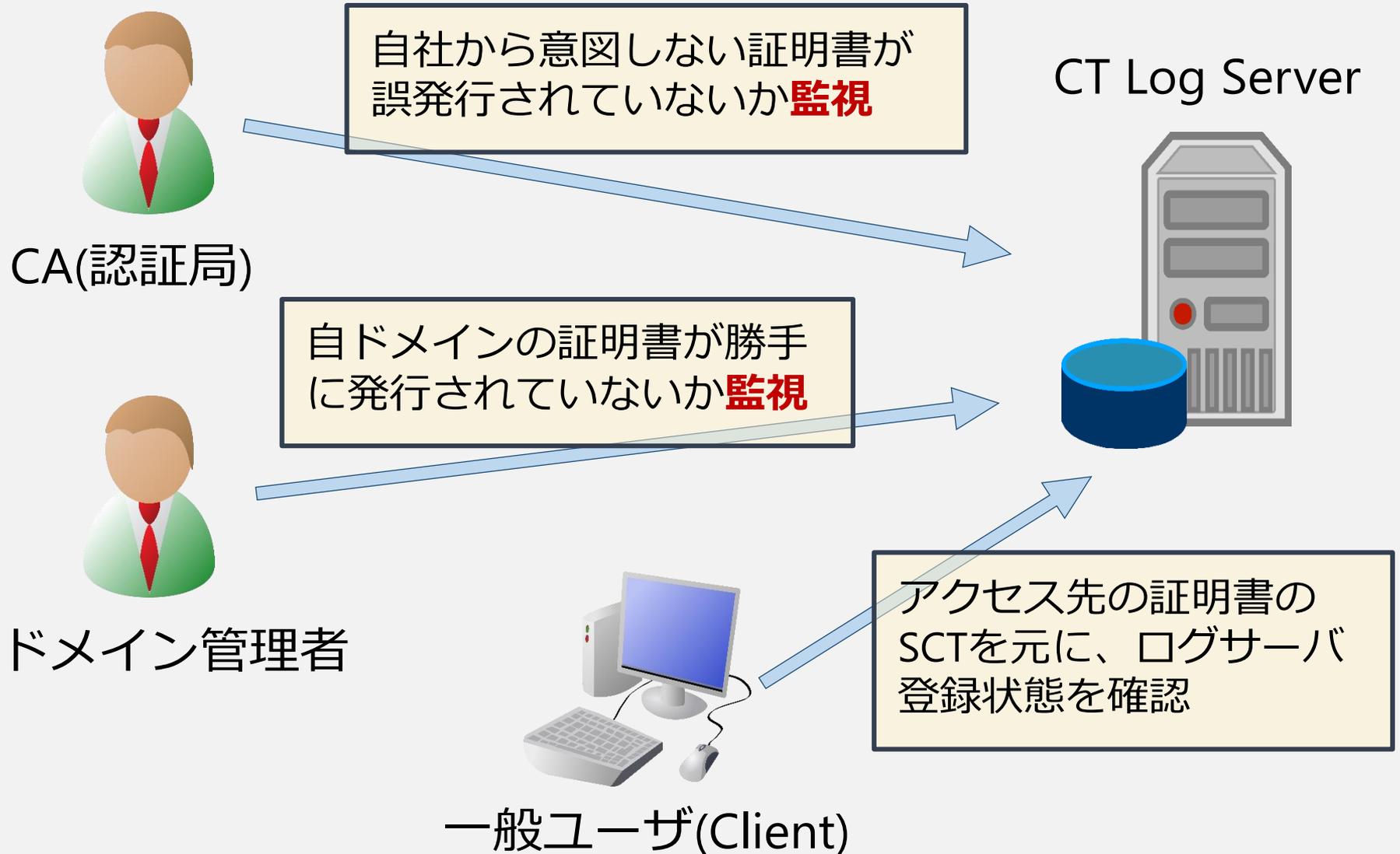
※Precertificateの問題があるのでこの図は若干不正確



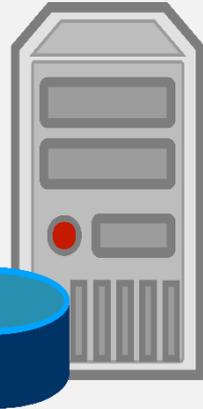
世界中で発行される
証明書(Certificate)

SCT: Signed Certificate Timestamp

CTで何ができるのか → 監視

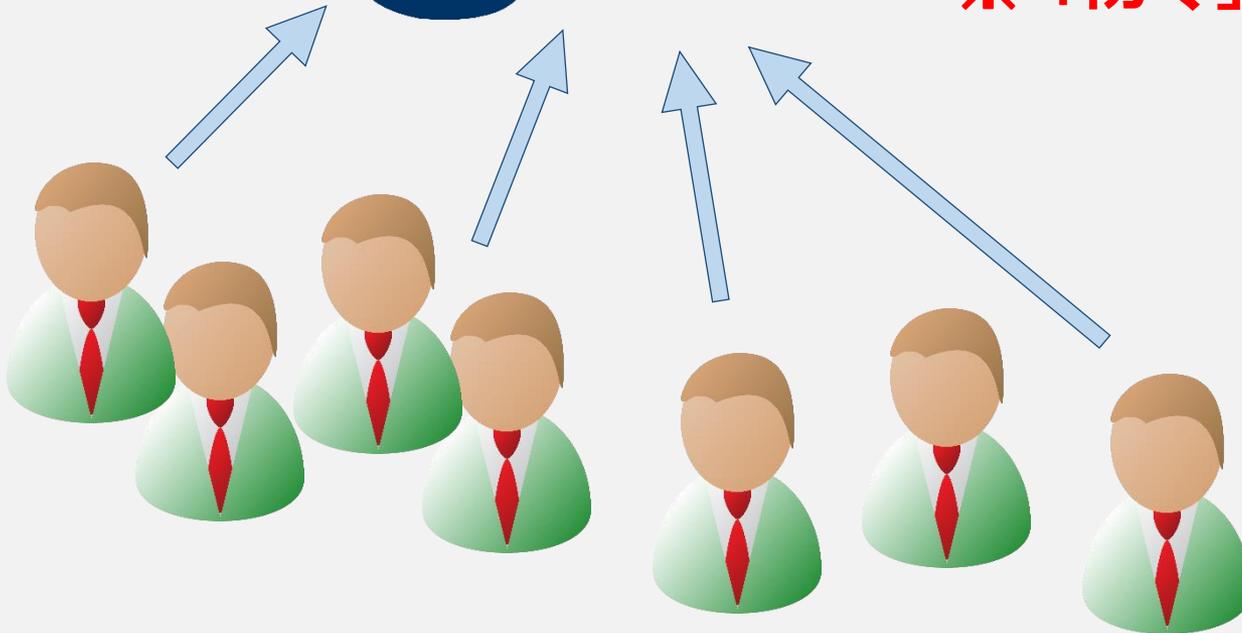


CT Log Server



「みんな」でCTログサーバを
monitorすることで、不正な
証明書発行をいち早く発見したい

※「防ぐ」わけではない



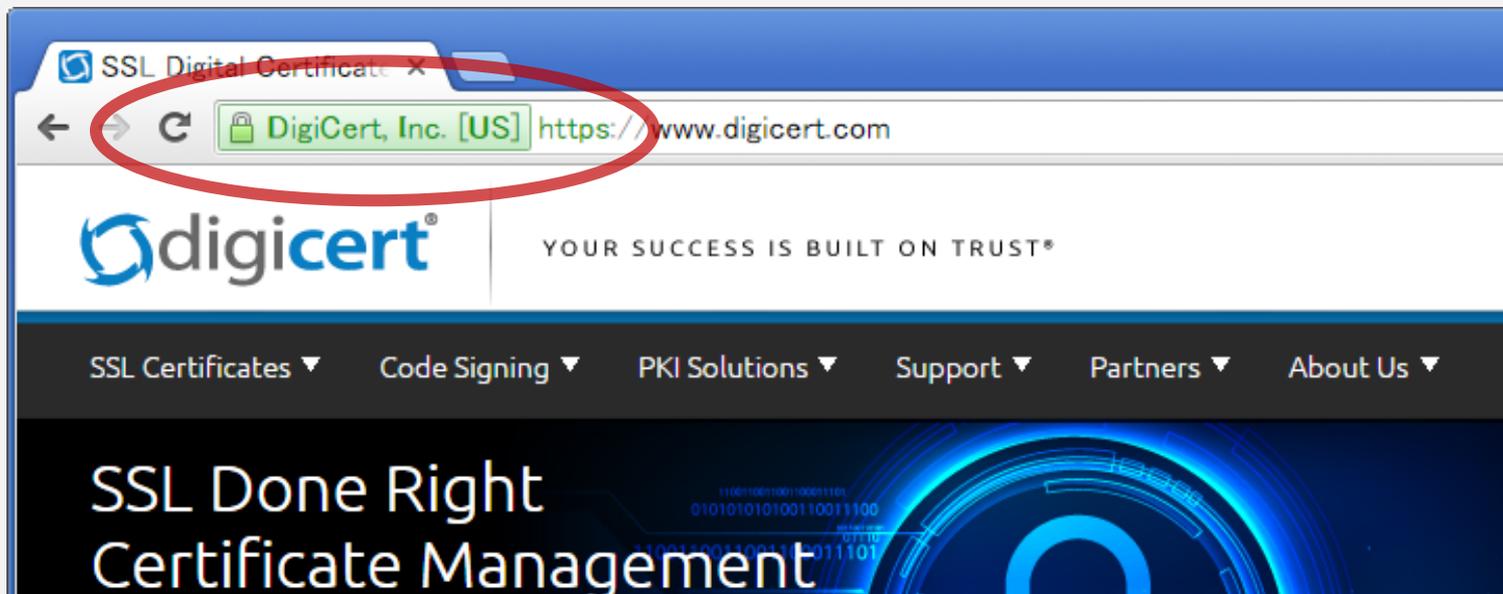
- **[背景]** 認証局による証明書の誤発行事例
 - 2011年：DigiNotarが不正アクセスを受け、攻撃者により不正な証明書が発行
 - 2013年：TURKTRUSTの運用ミスにより、不正証明書が発行可能に
 - 攻撃者は、google.comなど有名ドメインの証明書を真っ先に作りたがる
- **[思惑]** 認証局から発行された不正な証明書を、外部から見つけたい
 - 認証局を無条件に信頼しない
 - [証明書の発行]という行為が**透明(Transparency)**

Google Chromeだけが対応、かつ先走りすぎ

「Google Chromeでは、CTに対応していないEV証明書は、EVインジケータの表示をやめる」と既に宣言。

(EV証明書固有の、緑色表示をしなくなるということ)

Extended Validation in Chrome: <http://www.certificate-transparency.org/ev-ct-plan>

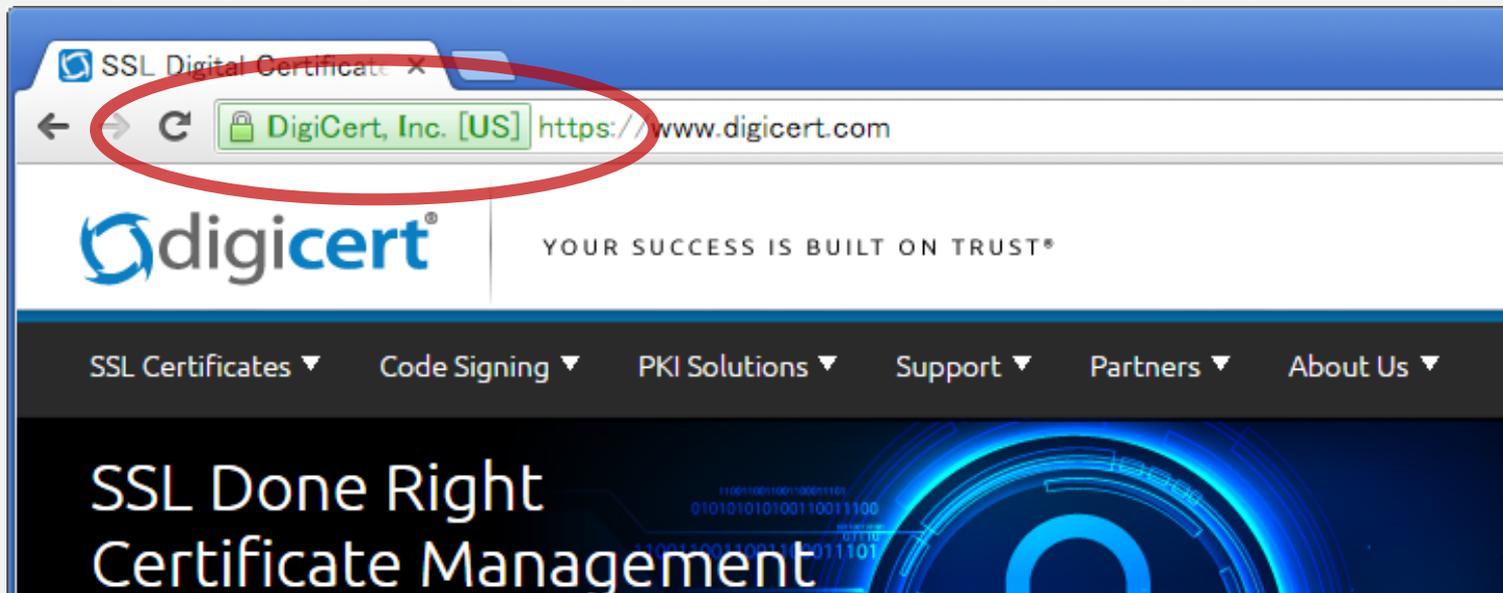


画像 : DigiCert社 (<https://www.digicert.com>) トップページ

Google Chromeだけが対応、かつ先走りすぎ

「Google
タの表示
(EV証明

EV証明書を使う企業の多くは、
「アドレスバーの緑色の表示を確認ください」と
案内するため、Chromeで緑にならない事態を嫌って
EV証明書のCT対応は迅速に進んだ



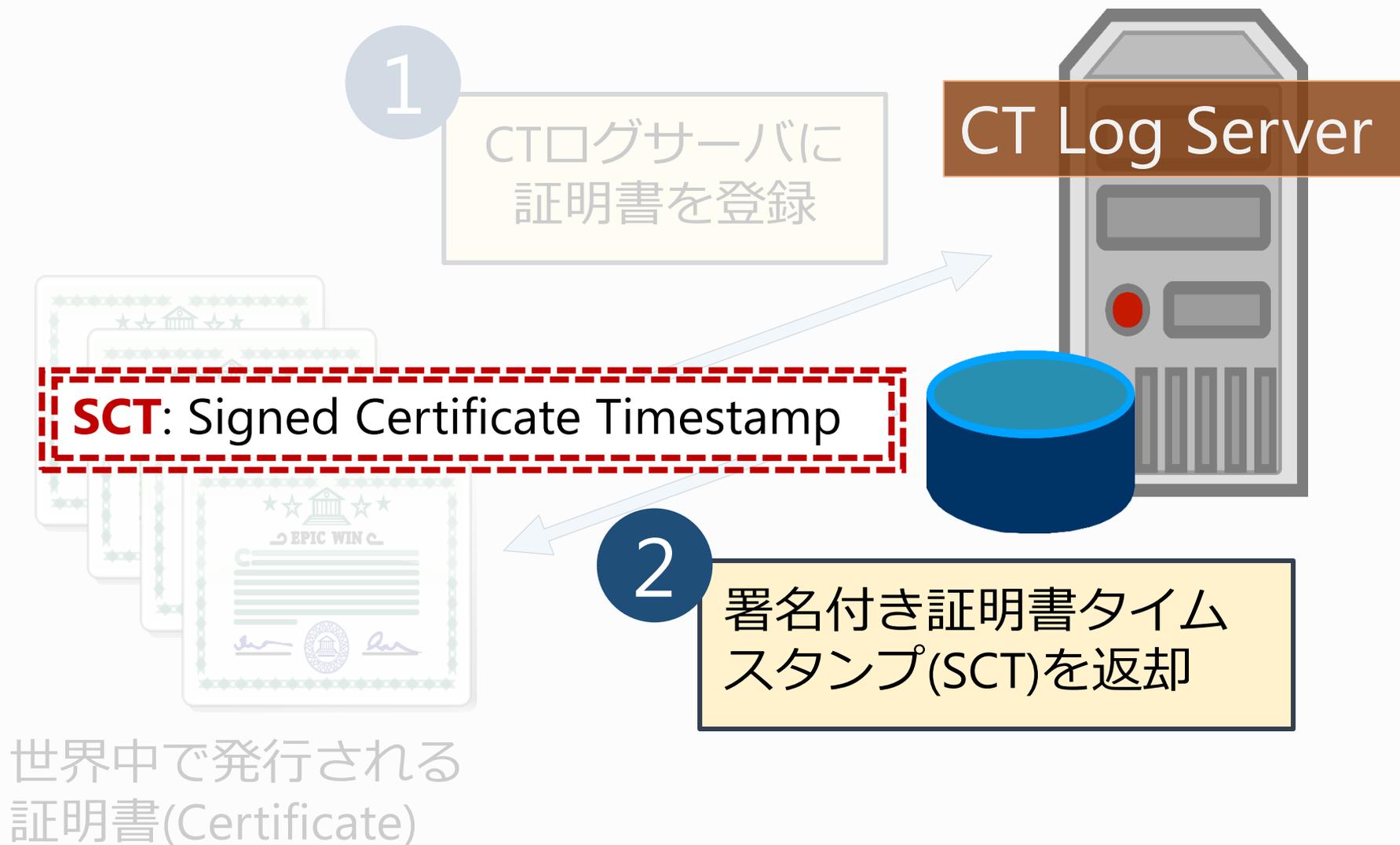
RFC 6962 says:

TLS clients **MUST reject** certificates that do not have a valid SCT for the end-entity certificate.

- 3. Log Format and Operation



CT対応の技術的方法（簡単に）



Facebook - フェイスブック - x

https://www.facebook.com

www.facebook.com
このサイトへの接続はプライベート接続です。
[詳細](#)

権限 接続

Chrome で DigiCert SHA2 High Assurance Server CA がこのウェブサイトの証明書を発行したことを確認しました。証明書の透明性に関する有効な情報がサーバーから提供されました。
[証明書情報](#)

www.facebook.com への接続は新しい暗号スイートにより暗号化されています。

この接続には TLS 1.2 を使用しています。

接続は AES_128_GCM を使用して暗号化および認証されており、ECDHE_ECDSA が鍵交換メカニズムとして使用されています。

[ヘルプ](#)

メールアドレスまたは携帯番号

ログインしたままにする

メールアドレスま

パスワード

生年月日

証明書の透明性に関する有効な情報がサーバーから提供されました。
=validなSCTがある証明書

画像 : facebook (https://www.facebook.com/) トップページ

www.jnsa.org
このサイトへの接続はプライベート接続です。
[詳細](#)

権限 接続

Chrome で SECOM Passport for Web SR 3.0 CA がこのウェブサイトの証明書を発行したことを確認しました。証明書の透明性に関する情報はサーバーから提供されませんでした。

[証明書情報](#)

www.jnsa.org への接続は新しい暗号スイートにより暗号化されています。
この接続には TLS 1.2 を使用しています。
接続は AES_128_GCM を使用して暗号化および認証されており、ECDHE_RSA が鍵交換メカニズムとして使用されています。

[ヘルプ](#)

証明書の透明性に関する情報はサーバーから提供されませんでした。
=SCTが無い証明書、すなわちCT対応していない

画像：JNSA (<https://www.jnsa.org/aboutus/quote.html>) お問い合わせページ

【転載・引用の条件】

The image shows a Chrome browser window with the Facebook homepage open. The DevTools Security panel is open, displaying the following information:

- Origin:** <https://www.facebook.com>
- Secure Origins:** <https://www.facebook.com>, <https://static.xx.fbcdn.net>
- Connection:** Protocol: TLS 1.2, Key Exchange: ECDHE_ECDSA, Cipher Suite: AES_128_GCM
- Certificate:** Subject: *.facebook.com, SAN: *.facebook.com, *.facebook.net, Valid From: Thu, 28 Aug 2014 00:00:00 GMT, Valid Until: Fri, 30 Dec 2016 12:00:00 GMT, Issuer: DigiCert SHA2 High Assurance Server CA

A red dashed box highlights the text "SCTs 3 valid SCTs" in the Certificate section. A yellow arrow points from a blue box containing the text "3 valid SCTs" to this red dashed box. Another red dashed box highlights the "詳細" (Details) link in the top left of the Security panel.

画面 : facebook (https://www.facebook.com/) トップページ

SCT: Signed Certificate Timestamp

方法	実際の利用
証明書に埋め込む (X.509v3 extension)	現在の主流。近年の認証局はデフォルトで埋め込んで証明書発行するケースが増えている (特にEV SSL証明書はほぼ100%)
TLS Extensionを利用 (signed_certificate_timestamp領域)	コードは既に提供され、実験的に利用されつつある <ul style="list-style-type: none">• Apache 2.5のmod_ssl_ct• nginxのnginx-ctモジュール
OCSP Staplingを利用	(まだ見たことがありません)

SCT: Signed Certificate Timestamp

方法	実際の利用
証明書に埋め込む (X.509v3 extension)	現在の主流。近年の認証局はデフォルトで埋め込んで証明書発行するケースが増えている (特にEV SSL証明書はほぼ100%)
TLS Extensionを利用 (signed_certificate_timestamp領域)	コードは既に提供され、実験的に利用されつつある <ul style="list-style-type: none">• Apache 2.5のmod_ssl_ct• nginxのnginx-ctモジュール
OCSP Staplingを利用	(まだ見たことがありません)

証明書ビューア: "*.facebook.com"

一般(G) 詳細(D)

証明書の階層(H)

- △DigiCert High Assurance EV Root CA
 - △DigiCert SHA2 High Assurance Server CA
 - *.facebook.com

証明書のフィールド(F)

- Certificate Key Usage
- Extended Key Usage
- CRL Distribution Points
- Certificate Policies
- Authority Information Access
- Certificate Basic Constraints
- Object Identifier (1 3 6 1 4 1 11129 2 4 2)**
- Certificate Signature Algorithm
- Certificate Signature Value

証明書埋め込みSCT :
OID = 1.3.6.1.4.1.11129.2.4.2



フィールドの値(V)

Not Critical
Size: 365 Bytes / 2920 Bits
04 82 01 69 01 67 00 75 00 a4 b9 09 90 b4 18 58
14 87 bb 13 a2 cc 67 70 0a 3c 35 98 04 f9 1b df
b8 e3 77 cd 0e c8 0d dc 10 00 00 01 51 ab 7b e9
61 00 00 04 03 00 40 00 44 00 00 00 0 71 00 51

OpenSSL 1.0.2g :

```
$ openssl x509 -text < hogehoge.crt
```

.....(省略).....

CT Precertificate SCTs:

Signed Certificate Timestamp:

Version : v1(0)

Log ID : A4:B9:09:90:B4:18:58:14:87:BB:13:A2:CC:67:70:0A:
3C:35:98:04:F9:1B:DF:B8:E3:77:CD:0E:C8:0D:DC:10

Timestamp : Dec 16 15:50:03.515 2015 GMT

Extensions: none

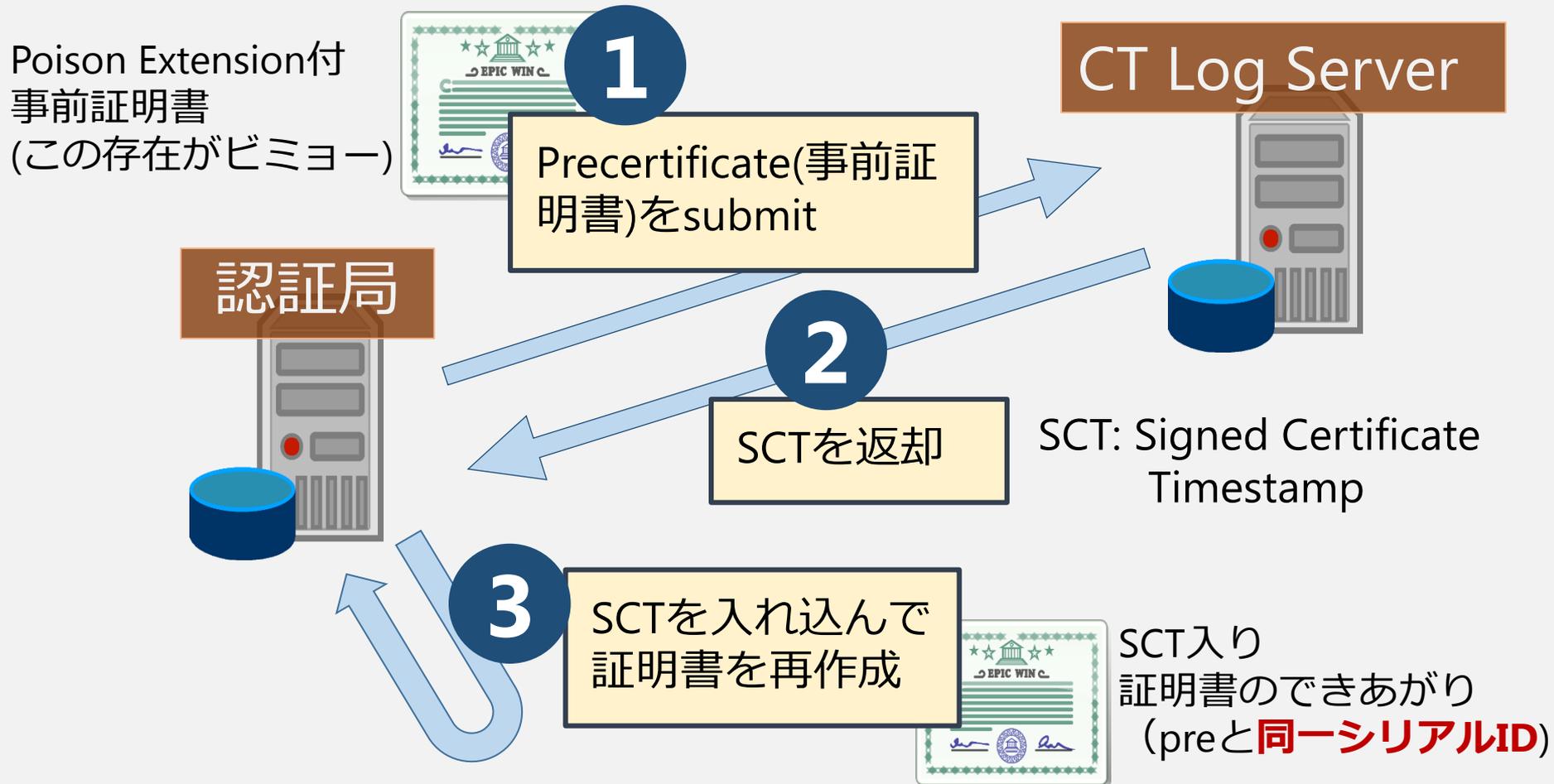
Signature : ecdsa-with-SHA256

30:44:02:20:28:C8:7D:86:5D:F1:14:32:9D:3A:50:3E:
2F:C2:99:80:EC:13:C8:F9:1F:5D:9F:8A:0A:81:FB:F9:
EA:02:8C:F5:02:20:28:6F:7F:97:B3:27:01:66:BB:89:
4D:C5:A8:53:3A:34:CE:F6:AB:46:AE:F1:70:BD:B8:27:
2D:C2:03:28:F6:2C

Signed Certificate Timestamp:

.....(省略).....

証明書をログサーバに登録する時点ではSCTが無いのに、どうしてSCT埋め込み証明書が作られるのか？



- 具体的なログの構造
 - Merkle Hash Trees
 - 追記のみで、削除機能は無い
- SCT(Signed Certificate Timestamp)の内部構造
- ログサーバのAPI仕様
- ログサーバから取得できるデータフォーマット
 - 若干ややこしい構造ですが、
「**証明書ファイルが取り出せる**」
ことだけ押さえておけば以後の話はだいじょうぶです

- Certificate Transparency (CT), RFC 6962
 - 証明書の透明性とは何か、その仕組み
- CTのメリット、デメリット
- CTで遊ぼう
 - CTを用いた攻撃シナリオを考える
- 最近の動向
 - RFC 6962-bis で何が変わるか
 - CTが役に立った(のか)? Thawte事件
 - Let's encryptの対応状況



CTのメリット

CTログサーバは誰でも閲覧できることから、多数の目による監視によって、不正な証明書発行を検知することができる（かもね）

ドメイン保有者は...

自ドメインの証明書が勝手に発行されていないか、定期的にログサーバをチェックすることで確認できる

一般ユーザは...

接続先ホストが提示した証明書から、証明書発行時の監査ログを確認できる

CTログサーバは誰でも閲覧できることから、
多数の目による監視によって、不正な証明書発行を検知
することができる（かもね）

確認できたところで、
何なんだ？
それは「監査」なのか？
という議論あり

ログサーバに証明書が登録されていることと、
その証明書が信頼できるかは、全く関係ない

一般ユーザは...

接続先ホストが提示した証明書から、
証明書発行時の監査
ログを確認できる

**※ログサーバに証明書が登録されていることと、
その証明書が信頼できるかは、全く関係ない**

- 世界中のSSL証明書を自動的に収集し、データ取得
 - 証明書の種類、内部に含まれるドメイン名・組織名情報
 - 証明書の発行枚数から、認証局の売上金額も。。。
- 認証局に対して、「上から目線」になれるカードを一枚持つことができる
 - 「証明書発行」という認証局の重要業務に対し、悪意を持ってSCTを発行しないことが原理的には可能

<https://www.chromium.org/Home/chromium-security/certificate-transparency>

Log Operator	Name	Log URL
Google	Google 'Pilot' Log	https://ct.googleapis.com/pilot
Google	Google 'Aviator' Log	https://ct.googleapis.com/aviator
DigiCert	DigiCert's Certificate Transparency log	https://ct1.digicert-ct.com/log/ct/v1/
Google	Google 'Rocketeer' Log	https://ct.googleapis.com/rocketeer
Certly	Certly.IO Log	https://log.certly.io
Izenpe	Izenpe Log	https://ct.izenpe.com
Symantec	Symantec Log	https://ct.ws.symantec.com
Venafi	Venafi CT Log Server	https://ctlog.api.venafi.com/ct/v1

Reject!

- 証明書は複数のログサーバに登録することが推奨
- RFC上、ログサーバは誰でも立てて良い
(Googleのものがデファクトスタンダードだけど)



CTのデメリット (いっぱいあるよ)

認証局は

SCT取得時に、Precertificateという、けったいなものを作らないといけない
⇒ 同一シリアルID問題、pre作成モジュールの運用管理コスト増

サーバ管理者は

ログサーバに登録された証明書から、関係者のみにしか公開したくないFQDNなどが漏えいする

一般ユーザは

ログサーバ管理者には、「いつ、どのIPアドレスから、どのFQDNにアクセスがあったか」が分かってしまう

攻撃者目線で、 今日はここに注目

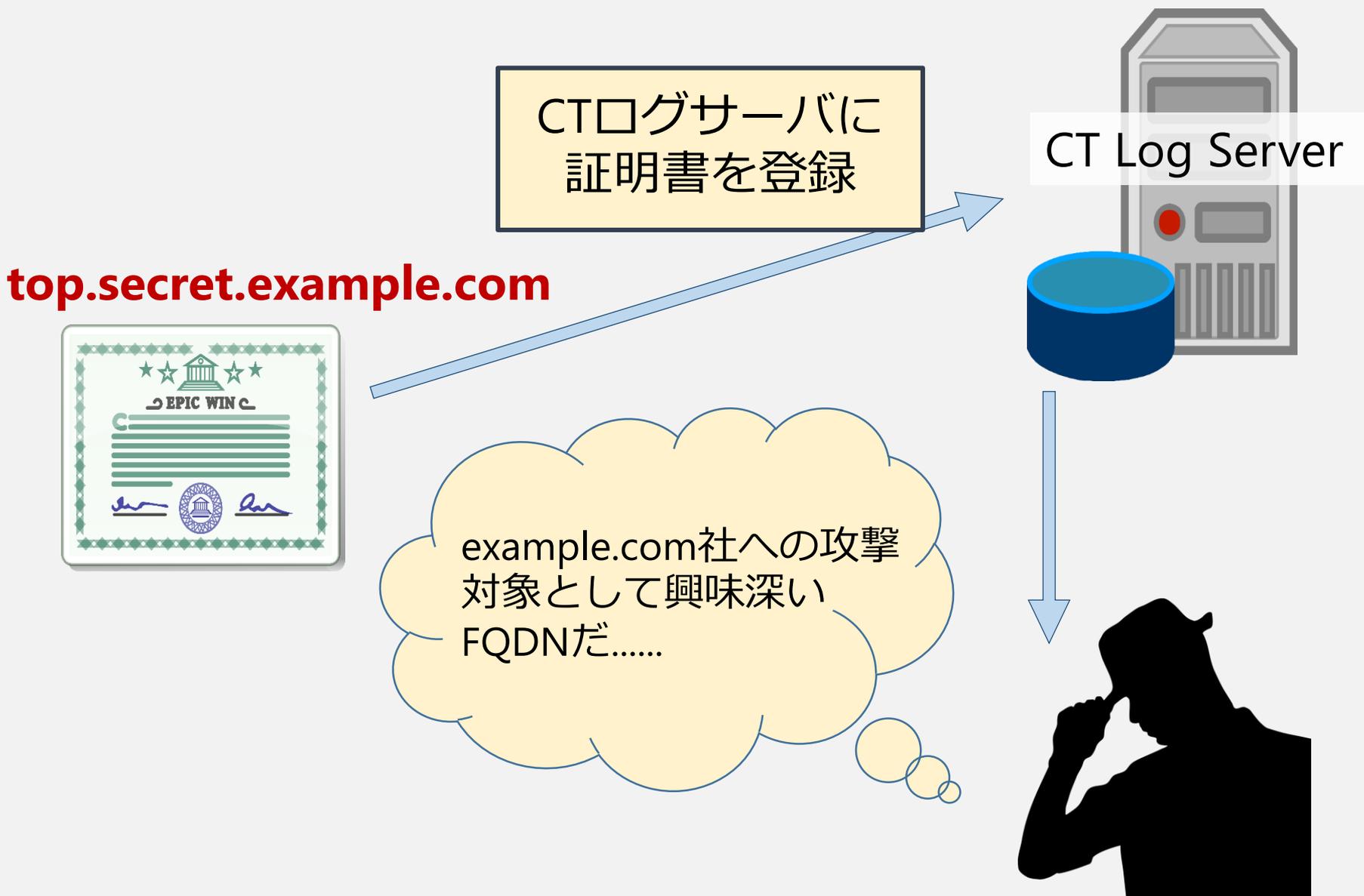
SCT取得時に、Precertificateという、けったのを作らないといけない
シリアルID問題、pre作成モジュール管理コスト

サーバ管理者は

ログサーバに登録された証明書から、関係者のみにしか公開したくないFQDNなどが漏えいする

一般ユーザは

ログサーバ管理者には、「いつ、どのIPアドレスから、どのFQDNにアクセスがあったか」が分かってしまう



FQDNが強制公開されることにより。。。。

- セキュリティ上のリスク

- 関係者のみしか知らないFQDNが全世界に強制公開
- 社内用VPN、BtoBのAPIサーバ、開発用サーバなど
- ログサーバは追記のみで、削除不可な点も注意

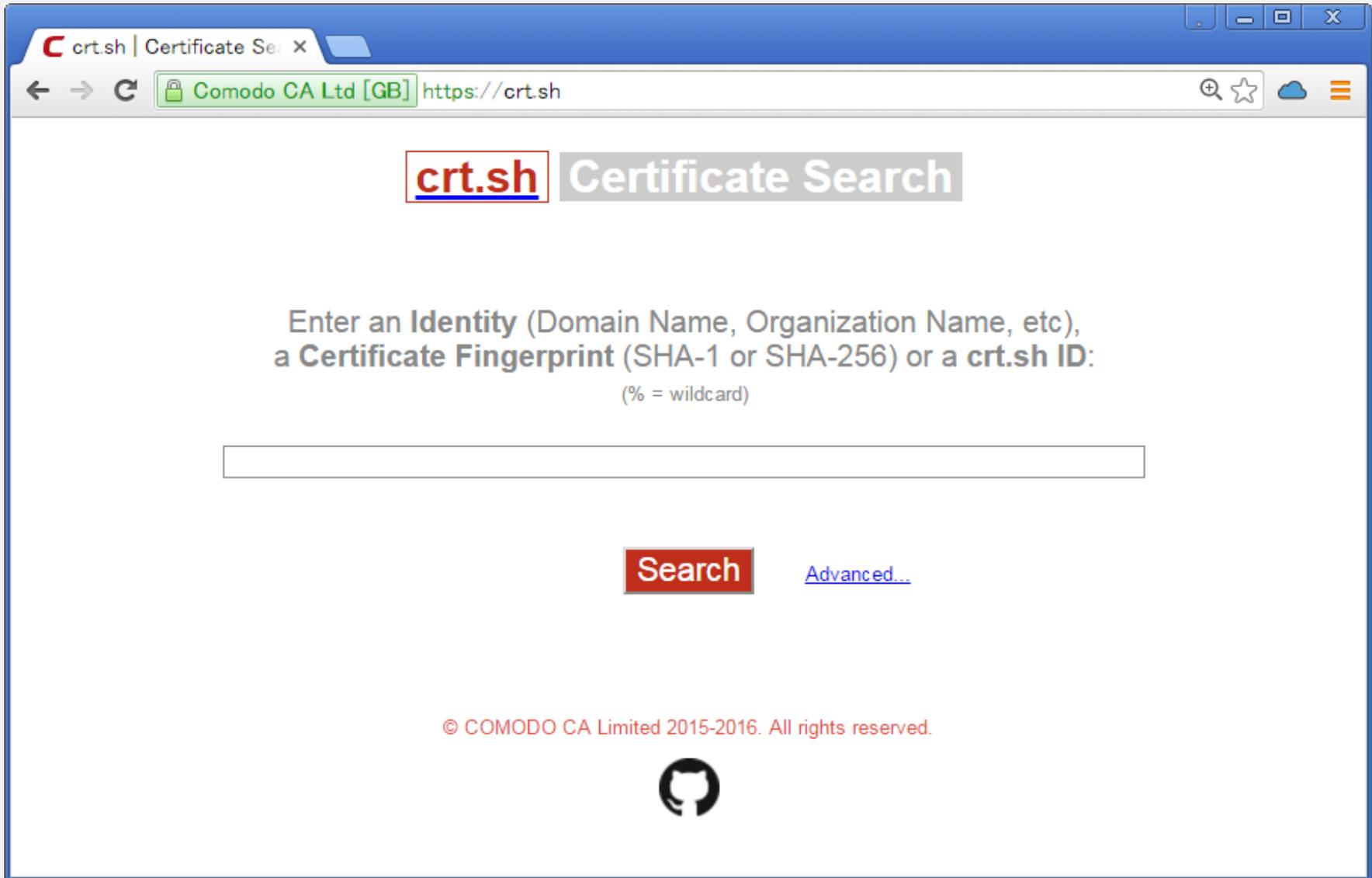
- マーケティング上のリスク

- リリース前に、サービス名・ブランド名をライバル社が取得可能。 **(新サービス名).example.com** など
- example.com社が、突然 **music.example.com** というFQDNの証明書を取れば、「音楽業界に参入か?」とライバル社が推測可能

FAQ

- **ワイルドカード証明書を使えばいいのでは？**
→ EV証明書は仕様上、ワイルドカード証明書不可です。
- **CA(認証局)が、CTログに登録する・しないを選択して証明書発行できるようサービスするべきでは？**
→ 選択できる会社もあります。また「EV証明書のみ登録」している会社があるため、CT登録したくない場合はOV証明書を勧めている会社もあります。

- Certificate Transparency (CT), RFC 6962
 - 証明書の透明性とは何か、その仕組み
- CTのメリット、デメリット
- CTで遊ぼう
 - CTを用いた攻撃シナリオを考える
- 最近の動向
 - RFC 6962-bis で何が変わるか
 - CTが役に立った(のか)? Thawte事件
 - Let's encryptの対応状況

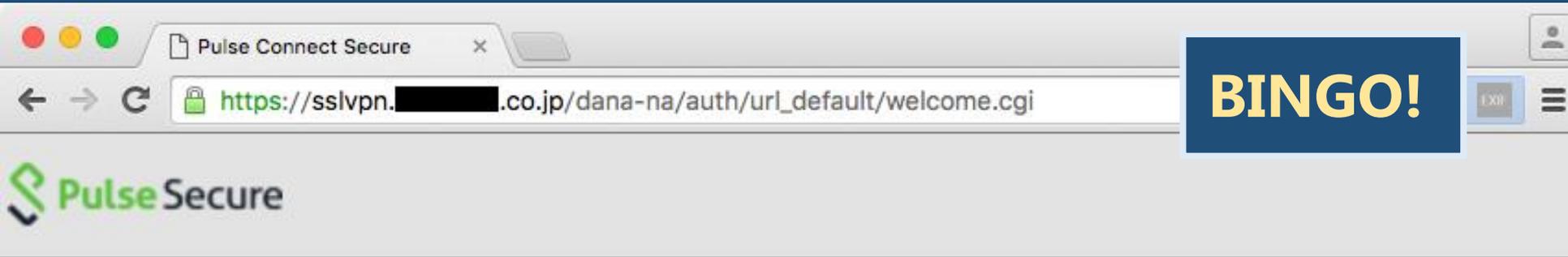


とある.co.jpを攻撃するシナリオ (1)

The screenshot shows a web browser window with the URL `https://crt.sh/?q=%25████████.co.jp`. The page title is "crt.sh Identity Search". Below the title, the search criteria are "Identity LIKE '%████████.co.jp'". The main content is a table of certificates.

Certificates	#	Identity	Details
	1	████████.co.jp	C=US, O=Symantec Corporation, OU=Symantec Trust Network, C=US, O=GeoTrust Inc., CN=RapidSSL SHA256 CA - G3
	1	noside.████████.co.jp	C=US, O=Symantec Corporation, OU=Symantec Trust Network, C=US, O=GeoTrust Inc., CN=RapidSSL SHA256 CA - G3
	1	product-support.████████.co.jp	C=US, O=Symantec Corporation, OU=Symantec Trust Network, C=US, O=GeoTrust Inc., CN=RapidSSL SHA256 CA - G3
	1	smx.████████.co.jp	C=US, O=Symantec Corporation, OU=Symantec Trust Network, C=US, O=GeoTrust Inc., CN=RapidSSL SHA256 CA - G3
	1	sslvpn.████████.co.jp	C=US, O=Symantec Corporation, OU=Symantec Trust Network, C=US, O=GeoTrust Inc., CN=RapidSSL SHA256 CA - G3
	1	sslvpn.████████.co.jp	C=US, O="VeriSign, Inc.", OU=VeriSign Trust Network, OU=Term
	1	www.████████.co.jp	C=US, O=Symantec Corporation, OU=Symantec Trust Network, C=US, O=GeoTrust Inc., CN=RapidSSL SHA256 CA - G3
	2	product-support.████████.co.jp	C=US, O="VeriSign, Inc.", OU=VeriSign Trust Network, OU=Term
	3	www.████████.co.jp	C=US, O="VeriSign, Inc.", OU=VeriSign Trust Network, OU=Term
	98	*.████████.co.jp	C=BE, O=GlobalSign nv-sa, CN=GlobalSign Organization Validati
	98	████████.co.jp	C=BE, O=GlobalSign nv-sa, CN=GlobalSign Organization Validati

sslvpn !



BINGO!

Welcome to the Pulse Connect Secure

Username

Password

Sign In

Please sign in to begin your secure session.

CITRIX

ログオン

メッセージ 

基本設定

citrix.% など

ようこそ

ログオンしてアプリケーションにアクセスします。



ユーザー名:

パスワード:

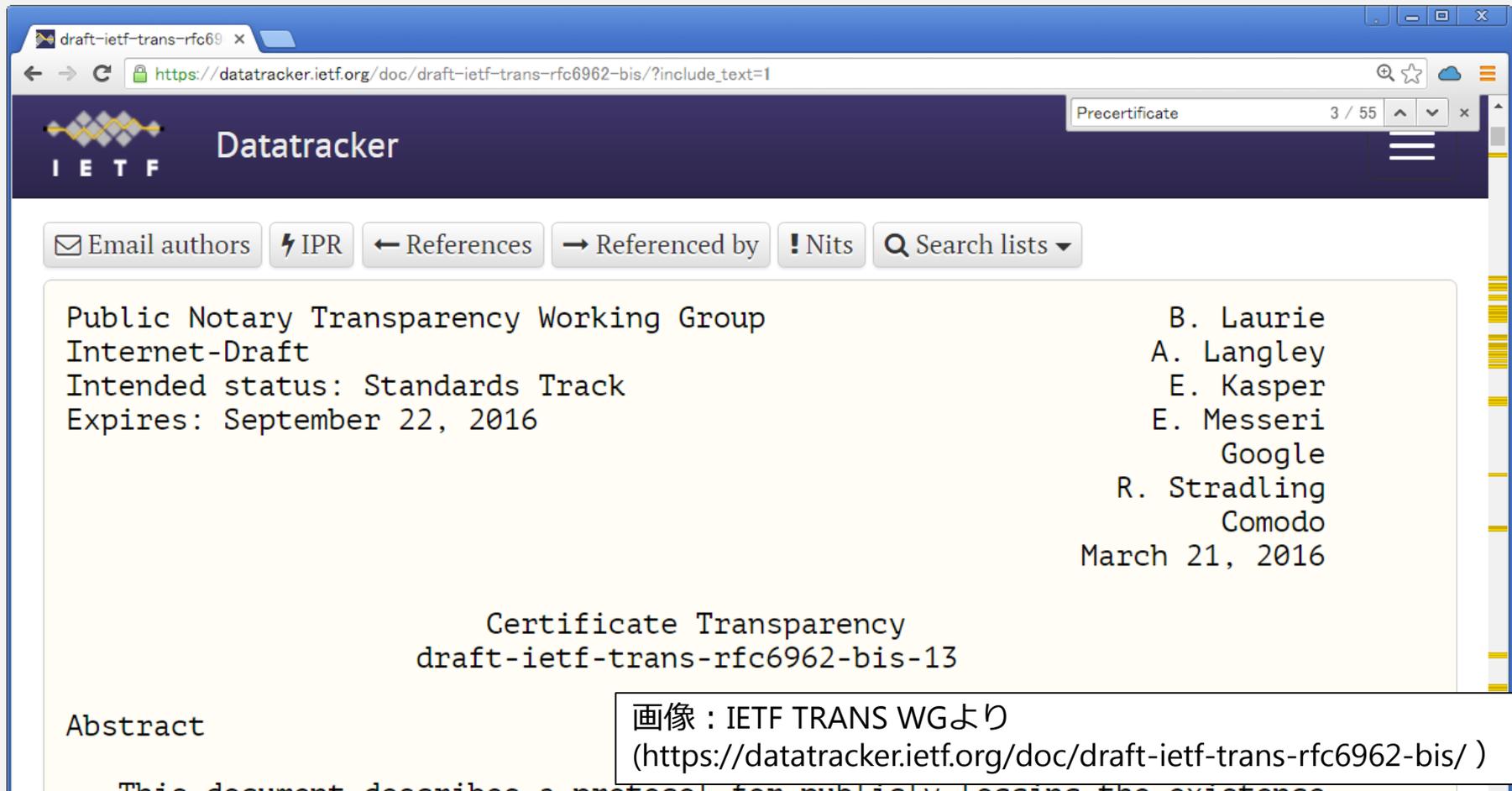
ログオン

CITRIX

- Certificate Transparency (CT), RFC 6962
 - 証明書の透明性とは何か、その仕組み
- CTのメリット、デメリット
- CTで遊ぼう
 - CTを用いた攻撃シナリオを考える
- 最近の動向
 - RFC 6962-bis で何が変わるか
 - CTが役に立った(のか)? Thawte事件
 - Let's encryptの対応状況

- 一言でいうと、だいぶ「マシ」になっています
- ログサーバ登録時のFQDNは、「**?.example.com**」と伏字で書いてもいいことになりました
 - でも、そんな改変をする工数が大変そうなので、本当に認証局が対応するかは疑問
- Precertificateは、X.509ではなくCMS(暗号メッセージ構文)になりPoison Extensionが消えました
 - 「だからPrecertificateはCertificateじゃないよ!」と言っていますが、個人的には「いや、フォーマットだけ変えてもやっぱムリあるだろ。。。と思います
- APIがエラーコード返すようになりました

- IETFのTRANS WGのメーリングリスト、リポジトリでオープンに見ることができます
 - <http://trac.tools.ietf.org/wg/trans/trac/report>
 - <https://datatracker.ietf.org/wg/trans/documents/>



The screenshot shows a web browser window displaying the IETF Datatracker page for draft-ietf-trans-rfc6962-bis-13. The browser address bar shows the URL: https://datatracker.ietf.org/doc/draft-ietf-trans-rfc6962-bis/?include_text=1. The page header includes the IETF logo and the word "Datatracker". Below the header, there are navigation buttons: "Email authors", "IPR", "References", "Referenced by", "Nits", and "Search lists". The main content area displays the following text:

```
Public Notary Transparency Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 22, 2016

B. Laurie
A. Langley
E. Kasper
E. Messeri
Google
R. Stradling
Comodo
March 21, 2016

Certificate Transparency
draft-ietf-trans-rfc6962-bis-13
```

Below the main content, there is an "Abstract" section. A text box at the bottom right of the screenshot contains the following text:

画像 : IETF TRANS WGより
(<https://datatracker.ietf.org/doc/draft-ietf-trans-rfc6962-bis/>)

最近の動向：
Thawteによるgoogle.comの
証明書誤発行(2015年9月)

[GB] <https://crt.sh/?id=9314698>

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

0a:b4:c7:3c:41:3a:01:94:9f:23:78:f2:b2:29:f6:6c

Signature Algorithm: sha256WithRSAEncryption

Issuer:

commonName = thawte EV SSL CA - G3

organizationName = "thawte, Inc."

countryName = US

Validity

Not Before: Sep 14 00:00:00 2015 GMT

Not After : Sep 15 23:59:59 2015 GMT

Subject:

commonName = www.google.com

localityName = Mountain view

stateOrProvinceName = California

countryName = US

serialNumber = 2158113

businessCategory = Private Organization

organizationName = Symantec Corp

jurisdictionStateOrProvinceName = Delaware

jurisdictionCountryName = US

画像 : crt.sh (<https://crt.sh/?id=9314698>)より

• 概要

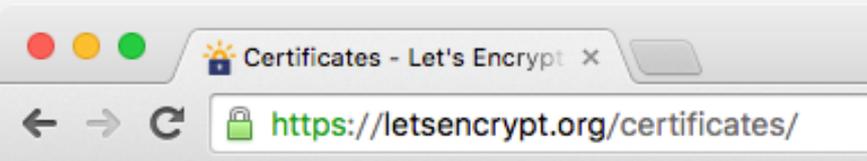
- 2015年9月、Symantecの子会社であるThawte社が、内部テストの目的でwww.google.comのEV SSL証明書を勝手に発行した
- CTログサーバに登録された証明書をGoogleが発見

• 影響

- CTログが発見の一助となったという一定の評価
- CT推進派は大きな後押しを得た
 - CTログサーバの運用は、そこまで信頼できるものなのか疑問だが権威を持ち始めている
 - 認証局が受けるような第三者機関監査をログサーバは受けてない
- Symantecは現在、CTに非常に積極的でログサーバも自前で構築している



時事ネタ(?)
Let's encryptの対応状況



ログサーバに登録はするけど、
証明書には埋め込みません

Certificate Transparency

We are dedicated to transparency in our operations and in the certificates we issue. We submit all certificates to [Certificate Transparency logs](#) as we issue them. You can view [all issued Let's Encrypt certificates at crt.sh](#).

画像 : Let's Encrypt公式ページ (<https://letsencrypt.org/certificates/>)より



ct-tls
このサ
権限

自分でログサーバからSCT取得して、nginx-ct
モジュール等でTLS Extensionで返せばOK。
<https://ct-tls-ext.suyaa.me/>

Chrome で Let's Encrypt Authority X3 がこのウェブサイトの証明書を発行したことを確認しました。証明書の透明性に関する有効な情報がサーバから提供されました。
[証明書情報](#)

ct-tls-ext.suyaa.me への接続は新しい暗号スイートにより暗号化されています。

この接続には TLS 1.2 を使用しています。

接続は AES_128_GCM を使用して暗号化および認証されており、ECDHE_RSA が鍵交換メカニズムとして使用されています。

- [1] RFC 6962
 - <https://tools.ietf.org/html/rfc6962>
 - IETF TRANS WG : <https://datatracker.ietf.org/wg/trans/documents/>
- [2] Certificate TransparencyによるSSLサーバー証明書公開監査情報とその課題の議論 (漆寫賢二氏)
 - <http://www.slideshare.net/kenjiurushima/certificate-transparencysssl>
 - 本発表の多くの部分において参考にさせていただきました。Precertificate問題や、ログサーバが信頼できるのか、ログサーバ管理者はログ改ざんできるかなど、本発表でほとんど触れられなかった部分も詳しく解説されています
- [3] IJ Internet Infrastructure Review (IIR) Vol.30
 - <http://www.ij.ad.jp/company/development/report/iir/030.html>
 - 「国内ではCTに関する問題が...(略)..指摘されている懸念事項の1つにプライバシー問題があります。例えば、今後サービスインする予定のサーバのFQDNがリリース前に漏れてしまう点などが考えられます。...(略)」
- [4] GlobalSign: Certificate Transparencyとはなにか
 - https://jp.globalsign.com/blog/2014/certificate_transparency.html
 - 非常に分かりやすい説明でシンプルにまとめられており参考になりました

その他多くのWebサイトを参考にさせていただきました

- Certificate Transparency (CT), RFC 6962
 - 証明書の透明性とは何か、その仕組み
- CTのメリット、デメリット
- CTで遊ぼう
 - CTを用いた攻撃シナリオを考える
- 最近の動向
 - RFC 6962-bis で何が変わるか
 - CTが役に立った(のか)? Thawte事件
 - Let's encryptの対応状況