プレスリリース
2025年8月4日

国立研究開発法人情報通信研究機構
国立大学法人大阪大学
日本電気株式会社
兵庫県立大学

分散型 SNS プロトコル「Nostr」に対する世界初の包括的な安全性評価を実施

～ハッキング対策で最難関の国際会議 Black Hat USA 2025 Briefings で講演～

【ポイント】

- 世界で約 110 万人が利用する分散型 SNS プロトコル「Nostr」に対する世界初の包括的な安全性評価を実施
- 投稿の改ざんやなりすましなどにつながる重大な脆弱性を特定、攻撃を回避するための対策手法を構築
- ハッキング対策で最難関とされる国際会議 Black Hat USA 2025 Briefings で講演予定

国立研究開発法人情報通信研究機構（NICT、理事長：徳田　英幸）、国立大学法人大阪大学（総長：熊ノ郷　淳）、日本電気株式会社（NEC、取締役　代表執行役社長　兼　CEO：森田　隆之）、兵庫県立大学（学長：髙坂　誠）から成る共同研究チームは、世界で約 110 万人が利用する分散型 SNS プロトコル「Nostr」[*1]に対して、世界で初めて包括的な安全性評価を「仕様解析、実装調査、概念実証」の手法を用いて実施しました。投稿の改ざんやなりすまし、暗号化ダイレクトメッセージの復元などにつながる重大な脆弱性を特定し、これらを突く攻撃シナリオをハッカーに先駆けて設計し、その有効性を検証するとともに、対策手法を構築しました。これらの安全性評価の結果及び対策手法を各アプリ開発者へ報告し、プロトコル設計全般に対する改善点を示しました。

本成果をまとめた論文が学術会議 IEEE EuroS&P 2025 に採録されるとともに、ハッキング対策で最難関とされる産業系国際会議 Black Hat USA 2025 Briefings での講演が決定しており、学術界と産業界の双方から高い評価を受けています。

【背景】

これまでの SNS は、X に代表される中央集権型のものが主流であり、サービスの提供からデータ管理までの多くをプラットフォーム運営者に委ねることが一般的でした。しかし近年、プラットフォーム運営者の意向を強く反映したアルゴリズム改変やトレンド情報の操作に加え、プライバシーやセキュリティのリスクに係る懸念から、新たな選択肢として分散型 SNS が注目され始めています。分散型 SNS では、異なる運営者によって管理されている複数のサーバを通じてサービスが提供されており、ユーザは信頼できる運営者を選んで利用できます。プライバシーやセキュリティの設定においても、高い自由度を持つのが特徴です。

分散型 SNS プロトコル「Nostr」を採用するアプリの普及が進む一方で、その仕様と実装の複雑さから十分なセキュリティ検証が行われていませんでした。そのため、ハッカーからいつ攻撃を受けるかわからず、早急に対策する必要がありました。

【今回の成果】

本研究では、分散型 SNS プロトコル「Nostr」とそのクライアントアプリを対象に、「仕様解析、実装調査、概念実証」の手法を用いて包括的な安全性評価を行いました（図 1 参照）。複数のプロトコル設計間の連携不足といった構造的な問題が重なることで、投稿やプロフィールの改ざん、なりすまし、暗号化されたダイレクトメッセージの偽造や復元、送金用情報の書き換えなどにつながる重大な脆弱性を創出することを特定しました。これらの脆弱

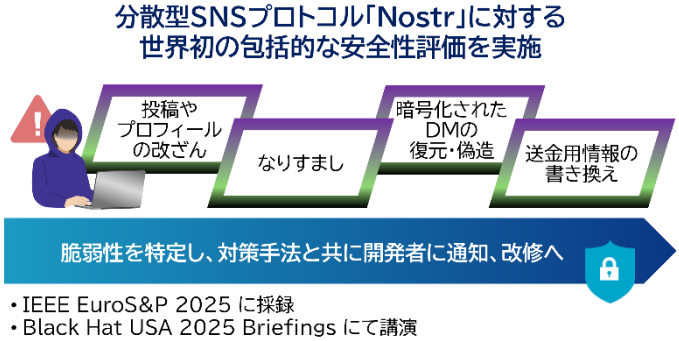

図 1 Nostr に対する安全性評価を実施

性を突く、具体的な攻撃シナリオをハッカーに先駆けて 8 種類設計し、Python による実証コードを用いて攻撃シナリオの有効性を検証しました。

これらの安全性評価の結果は、2023 年 6 月及び 2024 年 1 月に各アプリ開発者へ報告し、連携を開始しました。その際、攻撃シナリオを回避するための対策手法を提案するとともに、プロトコル設計全般に対する改善点を示しました。現在、これらの対策は主要クライアントアプリにおいて段階的にパッチ適用や機能改修が実施されています。

【今後の展望】

これまでの研究成果を基に、今後もその他の分散型 SNS アプリを含めた評価を行い、新世代 SNS の安全性向上を図ります。

＜論文情報＞

著者: Hayato Kimura, Ryoma Ito, Kazuhiko Minematsu, Shogo Shiraki, and Takanori Isobe
論文名: Not in The Prophecies: Practical Attacks on Nostr
掲載誌: The 10th IEEE European Symposium on Security and Privacy (EuroS&P) 2025

＜講演情報＞

講演者: Hayato Kimura
貢献者: Ryoma Ito, Kazuhiko Minematsu, Shogo Shiraki, and Takanori Isobe
講演タイトル: Not Sealed: Practical Attacks on Nostr, a Decentralized Censorship-Resistant Protocol
会議名: Black Hat USA 2025 Briefings
URL: https://www.blackhat.com/us-25/briefings/schedule/index.html#not-sealed-practical-attacks-on-nostr-a-decentralized-censorship-resistant-protocol-45726

なお、本研究は、JST、AIP 加速課題（AIP Accelerated Program）、JPMJCR24U1 及び JSPS 科研費 JP24H00696 の支援を受けたものです。

＜用語解説＞

***1 分散型 SNS プロトコル Nostr**

分散型 SNS プロトコル Nostr は、署名や暗号化など暗号学的手法をユーザが直接用いて認証とメッセージ整合性を確保する設計思想を採用しています。これは、プラットフォーム運営者がアカウントや鍵管理を集中管理する、X に代表される中央集権型 SNS とは大きく異なります。分散型 SNS が中央集権型 SNS の課題を補完するプラットフォームとして急速に普及する一方で、分散型 SNS プロトコルの代表例とも言える Nostr は、複数のサブプロトコル（Nostr Implementation Possibilities, NIPs）を組み合わせて構築されているため、仕様間の不整合と仕様と実装の不整合が重大なセキュリティ上の欠陥に発展する可能性について十分に検証されていませんでした。特に、エンドツーエンド暗号化 DM（NIP-04）やリモート署名（NIP-46）とリンクプレビュー機構の相互作用は未解明でした。本研究は、これらの課題に起因する実用的な攻撃シナリオを明確化し、安全性を定量的に示すことを目的としました。

＜ 本件に関する問合せ先 ＞

国立研究開発法人情報通信研究機構
サイバーセキュリティ研究所
セキュリティ基盤研究室
木村 隼人
E-mail: security@ml.nict.go.jp

国立大学法人大阪大学大学院
情報科学研究科マルチメディア工学専攻暗号基盤講座
教授 五十部 孝典
E-mail: takanori.isobe@ist.osaka-u.ac.jp

日本電気株式会社
NEC グローバルイノベーション戦略統括部
Web フォーム:
https://jpn.nec.com/cgi-bin/cs/opinion_form4.cgi

＜ 広報 （取材受付） ＞

国立研究開発法人情報通信研究機構
広報部 報道室
E-mail: publicity@nict.go.jp

国立大学法人大阪大学
大学院情報科学研究科研究戦略企画室
E-mail: ura-press@ist.osaka-u.ac.jp

日本電気株式会社
NEC グローバルイノベーション戦略統括部
Web フォーム:
https://jpn.nec.com/cgi-bin/cs/opinion_form4.cgi

兵庫県立大学 神戸情報科学キャンパス
E-mail: p-office@gsis.u-hyogo.ac.jp

補足資料

【解析の手法と結果の詳細】

本研究では以下の方法で Nostr を対象にセキュリティ解析と安全性評価を実施し、各サブプロトコルの相互作用に起因するリスクを整理しました。

1. **仕様解析**
   - Nostr の仕様書に記載された 56 個全ての機能（2023 年 12 月 6 日当時）を調査し、NIP-01、NIP-04、NIP-46 及び実装の欠陥の組合せによって潜在的に完全性を侵害することが可能であることを明らかにしました。
2. **実装調査**
   - iOS、Android、Web を含む主要クライアント 5 種を対象に、静的・動的な検査を実施し、複数のクライアントにおける署名検証の不備の脆弱性を発見しました。
   - 暗号化 DM のリンクプレビュー機構の実装上の不備を明らかにし、改ざん耐性のない暗号方式（AES-CBC）と組み合わせることで、効率的に暗号化 DM のメッセージを復元する手法を提案しました。
3. **概念実証**
   - 特定した 7 カテゴリの欠陥を組み合わせ、署名偽造・平文回復など 8 種の攻撃シナリオ（図 2 参照）を設計し、Python による実証コードで確認しました。

主な攻撃シナリオ

安全性評価	対応する セキュリティ要件	検査対象
偽造攻撃 （公開鍵の真正性検証の欠如）	完全性	プロフィール情報，連絡帳， 暗号化ダイレクトメッセージ
偽造攻撃 （署名検証の不備）	完全性	プロフィール情報，連絡帳， Bitcoin送金機能
暗号化ダイレクトメッセージへの偽造攻撃 （鍵分離の不備）	完全性	暗号化ダイレクトメッセージ
平文回復攻撃 （Link Previewを介した URL 復元攻撃 & oracle attack ）	機密性	暗号化ダイレクトメッセージ
クライアント側キャッシュ実装の不備による 署名検証処理の回避	完全性	プロフィール情報

※概念実証で設計した8種の攻撃シナリオのうちの代表的な5種を記載

図 2 概念実証で設計した主な攻撃シナリオ

このセキュリティ解析により、以下の脆弱性が特定されました。

- **真正性への影響:** Nostr の仕様にはデータ送信者及び受信者の公開鍵が本物であるかどうかの検証機構がありませんでした（公開鍵の真正性）。この仕様上の不備を特定し、Nostr のネットワークへ接続するクライアントアプリケーションは公開鍵の単純な置換、差し替え攻撃に対して脆弱であることを発見しました。
- **完全性への影響:** 署名検証の欠落により、プロフィール、投稿を任意に改ざん・偽造できることを示しました。また、サブプロトコル間での暗号化鍵の再利用により、暗号化 DM を任意の内容に改ざん・偽造できることを実証しました。
- **機密性への影響:** 受信端末上のリンクプレビューの自動実行と CBC モードの改ざん耐性を持たない性質を利用し、ユーザ操作なしに DM の平文及び機密 URL を取得可能であることを確認しました。

これらの安全性評価の結果は 2023 年 6 月及び 2024 年 1 月に各アプリケーション開発者へ報告、連携を開始し、修正方法として公開鍵の検証方法の導入、署名検証、メディア取得機構を安全に連携させるための設計指針を提案し、プロトコル設計全般への改善点を示しました。

- **提示した改善策**
  1. 全てのイベントに対する署名検証の必須化
  2. 暗号化 DM への メッセージ認証コードまたは認証暗号の適用
  3. 受信端末上でのリンクプレビュー機構を無効化し、プレビューを送信側で生成
  4. 公開鍵の検証方法の提供（Out-of-band 認証, Key Transparency など）

これらの対策は主要クライアントで段階的にパッチ適用と機能改修が実施されています。