中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）関連資料

設定解説資料
（Microsoft Teams）

ver1.0（2020.9.11）

本書は、総務省の令和２年度「テレワークセキュリティに係るチェックリスト策定に関する調査研究」事業（受託者：NRI セキュアテクノロジーズ株式会社）により作成したものです。

本書に関する問い合わせ先（個別のシステムおよび環境に関する御質問については、製品の開発元にお問い合わせください。）
総務省 サイバーセキュリティ統括官室
Email telework-security@ml.soumu.go.jp
URL https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

目次

1 はじめに

(ア) 本書の目的

本書は、「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）」の第 2 部に記載されているチェックリスト項目を、Microsoft Teams（以下単に「Teams」と記載します。）を利用している環境で実現する際の具体的な作業内容の解説を行うことで、管理者が実施すべき設定作業や利用者が利用時に実施すべき作業の理解を助けることを目的とする。

(イ) 前提条件

本製品のライセンス形態は無償ライセンスと Teams 及び複数の Office アプリケーション含む有償エディションが存在します。（2020 年 8 月 1 日現在）

利用するライセンス種類により使用可能な機能が異なります。本資料では「Microsoft 365 Business Basic」ライセンスの利用を前提としております。

(ウ) 本書の活用方法

本書は、中小企業のセキュリティ管理担当者やシステム管理担当者(担当者ではないがこれらに準ずる役割を担っている方を含む)を対象として、その方々がチェックリスト項目の具体的な対策を把握することを助力するために、第 2 章にてチェックリスト項目に紐づく解説内容と解説ページを記載している。解説としては第 3 章にて管理者向けの設定手順を、第 4 章にて利用者向けの注意事項をそれぞれ記載している。

表 1. 本書の全体構成

章題	概要
1 はじめに	本書を活用するための、目的、本書の前提条件、活用方法、免責次項を説明しています。
2 チェックリスト項目と設定解説の対応表	本書で解説するチェックリスト項目と、その項目に対応する設定作業手順および利用者向け注意事項の解説が記載されたページを記載しています。
3 管理者向け設定作業	対象のチェックリスト項目に対する管理者向けの具体的な設定手順を解説しています。
4 利用者向け作業	対象のチェックリスト項目に対する利用者向けの注意事項を解説しています。

(エ) 免責事項

本資料は現状有姿でご利用者様に提供するものであり、明示であると黙示であるとを問わず、
正確性、商品性、有用性、ご利用者様の特定の目的に対する適合性を含むその他の保証を一切行うものではありません。

本資料に掲載されている情報は、2020 年 8 月 1 日時点の各製品の操作画面を基に作成しており、
その後の製品仕様の更新、追加、変更、削除もしくは部分改廃により、画面表示等に差異が生じる可能性があります。

本資料は、初期出荷状態の製品を単体動作させている環境を利用して設定手順を解説しています。
本製品をご利用者様の業務環境で利用する際には、本資料に掲載している設定により業務環境
システムに影響がないかをご利用者様の責任にて確認の上、実施するようにしてください。
本資料に掲載されている製品仕様・設定方法について不明点がありましたら、製品提供元へお問い合わせください。

2 チェックリスト項目に対応する設定作業一覧

本書で解説するチェックリスト項目および対応する設定作業解説および利用者向け注意事項が記載されているページを示します。

表 2. チェックリスト項目と管理者向け設定作業の紐づけ

チェックリスト項目番号	対応する設定作業解説	ページ番号
3-5 アクセス制御（論理） **オンライン会議の主催者は必要に応じて不適切な参加者を退出させるなどし、会議を適切に進行している。** **(クラウドサービス(オンライン会議)の利用がない場合は対象外)**	・ロビーの有効化	P.6

表 3. チェックリスト項目と利用者向け作業の紐づけ

チェックリスト項目番号	対応する設定作業解説	ページ番号
3-3 アクセス制御（論理） **オンライン会議の主催者はミーティングの開始時および途中参加者が出た際に、参加者の本人確認を実施している。** **(クラウドサービス(オンライン会議)の利用がない場合は対象外)**	・ミーティング時の本人確認	P.8
3-4 アクセス制御（論理） **オンライン会議にアクセスするための URL や会議参加のパスワードを不要なメンバーには伝えないようにしている。** **また、会議参加のパスワード設定を強制させることが可能な場合は、パスワード設定を強制している。** **(クラウドサービス(オンライン会議)の利用がない場合は対象外)**	・会議 URL の取り扱いについて	P.8
3-5 アクセス制御（論理） **オンライン会議の主催者は必要に応じて不適切な参加者を退出させるなどし、会議を適切に進行している。** **(クラウドサービス(オンライン会議)の利用がない場合は対象外)**	・不適切な参加者の強制退室	P.9
4-1 アクセス制御（物理） **テレワーク端末に対して覗き見防止フィルタを貼付し、離席時にはスクリーンロックをかけるようルール化している。**	・第三者からの盗聴・覗き見の対策	P.10
5-2 脆弱性管理 **テレワーク端末の OS やアプリケーションソフトウェアに対して最新のセキュリティアップデートを適用している。**	・アプリケーションの最新化	P.10

8-5 データ保護 **オンライン会議を実施する際に、会議のタイトルや議題に重要情報を記載しないことや、会議の録画ファイルに対してパスワードの設定や期間指定の自動削除、等を実施している。上記のルールを強制することが可能な場合は、強制するように設定する。** **(クラウドサービス(オンライン会議)の利用がない場合は対象外)**	・ミーティング情報の件名に機密情報の記載禁止 ・ミーティング録画ファイルの削除	P.11

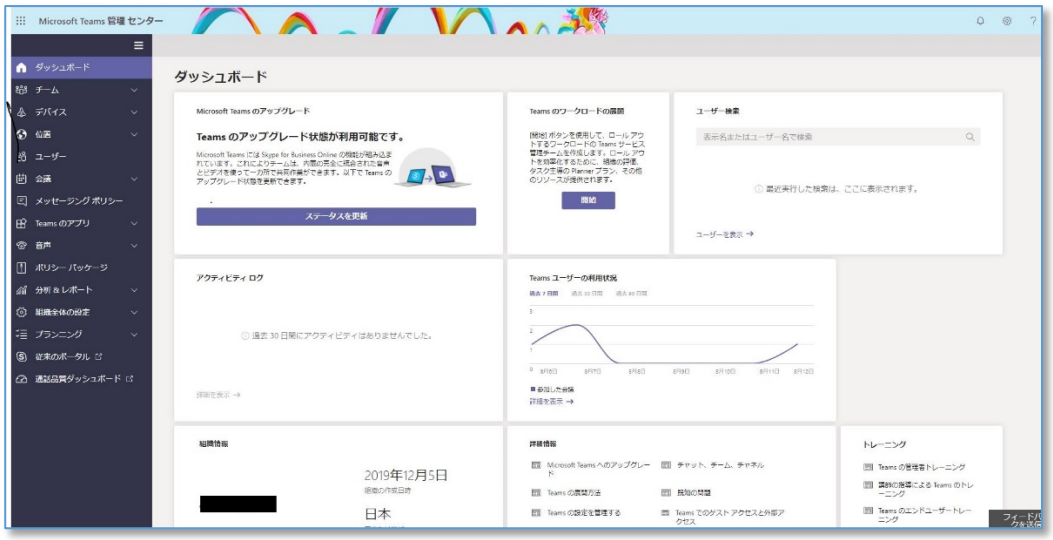
3 管理者向け設定作業

3-1 チェックリスト 3-5 に対応する設定作業

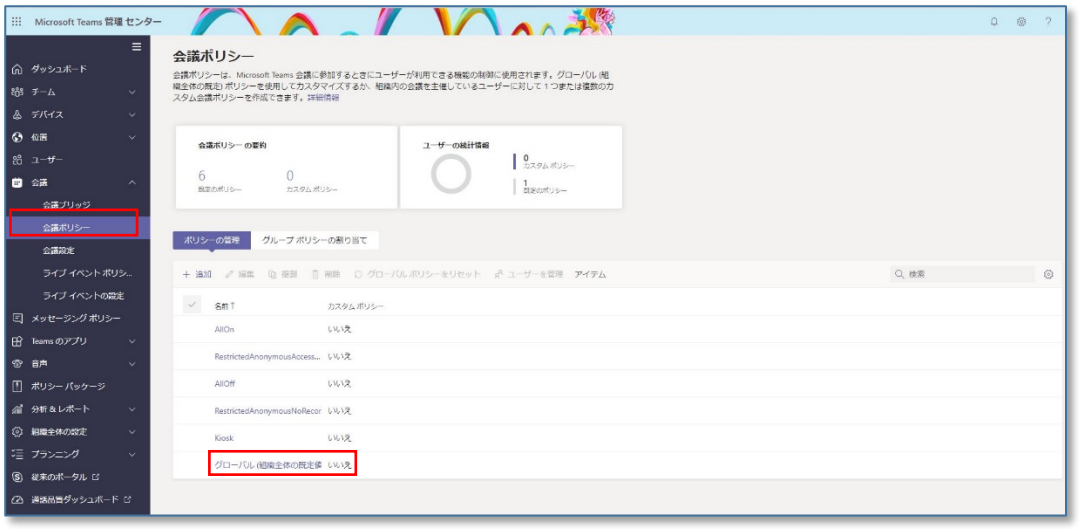
3-1-1 ロビーの有効化

ロビー機能により、会議主催者はミーティングに参加する参加者を制御することができます。
想定していない参加者がミーティングに参加出来ないようにすることにより安全なミーティングを確保します。

【手順①】
Teams 管理センター(https://admin.teams.microsoft.com)にログインし左ペインの「アカウント設定」をクリックするとミーティングに関連する設定画面が表示されます。



【手順②】
「会議」→「会議ポリシー」と進みポリシーの管理と進みます。
デフォルトで適用されているポリシーは「グローバル(組織全体の既定値)」になるためここではこちらのポリシーで変更していきます。対象のポリシーをクリックします。



【手順③】

次に「参加者とゲスト」の設定項目を設定していきます。

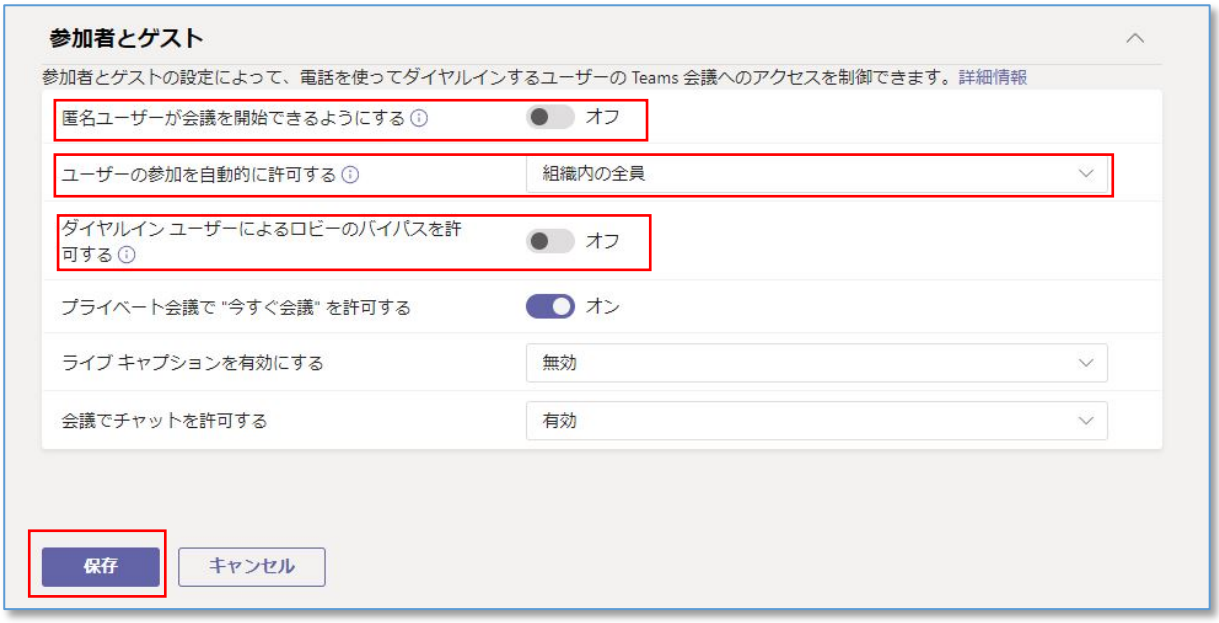
以下のように設定を変更します。

- 匿名ユーザーが会議を開始できるようにする → オフ
- ユーザーの参加を自動的に許可する → 組織内の全員（※1）
- ダイヤルインユーザーによるロビーのバイパスを許可する → オフ（※2）

※1：より厳しく制限したい場合は、全てユーザーを選択することも可能

※2：ダイヤルインユーザーとは Web 会議接続用の電話番号を使って参加するユーザーを示します。

最後に「保存」をクリックします。



これでロビー機能の有効化するポリシーの設定が完了します。

> ⚠ **注意事項**
>
> ポリシーの反映に関しては最大 24 時間のリードタイムが発生致します。
>
> 即時反映されませんのでご注意ください。

４利用者向け作業

ここでは本製品の利用者に対して、セキュリティ観点上、注意すべきことを記載致します。

４-１チェックリスト 3-3 に対する利用者向け作業

４-１-１ミーティング時の本人確認

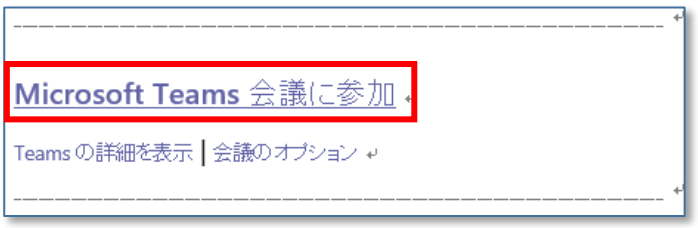
ミーティングは特別なアクセス制御を行わない限り**誰でも参加することが可能**です。
またミーティング参加時の参加者名の入力は参加者側で自由に設定が出来ます。
なりすました不正ユーザー（※3）が参加していないか確認するためにミーティング開始時や途中参加者が入った場合はカメラの映像とマイクを有効化させ映像と音声で本人確認することを推奨します。

※3：なりすました不正ユーザーによる機密情報の取得イメージ

４-２チェックリスト 3-4 に対する利用者向け作業

４-２-１会議 URL の取り扱いについて

不適切な人に会議 URL を送付しないようにします。
尚、会議に対してパスワードの設定は出来ないため会議 URL が漏洩した場合は不正なユーザーが URL にアクセスし簡単に会議室(またはロビー)へ入室が出来てしまいます。



4-3 チェックリスト 3-5 に対する利用者向け作業

4-3-1 不適切な参加者の退室

Teams のロビーには**誰でも入室出来てしまいます。**
そのため主催者は待機室機能を利用し待機している参加者名を確認し予め招待している参加者のみ許可をします。

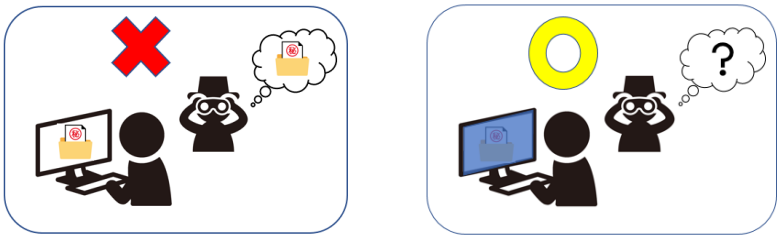
【手順】
ロビーの参加者を許可するにはミーティング画面の下部にある「参加者を表示」をクリックします。
上部がロビー(待機しているユーザー一覧)で下部がミーティング参加者です。
待機室にいる参加者が参加対象であれば「入室を許可する」をクリックします。
対象メンバーでなければ「外す」をクリックすると待機室から強制退場となります。

> ⚠ **注意事項**
> 悪意のあるユーザーは名前をなりすまして参加する可能性があります。
> 可能であればミーティング冒頭で参加者のカメラ機能を有効化して顔や音声で本人確認を実施することを推奨いたします。

4-4 チェックリスト 4-1 に対する利用者向け作業

4-4-1 第三者からの盗聴・覗き見の対策

オフィス外で利用する場合は第三者からの盗聴・盗み見されないように配慮する必要があります。
端末上に投影されている会議資料がのぞき見されないように**のぞき見防止フィルタの利用**や、会議音声が外部に漏れないようにイヤホンを利用するなど利用シーンにおいた対策が必要です。



4-5 チェックリスト 5-2 に対する利用者向け作業

4-5-1 アプリケーションの最新化

利用されるアプリケーションに関しては製品提供元からリリースされる最新バージョンアプリケーションを利用します。アプリケーションの脆弱性をついたサイバー攻撃に対して有効な手段となりますので定期的なアップデート確認をすることを推奨いたします。

Zoom の脆弱性について

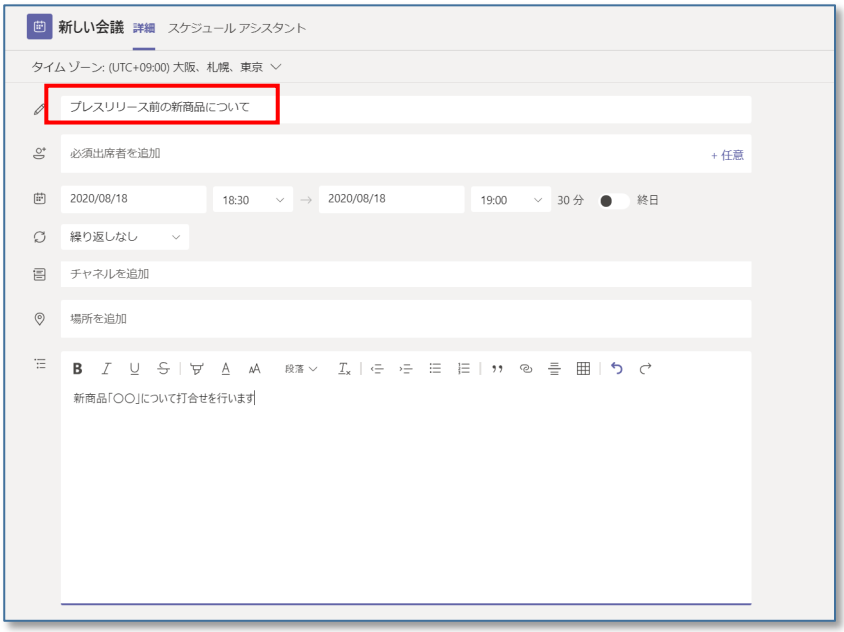
Zoom は過去に脆弱性をついたサイバー攻撃の対象となった事例が報告されました。
既にアプリケーションのバージョンアップ対応にて解消しておりますが古いバージョンのままのユーザーがいない確認することを推奨いたします。

引用：IPA 情報処理推進機構 HP「Zoom の脆弱性対策について」より
URL: https://www.ipa.go.jp/security/ciadr/vul/alert20200403.html

4-6チェックリスト 8-5 に対する利用者向け作業

4-6-1ミーティング情報の件名に機密情報の記載禁止

会議の件名や議題に**機密情報を含まれている場合、間違った相手に招待メールを送信してしまうと情報漏洩してしまいます**。Teams ではミーティングをスケジュールする際に件名と議題を記載する項目がありますが、機密情報を記載しないようにする必要があります。



4-6-2ミーティング録画ファイルの削除

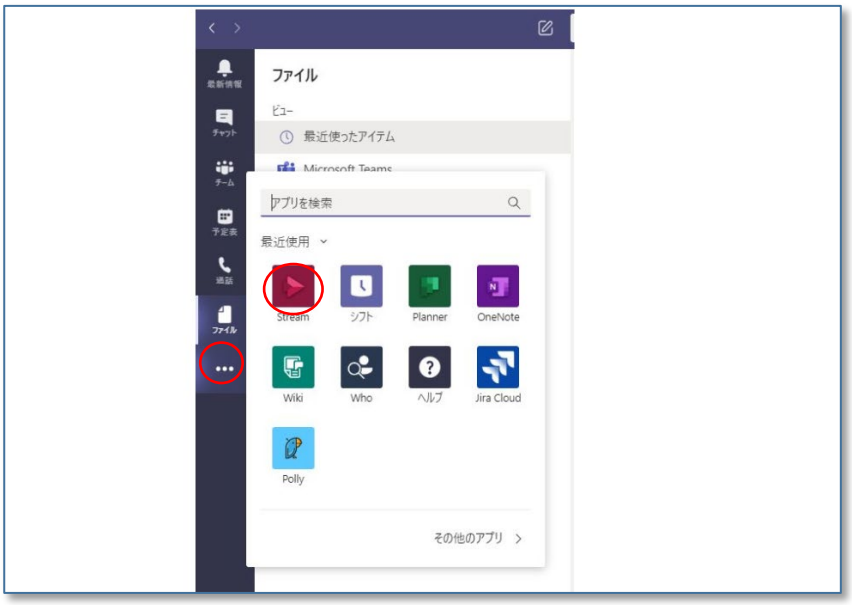
不要になった録画ファイルは適宜削除することを推奨します。

悪意のあるユーザーによる持ち出し、またはサイバー攻撃を受けた際の機密情報漏洩のリスク低減になります。

Teams の会議で録画したビデオは Microsoft Stream に保管されます。

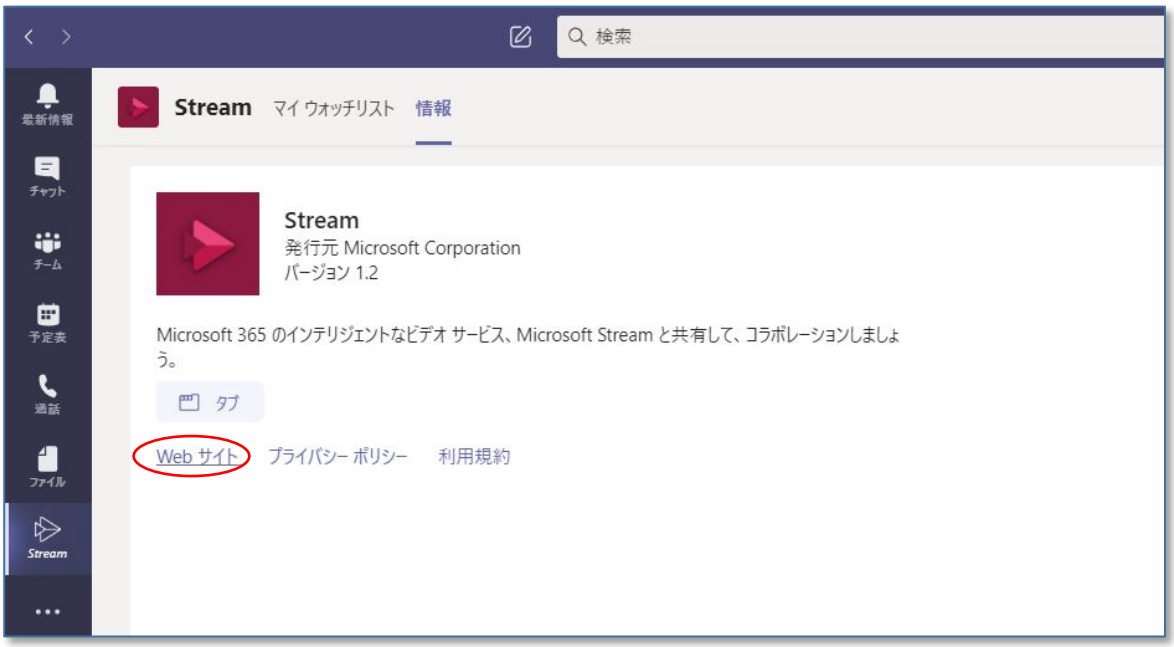
【手順①】

Teams の左ペインにある「その他追加されたアプリ」から stream をクリックします



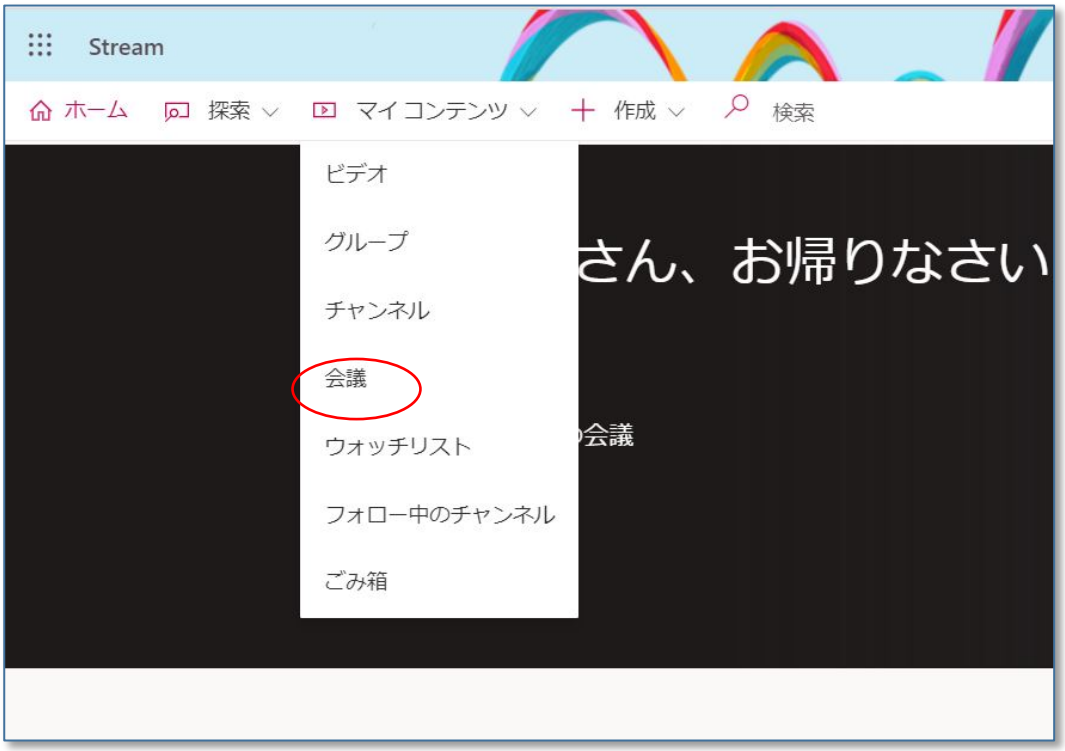
【手順②】

Stream の画面に移行するので「情報」タブからページを切り替え「Web サイト」をクリック



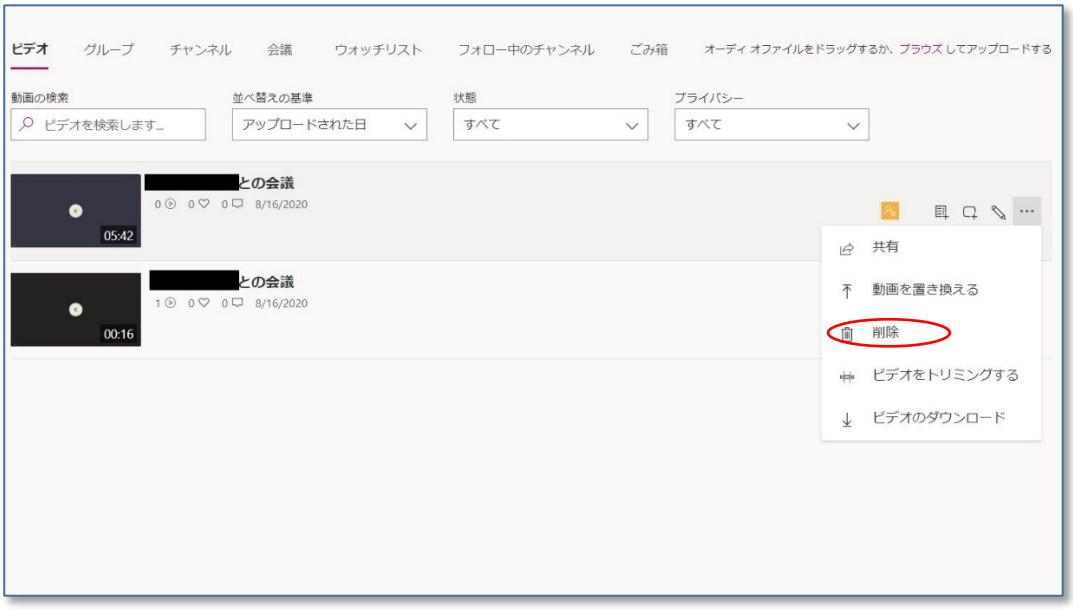
【手順③】

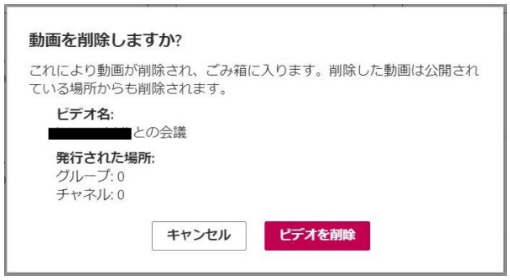
Stream の画面上部「マイコンテンツ」のプルダウンから「会議」を選択。



【手順④】

録画された会議一覧が表示されます。削除対象の録画ファイルを「その他」から削除を選択します。





上記のようにポップアップされますので削除をクリックすると削除されます。