統合ログWG

～統合ログマネジメントサービスガイドライン～

2010年2月16日

S&Jコンサルティング株式会社
三輪信雄

① 統合ログマネジメントサービスイメージ

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

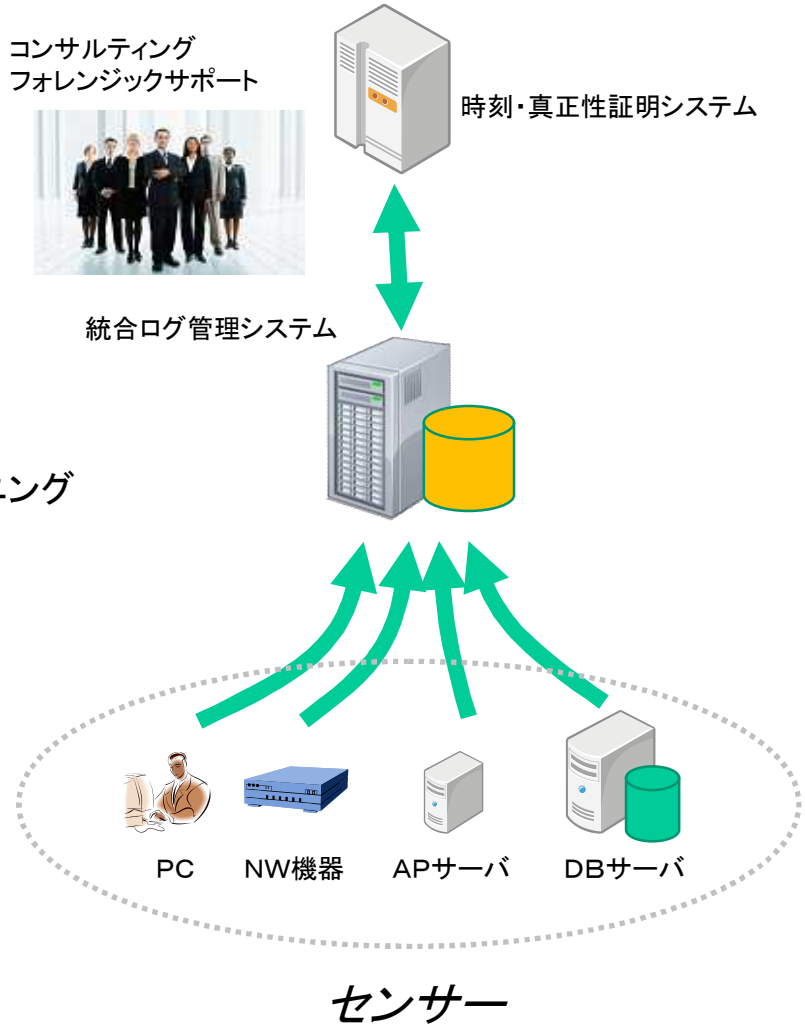
① 何が取得されているのか
② ギャップ分析
③ 改善提案
　・センサーのチューニング
　・統合ログ管理システムのチューニング

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ぎたい

- 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 サービスガイドラインの目次案

1. サービス概要
2. サービス内容
   - 2-1. 要件定義
     - 何をいつ見つけたいのか
     - 実現イメージ（システム、利便性、コスト）
   - 2-2. ログ設計
     - どうやって見つけるのか
     - システム設計、運用設計
   - 2-3. システム構築
     - 既存ログの移行
     - 統合ログ管理システムの要件定義

③ サービスガイドラインの目次案

2-4. 運用

- リアルタイムに見つけるもの
- 月次などの一定期間に見つけるもの
- 各種報告書の定義
- インシデント、予兆調査方法
- インシデント、予兆報告方法
- ログの保存方法、保存機関
- ピンポイント監視

③ サービスガイドラインの目次案

3. サービス事業者

3-1. 企業

- 企業規模、事業規模
- 実績の開示義務
- 運用事故、情報漏えい事故などの開示義務

3-2. サービス遂行者

- マネジメントスキル
- 技術スキル
- 正社員、勤続証明
- 教育、トレーニング過程

③ サービスガイドラインの目次案

４. 顧客向けSLA

５. 法的対処

5-1. 体制

5-2. 対応手順

④ ガイドラインの活用

・自社サービス構築時に参照

・自社の付加価値の明確化

・一定水準のサービス品質の確保

・法執行機関との情報共有、意見交換

・他業界との交流、情報交換

⑤ WGの進め方

・WG事務局を設置

・WG事務局が叩き台を作成

・メールによる議論

・月１～２回程度のWG開催、議論

・第１版はWebで公開

⑥ スケジュール案

１月　サービス概要叩き台　その１

２月　サービス概要叩き台　その２

３月　サービス詳細叩き台　その１

４月　サービス詳細叩き台　その２

５月　サービス詳細叩き台　その３

６月　サービスガイドライン第１版公開

７月以降　他団体との連携、ガイドライン拡張

⑦ 他団体との関係

- ネットワークセキュリティ関係
  - ネットワークセキュリティ機器のログ
  - 既存セキュリティサービスとの連携
- フォレンジック関係
  - 法的対応の可能性
- 警備業界
  - 監視カメラ、出入記録との連携

⑧ 課題

- 法執行機関との関係
  - 証拠としての有効性
  - 情報窃盗などとの関係
- ログの真性性の証明
- ログの有効性の技術的根拠
- マネジメント、技術教育

⑨ 参加企業一覧

S&Jコンサルティング株式会社　（WGリーダ）
インフォサイエンス株式会社
兼松エレクロトニクス株式会社
クエスト・ソフトウェア株式会社
新日鉄ソリューションズ株式会社
日本オラクル株式会社
日本電気株式会社
株式会社日立システムアンドサービス
富士通株式会社
三井物産セキュアディレクション株式会社　（WG事務局）
株式会社ラック

（あいうえお順）

活動状況)(1)ログの分類と目的

	ログの分類	具体例
1	DB	
2	ネットワーク機器	ゲートウェイ系，ルータ，ファイアウォール，IDS，Proxy等
3	端末	PC，携帯/スマートフォン，プリンタ等
4	物理	入退室，カメラ
5	OS,アプリケーション,ミドルウェア,認証	アクセスログ，Mailサーバ，メインフレーム

	ログの目的	具体例
1	情報セキュリティ	ウィルス，漏洩
2	コンプライアンス	労務管理，不正経理
3	事業継続	障害，ダッシュボード

活動状況）（2）提供可能なサービス

社内セキュリティ

ワークフローのモニタリング・監査レポート	予兆・抑止・分析	ログの真正性確保
・申請と実作業を記録・管理 ・労務管理	・内部犯行の予防・予兆発見 ・インシデント発生時分析	・管理者の不正を記録、抑止
要件定義 支援サービス	解析サービス	システム設計・運用 コンサルティング
モニタリングするためのワークフロー分析とシステム化要件定義等のサービス	不審なアクセスを指摘することで、不正の抑止効果	ログ発生時と統合ログシステムに保存される間で欠落がないかシステム全体を把握しコンサルティングを提供する