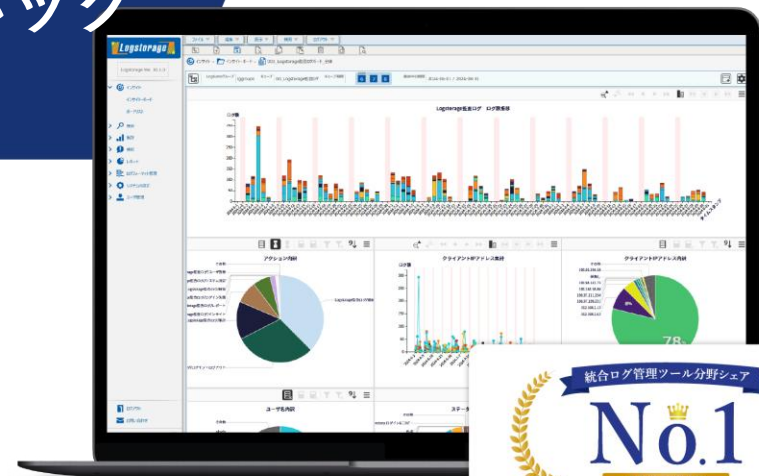


Logstorage **VER. 10**

統合ログ管理システム「ログストレージ」

Logstorage

Palo Alto Networks NGFW 連携パック
参考資料



Logstorage 連携パックとは

連携パックは、各分野で人気の製品と連携して開発した「ログの収集・分析がすぐにスタートできる」Logstorageのオプション製品です。

連携パックを導入することで、各連携製品のログ管理のセットアップを簡略化できるほか、運用中に、収集対象のログのフォーマット(並び順や表示の仕方)や出力方法に変更があっても、各連携パックのバージョンアップで、変更を反映できます。

「アップデートでログの保管先が変わった」

「出力されるログの内容が変わった」

「保管するログのサイズが増えた」

「仕様変更でログの種類が増えた」

「独自の収集プログラムが
仕様変更で作り直し」



技術者のリソースが
ログ管理に取られすぎる



パッケージ内容

Logstorage 連携パックには、専用のログ収集モジュール・ログフォーマット定義ファイル・分析テンプレートが含まれます。

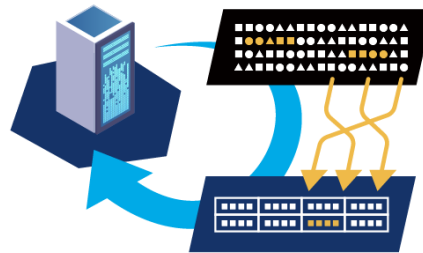
ログ収集モジュール



製品ごとにログの出力方法や出力先は異なります。各製品のログにあわせたログ収集モジュールをご用意しております。

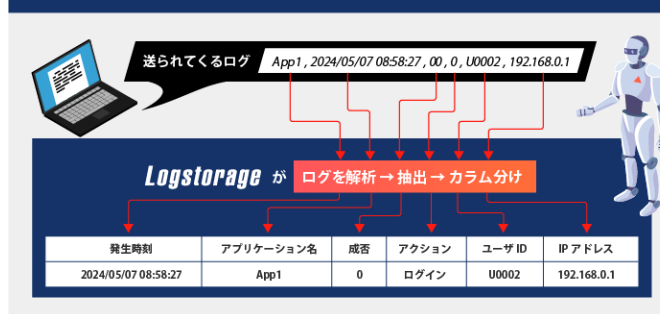
※製品によっては収集モジュールが不要の場合もございます。
その場合、パッケージに含まれませんので、ご了承ください。

ログフォーマット定義ファイル



連携している製品のログフォーマット（並び順や表示の仕方）を分析し、ログを項目ごとに抽出します。

ログフォーマット定義とは？

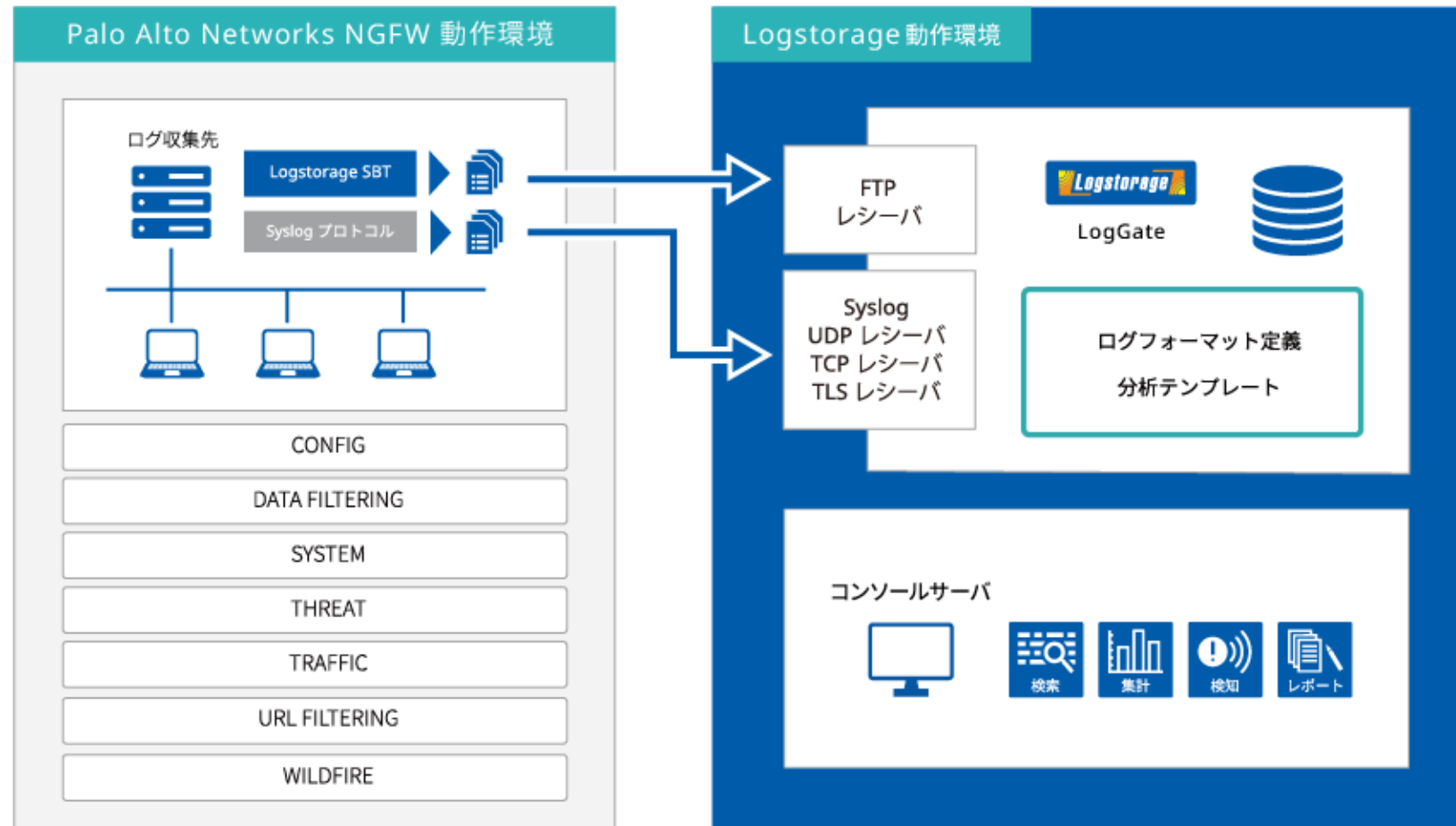


分析テンプレート



各製品から出力される多数のログの中から、どのログを検索すればよいのか・何を集計したらよいのか・どんなレポートを出力すればよいのか、ログ分析をサポートする分析テンプレートをご提供いたします。

システム構成



検索テンプレート一覧

Logstorage Palo Alto Networks NGFW 連携パック の検索テンプレートは以下の通りです。

ファイル名	検索条件テンプレート名
ログ分析レポート	脅威可視化レポート

検索条件テンプレート名
DATAフィルタリングログ
THREAT-WILDFIRE
URLフィルタリングログ
コンフィグログ
システムログ
トラフィックログ
全ログ
脅威ログ

集計テンプレート一覧

Logstorage Palo Alto Networks NGFW 連携パック の集計テンプレートは以下の通りです。

フォルダ名	集計条件テンプレート名
URLフィルタリングログ	Webアクセス件数推移(1日合計／月次)
URLフィルタリングログ	Webアクセス件数推移(1時間合計／日次)
URLフィルタリングログ	Webアクセス件数推移(曜日合計／週次)
URLフィルタリングログ	Webアクセス件数／カテゴリ別
URLフィルタリングログ	Webアクセス件数／サイト別
URLフィルタリングログ	Webカテゴリ別利用ユーザー一覧
URLフィルタリングログ	Webサイト別利用ユーザー一覧
トラフィックログ	アプリケーションの利用状況
トラフィックログ	アプリケーション別利用ユーザ／端末一覧
トラフィックログ	通信量推移(1日合計／月次)
トラフィックログ	通信量推移(1時間合計／日次)
トラフィックログ	通信量推移（曜日合計／週次）
脅威ログ	ウィルス検知
脅威ログ	ウィルス検知 ウィルス毎発生比率
脅威ログ	スパイウェア検知
脅威ログ	脆弱性検知
脅威ログ	脆弱性検知 脆弱性毎発生比率

レポートテンプレート一覧

Logstorage Palo Alto Networks NGFW 連携パック のレポートテンプレートは以下の通りです。

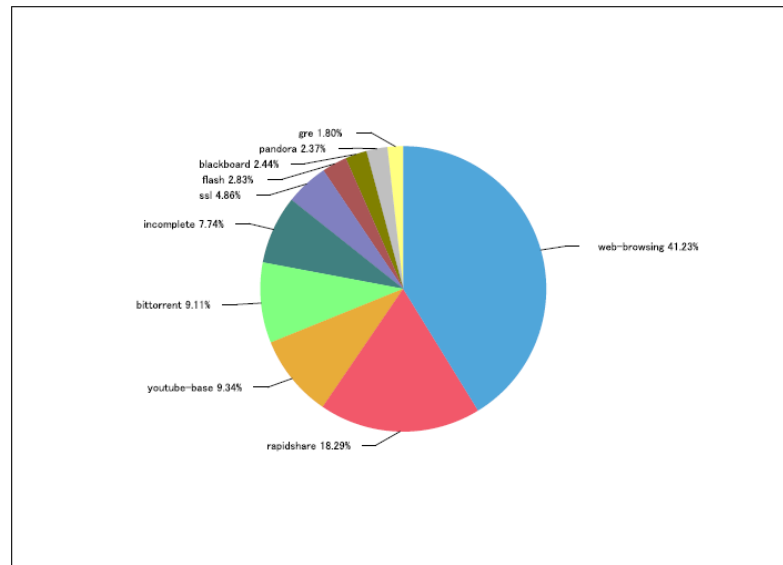
フォルダ名	検索条件テンプレート名	概要
URLフィルタリングログ	Webアクセス件数推移(1日合計／月次)	アクセス先上位10サイト (1日合計／月次)
URLフィルタリングログ	Webアクセス件数推移(1時間合計／日次)	アクセス先上位10サイト (1時間合計／日次)
URLフィルタリングログ	Webアクセス件数推移(曜日合計／週次)	アクセス先上位10サイト (曜日合計／週次)
URLフィルタリングログ	Webアクセス件数／カテゴリ別	アクセス先上位10カテゴリ
URLフィルタリングログ	Webアクセス件数／サイト別	アクセス先上位10サイト
URLフィルタリングログ	Webカテゴリ別利用ユーザー一覧	アクセス先Webカテゴリ別利用ユーザー一覧
URLフィルタリングログ	Webサイト別利用ユーザー一覧	アクセス先Webサイト別利用ユーザー一覧
トラフィックログ	アプリケーションの利用状況	通信量上位10アプリケーション
トラフィックログ	アプリケーション別利用ユーザー／端末一覧	アプリケーション別利用ユーザー／端末一覧
トラフィックログ	通信量推移(1日合計／月次)	通信量上位10アプリケーション別通信量推移(1日合計／月次)
トラフィックログ	通信量推移(1時間合計／日次)	通信量上位10アプリケーション別通信量推移(1時間合計／日次)
トラフィックログ	通信量推移(曜日合計／週次)	通信量上位10アプリケーション別通信量推移(曜日合計／週次)
ログ分析レポート	脅威可視化レポート	-
脅威ログ	ウィルス検知 ウィルス毎発生比率	-
脅威ログ	スパイウェア検知	-
脅威ログ	スパイウェア検知 スパイウェア毎発生比率	-
脅威ログ	脆弱性検知	-
脅威ログ	脆弱性検知 脆弱性毎発生比率	-

レポート例 1

トラフィックログ

アプリケーションの利用状況

概要 通信量上位10アプリケーション
作成日 2013-04-03 10:35:07
対象期間 2013-03-20 00:00:00 - 2013-03-31 23:59:59



順位	アプリケーション	通信量 (Mバイト)
1	web-browsing	6263.62
2	rapidshare	2779.19
3	youtube-base	1419.29
4	bittorrent	1383.97
5	incomplete	1176.45
6	ssl	737.65
7	flash	429.87
8	blackboard	370.99
9	pandora	359.67
10	gre	272.75

アプリケーション別利用ユーザ／端末一覧

概要 通信量上位10アプリケーション別利用ユーザ／端末一覧
作成日 2013-04-03 10:40:42
対象期間 2013-03-20 00:00:00 - 2013-03-31 23:59:59

アプリケーション	順位	src_ip	src_user	通信量 (Mバイト)
web-browsing	1	10.10.10.1	bigcompany*	719.26
	2	10.10.10.2	bigcompany*	355.79
	3	10.10.10.3	bigcompany*	287.14
	4	10.10.10.4	bigcompany*	242.06
	5	10.10.10.5	bigcompany*	158.03
	6	10.10.10.6	bigcompany*	130.27
	7	10.10.10.7	bigcompany*	107.27
	8	10.10.10.8	bigcompany*	93.44
	9	10.10.10.9	bigcompany*	91.31
	10	10.10.10.10	bigcompany*	79.32

アプリケーション	順位	src_ip	src_user	通信量 (Mバイト)
rapidshare	1	10.10.10.1	bigcompany*	2779.12
	2	10.10.10.2	bigcompany*	0.05
	3	10.10.10.3	bigcompany*	0.02

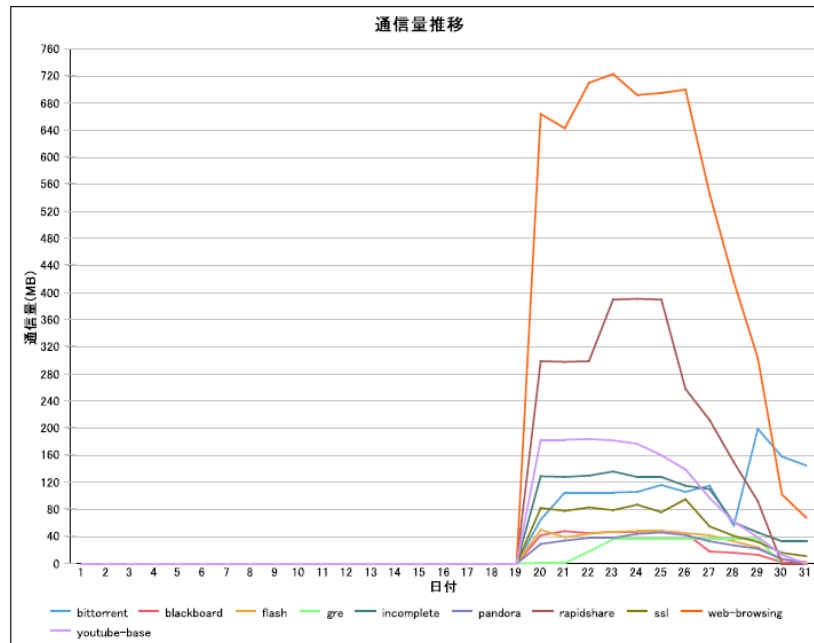
アプリケーション	順位	src_ip	src_user	通信量 (Mバイト)
youtube-base	1	10.10.10.1	bigcompany*	253.82
	2	10.10.10.2	bigcompany*	161.82
	3	10.10.10.3	bigcompany*	135.51
	4	10.10.10.4	bigcompany*	123.62
	5	10.10.10.5	bigcompany*	120.92
	6	10.10.10.6	bigcompany*	103.15
	7	10.10.10.7	bigcompany*	82.93
	8	10.10.10.8	bigcompany*	79.89
	9	10.10.10.9	bigcompany*	67.77
	10	10.10.10.10	bigcompany*	60.66

レポート例 2

トラフィックログ

通信量推移(1日合計／月次)

概要 通信量上位10アプリケーション別通信量推移(1日合計／月次)
作成日 2013-04-03 10:56:32
対象期間 2013-03-01 00:00:00 - 2013-03-31 23:59:59



通信量推移(1時間平均／週次)

概要 通信量上位10アプリケーション別通信量推移(1時間平均／週次)
作成日 2013-04-03 14:53:02
対象期間 2013-03-20 00:00:00 - 2013-03-26 23:59:59

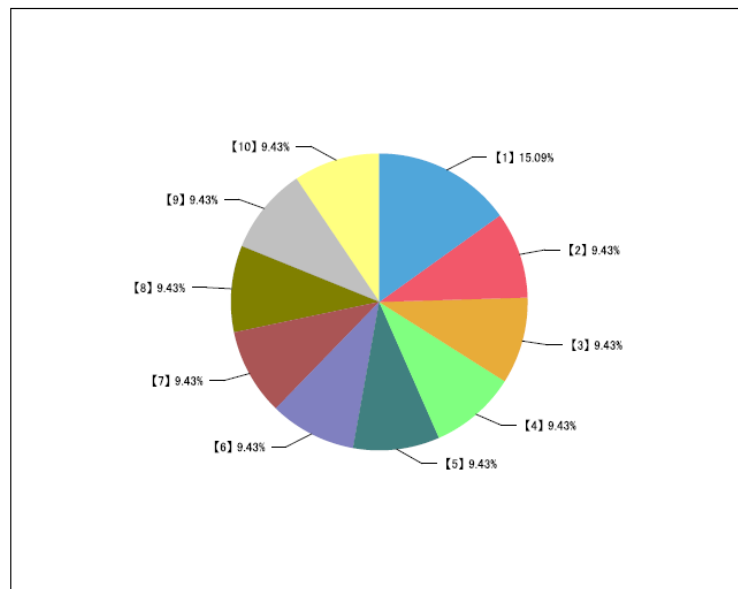


レポート例 3

脅威ログ

ウイルス検知 ウィルス毎発生比率

概要 上位10ウイルスイベント発生比率
作成日 2013-04-03 11:24:22
対象期間 2013-03-27 00:00:00 - 2013-03-27 23:59:59



順位	脅威ID	レベル	件数
1	Trojan/Heur.ucky.t(2057199)	medium	8
2	Backdoor/Win32.HackTack.c(2016111)	medium	5
3	Backdoor/Win32.Rbot.agw(2007829)	medium	5
4	Backdoor/Win32.Rbot.ais(2015339)	medium	5
5	Backdoor/Win32.Rbot.bky(2017392)	medium	5
6	Backdoor/Win32.turkojan.r(2002785)	medium	5
7	Email/Win32.Brntoks.s(2005377)	medium	5
8	JS/Exploit.pdf-js.cm(280076)	medium	5
9	JS/Exploit.pdf-js.kz(281505)	medium	5
10	JS/Exploit.pdfka.hyv(280404)	medium	5

ウイルス検知

概要 上位10ウイルスイベント別送信元IP、送信元IP/ポート
作成日 2013-04-03 11:22:32
対象期間 2013-03-27 00:00:00 - 2013-03-27 23:59:59

Trojan/Heur.ucky.t(2057199)

順位	src_ip	dst_ip	dst_port	件数
1	10.10.10.10	66.255.255.255	58831	4
2	10.10.10.10	66.255.255.255	31371	4

Backdoor/Win32.HackTack.c(2016111)

順位	src_ip	dst_ip	dst_port	件数
1	66.255.255.255	10.10.10.10	25	5

Backdoor/Win32.Rbot.agw(2007829)

順位	src_ip	dst_ip	dst_port	件数
1	66.255.255.255	10.10.10.10	25	5

Backdoor/Win32.Rbot.ais(2015339)

順位	src_ip	dst_ip	dst_port	件数
1	66.255.255.255	10.10.10.10	25	5

Backdoor/Win32.Rbot.bky(2017392)

順位	src_ip	dst_ip	dst_port	件数
1	66.255.255.255	10.10.10.10	25	5

Backdoor/Win32.turkojan.r(2002785)

順位	src_ip	dst_ip	dst_port	件数
1	66.255.255.255	10.10.10.10	25	5

Email/Win32.Brntoks.s(2005377)

順位	src_ip	dst_ip	dst_port	件数
1	66.255.255.255	10.10.10.10	25	5

JS/Exploit.pdf-js.cm(280076)

順位	src_ip	dst_ip	dst_port	件数
1	66.255.255.255	10.10.10.10	25	5

JS/Exploit.pdf-js.kz(281505)

順位	src_ip	dst_ip	dst_port	件数
1	66.255.255.255	10.10.10.10	25	5

JS/Exploit.pdfka.hyv(280404)

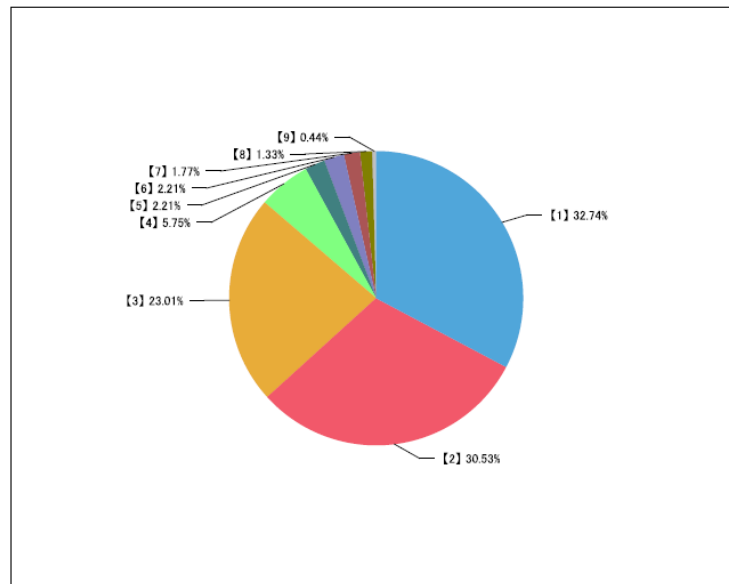
順位	src_ip	dst_ip	dst_port	件数
1	66.255.255.255	10.10.10.10	25	5

レポート例 4

脅威ログ

スパイウェア検知 スパイウェア毎発生比率

概要 上位10スパイウェアイベント発生比率
作成日 2013-04-03 11:28:07
対象期間 2013-03-27 00:00:00-2013-03-27 23:59:59



順位	脅威ID	レベル	件数
1	Trojan-Virtumondo.Phonehome(19882)	high	74
2	PDF Object Definition Anomaly(12600)	informational	69
3	Sipivicious.sundayddr User-Agent Traffic(13273)	low	52
4	ZeroAccess.Gen Command and Control Traffic(13235)	critical	13
5	Hotbar.10.0.368 Get image Request(11964)	medium	5
6	Suspicious user-agent strings(10004)	medium	5
7	Nsanti User-Agent Traffic(10028)	medium	4
8	Trojan.Hanabot(12646)	low	3
9	Rogue DNS Servers Request(13125)	medium	1

スパイウェア検知

概要 上位10スパイウェアイベント別送信元IP、送信先IP/ポート
作成日 2013-04-03 11:28:12
対象期間 2013-03-27 00:00:00-2013-03-27 23:59:59

順位	src_ip	dst_ip	dst_port	件数
1	82.207.10.10	10.10.10.10	2583	5
2	82.207.10.10	10.10.10.10	2670	5
3	82.207.10.10	10.10.10.10	2720	5
4	82.207.10.10	10.10.10.10	2793	5
5	82.207.10.10	10.10.10.10	2813	5
6	82.207.10.10	10.10.10.10	2986	5
7	82.207.10.10	10.10.10.10	3015	5
8	82.207.10.10	10.10.10.10	3182	5
9	82.207.10.10	10.10.10.10	3193	5
10	82.207.10.10	10.10.10.10	3208	5

順位	src_ip	dst_ip	dst_port	件数
1	66.255.149.100	10.10.10.10	25	5
2	10.10.10.10	66.255.149.100	21850	4
3	10.10.10.10	66.255.149.100	30995	4
4	10.10.10.10	66.255.149.100	35265	4
5	10.10.10.10	66.255.149.100	40592	4
6	10.10.10.10	66.255.149.100	9073	4
7	10.10.10.10	66.255.149.100	64508	4
8	10.10.10.10	66.255.149.100	30381	4
9	10.10.10.10	66.255.149.100	49893	4
10	10.10.10.10	66.255.149.100	31023	4

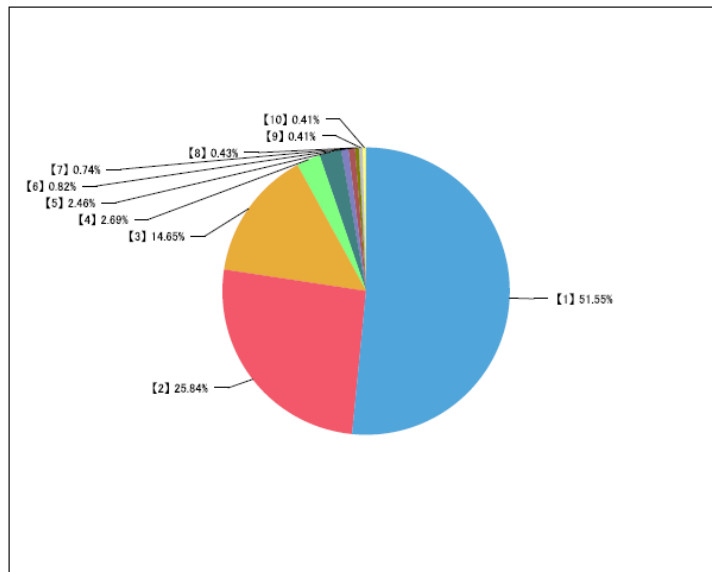
順位	src_ip	dst_ip	dst_port	件数
1	115.159.10.10	10.10.10.10	5060	5
2	115.159.10.10	10.10.10.10	5060	5
3	202.10.10.10	10.10.10.10	5060	5
4	202.10.10.10	10.10.10.10	5060	5
5	219.10.10.10	10.10.10.10	5060	5
6	219.10.10.10	10.10.10.10	5060	5
7	219.10.10.10	10.10.10.10	5060	5
8	219.10.10.10	10.10.10.10	5060	5
9	219.10.10.10	10.10.10.10	5060	5
10	202.10.10.10	10.10.10.10	5060	4

レポート例 5

脅威ログ

脆弱性検知 脆弱性毎発生比率

概要 上位10脆弱性イベント発生比率
作成日 2013-04-03 11:31:42
対象期間 2013-03-27 00:00:00-2013-03-27 23:59:59



順位	脅威ID	レベル	件数
1	SSH2 Login Attempt(31914)	informational	28823
2	Microsoft SQL Server Stack Overflow Vulnerability(30009)	critical	14449
3	SSH User Authentication Brute-force Attempt(40015)	high	8191
4	Email Protocol Attachment Evasive Encoding Found(33797)	high	1503
5	DNS ANY Request(34842)	informational	1376
6	FTP Login Failed(40000)	informational	456
7	Cisco IOS HTTP Configuration Arbitrary Administrative Access Vulnerability(30921)	high	415
8	HTTP Unauthorized Error(34556)	informational	239
9	Microsoft Office Object Type Confusion Vulnerability(33845)	high	230
10	SSL Renegotiation Denial of Service Vulnerability(33862)	low	228

脆弱性検知

概要 上位10脆弱性イベント別送信元IP、送信元IP/ポート
作成日 2013-04-03 11:29:27
対象期間 2013-03-27 00:00:00-2013-03-27 23:59:59

順位	src_ip	dst_ip	dst_port	件数
1	202.10.10.10	10.10.10.10	22	419
2	202.10.10.10	10.10.10.10	22	415
3	202.10.10.10	10.10.10.10	22	414
4	202.10.10.10	10.10.10.10	22	413
5	202.10.10.10	10.10.10.10	22	413
6	202.10.10.10	10.10.10.10	22	412
7	202.10.10.10	10.10.10.10	22	411
8	202.10.10.10	10.10.10.10	22	410
9	202.10.10.10	10.10.10.10	22	408
10	202.10.10.10	10.10.10.10	22	405

順位	src_ip	dst_ip	dst_port	件数
1	10.10.10.10	10.10.10.10	1434	5
2	10.10.10.10	10.10.10.10	1434	5
3	10.10.10.10	10.10.10.10	1434	5
4	10.10.10.10	10.10.10.10	1434	5
5	10.10.10.10	10.10.10.10	1434	5
6	10.10.10.10	10.10.10.10	1434	5
7	10.10.10.10	10.10.10.10	1434	5
8	10.10.10.10	10.10.10.10	1434	5
9	10.10.10.10	10.10.10.10	1434	5
10	10.10.10.10	10.10.10.10	1434	5

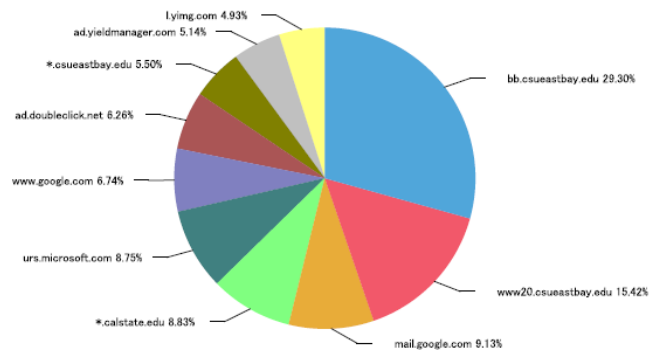
順位	src_ip	dst_ip	dst_port	件数
1	202.10.10.10	10.10.10.10	22	314
2	202.10.10.10	10.10.10.10	22	303
3	202.10.10.10	10.10.10.10	22	297
4	202.10.10.10	10.10.10.10	22	295
5	202.10.10.10	10.10.10.10	22	294
6	202.10.10.10	10.10.10.10	22	293
7	202.10.10.10	10.10.10.10	22	290
8	202.10.10.10	10.10.10.10	22	273
9	202.10.10.10	10.10.10.10	22	272
10	202.10.10.10	10.10.10.10	22	264

レポート例 6

URLフィルタリングログレポート

Webアクセス件数／サイト別

概要 アクセス先上位10サイト
作成日 2013-04-03 13:52:12
対象期間 2013-03-19 00:00:00 - 2013-03-19 23:59:59



順位	Webサイト	件数
1	bb.csueastbay.edu	3920
2	www20.csueastbay.edu	2063
3	mail.google.com	1221
4	*.calstate.edu	1181
5	urs.microsoft.com	1170
6	www.google.com	902
7	ad.doubleclick.net	837
8	*.csueastbay.edu	736
9	ad.yieldmanager.com	688
10	lyimg.com	660

Webサイト別利用ユーザー一覧

概要 アクセス先Webサイト別利用ユーザー一覧
作成日 2013-04-03 13:55:07
対象期間 2013-03-19 00:00:00 - 2013-03-19 23:59:59

Webサイト	順位	src_ip	src_user	件数
bb.csueastbay.edu/	1	137.162.1.1	--	90
	2	50.1.1.1	--	55
	3	67.1.1.1	--	52
	4	68.1.1.1	--	52
	5	66.2.1.1	--	51
	6	162.1.1.1	--	48
	7	76.2.1.1	--	48
	8	67.1.1.1	--	44
	9	75.1.1.1	--	39
	10	166.1.1.1	--	38

Webサイト	順位	src_ip	src_user	件数
.calstate.edu/	1	10.1.1.1	bigcompany	107
	2	10.1.1.1	bigcompany*	73
	3	10.1.1.1	bigcompany*	48
	4	10.1.1.1	bigcompany*	37
	5	10.1.1.1	bigcompany*	34
	6	10.1.1.1	bigcompany*	32
	7	10.1.1.1	bigcompany*	31
	8	10.1.1.1	bigcompany*	31
	9	10.1.1.1	bigcompany*	30
	10	10.1.1.1	bigcompany*	30

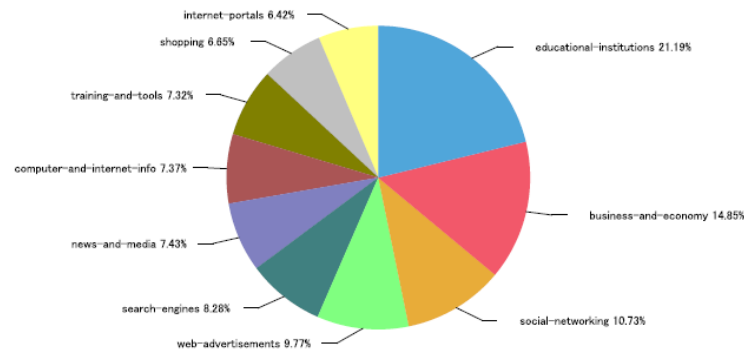
Webサイト	順位	src_ip	src_user	件数
urs.microsoft.com/	1	10.1.1.1	bigcompany*	36
	2	10.1.1.1	bigcompany*	28
	3	10.1.1.1	bigcompany*	27
	4	10.1.1.1	bigcompany*	25
	5	10.1.1.1	bigcompany*	24
	6	10.1.1.1	bigcompany*	24
	7	10.1.1.1	bigcompany*	23
	8	10.1.1.1	bigcompany*	22
	9	10.1.1.1	bigcompany*	22
	10	10.1.1.1	bigcompany*	21

レポート例 7

URLフィルタリングログレポート

Webサイトアクセス件数／カテゴリ別

概要 アクセス先上位10カテゴリ
作成日 2013-04-03 13:53:37
対象期間 2013-03-19 00:00:00 - 2013-03-19 23:59:59



順位	カテゴリ	件数
1	educational-institutions	9253
2	business-and-economy	6486
3	social-networking	4687
4	web-advertisements	4266
5	search-engines	3615
6	news-and-media	3246
7	computer-and-internet-info	3220
8	training-and-tools	3198
9	shopping	2903
10	internet-portals	2802

Webサイトカテゴリ別利用ユーザー一覧

概要 アクセス先Webサイトカテゴリ別利用ユーザー一覧
作成日 2013-04-04 10:44:18
対象期間 2013-03-19 00:00:00 - 2013-03-19 23:59:59

カテゴリ	順位	src_ip	src_user	件数
educational-institutions	1	10.10.10.10	-	115
	2	10.10.10.10	bigcompany¥	112
	3	10.10.10.10	-	110
	4	10.10.10.10	-	95
	5	10.10.10.10	-	95
	6	10.10.10.10	-	91
	7	10.10.10.10	-	81
	8	10.10.10.10	bigcompany¥	78
	9	10.10.10.10	bigcompany¥	77
	10	10.10.10.10	-	77

カテゴリ	順位	src_ip	src_user	件数
business-and-economy	1	10.10.10.10	bigcompany¥	229
	2	10.10.10.10	bigcompany¥	174
	3	10.10.10.10	bigcompany¥	166
	4	10.10.10.10	bigcompany¥	122
	5	10.10.10.10	bigcompany¥	98
	6	10.10.10.10	bigcompany¥	90
	7	10.10.10.10	bigcompany¥	82
	8	10.10.10.10	bigcompany¥	82
	9	10.10.10.10	bigcompany¥	74
	10	10.10.10.10	bigcompany¥	71

カテゴリ	順位	src_ip	src_user	件数
social-networking	1	10.10.10.10	bigcompany¥	207
	2	10.10.10.10	bigcompany¥	185
	3	10.10.10.10	bigcompany¥	174
	4	10.10.10.10	bigcompany¥	119
	5	10.10.10.10	bigcompany¥	108
	6	10.10.10.10	bigcompany¥	102
	7	10.10.10.10	bigcompany¥	101
	8	10.10.10.10	bigcompany¥	99
	9	10.10.10.10	bigcompany¥	97
	10	10.10.10.10	bigcompany¥	93

お問い合わせ

ご不明点、ご相談につきましては、下記お問い合わせ先からご連絡ください。

電話でのお問い合わせ

03-5427-3503

【受付】 平日 9:00～17:30

メールでのお問い合わせ

info@logstorage.com

会社名・氏名・メールアドレス・電話番号を
ご記入の上、お問い合わせください

当社のホームページでも資料請求・お問い合わせができます。

<https://logstorage.com>