

10分で分る！

Zabbixと連携できる

Syslogサーバでログ監視をする方法

2025年11月4日

ぷらっとホーム株式会社 清水



はじめに

Zabbixとログ保存の深い関係

- ネットワーク構築のご相談をいただくケースが多々あり、
「監視機能ならZabbix」「ログ保存なら当社Syslogアプライアンス」を提案している
- 「Zabbixサーバーでのログ監視を行いたいが、サーバーの負荷やストレージ容量が気になる」
というご相談を頂くことが増えている

お問い合わせを受けて、Zabbixサーバー連携機能を実装

- 上記の問い合わせ状況を踏まえて、2024年5月に当社のSyslogサーバーから
Zabbixサーバーへログを転送する機能が追加
- Zabbix Agentに対応していない機器のログ収集や大量のログ保存・ログ監視にも対応

本日の流れ

- 01 自己紹介と会社概要
- 02 Zabbix Japanとの歴史
- 03 アプライアンス製品のトレンドは？
- 04 Zabbix連携機能について
- 05 EasyBlocks Smart log seriesとは
- 06 欠かせない3つのサイジング方法
- 07 【参考】自社環境でサイジングしてみた！

自己紹介



ぷらっとホーム株式会社
清水 教彦

所属部署

事業推進グループ パートナー営業担当

営業活動の一環としてセミナーや展示会などのイベント・ブログ執筆など、多岐に渡りパートナー様向けの活動を行う。

ひとこと

ハードウェアメーカーとして2014年からZabbixサービスの推進を行うぷらっとホームで、パートナー営業を担当しています。本イベントでは異色な存在かもしれませんが、Zabbix Japan創立初期から携わるのメーカー企業の目線を大切に、Zabbixに関連するイベントへの参加・セミナーへの登壇を行なっています。

ちなみに、バランスボールに乗って仕事をしています。

会社概要 COMPANY IDENTIFICATION

Plat'Home ぷらっとホーム株式会社

✦ TECHNOLOGY to serve you.

1993年創業。Linuxをはじめとするコンピューターに関わるアプライアンス、サービスを提供しており、Zabbixリセラーとして12年目を迎えました。
ただ製品を提供するだけではなく「成長をともにするパートナーに。」をコンセプトに、ブログやセミナー無料相談会などお客様への価値提供にも力をいれています。

設立 : 1993年3月23日

資本金 : 1億円

所在地 : 東京都千代田区九段北4-1-3日本ビルディング九段別館3F

代表 : 代表取締役社長 鈴木友康

事業内容: IoTゲートウェイ・マイクロサーバー
ネットワーク関連製品の開発・販売

上場市場: 東京証券取引所 スタンダード市場



ログ監視、必要？

— EasyBlocks Smart log series —

アプライアンス製品のトレンドは？

※2022年度と2024年度の比較

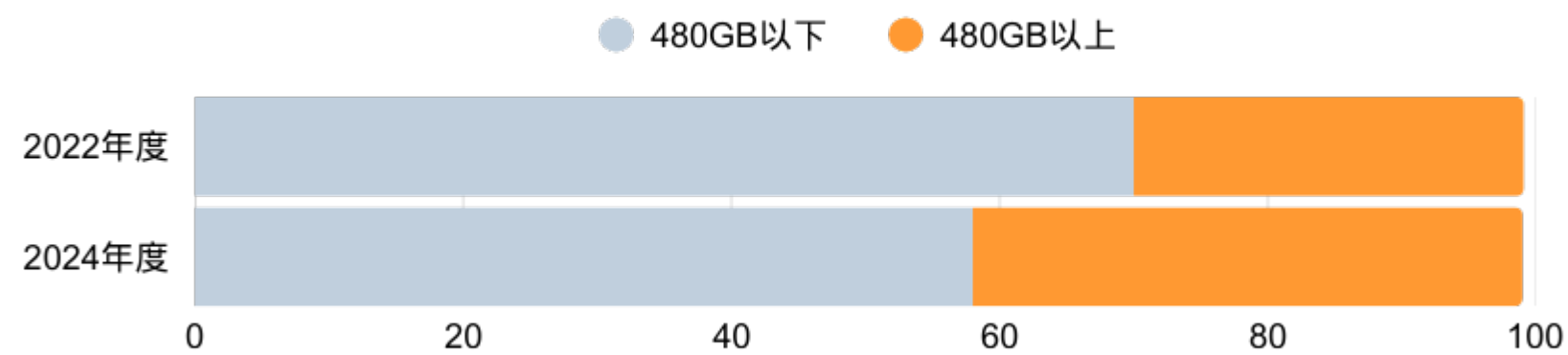
『Syslogアプライアンス』

問合せ数

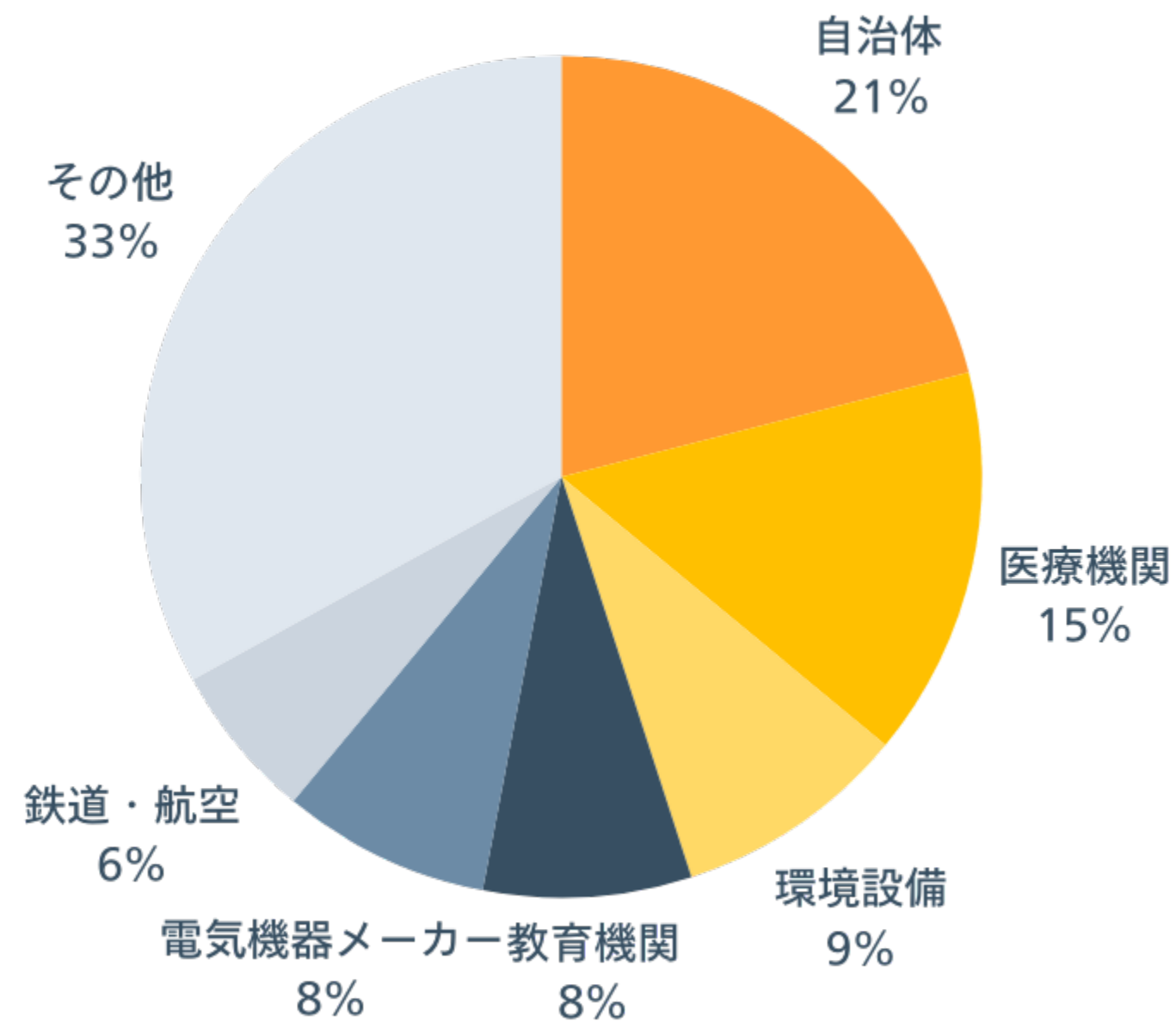
約 **2** 倍に増加

ストレージ容量

問い合わせ増加に伴い、
実際の案件でもストレージ容量は**増加傾向**



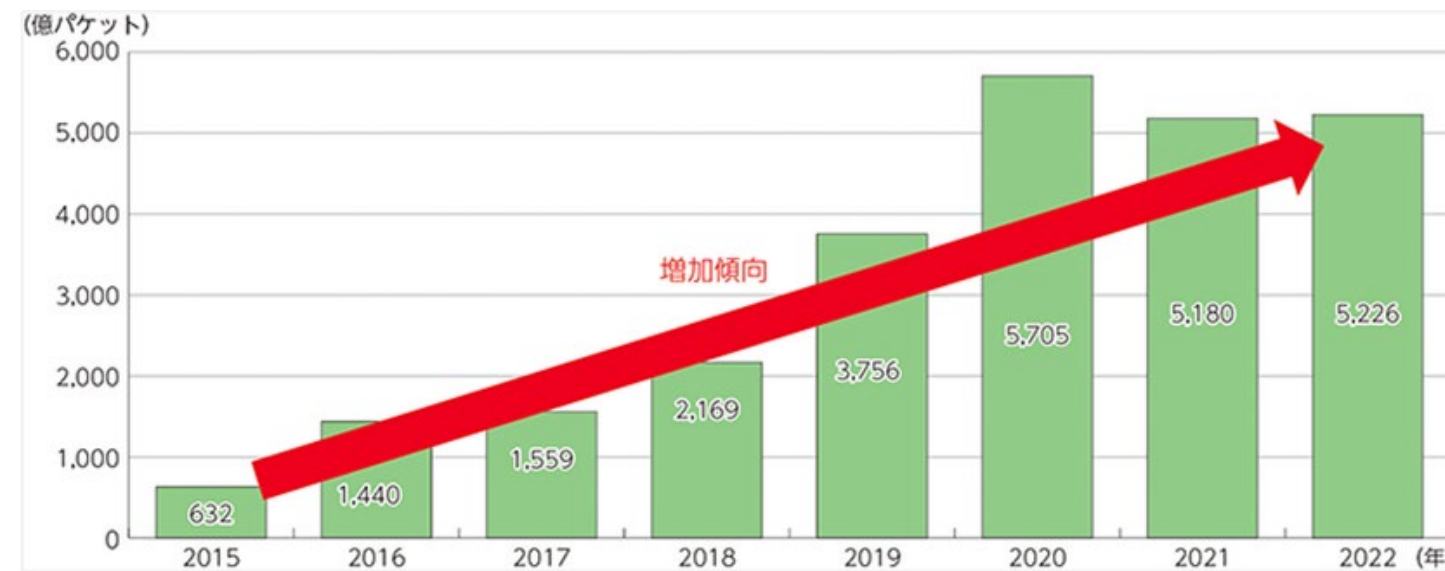
業種別比率



問い合わせ数増加の背景

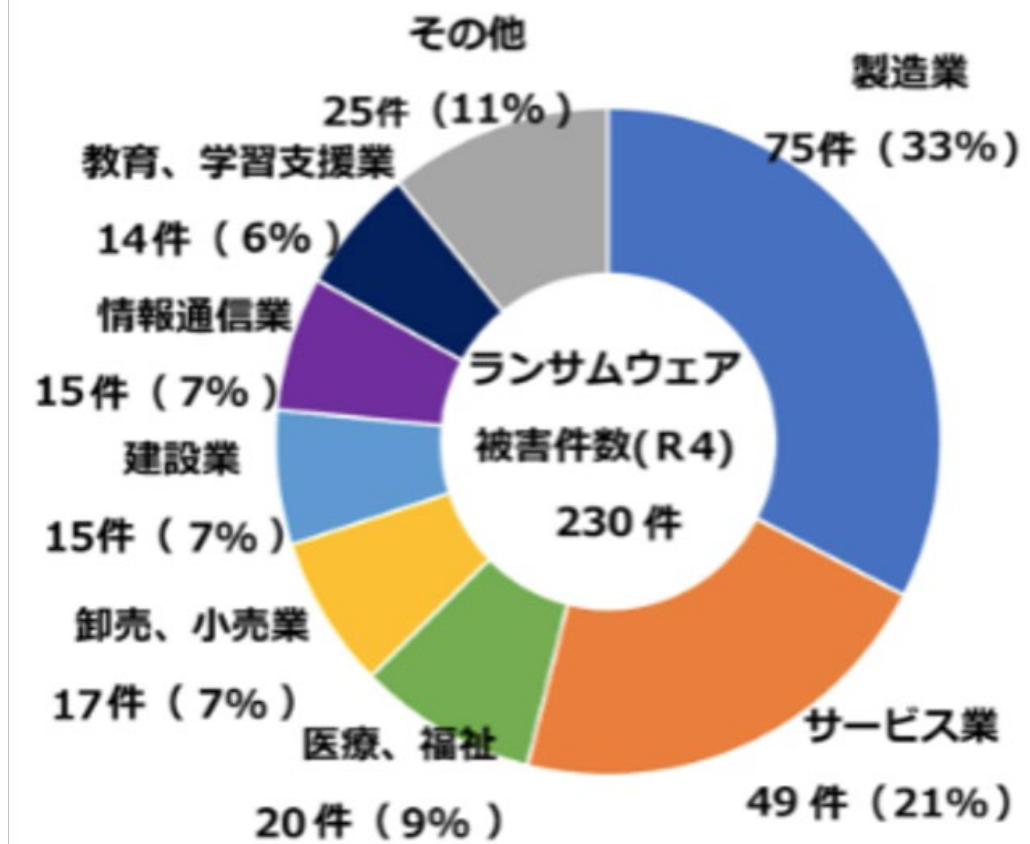
年々増加するサイバー攻撃対策

- 2015年以降、年々増加傾向にある
- 各IPアドレスに対して、17秒に1回の頻度で攻撃関連の通信が行われている



出典) 総務省 情報通信白書 令和5年版「情報通信分野の現状と課題」NICT「NICTER観測レポート2022」
<https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r05/html/nd24a210.html>

サイバー攻撃の事例



注 図中の割合は小数点第1位以下を四捨五入しているため、総計が必ずしも100にならない。

出展)警察庁 令和4年におけるサイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf

Zabbix連携機能

— EasyBlocks Smart log series —

Zabbixサーバーへのログ転送機能

新機能追加の背景

問い合わせの増加

セキュリティ対策の一環としてログサーバーの需要が高まる中、Zabbix Agentに対応していない機器のログ収集課題などZabbixを使用したログ監視に関する問い合わせが増加傾向にある

Zabbixサーバーへの負荷やストレージ容量の懸念

監視とログの収集をZabbixサーバーで同時に行うと負荷がかかったり、ストレージ容量が足りなくなったりするなどの課題がある

構築・運用の手間がかかる

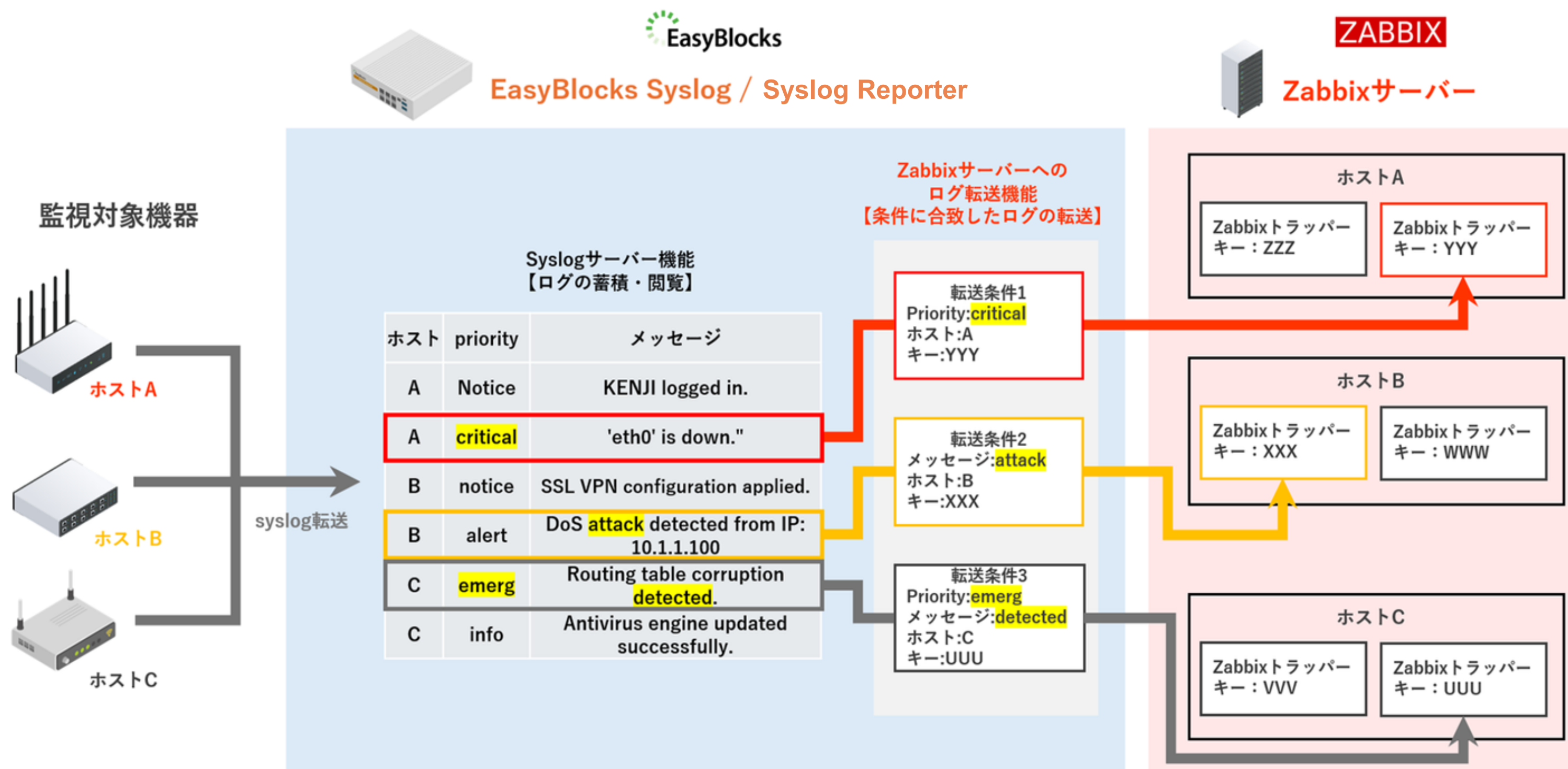
ログ収集を別で行う場合、Zabbixを使用したログ監視を行うための仕組みをつくる必要があるため、構築や運用の手間がかかる

Syslogアプライアンスで解決！

『EasyBlocks Smart log series』で そのお悩み、解決できます！

Syslogの収集はアプライアンス製品が担い、Zabbixサーバーへは特定の文字列やPriorityに合致したログのみを転送することで、
Zabbixサーバーへの負荷、
ストレージ消費量を最小限に抑えたログ監視の
システムを構築することが可能。

WebUIで簡単設定！機能概要図



Zabbix側の設定①

アイテム作成

アイテム

すべてのホスト / RTX830-01 有効 ZBX アイテム 2 トリガー 2 グラフ ディスカバリールール Webシナリオ

アイテム タグ 保存前処理

① * 名前 RTX830-01-リンク情報

タイプ Zabbixトラッパー

② * キー rtx830-01-link 選択

③ データ型 ログ

* ヒストリの保存期間 ヒストリを保存しない 保存期間 90d

ログの時間の形式

許可されたホスト

説明

アイテムの作成から、

①名前

②キー

③データ型

それぞれ適時設定します。

タイプは「Zabbixトラッパー」を選択。

※キーはEasyBlocks Syslogからログを送信する際に使用するため、判別しやすいキー名を設定してください。

Zabbix側の設定②

トリガー作成

トリガー

すべてのホスト / RTX830-01 有効 ZBX アイテム 2 トリガー 2 グラフ ディスカバリールール Webシナリオ

トリガー タグ 依存関係

① * 名前 RTX830-01-リンクアップダウン

イベント名 RTX830-01-リンクアップダウン

運用データ

深刻度 未分類 情報 警告 軽度の障害 重度の障害 致命的な障害

② * 障害の条件式 `find(/RTX830-01/rtx830-01-link,,,"link down")=1` 追加

条件式ビルダー

正常イベントの生成 条件式 復旧条件式 なし

③ * 復旧条件式 `find(/RTX830-01/rtx830-01-link,,,"link up")=1` 追加

条件式ビルダー

トリガーの作成から、

①名前

②障害の条件設定

③復旧条件式

それぞれ適時設定します。

※画面では監視対象機器「ヤマハ RTX830」、
「EasyBlocks Syslog」、「Zabbixサーバー」それぞれで
必要な設定を行っています。

障害・復旧の条件式は、実際の運用ポリシーによって
内容が異なりますので、今回の設定はあくまでも一例です。

EasyBlocks Syslog側の設定

Zabbixトラッパー連携

Zabbixトラッパー連携 (?)

Zabbixトラッパー連携する (?) ① ☒ はい ☐ いいえ

トラッパー通知条件 トラッパー条件追加

条件1

ホスト ② 192.168.200.1

Priority emerg alert crit err warn

メッセージ ③ link

Zabbix登録ホスト ④ RTX830-01

Zabbixアイテムキー ⑤ tx830-01-link

Zabbixトラッパー連携から、

①連携する

②ホスト(RTX830のIPアドレス)

③メッセージ

④Zabbix登録ホスト

(ホスト作成で設定したホスト名)

⑤Zabbixアイテムキー

(アイテム作成で設定したキー名)

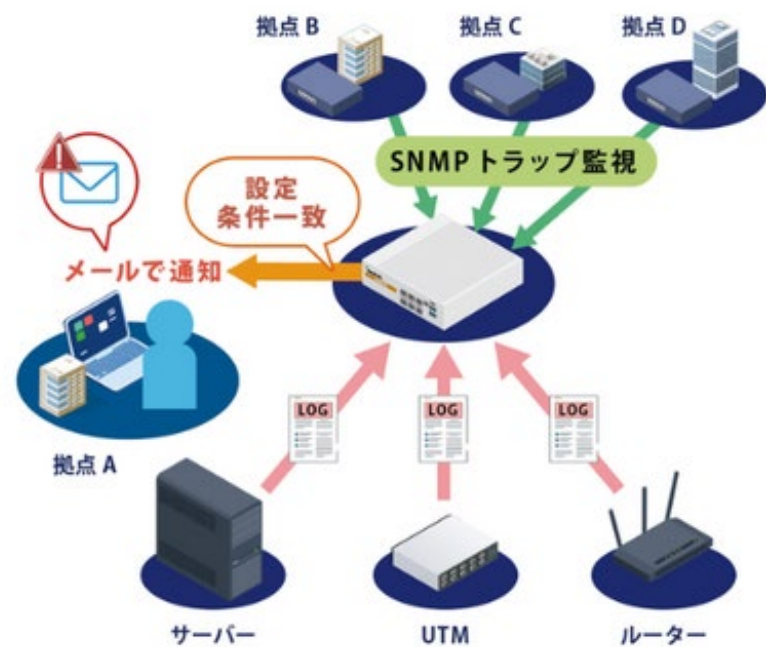
それぞれ設定していきます。

※画面では監視対象機器「ヤマハ RTX830」、「EasyBlocks Syslog」、「Zabbixサーバー」それぞれで必要な設定を行っています。

障害・復旧の条件式は、実際の運用ポリシーによって内容が異なりますので、今回の設定はあくまでも一例です。

EasyBlocks Smart log series 機能一覧

ログ保存・表示

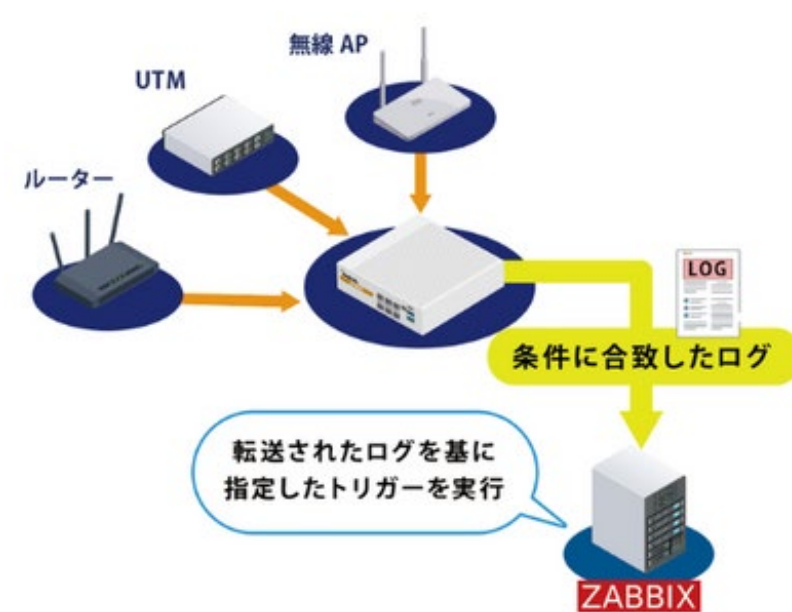


収集したログを本体内に保存し
Web UI上で閲覧
フィルタリングルール搭載

| ユースケース |

- 複数のサーバー、ネットワーク、UTMなどの機器ログを一元管理
- 複数機器のログやSNMPトラップ監視

Zabbixログ転送



受信した特定の文字列や
Priorityに合致したログのみを Zabbix
サーバーへ転送する

| ユースケース |

- Zabbix Agentが導入できない機器ログの監視
- 構築の手間をかけずに Zabbixでログ監視

レポート機能



ヤマハ製ルーター（RTXルーター、NVR
ルーター）の稼働状況をレポートニング
※Syslog Reporterのみ

| 対応機種の一覧 |

<https://www.plathome.co.jp/product/easyblocks/syslog-appliance/syslogreporter/>

サポートサービス



リモートで保守管理ができる
『AirManage 2』などの充実した
サポートサービス

| サポートサービス詳細 |

<https://www.plathome.co.jp/product/easyblocks/eb-support/>

【参考】EasyBlocks Smart log series ラインナップ一覧

項目	EasyBlocks Syslogシリーズ	EasyBlocks Syslog Reporter	EasyBlocks Syslog ProLine
ストレージ容量 ラインナップ	120GB / 240GB / 480GB 1TB / 2TB	120GB / 240GB / 480GB 1TB / 2TB	4TB / 15TB / 69TB / 115TB ～242TB
ログ保存・表示	○	○	○
Zabbix連携	○	○	○
レポート機能	-	○	-
ストレージRAID構成	-	-	○
リモートマネジメント サービス	○（サポートサービスに付随）		
参考販売価格※	¥220,000～	¥299,000～	¥2,980,000～
初回無償サポート年数	1年		3年
サポート年数	最長7年		
サポートサービス詳細	https://www.plathome.co.jp/product/easyblocks/eb-support/		

※価格はエンドユーザー様向けの直販価格です。Sler様、販売店様向け価格もございますので、詳細はお問い合わせください。

※無償サポート年数以降のサポートサービス延長は有償での提供となります。

サイジングしてみた

— EasyBlocks Smart log series —

Syslogサーバーのサイジング方法

01

貸出機を使用した
実環境でのサイジング

当社での推奨方法。実機を実環境に設置し、ログを収集したい装置でログ送信設定を行い、一定期間ログを蓄積します。

02

ネットワーク管理者や
Sler業者の選定

実環境のネットワーク管理者やSler業者がログ総量などある程度把握している場合は、当社の選定表からモデル選定が可能です。

03

ログの件数やバイト
数に基づく試算

以下の計算式を使用して、モデル選定することも可能です。
【ログ出力秒間件数 × ログ1件当たりのバイト数 × 1.3～1.5】

【参考】各サイジング方法の詳細

01

貸出機を使用した
実環境でのサイジング

【実践編】 自社環境でSyslogサーバーのサイジングしてみた

<https://blog.plathome.co.jp/syslog-server-sizing/>

02

ネットワーク管理者や
Sler業者の選定

最適な容量はどれ？ EasyBlocks Syslogのスマートな選定方法

<https://blog.plathome.co.jp/easyblocks-syslog-smartselection/>

03

ログの件数やバイト
数に基づく試算

どのストレージを選べばいい？ EasyBlocks Syslogシリーズ & Network Reporterの選定方法

<https://blog.plathome.co.jp/easyblocks-syslog-network-reporter-storage/>

まとめ

- ① 年々増加するサイバー攻撃に備えセキュリティ意識が高まり、
アプライアンス製品は「**Syslog**」が**トレンド**に。

お問い合わせ数・容量ともに増加傾向です。

- ② Zabbixサーバーに負荷なく、複数のログを収集・監視するには
「**EasyBlocks Syslogシリーズ**」！

新機能の「**Zabbixサーバへのデータ転送機能**」を
是非ご検討下さい。

- ③ 実際にSyslogサーバを導入する際は、サイジングが必要！



THANK YOU

最後までご清聴いただき、誠にありがとうございます。
アンケートのご協力をお願いいたします。

【参考】

- EasyBlocks Smart log series

<https://www.plathome.co.jp/product/easyblocks/syslog-appliance/syslog-top/>

- ふらっとブログ

<https://blog.plathome.co.jp/>