NTT西日本

事業利用向け

セキュリティおまかせプラン

レポート解説

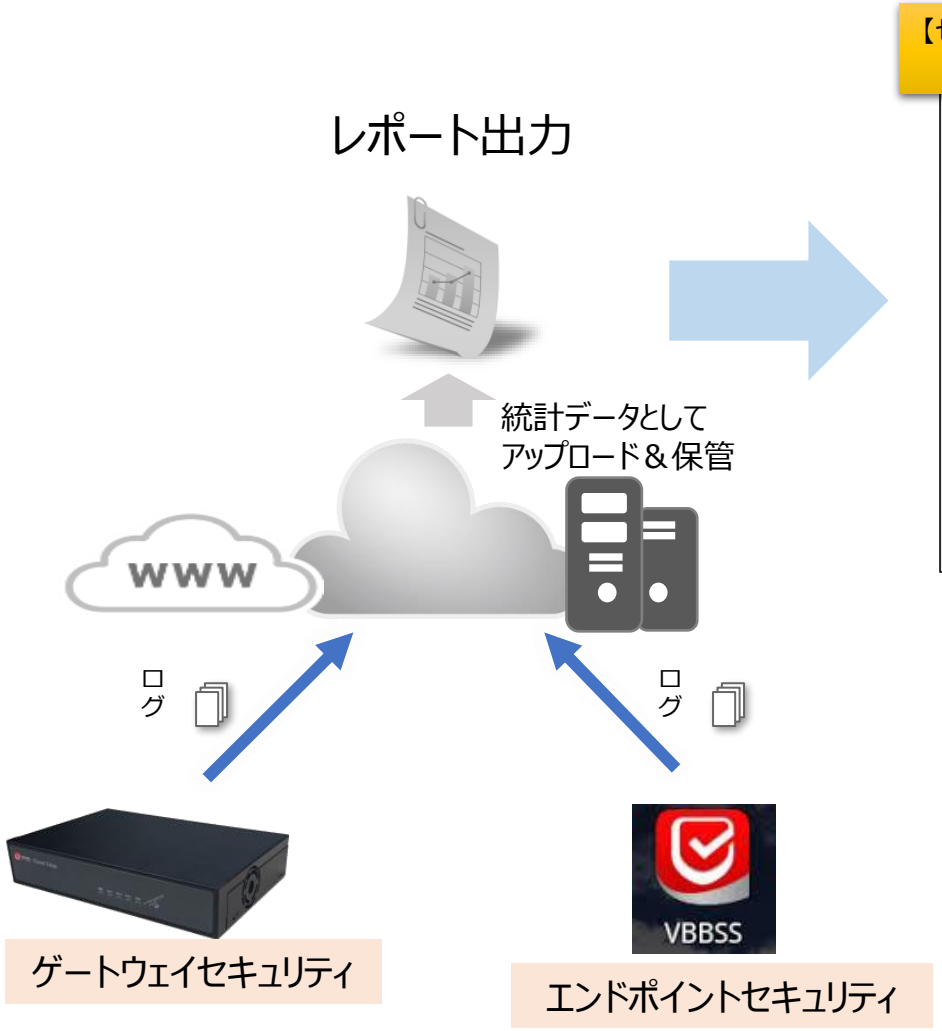
サマリーレポート ゲートウェイ編

NTT西日本株式会社

審査　26-S1068

セキュリティおまかせプランのレポートとは

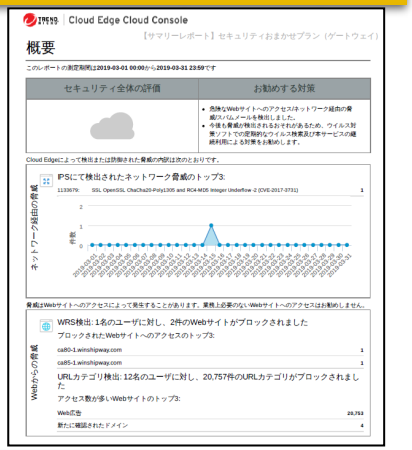
- ゲートウェイセキュリティおよびエンドポイントセキュリティご利用のお客さま向けに、毎月1度検出されたウイルスや不正コード等に関するレポートを登録されたメールアドレス宛に配信いたします。
- セキュリティの状況把握だけでなく、設定やポリシーの最適化検討を図る材料としても活用いただけます。



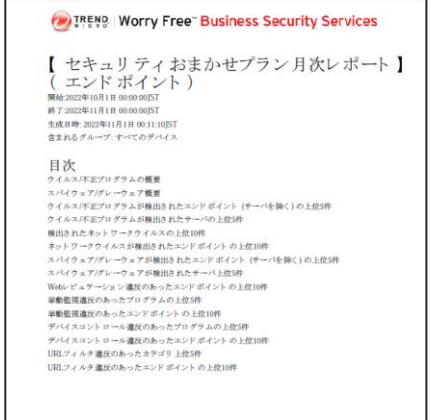
【セキュリティおまかせプラン月次レポート】ゲートウェイ



【サマリーレポート】セキュリティおまかせプラン(ゲートウェイ)

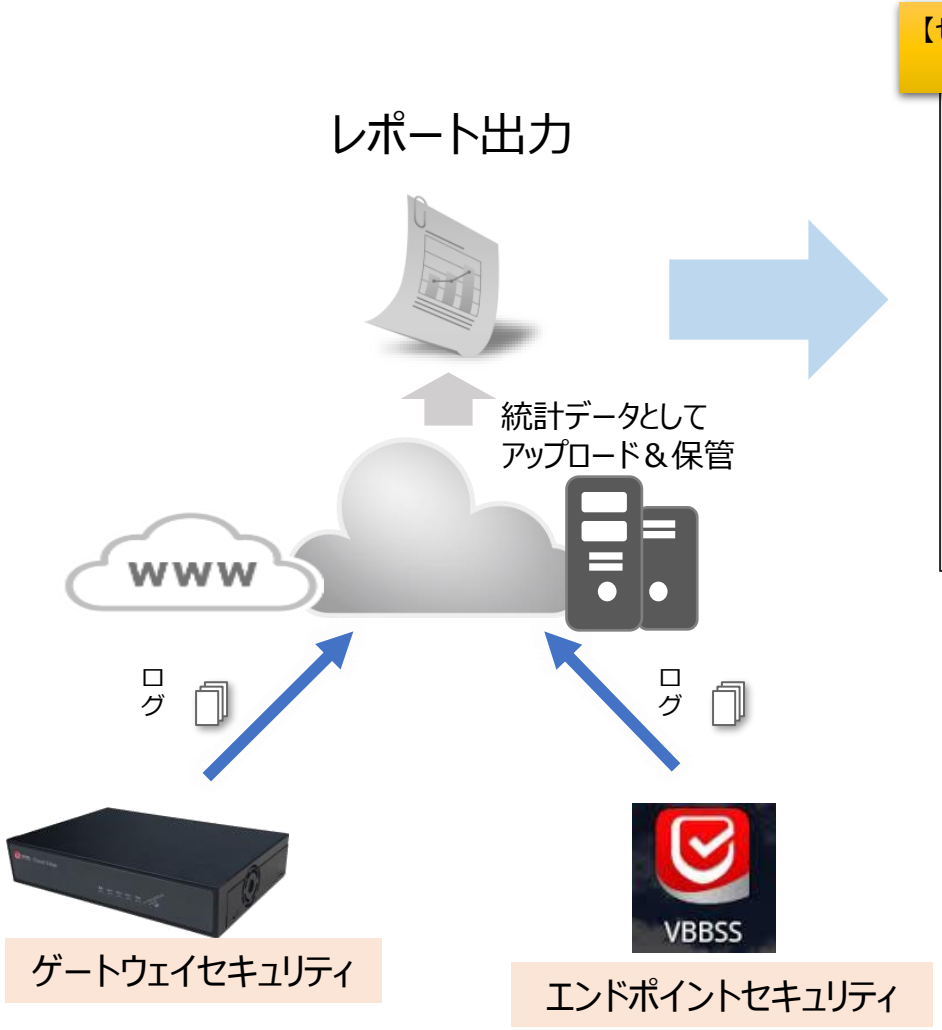


【セキュリティおまかせプラン月次レポート】（エンドポイント）



セキュリティおまかせプランのレポートとは

- ゲートウェイセキュリティおよびエンドポイントセキュリティご利用のお客さま向けに、毎月1度検出されたウイルスや不正コード等に関するレポートを登録されたメールアドレス宛に配信いたします。
- セキュリティの状況把握だけでなく、設定やポリシーの最適化検討を図る材料としても活用いただけます。

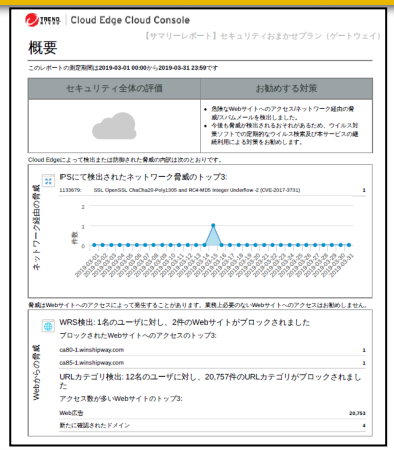


【セキュリティおまかせプラン月次レポート】ゲートウェイ


【セキュリティおまかせプラン月次レポート】
ゲートウェイ

生成者: kensho00
生成日: 2022-11-01 05:32
レポート期間: 過去1か月間 (2022-10-01 00:00 - 2022-10-31 23:59)

【サマリーレポート】セキュリティおまかせプラン(ゲートウェイ)


Cloud Edge Cloud Console
概要

【セキュリティおまかせプラン月次レポート】（エンドポイント）


Worry Free™ Business Security Services

【 セキュリティおまかせプラン月次レポート 】
（ エンドポイント ）

サマリーレポートとは

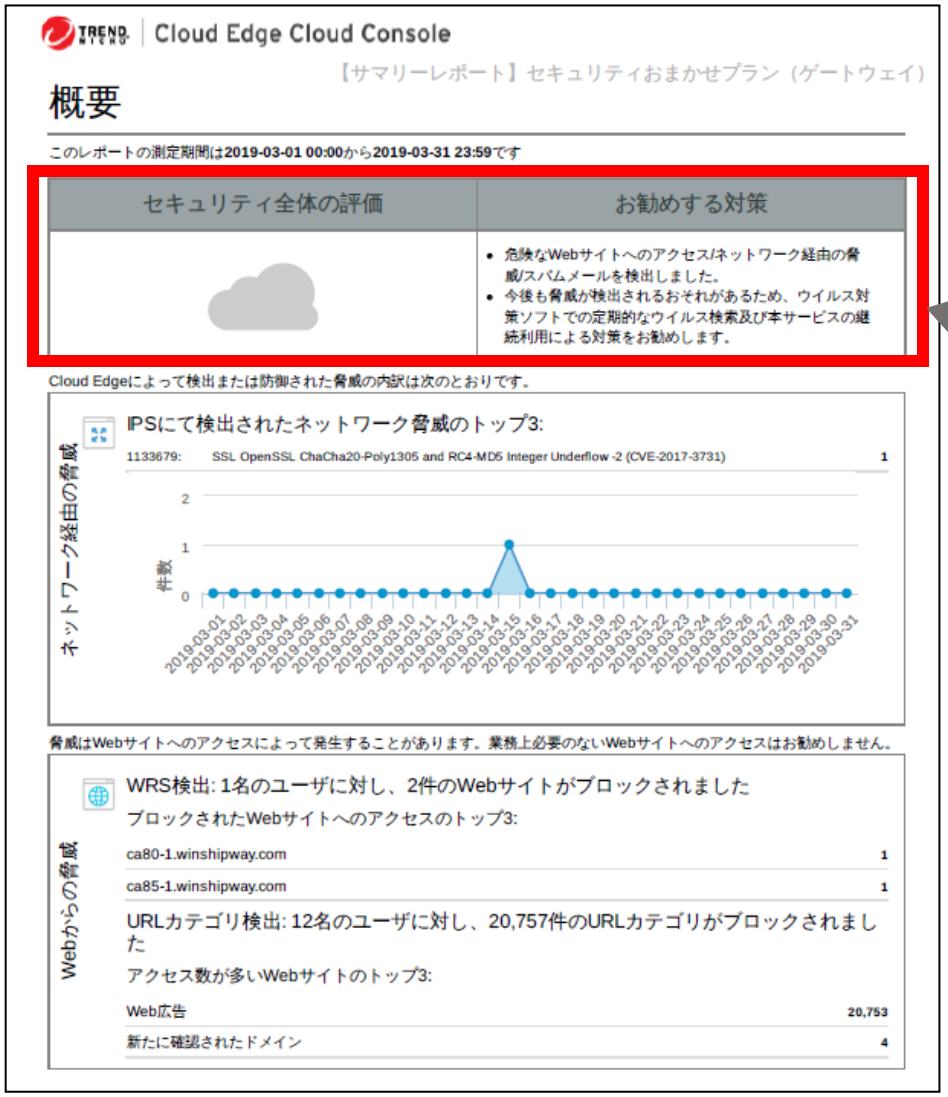
- サマリーレポートとは、月1回(月初)メールでお送りしている月次レポートの内容を要約し、よりお客様の脅威の検知状況をわかりやすくお伝えするものです。
- サマリーレポートは月次レポートとは異なるメールにて送付いたします。
- サマリーレポートは以下の表に記載する5項目から構成されています。

※**Cloud Edge**はトレンドマイクロ株式会社の登録商標です。

タイトル	内容
セキュリティ全体の評価・お勧めする対策	お天気マークでお客様のセキュリティ対策状況の評価を表し、お客様のセキュリティリスクの検出状況に応じたお勧めの対策をお知らせします。
ネットワーク経由の脅威	IPS(不正侵入防御システム)機能によって検知されたネットワーク脅威に関する情報を把握することができます。
Webからの脅威	WRS(危険Webサイトのアクセスブロック)機能によって検知・ブロックした不正サイトへの接続要求数や、アクセスが多い URL カテゴリの情報を把握することができます。
スパムメール対策の状況	スパムメール対策機能によって検知・メール件名へのタグ付けを行ったメール件数を時系列で把握することができます。
使用状況	Cloud Edge下部の端末の通信状況(送受信データ量や最もアクセスされているWebサイト名等)を把握することができます。

サマリーレポート詳細

- 本ページでは、「セキュリティ全体の評価・お勧めする対策」、「ネットワーク経由の脅威」、「Webからの脅威」に関する情報を把握することができます。

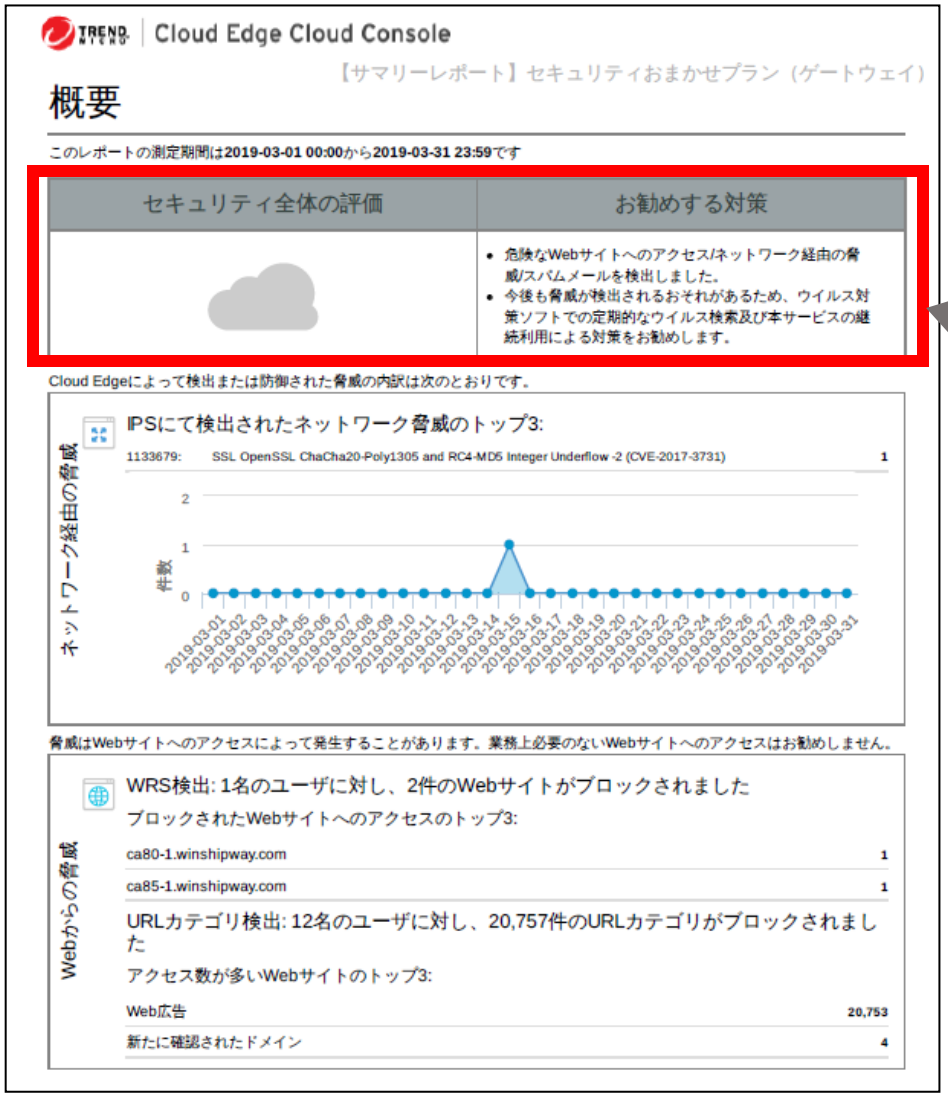




・「セキュリティ全体の評価」には、晴れマーク・曇りマーク・雨マークの3段階があり、曇りマークや雨マークのお客様は、期間中に何らかのセキュリティリスクを検出した形跡があります。

サマリーレポート詳細

□ 本ページでは、「セキュリティ全体の評価・お勧めする対策」、「ネットワーク経由の脅威」、「Webからの脅威」に関する情報を把握することができます。



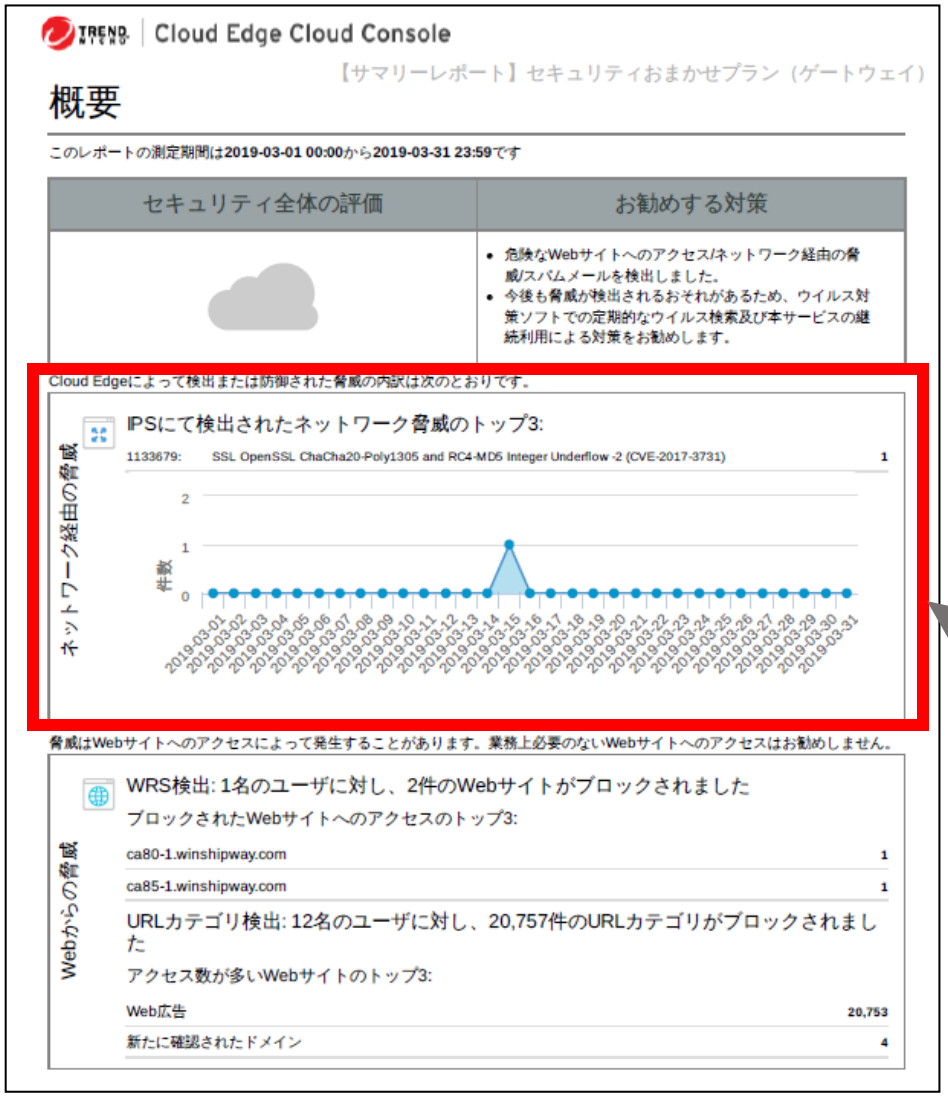


・晴れマークのお客様も、当該期間中は脅威の検出はありませんでしたが、油断すると次回は曇りマークや雨マークに変化する可能性があるため、セキュリティ対策を継続する必要があります。

・また「お勧めする対策」をご覧いただき、必要な対策を実施ください。

サマリーレポート詳細

□ 本ページでは、「セキュリティ全体の評価・お勧めする対策」、「ネットワーク経由の脅威」、「Webからの脅威」に関する情報を把握することができます。





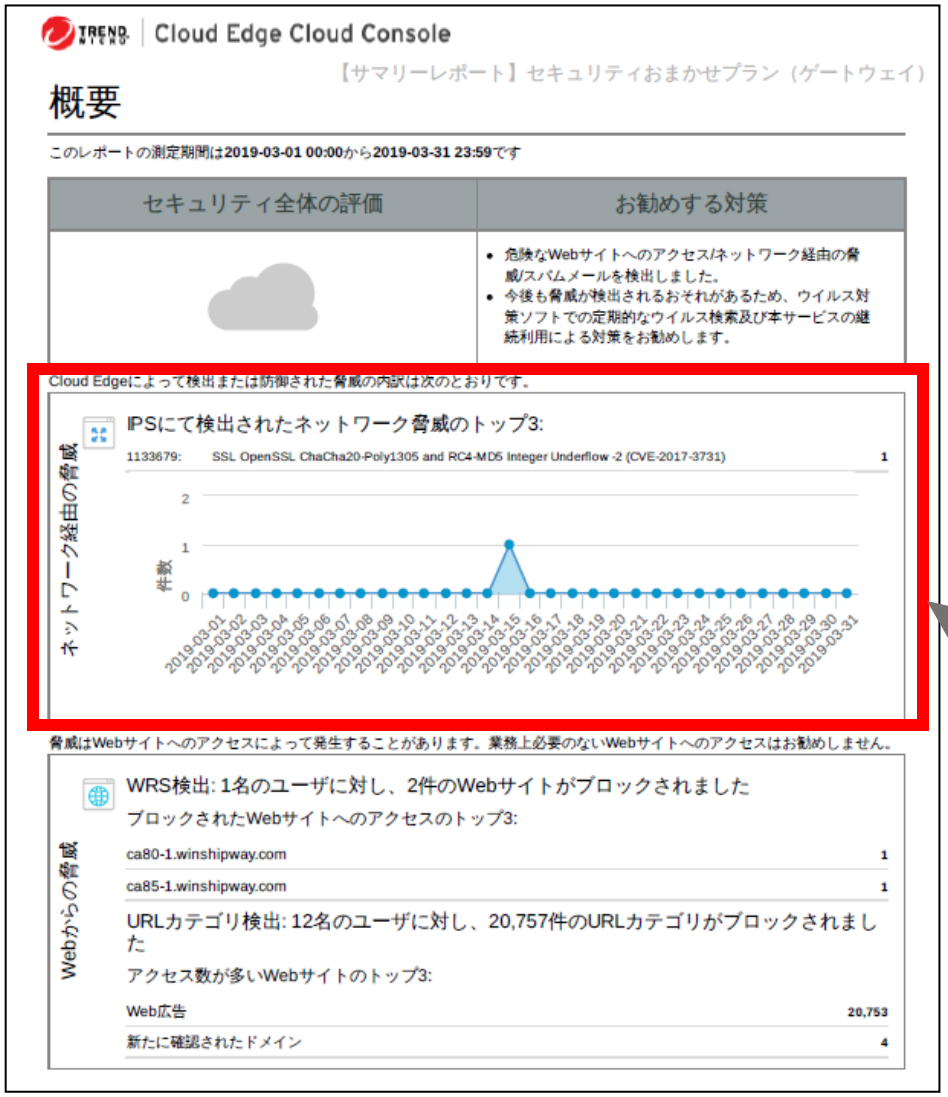
・IPSとは「不正侵入防御システム」の略称で、利用中のシステムの脆弱性を狙った攻撃等ネットワークを介した攻撃をブロックする機能です。

・上段では、検知件数が TOP3 に多い IPSルール名が確認できます。

・下段のグラフでは、IPS機能における時系列の検出件数を把握することができます。

サマリーレポート詳細

- 本ページでは、「セキュリティ全体の評価・お勧めする対策」、「ネットワーク経由の脅威」、「Webからの脅威」に関する情報を把握することができます。



TREND MICRO | Cloud Edge Cloud Console

【サマリーレポート】セキュリティおまかせプラン（ゲートウェイ）

概要

このレポートの測定期間は2019-03-01 00:00から2019-03-31 23:59です

セキュリティ全体の評価	お勧めする対策
	• 危険なWebサイトへのアクセス/ネットワーク経由の脅威/スパムメールを検出しました。 • 今後も脅威が検出されるおそれがあるため、ウイルス対策ソフトでの定期的なウイルス検索及び本サービスの継続利用による対策をお勧めします。

Cloud Edgeによって検出または防御された脅威の内訳は次のとおりです。

ネットワーク経由の脅威

IPSにて検出されたネットワーク脅威のトップ3:

1133679: SSL OpenSSL ChaCha20-Poly1305 and RC4-MD5 Integer Underflow -2 (CVE-2017-3731) 1

脅威はWebサイトへのアクセスによって発生することがあります。業務上必要のないWebサイトへのアクセスはお勧めしません。

Webからの脅威

WRS検出: 1名のユーザに対し、2件のWebサイトがブロックされました

ブロックされたWebサイトへのアクセスのトップ3:

ca80-1.winshipway.com	1
ca85-1.winshipway.com	1

URLカテゴリ検出: 12名のユーザに対し、20,757件のURLカテゴリがブロックされました

アクセス数が多いWebサイトのトップ3:

Web広告	20,753
新たに確認されたドメイン	4

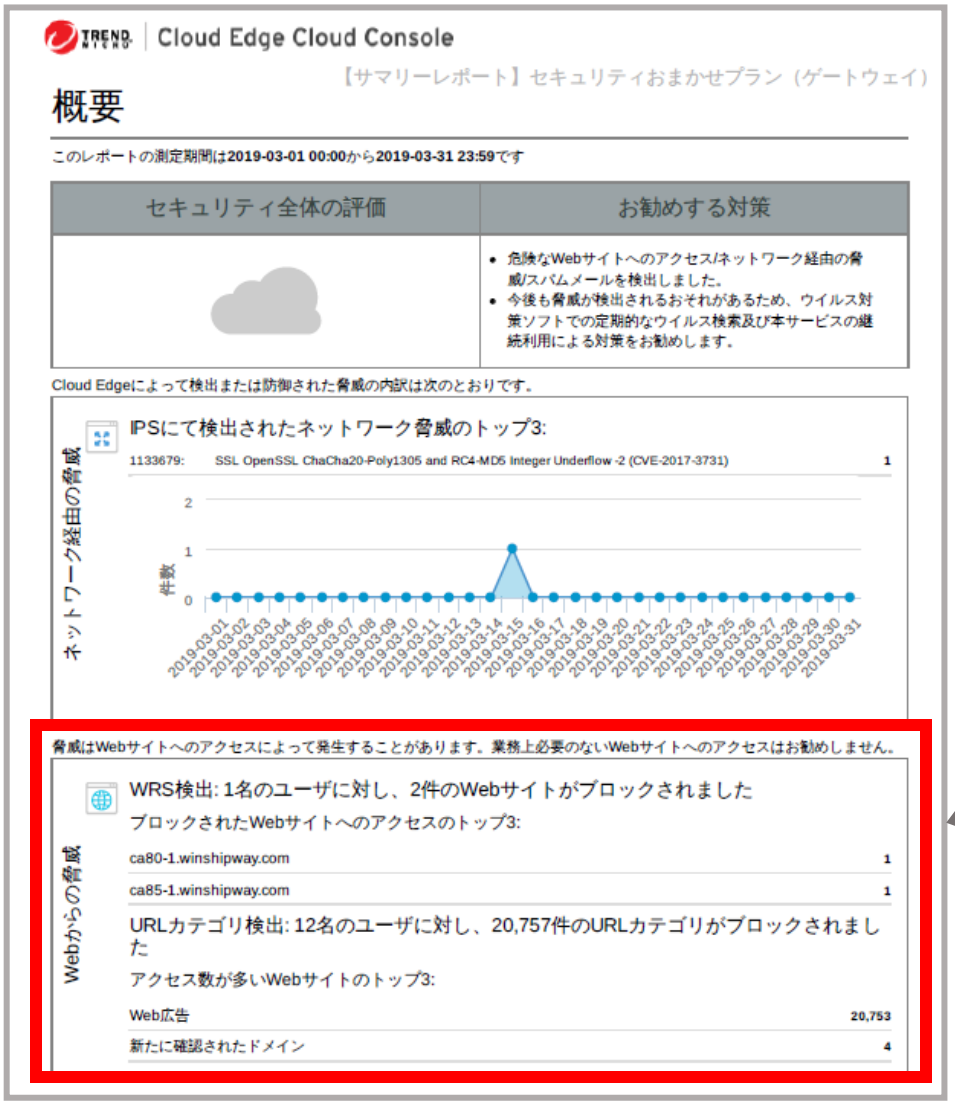


・該当のシステムにおいて、修正プログラムなどがないか確認および適用をし、システムやソフトウェアが最新の状態になってかいるかを改めて確認をしてください。

・またアクセス元に対しIPSの処理がブロックになっていることをご確認ください。

サマリーレポート詳細

□ 本ページでは、「セキュリティ全体の評価・お勧めする対策」、「ネットワーク経由の脅威」、「Webからの脅威」に関する情報を把握することができます。





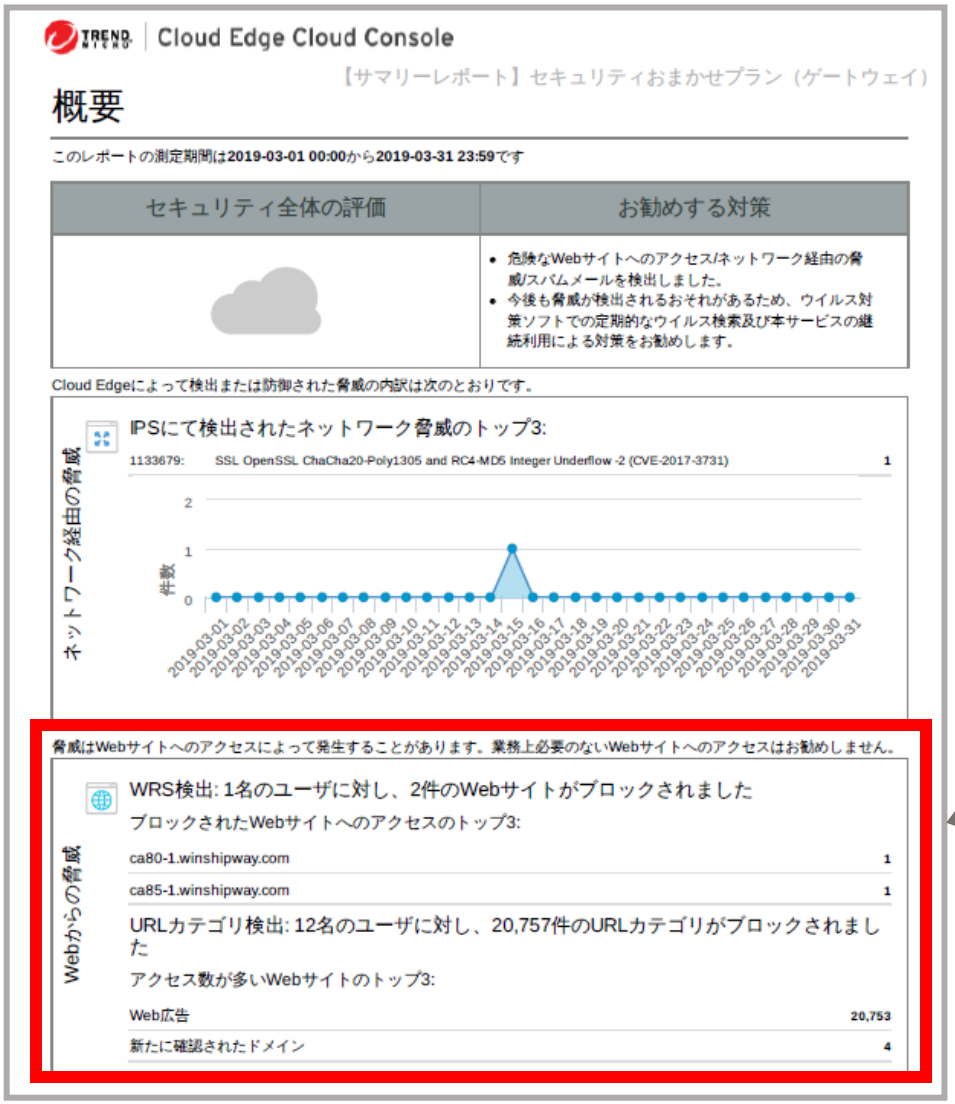
・WRS とは「Webレピュテーションサービス」の略称で、トレンドマイクロ社が危険と判断するWebページ(詐欺サイトやウイルス感染の危険性が高いサイト等)へのアクセスをブロックする機能です。

・上段では、WRSにより検知されたユーザ数やWebページ数及び、件数がTOP3に多いWebページのURLが確認できます。

・下段では、URL フィルタリング機能によりアクセスがブロックされたユーザ数やWebページ数及び、Cloud Edge下部からアクセスが多いURLのカテゴリ名が確認できます。

サマリーレポート詳細

- 本ページでは、「セキュリティ全体の評価・お勧めする対策」、「ネットワーク経由の脅威」、「Webからの脅威」に関する情報を把握することができます。

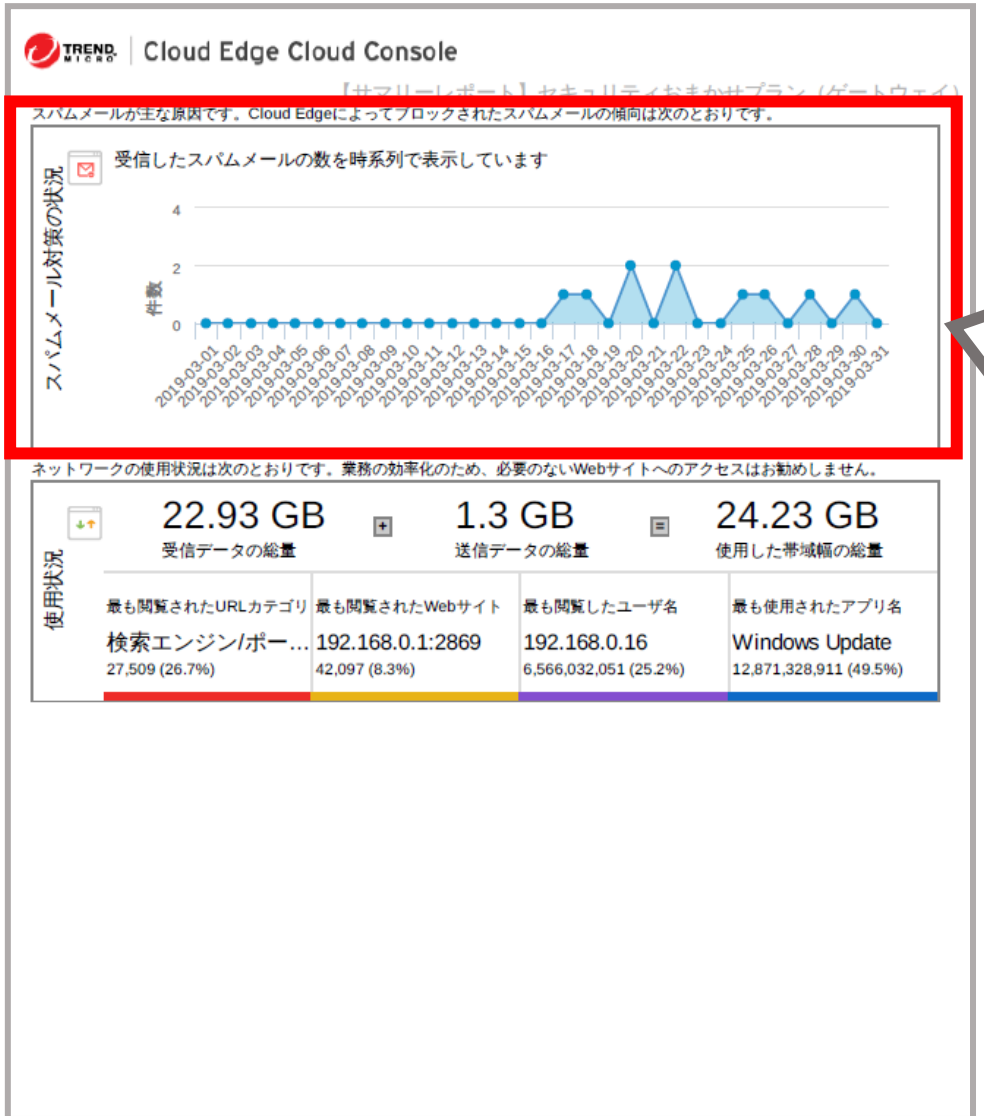




・WRS機能によりWebの脅威からの保護は実行されているものの、スパムメール等の不審なメールや、ブロックされたURLやそのカテゴリー、普段利用しないWebサイトURLをクリックしないなどの、社内での注意喚起・啓蒙活動を推奨いたします。

サマリーレポート詳細

■ 本ページでは、「スパムメール対策の状況」、「使用状況」に関する情報を把握することができます。



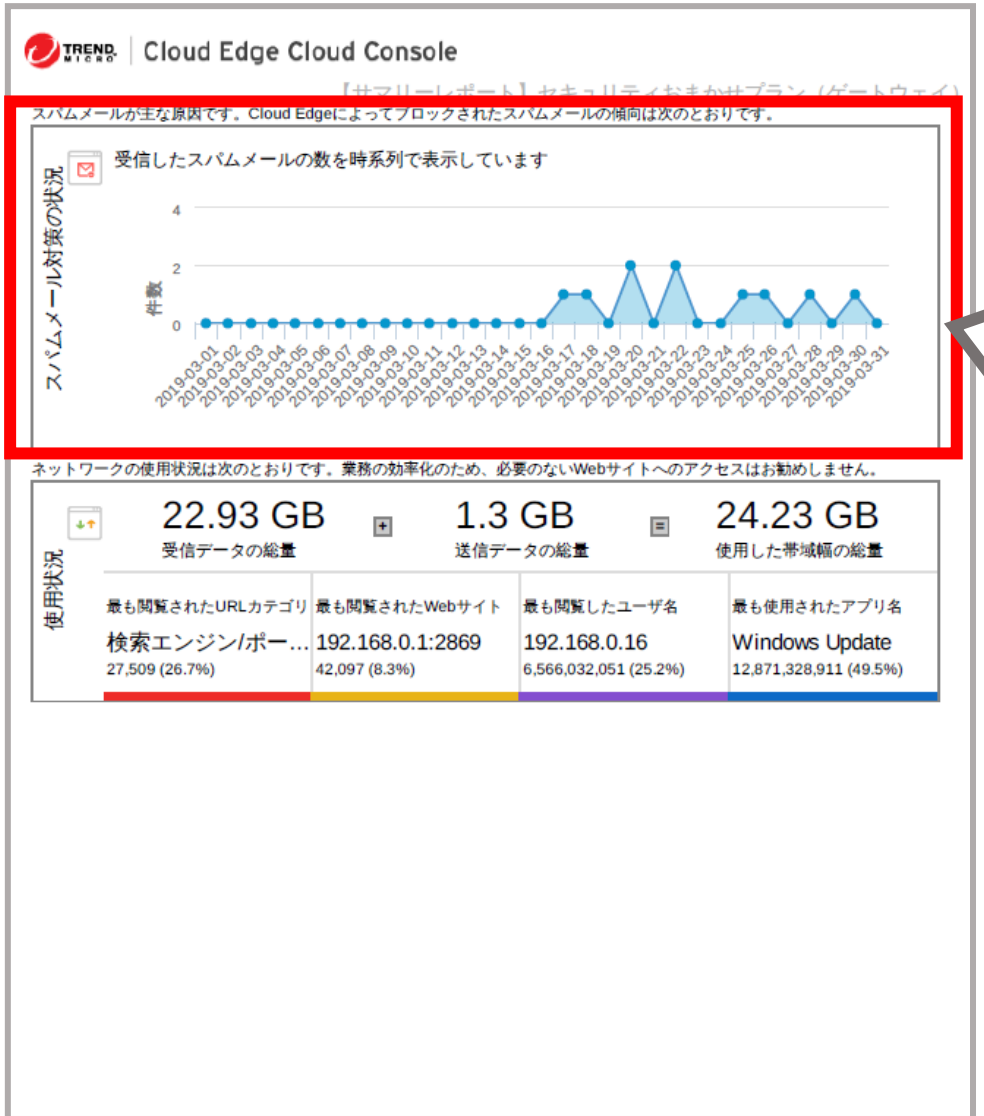


・スパムメール対策機能とは、受信者の意向を無視して一方的に送付される迷惑メールを検出する機能です。

・グラフでは検出したスパムメール数を時系列で把握することができます。

サマリーレポート詳細

■ 本ページでは、「スパムメール対策の状況」に関する情報を把握することができます。





・マルウェアや不正リモートユーザ、または受信者の移行を無視して一方的に送られています。

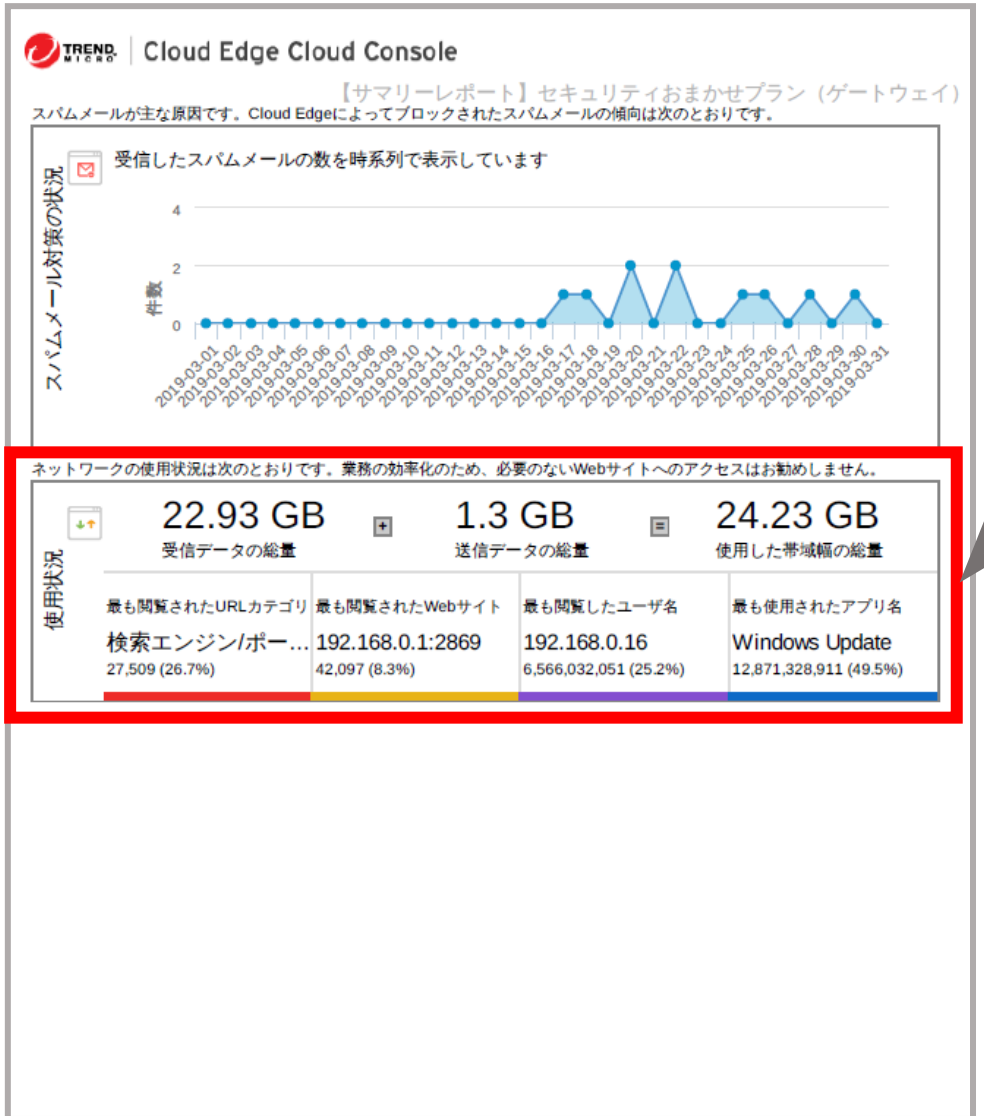
・スパムメールは宣伝目的のものからフィッシングサイトへの誘導やウイルスへの感染を引き起こすものもあるため、スパムメールとタグ付けされたメールに記載のURLや添付ファイルは開かないようご注意ください。

・スパムメールにもかかわらずスパムメールと判定されない場合は、UTMのスパムメール対策による検出率を標準の「中」から「高」に上げることをご検討ください。

・また大量のスパムメールは外部からの攻撃の予兆である可能性があるため、社員への注意喚起・啓蒙活動を推奨いたします。

サマリーレポート詳細

- 本ページでは、受信データの総量、送信データの総量、使用した帯域幅の総量を含む、ネットワークの使用状況を把握することができます。
- また最も閲覧されたURLカテゴリ・Webサイト・ユーザ名・アプリ名もご確認頂けます。



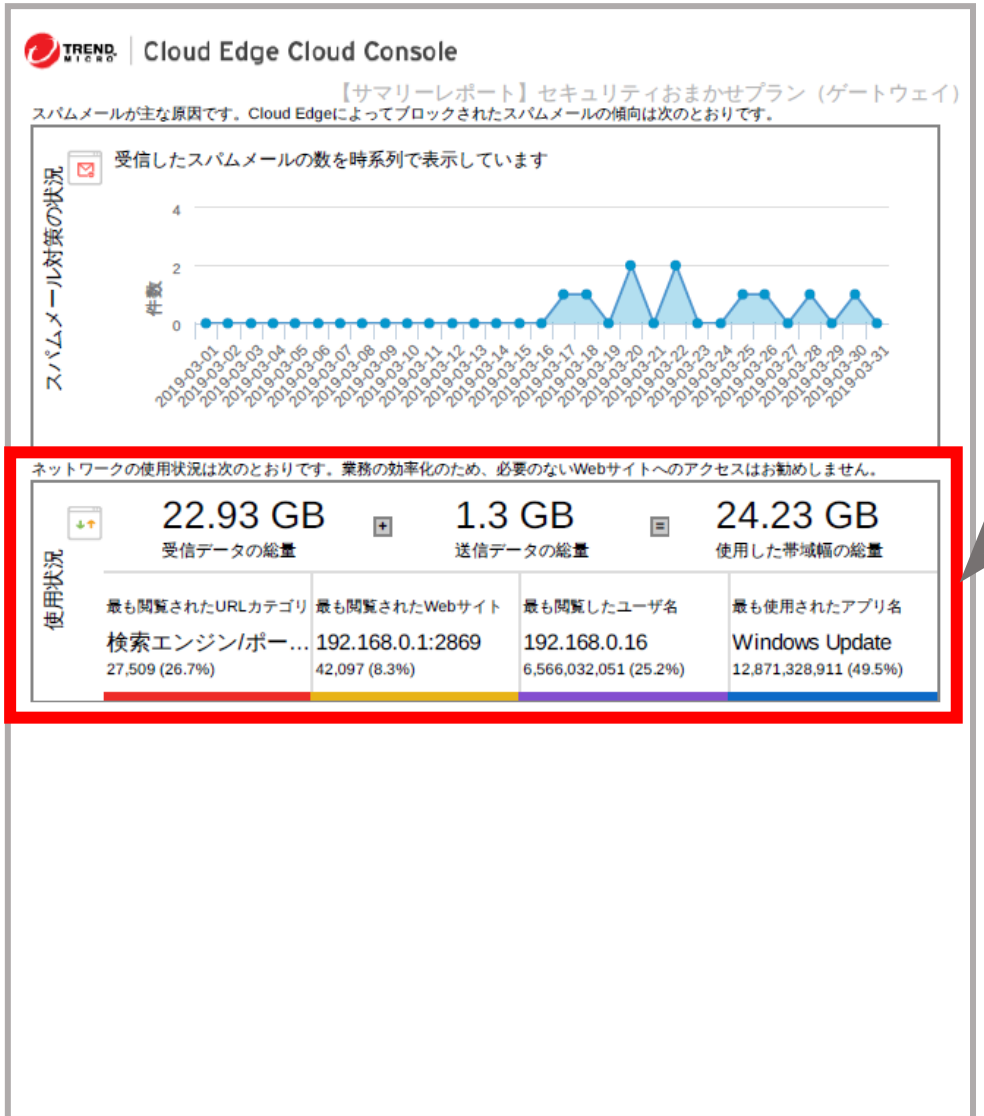


・Cloud Edge下部の端末から当該期間中に実施した通信量(送受信したデータ量)を把握することが出来ます。

・また、下部の端末から最もアクセスされたURLのカテゴリや最も利用されたアプリケーション名等も把握することができます。

サマリーレポート詳細

- 本ページでは、受信データの総量、送信データの総量、使用した帯域幅の総量を含む、ネットワークの使用状況を把握することができます。
- また最も閲覧されたURLカテゴリ・Webサイト・ユーザ名・アプリ名もご確認頂けます。





・通信内容を詳細にご確認されたい場合は、例えばNTT西日本の「働き方みえ～る」を活用し、社員別のPCログをご確認頂くことも可能です。

・大量の通信をしている不要なアプリケーションやWebサイトがあれば、業務への必要性をご確認のうえ、規制や社内での注意喚起をご検討ください。