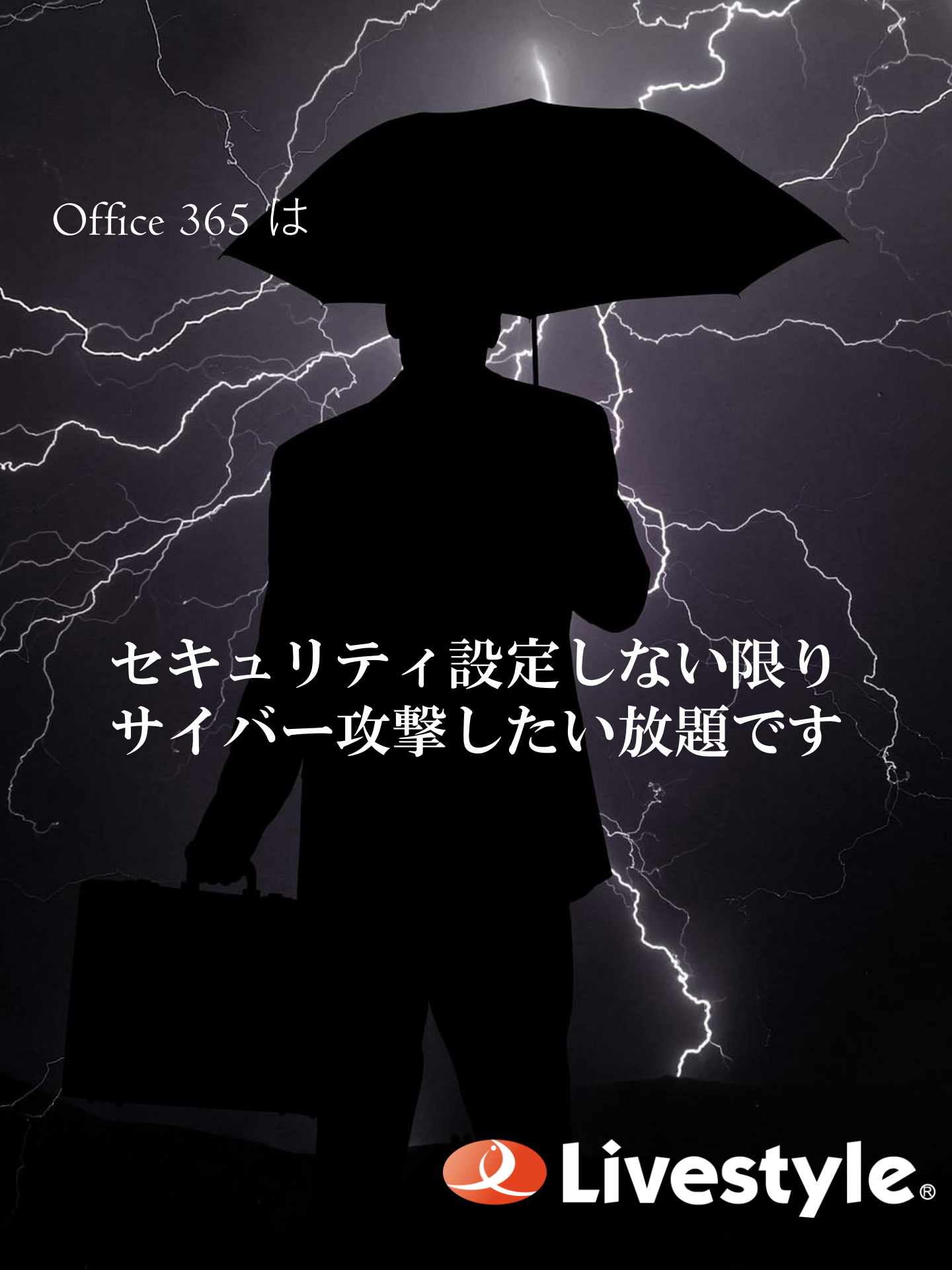
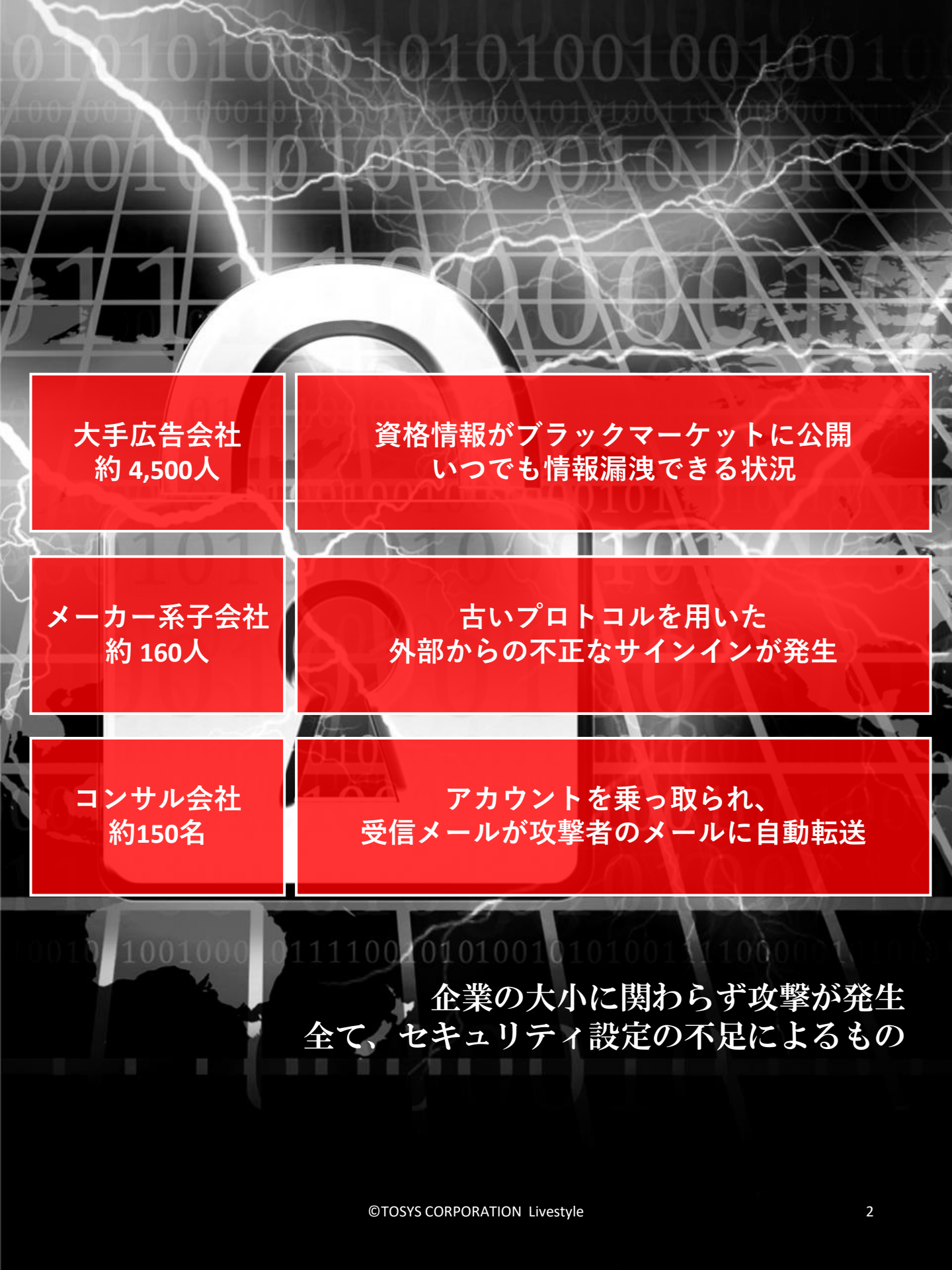

Office 365 は
セキュリティ設定しない限り
サイバー攻撃したい放題です
Livestyle®



大手広告会社 約 4,500人	資格情報がブラックマーケットに公開 いつでも情報漏洩できる状況
メーカー系子会社 約 160人	古いプロトコルを用いた 外部からの不正なサインインが発生
コンサル会社 約150名	アカウントを乗っ取られ、 受信メールが攻撃者のメールに自動転送

企業の大小に関わらず攻撃が発生
全て、セキュリティ設定の不足によるもの


貴社のクラウドセキュリティは大丈夫ですか
Microsoft 365
簡易版セキュリティチェックシート

目次

ライセンス別確認項目

EMS E3 相当のライセンスご契約のお客様

EMS E5 相当のライセンスご契約のお客様

Office 365にアクセスするときに、会社のPCやIPアドレス以外の場合の制御はできていますか？

簡易確認方法
- 私用のPC(スマホ)/私用のWi-Fiを用意します。
- ブラウザからOffice 365にアクセスし、普段利用する資格情報でサインインをします。
- ポップアップが表示され、多要素認証の要求やサインインできない事を確認します。

簡易確認方法(管理者向け)
- 管理者にてAzure ポータルにサインインします。
- [Azure Active Directory]-[セキュリティ]-[条件付きアクセス]をクリックします。
- ポリシー内にアクセス制御をしていて、状態が「オン」のポリシーが存在するか確認します。

制御していない場合
社外から不正なアクセスが自由にできる可能性大です

レガシー認証と呼ばれる、古いプロトコルからのアクセスを完全にブロックしていますか？

簡易確認方法

・iPhoneを用意し、以下URLの手順に従って、メール設定をします。
https://support.apple.com/ja-jp/HT201729
※手順3では「手動構成」を選択し、Server欄には「outlook.office365.com」を入力ください。

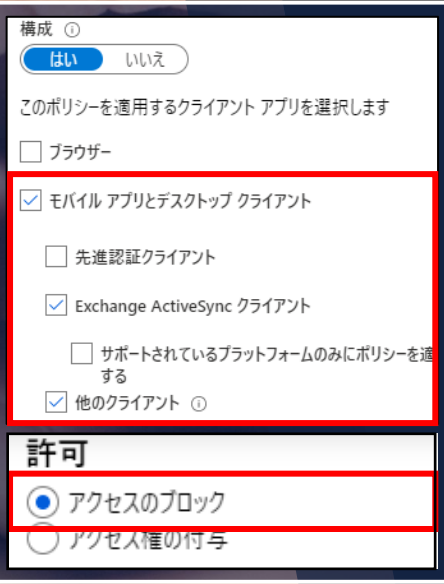
・メールアプリを開いた際に、受信できない、できたとしても管理者で制御されている旨のメールが送信される事を確認します。

簡易確認方法(管理者向け)

・管理者にてAzure ポータルにサインインします。

・[Azure Active Directory]-[セキュリティ]-[条件付きアクセス]をクリックします。

・以下URLと同等設定であるポリシーを確認します。
https://support.live-style.jp/?p=5186



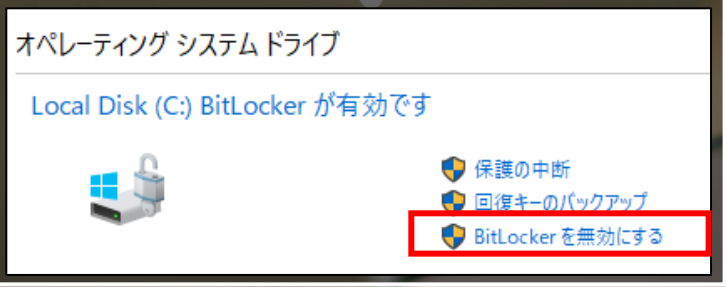
制御していない場合

古いプロトコルから不正アクセスできる可能性大です

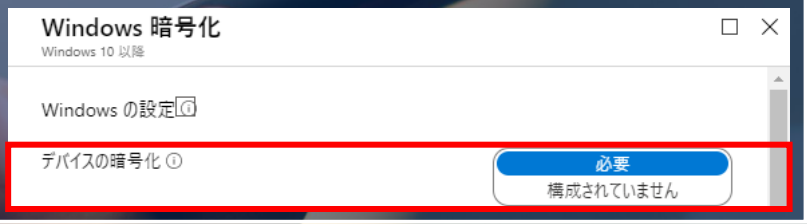
※サイバー攻撃に利用されるケースが非常に高い方法です。

ウイルススキャンやBitLockerを
自由に無効化できないようにしていますか？

簡易確認方法
- 会社のPCでコントロールパネルを開き、「Bitlockerドライブの暗号化」をクリックします。
- Bitlockerを無効にします。
- 一定期間（最大1日）経過後に有効を促すポップアップが表示されるか確認します。



簡易確認方法(管理者向け)
- 管理者にてAzure ポータルにサインインします。
- [Intune]-[デバイス構成]-[プロファイル] をクリックします。
- プロファイルの種類が[Endpoint Protection]であるポリシーを選択します
- ポリシー内の[Windows 暗号化]-[デバイスの暗号化]が「必須」となっていることを確認します。

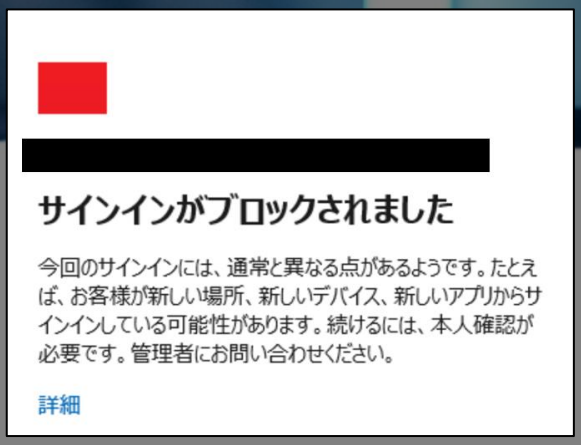


制御していない場合
ユーザー依存で、脆弱性や紛失時のリスクが発生します

サインインリスクを検知した時に、自動的にアクセスブロックや多要素認証要求されますか？

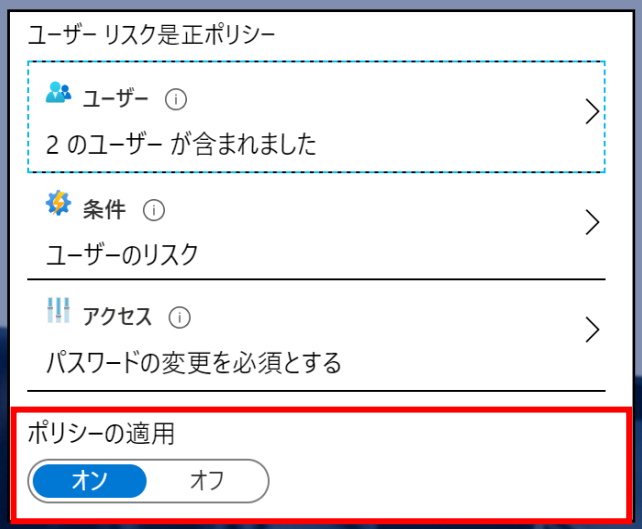
簡易確認方法

- 私用のPC(スマホ)/私用のWi-Fiを用意します。
- ブラウザからOffice 365にアクセスし、普段利用する資格情報でサインインをします。
- ポップアップが表示され、多要素認証の要求やサインインできない事を確認します。



簡易確認方法(管理者向け)

- 管理者にてAzure ポータルにサインインします。
- [Azure Active Directory]-[セキュリティ]-[Identity Protection]をクリックします。
- ユーザーリスクポリシーとサインインリスクポリシーをクリックし、ポリシーがONである事を確認します。



制御していない場合

不正アクセスの制御ができていない可能性があります

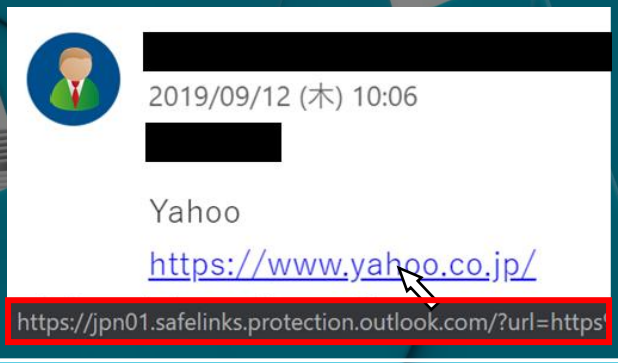
フィッシングメールに対して
自動でリスク有無の調査をしていますか？

簡易確認方法

・自身の受信メールに送付された本文にURLがある任意のメールを開きます。

・URLをマウスオーバーし、「https://jpn01.safelinks....」から始まるURLが表示される事を確認します。

※メールがテキスト形式の場合はマウスオーバー不要です



簡易確認方法(管理者向け)

・Office 365 セキュリティ/コンプライアンスセンターにアクセスします。

・[脅威の管理]-[ポリシー]-[ATPの安全なリンク]をクリックします。

・「Default」以外のポリシーがある事を確認します。

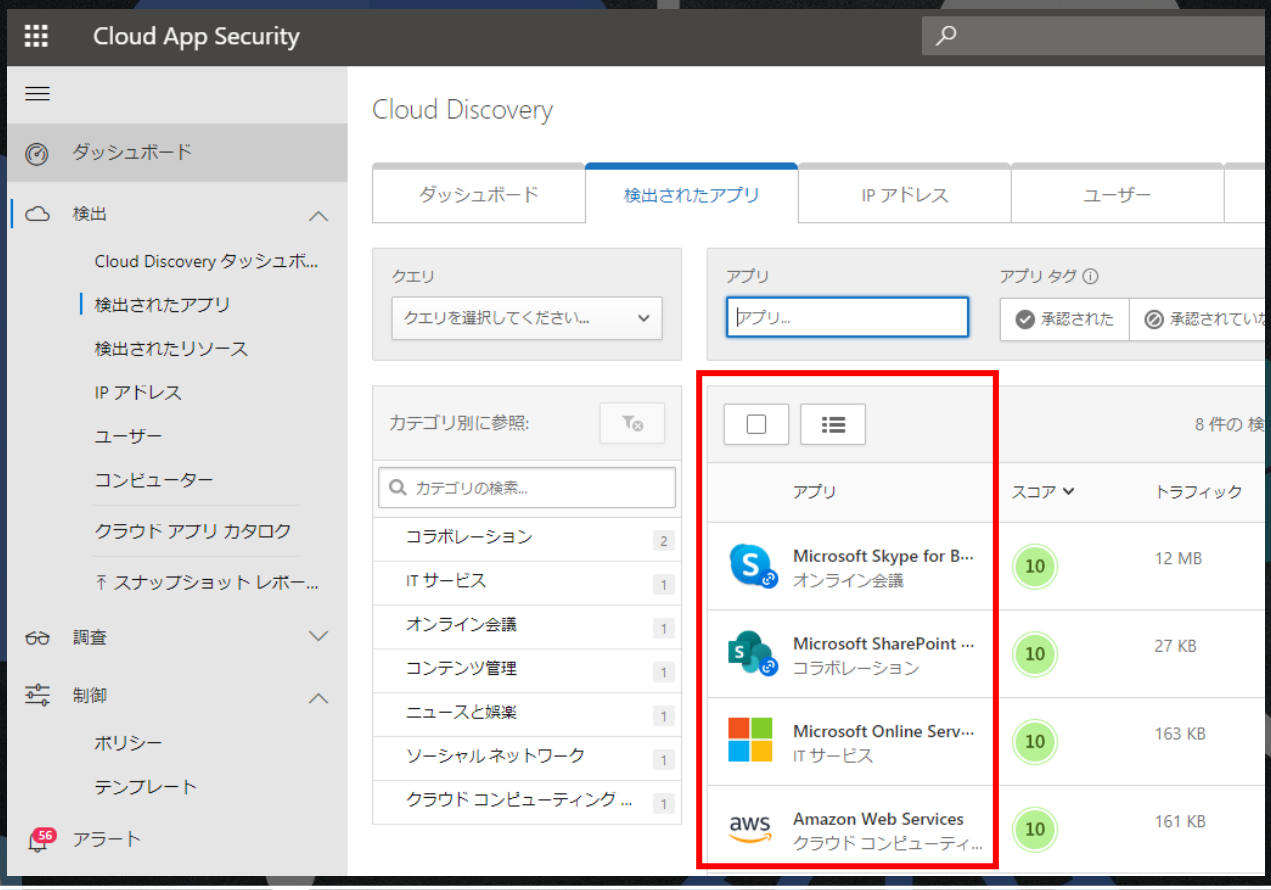
制御していない場合

フィッシングメールにより資格情報漏洩の可能性有です

会社が認めていないSaaSを監視できていますか？

簡易確認方法(管理者向け)

・管理者にてMCAS ポータルにサインインします。
(https://portal.cloudappsecurity.com)
・[検出]-[検出されたアプリ]をクリックします。
・利用しているSaaSの一覧が表示される事を確認します。



制御していない場合
許可していないSaaSからデータが漏洩する可能性有

目次に記載の重要度

A　1つ以上　　B　2つ以上で

資格情報、データ漏洩の可能性が極めて高い状況です

対策に以下をご検討ください

◆更に詳しくセキュリティ健康診断を行う

弊社はじめ、一部の企業で実施している
「**脅威対策可視化アセスメント**」の実施を
ご検討ください

◆早速セキュリティ設定を行う

ご契約されているベンダーに構築をご依頼下さい。
ご契約ベンダーで難しい場合は、まずは弊社に
ご相談いただければ幸いです。

Livestyle®

ここちよいクラウドサービスを。

お客様の成長を支えるIT基盤 ベストな環境をご提供

TOSYS

株式会社TOSYS

クラウドサービス部 Livestyleサービス窓口

TEL： 0120-742-500

E-mail： sales@team.live-style.jp

URL： https://www.live-style.jp