SECIOSS LINK

Office 365 アクセス制御について

【補足資料】

株式会社セシオス

2018年10月

はじめに

- 本資料は弊社クラウドサービス「SeciossLink」を利用して、マイクロソフト社提供のクラウドサービス「Office 365」へのアクセス制限を行う場合の注意事項や参考設定を記載した資料です。
- 「Office365」を利用する場合、Webブラウザのほか、Outlookやスマートデバイス向けアプリケーション、ActiveSync接続など様々なアクセス方法があります。これらのアクセスを意図通りに制御するためには、「Office 365」のアクセス方式の仕組みや「SeciossLink」のアクセス制限の理解が必要です。
- 本資料の内容は「2018年10月」時点で弊社が把握している情報となります。Officeアプリケーションの種類やアクセス方式、「Office 365」の通信仕様については、変更になる可能性もありますので、ご注意ください。

Office365に対するアクセスの種類

- Office 365へアクセスする方式は以下の2つに分けられます。
  - 先進認証方式（Modern Authentication）
  - レガシー認証方式
- クライアントの種類によってアクセス方式が異なります。

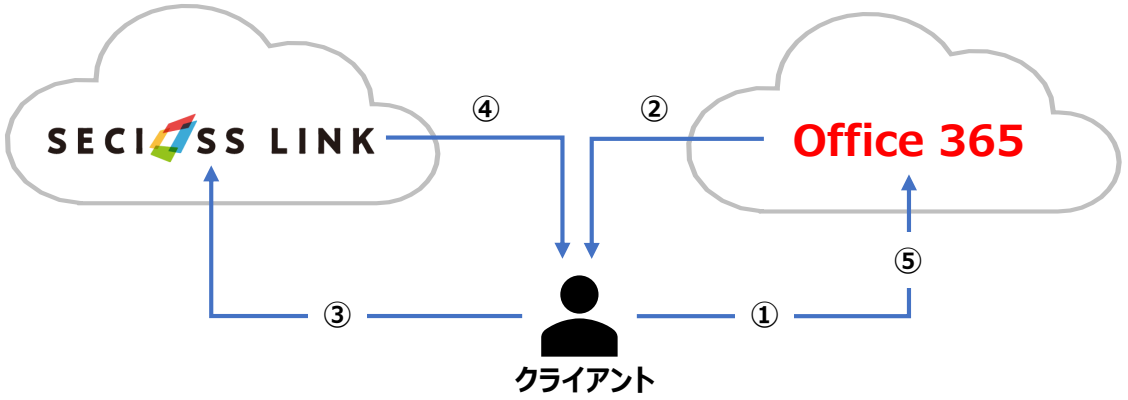
アクセス方式	クライアントの種類	
先進認証方式	IE / Chrome / Firefox / Safari などのブラウザ	
	先進認証に対応した Officeアプリケーション	・Outlook2016 ・Outlook2013　※設定が必要 ・Officeアプリケーション（Word/Excelなど） ・スマートデバイス向けアプリケーション
レガシー認証方式①	POP / IMAP / SMTP Auth を利用するメールクライアント	
	スマートデバイス標準の ActiveSync接続	
レガシー認証方式②	先進認証を利用しない（対応していない）Officeアプリケーション（WS-Trust認証方式）	

ポイント

フェデレーション環境下での「レガシー認証」はOffice 365からId Provider（SeciossLink）に対して直接アクセスが発生します。その際、Office 365は必ず「ID/パスワード」での認証を要求します。
※レガシー認証方式①と②ではアクセスフローが若干異なります。

アクセス概要図①

■先進認証方式



①アクセス（ブラウザ・先進認証方式）

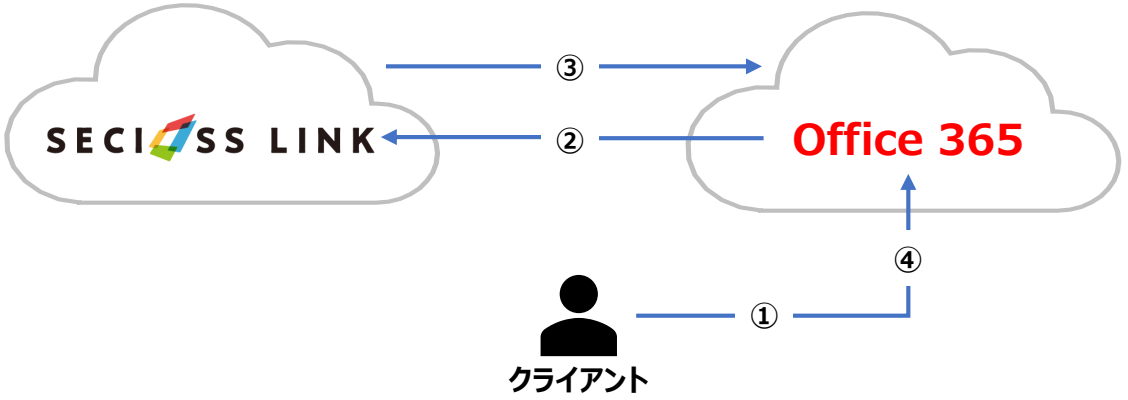
②アクセス元にリダイレクト

③認証サーバにリダイレクト

④認証完了後、アクセス元にリダイレクト

⑤サービス利用開始

■レガシー認証方式①



①アクセス（POP/IMAPなど）

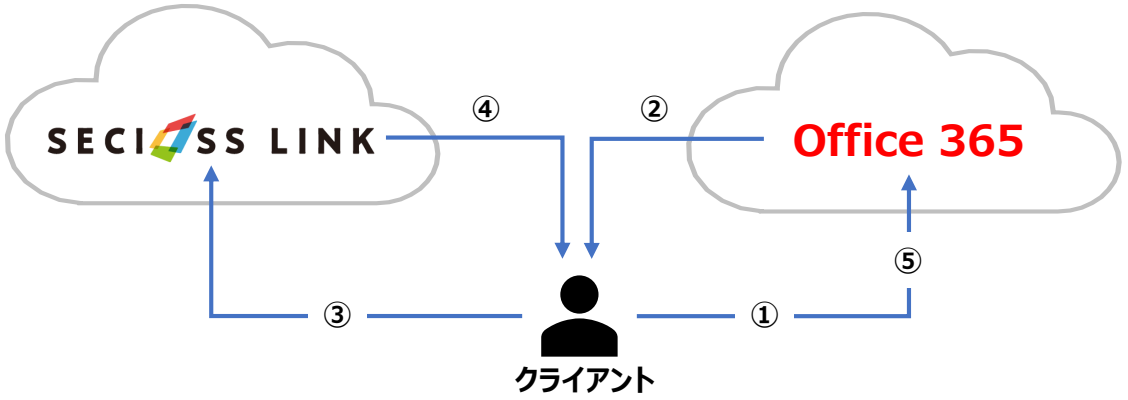
②認証サーバに「ID/Pass」を要求

③認証サーバで認証、結果返却

④認証完了後、サービス利用開始

アクセス概要図②

■レガシー認証方式②



①アクセス（先進認証未対応アプリ）

②認証サーバにアクセスするよう指示

③認証サーバにアクセス

④認証完了後、トークン発行

⑤トークンを利用してアクセス、利用開始

ポイント

先進認証に対応していないアプリケーション（Outlook2010など）は、Office 365にアクセスすると認証サーバに問い合わせるような命令が内部的に行われます。
なお、「レガシー認証①」、「レガシー認証②」はSeciossLinkのアクセス制御設定では違いを意識する必要がないため、以降は合わせて「レガシー認証」と表現します。

SeciossLinkでのアクセス制限

▶SeciossLinkではアクセスユーザ全てに適用される「認証ルール」と認証後に適用される「アクセス権限」機能があります。

機能	説明
認証ルール	全てのユーザに適用されるルールです。認証方式やIPアドレス制限が可能で、必ず1つ作成する必要があります。 ※1つも作成していない場合、全ユーザはアクセスができません。
アクセス権限	「認証ルール」通過後に適用されるルールです。IPアドレス制限やOfficeアプリケーションの種類に応じた制御が可能です。ルールが1つも作成されていない場合、アクセス制限はかかりません。

先進認証のアクセスは「認証ルール」通過後、「アクセス権限」も適用されます。

レガシー認証のアクセスは「認証ルール」を通らず、「アクセス権限」で評価されます。また認証方式は「ID/パスワード」と決まっているため、「アクセス権限」に設定した認証方式も適用されません。適用される条件はアクセスを通過させる「クライアント」の種類、「IPアドレス制限」、「ユーザ・グループ制限」、「許可する時間」です。

※「認証ルール」だけではレガシー認証方式のアクセス制御はできません。

具体的な設定例
Case①

Office 365の利用に際して以下の要件を満たす設定例

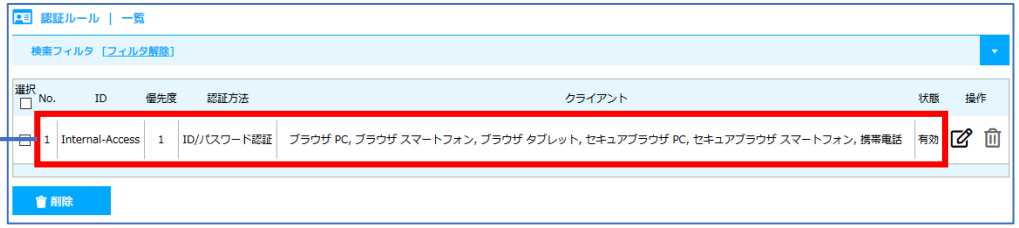
1・社内IPアドレスのみアクセス可能

2・社外からのアクセスは全て拒否

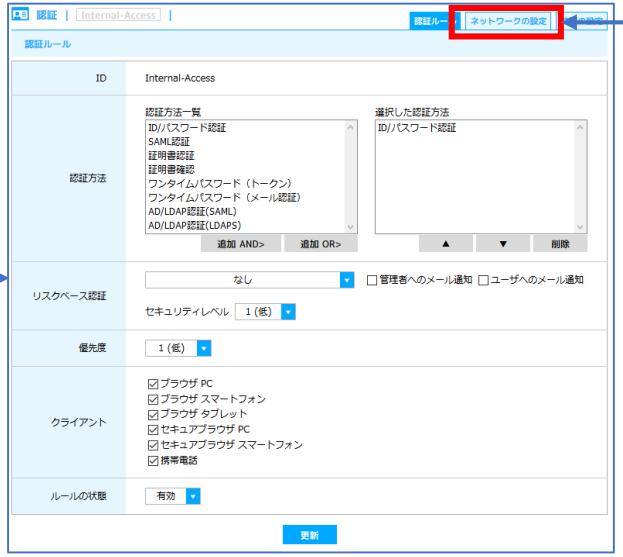
具体的な設定例①-①

▶Office 365のアクセスは、社内IPアドレスのみアクセス可能とする設定例です。「認証ルール」と「アクセス権限」の作成が必要となります。

「認証ルール」の作成



←「Internal」用の認証ルールを作成します。



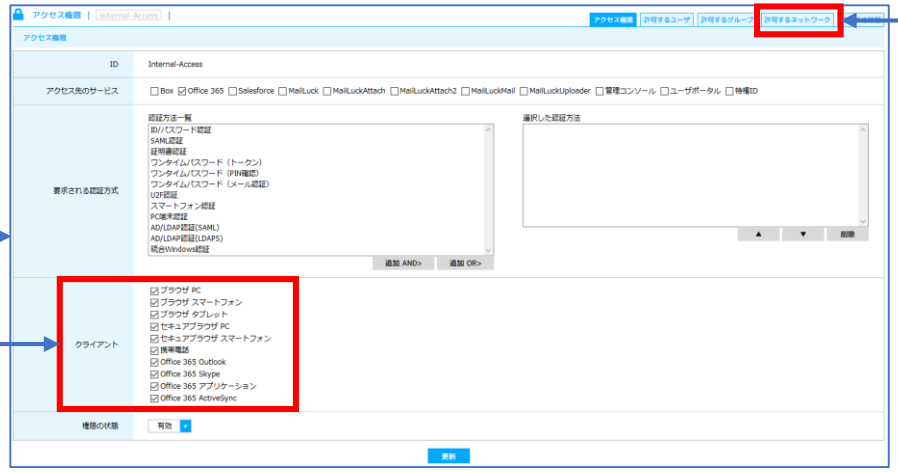
↑「ネットワークの作成」で会社のグローバルIPアドレスを入力します。

←「Internal」用の認証方式は「ID/パスワード」とします。

具体的な設定例①-②

「アクセス権限」の作成

←「アクセス権限」を作成します。



↑「ネットワークの作成」で会社のグローバルIPアドレスを入力します。
※「認証ルール」で設定したIPと同じ値を入力します。

・認証方式の選択は行いません。追加の認証を行う場合には設定を行ってください（先進認証方式のアクセスに対してのみ有効）。
・レガシー認証方式のアクセスに対する認証方式は必ず「ID/パスワード」となります（画面からの設定は不要です）。
・「クライアント」の種類は以下となります。通過させるクライアントにチェックを入れてください。

■先進認証方式のアクセス
・ブラウザ PC
・ブラウザ スマートフォン
・セキュアブラウザPC（弊社セキュアブラウザを利用している場合）
・セキュアブラウザ スマートフォン（弊社セキュアブラウザを利用している場合）

■レガシー認証方式のアクセス
・Office 365 Outlook
・Office 365 Skype
・Office 365 アプリケーション
・Office 365 ActiveSync

具体的な設定例
Case②

Office 365の利用に際して以下の要件を満たす設定例

1・社内IPアドレスからのアクセスは「ID/パスワード」で認証

2・社外からのアクセスは「証明書認証」方式で認証

3・特定のユーザは外部から「POP/IMAP」接続を許可

具体的な設定例②-①

- Office 365の利用に際して、社内IPアドレスからのアクセスは「ID/パスワード」で認証、社外からのアクセスは「クライアント証明書」を確認する「証明書認証」方式で認証します。また、特定のユーザは外部から「POP/IMAP」接続を許可する設定例です。これらを実現するには「認証ルール」と「アクセス権限」の作成が必要です。
- 「認証ルール」を作成し、以下のように設定を行います。

認証ルール	項目	設定例
Internal-Access （社内アクセス用ルール）	認証ルール	ID//パスワード
	ネットワークの設定	181.111.xxx.xxx,182.222.xxx.xxx
	クライアント	全てにチェック
External-Access （社外アクセス用ルール）	認証ルール	証明書認証
	ネットワークの設定	！181.111.xxx.xxx, ！182.222.xxx.xxx（Notの設定）
	クライアント	全てにチェック

具体的な設定例②-②

▶「アクセス権限」を作成し、以下のように設定を行います。

アクセス権限	項目	設定例
Internal-Access （社内アクセス用ルール）	アクセス先のサービス	「Office 365」にチェック
	認証ルール	なし
	ネットワークの設定	181.111.xxx.xxx,182.222.xxx.xxx
	クライアント	全てにチェック
External-Access （社外アクセス用ルール）	アクセス先のサービス	「Office 365」にチェック
	認証ルール	証明書認証
	ネットワークの設定	！181.111.xxx.xxx, ！182.222.xxx.xxx（Notの設定）
	クライアント	「ブラウザ PC」、「ブラウザ スマートフォン」にチェック 弊社提供ブラウザを利用している場合は“セキュアブラウザ”にチェック

ポイント

社外アクセス用ルールの「クライアント」設定で“Office 365系”の項目のチェックを**外す**ことで、外部からのレガシー認証方式のアクセス（POP/IMAPやOutlook2010など）を遮断しています。

具体的な設定例②-③

▶特定のユーザに対して、外部から「POP/IMAP」接続を許可する設定を「アクセス権限」を追加します。

アクセス権限	項目	設定例
External-Access-02 （特別ルールの追加）	アクセス先のサービス	「Office 365」にチェック
	認証ルール	なし
	ネットワークの設定	！181.111.xxx.xxx, ！182.222.xxx.xxx（Notの設定）
	クライアント	「Office 365 Outlook」にのみチェック
	許可するユーザ	「POP/IMAP」接続を許可するユーザを設定

補足事項

- アクセス制御を行う場合、連携しているサービス側のアクセス方式を理解する必要があります。特にOffice 365は、提供されているアプリケーションの種類が多く、バージョンによっても動作が異なる（先進認証への対応可否など）ため、十分なテストを実施してください。
  - テストを実施すべき主なクライアント
    主要ブラウザ/Outlook2016,2013/POP/IMAP/スマートフォン向けアプリケーション/ActiveSync
- Office 365の管理者コンソールでもアクセスを遮断する設定があります。
  - POP/IMAP,ActiveSync,レガシー認証の利用可否が設定できます。
    ※詳しくはマイクロソフト社へお問い合わせください。

- iOSでクライアント証明書を利用する場合、マイクロソフト社提供のアプリケーション「MS Authenticator」の導入が必要になります。iOSにインストールされた証明書領域に対して、ビルトイン以外のアプリケーションは通常、アクセスできないためです。※「MS Authenticator 」はアクセス可能です。

SECIOSS LINK

https://seciosslink.com

株式会社セシオス

https://www.secioss.co.jp