



統合ログWG中間報告

2010年5月25日

統合ログWG

リーダー

三輪信雄

1. 統合ログ管理サービスイメージ(発足時)



① ログ設計

- ① ログのポテンシャル分析
- ② 基本方針策定
 - ・何をを見つけるのか
- ③ センサー設定、運用設計

② ログ現状調査

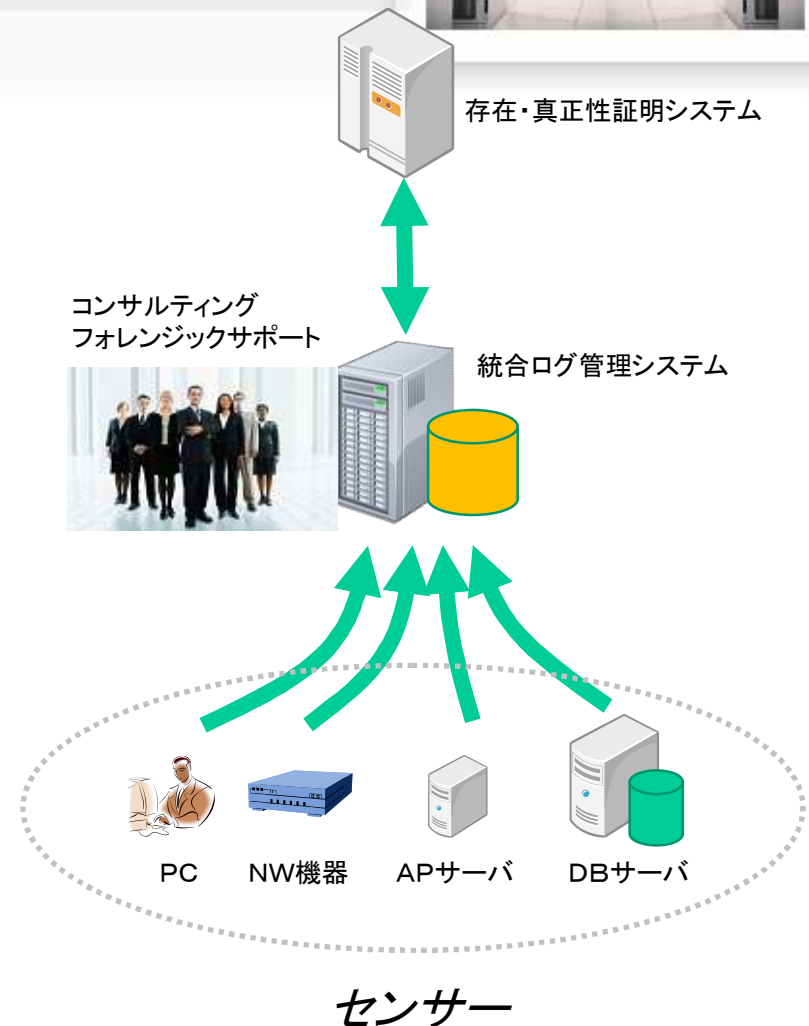
- ① 何が取得されているのか
- ② ギャップ分析
- ③ 改善提案
 - ・センサーのチューニング
 - ・統合ログ管理システムのチューニング

③ ログ運用

- ① オンサイト監査(月次)
 - ・インシデント発見、兆候検出
 - ・チューニング提案 拡張サービス
- ② リモート監視
 - ・インシデント発見、通報
- ③ インシデント調査

④ ログ保管、時刻・真正性認証

- ① ログを安全に保管
- ② 時刻、真正性認証



2. サービスガイドラインの必要性



- ・サービスの価格競争による信頼の低下を防ぐ
 - 同名異種の乱立が予想される
 - 品質の維持、向上（顧客がチェックできる）
 - 標準品質以上のサービスの付加価値の明確化
- ・顧客がサービスそのものを警戒する
 - 顧客組織の機密情報に深く触れる
 - サービス事業者を信用しなければならない

3. これまでの活動



- 12月10日 統合ログWG発足説明会
- 1月28日 第1回WG開催
 - 取り扱うログの種類に関する議論
- 2月12日 第2回WG開催
 - ログの種類に関する意識合わせ
 - サービスイメージに関する議論
- 3月12日 第3回WG開催
 - サービスイメージに関する議論
- 4月22日 第4回WG開催
 - ガイドラインの叩き台提示

4. 目次



第1章 はじめに

- 1.1 目的
- 1.2 本ガイドラインの前提
- 1.3 本ガイドラインに関する注意事項

第2章 統合ログ管理の概要

- 2.1 統合ログ管理とは
- 2.2 統合ログ管理の目的
- 2.3 統合ログ管理の期待効果
- 2.4 統合ログ管理の要素
- 2.5 対象となるログの分類

4. 目次



第3章 統合ログ管理サービス

- 3.1 サービス提供形態
- 3.2 統合ログ管理サービスの機能概要
- 3.3 提供形態と各機能の関連
- 3.4 ログの収集機能
- 3.5 複数ログの相関分析
- 3.6 ログの保管機能
- 3.7 ログの分析レポートニング機能
- 3.8 ログ発生のパターンによるアラート機能
- 3.9 レポート分析に基づくコンサルティング
- 3.10 導入支援機能

4. 目次



第4章 ログ管理の導入プロセス

4.1 要件定義

4.1.1 統合ログ管理の目的の確認

4.1.2 対象システムの特定

4.1.3 サービス提供形態の決定

4.2 統合ログ設計

4.2.1 システム設計

4.2.2 運用設計

4.3 システム構築

4.4 運用

4. 目次



第5章 統合ログサービス提供事業者

5.1 サービス提供事業者の条件

5.1.1 情報の開示

5.1.2 必要な規模及び体制・サービスレベル

5.2 サービス遂行者に求められる条件

5.2.1 サービス遂行者の所属

5.2.2 サービス遂行者のスキル

5.2.3 サービス遂行者への教育及びトレーニング

4. 目次



第6章 SLA

6.1 SLAの重要性

6.2 情報セキュリティに関する各要素への準拠

6.2.1 ログの機密性に関する要素の確認

6.2.2 ログの完全性に関する要素の確認

6.2.3 ログの可用性に関する要素の確認

第7章 法令対処

7.1 ログの保管期間

7.2 関連法令等

5. 抜粋



2.3 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めて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. 一括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えいの抑止につながる

5. 抜粋



2.4 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、また効率的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

統合ログは大量の情報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される。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され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。

4. ログの真正性

取得されたログに関してその時刻と内容が改ざんされていないことを証明出来る。

5. 抜粋



2.5 対象となるログ

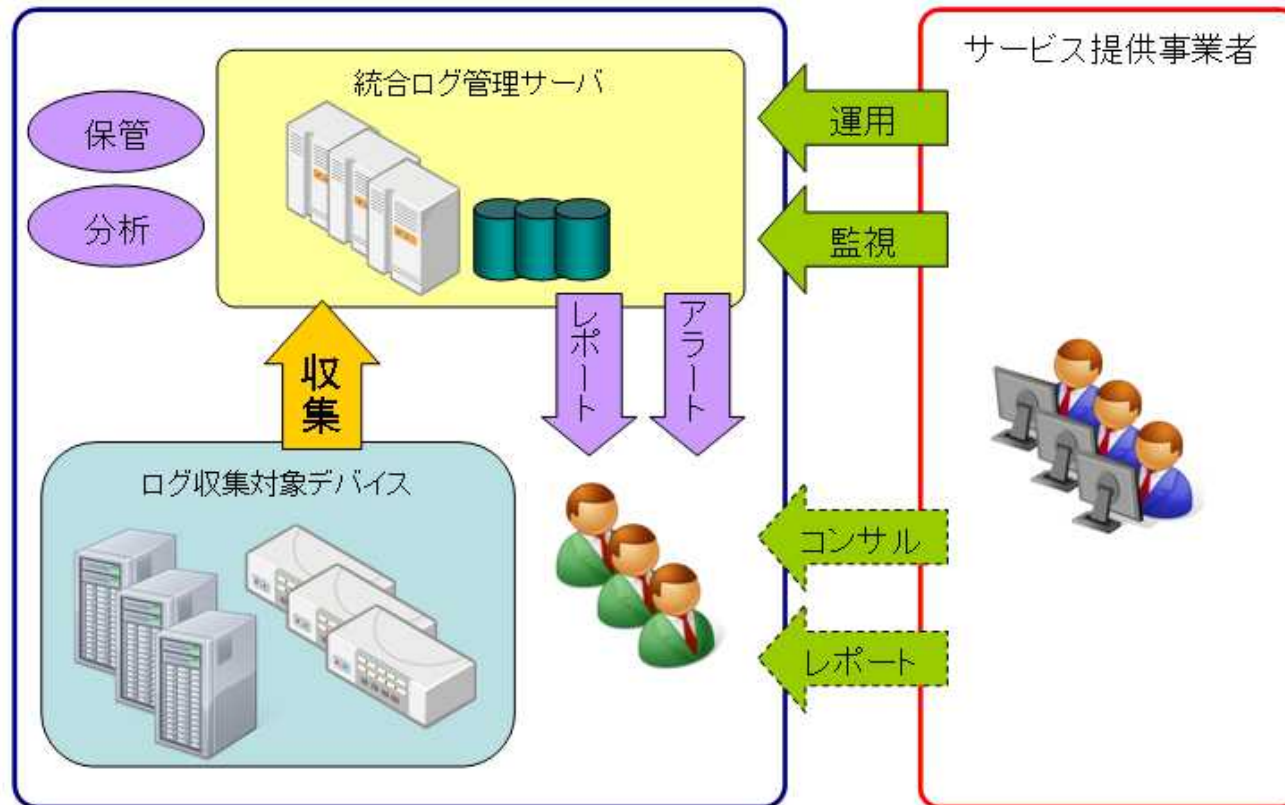
分類	対象	ログ取得目的
個人デバイス	PC、携帯電話、スマートフォン・・・	個人の直接的な行動(不正操作、情報漏えい、労務管理)
ネットワークインフラ (足まわり)	ルーター、スイッチ、負荷分散装置・・・	障害対応
境界	FW、Proxy、VPN、IDS/IPS、無線LANアクセスポイント、リモートアクセスサーバ・・・	不正アクセス、情報漏えい、フォレンジック
インターネットサーバ	Web、メールゲートウェイ、DNS・・・	不正アクセス、情報漏えい、利用統計
イントラネットサーバ	Web、ファイルサーバ、ディレクトリ、DHCP、メールボックス、アンチウイルス(マルウェア対策)、DB、SFA、CRM、会計、人事・・・	不正操作、管理者の管理、労務管理、リソース管理、稼働管理、法令対応
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・・・	不正アクセス、労務管理

5. 抜粋



3.1 サービス提供形態

アウトソース型

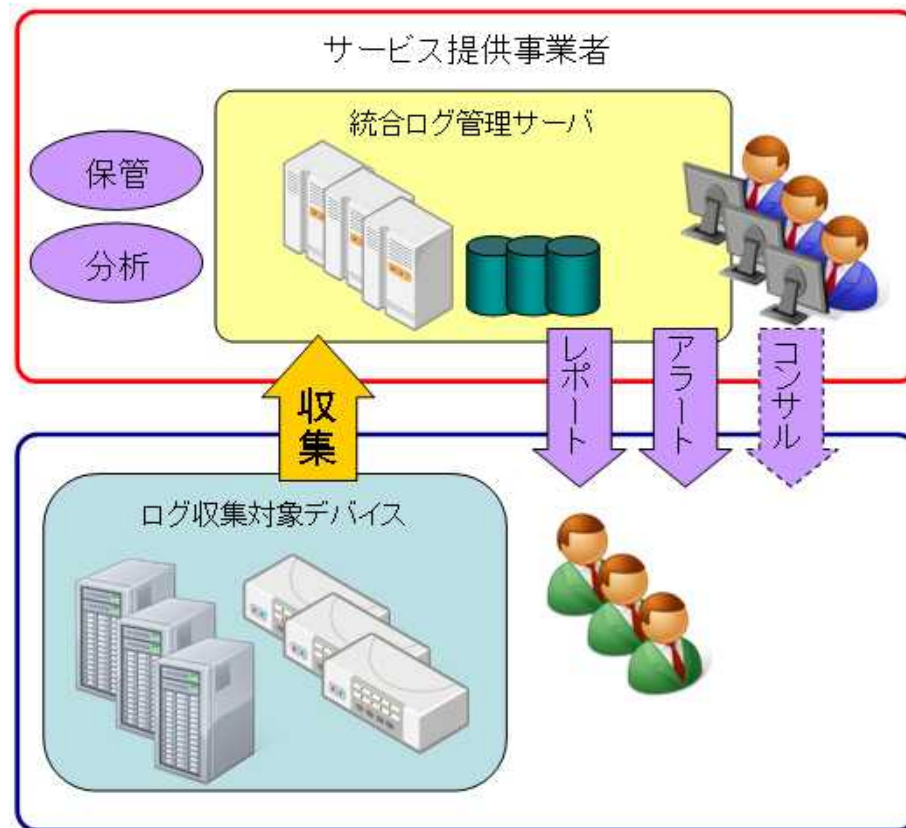


5. 抜粋



3.1 サービス提供形態

ASP, SaaS型

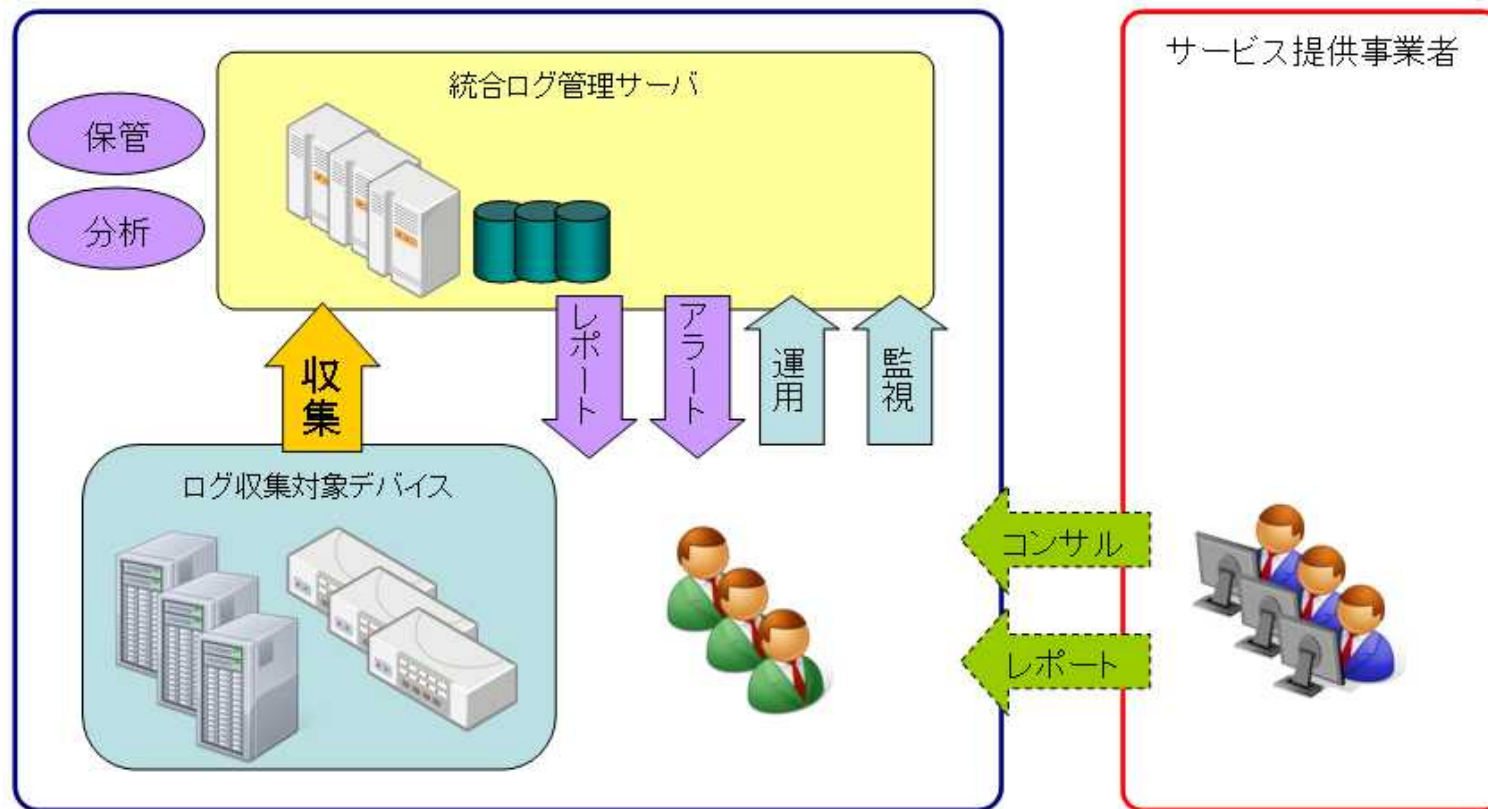


5. 抜粋



3.1 サービス提供形態

アドバイザリ提供型(自組織運用)

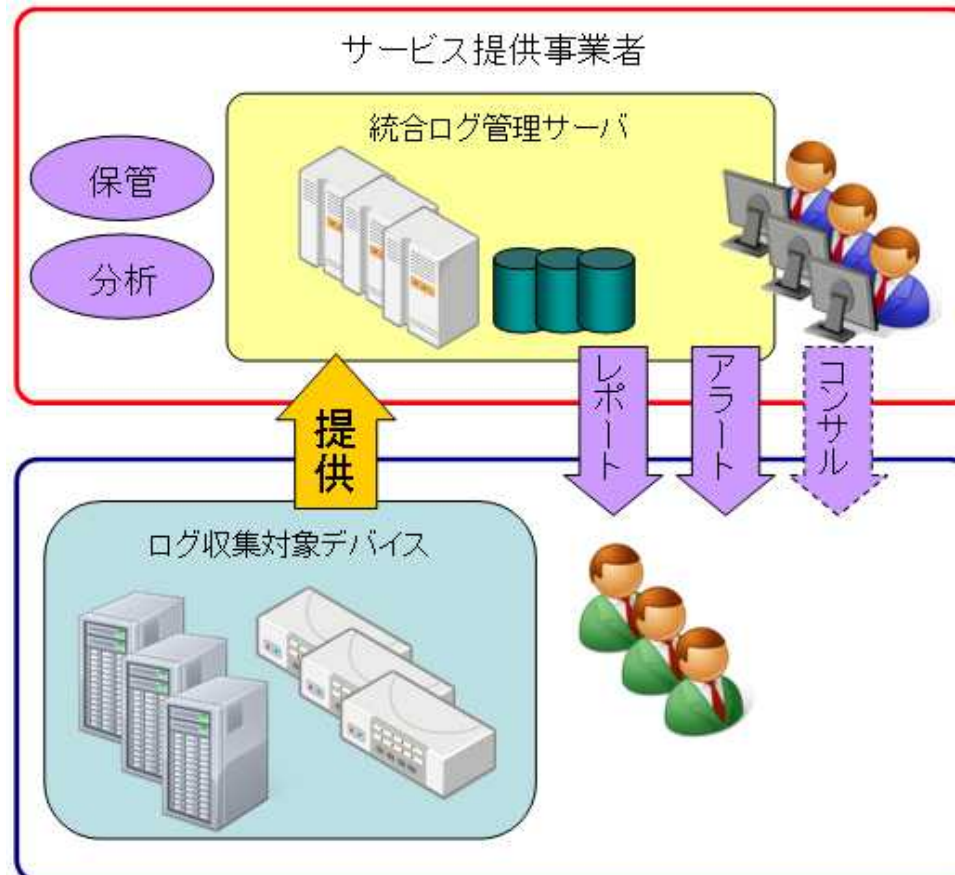


5. 抜粋



3.1 サービス提供形態

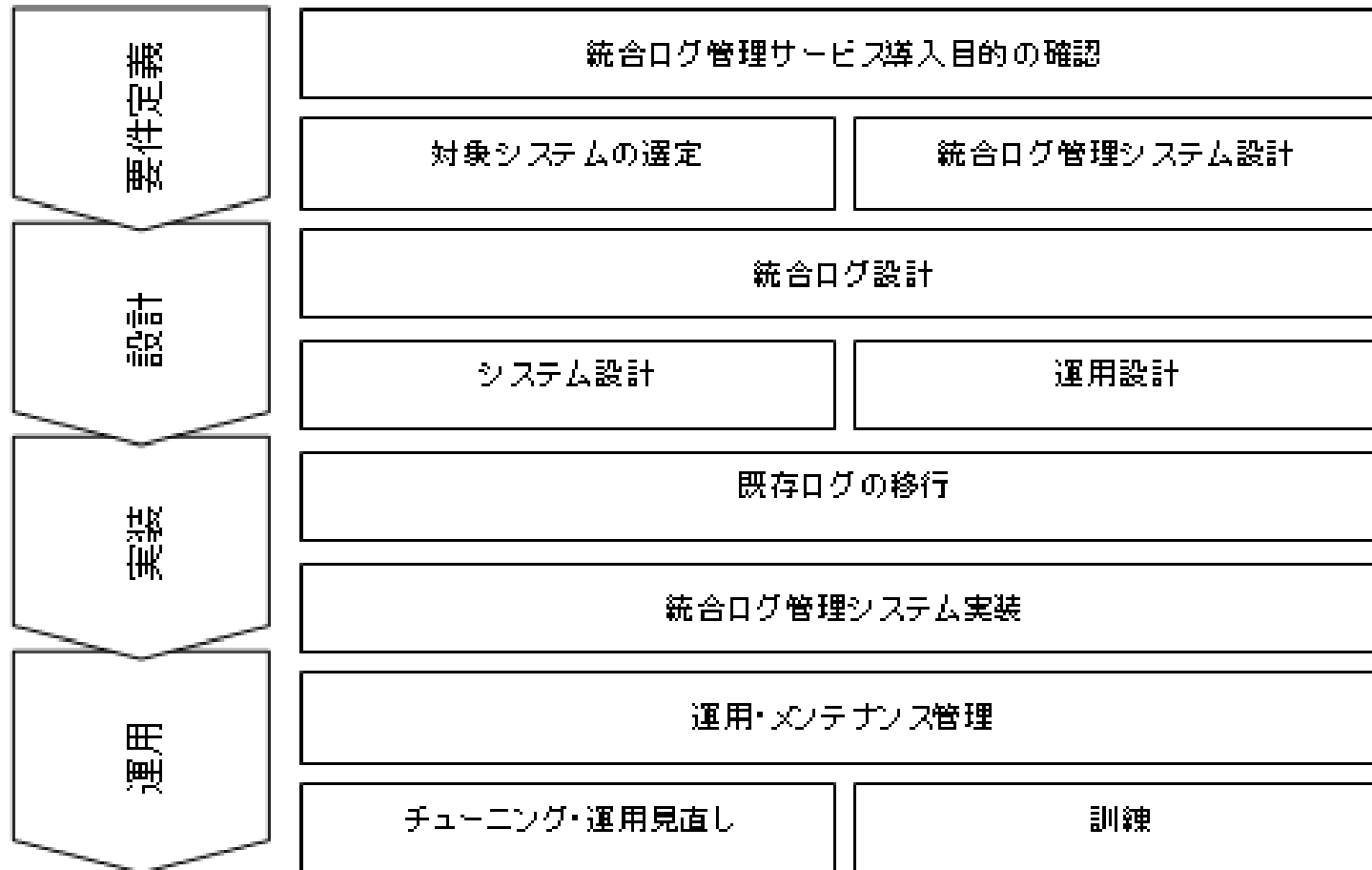
ログ提供型(オフライン)



5. 抜粋



4章 統合ログ管理の導入プロセス



5. 抜粋



6.2.2 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/デバイス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、特にテクニカル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。

マネジメント系

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

テクニカル系

OS

Windows系、Linux系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、物事を鳥瞰出来る力

統計学、BIツールやDB構築の知識

システム運用、トラブルシューティングの経験

6. 今後の予定



- ・第5回WG開催 5月20日
ガイドライン(案)最終版議論
- ・第6回WG開催 6月未定
ガイドライン(案)最終版確定
- ・7月 統合ログ管理サービスガイドライン(案)公開
パブリックコメント募集