BALABIT
CONTEXTUAL SECURITY INTELLIGENCE

Shell Control Box 5 LTS

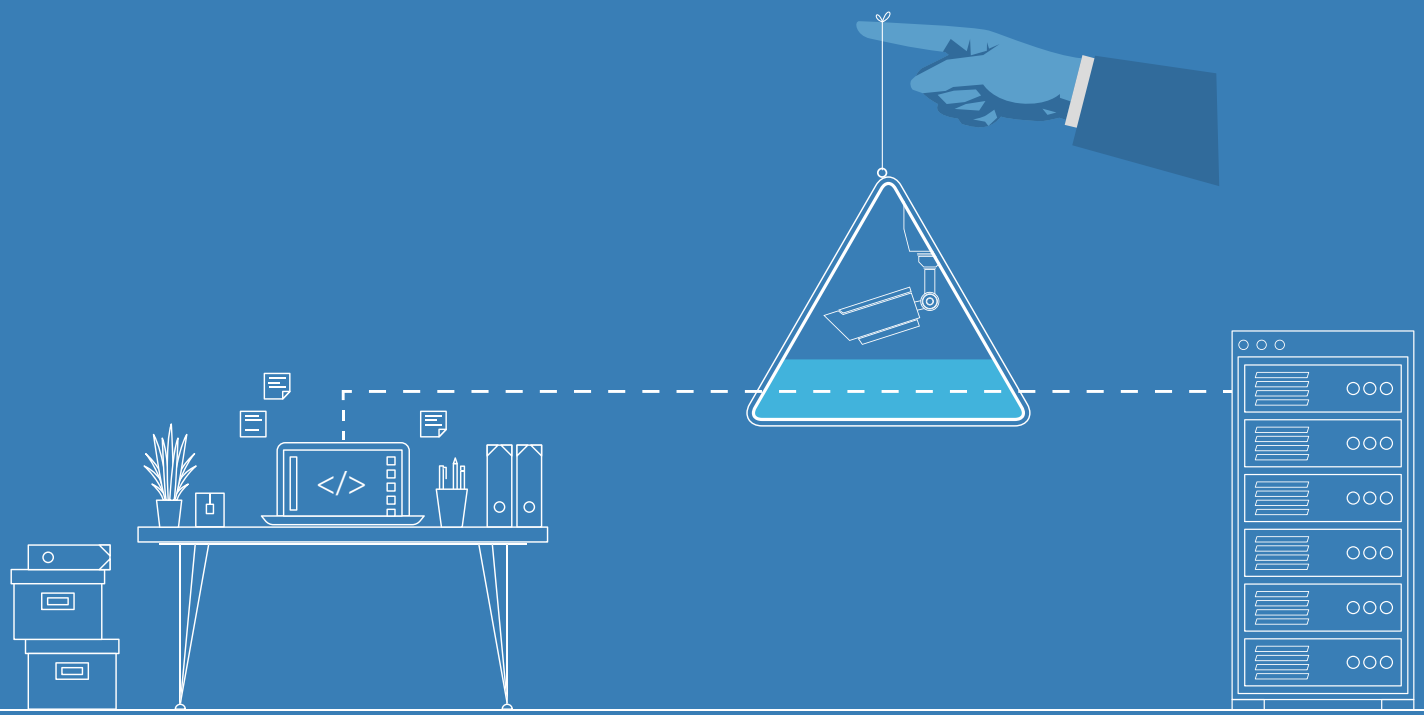
PRODUCT DESCRIPTION

2017年7月21日

JTC-i Jupiter Technology corp. ジュピターテクノロジー

イントロダクション

独立した透過的な
ユーザー監視

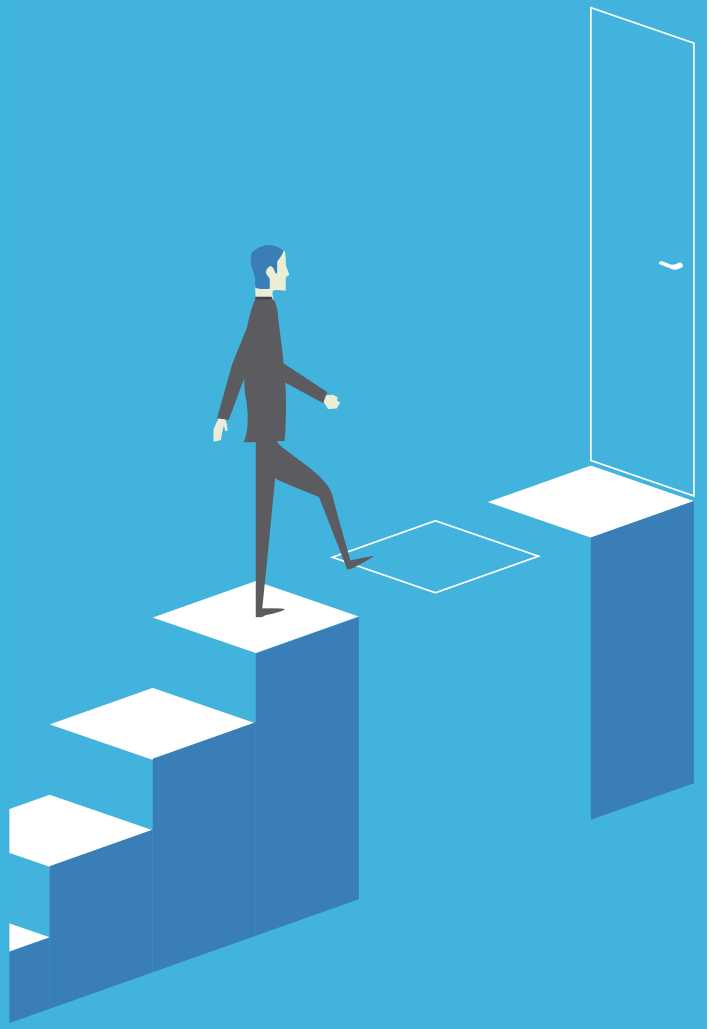


Shell Control Box (SCB) は、リモートサーバー、仮想デスクトップ、ネットワークデバイスへのアクセスを管理し、これらのシステムにアクセスするユーザーのアクティビティを記録する、ターンキーアクティビティ監視アプライアンスです。例えば、システム管理者がウェブサーバーを更新したり、サードパーティー IT プロバイダーがネットワークルーターを構成する時に記録します。記録された監査証跡を映画のように再生して、イベントをまさに起こった通りに確認できます。監査証跡の内容は、イベントを検索できるようにインデックスが付けられ、自動レポートも可能です。SCB は PCI-DSS や ISO27000 のようなコンプライアンス要件が定める通りに、特権ユーザーによって引き起こされるセキュリティリスクを軽減するために特権ユーザーのアクセスを監視する場合に最適です。

SCB は、（コンフィギュレーションの変更や実行されたコマンドなどを含む）すべての管理上のトラフィックを監査証跡に記録します。すべてのデータは暗号化され、タイムスタンプと署名が付いたファイルとして保存されるので、データの修正や改ざんは一切できません。何らかの事故（サーバーの設定ミス、データベースの改ざん、予期せぬシャットダウン）が発生した場合、そのイベントの前後の状況を監査証跡ですぐに確認できるので、事故原因を簡単に特定できます。

SCB は素早く展開できる企業向けのツールです。SCB は外部設置タイプの透過的なデバイスで、クライアントとサーバーからは完全に独立しています。SCB のために、サーバーやクライアントのアプリケーションを修正する必要はありません：既存のネットワークにシームレスに統合できます。

応用分野と
代表的なエンドユーザー



コンプライアンス

複数の産業において、コンプライアンスはますます重要になっています。法律、規制、工業規格によって、より高いセキュリティ意識と顧客情報の保護を求められています。PCI-DSS (Payment Card Industry –Data Security Standard),ISO27001,GDRP などの法律は、すべて機密情報の厳格な保護を義務付けています。ログ収集システムに取りこぼしがあると、インシデントが発生した場合、多くの疑問点が残ることになります。従って、企業はコンプライアンスを遵守するために、特権ユーザーのアクションを監査し、レポートする、信頼できるソリューションを見つける必要があります。

機密データの保護

多くの企業が支払い情報、支払取引データ、個人の財務情報などの個人情報を管理し、保存しています。これらのデータへのユーザーアクセスは、ログに記録され、数年間は保存されるべきです。不正なアクセスやデータの漏洩が発生した場合、企業の評判は大きく損なわれることになります。SCB は企業の機密データを扱うシステムを、未確認の侵入者や不正なユーザーから完全に隔離します。さらに、機密データへの承認されたアクセスをすべて記録し、ヒューマンエラーや異常な挙動が発生した際に、実用的な情報を提供します。

VDI ユーザーの監査

仮想デスクトップインフラを実装する企業は益々増え、それに伴い、ユーザーがローカルマシンから作業を行う際、使用されるアプリケーション、プロセス、データはすべてサーバーに保存され、一元的に実行されます。しかし、これらのターミナルサーバーで実行されている数え切れないほど多くのビジネスアプリケーションについて、十分なログ記録を行うことは不可能です。その結果、数百または数千のシンクライアントユーザーのアクティビティを管理することはほとんど不可能です。SCB は、主要な VDI アプリケーション（例えば CITRIX XenDesktop, RD Session Host など）で使用されているプロトコルの監査を行うことができ、使用されているアプリケーションのユーザーのすべてのアクティビティを独立して監視し、記録できます。

内部 IT スタッフの監視

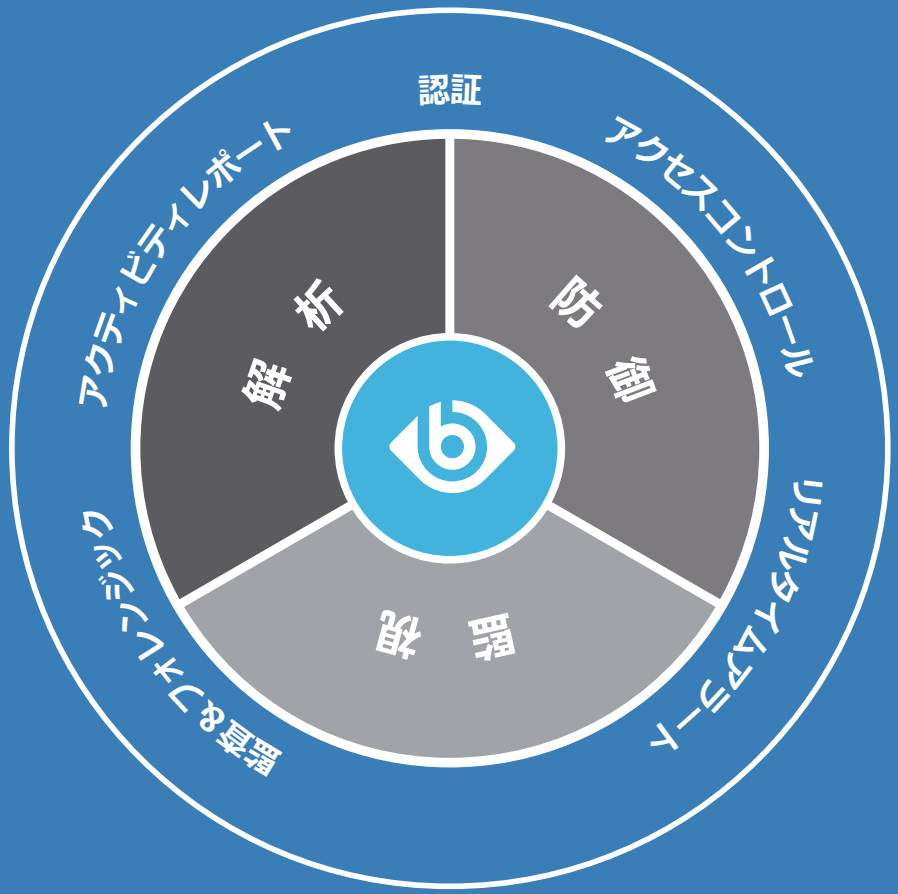
システム管理者は IT 環境において最も権力のあるユーザーです。組織階層で底辺に位置していても、オペレーティングシステム、データベース、アプリケーションにアクセスする権利を高度にもしくは無制限に有しています。サーバーにおけるスーパーユーザーの特権で管理者は企業の機密システムに直接アクセスし、操作することができ、システムに偶然に（もしくは故意に）甚大な損害を与えることができます。システム管理者はしばしば特権アカウントのパスワードを共有していますが、これはセキュリティポリシー違反です。加えて、動作を誤魔化す機会があります。その結果、「誰が何をしたか？」との質問に答えることはほぼ不可能であり、インシデントを調査する際に時間とお金を無駄にしているという非難に繋がることも多くあります。

IT 外部委託事業者の管理

グローバル経済において、IT 機能はクラウドやホスティングサービスのプロバイダーといった請負先に外部委託することが多くあります。IT プロバイダーに責任を与えることはいつもリスクを含みます。注目を浴びるようなデータ侵害は請負先が使用している特権アカウントを活用していることが多くあるからです。契約上の義務がありますが、サービス品質保証（SLA = Service Level Agreement）で外部事業者の従業員を監視することは実際できません。IT SLAs の正当性を確認し、代金を払う価値のある業務であることを証明できる、信頼に足る使い易いソリューションはほとんどありません。対応時間のような重要業績評価指標（KPI = Key Performance Indicators ）を測定したり、外部管理者のアクセスを制限したりすることも、重要な課題です。外部事業者のアクセスを監視することが必要不可欠である理由がここにあります。外部委託業者が企業のシステムに接続している際に何を行っているかを知る必要があるのです。

導入企業例

TELCO	IT	FINANCE	OTHER INDUSTRIES
T-Mobile	Adobe	KMF	CEZ GROUP
orange	Solvinity. This is IT	BAI TUSHUM BANK	e·on
MedNautilus TELECOM ITALIA SPARKLE GROUP	lrz	Handelsbanken	REPUBLIQUE ET CANTON DE GENEVE
MTS	NICE	NBK	HÉMA-QUÉBEC
Bouygues Telecom	FIDUCIA Ihr IT-Partner	EMPH	ACCOR HOTELS Feel Welcome
cyta	GoodData	CENTRAL BANK OF THE REPUBLIC OF AZERBAIJAN	MNT
etisalat		Tinkoff Bank	EADS
		merkantilbank	DOCAPOST
		Dubai Islamic Bank	ANKARA UNIVERSITY
		alBaraka	PADDYPOWER. betfair

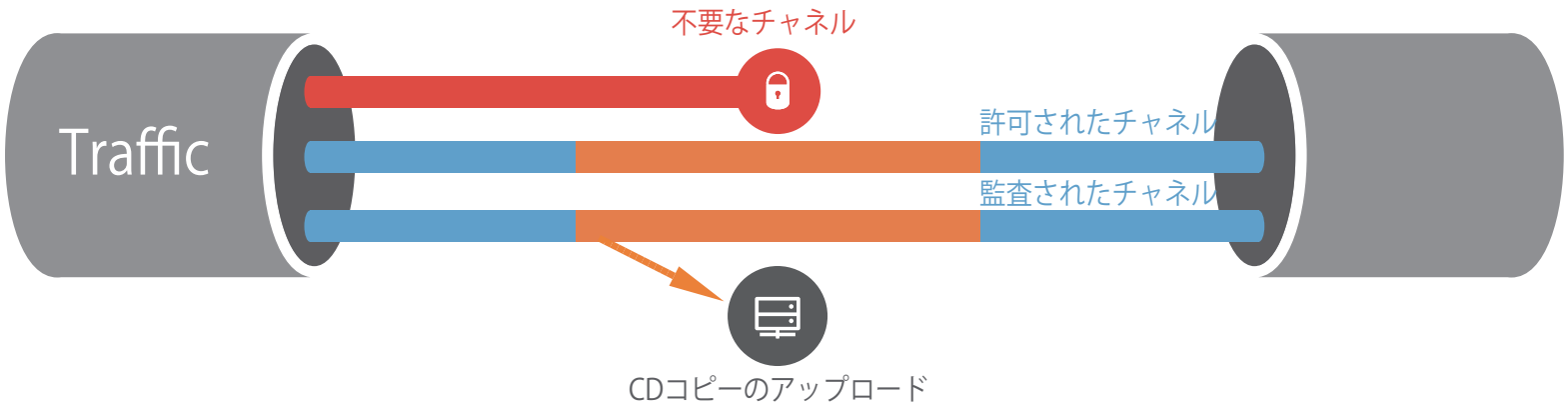


製品の機能とベネフィット

- サーバーとクライアントから独立しており、侵害されにくい
- 透過的な運用で既存のインフラと簡単に統合可能
- SSH, RDP, HTTP(s), Citrix ICA, VNC, Telnet など、管理者が広く利用しているすべてのプロトコルを管理
- サーバーとネットワーク機器への詳細なアクセス制御
- リモートシステムとデータアクセスの 4 –eyes 認証
- 危険なアクションをリアルタイムで防止
- SCP と SFTP 接続監査、ファイル操作をリスト化、転送ファイルの抽出
- フォレンジック調査のために改ざんできない情報を収集
- 記録したセッションの動画再生
- 素早いトラブルシューティングのためのフリーテキスト検索
- コンプライアンスのためのアクティビティカスタムレポート
- 簡単な Web ベースの管理
- ハイアベイラビリティオプション
- 自動データアーカイブとバックアップ

包括的なプロトコル検査

SCB は、アプリケーションレベルのプロキシゲートウェイとして動作します。接続とトラフィックはアプリケーションレベ ル（OSI モデルのレイヤ 7）を調査し、プロトコル違反の全てのトラフィックを拒否します。これは攻撃に対する効果的なシー ルドになります。トラフィックについてのこの高レベルな理解により、SSH 接続で使用する認証方式と暗号化方式、または RDP トラフィッ クで許可されたチャネルのように、プロトコルのさまざまな機能をコントロールできます。



広範なプロトコルをカバー

- Unix ベースのサーバーやネットワークデバイスにアクセスするために使用されるセキュアシェル（SSH）プロトコル（バージョン 2）
- Windows 2012R2 と Windows 10 を含む Microsoft Windows プラットフォームにアクセスするために使用されるリモートデスクトッププロトコル（RDP）のバージョン 5、6、7
- さまざまなデバイスやアプリケーションの Web インターフェー スへの管理アクセスのために使用される HTTP/ HTTPS プロトコル。例えば、ルータ、ファイアーウォール、アプライアンス、Web サービスなど
- Unix のようなシステムのグラフィカルインターフェースにリモートアクセスするために使用される SSH でフォワードされる X11 プロトコル
- ネットワークデバイス（スイッチ、ルータ）で使用される Telnet プロトコルと、レガシー UNIX システムや IBM メインフレームアクセスに使用される TN3270/TN5250 プロトコル。Telnet と TN3270 では TLS または SSL 暗号化もサポートされます
- マルチプラットフォーム環境でのリモートグラフィカルアクセスに使用される仮想ネットワークコンピューティング（VNC）グラフィカルデスクトップ。VNC の TLS または SSL 暗号化も サポートされています
- リモート仮想デスクトップにアクセスするために使用される VMware View アプリケーション（現在は RDP ディスプレイプロトコルを使用した直接接続のみがサポートされています）
- シトリックスシステムズが設計した仮想デスクトップおよびアプリケーションサーバーインフラストラクチャにアクセスするための Citrix の ICA プロトコル（SCB は XenDesktop および XenApp7.x に対して Citrix Ready と認定されています）。Common Gateway Protocol(CGP) として知られている信頼性 の高い接続もサポートされています
- SCB がターミナルサービスゲートウェイ（また、TS ゲートウェイまたはリモートデスクトップゲートウェイとも呼ばれています）として機能できるように、ターミナルサービスゲートウェイサーバープロトコルがサポートされています

アクセス制御の詳細

SCB ではユーザーが接続を定義することができます： リストに登録されたクライアント IP アドレスからのみサーバーにアクセスできます。これは、様々な接続のパラメーターを制限することによって、絞り込むことができます。例えば、サーバーに接続できる時間、ユーザー名および SSH で使用する認証方式、または SSH または RDP の接続で許可されたさまざまなチャネルのタイプを絞り込みます。認証を制御することは、SCB が強力な認証方式（パブリックキー）の使用を強制し、また、ユーザーのパブリックキーを 検証できることを意味します。SCB は SSH のホストキーとサーバーを識別する証明書を検証する組込み機能を有しており、man-in-the-middle 攻撃や他の操作を防止できます。また、SCB は、外部のユーザーディレクトリでユーザーを認証することができます。この認証は、ユーザーがリモートサーバー上で行う認証とは完全に独立しています。

SCB はローカルクレデンシャル•ストアをサポートしています。ローカルクレデンシャル•ストアは、ユーザーが認証情報（パスワード、プライベートキー、証明書等）にアクセスすることなくユーザー認証情報を格納する方法を提供し、ターゲットサーバーにログインできるようにします。このようにすることで、ユーザーは通常のパスワード（SCB 上のローカルまたは中央 の LDAP データベースに格納された）を使用して、SCB で認証するだけになります。ユーザーがターゲットサーバーへのアクセスを許可された場合、SCB は自動的に認証情報ストアからのデータを使用してログインします。

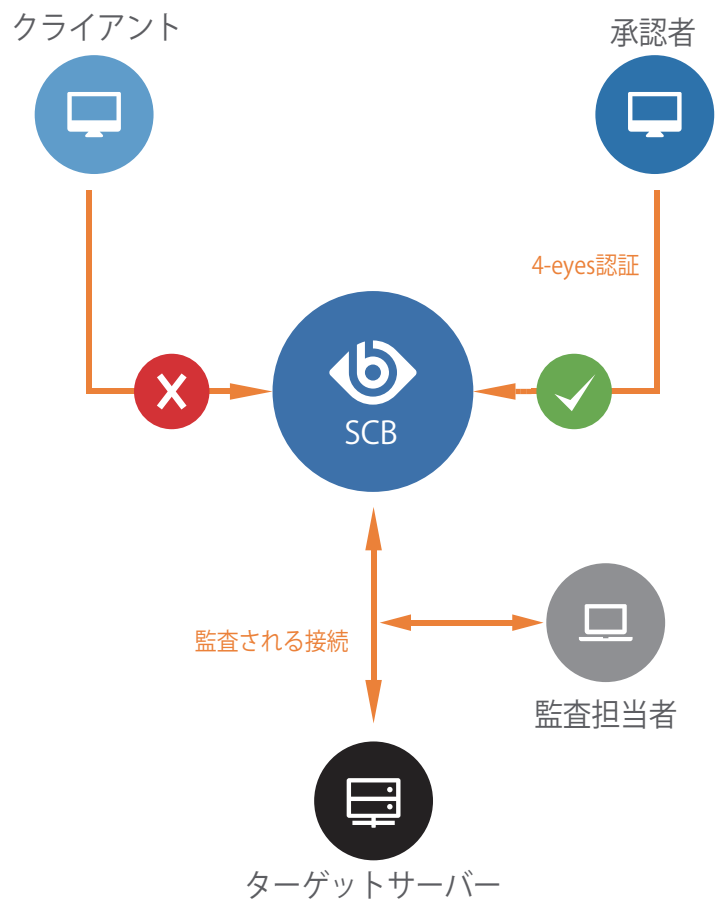
以下のパラメーターをコントロールできます：

- SSH 、Telnet またはネットワーク層認証の RDP 6 を使用する場合、サーバーへのアクセスを管理者グループに許可します（ユーザー名ブラックおよびホワイトリストまたは LDAP グループに基づく）
- リモートサーバー上で行われる認証に加えて、SCB Web インターフェースで追加の帯域外認証を要求することも可能です。同様に、この帯域外認証に基づいて許可を行うことが可能
- サーバーへのアクセスを許可されたクライアントマシンの IP アドレス
- SSH を使用してサーバーにアクセスするために必要な認証方式（パスワード、公開キー、証明書等）
- サーバーにアクセスすることができる時間（労働時間中のみなど）
- サーバーに許可されている SSH または RDP チャネルタイプ（SSH ターミナルやポートフォワード、RDP ファイル共有、など）

上記のルールは、接続レベルとチャネルレベルの両方に適用することができます。特殊チャネルへのアクセス方法は、より小さな管理者グループ（本当にそれを必要とする人のみ）に制限することができます。

4-eyes 認証

設定ミスやその他のヒューマンエラーを回避するため、SCB は 4-eyes 認証の原則をサポートしています。4-eyes 認証では、管理者はサーバーへのアクセス権を承認者に要求します。
承認者は管理者の作業を、同じ画面を見ているかのように、リアルタイムに監視できます。



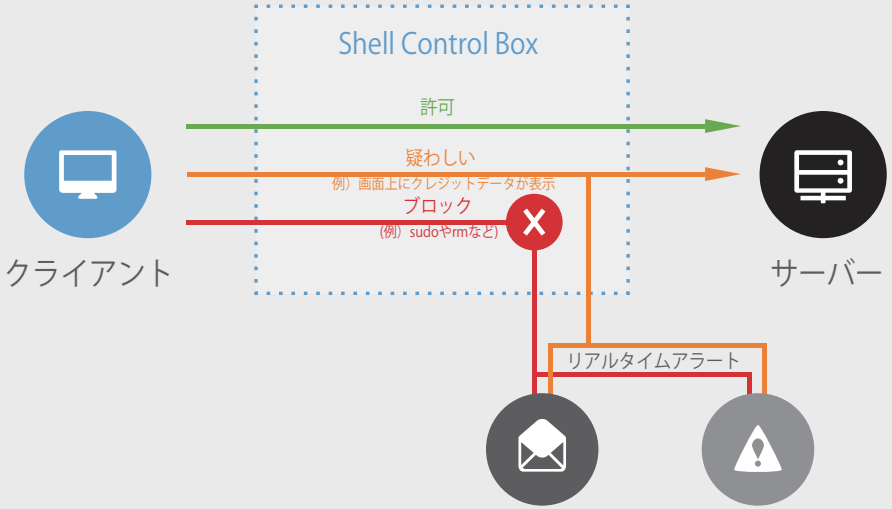
4-eyes 原則は、同様に監査担当者にも適用することができます。SCB は監査証跡を暗号化するために、複数のキーを使用することができます。この場合、監査証跡を再生するために複数の復号キーが必要なので、監査担当者一人のキーだけではネットワーク・システムに関するすべての情報にアクセスすることはできません。

リアルタイムのアラートとブロック

SCB は SSH や Telnet、RDP、ICA と VNC 接続のトラフィックをリアルタイムで監視し、特定のパターンがコマンドラインまたは画面に表示された場合に様々なアクションを実行することができます。事前定義されたパターンとは、例えば危険なコマンドまたはテキスト中心プロトコル中のテキスト、グラフィカルな接続中の不審なウィンドウタイトルです。この機能は悪質なユーザー操作を記録や報告するのではなく、その場でブロックします。例えば SCB は「削除」コマンド等の破壊的な管理者コマンドの実行前に接続をブロックすることができます。さらに SCB は、クレジットカード番号のような数字を検出することができます。検索するパターンは正規表現として定義することができます。

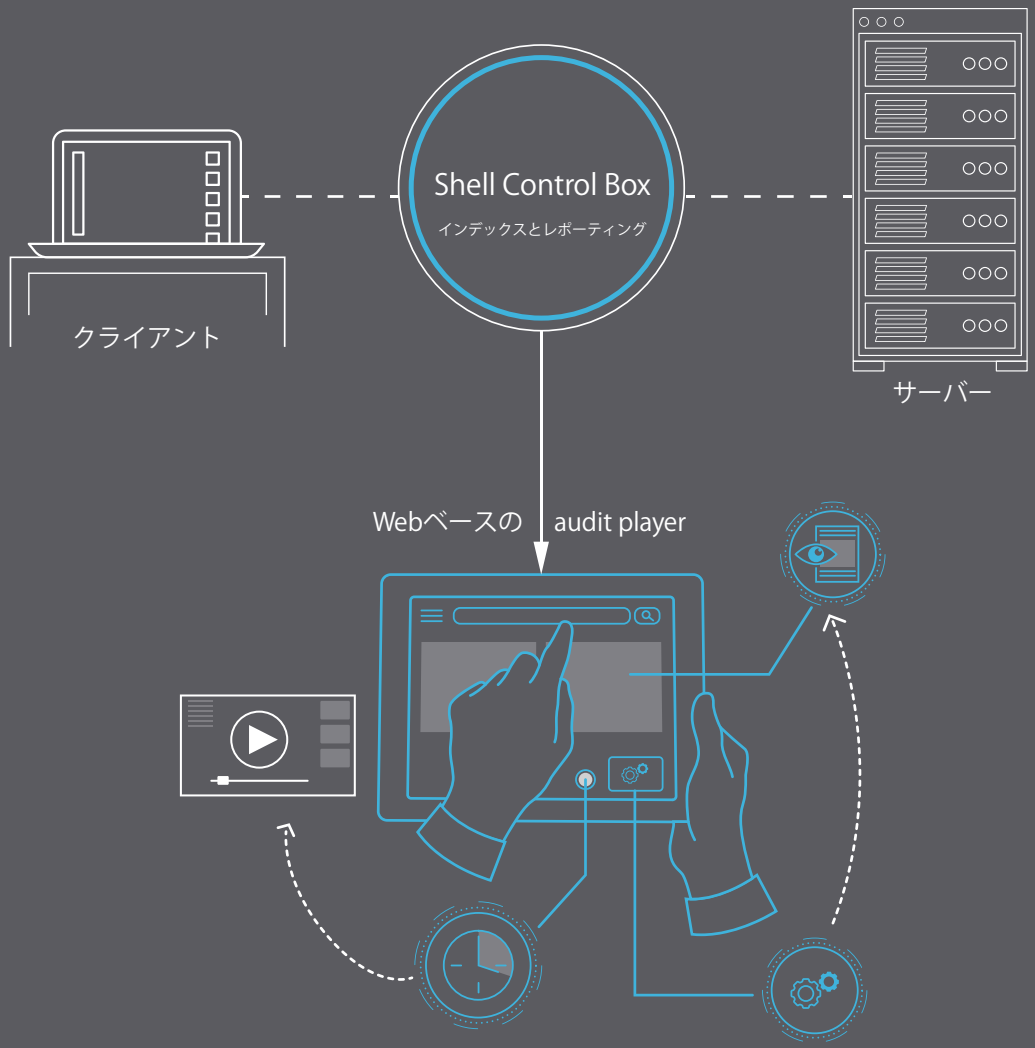
不審なユーザーアクションを検出した場合、SCB は以下のような対策を実行することができます。

- A: システムログにイベントを記録
- B: すぐに接続を終了
- C: 電子メールの送信や SNMP アラート通知
- D: SCB の接続データベースにイベントを保存



SCB によるリアルタイムアラートとブロック

映画のような再生と フリーテキスト検索



SCB は検索可能な監査証跡にすべてのセッションを記録し、法廷で使用できる捜査情報の発見を容易にします。監査証跡はオンラインで閲覧したり、特権ユーザーのアクティビティを監視するためにリアルタイムで追跡することができます。SCB とアーカイブサーバーに保存されているすべての監査証跡は SCB の Web インターフェースからアクセスできます。Web ベースの Audit Data Player アプリケーションはちょうど映画のように記録されたセッションを再生します - 管理者のすべてのアクションはモニターに表示されたものと同じように、正確に見ることができます。監査証跡は内部、または任意で外部のインデックス付けサービスによってインデックスが付けられます。このことによって SCB の Web GUI 上で結果が検索可能になります。改良された検索機能でインシデント発生後の解析が容易になりました。監査担当者が詳細な検索結果にアクセスすることができます。例えば、検索式を含む正確なタイムスタンプやスクリーンショットに一致する検索結果にアクセスできます。フルテキスト検索機能は適合順に並べられた検索結果や多くの強力なクエリタイプを提供し、また非ラテン文字をサポートします。

Audit Data Player では再生中の早送り、イベント（例えばマウスクリック、Enter キーを押すとき）の検索、テキストの検索ができます。マルチプラットフォーム監査再生アプリケーション（Balabit Desktop Player）も調査と監査をさらに便利にすることができます。また、多数の監査証跡の検索を実行して、特定の情報やイベントを含むセッションを見つけることもできます。また SCB は新しい監査証跡で自動的に検索を実行し、レポートを生成します。それに加えて SCB は検索結果に基づいてユーザーが作成した表やグラフを含む統計、監査証跡の内容やおよびその他のカスタマイズ可能なコンテンツを含むレポートを作成します。SCB のコンプライアンスステータスでレポートを作成することができ、PCI DSS の規制を遵守する手助けになります。

ファイル転送閲覧

検査プロトコルの監査証跡の記録に加えて、組み込みのプロトコル（例えば、SSH でトンネルされた他のプロトコル、ポートフォワード）と転送されたファイルも同様に記録することができます。SCP や SFTP 接続から記録されたファイルを更なる分析のために抽出することができます。外部ツールでの解析のために監査トラフィックをパケットキャプチャ（PCAP）形式に変換することすら可能です。

監査証跡は圧縮されており、アイドル状態の接続はディスクスペースを消費しません。

信頼性の高い監査

監査は通常、監査対象サーバーで生成されたログに基づいています。インタラクティブイベントのログでは通常、詳細な監査情報まで得られないという難点があり、サーバーに保存されているまたはサーバーから送信されたログが管理者または攻撃者によって操作されていないことを確認する方法はありません。しかし、SCB はユーザーに透過的な独立したデバイスであり、クライアントとサーバー間の通信から直接監査情報を抽出します。また、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、監査対象の情報が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。

すべてのデータを一年以上保持

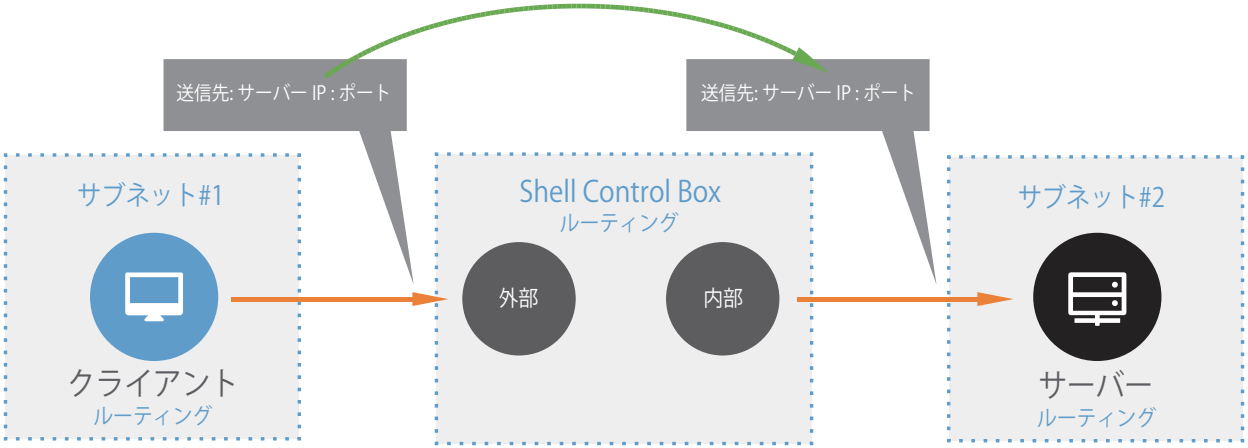
システム管理作業の大部分を占める SSH および Telnet ターミナルセッションは、監査の際の最も興味深いトラフィックタイプです。しかし、そのようなトラフィックは通常ハードディスクの容量はあまり必要ありません（環境しだいですが、だいたい 1 時間当たり 1MB くらいの容量しか占めません）。したがって SCB は、システム管理者のアクティビティを 500.000 時間近く保存することができます。
つまり、常にオンラインで作業している管理者が 50 人いる企業（7x24）では 1 年以上 SCB 上ですべての SSH および Telnet セッションを検索可能、再生可能、容易にアクセス可能な形式で保存することができます。しかし、これらは、SCB から同様にアクセス可能なリモートバックアップサーバーにアーカイブされたデータは含みません。RDP セッションではもっと多くのスペースを取ります。（ただし、通常 1 分あたり 1MB 以下）つまり、SCB は数週間分の仕事のデータを格納することができることを意味します

スムースな統合

ネットワークインフラへの統合をスムースにするために、SCB は、透過オペレーションと非透過オペレーションをサポートします。ファイアーウォール設置環境の統合を簡単なものにするために、SCB はソースおよびデスティネーションアドレス変換 (SNAT と DNAT) の両方をサポートします。

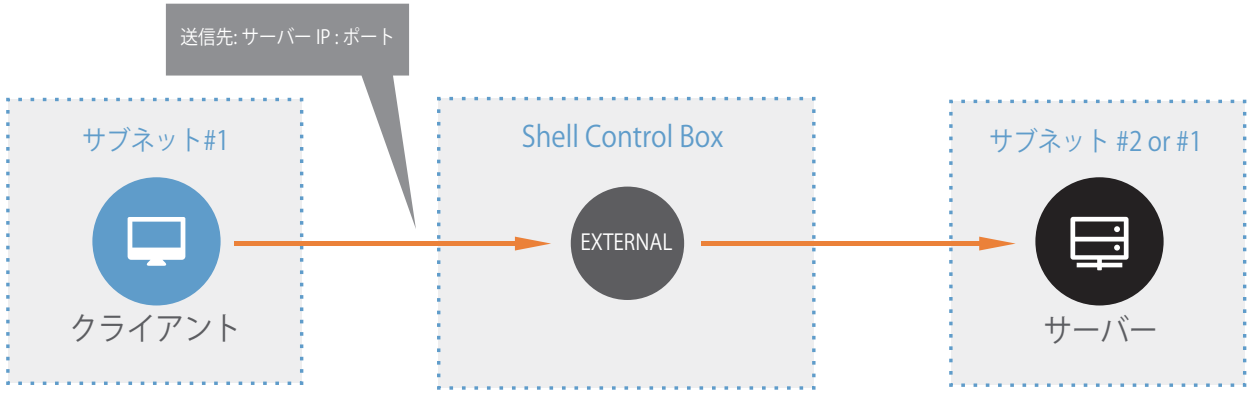
透過モード

透過モードにおいて、SCB は透過的なルータとして働き、管理者のネットワークセグメントを保護されたサーバーのセグメントにネットワーク層 (OSI モデルの 3 層) で接続します。



非透過モード

非透過モードにおいて、SCB はバスシオンホストとして働き、管理者は SCB だけにアクセスできます。管理サーバーには直接アクセスできません。SCB から始まる接続だけが、サーバーにアクセスできるように、ネットワークのファイアーウォールは、サーバー接続は SCB からの要求だけを許可するように設定しなければなりません。SCB は、接続 (管理者の IP アドレス、ターゲット IP、およびポート) パラメーターに基づいて、どのサーバーに接続するか決めます。



ネットワーク構成を柔軟にするために、SCB は仮想ネットワーク（VLAN）をサポートしています。VLAN 環境では透過オペレーションと非透過オペレーションがマージされます：SCB は非透過（バスシオンモード）と透過（ルータモード）を同時に管理することができます。

ユーザーディレクトリの統合

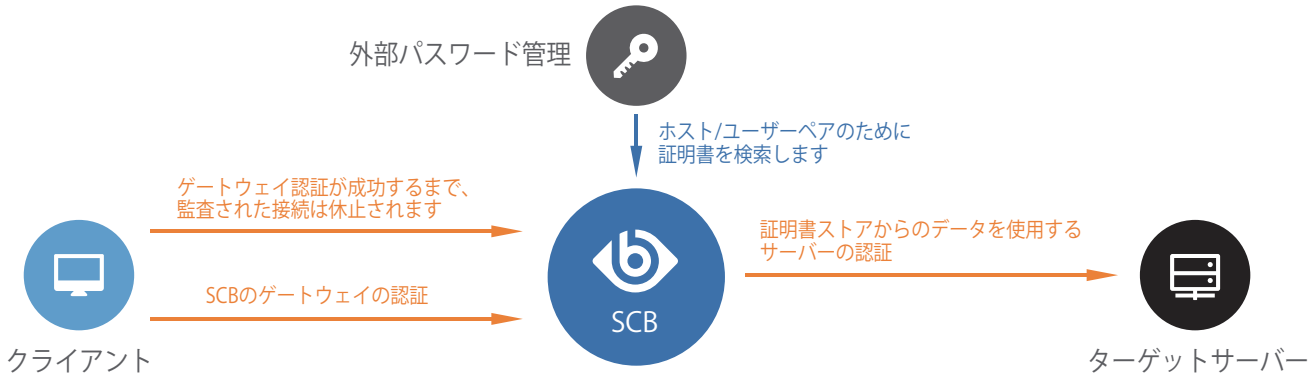
SCB は、リモート LDAP データベースに接続することができます (例えばマイクロソフト・アクティブ・ディレクトリ・サーバー)。それにより、保護されたサーバーにアクセスするユーザーのグループ・メンバーシップを解決することができます。ルールとポリシーはグループのメンバーシップに基づいて定義することができます。SSH で公開鍵認証を使用する場合、SCB は LDAP データベースに格納されたキーまたは X509 証明書に対応するユーザーを認証することができます。

SCB の Web インターフェースにアクセスする管理者も監査者も、LDAP データベースから認証することができます。RADIUS 認証 (例えば、SecurID を使用して) を使って、Web インターフェースアクセス、および SSH 監査セッションの認証ができます。

SCB には柔軟なプラグインフレームワークが含まれていて、SCB の監視対象と接続するために外部のサードパーティーの認証または認証ツール (例えば、OKTA) と統合できます。プラグインはユーザーまたは外部のシステム (例えば、LDAP または Active Directory) から追加の認証情報を要求することで多要素認証をサポートしていて、この情報に基づいて接続を許可または拒否します。

特権 ID 管理ソリューションの統合

ローカルの資格情報を格納することに加えて、SCB は Lieberman 社のエンタープライズランダムパスワードマネージャ（ERPM）と Thycotic 社の Secret Server パスワード管理ソリューションに完璧に統合することができます。このように、上記のパスワード・マネージャーを使用して、目標サーバーのパスワードを中央管理します。一方で SCB は、保護されたサーバーが SCB だけを通してアクセスするのを確実にします。ユーザーがダイレクトなアクセスのために必要なパスワードを知らないためです。



ERPM 統合のみならず、SCB は、汎用アプリケーション・プログラミングインターフェース (API) を提供して、さらなるパスワード管理システムとの統合を可能にします。

Blindspotter の統合

SCB は Balabit のリアルタイムでのユーザー行動分析ソリューションである Blindspotter の運用をサポートしています。Blindspotter はヒューマンリスクを明らかにするためにユーザー行動をマッピングしてプロファイリングする監視ツールで、SCB が記録した監査証跡から取得したデータを使ってユーザー行動を分析できます。

パブリッククラウドでの展開

Microsoft Azure Marketplace から BYOL モデルで SCB を展開できます。これによって仮想化されたインフラ全体のアクセスの監査を便利に行うことができます。

SIEM システムとの統合

SCB は主要な SIEM(Security Information and Event Management) システムである HP ArcSight、Splunk と統合できます。SCB は両方のベンダの市場で利用でき、特権ユーザーアクセスに関する詳細かつ質のいいデータを送信することで、レポートとアラートの機能を向上させることができます。

チケットシステムとの統合

SCBは､プラグインフレームワークの提供で､フレームワークを外部ヘルプデスク（または問題追跡）チケッティング・システムに統合します。これにより対象サーバー上で認証する前にチケット ID を要求することが可能になります。このように SCB は、ユーザーがサーバーにアクセスする正当な理由を持っていることを確認することができます。また、ユーザーが正当な理由を持っていない場合は、任意に接続を終了することができます。チケット ID リクエストは現在次のプロトコルをサポートしています： SSH、RDP、TELNET および TN3270。

サードパーティアプリケーションへの統合

SOAP ベースの RPC API により、リモートアプリケーションから SCB にアクセス、検索、管理することができます。さらに、リモート API(RPC API) に基づいた Web サービスを SCB で管理し統合することができます。RESTful API を使って SCB にアクセスすることもできます。API による SCB へのアクセスには以下の長所があります：

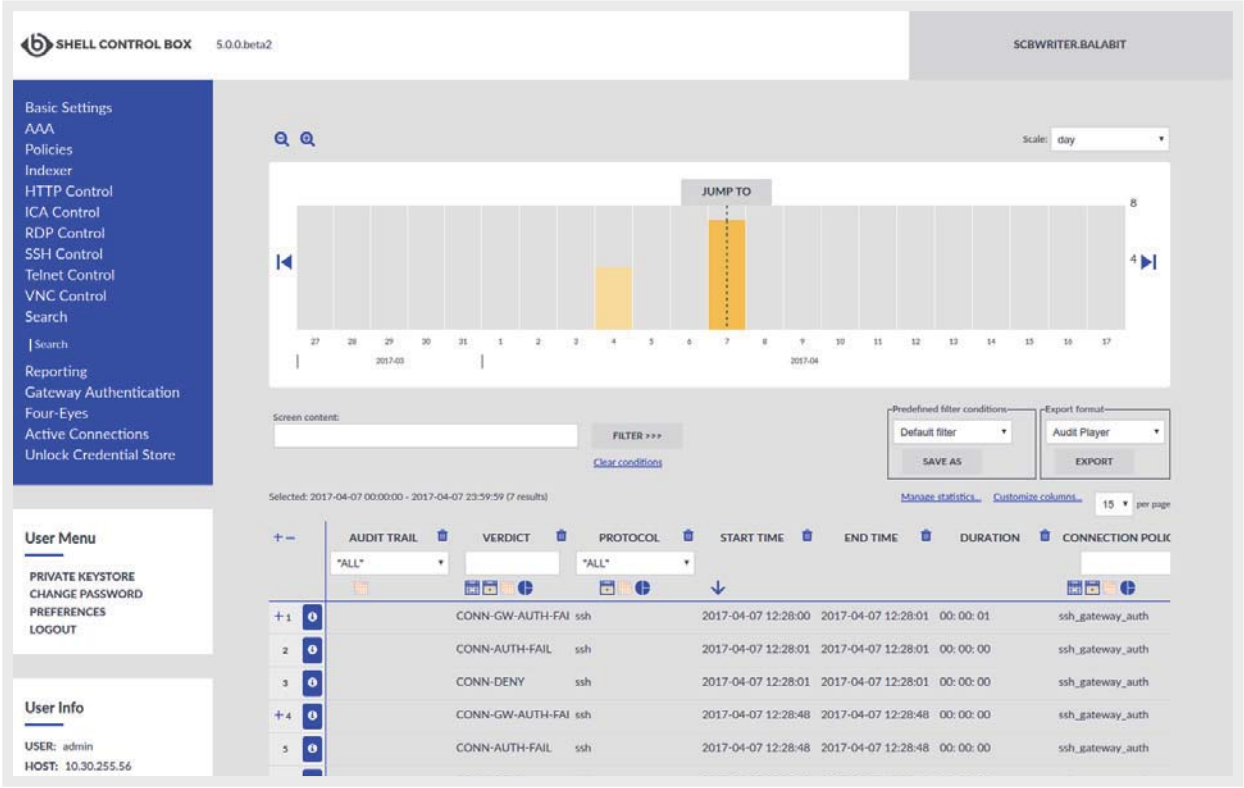
1. カスタムアプリケーションおよび環境 (例えばヘルプデスクのチケットシステム) への統合
2. 外部のアプリケーション (例えば SIEM ツール) からの接続データ､SCB イベント、アラートの検索
3. SSH キーマネジメントシステムとの統合
4. サードパーティシステム管理マネジメントアプリケーションからの SCB の設定

シンプルな管理

SCB はきれいで直観的な Web インターフェースで設定できます。各 SCB 管理者の役割は明確に以下の特権セットで、定義することができます：

- ホストとして SCB を管理する；
- サーバーへの接続を管理する；
- 監査証跡およびレポートなどを見る

SCB Web インターフェースへのアクセスは、管理トラフィック専用の物理的分離したネットワークに制限することができます。この管理インターフェースは、バックアップや、リモートサーバーへのログ、他の管理上のトラフィックにも使用されます。Web インターフェースにアクセスするユーザーは、LDAP あるいは RADIUS データベースで認証できます。Web インターフェースにアクセスするユーザーは、X.509 証明書による強固な認証を要求できます。すべての設定変更は自動的に記録されます。管理者が SCB の設定を変更する場合に、SCB はコメントを追加することを要求できます。SCB は設定変更レポートを作成します。また、修正の詳細および記述は Web インターフェースから閲覧と検索可能なため、SCB の監査が単純化されます。



高可用性

SCB は高可用性 (HA) 構成も、利用可能です。この場合、同一構成の 2 台の SCB ユニット (マスターとスレイブ) は、同時に動作します。2 台のユニットは共用ファイル・サブシステムを持っています。データを受信するとすぐに、マスターはスレイブノードとデータを共有します。すべての設定変更あるいは記録したトラフィックは、スレイブノードとすぐに同期されます。マスタユニットが機能を止めると、スレイブユニットは直ちにアクティブになります。したがって、保護されたサーバーに継続してアクセスすることができます。SCB-T4 とそれ以上の製品は二重電源ユニットを装備しています。

ソフトウェアのアップグレード

ソフトウェアのアップグレードはファームウェア・イメージとして提供されます。SCB Web インターフェースを使用しての、SCB のアップグレードはネットワークルーターのアップグレードと同じくらい簡単です。SCB は 5 世代のファームウェア・バージョンを保存するので、何らかの問題が発生した場合には簡単にロールバックできます。

自動データアーカイブ

記録された監査証跡は、リモートサーバーまたはストレージに自動的にアーカイブされます。リモートサーバー上のデータはアクセス可能で、検索できます。数テラバイトの監査証跡は SCB Web インターフェースからアクセスすることができます。SCB は、ネットワーク・ファイル・システム (NFS) あるいはサーバー・メッセージ・ブロック (SMB/CIFS) プロトコルを経由したネットワーク・ドライブとしてリモートサーバーを使用します。

サポートと保証

SCB のサポートとソフトウェアサブスクリプションは様々なパッケージを年単位で購入することができます。7x24 サポートおよびオンサイトのハードウェアのリプレースを含みます（日本では未対応）。詳細はジュピターテクノロジー株式会社までお問合せください。

ハードウェア仕様書

SCB アプライアンスは高速、高効率、高信頼サーバー上に構築されており、標準ラックに簡単にマウントできます。

T1

BALABIT SHELL CONTROL BOX T1

- 1xQuadCore CPU、8GB の RAM、1TB の HDD。- ソフトウェア RAID。
- 監査 10 サーバーのソフトウェアライセンス (500 サーバーまでアップグレード可能)

T4

BALABIT SHELL CONTROL BOX T4

- 1xQuadCoreCPU、8GB の RAM、冗長電源、4TB の HDD。- ハードウェア RAID
- 監査 10 サーバーのソフトウェアライセンス (5000 サーバーまでアップグレード可能)

T10

BALABIT SHELL CONTROL BOX T10

- 2x6 コア CPU、32GB の RAM、冗長電源、10TB の HDD。- ハードウェア RAID
- 監査 100 サーバーのソフトウェアライセンス (10000 サーバーまでアップグレード可能)

VA

BALABIT SHELL CONTROL BOX VA

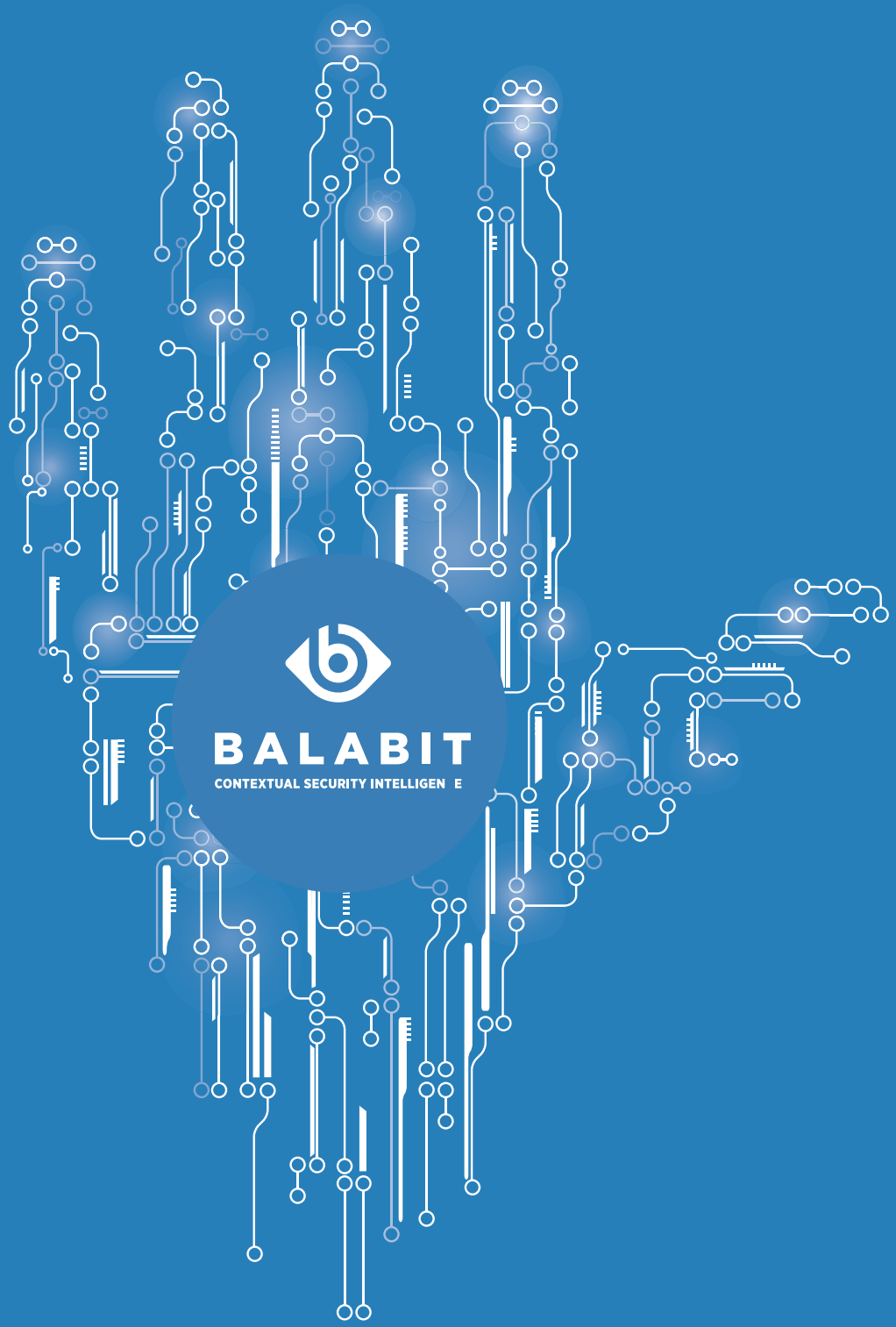
- VMware ESXi あるいは Microsoft Hyper-V あるいは Microsoft Azure の下で動作するバーチャル・アプライアンス
- 監査 10 サーバーのソフトウェアライセンス (10000 サーバーまでアップグレード可能)

無償評価版

SCB のフル機能評価版は、VMware イメージとして利用可能です。SCB をテストするためには評価バージョンを https://www.jtc-i.co.jp/contact/scontact.php でリクエストしてください。

詳細について

BalaBit 製品に関してよりよく知るためには、以下のリンクをご覧ください :
Shell Control Box 製品ページ :
https://www.jtc-i.co.jp/product/scb/scb.html
Syslog-ng Store Box 製品ページ :
https://www.jtc-i.co.jp/product/ssb/ssb.html
製品マニュアル、ガイド、他のドキュメント :
https://www.jtc-i.co.jp/support/documents/scbdoc.html
評価版リクエスト :
https://www.jtc-i.co.jp/contact/scontact.php



Balabit 社について

Balabit 社は、ハンガリーのブダペストに設立された国際的な IT セキュリティベンダーです。Balabit 社は、ビジネスを制限することなく情報漏えいを防ぐことをミッションとする、コンテクスチュアルセキュリティ（contextual security）技術のリーディングプロバイダーです。Balabit 社は、アメリカとヨーロッパの支店やパートナーを通じてグローバルなネットワークを運用しています。

Balabit 社の Contextual Security Intelligence™ストラテジーは、ハイリスクな特権アカウントの不正使用によって発生する脅威からリアルタイムで組織を保護します。そのソリューションには、文脈豊富なデータ収集機能を持つログ管理、特権ユーザー監視、ユーザー行動分析といった信頼できるシステムとアプリケーションが含まれています。普段と違うユーザー行動を特定して潜在的な脅威を深いところまで見通すことができます。既存の管理ベースのストラテジーと併用することで、Balabit 社はビジネスの実務に新たな障壁を加えることなく、柔軟なユーザーベースのアプローチを可能にしてセキュリティを向上させます。

Balabit 社は、2000 年に設立され、世界中で Fortune100 に含まれる 23 社の顧客と 1,000,000 人以上の法人ユーザーという確固とした実績をあげています。

JTC-i ジュピターテクノロジー