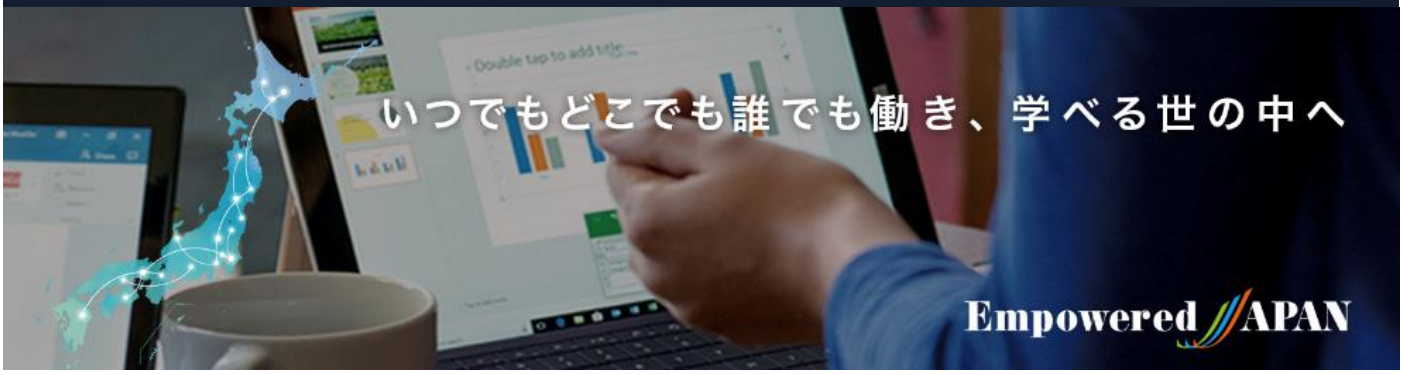
Empowered JAPAN 実行委員会 緊急ウェブセミナー 講演レポート



Empowered JAPAN 緊急ウェブセミナー

Empowered JAPAN 実行委員会はテレワークをはじめとする働き方改革や学び直しを通した「いつでもどこでも誰でも、働き、学べる世の中へ」をコンセプトに、2018 年に発足しました。東京圏および地方都市におけるテレワーク啓蒙イベントをはじめ、多くの自治体や協力会社と共に企業・個人向けテレワーク研修を実施してきました。この度のコロナウイルス感染拡大と 2020 年 2 月 25 日の政府基本方針に含まれた「テレワーク推奨」の呼びかけを受け、全国の組織や個人がテレワークを早期に実施するため、実践的な情報をお伝えするための緊急ウェブセミナーを 2020 年 3 月 17 日より連続的に無料開催しています。

カテゴリ：

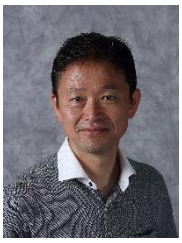
IT ツール、環境

開催日時：2020 年 4 月 16 日

講師：

Microsoft

マイクロソフトコーポレーション
サイバーセキュリティ・ソリューションズ・グループ
（CSG） チーフ セキュリティ アドバイザー



日本マイクロソフト株式会社
政策渉外・法務本部 弁護士
中島 麻里氏

Teams プライバシー・セキュリティへの取り組み

テレワークの急速な普及によって、オンライン会議のシステムの利用も急増しています。利用にあたっては、利便性だけでなく"安全性"の担保が重要に。代表的なサービスの一つ、「Microsoft Teams」のセキュリティに対する取り組みを解説します。

同サービスを提供するマイクロソフトでは、セキュリティ対策のために毎年 1,000 億円の投資を行い、全世界から 3,500 人のスペシャリストを集めています。その一人として、米国本社に在籍する花村実さんによると、情報セキュリティはこの 10 年で大きく変化してきたのだと言います。「かつては重要なデータをできるだけ内部の"信頼ゾーン"に囲って守るというネットワーク境界モデルが一般的でしたが、それでは限界があったことからクラウド活用へのシフトが進みました」（花村氏）

クラウドを活用することによって、セキュリティの管理責任の一部をクラウドベンダーに委託することも可能に。経験が蓄積されるベンダーを経由することで、不正アクセスの検知・対処にかける時間が短縮。より効率的なセキュリティ対策が可能になります。

「生産性をとるか、セキュリティをとるか」という"OR"から、両立を目指す"AND"の発想へと移行したのはテクノロジーの進化によるもの。生体認証や多要素認証、条件付きアクセスなどの技術の普及により、安全性を確保しながら業務効率も高められる環境が整ってきました。
また、「失敗を前提にするマインドシフト」が起きたのも大きな変化です。「鉄壁の防御を目指すのではなく、"どんなに備えても侵入される"という前提で、レジリエンス（早くリカバリーする）で挑むのが基本姿勢に。こういった流れの中で、マイクロソフトが提供する各サービスの安全性も日夜進歩しています」（花村氏）。

Empowered JAPAN 実行委員会 緊急ウェブセミナー 講演レポート

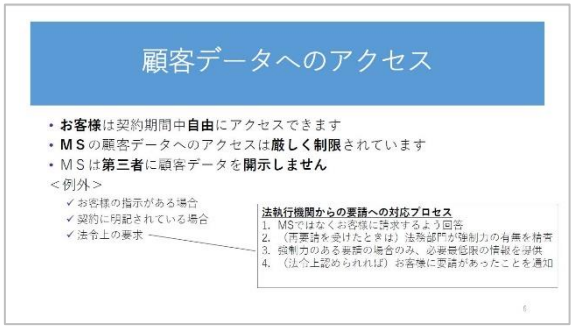
また、「失敗を前提にするマインドシフト」が起きたのも大きな変化です。「鉄壁の防御を目指すのではなく、"どんなに備えても侵入される"という前提で、レジリエンス（早くリカバリーする）で挑むのが基本姿勢に。こういった流れの中で、マイクロソフトが提供する各サービスの安全性も日夜進歩しています」（花村氏）。

実際、テレワークで注目を集めるオンライン会議システム「Microsoft Teams」では、どのようなセキュリティ対策が講じられているのでしょうか。

まず製品設計としては、データ流出を防ぐための対策が、多段階で取られています。組織外のメンバーが会議参加する際には「待機」の設定が可能であったり、多要素認証によって不正アクセスからの攻撃を防いだりと、"招かれざる客"を入室させない対策を徹底。加えて、会議の内容を記録したデータはチャットも含めてすべて暗号化され、組織外の参加者に自社データを共有する際にも一定の制御も可能。さらに、AI がチャットを巡回し、ハラスメントを防止する機能も備えています。これらの対策は、90 以上の国際的な規制基準や法律に準拠し、チェックを受けており、「どこで働いても、会社で働くのと同レベルの安全性を担保できる環境を目指しています」（花村氏）。

では、万が一の対策も含めてのコンプライアンスはどのように規定しているのでしょうか。日本マイクロソフトで法務の視点から国内導入企業の支援を行なっている弁護士の中島麻里さんが、その概要を解説します。

「お客様からお預かりしたデータの保護が最優先である。このポリシーに基づいて、製品やサービスの設計がなされています」（中島氏）。
具体的な取り組みとして、まず挙げられるのは「データはお客様のもの」という姿勢の明示です。「Microsoft Teams」を利用して実施された会議の録画や、チャットなどの関連データ(顧客データ)は「すべて顧客が権利を持つ」と規定しています。
それらの顧客データの使用目的（クラウドサービス機能の提供や、トラブルシューティングなど）は契約に明記し、目的外使用を禁止。広告目的の利用などは一切許されていません。
マイクロソフトからのアクセスも厳しく制限されています。お客様の要望などで例外的にデータにアクセスする場合介入が必要な場合などは例外になります。「その際には、いつどのようなアクセスをしたのかの記録が残り、顧客はいつでも監視できるようになっています」（中島氏）。サービス提供に関わる下請会社のリストもウェブ上で公開されています。
顧客の指示がある場合や法令上の要求がある場合を除いては「第三者への情報開示はしない」という方針も徹底。警察・司法当局などから法令上の要求をうけた場合、まずは顧客に直接請求するように回答し、再要請を受けたときにはマイクロソフトに対する強制力の有無を確認。強制力があると判断した場合のみ、必要最低限の情報を提供し、法令で禁止されていない限り顧客に報告するという対応プロセスを策定しています。実際の対応状況や件数もウェブで公開しており、透明性のある情報公開に努めています。「2019 年上半期、法人向けクラウドに関して、全世界で受けた開示請求は 74 件。うち 32 件は非開示の回答をしています」（中島氏）。



契約終了後のデータ削除プロセスについても、明確にルール化されています。契約終了から 90 日間は、顧客によるデータ抽出が可能になるよう、機能限定アカウントにデータは保持されますが、90 日を過ぎるとその機能も凍結。契約終了から 180 日後までにデータは消去されます。

以上の取り組みの詳細や関連情報については、マイクロソフトのウェブサイト内「トラスト センター」に随時公開されています。各国の法規制など一般情報も閲覧できるのでご活用ください。