



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)

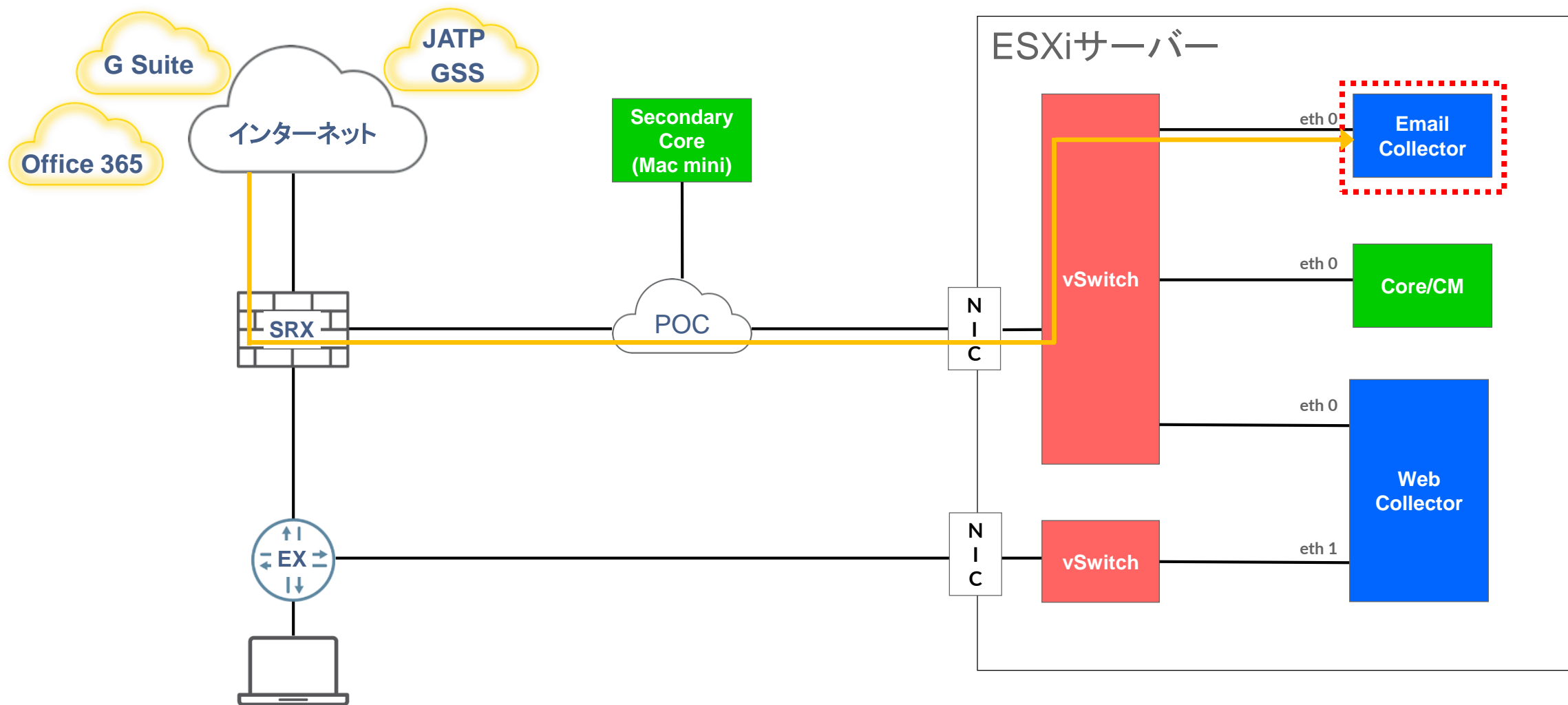
更新履歴

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

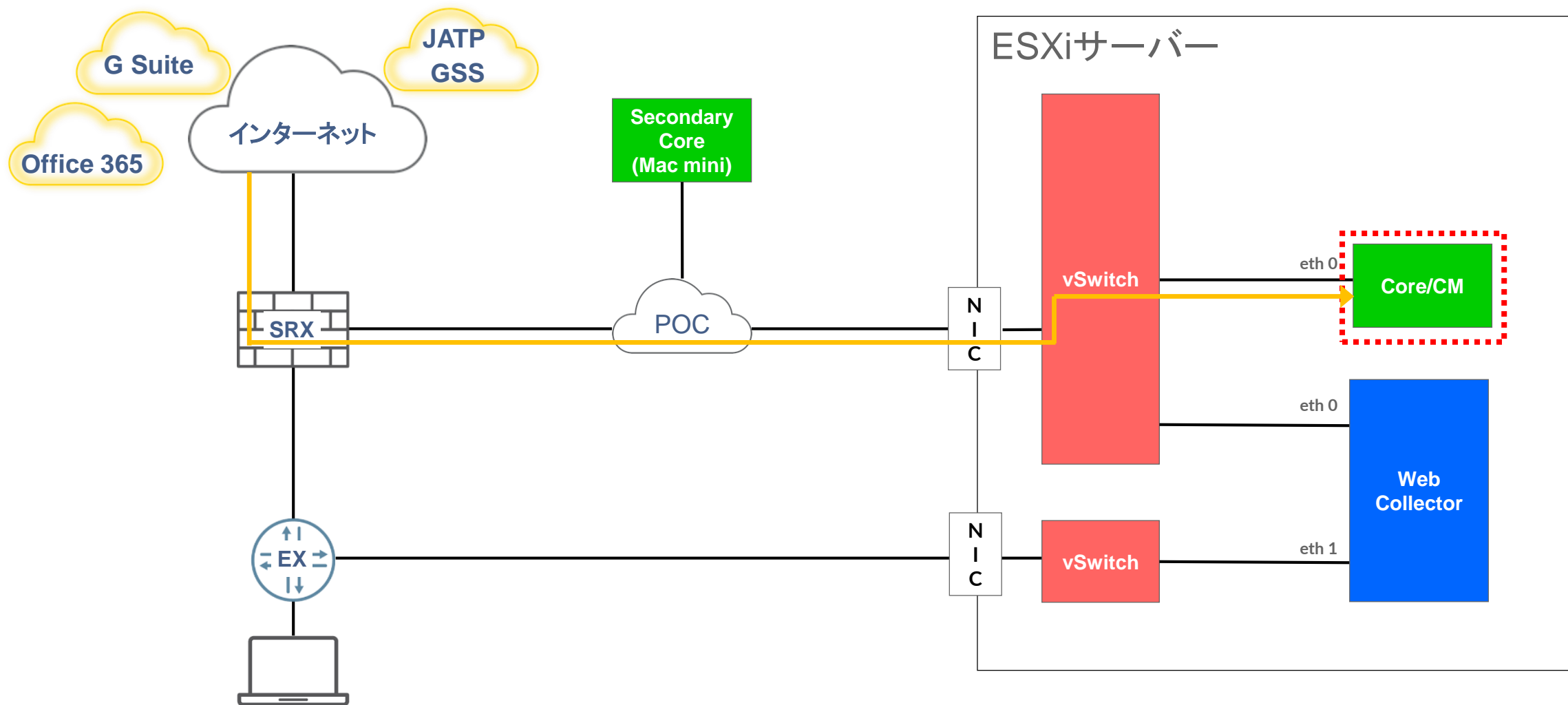
アジェンダ

- 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	スタンダードライセンスで対応 (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



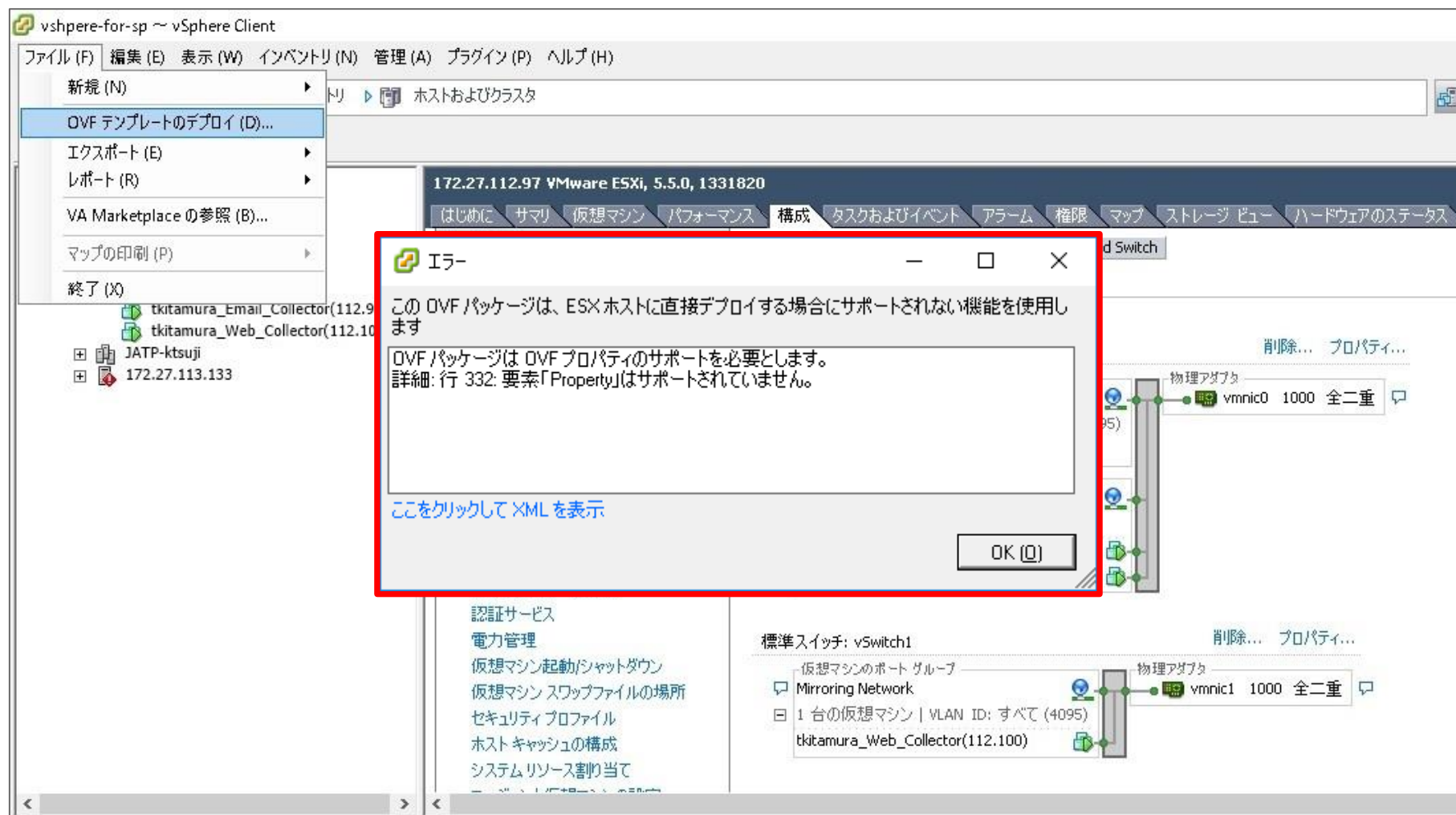
仮想サーバー設定手順 OVAファイル

仮想サーバー設定手順(OVAファイル)

The screenshot shows the vSphere Client interface with the following components:

- Left Panel (Inventory):** A tree view showing the hierarchy: vshpere-for-sp > JAPAN-POC-SP-SE > DELL Servers Cluster > 172.27.112.97. The IP address 172.27.112.97 is highlighted with a green callout box.
- Top Panel (Hardware):** A list of hardware components including プロセッサ, メモリ, ストレージ, ネットワーク, ストレージ アダプタ, ネットワーク アダプタ, 詳細設定, and 電力管理.
- Right Panel (Network):** A diagram showing the network configuration. It includes a 'Management Network' with a VMkernel port (vmk0) connected to a physical adapter (vmnic0). The IP address 172.27.112.97 is associated with vmk0. Below this, a 'JATPネットワーク' is shown with two virtual machines connected to it.
- Callouts:**
 - A green callout box points to the IP address 172.27.112.97 in the inventory, containing the text: "vCenter ServerからESXi上で仮想サーバーを構築する物理サーバーを選択".
 - A yellow starburst callout box contains the text: "※注意※ vCenter Server以外からデプロイするとエラーが発生する (次ページ参照)".

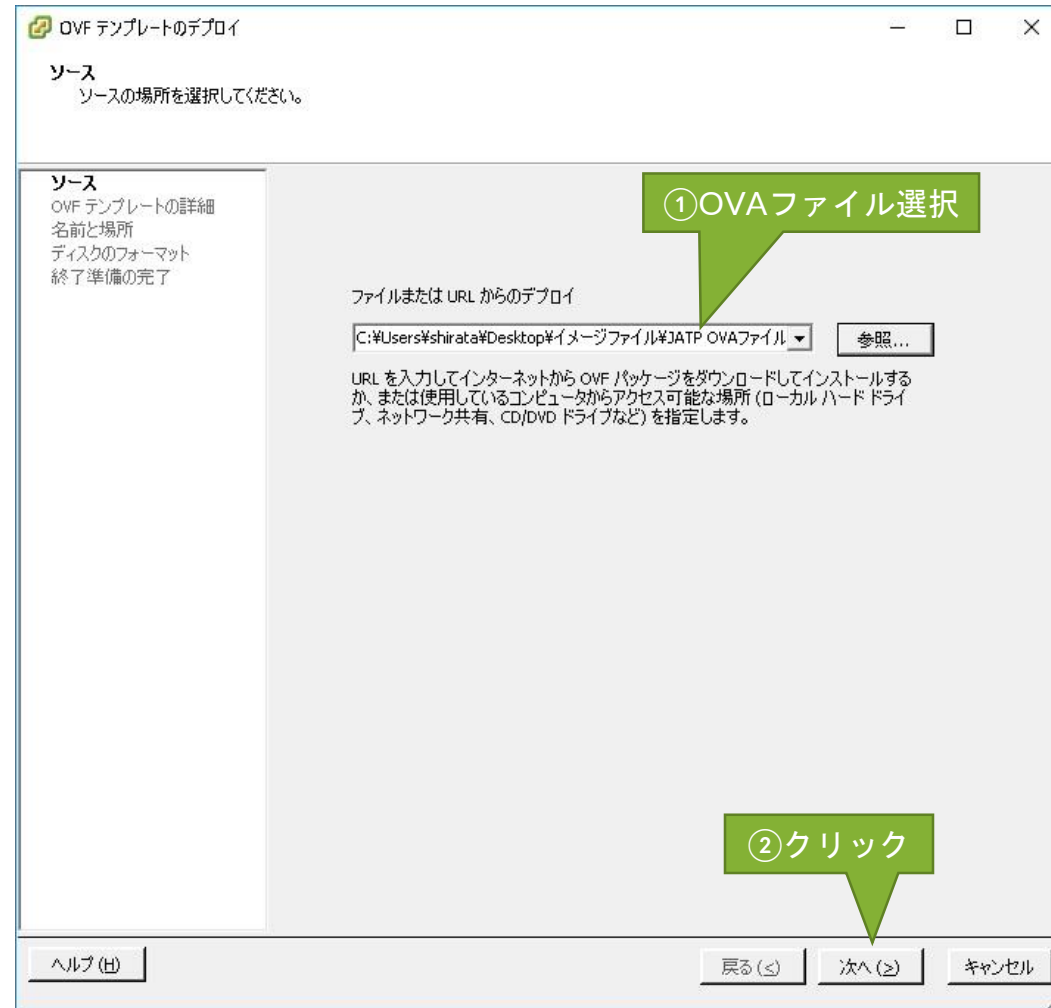
仮想サーバー設定手順(OVAファイル) エラー表示一例



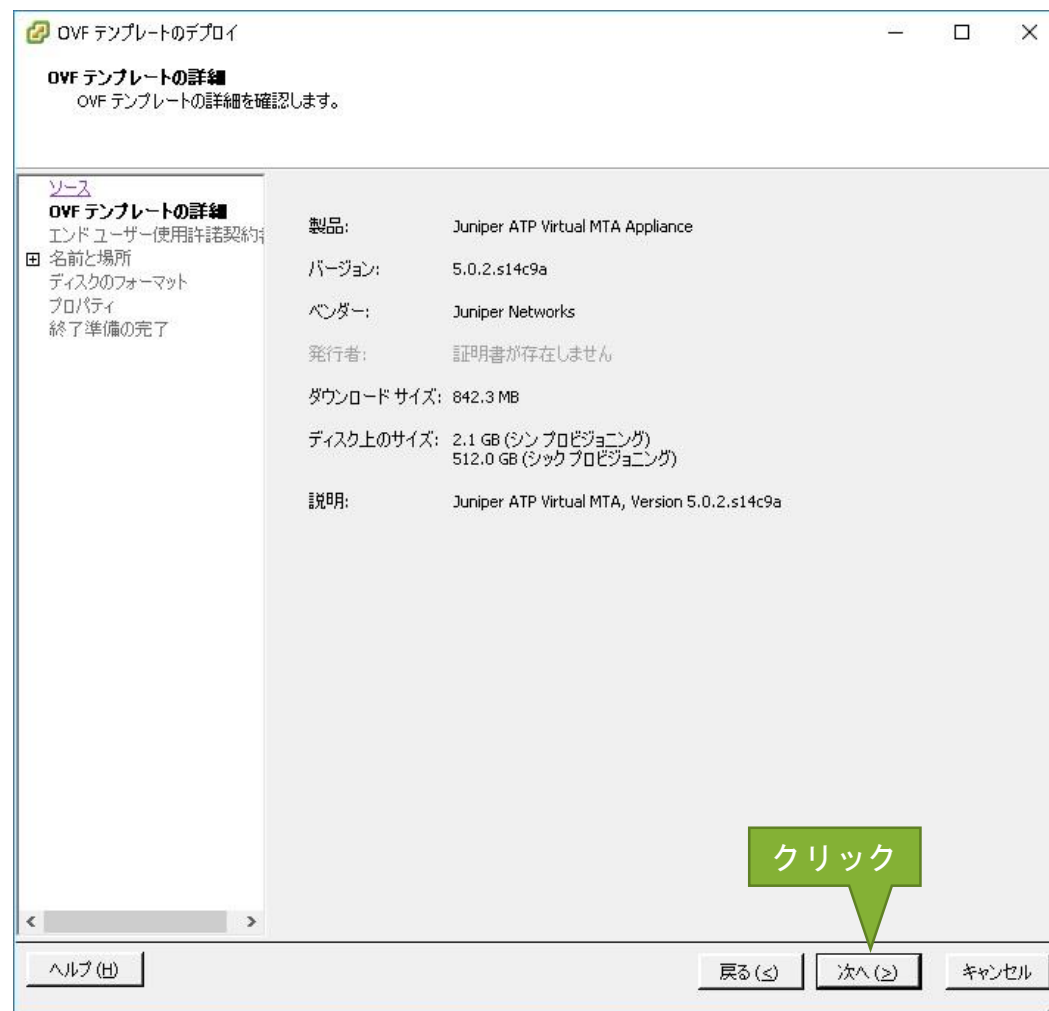
仮想サーバー設定手順(OVAファイル)



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)

OVF テンプレートのデプロイ

名前と場所
デプロイされたテンプレートの名前と場所を指定します

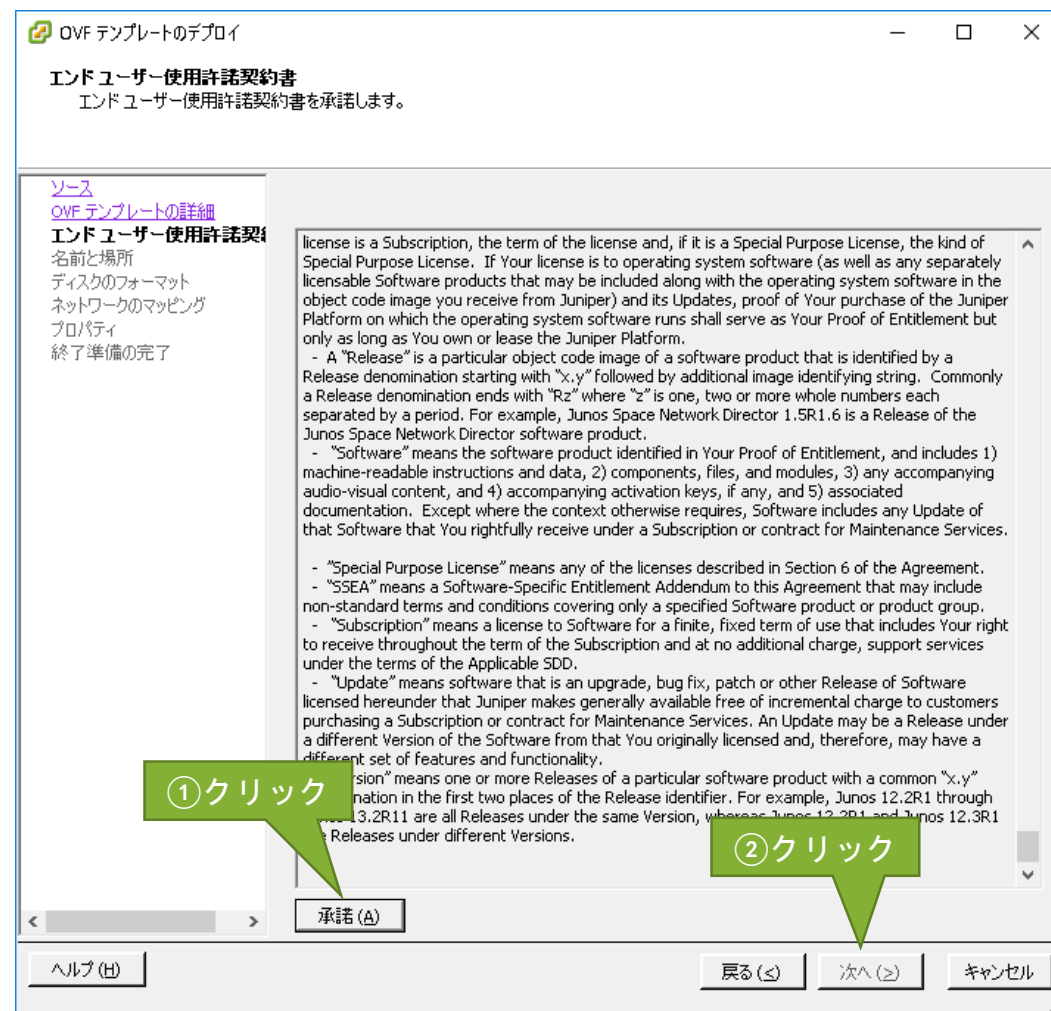
ソース
OVF テンプレートの詳細
エンド ユーザー使用許諾契約
名前と場所
ディスクのフォーマット
ネットワークのマッピング
プロパティ
終了準備の完了

名前:
Juniper ATP Virtual MTA Appliance
名前は最大 80 文字で設定できますが、各インベントリのフォルダ内で一意でなければなりません。

インベントリの場所:
JAPAN-POC-SP-SE
Discovered virtual machine

ヘルプ (H) 戻る (←) 次へ (→) キャンセル

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)

The screenshot shows the 'Disk Format' step of the OVF Template Deployment Wizard. The window title is 'OVF テンプレートのデプロイ'. The main heading is 'ディスクのフォーマット' with the subtext '仮想ディスクはどのフォーマットで保存しますか?'. On the left, a navigation pane lists steps: ソース, OVF テンプレートの詳細, エンド ユーザー使用許諾契約, 名前と場所, ディスクのフォーマット (selected), ネットワークのマッピング, プロパティ, and 終了準備の完了. The main area shows 'データストア: datastore1' and '使用可能な容量 (GB): 615.6'. Three radio buttons are available: 'シック プロビジョニング (Lazy Zeroed)' (selected and highlighted with a red box), 'シック プロビジョニング (Eager Zeroed)', and 'Thin Provision'. A green callout box with an arrow points to the 'Thin Provision' option, containing the text '①サーバーの物理リソースに応じて適切なものを選択 推奨 : Thin Provision'. At the bottom right, another green callout box with an arrow points to the '次へ (N)' button, containing the text '②クリック'. The bottom of the window has buttons for 'ヘルプ (H)', '戻る (P)', '次へ (N)', and 'キャンセル'.

OVF テンプレートのデプロイ

ディスクのフォーマット
仮想ディスクはどのフォーマットで保存しますか?

ソース
OVF テンプレートの詳細
エンド ユーザー使用許諾契約
名前と場所
ディスクのフォーマット
ネットワークのマッピング
プロパティ
終了準備の完了

データストア: datastore1
使用可能な容量 (GB): 615.6

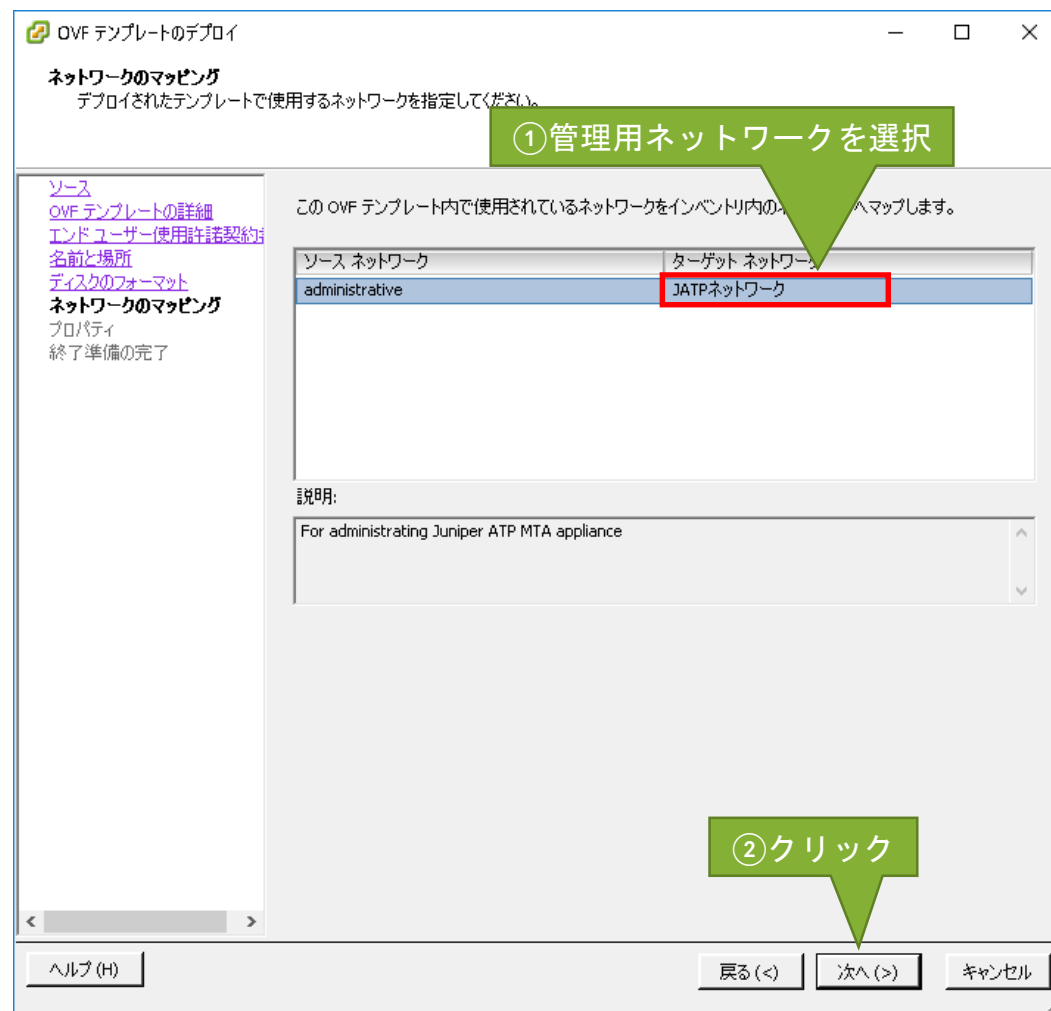
☒ シック プロビジョニング (Lazy Zeroed)
☐ シック プロビジョニング (Eager Zeroed)
☐ Thin Provision

①サーバーの物理リソースに応じて適切なものを選択
推奨 : Thin Provision

②クリック

ヘルプ (H) 戻る (P) 次へ (N) キャンセル

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 <div>DHCP</div> DHCP / Staticを選択
IP address Ignore this property if the IP allocation policy is DHCP. <div>0 . 0 . 0 . 0</div> 仮想サーバーのIPアドレスの設定
Netmask Ignore this property if the IP allocation policy is DHCP. <div>255 . 255 . 255 . 255</div> サブネットマスクの設定
Gateway Ignore this property if the IP allocation policy is DHCP. <div>0 . 0 . 0 . 0</div> ゲートウェイの設定
DNS address 1 Ignore this property if the IP allocation policy is DHCP. <div>0 . 0 . 0 . 0</div> DNS1の設定
DNS address 2 Ignore this property if the IP allocation policy is DHCP. <div>0 . 0 . 0 . 0</div> DNS2の設定(任意)
Search domain Multiple search domains separated by space. <div></div> 検索用ドメイン名の設定(任意)
Hostname <div></div> <small>1 から 255 の文字の文字列の値を入力してください。</small> 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

パスワードの確認

Juniper ATP Central Manager IP address

IP アドレスを入力します。

Device name

1 から 255 の文字の文字列の値を入力してください。

Device description

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

パスワードの確認

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。

.....

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

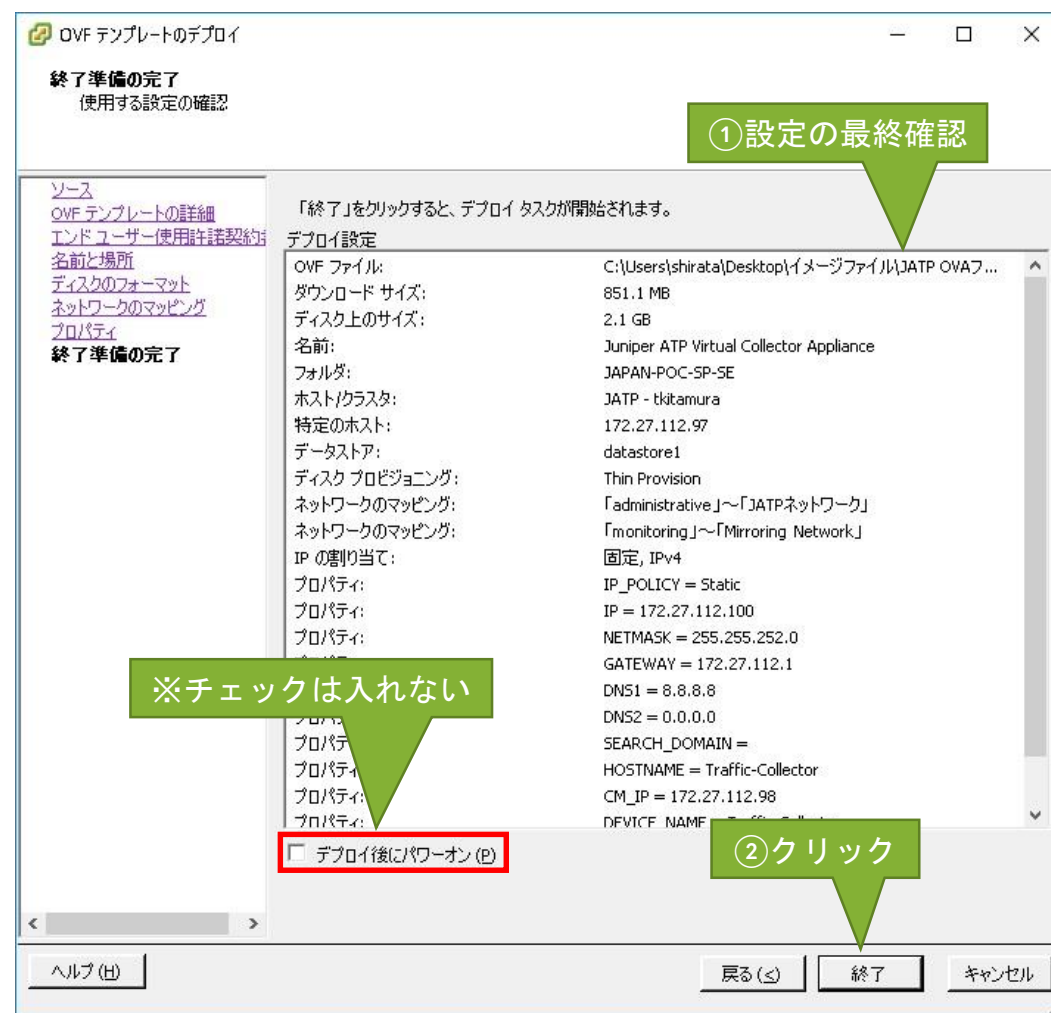
.....

デバイスの説明

.....

接続するCore,Collectorで
すべて共通の値を入力

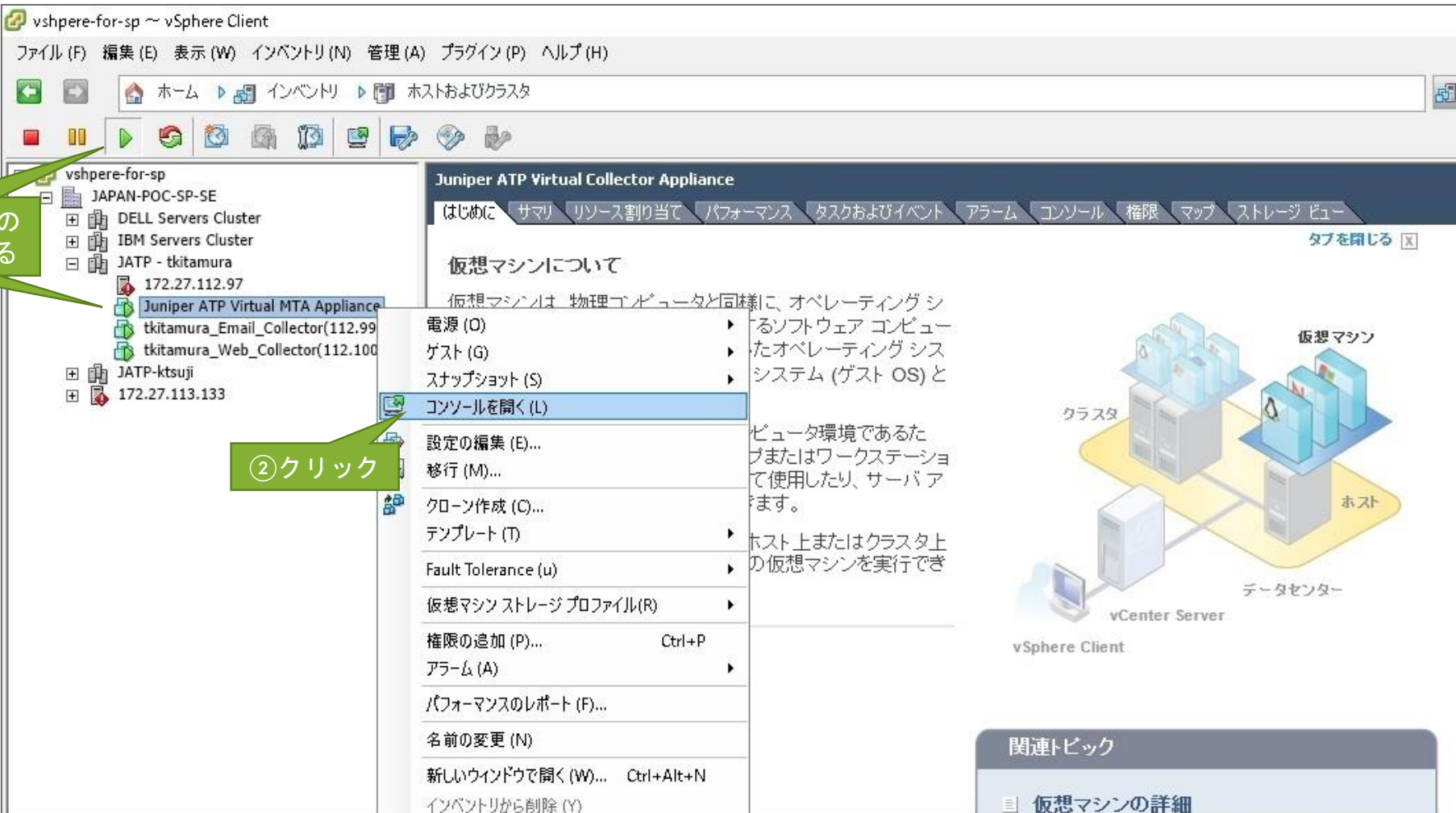
仮想サーバー設定手順(OVAファイル)



仮想サーバー設定手順(OVAファイル)

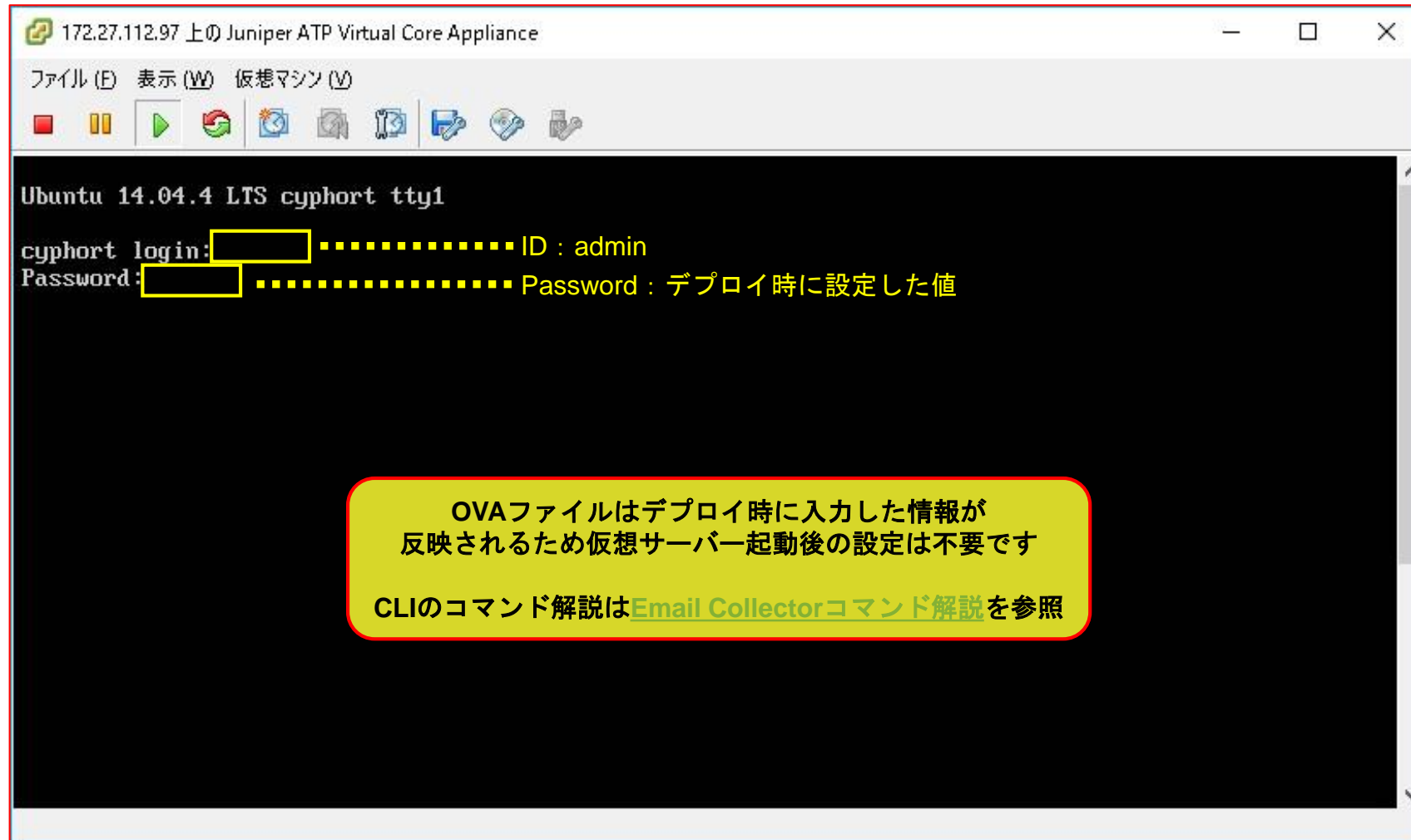
①仮想サーバーの電源をオンにする

②クリック



The screenshot shows the vSphere Client interface. On the left, the inventory tree lists several virtual machines, including 'Juniper ATP Virtual MTA Appliance'. A green callout points to this VM with the text '①仮想サーバーの電源をオンにする'. The main pane shows the 'Juniper ATP Virtual Collector Appliance' details. A context menu is open over the VM, with '電源 (O)' (Power) selected. A green callout points to the '電源' menu with the text '②クリック'. The '電源' menu includes options like '電源 (O)', 'ゲスト (G)', 'スナップショット (S)', 'コンソールを開く (L)', '設定の編集 (E)...', '移行 (M)...', 'クローン作成 (C)...', 'テンプレート (T)', 'Fault Tolerance (u)', '仮想マシンストレージプロファイル (R)', '権限の追加 (P)...', 'アラーム (A)', 'パフォーマンスのレポート (F)...', '名前の変更 (N)', '新しいウィンドウで開く (W)...', and 'インベントリから削除 (Y)'. The right pane shows the '仮想マシンについて' (About this virtual machine) tab, which contains text about virtual machines and their operation. Below the main pane, there is a diagram of a data center architecture showing a 'vCenter Server' connected to a 'vSphere Client' and a 'ホスト' (Host) containing a 'クラスタ' (Cluster) of virtual machines. A '仮想マシン' (Virtual Machine) is also shown. The bottom right corner has a '関連トピック' (Related topics) section with a link to '仮想マシンの詳細' (Virtual machine details).

仮想サーバー設定手順(OVAファイル)



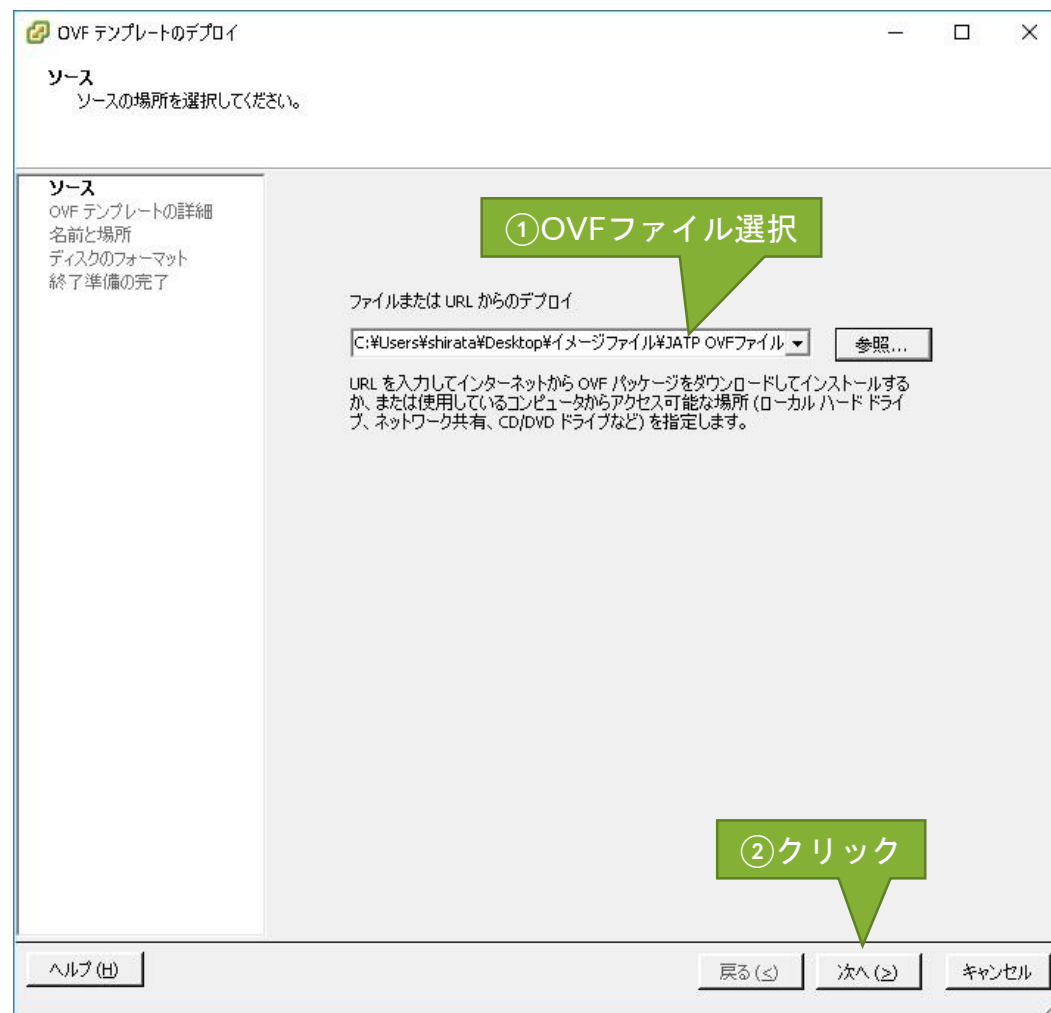


仮想サーバー設定手順 OVFファイル

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)

OVF テンプレートのデプロイ

名前と場所
デプロイされたテンプレートの名前と場所を指定します

ソース
OVF テンプレートの詳細
名前と場所
ディスクのフォーマット
ネットワークのマッピング
終了準備の完了

名前:
Juniper ATP Virtual MTA Appliance
名前は最大 80 文字で設定できますが、各インベントリのフォルダ内で一意でなければなりません。

インベントリの場所:
JAPAN-POC-SP-SE
Discovered virtual machine

ヘルプ (H) 戻る (←) 次へ (→) キャンセル

仮想サーバー設定手順(OVFファイル)

OVF テンプレートのデプロイ

ディスクのフォーマット
仮想ディスクはどのフォーマットで保存しますか?

ソース
OVF テンプレートの詳細
名前と場所
ディスクのフォーマット
ネットワークのマッピング
終了準備の完了

データストア: datastore1
使用可能な容量 (GB): 1257.8

☐ シック プロビジョニング (Lazy Zeroed)
☐ シック プロビジョニング (Eager Zeroed)
☒ Thin Provision

①サーバーの物理リソースに応じて適切なものを選択
推奨: Thin Provision

②クリック

ヘルプ (H) 戻る (L) 次へ (N) キャンセル

仮想サーバー設定手順(OVFファイル)

OVF テンプレートのデプロイ

ネットワークのマッピング
デプロイされたテンプレートで使用するネットワークを指定してください。

①管理用ネットワークを選択

ソース ネットワーク ターゲット ネットワーク

administrative	JATPネットワーク
----------------	------------

説明:
For administrating Juniper ATP MTA appliance

ヘルプ (H) 戻る (<) 次へ (>) キャンセル

仮想サーバー設定手順(OVFファイル)

OVF テンプレートのデプロイ

終了準備の完了
使用する設定の確認

① 設定の最終確認

ソース
OVF テンプレートの詳細
名前と場所
ディスクのフォーマット
ネットワークのマッピング
終了準備の完了

「終了」をクリックすると、デプロイ タスクが開始されます。

デプロイ設定

OVF ファイル:	C:\Users\shirata\Desktop\イメージファイル\JATP ver 5.0.2\...
ダウンロード サイズ:	905.4 MB
ディスク上のサイズ:	不明
名前:	Juniper ATP Virtual MTA Appliance
フォルダ:	JAPAN-POC-SP-SE
ホスト/クラス:	JATP - tkitamura
特定のホスト:	172.27.112.97
データストア:	datastore1
ディスク プロビジョニング:	Thin Provision
ネットワークのマッピング:	「administrative」～「JATPネットワーク」

※チェックは入れない

☐ デプロイ後にパワーオン (P)

② クリック

ヘルプ (H) 戻る (L) 終了 キャンセル

仮想サーバー設定手順(OVFファイル)

①仮想サーバーの電源をオンにする

②クリック

The screenshot shows the vSphere Client interface. The left pane displays the inventory tree with the following structure:

- vshpere-for-sp ~ vSphere Client
 - JAPAN-POC-SP-SE
 - DELL Servers Cluster
 - IBM Servers Cluster
 - JATP - tkitamura
 - 172.27.112.97
 - Juniper ATP Virtual MTA Appliance
 - tkitamura_Email_Collector(112.99)
 - tkitamura_Web_Collector(112.100)
 - JATP-ktsuji
 - 172.27.113.133

The right pane shows the 'Juniper ATP Virtual Collector Appliance' details. The '電源' (Power) menu is open, and the '電源をオンにする' (Power On) option is selected. The menu options are:

- 電源 (O)
- ゲスト (G)
- スナップショット (S)
- コンソールを開く (L)
- 設定の編集 (E)...
- 移行 (M)...
- クローン作成 (C)...
- テンプレート (T)
- Fault Tolerance (u)
- 仮想マシンストレージプロファイル(R)
- 権限の追加 (P)...
- アラーム (A)
- パフォーマンスのレポート (F)...
- 名前の変更 (N)
- 新しいウィンドウで開く (W)...
- インベントリから削除 (Y)

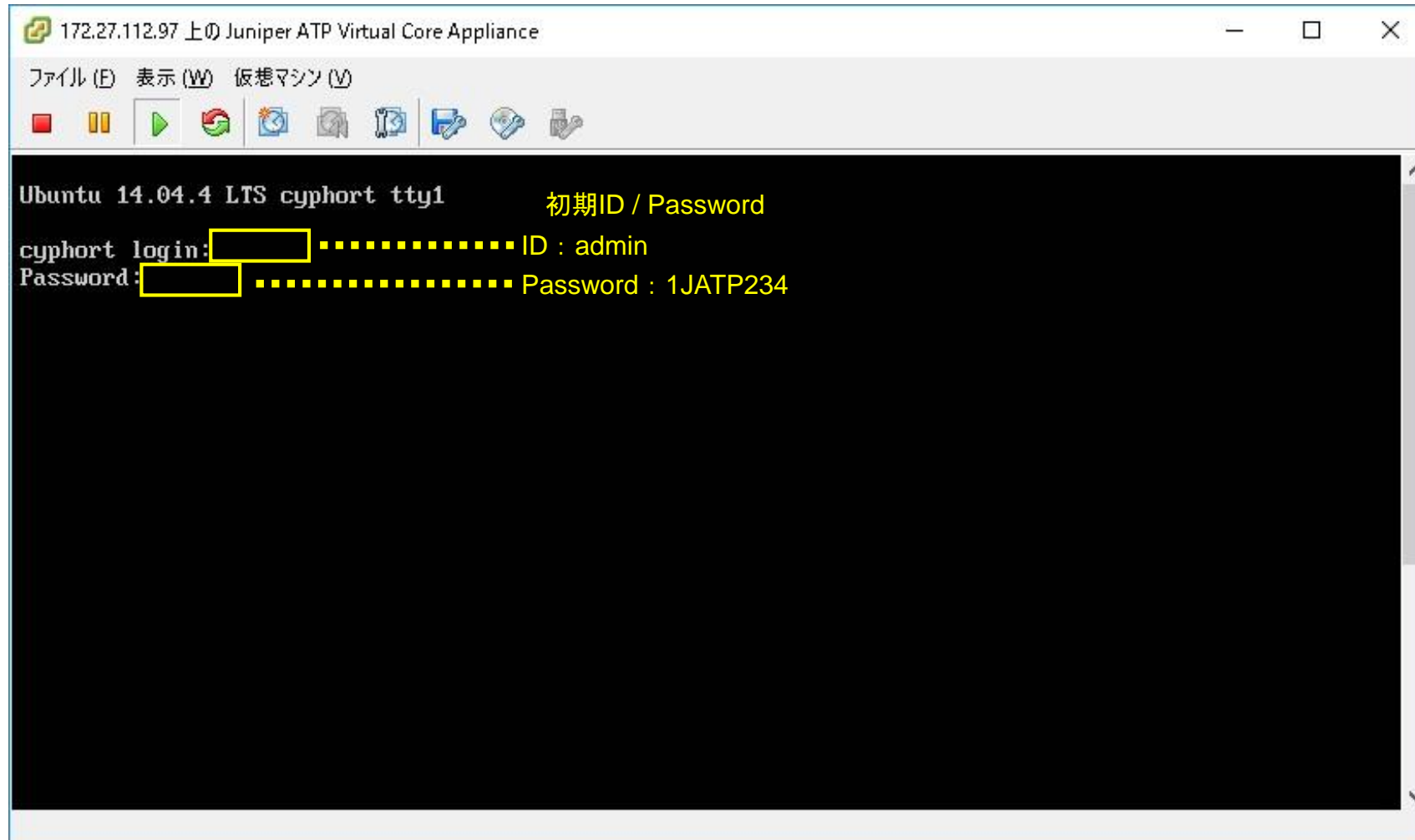
The diagram on the right illustrates the architecture:

- クラスタ (Cluster)
- 仮想マシン (Virtual Machine)
- ホスト (Host)
- データセンター (Data Center)
- vCenter Server
- vSphere Client

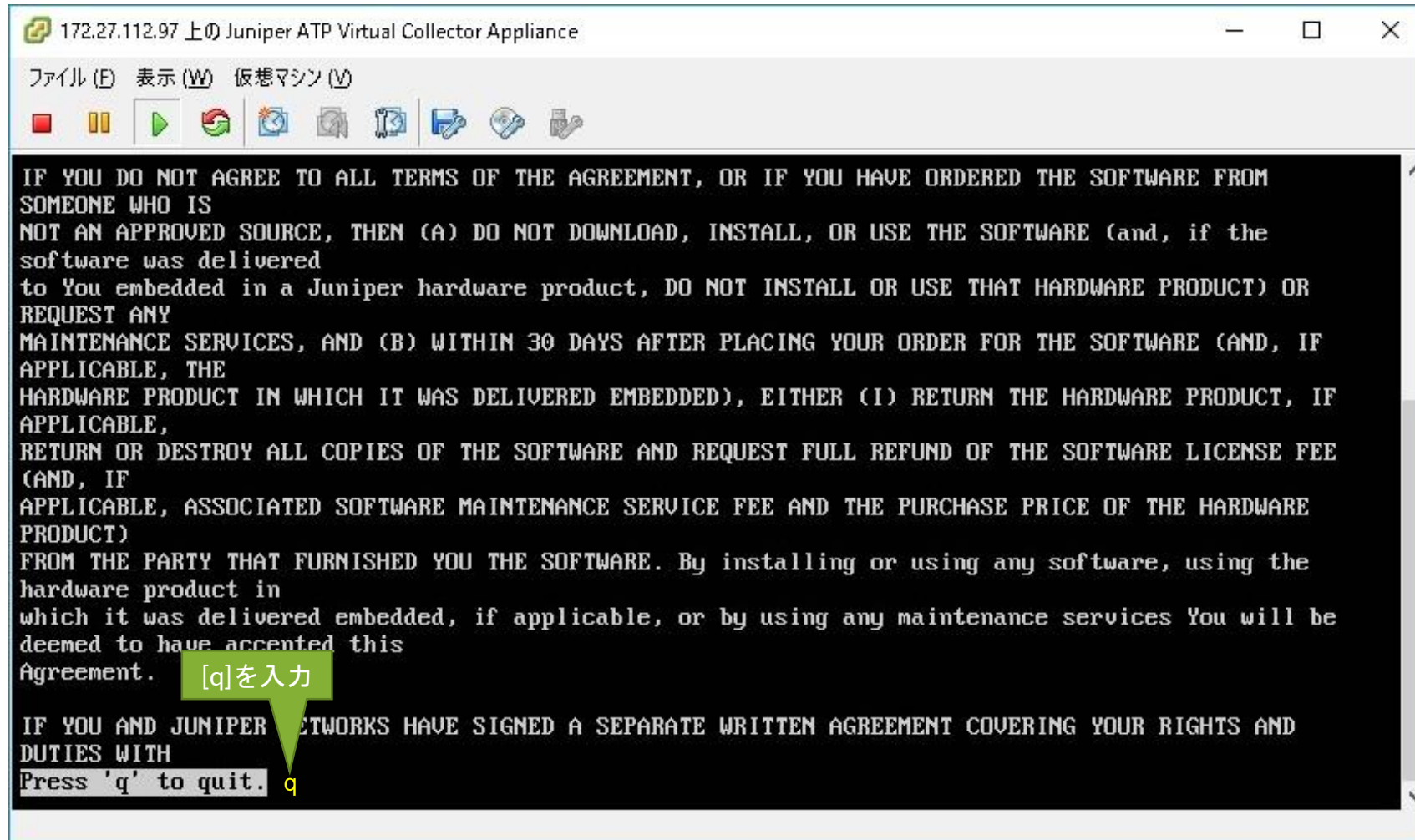
関連トピック (Related Topics):

- 仮想マシンの詳細 (Virtual Machine Details)

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と共通のキープレーズを入力
```

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 コマンドー例

EMAIL COLLECTORコマンド例

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 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 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
```

- ・ キャプチャーファイルのコピー

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

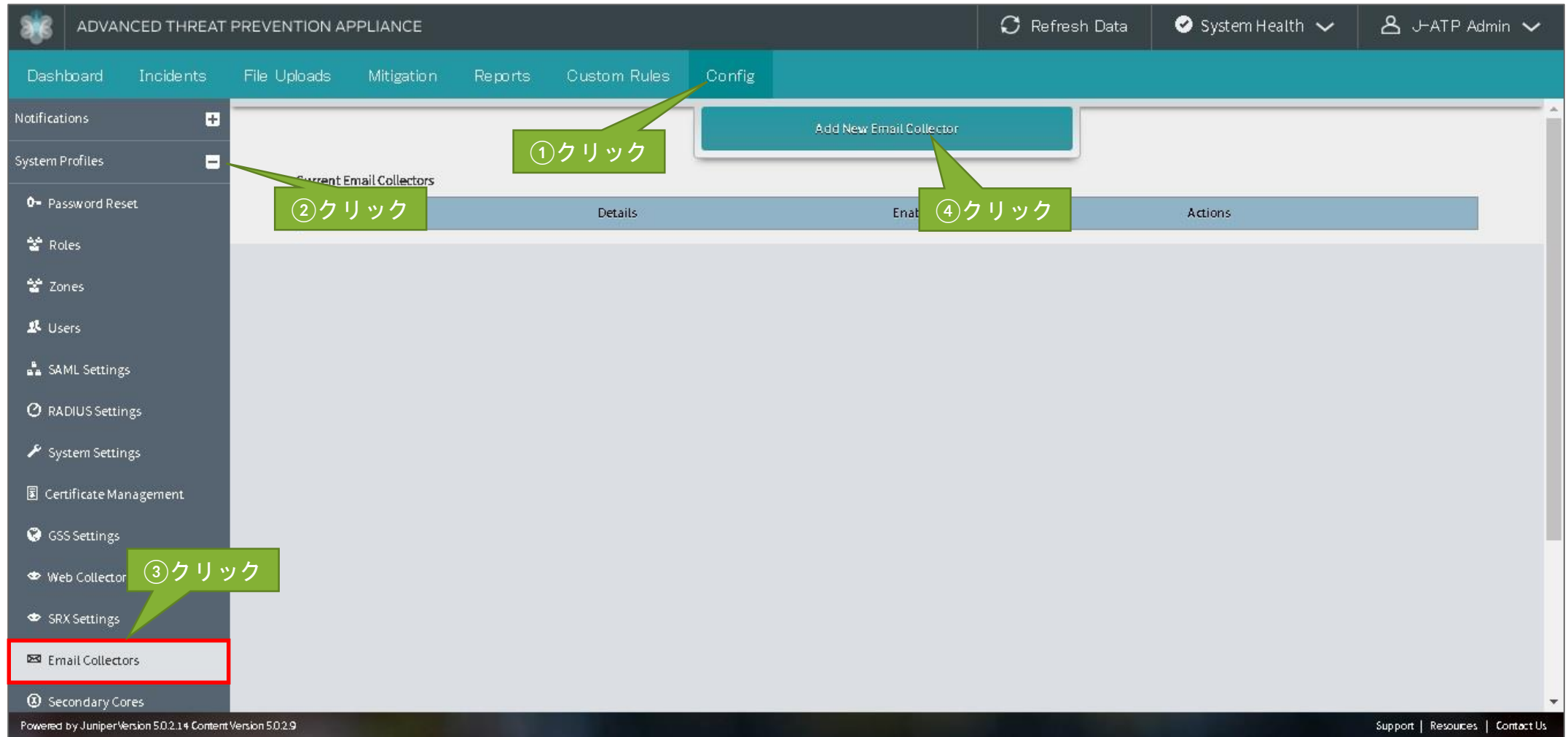


Email Collector設定手順 (BCC)

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)

①クリック

②受信メールサーバーを指定

③プロトコルを選択

④クリック

⑤Journalingの送り先メールアドレスとパスワード

⑥mitigation対象となるドメイン（オプション）

⑦ポーリング間隔の指定（デフォルト：5分）

⑧Journalingを保存するか削除するか選択

⑨クリック

⑩クリック

Capture Method	Details	Enabled	Actions
BCC		Enabled	



Email Collector設定手順 (MTA Receiver)

EMAIL COLLECTOR設定手順 (MTA RECEIVER)

The screenshot displays the configuration interface of the Advanced Threat Prevention Appliance (ATP). The top navigation bar includes tabs for Dashboard, Incidents, File Uploads, Mitigation, Reports, Custom Rules, and Config. The left sidebar lists various system settings, with 'Email Collectors' highlighted in a red box. The main content area shows the 'Add New Email Collector' button and a table for 'Current Email Collectors' with columns for Details, Enable, and Actions. Four numbered green callouts indicate the steps: ① Click 'Add New Email Collector', ② Click the plus icon in the left sidebar, ③ Click 'Email Collectors' in the left sidebar, and ④ Click the 'Add New Email Collector' button.

ADVANCED THREAT PREVENTION APPLIANCE

Refresh Data System Health J-ATP Admin

Dashboard Incidents File Uploads Mitigation Reports Custom Rules Config

Notifications +

System Profiles -

Password Reset

Roles

Zones

Users

SAML Settings

RADIUS Settings

System Settings

Certificate Management

GSS Settings

Web Collector

SRX Settings

Email Collectors

Secondary Cores

Current Email Collectors

Add New Email Collector

Details Enable Actions

① クリック

② クリック

③ クリック

④ クリック

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)

①クリック

②Email CollectorまたはCoreのIPアドレス
(※127.0.0.1は使用負荷)

③Journalingの受け取り用アドレス
{任意のアドレス}@[グローバルアドレス]

④mitigation対象となる
ドメイン (オプション)

⑤クリック

⑥クリック

⑦クリック

Dashboard Incidents

Notification

System Profiles

0 Password Reset

Roles

Zones

Users

SAML Settings

RADIUS Settings

System Settings

Certificate Management

GSS Settings

Web Collectors

SRX Settings

Email Collectors

Secondary Cores

ADVANCED THREAT PROTECTION

Refresh Data

System Health

J-ATP Admin

Capture Method:

BCC

JATP MTA Receiver

Collect from Juniper Cloud

MTA Receiver IP:

Recipient Email Address:

Domains:

Receive from my Email Servers only:

Yes

No

Enabled:

Enabled

Disabled

Add

Cancel

Current Email Collectors

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 **※設定例※** Refresh Data System Health J-ATP Admin

Dashboard Incidents File Uploads Mitigation Reports Custom Rules **Config**

Notifications +
System Profiles -

0 Password Reset
Roles
Zones
Users
SAML Settings
RADIUS Settings
System Settings
Certificate Management
GSS Settings
Web Collectors
SRX Settings
Email Collectors
Secondary Cores

Capture Method:
☐ BCC
☒ JATP MTA Receiver
☐ Collect from Juniper Cloud

MTA Receiver IP:
172.27.115.127

Recipient Email Address:
jatp_mta@

Domains:
jatp-test.ddo.jp

Receive from my Email Servers only:
☐ Yes
☒ No

Enabled:
☒ Enabled
☐ Disabled

Add

Cancel

Current Email Collectors

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

Powered by Juniper Version 50.2.14 Content Version 50.2.9 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

Password Reset Roles Zones Users SAML Settings RADIUS Settings System Settings Certificate Management GSS Settings Web Collectors SRX Settings Email Collectors 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 5.0.2.14 Content Version 5.0.2.9 Support Resources Contact Us



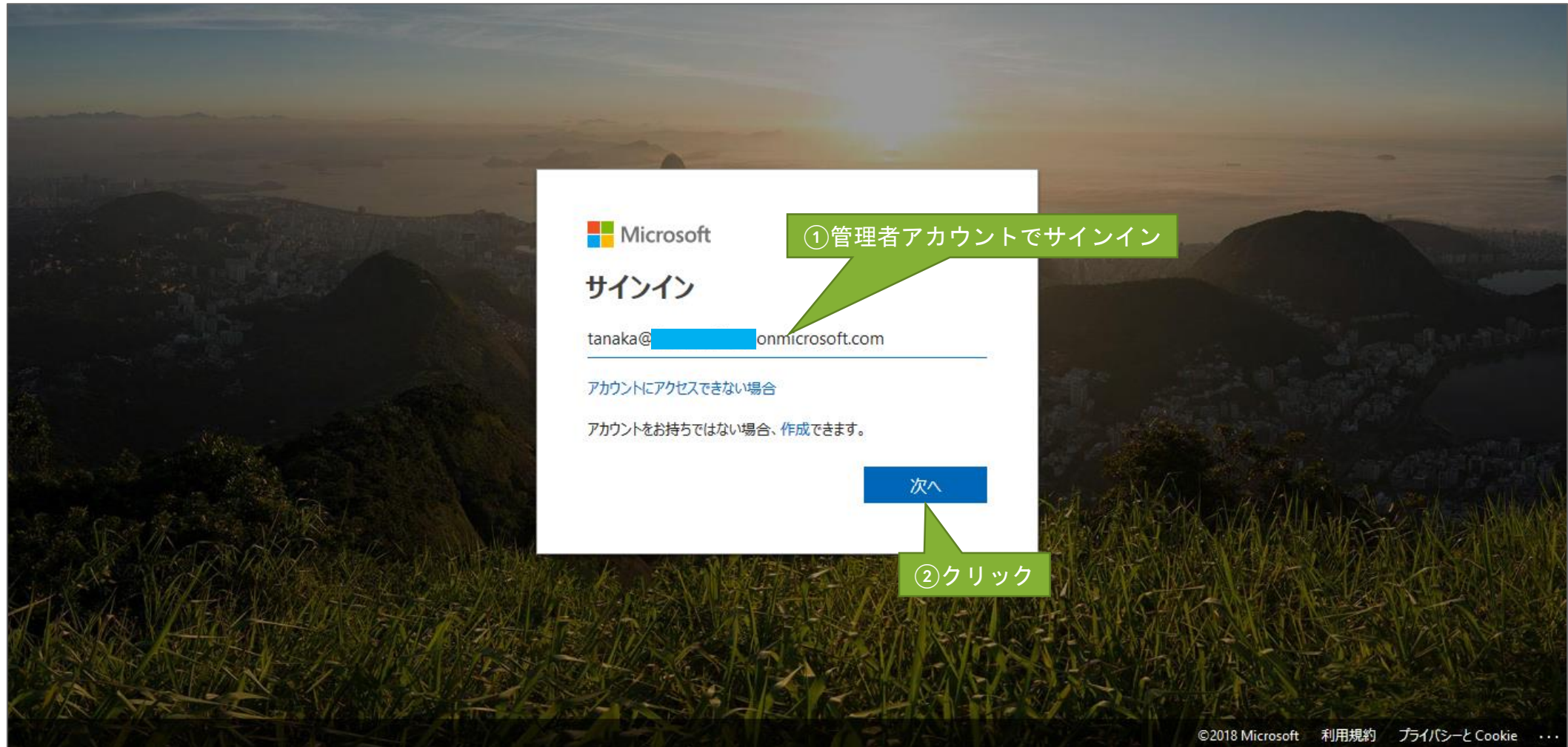
Office 365 ジャーナル設定手順 (BCC,MTA Receiver)

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

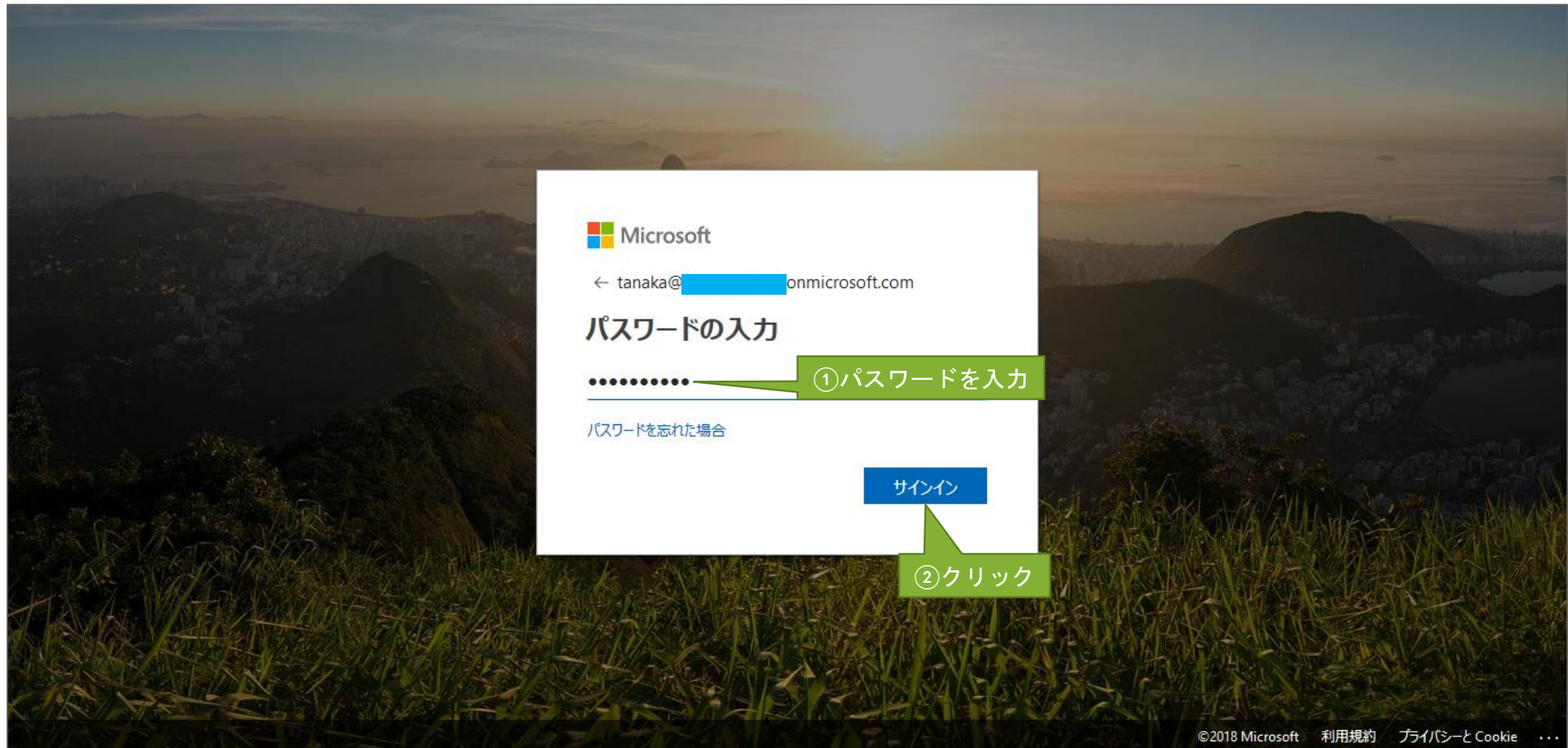
<https://www.office.com/> にアクセス



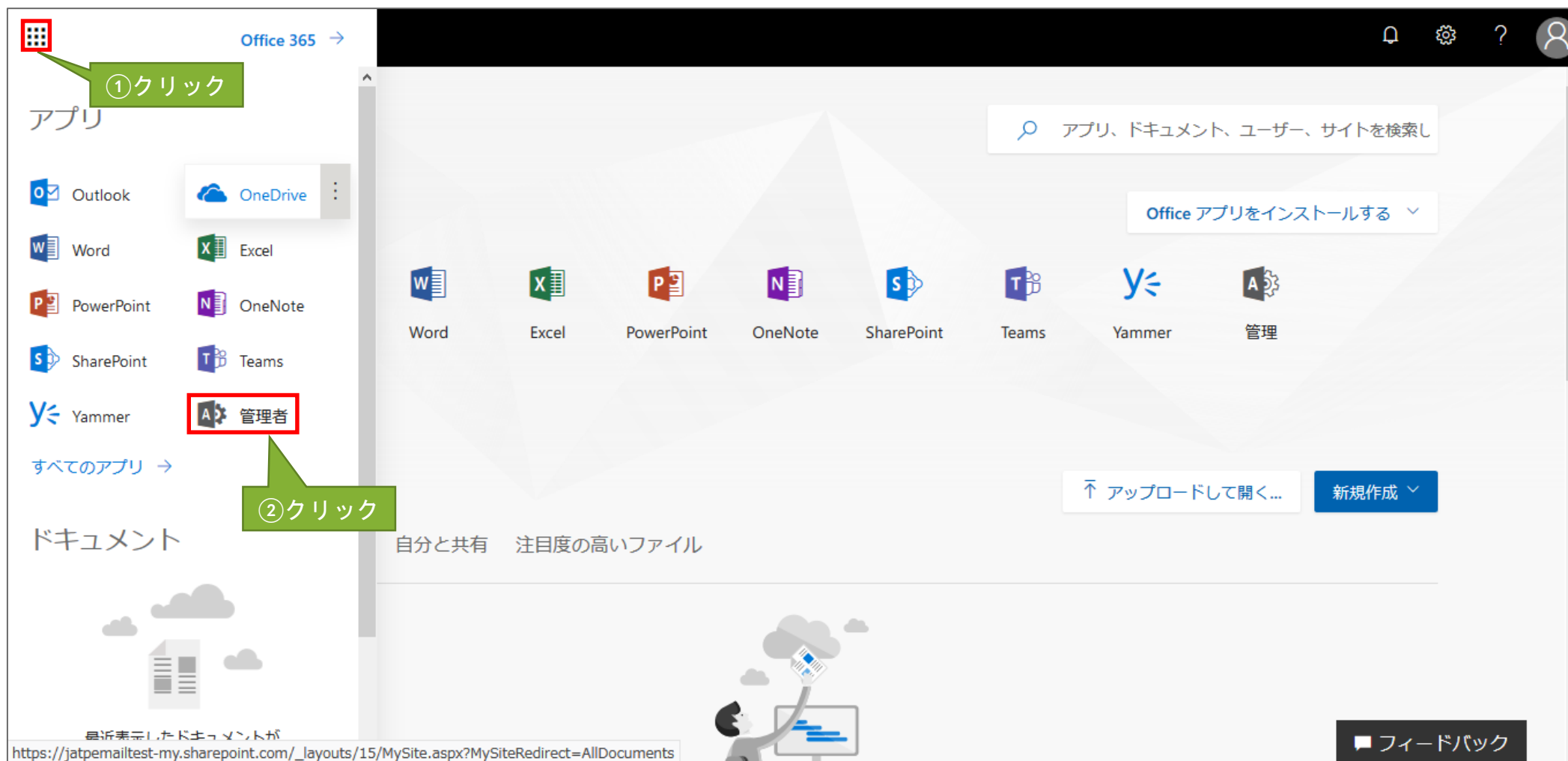
OFFICE 365 ジャーナル設定手順 (BCC,MTA RECEIVER)



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

test

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。

アプリを入手する

設定に移動

クリック

アクティブなユーザー >

- + ユーザーの追加
- 🗑 ユーザーの削除
- ✎ ユーザーの編集
- 🔑 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ー...

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 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、既存の検索を削除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

ヘルプが必要です

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

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**

+ ✎ 🗑️ ↺

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

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

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

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

組織における電子メール保存戦略または
配信できないジャーナル レポートの送信先:

配信できないジャーナル レポートの送信先:

オン ルール

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

クリック

合計 0 件のうち 0 件を選択

ヘルプが必要です

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

組織における電子メール保存戦略または

配信できないジャーナルレポートの送信先:

+

オン

ルール

ジャーナル ルール

ジャーナルレポート NDR の送信先の選択 - Mozilla Fi...

https://outlook.office365.com/ecp/Pick...

表示名

プライマリ メール アドレス

JATP jatp@onmicrosoft.com

ジャーナルメールボックスでメールを受信できない場合の代替を指定

OK

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?

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

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

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

配信できないジャーナルレポートの送信先:

オン ルール

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:

jatp@onmicrosoft.co

参照...

保存 キャンセル

クリック

合計 0 件のうち 0 件を選択

ヘルプが必要です

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
配信できないジャーナルレポートの送信先:

オン	ルール

ジャーナルレポートの送信先

配信 警告

配信できないジャーナルレポートに使用されているアドレスに送信されたメールは、ジャーナルされず、トランスポートおよびメールボックスのルールの設定も有効になりません。配信不能なジャーナルレポート専用のメールボックスを作成することをお勧めします。

OK

合計 0 件のうち 0 件を選択

ヘルプが必要です

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

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

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

組織における電子メ

配信できないジャーナル

ジャーナル ルールの新規作成

このルールを適用します...

*ジャーナルレポートの送信先:

jatp_mta@

名前:

JATP

*メッセージの送信先または受信元が次の場合...

[すべてのメッセージに適用]

*以下のメッセージをジャーナリングします...

すべてのメッセージ

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?

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

組織における電子メ
配信できないジャーナル
+ ✎ 🗑️ ↺
オン ルー

ジャーナル ルールの新規作成

このルールを適用します...

*ジャーナル レポートの送
jatp_mta@
名前:
JATP
*メッセージの送信先ま
[すべてのメッセージに]
*以下のメッセージをジ
すべてのメッセージ

警告
このルールを今後受信するすべてのメッセージに適用しますか?

はい いいえ

クリック

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

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
<input checked="" type="checkbox"/>	JATP		jatp_mta@122.208.14.164

合計 1 件のうち 1 件を選択

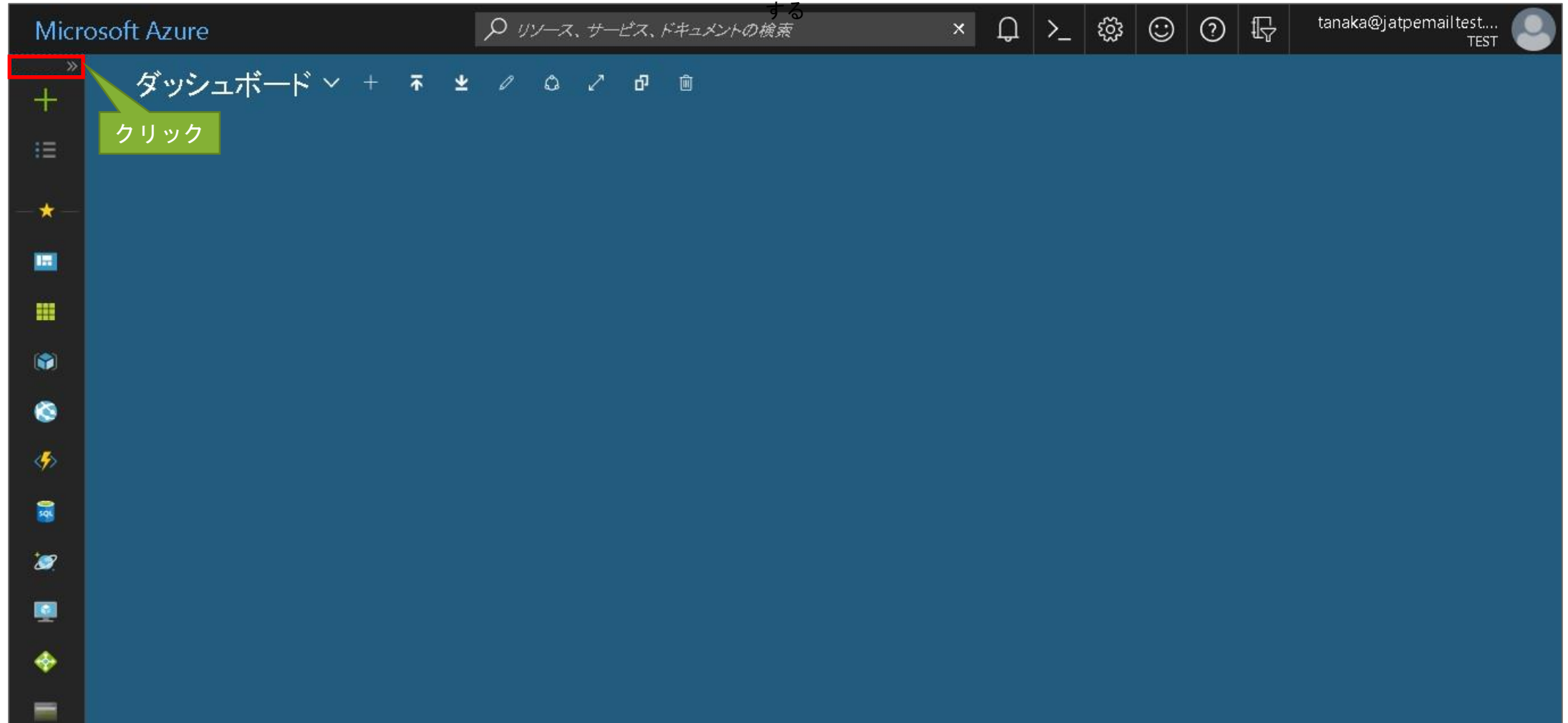
ヘルプが必要ですか?



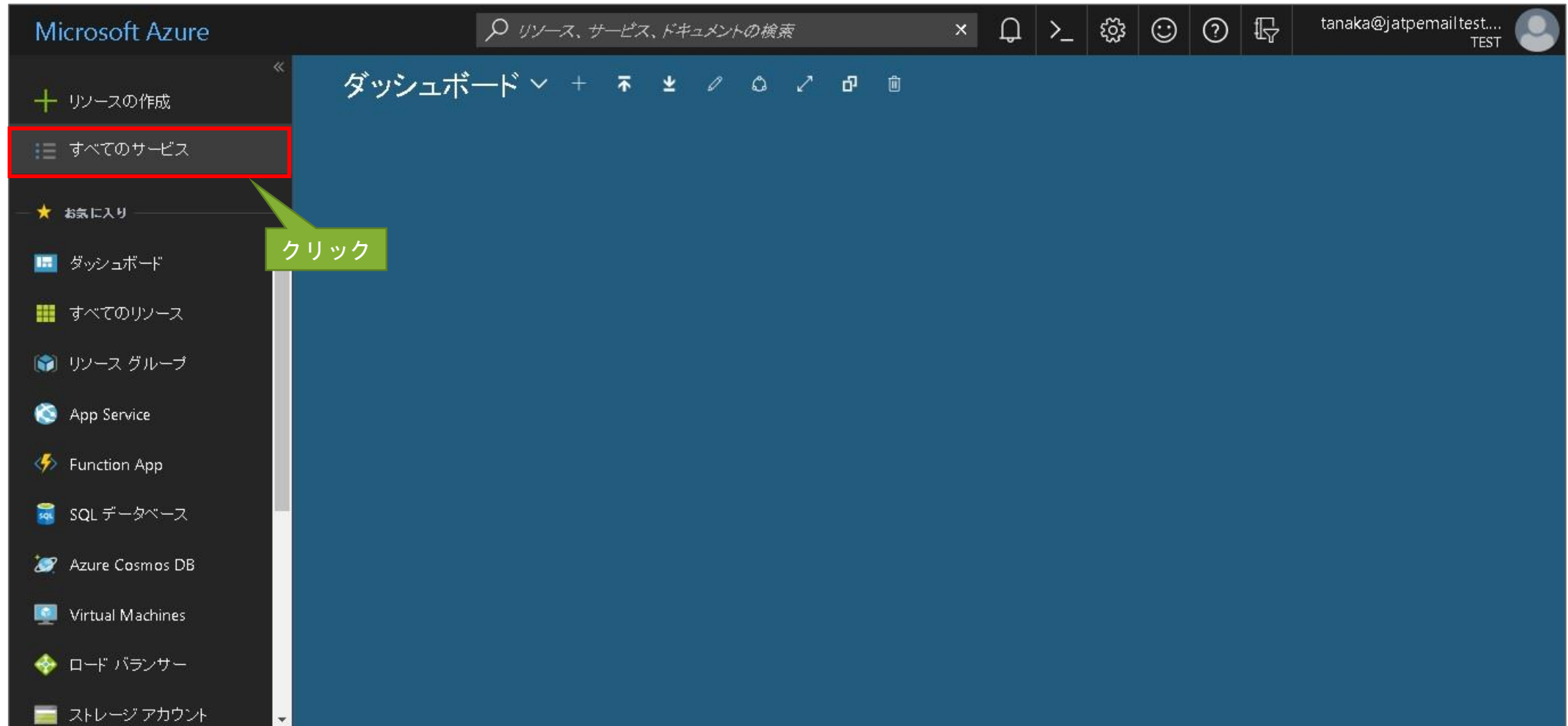
Office 365 Mitigation設定手順 (BCC,MTA Receiver)

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

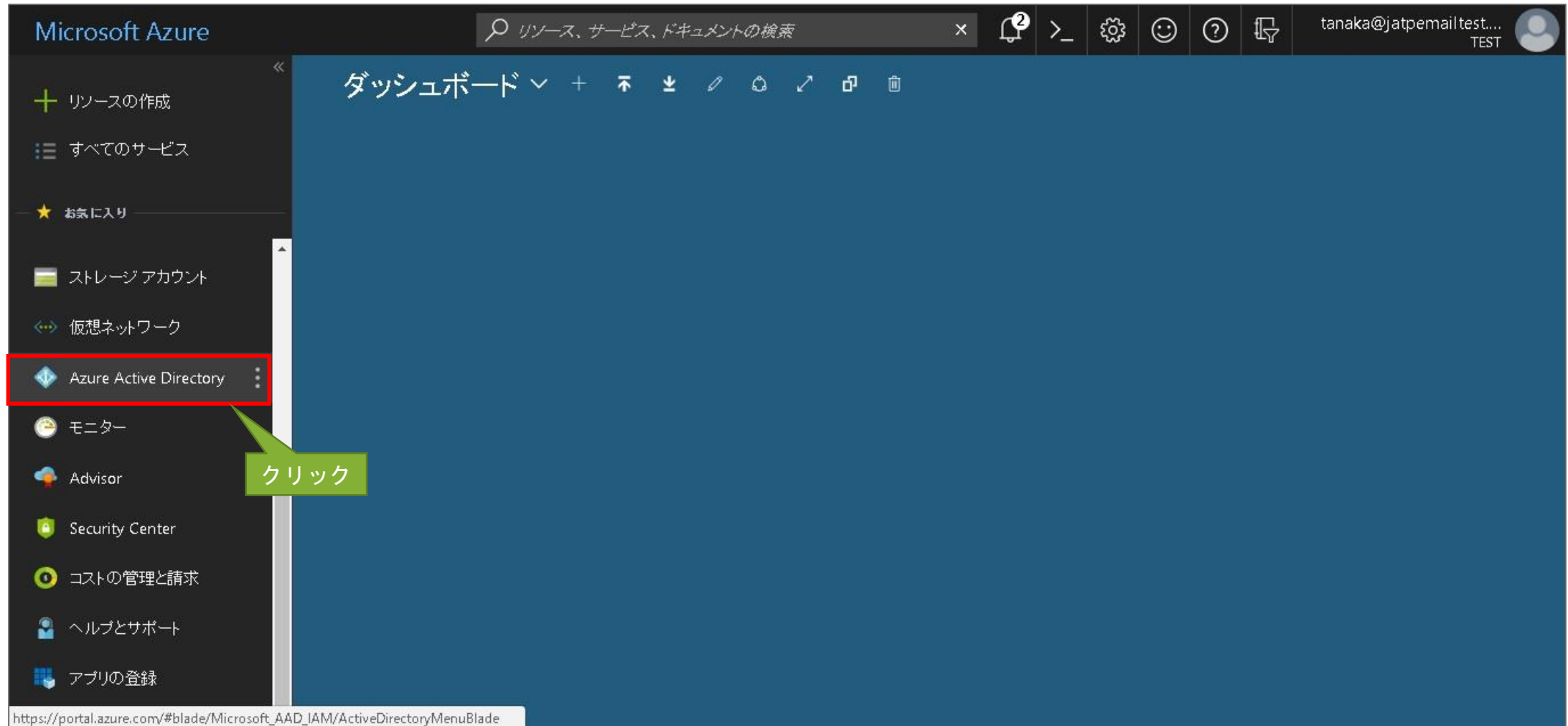
Azureポータル(<https://www.office.com/>) へアクセスして**管理者アカウント**でログイン



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+F)

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

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

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

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

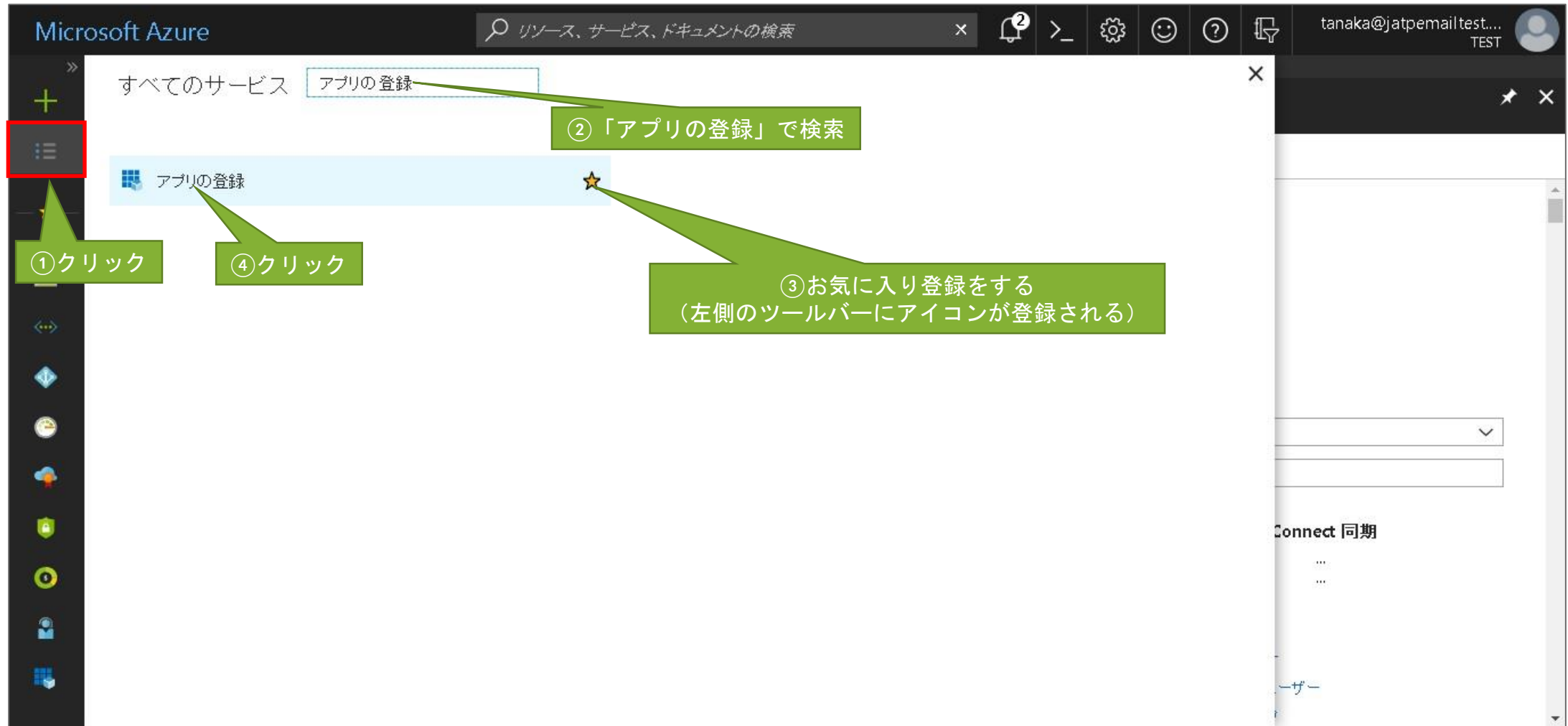
技術部連絡先
skyatptest01@gmail.com

グローバル プライバシー連絡先

①クリック

②後程必要となるためディレクトリIDを
て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)



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 > 作成

作成

① 名前の入力

* 名前 ①

JATP

② "Web アプリ/API" を選択

アプリケーションの種類 ①

Web アプリ/API

③ サインオンURLを入力
http://localhost: 《任意のポート番号》

* サインオン URL ①

http://localhost:《ポート番号》

④ クリック

作成

トラブルシューティング

Microsoft Application Console にアクセスしてください。

アプリケーションの種類

アプリケーション ID

このディレクトリに登録されたアプリケーションはありません。

アプリケーションの登録

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

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the 'Microsoft Azure' logo, a search bar, and user information for 'tanaka@jatpemailtest... TEST'. The left sidebar shows the navigation menu with 'ホーム > アプリの登録 > JATP' selected. The main content area displays the 'JATP' application registration details. A table lists the application's properties:

アプリケーションの種類	アプリケーション ID
Web アプリ/API	f631a02e-8639-4f2d-9380-de679f550fca

On the right, the 'JATP' application details are shown, including the 'アプリケーション ID' (f631a02e-8639-4f2d-9380-de679f550fca) which is highlighted in a red box. A green callout box points to this ID 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'.

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

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the 'Microsoft Azure' logo, a search bar, and user information for 'tanaka@jatpemailtest... TEST'. The left sidebar shows the 'アプリの登録' (App registrations) section, with 'JATP' selected. The main content area displays the 'JATP' application registration details. A green arrow points to the '設定' (Settings) button, with the text 'クリック' (Click) next to it. The application details table shows the following information:

表示名	アプリケーション ID
JATP	f631a02e-8639-4f2d-9380-de679f550fca
アプリの Web URL	オブジェクト ID
http://localhost:60000	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)

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
登録済みのアプリ

設定 マニフェスト 削除

表示名 JATP	アプリケーション ID f631a02e-8639-4f2d-9380-de679f550fca
アプリケーションの種類 Web アプリ/API	オブジェクト ID 47de93f9-9645-4102-9f85-2ef3f50ec0c4
ホーム ページ http://localhost:60000	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

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 >
- 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 >

クリック

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

フィルター設定

全観

- 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
- 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

必要なアクセス許可

+ 追加 アクセス許可の付与

API クリック

API	アプリケーションのア...	委任されたアクセス...
Windows Azure Active Directory	0	1

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 > APIアクセスの追加 > APIを選択します

APIアクセスの追加

1 APIを選択します
Office 365 Exchange Online

①クリック

許可を選択します

②クリック

③クリック

完了

APIを選択します

サービス プリンシパル名で他のアプリケーションを検索します

Windows Azure Active Directory

Office 365 Exchange Online

Microsoft Graph

Office 365 SharePoint Online

Skype for Business Online

Office 365 Yammer

Power BI Service

Microsoft Rights Management Services

選択

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 > APIアクセスの追加 > アクセスの有効化

APIアクセスの追加

1 APIを選択します
Office 365 Exchange Online

2 アクセス許可を選択します
1ロール、0スコープ

完了

アクセスの有効化

Read calendars in all mailboxes	はい
Read contacts in all mailboxes	はい
Read mail in all mailboxes	はい
<input checked="" type="checkbox"/> Read and write mail in all mailboxes	はい
Read and write contacts in all mailboxes	はい
Read and write all user mailbox settings	はい
Read user tasks in all mailboxes	はい
Read and write tasks in all mailboxes	はい
Read and write calendars in all mailboxes	はい
Read calendars in all mailboxes	はい

①クリック

②クリック

選択

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

The screenshot shows the Microsoft Azure portal interface. The breadcrumb navigation at the top reads: ホーム > アプリの登録 > JATP > 設定 > 必要なアクセス許可 > API アクセスの追加. The left sidebar contains a search bar and a list of navigation items: 全般 (General), プロパティ (Properties), 応答 URL (Response URL), 所有者 (Owner), API アクセス (API Access), 必要なアクセス許可 (Required Access Permissions), キー (Keys), and トラブルシューティング + サポート (Troubleshooting + Support). The main content area is divided into three panes. The first pane, titled '必要なアクセス許可' (Required Access Permissions), shows a table with one entry: Windows Azure Active Directory. The second pane, titled 'API アクセスの追加' (Add API Access), shows two steps: 1. API を選択します (Select API) with 'Office 365 Exchange Online' selected, and 2. アクセス許可を選択します (Select permissions) with '1 ロール、0 スコープ' (1 role, 0 scope) selected. A green callout bubble with the text 'クリック' (Click) points to a blue '完了' (Done) button at the bottom right of the second pane.

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 > 設定 > 必要なアクセス許可 > API アクセスの追加

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

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

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...	委任されたアクセス...
Windows Azure Active Directory	0	1

1 API を選択します
Office 365 Exchange Online

2 アクセス許可を選択します
1 ロール、0 スコープ

クリック

完了

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

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and user information (tanaka@jatpemailtest... TEST). The left sidebar shows the navigation menu with the 'Required Access Permissions' option selected. The main content area is divided into three panes:

- Left Pane:** Application details for 'JATP' (Application ID: f631a02e-8639-4f2d-9380-de679f550fca, Object ID: 47de93f9-9645-4102-9f85-2ef3f50ec0c4).
- Middle Pane:** '設定' (Settings) section with a search bar and a list of settings: 'プロパティ' (Properties), '応答 URL' (Response URL), '所有者' (Owner), 'API アクセス' (API Access), and 'トラブルシューティング + サポート' (Troubleshooting + Support). The '必要なアクセス許可' (Required Access Permissions) option is highlighted.
- Right Pane:** '必要なアクセス許可' (Required Access Permissions) section. It includes a '+ 追加' (Add) button and a table showing the permissions granted to the application.

The table in the right pane has the following data:

API	アプリケーションのア...	委任されたアクセス...
Windows Azure Active Directory	0	1
Office 365 Exchange Online	1	0

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

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

③ クリック

アクセス許可の付与

② クリック

現在のディレクトリのすべてのアカウントに対して JATP の以下のアクセス許可を付与しますか? この操作により、このアプリケーションが既に持っている、以下の一覧にある内容に一致する既存のアクセス許可が更新されます。

はい いいえ

① クリック

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

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

キー

新しいサポート要求

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>JATPのWeb UIへアクセスします。

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

The screenshot displays the configuration interface of the Advanced Threat Prevention Appliance. The interface includes a top navigation bar with tabs for Dashboard, Incidents, File Uploads, Mitigation, Reports, Custom Rules, and Config. The Config tab is selected, and a green callout labeled "①クリック" points to it. On the left sidebar, the "Email Mitigation Settings" option is highlighted with a red box and a green callout labeled "②クリック". Below it, the "Firewall Mitigation Settings" option is also visible. A green callout labeled "③クリック" points to the "Email Mitigation Settings" option. In the main content area, the "Add New Mitigation" button is highlighted with a green callout labeled "④クリック". Below this button, a table titled "Current Email Mitigations Configured" is visible, with columns for "Description" and "Actions". The footer of the interface shows the version information: "Powered by JuniperVersion 5.0.2.20 Content Version 5.0.2.14" and links for Support, Resources, and Contact Us.

ADVANCED THREAT PREVENTION APPLIANCE

①クリック

Refresh Data

System Health

J-ATP Admin

Dashboard Incidents File Uploads Mitigation Reports Custom Rules Config

Notifications

System Profiles

Environmental Settings

②クリック

③クリック

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

④クリック

Current Email Mitigations Configured

Description Actions

Powered by JuniperVersion 5.0.2.20 Content Version 5.0.2.14

Support Resources Contact Us

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

⑤チェックを入れる

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

⑥保護対象のドメインを入力

⑦クリック

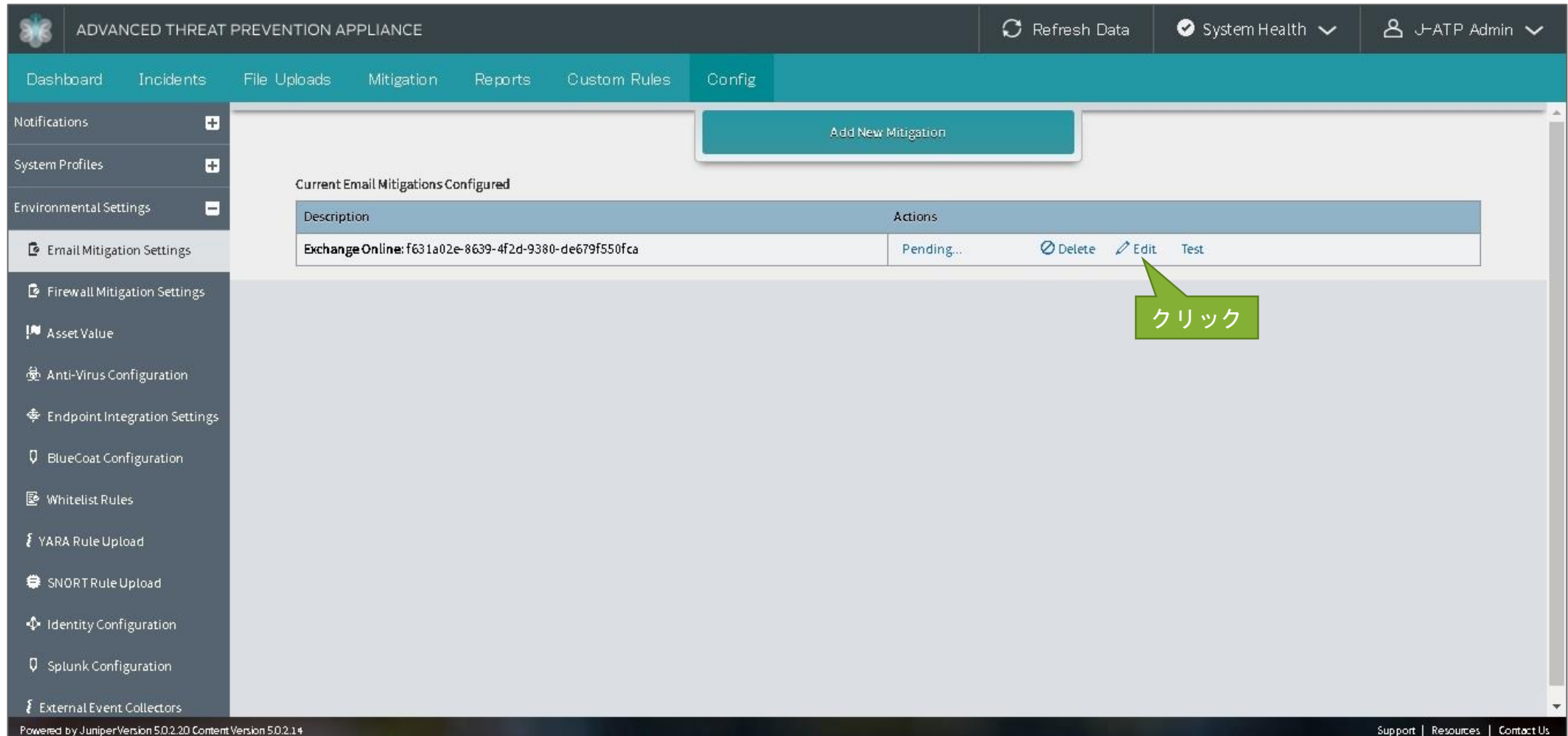
Cancel

Description	Actions
Gmail	Disable Delete Edit Test

Powered by JuniperVersion 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
ExchangeOnline: f631a02e-8639-4f2d-9380-de679f550fca	Pending... Delete Edit Test

クリック

Powered by JuniperVersion 50.2.20 Content Version 50.2.14

Support Resources Contact Us

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

ADVANCED THREAT PREVENTION APPLIANCE

Refresh Data System Health JATP 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

Email Type: ☐ Gmail ☒ Exchange Online

Authority Host URL:

Office Resource URL:

Tenant:

Client ID:

Quarantine Folder:

☐ Generate New Azure Key Credentials

Key Bits:

Certificate Lifetime (Days):

Azure Manifest Key Credentials:

```
{
  "keyCredentials": [
    {
      "customKeyIdentifier": "rqE11bDjZdJQJ1w9ec+JP68Cojc=",
      "keyId": "10520fad-88e5-40d0-9a0b-b91121583673",
      "type": "AsymmetricX509Cert"
    }
  ]
}
```

Domains: Save

Cancel

Current Email Mitigations Configured

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

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

Powered by JuniperVersion 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 Microsoft Azure portal interface. The top navigation bar includes the 'Microsoft Azure' logo, a search bar, and user information for 'tanaka@jatpemailtest... TEST'. The breadcrumb trail indicates the path: 'ホーム > アプリの登録 > JATP'. The main content area is divided into two panes. The left pane shows a list of applications with columns for 'アプリケーションの種類' and 'アプリケーション ID'. The right pane displays the details for the 'JATP' application, including icons for '設定' (Settings), 'マニフェスト' (Manifest), and '削除' (Delete). A green callout box with the text 'クリック' (Click) points to the '設定' icon. The application details include:

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	オブジェクト ID
Web アプリ/API	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 > 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 "informational": {  
12   "privacy": null,  
13   "termsOfService": null  
14 },  
15 "identifierUri": [  
16   "https://jatpemailtest.onmicrosoft.com/71d11d58-6eac-4c0a-8155-bb7db4ca68bd"  
17 ],  
18 "keyCredentials": [],  
19 "knownClientApplications": [],  
20 "logoutUrl": null,  
21 "oauth2AllowImplicitFlow": true,  
22 "oauth2AllowUrlPathParameters": true,  
23 "oauth2Permissions": [  
24   {  
25     "adminConsentDescription": "Allow the application to access JATP on behalf of the signed-in user.",  
26     "adminConsentDisplayName": "Access JATP",  
27     "id": "c961090d-dbd8-4ef4-b2c7-9fc44b55420d",  
28     "isEnabled": true,  
29     "type": "User",  
30     "userConsentDescription": "Allow the application to access JATP on your behalf.",  
31     "userConsentDisplayName": "Access JATP",
```

“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

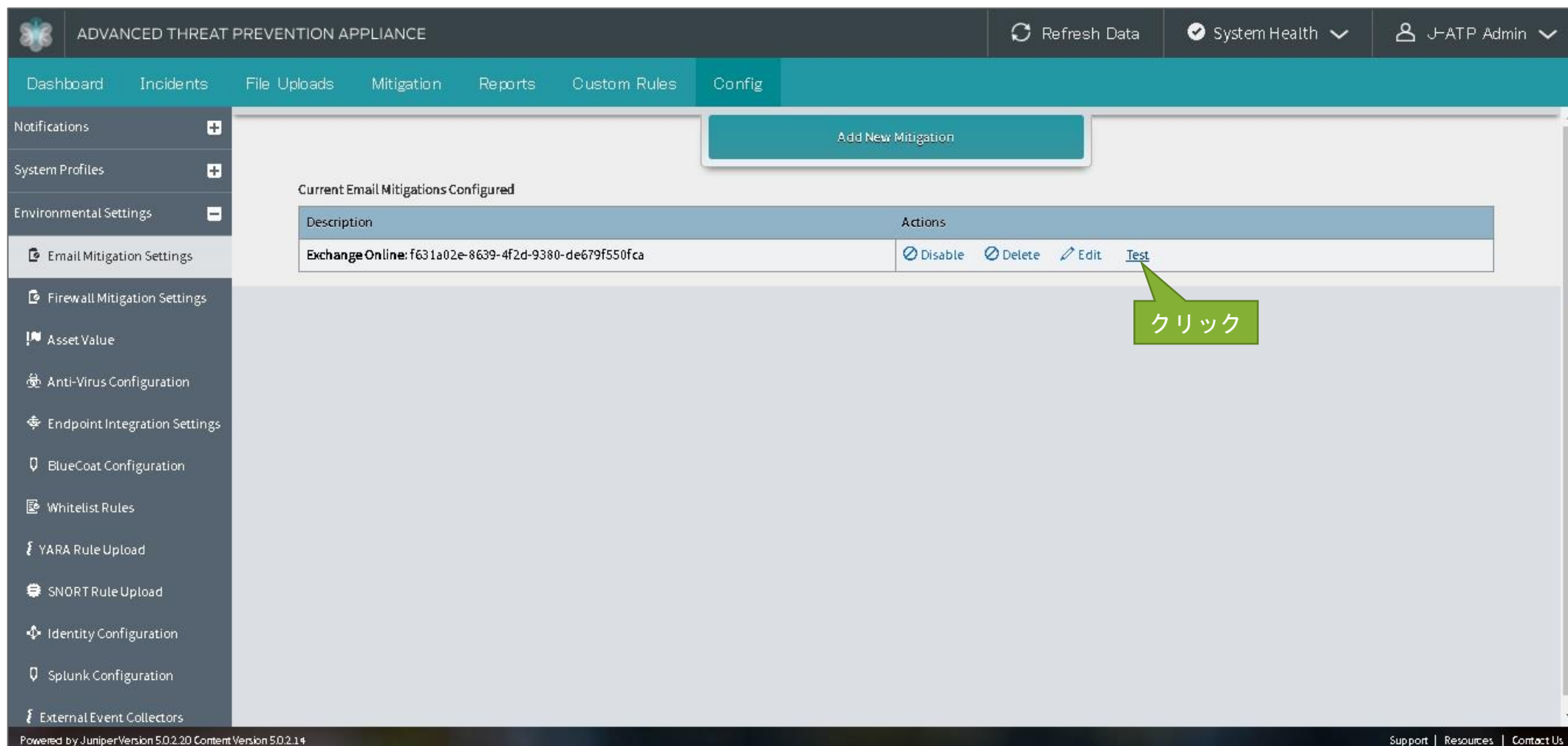
ローカル ディレクトリでのマネージド アプリケーション
JATP

```
11  "informational": {  
12    "privacy": null,  
13    "termsOfService": null  
14  },  
15  "identifierUri": [  
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": "MIIIFejCCA2ICAQAwDQYJKoZIhvcNAQEFBQAwgYIxCzAJBgNVBAYTA1VTMRMwEQYDVQQIDApDYWxpZm9ybmlhMRQw...  
25    }  
26  ],  
27  "knownClientApplications": [],  
28  "logoutUri": 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 50.2.20 Content Version 50.2.14

Support Resources Contact Us

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

The screenshot displays the Juniper ATP Admin console interface. The top navigation bar includes 'Dashboard', 'Incidents', 'File Uploads', 'Mitigation', 'Reports', 'Custom Rules', and 'Config'. The left sidebar lists various settings, with 'Email Mitigation Settings' selected. The main content area shows 'Current Email Mitigations Configured' with a table containing one entry: 'Exchange Online: f631a02e-8639-4f2d-9380-de679f550fca'. Above this table is a 'Add New Mitigation' button. Below the table, a red-bordered box highlights a yellow banner reading '※接続テスト成功※' and a white modal dialog box with the text 'Test Successful' and an 'OK' button. The bottom of the screen shows the footer with 'Powered by Juniper Version 50.2.20 Content Version 50.2.14' and links for 'Support', 'Resources', and 'Contact Us'.

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

Current Email Mitigations Configured

Add New Mitigation

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 50.2.20 Content Version 50.2.14

Support Resources Contact Us

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

The screenshot shows the Juniper ATP Admin console interface. The top navigation bar includes 'Dashboard', 'Incidents', 'File Uploads', 'Mitigation', 'Reports', 'Custom Rules', and 'Config'. The left sidebar lists various settings, with 'Email Mitigation Settings' selected. The main content area shows 'Current Email Mitigations Configured' with a table containing one entry: 'Exchange Online: f631a02e-8639-4f2d-9380-de679f550fca'. An error dialog box is displayed in the center, stating 'Unable to obtain access token' with an 'OK' button. A yellow callout box with red text provides troubleshooting steps.

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 Correlation

Splunk Configuration

External Event Collectors

Powered by Juniper Version 50.2.20 Content Version 50.2.14

Support Resources Contact Us

Current Email Mitigations Configured

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

※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)

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)

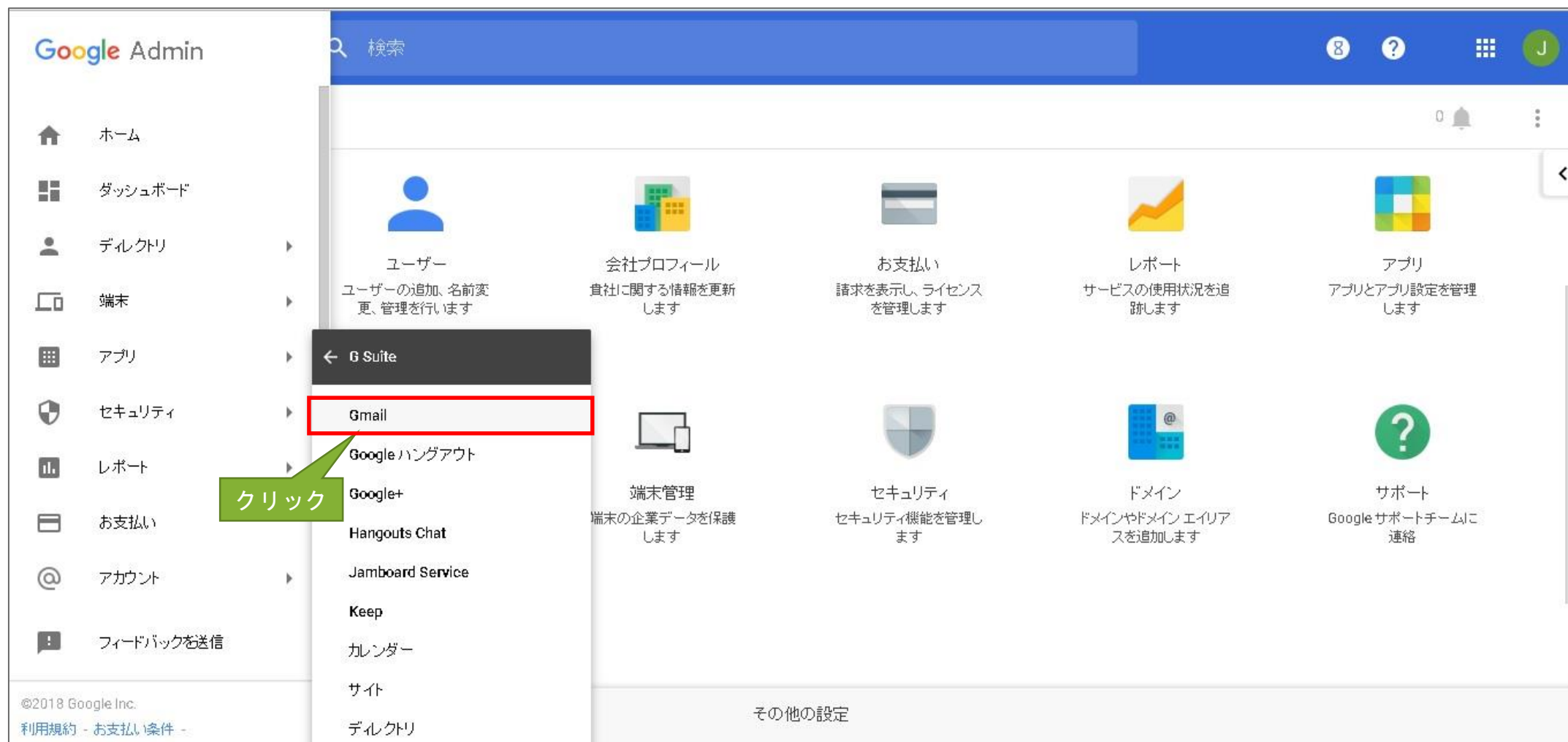
管理者アカウントでログイン後、管理ホーム画面（ <https://admin.google.com/AdminHomeGoogle> ）へアクセス



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)

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

検疫

設定項目を検索

セットアップ

ウェブアドレス

ローカルに適用しました

ユーザー用の Gmail の URL:

https://mail.google.com/a/jatp-test.ddo.jp

URL を変更

MXレコード

ローカルに適用しました

jatp-test.ddo.jp の現在の MXレコード:

優先順位	参照先
10	ASPMXL.GOOGLE.COM.
20	ALT1.ASPMXL.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

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。

クリック

G SUITE ジャーナル設定手順 (BCC,MTA RECEIVER)

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 検疫

設定項目を検索

①コンテンツ コンプライアンス名

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

次の一部がメールに一致する場合 ▼

表現 追加

キャンセル 設定を追加

②検査対象のものに
チェックを入れる

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
まだ設定されていません

配信を制限
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
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

G SUITE ジャーナル設定手順 (BCC,MTA RECEIVER)

The screenshot shows the Google Admin console interface. The top navigation bar includes the Google Admin logo, a search bar, and user profile icons. The main content area displays the 'Gmail の設定' (Gmail Settings) page, specifically the '詳細設定' (Advanced Settings) tab. A modal dialog titled '設定を追加' (Add Settings) is open, showing a list of search criteria. A green callout box with the text '①一致条件を選択' (Select matching conditions) points to the '一致条件' (Matching conditions) section. Another green callout box with the text '②クリック' (Click) points to the '追加' (Add) button. The dialog also includes a section for 'メッセージを変更' (Change message) with checkboxes for 'X-Gm-Original-To' and 'X-Gm-Spam' headers. The background settings page shows various options like '包括的なメール ストレージ' (Comprehensive email storage), 'フッターを追加' (Add footer), '配信を制限' (Limit distribution), 'コンテンツ コンプライアンス' (Content compliance), and '不快なコンテンツ' (Unpleasant content).

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 検疫

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に適用されません。ゴミ箱のメッセージには適用されません。ゴミ箱

包括的なメール ストレージ
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
まだ設定されていません

コンテンツ コンプライアンス
まだ設定されていません

不快なコンテンツ
まだ設定されていません

設定を追加

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

まだ表現が追加されていません。追加

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

☐ X-Gm-Spam ヘッダーと X-Gm-Phishy ヘッダーを追加

キャンセル 設定を追加

①一致条件を選択

②クリック

G SUITE ジャーナル設定手順 (BCC,MTA RECEIVER)

The screenshot shows the Google Admin console interface. The top navigation bar includes the Google Admin logo, a search bar, and user profile icons. The main content area displays the 'Gmail の設定 > 詳細設定' (Gmail Settings > Detailed Settings) page. A modal dialog titled '設定を追加' (Add Setting) is open, showing the '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' (Add an expression to represent content to search in each message) step. The dialog has a dropdown menu set to '次の一部がメールに一致する場合' (If the following part matches the email). Below this, there are sections for '表現' (Expression) and 'コンテンツ' (Content). The 'コンテンツ' section has a text input field containing 'user1@jntp-test.ddo.jp'. A green callout bubble points to this field with the text '① Journaling対象のメールアドレスを入力 ※全てのメールをJournalingする場合は"@"と入力' (Enter the email address of the journaling target. ※ If you want to journal all emails, enter '@'). Below the input field are 'キャンセル' (Cancel) and '保存' (Save) buttons. Another green callout bubble points to the '保存' button with the text '② クリック' (Click).

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 検疫

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には適用されません。ゴミ箱のメッセージには適用されません。

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は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、宣伝の目的で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可するかどうかは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、パターンに基づいて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てコンテンツをまだ設定されていません

設定を追加

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

シンプルなコンテンツ マッチ

コンテンツ

user1@jntp-test.ddo.jp

キャンセル 保存

① Journaling対象のメールアドレスを入力
※全てのメールをJournalingする場合は"&@"と入力

② クリック

設定

G SUITE ジャーナル設定手順 (BCC,MTA RECEIVER)

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 検疫

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にのみ適用されます。

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は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、宣伝の目的で、メールのフッターを追加できます。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可または拒否できます。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、パターンに基づいて、迷惑メールを識別します。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て、不快なコンテンツを識別します。まだ設定されていません

※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
ヘッダーと本文

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

設定

G SUITE ジャーナル設定手順 (BCC,MTA RECEIVER)

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 検疫

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 まだ設定されていません ☐ 関連付けられているユーザー

フッターを追加 まだ設定されていません 法令遵守や情報提供、宣伝の

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

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

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

設定を追加

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

キャンセル 設定を追加

設定

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

G SUITE ジャーナル設定手順 (BCC,MTA RECEIVER)

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 検疫

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 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 まだ設定されていません

コンテンツコンプライアンス まだ設定されていません

不快なコンテンツ まだ設定されていません

設定を追加

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

☐ メッセージから送信元アドレスを削除

その他の送信先

☒ 受信者を追加

登録ユーザー

追加

まだ他の受信者が追加されていません。追加

キャンセル 設定を追加

①チェックを入れる

②クリック

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 また設定されていません

フッターを追加 また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可 また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、パターンに基づいて また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 また設定されていません

設定を追加

登録ユーザー

基本

受信者のアドレス:
admin@jatp-test.ddo.jp

キャンセル 保存

暗号化(配信時のみ)
☐ セキュアなトランスポート(TLS)を使用する

キャンセル 設定を追加

① Journalingの送り先を指定する
BCC : Journalingの収集先のアドレス
MTA Receiver : JATPで設定したMAT Receiverのアドレス

② クリック

設定

G SUITE ジャーナル設定手順 (BCC,MTA RECEIVER)

The screenshot shows the Google Admin console interface. At the top, there's a navigation bar with the Google Admin logo and a search bar. Below it, the breadcrumb trail reads: アプリ > G Suite > Gmail の設定 > 詳細設定. The main content area has tabs for 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, and 検索. A modal dialog titled "設定を追加" (Add setting) is open in the center. It has a close button (X) in the top right corner. Inside the dialog, there's a section "その他の送信先" (Other destinations) with a checked checkbox "受信者を追加" (Add recipients). Below this is a box for "登録ユーザー" (Registered user) with a "追加" (Add) button. The box contains the email "配信先: admin@jatp-test.ddo.jp" and two lines of text: "この受信者に迷惑メールを送信しない" (Do not send spam to this recipient) and "この受信者からのバウンスメールを送信元に送信しない" (Do not send bounce messages from this recipient to the sender). Below the box is a section "暗号化(配信時のみ)" (Encryption (delivery only)) with an unchecked checkbox "セキュアなトランスポート(TLS)を使用する" (Use secure transport (TLS)). At the bottom of the dialog is a link "オプションを表示" (Show options). A green callout bubble with the text "クリック" (Click) points to the "設定を追加" (Add setting) button at the bottom right of the dialog. The background settings page shows various options like "包括的なメール ストレージ" (Comprehensive mail storage), "フッターを追加" (Add footer), "配信を制限" (Limit distribution), "コンテンツ コンプライアンス" (Content compliance), and "不快なコンテンツ" (Unpleasant content).

G SUITE ジャーナル設定手順 (BCC,MTA RECEIVER)

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 検索

設定項目を検索

コンテンツコンプライアンス Email Collector
ローカルに適用しました
メッセージ: すべて
一致する: 2
結果: メッセージを変更, 追加の配信: 1回

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。
①確認

添付ファイルのコンプライアンス ファイル形式、ファイル名、メール サイズに基づいて添付ファイル フィルタを設定します。
まだ設定されていません
設定

セキュアなトランスポート (TLS) に準拠 指定されたドメインとの通信に TLS を必要とします。
まだ設定されていません
②クリック

❗ 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](#)

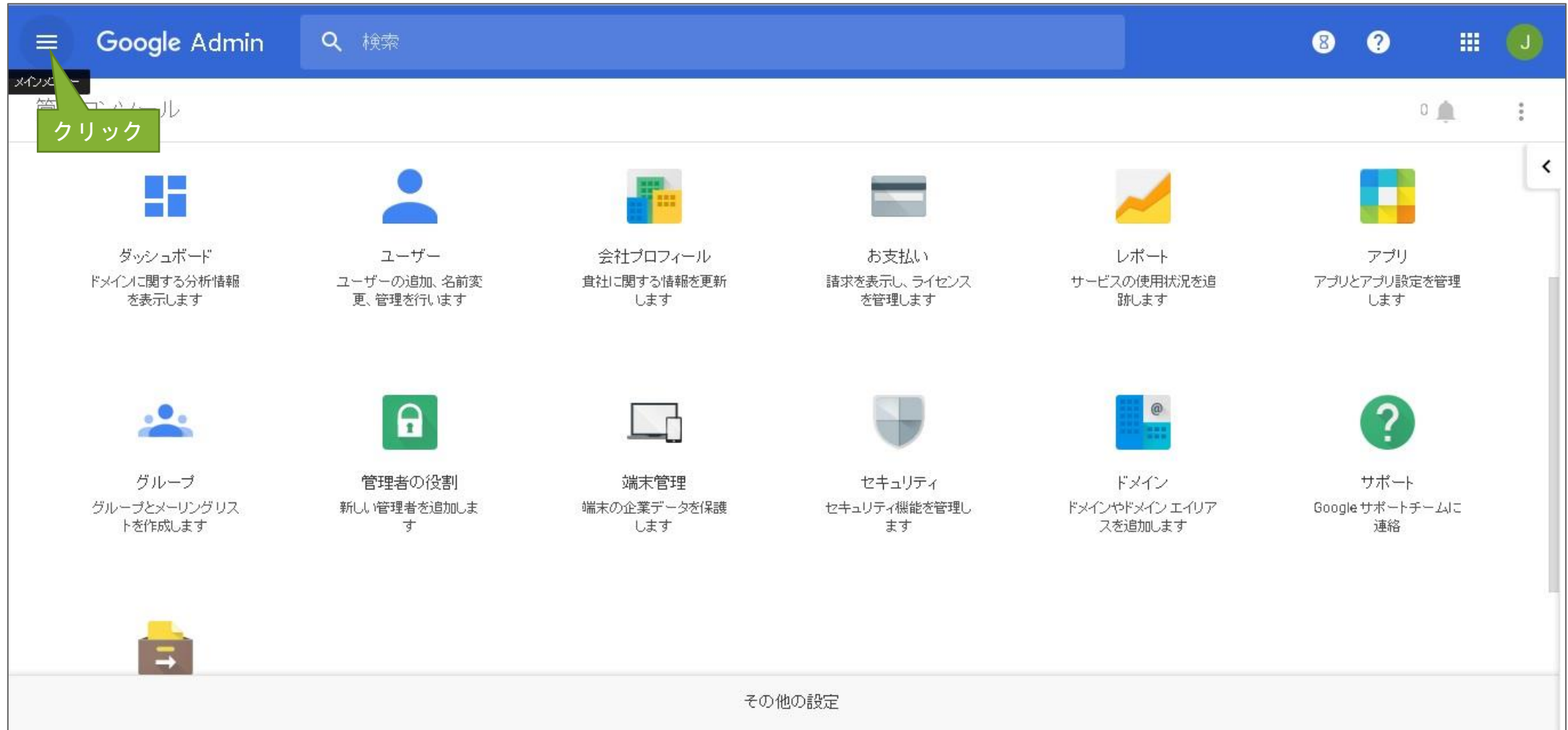
破棄 保存



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)

へ 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 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。②

☒ 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カウントを許可しないことをお勧めします。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ください。②

安全性の低いアプリの設定に移動 »

クリック

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。 ?

グループのフィルタ ? 選択

管理者グループが選択されて

② クリック

破棄 保存

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](#)

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 >

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

 個人情報とプライバシー >

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

広告設定

 アカウント設定 >

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

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

個人情報

連絡先

Google でのアクティビティの管理

広告設定

アカウント設定 >

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

© 2019 Juniper Networks

Juniper Business Use Only

JUNIPER
NETWORKS

120

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。



GMAIL セキュリティ設定の変更 (BCC)

Google

メール ▾ 設定

作成

受信トレイ
スター付き
送信済みメール
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始しませんか

0 GB (0%) / 30 GB を使用中
管理

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](#)

② クリック

ステータス: IMAP 無効

- ☒ IMAP を有効にする
- ☐ IMAP を無効にする

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

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™

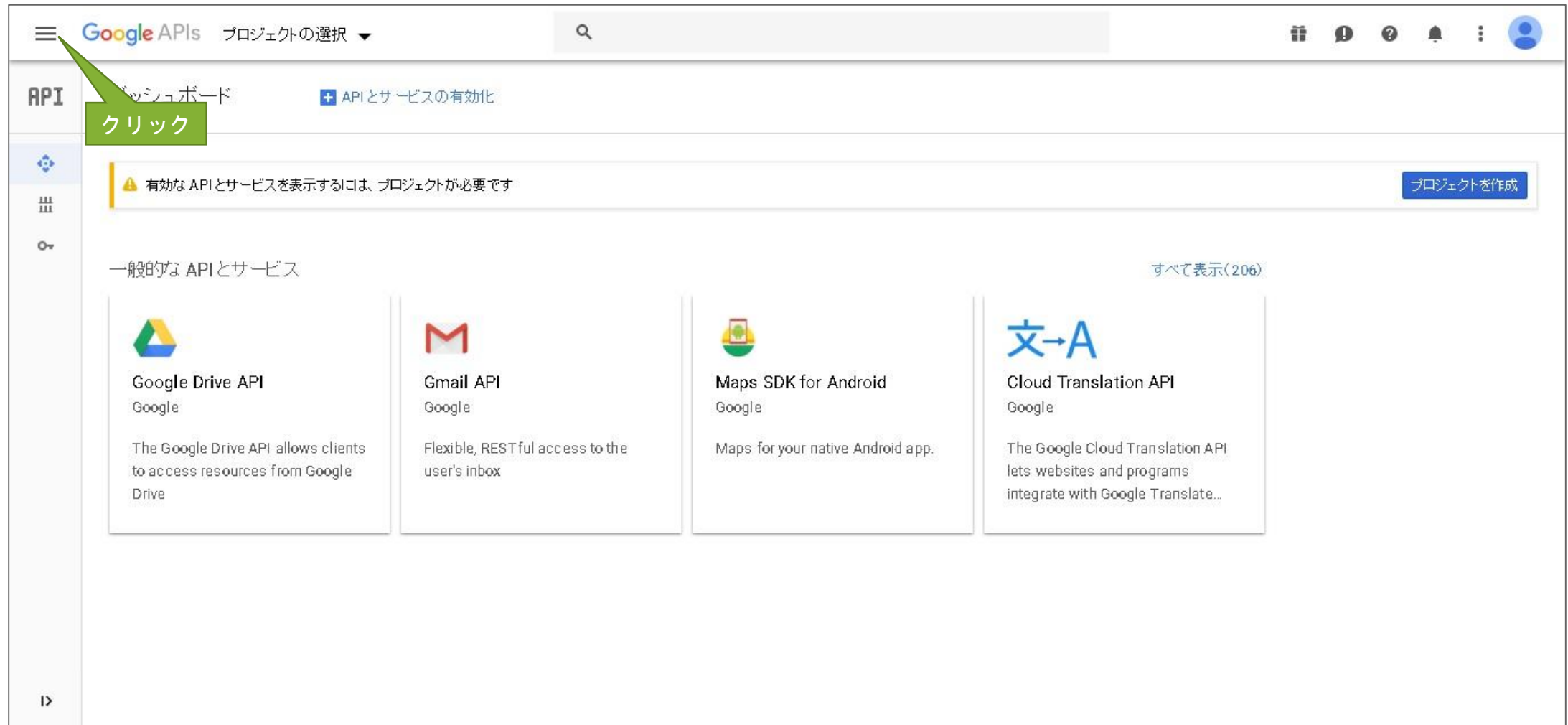
前回のアカウント アクティビティ: 0 分前
他の 1 か所で開かれています [アカウント アクティビティの詳細](#)



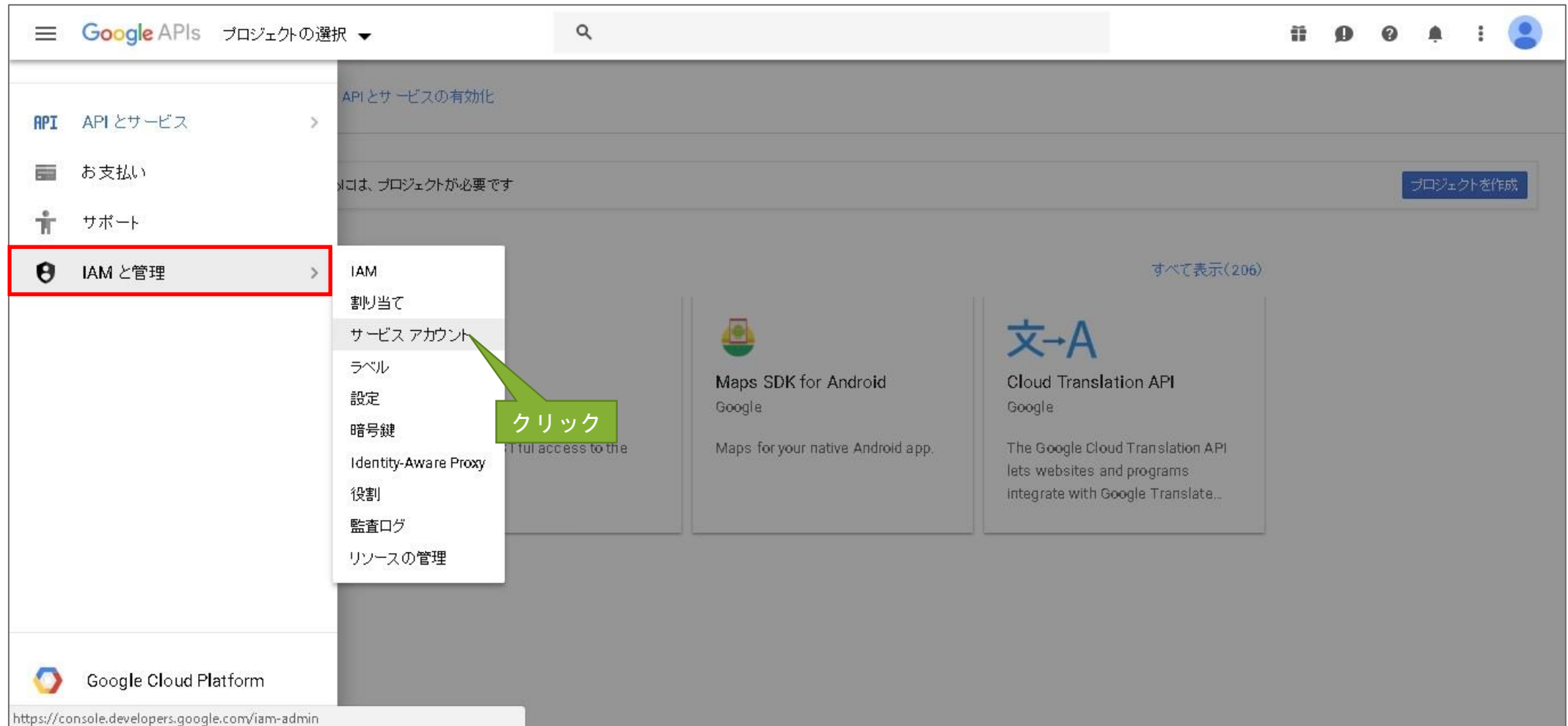
G Suite Mitigation設定手順 (BCC,MTA Receiver)

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)

The screenshot shows the '新しいプロジェクト' (New Project) page on the Google APIs console. The page is in Japanese. At the top, there is a header with the Google APIs logo, a search bar, and several utility icons. The main content area contains the following fields and annotations:

- プロジェクト名*** (Project Name): The text 'jatp-mitigation' is entered. A green callout box with the text '①プロジェクト名を入力' (Enter project name) points to this field.
- プロジェクト ID** (Project ID): The text 'jatp-mitigation' is displayed, followed by the note '後で変更することはできません。' (Cannot be changed later) and a '編集' (Edit) link.
- 組織** (Organization): The text 'juni-test.jp' is entered. A green callout box with the text '②クリック' (Click) points to the '作成' (Create) button below this section.
- 場所*** (Location): The text 'juni-test.jp' is entered, preceded by a location icon. A '参照' (Reference) link is visible to the right.
- 親組織またはフォルダ** (Parent organization or folder): This section is currently empty.
- Buttons**: At the bottom left, there are two buttons: '作成' (Create) in blue and 'キャンセル' (Cancel) in white.

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 **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)

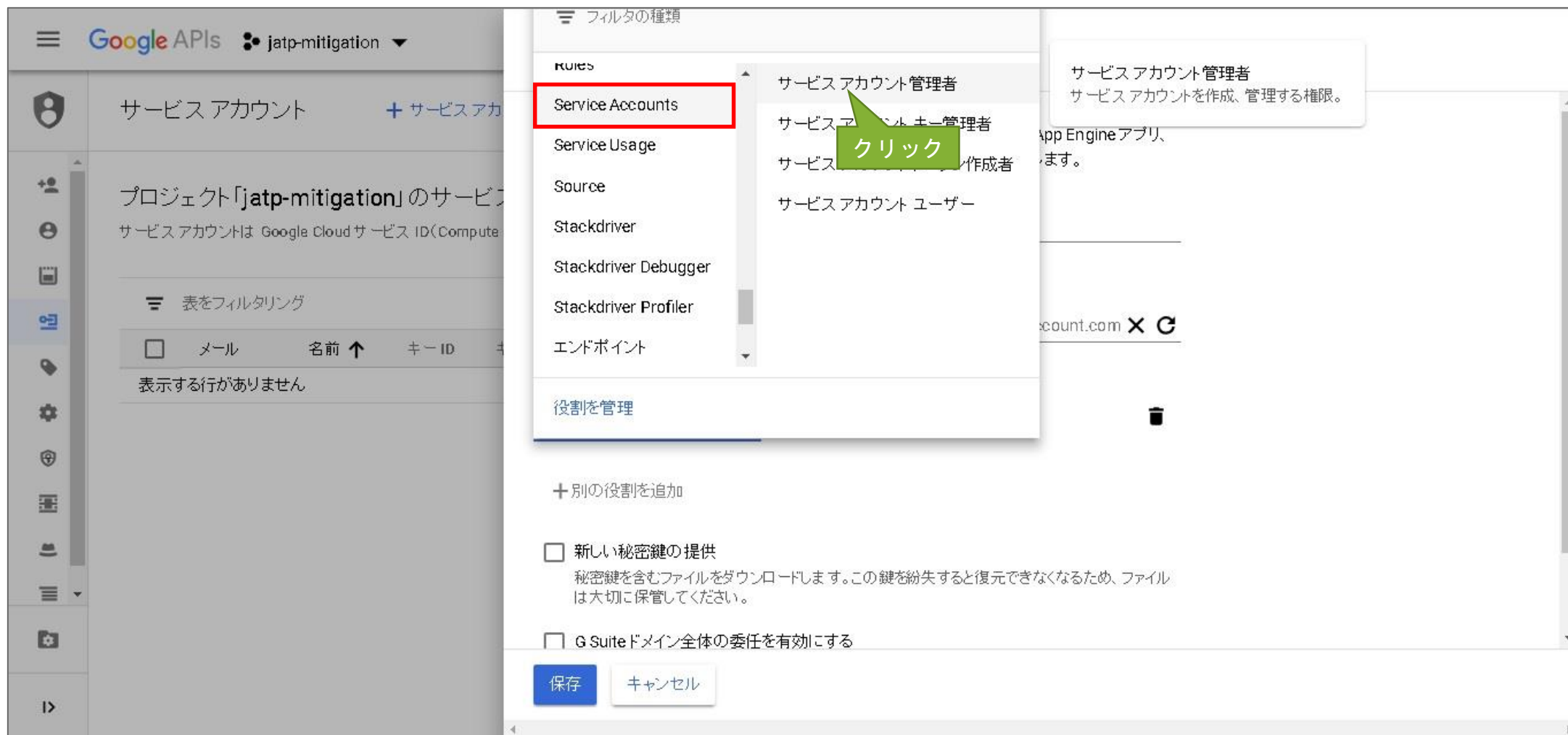
The screenshot shows the 'Create Service Account' dialog in the Google Cloud IAM console. The left sidebar shows the 'Service Accounts' section. The main panel contains the following fields and options:

- サービス アカウント名** (Service Account Name): JATP-Mitigation
- このサービス アカウントで行うことを説明します** (Describe what this service account will do):
- サービス アカウント ID** (Service Account ID): jatp-mitigation
- プロジェクト ID** (Project ID): @jatp-mitigation.iam.gserviceaccount.com
- プロジェクト役割** (Project Role): A dropdown menu with '役割を選択' (Select role) and a green callout '③クリック' (Click) pointing to it.
- + 別の役割を追加** (Add another role)
- ☐ **新しい秘密鍵の提供** (Provide new private key): Includes a note about downloading and securely storing the key file.
- ☐ **G Suiteドメイン全体の委任を有効にする** (Enable delegation to all domains in the G Suite domain)
- 保存** (Save) and **キャンセル** (Cancel) buttons.

Annotations on the left sidebar:

- ① サービスアカウント名を入力** (Enter service account name) points to the 'サービス アカウント名' field.
- ② サービスアカウントIDを入力** (Enter service account ID) points to the 'サービス アカウント ID' field.

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

①チェックを入れる

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

②チェックを入れる

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](#)

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

保存 キャンセル

Information: 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](#)

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](#)

i 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.

[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

<input type="checkbox"/>	メール	名前 ↑	キー ID	キーを削除	キーの作成日	Domain wide delegation ?	操作
<input type="checkbox"/>	jatp-mitigation@jatp-mitigation.iam.gserviceaccount.com	JATP-Mitigation				有効 クライアント ID を表示	⋮

クリック

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

Google APIs jatp-mitigation

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

①クライアントIDをtextファイルなどにコピーしておく

サービスアカウントクライアントは、サービスアカウントで承認を有効にすると作成されます。 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

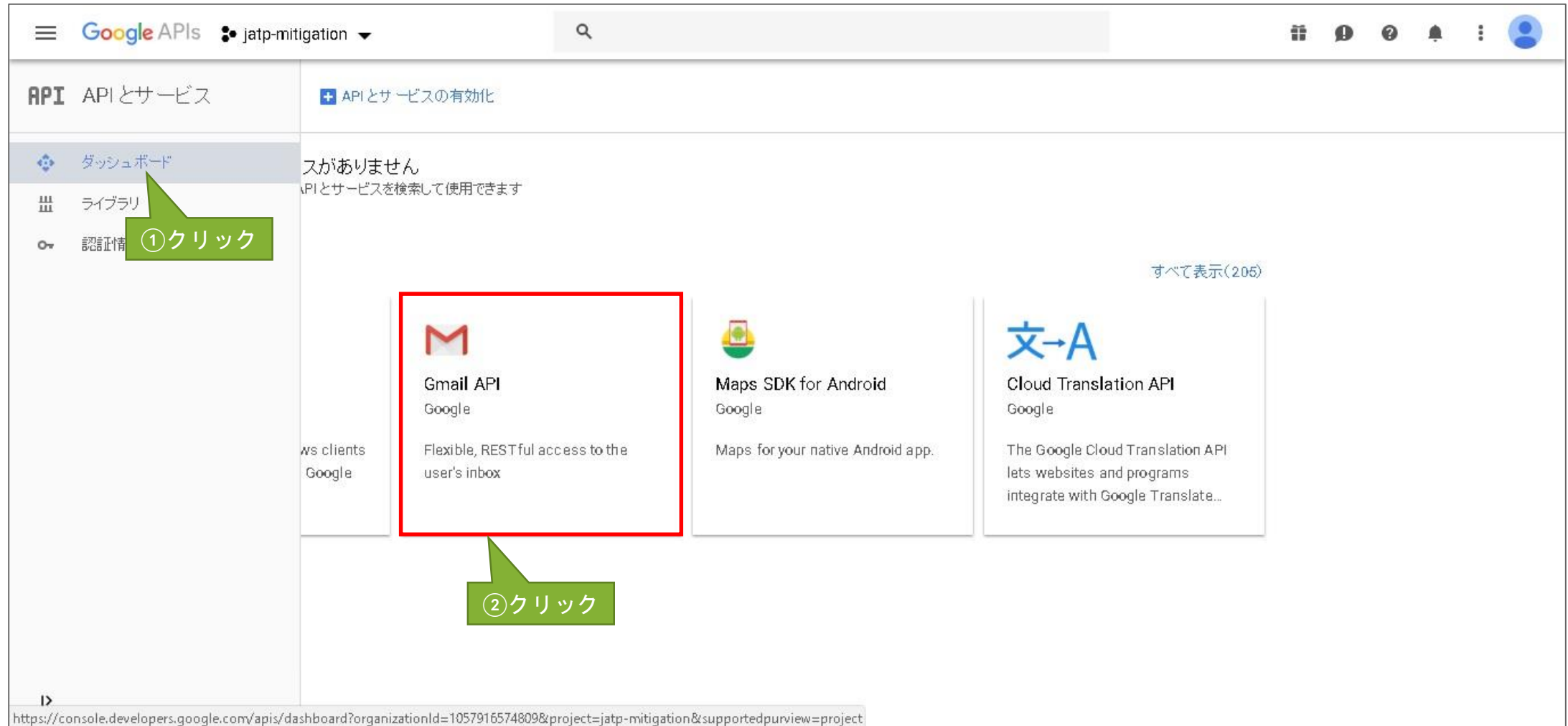
名前 ?

jatp-mitigation のクライアント

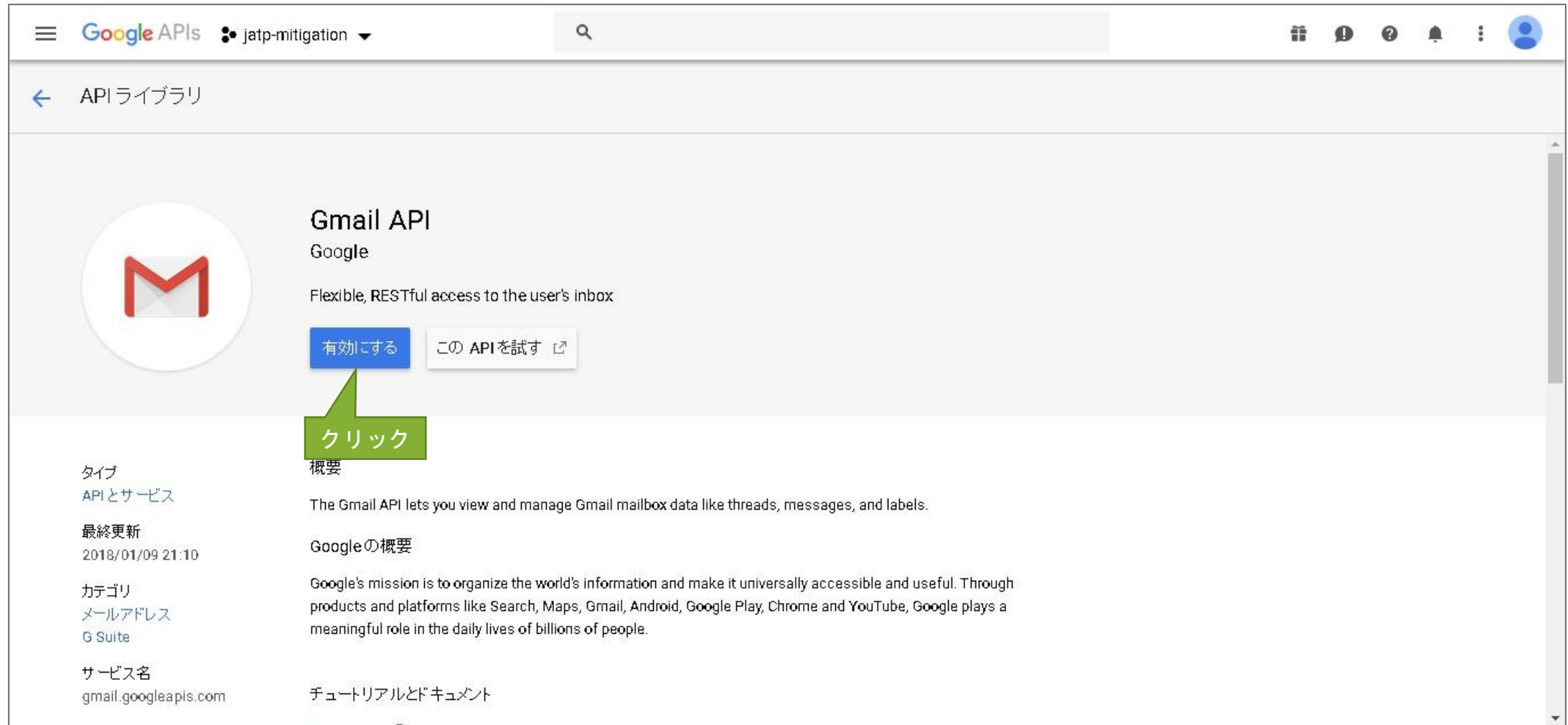
保存 キャンセル

②クリック

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




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



The screenshot shows the Google APIs console interface. At the top, there's a header with the Google APIs logo, a dropdown menu set to 'jatp-mitigation', and a search bar. Below the header, the page title is 'API ライブラリ' (API Library). The main content area displays the 'Gmail API' by Google. It features the Gmail logo, the text 'Flexible, RESTful access to the user's inbox', and two buttons: '有効にする' (Enable) and 'この API を試す' (Try this API). A green callout bubble with the text 'クリック' (Click) points to the '有効にする' button. On the left side, there's a sidebar with metadata: 'タイプ' (Type) as 'API とサービス' (API and Service), '最終更新' (Last updated) as '2018/01/09 21:10', 'カテゴリ' (Category) as 'メールアドレス' (Email address) and 'G Suite', and 'サービス名' (Service name) as 'gmail.googleapis.com'. The main content area also includes a '概要' (Overview) section with a description of the Gmail API and a 'Google の概要' (About Google) section with a brief description of Google's mission.

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

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

概要

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

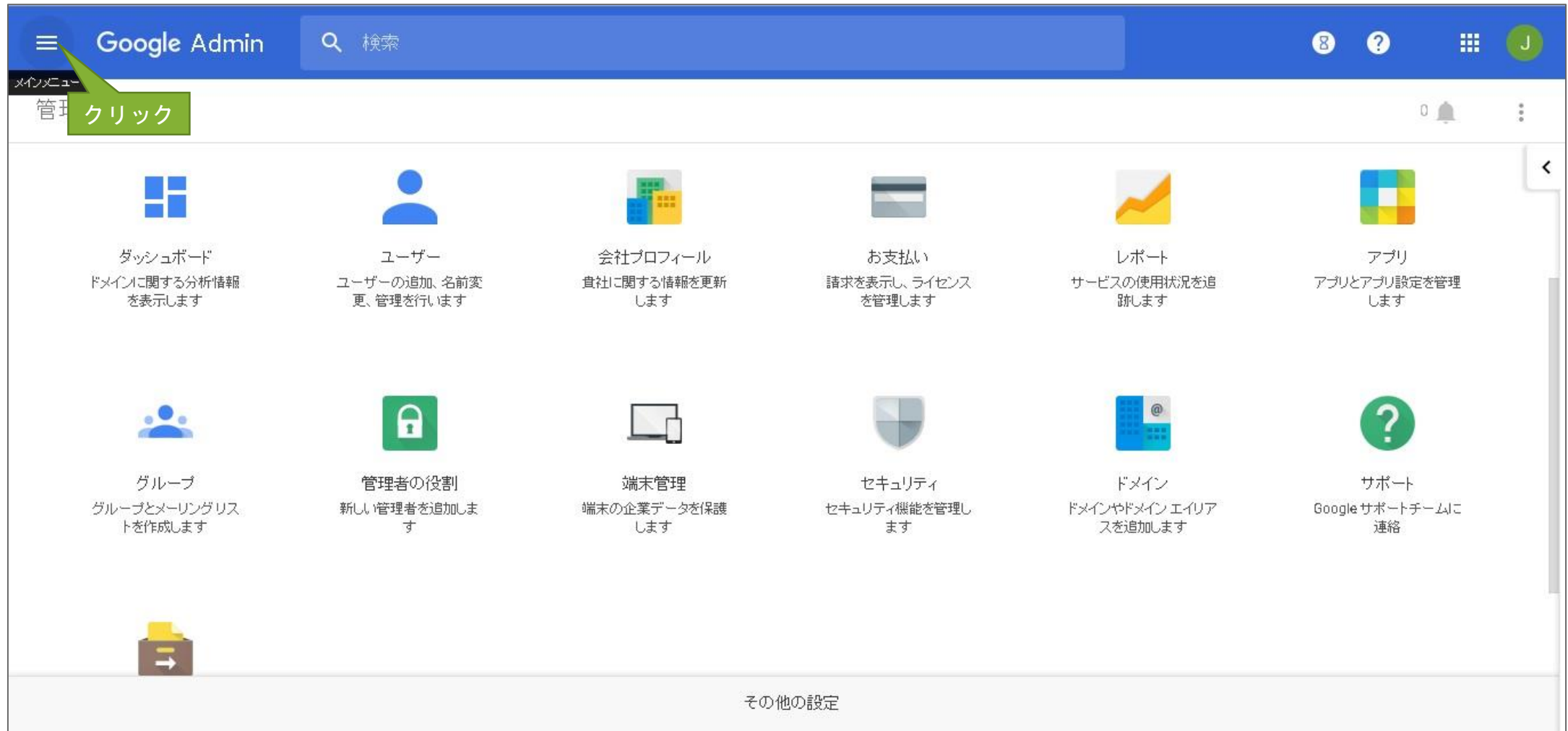
Google の概要

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.

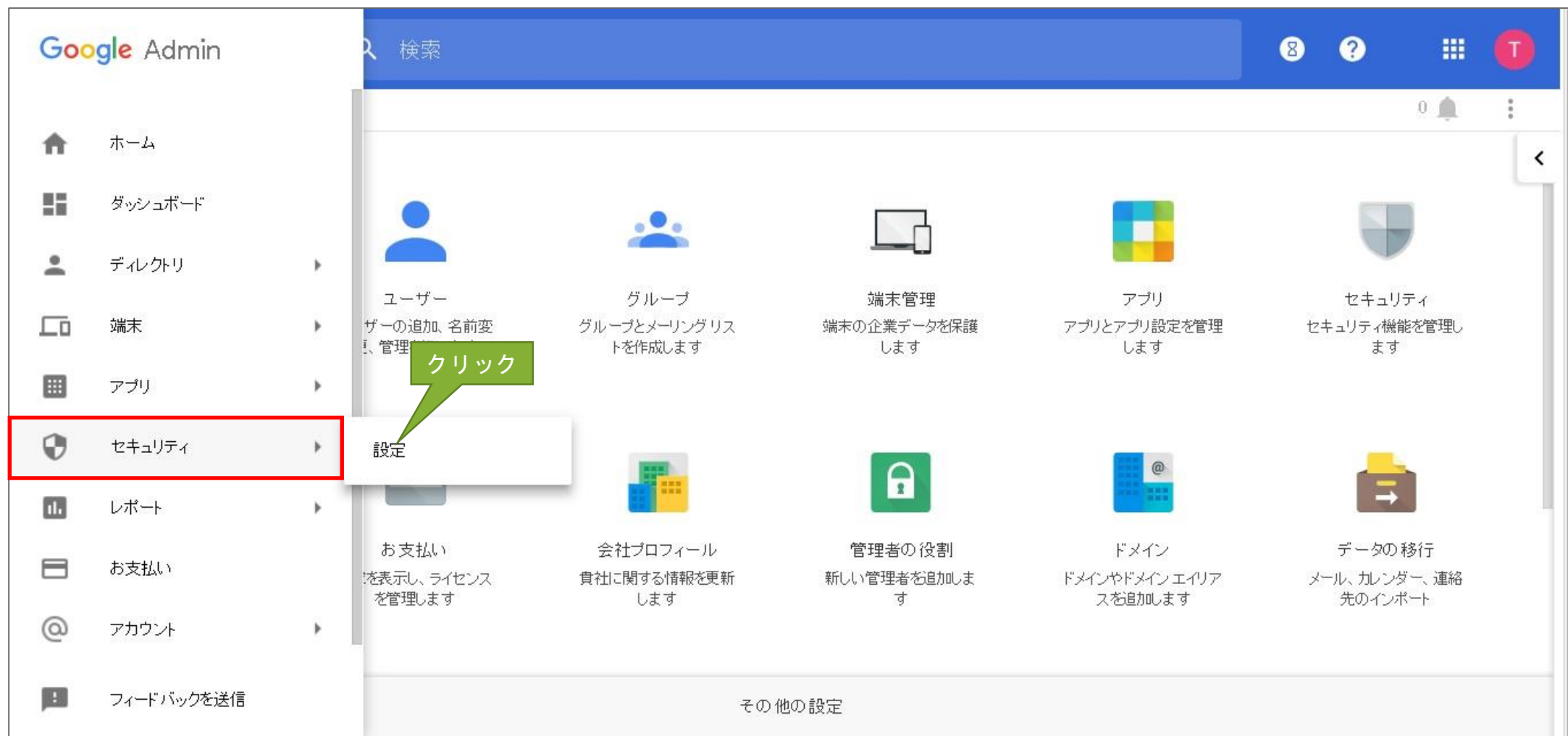
チュートリアルとドキュメント

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>) 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)

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	1 つ以上の API スコープ	
109021442147403274090 例: www.example.com	https://mail.google.com/ 例: http://www.google.com/calendar/feeds/ (カンマ区切り)	承認

[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

8 ?

T

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

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

Dashboard Incidents File Uploads Mitigation Reports Custom Rules **Config**

Notifications

System Profiles

System Settings

System Defaults

Hostname: Core1

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

IYP format: MSI Self-extracting Zip file Download MSI

Software Update enabled: ☒

Content Update enabled: ☒

Enable JATP support account: ☒

Restart services now: restart

Reboot appliance now: reboot

Clear event database: clear

Submit

Proxy Settings

Proxy Type: No Proxy Manual Proxy

Submit

Auto Mitigation Settings

Enable for Web: ☐

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)

ADVANCED THREAT PREVENTION APPLIANCE

Refresh Data System Health J-ATP Admin

Dashboard Incidents File Uploads Mitigation Reports Custom Rules Config

Users

Enable JATP support account: ☒

Restart services now: restart

Reboot appliance now: reboot

Clear event database: clear

Submit

Proxy Settings

Proxy Type: ☒ No Proxy ☐ Manual Proxy

Submit

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)

Submit

Display Settings

Maximum threats: 500

Default display period: Last Week

Session timeout: 15 (2 to 9999 minutes)

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

Powered by JuniperVersion 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 displays the Juniper J-ATP Admin web interface. The top navigation bar includes the Juniper logo, the title "ADVANCED THREAT PREVENTION APPLIANCE", and links for "Refresh Data", "System Health", and the user "J-ATP Admin". The main navigation menu on the left lists various configuration sections: Dashboard, Incidents, File Uploads, Mitigation, Reports, Custom Rules, and Config (which is currently selected). The left sidebar contains a list of settings: SAML Settings, RADIUS Settings, System Settings, Certificate Management, GSS Settings, Web Collectors, SRX Settings, Email Collectors, Secondary Cores, Golden Image VMs, Licensing, Backups/Restore, Test Malware Detection, and Environmental Settings. The main content area shows the "Config" page with several sections: "Enable JATP support account" (checked), "Restart services now" (restart), "Reboot appliance now" (reboot), "Clear event database" (clear), and a "Submit" button. Below this is the "Proxy Settings" section with "Proxy Type" set to "No Proxy" and a "Submit" button. The "Auto Mitigation Settings" section shows "Enable for Web" (unchecked), "Enable for Email" (checked), "Mitigation Aggressiveness Level" set to "Moderate" (with a note "(Only Max and High Threat confidence level)" and "(Threat Confidence Levels)"), and a "Submit" button. A white modal dialog box with the text "Auto Mitigation settings changed on the server" and an "OK" button is overlaid on the "Auto Mitigation Settings" section. A green callout bubble with the text "クリック" (Click) points to the "OK" button. The "Display Settings" section at the bottom shows "Maximum threats" set to 500, "Default display period" set to "Last Week", and "Session timeout" set to 15 minutes (with a note "(2 to 9999 minutes)"). The footer of the interface includes "Powered by Juniper Version 5.0.2.20 Content Version 5.0.2.14" and links for "Support", "Resources", and "Contact Us".

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

The screenshot displays the Juniper ATP configuration interface. The top navigation bar includes 'Dashboard', 'Incidents', 'File Uploads', 'Mitigation', 'Reports', 'Custom Rules', and 'Config'. The left sidebar lists various configuration categories, with 'Email Mitigation Settings' highlighted by a red box. Three green callout boxes with Japanese text provide instructions: '① クリック' (Click) points to the 'Email Mitigation Settings' item, '② クリック' (Click) points to the 'Add New Mitigation' button, and '③ クリック' (Click) points to the 'Description' field in the 'Current Email Mitigations Configured' table.

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

① クリック

② クリック

③ 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)

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

ADVANCED THREAT PREVENTION APPLIANCE

Dashboard Incidents File Uploads Mitigation Custom Rules Config

Notifications

System Profiles

Environmental Settings

Email Mitigation Settings

Firewall Mitigation Settings

Anti-Virus Configuration

Endpoint Integration Settings

BlueCoat Configuration

Whitelist Rules

YARA Rule Upload

SNORT Rule Upload

Identity Configuration

Splunk Configuration

External Event Collectors

Email Type:

Gmail

Exchange Online

Quarantine Label:

QuarantinedByJATP

Email Address (for Testing):

admin@juni-test.jp

Gmail JSON Key File:

```
{
  "type": "service_account",
  "project_id": "jatp-mitigation",
  "private_key_id": "c3e1d072774ac389b9dedb37420ed3f8d61cfeb2",
  "private_key": "-----BEGIN PRIVATE KEY-----
#nMIEvgIBADANBgkqhkiG9w0BAQEFAASCBAgEAAoIBAQDLcJ1LASTcdVxI#n
qKUr9jZDDi29DnqOmrVXj3Ua5KG91nxNLdUUcPS9ihwQkO92I9LTk99dAQ3wnLMm#nQ
-----END PRIVATE KEY-----"
```

Domains:

juni-test.jp

Add

Cancel

Current Email Mitigations Configured

Description	Actions
-------------	---------

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 displays the Juniper ATP Admin console interface. The top navigation bar includes 'Dashboard', 'Incidents', 'File Uploads', 'Mitigation', 'Reports', 'Custom Rules', and 'Config'. The left sidebar lists various settings, with 'Email Mitigation Settings' selected. The main content area shows 'Current Email Mitigations Configured' with a table containing one entry, 'Gmail'. The 'Actions' column for this entry includes 'Disable', 'Delete', 'Edit', and 'Test'. A green callout bubble with the text 'クリック' (Click) points to the 'Test' link. Above the table is a button labeled 'Add New Mitigation'.

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 50.2.20 Content Version 50.2.14

Support Resources Contact Us

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

The screenshot displays the Juniper ATP Admin console interface. The top navigation bar includes the Juniper logo, the title "ADVANCED THREAT PREVENTION APPLIANCE", and links for "Refresh Data", "System Health", and the user "J-ATP Admin". The main navigation menu on the left lists various configuration options, with "Email Mitigation Settings" selected. The central panel shows the "Current Email Mitigations Configured" section, which contains a table with one entry: "Gmail". Above this table is a button labeled "Add New Mitigation". A yellow callout box with the text "※接続テスト成功※" (Connection test successful) is overlaid on the table. Below the table, a white modal box with a red border displays the message "Test Successful" and an "OK" button. The footer of the console shows the version information "Powered by Juniper Version 50.2.20 Content Version 50.2.14" and links for "Support", "Resources", and "Contact Us".

Description	Actions
Gmail	Disable Delete Edit Test

※接続テスト成功※

Test Successful

OK

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

The screenshot shows the Juniper ATP Admin console interface. The top navigation bar includes 'Dashboard', 'Incidents', 'File Uploads', 'Mitigation', 'Reports', 'Custom Rules', and 'Config'. The left sidebar lists various settings, with 'Email Mitigation Settings' selected. The main content area shows 'Current Email Mitigations Configured' with a table containing one entry, 'Gmail'. A modal dialog is open, displaying the message 'Test Failed: No JSON object could be decoded' and an 'OK' button. A yellow callout box with the text '※接続テスト失敗※' (Connection test failed) is overlaid on the dialog.

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

※接続テスト失敗※

Test Failed: No JSON object could be decoded

OK

Powered by Juniper Version 50.2.20 Content Version 50.2.14

Support Resources Contact Us

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

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

ADVANCED THREAT PREVENTION APPLIANCE

Refresh Data System Health J-ATP Admin

Dashboard Incidents File Uploads Mitigation Reports

All Incidents (20 shown, 20 total)

Search: Show Threat Show Suspicious Show Benign Last Week

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

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

Threat : 驚異
Suspicious : 疑わしい
Benign : 良性

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

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

Triggers:

Reputation Behavior Network Static

Powered by JuniperVersion 50.2.20 Content Version 50.2.14

Support | Resources | Contact Us

EMAIL COLLECTOR動作確認手順

ADVANCED THREAT PREVENTION APPLIANCE

Refresh DataSystem HealthJ-ATP Admin

DashboardIncidentsFile UploadsMitigationReportsCustom RulesConfig

All Incidents (17 shown, 17 total)

Search:Show ThreatLast WeekCSV

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

SUMMARYPHISHING

Actions

Target:

Incident ID: 27

Hostname: -

Username: -

IP Address: -

FQDN: -

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

Progression:

DELIVERYEXPLOITATION & INSTALLATIONCOMMAND & CONTROLACTION ON TARGETS

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


Triggers:

ReputationBehaviorNetworkStatic

Powered by Juniper Version 50.2.20 Content Version 50.2.14SupportResourcesContact Us

分析結果がIncidentsに表示される

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@jntp-test.ddo.jp

Email Message ID: CADh4wB_rdAAcZr6eM4Ga2Lo_fabPKrrqyCk_fg= TTYBqE ttHA@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

Phishing 1

Exploits 0

Executions 0

Infections 0

Custom Rules 0

Lateral Spread 0

Triggers:

Reputation

Behavior

Network

Static

Custom Rules

Lateral Spread

Infection

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