

# Powered BLUE シスログ・サーバー

ログサーバーアプライアンス

&

インターネットサーバー機能

Web/DNS/Mail/ftp

— Powered BLUE 870 Syslog —

## ログサーバー機能

シスログの受信・転送・保存

機器の認証や暗号化によるログ送受時の「なりすまし&盗聴」防止

## インターネットサーバー機能

Web/Mail/DNS/FTP/ サーバー機能を1台で運用

## セキュリティ機能

SNI対応(常時SSL化)

SELinux対応(セキュアOS)

## 仮想・クラウド対応

RedHat / CentOS 7.x (64bit) に対応

VMWare / Hyper-V に対応

アマゾンウェブサービス (AWS/EC2) 対応

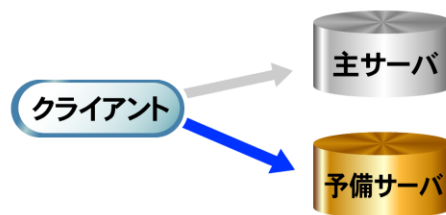
# ログサーバー機能 (rsyslog)

The screenshot shows the Powered BLUE web management interface. The top navigation bar includes 'サーバの管理', 'サイトの管理', 'アップデート', '個人プロフィール', and 'ライセンス管理'. The left sidebar lists various system settings, with 'シスログ' (System Log) selected. The main content area is titled 'シスログ転送設定' (System Log Transfer Settings) and contains the following configuration options:

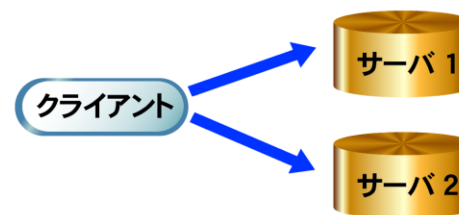
- シスログ転送を有効にする
- 転送先のホスト: 127.0.0.1
- プロトコル:
  - UDP (ポート514)
  - TCP (ポート514)
  - RELP (TCPポート10514)
  - TLS (TCPポート6514)
  - TLS / RELP (TCPポート16514)
  - MySQL (TCPポート3306)
- 圧縮:
- ユーザ名: rsyslog-admin
- パスワード: ;W3Gv8SB3j-e3sdsd
- ポートの変更 (省略可): [ ]
- キューモード: ディスク・キュー
- TLS認証方法: サーバ証明書に記載されたホスト名(CN)
- TLS接続サーバ名: [ ]

A '保存' (Save) button is located at the bottom of the configuration area. A footer note reads: '? シスログに関連した設定項目。'

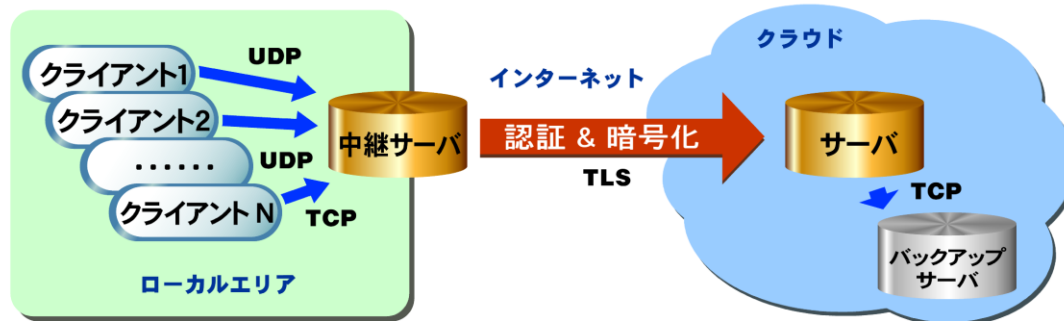
# ログサーバー機能



バックアップサーバへの切替え



ログの同時転送



既存のサーバ(クライアント)のログをリモートサーバへ送る

1)冗長送信

最大 3台へ同時 に送信

2)漏洩防止

TLS( 暗号化通信 & 機器認証 )

3)欠落防止

送信キュー によるログの一時保管

## ログサーバー機能

機能	内容
UDP/TCP/TLS/RELPL	TLSによる暗号化経路での通信に対応
サーバー認証	TLS通信では、クライアントとサーバー間の機器の認証による「なりすまし」も防止
改竄防止	TLS通信では、偽造メッセージの挿入や改竄も防ぎます
動作モード	ログ送信・転送・受信のいずれのモードでも運用可能
ログ冗長送信	最大3台への同時送信
ログ転送	ログの転送時にも、保存が可能
ログ保存	ローテーション回数・保存期間は任意指定・ ログのダウンロード
送信キュー	回線途絶や受信側サーバー不調時は、送信キューへの一時保管によりログの欠落を防止
アラート	キーワード指定によるログのトラップ & メール通知
対応形式	rsyslog
サーバー証明書	SSLサーバー証明書のインポート機能

# ソフトウェア機能（標準 / フリープラグイン）

項目	有無	内容
http /https Server	○	複数サイトの運用可能
DNS Server	○	
SMTP/SMTPS/POP/POPS/IMAP/IMAPS	○	Postfix・SMTP Auth・Submission port
メールの中継設定	○	ドメイン・アドレスごとの配送設定可能
SNMP / Firewall 機能 / SPF レコード	○	
SNI	○	IPアドレス1個で全WebサイトのSSL化
HSTS	○	httpアクセスをhttps通信への切り替え
仮想サイト管理者での設定	○	仮想サイトごとに権限移譲可能
OSアップデート	○	スケジュールアップデート 対応
CMS	○	WordPress(フリープラグイン)

## ソフトウェア機能

項目	有無	内容
http /https Server	○	複数サイトの運用可能
DNS Server	○	
SMTP/SMTPTS/POP/POPS/IMAP/IMAPS	○	Postfix・SMTP Auth・Submission port
SNMP / Firewall 機能 / SPF レコード	○	
FTP / anonymous FTP	○	
メールの中継設定	○	ドメイン・アドレスごとの配送設定可能
仮想サイト管理者での設定	○	仮想サイトごとに権限移譲可能
OSアップデート	○	スケジュールアップデート 対応
メール添付ファイルZIP暗号化	△	オプション
メール添付ファイルWebダウンロード	△	オプション
大容量ファイルの送受信	△	オプション
Private CA機能	△	オプション
リバースプロキシ	△	オプション

# 動作環境

OS	RedHat 7.x (64bit) / CentOS 7.x (64bit)
仮想環境	VMWareESXi 5.1 / 5.5 / 6.0 / 6.5 Hyper-V 7.X
クラウド環境	AWS (アマゾンウェブサービス / EC2) Azure / 他
ハードウェア アプライアンス	19インチ1U / 他
スペック	1 Core(min) / 512MB mem (min) / 10GB HDD (min) / Ethernet x 1



The screenshot shows the 'ウェブの設定' (Web Settings) page in the Powered BLUE management interface. The left sidebar contains a navigation menu with items like 'サーバの管理者', 'ネットワークサービス', 'ウェブ', 'FTP', '電子メール', 'DNS', 'シェル', 'データベース', 'セキュリティ', 'システムの設定', '保守', '利用状況', 'アクティブモニタ', 'オプション', and 'サポート情報'. The top navigation bar includes 'サーバの管理', 'サイトの管理', 'アップデート', '個人プロフィール', and 'ライセンス管理'. The main content area is titled 'ウェブの設定' and has three tabs: '基本', 'セキュリティ', and '詳細'. The 'セキュリティ' tab is active, showing a 'セキュリティ設定' (Security Settings) section with the following items:

バージョン情報を公開しない	<input checked="" type="checkbox"/>
PHPヘッダを応答しない	<input checked="" type="checkbox"/>
HTTP Traceメソッドを無効にする	<input checked="" type="checkbox"/>
SSLセキュアレベル	TLS1.2以上を使用する(強レベル) ▼

Below the table is a blue '保存' (Save) button. At the bottom of the page, a blue banner contains the text: '? セキュリティに関する設定を行います。' (Security settings will be performed.)

- 1) 日本語・英語の2か国語対応
- 2) パッチなどの自動アップデート機能

# 常時SSL化対応 セキュリティの強化

## ■ SNI (Server Name Indication) 機能

ウェブの設定

名前ベースのSSL仮想サイトを使う

SNIを有効にする

IPアドレス1個で、全WebサイトのSSL化に対応

## ■ Webバージョンの非公開やSSLセキュアレベルの指定機能

ウェブの設定

セキュリティ設定

バージョン情報を公開しない	<input checked="" type="checkbox"/>
PHPヘッダを応答しない	<input checked="" type="checkbox"/>
HTTP Traceメソッドを無効にする	<input checked="" type="checkbox"/>
SSLセキュアレベル	TLS1.2以上を使用する

## ■ HSTS (HTTP Strict Transport Security)対応

httpでアクセスを受けると、次回以降はhttpsでの接続に切り替えて、通信経路の安全を確保する機能

## ■ SELinux対応(セキュアOS)

SELinuxの設定

SELinuxを有効にする

システムの動作状況 - 概要	
4 エントリ	
▼ コンポーネント名	▼ 詳細
● CPU の使用状況	🔍
● ディスクの使用状況	🔍
● ネットワークの状態	🔍
● メモリの使用状況	🔍

サービスの動作状況 - 概要	
8 エントリ	
▼ コンポーネント名	▼ 詳細
● DNS サーバ	🔍
● FTP サーバ	🔍
○ SNMP サーバ	🔍
● Telnet サーバ	🔍
● ウェブサーバ	🔍
● サーバデスクトップ	🔍
● サーバ・ライセンス	🔍
● 電子メールサーバ	🔍

その他の動作状況 - 概要	
2 エントリ	
▼ コンポーネント名	▼ 詳細
● アンチウイルス・ゲートウェイ	🔍
● 電子メールプラス	🔍

色と意味: ○ 情報がないか、監視が無効に設定されています。

- 正常に動作中
- 問題発生
- 深刻な問題発生

## サーバーのモニタリング & サービスの自動再起動