

標的型攻撃メール訓練 ホワイトリスト設定項目

※協会の訓練向けに加筆およびマスキングをしております。

2024年9月

ホワイトリスト設定項目 (1/2)

社外秘

[Redacted]

[Redacted]

[Redacted]	
------------	--

[Redacted]

[Redacted]

[Redacted]

社外秘

ホワイトリスト設定項目（2/2）

社外秘

3. 訓練メール、教育コンテンツ、アンケート通知メール

本番用の訓練メール、教育コンテンツ受講依頼とアンケート回答依頼のメールは以下の内容で送付されます。必要な項目をホワイトリストへご登録ください。

差出人メールアドレス	訓練メール	“ローカルパート”@infomaton.com（IPアドレス：40.115.243.190） “ローカルパート”はユーザ協会で設定
	教育コンテンツ受講依頼	info@infomaton.com（IPアドレス：40.115.243.190）
件名	訓練メール	協会にて設定
	教育コンテンツ受講依頼	標的型攻撃メール訓練サービス(eラーニング受講依頼)
開封ログ収集用URL		https://toresavi.com/beacon?token=<半角英数の識別子> （IPアドレス：20.43.89.245）
URL	教育コンテンツ	https://toresavi.com/（IPアドレス：20.43.89.245）

社外秘

注意事項：環境確認のお願い

本番の訓練が正常に実行できないケースがあります。下記のケースと本サービスの仕様を参考にお申込前に必ずメール受信/閲覧環境をご確認ください。

発生事象	推測される原因	本サービスの仕様
訓練メールが届かない	■時間当たりのメール送受信数上限を超えブロック 同時刻に訓練メールを大量に送ったところ、お客様側のメールサーバに設定されているメール送受信上限数を超え、受信ができなかった。	<ul style="list-style-type: none">・1回の訓練（1時間枠）は最大600通の送信が可能で、約6秒間隔で送信します。・送信元ドメイン [redacted] “ローカルパート”@infomaton.com ※“ローカルパート”部分はユーザ協会で設定します。・開封者のメーラー設定は本サービスから変更できません。
	■セキュリティ機器によるブロック 訓練メールの送信元ドメインをファイアウォールやUTM等が不審と判断し、ブロックされた。	
	■メーラーによる迷惑メール判定 メールの受信はできたが、メーラーが迷惑メールと判定し、受信に気づかなかった。	
身に覚えのない開封が記録されている	■システムが開封している サンドボックス等が添付ファイルの開封やURLのクリックを実行した。	<ul style="list-style-type: none">・開封操作については人手とそれ以外を判別しません。システムによる開封操作も記録されます。・開封は3回まで記録が可能です [redacted]
開封しているが記録がない	■開封を記録する通信がブロック お客様のセキュリティ機器が開封を記録する通信（開封ログ収集用URLへのアクセス）をブロックし、開封しても記録されない。	<ul style="list-style-type: none">・ファイルの開封時にインターネット通信を行うことで開封とみなします。ファイル開封時にセキュリティ機器やOffice、Adobeの機能でインターネット通信がブロックされた場合は開封とはみなしません。

【参考】Microsoft365をご利用の場合

Microsoft365では、以下2つの手順でホワイトリストの登録ができます。

登録するIPアドレスは、「**40.115.243.190**」になります。

手順1・2の設定が反映されるまで最大24時間かかります。

※以下の手順は、Microsoft365 バージョン2408 ビルド16.0.17928.20114（2024年9月時点）の参考情報です。詳細はマイクロソフトまでお問い合わせください。

■手順1 コネクタの設定（1/5）

Exchange管理センターにて①②③の順に選択

Exchange 管理センター

Home > コネクタ

コネクタ

Connectors help control the flow of email messages to and from your Office 365 organization. We recommend that you [check to see if you should create a connector](#), since most organizations don't need to use them.

③ + コネクタを追加 [最新の情報に更新](#)

状態	名前	差出人	終了
データがありません			

① 連絡先

② コネクタ

【参考】Microsoft365をご利用の場合

社外秘

■手順1 コネクタの設定（2 / 5）

①②③④の順に設定を実施

コネクタを追加

新しいコネクタ

名前

送信メールを認証する

コネクタを確認する

新しいコネクタ

メール フローのシナリオを指定してください。コネクタを設定する必要があるかどうかをお知らせします。

接続元

Office 365

① 組織のメール サーバー

パートナー組織

接続先

Office 365

② 次

コネクタを追加

新しいコネクタ

名前

送信メールを認証する

コネクタを確認する

コネクタ名

このコネクタを使用すると、Office 365 があなたの組織のメール サーバーからメッセージを配信できるようになります。

名前 *

③ 標的型攻撃メール訓練サービス

説明

コネクタの保存後に、何を行いますか？

オンにする

内部 Exchange メール ヘッダーを保持する (推奨)

戻る 次 ④

任意の名前を設定

社外秘

【参考】Microsoft365をご利用の場合

社外秘

■手順1 コネクタの設定 (3 / 5)

①②③④の順に設定を実施

コネクタを追加

- ✓ 新しいコネクタ
- ✓ 名前
- **送信メールを認証する**
- コネクタを確認する

送信メールを認証する

メール サーバーからのメールを Office 365 が識別する方法を選んでください。

あなたのメール サーバーから送信されたメールを Office 365 がどのように認証して受け入れるかを選択します。

送信側サーバーが Office 365 での認証に使用する証明書のサブジェクト名が、下のテキストボックスに入力されたドメインと一致することを確認する (推奨)

例: contoso.com または *.contoso.com

① 送信側サーバーの IP アドレスが、あなたの組織にのみ属している次の IP アドレスのいずれかと一致することを確認する

② 「40.115.243.190」を登録 **+** **③**

戻る **次** **④**

社外秘

【参考】Microsoft365をご利用の場合

社外秘

■手順1 コネクタの設定（4 / 5）

①②の順に選択

コネクタを追加

- 新しいコネクタ
- 名前
- 送信メールを認証する
- コネクタを確認する

コネクタを確認する

メール フローのシナリオ

接続元: あなたの組織のメール サーバー
接続先: Office 365

名前

標的型攻撃メール訓練サービス

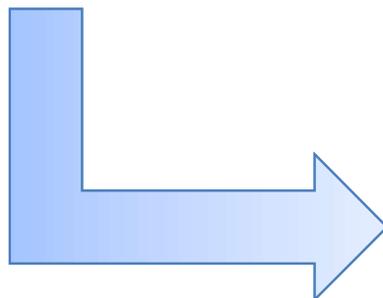
状態

保存後にオンにする
内部 Exchange メール ヘッダーを保持する (推奨)
[名前を編集](#)

あなたのメール サーバーから送信されたメールを特定する方法

あなたのメール サーバーからの着信メッセージを特定するには、送信側サーバーの IP アドレスが IP アドレス範囲 40.115.243.190 中にあること、送信者のメール アドレスが組織の承認済みドメインの中にあることを確認します。

[戻る](#) [コネクタを作成](#) ①



コネクタを追加

- 新しいコネクタ
- 名前
- 送信メールを認証する
- コネクタを確認する

コネクタが作成されました
[別のコネクタを追加](#)

[完了](#) ②

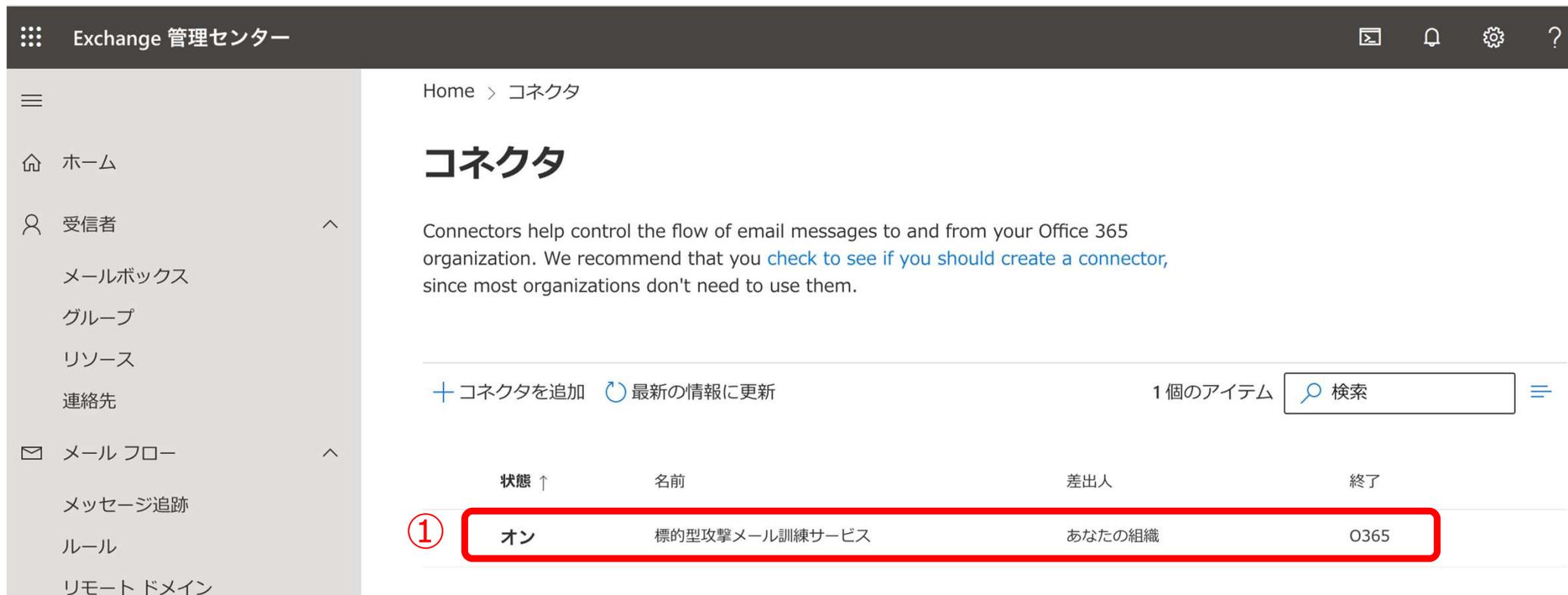
社外秘

【参考】Microsoft365をご利用の場合

社外秘

■手順1 コネクタの設定 (5/5)

①各種ステータスを確認 ※名前は任意の値



Exchange 管理センター

Home > コネクタ

コネクタ

Connectors help control the flow of email messages to and from your Office 365 organization. We recommend that you [check to see if you should create a connector](#), since most organizations don't need to use them.

+ コネクタを追加 最新の情報に更新 1個のアイテム 検索

状態 ↑	名前	差出人	終了
① オン	標的型攻撃メール訓練サービス	あなたの組織	0365

手順2へ

社外秘

【参考】Microsoft365をご利用の場合

社外秘

■手順2 ルールの設定 (2/6)

①②③④⑤⑥⑦⑧の順に設定を実施

トランスポート ルールの名前と設定された条件

任意の名前を設定

① 名前 *
標的型攻撃メール訓練サービス 1つ選択 ③

② このルールを適用する *
送信者

送信者
受信者
件名または本文
いずれかの添付ファイル
すべての受信者
メッセージ...
送信者と受信者
メッセージのプロパティ
メッセージ ヘッダー...
すべてのメッセージに適用

次へ

トランスポート ルールの名前と設定された条件

名前 *
標的型攻撃メール訓練サービス

この人物である
外部/内部である ④ 1つ選択 +

このグループのメンバーである

アドレスに次のいずれかの単語が含まれる

アドレスが次のいずれかのテキスト パターンと一致する

受信者の監督の一覧に含まれる 1つ選択 +

特定のプロパティが次の単語のいずれかを含む

特定のプロパティが次のテキスト パターンと一致する 1つ選択 +

⑤ IP アドレスが次の範囲内にあるか、完全に一致する
ドメインは

トランスポート ルールの名前と設定された条件

⑥

IP アドレス範囲の指定 ⑦

IPv4 または IPv6 のアドレス、または範囲を入力します

追加

1つのアイテム

40.115.243.190

次へ ⑧ 保存 キャンセル

「40.115.243.190」を登録

【参考】Microsoft365をご利用の場合

社外秘

■手順2 ルールの設定 (3/6)

①②③④⑤⑥の順に設定を実施

トランスポート ルールの名前と設定された条件

名前 *

標的型攻撃メール訓練サービス

このルールを適用する *

送信者 1つ選択

送信者の IP アドレスが次の範囲内である '40.115.2'

メッセージを転送して承認を受ける

メッセージのリダイレクト先

メッセージをブロックする

① メッセージのプロパティの変更

受信者を追加

メッセージに免責事項を適用する

② メッセージのプロパティの変更

メッセージのセキュリティを変更する

メッセージの件名の先頭に追加する

インシデント レポートの生成と送信先

受信者にメッセージを通知する

次へ

トランスポート ルールの名前と設定された条件

名前 *

標的型攻撃メール訓練サービス

このルールを適用する *

送信者 IP アドレスが次の範囲内にあるか、完全に...

送信者の IP アドレスが次の範囲内である '40.115.243.190'

次を実行します *

メッセージのプロパティの変更 ③ 1つ選択

メッセージヘッダーの削除

メッセージヘッダーの設定

メッセージ分類の適用

④ SCL (スパム信頼度レベル) の設定

次へ

トランスポート ルールの名前と設定された条件

名前 *

標的型攻撃メール訓練サービス ⑤

SCL の指定

Bypass spam filtering

このルールを適用する *

送信者

送信者の IP アドレスが次の範囲内である '40.1

次を実行します *

メッセージのプロパティの変更

SCL (Spam Confidence Level) を次の値に設

次の場合を除く

1つ選択

⑥ 保存 キャンセル

社外秘

【参考】Microsoft365をご利用の場合

社外秘

■手順2 ルールの設定 (4/6)

①②の順に設定を実施 ※「セットルールの設定」は変更なし

セットルールの条件

トランスポート ルールの名前と設定された条件

名前 *

標的型攻撃メール訓練サービス

このルールを適用する *

送信者 送信者の IP アドレスが次の範囲内にあるか、完全に...

送信者の IP アドレスが次の範囲内である '40.115.243.190'

次を実行します *

メッセージのプロパティの変更 SCL (スパム信頼度レベル) の設定

SCL (Spam Confidence Level) を次の値に設定する '-1'

① 次の場合を...

次へ

セットルールの設定

トランスポート ルールの設定のセットです

ルール モード

適用

ポリシー ヒントありのテスト

ポリシー ヒントなしのテスト

重要度 *

指定なし

このルールをアクティブ化する日にち

9/13/2024 - 9:30 AM

②

このルール...

戻る 次へ

社外秘

【参考】Microsoft365をご利用の場合

社外秘

■手順2 ルールの設定 (5/6)

①各種ステータスを確認し、②を選択

新規のトランスポート ルール	
	ルールに関するコメント
	①
<p>ルールの条件</p> <p>このルールを適用する 送信者の IP アドレスが次の範囲内である '40.115.243.190'</p> <p>次を実行します SCL (Spam Confidence Level) を次の値に設定する '-1'</p> <p>次の場合を除く</p> <p>ルール条件の編集</p>	<p>ルールの設定</p> <p>モード Enforce</p> <p>期間の設定 特定の日付範囲が設定されていません</p> <p>優先度 0</p> <p>重要度 指定なし</p> <p>ルール処理エラーの場合 Ignore</p> <p>以降のルールは処理しない false</p> <p>ルール設定の編集</p>
	②
	<p>戻る</p> <p>完了</p>

社外秘

【参考】Microsoft365をご利用の場合

社外秘

■手順2 ルールの設定（6 / 6）

①ルール名を押下し、②無効を有効にする

Exchange 管理センター

ホーム > ルール

① メールフロー、ルールの DLP ポリシーと DLP 関連の条件とアクションはサポートを使用したりすることはできなくなりました。DLP 関連のすべてのルールを、で移行したら、EAC または PowerShell でここで削除してください。詳細情報

ルール

トランスポート ルールを追加、編集、またはその他の変更を行います。

②

ルールを有効または無効にする

無効

ルールの設定

ルール名	モード
標的型攻撃メール訓練サービス	Enforce
重要度	期間の設定
指定なし	特定の日付範囲が設定されていません
送信者のアドレス	優先度
Matching Header	0
ルール処理エラーの場合	
Ignore	

状態	ルール	優先度
Disabled	標的型攻撃メール訓...	0

Exchange 管理センター

ホーム > ルール

① メールフロー、ルールの DLP ポリシーと DLP 関連の条件とアクションはサポートを使用したりすることはできなくなりました。DLP 関連のすべてのルールを、で移行したら、EAC または PowerShell でここで削除してください。詳細情報

ルール

トランスポート ルールを追加、編集、またはその他の変更を行います。

ルールを有効または無効にする

有効

ルールの設定

ルール名	モード
標的型攻撃メール訓練サービス	Enforce
重要度	期間の設定
指定なし	特定の日付範囲が設定されていません
送信者のアドレス	優先度
Matching Header	0
ルール処理エラーの場合	
Ignore	

状態	ルール	優先度
Enabled	標的型攻撃メール訓...	0

Enabledになっていることを確認

社外秘