Web会議は“3つのセキュリティリスク”に対策を！

テレワーク実施時の注意点

01

Web会議には「セキュリティ対策」が必須

テレワークでは、Web会議システム上での情報漏洩や、使用している端末が不正アクセスを受けることによる情報漏洩、自宅以外のスペースで会議に参加し会話を盗み聞かれることによる情報漏洩など、幾重にもリスクが広がっています。

働き方改革の推進や、新型コロナウイルス感染症が広まった影響で、テレワークという働き方を選択する企業や就業者が増加し続けています。国土交通省の調査によると、令和2年度におけるテレワーカーは雇用・自営型を合わせた全体の就業者の22.5%を占めて過去最高となり、前年度（令和元年度）と比較すると約7ポイントも上昇しました。
（参照元：国土交通省「令和2年度　テレワーク人口実態調査」https://www.mlit.go.jp/report/press/content/001391381.pdf）

テレワークは、オフィスという場所にとらわれない柔軟な働き方であり、「社員が育児や介護をしながら仕事ができる」、「遠隔にいる優秀な人材を取り込める」など多くのメリットをもたらします。一方で、勤怠管理が難しいことや社員評価制度の見直しが必要となるなど、急激に普及が進んだことによる新たな課題が出てきているのも事実です。中でも「セキュリティ対策」は、重要な課題の1つとされています。

例えば通常、出社せずに社内ミーティングを行う場合や、取引先とやり取りを行う際にはZoomなどのWeb会議システムを利用します。これらはお互いが遠くにいても音声や動画で話すことが可能な、便利なシステムです。しかし、Web会議システム上での情報漏洩や、使用している端末が不正アクセスを受けることによる情報漏洩、自宅以外のスペースで会議に参加し会話を盗み聞かれることによる情報漏洩など、幾重にもリスクが広がっています。

テレワークでは、これまでオフィス内で守られていた企業の情報やデータを、書類などを物理的に持ち出さなくても漏らしてしまう危険性があるのです。セキュリティ対策を行わなければ、重大なインシデントを招きかねません。

02

Web会議における3つのセキュリティリスクの事例と対策

テレワークなどに利用されるWeb会議システムにおけるセキュリティリスクには、どのようなものがあるのでしょうか。

ここでは3つのリスクにスポットを当てて、どのような事態を引き起こすことが考えられるのか、そしてどのような対策が効果的なのかをみていきます。

リスク 01

Web会議システムの脆弱性を狙った不正アクセス

- まずセキュリティ面で信頼できるWeb会議システムを選定することが最も重要
- 機能面では、アクセス制限などの機能が備わっているのか、また会議データなどは暗号化されているのかといった点についてもチェック
- Web会議システムを導入してからも、使用しているそれぞれの端末で、こまめにアップデートを行うように注意喚起

Web会議システムでは音声や動画のやり取りに加えて、チャットや資料のアップロードができる機能などがあります。いわば日常の業務で取り扱っているさまざまな情報のやり取りがそこに集約されているわけです。セキュリティ対策を講じているWeb会議システムを選択しなければ、不正アクセスによって会議内容を盗み見られる、資料が不正ダウンロードされる、使用している端末を危険にさらすようなファイルがアップロードされるといった被害に遭遇する可能性があります。
このようなリスクを避けるためには、まずセキュリティ面で信頼できるWeb会議システムを選定することが最も重要です。運営元は信頼できる企業なのか、企業や法人が使用することを想定してセキュリティ対策を行っているのかを予め確認しておきましょう。
機能面では、アクセス制限などの機能が備わっているのか、また会議データなどは暗号化されているのかといった点についてもチェックして選ぶことをおすすめします。さらに、Web会議システムを導入してからも、使用しているそれぞれの端末で、こまめにアップデートを行うように注意喚起することも必要です。常に最新の状態にしておくことは、あらゆる脆弱性への対応力を高めることにつながります。

03

Web会議における3つのセキュリティリスクの事例と対策

リスク 02

Web会議参加者の保存データが社外に流出

- Web会議に利用するPCやタブレット側にも適切なセキュリティ対策を
- Web会議のデータなどの取り扱いに関するルールを策定
- ルールにはWeb会議のデータを閲覧するために共有するIDやURLなどの取り扱いについて明記

Web会議に利用するデータや、会議内容を端末に保存することもあるでしょう。そのような場面においては、Web会議に利用するPCやタブレット側にも適切なセキュリティ対策がなされていなければなりません。対策を怠ると、マルウェアに感染し保存データが流出してしまうことがあります。また、企業内のネットワークに保存する場合においても、不正ログインなどにより情報が漏れてしまう危険性をはらんでいます。

このようなケースにおいても、まずは端末やサーバーなどにセキュリティ対策を講じておくことが必要不可欠です。特にテレワークにおいては、誰がどのような端末を使用して、どのようなセキュリティ対策を施しているのかを把握しておかなければなりません。その上で、Web会議データなどの取り扱いに関するルールを策定して、会議に参加する社員に周知徹底するとよいでしょう。

ルールには、Web会議のデータを閲覧するために共有するIDやURLなどの取り扱いについて明記しておく必要があります。

04

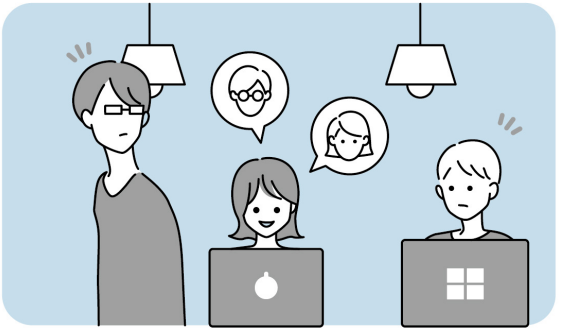
Web会議における3つのセキュリティリスクの事例と対策

リスク 03

オープンスペースでのWeb会議参加による情報漏洩

- セキュリティ対策は、「**どこでWeb会議に参加するのか**」も見落としてはいけないポイント
- オープンスペースでは、**周囲に話の内容を聞かれたり、会議中の画面を見られてしまったり**など、情報が漏れる可能性
- **公共のWi-fiは暗号化されていないものが多い**ため、情報漏洩のリスクがあるときには使用を避ける

セキュリティ対策は、Web会議システムや企業内ネットワークなどのソフト面に加え、「どこでWeb会議に参加するのか」も見落としてはいけないポイントです。利用場所が自宅であれば他の人に話を聞かれるといった心配は非常に少ないでしょう。
しかし、サテライトオフィスやコワーキングスペースなど、さまざまな人がいる場所でWeb会議システムを利用したときには周囲に話の内容を聞かれたり、会議中の画面を見られてしまったりなど、情報が漏れる可能性があります。
このような場合、テレワークを行っている社員の働く環境が自宅なのか、それ以外の場所なのかを把握しておく必要があります。同時に、コワーキングスペースなどを利用する際には、Web会議の内容が周りに聞かれることのないような工夫がされている場所を利用するよう、社員に徹底するとよいでしょう。また、外で仕事をする際には、公共のWi-fiサービスを使うこともあります。公共のWi-fiは暗号化されていないものが多いため、Web会議に参加する際や、機密性の高い情報を扱う際など、情報漏洩のリスクがあるときには使用を避けるように、社員に周知しておきましょう。



05

まとめ

テレワークは、Web会議システムを利用するがゆえに、さまざまな情報漏洩のリスクが発生します。
想定されるセキュリティリスクを理解して、それぞれに有効な対策を講じていかなければなりません。
また、同時に社員のセキュリティ・リテラシーも高めていく必要があります。

プラザクリエイトが提供する**パーソナル・ミーティング・ボックス「One-Bo（ワンボ）」**は、防音性能や視認度を変更できるスマートガラスを備えており、あらゆるWeb会議のセキュリティリスクを解決することができる個別空間です。オフィス内の会議室不足や、イヤホンの音漏れ防止にも役立ちます。
強固なセキュリティ体制づくりを進めるためにも導入を検討されてみてはいかがでしょうか。
（https://www.one-bo.com/）

また、自社で導入している**「リモートワークと出社勤務のハイブリッド体制」における従業員向けガイドラインをWeb上で公開**しておりますので、テレワークの導入・定着を実現するソリューションとしてぜひ、ご活用ください。
(https://www.one-bo.com/guide/)

パーソナル・ミーティング・ボックス
「One-Bo（ワンボ）

「リモートワークと出社勤務の
ハイブリッド体制」
における従業員向けガイドライン