統合ログ管理サービスガイドライン

第1.0版

2010年12月

データベース・セキュリティ・コンソーシアム

統合ログWG

目次

第1章 はじめに

1.1 目的

昨今の相次ぐ情報漏洩事件事故、コンプライアンス違反事例を振り返ると、ログ管理が重要であることは明らかであり、個々の組織においてログ管理が十分に行うことが必要である。そして、セキュリティ・ポリシーの履行状況を確認したり、事件事故の状況を確認したりするためには、ログの活用が欠かせない。

しかし、多くのシステムから発生するログを統合管理できるシステムが普及し始めているが、ただ保存することを目的としていることが散見され、本来の目的であるコンプライアンス違反の発見やインシデント調査などが実現していないことが多い。

一方でログを統合的に扱うには、高度な分析能力が求められるとともに、コンプライアンスやセキュリティだけでなくシステム管理全般の広い知識が必要となる。同時にログそのものが機密情報であり、統合することによって、より機密性が高まる。

このような状況を鑑みて、本ガイドラインでは統合ログ管理に求められる機能・要件を定義すると共に、導入・運用に関わるサービスの内容やスキル等を提言する。

1.2 本ガイドラインに関する注意事項

本ガイドラインに関する注意事項を以下に記述する。

- 著作権の所在

本ガイドラインの版権は、データベース・セキュリティ・コンソーシアム（DBSC）に属する。

- 利用制限

本ガイドラインの販売は禁止する。それ以外の本ガイドラインを利用したサービス提供に関しては一切制限しない。

- 利用元の明記

本ガイドラインの全文もしくは一部を引用する場合には、営利目的・非営利目的の区別なく必ず引用元として「統合ログ管理サービスガイドライン」を明記する。

- ガイドラインの全部あるいは一部をそのまま、使用する場合

【出典】「統合ログ管理サービスガイドライン(0.9 版)」
データベース・セキュリティ・コンソーシアム(DBSC)
http://www.db-security.org

- ガイドラインを一部加工して、使用する場合

【参考文献】「統合ログ管理サービスガイドライン(0.9 版)」
データベース・セキュリティ・コンソーシアム(DBSC)
http://www.db-security.org

- 免責事項

本ガイドラインを利用したことによって生じるいかなる損害に関しても、DBSC は一切責任を負わないものとする。

- 本ガイドライン利用時の問い合わせ窓口

本ガイドラインを報道、記事などメディアで用いる場合には、DBSC 事務局(info@db-security.org)まで連絡する。

第2章 統合ログ管理の概要

2.1 統合ログ管理とは

統合ログ管理とは、組織内に存在する複数のシステムが発行するログをシステムの種類、フォーマットを問わず一元的に管理することをという。これによりシステム横断的にイベント（事象）の検索・分析をすることが可能となる。

2.2 統合ログ管理の期待効果

1．情報セキュリティ事件（予兆を含む）を容易に早期発見できる
2．ログデータの検索性が向上することにより、事件発生後の調査が容易になる
3．一元管理することにより、効率的な管理ができる
4．ログデータを一か所に集めることにより、ログデータの破損・破壊・改ざん等から保護し易くなる
5．以上のような効果により、情報漏洩の抑止につながる

2.3 統合ログ管理の要素

1．複数種類のログの一元管理
各システムが出力するあらゆるログを、フォーマットを問わず一元的に管理することが求められる。また、ログの転送時に内容の機密性を保つ安全管理機能があること、効率的な運用の為のログデータの圧縮機能も求められる。
2．ログの検索性
統合ログ管理では、大量のログであっても高速検索が可能な状態が求められる。同時に、複数種のログを横断的に結合して検索可能な状態も必要となる。またログデータは収集後に正規化、データベース化された状態でシステム等に格納することが求められる。
3．ログの保管
収集されたログは機密性、完全性、可用性を担保した状態で保管する。

2.4 ログの分類

本ガイドラインにおける統合ログ管理の標準的なログの分類を示す。

大分類	中分類	ログの種類	主な対象
個人デバイス （PC、携帯電話、スマートフォン）	OS	操作記録 設定変更記録 認証ログ	クライアント PC 用、 モバイル、スマートフォン用
	アプリケーション	操作記録 通話・通信記録 チェック記録	Office、ブラウザー、メーラー、業務用ソフト、アンチウィルスソフト、パーソナルファイアウォール、URL フィルタリング　他
サーバ	OS	認証ログ 操作記録 SYSLOG エラーログ	サーバ OS
	ミドルウェア	認証ログ 操作記録 アクセスログ エラーログ	Web エンジン、メールゲートウェイ、DBMS、アプリケーションサーバ
	アプリケーション	認証ログ 操作記録 アクセスログ エラーログ	FW、Proxy、VPN、IDS/IPS、リモートアクセスサーバ、Web アプリケーション、ファイルサーバ、ディレクトリ、DHCP、メールボックス、アンチウィルス（マルウェア対策）、DB、SFA、CRM、会計、人事
ネットワークデバイス （ルーター、スイッチ、負荷分散装置、無線ＬＡＮアクセスポイント）		操作記録 通信記録 アクセスログ	独自ハードウェア SNMP
物理 （監視カメラ、入退室、キャビネ閉開､キーBOX、プリンター、RFID 関連）		カメラ映像 入退室記録 印刷ログ ドア閉開記録 他	独自管理サーバ

表１　ログの分類

第3章 統合ログ管理サービス

3.1 サービス提供形態

１． アウトソース型
ユーザーのネットワーク内に設定したログ収集サーバに対してサービス提供事業者がログ管理、分析、レポーティング、監視等のサービスを提供する形態

２． ASP・SaaS 型
サービス提供事業者側に設置したログ収集サーバにより、ログの収集から分析、レポーティングまで一貫して ASP スタイルで提供する形態

３． アドバイザリ提供（自組織運用）型
ログの管理や統合ログの運用はすべて自組織で運用しているが、必要に応じてレポート内容の詳細や項目別の管理策、運用に関するアドバイス等をコンサルティングの形で提供する形態

４． ログ提供（オフライン）型
ユーザー側で収集したログをサービス提供事業者にファイルとして提供し、事業者側はそれに基づいた分析をまとめレポーティングする形態

※統合ログ管理サービスを提供する統合ログ管理システムには、統合ログ管理ソフト、アプライアンス、ストレージなどを含む「統合ログ管理サーバ」および、各種業務システム等のログ収集エージェント、ログ発行プロセス等が含まれる。

※サービス提供形態イメージ図

1． アウトソース型

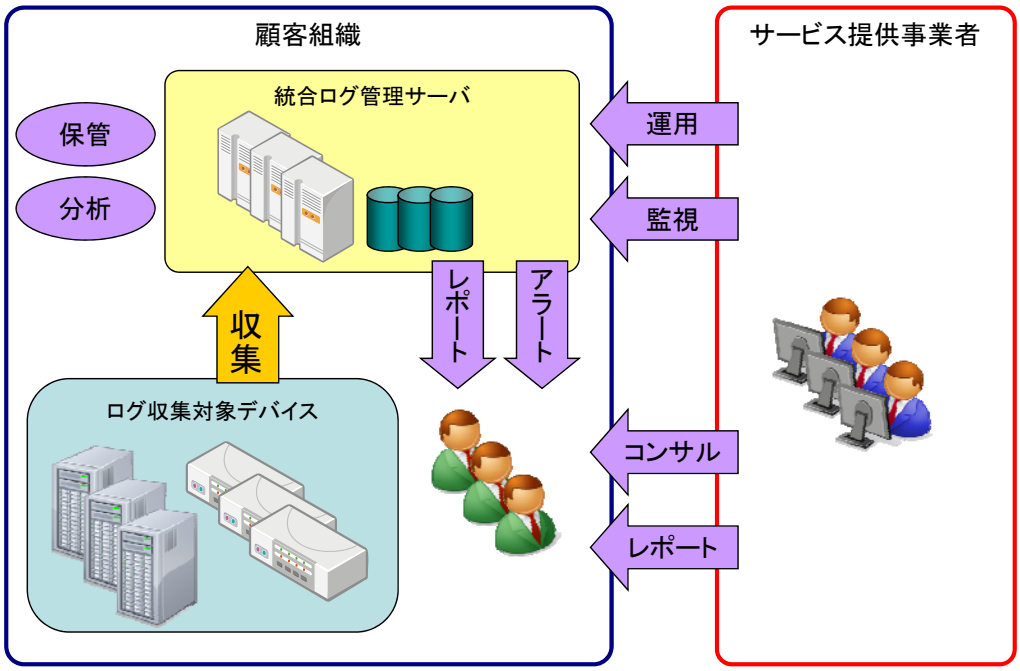

図 1　アウトソース型のサービス提供形態

2． ASP・SaaS 型

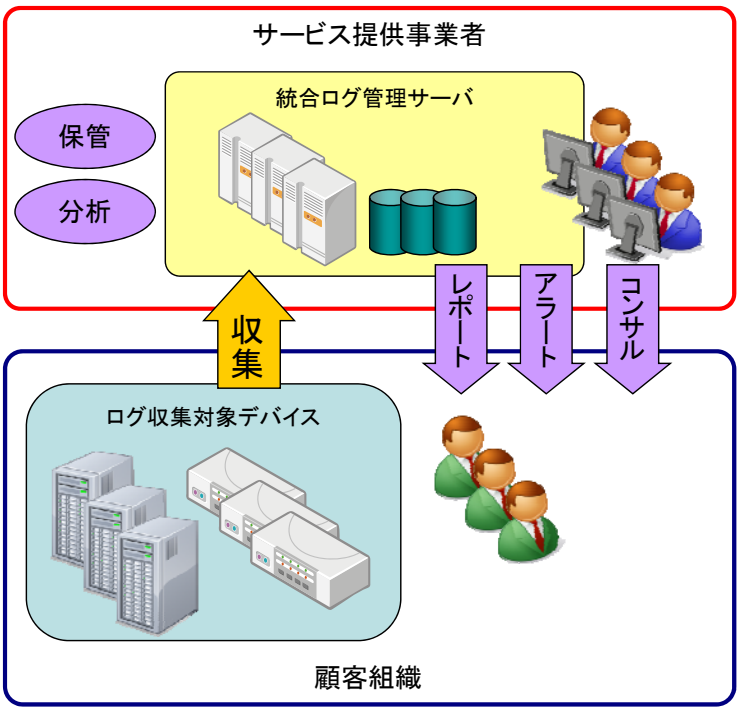

図 2　ASP・SaaS 型のサービス提供形態

3． アドバイザリ提供（自組織運用）型

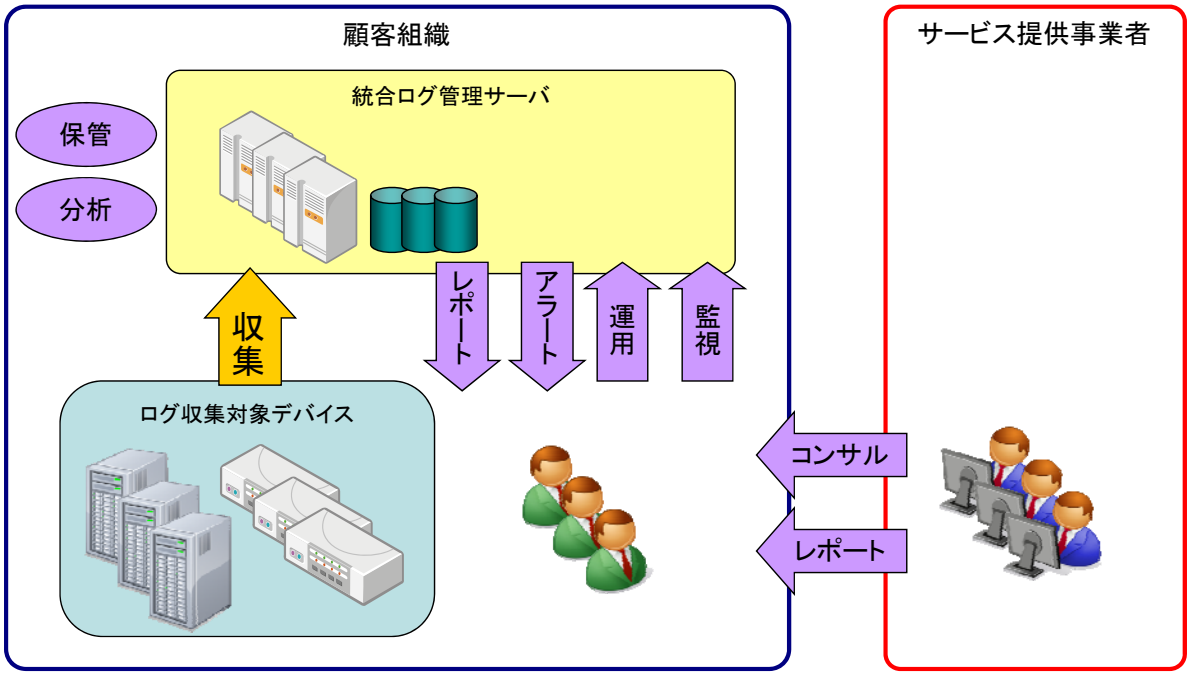

図３　アドバイザリ提供型のサービス提供形態

4． ログ提供（オフライン）型

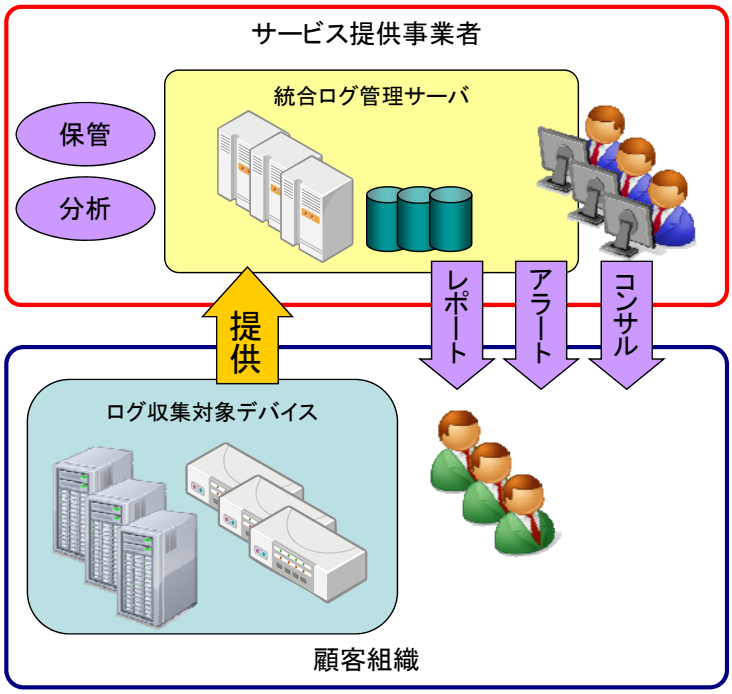

図４　ログ提供型のサービス提供形態

3.2 統合ログ管理サービスの概要

１． 導入支援サービス
統合ログ管理サービスを導入する為に必要な要件定義から実装までのプロジェクト支援を行う。

２． ログの収集
各種機器やソフトウェアからログデータを収集し、必要なフォーマットに変換して集約する。

３． 複数ログの相関分析
複数のログを特定のキー項目やキーワード等を軸に相関分析を行う。

４． ログの保管
収集されたログを整理して保管する機能。保管時には暗号化やアクセスコントロール等の機密性・完全性・可用性を考慮した対策を行う。

５． ログの分析レポーティング
予め決められた形式に決められたタイミングでレポートを提供する。

６． ログ発生のパターンによるアラート
予め決められたログの発生パターンが検知された場合に、決められたタイミングでアラートを発行する。

７． レポート、分析に基づくコンサルティング
決められたタイミングで集計されたログより、事故及び事故の予兆、あるいは情報セキュリティに関するリスク、推奨する管理策等の報告をコンサルタントより提示する。

８． 追跡調査
事件・事故の発生時、顧客の要望等をトリガーとして、各ログを組み合わせた横断的な調査・追跡を行う。

９． 運用管理
アラートパターンやレポート内容、エージェント設定等の変更、デバイスの追加削除、システムリソース管理等を行う。

１０． ログの真正性証明
ログが改ざんされていないことを論理的に証明する機能。「ログが欠落していないこと」と「ログが改ざんされていないこと」の２つを証明する。

3.3 提供形態とサービス項目の関連

各サービス提供形態におけるサービス提供事業者の提供するサービス項目を以下の表に示す。

提供形態 / サービス項目	アウトソース型	ASP・SaaS 型	アドバイザリ提供（自組織運用）型	ログ提供（オフライン）型
導入支援サービス	○	○	○	△
ログの収集	○	○	×	×
複数ログの相関分析	○	○	×	○
ログの保管	△	○	×	△
ログの分析レポーティング	○	○	×	○
ログ発生のパターンによるアラート	○	○	×	×
レポート、分析に基づくコンサルティング	△	△	△	△
追跡調査	○	○	○	○
運用管理	○	○	△	△
ログの真正性証明	△	△	△	△

○：提供あり　　×：提供なし　　△：契約内容による

表 2　サービス提供形態とサービス項目

3.4 導入支援サービス

統合ログ管理サービスを導入する際に必要なプロセスを推進させるための支援コンサルティング。

1．　要件定義
　　統合ログ管理の目的確認、対象システムの特定、サービス提供形態の決定
2．　統合ログの設計
　　システム設計、運用設計
3．　システム構築

統合ログ管理システム製品の導入と既存ログの移行　他

3.5　ログの収集

収集方法、利用目的、対象となるシステムの種類別にデータ授受のルールやモジュールの有無、設定の役割分担が明確になっていること。

1．ログの収集形態

Push 型、Pull 型、オフライン提供型、ツール中継型　他

2．収集のタイミング

目的や用途によって検討する。

3．収集の手段

syslog、FTP、SNMP trap、エージェント、外部記憶媒体、ログ管理ツール　他

4．機密性の確保

通信の暗号化、収集されたデータの暗号化、アクセスコントロールをすること。

5．通信エラーや機器の死活確認

ログの送信の際に発生するネットワーク切断や認証エラーについては、発生したことを想定し、ログの欠損が発生しない対策を行う。また機器自身に何らかの障害が発生しログが欠損する場合も想定して、対象機器の死活状況は把握できるようにしておく。

3.6　複数ログの相関分析

1．特定キーワードを使っての複数ログ内容の横断的検索

ID、ファイル名、IP アドレス、サーバ名、ポート番号、アプリケーション名、コマンド、操作内容（コピー、削除、ファイル添付、権限の変更　等)、時刻　他

2．組合せパターン

1 つの行動に繋がる複数のログの検知を想定し、そこからかい離するようなログが発生した場合に通知する。例としては以下のようなパターンが挙げられる。

(ア) 入室ログが無い ID についてシステムへのログインが室内から行われた。

(イ) 複数のシステムへの認証エラーが集中的に続発している。

(ウ) 申請承認のない特権アカウントの作業ログが発生している。

3.7　ログの保管

保管するログは以下のようなステイタス別に管理される。

1．即時検索可能なステイタス

即時の分析が可能な状態で整理され、データベースに保管されていることが望ましい。ただ

しデータの保存容量が増加すると分析能力の低下を招く恐れがあるので、定められた期間を過ぎたあるいはログの量が一定量を超えた場合、古いログから順次アーカイブのステイタスに移送する運用が必要である。

2． アーカイブ・ステイタス
即時検索は出来ないが、事後の追跡調査の為に①のステイタスに復旧可能な状態で保管する。保管する媒体は任意であるが、テープ、DVD 等の可搬型記憶媒体を用いる場合には物理的なアクセス制御について慎重な注意を払う必要がある。

収集したログを紛失、破損、改ざんから保護し、許可されない参照を防止する。
以下の設定を基本として対策を行う。

1． 暗号化（データベースやその他の保管状況で実施）
2． アクセスコントロール（ログの参照、分析、アーカイブやバックアップ作業について管理）
3． 改ざん検知（ハッシュ値等を利用）
4． ストレージの多重化とバックアップ（毀損防止対策）

3.8 ログの分析レポーティング

1． 予め設定された形式で定期的にレポーティングする。
2． 内容はグラフ等を用いてビジュアル化されたものを中心とする。
3． 定期的なレポート上での統計で得られた値について、過去の平均数値から一定レベル以上にかい離が発生している場合に、そのレポーティングを行う。

3.9 ログ発生のパターンによるアラート

1． 予め設定されたログの組合せパターンが収集されたログデータの中や分析作業上で発見された場合に、アラートを発行する。
2． アラートを発行するパターンをユーザー側である程度カスタマイズできる機能がある。
3． アラートの発行は以下のような方法が設定できる。
メール、警告ランプ、サイレン、レポート上へ反映、コンソール画面へ反映　他
4． アラートの発行タイミングは重要度に合わせて以下のようなタイミングを設定できる。
即時、日次、月次レポート時　等

3.10 レポート分析に基づくコンサルティング

平常運用時において、レポートから読み取れる情報セキュリティに関するリスクを列記し、世の中のセキュリティ脅威の状況や脆弱性の発生状況等を踏まえて、その管理策についてコンサルティ

ングを行う。

3.11 追跡調査

事件・事故の発生等の緊急時において、各ログを組み合わせた横断的な調査・追跡を行い、事件・事故の発生日時、場所、関係した人物などの特定を行う。また、顧客組織のリクエストに基づいて調査・追跡を実施する場合もある。

調査の手法としては以下のものを参考にする。

1． 相関分析

複数のログをキーワードで結合して情報セキュリティ上のリスクを洗い出す。

・ 時間軸での分析

特定のイベントに繋がるログを紐づけて、イベント発生の経緯を探り出す。

・ ユーザーID での分析

特定のユーザーに着目し、ログ上に現れる記録を紐づけてその行動を追跡する。

・ 操作ファイルを軸とした分析

重要な情報や機器に対するアクセスから、リスクに繋がるような事象が読み取れるか分析する。

2． シナリオ分析

過去の事例や想定される漏洩経路や方法についてシナリオを作成して、統合ログ上に一致するような結果が出ていないか確認する。

【分析事例】

・ 重要情報のローカルへの保存→USB メモリの使用（情報の持出しの可能性）

・ サーバルームへの入退室記録が無いのに、ネットワークへログイン（成りすましの可能性） 等

3.12 運用管理

管理対象システム、リスク状況や顧客要望の変化により、必要に応じて対象機器や集約項目の追加・削除を行う。また、統合ログ管理サービスの有効性確認のため、顧客と協力しサイバー演習を行う。

3.13 ログの真正性証明

統合ログシステムで収集されたログデータは、その真正性が保たれなければならない。そのため、以下の機能を設けることが望ましい。

1． ログデータのタイムスタンプ*1 を統合ログシステムとは別のシステムに保管する。

２． ハッシュ値等によりログの欠落や改ざんの有無を検出する。
３． ログを複数ロケーションに同時保存し比較することで、改ざんの有無を検出する。

*1 タイムスタンプ：第三者証明としての時刻認証などを想定しており、発行時点以降に改ざんなどが検証可能なものをいう。

第4章 統合ログ管理サービスの導入プロセス

統合ログ管理サービスの導入においては、新規に導入する場合と、既に導入している統合ログ管理システムを活用してサービスを導入する場合がある。其々のケースにおいて導入プロセスは異なる。新規に導入する場合を図 5、既に導入している場合を図 6 に示す。

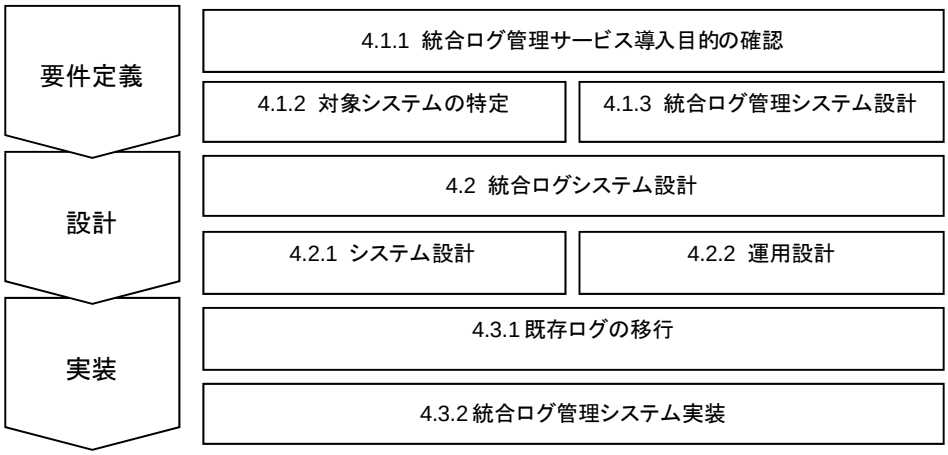

図 5　新規導入の場合の導入プロセス

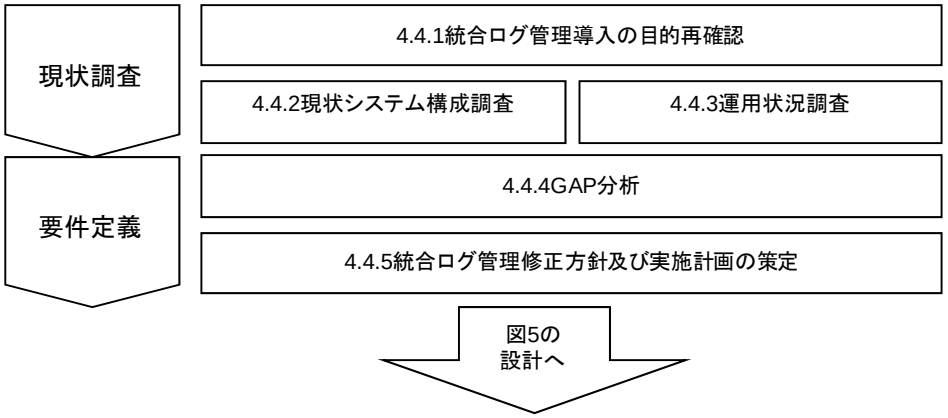

図 6　既に導入している統合ログシステムを活用する場合の導入プロセス

4.1 要件定義

4.1.1 統合ログ管理サービス導入目的の確認

統合ログ管理サービスの導入目的を達成するために、「何を」「どのタイミングで」発見する必要があるのか整理する。目的を明確に定めることが統合ログ管理サービスの導入成功の鍵となる。

１． 目的の事例
・ ログの確実な保管（J-SOX、ISMS、P マーク等の審査対応）
・ ポリシー遵守状況の確認（内部監査の補完データ）
・ 情報漏洩（外部、内部）の発見、追跡
２． 何を
・ 情報セキュリティインシデント
・ 操作記録（操作ミス）
・ 悪意の攻撃
・ 予兆
３． どのタイミングで
・ リアルタイム
・ 定期的（スケジュール処理）

「何を」「どのタイミングで」発見する必要があるのかを明確にするステップを省略してはならない。

4.1.2 対象システムの特定

業態、保持する情報の属性、業務フロー等より、インシデントの発生によるリスクを分析し、統合ログ管理の対象となるシステムを特定する。統合ログ管理サービスの導入目的に従い、管理すべきシステムをリストアップすることは効率的に設計、運用を行うための必須事項である。既にどのようなログ管理が実施されているのかを確認する現状調査もこのフェーズに含まれる。

【対象となるシステムの例】
・ 個人情報を取り扱うシステム
・ 入退室管理システム
・ 電子商取引システム
・ 外部公開サーバ
・ メールサーバ
・ 基幹系システム
・ ファイアウォール
・ IDS、IPS
・ マルウェア対策システム
・ レイヤー3 スイッチ
・ ファイルサーバ
・ ログ管理サーバ(入退室管理サーバ、エンドポイント監視ツール、DBMS、運用管理ツール　等)

【ログ管理の現状調査項目の例】

・　ログの形式（フォーマット、ASCII/バイナリ等）
・　情報量
・　ログの収集方法（syslog、FTP、SNMP trap、外部記憶媒体等）

※ 対象システムのリストアップにおいて、抜け漏れがないように調査することは重要である。そのためには、マネジメントレベルから、個々のデバイスセンサーに至るまでの高度な知見が必須となる。個人ですべての領域に高度な知見を有することは困難なため、複数人の知見をあわせ、チームとして活動することが望まれる。

4.1.3 サービス提供形態の決定

「3.3 提供形態とサービス項目の関連」を参考に、統合ログ管理サービスの提供形態を選択する。統合ログ管理を効率的に行うためには、日々の運用・監視、レポート・アラートの発行パラメータのチューニング、新しい攻撃、不正行為への対応などを継続的に行うことが必要となる。自組織のリソース、人員のスキルなどを考慮して統合ログ管理サービスの提供形態を選択しなければならない。

4.2 統合ログ管理システム設計

要件定義フェーズで明確となった目的を達成するための統合ログ管理システムを設計する。

4.2.1 システム設計

4.2.1.1.　ログ収集用ネットワークの設計

収集用のネットワークを設計することで下記のような効果がある。

・　対象システムから直接統合ログ管理システムへ転送する。
　－　システムから直接転送するため、構成が単純になる。
・　一旦、組織内のログ集約サーバにてログを集約し、統合ログ管理システムへ転送する。
　－　ログ集約サーバ上でログの正規化、圧縮などが可能なため、広い回線帯域を必要としない。
・　ログの機能別にログを集約するようなソフトウェアがある場合には、そのソフトウェアを通じて間接的に統合ログ管理システムに転送する。
　－　統合ログ管理側の負荷が軽減できる。
　－　既存のログ管理機能を使うことができる。
　－　ログ上で管理すべき時刻のズレが大きくなる可能性がある。
　－　運用管理との結合、あるいは役割分担を行う必要がある。

4.2.1.2. ログ収集エージェント

ログ収集のための専用エージェントをインストールするか、システムが備えるログシステムの設定変更を行うか選択する。

- エージェントのインストール
  - エージェントがログを適切な形式に加工してから送出する。そのため、ネットワーク帯域、ログ管理サーバのリソースを節約できる。
  - エージェントをインストールするため、システムに対応するエージェントが提供されていることが必要となる。対応エージェントが提供されていない場合、開発に費用がかかる場合がある。
  - エージェントが既存システムに影響を及ぼす可能性がある。
- 設定変更
  - 新たなアプリケーションをインストールしないため、比較的安全である。
  - 通常はログの送出前に正規化などの加工を行うことは困難である。

4.2.1.3. 真正性証明機能の設計

ログの真正性の証明には「存在証明機能」と「非改ざん証明機能」があり、それぞれを満足するような設計を行うことが望ましい。なお本機能を設計する場合にはハッシュ値及びタイムスタンプを使う仕組みが必要になることが想定される。また、ログのハッシュ値やタイムスタンプを統合ログシステムとは別のシステムに保管することが望ましい。また、時刻そのものの証明は、精度によりコストが多大にかかることがあるので、必要なレベルの精度を設定して設計するべきである。

(1) 存在証明機能

各ログに記録されたタイムスタンプの時刻にログデータ自体が存在していたことを証明する機能を提供する。方法としては、ログ収集の機能と外部の第三者機関による時刻認証サービスと連動させることが考えられる。その際には導入に掛るコストやネットワーク的なレスポンス、機器への負荷、またログの重要度、取得目的に留意しながら設計することが望ましい。

(2) 非改ざん証明機能

収集されたログが改ざんされていないことを証明するために必要に応じて導入する。ログの発生時あるいは収集時にハッシュ値を取得し、その内容を別管理することで実装される。(1)に述べられている時刻認証と連動すればより強固な非改ざん証明を実現できる。また、複数のロケーションにあるログを同時に改ざんされる確率は低いことを利用し、ログは複数ロケーションに同時保存し比較することで､改ざんの有無を検出することができる。

4.2.1.4. ログの分析

目的を達成するためには、複数のログを組み合わせ分析することが有用である。データベースのログ単体では発見できなかった攻撃の予兆をファイアウォールのログ、ウェブサーバのログ、他の

データベースのログなどを組み合わせて分析することで発見できる場合がある。その観点から、どのログを組み合わせて分析すればどのようなインシデントを発見できるのか検証する。

4.2.1.5. ログのフォーマット

各システムより出力されるログはそれぞれ形式が異なる。そのため、統合ログ管理においては、異なる形式のログを統合管理するために、以下の機能が必要となる。

- ログの構文解析 – タブ区切り、カンマ区切り等の構文を解析し、フィールドを抽出する。
- ログの変換 – 文字コードの変換、XML から CSV への変換などの処理を行う。
- ログの正規化 – 時刻表示形式の統一（24 時間表記と 12 時間表記、タイムゾーンの違いなど）や、ポート番号の表記（80 と http など）を行う。

4.2.1.6. ログの必要項目

統合ログ管理システム導入の目的に従って、最低限必要なフィールドを定義する。

【最低限必要なフィールドの例】

- ログが発生した場所、機器 ID
- 日付・時刻
- 操作元 IP アドレス
- 操作内容
- 操作したファイル名
- アカウント ID

4.2.1.7. ログ取得のタイミング

統合ログ管理システム導入の目的に従って、ログ取得のタイミングを定義する。

- リアルタイム
- バッチ（スケジュール）

予兆検知を目的としている場合に、ログの取得を 1 日に 1 回のバッチで取得した場合、目的を果たせないことは明白である。ログ収集先システムに依存するが、可能な限りリアルタイムでのログ収集を実施することを推奨する。

4.2.1.8. ログ取得の方向

ログ取得の方向の決定は主にログ収集先システムに依存する。

- Push – システムから統合ログ管理システムへログを送出する。
- Pull – 統合ログ管理システムがシステムからログを取得する。
- オフライン提供型 – システムのログをオフラインで提供する。ログの欠損、改ざんに注意が必要となる。

4.2.1.9.　システムの死活確認

特に Push 型のリアルタイム型でログを取得する場合、ログを発行するイベントが発生していないためにログが発行されていないのか、ログ発行プロセスが停止しているためにログが発行されていないのか判断する必要がある。具体的には、システムおよび、ログ発行プロセスの死活確認を行う仕組みを実装しなければならない。一方、Pull 型でログを取得する場合は、ログ収集先システムの死活確認を兼ねることができる。

4.2.1.10. ログ収集経路の安全性確保

収集するログには個人情報や、営業秘密などが含まれる可能性があり、組織の活動記録そのものであるため、機密性は非常に重要な項目である。同様に完全性・可用性についても確保することが重要である。

- 機密性の確保　－　ログ情報の暗号化、通信経路の暗号化、ログ専用経路の使用
- 完全性の確保　－　syslog は通常 UDP を使用するため完全性は保証されない。TCP を使用する syslog の利用、FTP、FTPS、SSH によるトンネリングなどの利用が考えられる。また、メッセージ・ダイジェストを利用すれば完全性を担保することも可能。
- 可用性の確保　－　ログの発行量を予測し、必要な回線容量を決定する。外部からの攻撃時など、ログの発行量が通常時の数倍～数十倍になることも想定することを推奨する。また、ログ転送専用の通信回線を準備することで、ログ発行量の増大時に通常業務への影響を減らすことが可能となる。

4.2.1.11. 保管期間

収集するログを長期間にわたり保管することは事後の調査に役立つ。しかし、ログの長期保管は多くの費用とリソースを必要とするため、関連する法令、ガイドライン等を参照の上、決定することが推奨される。明確な基準が見当たらない場合は、少なくとも 1 年間は保管することを推奨する。

4.2.1.12. 容量

ログの保管期間を考慮し、ストレージの容量を決定する。テープ等へ退避したログは可用性が低下するため、可能な限り HDD 上に保管できるよう設計する。また、ログの容量の増大にあわせて容易にストレージを追加できる構成が推奨される。

4.2.1.13. 時刻同期

複数のログを管理する統合ログでは、ログの時刻の正確性を確保することは重要である。NTP サーバによる時刻同期、ログ管理サーバでの時刻補正等を採用することが推奨される。

4.2.2 運用設計

4.2.2.1. 組織内規程の整備

統合ログ管理に関する組織内規程を以下の観点を考慮して整備する。

- ログを統合管理する対象（システム）の定義
- 統合ログ管理手順
- 統合ログ管理システムの SLA（24 時間 365 日運用、稼働率 99.9%など）
- アラート発行基準（想定インシデントに対する報告手順）
- アラート対応基準（想定インシデントに対する対応手順）
- 外部委託先選定基準（通常の外部委託先選定基準より厳しい基準が好ましい）
- ログ、レポート等の情報のオフライン転送手順

4.2.2.2. ログの保護

以下の要素を考慮してログの保護施策を策定する。

- 完全性 － 転送経路・ストレージ上での改変、破損を防ぎ、もしそれらが発生した場合には検出できるようにする（TCP による転送、メッセージ・ダイジェストの保存等）。システム障害発生時のログ確保の方法についても、決められた保証レベルを実現する機能を持つ必要がある。
- 可用性 － 電源、回線、HDD（ストレージ）を多重化する。更に、データのバックアップを取得する。統合ログ管理システムの可用性が失われた場合、ログの収集に障害が発生し、ログの完全性が失われる可能性があることを十分考慮する。
- 機密性 － 転送経路・ストレージ上でデータを暗号化する。もしくは、独立した転送経路を使用する。更に、統合ログ管理システムの設置場所の物理的対策を講じる（入退室管理、耐震・耐火設備、監視など）。

4.2.2.3. ログの分析

以下の要素を考慮してログの分析を実施する。

- リアルタイム対応すべきインシデント
- 月次・週次など定期的に対応すべきイベント
- ログ発生の時刻と実際のインシデントとの時間的関係の検証（予兆、発生時、事後）

4.2.2.4. 消去・廃棄

保管期間の満了、サービス提供契約の終了等、ログ保管の必要がなくなったログデータについては速やかに消去・廃棄を行う。消去・廃棄の方法、手順については予め文書化し、確実に実施できる体制を構築する。併せて、バックアップメディア、レポート資料、送受信メール等を消去・廃棄対象とするか、事前に明確しておく必要がある。

4.2.2.5.　訓練計画の策定

実際に起こりうる事件・事故に対する統合ログ管理の有効性を確認するために、サイバー演習を定期的に行う。演習では以下の観点を考慮する。

- トレース調査能力を確認するために、実際の事件・事故を想定したシナリオを策定する。
- 統合ログ管理サービス事業者だけでなく、顧客組織と合同で行う。

4.3 システム構築

4.3.1 既存ログの移行

既存のログを統合ログ管理システムに移行する場合、移行時にログが失われないよう配慮する。特に重要なシステムの場合は、既存ログ管理システムに切り戻せるよう移行計画を策定する。

4.3.2 統合ログ管理システム製品/サービスの活用

統合ログ管理には以下のような項目が要求される。統合ログ管理の専用製品、サービスにはこのような項目のほとんど、またはすべてが含まれているため、統合ログ管理システムの構築に採用することは有用である。

- ログの構文解析
- ログの正規化
- ログのアーカイブ
- ログの圧縮
- ログの完全性チェック
- 相関分析
- レポート機能
- ログの消去

4.4 既存のログ管理機能に追加を行う場合

統合ログ管理を既存のログ管理あるいはシステム管理に組み込む場合には、新規導入プロセスの前に以下のプロセスを経ることを推奨する。

4.4.1 統合ログ管理導入の目的再確認

従来導入されているログ管理の要件定義や利用目的に囚われずに、その企業が統合ログ管理を導

入する目的について再確認を行う。そこから導き出された新たな目的に沿って、現状調査・GAP 分析を行うためのベースラインを策定する。

4.4.2 現状システム構成調査

4.4.1 で確認した導入目的に照らして、現状のログ管理に関わるシステム構成に過不足が無いかどうかを調査する。

●着目点　例

- 取得するログの種類、ログの項目内容
- 取扱うログの量
- ログの保管期間、保管方法
- 設定されているアラートの内容　等

4.4.3 運用状況調査

4.4.1 で確認した導入目的に照らして、現状のログ管理の運用に関して過不足が無いかどうかを調査する。

●着目点　例

- ログの収集タイミング
- ログの収集手段
- 登用されているシステムの機能
- 分析に関わる担当者のスキル
- レポーティング内容及びアラート対応　他

4.4.4 GAP 分析

これまでの調査分析結果を取りまとめて、策定したベースラインからの GAP を洗い出し、列挙する。

4.4.5 統合ログ管理の修正方針及び実施計画の策定

4.4.4 で洗い出した課題をどのように解決していくかの導入実施計画策定を行う。

GAP を埋めるためには、導入プロセスのどのフェーズを再検討する必要があるか決定し、計画に反映させる。

策定に際しては以下の点に配慮する。

- 解決すべき課題の選択と優先順位

- 既存システム、運用、組織との整合性
- 既存ログの移行方針とタイミング
- 導入プロセスの再検討項目

4.5 設計上の注意点

4.5.1 ログ管理の精度と運用のバランス

統合ログ管理サービスの設計にはバランスを考えなければならない項目がある。利用目的に応じて最適なバランスを保つように設計しなければならない。

4.5.2 タイムスタンプ

この項目を有効に利用するためにはログを発生させるデバイス同士の時刻同期がなされていることが重要である。また各ログのタイムスタンプはどの時点で生成されたものかは予め整理しておく必要がある。

4.5.3 ユーザーID

ログインするデバイス、アプリケーション、サービスによって各種の ID が存在することが予想されるが、統合ログの有効性を高めるにはこれらの ID が可能な限り統合して管理されていることが望ましい。ID の統合した管理が出来ない場合には、読み替えの出来る互換表を用意することで代用させることも可能である。また、ログ上での ID の正確性を高めるために多要素認証や生体認証等の認証強化対策も併せて検討することが望ましい。

4.5.4 各種ログの収集に関する留意点

収集対象となる各種ログの違いを把握し、必要とされるログ項目や粒度に配慮する必要がある。１つのサーバから発せられるログは OS のイベントログや SYSLOG だけではなく、その上で稼働するアプリケーションからも別個のログが作られており、収集すべきログは１つの機器から１つのログになるとは限らない。統合ログ管理の利用目的に応じて必要なログを不足なく収集することが望ましい。例えば、SQL インジェクション等の不正アクセスによる情報漏洩や、データベース管理者による不正行為の検知を目的にした統合ログ管理の場合には、サーバ OS のログだけでは目的の事象を全てカバーすることができない。データベースの操作ログや各種セキュリティ関連ソフトのワーニング・ログ等を合わせて取得することにより目的の事象をカバーすることが可能になる。

第5章 運用管理

統合ログの運用管理は大きく 2 つの作業に分かれる。1 つは予め設定されたログの発生パターンが検知された際のアラートに対する対応であり、もう 1 つは統合ログの管理を維持するための運用保守チェックである。このチェックを起点として情報セキュリティインシデントが検出されると、アラートの設定やログのチューニングなど、必要な改善策を実施することとなる。また、統合ログ管理の作業にも支障が発生しないようにシステムの運用をきちんと行う必要がある。

5.1 アラート管理

1．アラートが発生した場合には、発見者がアラート対応基準に従い必要な関係部署あるいは上長に報告する。
2．アラート対応基準に従い調査担当者は状況の確認を行う。
3．状況の確認が終了したのち、状況の重要度や対応の優先度を判断し修復作業を実施する。状況確認の進捗度に応じて応急処置的な対応を優先する場合もある。
4．状況が収束したのちに、アラートの発生から収束までの作業を評価してアラート設定の改善を検討する。必要に応じて運用対応の手順や体制についても検討の範囲に入れて改善策を検討する。

5.2 保守管理

1．ログ保存領域のディスク容量チェック
ログの保存領域は常時確保するために適切な閾値を設定して、ログの収集・保管の停止を回避する。
2．システムリソースの状況チェック
ログを収集するシステムの負荷状況を確認する。CPU やネットワークの帯域利用状況を把握して処理時間の増大やタイムアウトの発生を未然に防ぐ。これらに関しても閾値を設定して、リアルタイムに管理することが望ましい。
3．ログの欠損状況のチェック
ログの発生の無い状況が、イベントの発生が無い状況か収集作業上のトラブルか識別できるよう、ログ収集対象機器の死活監視情報やログの転送記録等を確保し、確認しておくことが望ましい。
4．ログの発生件数チェック
ログの発生件数は状況により変化する。日頃より全体的な統計情報を確保し、件数等の増大

があればディスク容量の追加やシステムリソースの拡張を検討する。

5.3 チューニング

チューニングを行うことにより、インシデントの予兆を高精度で検知することが可能となる。チューニングは社会情勢の変化、顧客の状況・要望の変化に応じて行われる他、日々の運用の結果、改善項目を見いだし、サービス提供事業者側より提案されることもあり得る。チューニングには以下のような項目が含まれる。

- 新しいシステムの追加、削除等の構成変更の統合ログ管理システムへの反映
- システムの重要度の変化による、ログ取得タイミングの変更
- 新しい脅威に対応するための構成変更
- 顧客の要求に応じた構成変更
- リソースの管理（ログを保管するストレージのサイズ、回線の帯域）

第6章 サイバー演習

策定された演習計画に基づき、顧客組織と共同してサービス提供事業者が中心となり実施する。演習結果に基づき、トレース調査可能な範囲、トレース不可能なインシデントなどを顧客組織とサービス提供事業者間で共有し、必要に応じて改善する為にサイバー演習を行う。

6.1 演習実施手順

1． 演習シナリオの作成
ログ収集対象としているシステムに対する脅威、脆弱性を元に想定される情報セキュリティ事象を選択する。シナリオの作成にあたっては以下の情報を参考にすることが望ましい。

・ 最近発生した情報セキュリティに関する事故事例
・ 最近発見されたシステム上の脆弱性
・ 最新のマルウェア（コンピュータウィルス）の情報
・ 社内で起こったヒヤリハットの事例

2． シナリオの再現、あるいはシミュレーション
シナリオを元にシステム上に事象を再現し、ログを発生させる。あるいはシミュレーションによりそうした状況を予測する。

3． 結果の検証
２．により再現あるいはシミュレートされた結果を検証し、現状の統合ログの管理機能に不足や不備が無いか検証し、課題を抽出する。

4． 改善策の検討と実施
３．で抽出された課題についてチューニングや運用の改善を行う。

6.2 サイバー演習シナリオの例

サイバー演習のシナリオを策定する。簡単なシナリオ例を以下に述べる。

・ P2P ネットワーク上に流通してしまった機密情報の漏洩ルートが特定できるかを確認する。
想定される漏洩ルート：USB メモリへのコピー、メールへの添付送信、印刷物　他
・ 事前にファイルサーバ上の機密情報を、名前を変更した上で USB メモリにコピーしておき、それをトレース調査によって発見可能であるか確認する。

第7章 統合ログ管理サービス提供事業者

7.1 サービス提供事業者に求められる事項

本サービスで取り扱うログには、組織内部の様々な情報が含まれる。したがって、そのログを取り扱うことになるサービス提供事業者は、顧客から信用を得ることが重要であり、そして極めて大きな責任が求められる。

顧客から信用を得るために、サービス提供事業者は事業所の住所や連絡先、資本金、従業員数等の基本情報を開示しなければならない。また、過去に起きた事件・事故等について開示をすることも求められる。顧客側は、サービス提供事業者が開示する情報に基づいて、サービス提供事業者を選定することが望ましい。

また、統合ログ管理サービスを提供するに際しては、サービスの可用性や完全性といった観点を考慮し、サービス提供事業者として一定以上の規模及び体制・サービスレベルを構え、更にそれを維持していくことが求められる。

7.1.1 情報の開示

1．基本情報

サービス提供事業者は、次の基本情報を開示しなければならない。

(ア) 事業社名（商号）
(イ) 設立年・事業年数
(ウ) 住所（本社・主な事業所）
(エ) 連絡先（電話・FAX）
(オ) 主な事業の概要
(カ) 代表者氏名
(キ) 従業員数（単独ベース）
(ク) 資本金
(ケ) 事業者全体の売上高
(コ) 自己資本比率
(サ) 株主構成
(シ) 株式上場の有無（上場の場合は市場名）
(ス) 決算公告実施の有無
(セ) 認証取得（プライバシーマーク・ISMS・ITSMS 等）
(ソ) 開示情報の年月日

２．その他の情報

サービス提供事業者は、基本情報に加え、次の情報についても開示することが求められる。

(ア) 過去に起きた運用事故（サービス停止等)、情報の漏洩事故等

(イ) サービス稼働率等のこれまでの実績値

7.1.2 必要な規模及び体制・サービスレベル

１．規模

サービス提供事業者は、統合ログ管理サービスを提供するに際し、次の規模を維持することが望ましい。

(ア) 情報セキュリティ関連の事業年数が 5 年以上

(イ) 資本金が 1 億円以上

(ウ) 正社員数が 10 名以上

(エ) ISMS 認証の取得、もしくはそれに準ずる運用の実施

２．体制・サービスレベル

サービス提供事業者は、統合ログ管理サービスを提供するに際し、次の体制・サービスレベルを維持しなければならない。

(ア) 情報セキュリティに関する基本方針・規程・マニュアル等の文書類の整備

(イ) 従業員への情報セキュリティに関する教育の定期的な実施

(ウ) 情報セキュリティ対策の実態に関する監査の定期的な実施

(エ) 顧客からの問い合わせを受け付ける窓口の設置

(オ) コンプライアンス担当者の任命

(カ) 目標サービス稼働率を確定、及びその値の公表（99.9%以上を推奨）

３．物理的対策

統合ログ管理サービスを提供する事業所では、次の物理的対策を維持しなければならない。

(ア) 免震または制震の施設・建物（耐震のみは不可）

(イ) 2 系統以上の異なる変電施設からの受電

(ウ) 上記の他、想定される災害（自然災害・人災）がもたらす脅威リスクを把握・分析、必要な対策の実施

7.2 サービス遂行者に求められる条件

7.2.1 サービス遂行者の所属

サービス遂行者はサービス提供事業者の正社員であることが望ましい。また、顧客からの要望が有れば、当該サービス遂行者の勤続・在職証明書類を速やかに顧客へ提供することが求められる。

なお、サービス遂行者をアサインする際には、これまでの経歴等の考慮が必要である。特に、顧客と何らかの関係を持つ者（利害関係者など）の扱いについては注意すべきである。

7.2.2 サービス提供事業者のスキル

サービス提供事業者にはデータベース技術に関する高度な知見が求められることは当然として、その他にも様々なシステムの知識と実務経験を有していなければならない。併せて、情報セキュリティについての知見も必須であり、特に技術分野に造詣が深いことが望まれる。これらの条件を満たす為、サービス提供事業者はサービス遂行者を適切に組織することが重要となる。

具体的には次の条件を満たしていることが望ましい。

大分類	中分類	経験
管理系		セキュリティ関連の基準や規程類の策定、整備、及び施行に関する知識、及び実務経験
技術系	OS	クライアント PC、サーバ用 OS に関する知識、及び実務経験
	ネットワーク	ファイアウォール、ルーター等のネットワーク機器に関する知識、及び実務経験
	データベース	データベースに関する知識、及び実務経験
	アプリケーション	開発に関する知識、及び経験 製品に関する知識、及び経験
その他		洞察力、物事を鳥瞰（俯瞰）できる力 統計学、BI ツールや DB 構築の知識 システムやネットワーク運用業務の経験 トラブルシューティングの業務経験 情報セキュリティに関する監査業務、ヒアリング経験

表 3　サービス提供事業者に望まれるスキル

7.2.3 サービス遂行者への教育及びトレーニング

前述の通り、サービス遂行者にはデータベースやセキュリティ等に関する高度な知見が求められる。したがって、常に新しい技術・情報の習得を重ねていくことが求められるものである。

サービス提供事業者は、必要な教育及びトレーニングを明確にした上で、サービス遂行者に受講させることが求められる。受講していない、若しくは受講した結果が芳しくないサービス遂行者については、サービス業務の担当から外すことも含め、措置を講じなければならない。

サービス遂行者は以下の分野において、教育及びトレーニングを受講することが望ましい。

- 倫理、コンプライアンスに関わるもの
- ネットワーク管理、システム管理

・ 運用監視
・ 最新の情報セキュリティインシデントのケーススタディー
・ 脆弱性情報に関する件

なお、毎年実施している DBSC セミナーには、本サービスに関わる全ての者が参加することが望ましい。

第8章 Service Level Agreement (SLA)

8.1 SLA の重要性

第 2 章で述べた通り、統合ログ管理サービスを利用することで顧客側では様々なメリットが想定される。その一方で、パフォーマンスやサポート体制、セキュリティ対策等の面において顧客には不安が存在することも考慮すべき事柄である。顧客のこういった不安や懸念は、顧客の期待するものと、サービス提供事業者が提供するサービスの実体について、両者の間で明確なコンセンサスが得られていないことに端を発していることが少なくない。こういった状況のままでサービスの提供・利用を続けていくと、顧客の期待を裏切ることや、サービス提供者に過度な負担がのしかかるようなことになりかねない。場合によってはトラブルにまで発展する恐れもある。

当事者間の認識のズレを解消し、適正な取引関係を構築する為には、サービスの内容や品質等について予め両者で合意しておく必要がある。合意すべき事項は SLA として明文化しておく。なお、SLA は契約の締結時に契約内容として盛り込むことが一般的である。

8.2 各サービス項目について表示する SLA 事例

統合ログ管理サービスを提供する事業者は自らが提供するサービスがサービス項目のどの部分をカバーしているかを明示する必要がある。また、各々の項目がどういったレベルで提供されるかを合わせて提示することが望ましい。各項目で示すべきサービスレベルの記述例を下記に列挙する。

8.2.1 導入支援サービスに関する SLA 項目

- 要件定義、統合ログの設計、システム構築のどの部分をカバーするサービスであるかを明確に定義する。
- アドバイザリのみか、設定作業まで行うのかサービス側と顧客側の役割分担を明確にする。

8.2.2 ログの収集に関する SLA 項目

- ログの収集対象にできるデバイス、アプリケーション、ログの種類を明確にし、その対象毎に利用可能な手段を明確にする。
- ログの収集手段については、サーバの負荷やネットワークに対する負荷の度合いを示す指標を設けて表示し、ユーザーが状況に応じて選択できる環境を整えることが望ましい。
- 障害発生時のログ収集の保証について特に以下の状況の対応について明確にする。
- ネットワーク障害発生時の対応（ログの保管、送信のリトライの設定　他）
- ログ収集対象機器の障害時の対応（機器の応答監視の報告あり　他）

・　収集時の通信の安全性について記述する。
　例：暗号化有無、あるいは移送デバイスのセキュリティ対策（パスワード等）

8.2.3　複数ログの相関分析に関する SLA 項目

相関分析を行う場合の前提条件を提示する。
例：ログのタイムスタンプを検査キーとする場合は、各機器の時刻は予め同期されていること。
例：ユーザーID を検索キーにする場合には、各機器のユーザーID は統一されているか互換情報が提供されていること。また成りすましの可能性が極力排除される管理策が施されていること。

8.2.4　ログの保管に関する SLA 項目

ログの保管状況は以下の項目の状況を明示する。
・　ログの即時検索の可否（オンライン、オフライン）
・　ログの暗号化の有無、暗号化がある場合はその手法
・　ログの保管に関する BCP（災害対策等）
・　オフラインログの参照方法
・　ログの保管期限の上限
・　ログの保管容量の上限

8.2.5　ログの分析レポーティングに関する SLA 項目

指定可能なログレポートの作成タイミング及び使用される情報の期間を明記する。
・　月次、週次、日次等の作成タイミング
・　使用するデータの期間と納品タイミング
　例：日曜日 0 時～土曜日 24 時のデータを翌週の水曜日に納品
・　レポートする内容
　例：発生ログの 1 時間毎の件数遷移のグラフ、アラートログの明細全て　等

8.2.6　ログの発生パターンによるアラートに関する SLA 項目

サービス側から提供される発生パターンテンプレートの内容は一覧できるものを用意する。
・　発生パターンを変更する場合の基準、変更手順、公示方法は予め決めて公表する。
・　ユーザー独自のパターンについては作成方法、設定数の上限等の制約事項を明確にしておく。

8.2.7 レポート、分析に基づくコンサルティングに関する SLA 項目

コンサルティング内容はあくまでサービス提供者の知見に基づいた見解であることを明記する。

8.2.8 追跡調査に関する SLA 項目

- 全てのインシデントの状況を把握できるものではない旨を記載する。
- ログとして残らない事象に関する調査は対象外である。

8.2.9 運用管理に関する SLA 項目

サービス側から提供される運用管理について以下の項目について明示する。

1． アラート管理
- アラートの発生時の報告経路（一次対応者と報告方法、チェックのタイミング）
- 対応に関する検討手順と意思決定プロセス（アラート事象のエスカレーション範囲と対応策の最終承認者）

2． 保守管理
- 保守管理に必要な監視項目の閾値
  ※ 閾値を設定すべき項目は「5.2 保守管理」の項目を参照。
- 閾値監視の担当者とタイミング
- 閾値を超える事象が発生した場合の報告ルート、対応手順、最終承認者

3． チューニング
- チューニング実施の検討に入るトリガーとなる事象（ネットワークや機器構成の変更、セキュリティ・ポリシーの変更、特定アラートの多発、保守管理からの要請、サイバー演習からの指摘　他）
- チューニング実施検討の手順（検討の担当者、対応手順、最終承認者）
- チューニングを行う際のポリシー（チューニングで変更するパラメータや設定の範囲、変更の優先順位、タイミング　他）

8.2.10 ログの真正性証明に関する SLA 項目

- 真正性の保証は裁判での証拠能力を保証するものではない。
- 外部の時刻認証サービスや非改ざん証明サービスを利用する場合は、各々の SLA を加味し、矛盾のない SLA を提示することが望ましい。

第9章【参考】法令対処

9.1 ログの保管期間

- PCIDSS(クレジット業界におけるグローバルセキュリティ基準)
  - 最低 3 ヶ月の保管、1 年程度の保管を推奨
- 金融商品取引法（JSOX）
  - ログの保管期間に関しては特に記載なし。(内部統制に関わる書類は 5 年間の保存義務)
- NIST(National Institute of Standards and Technology) : Guide to Computer Security Log Management
  - 高影響度レベルのシステム　3 ヶ月～12 ヶ月
  - 中位影響レベルのシステム　1 ヶ月～ 3 ヶ月
  - 低位影響レベルのシステム　1 週間～ 2 週間

9.2 関連法令

- 不正競争防止法
- 個人情報保護法
- 会社法
- 金融商品取引法（JSOX　インサイダー取引）
- 暗号輸出規制

9.2.1 規格・関連ガイドライン　他

- ISO/IEC 27001
- JIS Q 15001
- COBIT4.1
- 情報セキュリティ監査基準　実施基準ガイドライン　（経済産業省）
- FISC ガイドライン　情報セキュリティ管理基準　　（金融情報システムセンター）
- ASP・SaaS における情報セキュリティ対策ガイドライン　（総務省）

統合ログ管理サービスガイドライン　第一版

DBSC 統合ログワーキンググループ　（社名 50 音順）

リーダ	S&J コンサルティング株式会社	三輪　信雄
	インフォサイエンス株式会社	稲村　大介
	新日鉄ソリューションズ株式会社	松本　泰行
	日本オラクル株式会社	田口　裕也
	日本電気株式会社	後藤　兼太
		村本　栄治
	株式会社日立システムアンドサービス	猪俣　健一
	富士通株式会社	曽根崎健一
		安澤　弘子
	三井物産セキュアディレクション株式会社	大河内智秀
		清水　淳一
	株式会社ラック	西村　稔
		須田　堅一
事務局	三井物産セキュアディレクション株式会社	坂　恵理子