Zoom における情報セキュリティの留意点
Inomata-20200407-v1

Zoom 社によるテレビ会議システムにおいてはいくつかのセキュリティに対する懸念事項が報告されているが、大阪大学として関係のある点のみ以下にまとめておく。なお、セキュリティ的な課題はあるものの Zoom そのもののサービスを否定するものではない。利用者において注意していただきたいのは、テレビ会議で扱われる内容のレベルをきちんと把握した上で利用してほしいという点である。教育目的として、例えば公開型の授業のライブ配信では十分利用しても問題ないと思われるが、テレビ会議主催者が取り扱う内容、参加者を事前に把握した上で提供することが大切である。

Zoom 爆弾によるテレビ会議妨害

Zoom では会議参加用の URL が提供され、参加者はその URL へのリンクをクリックするだけで参加できるようになっている。この URL がテレビ会議 ID であることの利点を悪用し、テレビ会議のパスワードを設定していない場合には悪意あるユーザがテレビ会議を妨害することが可能となる。

対処方法：テレビ会議主催者がパスワードを設定（ただしパスワードが漏洩すれば同様のリスクは発生する）。現在はデフォルトでパスワード必須となっている。

対策案：現在はテレビ会議開始時に参加者を待ち合い室に待機させる仕様となっており、主催者によって参加承認処理が行われないとテレビ会議に参加できない（設定でこれを無効にする変更は可能）。

暗号モジュール問題

End-to-End 暗号化が不十分な実装のため、正確にいうならば End-to-End で暗号化はされていない。これについては Zoom 社も認めている。さらに問題として指摘されているのは暗号化鍵を管理する Zoom 社のサーバが中国に存在していたという点である。
https://blog.zoom.us/wordpress/2020/04/01/facts-around-zoom-encryption-for-meetings-webinars/

これにより想定されるリスクとしては Zoom によるテレビ会議を録画していた場合には、暗号化されていたはずの録画内容が Zoom 社によって復号可能である点である。

対処方法：現在においては Zoom 社は修正したと述べている

実装不具合

Windows 版において報告されている実装の不具合として、チャット機能において使われている UNC パス(Universal Naming Convention Path)の脆弱性（パスワードハッシュ実装不具合）を有している点である。これによりログイン情報を悪意あるユーザに窃取される可能性がある。

対処方法：クライアントを version 4.6.9 以降にアップデート

詳細については、別途情報推進部による「Zoom による遠隔授業・会議の際の情報セキュリティに関する留意点について」を参照のこと。