bibital

# IETFにおけるEnd-to-End暗号・プライバシー強化関連技術の調査及び規格提案

合同会社 bibital
安次富 大介

TTC主催 ICTビジネス戦略オンラインセミナー
「デジュール及びフォーラム標準に関する 国際標準化活動動向調査」
（2024-02-22）

# 報告者紹介：安次富大介 (Ajitomi Daisuke)

- 2002年 株式会社東芝 研究開発センター入社。以降、ネット家電やデジタルテレビ、これらのバックエンドの通信システムなど、製品寄りの研究開発に従事
- 現在、同社クラウドCoE担当部門のシニアマネージャとして、東芝グループ全体のクラウド活用推進・統制、基盤整備、人材育成を担当。その傍ら、Webやセキュリティ技術の調査・技術開発を主たる事業とする合同会社を設立
- 標準化との関わりは、UOPF、IPTVフォーラムなどの国内業界標準を中心に実装者として。2015-2021年、W3C の AC Representative。W3C HTTPS in Loal Network CG の設立・運営にたずさわり、現在も W3C WoT Japanese CG の運営サポートを継続
- これまで実装者として関わったIETF標準：
  - HTTP/1.1、MLD/IPv6、WebSocket、SIP、OAuth、JOSE/COSE、HPKE

# プライバシー強化技術

Privacy Enhancing Technologies (**PETs**)

- 個人データを活用したサービスが人々の生活を豊かにし、企業に莫大な収益をもたらす一方、個人のプライバシーを尊重する世界的な潮流の中で、世界各国でプライバシー保護規制の整備(GDPR、CCPAなど) が進んでいる
- こうした背景のもと、近年 サービスの発展と積極的な規制遵守を両立させる技術としてプライバシー強化技術 (PETs)が注目されている。
- PETs は、主に OECD Privacy Principles (1980)を源流とするプライバシー原則を実現・強化するための技術。主として、オンラインサービスの個人データ管理者(data controller)による個人データ保護技術を指す

# プライバシー原則とプライバシー強化技術

- OECD・ISO/IEC29100の原則は、GDPR等のプライバシー保護規制の下敷きになっている
- 本発表でのPETsは、主に 個人データの収集・処理・開示(提供)の最小化 に寄与するものとする

| OECD Privacy Principles (1980) | ISO/IEC29100 Privacy Framework (2011) | プライバシー強化技術 (PETs) |
|---|---|---|
| **1. 収集の制限 (Collection Limitation)**<br>合法かつ公正な方法で、正しい情報提供と同意に基づいて収集する | **1. 同意及び選択 (Consent and choice)**<br>**3. 収集の制限 (Collection Limitation)** | 認証認可、アクセス制御 |
| **2. データ品質 (Data Quality)**<br>個人データは利用目的に関連した、正確、完全かつ最新のものである | **3. 収集の制限 (Collection Limitation)** ※“収集”する個人データの最小化<br>**4. データ最小化 (Data minimization)** ※“処理”する個人データの最小化<br>**6. 正確性及び品質 (Accuracy and quality)** | デジタル署名、暗号化(含む End-to-End暗号)<br>連合学習 |
| **3. 目的の明確化 (Purpose Specification)**<br>収集の目的を明確にし、データの利用は目的に合致させる | **2. 目的の正当性及び明確化 (Purpose legitimacy and specification)** | |
| **4. 利用の制限 (Use Limitation)**<br>本人同意か法令に基づく場合以外での目的外の開示・利用を禁止する | **5. 利用、保持及び開示の制限 (Use、retention and disclosure limitation)**<br>+ データ保持期間への言及 ※“開示(提供)”する個人データの最小化 | 認証認可、アクセス制御<br>匿名化、選択的開示、ゼロ知識証明<br>秘密計算、差分プライバシー、連合学習 |
| **5. セキュリティ保護 (Security Safeguard)**<br>個人データを不正アクセス、破壊や改ざんから保護する | **10. 情報セキュリティ (Information Security)** | 認証認可、アクセス制御<br>デジタル署名、暗号化 |
| **6. 公開 (Openness)**<br>処理のポリシー、目的、手順、data controllerの情報等を開示・提供する | **7. 公開性、透明性及び通知 (Openness、transparency and Notice)** | |
| **7. 個人参加 (Individual Participation)**<br>本人がdata controllerから個人データの取得、削除等を要求できる | **8. 個人参加及びアクセス (Individual participation and access)** | （認証認可、アクセス制御） |
| **8. 責任 (Accountability)**<br>data controllerは、上記原則を実現する措置を遵守する責任を負う | **9. 責任 (Accountability)**<br>**11. プライバシーコンプライアンス (Privacy compliance)**<br>+ 監査による検証と実証、監督機関への協力 | |

# IETFにおけるセキュリティ・プライバシーへの取り組み

- Topics of Interest
  - Automated network management
  - The Internet of Things
  - New transport technology
  - Security & privacy
- Active IETF Working Groups

Security & privacy は
Topics of Interest の１つ

*“Trust by users in security and privacy on the Internet is a critical part of its success.”*

セキュリティエリアは
WG数の最も多い技術領域

| 技術領域 | WG数 |
|---|---|
| ART: Application and Real-Time Area | 24 |
| GEN: General Area | 1 |
| INT: Internet Area | 16 |
| OPS: Operations and Management Area | 17 |
| RTG: Routing Area | 24 |
| **SEC: Security Area** | **29** |
| TSV: Transport Area | 0 (廃止) |
| WIT: Web and Internet Transport | 16 (新設) |

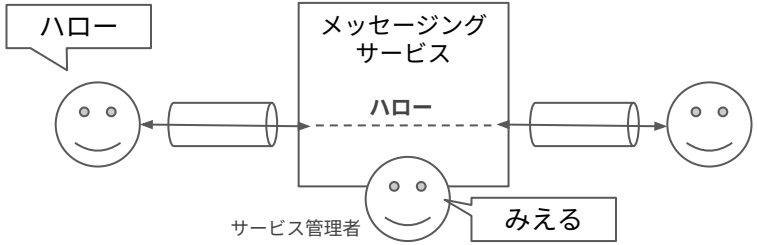
※ 2024年2月22日現在

**RFC6973 - Privacy Considerations for Internet Protocols**
プロトコル仕様にプライバシー考慮事項を入れるためのガイダンス
**RFC7258 - Pervasive Monitoring Is an Attack**
広域監視はプロトコル設計時に可能な限り回避すべき攻撃とみなす宣言
**RFC7624 - Confidentiality in the Face of Pervasive Surveillance: A Thread Model and Problem Statement**
広域監視などインターネットの機密性に対する攻撃(脅威モデル)の定義

# IETFにおけるプライバシー強化技術：アプローチ

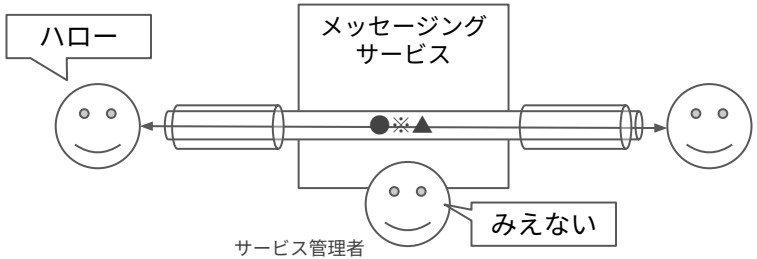
- 広域監視を攻撃と捉えたプロトコル設計時の秘匿化の追求、収集・処理・開示される個人データの最小化を志向
- できる限り見ない、できる限り関連付けない（個人データ化しない）

TLS(トランスポート層)の暗号化だけだとサーバ側で生データが見えてしまう

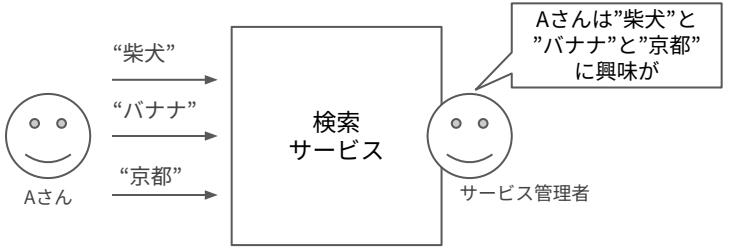



End-to-End暗号

アプリケーション層の暗号化だとサーバ側で生データは見えない

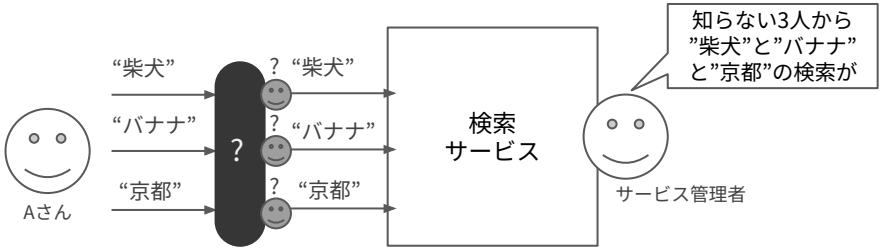



例：Messaging Layer Security (MLS)




Oblivious な通信

Unlinkable なデータ




例：Oblivious HTTP (OHTTP)

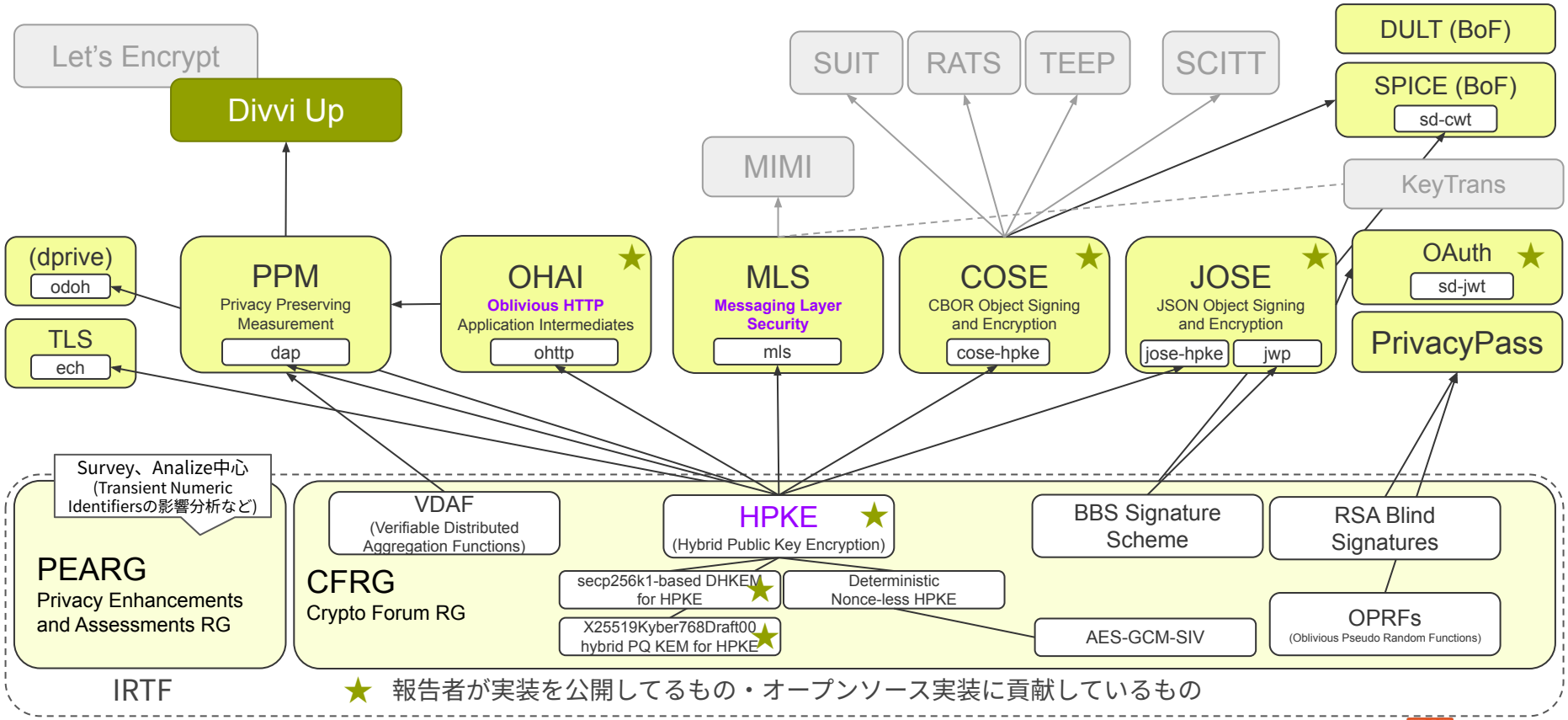
# IETFにおけるプライバシー強化技術の概要と動向 ①

| WG | 技術 | 概要・動向 |
|---|---|---|
| TLS | TLS Encrypted Client Hello (ECH) | **TLSハンドシェイクにおけるSNI (Server Name Indication)の秘匿化**<br>ECHのRFC化は未。デプロイ時の考慮点を扱う文書の議論がおこなわれている |
| ー<br>(DPRIVE) | Oblivious DNS over HTTPS | **DNSリゾルバでのクライアントの送信IPアドレスの秘匿化**<br>ODoHはExperimentalな位置づけで2022年7月にRFC化 (RFC9230)。 |
| MLS | Messaging Layer Security | **End-to-Endメッセージングをセキュアに行うためのアーキテクチャ、プロトコル**<br>MLSプロトコルはRFC9420として 2023年7月にRFC化。アーキテクチャのRFC化も目前。現在WGのチャーターを更新中。拡張領域にフォーカスしていく |
| OHAI | Oblivious HTTP | **HTTPサーバでのクライアントの送信IPアドレスの秘匿化**<br>OHTTPはRFC9458として2024年1月にRFC化。現在、別文書になっている公開鍵共有の仕組みや、chunkedエンコーディング対応に取り組んでいる |
| PrivacyPass | PrivacyPass | **プライバシー保護されたCAPCHAに応用されるトークン発行等のアーキテクチャ、プロトコル**<br>アーキテクチャやプロトコルの文書のRFC化が目前。特定用途のトークンの仕様や認証スキームなどが継続議論されている |
| PPM | Distributed Aggregation Protocol for Privacy Preserving Measurement (DAP) | **プライバシーを保護しつつメトリクス収集・集約するためのアーキテクチャ、プロトコル**<br>DivviUpというサービス開発と並行してDAPというプロトコル開発が活発に進められている |

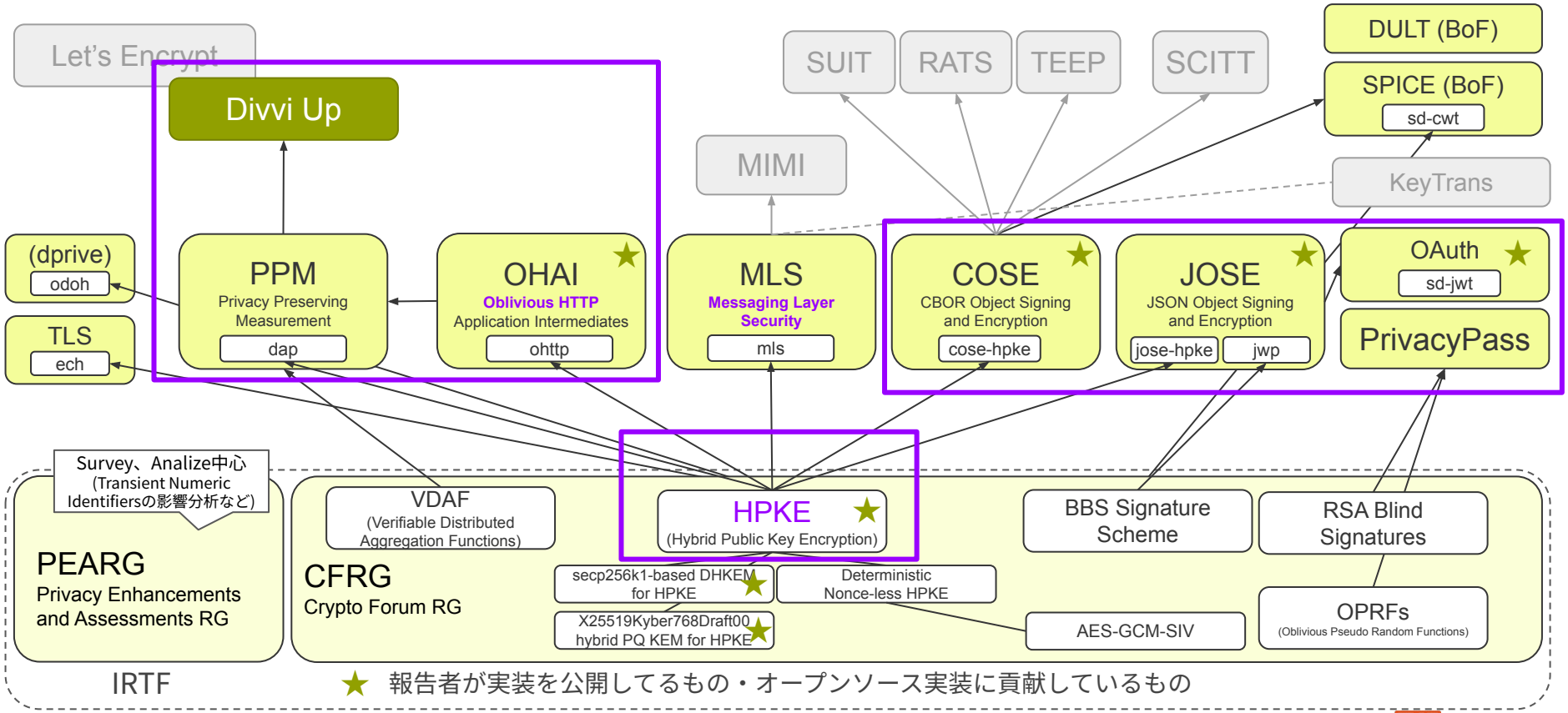
# IETFにおけるプライバシー強化技術の概要と動向 ②

| WG | 技術 | 概要・動向 |
|---|---|---|
| JOSE | JSON Web Proof (JWP) | **ゼロ知識証明のためのJOSE(JSON形式のセキュリティデータコンテナ)拡張**<br>2015年にクローズされたが、2023年、JWPをJOSEファミリーに加えるために再開。<br>現在は、アルゴリズム属性指定ルールの見直しなど、JWP以外の(従来のJOSEの)トピックも議論されている。 |
| COSE | Use of HPKE with COSE | **COSE(CBOR形式セキュリティデータコンテナ)でのHPKEを用いたEnd-to-End暗号**<br>報告者が策定に関与している。COSEには元々公開鍵暗号ベースのEnd-to-End暗号を利用する仕組みはあったが、HPKEも使えるようにする。SUIT WGでのFW暗号化鍵配送を想定ユースケースとして検討がはじまったが、Unlinkableな暗号化トークンとしての用途も想定される |
| OAuth | Selective Disclosure for JWTs (SD-JWT) | **JWT(JSON Web Token)クレームの選択的開示**<br>W3C Verifiable Credentials での利用を想定したJWTにふくまれる各属性の選択的開示を実現する。JWPと比較してunlinkabilityが担保されない。 |
| SPICE (BoF) | Selective Disclosure for CWTs (SD-CWT) | **CWT (CBOR Web Token)クレームの選択的開示**<br>IETF118でBoFが開催された。Verifiable Credentials で利用されるSD-JWT/JWPは、テキスト(JSON)形式の仕様だが、このバイナリ版の仕様策定を想定している。 |
| DULT (BoF) | Detecting Unwanted Location Trackers | **AirTagのような小さい通信デバイスを使った他者によるトラッキングの検知**<br>2023年、2回のBoFが開催され、WGのチャーターがブラッシュアップされた。現状、トラッキングアクセサリーと近隣デバイス間のプロトコルの標準化をおこない、望まないトラッキングを検知できるようにすることを主な目的としている。 |

# IETF/IRTFにおけるプライバシー強化技術の全体像

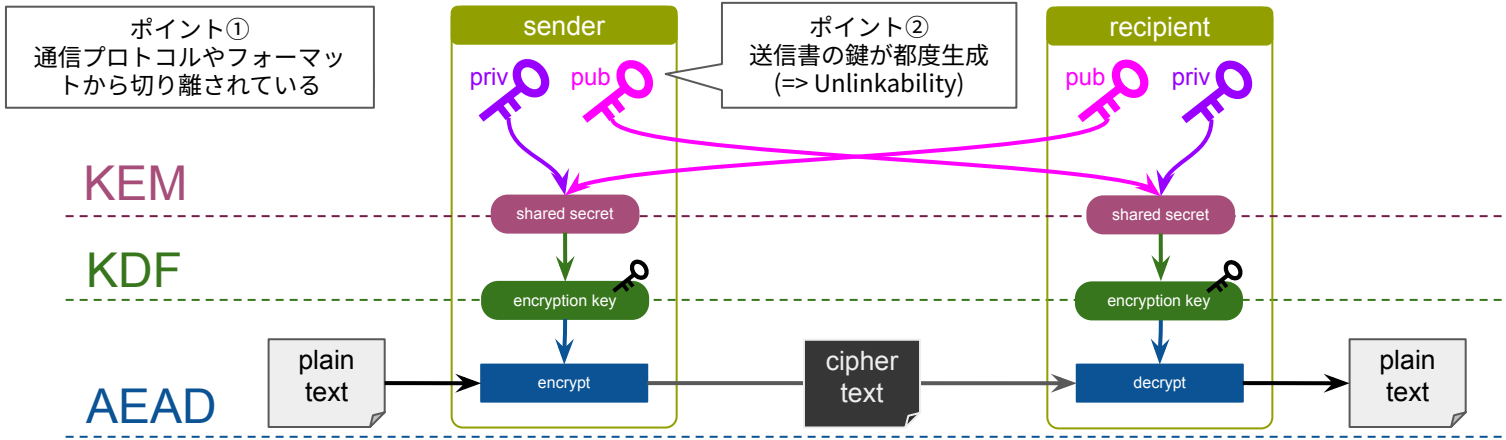


# 本日ピックアップする取り組み



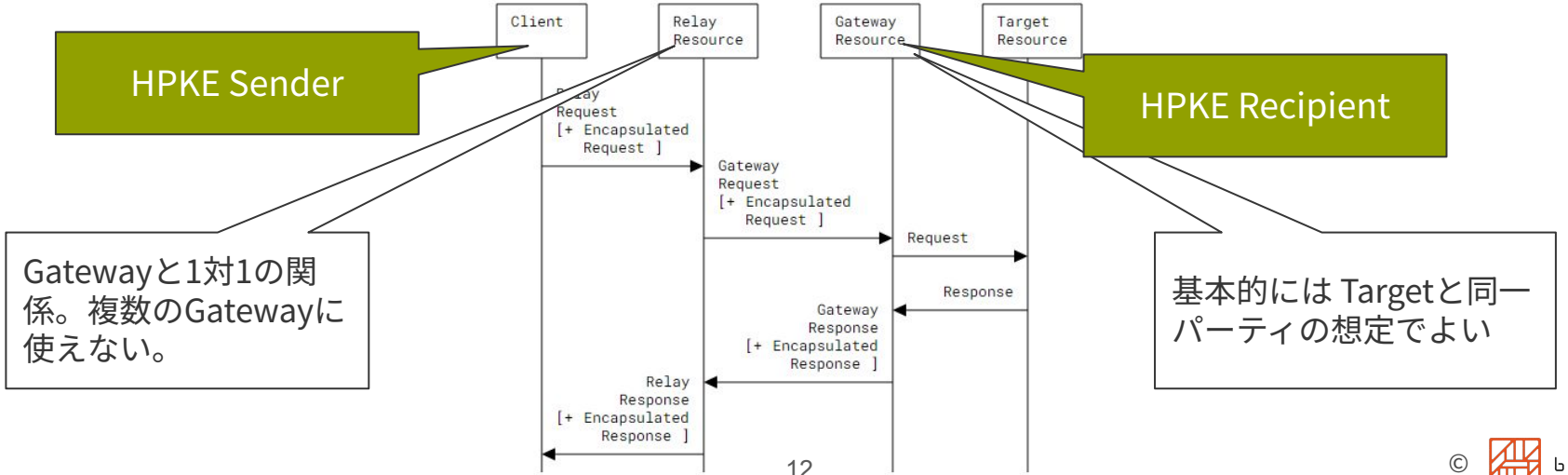
# HPKE (RFC9180: Hybrid Public Key Encryption)

- 公開鍵ベースのEnd-to-End暗号スキーム。いわばトータルソリューション
- End-to-End暗号の3ステップをパッケージ化したもの。耐量子暗号も見据えた設計
  - 1) KEM: 公開鍵の交換と鍵素材の生成、2) KDF: 鍵素材から鍵生成、3) AEAD: 暗号化
- 様々な応用規格・拡張規格がIETFで策定中
  - ECH、ODoH、OHTTP、MLS など End-to-End暗号/プライバシー強化プロトコルで採用
  - 耐量子ハイブリッドKEM（X25519Kyber768）のHPKE拡張仕様も CFRGで提案



# Oblivious HTTP Application Intermediates (OHAI) WG

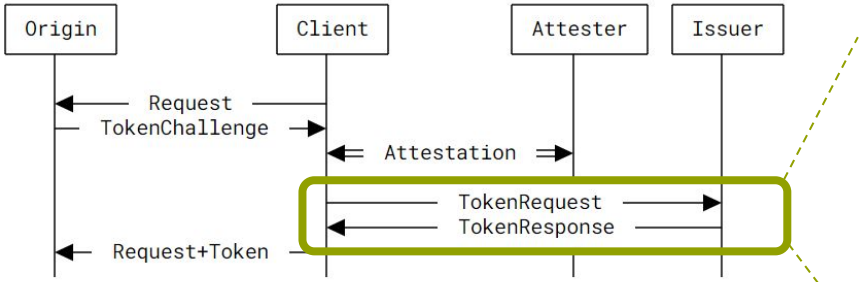
- 匿名性の高い Privacy-Preserving なHTTPアクセス仕様を扱う
  - Oblivious HTTP：個々のHTTPリクエストをUnlinkableにする
- Client-Server間に、RelayとGatewayという中間者を置くことで達成
  - Relay: ClientのIPアドレスは分かるがリクエストの内容が分からない
  - Gateway:  ClientのIPアドレスはわからないがリクエストの内容は分かる



# Privacy Pass WG

- トークンが提示された場所・時期を明らかにせず クライアントがサーバから信頼されていることを第三者に示すためのトークン発行・償還を実現するアーキテクチャやプロトコルを扱う
- 典型的なユースケース：CAPCHAの置き換え。プライバシー保護されたCAPCHA
- Cloudflare、Fastly、Apple、Googleなどが規格策定を推進。実用化も進んでいる
- コアとなる暗号技術
  - VOPRF (for privately verifiable token)
  - RSA Blind Signatures (for publicly verifiable token)

Verifiable Oblivious PRF (VOPRF)
サーバはクライアントの情報(input)を知らず、クライアントはサーバの秘密鍵(skS)を知らずに、サーバが提供する値 (evaluatedElement) が、疑似乱数関数*F(info、skS=pkSに対応する秘密鍵)*で生成されたことをクライアントに証明できる



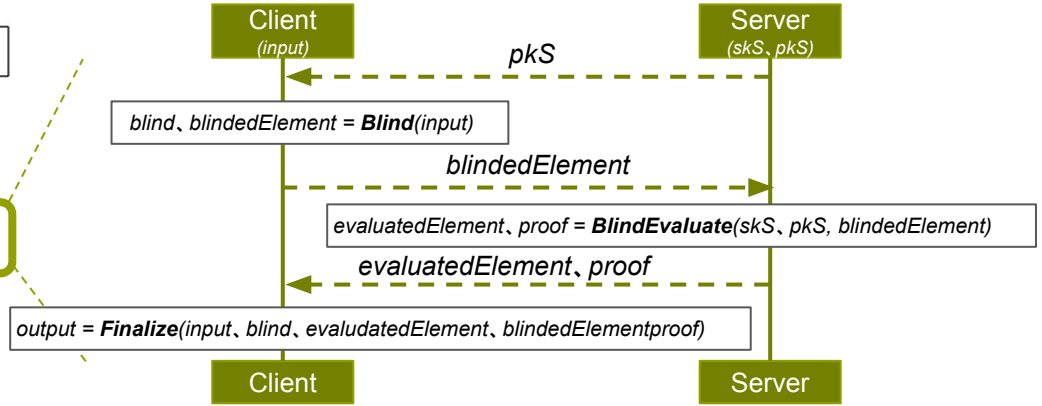



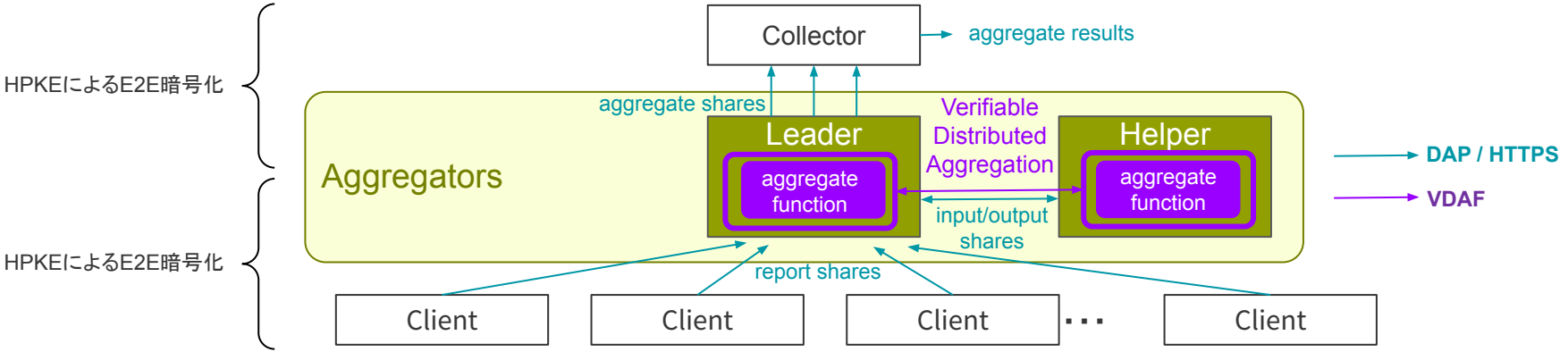

*Figure 1: Privacy pass redemption and issuance protocol interaction*

# Key Consistency and Discovery

- Key Consistency: OHAIからPrivacyPassに移された話題
- 公開鍵が十分に多数のクライアントで共用されていてプライバシー保護機能の低減につながっていないかを担保することが実は難しい。この性質を Key Consistency と呼ぶ
- システム構成を列挙してソリューション案を提示している。例えばー
  - DoubleCheck: ClientはRelayとTarget両方から公開鍵を取得して比較

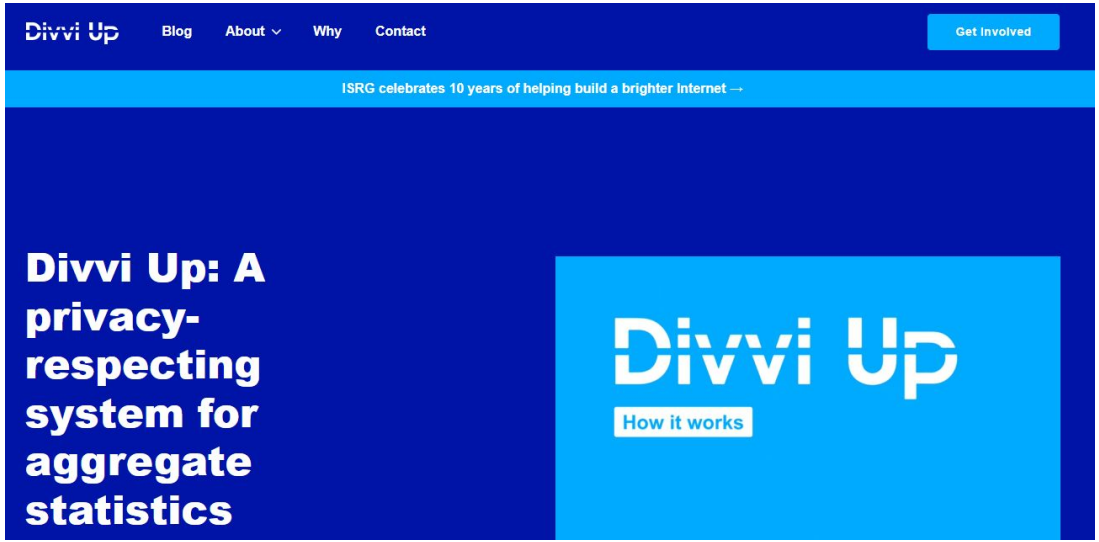
# Privacy Preserving Measurement (PPM) WG

- プライバシーを保護しつつメトリクス収集・集約するためのプロトコルを扱う
- 以下の２つのプロトコル
  - VDAF: Verifiable Distributed Aggregation Functions <= これは CFRG の作業アイテム
    - 個々の測定値を明らかにせずに集約パラメータと測定値集合から検証可能な集約値を出力できる関数(VDAF)のスキームとインタフェースの定義、具体的な関数(Prio3、Poplar1)定義を含む
  - DAP: Distributed Aggregation Protocol for Privacy Preserving Measurement
    - VDAFを核としたHTTPSベースのプライバシー保護計測システムのプロトコル定義



# PPM WG - Divvi Up https://divviup.org

- Let’s Encrypt (無料・自動のDV証明書払い出しサービス)を運営している ISRG (Internet Security Research Group) がPPMサービス ”Divvi Up”のローンチ準備中
- 開発者がPPMのメンバであり、Divvi Upをつくりながら仕様策定を進めている

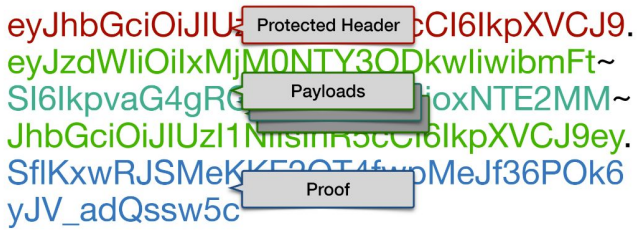



- libprio-rs
  - Implements Prio3 and Poplar1 VDAF families and VDAF abstraction
  - VDAF-06 in prio-0.13.x
  - We'd (still) love to see more implementations – Go would be great
- Daphne
  - Helper implementation targeting Cloudflare Workers
  - Moving to DAP-05 soon
- Janus
  - Client, Leader, Helper, Collector implementations
  - DAP-05 "ping-pong" implementation is prototyped, will be merged soon
- divviup-ts
  - Typescript Client implementation
  - DAP-04 implementation complete (Prio3 only)
  - Only minor changes needed for DAP-05/VDAF-06 (domain separation strings)
  - Ongoing integration test against Janus
- Firefox
  - DAP-05 client coming

divviup-ts(クライアントライブラリ)が 報告者の実装(hpke-js)を採用してくれている

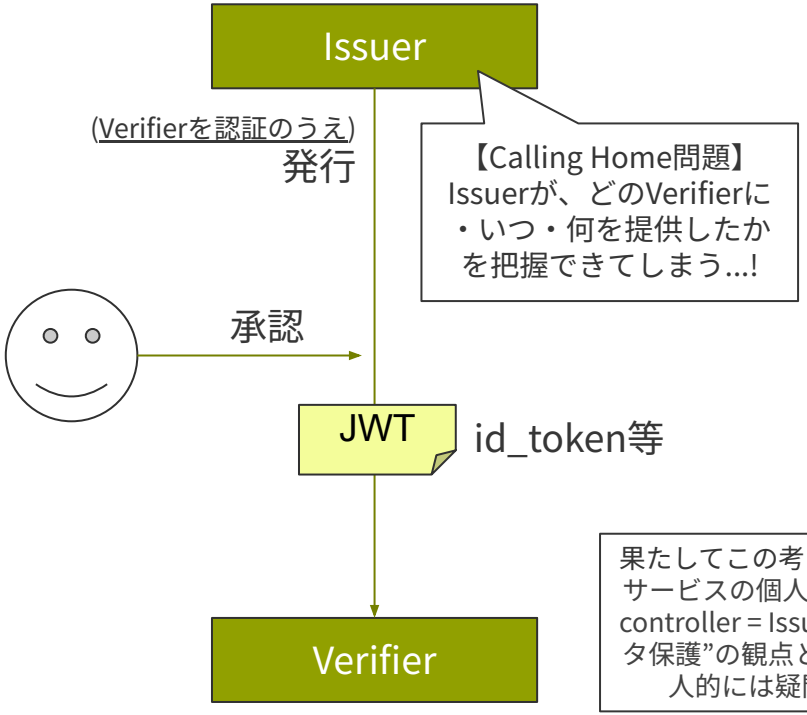
# JSON Object Signing and Encryption (JOSE) WG

- IETF116(2023-03)から再開
  - 端的には、Microsoftを中心としたJWP (JSON Web Proof) 標準化活動
    - JWA/JWE/JWS/JWT/JWP(<=new!)
  - 新しい文脈として”プライバシーを守りたいアプリケーション”が追加
  - ゼロ知識証明系の追加がメイン
  - W3C Verifiable Credentials、Privacy Pass、SD-JWT、CBOR、CFRGと連携
- JPT(JSON Proof Token)/JWP (JSON Web Proof)
  - JWP アルゴリズムは以下を可能にする
    - ペイロードの一部の選択的開示。Unlinkable。
    - ペイロードの値を公開しない述語証明
  - 具体的には、BBSやZkSNARKなどのアルゴリズムを利用
  - フォーマットは、JWSと似た3パート構成：ヘッダ、ペイロード(複数)、プルーフ

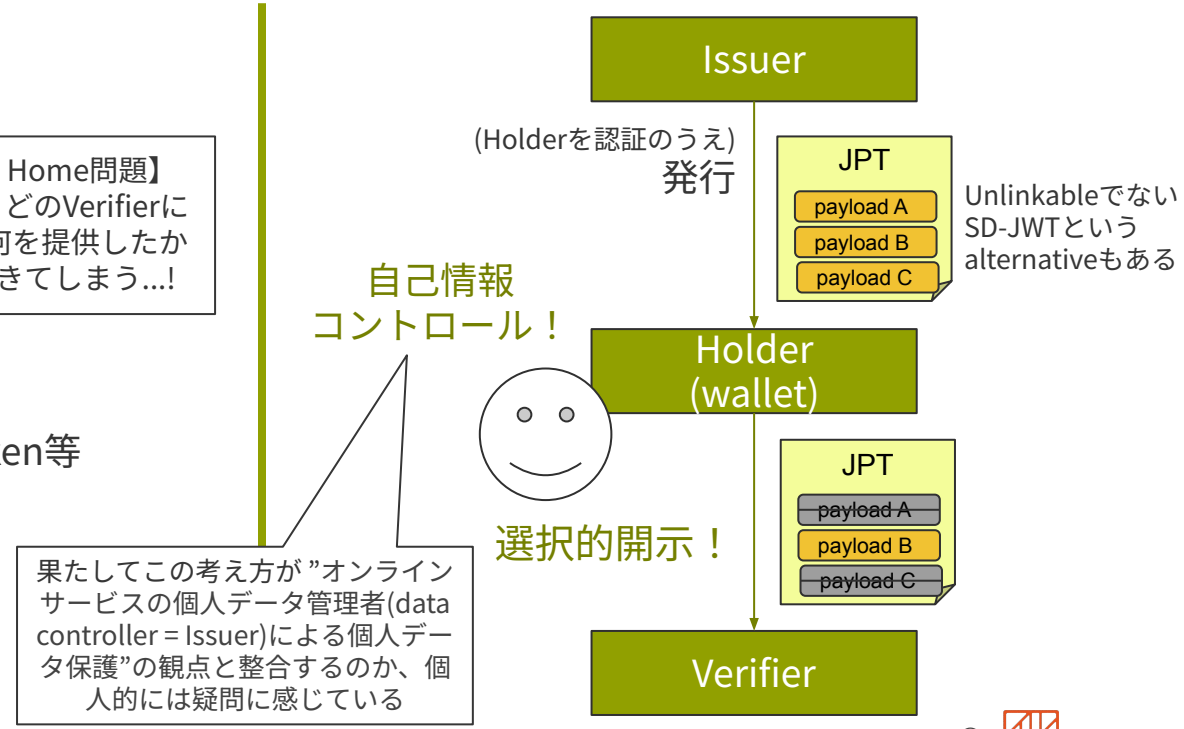


# JSON Object Signing and Encryption (JOSE) WG

- 従来モデル




- JWPの背後にある Issuer-Holder-Verifierモデル



# COSE (CBOR Object Signing and Encryption) WG

- 近年普及が進むJWT/JOSEのバイナリ版 CWT/COSEを扱うWG
  - JSONではなくCBORベース
  - 先行したJOSEの問題のいくつかが解消されているが(alg:noneが無い等)、逆に問題も？
- メッセージの省スペース性が買われ、意外と(?)使われている
  - WebAuthn、EUDCC (欧州のデジタルワクチン接種証明書)
- IoT領域の様々なWGがCOSEを採用しており、コミュニティは活発
  - ACE(OSCORE)、RATS(EAT)、SUIT、TEEP、SCITT、etc.
- 報告者は主にこのWGでコントリビューションをおこなっている
  - 2023年11月より “Use of COSE with HPKE (COSE-HPKE)” の共著者に
    - IETF118では、COSE-HPKEでの暗号スイート選定に関する提案発表
  - その他、Acknowledgementに名前を記載いただいた仕様 2件

# まとめ

- プライバシー強化技術という切り口で、IETFの標準化動向を概観した
- IETFでは、広域監視を一種の攻撃と捉えプロトコル設計時のインターネット上での秘匿化の追求、収集・処理・開示される個人データの最小化を志向した様々な取り組みがあり、実用化も並行して進んでいる
- 個人データ扱うサービスを始める・既に展開している国内事業者にとって、国際標準のなかで、どこまで”最小化”の解釈が進んでいるのかを知ることは有益であると考えている
- なお、COSE WGにおけるCOSE-HPKE等の仕様策定への貢献は 別途提出させて頂く報告書や、以下のブログ記事を参照頂きたい
  - JPNICブログ - IETFアップデート – 第118回IETF [第3弾] ハイブリッド公開鍵暗号スキーム HPKE とその応用技術の動向

bibital