



JATP環境構築マニュアル

03.EMAIL COLLECTOR編

ジュニパーネットワークス株式会社

2018年8月28日

JUNIPER
NETWORKS | Engineering
Simplicity

はじめに

- ・ 本資料にある内容は、資料作成時点におけるものであり、事前の予告なしに内容を変更する場合があります。
- ・ 本資料は内容の正確さを保つために努めて作成しておりますが、本資料を利用することによって生じた損害について、当社は一切責任を負わないものとします。
- ・ また、本資料の内容と公式情報との間に差分がある場合、公式情報を正としてお取り扱いください。
- ・ 本資料は下記のソフトウェア/サービスを用いてJATPのセットアップを行っています。
 - JATP(OVA版/OVF版) v5.0.2
 - ESXi/vCenter Server 5.5
 - G Suite,Office 365(※2018年7月時点)

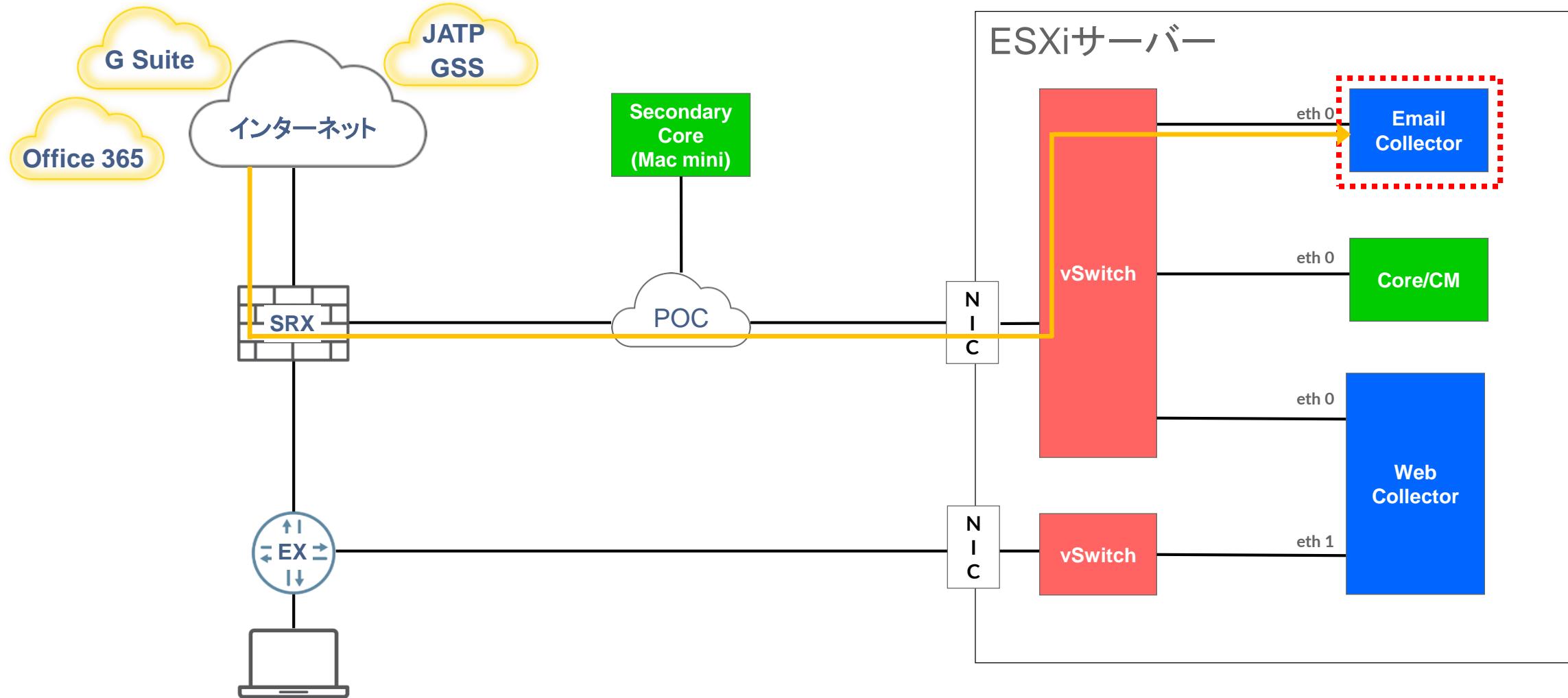
更新履歴

| バージョン | 更新日 | 更新内容 |
|-------|------------|-----------------|
| 1.0 | 2018/08/28 | 初版公開 |
| 1.1 | 2019/07/30 | マニュアルのフォーマットを変更 |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

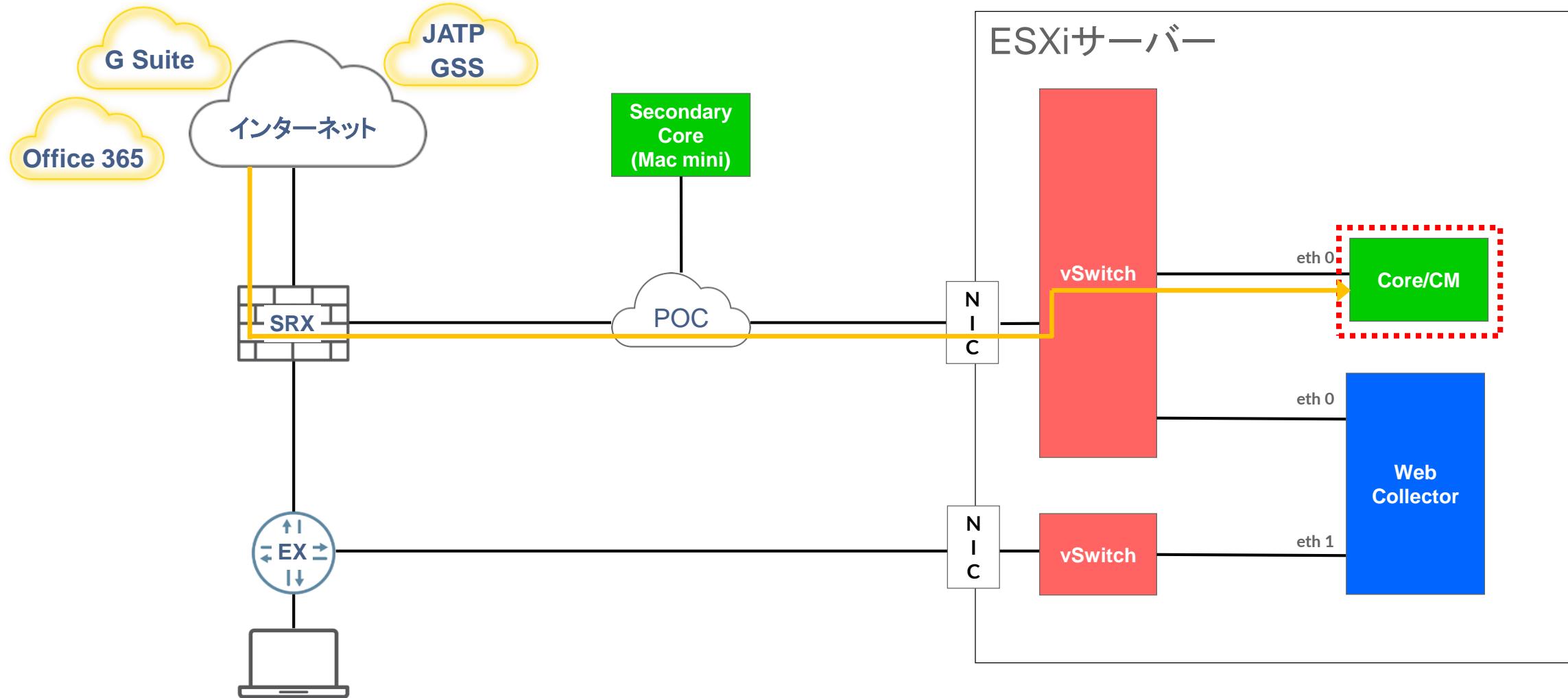
アジェンダ

- 仮想サーバー設定手順(OVAファイル)
- 仮想サーバー設定手順(OVFファイル)
- Email Collectorコマンド一例
- Email Collector設定手順(BCC)
- Email Collector設定手順(MTA Receiver)
- Office 365 ジャーナル設定手順(BCC,MTA Receiver)
- Office 365 Mitigation設定手順(BCC,MTA Receiver)
- G Suite ジャーナル設定手順(BCC,MTA Receiver)
- Gmail セキュリティ設定の変更(BCC)
- G Suite Mitigation設定手順(BCC,MTA Receiver)
- Email Collector動作確認手順

構成イメージ① : MTA RECEIVER



構成イメージ② : BCC, MTA RECEIVER



EMAIL COLLECTOR モードについて

- JATPのEmail Collectorは下記2つのモードがあります。
 - MTA Receiver
Office 365, G Suiteといった外部メールサーバーからJATP宛にメールコピーを送る方式です。
Email CollectorはMTA(Mail Transfer Agent)として動作します。
 - BCCアカウント
Office 365, G Suiteといった外部メールサーバーに保存されているメールをJATPから取得しに行く方式です。
Email CollectorはMUA(Mail User Agent)として動作します。

MTA RECEIVERとBCCアカウント比較

| | MTA Receiver | BCCアカウント |
|------------------|--|--|
| 性能 | 最大 2.4M messages/day | 最大 50K messages/day |
| 通信要件 | 外部サーバーから内部のEmail Collector宛のSMTPを許可する必要あり (Email CollectorにグローバルIPを割り当てるか、ファイアーウォール等でDst NATする必要あり) | 内部から外部サーバーへのIMAP/POP等を許可する必要あり (CoreにプライベートIPを割り当てる場合は、ファイアーウォール等でSrc NATする必要あり) |
| ライセンス | エンタープライズライセンスが必要 | スタンダートライセンスで対応 (エンタープライズライセンス不要) |
| 専用のメールアカウント／ボックス | 不要 | 必要 BCCアカウント用のメールボックスのサイズに注意 O365の場合、ジャーナルの送り先を外部にしなければならない。 (同一ドメインのメールボックスを指定できない) |

EMAIL COLLECTORの構成について

- Email Collectorには、下記2通りの構成があります。

- Collector専用仮想サーバーを使用する (構成イメージ①)

(※Collector専用仮想サーバーはMTA Receiverとしてのみ動作します)

OVAファイルを使用する (※vCenter Serverが必要)

⇒次ページ以降を参照

OVFファイルを使用する

⇒仮想サーバー設定手順(OVFファイル)を参照

- CoreをEmail Collectorとして使用する (構成イメージ②)

⇒Email Collector設定手順(BCC)

もしくはEmail Collector設定手順(MTA Receiver)を参照

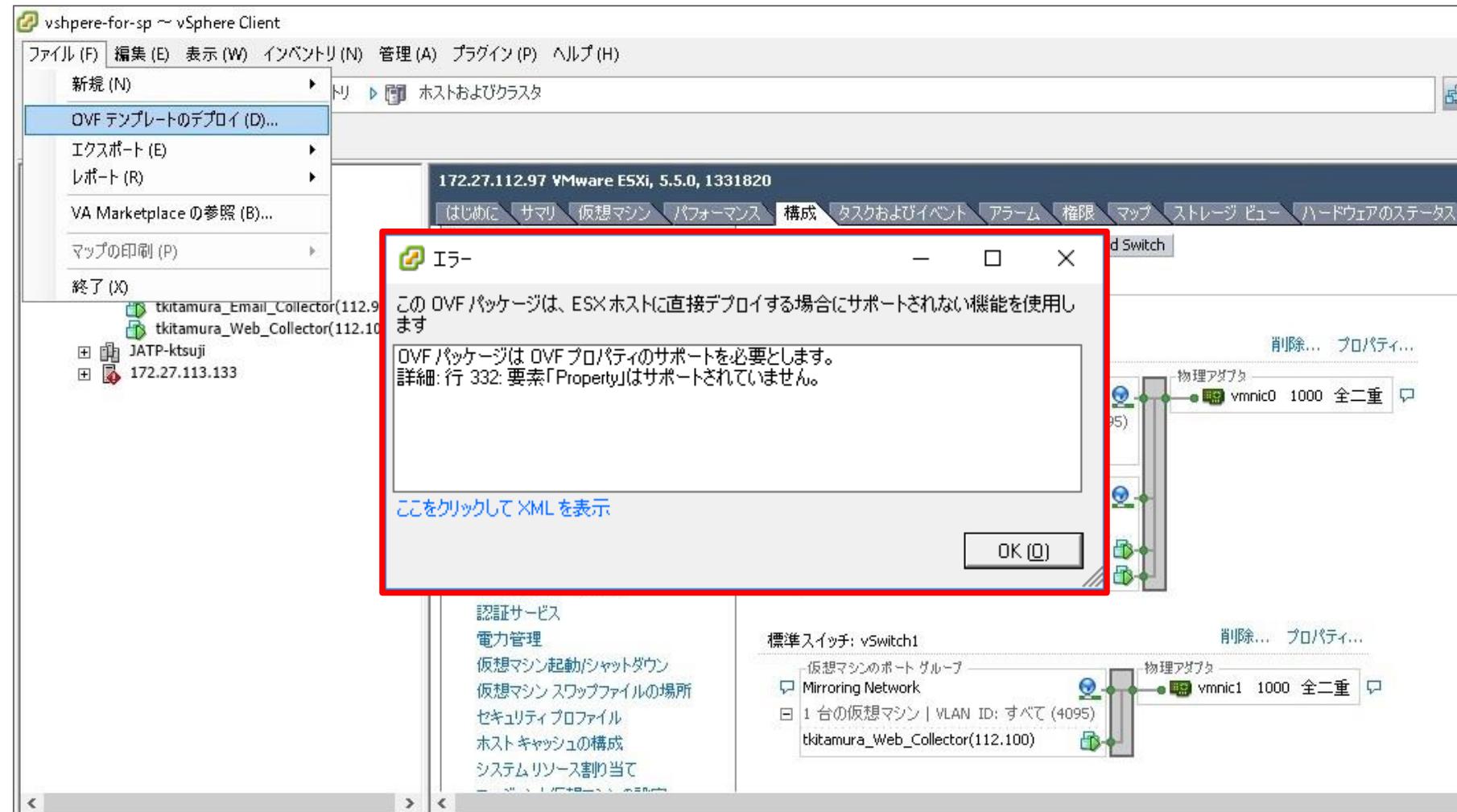


仮想サーバー設定手順 OVAファイル

仮想サーバー設定手順(OVAファイル)



仮想サーバー設定手順(OVAファイル) エラー表示一例



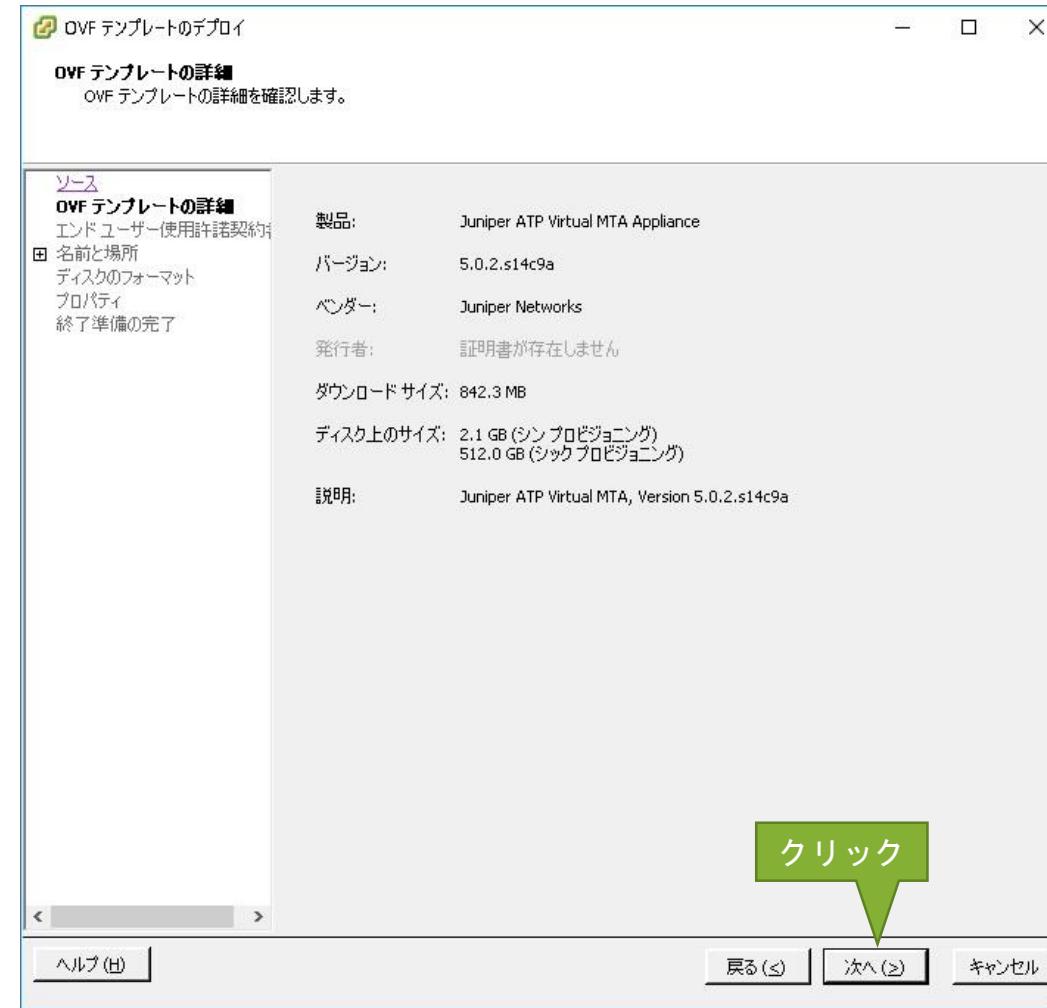
仮想サーバー設定手順(OVAファイル)



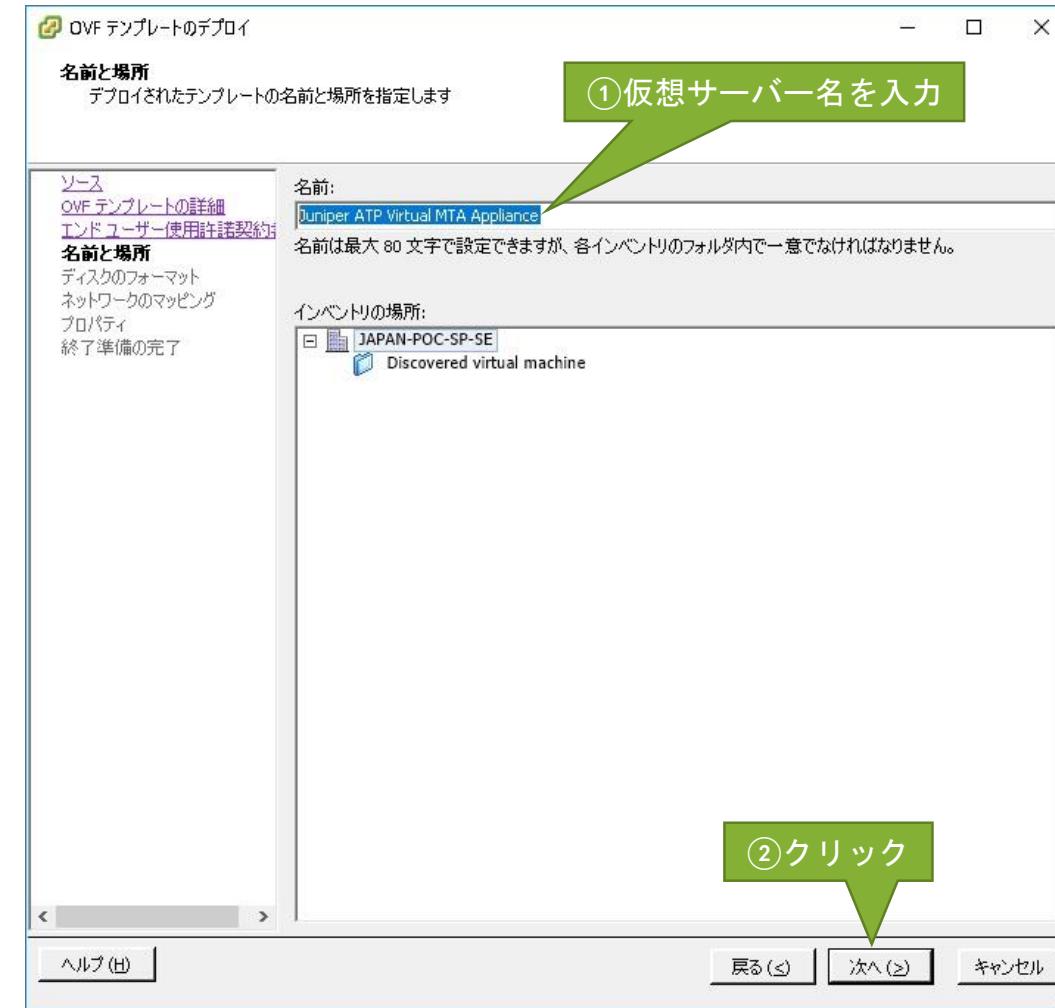
仮想サーバー設定手順(OVAファイル)



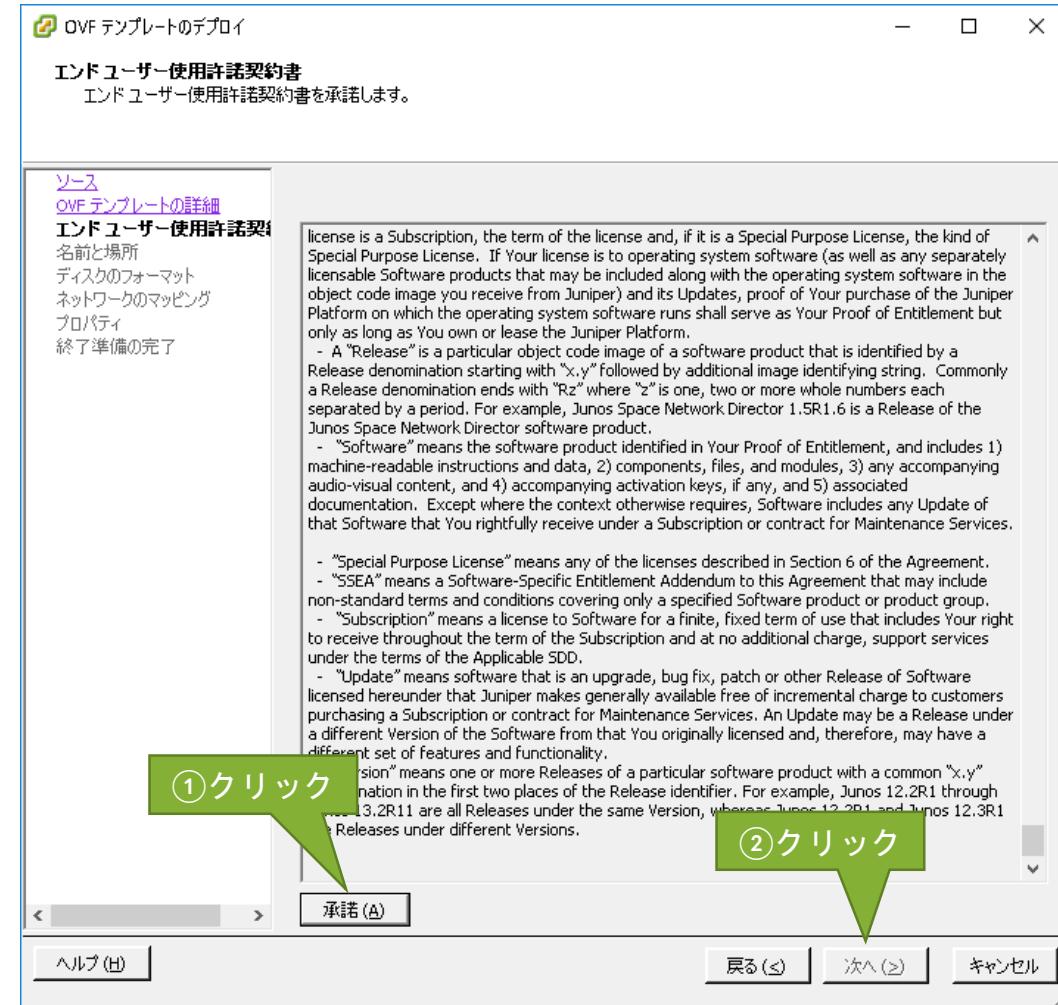
仮想サーバー設定手順(OVAファイル)



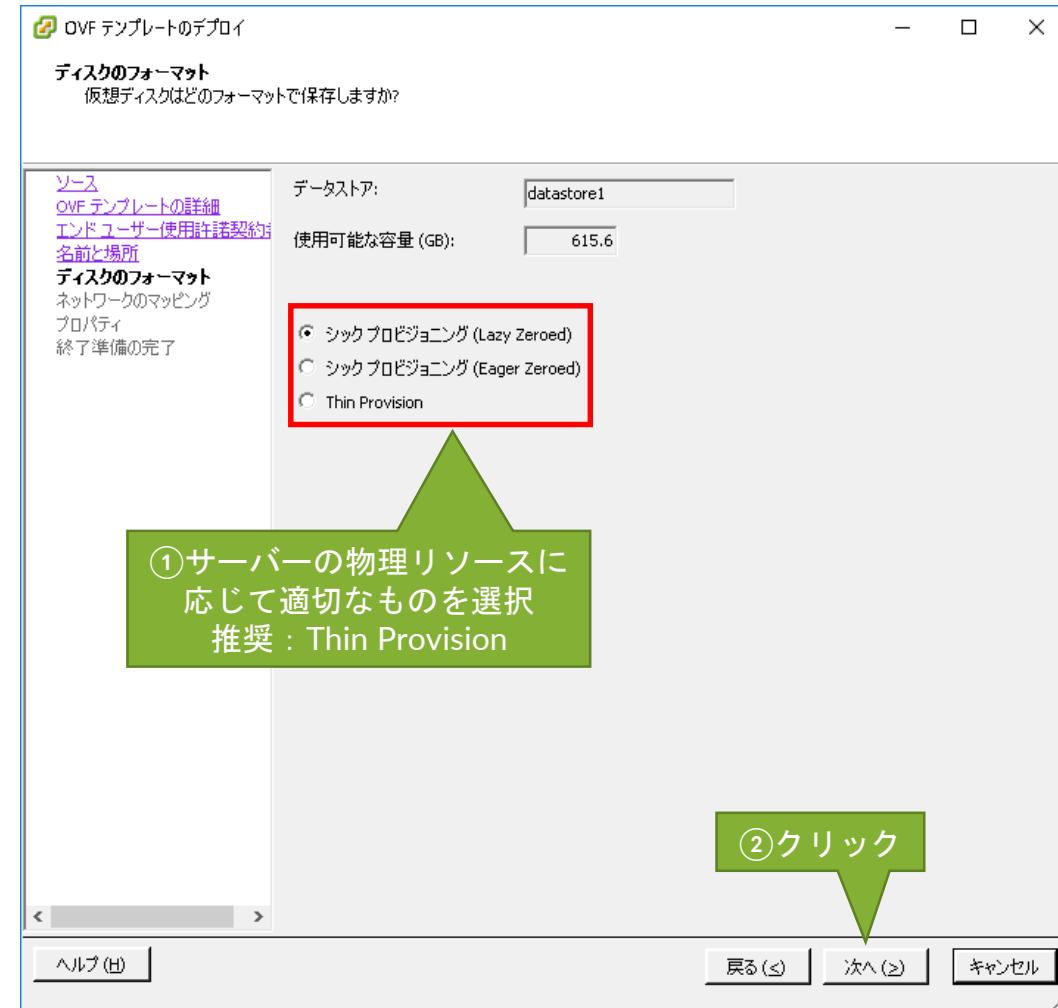
仮想サーバー設定手順(OVAファイル)



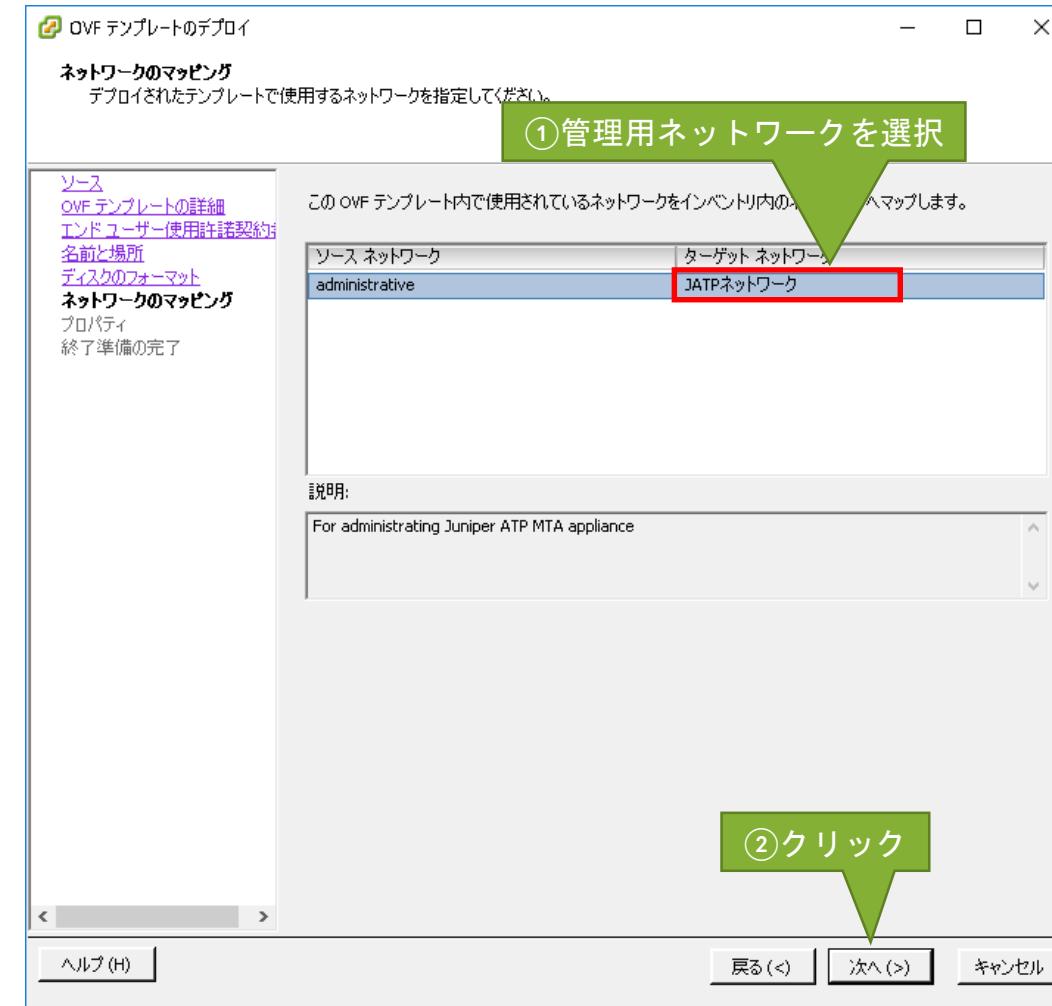
仮想サーバー設定手順(OVAファイル)



仮想サーバー設定手順(OVAファイル)



仮想サーバー設定手順(OVAファイル)



仮想サーバー設定手順(OVAファイル)

Juniper ATP Virtual Core Network Settings

IP Allocation Policy
DHCP

IP address
Ignore this property if the IP allocation policy is DHCP.
0 . 0 . 0 . 0

Netmask
Ignore this property if the IP allocation policy is DHCP.
255 . 255 . 255 . 255

Gateway
Ignore this property if the IP allocation policy is DHCP.
0 . 0 . 0 . 0

DNS address 1
Ignore this property if the IP allocation policy is DHCP.
0 . 0 . 0 . 0

DNS address 2
Ignore this property if the IP allocation policy is DHCP.
0 . 0 . 0 . 0

Search domain
Multiple search domains separated by space.
[empty input field]

Hostname
[empty input field]

1 から 255 の文字の文字列の値を入力してください。

DHCP / Staticを選択
仮想サーバーのIPアドレスの設定
サブネットマスクの設定
ゲートウェイの設定
DNS1の設定
DNS2の設定(任意)
検索用ドメイン名の設定(任意)
サーバーのホストネームの設定

仮想サーバー設定手順(OVAファイル)

Juniper ATP Collector Settings

New CLI admin password

パスワードの入力 adminログインパスワードの設定

パスワードの確認

Juniper ATP Central Manager IP address

Core/CMのIPアドレスを入力

IP アドレスを入力します。

Device name

デバイスネームの設定

1 から 255 の文字の文字列の値を入力してください。

Device description

デバイスの説明

1 から 255 の文字の文字列の値を入力してください。

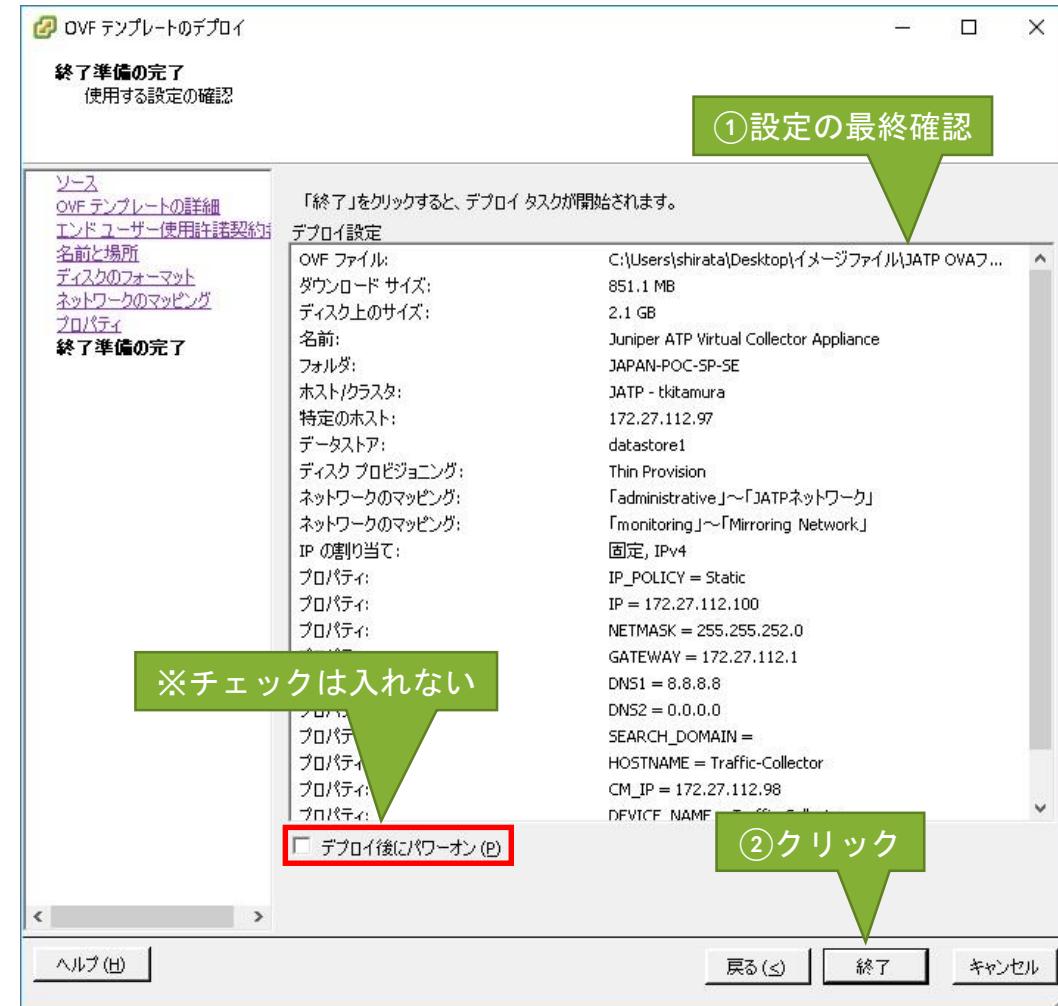
Device key passphrase

パスワードの入力 接続するCore,Collectorで

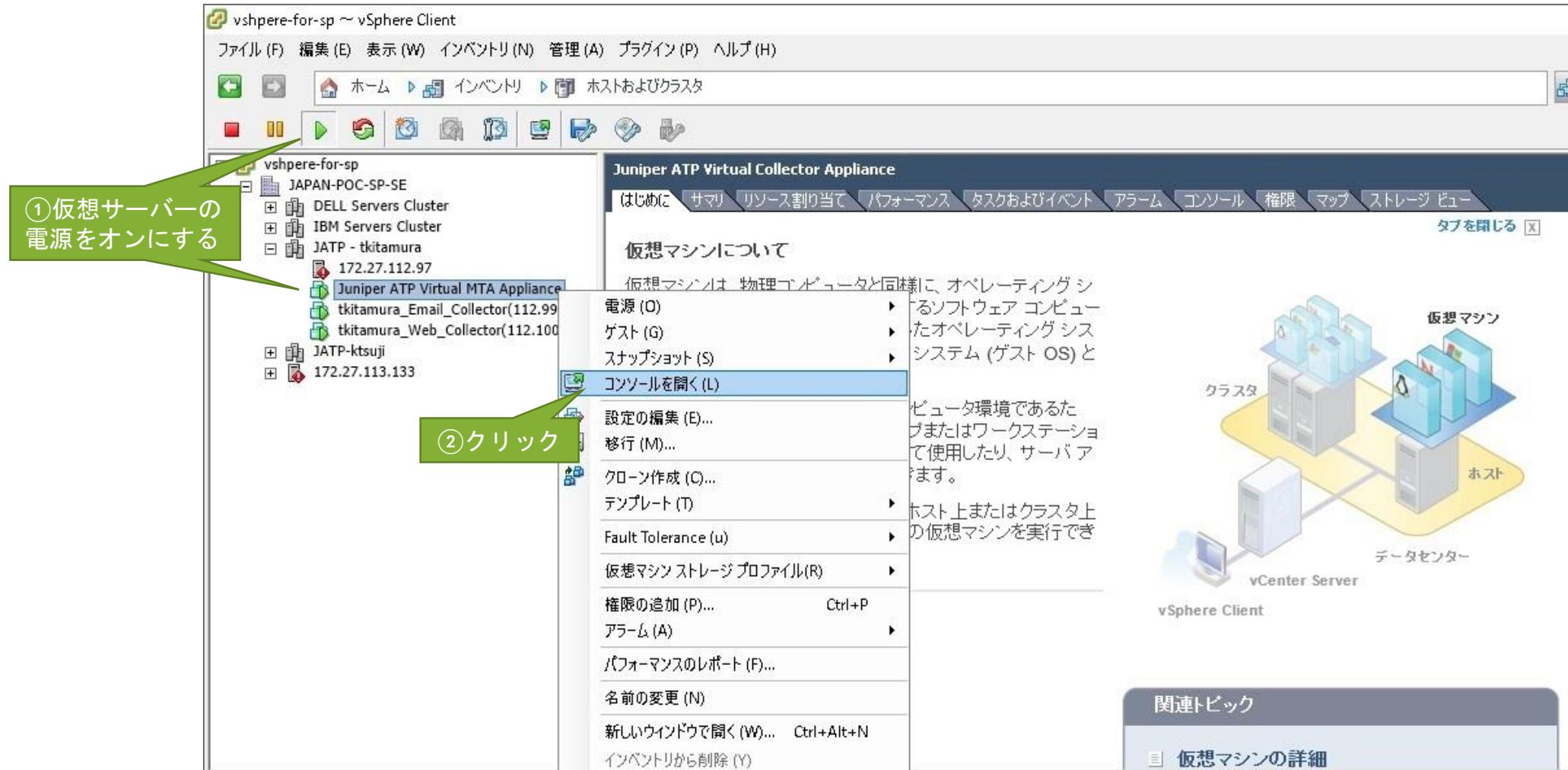
パスワードの確認 すべて共通の値を入力

無効な値を持つプロパティは割り当てられません。すべてのプロパティの値が有効になるまで vApp をパワーオンすることはできません。

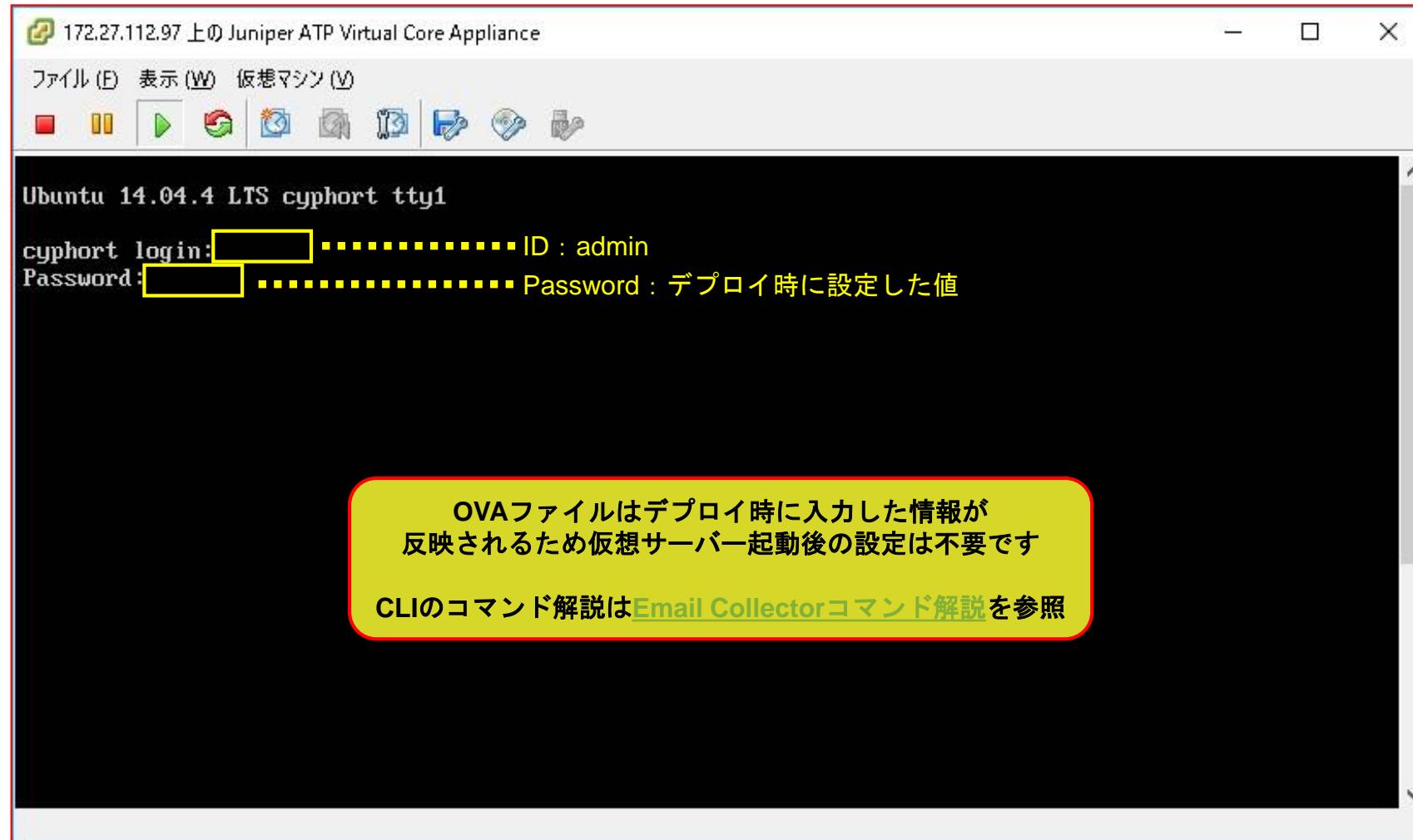
仮想サーバー設定手順(OVAファイル)



仮想サーバー設定手順(OVAファイル)



仮想サーバー設定手順(OVAファイル)





仮想サーバー設定手順 OVFファイル

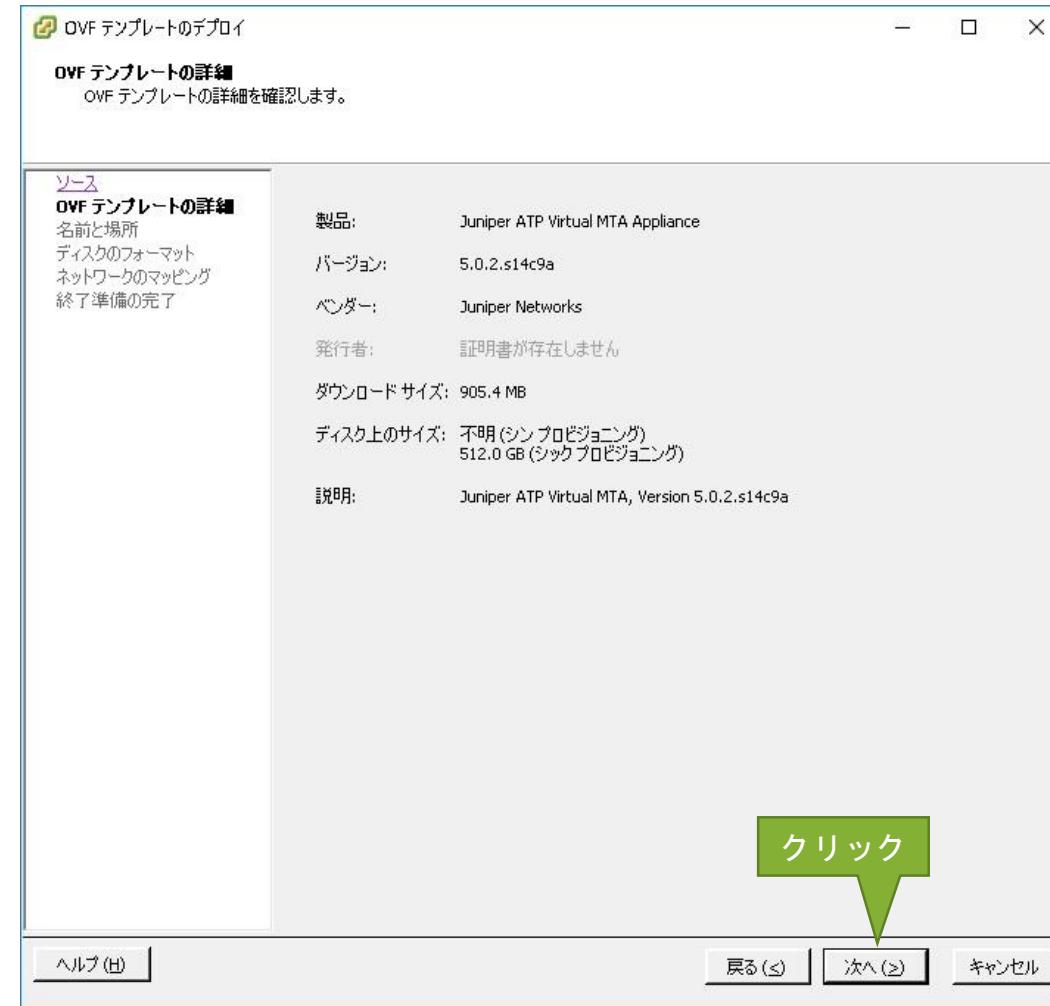
仮想サーバー設定手順(OVFファイル)



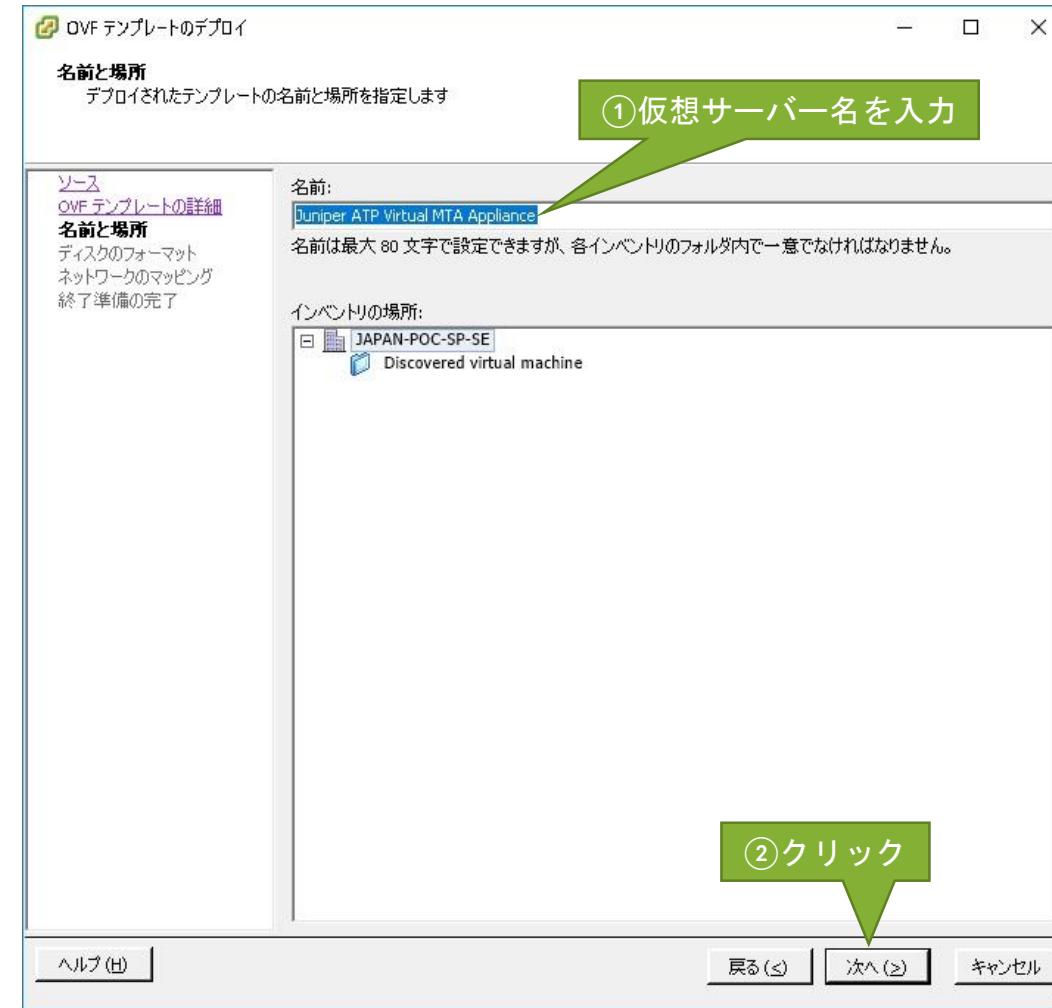
仮想サーバー設定手順(OVFファイル)



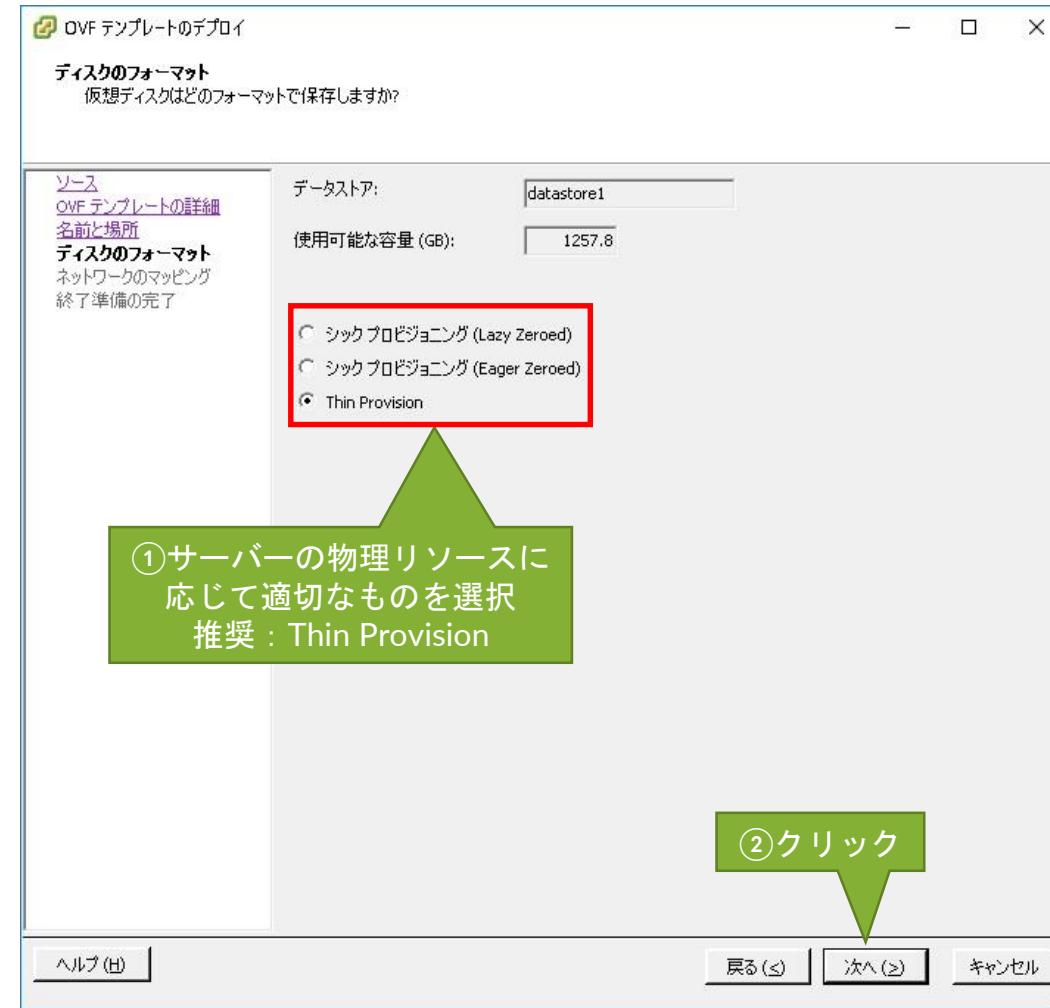
仮想サーバー設定手順(OVFファイル)



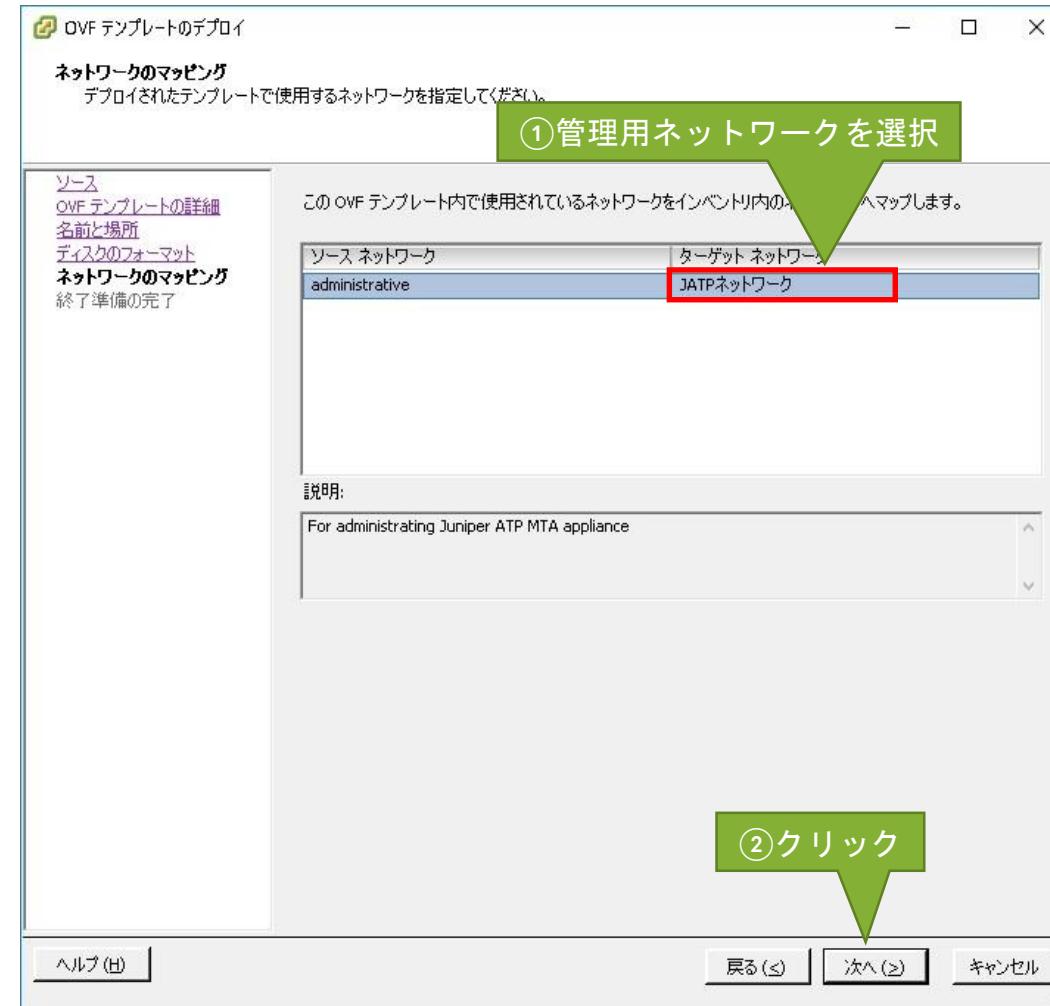
仮想サーバー設定手順(OVFファイル)



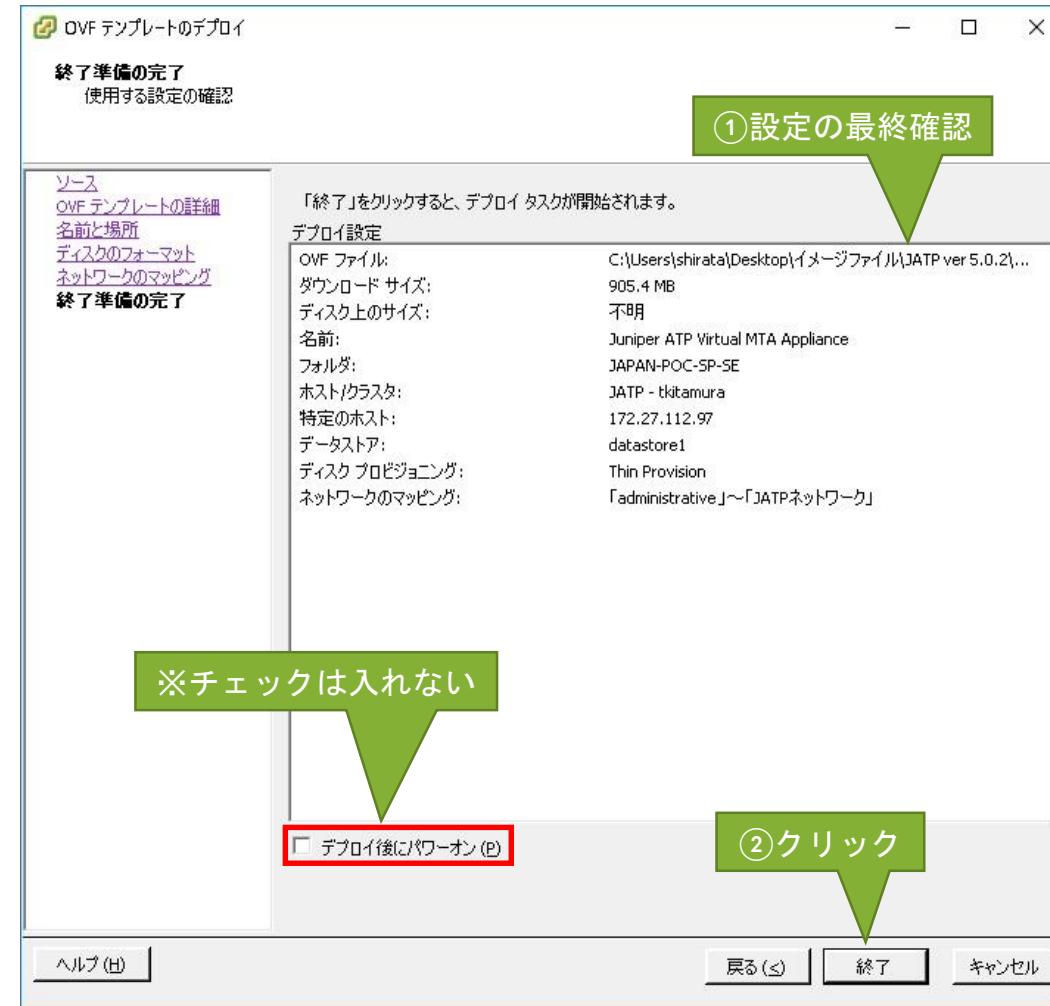
仮想サーバー設定手順(OVFファイル)



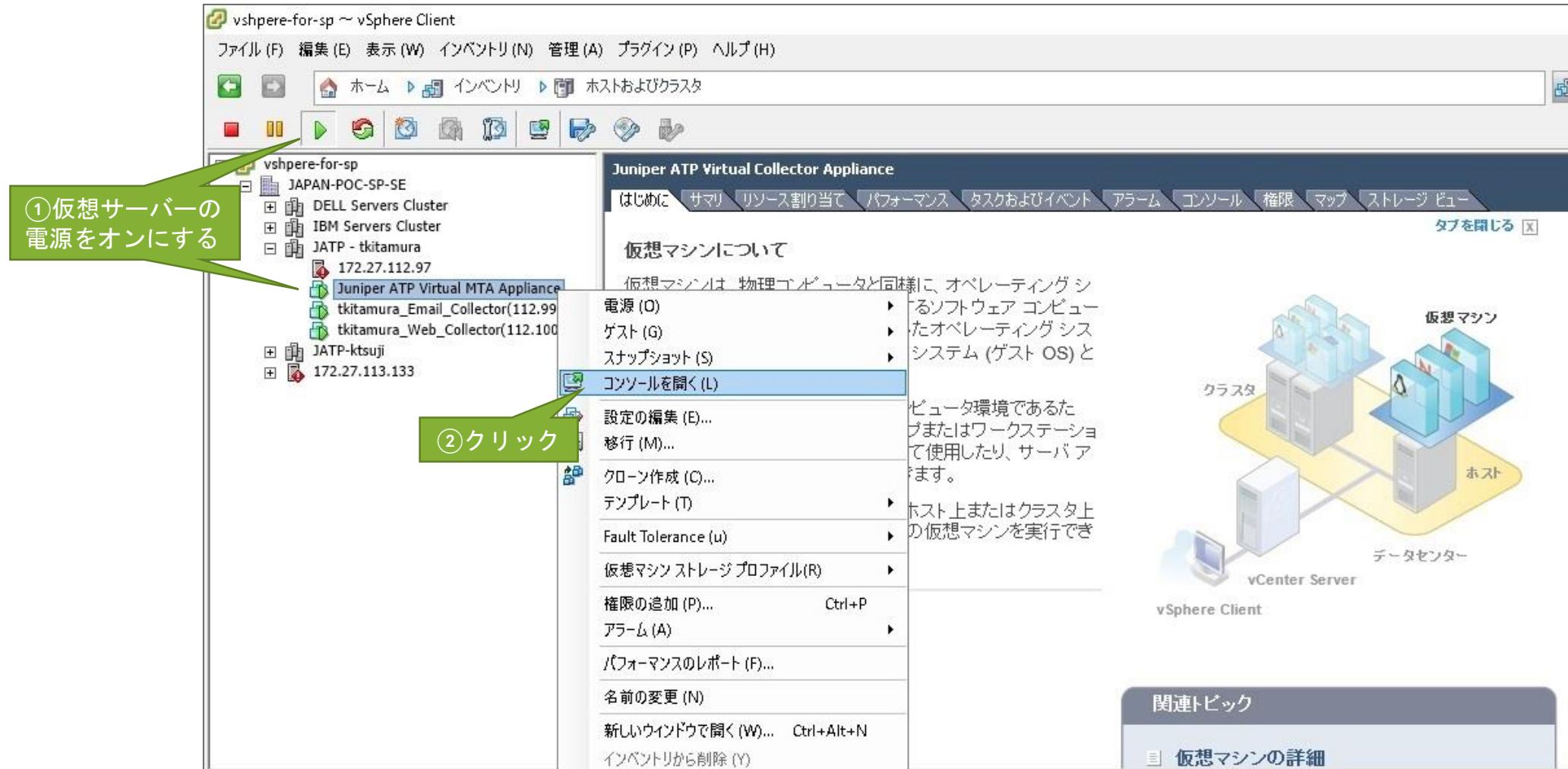
仮想サーバー設定手順(OVFファイル)



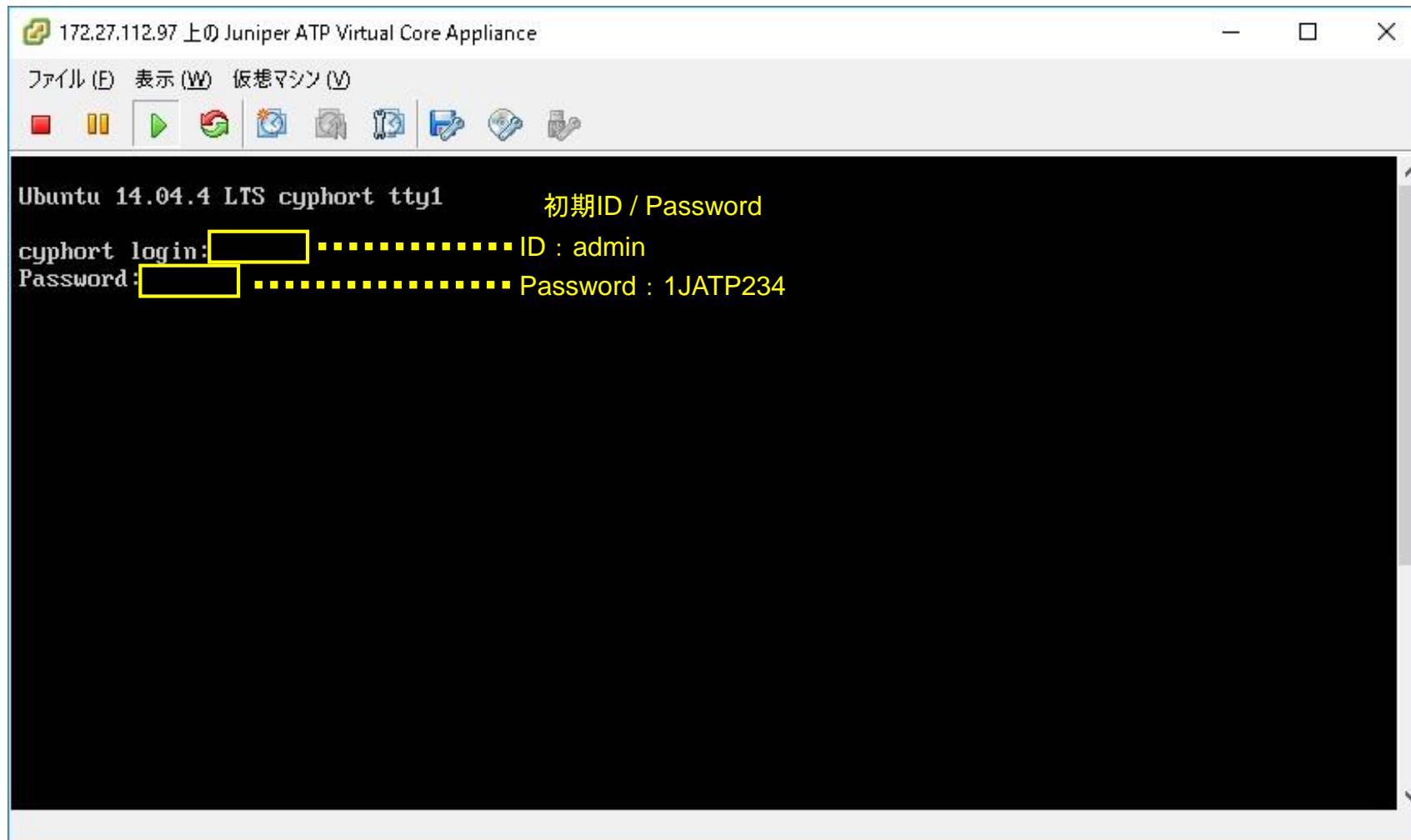
仮想サーバー設定手順(OVFファイル)



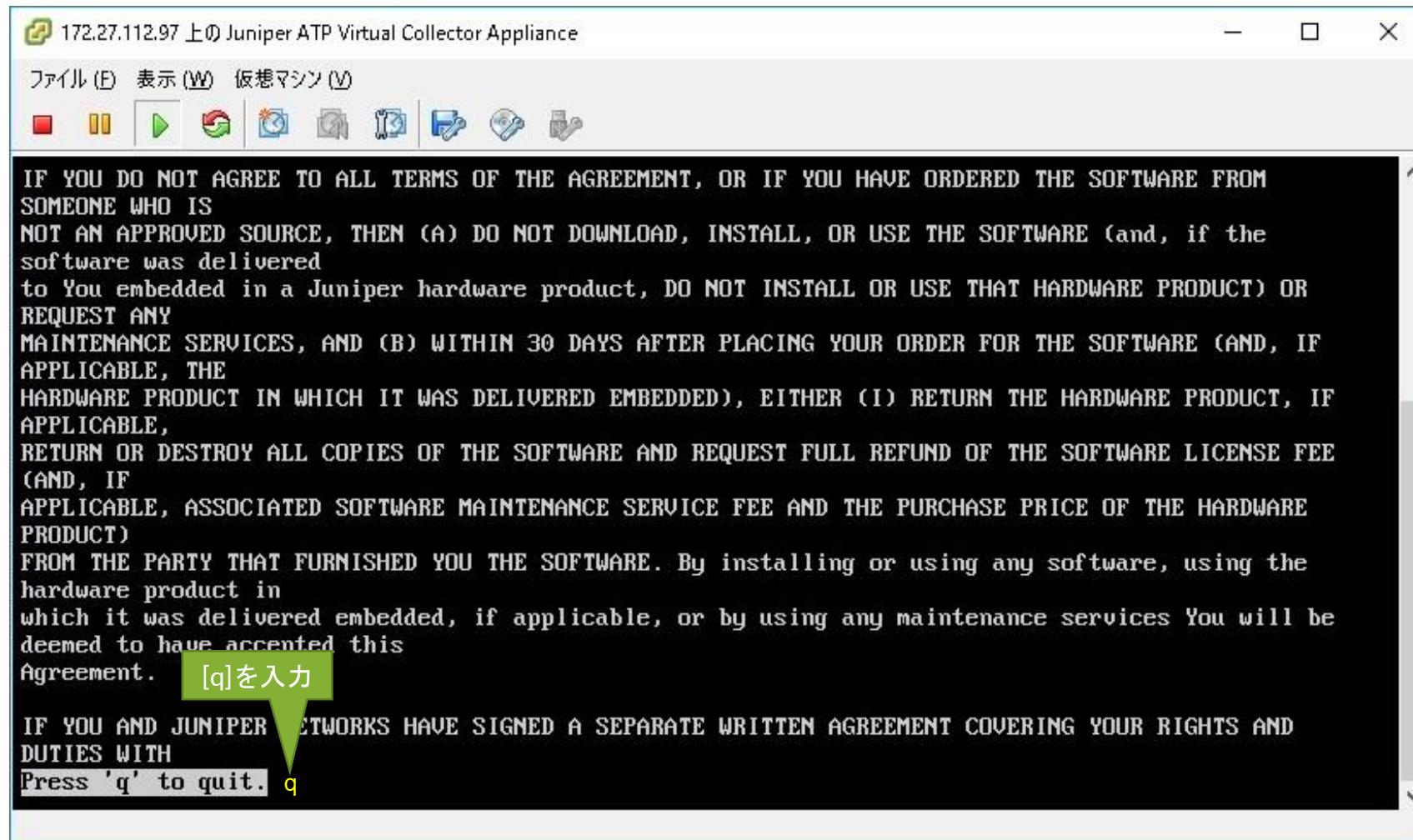
仮想サーバー設定手順(OVFファイル)



仮想サーバー設定手順(OVFファイル)



仮想サーバー設定手順(OVFファイル)



仮想サーバー設定手順(OVFファイル)

```
*****  
*      Juniper Networks Advanced Threat Prevention Appliance      *  
*  
*****  
  
Do you accept the End-user License Agreement (Yes/No)? yes  
  
The CLI admin password needs to be changed from the default.  
Enter the new password of CLI admin: 新規のパスワードを入力  
The entered password *****: it is based on a dictionary word.  
Use this password anyway? (Yes/No)? yes  
Retype the new password of CLI admin: 再度同じパスワードを入力
```

仮想サーバー設定手順(OVFファイル)

```
*****  
*      Juniper Networks Advanced Threat Prevention Appliance      *  
*  
*****  
  
Do you want to configure the system by using the configuration wizard (Yes/No)? yes / no  
(※wizardを使用せずに個別に設定・変更することも可能)  
  
***** Setting the IP address and Domain Name Servers *****  
Use DHCP to obtain the IP address and DNS server address for the management (eth0) interface (Yes/No)? yes / no  
Enter IP address for this management (eth0) interface: 管理用IPアドレスを入力  
Enter netmask for this management (eth0) interface: サブネットマスクを入力  
Enter gateway IP Address for this management (eth0) interface: デフォルトゲートウェイのIPアドレス入力  
Enter primary DNS server IP Address for the management (eth0) interface: DNSサーバーのアドレスを入力  
Do you have a secondary DNS server for the management (eth0) interface? (Yes/No)? yes / no (任意)  
Do you want to enter the search domains for management (eth0) interface? (Yes/No)? yes / no (任意)  
Restart the management (eth0) interface (Yes/No)? yes  
  
***** Setting the device host name *****  
Please enter a valid hostname: ホスト名を入力  
Regenerate the SSL self-signed certificate? (Yes/No)? yes / no  
  
***** Setting the device basic attributes *****  
Please enter the following server attributes...  
Is this a Central Manager device (Yes/No)? No  
Central Manager IP address: Core/CMのIPアドレスを入力  
Device name: デバイス名を入力 (Web UI上の表記)  
Device description: デバイスのディスクリプションを入力 (Web UI上の表記)  
Device key passphrase: Coreと共通のキーフレーズを入力
```

仮想サーバー設定手順(OVFファイル)

Wizard終了後、以下の設定を行います

- ・タイムゾーンの設定

```
Hostname-Core# server
Hostname-Core(server)# set timezone Asia/Tokyo
Current time zone is: JST (UTC+09:00)
```

- ・NTPサーバーの設定

```
Hostname-Core# server
Hostname-Core(server)# set ntpserver
Change the ntp server settings? (Yes/No)? yes
Enter the new ntp server name: xxxx.xxxx.xxxx.xxxx
```



Email Collector コマンド一例

EMAIL COLLECTORコマンド一例

CLI画面で設定の確認・変更を行う際は、各モードに入る必要があります

| | |
|------------------|--|
| diagnosis | Diagnosisの設定やステータス確認 |
| exit | CLIセッションを終了 |
| help | 使用可能なSyntax一覧の表示 |
| history | 現在のセッションでのコマンド履歴の表示 |
| server | Serverの設定変更・確認 (UUIDの確認、Pingの送信、サーバー設定の変更、サーバーの再起動など) |
| wizard | Wizardを起動して再設定 |

EMAIL COLLECTORコマンドー例

- ・インターフェース情報の確認

```
Email-Collector# server
Email-Collector(server)# show interface
Interface: management (eth0) Enabled: Yes Link: Yes
  IP Address: 172.27.112.98 Mask: 255.255.252.0 MTU: 1500
  MAC Address: 00:50:56:b4:f5:5d Speed: 10000Mb/s Duplex: Full
  Auto-negotiation: No Medium: Copper
  RX packets: 10238 Bytes: 1417570 Errors: 0 Overruns: 0
  TX packets: 1760 Bytes: 975221 Errors: 0 Overruns: 0
  Traffic rate for the last 5 seconds/1 minute/5 minutes
    RX bits/sec: 41472/41576/19592
    RX packets/sec: 34/33/15
    TX bits/sec: 35584/39792/18920
    TX packets/sec: 6/7/3
```

- ・タイムゾーンの設定

```
Email-Collector# server
Email-Collector(server)# set timezone Asia/Tokyo
```

- ・NTPサーバーの設定

```
Email-Collector# server
Email-Collector(server)# set ntpserver
Change the ntp server settings? (Yes/No)? yes
Enter the new ntp server name: xxxx.xxxx.xxxx.xxxx
```

EMAIL COLLECTORコマンド一例

- ・IPアドレスの個別設定

```
Email-Collector# server
Email-Collector# set ip interface management
Use DHCP to obtain an IP address for management (eth0) interface (Yes/No)? yes / no
Enter IP address for the management (eth0) interface: xxxx.xxxx.xxxx.xxxx
Enter netmask for the management (eth0) interface: xxxx.xxxx.xxxx.xxxx
Enter gateway IP Address for the management (eth0) interface: xxxx.xxxx.xxxx.xxxx
```

- ・CMの指定

```
Email-Collector# server
Email-Collector# set cm xxxx.xxxx.xxxx.xxxx
```

- ・CLIログインパスワードの変更

```
Email-Collector# server
Email-Collector# set password
Enter the current password of CLI admin: 現在のパスワード
Enter the new password of CLI admin: 新しいパスワード
Retype the new password of CLI admin: 新しいパスワードを再入力
```

- ・CLIタイムアウト時間の設定

```
Email-Collector# server
Email-Collector# set cli timeout 0 (秒単位: 0=タイムアウトなし)
```

EMAIL COLLECTORコマンド一例

- Pingの送信

```
Email-Collector# server  
Email-Collector(server)# ping xxxx.xxxx.xxxx.xxxx
```

- サーバーのシャットダウン

```
Email-Collector# server  
Email-Collector(server)# shutdown
```

- セットアップチェック

```
Email-Collector# diagnosis  
Email-Collector(diagnosis)# setupcheck all / report / basic / analysis
```

- パケットキャプチャー

```
Email-Collector# diagnosis  
Email-Collector(diagnosis)# capture-start
```

- キャプチファイルのコピー

```
Email-Collector# diagnosis  
Email-Collector(diagnosis)# copy capture user@hostname:path
```

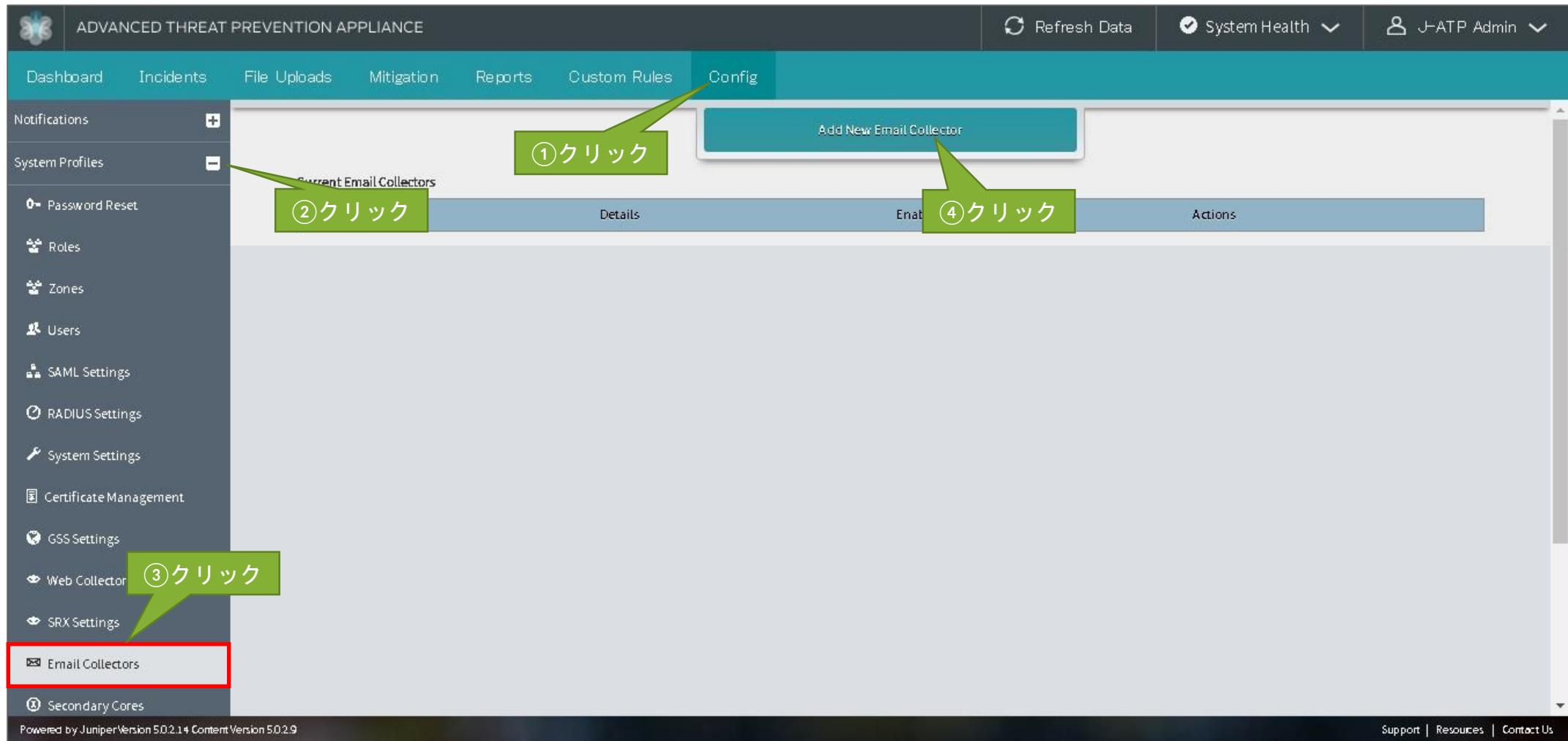


Email Collector設定手順 (BCC)

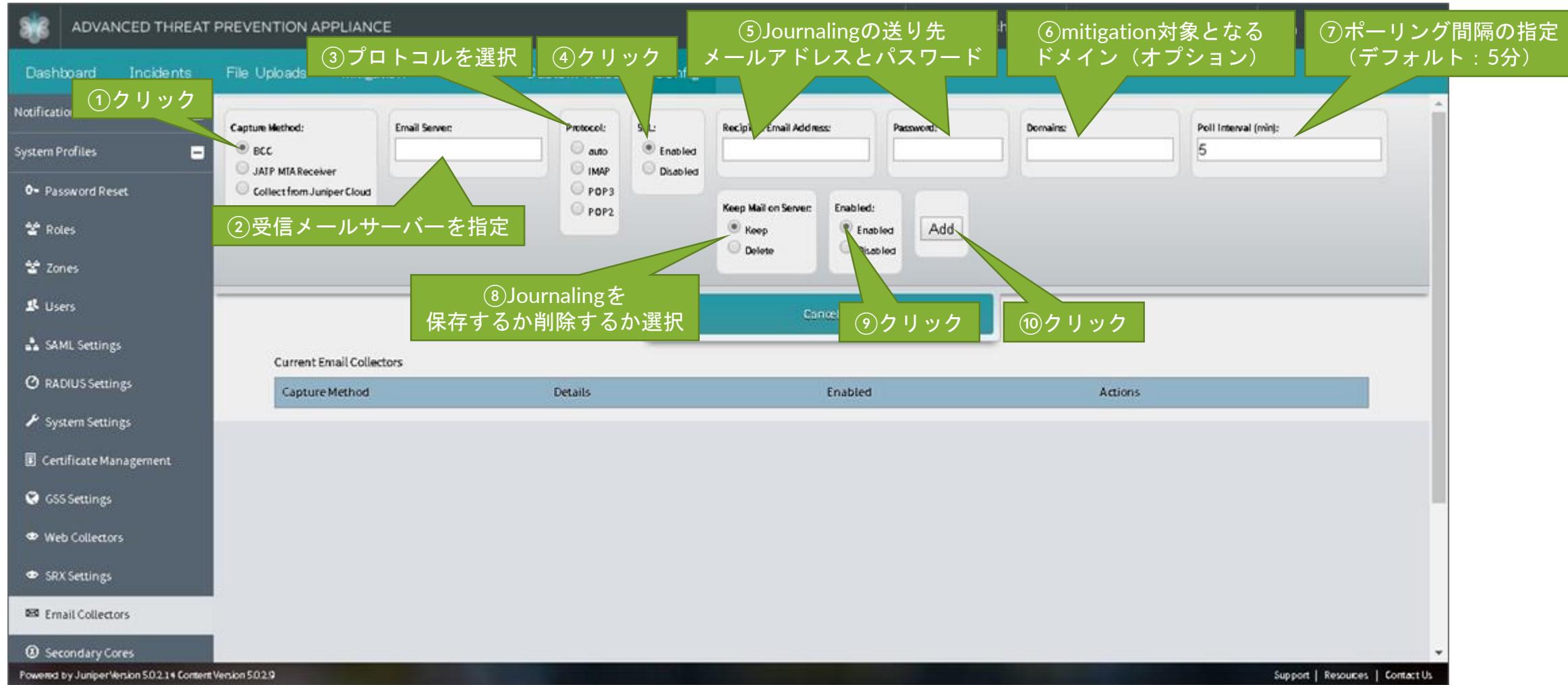
EMAIL COLLECTORについて

- Email Collectorの設定はCore/CMのWeb UI上で行います。
下記 2 通りの設定方法があります。
 - BCCを使用してのJournalingの取得
⇒次ページ以降を参照
 - MTA Receiverを使用してのJournalingの取得
⇒Email Collector設定手順(MTA Receiver)を参照

EMAIL COLLECTOR設定手順 (BCC)



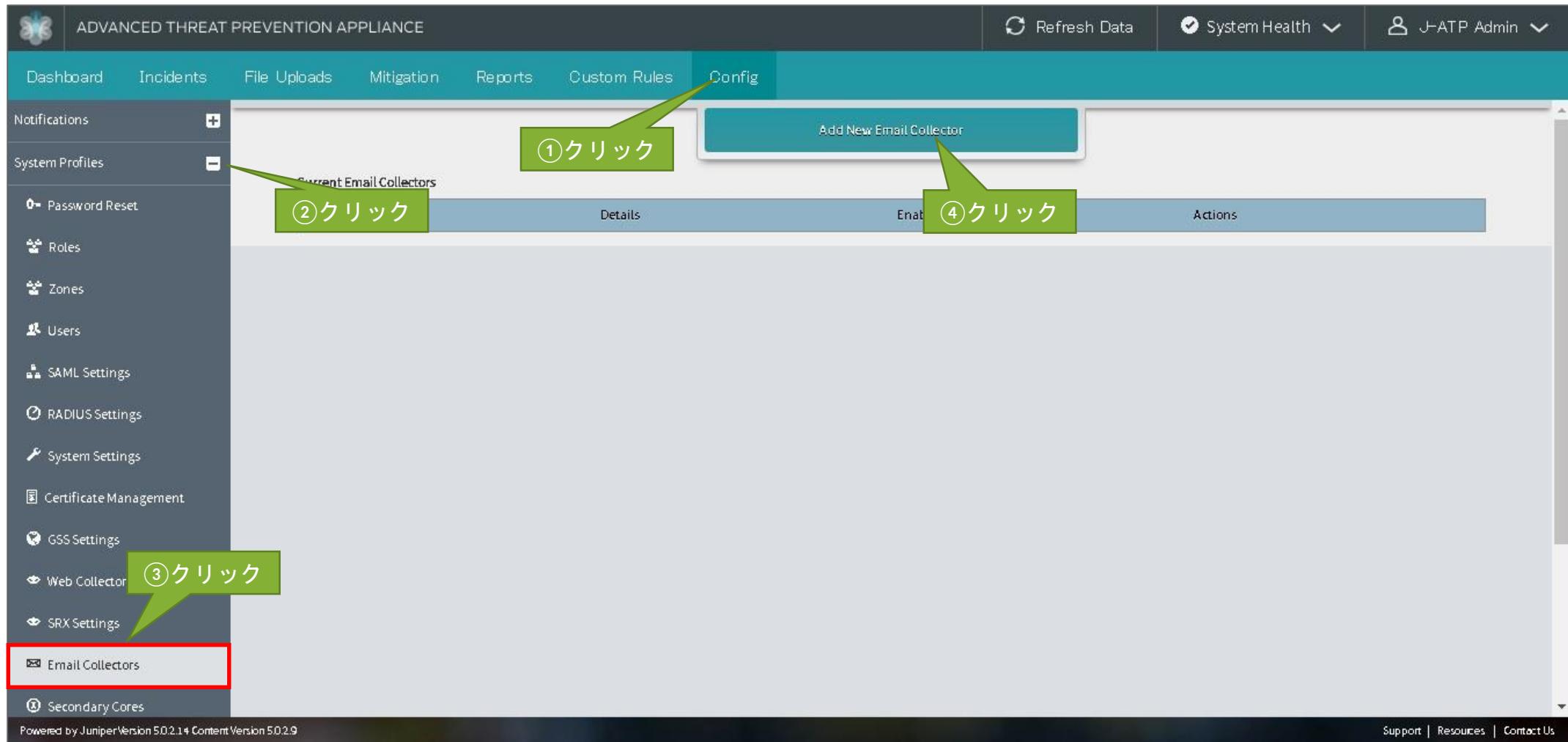
EMAIL COLLECTOR設定手順 (BCC)



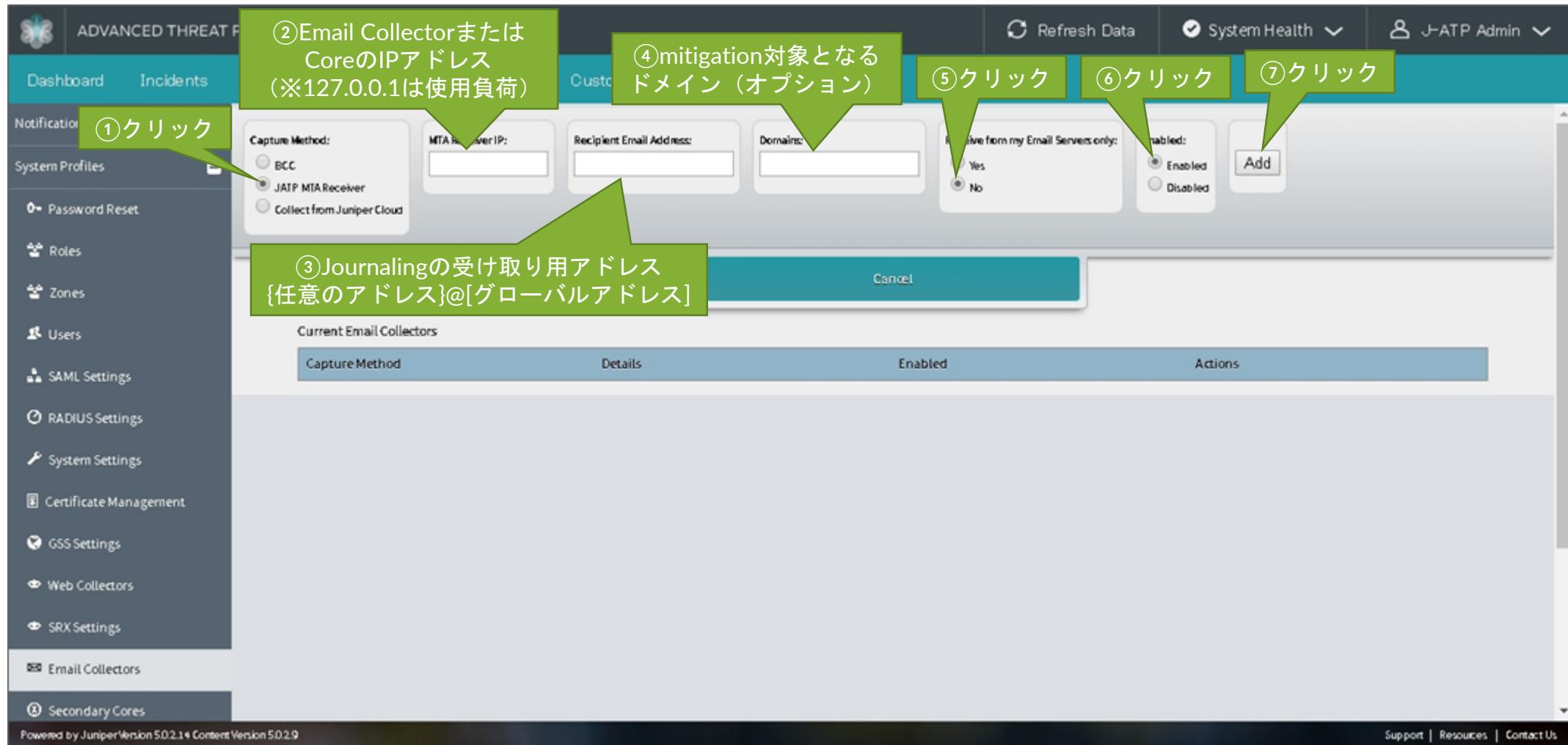


Email Collector設定手順 (MTA Receiver)

EMAIL COLLECTOR設定手順 (MTA RECEIVER)



EMAIL COLLECTOR設定手順 (MTA RECEIVER)



EMAIL COLLECTOR設定手順 (MTA RECEIVER)

※設定例※

Capture Method: JATP MTA Receiver

MTA Receiver IP: 172.27.115.127

Recipient Email Address: jatp_mta@jatp-test.ddo.jp

Domains: jatp-test.ddo.jp

Receive from my Email Servers only: Yes

Enabled: Enabled

Add

Cancel

| Capture Method | Details | Enabled | Actions |
|----------------|---------|---------|---------|
| | | | |

Powered by Juniper Version 5.0.2.14 Content Version 5.0.2.9

Support | Resources | Contact Us

EMAIL COLLECTOR設定手順 (MTA RECEIVER)

ADVANCED THREAT PREVENTION APPLIANCE

Refresh Data System Health J-ATP Admin

Dashboard Incidents File Uploads Mitigation Reports Custom Rules Config

Notifications +

System Profiles -

0 Password Reset

0 Roles

0 Zones

1 Users

0 SAML Settings

0 RADIUS Settings

0 System Settings

0 Certificate Management

0 GSS Settings

0 Web Collectors

0 SRX Settings

1 Email Collectors

0 Secondary Cores

Add New Email Collector

Current Email Collectors

| Capture Method | Details | Enabled | Actions |
|-------------------|---|---------|---|
| JATP MTA Receiver | MTA Receiver IP: 172.27.115.127 Recipient Email: jatp_mta@122.208.14.164 Receive from my Email Servers only: No | Yes | Delete Edit |

設定が登録されているか確認

Powered by Juniper Version 5.02.14 Content Version 5.02.9

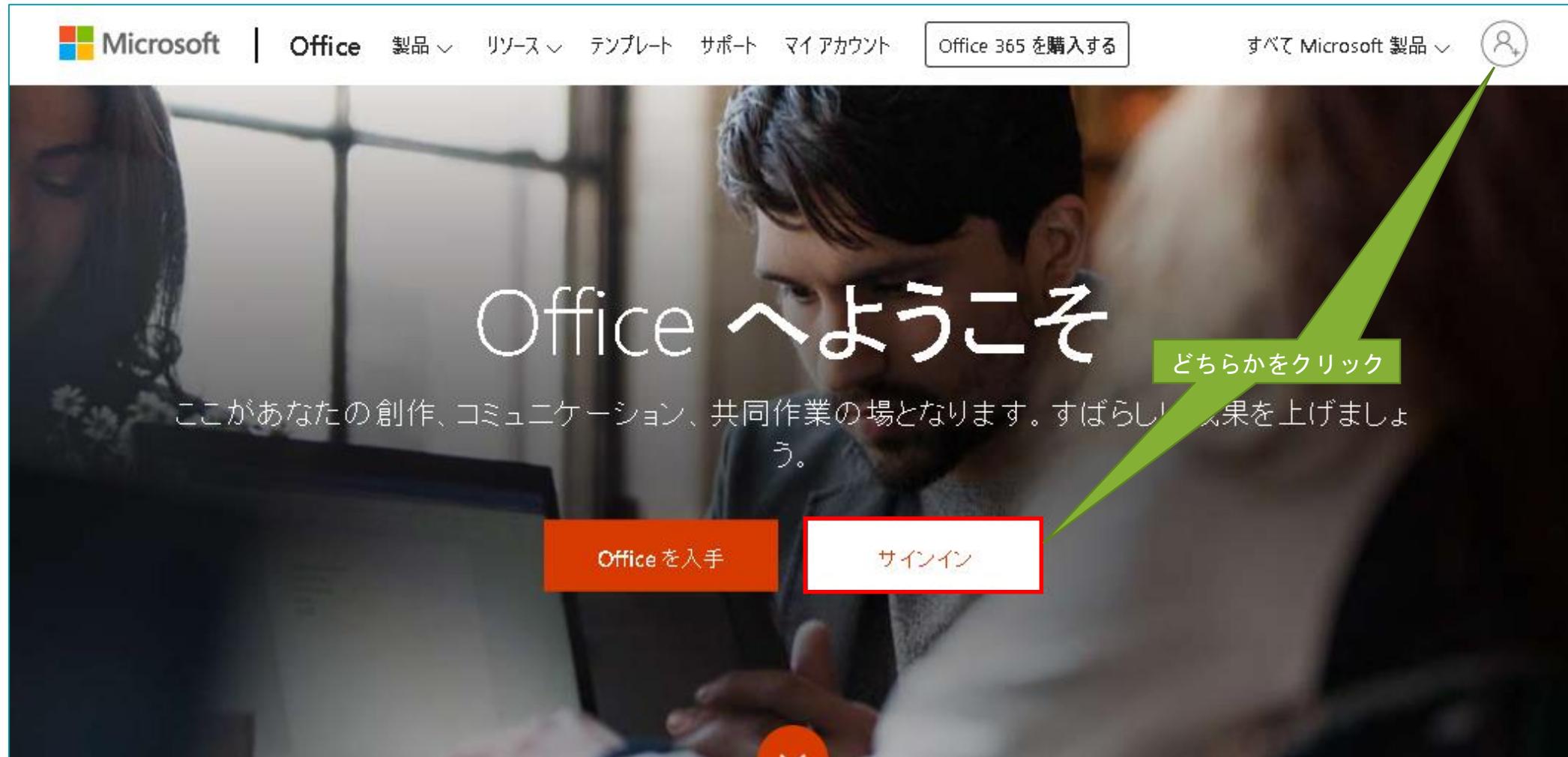
Support | Resources | Contact Us



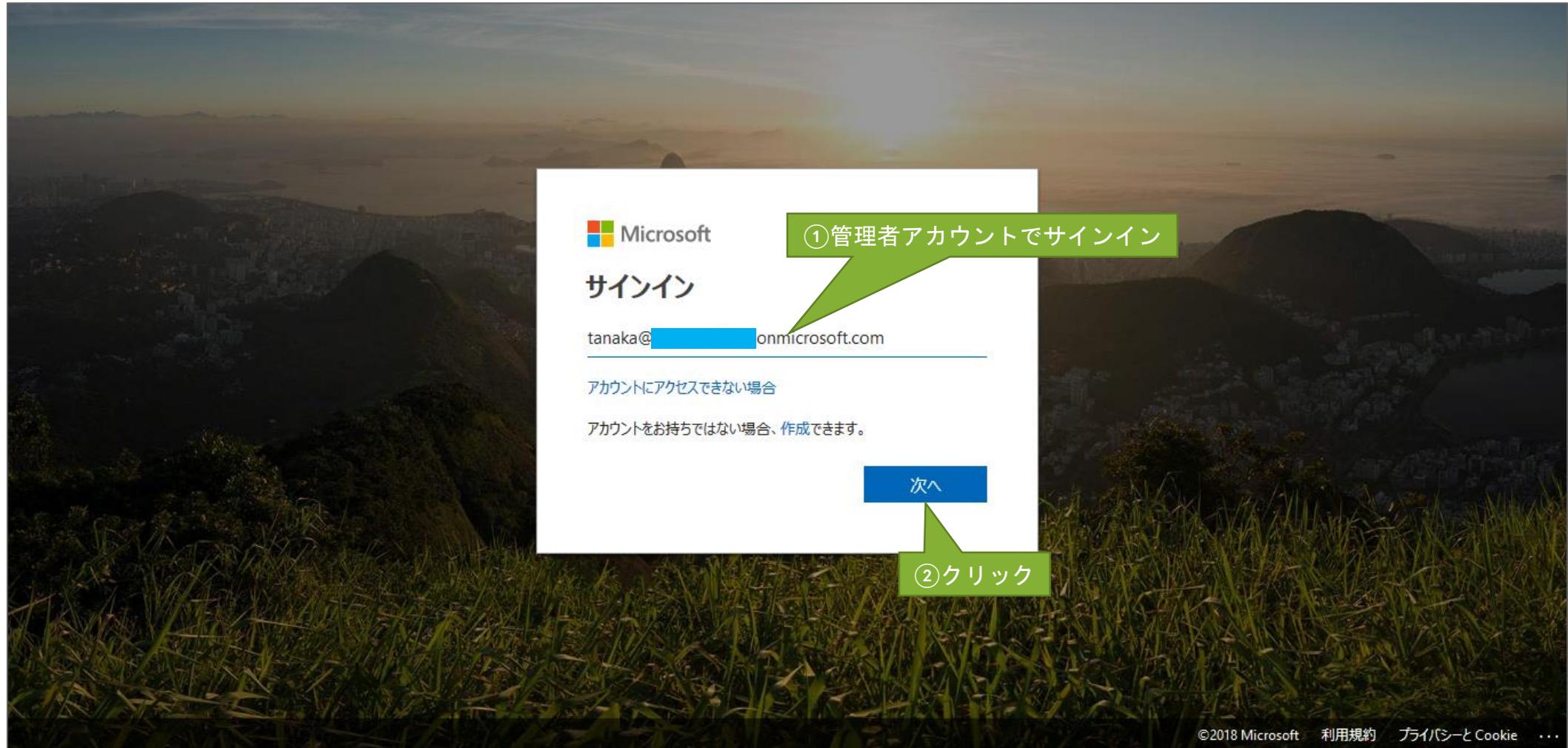
Office 365 ジャーナル設定手順 (BCC, MTA Receiver)

OFFICE 365 ジャーナル設定手順 (BCC,MTA RECEIVER)

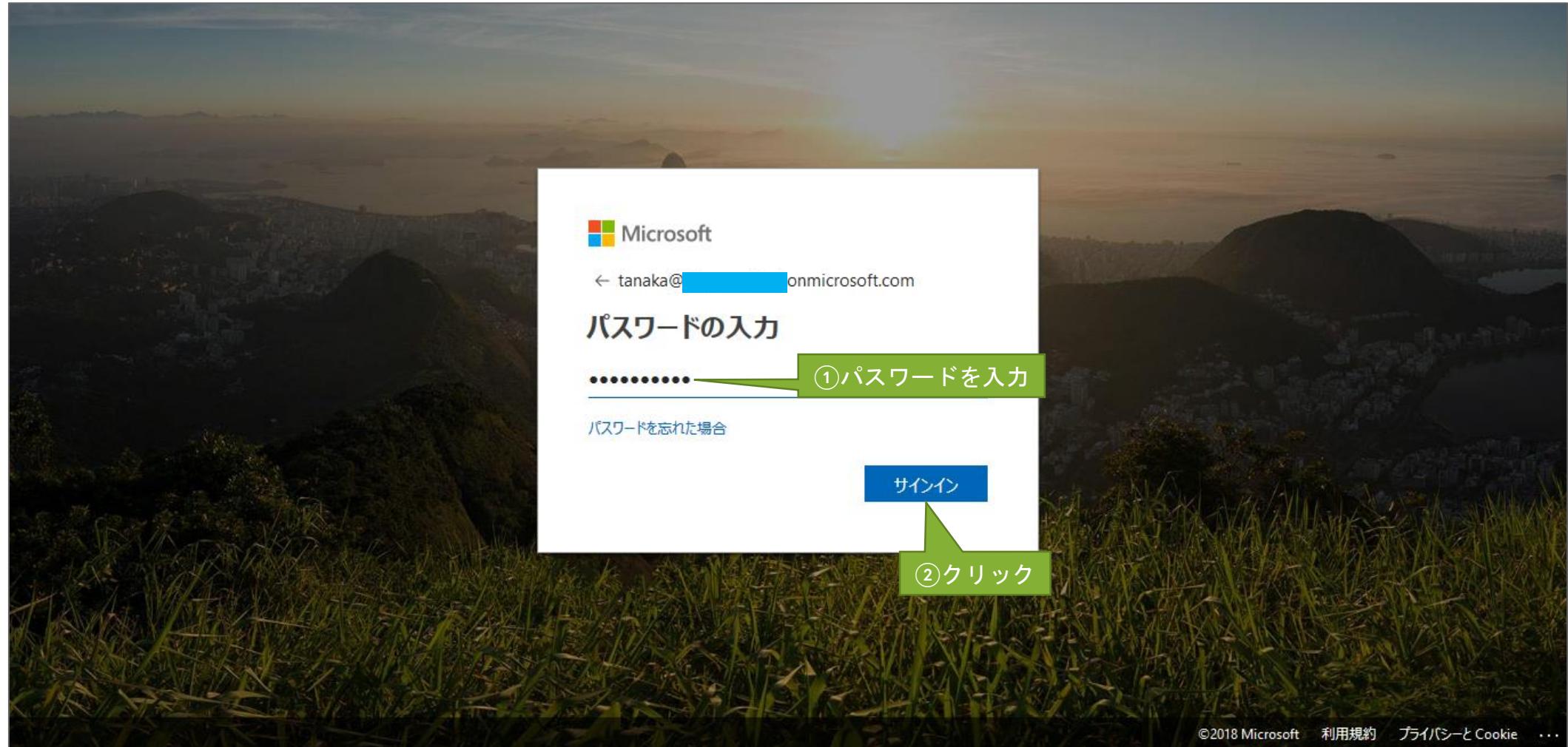
<https://www.office.com/> にアクセス



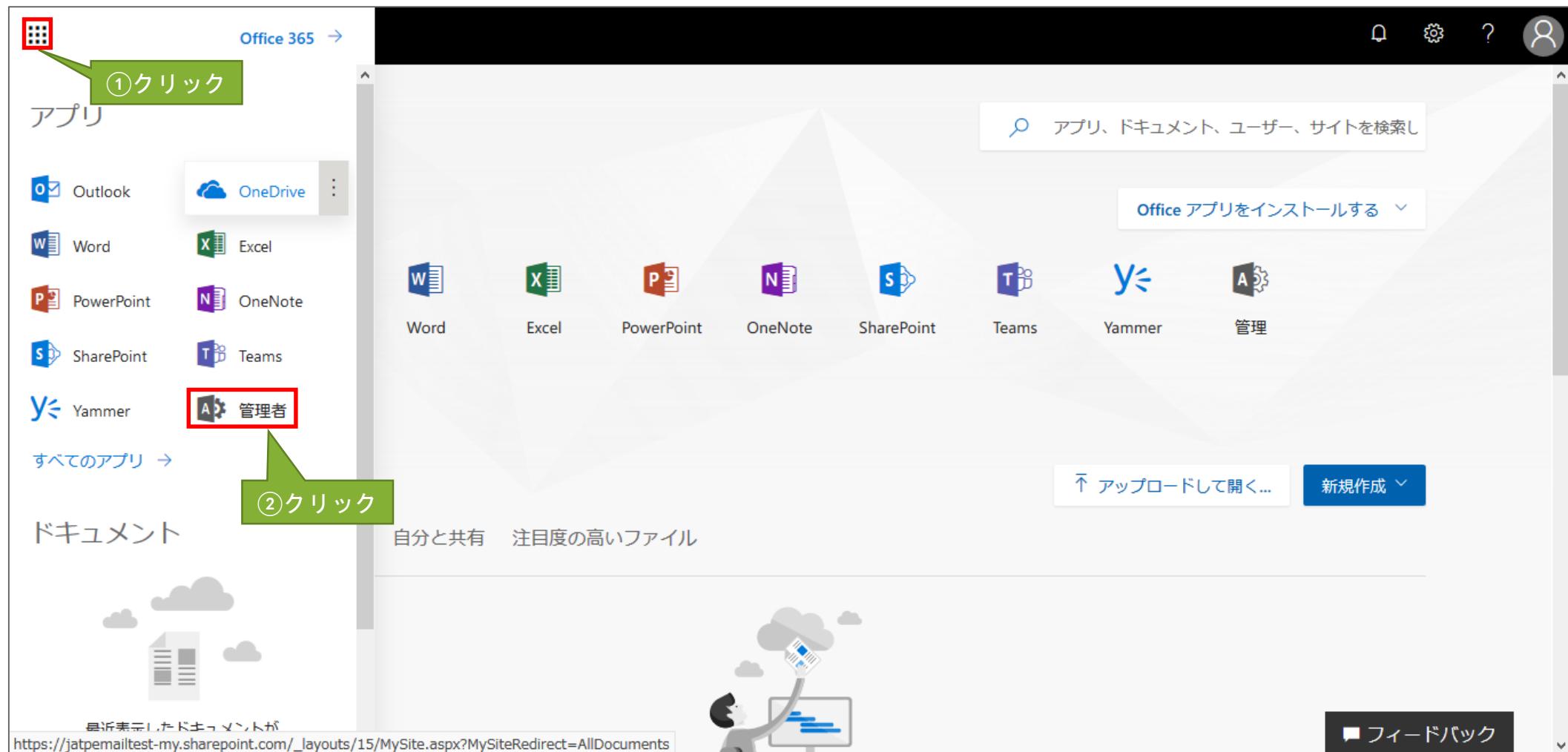
OFFICE 365 ジャーナル設定手順 (BCC,MTA RECEIVER)



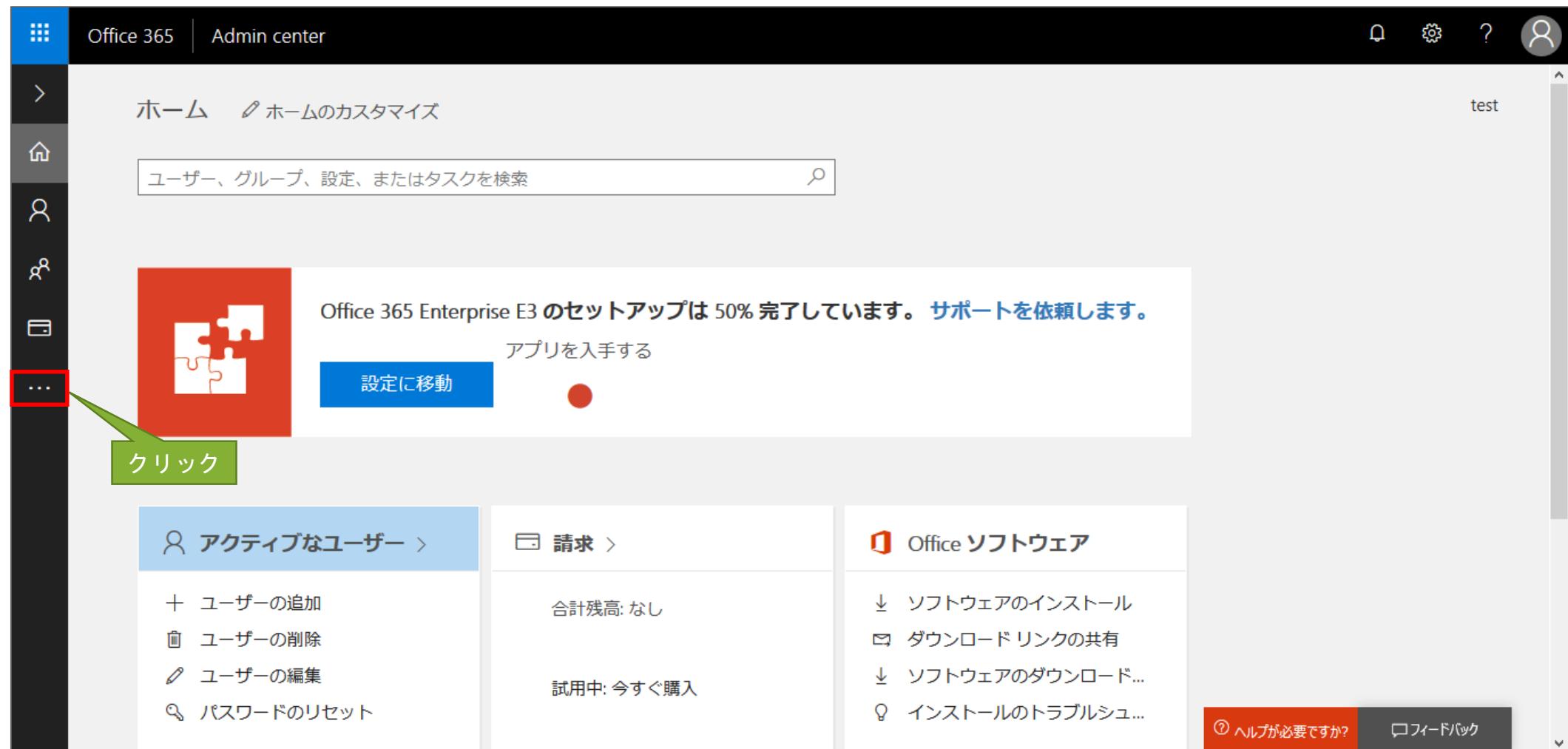
OFFICE 365 ジャーナル設定手順 (BCC,MTA RECEIVER)



OFFICE 365 ジャーナル設定手順 (BCC,MTA RECEIVER)



OFFICE 365 ジャーナル設定手順 (BCC,MTA RECEIVER)



Office 365 Admin center

ホーム ホームのカスタマイズ

ユーザー、グループ、設定、またはタスクを検索

Office 365 Enterprise E3 のセットアップは 50% 完了しています。サポートを依頼します。

アプリ入手する

設定に移動

... (More)

クリック

アクティブなユーザー >

- + ユーザーの追加
- 刪除 ユーザーの削除
- 編集 ユーザーの編集
- リセット パスワードのリセット

請求 >

合計残高: なし

試用中: 今すぐ購入

Office ソフトウェア

- ソフトウェアのインストール
- ダウンロード リンクの共有
- ソフトウェアのダウンロード...
- インストールのトラブルシュ...

ヘルプが必要ですか? フィードバック

OFFICE 365 ジャーナル設定手順 (BCC,MTA RECEIVER)



Office 365 Admin center

Office 365 Enterprise E3 のセットアップは 50% 完了しています。サポートを依頼します。

アプリを入手する

設定に移動

管理センター

Exchange

Teams と Skype

SharePoint

OneDrive

Yammer

PowerApps

Flow

セキュリティ

Azure Active Directory

エンドユーザー向け

請求

合計残高: なし

試用中: 今すぐ購入

Office ソフトウェア

- ↓ ソフトウェアのインストール
- ✉ ダウンロードリンクの共有
- ↓ ソフトウェアのダウンロード...
- 💡 インストールのトラブルシュ...

ヘルプが必要ですか? フィードバック

https://outlook.office365.com/ecp/?rfr=Admin_o365&exsvurl=1&mkt=ja-JP&Realm=jatpemailtest.onmicrosoft.com

クリック

OFFICE 365 ジャーナル設定手順 (BCC,MTA RECEIVER)



The screenshot shows the Microsoft Exchange Admin Center interface. The left sidebar has a red box around the 'Compliance Management' link, and a green box with the text 'クリック' (Click) is placed over it. A green arrow points from the 'Compliance Management' link to the 'Compliance' section in the main content area. The main content area is titled 'ようこそ' (Welcome) and contains several sections: 'Senders' (受信者), 'Access Control' (アクセス許可), 'Compliance Management' (コンプライアンス管理), 'Organization' (組織), 'Protection' (保護), 'Email Flow' (メールフロー), 'Mobile' (モバイル), 'Public Folder' (パブリック フォルダー), 'Unified Messaging' (ユニファイド メッセージング), and 'Hybrid' (ハイブリッド). The 'Compliance Management' section is expanded, showing sub-options like 'Access Control' (アクセス許可), 'Outlook Web App Policy' (Outlook Web App ポリシー), and 'Retention' (監査). A red box with the question 'Help needed?' (ヘルプが必要ですか?) is at the bottom right of this section.

OFFICE 365 ジャーナル設定手順 (BCC,MTA RECEIVER)



Office 365 管理者

Exchange 管理センター

ジャーナルルール

クリック

ヘルプが必要ですか?

インプレース電子情報開示と保留リスト 監査 データ損失防止 アイテム保持ポリシー 保持タグ ジャーナルルール

組織内のメールボックスで、特定のキーワードを含む、または他の検索基準を満たすメールとその他の種類のメッセージを検索します。新しい検索を作成することも、既存の検索を更新することもできます。検索の一覧を更新するには、下の [最新の情報に更新] をクリックします。

EAC でのインプレース電子情報開示検索とホールドの新規作成機能を廃止する計画は依然として進行中です。日程が確定したら、改めて発表します。今後は、Office 365 セキュリティ/コンプライアンス センターのコンテンツ検索を使用してください。Exchange ハイブリッド展開でオンプレミス組織から実行される検索には、この変更の影響はありません。詳細については、セキュリティ/コンプライアンス センターのコンテンツ検索とアイテム保持の説明をご覧ください。

| 名前 | 保留状態 | 更新日 | 作成者 |
|-----------------------|------|-----|-----|
| このビューに表示するアイテムはありません。 | | | |

合計 0 件のうち 0 件を選択

OFFICE 365 ジャーナル設定手順 (BCC,MTA RECEIVER)



Office 365 管理者

Exchange 管理センター

ダッシュボード インプレース電子情報開示と保留リスト 監査 データ損失防止 アイテム保持ポリシー 保持タグ ジャーナルルール

受信者 アクセス許可 コンプライアンス管理

組織 保護 メールフロー モバイル パブリック フォルダー ユニファイド メッセージング ハイブリッド

組織における電子メール保存戦略またはアーカイブ戦略の支援として、ジャーナルルールを使用してすべての通信を記録します。[詳細情報](#)

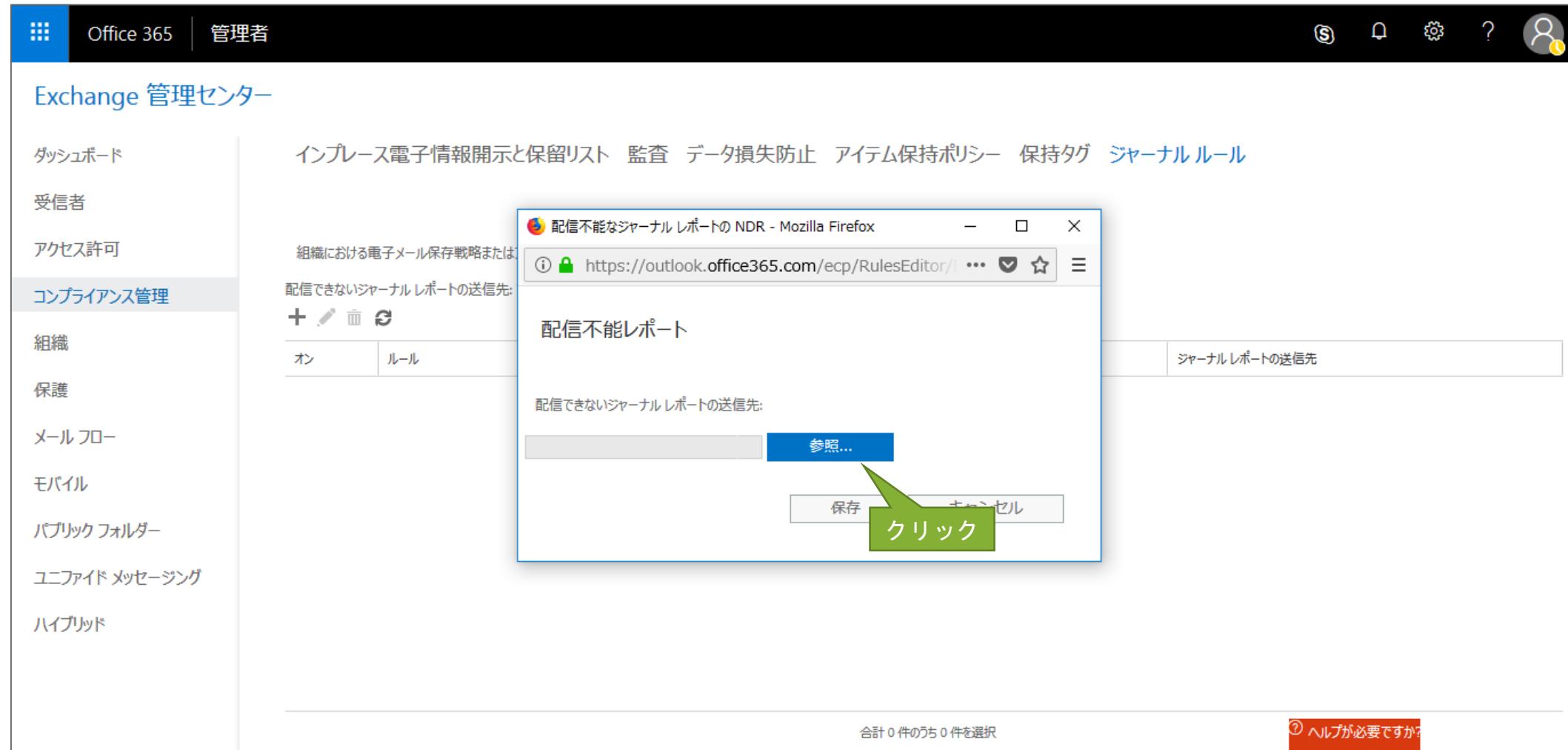
配信できないジャーナルレポートの送信先 **アドレスの選択**

+ ルール クリック

このビューに表示するアイテムはありません。

合計 0 件のうち 0 件を選択 ⑦ ヘルプが必要ですか?

OFFICE 365 ジャーナル設定手順 (BCC,MTA RECEIVER)



Office 365 管理者

Exchange 管理センター

ダッシュボード インプレース電子情報開示と保留リスト 監査 データ損失防止 アイテム保持ポリシー 保持タグ ジャーナルルール

受信者 アクセス許可 コンプライアンス管理 組織 保護 メールフロー モバイル パブリック フォルダー ユニファイド メッセージング ハイブリッド

組織における電子メール保存戦略またはルール

配信できないジャーナルレポートの送信先:

+

配信不能レポート

配信できないジャーナルレポートの送信先:

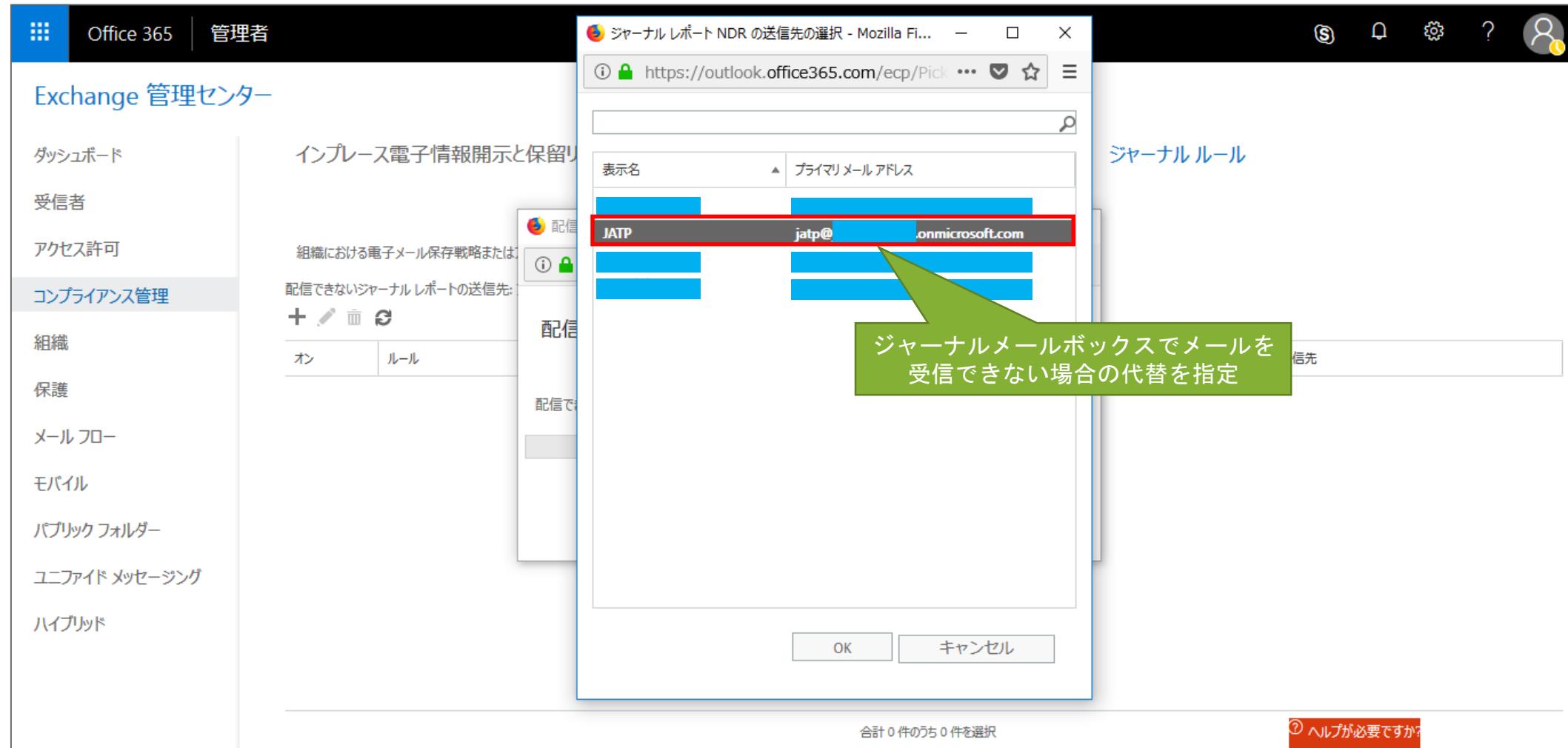
参照...

保存 キャンセル

合計 0 件のうち 0 件を選択

⑦ ヘルプが必要ですか?

OFFICE 365 ジャーナル設定手順 (BCC,MTA RECEIVER)



OFFICE 365 ジャーナル設定手順 (BCC,MTA RECEIVER)



Office 365 管理者

Exchange 管理センター

ダッシュボード

受信者

アクセス許可

コンプライアンス管理

組織

保護

メールフロー

モバイル

パブリック フォルダー

ユニファイド メッセージング

ハイブリッド

インプレース電子情報開示と保留リスト 監査 データ損失防止 アイテム保持ポリシー 保持タグ ジャーナルルール

組織における電子メール保存戦略またはルール

配信できないジャーナルレポートの送信先:

+

オブジェクト

ルール

配信不能レポート

配信できないジャーナルレポートの送信先:

jatp@[REDACTED].onmicrosoft.com

参照...

保存 キャンセル

合計 0 件のうち 0 件を選択

ヘルプが必要ですか?

クリック

OFFICE 365 ジャーナル設定手順 (BCC,MTA RECEIVER)



OFFICE 365 ジャーナル設定手順 (BCC,MTA RECEIVER)



Office 365 管理者

Exchange 管理センター

ダッシュボード インプレース電子情報開示と保留リスト 監査 データ損失防止 アイテム保持ポリシー 保持タグ ジャーナルルール

受信者 アクセス許可 コンプライアンス管理

組織 保護 メールフロー モバイル パブリック フォルダー ユニファイド メッセージング ハイブリッド

組織における電子メール保存戦略またはアーカイブ戦略の支援として、ジャーナル ルールを使用してすべての通信を記録します。[詳細情報](#)

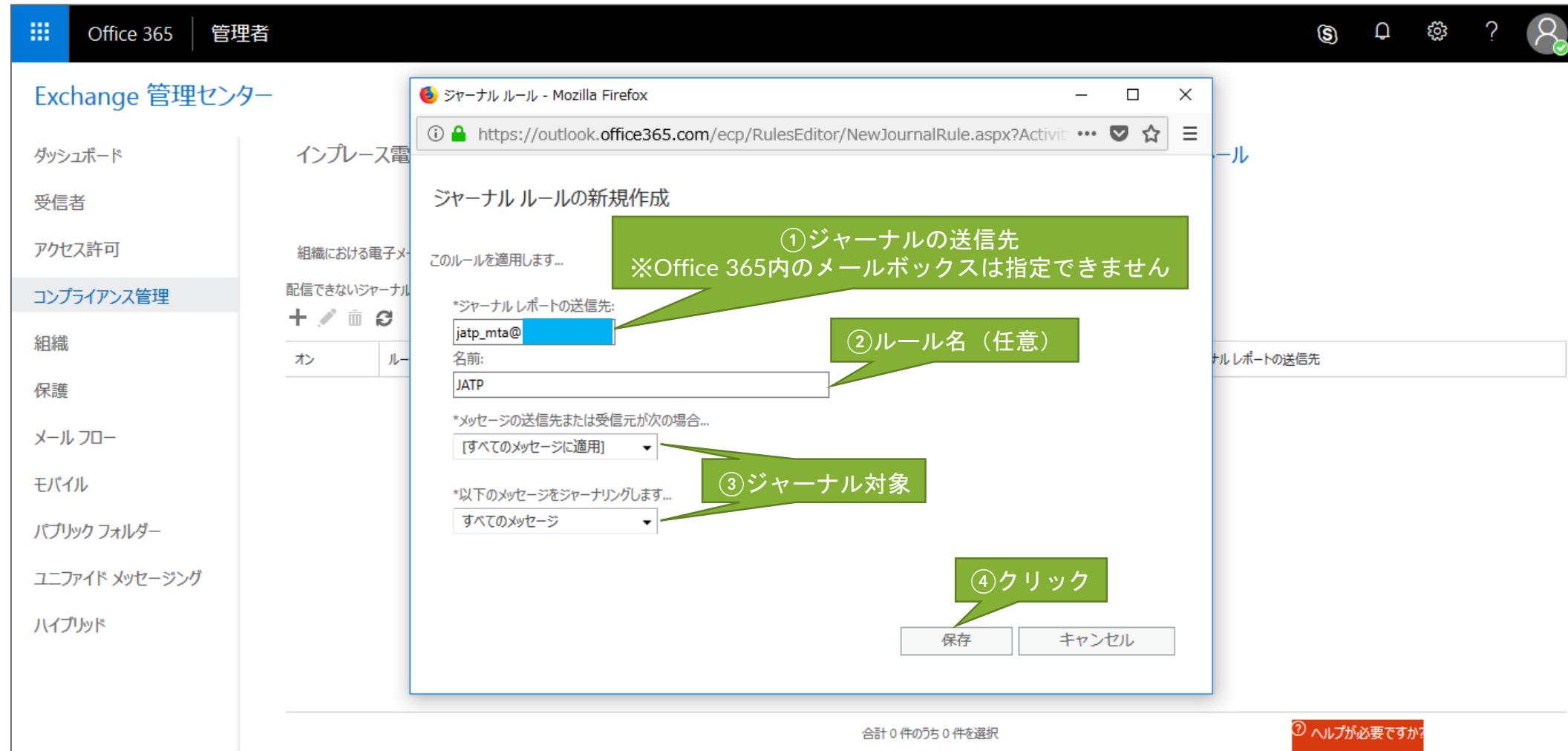
配信できないジャーナル レポートの送信先: jatp@[REDACTED]onmicrosoft.com

| オン | ルール | ユーザー | ジャーナル レポートの送信先 |
|-----------------------|-----|------|----------------|
| このビューに表示するアイテムはありません。 | | | |

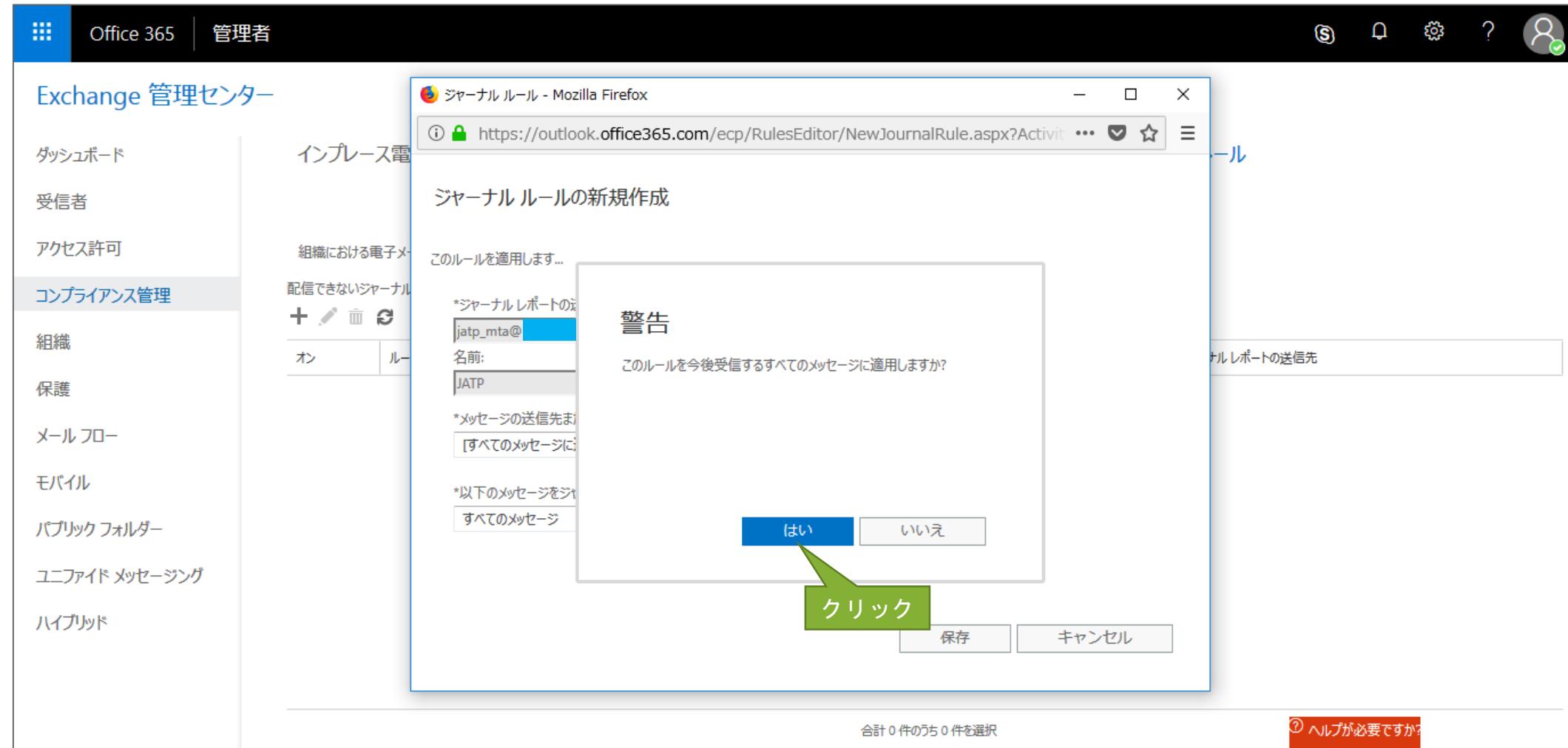
合計 0 件のうち 0 件を選択

⑦ ヘルプが必要ですか?

OFFICE 365 ジャーナル設定手順 (BCC,MTA RECEIVER)



OFFICE 365 ジャーナル設定手順 (BCC,MTA RECEIVER)



OFFICE 365 ジャーナル設定手順 (BCC,MTA RECEIVER)



Office 365 管理者

Exchange 管理センター

ダッシュボード インプレース電子情報開示と保留リスト 監査 データ損失防止 アイテム保持ポリシー 保持タグ ジャーナルルール

受信者 アクセス許可 コンプライアンス管理

組織 保護 メールフロー モバイル パブリック フォルダー ユニファイド メッセージング ハイブリッド

組織における電子メール保存戦略またはアーカイブ戦略の支援として、ジャーナルルールを使用してすべての通信を記録します。[詳細情報](#)

配信できないジャーナルレポートの送信先: jatp@[REDACTED]onmicrosoft.com

+ ルール ユーザー ジャーナルレポートの送信先

| | | | |
|-------------------------------------|------|------|-------------------------|
| オン | ルール | ユーザー | ジャーナルレポートの送信先 |
| <input checked="" type="checkbox"/> | JATP | | jatp_mta@122.208.14.164 |

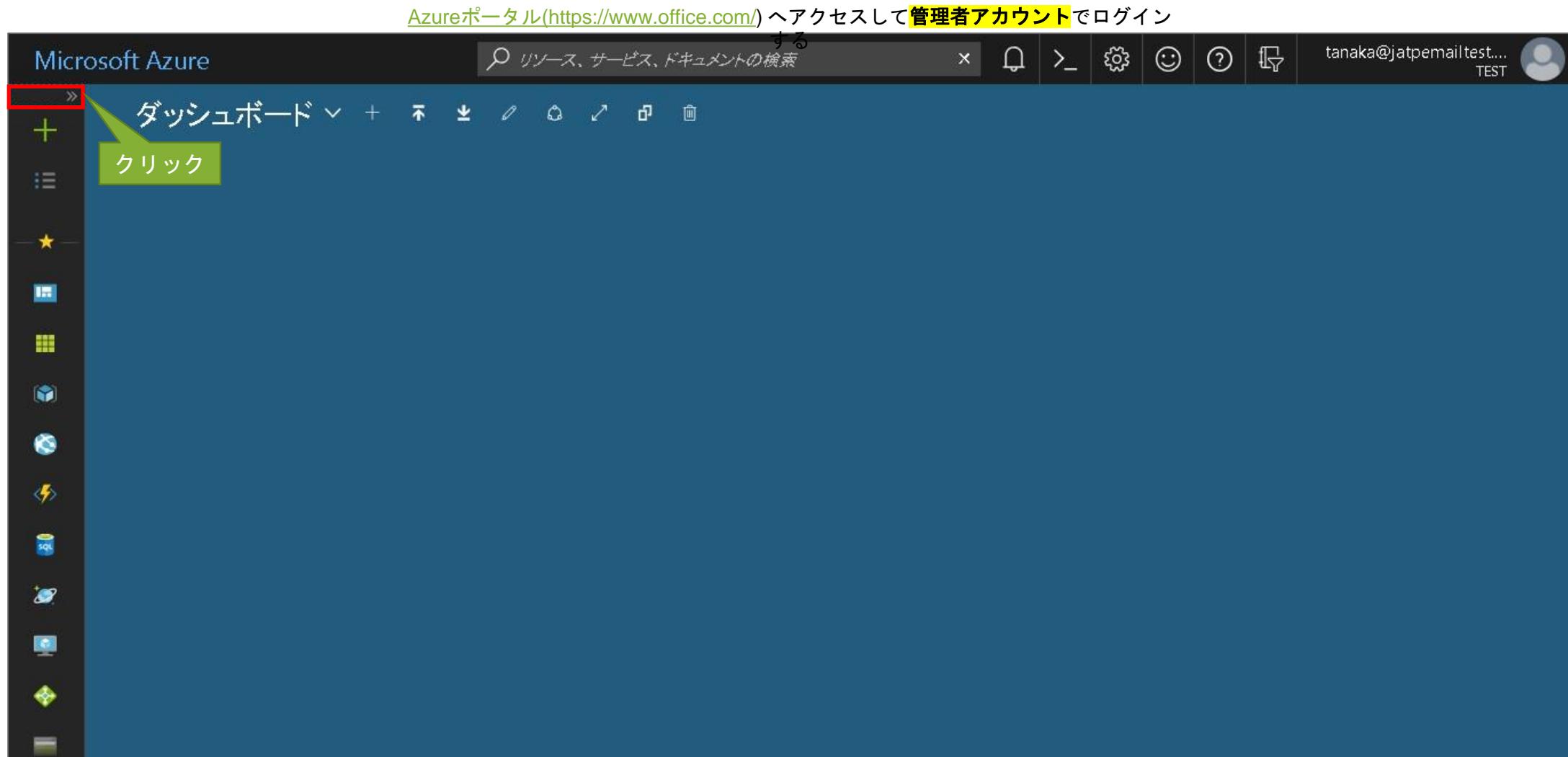
設定完了

合計 1 件のうち 1 件を選択 ⑦ ヘルプが必要ですか?

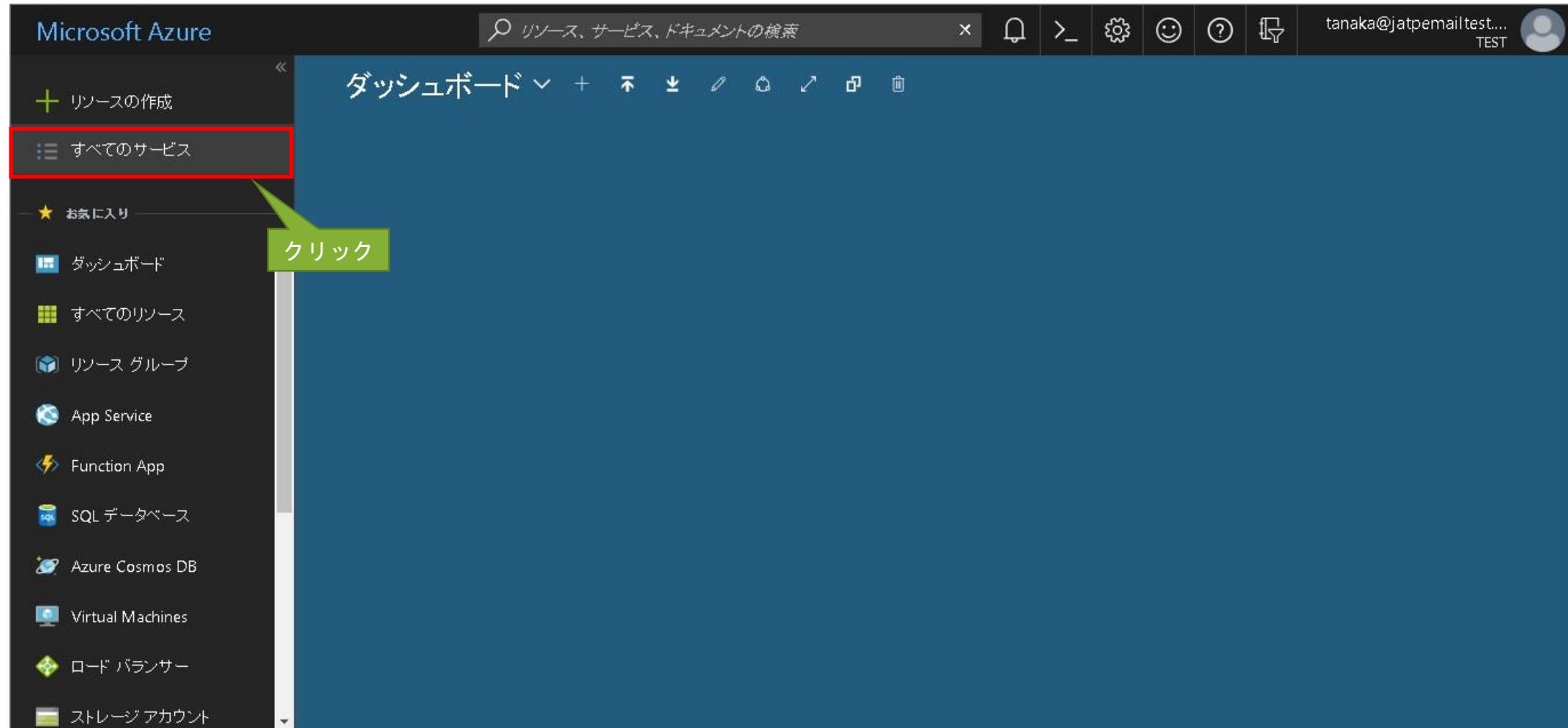


Office 365 Mitigation設定手順 (BCC, MTA Receiver)

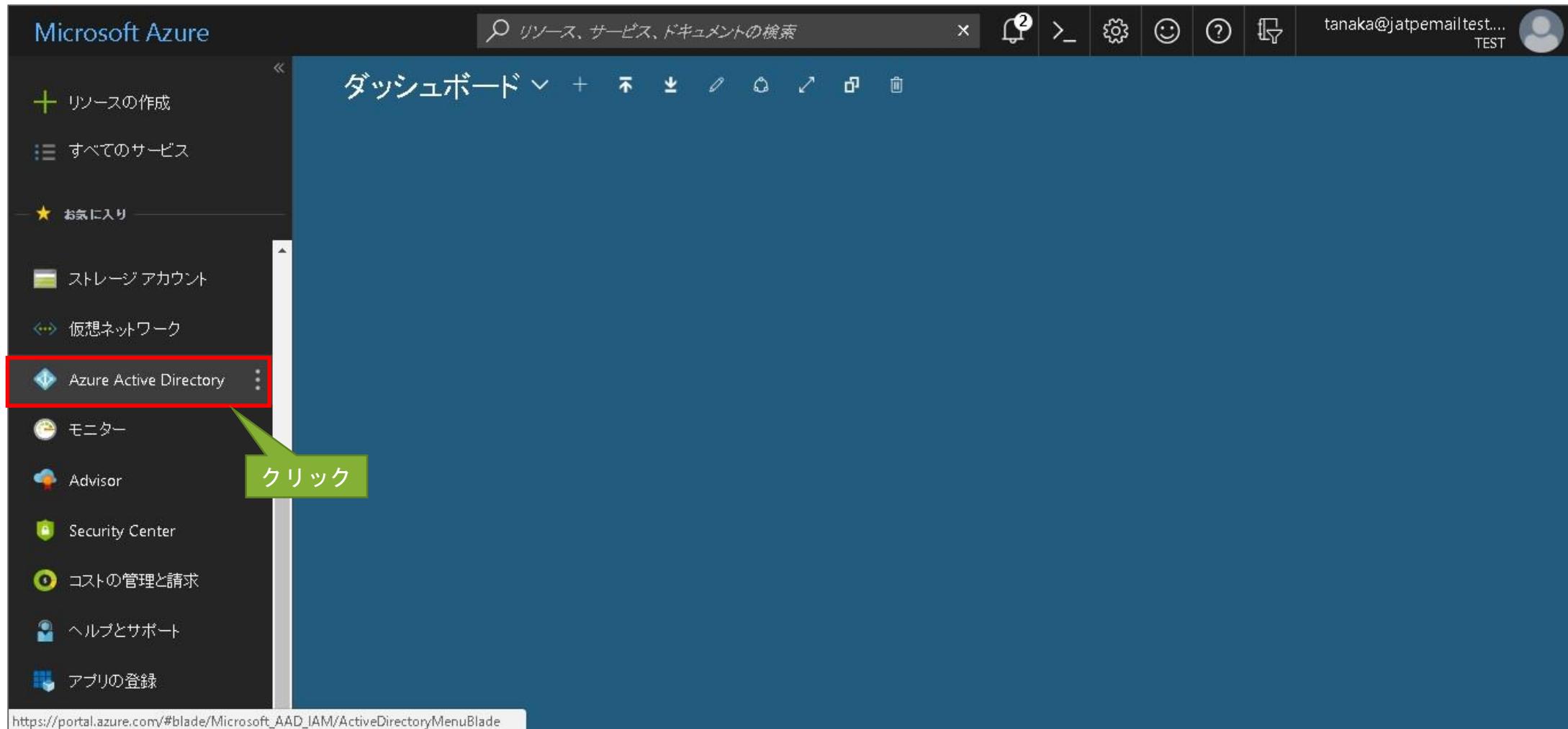
OFFICE 365 MITIGATION設定手順 (BCC,MTA RECEIVER)



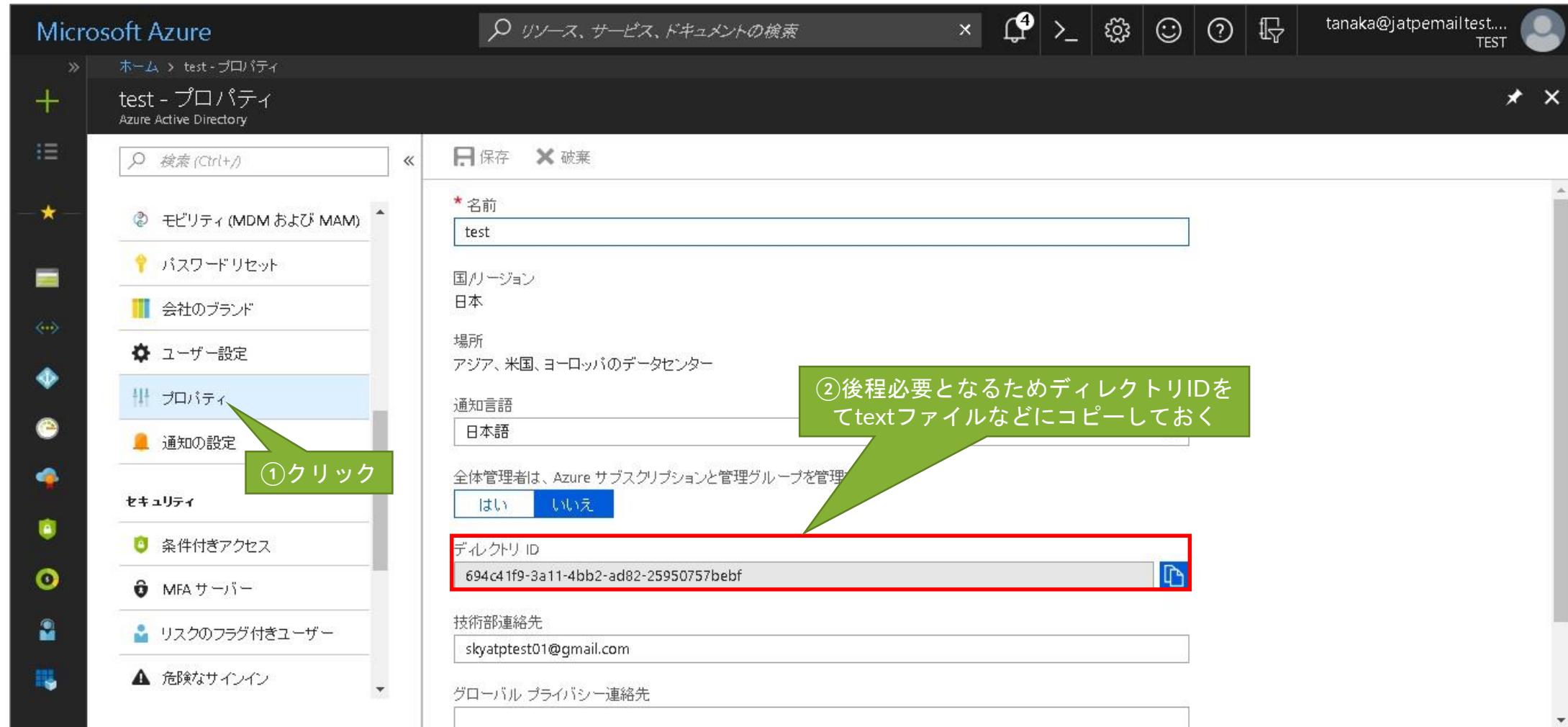
OFFICE 365 MITIGATION設定手順 (BCC,MTA RECEIVER)



OFFICE 365 MITIGATION設定手順 (BCC,MTA RECEIVER)



OFFICE 365 MITIGATION設定手順 (BCC,MTA RECEIVER)



Microsoft Azure

リソース、サービス、ドキュメントの検索

tanaka@jatpemailtest... TEST

ホーム > test - プロパティ

test - プロパティ

Azure Active Directory

検索 (Ctrl+ /)

モビリティ (MDM および MAM)

パスワードリセット

会社のブランド

ユーザー設定

①クリック

プロパティ

通知の設定

セキュリティ

条件付きアクセス

MFA サーバー

リスクのフラグ付きユーザー

危険なサインイン

保存 破棄

*名前
test

国/リージョン
日本

場所
アジア、米国、ヨーロッパのデータセンター

通知言語
日本語

全体管理者は、Azure サブスクリプションと管理グループを管理

はい いいえ

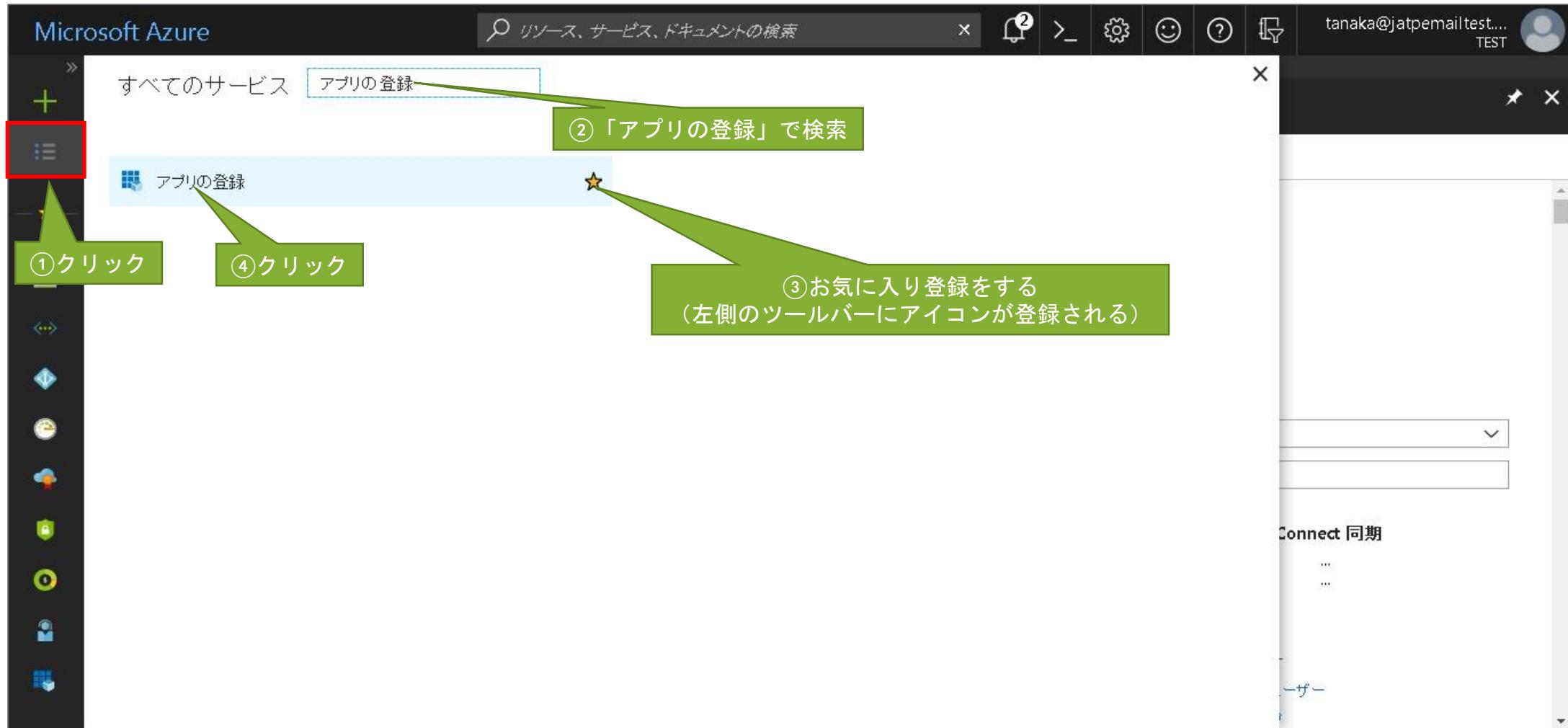
②後程必要となるためディレクトリIDをtextファイルなどにコピーしておく

ディレクトリ ID
694c41f9-3a11-4bb2-ad82-25950757bebf

技術部連絡先
skyatptest01@gmail.com

グローバル プライバシー連絡先

OFFICE 365 MITIGATION設定手順 (BCC,MTA RECEIVER)



OFFICE 365 MITIGATION設定手順 (BCC,MTA RECEIVER)



Microsoft Azure リソース、サービス、ドキュメントの検索 tanaka@jatpemailtest... TEST

ホーム > アプリの登録

アプリの登録 Azure Active Directory

+ 新しいアプリケーションの登録 エンドポイント トラブルシューティング

集中型アプリケーションの登録を表示または管理するには、Microsoft Application Console にアクセスしてください。

名前またはID クリックして... マイアプリ

表示名 アプリケーションの種類 アプリケーション ID

このディレクトリ内のどのアプリケーションの所有者でもありません。

アプリケーションをすべて表示

OFFICE 365 MITIGATION設定手順 (BCC,MTA RECEIVER)



OFFICE 365 MITIGATION設定手順 (BCC,MTA RECEIVER)



The screenshot shows the Microsoft Azure portal interface. On the left, the 'Azure Active Directory' blade is open, showing a list of registered applications. One application, 'JATP', is selected. On the right, the 'JATP' application details page is displayed. A green callout box with the text 'アプリケーションIDも textファイルなどにコピーしておく' (Copy the Application ID to a text file, etc.) points to the 'Application ID' field, which is highlighted with a red border. The 'Application ID' value is f631a02e-8639-4f2d-9380-de679f550fca.

Microsoft Azure

リソース、サービス、ドキュメントの検索

ホーム > アプリの登録 > JATP

JATP

設定 マニフェスト 削除

表示名 JATP

アプリケーションの種類 Web アプリ/API

ホーム ページ http://localhost:60000

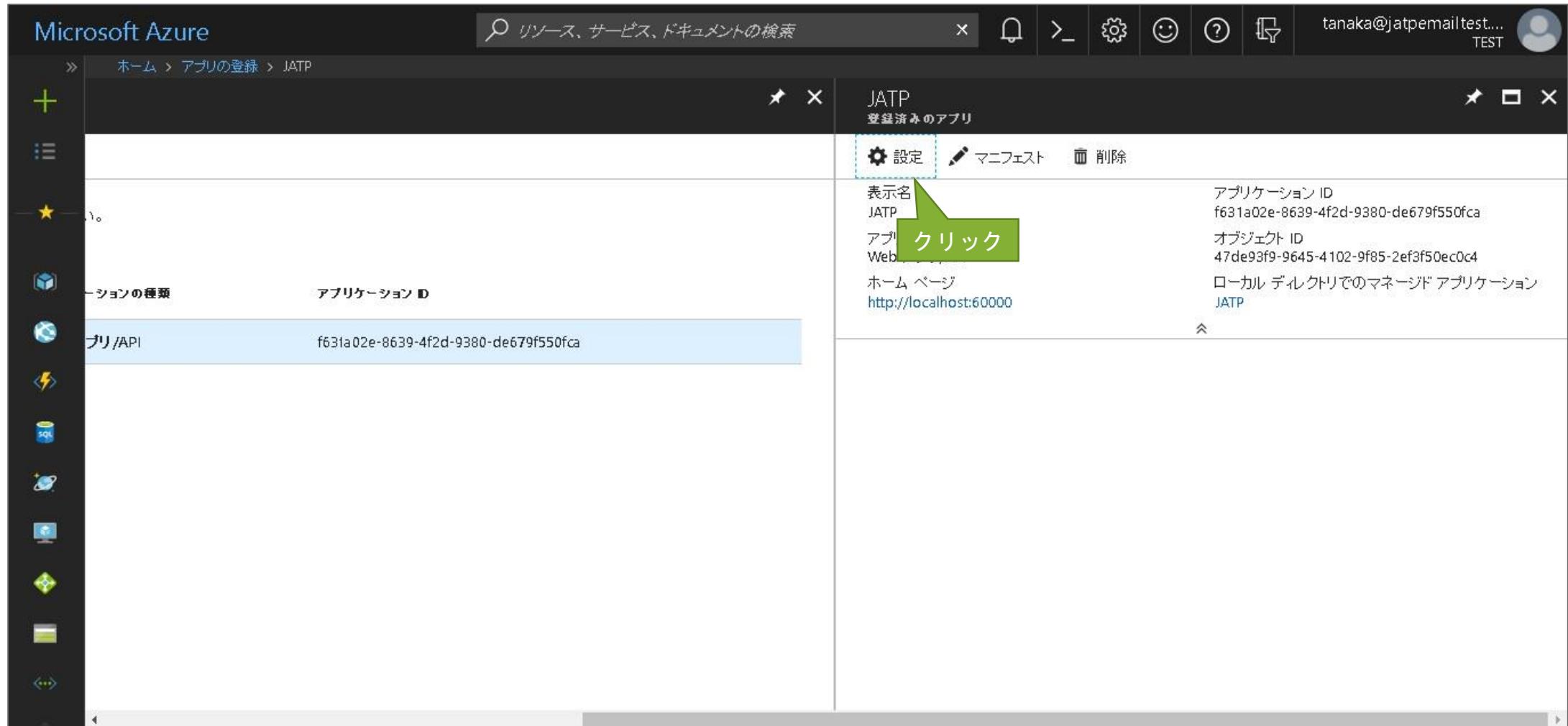
アプリケーション ID f631a02e-8639-4f2d-9380-de679f550fca

オブジェクト ID 47de9645-4102-9f85-2ef3f50ec0c4

ロード バランシング プリントでのマネージド アプリケーション

アプリケーションIDも textファイルなどにコピーしておく

OFFICE 365 MITIGATION設定手順 (BCC,MTA RECEIVER)



The screenshot shows the Microsoft Azure portal interface. The left sidebar lists various service icons. The main navigation bar shows 'Microsoft Azure', 'リソース、サービス、ドキュメントの検索', and a user profile for 'tanaka@jatpemailtest... TEST'. The current page is 'Azure Active Directory > アプリの登録 > JATP'. The 'JATP' application registration is selected, and its settings are displayed on the right. A green callout box with the text 'クリック' (Click) points to the '設定' (Settings) tab. The application details are as follows:

| 表示名 | アプリケーション ID |
|------------------------|--------------------------------------|
| JATP | f631a02e-8639-4f2d-9380-de679f550fca |
| アプリケーションの種類 | アプリケーション ID |
| Web | 47de93f9-9645-4102-9f85-2ef3f50ec0c4 |
| ホーム ページ | ローカル ディレクトリでのマネージド アプリケーション |
| http://localhost:60000 | JATP |

OFFICE 365 MITIGATION設定手順 (BCC,MTA RECEIVER)



Microsoft Azure リソース、サービス、ドキュメントの検索 tanaka@jatpemailtest... TEST

ホーム > アプリの登録 > JATP > 設定

JATP 設定

表示名: JATP
アプリケーションの種類: Web アプリ/API
ホーム ページ: <http://localhost:60000>

アプリケーション ID: f631a02e-8639-4f2d-9380-de679f550fca
オブジェクト ID: 47de93f9-9645-4102-9f85-2ef3f50ec0c4
ローカル ディレクトリでのマネージド アプリケーション: JATP

設定

フィルター設定

全般

- プロパティ >
- 応答 URL >
- 所有者 >

API アクセス

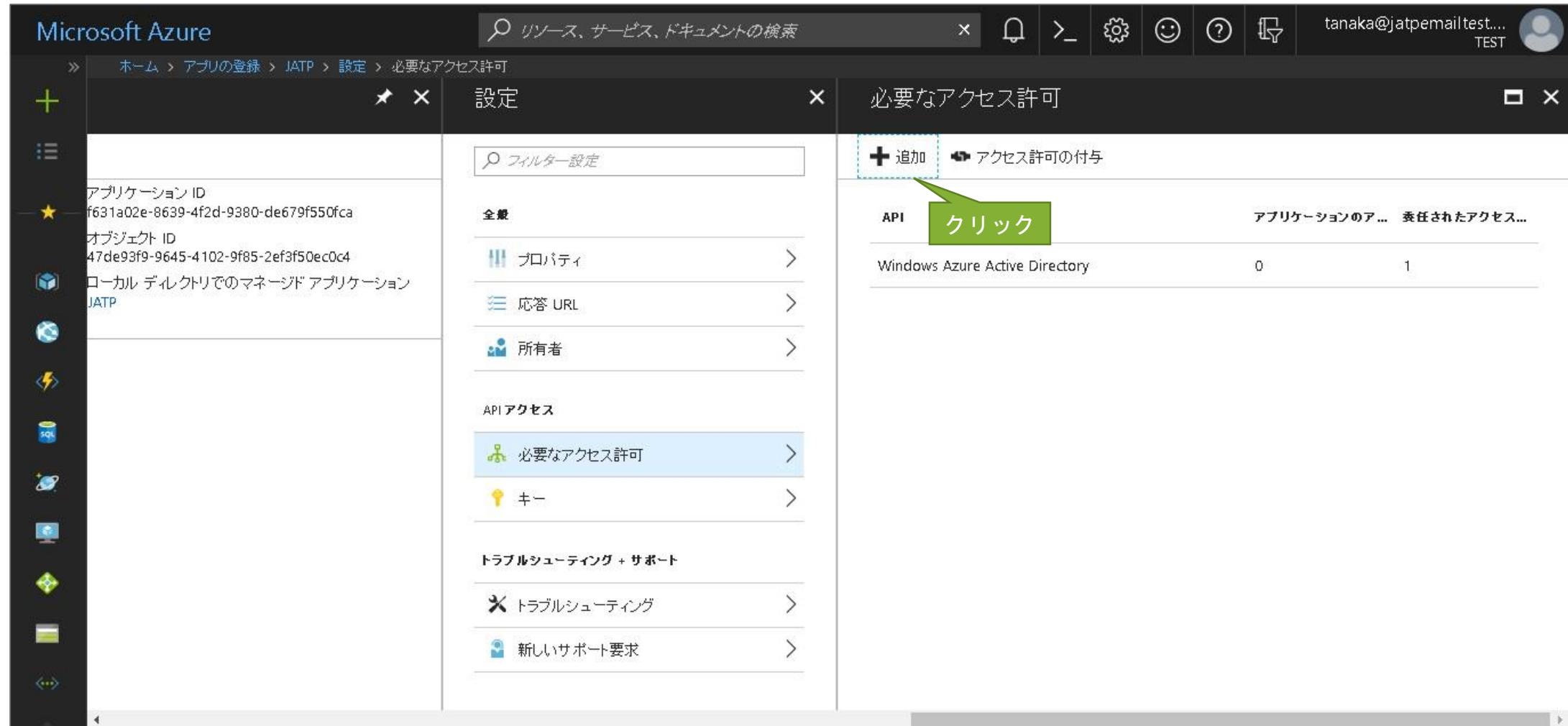
- 必要なアクセス許可 > (クリック)
- キー >

トラブルシューティング + サポート

トラブルシューティング >

新しいサポート要求 >

OFFICE 365 MITIGATION設定手順 (BCC,MTA RECEIVER)



Microsoft Azure リソース、サービス、ドキュメントの検索 tanaka@jatpemailtest... TEST

ホーム > アプリの登録 > JATP > 設定 > 必要なアクセス許可

設定 必要なアクセス許可

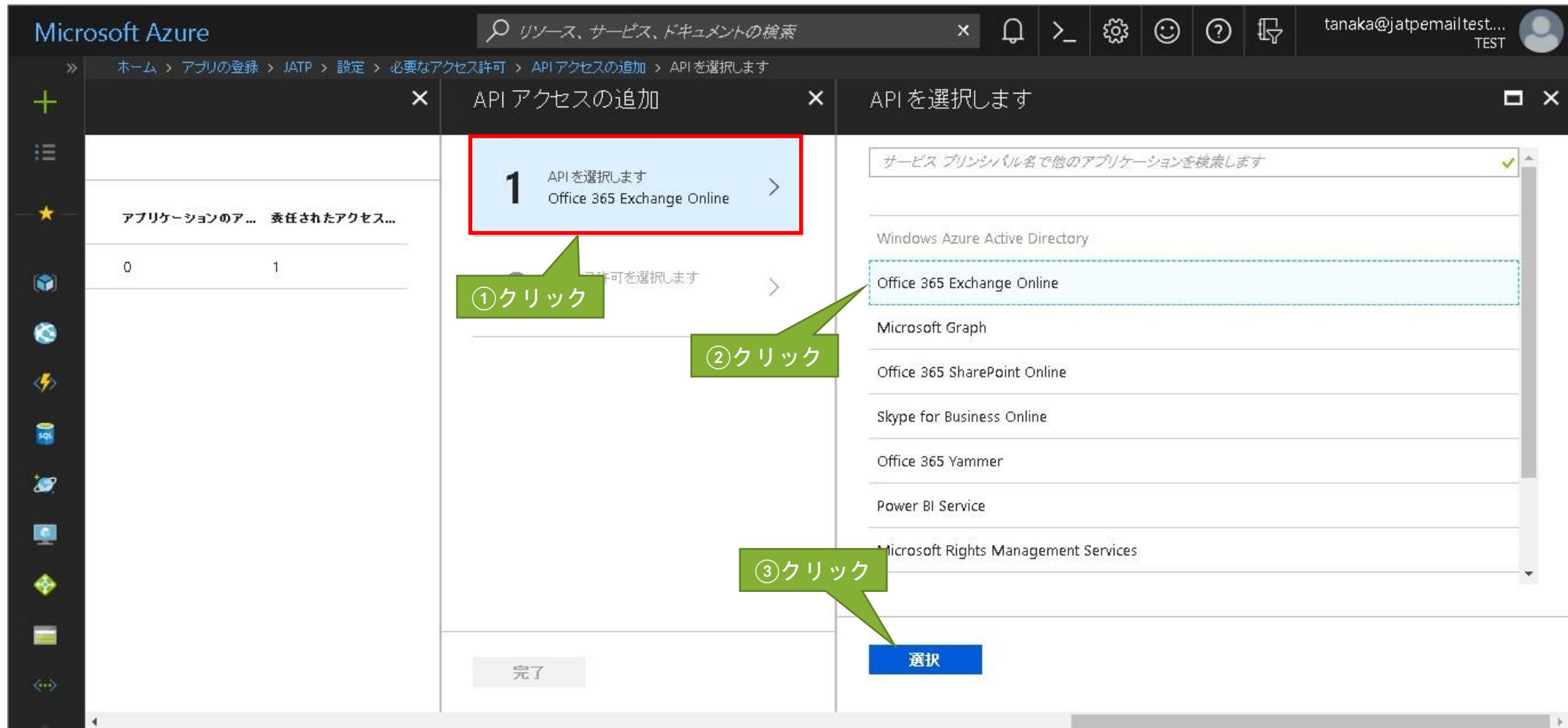
アプリケーション ID: f631a02e-8639-4f2d-9380-de679f550fc4
オブジェクト ID: 47de93f9-9645-4102-9f85-2ef3f50ec0c4
ローカル ディレクトリでのマネージド アプリケーション: JATP

必要なアクセス許可

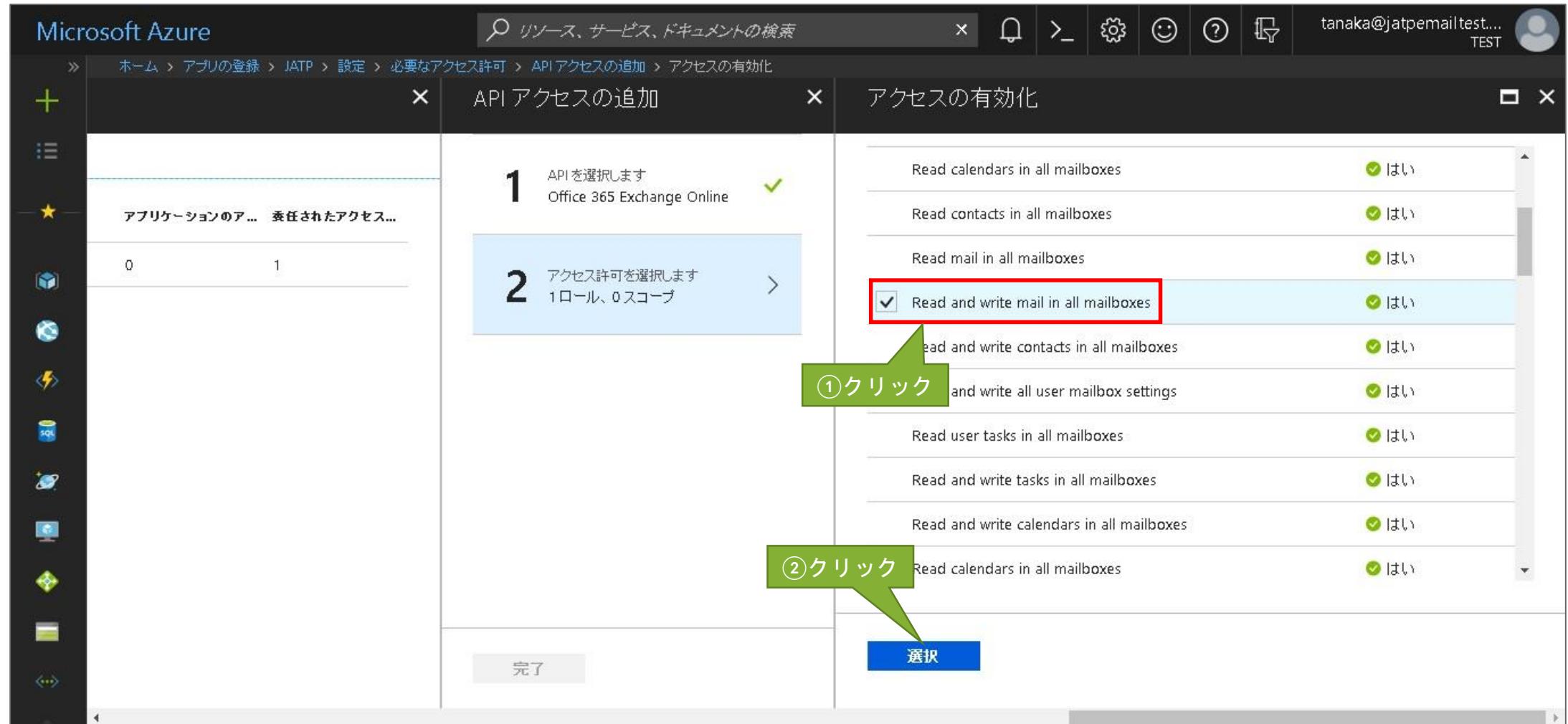
API クリック

Windows Azure Active Directory 0 1

OFFICE 365 MITIGATION設定手順 (BCC,MTA RECEIVER)



OFFICE 365 MITIGATION設定手順 (BCC,MTA RECEIVER)



OFFICE 365 MITIGATION設定手順 (BCC,MTA RECEIVER)

The screenshot shows the Microsoft Azure portal interface with three open windows:

- Left Window (Setting):** Shows the navigation menu with "必要なアクセス許可" (Required Access) selected in the "API Access" section.
- Middle Window (Required Access):** Shows the "Add" button and the "Grant permission" button. It lists "Windows Azure Active Directory" with 0 and 1 respectively.
- Right Window (Add API Access):** Shows two steps:
 - 1 API を選択します**: Office 365 Exchange Online (checked)
 - 2 アクセス許可を選択します**: 1 ロール、0 スコープ (checked)

A green callout bubble with the text "クリック" (Click) points to the "完了" (Done) button at the bottom right of the right window.

OFFICE 365 MITIGATION設定手順 (BCC,MTA RECEIVER)



Microsoft Azure リソース、サービス、ドキュメントの検索 tanaka@jatpemailtest... TEST

ホーム > アプリの登録 > JATP > 設定 > 必要なアクセス許可

設定 必要なアクセス許可

必要なアクセス許可

+ 追加 アクセス許可の付与

API アプリケーションのア... 委任されたアクセ...

| 権限 | アカウント | 委任された権限 |
|--------------------------------|-------|---------|
| Windows Azure Active Directory | 0 | 1 |
| Office 365 Exchange Online | 1 | 0 |

クリック

必要なアクセス許可

キー

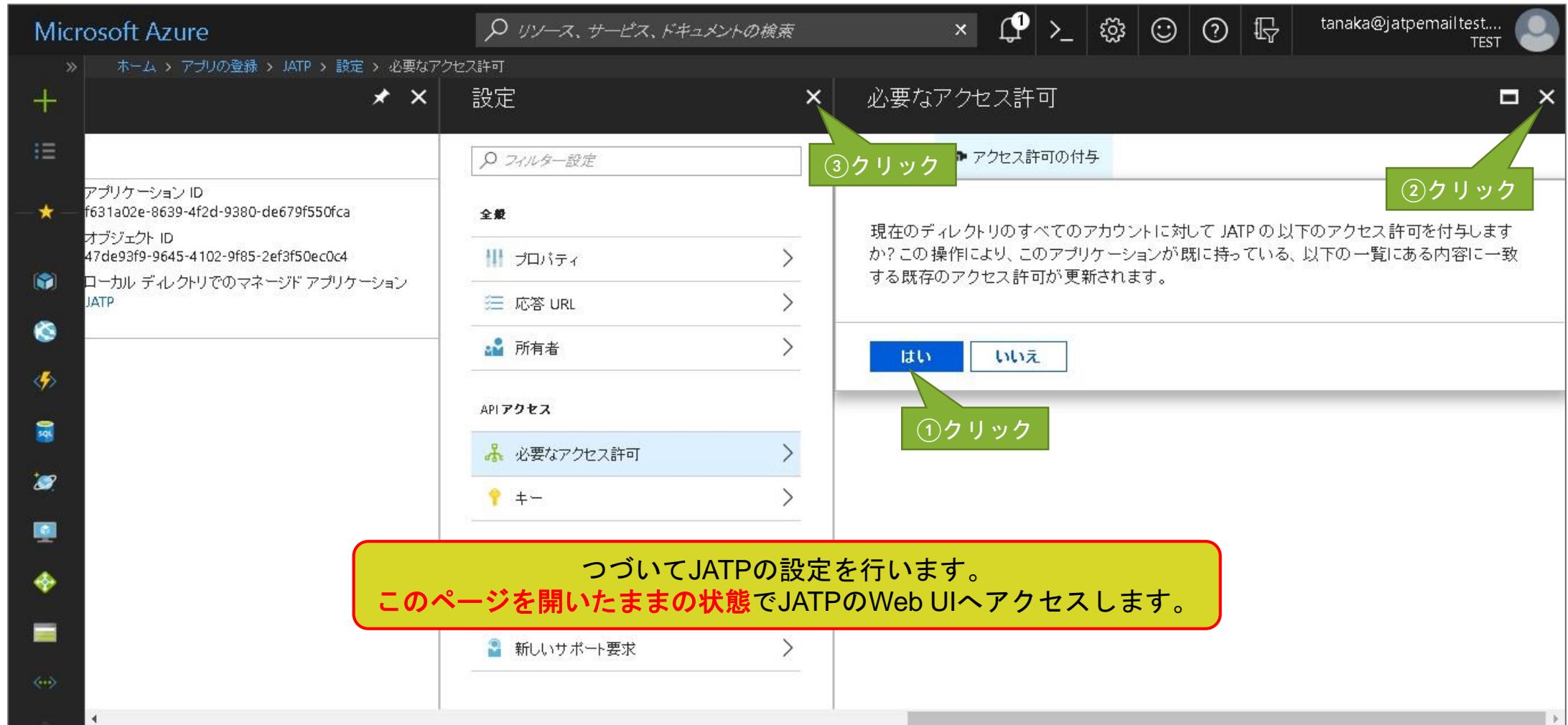
トラブルシューティング + サポート

トラブルシューティング

新しいサポート要求

アプリケーション ID: f631a02e-8639-4f2d-9380-de679f550fc4
オブジェクト ID: 47de93f9-9645-4102-9f85-2ef3f50ec0c4
ローカル ディレクトリでのマネージド アプリケーション: JATP

OFFICE 365 MITIGATION設定手順 (BCC,MTA RECEIVER)



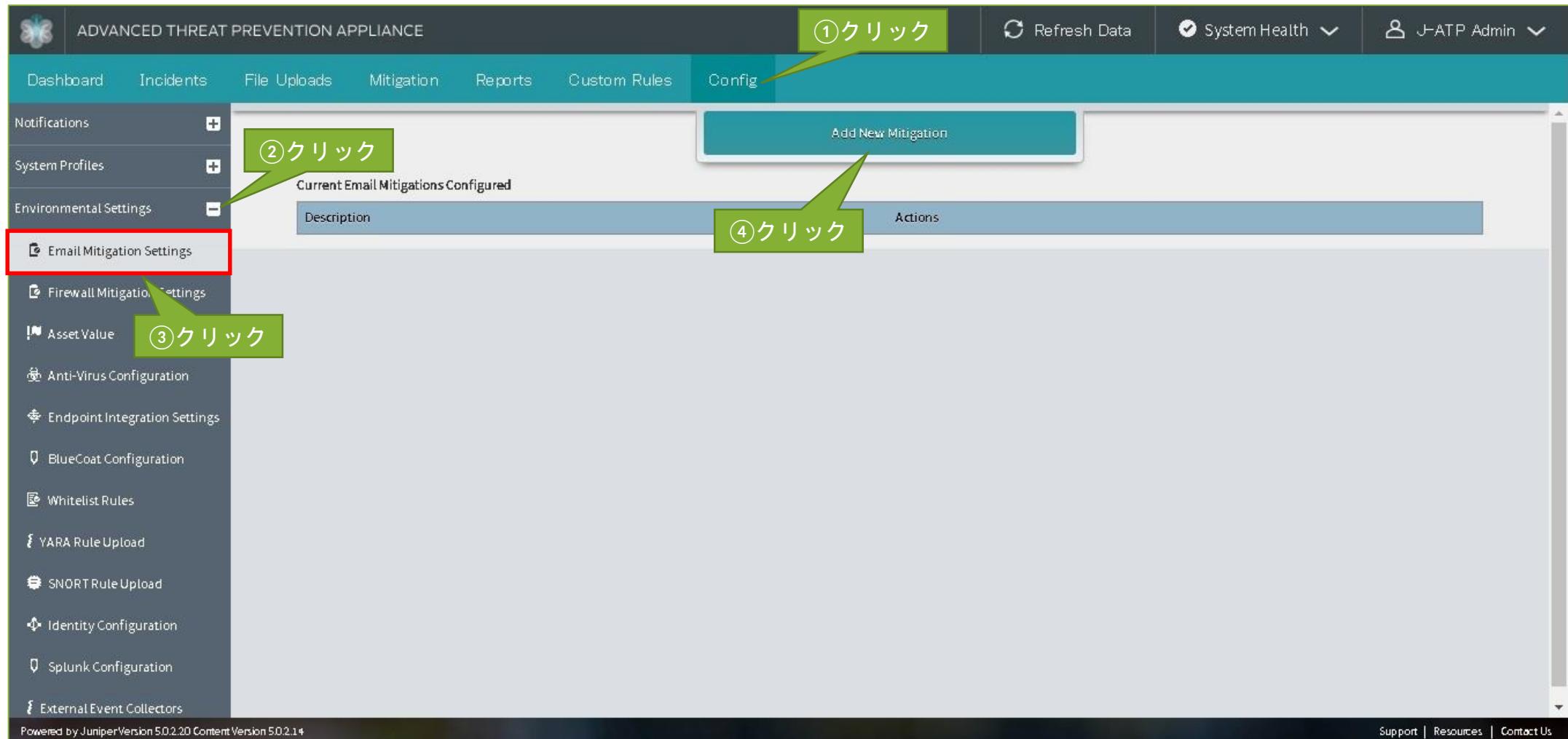
つづいてJATPの設定を行います。
このページを開いたままの状態でJATPのWeb UIへアクセスします。

①クリック

②クリック

③クリック

OFFICE 365 MITIGATION設定手順 (BCC,MTA RECEIVER)



OFFICE 365 MITIGATION設定手順 (BCC,MTA RECEIVER)

①クリック

②ディレクトリIDを入力

③アプリケーションIDを入力

④隔離用フォルダの名称を入力

⑤チェックを入れる

⑥保護対象のドメインを入力

⑦クリック

ADVANCED THREAT PREVENTION APPLIANCE

Refresh Data

System Health

J-ATP Admin

Dashboard Incidents File Uploads Mitigation Reports Custom Rules Config

Notifications

System Profiles

Environmental Settings

Endpoint Integration Settings

BlueCoat Configuration

Whitelist Rules

YARA Rule Upload

SNORT Rule Upload

Identity Configuration

Splunk Configuration

External Event Collectors

Powered by Juniper Version 5.0.2.20 Content Version 5.0.2.14

Support | Resources | Contact Us

Current Email Mitigations Configured

| Description | Actions |
|-------------|--|
| Gmail | <input type="button" value="Disable"/> <input type="button" value="Delete"/> <input type="button" value="Edit"/> <input type="button" value="Test"/> |

Generate New Azure Key Credentials

Key Bits: 4096

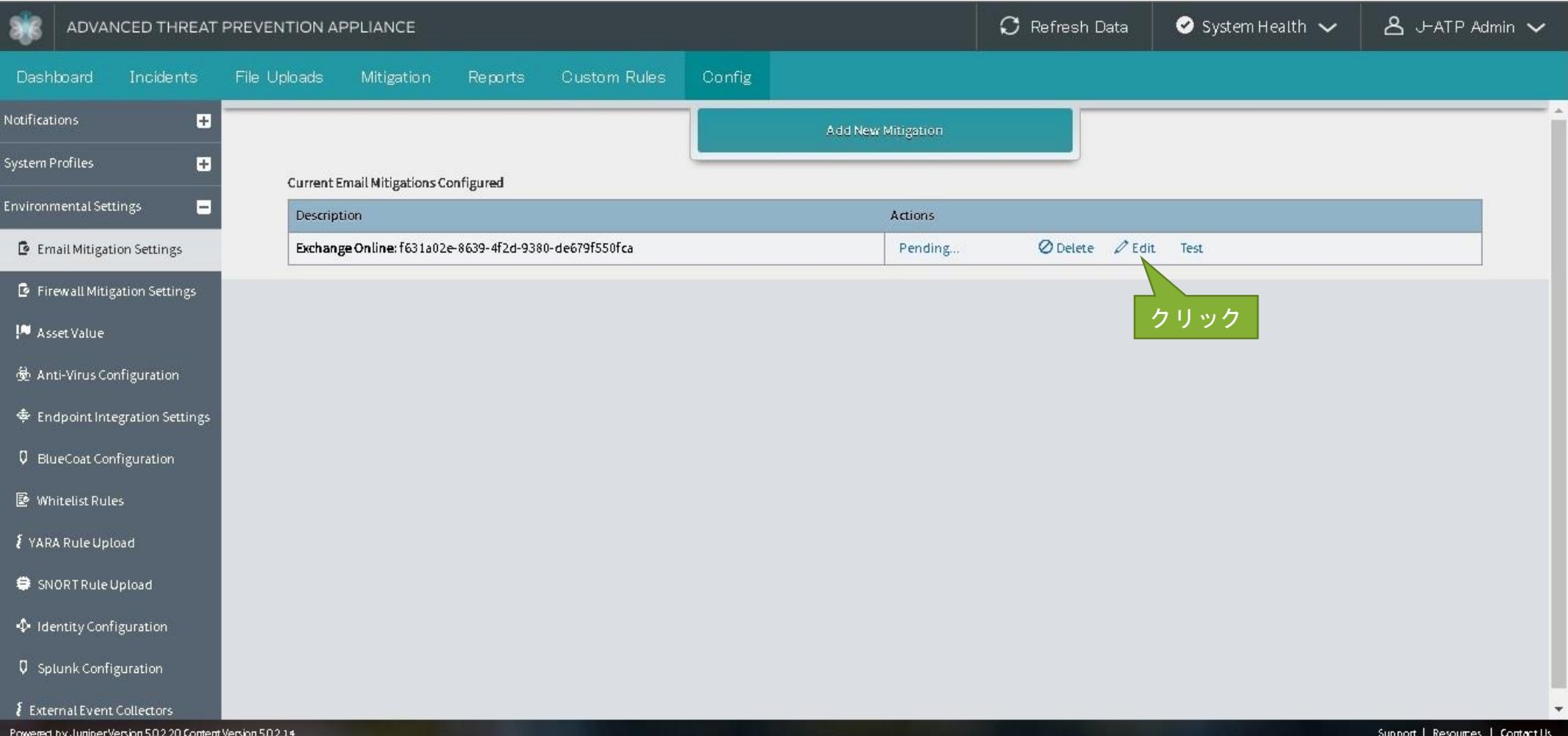
Certificate Lifetime (Days): 3650

Domains: jatpemailtest.onmicrosoft.com

Add

Cancel

OFFICE 365 MITIGATION設定手順 (BCC,MTA RECEIVER)



ADVANCED THREAT PREVENTION APPLIANCE

Refresh Data System Health J-ATP Admin

Dashboard Incidents File Uploads Mitigation Reports Custom Rules Config

Notifications +

System Profiles +

Environmental Settings -

Email Mitigation Settings

Firewall Mitigation Settings

Asset Value

Anti-Virus Configuration

Endpoint Integration Settings

BlueCoat Configuration

Whitelist Rules

YARA Rule Upload

SNORT Rule Upload

Identity Configuration

Splunk Configuration

External Event Collectors

Add New Mitigation

Current Email Mitigations Configured

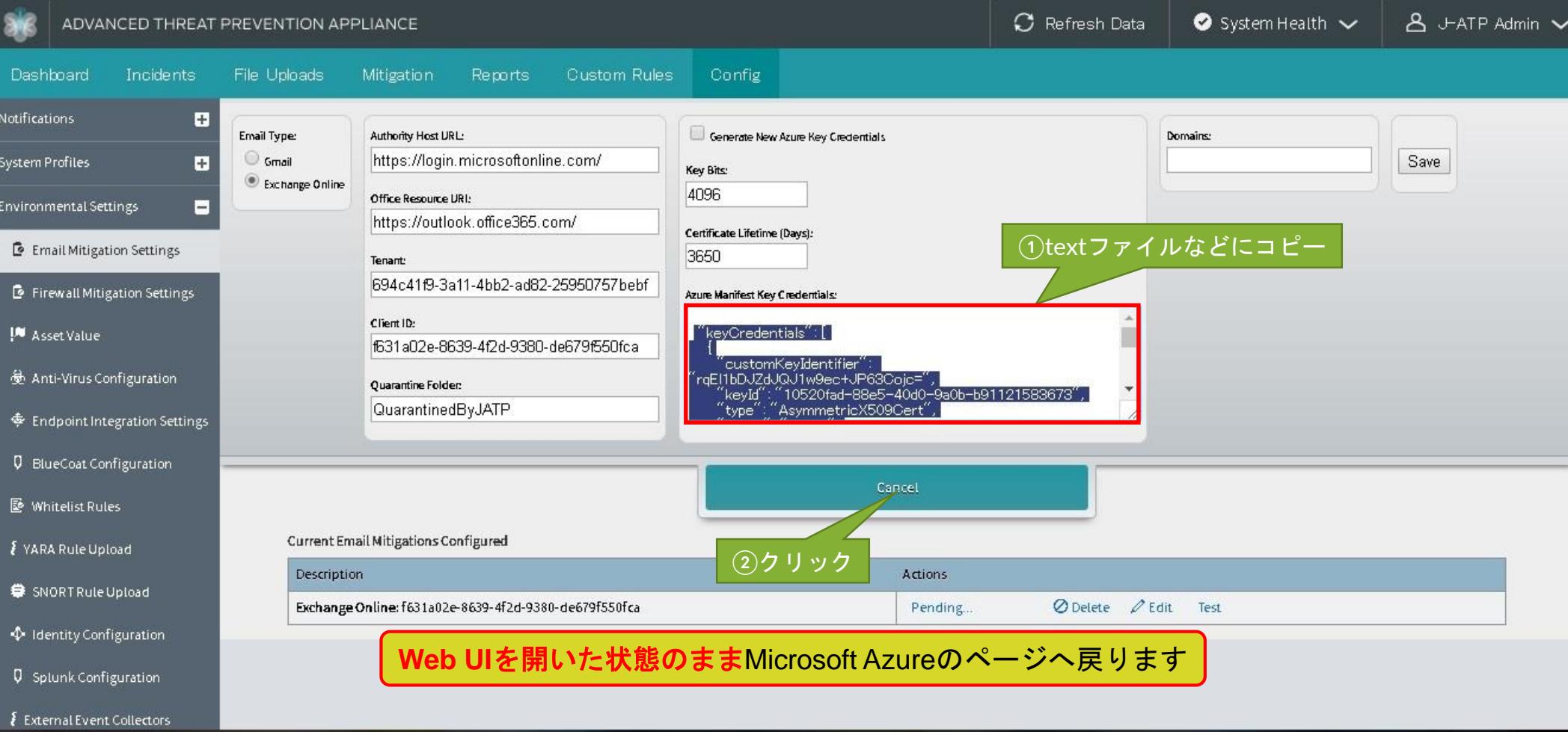
| Description | Actions |
|--|-----------------------------|
| Exchange Online:f631a02e-8639-4f2d-9380-de679f550fca | Pending... Delete Edit Test |

クリック

Powered by Juniper Version 5.0.2.20 Content Version 5.0.2.14

Support | Resources | Contact Us

OFFICE 365 MITIGATION 設定手順 (BCC, MTA RECEIVER)

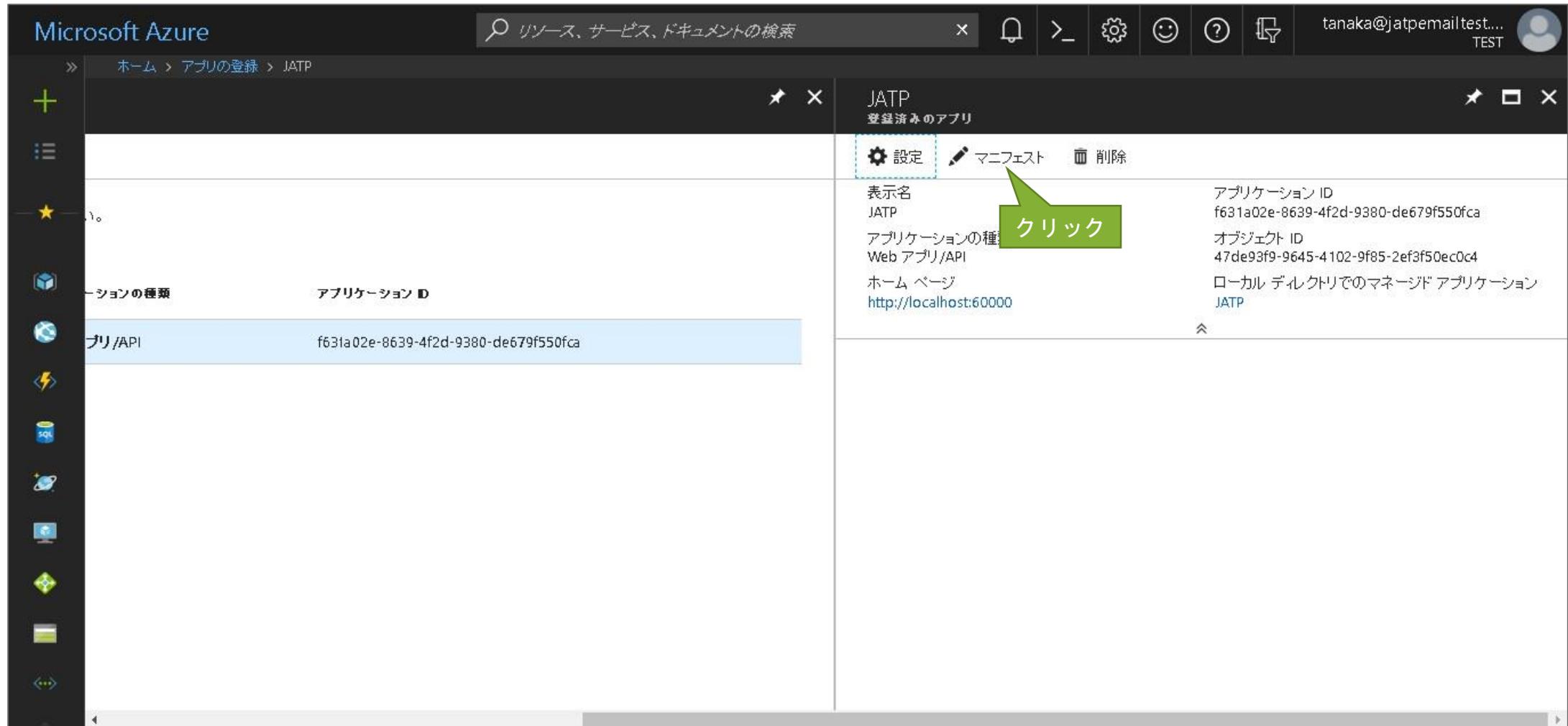


①textファイルなどにコピー

②クリック

Web UIを開いた状態のまま Microsoft Azureのページへ戻ります

OFFICE 365 MITIGATION設定手順 (BCC,MTA RECEIVER)



Microsoft Azure リソース、サービス、ドキュメントの検索 tanaka@jatpemailtest... TEST

ホーム > アプリの登録 > JATP

JATP 設定済みのアプリ

設定 マニフェスト 削除

表示名: JATP
アプリケーションの種類: Web アプリ/API
ホームページ: <http://localhost:60000>

アプリケーション ID: f631a02e-8639-4f2d-9380-de679f550fca
オブジェクト ID: 47de93f9-9645-4102-9f85-2ef3f50ec0c4
ローカル ディレクトリでのマネージド アプリケーション: JATP

クリック

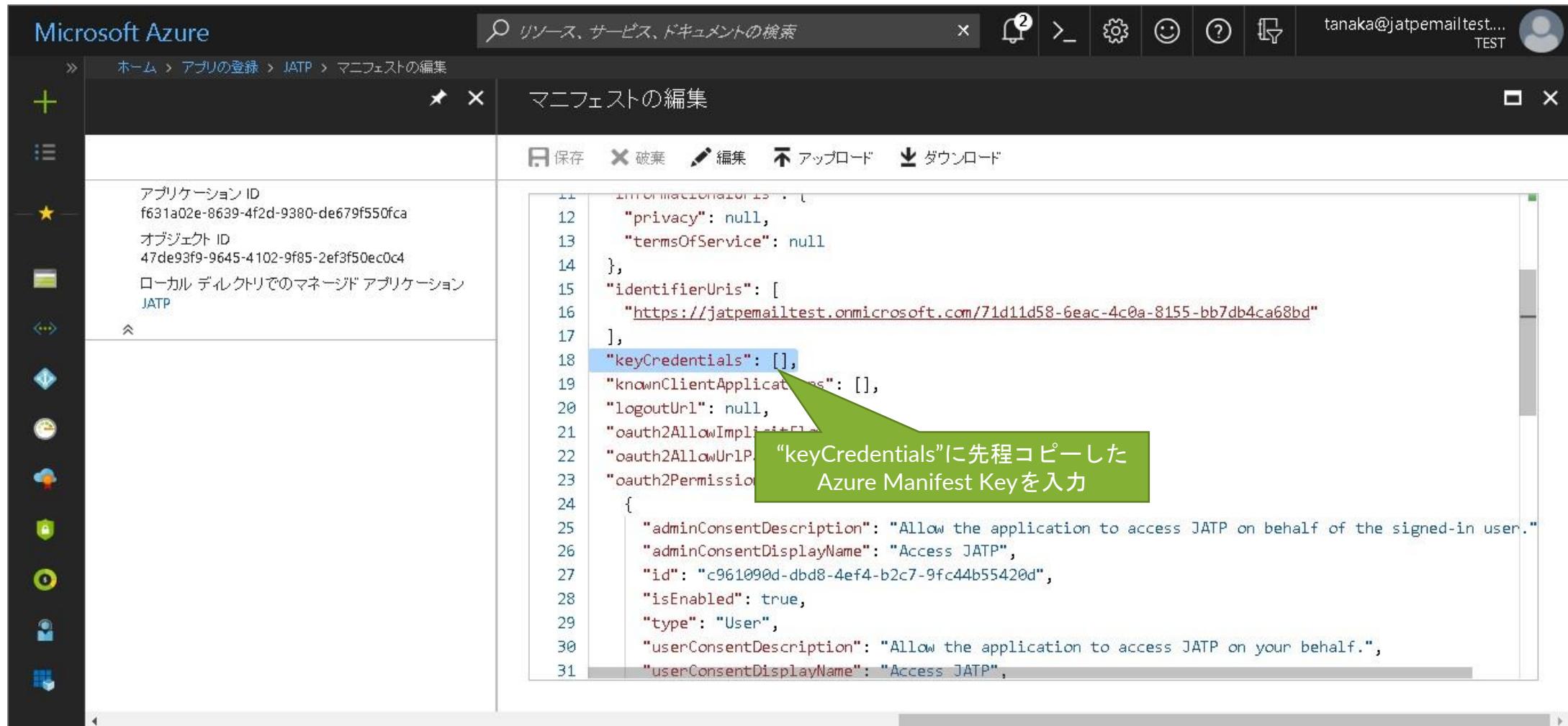
アプリケーションの種類

アプリケーション ID

API/API

f631a02e-8639-4f2d-9380-de679f550fca

OFFICE 365 MITIGATION設定手順 (BCC,MTA RECEIVER)



Microsoft Azure リソース、サービス、ドキュメントの検索 tanaka@jatpemailtest... TEST

ホーム > アプリの登録 > JATP > マニフェストの編集

マニフェストの編集

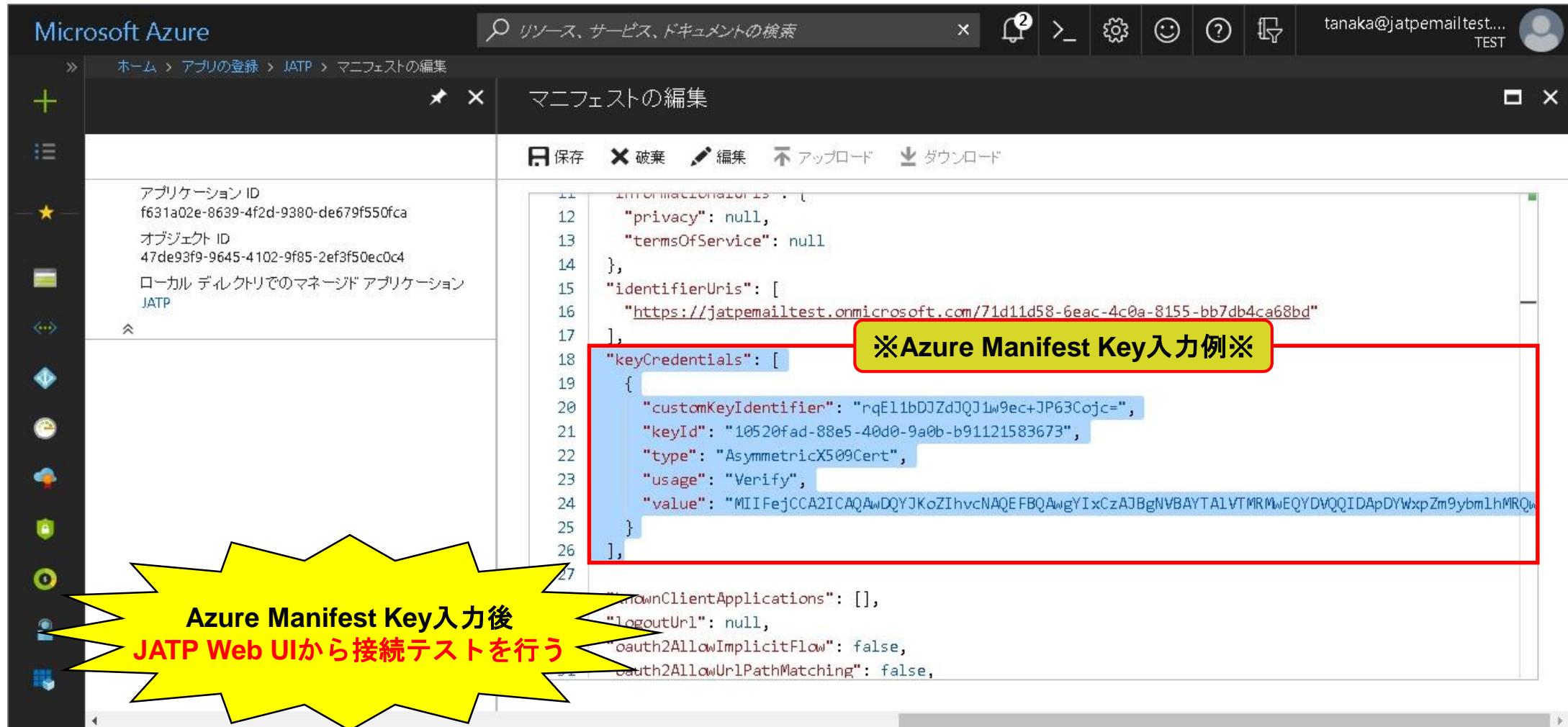
保存 破棄 編集 アップロード ダウンロード

| | | |
|---|---|-------------------------------------|
| アプリケーション ID f631a02e-8639-4f2d-9380-de679f550fca | オブジェクト ID 47de93f9-9645-4102-9f85-2ef3f50ec0c4 | ローカル ディレクトリでのマネージド アプリケーション JATP |
|---|---|-------------------------------------|

```
11 "informationalUrls": {  
12   "privacy": null,  
13   "termsOfService": null  
14 },  
15 "identifierUris": [  
16   "https://jatpemailtest.onmicrosoft.com/71d11d58-6eac-4c0a-8155-bb7db4ca68bd"  
17 ],  
18 "keyCredentials": [],  
19 "knownClientApplications": [],  
20 "logoutUrl": null,  
21 "oauth2AllowImplicitFlow": true,  
22 "oauth2AllowUrlRevoke": true,  
23 "oauth2Permissions": {  
24   "adminConsentDescription": "Allow the application to access JATP on behalf of the signed-in user.",  
25   "adminConsentDisplayName": "Access JATP",  
26   "id": "c961090d-dbd8-4ef4-b2c7-9fc44b55420d",  
27   "isEnabled": true,  
28   "type": "User",  
29   "userConsentDescription": "Allow the application to access JATP on your behalf.",  
30   "userConsentDisplayName": "Access JATP",  
31 }
```

“keyCredentials”に先程コピーした Azure Manifest Key を入力

OFFICE 365 MITIGATION設定手順 (BCC,MTA RECEIVER)



Microsoft Azure リソース、サービス、ドキュメントの検索 tanaka@jatpemailtest... TEST

ホーム > アプリの登録 > JATP > マニフェストの編集

マニフェストの編集

保存 破棄 編集 アップロード ダウンロード

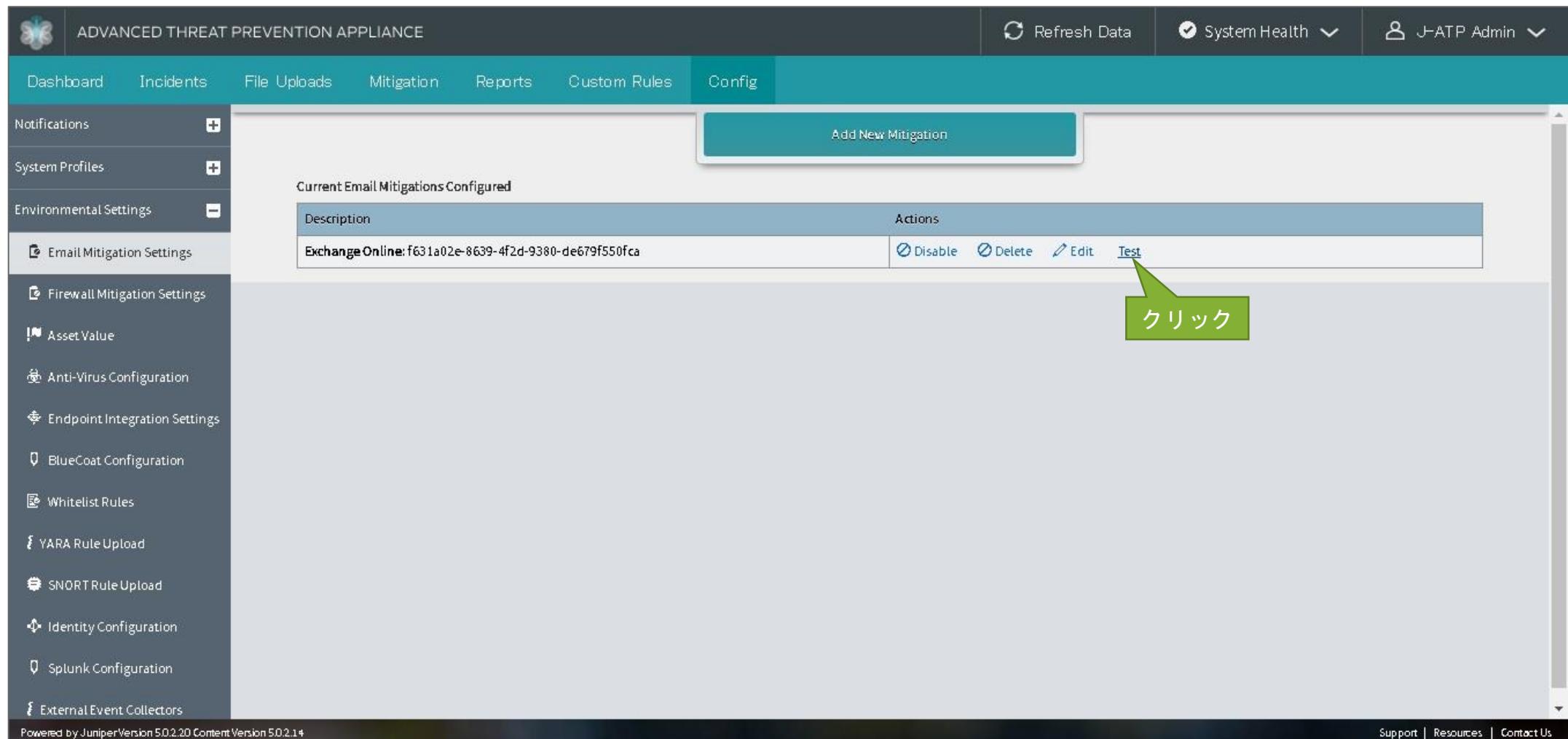
アプリケーション ID: f631a02e-8639-4f2d-9380-de679f550fca
オブジェクト ID: 47de93f9-9645-4102-9f85-2ef3f50ec0c4
ローカル ディレクトリでのマネージド アプリケーション: JATP

```
11 "informationalUrls": {  
12     "privacy": null,  
13     "termsOfService": null  
14 },  
15 "identifierUris": [  
16     "https://jatpemailtest.onmicrosoft.com/71d11d58-6eac-4c0a-8155-bb7db4ca68bd"  
17 ],  
18 "keyCredentials": [  
19     {  
20         "customKeyIdentifier": "rqE11bDJZdJQJ1w9ec+JP63Cojc=",  
21         "keyId": "10520fad-88e5-40d0-9a0b-b91121583673",  
22         "type": "AsymmetricX509Cert",  
23         "usage": "Verify",  
24         "value": "MIIEejCCA2ICAQAwDQYJKoZIhvcNAQEFBQAwgYIxszAJBgNVBAYTA1VTMRMwEQYDVQQIDAoDYWxpZm9ybmlhMRQw  
25     }  
26 ],  
27 "knownClientApplications": [],  
28 "logoutUrl": null,  
29 "oauth2AllowImplicitFlow": false,  
30 "oauth2AllowUrlPathMatching": false,
```

※Azure Manifest Key入力例※

Azure Manifest Key入力後
JATP Web UIから接続テストを行う

OFFICE 365 MITIGATION設定手順 (BCC,MTA RECEIVER)



ADVANCED THREAT PREVENTION APPLIANCE

Refresh Data System Health J-ATP Admin

Dashboard Incidents File Uploads Mitigation Reports Custom Rules Config

Notifications +

System Profiles +

Environmental Settings -

Email Mitigation Settings

Firewall Mitigation Settings

Asset Value

Anti-Virus Configuration

Endpoint Integration Settings

BlueCoat Configuration

Whitelist Rules

YARA Rule Upload

SNORT Rule Upload

Identity Configuration

Splunk Configuration

External Event Collectors

Add New Mitigation

Current Email Mitigations Configured

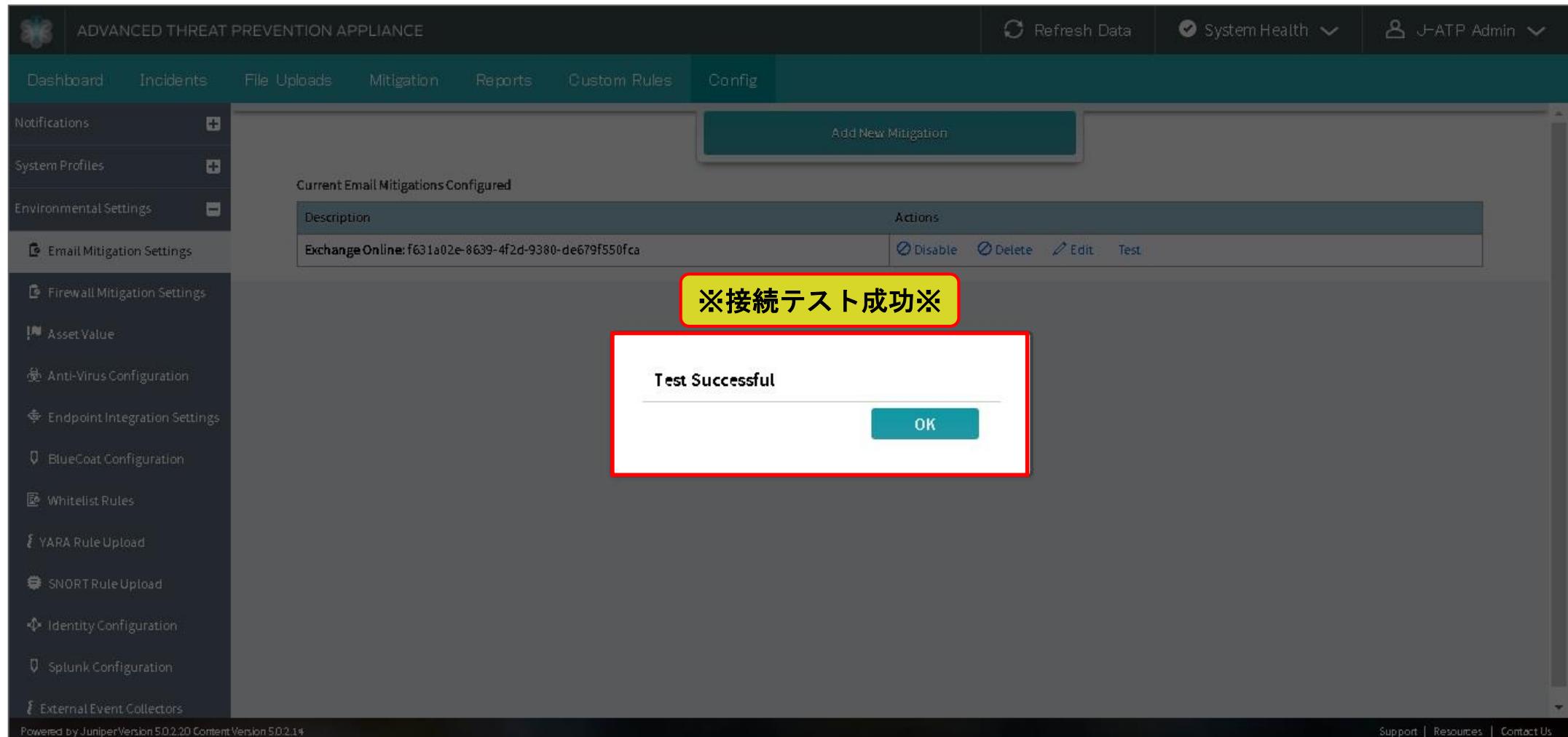
| Description | Actions |
|--|--------------------------|
| Exchange Online:f631a02e-8639-4f2d-9380-de679f550fca | Disable Delete Edit Test |

クリック

Powered by Juniper Version 5.0.2.20 Content Version 5.0.2.14

Support | Resources | Contact Us

OFFICE 365 MITIGATION設定手順 (BCC,MTA RECEIVER)



ADVANCED THREAT PREVENTION APPLIANCE

Refresh Data System Health J-ATP Admin

Dashboard Incidents File Uploads Mitigation Reports Custom Rules Config

Notifications System Profiles Environmental Settings Email Mitigation Settings Firewall Mitigation Settings Asset Value Anti-Virus Configuration Endpoint Integration Settings BlueCoat Configuration Whitelist Rules YARA Rule Upload SNORT Rule Upload Identity Configuration Splunk Configuration External Event Collectors

Add New Mitigation

Current Email Mitigations Configured

| Description | Actions |
|---|--------------------------|
| Exchange Online: f631a02e-8639-4f2d-9380-de679f550fca | Disable Delete Edit Test |

※接続テスト成功※

Test Successful

OK

Powered by Juniper Version 5.0.2.20 Content Version 5.0.2.14

Support | Resources | Contact Us

OFFICE 365 MITIGATION設定手順 (BCC,MTA RECEIVER)

The screenshot shows the ATPA interface with the 'Config' tab selected. A message box in the center says 'Unable to obtain access token' with an 'OK' button. A yellow box with a red border highlights this message. A large yellow starburst graphic points to the message box from the left, containing Japanese text about connection test failures.

※接続テスト失敗※

Unable to obtain access token

OK

この場合、以下の可能性が考えられます

- ・APIアクセス権を付与していない(P.82~)
- ・ディレクトリID/アプリケーションIDが違う
(P.77/P.81)

Powered by Juniper Version 5.0.2.20 Content Version 5.0.2.14

Support | Resources | Contact Us

OFFICE 365 MITIGATION設定手順 (BCC,MTA RECEIVER)

※Mitigation動作一例※

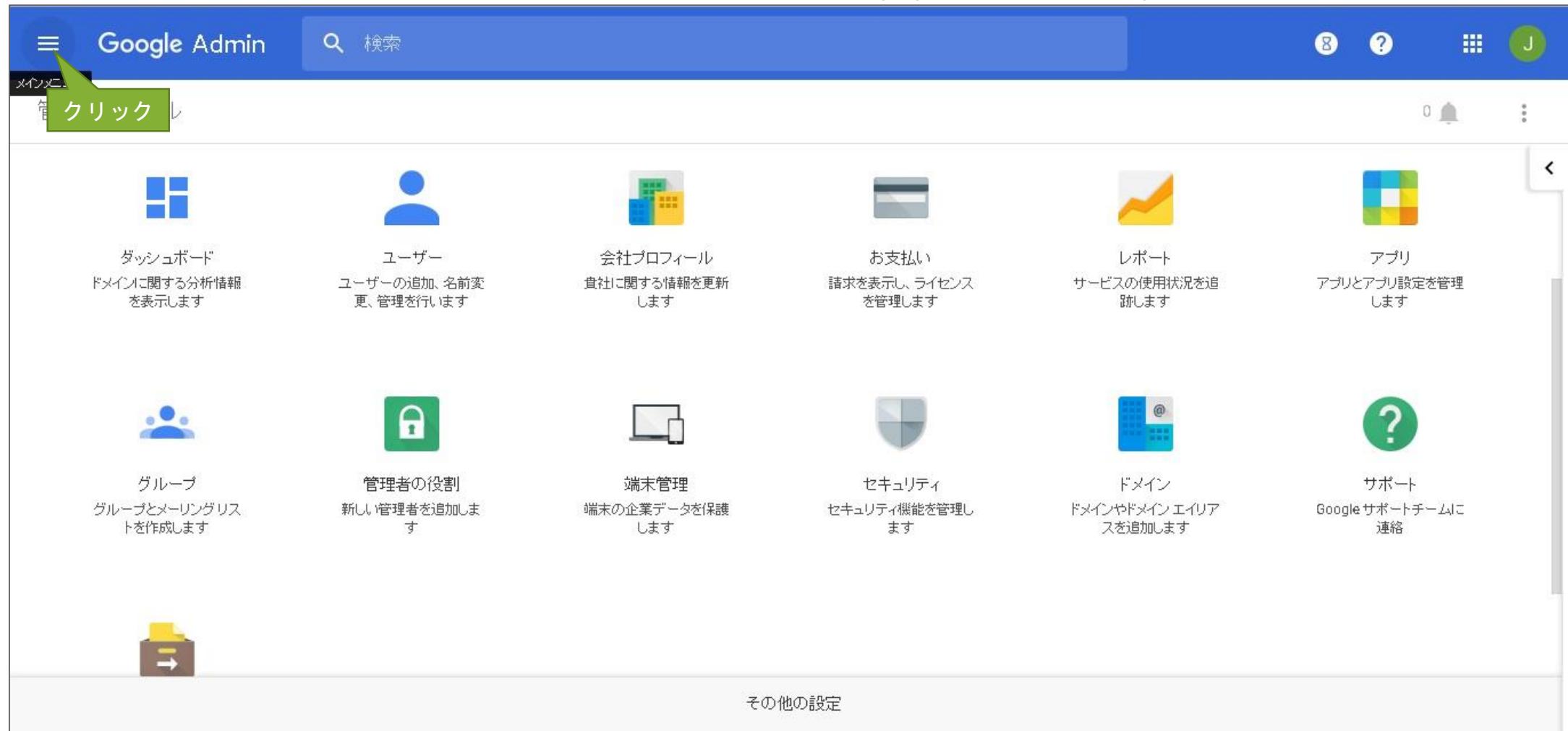
The screenshot shows the Microsoft Outlook interface with a yellow box highlighting the title '※Mitigation動作一例※'. The left sidebar shows a folder structure with 'QuarantinedByJATP' selected, which has 1 item. The main pane displays an email from '山田太郎 <sb.ymd.2z.0364@gmail.com>' with the subject 'test'. The email was sent at 12:30 today by '田中次郎'. A download link for 'slimcleanerplus.zip' (129 KB) is shown. The message body contains '(メッセージ テキストなし)'. The top navigation bar includes 'Office 365' and 'Outlook' buttons, and a ribbon with '新規作成', '削除', 'アーカイブ', '迷惑メール', '一括処理', '移動', '分類', and '...'. The top right corner has icons for settings, help, and a user profile.



G Suite ジャーナル設定手順 (BCC, MTA Receiver)

G SUITE ジャーナル設定手順 (BCC,MTA RECEIVER)

管理者アカウントでログイン後、管理ホーム画面（<https://admin.google.com/AdminHomeGoogle>）へアクセス



Google Admin

管理者アカウントでログイン後、管理ホーム画面（<https://admin.google.com/AdminHomeGoogle>）へアクセス

クリック

メインメニュー

検索

0 ベル

⋮

Google Admin

ダッシュボード

会社に関する分析情報を表示します

ユーザー

ユーザーの追加、名前変更、管理を行います

会社プロフィール

会社に関する情報を更新します

お支払い

請求を表示し、ライセンスを管理します

レポート

サービスの使用状況を追跡します

アプリ

アプリとアプリ設定を管理します

グループ

グループとメーリングリストを作成します

管理者の役割

新しい管理者を追加します

端末管理

端末の企業データを保護します

セキュリティ

セキュリティ機能を管理します

ドメイン

ドメインやドメインエイリアスを追加します

サポート

Googleサポートチームに連絡

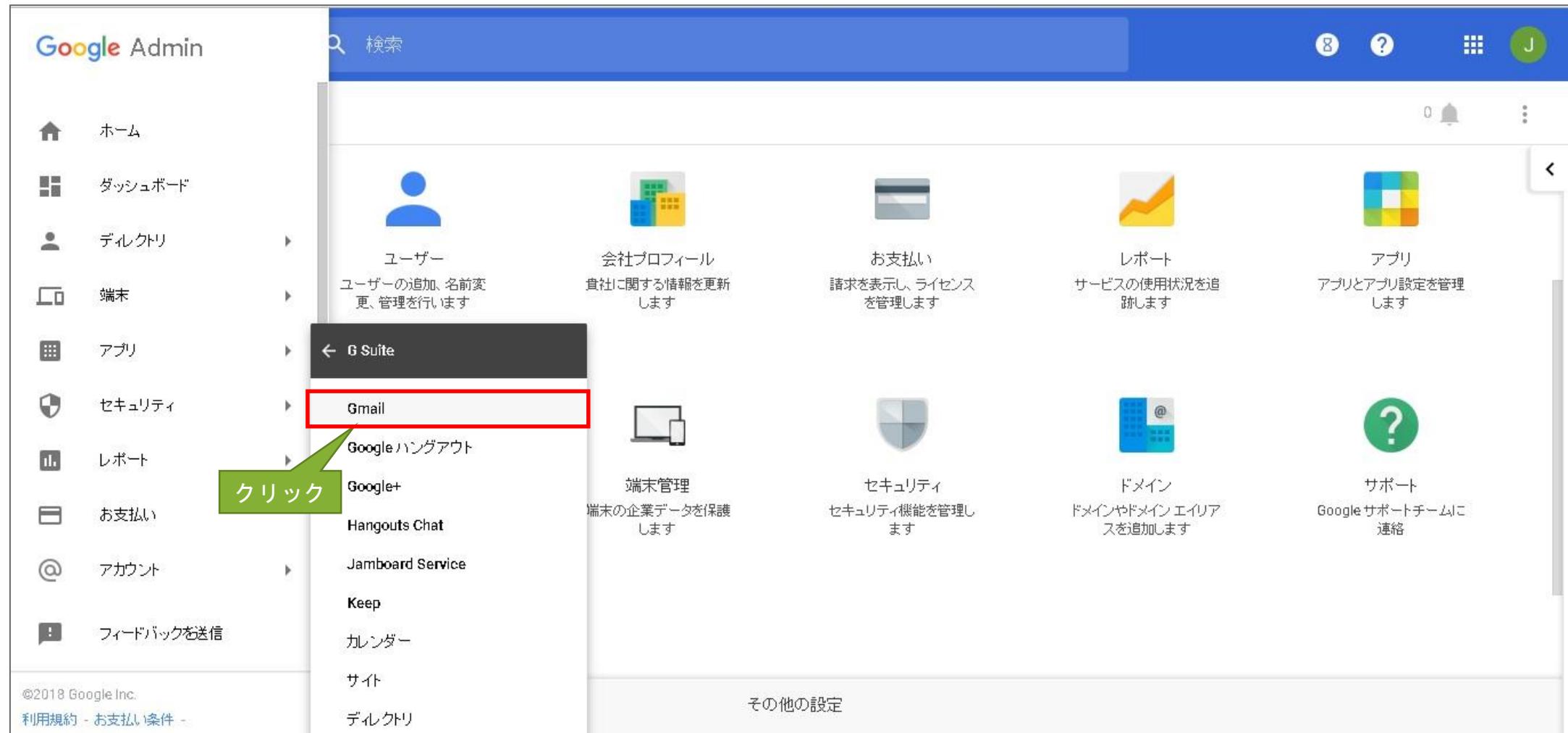
その他の設定

G SUITE ジャーナル設定手順 (BCC,MTA RECEIVER)



The screenshot shows the Google Admin console interface. The left sidebar has a red box around the 'ホーム' (Home) button. The 'アプリ' (App) button is also highlighted with a red box. A green box with the text 'クリック' (Click) is placed over the 'G Suite' icon in the main content area. The 'G Suite' icon is surrounded by other service icons: '会社プロフィール' (Company Profile), 'お支払い' (Billing), 'レポート' (Report), 'アプリ' (App), '管理者の役割' (Manager's Role), '端末管理' (Device Management), 'セキュリティ' (Security), 'ドメイン' (Domain), and 'サポート' (Support). The main menu bar at the top includes 'Google Admin', a search bar, and various navigation icons.

G SUITE ジャーナル設定手順 (BCC,MTA RECEIVER)



G SUITE ジャーナル設定手順 (BCC, MTA RECEIVER)



G SUITE ジャーナル設定手順 (BCC, MTA RECEIVER)



全般設定 メールアドレス一覧 ホスト デフォルトの転送 Labs 検索

設定項目を検索

セットアップ

ウェブアドレス ユーザー用の Gmail の URL:
ローカルに適用しました <https://mail.google.com/a/jatp-test.ddo.jp>

[URL を変更](#)

MXレコード jatp-test.ddo.jp の現在の MXレコード:

| 優先順位 | 参照先 |
|------|--------------------------|
| 10 | ASPMX.L.GOOGLE.COM. |
| 20 | ALT1.ASPMX.L.GOOGLE.COM. |

MX 設定の手順

配信を制限 まだ設定されていません ユーザーにメールの送受信を許可するドメインを制限します。

コンテンツコンプライアンス まだ設定されていません 単語、フレーズ、パターンに基づいた高度なコンテンツフィルタを設定します。

設定

クリック

不快なコンテンツ まだ設定されていません 単語リストに基づいたコンテンツフィルタを設定します。

G SUITE ジャーナル設定手順 (BCC, MTA RECEIVER)



Google Admin

アプリ > G Suite > Gmailの設定 > 詳細設定

全般設定 メールアドレス一覧 ホスト デフォルトの転送 Labs 検索

設定項目を検索

①コンテンツ コンプライアンス名

包括的なメールストレージ 関連付けられているユーザ
まだ設定されていません

フッターを追加 法令遵守や情報提供、宣伝の
まだ設定されていません

配信を制限 次の一部がメールに一致する場合

コンテンツ コンプライアンス 単語、フレーズ、パターンに基づく
まだ設定されていません

不快なコンテンツ 単語リストに基づいたコンテンツ
まだ設定されていません

設定

設定を追加

コンテンツ コンプライアンス

必須: 設定の概要に表示される短い説明を入力します。

1. 影響を受けるメール

受信 送信 内部 - 送信 内部 - 受信

2. 各メッセージで検索するコンテンツを表す表現を追加

表現 追加 設定

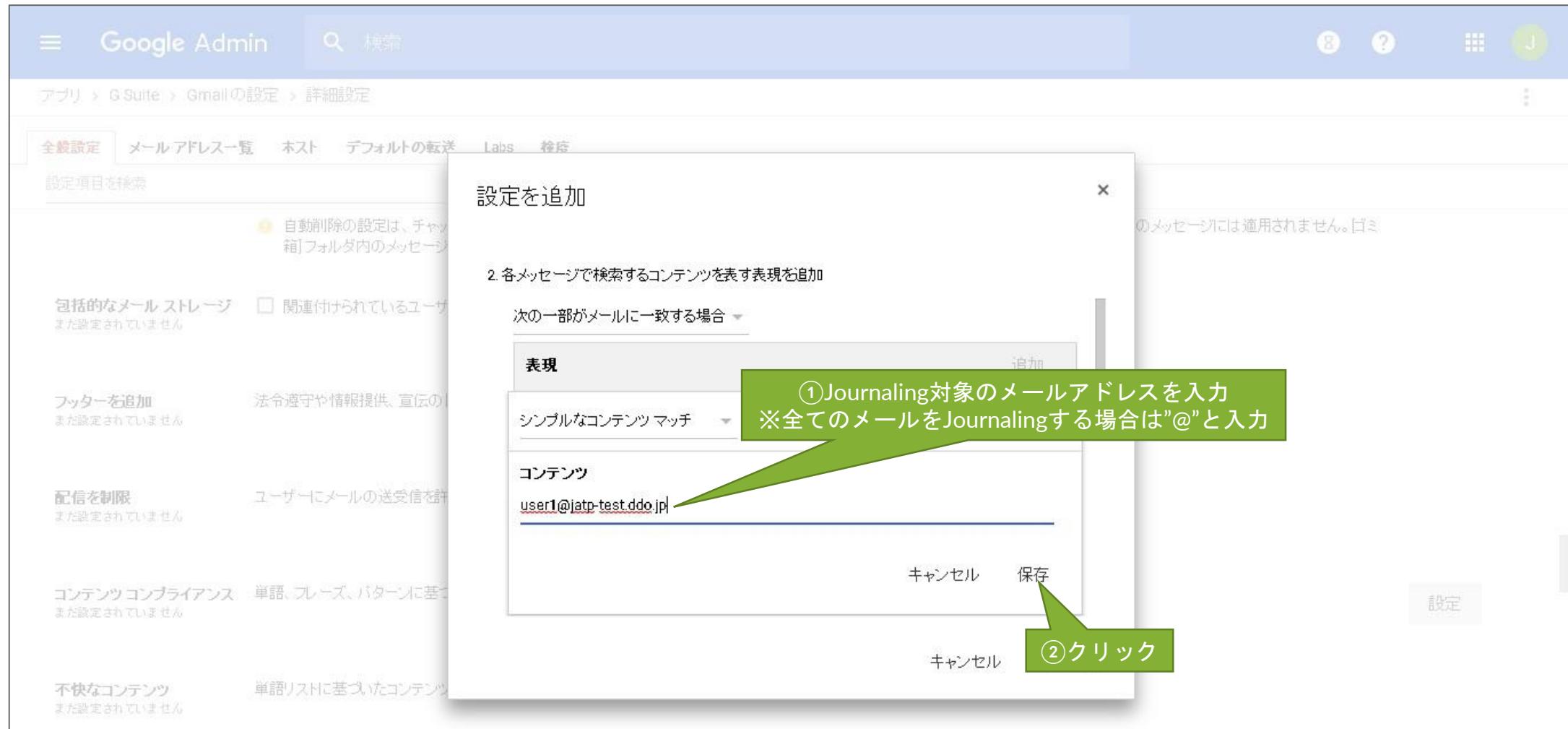
キャンセル 設定を追加

G SUITE ジャーナル設定手順 (BCC,MTA RECEIVER)

The screenshot shows the Google Admin interface for G Suite settings. The main menu path is 'アプリ > G Suite > Gmailの設定 > 詳細設定'. The '全般設定' tab is selected. A modal window titled '設定を追加' (Add setting) is open, showing the configuration for BCC and MTA Receiver. The modal has the following steps:

2. 各メッセージで検索するコンテンツを表す表現を追加
Next, one or more expressions are added to search for specific content in messages.
- ①一致条件を選択
②クリック
The '表現' (Expression) field is empty, and the '追加' (Add) button is highlighted with a green arrow and the label '②クリック' (Click).
3. 上記の表現が一致する場合は、次の処理を行います
The 'メッセージを変更' (Change message) section is shown, with the 'ヘッダー' (Header) section expanded. It contains two checkboxes:
 - X-Gm-Original-To ヘッダーを追加
 - X-Gm-Spam ヘッダーと X-Gm-Phishy ヘッダーを追加

G SUITE ジャーナル設定手順 (BCC,MTA RECEIVER)



G SUITE ジャーナル設定手順 (BCC, MTA RECEIVER)

※補足：更に詳細に条件設定することも可能です

設定を追加

高度なコンテンツ マッチ

場所

一致タイプ

テキストを含む

コンテンツ

user1@jatp-test.ddo.jp

キャンセル 保存

クリック

Google Admin

検索

アプリ > G Suite > Gmailの設定 > 詳細設定

全般設定 メールアドレス一覧 ホスト デフォルトの転送 Labs 痘症

設定項目を検索

自動削除の設定は、チャットボックス フォルダ内のメッセージ

包括的なメールストレージ 関連付けられているユーザー
まだ設定されていません

フッターを追加 法令遵守や情報提供、宣伝の

配信を制限 ユーザーにメールの送受信を許す

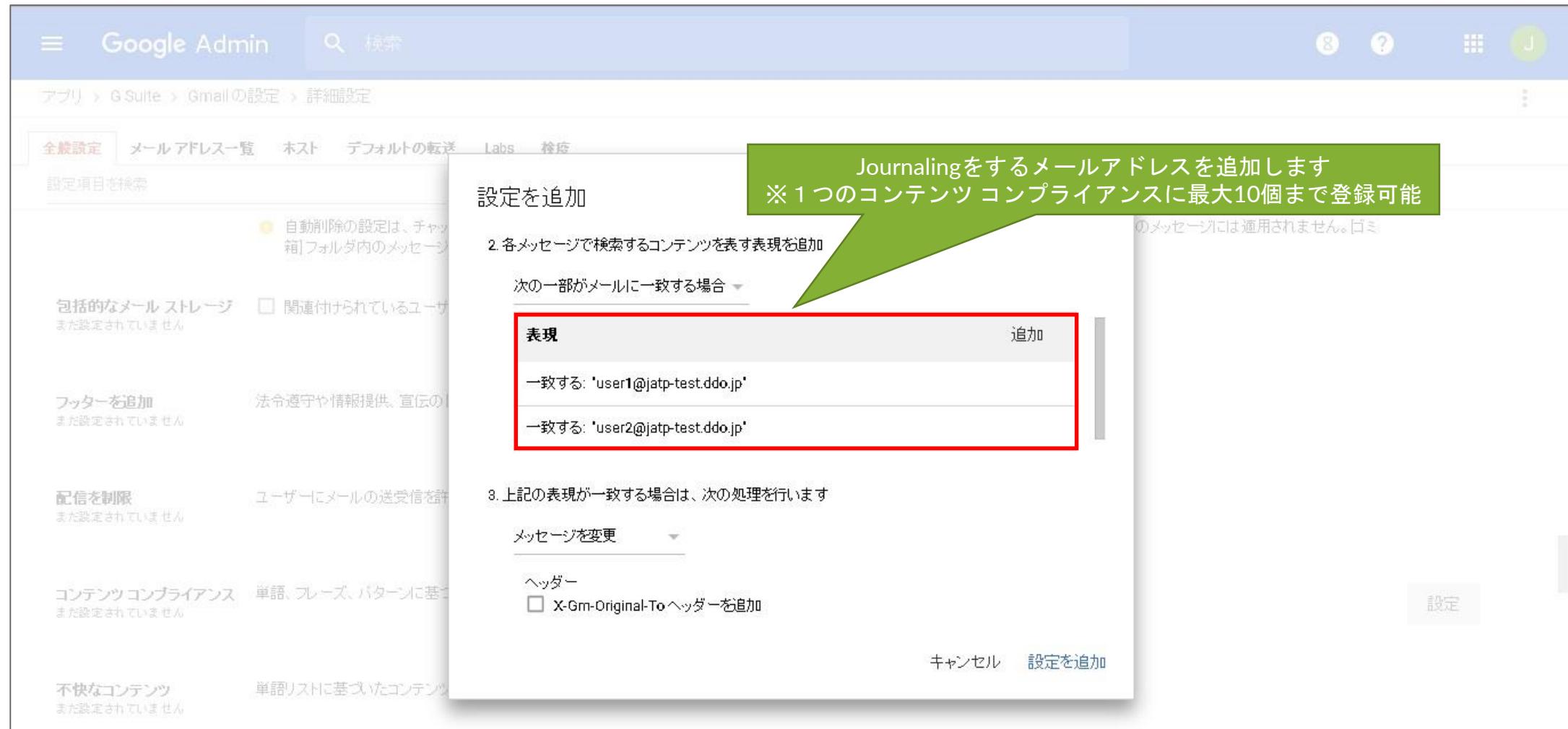
コンテンツコンプライアンス 単語、フレーズ、パターンに基づく

不快なコンテンツ 単語リストに基づいたコンテンツ

のメッセージには適用されません。ゴミ

設定

G SUITE ジャーナル設定手順 (BCC,MTA RECEIVER)



Google Admin

アプリ > G Suite > Gmailの設定 > 詳細設定

全般設定 メールアドレス一覧 ホスト デフォルトの転送 Labs 検索

設定項目を検索

自動削除の設定は、チャットボックス内にメッセージ

包括的なメールストレージ 関連付けられているユーザー
まだ設定されていません

フッターを追加
まだ設定されていません

配信を制限
ユーザーにメールの送受信を許す
まだ設定されていません

コンテンツコンプライアンス
単語、フレーズ、パターンに基づく
まだ設定されていません

不快なコンテンツ
単語リストに基づいたコンテンツ
まだ設定されていません

設定を追加

Journalingをするメールアドレスを追加します
※1つのコンテンツコンプライアンスに最大10個まで登録可能

2. 各メッセージで検索するコンテンツを表す表現を追加

次の一部がメールに一致する場合

表現 追加

一致する: 'user1@jatp-test.ddo.jp'

一致する: 'user2@jatp-test.ddo.jp'

3. 上記の表現が一致する場合は、次の処理を行います

メッセージを変更

ヘッダー
 X-Gm-Original-Toヘッダーを追加

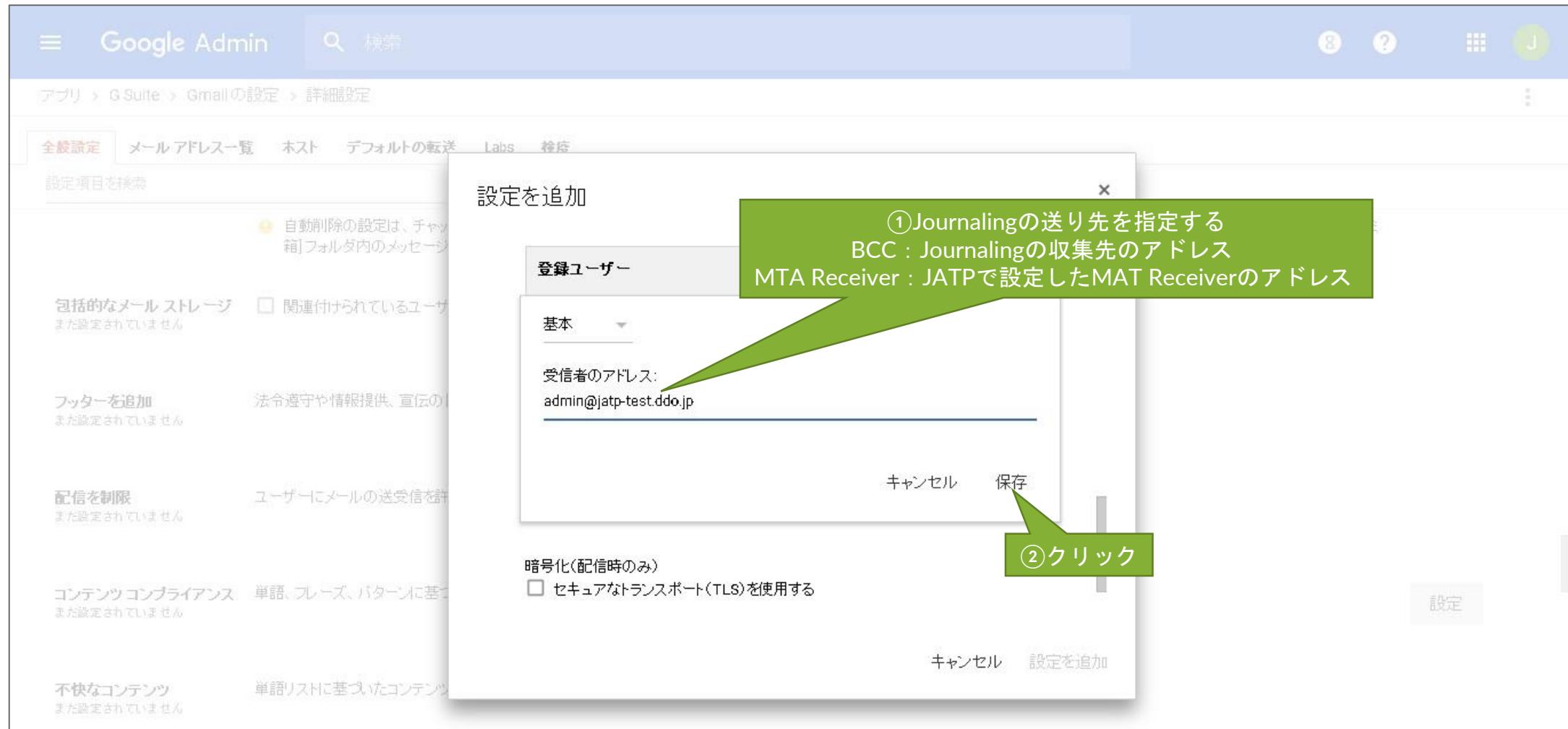
設定

キャンセル 設定を追加

G SUITE ジャーナル設定手順 (BCC,MTA RECEIVER)



G SUITE ジャーナル設定手順 (BCC, MTA RECEIVER)



G SUITE ジャーナル設定手順 (BCC, MTA RECEIVER)



G SUITE ジャーナル設定手順 (BCC, MTA RECEIVER)

The screenshot shows the Google Admin interface for G Suite Gmail settings. The top navigation bar includes 'Google Admin', a search bar, and various icons. The main page title is 'G Suite > Gmail の設定 > 詳細設定'. The '全般設定' tab is selected. A red box highlights the 'コンテンツ コンプライアンス' section, which contains 'Email Collector' and 'ローカルに適用しました'.

Below this, a green callout with the number ① points to a '確認' (Confirm) button. The '不快なコンテンツ' section is shown with the message 'まだ設定されていません'.

The '添付ファイルのコンプライアンス' section is also present with the message 'まだ設定されていません'.

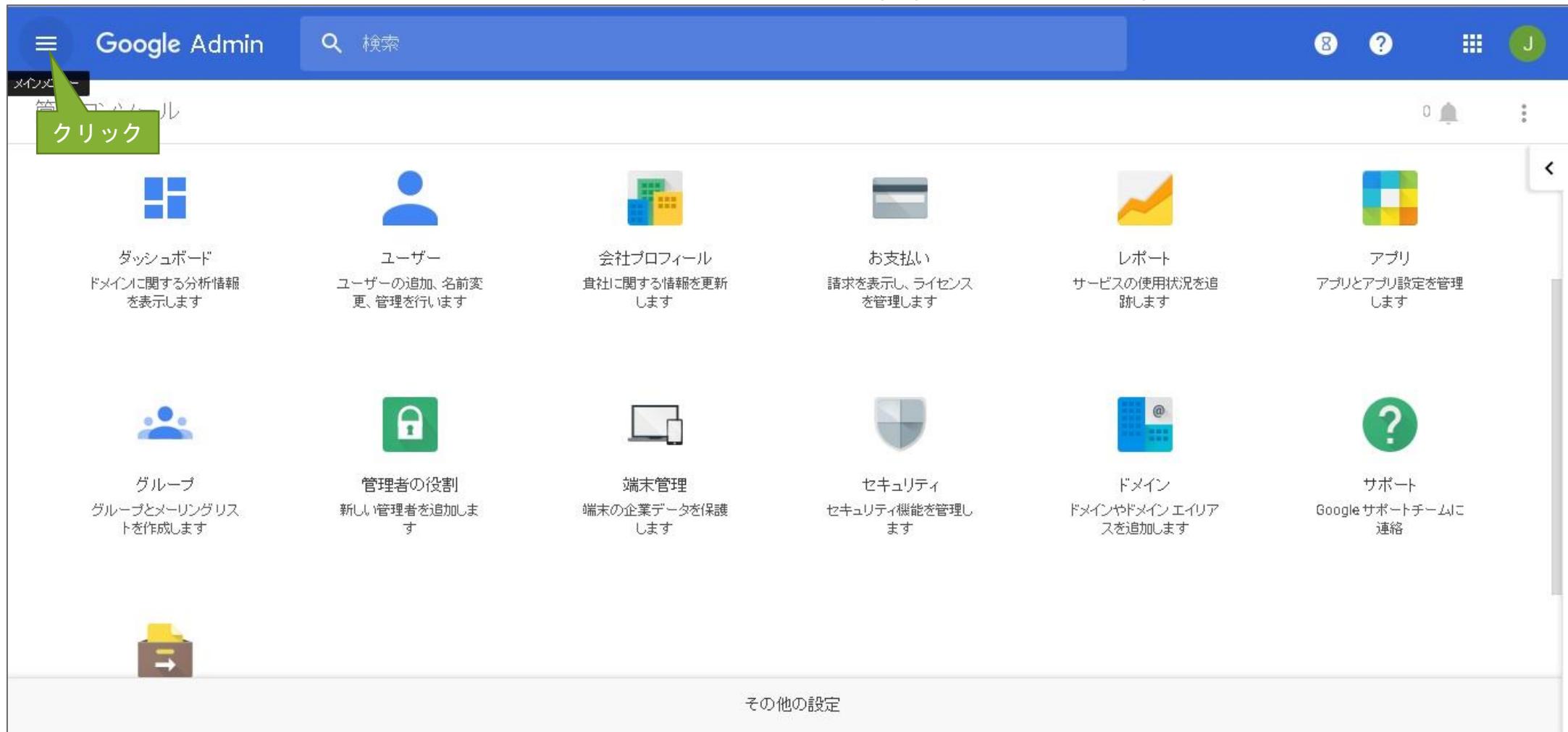
The 'セキュアなトランспорト (TLS)に準拠' section is highlighted with a green callout containing the number ②, pointing to a '保存' (Save) button. A note at the bottom left states: 'これらの変更がすべてのユーザーに反映されるまでに最大 1 時間程度かかることがあります。以前の変更を確認できます: 監査ログ'.



G mail セキュリティ設定の変更 (BCC)

GMAIL セキュリティ設定の変更 (BCC)

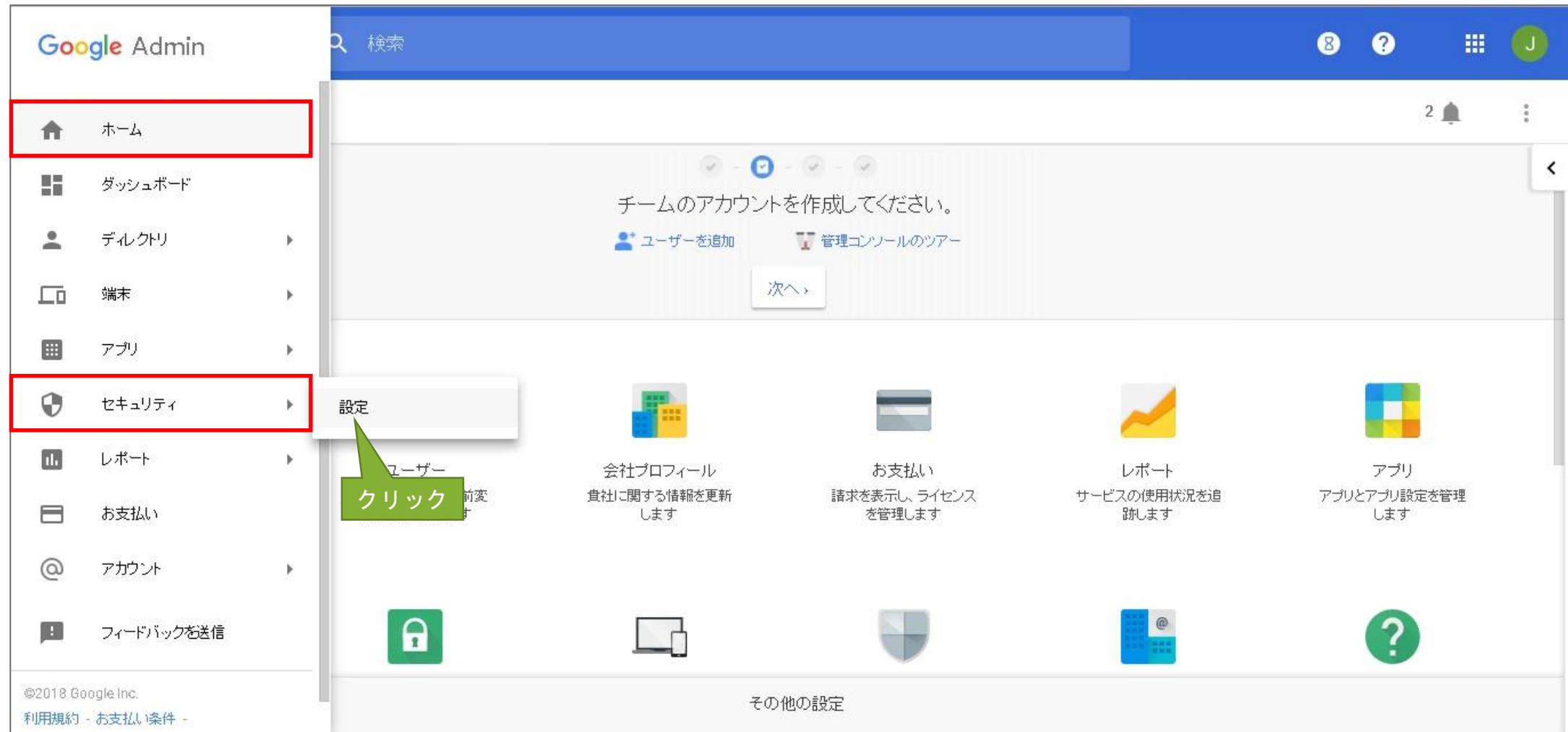
管理者アカウントでログイン後、管理ホーム画面（<https://admin.google.com/AdminHomeGoogle>）へアクセス



The screenshot shows the Google Admin Home page. A green box with the text "クリック" (Click) is placed over the "Main menu" icon in the top-left corner. The page is divided into several sections:

- Top Row:** メインメニュー (Main menu), 検索 (Search), Help (ヘルプ), Help (ヘルプ), Grid icon, User icon (J).
- Second Row:**
 - ダッシュボード**: ドメインに関する分析情報を表示します.
 - ユーザー**: ユーザーの追加、名前変更、管理を行います.
 - 会社プロフィール**: 会社に関する情報を更新します.
 - お支払い**: 請求を表示し、ライセンスを管理します.
 - レポート**: サービスの使用状況を追跡します.
 - アプリ**: アプリとアプリ設定を管理します.
- Third Row:**
 - グループ**: グループとメーリングリストを作成します.
 - 管理者の役割**: 新しい管理者を追加します.
 - 端末管理**: 端末の企業データを保護します.
 - セキュリティ**: セキュリティ機能を管理します.
 - ドメイン**: ドメインやドメインエイリアスを追加します.
 - サポート**: Googleサポートチームに連絡.
- Bottom Row:** その他の設定 (Other settings).

GMAIL セキュリティ設定の変更 (BCC)



The screenshot shows the Google Admin console interface. On the left, a sidebar menu is visible with the following items:

- ホーム (Home) (highlighted with a red box)
- ダッシュボード (Dashboard)
- ディレクトリ (Directory)
- 端末 (Devices)
- アプリ (Apps)
- セキュリティ (Security) (highlighted with a red box)
- レポート (Reports)
- お支払い (Billing)
- アカウント (Accounts)
- フィードバックを送信 (Send Feedback)

Below the sidebar, a sub-menu for 'セキュリティ' (Security) is open, showing the '設定' (Settings) option. A green callout bubble with the text 'クリック' (Click) points to the '設定' button. The main content area displays various management tools:

- 会社プロフィール (Company Profile): Update company information.
- お支払い (Billing): View invoices and manage licenses.
- レポート (Reports): Track service usage.
- アプリ (Apps): Manage app settings.
- その他 (Other): Includes a lock icon, a monitor icon, a shield icon, and a question mark icon.

At the bottom of the sidebar, there are copyright and legal links: ©2018 Google Inc., 利用規約 - お支払い条件 -.

GMAIL セキュリティ設定の変更 (BCC)



セキュリティ
jatp-test.ddo.jp

クリック

基本設定

2SV を適用して安全性の低いアプリを管理します。

パスワードの監視

ユーザーによるパスワードの安全度を監視します。

APIリファレンス

API を有効化し、独自に作成したアプリケーションやサードパーティ製アプリケーションを介して、プロビジョニング、レポート、移行をプログラムで管理します。

シングルサインオン(SSO)の設定

ウェブベースのアプリケーション(Gmail やカレンダーなど)のユーザー認証を設定します。

GMAIL セキュリティ設定の変更 (BCC)

▲ 基本設定

パスワードの再設定

パスワードの安全度

最小の長さ
8

最大の長さ
100

パスワードの長さは、8~100文字にする必要があります。

デフォルトでは、ユーザーがパスワードを忘れた場合に自動システムを使用して再設定できるのは管理者のみです。この設定を変更すると、他のユーザーもパスワードを再設定できるようになります。

管理者以外によるユーザーのパスワードの再設定を有効/無効にする

2段階認証プロセス

2段階認証プロセスを導入すると、G Suite アカウントのセキュリティをさらに強化することができます。ユーザーはログイン時に、ユーザー名やパスワードの他に、Google から受け取った確認コードの入力を求められます。?

ユーザーが 2段階認証プロセスを有効にできるようにする

2段階認証プロセスを適用するには、詳細設定にアクセスしてください

安全性の低いアプリ

安全性の低いログイン技術、アカウントの脆弱性が高まる可能性があります。このようなアプリについてはアクセスをすすめします。アプリのアクセスを許可する場合は、そのリスクをご理解ください。おつづきお願いします。?

安全性の低いアプリの設定に移動

GMAIL セキュリティ設定の変更 (BCC)



Google Admin

検索

セキュリティ > 高度なセキュリティ設定

組織 設定: jatp-test.ddo.jp、管理者グループが選択されていません。

jatp-test.ddo.jp

安全性の低いアプリ
ローカルに適用しました

①クリック

安全性の低いアプリへのアクセスをすべてのユーザーで無効にする(推奨)
 安全性の低いアプリの管理をユーザーに許可する
 安全性の低いアプリへのアクセス有効化をすべてのユーザーに適用する(非推奨)

安全性の低いログイン技術を使用しているアプリでは、アカウントの脆弱性が高まる可能性があります。このようなアプリについてはアクセスを許可しないことをおすすめします。アプリのアクセスを許可する場合は、そうしたリスクをご理解いただいた上で行うようお願いします。②

グループのフィルタ ② 選択

管理者グループが選択されて

① これらの変更がすべてのユーザーに反映されるまでに最大 24 時間程度かかることがあります。
以前の変更を確認できます: [監査ログ](#)

②クリック

破棄 保存

GMAIL セキュリティ設定の変更 (BCC)

つづいてJournaling対象の各アカウントごとの設定となります。
Journaling対象の各アカウントでログインし、アカウント画面へアクセスします。



アカウント情報

ようこそ、ユーザ2ユーザ2さん

アカウントの管理、保護、安全対策を 1 か所で行えます。

[アカウント情報] では、設定やツールにアクセスしてデータの安全保護対策やプライバシーの保護を行えるほか、ご自分の情報を Google のツールやサービスの向上に役立てる方法を選択できます。

| | | |
|--|---|--|
|  ログインとセキュリティ > |  個人情報とプライバシー > |  アカウント設定 > |
| パスワードや Google アカウントへのアクセスを管理できます。 Googleへのログイン 端末のアクティビティとセキュリティイベント アカウントにアクセスできるアプリ | 公開設定の管理や、Googleがユーザーの利便性のカスタマイズに使用するデータの管理を行えます。 個人情報 連絡先 Googleでのアクティビティの管理 広告認定 | お支払い方法、言語、ストレージ オプションなど、アカウント設定を調整できます。 お支払い 言語と入力ツール ユーザー補助 Google ドライブ ストレージ |

クリック

GMAIL セキュリティ設定の変更 (BCC)



ログインとセキュリティ

アカウントにアクセスできるアプリ

アカウントへのアクセスを許可したアプリやサービスを把握しておき、使用または信頼しなくなったアプリやサービスの許可は取り消すようにしましょう。

アカウントにアクセスできるアプリ

これらのアプリを今後も使用し、信頼して情報にアクセスさせるかどうかを確認しましょう。

アプリを管理

保存したパスワード

同期しているパスワードはありません。

ヘルプ

安全性の低いアプリの許可: 有効

一部のアプリや端末では安全性の低いログイン技術が使用されており、アカウントの脆弱性が高まる可能性があります。こうしたアプリについてはアクセスを無効にすることをおすすめします。有効にする場合は、そのようなリスクをご理解の上でお使いください。

有効にする
(デフォルトでは無効)

GMAIL セキュリティ設定の変更 (BCC)

GmailではPOP3/IMAPの設定がデフォルトでは無効になっているため、設定の変更が必要となります。
Journaling対象の各アカウントでログインし、Gmail(<https://mail.google.com/mail/>)へアクセスします。



Google 検索

メール ▾ □ C その他 ▾

作成

新着メールはありません。

受信トレイ

スター付き

送信済みメール 0 GB (0%) / 30 GB を使用中 管理

下書き

その他のラベル ▾

JATP +

最近のチャットはありません
新しいチャットを開設しませんか

①クリック

表示モード:
✓ タッチ対応
標準
小
最小
受信トレイを設定
②クリック
設定
ドメインの管理
テーマ
アドオンを取得
フィードバックを送信
ヘルプ
Gmail の設定 (10%)

GMAIL セキュリティ設定の変更 (BCC)

Google メール 設定 作成 全般 ラベル 受信トレイ アカウント フィルタとブロック中のアドレス メール転送と POP/IMAP アドオン チャット Labs オフライン テーマ

IMAP アクセス: (IMAP を使用して他のクライアントから JATP Test メール にアクセスします) 詳細

ステータス: IMAP 無効 IMAP を有効にする IMAP を無効にする

①クリック

IMAP のメールを削除するようマークを付けた場合: 自動消去をオン - 直ちにサーバーを更新する(デフォルト) 自動消去をオフ - クライアント側でサーバーを更新するのを待機する

②クリック

最後に表示された IMAP フォルダからメールを削除/消去するようマークを付けた場合: メールをアーカイブする(デフォルト) メッセージをゴミ箱に移動 メールを今すぐ完全に削除する

フォルダ サイズの制限 IMAP フォルダのメールの数を制限しない(デフォルト) IMAP フォルダ内のメッセージ数をこの件数に制限する 1,000

メール クライアントの設定(例: Outlook, Thunderbird, iPhone) 設定手順

③クリック

変更を保存 キャンセル プログラム ポリシー Powered by Google 前回のアカウント アクティビティ: 0 分前 他の 1 か所で開かれています アカウント アクティビティの詳細

0 GB(0%) / 30 GB を使用中 管理

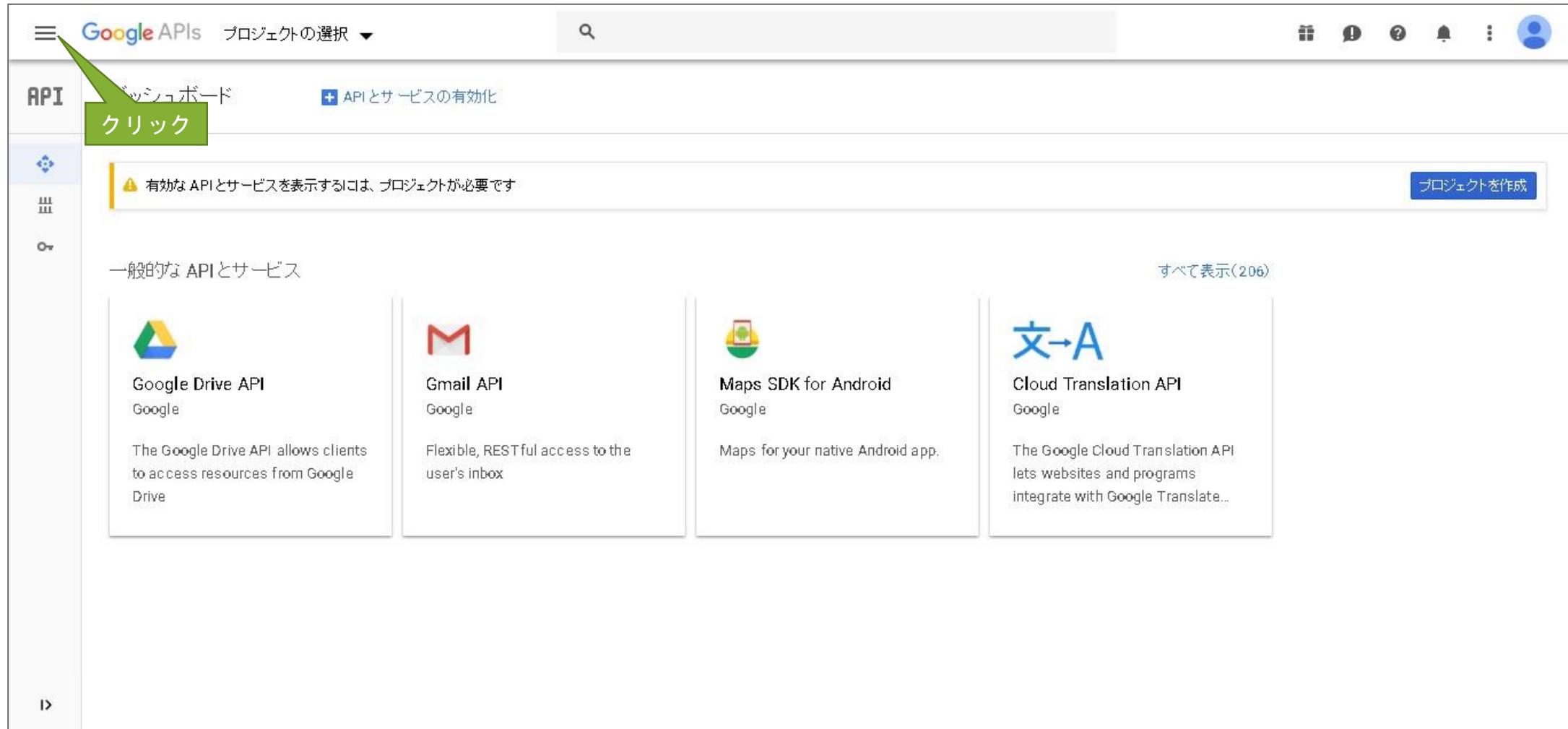
最近のチャットはありません 新しいチャットを開始しませんか



G Suite Mitigation設定手順 (BCC, MTA Receiver)

G SUITE MITIGATION設定手順 (BCC,MTA RECEIVER)

Google APIs Console (<https://console.developers.google.com/>) へアクセスして**管理者アカウント**でログインする



Google APIs プロジェクトの選択 ▼

API & Services

API

プロジェクトの選択

検索

管理者アカウント

API & Services

プロジェクトを作成

有効な API とサービスを表示するには、プロジェクトが必要です

一般的な API とサービス

すべて表示(206)

Google Drive API

Google

The Google Drive API allows clients to access resources from Google Drive

Gmail API

Google

Flexible, RESTful access to the user's inbox

Maps SDK for Android

Google

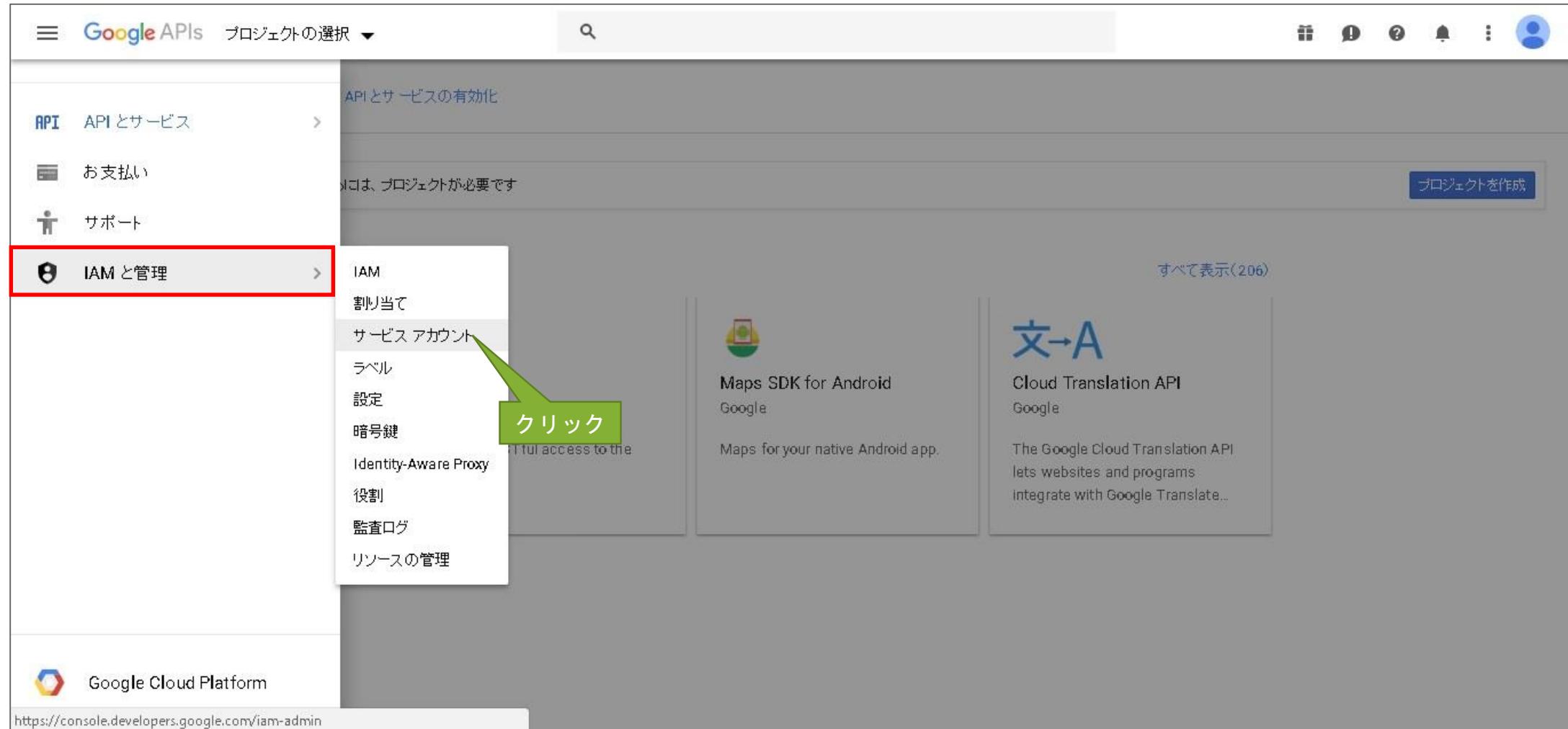
Maps for your native Android app.

Cloud Translation API

Google

The Google Cloud Translation API lets websites and programs integrate with Google Translate...

G SUITE MITIGATION設定手順 (BCC,MTA RECEIVER)



Google APIs プロジェクトの選択 ▼

API とサービス

お支払い

サポート

IAM & 管理

IAM

割り当て

サービス アカウント

ラベル

設定

暗号鍵

Identity-Aware Proxy

役割

監査ログ

リソースの管理

Maps SDK for Android

Maps for your native Android app.

Cloud Translation API

The Google Cloud Translation API lets websites and programs integrate with Google Translate...

すべて表示(206)

Google Cloud Platform

<https://console.developers.google.com/iam-admin>

クリック

ナビゲーションメニュー

APIとサービス

お支払い

サポート

IAM & 管理

IAM

割り当て

サービス アカウント

ラベル

設定

暗号鍵

Identity-Aware Proxy

役割

監査ログ

リソースの管理

Maps SDK for Android

Maps for your native Android app.

Cloud Translation API

The Google Cloud Translation API lets websites and programs integrate with Google Translate...

すべて表示(206)

Google Cloud Platform

<https://console.developers.google.com/iam-admin>

ナビゲーションメニュー

APIとサービス

お支払い

サポート

IAM & 管理

IAM

割り当て

サービス アカウント

ラベル

設定

暗号鍵

Identity-Aware Proxy

役割

監査ログ

リソースの管理

Maps SDK for Android

Maps for your native Android app.

Cloud Translation API

The Google Cloud Translation API lets websites and programs integrate with Google Translate...

すべて表示(206)

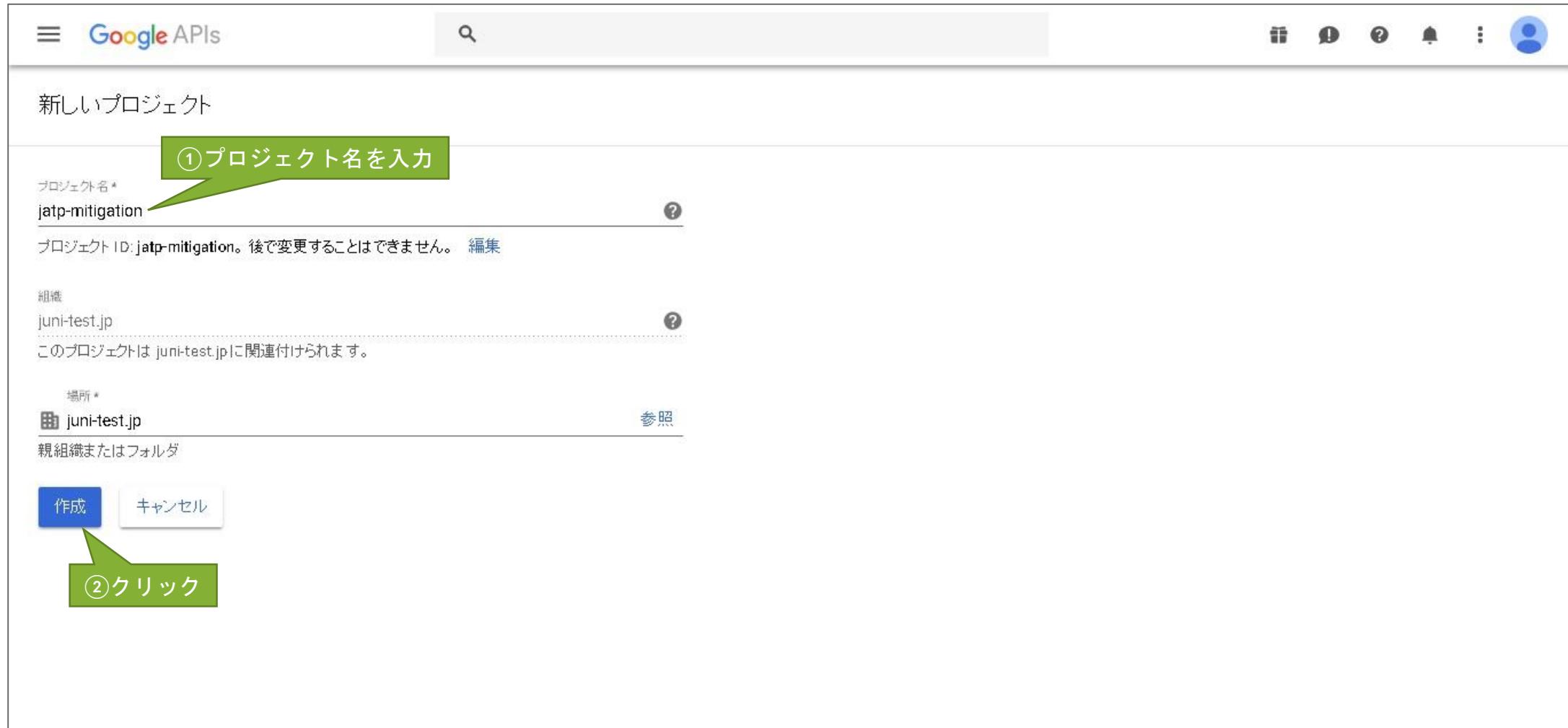
Google Cloud Platform

<https://console.developers.google.com/iam-admin>

G SUITE MITIGATION設定手順 (BCC,MTA RECEIVER)



G SUITE MITIGATION設定手順 (BCC,MTA RECEIVER)



G SUITE MITIGATION設定手順 (BCC,MTA RECEIVER)



Google APIs **jatp-mitigation** 1 ⋮

IAMと管理 IAM ID 割り当て サービス アカウント + サービス アカウントを作成 削除 情報パネルを表示

プロジェクト「jatp-mitigation」のサービスアカウント クリック

サービスアカウントは Google Cloud サービス ID(Compute Engine VM、App Engine アプリ、Google 以外で実行中のシステムで実行されているコードなど)を表します。[詳細](#)

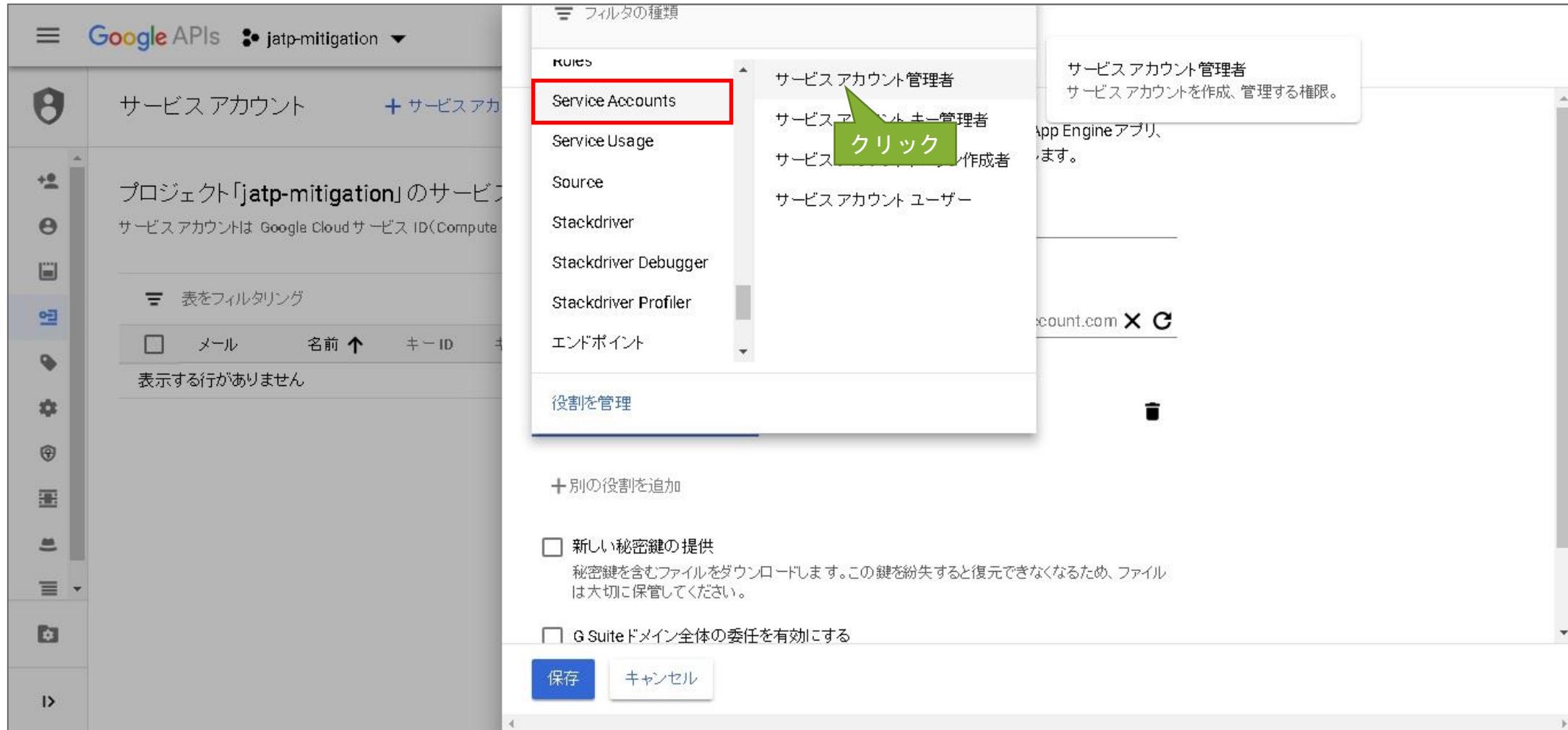
表をフィルタリング

| <input type="checkbox"/> | メール | 名前 ↑ | キー ID | キーを削除 | キーの作成日 | 操作 |
|--------------------------|-----|------|-------|-------|--------|----|
| 表示する行がありません | | | | | | |

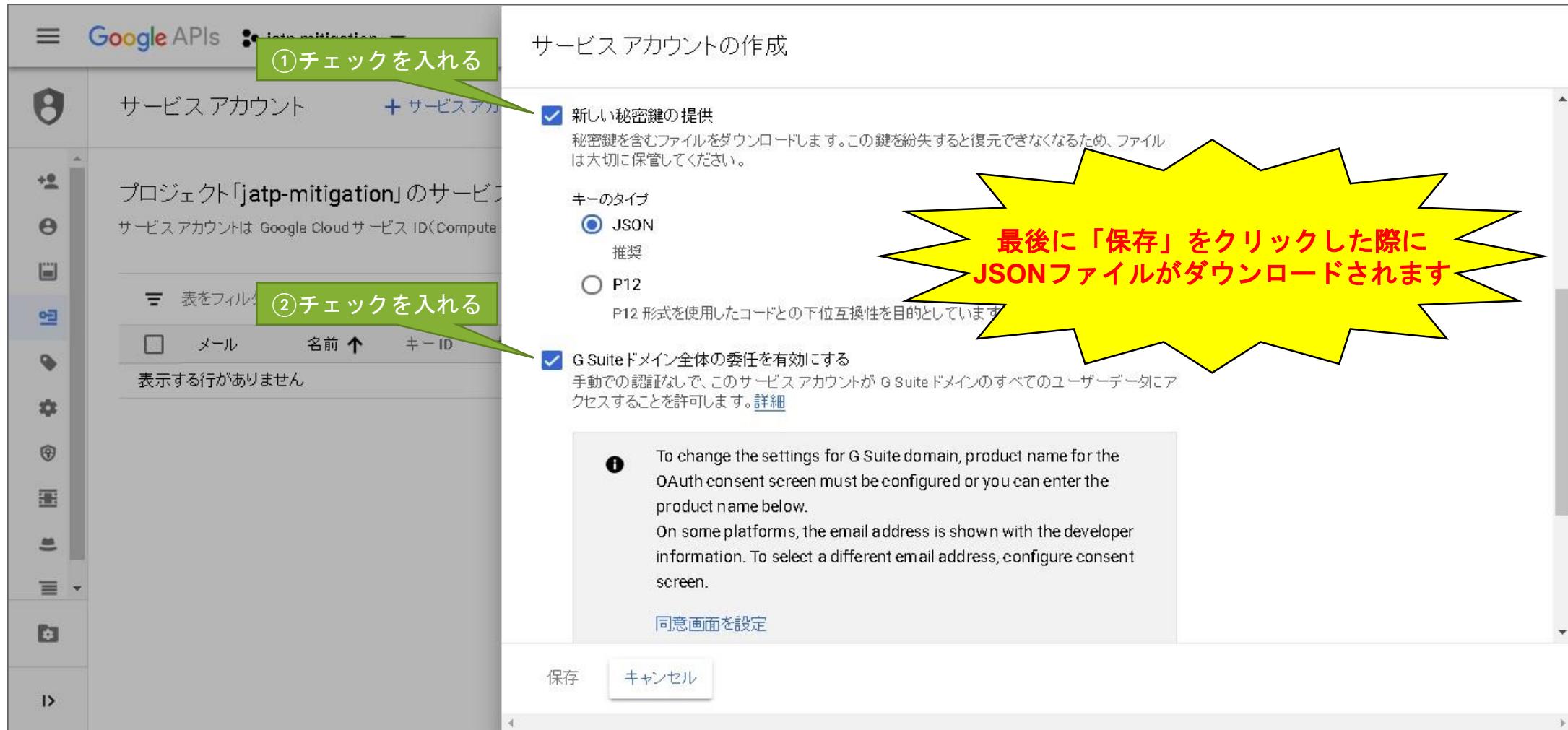
G SUITE MITIGATION設定手順 (BCC,MTA RECEIVER)



G SUITE MITIGATION設定手順 (BCC,MTA RECEIVER)



G SUITE MITIGATION設定手順 (BCC,MTA RECEIVER)



サービスアカウントの作成

新しい秘密鍵の提供
秘密鍵を含むファイルをダウンロードします。この鍵を紛失すると復元できなくなるため、ファイルは大切に保管してください。

キーのタイプ

JSON
推奨

P12
P12 形式を使用したコードとの下位互換性を目的としています

G Suite ドメイン全体の委任を有効にする
手動での認証なしで、このサービスアカウントが G Suite ドメインのすべてのユーザーにアクセスすることを許可します。[詳細](#)

①チェックを入れる

②チェックを入れる

最後に「保存」をクリックした際に
JSONファイルがダウンロードされます

To change the settings for G Suite domain, product name for the OAuth consent screen must be configured or you can enter the product name below.
On some platforms, the email address is shown with the developer information. To select a different email address, configure consent screen.

同意画面を設定

保存 キャンセル

G SUITE MITIGATION設定手順 (BCC,MTA RECEIVER)



サービス アカウントの作成

G Suite ドメイン全体の委任を有効にする
手動での認証なしで、このサービスアカウントが G Suite ドメインのすべてのユーザーデータにアクセスすることを許可します。[詳細](#)

To change the settings for G Suite domain, product name for the OAuth consent screen must be configured or you can enter the product name below.
On some platforms, the email address is shown with the developer information. To select a different email address, configure consent screen.

同意画面を設定

同意画面のプロダクト名
JATP

Assign product name.

Email address
gyj600bv4y@juni-test.jp

Shown on consent screen for user support.

①プロダクト名を入力

②クリック

保存 キャンセル

G SUITE MITIGATION設定手順 (BCC,MTA RECEIVER)



Google APIs jatp-mitigation

サービスアカウント + サービスアカウントを作成 削除 情報パネルを表示

プロジェクト「jatp-mitigation」のサービスアカウント
サービスアカウントは Google Cloud サービス ID(Compute Engine VM、App Engine アプリ、Google 以外で実行中のシステムで実行されているコードなど)を表します。[詳細](#)

表をフィルタリング

| 名前 | キー ID | キーを削除 | キーの作成日 | Domain wide delegation | 操作 |
|---|-----------------|-------|--------|------------------------|----|
| メール | | | | | |
| jatp-mitigation@jatp-mitigation.iam.gserviceaccount.com | JATP-Mitigation | | | 有効 クライアント ID を表示 | ⋮ |

G SUITE MITIGATION設定手順 (BCC,MTA RECEIVER)

①クライアントIDをtextファイルなどにコピーしておく

②クリック

サービスアカウント クライアント のクライアント ID 削除

サービスアカウントの管理

クライアント ID: 109021442147403274090

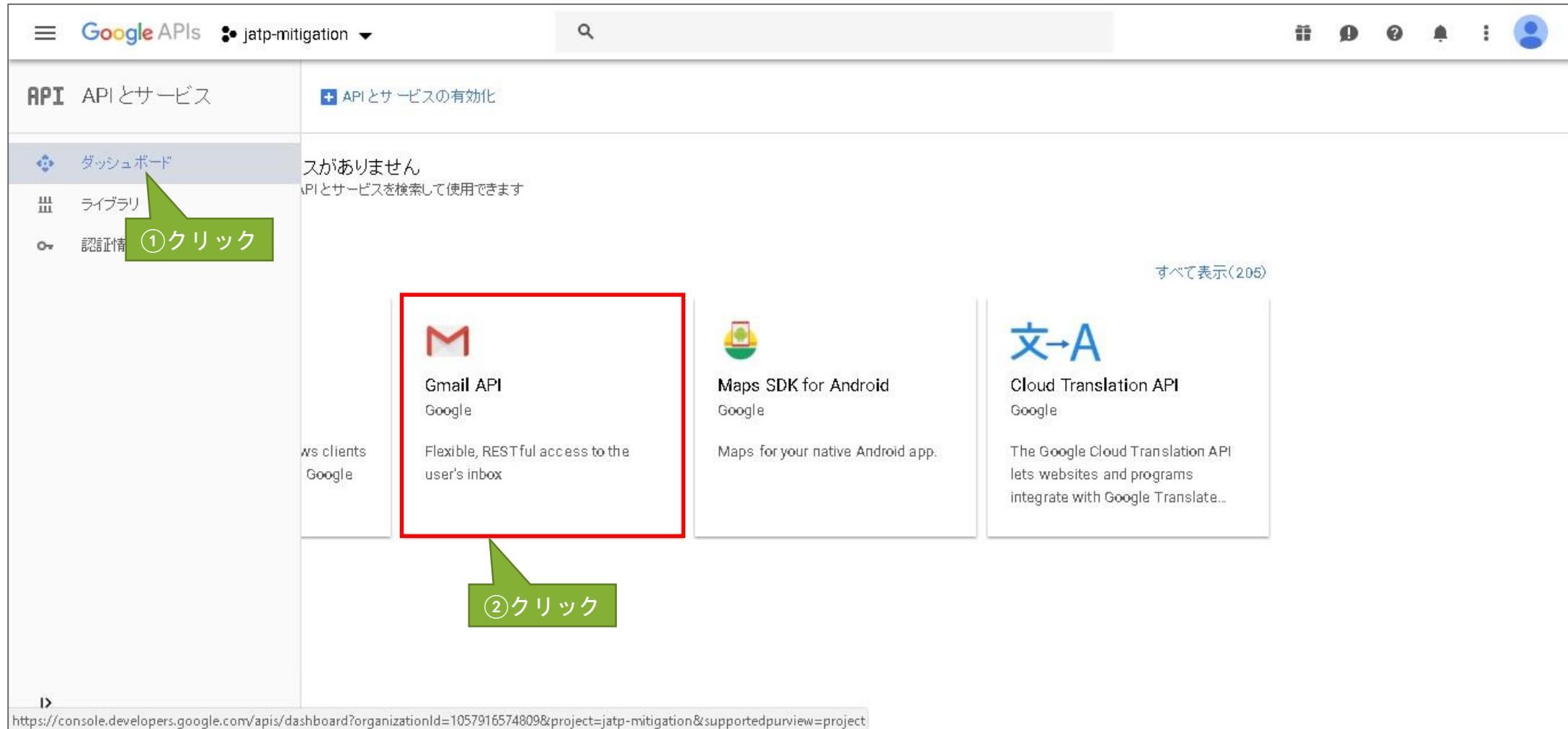
サービスアカウント: JATP-Mitigation
jatp-mitigation@jatp-mitigation.iam.gserviceaccount.com

作成日: 2018/07/20 14:37:47

名前: jatp-mitigation のクライアント

保存 キャンセル

G SUITE MITIGATION設定手順 (BCC,MTA RECEIVER)



The screenshot shows the Google Cloud Platform API library interface. The left sidebar is titled 'API APIとサービス' and contains three items: 'ダッシュボード' (selected, highlighted with a green arrow), 'ライブラリ' (Library), and '認証情報' (Authentication). The main area is titled '+ APIとサービスの有効化' (Enable API and service) and displays a list of APIs. The 'Gmail API' is highlighted with a red box and a green arrow pointing to it. Other APIs listed are 'Maps SDK for Android' and 'Cloud Translation API'.

API APIとサービス

+ APIとサービスの有効化

ダッシュボード

ライブラリ

認証情報 ①クリック

Gmail API

Maps SDK for Android

Cloud Translation API

すべて表示(205)

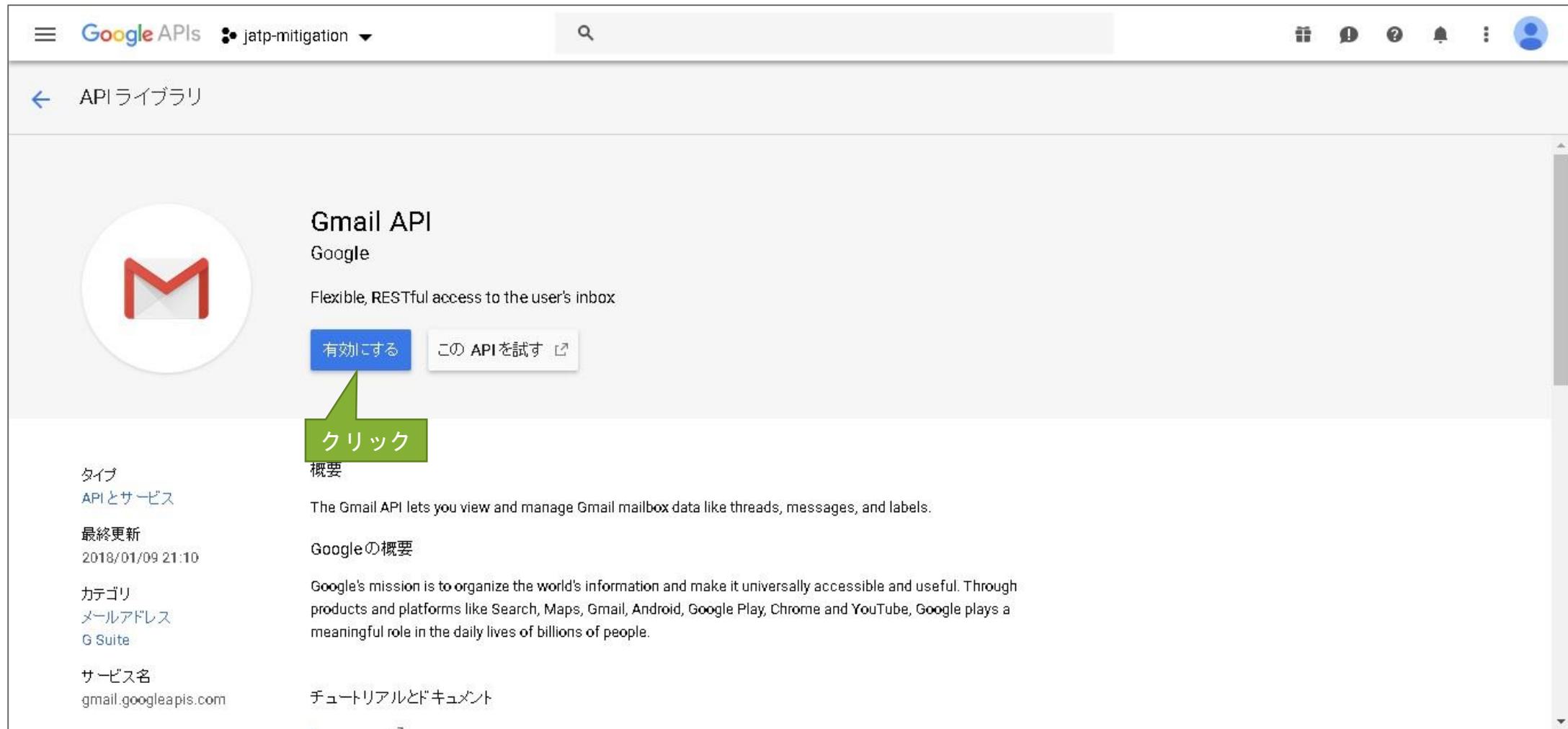
Flexible, RESTful access to the user's inbox

Maps for your native Android app.

The Google Cloud Translation API lets websites and programs integrate with Google Translate...

https://console.developers.google.com/apis/dashboard?organizationId=1057916574809&project=jatp-mitigation&supportedpurview=project

G SUITE MITIGATION設定手順 (BCC,MTA RECEIVER)



Google APIs jatp-mitigation ≡ ? ! ! ! ... 👤

← API ライブラリ

Gmail API
Google

Flexible, RESTful access to the user's inbox

有効にする この API を試す

クリック

概要

タイプ API とサービス

最終更新 2018/01/09 21:10

カテゴリ メールアドレス

G Suite

サービス名 gmail.googleapis.com

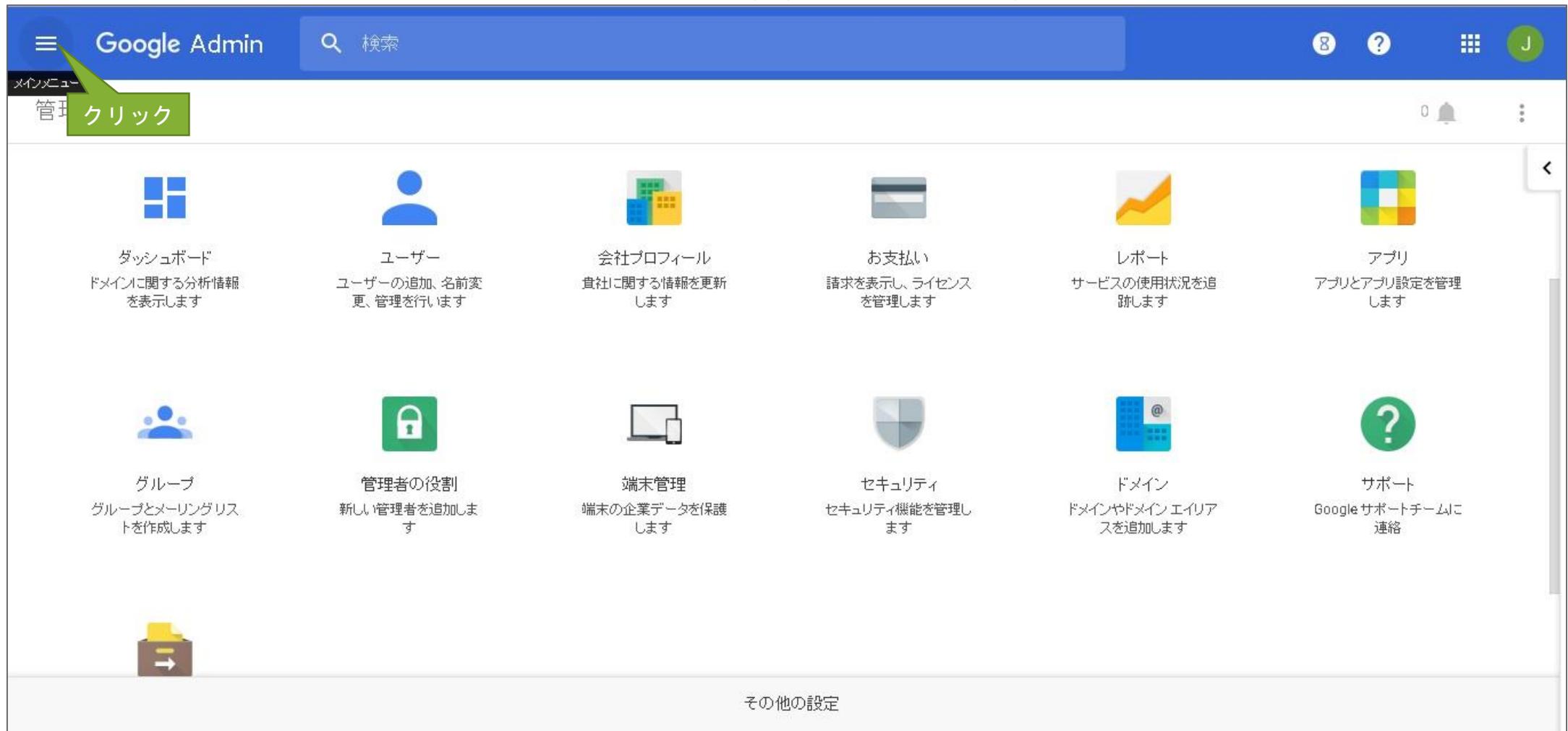
The Gmail API lets you view and manage Gmail mailbox data like threads, messages, and labels.

Google's mission is to organize the world's information and make it universally accessible and useful. Through products and platforms like Search, Maps, Gmail, Android, Google Play, Chrome and YouTube, Google plays a meaningful role in the daily lives of billions of people.

チュートリアルとドキュメント

G SUITE MITIGATION設定手順 (BCC,MTA RECEIVER)

G Suiteの管理ホーム画面 (<https://admin.google.com/AdminHomeGoogle>) ヘアクセスする

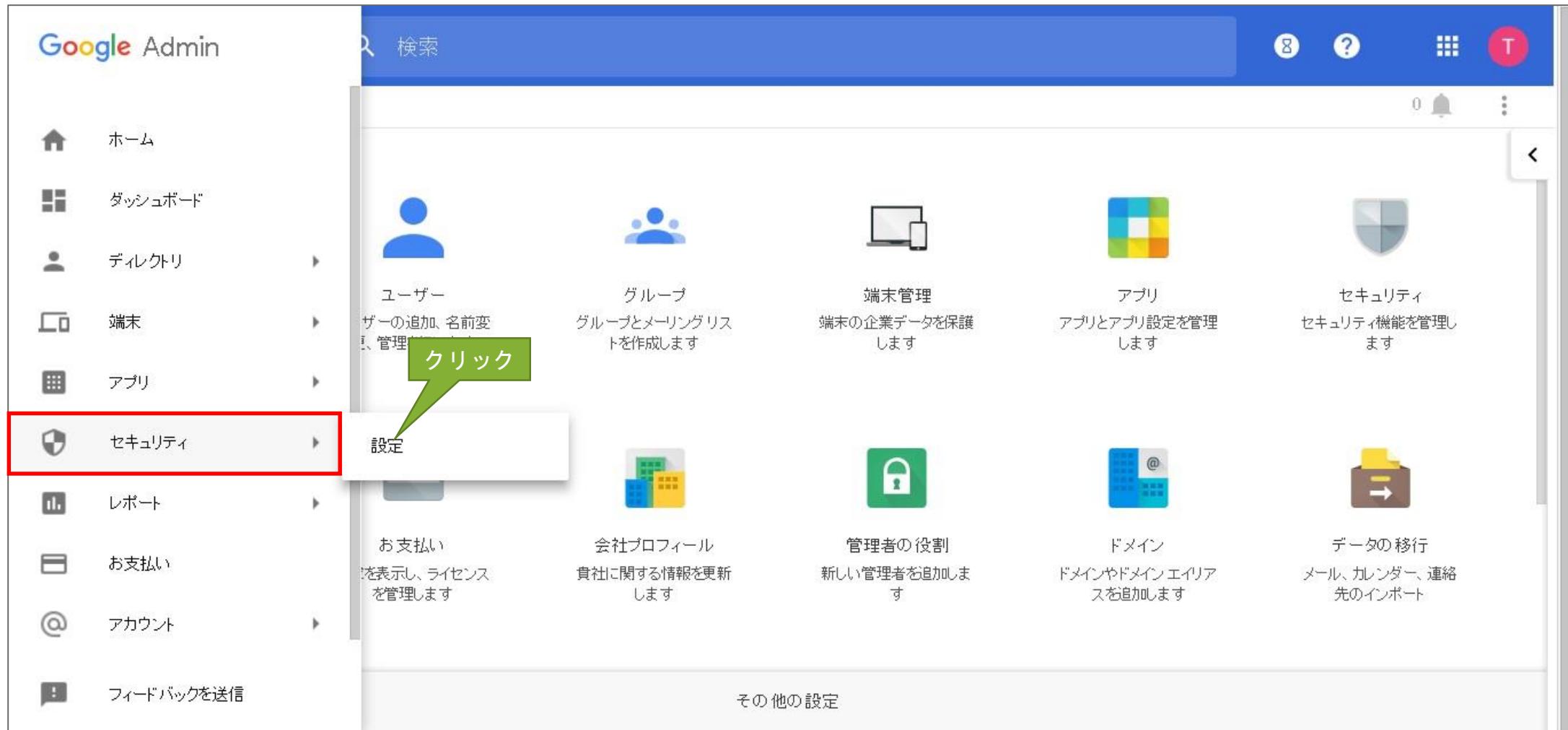


The screenshot shows the Google Admin Home page. A green box highlights the '管理' (Management) link in the top-left corner of the main menu bar. The page is filled with various management icons and their descriptions:

- ダッシュボード**: ドメインに関する分析情報を表示します
- ユーザー**: ユーザーの追加、名前変更、管理を行います
- 会社プロフィール**: 会社に関する情報を更新します
- お支払い**: 請求を表示し、ライセンスを管理します
- レポート**: サービスの使用状況を追跡します
- アプリ**: アプリとアプリ設定を管理します
- グループ**: グループとメーリングリストを作成します
- 管理者の役割**: 新しい管理者を追加します
- 端末管理**: 端末の企業データを保護します
- セキュリティ**: セキュリティ機能を管理します
- ドメイン**: ドメインやドメインエイリアスを追加します
- サポート**: Googleサポートチームに連絡

At the bottom center, there is a link labeled 'その他の設定' (Other Settings).

G SUITE MITIGATION設定手順 (BCC,MTA RECEIVER)



Google Admin

検索

ホーム

ダッシュボード

ディレクトリ

端末

アプリ

セキュリティ

レポート

お支払い

アカウント

フィードバックを送信

クリック

設定

ユーザー

グループ

端末管理

アプリ

セキュリティ

お支払い

会社プロフィール

管理者の役割

ドメイン

データの移行

その他の設定

その他の設定

G SUITE MITIGATION設定手順 (BCC,MTA RECEIVER)



G SUITE MITIGATION設定手順 (BCC,MTA RECEIVER)



Google Admin 検索

セキュリティ

API クライアント アクセスを管理する

開発者が Google に登録したウェブアプリケーションや他の API クライアントで、カレンダーのような Google サービスのデータにアクセスできます。登録されたクライアントが個別の許可やパスワード入力なしにユーザー データにアクセスすることを許可できます。[詳細](#)

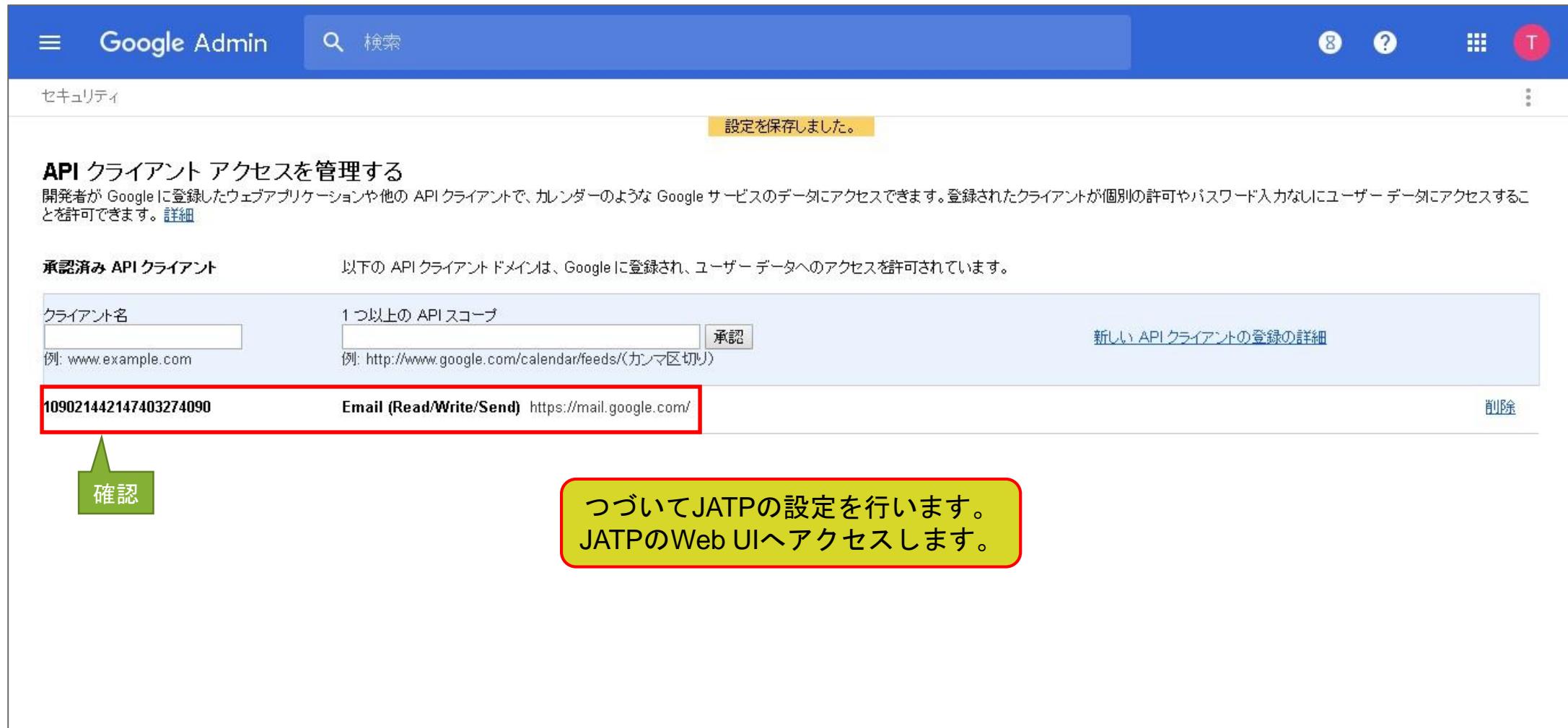
承認済み API クライアント

以下の API クライアントドメインは、Google に登録され、ユーザー データへのアクセスを許可されています。

| | | |
|--|---|--------------------------------------|
| クライアント名 109021442147403274090 例: www.example.com | 1 つ以上の API スコープ <input type="text" value="https://mail.google.com/"/> 承認 例: http://www.google.com/calendar/feeds/(カンマ区切り) | 新しい API クライアントの登録の詳細 |
|--|---|--------------------------------------|

①コピーしたクライアントIDを入力
②下記アドレスを入力
https://mail.google.com/
③クリック

G SUITE MITIGATION設定手順 (BCC,MTA RECEIVER)



Google Admin 検索

セキュリティ 設定を保存しました。

API クライアント アクセスを管理する

開発者が Google に登録したウェブアプリケーションや他の API クライアントで、カレンダーのような Google サービスのデータにアクセスできます。登録されたクライアントが個別の許可やパスワード入力なしにユーザー データにアクセスするごとを許可できます。[詳細](#)

承認済み API クライアント

以下の API クライアントドメインは、Google に登録され、ユーザー データへのアクセスを許可されています。

| クライアント名 | 1 つ以上の API スコープ | 承認 | 新しい API クライアントの登録の詳細 |
|-----------------------|--|----|----------------------|
| 例: www.example.com | 例: http://www.google.com/calendar/feeds/(カンマ区切り) | | |
| 109021442147403274090 | Email (Read/Write/Send) https://mail.google.com/ | | 削除 |

確認

つづいてJATPの設定を行います。
JATPのWeb UIへアクセスします。

G SUITE MITIGATION設定手順 (BCC,MTA RECEIVER)

ADVANCED THREAT PREVENTION APPLIANCE

Refresh Data System Health J-ATP Admin

Hostname: Core1

① クリック

② クリック

③ クリック

System Profiles

④ Password Reset

⑤ Roles

⑥ Zones

⑦ Users

⑧ SAML Settings

⑨ RADIUS Settings

⑩ System Settings

⑪ Certificate Management

⑫ GSS Settings

⑬ Web Collectors

⑭ SRX Settings

⑮ Email Collectors

⑯ Secondary Cores

⑰ System Defaults

⑱ Server fully-qualified domain name: Core1.eng.Core1.com

⑲ IVP format: MSI (radio button selected) Self-extracting Zip file [Download MSI](#)

⑳ Software Update enabled:

⑳ Content Update enabled:

⑳ Enable JATP support account:

⑳ Restart services now: [restart](#)

⑳ Reboot appliance now: [reboot](#)

⑳ Clear event database: [clear](#)

⑳ Submit

⑳ Proxy Settings

⑳ Proxy Type: No Proxy (radio button selected) Manual Proxy

⑳ Submit

⑳ Auto Mitigation Settings

⑳ Enable for Web:

⑳ Enable for Email:

Powered by Juniper Version 5.0.2.20 Content Version 5.0.2.14

Support | Resources | Contact Us

G SUITE MITIGATION設定手順 (BCC,MTA RECEIVER)

① チェックを入れる

② 自動でMitigationする脅威度レベルの選択
・ Moderate (MaxかHighのみ)
・ Aggressive (全てのレベル)

③ クリック

ADVANCED THREAT PREVENTION APPLIANCE

Dashboard Incidents File Uploads Mitigation Reports Custom Rules Config

Enable J-ATP support account:

Restart services now:

Reboot appliance now:

Clear event database:

Proxy Settings

Proxy Type: No Proxy Manual Proxy

Auto Mitigation Settings

Enable for Web:

Enable for Email:

Mitigation Aggressiveness Level: Moderate (Only Max and High Threat confidence levels) Aggressive (All Threat Confidence Levels)

Display Settings

Maximum threats: 500

Default display period: Last Week

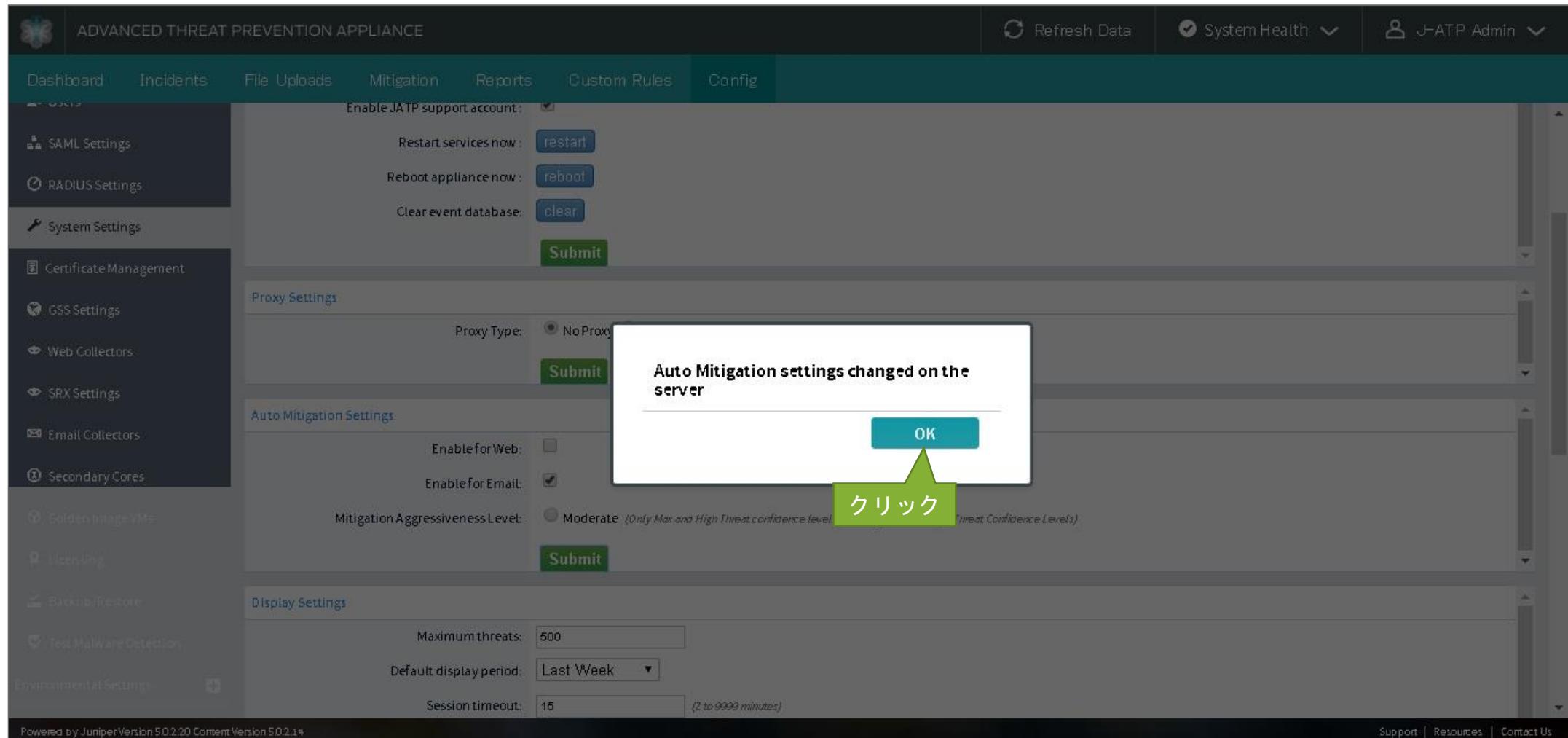
Session timeout: 15 (2 to 9999 minutes)

Refresh Data System Health J-ATP Admin

Powered by Juniper Version 5.0.2.20 Content Version 5.0.2.14

Support | Resources | Contact Us

G SUITE MITIGATION設定手順 (BCC, MTA RECEIVER)



ADVANCED THREAT PREVENTION APPLIANCE

Dashboard Incidents File Uploads Mitigation Reports Custom Rules Config

Enable J-ATP support account:

Restart services now:

Reboot appliance now:

Clear event database:

Submit

Proxy Settings

Proxy Type: No Proxy []

Submit

Auto Mitigation Settings

Enable for Web:

Enable for Email:

Mitigation Aggressiveness Level: Moderate (Only Max and High Threat confidence level) [] (Low Threat Confidence Levels)

Submit

Display Settings

Maximum threats:

Default display period:

Session timeout: (2 to 9999 minutes)

Auto Mitigation settings changed on the server

OK

クリック

Powered by Juniper Version 5.0.2.20 Content Version 5.0.2.14

Support | Resources | Contact Us

G SUITE MITIGATION設定手順 (BCC,MTA RECEIVER)

The screenshot shows the Juniper Advanced Threat Prevention Appliance interface. The top navigation bar includes 'ADVANCED THREAT PREVENTION APPLIANCE', 'Refresh Data', 'System Health', and 'J-ATP Admin'. The main menu has tabs for 'Dashboard', 'Incidents', 'File Uploads', 'Mitigation', 'Reports', 'Custom Rules', and 'Config'. The 'Config' tab is selected. On the left, a sidebar lists various settings: 'Notifications', 'System Profiles', 'Environmental Settings' (with a red box around 'Email Mitigation Settings'), 'Email Mitigation Settings' (highlighted with a green box and labeled ①), 'Firewall Mitigation Settings' (highlighted with a green box and labeled ②), 'Asset Value', 'Anti-Virus Configuration', 'Endpoint Integration Settings', 'BlueCoat Configuration', 'Whitelist Rules', 'YARA Rule Upload', 'SNORT Rule Upload', 'Identity Configuration', 'Splunk Configuration', and 'External Event Collectors'. The main content area shows 'Current Email Mitigations Configured' with a table header 'Description'. A large green box labeled ③ points to a 'Add New Mitigation' button. The bottom of the screen shows 'Powered by Juniper Version 5.0.2.20 Content Version 5.0.2.14' and links for 'Support | Resources | Contact Us'.

G SUITE MITIGATION設定手順 (BCC,MTA RECEIVER)

①クリック

②隔離フォルダ名の入力

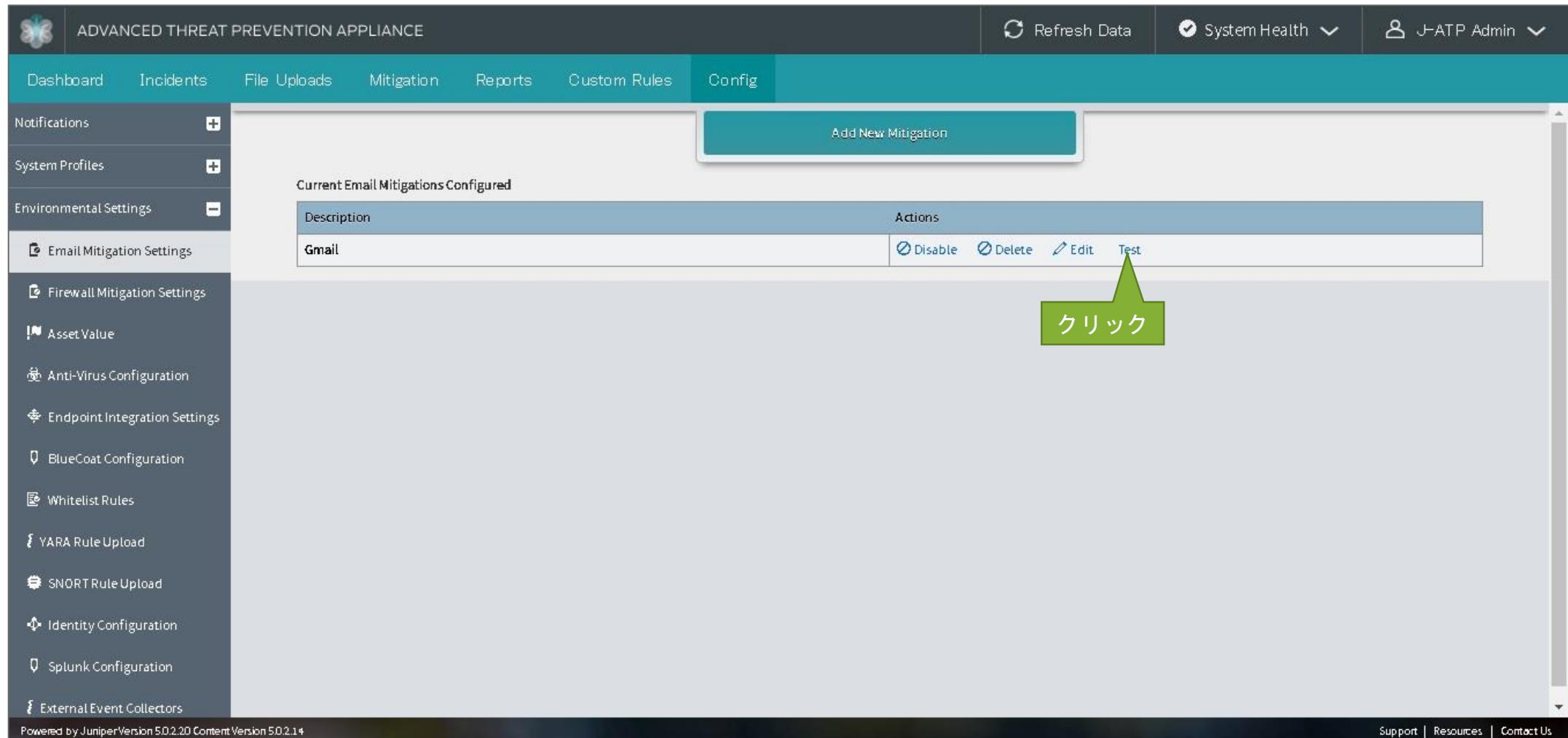
③接続テスト用メールアドレスの入力

④ダウンロードした秘密鍵（JSONファイル）を
エディタなどで開き内容をコピー&ペースト

⑤保護対象のドメインを入力

⑥クリック

G SUITE MITIGATION設定手順 (BCC,MTA RECEIVER)



ADVANCED THREAT PREVENTION APPLIANCE

Refresh Data System Health J-ATP Admin

Dashboard Incidents File Uploads Mitigation Reports Custom Rules Config

Notifications +

System Profiles +

Environmental Settings -

Email Mitigation Settings

Firewall Mitigation Settings

Asset Value

Anti-Virus Configuration

Endpoint Integration Settings

BlueCoat Configuration

Whitelist Rules

YARA Rule Upload

SNORT Rule Upload

Identity Configuration

Splunk Configuration

External Event Collectors

Add New Mitigation

Current Email Mitigations Configured

| Description | Actions |
|-------------|--------------------------|
| Gmail | Disable Delete Edit Test |

クリック

Powered by Juniper Version 5.0.2.20 Content Version 5.0.2.14

Support | Resources | Contact Us

G SUITE MITIGATION設定手順 (BCC,MTA RECEIVER)

The screenshot shows the Juniper Advanced Threat Prevention Appliance (ATPA) interface. The top navigation bar includes 'ADVANCED THREAT PREVENTION APPLIANCE', 'Refresh Data', 'System Health', and 'J-ATP Admin'. The 'Config' tab is selected. On the left, a sidebar lists various mitigation settings: Notifications, System Profiles, Environmental Settings, Email Mitigation Settings, Firewall Mitigation Settings, Asset Value, Anti-Virus Configuration, Endpoint Integration Settings, BlueCoat Configuration, Whitelist Rules, YARA Rule Upload, SNORT Rule Upload, Identity Configuration, Splunk Configuration, and External Event Collectors. The main content area shows 'Current Email Mitigations Configured' with a table:

| Description | Actions |
|-------------|--|
| Gmail | <input type="button" value="Disable"/> <input type="button" value="Delete"/> <input type="button" value="Edit"/> <input type="button" value="Test"/> |

A yellow callout box with a red border and the text '※接続テスト成功※' (Connection Test Success) is overlaid on the interface. A red box highlights a modal dialog box in the center that says 'Test Successful' with an 'OK' button. The bottom of the screen shows the Juniper logo and the text 'Powered by Juniper Version 5.0.2.20 Content Version 5.0.2.14' and 'Support | Resources | Contact Us'.

G SUITE MITIGATION設定手順 (BCC,MTA RECEIVER)

The screenshot shows the Juniper Advanced Threat Prevention Appliance interface. The top navigation bar includes 'ADVANCED THREAT PREVENTION APPLIANCE', 'Refresh Data', 'System Health', and 'J-ATP Admin'. The left sidebar lists various configuration sections: Notifications, System Profiles, Environmental Settings, Email Mitigation Settings, Firewall Mitigation Settings, Asset Value, Anti-Virus Configuration, Endpoint Integration Settings, BlueCoat Configuration, Whitelist Rules, YARA Rule Upload, SNORT Rule Upload, Identity Configuration, Splunk Configuration, and External Event Collectors. The 'Config' tab is selected. In the main content area, a table titled 'Current Email Mitigations Configured' shows a single entry for 'Gmail'. A yellow callout box highlights the 'Test' button in the 'Actions' column for the Gmail row. A red box highlights a modal dialog box with the text 'Test Failed: No JSON object could be decoded' and an 'OK' button. The bottom of the screen shows the Juniper logo and the text 'Powered by Juniper Version 5.0.2.20 Content Version 5.0.2.14'.

※接続テスト失敗※

Test Failed: No JSON object could be decoded

OK

G SUITE MITIGATION設定手順 (BCC,MTA RECEIVER)



G SUITE MITIGATION設定手順 (BCC,MTA RECEIVER)

※Mitigation動作一例※



label:quarantinedbyjatp

Google メール ラベルを削除 その他

作成 test QuarantinedByJATP x

受信トレイ 田中次郎 17:38 (1分前) 返信 転送

スター付き To 自分

送信済みメール

下書き

QuarantinedByJATP

重要

チャット

すべてのメール

迷惑メール

ゴミ箱

カテゴリ

ラベルの管理

新しいラベルを作成

0 GB (0%) / 30 GB を使用中

一部のラベルを非表示

返信または転送するには、ここをクリックしてください

プログラム ポリシー
Powered by Google

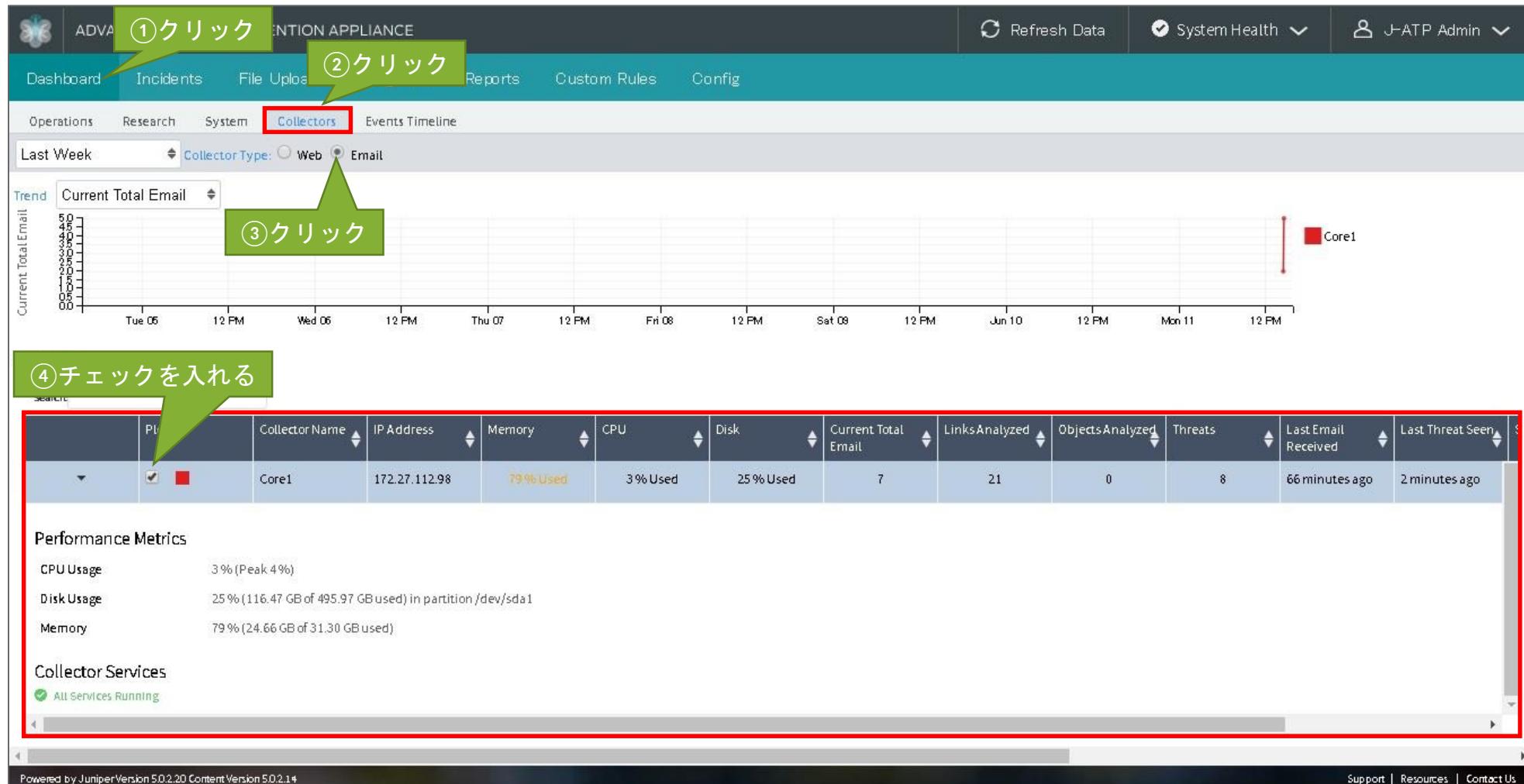
前回のアカウント アクティビティ: 1分前
アカウント アクティビティの詳細

<https://mail.google.com/mail/u/1/#label/QuarantinedByJATP>



Email collector 動作確認手順

EMAIL COLLECTOR動作確認手順



①クリック

②クリック

③クリック

④チェックを入れる

| Collector Name | IP Address | Memory | CPU | Disk | Current Total Email | Links Analyzed | Objects Analyzed | Threats | Last Email Received | Last Threat Seen |
|----------------|---------------|----------|---------|----------|---------------------|----------------|------------------|---------|---------------------|------------------|
| Core1 | 172.27.112.98 | 79% Used | 3% Used | 25% Used | 7 | 21 | 0 | 8 | 66 minutes ago | 2 minutes ago |

Performance Metrics

CPU Usage: 3% (Peak 4%)

Disk Usage: 25% (116.47 GB of 495.97 GB used) in partition /dev/sda1

Memory: 79% (24.66 GB of 31.30 GB used)

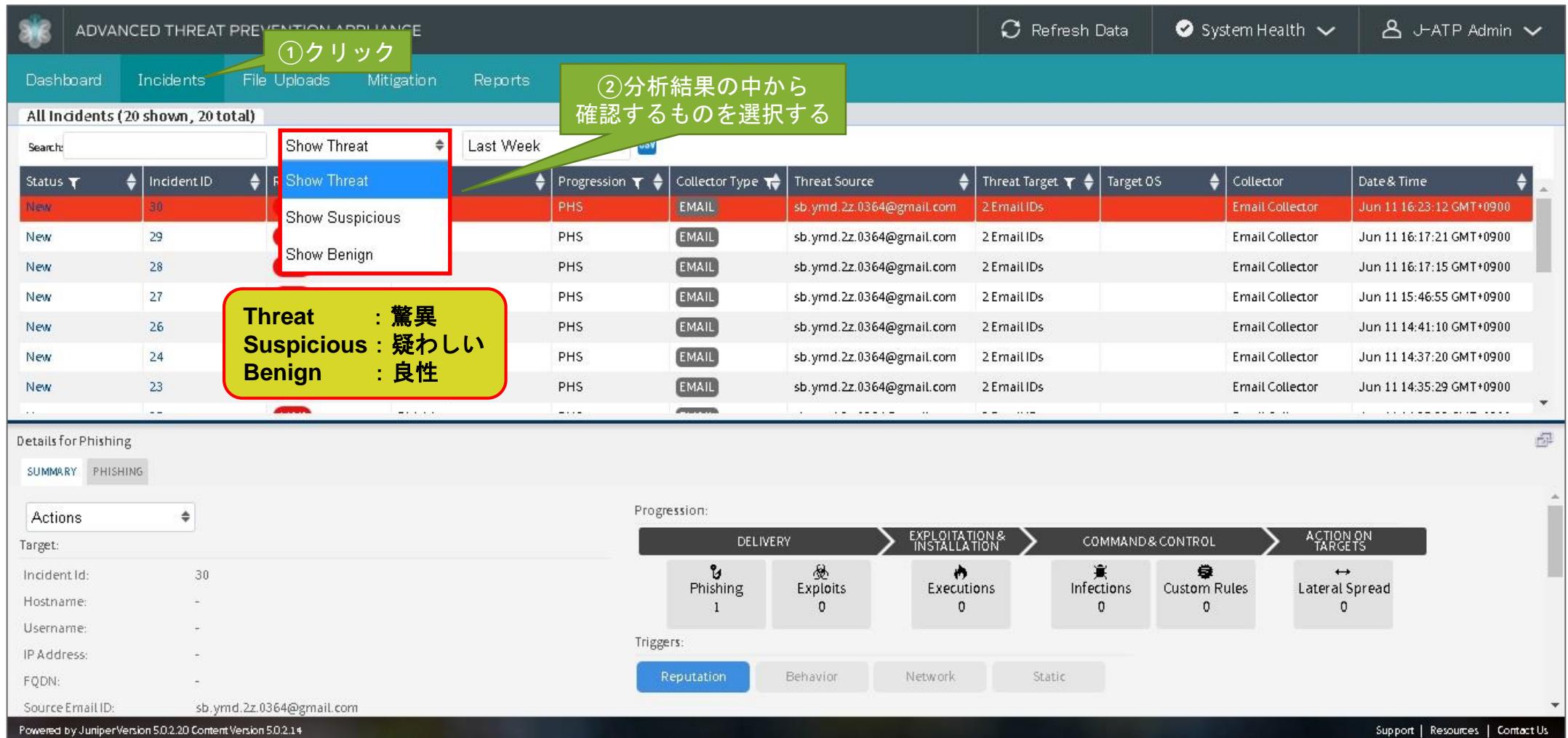
Collector Services

All Services Running

Powered by Juniper Version 5.0.2.20 Content Version 5.0.2.14

Support | Resources | Contact Us

EMAIL COLLECTOR動作確認手順



①クリック

②分析結果の中から確認するものを選択する

Threat : 驚異
Suspicious : 疑わしい
Benign : 良性

| Status | Incident ID | Progression | Collector Type | Threat Source | Threat Target | Target OS | Collector | Date & Time |
|--------|-------------|-------------|----------------|--------------------------|---------------|-----------|-----------------|--------------------------|
| New | 30 | PHS | EMAIL | sb.ymd.2z.0364@gmail.com | 2 Email IDs | | Email Collector | Jun 11 16:23:12 GMT+0900 |
| New | 29 | PHS | EMAIL | sb.ymd.2z.0364@gmail.com | 2 Email IDs | | Email Collector | Jun 11 16:17:21 GMT+0900 |
| New | 28 | PHS | EMAIL | sb.ymd.2z.0364@gmail.com | 2 Email IDs | | Email Collector | Jun 11 16:17:15 GMT+0900 |
| New | 27 | PHS | EMAIL | sb.ymd.2z.0364@gmail.com | 2 Email IDs | | Email Collector | Jun 11 15:46:55 GMT+0900 |
| New | 26 | PHS | EMAIL | sb.ymd.2z.0364@gmail.com | 2 Email IDs | | Email Collector | Jun 11 14:41:10 GMT+0900 |
| New | 24 | PHS | EMAIL | sb.ymd.2z.0364@gmail.com | 2 Email IDs | | Email Collector | Jun 11 14:37:20 GMT+0900 |
| New | 23 | PHS | EMAIL | sb.ymd.2z.0364@gmail.com | 2 Email IDs | | Email Collector | Jun 11 14:35:29 GMT+0900 |

Details for Phishing

SUMMARY: PHISHING

Actions: Target: Incident ID: 30 Hostname: - Username: - IP Address: - FQDN: - Source Email ID: sb.ymd.2z.0364@gmail.com

Progression:

DELIVERY > EXPLOITATION & INSTALLATION > COMMAND & CONTROL > ACTION ON TARGETS

Triggers: Reputation Behavior Network Static

Phishing: 1 Exploits: 0 Executions: 0 Infections: 0 Custom Rules: 0 Lateral Spread: 0

Powered by Juniper Version 5.0.2.0 Content Version 5.0.2.14

Support | Resources | Contact Us

EMAIL COLLECTOR動作確認手順

ADVANCED THREAT PREVENTION APPLIANCE

Refresh Data System Health J-ATP Admin

Dashboard Incidents File Uploads Mitigation Reports Custom Rules Config

All Incidents (17 shown, 17 total)

| Status | Incident ID | Risk | Threat | Progression | Collector Type | Threat Source | Threat Target | Target OS | Collector | Date & Time |
|--------|-------------|------|----------|-------------|----------------|--------------------------|---------------|-----------|-----------------|--------------------------|
| New | 27 | MAX | Phishing | PHS | EMAIL | sb.ymd.2z.0364@gmail.com | 2 Email IDs | | Email Collector | Jun 11 15:46:55 GMT+0900 |
| New | 26 | MAX | Phishing | PHS | EMAIL | sb.ymd.2z.0364@gmail.com | 2 Email IDs | | Email Collector | Jun 11 14:41:10 GMT+0900 |
| New | 24 | MAX | Phishing | PHS | EMAIL | sb.ymd.2z.0364@gmail.com | 2 Email IDs | | Email Collector | Jun 11 14:37:20 GMT+0900 |
| New | 23 | MAX | Phishing | PHS | EMAIL | sb.ymd.2z.0364@gmail.com | 2 Email IDs | | Email Collector | Jun 11 14:35:29 GMT+0900 |
| New | 25 | MAX | Phishing | PHS | EMAIL | sb.ymd.2z.0364@gmail.com | 2 Email IDs | | Email Collector | Jun 11 14:35:22 GMT+0900 |
| New | 22 | MAX | Phishing | PHS | EMAIL | sb.ymd.2z.0364@gmail.com | 2 Email IDs | | Email Collector | Jun 11 14:35:14 GMT+0900 |
| New | 21 | MAX | Phishing | PHS | EMAIL | sb.ymd.2z.0364@gmail.com | 2 Email IDs | | Email Collector | Jun 11 14:21:44 GMT+0900 |
| ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... |

Details for Phishing

SUMMARY: PHISHING

Actions

Target:

Incident ID: 27
Hostname: -
Username: -
IP Address: -
FQDN: -
Source Email ID: sb.ymd.2z.0364@gmail.com

Progression:

DELIVERY > EXPLOITATION & INSTALLATION > COMMAND & CONTROL > ACTION ON TARGETS

Triggers:

Reputation Behavior Network Static

Phishing 1
Exploits 0
Executions 0
Infections 0
Custom Rules 0
Lateral Spread 0

Powered by Juniper Version 5.0.2.0 Content Version 5.0.2.14

Support | Resources | Contact Us

EMAIL COLLECTOR動作確認手順

ADVANCED THREAT PREVENTION APPLIANCE

※フィッシング検出結果一例※

Details for Phishing

SUMMARY PHISHING

Actions

Target:

Incident Id: 12

Hostname: -

Username: -

IP Address: -

FQDN: -

Source Email ID: sb.ymd.2z.0364@gmail.com

Destination Email ID: user1@jatp-test.ddo.jp

Email Message ID: CADh4wB_rdAAcZr6eM4Ga2Lo_fabPKrrqyCk_fg=TlYBqEtHA@mail.gmail.com

Risk: Max

Asset Value: -

Relevance: Max

Progression: Phishing

Protocol: EMAIL

OS Matched: -

Summary: -

Collectors: Email Collector

Source: -

Golden Images: Not Configured

Progression:

DELIVERY > EXPLOITATION & INSTALLATION > COMMAND & CONTROL > ACTION ON TARGETS

Triggers:

Reputation Behavior Network Static

Custom Rules

Lateral Spread
Execution
Downloads
Exploit
Phishing

Jun 11 16:21:00 Jun 11 16:22:00 Jun 11 16:23:00 Jun 11 16:24:00 Jun 11 16:25:00



THANK YOU

JUNIPER
NETWORKS | Engineering
Simplicity