BALABIT

CONTEXTUAL SECURITY INTELLIGENCE

Shell Control Box 5LTS ご紹介

製品ガイド

Rev 3.0

平成29年8月23日

ジュピターテクノロジー

変更履歴

BALABIT
CONTEXTUAL SECURITY INTELLIGENCE

版	発行日	変更内容
第3.0 版	2017/8/23	新規作成

SCB概要

BALABIT
CONTEXTUAL SECURITY INTELLIGENCE

BalaBit SCB（Shell Control Box）は、ハンガリーのBalaBit社が開発した、特権ユーザー管理アプライアンスです。

- 特権ユーザーによるサーバーアクセスのアクティビティ監視と監査のためのプロキシゲートウェイです。
- ユーザーの操作ログを動画で記録し、監査に耐えうる証跡を取得するとともに、国際基準のコンプライアンスに対応します。
- エージェントレスで、サーバーとクライアントの間に設置するだけで、透過的に動作するため、現環境を変更することなく、サーバーへのアクセスを監視/コントロールし、簡単にセキュリティーレベルを強化できます。

SCB適用エリア

BALABIT
CONTEXTUAL SECURITY INTELLIGENCE

- IT管理者／ITスタッフ／特権ユーザーの管理・監査
- クラウド／ホスティングサービス事業者の監視
- ITアウトソーシングパートナーの監視
- VDI(仮想デスクトップインフラ)ユーザーの監査
- ITインシデントのトラブルシューティングおよびフォレンジック対応
- 機密情報・データの保護
- 業界や国際基準の遵守

  J-SOX、ISO27001、など

SCBの主要機能

BALABIT
CONTEXTUAL SECURITY INTELLIGENCE

- ユーザー操作のリアルタイム監視
  監査証跡として動画を安全に保存(圧縮、暗号化、タイムスタンプ、電子署名)
- 記録したユーザー操作の動画再生
- ゲートウェイ認証(ローカル、LDAP連携、証明書ストア 等)
- アクセスコントロール
  対応プロトコル：SSH, RDP, HTTP(s), Citrix ICA, VNC, Telnet
- 不正操作のリアルタイム防御
- 監査証跡の再生・フリーテキスト検索
- Eメール 、SNMPトラップ によるアラート
- コンプライアンスレポート作成
- 保存データの自動アーカイブ、バックアップ
- HA(ハイアベイラビリティ)構成サポート
- WebAPI (RPC API / REST API)

SCB製品モデル

BALABIT
CONTEXTUAL SECURITY INTELLIGENCE

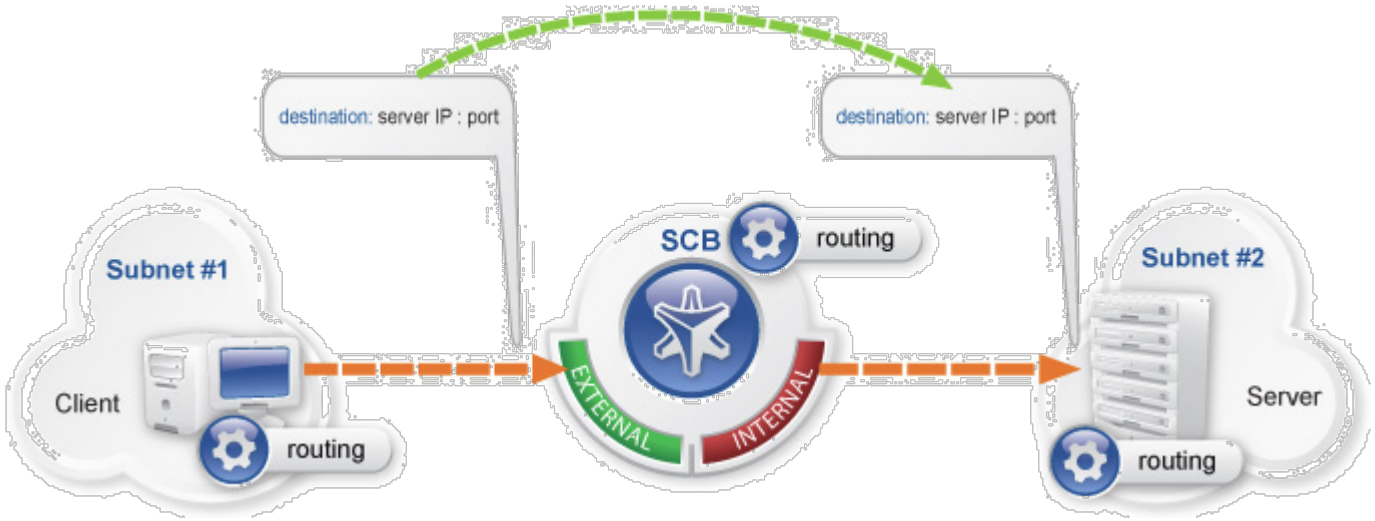
BalaBit SCBは、ハードウェアアプライアンスとVMwareバーチャルアプライアンス、BlueVaultアプライアンスとして提供します。

※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
ハードウェア 	T1	物理 1U	1X4 core INTEL Xeon X3430 @2.40GHz	8GB (2 x 4 GB)	1TB (2 x 1TB)	Software RAID
	T4	物理 1U	1X4 core INTEL Xeon E3-1275V2 @3.50GHz	8GB (2 x 4 GB)	4TB (4 x 2TB)	Hardware RAID LSI MegaRAID SAS 9271-4i SGL
	T10	物理 2U	2x6 core INTEL 2x Xeon E5-2630V2 @ 2.6GHz	32GB (8 x 4 GB)	10TB (13 x 1TB)	Hardware RAID LSI 2208 (1GB cache)
バーチャル vmware	VA	仮想 マシン	VMware ESX 4.0、ESXi 5.0以降、 Microsoft Hyper-V、Microsoft Azure、KVM			
BlueVault® VmwareESXiで動作	H2 /H2H	物理 1U	1X4 core INTEL Xeon E3-1220V5 @3.0GHz	16GB	2T(2 x 2TB) /2T(4 x 1TB)	RAID1 /RAID10
	H4		1X4 core INTEL Xeon E5-2623V3.2 @2.8Ghz		4T (4 x 2TB)	RAID10
	H10	物理 2U	2X8 core INTEL Xeon E5-2620V4 @2.1Ghz	48GB	10T (12 x 1TB)	RAID50

動作モード1）トランスペアレントモード*

- ネットワーク層（OSIモデルのレイヤ3）で保護されたサーバーのセグメントに管理者のネットワークセグメントを接続する透過ルータとして働きます。
- すべての接続はSCBを通過してサーバーに到達します。
- SCBはプロキシゲートウェイであり、保護されたサーバーをネットワークの他の部分から完全に分離します。

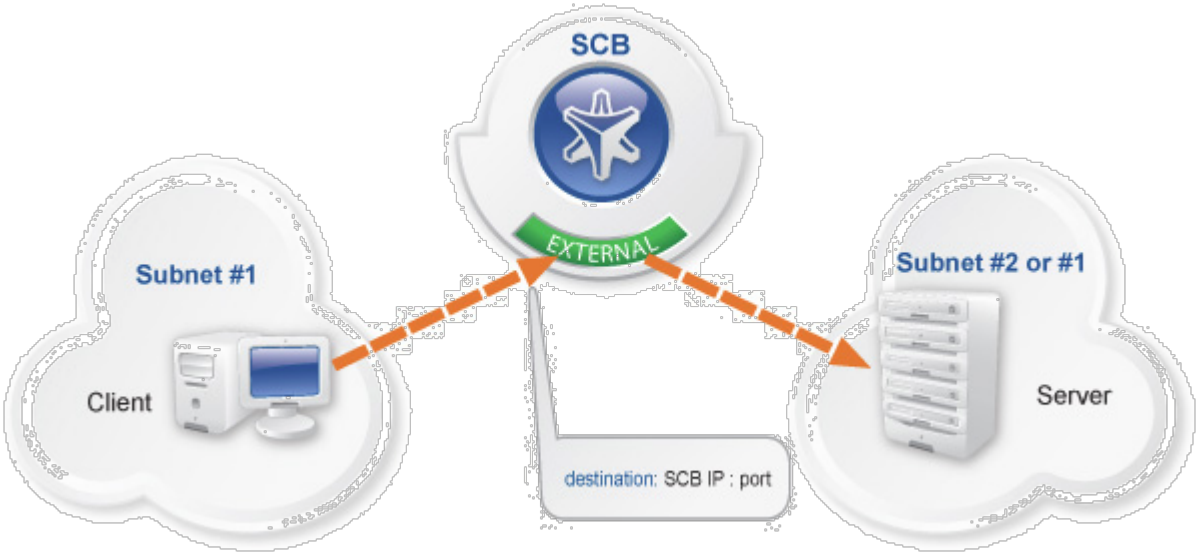


＊マルチキャストはサポートしません。

＊シングルインターフェース・トランスペアレントモードもあります。

動作モード2) ノントランスペアレントモード*

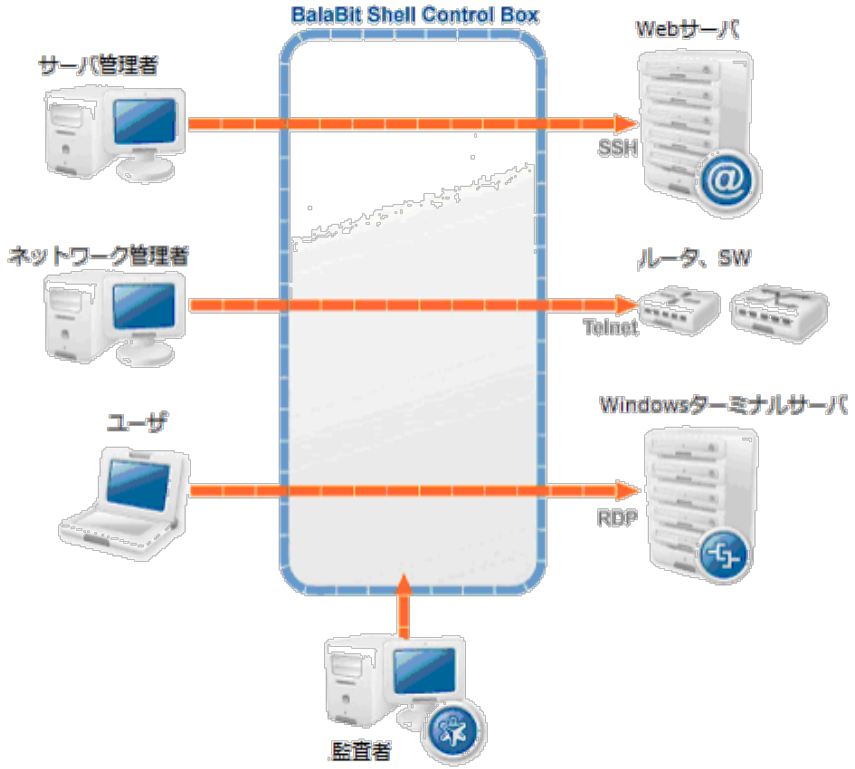
- SCBは、着信接続のパラメータ（管理者のIPアドレスとターゲットIPおよびポート）に基づいて、接続するサーバーを決定します。
- ユーザーは直接目的のサーバーにアクセスできません。
- SCBが故障した場合でも、サーバー上で実行されているサービスとアプリケーションにアクセスできるため、SCBは単一障害点にはなりません。



＊ファイアウォールは、SCBからの接続のみがサーバーにアクセスできるように設定します。

特徴) エージェントレス

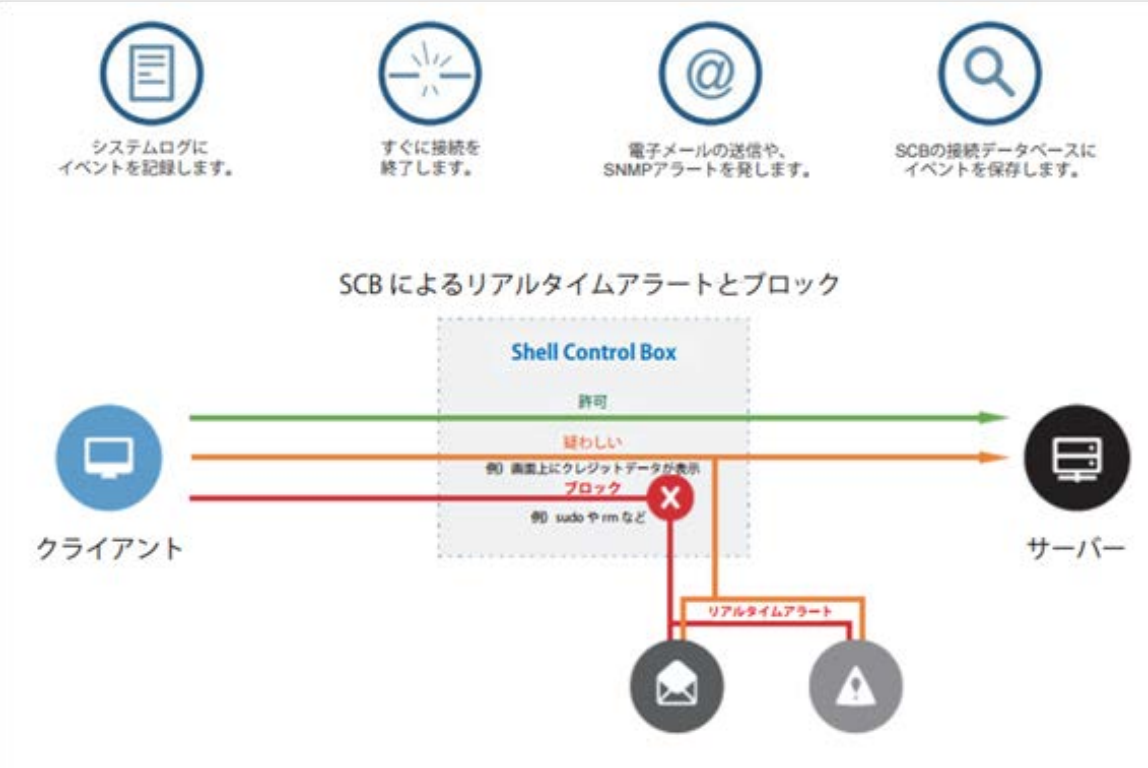
- エージェントをインストールできないルータ、スイッチなども監視対象にできます。
- 本番サーバーへの影響がないので、現行システムに負荷の掛からない構築が可能です。



特徴）不正操作のリアルタイム防止

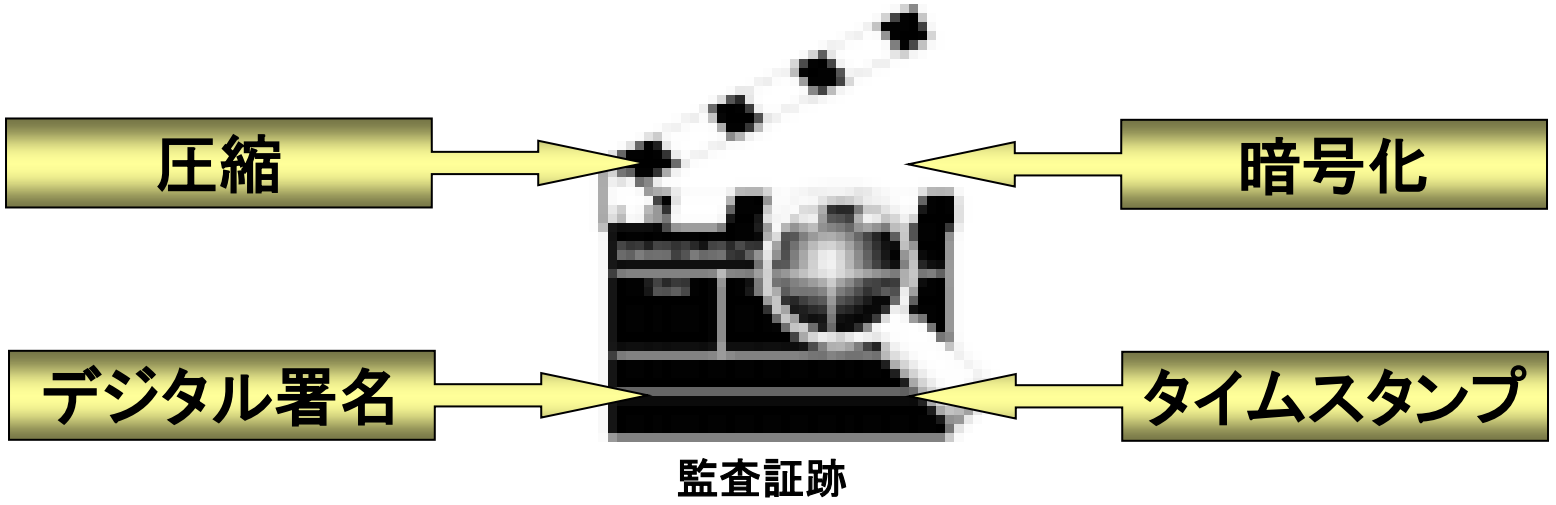
BALABIT
CONTEXTUAL SECURITY INTELLIGENCE

- リアルタイムにネットワークトラフィックを監視し、画面にあるパターン（たとえば、問題と思われるコマンド、不審なウィンドウタイトルなど）を発見すると指定されたアクションを実行します。
- たとえば、壊滅的な結果になりかねない「削除」のようなコマンドが実行される前に、接続を遮断できます。例：$ sudo rm -rf directory



特徴）信頼性の高い監査

- 第三者の操作を防止し、監査担当者のための信頼性の高い情報を提供するために、SCB はすべての監査証跡にタイムスタンプ、暗号化、署名などが可能です。
- これは、監査対象の情報を変更されることを防止します。SCB の管理者であっても暗号化された監査証跡を改ざんできません。
- また、SCB は構成のどんな些細な変更であっても変更履歴が生成されます。



特徴）詳細なアクセス制御

- SSH, RDP, HTTPSのような暗号化プロトコルも含め、サーバーに誰が（ユーザー名）、何を（チャネルタイプ）、いつ（時間）アクセスできるかをコントロールできます。
- 特定のチャネルだけを許可するようにコントロールできます。たとえば、ファイル転送やファイル共有のような不要なチャネルを無効にし、サーバーのセキュリティリスクを軽減することができます。
- SCBを導入すると１台の簡単なシステムですべてのアクセスポリシーを強制適用できます。その結果、最小コストでインフラ全体のセキュリティレベルを確保できます。

機能）設定・管理

- ブラウザでアクセスする直感的なWebインターフェースです。
  SCBを管理、サーバーへの接続を管理、監査証跡・レポート閲覧できます。
- 全ての設定変更は記録されます。
  設定変更する場合、コメントを追加することを要求できます。
- SCBの設定情報をエクスポート/インポートできます。

画面例：監査証跡の検索

機能）認証

- Active Directory等のディレクトリサービスと統合できるので、サーバーにアクセスする前にだれがアクセスしたかを明確にできます。
- サーバーにアクセスするための資格情報は、SCBローカル証明書ストアや、サードパーティーのパスワード管理システムから透過的に取得します。

機能）ゲートウェイ認証（二次認証）

- 特権ユーザーのＩＤ（rootなど）を、個人のＩＤによる二次認証で、アクセスするユーザーを特定することができます。

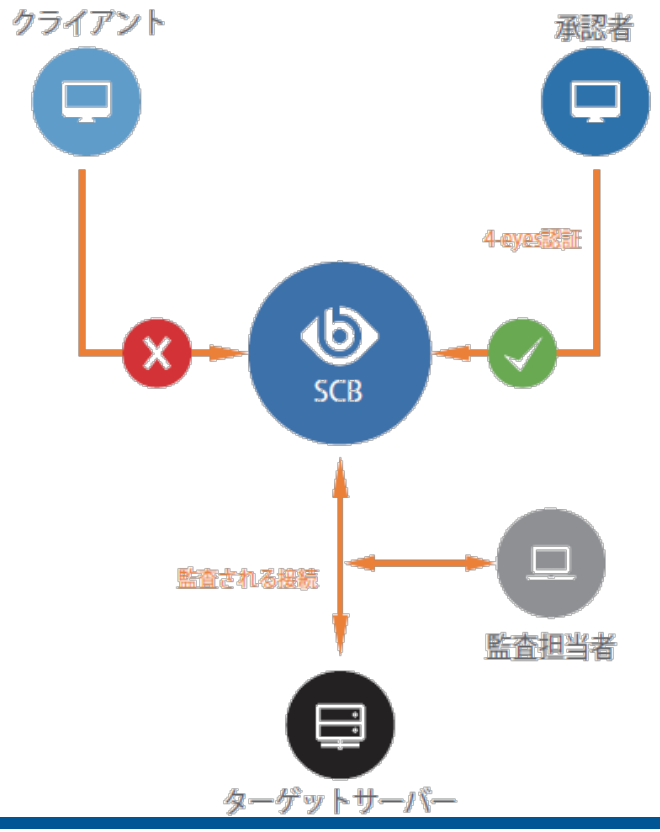
一次認証

二次認証

```
[root@centos68 ~]# ssh root@192.168.56.21
Gateway authentication and authorization
Please specify the requested information
Gateway username: hoge
Gateway password:
Password: _
```

機能) Four-Eyes承認/監視

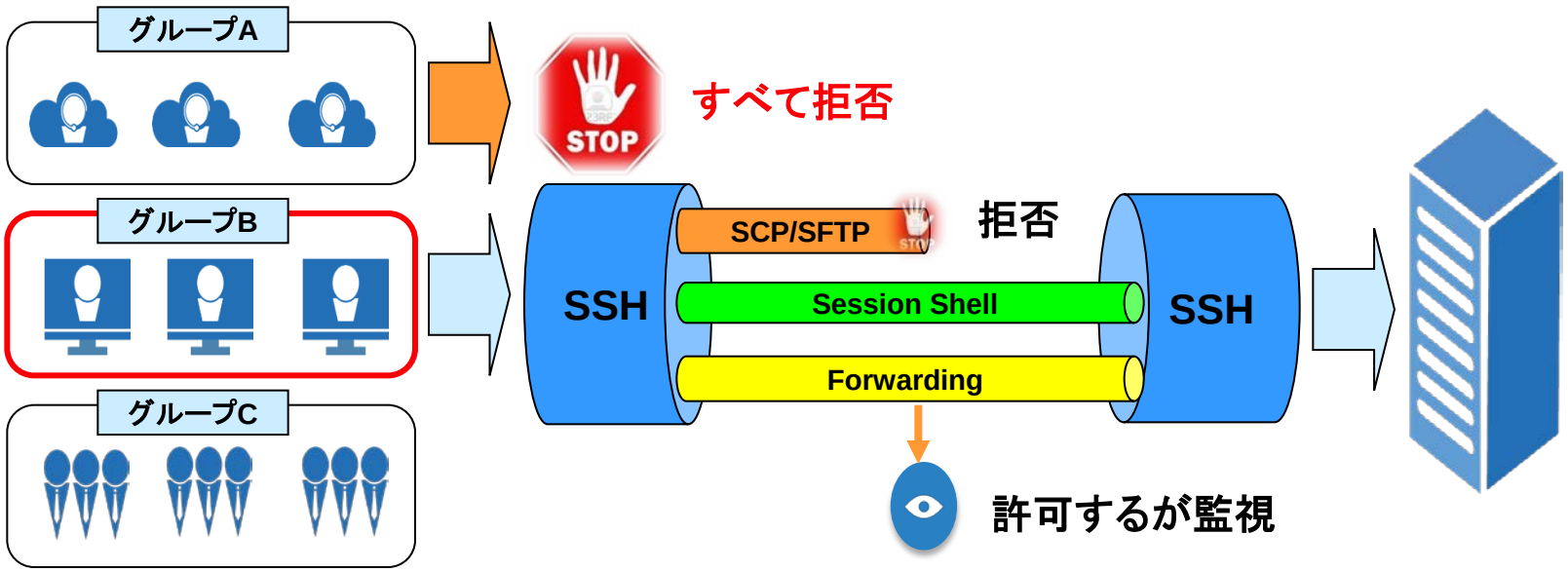
- ユーザーがサーバーにアクセスする時、承認者が接続を許可/拒否します。
- 承認者はユーザーの作業をリアルタイムに画面を共有監視でき、必要があれば接続を終了させることができます。



機能) 監視・制御

- ユーザー操作(サーバー、コンソール接続等)のリアルタイム監視ができます。
- 細かいアクセスコントロールができます。

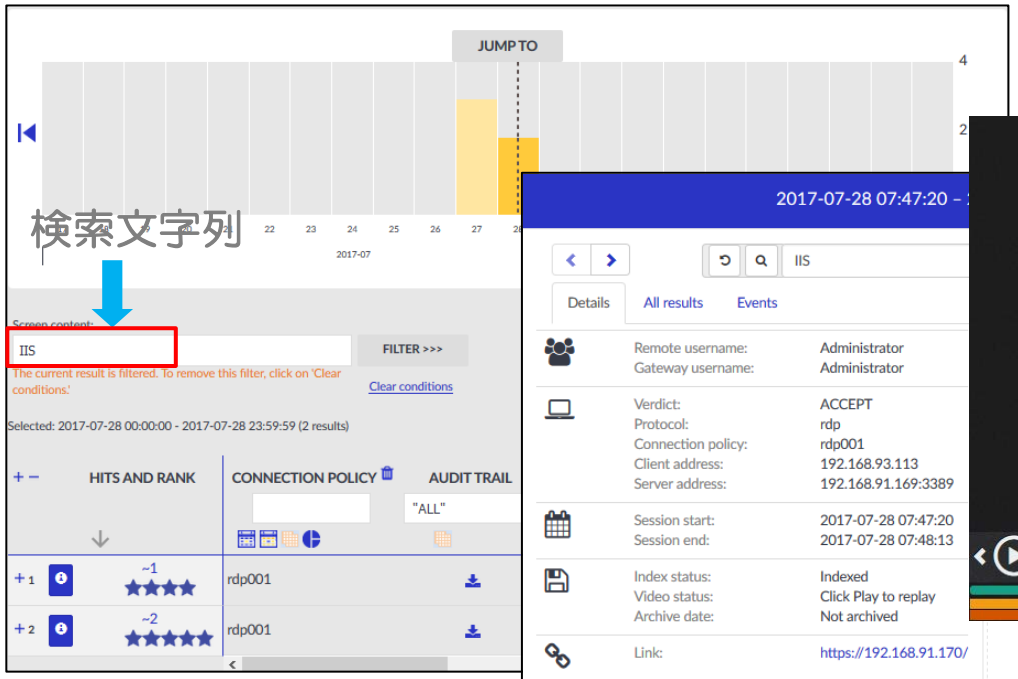
  対応プロトコル：SSH, RDP, HTTP(s), Citrix ICA, VNC, Telnet



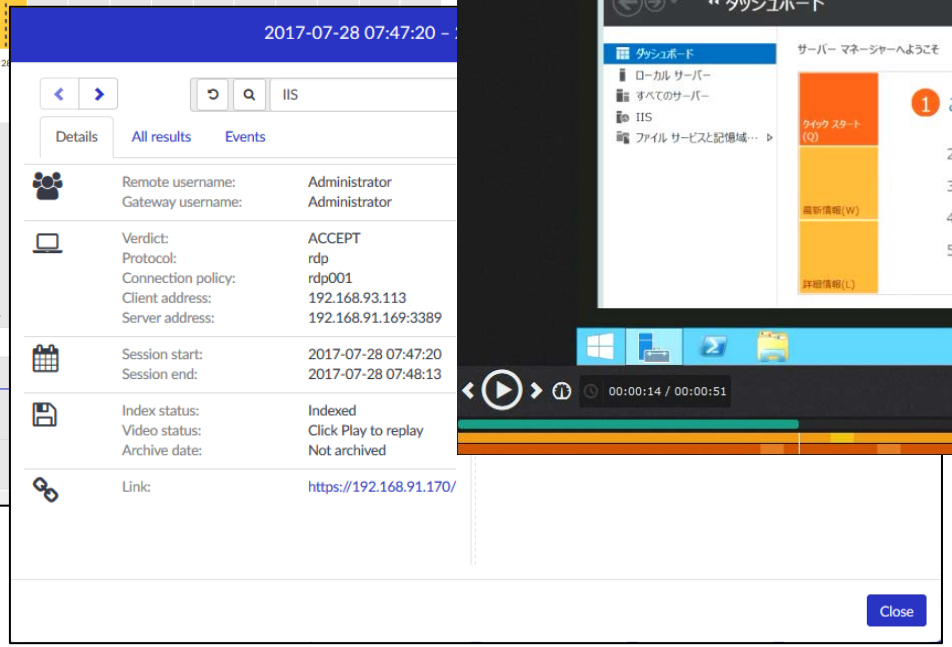
役割に応じて必要最小限のアクセス権を割り当て、
ユーザグループメンバやIPアドレス等のきめ細やかなアクセス制御ができます。

機能) 監査証跡の再生・検索

- 監査証跡に記録したユーザー操作を正確に動画再生できます。
  専用プレーヤーおよびブラウザで再生できます。
- 監査証跡データにはインデックスが付けられ、フリーテキスト検索ができます。



検索結果

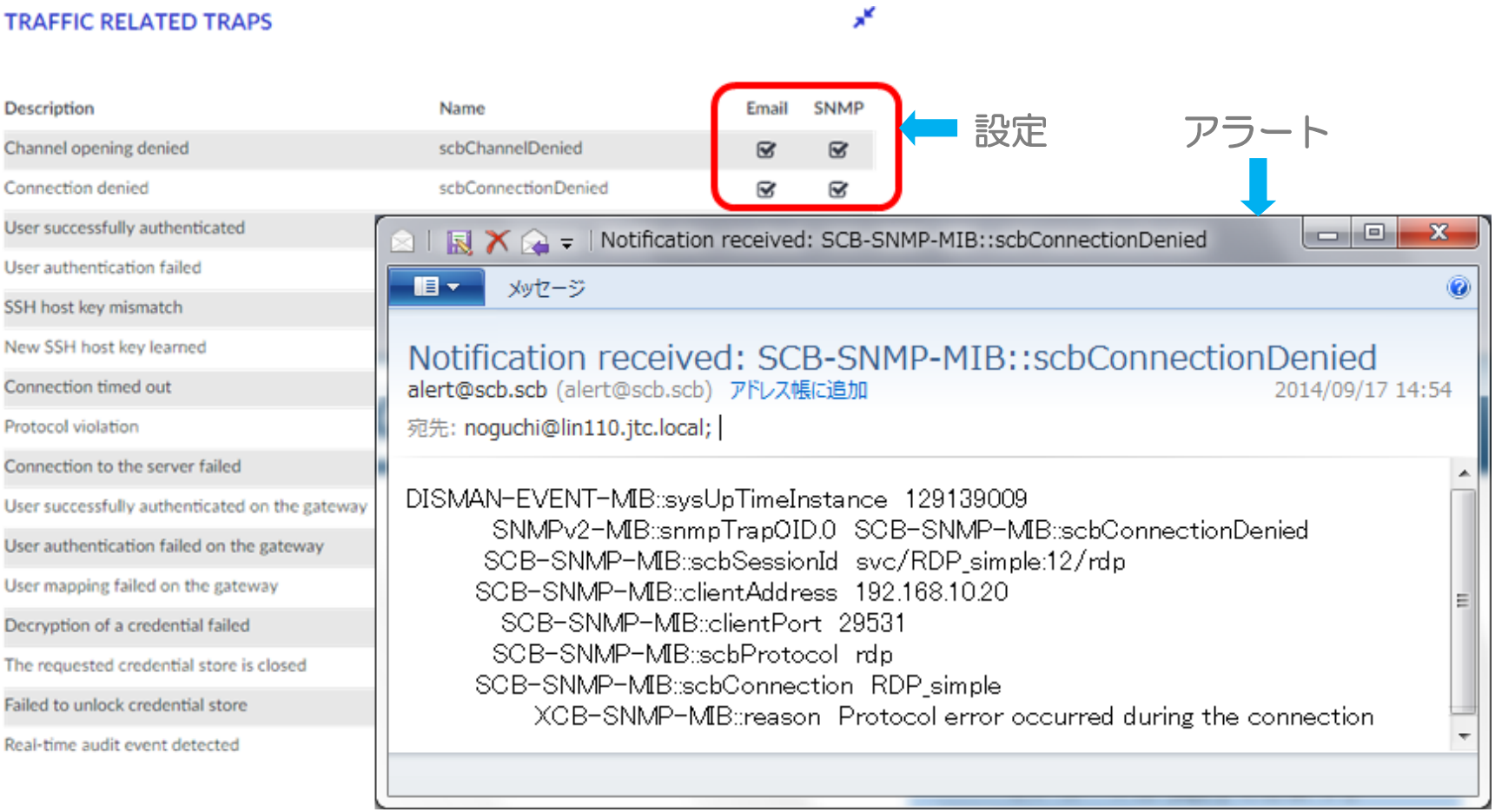


詳細情報

再生画面

機能) アラート

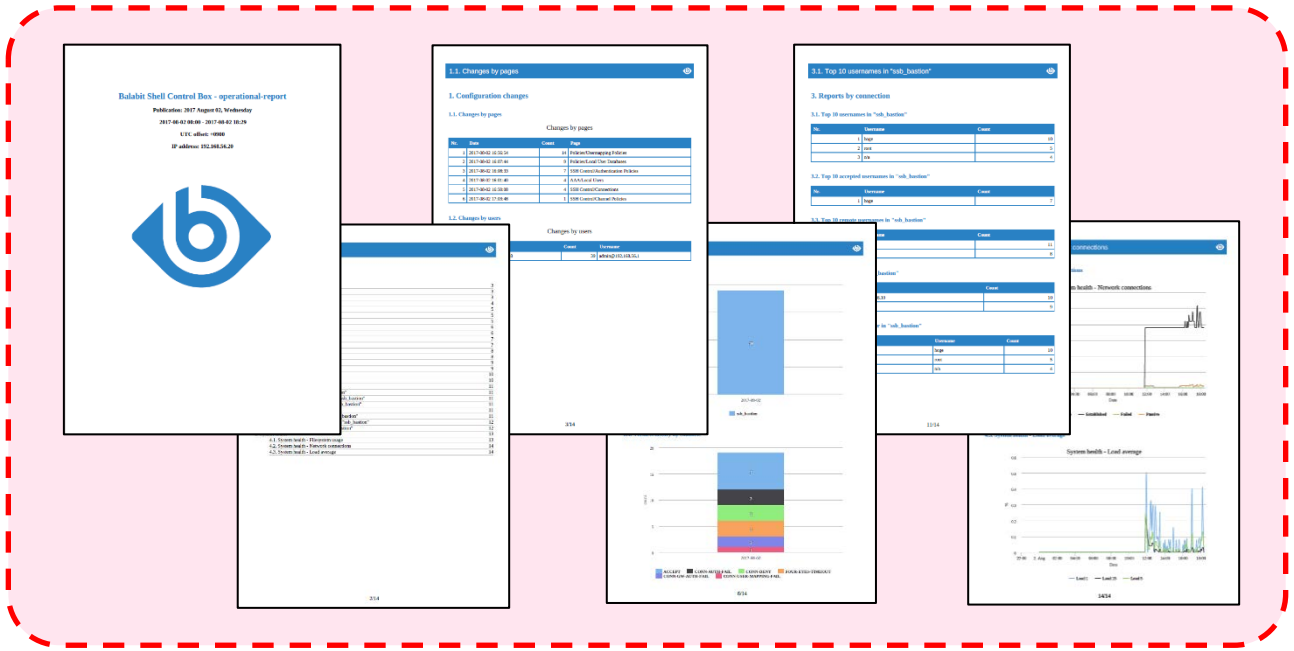
- イベントにあわせて、ＥメールやＳＮＭＰでアラートが発行できます。
  イベントには、SCBのシステム関連やトラフィック関連（接続など）があります。



機能) 運用レポート

- トラフィックや管理者の活動およびシステムの稼動状態の統計情報を定期的にPDFファイルにまとめます。管理者のメールアドレスに送信することもできます。
- 運用内容に応じて、カスタマイズしたレポートを作成できます。
  例：監査証跡データから、検索結果の統計情報など。
- PCIDSS要件に対するSCBのコンプライアンス状況をレポートできます。

レポート例：
- 設定の変更履歴
- 全トラフィックの統計情報
- 接続ポリシー毎の統計情報
- システム稼働情報



機能）バックアップ・アーカイブ

監査証跡データをリモートサーバ（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（データを複写）

- データをSCB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SCBへリストアできません。
- プロトコル：SMB/CIFS、NFS

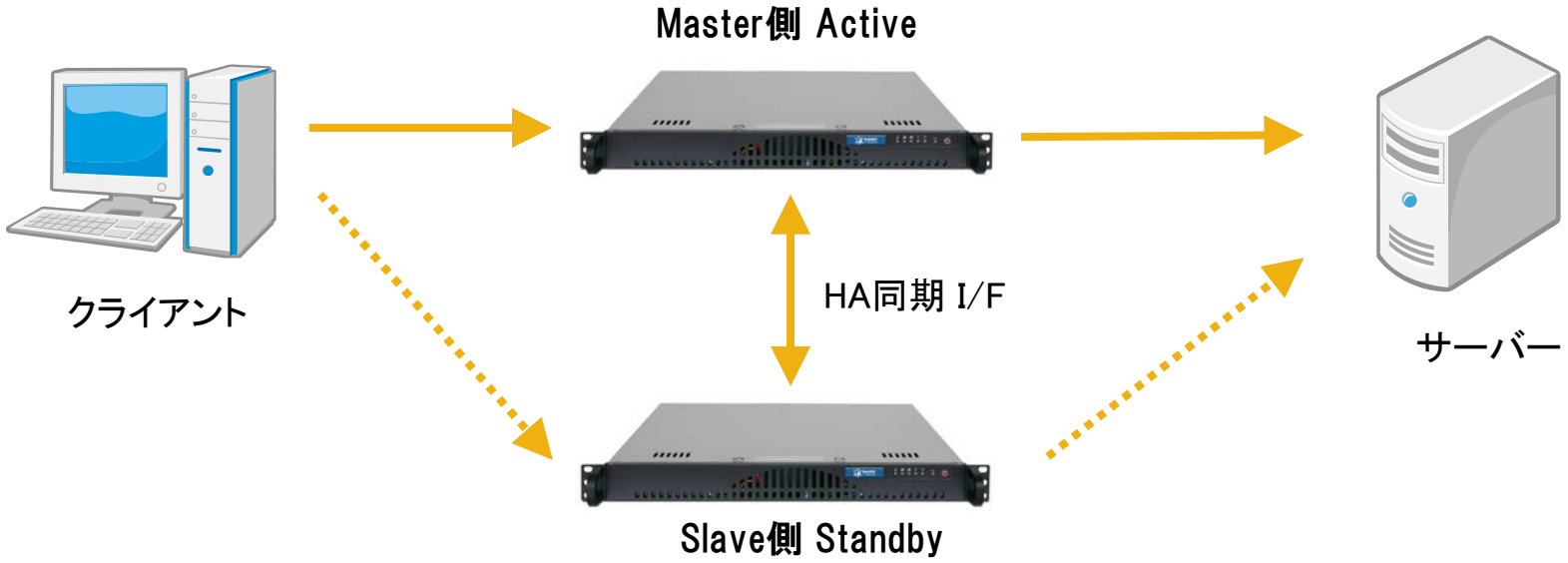
クリーンアップ（指定日数より古いデータを削除）

- 内蔵データを最新状態に保持します。

機能) HA構成（高可用性構成）

BalaBit SCB 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形式となります。
- Masterノードの設定、保存したすべてのデータが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。



機能）HA構成（故障時）

BalaBit SCB 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BalaBit SCB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。

機能) 統合・連携

BALABIT
CONTEXTUAL SECURITY INTELLIGENCE

- WebAPI

  SCB RPC API、SCB REST API

- プラグインフレームワーク

  AA（Authentication and Authorization）、チケットシステム

- 認証サービス

  LDAP（Active Directory）、RADIUS

- SIEM（Security Information and Event Management）

  ArcSight、Splunk

お問い合わせ

ジュピターテクノロジー株式会社
（Jupiter Technology Corp.）
住所 〒183-0023　東京都府中市宮町2-15-13
第15三ツ木ビル8F
URL http://www.jtc-i.co.jp/

製品に関するお問合せ
Tel 042-358-1250
Fax 042-360-0221
Email info@jtc-i.co.jp