GUARDIANWALL

Mail セキュリティ・クラウド　ベーシック
スタートアップガイド

Canon キヤノンマーケティングジャパン株式会社

2025-Mar.-12

目次

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いたします。

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。

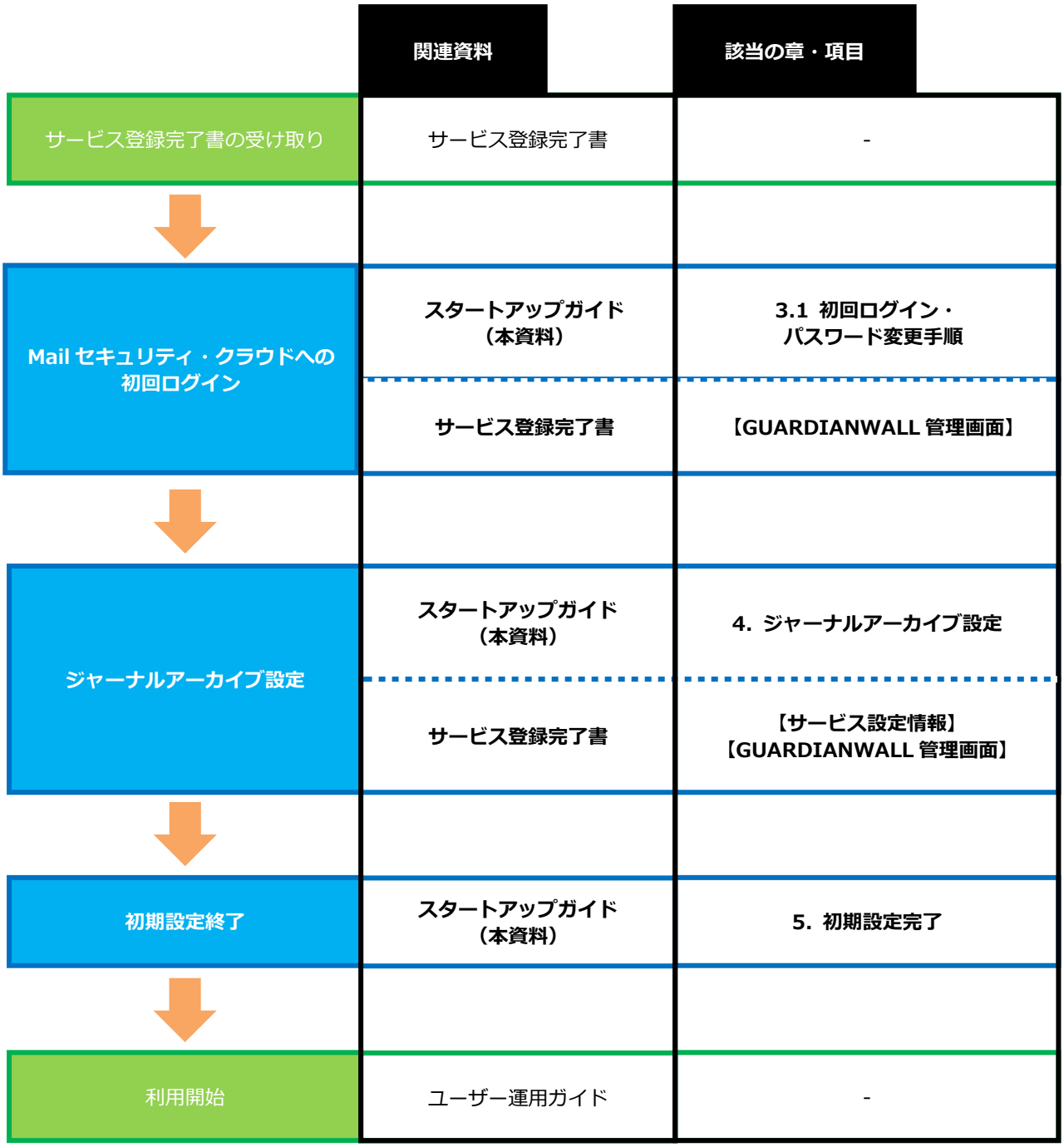
パターン A の場合

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。



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ございます。
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 [4.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ございます。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単体でご利用の場合、「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単体でご利用の場合、「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

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。

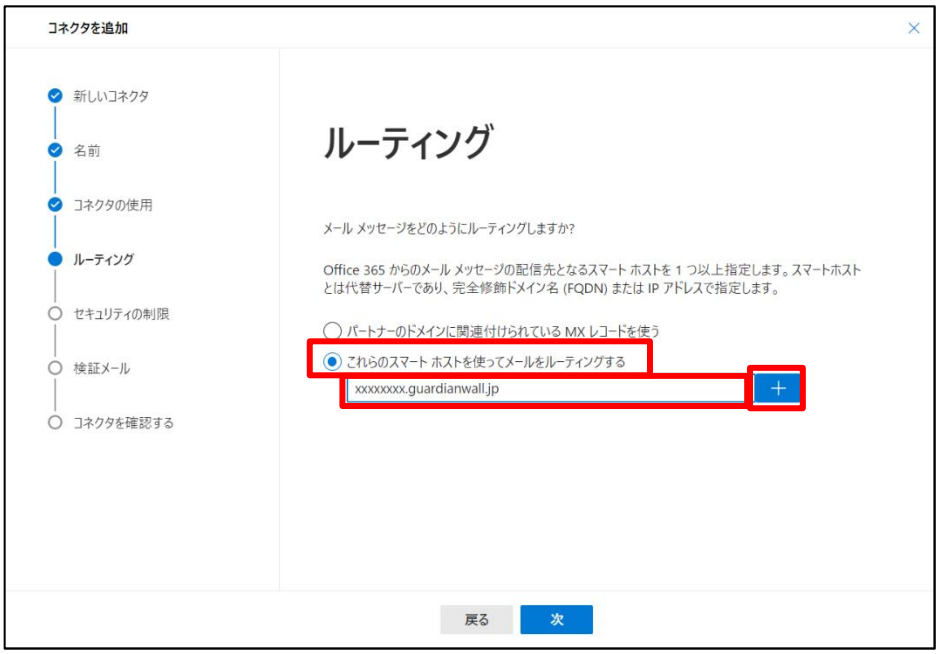
   設定後、「次」をクリックします。

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

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。

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。

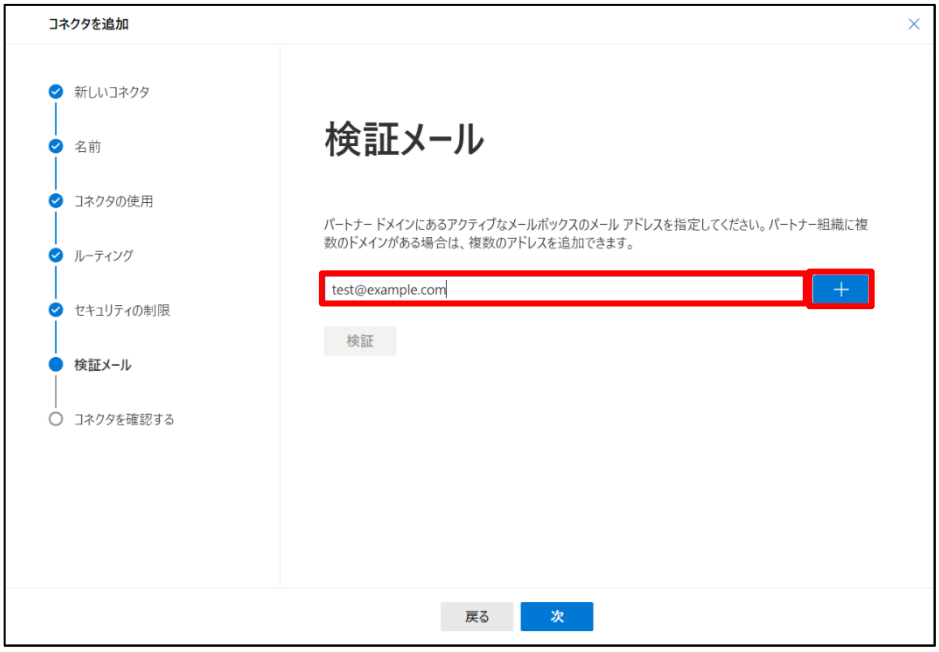
10. Mail セキュリティ・クラウドへの接続方法を以下のとおりに設定し、「次」をクリックします。

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	○

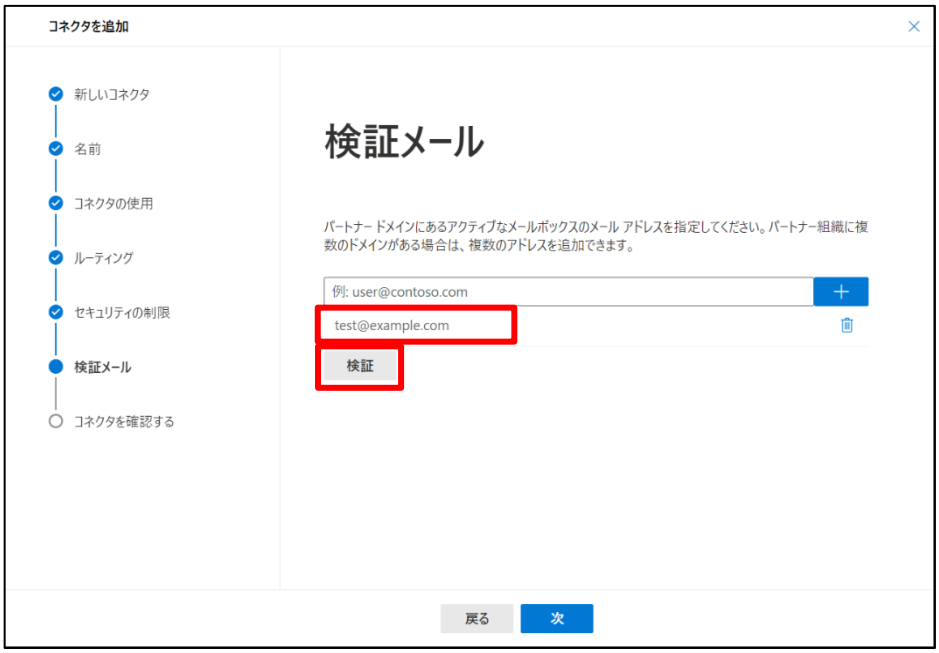
11. 設定したコネクタが利用できることを検証します。

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。

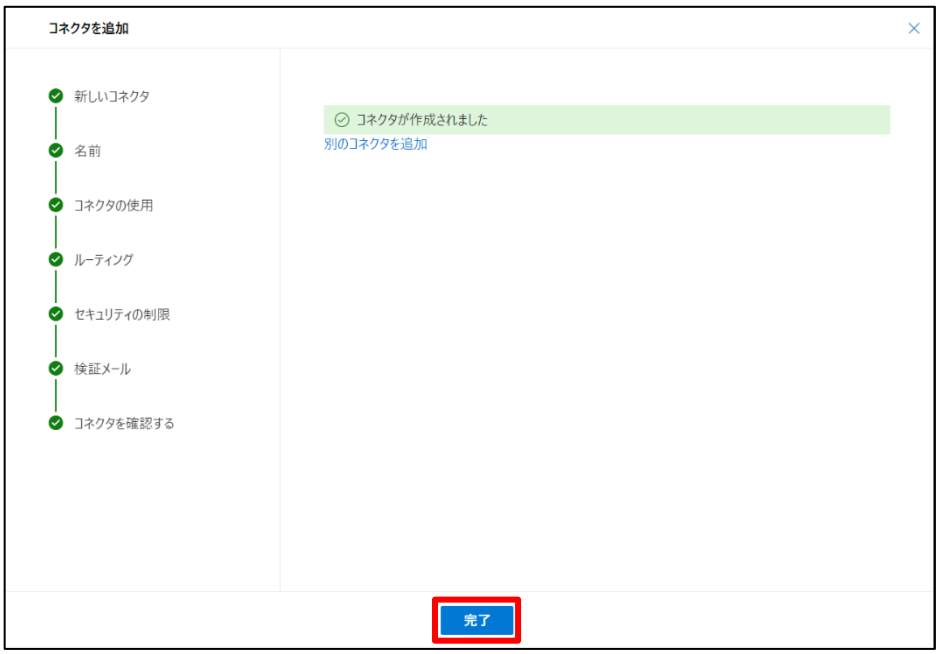


13. 「検証が成功しました」と表示されることを確認し、「次」をクリックします。

※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。

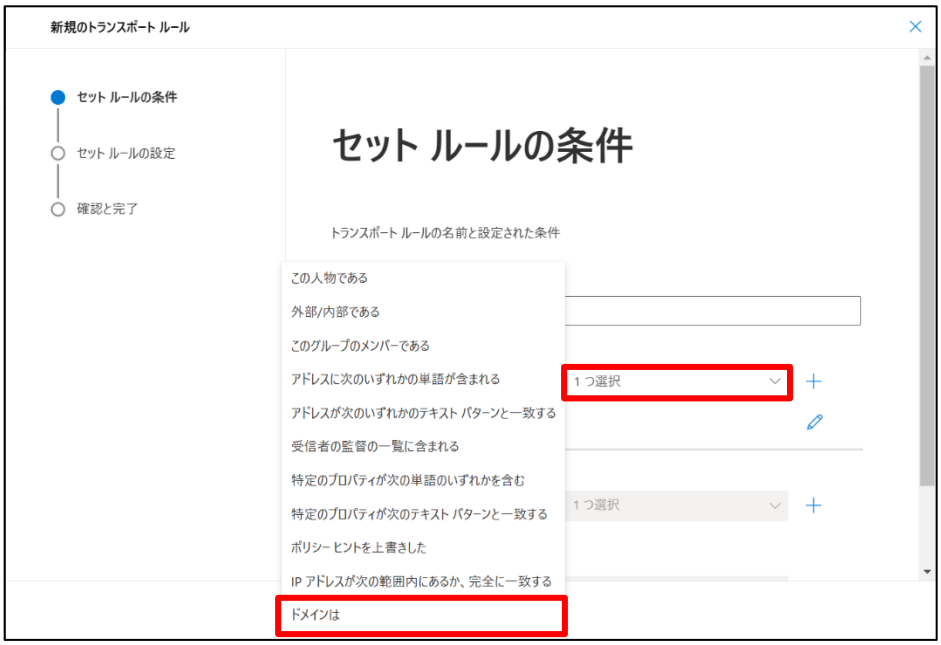
1.　「Exchange 管理センター」の画面にて「メールフロー」-「ルール」をクリックします。

「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。

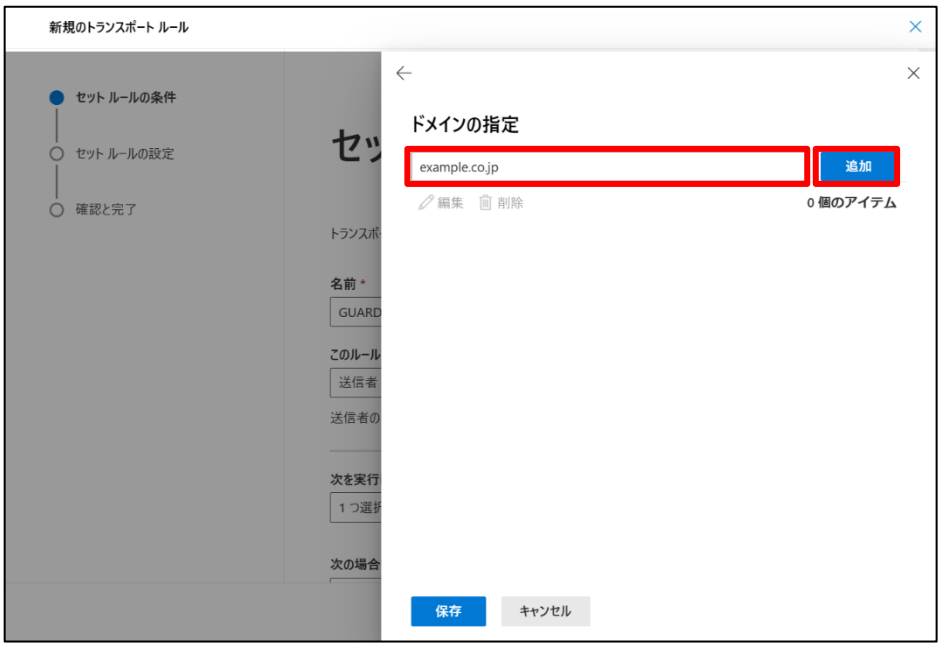
2.　ルールの新規作成画面に移行後、名前を設定し、「このルールを適用する」にて「送信者」を選択します。

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

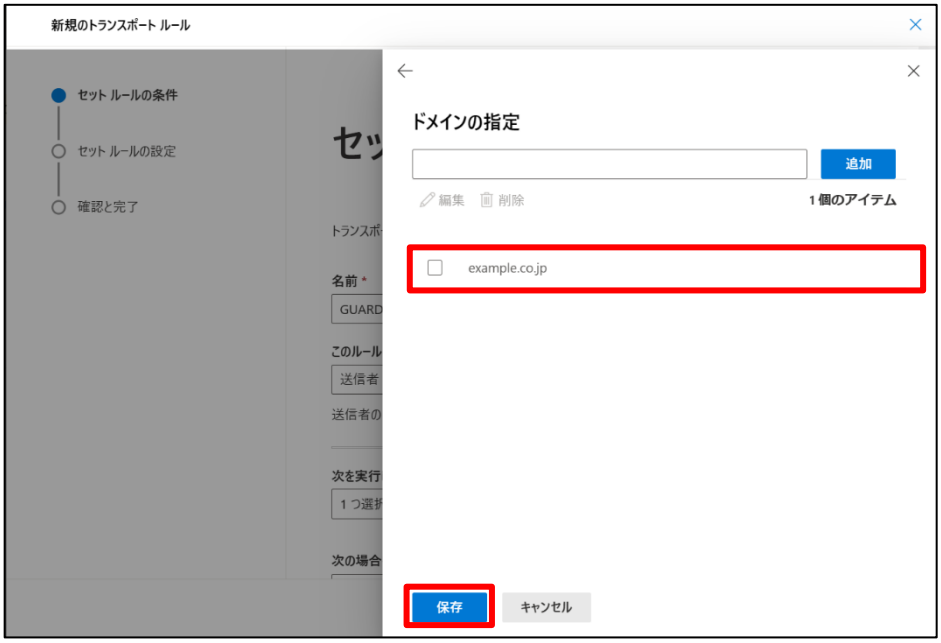
3. 「このルールを適用する」にて「送信者」を選択すると、右に追加の設定項目が表示されるので、リストから「ドメインは」を選択します。



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。



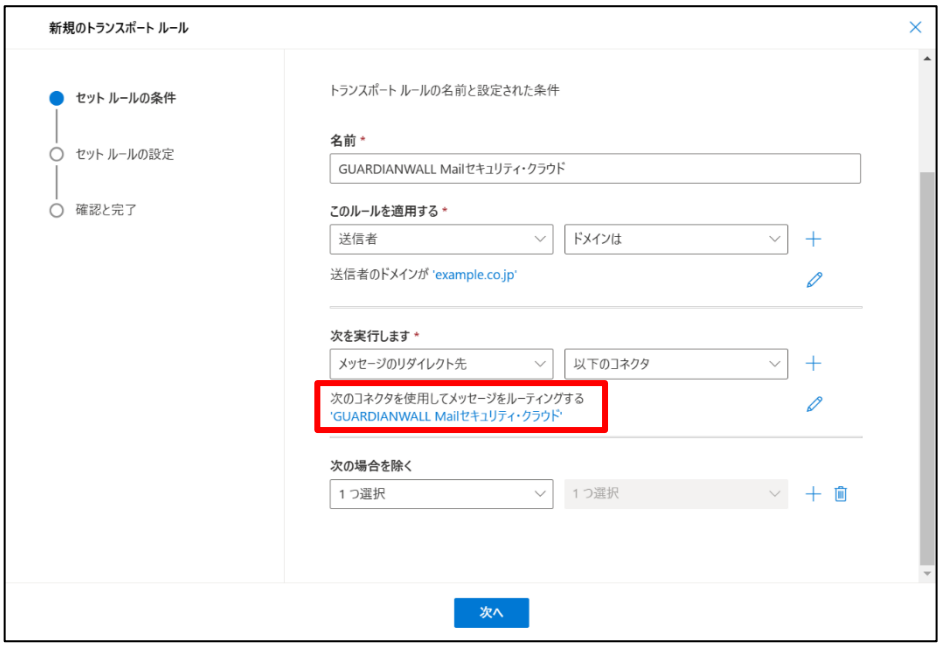
6. 「このルールを適用する」に「お客様ドメイン名」が反映されていることを確認します。

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。

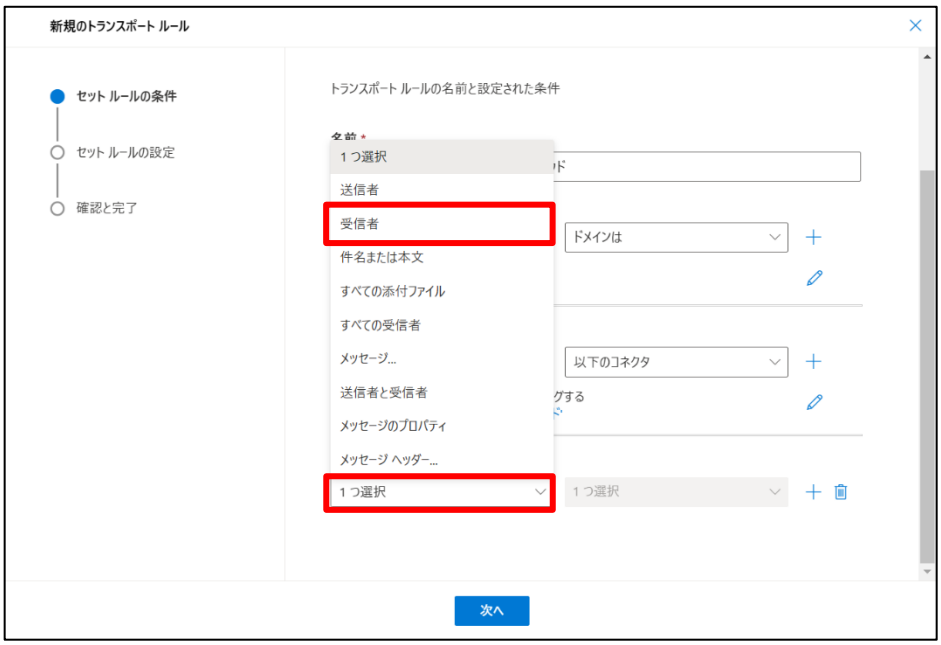
8. 「次を実行します」にて「メッセージのリダイレクト先」を選択すると、右に追加の設定項目が表示されるので、リストから「以下のコネクタ」を選択します。

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。

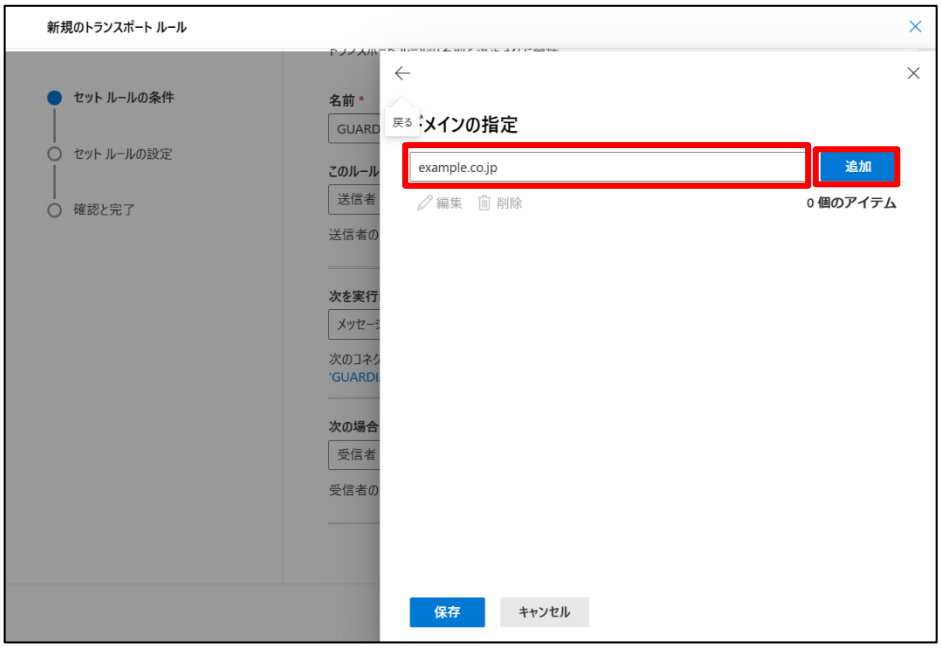


11. 「次の場合を除く」にて「受信者」を選択します。



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。

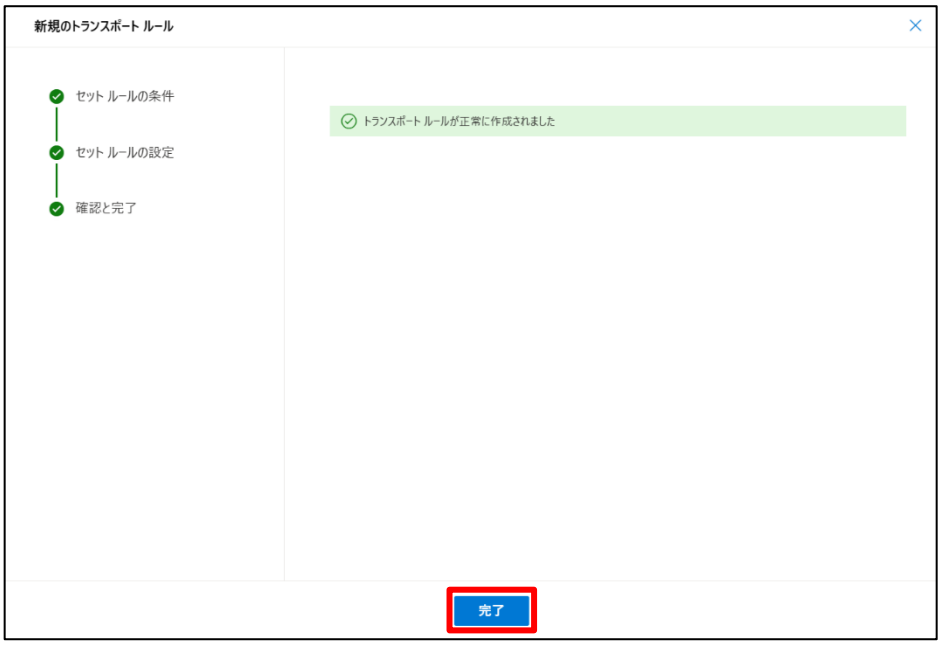
15. ルールの例外条件に「お客様ドメイン名」が反映されていることを確認し、「次へ」をクリックします。

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。

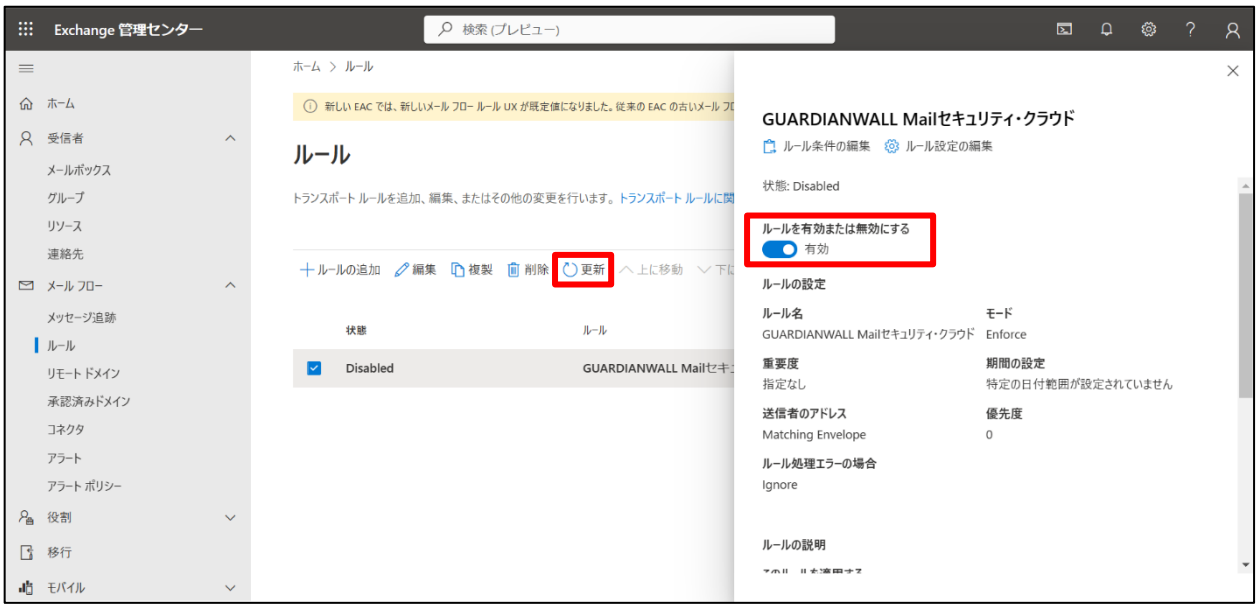
18. 「トランスポート ルールが正常に作成されました」と表示されることを確認し、「完了」をクリックします。



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。

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

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。

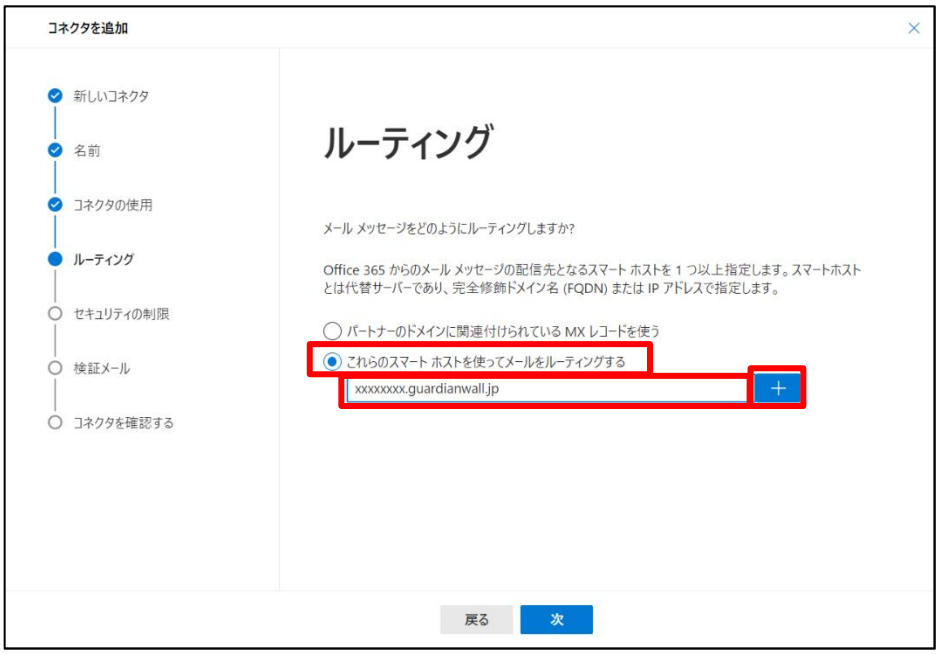
   設定後、「次」をクリックします。

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

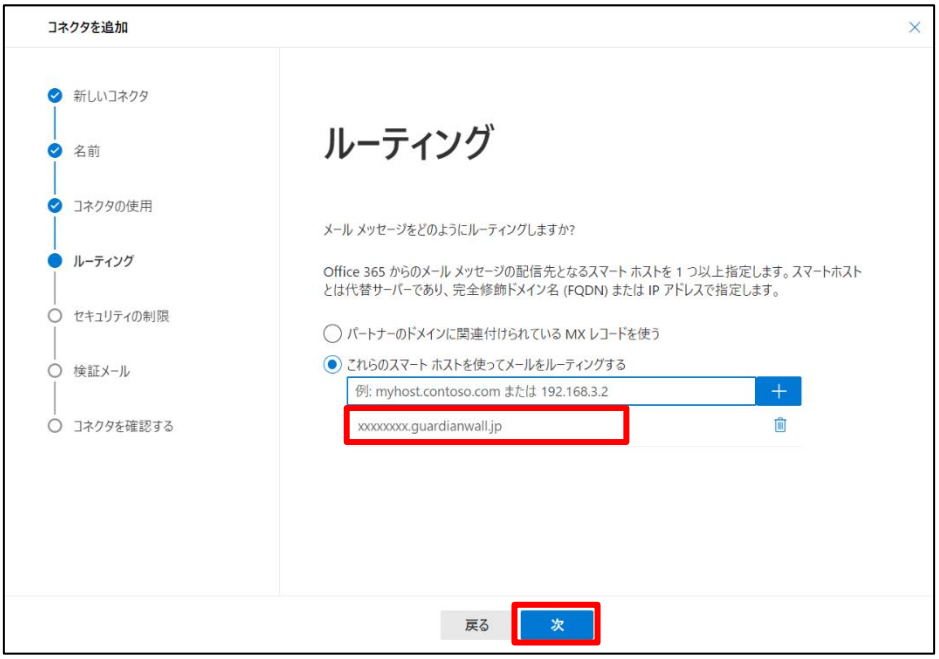
7. 「メッセージをこのコネクタにリダイレクトするトランスポートルールが設定されている場合のみ」を選択し、

   「次」をクリックします。

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。



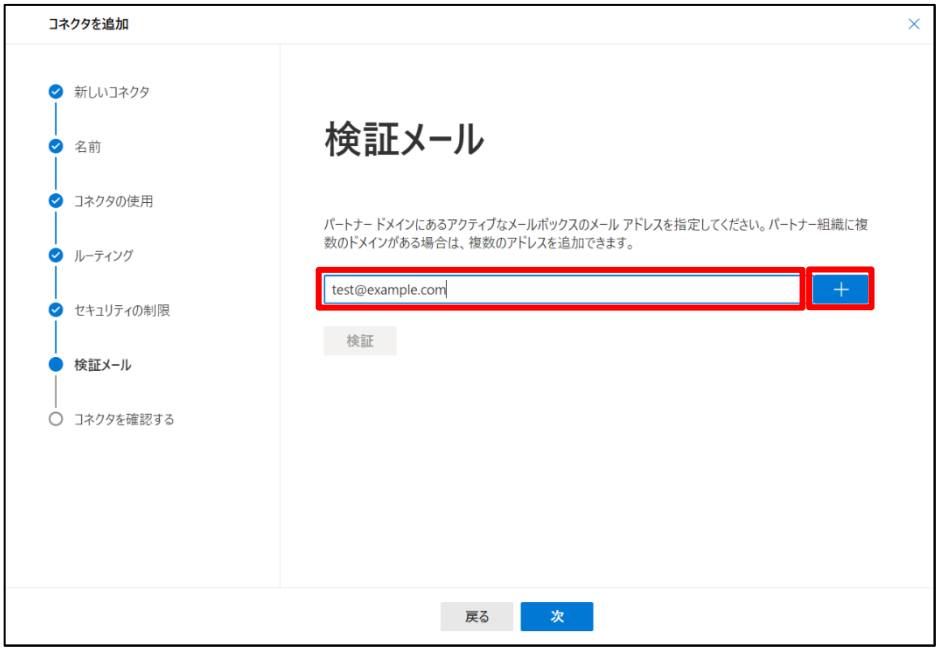
10. Mail セキュリティ・クラウドへの接続方法を以下のとおりに設定し、「次」をクリックします。

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	○

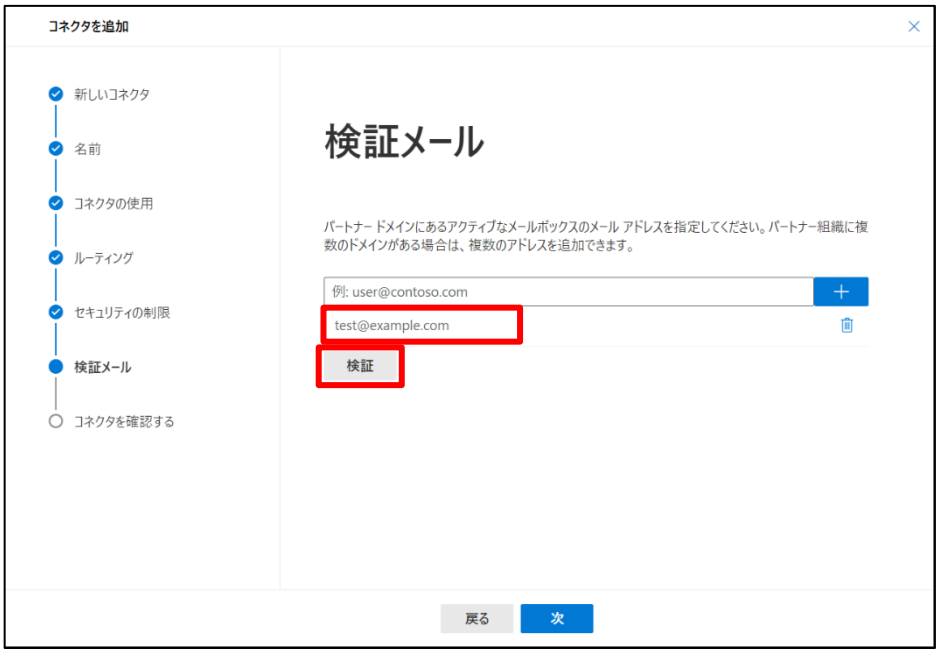
11. 設定したコネクタが利用できることを検証します。

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。

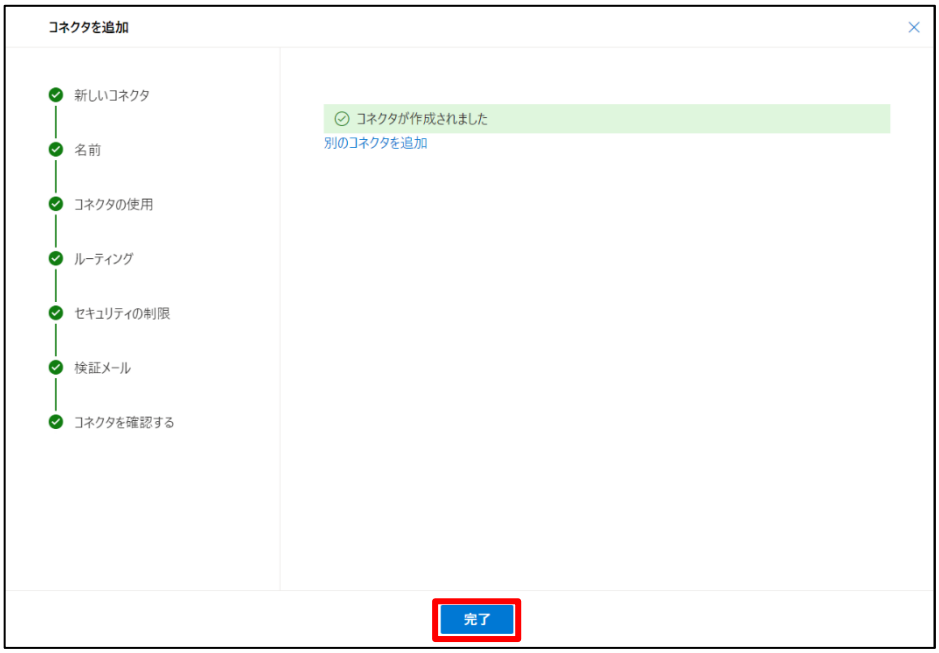


13. 「検証が成功しました」と表示されることを確認し、「次」をクリックします。

※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。

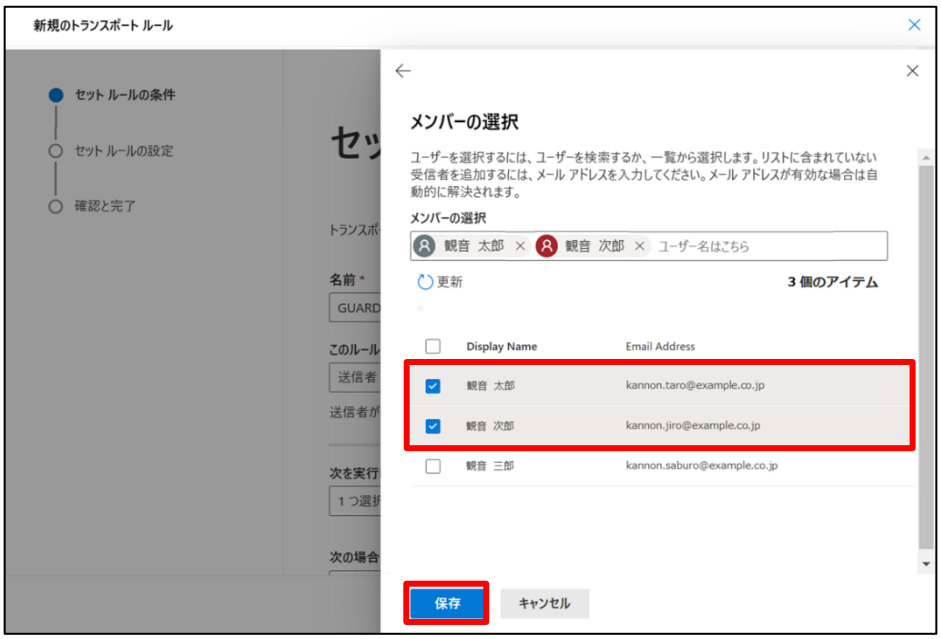
「ルール」の画面より「＋ルールの追加」をクリックし、「新しいルールの作成」を選択します。

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。



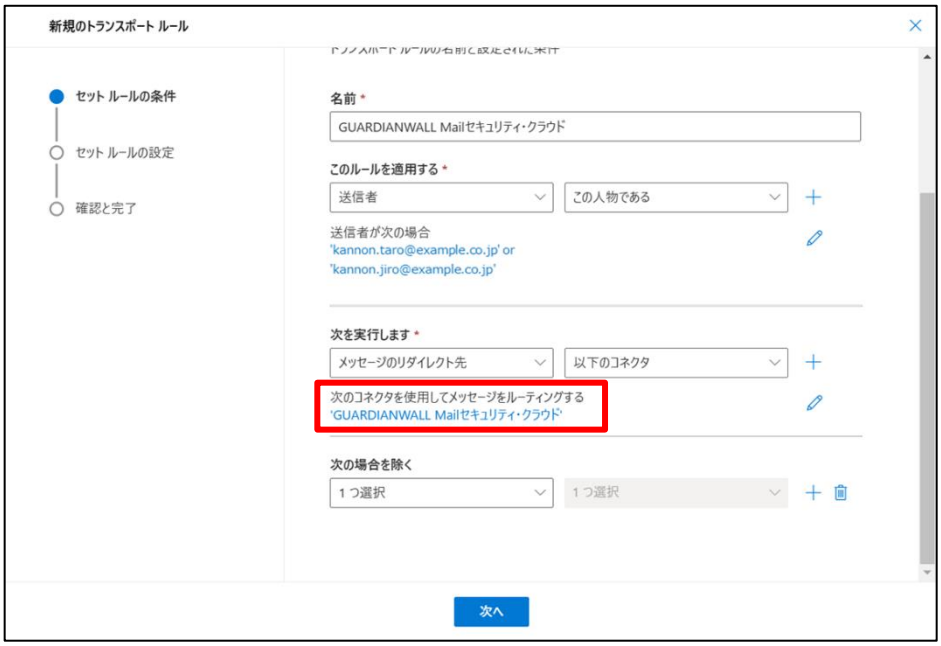
5. 「このルールを適用する条件」に「ユーザー」が反映されていることを確認します。

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。

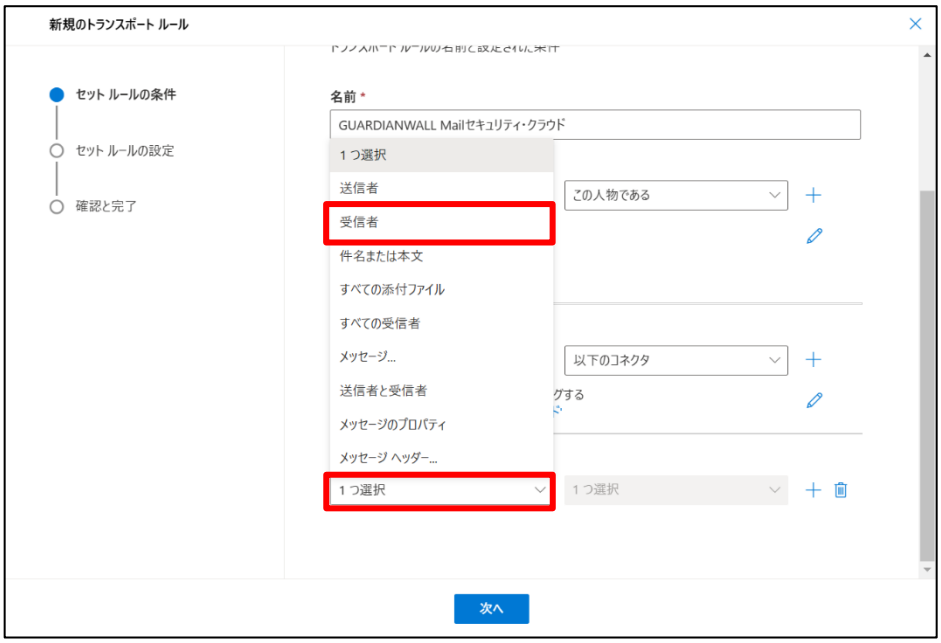
7. 「次を実行します」にて「メッセージのリダイレクト先」を選択すると、右に追加の設定項目が表示されるので、リストから「以下のコネクタ」を選択します。

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。

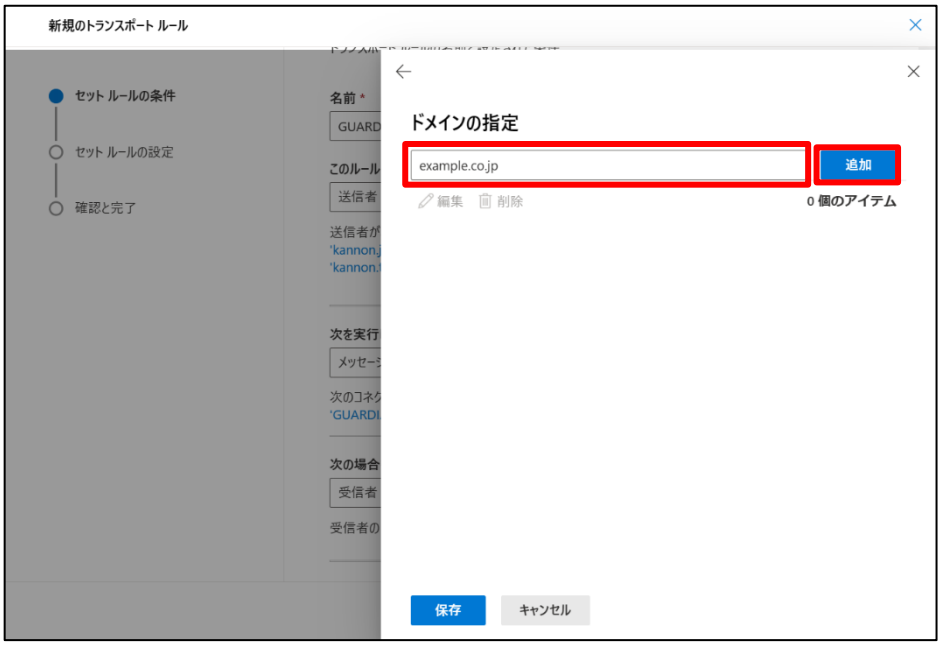


10. 「次の場合を除く」にて「受信者」を選択します。



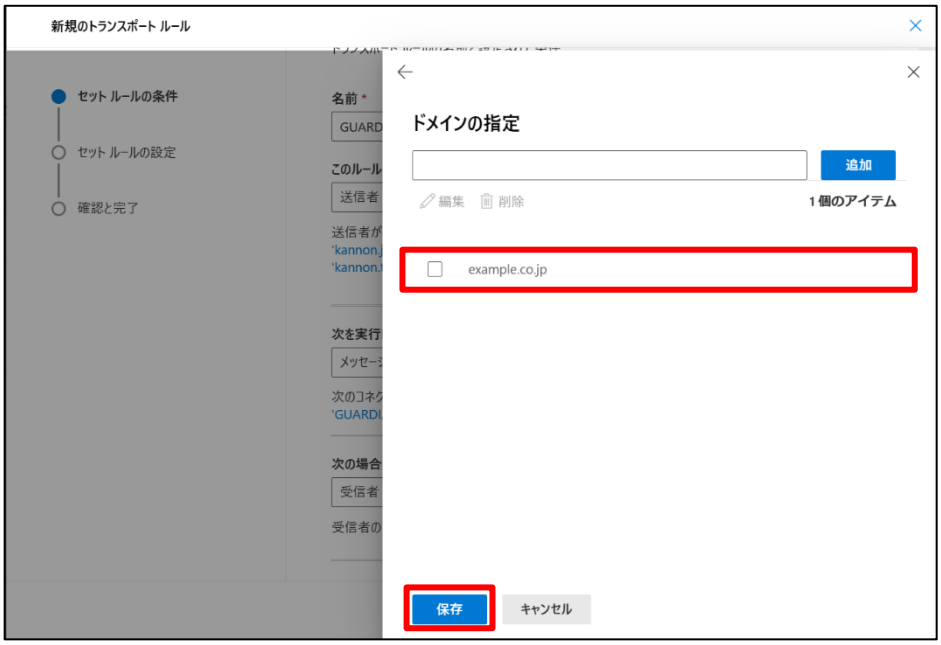
11. 「次の場合を除く」にて「受信者」を選択すると、右に追加の設定項目が表示されるので、リストから「ドメインは」を選択します。

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。



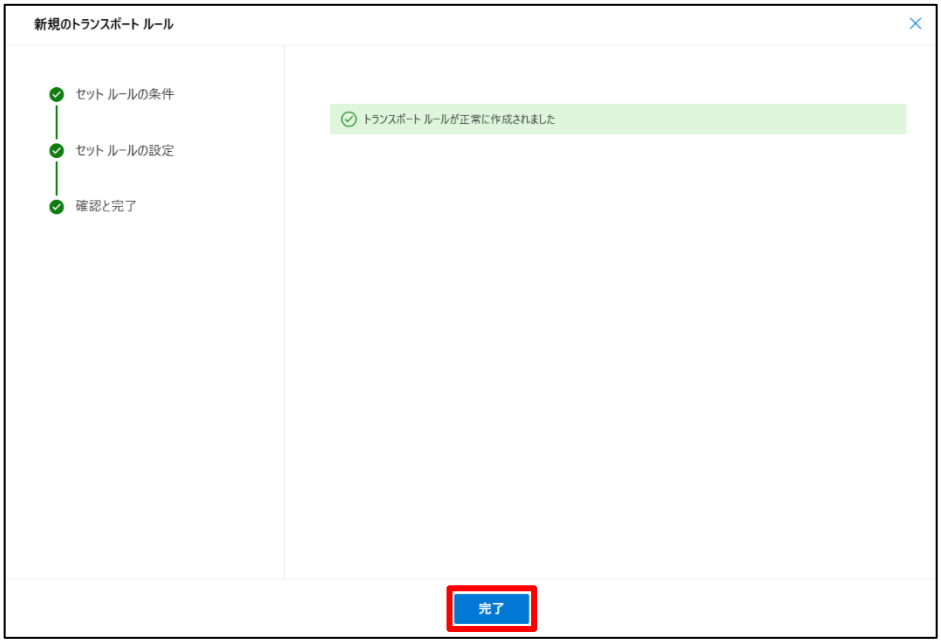
14. ルールの例外条件に「お客様ドメイン名」が反映されていることを確認し、「次へ」をクリックします。

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。

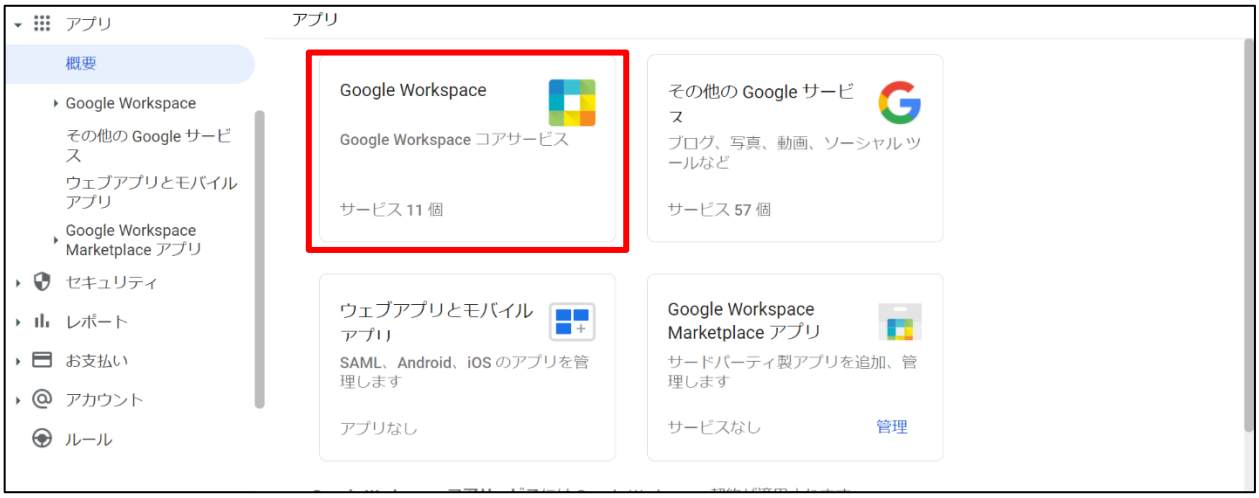
1　ルートの設定

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。

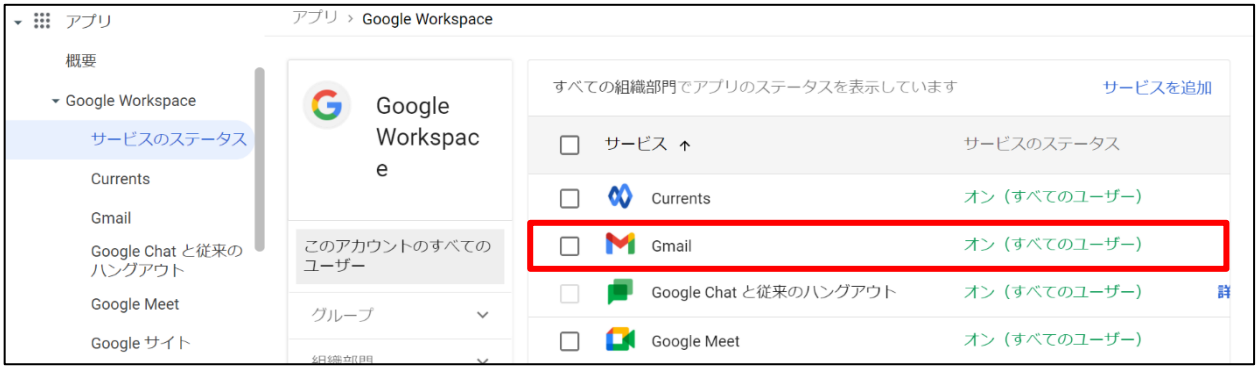
※本手順では「サービス登録完了書」を参照する項目がございます。

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。

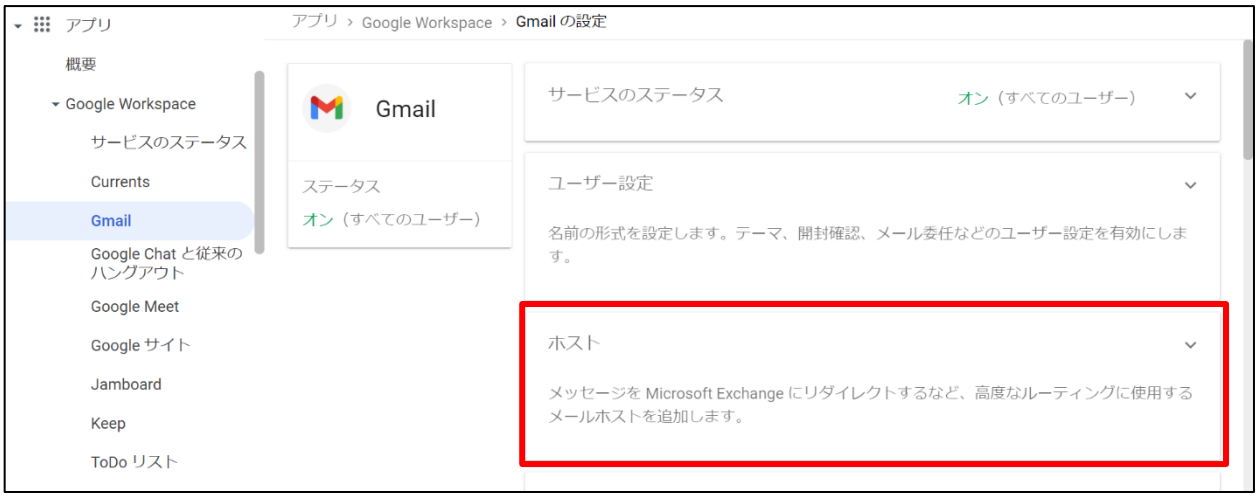
2.　「アプリ」の画面に移行後、「Google Workspace」をクリックします。



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



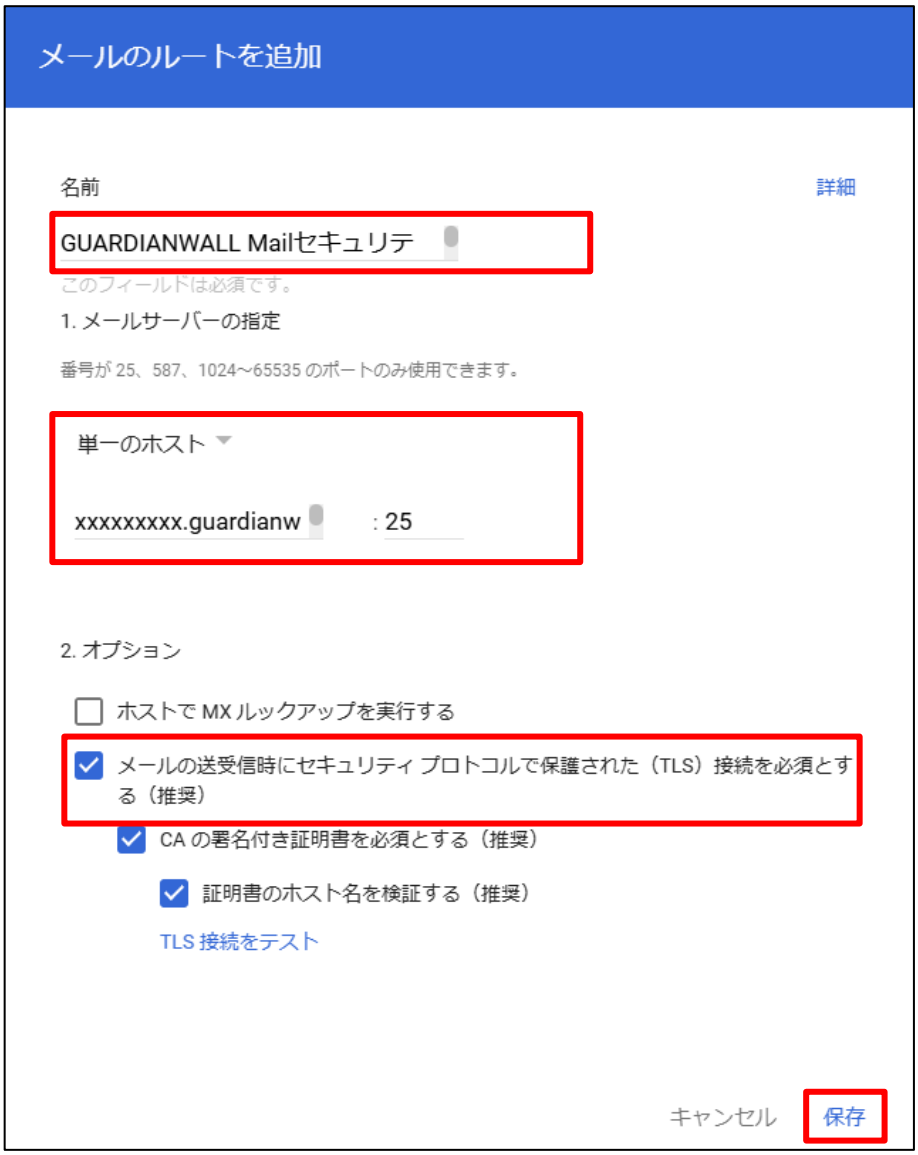
4. 「Gmail の設定」の画面に移行後、「ホスト」をクリックします。



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）	■

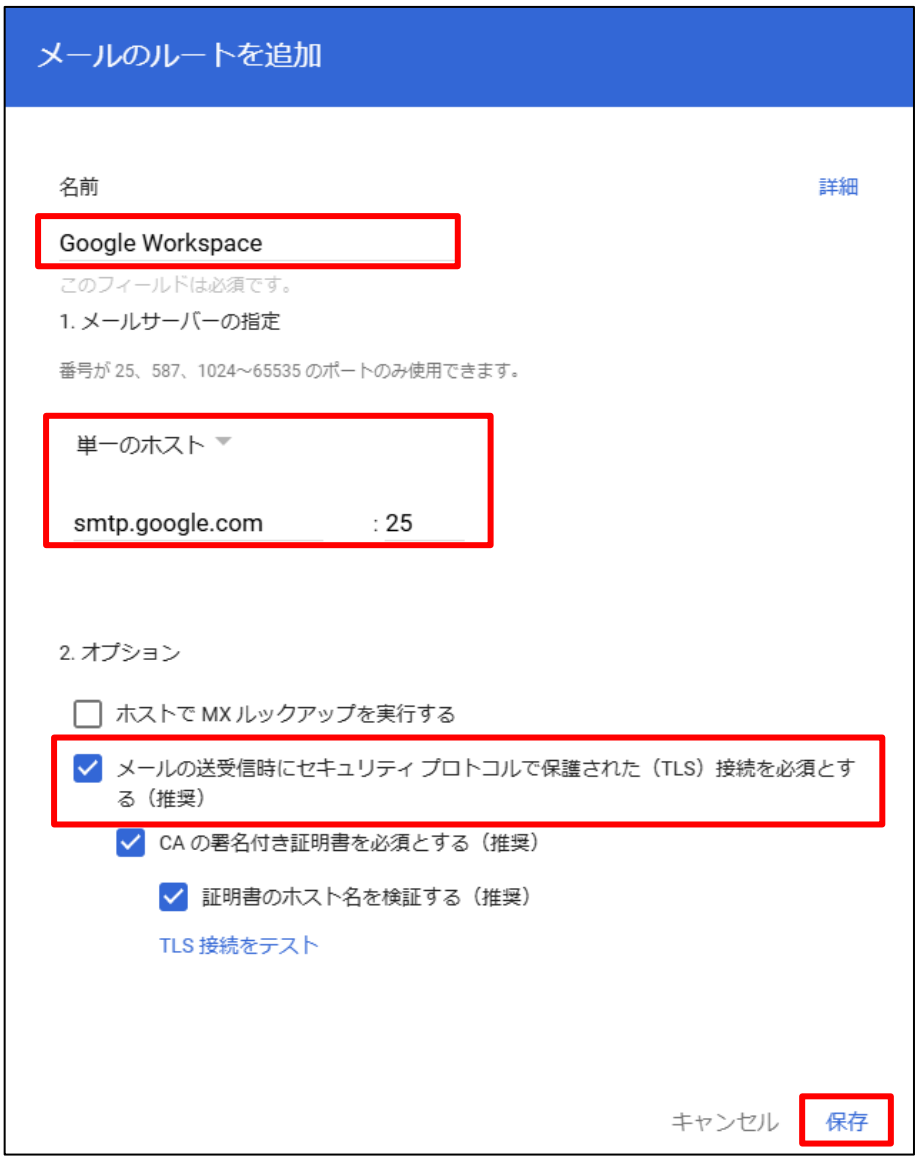


7. 社内間のメールについては、Google Workspace の MX レコード先へ送信されるように設定します。

「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）	■



以上で、ルートの設定は終了です。メールリレールールの設定に進みます。

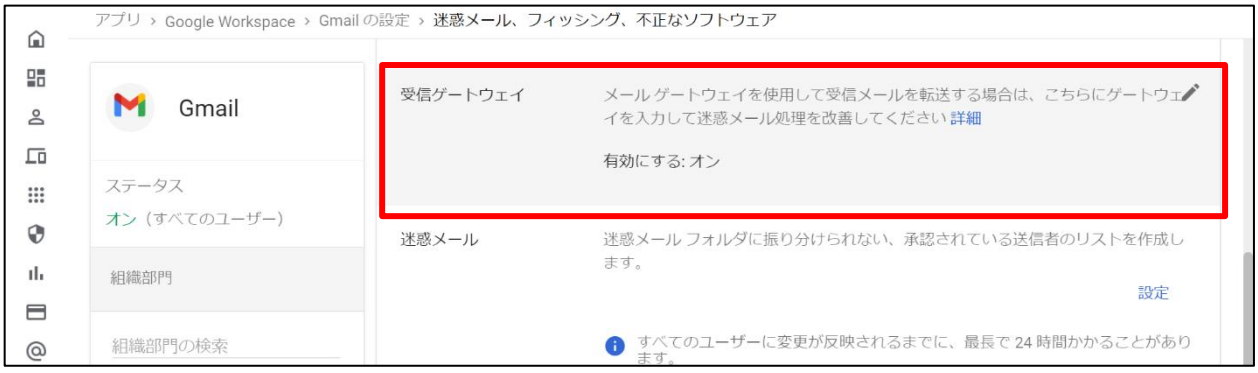
2　メールリレールールの設定

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。

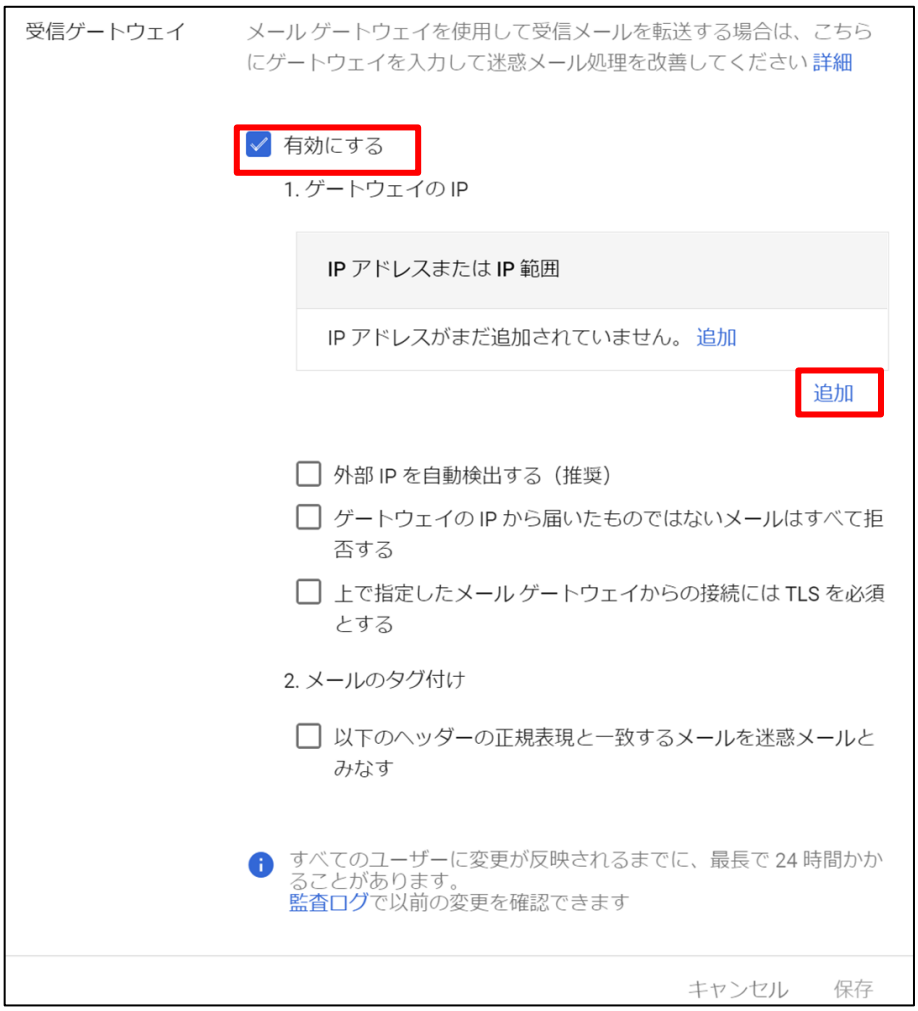
1.　「Gmail の設定」をクリックします。

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。

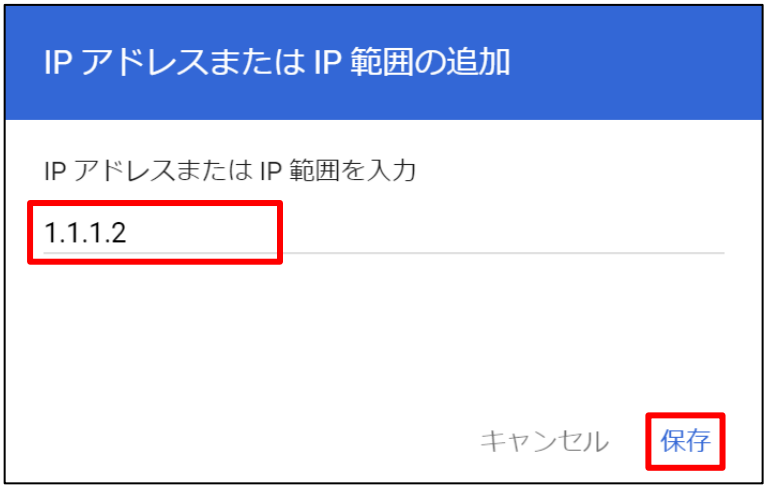


4. 「有効にする」にチェックを入れ、「追加」をクリックします。

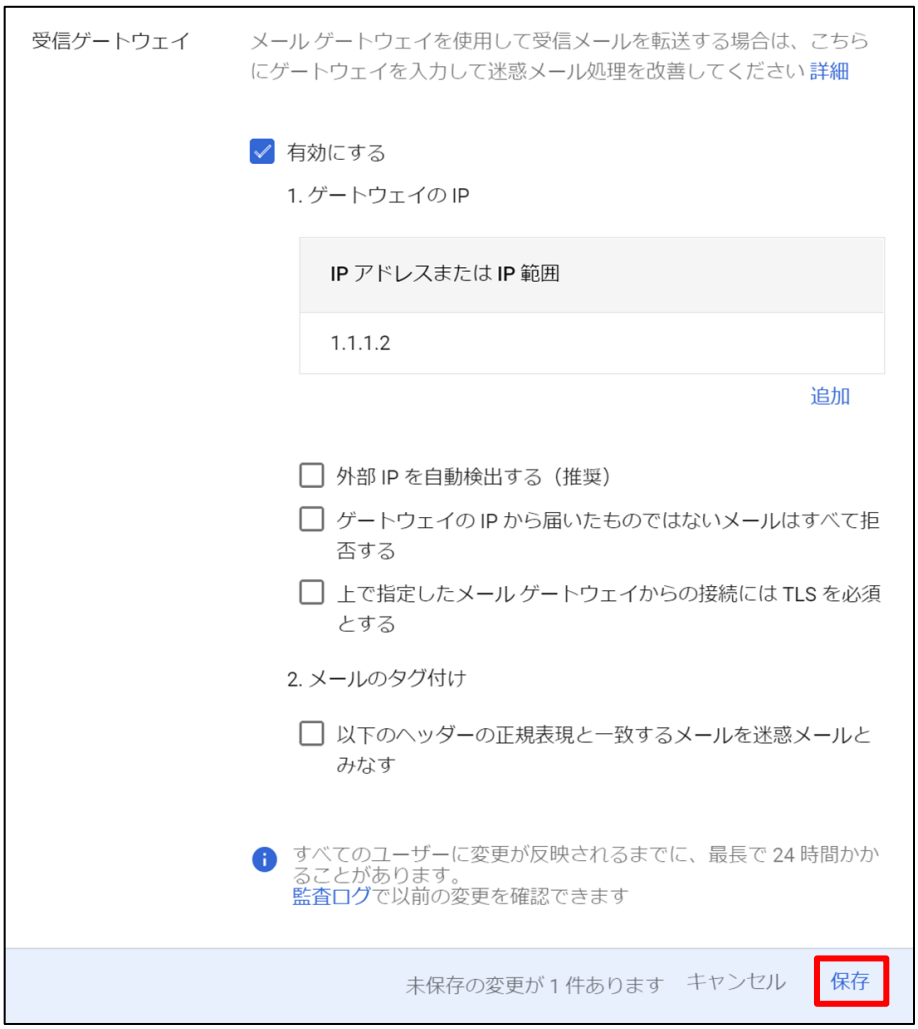


5. サービス登録完了書に記載されたすべての「受信ゲートウェイ IP」を入力し、「保存」をクリックします。

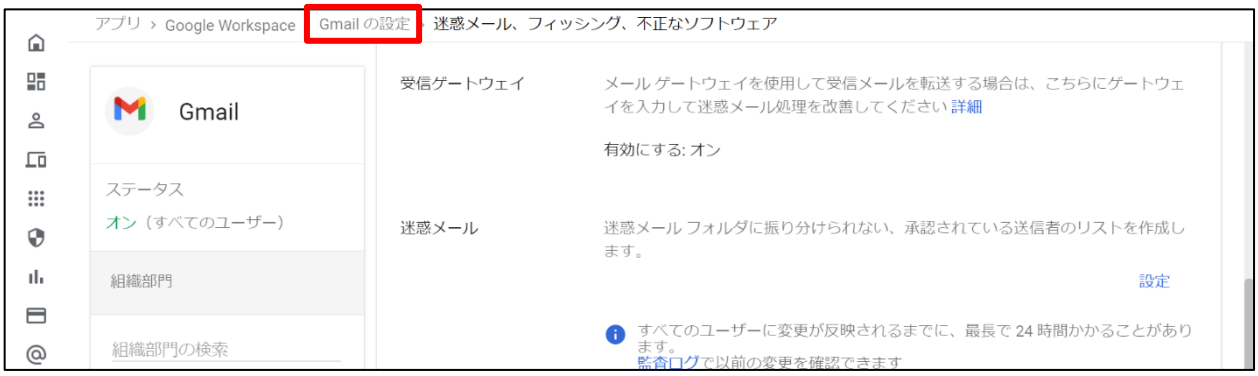
   IP アドレスの設定は、 1 つずつ行い、すべての「受信ゲートウェイ IP」を入力し終わるまで、繰り返します。



6. すべての IP アドレスを追加後、「保存」をクリックします。



7. 「Gmail の設定」をクリックします。



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

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。

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。

14. 以下のとおりに設定し、「設定を追加」をクリックします。

項目	設定値
ユーザー	■
グループ	■

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。

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

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。

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。

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	■

20. 追加されていることを確認します。

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。

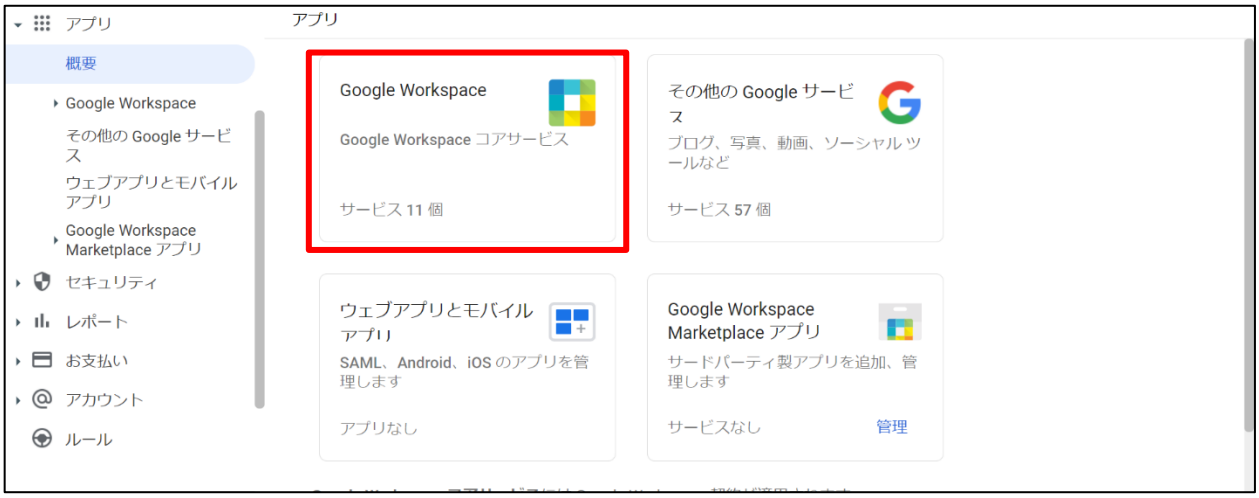
1　ルートの設定

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。

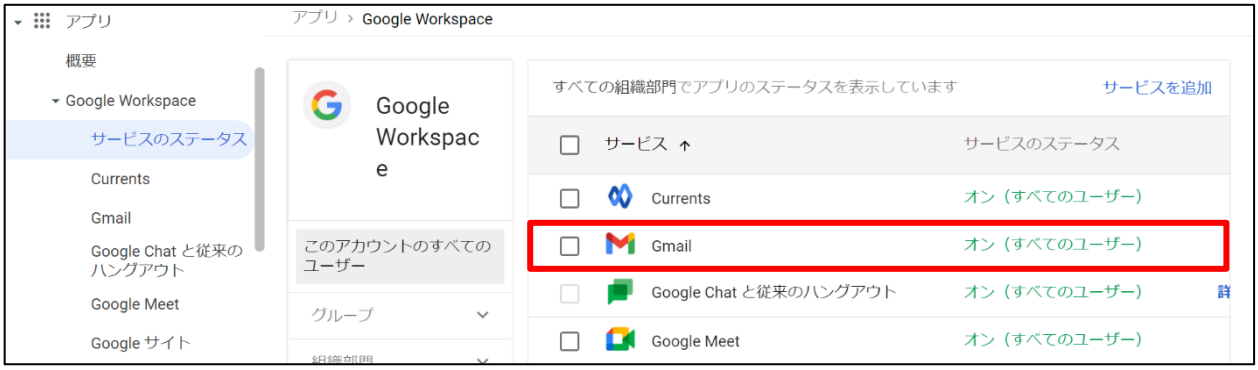
※本手順では「サービス登録完了書」を参照する項目がございます。

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。

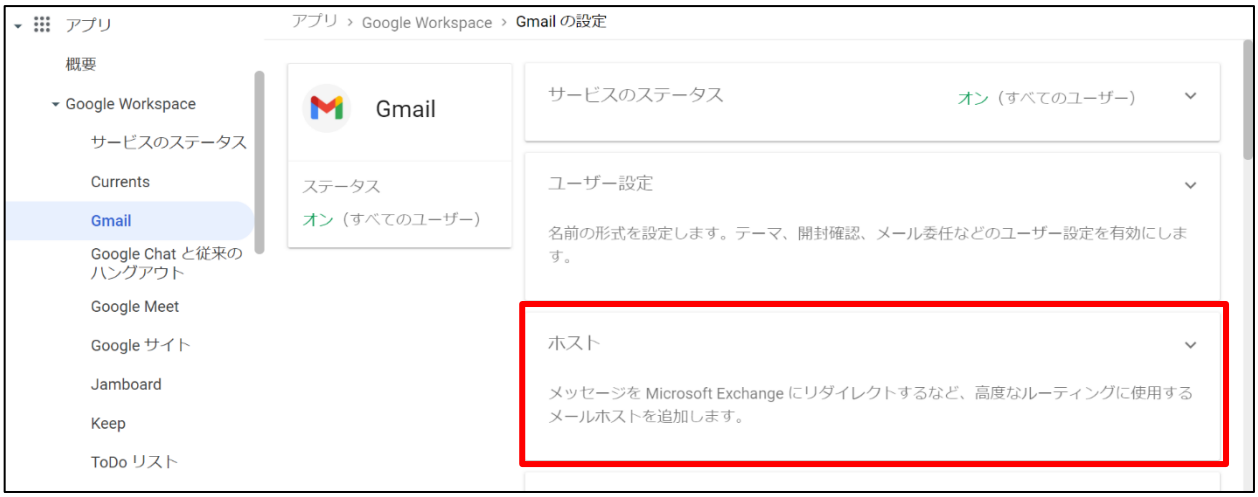
2.　「アプリ」の画面に移行後、「Google Workspace」をクリックします。



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



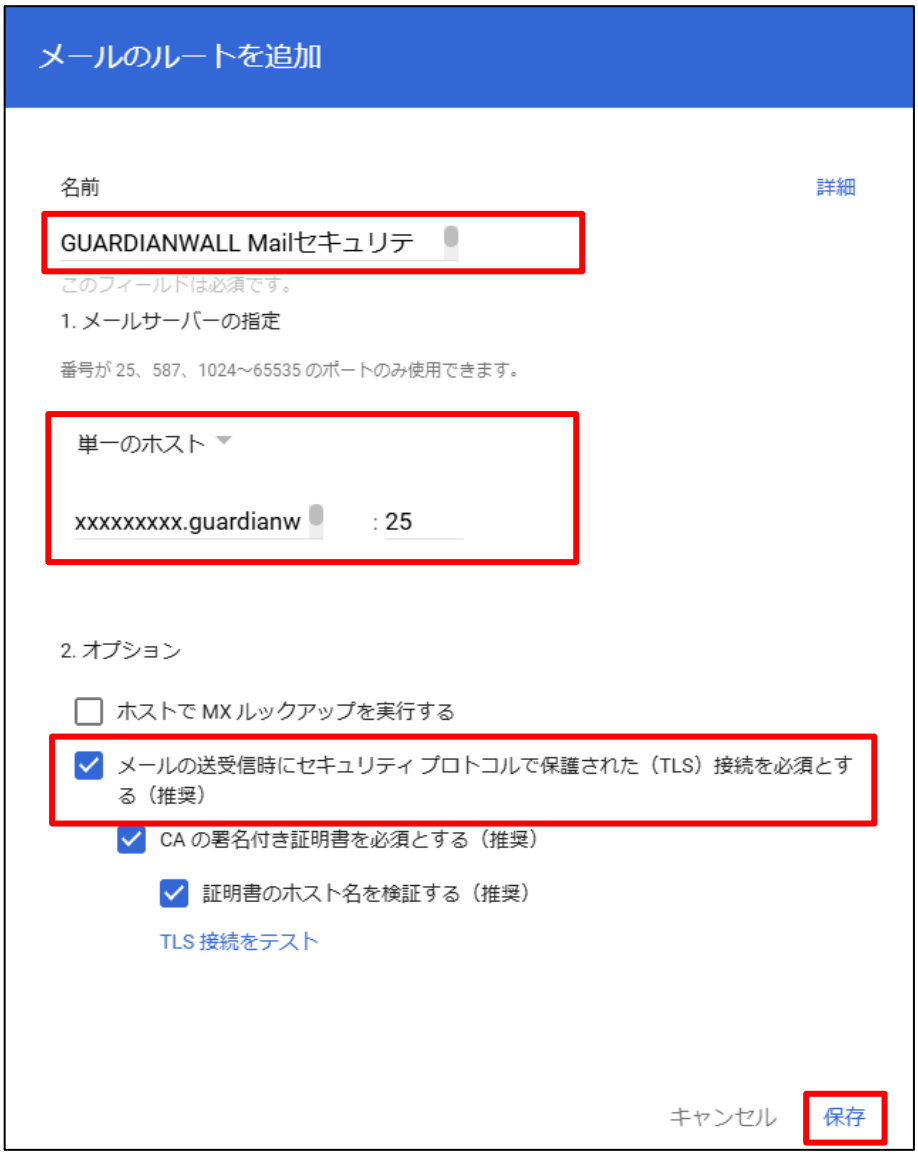
4. 「Gmail の設定」の画面に移行後、「ホスト」をクリックします。



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）	■

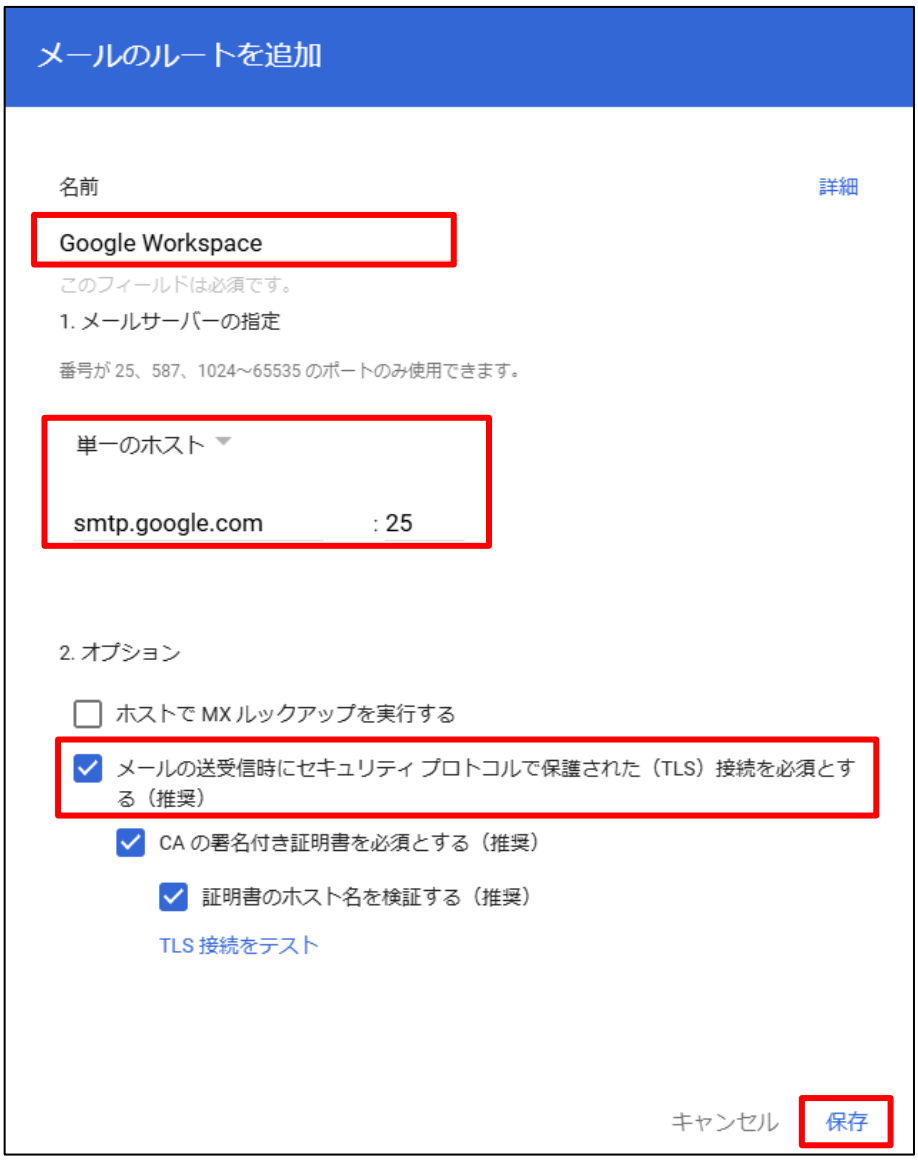


7. 社内間のメールについては、Google Workspace の MX レコード先へ送信されるように設定します。

「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）	■



以上で、ルートの設定は終了です。メールリレールールの設定に進みます。

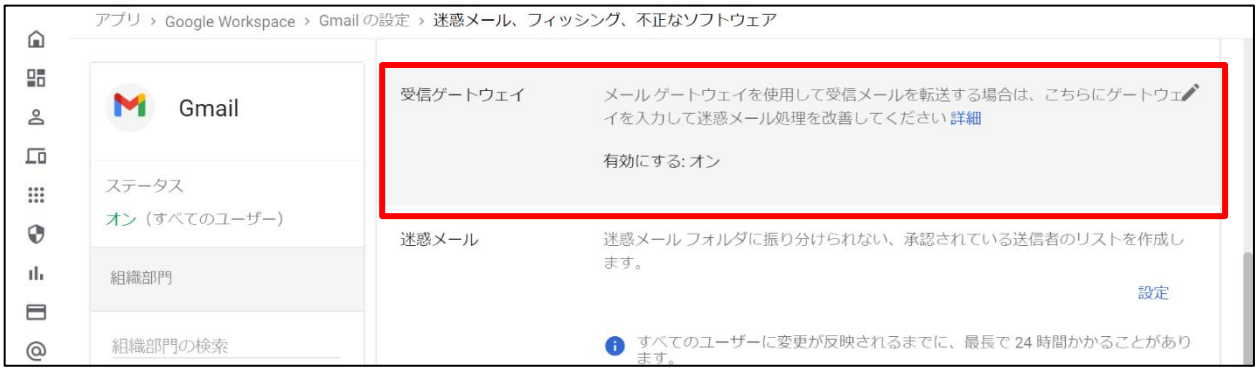
2　メールリレールールの設定

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。

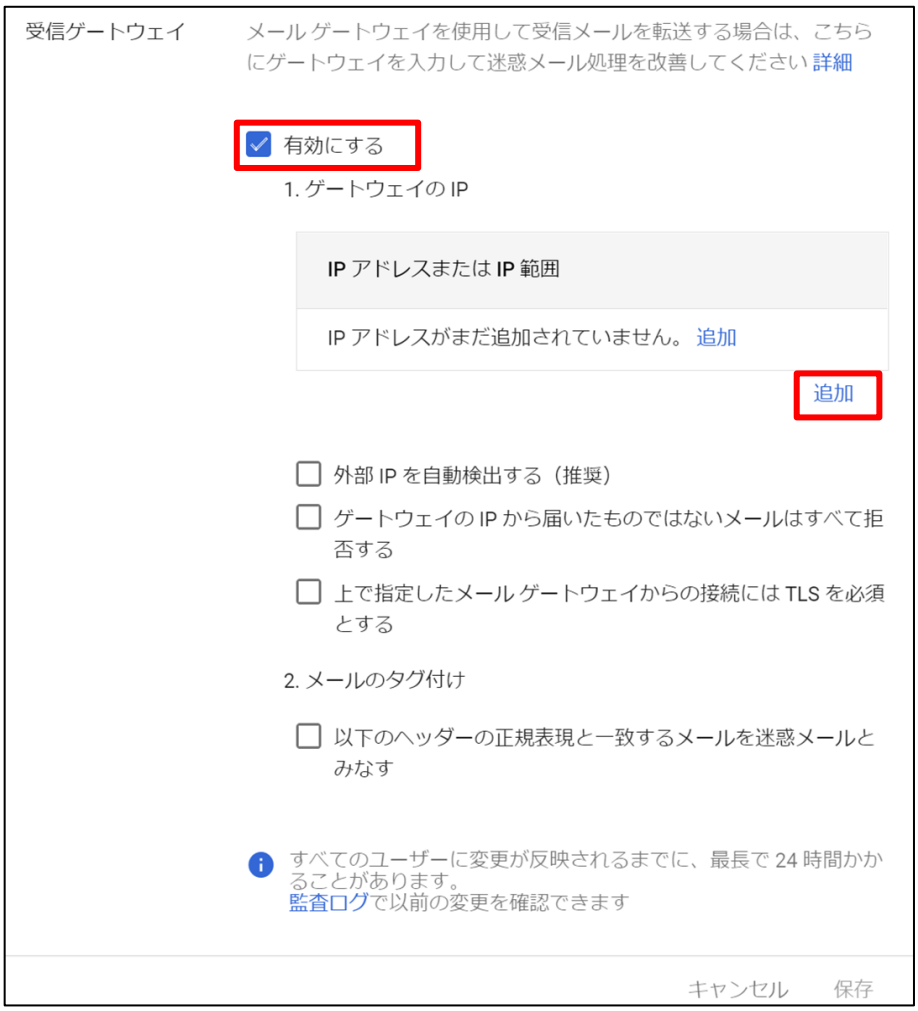
1.　「Gmail の設定」をクリックします。

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。

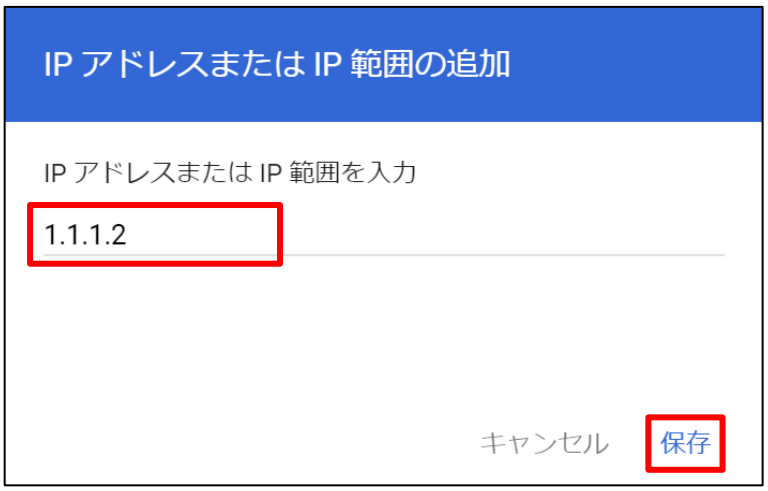


4. 「有効にする」にチェックを入れ、「追加」をクリックします。

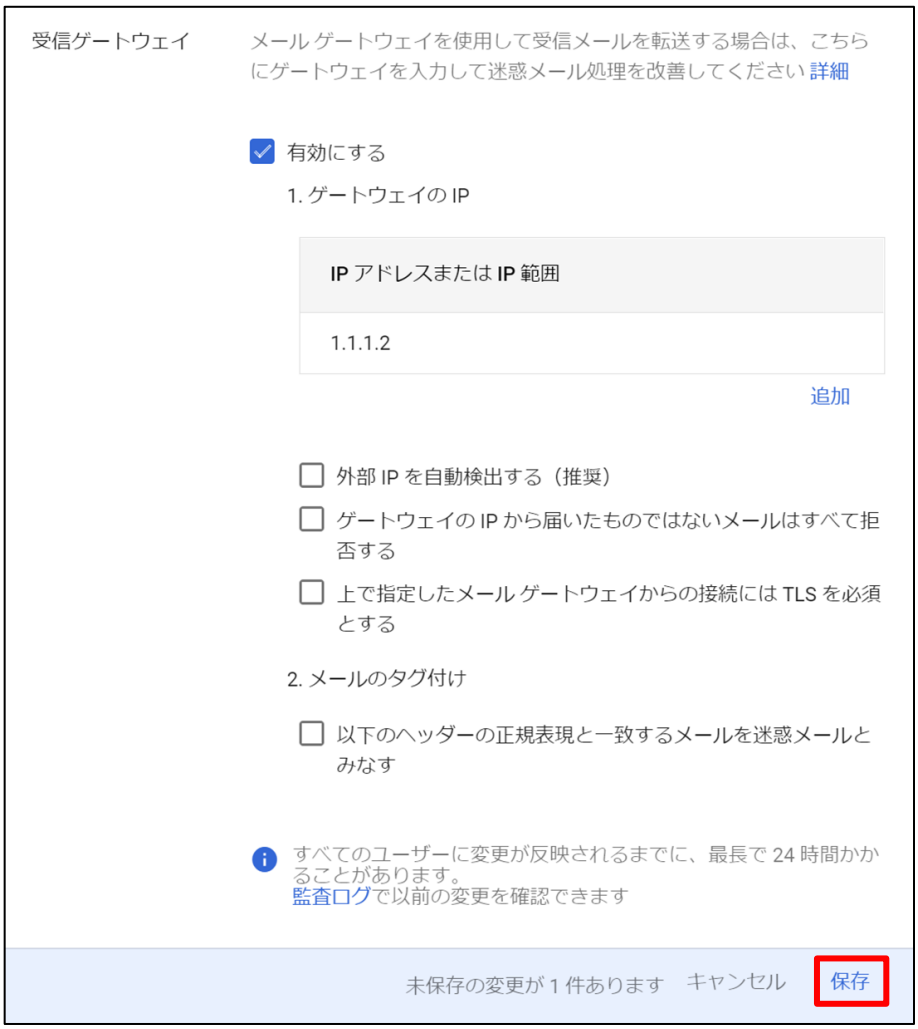


5. サービス登録完了書に記載されたすべての「受信ゲートウェイ IP」を入力し、「保存」をクリックします。

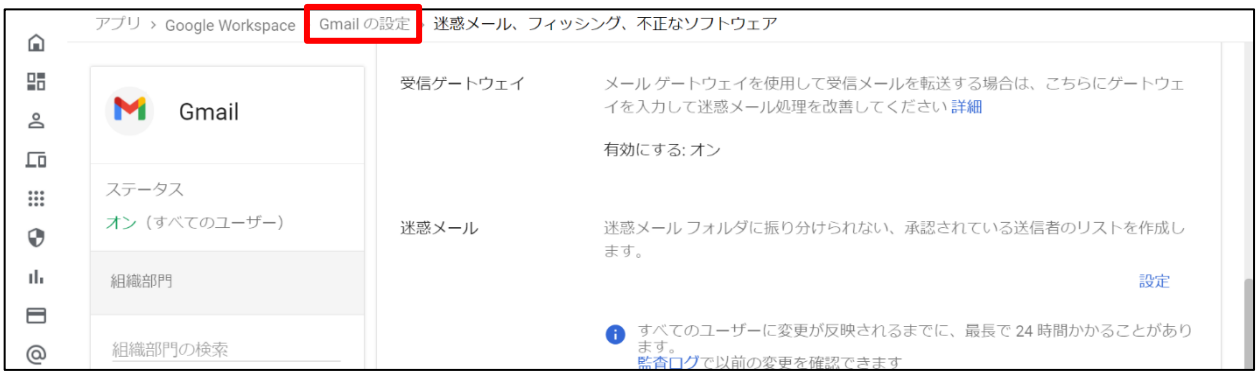
IP アドレスの設定は、 1 つずつ行い、すべての「受信ゲートウェイ IP」を入力し終わるまで、繰り返します。



6. すべての IP アドレスを追加後、「保存」をクリックします。



7. 「Gmail の設定」をクリックします。



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

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。

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。

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	■

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。

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。

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

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。

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。

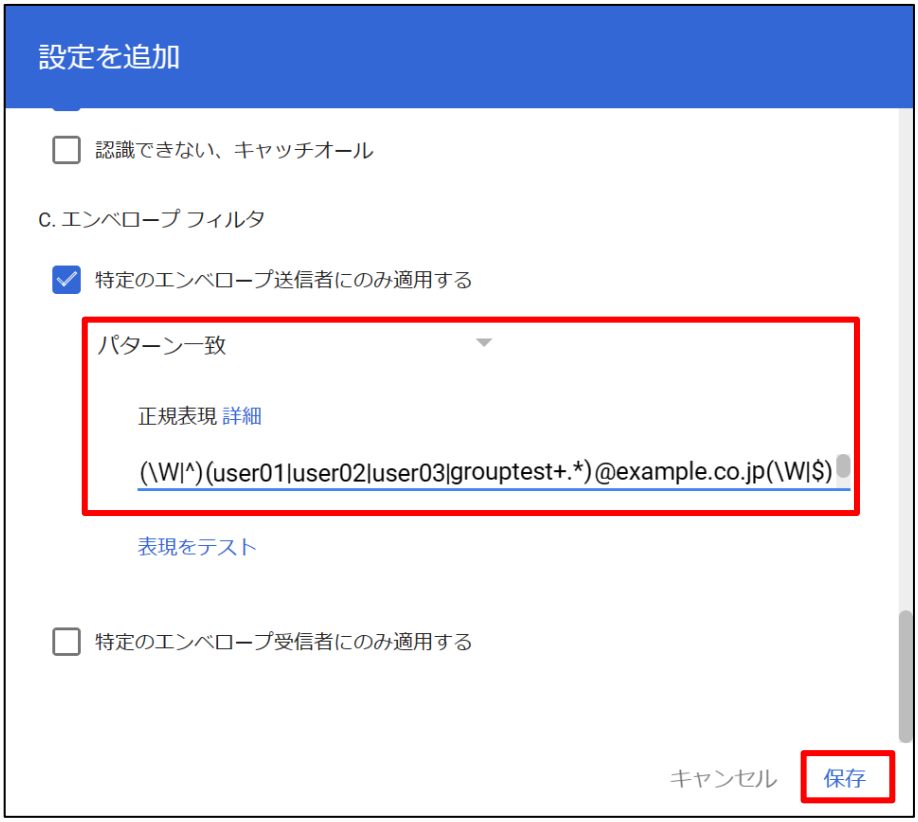
20. 以下のとおりに設定します。

項目	設定値
ユーザー	■
グループ	■

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。



22. 追加されていることを確認します。

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・メールの疎通確認を実施ください。

MailFilter on Cloud をご利用のお客様の場合、添付ファイル送信利用制限機能のデフォルトの設定で社外宛て添付ファイルの送信に制限がかかっております。
添付ファイルを送信するためには制限の解除をするため、［3.2 添付ファイル送信利用制限の解除］の手順を実施いただく必要がございます。
MailFilter on Cloud と MailConvert on Cloud の両方をご利用のお客様は、必ず手順を実施ください。

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

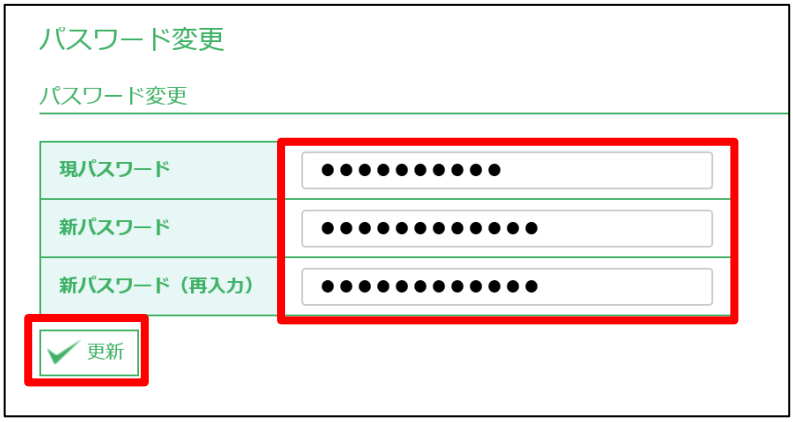
2. ログイン画面が表示されるので、以下の情報を入力し、「ログイン」をクリックします。

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①
パスワード	サービス登録完了書に記載されたアカウント①のパスワード

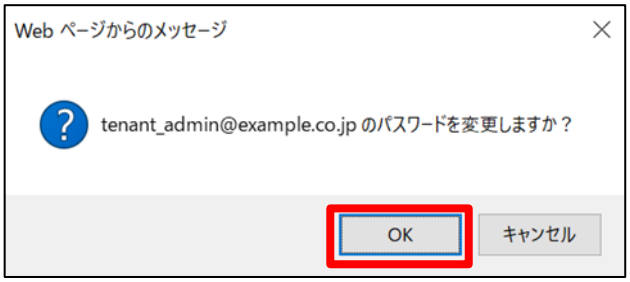
3. ログイン後、右上のアカウント名にカーソルを合わせると、「パスワード変更」が表示されるのでクリックします。

4. パスワード変更画面が表示されます。

   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。



5. 「OK」をクリックします。



6. 「パスワードを変更しました。」と表示されます。

以上で、パスワードの変更は完了です。

3.2 メールの疎通確認

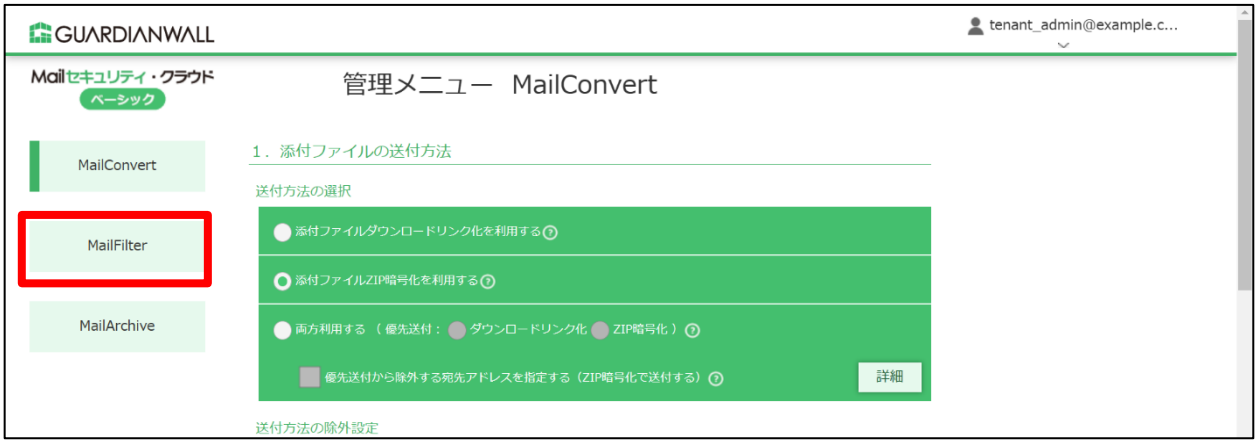
外部へメールを送信し、メールがGUARDIANWALLを経由していることをご確認ください。

なお、MailFilter on Cloudをご利用のお客様の場合、社外宛てに添付ファイルを送信するためには、事前に「添付ファイル送信利用制限機能」の設定を変更する必要がございます。

デフォルトではすべてのファイルの送信を禁止しておりますので、必要に応じて、以下設定をお願いいたします。

> MailFilter on Cloud と MailConvert on Cloud の両方をご利用のお客様は、必ず手順を実施ください。

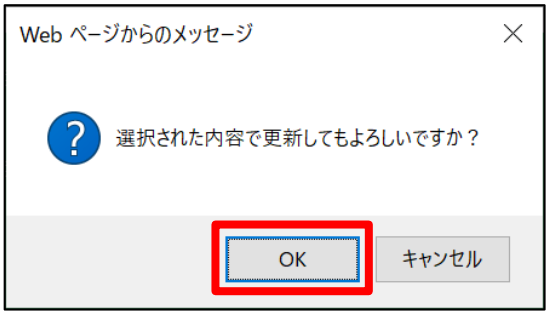
1. 管理画面にログインし、「MailFilter」をクリックします。



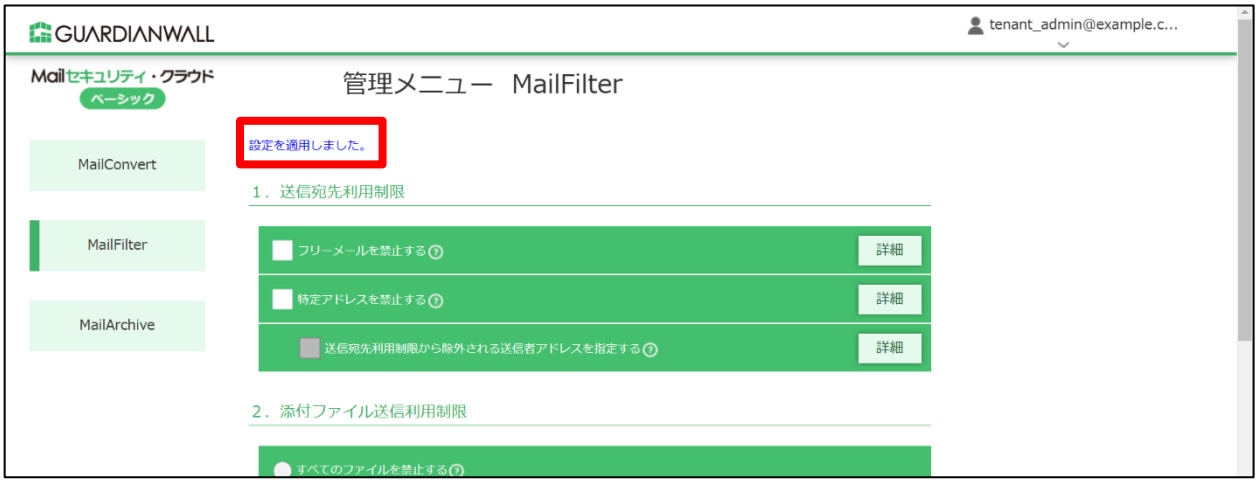
2. 「2.添付ファイル送信利用制限」-「何もしない」にチェックを入れます。

3. 「更新」をクリックします。

4. 「OK」をクリックします。



5. 「設定を適用しました。」と表示されることを確認します。



以上で、設定の変更は完了です。

3.2.1 MailFilter on Cloud をご利用の場合

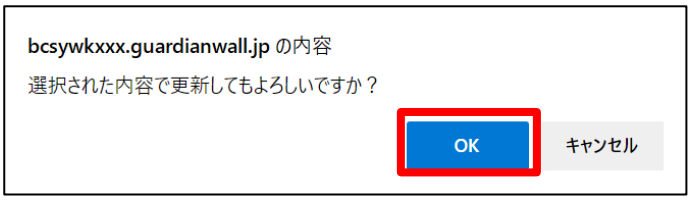
外部向けに送信されたメールについて、送信メールが遅延することを確認します。

1　メール送信遅延ルールの設定

外部へ送信したメールが遅延するよう、ルールを設定します。

1. 管理画面にログインし、「MailFilter」-「送信遅延をセットする」にチェックを入れ、「更新」をクリックします。

2. 「OK」をクリックします。



3. 「設定を適用しました。」と表示されることを確認します。

以上で、ルールの設定は完了です。

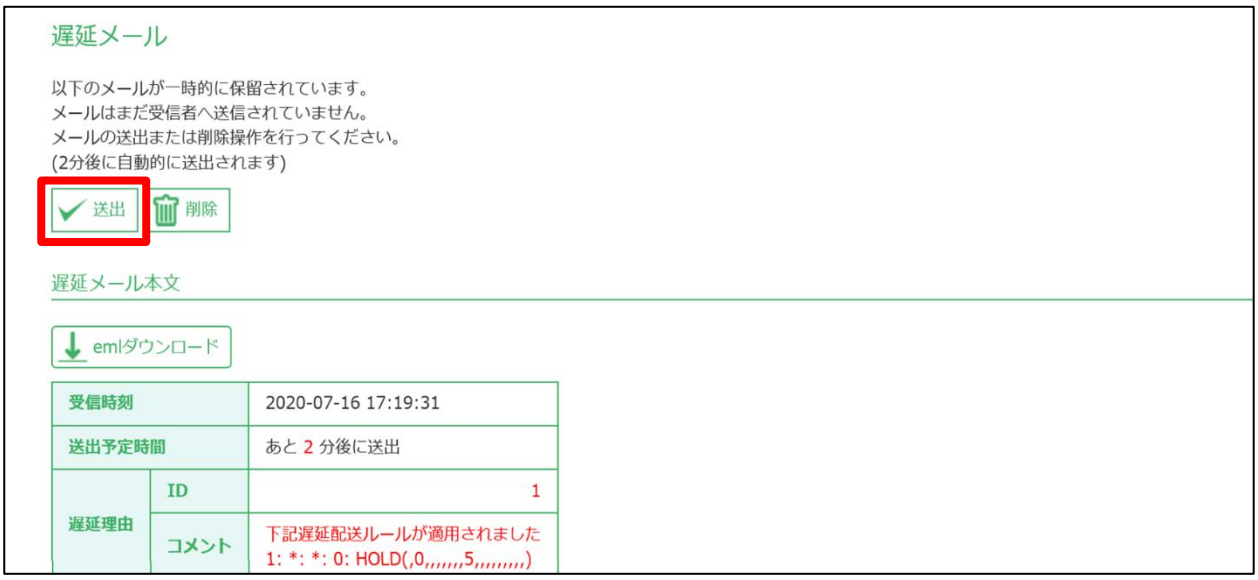
2　テストメールの送信

テストメールを送信し、外部ドメイン宛に送信したメールが遅延されることを確認します。

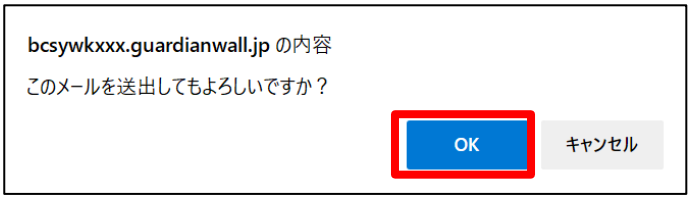
1.　外部ドメイン宛にメールを送信します。

2.　メールが遅延したことを通知するメールが届きます。通知メールに記載の「■保留メールの内容を確認するには以下の URL をクリックしてください。」の下部に記載の URL をクリックします。

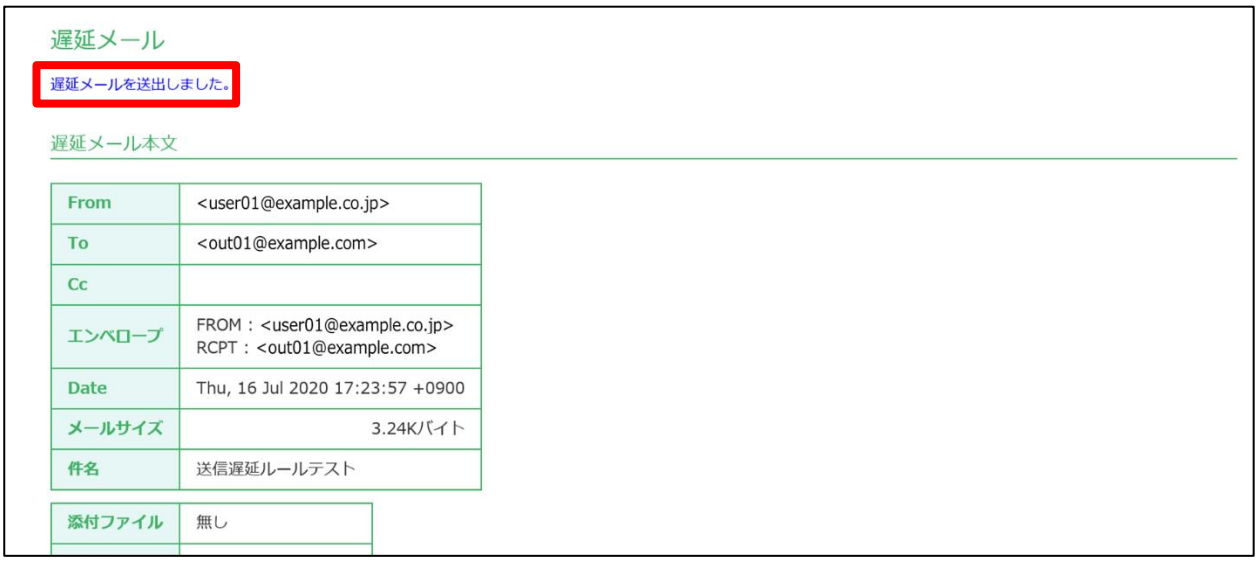
3. メールの内容を確認し、画面上部の「送出」をクリックします。



4. 「OK」をクリックします。

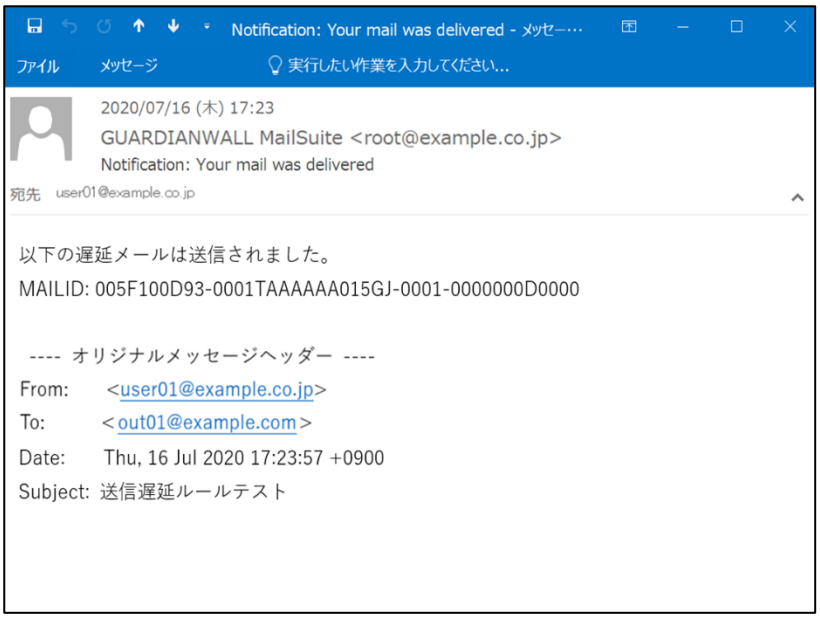


5. 「遅延メールを送出しました。」と表示されることを確認します。



6. 送信されたことを通知するメールが届くことを確認します。

   通知メールが届かない場合、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、MailFilter on Cloud をご利用の場合のメールの疎通確認は完了です。

3.2.2 MailConvert on Cloud をご利用の場合

外部へメールを送信した際に、添付ファイルがダウンロードリンク化されることを確認します。

1　テストメールの送信

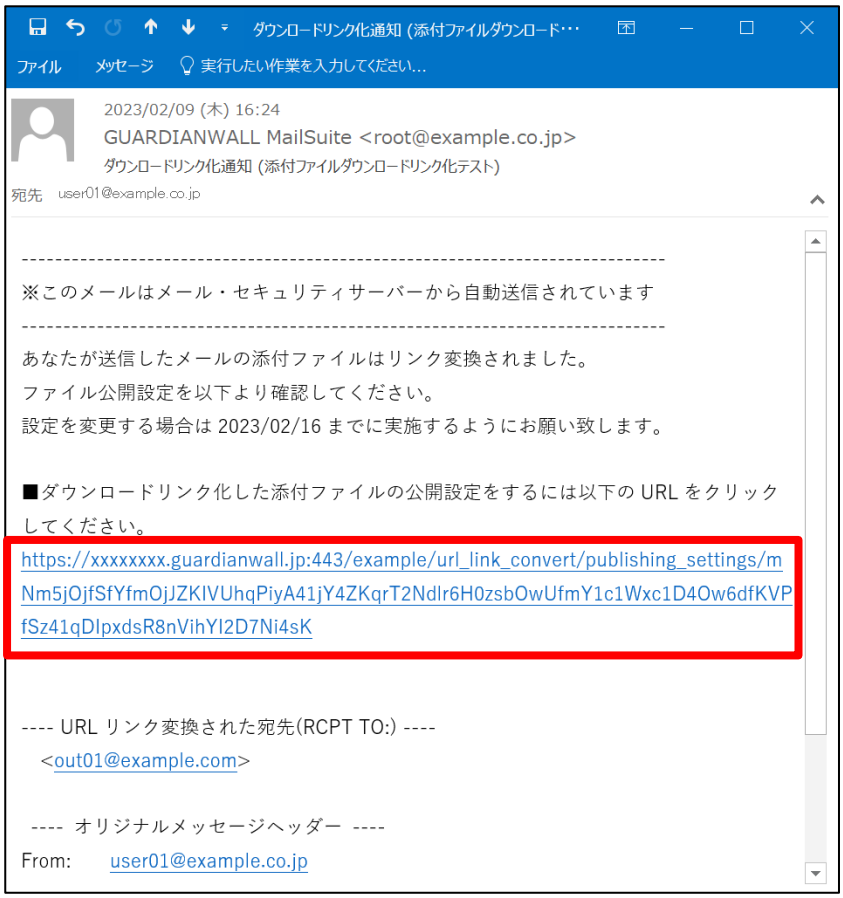
テストメールを送信し、メールの添付ファイルが自動的にダウンロードリンク化されることを確認します。

1.　外部ドメイン宛に添付ファイル付きのメールを送信します。

MailFilter on Cloud もご契約いただいている場合は、メールを送信後、メールが遅延したことを通知するメールと、送信されたことを通知するメールが届きます。
MailFilter on Cloud のメール疎通確認につきましては、[3.2.1 MailFilter on Cloud をご利用の場合]をご参照ください。

2. 送信元にダウンロードリンク化通知メールが届くことを確認します。

通知メールが届かない場合、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、MailConvert on Cloudをご利用の場合のメールの疎通確認は完了です。

3.2.3 MailArchive on Cloud をご利用の場合

メール検索機能を用いて、送受信したメールが検索できることを確認します。

なお、メールのアーカイブの確認は、メールを送信した翌日以降に実施してください。

1　テストメールの送信

外部ドメイン宛にテストメールを予め送信し、宛先に届いていることを確認します。

MailFilter on Cloud もご契約いただいている場合は、メールを送信後、メールが遅延したことを通知するメールと、送信されたことを通知するメールが届きます。
メール送信遅延機能につきましては、[3.2.1 MailFilter on Cloud をご利用の場合]をご参照ください。

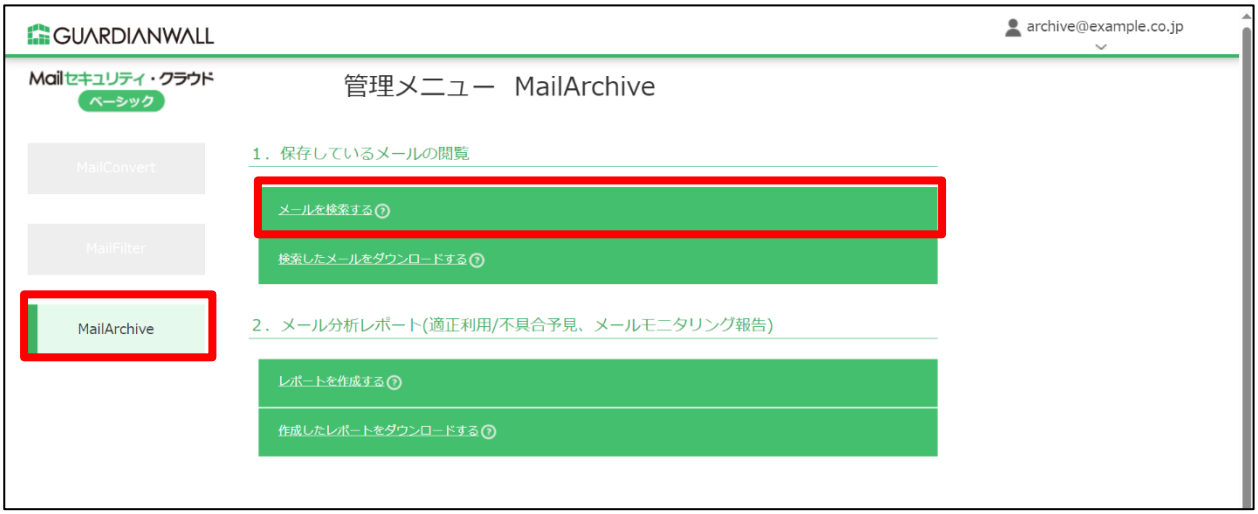
MailFilter on Cloud と MailConvert on Cloud の両方をご利用のお客様は、[3.2 メールの疎通確認] に記載の、添付ファイル送信利用制限機能設定を変更する手順を実施ください。

2　メールアーカイブの検索

メールを送信した翌日以降に、メールの検索ができることを確認します。

Microsoft 365 や Google Workspace 側の仕様として、送信した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。複数に分かれた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。

1.　管理画面にログインし、「MailArchive」-「メールを検索する」をクリックします。



2. メール検索画面に移行後、メールを検索する期間とキーワードを指定して画面下部の「検索」をクリックします。

項目	値
期間	検索したい日時
キーワード	検索したいメールに含まれるキーワード

3. 検索結果が表示されることを確認します。

検索結果が表示されない場合、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、MailArchive on Cloudをご利用の場合の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ございます。

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ございます。

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。

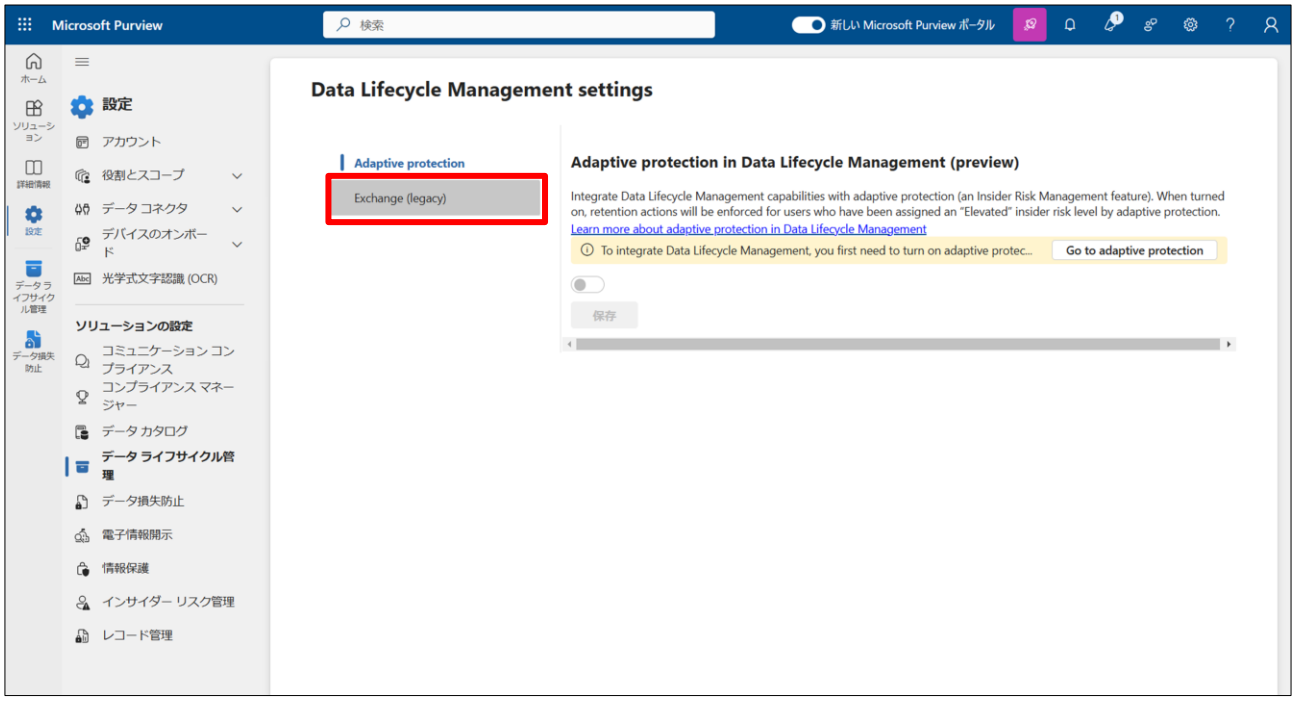
2. 「Microsoft 365 管理センター」の画面に移行後、左側の「≡」をクリックし、「すべてを表示」をクリックします。

3. 「コンプライアンス」をクリックします。

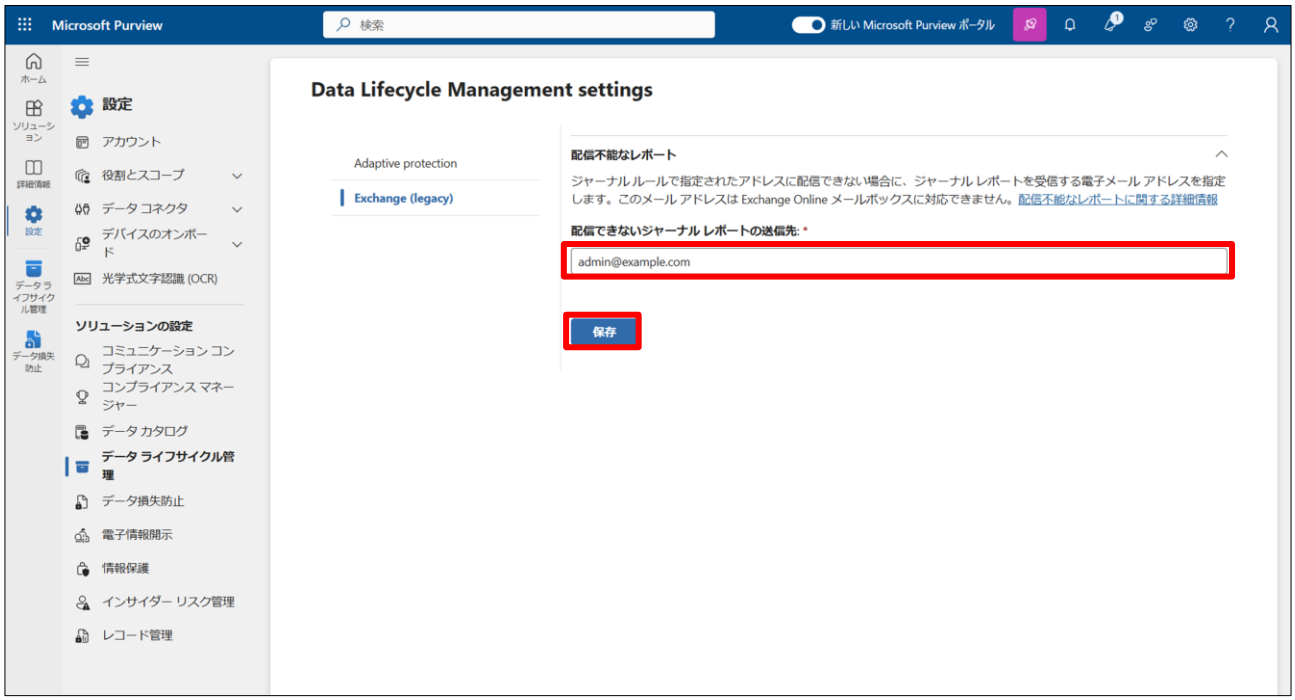
4. 「Microsoft Purview」の画面に移行後、「設定」をクリックします。

5. 「データライフサイクル管理」をクリックします。

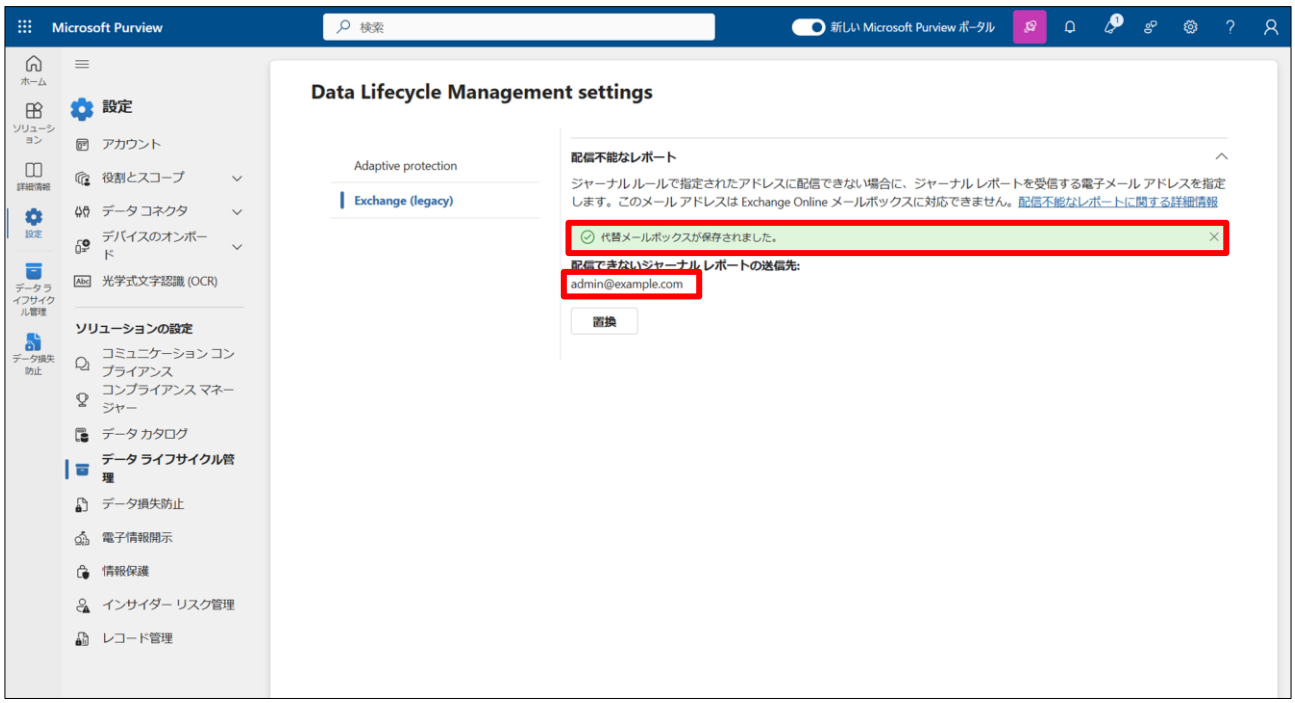
6. 「Exchange（legacy)」をクリックします。



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。

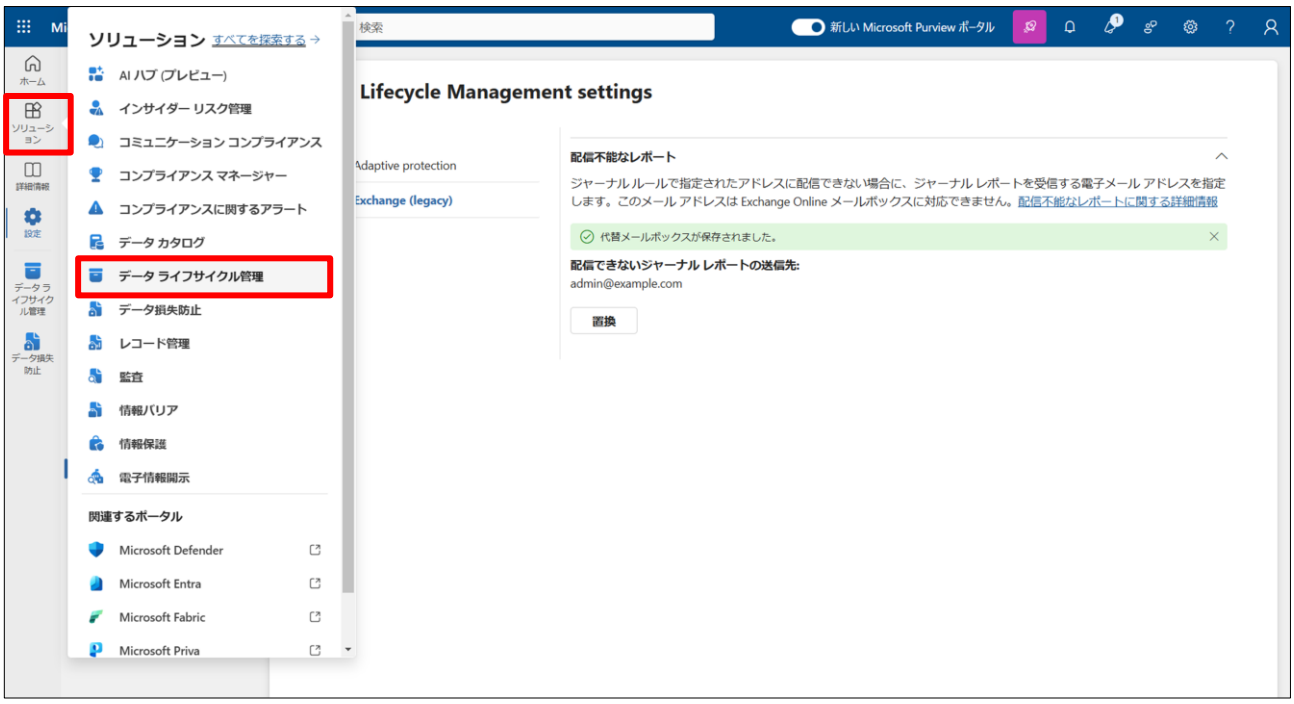


以上で、配信できないジャーナルレポートの送信先の設定は終了です。ジャーナルルールの設定に進みます。

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。

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。

なお、［3.2 メールの疎通確認］にて設定変更した箇所は、ご利用の用途に応じて設定を戻していただきますようお願いいたします。

Mailセキュリティ・クラウドの設定方法につきましては、「ユーザー運用ガイド」をご参照ください。

GUARDIANWALL

Mail セキュリティ・クラウド ベーシック スタートアップガイド

2025 年 3 月 ver.3.10