【kUTMみまもりサポート】
レポート解説書

株式会社KDDIウェブコミュニケーションズ

サマリレポート編

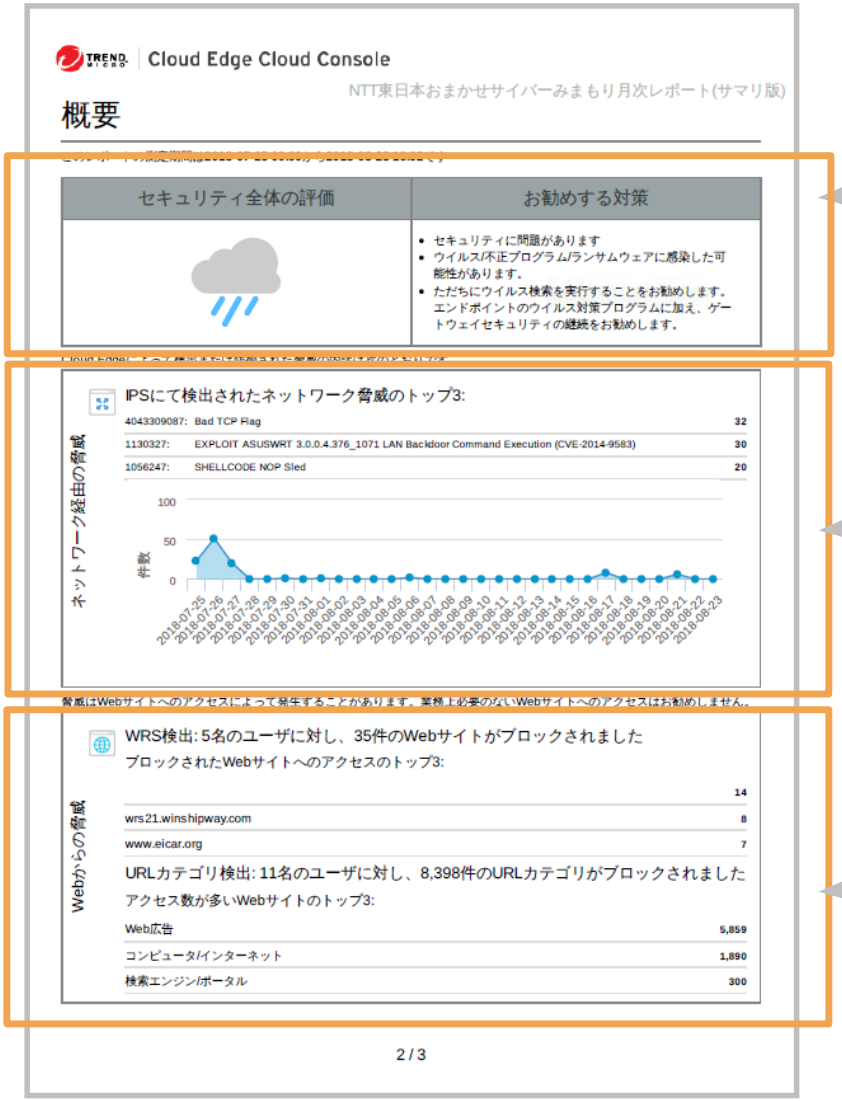
サマリレポート概要

- 月１回(月初)メール送付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。
- サマリレポートは以下の表に記載する６項目から構成されています。
- サマリ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。

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(Webサイトアクセスブロック)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。
メール経由の状況	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。
その他の脅威	上記以外のランサムウェア検出機能、不正プログラム検出機能等セキュリティ機能等により検出された脅威の数を把握することができます。
ネットワーク使用状況	専用BOX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。



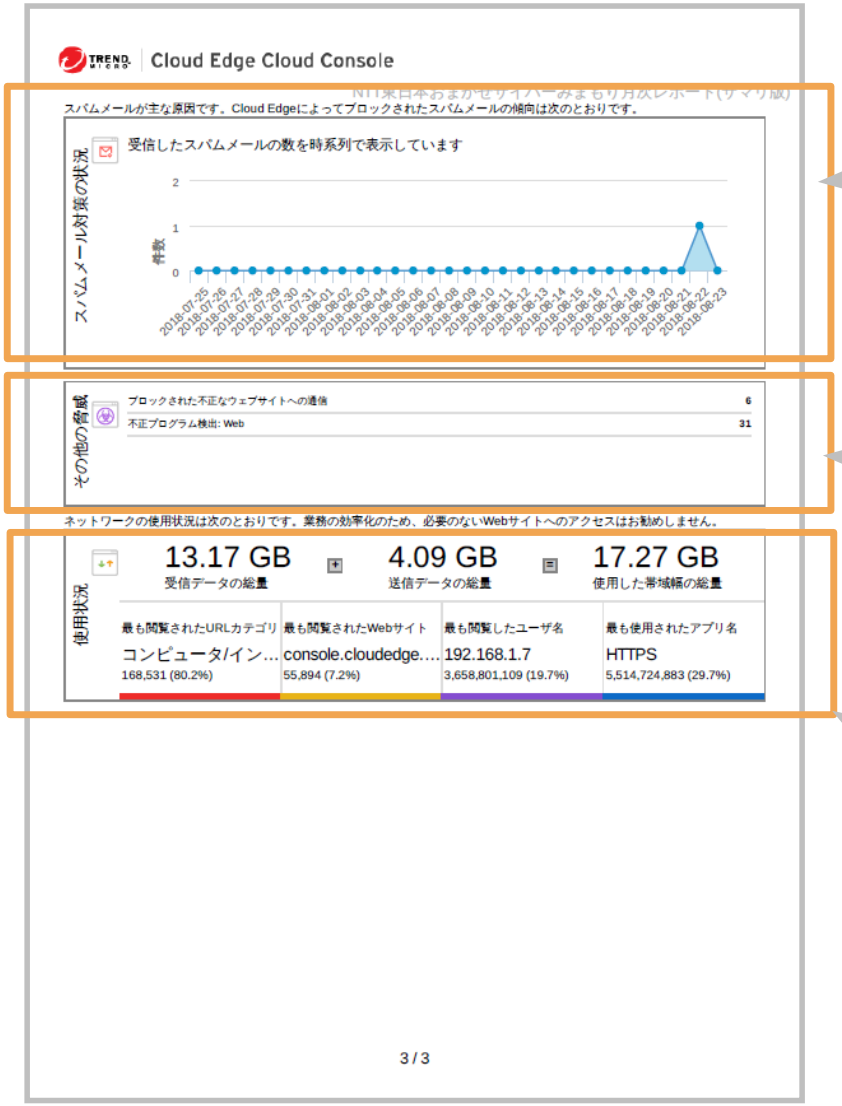
晴れマーク ☀・曇りマーク ☁・雨マーク 🌧 の３段階があり、曇りマークや雨マークのお客様は、期間中に何らかのセキュリティリスクを検出した形跡があります。晴れマークのお客様も、当該期間中は脅威の検出はありませんでしたが、油断すると次回は曇りマークや雨マークに変化する可能性があるため、セキュリティ対策を継続する必要があります。

- 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。
- 検出がある場合は、該当のシステムを最新の状態にアップデートし、修正プログラムを適用する事が必要となります。
- 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。

- 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(悪意ある第三者により改ざんされたサイト等）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、専用BOX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。

サマリレポート詳細

□ 本ページでは、「**メール経由の脅威**」、「**その他の脅威検知状況**」、「**ネットワーク使用状況**」に関する情報を把握することができます。


Cloud Edge Cloud Console

スパムメールが主な原因です。Cloud Edgeによってブロックされたスパムメールの傾向は次のとおりです。

スパムメール対策の状況

受信したスパムメールの数を時系列で表示しています

件数

その他の脅威

ブロックされた不正なウェブサイトへの通信 6

不正プログラム検出: Web 31

ネットワークの使用状況は次のとおりです。業務の効率化のため、必要のないWebサイトへのアクセスはお勧めしません。

使用状況

13.17 GB 受信データの総量

4.09 GB 送信データの総量

17.27 GB 使用した帯域幅の総量

最も閲覧されたURLカテゴリ	最も閲覧されたWebサイト	最も閲覧したユーザ名	最も使用されたアプリ名
コンピュータ/イン…	console.cloudedge.…	192.168.1.7	HTTPS
168,531 (80.2%)	55,894 (7.2%)	3,658,801,109 (19.7%)	5,514,724,883 (29.7%)

3 / 3

- 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。
- 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。
- 本ページ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。

- 「ブロックされた不正なウェブサイトへの通信」が検出されている場合はC&Cサーバへの通信を検出している場合があります。月次レポートの本編を確認してください。
- C&Cサーバは侵入して乗っ取ったコンピュータを踏み台にし、制御する役割を担うコンピュータの事で、検出された場合は早期対応が必要です。

- 専用BOX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。

月次レポート編

月次レポートの内容

- 本サービスでは、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。

・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/スパイウェアの検出の傾向
- 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）
- 不正サイトによってブロックされた上位のユーザ
- 不正プログラムによって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
- ランサムウェアによって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）
- ランサムウェアによってブロックされた上位のユーザ(メールチャネル)
- ランサムウェアによってブロックされた上位のユーザ(ネットワークチャネル)
- スパムメール対策によって検出された上位のユーザ
- メールの機械学習型検索によって検出された上位のユーザ
- C&Cコールバックによって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

専用BOX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

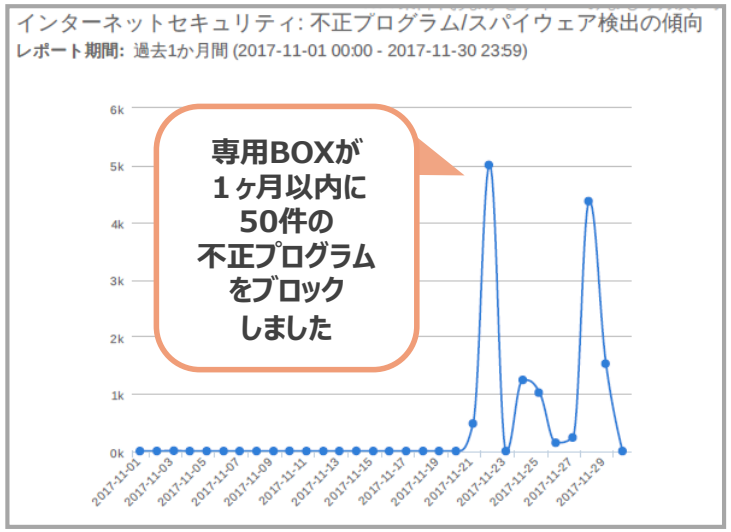
・ インターネットアクセス

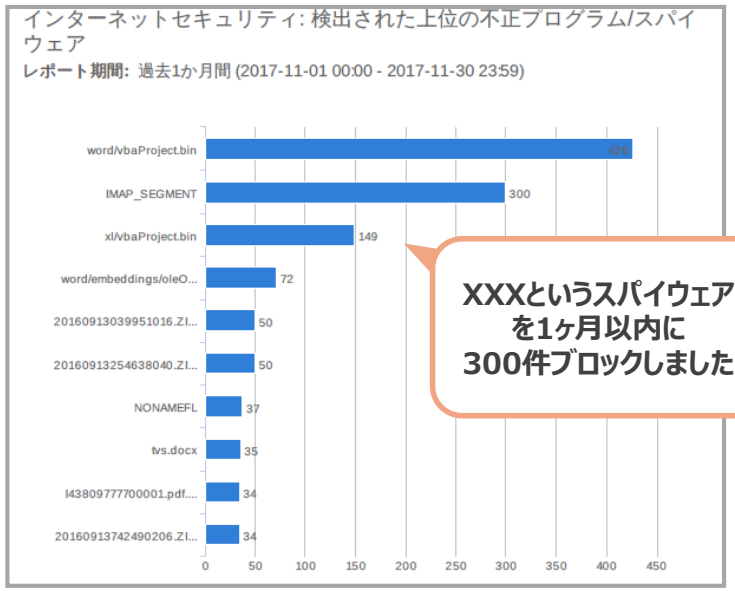
専用BOX配下の端末からのインターネット利用状況に関する情報

- 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

不正プログラム/スパイウェアに関する情報

- 本ページでは、設置した専用BOX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)**と、**検出数が多い10件の不正プログラム/スパイウェア名**を得ることができます。
- 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。





■ユーザが専用BOX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

■専用BOX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

不正プログラム/スパイウェアに関する情報

□　本ページでは、**各不正プログラム/スパイウェアを検出した履歴を日付別**に把握することができます。

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/スパイウェア (日付別)

レポート期間: 過去1か月間 (2017-11-01 00:00 - 2017-11-30 23:59)

17/11/02	
filename-3.doc	1
new document-69.doc	1
919294976.doc	1
総数	**3**
17/11/03	
919294976.doc	3
Invoice INV0000935.doc	3
4890_Invoice.doc	3
8682_Invoice.doc	3
81849826.doc	2
34489940.doc	2
19003187.doc	2
Invoice INV0000760.doc	2
総数	**20**
17/11/05	
001_1938.doc	1
総数	**1**
17/11/11	
word/embeddings/oleObject1.bin	1
総数	**1**

専用BOXが
●月●日に「XXX」という不正プログラムを
1件検出しました

■ **不正プログラム/スパイウェアの日付別の検出件数**です。

■ **セキュリティデータベース**

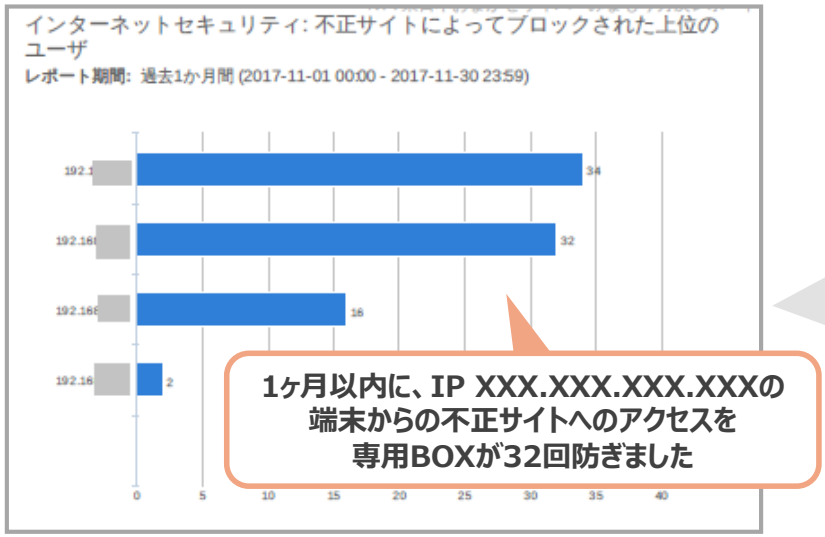
「**トレンドマイクロ社 セキュリティデータベース**」より、不正プログラム/スパイウェア名を検索すると、**感染経路や対処法等の情報を確認**することができます。

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

https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/

不正サイトへのアクセスに関する情報

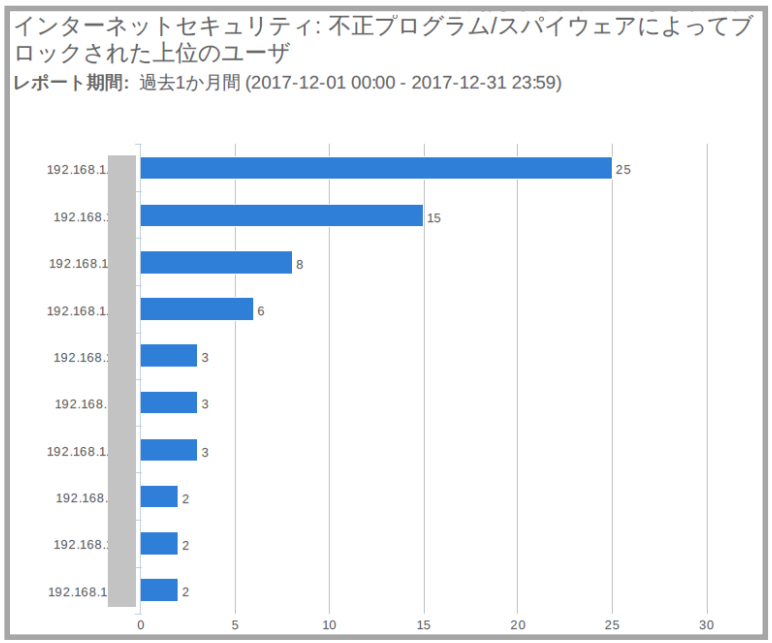
- 本ページでは、Webサイトアクセスブロック機能により、専用BOXが1ヶ月以内に**不正サイトへの接続**を検知・ブロックした結果を把握することができます。
- **IPアドレスの情報から、どのユーザが不正サイトへのアクセスを試みているか**を把握することができます。



■専用BOX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。

■横軸：検出した件数

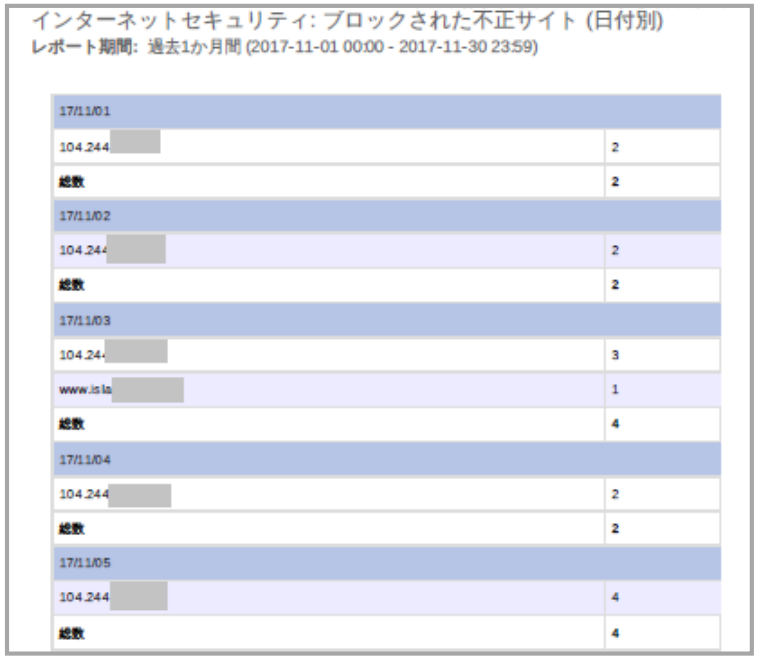
■縦軸：検出件数が多い、上位10件のユーザ
（表記されているIPアドレスを保持する端末）

※Webサイトアクセスブロック機能

不正なWebサイトへのアクセスを阻止することにより、不正プログラムを実行することによる脅威への感染、フィッシング詐欺被害等を未然に防止する機能。

不正サイトへのアクセスに関する情報

- 本ページでは、 専用BOXを経由してアクセスを試みた**不正サイトのURL**を、**日付別**に把握することができます。
- 下図のページでは、アクセスが多い**不正サイトのURL/IPアドレス**を把握することができます。

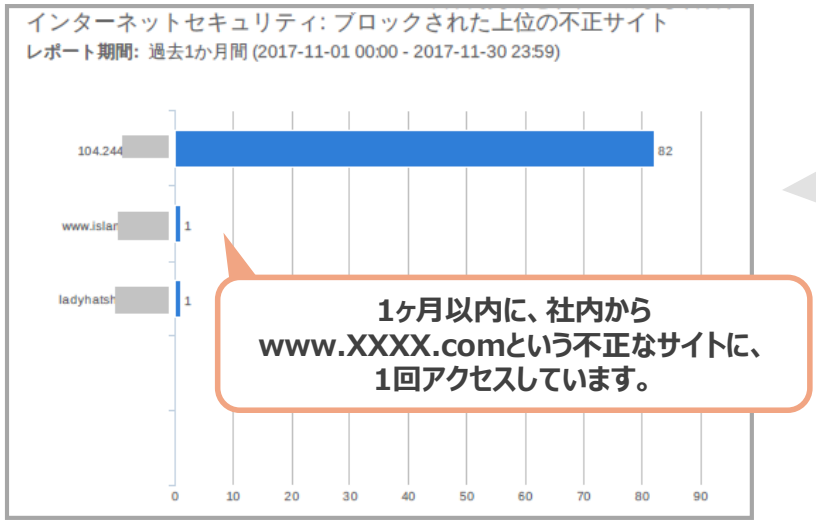


インターネットセキュリティ: ブロックされた不正サイト (日付別)

レポート期間: 過去1か月間 (2017-11-01 00:00 - 2017-11-30 23:59)

17/11/01	
104.244	2
総数	2
17/11/02	
104.244	2
総数	2
17/11/03	
104.24	3
www.isla	1
総数	4
17/11/04	
104.244	2
総数	2
17/11/05	
104.244	4
総数	4

■専用BOX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URL**の情報です（日付別）



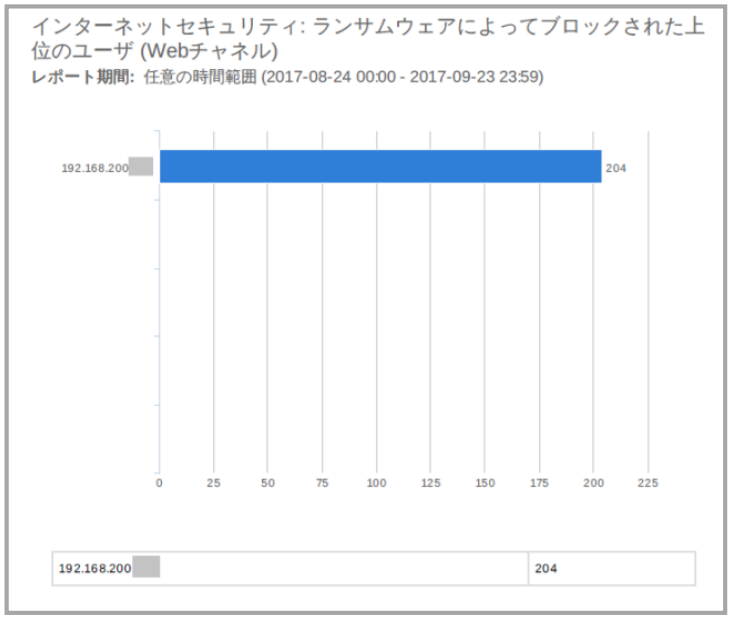
■専用BOXを経由してアクセスされた**不正サイトのURL/IPアドレス**のうち、アクセスが多い**上位10件のURL/IPアドレス**の情報です。

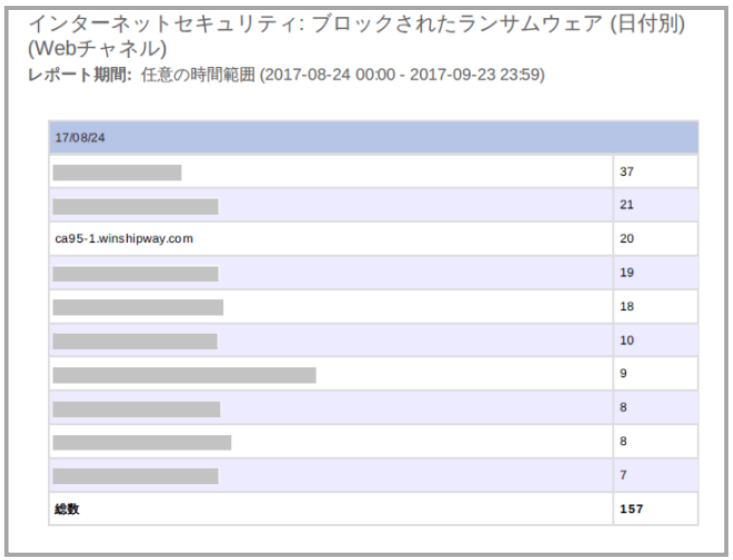
■横軸：検出した件数

■縦軸：検出件数が多い、上位10件の不正サイトURL/IPアドレス

ランサムウェアに関する情報

- 本ページでは、１ヶ月以内にWebチャネルからの**ランサムウェアの侵入を検出しブロックした件数と、あて先となっていたユーザを把握することが出来ます。**
- 下図のページでは、検出した**日付別**に**ランサムウェアのファイル名と件数**を把握することが出来ます。





■ Webチャネルからのランサムウェアの侵入を検出し、ブロックしたユーザ毎の件数です。

■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）

■ **Webチャネルからの侵入を検出したランサムウェアのファイル名とその件数**を把握することが出来ます。

※ランサムウェア

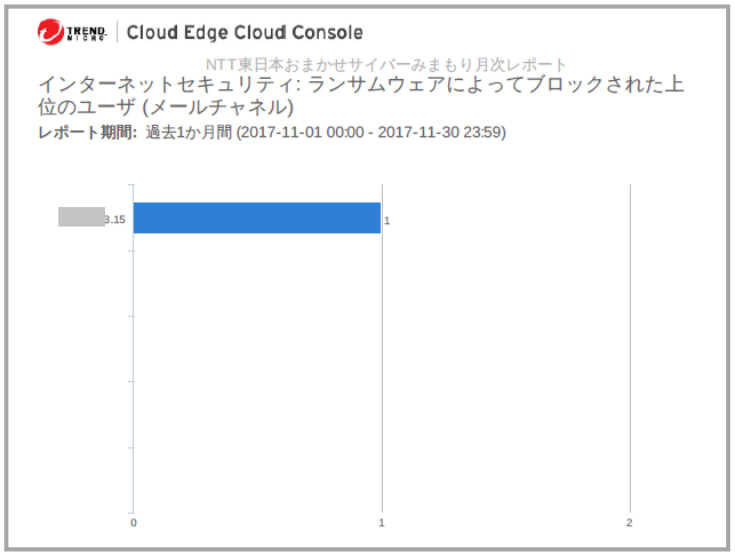
PC内のファイルを暗号化したりロックすることで使用できない状況に追いこみ、元に戻すことと引き換えに「身代金」(Ransom)を要求する不正プログラムです。2017年には「WannaCry」と呼ばれるランサムウェアが世界で流行し、多くの被害をもたらしました。

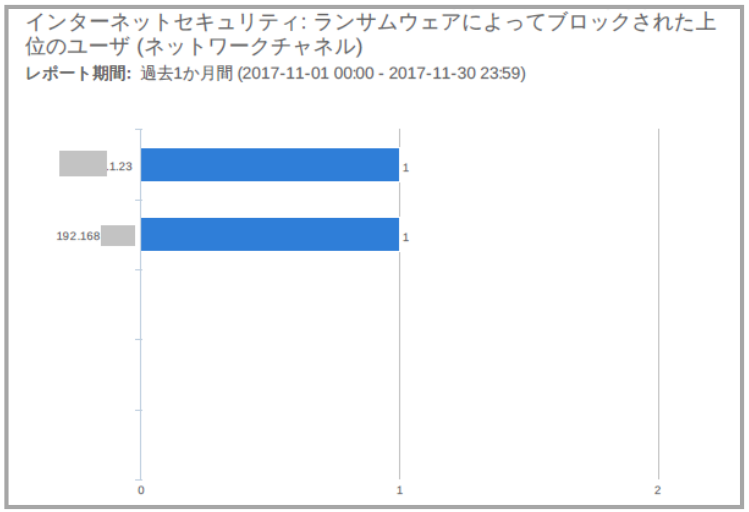
※Webチャネル

ランサムウェアがWebサイトアクセスブロック機能、URL指定によるアクセス制御機能、不正プログラム対策機能により検出されたことを表します。

ランサムウェアに関する情報

□ 本ページでは、１ヶ月以内にメールチャネルおよびネットワークチャネルからの**ランサムウェアの侵入を検出しブロックした件数とあて先となっていたユーザを把握することが出来ます。**





■ メールチャネルからのランサムウェアの侵入を検出し、ブロックした件数です。（ユーザ毎）

■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）

■ ネットワークチャネルからのランサムウェアの侵入を検出し、ブロックした件数です。（ユーザ毎）

■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）

※メールチャネル

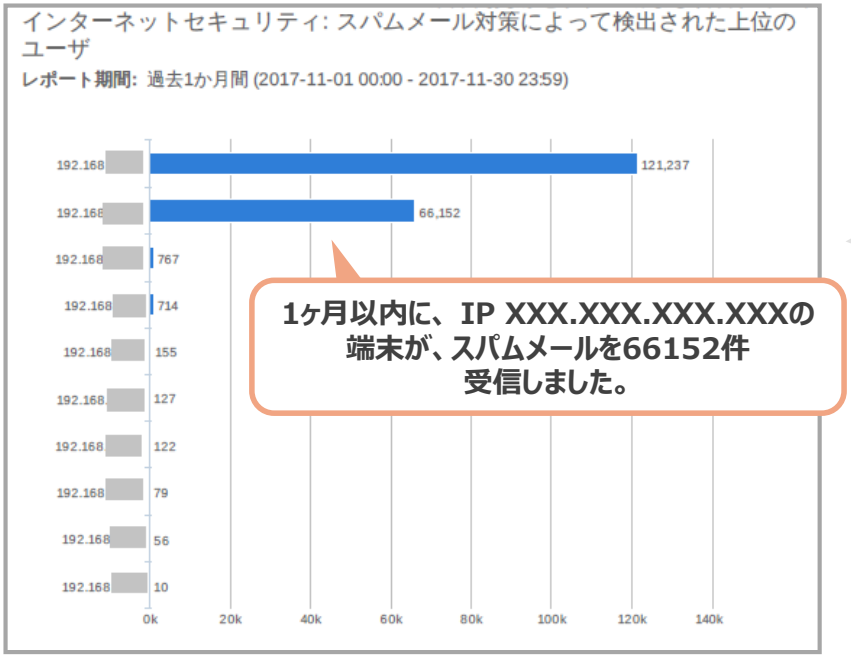
ランサムウェアがメール不正プログラム対策機能により検出されたことを表します。
※メールの添付ファイル等

※ネットワークチャネル

ランサムウェアが不正侵入対策機能により検出されたことを表します。
※ソフトウェアの脆弱性をつく攻撃等が原因

スパムメールに関する情報

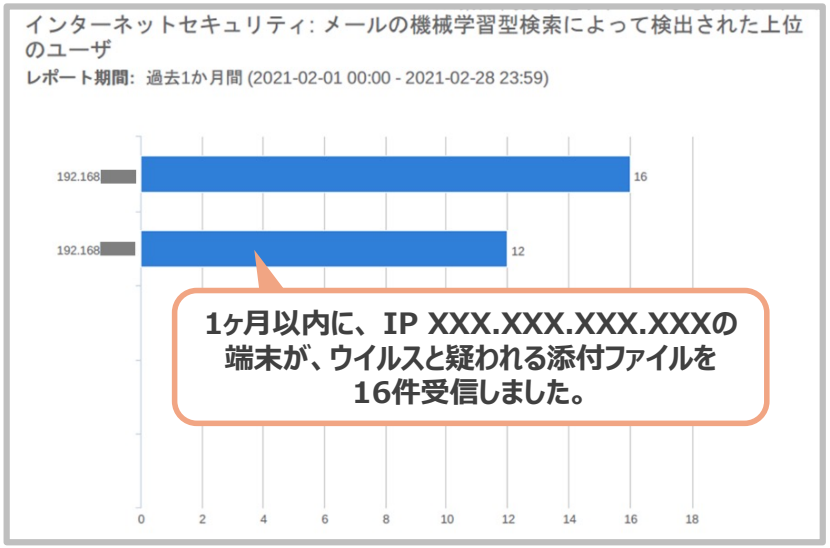
- 本ページでは、メールセキュリティ機能により、専用BOXが１ヶ月以内に**スパムメールを検知**した結果を把握することが出来ます。
- IPアドレスにより、**どのユーザがスパムメールを受け取っているか**、把握することが出来ます。
- スパムメールとは主に**宣伝広告目的で、ユーザの同意なしに勝手に送られてくる電子メールのこと**です。
- メールを利用した攻撃の中には、**ウイルスが添付されていたり、アクセスのみで感染にいたるURLが記されている「標的型攻撃メール」があります。**メールの件名に**[スパムメール]と表記のメールは開封しないようお願いいたします。**
- 専用BOXにより、添付ファイルが不正な物だと判断された場合は、そのファイルを削除し、件名に[ウイルス駆除済み]と表記します。
  不正なプログラムは駆除されておりますが、メール本文中のURL等にはアクセスしないようにしてください。



- **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）

メールの機械学習型検索機能に関する情報

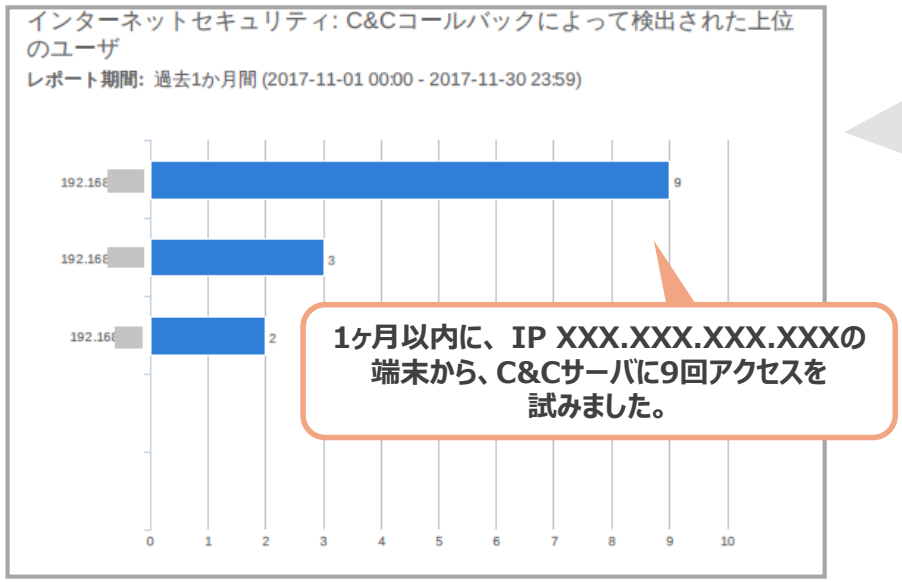
- 本ページでは、機械学習型検索機能により、専用BOXが１ヶ月以内に**ウイルスと疑われる添付ファイルを検知**した結果を把握することが出来ます。
- 機械学習型検索機能では、既存のウイルスの特徴を学習した**AIによる判断で、亜種など最新の脅威を検知**することができます。
- 機械学習型検索機能で不正な添付ファイルと判断された場合は、そのファイルを削除し、件名に[ウイルス駆除済み]と表記します。
  不正な添付ファイルは駆除されておりますが、メール本文中のURL等にはアクセスしないようにしてください。



- **ウイルスと疑われる添付ファイルを受信**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）

C&Cサーバへのアクセスに関する情報

- 本ページでは、不正プログラム侵入検知機能により、専用BOX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**、把握することができます。
- C&Cサーバとは、**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コンピュータ**のことであり、検出された端末は**感染が強く疑われます**。早期の対応が必要です。
- C&Cサーバへの通信は専用BOXによりブロックされており、情報漏えいの発生はございません。



■専用BOX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サーバ

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コンピュータ。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る。

2）サーバから、重要な機密情報を抜き取る。

※不正プログラム対策機能

不正な通信、プログラムによる攻撃を検知。どこから、どこに、どんな通信が行われているか判別し、内部感染を早期に発見。C&Cサーバ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。

IPS(不正侵入対策)に関する情報

□ 本ページでは、専用BOXを経由する通信のうち、**ソフトウェアやネットワークの脆弱性をついた攻撃と疑われる通信**を検知・ブロックした結果を把握することができます。

Cloud Edge Cloud Console

インターネットセキュリティ: 上位のIPS検出
レポート期間: 任意の時間範囲 (2018-04-12 00:00 - 2018-05-09 23:59)

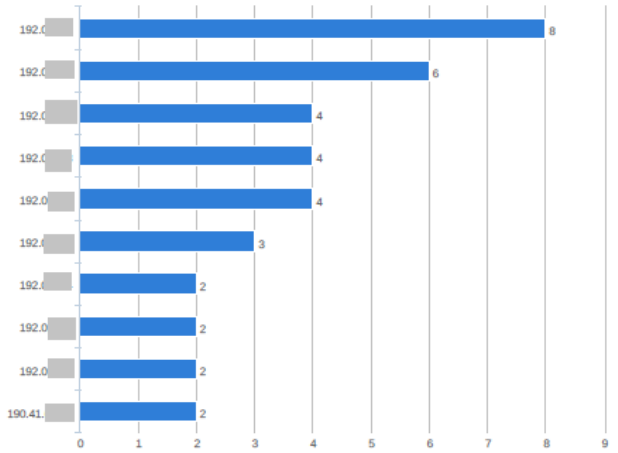
1133548:WEB Microsoft IIS WebDAV ScStoragePathFromUrl Buffer Overflow -1 (CVE-2017-7269)	28
4043309057:TCP Broadcast	14
1130226:SSL OpenSSL Invalid Session Ticket Denial of Service -1 (CVE-2014-3567)	10
1134359:WEB Oracle WebLogic Server WorkContextXmlInputAdapter Insecure Deserialization -1 (CVE-2017-10271)	9
1131496	4
1133304:WEB Cross-site Scripting -1.b	4
4043309087:Bad TCP Flag	4
1134209:WEB Masscan/Sysscan Scanner Activity -1.1	3
1142531	2
1052992:FILE Microsoft Excel Workspace Index Value Memory Corruption -1 (CVE-2007-3890)	2

■専用BOXを経由する通信のうち、**ソフトウェアやネットワークの脆弱性をついた攻撃と疑われる通信**を検知・ブロックした情報です。

■**通信が合致した脆弱性に関するルール毎の件数**を把握することができます。

Cloud Edge Cloud Console

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
レポート期間: 任意の時間範囲 (2018-04-12 00:00 - 2018-05-09 23:59)



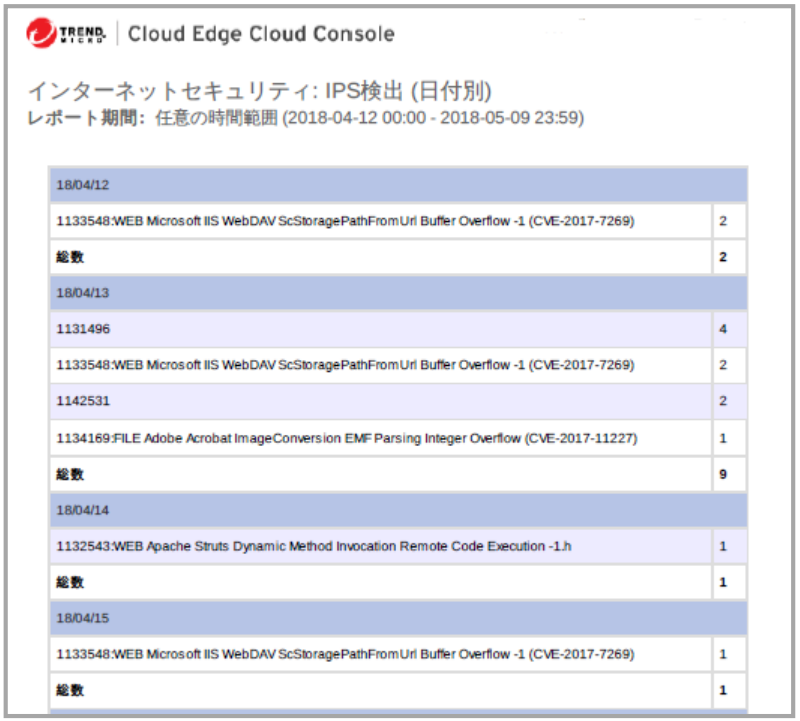
■**ソフトウェアやネットワークの脆弱性をついた攻撃と疑われる通信が**ブロックされた**上位10件のIPアドレス**に関する情報です。

■横軸：件数

■縦軸：該当の通信を開始したユーザ
（表記されているIPアドレスを保持する端末）

IPS(不正侵入対策)に関する情報

- 本ページでは、専用BOXを経由する通信のうち、**ソフトウェアやネットワークの脆弱性をついた攻撃と疑われる通信**を検知・ブロックした結果を把握することができます。



Cloud Edge Cloud Console

インターネットセキュリティ: IPS検出 (日付別)
レポート期間: 任意の時間範囲 (2018-04-12 00:00 - 2018-05-09 23:59)

18/04/12	
1133548:WEB Microsoft IIS WebDAV ScStoragePathFromUrl Buffer Overflow -1 (CVE-2017-7269)	2
総数	**2**
18/04/13	
1131496	4
1133548:WEB Microsoft IIS WebDAV ScStoragePathFromUrl Buffer Overflow -1 (CVE-2017-7269)	2
1142531	2
1134169:FILE Adobe Acrobat ImageConversion EMF Parsing Integer Overflow (CVE-2017-11227)	1
総数	**9**
18/04/14	
1132543:WEB Apache Struts Dynamic Method Invocation Remote Code Execution -1.h	1
総数	**1**
18/04/15	
1133548:WEB Microsoft IIS WebDAV ScStoragePathFromUrl Buffer Overflow -1 (CVE-2017-7269)	1
総数	**1**

■ **ソフトウェアやネットワークの脆弱性をついた攻撃と疑われる通信の**日付別の検出件数です

(通信が合致した脆弱性に関するルール毎)。

※脆弱性

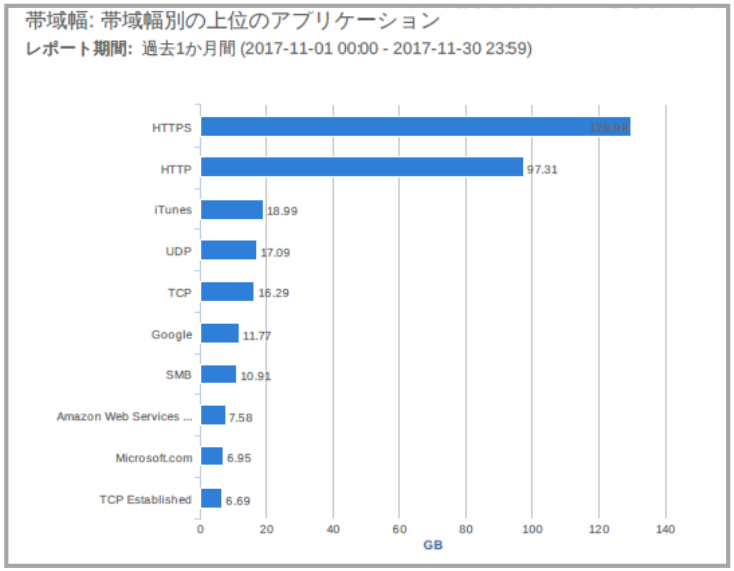
ソフトウェアやネットワークが抱えるセキュリティ上の問題点のこと。
脆弱性を利用されると、システムの乗っ取りや機密情報の漏洩被害にあう可能性があります。
未対応の脆弱性に関しては、OSやアプリケーションを開発しているメーカー等が脆弱性を修正するセキュリティプログラム（パッチ)を提供しているため、可能な限り迅速にアップデートを行う必要があります。

※CVE(Common Vulnerabilities and Exposures)

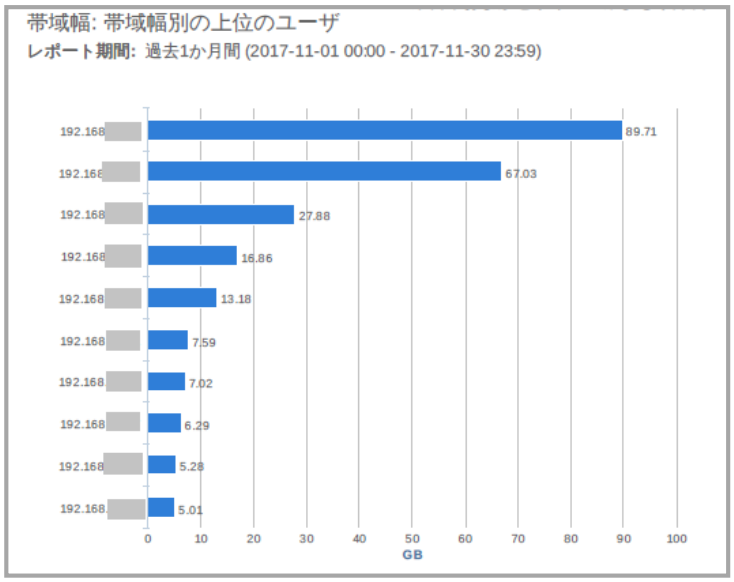
米国政府の支援を受けた非営利団体のMITRE社が様々なソフトウェアの脆弱性についてそれぞれ固有の名前や番号を付与し、リスト化したもの。脆弱性の概要やインパクト、影響するソフトウェアや対応策についての情報を管理しています。

帯域幅に関する情報

- 上図のページでは、専用BOXを通過した通信のうち、**帯域幅（通信量）を多く要したアプリケーション**を把握することができます。
- 下図のページでは、過去1ヶ月間で**帯域幅が上位のユーザ**を把握することができます。



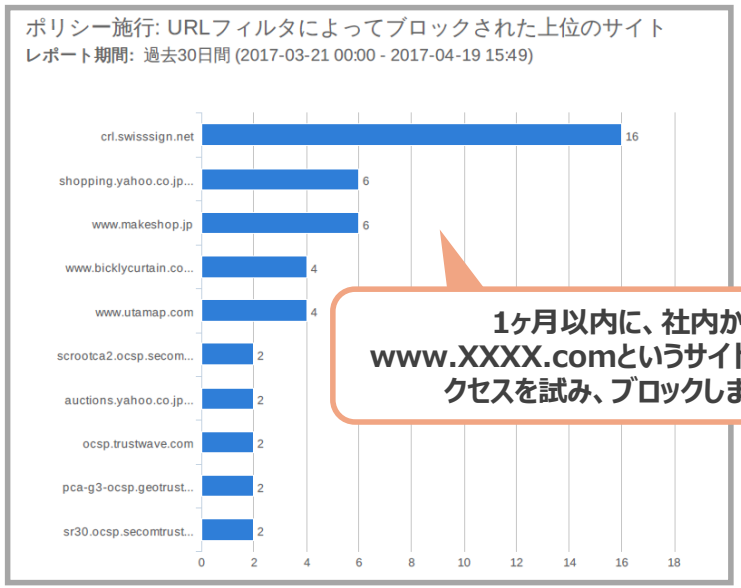
■ **帯域幅**を要したアプリケーションに関する情報です。
■ 横軸：帯域幅(Gbyte)
■ 縦軸：アプリケーション名(通信プロトコル名)



■ **帯域幅を要した**上位10人のユーザに関する情報です。
■ 横軸：帯域幅(Gbyte)
■ 縦軸：ユーザ（表記されているIPアドレスを保持する端末）

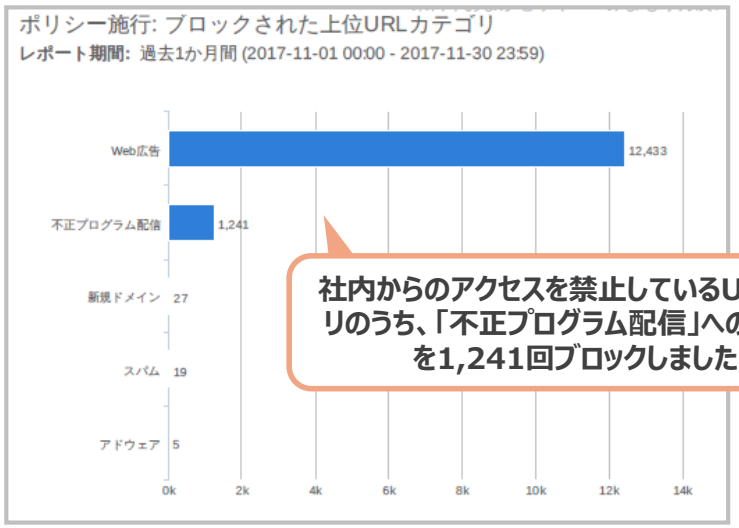
ポリシー施行に関する情報

□　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URLやカテゴリ情報を得ることが出来ます。**



1ヶ月以内に、社内から www.XXXX.comというサイトに、16回アクセスを試み、ブロックしました。

■ **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Webサイトに関する情報です。
■ 横軸：検出した件数
■ 縦軸：URL/IPアドレス



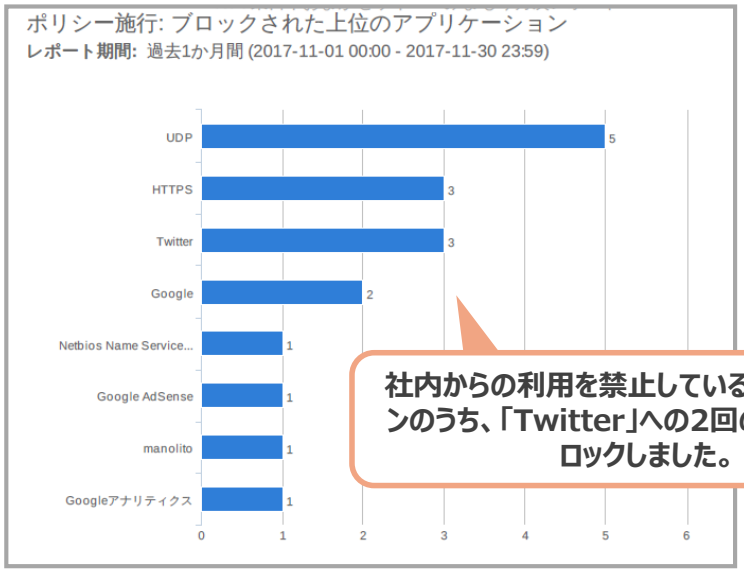
社内からのアクセスを禁止しているURLカテゴリのうち、「不正プログラム配信」へのアクセスを1,241回ブロックしました。

■ **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**に関する情報です。
■ 横軸：検出した件数
■ 縦軸：カテゴリ名

※新規ドメイン
トレンドマイクロ社が実施するWebサイトの安全性評価において「未評価」の場合に新規ドメインカテゴリのWebサイトと認識されます。

ポリシー施行に関する情報

- 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得ることが出来ます。**
- 制限中のアプリケーションは、専用BOX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。



社内からの利用を禁止しているアプリケーションのうち、「Twitter」への2回のアクセスをブロックしました。

■ **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

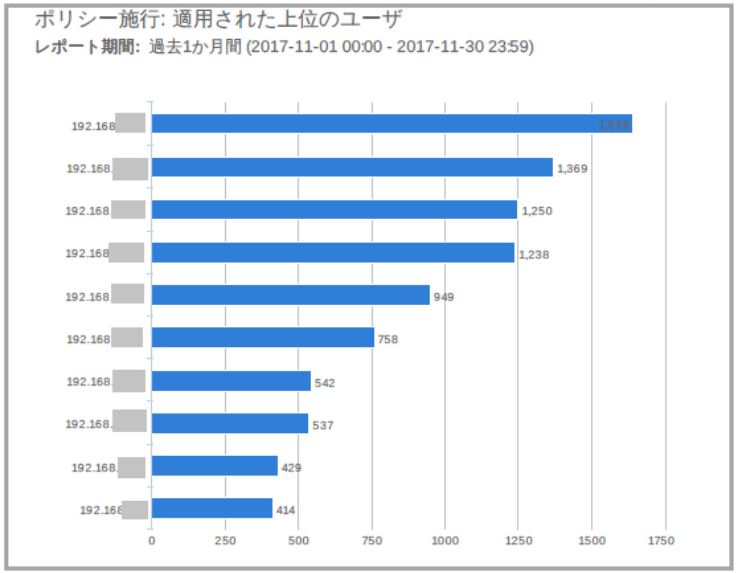
■ 縦軸：利用を禁止しているアプリケーション名(プロトコル)

※アプリケーション利用制限

アプリケーションの利用制限を行う機能。専用BOX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。

ポリシー施行に関する情報

- 本ページでは、**ファイアウォールやURL指定によるアクセス制御機能及びアプリケーション利用制限機能により、Webサイトへのアクセスや、アプリケーションの利用がブロックされた上位のユーザを得ることが出来ます。**
- ポリシー施行に分類される機能は、**業務の効率化やセキュリティリスクの低減を図るために有効な機能**であり、初期設定では「P2P」に分類されるアプリケーションの利用と、「インターネットセキュリティ」に分類されるWebページへのアクセスが制限されています。



■ **ファイアウォールやURL指定によるアクセス制御機能及びアプリケーション利用制限機能**によりアクセスがブロックされたユーザとブロック件数に関する情報です。

■ 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）

※ポリシー施行

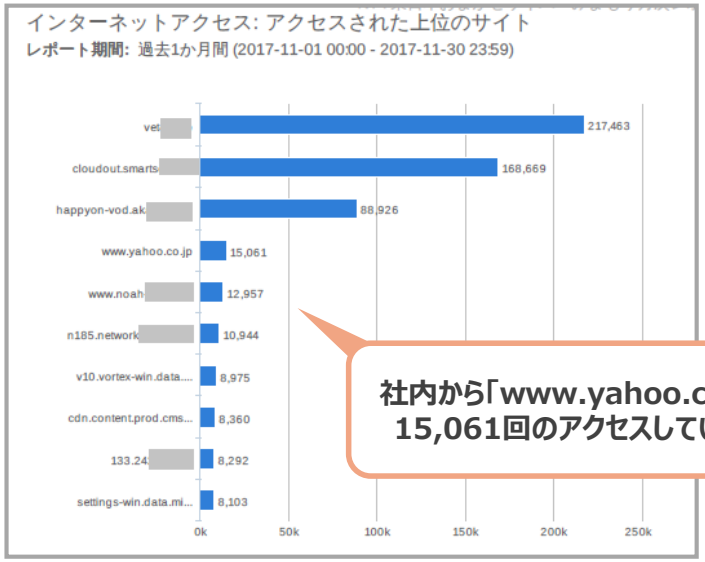
ここでのポリシーとは、ネットワークトラフィックの制御方法をルールとしたものを指します。URLやアプリケーション、IPアドレスなどいくつかの条件を指定し、通信の可否を設定することが出来ます。
設定変更依頼はセキュリティサポートデスクまでお願いいたします。

※インターネットセキュリティカテゴリ

アドウェア、スパイウェア、スパム、ハッキング、フィッシング、不正ドメイン等のカテゴリより構成される。URL指定によるアクセス制御機能によりブロック設定が可能なカテゴリの１つ。

インターネットアクセス(社内からアクセスしたサイト)に関する情報

- 本ページおよび次ページでは、１ヶ月以内に**専用BOXを経由してアクセスした上位10件のWebサイトのURLやカテゴリおよびアプリケーション、インターネットへのアクセスが多い上位ユーザ**に関する情報を得ることができます。
- これにより、業務中に専用BOX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。

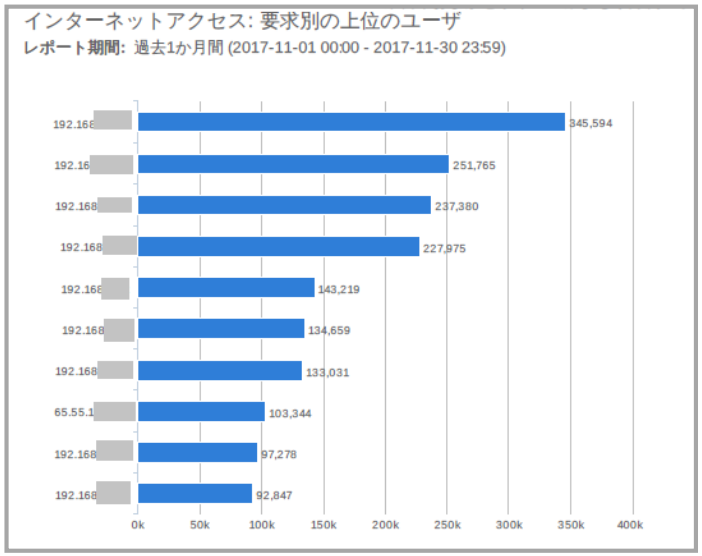


社内から「www.yahoo.co.jp」へ15,061回のアクセスしています。

■ **専用BOX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：URL



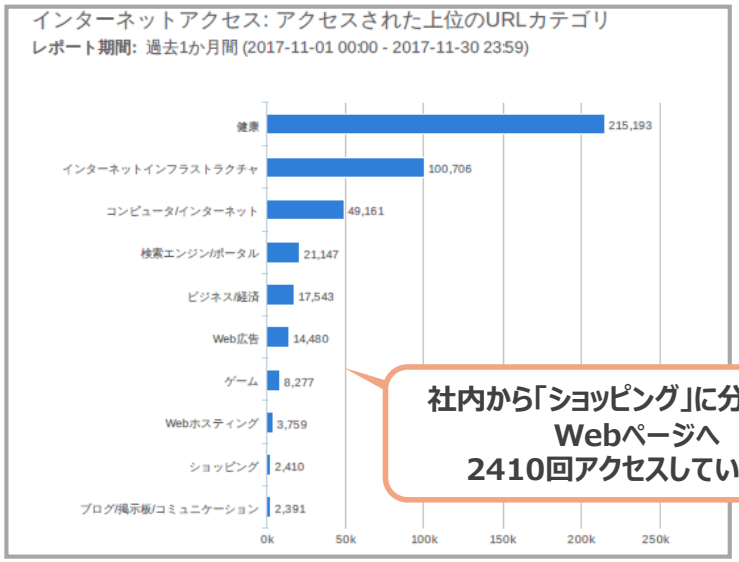
■ **専用BOXを経由してインターネットへのアクセスが多い上位のユーザ**に関する情報です。

■ 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）

インターネットアクセス(社内からアクセスしたサイト)に関する情報

- 本ページおよび次ページでは、１ヶ月以内に**専用BOXを経由してアクセスした上位10件のWebサイトのURLやカテゴリおよびアプリケーション、インターネットへのアクセスが多い上位ユーザ**に関する情報を得ることができます。
- これにより、業務中に専用BOX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。

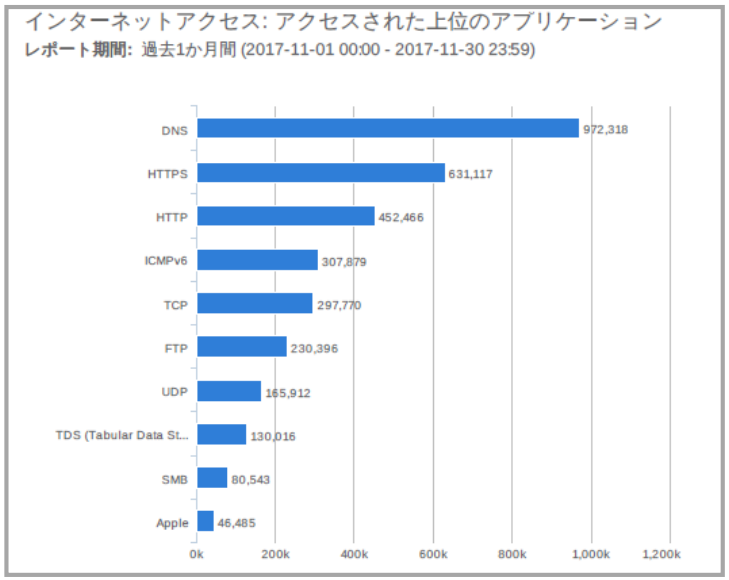


社内から「ショッピング」に分類される Webページへ 2410回アクセスしています。

■ **専用BOXを経由してアクセスした上位10件のWebサイトのカテゴリ**に関する情報です。

■ 横軸：検出した件数

■ 縦軸：カテゴリ名



■ **インターネットへのアクセスが多い上位のアプリケーション**に関する情報です。

■ 横軸：検出した件数

■ 縦軸：アプリケーション名(プロトコル)