

配信先: 総務省記者クラブ、テレコム記者会、
文部科学記者会、科学記者会、
大阪科学・大学記者クラブ

プレスリリース
2026年4月23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

世界で利用されるチャットツール「Rocket.Chat」で複数の脆弱性を発見し改善へ

～産業系セキュリティ分野で難関の国際会議 Black Hat Asia 2026 Briefings で講演～

【ポイント】

- 世界で利用されるチャットツール「Rocket.Chat」に対して、“暗号の使い方の観点からの安全性評価”を世界で初めて実施
- 「メッセージの偽造」「暗号化メッセージの解読」「攻撃の長期化」などにつながる重大な脆弱性を発見し、攻撃を回避するための対策手法を構築
- 産業系セキュリティ分野で難関とされる国際会議 Black Hat Asia 2026 Briefings で講演予定

国立研究開発法人情報通信研究機構エヌアイシーティ(NICT、理事長: 大野 英男)、国立大学法人大阪大学(総長: 熊ノ郷 淳)大学院情報科学研究科、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)から成る共同研究チームは、商用として世界で約 1,200 万人が利用するオンプレミス型チャットツール「Rocket.Chat」¹を対象に、“暗号の使い方の観点からの安全性評価”を「仕様解析・実装調査・概念実証」の手法を用いて世界で初めて(NICT 調べ)実施しました。「メッセージの偽造」「暗号化メッセージの解読」「攻撃の長期化」などにつながる重大な脆弱性を発見し、これらを利用する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開発企業に報告し、プロトコル設計全般に対する改善点を示しました。

脆弱性を利用する攻撃を未然に防ぐことに貢献したこれらの成果をまとめた論文が学術会議 ACSAC 2025 に採録されるとともに、産業系セキュリティ分野で難関とされる国際会議 Black Hat Asia 2026 Briefings での講演(開催地: シンガポール、4月24日)が決定しており、学术界と産業界の双方から高い評価を受けています。

【背景】

これまでの商用チャットツールは Slack や Microsoft Teams に代表される Software as a Service (SaaS) 形式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運営者に委ねることが一般的でした。しかし近年、企業における高機密データの管理や外国企業の SaaS 利用による越境データ管理のリスクに係る懸念から、自組織の管理するサーバにプログラムを設置し、メッセージやユーザデータを自組織に留めることができるオンプレミス型のチャットツールが注目され始めています。

オンプレミス型の商用チャットツールである「Rocket.Chat」は、高機密データを安全に扱うための機能としてテキストメッセージのエンドツーエンド暗号化²を採用しています。国内外の民間企業や外国の自治体への普及が進む一方で、「Rocket.Chat」のエンドツーエンド暗号化は独自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、未知の脆弱性による攻撃のリスクがあり、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、オンプレミス型チャットツール「Rocket.Chat」を対象に、“暗号の使い方の観点からの安全性評価”を「仕様解析・実装調査・概念実証」の手法を用いて世界で初めて行いました(図 1 参照)。その結果、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、「メッセージの偽造」や「暗号化メッセージの解読」につながり、また、暗号化・復号の両方に使う鍵³の漏えい対策機能の不備により「攻撃の長期化」につながる脆弱性を発見しました。

これらの脆弱性について、想定される攻撃の成立条件を明らかにするため、具体的な 5 種類の攻撃シナリオを設

計しました。さらに、概念実証として、攻撃シナリオを実装し各シナリオが実際に成立することを検証しました。

安全性評価の結果は、2024年5月に開発企業である Rocket.Chat Technology 社へ報告し、同社との連携を開始しました。その際、発見された攻撃を回避するための対策手法を提案するとともに、プロトコル設計全体に対する改善点を提示しました。その後、2024年10月から2025年12月にかけて、影響度の高い攻撃シナリオに対するパッチ適用や機能改修が実施されました（リリースノート <https://github.com/RocketChat/Rocket.Chat.ReactNative/releases/tag/4.51.0> にはこの連携に対する謝意表明 (special thanks) が付されています）。

本成果は、脆弱性を利用する攻撃を未然に防ぐことに貢献したものであり、産業系セキュリティ分野で難関とされる国際会議 Black Hat Asia 2026 Briefings で講演が予定されるなど、学术界と産業界の双方から高い評価を受けています。

【今後の展望】

これまでの研究成果を基に、今後もチャットやメッセージングサービスで利用される暗号方式の評価を行い、新しい世代のコミュニケーションツールの安全性向上を図ります。

<論文情報>

著者: Hayato Kimura, Ryoma Ito, Kazuhiko Minematsu, and Takanori Isobe

論文名: Gravity of the Situation: Security Analysis on Rocket.Chat E2EE

掲載誌: The 41st meeting of the Annual Computer Security Applications Conference (ACSAC 2025)

URL: <https://ieeexplore.ieee.org/document/11392069>

<講演情報>

日時: 2026年4月24日(現地時間)

講演者: Hayato Kimura

貢献者: Ryoma Ito, Kazuhiko Minematsu, and Takanori Isobe

講演タイトル: Payload Compromised: Full Key Recovery in Rocket.Chat E2EE

会議名: Black Hat Asia 2026 Briefings

URL: <https://blackhat.com/asia-26/briefings/schedule/?#payload-compromised-full-key-recovery-in-rocketchat-e2ee-50105>

なお、本研究は、JST ACT-X JPMJAX25M8、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。

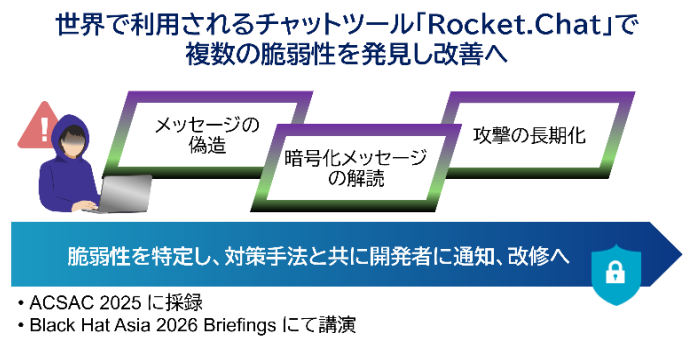


図1 「Rocket.Chat」に対する安全性評価を実施し改善へ

【解析の手法と結果の詳細】

本研究では以下の方法で「Rocket.Chat」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

- 「Rocket.Chat」の仕様書に記載された E2EE 機能(2023 年 12 月 6 日当時)を調査し、仕様及び実装の欠陥の組合せによって潜在的に完全性と機密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 3 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。

3. 概念実証

- 特定した 6 カテゴリの欠陥を組み合わせ、メッセージの偽造、暗号化・復号鍵回復など 5 種の攻撃シナリオ(図 2 参照)を設計し、HTTP プロキシツール及び Rust 言語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
公開鍵の鍵置換・鍵挿入による中間者攻撃(公開鍵の真正性検証の欠如)	機密性	暗号化鍵配送プロトコル
鍵回復攻撃(オフライン攻撃耐性の欠如 & 初期パスワード生成器の脆弱性)	機密性	鍵バックアッププロトコル
暗号化メッセージへの偽造攻撃(完全性検証の欠如 & 既知のメタデータの暗号化 & メッセージフォーマットの検証不備)	完全性	メッセージ暗号化プロトコル
再送攻撃(メタデータの完全性検証の欠如)	完全性	メッセージ暗号化プロトコル
ダウングレード攻撃	完全性	メッセージ暗号化プロトコル

※概念実証で設計した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:** 「Rocket.Chat」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、「Rocket.Chat」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、差替え攻撃に対して脆弱であることを発見しました。攻撃者は鍵配布時に鍵の置換・差替えによる中間者攻撃を行うことで暗号化メッセージの暗号化・復号鍵を不正に入手できることを実証しました。
- 完全性への影響:** 暗号化メッセージに改ざん検知機能が提供されていないことを明らかにしました。また、攻撃者は暗号文中に第三者が推測可能な情報(既知平文)が含まれることを利用し、暗号化メッセージを任意の内容に偽造できることを実証しました。
- 機密性への影響:** 暗号化バックアップにおいて E2EE 用鍵の保護に使用される初期パスワード生成アルゴリズムの不備を明らかにしました。これにより、バックアップにアクセス可能な攻撃者が現実的な時間(2 週間程度)でグループメッセージの暗号化鍵を復元する手法を提案しました。
- 回復能力の不備:** 「Rocket.Chat」は暗号化バックアップ用パスワードの更新及びリセット機能が提供されており、パスワード紛失時や漏えい時に使用することができます。しかし今回の解析により、更新及びリセット時に暗号化・復号鍵が更新されず、漏えいした可能性のある鍵を新規メッセージの暗号化・復号に使用し続けることを明らかにしました。これにより、本機能がパスワード漏えい時の対策としては不十分であることを示しました。

これらの安全性評価の結果は 2024 年 5 月 30 日に開発企業である Rocket.Chat Technology 社へ報告、連携を開始し、修正方法として公開鍵の検証方法の導入、暗号文の完全性検証の導入、パスワード生成方式の修正、パスワードリセット方式の修正に関する設計指針を提案し、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

- 暗号化ダイレクトメッセージへのメッセージ認証コード又は認証暗号の適用
- 公開鍵の検証方法の提供(Out-of-band 認証など)
- パスワードに依拠しない暗号化バックアップの構成方法

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。

<用語解説>

*1 オンプレミス型チャットツール「Rocket.Chat」

オンプレミス型チャットツール「Rocket.Chat」は、エンドツーエンド暗号化を採用している。オンプレミス型とは開発企業がサーバプログラムを配布し、ユーザ組織が運用するもので、Slack や Microsoft Teams に代表される SaaS 型チャットツールとは大きく異なる。また、エンドツーエンド暗号化はサーバを含む通信経路上の攻撃者による送受信メッセージの閲覧や改ざんを防止する技術である。オンプレミス型チャットツールが SaaS 型の課題を補完するツールとして急速に普及する一方で、オンプレミス型チャットツールの代表例とも言える「Rocket.Chat」は、複数のプロトコル(鍵配布、メッセージ暗号化、鍵の暗号化バックアップ)を組み合わせられ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なかった。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た。

*2 エンドツーエンド暗号化

エンドツーエンド暗号化(E2EE)は、スマートフォンや PC などの通信を行う端末間でデータを保護する暗号化通信方式であり、通信経路上のネットワーク機器やサービス事業者のサーバなどの第三者による盗聴や改ざん攻撃からメッセージを保護する。これにより、通信内容は送信者と意図された受信者のみが閲覧可能となる。エンドツーエンド暗号化は、メッセージングサービスやクラウドストレージサービスなどに広く実装されており、近年のデジタルコミュニケーションにおいて利用者のプライバシー保護と安全な通信を支える重要な役割を果たしている。その一方で、事業者ごとに異なる暗号化方式が採用されているため、その安全性や実装内容を個別に評価することが重要である。

*3 暗号化・復号の両方に使う鍵

暗号化と復号に同一の鍵を用いる共通鍵暗号方式における鍵を指し、「Rocket.Chat」のエンドツーエンド暗号化方式ではメッセージの暗号化に使用される。本研究では鍵の暗号化バックアップ機能の設計と実装の不備により攻撃者がこの鍵を入手し、通信内容の盗聴及び暗号文の偽造ができることを示した。