おまかせアンチウイルス
（EDRプラスオプション）
ダッシュボード解説書

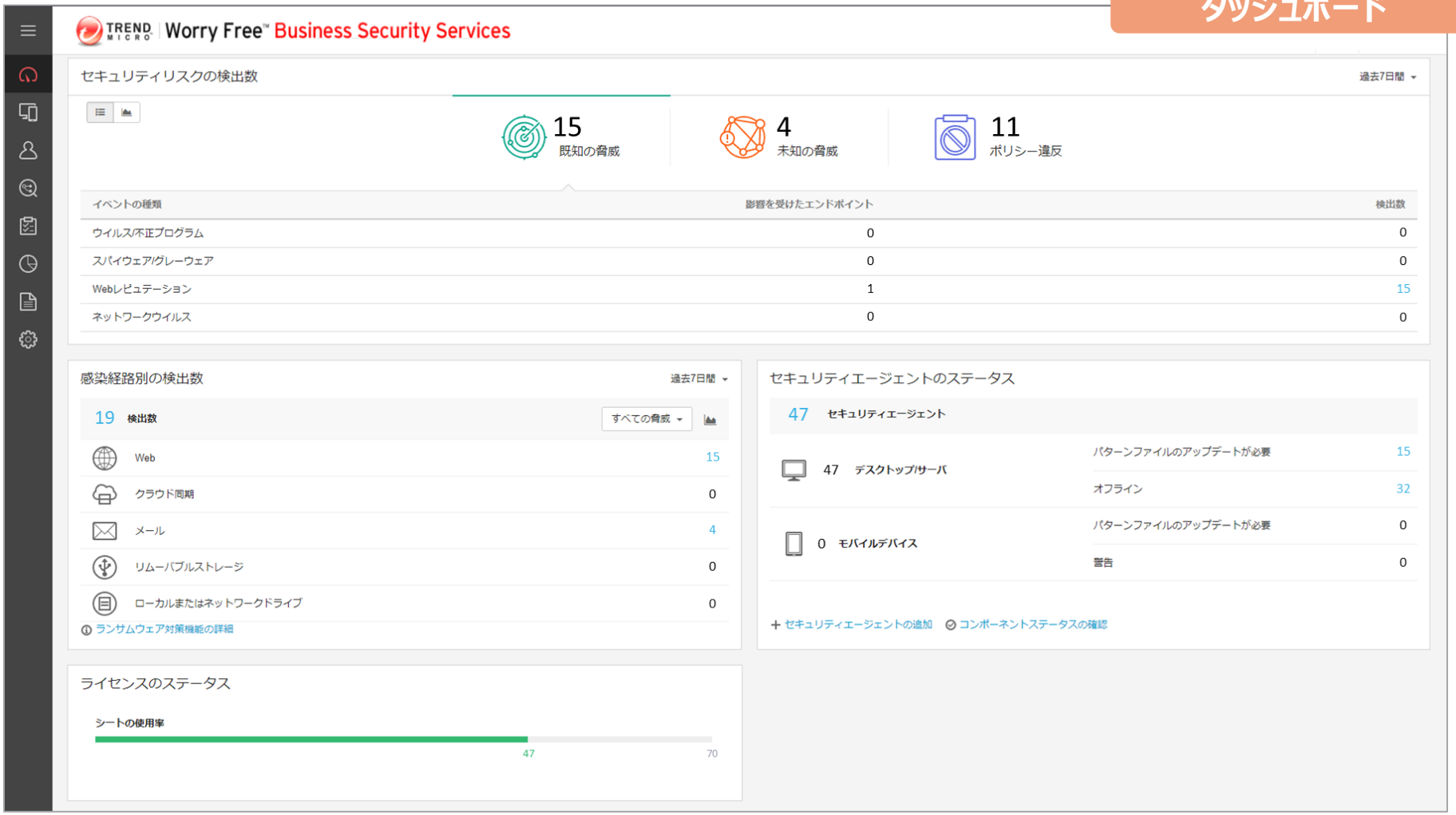
2024.09

東日本電信電話株式会社

1. おまかせアンチウイルスダッシュボードの概要

- おまかせアンチウイルスのダッシュボードにアクセスすることで、おまかせアンチウイルスをご契約・インストール頂いているパソコン等端末のセキュリティリスクをリアルタイムに確認することができます
- 本解説書では、ダッシュボードへのログイン方法やダッシュボードの見方など、活用の仕方を紹介します

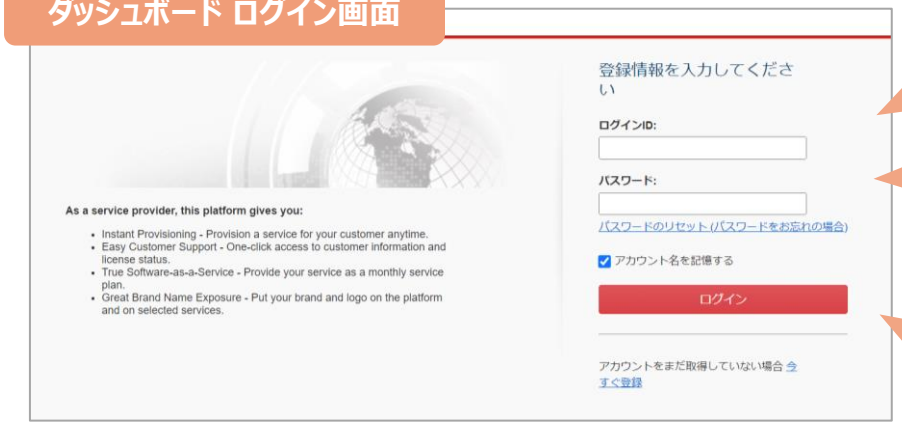
ダッシュボード



2. ダッシュボードへのログイン手順

- おまかせアンチウイルスのダッシュボードにアクセスするには、事前に通知しているログインIDによりログインする必要があります
- ログインID・パスワードが不明な場合は、弊社サポートデスクまでお問い合わせください

ダッシュボード ログイン画面



二要素認証画面

Step1：Webサイトへのアクセス

お使いのブラウザを開き、以下のURLにアクセスします

おまかせアンチウイルスログインページ

[https://n7od2.login.trendmicro.com]

Step2：ログインID・パスワードの入力

「ログインID」　：事前に通知しているログインIDを入力します

「パスワード」　：ご自身が設定したパスワードを入力します

Step3：ログインボタンのクリック

ログインIDとパスワードを入力後、「ログイン」ボタンをクリックします。

セキュリティを高めるために二要素認証を設定している場合、確認コードの入力を求められることがあります。

Google Authenticatorアプリから取得した確認コードを入力し、「送信」ボタンをクリックします。

※二要素認証の設定手順はおまかせアンチウイルス公式HPに掲載されているマニュアルを参照ください

おまかせアンチウイルス公式HP

[https://business.ntt-east.co.jp/support/antivirus/]

Step4：ログイン完了！

正しくログイン出来ると、ダッシュボードが表示されます

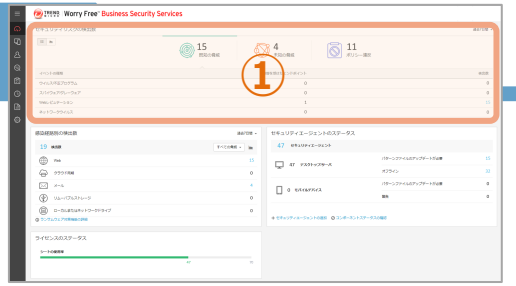
【ログインID・パスワードが不明の場合】

- 登録したログインIDが不明な場合は、サポートデスクまでお問い合わせください（問い合わせ先は、12ページをご参照下さい）
- パスワードを忘れた場合、ログイン画面から「パスワードのリセット」をクリックし、パスワード再設定の手続きを行います。登録済みメールアドレスに送信された指示に従い、新しいパスワードを設定してください。上記の手順で解決しない場合や、メールが届かない場合は、サポートデスクまでお問い合わせください

3-1. ダッシュボードの全体概要

- ダッシュボードにアクセスすることで、① セキュリティリスク、② 感染経路別のリスク、③ インストールしているアンチウイルスの状態、④ 契約ライセンス数を、リアルタイムに確認することができます（各項目については次ページから解説します）

3-2. セキュリティリスクの検出数（①）



- ここでは、「既知の脅威」「未知の脅威」「ポリシー違反」の3つに分類し、イベント毎の検出数を確認できます

既知の脅威

- 世の中で既に見つかっているウイルスや、悪質なソフトウェアの検知数を表示します
- 既知の脅威は、アンチウイルスソフトのデータベースに登録されているため、検知・駆除することができます

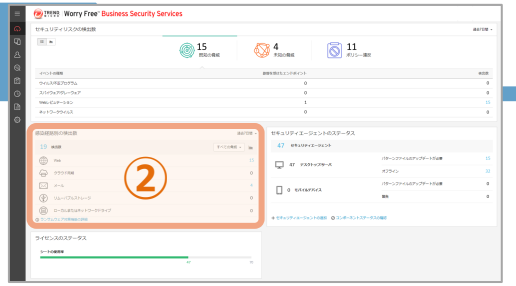
未知の脅威

- 新たに作成されたウイルスや、これまでにないタイプのソフトウェアの検出数を表示します
- 未知の脅威は、怪しい動きやAIでの判断、また安全な環境においてテストすることで見つけ出すことができます

ポリシー違反

- ソフトウェアを勝手にインストールする、重要な設定を変更するなど、ポリシー違反の検出数を表示します

3-3. 感染経路別の検出数（②）



- ここでは、感染経路ごとに脅威の検出数を確認できます

感染経路別の検出数　　過去7日間

10 検出数　　すべての脅威

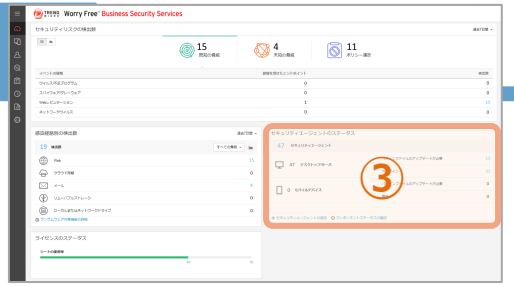
Web	5
クラウド同期	0
メール	3
リムーバブルストレージ	0
ローカルまたはネットワークドライブ	2

ランサムウェア対策機能の詳細

POINT

想定していない経路での感染が見つかっていないか、確認してください

3-4. アンチウイルスの状態確認（③）



- ここでは、本ウイルス対策ソフトのウイルス検知用ファイル（パターンファイル）が最新化されているかを確認することができます

オフライン：
ウイルス対策ソフトをインストールしたパソコン等の電源が入っていない、またはインターネットに接続されていないことを示しています

セキュリティエージェントのステータス

144 セキュリティエージェント

144 デスクトップ/サーバ

- パターンファイルのアップデートが必要 33
- オフライン 111

0 モバイルデバイス

- パターンファイルのアップデートが必要 0
- 警告 0

＋ セキュリティエージェントの追加　コンポーネントステータスの確認

POINT

新たな脅威を検知するため、パターンファイルが最新であることを確認してください

最新化手順：対象のパソコンを起動してインターネットに接続したのちに自動で最新化されます、
もしくは画面右下のタスクバー等からウイルス対策ソフトのアイコンを右クリックし、更新を押下してください

3-5. 契約ライセンス数の確認（④）

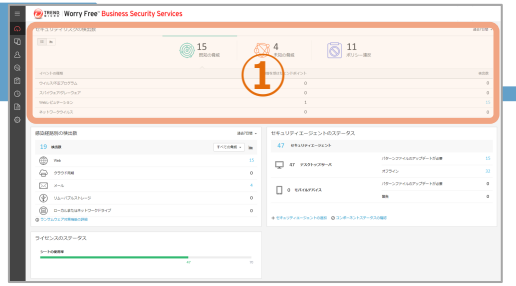
- ここでは、ライセンスの使用率を確認することができます

POINT

ライセンスの使用率（シートの使用率）が、100%に近付いていないか確認してください

ライセンス超過が見込まれる場合には、セキュリティサポートデスクまでお問い合わせください

（参考）セキュリティリスクの検出数：既知の脅威



- 既知の脅威では、「ウイルス/不正プログラム」「スパイウェア/グレーウェア」「Webレピュテーション」「ネットワークウイルス」の4つのイベントの検出数を表示します

ウイルス/不正プログラム

- ウイルスと不正プログラムにはさまざまな種類があります。例えば、トロイの木馬はシステムに侵入し不正な処理を行い、ウイルスは他のプログラムに感染して複製を繰り返し、さまざまな形態でシステムに影響を与えます

スパイウェア/グレーウェア

- スパイウェア/グレーウェアは、不正な処理を実行する可能性のあるソフトウェアです。ネットワーク上のエンドポイントのパフォーマンスに悪影響を与えたり、機密性に関する重大なリスクを与える可能性があります

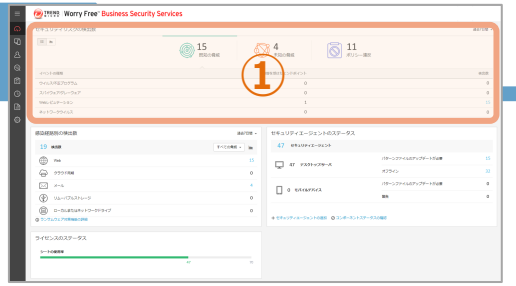
Webレピュテーション

- Webレピュテーションは、ウェブサイトの安全性を評価し、不正なサイトや危険なコンテンツへのアクセスをブロックする技術です。これにより、お客様をマルウェアやフィッシングサイトなどのリスクから守ります

ネットワークウイルス

- ネットワークウイルスは、ネットワークプロトコルを使って広がり、主にメモリに感染してネットワークの速度を低下させたり、ダウンさせたりします。システムファイルを変更することが少ないため見つけにくい特徴があります

（参考）セキュリティリスクの検出数：未知の脅威



- 既知の脅威では、「ウイルス/不正プログラム」「スパイウェア/グレーウェア」「Webレピュテーション」「ネットワークウイルス」の4つのイベントの検出数を表示します

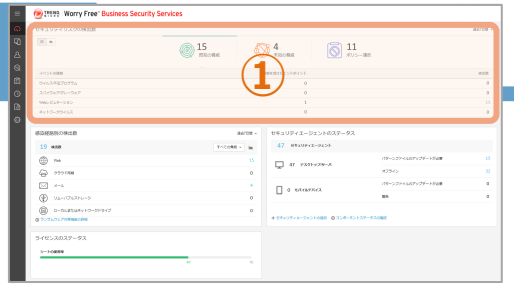
挙動監視

- 挙動監視では、プログラムの挙動を分析して、既知および未知の両方の脅威からの保護を予防的に実行します。また、システムイベントを監視して、不正な活動を示したプログラムをブロックします。この機能を使用すると、新たに出現した脅威に対する保護のレベルを向上できます

機械学習型検索

- 機械学習型検索は、高度な機械学習テクノロジを使用して脅威情報を関連付け、デジタルDNAフィンガープリントやAPIマッピングなどのファイル機能を使用した詳細なファイル分析により未知のセキュリティリスクを検出します
- また、不明なプロセスやあまり普及していないプロセスの挙動分析を実行し、ネットワークへの侵入を試みる未知の新しい脅威が無いかを判定します
- 機械学習型検索は、未知の脅威およびゼロデイ攻撃から環境を保護するのに役立つ強力な検索方法です

（参考）セキュリティリスクの検出数：ポリシー違反



- ポリシー違反では、「URLフィルタ」「デバイスコントロール」「情報漏えい対策」「アプリケーションコントロール」の4つのイベントの検出数を表示します。

URLフィルタ

- URLフィルタは、特定のWebサイトへのアクセスを制限し、業務中に社員がソーシャルメディアや動画サイトなどに費やす時間を減らすことか可能です。フィルタの設定は自由にカスタマイズでき、アクセスを許可するWebサイトやブロックするカテゴリを細かく調整できます

デバイスコントロール

- デバイスコントロールは、コンピュータに接続されている外部のストレージデバイスやネットワークリソースへのアクセスを規制します。これにより、データの損失や漏えいを防ぐことができます

情報漏えい対策

- 情報漏えい対策は、機密データを守るための機能です。従来の外部からの脅威対策だけでなく、内部からの漏えいも防ぐ必要があります。データの識別、転送制限、プライバシー基準の遵守などを行い、不正なアクセスや流出を防ぎます。これにより、組織はデータの安全性と信頼を維持します

アプリケーションコントロール

- アプリケーションコントロールは、エンドポイントで実行またはインストールできるアプリケーションを制限することが可能です

お問い合わせ先

＜Webからのお問い合わせ＞

こちらのお問い合わせフォームへ内容をご入力ください。
https://business.ntt-east.co.jp/support/antivirus/#anc-03

※お問い合せいただく際には、開通時にNTT東日本より送付される
メールに記載されているお客さまIDが必要となります

＜お電話でのお問い合わせ＞

サービスご契約時に郵送している開通のご案内に同封している
重要事項説明書“「おまかせアンチウイルス」をご契約のお客さまへ"をご確認ください