クラウド型セキュリティ対策サービス

Cloud Edge あんしんプラス

月次レポート解説書

第 1.0 版

日本事務器株式会社

改版履歴

版数	日付	変更内容
1.0	2016/03/07	新規作成

目次

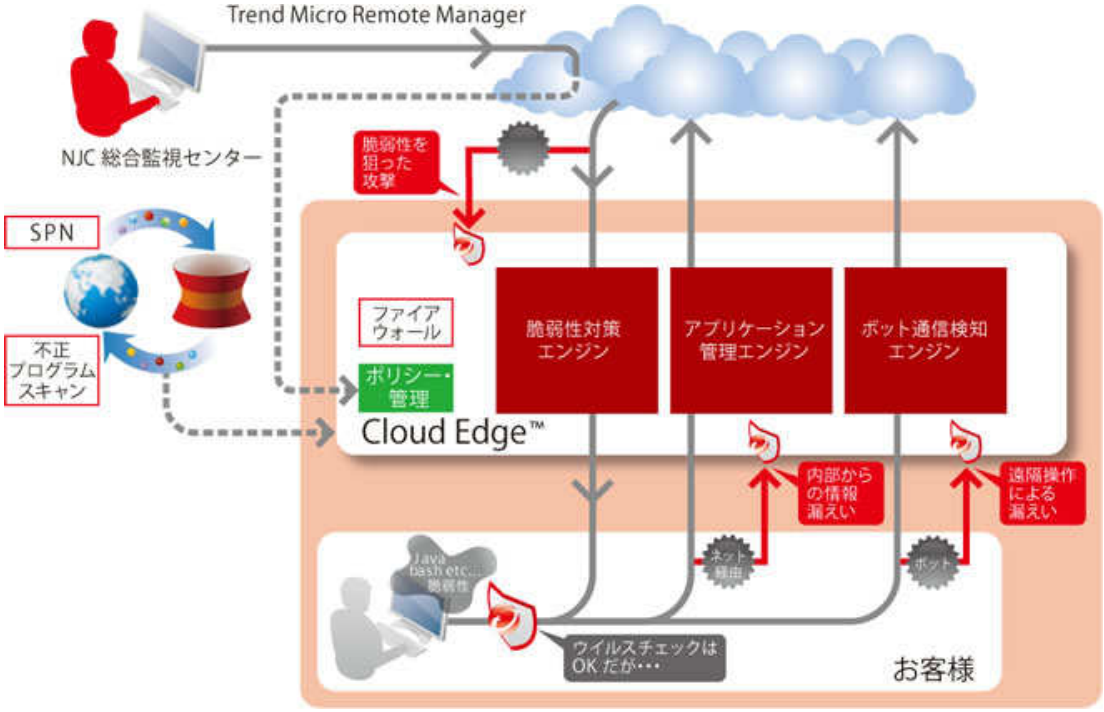
1. サービス概要

本サービスの概要について説明いたします。

1.1. Cloud Edge あんしんプラスとは

本サービスは、トレンドマイクロ株式会社クラウド型セキュリティ BOX「Cloud Edge」をベースとした、ゲートウェイセキュリティマネージドサービスです。「脆弱性をついた攻撃」や「遠隔操作」、「情報漏えい」等、企業や組織を狙った攻撃が高度化・多様化する新しい課題に対応できるゲートウェイセキュリティソリューションです。
また、本サービスでは、セキュリティの各設定、インシデント監視、バージョンやファームウェアのアップデートからレポートなど、面倒な管理を運営者の総合監視センターで実施いたします。初期導入時や運用時にお客様が行う作業を最小限に抑え、セキュリティ対策を効率的に管理・運用することができます。

「サービスの全体イメージ図」



2. 月次レポート解説

本サービスで提供される月次レポートの各項目の内容について説明します。

2.1. VBBSS がインストールされているクライアントの概要

1. VBBSSがインストールされているクライアントの概要			
デスクトップクライアント	モバイルデバイスクライアント	シート	利用率
			0

※現在、レポートでは結果表示されません。

2.2. 接続の概要

2. 接続の概要	
デバイス名	接続
CE50_RD	1266
合計	1266

* Cloud Edgeデバイスがルーティングモードの場合、接続数が正確でないことがあります。

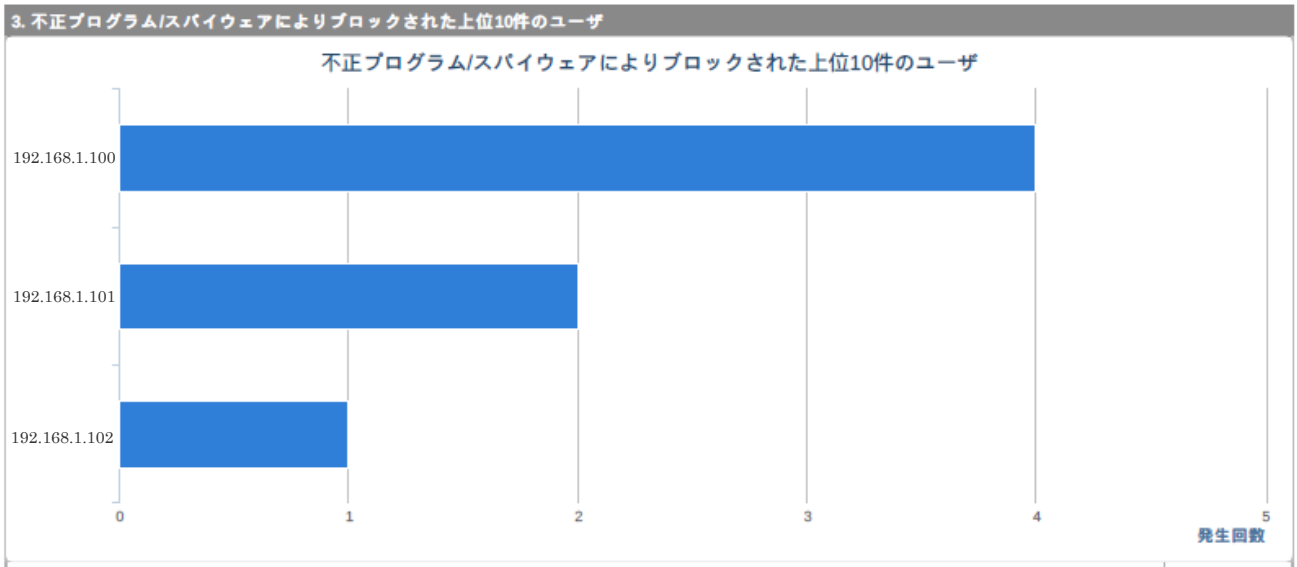
Cloud Edge が認識した社内ネットワーク上の MAC アドレスの数です。

・デバイス名：出荷時に設定された CloudEdge 自身の名前

・接続：MAC アドレスの数

※社内ネットワーク（CloudEdge 配下）に存在する端末数を把握するための目安情報となります。

2.3. 不正プログラム/スパイウェアによりブロックされた上位 10 件のユーザ



ユーザ	発生回数
192.168.1.100	4
192.168.1.101	2
192.168.1.102	1

ユーザが、CloudEdge を経由して、受信したメールの添付ファイルや Web サイトからダウンロードしたファイル等が、不正プログラムやスパイウェア（以下、ウイルス）であることを、Cloud Console が検知しブロック（削除）したユーザごとの結果です。

・ユーザ：表記されている IP アドレスを持つ端末

・発生回数：ブロックしたウイルスの数

尚、本レポートでは、発生回数が多い上位 10 件までのユーザとなります。

その他のユーザおよび詳細な情報については、Cloud Edge Cloud Console（Web 管理コンソール）にて確認できます。

※不正プログラム/スパウェア対策機能は、以下プロトコルをサポートしています。

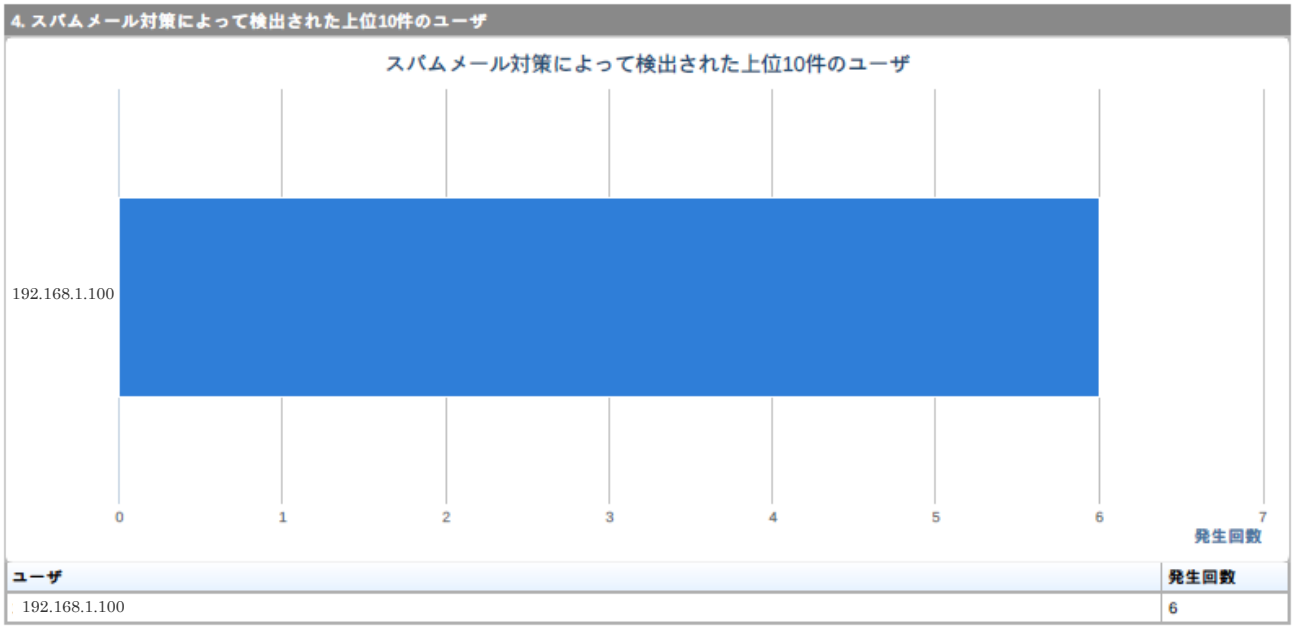
・HTTP/HTTPS

・SMTP

・POP

・FTP

2.4. スパムメール対策によって検出された上位 10 件のユーザ



ユーザ	発生回数
192.168.1.100	6

ユーザが、CloudEdge を経由したメールの送受信において、Cloud Console がスパムメールと判断したユーザごとのメール
の数の結果です。

・ユーザ：表記されている IP アドレスを持つ端末

・発生回数：検知したスパムメールの数

尚、本レポートでは、発生回数が多い上位 10 件までのユーザとなります。

その他のユーザおよび詳細な情報については、Cloud Edge Cloud Console（Web 管理コンソール）にて確認できます。

CloudEdge では、以下３つの機能でスパムメールと判断いたします。

■スパムメール検索エンジン

CloudEdge に搭載されているスパムメール検索エンジンにてスパムメールを検知します。

※SMTP/POP3 に対応

■Email Reputation サービス(ERS)機能

トレンドマイクロ社スパムメール送信元 IP アドレスデータベースを参照して、受信メールメッセージの IP アドレスを検証してスパムメールの送信元を特定し、該当する IP アドレスからのメールを検知します。

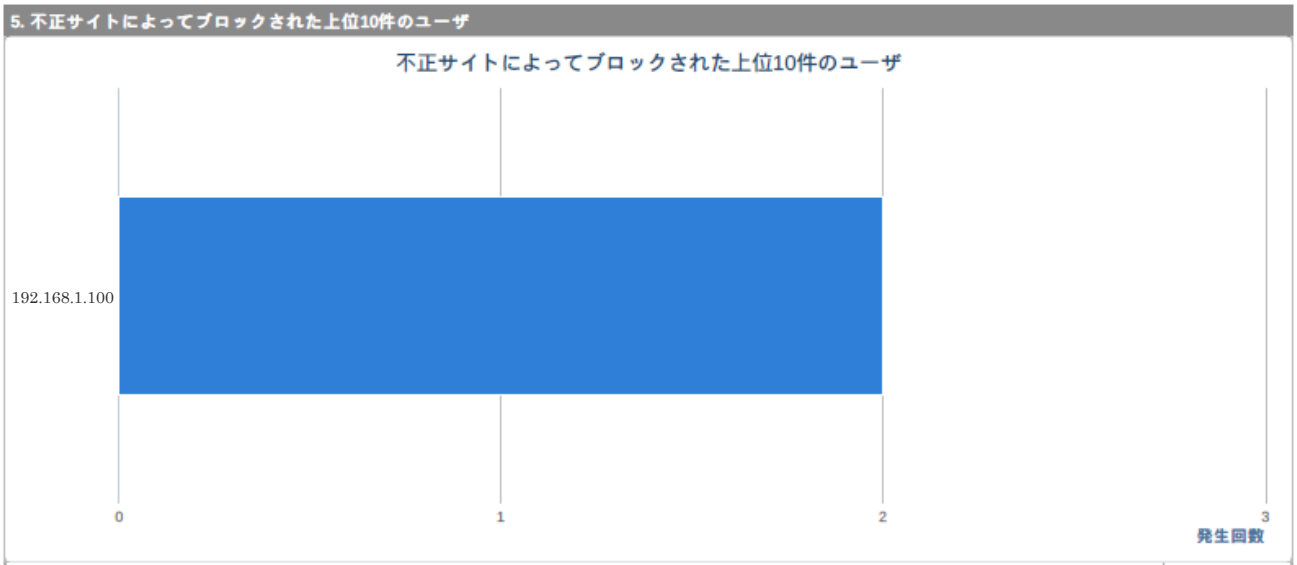
※SMTP プロトコル（パブリック IP）のみ対応

■コンテンツフィルタ機能

任意に設定したキーワードやメッセージサイズによりメールを検知します。

※SMTP/POP3 に対応

2.5. 不正サイトによってブロックされた上位 10 件のユーザ



ユーザ	発生回数
192.168.1.100	2

ユーザが、CloudEdge を経由して Web サイトにアクセスした際に、トレンドマイクロ Web セキュリティデータベース（Web レピュテーションサービス（WRS））で安全性を確認し、不正サイトへの接続であることを検知、ブロックしたユーザごとの Web アクセスの数の結果です。

・ユーザ：表記されている IP アドレスを持つ端末

・発生回数：検知（ブロック）した不正サイトへのアクセス回数

尚、本レポートでは、発生回数が多い上位 10 件までのユーザとなります。

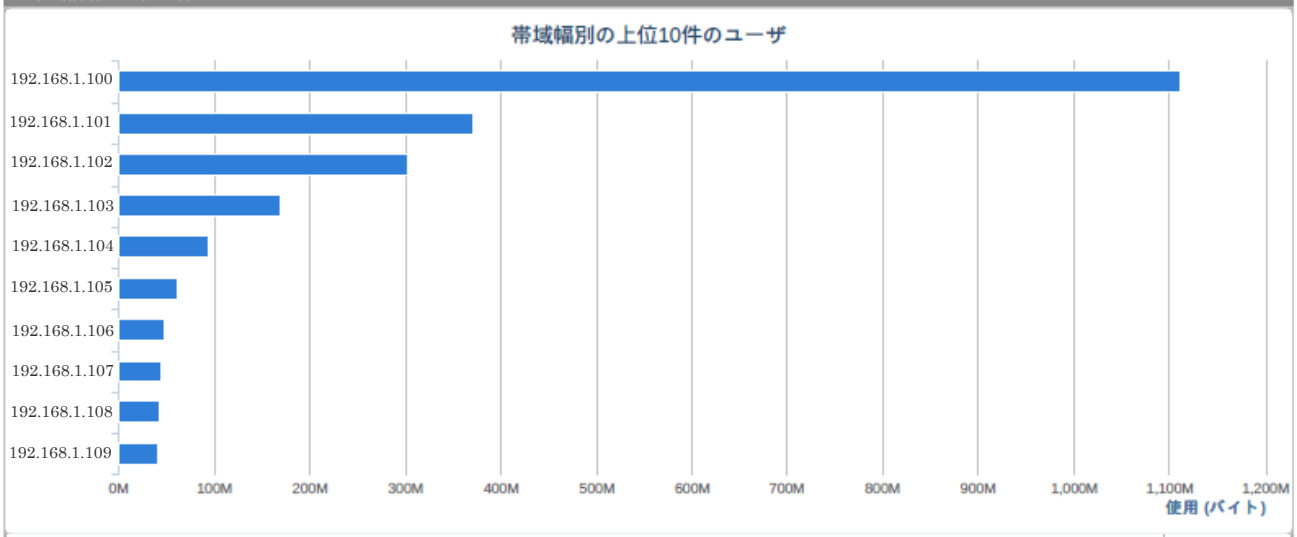
その他のユーザおよび詳細な情報については、Cloud Edge Cloud Console（Web 管理コンソール）にて確認できます。

※Web レピュテーションサービス（WRS）機能

ユーザが Web サイトにアクセスするなどの通信が発生する際に Trend Micro Smart Protection Network に自動的に問い合わせを行い、接続先ドメイン、Web サイト、Web ページが不正な場合にはアクセス自体をブロックすることによって不正プログラムによる感染、フィッシング詐欺による被害を防ぐことができます。

2.6. 帯域幅別の上位 10 件のユーザ

6. 帯域幅別の上位10件のユーザ



ユーザ	使用 (バイト)
192.168.1.100	1112726633
192.168.1.101	369662980
192.168.1.102	303659689
192.168.1.103	169487731
192.168.1.104	94735259
192.168.1.105	61826639
192.168.1.106	48622558
192.168.1.107	44240584
192.168.1.108	41885463
192.168.1.109	40958084

ユーザごとの、CloudEdge を経由したインターネットへのデータ通信量です。ネットワークの輻湊（ふくそう）を緩和する

ため、不要なトラフィックの把握や重要なトラフィック/サービスへの適切な帯域幅の割り当てなど、セキュリティリスクを減らし安定したネットワーク環境構築の参考データとなります。

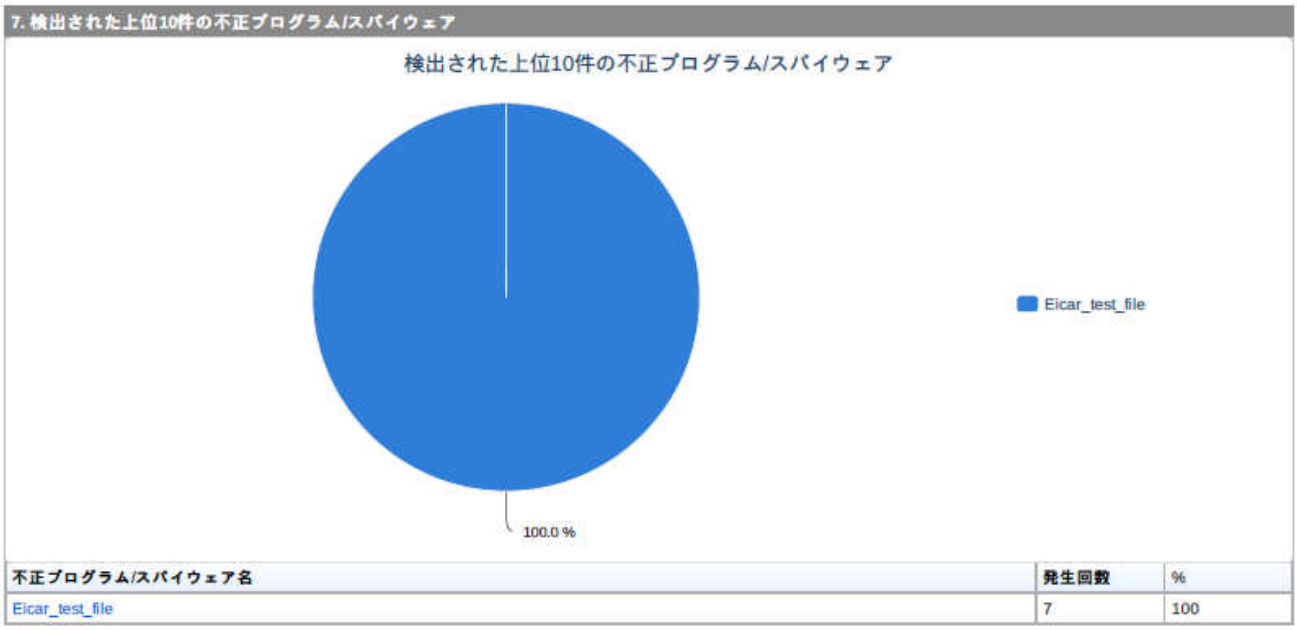
・ユーザ：表記されている IP アドレスを持つ端末

・使用（バイト）：データ通通信量の合計

尚、本レポートでは、発生回数が多い上位 10 件までのユーザとなります。

その他のユーザおよび詳細な情報については、Cloud Edge Cloud Console（Web 管理コンソール）にて確認できます。

2.7. 検出された上位 10 件の不正プログラム/スパイウェア



不正プログラム/スパイウェア名	発生回数	%
Eicar_test_file	7	100

CloudEdge で検出（およびブロック）された不正プログラム/スパイウェア名ごとの検出結果です。

・不正プログラム/スパイウェア名：検出した不正プログラム/スパイウェアの名前（検出名）

・発生回数：検知した不正プログラム/スパイウェアの数

尚、本レポートでは、発生回数が多い上位 10 件までのユーザとなります。

その他のユーザおよび詳細な情報については、Cloud Edge Cloud Console（Web 管理コンソール）にて確認できます。

（参考）

以下サイトで、不正プログラム/スパイウェア名（検出名）より、どのような脅威があるか、また対処方法についてなど確認することができます。

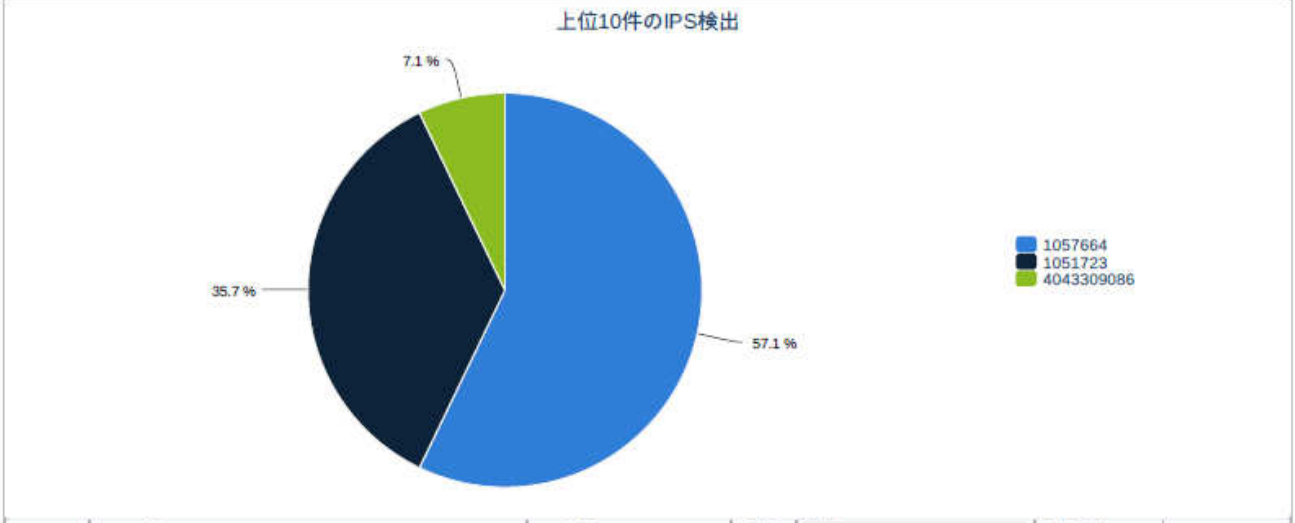
・トレンドマイクロ社セキュリティ情報ページ

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

⇒セキュリティデータベース

2.8. 上位 10 件の IPS 検出

8. 上位10件のIPS検出



ルールID	ルール名	CVE番号	重大度		発生回数	%
1057664	WEB Nginx ngx_http_parse_chunked Buffer Overflow -1 (CVE-2013-2028)	CVE-2013-2028; CVE-2013-4322	高		16	57.14
1051723	VIRUS Eicar test string		重大		10	35.71
4043309086	ICMP SMURF		高		2	7.14

※IPS（Intrusion prevention system（侵入防御システム））
OS やアプリケーションに残る脆弱性を付いた攻撃などの不正アクセスを、シグネチャ（不正な侵入データが定義されたルール）と照合して、悪意あるトラフィックを検出して防御（通信を遮断）するシステム。

CloudEdge を経由するデータ通信を、約 6500 のシグネチャと照合して、不正な通信を検知および防御（ブロック）した結果です。

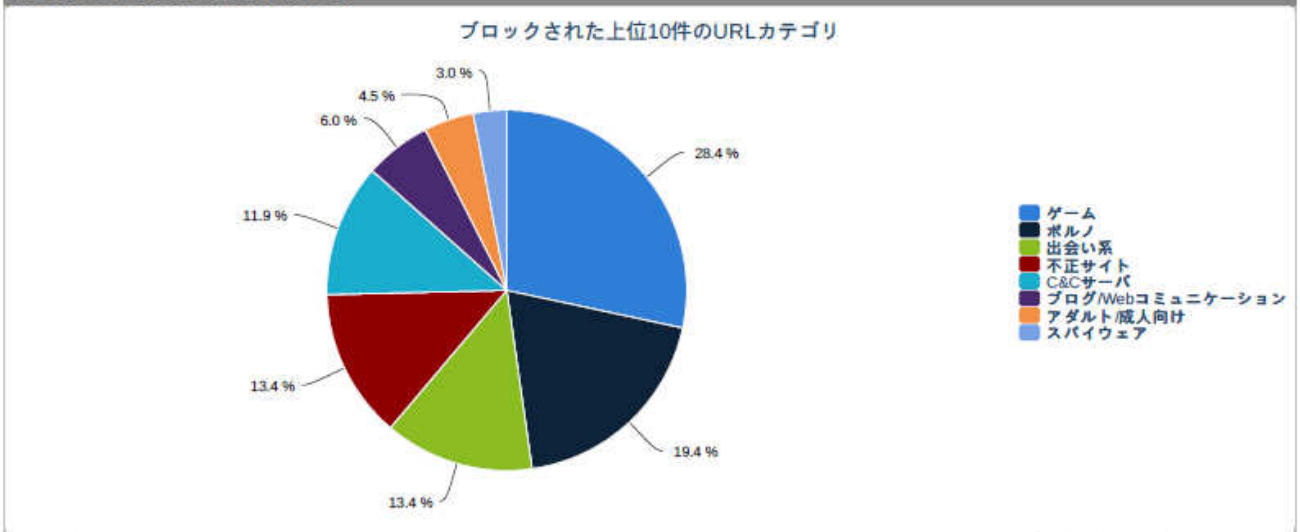
・ルール ID：各シグネチャの ID
・ルール名：各シグネチャの名前
・CVE 番号：共通脆弱性識別子 CVE(Common Vulnerabilities and Exposures)は、OS やアプリケーションなど個別製品中の脆弱性を対象として、米国政府の支援を受けた非営利団体の MITRE 社が採番している識別子です。
個別製品中の脆弱性に一意の識別番号「CVE 識別番号(CVE-ID)」を付与することにより、組織 A の発行する脆弱性対策情報と、組織 X の発行する脆弱性対策情報とが同じ脆弱性に関する対策情報であることを判断したり、対策情報同士の相互参照や関連付けに利用したりできます。
検出したルールがどのような脆弱性かどうかについては、CVE 番号より、以下サイト等で検索いたします。
【脆弱性対策情報データベース検索】
http://jvndb.jvn.jp/search/index.php?mode=_vulnerability_search_IA_VulnSearch&lang=ja
・重大度：
・発生回数：防御した通信の数

尚、本レポートでは、発生回数が多い上位 10 件までのユーザとなります。
その他のユーザおよび詳細な情報については、Cloud Edge Cloud Console（Web 管理コンソール）にて確認できます。

※Cloud Edge はクライアント/サーバ側に実際に脆弱性があるかどうかを判断しているわけではなく、通信するパケットの中身をみているため実際は脆弱性がない場合もありえます。また、実際の攻撃ではなく、通常の http リクエスト/レスポンスが攻撃パターンと合致し IPS で検知されるというケースも起こりえます。

2.9. ブロックされた上位 10 件の URL カテゴリ

9. ブロックされた上位10件のURLカテゴリ



カテゴリ	発生回数	%
ゲーム	19	28.36
ポルノ	13	19.4
出会い系	9	13.43
不正サイト	9	13.43
C&Cサーバ	8	11.94
ブログ/Webコミュニケーション	4	5.97
アダルト/成人向け	3	4.48
スパイウェア	2	2.99

CloudEdge を経由した Web サイトのアクセスにおいて、ポリシー設定にてブロック設定した URL カテゴリに含まれた Web サイトに、実際にアクセスしブロックした結果です。

・カテゴリ：インターネット上の Web サイトの URL を、分類やジャンル別に仕分けしたグループ

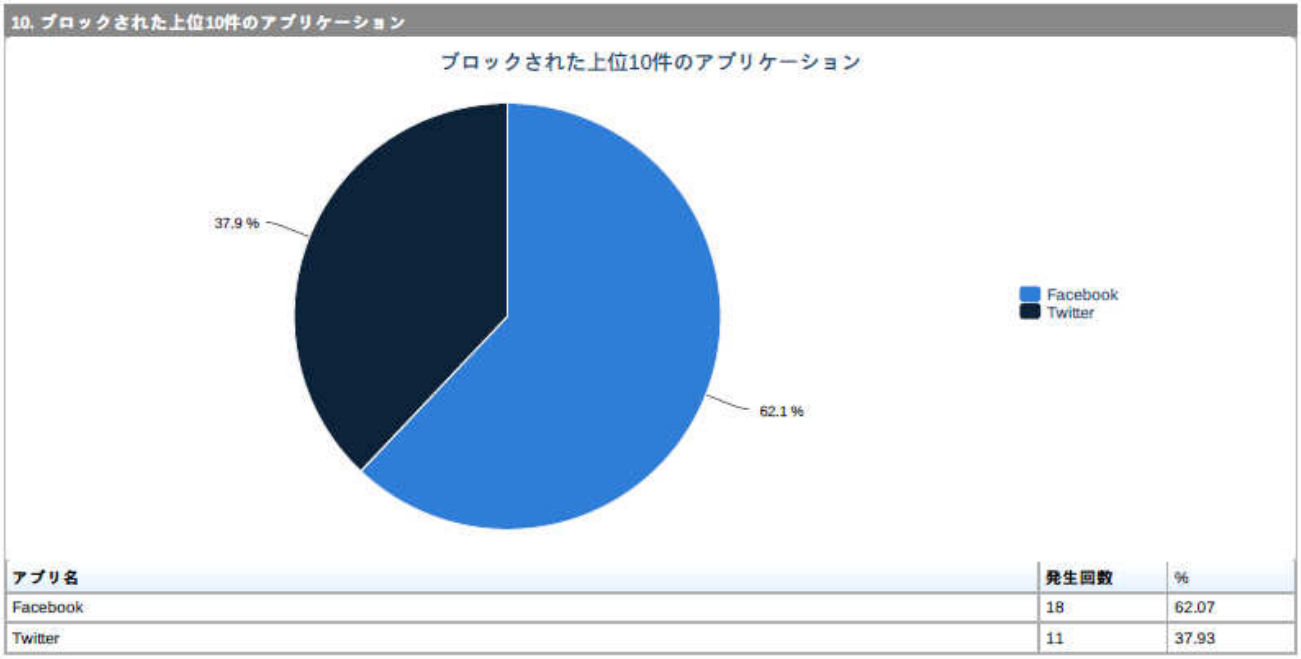
※インターネット上のすべての URL が含まれているわけではありません。

・発生回数：Web アクセスをブロックした数

尚、本レポートでは、発生回数が多い上位 10 件までのユーザとなります。

その他のユーザおよび詳細な情報については、Cloud Edge Cloud Console（Web 管理コンソール）にて確認できます。

2.10. ブロックされた上位 10 件のアプリケーション



アプリ名	発生回数	%
Facebook	18	62.07
Twitter	11	37.93

CloudEdge を経由した HTTP/HTTPS 通信を利用したアプリケーション等 に対して、ポリシー設定にてブロック設定したアプ

リケーションに、実際にアクセスしブロックした結果です。

・アプリ名：実際にアクセスしたアプリケーション名

・発生回数：アクセスをブロックした数

尚、本レポートでは、発生回数が多い上位 10 件までのユーザとなります。

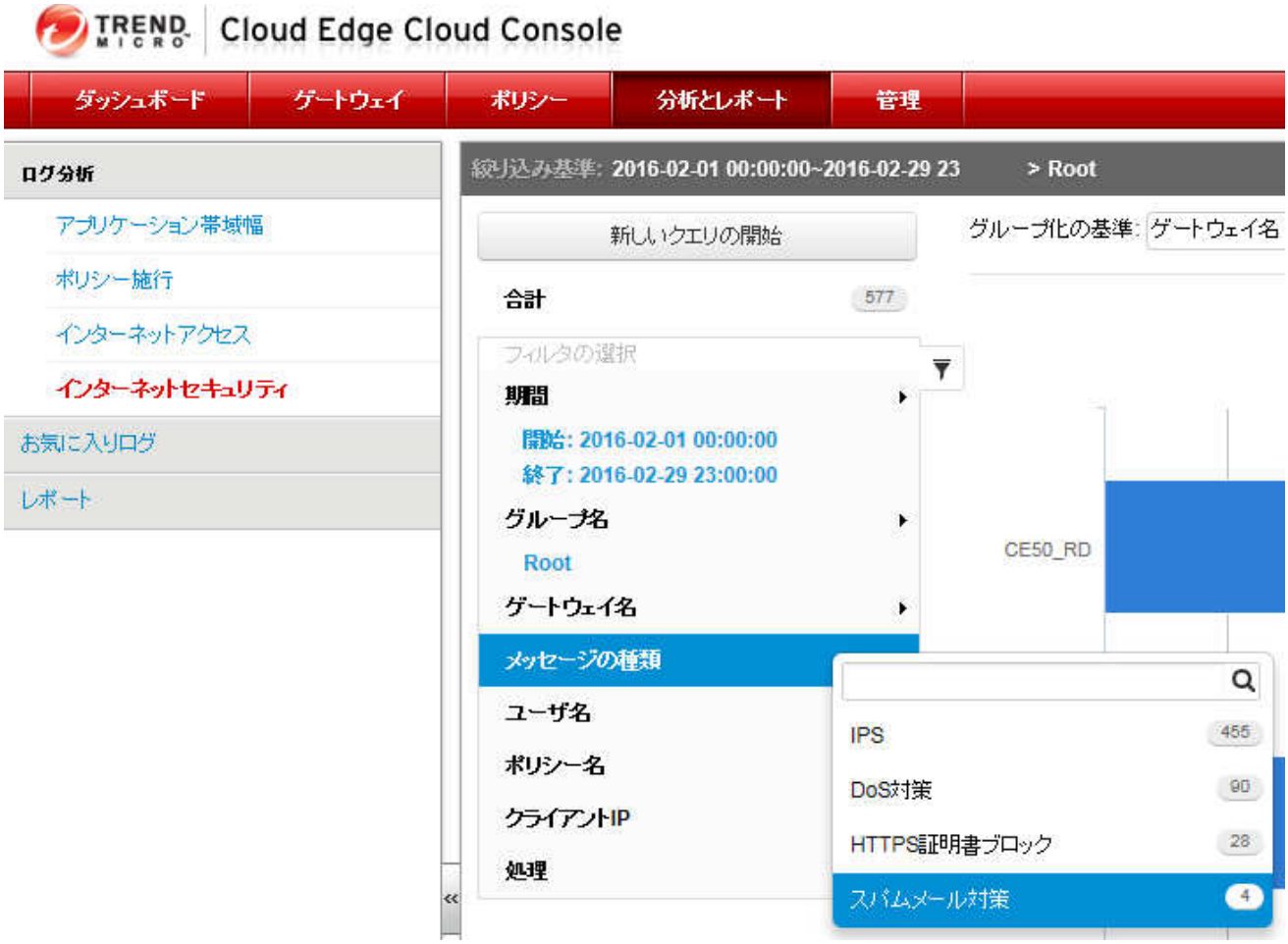
その他のユーザおよび詳細な情報については、Cloud Edge Cloud Console（Web 管理コンソール）にて確認できます。

3. （参考）Cloud Edge Cloud Console「分析とレポート」概要

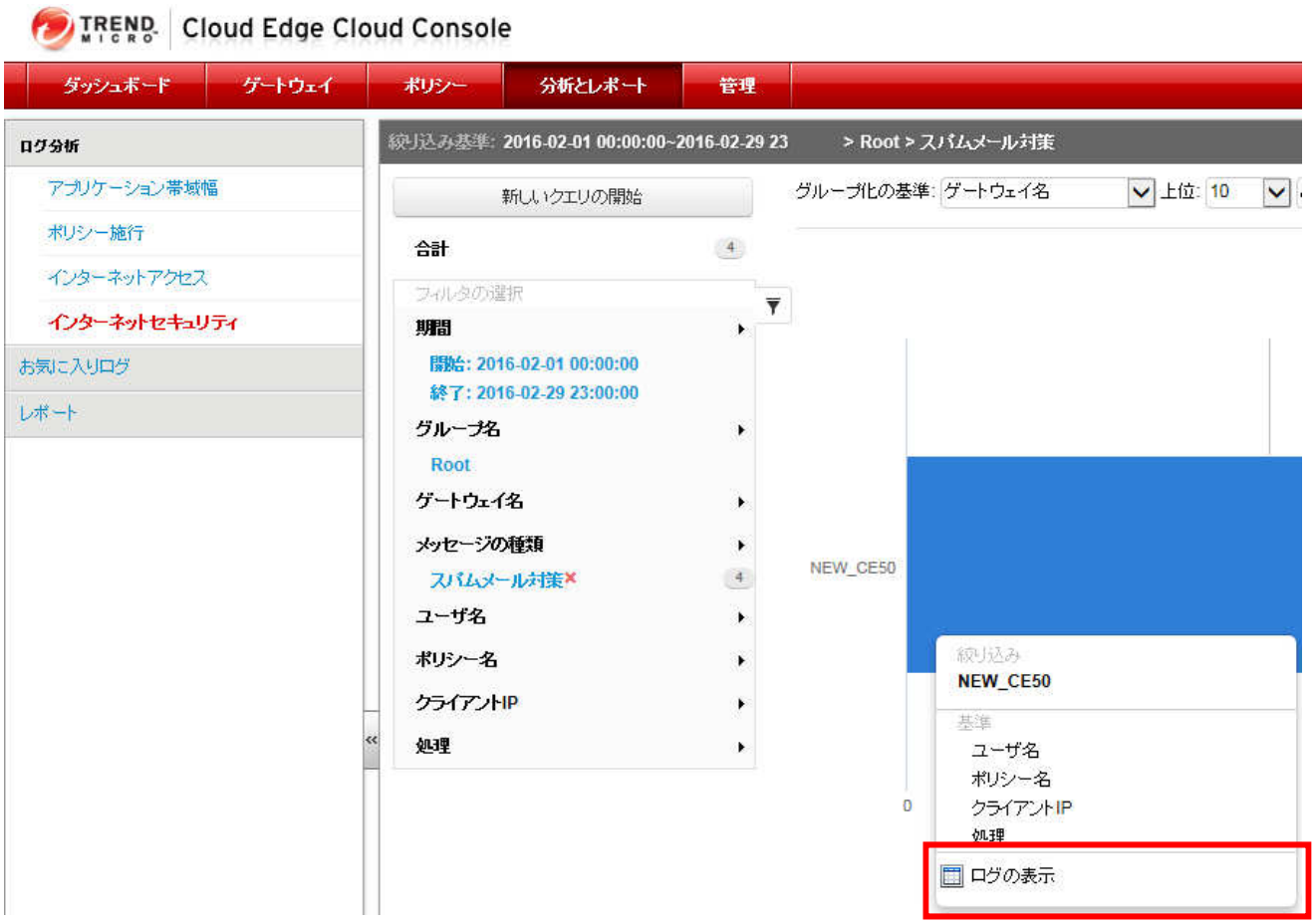
月次レポートの上位 10 件以下の状況や、その他詳細な情報が確認できる Cloud Edge Cloud Console での「分析とレポート」の一例を説明します。

3.1. スパムメール対策の詳細ログについて

Cloud Edge Cloud Console にログインし、『分析とレポート』→『インターネットセキュリティ』→『期間（ログ抽出期間を指定）』→『メッセージの種類』→『スパムメール対策』を選択



『グラフ選択』→『ログの表示』を選択



全ての検出結果および詳細情報が表示されます。

時間	メッセージの種類	クライアントIP	サーバIP	処理	メールの送信者	メールの受信者	メールの件名
2016-02-25 11:36:06 JST+0900	スパムメール対策	172.16.16.162	172.22.67.174	タグ	makinom@makinom.com	makinom2	[スパムメール]test
2016-02-25 11:20:10 JST+0900	スパムメール対策	172.16.16.162	172.22.67.174	タグ	makinom@makinom.com	makinom3	[スパムメール]てすと11
2016-02-25 11:13:06 JST+0900	スパムメール対策	172.16.16.162	172.22.67.174	タグ	makinom@makinom.com	makinom2	[スパムメール]test10
2016-02-25 11:09:00 JST+0900	スパムメール対策	172.16.16.162	172.22.67.174	タグ	makinom@makinom.com	makinom2	[スパムメール]てすと9

クラウド型セキュリティ対策サービス

Cloud Edge あんしんプラス

月次レポート解説書　第 1.0 版

発行日　：　2016 年 03 月 07 日

発行元　：　日本事務器株式会社