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)

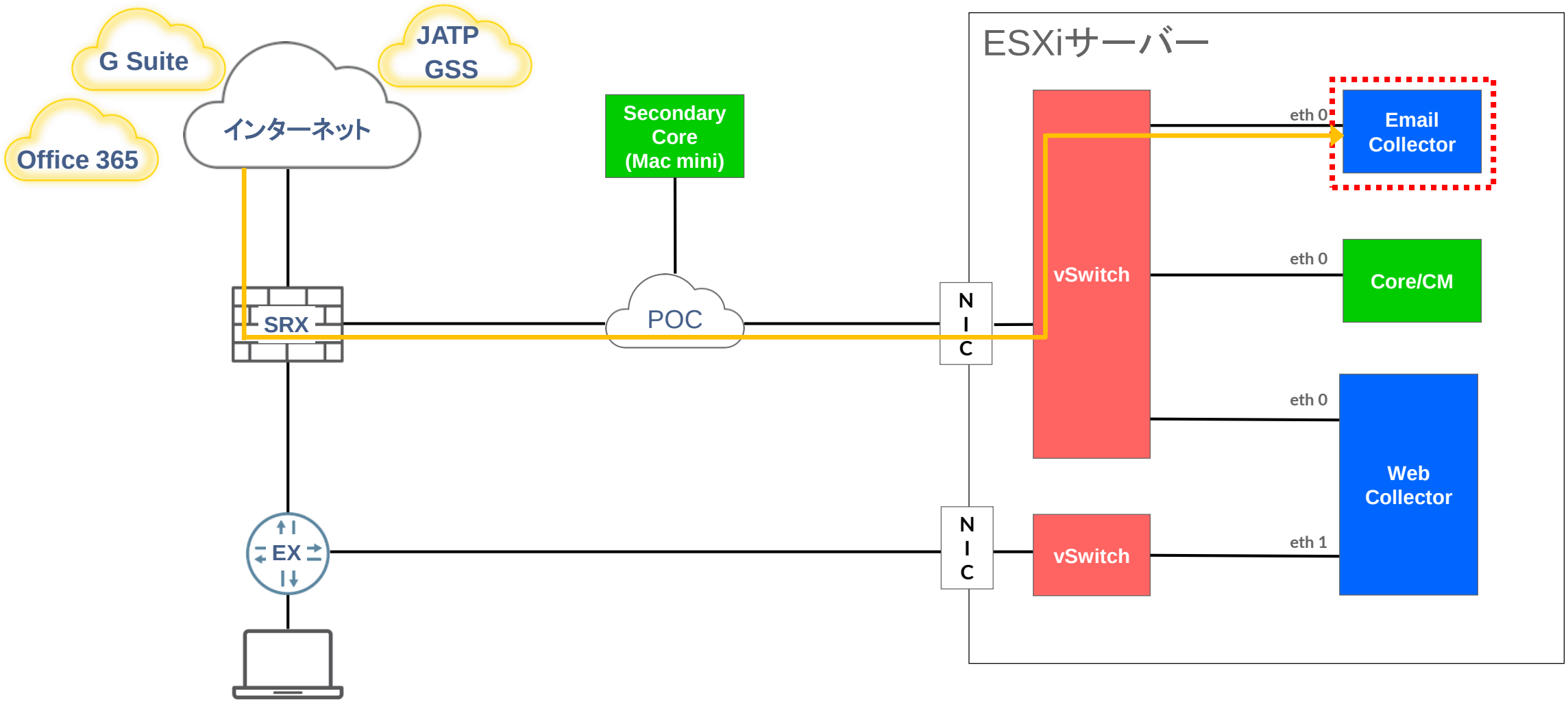
更新履歴

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

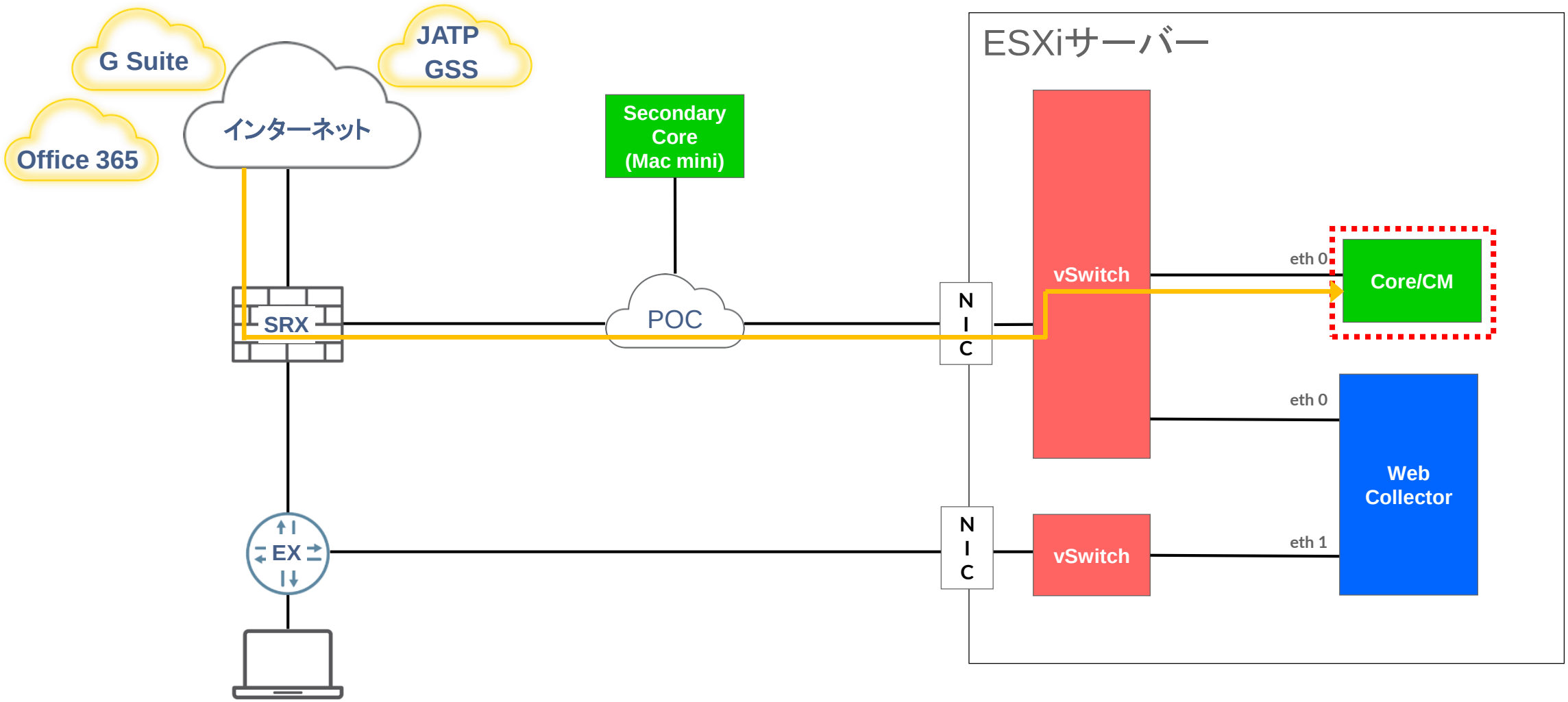
アジェンダ

- 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コマンドー例
- 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を割り当てている場合は、ファイアウォール等で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

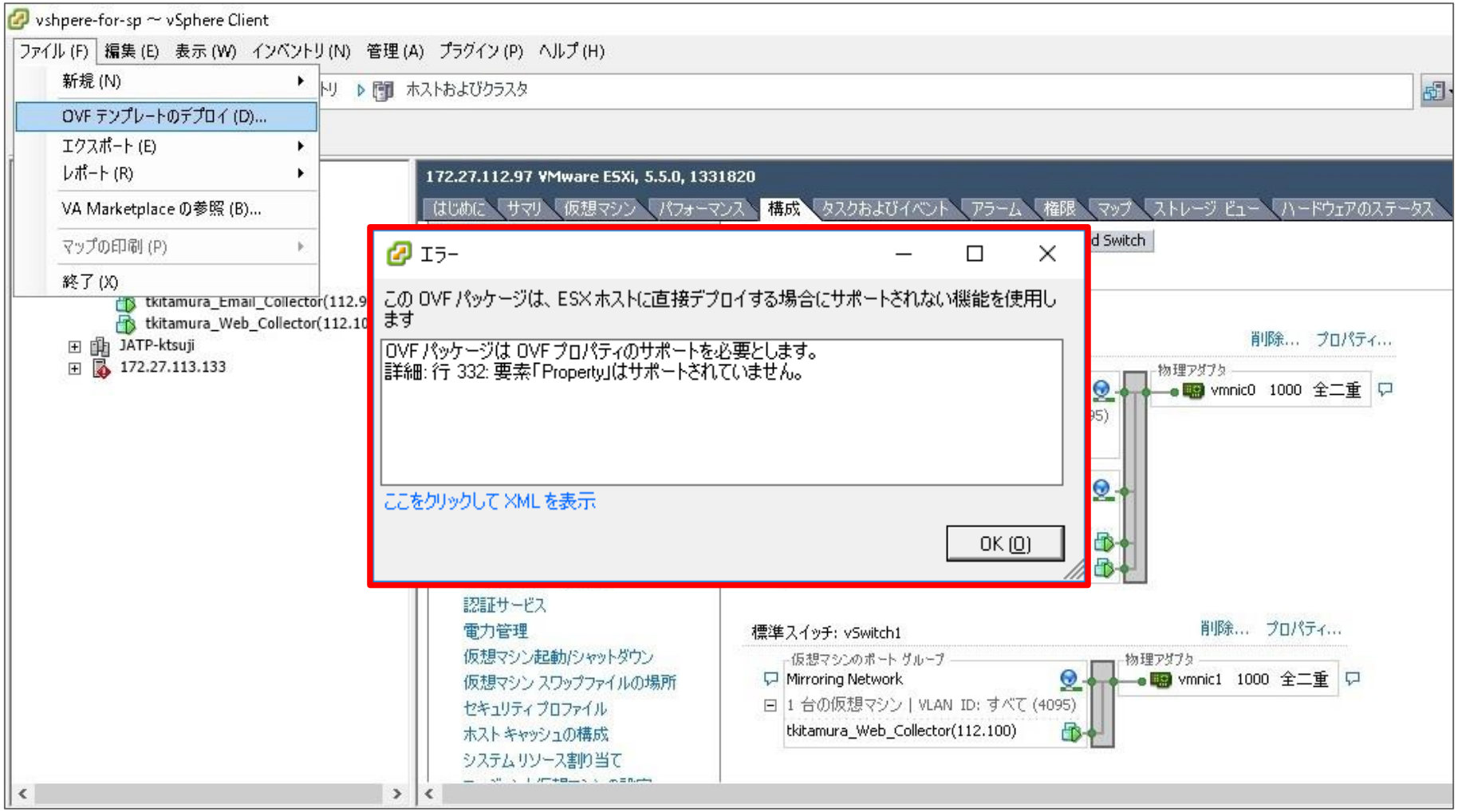
    OVFファイルを使用する
    ⇒仮想サーバー設定手順(OVFファイル)を参照

  - 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

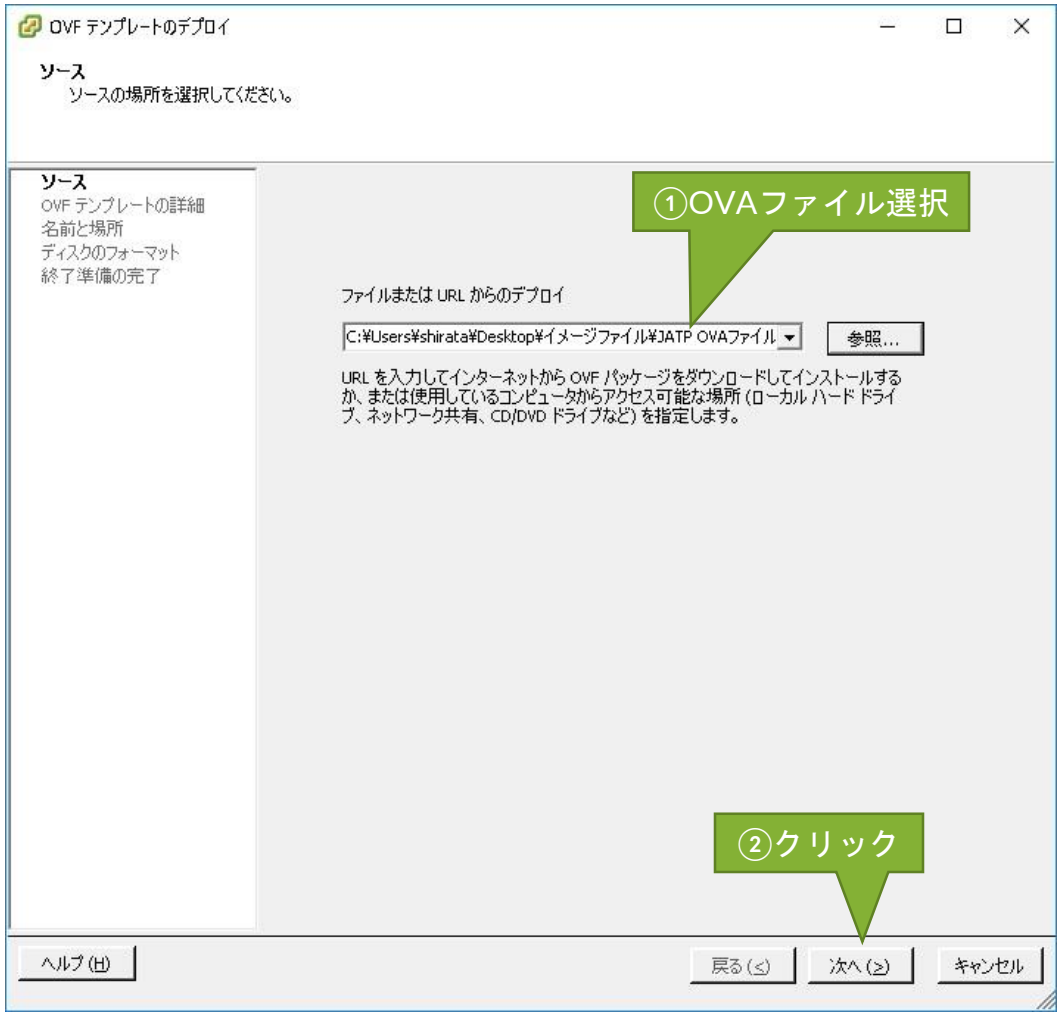
仮想サーバー設定手順(OVAファイル)

仮想サーバー設定手順(OVAファイル)
エラー表示一例

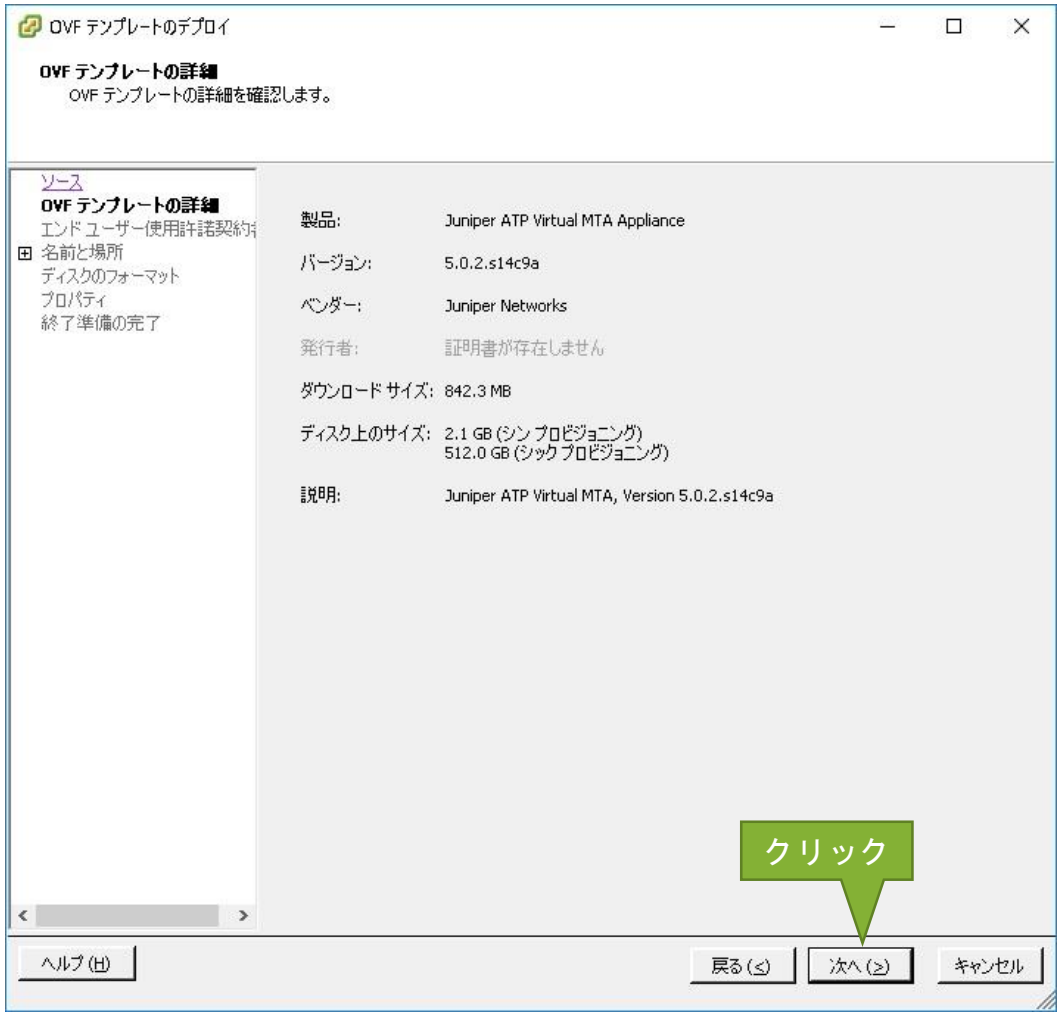


仮想サーバー設定手順(OVAファイル)

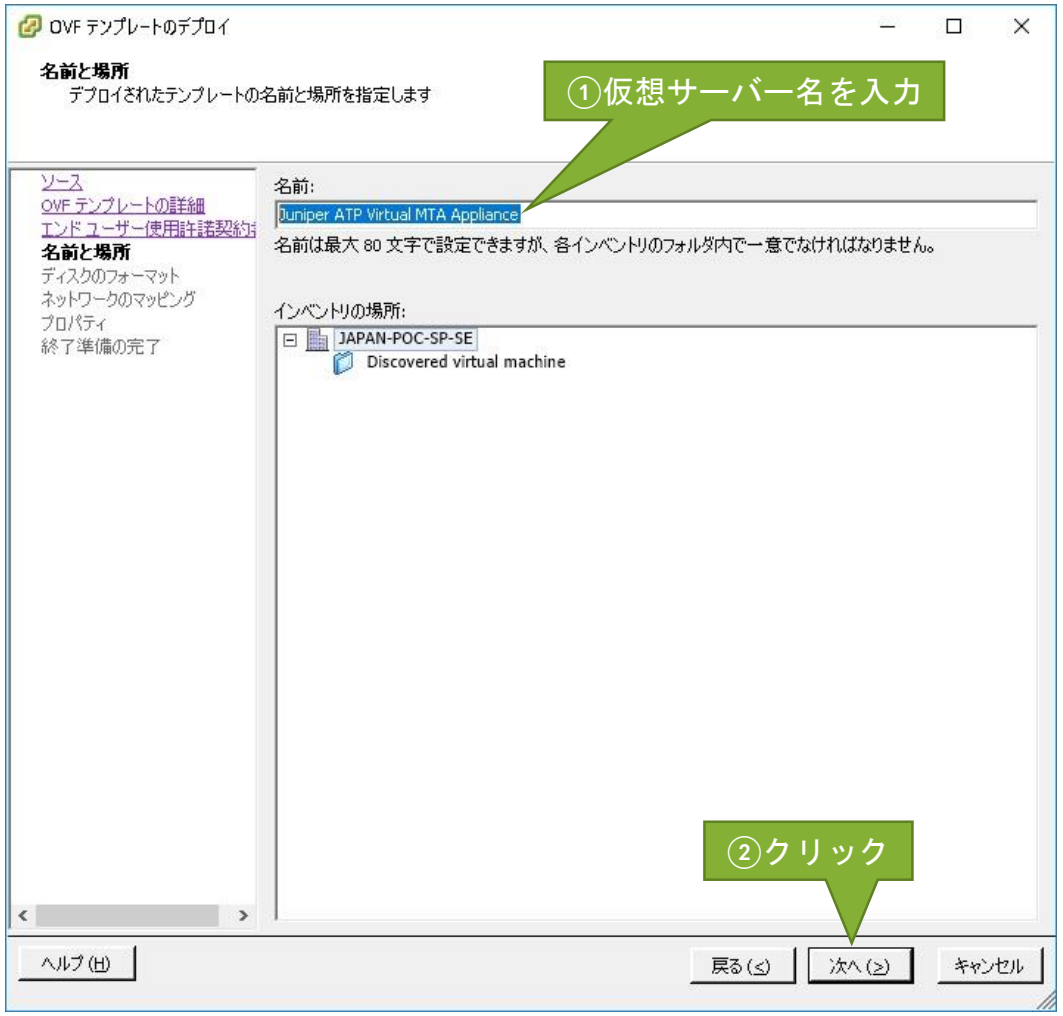
仮想サーバー設定手順(OVAファイル)



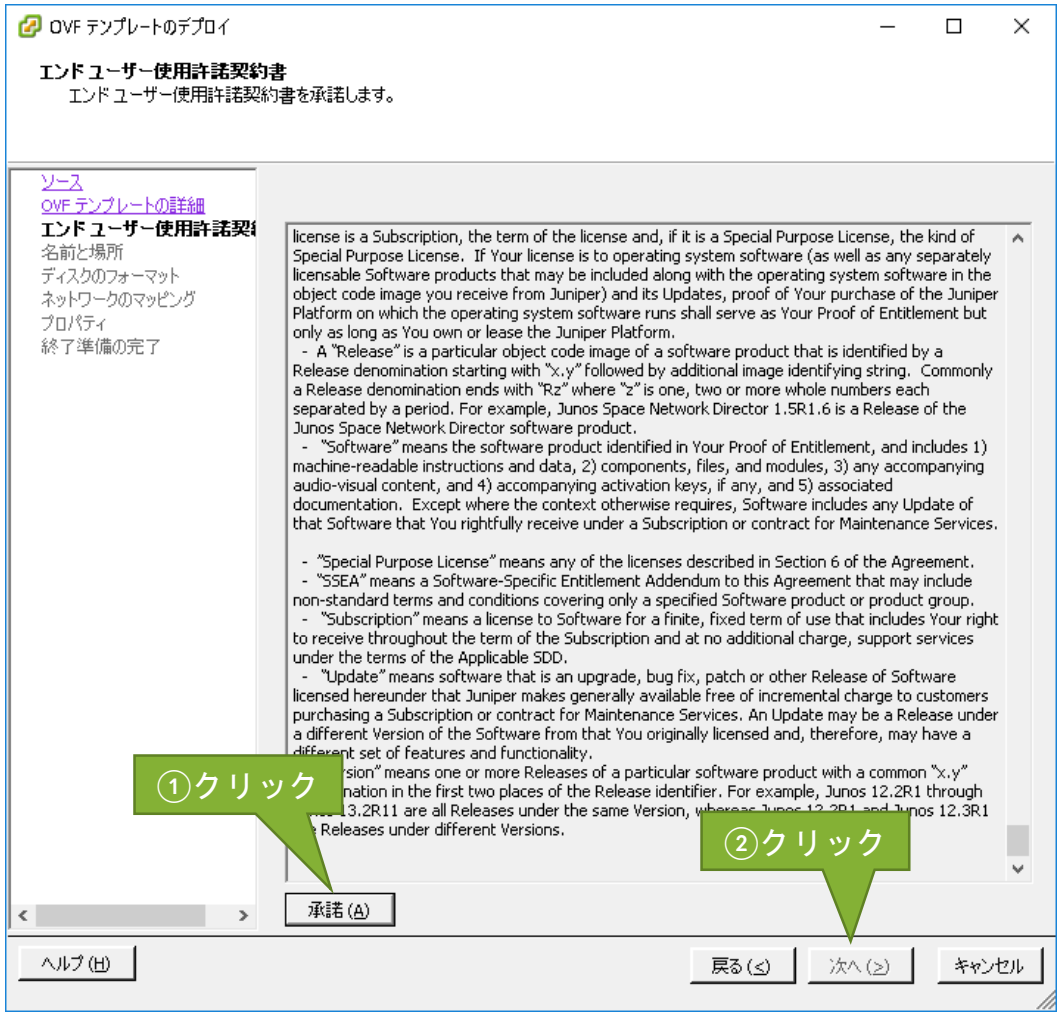
仮想サーバー設定手順(OVAファイル)



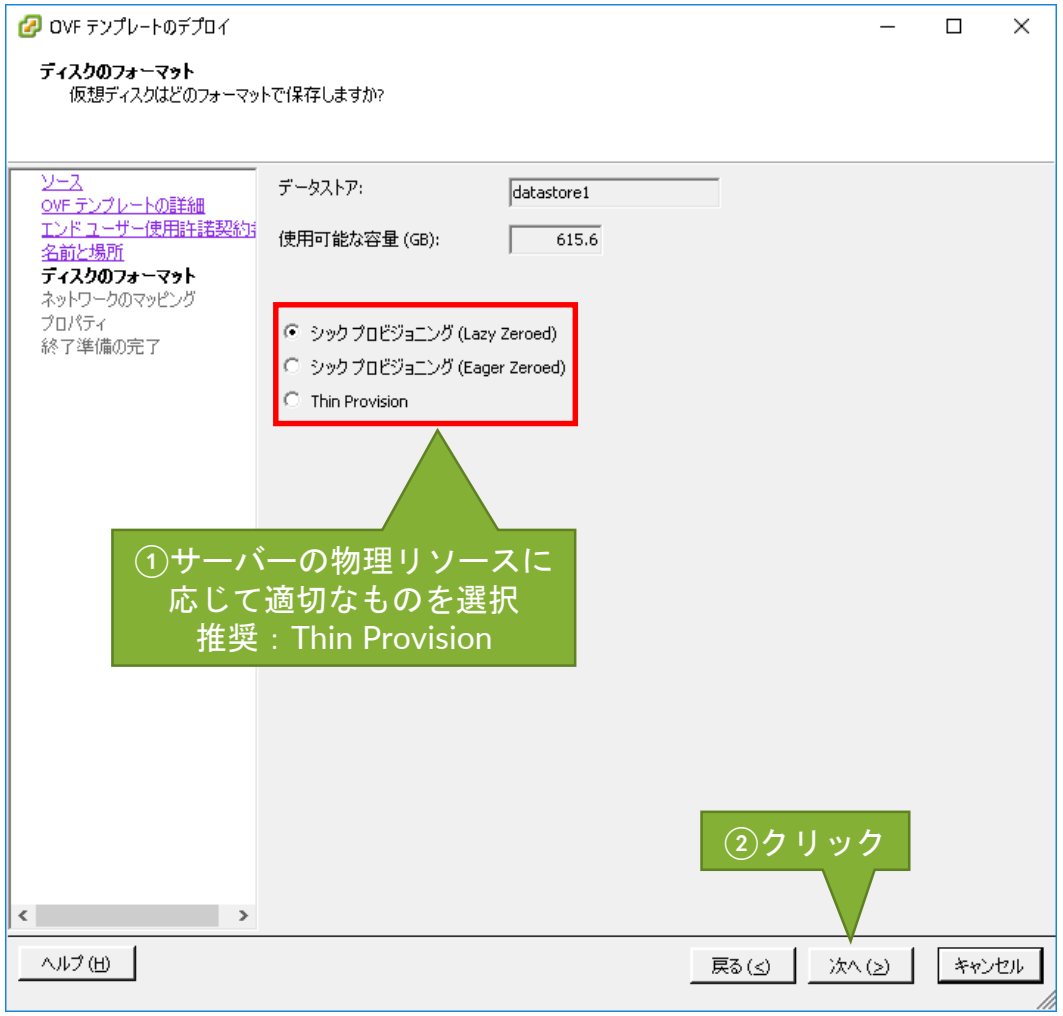
仮想サーバー設定手順(OVAファイル)



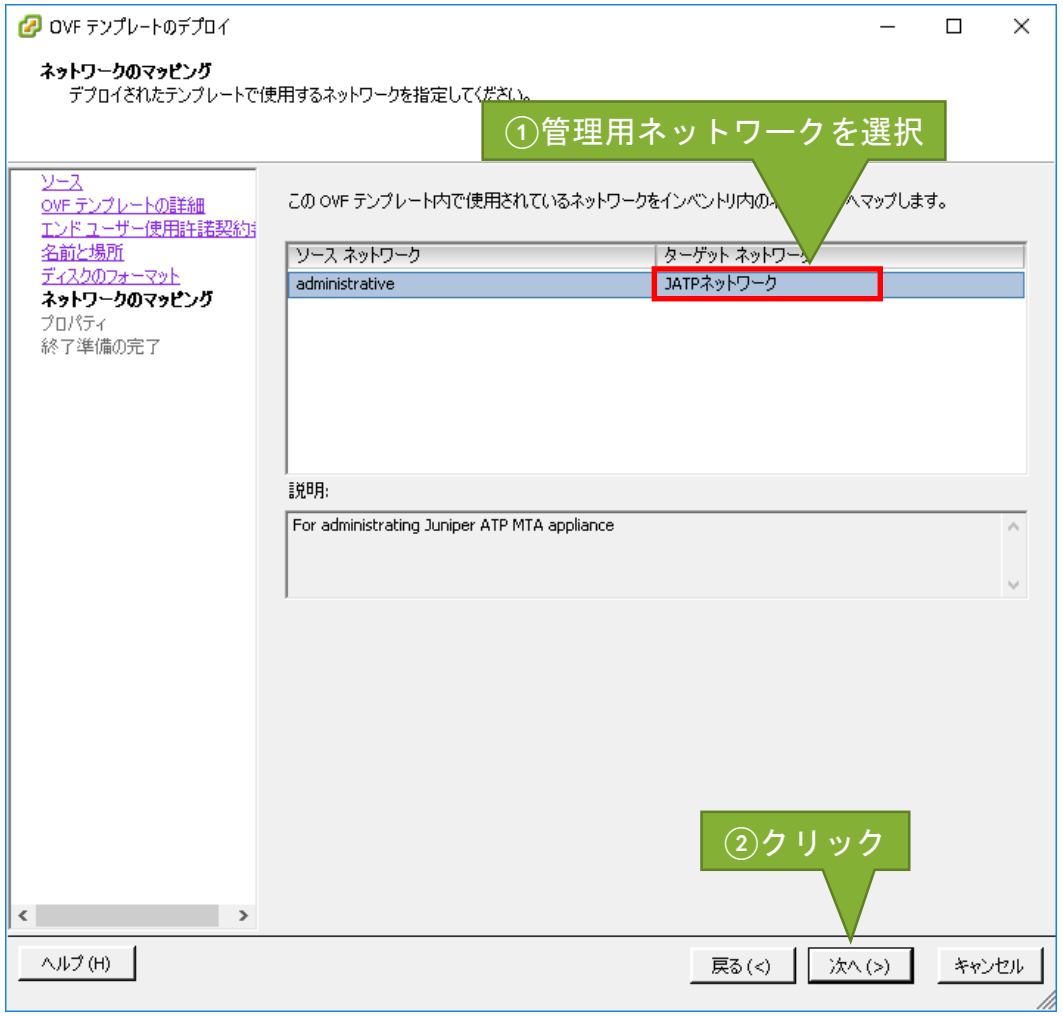
仮想サーバー設定手順(OVAファイル)



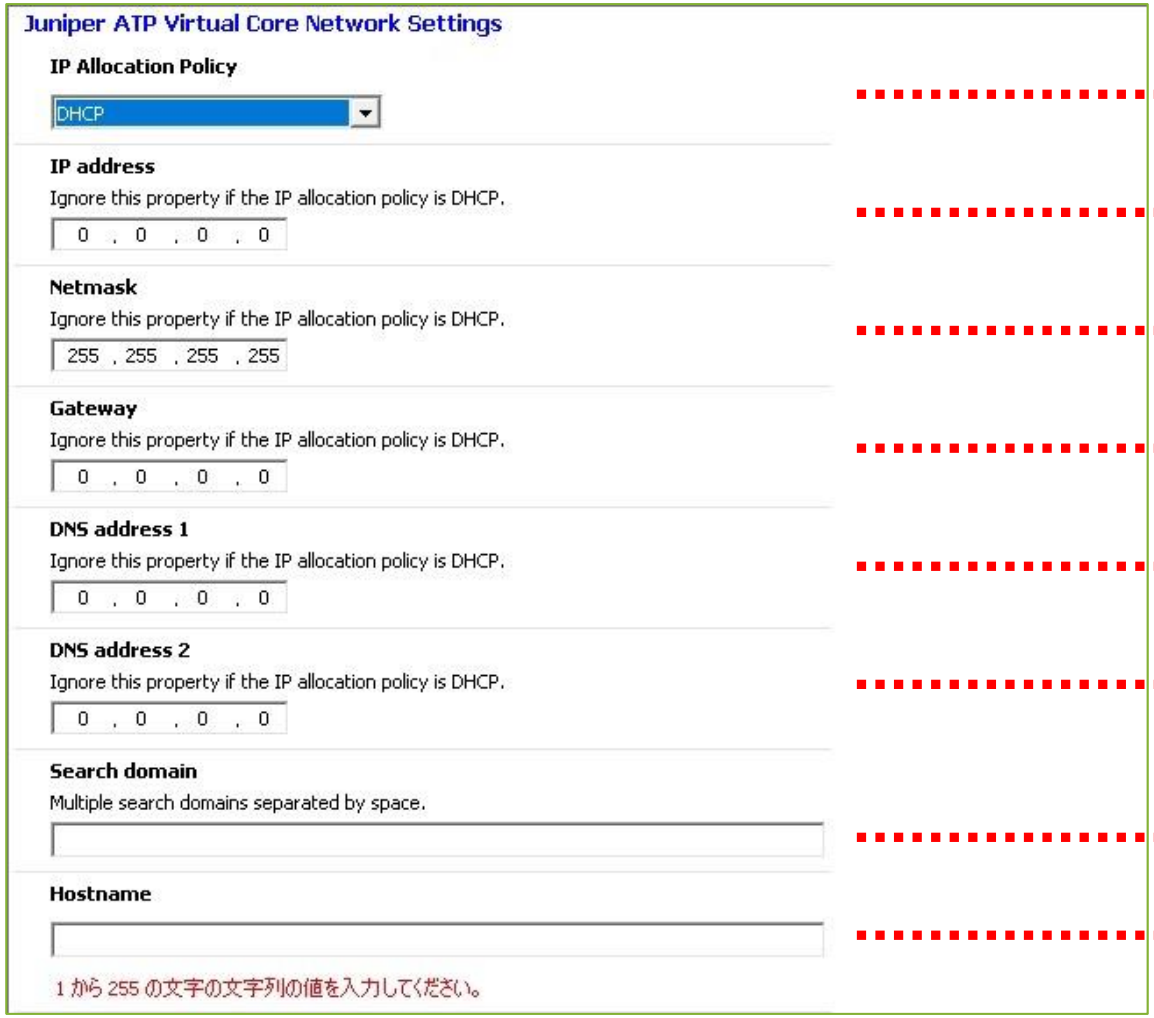
仮想サーバー設定手順(OVAファイル)



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)



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

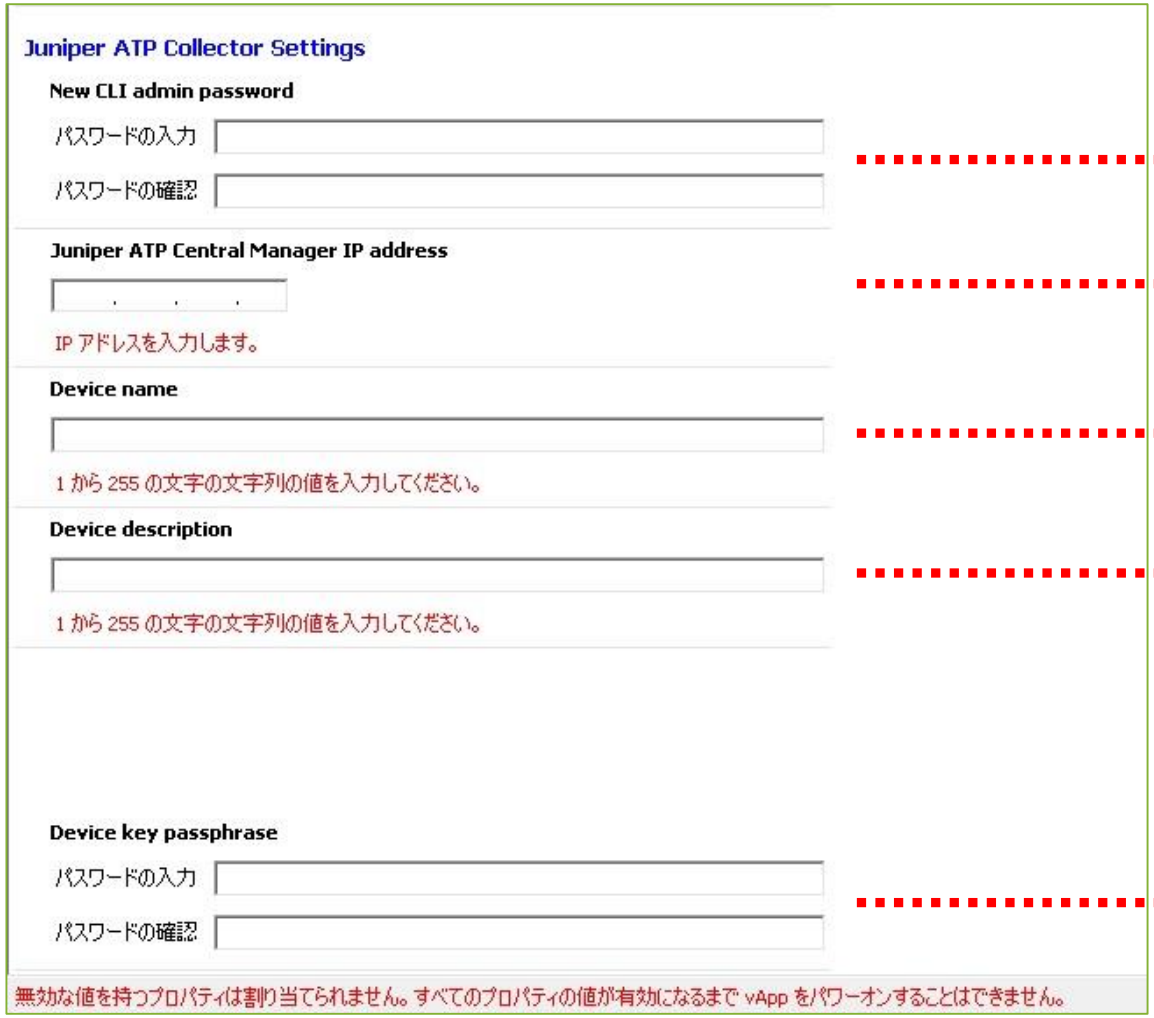
DNS1の設定

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)



adminログインパスワードの設定

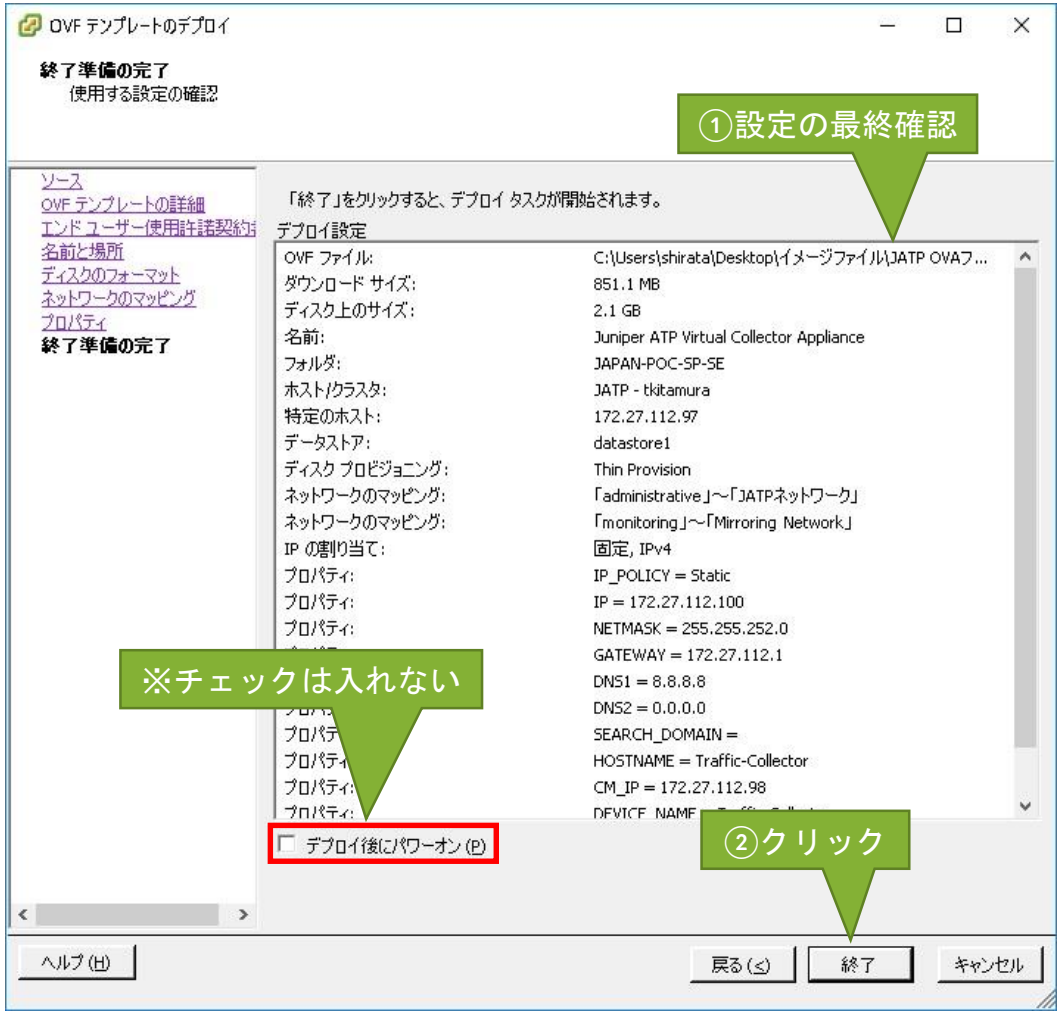
Core/CMのIPアドレスを入力

デバイスネームの設定

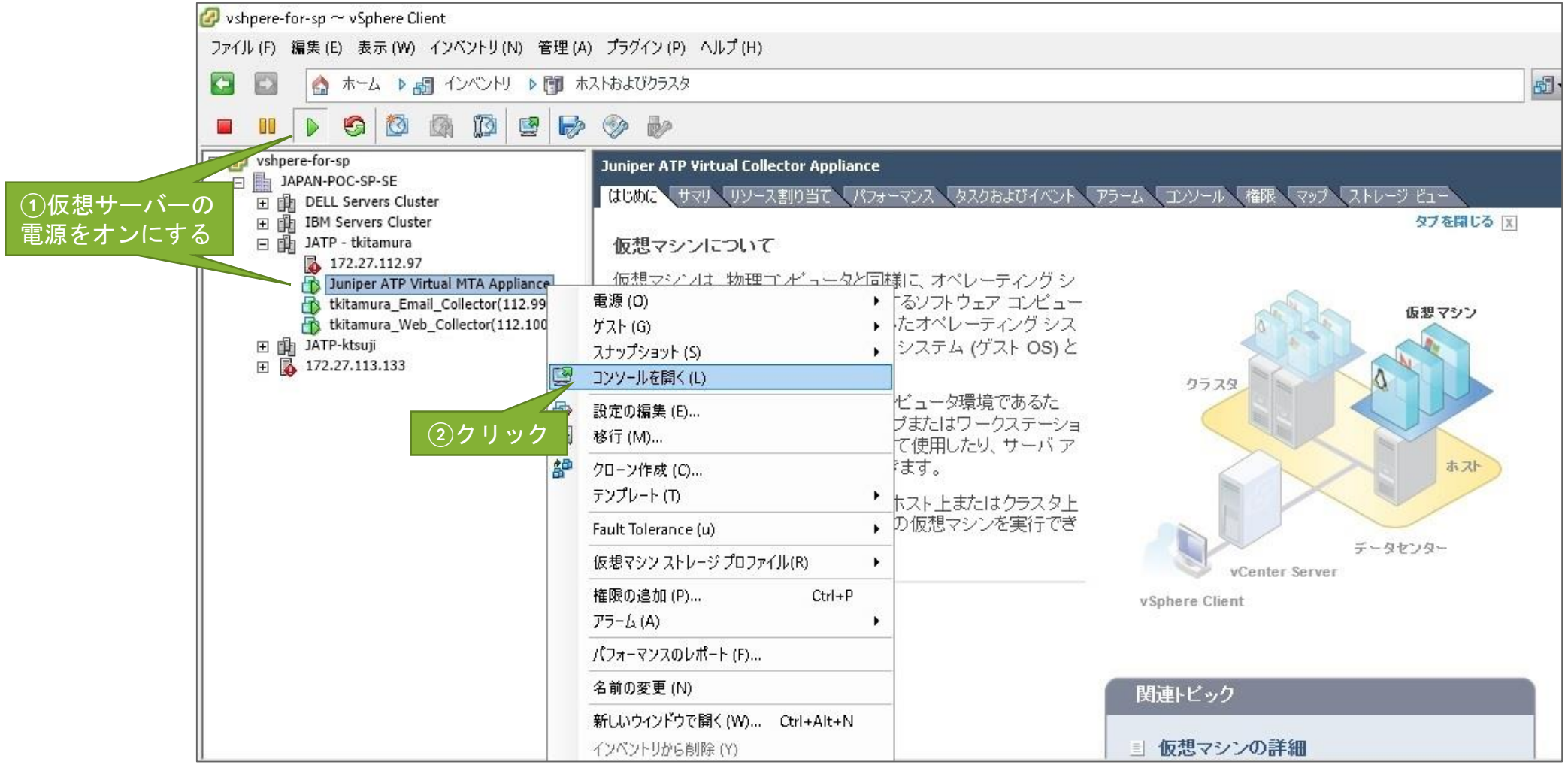
デバイスの説明

接続するCore,Collectorで
すべて共通の値を入力

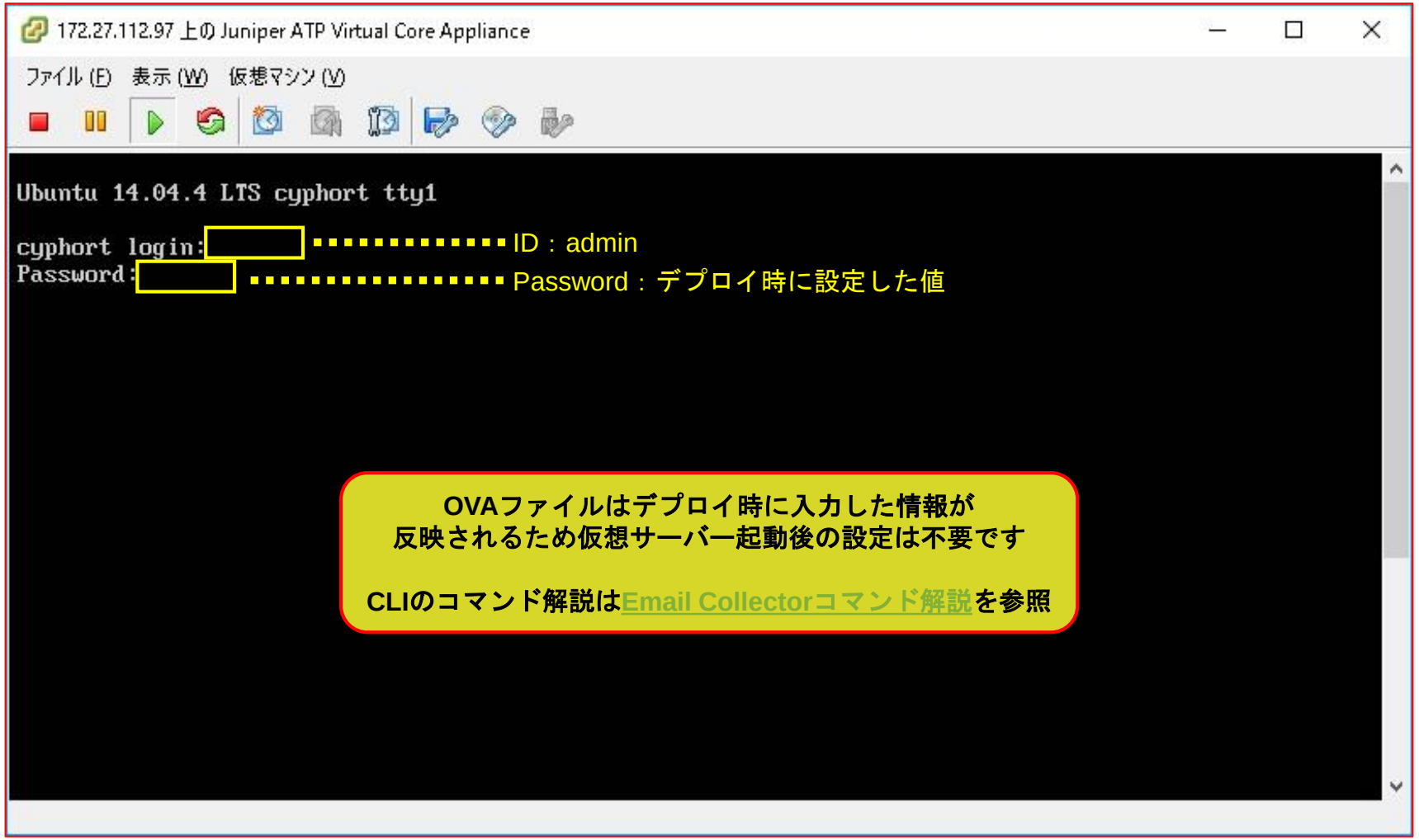
仮想サーバー設定手順(OVAファイル)



仮想サーバー設定手順(OVAファイル)



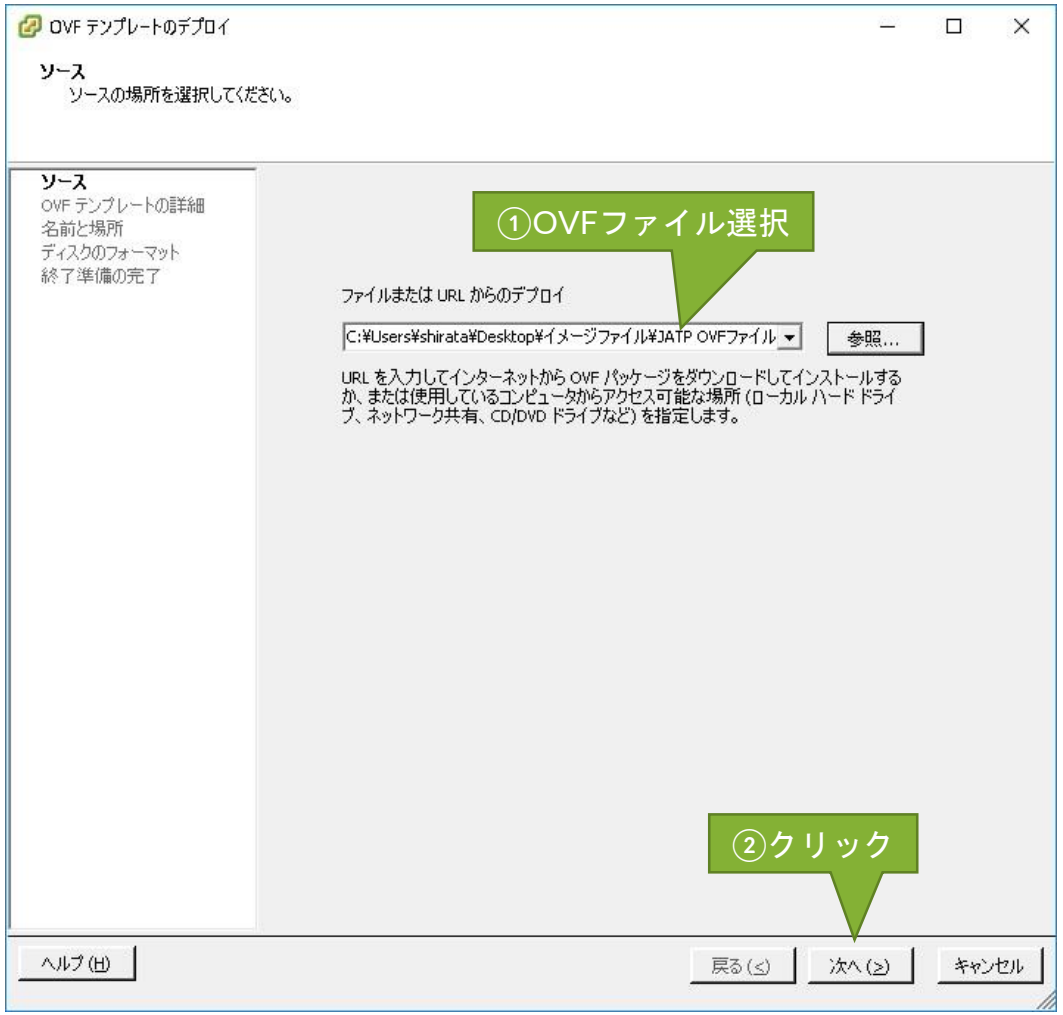
仮想サーバー設定手順(OVAファイル)



仮想サーバー設定手順
OVFファイル

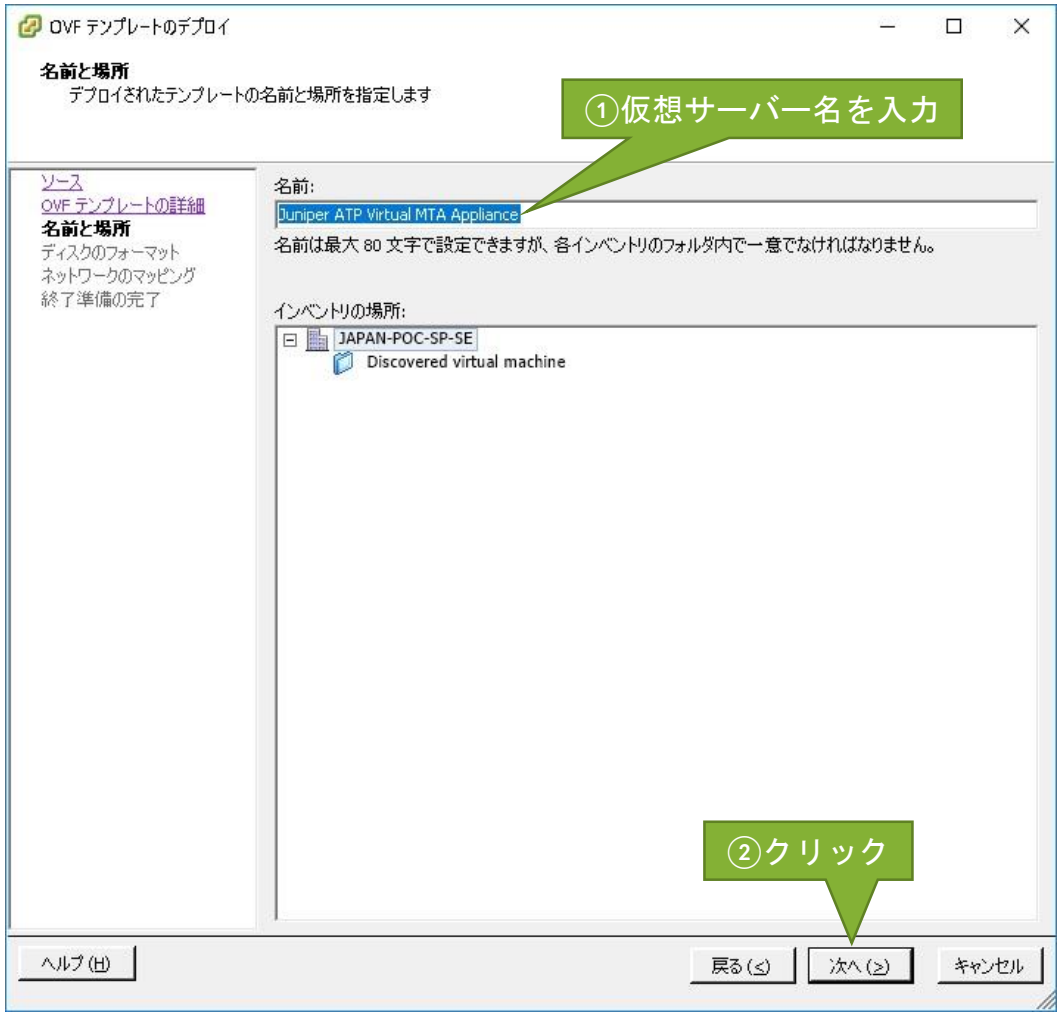
仮想サーバー設定手順(OVFファイル)

仮想サーバー設定手順(OVFファイル)

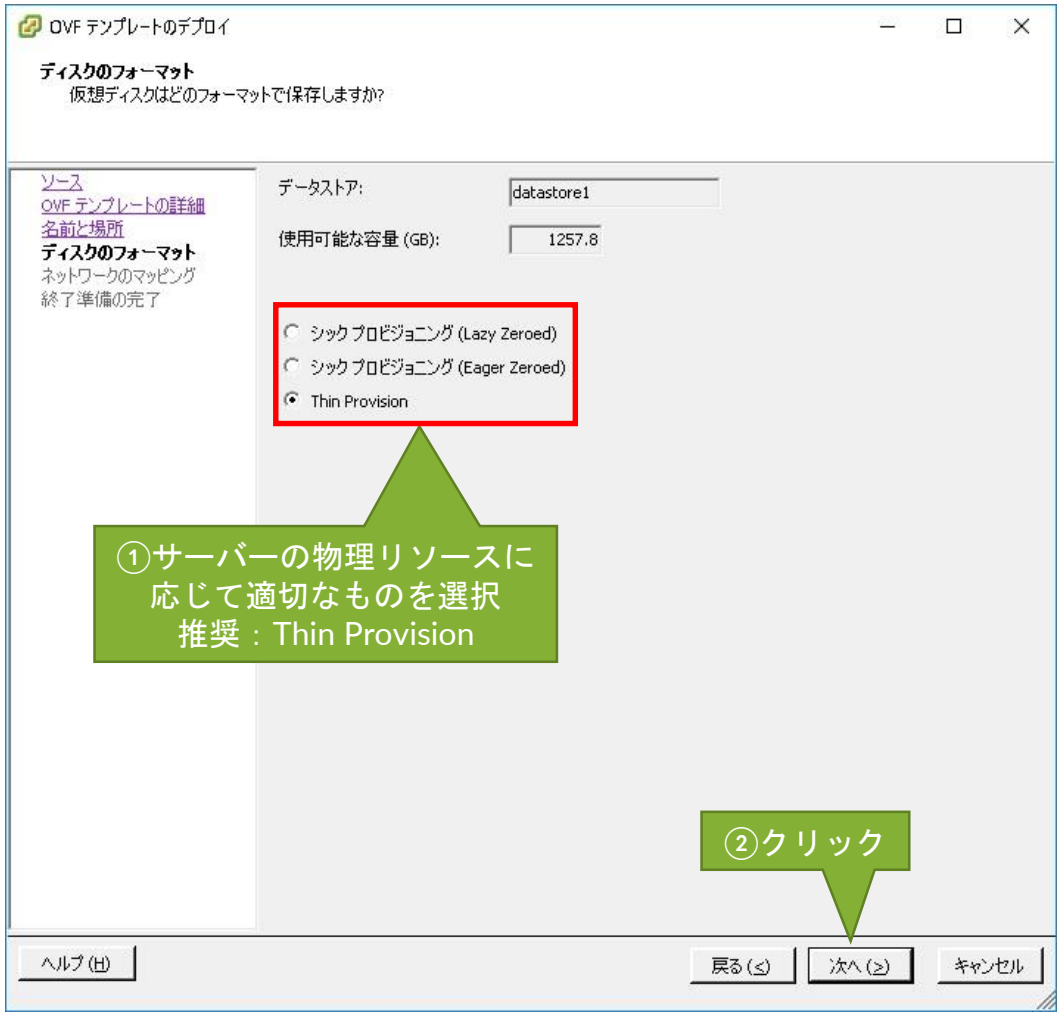


仮想サーバー設定手順(OVFファイル)

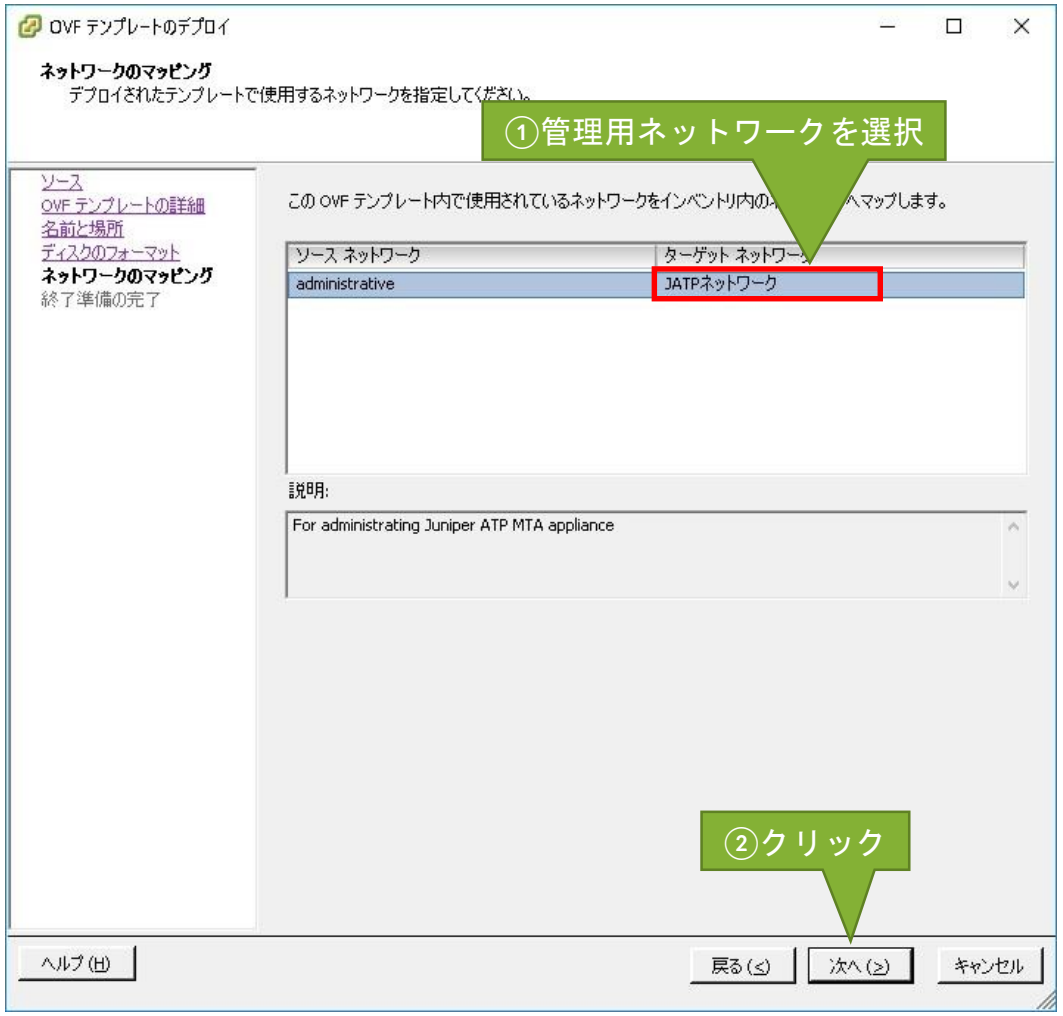
仮想サーバー設定手順(OVFファイル)



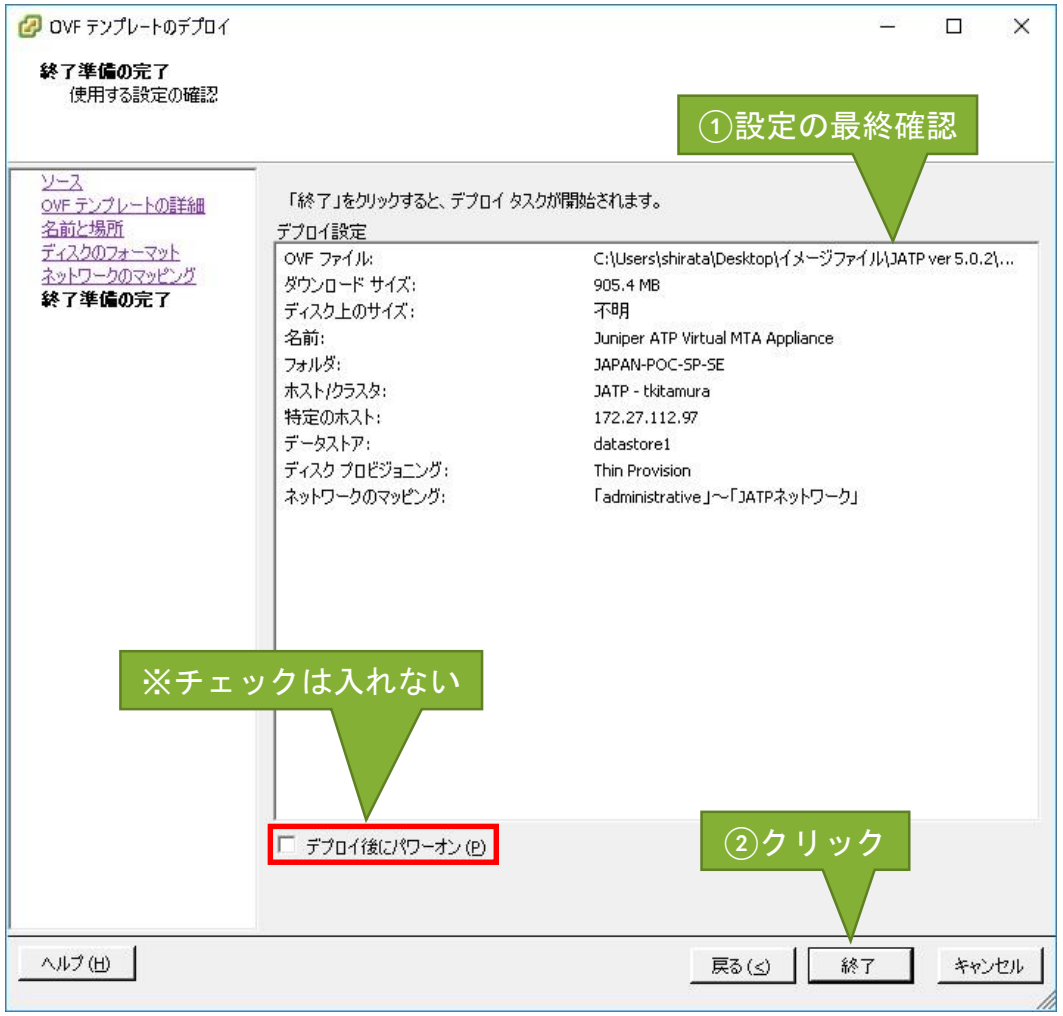
仮想サーバー設定手順(OVFファイル)



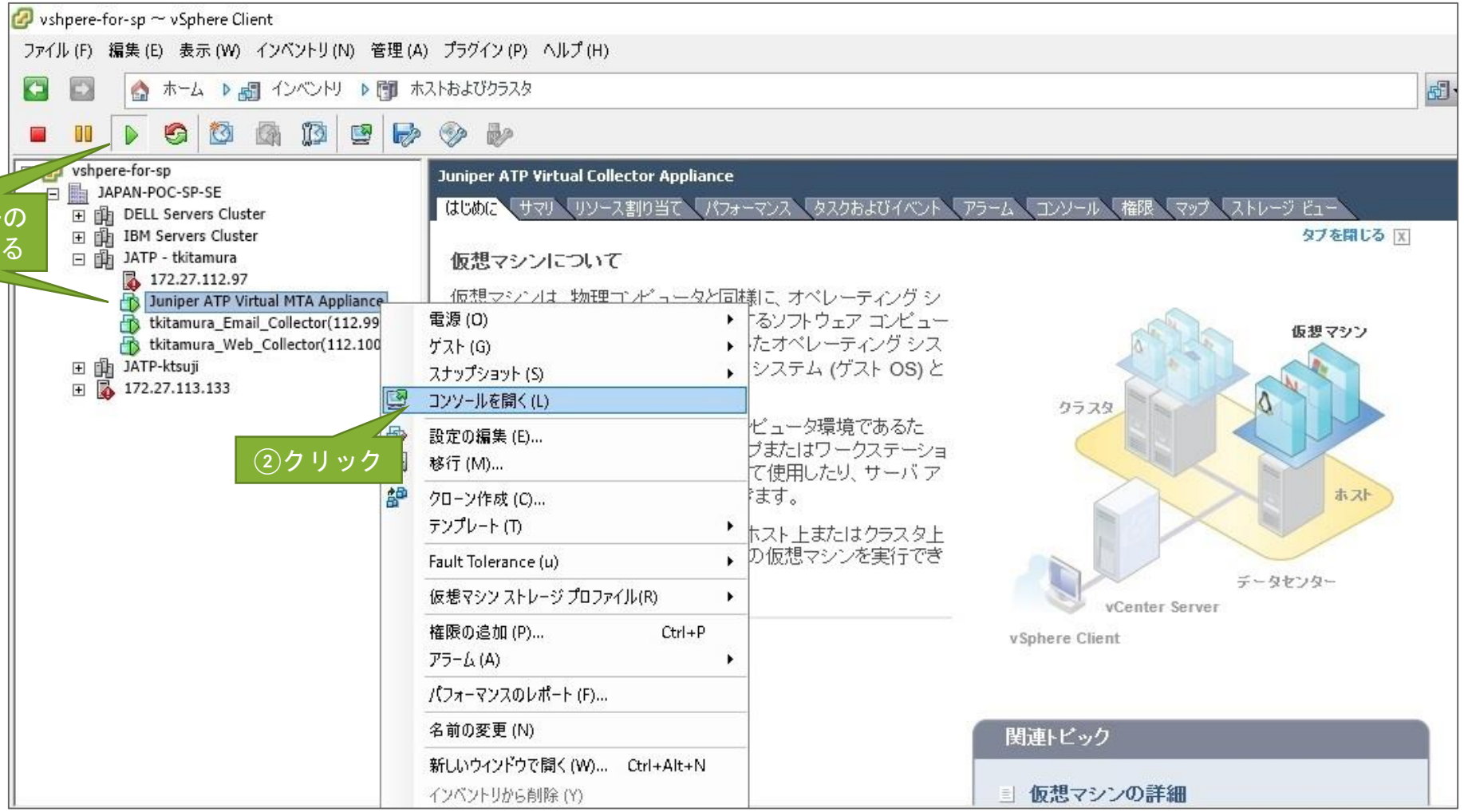
仮想サーバー設定手順(OVFファイル)



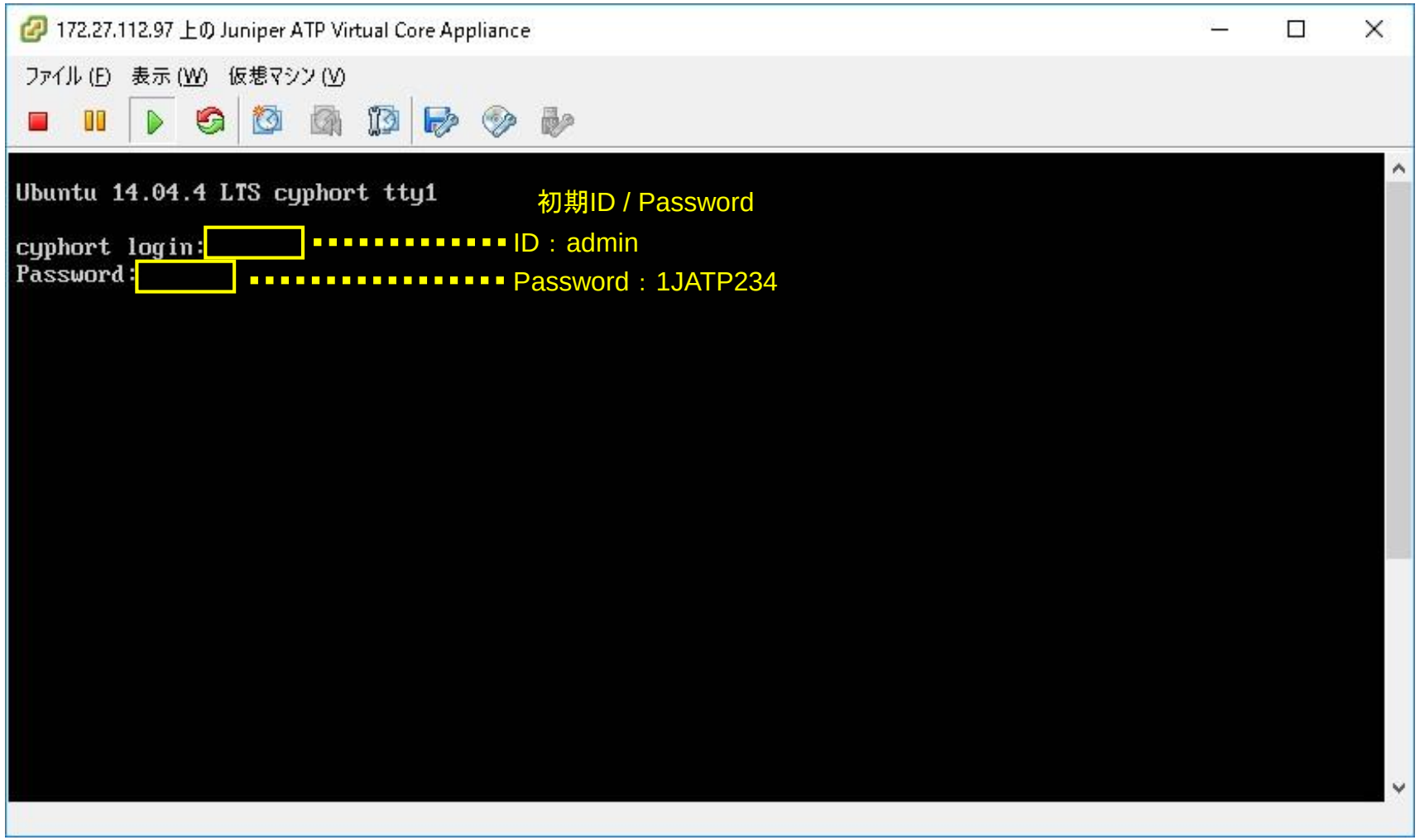
仮想サーバー設定手順(OVFファイル)



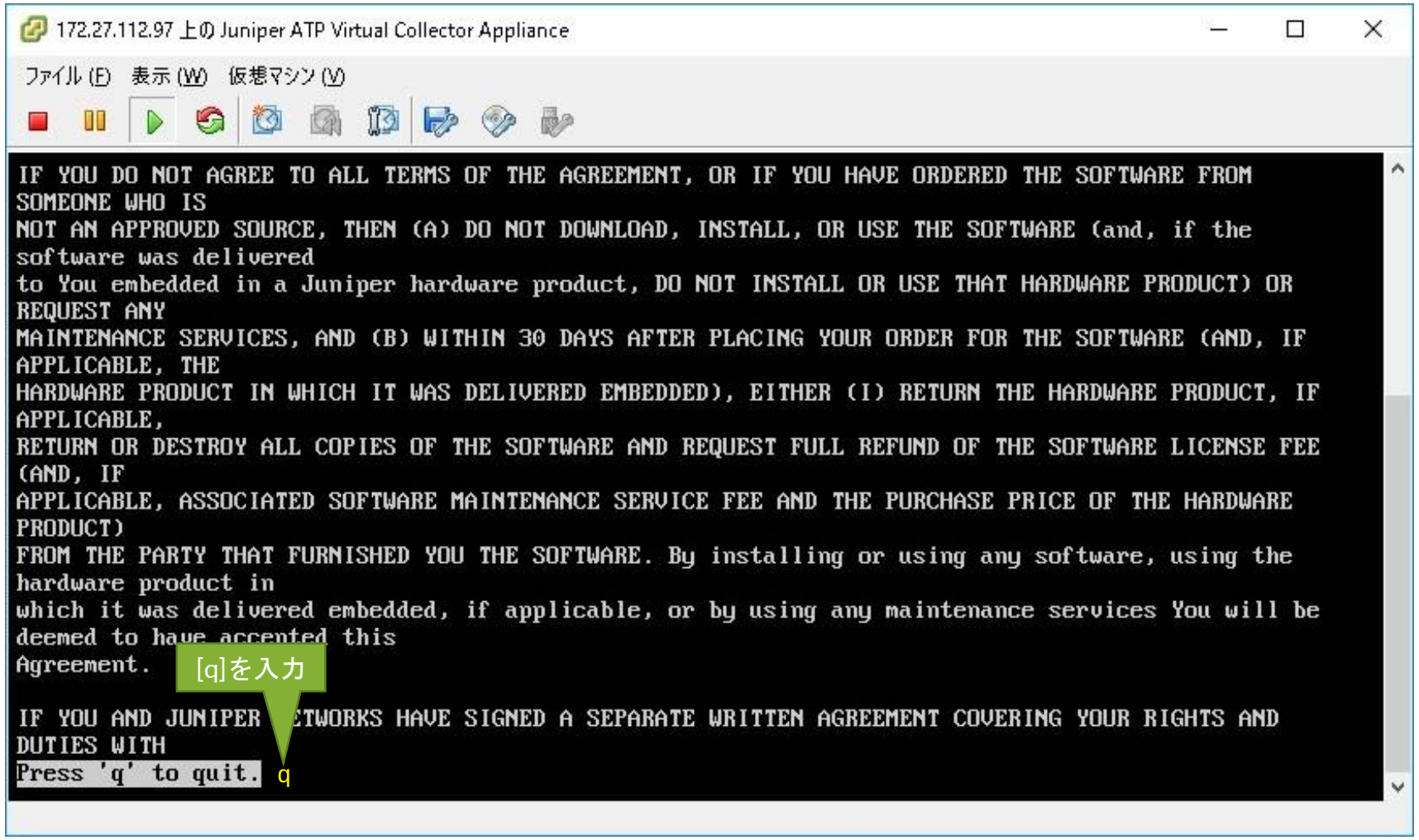
仮想サーバー設定手順(OVFファイル)



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コマンド一例

・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(server)# 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(server)# set cm xxxx.xxxx.xxxx.xxxx
```

・CLIログインパスワードの変更

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

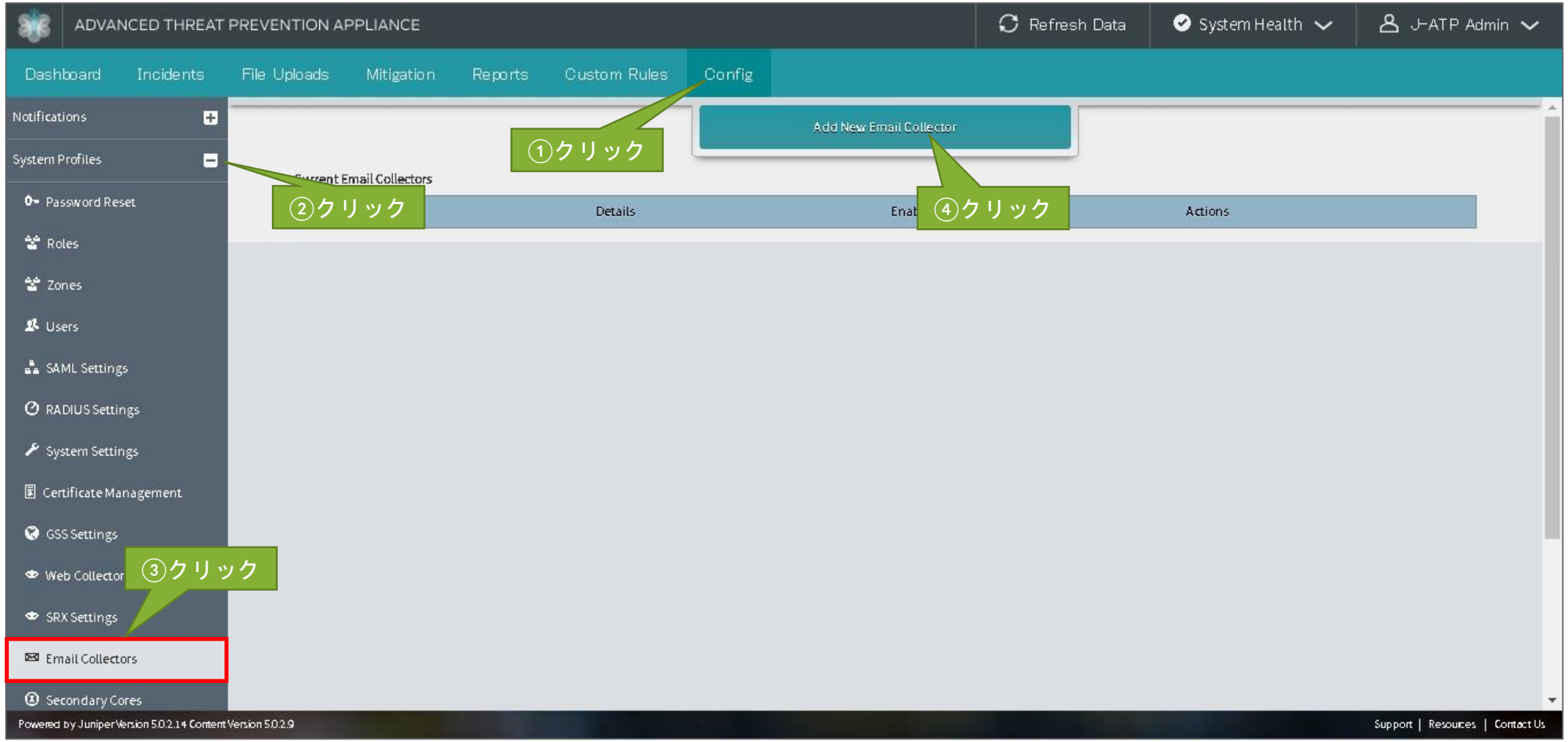
・キャプチーファイルのコピー
```
Email-Collector# diagnosis
Email-Collector(diagnosis)# copy capture user@hostname:path
```

Email Collector設定手順 (BCC)

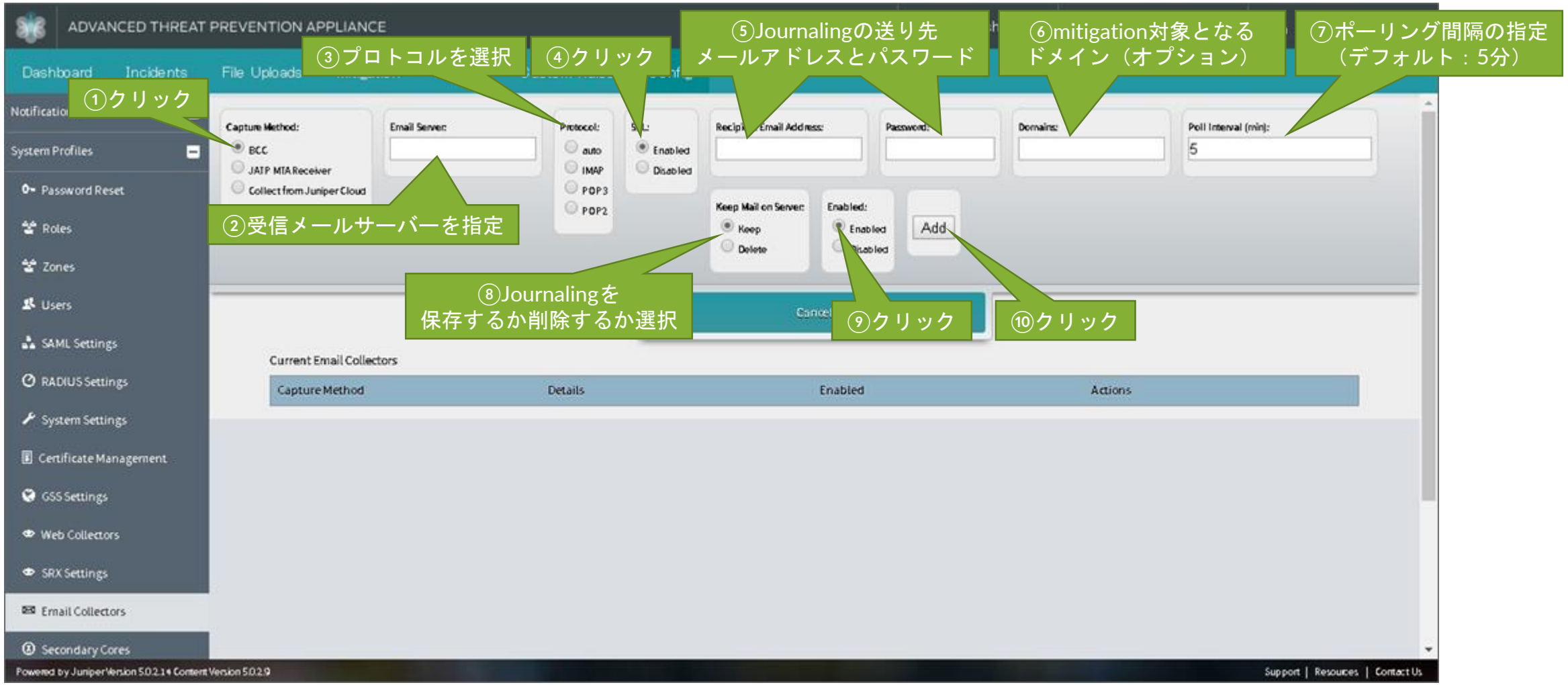
EMAIL COLLECTORについて

- 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)

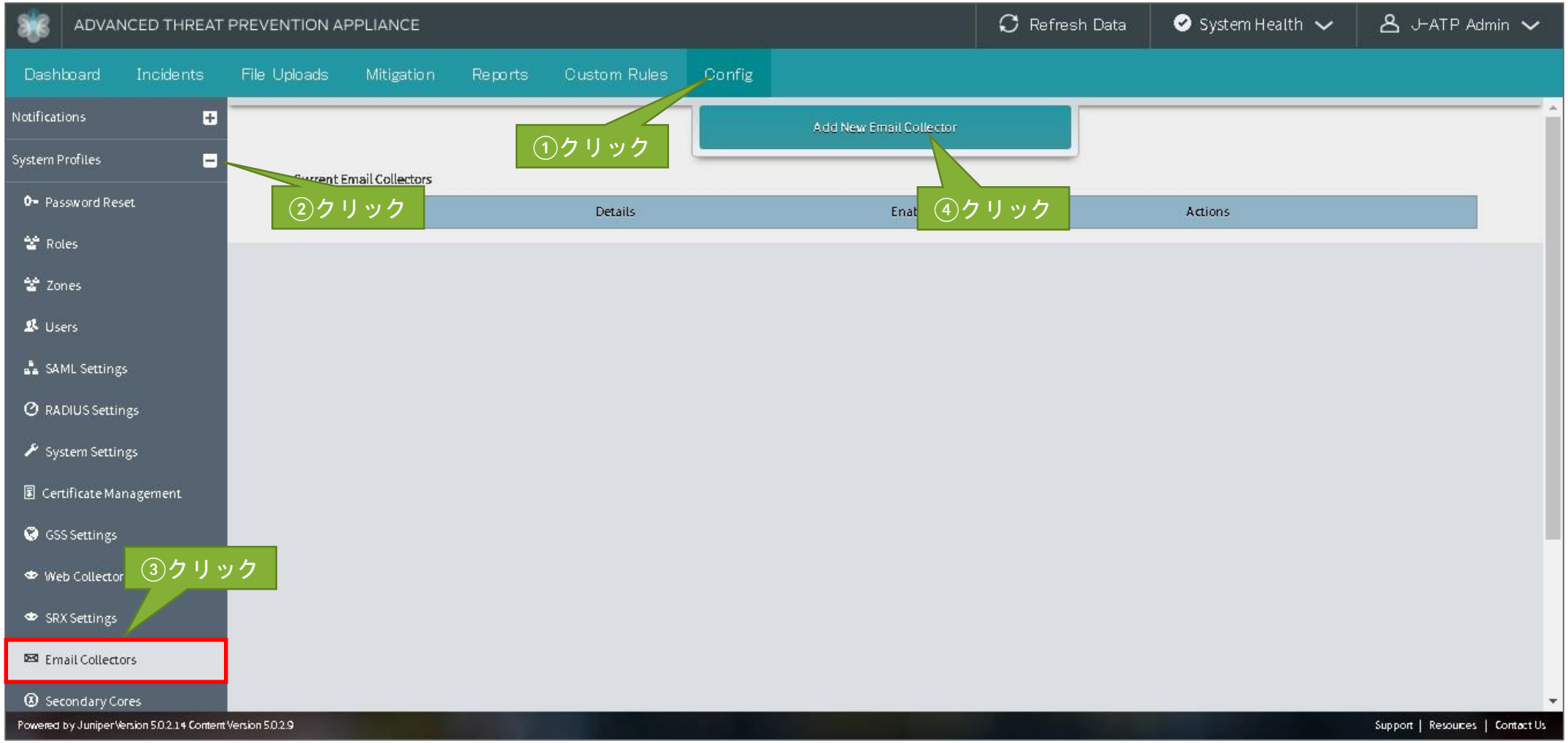


EMAIL COLLECTOR設定手順 (BCC)

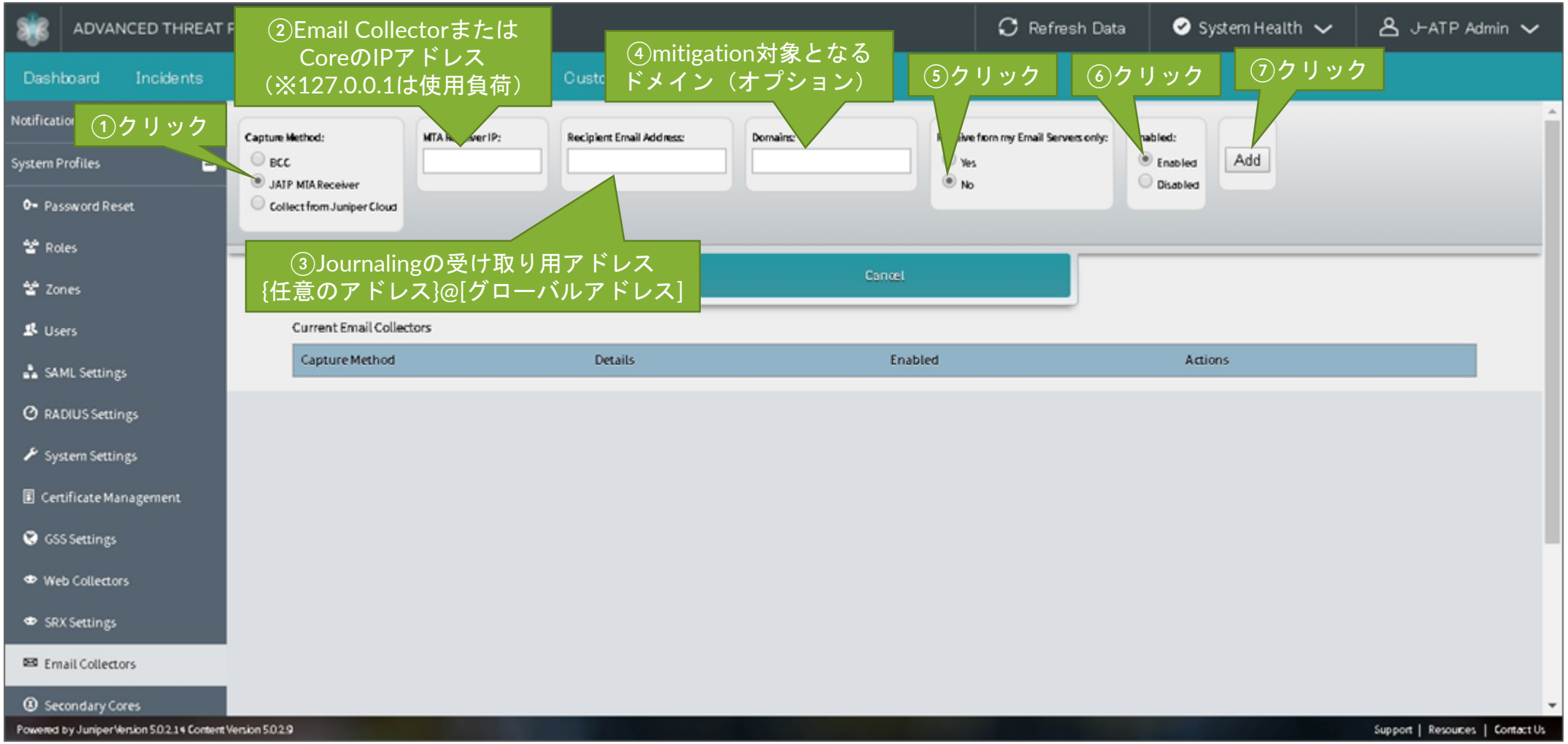


Email Collector設定手順 (MTA Receiver)

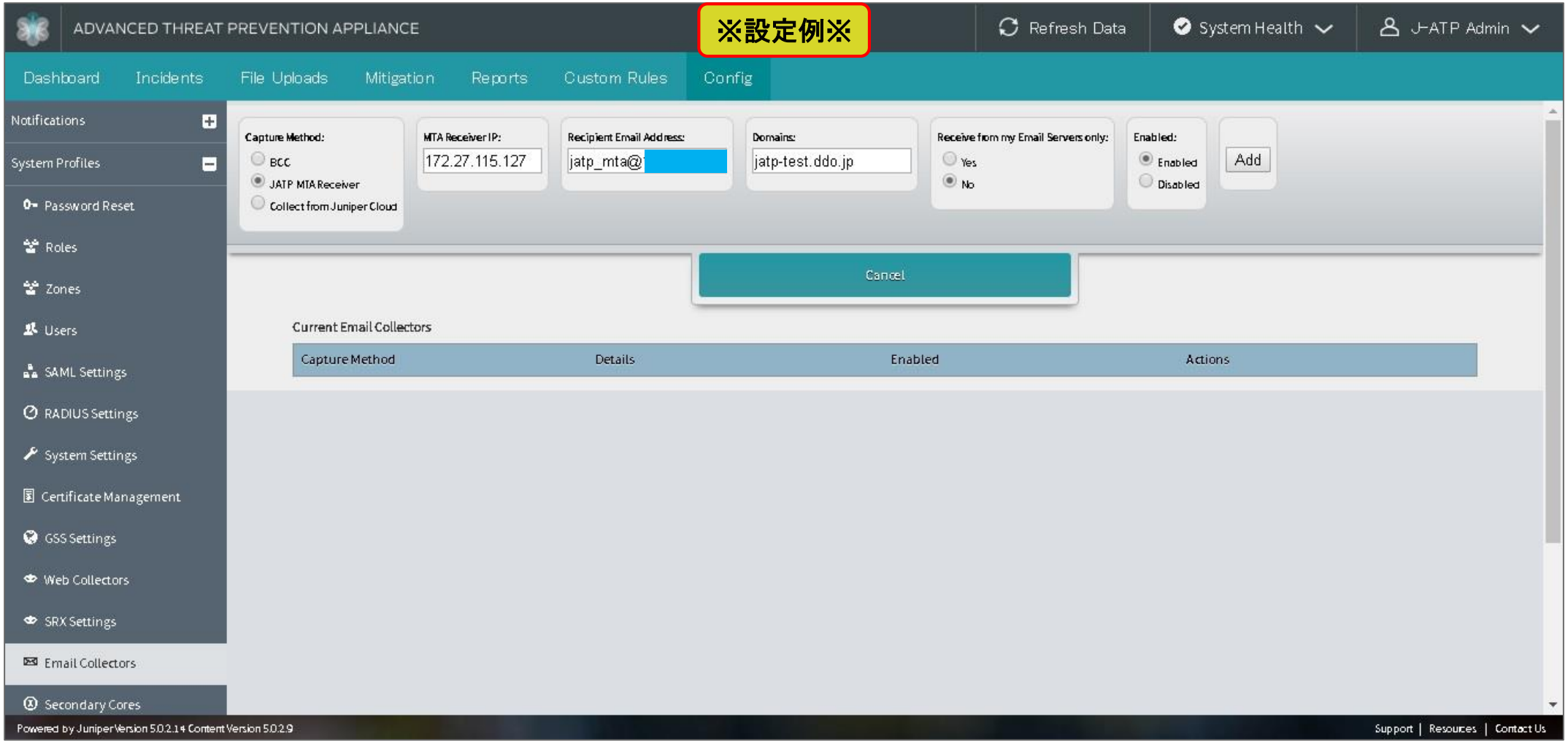
EMAIL COLLECTOR設定手順 (MTA RECEIVER)



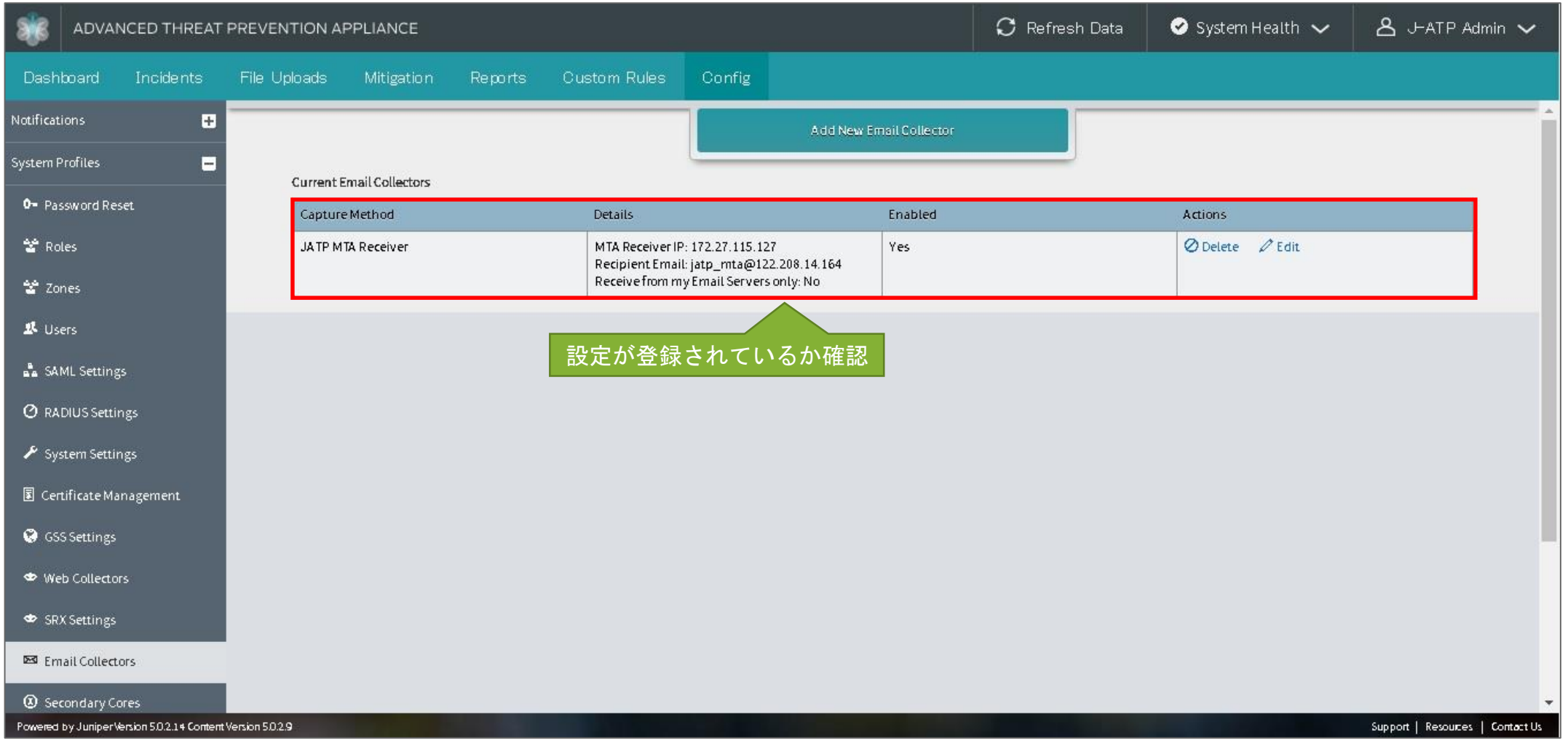
EMAIL COLLECTOR設定手順 (MTA RECEIVER)



EMAIL COLLECTOR設定手順 (MTA RECEIVER)



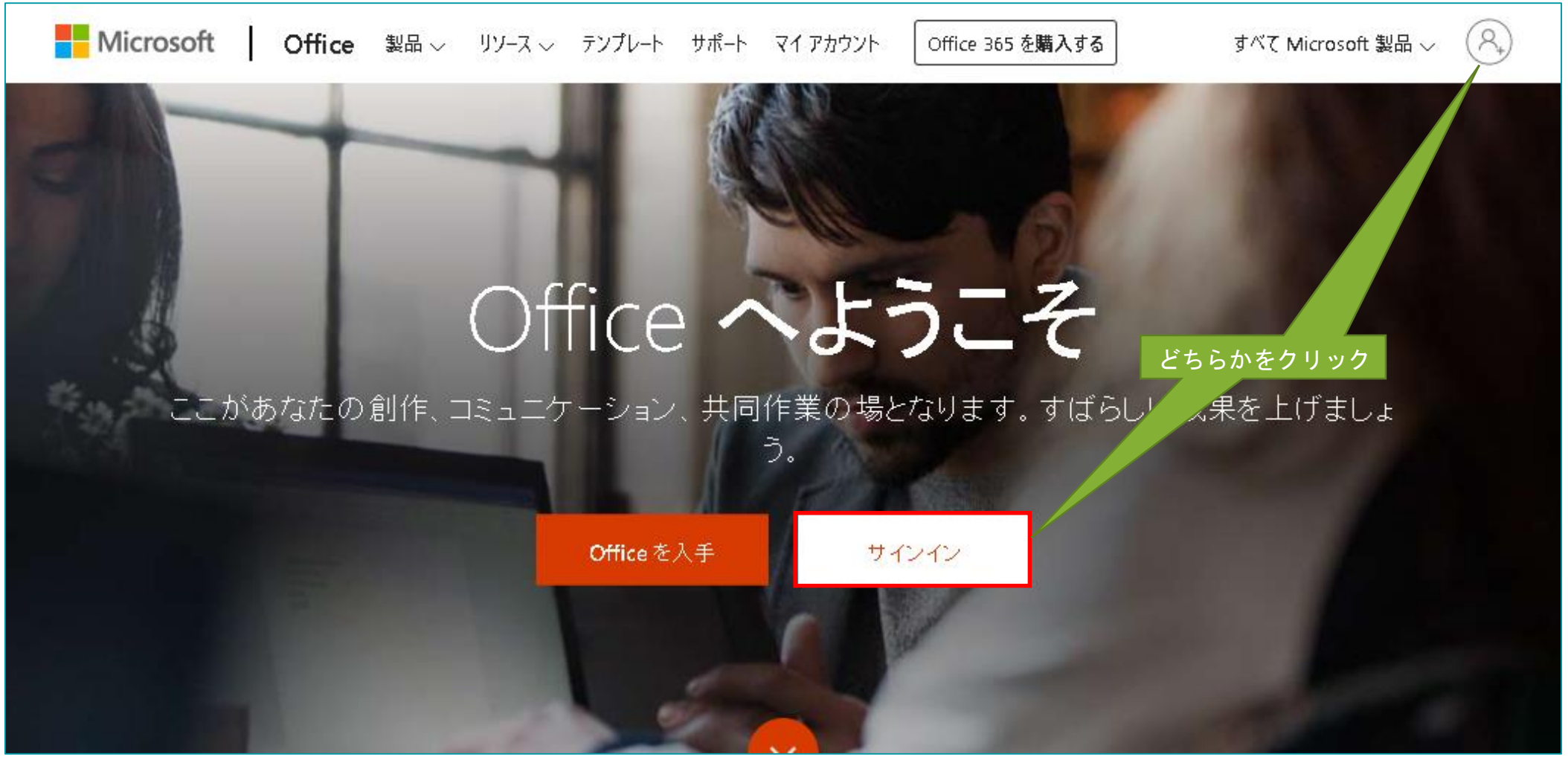
EMAIL COLLECTOR設定手順 (MTA RECEIVER)



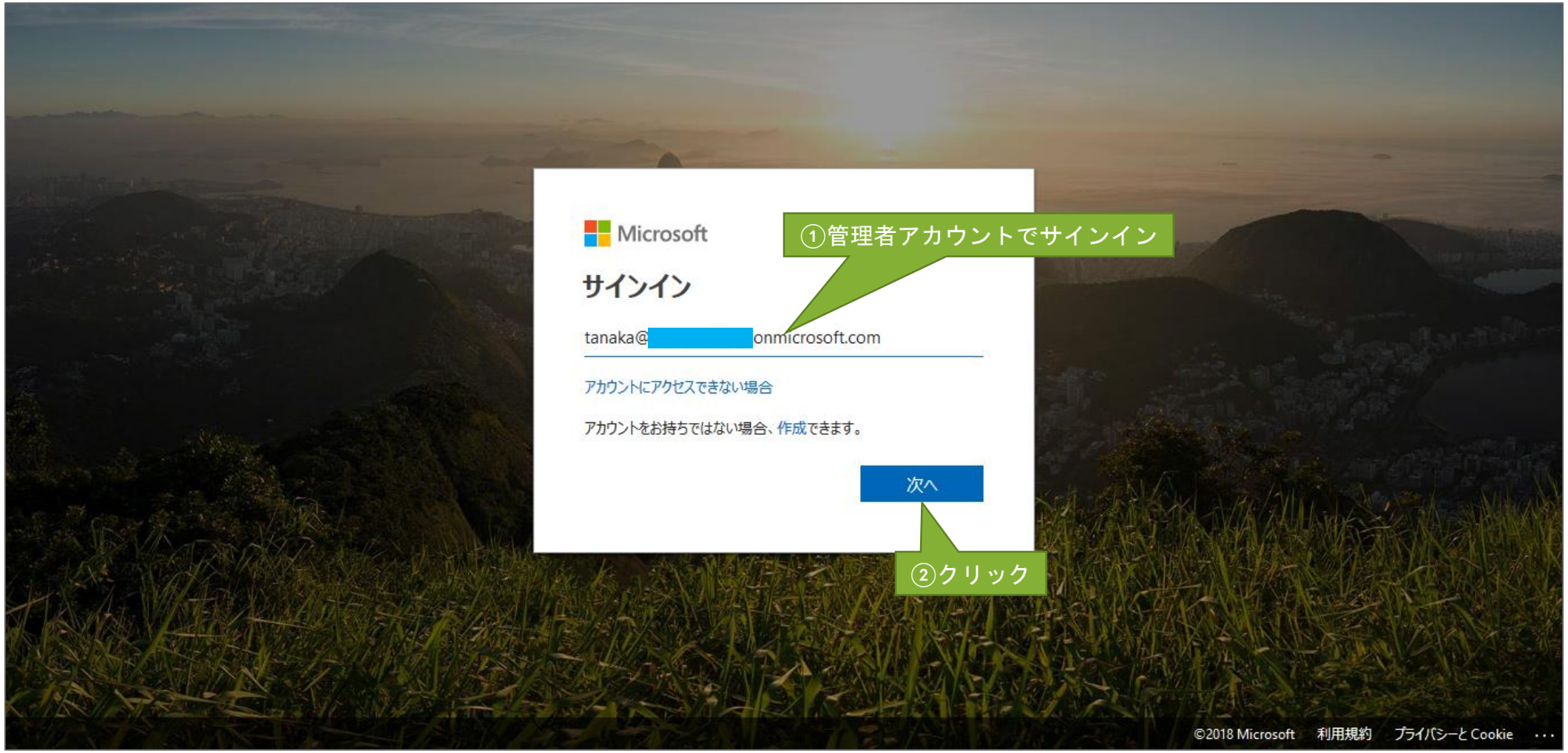
Office 365 ジャーナル設定手順 (BCC,MTA Receiver)

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

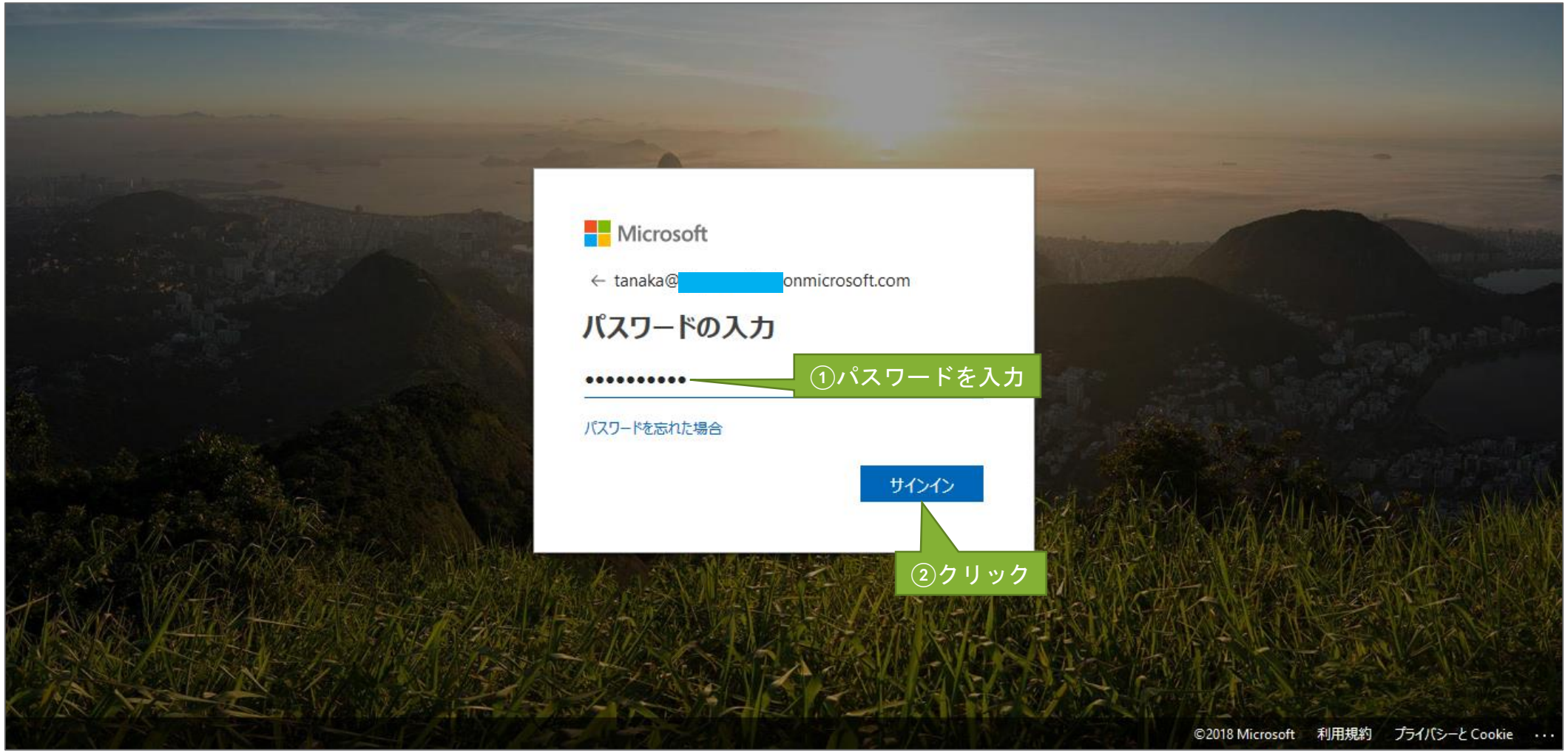
https://www.office.com/ にアクセス



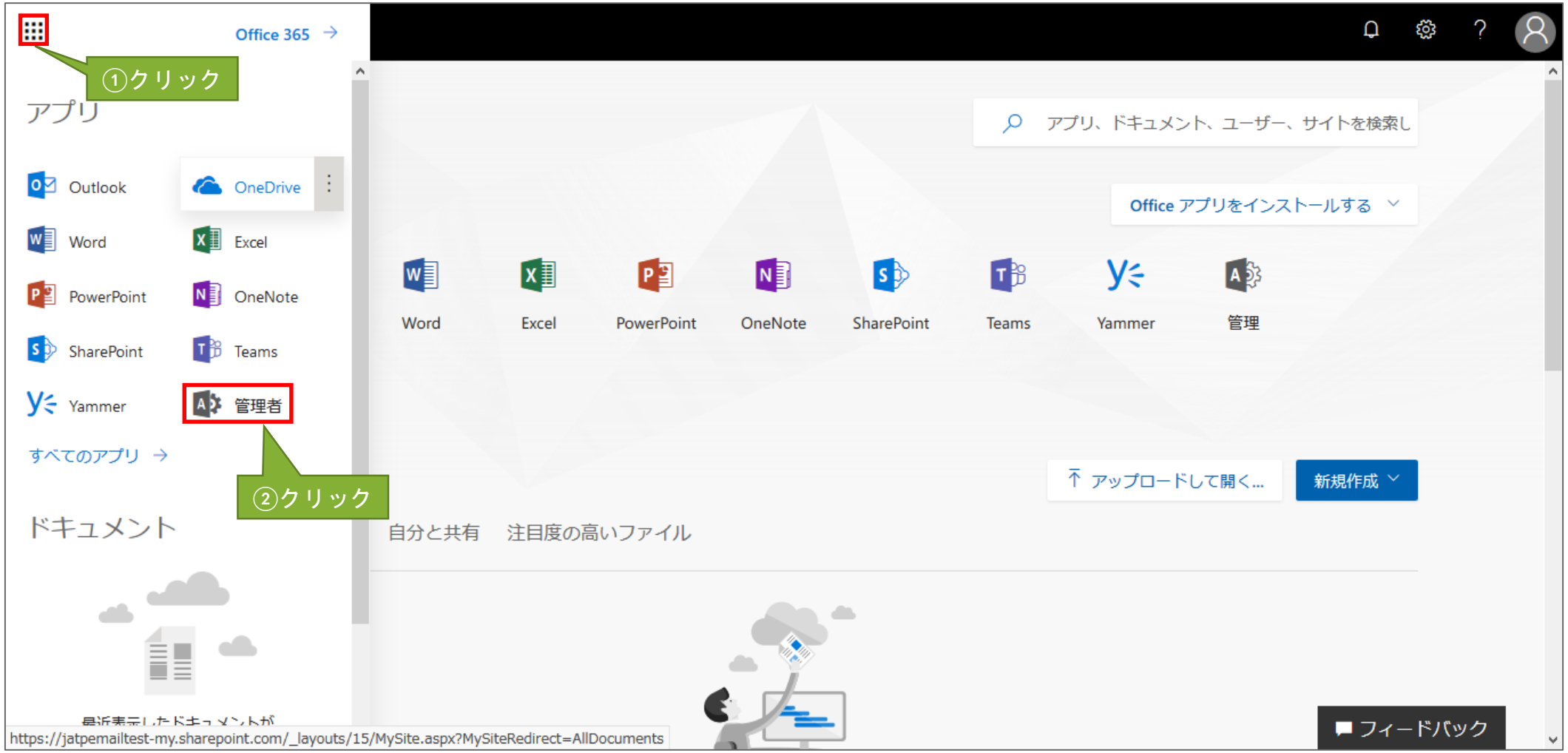
OFFICE 365 ジャーナル設定手順 (BCC,MTA RECEIVER)



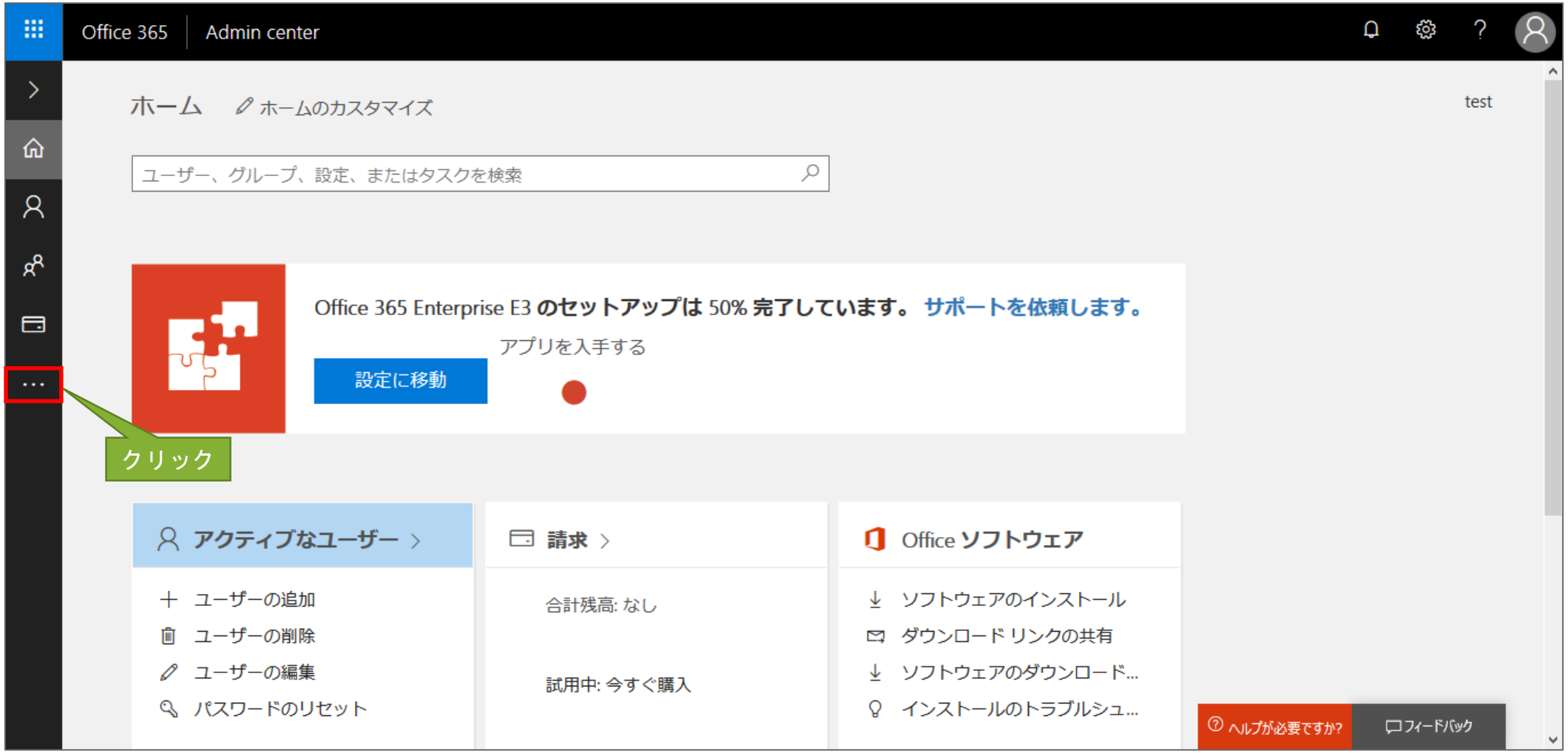
OFFICE 365 ジャーナル設定手順 (BCC,MTA RECEIVER)



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)



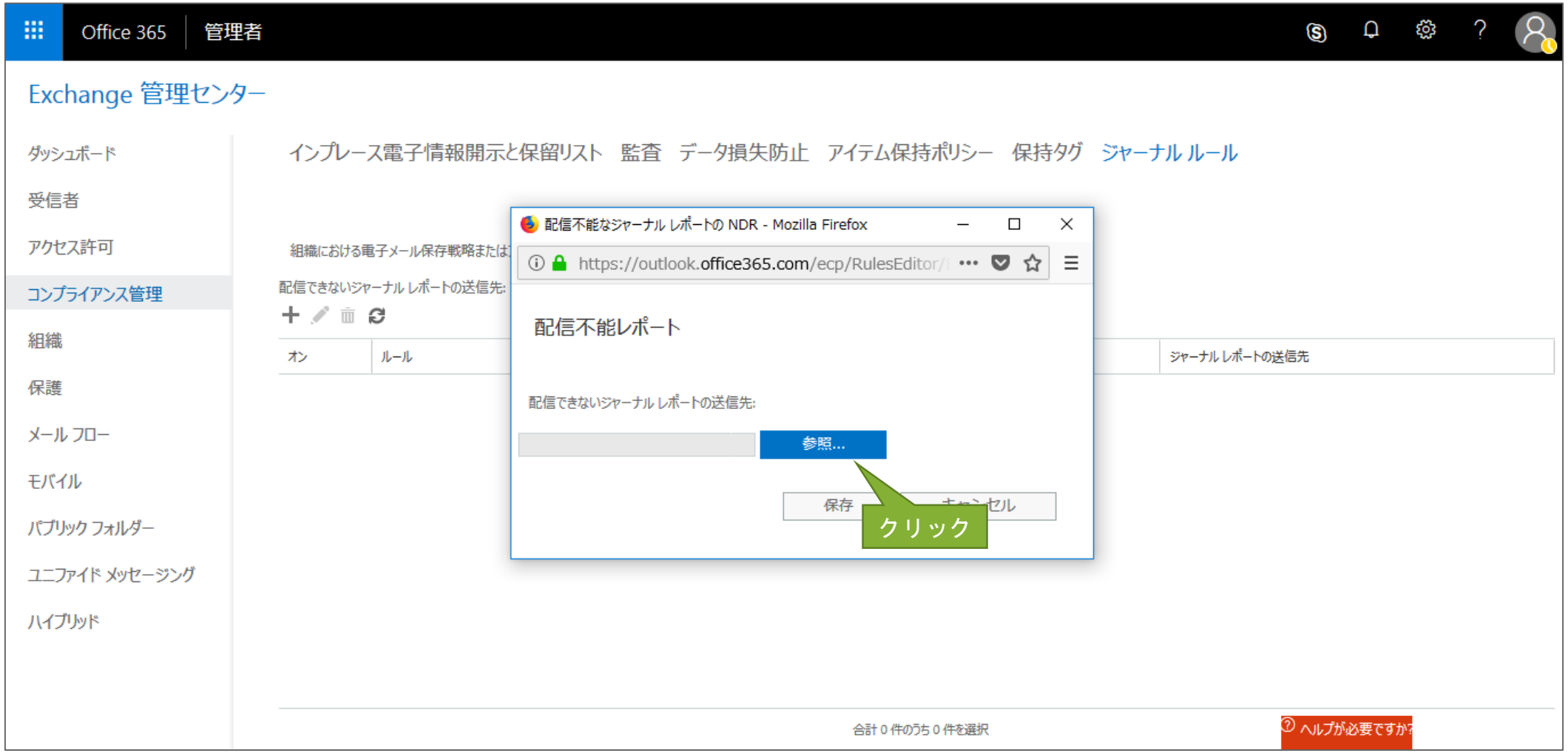
OFFICE 365 ジャーナル設定手順 (BCC,MTA RECEIVER)

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

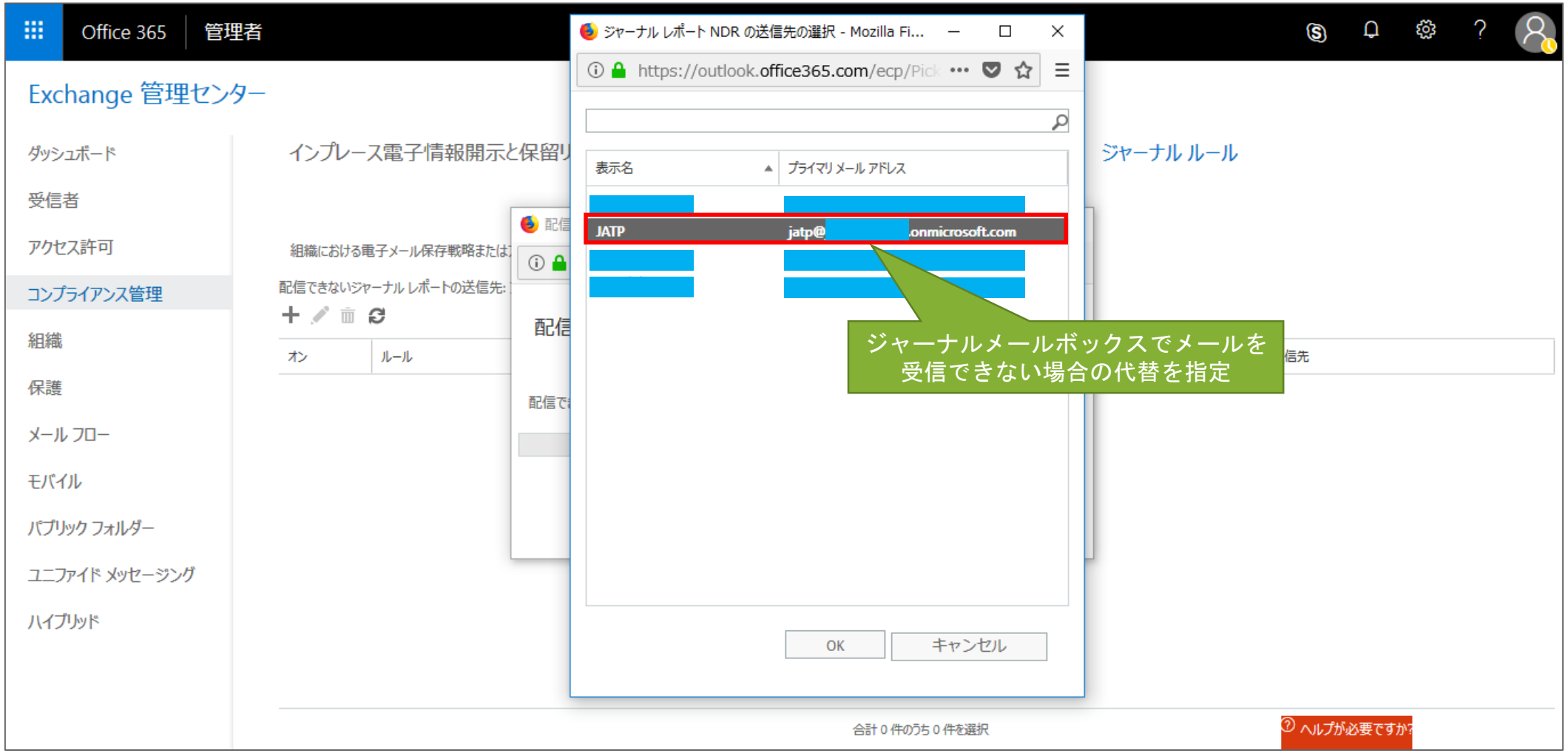
OFFICE 365 ジャーナル設定手順 (BCC,MTA RECEIVER)

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

OFFICE 365 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)

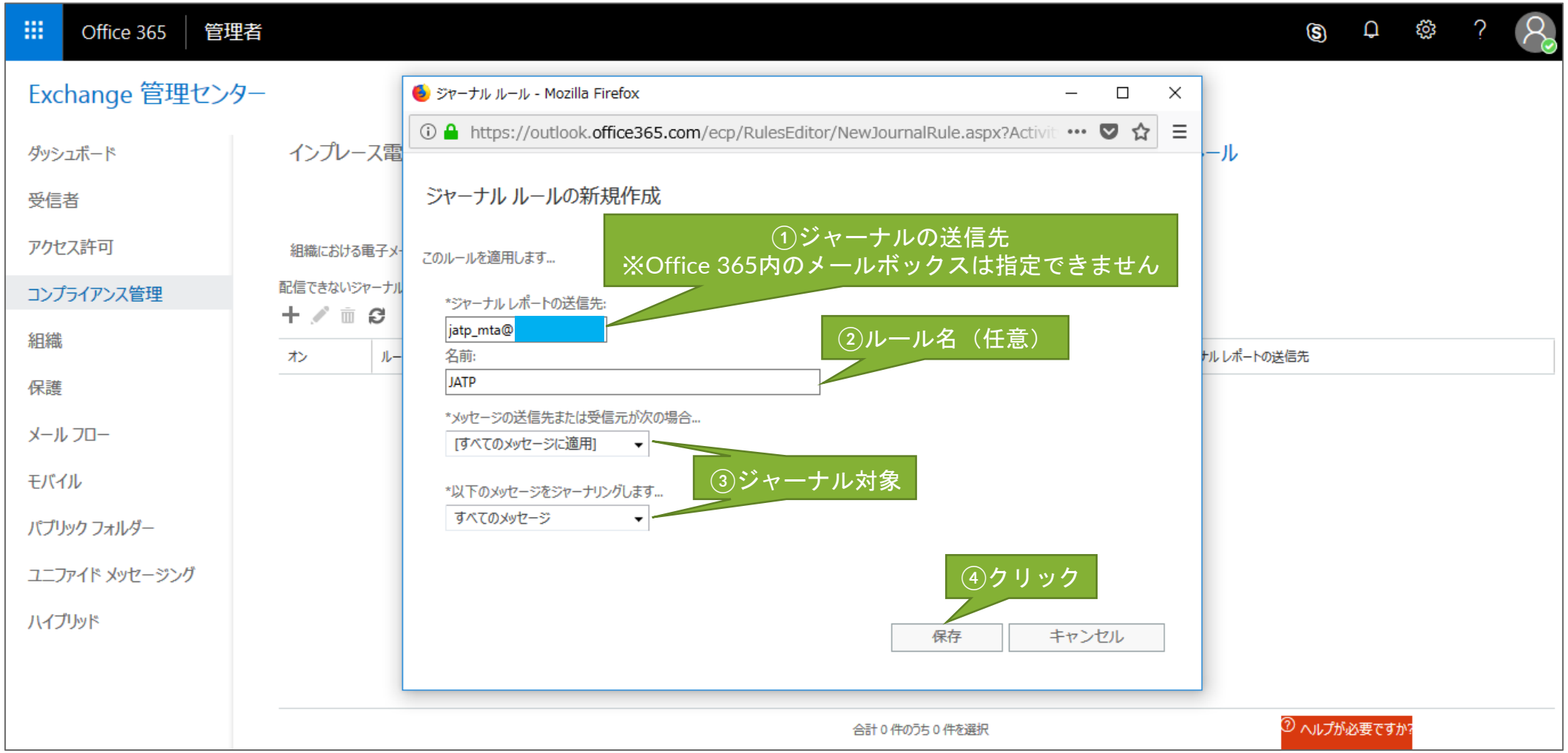


OFFICE 365 ジャーナル設定手順 (BCC,MTA RECEIVER)

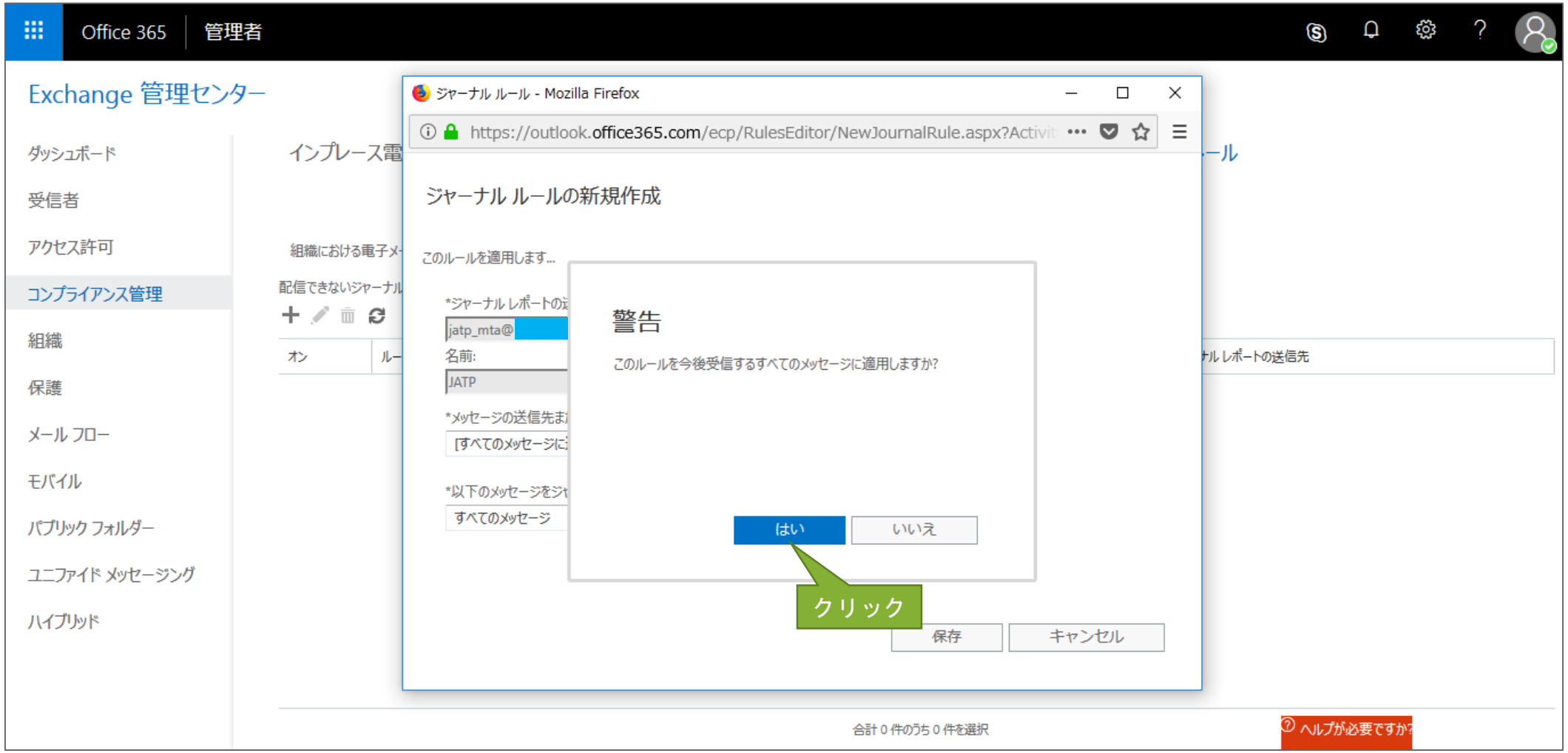
OFFICE 365 ジャーナル設定手順 (BCC,MTA RECEIVER)

OFFICE 365 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)

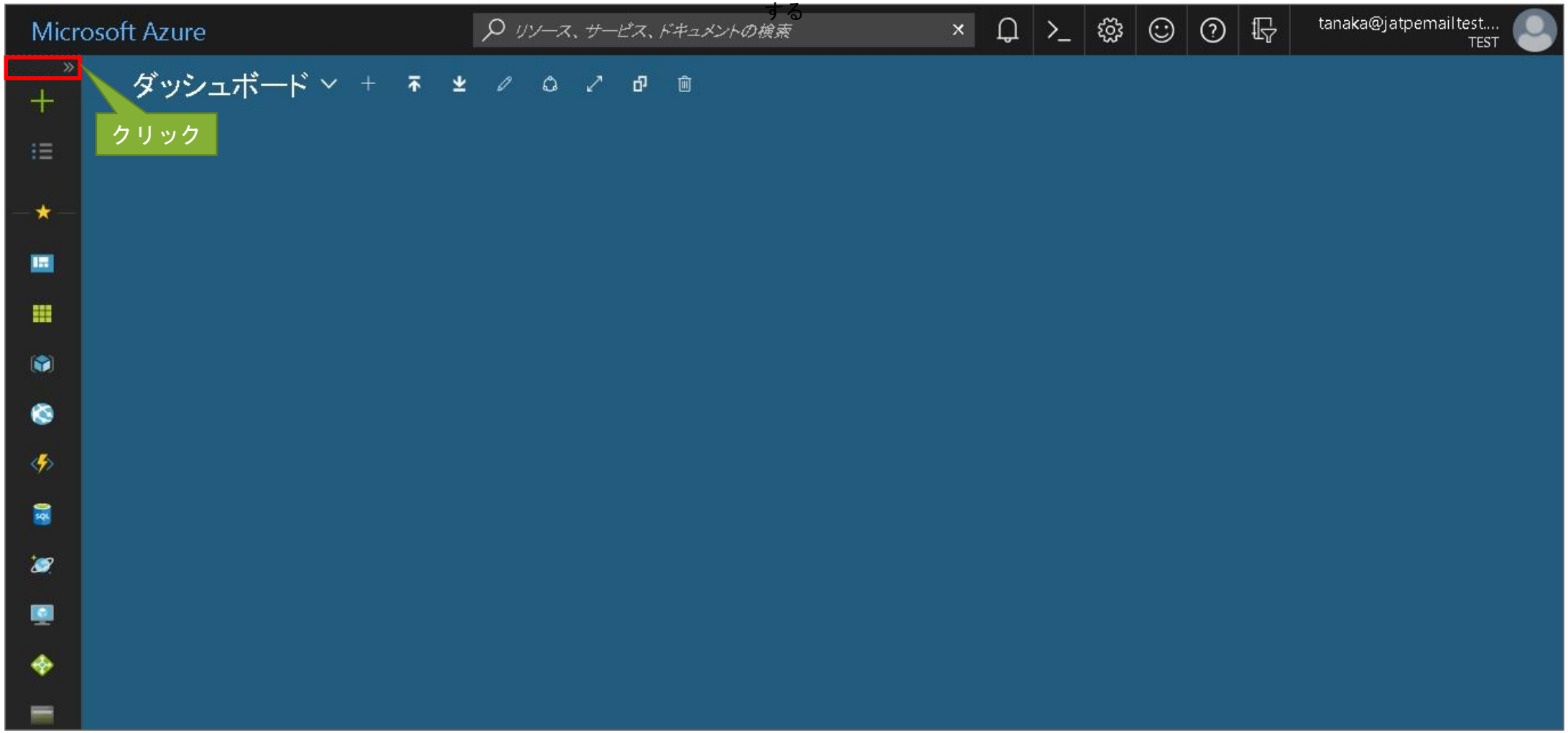


OFFICE 365 ジャーナル設定手順 (BCC,MTA RECEIVER)

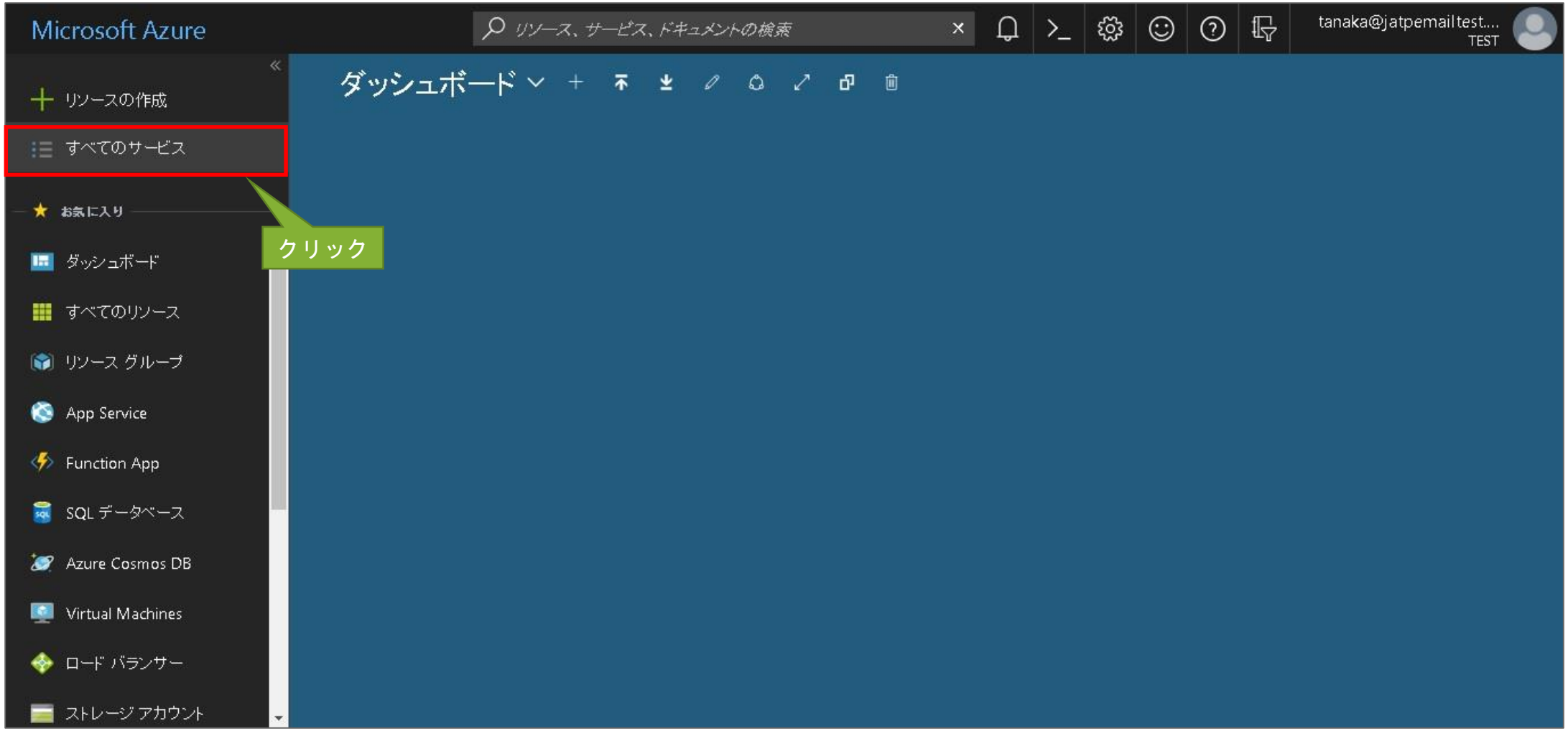
Office 365 Mitigation設定手順 (BCC,MTA Receiver)

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

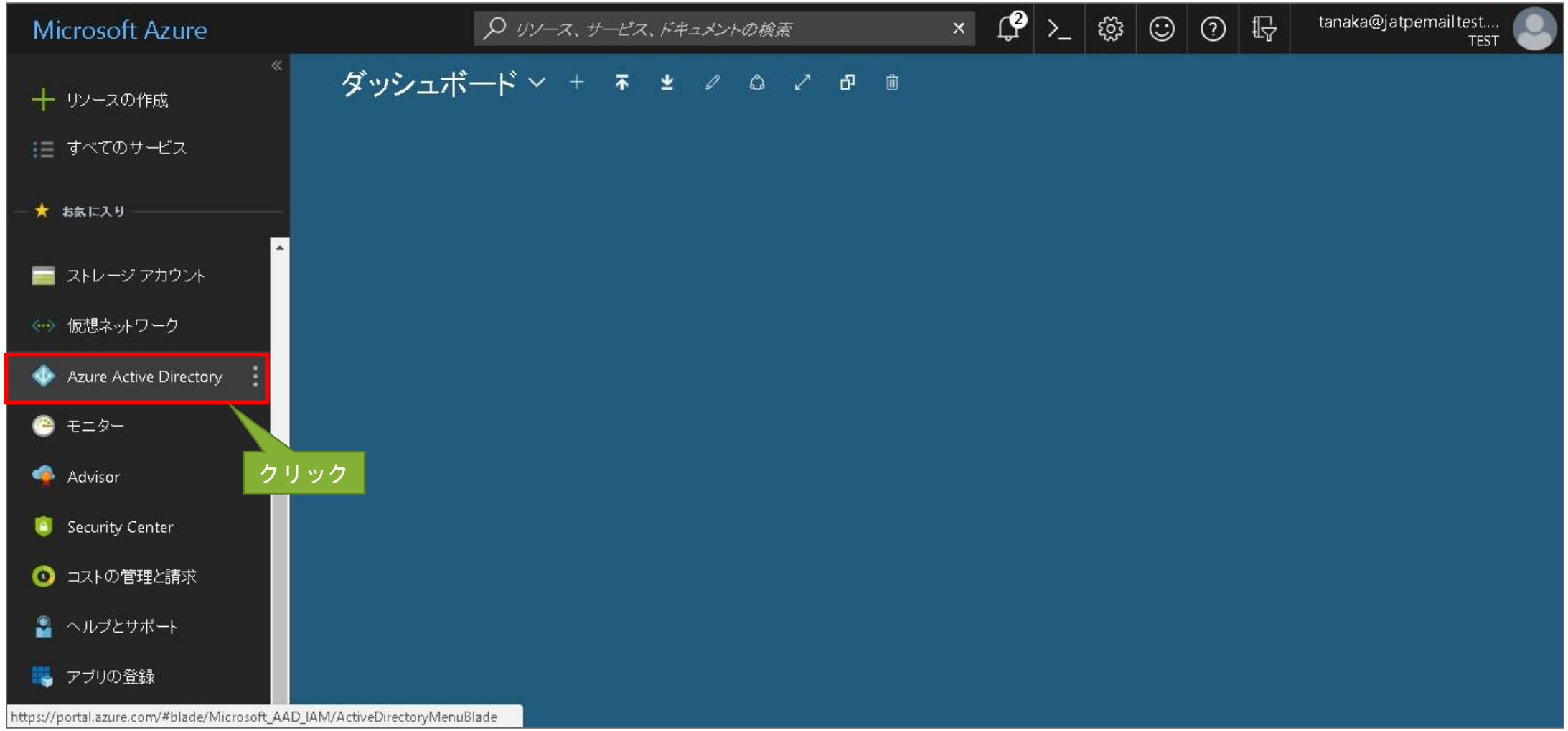
Azureポータル(https://www.office.com/) へアクセスして**管理者アカウント**でログインする



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

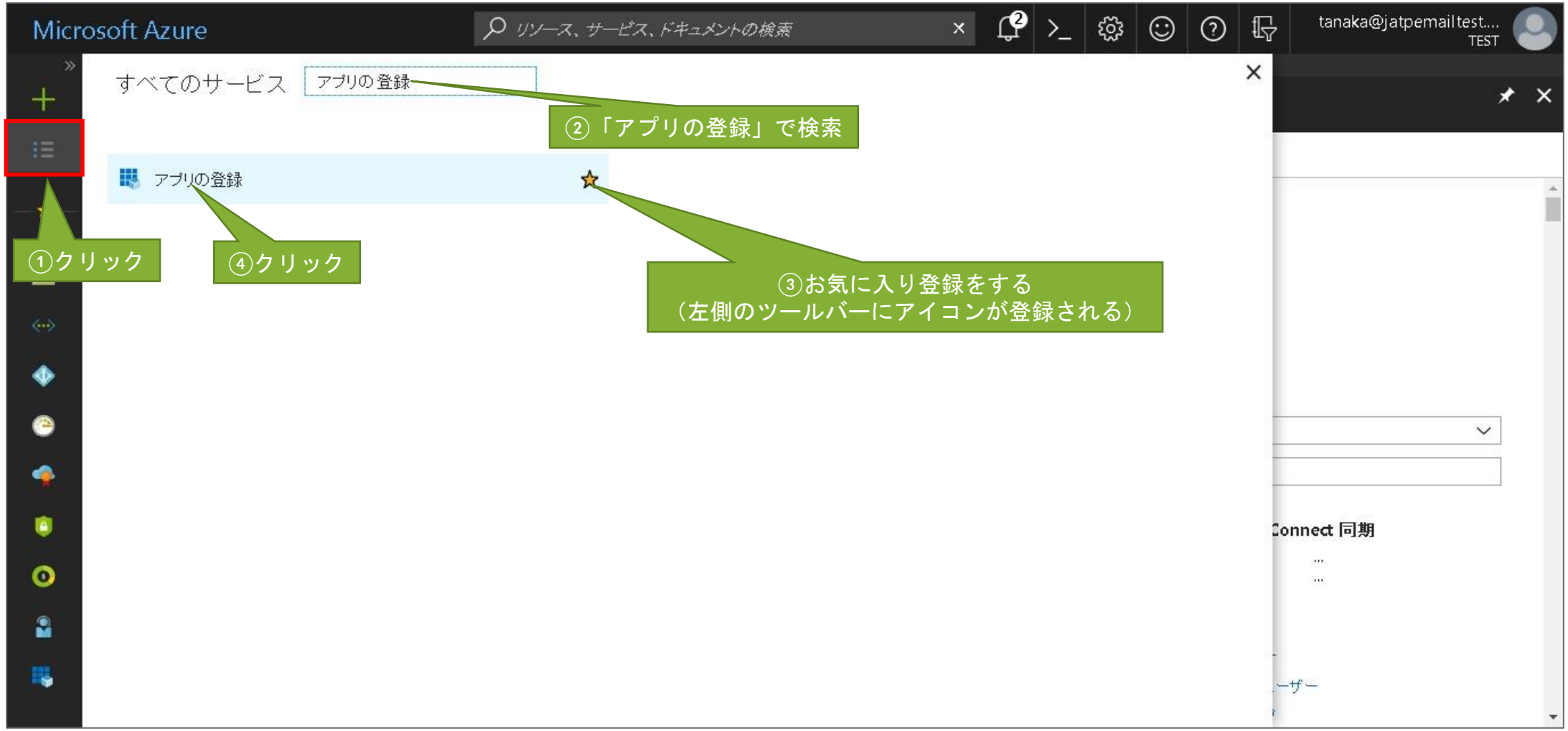


OFFICE 365 MITIGATION設定手順 (BCC,MTA RECEIVER)



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

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

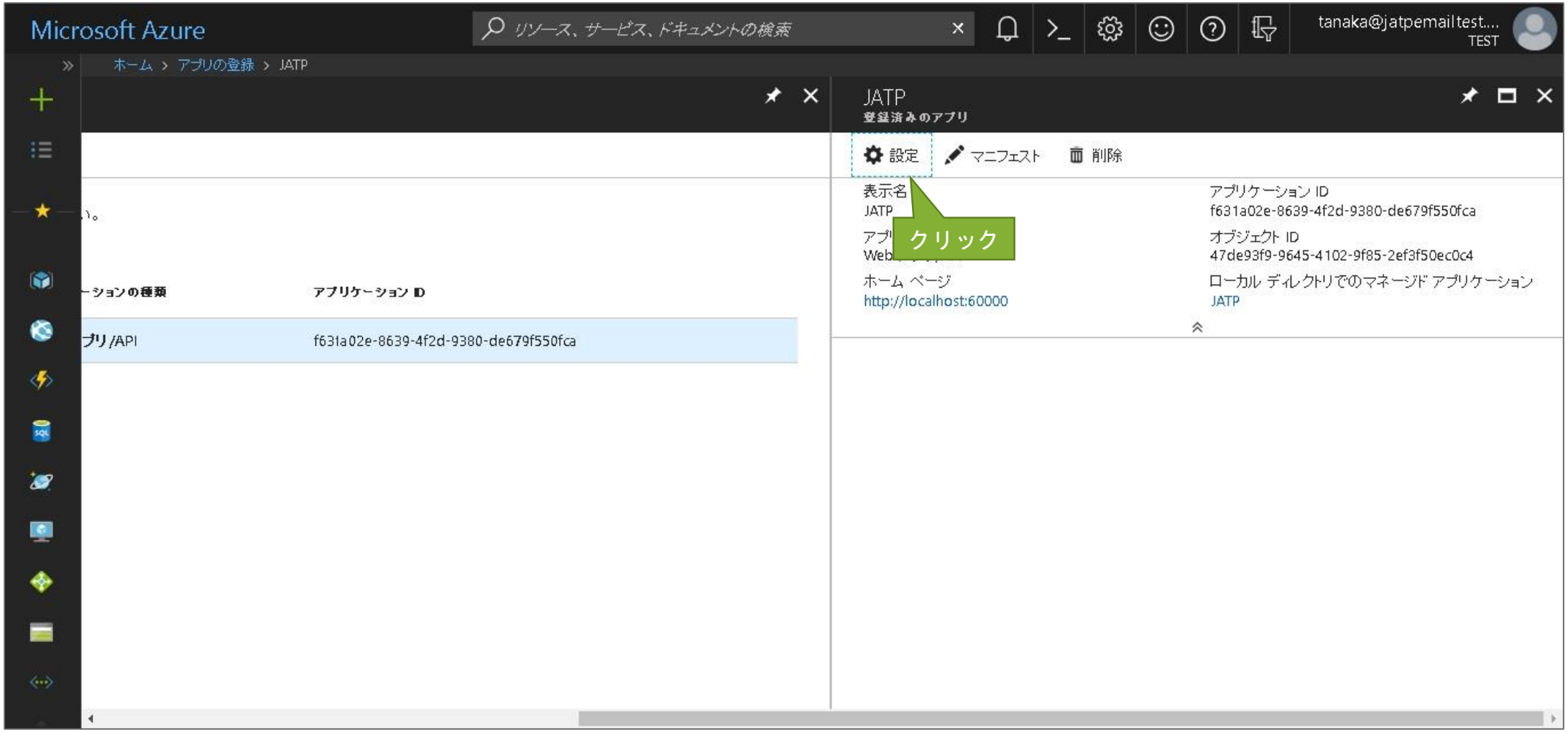


OFFICE 365 MITIGATION設定手順 (BCC,MTA RECEIVER)

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

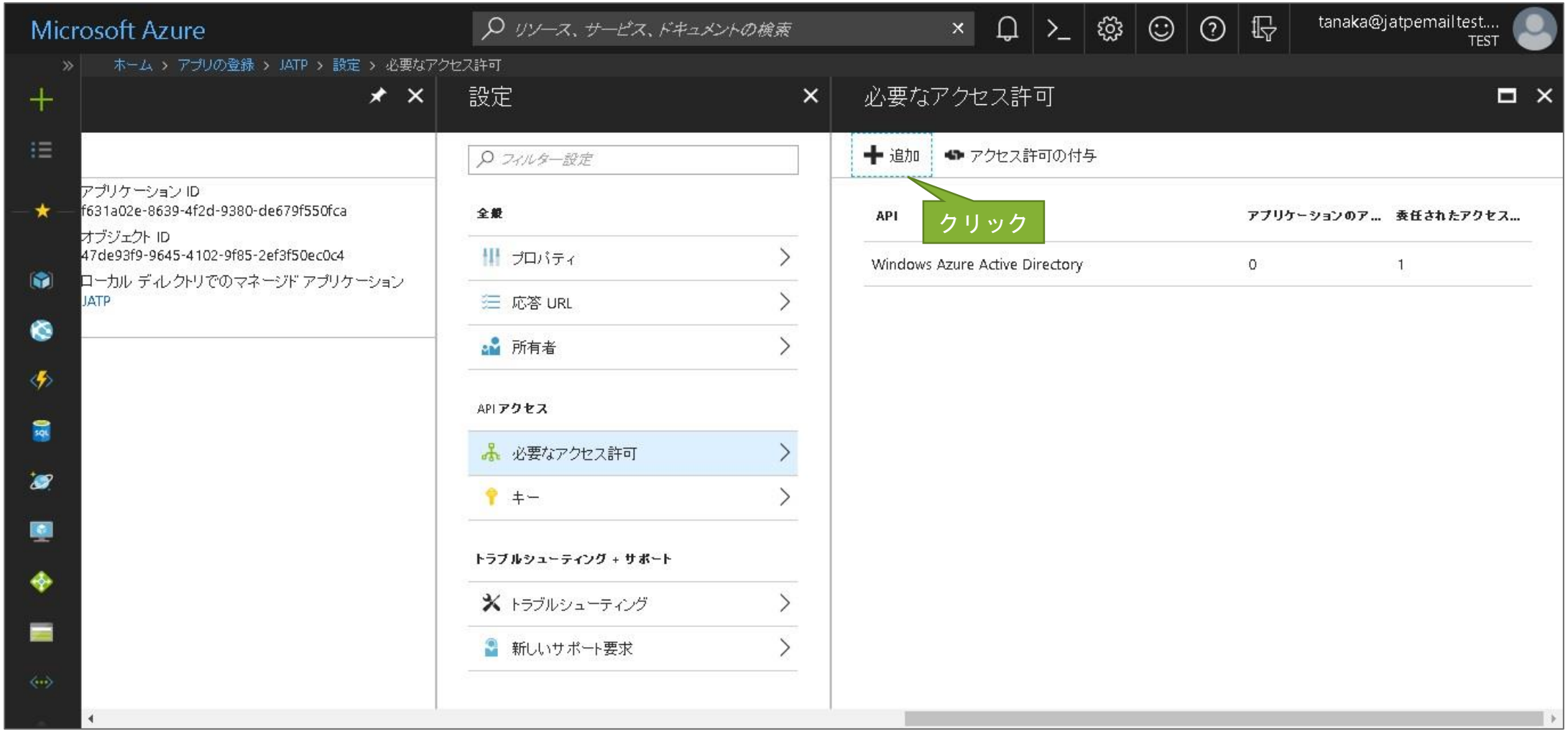
OFFICE 365 MITIGATION設定手順 (BCC,MTA RECEIVER)

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

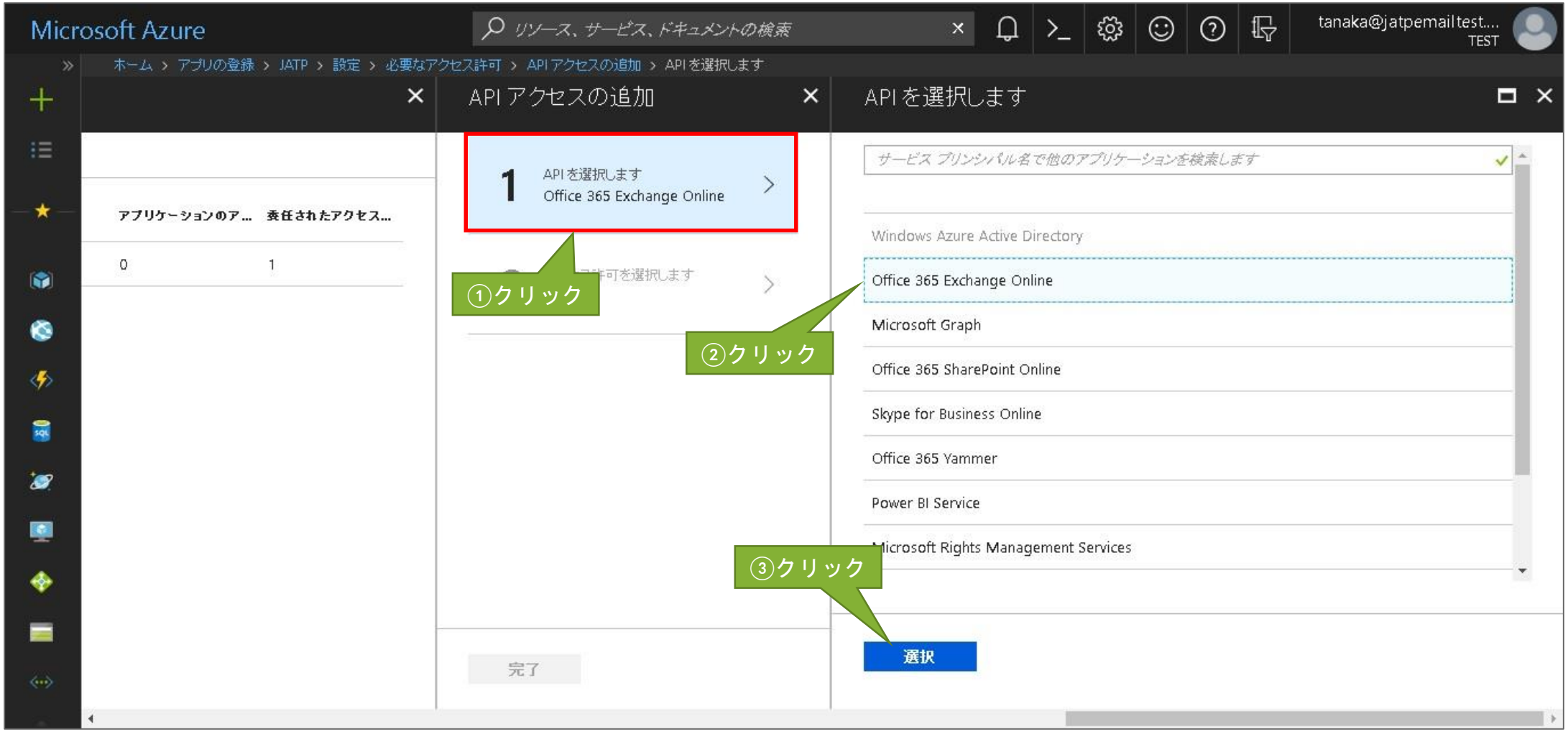


OFFICE 365 MITIGATION設定手順 (BCC,MTA RECEIVER)

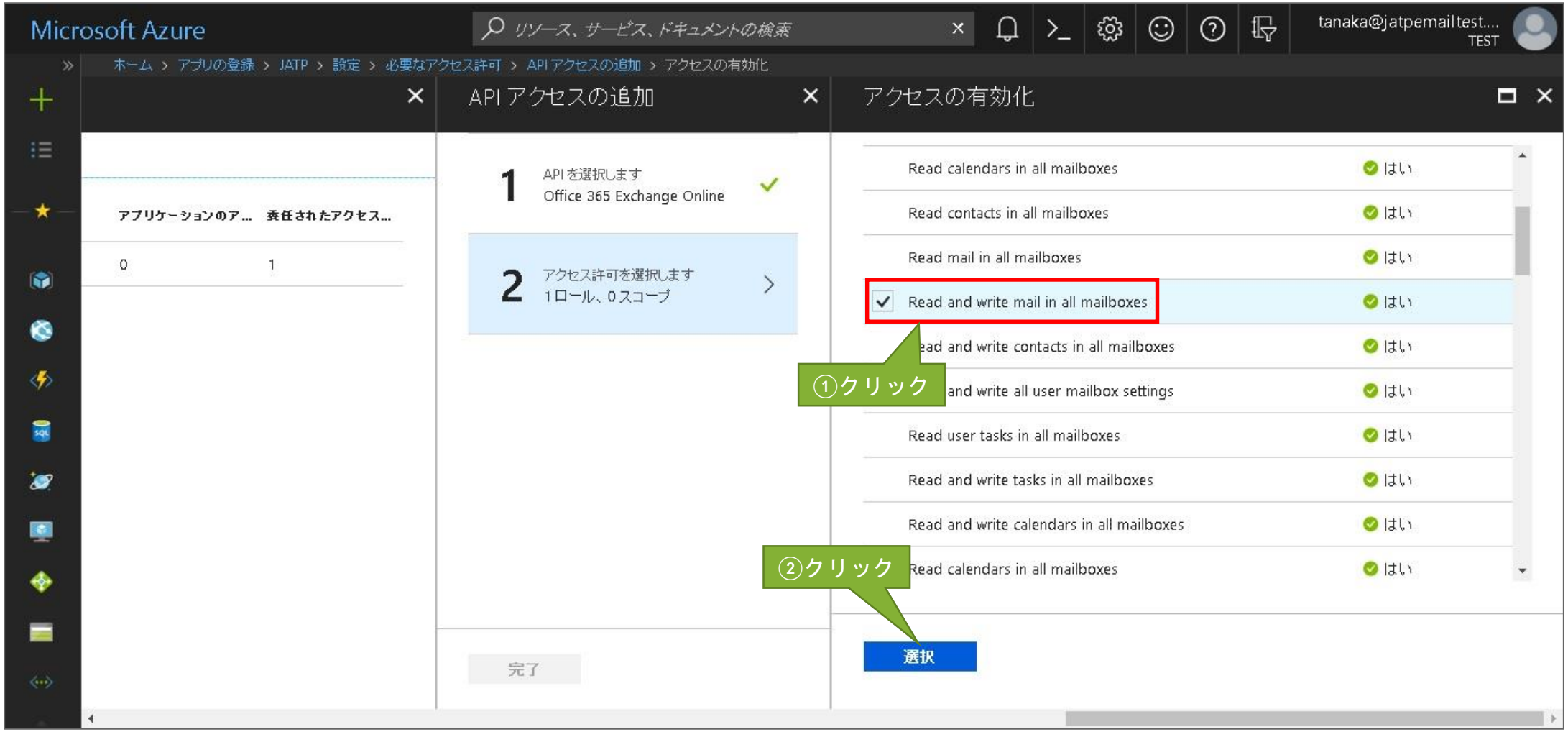
OFFICE 365 MITIGATION設定手順 (BCC,MTA RECEIVER)



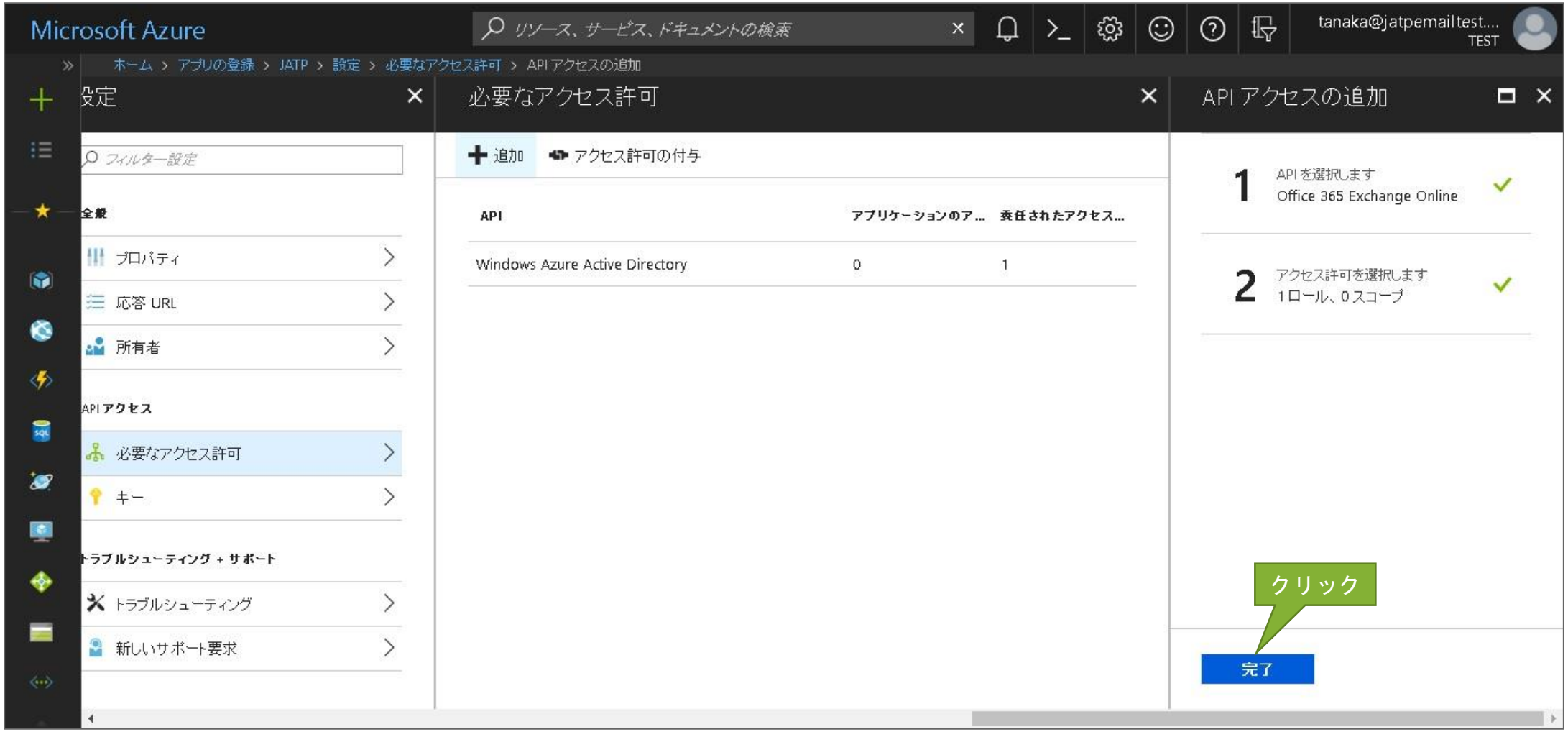
OFFICE 365 MITIGATION設定手順 (BCC,MTA RECEIVER)



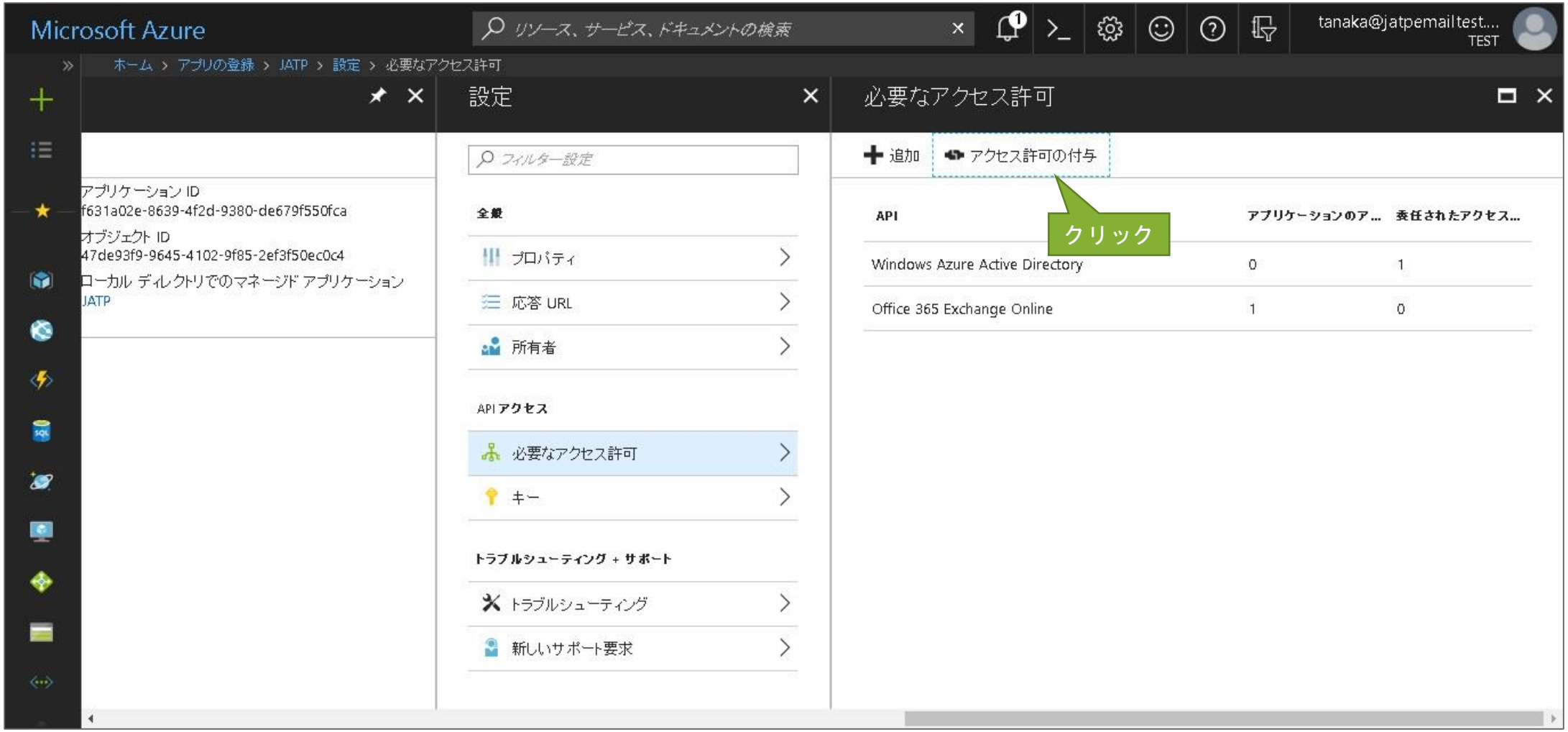
OFFICE 365 MITIGATION設定手順 (BCC,MTA RECEIVER)



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

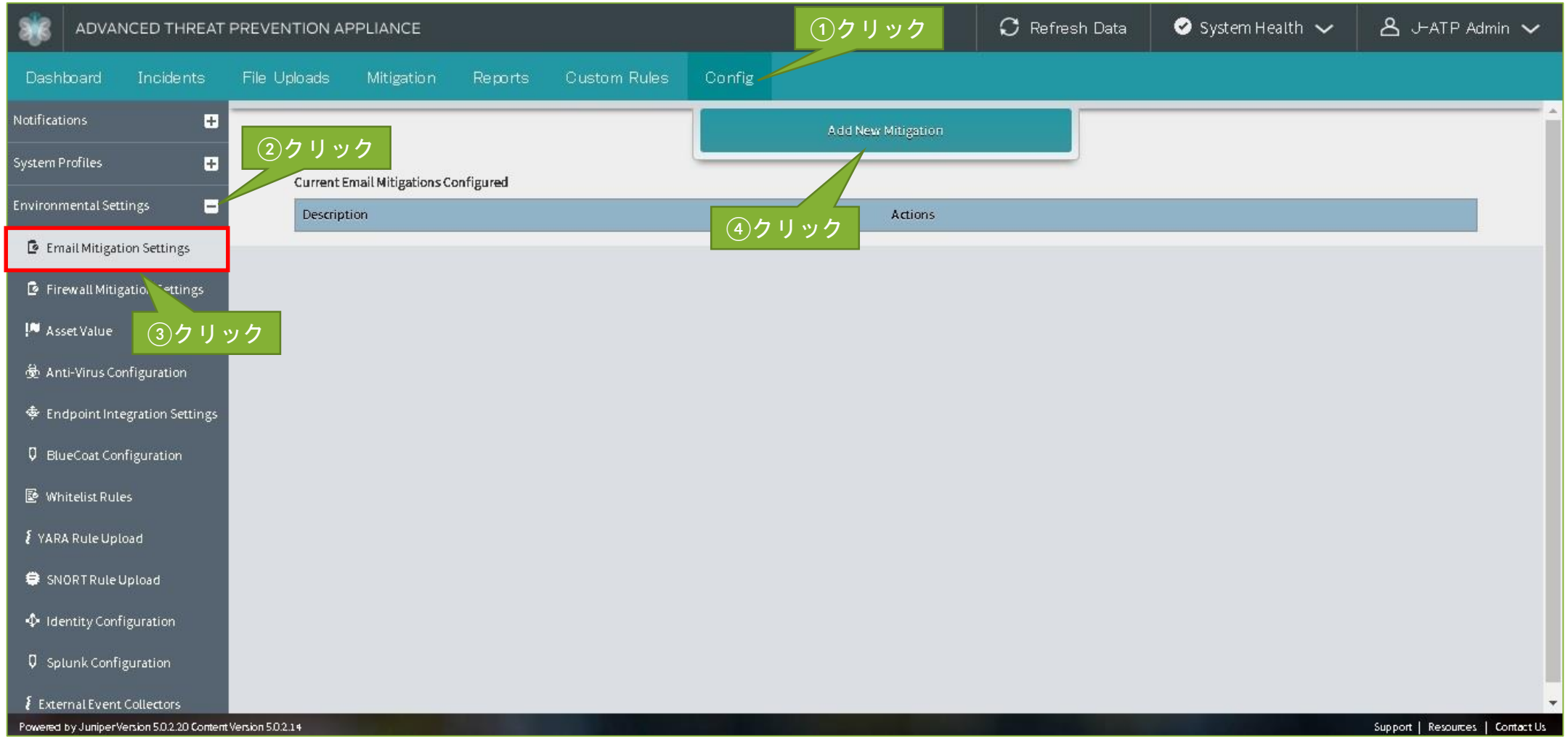


OFFICE 365 MITIGATION設定手順 (BCC,MTA RECEIVER)

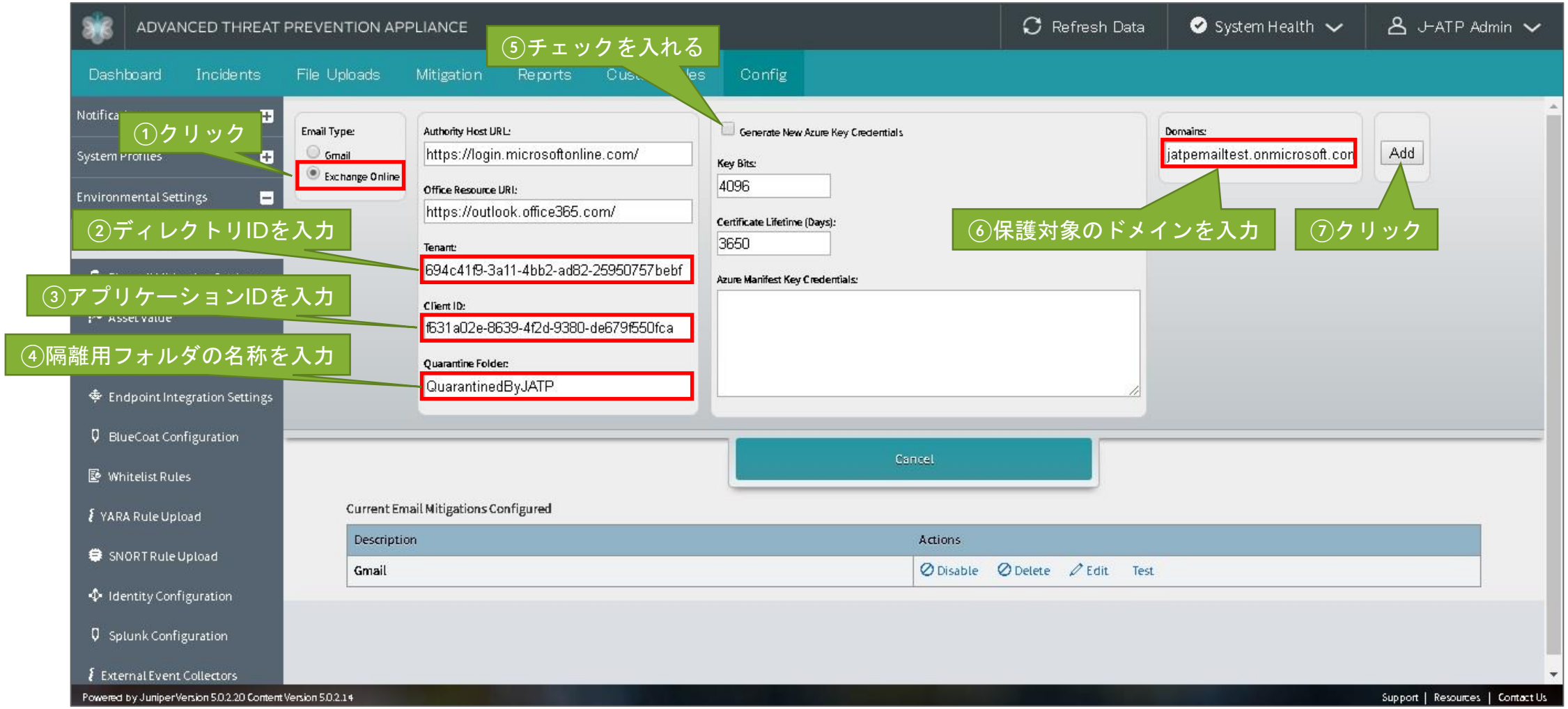


OFFICE 365 MITIGATION設定手順 (BCC,MTA RECEIVER)

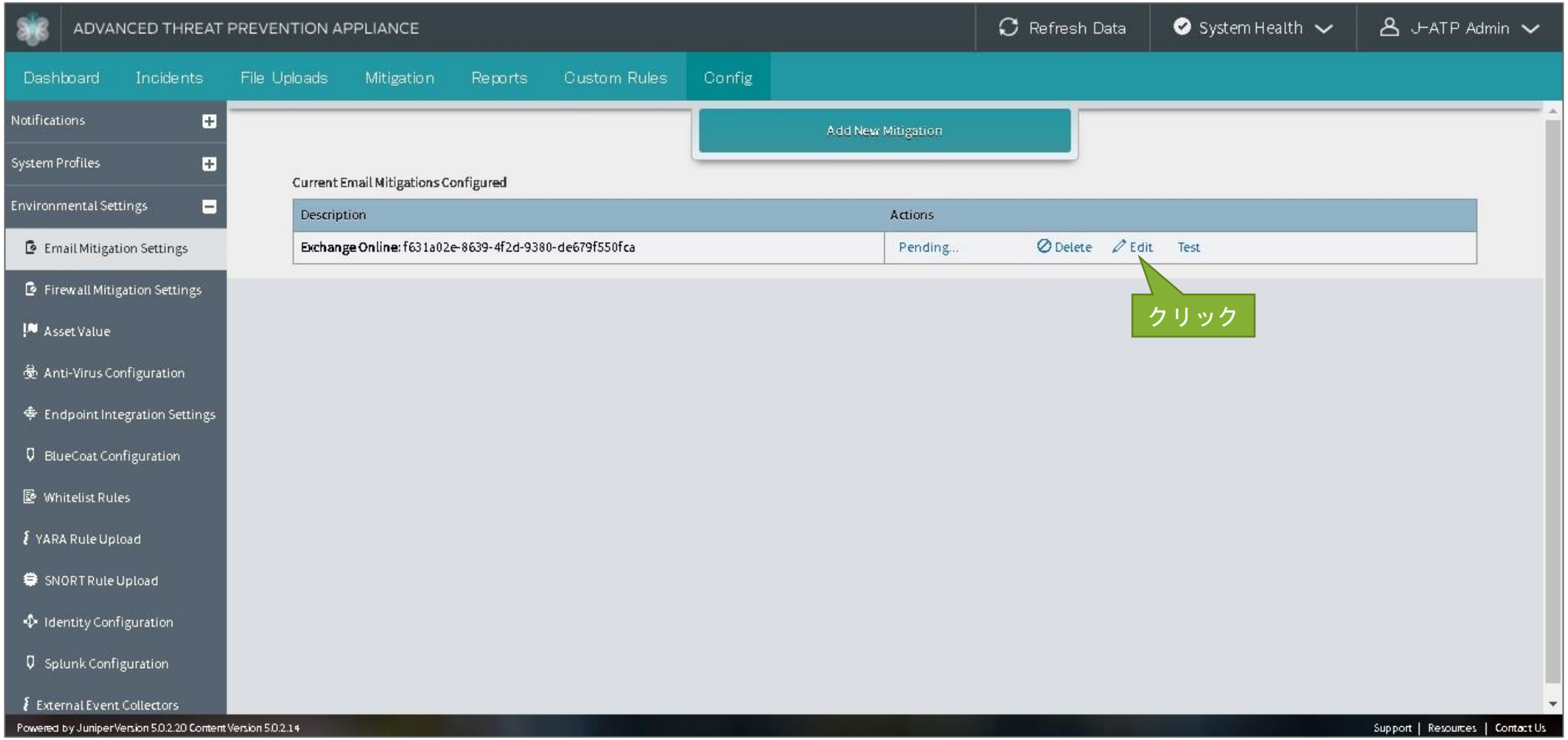
OFFICE 365 MITIGATION設定手順 (BCC,MTA RECEIVER)



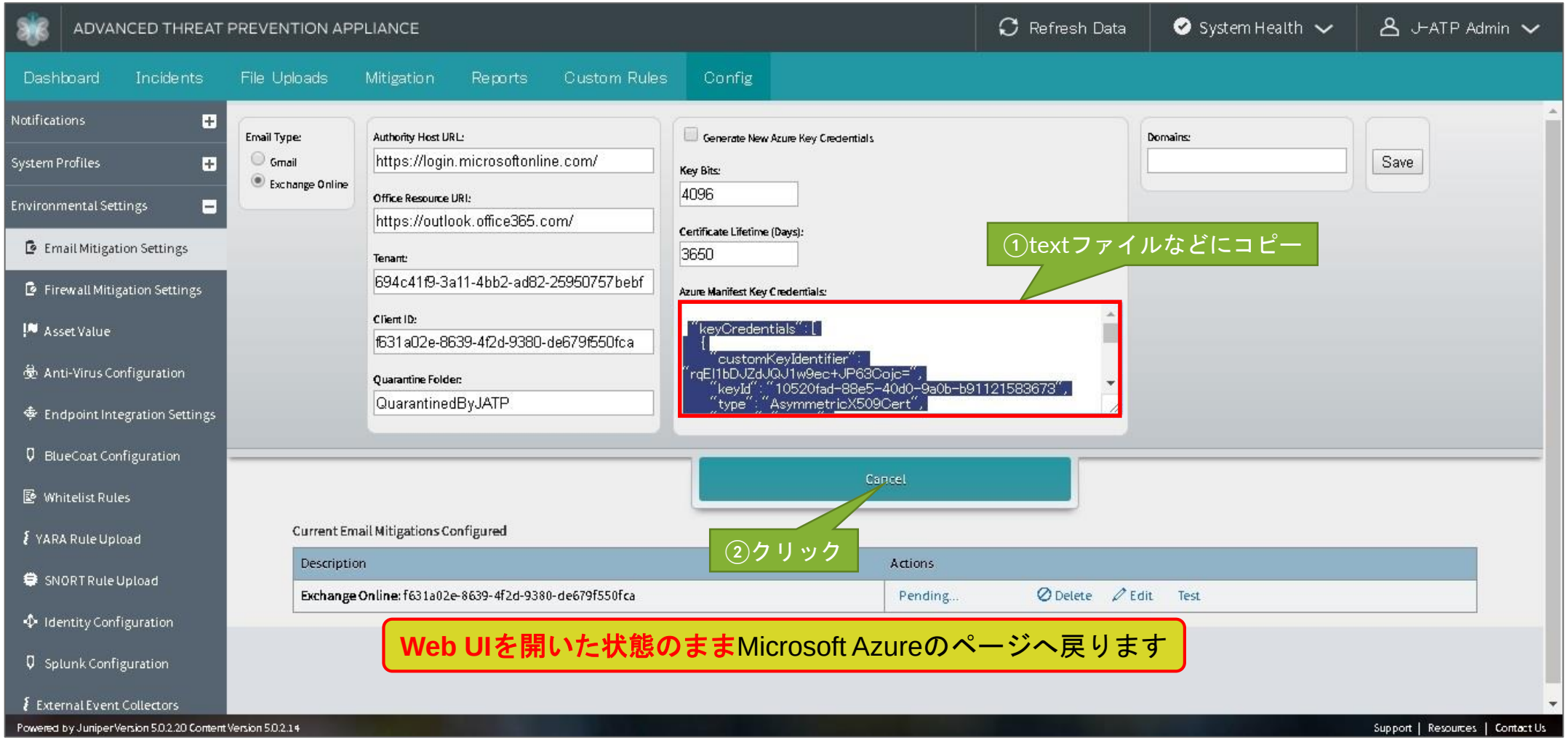
OFFICE 365 MITIGATION設定手順 (BCC,MTA RECEIVER)



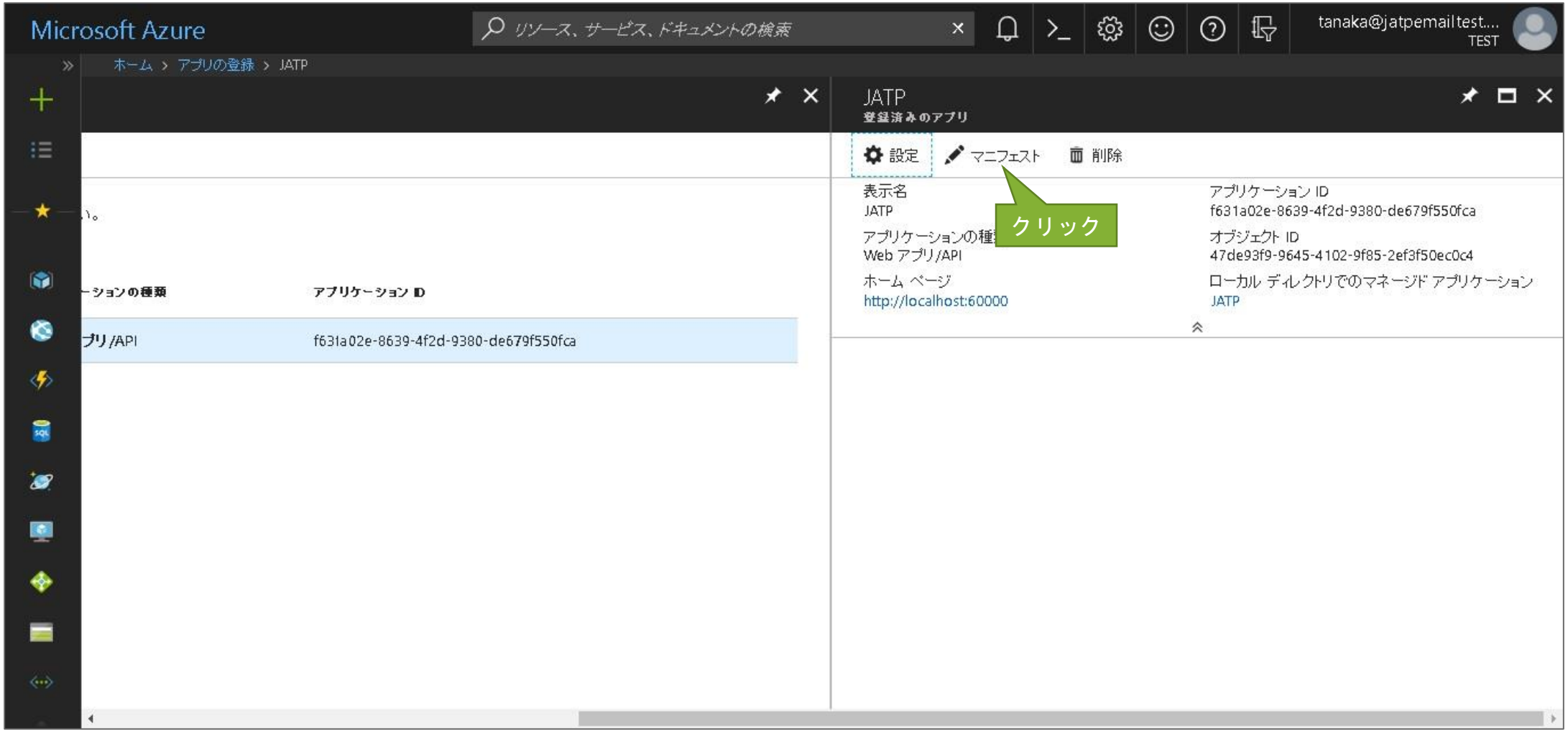
OFFICE 365 MITIGATION設定手順 (BCC,MTA RECEIVER)



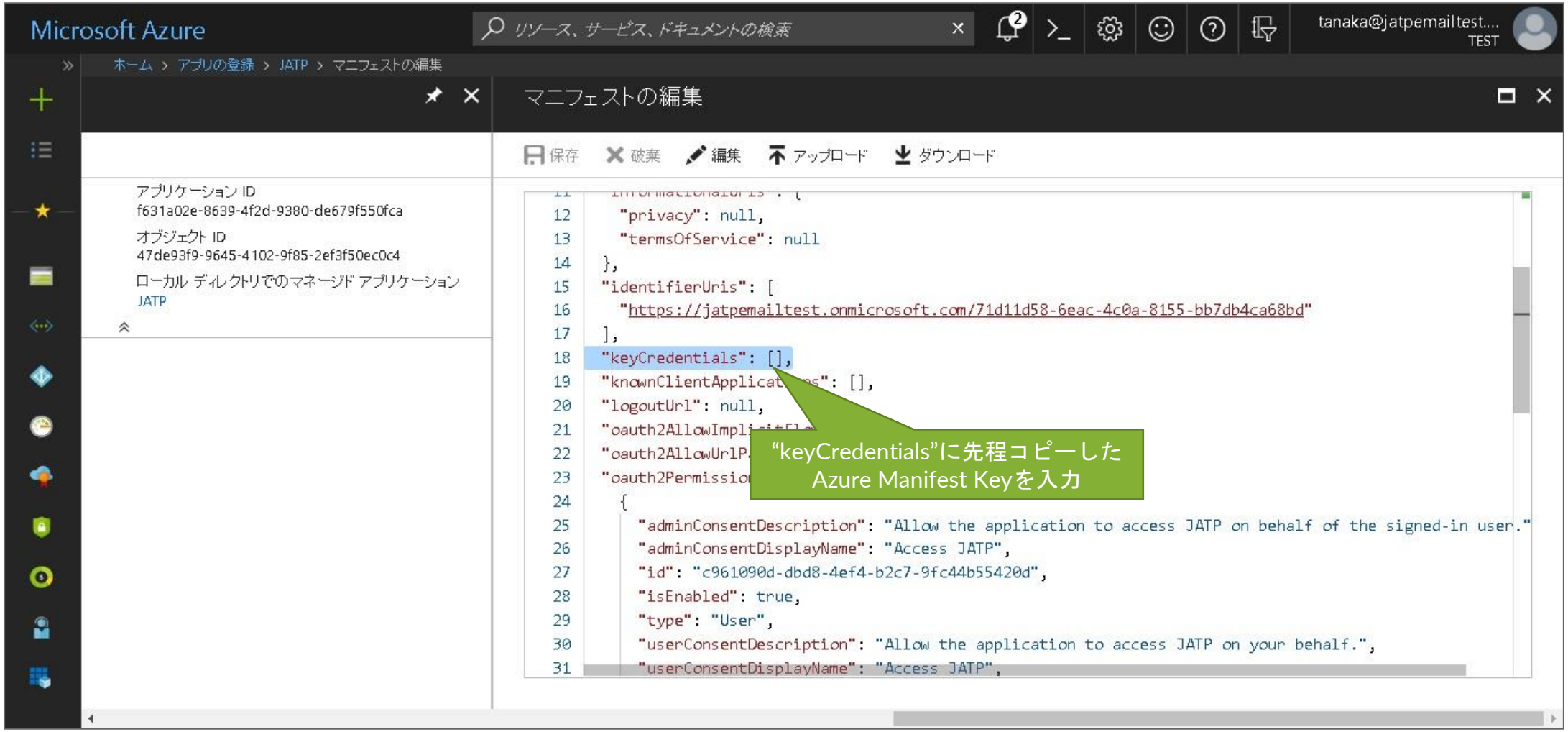
OFFICE 365 MITIGATION設定手順 (BCC,MTA RECEIVER)



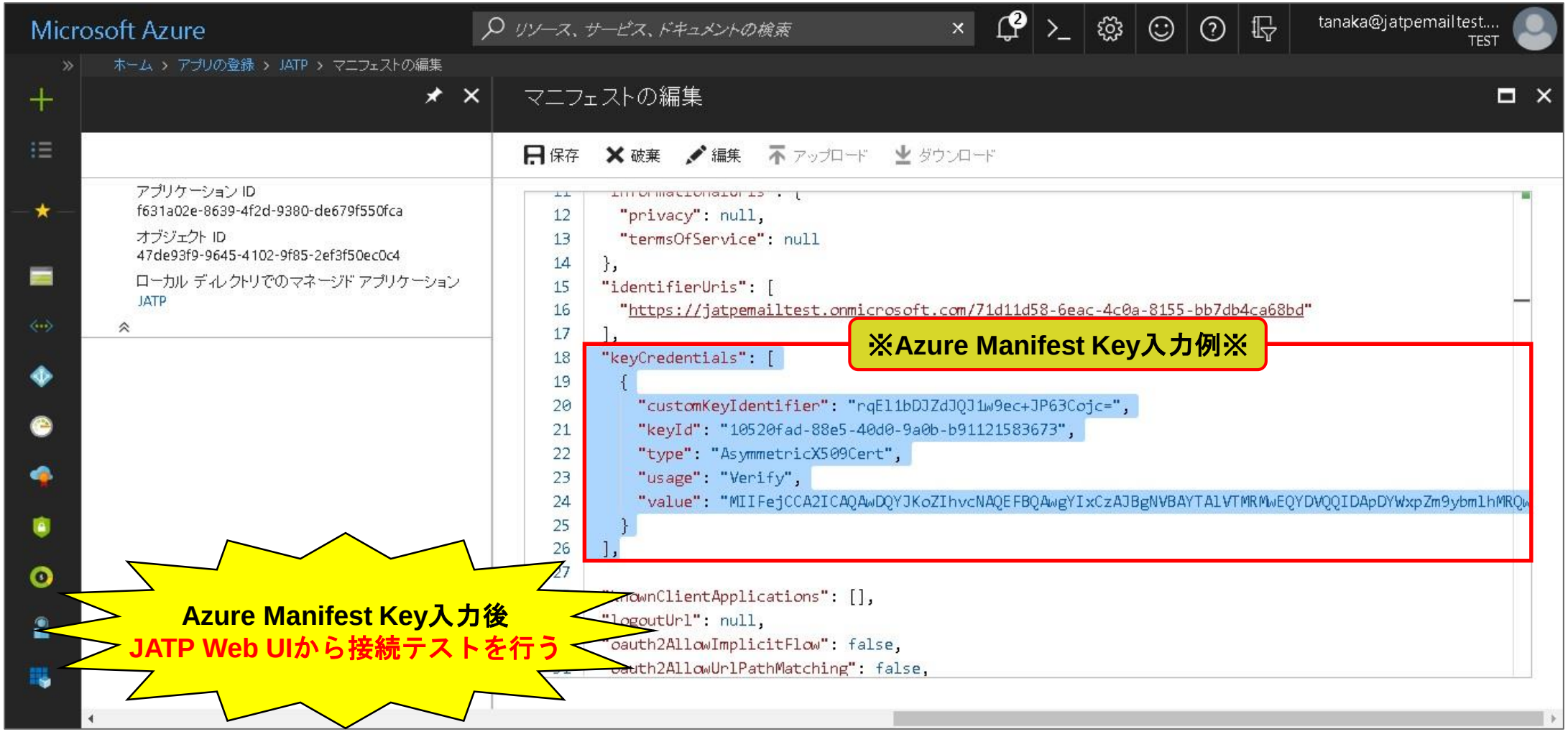
OFFICE 365 MITIGATION設定手順 (BCC,MTA RECEIVER)



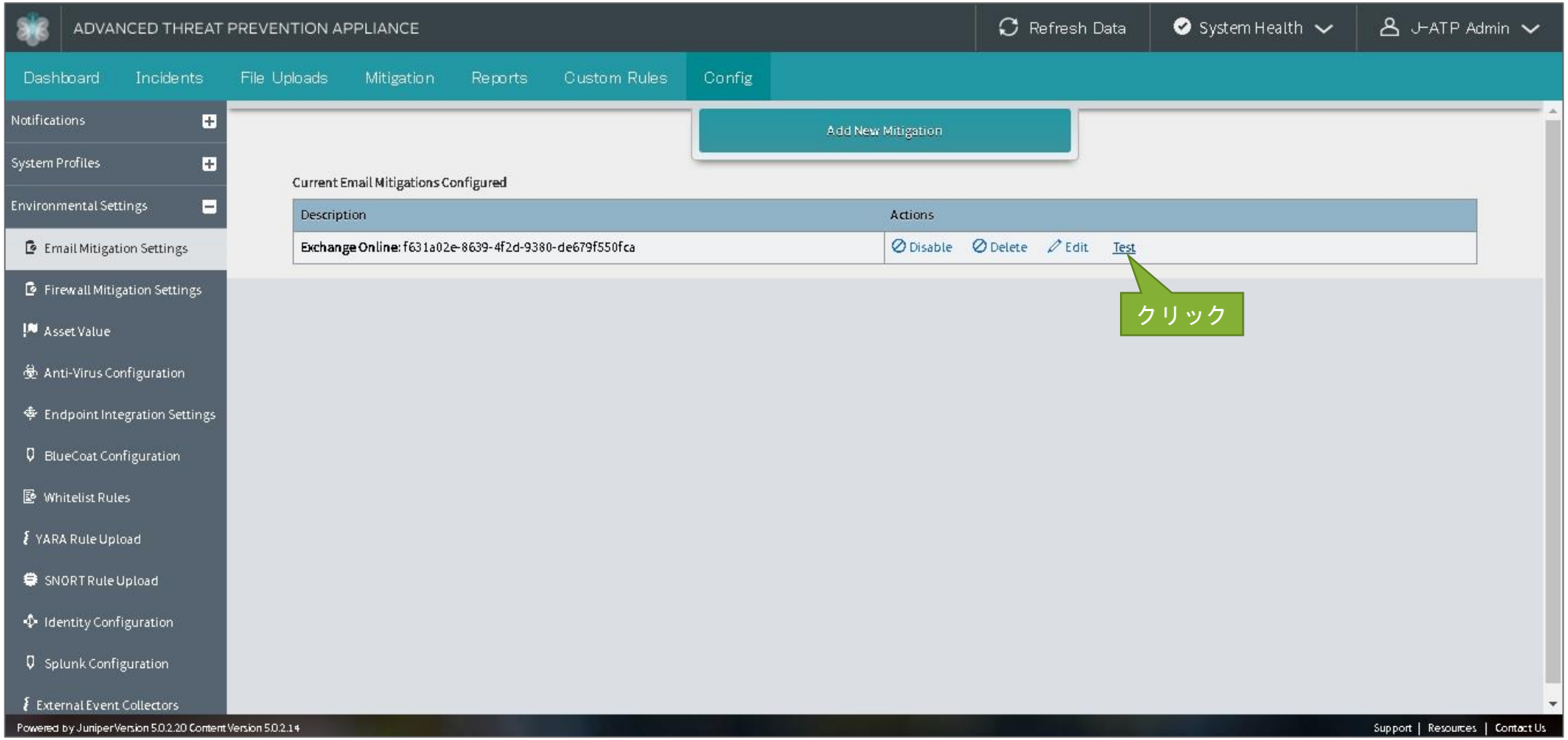
OFFICE 365 MITIGATION設定手順 (BCC,MTA RECEIVER)



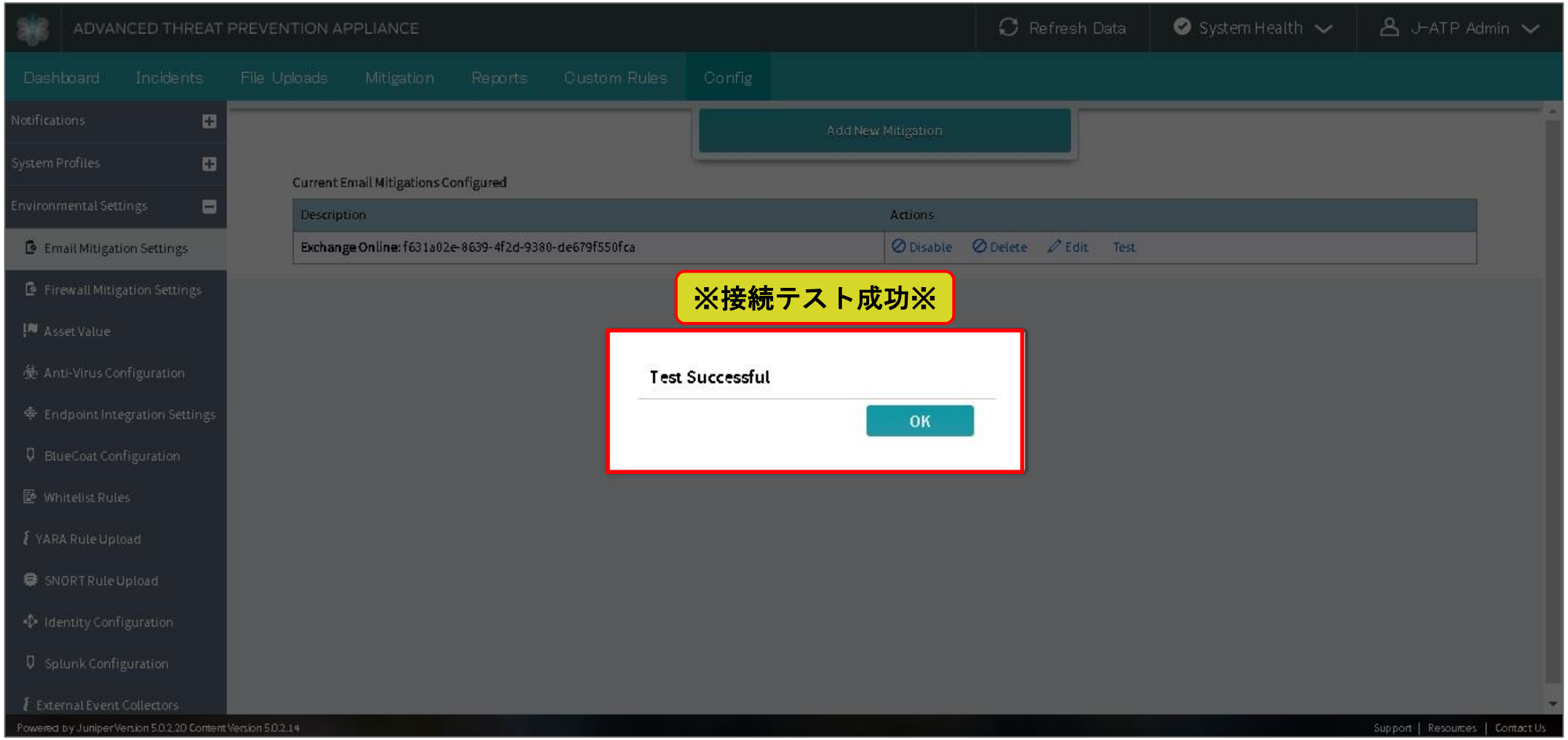
OFFICE 365 MITIGATION設定手順 (BCC,MTA RECEIVER)



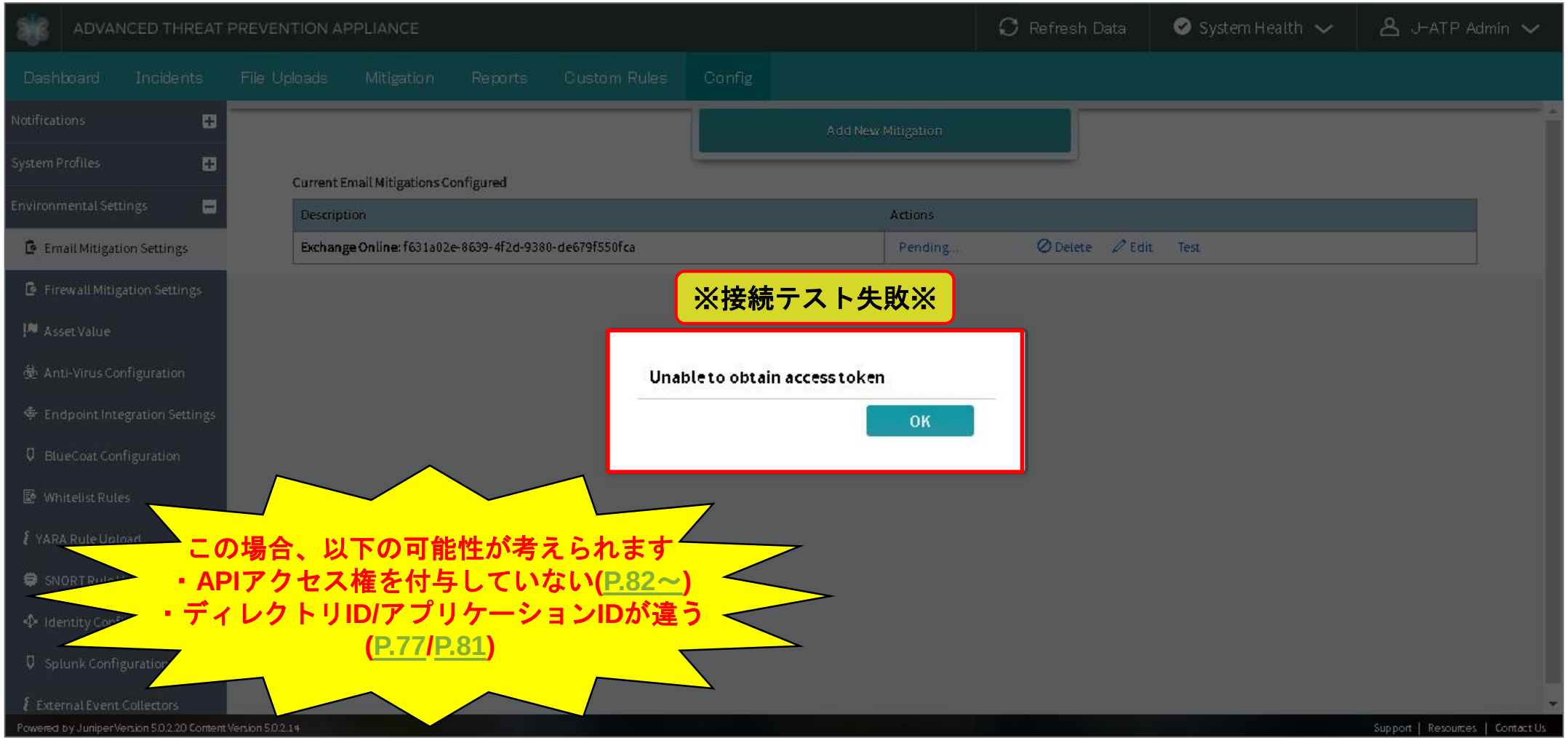
OFFICE 365 MITIGATION設定手順 (BCC,MTA RECEIVER)



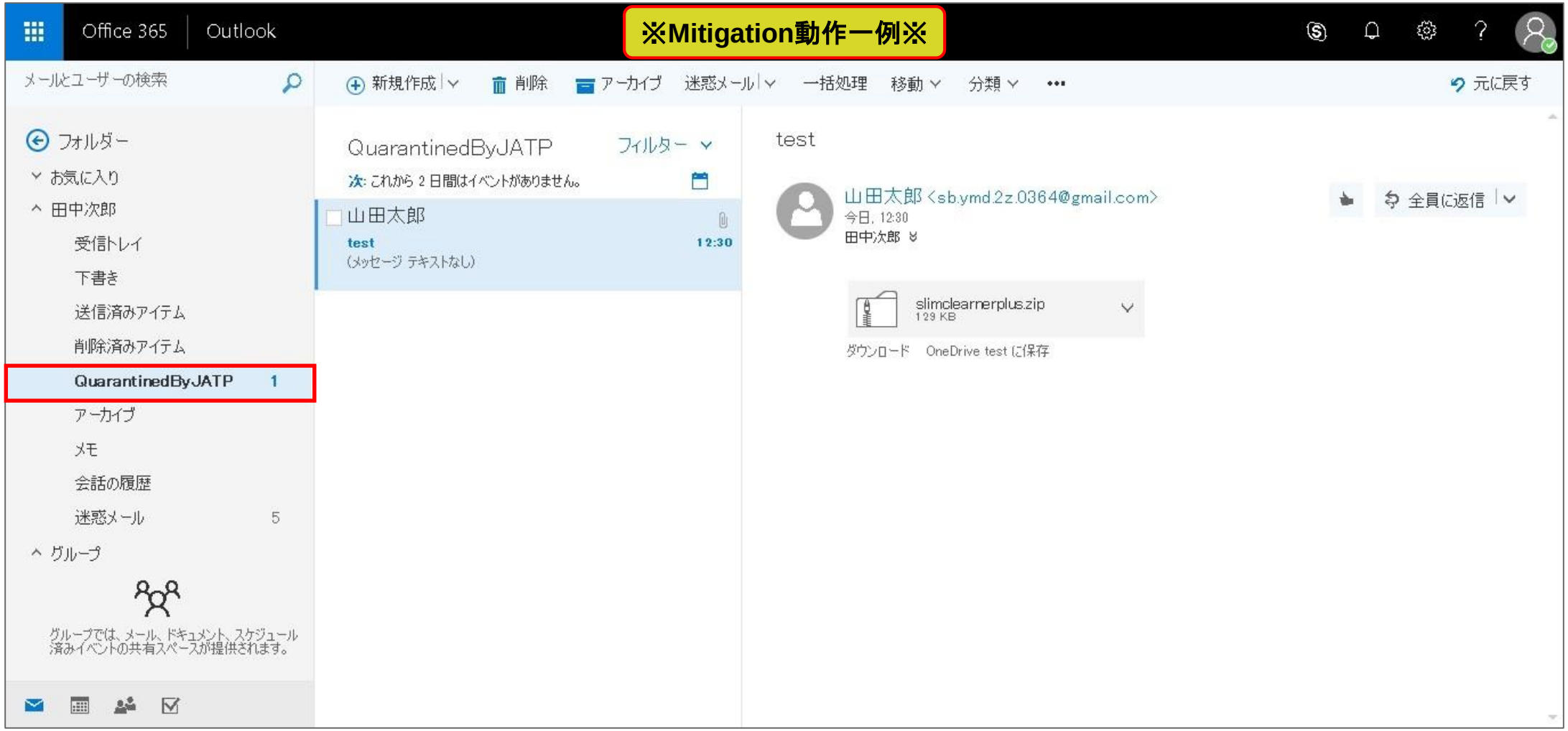
OFFICE 365 MITIGATION設定手順 (BCC,MTA RECEIVER)



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



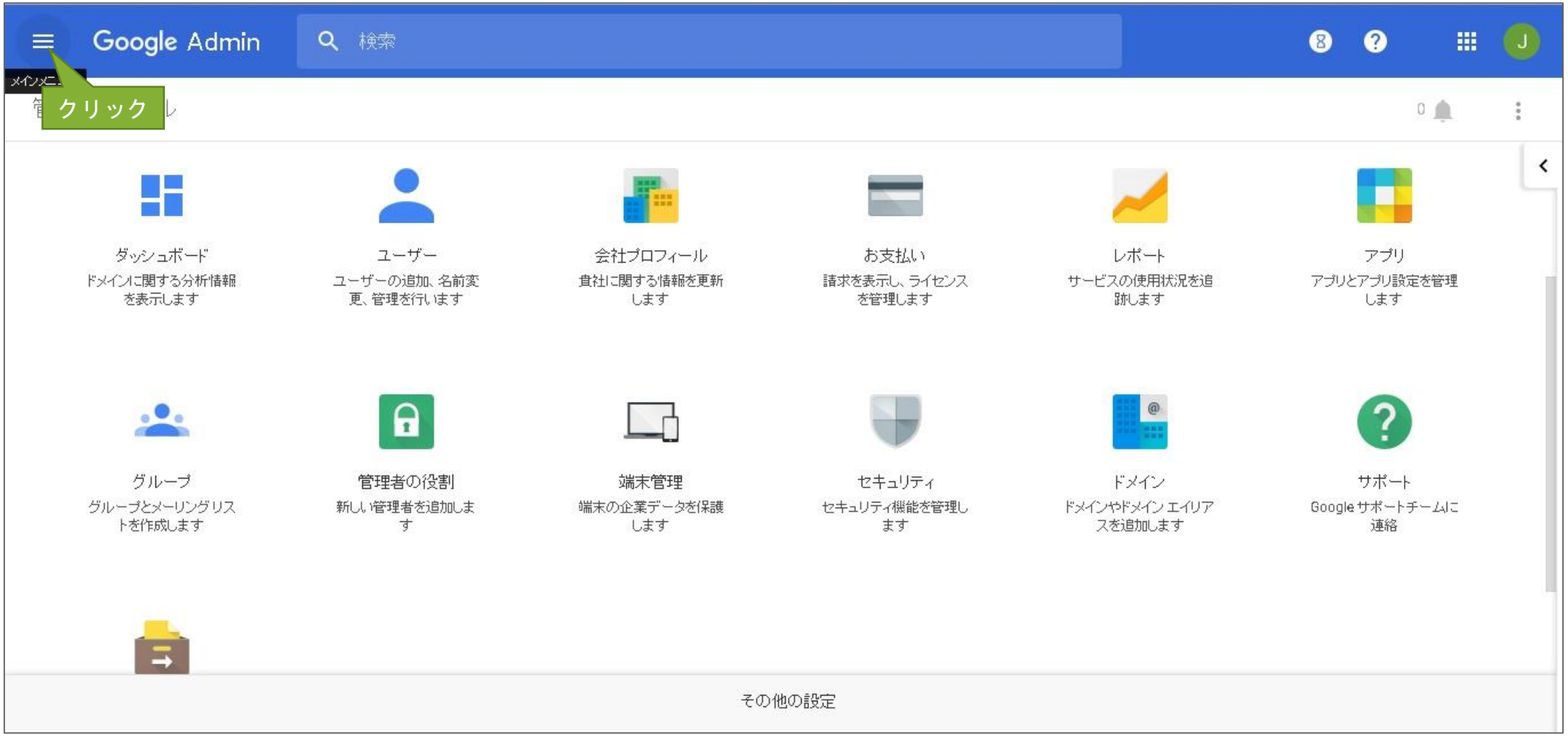
OFFICE 365 MITIGATION設定手順 (BCC,MTA RECEIVER)



G Suite ジャーナル設定手順 (BCC,MTA Receiver)

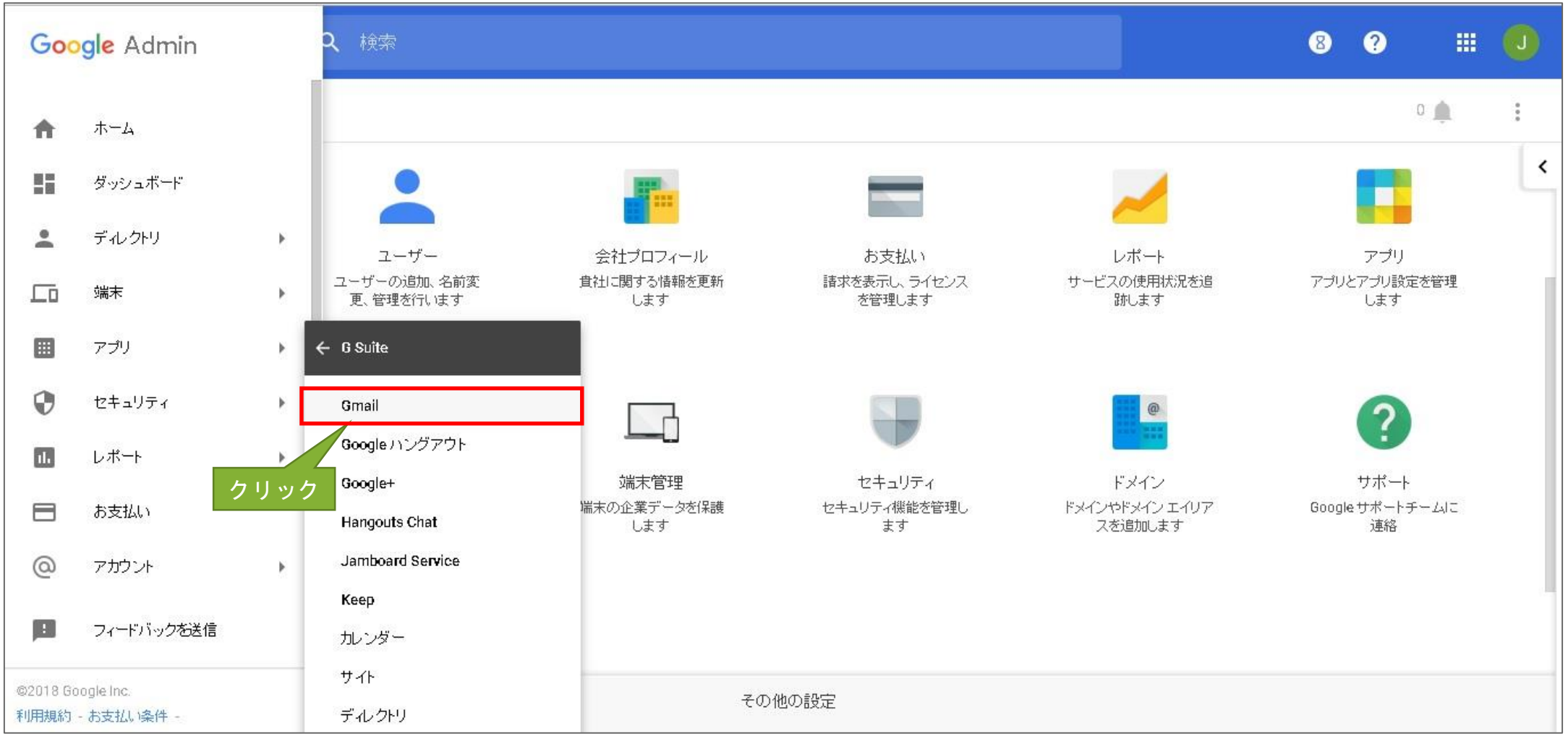
G SUITE ジャーナル設定手順 (BCC,MTA RECEIVER)

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



G SUITE ジャーナル設定手順 (BCC,MTA RECEIVER)

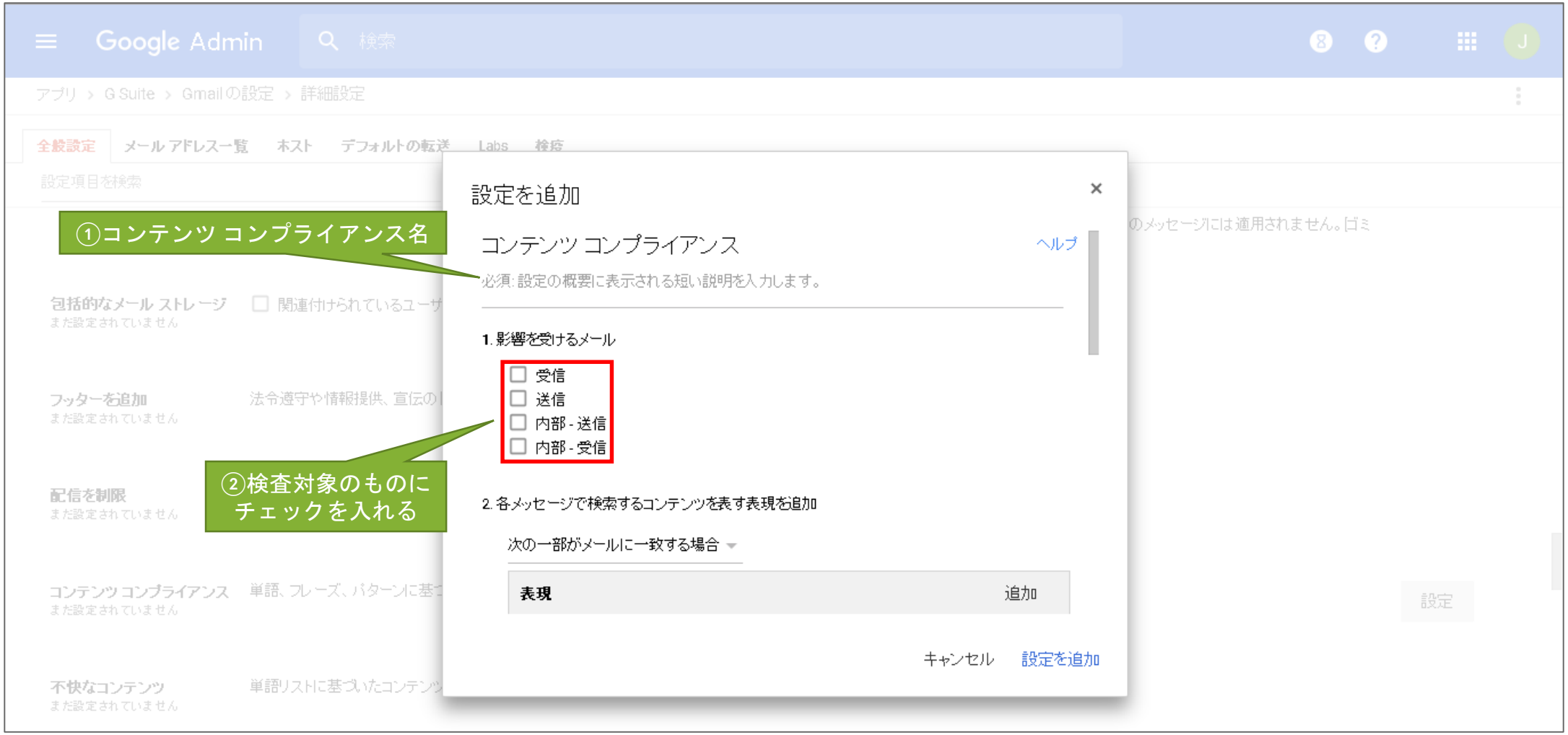
G SUITE ジャーナル設定手順 (BCC,MTA RECEIVER)



G SUITE ジャーナル設定手順 (BCC,MTA RECEIVER)

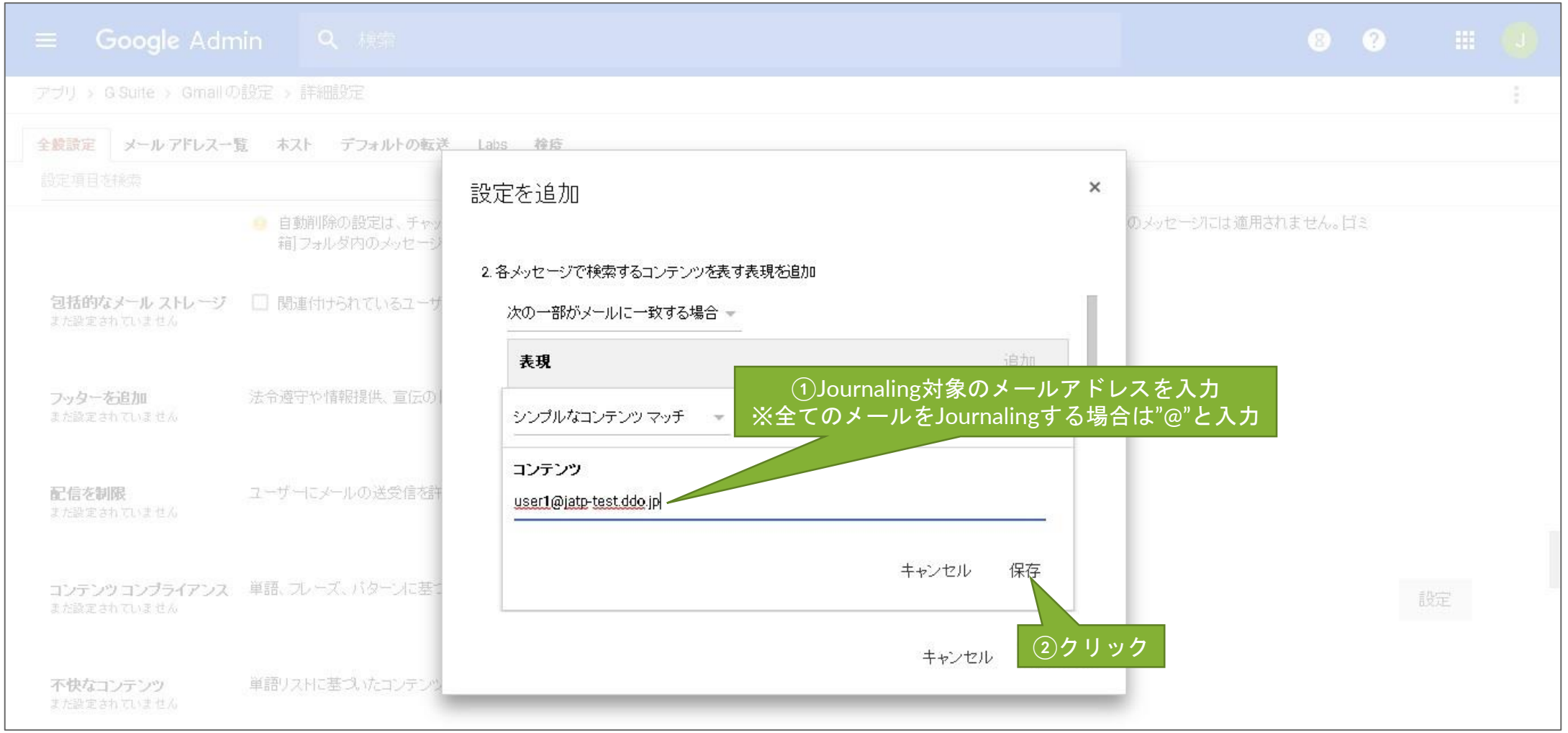
G SUITE ジャーナル設定手順 (BCC,MTA RECEIVER)

G SUITE ジャーナル設定手順 (BCC,MTA RECEIVER)

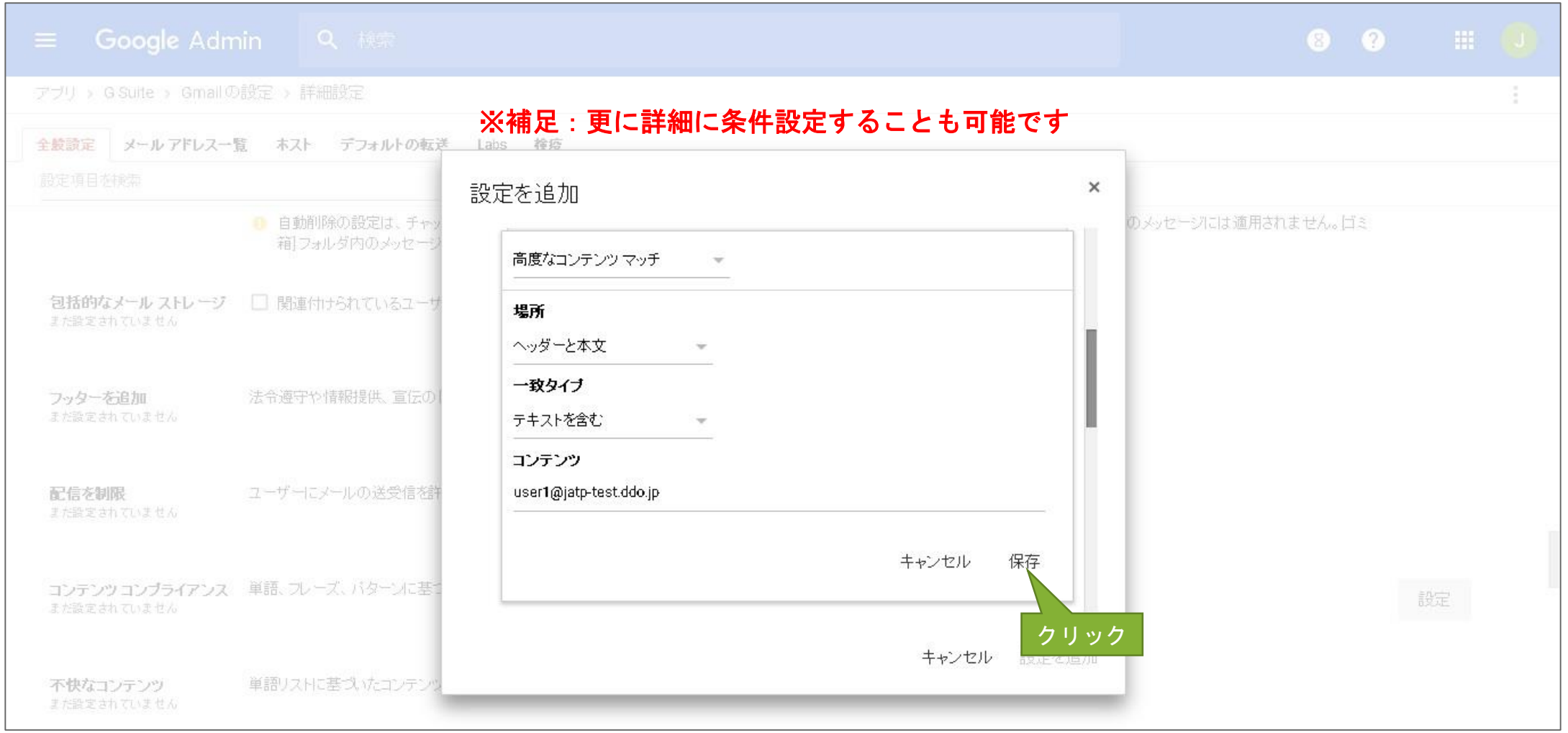


G SUITE ジャーナル設定手順 (BCC,MTA RECEIVER)

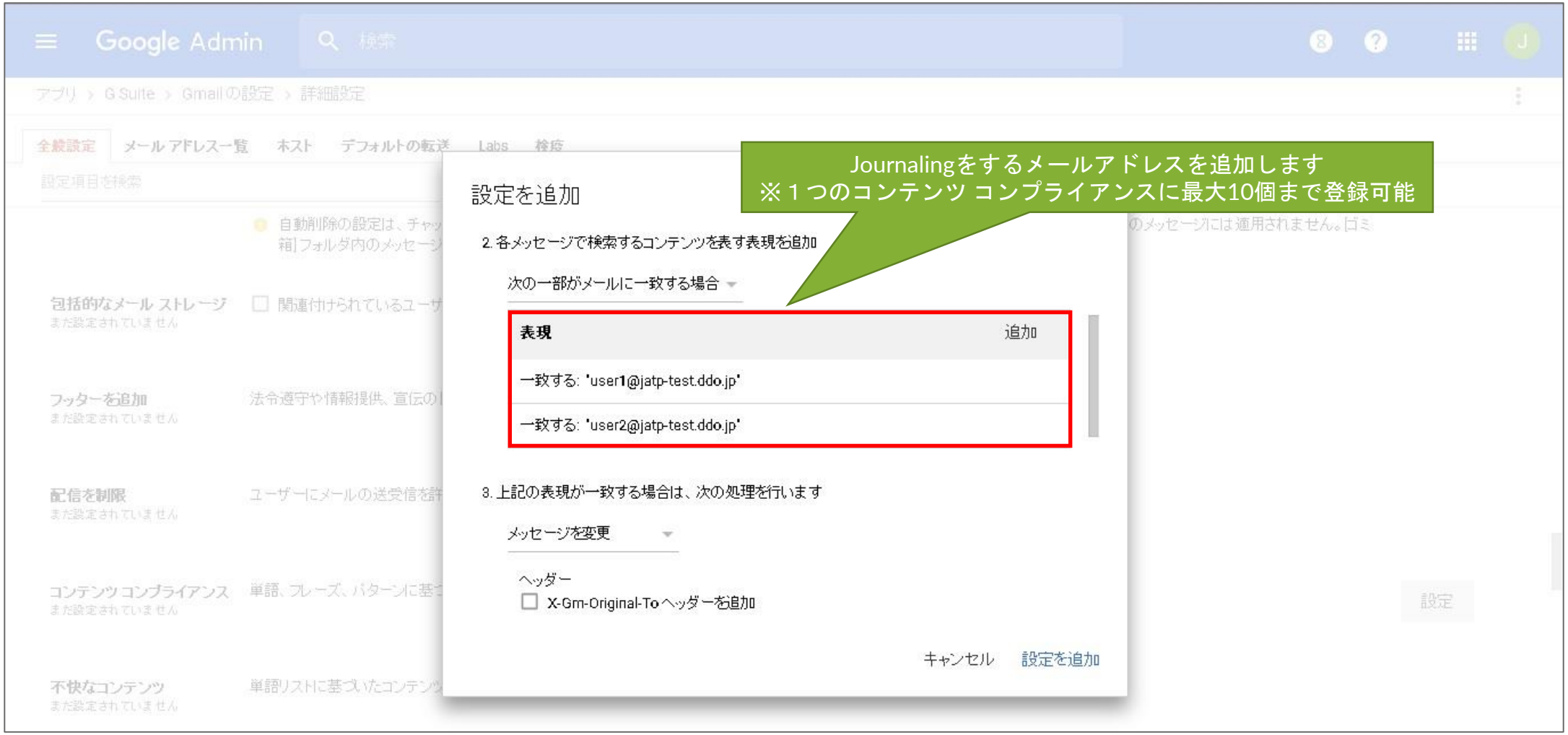
G SUITE ジャーナル設定手順
(BCC,MTA RECEIVER)



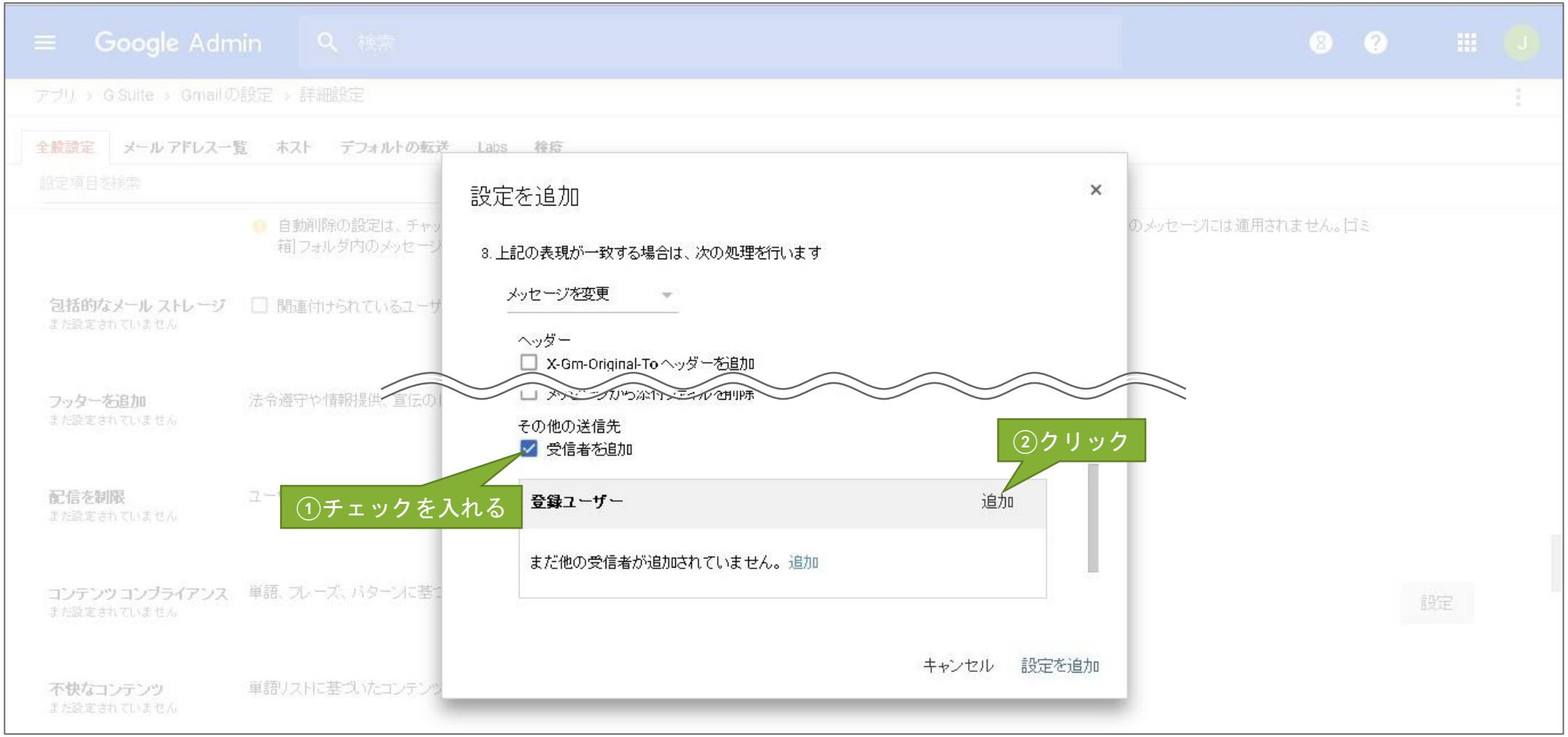
G SUITE ジャーナル設定手順 (BCC,MTA RECEIVER)



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)

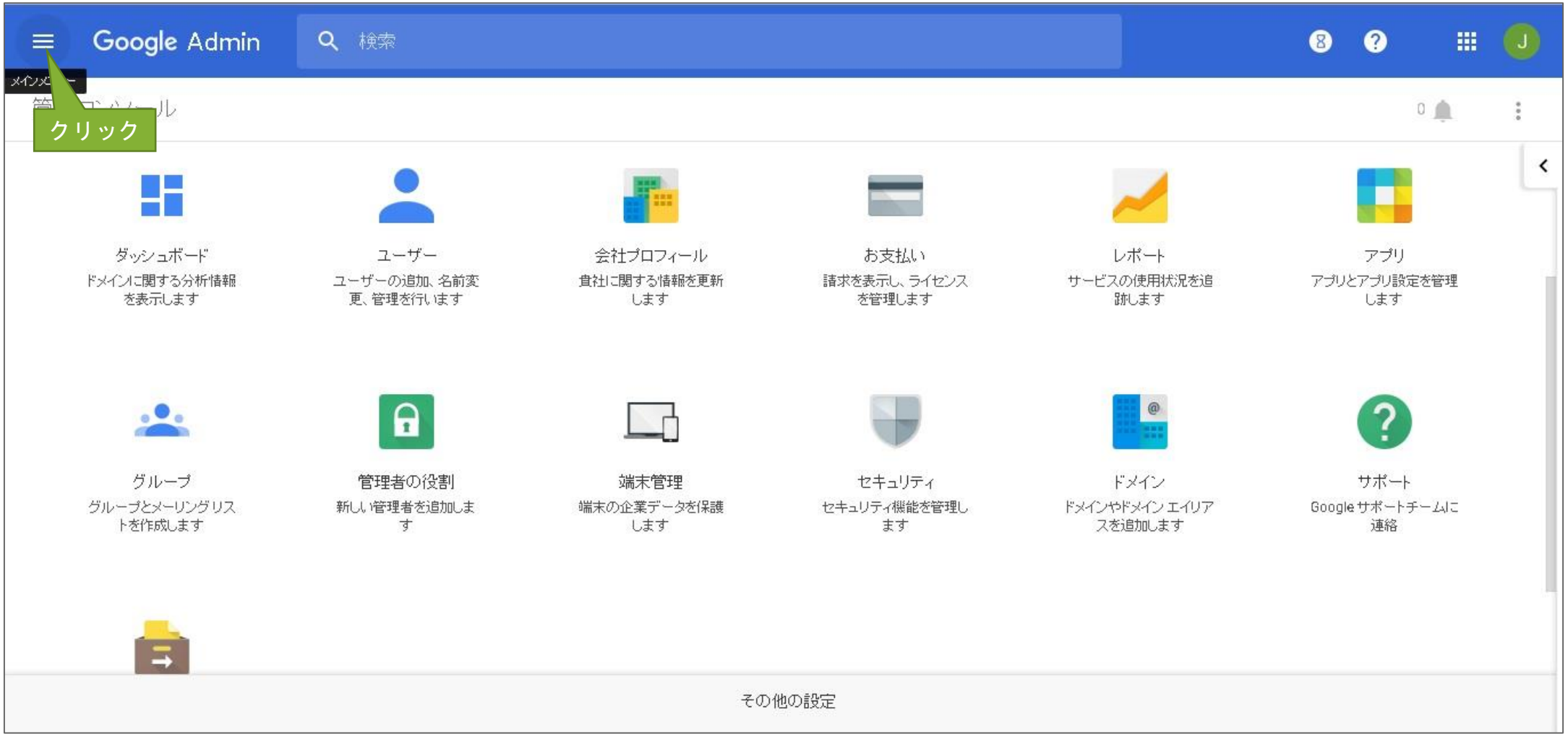
G SUITE ジャーナル設定手順 (BCC,MTA RECEIVER)

G SUITE ジャーナル設定手順 (BCC,MTA RECEIVER)

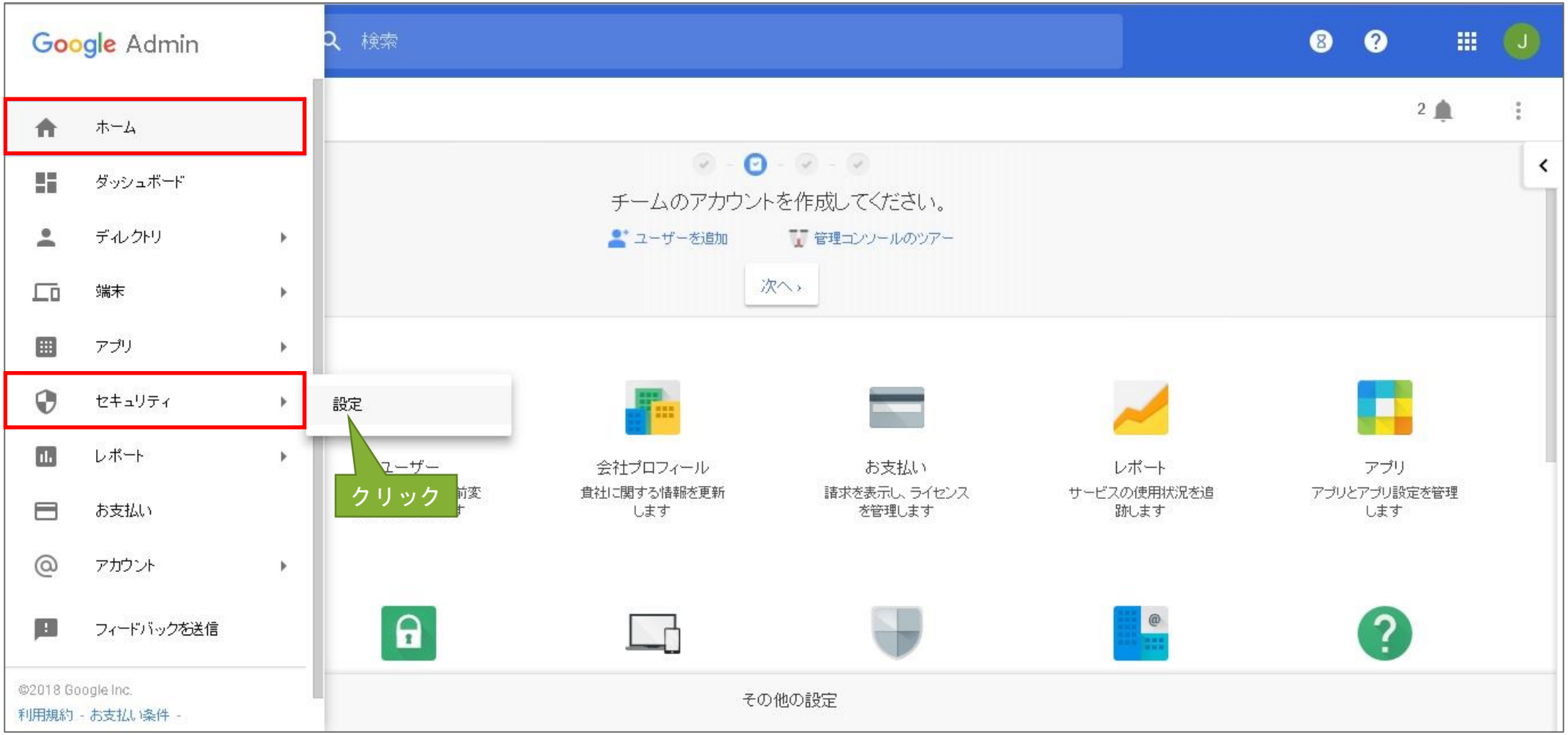
G mail セキュリティ設定の変更 (BCC)

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



GMAIL 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)

GMAIL 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)

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。

GMAIL 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)

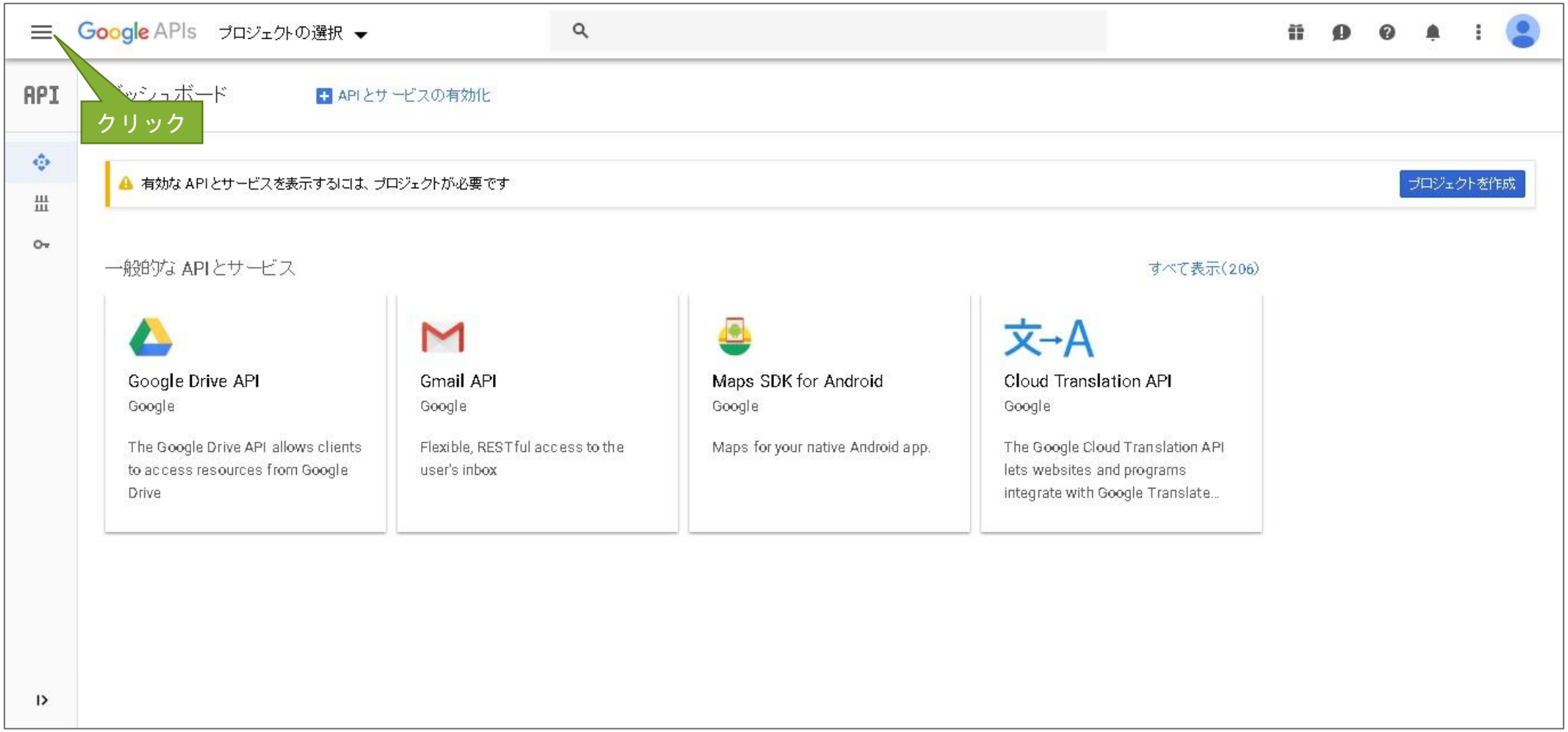
GmailではPOP3/IMAPの設定がデフォルトでは無効になっているため、設定の変更が必要となります。
Journaling対象の各アカウントでログインし、 Gmail(https://mail.google.com/mail/)へアクセスします。

GMAIL セキュリティ設定の変更 (BCC)

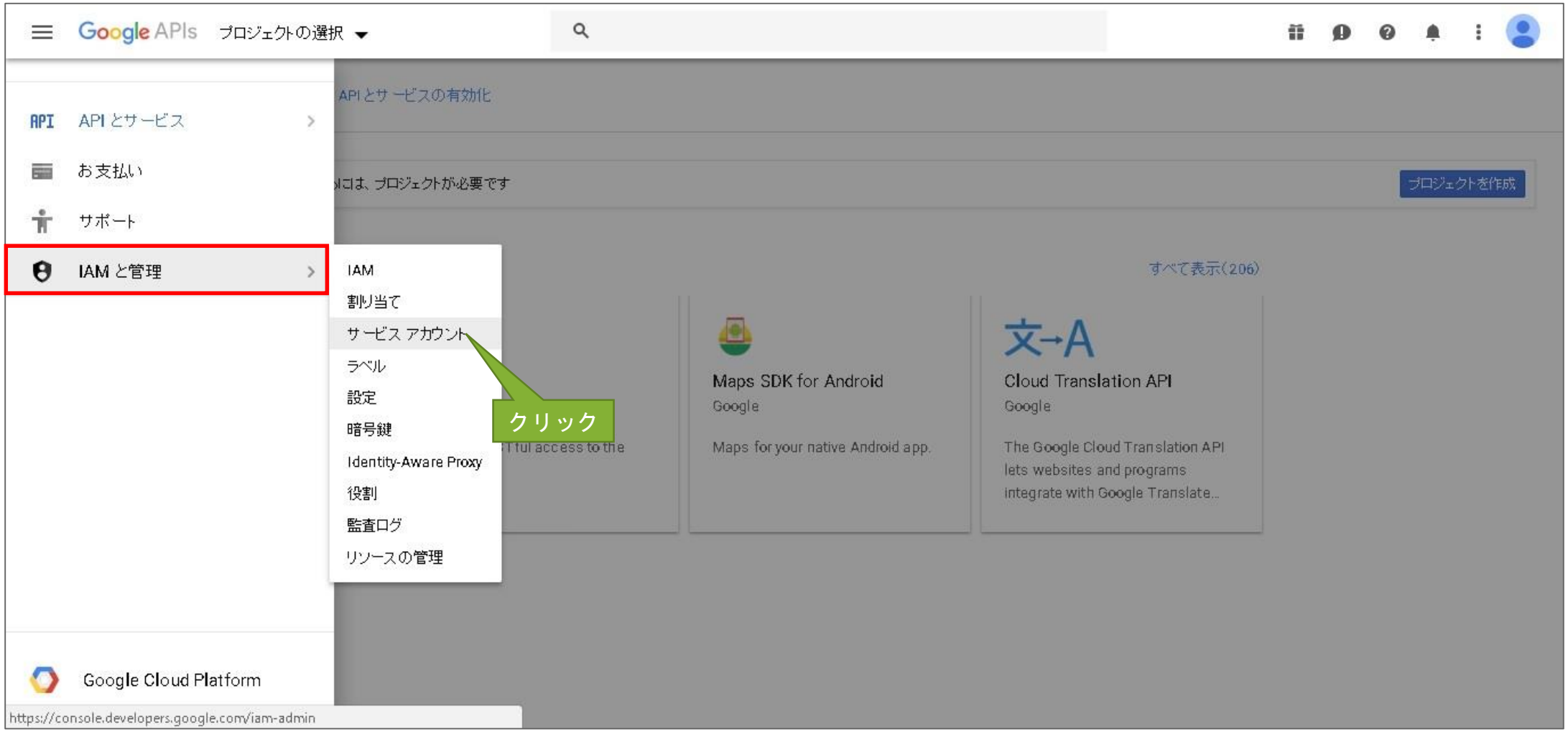
G Suite Mitigation設定手順 (BCC,MTA Receiver)

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

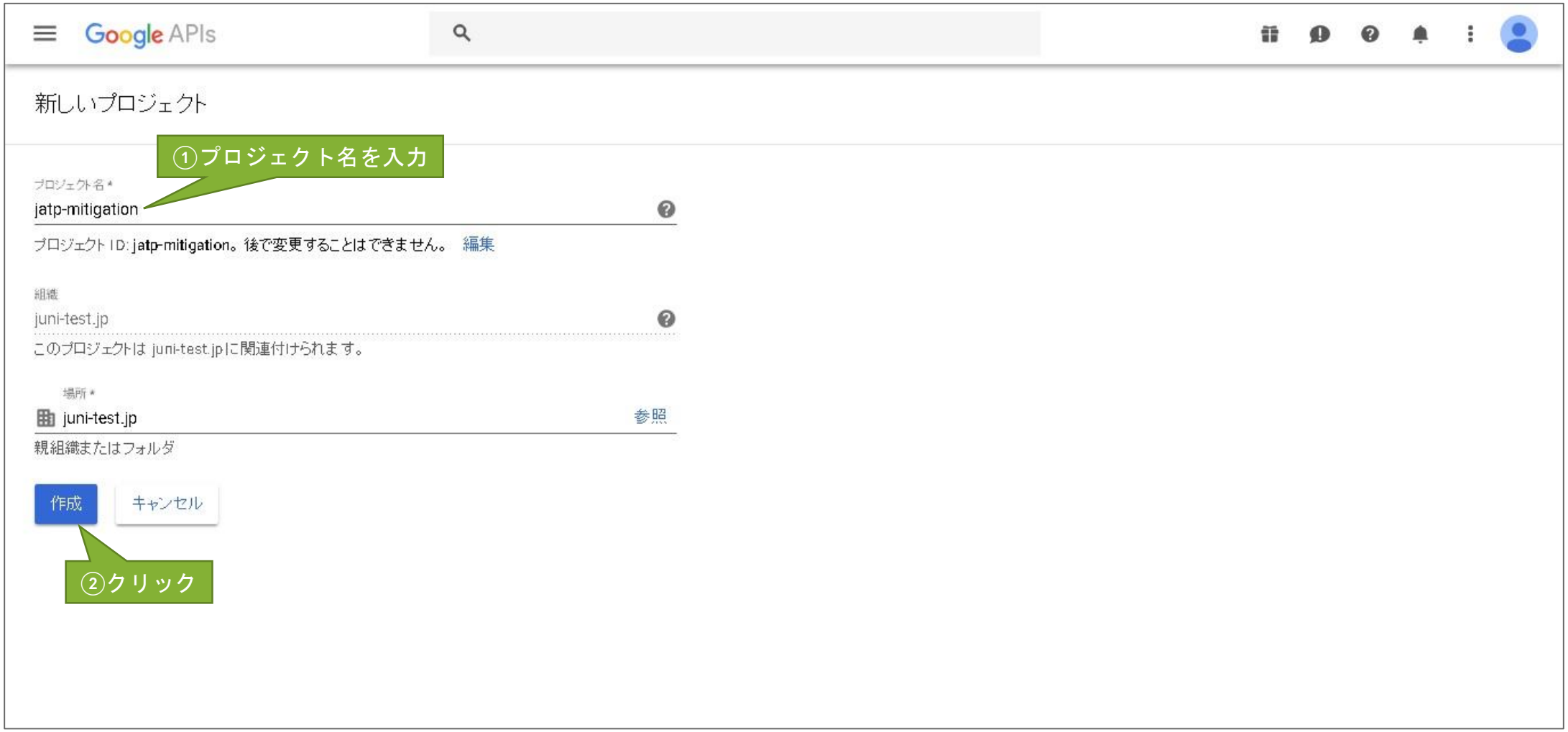


G SUITE MITIGATION設定手順 (BCC,MTA RECEIVER)



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

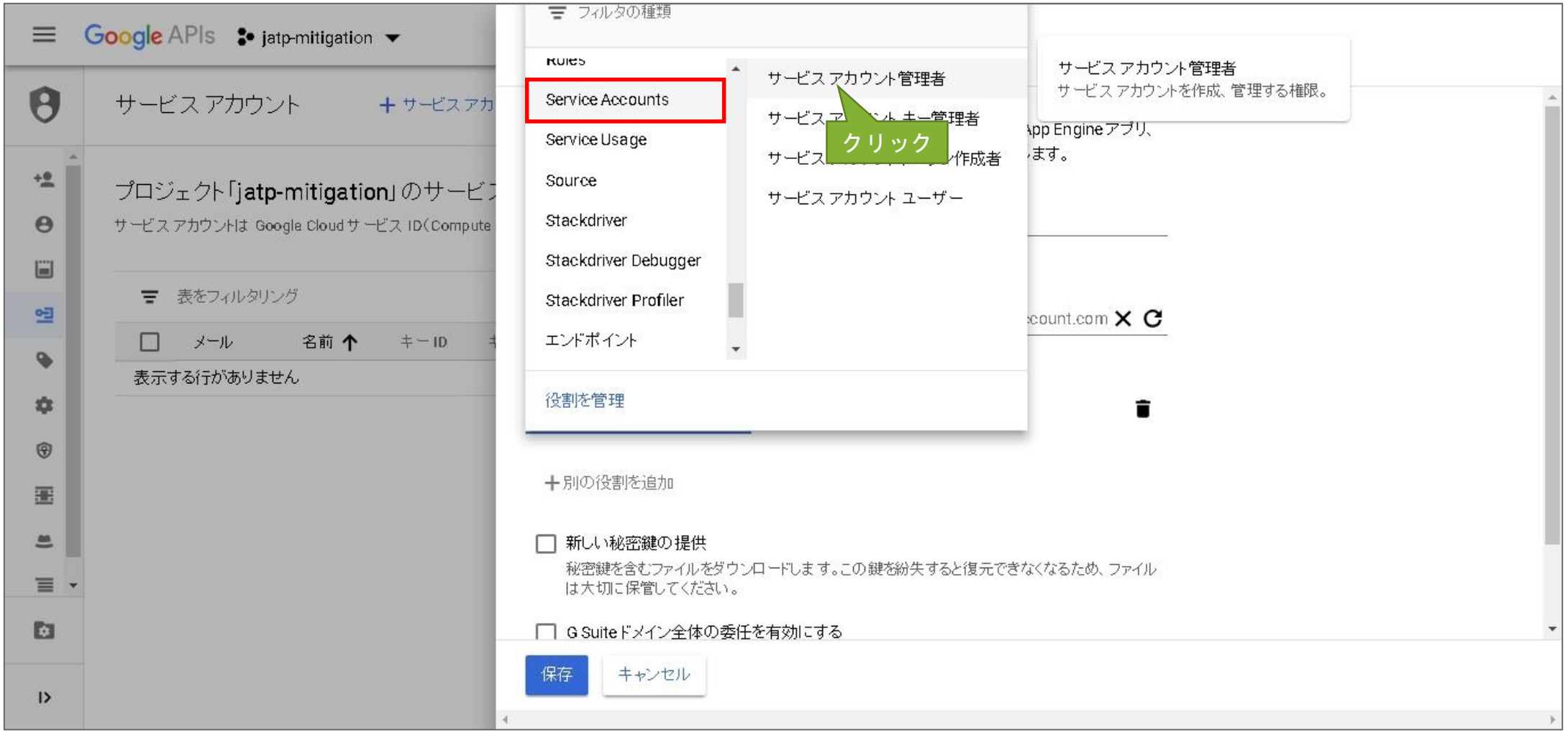
G SUITE MITIGATION設定手順 (BCC,MTA RECEIVER)



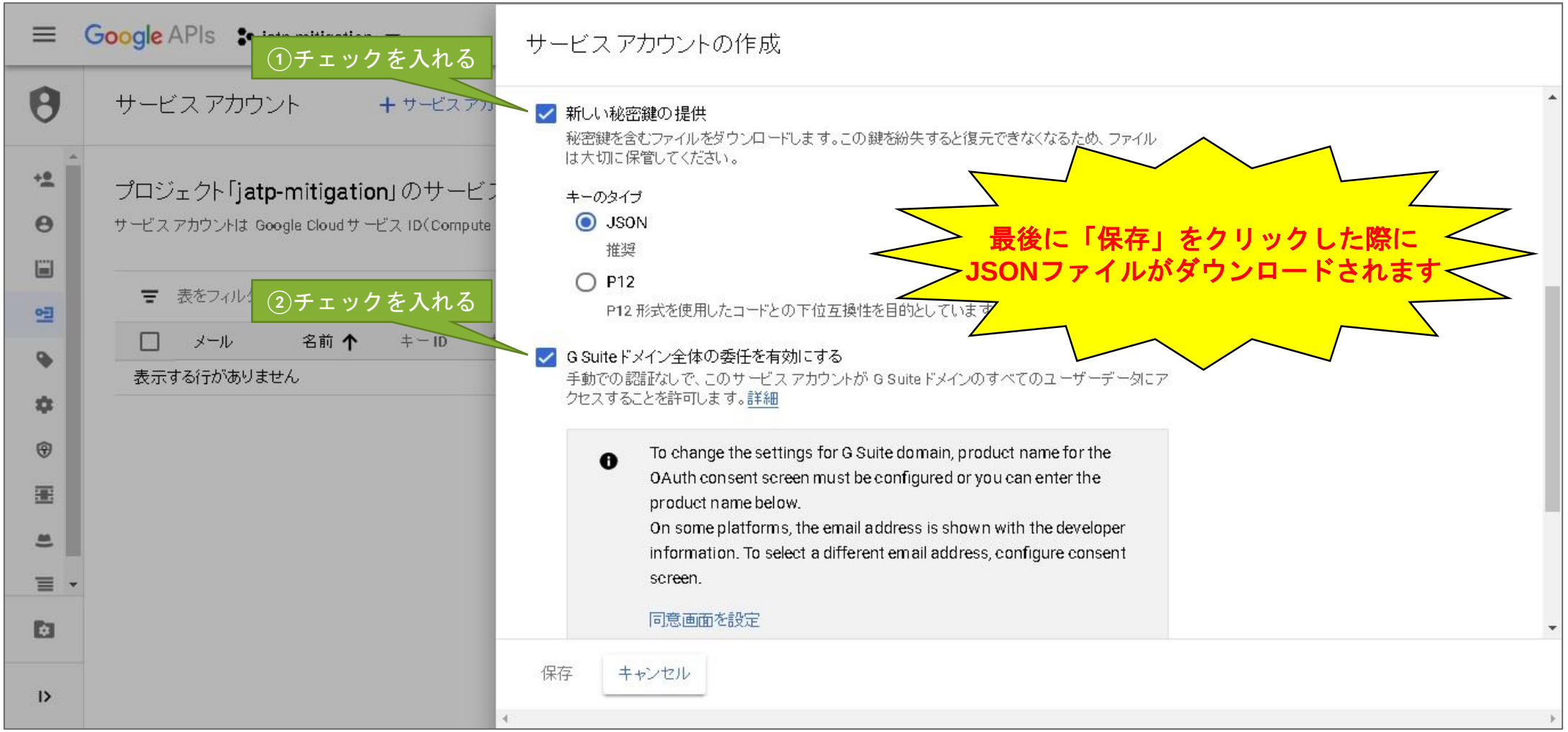
G SUITE MITIGATION設定手順 (BCC,MTA RECEIVER)

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

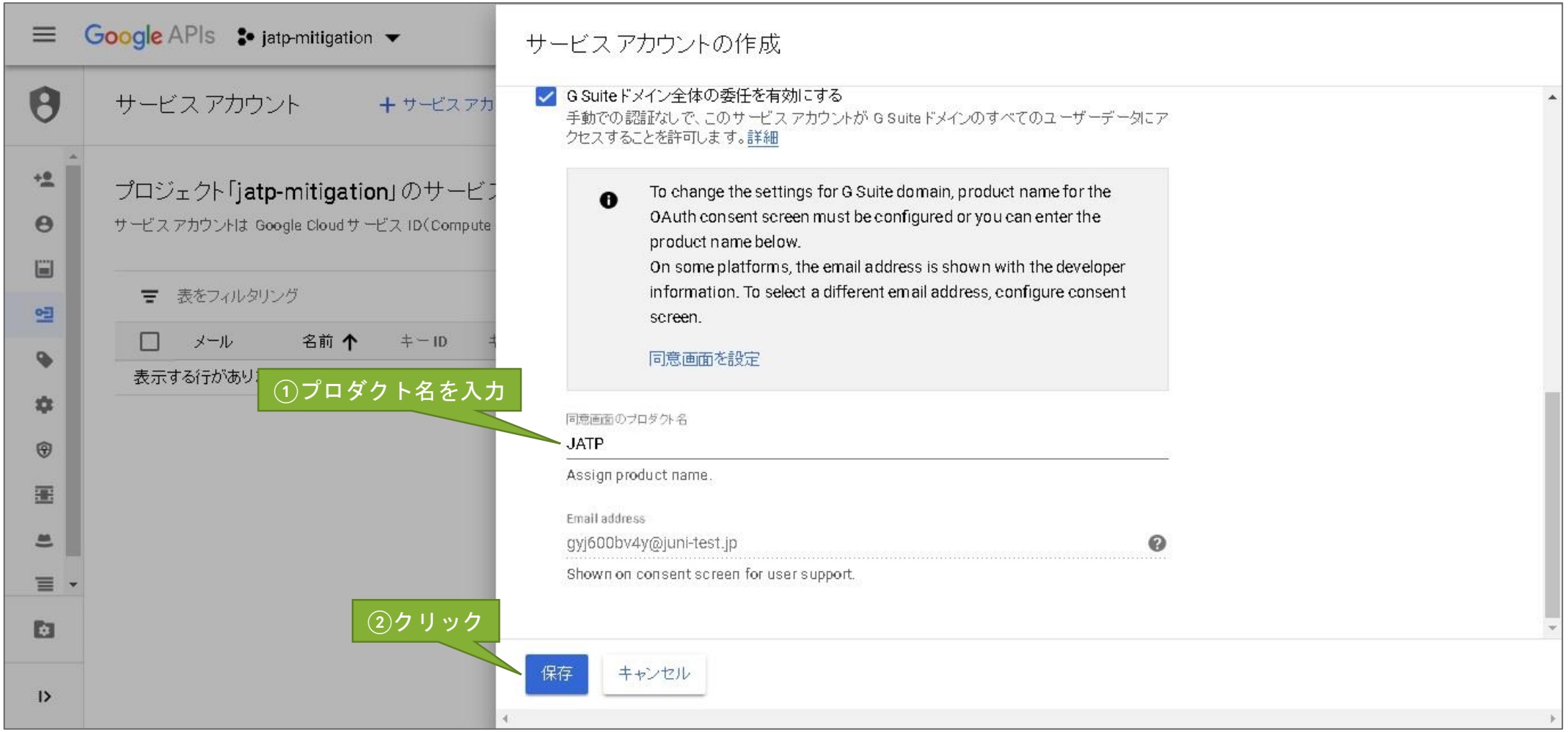
G SUITE MITIGATION設定手順 (BCC,MTA RECEIVER)



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



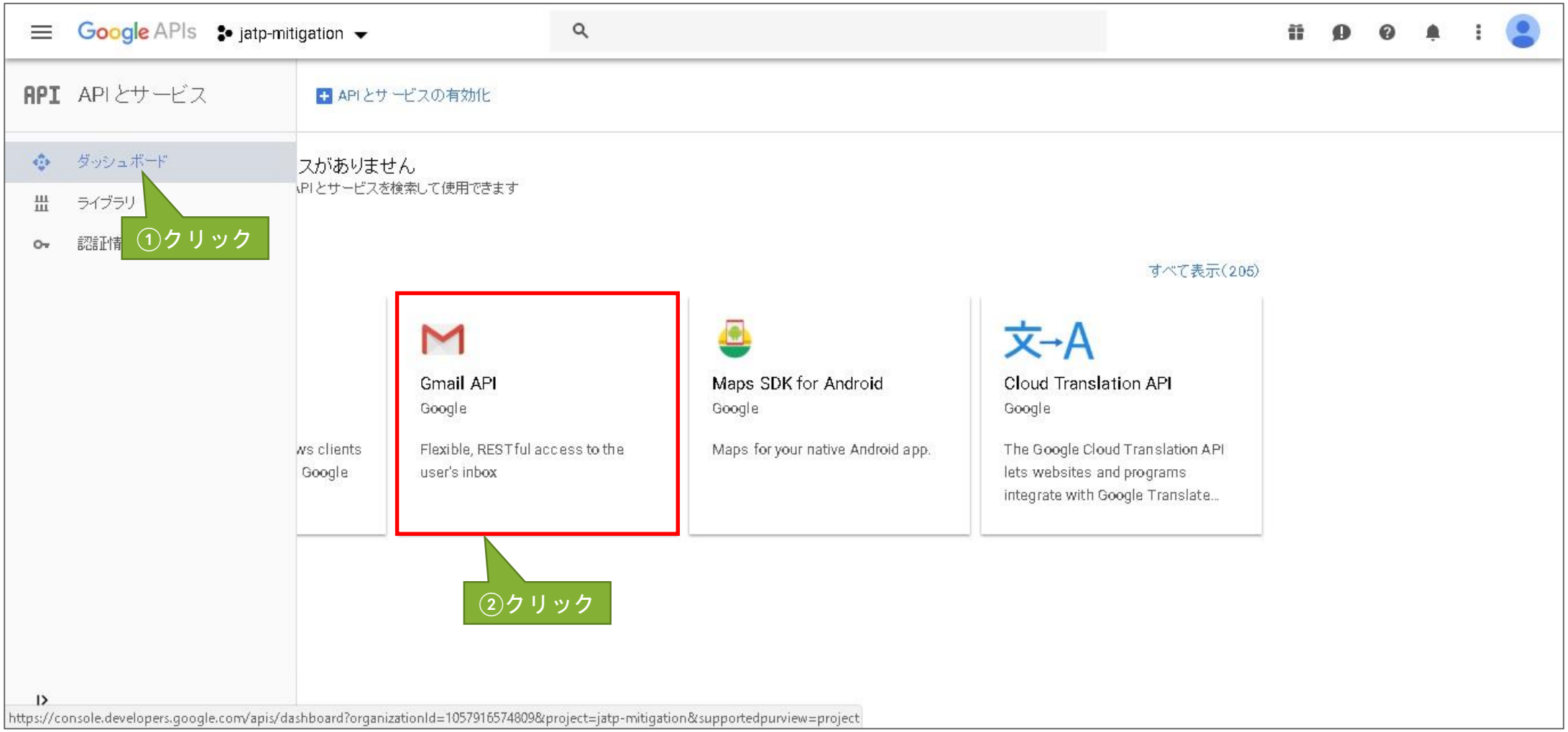
G SUITE MITIGATION設定手順 (BCC,MTA RECEIVER)



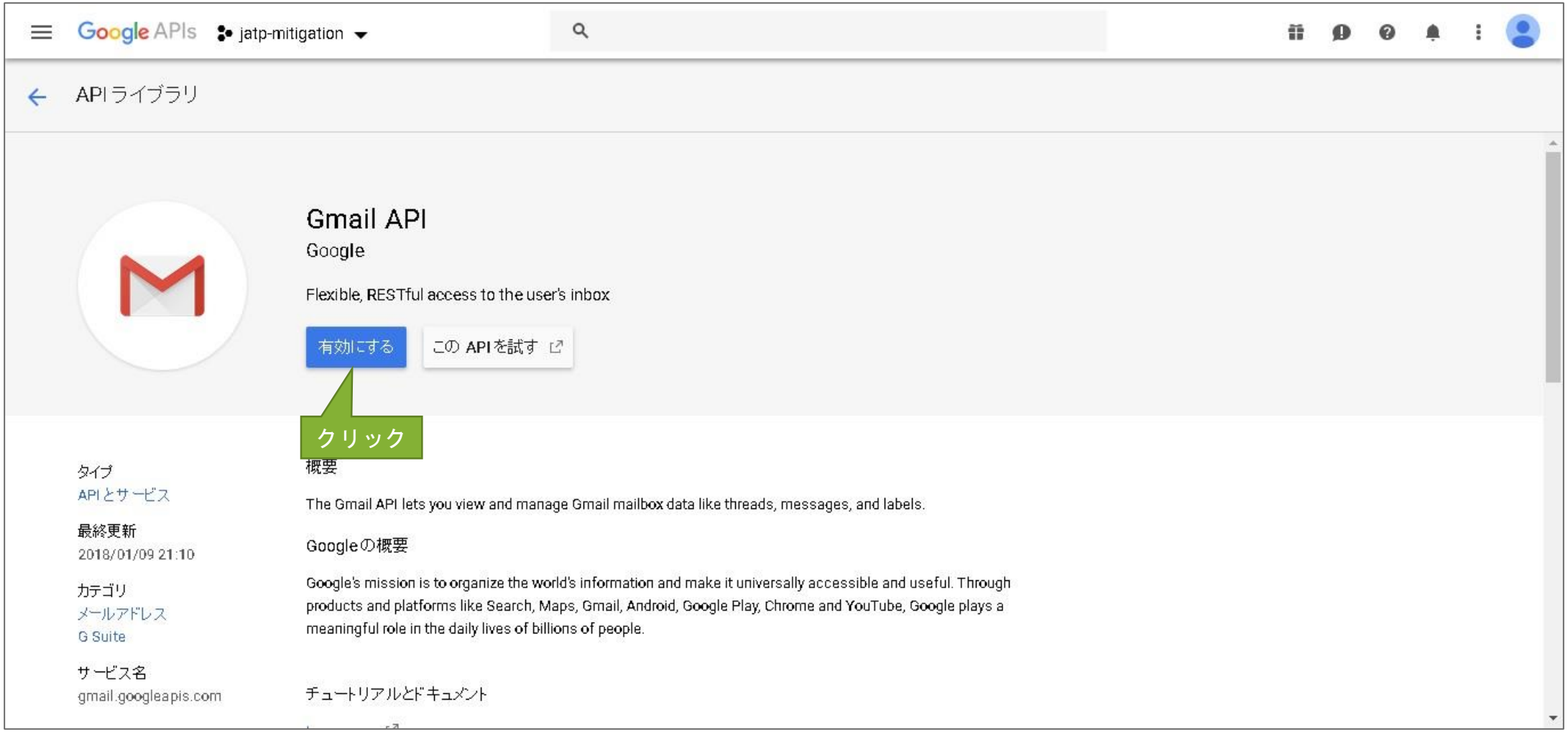
G SUITE MITIGATION設定手順 (BCC,MTA RECEIVER)

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

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

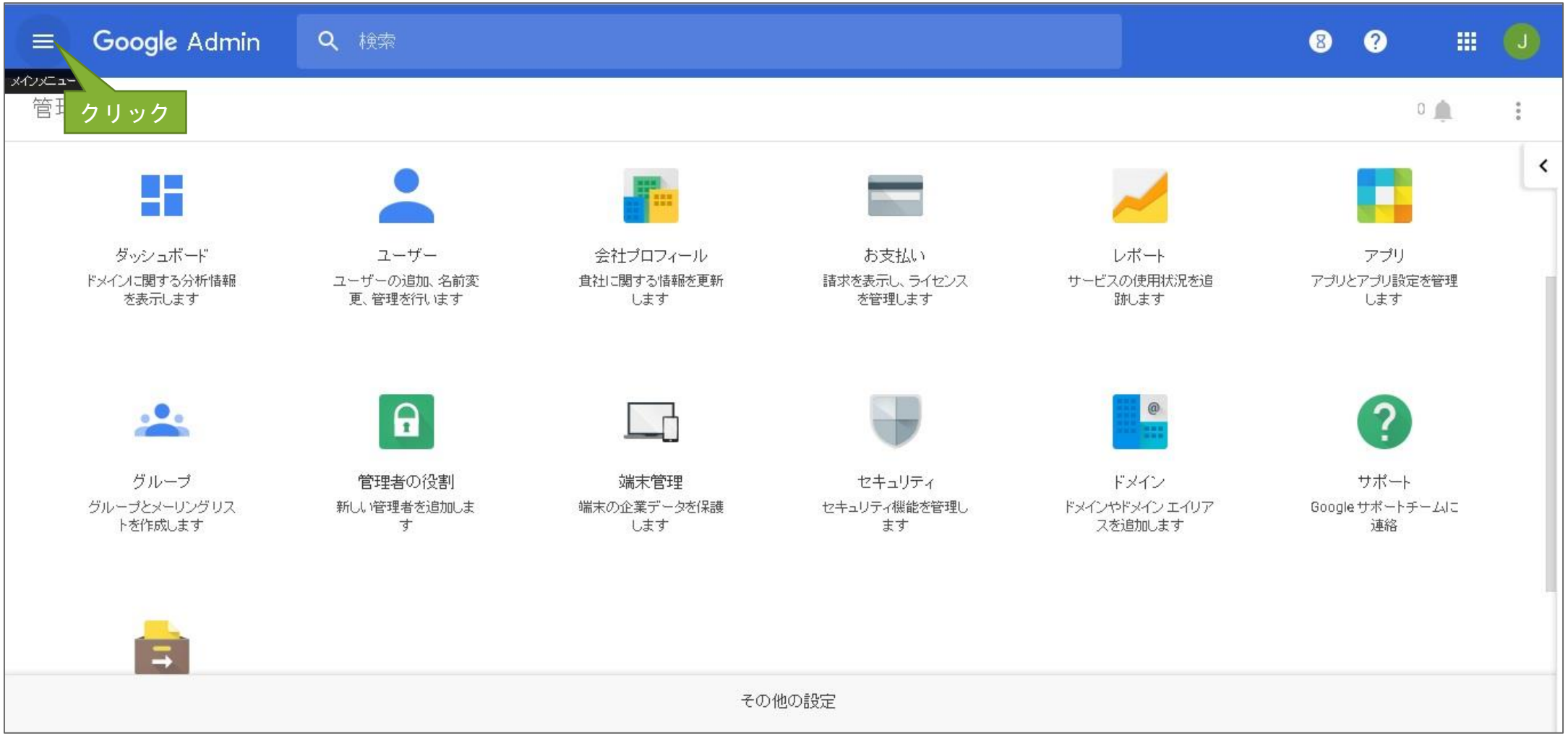


G SUITE MITIGATION設定手順 (BCC,MTA RECEIVER)

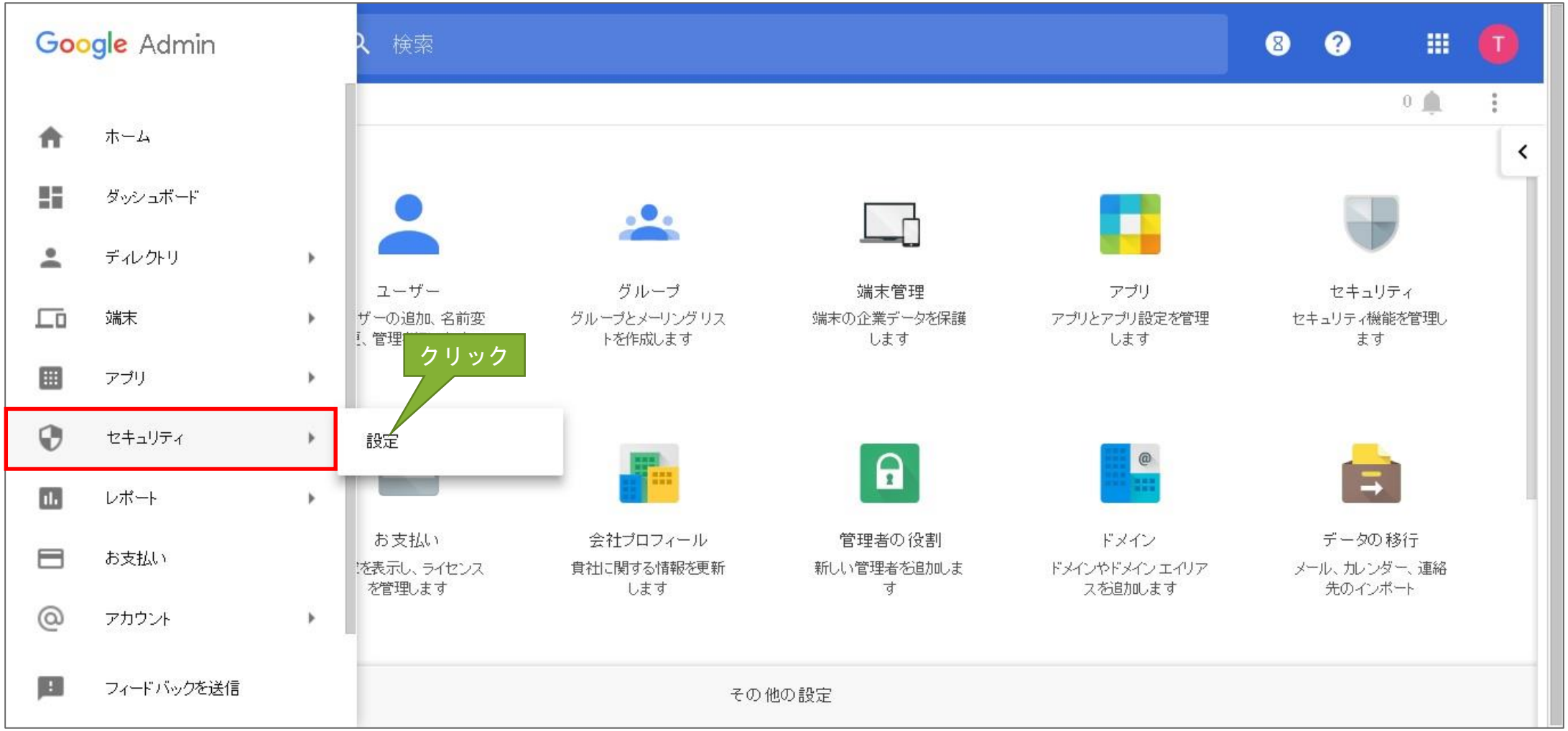


G SUITE MITIGATION設定手順 (BCC,MTA RECEIVER)

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



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

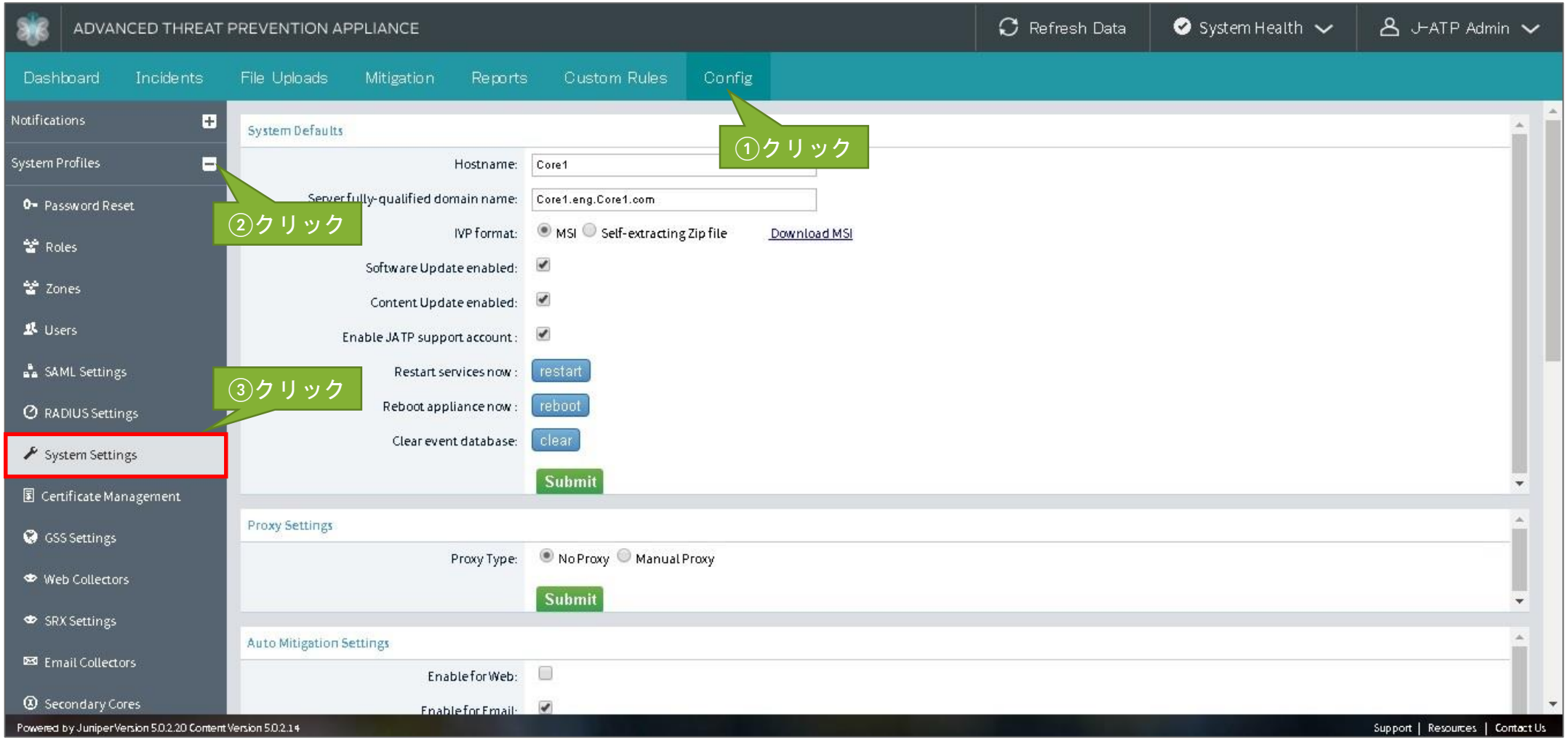


G SUITE MITIGATION設定手順 (BCC,MTA RECEIVER)

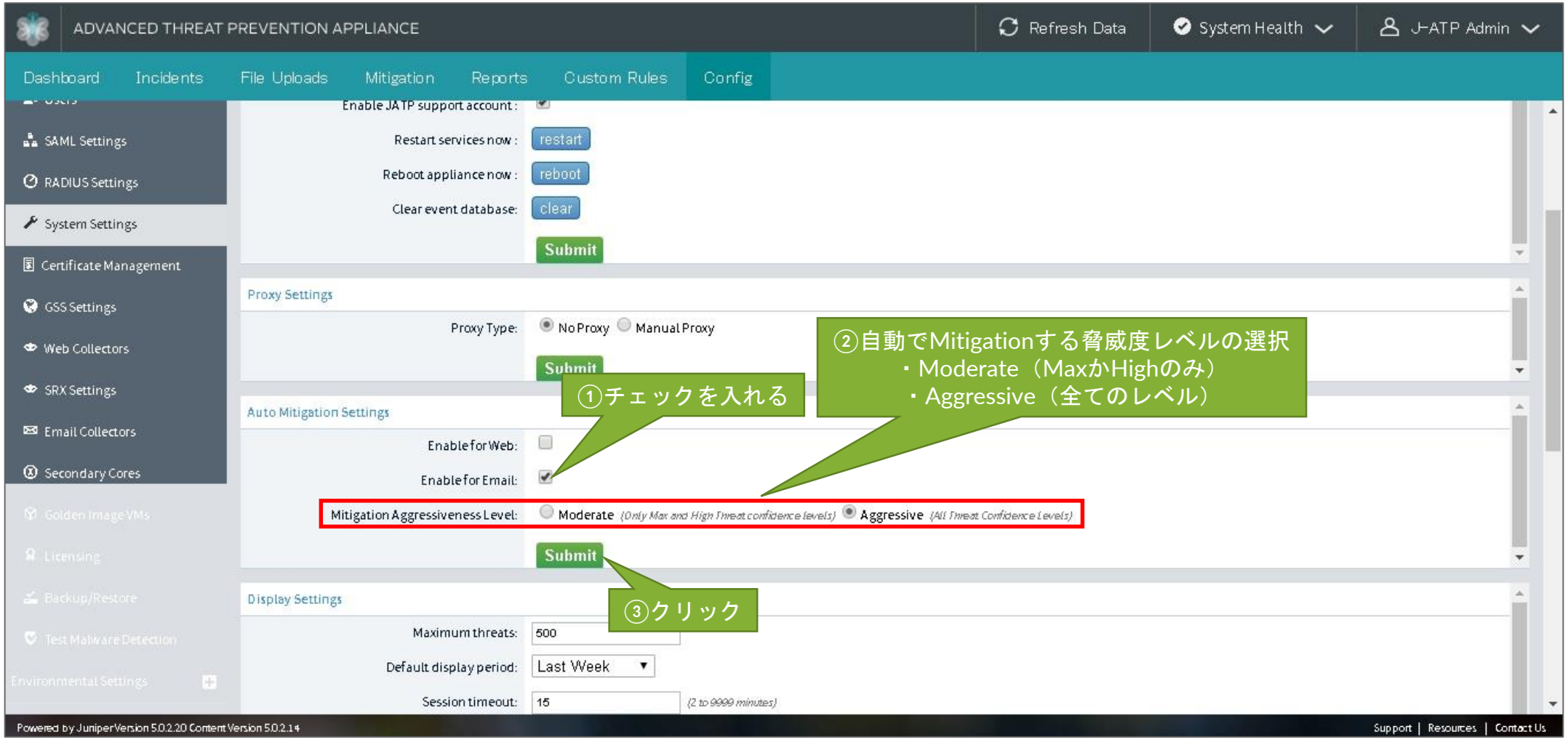
G SUITE MITIGATION設定手順 (BCC,MTA RECEIVER)

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

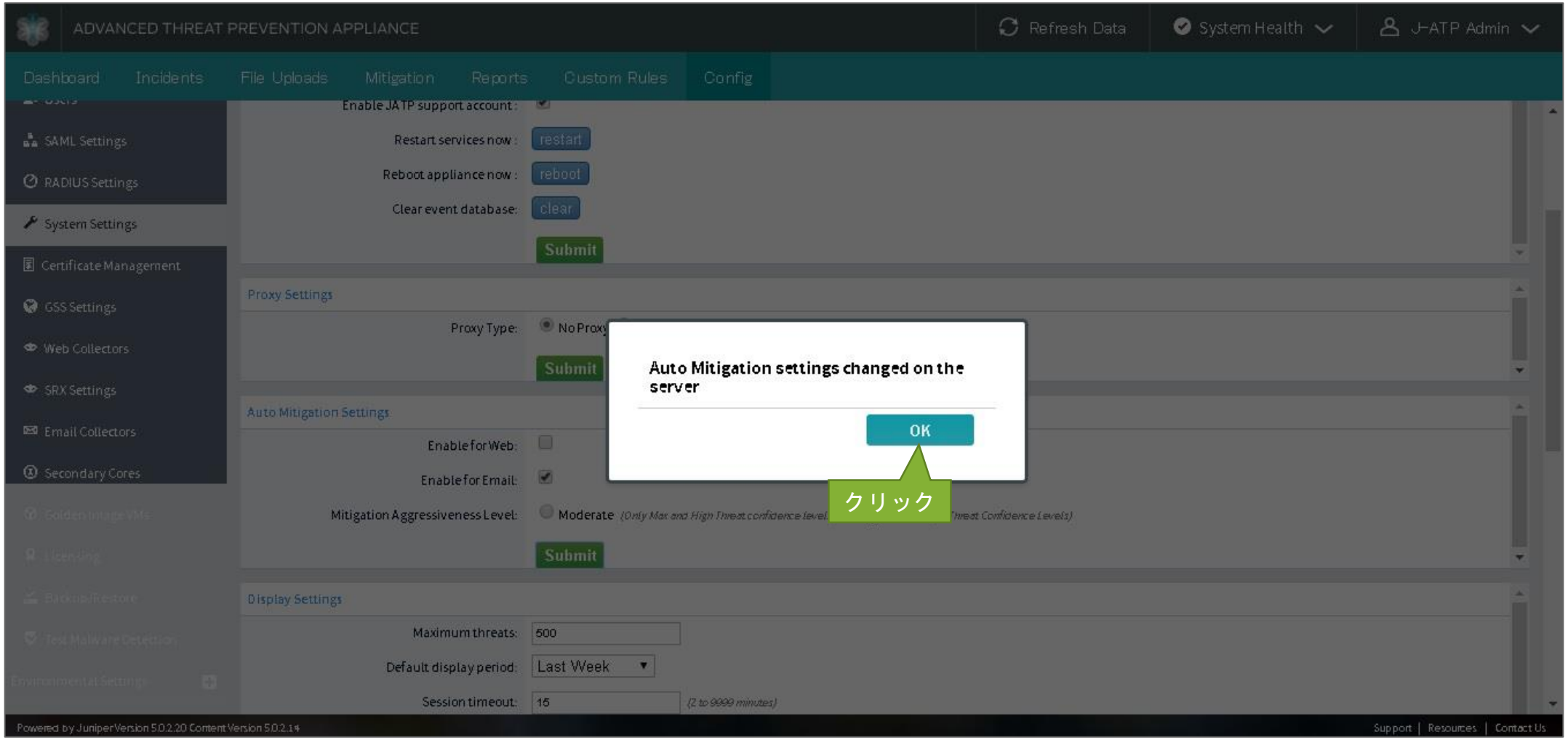
G SUITE MITIGATION設定手順 (BCC,MTA RECEIVER)



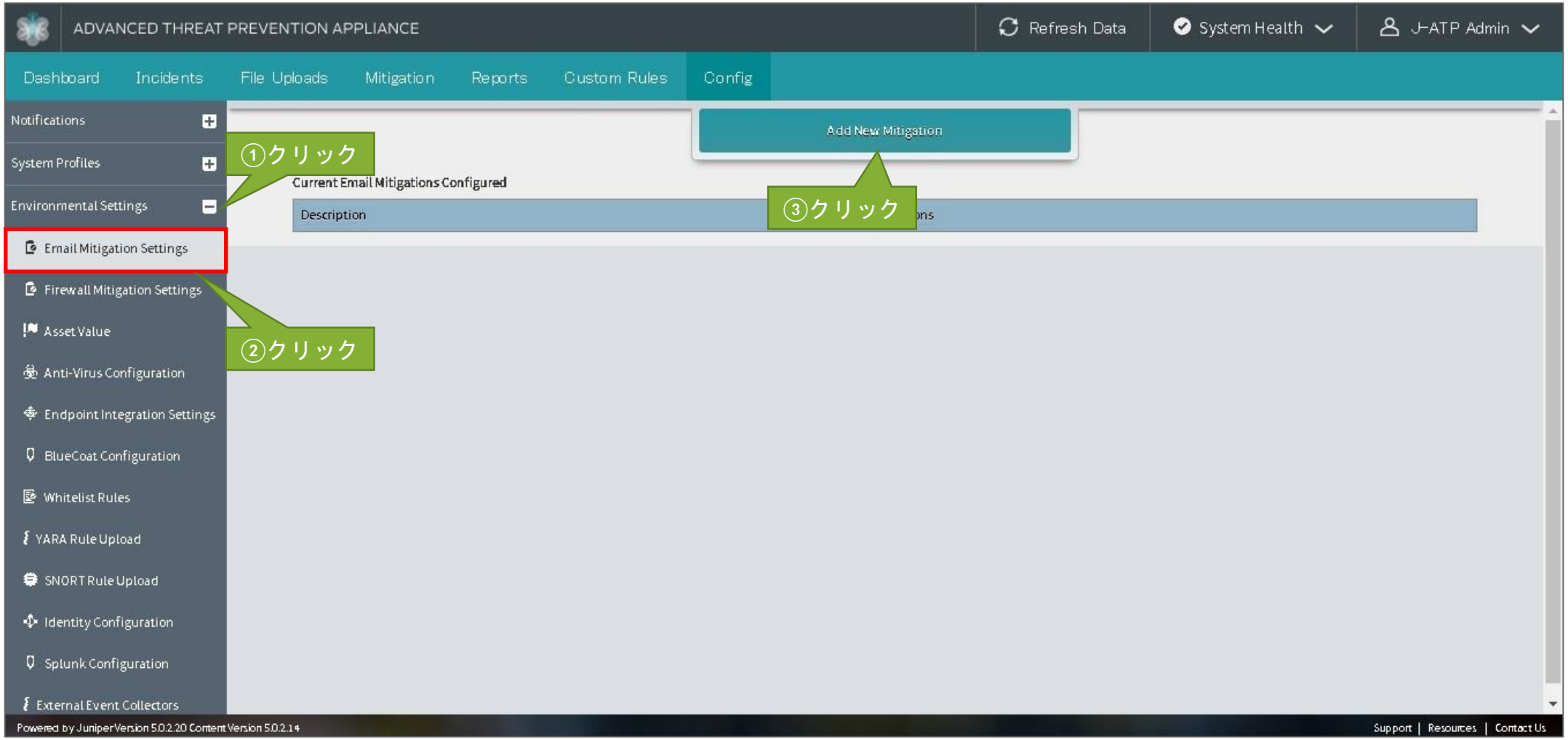
G SUITE MITIGATION設定手順 (BCC,MTA RECEIVER)



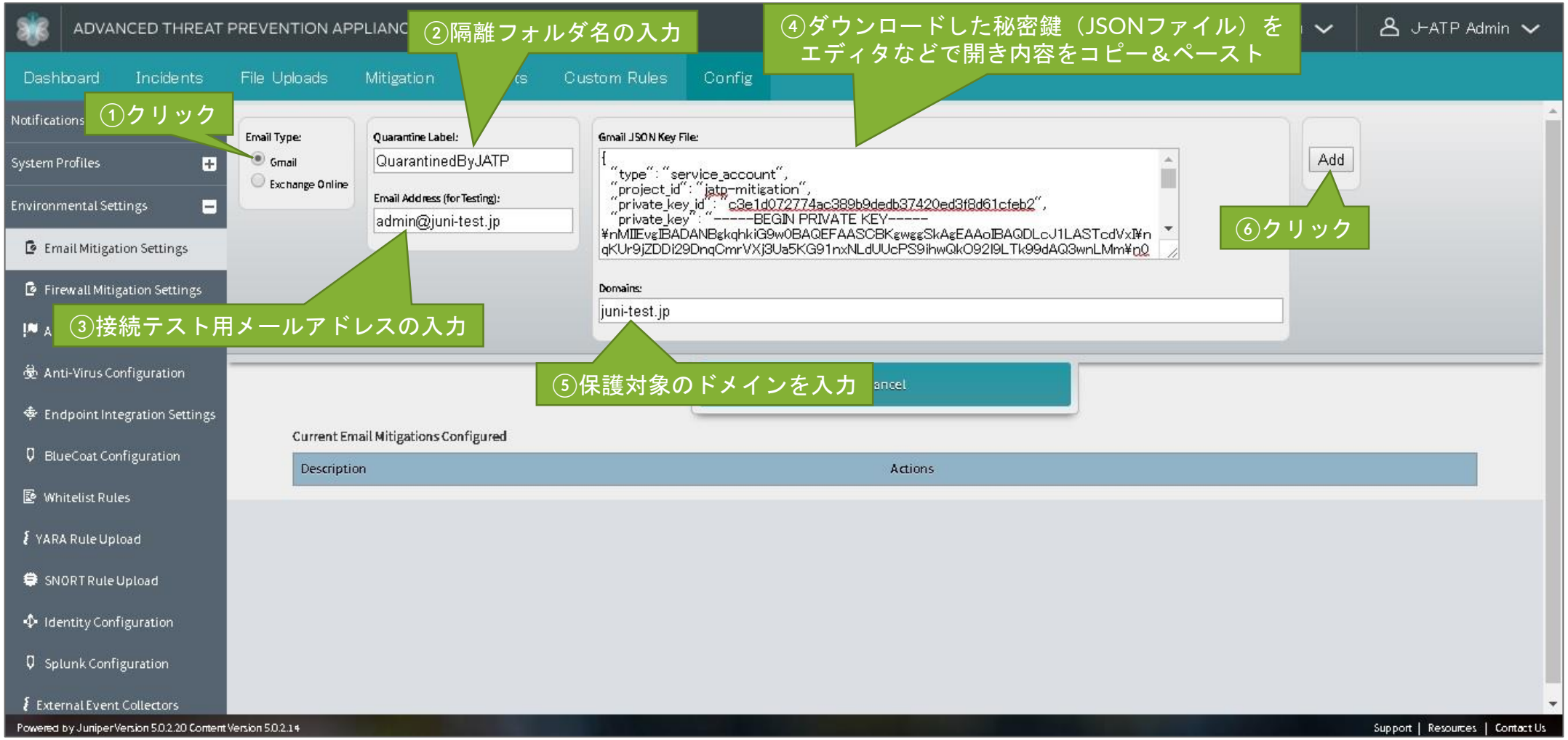
G SUITE MITIGATION設定手順 (BCC,MTA RECEIVER)



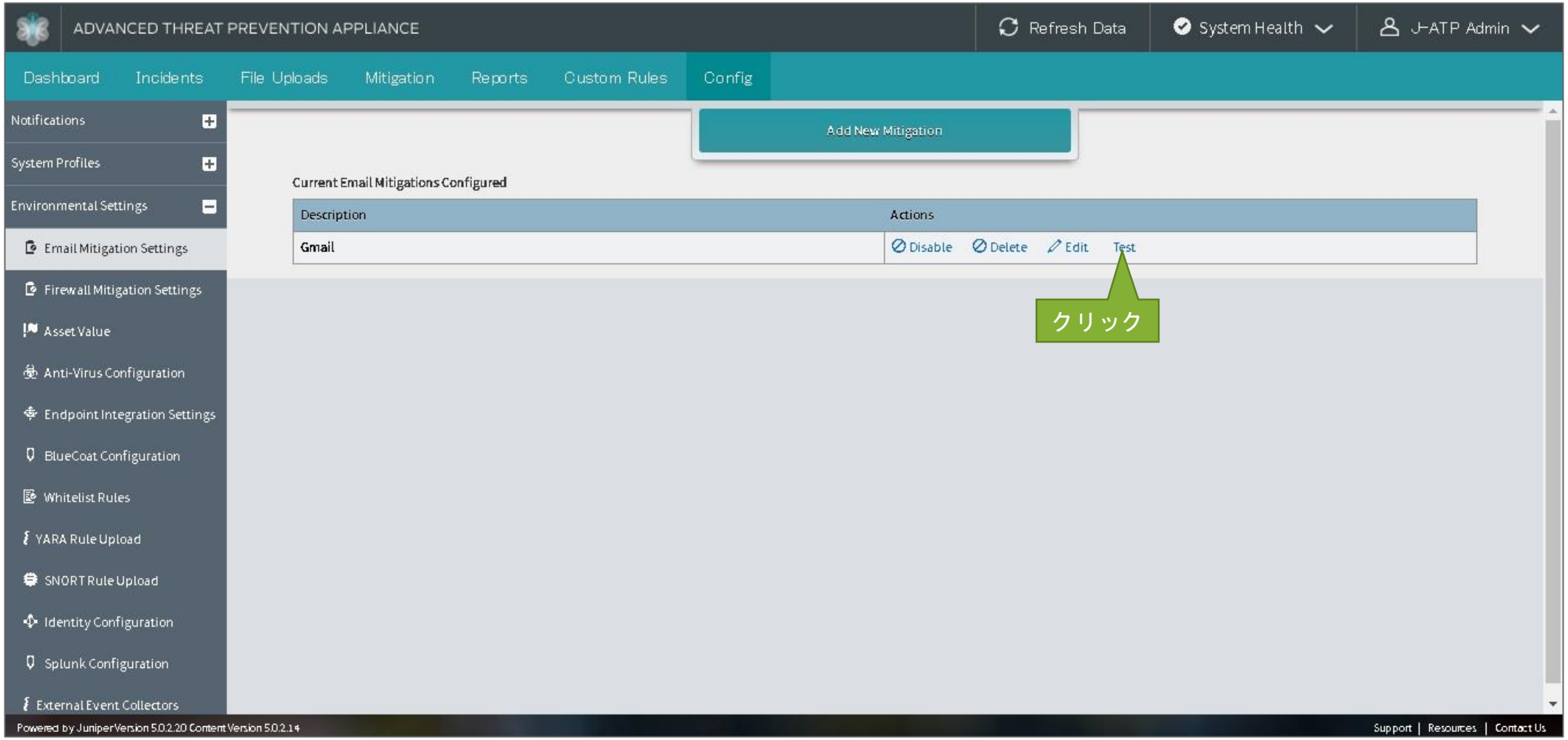
G SUITE MITIGATION設定手順 (BCC,MTA RECEIVER)



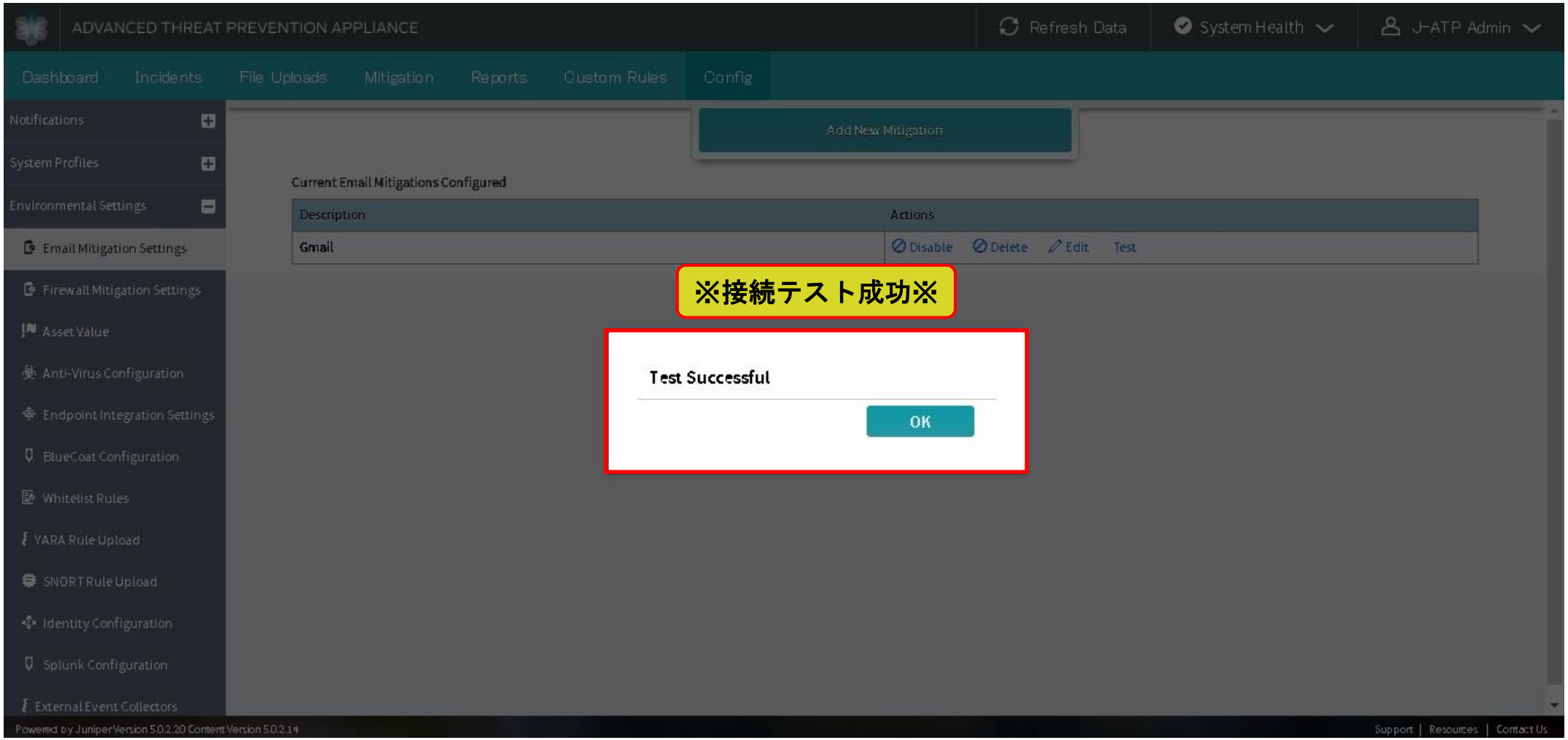
G SUITE MITIGATION設定手順 (BCC,MTA RECEIVER)



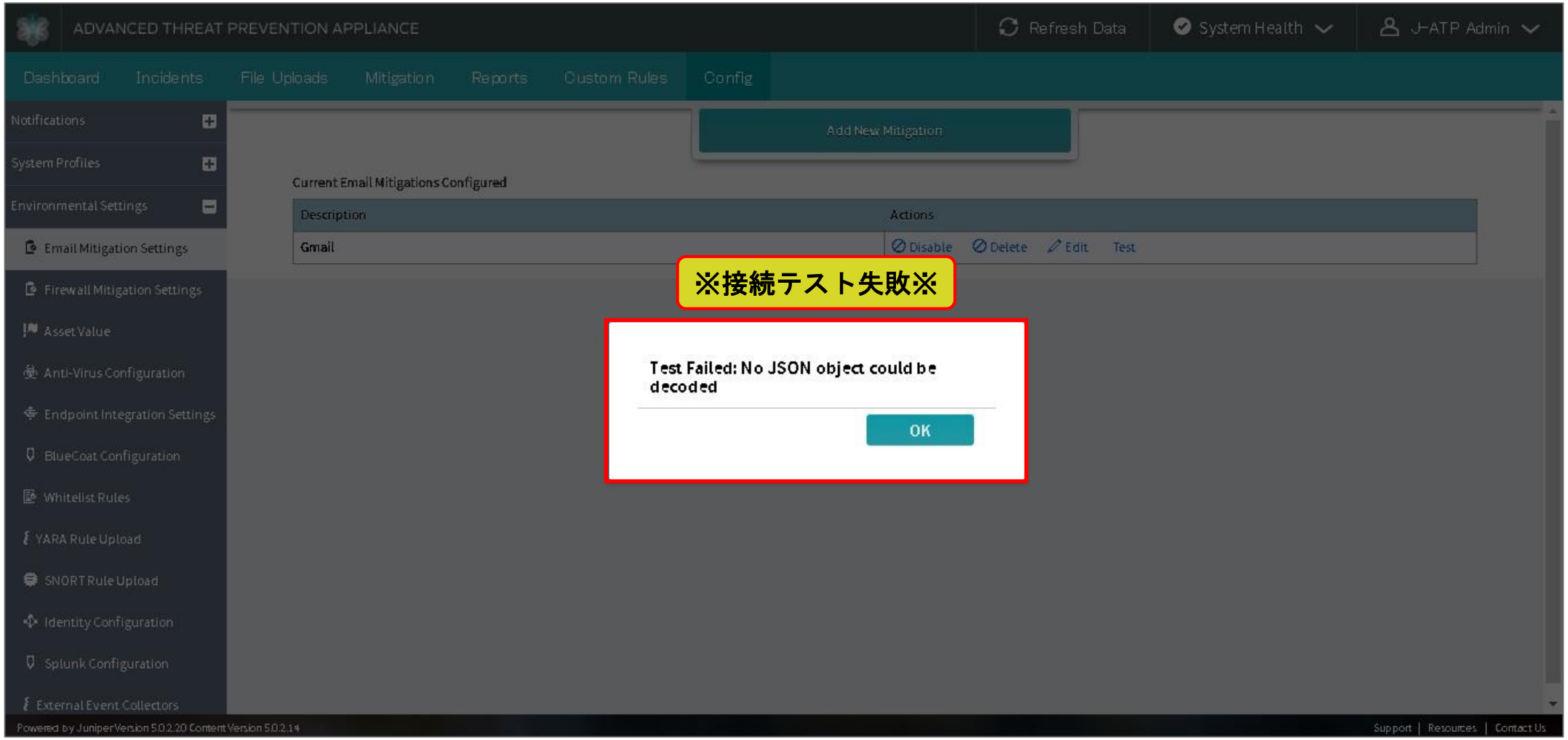
G SUITE MITIGATION設定手順 (BCC,MTA RECEIVER)



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



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

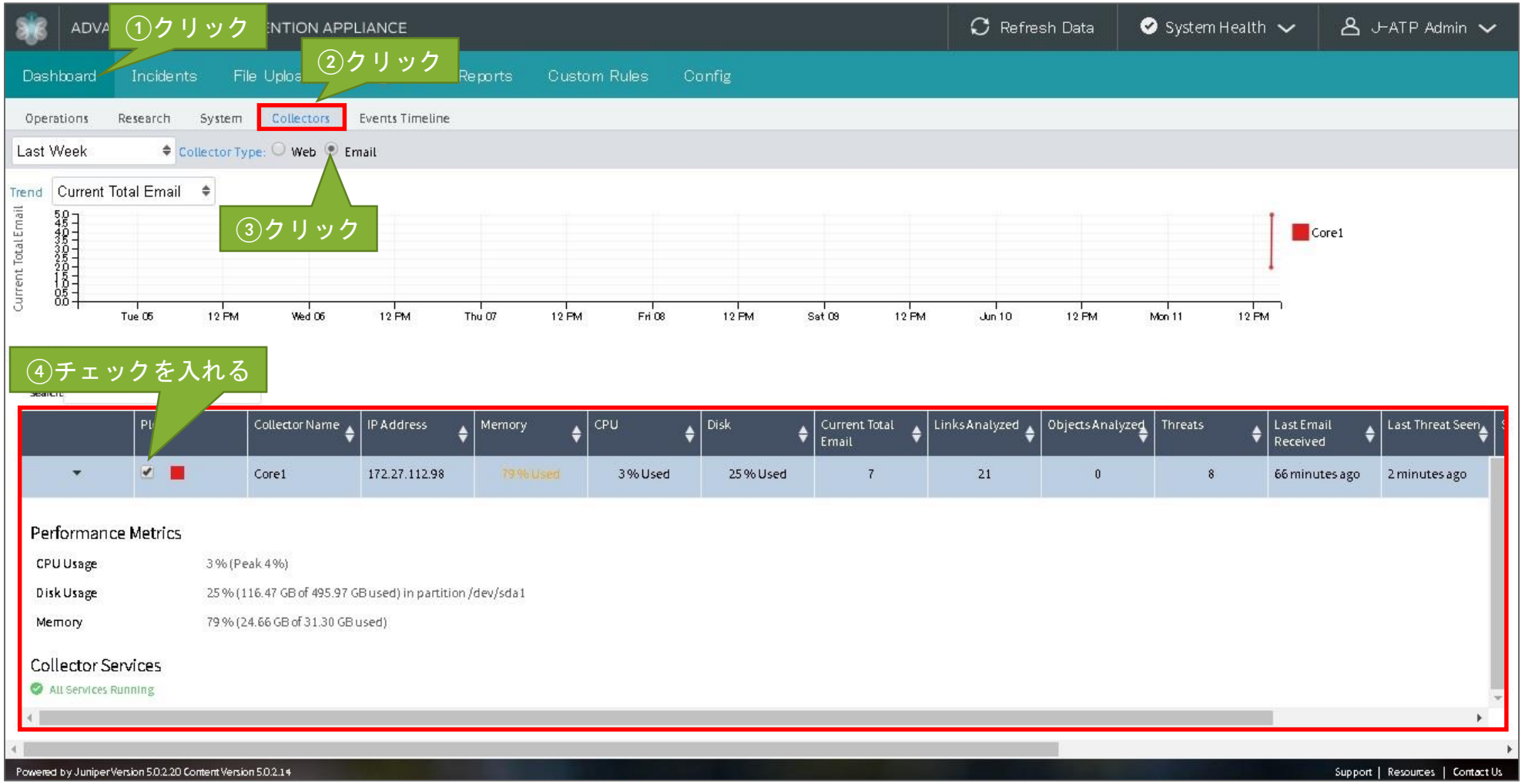


G SUITE MITIGATION設定手順 (BCC,MTA RECEIVER)

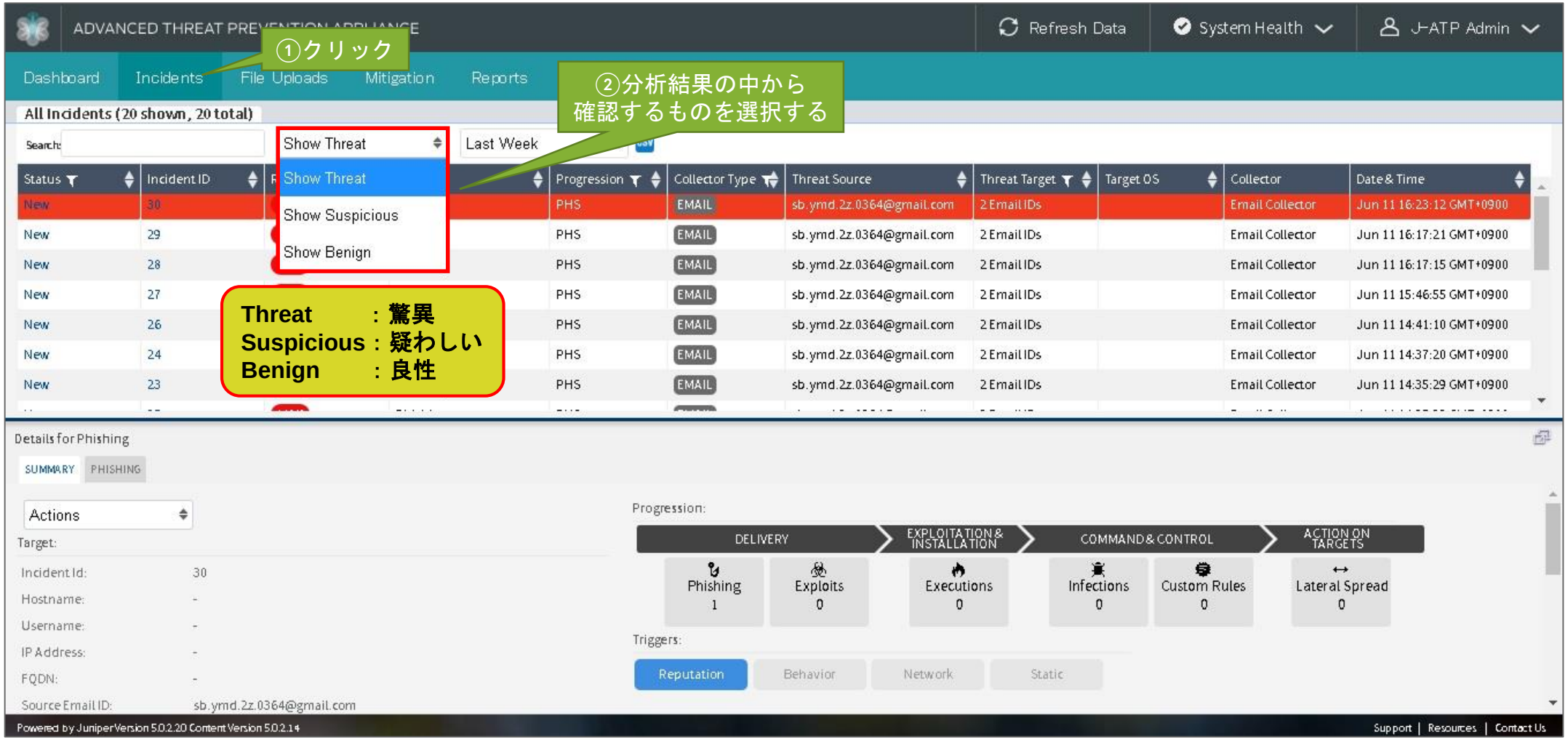
G SUITE MITIGATION設定手順 (BCC,MTA RECEIVER)

Email collector
動作確認手順

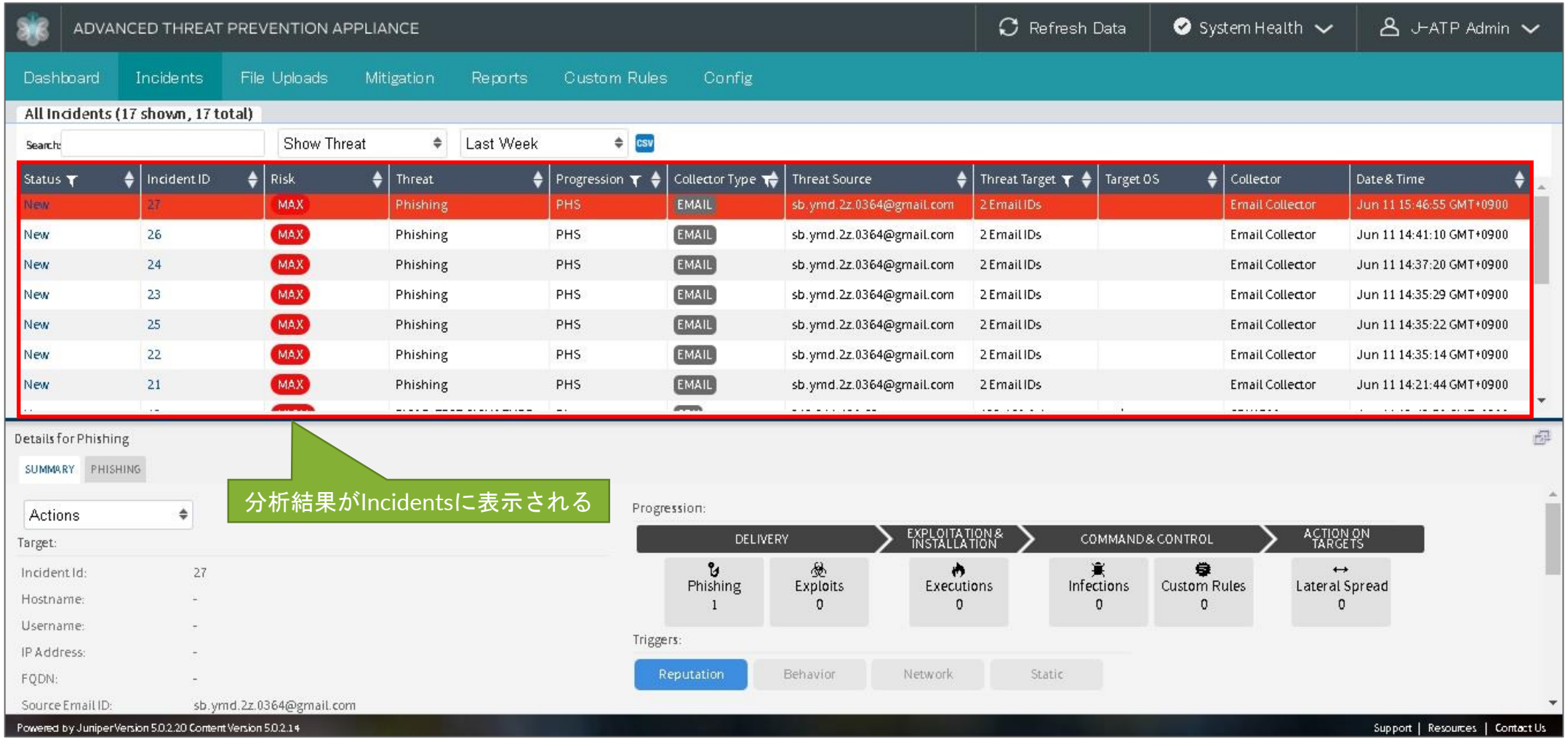
EMAIL COLLECTOR動作確認手順



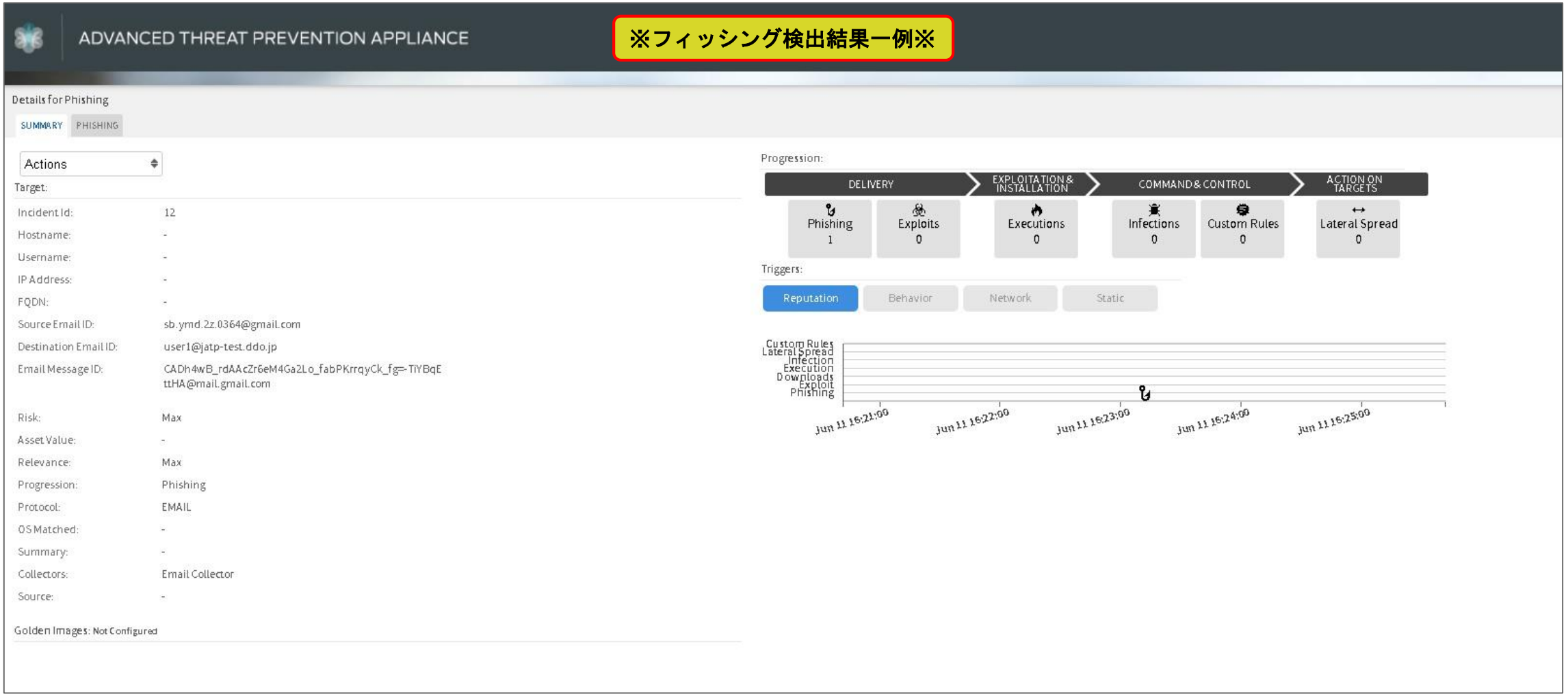
EMAIL COLLECTOR動作確認手順



EMAIL COLLECTOR動作確認手順



EMAIL COLLECTOR動作確認手順




THANK YOU
JUNIPER NETWORKS
Engineering
Simplicity