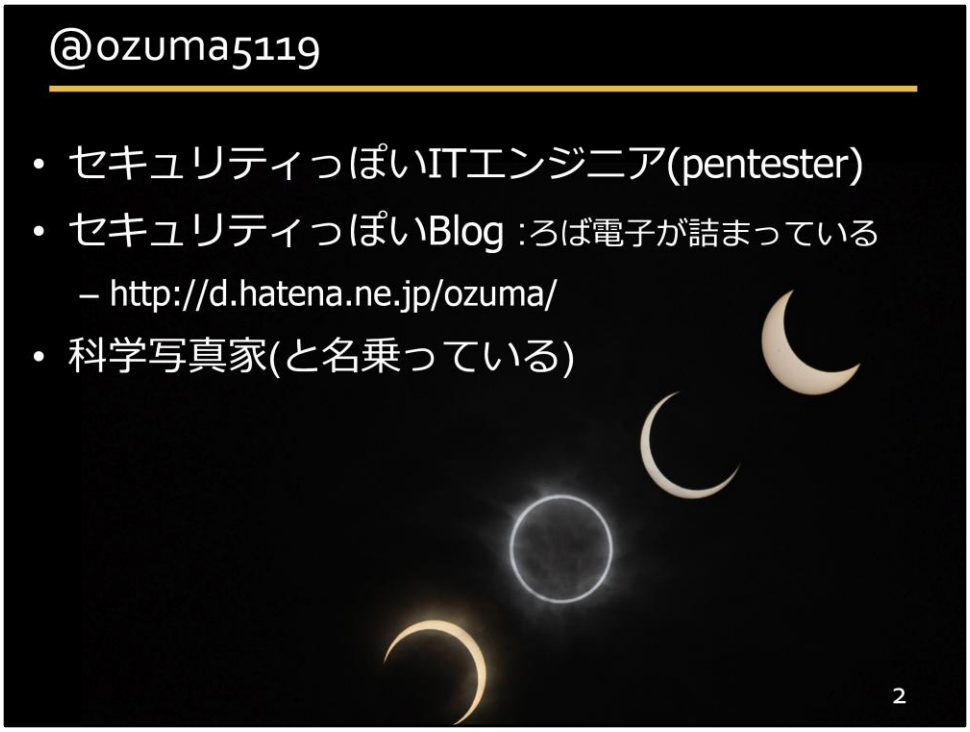
俺とお前と Certificate Transparency

すみだセキュリティ勉強会 2015#1
2015/05/09 by @ozuma5119

「俺とお前とCertificate Transparency」というタイトルで発表します、すみだセキュリティ勉強会主催のozuma5119です。



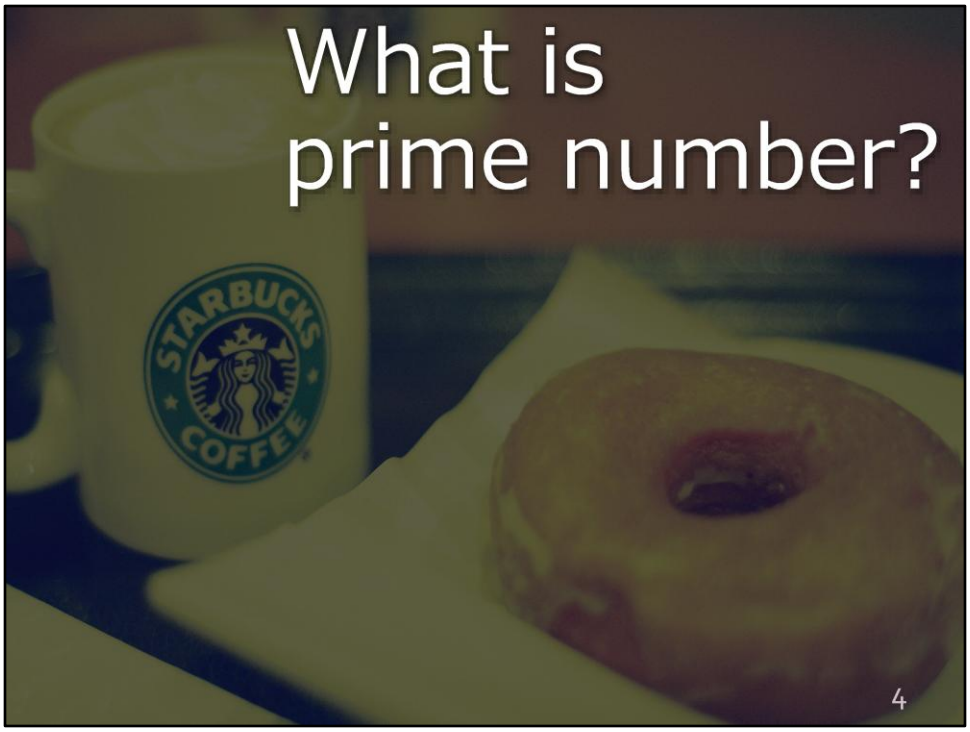
すみだセキュリティ勉強会を主催しています、ozuma5119と申します。
ふだんは、比較的固めの会社でセキュリティエンジニアをしています。ブログはこちら。
http://d.hatena.ne.jp/ozuma/

科学写真家というのは、「理科の教科書に載ってるような写真」を撮る人たちです。
こちらは副業ということで、小学生向けの教材の写真とか撮って、ときどき本に載ったりします。

今回の概要はこんな感じです。

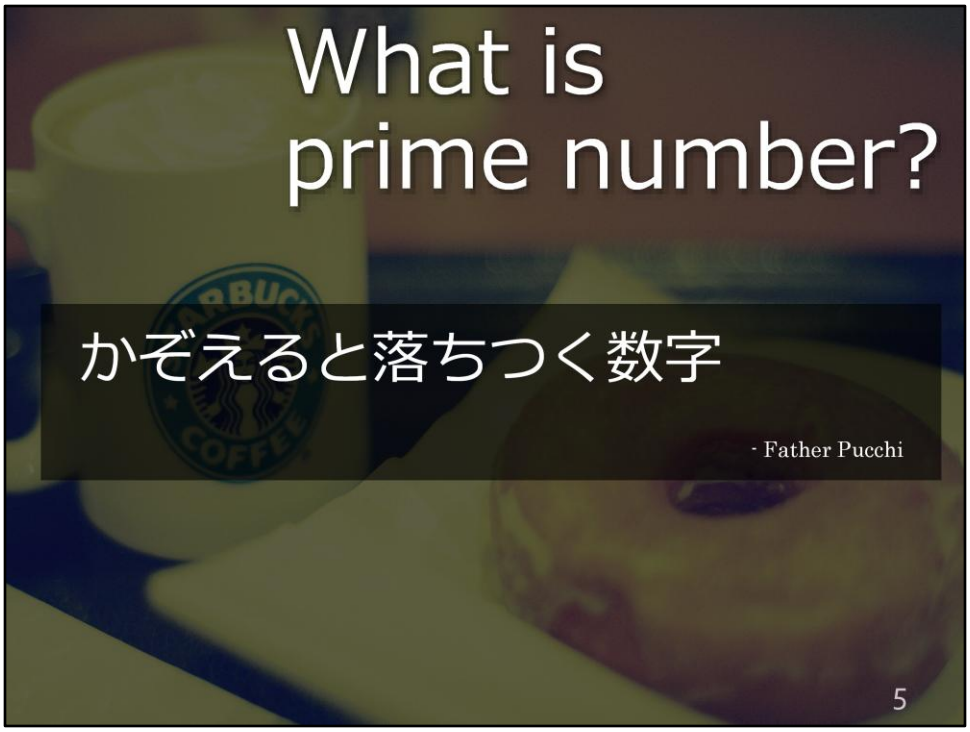
今日のメインは、2つめのCertificate Transparencyというものです。これについて話そうと思うのですが、その前にまずSSL証明書の鑑賞方法を学んでおきましょう。
CTを理解するには、証明書の見方を知らないといけないためです。

ただ、単に証明書を見ても、証明書マニアじゃないとつらいと思うので、今日は素数に注目して証明書を見てみましょう。
素数に注目して証明書を見る→見方が分かったところでCTを理解する、という流れです。

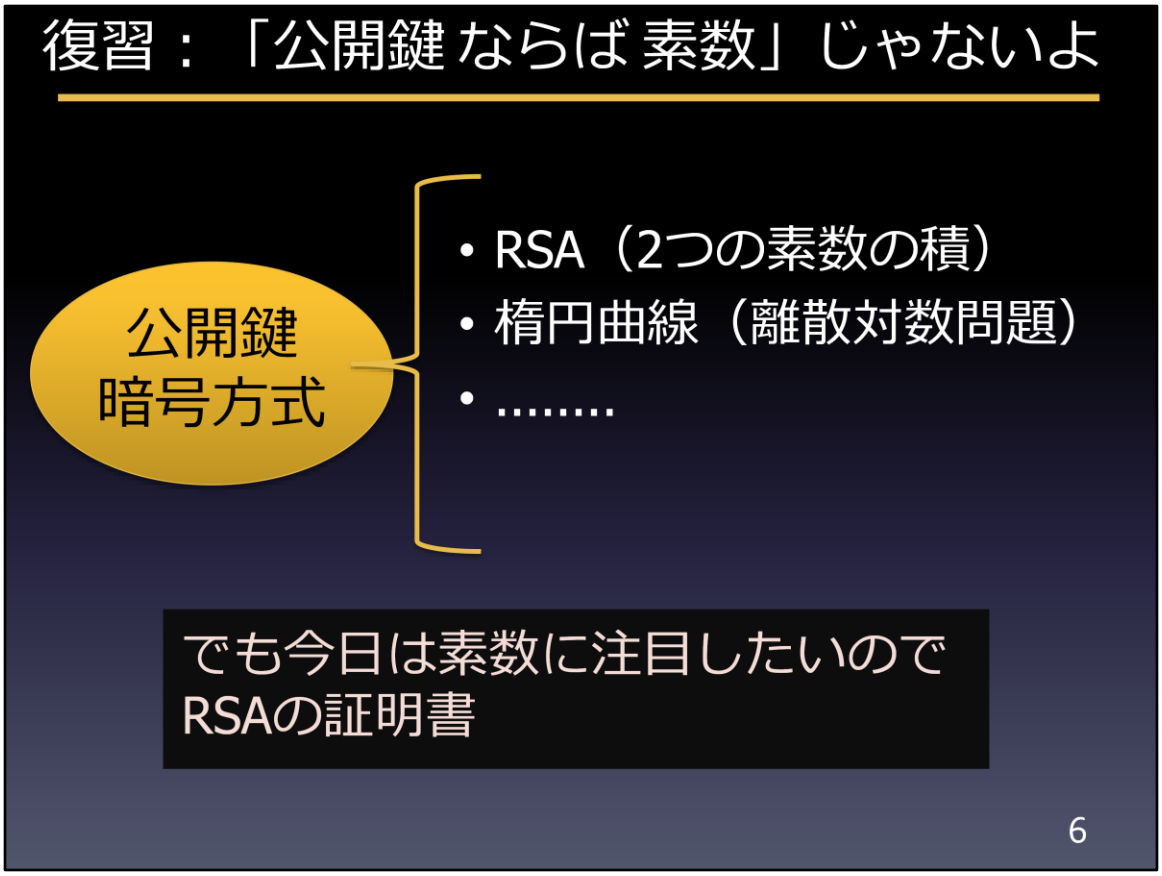


で、まず素数についてです。英語ではprime numberと言います。RSA公開鍵の中身を見たりするとprimeという言葉が出てくるので、慣れておきましょう

素数。素数ってなんでしょうか？ まぁこの勉強会に来るような方なら皆さんご存じと思いますが……



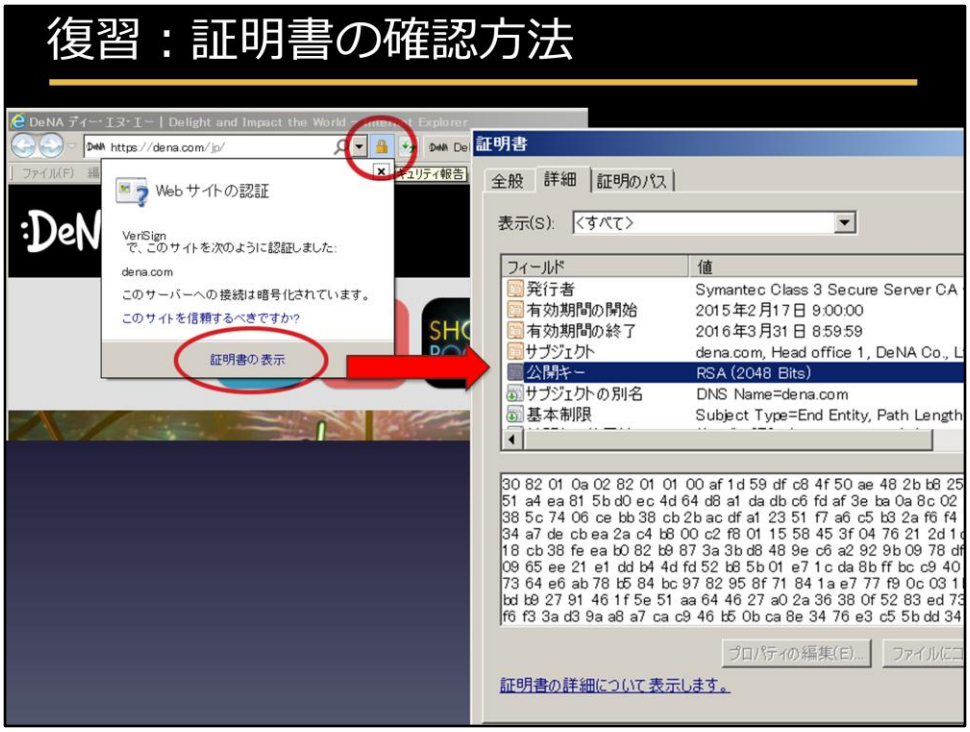
はい。素数とは、かぞえると落ち着く数ですね。
Father Pucchiが言っていましたから間違いありません。



証明書の公開鍵を見る前に、一点、確認しておきましょう。
現在多くのSSL証明書では、公開鍵暗号方式としてRSAを利用しています。これは比較的有名な、素因数分解の困難さを利用したものです。
でも、公開鍵暗号方式にはいくつもの実装があり、実際最近は、楕円曲線によるものも増えつつあります。

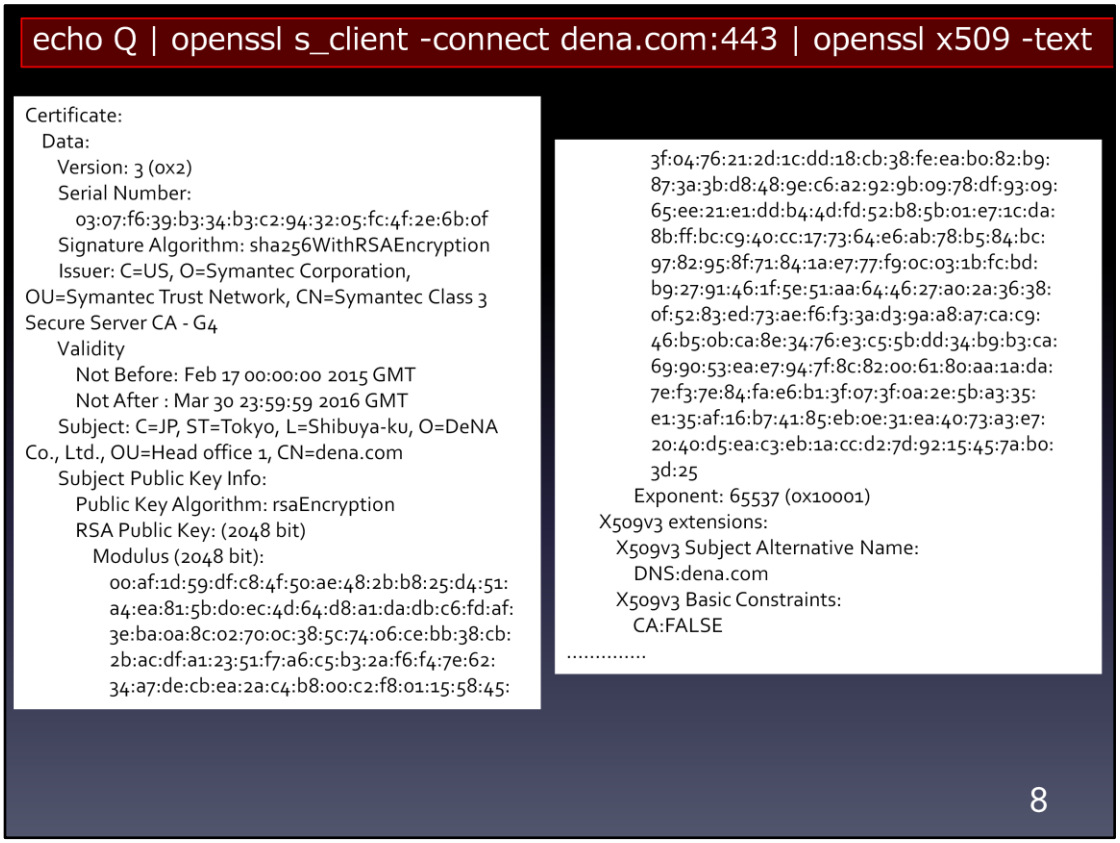
が、今日は現在もっともポピュラーな、素数を利用したRSAの証明書を見ます。

復習：証明書の確認方法



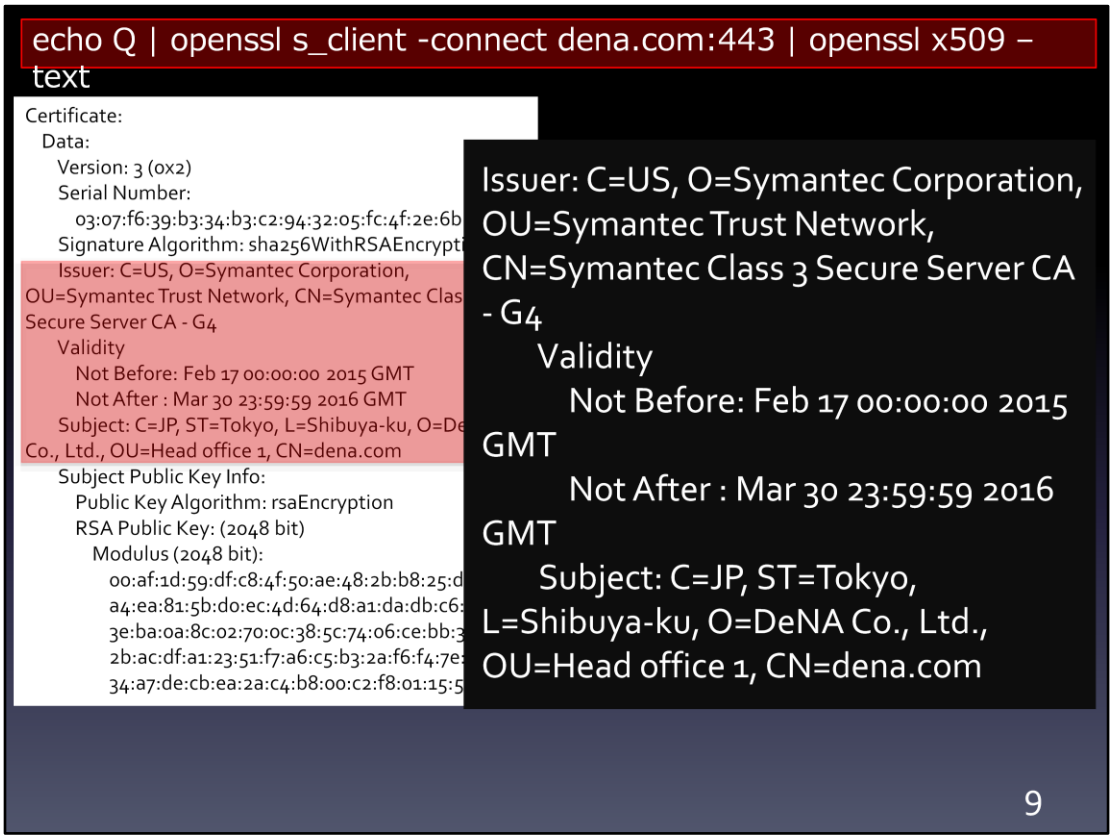
証明書の見方を復習しておきましょう。ブラウザによって若干違いますが、多くの場合には鍵マークをクリックして証明書を表示できます。
RSAを利用した公開鍵証明書ならば、このように公開キーとして現在は一般的に2048bitの数値が入っています。

次のOpenSSLコマンドを利用した例で、もうちっと証明書について細かく見てみましょう。

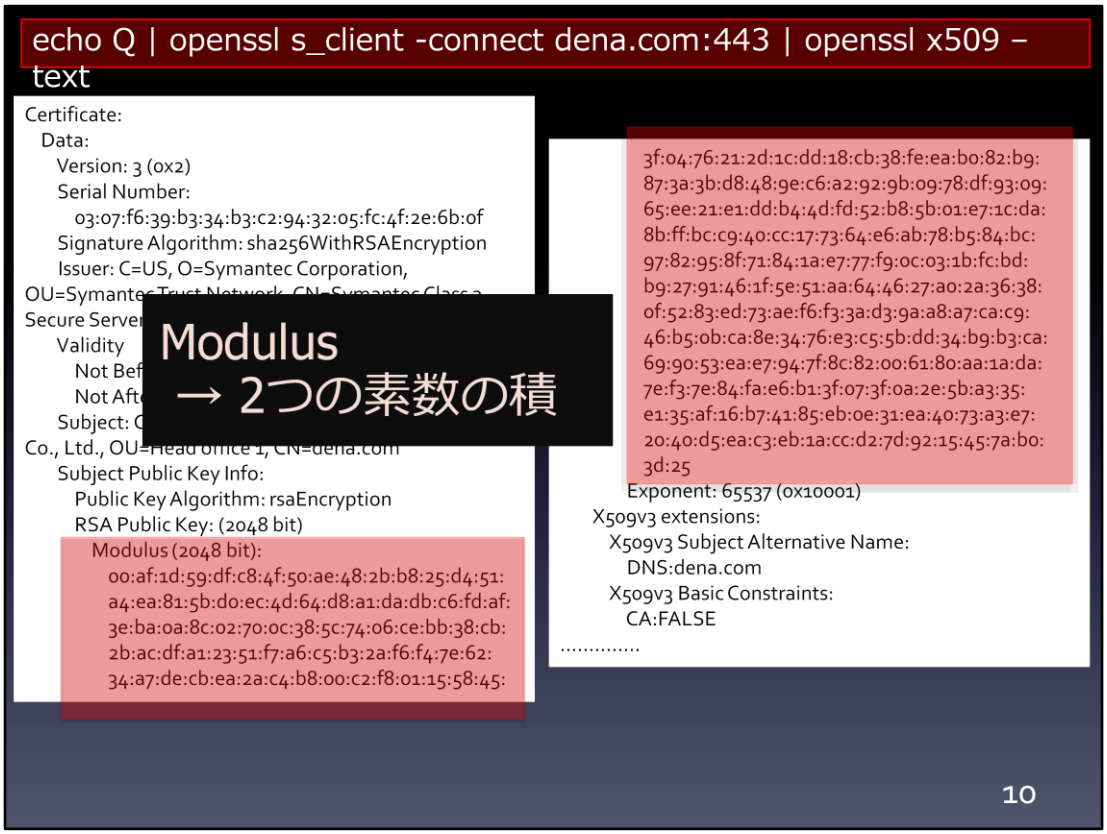


証明書はOpenSSLコマンドで直接見てみることもできます。慣れているひとなら、こちらの方がいいでしょう。
echo Q | openssl s_client -connect dena.com:443 | openssl x509 -text

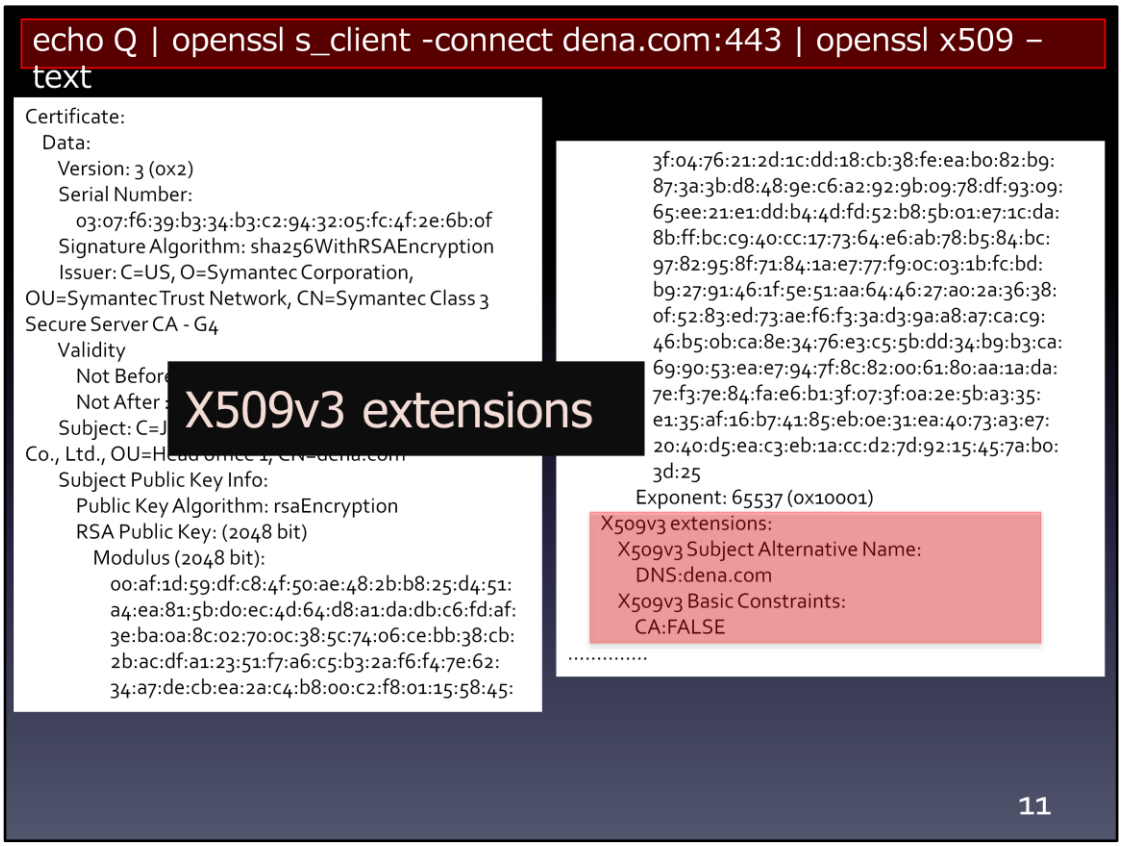
はじめにecho Qしているのは、普通につなぐとコネクションが張りっぱなしになるのでいきなりQUITするためです。まぁ手でやるならCtrl+C押せばいいので不要ですが、シェルスクリプトなどで証明書を集めたいときはこういうことをすると良いでしょう。



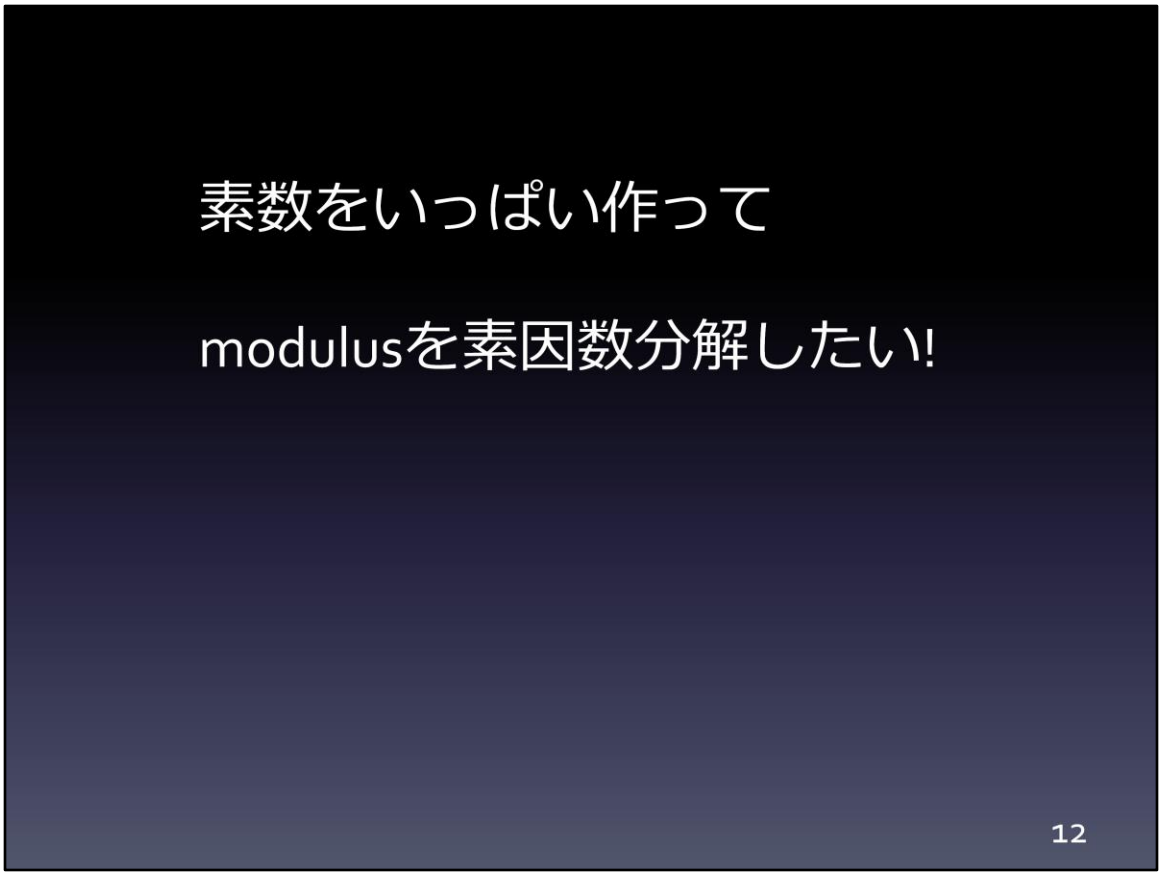
Issuer、証明書を発行した人。
Subjectは証明書の主体者、組織名とかドメイン名が入っています。これはDeNAのサーバなので、CNにdena.comと入ってますね。



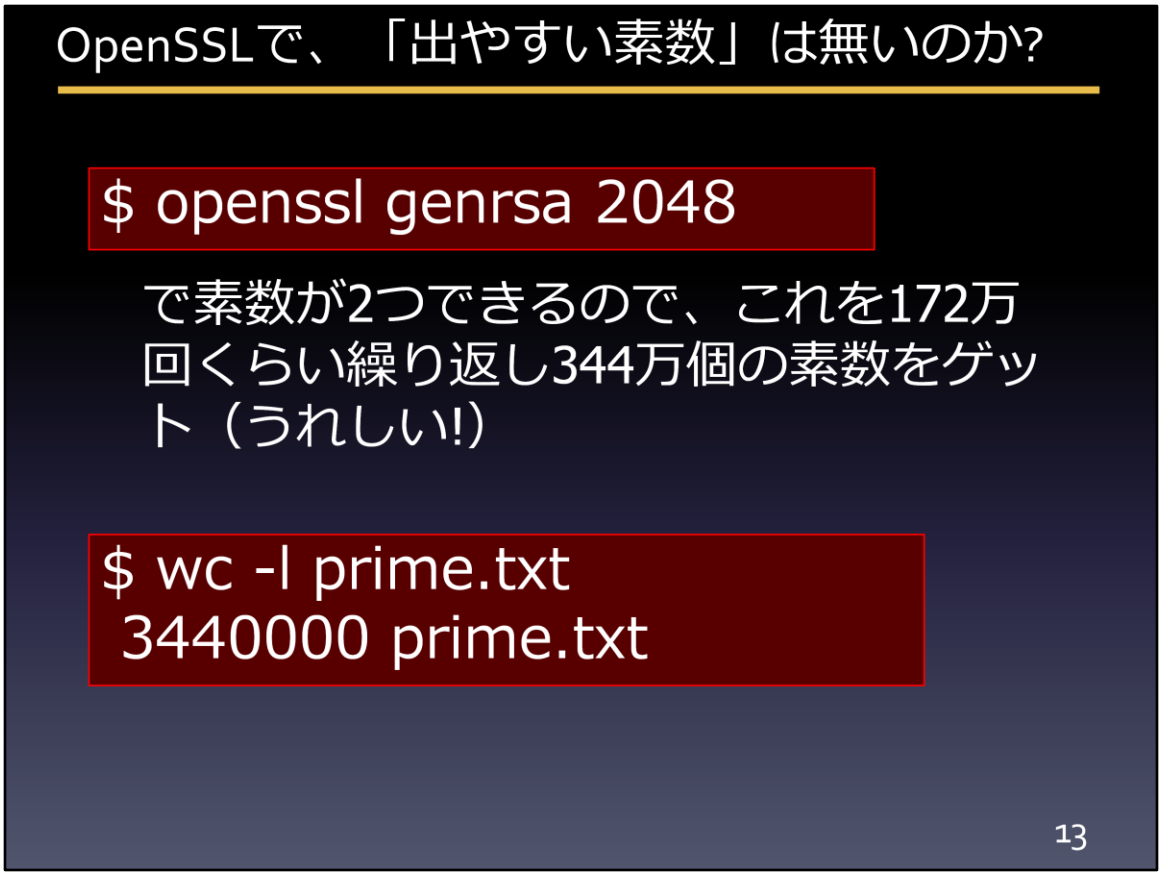
Modulusが2つの素数の積ですね。
コロン区切りの16進数で書かれています。これを素因数分解できればいいわけだ。



また、後ろにはX509v3 extensionsとして色々な拡張領域が定義されていますね。後でここも見ます。
証明書を細かく見ていくとそれだけで終わっちゃうので、次にModulusと素数の小ネタだけ話しておきましょう。



素数をいっぱい作って
modulusを素因数分解したい!

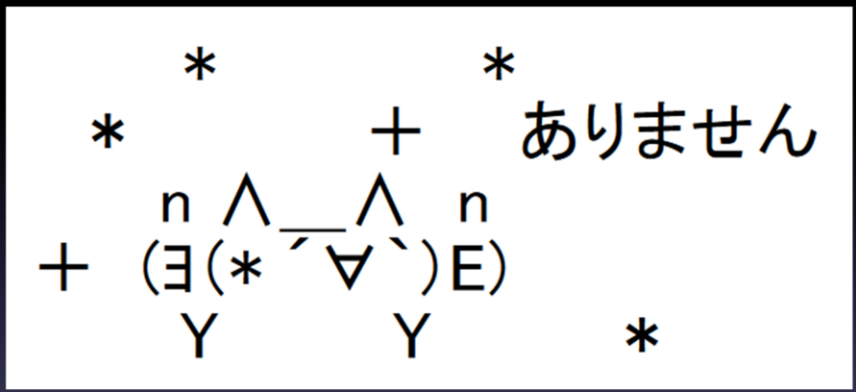


先ほどModulusを見ましたが、あれを素因数分解できれば私の勝ちなわけです。
で、まっとうに素因数分解にチャレンジするやり方よりも、こういうアプローチが考えられます。
「ふつうの人はopenssl genrsaで素数を作る」→「もしこの素数生成に偏りがあれば、出やすい素数で因数分解できるmodulusが結構あるのでは?」

これは実際、今から7,8年前のDebianで発生した事例です。

とりあえずここでは、CentOS 6.6上で、344万個の素数を作りました。HDDにこんなにたくさん素数があると思うと、わくわくしますよね。
もしこの中に、何度も出ている素数があれば私の「勝ち」なわけですが……。

「出やすい素数」



14

さて、出やすい素数は……ありませんでした。

ぜんぶuniqueだった

```
$ wc -l prime.txt
 3440000 prime.txt
$ sort prime.txt | uniq | wc -l
 3440000
```

ついでに国内の有名なHTTPSサイト200個ほどのmodulusを、340万個の素数で片っ端から割ってみたけど、割りきれる（素因数が見つかった）ものもなかった

15

この通り、作ったものからuniqして数えてみましたが一つも同じ素数は生成されませんでした。
まぁ340万個という数は実は……少なすぎるのです。

素数定理: 自然数x下の素数の個数π(x)は?

$$\pi(x) \cong \frac{x}{\ln x}$$

今、modulusが2048bitなので、2つの素数はだいたい2^1024のオーダー。

素数候補の個数

$$\pi(2^{1024}) \cong \frac{2^{1024}}{\ln 2^{1024}} = \frac{2^{1024}}{1024 \times \ln 2} \cong 2^{1014} \times 1.4$$

16

ある自然数xが与えられたとき、そのx以下に素数がどのくらいあるか？　という素数の濃度を測る際に使われるのが素数定理です。
おおむね、素数は自然対数(eを底としたlog、lnと書く)で割った値の数となります。

いま、modulus、すなわち2つの素数の積が2048bitなので、素数はおおむね2^1024のオーダーになります。
ということで素数の数は。。。だいたい2^1014(個)。

$2^{1014} \times 1.4$ 個の素数候補

- 300万（2^21くらい）個で太刀打ちできるレベルではない
  - 例えるならば、
    1巻のヤムチャ v.s. セルの完全体

17

これだけの数の素数がある中、たった300万個の素数を作ったところでヒットするわけがないわけです。
宝くじに当たるよりもずーーーーっと低い確率なので実質「衝突」しない。

前座終わり

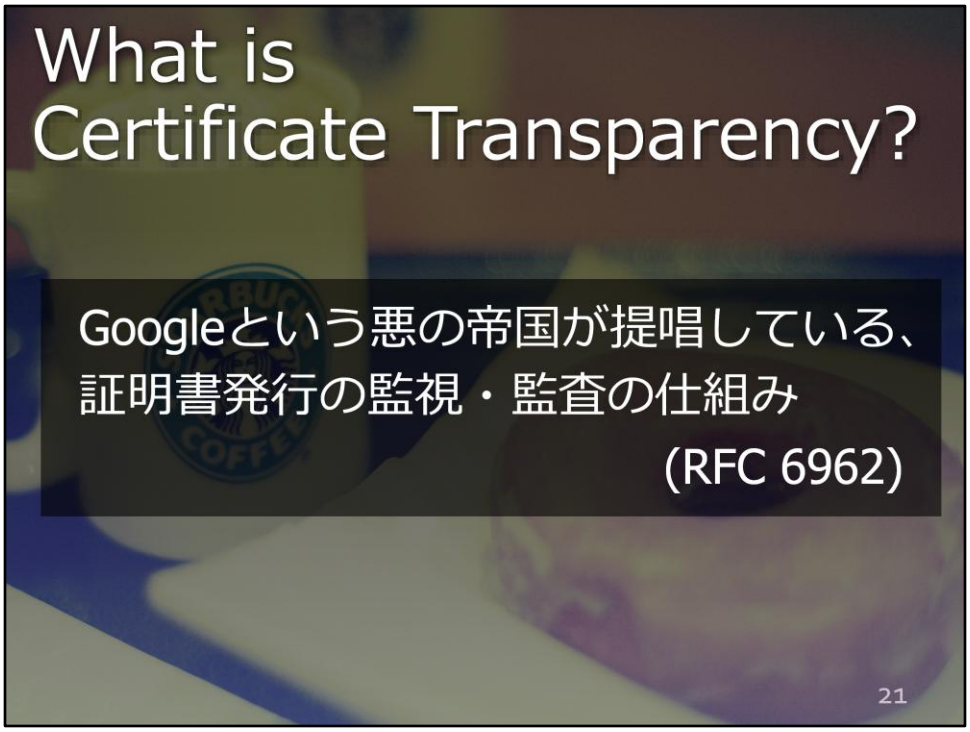
SSL証明書に親しみが湧いたところで

第二部
Certificate Transparencyに続きます

ようやく、今日のメインテーマです。
Certificate Transparencyとは何か？これは公開鍵証明書に入れるモノなので、証明書の見方が分かっていないとチンプンカンプンになってしまう。
そのため、まずは素数をテーマにちょっと証明書鑑賞をしてみたわけです。

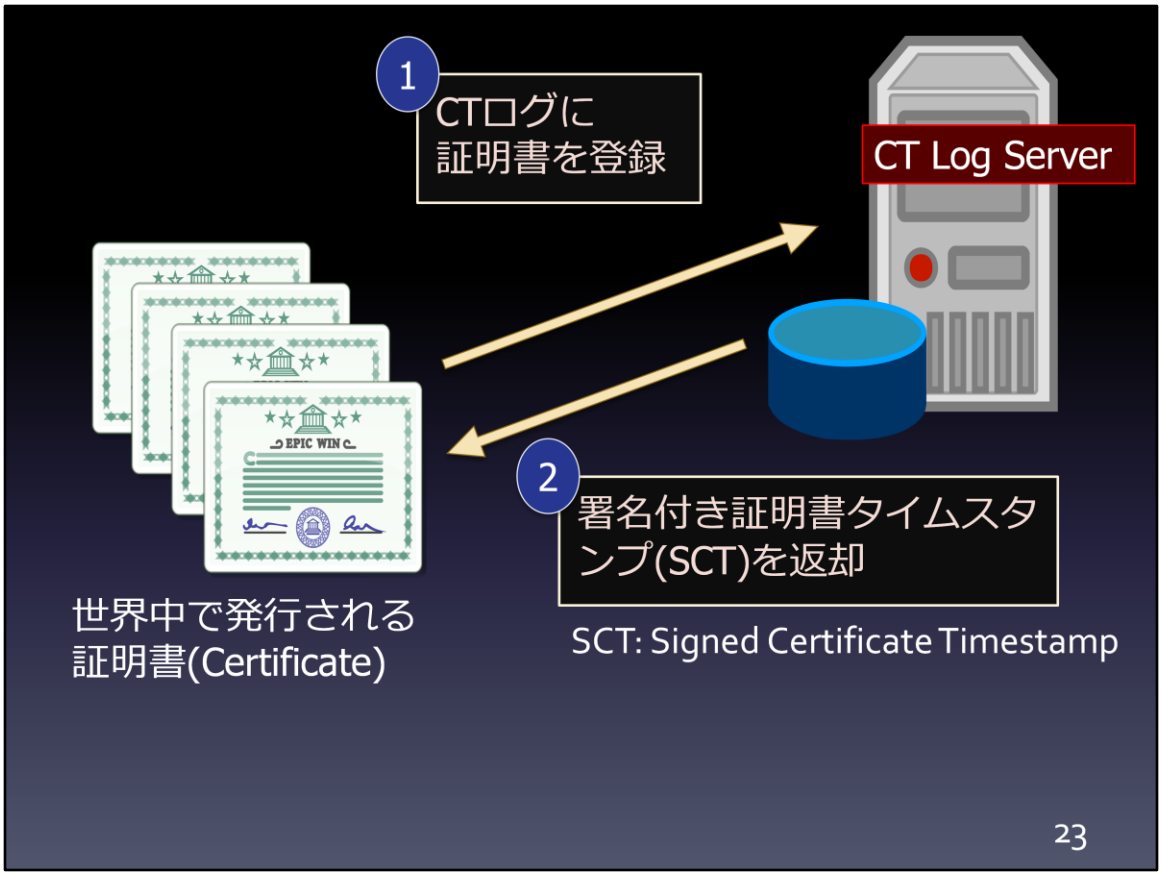
Certificateは証明書、そしてTransparencyは文脈に応じて訳すのが難しいですが、Googleは透明性と訳しています。
ここで言う透明性とは、「証明書の発行」という行為が透明であり、監査(Audit)可能であるということです。

なおこの頭文字を取って「CT」と呼びます、このスライドでも頻繁に出てきますので混乱しないでください。

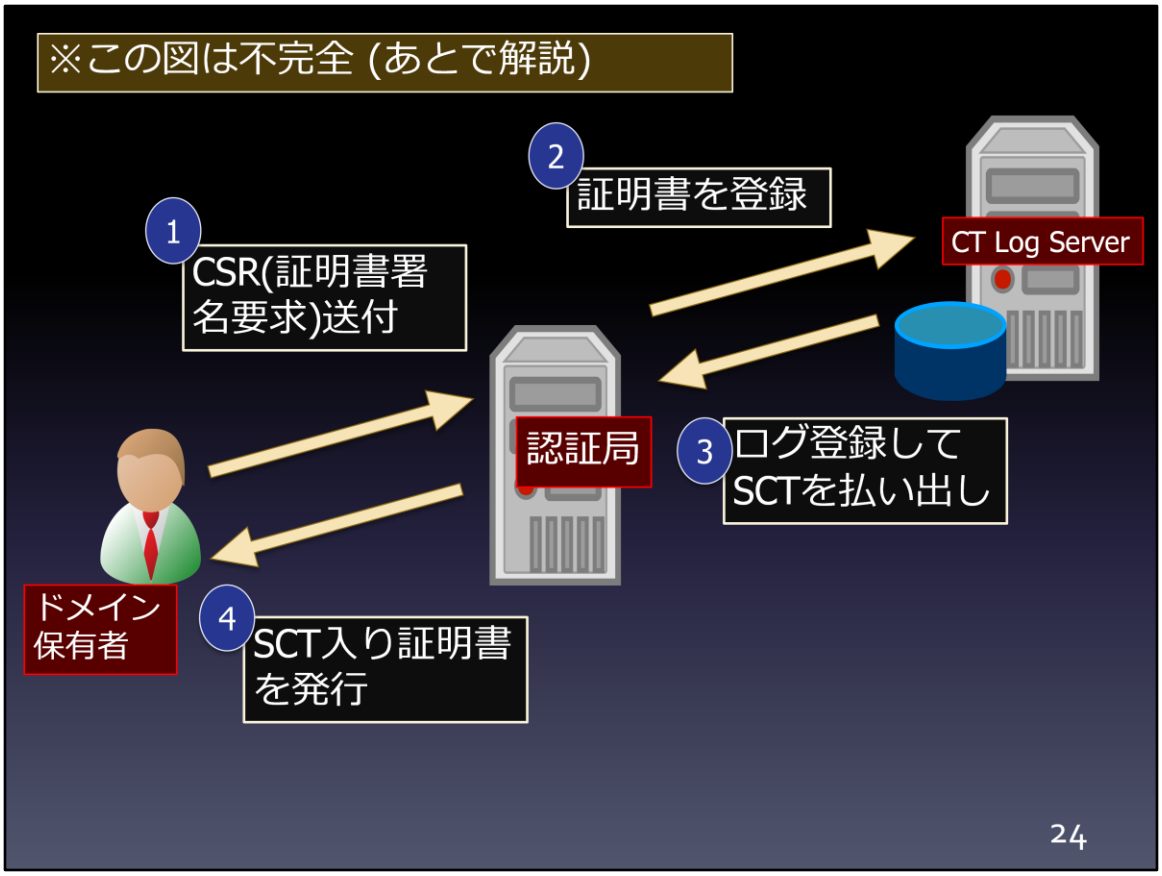


Certificate Transparencyは、皆さんご存じないでしょうがインターネットにはGoogleという悪の帝国がありまして。
CTはこのGoogleが提唱しており、SSL証明書の発行のログを誰でも参照可能な形で取ることで、監視(monitor)と監査(Audit)を可能にするものです。
既にRFC 6962(Experimental)が出ており、Google Chromeで対応しています。IEやSafariは当然まだ。

このように、ChromeでCTに対応している証明書を閲覧すると、「公開監査が可能です。」という表示と、「透明性に関する情報」というやつが出ます。

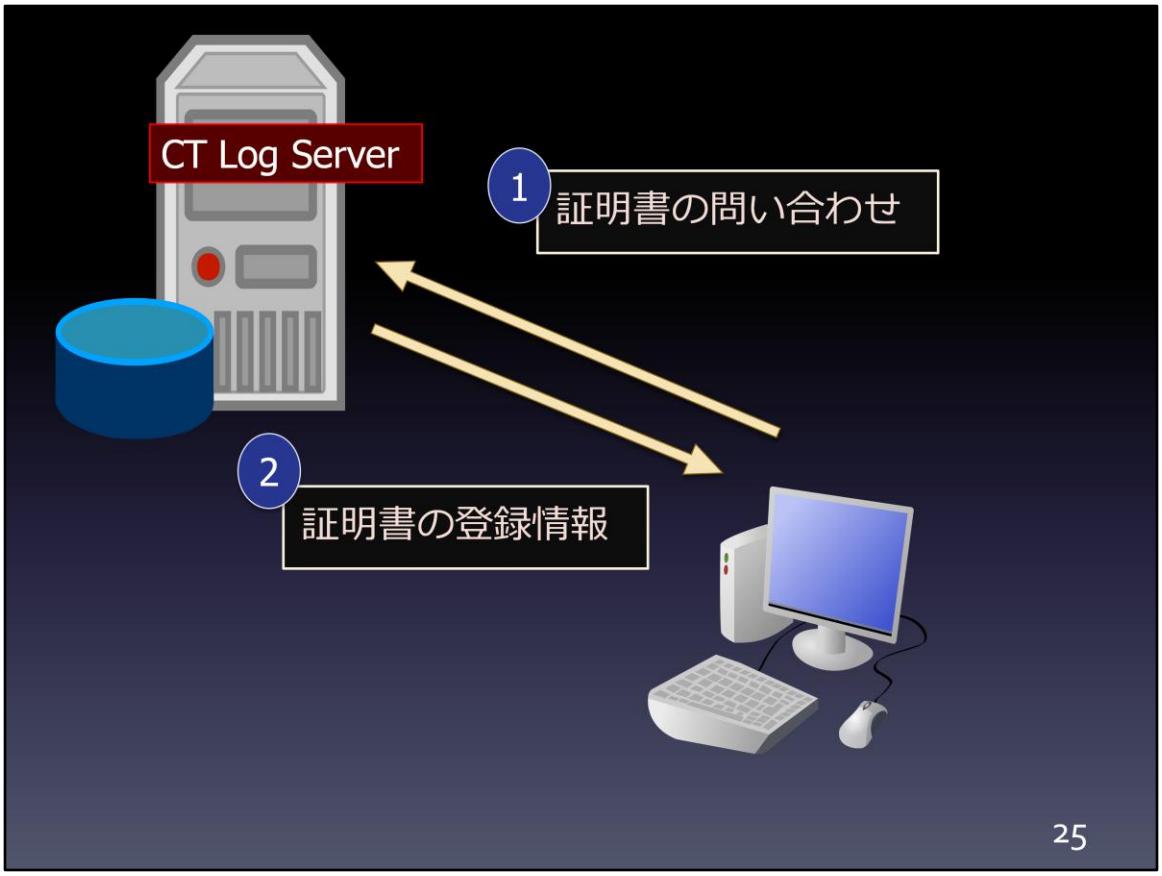


何がしたいのか。
究極の理想的には……世界中で発行されるデジタル証明書を、すべてCTログに登録したいんです。CTログサーバは、証明書が登録されるとそのログを保存し、署名を付けたタイムスタンプを返します。これをSCT(Signed Certificate Timestamp)と言います。このSCT、今後何度も出てくるので覚えておいてください。証明書をCTログに登録時に発行される、タイムスタンプです。



実際には、証明書はドメイン保有者が認証局に依頼するのが普通ですね。そのためこのような流れになります。
なお、この図は細かい部分をはしょっているので実は不正確です、それはあとで解説します。今は流れをまず理解するために簡略しています。

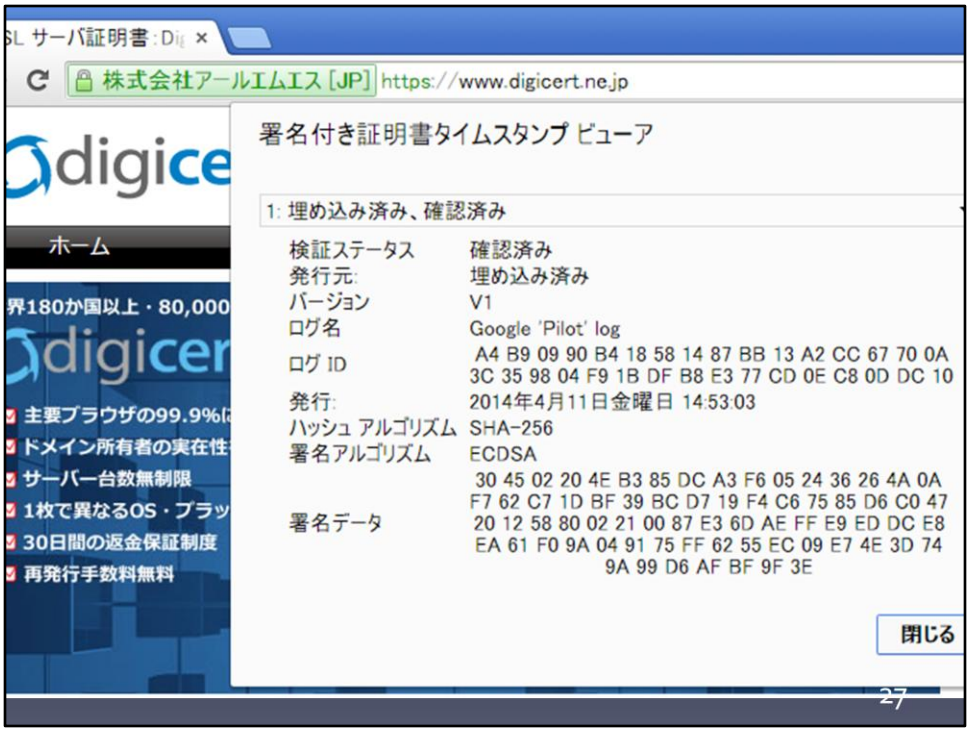
（具体的には、SCTを払い出してSCT入り証明書を作る部分が、Precertificateを作らないといけないのでこの図では正確ではない）



そして、CTログサーバは一般公開されているため誰でも参照可能です。
それがナニが嬉しいのかは、ちょっと後で解説します。

Certificate Transparencyですが、これはGoogleが提唱しているものなので、今のところ対応しているブラウザもChromeだけです。
それもMac版Chromeではダメで、今はWindows版Chfomeしか対応していないようです。

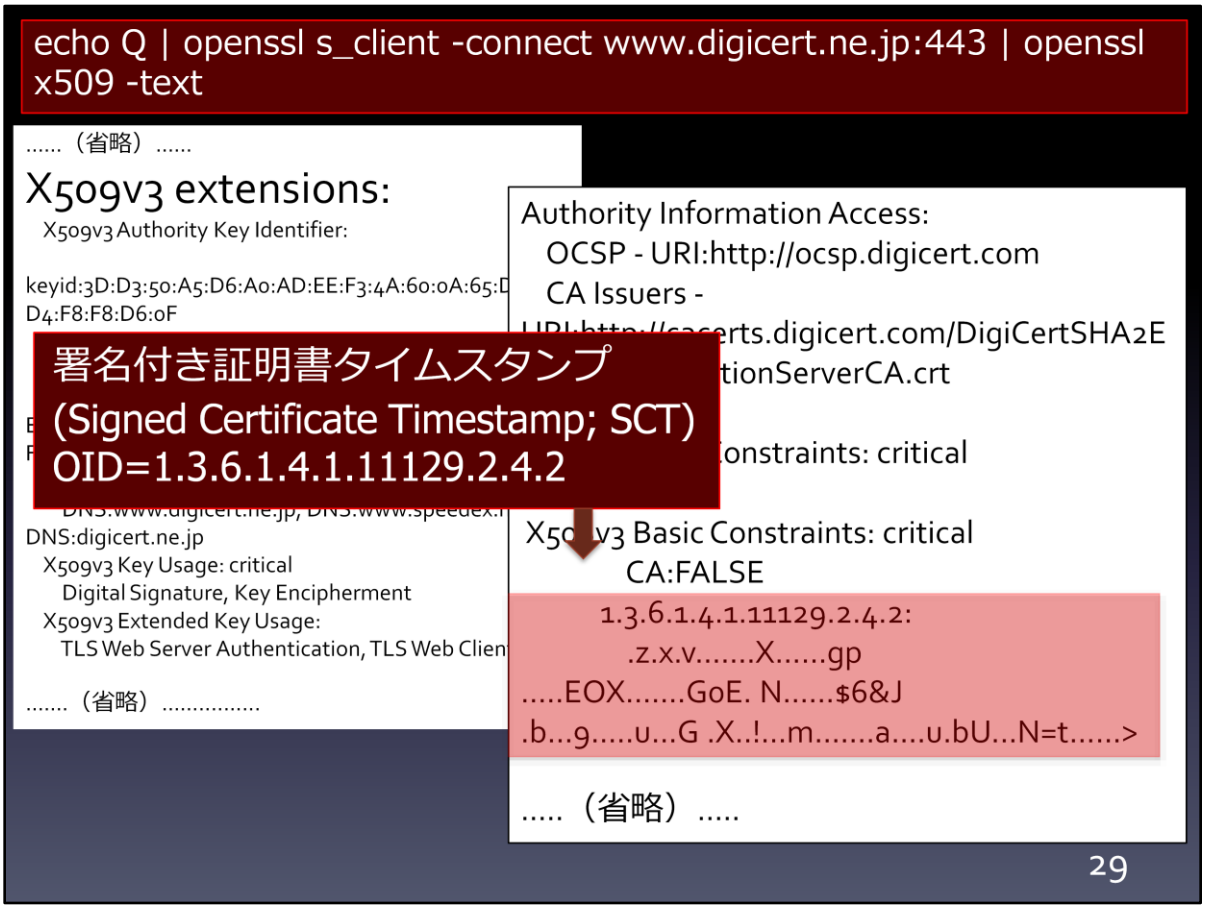
Chromeには既にCTを確認する機能が実装されているので、簡単に確認できます。
DigiCertなど、対応しているWebを見てみましょう。この通り、「公開監査が可能です」と出ています。また、「透明性に関する情報」から詳しいログ情報を見ることもできます。



先ほどの「透明性に関する情報」をクリックすると、このように監査ログが表示できます。
ここで出ているログ名「Google 'Pilot'」がCTログサーバのひとつです。

一方、これはCOOKPADの証明書ですが、監査ログが無いのでこのようなメッセージが出ます。「公開監査記録がありません。」とかなんだか気になる表示です。
CTはGoogleが提唱して普及させようとしているものなので……こういう不安を煽るようなメッセージは、わざとだと思います。悪の帝国のやり口ですね。

それにしてもCOOKPAD、言い方は悪いですがレシピサイトにEV証明書とは、随分まぁ金持ちですなぁ～。



なおSCTは、先ほどOpenSSL手打ちで見たX509 Extensionsという領域に格納されています（実は規格上はそうではない形式のものもあるんですが、誰も使っていないので省略します）
opensslでも、フィールド名は出ませんが、このようにOIDそのままで良ければCTな証明書かは確認することができます。(最新のOpenSSL 1.0.2aなら対応しています)
OID=1.3.6.1.4.1.11129.2.4.2

ここに付いているのが、先ほどの図で証明書登録時にCTログサーバから払い出されたタイムスタンプ、SCT(Signed Certificate Timestamp)ですね。

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…	利用者(Webブラウザ)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

30

Certificate Transparency, 何が嬉しいか。

CTログサーバは別にCA認証局などだけでなく、誰でも閲覧できます。
皆さんも普通にURLを叩いてアクセスできますし、Webブラウザもアクセスします。

こうして多数の目による監視によって、不正な証明書発行、あるいは誤った証明書を検知したいというのが目的です。

例えば皆さんがmicrosoft.comのサーバ管理者だったとして、CTログサーバを定期的にチェックしてmicrosoft.comドメインへの証明書発行がされていないかを監視します。
ある日、自分は発行していないのにwww.microsoft.comの証明書が発行されたログがあれば、誰かが不正に証明書を発行した!?と検知できるわけです。

Certificate Transparency, (Googleには)何が嬉しい?

- 世界中の証明書を手元に持つことができる
  - 証明書の種類、ドメイン名などのデータ
  - 認証局の証明書販売数の把握
- 認証局に対して、「上から目線」になれるカードを1枚持つことができる(SCTの発行)
- CTログサーバを、Googleが悪意を持ってアレをナニしないとは限らない

31

先ほどのが表向きの理由ですが。
おそらく悪の帝国Googleのメインの目的はこちらだと思います。何より、このようなログサーバを運営していると、世界中で発行されるSSL証明書が自動的に手元に集まってきます。
そのようにインターネットのトラヒックやリソースに関する大量のデータ収集というのは、あの悪の帝国が常々狙っているところです。
大量の証明書を収集することで、今後のデータ利用に繋げたいのでしょう。

また、もしGoogleが悪意を持ってログサーバに何かしらの細工をするかも……ということも当然考えないといけません。
このようなことを考えると、例えばMacのSafariがCTに対応することはまず無いと思います(GoogleとAppleの仲の悪さは、まぁなんとなく分かりますよね)

Chromeの~~横暴な~~計画

「Chromeでは、CTログに登録されていないEV証明書は、EVインジケータの表示をやめる」と宣言
（緑色の表示をしなくなると思われる）

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

32

またChromeの横暴で注意すべき点があります。

実はChromeは既に、CTログに対応していないEV証明書では緑表示をやめるということを宣言しています。（なんて身勝手な!）
銀行サイトなどでは、「安心のために緑表示を確認してください」という言い方をしていますが、あれができなくなってしまう。

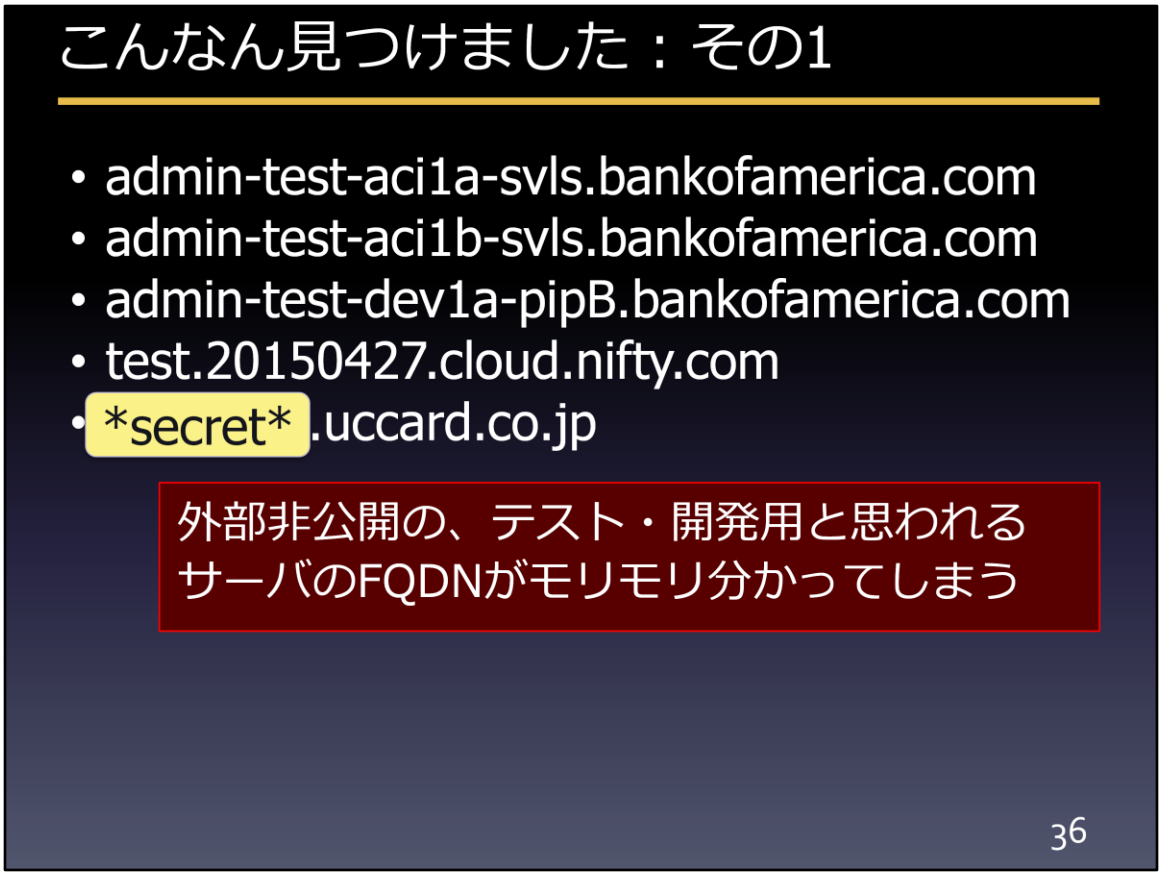
ですからEV証明書を使う場合、CTログに対応させるか、あるいはChromeで緑表示されないことを無視するか、の2拓になります。
なお、Googleに証明書を提出して「どうかホワイトリストに載せてください」と頼むこともできます。現実的に、もう結構なサイトがこのホワイトリスト登録で対応しています。

気をつけろ! これが悪の帝国の兵器だ!

ひるめしを食べようと会社を出たところで、悪の帝国の車を見つけたので撮りました。
そのうち、私が写真を撮っている様子の写真が地図に載ります。

次にCertificate Transparencyのイヤなところも見ていきます。

私がイヤだな……と思ったのはこれですね。
今回の発表に当たってCTログから色々データを取得してみたのですが、少しクロールしてみると、結構色んな情報が分かるなぁ～、これあんまり出しちゃいけないんじゃないかなぁ～、というのが率直な印象です。



例えば上の3つはBANK Of Americaのものですが、見るからにテスト用のサーバですよね。
4つめは、ニフティクラウドの何かですね。
あるドメインへの攻撃をする際、攻撃者はホスト列挙という行為を行うのですが、それが簡単にできます。

なお一番下のはUCカード、カード会社のものだったので……たぶんテスト用サーバだろうなというFQDNでしたが、変なちょっかいを受けるとイヤなので、これは出さないことにしておきます。

こんなん見つけました：Citrix XenApp

- citrix.●●●●.com
- citrix.■■■■.com
- citrix.▼▼▼▼▼.com
- citrix.○○○.de
- など……

maskしてます

他にも、こんな列挙ができました。Ctrix XenAppという、デスクトップ仮想化のサーバが簡単に列挙できました。

CTにより、証明書を利用するサーバのFQDNを秘密にすることができなくなる

- We don't need metasploit anymore.
  - `msf > use auxiliary/gather/dns_enum`
- 関係者にしかFQDNを教えないことは、もちろん「気休め」でしか無い。でも気持ち悪い。
- この他、商品名などを入れたFQDNがサービスイン前に分かってしまう
  - (新サービス名?).(会社名).co.jp

38

というMetasploitを使わなくてもCTログから、攻撃対象ドメインのFQDN列挙が可能になります。

また、FQDNから新サービスの名前が分かってしまうかもしれない。

認証局がCTログを(勝手に)登録していいの?

トレンドマイクロの主張

http://esupport.trendmicro.com/solution/ja-JP/1106400.aspx より引用

Certificate Transparency への対応について：

（略）....また、あらゆるドメインに対して発行された証明書について、誰でも調べることができます。これは、SSL 証明書のセキュリティ上の問題にも見えますが、（中略）CT Log では、外部に公開されていない情報を閲覧することはできません。

内部サーバをご利用で、サーバの情報を CT Log に登録したくない場合は、OV 証明書を発行してください。現在 CT Log に登録されるのは EV 証明書のみです。

39

さてこうなると、そもそも証明書を発行するときにそんな外部の第三者のサーバに登録しないで欲しい、というニーズも出てくるでしょう。
しかし、例えばトレンドマイクロのWebページにはこのように書かれています。
http://esupport.trendmicro.com/solution/ja-JP/1106400.aspx

なんと、FQDNの秘匿という観点では、EV証明書よりもOV証明書の方がセキュアです。逆転現象が起きています。

認証局がCTログを(勝手に)登録していいの?

トレンドマイクロの主張

http://esupport.trendmicro.com/solution/ja-JP/1106400.aspx より引用

Certificate Transparency への対応について：

CTログに登録されたくなければ、EV証明書は諦めてください。

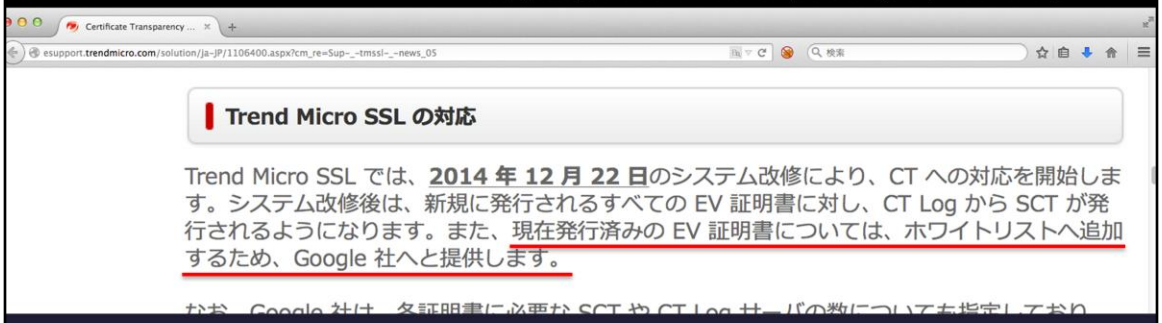
インに対して発行された証明書に
バの情報を CT Log に登録したく
行してください。現在 CT Log に登録されるのは EV 証明書のみです。

40

なんだかぼかして書いていますが，要するにEV証明書をCTログに登録されることからは逃れられません。

既存の証明書もホワイトリストとして提出

トレンドマイクロ Q&A http://esupport.trendmicro.com/solution/ja-JP/1106400.aspx



現在発行済みのEV証明書については、
ホワイトリストへ追加するため、
Google社へと提供します。

41

さらに、Google(悪の帝国)は、CTログに登録せずに発行された証明書については、ホワイトリストを作っているから受け付けるよ! という声明を出しています。
このホワイトリストに入れてもらわないと、EV証明書なのにChromeで緑色のインジケータが出ない、ということになります。これを重視して、一部の認証局はホワイトリスト登録を既にしてしまっています。

トレンドマイクロはこのように、ホワイトリストを提出済みです。一方、DigiCertは、「EV証明書を再発行すれば今はCTログに乗るから、そうしてくれ」というスタンスのようです。

次にCertificate Transparencyの見方について。

CT LogsはAPIなので、人間には見づらい

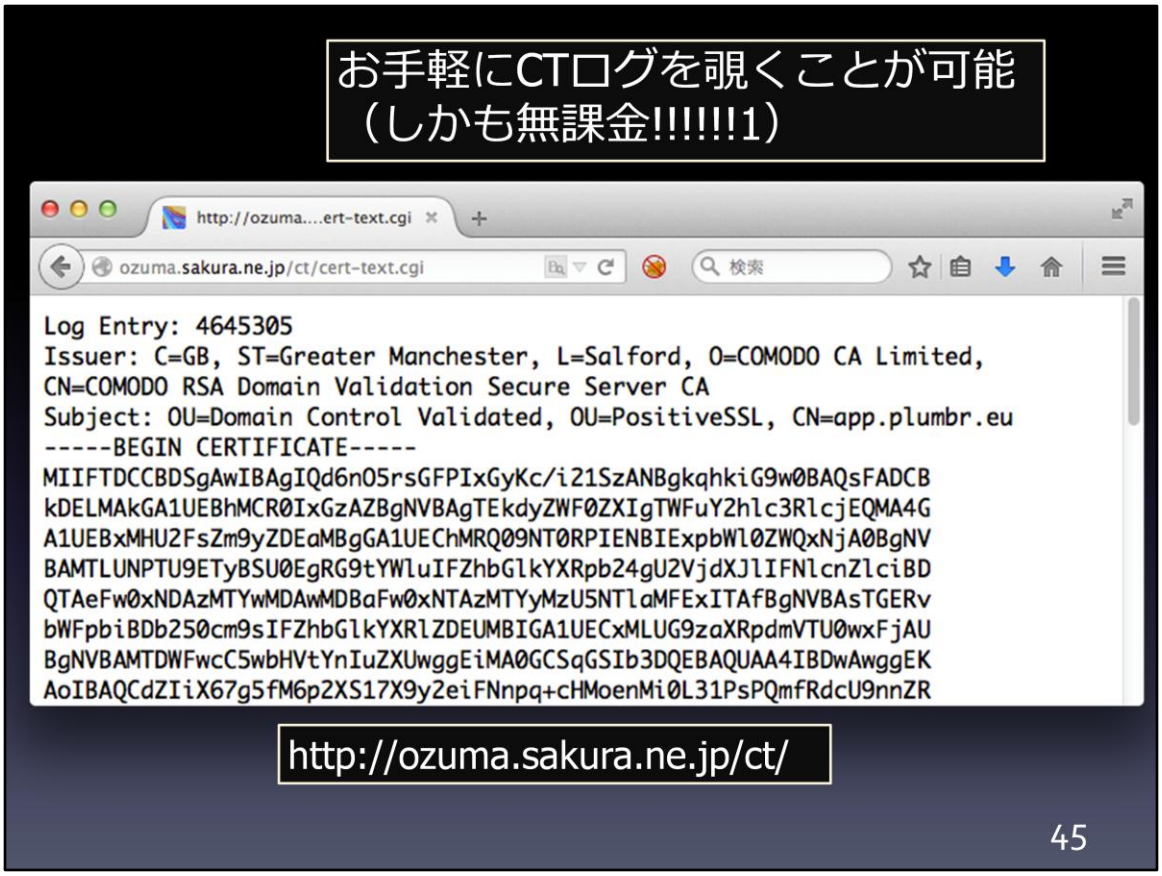
Retrieve Entries from Log:

https://ct.googleapis.com/aviator/ct/v1/get-entries?start=1&end=1

最初の方でCTログは誰でも参照可能と言いました。
https://ct.googleapis.com/aviator/ct/v1/get-entries?start=1&end=1
確かにそうなのですが、実はこれがAPIしか提供されておらず、人間が見るにはなかなかキツい状態となっています。

というわけで、作ってみました。簡単にCTログを見るためのツール、Certificate Transparencyガチャです。
http://ozuma.sakura.ne.jp/ct/

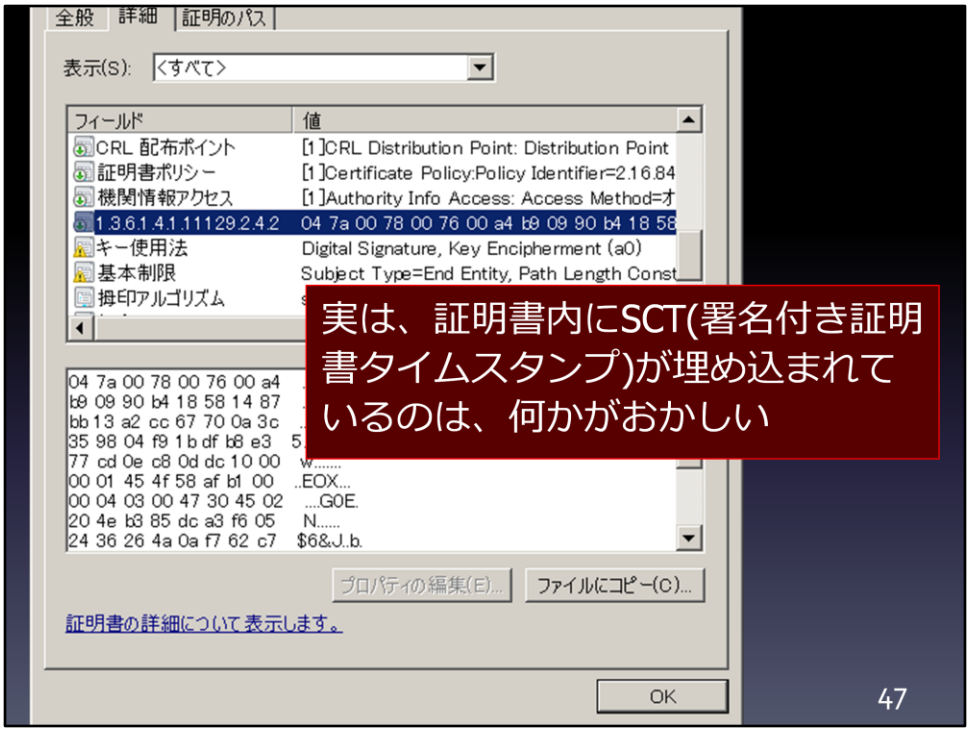
CTログには通し番号が振られているので、それを入れてもいいですし、下の「ガチャ」でランダムに引くこともできます。なんとこのガチャ、課金が不要です!!!!!!!1



何度かやってみると、レアFQDNとか引けるかもしれません。なかなかヒマつぶしになります（自画自賛）。

http://ozuma.sakura.ne.jp/ct/

時間が無いので発表できなかったこと



先ほど何気なく、証明書に確かにSCT（覚えていますか? 要するにCTログから発行されたタイムスタンプです）が埋め込まれているのを見ましたが……
鋭い人はもう気がついているでしょうが、これ、おかしな話なんです。

続きはブログで

- CT対応して証明書にSCTを入れるには、事前証明書(Precertificate)という気持ち悪いものを作らないといけない
- これはあまりスマートではない（と思う）

- 後日ブログに書こうと思います

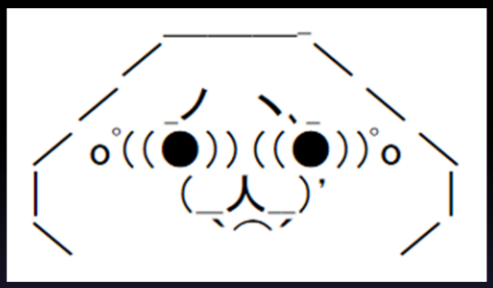
48

CTログに、タイムスタンプ（SCT）をもらうにはまず証明書を作らないといけない。この時点では、当然SCTはまだ付いていない。
しかし皆さんがさっき見た証明書には、SCTが付いていた。なぜ？

実は証明書にSCTを入れるには、事前証明書(Precertificate)という気持ち悪いものを作らないといけないのです。
これは、後に発行する証明書と同じシリアルIDを持つなど、あまりスマートではない（と思います）。

後日ブログに書こうと思います
　→書きました。
http://d.hatena.ne.jp/ozuma/20150516/1431769141

Certificate Transparency (個人的な感想です)



なんだか気持ちわるいお。。。
主要ブラウザには実装して欲しくないお。。。
でもFirefoxも対応するらしいお。。。

https://threatpost.com/mozilla-to-support-certificate-transparency-in-firefox/109819

49

FirefoxのCT対応
https://threatpost.com/mozilla-to-support-certificate-transparency-in-firefox/109819

デフォルトではONにしない、とは言っています。

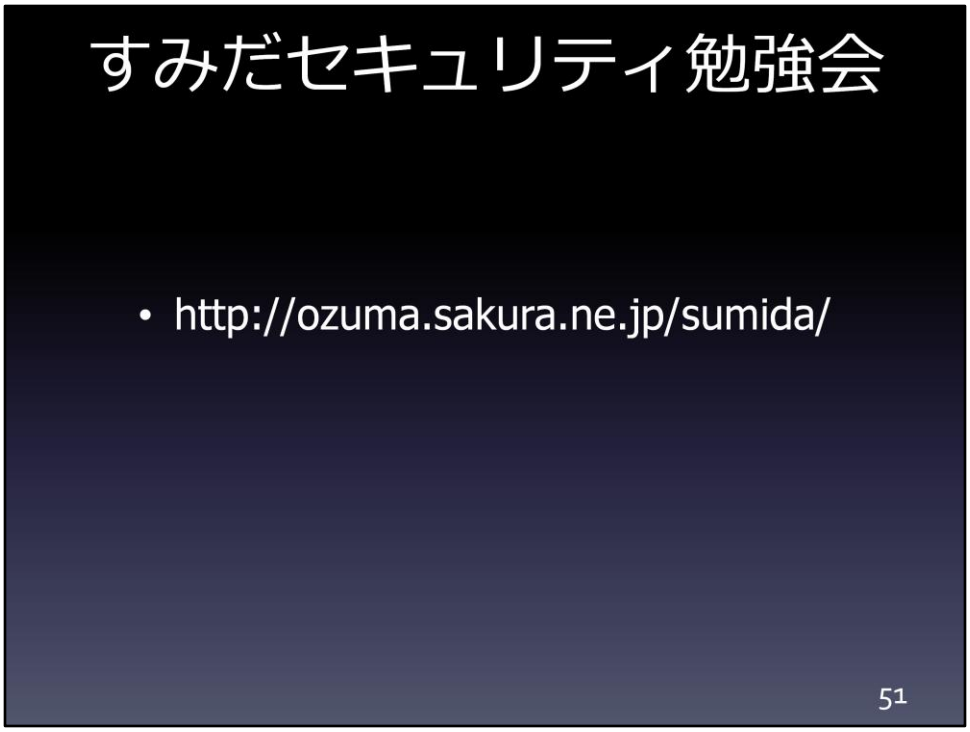
参考

- GMO GlobalSignさんの記事が大変参考になりました。
  - https://jp.globalsign.com/blog/2014/certificate_transparency.html

50

GMO GlobalSignさんの記事が大変参考になりました。

https://jp.globalsign.com/blog/2014/certificate_transparency.html



すみだセキュリティ勉強会

http://ozuma.sakura.ne.jp/sumida/