



Mail セキュリティ・クラウド プレミアム スタートアップガイド

* Microsoft、Microsoft 365、Exchange は米国 Microsoft Corporation の、米国、日本およびその他の国における登録商標または商標です。

* 記載されている会社名及び商品名は、それぞれ各社の登録商標または商標です。本データ内の文章・画像・図版の著作権についてはそれぞれの著者に帰属します。

© Canon Marketing Japan Inc. 2025

本ドキュメントの一部あるいは全部について、キヤノンマーケティングジャパン株式会社の事前の承認なく、複製、転載することを禁止します。

2025-Mar.-12

目次

1. はじめに	2
1.1 ご利用までの流れ	2
2. お客様環境の変更	5
2.1 DNS サーバーの設定変更	5
2.2 メールサーバーの設定変更	7
2.2.1 Microsoft 365 のみ利用している場合（すべてのユーザーで利用）	8
2.2.2 Microsoft 365 のみ利用している場合（一部のユーザーで利用）	28
2.2.3 Google Workspace のみ利用している場合（すべてのユーザーで利用）	47
2.2.4 Google Workspace のみ利用している場合（一部のユーザーで利用）	62
3. Mail セキュリティ・クラウドへの初回ログインおよびメール疎通確認	79
3.1 初回ログイン・パスワード変更手順	79
3.2 メール疎通確認	81
4. ジャーナルアーカイブ設定	84
4.1 Microsoft 365 の設定変更	84
4.1.1 配信できないジャーナルレポートの送信先の設定	85
4.1.2 ジャーナルルールの設定	90
4.2 Mail セキュリティ・クラウドの設定変更	94
4.2.1 MailArchive on Cloud [ジャーナルメール] + MailFilter on Cloud をご利用の場合	94
4.2.2 MailArchive on Cloud [ジャーナルメール] + MailConvert on Cloud のみをご利用の場合	98
4.2.3 MailArchive on Cloud [ジャーナルメール] のみをご利用の場合	102
4.3 テストメールの送信・確認	105
5. 初期設定完了	110

1. はじめに

この度は、Mailセキュリティ・クラウドをご購入くださり、誠にありがとうございます。
本資料は、Mailセキュリティ・クラウドの運用を開始いただくまでの手順をご紹介します。

1.1 ご利用までの流れ

Mailセキュリティ・クラウドの運用開始までの全体的な流れは次頁のとおりです。

ご利用になるサービスによって、運用開始までの流れが異なりますので、ご利用になるサービスを確認し、該当する流れに沿って設定を実施ください。

ご利用パターン

ご利用サービス

- ・ MailFilter on Cloud [送信メール]
- ・ MailFilter on Cloud [受信メール]
- ・ MailConvert on Cloud
- ・ MailArchive on Cloud [送信メール]
- ・ MailArchive on Cloud [受信メール]
- ・ MailArchive on Cloud [ジャーナルメール]



[パターン A の場合]をご確認ください。

※MailArchive on Cloud [ジャーナルメール] のみ
ご利用の場合は、[パターン B の場合]を
ご確認ください。

ご利用サービス

- ・ MailFilter on Cloud [送信メール]
- ・ MailFilter on Cloud [受信メール]
- ・ MailConvert on Cloud
- ・ MailArchive on Cloud [送信メール]
- ・ MailArchive on Cloud [受信メール]
- ・ MailArchive on Cloud [ジャーナルメール]



[パターン B の場合]をご確認ください。

パターン A の場合

本資料は青枠部分の手順について記載しております。

	関連資料	該当の章・項目
サービス登録完了書の受け取り	サービス登録完了書	-
お客様環境の変更	スタートアップガイド (本資料)	2. お客様環境の変更
	サービス登録完了書	【サービス設定情報】
Mail セキュリティ・クラウドへの 初回ログイン・メール疎通確認	スタートアップガイド (本資料)	3. Mail セキュリティ・クラウドへの 初回ログインおよびメール疎通確認
	サービス登録完了書	【GUARDIANWALL 管理画面】
ジャーナルアーカイブ設定 MailArchive on Cloud [ジャーナルメール]を ご利用の場合のみ	スタートアップガイド (本資料)	4. ジャーナルアーカイブ設定
	サービス登録完了書	【サービス設定情報】 【GUARDIANWALL 管理画面】
初期設定完了	スタートアップガイド (本資料)	5. 初期設定完了
利用開始	ユーザー運用ガイド	-

パターン B の場合

本資料は**青枠部分**の手順について記載しております。

	関連資料	該当の章・項目
サービス登録完了書の受け取り	サービス登録完了書	-
↓		
Mail セキュリティ・クラウドへの 初回ログイン	スタートアップガイド (本資料)	3.1 初回ログイン・ パスワード変更手順
	サービス登録完了書	【GUARDIANWALL 管理画面】
↓		
ジャーナルアーカイブ設定	スタートアップガイド (本資料)	4. ジャーナルアーカイブ設定
	サービス登録完了書	【サービス設定情報】 【GUARDIANWALL 管理画面】
↓		
初期設定終了	スタートアップガイド (本資料)	5. 初期設定完了
↓		
利用開始	ユーザー運用ガイド	-

2. お客様環境の変更

Mailセキュリティ・クラウドをご利用いただくにあたり、お客様環境の設定変更を実施ください。

本章では、DNSサーバーの設定変更とメールサーバーの設定変更を行います。

2.1 DNS サーバーの設定変更

Mailセキュリティ・クラウドで送信・受信メールサービスをご利用いただくには、DNSサーバーの設定を変更する必要があります。

下記の [メールプロバイダー(システム管理会社)への依頼] をご参照の上、ご契約中のメールプロバイダー様へ設定変更をご依頼ください。

ご自身で変更される場合、サービス登録完了書をご参照の上、それぞれご利用いただくサービスごとにSPFレコードの追加とMXレコードの変更を実施ください。

メールプロバイダー(システム管理会社)への依頼

ご契約中のメールプロバイダー様またはシステム管理会社様へ、以下[依頼文]をご参照の上、DNSサーバーの設定変更をご依頼ください。

ご利用いただくサービスごとに、変更する内容が異なりますのでご注意ください。

また、ご利用サービス①と②の両方をご利用いただく場合は、依頼文①と②の両方をご依頼ください。

●ご利用サービス①

- MailFilter on Cloud [送信メール]
- MailFilter on Cloud [受信メール]
- MailConvert on Cloud
- MailArchive on Cloud [送信メール]
- MailArchive on Cloud [受信メール]

----[依頼文①]----

導入を検討しているメールセキュリティサービスを利用するためにSPFレコードの追加が必要です。

[SPFレコード※]を追加いただけますでしょうか。

<追加前が下記の場合>

v=spf1 +ip4:xxx.xxx.xxx.xxx ~all

<追加後>

v=spf1 +ip4:xxx.xxx.xxx.xxx [SPFレコード※] ~all

※サービス登録完了書に記載された「SPFレコード」を参照して入力してください。

●ご利用サービス②

- MailFilter on Cloud [受信メール]
- MailArchive on Cloud [受信メール]

----[依頼文②]----

導入を検討しているメールセキュリティサービスを利用するためにDNSサーバーの設定変更が必要です。
MXレコードを[MXレコード※]に変更いただけますでしょうか。

※サービス登録完了書に記載された「MXレコード」を参照して入力してください。

ご利用サービス②をご利用いただく場合、変更完了後メール受信が正常に行えることをご確認ください。
また、ご利用サービス②のみご利用いただく場合、[2.2 メールサーバーの設定変更]の作業は必要ございません。次に [5.初期設定完了] をご参照ください。

※SPFとは送信ドメイン認証の仕組みの一つです。送信経路が正しい経路かDNSを利用して検証します。

SPFレコードに登録されていないドメインからメールを送付した場合、受信を拒否される可能性がございます。

※MXレコードとは、メール送信先のメールサーバーを決定する際に使用される情報を記載したものです。

2.2 メールサーバーの設定変更

Mailセキュリティ・クラウドで送信メールに対するサービス(※)をご利用いただくには、Microsoft 365やGoogle Workspaceから送信されるメールの送信経路を変更しMailセキュリティ・クラウドを経由させる必要があります。お客様のご利用状況にあわせて以下手順を実施ください。

(※)送信メールに対するサービス

- MailFilter on Cloud [送信メール]
- MailConvert on Cloud
- MailArchive on Cloud [送信メール]

・ Microsoft 365単体をご利用の場合、「2.2.1 Microsoft 365のみ利用している場合（すべてのユーザーで利用）」、「2.2.2 Microsoft 365のみ利用している場合（一部のユーザーで利用）」へ
[イメージ図]



・ Google Workspace単体をご利用の場合、「2.2.3 Google Workspaceのみ利用している場合（すべてのユーザーで利用）」、「2.2.4 Google Workspaceのみ利用している場合（一部のユーザーで利用）」へ
[イメージ図]



2.2.1 Microsoft 365 のみ利用している場合（すべてのユーザーで利用）

すべてのユーザーのMicrosoft 365から送信されるメールをMailセキュリティ・クラウド経由とするため、以下手順を実施ください。

1 コネクタの設定

Mailセキュリティ・クラウドの環境に接続するためのコネクタを設定します。

※本手順では「サービス登録完了書」を参照する項目がございます。

1. Microsoft 365 に管理者権限でログインし、「管理」をクリックします。



2. 「Microsoft 365 管理センター」の画面に移行後、左側のタブの「すべてを表示」をクリックし、表示された「管理センター」 - 「Exchange」をクリックします。



3. 「Exchange 管理センター」の画面に移行後、「メールフロー」 - 「コネクタ」をクリックします。



4. 「コネクタ」の画面に移行後、「+コネクタを追加」をクリックし、コネクタを新規作成します。



5. メールの送信元と送信先を以下のとおりに設定し、「次」をクリックします。

項目	説明	設定値
接続元	メールの送信元を指定します。Microsoft 365 が送信元になるため「Office 365」を設定します。	Office 365
接続先	メールのリレー先を指定します。クラウドサービスの Mail セキュリティ・クラウドへ送信するため、「パートナー組織」を指定します。	パートナー組織

コネクタを追加

新しいコネクタ

名前

コネクタの使用

ルーティング

セキュリティの制限

検証メール

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

組織のメール サーバー

パートナー組織

接続先

組織のメール サーバー

パートナー組織

次

6. コネクタ名・説明を設定し、「コネクタの保存後に、何を行いますか？」を「オンにする」に設定します。
設定後、「次」をクリックします。

項目	設定値
名前	GUARDIANWALL Mail セキュリティ・クラウド
説明	GUARDIANWALL Mail セキュリティ・クラウド用コネクタ

コネクタを追加

新しいコネクタ

名前

コネクタの使用

ルーティング

セキュリティの制限

検証メール

コネクタを確認する

コネクタ名

このコネクタは、Office 365 からパートナー組織またはサービス プロバイダーに送信されるメール メッセージに対して、ルーティングとセキュリティの制約を強制します。

名前 *

GUARDIANWALL Mail セキュリティ・クラウド

説明

GUARDIANWALL Mail セキュリティ・クラウド用コネクタ

コネクタの保存後に、何を行いますか?

オンにする

戻る 次

7. 「メッセージをこのコネクタにリダイレクトするトランスポートルールが設定されている場合のみ」を選択し、「次」をクリックします。

コネクタを追加

新しいコネクタ

名前

コネクタの使用

ルーティング

セキュリティの制限

検証メール

コネクタを確認する

コネクタの使用

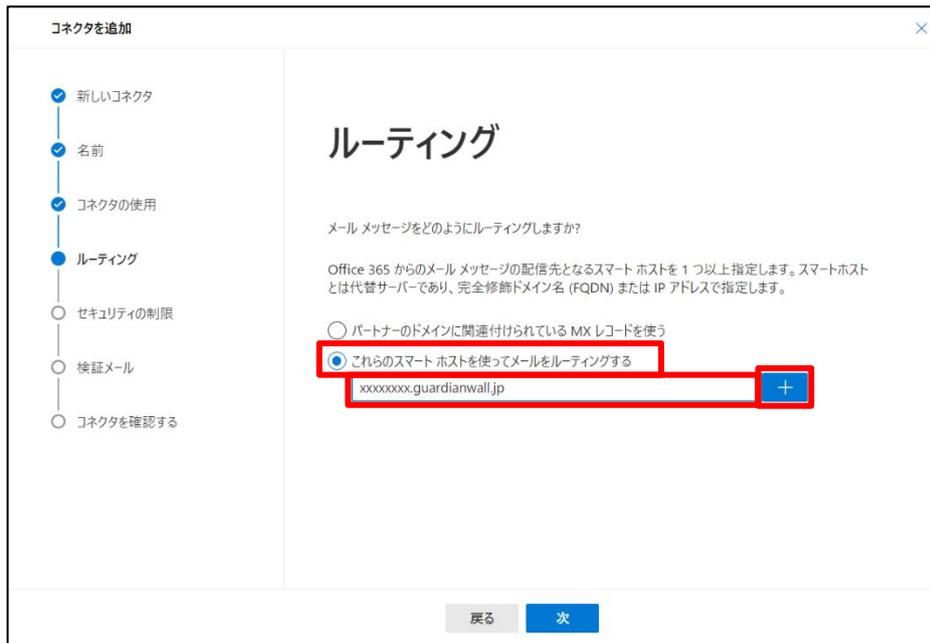
このコネクタをいつ使用するかを指定します。

メッセージをこのコネクタにリダイレクトするトランスポートルールが設定されている場合のみ

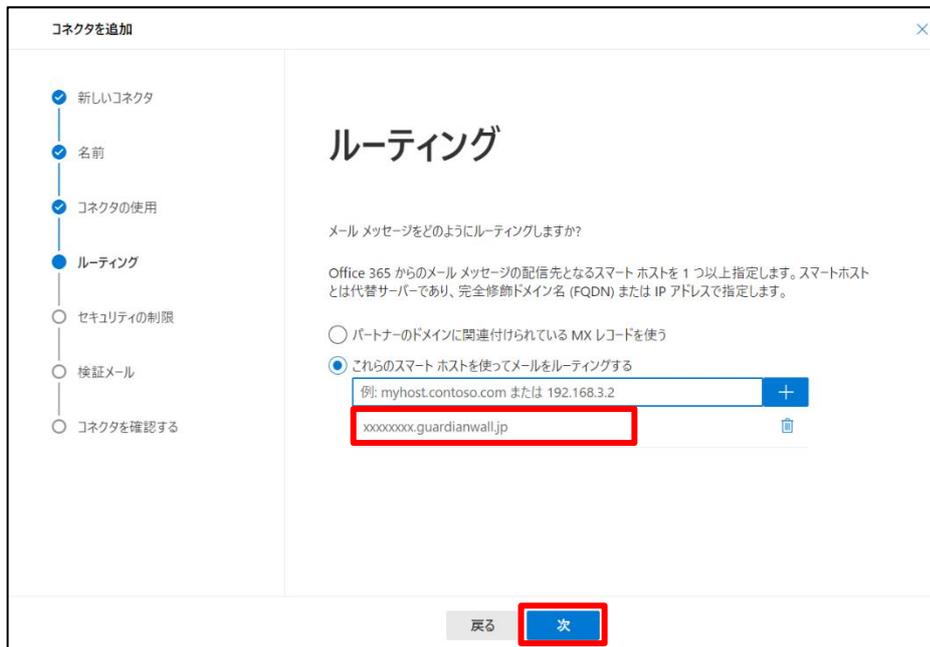
メール メッセージの送信先がこれらのドメインのときのみ

戻る 次

8. 「これらのスマートホストを使ってメールをルーティングする」を選択し、スマートホストのリレー先としてサービス登録完了書に記載された「リレー先ホスト名」を入力して、「+」をクリックします。



9. スマートホストのリレー先としてサービス登録完了書に記載された「リレー先ホスト名」が設定されていることを確認し、「次」をクリックします。



10. Mail セキュリティ・クラウドへの接続方法を以下のとおりに設定し、「次」をクリックします。

項目	設定値
常にトランスポート層セキュリティ(TLS)を使って接続をセキュリティで保護する(推奨)	■
任意のデジタル証明書（これには自己署名証明書も含まれます）	●
信頼できる証明機関（CA）によって発行された	○

11. 設定したコネクタが利用できることを検証します。

メール送信の検証用のアドレスとしてお客様がご確認いただける「Mail セキュリティ・クラウドを利用しないメールアドレス」を入力し、「OK」をクリックします。

※Mail セキュリティ・クラウドを利用するお客様ドメイン以外且つ Gmail 等メール疎通が確認できるメールアドレスを使用ください。



12. 検証に使用する「Mail セキュリティ・クラウドを利用しないメールアドレス」が設定されていることを確認し、

「検証」をクリックしてテストメールの送信を行います。



13. 「検証が成功しました」と表示されることを確認し、「次」をクリックします。

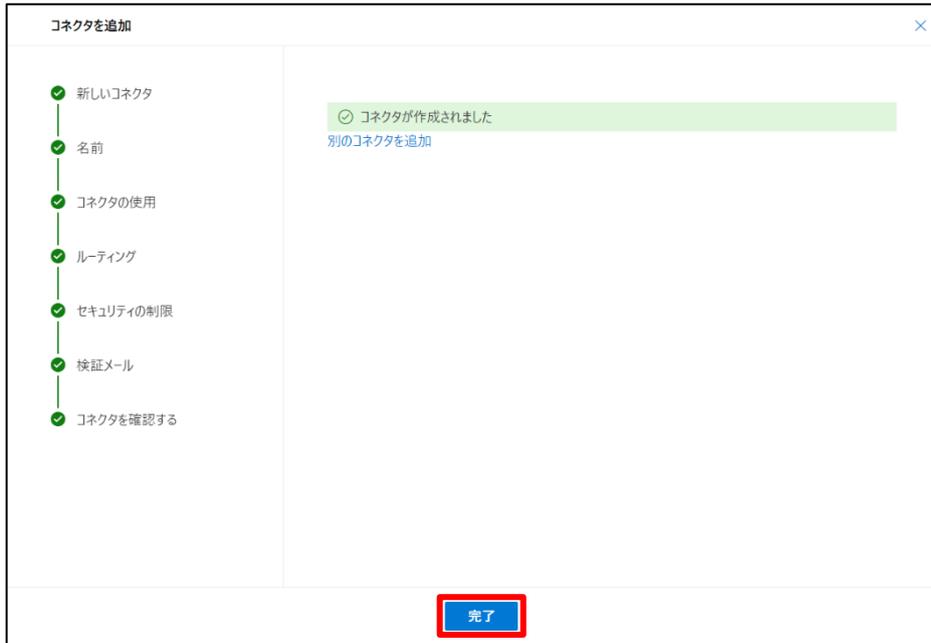
※正しい値を入力していても「検証中にエラーが発生しました」が表示される場合がありますが、コネクタの作成には影響ありません。



14. これまでの設定内容を確認し、「コネクタを作成」をクリックします。



15. 「コネクタが作成されました」と表示されたら、「完了」をクリックします。



16. 「コネクタ」の画面に設定したコネクタが追加され、状態がオンになっていることを確認します。



以上で、コネクタの設定は終了です。トランスポートルールの設定に進みます。

2 トランスポートルールの設定

設定したコネクタを利用して、メールをリレーするためのルールを設定します。

1. 「Exchange 管理センター」の画面にて「メールフロー」-「ルール」をクリックします。

「ルール」の画面より「+ルールの追加」をクリックし、「新しいルールの作成」を選択します。



2. ルールの新規作成画面に移行後、名前を設定し、「このルールを適用する」にて「送信者」を選択します。

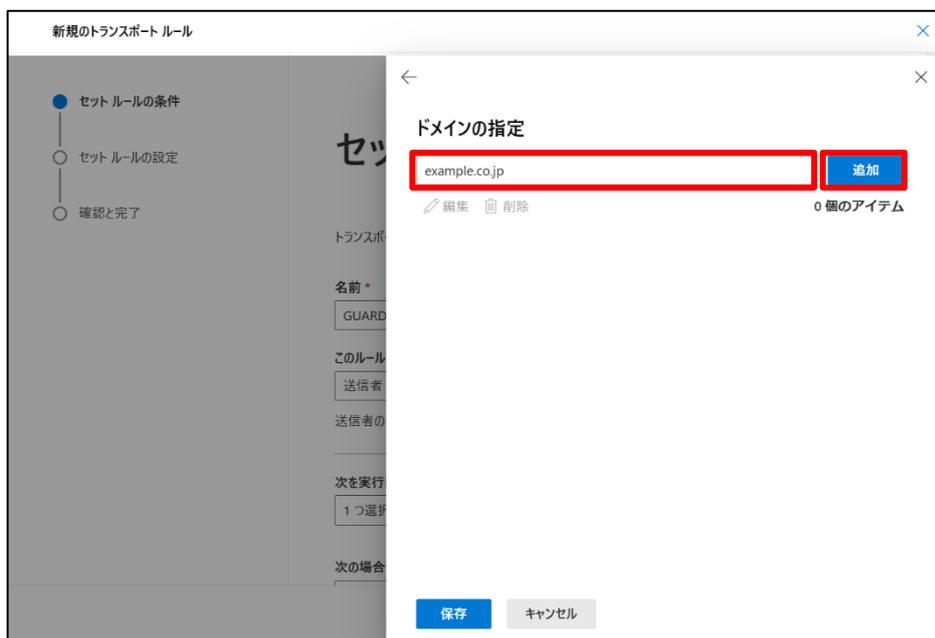
項目	設定値
名前	GUARDIANWALL Mail セキュリティ・クラウド



3. 「このルールを適用する」にて「送信者」を選択すると、右に追加の設定項目が表示されるので、リストから「ドメインは」を選択します。



4. 「Mail セキュリティ・クラウドを利用するお客様ドメイン名」を入力し、「追加」をクリックします。



5. 「お客様ドメイン名」が反映されたことを確認し、「保存」をクリックします。

The screenshot shows the 'New Transport Rule' dialog box with the 'Domain Specification' screen active. The left sidebar shows the progress: 'Set Rule Conditions' (selected), 'Set Rule Settings', and 'Confirm and Complete'. The main area is titled 'ドメインの指定' (Domain Specification). It features a search input field with a blue '追加' (Add) button. Below the input, there are icons for '編集' (Edit) and '削除' (Delete), and a counter showing '1個のアイテム' (1 item). A red box highlights the 'example.co.jp' domain name. At the bottom, there are '保存' (Save) and 'キャンセル' (Cancel) buttons, with '保存' also highlighted by a red box.

6. 「このルールを適用する」に「お客様ドメイン名」が反映されていることを確認します。

The screenshot shows the 'New Transport Rule' dialog box with the 'Set Rule Conditions' screen active. The left sidebar shows the progress: 'Set Rule Conditions' (selected), 'Set Rule Settings', and 'Confirm and Complete'. The main area is titled 'セット ルールの条件' (Set Rule Conditions). It features a text input field for the rule name, currently containing 'GUARDIANWALL Mailセキュリティクラウド'. Below this, there are two dropdown menus for 'このルールを適用する*' (Apply this rule to): '送信者' (Sender) and 'ドメインは' (Domain is). The '送信者のドメインが'example.co.jp'' option is selected and highlighted with a red box. Below these are two more dropdown menus for '次を実行します*' (Execute next): '1つ選択' (Select 1) and '1つ選択' (Select 1). At the bottom, there is a '次の場合を除く' (Except in the following cases) section and a '次へ' (Next) button.

7. 確認後、「次を実行します」にて「メッセージのリダイレクト先」を選択します。



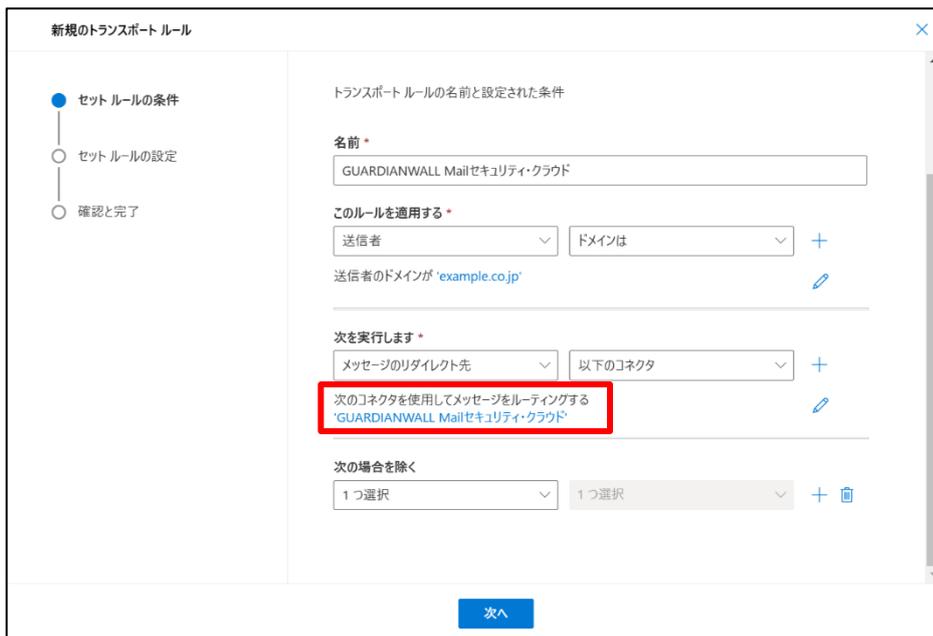
8. 「次を実行します」にて「メッセージのリダイレクト先」を選択すると、右に追加の設定項目が表示されるので、リストから「以下のコネクタ」を選択します。



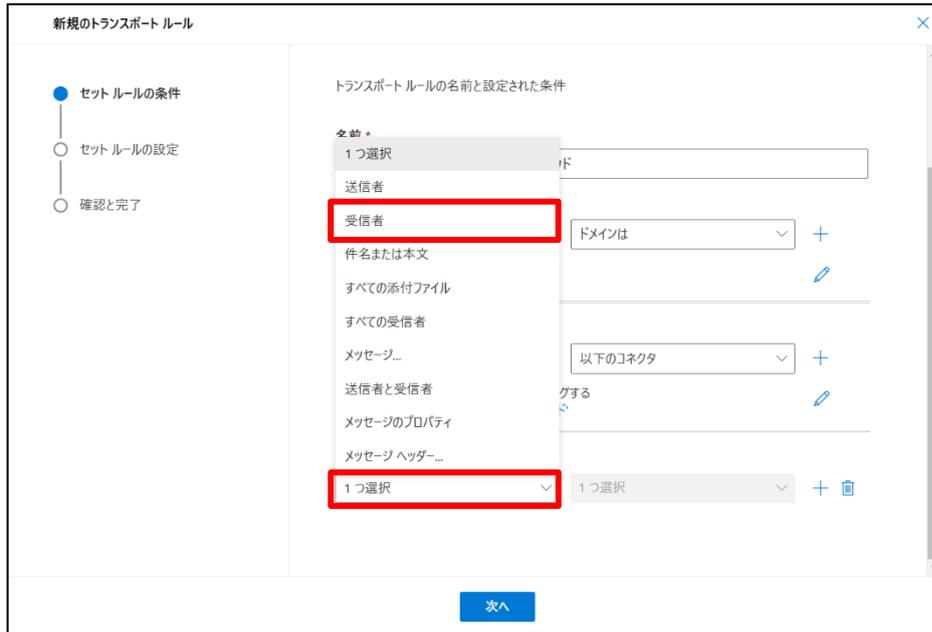
9. 前項にて設定したコネクタを選択し、「保存」をクリックします。



10. 「次を実行します」にコネクタが反映されていることを確認します。



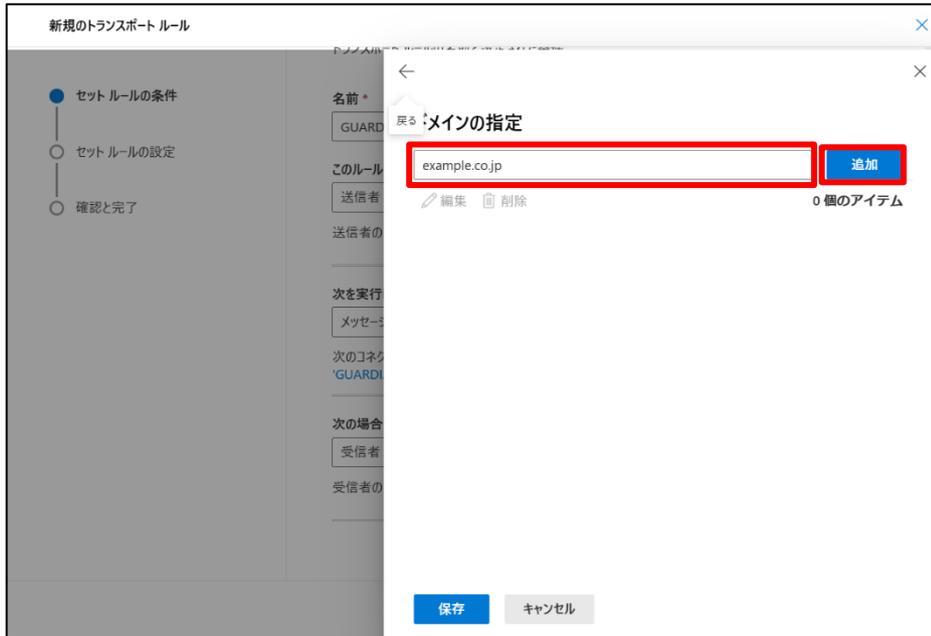
11. 「次の場合を除く」にて「受信者」を選択します。



12. 「次の場合を除く」にて「受信者」を選択すると、右に追加の設定項目が表示されるので、リストから「ドメインは」を選択します。

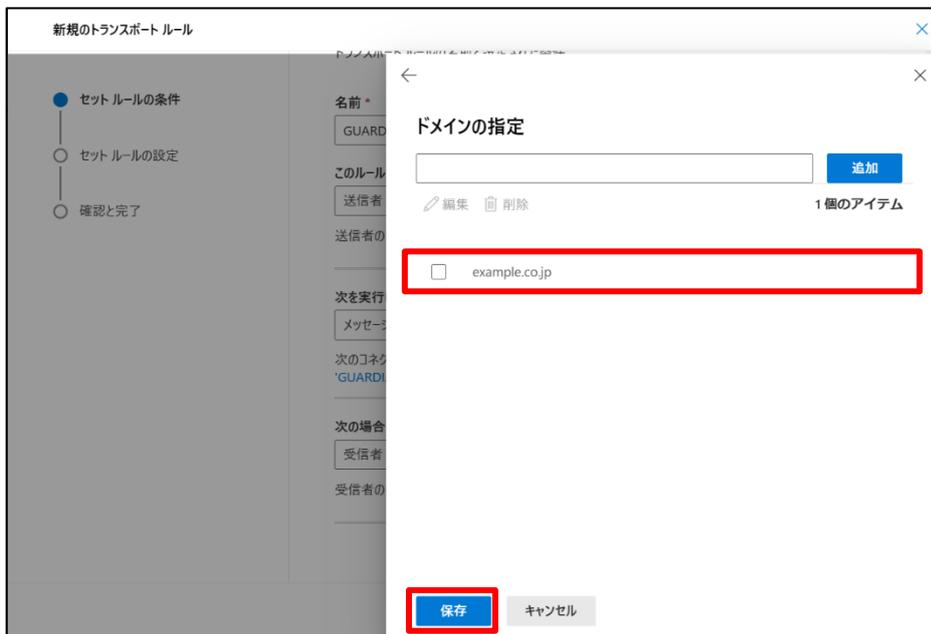


13. 「Mail セキュリティ・クラウドを利用するお客様ドメイン名」を入力し、「追加」をクリックします。



Microsoft 365 同テナント内に複数のドメインのご利用がある場合は、すべてのドメインを入力してください。

14. 「お客様ドメイン名」が反映されたことを確認し、「保存」をクリックします。



15. ルールの例外条件に「お客様ドメイン名」が反映されていることを確認し、「次へ」をクリックします。



16. 画面を下にスクロールし、「メッセージの送信者アドレスに一致します」にて「エンベロープ」を選択します。
選択後、「次へ」をクリックします。



17. これまでの設定内容を確認し、「完了」をクリックします。

新規のトランスポートルール

セットルールの条件
セットルールの設定
確認と完了

確認と完了

このルールの作成が完了すると、[ルール] ページから有効にするまで既定で無効になります

ルール名
GUARDIANWALL Mailセキュリティクラウド

ルールに関するコメント

ルールの条件	ルールの設定
このルールを適用する 送信者のドメインが 'example.co.jp'	モード Enforce
次を実行します 次のコネクタを使用してメッセージをルーティングする 'GUARDIANWALL Mailセキュリティクラウド'	期間の設定 特定の日付範囲が設定されていません
次の場合を除く	優先度 0

戻る 完了

18. 「トランスポートルールが正常に作成されました」と表示されることを確認し、「完了」をクリックします。

新規のトランスポートルール

セットルールの条件
セットルールの設定
確認と完了

トランスポートルールが正常に作成されました

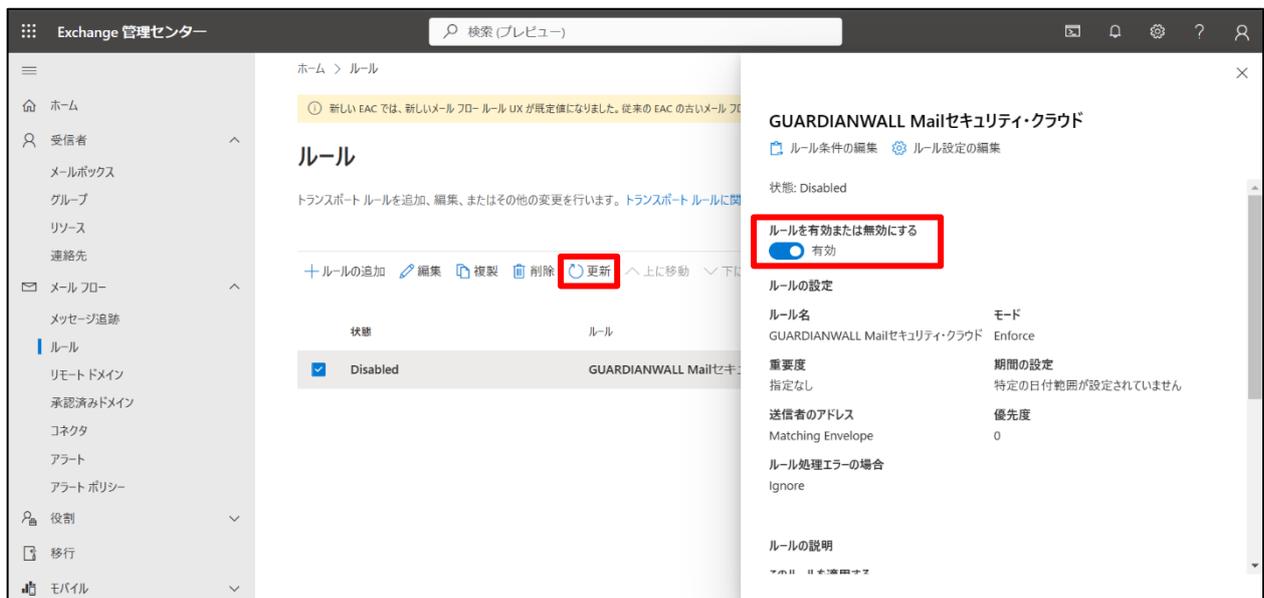
完了

19. ルールの画面に設定したルールが追加されていることを確認し、追加されたルールをクリックします。



20. 「ルールを有効または無効にする」をクリックし、「有効」にします。

有効後、更新をクリックします。



21. 状態が「Enabled」になっていることを確認します。

Exchange 管理センター

ホーム > ルール

新しい EAC では、新しいメール フロー ルール UX が既定値になりました。従来の EAC の古いメール フロー ルール UX は、2023 年 1 月末までに廃止される予定です。従来の EAC の古いバージョンに移動します。

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。[トランスポート ルールに関する詳細情報](#)

+ ルールの追加 編集 複製 更新 上に移動 下に移動

1 個のアイテム 検索

状態	ルール	優先度	処理の停止のルール
<input checked="" type="checkbox"/> Enabled	GUARDIANWALL Mailセキュリティ・クラウド	0	X

以上で、Microsoft 365の設定は終了です。

2.2.2 Microsoft 365 のみ利用している場合（一部のユーザーで利用）

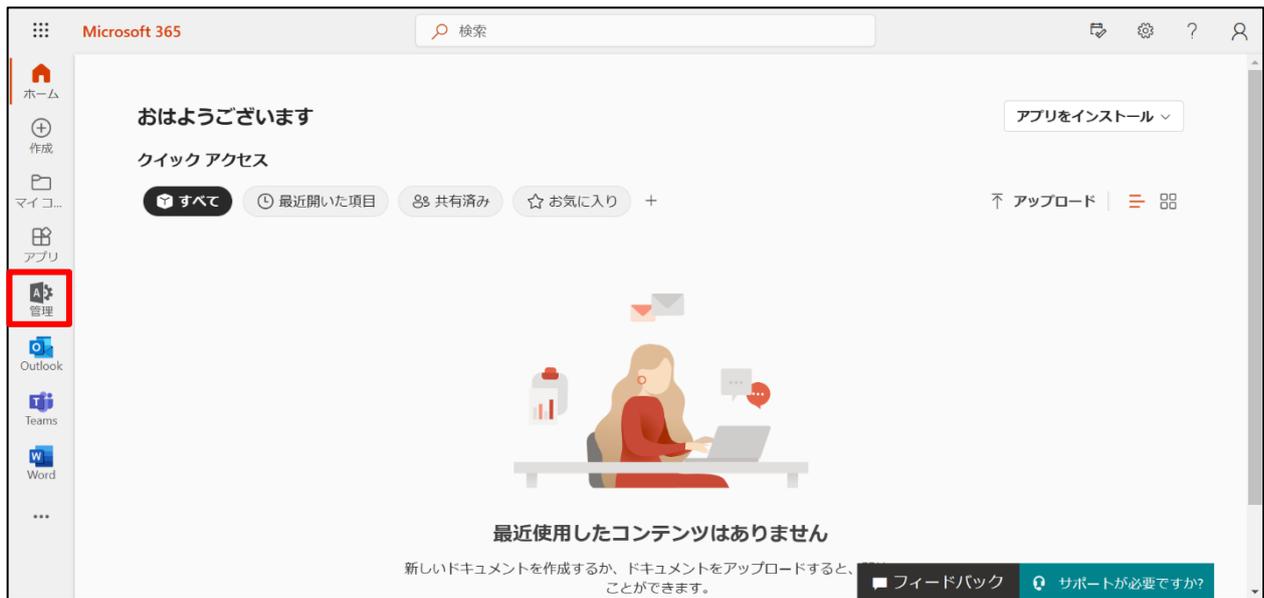
一部のユーザーのMicrosoft 365から送信されるメールをMailセキュリティ・クラウド経由とするため、以下手順を実施ください。

1 コネクタの設定

Mailセキュリティ・クラウドの環境に接続するためのコネクタを設定します。

※本手順では「サービス登録完了書」を参照する項目がございます。

1. Microsoft 365 に管理者権限でログインし、「管理」をクリックします。



2. 「Microsoft 365 管理センター」の画面に移行後、左側のタブの「すべてを表示」をクリックし、表示された「管理センター」 - 「Exchange」をクリックします。



3. 「Exchange 管理センター」の画面に移行後、「メールフロー」 - 「コネクタ」をクリックします。



4. 「コネクタ」の画面に移行後、「+コネクタを追加」をクリックし、コネクタを新規作成します。



5. メールの送信元と送信先を以下のとおりに設定し、「次」をクリックします。

項目	説明	設定値
接続元	メールの送信元を指定します。Microsoft 365 が送信元になるため「Office 365」を設定します。	Office 365
接続先	メールのリレー先を指定します。クラウドサービスの Mail セキュリティ・クラウドへ送信するため、「パートナー組織」を指定します。	パートナー組織

コネクタを追加

新しいコネクタ

名前

コネクタの使用

ルーティング

セキュリティの制限

検証メール

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
- 組織のメール サーバー
- パートナー組織

接続先

- 組織のメール サーバー
- パートナー組織

次

6. コネクタ名・説明を設定し、「コネクタの保存後に、何を行いますか？」を「オンにする」に設定します。
設定後、「次」をクリックします。

項目	設定値
名前	GUARDIANWALL Mail セキュリティ・クラウド
説明	GUARDIANWALL Mail セキュリティ・クラウド用コネクタ

コネクタを追加

新しいコネクタ

名前

コネクタの使用

ルーティング

セキュリティの制限

検証メール

コネクタを確認する

コネクタ名

このコネクタは、Office 365 からパートナー組織またはサービス プロバイダーに送信されるメール メッセージに対して、ルーティングとセキュリティの制約を強制します。

名前 *

GUARDIANWALL Mailセキュリティクラウド

説明

GUARDIANWALL Mailセキュリティクラウド用コネクタ

コネクタの保存後に、何を行いますか?

オンにする

戻る 次

7. 「メッセージをこのコネクタにリダイレクトするトランスポートルールが設定されている場合のみ」を選択し、「次」をクリックします。

コネクタを追加

新しいコネクタ

名前

コネクタの使用

ルーティング

セキュリティの制限

検証メール

コネクタを確認する

コネクタの使用

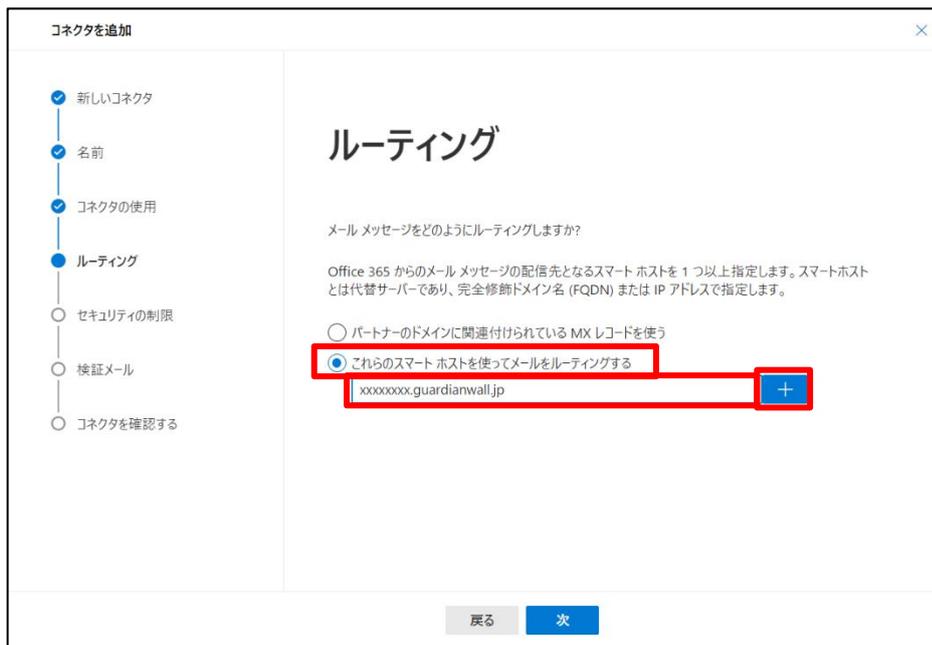
このコネクタをいつ使用するかを指定します。

メッセージをこのコネクタにリダイレクトするトランスポートルールが設定されている場合のみ

メール メッセージの送信先がこれらのドメインのときのみ

戻る 次

8. 「これらのスマートホストを使ってメールをルーティングする」を選択し、スマートホストのリレー先としてサービス登録完了書に記載された「リレー先ホスト名」を入力して、「+」をクリックします。



9. スマートホストのリレー先としてサービス登録完了書に記載された「リレー先ホスト名」が設定されていることを確認し、「次」をクリックします。



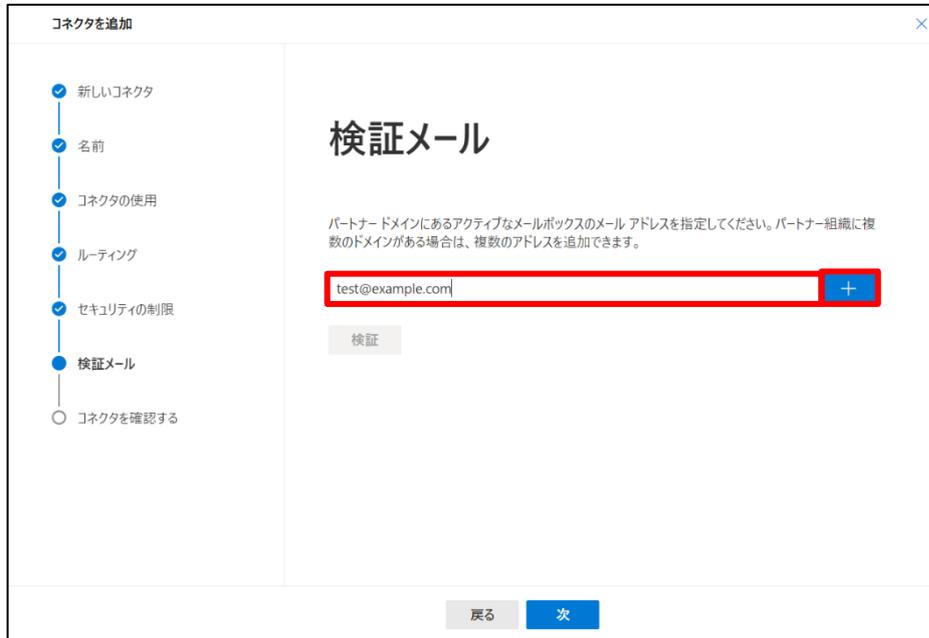
10. Mail セキュリティ・クラウドへの接続方法を以下のとおりに設定し、「次」をクリックします。

項目	設定値
常にトランスポート層セキュリティ(TLS)を使って接続をセキュリティで保護する(推奨)	■
任意のデジタル証明書（これには自己署名証明書も含まれます）	●
信頼できる証明機関（CA）によって発行された	○

11. 設定したコネクタが利用できることを検証します。

メール送信の検証用のアドレスとしてお客様がご確認いただける「Mail セキュリティ・クラウドを利用しないメールアドレス」を入力し、「OK」をクリックします。

※Mail セキュリティ・クラウドを利用するお客様ドメイン以外且つ Gmail 等メール疎通が確認できるメールアドレスを使用ください。



12. 検証に使用する「Mail セキュリティ・クラウドを利用しないメールアドレス」が設定されていることを確認し、

「検証」をクリックしてテストメールの送信を行います。



13. 「検証が成功しました」と表示されることを確認し、「次」をクリックします。

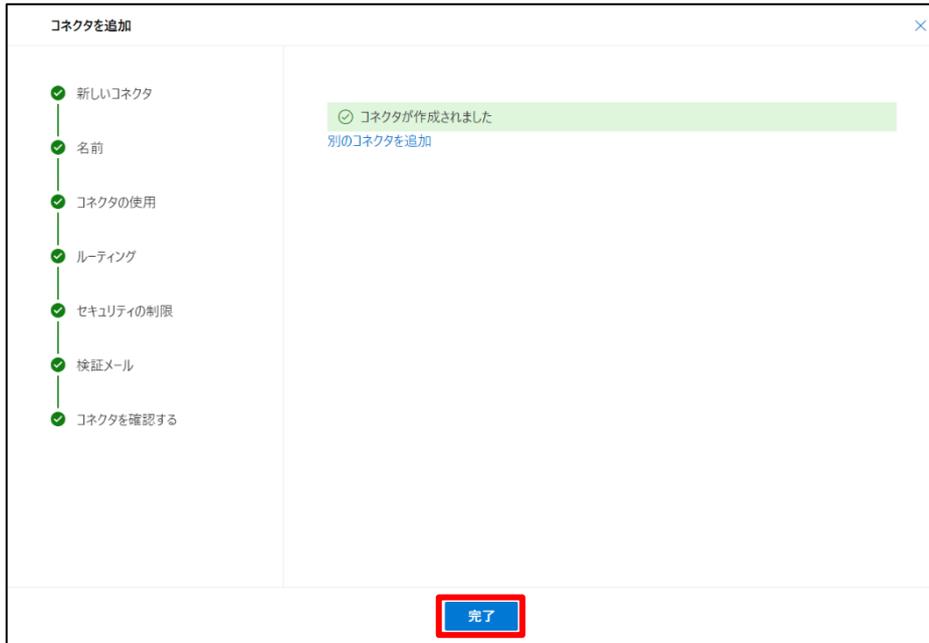
※正しい値を入力していても「検証中にエラーが発生しました」が表示される場合がありますが、コネクタの作成には影響ありません。



14. これまでの設定内容を確認し、「コネクタを作成」をクリックします。



15. 「コネクタが作成されました」と表示されたら、「完了」をクリックします。



16. 「コネクタ」の画面に設定したコネクタが追加され、状態がオンになっていることを確認します。



以上で、コネクタの設定は終了です。トランスポートルールの設定に進みます。

2 トランスポートルールの設定

設定したコネクタを利用して、メールをリレーするためのルールを設定します。

1. 「Exchange 管理センター」の画面にて「メールフロー」-「ルール」をクリックします。

「ルール」の画面より「+ルールの追加」をクリックし、「新しいルールの作成」を選択します。



2. ルールの新規作成画面に移行後、名前を設定し、「このルールを適用する」にて「送信者」を選択します。

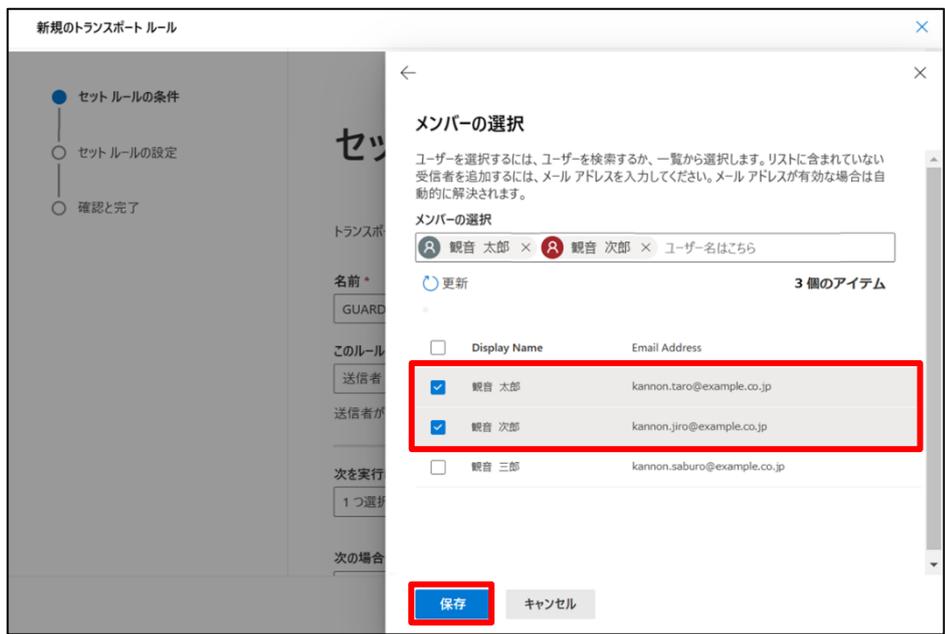
項目	設定値
名前	GUARDIANWALL Mail セキュリティ・クラウド



3. 「このルールを適用する」にて「送信者」を選択すると、右に追加の設定項目が表示されるので、リストから「この人物である」を選択します。



4. 「Mail セキュリティ・クラウドを利用するユーザー」を選択し、「保存」をクリックします。



5. 「このルールを適用する条件」に「ユーザー」が反映されていることを確認します。

新規のトランスポートルール

● セットルールの条件
○ セットルールの設定
○ 確認と完了

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*

GUARDIANWALL Mailセキュリティクラウド

このルールを適用する*

送信者 ▼ この人物である ▼ +

送信者が次の場合
'kannon.taro@example.co.jp' or
'kannon.jiro@example.co.jp'

次を実行します*

1つ選択 ▼ 1つ選択 ▼ +

次へ

6. 確認後、「次を実行します」にて「メッセージのリダイレクト先」を選択します。

新規のトランスポートルール

● セットルールの条件
○ セットルールの設定
○ 確認と完了

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*

GUARDIANWALL Mailセキュリティクラウド

このルールを適用する*

送信者 ▼ 1つ選択 ▼ +

送信者が次の場合
'kannon.taro@example.co.jp' or
'kannon.jiro@example.co.jp'

次を実行します*

1つ選択 ▼

次の場合を除く

1つ選択 ▼

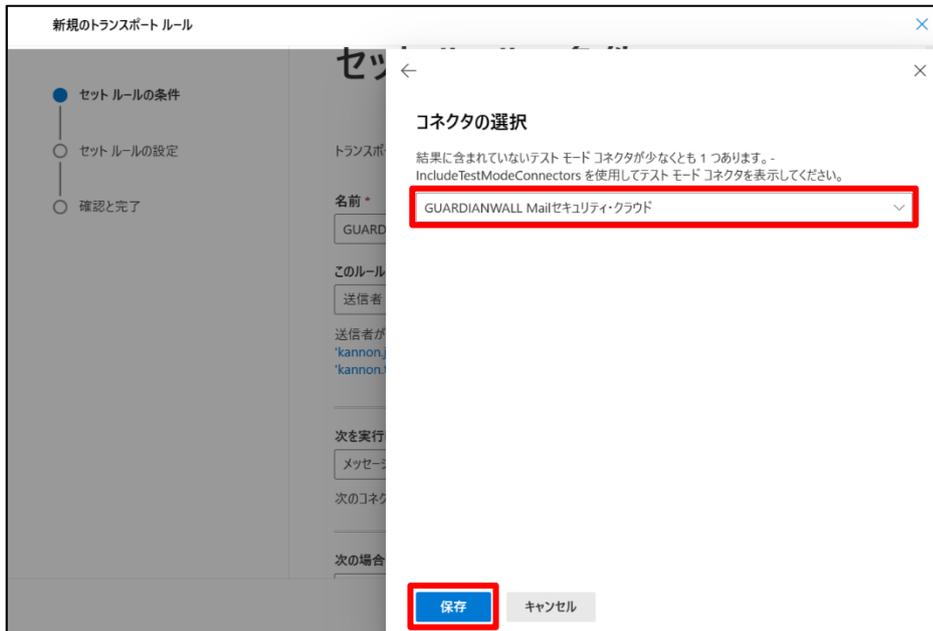
メッセージを転送して承認を受ける
メッセージのリダイレクト先
メッセージをブロックする
受信者を追加
メッセージに免責事項を適用する
メッセージのプロパティの変更
メッセージのセキュリティを変更する
メッセージの件名の先頭に追加する
ポリシー ヒントを使用して送信者に通知
インシデントレポートの生成と送信先
受信者にメッセージを通知する

次へ

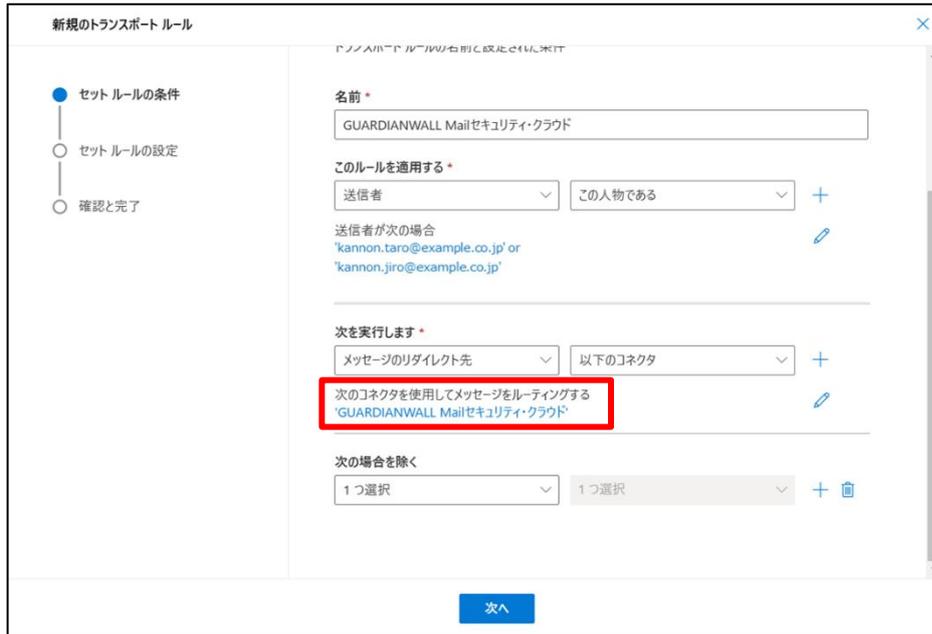
7. 「次を実行します」にて「メッセージのリダイレクト先」を選択すると、右に追加の設定項目が表示されるので、リストから「以下のコネクタ」を選択します。



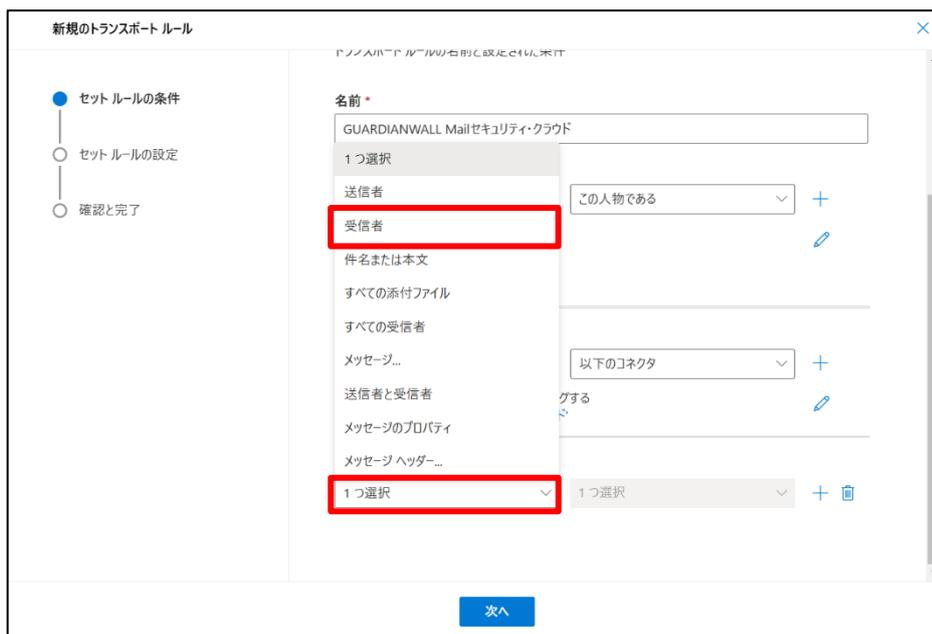
8. 前項にて設定したコネクタを選択し、「保存」をクリックします。



9. 「次を実行します」にコネクタが反映されていることを確認します。



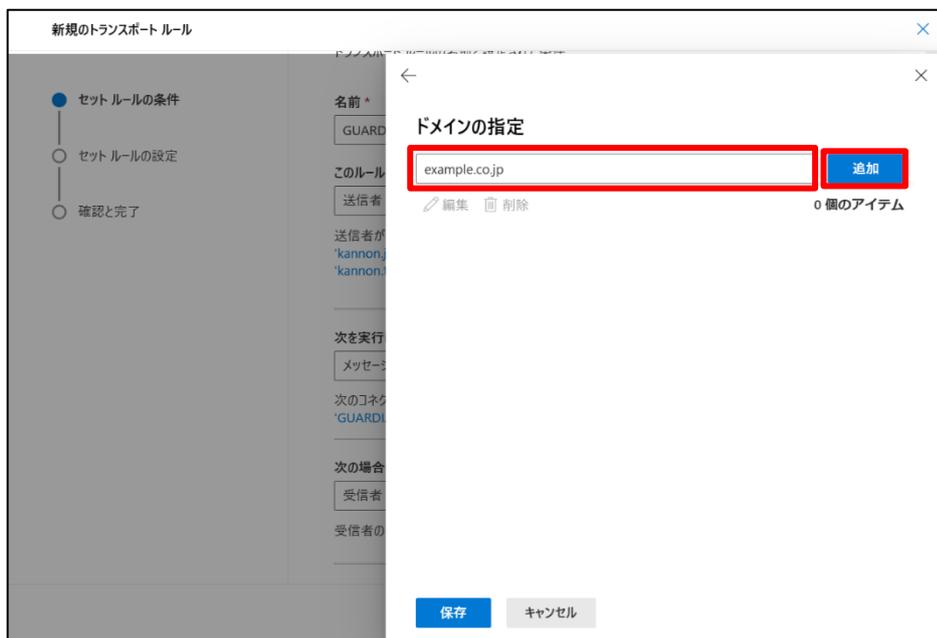
10. 「次の場合を除く」にて「受信者」を選択します。



11. 「次の場合を除く」にて「受信者」を選択すると、右に追加の設定項目が表示されるので、リストから「ドメインは」を選択します。

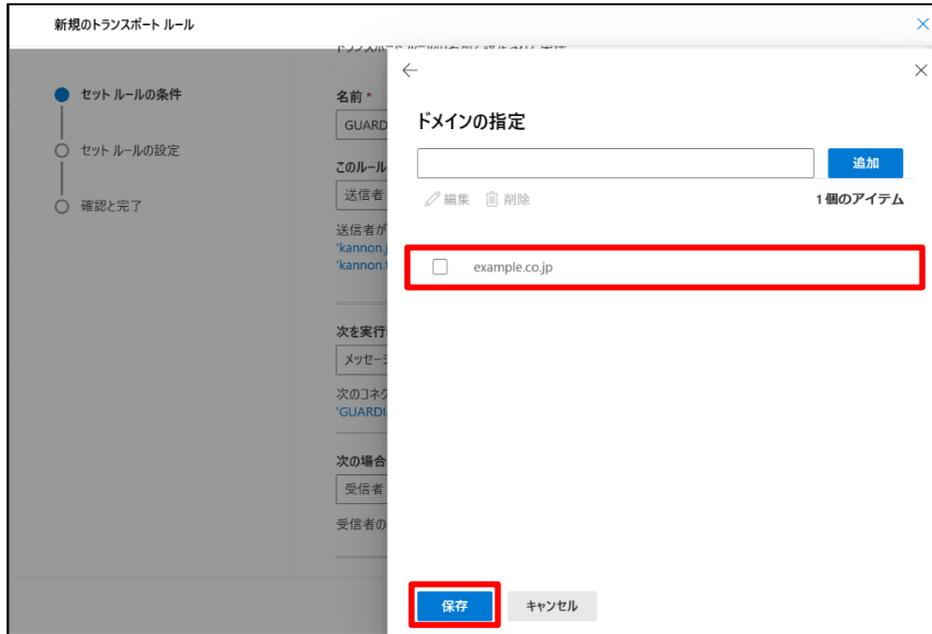


12. 「Mail セキュリティ・クラウドを利用するお客様ドメイン名」を入力し、「追加」をクリックします。



 Microsoft 365 同テナント内に複数のドメインのご利用がある場合は、すべてのドメインを入力してください。

13. 「お客様ドメイン名」が反映されたことを確認し、「保存」をクリックします。



14. ルールの例外条件に「お客様ドメイン名」が反映されていることを確認し、「次へ」をクリックします。



15. 画面を下にスクロールし、「メッセージの送信者アドレスに一致します」にて「エンベロープ」を選択します。

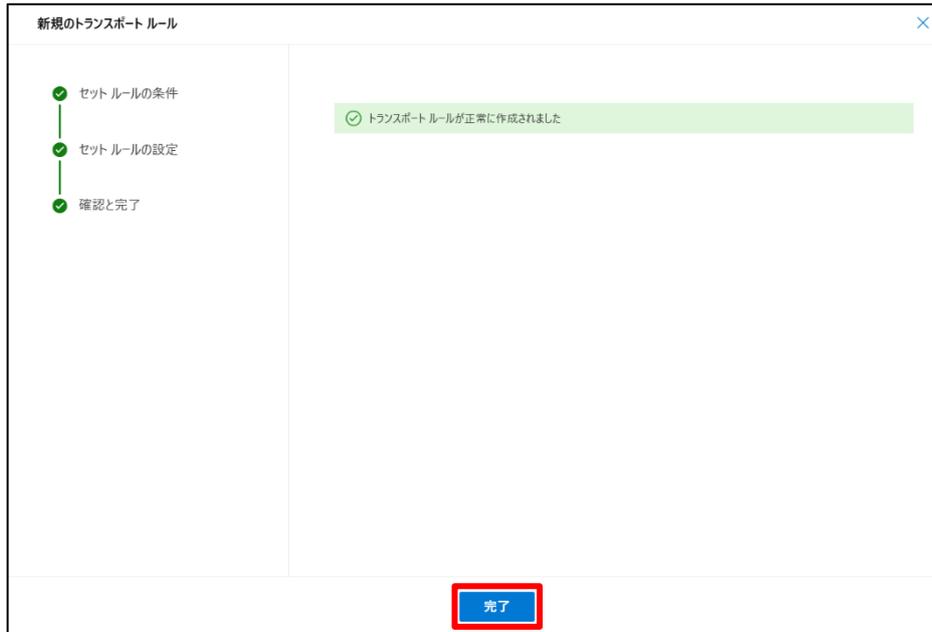
選択後、「次へ」をクリックします。



16. これまでの設定内容を確認し、「完了」をクリックします。



17. 「トランスポート ルールが正常に作成されました」と表示されることを確認し、「完了」をクリックします。

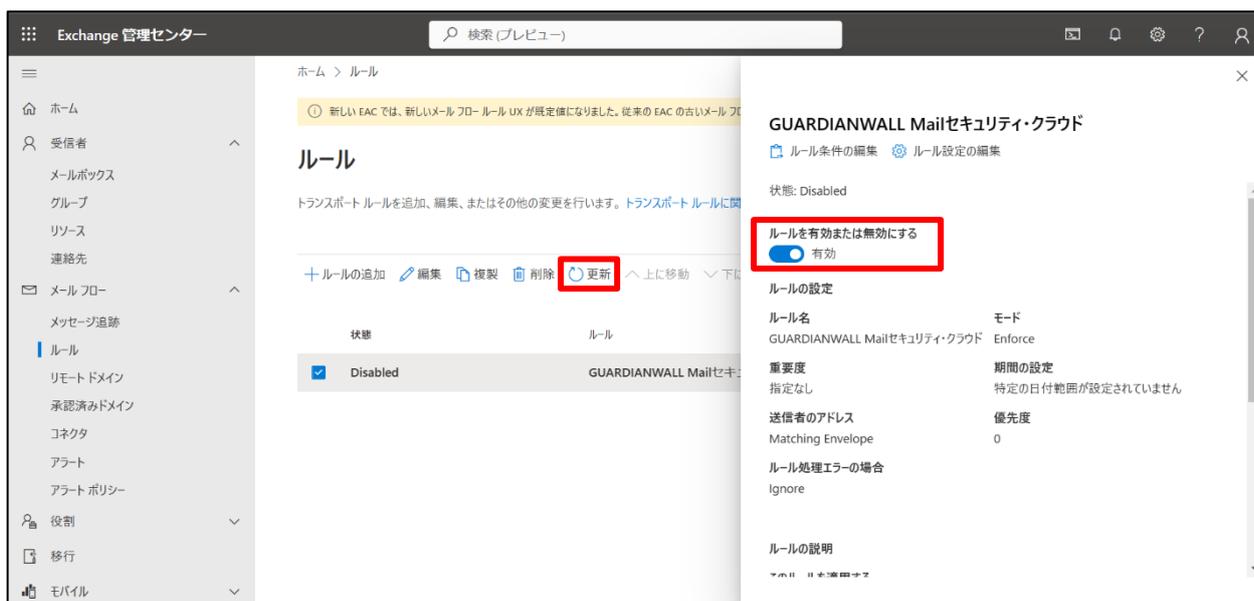


18. ルールの画面に設定したルールが追加されていることを確認し、追加されたルールをクリックします。



19. 「ルールを有効または無効にする」をクリックし、「有効」にします。

有効後、更新をクリックします。



20. 状態が「Enabled」になっていることを確認します。



以上で、Microsoft 365の設定は終了です。

2.2.3 Google Workspace のみ利用している場合（すべてのユーザーで利用）

すべてのユーザーのGoogle Workspaceから送信されるメールをMailセキュリティ・クラウド経由とするため、以下手順を実施ください。

1 ルートの設定

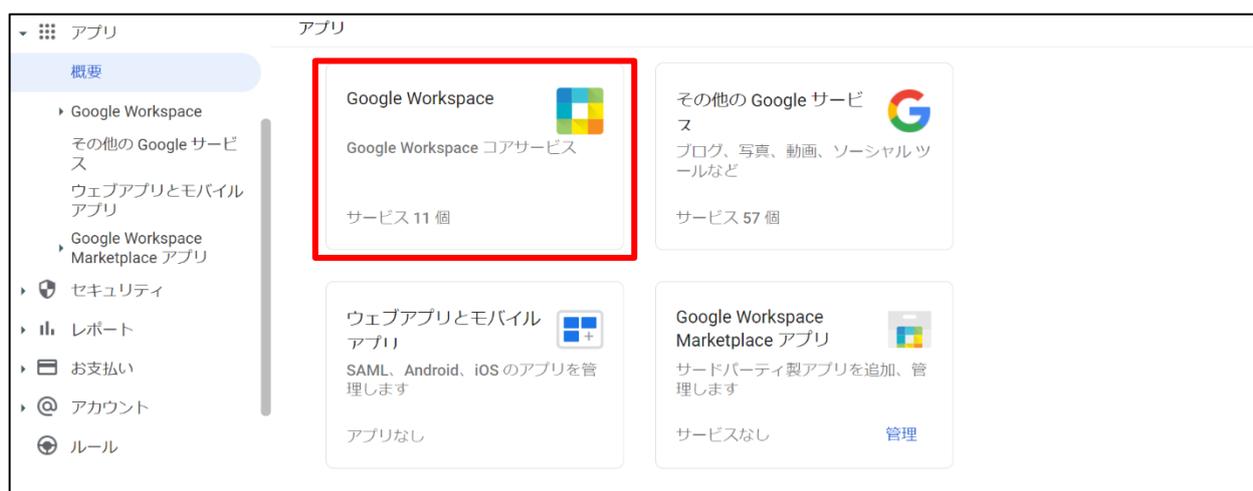
Mailセキュリティ・クラウドの環境に接続するためのルートを設定します。

※本手順では「サービス登録完了書」を参照する項目がございます。

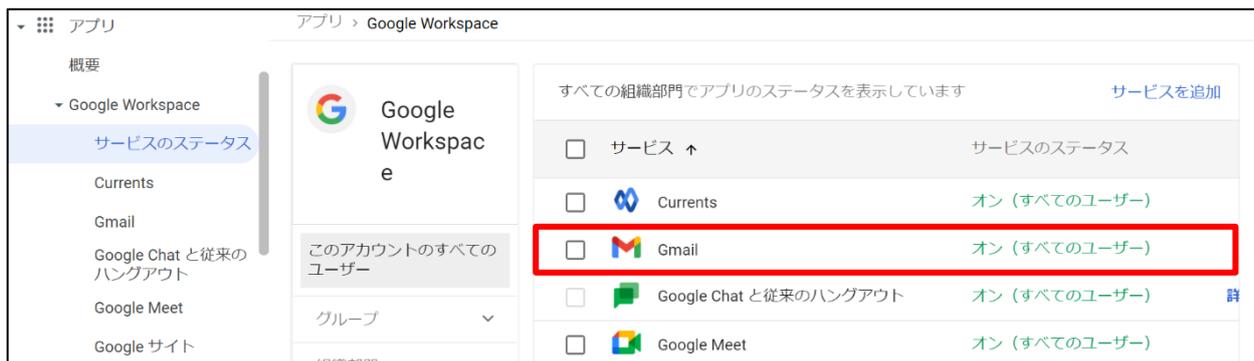
1. Google Workspace に管理者権限でログインし、管理コンソールを開き、「アプリ」をクリックします。



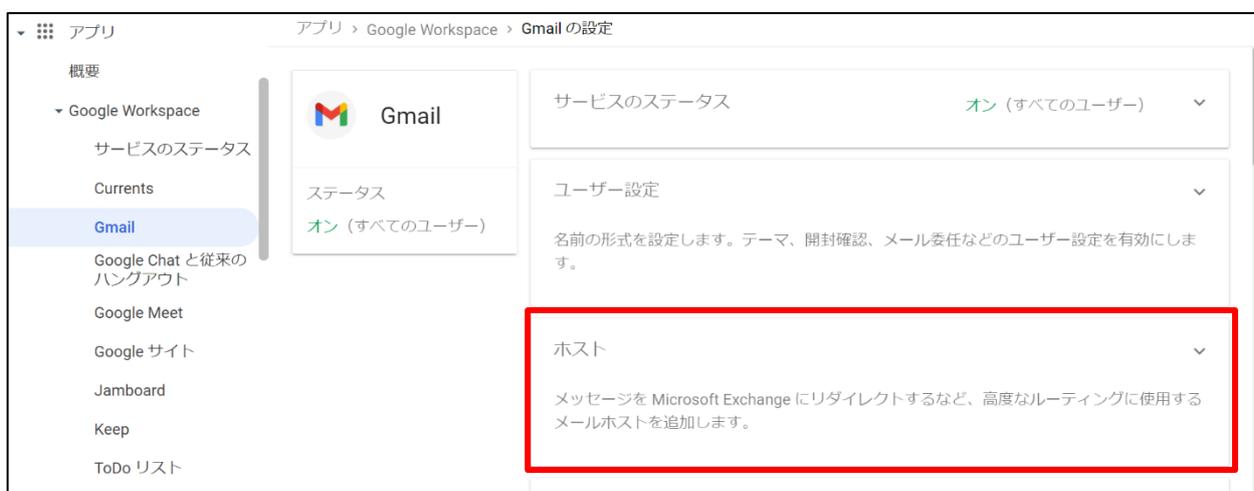
2. 「アプリ」の画面に移行後、「Google Workspace」をクリックします。



3. 「Google Workspace」(Google Apps)の画面に移行後、「Gmail」をクリックします。



4. 「Gmail の設定」の画面に移行後、「ホスト」をクリックします。



5. 「ホスト」画面にて、「ルートを追加」をクリックします。



6. 以下のとおりに設定し、「保存」をクリックします。

項目	設定値
名前	GUARDIANWALL Mail セキュリティ・クラウド
ホスト	単一のホスト
ホスト名または IP を入力	サービス登録完了書に記載された「リレー先ホスト名」 ポート：25
メールの送受信時にセキュリティ プロトコルで保護された（TLS）接続を必須とする（推奨）	■

メールのルートを追加

名前 [詳細](#)

GUARDIANWALL Mailセキュリティ

このフィールドは必須です。

1. メールサーバーの指定

番号が 25、587、1024～65535 のポートのみ使用できます。

単一のホスト ▼
 xxxxxxxx.guardianw : 25

2. オプション

ホストで MX ルックアップを実行する

メール送受信時にセキュリティ プロトコルで保護された（TLS）接続を必須とする（推奨）

CA の署名付き証明書を必須とする（推奨）

証明書のホスト名を検証する（推奨）

[TLS 接続をテスト](#)

キャンセル 保存

7. 社内間のメールについては、Google Workspace の MX レコード先へ送信されるように設定します。

「ルートを追加」をクリックします。



8. 以下のとおりに設定し、「保存」をクリックします。

項目	設定値
名前	Google Workspace
ホスト	単一のホスト
ホスト名または IP を入力	ホスト名 : smtp.google.com ポート : 25
メールの送受信時にセキュリティ プロトコルで保護された (TLS) 接続を必須とする (推奨)	■

メールのルートを追加

名前 詳細

Google Workspace

このフィールドは必須です。

1. メールサーバーの指定

番号が 25、587、1024~65535 のポートのみ使用できます。

単一のホスト ▼
 smtp.google.com : 25

2. オプション

ホストで MX ルックアップを実行する

メール送受信時にセキュリティ プロトコルで保護された (TLS) 接続を必須とする (推奨)

CA の署名付き証明書を必須とする (推奨)

証明書のホスト名を検証する (推奨)

[TLS 接続をテスト](#)

キャンセル 保存

以上で、ルートの設定は終了です。メールリレールール設定に進みます。

2 メールリレールールの設定

設定したルートを利用して、メールをリレーするためのルールを設定します。

1. 「Gmail の設定」をクリックします。



2. 「Gmail の設定」画面に移動後、画面を下にスクロールし、「迷惑メール、フィッシング、不正なソフトウェア」をクリックします。



3. 「迷惑メール、フィッシング、不正なソフトウェア」の画面にて、画面を下にスクロールし、「受信ゲートウェイ」をクリックします。



4. 「有効にする」にチェックを入れ、「追加」をクリックします。

受信ゲートウェイ メールゲートウェイを使用して受信メールを転送する場合は、こちらにゲートウェイを入力して迷惑メール処理を改善してください [詳細](#)

有効にする

1. ゲートウェイの IP

IP アドレスまたは IP 範囲

IP アドレスがまだ追加されていません。 [追加](#)

[追加](#)

外部 IP を自動検出する (推奨)

ゲートウェイの IP から届いたものではないメールはすべて拒否する

上で指定したメールゲートウェイからの接続には TLS を必須とする

2. メールのタグ付け

以下のヘッダーの正規表現と一致するメールを迷惑メールとみなす

i すべてのユーザーに変更が反映されるまでに、最長で 24 時間かかることがあります。
[監査ログ](#)で以前の変更を確認できます

キャンセル 保存

5. サービス登録完了書に記載されたすべての「受信ゲートウェイ IP」を入力し、「保存」をクリックします。

IP アドレスの設定は、1 つずつ行い、すべての「受信ゲートウェイ IP」を入力し終わるまで、繰り返します。

IP アドレスまたは IP 範囲の追加

IP アドレスまたは IP 範囲を入力

1.1.1.2

キャンセル [保存](#)

6. すべての IP アドレスを追加後、「保存」をクリックします。

受信ゲートウェイ メールゲートウェイを使用して受信メールを転送する場合は、こちらにゲートウェイを入力して迷惑メール処理を改善してください [詳細](#)

有効にする

1. ゲートウェイの IP

IP アドレスまたは IP 範囲
1.1.1.2

[追加](#)

外部 IP を自動検出する (推奨)

ゲートウェイの IP から届いたものではないメールはすべて拒否する

上で指定したメールゲートウェイからの接続には TLS を必須とする

2. メールのタグ付け

以下のヘッダーの正規表現と一致するメールを迷惑メールとみなす

i すべてのユーザーに変更が反映されるまでに、最長で 24 時間かかることがあります。
[監査ログ](#)で以前の変更を確認できます

未保存の変更が 1 件あります [キャンセル](#) 保存

7. 「Gmail の設定」をクリックします。

アプリ > Google Workspace Gmail の設定 迷惑メール、フィッシング、不正なソフトウェア

Gmail

ステータス
オン (すべてのユーザー)

組織部門

組織部門の検索

受信ゲートウェイ メールゲートウェイを使用して受信メールを転送する場合は、こちらにゲートウェイを入力して迷惑メール処理を改善してください [詳細](#)

有効にする: オン

迷惑メール 迷惑メールフォルダに振り分けられない、承認されている送信者のリストを作成します。 [設定](#)

i すべてのユーザーに変更が反映されるまでに、最長で 24 時間かかることがあります。
[監査ログ](#)で以前の変更を確認できます

8. 「Gmail の設定」画面に移動後、画面を下にスクロールし、「ルーティング」をクリックします。



9. 「ルーティング」の画面にて、「送信ゲートウェイ」が空欄となっているか確認してください。



10. 「ルーティング」の「設定」をクリックします。



11. 名前を設定し、「送信」を選択します。

項目	設定値
名前	GUARDIANWALL Mail セキュリティ・クラウド

設定を追加

ルーティング [詳細](#)

GUARDIANWALL Mailセキュリティ・クラウド

1. 影響を受けるメール

- 受信
- 送信
- 内部 - 送信
- 内部 - 受信

2. 上記の種類メッセージに対し、次の処理を行う

メッセージを変更 ▼

ヘッダー

キャンセル [保存](#)

12. 「ルートを変更」を選択し、[1 ルートの設定]の手順 6 にて設定したルートを選択します。

設定を追加

件名

件名の先頭に追加するカスタムテキスト

ルート

ルートを変更

迷惑メールのルートも変更する

この受信者からのバウンスメールを送信元に送信しない

GUARDIANWALL Mailセキュリティ・クラウド

エンベロープ受信者

エンベロープ受信者を変更する

キャンセル 保存

13. 下にスクロールし、「オプションを表示」をクリックします。

設定を追加

このメッセージには迷惑メールフィルタを適用しない

添付ファイル

メッセージから添付ファイルを削除

その他の配信先

受信者を追加

暗号化（配信時のみ）

セキュアなトランスポート（TLS）を使用

オプションを表示

キャンセル 保存

14. 以下のとおりに設定し、「保存」をクリックします。

項目	設定値
ユーザー	■
グループ	■

設定を追加

オプションを表示しない

A. アドレスリスト

アドレスリストを使用して、この設定を適用するアプリケーションを除外、制御する

アドレスリストを該当するユーザーに適用する ▼

特定のアドレスまたはドメインにはこの設定を適用しない

特定のアドレスまたはドメインにのみ、この設定を適用する

B. 影響を受けるアカウントの種類

ユーザー

グループ

認識できない、キャッチオール

キャンセル
保存

15. ルールが追加されていることを確認します。

社内間のメールをリレーするルールを設定するため、「別のルールを追加」をクリックします。

アプリ > Google Workspace > Gmail の設定 > ルーティング

Gmail

ステータス
オン (すべてのユーザー)

組織部門

組織部門の検索

▶ 全ユーザー

次の組織部門のユーザー設定を表示しています: 全ユーザー

ルーティング

送信ゲートウェイ [詳細](#)
「全ユーザー」で適用しました
送信メールを次の SMTP サーバーに転送します:

説明	ステータス	ソース
GUARDIANWALL Mailセキュリティ・クラウド	有効	ローカルに適用

別のルールを追加

すべてのユーザーに変更が反映されるまでに、最長で 24 時間かかることがあります。

16. 名前を設定し、「内部-送信」を選択します。

項目	設定値
名前	Google Workspace

設定を追加

ルーティング [詳細](#)

Google Workspace

1. 影響を受けるメール

- 受信
- 送信
- 内部-送信
- 内部-受信

2. 上記の種類メッセージに対し、次の処理を行う

メッセージを変更 ▼

ヘッダー

キャンセル [保存](#)

17. 「ルートを変更」を選択し、[1 ルートの設定]の手順 8 にて設定したルートを選択します。

設定を追加

件名

件名の先頭に追加するカスタム テキスト

ルート

ルートを変更

迷惑メールのルートも変更する

この受信者からのバウンスメールを送信元に送信しない

Google Workspace

エンベロープ受信者

エンベロープ受信者を変更する

キャンセル 保存

18. 下にスクロールし、「オプションを表示」をクリックします。

設定を追加

このメッセージには迷惑メールフィルタを適用しない

添付ファイル

メッセージから添付ファイルを削除

その他の配信先

受信者を追加

暗号化（配信時のみ）

セキュアなトランスポート（TLS）を使用

オプションを表示

キャンセル 保存

19. 以下のとおりに設定し、「保存」をクリックします。

項目	設定値
ユーザー	■
グループ	■

設定を追加

オプションを表示しない

A. アドレスリスト

アドレスリストを使用して、この設定を適用するアプリケーションを除外、制御する

アドレスリストを該当するユーザーに適用する ▼

特定のアドレスまたはドメインにはこの設定を適用しない

特定のアドレスまたはドメインにのみ、この設定を適用する

B. 影響を受けるアカウントの種類

ユーザー

グループ

認識できない、キャッチオール

キャンセル 保存

20. 追加されていることを確認します。

アプリ > Google Workspace > Gmail の設定 > ルーティング

Gmail

ステータス
オン (すべてのユーザー)

組織部門

組織部門の検索

ルーティング

説明	ステータス	ソース
GUARDIANWALL Mailセキュリティ・クラウド	有効	ローカルに適用
Google Workspace	有効	ローカルに適用

別のルールを追加

i すべてのユーザーに変更が反映されるまでに、最長で 24 時間かかることがあります。
[監査ログ](#)で以前の変更を確認できます

以上で、Google Workspaceの設定は終了です。

2.2.4 Google Workspace のみ利用している場合（一部のユーザーで利用）

一部のユーザーのGoogle Workspaceから送信されるメールをMailセキュリティ・クラウド経由とするため、以下手順を実施ください。

1 ルートの設定

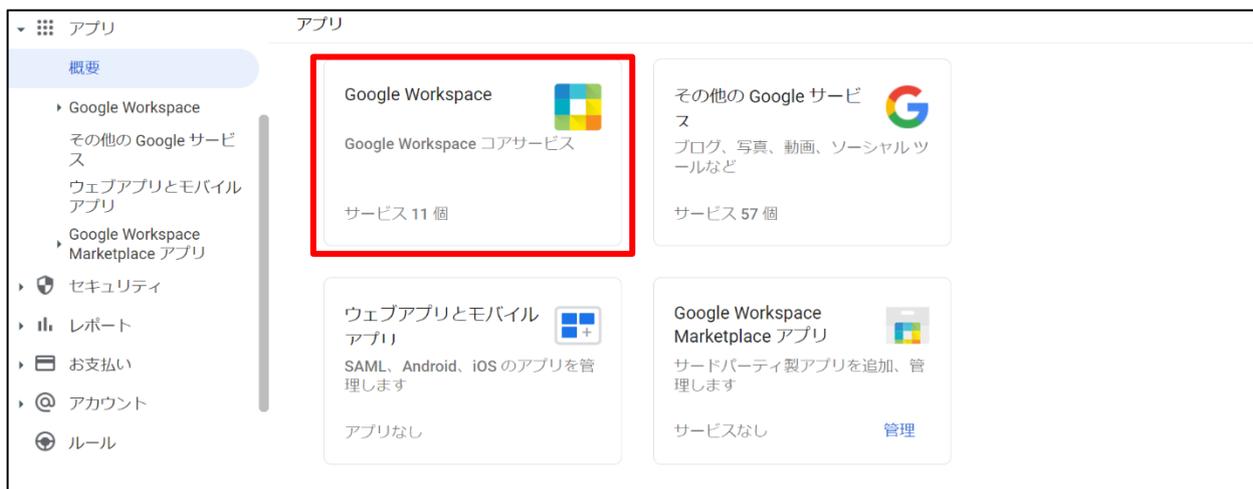
Mailセキュリティ・クラウドの環境に接続するためのルートを設定します。

※本手順では「サービス登録完了書」を参照する項目がございます。

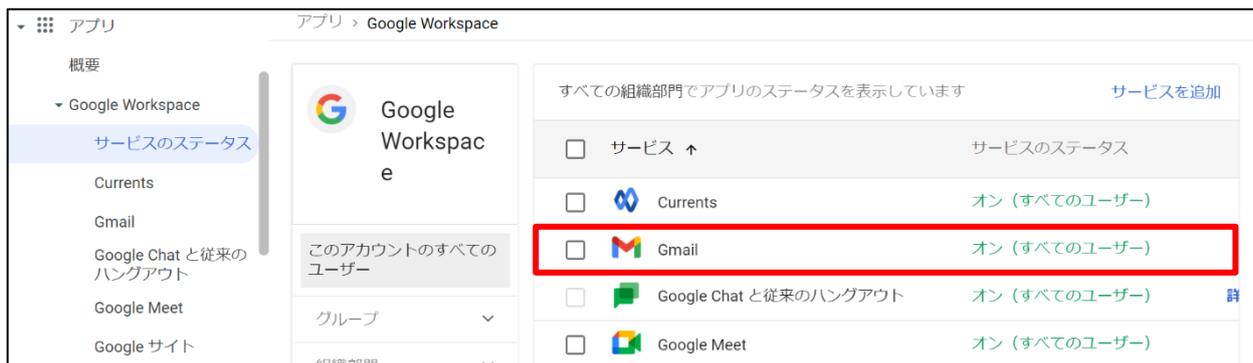
1. Google Workspace に管理者権限でログインし、管理コンソールを開き、「アプリ」をクリックします。



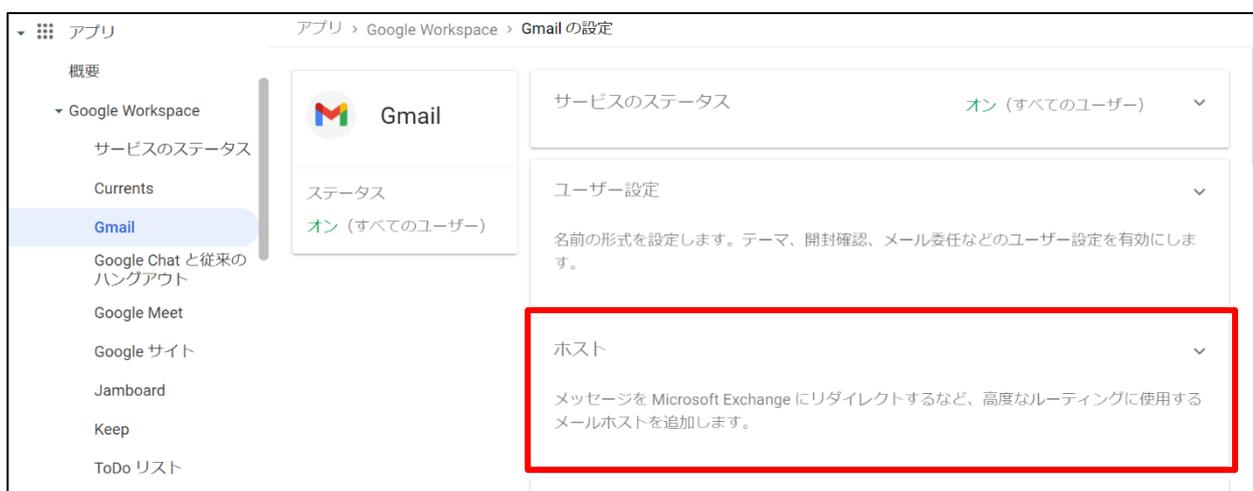
2. 「アプリ」の画面に移行後、「Google Workspace」をクリックします。



3. 「Google Workspace」(Google Apps)の画面に移行後、「Gmail」をクリックします。



4. 「Gmail の設定」の画面に移行後、「ホスト」をクリックします。



5. 「ホスト」画面にて、「ルートを追加」をクリックします。



6. 以下のとおりに設定し、「保存」をクリックします。

項目	設定値
名前	GUARDIANWALL Mail セキュリティ・クラウド
ホスト	単一のホスト
ホスト名または IP を入力	サービス登録完了書に記載された「リレー先ホスト名」 ポート : 25
メールの送受信時にセキュリティ プロトコルで保護された (TLS) 接続を必須とする (推奨)	■

メールのルートを追加

名前
詳細

GUARDIANWALL Mailセキュリティ

このフィールドは必須です。

1. メールサーバーの指定

番号が 25、587、1024~65535 のポートのみ使用できます。

単一のホスト ▼

xxxxxxxxx.guardianw : 25

2. オプション

ホストで MX ルックアップを実行する

メールを送受信時にセキュリティ プロトコルで保護された (TLS) 接続を必須とする (推奨)

CA の署名付き証明書を必須とする (推奨)

証明書のホスト名を検証する (推奨)

TLS 接続をテスト

キャンセル
保存

7. 社内間のメールについては、Google Workspace の MX レコード先へ送信されるように設定します。

「ルートを追加」をクリックします。



8. 以下のとおりに設定し、「保存」をクリックします。

項目	設定値
名前	Google Workspace
ホスト	単一のホスト
ホスト名または IP を入力	ホスト名 : smtp.google.com ポート : 25
メールの送受信時にセキュリティ プロトコルで保護された (TLS) 接続を必須とする (推奨)	■

メールのルートを追加

名前 詳細

Google Workspace

このフィールドは必須です。

1. メールサーバーの指定

番号が 25、587、1024~65535 のポートのみ使用できます。

単一のホスト ▼

smtp.google.com : 25

2. オプション

ホストで MX ルックアップを実行する

メール送受信時にセキュリティ プロトコルで保護された (TLS) 接続を必須とする (推奨)

CA の署名付き証明書を必須とする (推奨)

証明書のホスト名を検証する (推奨)

[TLS 接続をテスト](#)

キャンセル 保存

以上で、ルートの設定は終了です。メールリレールール設定に進みます。

2 メールリレールールの設定

設定したルートを利用して、メールをリレーするためのルールを設定します。

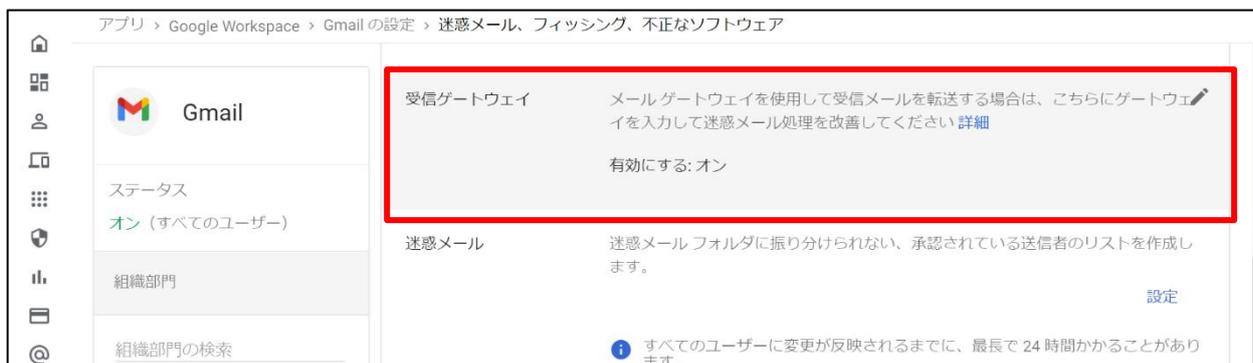
1. 「Gmail の設定」をクリックします。



2. 「Gmail の設定」画面に移動後、画面を下にスクロールし、「迷惑メール、フィッシング、不正なソフトウェア」をクリックします。



3. 「迷惑メール、フィッシング、不正なソフトウェア」の画面にて、画面を下にスクロールし、「受信ゲートウェイ」をクリックします。



4. 「有効にする」にチェックを入れ、「追加」をクリックします。

受信ゲートウェイ メールゲートウェイを使用して受信メールを転送する場合は、こちらにゲートウェイを入力して迷惑メール処理を改善してください [詳細](#)

有効にする

1. ゲートウェイの IP

IP アドレスまたは IP 範囲

IP アドレスがまだ追加されていません。 [追加](#)

[追加](#)

外部 IP を自動検出する (推奨)

ゲートウェイの IP から届いたものではないメールはすべて拒否する

上で指定したメールゲートウェイからの接続には TLS を必須とする

2. メールのタグ付け

以下のヘッダーの正規表現と一致するメールを迷惑メールとみなす

i すべてのユーザーに変更が反映されるまでに、最長で 24 時間かかることがあります。
[監査ログ](#)で以前の変更を確認できます

キャンセル 保存

5. サービス登録完了書に記載されたすべての「受信ゲートウェイ IP」を入力し、「保存」をクリックします。

IP アドレスの設定は、1 つずつ行い、すべての「受信ゲートウェイ IP」を入力し終わるまで、繰り返します。

IP アドレスまたは IP 範囲の追加

IP アドレスまたは IP 範囲を入力

1.1.1.2

キャンセル [保存](#)

6. すべての IP アドレスを追加後、「保存」をクリックします。

受信ゲートウェイ メールゲートウェイを使用して受信メールを転送する場合は、こちらにゲートウェイを入力して迷惑メール処理を改善してください [詳細](#)

有効にする

1. ゲートウェイの IP

IP アドレスまたは IP 範囲
1.1.1.2

[追加](#)

外部 IP を自動検出する (推奨)

ゲートウェイの IP から届いたものではないメールはすべて拒否する

上で指定したメールゲートウェイからの接続には TLS を必須とする

2. メールのタグ付け

以下のヘッダーの正規表現と一致するメールを迷惑メールとみなす

i すべてのユーザーに変更が反映されるまでに、最長で 24 時間かかることがあります。
[監査ログ](#)で以前の変更を確認できます

未保存の変更が 1 件あります [キャンセル](#) 保存

7. 「Gmail の設定」をクリックします。

アプリ > Google Workspace Gmail の設定 迷惑メール、フィッシング、不正なソフトウェア

Gmail

ステータス

オン (すべてのユーザー)

組織部門

組織部門の検索

受信ゲートウェイ メールゲートウェイを使用して受信メールを転送する場合は、こちらにゲートウェイを入力して迷惑メール処理を改善してください [詳細](#)

有効にする: オン

迷惑メール [設定](#)

迷惑メールフォルダに振り分けられない、承認されている送信者のリストを作成します。

i すべてのユーザーに変更が反映されるまでに、最長で 24 時間かかることがあります。
[監査ログ](#)で以前の変更を確認できます

8. 「Gmail の設定」画面に移動後、画面を下にスクロールし、「ルーティング」をクリックします。



9. 「ルーティング」の画面にて、「送信ゲートウェイ」が空欄となっているか確認してください。



10. 「ルーティング」の「設定」をクリックします。



11. 名前を設定し、「送信」を選択します。

項目	設定値
名前	GUARDIANWALL Mail セキュリティ・クラウド

設定を追加

ルーティング [詳細](#)

GUARDIANWALL Mailセキュリティ・クラウド

1. 影響を受けるメール

- 受信
- 送信
- 内部 - 送信
- 内部 - 受信

2. 上記の種類メッセージに対し、次の処理を行う

メッセージを変更 ▼

ヘッダー

[キャンセル](#) [保存](#)

12. 「ルートを変更」を選択し、[1 ルートの設定]の手順 6 にて設定したルートを選択します。

設定を追加

件名

件名の先頭に追加するカスタムテキスト

ルート

ルートを変更

迷惑メールのルートも変更する

この受信者からのバウンスメールを送信元に送信しない

GUARDIANWALL Mailセキュリティ・クラウド

エンベロープ受信者

エンベロープ受信者を変更する

キャンセル 保存

13. 下にスクロールし、「オプションを表示」をクリックします。

設定を追加

このメッセージには迷惑メールフィルタを適用しない

添付ファイル

メッセージから添付ファイルを削除

その他の配信先

受信者を追加

暗号化（配信時のみ）

セキュアなトランスポート（TLS）を使用

オプションを表示

キャンセル 保存

14. 以下のとおりに設定します。

項目	設定値
ユーザー	■
グループ	■

設定を追加

オプションを表示しない

A. アドレスリスト

アドレスリストを使用して、この設定を適用するアプリケーションを除外、制御する

アドレスリストを該当するユーザーに適用する ▼

特定のアドレスまたはドメインにはこの設定を適用しない

特定のアドレスまたはドメインにのみ、この設定を適用する

B. 影響を受けるアカウントの種類

ユーザー

グループ

認識できない、キャッチオール

キャンセル 保存

15. 「特定のエンベロープ送信者にのみ適用する」 - 「パターン一致」を選択し、「正規表現」に「Mail セキュリティ・クラウドを利用するメールアドレス」を登録します。入力後、「保存」をクリックします。

※user01@example.co.jp、user02@example.co.jp、user03@example.co.jp、grouptest@example.co.jp
(グループアドレス) を Mail セキュリティ・クラウドにリレーしたい場合は、
「(¥W|^)(user01|user02|user03|grouptest+.*)@example.co.jp(¥W|\$)」と入力します。

設定を追加

認識できない、キャッチオール

c. エンベロープフィルタ

特定のエンベロープ送信者にのみ適用する

パターン一致

正規表現 [詳細](#)

(¥W|^)(user01|user02|user03|grouptest+.*)@example.co.jp(¥W|\$)

[表現をテスト](#)

特定のエンベロープ受信者にのみ適用する

キャンセル **保存**

16. ルールが追加されていることを確認します。

社内間のメールをリレーするルールを設定するため、「別のルールを追加」をクリックします。

アプリ > Google Workspace > Gmail の設定 > ルーティング

次の組織部門のユーザー設定を表示しています: 全ユーザー

ルーティング

送信ゲートウェイ [詳細](#)
「全ユーザー」で適用しました
送信メールを次の SMTP サーバーに転送します:

説明	ステータス	ソース
GUARDIANWALL Mailセキュリティ・クラウド	有効	ローカルに適用

[別のルールを追加](#)

すべてのユーザーに変更が反映されるまでに、最長で 24 時間かかることがあります。

17. 名前を設定し、「内部-送信」を選択します。

項目	設定値
名前	Google Workspace

設定を追加

ルーティング [詳細](#)

Google Workspace

1. 影響を受けるメール

- 受信
- 送信
- 内部-送信
- 内部-受信

2. 上記の種類メッセージに対し、次の処理を行う

メッセージを変更 ▼

ヘッダー

キャンセル [保存](#)

18. 「ルートを変更」を選択し、[1 ルートの設定]の手順 8 にて設定したルートを選択します。

設定を追加

件名

件名の先頭に追加するカスタム テキスト

ルート

ルートを変更

迷惑メールのルートも変更する

この受信者からのバウンスメールを送信元に送信しない

Google Workspace

エンベロープ受信者

エンベロープ受信者を変更する

キャンセル 保存

19. 下にスクロールし、「オプションを表示」をクリックします。

設定を追加

このメッセージには迷惑メールフィルタを適用しない

添付ファイル

メッセージから添付ファイルを削除

その他の配信先

受信者を追加

暗号化 (配信時のみ)

セキュアなトランスポート (TLS) を使用

オプションを表示

キャンセル 保存

20. 以下のとおりに設定します。

項目	設定値
ユーザー	■
グループ	■

設定を追加

オプションを表示しない

A. アドレスリスト

アドレスリストを使用して、この設定を適用するアプリケーションを除外、制御する

アドレスリストを該当するユーザーに適用する ▼

特定のアドレスまたはドメインにはこの設定を適用しない

特定のアドレスまたはドメインにのみ、この設定を適用する

B. 影響を受けるアカウントの種類

ユーザー

グループ

認識できない、キャッチオール

キャンセル 保存

21. 「特定のエンベロープ送信者にのみ適用する」 - 「パターン一致」を選択し、「正規表現」に手順 15 で設定したメールアドレスを登録します。入力後、「保存」をクリックします。

※user01@example.co.jp、user02@example.co.jp、user03@example.co.jp、grouptest@example.co.jp
(グループアドレス) を Mail セキュリティ・クラウドにリレーしたい場合は、
「(¥W|^)(user01|user02|user03|grouptest+.*)@example.co.jp(¥W|\$)」と入力します。

設定を追加

認識できない、キャッチオール

C. エンベロープフィルタ

特定のエンベロープ送信者にのみ適用する

パターン一致

正規表現 [詳細](#)

(¥W|^)(user01|user02|user03|grouptest+.*)@example.co.jp(¥W|\$)

[表現をテスト](#)

特定のエンベロープ受信者にのみ適用する

キャンセル **保存**

22. 追加されていることを確認します。

アプリ > Google Workspace > Gmail の設定 > ルーティング

ルーティング

説明	ステータス	ソース
GUARDIANWALL Mailセキュリティ・クラウド	有効	ローカルに適用
Google Workspace	有効	ローカルに適用

[別のルールを追加](#)

i すべてのユーザーに変更が反映されるまでに、最長で 24 時間かかることがあります。
[監査ログ](#)で以前の変更を確認できます

以上で、Google Workspaceの設定は終了です。

3. Mail セキュリティ・クラウドへの初回ログインおよびメール疎通確認

Mailセキュリティ・クラウドをご利用いただくにあたり、管理者アカウントのパスワード変更とメール疎通確認を実施ください。

3.1 初回ログイン・パスワード変更手順

初回ログイン時にパスワードを変更します。

※本手順では、「サービス登録完了書」を参照する項目がございます。

1. Web ブラウザより管理画面へ接続します。

下記 URL を Web ブラウザのアドレス欄に入力し、管理画面へアクセスします。

項目	値
URL	サービス登録完了書に記載された管理画面 URL

2. ログイン画面が表示されるので、以下の情報を入力し、「ログイン」をクリックします。

項目	値
アカウント	サービス登録完了書に記載されたアカウント
パスワード	サービス登録完了書に記載されたパスワード



3. 「パスワードの有効期限が過ぎました。」と表示されます。

現パスワードに上記手順 2 で入力したパスワードを再度入力、新パスワードに 8 文字以上の任意の新しいパスワードを入力し、「更新」をクリックします。

The screenshot shows a web form titled "パスワード変更" (Change Password). Below the title, there is a sub-header "パスワード変更" and a red error message: "パスワードの有効期限が過ぎました。" (Your password's validity period has expired). The form contains three input fields: "現パスワード" (Current Password), "新パスワード" (New Password), and "新パスワード (再入力)" (New Password (Re-enter)). Each field contains a series of black dots representing masked characters. A red rectangular box highlights the three input fields. At the bottom left, there is a button with a green checkmark and the text "更新" (Update), which is also highlighted with a red rectangular box.

4. 「更新」をクリックします。

The screenshot shows the same "パスワード変更" (Change Password) form. Below the sub-header, there is a confirmation question: "tenant@example.co.jp のパスワードを変更しますか?" (Do you want to change the password for tenant@example.co.jp?). Below the question, there are two buttons: "更新" (Update) with a green checkmark and "キャンセル" (Cancel) with a red X. The "更新" button is highlighted with a red rectangular box.

5. 「パスワードを変更しました。」と表示されます。

The screenshot shows the "パスワード変更" (Change Password) form. A blue success message "パスワードを変更しました。" (Your password has been changed.) is displayed at the top, highlighted with a red rectangular box. Below the message, there are three empty input fields: "現パスワード", "新パスワード", and "新パスワード (再入力)". At the bottom left, there is a button with a green checkmark and the text "更新" (Update).

以上で、パスワードの変更は完了です。

3.2 メール疎通確認

メールの送受信が行われた後に、管理画面上の「メールログ」に該当のメールがあるか確認し、メール送受信が GUARDIANWALL を経由していることをご確認ください。

1. メール送受信ができていることを確認します。以下のメールを送信します。

ご利用いただくサービスごとに、確認内容が異なります。

また、ご利用サービス①と②の両方をご利用いただく場合は、①と②の両方をご確認ください。

●ご利用サービス①

- MailFilter on Cloud [送信メール]
- MailConvert on Cloud
- MailArchive on Cloud [送信メール]

内部ドメインから外部ドメイン宛てのメールを送信

●ご利用サービス②

- MailFilter on Cloud [受信メール]
- MailArchive on Cloud [受信メール]

外部ドメインから内部ドメイン宛てのメールを送信

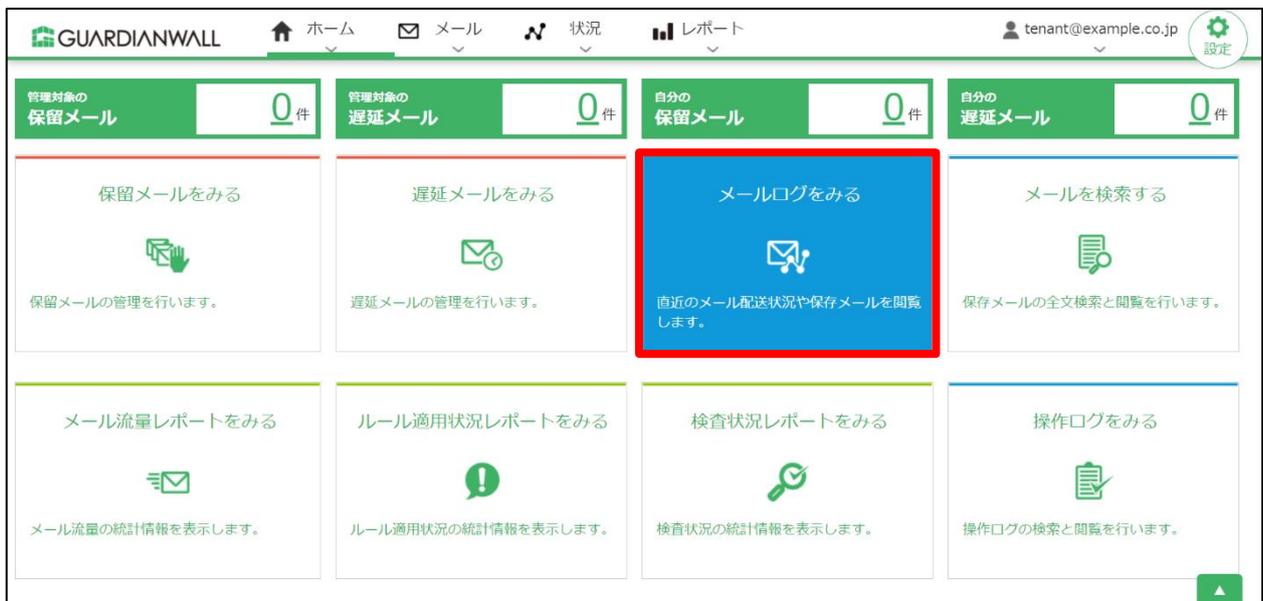
2. Web ブラウザより管理画面へ接続します。以下の情報を入力し、「ログイン」をクリックします。

項目	値
URL	サービス登録完了書に記載された管理画面 URL
アカウント	サービス登録完了書に記載されたアカウント
パスワード	初回ログイン後、更新したパスワード



3. 「メールログをみる」をクリックします。

※ご利用サービスによって、表示されているメニューの種類が異なります。



4. メールログ閲覧画面に移行後、画面下部の「検索」をクリックします。



5. 送信したメールのログが表示されます。手順1で送信したメールが表示されることを確認してください。

表示されない場合、その他予期せぬ動作を確認された場合は、サポート窓口までご連絡ください。



以上で、メールの疎通確認は完了です。

4. ジャーナルアーカイブ設定

Mailセキュリティ・クラウドでMailArchive on Cloudの機能の一つである、ジャーナルアーカイブ機能をご利用いただくためには、Microsoft 365とMailセキュリティ・クラウドの設定を変更する必要があります。

また、ジャーナルアーカイブ機能をご利用いただけるサービスは以下のとおりです。

- ご利用サービス

- MailArchive on Cloud [ジャーナルメール]



本設定を行う際、配信不能レポートを受け取るためのメールアドレスをお客様にてご用意いただく必要があります。

本メールアドレスで送受信したメールについてはジャーナルレポートが送信されず、本サービスにおいてアーカイブの対象外となるため、システムメールでご利用されているメールアドレス等をご用意ください。

※配信不能レポートは、Mail セキュリティ・クラウドにジャーナルメールを送信できなかった場合に送信される通知メールです。

4.1 Microsoft 365 の設定変更

Microsoft 365から送信されるジャーナルメールをMailセキュリティ・クラウドへ送信するため、以下手順を実施ください。

本章の設定では、以下のメールが対象になります。

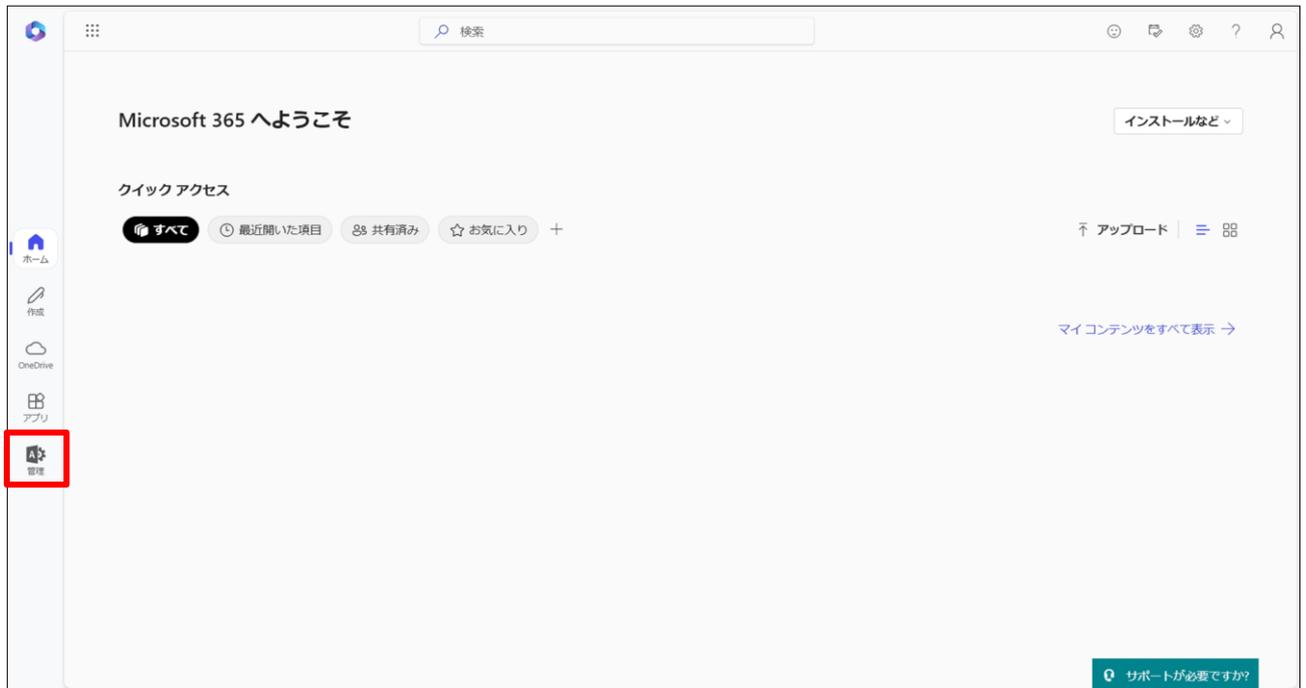
- ・社外との送受信メール
- ・社内間の送受信メール

※本手順では「サービス登録完了書」を参照する項目がございます。

4.1.1 配信できないジャーナルレポートの送信先の設定

Mailセキュリティ・クラウドにジャーナルメールを送信できなかった場合、配信不能レポートという通知が送信されます。本項では、配信不能レポートの送信先を設定します。

1. Microsoft 365 に管理者権限でログインし、「管理」をクリックします。



- 「Microsoft 365 管理センター」の画面に移行後、左側の「≡」をクリックし、「すべてを表示」をクリックします。



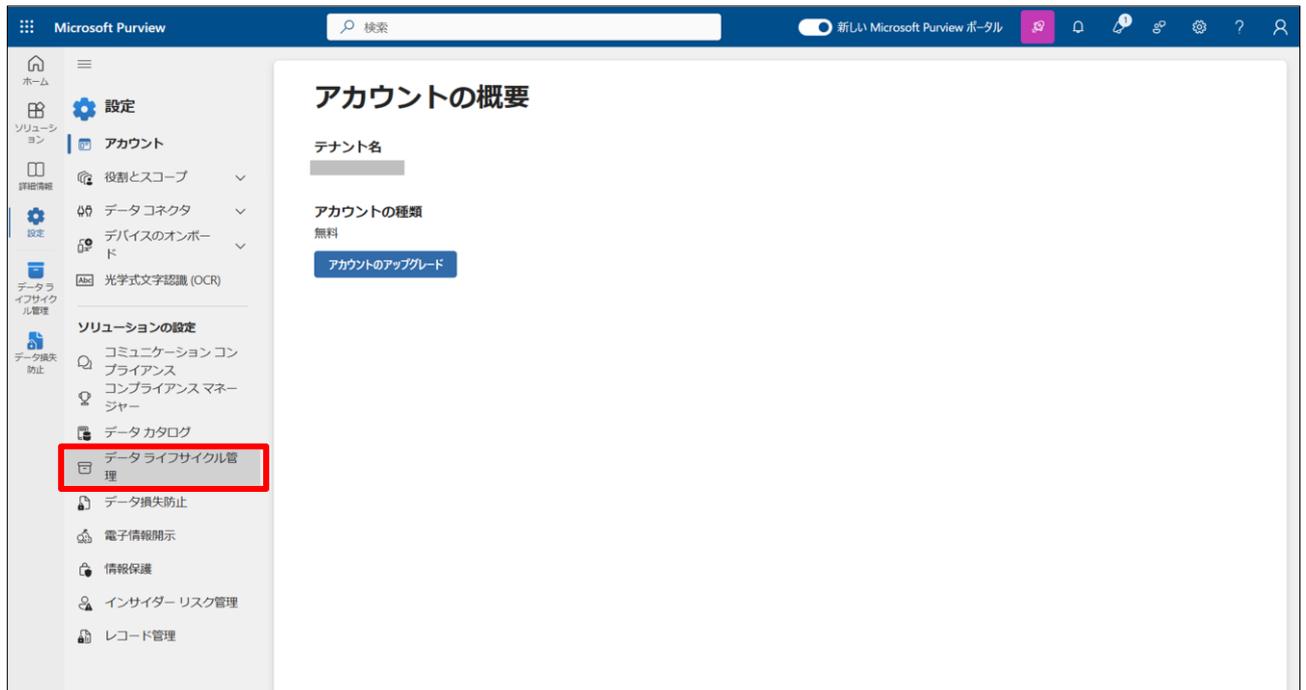
- 「コンプライアンス」をクリックします。



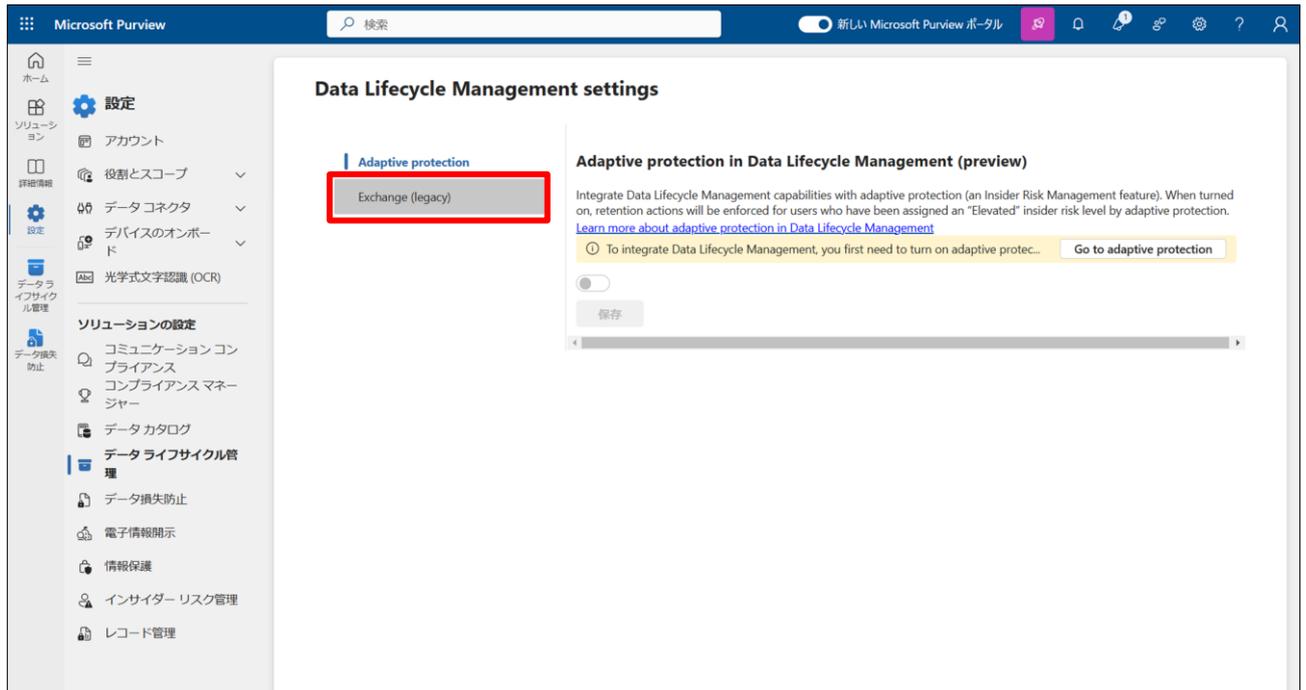
4. 「Microsoft Purview」の画面に移行後、「設定」をクリックします。



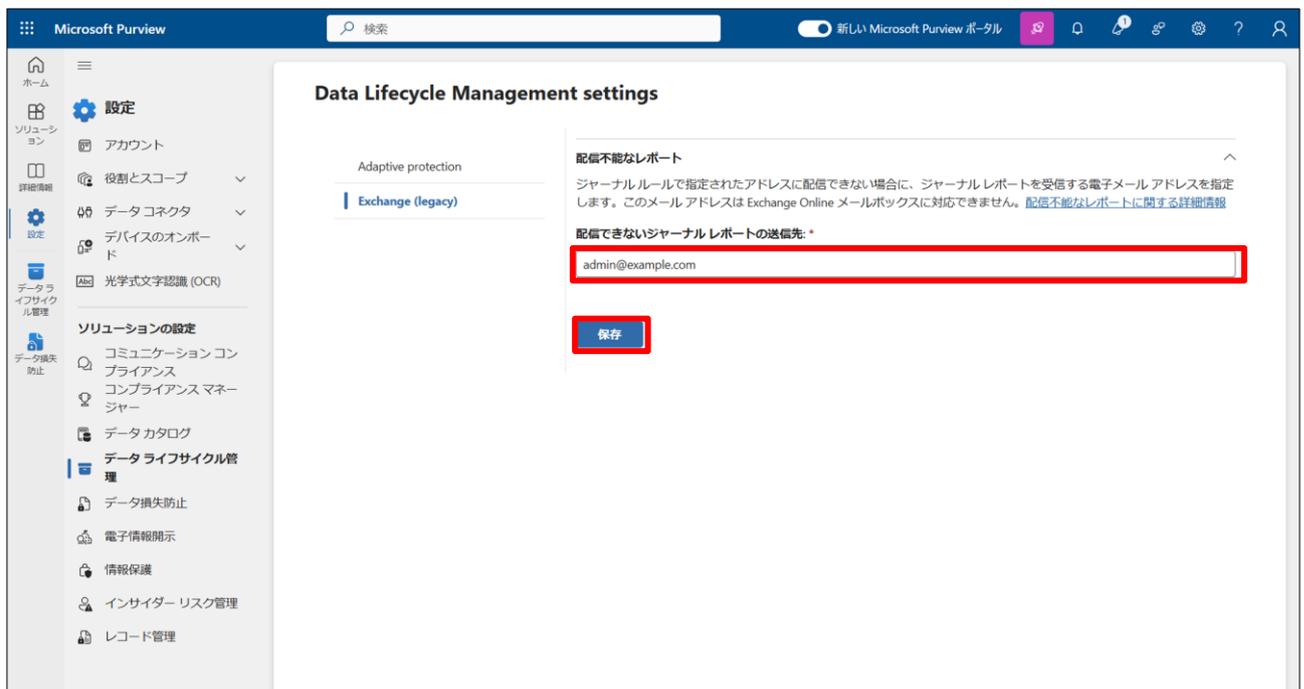
5. 「データライフサイクル管理」をクリックします。



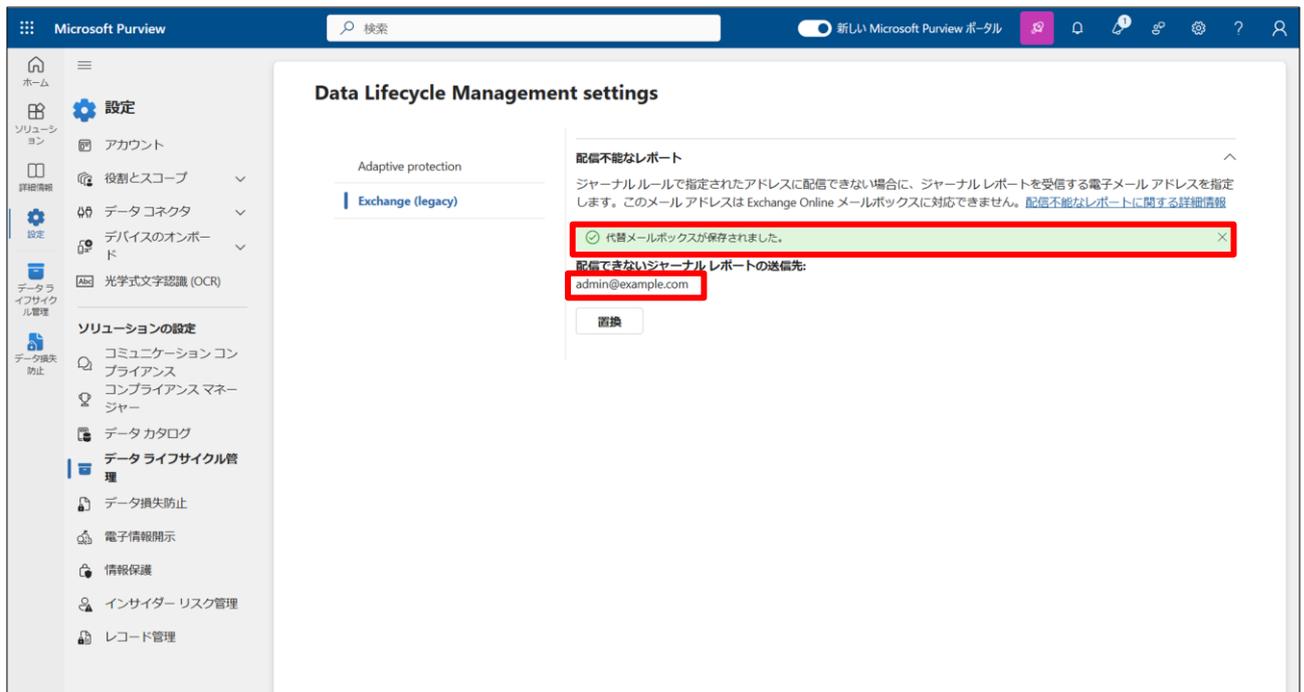
6. 「Exchange (legacy)」をクリックします。



7. 「配信できないジャーナルレポートの送信先」に、本来のジャーナルメールの送信先がジャーナルメールを受信できない場合、配信不能レポートを受信する「お客様メールアドレス」を入力し「保存」ボタンをクリックします。
 ※この項目で設定したメールアドレスはジャーナルアーカイブの対象外になりますのでご注意ください。



8. 「代替メールボックスが保存されました。」と表示され、「配信できないジャーナルレポートの送信先」にメールアドレスが設定されていることを確認します。

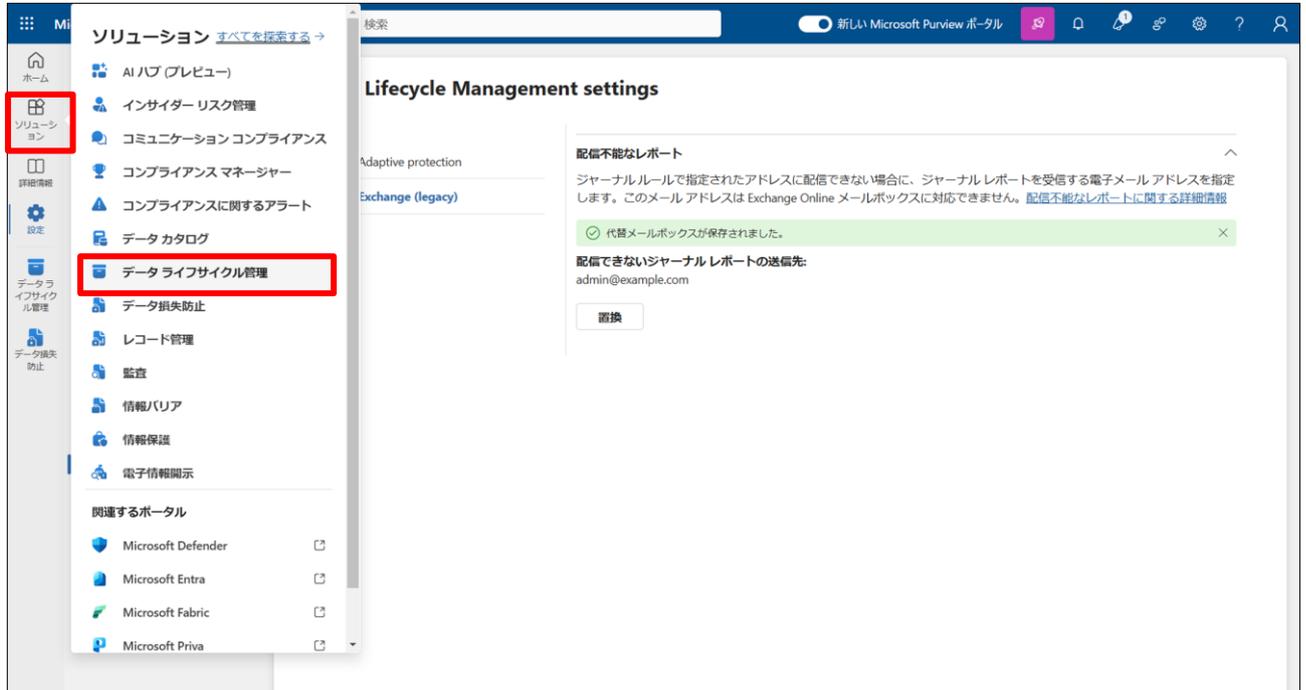


以上で、配信できないジャーナルレポートの送信先の設定は終了です。ジャーナルルールの設定に進みます。

4.1.2 ジャーナルルールの設定

ジャーナルメールをMailセキュリティ・クラウドに送信するためのルールを設定します。

1. 左側のタブの「ソリューション」をクリックし、「データライフサイクル管理」をクリックします。



2. 「Exchange (従来版)」をクリックし、「ジャーナルルール」をクリックします。



3. 「+新しいルール」をクリックします。



4. 以下のとおりに設定し、「次へ」ボタンをクリックします。

項目	設定値
ジャーナルレポートの送信先	サービス登録完了書に記載されたジャーナルレポートの送信先
ジャーナルルール名	journal
ジャーナルメッセージの送信元または受信元	すべてのユーザー
ジャーナルするメッセージの種類	すべてのメッセージ



5. 「送信」ボタンをクリックします。



6. 「ジャーナルルールが作成されました」という画面が表示されたら、「完了」ボタンをクリックします。



7. ジャーナルルールの画面に設定したルールが追加され、「状態」が「オン」になっていることを確認します。



以上で、ジャーナルルールの設定は終了です。

4.2 Mailセキュリティ・クラウドの設定変更

Microsoft 365から送信されるジャーナルメールをMailセキュリティ・クラウドでジャーナルメールをアーカイブするため、以下の手順を実施ください。

※本手順では「サービス登録完了書」を参照する項目がございます。

4.2.1 MailArchive on Cloud [ジャーナルメール] + MailFilter on Cloud をご利用の場合

MailArchive on Cloud [ジャーナルメール]の他に、MailFilter on Cloudをご利用の場合は、本手順を実施ください。

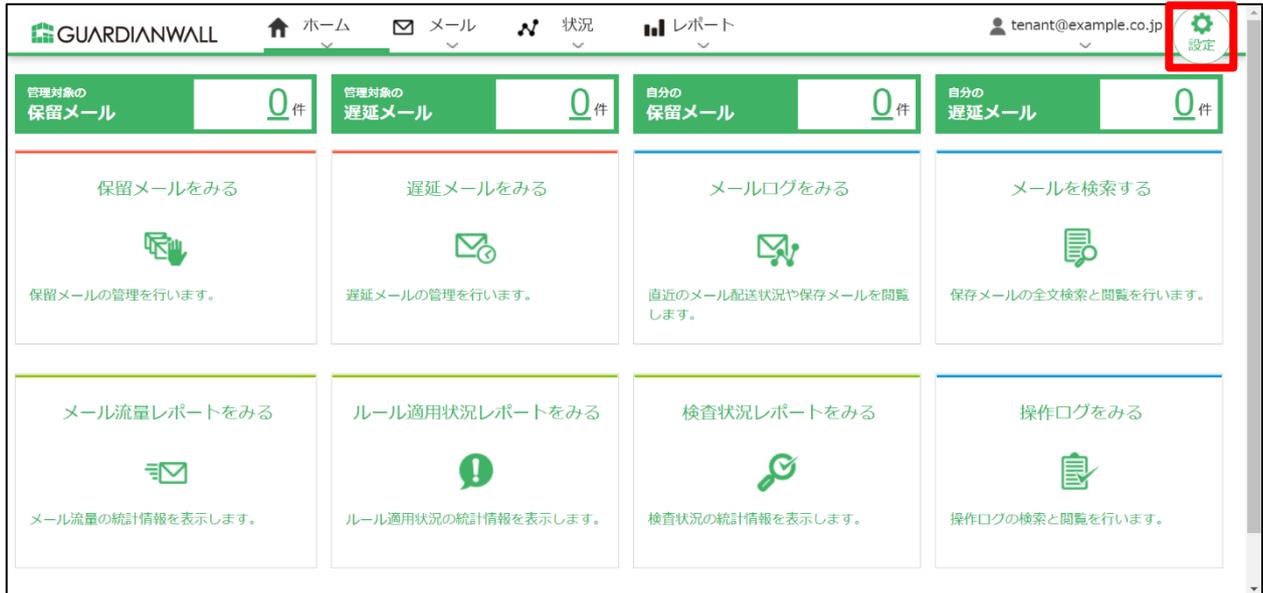
※本手順の設定を行うことで、通常のメールとジャーナルメールとの二重アーカイブを回避することができます。

1. Web ブラウザより管理画面へ接続します。以下の情報を入力し、「ログイン」をクリックします。

項目	値
URL	サービス登録完了書に記載された管理画面 URL
アカウント	サービス登録完了書に記載されたアカウント
パスワード	初回ログイン後、更新したパスワード



2. 管理画面右上の「設定」をクリックします。



3. 「システム設定」 - 「メール保存機能設定」をクリックします。



4. 「ジャーナルアーカイブ機能」の「オン」を選択します。



5. 「メール保存設定」を以下のとおりに設定し、「更新」をクリックします。

項目	値
保存対象	内部から内部へのメール： ■ 外部から外部へのメール： ■
保存対象外メール受信時の対応コード	成功コード(250)

GUARDIANWALL

ルール管理 | ルール編集 | アカウント管理 | システム設定 | 人事情報連携

tenant@example.co.jp

基本設定

情報検査機能設定

メール保存機能設定

スケジューラサービス

ジャーナルアーカイブ

○ フィルタリングルールで指定されたメールのみ保存する

ジャーナルアーカイブ機能 (※1) ○ オフ ● オン

メール保存設定

保存対象

内部から内部へのメール

内部から外部へのメール

外部から内部へのメール

外部から外部へのメール

宛先が分割された重複メールを保存しない (※2)

保存対象外メール受信時の対応コード

エラーコード(554) ● 成功コード(250)

タイムゾーン

リッチテキスト形式メールのテキスト変換

●変換しない ○変換する

(※1) オンの場合、ジャーナルメールはルール適用対象外となりアーカイブ処理のみ実施されます。

(※2) 宛先に内部と外部が含まれたメールの場合、[内部から内部]と[内部から外部]への2通のジャーナルメールが発生します。その重複保存を防ぎます。

更新

6. 「OK」をクリックします。

Web ページからのメッセージ

?

入力された内容でメール保存機能設定を更新してもよろしいですか？

OK キャンセル

7. 画面上部に「メール保存機能設定を変更しました。」と表示されることを確認します。

The screenshot shows the GuardianWall management interface. The top navigation bar includes 'ルール管理', 'ルール編集', 'アカウント管理', 'システム設定', and '人事情報連携'. The user is logged in as 'tenant@example.co.jp'. The left sidebar has '基本設定', '情報検査機能設定', 'メール保存機能設定', and 'スケジューラーサービス'. The main content area is titled 'メール保存機能設定' and displays a confirmation message 'メール保存機能設定を変更しました。' in a red box. Below this, there are sections for '保存対象' (Save targets) and 'ジャーナルアーカイブ' (Journal archiving).

保存対象	
<input checked="" type="radio"/>	全メール保存
<input type="radio"/>	内部から発信されるメールのみ保存
<input type="radio"/>	外部から受信したメールのみ保存
<input type="radio"/>	フィルタリングルールで指定されたメールのみ保存する

ジャーナルアーカイブ機能 (※1)	
<input type="radio"/> オフ <input checked="" type="radio"/> オン	
メール保存設定	保存対象
	<input checked="" type="checkbox"/> 内部から内部へのメール <input type="checkbox"/> 内部から外部へのメール <input type="checkbox"/> 外部から内部へのメール <input checked="" type="checkbox"/> 外部から外部へのメール
<input type="checkbox"/> 宛先が分割された重複メールを保存しない (※2)	

以上で、MailFilter on Cloudをご利用の場合の、ジャーナルアーカイブ機能設定は終了です。

4.2.2 MailArchive on Cloud [ジャーナルメール] + MailConvert on Cloud のみをご利用の場合

MailArchive on Cloud [ジャーナルメール]の他に、MailConvert on Cloudのみをご利用の場合は、本手順を実施ください。

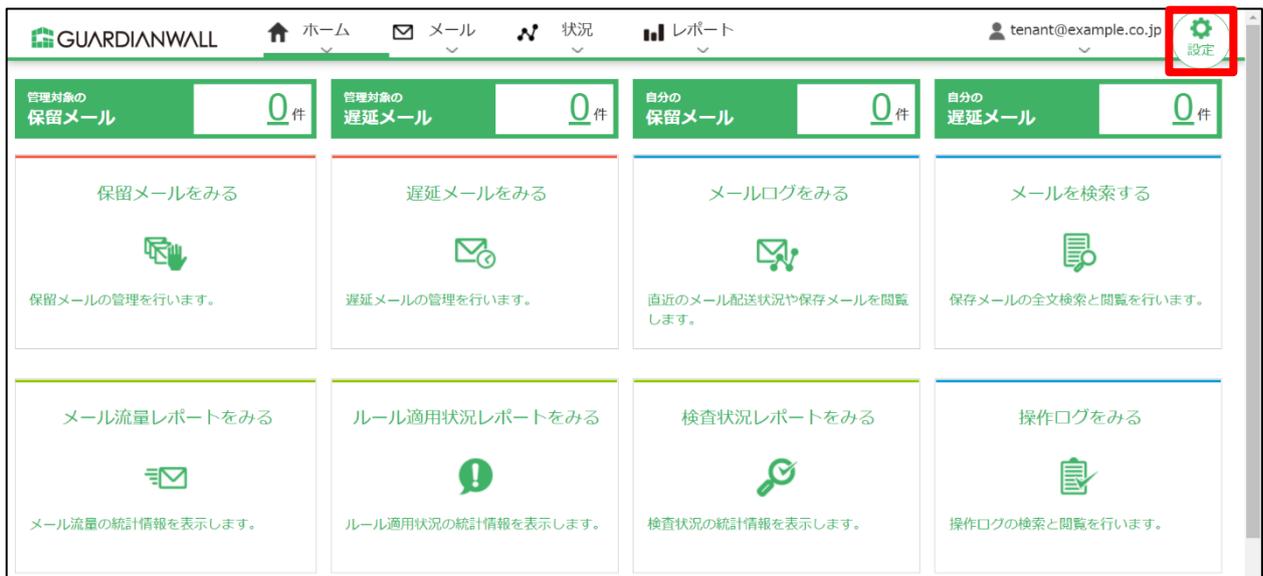
※本手順の設定を行うことで、通常のメールとジャーナルメールとの二重アーカイブを回避することができます。

1. Web ブラウザより管理画面へ接続します。以下の情報を入力し、「ログイン」をクリックします。

項目	値
URL	サービス登録完了書に記載された管理画面 URL
アカウント	サービス登録完了書に記載されたアカウント
パスワード	初回ログイン後、更新したパスワード



2. 管理画面右上の「設定」をクリックします。



3. 「システム設定」 - 「メール保存機能設定」をクリックします。



4. 「ジャーナルアーカイブ機能」の「オン」を選択します。



5. 「メール保存設定」を以下のとおりに設定し、「更新」をクリックします。

項目	値
保存対象	内部から内部へのメール： ■ 外部から内部へのメール： ■ 外部から外部へのメール： ■
保存対象外メール受信時の対応コード	成功コード(250)

GUARDIANWALL

ルール管理 ルール編集 アカウント管理 システム設定 人事情報連携

tenant@example.co.jp 操作

基本設定

情報検査機能設定

メール保存機能設定

スケジューラーサービス

フィルタリングルールで指定されたメールのみ保存する

ジャーナルアーカイブ

ジャーナルアーカイブ機能 (※1) オフ オン

メール保存設定

保存対象

内部から内部へのメール

内部から外部へのメール

外部から内部へのメール

外部から外部へのメール

宛先が分割された重複メールを保存しない (※2)

保存対象外メール受信時の対応コード

エラーコード(554) 成功コード(250)

タイムゾーン

リッチテキスト形式メールのテキスト変換

変換しない 変換する

(※1) オンの場合、ジャーナルメールはルール適用対象外となりアーカイブ処理のみ実施されます。

(※2) 宛先に内部と外部が含まれたメールの場合、[内部から内部]と[内部から外部]への2通のジャーナルメールが発生します。その重複保存を防ぎます。

更新

6. 「OK」をクリックします。

Web ページからのメッセージ

?

入力された内容でメール保存機能設定を更新してもよろしいですか？

OK キャンセル

7. 画面上部に「メール保存機能設定を変更しました。」と表示されることを確認します。

The screenshot shows the GuardianWall management interface. The top navigation bar includes 'ルール管理', 'ルール編集', 'アカウント管理', 'システム設定', and '人事情報連携'. The user is logged in as 'tenant@example.co.jp'. The left sidebar shows the navigation menu with 'メール保存機能設定' selected. The main content area is titled 'メール保存機能設定' and displays a confirmation message 'メール保存機能設定を変更しました。' in a red box. Below this, there are sections for '保存対象' (Save Target) and 'ジャーナルアーカイブ' (Journal Archiving). The '保存対象' section has four radio button options, with '全メール保存' (Save all mail) selected. The 'ジャーナルアーカイブ' section has a table with settings for 'ジャーナルアーカイブ機能' and 'メール保存設定'.

ジャーナルアーカイブ機能 (※1)		メール保存設定	
<input type="radio"/> オフ <input checked="" type="radio"/> オン			
<input checked="" type="checkbox"/> 内部から内部へのメール	<input type="checkbox"/> 内部から外部へのメール	<input type="checkbox"/> 宛先が分割された重複メールを保存しない (※2)	
<input checked="" type="checkbox"/> 外部から内部へのメール	<input checked="" type="checkbox"/> 外部から外部へのメール		

以上で、MailConvert on Cloudをご利用の場合の、ジャーナルアーカイブ機能設定は終了です。

4.2.3 MailArchive on Cloud [ジャーナルメール] のみをご利用の場合

MailArchive on Cloud [ジャーナルメール]のみをご利用のお客様は、本手順を実施ください。

1. Web ブラウザより管理画面へ接続します。以下の情報を入力し、「ログイン」をクリックします

項目	値
URL	サービス登録完了書に記載された管理画面 URL
アカウント	サービス登録完了書に記載されたアカウント
パスワード	初回ログイン後、更新したパスワード



2. 管理画面右上の「設定」をクリックします。



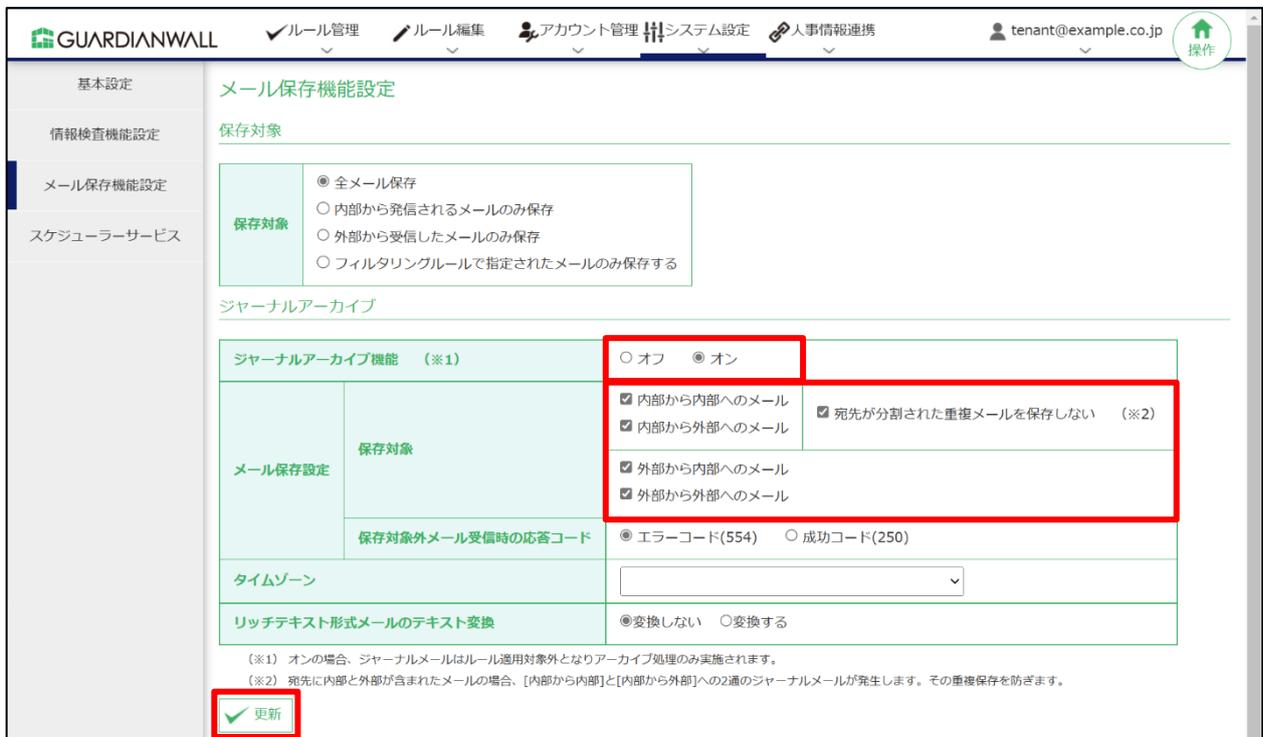
3. 「システム設定」 - 「メール保存機能設定」をクリックします。



4. 「ジャーナルアーカイブ機能」の「オン」にチェックを入れます。

「メール保存設定」 - 「保存対象」のすべての項目にチェックを入れます。

「更新」をクリックします。



5. 「OK」をクリックします。



6. 画面上部に「メール保存機能設定を変更しました。」と表示されることを確認します。



以上で、MailArchive on Cloud [ジャーナルメール] のみをご利用の場合の、ジャーナルアーカイブ機能設定は終了です。

4.3 テストメールの送信・確認

テストメールを送信し、ジャーナルメールがアーカイブされていることを確認するため、以下の手順を実施ください。

本手順は、社内間メールの送受信によるジャーナルアーカイブの動作を確認する手順となっております。

※本手順では「サービス登録完了書」を参照する項目がございます。

1. 以下の条件を満たしたメールを Microsoft 365 から送信します。

- 宛先：お客様ドメイン
- 送信者：お客様ドメインのユーザー

2. 送信者に手順 1 で送信したメールが届くことを確認します。



3. Web ブラウザよりジャーナルアーカイブされているか確認を行います。

管理画面へ接続します。以下の情報を入力し、「ログイン」をクリックします。

項目	値
URL	サービス登録完了書に記載された管理画面 URL
アカウント	サービス登録完了書に記載されたアカウント
パスワード	初回ログイン後、更新したパスワード



4. 「メールログをみる」をクリックします。



5. 以下のとおりに条件を入力し、「検索」をクリックします。

- 期間：テストメールを送信した日時
- キーワード：「件名」にて送信したテストメールの件名を入力

GUARDIANWALL

ホーム メール 状況 レポート

tenant@example.co.jp 設定

メールログ閲覧

メール全文検索

ダウンロードデータ管理

操作ログ閲覧

メールログ閲覧

検索条件

本日は 2023年02月14日 です。
検索可能期間は 2023年02月02日 ~ 2023年02月14日 です。

期間 2023年 2月 14日 ... ~ 2023年 2月 14日 ...

キーワード

対象	以外
件名 <input type="text" value="ジャーナルアーカイブテスト"/>	<input type="checkbox"/> 追加
差出人 <input type="text" value="ヘッダーFrom"/> <input type="text" value="を含む"/>	<input type="checkbox"/> 追加
宛先 <input type="text" value="ヘッダーTo,Cc"/> <input type="text" value="を含む"/>	<input type="checkbox"/> 追加

キーワード条件 すべて満たす いずれかを満たす

その他

ダウンロードデータ管理

操作ログ閲覧

メールアドレス
生年月日/年齢
組織名
クレジットカード番号

表示形式

表示件数 件/ページずつ表示

表示順
昇順 降順

6. 検索結果が表示されますので、送信したテストメールの受信時刻の枠内に「ジャーナルアーカイブ」のアイコンが表示されていることを確認します。



Microsoft 365 側の仕様として、ジャーナルメールが複数のメールに分かれて配信される場合があります。複数のメールに分かれたジャーナルメールを検索した場合、同じ内容のメールが複数検索される可能性があります。

The screenshot shows the GuardianWall interface with search results for the keyword "ジャーナルアーカイブテスト". The search period is from 2023-02-14 to 2023-02-14. The results table is as follows:

受信時刻	ヘッダーFrom	件名	サイズ	遅延配送ルール ID/動作	フィルタリングルール ID/動作	メール変換ルール ID/動作	状態
2023-02-14 11:19:55	user01@example.co.jp	ジャーナルアーカイブテスト	16.27K バイト	0/無し	0/無し	0 / 無し	-

7. 確認後、テストメールの受信時刻をクリックします。

The screenshot shows the details of the selected email. The search results table is as follows:

受信時刻	ヘッダーFrom	件名	サイズ	遅延配送ルール ID/動作	フィルタリングルール ID/動作	メール変換ルール ID/動作	状態
2023-02-14 11:19:55	user01@example.co.jp	ジャーナルアーカイブテスト	16.27K バイト	0/無し	0/無し	0 / 無し	-

8. 「保存メール本文」の画面に移行し、メール本文を閲覧できるかどうか確認します。

保存メール本文

↓ emlダウンロード

From	USER1 <user01@example.co.jp>
To	USER2 <user02@example.co.jp>
Cc	
Bcc	
エンベロープ	FROM : <user01@example.co.jp> RCPT : <user02@example.co.jp>
Date	Tue, 14 Feb 2023 02:19:54 +0000
メールサイズ	16.27Kバイト
件名	ジャーナルアーカイブテスト
MAILID	0063EAEFCB-S12WER3BAAA012E6-0001-000000240000

添付	無し
本文	ジャーナルアーカイブテスト用メール
ヘッダー 表示	
操作履歴 取得	
承認履歴 取得	無し

承認

閉じる

以上で、ジャーナルアーカイブ機能の動作確認は完了です。

5. 初期設定完了

サービス利用開始前に実施いただく作業は以上となります。

本資料での設定変更が完了後、お申込みいただいたサービスが利用可能です。

以降、「ユーザー運用ガイド」をご参照の上、ルール作成手順、確認手順を実施ください。

MailArchive on Cloud [ジャーナルメール]のみをご利用の場合は、本資料にて設定は終了です。

GUARDIANWALL

Mail セキュリティ・クラウド プレミアム

スタートアップガイド

2025 年 3 月 ver.4.1