syslog-ng Store Box

製品ガイド

Rev 3.1

平成30年5月28日

ジュピターテクノロジー

変更履歴

版	発行日	変更内容
第3.0 版	2018/3/1	syslog-ng Store Box 5 LTS
第3.1 版	2018/5/28	記載内容を修正

製品概要

syslog-ng Store Box（SSB）は、　ハンガリーのBalabit社が開発した、高信頼性と高パフォーマンス性能を併せ持つシスログ管理アプライアンスです。

搭載された検索インターフェースやカスタマイズ可能なレポート・統計エンジンにより、簡単なログの調査や監査手段も提供します。

また取得するログを極秘データと位置づけ、送受信経路や保存データを暗号化し、ユーザ毎のアクセスコントロール機能と合わせる事で、不正アクセスや改竄・漏洩を防止し、コンプライアンスに対応した最高水準の機密保護基準を満たします。

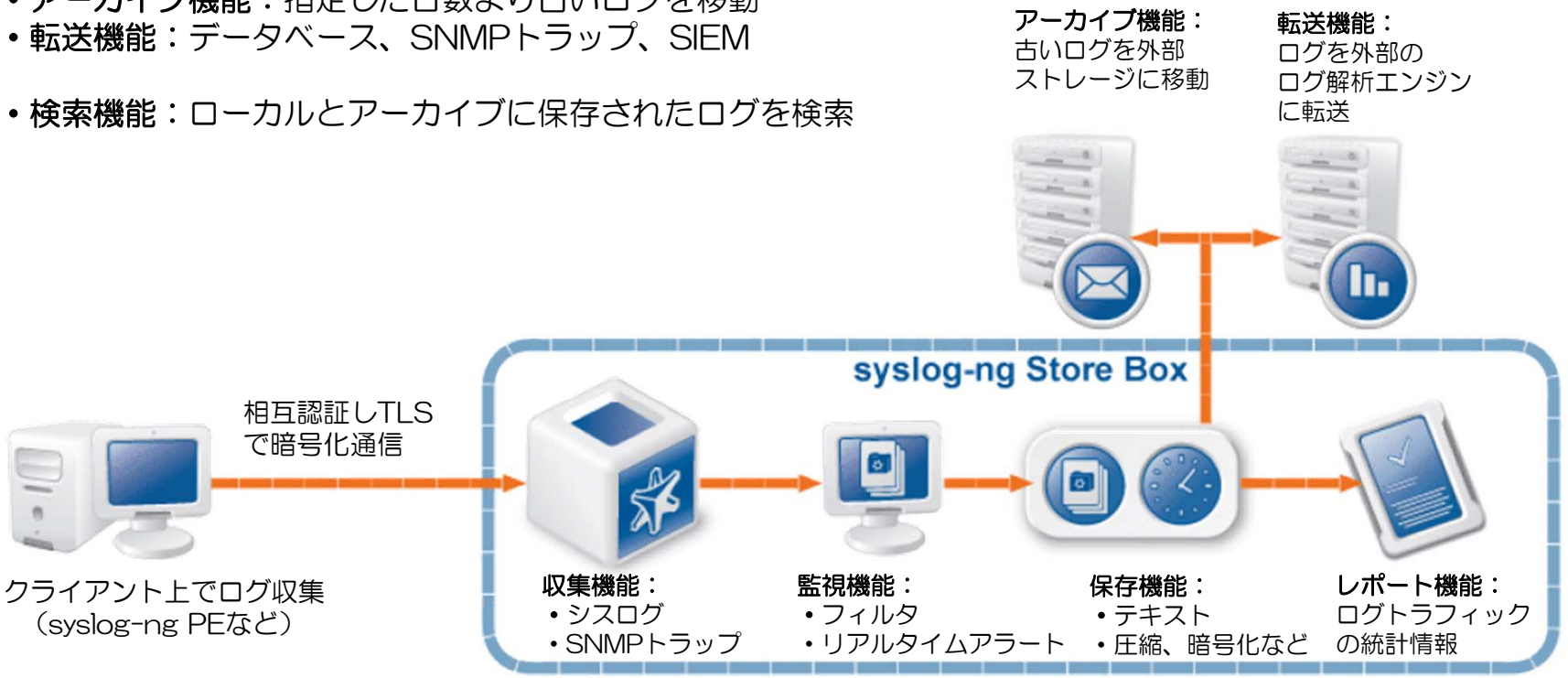
超高速･多機能シスログサーバとして、また極秘データを取り扱うセキュアなログサーバとして、ログインフラストラクチャーの中核に最適な製品です。

ログ管理の基本機能

SSBの基本機能は以下の通りです。

- **収集機能**：シスログ、SNMPトラップ
- **監視機能**：フィルタ（絞込みと振分け）、アラート
- **保存機能**：テキスト、バイナリ（圧縮、暗号化、タイムスタンプ）
- **レポート機能**：ログの送信元数やログ量などの統計情報
- **アーカイブ機能**：指定した日数より古いログを移動
- **転送機能**：データベース、SNMPトラップ、SIEM

- **検索機能**：ローカルとアーカイブに保存されたログを検索



特徴 超高速なログ処理性能

syslog-ng STORE BOX

モデル別のログ処理性能

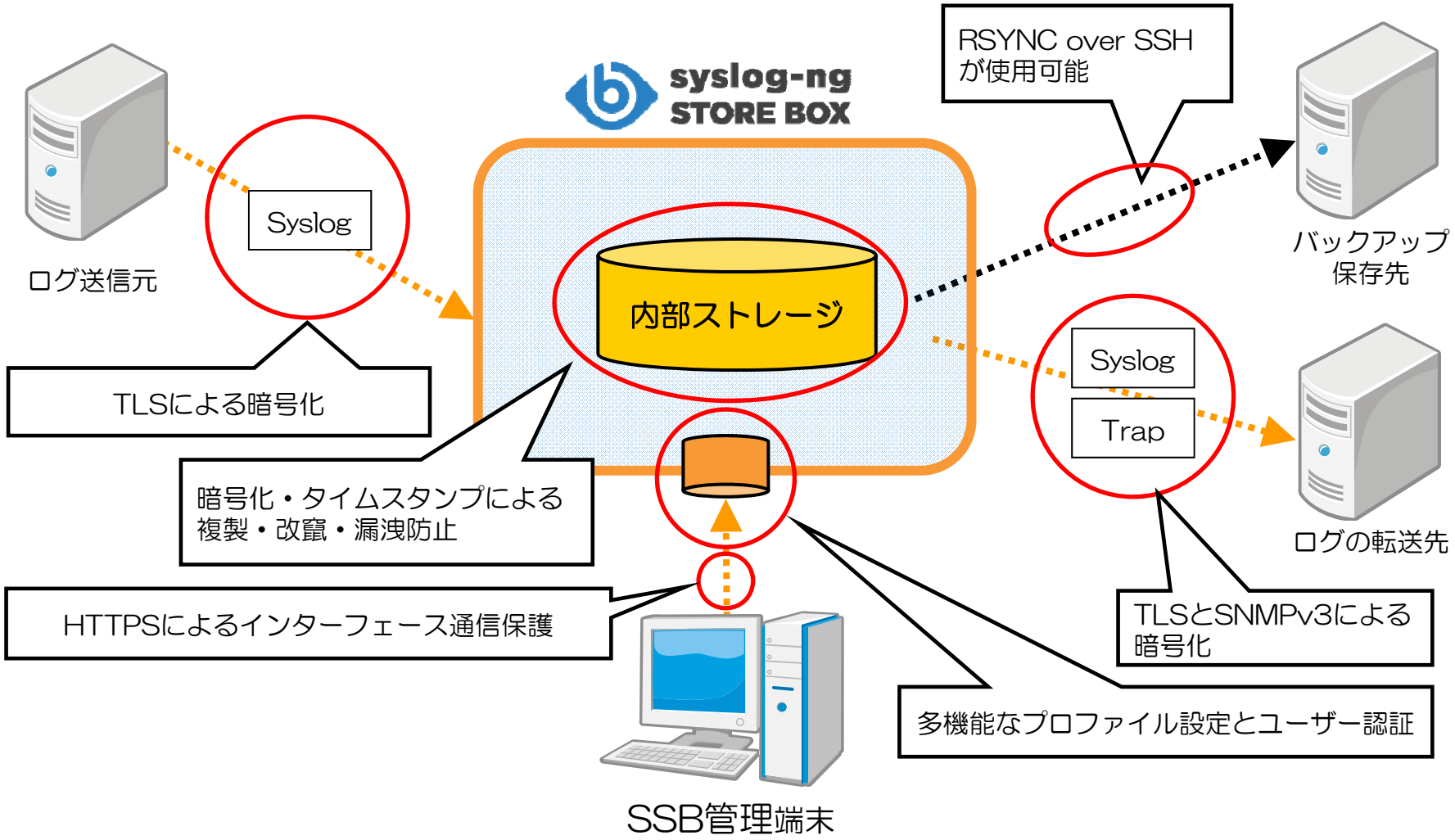
モデル	EPS (Event Per Second)
T1 or H2	～ 10,000 EPS
T4 or H4	～ 40,000 EPS
T10 or H10	～ 70,000 EPS

注意：

- プロトコル：TCP　平均メッセージ長：450バイト
- 実測値は、ハードウェア/仮想マシンのリソース、運用設定、環境、ログサイズ等によって、異なりますのでご注意ください。

特徴 機密保護機構を装備

SSBは、下図の部分で機密保護が可能です。



特徴 オールインワンアプライアンス

SSBには下記のソフトウェアが既にインストール済みです。起動してすぐにご利用できます。

- Linuxベースの独自OS
- ログサーバー（syslog-ng）
- 管理GUI用のWebサーバ
- ログ閲覧・検索
- ログデータのバックアップ・アーカイブ
- HA（ハイアベイラビリティ）注意：ハードウェアアプライアンスのみ有効

※これらのソフトウェアはファームウェアとして提供されます。セキュリティ対応やバグ修正時は、このファームウェアが更新されて提供され、管理GUIから更新できます。

運用オペレーションには、Webブラウザが動くお手持ちのPC等をご利用いただけます。

また、収集したシスログのアーカイブやシステムのバックアップ用としてネットワークストレージを使用することも可能です。

製品ラインアップ

syslog-ng STORE BOX

SSBは、ハードウェア アプライアンスとバーチャル アプライアンス、BlueVaultアプライアンスとして提供します。

	ハードウェア アプライアンス	バーチャル アプライアンス	BlueVault アプライアンス　※1
ログホスト数	100 ～ 無制限	25 ～ 無制限	25 ～ 無制限
サーバ	T1 / T4 / T10	仮想システム　※2	H2/H2H/H4/H10 + 仮想
HA化	可能	不可　※3	不可
ログ受信性能 メッセージ数/秒 (TCP接続)	T1： 1万以下 T4： 4万以下 T10： 7万以下	サーバの性能に依存	H2/H2H：1万以下 H4：4万以下 H10：7万以下
内蔵ディスク	T1： 1TB T4： 4TB T10： 10TB	仮想マシンのディスク割り当てサイズに依存	H2/H2H： 2TB H4： 4TB H10： 10TB
ハードウェア保守	・センドバック ・先出しセンドバック	N/A	・ハードウェアベンダーによるオンサイト保守　※4

※1　国内で調達したサーバにVMwareESXiをインストールし、SSBはその上の仮想マシンとして動作します。
HA構成はサポートしていません。その他の機能は、ハードウェアアプライアンスと同じです。
※2　VMware ESX 4.0以降、ESXi 4.0以降、Microsoft Hyper-V、Microsoft Azure、Amazon Web Services
※3　仮想システムのHA/フォルトトレランスの利用を推奨
※4　HPE社がハードウェアのみを修理。出荷時への復旧やログデータのリストアなどはお客様に対応頂きます。
BlueVaultのサポート契約可能期間は5年迄です。 弊社の受付対応は、平日9：00－17：00

製品モデル仕様

syslog-ng STORE BOX

各製品モデルの仕様は以下です。

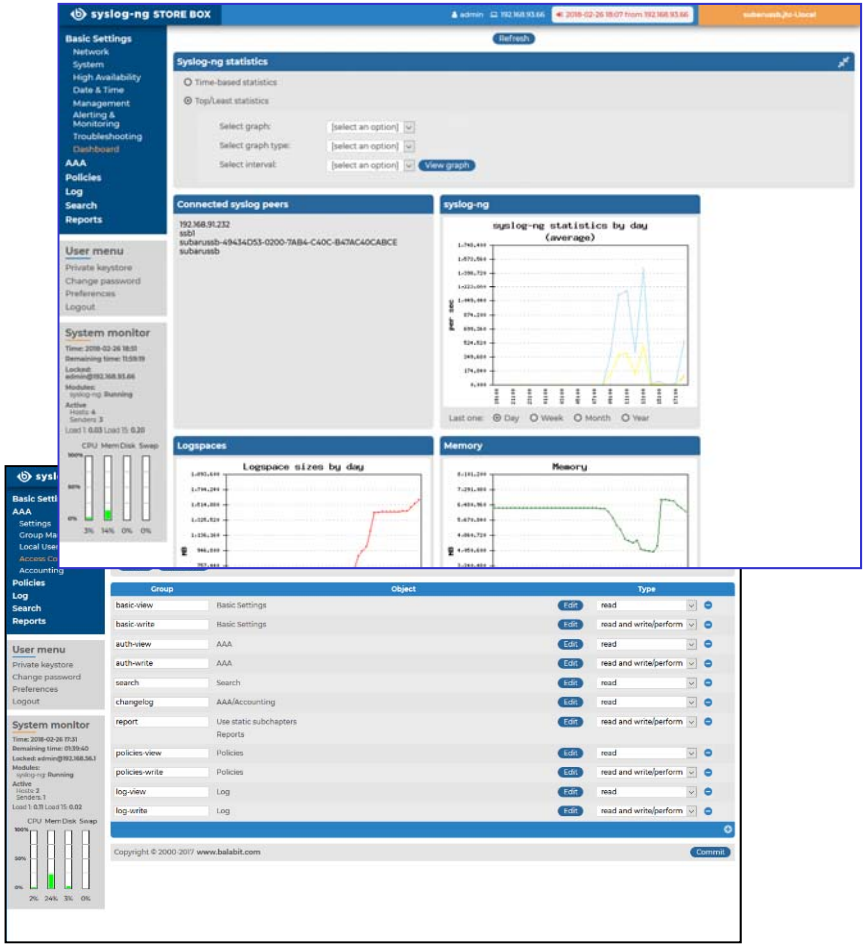
※製品仕様は、予告なく変更される可能性があります。

シリーズ	モデル	形態	CPU	メモリ	HDD	RAID	NIC
ハードウェア（IPMIあり） 	T1	物理 1U	1X4 core INTEL Xeon X3430 @2.40GHz	8GB (2 x 4 GB)	1TB (2 x 1TB)	Software	4 x 1Gbps
	T4 （冗長化電源）	物理 1U	1X4 core INTEL Xeon E3-1275V2 @3.50GHz	8GB (2 x 4 GB)	4TB (4 x 2TB)	RAID10	4 x 1Gbps
	T10 （冗長化電源）	物理 2U	2x6 core INTEL 2x Xeon E5-2630V2 @ 2.6GHz	32GB (8 x 4 GB)	10TB (13 x 1TB)	RAID50	4 x 1Gbps 2 x 10Gbps （オプション※）
バーチャル	VA	仮想マシン	VMware ESX 4.0以降、ESXi 4.0以降、Microsoft Hyper-V、Microsoft Azure、Amazon Web Services				
BlueVault （VMware ESXi上で動作） （iLoあり） 	H2 /H2H（冗長化電源）	物理 1U	1X4 core INTEL Xeon E3-1220V5 @3.0GHz	16GB	2T(2 x 2TB) /2T(4 x 1TB)	RAID1 /RAID10	2 x 1Gbps
	H4 （冗長化電源）		1X4 core INTEL Xeon E5-2623V4 @2.6Ghz		4T (4 x 2TB)	RAID10	2 x 1Gbps
	H10 （冗長化電源）	物理 2U	2X8 core INTEL Xeon E5-2620V4 @2.1Ghz	48GB	10T (12 x 1TB)	RAID50	2 x 1Gbps

※10Gbitトランシーバー（10GB SFP+ SR）のオプション購入が必要です。

Web インターフェース

SSBでは、通常のオペレーションは、WebベースのGUI
インターフェースを通じて操作を行います。



サポートしているログ

SSBは、下記のログを受信、送信できます。

シスログ（受信、送信）
- BSD-Syslogプロトコル（RFC 3164）
- IETF-Syslogプロトコル（RFC 5424-5428）

SNMPトラップ
- SNMP v2c（受信、送信）、v3（送信）

データベースのテーブルデータ（受信、送信）
- ORACLE データベース
- Microsoft SQL Serverデータベース
- MySQL データベース
- PostgreSQL データベース

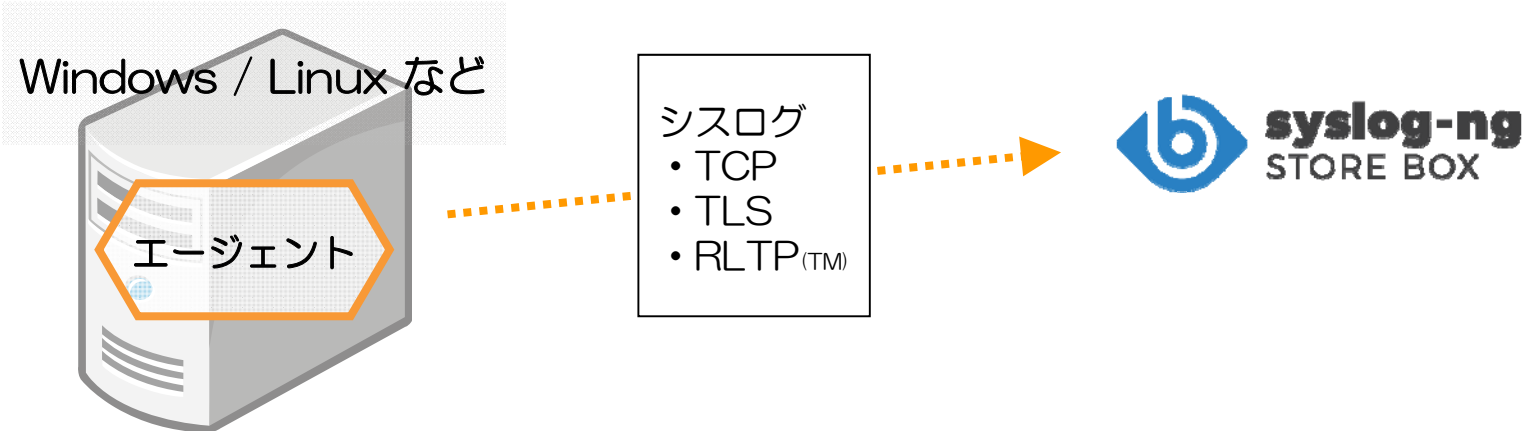
ログ収集エージェント

クライアントにエージェントを利用する事で以下が可能となります。

- Windowsのイベントログ やLinuxのログをシスログに変換して送信
- アプリケーションの出力するテキストログをシスログに変換して送信
- シスログを暗号化してSSBへ送信

注意事項：

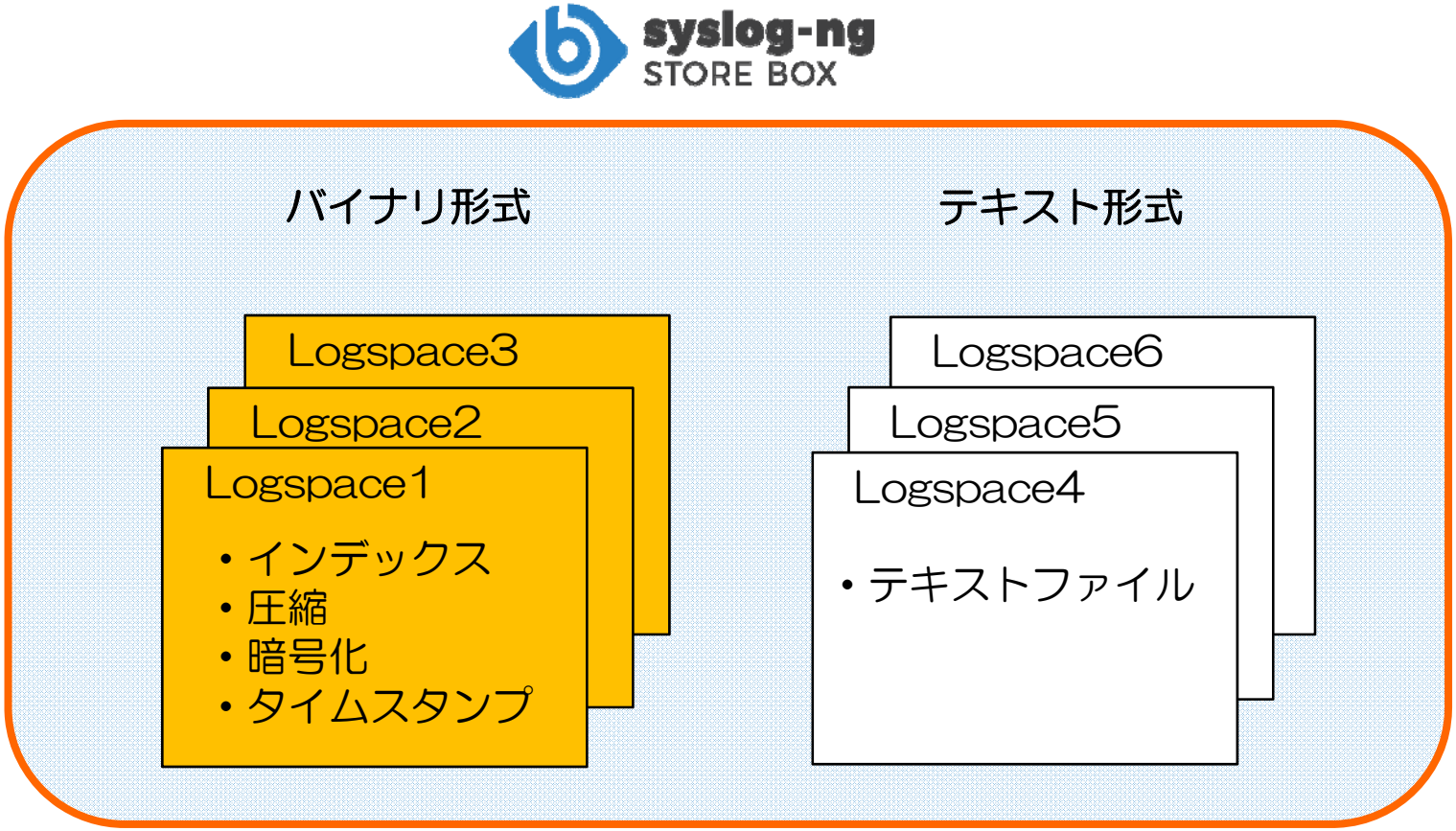
＊シスログを送信できるネットワーク機器、サーバーの場合、エージェントを
インストールする必要はありません。
＊ SSB ライセンスでsyslog-ng Premium Edition アプリケーション
（syslog-ng Agent for Windows 含む）をSSB用のログ収集エージェント
として様々なプラットフォームにインストールして利用できます。



ログの保存

受信したログはログスペースに保存されます。保存形式は2種類あります。

- バイナリ形式：圧縮や暗号化などで効率的に安全に保存（SSBで検索可能）
- テキスト形式：ログ解析などの外部アプリとの連携に利用可能（SSBで検索は不可）



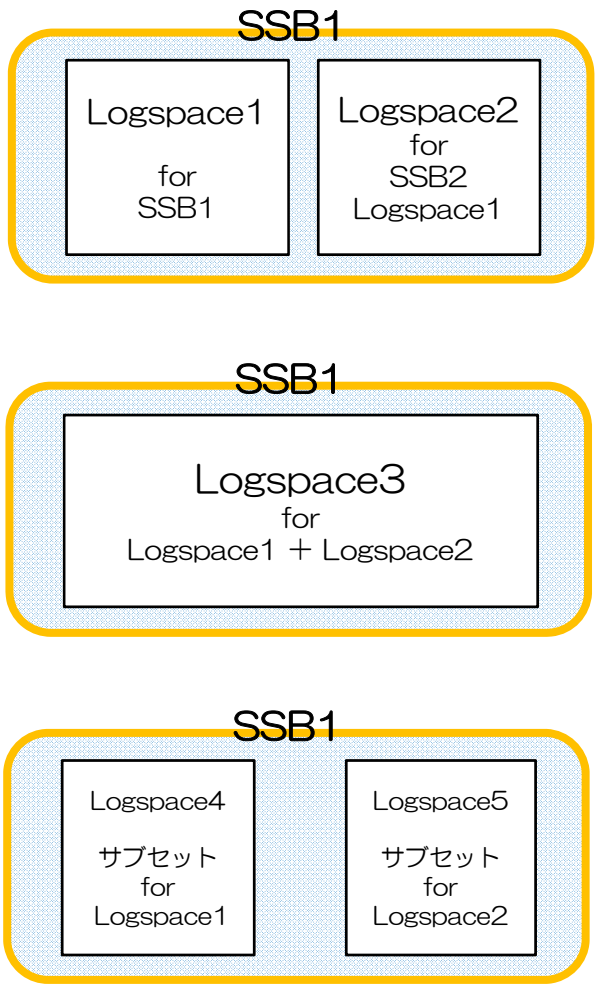
ログスペースの定義

仮想的なログスペースを定義できます。

- リモート ログスペース
  （Remote Logspace）
  リモートを含む他のSSBのログスペース（フィルターされたログ含む）を定義できます。一度設定すると、ローカルのログと同様に閲覧・検索できます。

- マルチプル ログスペース（ログスペースの統合）
  （Multiple Logspace）
  複数のSSBのログスペース（リモートも含む）を統合して１つのログスペースとして定義できます。これにより、複数のログスペースをまとめて閲覧・検索できます。

- フィルター ログスペース（ログスペースのサブセット）
  （Filtered Logspace）
  ログスペース（リモートも含む）をフィルタで絞り込みサブセットを作成できます。このログにアクセスできるユーザグループを設定することにより、より細かいアクセス制御ができるようになります。

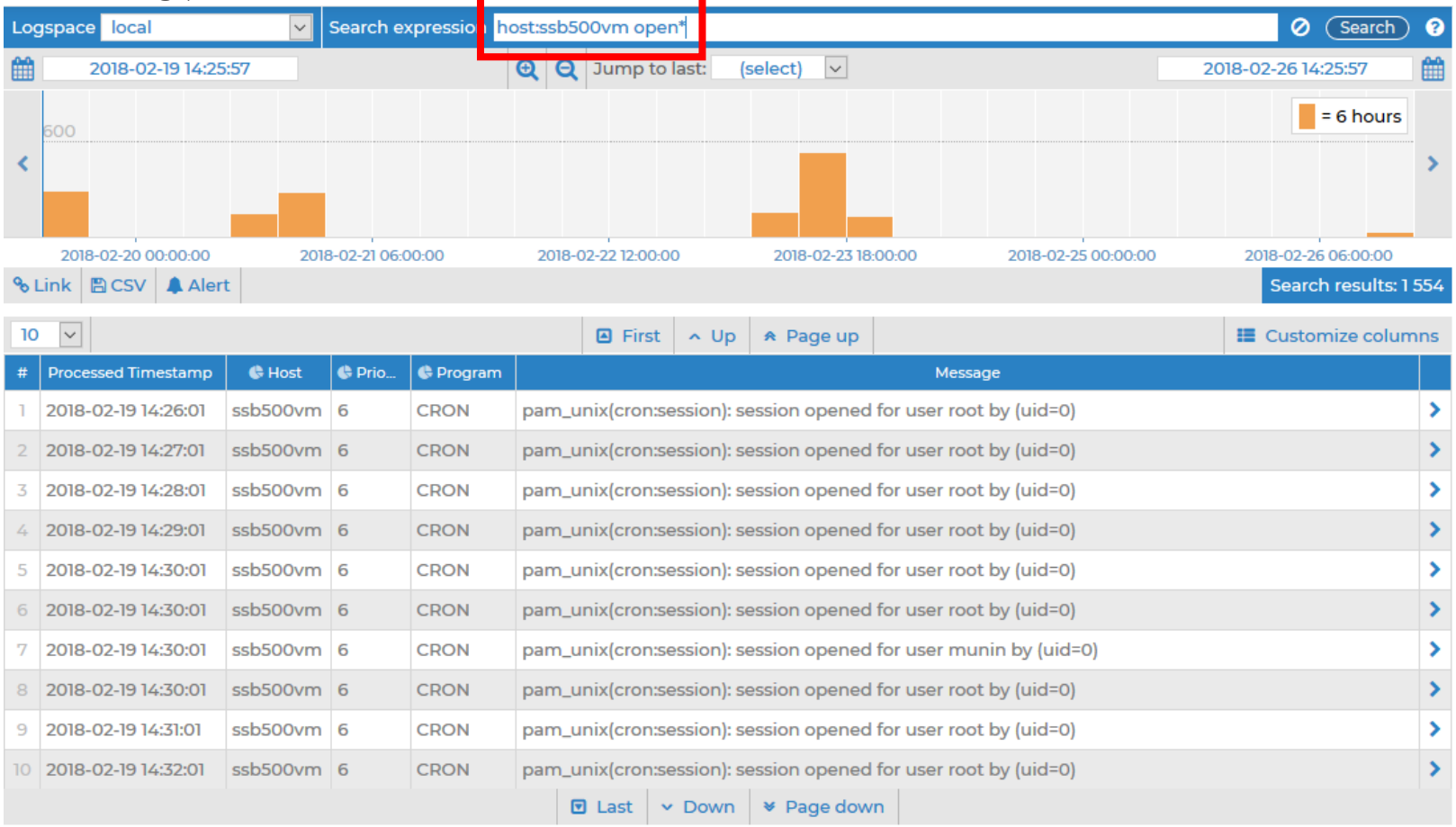


ログの検索

SSBは、ログの検索機能を搭載しています。ワイルドカードなど強力な検索式を駆使して、高速で柔軟な検索が可能です。

ホスト名がssb500vmで、かつ、メッセージにopenからはじまる文字列を含むシスログを検索した例。

Search -> Logspaces

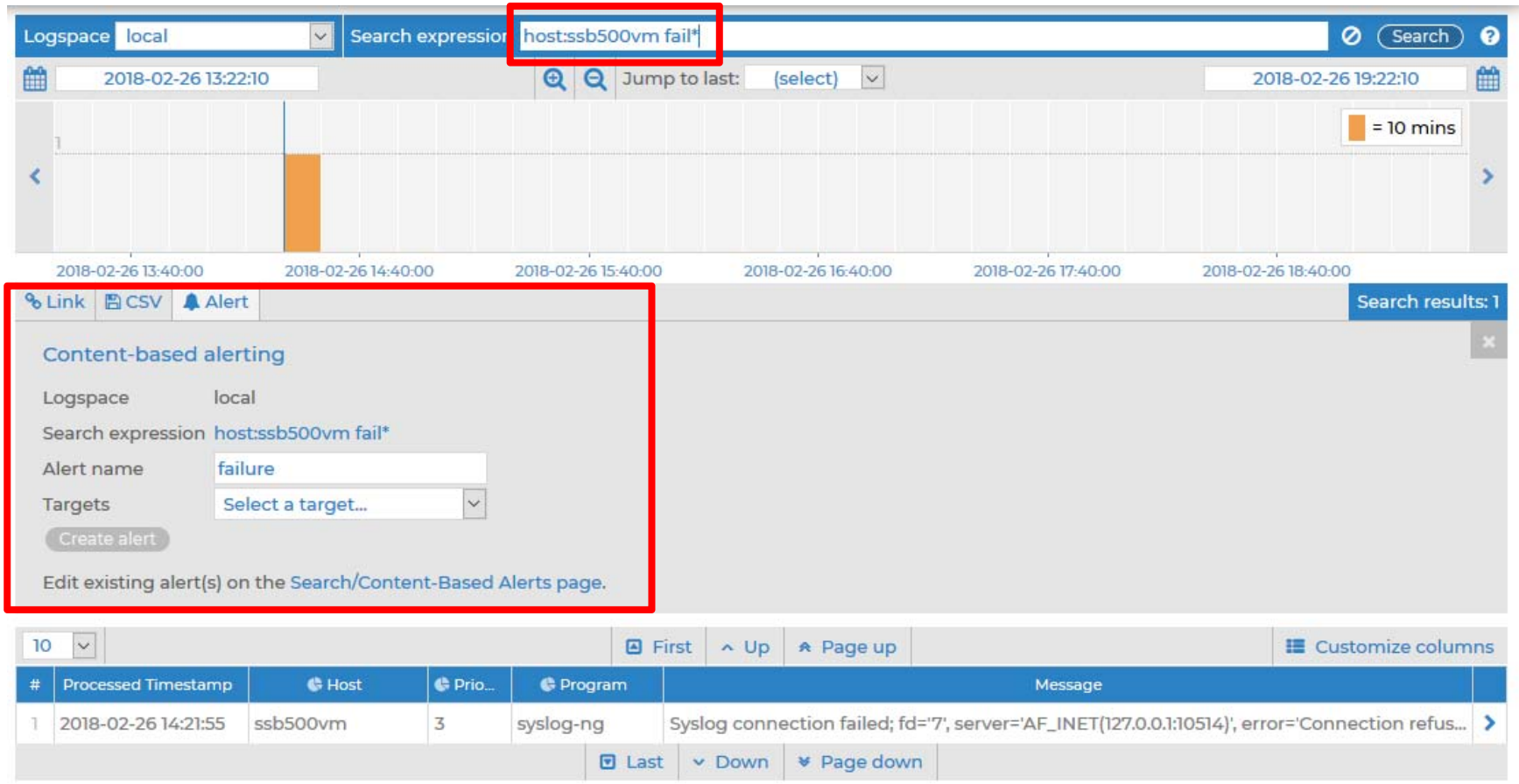


#	Processed Timestamp	Host	Prio...	Program	Message
1	2018-02-19 14:26:01	ssb500vm	6	CRON	pam_unix(cron:session): session opened for user root by (uid=0)
2	2018-02-19 14:27:01	ssb500vm	6	CRON	pam_unix(cron:session): session opened for user root by (uid=0)
3	2018-02-19 14:28:01	ssb500vm	6	CRON	pam_unix(cron:session): session opened for user root by (uid=0)
4	2018-02-19 14:29:01	ssb500vm	6	CRON	pam_unix(cron:session): session opened for user root by (uid=0)
5	2018-02-19 14:30:01	ssb500vm	6	CRON	pam_unix(cron:session): session opened for user root by (uid=0)
6	2018-02-19 14:30:01	ssb500vm	6	CRON	pam_unix(cron:session): session opened for user root by (uid=0)
7	2018-02-19 14:30:01	ssb500vm	6	CRON	pam_unix(cron:session): session opened for user munin by (uid=0)
8	2018-02-19 14:30:01	ssb500vm	6	CRON	pam_unix(cron:session): session opened for user root by (uid=0)
9	2018-02-19 14:31:01	ssb500vm	6	CRON	pam_unix(cron:session): session opened for user root by (uid=0)
10	2018-02-19 14:32:01	ssb500vm	6	CRON	pam_unix(cron:session): session opened for user root by (uid=0)

コンテンツベースのアラート

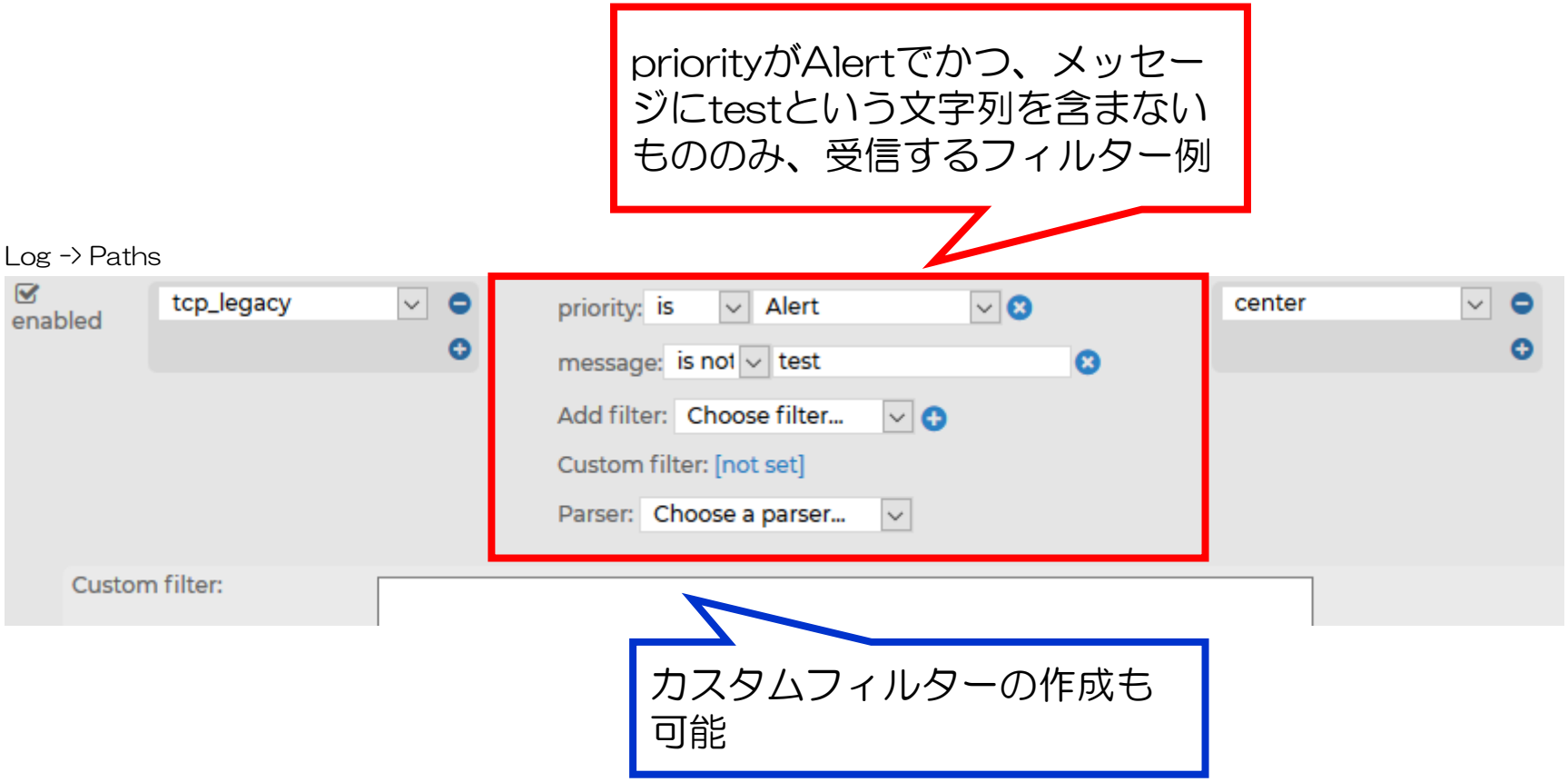
SSBは、ログを数秒間隔で自動検索して検索式に一致した場合に
アラートメールを発行することができます。

Search -> Logspaces



フィルター

SSBは、強力なフィルターを搭載しています。指定条件に合致するシスログのみを、絞込み受信あるいは振分け転送といった処理が可能です。



リライト（ログの書換え）

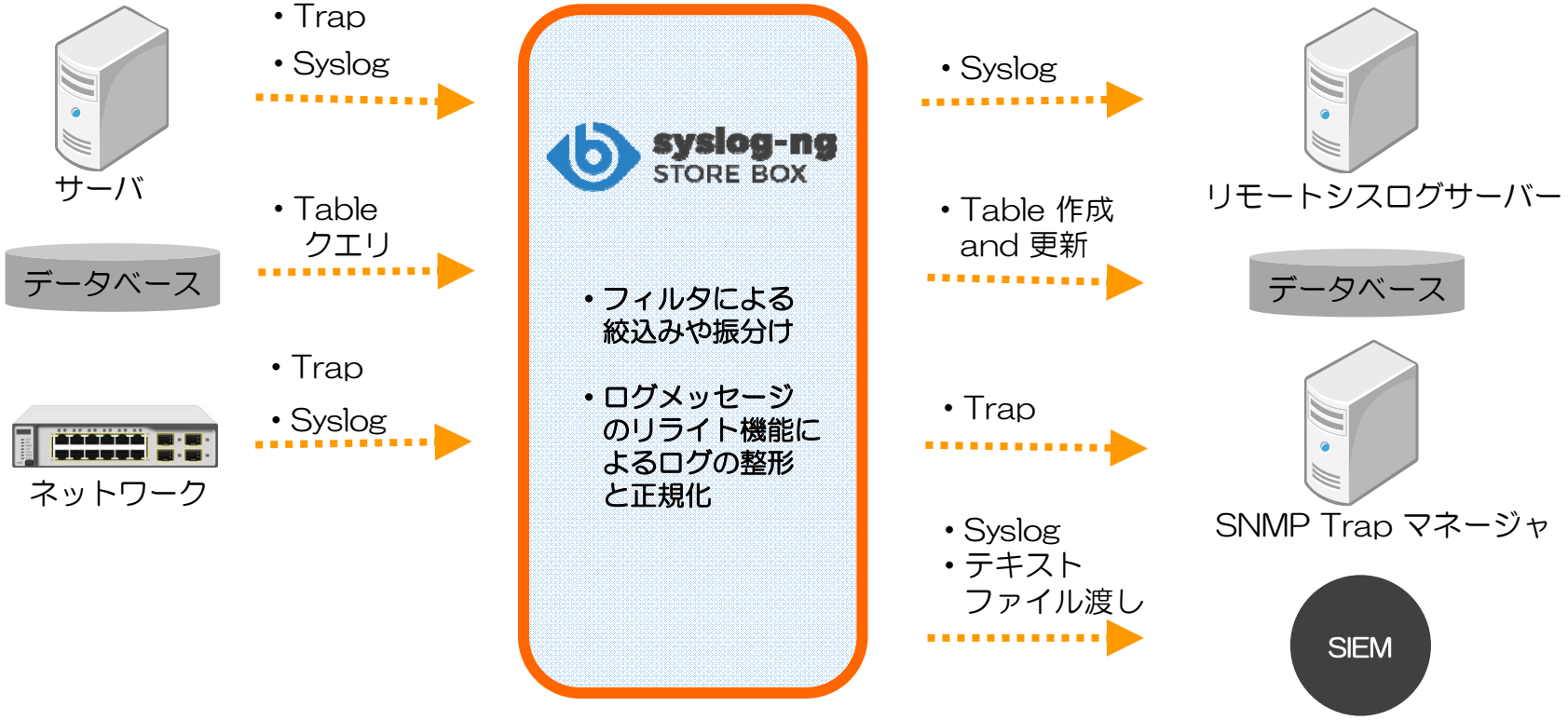
SSBは受信中のログのリライト機能を有しており、他のログ解析ソフトウェア（SIEMなど）用にログの整形や正規化ができます。

- リライトルールは、マクロで定義されたデータの書き換え、文字列に一致したデータの置換を設定します。
- リライトルールは、フィルター前とフィルター後に実行することができます。

受信ログの受信と送信

SSBは、受信したシスログやトラップなどをフィルターなどで処理し
外部サーバやSIEMなどの連携システムへ送信することができます。

送信先の設定は、複数用意する事が出来ます。

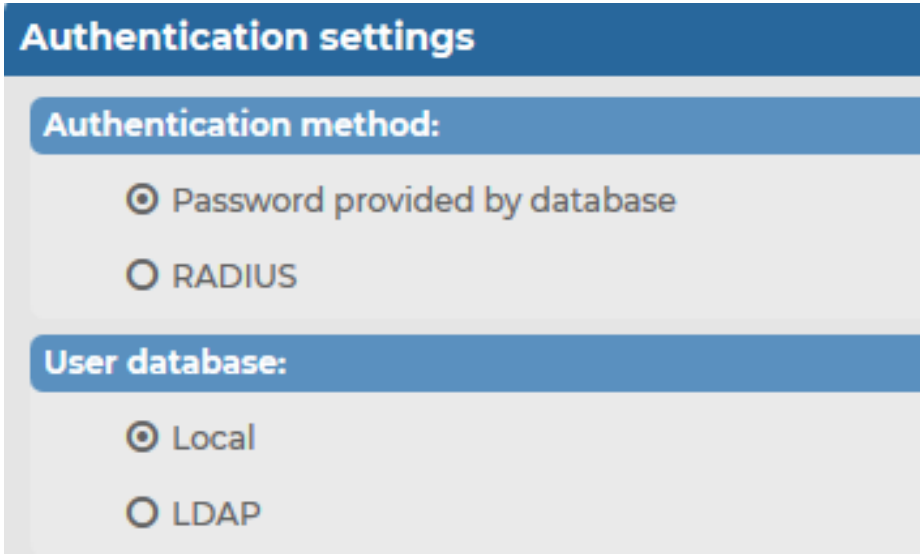


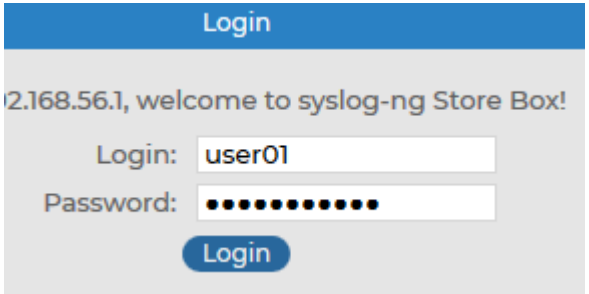
ユーザー認証

SSBを管理するWebインターフェースへのアクセス認証は、
以下の方法を選択できます。

- SSB内データベースでの認証
- LDAPサーバと連携した認証
- RADIUSサーバと連携した認証

AAA -> Settings

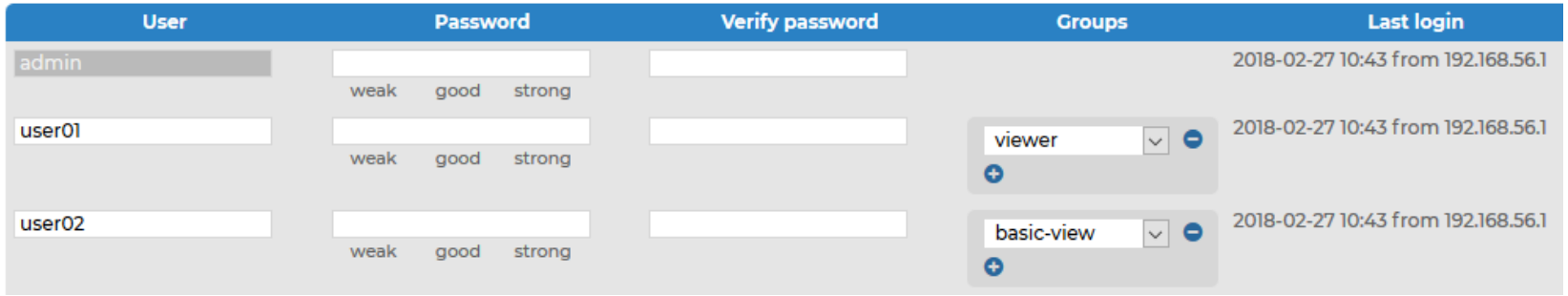




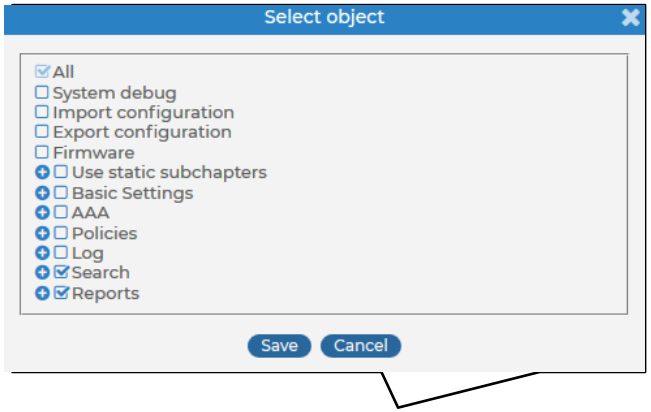
ユーザのアクセス制御

SSBではローカルにユーザーアカウントを作成でき、ユーザが属するグループごとにアクセス権限（全権限やログ検索のみなど）を詳細に設定し管理できます。

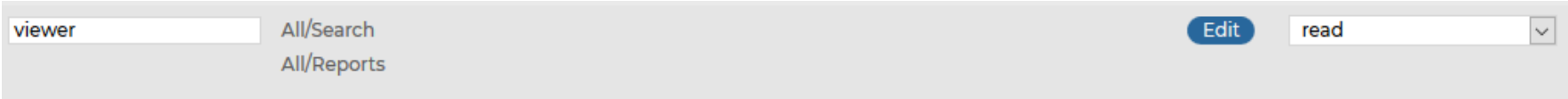
AAA -> Local Users



ログ検索とレポートページのみを閲覧する権利を与えられたグループを作成した例

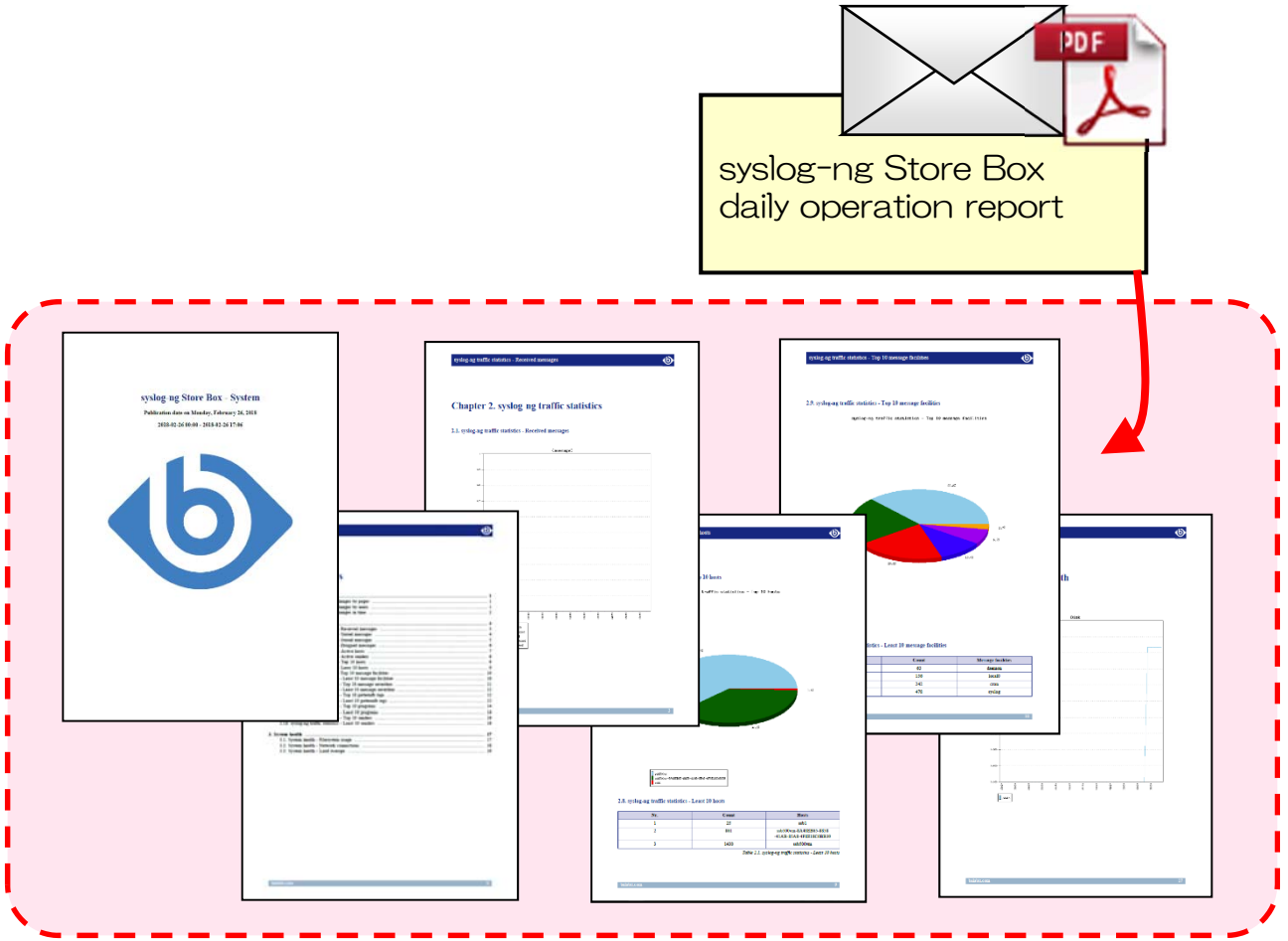


AAA -> Access Control



シスログの統計レポート

SSBは、シスログのトラフィックなどの統計レポートをPDF文書にし、
定期的に管理者へメールでレポートを送信できます。



レポート例：

- 受信したメッセージ数
- 最も多くのログを受信したホストランキング
- 最も多いファシリティランキング
- SSBのシステムヘルス
- 他

バックアップ・アーカイブ

ログデータをリモートサーバやネットワークストレージに自動的に保存できます。毎日の実行時間をスケジュールできます。

バックアップ（データを複製）

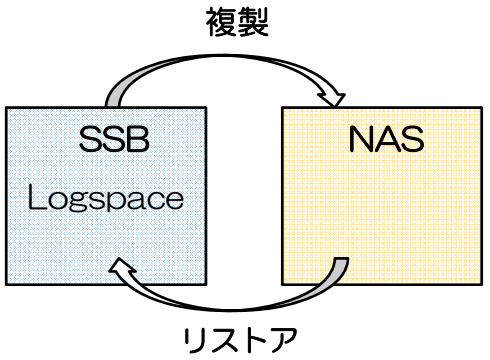
- データをSSBへリストアして復旧できます。
- プロトコル：Rsync、SMB/CIFS、NFS

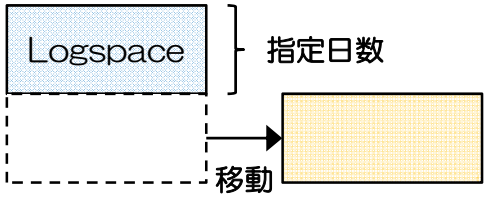
アーカイブ（指定日数より古いデータを移動）

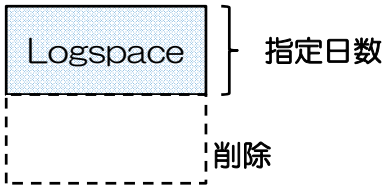
- 内蔵データと同様に検索・閲覧できます。
- データをSSBへリストアできません。
- プロトコル：SMB/CIFS、NFS

クリーンアップ（指定日数より古いデータを削除）

- 内蔵データを最新状態に保持します。



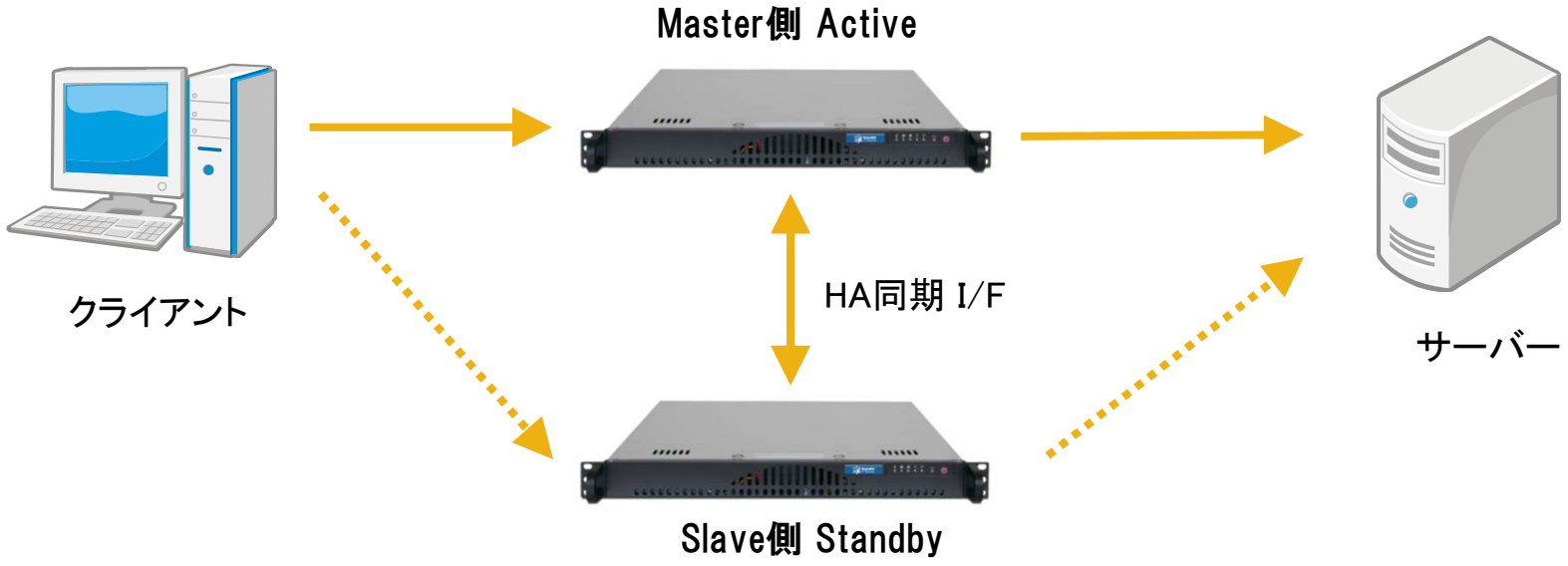




HA構成（高可用性構成）（1）

SSB T1/T4/T10は、 HA構成（High Availability／高可用性）でシステムを冗長化する事が出来ます。

- HA構成は、Master-Slave型のActive-Standby形式です。
- Masterノードの設定、保存した全てのデータがHAデータ同期用LANケーブルにて、Slave側にリアルタイムでコピーされます。



HA構成（高可用性構成） (2)

SSB T1/T4/T10をHA運用する場合、Masterノードがサービスを提供できなくなった際は、SlaveノードがMasterノードのIPアドレスを引き継ぎ、サービスの提供を引き継ぎます。

※ HAはハードウエア・アプライアンスのみの機能です。バーチャル・アプライアンスでは利用できません。

※ シングルノードとHAオプションの2台のSSBが必要です。

※ HA機能による冗長化は2台構成のみとなります。

SSBの監視とアラート

SSBは、ディスク容量が閾値を越えた場合など、設定した条件で
アラートをEmailやSNMP Trapで通知することができます。

アラート例：

- SSBにログイン失敗
- アーカイブ失敗
- ライセンス数に到達
- ディスク容量が超過
- 他

Basic Settings -> Alerting & Monitoring

System related traps

Description	Name	Email	SNMP
Login failed	xcbLoginFailure	Email ☑	SNMP ☑
Successful login	xcbLogin	Email ☐	SNMP ☐
Logout from the management interface	xcbLogout	Email ☐	SNMP ☐
Configuration changed	xcbConfigChange	Email ☐	SNMP ☐
General alert	xcbAlert	Email ☐	SNMP ☐
General error	xcbError	Email ☐	SNMP ☐
Data and configuration backup failed	xcbBackupFailed	Email ☐	SNMP ☐
Data archiving failed	xcbArchiveFailed	Email ☑	SNMP ☑
Database error occurred	xcbDBError	Email ☐	SNMP ☐
License limit reached	xcbLimitReached	Email ☑	SNMP ☑
HA node state changed	xcbHaNodeChanged	Email ☐	SNMP ☐
Timestamping error occurred	xcbTimestampError	Email ☐	SNMP ☐
Time sync lost	xcbTimeSyncLost	Email ☐	SNMP ☐
Raid status changed	xcbRaidStatus	Email ☐	SNMP ☐
Hardware error occurred	xcbHWError	Email ☐	SNMP ☐
Firmware is tainted	xcbFirmwareTainted	Email ☐	SNMP ☐

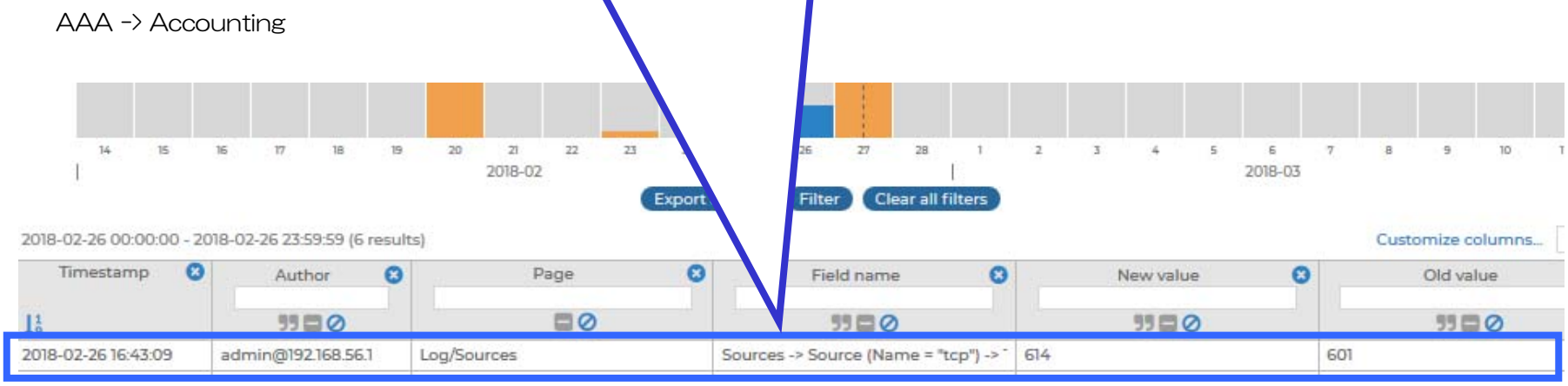
Health related traps

Description	Name	Email	SNMP
Disk usage is above the defined ratio	xcbDiskFull	Email ☑	SNMP ☑

設定変更履歴記録機能

SSBは、SSBの設定変更の履歴を「いつ、だれが、どのパラメーターを、何から、何に変更したか」克明に記録します。不正な変更の調査や、トラブルシューティングに大変役立ち、コンプライアンス対応にもなります。

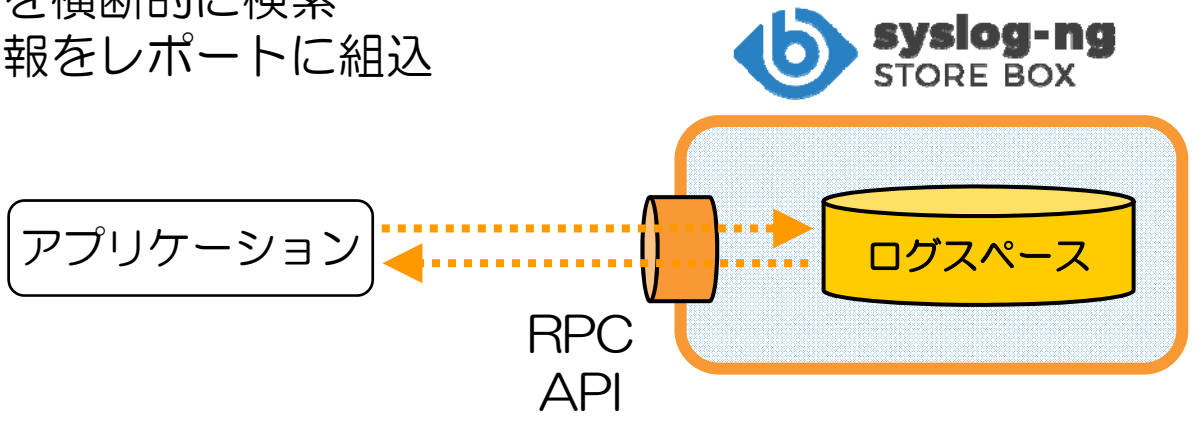
192.168.56.1からadminアカウントでログインしたユーザーが、2018年2月26日16時43分09秒にtcpのポート番号を、601から614に変更したことを記録した履歴。



RESTfulのAPI

SSBに格納されたログメッセージに、リモートアプリからアクセスやクエリを実行可能です。これはHTTPS上のRESTfulプロトコルを用いてAPIにアクセスすることで実現されます。様々なプログラミング言語を用いてSSBをシステム環境に統合することができます。

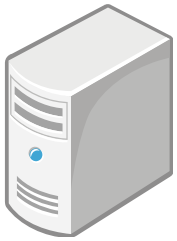
- カスタムアプリ、環境への統合
- 柔軟で動的な検索クエリ
- 複数のログストアを横断的に検索
- 検索結果や統計情報をレポートに組込



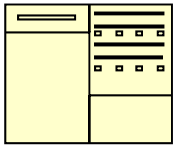
ライセンス

SSBのライセンスは、LSH（ログソースホスト：ログ送信元）数で計算します。LSHは IPアドレスで区別されます。

192.168.1.1



192.168.1.2



192.168.1.3

- SSBはライセンスを登録して使用します。
  例：100LSHは、送信元デバイス数 100 IP まで対応可能なライセンスです。
- 機能評価用に評価ライセンス（30日間）を用意しています。

その他 ログの解析

SSBは、ログの受信に特化しているため、受信したログの体系的な統計解析には、専用の外部アプリケーションをご利用下さい。

例えば、Flowerfire社（米国）のログ解析ソフト「 SAWMILL 」は専用エージェントであるsyslog-ng用のプラグインを標準で備えています。

お問い合わせ

syslog-ng STORE BOX

ジュピターテクノロジー株式会社（Jupiter Technology Corp.）

URL: http://www.jtc-i.co.jp/　Email info@jtc-i.co.jp

本社

住所 〒183-0023

東京都府中市宮町2-15-13　第15三ツ木ビル8Ｆ

Tel 042-358-1250

大阪営業所

住所 〒530-0001

大阪府大阪市北区梅田1-1-3 大阪駅前第3ビル11Ｆ

Tel 06-6131-8471

JTC-i Jupiter Technology corp.