Zabbix × Syslogサーバーでもう見落とさない！

ログ監視の方法を徹底解説

2024年11月22日

ぷらっとホーム株式会社 清水

Plat'Home

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　事例からみる、ログ監視って必要？

05　Zabbix連携機能について

06　EasyBlocks Smart log seriesとは

07　アップデート情報

Plat'Home

自己紹介

ぷらっとホーム株式会社

清水　教彦

所属部署

ネットワーク事業部　パートナー営業課

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 TECHNOLOGY to serve you.

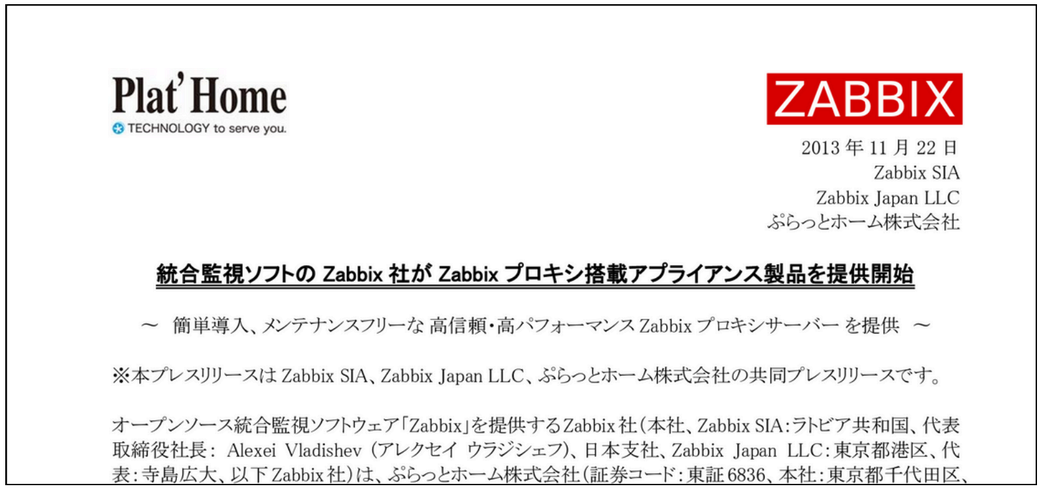
ぷらっとホーム株式会社

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10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

Zabbix Japanとの歴史①

【2013/11/22～】
ぷらっとホーム製のハードウェアを採用した
「Zabbix プロキシ搭載アプライアンス製品」の提供を開始



Plat'Home
TECHNOLOGY to serve you.

ZABBIX

2013 年 11 月 22 日
Zabbix SIA
Zabbix Japan LLC
ぷらっとホーム株式会社

統合監視ソフトの Zabbix 社が Zabbix プロキシ搭載アプライアンス製品を提供開始

～ 簡単導入、メンテナンスフリーな 高信頼・高パフォーマンス Zabbix プロキシサーバー を提供 ～

※本プレスリリースは Zabbix SIA、Zabbix Japan LLC、ぷらっとホーム株式会社の共同プレスリリースです。

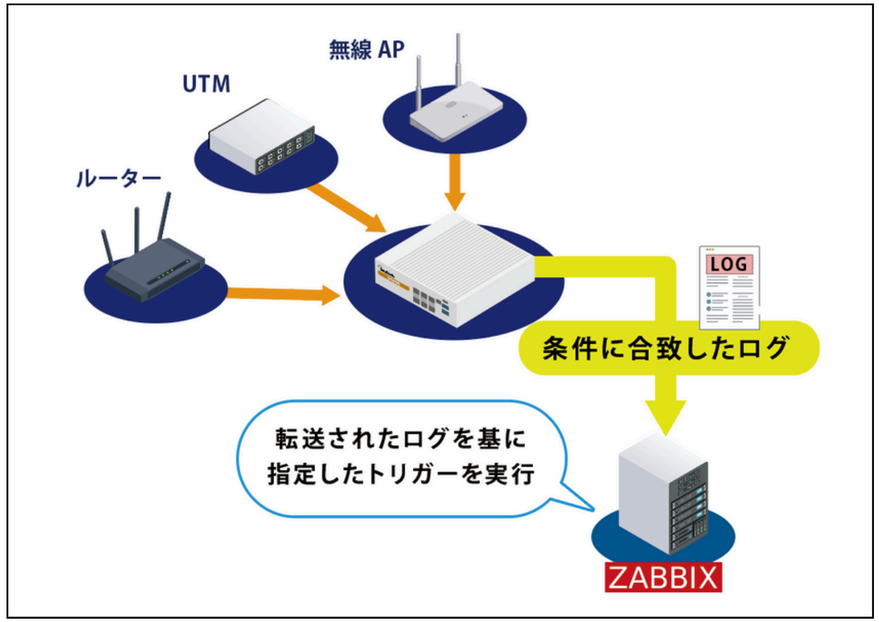
オープンソース統合監視ソフトウェア「Zabbix」を提供するZabbix 社（本社、Zabbix SIA：ラトビア共和国、代表取締役社長： Alexei Vladishev （アレクセイ ウラジシェフ）、日本支社、Zabbix Japan LLC：東京都港区、代表：寺島広大、以下Zabbix 社）は、ぷらっとホーム株式会社（証券コード：東証 6836、本社：東京都千代田区、

https://www.plathome.co.jp/about/press/pdf/Zabbix_Appliance_ZP-1200-20131122_fix.pdf

Zabbix Japanとの歴史②

【2024/5/21～】
ぷらっとホームSyslogサーバー機能を搭載した
アプライアンス製品「EasyBlocks Smart log series」にて、「Zabbixサーバーへのログ転送機能」の提供を開始

＜機能概要図＞



https://www.plathome.co.jp/press-release/20240425-zabbix-server-easyblocks/

Plat'Home

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？

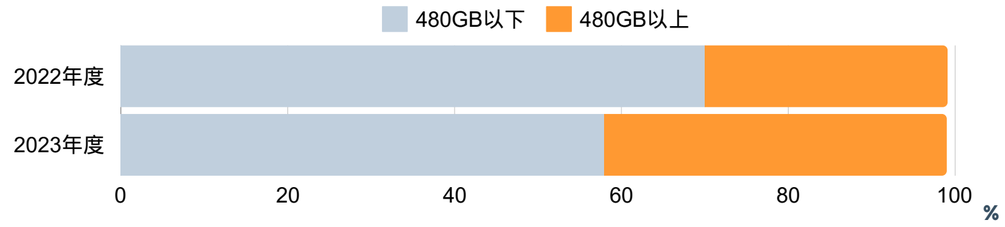
※2022年度と2023年度の比較

『Syslogアプライアンス』

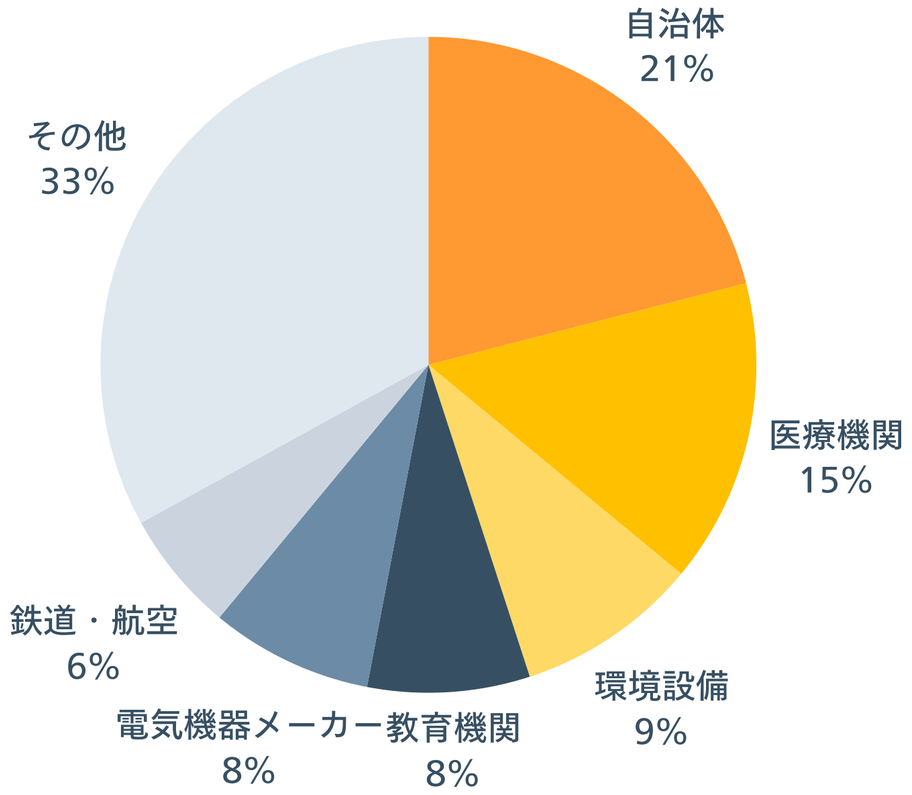
問合せ数　**約 2 倍に増加**

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**



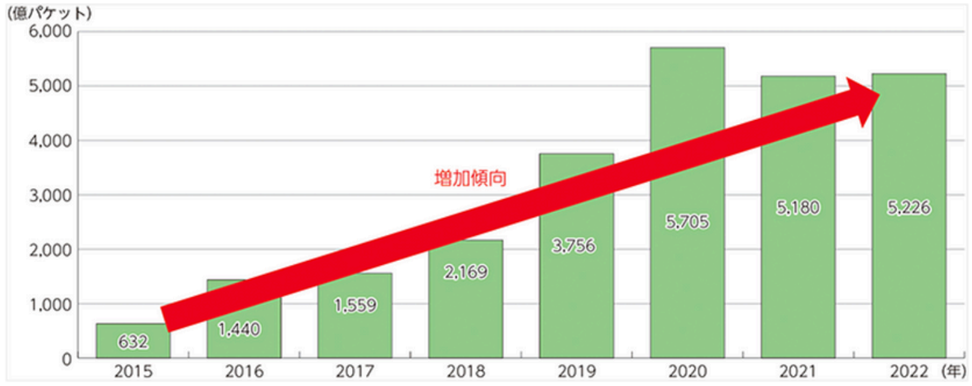
業種別比率



問い合わせ数増加の背景

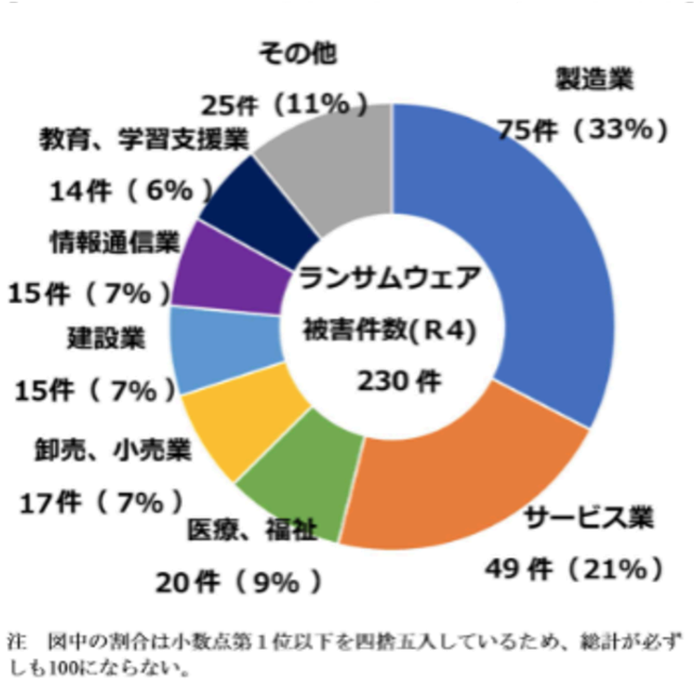
年々増加するサイバー攻撃対策

- 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

サイバー攻撃の事例

２０２１年１０月
徳島県　つるぎ町立半田病院

被害：電子カルテが使用できず、２ヶ月間にわたる新規患者の受け入れ停止など

侵入経路：UTMを通じて院内ネットワークへ侵入

引用元：徳島新聞デジタル　https://www.topics.or.jp/articles/-/612733

２０２２年１０月
大阪府　大阪急性期・総合医療センター

被害：電子カルテシステムに障害が起き、２ヶ月間にわたる緊急以外の手術や
　　外来診療の停止など

侵入経路：VPNルーターを通じて院内ネットワークへ侵入

引用元：朝日新聞デジタル　https://www.asahi.com/articles/ASQB075DWQB0OXIE022.html

2つの事件の共通点

2つの事件の侵入経路

半田病院

UTMを通じて院内ネットワークへ侵入

大阪総合医療センター

VPNルーターを通じて院内ネットワークへ侵入

共通するシステムの特徴

01 詳細なネットワーク構成図がない

02 セグメントを分けていない

03 ログの管理ができていない

ログ管理＝UTM、ルーター、FWなどを指している。
どちらも電子カルテではなく、ネットワーク経由でサイバー攻撃を受けていた

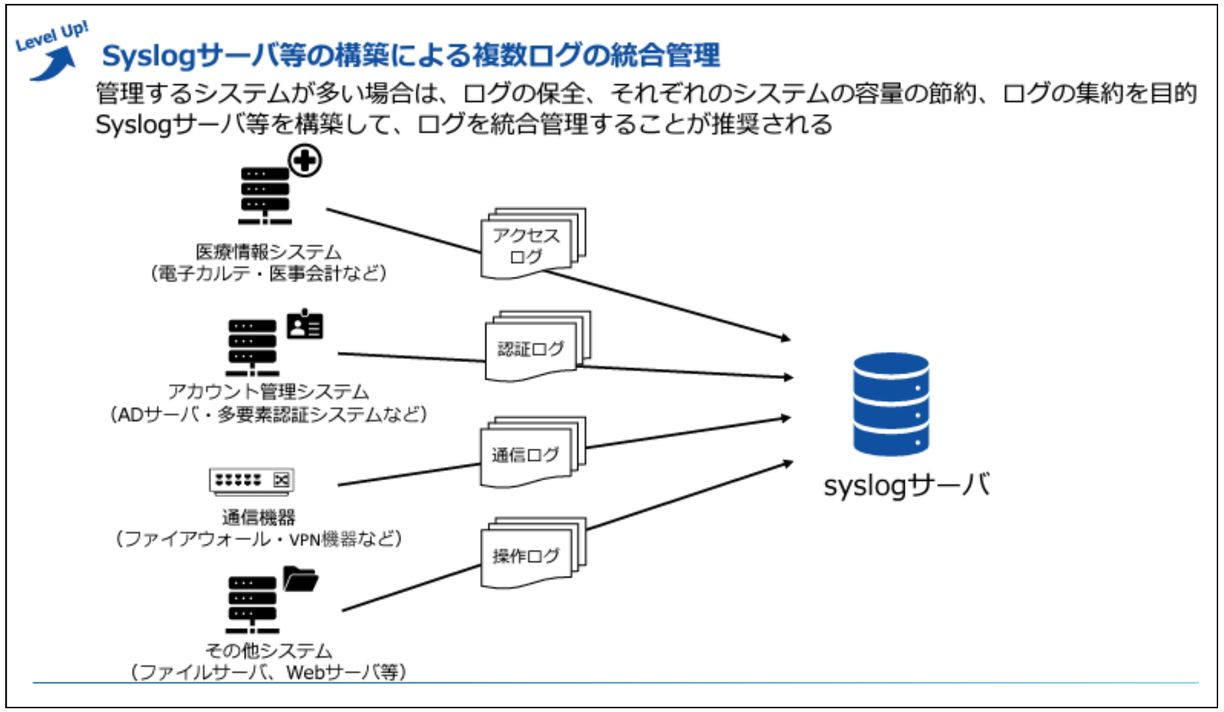
引用元：日経クロステック「ランサムウエア被害に遭うシステムの3つの「ない」、攻撃を前提とした対策を急げ」　https://xtech.nikkei.com/atcl/nxt/column/18/02362/021500004/

【参考】ログ管理の事例ー徳島県の例

サイバー攻撃の増加を受け、
徳島県では独自に医療機関向けのサイバーセキュリティ対策マニュアルを発行。

医療情報システム・認証ログ・
通信ログ・ファイルサーバーのログを
Syslogサーバーで一括管理することを推奨

セキュリティ対策の観点から
ログ保存の需要性が浸透



引用元：徳島県「徳島県医療機関向けサイバーセキュリティ対策マニュアル及びチェックリストについて」
https://www.pref.tokushima.lg.jp/med/categoryMedical/sonota/kikan/7234660/

【参考】適切なログの保管期間は？

事例①　日本セキュリティ監査協会

インシデントの内容の全体像を正しく分析するためにログは長期間保存しておく。
保存期間は1年以上とすることが望ましい。

引用元：日本セキュリティ監査協会サイバーセキュリティ対策マネジメントガイドライン2.0
https://www.jasa.jp/wp-content/uploads/%E3%82%B5%E3%82%A4%E3%83%90%E3%83%BC%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E5%AF%BE%E7%AD%96%E3%83%9E%E3%83%8D%E3%82%B8%E3%83%A1%E3%83%B3%E3%83%88%E3%82%AC%E3%82%A4%E3%83%89%E3%83%A9%E3%82%A4%E3%83%B3

事例②　文部科学省

校務系システム及び校務外部接続系システムのログについては6か月以上保存することが望ましい。

引用元：文部科学省　教育情報セキュリティポリシーに関するガイドライン（令和6年1月）
https://www.mext.go.jp/content/20240202-mxt_jogai01-100003157_1.pdf

【参考】ログ保存の導入手段

機器本体への保存

UTMやルーター、アクセスポイントなどを活用する例。
初期導入はラクだが、ストレージが小さいので長期保存には向かず、汎用性はほぼない。
ログの長期保存を求めない方向け

機器ベンダーのログ保存サービス

クラウドサービスを活用する例。導入の手間がなく運用も手軽でコストもさほど高くないが、他社機器のログ保存に対応していない可能性が高く、汎用性が低い。
特定の機器のみログ保存をしたい方向け

自作ログサーバー

自分で作成するので、要件に合わせて自由にカスタマイズができる。導入や運用コストは作った人に依存してしまう可能性がある。
複数機器のログを長期で保存したい方、さらに拡張性を求める方向け

ログアプライアンス

汎用性は自作ログサーバーに劣るが、導入や運用コストは比較的低くすむことが多い。トラブル時はメーカーに対応を丸投げできる。
手間暇かけずに複数機器のログを長期で保存したい方向け

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

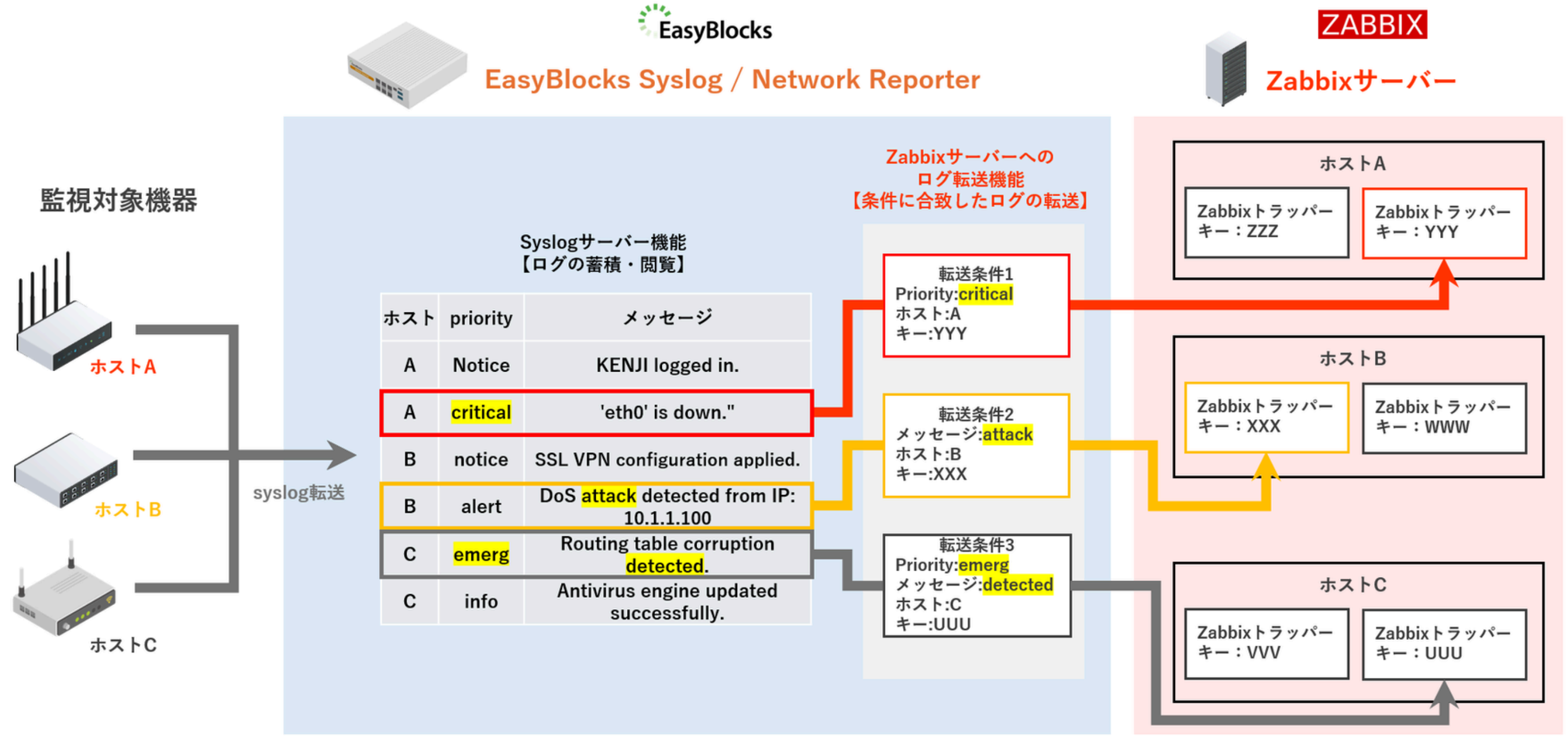
Syslogアプライアンスで解決！

**『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**

Plat'Home

WebUIで簡単設定！機能概要図



Zabbix側の設定

アイテム作成

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

トリガー作成

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

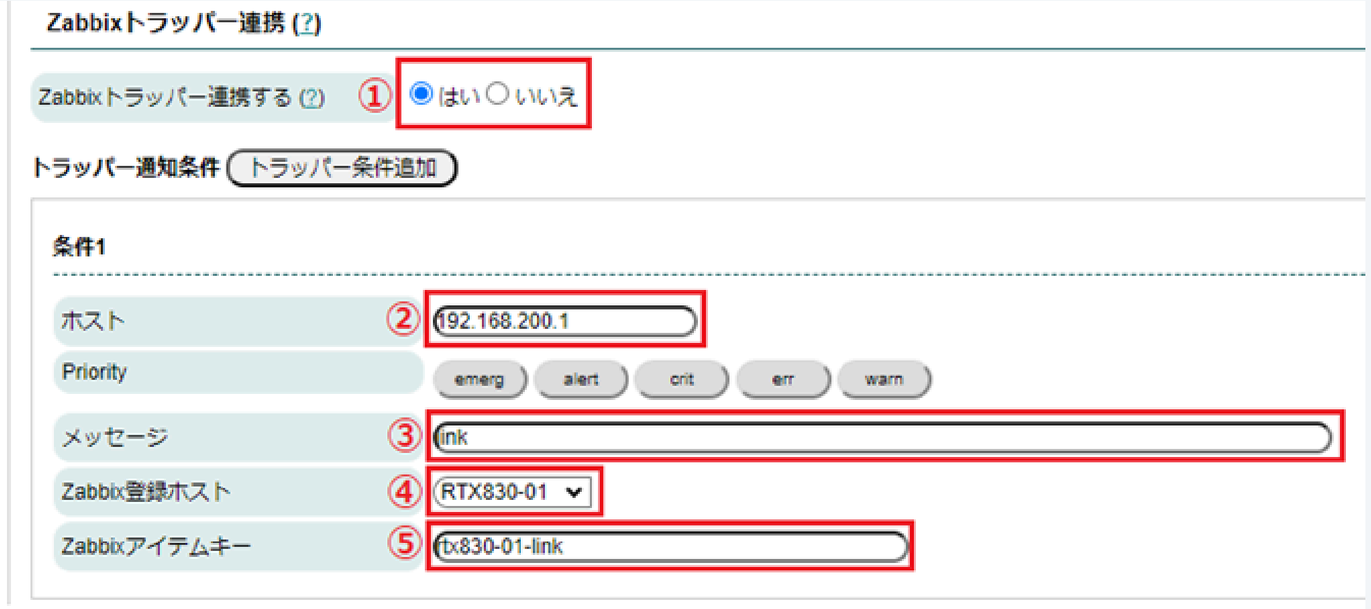
それぞれ適時設定します。

※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

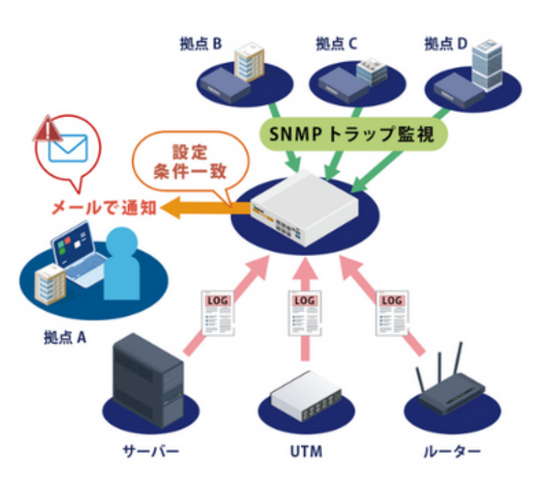


Zabbixトラッパー連携から、
①連携する
②ホスト(RTX830のIPアドレス)
③メッセージ
④Zabbix登録ホスト
(ホスト作成で設定したホスト名)
⑤Zabbixアイテムキー
(アイテム作成で設定したキー名)
それぞれ設定していきます。

※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

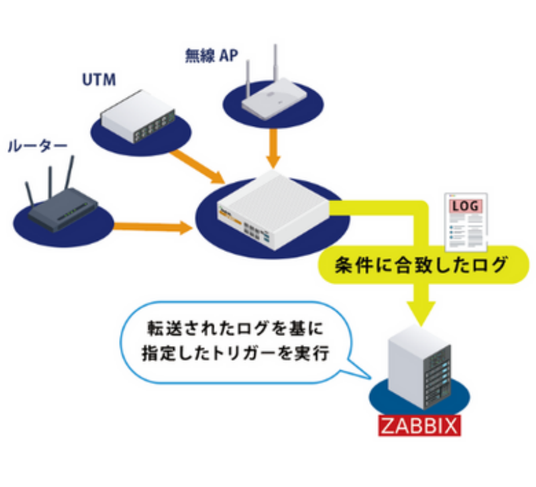


収集したログを本体内に保存し
WebUI上で閲覧
フィルタリングルール搭載

| 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

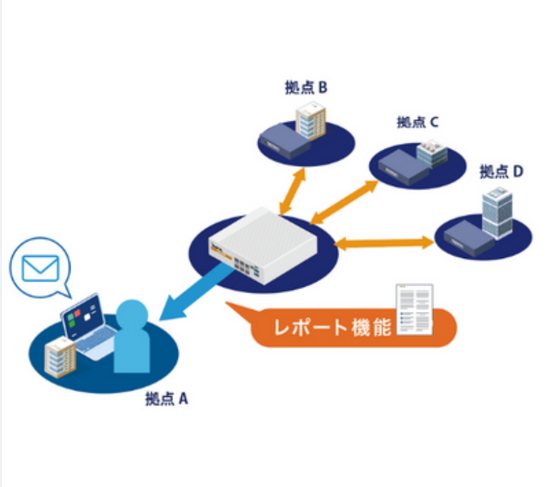


受信した特定の文字列や
Priorityに合致したログのみを Zabbix
サーバーへ転送する

| 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）やFortinet製UTMの
稼働状況をレポーティング
※Network Reporterのみ

| 対応機種の一覧 |

https://www.plathome.co.jp/product/easyblocks/networkreporter/

サポートサービス

リモートで保守管理ができる
『AirManage2』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 Network 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～最大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※	¥182,000～	¥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。SIer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。

Plat'Home

アプデ情報

— EasyBlocks Smart log series —

アップデート情報

2024年9月のアップデート

①統計情報送信

ホスト毎のプライオリティ別ログ件数
(EBログ統計グラフで使用している値)

②重複制御

同一メッセージを任意の秒間、制御する

③送信時プレフィックス

任意のプレフィックスを設定可能

④ブラックリスト(正規表現)

フィルタリング機能

⑤IETF-Syslog形式

IETF-Syslog形式の受信・Syslog転送に対応

⑥タイムゾーンを考慮

タイムゾーンを含んだSyslog受信時に
当機のタイムゾーンに変換して保管

アップデート情報

2024年12月のアップデート

⑦バックアップ先の拡充

「バックアップ送信」機能・
「CSVログ送信」機能の送信先に、
AWS S3/Azure Blobを追加

⑧ボンディング機能

LANポートの冗長化機能を追加

アップデート情報参考記事

【24年上半期】EasyBlocksシリーズアプデ情報

https://blog.plathome.co.jp/easyblocks_update2024_1/

【アプデ告知】EasyBlocks Syslogシリーズのバックアップ先拡充をチラ見せ

https://blog.plathome.co.jp/update-ebsyslog-backup/

THANK YOU

Plat'Home

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/

- ぷらっとブログ

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

Plat' Home
TECHNOLOGY to serve you.

〒102-0073　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
03-5213-4370
sales@plathome.co.jp