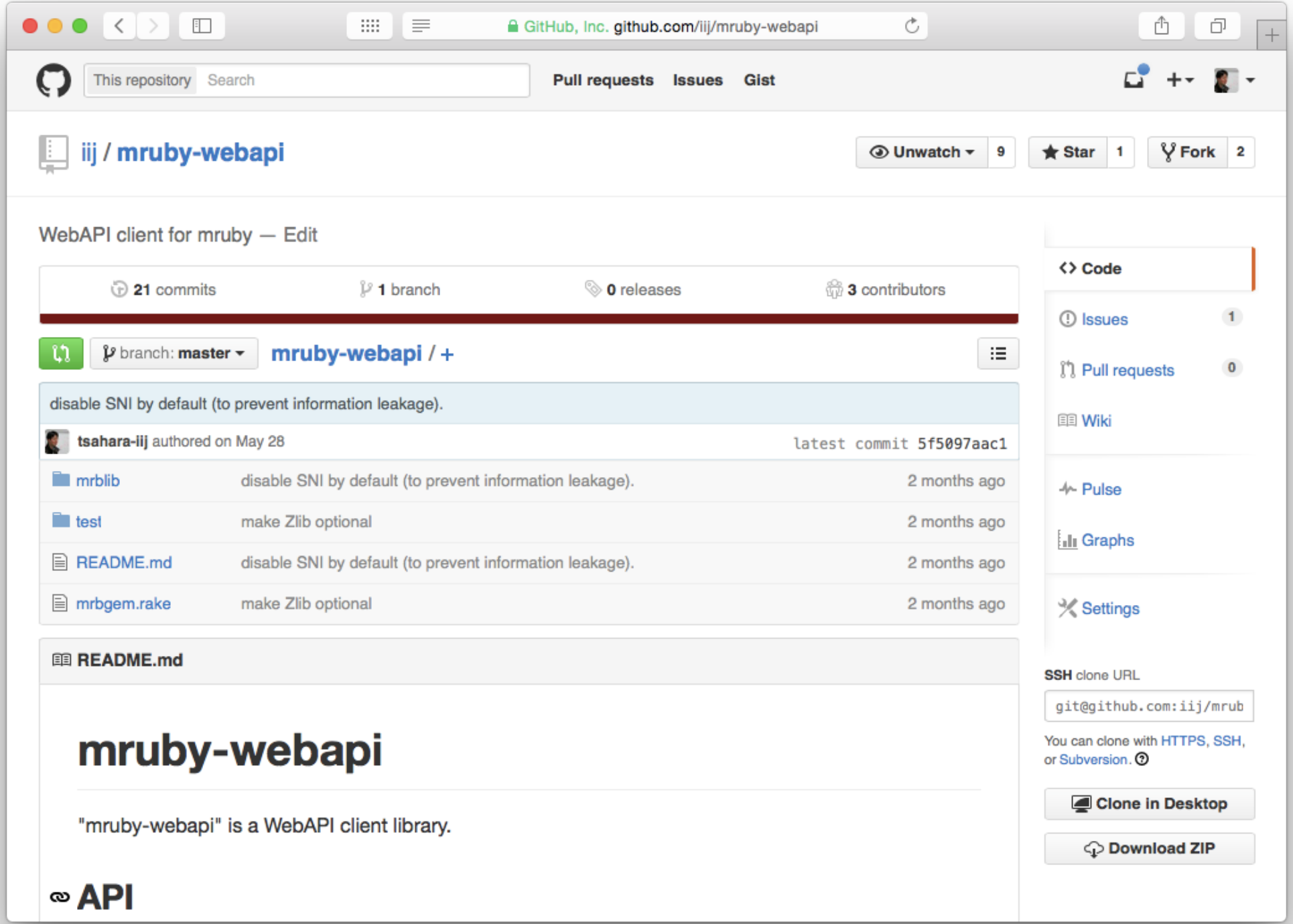
DNSとTLSのビミョーな関係

佐原 具幸

株式会社インターネットイニシアティブ

HTTPSクライアント


GitHub, Inc. github.com/iij/mruby-webapi
This repository
Search
Pull requests
Issues
Gist
iij / mruby-webapi
Unwatch 9
Star 1
Fork 2
WebAPI client for mruby — Edit
21 commits
1 branch
0 releases
3 contributors
branch: master
mruby-webapi / +
disable SNI by default (to prevent information leakage).
tsahara-iij authored on May 28
latest commit 5f5097aac1
mrblib disable SNI by default (to prevent information leakage). 2 months ago
test make Zlib optional 2 months ago
README.md disable SNI by default (to prevent information leakage). 2 months ago
mrbgem.rake make Zlib optional 2 months ago
README.md
mruby-webapi
"mruby-webapi" is a WebAPI client library.
API
Code
Issues 1
Pull requests 0
Wiki
Pulse
Graphs
Settings
SSH clone URL
git@github.com:iij/mrub
You can clone with HTTPS, SSH, or Subversion.
Clone in Desktop
Download ZIP

作っていて困ったこと。

ドメイン名とTLSの関係

TLS といえば

HTTPS が代表格

HTTPS は
HTTP を安全にしたもの

何をもって

「安全」

と言っているのか？

ブラウザが HTTP で
取ってきた内容
HTML/CSS/JavaScript

と

ブラウザの上の方に表示されている

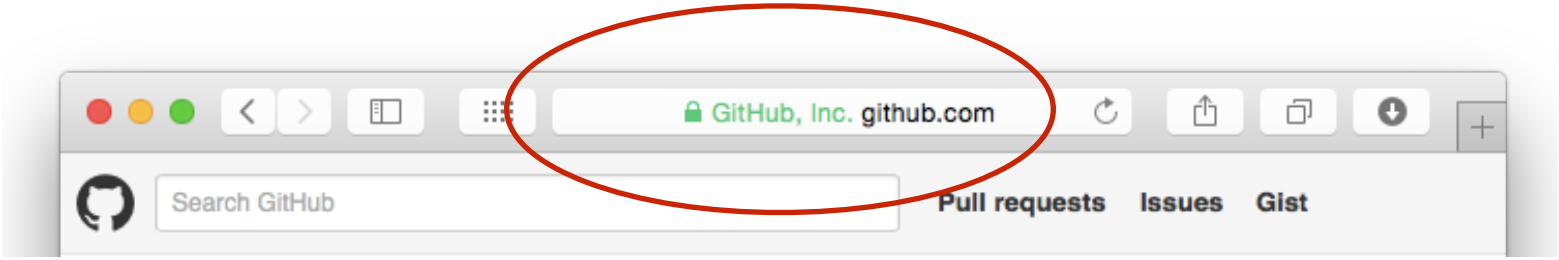
謎の文字列


www.ietf.org
I E T F
Search
Chat Live with the
IETF Community
The Internet Engineering Task Force (IETF®)
The goal of the IETF is to make the Internet work better.
The mission of the IETF is to make the Internet work better by producing hi

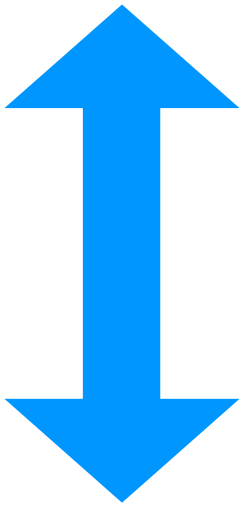
の 対応付け が、

OS / ブラウザの開発元が認めた、
認証局によって保証されている、
証明書を使って検証されたこと、
をもって 安全 だとしている。

EV証明書だと
もうちょっと
わかりやすい


GitHub, Inc. github.com
Search GitHub
Pull requests
Issues
Gist

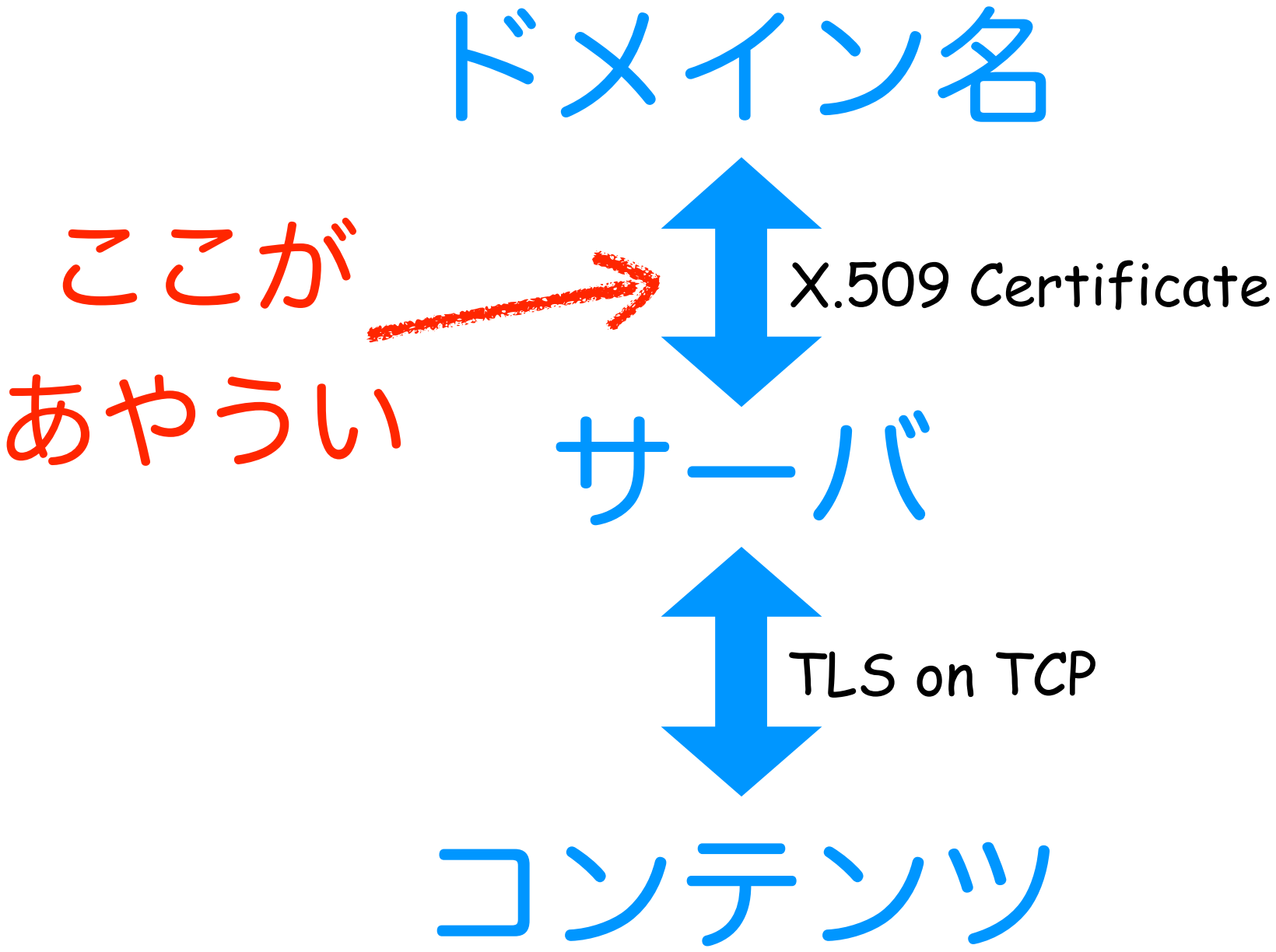
ドメイン名



コンテンツ

(HTML等)

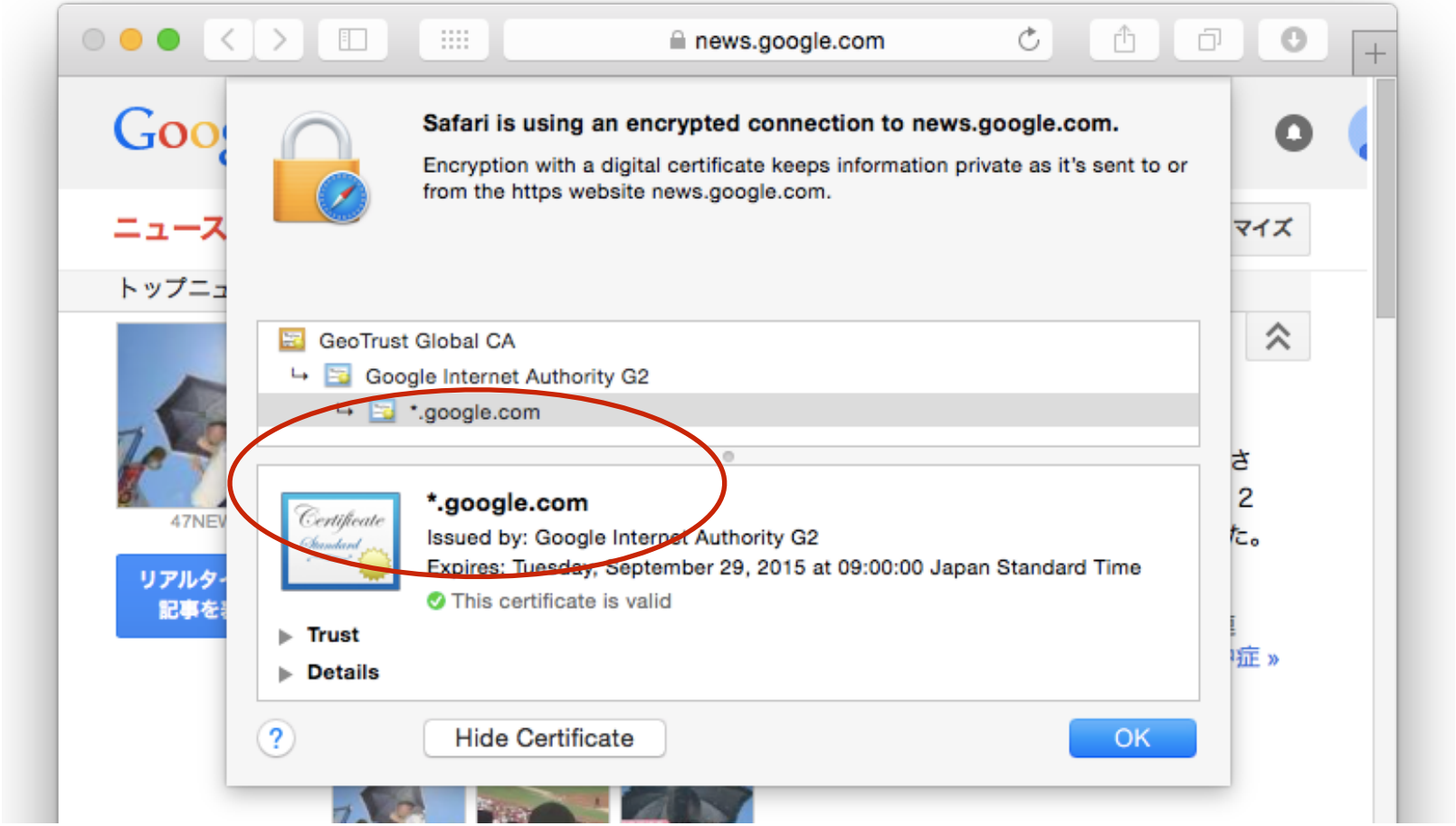
実はまだ
ギャップ
がある


ドメイン名
ここが
あやうい
X.509 Certificate
サーバ
TLS on TCP
コンテンツ

キモ(いの)は

ワイルドカード証明書

広く使われている技術


news.google.com
Safari is using an encrypted connection to news.google.com.
Encryption with a digital certificate keeps information private as it's sent to or from the https website news.google.com.
GeoTrust Global CA
Google Internet Authority G2
*.google.com
*.google.com
Issued by: Google Internet Authority G2
Expires: Tuesday, September 29, 2015 at 09:00:00 Japan Standard Time
This certificate is valid
Trust
Details
Hide Certificate
OK

ワイルドカード文字

＊(スター)

は任意の文字列にマッチ

images.google.com

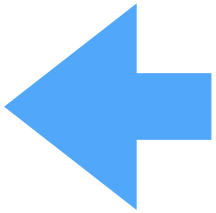
maps.google.com

news.google.com

play.google.com

plus.google.com

video.google.com



*.google.com

なんて便利 ♥

ん？ ひょっとして…

最強の証明書

"*"

RFC2818 3.1.:

> Names may contain the wildcard character * which is considered to match any single domain name component or component fragment.

Safari can't verify the identity of the website "www.gorillavid.in".

The certificate for this website is invalid. You might be connecting to a website that is pretending to be "www.gorillavid.in", which could put your confidential information at risk. Would you like to connect to the website anyway?

☐ Always trust "*" when connecting to "www.gorillavid.in"

*

*

Self-signed root certificate

Expires: Saturday, June 26, 2021 at 09:32:12 Japan Standard Time

⚠ This certificate has not been verified by a third party

▶ **Trust**

▶ **Details**

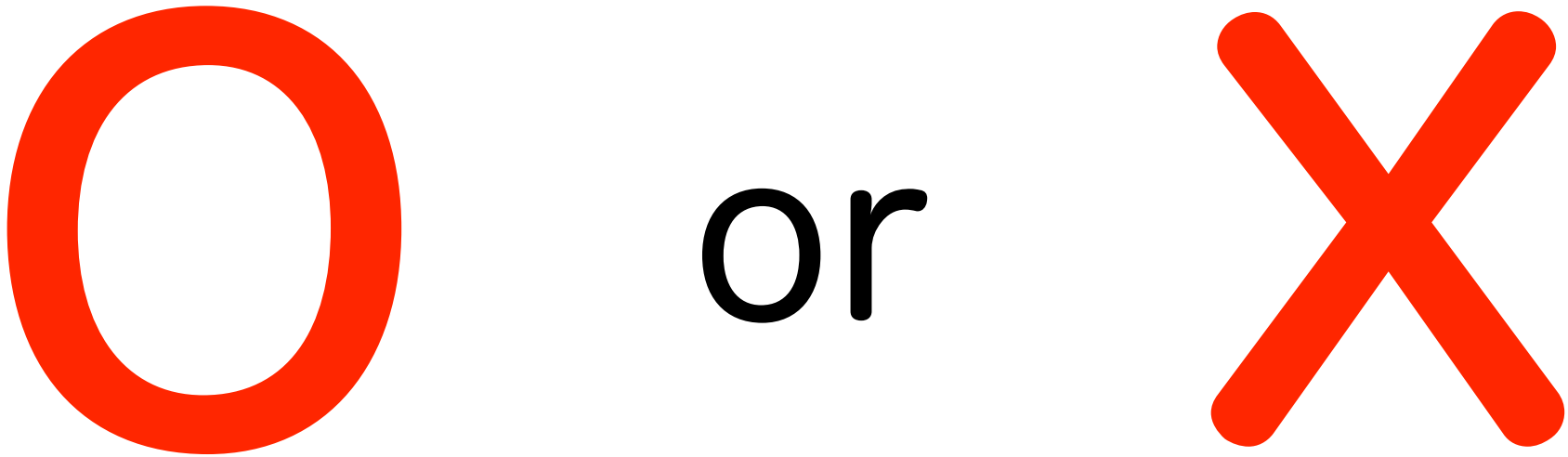
?

Hide Certificate

Cancel

Continue

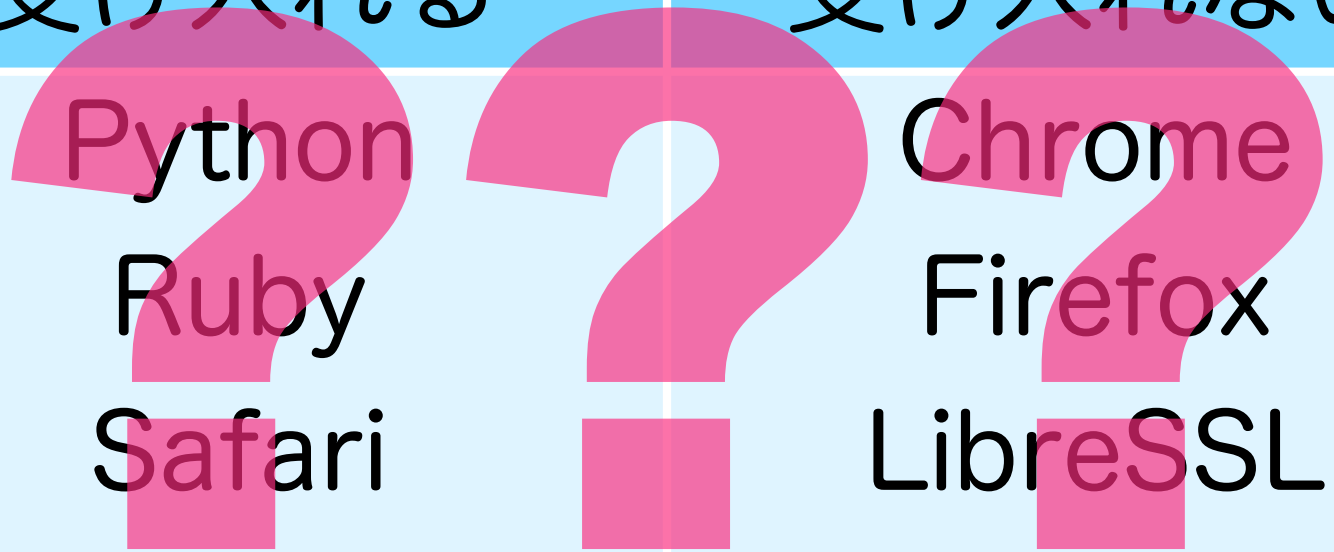
では “*.jp” なら？


O
or
X

実装依存... orz

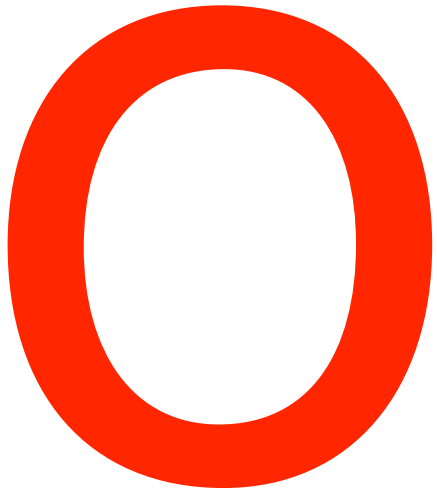
"*.jp" というワイルドカード証明書を

受け入れる	受け入れない
Python	Chrome
Ruby	Firefox
Safari	LibreSSL
curl (Mac)	curl (OpenSSL)
wget	



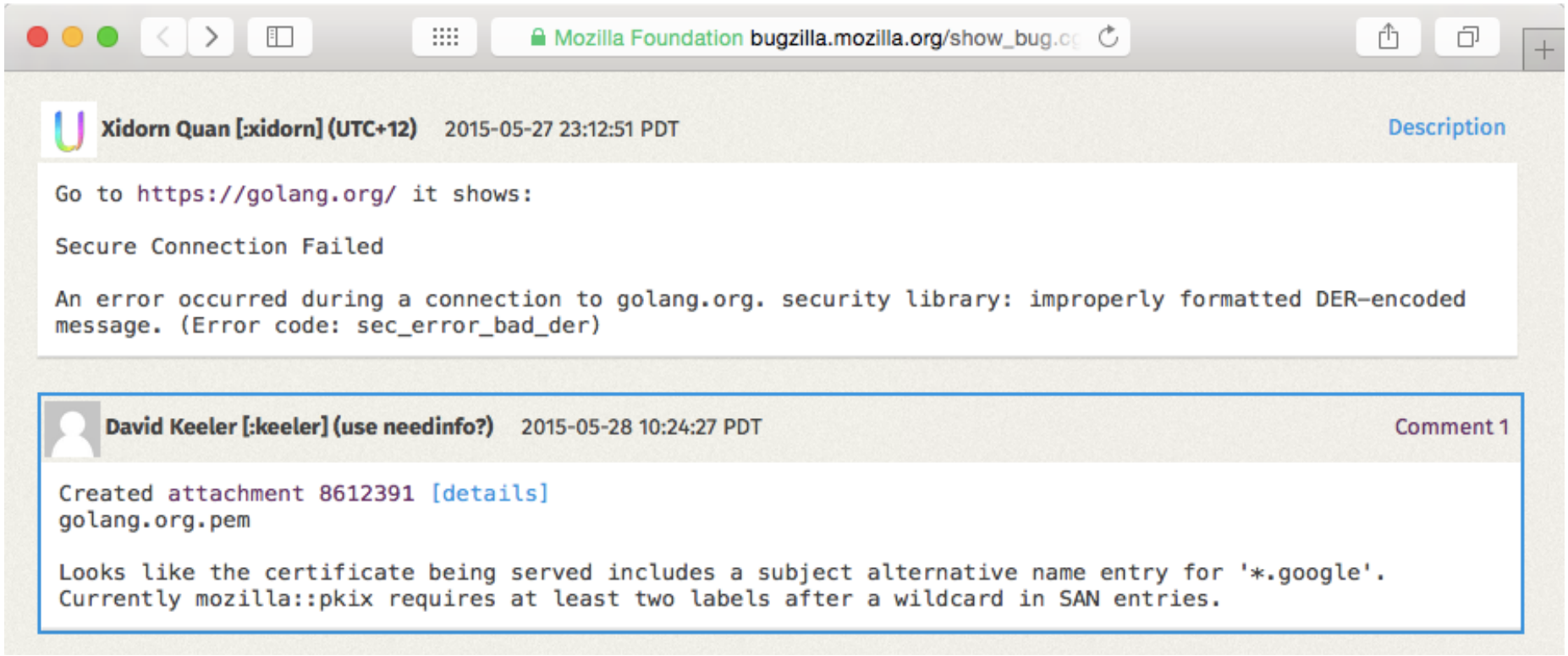
"*.jp" なんて証明書を
信じるのは脆弱性だ！
直せばいいじゃないか

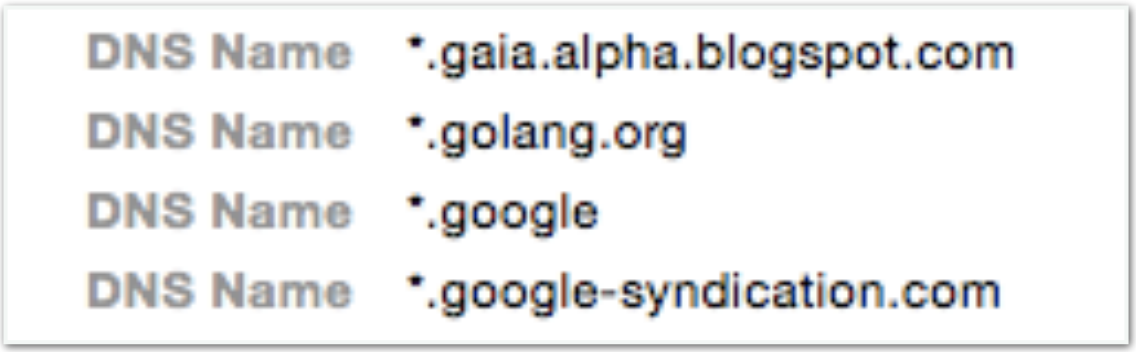
では “*.google” なら...?



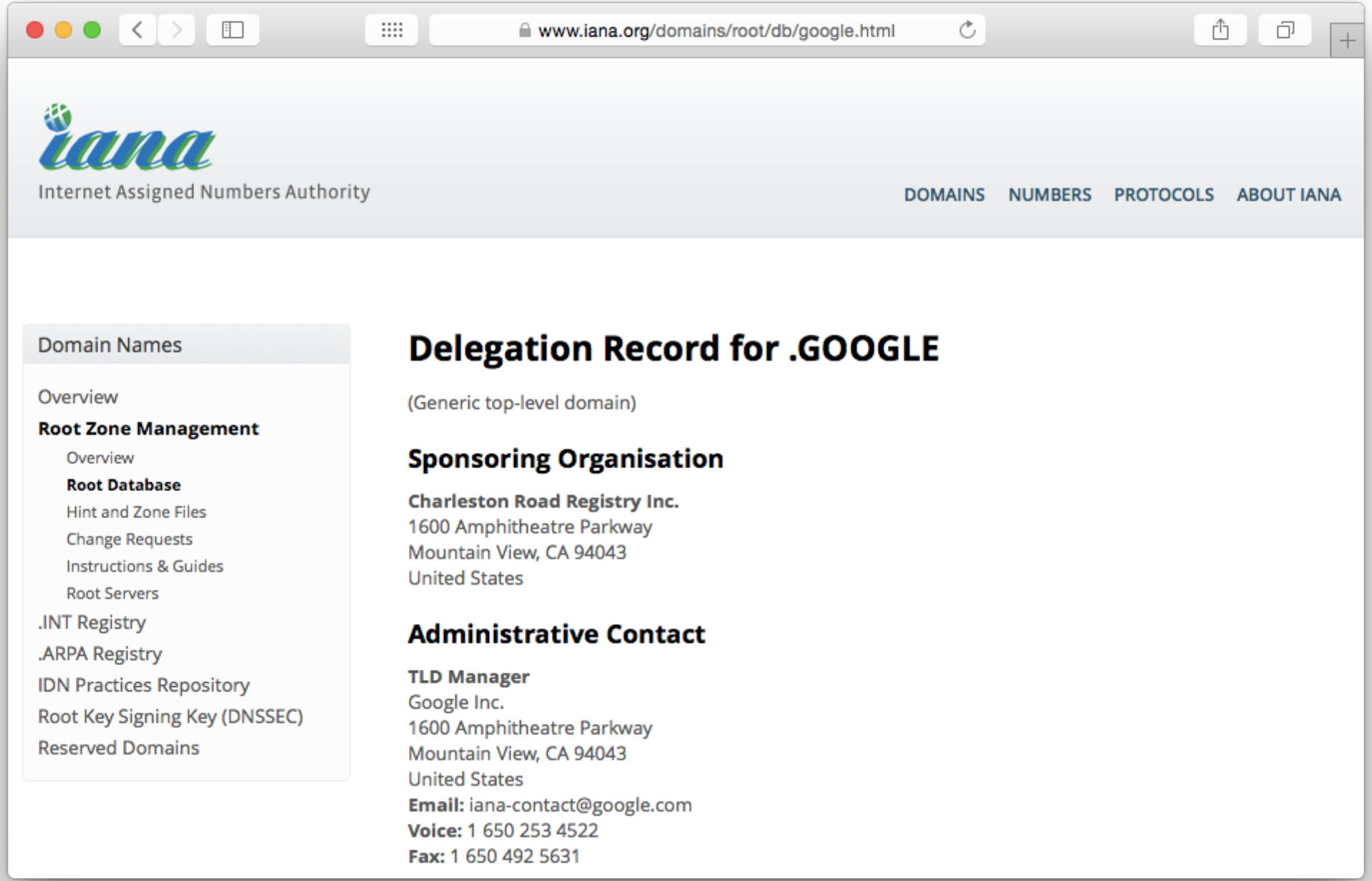
or

状況は “*.jp” と変わらない。


Mozilla Foundation bugzilla.mozilla.org/show_bug.cg
Xidorn Quan [:xidorn] (UTC+12) 2015-05-27 23:12:51 PDT
Description
Go to https://golang.org/ it shows:
Secure Connection Failed
An error occurred during a connection to golang.org. security library: improperly formatted DER-encoded message. (Error code: sec_error_bad_der)
David Keeler [:keeler] (use needinfo?) 2015-05-28 10:24:27 PDT
Comment 1
Created attachment 8612391 [details]
golang.org.pem
Looks like the certificate being served includes a subject alternative name entry for '*.google'.
Currently mozilla::pkix requires at least two labels after a wildcard in SAN entries.


DNS Name *.gaia.alpha.blogspot.com
DNS Name *.golang.org
DNS Name *.google
DNS Name *.google-syndication.com

えー、何も悪いこと
してないのに。


www.iana.org/domains/root/db/google.html
iana
Internet Assigned Numbers Authority
DOMAINS
NUMBERS
PROTOCOLS
ABOUT IANA
Domain Names
Overview
Root Zone Management
Overview
Root Database
Hint and Zone Files
Change Requests
Instructions & Guides
Root Servers
.INT Registry
.ARPA Registry
IDN Practices Repository
Root Key Signing Key (DNSSEC)
Reserved Domains
Delegation Record for .GOOGLE
(Generic top-level domain)
Sponsoring Organisation
Charleston Road Registry Inc.
1600 Amphitheatre Parkway
Mountain View, CA 94043
United States
Administrative Contact
TLD Manager
Google Inc.
1600 Amphitheatre Parkway
Mountain View, CA 94043
United States
Email: iana-contact@google.com
Voice: 1 650 253 4522
Fax: 1 650 492 5631

要するに単一の管理主体の元に運営されていると証明できれば良い?

あ、これどこかで聞いた。

Public Suffix List !

と、いうわけで

ワイルドカード証明書の検証にも

Public Suffix List

を使う時代が来てしまうかも…？

おしまい