Office 365 メールボックスのメッセージの自動修復

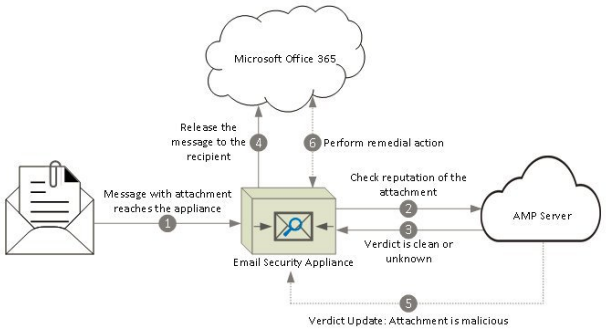
この章は、次の項で構成されています。

脅威の判定が「悪意がある」に変更されたときのエンドユーザに配信されるメッセージに応じた是正措置の実行

ファイルは常に、ユーザのメールボックスに達した後であっても、悪意のあるファイルに変化する可能性があります。AMP は、新しい情報が発生する際にこの変化を識別し、アプライアンスにレトロスペクティブアラートを送信することができます。今回のリリースでは、単なるアラートを超えた機能が提供されます。ご所属の組織がメールボックスの管理に Office 365 を使用している場合、脅威判定が変更されたときにはユーザのメールボックス内のメッセージに対して自動修復アクションを実行するようにアプライアンスの設定を設定することができます。たとえば、添付ファイルに対する判定が「正常」から「悪意がある」に変更されたときには受信者のメールボックスからメッセージを削除するようにアプライアンスを設定することができます。

ワークフロー

図 *1:* メールボックス自動修復ワークフロー



1. 添付ファイル付きメッセージがアプライアンスに到達します。
2. アプライアンスは、添付ファイルのレピュテーションを評価する AMP サーバを照会します。
3. AMP サーバは、判定をアプライアンスに送信します。判定は、[正常（clean）] または [不明（unknown）] です。
4. アプライアンスは、受信者へメッセージをリリースします。
5. 一定期間後に、アプライアンスは、AMP サーバから判定の更新を受け取ります。新しい判定は、[悪意のある（malicious）] です。
6. アプライアンスは、受信者のメールボックスに存在する（悪意のある添付ファイルを含む）メッセージに対し、設定された修復アクションを実行します。

脅威の判定が「悪意がある」に変更されたときにエンドユーザに配信されるメッセージに応じて是正措置を実行する方法

	操作内容	詳細
ステップ 1	前提条件を確認します。	前提条件 （3 ページ）
ステップ 2	Azure AD（Azure 管理ポータル）上のアプリケーションとして、E メールセキュリティ アプライアンスを登録します。	Azure AD 上のアプリケーションとしてのアプライアンスの登録 （4 ページ）
ステップ 3：	アプライアンスで Office 365 メールボックスを設定します。	Cisco E メール セキュリティ アプライアンスでの Office 365 メールボックス設定の構成 （6 ページ）
ステップ 4：	脅威の判定が「悪意がある」に変更された時点でエンド ユーザに送信されるメッセージに対して修復アクションを実行するようにアプライアンスを設定します。	脅威の判定が「悪意がある」に変更されたときのエンドユーザに配信されるメッセージに応じた是正措置の設定 （7 ページ）

前提条件

ファイル レピュテーション サービスとファイル分析サービスの機能キー

次の内容について確認してください。

- ファイル レピュテーション サービスおよびファイル分析サービスの機能キーをお使いのアプライアンスに追加していること。
- アプライアンスでのファイル レピュテーションと分析機能が有効になっている。ファイル レピュテーション フィルタリングとファイル分析を参照してください。

Office 365 アカウント

Azure AD に、アプライアンスを登録する必要がある次のアカウントがあることを確認します。

- Office 365 のビジネス アカウント
- Office 365 のビジネス アカウントに関連付けられた Azure AD サブスクリプション

詳細については、Office 365 のシステム管理者にお問い合わせください。

セキュアな通信の証明書

Office 365 サービスとアプライアンス間の通信をセキュリティで保護するには、自己署名証明書を作成する、または信頼された CA から証明書を取得する方法のいずれかで証明書を設定する必要があります。

次のものが必要です。

- .crt または .p12 形式の公開キー。emailAddress に Office 365 の管理者の電子メール アドレスが設定されていること（<admin_username>@<domain>.com）。
- キーサイズが少なくとも 2048 ビットで、関連付けられた .pem 形式の秘密キー。

（注） パスフレーズを含む秘密キーはこのリリースではサポートされません。

Azure AD 上のアプリケーションとしてのアプライアンスの登録

Office 365 サービスは、ユーザのメールボックスへのセキュアなアクセスを提供する Azure Active Directory（Azure AD）を使用します。Office 365 のメールボックスにアプライアンスがアクセスするには、Azure AD でアプライアンスを登録しなければなりません。Azure AD でアプライアンスを登録するために実行する必要がある手順の概要を次に示します。詳細については、Microsoft のマニュアルを参照してください（https://msdn.microsoft.com/en-us/office/office365/howto/add-common-consent-manually）。

はじめる前に

前提条件 （3 ページ）で説明されている作業を行います。

ステップ 1 Office 365 のビジネス アカウントの資格情報を使用して Azure 管理ポータルにログインします。

ステップ 2 Office 365 のサブスクリプションにリンクされているディレクトリに新しいアプリケーションを追加します。新しいアプリケーションを追加している間に、次のことを確認します。

- WEB APPLICATION や WEB API としてアプリケーションのタイプを選択します。
- 次のパラメータを指定します。
  - サインオンの URL。これは、ユーザがサインインしてアプライアンスを使用する URL で、たとえば、`https://<company_domain.com>/ManualRegistration` などです。
  - App ID の URI。Microsoft Azure AD がアプライアンス用に使用できる一意の URI で、たとえば、`https://<company_domain.com>` などです。

ステップ 3 アプリケーションおよびアプリケーションに必要なアクセス許可を設定します。新しく作成されたアプリケーションの [設定（Configure）] タブの下に、アプリケーションとして Office 365 Exchange Online を追加し、次のアクセス許可を設定します。

- アプリケーションのアクセス許可
  - 任意のユーザとしてのメールの送信
  - すべてのメールボックスのメールの読み取りと書き込み
  - すべてのメールボックスのメールの読み取り
  - すべてのメールボックスへのフル アクセスによる Exchange Web サービスの使用
- 委任管理用のアクセス許可
  - ユーザとしてのメールの送信
  - ユーザのメールの読み取りと書き込み

- ユーザのメールの読み取り
- Exchange Web サービス経由でサインインしているユーザとしてのメールボックスへのアクセス

ステップ 4 パブリックキー証明書からのキー資格情報によりアプリケーション マニフェストを更新して、Office 365 サービスとアプライアンス間の通信を保護します。次の操作を行ってください。

a) Windows PowerShell プロンプトを使用して、パブリックキー証明書から、`$base64Thumbprint`、`$base64Value`、および `$keyid` の値を取得します。次の例を参照してください。

Windows PowerShell プロンプトから公開キー証明書を含むディレクトリに移動し、次を実行します。

例：

```
$cer = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2
$cer.Import(".\mycer.cer")
$bin = $cer.GetRawCertData()
$base64Value = [System.Convert]::ToBase64String($bin)
$bin = $cer.GetCertHash()
$base64Thumbprint = [System.Convert]::ToBase64String($bin)
$keyid = [System.Guid]::NewGuid().ToString()
```

上記のコマンドを実行した後、次のコマンドを実行して、その値を抽出します。

- `$keyid`
- `$base64Value`
- `$base64Thumbprint`

b) Azure 管理ポータルからアプリケーションのマニフェストをダウンロードします。

c) テキスト エディタを使用してダウンロードしたマニフェストを開き、次の JSON で空の KeyCredentials プロパティを置き換えます。

例：

```
"keyCredentials": [
     {
        "customKeyIdentifier" : "$base64Thumbprint_from_step_1",
        "keyId": "$keyid_from_step1",
        "type": "AsymmetricX509Cert",
        "usage": "Verify",
        "value": "$base64Value_from_step1"
     }
],
```

前述の JSON スニペットで、`$base64Thumbprint`、`$base64Value`、および `$keyid` の値を、手順 a で取得した値で置き換えていることを確認します。各値は 1 行で入力する必要があります。

d) 変更を保存し、変更したマニフェストを Azure 管理ポータルにアップロードします。

ステップ 5 アプライアンスを Azure AD に登録した後で、Azure 管理ポータルから次の詳細を書き留めてください。

- [設定（Configure）] タブのクライアント ID。
- [ビューエンドポイント（View Endpoints）]>[アプリケーションエンドポイント（App Endpoints）] ページのテナント ID。テナント ID は、このページに記載されているすべての URL で使用できる一意の値です。たとえば、このページに記載されている次のような URL です。
  - https://login.microsoftonline.com/abcd1234-bcdd-469d-8545-a0662708cbc3/federationmetadata/2007-06/federationmetadata.xml

- https://login.microsoftonline.com/abcd1234-bcdd-469d-8545-a0662708cbc3/wsfed
- https://login.microsoftonline.com/abcd1234-bcdd-469d-8545-a0662708cbc3/saml2

この例では、テナント ID は abcd1234-bcdd-469d-8545-a0662708cbc3 です。

Cisco E メール セキュリティ アプライアンスでの Office 365 メールボックス設定の構成

はじめる前に

次の内容について確認してください。

- アプライアンスでのファイル レピュテーションと分析機能が有効になっている。ファイル レピュテーション フィルタリングとファイル分析を参照してください。
- .pem 形式の証明書の秘密キーを取得します。セキュアな通信の証明書 （3 ページ）を参照してください。
- 次のパラメータの値です。
  - Azure 管理ポータルで登録したアプリケーションのクライアント ID とテナント ID。Azure AD 上のアプリケーションとしてのアプライアンスの登録 （4 ページ）のステップ 5 を参照してください。
  - 証明書サムプリント（$base64Thumbprint）。Azure AD 上のアプリケーションとしてのアプライアンスの登録 （4 ページ）のステップ 4 を参照してください。

ステップ 1 アプライアンスへのログイン

ステップ 2 [システム管理（System Administration）] > [メールボックス設定（Mailbox Settings）] をクリックします。

ステップ 3 [有効（Enable）] をクリックします。

ステップ 4 [Office 365 メールボックス設定を有効にする（Enable Office 365 Mailbox Settings）] を選択します。

ステップ 5 次の詳細を入力します。

- Azure 管理ポータルで登録したアプリケーションのクライアント ID とテナント ID。
- 証明書のサムプリント（$base64Thumbprint の値）。

ステップ 6 証明書の秘密キーをアップロードします。[ファイルの選択（Choose File）] をクリックして、.pem ファイルを選択します。

ステップ 7 変更を送信し、保存します。

ステップ 8 アプライアンスが Office 365 サービスに接続できるかどうかを確認します。

1. [接続の確認（Check Connection）] をクリックします。
2. Office 365 の電子メール アドレスを入力します。これは Office 365 ドメインで有効な電子メール アドレスでなければなりません。
3. [テスト接続（Test Connection）] をクリックします。

ポップアップで、アプライアンスが Office 365 サービスに接続できるかどうかが表示されます。接続できない場合は、次を確認します。

- クライアント ID、テナント ID、およびサムプリントが正しい。
- アップロードした秘密キーが正しく、有効期限が切れていない。

脅威の判定が「悪意がある」に変更されたときのエンドユーザに配信されるメッセージに応じた是正措置の設定

はじめる前に

アプライアンスで Office 365 メールボックスの設定が構成済みであることを確認します。Cisco E メール セキュリティ アプライアンスでの Office 365 メールボックス設定の構成 （6 ページ）を参照してください。

ステップ 1 [メールポリシー（Mail Policies）] > [受信メールポリシー（Incoming Mail Policies）] を選択します。

ステップ 2 変更するメール ポリシーの [高度なマルウェア防御（Advanced Malware Protection）] カラム内のリンクをクリックします。

ステップ 3 [メールボックス自動修復の有効化（Enable Mailbox Auto Remediation）] を選択します。

ステップ 4 脅威の判定が悪意に変更されたときにエンドユーザに配信されたメッセージ基づいて実行するアクションを指定します。要件に応じて、次のいずれかの修復アクションを選択します。

- [電子メール アドレスに転送（Forward to an email address）]。指定したユーザ（たとえば、電子メール管理者など）に悪意のある添付ファイルを転送する場合は、このオプションを選択します。
- メッセージを削除します。悪意のある添付ファイルをエンドユーザのメールボックスから完全に削除する場合は、このオプションを選択します。
- [指定した電子メール アドレスに転送してメッセージを削除（Forward to an email address and delete the message）]。指定したユーザ（たとえば、電子メール管理者など）に悪意のある添付ファイルを転送して、悪意のある添付ファイルをエンドユーザのメールボックスから完全に削除する場合は、このオプションを選択します。

（注） Office 365 サービスでは特定のフォルダからのメッセージの削除をサポートしていないため、それらのフォルダ（[削除済みアイテム（Deleted Items）] など）からメッセージを削除することはできません。

ステップ 5 変更を送信し、保存します。

メールボックス修復結果のモニタリング

[メールボックスの自動修復レポート（Mailbox Auto Remediation report）] ページを使用して（[モニタ（Monitor）] > [メールボックスの自動修復（Mailbox Auto Remediation）]）、メールボックス修復結果の詳細を表示できます。このレポートを使用して次の詳細を表示します。

- 受信者のメールボックス修復の成功または失敗を示す一覧
- メッセージに対してとられる修復のアクション

- SHA-256 ハッシュに関連付けられているファイル名

[修復が失敗した受信者（Recipients for whom remediation was unsuccessful）] フィールドは、次のシナリオで更新されます。

- 受信者が有効な Office 365 ユーザではない、または受信者がアプライアンスで構成されている Office 365 ドメイン アカウントに属していない。
- 添付ファイルを含むメッセージをメールボックスで使用できない。たとえば、エンドユーザがメッセージを削除した。
- アプライアンスが設定済みの修復のアクションを実行しようとしたときにアプライアンスと Office 365 サービス間の接続に問題があった。

メッセージ トラッキングに関連メッセージを表示するには、SHA-256 ハッシュをクリックします。

メッセージトラッキングでのメールボックス修復の詳細の表示

メッセージ トラッキングでメールボックス修復の詳細を表示するには、

- メッセージトラッキングが有効になっている必要があります。参照先：メッセージトラッキング
- Office 365 メールボックス設定（[システム管理（System Administration）]>[メールボックスの設定（Mailbox Settings）]）を設定する必要があります。Cisco E メール セキュリティ アプライアンスでの Office 365 メールボックス設定の構成 （6 ページ）を参照してください。
- メールボックスの修復アクション（[セキュリティサービス（Security Services）]>[メールボックス自動修復（Mailbox Auto Remediation）]）を設定する必要があります。脅威の判定が「悪意がある」に変更されたときのエンドユーザに配信されるメッセージに応じた是正措置の設定 （7 ページ）を参照してください。

表示されるデータの詳細については、メッセージ トラッキングの詳細 を参照してください。

メールボックス修復のトラブルシューティング

アプライアンスと Office 365 サービスとの間の接続を確認できない

問題

[メールボックスの設定（Mailbox Settings）] ページ（[システム管理（System Administration）]>[メールボックスの設定（Mailbox Settings）]）でアプライアンスと Office 365 サービスとの間の接続を確認中に、エラー メッセージ「接続に失敗しました（`Connection Unsuccessful`）」を受け取ります。

ソリューション

サーバからの応答に応じて、次のいずれかを実行します。

エラー メッセージ	理由とソリューション
`The SMTP address has no mailbox associated with it`	Office 365 ドメインの一部ではない電子メール アドレスを入力しました。 有効な電子メール アドレスを入力して、接続を再度確認します。
`Application with identifier '<client_id>' was not found in the directory <tenant_id>`	無効なクライアント ID を入力しました。 [メールボックスの設定（Mailbox Settings）] ページで、クライアント ID を変更し、接続を再度確認します。
`No service namespace named '<tenant_id>' was found in the data store.`	無効なテナント ID を入力しました。 [メールボックスの設定（Mailbox Settings）] ページで、テナント ID を変更し、接続を再度確認します。
`Error validating credentials. Credential validation failed`	無効な証明書サムプリントを入力しました。 [メールボックスの設定（Mailbox Settings）] ページで、証明書サムプリントを変更し、接続を再度確認します。
`Error validating credentials. Client assertion contains an invalid signature.`	誤った証明書サムプリントを入力したか、または無効なあるいは誤った証明書秘密キーをアップロードしました。 以下を確認します。 • 正しいサムプリントを入力しました。 • 正しい証明書の秘密キーをアップロードしました。 • 証明書の秘密キーは有効期限が切れていません。 • アプライアンスの時間帯は、証明書の秘密キーの時間帯と一致します。

ログの表示

メールボックスの修復情報は、次のログに書き込まれます。

- メール ログ（mail_logs）。メールボックスの修復プロセスの開始時刻は、このログに転記されます。
- メールボックスの自動修復ログ（mar）。修復状態、実行された操作、エラーに関連する情報などがこのログに転記されます。

アラート

アラート：検出されたアプライアンスと Office 365 サービスとの間の接続の問題

問題

アプライアンスと Office 365 サービスとの間の接続の問題があり、構成された是正措置をアプライアンスが実行できないことを示す情報レベルのアラートを受け取ります。

ソリューション

次の手順を実行します。

- アプライアンスと Office 365 サービスとの間の通信を妨げる可能性のあるネットワークの問題を確認します。

  アプライアンスのネットワーク設定を確認します。ネットワーク設定値の変更を参照してください。

- ファイアウォールの問題を確認します。参照先： ファイアウォール情報
- Office 365 サービスが動作するかどうかを確認します。

設定された是正措置が実行されない

問題

AMP サーバからレトロスペクティブ アラートを受信した後、設定済みの修復アクションが Office 365 メールボックス内の悪意のあるメッセージで実行されません。

ソリューション

次の手順を実行します。

- アプライアンスと Office 365 サービス間の接続をテストします。Cisco E メール セキュリティ アプライアンスでの Office 365 メールボックス設定の構成 （6 ページ）のステップ 8 を参照してください。
- 次のアラートを受信しているかどうかを確認してください。「アプライアンスと Office 365 サービスの間の接続の問題が検出されました。（Connectivity Issues Between Appliance and Office 365 Services Detected.）」アラート （10 ページ）を参照してください。