

# 90分で分かるサーバ証明書の最新動向 ～いまTLSとトラストが熱いんです～

## パネルディスカッション

# パネルディスカッション

---

- **パネリスト**

- 大津繁樹氏(ヤフー株式会社)
- 島岡政基氏(セコム株式会社 IS研究所)

- **モデレーター**

- 木村泰司(日本ネットワークインフォメーションセンター)

# HTTPS使ってますか？

- 全部
- 一部
- まだ
- 使うつもりはない

# 「常時SSL化」できない 理由は何です？

# ディスカッション

**(導入前)**  
**HTTPSを導入するために  
何を考えればいいのか？**



# HTTPSを導入するために 何を考えればいいの？

常にソフトウェアを最新にする。

大津さん

設定すればいいレベルに洗練されてきた。間違った知識を踏まないように。

スライドあり

島岡さん

# Mozilla SSL Configuration Generator

サーバを選択

- Apache
- Nginx
- Lighttpd
- HAProxy
- AWS ELB

設定プロファイルを選択

- Modern
- Intermediate
- Old

Server Version

OpenSSL Version

HSTS Enabled

必要に応じてバージョンなどを指定

apache 2.2.15 | intermediate profile | OpenSSL 1.0.1e | [link](#)

Oldest compatible clients: Firefox 1, Chrome 1, IE 7, Opera 5, Safari 1, Windows XP IE8, Android

リファレンス設定が表示される

各ブラウザのどのバージョンから利用可能な設定か確認できる

```
...
SSL Engine on
SSLCertificateFile /path/to/signed_certificate
SSLCertificateChainFile /path/to/intermediate_certificate
SSLCertificateKeyFile /path/to/private/key

# Uncomment the following directive when using client certificate authentication
#SSLCACertificateFile /path/to/ca_certs_for_client_authentication

# HSTS (mod_headers is required) (15768000 seconds = 6 months)
Header always set Strict-Transport-Security "max-age=15768000"
...
</VirtualHost>

# intermediate configuration, tweak to your needs
SSLProtocol all -SSLv2 -SSLv3
SSLCipherSuite ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-S
SSLHonorCipherOrder on
```



**(導入済み)  
HTTPSと証明書の運用で  
考えるべきことは？**

# HTTPSと証明書の運用で 考えるべきことは？

将来的な短期化に備え  
自動化。

大津さん

自動化。(弊社これから  
ですごめんなさい)

島岡さん

色々「熱い」ようですが、  
どの証明書を使ったらいいの？

# どの証明書を使ったらいいの？

すっかりコモディティ化した。最後はサポート。

大津さん

自動化されたら証明書の主な外部リスクは認証局BAN。よってサポート重要。

島岡さん

# Webブラウザは今後どうなっていくのか

# Webブラウザは今後どうなっていくのか

十分でかくなかった。  
IoT時代を乗り切れる  
か。

大津さん

(ルータストアプロバイダ  
の側面だけ)質から量へ。  
無謬性から可用性の世界  
へ。

島岡さん



**(もう一歩つっこんで)  
今後、どうなっていくのか**

# 今後、どうなっていくのか

Googleがブチ切れる  
未来の先にある世界。

大津さん

IoT用クライアントや  
プライベートなTLSな  
ど、プライベートな空  
間だが多様なクライア  
ントで、という状況は  
増えつつある。

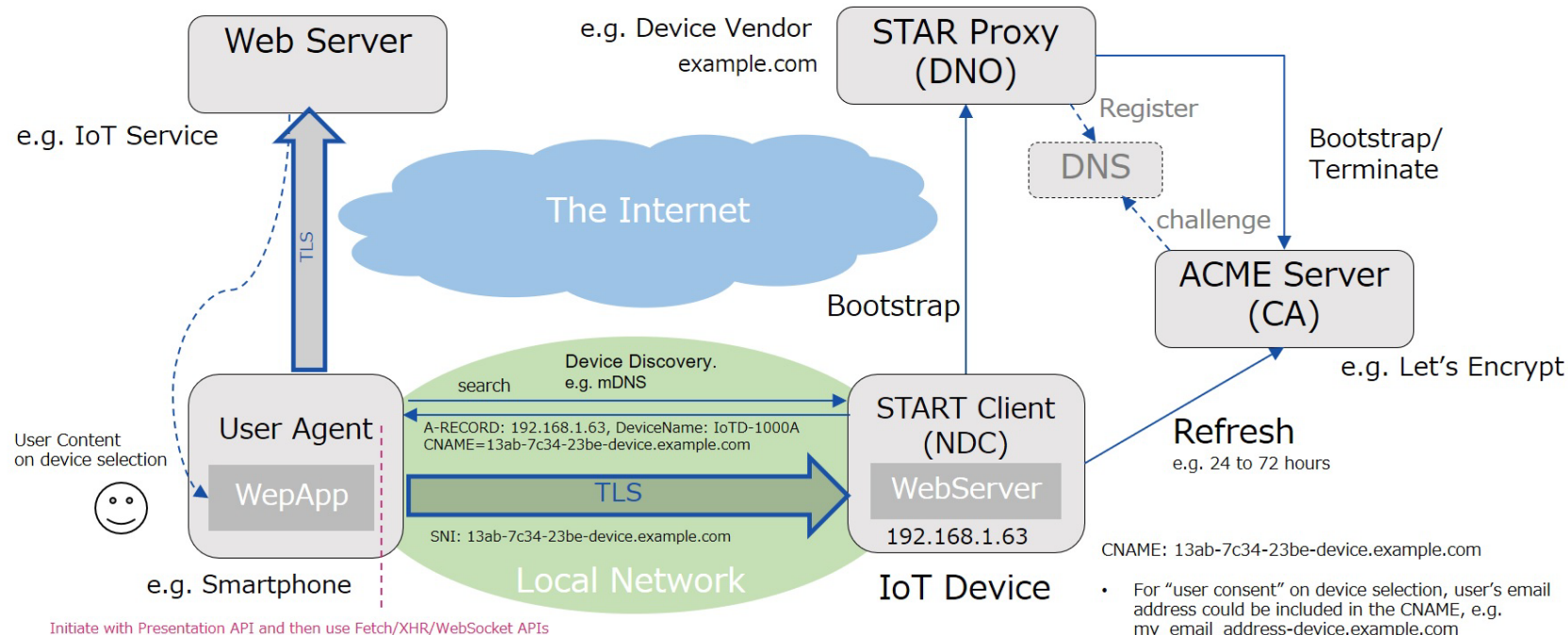
スライドあり

島岡さん

# ローカルネットワークでのTLS(一例)

## HTTPS in local network featuring STAR

- IoT device is configured to get a short-term server cert. via STAR Proxy and refresh the server cert. with ACME server
- On TLS handshake with IoT device, User Agent verifies the server cert. with CNAME in Device Discovery
- For User Content, User Agent shows green colored DeviceName and CNAME by checking with “pre-flight”.



**私たちがウォッチしていくべき  
もの。考えておくべき事。**

# 私たちがウォッチしていくべきもの。 考えておくべき事。

PKIステークホルダーの寡占化、独占化。

スライドあり

大津さん

認証局インシデント。  
プライベート空間の  
TLS。

島岡さん

# おわり