

情報通信研究機構

# NICT 先端研究

(199)

ビデオ会議システム  
のZoomやWebex  
などで幅広く導入さ  
れているエンドツーエ  
ンド暗号化技術。TL  
S通信のようなサーバ  
ー・クライアント暗号  
化通信とは異なり、通  
信相手との間でのみメ  
ッセージの送受信が可

能であり、サービスのセキュリティ確保  
ロバイダーであってもに欠かせない技術であ  
メッセージの盗聴、改ざん、改ざん、サ  
びンライン教育の場でもエンドツーエ  
デオ会議システムの利

用が拡大していること  
を踏まえると、安心・  
安全なテレワーク時代

情報通信研究機構  
(NICT)では、兵  
価では、他人へのなり  
攻撃として、我々が提  
防対策について提案

Zoomの安全性評  
定するよりも強力な攻  
撃として、我々が提  
防対策について提案

これらの脆弱性を利  
用した3種類の攻撃手  
法を提示するとともに  
、電子署名方式を採用  
しているにもかかわらず  
、Zoomの安全性評

御対策について提案し  
た。特に、Zoomの  
脆弱性を利用した3種  
類の攻撃手法を提示  
するとともに、電子  
署名方式を採用して  
いるにもかかわらず、  
Zoomの安全性評

めがメッセージの真  
正性を保証するために  
、電子署名方式を採  
用しているにもかかわらず  
、Zoomの安全性評

Zoomの安全性評  
価チームとSFrame  
eの設計者に対して速  
やかに脆弱性報告を  
実施したところ、Zoom  
とSFrameの仕  
様が速やかに修正さ  
れていることを確認し  
た。

Google Duo、Cisco  
Webex、Jitsi Meet  
などの導入予定のエ  
ンドツーエンド暗号化  
技術の脆弱性を発見し  
、これを指摘した。

これらの脆弱性を利  
用した8種類の攻撃手  
法を提示するとともに  
、この脆弱性に繋がる  
3種類の脆弱性を発見  
し、これを指摘した。

SFrameの安全  
性評価では、他人へ  
の脆弱性を発見し、  
これを指摘した。

これらの脆弱性を利  
用した3種類の攻撃手  
法を提示するとともに  
、電子署名方式を採用  
しているにもかかわらず  
、Zoomの安全性評

## エンドツー ビデオ会議安全運用

サイバーセキュリティ研究所・  
セキュリティ基盤研究室 主任研究員

伊藤 竜馬

19年阪大院博士後期課程修了、20年4月  
NICT入所。共通鍵暗号の安全性評価に  
関する研究開発に従事。博士（工学）。



### テレワーク時代のセキュリティー技術

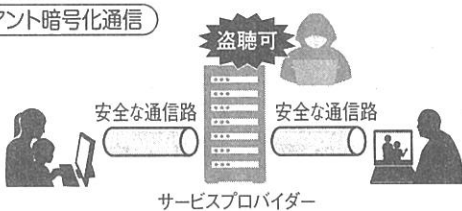
#### エンドツーエンド暗号化通信

- Zoom
- Google Duo
- Cisco Webex
- Jitsi Meet



#### サーバー・クライアント暗号化通信

- TLS



我々の安全性評価  
は、なりすまし、改ざ  
ん、サービス利用拒否  
などの攻撃手法に対し  
て耐性のあるシステム  
を設計する場面で効果  
を発揮し、テレワーク  
などで利用するビデオ  
会議システムの安心・  
安全な運用に貢献でき  
るものとして期待され  
ている。

(火曜日に掲載)