中小企業の

セキュリティー対策

―41―

Web会議の注意事項

在宅勤務で急速に拡大

新型コロナウイルス感染症の影響により在宅勤務が広く行われ、Web会議サービスの利用が急速に拡大している。Web会議サービスの活用は大変有益である一方、盗聴、情報漏えい、サイバー攻撃などのセキュリティーリスクに十分注意する必要がある。

独立行政法人情報処理推進機構（IPA）では、Web会議サービスを使用する場合に注意すべきセキュリティー上のポイントをまとめてWebサイト（https://www.ipa.go.jp/files/000083955.pdf）で公開したので参考にしてほしい。

サービス選定時には

Web会議サービス選定時に考慮すべきポイントとしては、次の点が挙げられる。

①会議データの所在

Web会議サービスは、音声、映像、共有資料、チャット、録画・録音データなど、多種のデータを扱う。これらのデータがどこに格納されるかは、情報漏えいリスクに大きく影響する。

クラウドサービスの場合、負荷分散のため海外のデータセンターが利用されることがある。データセンターが置かれた国によっては、政府が法に基づきデータを強制収容するリスクがある。どの国のデータセンターを使用するかは通常契約で決められるが、無料サービスでは契約プロセスを通さないため、特に注意が必要である。

また、クラウド上に録画・録音データを保存する場合には、復元不可能な形で完全削除ができるかの確認も重要である。

②暗号化

通信路が安全でない場合、重要な会議データの盗聴、改ざんの脅威が発生する。

Web会議サービスがエンドツーエンド暗号化の場合は、会議参加者の音声・映像データが参加者端末で暗号化され、他の参加者端末で復号される。暗号鍵は参加者のみが保有するため、サービス提供者は復号できない。

一方、サービス提供者が暗号鍵を持つ場合、サービス提供者が信頼できるとしても、海外には政府によるサーバのデータの強制収容リスクがあることに注意する。

③会議参加者の確認・認証方式

意図しない者が会議に参加することにより、会議進行の妨害、機密情報の漏えいが発生する。

Web会議サービスのデータセンター配置イメージ

意図しない者の会議への参加を防ぐためには、会議案内メールの安全な経路での配付と共に、会議パスワードが一の場合には参加者を強制退室できる機能も重要である。

④プライバシーポリシー

Web会議サービスでは音声・映像、参加者のメールアドレスの属性など、さまざまな個人情報を扱う。これら個人情報が会議目的以外で第三者提供を含め使用されないこと、個人情報保護法などの法律、規制に準拠していることを確認する必要がある。

⑤脆弱性と企業姿勢

サービス提供者のウェブサイト、JVN iPedia、ニュースなどの脆弱（ぜいじゃく）性情報をウオッチし、Web会議サービスの脆弱性の発生状況、対策状況を把握する。また、サービス提供者のセキュリティーに対する取り組み姿勢と情報公開姿勢も重要である。サービス提供各社のウェブサイトなどで最新のセキュリティー対策状況を確認することをお勧めする。

取引先などの指定もあるかと思うが従業員任せにせず、企業としてどのWeb会議サービスを利用するか選定し、従業員に対して利用の可否を指示することが重要である。

（独立行政法人情報処理推進機構・江島将和）