コンプライアンスとシスログ

Rev. 1.0

（2010 年 12 月 14 日版）

ジュピターテクノロジー

目次

1 前書

この文書では SSB (Syslog-ng Store Box)によるシスログやイベントログメッセージの収集・保存・管理が SOX, HIPPA, PCI-DSS のような規制を伴うコンプライアンスにどのように役立つかを論じます。この文書は集中ログソリューションに関する技術専門家や最終決定権者に読んでいただくためのものですが、基本的なネットワーク知識を有する方であれば誰でもその内容を理解できます。ここで明らかにされるプロシージャやコンセプトは SSB v1 に対応します。

1.1 内容の要約

この文書は以下のセクションで構成されます:

“セクション2 紹介”はシスログとは何か、なぜそれがポリシーコンプライアンスの重要な要素であるかを説明します。

“セクション3 ポリシーコンプライアンスのために SSB を使用、セクション4 HIPaa コンプライアンスとログ”はポリシーコンプライアンス要件の詳細なリストです。SSB や Syslog-ng PE で可能になる PCI-DSS, COBIT 4.1, HIPAA の要件を含みます。

“セクション5 その他の重要な機能”ではシスログアーキテクチャの設計や導入するにあたって SSB が手軽に使用できるというその他の機能を説明します。

“セクション6 追加情報”には BalaBit IT Security の簡単な紹介です。

2 はじめに

2.1 シスログとは

OS、アプリケーション、ネットワークデバイスはそれらで発生する様々なイベントのテキストメッセージを生成します。ユーザーログイン、ファイル生成、リモートホストへの接続開始などです。これらのメッセージ、ログメッセージと呼ばれます、は通常システムのローカルディスクに保存されます。集中化シスログの目的は、メッセージを1台の中央ログサーバーが収集することです。シスログアーキテクチャの詳細な紹介はホワイトペーパー“分散シスログアーキテクチャと Syslog-ng PE”を参照してください。

2.2 ポリシーコンプライアンス処理でシスログが重要な理由

ログメッセージはネットワーク、デバイス、そしてこれらで実行するアプリケーションのイベントについて重要な情報を提供します。ログメッセージはセキュリティインシデント、オペレーションの問題、ポリシー違反などの検出に利用でき、監査やフォレンジックにおいても有効です。ログメッセージの収集や解析はいくつかの規制で直接的あるいは間接的に必要です。これらは SOX, Basel II, HIPAA あるいは PCI-DSS を含みます。

2.3 Syslog-ngとSSBについて

Syslog-ng アプリケーションはシスログ収集と転送ツールでありファイルやその他のソースからログメッセージを収集し、さらにリモートホストから送信されたログメッセージを受信します。強力なメッセージフィルターとルーティング機能もあります。SSB は Syslog-ng を利用したログサーバーアプライアンスです。Web ベースのコンフィグレーション及びログ閲覧インターフェイス、暗号化・デジタルサイン付ログ保存などの機能が追加されています。

2.4 ログ管理で解決されなければならない問題

使用可能なログインフラの作成においては解決しなければならないいくつかの問題と困難さがあります。考慮すべき主要な問題をまとめます。どのように Syslog-ng PE アプリケーションで解決できるかを簡単に説明します。

- “多数の異なるデバイスと多数の OS で実行するアプリケーション” のログメッセージの中央ログサーバーへの収集を開始するには、メッセージを生成するデバイスからログを取り出さなければなりません。これらのデバイス（デスクトップコンピュータ、サーバー、スイッチやルータ・ファイアーウォールなどのネットワークデバイス、その他）は通常多数の異なる OS を使用しています。これらは全て中央サーバーにログを送信しなければなりません。OS の種類が多いという問題は、それぞれが異なるコンフィグレーション要件と能力のログソリューションを持っているということです。この問題に対して、Syslog-ng は通常の OS（Linux, Solaris, HP-UX, BSD, IBM AIX を含む）にインストールでき、さらに Microsoft Windows や IBM System i プラットホームからログを収集する専用エージェントアプリケーションを用意しています。単一のロギングアプリケーションを使うことはコンフィグレーションと管理に関する問題を大幅に単純化し、全てのデバイスで先進のロギング機能（TLS 暗号化ログ転送やディスクベースバッファリング）の利用を可能にします。何らかの理由でデバイスに Syslog-ng をインストールできない（たとえば変更不能な組み込みファームウェアを実行している）場合は、Syslog-ng を実行するローカルコンピュータはデバイスからシスログメッセージを受信し中央ログサーバーに転送します。

- “異なるタイムスタンプとメッセージフォーマット” 異なるログメッセージはしばしば異なるタイムスタンプフォーマットのメッセージ日付（たとえばソースタイムスタンプが年や時間帯情報を持たない）となり、あとでメッセージを探したり、イベントの流れの中でその場所を正しく見ることが困難です。Syslog-ng を使えばタイムスタンプをひとつのフォーマット（たとえば ISO 8601 標準）にすることが可能になり、SSB がアプリケーションやリモートホストからの受信日付を使用できるため、保存されたメッセージはリモートホストやアプリケーションのクロックが不正確でも正確な日付情報を持ちます。Syslog-ng アプリケーションはマクロや強力なメッセージ再書き込み機能でメッセージをリフォーマットあるいはノーマライズし共通フォーマットに変換することによりメッセージのデータフィールドを他のメッセージと同じにできます。新たな IETF シスログプロトコルサポートにより SSB は全てのログメッセージとロギングクライアントを共通フレームワークに統合できます。
- “メッセージ転送における整合性と機密性” ログメッセージはネットワークセキュリティの観点から重要です。ログメッセージはパスワード、ユーザー名などの機密情報や個人情報を含むことがあります。そのため、これらの情報はネットワーク転送の間、盗聴から保護されなければなりません。通信者間（メッセージ送信ホストと中央サーバー）の識別が重要であり、サーバーが目標ターゲット（ログサーバー）だけに受信されたか、サーバーが受信したメッセージが本当にクライアントホストから送信されたかを確実にしなければなりません。メッセージの整合性を確保することにより、未承認者によるメッセージ改竄が皆無であることが補償されなければなりません。この点に関して Syslog-ng PE アプリケーションはセキュアな TLS プロトコルで SSB との通信を暗号化します。Syslog-ng PE クライアントとサーバーは X.509 証明で認証されます。
- “ログサーバーに保存されたメッセージの整合性と機密性確保” ログメッセージはログサーバーによる受信後も、操作や未承認アクセスを許可すべきではありません。そのため SSB はログメッセージを暗号化しデジタル署名付ファイルとして保存します。ログファイルの暗号化により、ログファイルは複合化キーを持つ管理者以外によるアクセスは不可能です。デジタル署名により勝手なメッセージ変更ができません。ログメッセージ時刻信頼性のために外部時刻認証局（TSA）にタイムスタンプを要求することもできます。
- “メッセージロスがないことを確実に” Syslog-ng PE アプリケーションは全メッセージにユニークな ID を付けネットワークやシステム障害によるメッセージロスがないことを確実にします。Syslog-ng PE は、ログサーバーが受信できるようになるまで、未送信ログをローカルハードディスクに保存します。Syslog-ng PE と SSB はメッセージのフローコントロールが可能です。フローコントロールとはあて先サーバーやデータベースが過負荷になると、Syslog-ng PE や SSB がアプリケーションやホストからのメッセージ受信を停止できるということです。このようにして送信側はログインフラの問題を知ることにより、その対応ができます。たとえば、ポリシーコンプライアンスにより全イベント記録が必要な環境では、アプリケーションはログインフラ回復ま

で一時的に停止します。そのためログ記録のないアクションは存在しません。サーバーダウンタイム処理の代案として Syslog-ng PE はプライマリーサーバーが使用できるまでバックアップサーバーにログメッセージを送信できます。サーバー側でのログ喪失を避けるため SSB アプライアンスはディスクホットスワップ可能な RAID でディスク障害対策を行い、さらにファイルオーバークラスタ構成による HA サポートも行います。クラスタのノードは自動同期される一般的なブロックデバイスサブシステムを使用します。さらに、SSB は受信メッセージをリモートバックアップサーバーに繰り返しアーカイブします。

- “ログメッセージ解析の SIEM デバイス補助” ログ解析はネットワークセキュリティにとっての基本要素です。SSB はログ解析アプライアンスではありませんが、いくつかの機能があります。ログ解析エンジンのためのメッセージ規格化も含まれています。Syslog-ng アプリケーションは強力なメッセージフィルターとソート機能で、些細で重要度の低いメッセージを無視できます。メッセージフィルターはクライアントでも可能であり、重要でないメッセージの廃棄で貴重なネットワーク帯域を節約でき、同時に SIEM デバイスの負荷を減らすことができます。また、ログ解析アプリケーション能力には限度があるため SSB はメッセージ送信速度を制限できます。これはメッセージバーストを平準化し、ログ解析エンジンの過負荷を防ぎます。ある SIEM デバイスはログをデータベースから読みますが、SSB はログを直接データベースに送信します。最も人気のあるデータベース、MSSQL, MySQL, Oracle, PostgreSQL をサポートします。SSB と Syslog-ng のさらに強力な機能はメッセージを殆どリアルタイムに分類し、結果を人工的に無視できることです。ログトラフィックに現れるログメッセージのパターンデータベースを生成でき、それらに普通、セキュリティ関連、違反などのラベルをつけ、全ての受信メッセージをこのデータベースと比較できます。重要というラベルのあるメッセージは必要であればアラートを生成でき、ネットワークで初めてのメッセージでありそのため重要な道のメッセージ、はレビューのために収集できます。
- “メッセージ保存” 組織はしばしば長期間ログメッセージを保存し、すぐには判明できなかったセキュリティインシデントのレビューに使用します。いくつかの規制は数ヶ月や数年のログ解析が可能であることを要求します。ログトラフィックが非常に多い場合（たとえば1時間当たりの生ログが数 GB の場合）ログメッセージ保存は重大な問題です。保存ログを減少させるために SSB は強力なメッセージフィルターとソート機能があります：重要でないメッセージを廃棄あるいは分離し、送信ホスト、アプリケーション、内容により異なるファイルやデータベースに再編します。ログファイルを自動的に圧縮、暗号化し、周期的に新たなファイルを作成し、古いファイルをアーカイブしサーバーから削除します。SSB は大容量 HDD を持ち（最大 10TB）、iSCSI やファイバーチャンネルインターフェイス経由で SAN に直接接続することも可能です。

3　ポリシーコンプライアンスにSSBを使用

いくつかの分野で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、工業基準はセキュリティへの考慮や機密データの保護の必要性を増しています。結果的に企業はビジネスプロセスの管理や監査能力を強化させなければならなくなり、完全なログ管理が必要になりました。特にいくつかの規制は集中化ログ収集（数年に及ぶログ保存必要とすることもある）を要求しています。

SSB と Syslog-ng PE ログ収集アプライアンスは完全で、信頼でき、安心できるログインフラを生成するツールになります。クライアントからのログメッセージを中央ログサーバーに収集し、多くの OS からのログメッセージのセキュアなログ転送と保存を確実にします。

3.1　PCI-DSSコンプライアンスとログ収集

下記の表は PCI-DSS のログ管理と監査に関する詳細な要件です。他の規制、SOX や Basel II、も同様な要件を必要とします。

PCI 要件	SSB のサポート
3. 保存したカード所有者データの保護すること	シスログには PIN やカード所有者コードなどの機密情報を含む可能性があります。これらのメッセージは一般的には平文テキストとして保存されますが、SSB は暗号化ファイルに保存することにより保護します。Syslog-ng のメッセージ書き換え機能により自動的に機密情報を削除することも可能です。
4. オープンな公共ネットワーク経由カード所有者情報を転送する場合は暗号化すること 4.1 SSL/TLS/SSH のような強力な暗号化でセキュアなプロトコルを使用すること	クライアントとログサーバー間転送は TLS で暗号化でき、メッセージの整合性を保護できます。TLS 暗号化の使用で第三者による通信データのアクセスと改竄から保護できます。Syslog-ng クライアントとログサーバー間は X.509 証明書で相互認証でき、通信者間の識別が可能なためログファイルへの偽メッセージの挿入を防止できます。

10.2 全システムに自動監査証跡機能を必要とすること	ログメッセージはアプリケーション、ホスト、ネットワークのイベントを再構築するために重要な役割を果たします。このプロセスを確実にするため Syslog-ng は中央ログサーバーで受信したログメッセージの改竄を確実に防御できるように考慮されています。メッセージはセキュアな TLS プロトコルで送信できますが、これは信頼できる TCP ネットワークプロトコルをベースにしており、ログサーバーによるメッセージ受信を確実にしています。Syslog-ng PE のディスクベースバッファリングはクライアント HDD でのメッセージバッファを行い、ログサーバーへのネットワーク接続が不可能な場合でもメッセージ喪失は避けられます。SSB は送信ホストとアプリケーションベースの監査証跡でメッセージを編集できますので、Web ベース検索インターフェイスからログメッセージを閲覧し、目的のログメッセージを取り出し、イベントの詳細を発見が簡単です。 自分自身の監査証跡として、SSB は設定変更のすべてを記録し、管理者に変更ログエントリーを要求できます。これらのログメッセージは独立して保存され、変更や監査を容易に行えます。SSB 管理者は LDAP データベース（たとえばアクティブディレクトリ）による認証も可能です。SSB は Syslog-ng PE ログ収集クライアントの設定が変更されたら自動的に通知を受けることが出来ます。

10.3 全システムコンポーネントの各イベントに対し少なくとも下記の監査証跡を記録すること 10.3.1 ユーザーID 10.3.2 イベントタイプ 10.3.3 日時 10.3.4 成功もしくは失敗情報 10.3.5 イベント発生元 10.3.6 影響されるデータ、システムコンポーネント、またはリソースIDまたは名前	Syslog-ng PE アプリケーションはこれらの情報のないログに自動的に下記を追記できます: ■ 各種標準フォーマットの日時(たとえばISO)と時間帯情報 ■ マクロを使用したカスタマイズ可能な日時情報 ■ メッセージを生成したクライアントホスト名 ■ メッセージを生成したアプリケーションやファシリティ名 SSB は管理者がその設定を変更するといつでもその要求を自動記録します。管理者 ID は LADP データベース(アクティブディレクトリなど)で認証できます。管理者が SSB にアクセスした IP アドレスも記録されます。
10.4 時刻同期技術により、すべてのクリティカルシステムクロックと時刻を同期し、受取、配信、保存時刻が確実であること	Syslog-ng PEサーバーはメッセージ受信日時を自動追加できるためログメッセージは正確な時刻情報を含みます。クライアントホストやアプリケーション時刻が不正確でも問題ありません。SSB自身はNTPサーバーのシステムクロックに同期します。
10.5 監査証跡は変更されないこと	すべてのログメッセージは中央ログサーバーのログストアファイルに公開鍵暗号化して保存することが出来ます。Syslog-ng アプリケーションは保存データのタイムスタンプを外部の時刻認証局(TSA)に要求しログファイルに信頼できる日時を含むことが出来ます。
10.5.1 監査証跡閲覧を業務関係で必要な場合に制限できること	SSB の詳細な権限管理機能は、ログメッセージアクセスの必要な人だけにアクセスを限定できます。暗号化されたログメッセージは必要な復号鍵の所有者以外は閲覧不可能です。

10.5.2 未承認変更から監査証跡ファイルを保護すること	SSB ログサーバーはログメッセージを暗号化ログストアファイルに保存でき、改竄を防止するためにデジタル署名をつけることが出来ます。メッセージの整合性はクライアントからサーバーへの転送時もチェックされます。Syslog-ng クライアントと SSB 間の通信は X.509 証明書で相互認証でき、ログインジェクション攻撃からの防御になります。
10.5.3 監査証跡は中央ログサーバーや変更不可能なメディアに速やかにバックアップできること	SSB アプライアンスはまさにこの目的のための製品です。ログメッセージを信頼できるソースから受信し、暗号化し、デジタル署名とタイムスタンプを付け、ログファイルを改竄されないようにするためのログサーバーです。 ログメッセージの喪失を防ぐため、SSB は信頼できる TCP ネットワークプロトコルでメッセージを受信できます。ネットワーク転送中の第三者によるアクセスや改竄を防ぐため、クライアントは相互認証や TLS 暗号化接続でメッセージを送信できます。 ログサーバーが連続して処理可能であることを保障するため、SSB アプライアンスは HA クラスタ構成をサポートします。これは主サーバーの障害時に待機サーバーがオンラインになるものです。メッセージ喪失のリスクを最小限にするために SSB クラスタは共通ディスクサブシステムを採用しています。 SSB は標準シスログプロトコル（RFC3164, RFC5428）を使うどのクライアントアプリケーションからでもログメッセージを受信できます。しかし可能な限り Syslog-ng PE ログ収集アプリケーションを利用してください。 ネットワーク障害の

	間、Syslog-ng PE はメッセージを HDD にバッファし、ログサーバー回復後メッセージを送信します。ログトラフィック量とホストの HDD 容量に依存しますが、長期間のネットワークダウンにも、メッセージは保全されます。
10.5.4 無線ネットワークのログを内部 LAN のログサーバーにコピーできること	Syslog-ng PE アプリケーションは無線デバイスから受信したログメッセージをリレーし、中央ログサーバーに転送できます。
10.5.5 ログの整合性監視と変更検出ソフトウェアで既存ログデータが変更されたらアラートを送信すること(新たなデータの追加ではアラートを出さない)	クライアントとログサーバー間を TLS 暗号化することによりログメッセージはネットワーク上では改竄されません。ログサーバーでは、Syslog-ng は特別な暗号化、デジタル署名ログファイルとして保存できるため改竄されません。保存データには外部時刻認証局(TSA)のタイムスタンプを要求できます。設定を変更すると Syslog-ng PE アプリケーションは自動的にログメッセージを送信しますので、ログインフラ監査が容易になります。
10.7 監査証跡の履歴は 1 年以上保存し、3 ヶ月以上はオンライン利用できること	SSB のログストアに保存したログメッセージはディスクスペース節約のため圧縮できます。リモートサーバーにアーカイブされたメッセージはサーバーがオンラインであれば、いつでも SSB Web インターフェイスから利用できます。 SSB は大容量内部 HDD を持ちますが、直接外部 SAN システムにも接続できます。

3.2 COBIT 4.1 コンプライアンスとログ収集

COBIT にとってログインフラコンプライアンスは、それほど要求が強くありませんが、重要です。他の規制(SOX, Basel II など)が正確な技術要件を指定していないけれども、よく整備された COBIT

のようなフレームワークを採用しているからです。

下記のテーブルは COBIT 4.1 のいくつかのオブジェクト管理を議論します。組織のログインフラにどのように影響し、どのように Syslog-ng PE が要件を満たすかということです。このリストは退屈なものでなく、他の要件もログインフラとログ管理に適用できることを理解してください。

** テーブルは省略します

4 HIPAAコンプライアンスとログ収集

HIPAA はログに関する直接要件は多くありませんが、ネットワーク経由のログ転送とコンピュータへの保存について機密情報の保護と暗号化を含みます。ログにはそのような情報を含みますので、ログインフラはこれらの要件に準拠しなければなりません。

下記の表は HIPAA のいくつかの要件について、それらが組織のログインフラに影響し、どのように Syslog-ng PE が要件を満たすかについて議論します。このリストは退屈なものでなく、他の要件もログインフラとログ管理に適用できることを理解してください。

** テーブルは省略します

5 その他の重要機能

ここでは今まで詳細に説明できなかったが有用な機能に焦点を当てます。

5.1 SSBを管理する

SSB はきれいで直感的な Web インターフェイスから設定できます。権限セットにより SSB の各管理者権限を明確に定義できます。SSB 全体、ログ収集、転送と保存、アラート設定、ログレポート閲覧権限などです。

Webインターフェイスは管理トラフィック専用のネットワークインターフェイス経由でアクセスできます。この管理インターフェイスはバックアップ、アラート送信、その他の管理トラフィックでも利用できます。すべての設定変更は自動的に記録されますので、SSB監査業務がすっきりします。

5.2 繊細なアクセス制御

SSB Web インターフェイスでアクセス管理の高度なカスタマイズが可能です。Syslog-ng の強力な

メッセージソート機能と共に利用することにより、ユーザーがどのメッセージにアクセスできるかを正確に設定できます。たとえば、特定のアプリケーションログへのアクセス権をそのアプリケーションのサポートエンジニアだけに許可できます。適切な時間だけデータにアクセスできるように時間帯を制限できます。

5.3 LDAP統合

SSB はリモート LDAP データベース（たとえばアクティブディレクトリサーバー）に接続し SSB Web インターフェイスを使用するグループメンバー権限を解決できます。SSB 設定や異なるログ閲覧権限をグループメンバー権限ベースで定義できます。

5.4 リアルタイムログ監視とアラート

SSB はログ解析エンジンではありませんが、人工的にメッセージを無視することにより、Unix のログチェックアプリケーションのようにログを分類できます。SSB は“normal”というログメッセージパターンを持つ組み込みデータベース付で出荷されます。アプリケーション実行中（たとえば Sendmail, Postfix, MySQL）これらのパターンに一致するメッセージが生み出され、あるメッセージはログ監視の観点から重要でないと判断され、残りは”interesting”となります。管理者は SSB インターフェイスでログパターンを定義でき、ラベルに一致するメッセージ（たとえばセキュリティイベントなど）に、特定のパターンが認められたらアラートを要求します。完全なログ解析のためには SSB は受信ログを外部ログ解析エンジンに転送できます。

5.5 多数のプラットホームに対応するログコレクタエージェント

SSB は Syslog-ng アプリケーションを使って異なる OS やプラットホームのログを収集します。Linux, Unix, BSD, Sun Solaris, HP-UX, IBM AIX, IBM System i, Windows XP, Server 2003, Vista や Server 2008 を含みます。

5.6 Windowsプラッホーム用エージェント

Windows 用 Syslog-ng エージェントはマイクロソフト Windows プラットホーム用、Windows Vista や Windows Server 2008 を含む、ログ収集と転送アプリケーションです。イベントロググループやログファイルからログを収集し通常あるいは TLS 暗号化 TCP 接続で Syslog-ng サーバーに転送します。Syslog-ng エージェントはグループポリシーを使ったドメインコントローラから管理でき、あるいはスタンドアローンアプリケーションとして実行できます。

5.7 IBM System i 用エージェント

IBM System i 用 Syslog-ng エージェントは IBM System i（以前の AS/400 と IBM i シリーズ)プラットホームのためのシスログ収集と転送機能です。アプリケーションとシステムメッセージ、System i

セキュリティ監査ジャーナル(QAUDJRN)とオペレータメッセージキュー(QSYSOPR)を収集します。収集したメッセージは通常または TLS 暗号化した TCP 接続で Syslog-ng サーバーに転送されます。Syslog-ng サーバーは別のマシンまたは PASE 環境で IBM System i で直接実行します。IBM System i 用 Syslog-ng エージェントはスタンドアローン製品として SSB と別にライセンスされます。

5.8 データと設定情報自動バックアップ

記録したログメッセージとSSB設定情報は下記のプロトコルで周期的にリモートサーバーに転送されます:

- NFS
- Rsync over SSH
- SMB/CIFS

最新のバックアップ、データバックアップを含み、は SSB Web インターフェイスから簡単にリストアできます。

5.9 自動データアーカイブ

SSB の設定情報と記録したログメッセージはリモートサーバーに自動的にアーカイブされます。リモートサーバーのデータはアクセスと検索が可能であり、SSB Web インターフェイスから数 TB のアクセスが可能です。SSB はリモートサーバーを NSF または SMB/CIFS 経由のドライブとみなします。

5.10 大負荷処理能力

SSB は大量のログを処理できるように最適化されています。コンフィグレーションに依存しますがリアルタイムに毎秒 75,000 以上のメッセージを処理できます。これは1時間当たり 24GB の生ログに相当します。インデックス付けや分類は毎秒 30,000 以上のメッセージを処理できます。大型アプライアンスは 10TB までのデータを保存できます。

6 その他

6.1 BalaBitについて

BalaBit IT セキュリティ社は高度な基準を満たすネットワークセキュリティソリューション開発会社です。BalaBit 社はハンガリーに設立され、ハンガリーに本拠地があります。主要製品は Syslog-ng であり、世界で最も広範に利用されています。BalaBit SCB は SSH< RDP< VNS< Telent などのトラフィックを透過的に管理、監査、再生できるアプライアンスです。

日本語マニュアル発行日　2011 年 11 月 11 日

本マニュアル原文は『Regulatory compliance and system loggig』です

ジュピターテクノロジー株式会社　翻訳グループ