暗号技術とIETFハッカソン

ISOC-JP・JPNIC 共催

IETF 情報交換会 — IETF126に向けて —

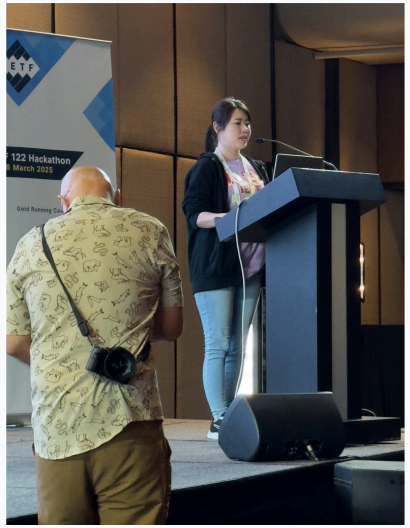
GMOコネクト株式会社 GMOインターネットグループ エキスパート

酒見 由美

2026年6月3日

自己紹介

- **名前**：酒見 由美（暗号のおねぇさん）
- **経歴**
  - 株式会社富士通研究所（現 富士通株式会社）
  - 株式会社レピダム（現 GMOサイバーセキュリティ byイエラエ）
  - GMOコネクト株式会社
- **現在のミッション**
  - 「インターネット × 暗号技術」の切り口で安心・安全を実現！
- **IETF活動**
  - **IETF124（Montreal）**：CFRGにてペアリング適性曲線の活動再開を発表
  - **IETF125（深圳）**：ハッカソンにリモート参加、活動推進中



Agenda

1. 暗号技術関連

- IETF125 での暗号技術動向の概要
- CFRGを中心とした気になる発表
  - ❶ Longfellow ZK
  - ❷ E2EE × AI
  - ❸ FHE 最新動向
- Pairing-Friendly Curves の最新動向（自分の活動）

2. IETF125 関連イベントの様子

- Hackathon
- GatherTown でのリモート参加体験

01

暗号技術関連

IETF125 での暗号技術動向

IETF125 は 2026年3月に中国・深圳で開催されました。今回のキーワードは **「PQC は当たり前になりつつある」** です。耐量子暗号の移行はもはや各グループで当然のこととして進められており、話題の中心は次の段階へ移りつつあります。

CFRG（暗号専門の研究グループ）では、特に以下の3テーマが盛り上がっていました。

今回の注目テーマ	一言で言うと
ZK 証明（ゼロ知識証明）	「内容を明かさずに、知っていることを証明する」技術が実用段階へ
FHE（完全準同型暗号）	「暗号化したまま計算できる」技術が AI との組み合わせで注目を集めている
E2EE × AI	暗号化メッセージで AI を使うと、そもそも E2EE と言えるのか？

IRTF CFRG at IETF125

CFRG（Crypto Forum Research Group）とは？

CFRG は、IETF の標準化を技術的に支える暗号専門の研究グループです。「この暗号アルゴリズムは安全か・インターネットで使えるか」を専門家が議論する場で、他のグループが暗号選択で困ったときの「相談窓口」的な役割も担っています。

IETF125 では2つのセッションが開催されました。

	Session 1（3/17 火）	Session 2（3/19 木）
時間（UTC+8）	11:30〜12:30	09:00〜11:00（2時間枠）
主なトピック	Chairs' update、PQ KEMs 議論	Two-lane model（続き）
	Sigma Protocols & Fiat-Shamir	**Longfellow ZK**
	End-to-End Encryption and AI	**FHE 最新動向**、ARKG 他

- 議長：Alexey Melnikov、Stanislav Smyshlyaev、Nick Sullivan
- 参加：多数がオンライン参加（現地参加は少なめ）

Chairs' update — Active な draft（全13本）

Chairs' update では、現在 CFRG で進行中のドラフト（仕様書案）の状況が報告されました。全13本が活発に議論されており、いくつかは正式な仕様書（RFC）まであと一歩のところまで来ています。

ドラフト	状況
draft-irtf-cfrg-pairing-friendly-curves	✅ 長期休止から再開。2025年11月より活発に議論中
draft-irtf-cfrg-bbs-signatures	活動中
draft-irtf-cfrg-sigma-protocols	活動中（2025年10月初版）
draft-irtf-cfrg-cpace	✅ IRSG review 中（パスワード認証プロトコルの選定優勝）
draft-irtf-cfrg-limits（AEAD limits）	Research Group Last Call 進行中
draft-irtf-cfrg-dnhp	Research Group Last Call 進行中
Hybrid KEM（combiner 類）	活動中（専門チームでセキュリティ証明を更新済み）

🔔 **暗号レビューパネル**：専門家9名によるレビュー体制。2026年4月に次の世代へ交代予定。

📌 **ペアリング適性曲線（私の関与）**：IETF126（2026年7月）での RGLC 開始を目標に活動中。

気になった発表 ❶ — Longfellow ZK

Longfellow ZK by Matteo Frigo, abhi shelat 他（Google）

ZK 証明（ゼロ知識証明）とは？

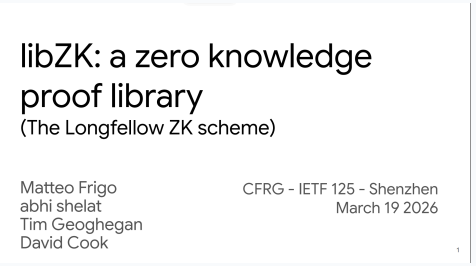
「知っていることを証明するのに、内容そのものを相手に見せなくて済む」技術です。たとえば年齢確認で「生年月日を教えずに、18歳以上であることだけを証明できる」といった使い方ができます。

Longfellow ZK の特徴

- ZK 証明はこれまで「計算が重すぎて実用にならない」のが課題でした
- Longfellow はそれをスマートフォンで動くレベルまで軽量化
- SHA-256 のみに依存する設計で、**量子コンピュータにも耐性あり**
- Google がオープンソースで公開し、欧州の年齢確認システムへの統合実績あり

IETF125 での新発表

ML-DSA（耐量子署名）の ZK 証明に初めて成功（約 850ms）。 世界初 の成果です。独立組織による実装・セキュリティレビューも3件完了しています。



気になった発表 ❷ — E2EE × AI

How To Think About End-To-End Encryption and AI by Mallory Knodel（NYU + Cornell）

問題の背景

WhatsApp（Meta AI）・Samsung/Google Messages・Apple Intelligence など、E2EE（エンドツーエンド暗号化）を謳うアプリが AI 機能を搭載し始めています。「メッセージはプライベートのまま」と説明されていますが、研究者たちはその実装を分析した結果、いずれも**クラウド上の TEE（信頼実行環境）で処理**していることを明らかにしました。

TEE は E2EE と同じか？ → 全く別物です

	E2EE	TEE
守ろうとしているもの	エンドポイント間の通信	ユーザー↔️クラウド間の計算
安全性の根拠	数学的な証明	ハードウェアへの信頼

論文の主な結論

- AI 学習にE2EE データを使うことは**明確に非互換**（NG）
- クラウドTEE での処理も「E2EEを維持している」とは言えない
- FHE（後述）を使ったオンデバイス処理なら互換の可能性あり

気になった発表 ❸ — FHE 最新動向

Recent Advances in Fully Homomorphic Encryption by Xianhui Lu（中国科学院）

FHE（完全準同型暗号）とは？

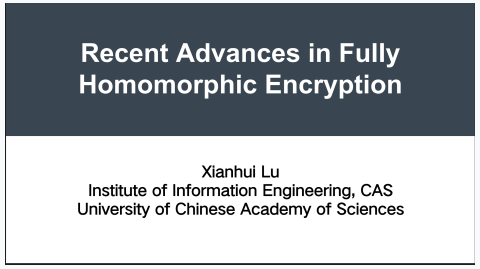
「暗号化したままデータを計算できる」技術です。通常は暗号化されたデータを処理するために一度復号（解読）が必要ですが、FHE ではそれが不要です。たとえば「病院データを AI に渡して分析させる際、AI 側には生データが一切見えない」状況を実現できます。

長い歴史と急速な進化

アイデアは 1978 年に提案されましたが、長らく「理論上は正しいが実用には重すぎる」状態でした。2009 年にようやく最初の実装が生まれ、そこから約 15 年で劇的に進化しています。

技術	進化の度合い
基本演算（Bootstrapping）	2009 年比で **40 万倍**高速化
専用チップ（Intel "Dapper" ASIC）	汎用 PC 比で **5,000 倍**高速
AES の準同型処理	かつて 1 週間 → いまは **14ms**
軽量ニューラルネット推論	顔認識・話者認証が **0.2〜0.6 秒**

ISO/IEC での標準化も進んでおり、1〜2 年以内の策定が見込まれます。



Pairing-Friendly Curves の背景 — なぜ今、標準化が必要か

ペアリング適性曲線とは？

ZK 証明・BBS 署名・ペアリングベース暗号の「土台」となる特殊な楕円曲線です。曲線のパラメータを標準化することで、異なる実装間の相互運用性が生まれます。

Kim の攻撃（2016年〜）が引き起こした問題

長年 128-bit 安全とされてきた **BN254** に対し、Kim-Barbulescu らの攻撃が有効であることが判明。安全性が事実上 **約 100-bit に低下**しました。

BN254 は今も現役で使われています

- Ethereum スマートコントラクト（EIP-196/197 プリコンパイル）
- 多くの ZK 証明ライブラリ（snarkjs 等）が BN254 を前提に実装

→ **「では安全なパラメータはどれを使えばいい？」** を明確にするのがこのドラフトの役割です。

曲線の安全性比較

曲線	Bit Security	備考
BN254	**≈ 100-bit**	⚠️ Kim攻撃で低下
BLS12-381	≈ 128-bit	KB攻撃後に設計
BN462	≈ 134-bit	128-bit 超えを確保
BLS48-581	≈ 256-bit	高セキュリティ向け

Pairing-Friendly Curves の最新動向（自分の活動）

draft-irtf-cfrg-pairing-friendly-curves

IETF125 時点の状況

- 長期休止（〜2025年10月）から再開してこの時点で約4ヶ月
- CFRG Chair の Nick Sullivan が合流し、チーム体制を再編
- Chairs' update でも「長期休止から復活した重要ドラフト」として言及

現在進行中の活動

- 採用する曲線セットの議論フェーズ（5/1〜5/22）が終了。著者評価（v16）を送付済み
- 楕円点のシリアライゼーションなどの Issue 対応後、Crypto Panel Review を予定
- **目標：IETF126（2026年7月）での RGLC（研究グループとしての最終確認）開始**

収録予定曲線（案）

曲線	Bit Security	主な用途
BLS12-381	≈ 128-bit	BBS署名・Ethereum
BN462	≈ 134-bit	標準用途
BLS48-581	≈ 256-bit	高セキュリティ

> *BN254 からの移行先として、安全な曲線セットを標準化します。*

02

IETF125 関連イベント

IETF Hackathon とは？

2015年3月（IETF92 Dallas）からスタートした、IETF 本会議直前の2日間イベントです。

目的

- 開発者と各領域の専門家が協力して、IETF 標準の**実用的な実装を加速**させる
- OSS 開発のスピードと協力精神を IETF に注入し、標準化活動の速度と関連性を向上させる
- 開発者や若手に IETF へ参加・興味を持ってもらう

取り扱うテーマ

DNS・QUIC・TLS・WebRTC・YANG/NETCONF・HTTP など、**ほぼすべての IETF 作業領域**にわたる幅広いトピック。プロジェクトごとに Champion（リード役）が必須で、最終日に成果発表の場があります。

規模の変化

	IETF92（2015年）	IETF123（2025年）	IETF125（2026年）
プロジェクト数	約12件	63件	57件
参加者数	少規模	678名	583名

IETF Hackathon の様子（過去回より）

IETF Community Wiki

Search...

GROUPS

Group Index

IAB

IESG

IRTF

MEETINGS

IETF 126 Meeting Wiki

/ meeting / 125 / hackathon

IETF 125 Hackathon

Edit | Edit on GitHub

The Internet Engineering Task Force (IETF) is holding a hackathon to encourage developers and subject matter experts to discuss, collaborate, and develop utilities, ideas, sample code, and solutions that show practical implementations of IETF standards.

When: 14 - 15 March 2026 (Saturday - Sunday)

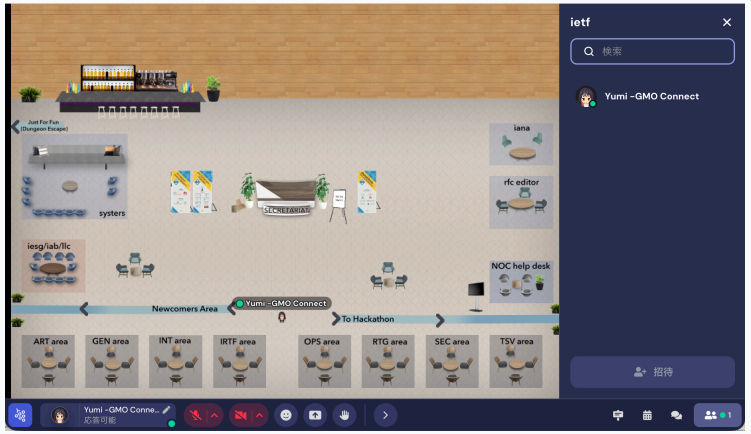
IETF125 Hackathon

IETF では本会議の直前に「Hackathon」が開催されます。参加プロジェクト数 **57**、参加者 **583名**（現地 474名 / リモート 109名）と大規模なイベントです。

今回は深圳開催（日本との時差1時間）のため、リモート参加を選択。菅野さんと渋谷セルリアンタワーのオフィスに集まり、IETF提供のバーチャル会場「**GatherTown**」を使って参加しました。

GatherTown とは？

2D のアバターが動き回るバーチャル空間で、アバター同士が近づくだけで自動的に音声通話・画面共有が始まります。オンラインながら「廊下で声をかける」感覚に近い自然な交流ができます。



Hackathon での活動① — Pairing-Friendly Curves

draft-irtf-cfrg-pairing-friendly-curves

IETF124（モントリオール）で RFC 化に向けた活動再開を発表してから、Hackathon では具体的な作業を進めました。

Hackathon での作業内容

- I-D（仕様書ドラフト）の既存 Issue を精査し、対応方針を整理
- Markdown 形式で書かれた Internet-Draft の更新作業
- GitHub リポジトリと datatracker の同期

現在（発表時点）の状況

5月の曲線セット議論フェーズが終了。著者評価（v16）を送付済み。楕円点のシリアライゼーションなどの Issue 対応後、Crypto Panel Review を経て **IETF126（2026年7月）での RGLC 開始**を目指して最終調整中です。

Hackathon での活動② — PCS / Secure Hybrid Network

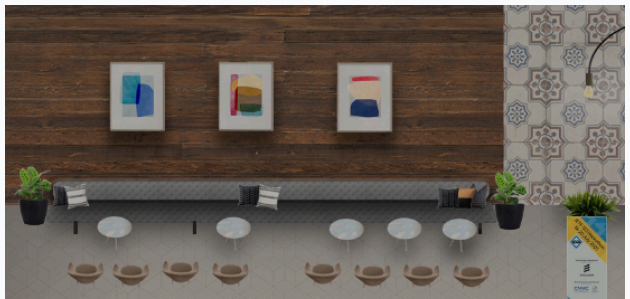
産総研（AIST）大岩さんのチームと共同で取り組んだプロジェクトです。

PCS（Path Characteristics Service）とは？

通信の経路がユーザーの意図（インテント）を満たしているかどうかを検証するサービスです。たとえば「この通信は本当に国内だけを通っているか」「信用できない国を経由していないか」といったことをポリシーとして定義し、pass / fail で判定します。

Hackathon での成果

- `domestic-only`・`no restricted country`・`no VPN` などのプリセットポリシーを搭載した Web UI を実装
- 最終日の **Hack Demo Happy Hour** にて GatherTown から発表



まとめ

IETF125 CFRG の注目発表

テーマ	発表	ひとこと
ZK証明の実用化	Longfellow ZK	スマホで動く PQ セキュアな ZK 証明。ML-DSA の証明も世界初達成
E2EE × AI	Mallory Knodel	TEE は E2EE ではない。AI搭載アプリの「本当のプライバシー」に問題提起
FHE 最新動向	Xianhui Lu	40万倍高速化。「暗号化したまま AI に計算させる」未来が近づいている

自分の活動：Pairing-Friendly Curves — 5月に曲線セット議論フェーズ終了、著者評価を送付済み。IETF126（2026年7月）での RGLC 開始を目指して最終調整中

所感

- PQC はいよいよ「当たり前」のフェーズへ移行しつつあります
- CFRG の次の焦点は **ZK 証明** と **FHE（暗号化したまま計算する技術）**
- **E2EE × AI** は暗号と AI が本格的に交差した時代を象徴するテーマとして、今後も議論が続くでしょう

IETF126（2026年7月）

次回は **現地参加**予定です！

- **Pairing-Friendly Curves**：RGLC 開始を目指してラストスパート
- **超低遅延暗号 Areion**：引き続き活動継続
- **PCS**：引き続き AIST チームと活動継続

ご参加のみなさま、よろしくお願いいたします 🙏