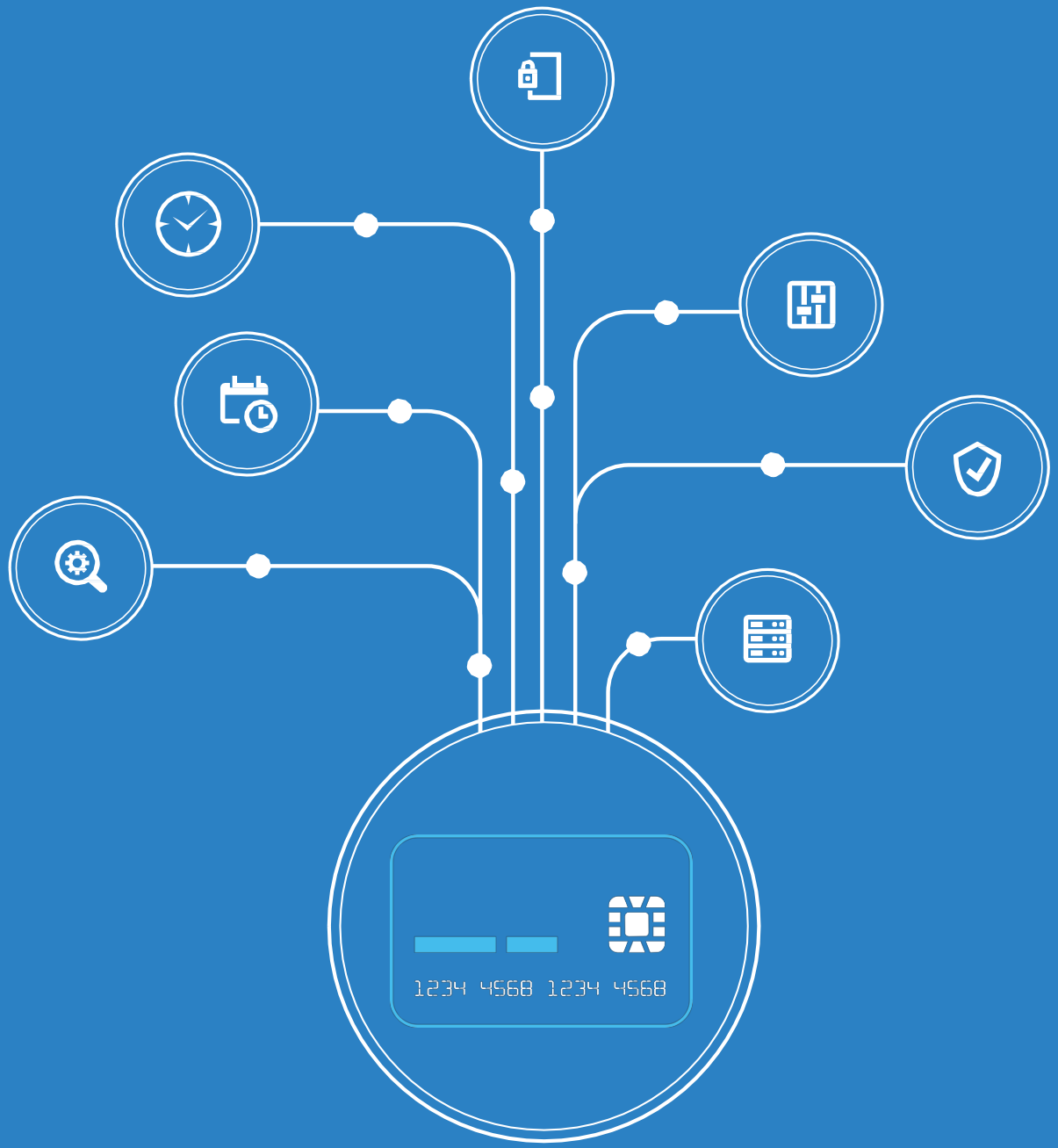

PCI DSS v3.2と BALABIT

クレジットカード会員データの保存、処理または送信等、ペイメントカードの処理に関与する組織は、クレジットカード業界（PCI）データセキュリティ基準（DSS）を実装するようにクレジットカード会社によって求められています。PCI DSSは、カード会員データを保護するように設計された技術的および運用上の要件のベースラインを提供します。この文章の内容は2016年5月に出版されたPCI-DSS3.2に基づいています。

本書の目的はBalabit社製品がPCI DSSへの対応にいかに有益かを知らせることです。

本書はリスクコンプライアンス管理者、監査人、最高情報セキュリティ責任者、その他セキュリティ管理者のようなコンプライアンスを担当するセキュリティ専門家を対象としています。

BALABIT
CONTEXTUAL SECURITY INTELLIGENCE

二つのメジャーフロントでPCI DSS コンプライアンスをサポートする

syslog-ngで安全にログデータを管理

なぜログ管理が必須の投資なのか？

ログメッセージは、ネットワーク、デバイス、およびこれらのデバイス上で動作するアプリケーションのイベントに関する重要な情報を提供します。ログメッセージはユーザーとシステムの活動を記録し、セキュリティインシデント、運用上の問題、その他、ポリシー違反等の問題の検出に使用することができるため、状況の監査とフォレンジックにおいて有用です。PCI　DSSの要件10を満たすにはログの収集、保存およびレビューが必須ですが、ログメッセージは標準の他の要件の遵守を証明するために非常に便利なツールです。

SYSLOG-NG製品ファミリー

SYSLOG-NG製品ラインは二つの製品から構成されます。ソフトウェア(syslog-ng Premium Edition)とアプライアンス（syslog-ng Sotre Box）バージョンです。二つの製品の特徴を下記に示します。

syslog-ng Premium Edition (syslog-ng PE)は企業がIT環境からログメッセージを収集、フィルタ、正規化、転送、および保存することを可能にします。syslog-ng Premium Editionを使用すると、運用の改善、セキュリティ脅威の可視化、コンプライアンス遵守のためにログ管理インフラストラクチャを一元化、また簡素化することができます。

syslog-ng Store Box (SSB)はsyslog-ng Premium Editionの強みの上に構築された高性能で信頼性の高いログ管理アプライアンスです。 syslog-ng Premium Editionの特徴の最高位にあるSSBではログデータをインデックス化し、組み込まれているGUIでの複雑な検索を遂行し、非常に細かいアクセスポリシーで機密情報を守り、コンプライアンス実証のレポートを生成し、サードパーティの分析ツールにログデータを送信することができます。

PCI DSSを満たす為syslog-ng使用の利点

ログはネットワークやセキュリティイベントの間で主要な情報源として機能を果たします。変更や喪失からログを守ることは保全性と信頼を保証するために極めて重要です。

・ディスクベースのバッファリング、クライアントサイドでのフェイルオーバーやアプリケーションレベルの応答確認のようなゼロメッセージロスポリシーで、ログは破壊や喪失することなく目的地へ到達することが保証されています。

ログの保全性はストレージと転送の間は最も攻撃されやすいです。転送の間、暗号化された回線が使用されます。一方、ストレージの間、ログは圧縮され、インデックス化され、暗号化され、電子署名化され、タイムスタンプされ、バイナリーフォーマットに変換されます。ログを権限の与えられた個人のみアクセス可能にします。

リアルタイムでの検索と報告はコンプライアンスの実証と証拠を提示するために必要不可欠です。管理されたログファイルは、SSB GUI内で整列された順序で表示されるので、より良い可視化を可能にし、監査とフォレンジックをより効果的にします。

Shell Control Boxで特権ユーザーを認証し、監視し、管理する

なぜ特権アクセス管理の識別が極めて重要なのか？

特権ユーザーはカード所有者のデータを管理・運用する能力を有するので、データの整合性を保証し、悪意のある動作が起きることを防ぐ為に監視が必要です。特権を与えられたアクセス管理は、重要なシステムへのアクセスや特権ユーザーのアクティビティをリアルタイム監視し、またセッション記録の形で実行された動作の信頼できる証拠を生成することを可能にします。

誰が特権ユーザーなのか？

特権ユーザーはIT管理者に限定されていません。特権ユーザーは一般ユーザーより多くの権限を有し、情報システムにアクセスします。、システムにおいてほぼすべての特権を有する‘スーパーユーザー’から、高位の特権を有する第三者プロバイダや経年的に特権を蓄積してきた年長の従業員にまで及ぶ可能性があります。

Shell Control Box

Shell Control Box (SCB) はサーバーへのリモート管理アクセスを制御、監視、監査するデバイスです。サーバー管理に使用される暗号化接続を制御することによって、サーバー管理者やサーバー管理プロセスを監視するツールです。SCBは透過的な外部デバイスで、クライアントやサーバーから完全に独立しています。SCBはすべての管理上のトラフィックを監査証跡として記録します。記録された監査証跡は、特権ユーザーのすべての動作を再現する映画のように再生できます。すべての監査証跡はインデックス付けされ、再生中に早送りが可能で、管理者が見たいイベントやテキストを検索することが可能です。SCBはSSH,RDP,Telnet,TN3270,Citrix ICA,VNC接続を完全に制御し、管理者の仕事のフレームワークを提供します。

PCI DSSを満たす為Shell Control Box使用の利点

コンプライアンスでは、予防手段や実証ツールとしてSCBの機能に使用できます。特権ユーザーの動作が気づかれない、または監視されない、ことがないことをSCBは保証します。

SCBはクライアントと指定されたサーバーの間に位置するプロキシベースでエージェントレスのman in the middle （中間者）ソリューションです。重要なサーバーへのすべての接続は、認証の為にSCBを通ります。

4-eyes承認は、セキュリティ専門家にポリシー違反の際に接続を中止する権限と、全リモートセッション中で特権ユーザーをリアルタイムに監視する権限を与えます。

SCBは、サードパーティの多因子認証ツールにオープンAPI経由で統合でき、強力な認証ゲートウェイとして機能します。

記録された監査証跡は、すべての実行コマンドを含むセッションのメタデータを記憶します。再生記録は、再調査により少ない時間で、重大なイベントを強調します。セッション記録はコンプライアンス、ポリシー施行、フォレンジックにおいて実証ツールとして利用できます。

PCI DSS Structure

PCI-DSS v3.2に記述されているポリシーと手順は6つの項目と12の要件で構成されています。要件はさらにいくつかに細分化されます。

1.	安全なネットワークとシステムの構築と維持	1. カード会員データを保護するために、ファイアウォールをインストールして維持する 2. システムパスワードおよびその他のセキュリティパラメータにベンダー提供のデフォルト値を使用しない
2.	カード会員データの保護	3. 保存されるカード会員データを保護する 4. オープンな公共ネットワーク経由でカード会員データを伝送する場合、暗号化する
3.	脆弱性管理プログラムの維持	5. マルウェアに対してすべてのシステムを保護し、ウィルス対策ソフトウェアを定期的に更新する 6. 安全性の高いシステムとアプリケーションを開発し、保守する
4.	強力なアクセス制御手法 の導入	7. カード会員データへのアクセスを、業務上必要な範囲内に制限する 8. システムコンポーネントへのアクセスを識別・認証する
5.	ネットワークの定期的な 監視およびテスト	9. カード会員データへの物理アクセスを制限する 10. ネットワークリソースおよびカード会員データへのすべてのアクセスを追跡および監視する
6.	情報セキュリティポリシーの維持	11. セキュリティシステムおよびプロセスを定期的にテストする 12. すべての担当者の情報セキュリティに対応するポリシーを維持する

Balabit ソリューションでどのようにコンプライアンスを達成するか？

次の表は、ペイメントカード業界データセキュリティ基準バージョン3.2（PCI-DSS v3.2に基づく）の要件についての詳細とBalabit製品の対応状況を説明します。

syslog-ng	PCI DSS 要件	Shell Control Box
ファイアウォールからログサーバーへの信頼できるログのパスを作成し、全ての構成変更の監査証跡を補完するための改竄防止機能、デジタル署名機能、タイムスタンプ機能のついたログストレージを提供します。 SSBは収集、転送、安全かつセキュアなストレージ、バックアップ、アーカイブ、クリーンアップを含む監査ログのライフサイクルを管理します。検索インターフェースまたはAPIを使用して、収集されたログを検索します。	1.1.1 すべてのネットワーク接 続およびファイアウォール/ ルーター構成への変更を承認およびテストする正式なプロセス	
ホスト上でメッセージの送信元の右側に 、未知のプログラムからのログにフラグをつけることができ、区別してルーティング、もしくはそれらに基づいてアラートを作成することができます。SSBは,サーバー機能について詳細に記載したカスタマイズレポートを生成することができます。	2.2.1：同じサーバーに異なったセキュリティレベルを必要とする機能が共存しないように、一つのサーバーには、主要機能を一つだけ実装する。	SCBはリモートアクセス接続を監視する専用アプライアンスです。他のアプリケーションをインストールすることはできません。
無効化されたサービスからのログを通常のログトラフィックから選別（フィルタ）し、セキュリティアナリストに警告することができます。	2.2.2：システムの機能に必要なサービス、プロトコル、デーモンなどのみを有効にする。	
	2.3：強力な暗号化を使用して、すべてのコンソール以外の管理アクセスを暗号化する。	サーバーへのリモートアクセスに暗号化を強制することが出来ます。リモートアクセスは完全な監査と再現が可能です。広範囲なプロトコルをサポートします：SSH,RDP,Citrix ICA, Telnet,VMware View,VNC
	3.3：表示時にPANをマスクして（最初の6桁と最後の４桁が最大表示桁数）、業務上の正当な必要性がある関係者だけがPAN全体を見ることができるようにする。	そのような情報が表示される前であっても、イベントについてアラートを上げる、または自動でユーザーの接続を終了することができます。

syslog-ng	PCI DSS 要件	Shell Control Box
必要に応じて強い、暗号化された安全なハッシュを使用して、任意の番号を隠すためにカード会員データを含むすべてのログをリライトすることができます。 このリライトは、カード会員データがシステムから流失することがないように、メッセージの送信元で適切に行うことができます。 また、ログは機密データが安全であることを確実にするために、強力な暗号化機能を使用したバイナリで、タイムスタンプ付きのファイルに保存することができます。許可されたユーザーのみが復号キーにアクセスすることができます。	3.4：以下の手法を使用して、全ての保存場所でPANを少なくとも読み取り不能にする（ポータブルデジタルメディア、バックアップメディア、ログを含む）。 ・強力な暗号化をベースにしたワンウェイハッシュ（PAN全体をハッシュする必要がある） ・トランケーション（PANの切り捨てられたセグメントの置き換えにはハッシュを使用できない） ・インデックストークンとパッド（パッドは安全に保存する必要がある） ・関連するキー管理プロセスおよび手順を伴う、強力な暗号化	SCBの監査証跡は、強力な公開鍵暗号を用いて暗号化することができます。要求される鍵を保有する人員だけが、記録した監査証跡にアクセスしPANを表示できます。
クライアントとログサーバー間でTSL暗号化を使用して、メッセージの完全性を保護し、第三者が通信にアクセスし、修正を加えるのを防ぎます。 クライアントとログサーバー間の通信は、X.509証明書を使用することでクライアントと相互認証することができ、通信相手の身元を確認します。ログファイルに偽のメッセージを注入することからの攻撃を防ぎます。	4.1：オープンな公共ネットワーク経由で機密性の高いカード会員データを伝送する場合、以下のような、強力な暗号化とセキュリティプロトコル（SSL/TLS、IPSEC、SSH など）を使用して保護する。 ・信頼できるキーと証明書のみを受け入れる。 ・使用されているプロトコルが、安全なバージョンまたは構成のみをサポートしている。 ・暗号化の強度が使用中の暗号化方式に適している。	
アンチウイルスツールのログを含んだ多種多様なログ供給源からログを収集します。 SSBはログメッセージをフィルタリングし、解析することで関連するデータに基づいたカスタマイズレポートを生成します。	5.2：すべてのウィルス対策メカニズムが以下のように維持されていることを確認する。 ・最新の状態である。 ・定期的にスキャンを行う。 ・PCI DSS 要件10.7 に従って監査ログを生成する。	
様々なフォーマット（例えば、プレーン・テキスト、JSON,、RFC3164、 RFC5424）と,様々な方式（例えば、UNIXドメインソケットやTCP、ファイルから読み取り、SQLから直接フェッチ、オペレーティングシステムの組込みロギング機能）を使用して、アプリケーションからログを直接収集することができます。 PatternDB機能を使用して、セキュリティイベントを特定するカスタムアプリケーションのためのパターンを書くことができます。 SSBは開発者とオペレータが、強力な検索インターフェースとAPIを通して、適切なオペレーションで、カスタムアプリケーションを監視できる手助けをします。	6.3：3 内部および外部ソフトウェアアプリケーション（アプリケーションへの Webベースの管理アクセスを含む）を次のように開発する。 ・PCI DSS （安全な認証やロギングなど）に従って。。 ・業界基準やベストプラクティスに基づいて。 ・ソフトウェア開発ライフサイクル全体に情報セキュリティを組み込む。	リモート・アプリケーションへの接続を安全にし、管理します。 リアルタイムモニターで内部もしくは外部のアプリケーションで実行されるすべてのリモートセッションを監視できます。

syslog-ng	PCI DSS 要件	Shell Control Box
ファイアウォールやIDSなどを含む様々なセキュリティデバイスから、ログを収集し、処理することができます。 PatternDBでは、既知の攻撃パターンのアラートを作成できます。 SSBはこれらのシステムのログから、既知の攻撃パターンを探す検索機能を、自動でまたは手動で、使用することができます。	要件6.6：一般公開のWebブアプリケーションは、継続的に、新たな脅威や脆弱性に対処し、これらのアプリケーションは、以下のいずれかの方法による既知の攻撃から保護されていることを確認する。： ■一般公開されている Web アプリケーションは、アプリケーションのセキュリティ脆弱性を手動/自動で評価するツールまたは手法によって、少なくとも年 1 回および何らかの変更を加えた後にレビューする。 ■継続的にすべてのトラフィックを確認するため、Web ベースの攻撃を一般公開されている Web アプリケーションの手前で検知および回避する自動の技術ソリューション（Web アプリケーションファイアウォールなど）をインストールする。	
強力な認証と細かなアクセスポリシーを使用して、ログへのアクセスを制限することができます。すべてのログメッセージは、いわゆるログストア™ファイルとして中央ログサーバー上に、公開鍵暗号方式を使用して、暗号化されます。デジタル署名やタイムスタンプもログファイルに追加されます。	7.1： システムコンポーネントとカード会員データへのアクセスを、業務上必要な人に限定する。 7.1.2： 特権ユーザーＩＤに与えるアクセス権を職務の実行に必要な最小限の特権に制限する。 7.1.3： 個人の職種と職務に基づくアクセス権を割り当てる。	SCBはロールベースアクセス制御（ＲＢＡＣ）モデルを使用してリモートアクセス接続を制御できるツールです。ＬＤＡＰデータベースからユーザーの所属するグループを取得でき、これらの役割をベースに接続や特定のプロトコルチャンネルにアクセス権を付与することができます。 ＳＣＢのアクセス権はＡＣＬ（アクセスコントロールリスト）とグループメンバーシップに完全に基づいています。大幅なカスタマイズやＬＤＡＰデータベースとの連携が可能です。
	7.2： システムコンポーネントで、ユーザーの必要性に基づいてアクセスが制限され、特に許可のない場合は「すべて拒否」に設定された、アクセス制御システムを確立する。	SCBはサーバーへのアクセスを、選択したLDAPやActive Directory ユーザーグループメンバーだけ、あるいは特別にリストしたユーザーだけに制限できます。クライアントIPアドレスベースのアクセスに限定することも可能です。 SCBは管理プロトコルのチャンネルに対してもアクセスを制限できます。たとえば、Windows Terminal Server アクセスで共有ドライブアクセスを無効化、あるいは選択したユーザーだけにSSH接続のポートフォワーディングを有効にします。
PatternDB機能を使用して、成功したログインログとログアウトログを組み合わせて、ユーザーのアクセスを容易に追跡するセッションイベントを作成します。 SSBはシステムコンポーネントへのアクセスを示すカスタムレポートを生成します。ユーザー名をADまたはLDAPデータベースに対応させます。 強力な認証を適用することで、カード会員データを含むログに潜在的にアクセスする人々のアカウンタビリティを保証します。	8.1： ：全てのシステムコンポーネント上の非消費者ユーザーと管理者のユーザーID 管理を保証するためのポリシーと手続きは、以下のように定義、実装される。 8.1.1： システムコンポーネントまたはカード会員データへのアクセスを許可する前に、すべてのユーザーに一意のIDを割り当てる。	SCBはAdministratorまたはrootのような共有アカウントでアクセスしても、ユーザーが所有する個別のユーザーIDを使用して認証できます。 SCBのローカルにログイン情報を保管するため、共有アカウントの使用を簡素化したり、アカウント変更を管理します。 SCBにより、パスワード管理システムによる認証が可能になります。

syslog-ng	PCI DSS 要件	Shell Control Box
	8.1.3： 契約終了したユーザーのアクセスを直ちに取り消す。	ユーザーが中央LDAPデータベースに認証時、SCBはそのユーザーの特権あるいは関連するグループメンバーシップが取り消されると直ちにアクセスを拒否します。 LDAPへユーザー認証できない共有アカウントやデバイスへのアクセスも直ちに拒否します。
	8.1.5： サードパーティがリモートアクセス経由でシステムコンポーネントへアクセス、サポート、メンテナンスするのに使用するユーザーIDを以下のように管理する。 ・必要な時間内だけ有効になり、使用されていないときは無効になっている。 ・使用時に監視されている。	クライアントが指定された時間枠（たとえば、スケジュールされたメンテナンス時間）の間だけ保護サーバーへのアクセスを有効にするタイムポリシーを作成できます。メンテナンス時間外のクライアントの接続を自動的に無効にできます。 ベンダがシステム上でることを監視し制御するために、４－ｅｙｅｓ承認を使用することができます。ベンダはSCBの管理者に接続が承認された場合にのみシステムにアクセスできます。 この機能により、Ａｕｄｉｔ Ｐｌａｙｅｒアプリケーションでベンダの動作をリアルタイムで見ることができます。 ユーザーが不適当または有害な動作をしていると判断したら、接続をいつでも終了させることができます。
	8.1.6：6 回以下の試行で、ユーザー ID をロックアウトすることによって、アクセスの試行回数を制限する。	失敗したログイン試行に基づいてアラートを生成します。 特定回数試行が失敗すると一定期間ログインを拒否します。
	8.1.8： セッションのアイドル状態が15分を超えた場合、ターミナルまたはセッションを再度アクティブにするため、ユーザーの再認証が必要となる。	ＳＣＢは指定された時間後のアイドル状態のセッションを自動的に終了します。

syslog-ng	PCI DSS 要件	Shell Control Box
8.2：一意のＩＤを割り当てることに加え、すべてのユーザーを認証するため、次の方法の少なくとも１つを使用することで、すべてのシステムコンポーネント上での顧客以外のユーザーと管理者の適切なユーザー認証管理を確認する。 ・ ユーザーが知っていること（パスワードやパスフレーズなど） ・ トークンデバイスやスマートカードなど、ユーザーが所有しているもの ・ ユーザー自身を示すもの（生体認証など）	ＳＣＢは中央ＬＤＡＰあるいはＲＡＤＩＵＳサーバーへの監査対象の接続を一元的に認証できます。また、パスワード、公開鍵や証明書、さらに特定のケースとしてスマートカードなどの強力な認証方法の使用を強制します。 SCBはサードパーティのパスワード管理ツールや認証情報ストアを統合することができます。	
	8.2.1： 強力な暗号化を使用して、すべてのシステムコンポーネントで、送信と保存中に認証情報（パスワード/パスフレーズなど）をすべて読み取り不能とする。	ＳＣＢはＬＤＡＰＳの暗号化をサポートします。同様に監査対象接続の強力な認証方法もサポートします。
	8.2.3：パスワード/フレーズは以下の条件を満たす必要がある。 ・少なくとも7文字以上の長さが必要。 ・数字とアルファベットの両方の文字を含む。 8.2.4：ユーザーパスワード/パスフレーズを少なくとも90日ごとに変更する。	パスワードポリシーを使用して、最小のパスワード強度と有効期限を強制できます。
	8.3：多要素認証を使用して、すべての個々の非コンソール管理アクセスとCDEへのすべてのリモートアクセスを保護する。	SCBはリモートアクセス接続の制御と調査のために設計されました。 ＳＣＢはアクセスするサーバーに依存せずにユーザー認証でき、公開鍵認証、X.509証明書、ＲＡＤＩＵＳやＬＤＡＰデータベース認証などの強力な認証をサポートします。 SCBは外部システムに統合するためのプラグインを提供しています。ターゲットサーバーを認証する前に、ユーザーを認証・承認します。このようなプラグインを提供することで、次のプロトコル：RDP、SSH、TELNETに複数要素の認証を可能にします。

syslog-ng	PCI DSS 要件	Shell Control Box
	8.5： 次のように、グループ、共有、または汎用のＩＤやパスワード、または他の認証方法が使用されていない。 ・汎用ユーザーＩＤが無効化または削除されている。 ・システム管理作業およびその他の重要な機能に対する共有ユーザーＩＤが存在しない。 ・システムコンポーネントの管理に共有および汎用ユーザーＩＤが使用されていない。	ＳＣＢは汎用ユーザーＩＤの使用を禁止することができます。また、汎用ＩＤや共有ＩＤを共有アカウントにアクセスすると、実際の個別なユーザーＩＤにリンクさせることもできます。 ＳＣＢはユーザーが実際に必要な資格情報を知らなくても、ユーザーからの共有アカウントの秘密の資格情報を維持しながら、監査対象のデバイスやサーバーに認証する構成も可能です。
	8.7： カード会員データを含むデータベースへのすべてのアクセス（アプリケーション、管理者、およびその他のすべてのユーザーによるアクセスを含む）が以下のように制限されている。 データベースへのユーザークセス、データベースのユーザークエリ、データベースに対するユーザークションはすべて、プログラムによる方法によってのみ行われる。 ・データベースへの直接アクセスまたはクエリはデータベース管理者のみに制限される。 ・データベースアプリケーション用のアプリケーションＩＤを使用できるのはそのアプリケーションのみである（個々のユーザーやその他の非アプリケーションプロセスは使用できない）。	ＳＣＢは保護サーバーへの管理者リモートアクセスの制御と監査を行います。 SCBはリモートサーバー管理で使用される最も一般的なアプリケーションやプロトコル（SSH、RDP、VNC、VMware View、Windowsターミナルサービス、HTTP、Citrix）を制御できます。 SCBは、クライアントとホスト間の中央認証ゲートウェイとして動作します。 アプリケーションに対するすべてのリモート管理接続は、監査証跡フォームで記録されます。
このような監査証跡のログを収集して保管します。PatternDB機能を使用すると、特権ユーザーによるログインやログデータへのアクセスなどのような、特別なイベントを含むコンテンツに基づいて、ログをフィルタリングできます。	10.1： システムコンポーネントへのすべてのアクセスを各ユーザーにリンクする監査証跡を確立する。	セッションを監査証跡として記録し、監査証跡の内容をインデックス付けします。監査証跡の内容は、Webインターフェースから検索できます。
このような監査証跡のログを収集して保管します。PatternDB機能を使用すると、特権ユーザーによるログインやログデータへのアクセスなどのような、特別なイベントを含むコンテンツに基づいて、ログをフィルタリングできます。	10.2： 次のイベントを再現するために、すべてのシステムコンポーネントの自動監査証跡を実装する。 10.2.1：カード会員データへのすべての個人アクセス 10.2.2： ルート権限または管理権限を持つ個人によって行われたすべてのアクション	SCBは保護サーバーに対する管理者リモートアクセスの制御と監査を行います。記録された監査証跡は発生したイベントを正確にレビューする映画のように再生できます。 管理者のすべての操作は監査証跡に表示されます。特定コマンドの使用あるいは接続で表示されるテキストを検索するため、ＳＣＢは監査証跡の内容を自動的に処理し、インデックス付けします。 ＳＣＢは記録されたセッションに基づいて、カスタムレポートを作成することができます。

syslog-ng	PCI DSS 要件	Shell Control Box
このような監査証跡のログを収集して保管します。PatternDB機能を使用すると、特権ユーザーによるログインやログデータへのアクセスなどのような、特別なイベントを含むコンテンツに基づいて、ログをフィルタリングできます。	10.2.3：すべての監査証跡へのアクセス	SCBに保存した監査証跡は、その実行権限のあるユーザーだけがアクセスできます。 監査証跡のダウンロードはログとして記録されます。 監査証跡は、一つまたは複数の暗号鍵による暗号化も可能です。 複数鍵で暗号化すれば、監査証跡はすべての必要な復号鍵所有者だけが閲覧できます。
このような監査証跡のログを収集して保管します。PatternDB機能を使用すると、特権ユーザーによるログインやログデータへのアクセスなどのような、特別なイベントを含むコンテンツに基づいて、ログをフィルタリングできます。	10.2.4： 無効な論理アクセス試行	ＳＣＢはリモートサーバーあるいは何らかの理由によって拒否された特定のプロトコルチャンネルへのアクセス試行を自動的に記録します。
	10.2.6： 監査ログの初期化、停止、一時停止	SCBは透過デバイスで、クライアントや監査対象サーバーから独立しています。 リモートサーバーのユーザーはＳＣＢのアカウントは必要ありません。ＳＣＢへの明示的なアクセス権を持つユーザーのみが監査できます。
	10.2.7： システムレベルオブジェクトの作成および削除	ＳＣＢのコンフィグレーション変更に対しては、SCBは詳細な変更ログを保持し、変更理由を説明するよう要求できます。
マクロと強力なメッセージ書き換え能力を提供します。これらは、共通なフォーマットに変換し、メッセージを再フォーマットし、正規化させます。 SSBは直感的な検索インターフェースを使用して、イベントのコンテキストを調査することができます。	10.3： イベントごとに、すべてのシステムコンポーネントについて少なくとも以下の監査証跡エントリを記録する。 10.3.1： ユーザー識別 10.3.2： イベントの種類 10.3.3： 日付と時刻 10.3.4： 成功または失敗を示す情報 10.3.5： イベントの発生元 10.3.6： 影響を受けるデータ、システムコンポーネント、またはリソースのＩＤまたは名前	SCBはこれらすべてのデータと他のメタデータを記録します。同様にサポートプロトコルを使用した保護サーバーへのアクセスを記録します。 ＳＣＢはユーザーに一般ユーザー名での認証を要求できます。汎用ユーザー名を使った接続を実アカウントに対応させることができます。

syslog-ng	PCI DSS 要件	Shell Control Box
タイムスタンプをISO 8601標準の単一のフォーマットに変換します。 メッセージを受信した時に、自動的に日付と時刻を追加します。 サードパーティであるTSAのタイムスタンプを使用してログメッセージにタイムスタンプを付与します。 SSBはNTPサーバーにシステムクロックを同期させることができます。	10.4：時刻同期技術を使用してすべての重要なシステムクロックおよび時間を同期し、時間を取得、配布、保存するために以下の要件が実施されていることを確認する。 10.4.1：重要なシステムが正確で一貫性のある時刻を持っている。 10.4.2：時刻データが保護されている。 10.4.3：時刻設定は、業界で認知されている時刻ソースから受信されている。	自動的にシステムクロックをリモートタイムサーバーに同期させることができます。そのため監査証跡は正確な時刻情報を持ちます。
公開鍵暗号方式を使って、一元管理サーバー上でログストア™と呼ばれるファイルのすべてのログメッセージを暗号化できます。 ファイルにデジタル署名を付けることもでき、外部のTSA（Timestamping Authority）にタイムスタンプを保存されたデータに対して要求できます。 SSBは、不正な外部からのアクセスを防いで安全なログストレージとして機能するように設定されています。	10.5：変更できないよう監査証跡をセキュリティで保護する。	すべての監査証跡は電子署名が付けられ公開鍵で暗号化されます。暗号化には複数鍵を使用することもできます。 監査証跡はローカルまたは外部の時刻認証局（TSA：Timestamping Authority）を使ってタイムスタンプを付けられます。
暗号化されたログメッセージを閲覧できるのは、必要な暗号鍵を持つユーザーだけです。 SSBは強力な認証ときめ細かなアクセスポリシーを使ってログへのアクセスを制限できます。 Active Directoryまたはその他のLDAPサーバーからの情報に基づいて、ログへのアクセスをグループの所属関係に紐づけることができます	10.5.1：仕事関連のニーズを持つ個人に監査証跡の表示を制限する。	監査証跡は必要な権限を持つユーザーのみダウンロード可能です。 監査証跡の暗号化には複数鍵を適用することもできます。 通信のアップストリームトラフィックをダウンストリームとは別に暗号化でき、別の暗号化鍵を持つ場合だけ表示されます。
変更ができないようにログメッセージは暗号化され、タイムスタンプが押され、デジタル署名が付けられ、バイナリーフォーマットで保存されます。 メッセージの完全性はクライアントからログサーバーに送信される際に確認されます。クライアントとログサーバーの間の通信は、X.509証明書を使って互いに認証することができます。	10.5.2：監査証跡ファイルを不正な変更から保護する。	SCBアプライアンスに保存された監査証跡は、監査対象サーバーから物理的に独立しています。 監査証跡は暗号化、タイムスタンプ付き、または電子署名付きが可能で、変更することはできません。 承認されたユーザーだけが直接アクセスできます。

syslog-ng	PCI DSS 要件	Shell Control Box
ログメッセージを変更できないように暗号化してデジタル署名を付けて保存できる一元管理ログコレクターおよびログサーバーとして機能し、アーカイブとバックアップを含むログのライフサイクル全体を処理します。 TCPの暗号化、RLTP (Reliable Log Transfer Protocol)経由でのアプリケーションレベルの応答確認、ディスクベースのバッファリングをサポートします。	10.5.3：監査証跡ファイルは、変更が困難な一元管理ログサーバーまたは媒体に即座にバックアップする。	クライアントとサーバー間のネットワーク接続から情報を抽出します。 記録セッションごとに、ローカルまたはリモートハードドライブへバックアップを作成できます。 記録された監査証跡をすぐにアーカイブできます。
ワイヤレスデバイス、ファイアウォール、DNS、メールサーバーのような外部に公開されているテクノロジのログをリアルタイムで一元管理のログサーバーに送信します。	10.5.4：外部に公開されているテクノロジのログを、安全な一元管理の内部ログサーバーまたは媒体デバイス上に書き込む。	レガシーなBSD-syslogと最新のIETF-syslogプロトコルをサポートし、ログメッセージを相互認証したTLS暗号化接続でログサーバーに送信できます。
メッセージを収集してログを転送する際に、RLTP(Reliable Log Transfer Protocol)を使ってアプリケーションレベルの応答確認で一元管理のサーバーにログロストが発生しないようにします。 ログメッセージのコンテンツ（メッセージの内容）を解析してフィルタをかけます。抽出した情報に基づいてアラートをあげます。レポートや統計データを作成でき、レビューの際に重要なログに焦点を当てるための手助けとなります 様々な種類の出力フォーマットをサポートしているので、サードパーティソリューションとスムーズに統合できます。 SSBの検索インターフェースは、素早いインデックスエンジンで補完して定期的なマニュアルでのレビューを実行し、アドホックチャートとタイムラインを作成できます。 検索APIを使って、スクリプトによるクエリを作成して分析ツールと統合することができます。	10.6：すべてのシステムコンポーネントのログとセキュリティイベントを調べ、異常や怪しい活動を特定する。 10.6.1：毎日一度以上以下をレビューする。 すべてのセキュリティイベント CHDやSADを保存、処理、または送信する、またはCHDやSADのセキュリティに影響を及ぼす可能性のあるすべてのシステムコンポーネントのログ すべての重要なシステムコンポーネントのログ すべてのサーバーとセキュリティ機能を実行するシステムコンポーネント（ファイアウォール、侵入検知システム/侵入防止システム（IDS/IPS）、認証サーバー、電子商取引リダイレクションサーバーなど）のログ 10.6.2：組織のポリシー、および年間リスク評価によって決定されたリスク管理戦略に基づいて他のシステムコンポーネントすべてのログを定期的にレビューする。 10.6.3：レビュープロセスで特定された例外と異常をフォローアップする。	10.6：監査対象の接続に関するレポートを毎日自動的に生成します。 特定コマンドの使用またはターミナルベースやグラフィカル接続で表示されるテキストを検索するために、監査証跡の内容にインデックスを自動的に付けることもできます。 特定キーワードや検索クエリの検索を自動的に定義し、カスタムレポートに結果を含めることが可能です。 SCBは自身のログをリモートサーバーまたはSIEMに暗号化接続で送信できます。 10.6.1：フォレンジック調査と同様に、定期的なレビューの有効性を大幅に向上させます。 映画のように特権ユーザーのセッションを再生することで、サーバーで何が起こったか正確に判断するために必要な時間も著しく削減できます。

syslog-ng	PCI DSS 要件	Shell Control Box
ディスク容量を節約するためにログメッセージを圧縮して異なるコンテナにフィルタをかけることができます。 ログストア™はログを即座に確認できます。 SSBはメッセージを自動的に外部ストレージにアーカイブできます。アーカイブされたメッセージは暗号化されたままですが、Webインターフェースで利用できます。 より多くのストレージ容量を使用するためにNFSまたはSMBプロトコルや既存のサードパーティのストレージソリューションを活用することができます。 検索機能はテラバイト単位のデータを処理できるように設計されています。	10.7：監査証跡の履歴を少なくとも1年間保持する。少なくとも3カ月はすぐに分析できる状態にしておく（オンライン、アーカイブ、バックアップから復元可能など）。	クライアントとユーザー間のネットワーク接続から情報を抽出します。 記録セッションごとに、ローカルまたはリモートハードドライブへバックアップを作成できます。 記録された監査証跡は、すぐにアーカイブできます。
	12.3.9：ベンダおよびビジネスパートナーには必要とする場合にのみリモートアクセステクノロジをアクティブ化し、使用後直ちに非アクティブ化する。	SCBの接続ポリシーは必要に応じて簡単に有効化、無効化できます。4-eyes承認の仕組みを使用すると、接続ポリシーのすべてのセッションは個別の認証が必要となり、ユーザー作業をリアルタイムに監視できます。 また、日あるいは週の指定時間における接続アクセスを制限できます。
	12.3.10：リモートアクセステクノロジ経由でカード会員データにアクセスする担当者については、定義されたビジネスニーズのために明示的に承認されない限り、ローカルドライブおよびリムーバブル電子媒体へのカード会員データのコピー、移動、保存を禁止する。承認されたビジネスニーズがある場合、使用ポリシーはデータが適用されるPCI DSS要件すべてに従って保護されることを要求する必要がある。	リモートアクセス接続をチャンネルレベルで制御できます。 SCBはSCPやSFTPのファイル転送も監査でき、それぞれのファイル操作を記録し、転送されたファイルのコピーを監査証跡に保存できます。
	12.5.5：すべてのデータへのアクセスを監視および管理する。	ユーザーやサーバー管理者から独立して、リモートサーバーへのアクセス制御や監査機能を提供します。その結果、システム管理者より上位の分離した監査レイヤーを生成することができます。
	A.1.1：各事業体が、その事業体のカード会員データ環境にアクセスするプロセスのみを実行するようにする。	リモートユーザーが許可されたサーバーだけにアクセスでき、またいくつかのプロトコルによるリモートアクセスも監査できます。 プロバイダは、すべての事業体に監査証跡へのアクセスを許可するために、SCBを使用することもできます。

syslog-ng	PCI DSS 要件	Shell Control Box
異なる種類のログを別々のログスペースに収集して保存します。 ログスペースにフィルタをかけることで関連するデータのみを表示する処理が可能です。	A.1.3：ログ記録と監査証跡が有効になっていて、各事業体のカード会員データ環境に一意であり、PCI DSS要件10と一致していることを確認する。	プロバイダのインフラの中央に配置し、すべてのリモートアクセスの監査証跡を自動的に収集するように設定することもできます。SCBは、すべてのセッションの監査証跡を別々のファイルに収集し、接続パラメータをベースに整理することができます。このように、関連事業体にのみ監査証跡へのアクセスを保証します。 監査証跡を暗号化することで監査証跡のセキュリティがさらに向上します。必要な復号鍵を持つ人員だけが監査証跡を開き再生できます。
	A.1.4：ホストされている加盟店またはサービスプロバイダへの侵害が発生した場合に、タイムリーなフォレンジック調査を提供するプロセスを可能にする。	記録された監査証跡への瞬時なアクセスを提供します。 監査証跡にインデックスを付けることで、すべての監査証跡の内容をフリーフォームで検索できます。ターミナル接続でのコマンド使用、あるいはターミナルやグラフィカル接続のサーバーで表示されたテキストも含みます。 映画のように監査証跡を再生することで、より効果的にレビューとフォレンジックを行うことができます。

結論

クレジットカード情報の管理と処理に関わる業務を行う組織は、ハイレベルなセキュリティの確立と、監査目的の証拠保有のために、PCI DSS要件を遵守する必要があります。Balabit社は、カード会員データに関する2つの主要なフロント部分、信頼できるログの管理とカード会員データにアクセスできる特権ユーザーの監視という点おいて、組織を支援します。これらのフロント部分の安全性を確保することで組織はカード会員データに対するすべてのアクションをリアルタイムに監視することができます。

Balabit社はAPT攻撃のリアルタイム防御についても非常に重視しています。それは既存の製品と新製品であるBlindspotter（特権ユーザーの行動分析ソリューション）を組み合わせることで実現しました。Blindspotterは、個人の現在の行動と学習済みの行動を比較し、それにより乗っ取られたアカウントまたは悪意のある内部脅威によって実行されたセッションを特定し、中断することができます。

BALABIT
CONTEXTUAL SECURITY INTELLIGENCE

JTC-i ジュピターテクノロジー

BALABIT社について

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社のContextual Security Intelligence™プラットフォームは、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。Balabit社は、2000年に設立され、世界中でFortune 100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。

Balabit社の商用製品またはオープンソースの製品の詳細、評価版のリクエストは下記をご参照ください：

- syslog-ng stoer Box (SSB)：
http://www.jtc-i.co.jp/product/ssb/ssb.html
- Shell Control Box：
http://www.jtc-i.co.jp/product/scb/scb.html
- Blindspotter：
準備中。詳しくはお問合せ下さい。
（https://www.jtc-i.co.jp/contact/scontact.php）

製品マニュアル、ガイド、その他のドキュメント：
（SSB）http://www.jtc-i.co.jp/support/documents/ssbdoc.html
（SCB）http://www.jtc-i.co.jp/support/documents/scbdoc.html

評価版リクエスト
https://www.jtc-i.co.jp/support/download/index.php