# Web 会議のセキュリティ

## Web 会議のセキュリティポイント

| | | |
|---|---|---|
| ① アプリの脆弱性 | ・・・ | 設計上の脆弱性、情報漏えいの可能性など |
| ② 通信の暗号化 | ・・・ | SSL や AES など、通信が暗号化されている |
| ③ 参加資格の制限 | ・・・ | 第三者が参加できないようにする |
| ④ サーバ側の対策 | ・・・ | アプリサーバが、セキュリティ対策されているか |
| ⑤ ログ管理 | ・・・ | 会議の入退出など必要な情報が記録されているか |
| ⑥ 参加者の意識 | ・・・ | 参加する場所や環境、過失が起こらないよう注意 |

テレワークにより、Web 会議が盛んに使用されるようになると、ネット会議のセキュリティが心配です。
Web 会議システムには、少人数であれば無料で使用できるものもたくさんあり、簡単な設定で使用できてしまうこととのトレードオフで、セキュリティが甘いと指摘されてニュースになっているツールさえあります。
使い勝手が良いツールは、当然人気があり流行って多くの人が使用します。そうなると、悪意を持った第三者にとっては、なおさらターゲットとしたい相手が使用する率もあがり、そのツールを狙って脆弱性を見つけ、時には勝手に他人の会議に参加して、秘密情報の入手を試みたりします。
クラウド型の Web 会議システムは、手軽で取り込みやすいので人気ですが、中には中国経由で通信されていると噂になるものがあったり、サーバ側の運用方法がよくわからないものもあるため、機能や導入のし易さだけでなく、セキュリティ面での仕組みや管理方法をチェックすることが重要です。
ツール選定だけ気を付ければよいのではなく、使用する側のセキュリティ意識も大切です。ネットを使用している訳なので、社内の会議室のように他人が出入りすることはないという考えは改めなければいけません。
便利さを追求すると、本来当たり前の個人認証や暗号化などの機能の組み込みが甘くなってしまいます。多くの Web 会議システムは、あらかじめ ID 登録しておかなくても、メールや SNS で招集すれば誰でも参加できるミーティングルームを作れるような機能も有しており、会議の目的に応じて参加資格を制限できるようになっています。
こうなると、Web 会議を使う側のセキュリティ対策として、テレワークで使用する会議は、面倒であっても例外なく事前登録して ID 認証によって参加資格を持つもの以外使用できないことを厳格化しておくべきです。また、招集についても、SNS 等のパブリックなクラウドを使用しているものを避け、VPN 接続された会社指定のメールシステムでのみ会議招集するようにルール化すべきです。重要な会議でないからと、安易にこの点を怠ると、本来社内でしか知られてはいけない内容を軽率にしゃべってしまい営業秘密が漏れるような事故を起こしかねません。
Web 会議システムも、セキュリティポリシーに照らし合わせ、脆弱性の確認はもちろん、いつだれが使用したかログを残し、見知らぬ人が参加していた形跡がないこともチェックできるように仕組みを作ることが必要です。
セキュリティポリシーも Web 会議の進化に合わせ、企業内で再確認してアップデートすることが望ましいです。


© CEC Customer Service Ltd.