レポート機能を使ってみよう

パロアルトネットワークス株式会社

はじめに

ITによるセキュリティ対策は「人の関与」が必要

- コンピュータは白か黒の判定しかできない（グレーゾーンの判断は不可）
  コンピュータ機器は「判定」を行うことはできるけれども「判断」ができるわけではない。パターンマッチングによる判定には限界があり、False PositiveとFalse Negativeが発生する

- 「検知」がゴールではなく、「対策の実施」までがゴールである
  検知だけでは攻撃を防げていないため、人による対策を実施しない限り被害が発生してしまう

- 「検知結果」だけではなく「結果に対する分析」が必要
  攻撃件数の報告だけではなく、検知した情報が本物の攻撃か否か、攻撃傾向の把握、対策できている脅威とできていない脅威などの分析が必要

100%正しい情報が保証されない環境において、人が関与し情報分析が行われていない状況では「安全」を宣言することは不可能であり、セキュリティ・マネジメントができているとは言えない

ITによるセキュリティ対策の考え方

- 100%正しい結果ではない
- 検知だけの状態では攻撃は防げていない

- 検知結果に対して対策の実施の必要性を判断
- 全体のセキュリティ対策の見直しの必要性を判断
- 費用対効果の分析
- 管理できていない項目の洗い出し
- 検知結果に対するルール作り

- 対策を実施

本テキストの
フォーカスポイント

情報分析の目的

- 統計的な多角分析　→　レポート機能を利用した傾向の可視化
  - ✓ トラフィックの傾向分析を行い、不要な通信の排除、危険な通信への対策の必要性を確認する
  - ✓ トラフィックの傾向分析を行い、標準的な通信の状態を把握することで異常な通信を発見しやすくする
  - ✓ 脅威情報の傾向分析を行い、攻撃を受けている傾向を把握する
  - ✓ 脅威情報の傾向分析を行い、攻撃の信憑性や対策を検討すべき脅威情報の分析を行う
  - ✓ トラフィックおよび脅威情報の傾向分析を行い、現在内部ネットワークに問題が発生している可能性について分析する

- ピンポイントでの分析　→　ログ機能を利用した攻撃の真偽に関する分析
  - ✓ 取得したログ情報や第三者機関の情報を利用して、検知した脅威情報が本当の攻撃か否かを分析

次世代ファイアウォールの
レポート機能概要

レポート機能概要

- 40種類の事前定義されたレポートを用意

- 自動的にレポートが作成されるが、無効化することも可能
  - ✓ Device > セットアップ > 管理画面の「ロギングとレポート」のPre-definedタブで設定
  - ✓ 事前定義されたレポート作成の有効化/無効化を行うことが可能
  - ✓ 領域が不足した場合は、古いレポートから上書きされる

レポートの種類

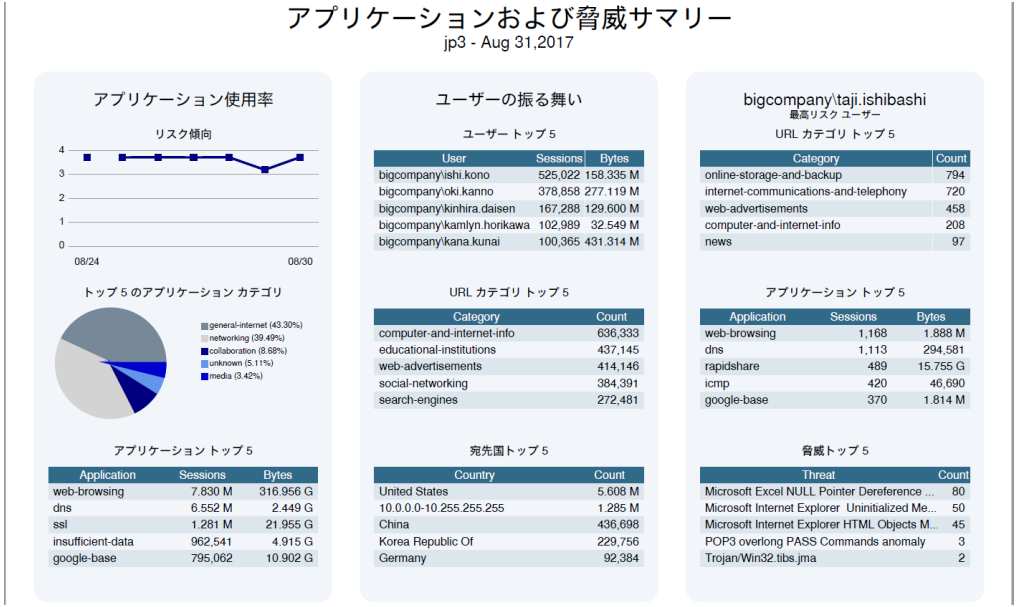
- アプリケーションスコープ
  - ✓ 過去の一定期間に対する直近の使用量の増減に関するレポート
- PDFサマリーレポート（Pre-defined, customize）
  - ✓ カテゴリ別にトップ5の情報を表示
  - ✓ 日単位
  - ✓ GUI上で参照できない（PDFファイルとして出力される）
- 各種レポート
  - ✓ アプリケーション、トラフィック、脅威などを日単位で表形式のレポートとして表示
- カスタムレポート
  - ✓ トラフィックレベルでのレポートを作成
  - ✓ ACCと同じレベルでの期間指定
  - ✓ 出力する項目を選択可能

アプリケーションスコープ

- 過去の一定期間のデータと直近のデータを比較
- モニターの内容により選択できる期間は異なる
- スコープの種類は以下のとおり
  - ✓ サマリー
  - ✓ 変化モニター
  - ✓ 脅威モニター
  - ✓ 脅威マップ
  - ✓ ネットワークモニター
  - ✓ トラフィックマップ

PDFサマリーレポート

- 1日単位で各カテゴリのトップ5データを表示
- 前日までのデータを1日単位でレポート



アプリケーションおよび脅威サマリー

jp3 - Aug 31,2017

アプリケーション使用率

リスク傾向

トップ 5 のアプリケーション カテゴリ

アプリケーション トップ 5

Application	Sessions	Bytes
web-browsing	7.830 M	316.956 G
dns	6.552 M	2.449 G
ssl	1.281 M	21.955 G
insufficient-data	962,541	4.915 G
google-base	795,062	10.902 G

ユーザーの振る舞い

ユーザー トップ 5

User	Sessions	Bytes
bigcompany\ishi.kono	525,022	158.335 M
bigcompany\oki.kanno	378,858	277.119 M
bigcompany\kinhira.daisen	167,288	129.600 M
bigcompany\kamlyn.horikawa	102,989	32.549 M
bigcompany\kana.kunai	100,365	431.314 M

URL カテゴリ トップ 5

Category	Count
computer-and-internet-info	636,333
educational-institutions	437,145
web-advertisements	414,146
social-networking	384,391
search-engines	272,481

宛先国トップ 5

Country	Count
United States	5.608 M
10.0.0.0-10.255.255.255	1.285 M
China	436,698
Korea Republic Of	229,756
Germany	92,384

bigcompany\taji.ishibashi

最高リスク ユーザー

URL カテゴリ トップ 5

Category	Count
online-storage-and-backup	794
internet-communications-and-telephony	720
web-advertisements	458
computer-and-internet-info	208
news	97

アプリケーション トップ 5

Application	Sessions	Bytes
web-browsing	1,168	1.888 M
dns	1,113	294,581
rapidshare	489	15.755 G
icmp	420	46,690
google-base	370	1.814 M

脅威トップ 5

Threat	Count
Microsoft Excel NULL Pointer Dereference ...	80
Microsoft Internet Explorer Uninitialized Me...	50
Microsoft Internet Explorer HTML Objects M...	45
POP3 overlong PASS Commands anomaly	3
Trojan/Win32.tibs.jma	2

各種レポート

アプリケーションレポート

	アプリケーション名	バイト	セッション
1	web-browsing	311.8G	6.7M
2	dns	2.3G	6.2M
3	ssl	33.6G	1.3M
4	insufficient-data	2.5G	751.2k
5	google-base	8.1G	535.1k
6	facebook-base	6.0G	424.2k
7	ntp	210.2M	416.3k
8	ppstream	10.5G	214.2k
9	skype-probe	58.4M	183.6k
10	qq-base	672.3M	175.8k
11	gnutella	207.0M	165.4k
12	icmp	36.8M	157.7k
13	unknown-udp	11.9G	156.2k
14	bittorrent	5.5G	126.0k
15	ping	46.8M	122.8k
16	flash	25.8G	109.8k
17	myspace-base	2.5G	99.7k
18	ipv6	2.9G	92.0k
19	gmail-base	5.2G	91.5k
20	blackboard	9.9G	90.7k
21	garena	30.5M	78.6k
22	google-analytics	424.3M	76.5k
23	youtube-base	2.0G	74.7k

PDF にエクスポート　CSV にエクスポート　XML にエクスポート

アプリケーション レポート
- 新規アプリケーション
- アプリケーション
- アプリケーション カテゴリ
- テクノロジ カテゴリ
- HTTP アプリケーション

脅威レポート

	脅威/コンテンツ名	ID	脅威/コンテンツタイプ	カウント
1	My Amazon Signature	411...	vulnerability	11.8k
2	ZeroAccess.Gen Command and Control Traffic	132...	spyware	10.8k
3	HTTP GET Requests Long URI Anomaly	308...	vulnerability	4.2k
4	Javascript WSF HTA JSE or VBS File Sent in Email	390...	vulnerability	3.4k
5	SIPVicious Scanner Detection	544...	vulnerability	2.4k
6	Microsoft Internet Explorer Install Engine Control Buffer Overflow Vulnerability	370...	vulnerability	2.2k
7	trojan/Win32 EXE.startsurf.v	206...	virus	1.8k
8	trojan/Win32 EXE.startsurf.v	206...	wildfire-virus	1.2k
9	Suspicious DNS Query (Worm.rimecud:butterfly.bigmoney.biz)	879...	spyware	1.2k
10	Trojan/Win32.chapak.pt	258...	wildfire-virus	1.0k
11	JavaScript Obfuscation Detected	542...	vulnerability	1.0k
12	Virus/Win32.WGeneric.yshpc	257...	wildfire-virus	685
13	Bot: Mariposa Command and Control	126...	spyware	596
14	Trojan-Ransom/Win32.wanna.b	179...	virus	569
15	Trojan/Win32.spnr.aeyy	218...	virus	541
16	Macromedia Shockwave swdir.dll ActiveX Control Remote Stack Overflow Vulnerability	334...	vulnerability	523
17	FTP: login Brute Force attempt	400...	vulnerability	512
18	Suspicious HTTP Response Found	398...	vulnerability	498
19	Virus/Win32.WGeneric.ruaby	202...	virus	384
20	VirTool/Win32.injector.ncyn	221...	virus	384
21	Microsoft Windows Graphics Rendering Engine WMF Record Parsing Vulnerability	302...	vulnerability	377

PDF にエクスポート　CSV にエクスポート　XML にエクスポート

アプリケーション レポート
トラフィック レポート
脅威レポート
- ボットネット
- 脅威
- 攻撃元アドレス
- 攻撃先アドレス
- 攻撃者（送信元国毎）
- 攻撃者（宛先国毎）
- 被害者の送信元

URL フィルタリング レポート
PDF サマリー レポート

2月 2019

日	月	火	水	木	金	土
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	1	2
3	4	5	6	7	8	9

カスタムレポート

- 特定の項目だけのレポートのカスタマイズが可能
- 期間を自由に指定することが可能
- 選択する項目はサマリーログ、詳細ログのすべての項目から選択することが可能
- 詳細ログ情報を参照する場合、CPに負荷がかかるケースがあるので、レポート作成はトラフィック量の少ない時間帯に実施する

レポート機能の使い方

レポートを使った分析方法は画一されたものではなく、ユーザによってもその利用方法は異なると思われるが、ここではたくさんあるレポート機能の中から、傾向分析で利用する「アプリケーションスコープ」の「ネットワークモニター」と「脅威モニター」を取り上げ、その利用方法について紹介する。

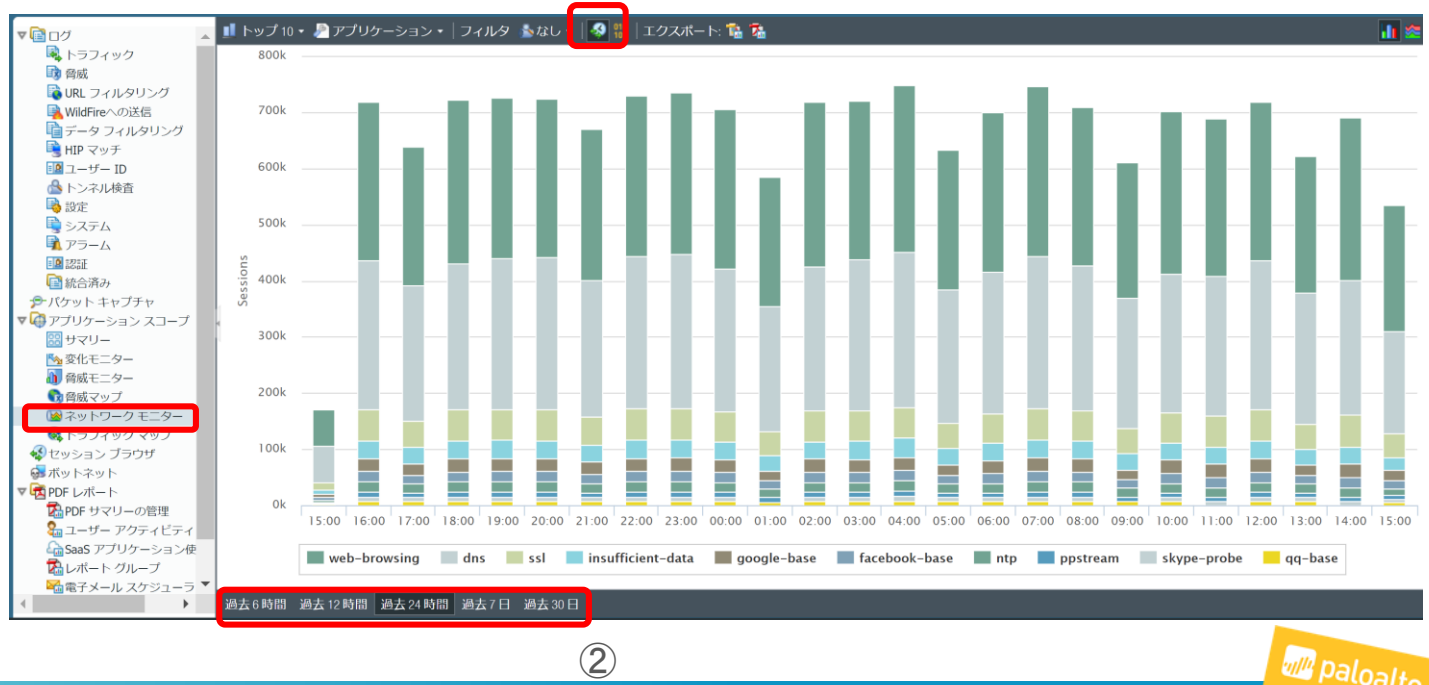
「利用アプリ」の傾向を把握しよう

トラフィックの傾向を理解しよう

① Monitor > アプリケーションスコープ > ネットワークモニター

② 過去24時間に変更する

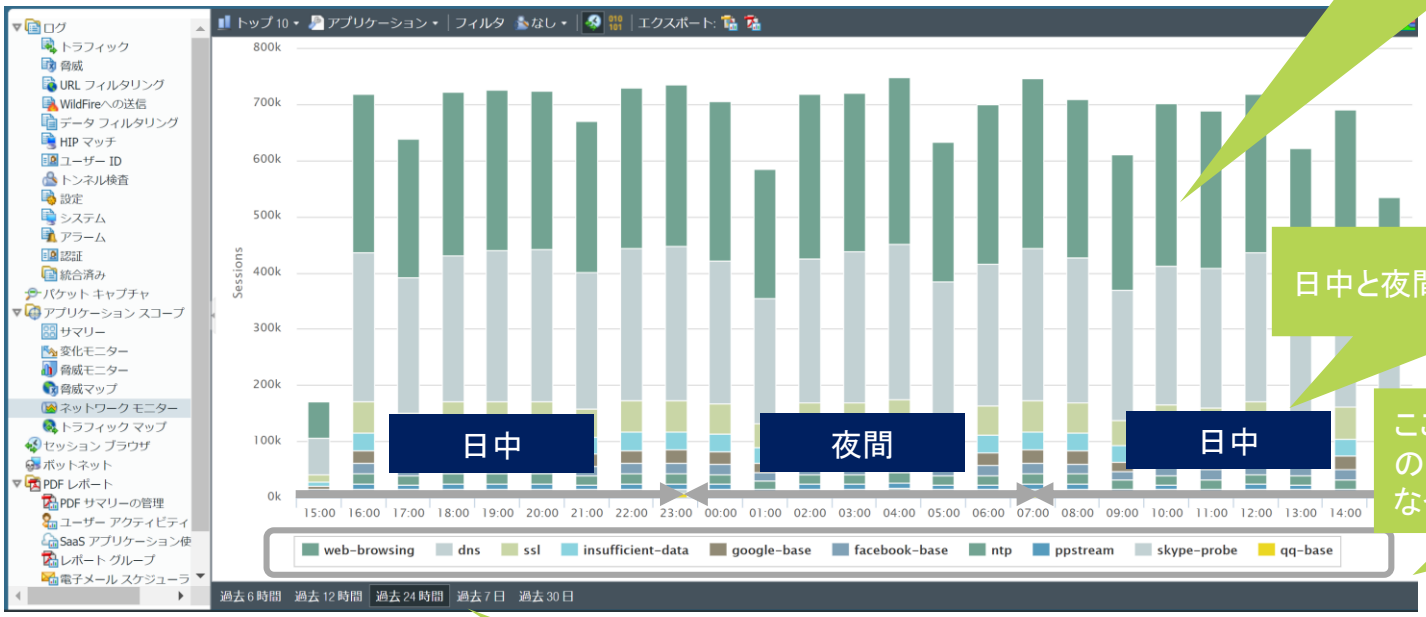
③ 表示をセッションの表示に変更（セッション数の上位）



以下のポイントを整理する

- どんなアプリケーションが利用されているかを認識する
- アプリケーションの利用用途や必要に応じたセキュリティ対策を実施できているかどうかを認識する
- データ転送量やセッション数を把握する
- 通信の特徴を理解する
  - ✓ 日中と夜間の通信の違い
  - ✓ 一日の変化の傾向
  - ✓ セッション数の上位とデータ転送量の上位
- 日々の変化の傾向をつかむ

「利用アプリ」の傾向を把握しよう（続き）



アプリケーション別のトラフィック量やセッション数を確認

日中と夜間の傾向の違いを確認

ここに表示されるアプリケーションの利用の必要性や目的は明確になっているか確認

一日の傾向だけでなく、1週間および1か月の傾向も把握する

※この画面はデモ画面を利用
傾向はユーザごとに異なる

一般的な指標

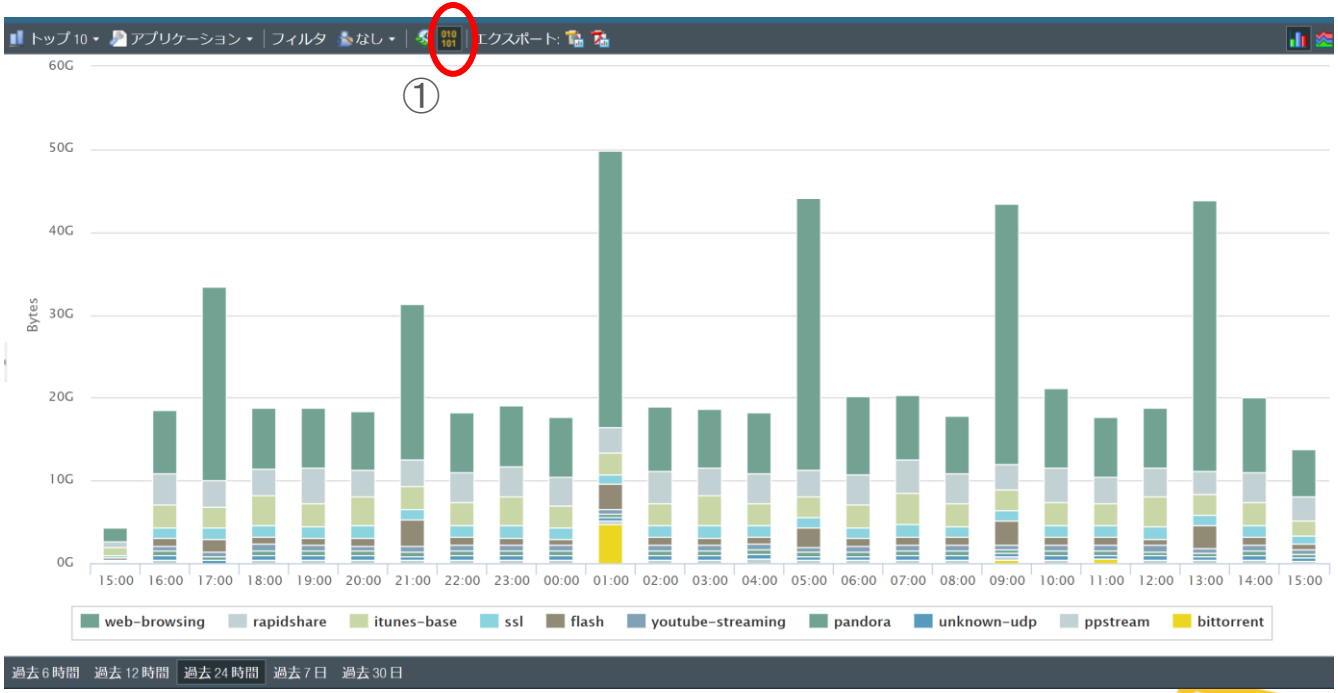
- 夜間のアプリケーションは、バックアップやデータ転送など夜間バッチ処理以外は利用がない
- DNSのような1セッションのデータ転送は少ないが、リクエスト数が多いアプリケーションはセッションでは上位になるが、転送データ数はリストされにくい
- バックアップやデータ転送で利用されるアプリケーションはセッション数は少なくても、バイト数は多くなる傾向にある
- Unknown通信が多い場合、社内アプリケーションの利用が考えられる。そのため、他のUnknownアプリと区別がつくようにカスタムアプリケーションの作成を推奨

できるだけ多くのアプリケーションが管理下にある状態する。
管理下とは、該当アプリの利用目的の把握、通常時のセッション数やトラフィック量の把握、対策の必要性の判断ができている状態を指す。

※上記はあくまで一つの指標のため、実際の利用状況に合わせて判断を行ってください。

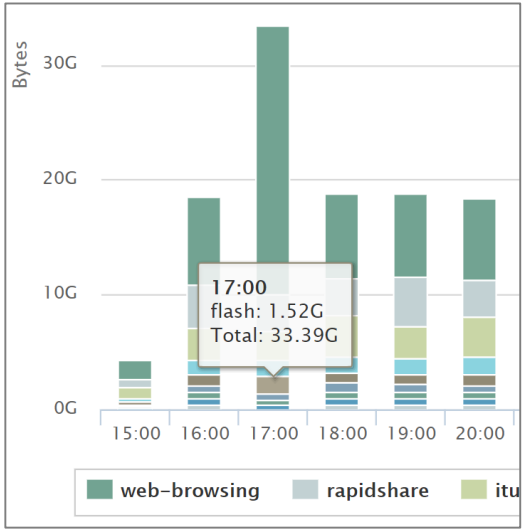
「ネットワークモニター」GUIの操作方法

セッション数ではなくデータサイズで転送データ量の多いアプリケーションを確認
画面上の①のボタンをクリックし、バイトのカウントに変更



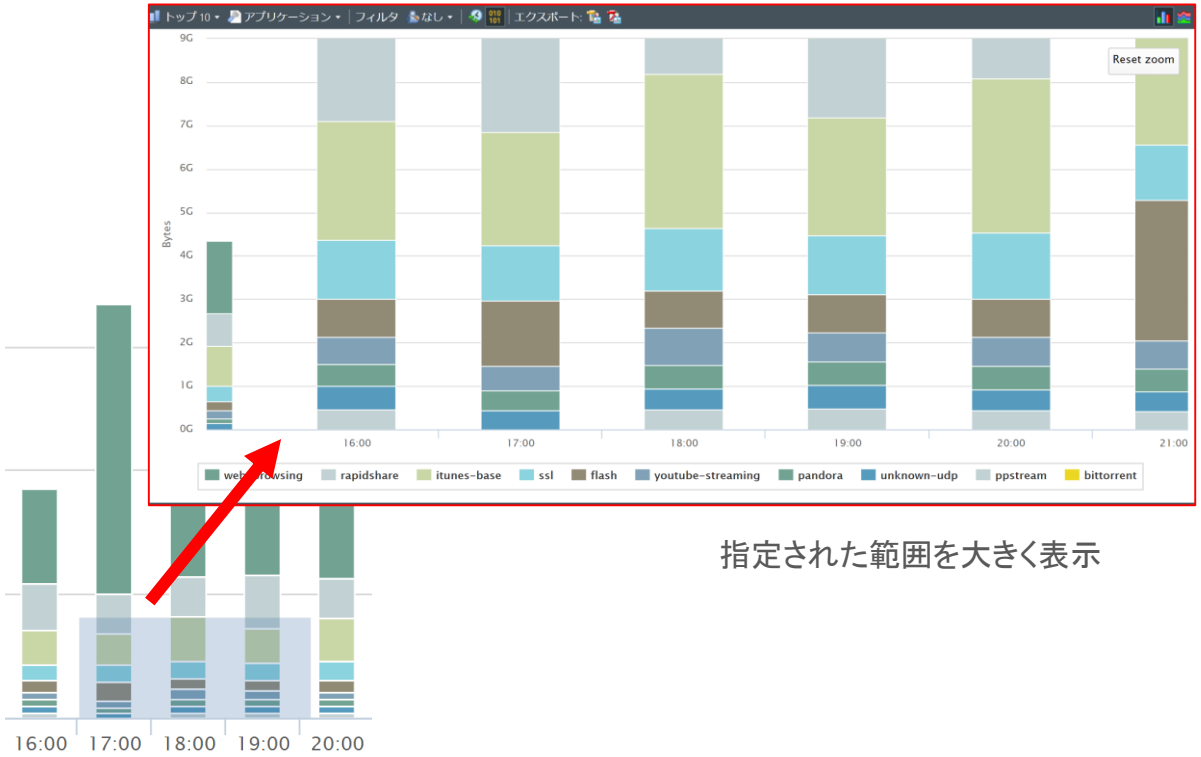
「ネットワークモニター」GUIの操作方法

数値の表示



カーソルを項目に合わせるとデータを表示

ズーム機能

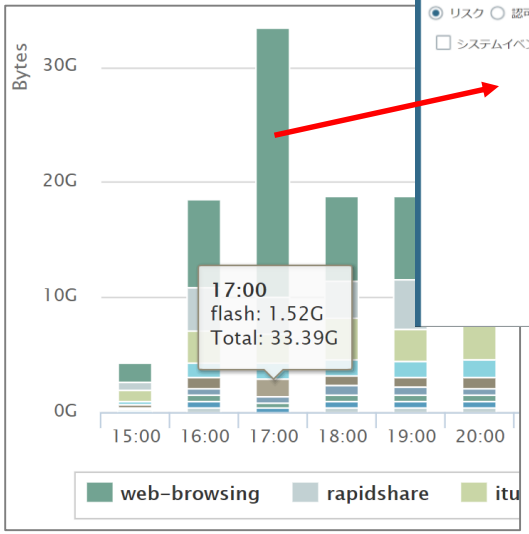


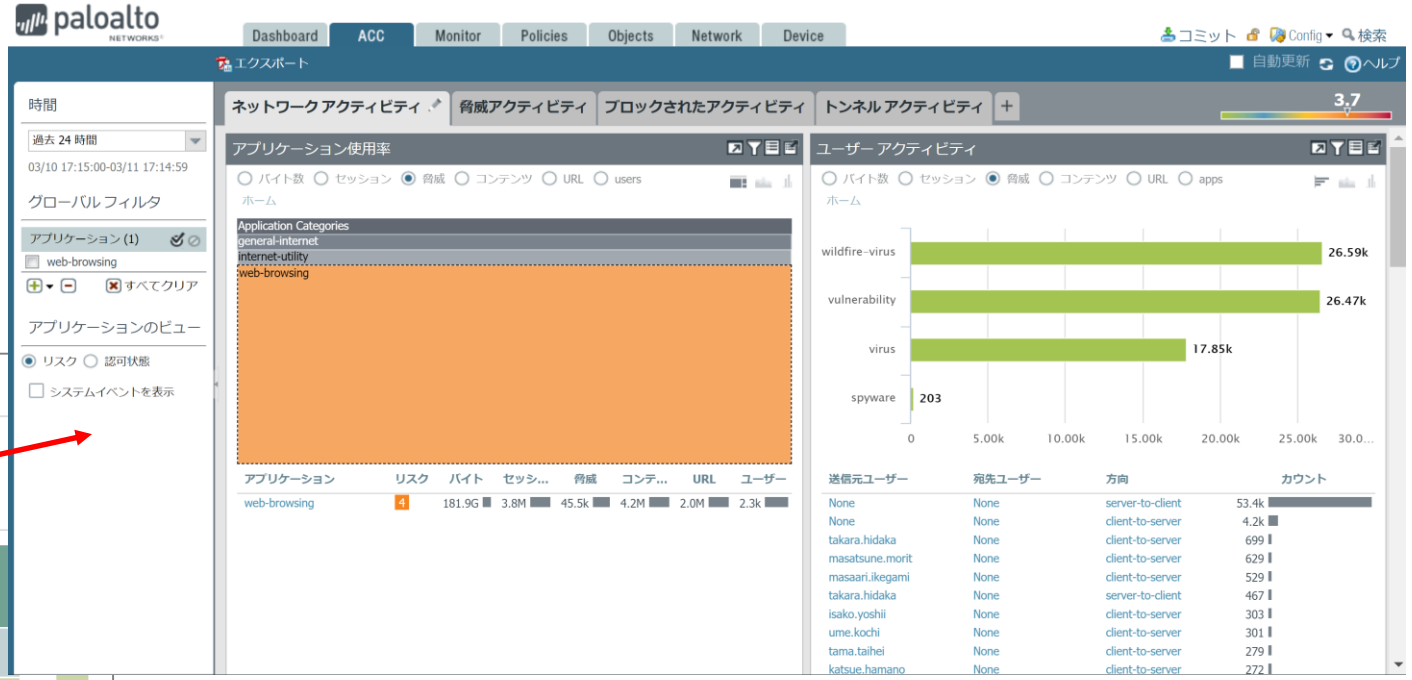
ドラッグ&ドロップで範囲を指定

指定された範囲を大きく表示

「ネットワークモニター」GUIの操作方法（続き）

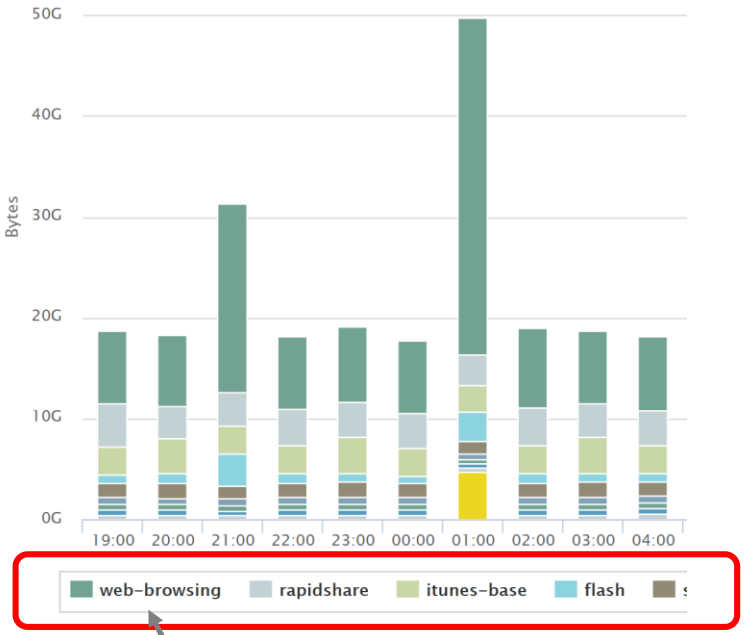
該当箇所をクリックすると、該当アプリケーションだけにフィルターされた24時間のACC画面に遷移する
例では、Web-browsingをクリック



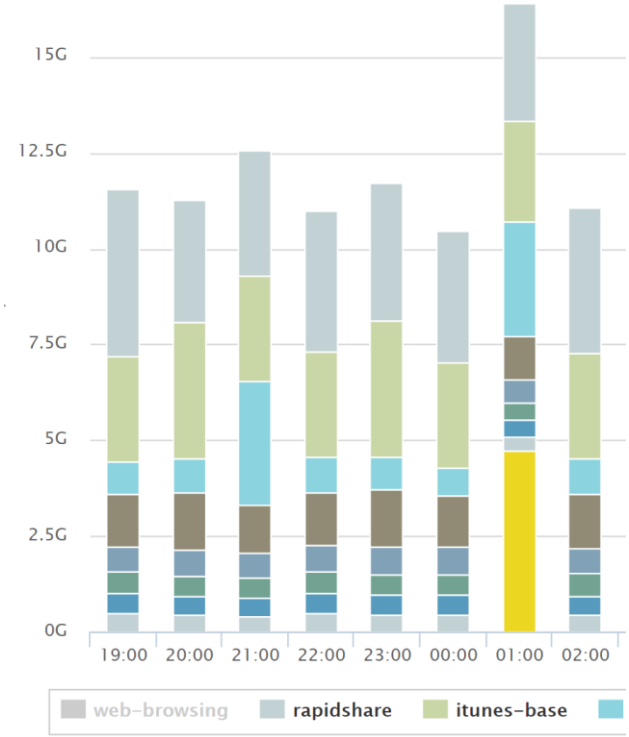


「ネットワークモニター」GUIの操作方法（続き）

非表示にしたいアプリケーション名をクリックすると、該当アプリケーションが非表示になる

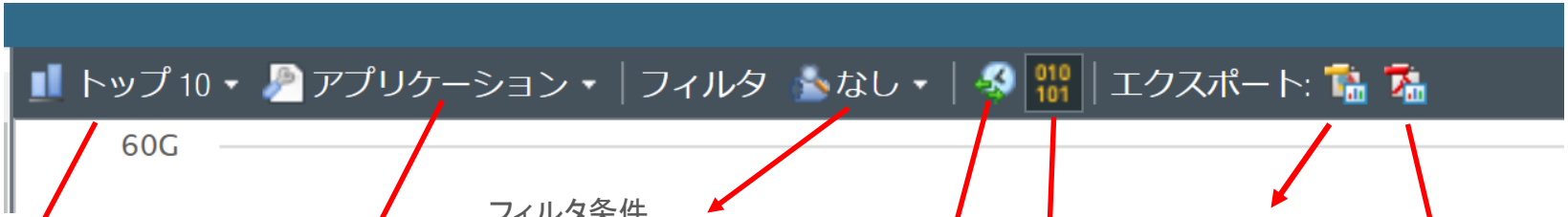


web-browsingをクリック



web-browsing以外を表示

「ネットワークモニター」GUIの操作方法（続き）



トップ
10/25/50/100から選択

- アプリケーション
- Appカテゴリ
- 送信IP/ユーザ
- 宛先IP/ユーザ

フィルタ条件
- なし
- ビジネスシステム
- コラボレーション
- 一般的なインターネット
- メディア
- ネットワーク
- 不明

セッション数の上位

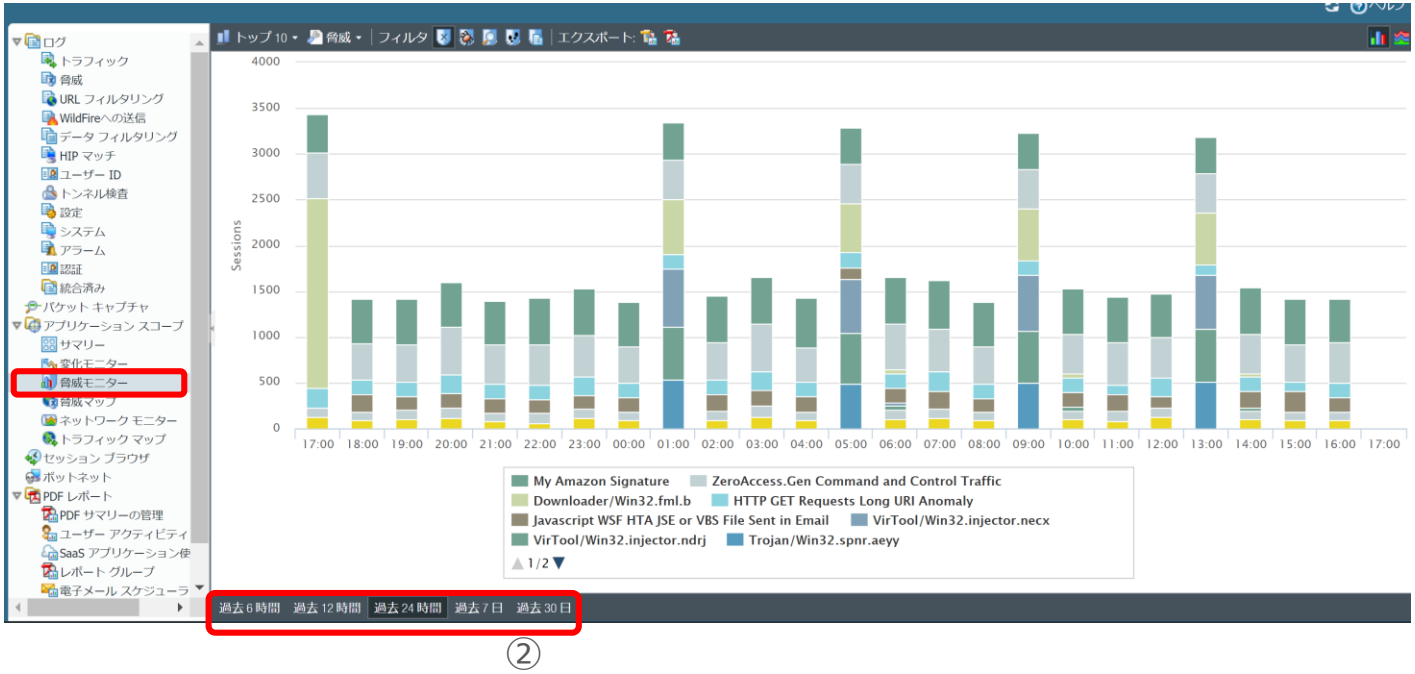
バイト数の上位

表示された表をPNGでエクスポート

表示された表をPDFでエクスポート

脅威モニターで攻撃されている傾向を把握

① Monitor > アプリケーションスコープ > 脅威モニター
② 過去24時間に変更



検知した「脅威」情報を把握しよう

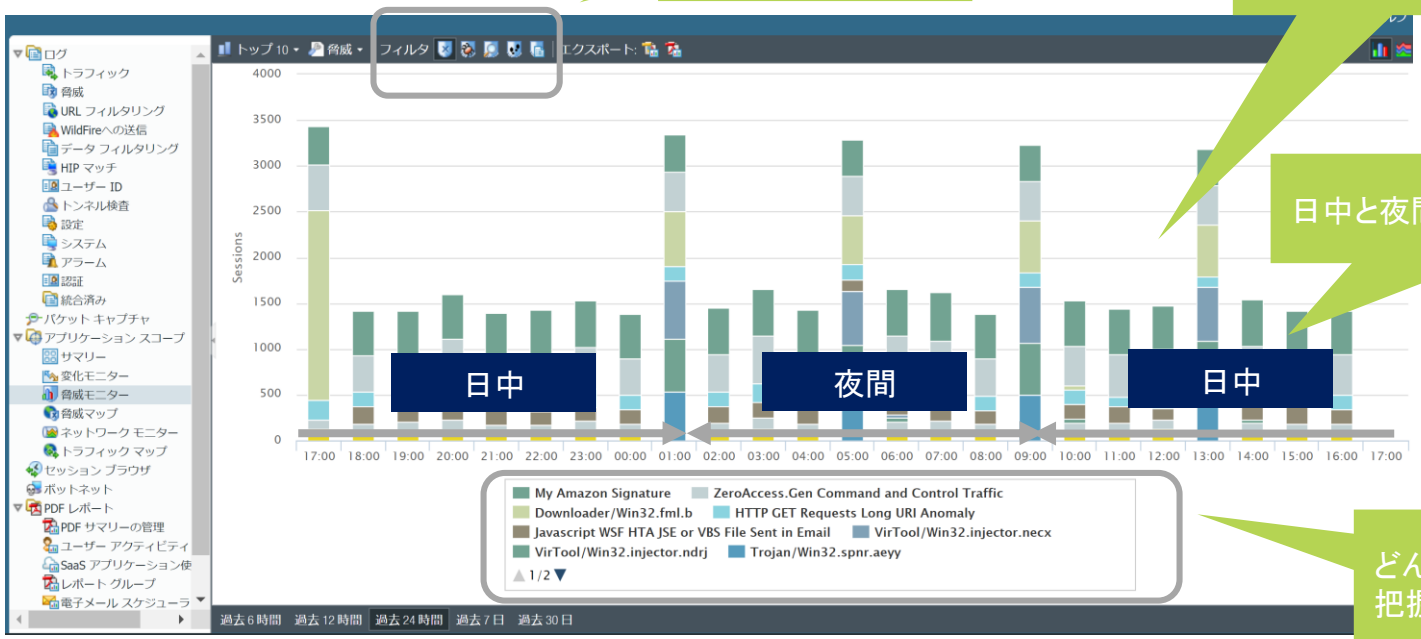
- どんな脅威が上位を占めているかを認識する
- 日中と夜間の傾向の違いを認識する
- 傾向を把握する
  - ✓ 突発的に発生しているのか、常時平均的に発生しているのか
- 日々の変化の傾向をつかむ
- 脅威別（ウィルス/脆弱性/スパイウェア）で上記内容を把握
- 上位を占めている脅威への対応がなされているかどうかを認識する
  （本テキストではこの部分には触れないが、該当項目を絞り込みMonitorで確認）
  - ✓ ブロックモードか検知モードか
  - ✓ 検知モードの場合、対策は行っているか
    未対応の場合、その理由は明確になっているか
    （対策を行うか否かよりも、ルールの基で制御管理されているかどうかが重要）

検知した「脅威」情報を把握しよう（続き）

脅威のカテゴリ別に
絞り込んで分析

検知した脅威情報の数や
傾向を把握

日中と夜間の傾向の違いを確認



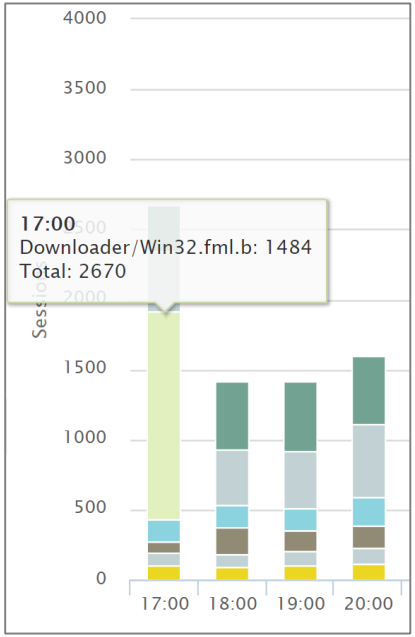
どんな脅威を検知しているのか
把握

一日の傾向だけでなく、1週間
および1か月の傾向も把握する

※この画面はデモ画面を利用しています。
傾向はユーザごとに異なります。

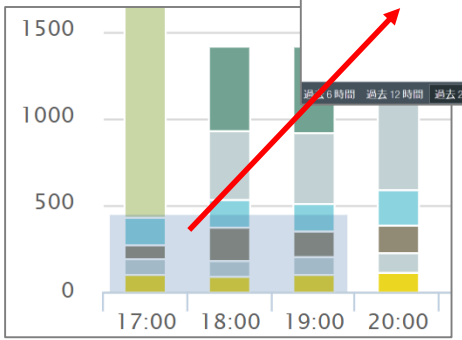
「脅威モニター」GUIの操作方法

数値の表示

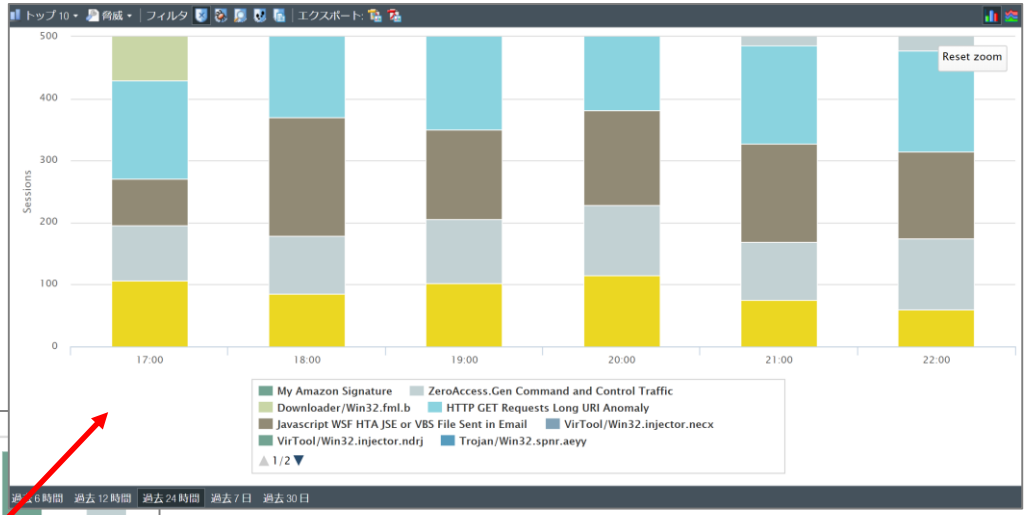


カーソルを項目に合わせるとデータを表示

ズーム機能



ドラッグ&ドロップで範囲を指定



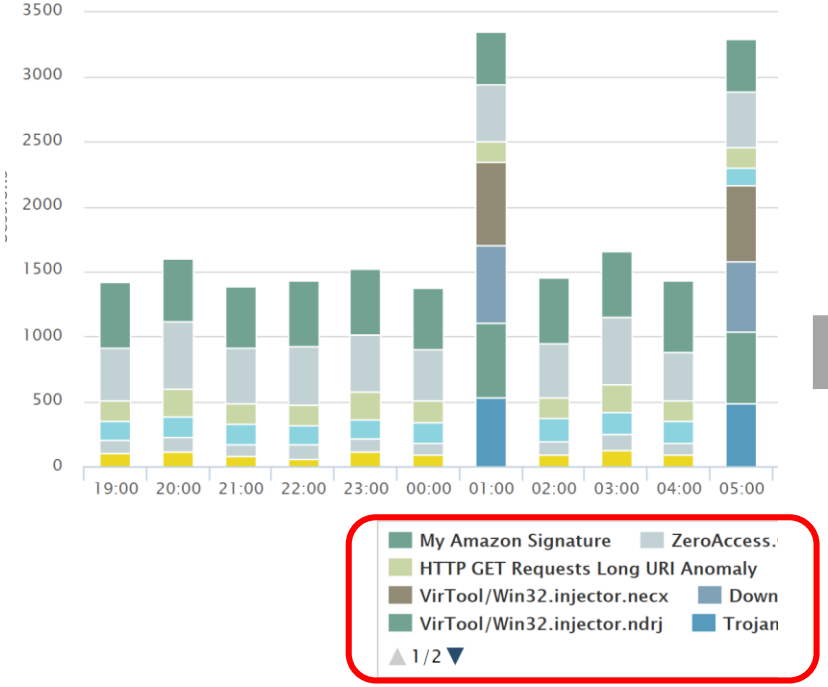
指定された範囲を大きく表示

「脅威モニター」GUIの操作方法（続き）

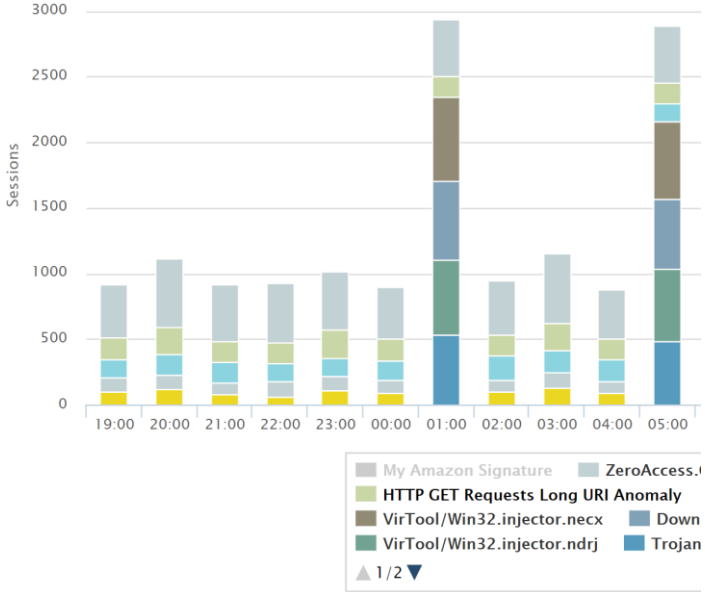
該当箇所をクリックすると、該当脅威だけにフィルターされた
24時間のACC画面に遷移する
例では、Downloader/Win32.fml.bをクリック

「脅威モニター」GUIの操作方法（続き）

非表示にしたい脅威名をクリックすると、該当の脅威情報が非表示になる

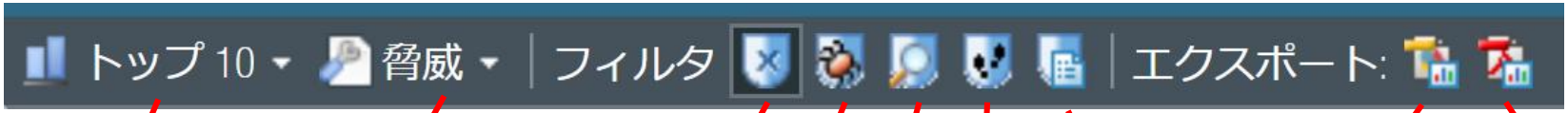


My Amazon Signatureをクリック



My Amazon Signatureが非表示に

「脅威モニター」GUIの操作方法（続き）



トップ
10/25

- 脅威
- 脅威カテゴリ
- 送信IP/ユーザ
- 宛先IP/ユーザ

すべての脅威
情報を表示

ウィルス情報を
表示

スパイウェア
情報を表示

脆弱性情報を
表示

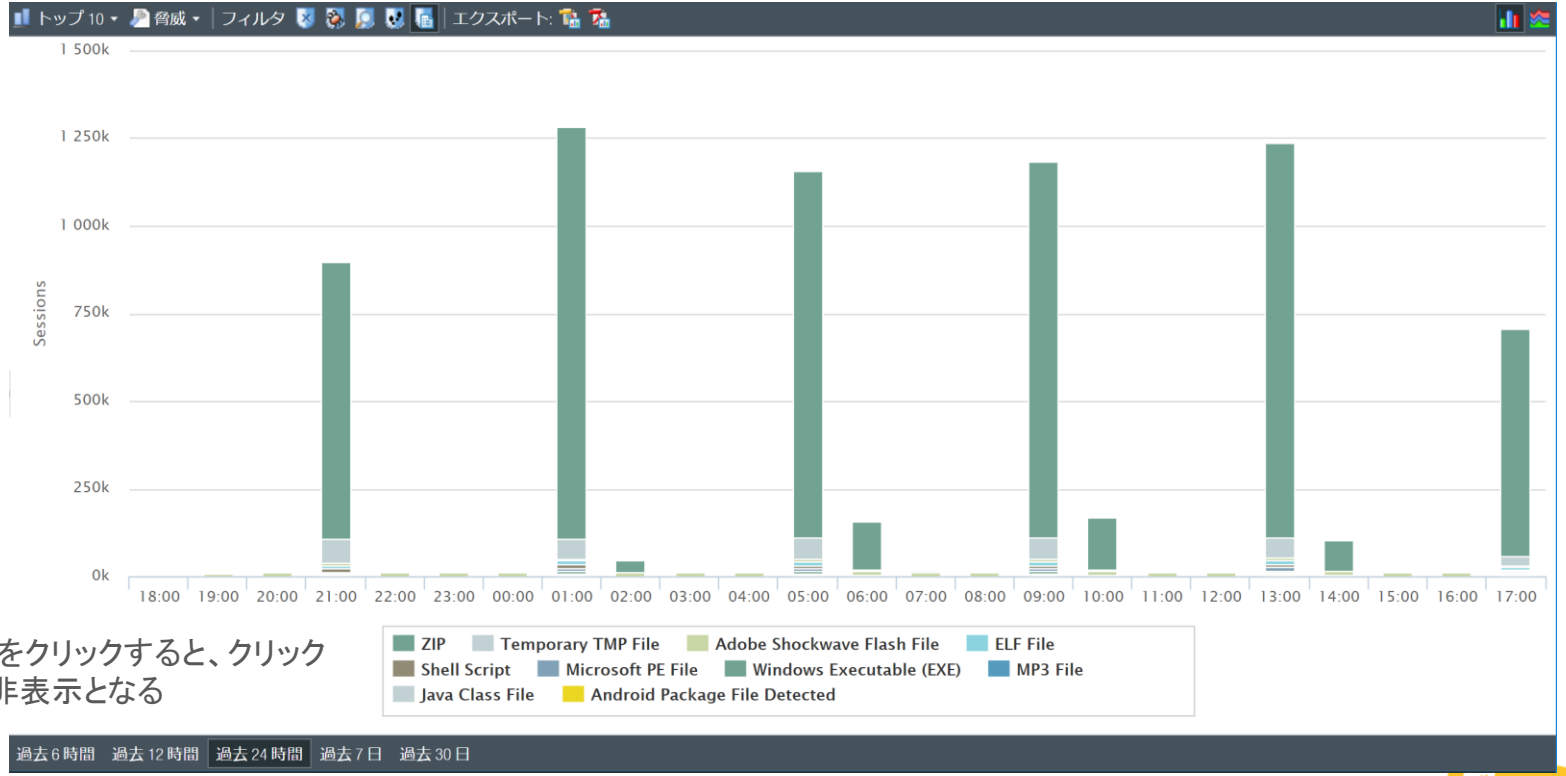
攻撃に利用された
ファイルタイプを表示

表示された表をPNGで
エクスポート

表示された表をPDFで
エクスポート

脅威情報（ファイル）の表示例

攻撃に利用されているファイルタイプを分析



該当のファイルをクリックすると、クリックしたファイルが非表示となる

THANK YOU