PCIDSSセキュリティフォーラム ２０１６　分科会２０

# 『シスログ管理』と『監査証跡』PCI DSS要件への適合性

２０１６年　6月２２日（水）　１６：００～１６：４０

ジュピターテクノロジー

プロダクト３部　野口浩史

# 資料概要と目次

## 資料概要

情報漏えい事件が多発している昨今、セキュリティの観点からログの管理は重要です。また、再生可能な監査証跡の記録はログを補完します。
PCI DSS準拠のためのログ管理と監査証跡の重要性についてご説明します。

**目次**

# 1　シスログ管理サーバと証跡管理


## 超高速シスログサーバー「syslog-ng Store Box」

syslog-ngベースの超高速・高機能ログ管理アプライアンスです。
PCI DSS 等のコンプライアンスとシステム管理のためのログインフラを必要とする企業向けのログ収集・分類・再編と安全な保存のための製品です。

http://www.jtc-i.co.jp/product/ssb/ssb.html


## エージェントレス証跡管理「Shell Control Box」

特権ユーザーによるサーバーアクセスの監視と監査のためのプロキシゲートウェイです。
サーバーとクライアント間に設置するだけで動作するエージェントレスなシステムで、今の環境を変更することなく、サーバーへのアクセスを監視、制御します。

http://www.jtc-i.co.jp/product/scb/scb.html

BALABIT

*„The syslog-ng company"*

BalaBit IT Secrity 社は、全世界で100万以上のユーザー数を持つオープンソースログサーバーアプリケーション「syslog-ng」の開発元として広く知られています。

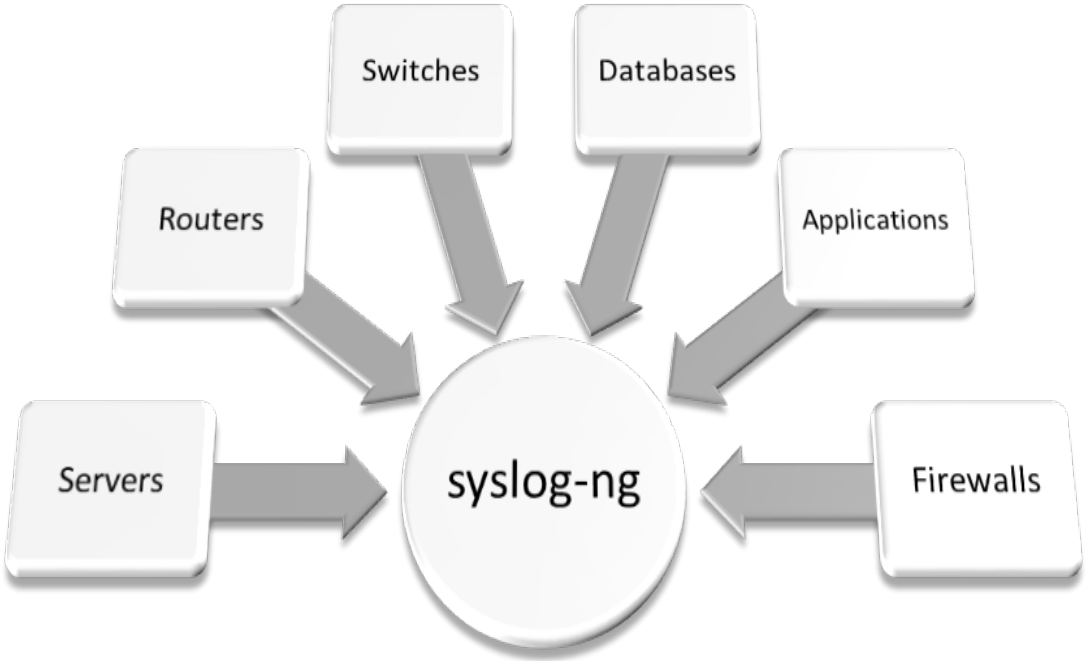
# 2　PCIデータセキュリティ基準と適合性

| PCI DSS 要件 | syslog-ng Store Box | Shell Control Box |
|---|---|---|
| **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 | 1.1.1 | |
| 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提供のデフォルト値を使用しない | 2.2.1、2.2.2 | |
| **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 | 3.4 | |
| 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 | 4.1 | |
| **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 | 5.2 | |
| 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 | | |
| **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 | | 7.1、7.2 |
| 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 | | 8.1.1、8.1.5 |
| 9.　カード会員データへの物理アクセスを制限する | | |
| **ネットワークの定期的な監視およびテスト** | | |
| 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 | 10.1～10.7 | 10.1～10.7 |
| 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 | | |
| **情報セキュリティポリシーの維持** | | |
| 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 | | |

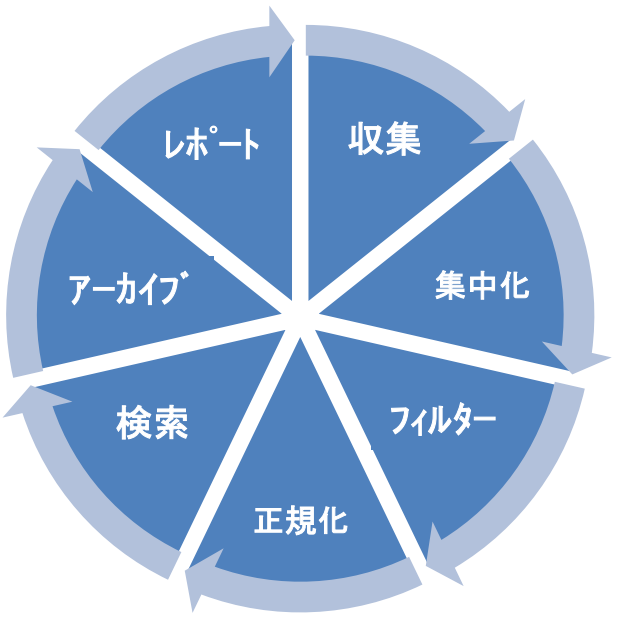
# 3　PCI DSS 要件１０とログ管理

■ログ記録メカニズムおよびユーザの行動を追跡する機能は、データへの侵害を防ぐ、検出する、またはその影響を最小限に抑えるうえで不可欠です。

⇒監査証跡のためのログ管理サーバは、基本的なツールです。




※「syslog-ng」はよりセキュアで信頼性の高いsyslogデーモンです。

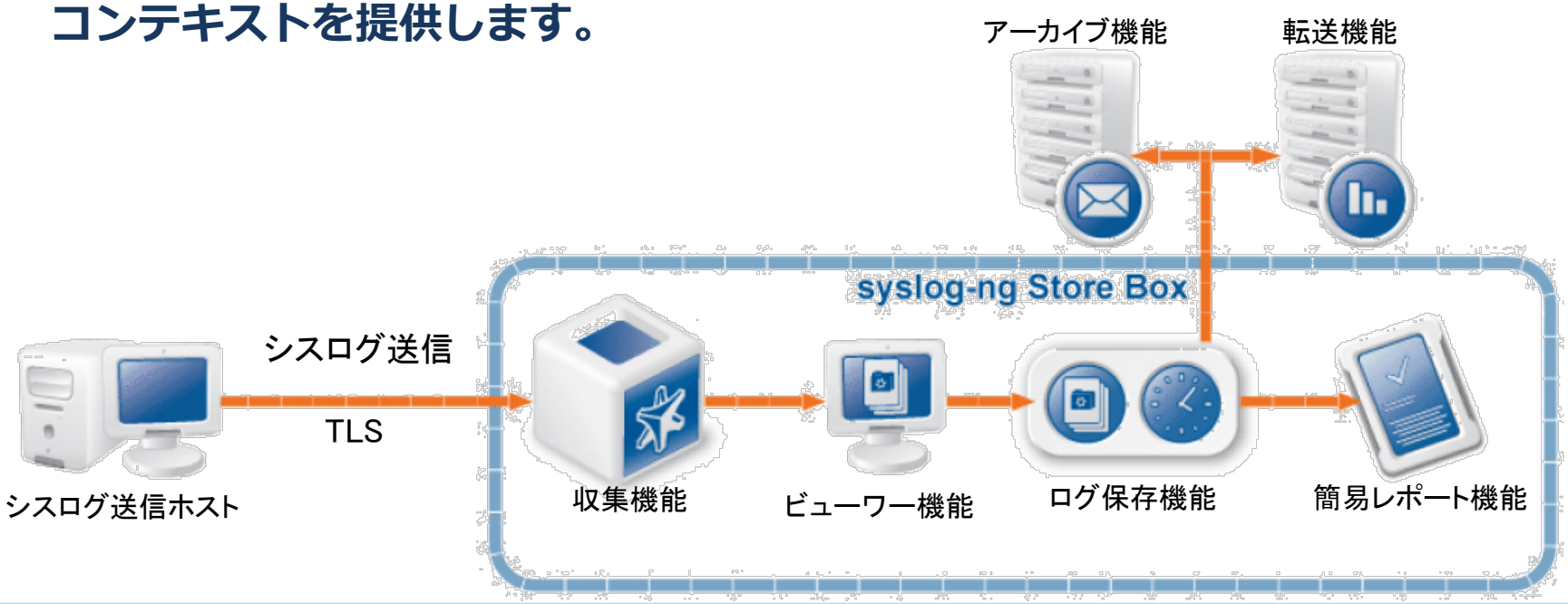



シスログ管理サーバの主な機能

# 4　シスログ管理サーバの適合性

| | |
|---|---|
| 要件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にリンクする監査証跡を確立する |
| 要件10.2 | イベントを再現するため、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 |

**⇒ユーザアクセスとシステムコンポーネントをリンクするシスログ管理サーバは基本的なツールで、生成ログは悪意のある活動を識別・追跡するためのコンテキストを提供します。**



# 5　ログ詳細情報の収集・正規化・検索

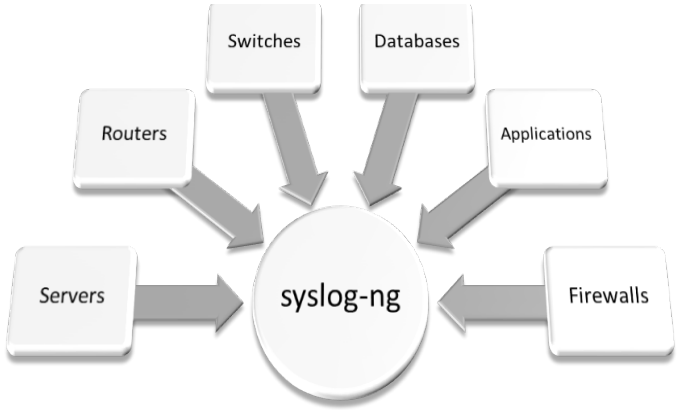
**要件10.3**

**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次の監査証跡エントリを記録する**

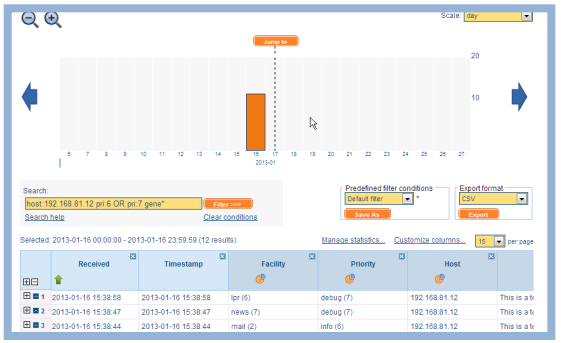
**「ユーザID」「イベントの種類」「日付と時刻」「成功または失敗を示す情報」「イベントの発生元」「影響を受けるデータ、システムコンポーネント、またはリソースのIDまたは名前」**

```
<30>Feb 2 03:40:01 abc rsyslogd: [origin software="rsyslogd" swVersion="5.8.10" x-pid="993" x-info="http://www.rsyslog.com"] rsyslogd was HUPed
```

```
192.168.1.1 - - [28/Feb/2014:03:15:54 +0900] "GET /support/customerportal/index.php HTTP/1.1" 200 124 http://www.jtc-i.co.jp/index.html
 "Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/7.0)" "-"
```




**syslog-ng Store Box の検索画面**



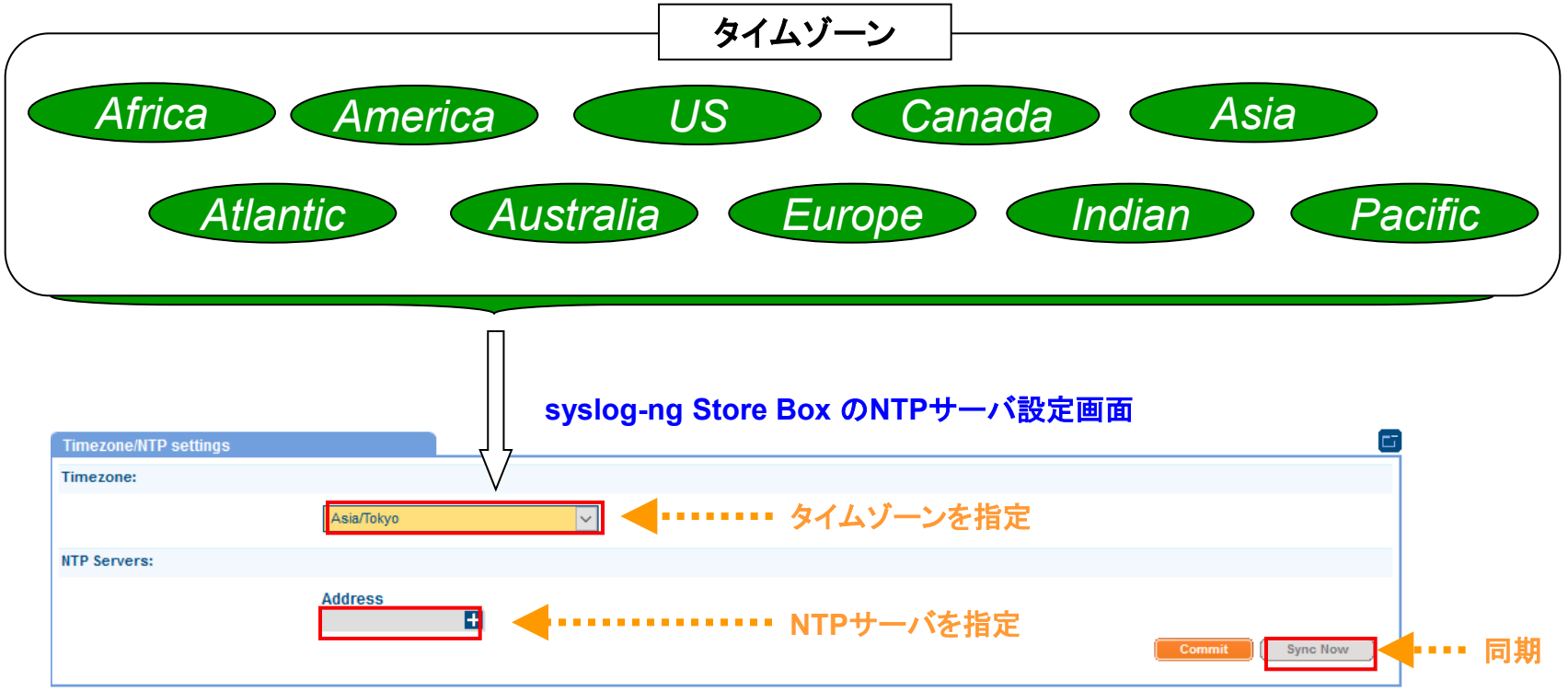
収集　→　正規化　→　検索

**⇒共通なフォーマットに変換し、直感的な検索インターフェースを使用することで、潜在的な出来事を識別するために必要な時間を短縮できます。**

# 6　ログメッセージの時刻同期

**要件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させる**

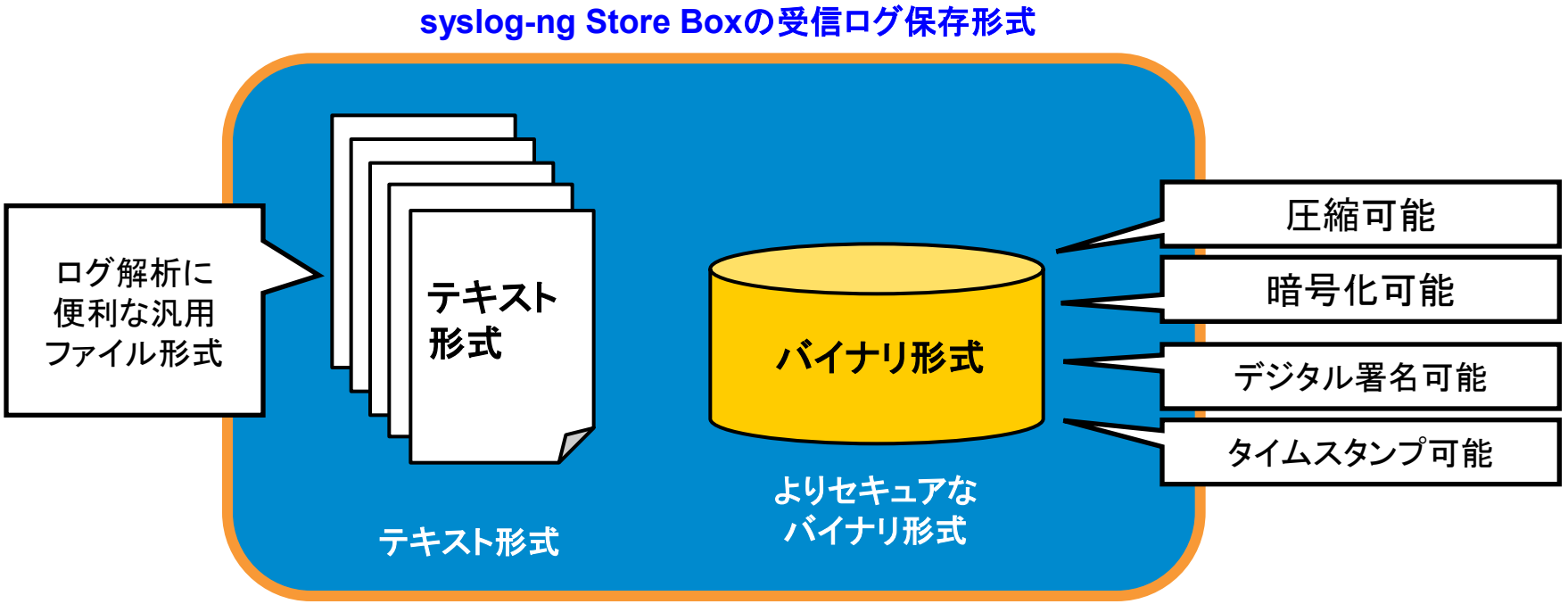



**⇒タイムスタンプを単一のフォーマットに変換し、シスログ管理サーバ自身がNTPサーバへシステムクロックを同期させることが必要です。**

# 7　ログメッセージの暗号化とデジタル署名

**要件10.5**　変更できないように監査証跡をセキュリティで保護する

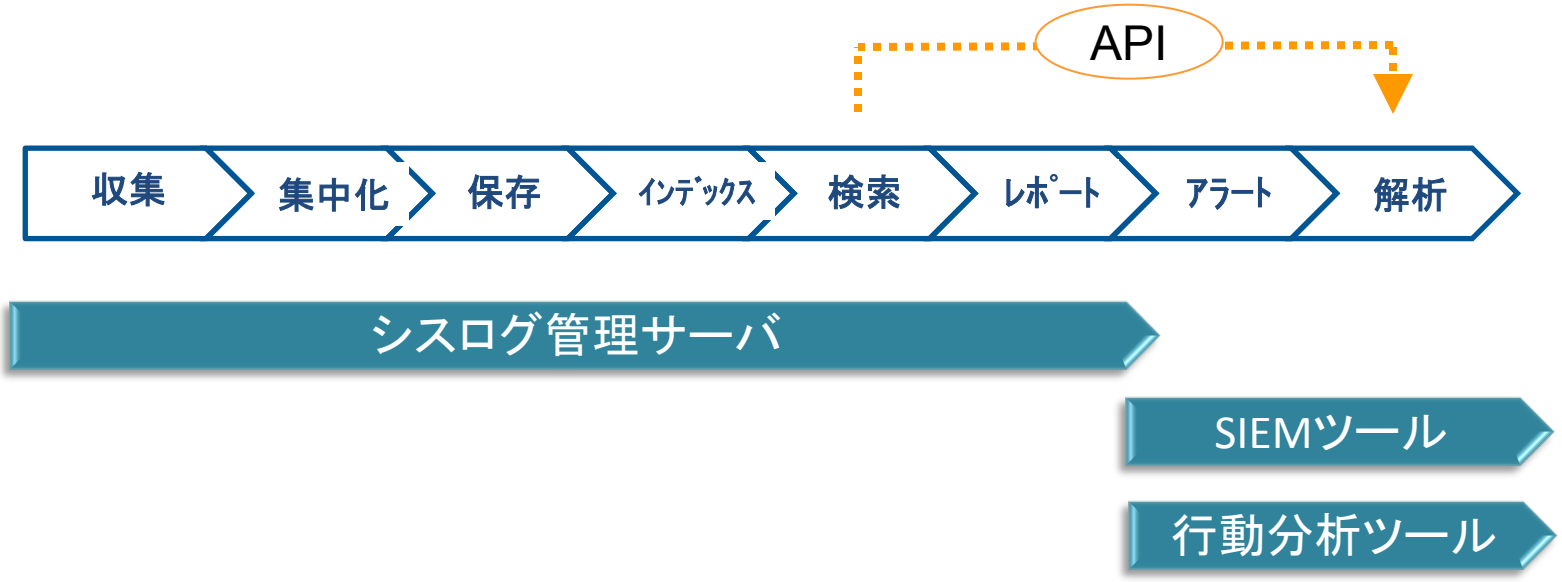
**⇒ログメッセージを公開鍵暗号方式で暗号化、デジタル署名、タイムスタンプは、安全なログ一元管理サーバを提供します。**



# 8　ログの定期的レビュー

**要件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**

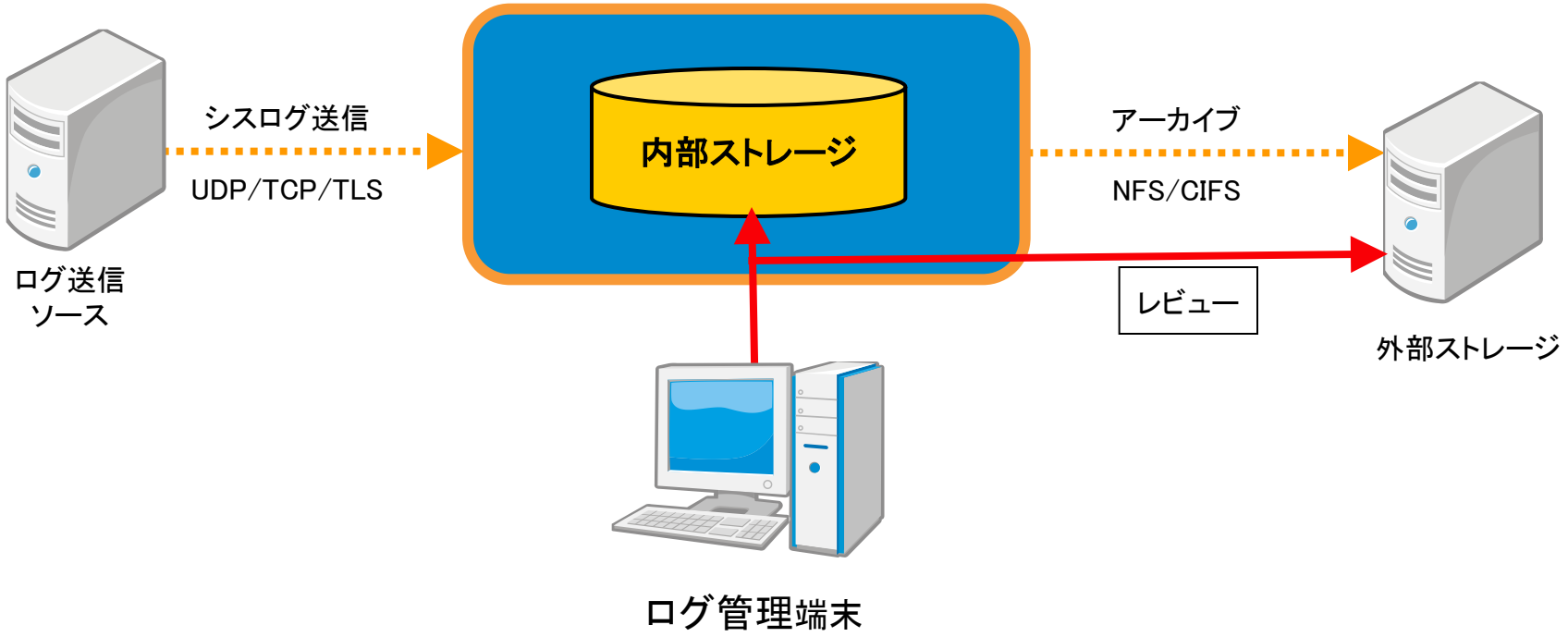



**⇒毎日ログをレビューしインシデントの危険性と被害を軽減するには、収集したログの素早い検索や解析・警告ツールとの統合が必要です。**

# 9　ログメッセージのアーカイブ

**要件10.7**

**監査証跡の履歴を少なくとも１年間保持し、少なくとも３ヵ月はすぐに分析できる状態にしておく**




**⇒シスログ管理サーバには、ログメッセージを自動的に外部ストレージにアーカイブする機能が必要で、ログデータはすぐに利用できる必要があります。**

# 10　ログメッセージ・伝送路の暗号化

**要件３.４**

**すべての場所で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）**

**⇒PANデータをログに含む必要がある場合は、強力な暗号化を使用してログメッセージをバイナリでタイムスタンプ付きのファイルで保存が必要です。**

**syslog-ng Store Box (SSB)**

暗号化・デジタル署名・タイムスタンプ可能

**要件4.1**

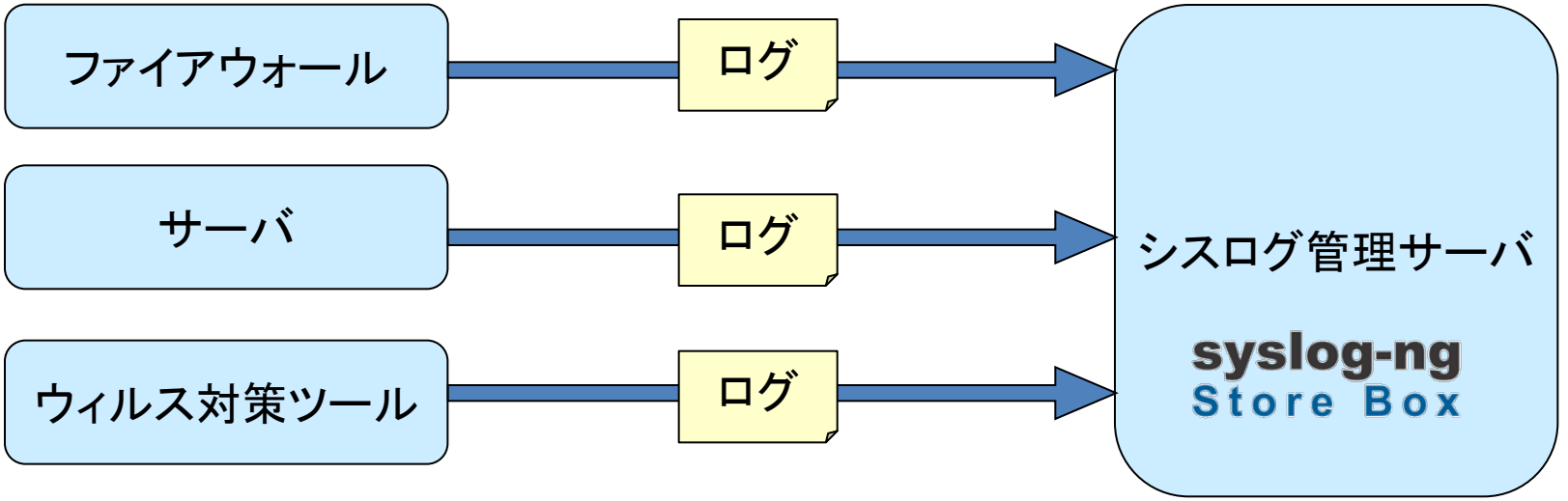
**公共ネットワーク経由で機密性の高いカード会員データを伝送する場合、強力な暗号化とセキュリティプロトコルを使用して保護する。**

**⇒ログを送受信する場合は、TLS v1.1 以降のセキュリティプロトコルをサポートする必要があります。**

**syslog-ng Store Box (SSB)**

TLS1.1、1.2サポート
（Webインターフェースも対応）

# 11 監査ログの間接的な効果




**シスログ管理サーバの役割**

■設定の変更をファイアウォールのログメッセージに記録できます。　【要件1.1.1】

■サーバログを示すレポートは、サーバが単独で主要な機能を実行していることを証明します。　【要件2.2.1、2.2.2】

■ウィルス対策メカニズムは、監査ログを生成・保持する必要があります。【要件5.2】

# 12　情報漏えいは“内から”起こる？！

## ■情報漏えいの80%は、内部要因で生じています

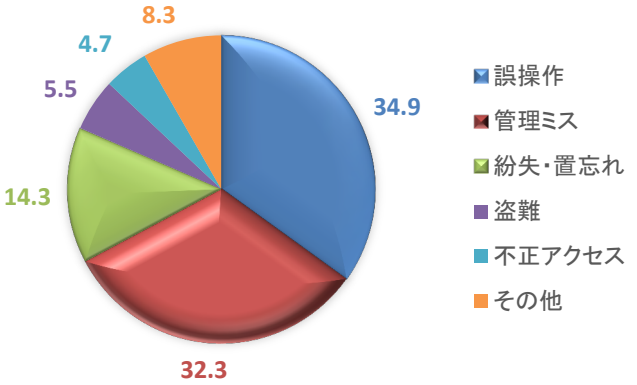
不正アクセスなどの外部要因によるものというイメージの強い情報漏えいですが、実際には多くの情報漏えい事案が内部要因によって発生しています。

日本ネットワークセキュリティ協会の「2013年情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～」によると、**情報漏えいの約80%が内部要因**によって発生しています。

情報漏えいの発生は、信用の失墜や多額の賠償請求に直結する可能性が高いため、ウィルス対策ソフトの導入などで外部要因への対応を進めるだけでなく、内部要因への対策も進めなければなりません。

その一環として、厳格なセキュリティポリシーを定めたうえで、ポリシー順守を徹底している企業が多く見受けられます。

**「誤操作」「管理ミス」「紛失・置き忘れ」といった内部要因が約80%を占める！**




日本ネットワークセキュリティ協会「2013年情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～」をもとに作成

**⇒セキュリティポリシーの順守を徹底する手段としては、ログ管理ツールの導入が一般的です。**

# 13　監査証跡に求められる新たな要件

## ■適切な情報を最適なタイミングで入手できるのが新しいトレンド

従来のログ管理ツールが抱える「“ログ”の限界」を超えるには、以下に挙げる2つの要件を満たした新たなツールの活用を検討する必要があります。

**ログの限界を超えるために必要な2つの要件**

**要件①　収集だけでなく、きちんと活用できること**

**要件②　ユーザーの操作を、漏れなく監視できること**

ひとつ目の要件は、**「収集だけでなく、活用できること」**です。

従来のツールが出力するログをすべてチェックすることは、現実的には不可能です。しかし、もし**一瞬で意味を把握できるログ**があればどうでしょうか。さらにはそのログを分析したり、**アラートを自動で生成**したり、**ルールに従って行動を制御**するツールがあればどうでしょうか。このようなツールがあれば、管理者はログをただ集めるだけでなく、きちんと活用することで、自社の情報資産を最低限の負荷で効果的に守ることができます。

次に、**「ユーザーの操作を、漏れなく確実に監視できること」**です。セキュリティリスクの要因は、どこに隠れているか分かりません。従来のツールではログの残らない操作についても、**漏れなく監視できる**必要があります。

**⇒ユーザの操作画面を記録する“カメラによる監視”という形で2つの要件を満たした新たな証跡管理（監視ツール）が登場しました。**

# 14 ユーザ操作画面記録による証跡管理


⇒【記録】すべての操作を画像で記録することで、情報漏洩を抑止します

⇒【検索】キーワード検索で、操作の分析や調査が簡単になります

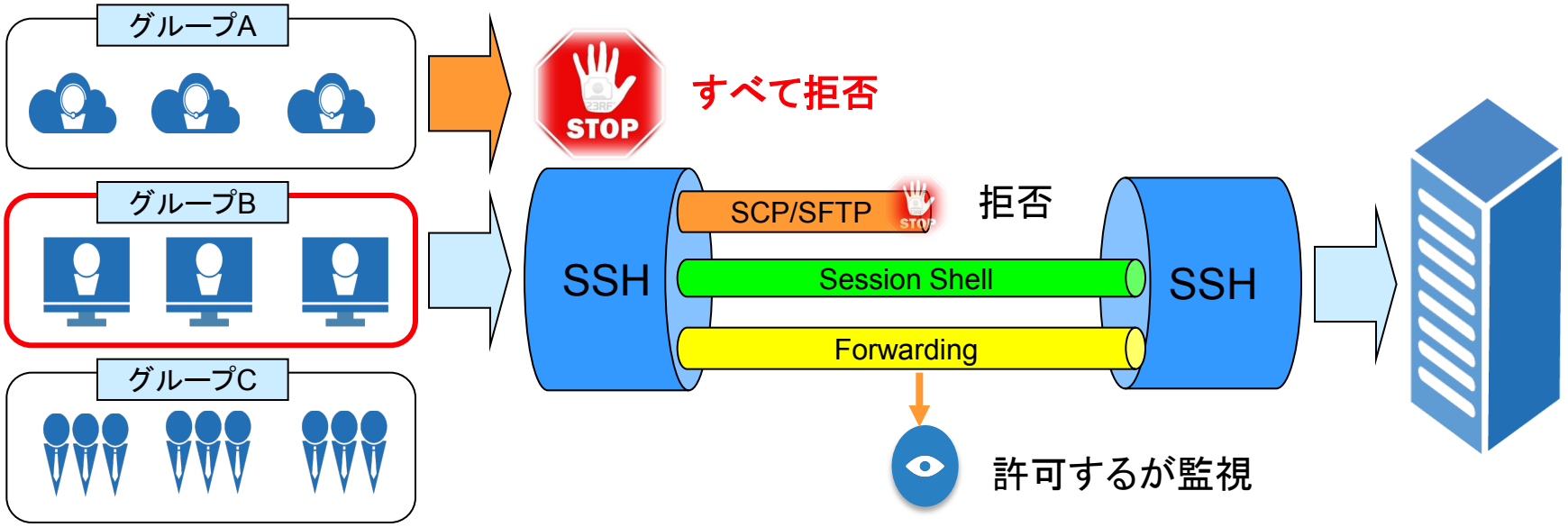
⇒【再生】いつ・誰が・何をしたのか、正確に再生し確認できます

⇒【アラート】アラート機能で、疑わしい操作をすばやく検出できます

# 15 業務上必要な範囲内にアクセス制限

**要件7.1** システムコンポーネントと会員データへのアクセスを、業務上必要な人に限定する

**要件7.2** システムコンポーネントで、ユーザの必要性に基づいてアクセスが制限された、アクセス制御システムを確立する




⇒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必要です。

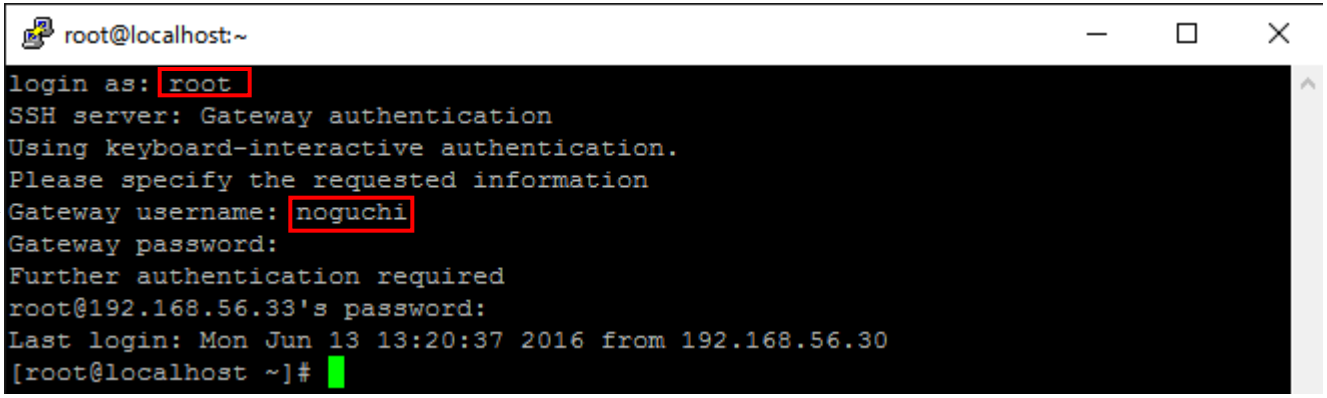
# 16 一意のユーザIDでの認証

**要件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、すべてのユーザに一意のIDを割り当てる**

一次認証 ➡

二次認証 ➡




| | | Verdict | Source IP | Server IP | Username | Username on server | Start time |
|---|---|---|---|---|---|---|---|
| 1 | ▶ | ACCEPT | 192.168.56.1 | 192.168.56.3 | demo01 | root | 2016-06-13 13:17:( |
| 2 | ▶ | CONN-AUTH-FAIL | 192.168.56.1 | | root | root | 2016-06-13 13:18:1 |
| 3 | ▶ | ACCEPT | 192.168.56.1 | 192.168.56.3 | noguchi | root | 2016-06-13 13:20:1 |
| 4 | ▶ | ACCEPT | 192.168.56.1 | 192.168.56.3 | noguchi | root | 2016-06-13 13:21:2 |

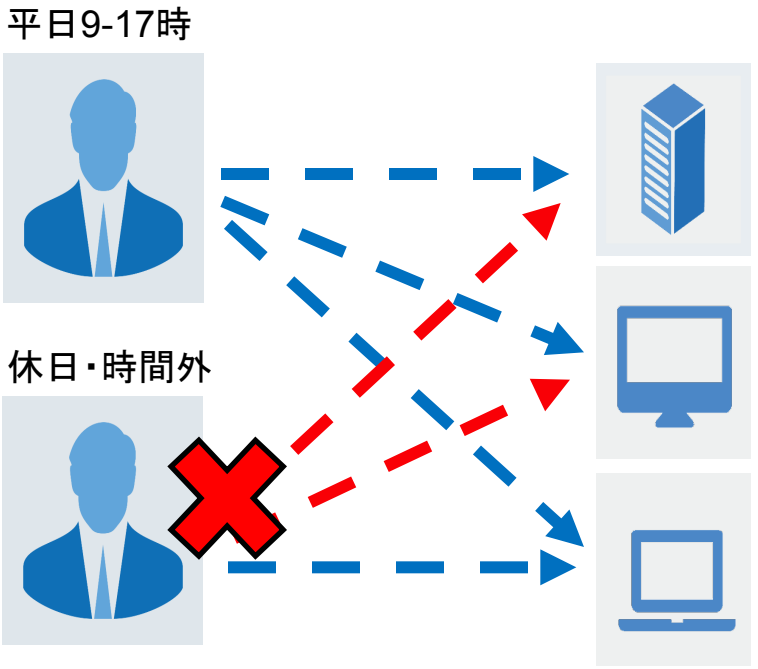
**⇒共有アカウントでアクセスしても、ユーザが所有する一意のユーザIDを使用して認証できます。**

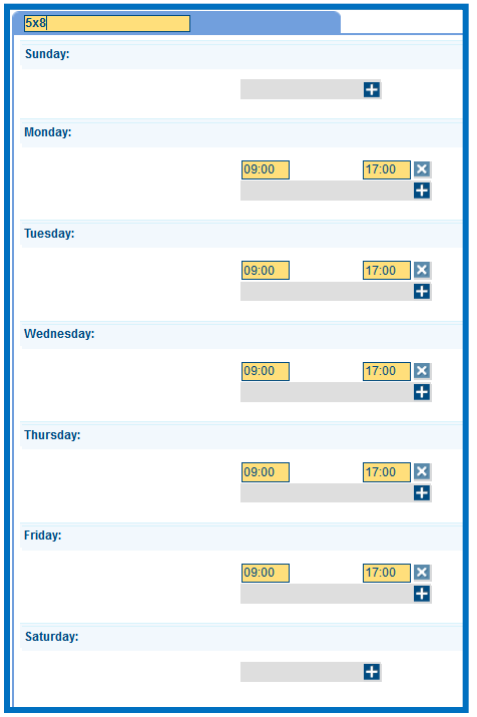
# 17 リモートアクセスの時間制限

**要件8.1.5**

ベンダがリモートアクセス経由でシステムコンポーネントのアクセス、サポート、メンテナンスに使用するユーザIDを管理する。

●必要な期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



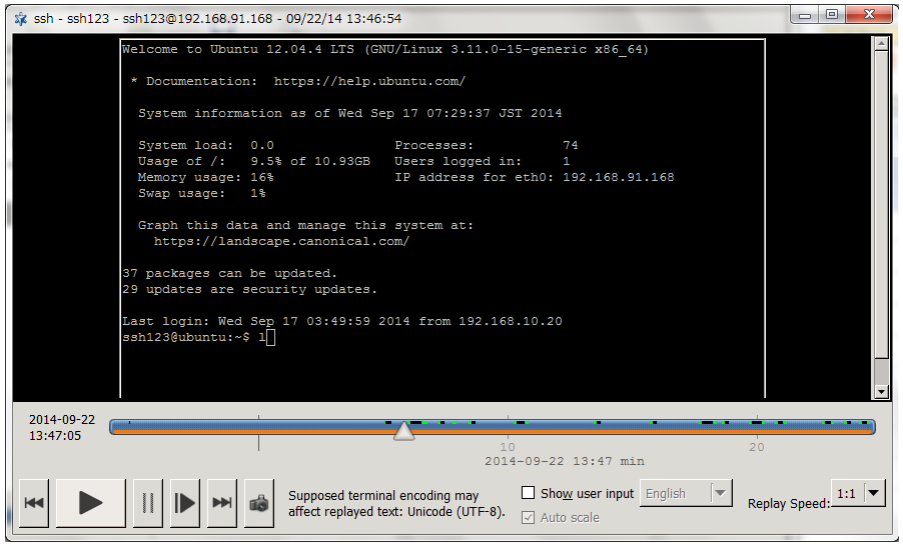

⇒指定された時間枠（例えば、スケジュールされたメンテナンス時間）の間だけアクセスを有効にするタイムポリシーが必要になります。

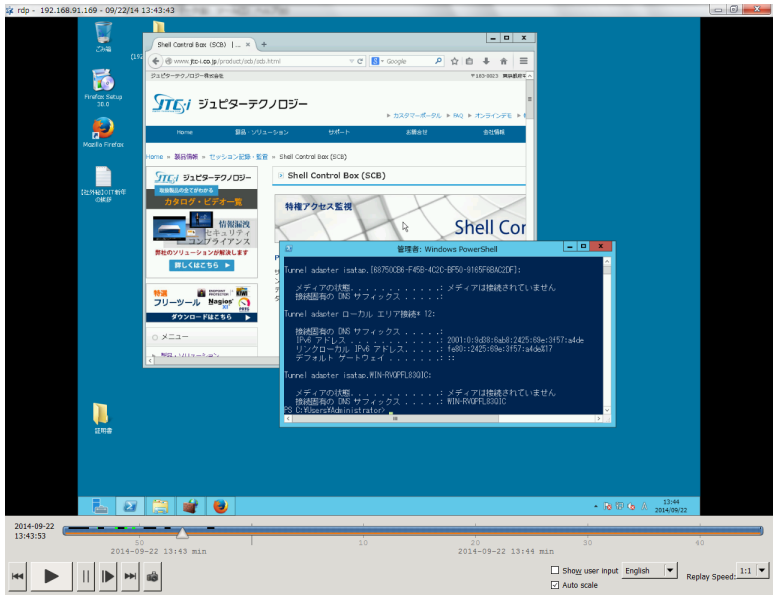
# 18 リモートベンダのアクセス監視

**要件8.1.5**

**ベンダがリモートアクセス経由でシステムコンポーネントのアクセス、サポート、メンテナンスに使用するユーザIDを管理する。**

- **使用時に監視されている。**




**⇒ベンダのアクセス時に、ユーザ操作画面をリアルタイムに再生できることは、不適当または有害な動作を監視するには有効です。**

# 19 アクセスの追跡および監視

**要件10** ネットワークリソースおよび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

- 特定のユーザアクセスを自動的に拒否できます【10.1】
- 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します【10.2】
- 保存した監査証跡は、実行権限のあるユーザだけがアクセスできます【10.2.3】
- 拒否された特定のアクセス試行を自動的に記録します【10.2.4】
- システムクロックをリモートタイムサーバに同期できます【10.4】
- すべての監査証跡は電子署名や公開鍵で暗号化されます【10.5】
- 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【10.6】
- 監査証跡をオンラインで保存できます【10.7】 等

⇒操作画面を記録し再生可能な監査証跡は、シスログ管理サーバを補完します

# 20 PCI DSSレポートサンプル（ご参考）

**BalaBit Shell Control Box - PCI DSS**

**Publication: 2015 April 13, Monday**

**2015-04-13 14:03**

**UTC offset: +0200**

**IP address: 10.50.10.184**

**Requirement 8.1.8**

**Requirement 8**

Identify and authenticate access to system components

**Requirement 8.1.8**

If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.

**SCB web interface timeout**

Idle connections to the **SCB web interface** are automatically closed after **15** minutes.

**Requirement 8.2.1**

Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.

**Passwords stored on SCB**

SCB stores passwords in the following locations:

- /initrd/mnt/grub/grub.cfg
  Hashed using PBKDF2-HMAC-SHA512
- /mnt/firmware/opt/scb/var/db/scb.xml
  Hashed using CRYPT_SHA512, and SNMP configuration stored in plain text
- /mnt/firmware/opt/scb/var/db/lcs.sqlite
  Hashed using SHA1
- /mnt/firmware/etc/shadow
  Hashed using SHA512 (salted)
- /mnt/firmware/etc/snmp/snmpd.conf
  Stored in plain text
- /mnt/firmware/etc/zorp/policies/credential_stores.py
  Hashed using CRYPT_SHA512
- /mnt/firmware/etc/zorp/policies/ldap_policy.py
  Hashed using CRYPT_SHA512
- /mnt/firmware/etc/zorp/policies/ssh/authentication_policies.py
  Hashed using CRYPT_SHA512
- /mnt/firmware/etc/zorp/policies/local_user_database.py
  Hashed using CRYPT_SHA512

**Requirement 10.5.3**

**Requirement 10**

Track and monitor all access to network resources and cardholder data

**Requirement 10.5.3**

Promptly back up audit trail files to a centralized log server or media that is difficult to alter.

**Local log messages**

SCB stores log messages locally. Every service is configured to send its log messages to syslog.

**Forwarding log messages**

SCB automatically forwards log messages to 10.50.1.11.

**Requirement 10.5.4**

Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.

**Forwarding log messages configurations**

| Nr. | Server IP | Port | Protocol |
|---|---|---|---|
| 1 | 10.50.1.11 | 514 | syslog-tcp |

**Forwarding log messages certificate configurations**

| Nr. | Server Key Check | CA x509 certificate | Client certificate |
|---|---|---|---|
| 1 | required_untrusted | Yes | No |

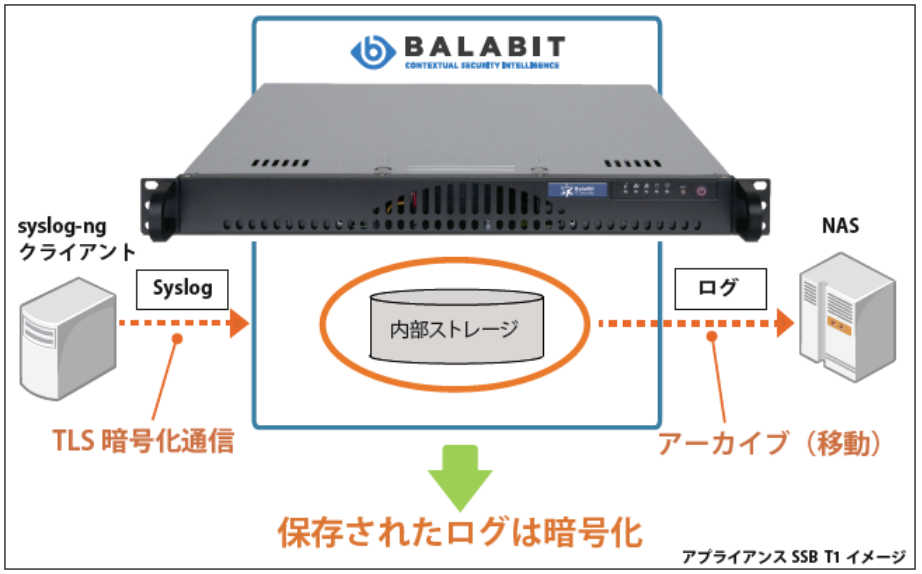
**Requirement 10.7**

Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis

**Log Retention**

Maximum retention time for local logs of SCB is **seven** days.

# 21 syslog-ng Store Box (SSB)




- 理論最大70,000メッセージ/秒の処理可能な超高速ログサーバーです
- ログを収集/保存する、信頼できる統合ログ管理アプライアンスです
- ログの送受信経路や保存ログデータを暗号化可能です
- 検索インタフェースやレポート・統計エンジンで、ログの調査や監査できます
- PCI DSS等のコンプライアンスに対応、最高水準の機密保護基準を満たします

「PCI DSS準拠とログ管理」のホワイトペーパーは以下URLよりダウンロードできます。

http://www.jtc-i.co.jp/product/ssb/ssb_pcidss.html

# 22 syslog-ng Store Box 導入事例

**目的**

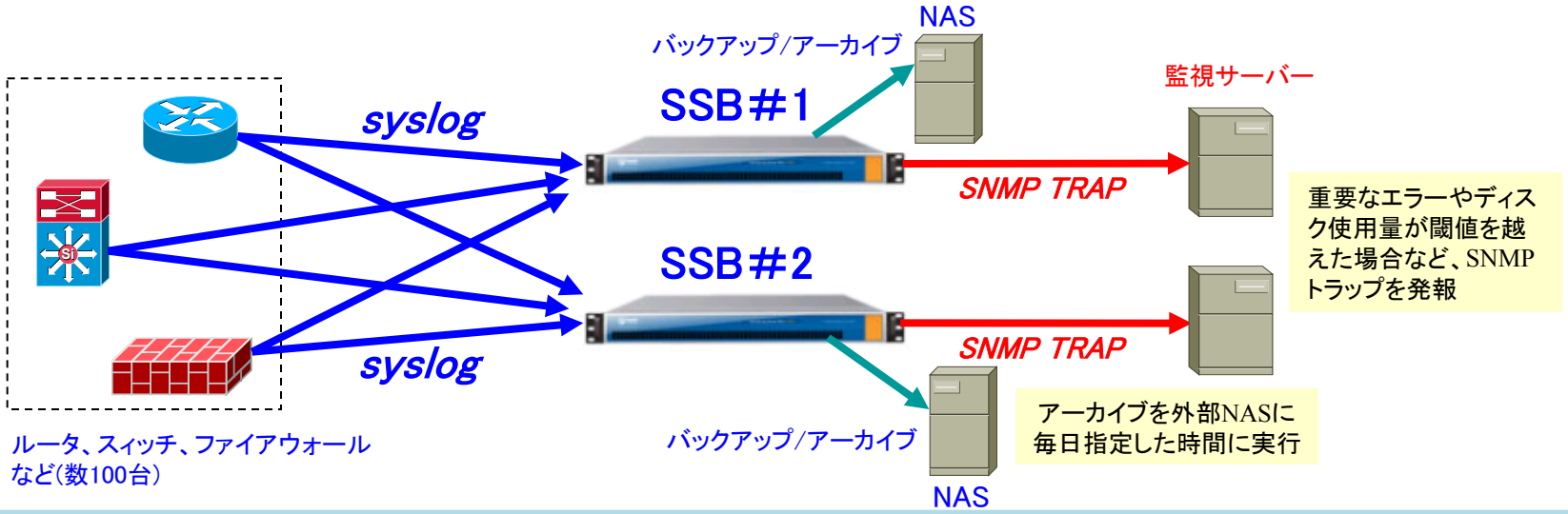
複数拠点から送信される大量のシスログ（ネットワーク機器等数100台）を取りこぼしなく、PCI DSSコンプライアンスに準拠し安全に保存、運用する。

また、シスログは１年間保存する必要がある。

**導入の決めて**

syslog-ng Store Box（SSB)の持つ、大量のログを受信できる高速性とPCI DSSコンプライアンスに対応した高い機密性（ログ暗号化、ユーザ管理、SSB自体の操作ログの記録等）。

また、大容量の内蔵ディスク、フレキシブルな運用が可能なアーカイブ機能（アーカイブした後も、SSB管理画面から検索が可能）。



# 23 Shell Control Box (SCB)


- 監視対象サーバーにエージェントのインストールが必要ありません
- 透過プロキシゲートウェイとして動作するターンキーアプライアンスです
- 監査証跡は動画で記録され、操作画面を映画のように正確に再現します
- IPアドレス、時間、チャンネルタイプ等のアクセス制御が可能です
- 特権IDアクセスに個人を特定するIDを使用して二段階認証できます

# 24 ログ管理ツール製品ラインナップ


## Windowsベースログサーバー「WinSyslog」

Windows用高機能シスログサーバーとして、信頼性、安定性、使いやすさ、低価格でネットワークやシステム専門家から高い評価を得ています。
ログリアルタイム表示と検索機能を含むWinSyslogパッケージも用意しています。

http://www.jtc-i.co.jp/product/winsyslog/winsyslog.html


## シスログサーバーの定番「Kiwi Syslog Server」

世界でもっとも著名なWindows用シスログサーバーです。
UDP/TCPシスログとSNMPトラップを受信できます。最大100個のルール（フィルタ条件とアクションの組み合わせ）を作成でき、柔軟にログを処理します。

http://www.jtc-i.co.jp/product/kiwisyslogserver/kiwisyslogserver.html

SAWMILL

## ログ解析ソリューション「Sawmill」

あらゆるログを解析するためのユニバーサルログ解析ソリューションです。
約1000種類以上の内臓ログフォーマットプラグインでWebサーバー、セキュリティアプリケーション、メールサーバー、シスログをはじめとするあらゆるログを解析します。

http://www.jtc-i.co.jp/product/sawmill/sawmill.html

# 25 操作画面記録・証跡管理製品ラインナップ

ObserveIT


## 行動分析機能搭載、高度な監視カメラ「ObserveIT」

ユーザーの操作をもとにリスクを点数化して可視化できるユーザー操作記録ツールです。
コンピュータ上のユーザー操作に対する監視カメラのように動作し、あらゆるプロトコル、あらゆるユーザーの操作を画像とテキストメタデータで記録します。

http://www.jtc-i.co.jp/product/observeit/observeit.html

Ekran


## 低コストで簡単に使える監視カメラ「Ekran」

ビデオ形式による監視を低コストで実現できるユーザー操作記録ツールです。
すべてのコンピュータやサーバー画面を画像で記録することにより、一般ユーザーはもとより特権ユーザー操作も完全に記録できます。

http://www.jtc-i.co.jp/product/ekran/ekransystem.html

Teramind


## 内部脅威セキュリティソリューション「Teramind」

ユーザーのすべての行動をモニターし記録する新世代セキュリティソリューションです。
特定の行動を制限することによって、内部脅威に対する防御を強化することができます。
ユーザーの危険な行動を未然に防ぎ、業務改善に活用できます。

http://www.jtc-i.co.jp/product/teramind/teramind.html

# 26 会社概要

| | |
|---|---|
| 社名 | ジュピターテクノロジー株式会社 |
| 所在地 | ＜本社＞<br>〒183-0023<br>東京都府中市宮町2-15-13　第15三ツ木ビル8Ｆ<br><br>＜大阪営業所＞<br>〒530-0001<br>大阪府大阪市北区梅田1-1-3 大阪駅前第3ビル11Ｆ |
| 設立年月日 | 2001年1月12日 |
| 代表取締役 CEO | 石川 幸洋 |
| 事業内容 | ・システム製品販売（ネットワーク管理とセキュリティ製品）<br>・システム構築事業 |

本資料についてのお問い合わせや各製品に関するご相談は下記までご連絡ください。


# ジュピターテクノロジー株式会社

〒183-0023
東京都府中市宮町2-15-13
第15三ツ木ビル8Ｆ

042-358-1250

sales@jtc-i.co.jp


| サービス詳細URL | http://www.jtc-i.co.jp |
|---|---|