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

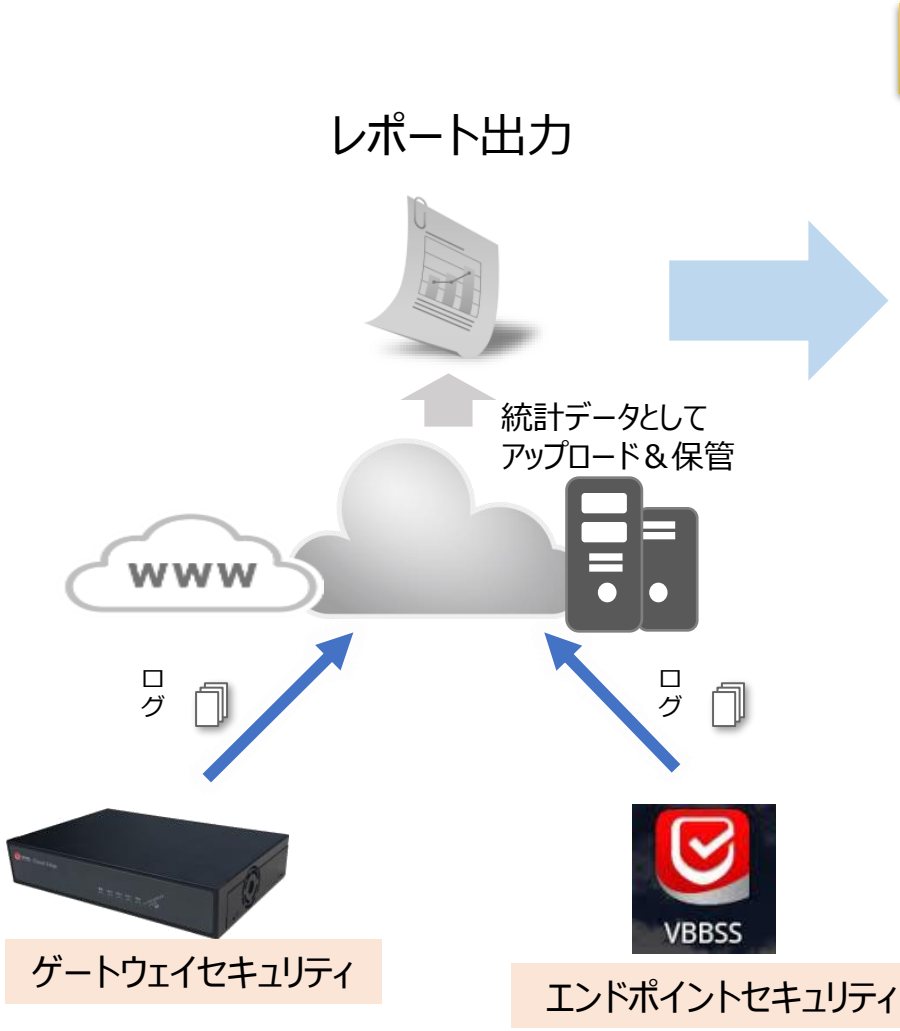
月次レポート ゲートウェイ編

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。

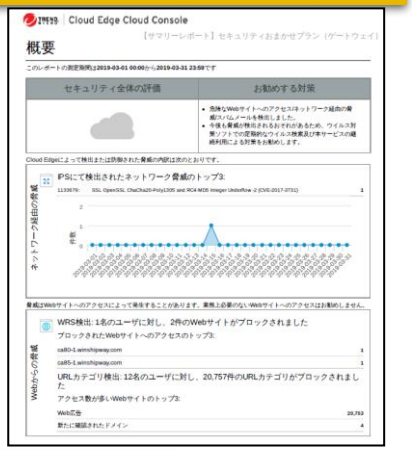


【セキュリティおまかせプラン月次レポート】ゲートウェイ


【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)

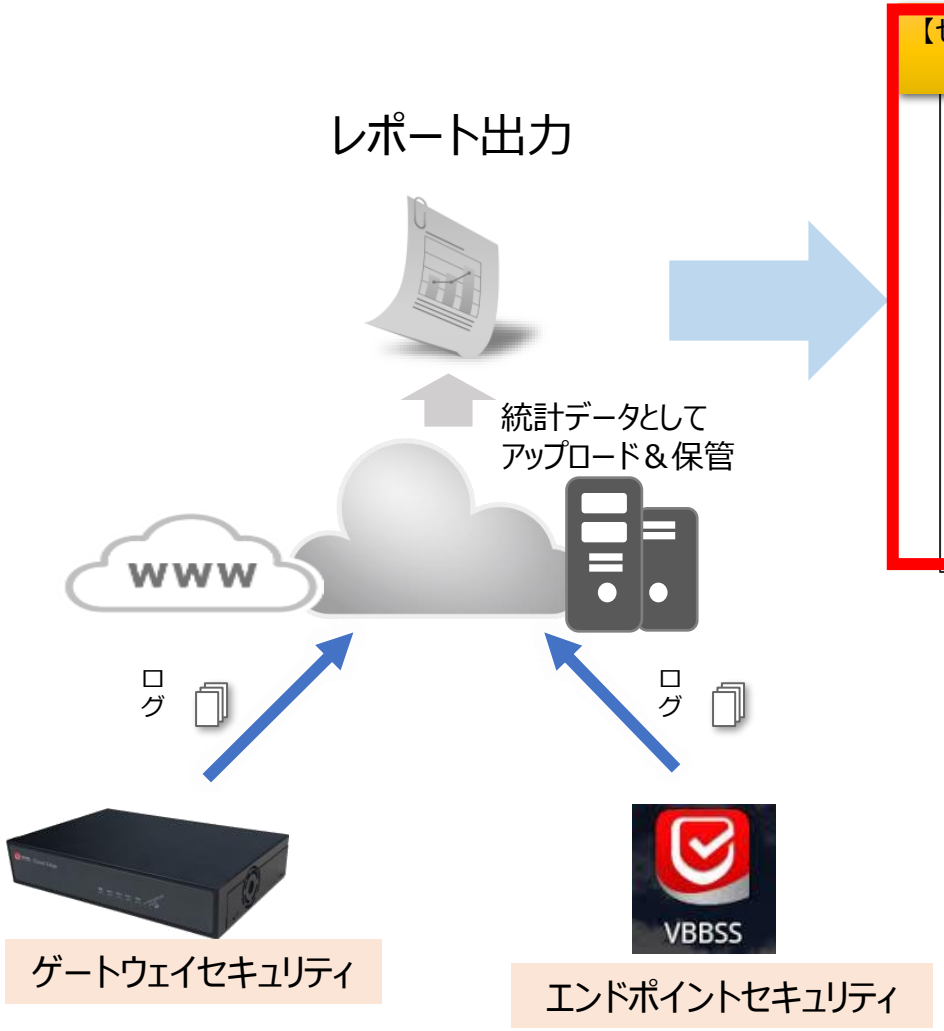

Cloud Edge Cloud Console
概要
セキュリティ全体の評価
お勧めする対策

【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 ）
目次

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。



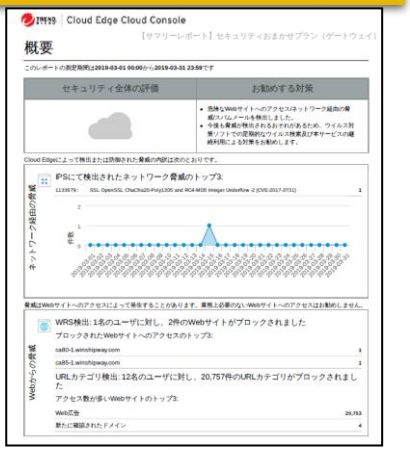
【セキュリティおまかせプラン月次レポート】ゲートウェイ


【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)

インターネットセキュリティ: 不正プログラム/スパイウェア検出の傾向 3
インターネットセキュリティ: 検出された上位の不正プログラムファイル 4
インターネットセキュリティ: 検出された不正プログラムファイル (日付別) 5
インターネットセキュリティ: 不正サイトによって検出された上位のユーザ 6
インターネットセキュリティ: 不正プログラムによって検出された上位のユーザ 7
インターネットセキュリティ: 検出された不正サイト (日付別) 8
インターネットセキュリティ: 検出された上位の不正サイト 9
インターネットセキュリティ: ランサムウェアによって検出された上位のユーザ (Webチャネル) 10
インターネットセキュリティ: 検出されたランサムウェア (Webチャネル/日付別) 11
インターネットセキュリティ: 検出された上位のランサムウェア (Webチャネル) 12
インターネットセキュリティ: ランサムウェアによってブロックされた上位のユーザ (メールチャネル) 13
インターネットセキュリティ: ランサムウェアによって検出された上位のユーザ (ネットワークチャネル) 14
インターネットセキュリティ: スパムメール対策によって検出された上位のユーザ 15
インターネットセキュリティ: マイナンバーによるフィルタで検出された上位のユーザ 16
インターネットセキュリティ: C&Cコールバックによって検出された上位のユーザ 17
インターネットセキュリティ: 上位のIPS検出 18
インターネットセキュリティ: IPSによって検出された上位のユーザ 19
インターネットセキュリティ: IPS検出 (日付別) 20
脅威種: 脅威種別の上位のアプリケーション 21
脅威種: 脅威種別の上位のユーザ 22
ポリシー施行: URLフィルタによってブロックされた上位のサイト 23
ポリシー施行: ブロックされた上位URLカテゴリ

【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
【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
セキュリティ全体の評価
お勧めする対策
IPSにて検出されたネットワーク脅威のトップ3:
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:
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:

【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）


TREND MICRO 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 ）
開始:2022年10月1日 00:00:00JST
終了:2022年11月1日 00:00:00JST
生成日時: 2022年11月1日 00:11:10JST
含まれるグループ: すべてのデバイス
目次
ウイルス/不正プログラムの概要
スパイウェア/グレーウェア概要
ウイルス/不正プログラムが検出されたエンドポイント（サーバを除く）の上位5件
ウイルス/不正プログラムが検出されたサーバの上位5件
検出されたネットワークウイルスの上位10件
ネットワークウイルスが検出されたエンドポイントの上位10件
スパイウェア/グレーウェアが検出されたエンドポイント（サーバを除く）の上位5件
スパイウェア/グレーウェアが検出されたサーバ上位5件
Web レピュテーション違反のあったエンドポイントの上位10件
挙動監視違反のあったプログラムの上位5件
挙動監視違反のあったエンドポイントの上位10件
デバイスコントロール違反のあったプログラムの上位5件
デバイスコントロール違反のあったエンドポイントの上位10件
URLフィルタ違反のあったカテゴリ上位5件
URLフィルタ違反のあったエンドポイントの上位10件

月次レポート（ゲートウェイ）の内容

- セキュリティおまかせプランでは、ゲートウェイが検知・ブロックした脅威に関する情報を月１回 (月初)にメールにて送付いたします。
- レポートには、下記の内容が記されております。

※**Cloud Edge**はトレンドマイクロ株式会社の登録商標です。

・インターネットセキュリティ

セキュリティ機能による脅威の検知状況に関する情報

– 不正プログラム/スパイウェア検出の傾向
– 検出された上位の不正プログラムファイル
– 検出された不正プログラムファイル(日付別)
– 不正サイトが検出された上位のユーザ
– 不正プログラムが検出された上位のユーザ
– 検出された不正サイト(日付別)
– 検出された上位の不正サイト
– ランサムウェアが検出された上位のユーザ(Webチャネル)
– 検出されたランサムウェア(Webチャネル/日付別)
– 検出された上位のランサムウェア(Webチャネル)
– ランサムウェアがブロックされた上位のユーザ(メールチャネル)
– ランサムウェアがブロックされた上位のユーザ(ネットワーク チャネル)
– スパムメール対策が検出された上位のユーザ
– マイナンバーによるフィルタで検出された上位のユーザ
– C&Cコールバックが検出された上位のユーザ
– 上位のIPS検出
– IPSによって検出された上位のユーザ
– IPS検出(日付別)

・帯域幅

Cloud Edge配下の端末からの通信量に関する情報

– 帯域幅別の上位のアプリケーション
– 帯域幅別の上位のユーザ

・ポリシー施行

URL指定及びアプリケーション指定によるアクセス制御機能の検知状況に関する情報

– URLフィルタによってブロックされた上位のサイト
– ブロックされた上位URLカテゴリ
– ブロックされた上位のアプリケーション
– 適用された上位のユーザ

・インターネットアクセス

Cloud Edge配下の端末からのインターネット利用状況に関する情報

– アクセスされた上位のサイト
– 要求別の上位のユーザ
– アクセスされた上位のURLカテゴリ
– アクセスされた上位のアプリケーション

月次レポート（ゲートウェイ）の内容

本動画でいくつか内容をご紹介いたします。

要注意レポートの紹介
危険レポートの紹介（まずは確認をおすすめ）
運用上是正すべきレポートの紹介

・インターネットセキュリティ

セキュリティ機能による脅威の検知状況に関する情報

- 不正プログラム/スパイウェア検出の傾向
- 検出された上位の不正プログラムファイル
- 検出された不正プログラムファイル(日付別)
- 不正サイトが検出された上位のユーザ
- 不正プログラムが検出された上位のユーザ
- 検出された不正サイト(日付別)
- 検出された上位の不正サイト
- ランサムウェアが検出された上位のユーザ(Webチャネル)
- 検出されたランサムウェア(Webチャネル/日付別)
- 検出された上位のランサムウェア(Webチャネル)
- ランサムウェアがブロックされた上位のユーザ(メールチャネル)
- ランサムウェアがブロックされた上位のユーザ(ネットワーク チャネル)
- スパムメール対策が検出された上位のユーザ
- マイナンバーによるフィルタで検出された上位のユーザ
- C&Cコールバックが検出された上位のユーザ
- 上位のIPS検出
- IPSによって検出された上位のユーザ
- IPS検出(日付別)

・帯域幅

Cloud Edge配下の端末からの通信量に関する情報

- 帯域幅別の上位のアプリケーション
- 帯域幅別の上位のユーザ

・ポリシー施行

URL指定及びアプリケーション指定によるアクセス制御機能の検知状況に関する情報

- URLフィルタによってブロックされた上位のサイト
- ブロックされた上位URLカテゴリ
- ブロックされた上位のアプリケーション
- 適用された上位のユーザ

・インターネットアクセス

Cloud Edge配下の端末からのインターネット利用状況に関する情報

- アクセスされた上位のサイト
- 要求別の上位のユーザ
- アクセスされた上位のURLカテゴリ
- アクセスされた上位のアプリケーション

月次レポート（ゲートウェイ）の内容

インターネットセキュリティ

セキュリティ機能による脅威の検知状況に関する情報

レポート項目タイトル	説明
不正プログラム/スパイウェア検出の傾向	指定した期間における不正プログラム/スパイウェアの検出数の傾向を示します。
検出された上位の不正プログラムファイル	検出数が上位の不正プログラムファイルを示します。
検出された不正プログラムファイル (日付別)	不正プログラムファイルの検出数を日付別に示します。
不正サイトによって検出された上位のユーザ	不正サイトへのアクセスが検出された上位のユーザに関する棒グラフを示します。
不正プログラムによって検出された上位のユーザ	不正プログラムの実行が検出された上位のユーザに関する棒グラフを示します。
検出された不正サイト (日付別)	不正サイトの検出数を日付別に示します。
検出された上位の不正サイト	検出数が上位の不正サイトを示します。
ランサムウェアが検出された上位のユーザ(Webチャネル)	Webチャネルによってランサムウェアが検出された上位のユーザ/グループに関する棒グラフを示します。
検出されたランサムウェア (Webチャネル/日付別)	Webチャネルによって検出されたランサムウェアの件数を日付別に示します。
検出された上位のランサムウェア (Webチャネル)	ランサムウェアが組み込まれている、上位のWebサイトを示します。

月次レポート（ゲートウェイ）の内容

インターネットセキュリティ

セキュリティ機能による脅威の検知状況に関する情報

レポート項目タイトル	説明
ランサムウェアがブロックされた上位のユーザ(メールチャネル)	メールチャネルによってランサムウェアがブロックされた上位のユーザに関する棒グラフを示します。
ランサムウェアがブロックされた上位のユーザ(ネットワーク チャネル)	ネットワークチャネルによってランサムウェアが検出された上位のユーザに関する棒グラフを示します。
スパムメール対策が検出された上位のユーザ	スパムメール対策エンジンによってスパムが検出された上位のユーザに関する棒グラフを示します。スパムメール対策エンジンとは、マルウェアや不正リモートユーザによって大量にばらまかれた迷惑メールをブロックまたはタグ付けを行うものです。
マイナンバーによるフィルタで検出された上位のユーザ	マイナンバーによるフィルタで検出された上位のユーザに関する棒グラフを示します。内部から送信されたメールに対して、メールの内容にマイナンバー情報が検出された上位のユーザに関する棒グラフを示します。マイナンバーによるフィルタを有効にすれば、マイナンバーの情報漏えいを防止できます。
C&Cコールバックが検出された上位のユーザ	C&Cコールバックによって脅威が検出された上位のユーザに関する棒グラフを示します。C&Cコールバックとは、ウイルスに感染したコンピュータに遠隔から不正な指示を送るC&Cサーバへの接続を監視し、ブロックする機能です。IPアドレスにより、どのユーザがC&Cサーバへの通信を実施しているかを把握することができます
上位のIPS検出	上位のIPS検出を示します。IPSとはネットワークへの脆弱性攻撃や不正侵入を検知・防御するものです。Cloud EdgeではIPSのパターンファイルを使用してIPS脆弱性をブロックします。
IPSによって検出された上位のユーザ	IPSによって脅威が検出された上位のユーザに関する棒グラフを示します。
IPS検出 (日付別)	IPS検出数を日付別に示します。

月次レポート（ゲートウェイ）の内容

帯域幅

Cloud Edge配下の端末からの通信量に関する情報

レポート項目タイトル	説明
帯域幅別の上位アプリケーション	帯域幅別にアクセス頻度が高いアプリケーションに関する棒グラフを示します。 ネットワーク上のIPアドレス、ユーザ、アプリケーションによる帯域幅の消費を確認できます。帯域幅とは、PCやスマートフォンなどでインターネットを利用する際に、それらの端末から送られる電波や電気信号の幅であり、一般的に帯域が広いと通信速度が速いとされています。
帯域幅別の上位のユーザ	上位のユーザの帯域幅に関する棒グラフを示します。

ポリシー施行

URL指定及びアプリケーション指定によるアクセス制御機能の検知状況に関する情報

レポート項目タイトル	説明
URLフィルタによってブロックされた上位のサイト	URLフィルタによってブロックされた上位のサイトに関する棒グラフを示します。
ブロックされた上位URLカテゴリ	URLフィルタによってブロックされた上位URLカテゴリに関する棒グラフを示します。
ブロックされた上位のアプリケーション	URLフィルタによってブロックされた上位のアプリケーションに関する棒グラフを示します。
適用された上位のユーザ	上位のユーザに関する棒グラフを示します。 ポリシー設定（例：Winny等）に該当した上位ユーザのネットワークトラフィックを確認できます。

月次レポート（ゲートウェイ）の内容

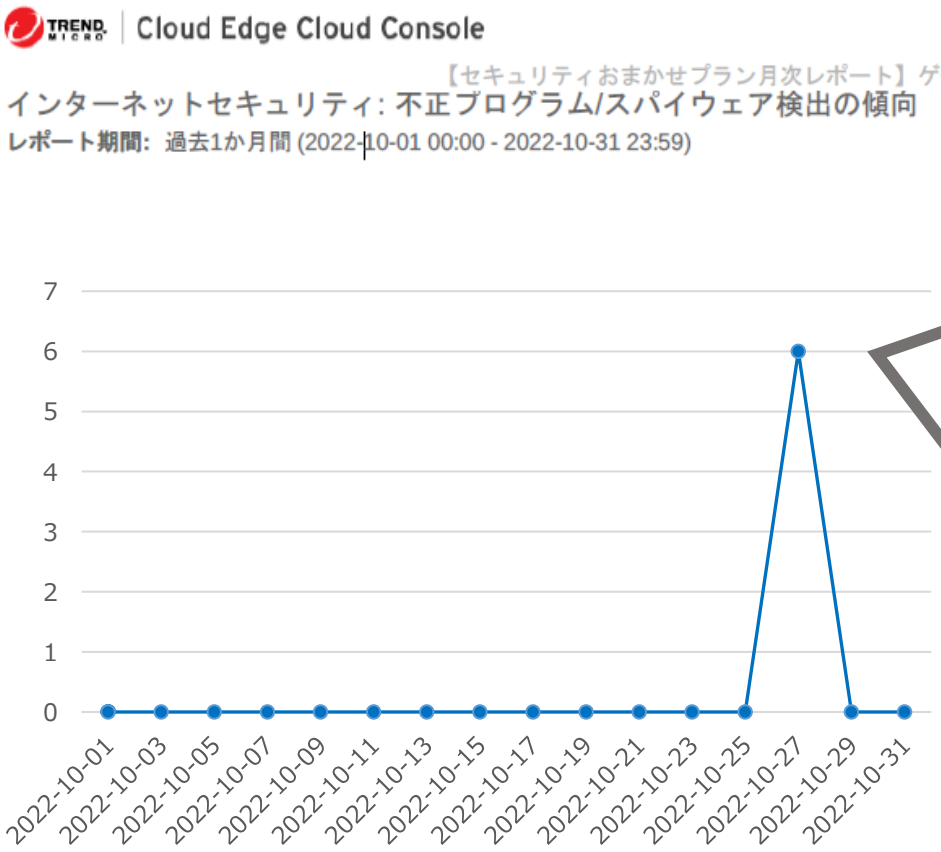
インターネットアクセス

Cloud Edge配下の端末からの
インターネット利用状況に関する情報

レポート項目タイトル	説明
アクセスされた上位のサイト	アクセス頻度が高いWebサイトに関する棒グラフを示します。
要求別の上位のユーザ	上位のユーザの要求件数に関する棒グラフを示します。
アクセスされた上位のURLカテゴリ	アクセス頻度が高いWebサイトカテゴリに関する棒グラフを示します。
アクセスされた上位のアプリケーション	アクセス頻度が高いアプリケーションに関する棒グラフを示します。

不正プログラム/スパイウェア検出の傾向

- 本ページでは、設置したCloud Edgeが当月中に不正プログラム/スパイウェアを検出した件数(日付別)を知ることができます。
- スパイウェアとは、コンピュータ内部からインターネットに対して情報を送り出したり、個人情報の収集を行う悪質なソフトウェアの総称です。



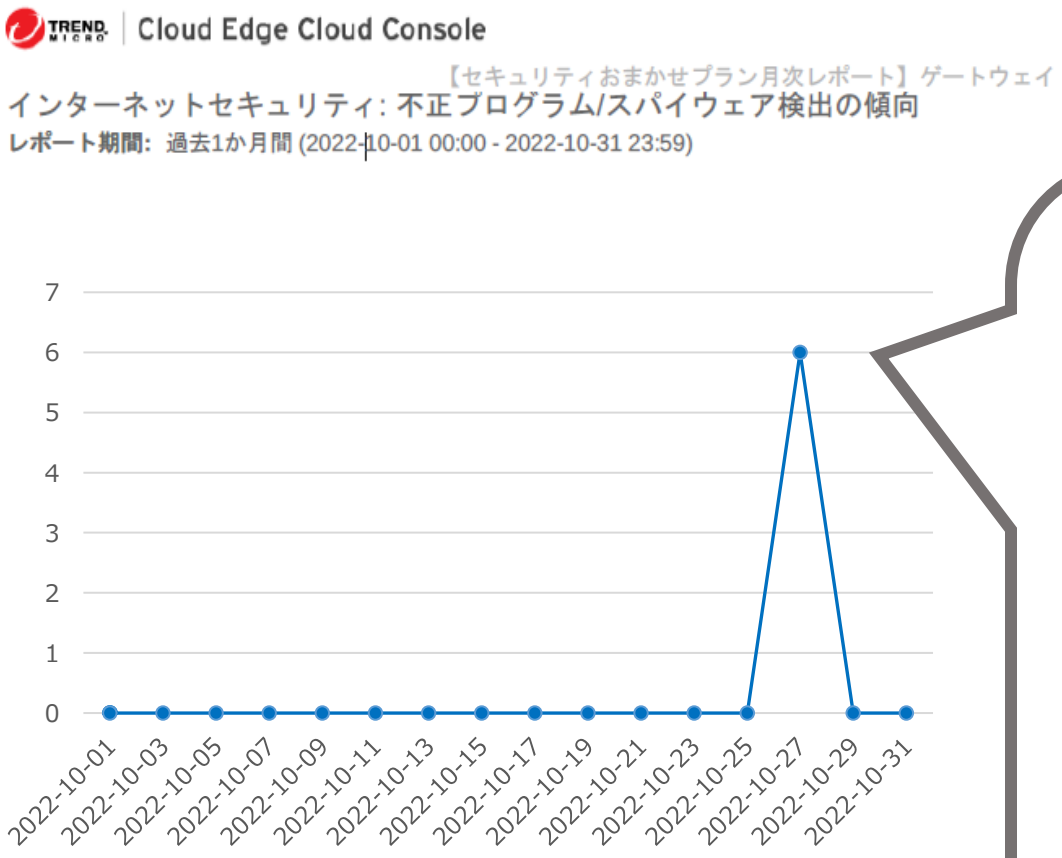
ユーザがCloud Edgeを経由して、
・受信したメールの添付ファイル
・Webからダウンロードしたファイル
が不正プログラムやスパイウェアであることを検知した日付別の件数です。

横軸：検出した日付
縦軸：検出した件数

※グラフはイメージです。実際のレポートに記載の内容とは異なります。

不正プログラム/スパイウェア検出の傾向

- 本ページでは、設置したCloud Edgeが当月中に不正プログラム/スパイウェアを検出した件数(日付別)を知ることができます。
- スパイウェアとは、コンピュータ内部からインターネットに対して情報を送り出したり、個人情報の収集を行う悪質なソフトウェアの総称です。





実施していたセキュリティ対策を通過した不正プログラムを10月27日に検出、ブロックしています。

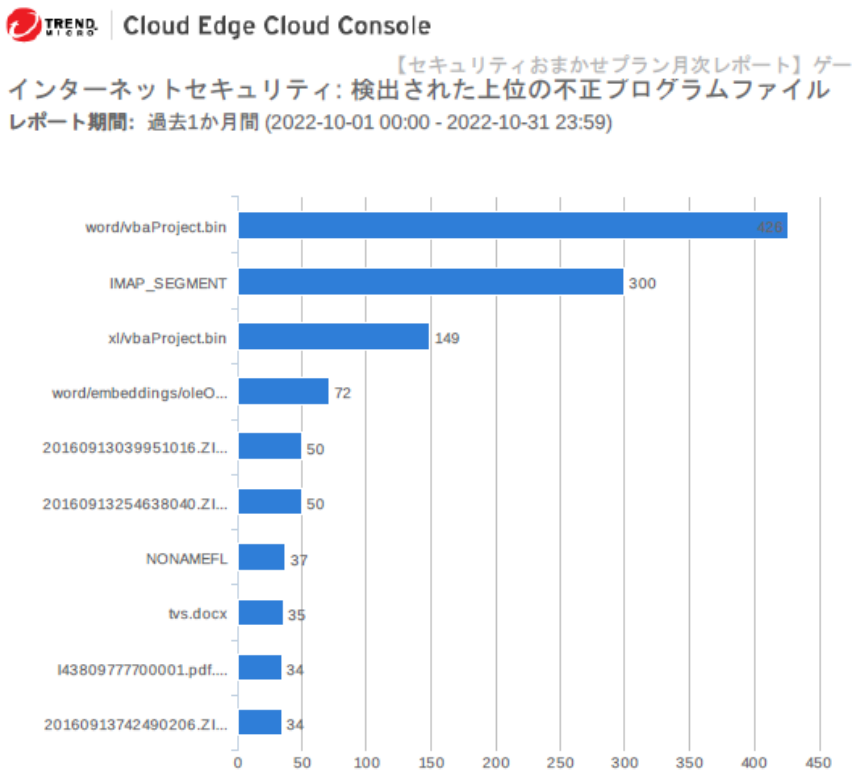
日付別の増減から傾向を把握いただき、検知された場合は「不正プログラムによって検出された上位のユーザ」を参照いただくことをお勧めいたします。

もしCloud Edgeが設置されていなければ、ウイルス感染している可能性がありました。

※グラフはイメージです。実際のレポートに記載の内容とは異なります。

検出された上位の不正プログラムファイル

- 本ページでは、設置したCloud Edgeが当月中に検出した数が多い上位10件の不正プログラム/スパイウェア名を知ることができます。



※グラフはイメージです。実際のレポートに記載の内容とは異なります。



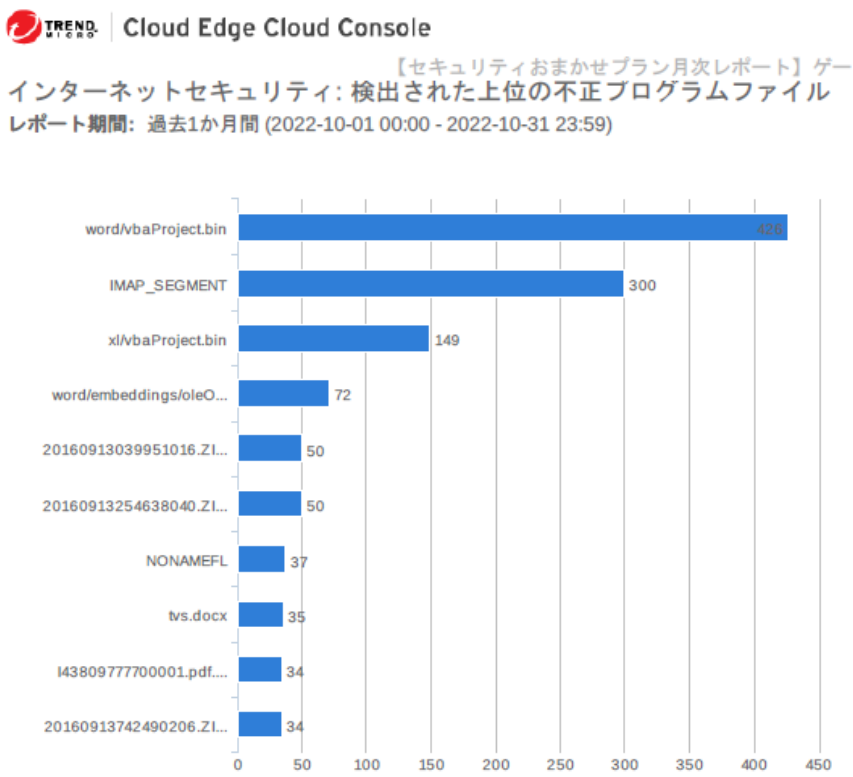
Cloud Edgeが検出した不正プログラム/スパイウェアのうち、検出数が多い不正プログラム/スパイウェアの上位10件です。

横軸：検出した件数

縦軸：検出件数が多い上位10件の不正プログラム/スパイウェア名

検出された上位の不正プログラムファイル

- 本ページでは、設置したCloud Edgeが当月中に検出した数が多い上位10件の不正プログラム/スパイウェア名を知ることができます。
- スパイウェアとは、コンピュータ内部からインターネットに対して情報を送り出す悪質なソフトウェアの総称です。



※グラフはイメージです。実際のレポートに記載の内容とは異なります。

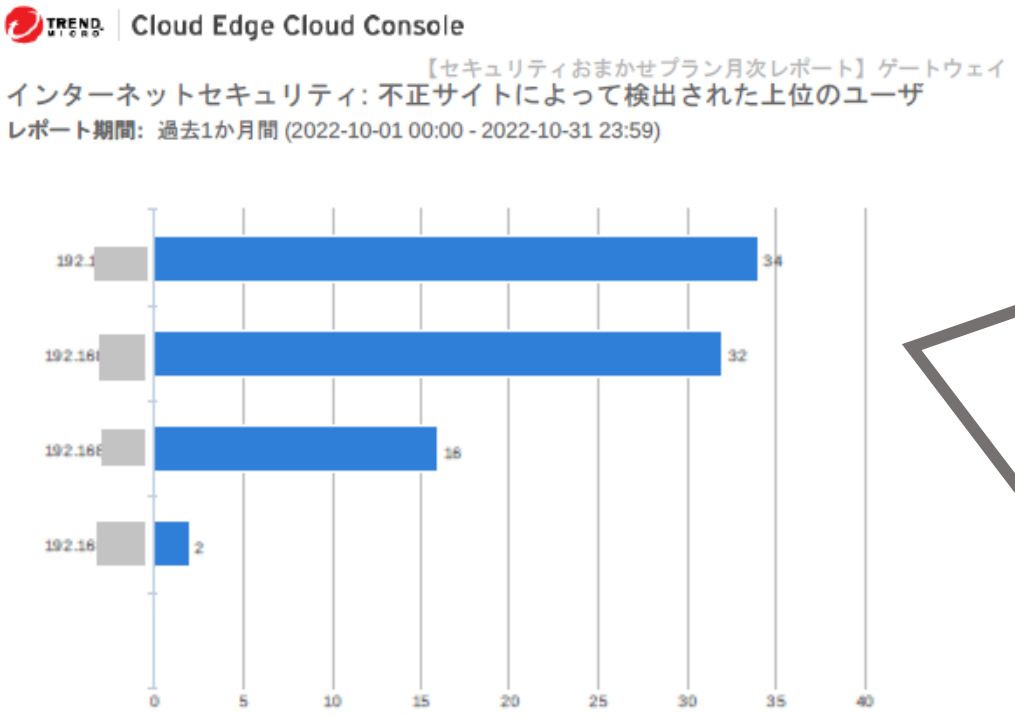


Cloud Edgeが不正プログラムの脅威からユーザを保護しています。

更なるセキュリティ強化のために、Cloud Edgeだけでなく端末側でのウイルススキャンの実施・強化をお勧めいたします。

不正サイトによって検出された上位のユーザ

- 本ページでは、Webサイトアクセスブロック機能により、Cloud Edgeが1 ヶ月以内に不正サイトへの接続を検知・ブロックした結果を把握することができます。
- IPアドレスの情報から、どのユーザが不正サイトへのアクセスを試みているかを把握することができます。



192.168.x.xxx	34
192.168.x.xxx	32
192.168.x.xxx	16
192.168.x.xxx	2

※グラフはイメージです。実際のレポートに記載の内容とは異なります。

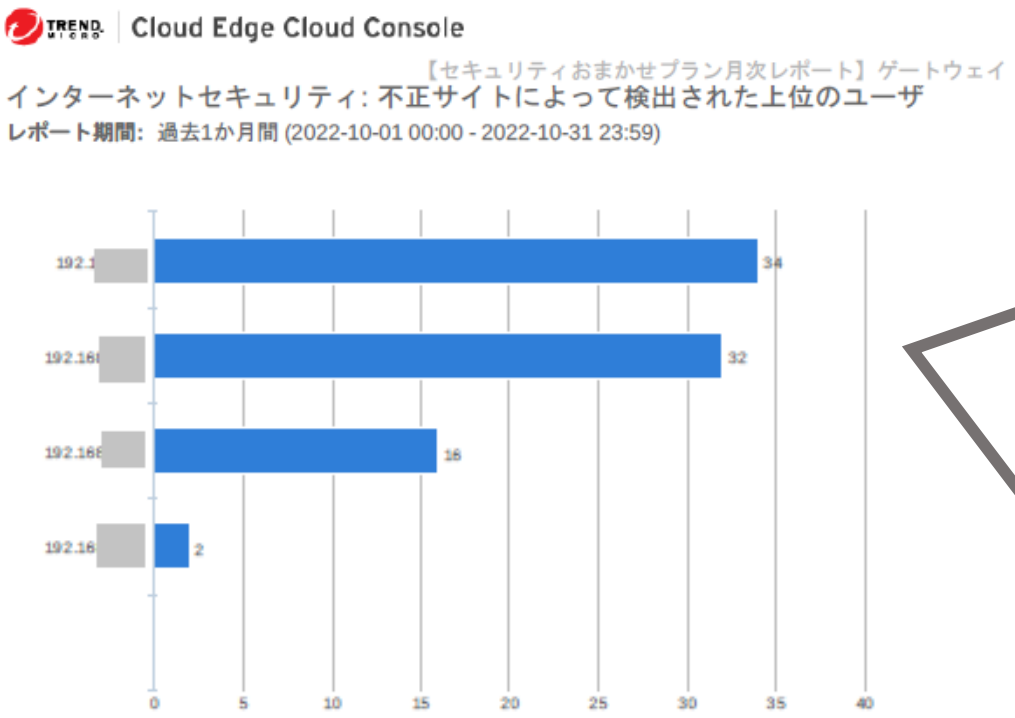
Cloud Edgeを経由してWebサイトにアクセスした際に、不正なサイトであることを検知し、ブロックした結果です（ユーザ別）

横軸：不正なWebアクセス数

縦軸：ユーザ（表記されているIPアドレスを保持する端末）

不正サイトによって検出された上位のユーザ

- 本ページでは、Webサイトアクセスブロック機能により、Cloud Edgeが1 ヶ月以内に不正サイトへの接続を検知・ブロックした結果を把握することができます。
- IPアドレスの情報から、どのユーザが不正サイトへのアクセスを試みているかを把握することができます。



192.168.x.xxx	34
192.168.x.xxx	32
192.168.x.xxx	16
192.168.x.xxx	2

※グラフはイメージです。実際のレポートに記載の内容とは異なります。

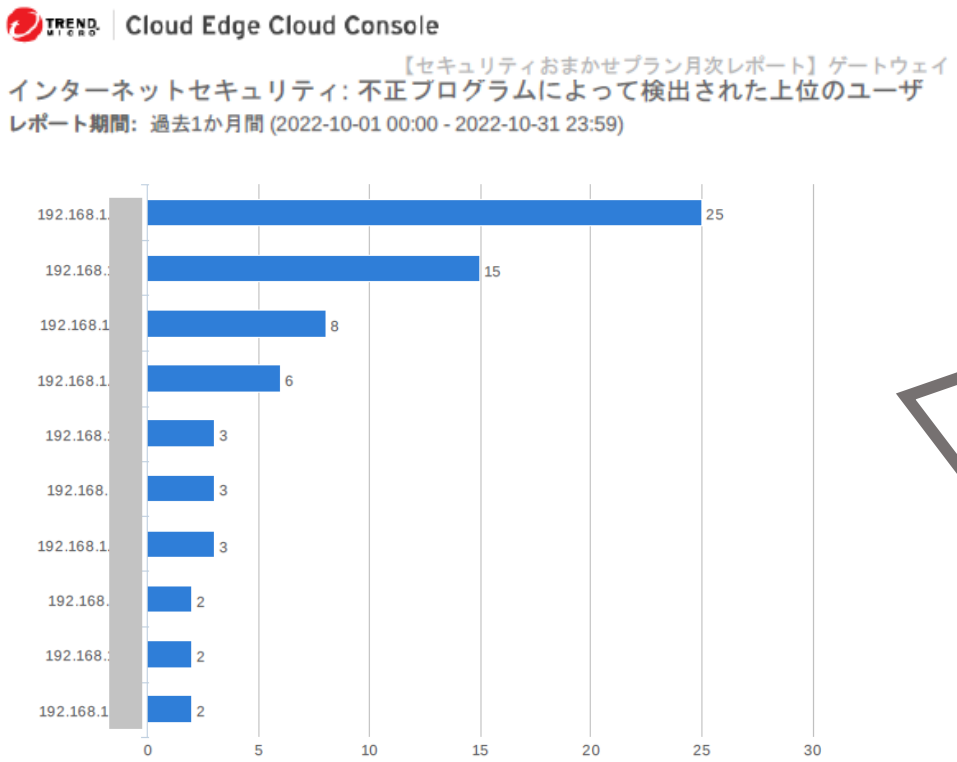


Cloud Edgeがアクセスをとめていますが、なければ不正プログラムの感染や、情報搾取、詐欺の被害にあっていた可能性があります。

各端末を操作している人に、アクセスの理由をヒアリングいただくことをお勧めします。

不正プログラムによって検出された上位のユーザ

- 本ページでは、Cloud Edgeが1 ヶ月以内に不正プログラム/スパイウェアを検知した結果を把握することができます。
- IPアドレスの情報から、どのユーザが不正プログラムの検知をしたかを把握することができます。



192.168.x.xxx	25
192.168.x.xxx	15
192.168.x.xxx	8
192.168.x.xxx	6
⋮	

※グラフはイメージです。実際のレポートに記載の内容とは異なります。



不正プログラム/スパイウェアのダウンロードを試みた回数が多いユーザの上位10件のアクセス数です。
Webからのダウンロードだけでなく、メールでの不正プログラム検知も対象となります。

横軸：検出した件数
縦軸：検出件数が多い、上位10件のユーザ
（表記されているIPアドレスを保持する端末）

不正プログラムによって検出された上位のユーザ

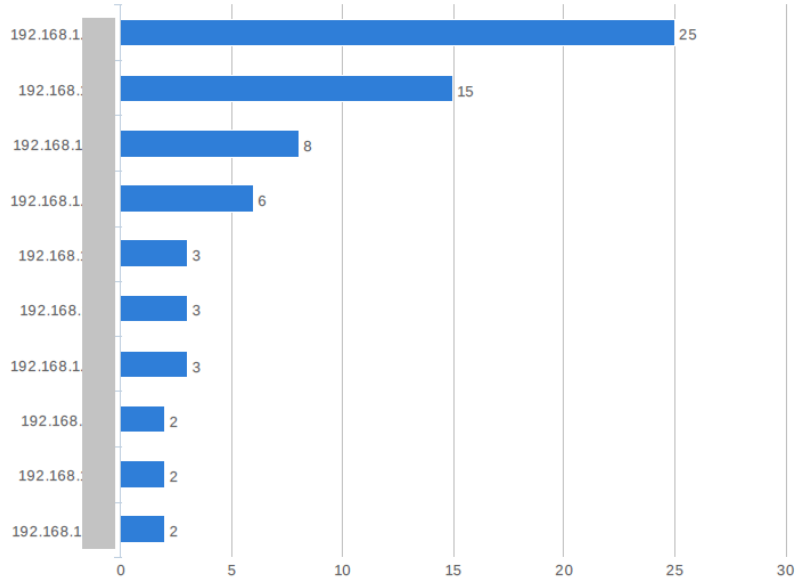
- 本ページでは、Cloud Edgeが1 ヶ月以内に不正プログラム/スパイウェアを検知した結果を把握することができます。
- IPアドレスの情報から、どのユーザが不正プログラムの検知をしたかを把握することができます。

Cloud Edge Cloud Console

【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

インターネットセキュリティ: 不正プログラムによって検出された上位のユーザ

レポート期間: 過去1か月間 (2022-10-01 00:00 - 2022-10-31 23:59)



192.168.x.xxx	25
192.168.x.xxx	15
192.168.x.xxx	8
192.168.x.xxx	6

※グラフはイメージです。実際のレポートに記載の内容とは異なります。

ウイルスを受け取っていた端末です。

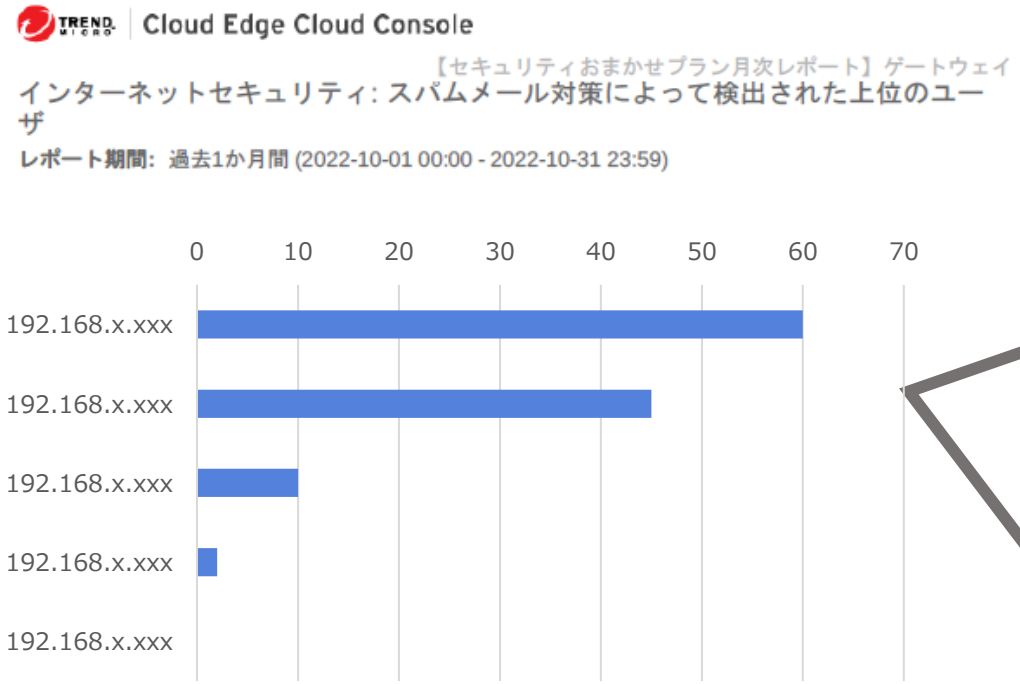
これらの端末は、Cloud Edgeがなければ感染の危険がありました。

危険な操作をしていなかったか？の確認と、注意喚起をすることをおすすめします。

また該当端末でウイルス対策がなされているかを確認し、なされている場合も最新パターンでフルスキャンを行うことをお勧めいたします。

スパムメール対策によって検出された上位のユーザ

- 本ページでは、メールセキュリティ機能によりCloud Edgeが１ヶ月以内にスパムメールを検知した結果を把握することが出来ます。
- IPアドレスにより、どのユーザがスパムメールを受け取っているかを把握することが出来ます。



192.168.x.xxx	60
192.168.x.xxx	45
192.168.x.xxx	10
192.168.x.xxx	5

※グラフはイメージです。実際のレポートに記載の内容とは異なります。

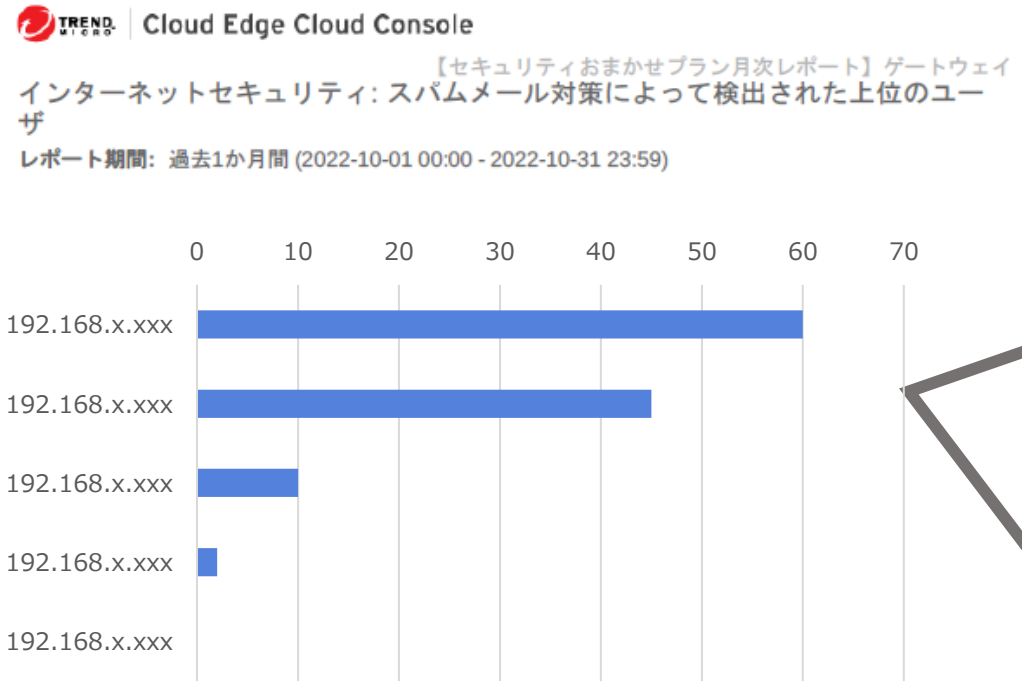
スパムメールを受信した上位10件のユーザに関する情報です。

横軸：検出した件数
縦軸　：ユーザ（表記されている IP アドレスを保持する端末）

スパムメールとは主に宣伝広告目的で、ユーザの同意なしに勝手に送られてくる電子メールのことです。中にはウイルス感染につながる攻撃のメールも含まれます。

スパムメール対策によって検出された上位のユーザ

- 本ページでは、メールセキュリティ機能によりCloud Edgeが１ヶ月以内にスパムメールを検知した結果を把握することが出来ます。
- IP アドレスにより、どのユーザがスパムメールを受け取っているかを把握することが出来ます。



192.168.x.xxx	60
192.168.x.xxx	45
192.168.x.xxx	10
192.168.x.xxx	5

※グラフはイメージです。実際のレポートに記載の内容とは異なります。



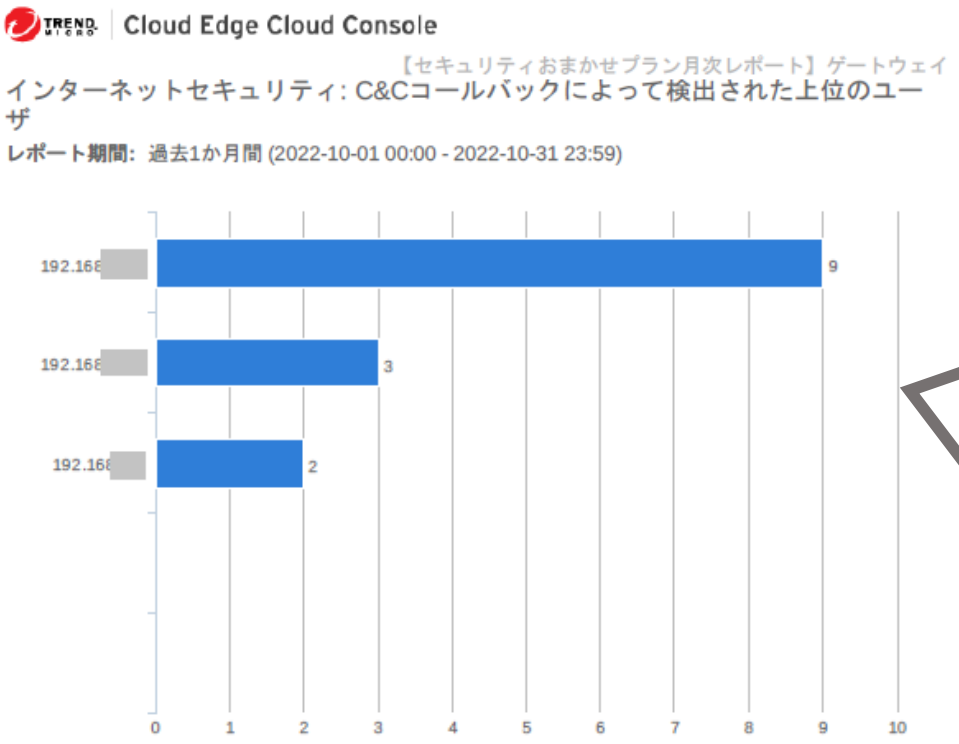
検出された端末は、Cloud Edgeがなければ不正プログラムの感染や、情報搾取、詐欺の被害にあっていた可能性がありました。

メールを利用した攻撃の中には、お客様や取引先、会社上層部を騙り、ウイルスの添付や危険なURL、または詐欺を計るといった「標的型攻撃メール」があります。メールの件名にスパムメールと記載のものは開封しないこと、本文記載のURLはクリックしないようお願いいたします。

また一度ターゲットになったメールアドレスは、今後も危険なメールのターゲットになるため、使用者への注意喚起も忘れずに実施ください。

C&Cコールバックによって検出された上位のユーザ

- 本ページでは、不正プログラム侵入検知機能により、Cloud Edgeが1 ヶ月以内にC&Cサーバへ接続を検知・ブロックした結果を把握することができます。
- IPアドレスにより、どのユーザがC&Cサーバへの通信を実施しているかを把握することができます。



192.168.x.xxx	9
192.168.x.xxx	3
192.168.x.xxx	2

※グラフはイメージです。実際のレポートに記載の内容とは異なります。



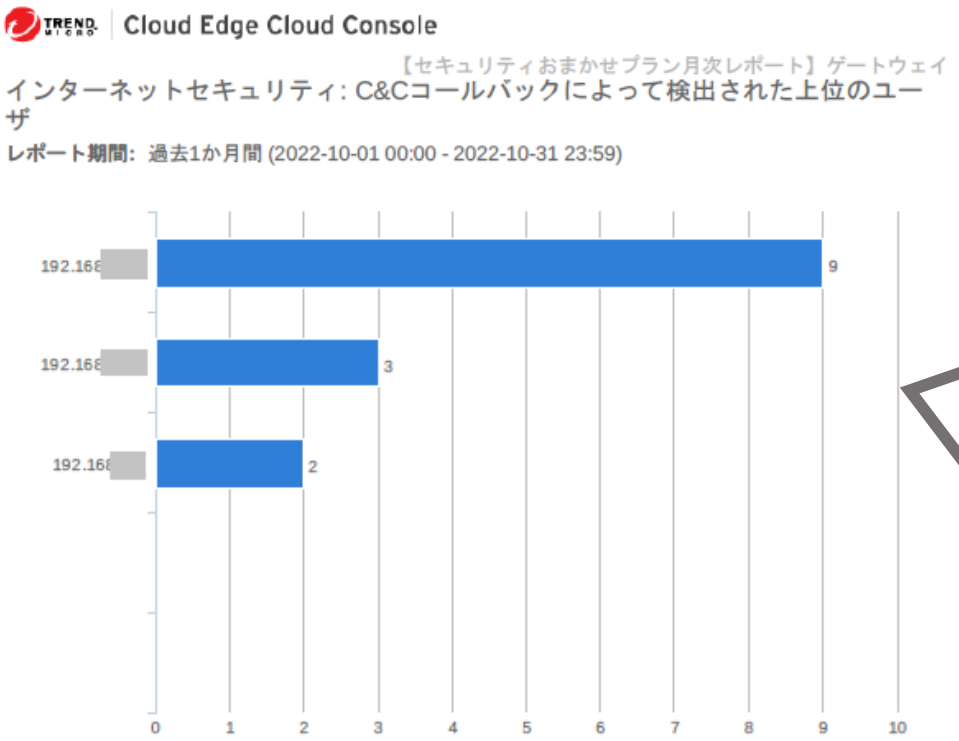
Cloud Edgeを経由してC&Cサーバへの接続を行った上位10件のユーザに関する情報です。

横軸：検出した件数

縦軸：ユーザ（表記されている IP アドレスを保持する端末）

C&Cコールバックによって検出された上位のユーザ

- 本ページでは、不正プログラム侵入検知機能により、Cloud Edgeが1 ヶ月以内にC&Cサーバへ接続を検知・ブロックした結果を把握することができます。
- IPアドレスにより、どのユーザがC&Cサーバへの通信を実施しているかを把握することができます。



192.168.x.xxx	9
192.168.x.xxx	3
192.168.x.xxx	2

※グラフはイメージです。実際のレポートに記載の内容とは異なります。

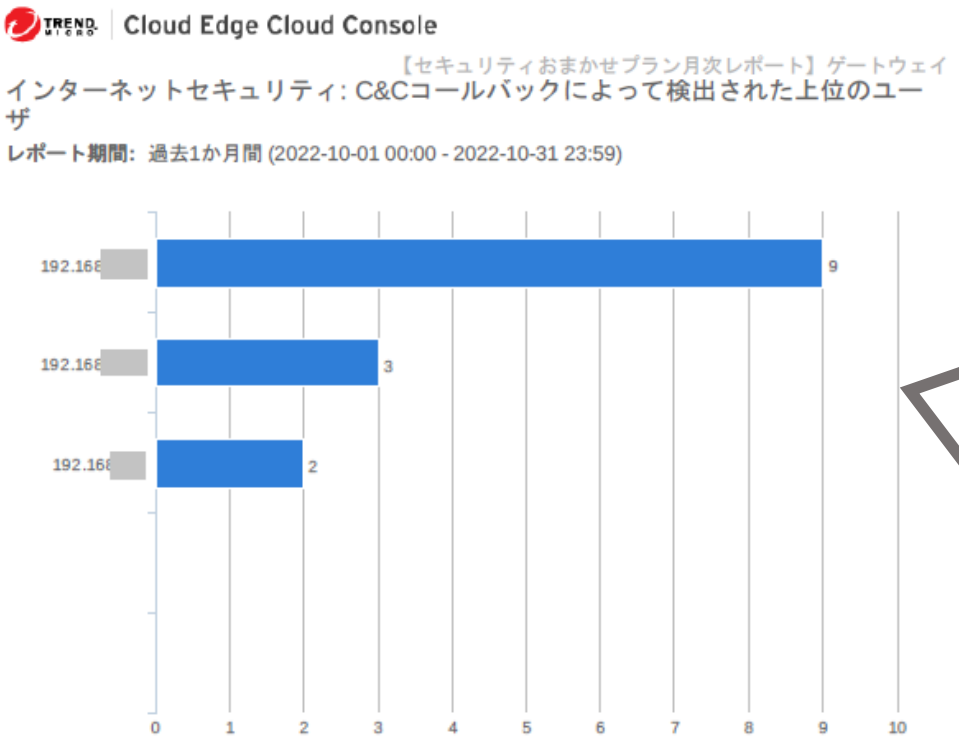


C&Cコールバック検知とは、遠隔操作やウイルスを送り込んでくるC&Cサーバへの通信を検知する機能です。

またC&Cサーバー通信の検知やプログラムの脆弱性を狙う攻撃などに対応します。

C&Cコールバックによって検出された上位のユーザ

- 本ページでは、不正プログラム侵入検知機能により、Cloud Edgeが1 ヶ月以内にC&Cサーバへ接続を検知・ブロックした結果を把握することができます。
- IPアドレスにより、どのユーザがC&Cサーバへの通信を実施しているかを把握することができます。



192.168.x.xxx	9
192.168.x.xxx	3
192.168.x.xxx	2

※グラフはイメージです。実際のレポートに記載の内容とは異なります。

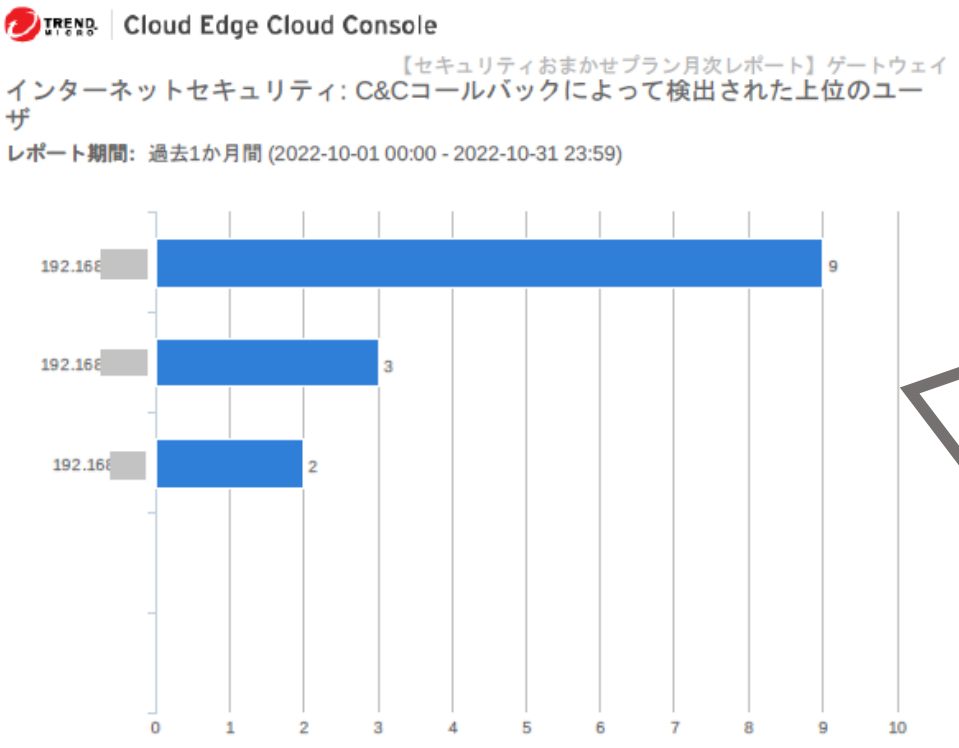


C&Cサーバーとは、外部から侵入して乗っ取ったコンピュータを踏み台にして制御したり命令を出したりする役割を担うサーバーコンピュータのことであり、通信が発生した場合、下記のような被害が想定されます。

１）特定のWebサイトへ負荷を与えるDDoS攻撃や、多くのメールを送信してフィッシング詐欺などを引き起こすスパムメール配信に加担させられる。
２）サーバーから、重要な機密情報を抜き取る。

C&Cコールバックによって検出された上位のユーザ

- 本ページでは、不正プログラム侵入検知機能により、Cloud Edgeが1 ヶ月以内にC&Cサーバへ接続を検知・ブロックした結果を把握することができます。
- IPアドレスにより、どのユーザがC&Cサーバへの通信を実施しているかを把握することができます。



192.168.x.xxx	9
192.168.x.xxx	3
192.168.x.xxx	2

※グラフはイメージです。実際のレポートに記載の内容とは異なります。



不正なプログラムなどによる別のウイルスのダウンロードや遠隔操作用の通信などが、御社の環境で検知しています。

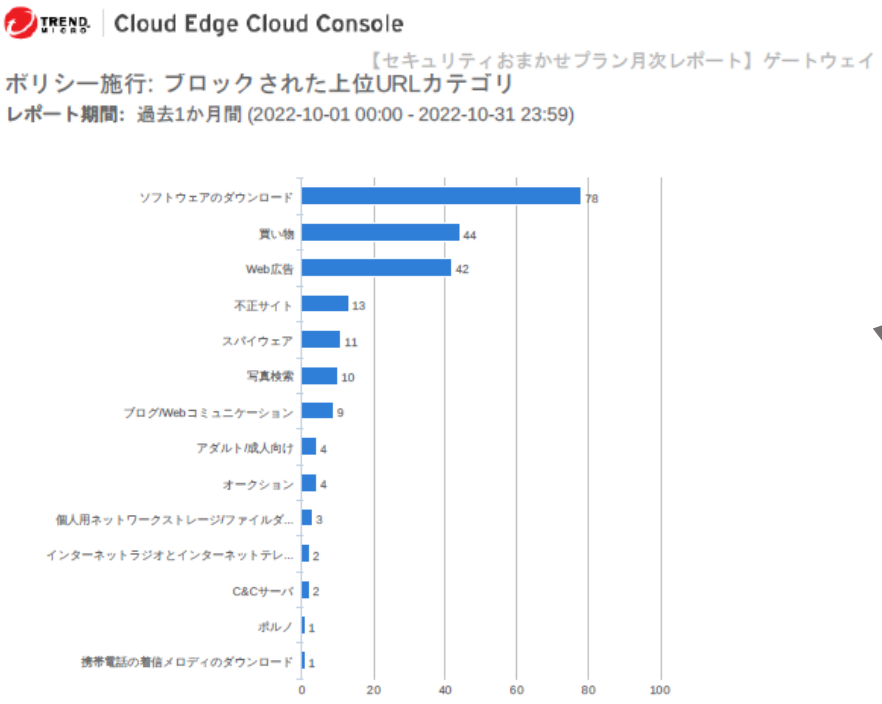
つまりウイルスに感染している可能性が非常に高いです。

Cloud Edgeがアクセスをとめていますが、なければ被害が出ていた可能性が高いです。検出された端末は感染している可能性が高く、即座にネットワークから切断することをお勧めします。

またウイルス対策ソフトを利用中の場合は最新パターンでのフルスキャンをお勧めいたします。

ブロックされた上位URLカテゴリ

- 本ページでは、URL指定によるアクセス制御機能によってアクセスがブロックされた回数の多いWebサイトのカテゴリー情報を得ることが出来ます。



ソフトウェアのダウンロード	78
買い物	44
Web広告	42

※グラフはイメージです。実際のレポートに記載の内容とは異なります。

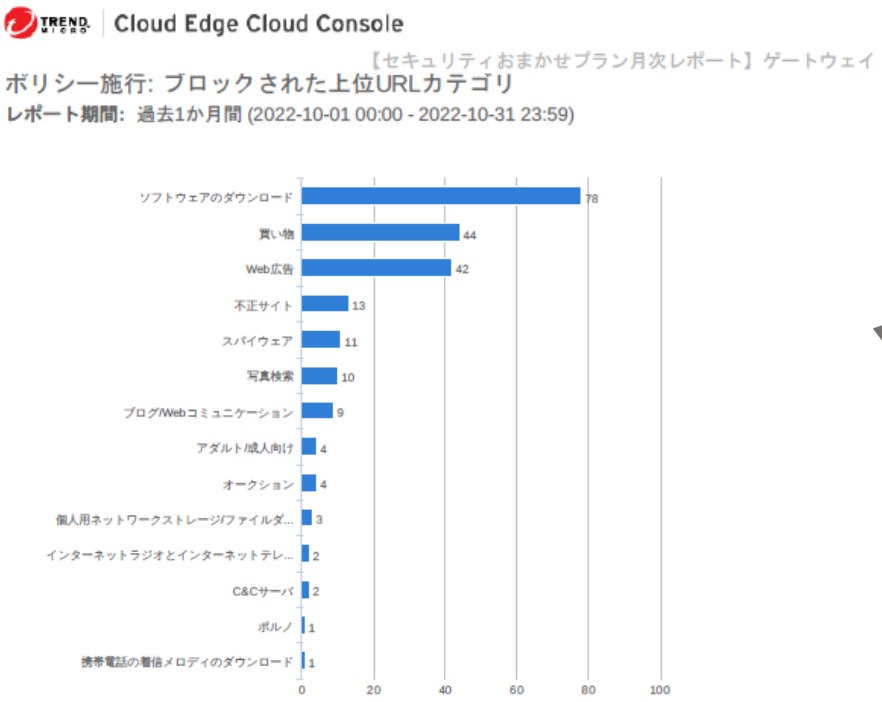
URL指定によるアクセス制御機能によってブロックされた上位のURLカテゴリーに関する情報です。

横軸　：検出した件数

縦軸：カテゴリー名

ブロックされた上位URLカテゴリ

- 本ページでは、URL指定によるアクセス制御機能によってアクセスがブロックされた回数の多いWebサイトのカテゴリー情報を得ることが出来ます。



ソフトウェアのダウンロード	78
買い物	44
Web広告	42
：	

※グラフはイメージです。実際のレポートに記載の内容とは異なります。

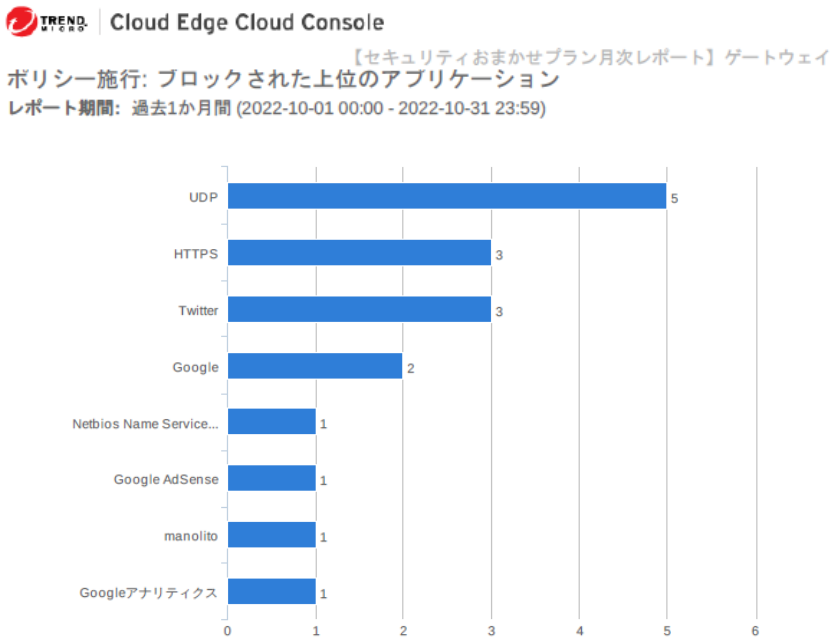


「C＆Cサーバ」や「不正サイト」といった不正なプログラムに感染するインターネットアクセスとともに、「アダルト」「ポルノ」といった業務に関係のないサイトへのアクセスや「個人用ネットワークストレージ」といった情報の持ち出しの可能性のあるサイトへのアクセスが客観的に確認できています。

業務で許可されていない、もしくは好ましくないカテゴリーがないかのご確認と、それらのカテゴリーのブロック/許可設定の実施をお勧めいたします。

ブロックされた上位のアプリケーション

- 本ページでは、アプリケーション利用制限機能によってブロックした回数の多いアプリケーション名や制限されているアプリケーションの利用を試みた回数の多いユーザを確認することが出来ます。
- 制限中のアプリケーションは、Cloud Edgeにより接続をブロックしているため、利用ができない状態にあります。



UDP	5
HTTPS	3
Twitter	3

※グラフはイメージです。実際のレポートに記載の内容とは異なります。

アプリケーション利用制限機能によってブロックされた上位のWebサイトに関する情報です。

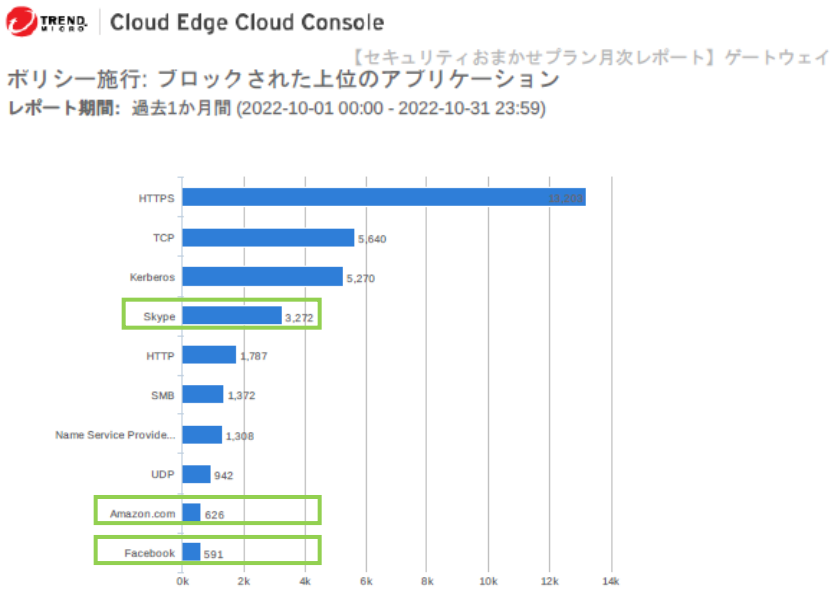
横軸：検出した件数

縦軸：利用を禁止しているアプリケーション・サービス・プロトコル

アプリケーション利用制限機能とは、アプリケーションの利用制限を行うことができる機能で、Cloud Edgeでは日本独自のアプリケーションを含む1,000以上のアプリケーションをサポートしています。

ブロックされた上位のアプリケーション

- 本ページでは、アプリケーション利用制限機能によってブロックした回数の多いアプリケーション名や制限されているアプリケーションの利用を試みた回数の多いユーザを確認することが出来ます。
- 制限中のアプリケーションは、Cloud Edgeにより接続をブロックしているため、利用ができない状態にあります。



HTTPS	13203
TCP	5640
Kerberos	5270

：

※グラフはイメージです。実際のレポートに記載の内容とは異なります。

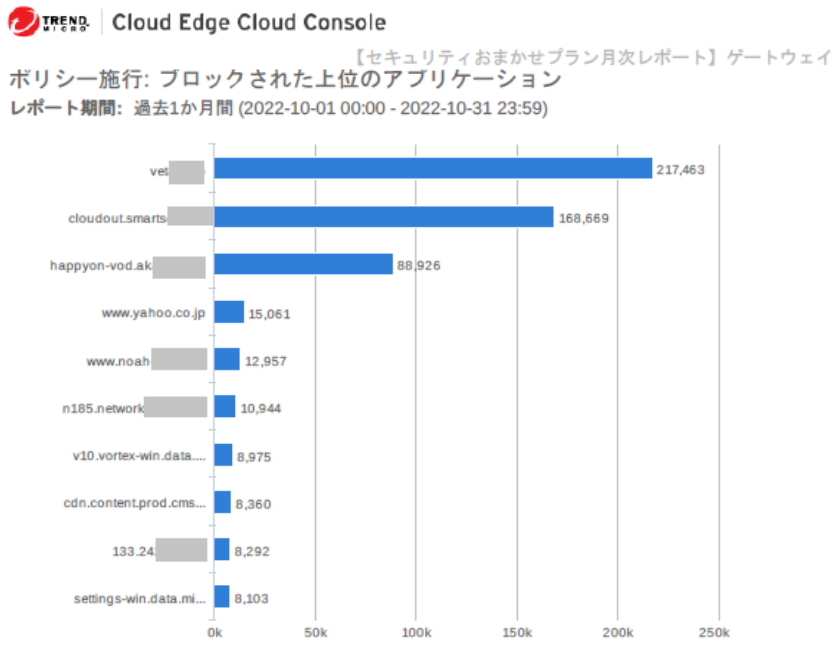


左記の図の場合、「Skype」や「amazon」「Facebook」のアプリケーションの通信が確認できています。

業務で許可されていない、もしくは好ましくないカテゴリーがないかのご確認と、それらのカテゴリーのブロック/許可設定の実施をお勧めいたします。

アクセスされた上位のサイト

- 本ページでは１ヶ月以内にCloud Edgeを経由してアクセスした上位10件のWebサイトのURLを確認することができます。
- これにより、業務中にCloud Edge配下の端末がどのようなサイトへアクセスする傾向があるか把握することができます。業務に支障があると判断されるサイトへの閲覧が多い場合、URL指定によるアクセス制御機能の設定を変更することにより、業務の効率化を図ることができます。



http://xxxxxx	217,463
http://xxxxxx	168,669
http://xxxxxx	88,926

⋮

※グラフはイメージです。実際のレポートに記載の内容とは異なります。



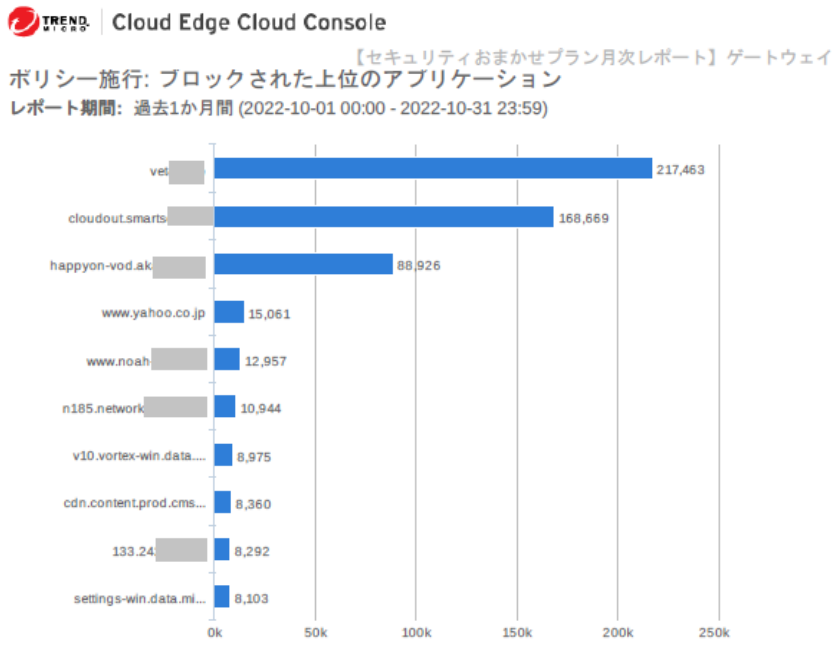
Cloud Edgeを経由してアクセスした上位10件のWeb サイトのURLの情報です。

横軸：検出した件数

縦軸：ポリシーによりブロックされたURL

アクセスされた上位のサイト

- 本ページでは１ヶ月以内にCloud Edgeを経由してアクセスした上位10件のWebサイトのURLを確認することができます。
- これにより、業務中にCloud Edge配下の端末がどのようなサイトへアクセスする傾向があるか把握することができます。業務に支障があると判断されるサイトへの閲覧が多い場合、URL指定によるアクセス制御機能の設定を変更することにより、業務の効率化を図ることができます。



http://xxxxxx	217,463
http://xxxxxx	168,669
http://xxxxxx	88,926

⋮

※グラフはイメージです。実際のレポートに記載の内容とは異なります。



御社でよくアクセスされているサイトとなります。

トレンドマイクロでは、アクセスされているサイトが何のサイトなのかを判断する、「Webサイト診断(Site Safety Center)」も合わせて提供しております。

https://global.sitesafety.trendmicro.com/