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）

Google Chromeと証明書の透明性

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。

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

Transparency(透明性)?

Agenda

- 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

Agenda

- 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: 証明書

Transparency: 透明性

Certificate Transparencyを一言で

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)

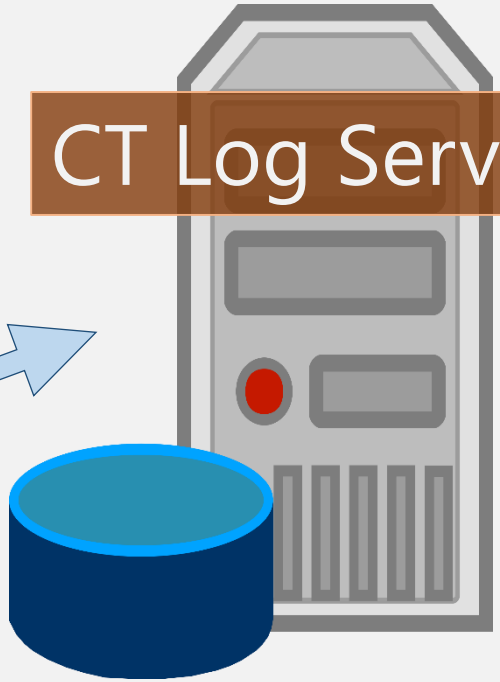
※まだExperimentalなRFC

画像：Certificate Transparecy公式ページ
https://www.certificate-transparency.org/

CTで何をするのか

※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)

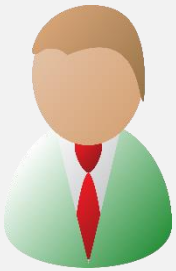


1 CTログサーバに
証明書を**登録**

2 ログサーバの署名付き
タイムスタンプ(**SCT**)を返却

SCT: Signed Certificate Timestamp

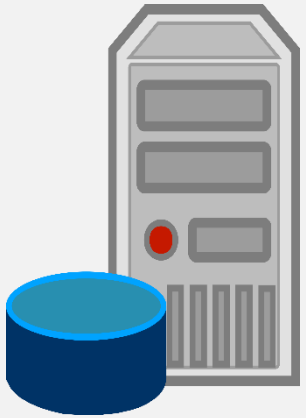
CTで何ができるのか → 監視



CA(認証局)

自社から意図しない証明書が
誤発行されていないか**監視**

CT Log Server



自ドメインの証明書が勝手
に発行されていないか**監視**

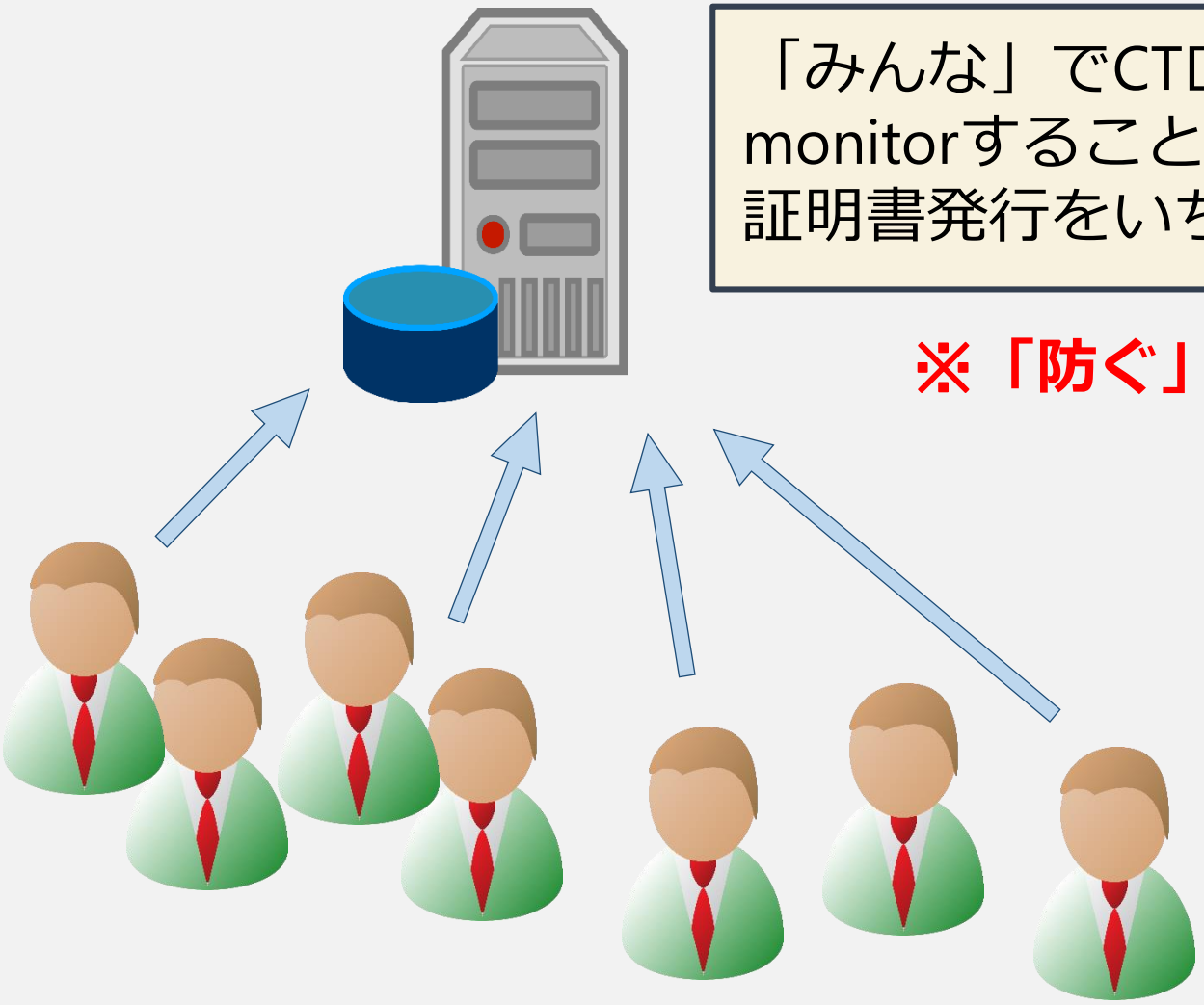
ドメイン管理者

一般ユーザ(Client)

アクセス先の証明書の
SCTを元に、ログサーバ
登録状態を確認

結局、CTで何がしたいのかを一言で

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

CT提唱の背景と思惑

- **[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

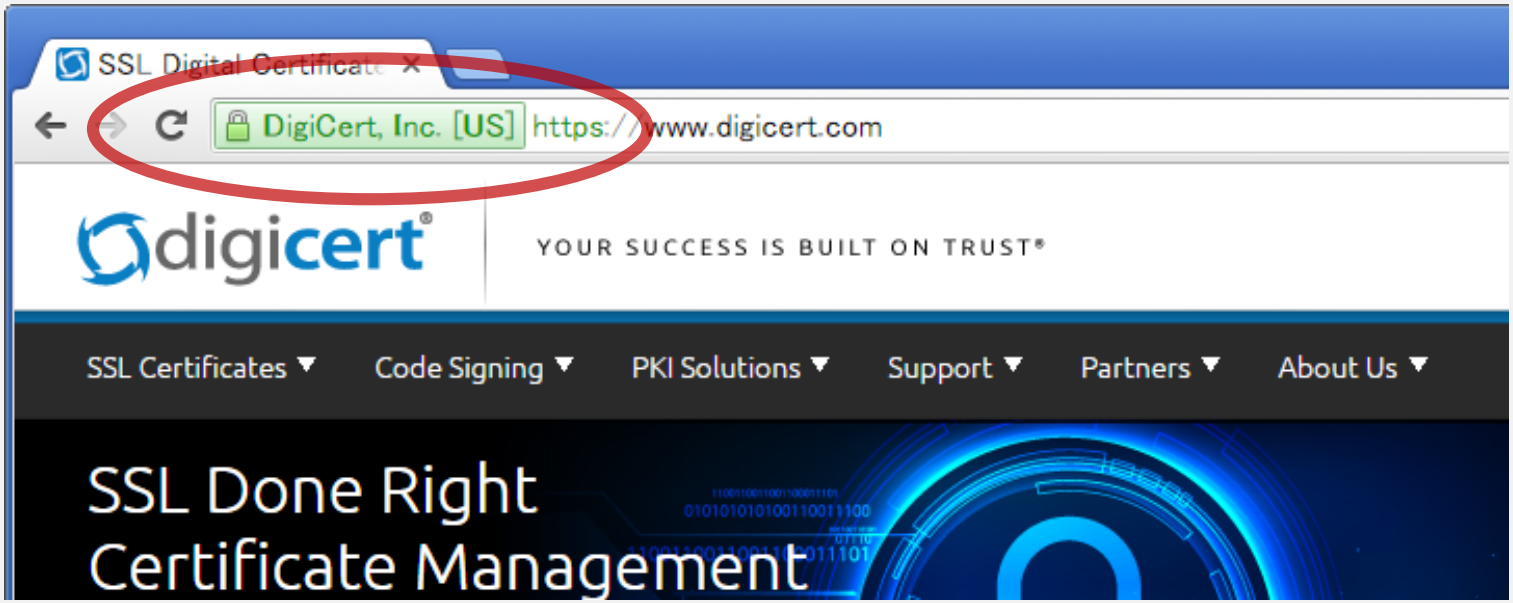
- **[思惑]** 認証局から発行された不正な証明書を、外部から見つけたい
  - 認証局を無条件に信頼しない
  - [証明書の発行]という行為が**透明(Transparency)**

WebブラウザのCT対応状況

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



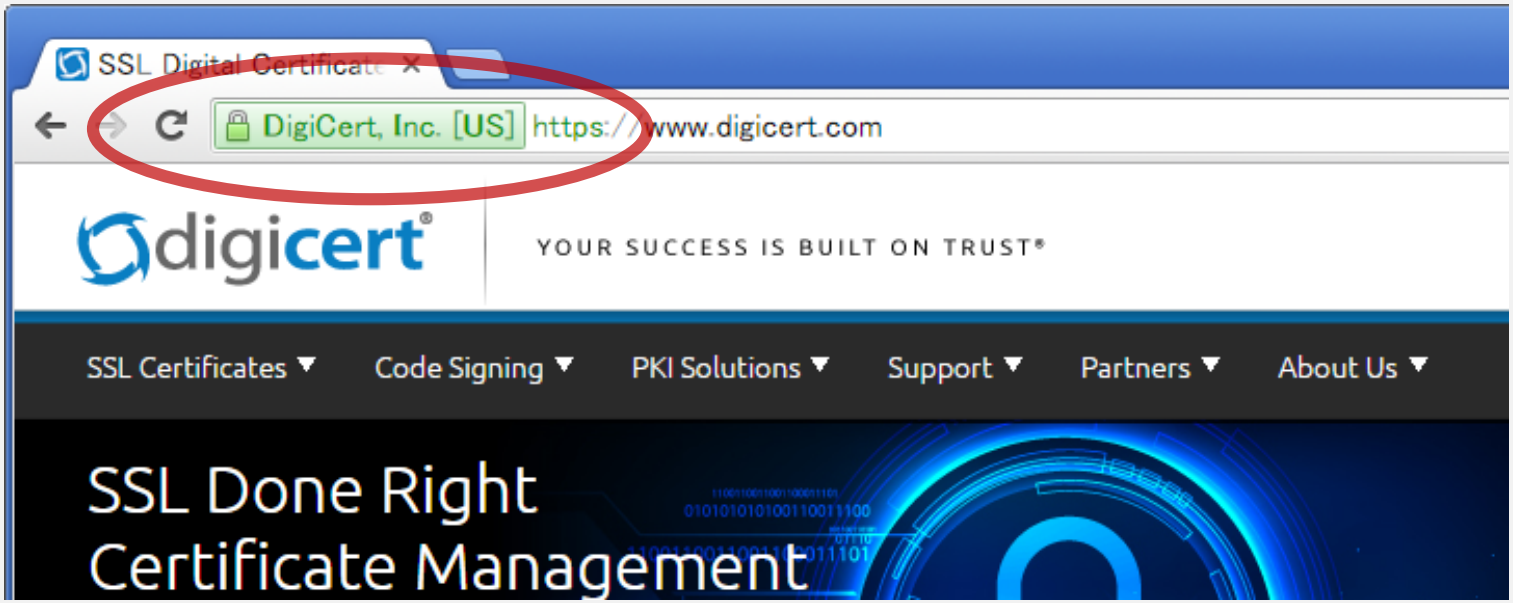
画像：DigiCert社 (https://www.digicert.com) トップページ

Webブラウザの CT対応状況

Google Chromeだけが対応、かつ先走りすぎ

「Google
タの表示を
（EV証明書

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



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

RFC上では、CT対応は必須

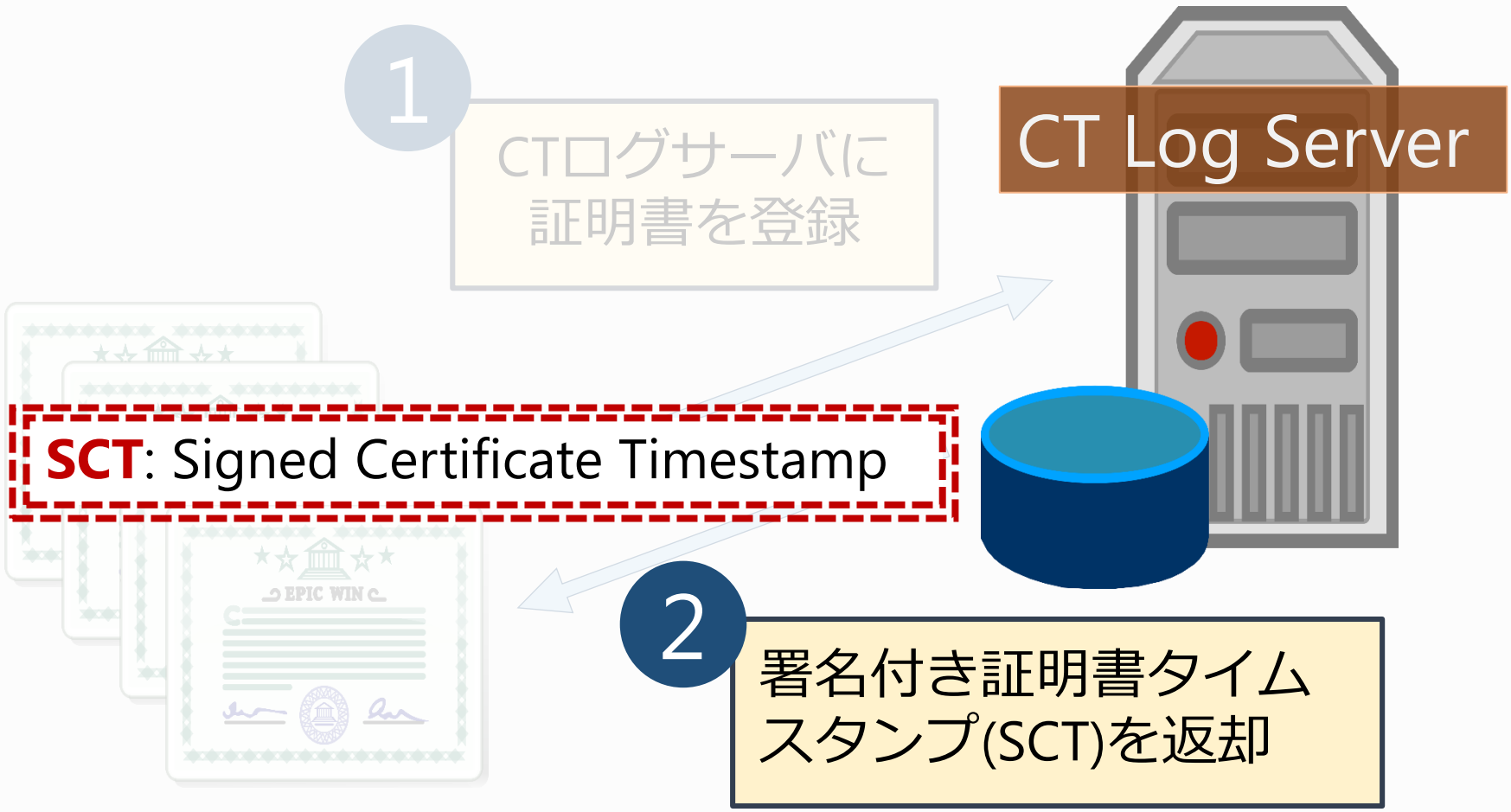
RFC 6962 says:

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）

CT登録フローの再確認



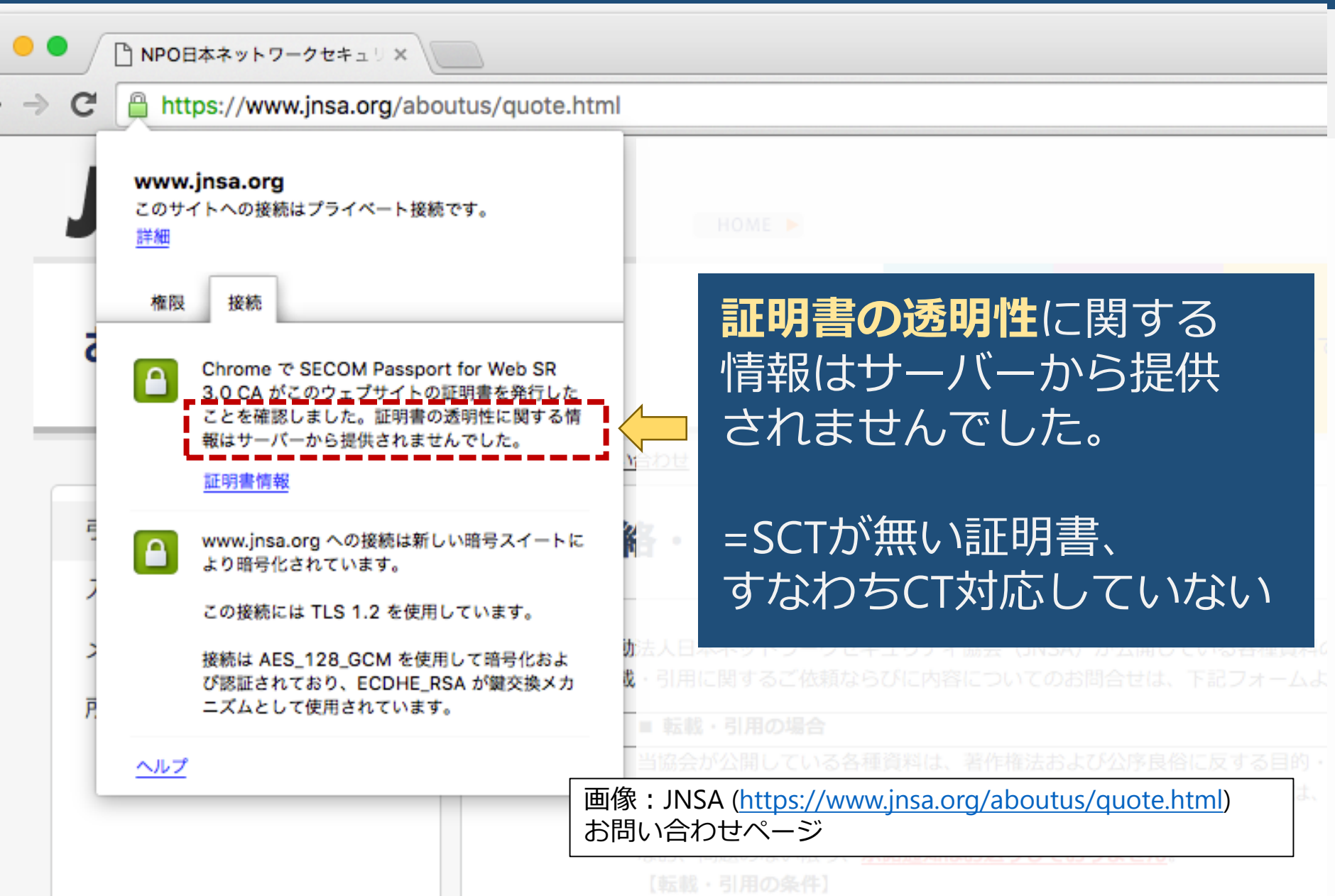
CTに対応している場合

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

CTに対応していない場合

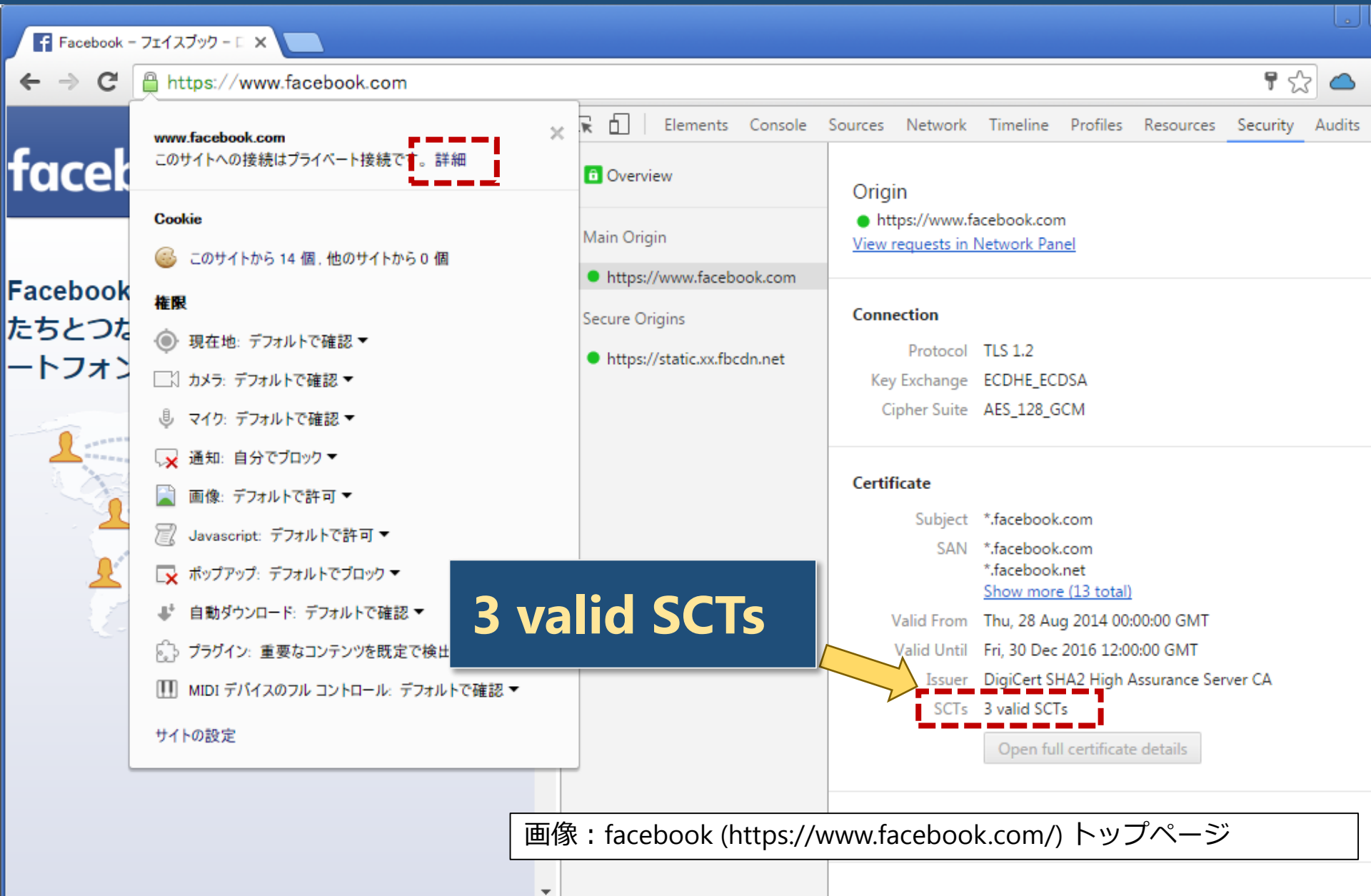


証明書の透明性に関する情報はサーバーから提供されませんでした。

=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

Chrome 50から見え方、変わりました



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

SCTのデリバリ方法は3種類

SCT: Signed Certificate Timestamp

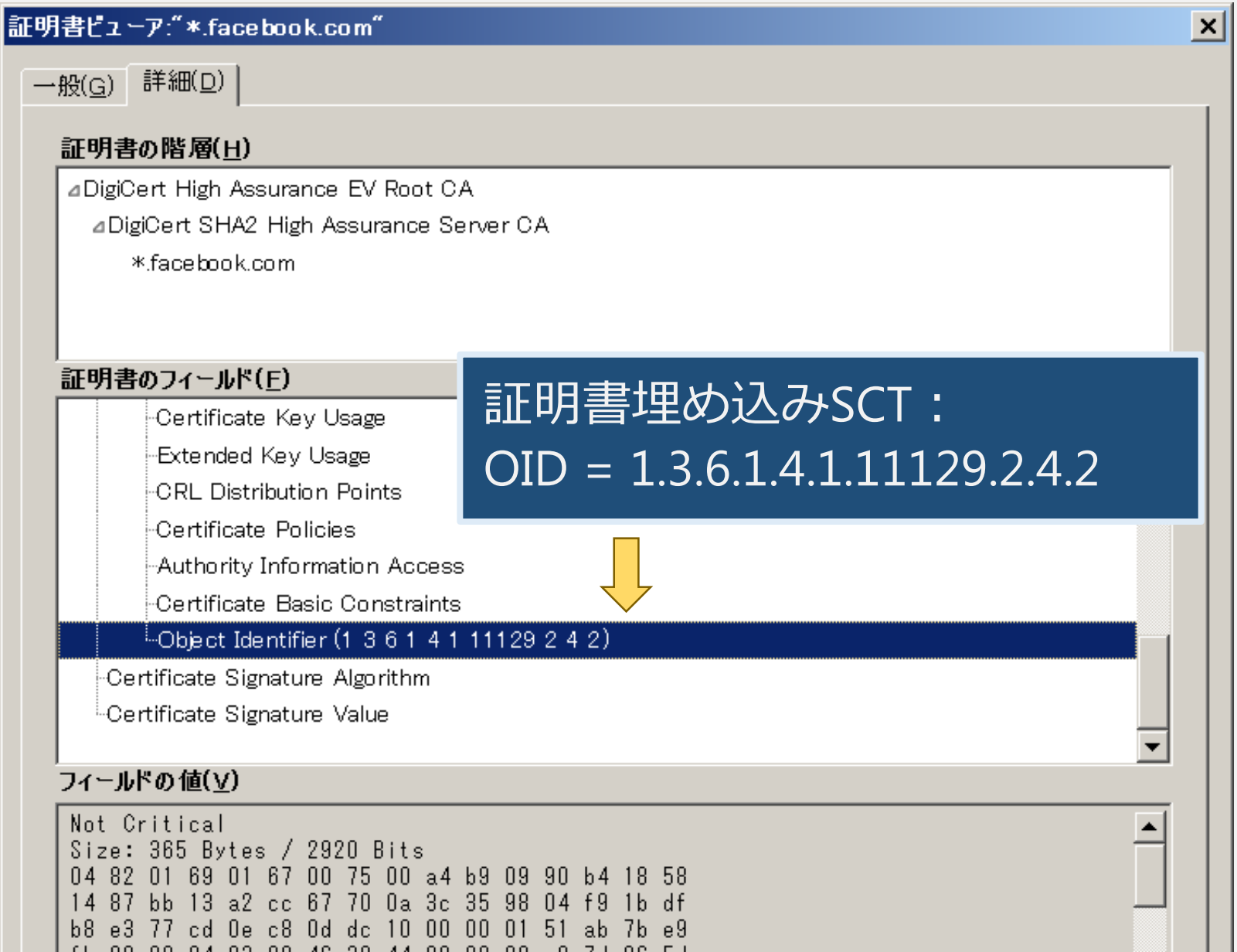
方法	実際の利用
証明書に埋め込む (X.509v3 extension)	現在の主流。近年の認証局はデフォルトで埋め込んで証明書発行するケースが増えている (特にEV SSL証明書はほぼ100%)
TLS Extensionを利用 (signed_certificate_timestamp領域)	コードは既に提供され、実験的に利用されつつある • Apache 2.5のmod_ssl_ct • nginxのnginx-ctモジュール
OCSP Staplingを利用	（まだ見たことがありません）

SCTのデリバリ方法は3種類

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 • 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）

証明書に埋め込まれたSCT



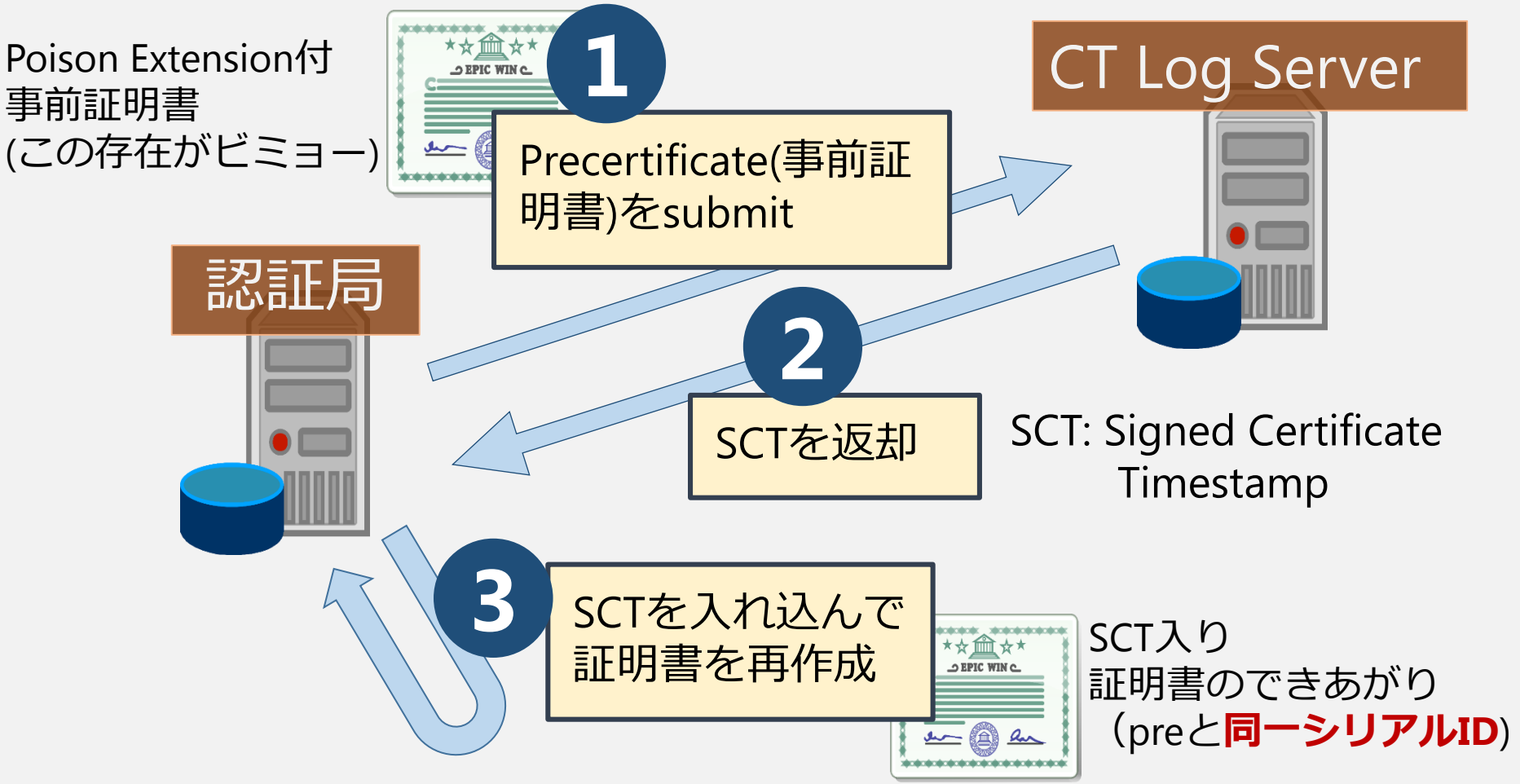
埋め込みSCTをopensslコマンドで

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).....

補足：Precertificate問題

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?



ここまでで省略したこと

- 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

Agenda

- 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

Certificate Transparency, 何が嬉しい?

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...	一般ユーザは...
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	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

Certificate Transparency, 何が嬉しい?

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

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**

CT, (Googleには)何が嬉しい?

- 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

CTログサーバはどこにいる

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）

CTのデメリット

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

CTのデメリット

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

**攻撃者目線で、
今日はここに注目**

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

ログサーバからの情報漏えい問題 (1)

CTログサーバに
証明書を登録

CT Log Server

top.secret.example.com

example.com社への攻撃
対象として興味深い
FQDNだ……

ログサーバからの情報漏えい問題 (2)

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

ログサーバからの情報漏えい問題 (3)

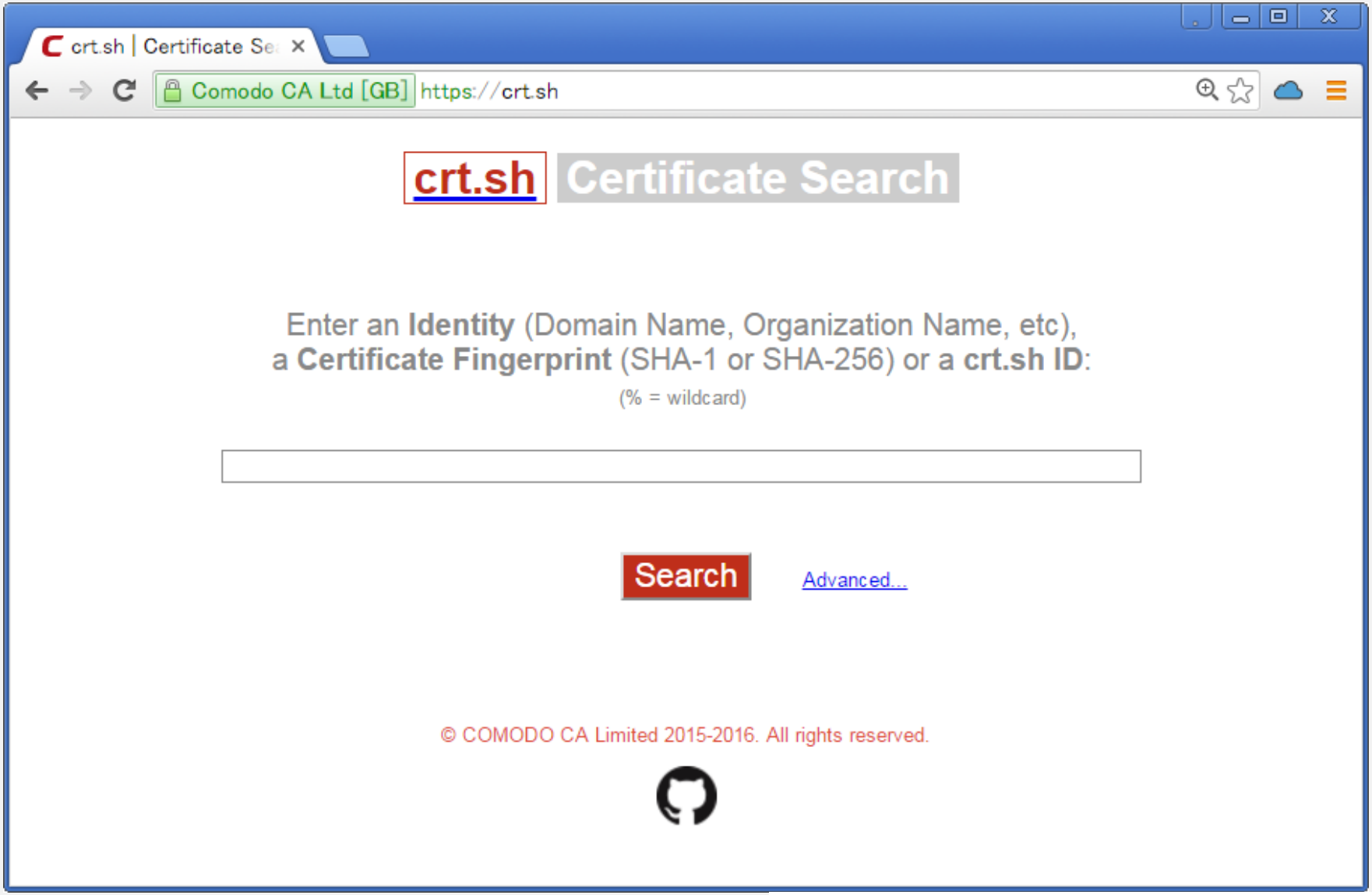
FAQ

- 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。

Agenda

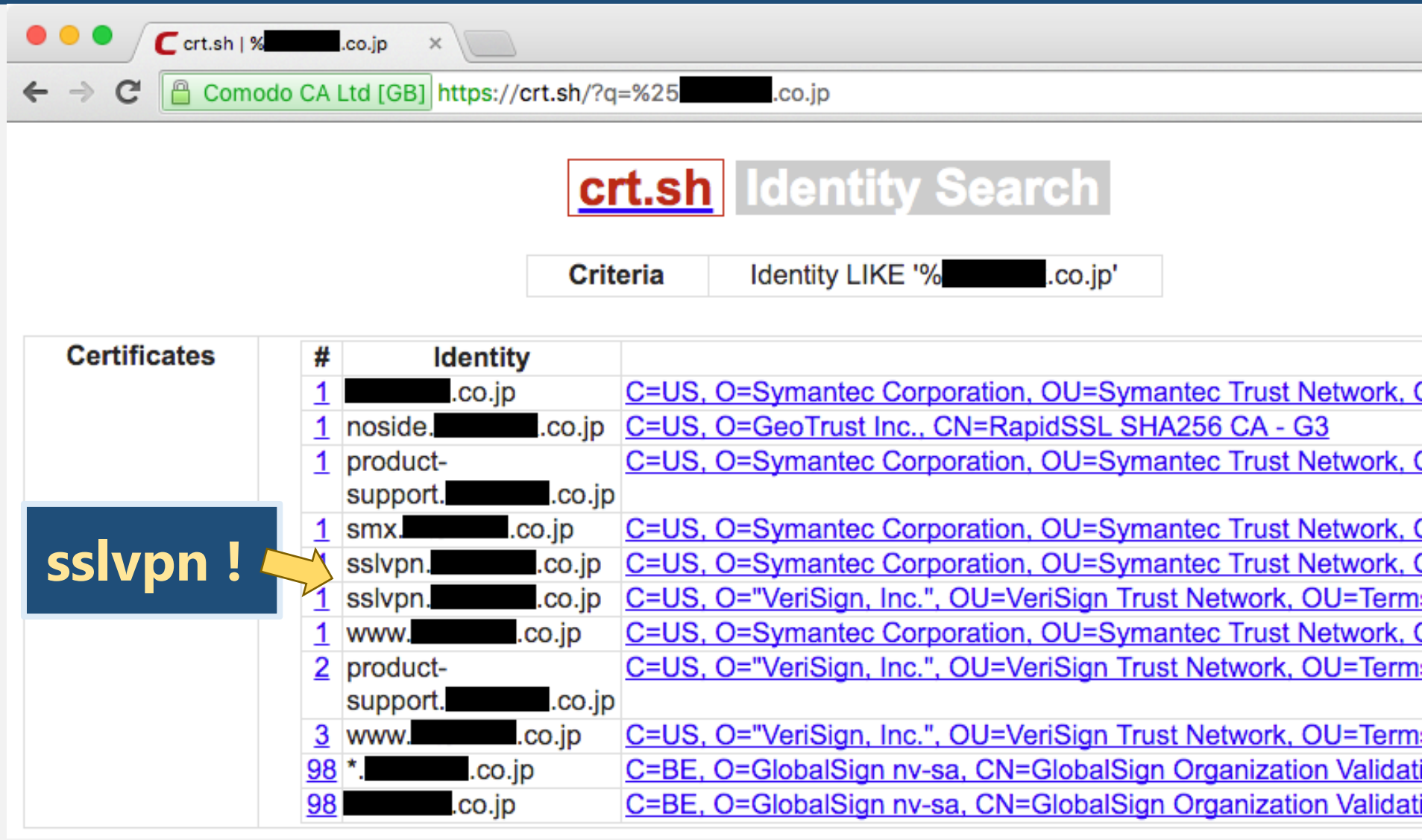
- Certificate Transparency (CT), RFC 6962
  - 証明書の透明性とは何か、その仕組み
- CTのメリット、デメリット
- CTで遊ぼう
  - CTを用いた攻撃シナリオを考える
- 最近の動向
  - RFC 6962-bis で何が変わるか
  - CTが役に立った(のか)? Thawte事件
  - Let’s encryptの対応状況

CTから証明書検索 - crt.sh



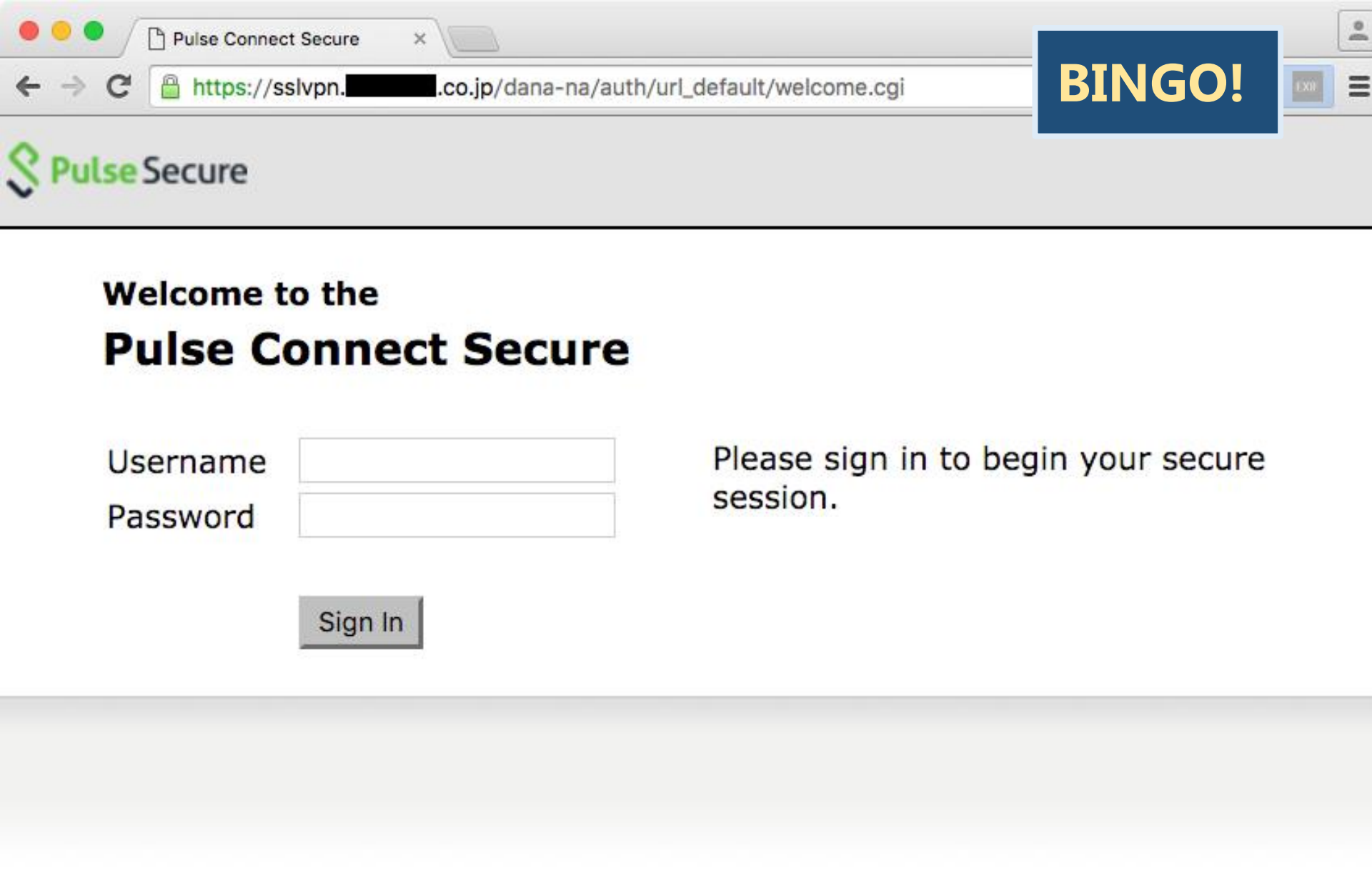
画像：COMODO社 crt.shより (https://crt.sh/)

とある.co.jpを攻撃するシナリオ (1)



画像：COMODO社 crt.shより (https://crt.sh/)

とある.co.jpを攻撃するシナリオ (2)



無差別攻撃シナリオ (1)


crt.sh | sslvpn.%
Comodo CA Ltd [GB] https://crt.sh/?q=sslvpn.%25
crt.sh Identity Search
Criteria Identity LIKE 'sslvpn.%'
Certificates
Identity
sslvpn.%
この他、
(ランダム文字列)-sslvpn.%
というFQDNも容易に発見可能
画像：COMODO社 crt.shより (https://crt.sh/)

無差別攻撃シナリオ (2)

citrix.% など

Agenda

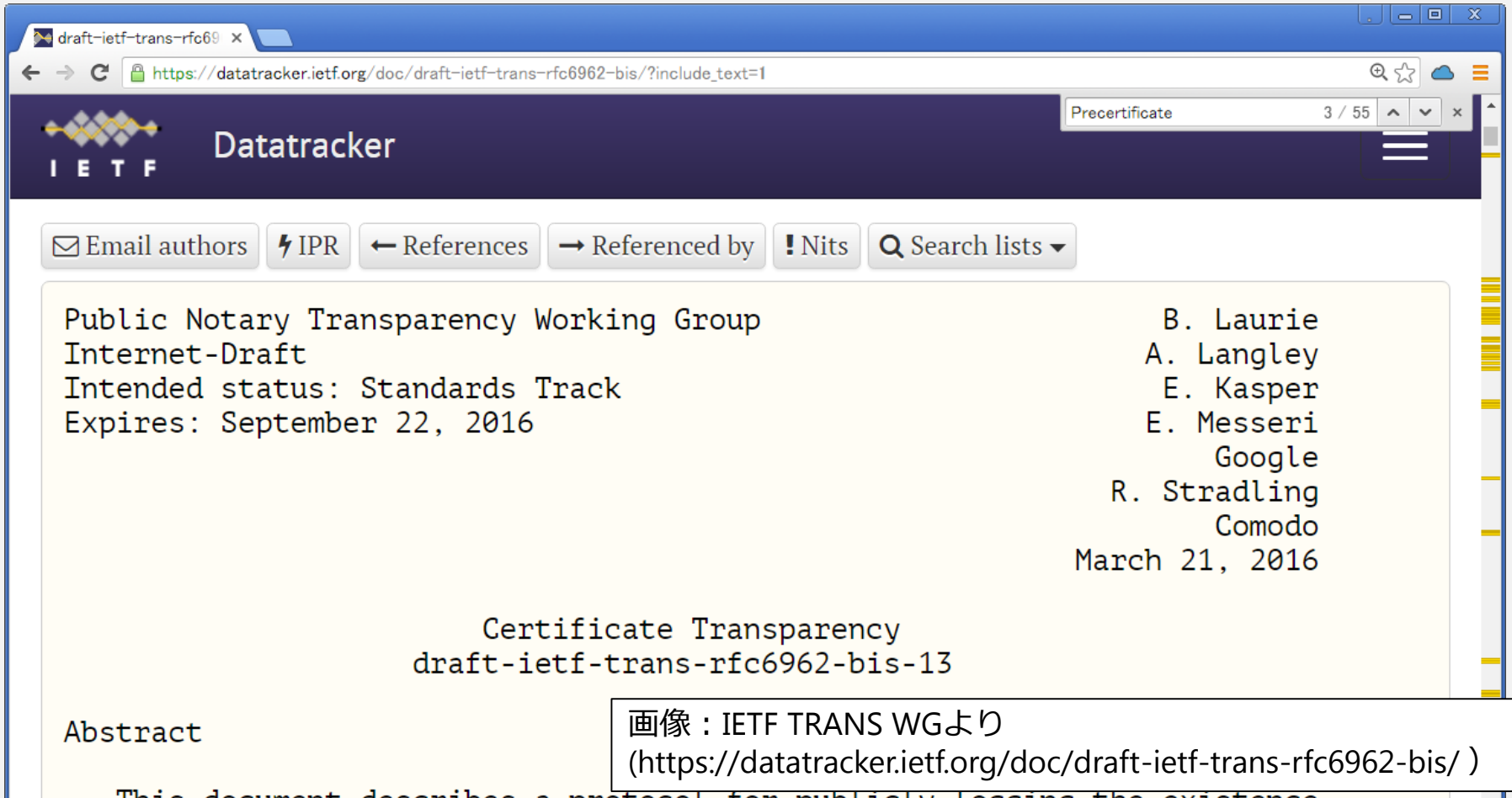
- Certificate Transparency (CT), RFC 6962
  - 証明書の透明性とは何か、その仕組み
- CTのメリット、デメリット
- CTで遊ぼう
  - CTを用いた攻撃シナリオを考える
- 最近の動向
  - RFC 6962-bis で何が変わるか
  - CTが役に立った(のか)? Thawte事件
  - Let’s encryptの対応状況

RFC 6962-bis (RFC6962改)

- 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

RFC 6962-bis (RFC6962改)を追う

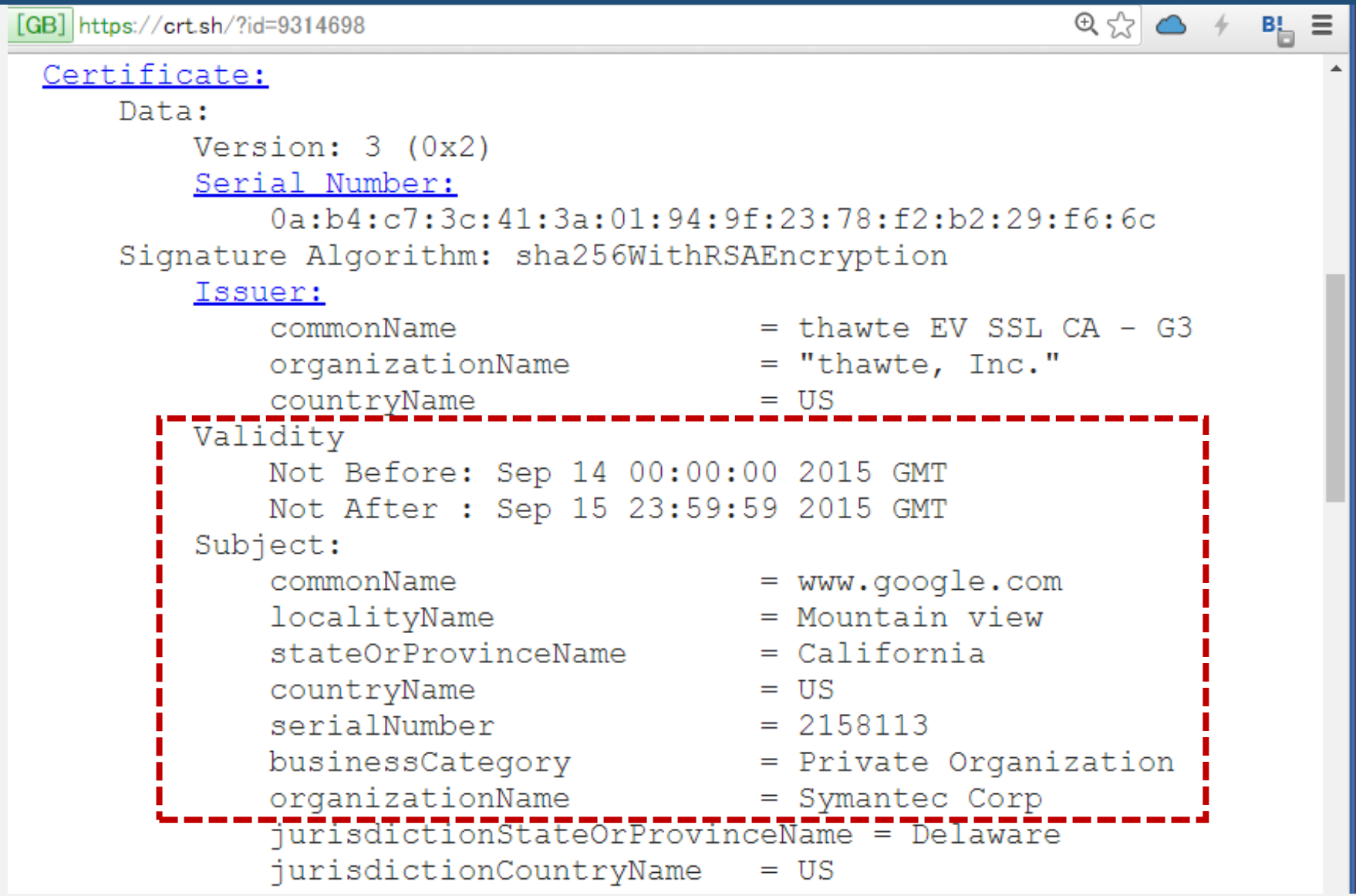
- IETFのTRANS WGのメーリングリスト、リポジトリでオープンに見ることができます
  - http://trac.tools.ietf.org/wg/trans/trac/report
  - https://datatracker.ietf.org/wg/trans/documents/



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)

問題の証明書



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

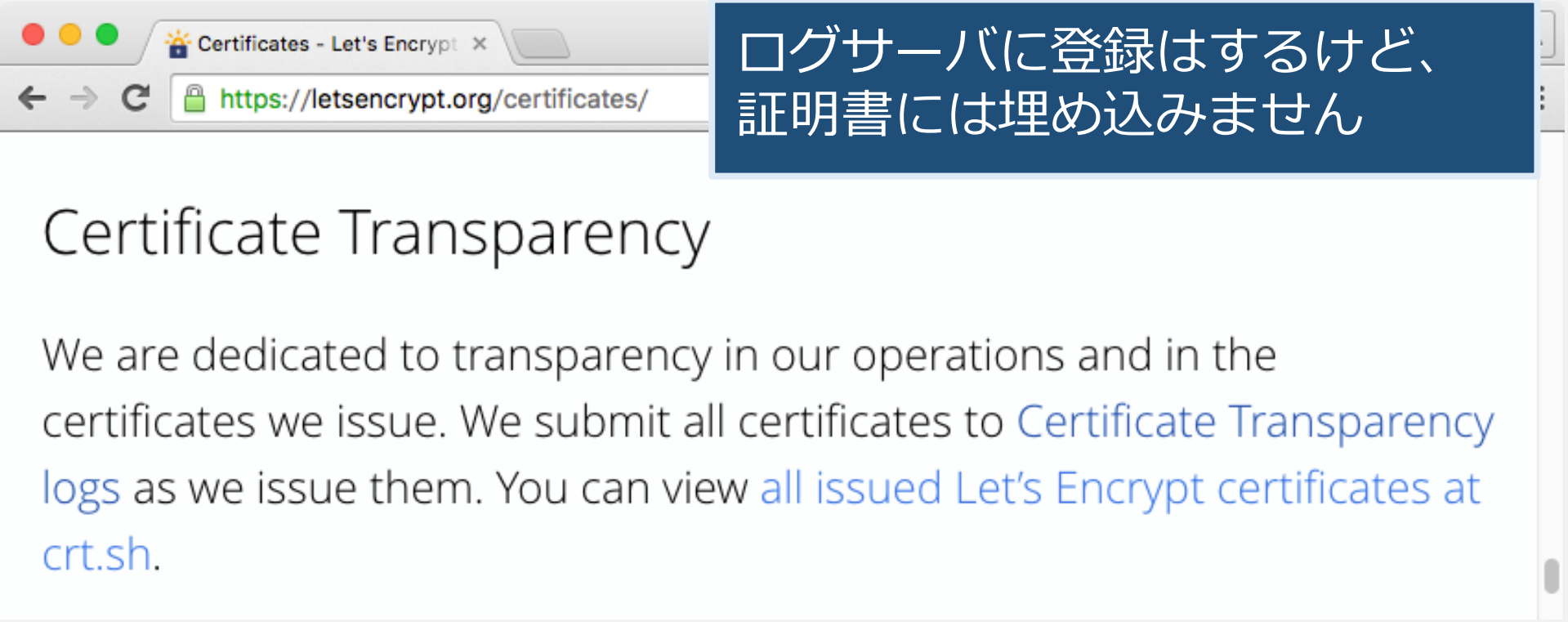
概要と影響

- 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

Let's EncryptのCT対応状況



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

Let's EncryptのCT対応状況 (2)

参考資料

- [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 (漆嶌賢二氏)
  - http://www.slideshare.net/kenjiurushima/certificate-transparencyssl
  - 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] IIJ Internet Infrastructure Review （IIR） Vol.30
  - http://www.iij.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

Agenda

- 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