国際会議から知っておくべき技術標準

IP meeting

2023年11月22日(水)

木村泰司

一般社団法人 日本ネットワークインフォメーションセンター

この話について

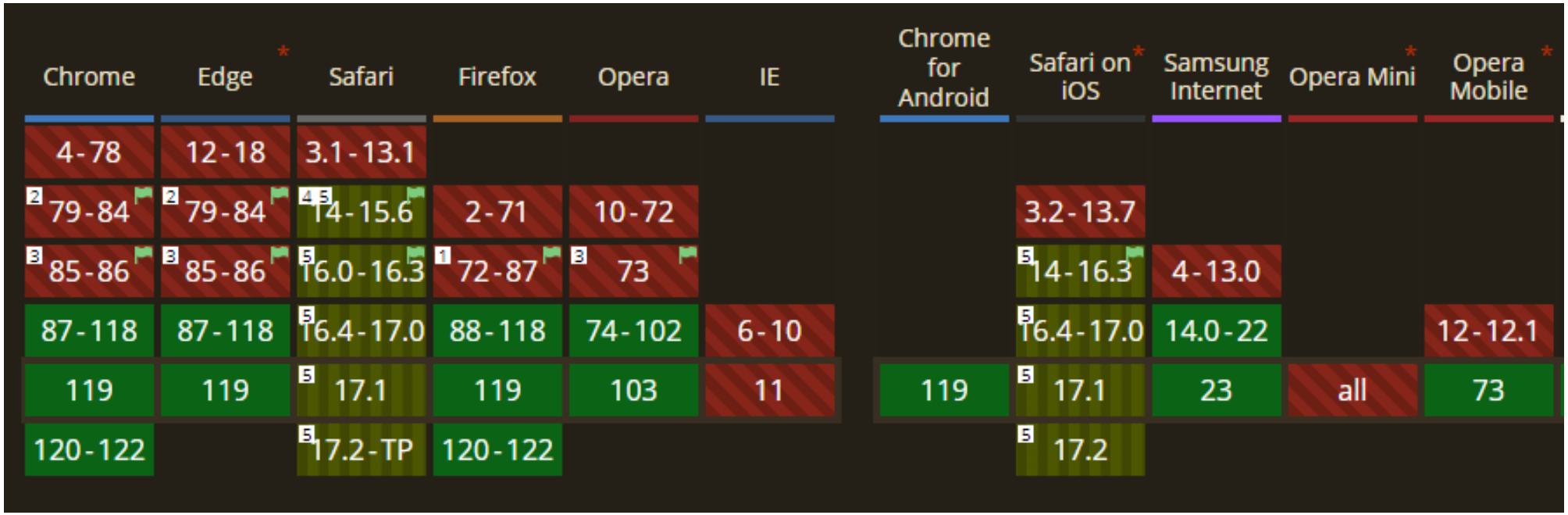
- **中期的な観点でIETF等の標準化動向をみていく。**
- **最近の話題をお届け。**

俯瞰して捉えていく標準化動向に関する勉強会を開催しています。その勉強会を中心としたトピックと木村によるピックアップです。

中期的な動き - Web関連

中期的な動き - Web関連

- QUICとHTTP/3



出典：HTTP/3 protocol | Can I use... Support tables for HTML5, CSS3, etc
https://caniuse.com/http3

中期的な動き - Web関連

- **QUICとHTTP/3に至るまで**

年	プロトコルとバージョン	内容
1991年	HTTP/0.9	GETのみ
1996年	HTTP/1.0 (RFC1945)	GET/POST/HEAD リクエスト対応、ステータスコード対応、Basic認証
1997年	HTTP/1.1 (RFC2608)	複数リクエスト、Keep-Alive対応、 Proxy詳細対応
		:
2015年	HTTP/2.0 (RFC7540)	ストリームと多重化（TCP + TLS）
2021年	QUIC (RFC9000)	UDP、ストリームごとのflow制御、TLS1.3のハンドシェイク
2022年	HTTP/3.0 (RFC9114)	HTTPセマンティクスをQUICストリームにマッピング

QUICを使う他の仕組み
- DNS over QUIC (DoQ) RFC9250
- SMB over QUIC

最近の話題
- マルチパスQUIC

キャプティブ・ポータル

中期的な動き - キャプティブ・ポータル

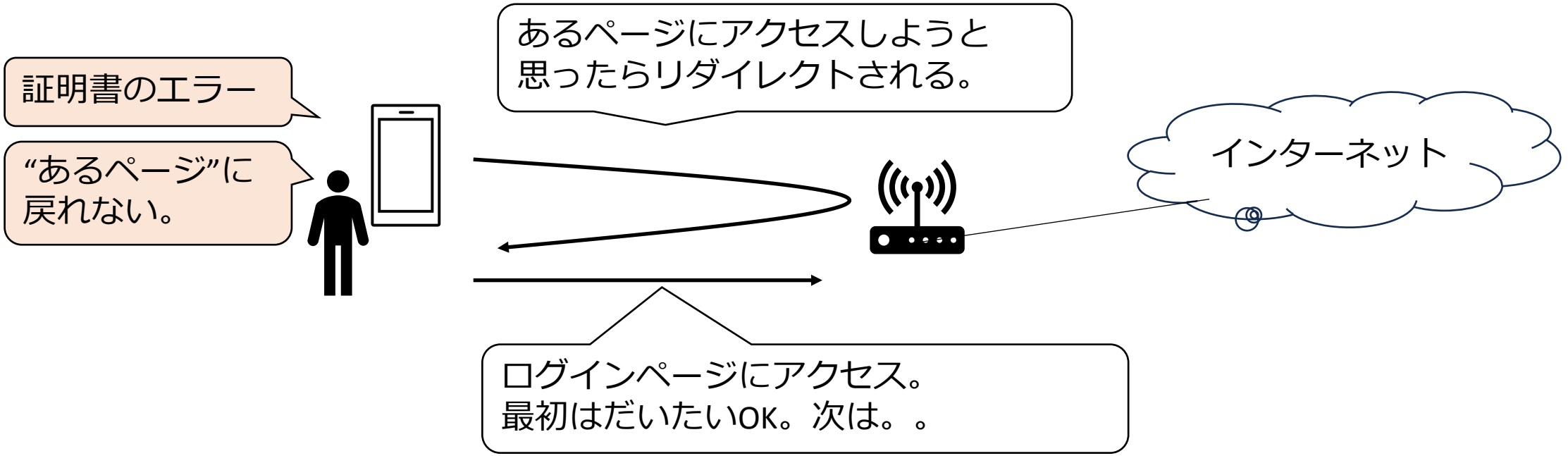
- **最近、まともに動作するキャプティブ・ポータル、増えてません？**

- **かつて指摘されたキャプティブ・ポータルにおける問題**
  - 閉じたネットワークであることの検知がうまく働かない。
  - タイムアウトしてしまって何度も認証させられる。
  - サーバ証明書のエラーがでる。DNSSEC検証できない。
    などなどなど

- 2020年に**RFC8910**「Captive-Portal Identification in DHCP and Router Advertisements (RAs)」が公開されてました。

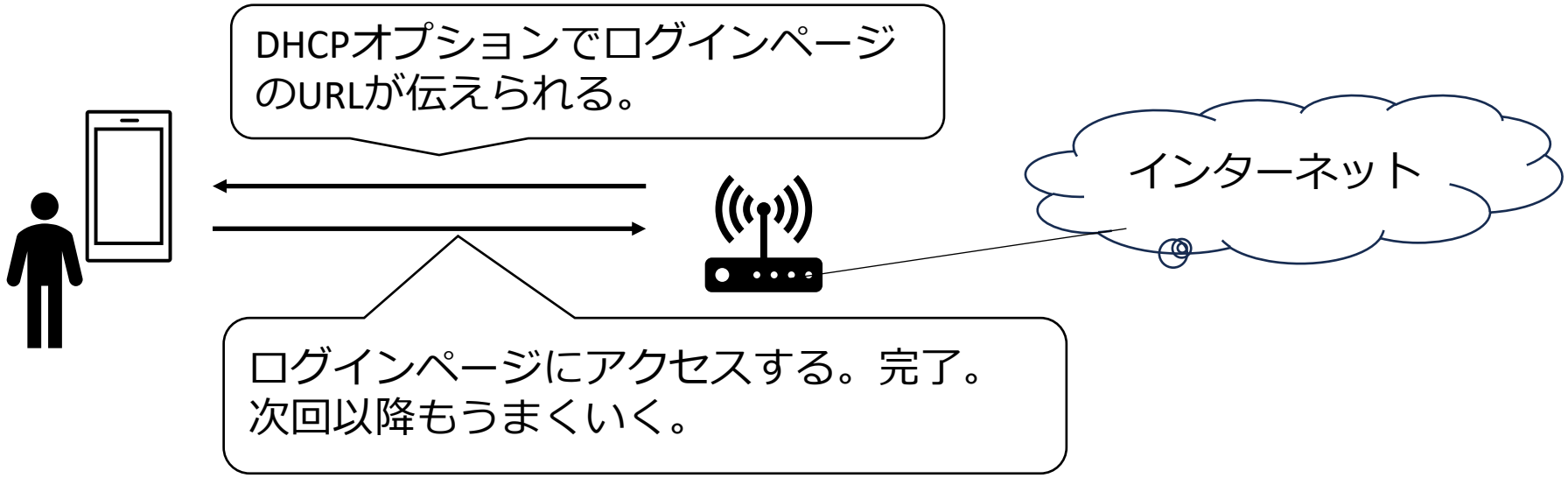
中期的な動き - キャプティブ・ポータル

RFC8910がないとき



中期的な動き - キャプティブ・ポータル

RFC8910があるとき



更にRFC8952「Captive Portal Architecture」で全体構成が整理されているので、きれいなキャプティブポータル(?)を作りたい人におすすめ。

考察 - プロトコルの策定とは

- ものごとがうまくいく仕組みや仕掛けを考えること...
- ネットワーク機器やスマホが違っているような利用場面について、メーカ各社では解決できないような問題を解決できる手段。
- ただし、うまく実装され普及した場合に。

中期的な動き - プライバシー関連

中期的な動き - プライバシー関連

- スノーデン事件のあとにRFC7258「Pervasive Monitoring Is an Attack」が策定された2014年頃
  ↓
  すべてのプロトコルに暗号化の機能を！
  ↓
  時は流れ
  ↓
  アプリケーションの通信が始まる前（TLSのSNI）から秘匿する動き。更にWebクライアントのIPアドレスを秘匿していく動き。

DNS問い合わせ応答の暗号化	TLSにおけるクライアントハローメッセージの暗号化(ECH)の暗号化	WebクライアントのIPアドレスの秘匿

時系列(1/3)

- **2013年**
  - 5月, スノーデン氏、PRISMSを公表
  - 11月 IETF88
    - W3C/IAB workshop - STRINT(**Strengthening the Internet Against Pervasive Monitoring**)
    - “**Pervasive Monitoring is an Attack**”, draft-farrell-perpass-attack-00 (RFC7258, 2014)
- **2014年**
  - 9月, dprive WG
    - "Specification for DNS over Transport Layer Security (TLS)", (**RFC7858, 2016**) **# DoT**
- **2015年**
  - 6月, "**DNS over DTLS**" draft-ietf-dprive-dnsodtls-00 (RFC8094, 2017)
  - 7月, **IETF93, スノーデン氏、遠隔登場**

時系列(2/3)

- **2017年**
  - 4月 "Specification of **DNS over QUIC**" draft-huitema-quic-dnsoquic-00 # current: 07
  - 5月, "DNS Queries over HTTPS", draft-hoffman-dns-over-https-00 (**RFC8484, 2018**) **# DoH**
  - 9月, doh WG
  - 11月, Quad9、DoTをサポート
- **2018年**
  - 4月, Android DoH client アプリ Intra 登場
  - 4月, CloudFlare、パブリックDNSがDoTとDoHをサポート
  - 6月, Firefox、DoHのベータテスト
  - 10月, Quad9、DoHをサポート

時系列(3/3)

- **2019年**
  - 1月, Google パブリックDNSでDoTをサポート
  - Google パブリックDNSでDoH(RFC8484)をサポート

DNS問い合わせ応答の暗号化

中期的な動き - プライバシー関連

- TLS Encrypted Client Hello / draft-ietf-tls-esni
  - TLS1.3の拡張。Server Name Indication(SNI)を含むTLSのクライアント・ハローメッセージを暗号化できる。
  - 暗号化に必要な公開鍵はDNSのHTTPSレコードを通じて取得できる。

  - 最初の発表は2018年のIETF102
  - TLS WGで議論されている。

TLSにおけるクライアントハローメッセージの暗号化(ECH)の暗号化

中期的な動き - プライバシー関連

- Oblivious HTTP
  - クライアント（Webブラウザ）のIPアドレスやリクエストの内容を秘匿する仕組み。
  - クライアントはリクエストの内容を暗号化してOHTTPプロキシーサーバに送信しプロキシーサーバはその内容をWebサーバに送信する。

  - 最初の発表は2021年のIETF11におけるBOF
  - 現在はOblivious HTTP Application Intermediation (OHAI) WGで議論されている。

WebクライアントのIPアドレスの秘匿

中期的な動き - プライバシー関連

DNS問い合わせ応答の暗号化

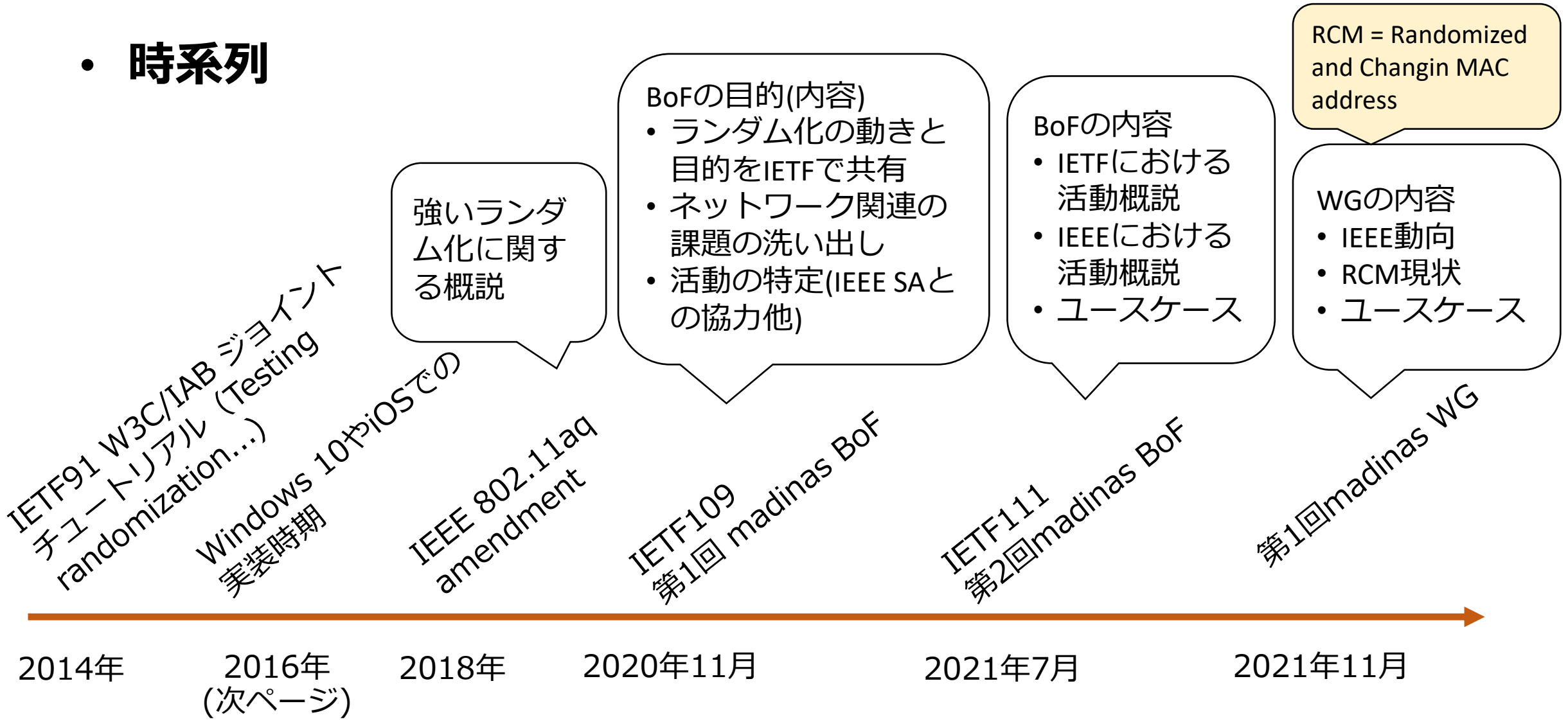
TLSにおけるクライアントハローメッセージの暗号化(ECH)の暗号化

WebクライアントのIPアドレスの秘匿

中期的な動き - MACアドレスのランダム化

中期的な動き - MACアドレスのランダム化

- **時系列**



MACアドレスランダム化の話題は2016年頃より

VAIO

[Windows 10] ランダムハードウェアアドレスの設定方法

2016/08/26 公開 | 2017/10/10 更新

対象OS

Windows 10 Home
Windows 10 Pro

説明

Windows 10 より、Wi-Fi のMACアドレス（物理アドレス、ハードウェアアドレス）としてランダムな値を使用することが出来るようになりました。
この「ランダムハードウェアアドレス」機能を利用すると、外出先からのWi-FiでMACアドレスを利用した追跡をされにくくすることが出来ます。

操作方法

[Windows 10] ランダムハードウェアアドレスの設定方法
2016/08/26 公開 | 2017/10/10 更新
https://solutions.vaio.com/2827

MACアドレスランダム化（Ephemeral MAC Address）

- iOS 8以降、APへのProbe時のMACアドレスがランダム化される
  - ただし接続時は本来のMACアドレス
- Windows 10でMACアドレスランダム化が実装される
  - デフォルトはオフ　一部NICでは使用不能
  - 同一SSIDには同一MACアドレスという実装
    - さらに毎日変更するオプションもあり
- IEEEでも802.1委員会で議論？

Wi-Fiを巡る【社会的】問題, 立命館大学 情報理工学部 上原哲太郎, InternetWeek2016
https://www.nic.ad.jp/ja/materials/iw/2016/proceedings/t15/t15-uehara.pdf

MACアドレスランダム化に関連するユースケース(1/2)

- **MACアドレスを使ったアクセスコントロール**
  - CPEにおけるMACアドレスフィルタリングが効かないケース
- **静的なDHCPによるアドレス割り当て**
  - 同じアドレスが割り当てられないケース。DMZやポート転送用途等。
- **DHCPアドレスプールの枯渇**
  - 多くのアドレスが(有効期限内に入ったまま)使えなくなるケース
- **ISPにおける問題分析(MACアドレスで識別しているとき)**
  - ユーザの端末をMACアドレスで識別できなくなるケース

“MADINAS Use Cases” より
https://datatracker.ietf.org/meeting/109/materials/slides-109-madinas-madinas-use-cases-00

MACアドレスランダム化に関連するユースケース(2/2)

- **MACアドレスによるホームネットワークの機器識別**
  - コンテンツフィルタリング、デバイスへの名前付けができなくなるケース
- **Cloud リソース管理**
  - デバイスをクラウドサービスで管理しているがレコードが増えすぎるケース
- **コミュニティWi-Fiの自動ログイン/モビリティ**
  - ユーザを識別してローミング時にログイン済と判別できないケース
- **Wi-FiにおけるQoE(Quality of Experience)計測**
  - コミュニティWi-Fiで品質の計測ができなくなるケース

“MADINAS Use Cases” より
https://datatracker.ietf.org/meeting/109/materials/slides-109-madinas-madinas-use-cases-00

2023年の話題

2023年の話題(1) - DULT BoF

- Detecting Unwanted Location Trackers (DULT)

- 位置情報を追跡できる小型のアクセサリ（トラッカー）が悪用されると本人が知らないうちに位置が特定され、プライバシー上の脅威となりうる。この脅威に対処するため、様々なトラッカーにおいても望まない追跡から守られるプロトコルを策定する。（趣意書案より抜粋/charter-ietf-dult-00-01）

  - Detecting Unwanted Location Trackers (dult) WGのページ https://datatracker.ietf.org/wg/dult/about/

2023年の話題(2) - “QUIC in Space”/HotRFC

- **月や火星といった地球からの通信遅延が大きい環境でQUICを使うための検討とテストベッドを検討中。**
  - 遅延1秒の月面でWi-Fiや5Gを使うIPネットワークを想定
  - 遅延4分から20分の火星でWi-Fiや5Gを使うIPネットワークを想定
  - QUICが動作するかどうかを検証
  - QUIC in Space, Marc Blanchet (IETF-117 HotRFC) https://datatracker.ietf.org/meeting/117/materials/slides-117-hotrfc-sessa-05-quic-in-space-00

2023年の話題(3)

- **“TCP Performance over Starlink” - IEPG**
  - StarlinkのデータTCP通信サービスでpingによるRTTを計測したり、輻輳制御アルゴリズムの異なるTCPやQUICでデータ伝送速度を計測。
  - ジッター率が高く、マイクロ・ロスの頻度が高い。
  - “Starlink Protocol Performance”, Geoff Huston, APNIC https://iepg.org/2023-11-05-ietf118/2023-11-05-starlink.pdf

おわり

一般社団法人 日本ネットワークインフォメーションセンター