



マトリックススキャン APEX ゲートウェイ概要

アンチスパム・ウイルス

マトリックススキャン APEX
アプライアンスサーバー

imatrix
アイマトリックス 株式会社

Confidential

本資料の開示を受けることを承認した者(以下「読者」)は、本資料に含まれるすべてのアイマトリックス株式会社及び関係する第三者の財務、事業計画、マーケティング、顧客、納入者、製品、技術、研究及びノウハウ等に関する情報 および、アイマトリックス株式会社から本資料の説明を受けて得たあらゆる情報(以下「情報」)を秘密にし、これをアイマトリックス株式会社から書面による承諾を得ずに、第三者に開示してはならない。「読者」は「情報」をアイマトリックス株式会社の目的とする事業への参画、関与、取引の検討もしくは製品の使用のみのために利用する。この制約は、「読者」が「情報」を開示される以前に知っていた情報、又は「読者」が法律上の手続きにより開示を要求される情報には適用されない。アイマトリックス株式会社が要請したとき、又は「読者」が事業への参画、関与もしくは取引の可能性がなくなったときは、「読者」は、本資料及び、「情報」を何らかの形で含有、構成、描写又はそれらに関連するあらゆる記録、データ、書類、媒体及びその他の品目並びにそれらの複製で、自らが所有又は管理しているものを、アイマトリックス株式会社に返却するか速やかに第三者に漏洩することなく破棄するものとする。

目次

1 . はじめに.....	1
2 . SMTP を透過的に扱うことによるメリット.....	2
3 . 配置構成について.....	4
4 . マルチ・ドメイン	5
5 . マルチ・レイヤ.....	6
6 . メールフィルタについて	7
7 . マルチ・ユニット.....	12
8 . Web ユーザインタフェース.....	14

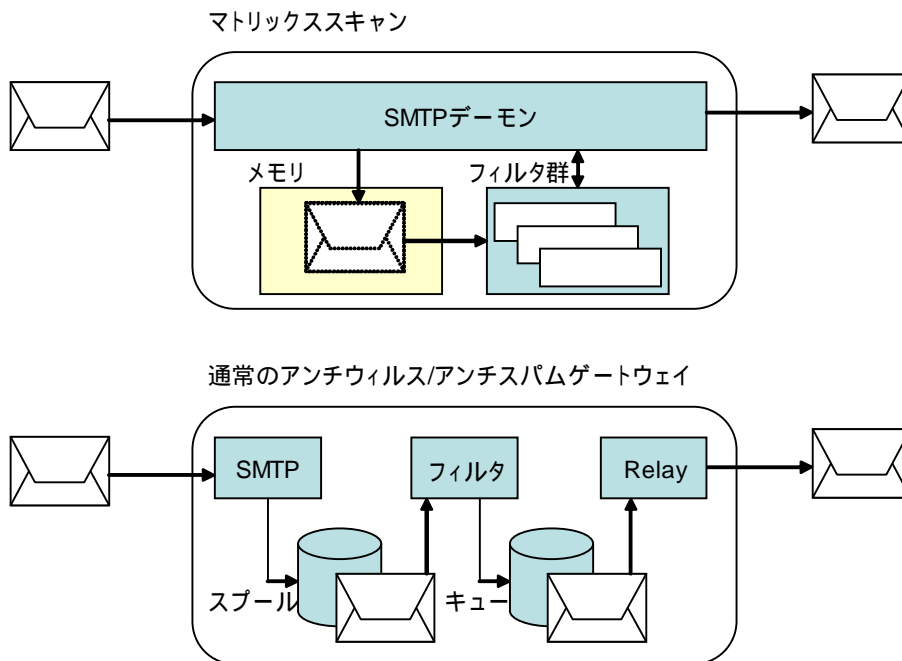
1. はじめに

マトリックススキャン APEX は以下の機能を持つメールセキュリティアプライアンスゲートウェイです。

- SMTP 透過
- マルチ・ドメイン/マルチ・レイヤ
- マルチ・アンチマルウェアフィルタ
- マルチ・ユニット
- Web ユーザインタフェース

2. SMTP を透過的に扱うことによるメリット

マトリックススキャンは SMTP を透過的に扱います。このため、以下のメリットを持ちます。



- 高速なメールスキャンおよびリレー

通常のアンチウイルス/アンチスパムゲートウェイ(メールサーバ含む)はハードディスク上にスプールしてからスキャンを行いキューイングしてから配送するという工程を踏むため、1通のメールを処理するために数回のハードディスク I/O が発生します。

マトリックススキャンは 1 通のメールの処理をすべてオンメモリで行います。このため、高速なメールスキャンおよびリレーを実現しています。

- 配送遅延/消失がない

通常のアンチウイルス/アンチスパムゲートウェイ(メールサーバ含む)は上述のようにメールをスプールします。このため、大量のメールを受信すると配送遅延が起こります。また、このときにハードディスク障害が発生した場合はメールの消失となります。

マトリックススキャンは SMTP を透過的に扱うため、マトリックススキャン自体に配送責任が発生しません。このため、配送遅延やメールの消失が起こりません。

配送責任:

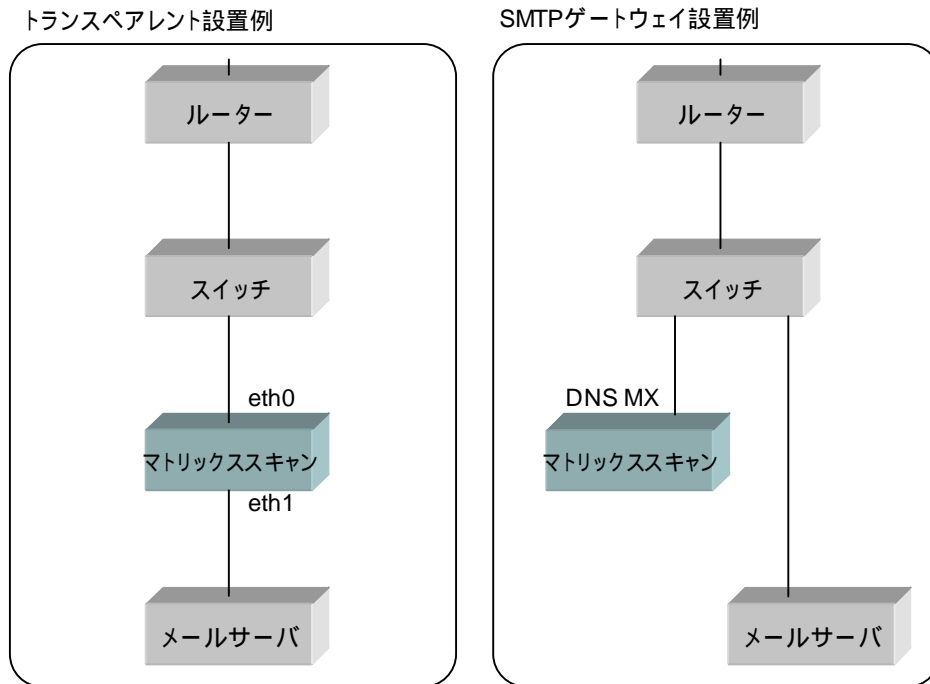
送信元メールサーバから来たメールを受け取ったことを応答した時点で、そのメールに対して配送責任が発生します。

マトリックススキャンは、送信元メールサーバへの応答を送信先メールサーバにメールを届けてから行います。

このため、マトリックススキャンに配送責任が発生することはありません。配送責任は送信元メールサーバから送信先メールサーバへ移行します。

3. 配置構成について

マトリックススキャンは以下の配置構成が可能です。



- トランスペアレント

スイッチ - メールサーバ間にブリッジとして接続するだけで配置可能です。マトリックススキャンに障害が発生した場合はバイパス NIC (標準搭載) によりメールの配信を止めることはありません。(マトリックススキャンのメールスキャンは行いません)

この構成時、マトリックススキャンはブリッジ (L2) のように動作します。SMTP (25 port/tcp) のみをフックし、スパム判定を行います。その他のプロトコルは透過します。

マトリックススキャンは送信元メールサーバの IP アドレスを用いて送信先メールサーバへ接続します。送信先/送信元メールサーバは間にマトリックススキャンが介在することに気が付きません。

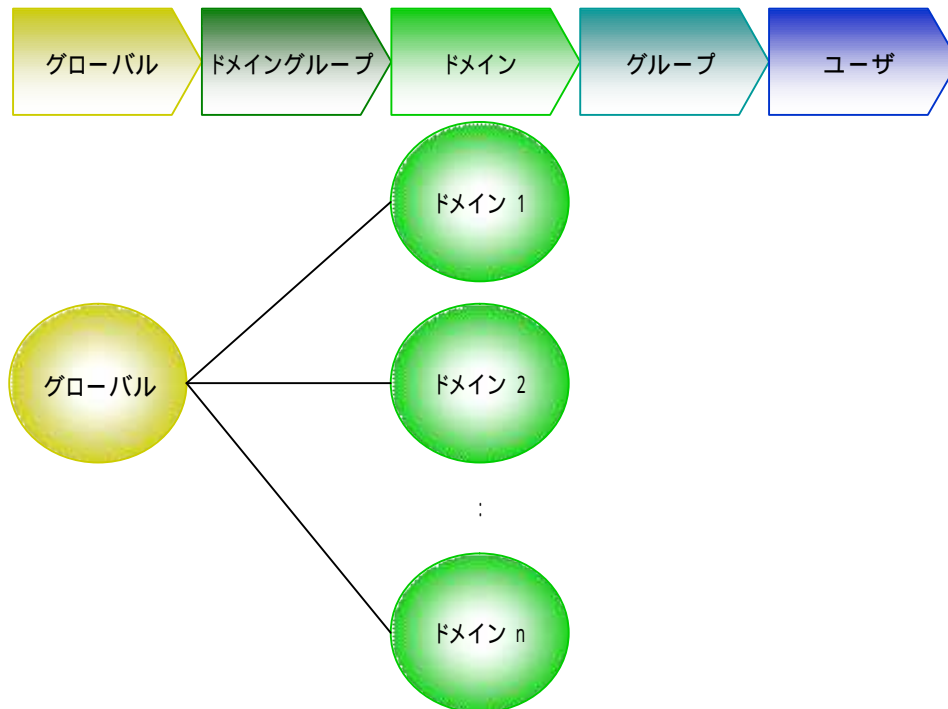
- SMTP ゲートウェイ

リレーサーバとして配置します。DNS の MX レコードをマトリックススキャンに向けるか、前段メールサーバのリレー先をマトリックススキャンに向けます。本構成時は、マトリックススキャンがメールの配送を行わないため、スマートホスト (配送

可能なメールサーバ)が必要となります。

4. マルチ・ドメイン

マトリックススキャンは1台で複数のドメインを扱うことができます。後述のマルチ・レイヤのドメイングループを使用することで複数のドメインを1つの設定で扱うことも可能です。



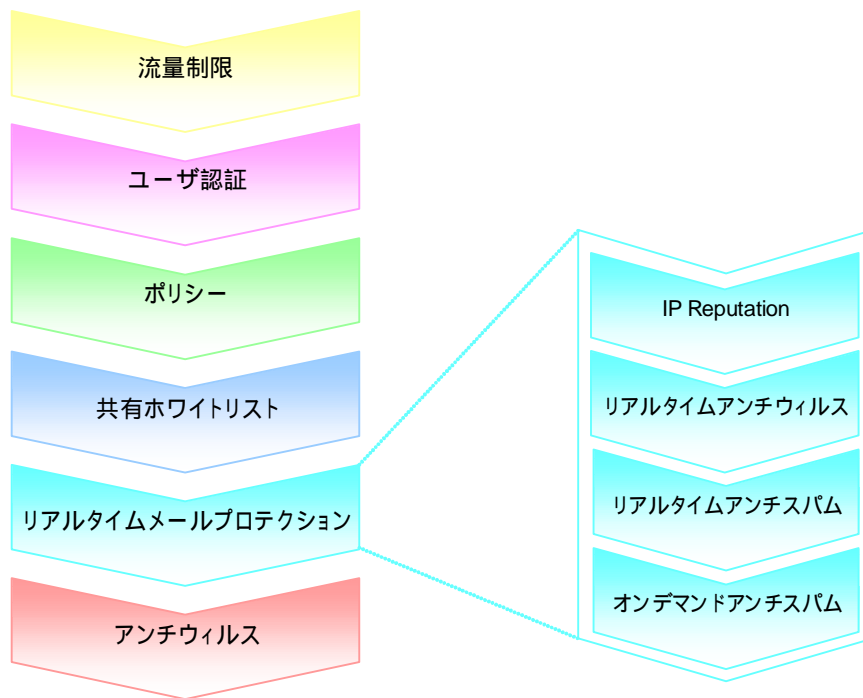
5. マルチ・レイヤ

マトリックススキャンは以下の5レイヤを用いて設定を管理できます。設定やポリシーはグローバルから順に適用されます。

- グローバル
マトリックススキャン全体を管理するレイヤです。ドメイン毎やユーザ毎にスパムメールの扱いが同じときはグローバルレイヤを設定するのみです。
- ドメイングループ
複数のドメインをまとめて管理するレイヤです。例えばある企業が複数のドメインを保持していてドメイン毎に管理する必要が無い場合や、B2B2C サービスの提供元などで使用するレイヤです。
- ドメイン
ドメインを管理するレイヤです。ドメインでスパムメールを扱うときに使用するレイヤです。
- グループ
複数のユーザをまとめて管理するレイヤです。例えば営業部のユーザは共通の設定にするといった用途に使用します。
- ユーザ
メールアドレスと等価なレイヤです。ユーザ毎にポリシー（ホワイトリストやブラックリスト）や隔離フォルダを利用するときに使用するレイヤです。

6. メールフィルタについて

マトリックススキャンは以下のフィルタによってスパムメールやウィルスメールおよび、不当なアクセスからメールサーバを防御します。



各フィルタは ON/OFF が可能です。またマトリックススキャンの管理階層毎に設定を変更することが可能です。以下に各フィルタの特徴を示します。

● 流量制限

流量制限は以下の機能を提供します。流量制限を通過した SMTP セッションは以降のフィルタに処理が渡ります。

- ◇ サーバ全体の SMTP コネクション制限
 - 最大接続数
 - 同一送信元毎の同時接続数
 - 同一送信先毎の同時接続数
- ◇ ポリシー (ホワイトリスト/ブラックリスト)
 - 対象: IP アドレス (ネットワークアドレス)、送信者 (送信者ドメイン)
 - 動作: 接続数や通数などを閾値で制限
- ◇ レート制限

- 対象:不特定の IP アドレスを自動トラック
- 動作:単位時間あたりの接続数や通数などを閾値で制限
- ◇ IP Reputation
 - 対象:不特定の IP アドレスを自動トラック
 - 動作:IP Reputation の評価値を閾値として制限
送信元メールサーバの IP アドレスを評価します。
SMTP コネクションのソース IP アドレス

流量制限はマトリックススキャンを最もインターネット側に設置 (DNS MX レコードがマトリックススキャン) した場合に利用することが最善です。内部 SMTP リレー経路中にマトリックススキャンを設置した場合は流量制限の使用は推奨できません。(内部メールサーバに対して流量制限がかかるため)

● ユーザ認証

ユーザ認証はドメインやユーザの存在確認によってメールの扱いを制限します。ユーザ認証では、以降のフィルタを適用しない/するが選択できます。適用しない設定のときは以降のフィルタは適用されずにメールを受信します。(注1)

利用可能な認証は以下の通りです。

- ◇ マトリックススキャン
- ◇ LDAP
- ◇ NIS

● ポリシー

ポリシー (ホワイトリスト/ブラックリスト) に従いメールを処理します。ポリシーを適用したメールは以降のフィルタは適用されません。(注1)

ポリシーは以下の項目から構成されます。

◇ 対象

- ドメイン (メールアドレスの@より後ろ)
- 差出人 (メールアドレス)
- ローカル (メールアドレスの@より前)
- IP アドレス (送信元メールサーバアドレス)

◇ 動作

- 承認
対象メールを受信します。

- 削除
対象メールを削除します。
- 隔離
対象メールを隔離します。
- 転送
対象アドレスを指定メールアドレスへ転送します。
- 拒否(ソフト/ハード) (注)グローバルレイヤのみ
対象メールを拒否(ソフト/ハード)します。
ソフトは一時エラー(4xx)、ハードは恒久エラー(5xx)を応答します。
- リダイレクト
対象メールを指定メールサーバへリダイレクトします。

ポリシーは、ブラックリストも設定できますが、ホワイトリストで運用することを推奨します。現状のスパムはブラックリストでは追従することが困難であるため、スパムの判定は後述の IP Reputation やリアルタイムメールプロテクションに比重を置いてください。

- 共有ホワイトリスト(msec)

共有ホワイトリストを用いて正当なメールを確定します。共有ホワイトリストを適用したメールは以降のフィルタは適用されません。(注1)

共有ホワイトリストはアイマトリックス社が運営する日本スパム検出センタで管理されています。共有ホワイトリストはコラボレーションモデルよりメンテナンスされます。共有ホワイトリストへの登録依頼はマトリックススキャンの Web ユーザーインタフェースから行えます。

共有ホワイトリストの詳細は『マトリックススキャン APEX 技術概要』を参照願います。

- リアルタイムメールプロテクション

マトリックススキャンは以下のフィルタ群を用いてスパム判定を行います。

- ◇ IP Reputation

IP アドレス毎の評価結果を閾値によってスパムメールおよび正当なメールを確定します。IP Reputation を適用したメールは以降のフィルタは適用されません。(注1)

メールヘッダから IP アドレス走査し、見つけた送信元 MTA メールサーバの

IP アドレスを評価します。(Received ヘッダから既知のアドレスを除いた IP アドレス)

◇ リアルタイムアンチスパム

コムタッチ社 RPD テクノロジーを用いてスパム判定を行います。リアルタイムアンチウイルスを適用したメールはオンデマンドアンチスパムにより、別のアンチスパム検出方法を持ってスパム判定を行います。コムタッチ社 RPD テクノロジーの特徴を以下に記述します。

- リアルタイム
- コンテンツ不問(言語、フォーマット非依存)
- 高検出率/低誤検出

◇ リアルタイムアンチウイルス(オプション提供)

コムタッチ社 Zero Hour Virus Protection を用いてウイルス判定を行います。リアルタイムアンチスパムを適用したメールは以降のフィルタを適用しません。(注1)

コムタッチ社 Zero Hour Virus Protection の特徴を以下に示します。

- リアルタイム
- コムタッチ社 RPD テクノロジーを応用
- ウィルス発生直後から判定可能
- ヒューリスティックや推量に依らない決定方法

◇ オンデマンドアンチスパム(msec)

アイマトリックス社が運営する日本スパム検出センタに収集したスパムメールから抽出した情報を基にスパム判定を行います。マトリックススキャンは受信したメールを判定するために必要なスパム情報を日本スパム検出センタに要求します。日本スパム検出センタは、そのメールに必要なスパム情報をオンデマンドで配信します。マトリックススキャンは配信されたスパム情報を用いて受信したメールの判定を行います。

オンデマンドアンチスパムの詳細は『マトリックススキャン APEX 技術概要』を参照願います。

● アンチウイルス(オプション提供)

カスペロスキー社アンチウイルスエンジンを用いてウイルス判定を行います。マトリックススキャンはオンメモリでウイルス判定ができるようカスペロスキー社アンチウイルスエンジンをインテグレートしています。

アンチウイルス判定はすべてのメールに対して行います。

カスペロスキー社アンチウイルスエンジンについてはカスペロスキー社サイト (<http://www.kaspersky.co.jp>)で確認願います。

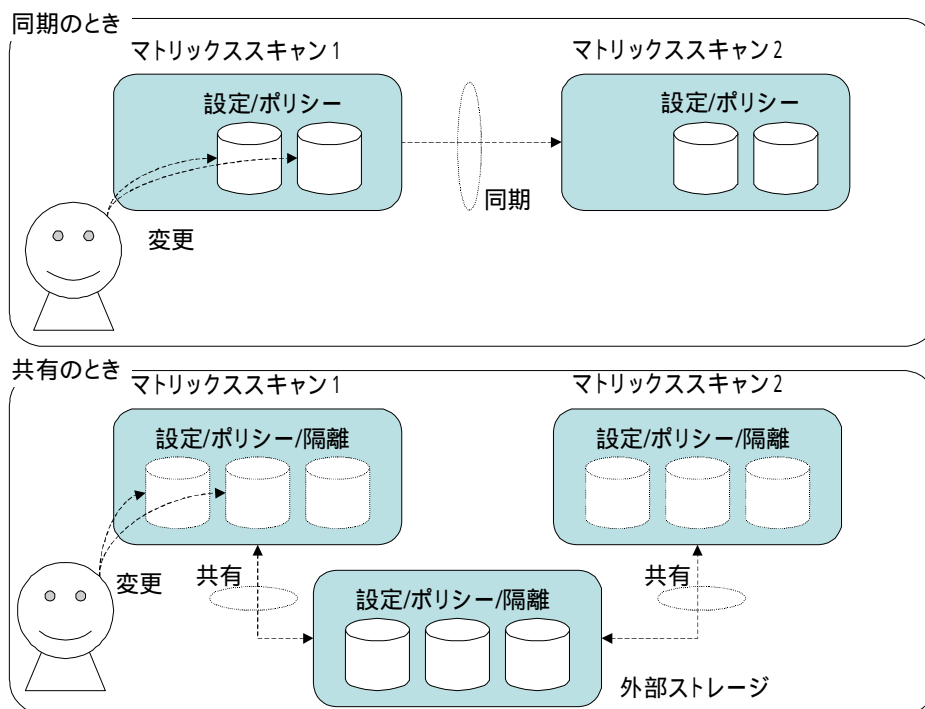
(注1) この場合もアンチウイルスは行います。

7. マルチ・ユニット

マトリックススキャンは複数台を同時に稼働させるために以下の機能を提供しています。

- 同期/共有

同期させる機能や設定・データ(隔離フォルダなど)を外部ストレージへ共有する機能があります。



- ◇ 同期

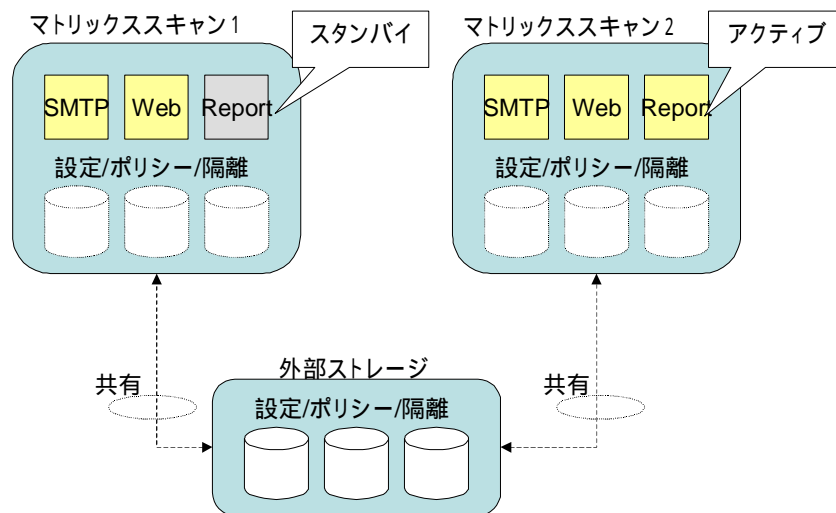
同期では以下の設定とポリシーを複数台のマトリックススキャンで同期します。隔離フォルダは同期されません。隔離フォルダを一元管理する場合は共有を使用してください。

- ◇ 共有

共有では設定・ポリシー・隔離フォルダ・ゴミ箱を複数台のマトリックススキャンで共有します。共有は NFS を使用しています。このため、外部ストレージが利用できます。

- 冗長化

冗長化機能によってサービス毎にアクティブ/スタンバイ(アクティブ/アクティブ含む)することによりサーバリソースの分散が可能です。



図のように SMTP サービスと Web ユーザインタフェースは両方のマトリックススキャンで動作させ、隔離フォルダレポートの送信はマトリックススキャン2のみで行うなどの運用が可能です。

8 . Web ユーザインタフェース

マトリックススキャンは設定や操作を Web ユーザインタフェースで行います。マトリックススキャンが管理するすべてのレイヤとシステム的な設定を提供します。

グローバル	ドメイングループ	ドメイン	グループ	ユーザ
システム設定 ネットワーク メール/ウェブ設定 ハニーポット 冗長化設定 メンテナンス ログ稼働状況 メールマネージャ システムレポート 流量制限 基本設定 ポリシーエディタ 共有ホワイトリスト 隔離フォルダ スпамウォッチ レポート ゴミ箱 検知漏れ・誤検知 管理者	基本設定 ポリシーエディタ 共有ホワイトリスト 隔離フォルダ スпамウォッチ レポート ゴミ箱 検知漏れ・誤検知 管理者	基本設定 ポリシーエディタ 共有ホワイトリスト 隔離フォルダ スпамウォッチ レポート ゴミ箱 検知漏れ・誤検知 管理者	基本設定 ポリシーエディタ 共有ホワイトリスト 隔離フォルダ スпамウォッチ レポート ゴミ箱 検知漏れ・誤検知 管理者	基本設定 ポリシーエディタ 隔離フォルダ サスペクトリスト ゴミ箱

各機能の詳細や操作・設定方法は『マトリックススキャン APEX オペレーションマニュアル』を参照願います。