おまかせアンチウイルス
（EDRプラスオプション）
月次レポート解説書

2023.11

東日本電信電話株式会社

月次レポート（おまかせアンチウイルス）の内容

- おまかせアンチウイルスが検知・ブロックした脅威に関する情報を**月１回、申込み時にいただいたメールアドレス宛**に送付します
- レポートには、下記の内容が記されています

・概要

脅威の検出状況に関する情報

1. 製品/サービス情報
2. インストールされているエージェントの概要
3. 検出の概要

・ウイルス/不正プログラム

ウイルス等の検出状況及び処理結果に関する情報

1. 検出総数
2. 検出数が上位のエンドポイント
3. 検出数が上位のサーバ
4. 検出の傾向
5. 処理の結果
6. 検出された上位のウイルス/不正プログラム

・スパイウェア/グレーウェア

ウイルス等の検出状況及び処理結果に関する情報

1. 検出総数
2. 検出数が上位のエンドポイント
3. 検出数が上位のサーバ
4. 検出の傾向
5. 処理の結果
6. 検出された上位のスパイウェア/グレーウェア

・Webレピュテーション

不正サイトへのアクセスに関する情報

1. 検出総数
2. 検出数が上位のエンドポイント
3. 検出の傾向

・挙動監視

不正な挙動を示すプログラムの検出状況に関する情報

1. 検出総数
2. 違反のあったエンドポイントの上位
3. 検出の傾向
4. 違反のあったアプリケーションの上位

・URLフィルタ

URLアクセス制御の検出状況に関する情報

1. 検出総数
2. 検出数が上位のエンドポイント
3. 検出の傾向
4. 検出された上位のURLカテゴリ

・ネットワークウイルス

ネットワーク経由のウイルス感染に関する情報

1. 検出総数
2. 検出数が上位のエンドポイント
3. 検出の傾向
4. 検出された上位のネットワークウイルス

※本資料の記載例は一例ですので、実際の記載内容とは異なります

1.概要

- 導入されている製品名を確認することができます
- おまかせアンチウイルスが実際にインストールされている台数が、デスクトップ(パソコン)・モバイルデバイス毎に表示され、管理者が把握することができます
- お客様がご契約している**ライセンスの数量および使用率**を確認をすることができます
- １ヶ月間の脅威の検出数および前月比を確認することができます

2-1.ウイルス/不正プログラム

- ウイルス/不正プログラム機能で検出した件数を確認することができます
- 脅威の検出数が多いデバイス名・サーバ名を確認することができます

1. ウイルスバスター ビジネスセキュリティサービス

ウイルス/不正プログラム

検出総数

検出数	13,986	+17.2%
影響を受けたエンドポイント	3	

前の期間との比較: 2019/05/13 - 2019/05/20

検出数が上位のエンドポイント

エンドポイント	検出数	%
Test001	6,992	50.0%
Test002	6,992	50.0%
Test003	2	0.0%

検出数が上位のサーバ

サーバ	検出数	%
Unauthorized File Encryption	5,244	37.5%
Sasser	2	0.0%
wannacry	144	21.8%
Iloveyou	144	21.8%
melisa	144	21.8%

POINT

特定のパソコン(Test001/Test002)で多量のウイルス/不正プログラムを検出している。

■セキュリティデータベース

「**トレンドマイクロ社 セキュリティデータベース**」より、不正プログラム/スパイウェア名を検索すると、**感染経路や対処法等の情報を確認**することができます。

ここに検索したい不正プログラム/スパイウェア名を入力

http://about-threats.trendmicro.com/ThreatEncyclopedia.aspx?language=jp

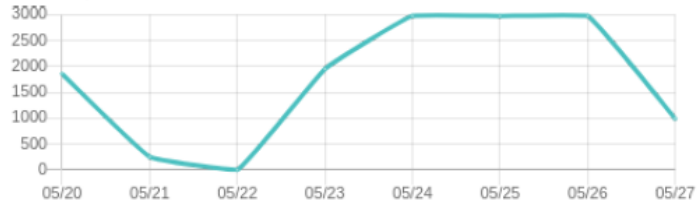
ウイルスが検知されたデバイスのうち、検出数が多い上位5台のデバイス名を表示します

ウイルスが検知されたサーバのうち、検出数が多い上位5台のサーバ名を表示します

2-2.ウイルス/不正プログラム

- 検出したウイルス/不正プログラムについてどのような対処が行われたかを確認することができます
- 多数検出されたウイルス/不正プログラム名を確認することができます

検出の傾向



処理の結果

駆除	6,118	43.7%
削除	874	6.2%
放置	0	0.0%
隔離	1,750	12.5%
拡張子変更	874	6.2%
要確認	4,370	31.2%

検出された上位のウイルス/不正プログラム

名前	検出数	%
Unauthorized File Encryption	5,244	37.5%
Sasser	2	0.0%
wannacry	144	21.8%
Iloveyou	144	21.8%
melisa	144	21.8%

POINT

休日と比較して平日(5/23-5/27)の方が検出数が多くなる傾向にある

日ごとの検出数の推移(傾向)を視覚的に確認することができます

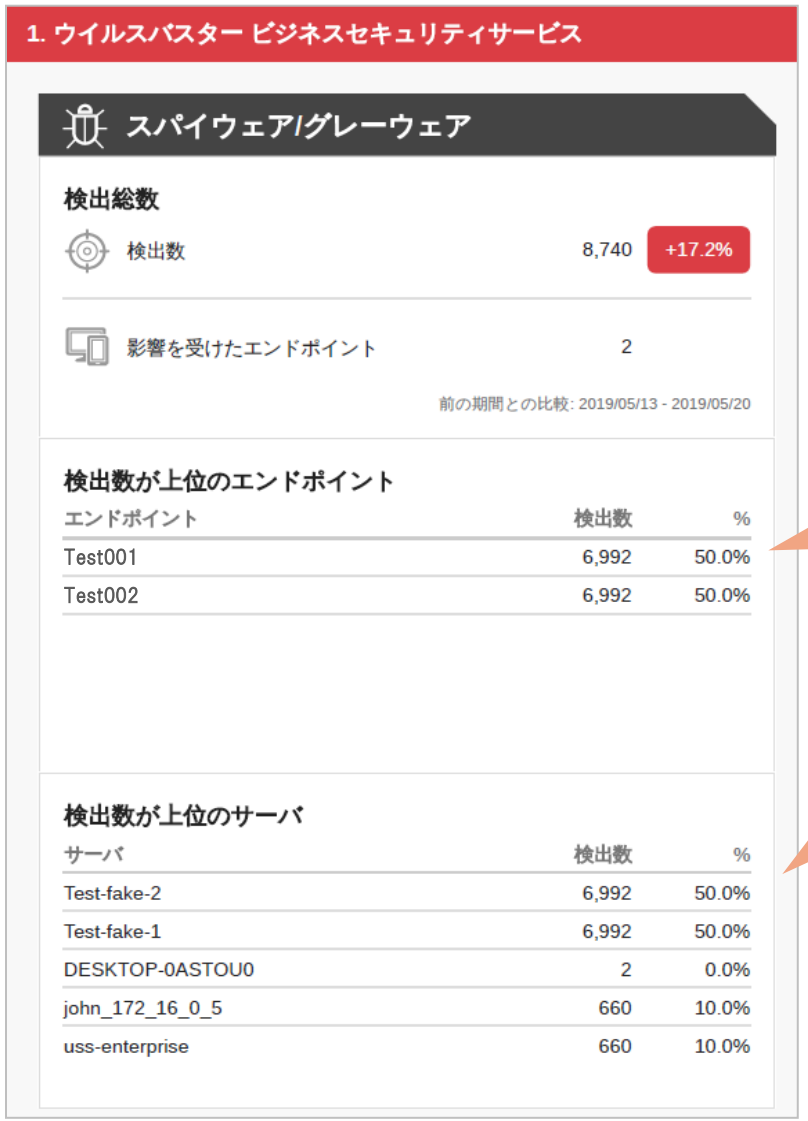
(処理項目について)

駆除　　：感染ファイルが通常のファイルに復元され、脅威をもたらすことはなくなりました
削除　　：「駆除」の処理ができないようなファイルをファイルごと消去しました
放置　　：ウイルスの可能性があるが、ウイルスと断定できない場合となります
隔離　　：ファイルは特定のフォルダに隔離され、問題の発生が阻止されました
拡張子変更：検出されたファイルの拡張子を「.vir」に変更し、ファイルを実行したり開いたりできないようにしています
要確認　　：ウイルスが検知された際の処理が失敗した場合となります
セキュリティサポートデスクからご連絡します

検出されたウイルスのうち、検出数が多い上位5種類のウイルス名を表示します

3-1.スパイウェア/グレーウェア

- スパイウェア※1/グレーウェア※2機能で検出した件数を確認することができます
- 脅威の検出数が多いデバイス名・サーバ名を確認することができます



POINT

特定のパソコン(Test001/Test002)で多量のスパイウェア/グレーウェアを検出している。

スパイウェアやグレーウェアが検知されたデバイス（パソコン・スマートフォン・タブレット）のうち、検出数が多い上位5台のデバイス名を表示します

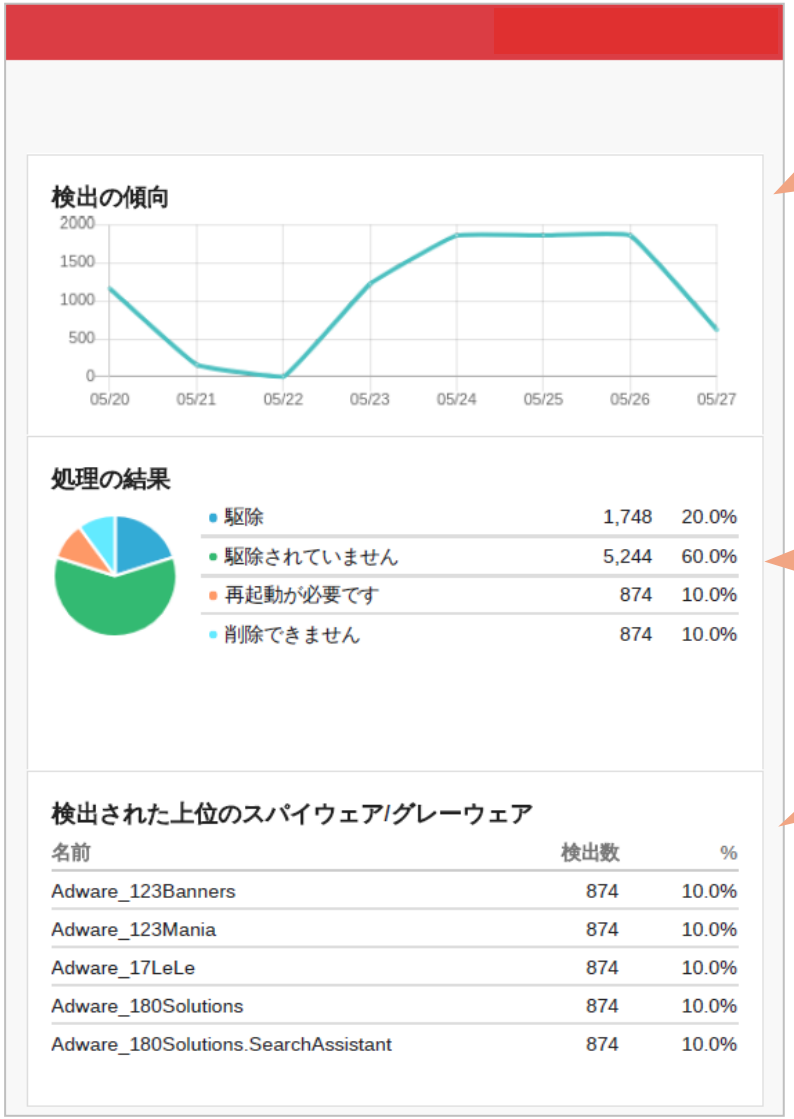
スパイウェアやグレーウェアが検知されたサーバの中で検出数が多い上位5台のサーバ名を表示します

※1 スパイウェア
アカウントユーザ名やパスワードなどのデータを収集し、第三者に不正に送信するソフトウェアです

※2 グレーウェア
マルウェアやスパイウェアに類するが、破壊活動やセキュリティ上危険な活動を特に行うものではないため、不正プログラムと見なすことが難しいソフトウェアです

3-2.スパイウェア/グレーウェア

- 検出したスパイウェア/グレーウェアについてどのような対処が行われたかを確認することができます
- 多数検出されたスパイウェア/グレーウェア名を確認することができます



日ごとの検出数の推移(傾向)を視覚的に確認することができます

(処理項目について)
駆除　：感染ファイルが通常のファイルに復元され、脅威をもたらすことはなくなりました
駆除されていません　：スパイウェアの駆除が出来なかった場合となり確認が
必要となるためセキュリティサポートデスクからご連絡します
再起動する：スパイウェア/グレーウェアの処理を完了するためにシステムの再起動が必要です
安全ではない：スパイウェア関連のプロセスを停止できず、駆除が完全でない場合です

検出されたスパイウェアやグレーウェアのうち、
検出数が多い上位5種類のスパイウェアやグレーウェア名を表示します

4.Webレピュテーション

□ 管理者は、フィッシング詐欺※1などの兆候を示すWebページにアクセスしようとしたデバイスを確認することができます

Webレピュテーション※2機能で制限されているWebサイトにアクセスしたデバイスのうち、アクセス頻度が多い上位10台のデバイス名を表示します

※1 フィッシング詐欺
金融機関などを装ったメールを送るなどして偽のWebサイトへ誘導しログイン情報やクレジットカード情報などをだまし取ろうとする詐欺です

※2 Webレピュテーション
お使いのコンピュータを安全でないWebサイトから保護する機能です

5.挙動監視

□ プログラムやOS、レジストリエントリ、フォルダなどが不正に変更されたコンピュータを監視し、意図せず編集されようとした対象のコンピュータ・アプリケーション（プログラム）を確認することができます

1. ウイルスバスター ビジネスセキュリティサービス

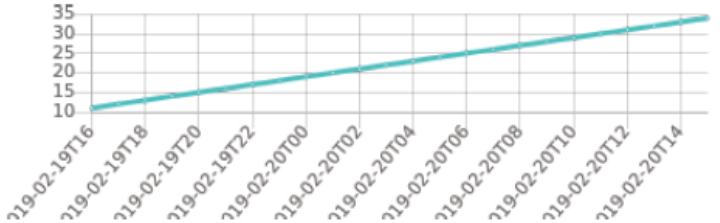
挙動監視

検出総数

検出数	540	+22%
影響を受けた...	1	+23%

前の期間との比較: 2019/03/02 - 2019/03/03

検出の傾向



違反のあったエンドポイントの上位

エンドポイント	検出数	%
john_172_16_0_1	540	103.0%

違反のあったアプリケーションの上位

名前	検出数	%
subject_1	207	38.3%
subject_2	169	31.3%
subject_3	164	30.4%
subject_4	164	30.4%
subject_5	164	30.4%
subject_6	164	30.4%
subject_7	164	30.4%
subject_8		
subject_9		
subject_10		

挙動監視※1違反が検出されたデバイスのうち、
検出数が多い上位5台のデバイス名を表示します

検出された挙動監視※1違反のうち、
検出数が多い上位10種類のプログラム名を表示します

※1 挙動監視
OS、レジストリエントリ、他のソフトウェア、ファイル、またはフォルダが不正に変更されないよう、コンピュータを監視し、保護する為の機能です

6.URLフィルタ

- URLフィルタで閲覧制限をかけているURLに、アクセスした回数の多いデバイスを確認することができます
- URLフィルタで閲覧制限をかけているURLについて、どのカテゴリにアクセスされていることが多いか確認することができます

1. ウイルスバスター ビジネスセキュリティサービス

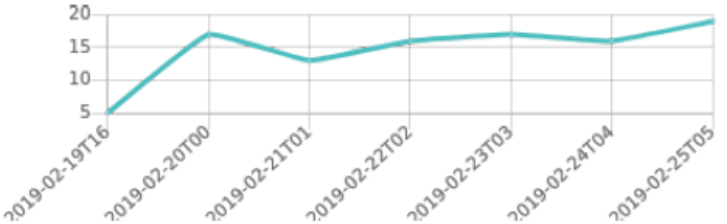
URLフィルタ

検出総数

違反数	381	+15.3%
影響を受けた...	1	+16.8%

前の期間との比較: 2019/03/02 - 2019/03/03

検出の傾向



検出数が上位のエンドポイント

エンドポイント	検出数	%
john_172_16_0_1	381	10.0%
john_172_16_0_2	381	10.0%
john_172_16_0_3	381	10.0%
	381	10.0%
	381	10.0%
	381	10.0%
	381	10.0%
john_172_16_0_8	381	10.0%
john_172_16_0_9	381	10.0%
john_172_16_0_10	381	10.0%

URLフィルタを設定している場合、
フィルタにかかった回数が多い
上位10台のデバイス名を表示します

検出された上位のURLカテゴリ

カテゴリ	検出数	%
フィッシング	39	10.2%
Ransomware	37	9.7%
スパムメール	35	9.2%
不正プログラム関連	35	9.2%
MFA (Made for AdSense) サイト	35	9.2%
スパイウェア	34	8.9%
不正プログラム配信	34	8.9%
不正と思われるプログラム (グレ...	30	7.9%

URLフィルタを設定している場合、フィルタにかかった回数を
サイトのカテゴリごとにランキングで表示します（上位10件）

7.ネットワークウイルス

- 検出された数の多いネットワークウイルス※1の上位10件を確認することができます
- ネットワークウイルスによって攻撃されたデバイス上位10件を確認することができます

1. ウイルスバスター ビジネスセキュリティサービス

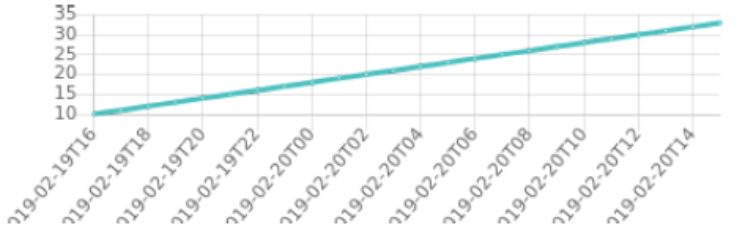
ネットワークウイルス

検出総数

検出数	516	+21%
影響を受けた...	14	+22%

前の期間との比較: 2019/03/02 - 2019/03/03

検出の傾向



検出数が上位のエンドポイント

エンドポイント	検出数	%
john_172_16_0_1	516	100.0%

検出された上位のネットワークウイルス

脅威名	検出数	%
123Banners	48	9.3%
123Mania	48	9.3%
17LeLe	48	9.3%
180Solutions	48	9.3%
180Solutions.SearchAssistant	48	9.3%
180Solutions.Seekmo	48	9.3%
180Solutions.Zango	48	9.3%
2020Sear		
2Call		
2ndThoug		

ネットワーク経由でのウイルス感染が検知されたデバイスのうち、検出数が多い上位10台のデバイス名を表示します

ネットワーク経由で検知されたネットワークウイルスのうち、検出数が多い上位10種類のネットワークウイルス名を表示します

※1 ネットワークウイルス

ネットワークウイルスとは Windows の脆弱性などをつき、ネットワーク経由での感染を行うネットワーク通信をさします

おまかせアンチウイルスでは、ファイアウォール機能にて、該当端末への通信を監視しており、ネットワーク通信の時点でネットワークウイルスを検出します

月次レポート（EDRプラスオプション）の内容

- EDRプラスオプションが検知した脅威に関する情報を**月１回、申込み時にいただいたメールアドレス宛**に送付します
- レポートには、下記の内容が記されています

・不審アクティビティの検出　**不審なアクティビティの検出状況**

1-1. 注意が必要なイベントの検出傾向
1-2. 注意が必要なオブジェクトのトップ５
1-3. リスクがあるエンドポイントのトップ５
1-4. 注意が必要なイベントのステータス
1-5. 注意が必要なオブジェクト

・保護の概要　**エージェントの状況**

2-1. オフラインエージェント
2-2. 保護機能が最新でないエージェント
2-3. サポートされていないオペレーティングシステムを
実行しているエンドポイント

・エンドポイント保護　**保護ポリシーの設定状況**

3-1. リアルタイム検索
3-2. 挙動監視
3-3. 機械学習型検索
3-4. Webレピュテーション
3-5. Endpoint Detection and Response

※本資料の記載例は一例ですので、実際の記載内容とは異なります

1-1. 注意が必要なイベントの検出傾向

- 注意が必要なイベントで検出した件数を確認することができます

※ 注意が必要なイベント
　端末で検出された不審なイベントを指し、不正なファイル操作や不正プログラムの実行などの不正な挙動の一連の流れを検出します。

1-2. 注意が必要なオブジェクトのトップ5

- 注意が必要なイベントで検出したオブジェクトの中で、検出数の多い上位5件を確認することができます

1-3. リスクがあるエンドポイントのトップ5

- 注意が必要なイベントで検出した端末の中で、検出数の多い上位5件を確認することができます

1-4. 注意が必要なイベントのステータス

- 注意が必要なイベントのレポート時点でのステータスを確認することができます

1-5. 注意が必要なオブジェクト

- 注意が必要なオブジェクトに対する処理結果を確認することができます

2-1. オフラインエージェント

- ご利用中の端末の中で長期間（14日以上）オフラインの状態の端末を確認することができます

2-2. 保護機能が最新ではないエージェント

- ご利用中の端末の中で最新のパターンファイルが適用されていない端末数を確認でき、アップデートが必要な端末の有無をご確認いただけます

2-3. サポートされていないオペレーティングシステムを実行しているエンドポイント

- サポート外のOSを利用している端末数を表示でき、サポート対象外OSを把握いただけます

3-1. リアルタイム検索

□ 検出機能「リアルタイム検索」が有効になっていない端末を確認することができ、ご利用いただいている端末のセキュリティ状況を見直すことができます

※ リアルタイム検索
ファイル操作やダウンロードなど実行されたタイミングで該当ファイルが脅威ファイルか判定します

3-2. 挙動監視

□ 検出機能「挙動監視」が有効になっていない端末を確認することができ、ご利用いただいている端末のセキュリティ状況を見直すことができます

※ 挙動監視
OS、レジストリエントリ、他のソフトウェア、ファイル、またはフォルダが不正に変更されないよう、コンピュータを監視し、保護する為の機能です

3-3. 機械学習型検索

□ 検出機能「機械学習型検索」が有効になっていない端末を確認することができ、ご利用いただいている端末のセキュリティ状況を見直すことができます

※ 機械学習型検索
人工知能を活用し、ファイルが不正プログラムと似た特性を持っているか判定し、悪性と判定した場合には自動隔離します

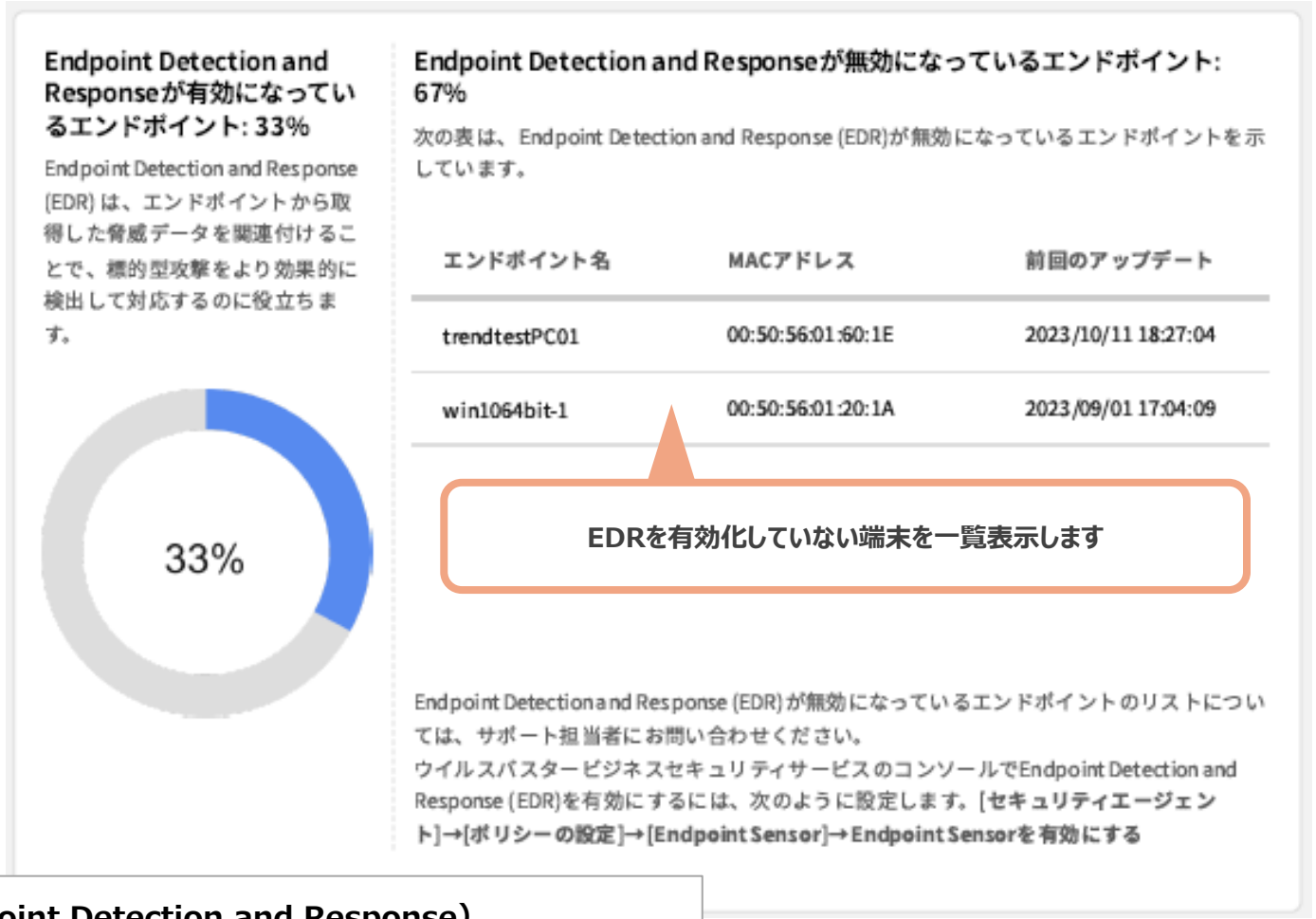
3-4. Webレピュテーション

□ 検出機能「Webレピュテーション」が有効になっていない端末を確認することができ、ご利用いただいている端末のセキュリティ状況を見直すことができます

※ Webレピュテーション
お使いのコンピュータを安全でないWebサイトから保護する機能です

3-5. Endpoint Detection and Response

- 検出機能「Endpoint Detection and Response」が有効になっていない端末を確認することができ、ご利用いただいている端末のセキュリティ状況を見直すことができます



※ EDR（Endpoint Detection and Response）
　端末で検出されたの不正な挙動の一連の流れ（不正なファイル操作や不正プログラムの実行など）を検出し、注意が必要なイベントとして通知します