コミュニケーションツールに導入される エンドツーエンド暗号化技術の安全性評価

セキュリティ基盤研究室 主任研究員

伊藤 竜馬

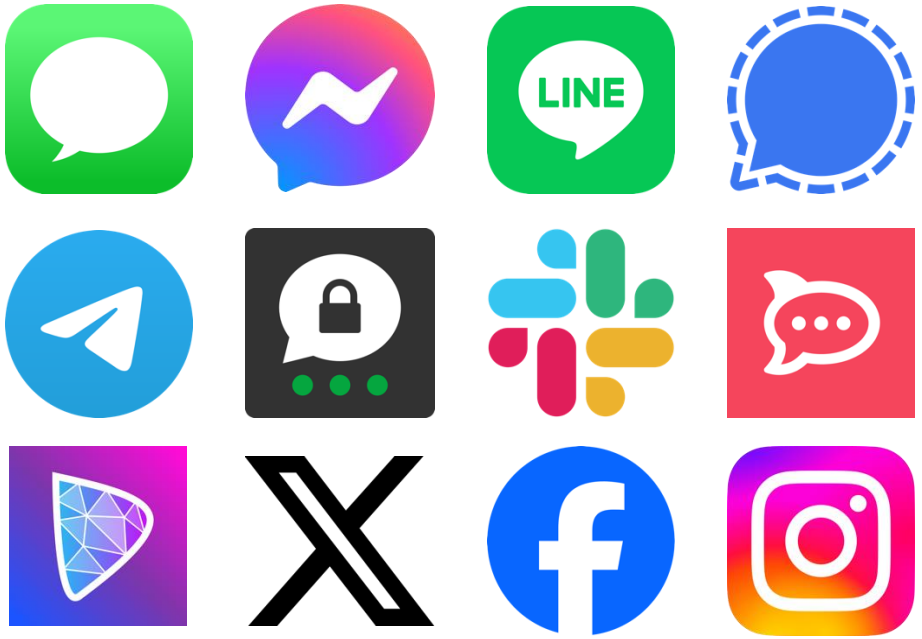
兵庫県立大学、NECとの共同研究

コミュニケーションツール

コロナ禍を経てコミュニケーションツールの利用が大幅に拡大

- リモートワーク、遠隔授業、遠隔医療、プライベート、他多数

メッセージングアプリ



ビデオ会議アプリ

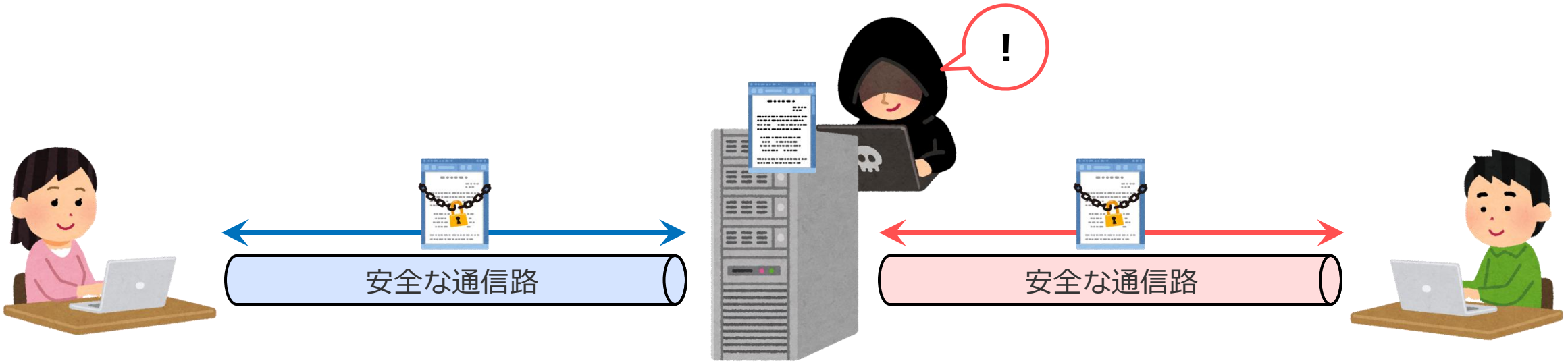
機密情報・プライバシー情報はどのように保護されるのか？

画像引用元：各公式サイト、Wikipedia

従来の暗号化通信

クライアント・サーバ間の暗号化通信（例：TLS）

- サービスプロバイダが管理するサーバで復号、再暗号化してデータを中継
- **悪意のあるサーバ管理者**が技術的にメッセージの盗聴、改ざん可能

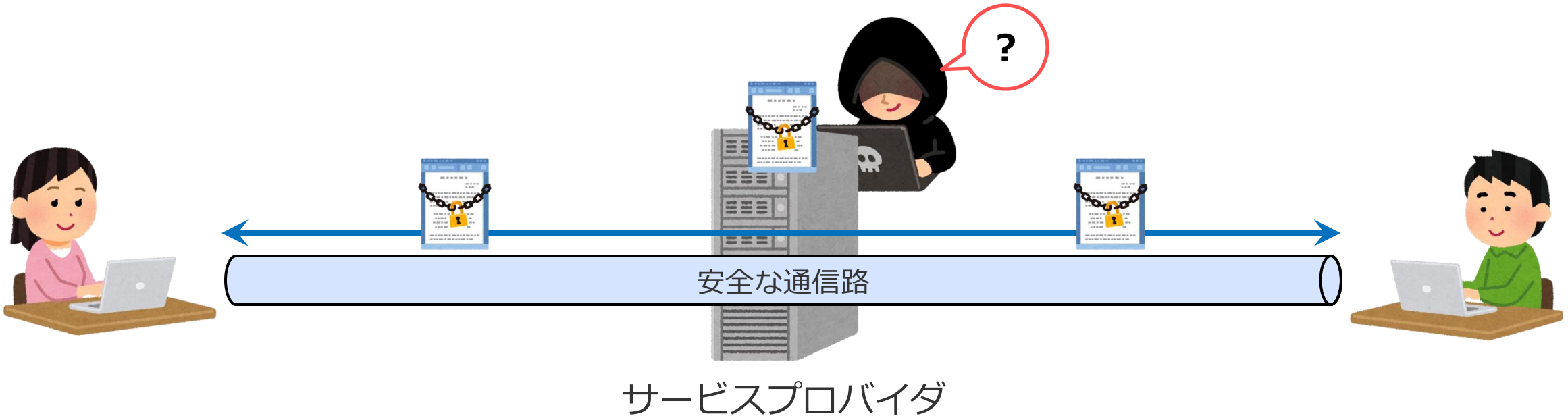


画像引用元：いらすとや

エンドツーエンド暗号化（E2EE）通信

通信するエンドユーザのみが暗号化・復号可能な通信方式

- **サービスプロバイダ**であっても技術的にメッセージの盗聴、改ざん不可
- スノーデン氏の暴露事件により、国家規模の監視・盗聴に対するE2EEの必要性が大



画像引用元：いらすとや

E2EE技術は本当に安全か？

E2EE技術の安全性評価に関する議論が不十分

- **悪意のあるサーバ管理者**によるE2EE技術を悪用した攻撃に対して安全か？
- **悪意のあるユーザ**によるE2EE技術を悪用した攻撃に対して安全か？

画像引用元：いらすとや

研究成果のまとめ ※ 暗号学的観点から

Zoom

ビデオ会議アプリ

脆弱性 6件

機密性	○
完全性	△
真正性	×

2020年12月：仕様の一部更新（2.3.1 → 3）

SFrame

リアルタイム通信用途のE2EEフレームワーク

脆弱性 3件

機密性	○
完全性	×
真正性	△

2021年3月：仕様の一部更新（1 → 2）

Nostr

𝕏（旧Twitter）に代わる分散型SNSアプリ

脆弱性 7件

機密性	×
完全性	×
真正性	×

2023年7月～2024年2月：仕様の一部更新

Rocket.Chat

slackライクなグループコミュニケーションアプリ

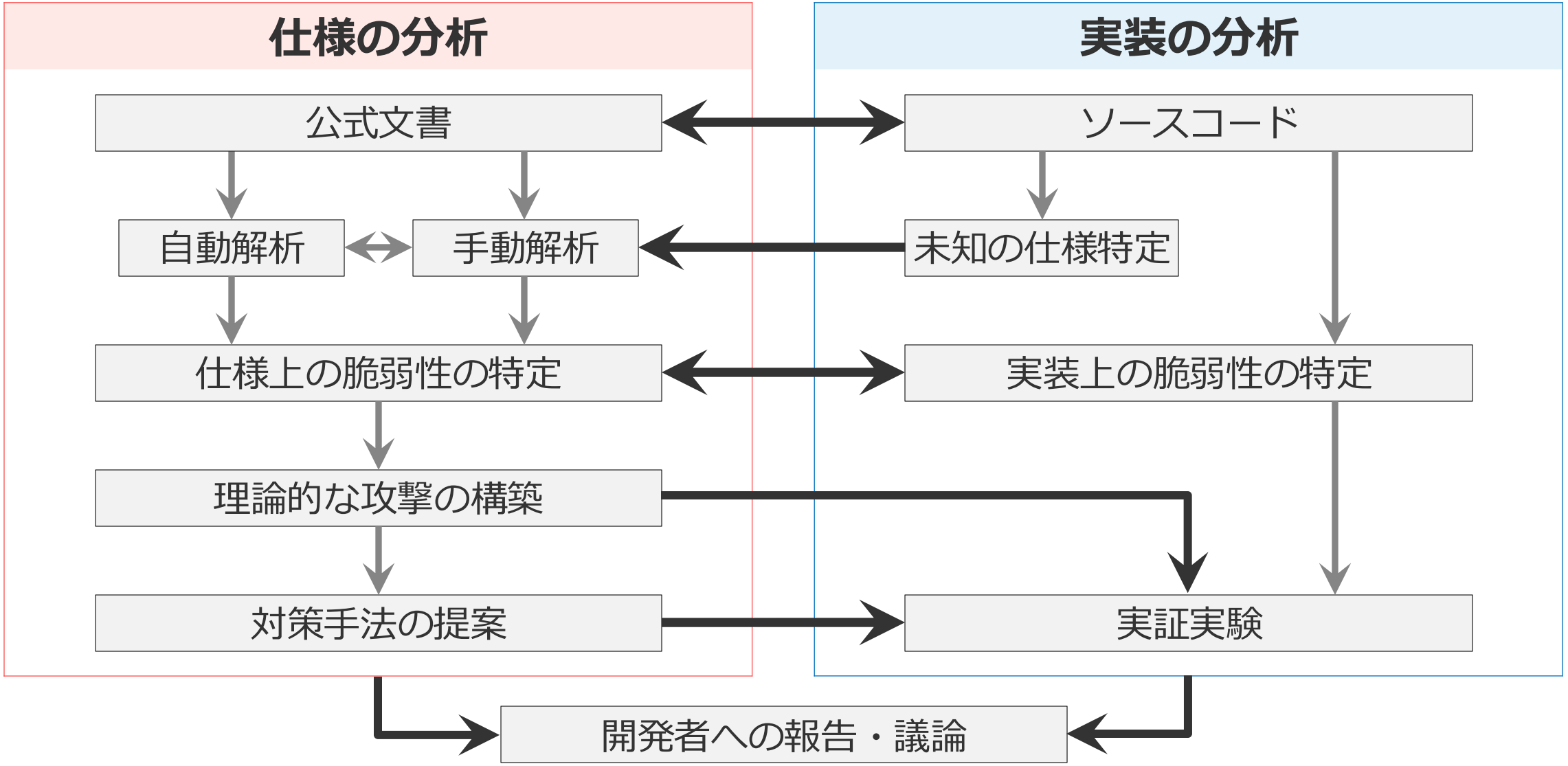
脆弱性 7件

機密性	×
完全性	×
真正性	×

2024年7～11月：仕様の一部更新

画像引用元：各公式サイト、Wikipedia

安全性評価の流れ


仕様の分析
実装の分析
公式文書
ソースコード
自動解析
手動解析
未知の仕様特定
仕様上の脆弱性の特定
実装上の脆弱性の特定
理論的な攻撃の構築
対策手法の提案
実証実験
開発者への報告・議論

得られた知見と教訓①：ビデオ会議アプリ

Zoom

ビデオ会議アプリ

脆弱性 **6件**

機密性	○
完全性	△
真正性	×

△ 仕様にNonce生成法が未記載

- AES-GCMにおけるNonce誤用の危険性
- 既存攻撃の適用：認証鍵入手 → 偽造可能

得られた知見・教訓

- 仕様にNonce生成法を明記
- Nonce誤用耐性のある認証暗号を採用

SFrame

リアルタイム通信用途のE2EEフレームワーク

脆弱性 **3件**

機密性	○
完全性	×
真正性	△

× 暗号方式・パラメータの選定ミス

署名済データに対して

- GHASH関数の線形性：$\mathcal{O}(1)$で偽造可能
- 短いタグ長（32ビット）：$\mathcal{O}(2^{32})$で偽造可能

得られた知見・教訓

- 適切な暗号方式の選定：**証明済**
- 適切なパラメータ（タグ長）の選定

画像引用元：各公式サイト、Wikipedia

得られた知見と教訓②：ビデオ会議アプリ

Zoom

ビデオ会議アプリ

脆弱性 6件

機密性	○
完全性	△
真正性	×

エンティティ認証の欠如

グループコミュニケーションのため

- AES-GCMによるデータの暗号化
- 署名機能の未実装：正当になりすまし可能

SFrame

リアルタイム通信用途のE2EEフレームワーク

脆弱性 3件

機密性	○
完全性	×
真正性	△

署名機能の削除

- 初期バージョン：（複数）タグに対する署名
- 我々の脆弱性報告に基づく削除

得られた知見・教訓

- 実装性能とのトレードオフ（開発者容認）
- 署名機能の導入方法：**今後の課題**

画像引用元：各公式サイト、Wikipedia

得られた知見と教訓③：メッセージアプリ

Nostr

𝕏（旧Twitter）に代わる分散型SNSアプリ

脆弱性 7件

機密性	×
完全性	×
真正性	×

Rocket.Chat

slackライクなグループコミュニケーションアプリ

脆弱性 7件

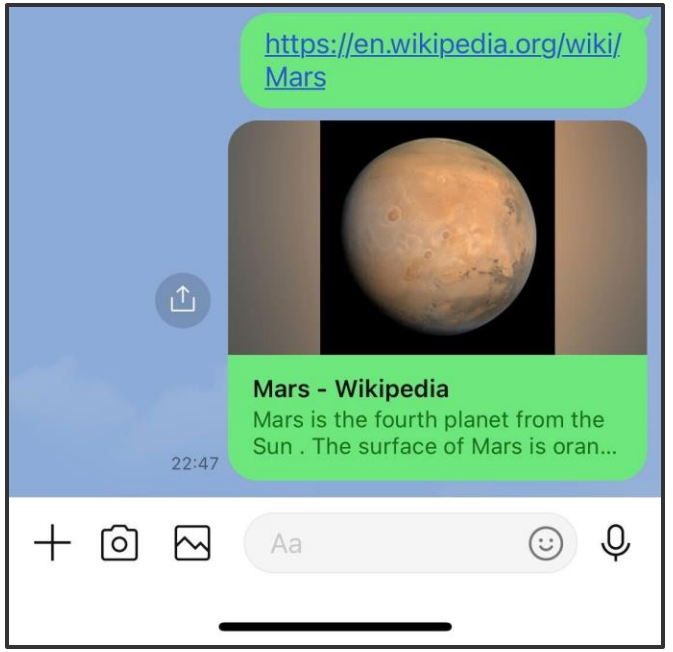
機密性	×
完全性	×
真正性	×

MACなしCBCモードの利用

- CBCに対する既存攻撃の適用：偽造可能
- 実装上の脆弱性（Link Preview機能）との組み合わせ：平文回復可能

得られた知見・教訓

- MACなしCBCモードの利用は非推奨
- E2EEの仕様だけでなく対象アプリの実装も考慮した解析が重要



LINEのLink Preview機能

得られた知見と教訓④：メッセージアプリ

Nostr

𝕏（旧Twitter）に代わる分散型SNSアプリ

脆弱性 **7**件

機密性	×
完全性	×
真正性	×

公開鍵の真正性検証の欠如

- 公開鍵：ユーザ識別用途、メタデータ
- **中間者攻撃**：通信内容の偽造可能

Rocket.Chat

slackライクなグループコミュニケーションアプリ

脆弱性 **7**件

機密性	×
完全性	×
真正性	×

公開鍵の真正性検証の欠如

- 公開鍵：鍵共有用途
- **中間者攻撃**：通信内容の傍受、偽造可能

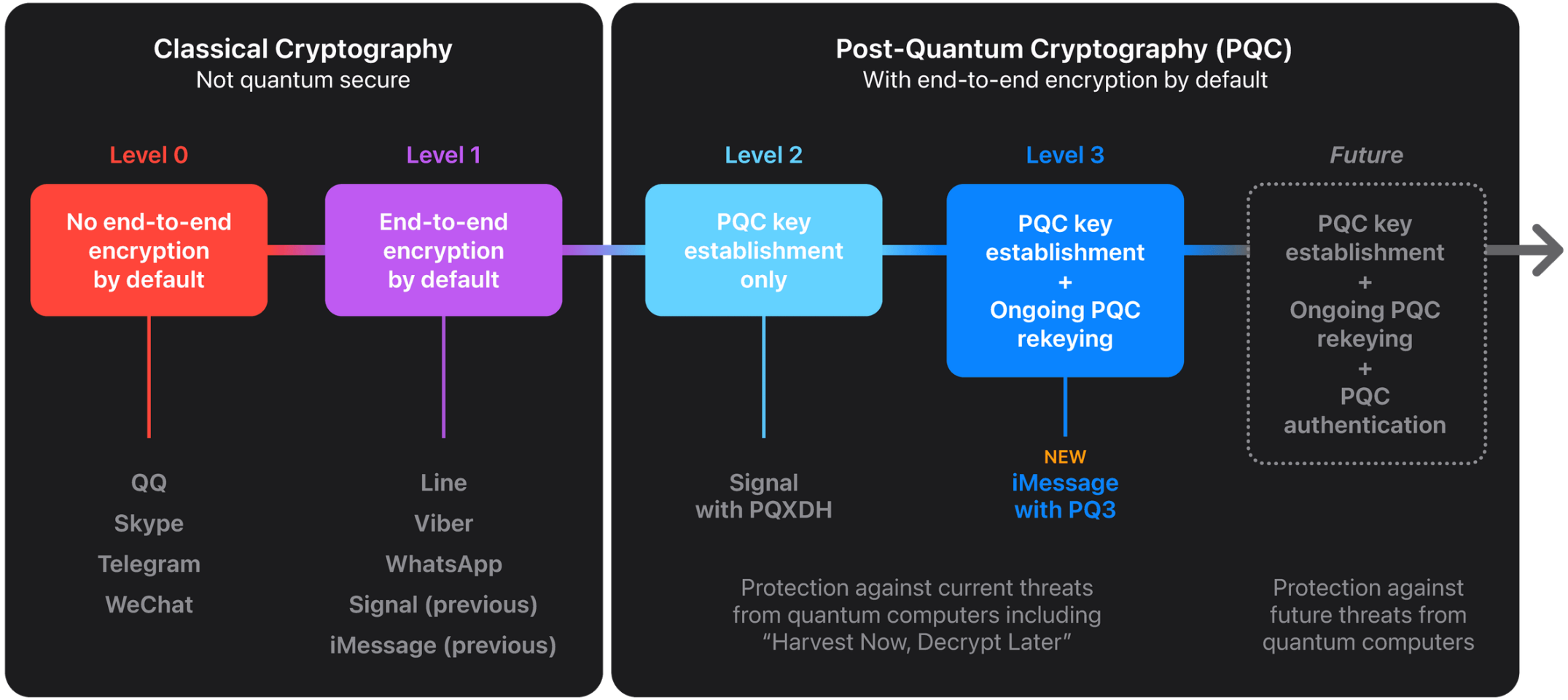
得られた知見・教訓

- 真正性検証のメカニズム導入：out-of-band認証など
- 中間者攻撃を防止するプロトコル設計

画像引用元：各公式サイト、Wikipedia

継 ～ つづける安全性評価、つなぐ安全性評価 ～

エンドツーエンド暗号化技術のPQC移行 – ハイブリッド方式の採用



Apple Security Blog "iMessage with PQ3: The new state of the art in quantum-secure messaging at scale"より*1

*1 https://security.apple.com/blog/imessage-pq3/ (February 2024).

画像引用元：Apple

継 ～ つづける安全性評価、つなぐ安全性評価 ～

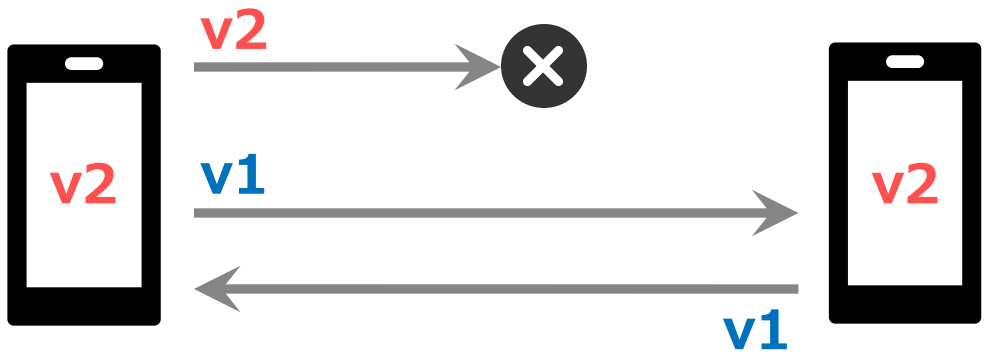
エンドツーエンド暗号化技術のPQC移行期間中における課題

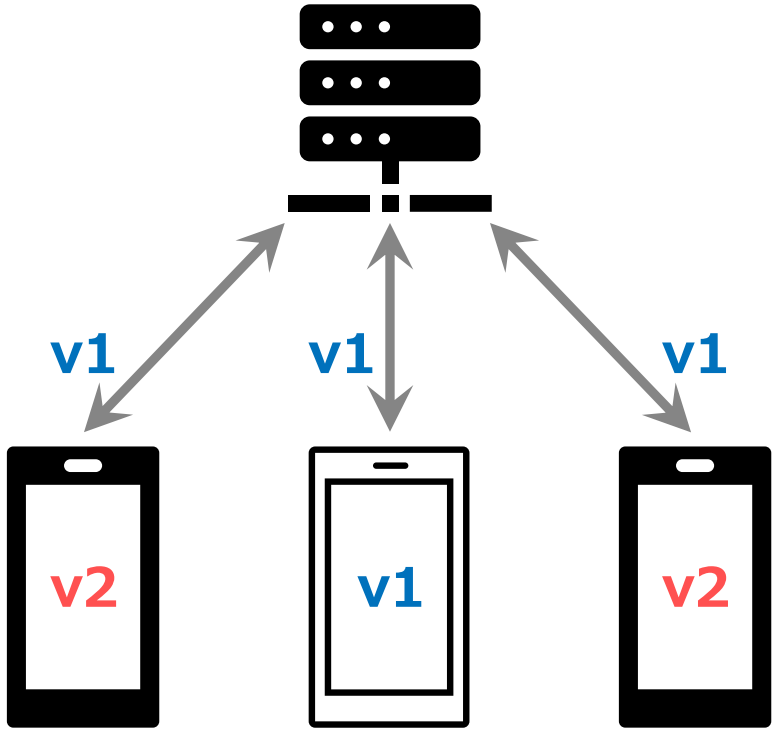
単純な移行

- ダウングレード攻撃への対策が必須

複数参加者のプロトコル

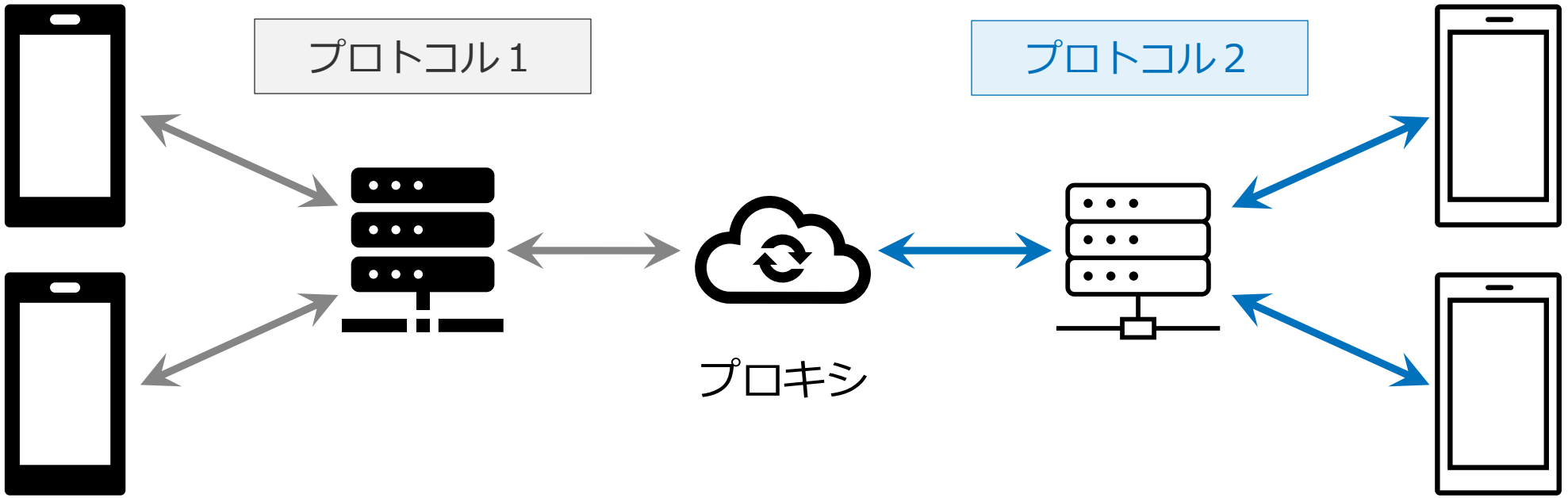
- 全参加者のアプリバージョンの一致が必須





継 ～ つづける安全性評価、つなぐ安全性評価 ～

相互運用性の確保（例：Matrix Bridge[*1]）



今後の展望

- PQC移行における**課題の再整理**、安全性評価による**教訓の収集**
- 相互運用性を確保する上での**課題の再整理**、安全性評価による**教訓の収集**

*1 https://matrix.org/ecosystem/bridges/