TSOC Managed Security Service 分析レポートサンプル

データ範囲: 2018-09-01 00:00 2018-11-30 23:59 JST (FAZ local)

お客様配布用 (Sample Rev.1)

このレポートの分析に用いたFortiGateのログ対象期間です。通常は 1か月分のログを分析し、レポートを発行致します。

セキュリティ分析レポート

トークネット
TOHKnet
つなげる力を、明日のために。

このレポートは、お客様がご利用されている「FortiGate」製品のログに基づき、「TSOC（Total Security Operation Center）」で包括的に実施したセキュリティ分析の結果をまとめたものです。お客様のネットワーク環境における各種脅威や、ネットワーク利用状況、ウェブアクセス状況、VPN接続状況、FortiGateの利用状況等について記載しております。

このMSSレポートはサンプルになります。そのため、通信元や通信先、ユーザなどの固有情報については非表示または無関係な値に表示を変更しております。あらかじめご了承願います。

TSOCのMSSレポートは、Fortinet社が提供するFortiGuardの各種サービスを用いて分析しており、攻撃などの判定基準はFortiGuardの情報に基づいています。ここでは、FortiGuardが提供している各種サービスについて説明しています。

FortiGuardのセキュリティとサービス

FortiGateのメーカーであるFortinet社は、日本を含めた世界各地にセキュリティ研究部門（FortiGuard Labs）を設置し、日々進化する脅威を世界規模で監視しています。世界中で発生するあらゆる脅威に対する情報を一元管理し、セキュリティのエキスパートたちがその対策のための研究と開発に日夜取り組んでいます。24時間365日の運用体制で検知した脅威は、「FortiGuard」というセキュリティサービスとして、契約されたお客様のFortiGateに以下の機能を提供しています。また、FortiGuardから提供される各種情報は、本レポートにおけるセキュリティ分析にも用いられています。

次世代アプリケーション制御＆IPS

アプリケーション制御と侵入防止（IPS）は、FortiGateのような次世代のファイアウォールにおける基盤となるセキュリティ技術です。世界中の組織はFortiGuardアプリケーション制御とIPSをFortiGateプラットフォームで利用してアプリケーションを管理し、ネットワークの侵入を阻止しています。

ウェブフィルタリング

FortiGuard Labsは、毎日毎分膨大なURL分類要求を処理し、悪意のあるWebサイトへのアクセスをブロックします。Webフィルタリングサービスは各種Webサイトを調査し、新しいURL評価を提供します。

アンチウイルスとモバイルセキュリティ

FortiGuard Labsは毎日1分ごとに、PC、モバイルおよびIoTプラットフォームを対象とした約95,000のマルウェアプログラムを駆除しています。FortiGuardアンチウィルスは、特許取得済みのテクノロジーにより、現在と将来の数千種類のマルウェアを単一のシグネチャで識別し、セキュリティの有効性とパフォーマンスを最適化します。

アンチスパム

FortiGuard Labsは毎日1分ごとに約21,000件のスパムメールをブロックし、毎週、約4,600件の新しいスパムルールと更新されたスパムルールを配信しています。 電子メール送信は、企業に対する先進的な攻撃の第一段階です。このため、スパム対策は企業のセキュリティ戦略において重要な部分となります。

高度な脅威防止（FortiSandbox）

世界中の何千もの組織が、FortiSandboxを活用して高度な脅威を特定しています。FortiSandboxは、業界テストでNSS Labsの違反検知システムの推奨評価を一貫して受けており、2015年にはNSS Labsテストで97%以上の違反検知率を達成しました。
※Sandobx=外部から受け取ったプログラムを保護された領域で動作させることでシステムが不正に操作されるのを防ぐセキュリティ機構。

IPレピュテーション

FortiGuard Labsは毎日毎分約32,000のボットネット、C＆C通信をブロックしています。重要なのはマルウェアなどの脅威がC＆Cサーバーと通信するときで、新たなマルウェアをダウンロードしたり、データを盗み外部に流出させたりするリスクがあります。IPとドメインに対する評価は、C&Cサーバとの通信をブロックし、企業におけるマルウェア感染の被害を縮小させます。

※ お客様のFortiGateにて、上記機能を含む各種設定及び分析に関わる機能が未設定または無効の場合、TSOCにて分析が行えないため分析結果が表示されない（N/Aやログデータが存在しない表記になる）場合があります。

レポート内に分析結果が表示されない項目がある場合、ご利用されているFortiGateでその項目に関する機能で必要な設定されていない、または無効になっている可能性がありますので、その場合お客様のFortiGateの設定をご確認下さい。

Copyright 2018 HighTechSystem Co., Ltd.

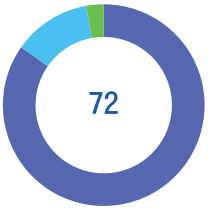
脅威の検知概要

分析結果の概要になります。このページの内容を以前のレポートと比較して頂くことで、全体の傾向が把握できます。

脅威検知種類数（脅威区分別）

検知した脅威の種類数になります。どの種類の脅威（例えば「Attack（攻撃）」や「Malware（マルウェア）」等）が多かったのかを把握できます。

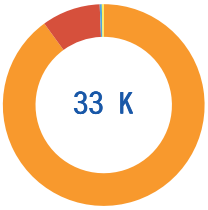
Critical & High Intrusion Attack	61
Malware & Botnet C&C	9
Malicious & Phishing Sites	2



脅威検知数（危険度別）

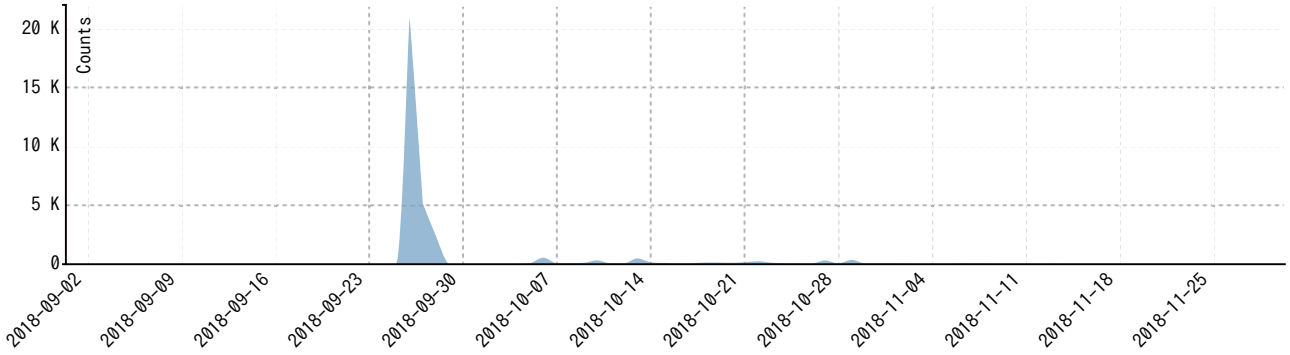
危険度別の検知した脅威数になり、どの危険度の脅威が多かったのかが把握できます。危険度は高い順で「Critical」「High」「Medium」「Low」の順になります。

High	30,137
Critical	3,147
Low	113
Medium	101



脅威検知数（時系列）

時系列で、いつ、どのくらいの数の脅威を検知したのかを示すグラフです。脅威の検知状況の推移が把握できます。突出している日があった場合は、異常や変化点がなかったかの確認が推奨されます。



項目	結果	説明
攻撃検知	33,405	サイバー攻撃の検知数です（成否問わず）。
アプリケーションの脆弱性を突いた攻撃	70	アプリの脆弱性を突いた攻撃の検知数です（成否問わず）。
VPNログイン成功	81	ユーザがVPNログインに成功した回数です。
VPNログイン失敗	26	ユーザがVPNログインに失敗した回数です。
マルウェア及びボットネット検知	9	マルウェア及びボットネット通信の可能性が疑われる件数です。
高リスクアプリケーション通信	2	危険なアプリケーション通信の可能性が疑われる件数です。
悪意のあるウェブサイト閲覧	0	悪意のあるウェブサイト閲覧の可能性が疑われる件数です。
フィッシングサイト閲覧	0	フィッシング（詐欺）サイト閲覧の可能性が疑われる件数です。
FortiGateのCPU使用率（平均）	0.41%	平均値が高い場合は、FortiGateの性能不足等が疑われます。
FortiGateのMemory使用率（平均）	47.27%	平均値が高い場合は、FortiGateの性能不足等が疑われます。
最大通信元ホスト	IPv4-43345	不明な通信元の場合は、詳細調査が推奨されます。
最大通信先ホスト	IPアドレスまたはホスト名	不明な通信先の場合は、詳細調査が推奨されます。
最大トラフィックウェブサイト	cdimage.ubuntulinux.jp	不明や非許可の通信先の場合は、詳細調査が推奨されます。
最大トラフィックアプリケーション	アプリ名またはプロトコル	不明や非許可のアプリ等の場合は、詳細調査が推奨されます。

脅威の主な項目と検知した結果及び説明になります。この表は管理者の方に把握して頂きたい情報をまとめたものになり、本レポート内の各分析項目で詳細を確認することができます。

Copyright 2018 HighTechSystem Co., Ltd.

脅威の検知概要説明

分析結果の概要についての説明になります。検知概要の各項目について、どういう視点で確認すべきかなどについて説明しています。

・攻撃検知…成否を問わない攻撃の検知総数です。FortiGateの設定が適切か、脆弱性対策を行っているかの確認が推奨されます。
・アプリの脆弱性を突いた攻撃…成否を問わない脆弱性攻撃の検知総数です。脆弱性対策を行っているかの確認が推奨されます。
・VPNログイン成功…VPN利用者数から見て著しく多い場合は、利用状況（正規ログインか）等の確認が推奨されます。
・VPNログイン失敗…VPN利用者数から見て著しく多い場合は、正規利用者の失敗か第三者の攻撃かの確認が推奨されます。

不正侵入、マルウェア、ボットネット、悪意のあるアプリケーション等は、企業ネットワークにとって大きなリスクを伴います。例えば、悪意のあるアプリケーションは、企業にとって重要なデータにアクセスを試み、情報そのものを盗み出したり、重要なファイルを勝手に開けないようにして身代金を要求したりします。こうした脅威が検知された場合、企業は適切な情報セキュリティ対策を講じる必要があります。また、インターネットから企業ネットワークへのVPN接続を許可している場合は、VPNユーザーに対して大量にログイン失敗の記録があったり、許可していないはずなのにログイン成功の記録があったりしないか確認が必要です。これを怠ると、不正侵入や情報漏えいのリスクが高まりますので、企業の管理者はVPN接続が悪用されていないかに注意を払わなければなりません。

◆該当項目

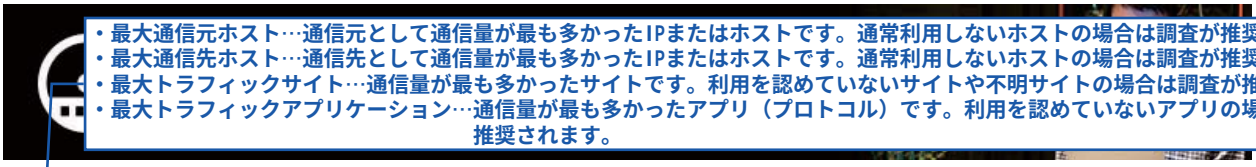
攻撃検知	33,405	アプリケーションの脆弱性を突いた攻撃	70
VPNログイン成功	81	VPNログイン失敗	26

・マルウェア及びボットネット検知…マルウェア、ボットの感染が疑われた件数です。検知時はウイルススキャン等が推奨されます。
・高リスクアプリケーション通信…リスクが高いアプリの使用が疑われた件数です。非許可アプリの使用がないか確認が推奨されます。
・悪意のあるウェブサイト閲覧…リスクの高いサイト閲覧が疑われた件数です。Webフィルタリングの有効化や設定確認が推奨されます。
・フィッシングサイト閲覧…フィッシングサイトの閲覧が疑われた件数です。Webフィルタリングの有効化や設定確認が推奨されます。
・FortiGateのCPU使用率（平均）…恒常的に高い場合は、設定が不適切、あるいは通信量に対して性能不足の可能性があります。
・FortiGateのMemory使用率（平均）…恒常的に高い場合は、設定が不適切、あるいは通信量に対して性能不足の可能性があります。

企業ネットワークの利用者による、業務と無関係なアプリケーションの利用やウェブ閲覧は、不要な通信により企業のネットワーク帯域を消費し、生産性を低下させる可能性があります。また、犯罪に関わるような危険なウェブ閲覧や、P2Pアプリケーション（インターネット上で不特定多数とファイル共有するソフト）の利用など、法律に抵触する恐れのある行為についても、企業は注意を払わなければなりません。さらに、業務による必要な通信であっても、利用しているFortiGateの性能を超えるような通信量になった場合、通信速度の低下を招いたり、セキュリティ機能が正常に働かなくなったりする恐れがあります。企業の管理者は、企業の生産性を維持するためにも、ネットワークの利用状況を把握し、適切に管理する必要があります。

◆該当項目

マルウェア及びボットネット検知	9	高リスクアプリケーション通信	2
悪意のあるウェブサイト閲覧	0	フィッシングサイト閲覧	0
FortiGateのCPU使用率（平均）	0.41%	FortiGateのMemory使用率（平均）	47.27%



・最大通信元ホスト…通信元として通信量が最も多かったIPまたはホストです。通常利用しないホストの場合は調査が推奨されます。
・最大通信先ホスト…通信先として通信量が最も多かったIPまたはホストです。通常利用しないホストの場合は調査が推奨されます。
・最大トラフィックサイト…通信量が最も多かったサイトです。利用を認めていないサイトや不明サイトの場合は調査が推奨されます。
・最大トラフィックアプリケーション…通信量が最も多かったアプリ（プロトコル）です。利用を認めていないアプリの場合は調査が推奨されます。

ネットワークトラフィックは、インターネットや企業ネットワーク上を流れるデータ量を示すものです。企業にとって意図しない通信（例えば外部からの攻撃やマルウェア感染による不正アクセス、利用者による企業ネットワークの不正利用など）が行われていないか、企業の管理者は注意を払う必要があります。また、トラフィック量が多いホストについては、業務上必要な通信によるものかどうかも確認する必要があります。

◆該当項目

最大通信元ホスト	最大通信先ホスト
IPv4-43345	ホスト名またはIPアドレス
最大トラフィックウェブサイト	最大トラフィックアプリケーション
cdimage.ubuntulinux.jp	アプリ名またはプロトコル

Copyright 2018 HighTechSystem Co., Ltd.

脅威分析

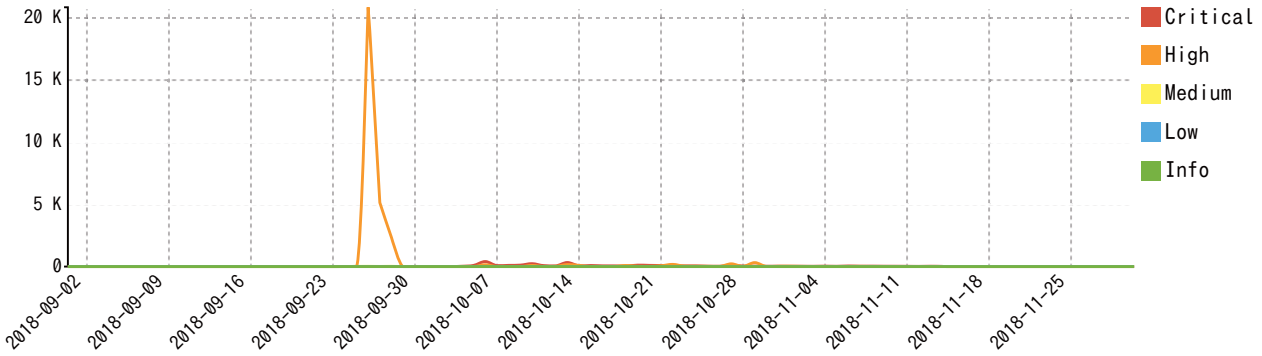
このセクションでは、お客様のネットワークにおいて検知された各種脅威（不正侵入、マルウェア、ボットネット、リスクのあるアプリケーション、ゼロデイ攻撃）についての分析結果を報告します。不正侵入やサイバー攻撃が成功した場合、企業の存続に関わるような事態に陥る可能性があります。サイバー攻撃により自社のサーバが停止に追い込まれ、業務停止による損害が発生するだけではなく、場合によっては自社のIT設備が第三者へのサイバー攻撃に悪用されるケースもあります。自社のセキュリティ対策に不備があった場合は、被害を与えてしまった相手から損害賠償を請求されることも考えられますので、企業の管理者は自社のネットワーク、サーバに対する脅威を可視化し、自社のIT設備が置かれている環境を把握して、適切な対処をすることが求められます。

侵入（攻撃）検知

侵入（攻撃）検知とは、お客様のネットワークへの不正なアクセスの兆候を検知するものです。ファイアウォールの機能だけでは防ぐことができない、不正プログラムの侵入や行為を発見することができます。侵入検知で検出された項目を分析することで、どういう攻撃内容で侵入を試みられているのかや、どういうウイルスが送られてきているかなどの情報を把握することができます。また、通信に利用されているリスクの高いアプリケーションも検知しますので、企業の管理者は自社のネットワークがどういう脅威にさらされているのかを多角的に見て、適切な対処をすることが求められます。

危険度別攻撃検知数の推移

危険度別で、攻撃が何件位あったのかの時系列グラフです。突出している時期があった場合は、そのタイミングで何か変化点や問題が無かったかの確認が推奨されます。また、「Critical」の検知数が多い場合は、高度な攻撃等にさらされている状況につき、FortiGateの適切な設定や、各種サイバー攻撃対策を行っているかの確認が推奨されます。



脅威及び危険度別攻撃検知数

脅威及び４段階の危険度別でどのくらい攻撃を検知したかの統計です。危険度「Critical」及び「High」の項目が多い脅威については、詳細項目で内容を把握し、対策を行っているかの確認が推奨されます。

Threat Type	Critical	High	Medium	Low
Botnets	24	0	0	0
Intrusions	3,054	30,137	101	113
Malware	69	0	0	0

攻撃元IPまたはホスト名TOP20（攻撃検知数順）

攻撃検知が多かった攻撃元IPまたはホスト名です。正規の通信元でなければ、一般的にはFortiGateで通信を恒久的に遮断するなどの対処が推奨されます。

Attack Source	Counts	Critical	High	Medium	Percent of Total Attacks
ホスト名またはIPアドレス	24,161				78.92%
	3,226				10.54%
	1,094				3.57%
	320				1.05%
	207				0.68%
	192				0.63%
	167				0.55%
	129				0.42%
	122				0.40%
	115				0.38%
	101				0.33%
	101				0.33%
	101				0.33%
	101				0.33%
	101				0.33%
	100				0.33%
	92				0.30%
	65				0.21%
	61				0.20%
	57				0.19%

Copyright 2018 HighTechSystem Co., Ltd.

FortiGateでブロックした攻撃のうち件数が多かった上位20種類です。
数が多いものは流行しているまたは無差別攻撃、もしくは意図的に狙った攻撃の可能性があります。

ブロックした攻撃TOP20（危険度→ブロック数順）

Intrusion Name	Intrusion Type	Severity	Counts
MS.IIS.WebDAV.PROPFIND.ScStoragePathFromUrl.Buffer.Overflow	Buffer Errors	Critical	394
D-Link.DSL-2750B.CLI.OS.Command.Injection	OS Command Injection	Critical	46
Netcore.Netis.Devices.Hardcoded.Password.Security.Bypass	Improper Authentication	Critical	42
Dasan.GPON.Remote.Code.Execution	OS Command Injection	Critical	27
Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution	Code Injection	Critical	19
Drupal.Core.Form.Rendering.Component.Remote.Code.Execution	OS Command Injection	Critical	5
Joomla.Core.Session.Remote.Code.Execution	Code Injection	Critical	3
TUTOS.CMD.Module.Unauthenticated.Remote.Command.Execution	OS Command Injection	Critical	1
NETGEAR.DGN1000.CGI.Unauthenticated.Remote.Code.Execution	Code Injection	Critical	1
OpenSSL.Heartbleed.Attack	Information Disclosure	Critical	1
Gh0st.Rat.Botnet		Critical	1
Zivif.PR115-204-P-RS.Web.Cameras.Credentials.Disclosure	Improper Authentication	Critical	1
Avtech.Devices.HTTP.Request.Parsing.Multiple.Vulnerabilities	OS Command Injection	High	133
Wordpress.Login.Brute.Force	Anomaly	High	46
Linksys.Routers.Administrative.Console.Authentication.Bypass	Permission/Priviledge/Access Control	High	24
HTTP.URI.SQL.Injection	SQL Injection	High	21
HTTP.Request.URI.Directory.Traversal	Path Traversal	High	20
PHP.Malicious.Shell	Malware	High	17
FTP.Login.Brute.Force	Anomaly	High	9
China.Chopper.Web.Shell.Client.Connection	Anomaly	High	3

Copyright 2018 HighTechSystem Co., Ltd.

攻撃先として検知されたIPまたはホストの上位20個です。検知数が多いIPまたはホストは、攻撃先として狙われている可能性があります。

攻撃先IPまたはホスト名TOP20（攻撃検知数順）

Attack Victim	Counts	Critical	High	Medium	Percent of Total Attacks
ホスト名またはIPアドレス	28,573				85.83%
	887				2.66%
	837				2.51%
	636				1.91%
	518				1.56%
	411				1.23%
	226				0.68%
	220				0.66%
	181				0.54%
	181				0.54%
	120				0.36%
	111				0.33%
	107				0.32%
	100				0.30%
	91				0.27%
	82				0.25%
	6				0.02%
	3				0.01%
	1				0.00%
	1				0.00%

どの種類の攻撃が多かったのか、攻撃タイプの上位20種類です。検知数が多い攻撃については、対策を行っているかの確認が推奨されます。

攻撃タイプ別検知数TOP20

Intrusion Type	Counts
Anomaly	28,211
OS Command Injection	1,496
Improper Authentication	797
Buffer Errors	767
Path Traversal	699
SQL Injection	679
Code Injection	459
Malware	148
Permission/Priviledge/Access Control	66
Other	23
Information Disclosure	17
DoS	6
Resource Management Errors	2

Copyright 2018 HighTechSystem Co., Ltd.

危険度【Critical】の攻撃検知数TOP20

危険度が最も高い「Critical」と判別された攻撃の検知数上位20種類です。危険度最高レベルでかつ件数が多い内容の攻撃につき、対策を行っているかの確認が推奨されます。また、脆弱性を突いた攻撃の場合は「CVE-ID」で脆弱性情報が検索できます。

Attack Name	CVE-ID	Intrusion Type	Counts
Netcore.Netis.Devices.Hard coded.Password.Security.Bypass		Improper Authentication	796
MS.IIS.WebDAV.PROPFIND.ScS toragePathFromUrl.Buffer.Overf low	CVE-2017-7269	Buffer Errors	754
Bash.Function.Definitions. Remote.Code.Execution	CVE-2014-6271,CVE-2014-6277,CV E-2014-6278,CVE-2014-7169,CVE-2014-7186,CVE-2014-7187	OS Command Injection	705
Dasan.GPON.Remote.Code.Exe cution	CVE-2018-10561,CVE-2018-10562	OS Command Injection	241
Apache.Struts.2.Jakarta.Mu ltipart.Parser.Code.Execution	CVE-2017-5638	Code Injection	210
D-Link.DSL-2750B.CLI.OS.Co mmand.Injection		OS Command Injection	151
Drupal.Core.Form.Rendering .Component.Remote.Code.Executi on	CVE-2018-7600	OS Command Injection	72
Gh0st.Rat.Botnet			35
Oracle.WebLogic.Server.wls -wsat.Component.Code.Injection	CVE-2017-3506,CVE-2017-10271	Code Injection	24
Joomla.Core.Session.Remote .Code.Execution	CVE-2015-8562	Code Injection	15
NETGEAR.DGN1000.CGI.Unauth enticated.Remote.Code.Executio n		Code Injection	15
OpenSSL.Heartbleed.Attack	CVE-2014-0160	Information Disclosure	11
WebNMS.Framework.Directory .Traversal	CVE-2016-6600,CVE-2016-6601	Path Traversal	6
Zyxel.Router.nslookup.Comm and.Injection	CVE-2017-6884	OS Command Injection	5
TUTOS.CMD.Module.Unauthent icated.Remote.Command.Executio n	CVE-2008-0148,CVE-2008-0149	OS Command Injection	4
PHPUnit.Eval-stdin.PHP.Rem ote.Code.Execution	CVE-2017-9841	Code Injection	3
Apache.Struts.2.DefaultAct ionMapper.Remote.Command.Execu tion	CVE-2013-2251	Other	2
Apache.Commons.Collection. InvokerTransformer.Code.Execut ion	CVE-2015-4852,CVE-2015-6420,CV E-2015-6555,CVE-2015-6576,CVE-2016-0788,CVE-2016-3427,CVE-2016-3642,CVE-2016-4385,CVE-2016-8735,CVE-2016-9498,CVE-2017-5645,CVE-2017-5792,CVE-2018-10611	OS Command Injection	2
Apache.Struts.2.REST.Plugi n.Remote.Code.Execution	CVE-2016-4438,CVE-2017-12611	Code Injection	1
Zivif.PR115-204-P-RS.Web.C ameras.Credentials.Disclosure	CVE-2017-17106	Improper Authentication	1

Copyright 2018 HighTechSystem Co., Ltd.

危険度が最も高い「Critical」と判別された攻撃の検知数上位20種類の詳細情報です。「Reference」に記載があるURLにて攻撃の詳細情報（英語）が確認できます。

危険度【Critical】の攻撃に関する参考情報TOP20

Attack Name	Reference	Total Num
Netcore.Netis.Devices.Hardcoded.Password.Security.Bypass	http://www.fortinet.com/ids/VID42781	796
MS.IIS.WebDAV.PROPFIND.ScStoragePathFromUrl.Buffer.Overflow	http://www.fortinet.com/ids/VID43844	754
Bash.Function.Definitions.Remote.Code.Execution	http://www.fortinet.com/ids/VID39294	705
Dasan.GPON.Remote.Code.Execution	http://www.fortinet.com/ids/VID46083	241
Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution	http://www.fortinet.com/ids/VID43745	210
D-Link.DSL-2750B.CLI.OS.Command.Injection	http://www.fortinet.com/ids/VID46176	151
Drupal.Core.Form.Rendering.Component.Remote.Code.Execution	http://www.fortinet.com/ids/VID45752	72
Gh0st.Rat.Botnet	http://www.fortinet.com/ids/VID38503	35
Oracle.WebLogic.Server.wls-wsat.Component.Code.Injection	http://www.fortinet.com/ids/VID45334	24
NETGEAR.DGN1000.CGI.Unauthenticated.Remote.Code.Execution	http://www.fortinet.com/ids/VID44738	15
Joomla.Core.Session.Remote.Code.Execution	http://www.fortinet.com/ids/VID41851	15
OpenSSL.Heartbleed.Attack	http://www.fortinet.com/ids/VID38315	11
WebNMS.Framework.Directory.Traversal	http://www.fortinet.com/ids/VID42836	6
Zyxel.Router.nslookup.Command.Injection	http://www.fortinet.com/ids/VID46494	5
TUTOS.CMD.Module.Unauthenticated.Remote.Command.Execution	http://www.fortinet.com/ids/VID46564	4
PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	http://www.fortinet.com/ids/VID45765	3
Apache.Commons.Collection.InvokerTransformer.Code.Execution	http://www.fortinet.com/ids/VID41663	2
Apache.Struts.2.DefaultActionMapper.Remote.Command.Execution	http://www.fortinet.com/ids/VID36453	2
WordPress.Marketplace.wpmp_pp_ajax_call.Remote.Code.Execution	http://www.fortinet.com/ids/VID45621	1
Zivif.PR115-204-P-RS.Web.Cameras.Credentials.Disclosure	http://www.fortinet.com/ids/VID45492	1

Copyright 2018 HighTechSystem Co., Ltd.

危険度が二番目に高い「High」と判別された攻撃の検知数上位20種類です。危険度が二番目に高いレベルでかつ件数が多い攻撃につき、Criticalに次いで対策を行っているかの確認が必要です。脆弱性を突いた攻撃の場合は「CVE-ID」で脆弱性情報が検索できます。

危険度【High】の攻撃検知数TOP20

Attack Name	CVE-ID	Intrusion Type	Counts
Wordpress.Login.Brute.Force	CVE-2009-2335	Anomaly	28,118
HTTP.Request.URI.Directory.Traversal	CVE-2001-0308,CVE-2017-10974,CVE-2018-11137	Path Traversal	684
HTTP.URI.SQL.Injection		SQL Injection	676
Avtech.Devices.HTTP.Request.Parsing.Multiple.Vulnerabilities		OS Command Injection	300
PHP.Malicious.Shell		Malware	73
PHP.CGI.Argument.Injection	CVE-2012-1823,CVE-2012-2311	Code Injection	58
Linksys.Routers.Administrative.Console.Authentication.Bypass		Permission/Priviledge/Access Control	56
China.Chopper.Web.Shell.Client.Connection		Anomaly	48
Adobe.XML.Entity.Injection	CVE-2009-3960	Other	19
PHP.URI.Code.Injection		Code Injection	11
FTP.Login.Brute.Force		Anomaly	9
Narcissus.Image.Configuration.Remote.Command.Execution		OS Command Injection	7
SSLv2.Openssl.Get.Shared.Ciphers.Overflow.Attempt	CVE-2006-3738	Buffer Errors	6
Ektron.XSLT.Transform.Remote.Code.Execution	CVE-2012-5357	Code Injection	5
Log1.CMS.WriteInfo.PHP.Code.Injection	CVE-2011-4825	Code Injection	5
DataLife.Engine.Catlist.Parameter.PHP.Code.Injection	CVE-2013-1412	Code Injection	5
VACRON.CCTV.Board.CGI.cmd.Parameter.Command.Execution		OS Command Injection	4
MS.IE.FTP.Client.Folder.Traversal	CVE-2004-1376	Path Traversal	4
PhpMoAdmin.moadmin.php.Unauthenticated.Remote.Code.Execution	CVE-2015-2208	Code Injection	4
FTP.USER.Command.Overflow	CVE-1999-0256,CVE-2000-0479,CVE-2002-0126,CVE-2005-3683,CVE-2006-2212,CVE-2013-5680	Buffer Errors	4

危険度が二番目に高い「High」と判別された攻撃の検知数上位20種類の詳細情報です。「Reference」に記載があるURLにて攻撃の詳細情報（英語）が確認できます。

危険度【High】の攻撃に関する参考情報TOP20

Attack Name	Reference	Total Num
Wordpress.Login.Brute.Force	http://www.fortinet.com/ids/VID29519	28,118
HTTP.Request.URI.Directory.Traversal	http://www.fortinet.com/ids/VID10604	684
HTTP.URI.SQL.Injection	http://www.fortinet.com/ids/VID15621	676
Avtech.Devices.HTTP.Request.Parsing.Multiple.Vulnerabilities	http://www.fortinet.com/ids/VID43635	300
PHP.Malicious.Shell	http://www.fortinet.com/ids/VID44580	73
PHP.CGI.Argument.Injection	http://www.fortinet.com/ids/VID31752	58
Linksys.Routers.Administrative.Console.Authentication.Bypass	http://www.fortinet.com/ids/VID44582	56
China.Chopper.Web.Shell.Client.Connection	http://www.fortinet.com/ids/VID37268	48
Adobe.XML.Entity.Injection	http://www.fortinet.com/ids/VID18162	19
PHP.URI.Code.Injection	http://www.fortinet.com/ids/VID15463	11
FTP.Login.Brute.Force	http://www.fortinet.com/ids/VID22909	9
Narcissus.Image.Configuration.Remote.Command.Execution	http://www.fortinet.com/ids/VID33932	7
SSLv2.Openssl.Get.Shared.Ciphers.Overflow.Attempt	http://www.fortinet.com/ids/VID13227	6
Ektron.XSLT.Transform.Remote.Code.Execution	http://www.fortinet.com/ids/VID34126	5
DataLife.Engine.Catlist.Parameter.PHP.Code.Injection	http://www.fortinet.com/ids/VID34579	5
Log1.CMS.WriteInfo.PHP.Code.Injection	http://www.fortinet.com/ids/VID32153	5
FTP.USER.Command.Overflow	http://www.fortinet.com/ids/VID12923	4
VACRON.CCTV.Board.CGI.cmd.Parameter.Command.Execution	http://www.fortinet.com/ids/VID44754	4
MS.IE.FTP.Client.Folder.Traversal	http://www.fortinet.com/ids/VID30570	4
PhpMoAdmin.moadmin.php.Unauthenticated.Remote.Code.Execution	http://www.fortinet.com/ids/VID40243	4

Copyright 2018 HighTechSystem Co., Ltd.

ウェブアクセスの通信を使った攻撃の検知数上位20種類です。FortiGate配下にホームページサーバ等がある場合は、対策を行っているかの確認が推奨されます。

HTTP／HTTPSプロトコルを使った攻撃TOP20（危険度→攻撃検知数順）

Attack Name	Severity	Attack Counts
MS.IIS.WebDAV.PROPFIND.ScStoragePathFromUrl.Buffer.Overflow	Critical	754
Bash.Function.Definitions.Remote.Code.Execution	Critical	705
Dasan.GPON.Remote.Code.Execution	Critical	241
Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution	Critical	210
D-Link.DSL-2750B.CLI.OS.Command.Injection	Critical	151
Drupal.Core.Form.Rendering.Component.Remote.Code.Execution	Critical	72
Gh0st.Rat.Botnet	Critical	35
Oracle.WebLogic.Server.wls-wsat.Component.Code.Injection	Critical	24
NETGEAR.DGN1000.CGI.Unauthenticated.Remote.Code.Execution	Critical	15
Joomla.Core.Session.Remote.Code.Execution	Critical	15
WebNMS.Framework.Directory.Traversal	Critical	6
Zyxel.Router.nslookup.Command.Injection	Critical	5
TUTOS.CMD.Module.Unauthenticated.Remote.Command.Execution	Critical	4
PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	Critical	3
Apache.Struts.2.DefaultActionMapper.Remote.Command.Execution	Critical	2
Apache.Commons.Collection.InvokerTransformer.Code.Execution	Critical	2
Zivif.PR115-204-P-RS.Web.Cameras.Credentials.Disclosure	Critical	1
Apache.Struts.2.REST.Plugin.Remote.Code.Execution	Critical	1
WordPress.Marketplace.wpmp_pp_ajax_call.Remote.Code.Execution	Critical	1
Wordpress.Login.Brute.Force	High	28,118

Copyright 2018 HighTechSystem Co., Ltd.

マルウェア及びボットネット

お客様のネットワーク内に侵入し、お客様のコンピュータに損傷を引き起こしたり、お客様の情報を盗み取ったりする悪意のあるソフトウェアや悪意のあるコード（コンピュータに対する処理や指示）を総称して、「Malware（マルウェア）」と呼びます。マルウェアには複数の種類がありますが、このセクションではマルウェアのうち主に以下の3種類について分析した結果を報告します。

Virus（ウイルス、コンピュータウイルス）	コンピュータに感染して破壊活動（データの勝手な変更や削除）を行ったり、他のコンピュータへと感染を広げることで、その影響範囲を拡大させることを目的としたもの。
Spywware（スパイウェア）	コンピュータの利用者が閲覧したウェブの履歴や、実行した操作の内容、メールアドレスなどの個人情報を外部に送信することを目的としたもの。
Adware（アドウェア）	パソコン上で、宣伝や広告を表示させることを目的としたもの。種類によっては正常な利用の妨げとなったりする場合がある。

また、「Botnet（ボットネット）」とは、マルウェアの一種であるボットというプログラムをコンピュータに侵入させ、これに感染したコンピュータを大量に集めて犯罪等に悪用するネットワークを指します。マルウェアに感染したコンピュータが、このボットネットと通信することで、新たなマルウェアがダウンロードされて被害が拡大したり、遠隔操作等によりサイバー攻撃に加担させられたりするリスクがあります。ボットネットとの通信が認められた場合は、直ちに通信元コンピュータを突き止め、ボットネットから切り離して再接続されないよう対策を講じる必要があります。

マルウェア別検知数TOP20

マルウェアの検知数上位20種類です。「Victim」はマルウェア感染が疑われたホスト（IP）数、「Source」はマルウェア攻撃元の可能性があるホスト（IP）数、「Count」はそのマルウェアが検知された総数です。検知されている場合は、対象ホストのウイルススキャンが推奨されます。

Malware Name	Malware Type	Victim	Source	Count
W32/GenKryptik.CMCA!tr	Virus	1	2	53
Malware	Virus	1	1	24
a6d7af8ce2ae317d2fe637d0aca5fd971315cb7b	Virus	1	1	6
Riskware/Babylon	Spyware	1	1	4
XM/Agent.F01B!tr.dldr	Virus	1	1	2
91218a24505bf77a99347950647255c777f96595	Virus	1	1	1
EICAR_TEST_FILE	Virus	1	1	1
W32/Kryptik.GLKH!tr	Virus	1	1	1
92872b11bd9831783d4f5daa8204c05b6edff528	Virus	1	1	1

ホスト（IP）別マルウェア検知数TOP10

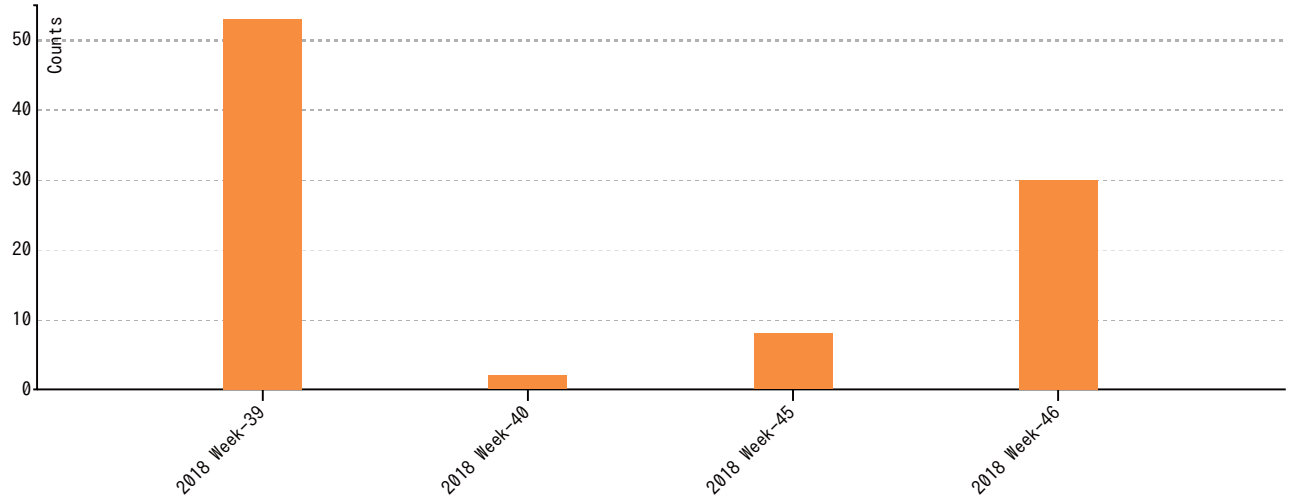
マルウェアの感染が疑われるホスト（IP）の上位10個です。記録されているホスト（IP）については、対象ホストのウイルススキャンが推奨されます。

Malware Source	Hostname (or IP)	Counts
IPv4-18338	ホスト名またはIPアドレス	49
IPv4-64340		24
IPv4-64340		6
IPv4-64340		4
IPv4-40641		4
IPv4-2216		2
IPv4-64340		1
IPv4-64340		1
IPv4-3857		1
IPv4-64340		1

Copyright 2018 HighTechSystem Co., Ltd.

ウイルス検知数の推移

ウイルスをいつ、どのくらい検知したのかの時系列データです。ウイルス検知状況の推移が確認できます。



スパイウェア別検知数TOP10

検知されたスパイウェアの検知数上位10種類です。検知されている場合は、ウイルス対策ソフトだけでなく、スパイウェア駆除ツールなども用いてスキャンすることが推奨されます。

Spyware Name	Occurrences
Riskware/Babylon	4

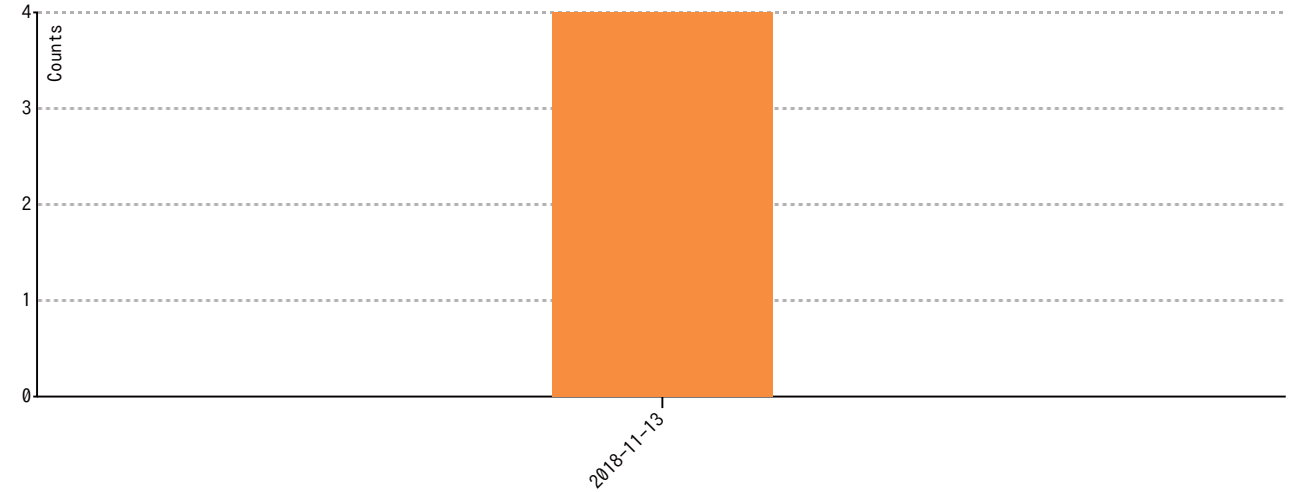
検知元別スパイウェアTOP10（検知数順）

スパイウェアが検知されたホスト（IP）の上位10個です。検知されたホストについては、スパイウェアの検査が推奨されます。

Spyware Victims	Occurrences
IPv4-64340	4

スパイウェア検知数の推移

いつ、どのくらいの数のスパイウェアが検知されたかの、時系列データです。スパイウェアの検知状況の推移が確認できます。



アドウェア別検知数TOP10

検知したアドウェアの検知数上位10種類です。検知されている場合は、ウイルス対策ソフトだけでなく、アドウェア駆除ツールなども用いてスキャンすることが推奨されます。

適合するログデータが指定期間内に存在しません

検知元別アドウェアTOP10（検知数順）

アドウェアが検知されたホスト（IP）の上位10個です。検知されたホストについては、アドウェアの検査が推奨されます。

適合するログデータが指定期間内に存在しません

Copyright 2018 HighTechSystem Co., Ltd.

アドウェア検知数の推移

いつ、どのくらいの数のアドウェアが検知されたかの、時系列データです。アドウェアの検知状況の推移が確認できます。

適合するログデータが指定期間内に存在しません

ボットネット検知数TOP10

検知されたボットネット通信の検知数上位10種類です。検知されている場合は、ウイルス対策ソフト等でスキャンすることが推奨されます。

適合するログデータが指定期間内に存在しません

ボットネット感染ホストTOP10

ボットネット通信が検知されたホスト（IP）の検知数上位10個です。検知されている場合は、ウイルス対策ソフト等でスキャンすることが推奨されます。

適合するログデータが指定期間内に存在しません

検出されたボットネット通信アプリケーション

検知されたボットネット通信を行っているアプリケーションの内容です。検知されている場合は、ウイルス対策ソフト等でスキャンすることが推奨されます。

適合するログデータが指定期間内に存在しません

ボットネット検知数の推移

いつ、どのくらいの数のボットネット通信が検知されたかの、時系列データです。ボットネット通信の検知状況の推移が確認できます。

適合するログデータが指定期間内に存在しません

Copyright 2018 HighTechSystem Co., Ltd.

アプリケーション

FortiGuardが判別しているアプリケーションの危険度評価です。数値が高いほど、使用時に危険を伴うアプリケーションであることを意味します。なお、数値が高いからといって全てが不正なアプリケーションとは限らず、正規利用のアプリケーションでも通信の特性上危険と判断される場合があります。

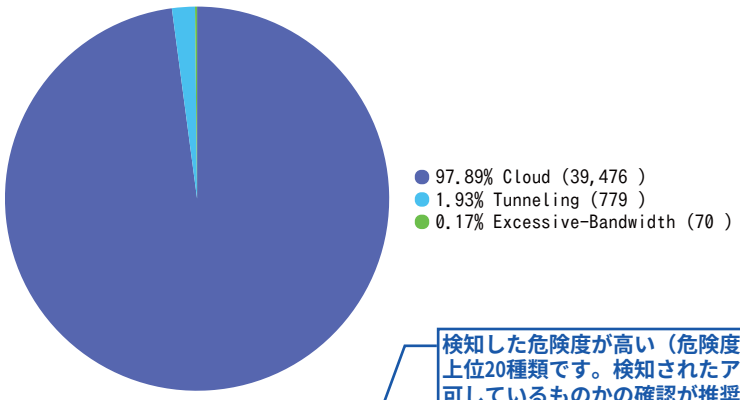
Application（アプリケーション）には、コンピュータ上で動作する際にインターネット接続を行うものが多数あります。これらのアプリケーションによる通信が企業の認めた通信ではない場合、不要なトラフィックにより企業のネットワークに負荷をかけている可能性や、そもそも利用を認めていないアプリケーションが利用されている可能性もあります。また、アプリケーションそのものに脆弱性が存在する場合、サイバー攻撃の足掛かりにされる可能性もありますので、企業の管理者は企業内のコンピュータでどういったアプリケーションが動作し、通信しているかを把握する必要があります。このセクションでは、FortiGateが検知したリスクの高いアプリケーションとその通信状況、脆弱性、及び電子メールの利用状況について分析した結果を報告します。

FortiGuardでは、アプリケーションの動作特性に基づいて、アプリケーションに1～5のリスク評価を割り当てています。リスク評価は、企業の管理者がリスクの高いアプリケーションを迅速に識別し、企業におけるアプリケーション制御ポリシーをより適切に判断するのに役立ちます。

危険度	特性	例
5 深刻	セキュリティ対策を回避する可能性のある、悪意のあるアプリケーション。	ボットネット、プロキシアプリケーション
4 高	マルウェアの感染やデータ漏洩を引き起こす可能性のあるアプリケーション。	P2P、リモートアクセスアプリケーション
3 注意	個人的なコミュニケーションに利用されるか、既知の脆弱性があるアプリケーション。	IM、Email、ストレージバックアップアプリケーション
2 警戒	トラフィックが大きいため、ネットワークに負荷がかかる可能性のあるアプリケーション。	ゲーム、ビデオ/オーディオアプリケーション
1 低	ビジネスアプリケーションまたはソフトウェア更新アプリケーション。	ビジネスアプリケーション、アップデート

アプリケーションリスクの割合

どういう区分のアプリケーションリスクが検知されたかの割合を示すデータです。割合が大きいもの程、利用されている割合も多いことを意味します。



検知した危険度が高い（危険度5または4）のアプリケーション通信の上位20種類です。検知されたアプリケーションについては、利用を許可しているものかの確認が推奨されます。

検知したハイリスクアプリケーション通信TOP20（リスク値→セッション数順）

Risk	Application Name	Category	Technology	User	Bandwidth	Session
5	Proxy.HTTP	Proxy	Network-Protocol	6	3.81 GB	779
5	Monero.Cryptocurrency.Miner	General.Interest	Client-Server	2	46.70 KB	14
4	Telnet	Remote.Access	Client-Server	82,632	0 B	224,480
4	Rsh	Remote.Access	Client-Server	51	131.56 KB	164,390
4	RDP	Remote.Access	Client-Server	2,348	9.90 KB	36,423
4	VNC	Remote.Access	Client-Server	951	0 B	4,908
4	Rexec	Remote.Access	Client-Server	46	0 B	463
4	Rlogin	Remote.Access	Client-Server	146	0 B	362

Copyright 2018 HighTechSystem Co., Ltd.

検知したアプリケーション通信の通信量上位30種類です。通信量が著しく多いアプリケーションは、正規の利用かどうかの確認や、ネットワーク帯域を圧迫していないかなどの調査が推奨されます。

検知したアプリケーション通信TOP30（通信量順）

Risk	Application Name	Category	Technology	User	Bandwidth	Session
5	Proxy.HTTP	Proxy	Network-Protocol	6	3.81 GB	779
3	HTTP.BROWSER	Web.Client	Browser-Based	15	2.07 GB	1,099
3	HTTPS.BROWSER	Web.Client	Browser-Based	19	2.03 GB	28,094
2	MS.Windows.Update	Update	Client-Server	13	1.55 GB	1,737
2	Microsoft.Office.Update	Update	Client-Server	3	803.43 MB	68
2	Microsoft.SharePoint	Collaboration	Browser-Based	3	674.05 MB	72
2	Google.Services	General.Interest	Browser-Based	16	490.21 MB	21,399
2	Zoom	Collaboration	Browser-Based,Client-Server	8	368.32 MB	194
1	Ubuntu.Update	Update	Client-Server	2	363.27 MB	136
3	Gmail	メール	Browser-Based	13	288.03 MB	981
3	HTTP.BROWSER_IE	Web.Client	Browser-Based	5	154.09 MB	2,216
2	Microsoft.Portal	Collaboration	Browser-Based	15	111.97 MB	1,830
2	Google.Accounts	General.Interest	Browser-Based	15	86.70 MB	10,471
2	HTTP.Download.Accelerator	General.Interest	Browser-Based	4	78.24 MB	10
2	Google.Play	General.Interest	Browser-Based	15	59.04 MB	8,390
2	HTTP.BROWSER_Chrome	Web.Client	Browser-Based	10	57.72 MB	1,993
2	HTTP.Segmented.Download	Network.Service	Browser-Based	6	53.37 MB	16
2	Yahoo.Services	General.Interest	Browser-Based	9	45.09 MB	1,285
3	Amazon.CloudFront	Cloud.IT	Browser-Based	8	40.29 MB	175
2	Google.Ads	General.Interest	Browser-Based	11	38.16 MB	1,839
2	Microsoft.Authentication	Collaboration	Browser-Based	11	37.02 MB	2,878
2	Ping	Network.Service	Network-Protocol	6	36.61 MB	272
3	Microsoft.Office.Online	Collaboration	Browser-Based,Client-Server	13	33.70 MB	959
3	SMTP	メール	Network-Protocol	607	32.98 MB	18,935
2	DNS	Network.Service	Network-Protocol	603	30.07 MB	321,708
3	SSL_TLSv1.2	Network.Service	Network-Protocol	14	24.20 MB	1,021
2	Amazon.Services	General.Interest	Browser-Based	8	23.73 MB	277
2	Slack	Collaboration	Browser-Based,Client-Server	3	20.40 MB	84
2	Microsoft.CDN	Collaboration	Browser-Based	7	17.56 MB	122
3	Amazon.AWS	Cloud.IT	Browser-Based	6	13.78 MB	295

Copyright 2018 HighTechSystem Co., Ltd.

アプリケーションの脆弱性を突いた攻撃の攻撃数上位30種類です。攻撃でターゲットにされている脆弱性への対策が行われているかの確認が推奨されます。また、「CVE-ID」を脆弱性情報サイトで検索すると脆弱性情報の詳細が確認できます。

アプリケーションの脆弱性を突いた攻撃TOP30（危険度→攻撃数順）

Severity	Malware Name	Malware Type	CVE-ID	Victim	Source	Count
5	Netcore.Netis.Devices.Hardcoded.Password.Security.Bypass	Improper Authentication		1	96	796
5	MS.IIS.WebDAV.PROPFIND.ScStoragePathFromUrl.Buffer.Overflow	Buffer Errors	CVE-2017-7269	15	678	754
5	Bash.Function.Definitions.Remote.Code.Execution	OS Command Injection	CVE-2014-6271,CVE-2014-6277,CVE-2014-6278,CVE-2014-7169,CVE-2014-7186,CVE-2014-7187	3	1	705
5	Dasan.GPON.Remote.Code.Execution	OS Command Injection	CVE-2018-10561,CVE-2018-10562	15	173	241
5	Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution	Code Injection	CVE-2017-5638	14	22	210
5	D-Link.DSL-2750B.CLI.OS.Command.Injection	OS Command Injection		15	126	151
5	Drupal.Core.Form.Rendering.Component.Remote.Code.Execution	OS Command Injection	CVE-2018-7600	5	5	72
5	Gh0st.Rat.Botnet			17	1	35
5	Oracle.WebLogic.Server.wls-wsat.Component.Code.Injection	Code Injection	CVE-2017-3506,CVE-2017-10271	13	17	24
5	Joomla.Core.Session.Remote.Code.Execution	Code Injection	CVE-2015-8562	7	11	15
5	NETGEAR.DGN1000.CGI.Unauthenticated.Remote.Code.Execution	Code Injection		3	7	15
5	OpenSSL.Heartbleed.Attack	Information Disclosure	CVE-2014-0160	5	5	11
5	WebNMS.Framework.Directory.Traversal	Path Traversal	CVE-2016-6600,CVE-2016-6601	1	2	6
5	Zyxel.Router.nslookup.Command.Injection	OS Command Injection	CVE-2017-6884	5	5	5
5	TUTOS.CMD.Module.Unauthenticated.Remote.Command.Execution	OS Command Injection	CVE-2008-0148,CVE-2008-0149	4	4	4
5	PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	Code Injection	CVE-2017-9841	2	3	3
5	Apache.Struts.2.DefaultActionMapper.Remote.Command.Execution	Other	CVE-2013-2251	1	1	2
5	Apache.Commons.Collection.InvokerTransformer.Code.Execution	OS Command Injection	CVE-2015-4852,CVE-2015-6420,CVE-2015-6555,CVE-2015-6576,CVE-2016-0788,CVE-2016-3427,CVE-2016-3642,CVE-2016-4385,CVE-2016-8735,CVE-2016-9498,CVE-2017-5645,CVE-2017-5792,CVE-2018-10611	1	1	2
5	Zivif.PR115-204-P-RS.Web.Cameras.Credentials.Disclosure	Improper Authentication	CVE-2017-17106	1	1	1
5	Apache.Struts.2.REST.Plugin.Remote.Code.Execution	Code Injection	CVE-2016-4438,CVE-2017-12611	1	1	1
5	WordPress.Marketplace.wpmp_pp_ajax_call.Remote.Code.Execution	Code Injection	CVE-2014-9013	1	1	1
4	Wordpress.Login.Brute.Force	Anomaly	CVE-2009-2335	1	16	28,118
4	HTTP.Request.URI.Directory.Traversal	Path Traversal	CVE-2001-0308,CVE-2017-10974,CVE-2018-11137	7	10	684
4	HTTP.URI.SQL.Injection	SQL Injection		5	35	676
4	Avtech.Devices.HTTP.Request.Parsing.Multiple.Vulnerabilities	OS Command Injection		15	266	300
4	PHP.Malicious.Shell	Malware		4	9	73
4	PHP.CGI.Argument.Injection	Code Injection	CVE-2012-1823,CVE-2012-2311	10	6	58
4	Linksys.Routers.Administrative.Console.Authentication.Bypass	Permission/Priviledge/Access Control		5	47	56
4	China.Chopper.Web.Shell.Client.Connection	Anomaly		3	3	48
4	Adobe.XML.Entity.Injection	Other	CVE-2009-3960	3	1	19

Copyright 2018 HighTechSystem Co., Ltd.

SMTPやOP25Bなどのメール送信系の通信が検知されたホスト（IP）の検知数上位10個です。FortiGateの外側（インターネット側）からの通信だけでなく、FortiGateの内側（LAN）からの通信についても検知されます。大量に通信しているホストがある場合は、ウイルス感染やスパムメールの転送などが疑われます。

電子メール通信（SMTP／OP25B等）検知ホスト（IP） TOP10

Sender	Number of Emails
IPv4-2360	2,778
IPv4-21269	2,478
IPv4-57336	1,208
IPv4-44990	1,138
IPv4-40997	464
IPv4-52802	420
IPv4-7270	366
IPv4-61829	339
IPv4-46551	287
IPv4-28107	281

POP3やIMAPなどのメール受信系の通信が検知されたホスト（IP）の検知数上位10個です。インターネット側からの通信も検知されますので、外部でのメール受信を許可していない場合などは、調査が推奨されます。

電子メール通信（POP3／IMAP等）検知ホスト（IP） TOP10

Recipient	Number of Emails
IPv4-60331	367
IPv4-32657	366
IPv4-54230	363
IPv4-62501	326
IPv4-10162	243
IPv4-4619	242
IPv4-27672	231
IPv4-55761	164
IPv4-9113	156
IPv4-50341	156

Copyright 2018 HighTechSystem Co., Ltd.

ゼロデイ攻撃

「Zero-day Attack（ゼロデイ攻撃）」とは、アプリケーションの脆弱性を狙ったサイバー攻撃のうち、脆弱性に対する対応策（パッチ適用やバージョンアップ等）が存在しない欠陥を突く攻撃を指します。セキュリティ対策が実施出来ていない無防備な状態を攻撃されてしまうため、非常に厄介な攻撃であり、かつ従来のセキュリティ対策だけではその攻撃を検知することも困難な場合があります。FortiGateはこうしたゼロデイ攻撃に対して、FortiGuardサービスの1つである「FortiCloud Sandbox」を用いて未知のマルウェアを識別しますので、より高度な脅威からお客様のネットワークを保護することが可能です。このセクションでは、お客様のFortiGateにて検知されたゼロデイ攻撃についての分析結果を報告します。

※ お客様のFortiGateにてFortiCloud Sandboxの機能が未設定または無効の場合、TSOCにて分析が行えないため本セクションの分析結果が表示されない場合があります。

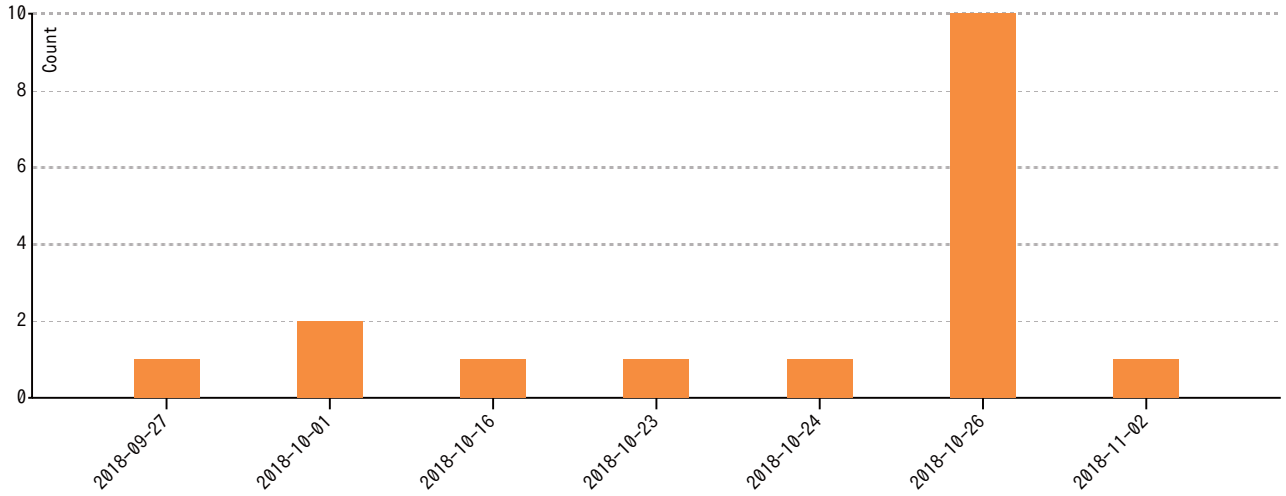
検知されたゼロデイ攻撃の可能性があるマルウェアの情報です。検知されている場合は、速やかに対策を行うことが推奨されます。

検知したゼロデイ攻撃マルウェア

適合するログデータが指定期間内に存在しません

FortiCloud Sandboxを利用している場合に、分析したファイル数の推移が確認できます。大量に分析されている場合は、ウイルス感染や外部からの攻撃の可能性が疑われます。

FortiCloud Sandboxで分析したファイル数の推移



Copyright 2018 HighTechSystem Co., Ltd.

FortiCloud Sandboxを利用している場合に、検知された悪意の可能性があるファイルの検知数上位30種類です。企業内で作成したファイル等が含まれている場合は、当該ファイルに未知のウイルスや不正なコードが仕掛けられていないか、調査が推奨されます。

FortiCloud Sandboxで検知した悪意の可能性があるファイルTOP30（検知数順）

File Name	MD5	Victim	Source
yads-iframe.html	c7acf8b52f5f23da60786e5731787ef19f4aed93dfde7630f8e48764147eefb3	6	1
s_retargeting.js	1f0c68ba09dc8891408f6b92fb17af1b9e77dbd7494144e22d90f7d06f71c049	6	1
bookmark_button.js	cf3900ce37ca5dfd6b803f241b00b753b421d0025f7194af04bd8716b893ee25	4	3
jquery-1.7.1.min.js	88171413fc76dda23ab32baa17b11e4fff89141c633ece737852445f1ba6c1bd	3	2
jquery.min.js	61c6caebd23921741fb5ffe6603f16634fca9840c2bf56ac8201e9264d6daccf	3	2
editorial-plain_html_text_areaclickable.min.js	77a07c8ed69df36639e1ef58d970687156c6ca439863250131166dc07db83a1d	3	1
SQB.js	269743a030f3826854e3d8e3b695d9d07c9828c4526fbc04c5f5f711f205e09e	3	1
v32_16.0.11001.20074.cab	c5ac747a8ab327c0447fd4df57e4283ec8a5ccaf943a61003fcce545f0e19c46	3	1
async_usersync.html	68fb304d37c3016c7346476f33b37bbae8765b51e3d06d88ef93732b354361a3	3	1
editorial-ultra_variable_free_image_responsive.min.js	d040e8c7c4946846be6a4bc9a3bd3998674f86c567b752adddc709b1e93cb8fc	3	1
banner.min.js	daba46c4a6a1309fb87f02201c9a8c5a922dae27c7c38bd417dcd98cc47fabce	3	1
jquery-2.1.1.min.js	b2ce8462d173fc92b60f98701f45443710e423af1b11525a762008ff2c1a0204	3	1
25378692_7154b6ec5b620523edb48d89051df96e82993cd8.cab	f946aa4fd4636c9f097b0eca18a0a3a22eae0ace3b54dd334f0550643a9c5e4a	3	1
iicon.min.js	49591830e7e54afde55cfbf952b97f1559d87df09293217e0e9fb9da4d7d2bf0	3	1
RestoreXidToMediaStorage.html	b1cf9494979497e2751b2b9933adb75ca049dbd1c9ee21a9981c630a83061cf1	3	1
thumbnail.min.js	135e0eba144cf6dcc01ec694c0dd814aae5ada38525352dfcc26cc4d55f481f6	3	1
yads_vimps.js	9f9bc54f15a1e78e4f46addf5179c3fd5f48123faa4acd33c96f318a69731902	3	1
b767e40b59c48c2ec52977502ac10e35b84c00600197162f42dd941b5095cafd.crxd	b767e40b59c48c2ec52977502ac10e35b84c00600197162f42dd941b5095cafd	2	2
mask.js	2b97ad55511b8459f18bc6818091d9a4bc4a8e71379d7873132867f14edaf5f2	2	2
popin_discovery5-min.js	30dc87fb603f59309c04dd7a8f501774ce56626b8d59db595016e492399d6ab4	2	2
jquery.js	24262baafef17092927c3dafe764aaa52a2a371b83ed2249cca7e414df99fac1	2	2
import.js	37da3742300c0803545ca6a4b26c8477f268dd65f3fbc9c65c5cd6fd24a5f78d	2	2
c2.js	43d2394b49d5c9665535f295d4ab2e81a9d6b641187971218813e6abb735ec5f	2	2
c7f2be6bc574328324264b38025ce5cc2d6939f1a9976ebb9251d40ad83d72e1.crxd	c7f2be6bc574328324264b38025ce5cc2d6939f1a9976ebb9251d40ad83d72e1	2	2
file_bit_article_bottom_ad.html	6f51bb51a88d5f8683986b2c1ad5302d26e0d85fdf8d8108e0cebced4ca41e51	2	2
5f2856968bedbbe7e52569cf89caef2d877d04738f6301aa718ae1ce147a4e70.crxd	5f2856968bedbbe7e52569cf89caef2d877d04738f6301aa718ae1ce147a4e70	2	2
bi.js	d85ef0c21bee5e2b88755a4bdf80bc4af215d1c0707237c3d1ced047de2b2d40	2	2
gnavi.js	9e3f39012b1ccee73d530a6eae16435b64834f6ecfe2317e90754e1713de77b2	2	2
25854b3557f8d4792217e2107ea302ece48c3eb4c1202cded3eeb844e0bffdea.crxd	25854b3557f8d4792217e2107ea302ece48c3eb4c1202cded3eeb844e0bffdea	2	2
26ca94ba6d9ed3ef18a65ffb3e8e95e54628b81f8594d1c7990f23e19b3a16db.crxd	26ca94ba6d9ed3ef18a65ffb3e8e95e54628b81f8594d1c7990f23e19b3a16db	2	2

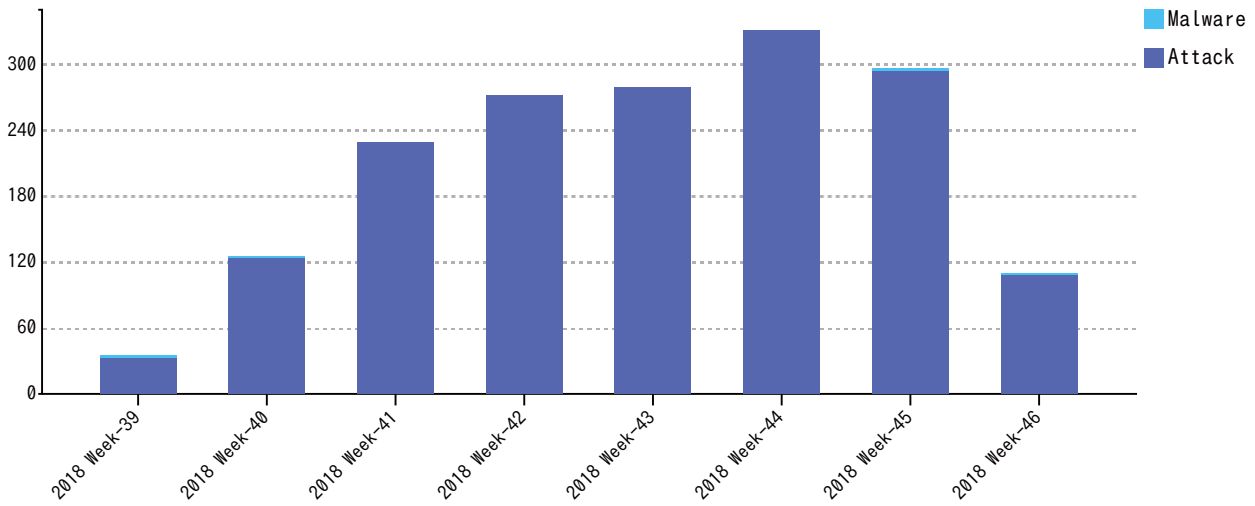
Copyright 2018 HighTechSystem Co., Ltd.

新たな脅威の検知

サイバー攻撃は日々変化し、巧妙化しています。お客様のネットワークに対しても、同じ種類の攻撃ばかりが繰り返されるとは限らず、インターネットに接続される機器は、多種多様な攻撃の危険性に晒されるということを、企業の管理者は理解しなければなりません。このセクションでは、お客様のFortiGateにて新たに検知された脅威についての分析結果を報告します。

新たなセキュリティ脅威の検知数推移

お客様のFortiGateにおいて初めて検知された脅威の検知数を時系列にしたデータです。増加傾向にある場合は、次々に新たなタイプの攻撃を仕掛けられている可能性が高いことを意味します。



新たに検知したセキュリティ脅威（対象ホスト数順）

お客様のFortiGateにおいて、初めて検知された脅威を攻撃対象ホスト（IP）が多い順に表示したデータです。これらの攻撃に対して対策を行っているかの確認が推奨されます。また、「CVE-ID」が表示されている項目は脆弱性を突いた攻撃につき、脆弱性情報サイト等で検索することで詳細な情報が確認できます。

Name	Category	Host	CVE
MS.IIS.WebDAV.PROPFIND.ScStoragePathFromUrl.Buffer.Overflow	Attack	678	CVE-2017-7269
Avtech.Devices.HTTP.Request.Parsing.Multiple.Vulnerabilities	Attack	266	
Dasan.GPON.Remote.Code.Execution	Attack	173	CVE-2018-10561,CVE-2018-10562
D-Link.DSL-2750B.CLI.OS.Command.Injection	Attack	126	
Netcore.Netis.Devices.Hardcoded.Password.Security.Bypass	Attack	96	
Linksys.Routers.Administrative.Console.Authentication.Bypass	Attack	47	
HTTP.URI.SQL.Injection	Attack	35	
Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution	Attack	22	CVE-2017-5638
Oracle.WebLogic.Server.wls-wsat.Component.Code.Injection	Attack	17	CVE-2017-3506,CVE-2017-10271
Wordpress.Login.Brute.Force	Attack	16	CVE-2009-2335
STUNSHELL.Web.Shell.Remote.Code.Execution	Attack	12	
Joomla.Core.Session.Remote.Code.Execution	Attack	11	CVE-2015-8562
HTTP.Request.URI.Directory.Traversal	Attack	10	CVE-2001-0308,CVE-2017-10974,CVE-2018-11137
PHP.URI.Code.Injection	Attack	10	
PHP.Malicious.Shell	Attack	9	
NETGEAR.DGN1000.CGI.Unauthenticated.Remote.Code.Execution	Attack	7	
PHP.CGI.Argument.Injection	Attack	6	CVE-2012-1823,CVE-2012-2311
Zyxel.Router.nslookup.Command.Injection	Attack	5	CVE-2017-6884
Drupal.Core.Form.Rendering.Component.Remote.Code.Execution	Attack	5	CVE-2018-7600

Copyright 2018 HighTechSystem Co., Ltd.

Name	Category	Host	CVE
OpenSSL.Heartbleed.Attack	Attack	5	CVE-2014-0160
SSLv2.Openssl.Get.Shared.Ciphers.Overflow.Attempt	Attack	4	CVE-2006-3738
TUTOS.CMD.Module.Unauthenticated.Remote.Command.Execution	Attack	4	CVE-2008-0148,CVE-2008-0149
VACRON.CCTV.Board.CGI.cmd.Parameter.Command.Execution	Attack	4	
Malicious.Shellcode.Detection	Attack	3	
China.Chopper.Web.Shell.Client.Connection	Attack	3	
Muieblackcat.Scanner	Attack	3	
PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	Attack	3	CVE-2017-9841
Multiple.CCTV.DVR.Vendors.Remote.Code.Execution	Attack	2	
Narcissus.Image.Configuration.Remote.Command.Execution	Attack	2	
Nmap.Script.Scanner	Attack	2	
DataLife.Engine.Catlist.Parameter.PHP.Code.Injection	Attack	2	CVE-2013-1412
HTTP.Header.SQL.Injection	Attack	2	
TCP.Window.Size.Zero.DoS	Attack	2	CVE-2009-1926
Ubiquiti.Networks.AirOS.admin.cgi.Remote.Command.Execution	Attack	2	
W32/GenKryptik.CMCA!tr	Malware	2	
Honeywell.IPCam.Information.Disclosure	Attack	2	
WebNMS.Framework.Directory.Traversal	Attack	2	CVE-2016-6600,CVE-2016-6601
JAWS.DVR.CCTV.Shell.Unauthenticated.Command.Execution	Attack	2	
WordPress.WP.Mobile.Detector.Arbitrary.File.Upload	Attack	2	
Log1.CMS.WriteInfo.PHP.Code.Injection	Attack	2	CVE-2011-4825
ZmEu.Vulnerability.Scanner	Attack	2	
a6d7af8ce2ae317d2fe637d0aca5fd971315cb7b	Malware	1	
92872b11bd9831783d4f5daa8204c05b6edff528	Malware	1	
ANS.Directory.Traversal	Attack	1	CVE-2002-0307
AUTH.TLS.Plaintext.Command.Injection	Attack	1	CVE-2011-1575
Adobe.XML.Entity.Injection	Attack	1	CVE-2009-3960
Apache.Commons.Collection.InvokerTransformer.Code.Execution	Attack	1	CVE-2015-4852,CVE-2015-6420,CVE-2015-6555,CVE-2015-6576,CVE-2016-0788,CVE-2016-3427,CVE-2016-3642,CVE-2016-4385,CVE-2016-8735,CVE-2016-9498,CVE-2017-5645,CVE-2017-5792,CVE-2018-10611
Apache.Struts.2.DefaultActionMapper.Remote.Command.Execution	Attack	1	CVE-2013-2251
Apache.Struts.2.REST.Plugin.Remote.Code.Execution	Attack	1	CVE-2016-4438,CVE-2017-12611
Apache.Tomcat.Arbitrary.JSP.file.Upload	Attack	1	CVE-2017-12615,CVE-2017-12617
Bash.Function.Definitions.Remote.Code.Execution	Attack	1	CVE-2014-6271,CVE-2014-6277,CVE-2014-6278,CVE-2014-7169,CVE-2014-7186,CVE-2014-7187
D-Link.Devices.Unauthenticated.Remote.Command.Execution	Attack	1	
EICAR_TEST_FILE	Malware	1	
EMC.AlphaStor.Library.Manager.Arbitrary.Command.Execution	Attack	1	CVE-2008-2157,CVE-2013-0928,CVE-2013-0929
Easy.Hosting.Control.Panel.FTP.Account.Security.Bypass	Attack	1	
Ektron.XSLT.Transform.Remote.Code.Execution	Attack	1	CVE-2012-5357
FTP.Login.Brute.Force	Attack	1	
FTP.USER.Command.Overflow	Attack	1	CVE-1999-0256,CVE-2000-0479,CVE-2002-0126,CVE-2005-3683,CVE-2006-2212,CVE-2013-5680
Generic.JavaScript.Cryptocurrency.Mining.Script	Attack	1	
Gh0st.Rat.Botnet	Attack	1	

Copyright 2018 HighTechSystem Co., Ltd.

Name	Category	Host	CVE
MS.IE.FTP.Client.Folder.Traversal	Attack	1	CVE-2004-1376
Malware	Malware	1	
Masscan.Scanner	Attack	1	
Openssl.AES.CBC.Padding.Oracle.Information.Disclosure	Attack	1	CVE-2016-2107
PHP.Charts.PHP.Code.Execution	Attack	1	
PHP.Charts.Type.Parameter.Parsing.Code.Execution	Attack	1	
PhpMoAdmin.moadmin.php.Unauthenticated.Remote.Code.Execution	Attack	1	CVE-2015-2208
Riskware/Babylon	Malware	1	
TLS.ROBOT.Attack	Attack	1	CVE-2012-5081,CVE-2016-6883,CVE-2017-6168,CVE-2017-12373,CVE-2017-13098,CVE-2017-13099,CVE-2017-17382,CVE-2017-17427,CVE-2017-17428
W32/Kryptik.GLKH!tr	Malware	1	
Web.Server.Password.Files.Access	Attack	1	
WordPress.Download.Manager.wpdm_upload_icons.Code.Execution	Attack	1	
WordPress.Marketplace.wpmp_pp_ajax_call.Remote.Code.Execution	Attack	1	CVE-2014-9013
WordPress.RevSlider.Arbitrary.File.Upload	Attack	1	
WordPress.WP.Symposium.Arbitrary.File.Upload	Attack	1	CVE-2014-10021
XAttacker.Tool.WebApp.Plugins.Arbitrary.File.Upload	Attack	1	
XM/Agent.F01B!tr.dldr	Malware	1	
Zivif.PR115-204-P-RS.Web.Cameras.Credentials.Disclosure	Attack	1	CVE-2017-17106
91218a24505bf77a99347950647255c777f96595	Malware	1	

Copyright 2018 HighTechSystem Co., Ltd.

トラフィック分析

このセクションでは、お客様のネットワーク利用状況について分析した結果を報告します。企業の管理者にとって、ネットワークの利用状況を把握しておくことは、適切な管理を行う上で必要不可欠です。日頃、どのくらいインターネット接続が行われ、どのくらいのデータが送受信され、どのコンピュータの通信量が多く、どのような通信をしているかを確認しておくことで、マルウェア感染等により普段と異なる通信が発生した場合に、異常を見つけやすくなります。また、自社が本来認めていない通信が行われていないかを確認し、適切な対処をすることで企業ネットワークにおける各種リスクを低下させることが可能です。

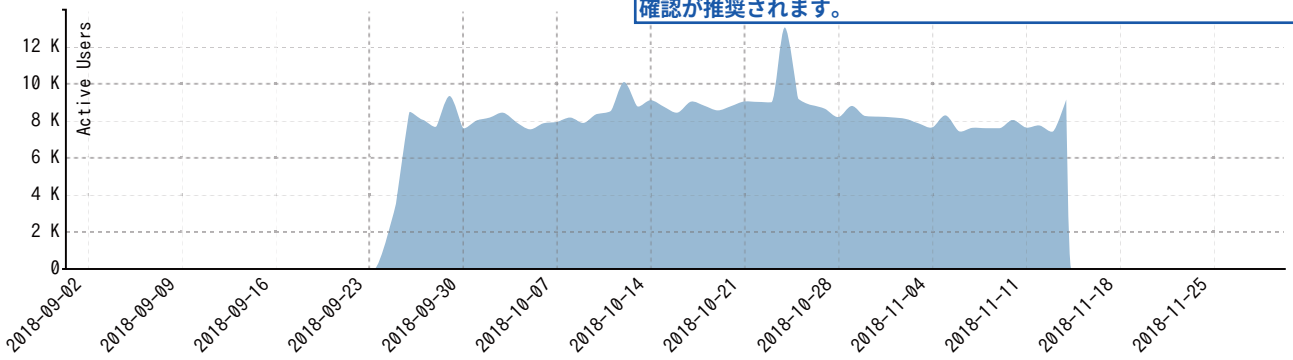
トラフィック情報の統計（分析期間トータル）

分析期間における通信情報の統計値です。ご利用されているFortiGateの性能が、お客様の利用状況に対して不足していないか確認いただく際の参考値になります。
- Total Sessions…セッション数の累計値です。
- Total Bytes Transferred…通信量の累計値です。
- Most Active Date By Sessions…最もセッション数が多かった日です。
- Total Users…通信したIP数の累計値です。
- Total Applications…通信したアプリケーション数の累計値です。
- Total Destinations…通信した宛先IP数の累計値です。
- Average Sessions Per Day…1日当たりの平均セッション数です。
- Average Bytes Per Day…1日当たりの平均通信量です。

Summary	Statistics
Total Sessions	18,499,543
Total Bytes Transferred	4,225.01GB
Most Active Date By Sessions	2018-11-08
Total Users	286,956
Total Applications	66,943
Total Destinations	8,609
Average Sessions Per Day	203,292
Average Bytes Per Day	46.43GB

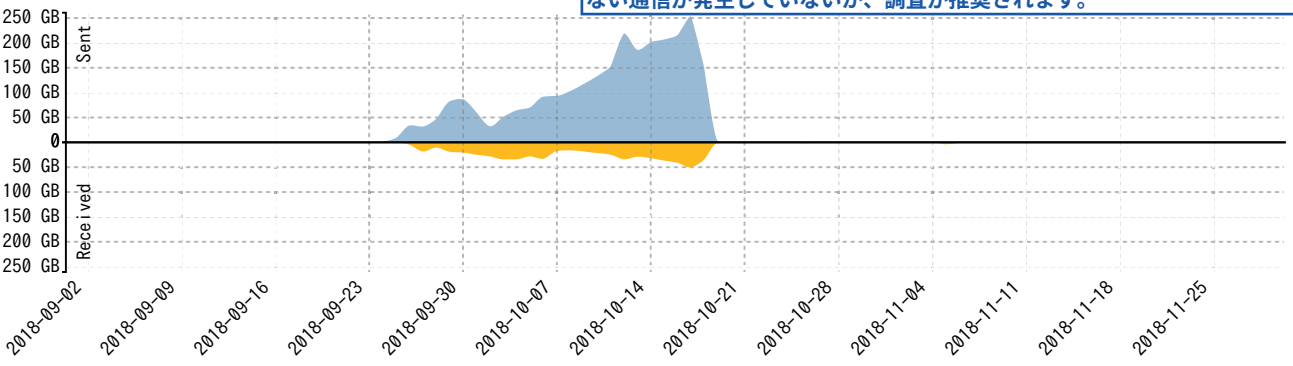
トラフィック状況の推移（送受信IP総数）

FortiGateを経由して送受信が行われたIPの総数になります。数が多いほど、多くのIPから通信が行われたことを意味し、突出して数値が多い日などがあった場合は、意図しない通信が内部から発生していなかったかや、攻撃などで不特定多数のIPから通信が行われていなかったかなどの確認が推奨されます。



トラフィック状況の推移（送受信量）

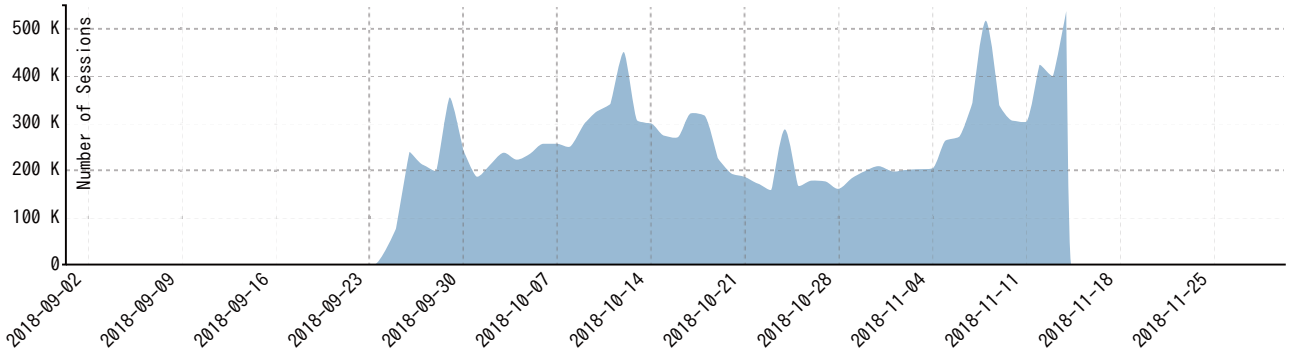
FortiGateを経由してデータの送信と受信がどのくらいあったか、送受信量の時系列データになります。通信量の推移が確認でき、著しく通信量が多い日があったり、送信または受信が極端に増えている場合などは、意図しない通信が発生していないか、調査が推奨されます。



Copyright 2018 HighTechSystem Co., Ltd.

セッション数の推移

いつ、どのくらいのセッションが張られていたかの推移が確認できる時系列データです。セッション数が突出して多い日などがある場合は、意図しない通信が発生していないか調査が推奨されます。



通信元別セッション数TOP10

セッション数が多かった通信元ホスト（IP）の上位10個です。突出して多いホストがいる場合は、意図しない通信が発生していないか調査が推奨されます。

User (or IP)	Sessions
IPv6-1431	1,929,558
IPv6-58785	1,738,916
IPv6-24131	912,493
IPv4-16886	680,949
IPv4-35152	661,440
IPv4-29477	590,143
IPv4-59745	517,503
IPv4-35380	516,362
Usr-46838	484,706
IPv4-27124	471,815

アプリケーション（プロトコル）別セッション数TOP10

セッション数が多かったアプリケーション（プロトコル）の上位10種類です。不明なアプリやプロトコルで大量にセッションが張られている場合は調査が推奨されます。

Application	Sessions
netbios forward	4,721,909
udp/5355	2,774,077
udp/1900	1,994,331
udp/19540	1,107,674
DHCP/DHCP Relay	619,379
プロトコル名	562,224
udp/17500	342,539
TELNET	327,851
DNS	321,708
udp/62976	289,840

国別通信量TOP10

通信量が多かった国の上位10か国です。一般的には日本国内の通信量に対して、通信している認識がない外国の通信量が多い場合は、調査が推奨されます。

Country	Bandwidth
Japan	4.01 TB
United States	7.74 MB
Ukraine	387.04 KB
China	292.18 KB
Sweden	195.43 KB
Netherlands	156.95 KB
Egypt	72.09 KB
Hong Kong	62.31 KB
Brazil	47.13 KB
Russian Federation	40.53 KB

Copyright 2018 HighTechSystem Co., Ltd.

アプリケーション別通信量及びセッション数（通信量順）

アプリケーション別の通信量及び通信許可区分、セッション数の情報です。どういうアプリがどれだけ通信していたかが確認できます。

Application	Action	Bandwidth	Session Count
アプリ名	Allowed	4.01 TB	562,153
HTTPS	Allowed	55.43 GB	202,734
HTTP	Allowed	33.99 GB	69,904
PING	Allowed	10.47 GB	31,216
Proxy.HTTP	Blocked	3.52 GB	67
HTTP.BROWSER	Allowed	2.07 GB	1,093
HTTPS.BROWSER	Allowed	2.03 GB	28,094
udp/56348	Allowed	1.79 GB	2
udp/8801	Allowed	1.77 GB	48
MS.Windows.Update	Allowed	1.55 GB	1,716
Microsoft.Office.Update	Allowed	803.43 MB	68
Microsoft.SharePoint	Allowed	674.05 MB	72
Google.Services	Allowed	489.76 MB	21,360
udp/443	Allowed	437.54 MB	28,916
Zoom	Allowed	368.32 MB	194
Ubuntu.Update	Allowed	363.27 MB	136
tcp/60022	Allowed	316.90 MB	249
Proxy.HTTP	Allowed	298.47 MB	712
Gmail	Allowed	288.03 MB	981
udp/62188	Allowed	243.74 MB	2
udp/57858	Allowed	188.31 MB	2
HTTP.BROWSER_IE	Allowed	151.45 MB	2,033
HTTP	Allowed	147.53 MB	1,831
udp/62665	Allowed	129.49 MB	2
Microsoft.Portal	Allowed	110.38 MB	1,762
udp/52190	Allowed	109.06 MB	2
Google.Accounts	Allowed	86.70 MB	10,470
tcp/43	Allowed	79.08 MB	27,674
HTTP.Download.Accelerator	Allowed	78.24 MB	10
Google.Play	Allowed	59.04 MB	8,390
HTTP.Segmented.Download	Allowed	53.37 MB	16
HTTP.BROWSER_Chrome	Allowed	47.39 MB	1,699
Yahoo.Services	Allowed	45.09 MB	1,284
udp/64659	Allowed	40.85 MB	2
Amazon.CloudFront	Allowed	40.25 MB	174
tcp/43	Allowed	38.01 MB	10,907
Google.Ads	Allowed	38.00 MB	1,804
Microsoft.Authentication	Allowed	37.02 MB	2,878
Ping	Allowed	36.61 MB	272
Microsoft.Office.Online	Allowed	33.70 MB	959
SMTP	Allowed	32.97 MB	2,640
udp/51819	Allowed	26.74 MB	2
DNS	Allowed	25.34 MB	159,802
SSL_TLSv1.2	Allowed	24.20 MB	1,021
Amazon.Services	Allowed	23.73 MB	275
tcp/8100	Allowed	23.48 MB	286
Slack	Allowed	20.40 MB	84
Microsoft.CDN	Allowed	17.56 MB	122
Amazon.AWS	Allowed	13.78 MB	295
Fortiguard.Search	Allowed	13.00 MB	32,187
udp/8888	Allowed	10.42 MB	3,350
HTTP.BROWSER_Chrome	Blocked	10.33 MB	294
Microsoft.Office.365.Portal	Allowed	9.96 MB	272
HTTPS	Allowed	9.74 MB	629
tcp/53458	Allowed	9.58 MB	1
tcp/59639	Allowed	9.35 MB	1
tcp/55249	Allowed	9.30 MB	1
Facebook	Allowed	8.77 MB	583
tcp/8801	Allowed	8.32 MB	18

Copyright 2018 HighTechSystem Co., Ltd.

Application	Action	Bandwidth	Session Count
SNMP	Allowed	8.18 MB	3,800
Github	Allowed	7.44 MB	537
Skype.Portals	Allowed	7.17 MB	541
SSH	Allowed	6.60 MB	84
udp/57253	Allowed	6.08 MB	1
Twitter	Allowed	6.04 MB	593
Slideshare	Allowed	5.63 MB	69
TrendMicro.WFBS	Allowed	5.32 MB	92
tcp/8013	Allowed	5.26 MB	106,008
DNS	Allowed	4.72 MB	23,781
MS.Windows.Update	Blocked	4.66 MB	21
HTTP.BROWSER_Firefox	Allowed	4.43 MB	447
Microsoft.Outlook	Allowed	4.28 MB	571
Dell.Service	Allowed	3.58 MB	72
Dropbox	Allowed	3.48 MB	508
tcp/10083	Allowed	3.46 MB	122
tcp/8013	Allowed	3.20 MB	64,446
Salesforce	Allowed	3.12 MB	507
tcp/4440	Allowed	2.96 MB	16
HTTP.BROWSER	Blocked	2.76 MB	6
HTTP.BROWSER_IE	Blocked	2.64 MB	183
tcp/12080	Allowed	2.53 MB	18,031
SMTPS	Allowed	2.50 MB	247
YouTube	Allowed	2.29 MB	40
Google.Analytics	Allowed	2.18 MB	164
Google.Drive	Allowed	2.11 MB	38
tcp/5228	Allowed	2.04 MB	243
Blogger	Allowed	1.96 MB	68
Amazon.AWS_Console	Allowed	1.88 MB	73
Slack_Message	Allowed	1.87 MB	39
Amazon.Ads	Allowed	1.77 MB	220
Microsoft.Portal	Blocked	1.60 MB	68
Root.Certificate.URL	Allowed	1.46 MB	541
Google.Push.Notification	Allowed	1.36 MB	117
OCSP	Allowed	1.14 MB	436
Microsoft.Office.365	Allowed	1.14 MB	27
tcp/2222	Allowed	909.93 KB	6,163
SNMP_GetRequest	Allowed	873.15 KB	61
NTP	Allowed	830.33 KB	2,316
Google.Translate	Allowed	702.85 KB	59
SSL	Allowed	630.76 KB	1,577

アプリケーション別通信量TOP10（送受信区別付）

通信量が多かったアプリケーションの上位10種類で、それぞれ送信と受信のどちらが多かったのか割合が確認できます。

Application	Bandwidth	Sent Received
アプリ名		4.01 TB
HTTPS		55.44 GB
HTTP		34.14 GB
PING		10.47 GB
Proxy.HTTP		3.81 GB
HTTP.BROWSER		2.28 GB
HTTPS.BROWSER		2.03 GB
udp/56348		1.79 GB
udp/8801		1.77 GB
MS.Windows.Update		1.55 GB

Copyright 2018 HighTechSystem Co., Ltd.

SaaSアプリケーション別通信量TOP10

検知したSaaS（クラウドサービス等）アプリケーションの通信量上位10種類です。
どういうSaaSアプリがどのくらい通信していたかが確認できます。

Application	Category	Bytes	Sent	Received	Sessions	Blocked	Allowed
Microsoft.SharePoint	Collaboration			674.05 MB			72
Zoom	Collaboration			348.05 MB			171
Gmail	メール			230.80 MB			887
Amazon.CloudFront	Cloud.IT			40.29 MB			175
Microsoft.Office.Online	Collaboration			33.56 MB			945
Amazon.Services	General.Interest			23.60 MB			270
Slack	Collaboration			20.40 MB			84
Amazon.AWS	Cloud.IT			13.78 MB			295
Fortiguard.Search	Cloud.IT			13.00 MB			32,186
Facebook	Social.Media			8.99 MB			764

Copyright 2018 HighTechSystem Co., Ltd.

通信元別通信量TOP5

通信量が多かった通信元ホスト（IP）上位5個です。それぞれ、セッション数、通信総量、通信先、通信アプリケーションなどの詳細が確認できます。また、アプリケーション別の通信量割合も確認できます。通信量が多かったホストについては、正規の利用によるものか確認することが推奨されます。

1st Highest Bandwidth User: IPv4-43345 Usage: 3.9 TB IP: IPv4-43345 Device: N/A

Traffic Summary

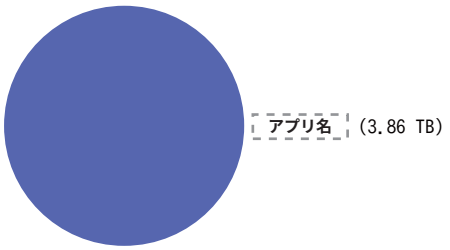
Total Number of Sessions	98,715
Total Number of Bytes	3.9 TB
	635.1 GB in 3.2 TB out

Top 10 Destinations

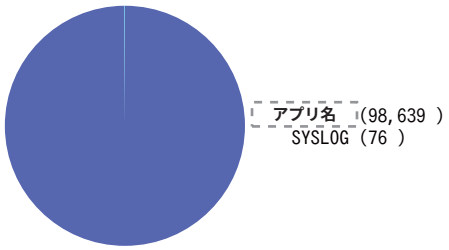
Destination	Bandwidth	Application
IPv4-39732	3.9 TB	アプリ名

Application Summary

Top 5 Application Bandwidth



Top 5 Application Sessions



Copyright 2018 HighTechSystem Co., Ltd.

2nd Highest Bandwidth User: IPv4-48893 Usage: 147.6 GB IP: IPv4-48893 Device: N/A

Traffic Summary

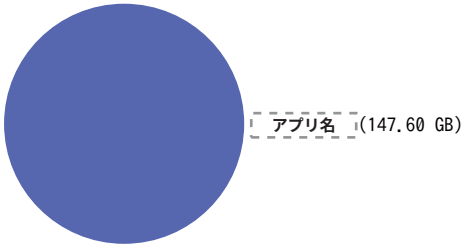
Total Number of Sessions	447,760	
Total Number of Bytes	147.6 GB	
	65.0 GB in	82.6 GB out

Top 10 Destinations

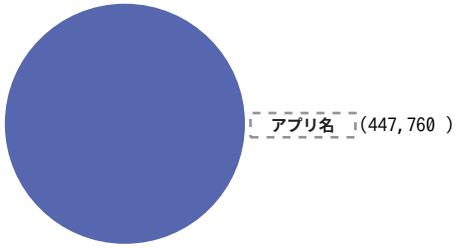
Destination	Bandwidth	Application
IPv4-39732	147.6 GB	アプリ名

Application Summary

Top 5 Application Bandwidth



Top 5 Application Sessions



Copyright 2018 HighTechSystem Co., Ltd.

3rd Highest Bandwidth User: IPv4-52513 Usage: 36.3 GB IP: IPv4-52513 Device: ubuntu

Traffic Summary

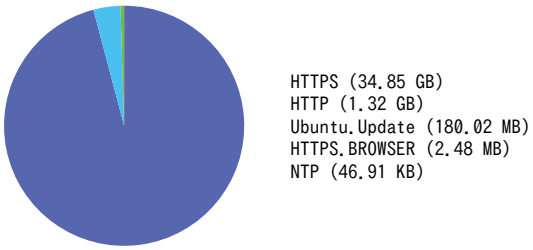
Total Number of Sessions	30,277
Total Number of Bytes	36.3 GB
	35.6 GB in 735.9 MB out

Top 10 Destinations

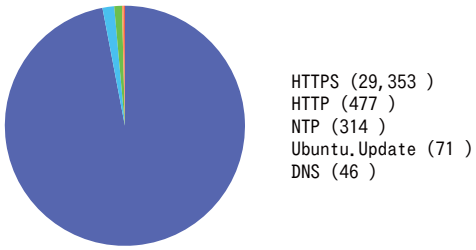
Destination	Bandwidth	Application
IPv4-3172	34.8 GB	HTTPS
IPv4-7227	1.1 GB	HTTP
IPv4-7227	136.1 MB	Ubuntu.Update
IPv4-7870	107.5 MB	HTTP
IPv4-36448	47.2 MB	HTTPS
IPv4-45369	37.0 MB	Ubuntu.Update
IPv4-57475	34.9 MB	HTTP
IPv4-37274	21.5 MB	HTTP
IPv4-23433	10.3 MB	HTTP
IPv4-26163	9.2 MB	HTTPS

Application Summary

Top 5 Application Bandwidth



Top 5 Application Sessions



Copyright 2018 HighTechSystem Co., Ltd.

4th Highest Bandwidth User: IPv4-23291 Usage: 22.7 GB IP: IPv4-23291 Device: tsocvmmng001

Traffic Summary

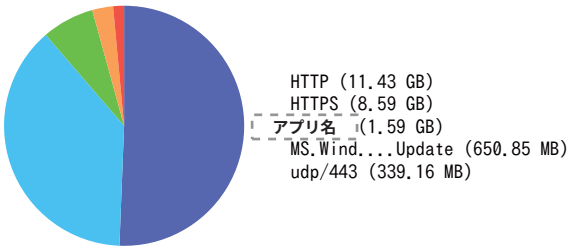
Total Number of Sessions	136,786
Total Number of Bytes	22.7 GB
	20.8 GB in 1.9 GB out

Top 10 Destinations

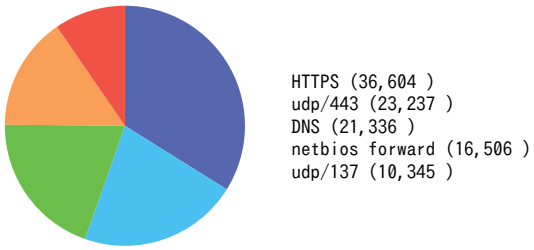
Destination	Bandwidth	Application
IPv4-7170	3.4 GB	HTTP
IPv4-27784	3.0 GB	HTTPS
IPv4-44357	2.8 GB	HTTP
IPv4-13683	2.6 GB	HTTP
IPv4-17195	1.6 GB	アプリ名
IPv4-50095	1.4 GB	HTTP
IPv4-64832	771.1 MB	HTTPS
IPv4-37365	564.9 MB	HTTPS
IPv4-7170	547.6 MB	MS.Windows.Updat
IPv4-49285	422.2 MB	HTTPS

Application Summary

Top 5 Application Bandwidth



Top 5 Application Sessions



Copyright 2018 HighTechSystem Co., Ltd.

5th Highest Bandwidth User: IPv4-40315 Usage: 22.5 GB IP: IPv4-40315 Device: DESKTOP-RNDL4OV

Traffic Summary

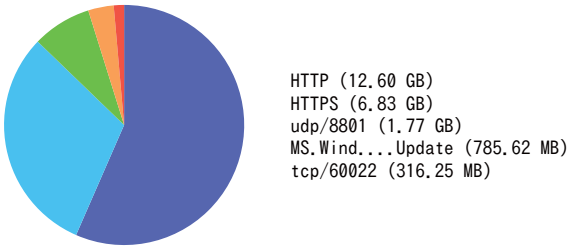
Total Number of Sessions	92,174
Total Number of Bytes	22.5 GB
	20.8 GB in 1.7 GB out

Top 10 Destinations

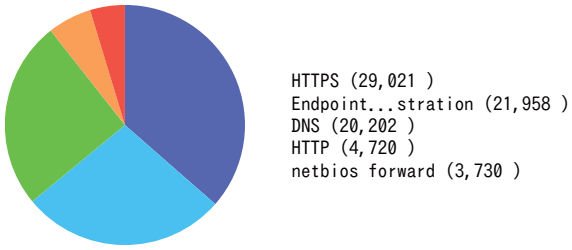
Destination	Bandwidth	Application
IPv4-18056	4.6 GB	HTTPS
IPv4-22331	3.9 GB	HTTP
IPv4-26541	3.8 GB	HTTP
IPv4-7170	1.8 GB	HTTP
IPv4-11752	1.8 GB	udp/8801
IPv4-13847	1.7 GB	HTTP
IPv4-38804	375.9 MB	MS.Windows.Updat
IPv4-44620	356.7 MB	HTTPS
IPv4-7170	348.2 MB	MS.Windows.Updat
IPv4-59080	316.9 MB	tcp/60022

Application Summary

Top 5 Application Bandwidth



Top 5 Application Sessions



Copyright 2018 HighTechSystem Co., Ltd.

通信量が多かったアプリケーションの上位10種類で、それぞれどこと、どのくらい通信していたかの詳細が確認できます。意図しない通信が行われていないかなどの確認が行えます。

アプリケーション別通信量TOP10（通信元詳細あり）

Application アプリ名	User (or IP)	Bandwidth	% 小計
	IPv4-43345	3.86 TB	96.36%
	IPv4-48893	147.60 GB	3.59%
	IPv4-23291	1.59 GB	0.04%
	IPv4-40315	100.09 MB	0.00%
	IPv4-37744	90.23 MB	0.00%
	IPv4-27124	13.74 MB	0.00%
	IPv4-2264	8.00 MB	0.00%
	IPv4-14414	3.60 MB	0.00%
	IPv4-44525	804.80 KB	0.00%
	IPv4-34600	4.77 KB	0.00%
	Others	225.11 KB	0.00%
	Subtotal	4.01 TB	97.19%
HTTPS	IPv4-52513	34.85 GB	62.85%
	IPv4-23291	8.59 GB	15.50%
	IPv4-40315	6.83 GB	12.32%
	IPv4-22658	1.74 GB	3.14%
	IPv4-2360	1.30 GB	2.34%
	IPv4-27124	1.19 GB	2.15%
	IPv4-26659	561.85 MB	0.99%
	IPv4-2264	207.24 MB	0.37%
	IPv4-14414	117.90 MB	0.21%
	IPv4-44525	62.14 MB	0.11%
	Others	17.33 MB	0.03%
	Subtotal	55.44 GB	1.31%
HTTP	IPv4-40315	12.60 GB	36.91%
	IPv4-23291	11.43 GB	33.48%
	IPv4-27124	3.59 GB	10.51%
	IPv4-14414	1.85 GB	5.42%
	IPv4-26659	1.69 GB	4.94%
	IPv4-52513	1.32 GB	3.86%
	IPv4-22658	1.20 GB	3.51%
	IPv4-2264	267.68 MB	0.77%
	Usr-10678	129.13 MB	0.37%
	IPv4-44525	79.98 MB	0.23%
	Others	1.38 MB	0.00%
	Subtotal	34.14 GB	0.81%
PING	IPv4-26659	8.98 GB	85.72%
	IPv4-27124	1.48 GB	14.17%
	IPv4-39499	7.35 MB	0.07%
	IPv4-40641	3.82 MB	0.04%
	IPv4-50979	227.96 KB	0.00%
	IPv4-16886	74.18 KB	0.00%
	IPv4-40315	4.23 KB	0.00%
	IPv4-22658	2.98 KB	0.00%
	IPv4-2360	1.80 KB	0.00%
	IPv4-63804	1.31 KB	0.00%
	Others	6.34 KB	0.00%
	Subtotal	10.47 GB	0.25%
Proxy.HTTP	IPv4-3857	3.52 GB	92.38%
	Usr-46838	280.53 MB	7.18%
	Usr-10678	13.72 MB	0.35%
	IPv4-64340	1.55 MB	0.04%
	IPv4-15587	883.05 KB	0.02%
	IPv4-27124	832.39 KB	0.02%
	Subtotal	3.81 GB	0.09%
HTTP.BROWSER	Usr-10678	829.66 MB	39.11%
	Usr-6403	313.89 MB	14.80%
	Usr-31145	293.12 MB	13.82%
	IPv4-15587	231.74 MB	10.93%
	Usr-46838	214.35 MB	10.11%
	IPv4-3189	122.26 MB	5.76%
	IPv4-23291	60.36 MB	2.85%
	IPv4-14414	51.84 MB	2.44%
	IPv4-27124	3.62 MB	0.17%
	IPv4-40315	128.08 KB	0.01%
	Others	194.54 KB	0.01%
	Subtotal	2.07 GB	0.05%
HTTPS.BROWSER	IPv4-64340	633.30 MB	30.50%

Copyright 2018 HighTechSystem Co., Ltd.

Application	User (or IP)	Bandwidth	% 小計
	Usr-10678	609.40 MB	29.35%
	Usr-46838	321.91 MB	15.50%
	IPv4-27124	169.53 MB	8.16%
	IPv4-2360	122.37 MB	5.89%
	Usr-6403	59.56 MB	2.87%
	IPv4-14414	43.25 MB	2.08%
	IPv4-3189	34.36 MB	1.65%
	IPv4-40315	28.69 MB	1.38%
	IPv4-15587	12.91 MB	0.62%
	Others	41.37 MB	1.99%
	Subtotal	2.03 GB	0.05%
udp/56348	IPv4-27124	1.79 GB	100.00%
	Subtotal	1.79 GB	0.04%
udp/8801	IPv4-40315	1.77 GB	99.86%
	IPv4-27124	2.52 MB	0.14%
	Subtotal	1.77 GB	0.04%
MS.Windows.Update	IPv4-40315	785.62 MB	49.38%
	IPv4-23291	650.85 MB	40.91%
	IPv4-26659	77.01 MB	4.84%
	Usr-46838	67.32 MB	4.23%
	Usr-10678	6.65 MB	0.42%
	IPv4-14414	1.15 MB	0.07%
	IPv4-27124	1.14 MB	0.07%
	Usr-31145	1.11 MB	0.07%
	IPv4-15587	164.96 KB	0.01%
	IPv4-23762	26.02 KB	0.00%
	Others	50.47 KB	0.00%
	Subtotal	1.55 GB	0.04%
Others		5.69 GB	0.13%
Total		4.13 TB	100.00%

Copyright 2018 HighTechSystem Co., Ltd.

ウェブアクセス分析

このセクションでは、お客様ネットワークからのウェブアクセスについて分析した結果を報告します。近年、ウェブアクセスが業務上欠かせないものになっており、企業の管理者は企業ネットワークからのウェブアクセスが適切なものかどうかを管理する必要があります。業務に無関係なウェブアクセスは、複数の面で企業の生産性低下に繋がりますので、企業の管理者は生産性の維持向上のため、適切なウェブアクセス管理を行う必要があります。

※ お客様のFortiGateにてWebフィルタの機能が未設定または無効の場合、TSOCにて分析が行えないため本セクションの分析結果が表示されない場合があります。

ウェブドメイン訪問数TOP20

検知したウェブドメインの訪問数上位20個です。意図しないウェブドメインに大量にアクセスしている場合や、利用を認識していないドメインが上位を占める場合などは、マルウェア感染の可能性が疑われます。

Domain	Category	Visits
pagead2.googlesyndication.com	広告	51
platform.twitter.com	ソーシャル・ネットワーキング	20
yj-a.p.adnxs.com	広告	19
jp.at.atwola.com	広告	18
www.googleadservices.com	広告	17
www.jra.go.jp	ギャンブル	17
stats.g.doubleclick.net	広告	16
ib.adnxs.com	広告	14
plus.google.com	ソーシャル・ネットワーキング	13
connect.facebook.net	ソーシャル・ネットワーキング	10
nagomi-cafe.com	エンタテインメント	10
banner.advertising.com	広告	9
graph.facebook.com	ソーシャル・ネットワーキング	8
cm.g.doubleclick.net	広告	8
contextual.media.net	広告	7
securepubads.g.doubleclick.net	広告	6
widgets.outbrain.com	広告	5
js.gsspcln.jp	広告	5
cdn.adaptv.advertising.com	広告	5
www.samuraiclick.com	ゲーム	5

ブロックされたウェブサイト及びカテゴリTOP20

Webフィルタの機能でブロックしたウェブサイトの上位20個です。数が多い場合は、正規の利用者が認められないアクセスを繰り返していないかや、マルウェア感染等の可能性がないか調査が推奨されます。

Website	Category	Requests
pagead2.googlesyndication.com	広告	51
platform.twitter.com	ソーシャル・ネットワーキング	20
yj-a.p.adnxs.com	広告	19
jp.at.atwola.com	広告	18
www.jra.go.jp	ギャンブル	17
www.googleadservices.com	広告	17
stats.g.doubleclick.net	広告	16
ib.adnxs.com	広告	14
plus.google.com	ソーシャル・ネットワーキング	13
nagomi-cafe.com	エンタテインメント	10
connect.facebook.net	ソーシャル・ネットワーキング	10
banner.advertising.com	広告	9
graph.facebook.com	ソーシャル・ネットワーキング	8
cm.g.doubleclick.net	広告	8
contextual.media.net	広告	7
securepubads.g.doubleclick.net	広告	6
adserver.cxad.cxense.com	広告	5
cdn.adaptv.advertising.com	広告	5
www.samuraiclick.com	ゲーム	5
widgets.outbrain.com	広告	5

Copyright 2018 HighTechSystem Co., Ltd.

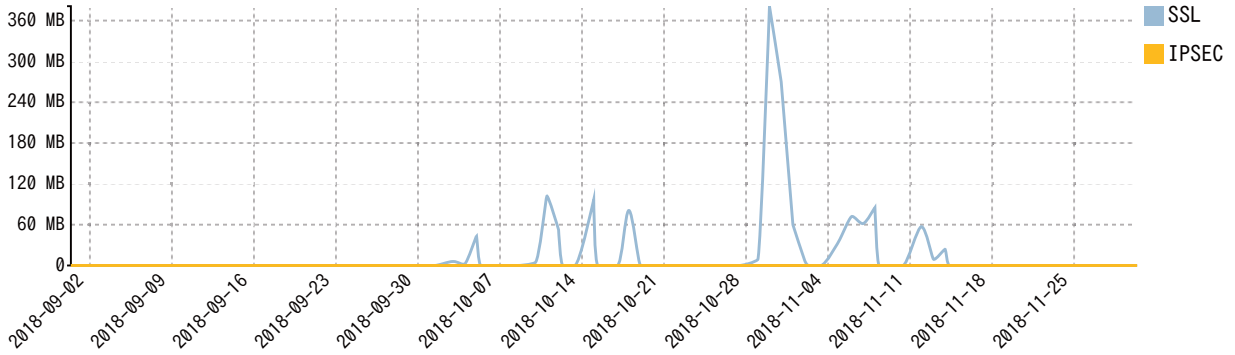
VPN接続分析

このセクションでは、お客様のネットワークにおけるVPNの利用状況についての分析結果を報告します。企業ネットワークに対するVPN接続を許可している場合、企業の管理者はVPN接続を認めたユーザのみが利用しているかや、認めた時間帯のみ利用しているかなど、利用状況を管理する必要があります。意図しないVPN接続は、企業の情報漏えいリスクを著しく高めます。また、VPN接続のログイン失敗が大量に検知されている場合などは、不正なVPN接続を試みられている可能性がありますので、注意が必要です。

※ お客様のFortiGateにてVPNの機能が未設定または無効の場合、TSOCにて分析が行えないため本セクションの分析結果が表示されない場合があります。

VPN通信の使用量推移

VPN通信の通信量を時系列にしたデータです。いつ、どのくらいVPN通信が行われたか、利用状況の推移が確認できます。



VPNログイン成功ユーザー

VPNログインしたユーザの上位10ユーザです。正規ユーザの利用かどうか、利用状況が適切かどうかなどの把握ができます。

ユーザ	Type	First Used	Total Number of Connections	Total Duration Connected(HH:MM:SS)
Usr-34750	ssl-tunnel	2018-10-03 10:53:12	81	159:15:36
Usr-34750	ssl-web	2018-10-03 13:53:48	1	00:15:35

VPNログイン失敗ユーザー

VPNログインに失敗したユーザの上位10ユーザです。失敗回数が著しく多い場合は、不正なログイン試行をされていないか調査が推奨されます。

ユーザ	Type	Total Number of Failed Attempts
Usr-34750	ssl-web	26

接続時間順SSLトンネリングユーザ情報及び通信量TOP10

SSL-VPNなどを利用している場合の通信量上位10ユーザです。VPN等の利用状況が適切かどうかの確認ができます。

User	IP	Connection Time(hh:mm:ss)	Bandwidth Sent Received
Usr-34750	IPアドレス	102:58:07	1.01 GB
Usr-34750		19:05:12	147.07 MB
Usr-34750		07:41:49	98.33 MB
Usr-34750		03:40:21	41.56 MB
Usr-34750		07:32:15	1.33 MB
Usr-34750		00:40:12	17.82 KB

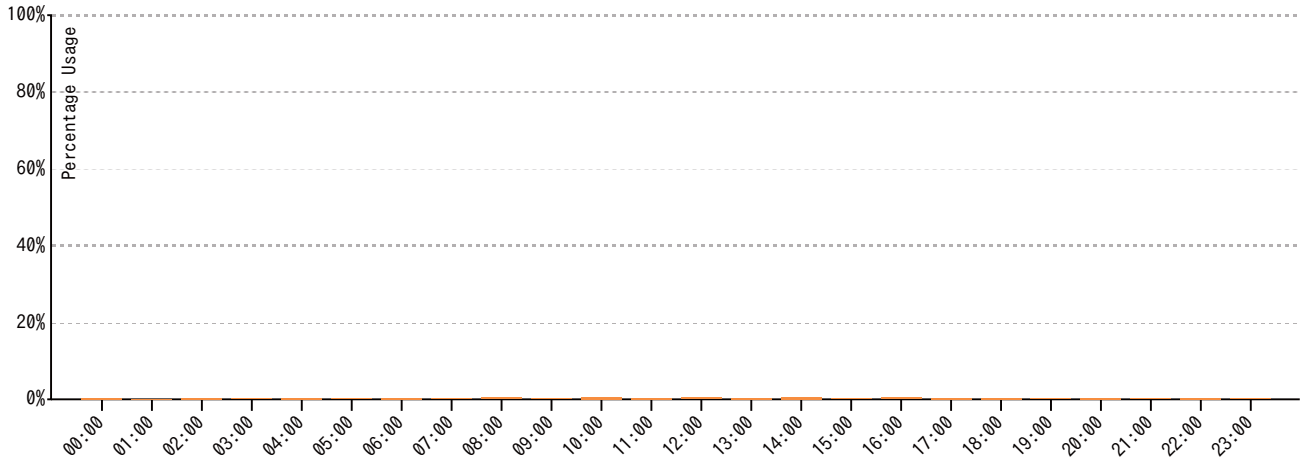
Copyright 2018 HighTechSystem Co., Ltd.

システムイベント分析

このセクションでは、お客様のFortiGateに記録された各種システムイベントについての分析結果を報告します。ご利用中のFortiGateの負荷が高まると、インターネット接続の速度が低下したり、UTM機能が正常に利用できなかったりする可能性があります。このため、企業の管理者は自社のネットワーク利用状況に対して、FortiGateが一時的な性能不足に陥ったのか、それとも恒常的に性能が不足している状態なのかを把握する必要があり、こうした情報をシステムイベントの分析結果から得ることができます。仮に、恒常的にFortiGateの性能が不足している場合は、より性能の高い機種への変更を検討頂く必要があります。また、性能以外の面でもFortiGateに異常が生じていないかや、意図しないFortiGateへのログインや設定変更がされていないかなども、システムイベントの情報から把握が可能です。

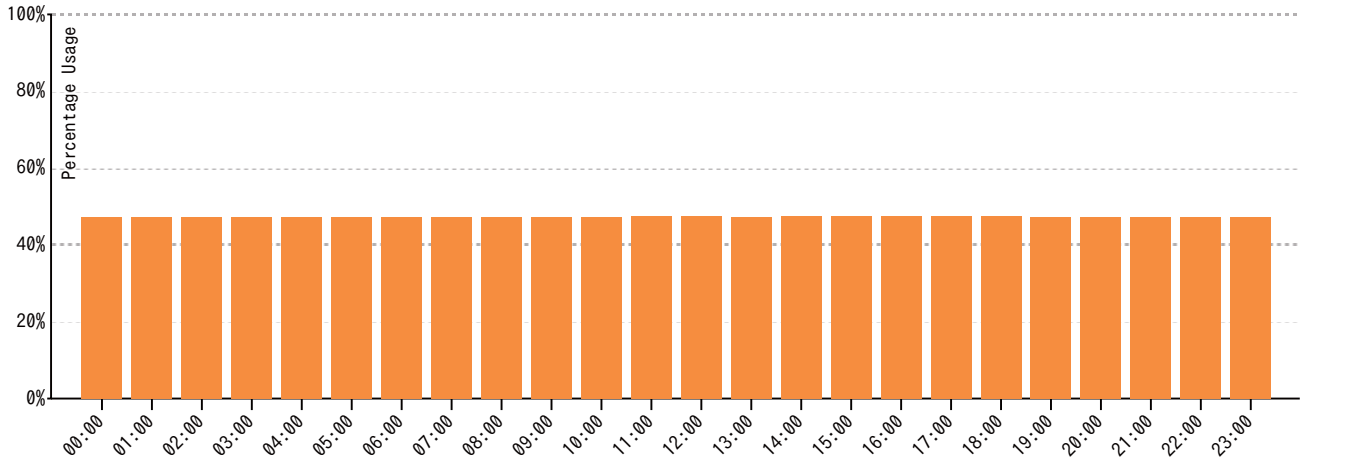
FortiGateのCPU使用率統計（時間帯別）

FortiGateのCPU使用率推移です。どの時間帯でどのくらい使用されているかの統計データです。突出している時間帯がある場合は、FortiGateに対して負荷がかかる通信が発生していないか調査が推奨されます。



FortiGateのメモリ使用率統計（時間帯別）

FortiGateのメモリ使用率推移です。どの時間帯でどのくらい使用されているかの統計データです。突出している時間帯がある場合は、FortiGateに対して負荷がかかる通信が発生していないか調査が推奨されます。



FortiGateのリソース使用状況（最高）

FortiGateのリソース使用最高値です。通常は分析対象のFortiGate（1台）の情報が表示されます。利用状況に対してFortiGateの性能が不足していないか確認するための参考データになります。

Device Name	CPU	Memory	Disk	Logs Per Second	Sessions	Bandwidth Rate (kbps)
FortiGateホスト名	33%	42%	0%		1,055 12,996	198,947
	96%	41%	0%		1,126 906	127,949
	56%	68%	0%		3,598 772	281,267

FortiGateのリソース使用状況（平均）

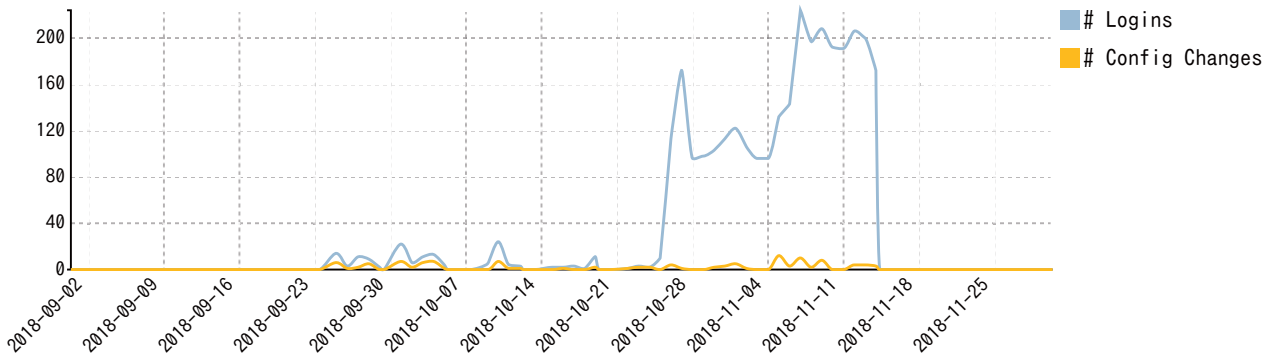
FortiGateのリソース使用平均値です。通常は分析対象のFortiGate（1台）の情報が表示されます。平均値が恒常的に高い場合は、性能不足等が疑われます。

Device Name	CPU	Memory	Disk	Logs Per Second	Sessions	Bandwidth Rate (kbps)	Sent	Received
FortiGateホスト名	0%	38%	0%		12 688			1,610
	1%	36%	0%		4 46			100
	0%	62%	0%		4 68			330

Copyright 2018 HighTechSystem Co., Ltd.

FortiGateへの管理者ログイン及び設定変更の推移

いつごろログインされ、設定変更が行われたのかの時系列データです。突出してログイン回数が多い日がある場合などは、不正なログイン試行が行われていないか調査が推奨されます。



FortiGateへの管理者ログイン成功

FortiGateに管理者ログインしたユーザ及びホスト（IP）のログイン数上位20件です。意図しないユーザやホストからのログインがないかが確認できます。

User Name	Login Interface	Total Number of Logins	Total Number of Configuration Changes	Total Duration (hh:mm:ss)
Usr-62089	ログイン方法及びIPアドレス	2,747	0	347:52:35
Usr-62089		99	20	39:18:41
Usr-34750		40	2	04:34:27
Usr-46838		32	9	54:57:07
Usr-62089		24	7	09:10:55
Usr-46838		23	11	24:24:34
Usr-62089		21	5	07:32:20
Usr-46838		21	8	06:51:40
Usr-31145		10	2	03:27:05
Usr-31145		10	7	04:52:21
Usr-46838		10	0	01:03:21
Usr-31145		9	7	01:14:12
Usr-34750		9	2	07:04:02
Usr-62089		8	0	02:07:49
Usr-46838		8	4	04:43:49
Usr-34750		7	1	00:47:43
Usr-34750		7	1	08:03:27
Usr-62089		6	6	01:41:01
Usr-46838		6	4	02:30:38
Usr-31145		4	0	02:41:49
Usr-7464		4	0	00:14:37
Usr-62089		4	0	01:29:59
Usr-62089		4	0	01:51:14
Usr-6403		3	2	01:17:00
Usr-31145		3	3	02:49:30
Usr-31145		3	2	01:34:12
Usr-31145		2	2	00:48:41
Usr-7464		2	0	00:01:56
Usr-62089		2	2	00:08:13
Usr-46838		2	1	00:06:18
Usr-62089		2	0	01:50:46
Usr-46838		2	2	01:04:08
Usr-31145		2	2	01:14:58
Usr-62089		1	0	00:15:22
Usr-6403		1	1	00:14:24
Usr-62089		1	1	00:20:55
Usr-62089		1	0	00:17:11
Usr-62089		1	0	00:00:00
Usr-6403		1	1	00:13:36
Usr-46838		1	0	00:03:00
Usr-62089		1	0	00:10:04
Usr-31145		1	1	01:38:00
Usr-31145		1	0	00:00:34

Copyright 2018 HighTechSystem Co., Ltd.

FortiGateへの管理者ログイン失敗

FortiGateに管理者ログインを失敗したホスト（IP）の上位20個です。失敗回数が多い場合は、不正なログインを試行されていないか調査が推奨されます。

Login Source	User Name	Total Number of Failed Logins
ログイン方法 及び IPアドレス	Usr-62089	91
	Usr-62089	9
	Usr-46838	5
	Usr-62089	4
	Usr-62089	4
	Usr-62089	3
	Usr-31145	3
	Usr-46838	3
	Usr-62089	2
	Usr-7464	2
	Usr-6403	2
	Usr-62089	2
	Usr-31145	1
	Usr-62089	1
	Usr-34750	1
	Usr-22584	1
	Usr-62089	1
	Usr-62089	1
	Usr-31145	1
	Usr-31145	1
	Usr-62089	1

FortiGateでの認証失敗

SSL-VPN接続など、FortiGateで認証機能を利用している場合の認証失敗記録上位5ユーザです。失敗回数が多い場合は、不正な認証を試行されていないか調査が推奨されます。

User	Type	# of Failed Authentications
Usr-34750	ssl-web	26

Copyright 2018 HighTechSystem Co., Ltd.

FortiGateの設定変更履歴

FortiGateでいつ、だれが、何の設定を行ったのかの変更履歴になります。管理者が把握している変更以外の履歴がある場合は調査が推奨されます。

User	Device	Date/Time	User Interface	Action Performed
Usr-62089	FortiGateホスト名	2018-09-25 12:41:05	ログイン方法及びIPアドレス	Edit system.global
Usr-62089		2018-09-25 12:41:41		Edit system.admin ユーザ名
Usr-62089		2018-09-25 12:42:59		Add system.admin ユーザ名
Usr-62089		2018-09-25 12:46:40		Add system.admin ユーザ名
Usr-62089		2018-09-25 12:47:26		Add system.admin ユーザ名
Usr-62089		2018-09-25 12:48:25		Add system.admin ユーザ名
Usr-46838		2018-09-25 12:49:16		Edit system.admin ユーザ名
Usr-62089		2018-09-25 17:58:39		Edit system.global
Usr-62089		2018-09-25 18:17:13		Edit system.global
Usr-62089		2018-09-25 19:06:09		Add ips.sensor:entries default :3
Usr-62089		2018-09-25 19:06:09		Delete ips.sensor:entries default:4
Usr-62089		2018-09-25 19:06:09		Delete ips.sensor:entries default:3
Usr-62089		2018-09-25 19:06:09		Move ips.sensor:entries default:2->default:2
Usr-62089		2018-09-25 19:10:50		Add ips.sensor:entries default :3
Usr-62089		2018-09-25 19:10:50		Delete ips.sensor:entries default:3
Usr-62089		2018-09-25 19:10:50		Add ips.sensor:entries default :4
Usr-62089		2018-09-25 19:10:50		Move ips.sensor:entries default:2->default:3
Usr-62089		2018-09-25 19:14:55		Add ips.sensor:entries default :3
Usr-62089		2018-09-25 19:14:55		Delete ips.sensor:entries default:3
Usr-62089		2018-09-25 19:14:55		Add ips.sensor:entries default :4
Usr-62089		2018-09-25 19:14:55		Move ips.sensor:entries default:2->default:3
Usr-62089		2018-09-25 19:14:55		Delete ips.sensor:entries default:4
Usr-62089		2018-09-25 19:18:05		Move ips.sensor:entries default:2->default:3
Usr-62089		2018-09-25 19:18:05		Add ips.sensor:entries default :3
Usr-62089		2018-09-25 19:18:05		Delete ips.sensor:entries default:4
Usr-62089		2018-09-25 19:18:05		Add ips.sensor:entries default :4
Usr-62089		2018-09-25 19:18:05		Delete ips.sensor:entries default:3
Usr-62089		2018-09-25 19:21:43		Add ips.sensor:entries default :3
Usr-62089		2018-09-25 19:21:43		Move ips.sensor:entries default:2->default:2
Usr-62089		2018-09-25 19:21:43		Delete ips.sensor:entries default:4

Copyright 2018 HighTechSystem Co., Ltd.

Appendix F

デバイスリスト

TSOCにて分析対象のログを収集したFortiGateの情報です。通常は対象のFortiGate（1台）の情報が表示され、複数台を対象に分析した場合は、対象機器が全て表示されます。

名前	SN	IPアドレス
FortiGateホスト名	FortiGate シリアルナンバー	FortiGate IPアドレス

Copyright 2018 HighTechSystem Co., Ltd.