Web 会議サービスを使用する際のセキュリティ上の注意事項

2020 年 7 月 14 日
独立行政法人情報処理推進機構
セキュリティセンター

1. はじめに

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ます。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、サイバー攻撃等のセキュリティリスクに十分注意する必要があります。

本資料では、Web 会議の主催者が、Web 会議サービスを使用する際に注意すべきセキュリティ上のポイントを紹介いたします。

（注）本資料における「Web 会議サービス」は、音声、映像、資料、チャット等をリアルタイムに交換可能なクラウドサービスとします（オンプレミスは除きます）。代表的な Web 会議サービスに関しては（※1）を参照下さい。

2. 対象とする読者

法人組織の Web 会議主催者、および、情報システム管理部門

3. Web 会議サービス選定時に考慮すべきポイント

Web 会議サービスを選定する際にセキュリティ上考慮すべきポイントを以下に示します。これらは、セキュリティリスクを極力軽減し、Web 会議サービスを安全に使用するために考慮すべき項目です。なお、米国国家安全保障局（NSA：National Security Agency）、CISA（Cybersecurity and Infrastructure Security Agency）が公表している政府職員向けの Web 会議サービス使用時の注意事項(※2、※3)を参考にしています。

3. 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・録音データ等、多種のデータを扱います。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します。主催者は使用する Web 会議サービスがクラウドサービス、オンプレミスのいずれかを、まず確認することが必要です。
- 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ります（図1参照）。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ります。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ますが、無料サービスでは契約プロセスを通さないため、本件は特に注意が必要です。
- 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（セキュアデリート機能の有無）の確認も重要です。

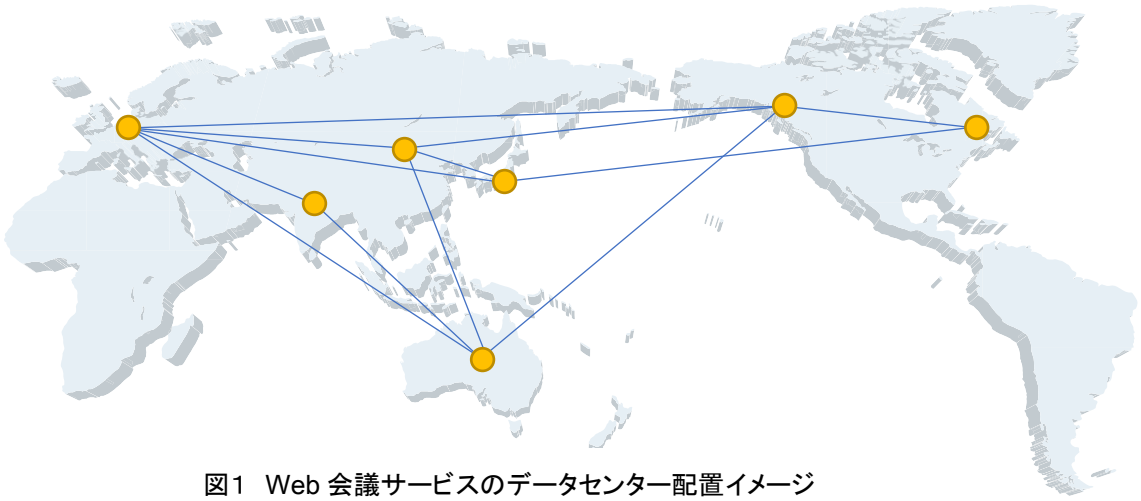

図1　Web 会議サービスのデータセンター配置イメージ

3．2　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します。

・まず、Web 会議サービスにおける会議データの暗号化方式で注意すべき点は、Web 会議サービス提供者（以下、サービス提供者）が暗号鍵を持つのか否か、という点です。Web 会議サービスが「サービス提供者が暗号鍵をもたないエンドツーエンド暗号化」か、「サービス提供者が暗号鍵を持ち会議データがサーバで復号可能な方式」かを確認しましょう。

・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ます。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ません。

・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しましょう。

・Web 会議サービスがエンドツーエンド暗号化とそれ以外の両方の動作モードを持つ場合、エンドツーエンド暗号化を選択するとサーバでの復号を必要とする機能は使えなくなる可能性があります。制限事項を事前に確認しましょう。

・サービス提供者の Web サイト等で、安全性が確認されている暗号アルゴリズムや通信方式が採用されているかを確認しましょう。安全性が確認されている暗号アルゴリズムとしては CRYPTREC 暗号リスト(※5)の「電子政府推奨暗号リスト」または「推奨候補暗号リスト」を、通信方式としては TLS 暗号設定ガイドライン(※6)の「推奨セキュリティ型」または「高セキュリティ型」等を参考にしてください。

3．3　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します。意図しない者の会議へ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、会議参加者の確認・認証方式の選定が重要です。

・ 会議参加者の確認・認証方式に関しては、会議パスワード設定機能、待機室（ロビー）での参加者確認機能、参加者の事前登録機能、参加者名の設定機能、二要素認証等、各種メニューが用意されています。主催する会議の機密性、参加人数等に応じた最適な方式の選択をする必要があります。

（注）参加者名の設定機能：参加者名に会議毎に特定の規則を設ける、参加者に参加者名を事前に申告させる等の運用を想定しています。

・ 主催者が、誰が参加しているかを容易に確認でき、万が一の場合には参加者を強制退室できる機能も重要です。

3．4　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等の属性等様々な個人情報を扱います。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、個人情報保護法等の法律、規制に準拠していることを確認する必要があります。

3．5　脆弱性と企業姿勢

・ サービス提供者のウェブサイト、JVN iPedia、ニュース等の脆弱性情報をウォッチし、Web 会議サービスの脆弱性の発生状況、対策状況を把握しましょう。

・ サービス提供者のセキュリティに対する取り組み姿勢と情報公開姿勢も重要です。また、各サービス提供者のウェブサイト等で、一般の利用者にもわかりやすいセキュリティ上の注意事項等や最新のセキュリティ対策状況が公開されているかを確認することをお勧めします。

・ サービス提供各社のウェブサイト等で最新のセキュリティ対策状況を確認することをお勧めします。

4．Web 会議サービスを安全に開催するためのポイント

Web 会議サービスを安全に開催するために注意すべき主なポイントを会議開催の流れにそって説明します。

4．1　会議の準備

（1）会議の機密性の確認

□　会議の機密性を確認したか？

・ セミナー・講演会と、経営情報・顧客情報等の機密情報を扱う会議では、会議の機密性が異なります。それぞれに応じ最適な会議開催方法を選択する必要があります。まず、各組織の規則に従い会議の機密性を確認して下さい。

（2）会議の機密性に応じた Web 会議開催方法の決定

会議の機密性に応じて以下の項目を考慮し会議開催方法を決定します。

□ エンドツーエンド暗号化の会議は利用可能か？利用できない場合、サーバで万が一復号されるリスクは許容可能か？

□ 会議参加者に外部組織の人がいる場合には、それら組織のセキュリティポリシーに準拠しているかについての参加者の同意を得たか？

□ Web 会議サービス参加者の制限を明確にし、会議の設定を適切に行っているか？
- 非公開会議の場合は、会議を非公開に設定する。
- 意図しない参加者を避けるため、会議パスワードを設定し、待機室機能を有効にする。
- 参加者の入室時に許可する機能（主催者以外全員ミュート状態等）を確認する。
- 会議の機密性、会議参加者の人数に応じ、会議案内メールと別経路での会議パスワードの送付、参加者の二要素認証、参加者の事前登録機能等を適切に使用する。

□ 万が一意図しない参加者が登場した場合に備え、参加者の強制退室機能が使えることを確認したか？

（3）Web 会議開催案内

□ 会議 URL、会議パスワード等を記載した会議開催案内の送付経路は安全か？
- 非公開会議の場合、ソーシャルメディア経由の案内は避けるべきです。

□ 機密性の高い会議の場合、万が一の案内メールの漏えいに備え、メールの題名は機密性を悟られない文面となっているか？

4．2 会議の実施

（1）参加者の確認

□ 組織外参加者がいる会議では特に、意図しない第三者が会議に参加しないよう、参加者確認業務の担当者を明確にしているか？
- 参加者の確認方法としては、顔、声による確認も有効です。

（2）会議終了後のデータ削除

□ 会議録音・録画データ、共有資料、チャット等の会議データがクラウド上に存在する場合には、クライアント端末への移動・暗号化、クラウド上からの削除を実施したか？

4．3 その他の一般的注意事項

以下の項目は参加者も含め守るべき一般的注意事項です。

（1）会議で使用するクライアント端末のセキュリティについて

□ クライアント端末のセキュリティ対策は十分か？
- 基本的にはセキュリティ対策が十分に管理されている組織からの支給端末、または、BYOD（Bring Your Own Device）として組織から許可され一定のセキュリティ対策が施されている私物端末の使用が望まれます。
- Web 会議サービスのクライアントソフト、および、クライアント端末の OS 等は、脆弱性の悪用を防ぐため常に最新の状態にアップデートを行う事が必要です。
- Web 会議サービスのクライアントソフトをダウンロードする時は「偽サイト」に注意しましょう。サービス提供者の公式サイトや公式マーケット等からダウンロードしてください。(※4)

（2）会議の参加環境

□ 機密情報および個人情報保護のために、意図しない映り込みや音声の漏えいを避けるよう、参加者端末の場所、映像の背景が配慮されているか？

5．機密性別の Web 会議の開催例

機密性の異なる Web 会議をいくつか取り上げ、3．で挙げたポイントの内、「（1）会議データの所在」、「（2）暗号化」、「（3）会議参加者の確認・認証方式」をどう考慮したかの例を以下に示します。

5．1 “機密性高”の会議

（1） 音声データ等の会議データのクラウド上での復号は、会議の機密性の観点から、いかなる形であれ許されないと判断した。Web 会議サービスの資料共有、録画機能は使用せず、音声・映像交換およびチャット機能のみを使用することとした。資料の共有は安全な形でメール添付ファイルとして事前配布し、それを参照する形とした。

（2） Web 会議サービスはエンドツーエンド暗号化ができる製品を使用することとした。また、国内データセンターのみを使用する契約とした。

（3） 会議パスワードを設定、待機室機能を有効とし、会議パスワードは会議案内メールとは別経路で組織外参加者に安全に届けることとした。また、組織外参加者については会議実施時に声、顔での確認を必ず実施することにした。

5．2 “機密性中”の会議

（1） 会議資料のクラウド上への保存は、情報漏えいリスクを考え望ましくないと判断した。Web 会議サービスの資料共有、録画機能は使用せず、資料の共有は安全な形でメール添付ファイルとして事前配布し、それを参照する形とした。また、ホワイト国のデータセンターのみを使用する契約とした。

（2）暗号化に関しては、サーバで一時的に復号される方式であることを確認し、参加者端末、サーバ間の通信が安全であることを確認した。

（3）会議パスワードを設定、待機室機能を有効とし、会議案内メールは安全な形で参加者に届け、会議実施時の参加者確認は担当者をアサインし実施した。

5．3 “機密性低”：事前申し込みを必要とする講習会

（1）会議資料、会議の内容とも機密性は低いため、Web 会議サービスは全機能（音声・映像交換、資料共有、チャット等）を使用することとし、データの所在（海外・国内等）にはこだわらなかった。

（2）参加者端末、サーバ間の通信が安全であることを確認した。

（3）参加人数が多いため、参加者事前登録の機能を使用し、参加者の事前確認をするとともに、会議の URL は参加者のみに届け、会議実施時の参加者確認は担当をアサインし実施した。

6．参考資料

（※1）ビデオ会議アプリをセキュリティ面からみる（株式会社カスペルスキー）
https://blog.kaspersky.co.jp/videoconference-software-security/28229

（※2）Selecting and Safely Using Collaboration Services for Telework（NSA）
https://media.defense.gov/2020/Jun/03/2002310067/-1/-1/0/CSI-SELECTING-AND-USING-COLLABORATION-SERVICES-SECURELY-LONG-20200602.PDF

（※3）Cybersecurity Recommendations for Federal Agencies using video Conferencing（CISA）
https://www.cisa.gov/sites/default/files/publications/CISA_Cybersecurity_Recommendations_for_Federal_Agencies_Using_Video_Conferencing_S508C.pdf

（※4）ソフトウェアのダウンロードは信頼できるサイトから！～そのソフトは、あなたが使いたいソフトですか？（IPA）
https://www.ipa.go.jp/security/anshin/mgdayori20200428.html

（※5）CRYPTREC 暗号リスト（CRYPTREC）
https://www.cryptrec.go.jp/list.html

（※6）TLS 暗号設定ガイドライン（IPA）
https://www.ipa.go.jp/security/ipg/documents/ipa-cryptrec-gl-3001-3.0.1.pdf