



おまかせアンチウイルス

おまかせアンチウイルス 新iOSエージェント機能説明資料

2 0 2 5 年 7 月

NTT 東日本 株式会社

本資料は、2024年4月リリースのiOSエージェントの新バージョンについて記載した資料です。

用語と略称について

本書では、下記の略称を用いている場合があります。

おまかせアンチウイルス・・・「VBBSS」

※VBBSS(ウイルスバスタービジネスセキュリティサービス)は、
トレンドマイクロ株式会社の登録商標です。

リリース概要

iOSエージェントで脅威対策が可能になりました

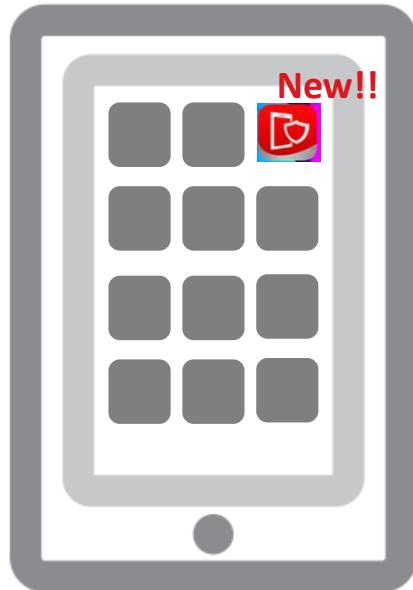
リリースされる新エージェントでは、リモートロックなど簡易MDM機能に加え、不正なWebサイトや不正なアプリなどからの脅威対策も実施いただけるようになりました。

iOS向けの主な機能

- New!!** • Webレビューテーション
- New!!** • Wi-Fi保護
- New!!** • 設定マネージャ
- New!!** • モバイル検索
- New!!** • 承認済み/ブロックするURLリスト
 - パスコード
 - リモートロック
 - Face ID、Touch ID、パスワードクリア
 - リモート消去

アプリタイプのエージェントとして登場

今まで、iOS向けのVBBSSエージェントはプロファイルとして提供していましたが、新エージェントはアプリとして提供いたします。



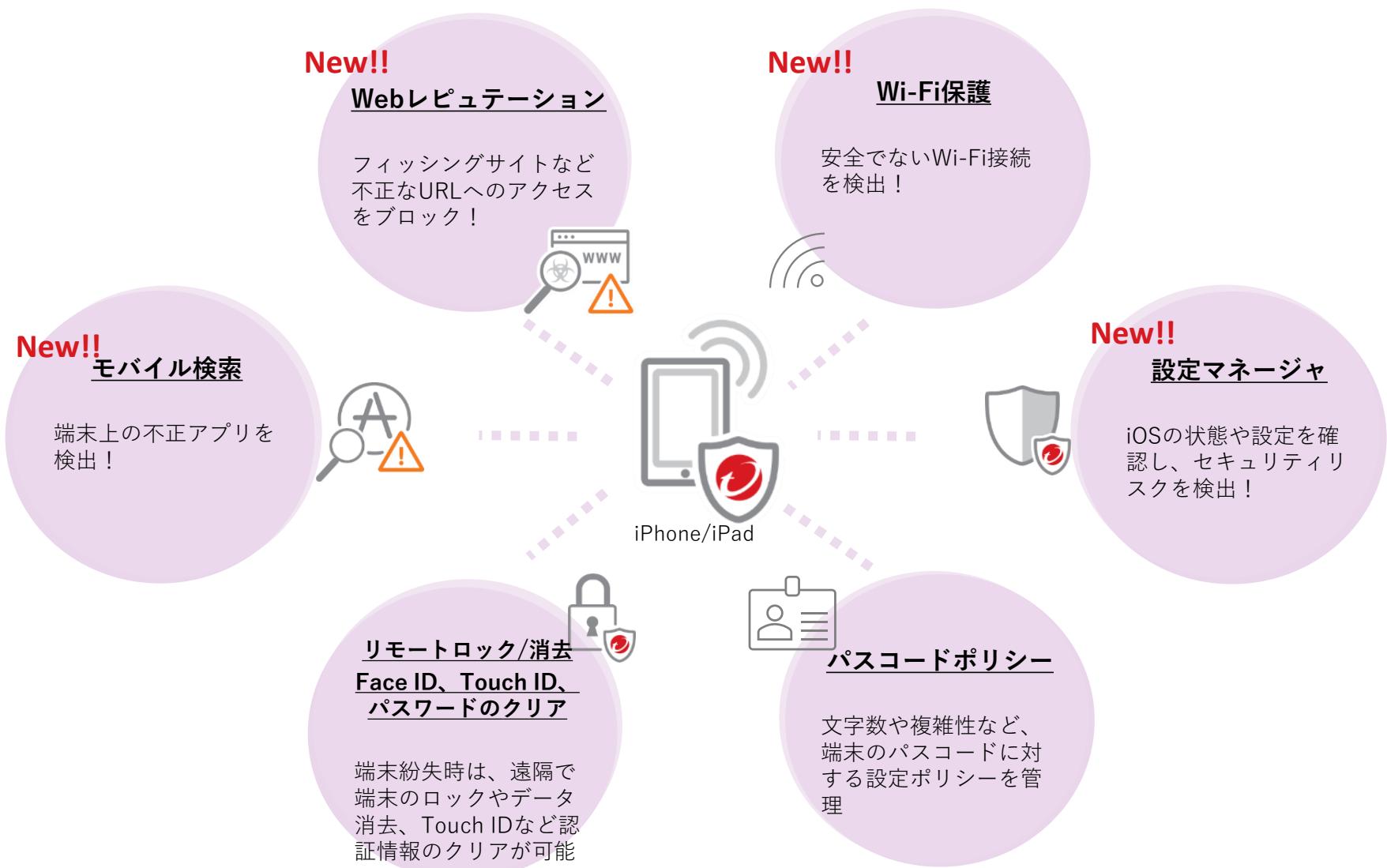
参考) 通信要件の追加

新エージェント利用にあたり、必要となる通信要件を追加します。

上位ネットワーク機器で通信制限を行っている場合は、以下URLのアウトバウンド通信を許可してください。

項目	ポート	URL	説明
VBBSSサーバ	80/443	*.mobile.trendmicro.com *.xdr.trendmicro.com	アカウント認証
VBBSSサーバ	80/443	wfbs-svc-nabu-aal.trendmicro.com	定期的なアクセス ・端末情報の更新 ・設定情報の取得 APNs証明書のダウンロード
スキャンサーバ	80/443	rest.mars.trendmicro.com rest-g.mars.trendmicro.com mint.mars.trendmicro.com portal-sg.mobile.trendmicro.com	クラウドスキャンサーバ
MARS Pattern Server	80/443	rest-g-au.mars.trendmicro.com	パターンアップデート
レビューションサーバ	80/443	mxdr1-0.url.trendmicro.com mxdr1-0-im.url.trendmicro.com mxdr1-0-ios.url.trendmicro.com	Webレビューションの問い合わせ
ブロックページ	80/443	mobile-block.wfbs-svc.trendmicro.com	WebレビューションでURLを ブロックした際のページ

新機能



Webレビューション

URLの信頼性評価情報を参照して、フィッシングサイトや不正URLなどへのアクセスをブロック。Webの脅威からiOSエージェントを保護します。

「セキュリティエージェント」 - 任意のグループの「ポリシーの設定」 - 「Webレビューション」

New!!

ポリシーの設定: デバイス (初期設定) X

対象とサービスの設定 ?

Windows Apple Android iOS ?

Webレビューション ?

Webレビューションは不正Webサイトの脅威からの保護を強化します。

セキュリティレベル

	危険	極めて不審	不審
高	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
中 (初期設定)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
低	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Webサイトのアクセスをブロックします ?

未評価のURL

トレンドマイクロによる評価が完了していないWebサイトをブロックする ?

Webレビューション

承認済み/ブロックするURL リスト

Webレビューション機能搭載に伴い、「承認済み/ブロックするURL」の登録も可能になりました。必要に応じて、接続を許可するURLやブロックするURLを登録できます。

「セキュリティエージェント」 - 任意のグループの「ポリシーの設定」 - 「承認済み/ブロックするURL」

ポリシーの設定: デバイス (初期設定)

対象とサービスの設定

Webレビューション

● パスコード

設定マネージャ

Wi-Fi保護

承認済み/ブロックするURL

承認済み/ブロックするURLのリスト

承認済み/ブロックするURLはWebレビューションに適用されます。

使用する除外:

グローバル承認済みおよびブロックするURLのリスト ⓘ

除外の指定

Webレビューションで誤って分類されている可能性のあるURLを通知するか、URLの安全性の
<http://sitesafety.trendmicro.com/>

New!!

設定マネージャ

iOS端末の状態や設定をスキャンし、セキュリティリスクを検出します。

「セキュリティエージェント」 - 任意のグループの「ポリシーの設定」 - 「設定マネージャ」

ポリシーの設定: デバイス (初期設定)

対象とサービスの設定

Windows Apple Android iOS GPS

Webレビュー
Webレビューション

● パスコード

New!! **設定マネージャ**

Wi-Fi保護

承認済み/ブロックするURL

設定マネージャ
構成スキャンの条件を指定します。

- Jailbreakされたデバイス
- ロック画面が無効
- 旧版のOS
- 脆弱なOS

悪意のあるアプリが実行できるように改ざん(ジェイルブレイク)されたOSを検出する

画面ロックの無効設定を検出する

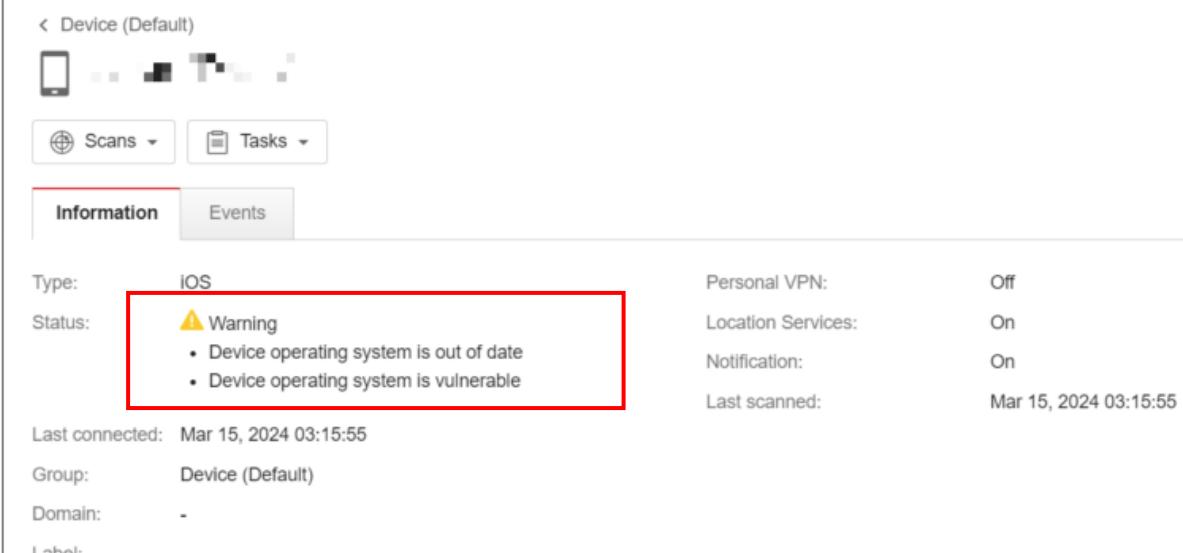
OSが最新でない状態を検出する

OSが脆弱であることを検出する

設定マネージャ

設定マネージャによるスキャンの結果、セキュリティリスクが検出された端末は、管理コンソール上の端末ステータスにアラート表示されます。

「セキュリティエージェント」 - 任意の端末をクリック - 「情報」



Device (Default)

Scans Tasks

Information Events

Type: iOS

Status: ⚠ Warning

- Device operating system is out of date
- Device operating system is vulnerable

Personal VPN: Off

Location Services: On

Notification: On

Last scanned: Mar 15, 2024 03:15:55

Last connected: Mar 15, 2024 03:15:55

Group: Device (Default)

Domain: -

Label: -

Wi-Fi保護

中間者攻撃やSSLストリッピング、暗号化が不十分なWi-Fi接続を検出しアラート表示します。

「セキュリティエージェント」 - 任意のグループの「ポリシーの設定」 - 「Wi-Fi保護」

ポリシーの設定: デバイス (初期設定)

対象とサービスの設定

Windows Apple Android iOS その他

Webレビューション

● パスコード

設定マネージャ

New!!

Wi-Fi保護

承認済み/ブロックするURL

Wi-Fi保護

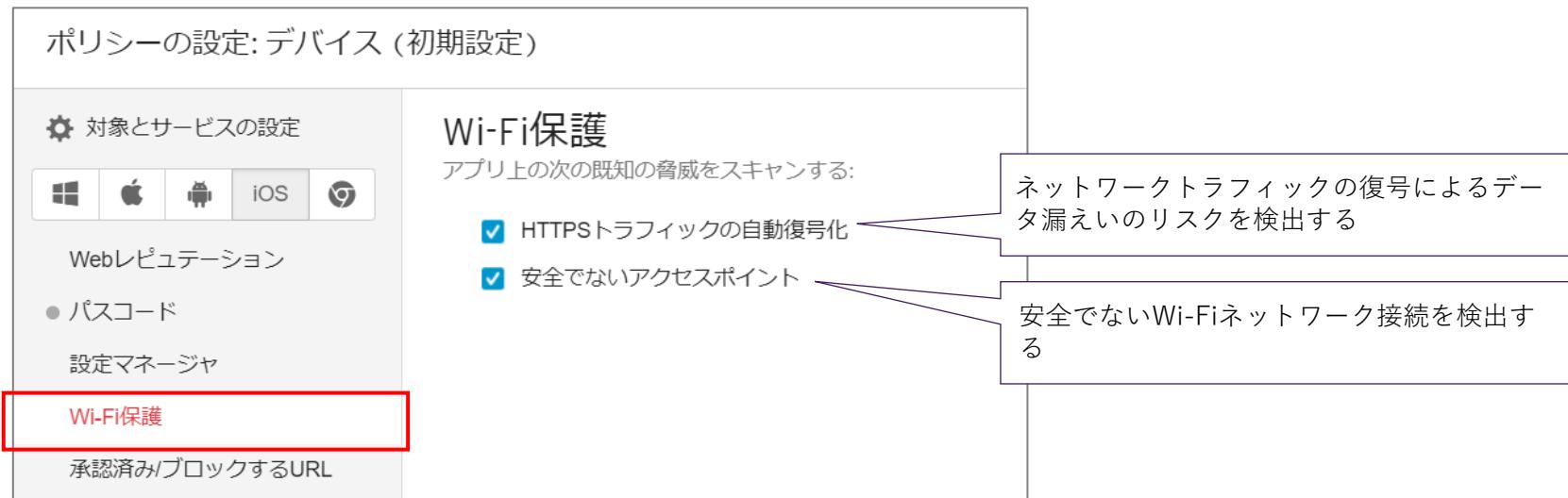
アプリ上の次の既知の脅威をスキャンする:

HTTPSトラフィックの自動復号化

安全でないアクセスポイント

ネットワークトラフィックの復号によるデータ漏えいのリスクを検出する

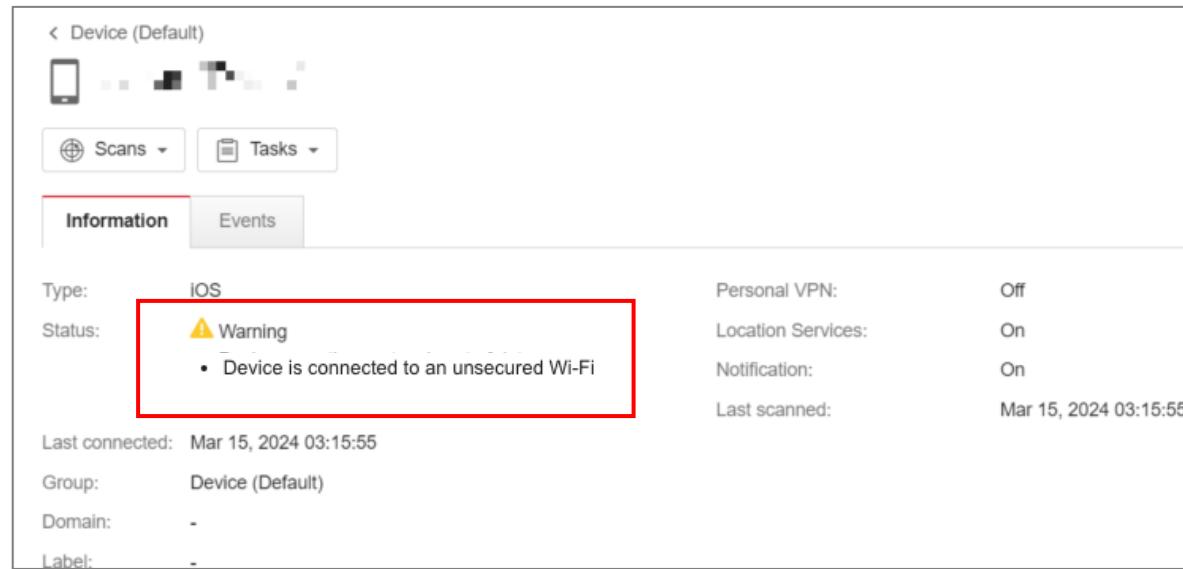
安全でないWi-Fiネットワーク接続を検出する



Wi-Fi保護

Wi-Fi保護機能によるスキャンの結果、セキュリティリスクが検出された端末は、管理コンソール上の端末ステータスにアラート表示されます。

「セキュリティエージェント」 - 任意の端末をクリック - 「情報」



The screenshot shows the 'Information' tab for a device named 'Device (Default)'. The device is identified as an 'iOS' type. A red box highlights the 'Status' section, which shows a 'Warning' icon and a list: 'Device is connected to an unsecured Wi-Fi'. To the right, device settings are listed: Personal VPN (Off), Location Services (On), Notification (On), and Last scanned (Mar 15, 2024 03:15:55). At the bottom, there are fields for Group (Device (Default)), Domain (-), and Label (-).

Type:	IOS
Status:	Warning <ul style="list-style-type: none">Device is connected to an unsecured Wi-Fi
Personal VPN:	Off
Location Services:	On
Notification:	On
Last scanned:	Mar 15, 2024 03:15:55
Last connected:	Mar 15, 2024 03:15:55
Group:	Device (Default)
Domain:	-
Label:	-

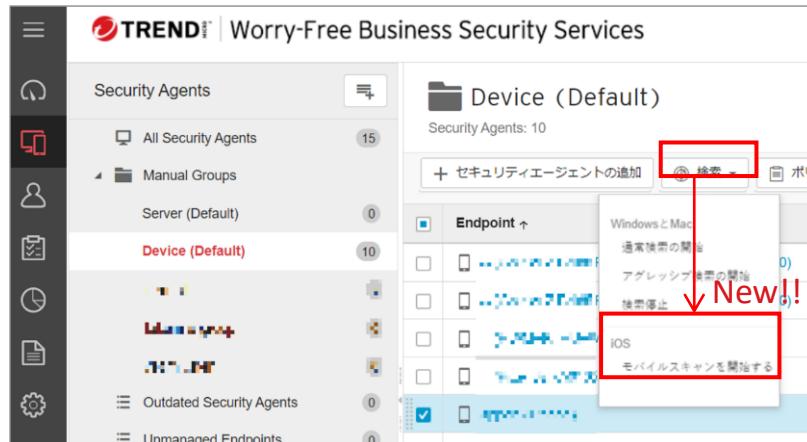
モバイル検索

iOS端末上に不正アプリがインストールされていないか検索します。

本機能に関する設定項目はありません。管理コンソールから任意のタイミングで手動検索を開始します。

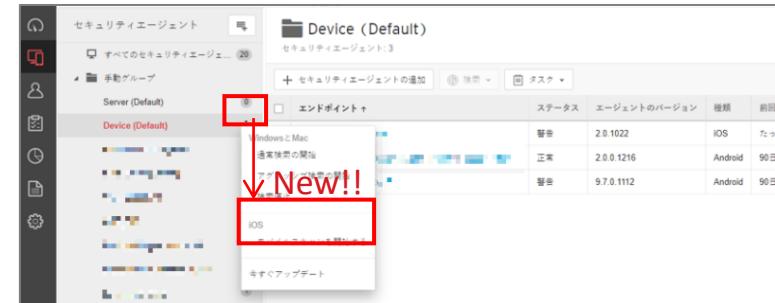
■任意の端末を選んで実行

「セキュリティエージェント」 - 任意の端末を選択し、
「検索」 - 「モバイル検索を開始する」



■任意のグループを選んで実行

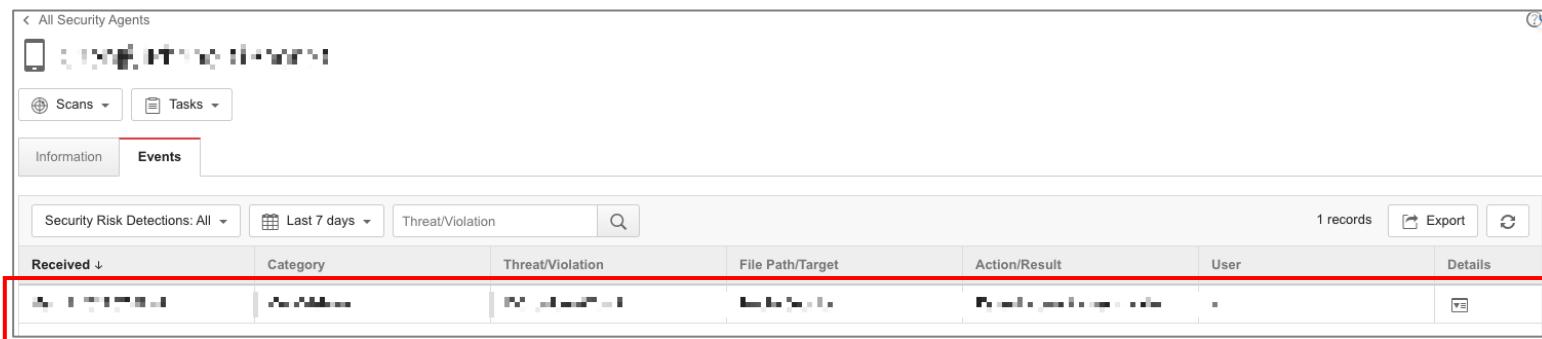
「セキュリティエージェント」 - 任意のグループの[...]を右クリック - 「モバイル検索を開始する」



モバイル検索

モバイル検索の結果、不正アプリが検出された端末は、
管理コンソール上の端末イベントログにアラート表示されます。
不正アプリが検出された場合は該当端末にて不正アプリを削除してください。

「セキュリティエージェント」 - 任意の端末をクリック - 「イベント」

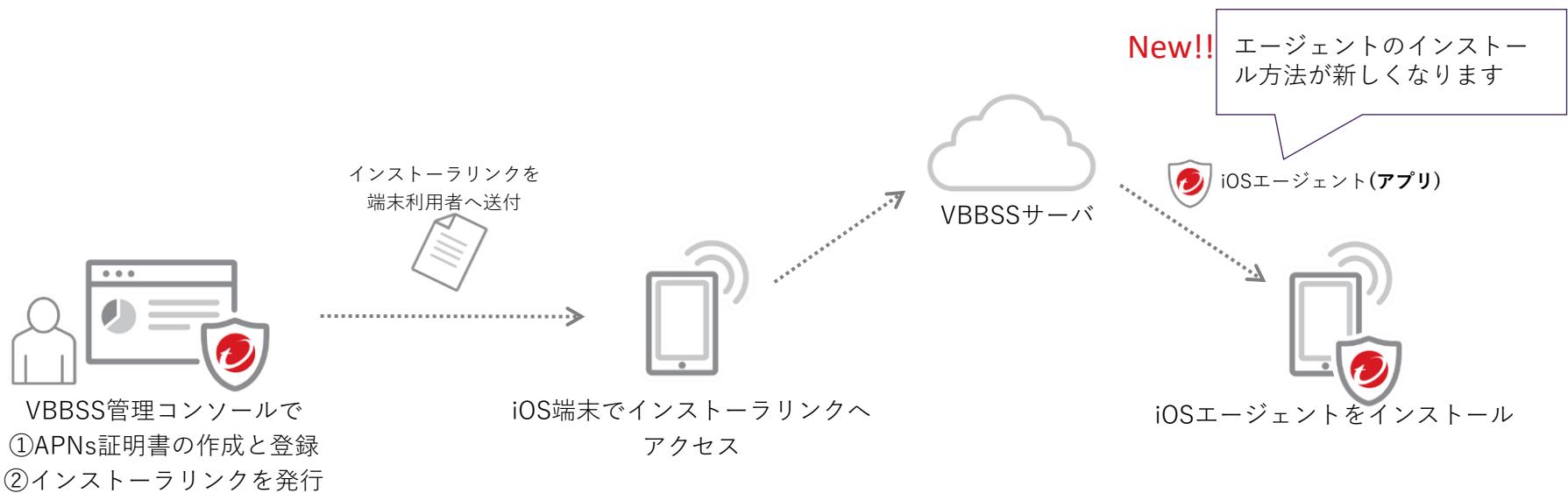


The screenshot shows the 'Events' tab of the Security Agent interface. A single record is listed, indicating a threat detection. The row is highlighted with a red box.

Received	Category	Threat/Violation	File Path/Target	Action/Result	User	Details
2023-10-01 10:00:00	Mobile Device	Malicious Application	/data/applications/malicious.apk	Quarantine		View Details

インストール手順

新エージェント インストールの流れ



インストーラリンクの発行と送付

インストーラリンクを発行し、各iOS端末利用者へメールなどで送付します。

セキュリティエージェントのインストール方法

インストール方法の選択: セキュリティエージェントの追加先: 初期設定

インストール用リンクの送信

一括送信 個別送信

CSVファイルに記載された複数のユーザーに送信します。 メールコンテンツの表示リンクの有効期限の設定

インストーラのダウンロード このエンドポイントにインストール

ダウンロード iOSエージェントは対象外 インストール

配信スクリプトを使用したインストール方法の使用 MSIパッケージを使った他のインストールオプションの手順

セキュリティエージェントをこのエンドポイントにインストールします。

「一括送信」または「個別送信」からインストーラリンクを送付

エージェントインストール開始！

端末上でURLまたはQRコードからインストーラリンクへアクセス

「個別送信」にてから配布した場合は、認証コードを入力して[次へ]

Provide the Authentication Code included in your invitation email message, then tap **Continue**.

RMNCrsc

Continue

A screenshot of a 'Terms of Use' dialog box. The title 'Terms of Use' is at the top. Below it is the text: 'To take advantage of all the features, you must accept the [Terms of Use](#)'. At the bottom are two buttons: 'Decline' on the left and 'Accept' on the right. The 'Accept' button is highlighted with a red border.

この Web サイトは構成プロファイルをダウンロードしようとしています。許可しますか?

アプリ(Mobile Security)が
インストールされるので開く

「VPN」をオンにして インストール完了！

VPNを有効にすると、このプロパティはアクセスしているIDとメイド名を表示するドロップダウン式のWebレビューションです。プロトコル、セキュリティ、ファイリングの履歴など、Webベースのページを完全に表示するためのメイドなど、事前に設定した情報を表示するWebマイクロソフトなどとともに表示します。

プロファイルがダウンロードされました
プロファイルをインストールするには設定Appで再確認してください。

閉じる

- 通知
- サウンドと触覚
- 集中モード
- スクリーンタイム
- 一般
- コントロールセンター

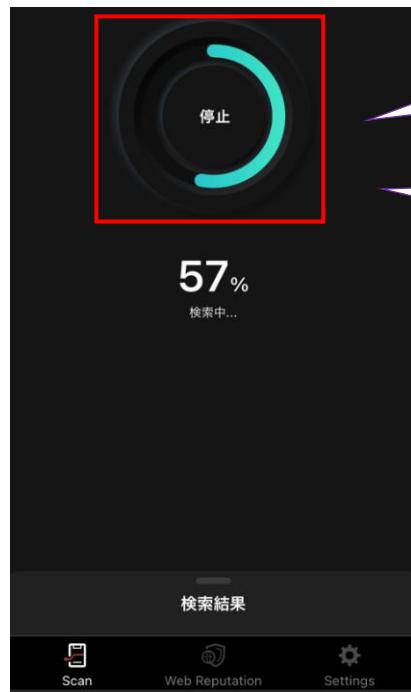
エージェントコンソールメニュー

エージェント(アプリ)のUI 概要

New!!



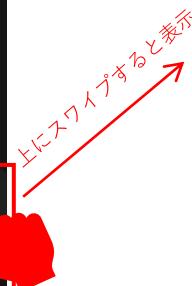
「検索」タブ



検索ボタンをタップすると
検索開始

検索結果により検索ボタンの
カラーが変わる

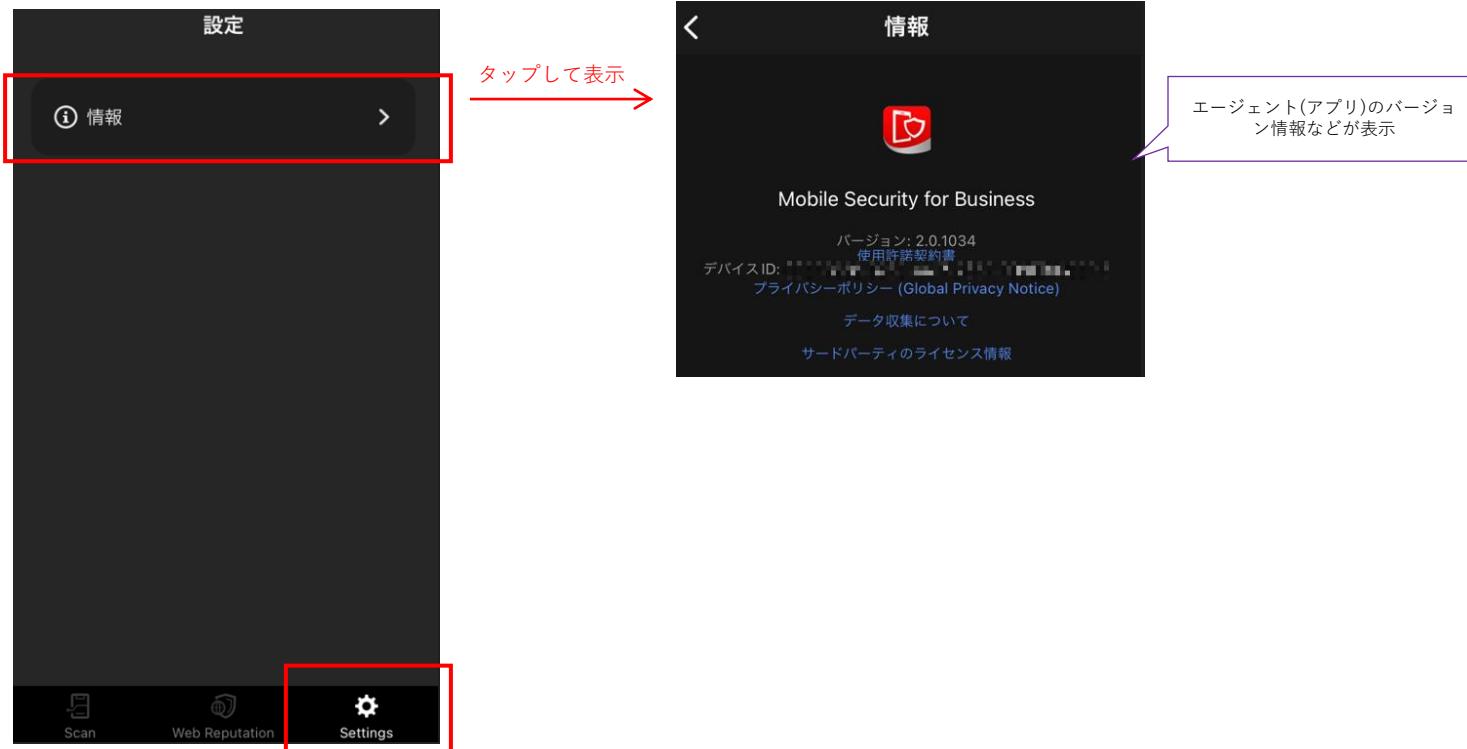
検索結果が表示



「Webレビューション」タブ



「設定」タブ



ご利用中のお客様へ

～旧エージェントのサポートについて

旧エージェントのサポートについて

- 本資料掲載の新機能は、旧iOSエージェントではご利用いただけません。
- 本資料の新機能をご利用される場合は、旧エージェントのアンインストール後、新エージェントのインストールを実施してください。
- ご利用中の旧iOSエージェントは、2025年4月にサポートを終了いたしました。旧エージェントをご利用の場合は早急に、新エージェントのインストールをお願いいたします。
- 新エージェントでは、本資料でご紹介した脅威対策機能がご利用いただけます。ぜひ、新エージェントをインストールしてセキュリティ対策の向上にご活用ください。

※参考) 旧エージェントのアンインストール手順

<https://success.trendmicro.com/dcx/s/solution/1116317?language=ja>