

ビデオ会議システムにおける エンドツーエンド暗号化技術の安全性

伊藤 竜馬^{1,a)}

概要：新型コロナウイルス感染症の世界的流行に伴い、ビデオ会議システムの利用が世界中で拡大している。また、ユーザのプライバシーを保護するためにエンドツーエンド暗号化（E2EE）技術の必要性も高まっており、多くのビデオ会議システムにおいて E2EE 技術の導入計画が進行中である。本講演では、代表的なビデオ会議システムの Zoom, Google Duo, Cisco Webex, Jitsi Meet など導入される E2EE 技術の安全性について紹介する。はじめに、Zoom Video Communications 社が発行するホワイトペーパーのバージョン 2.3.1 に基づき、Zoom に導入される E2EE 技術について紹介する。さらに、IETF が公開するインターネットドラフトのバージョン draft-omara-sframe-01 に基づき、Google Duo, Cisco Webex, Jitsi Meet など導入される E2EE 技術の SFrame について紹介する。次に、これらの E2EE 技術に内在する複数の脆弱性を明らかにするとともに、これらの脆弱性を悪用することで他人へのなりすまし、メッセージの偽造・改ざん、サービス利用の拒否に繋がる攻撃が実行できることを示す。最後に、これらの攻撃に対する効果的な対策手法について紹介する。本講演で紹介する評価結果については Zoom の安全性評価チームと SFrame の設計チームに報告済みである。なお、2021 年 10 月現在、Zoom の E2EE 技術に関するホワイトペーパーのバージョンは 3.1 であり、SFrame に関するインターネットドラフトのバージョンは draft-omara-sframe-03 である。

キーワード：エンドツーエンド暗号化, Zoom, Google Duo, Cisco Webex, Jitsi Meet, SFrame, 認証暗号, 署名, なりすまし, 偽造, 改ざん, サービス拒否

¹ 国立研究開発法人情報通信研究機構
National Institute of Information and Communications
Technology, Koganei, Tokyo 184-8795, Japan
^{a)} itorym@nict.go.jp