『統合ログ管理サービスガイドライン』のご紹介

2011年2月22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

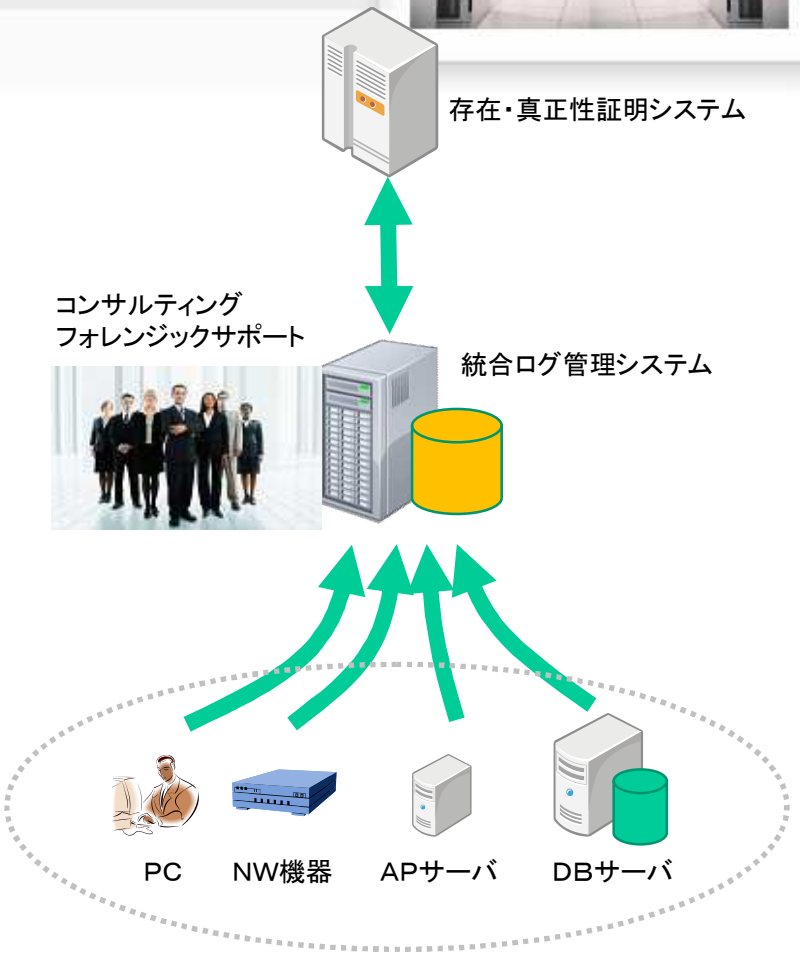
① 何が取得されているのか
② ギャップ分析
③ 改善提案
・センサーのチューニング
・統合ログ管理システムのチューニング

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

・自社で導入する際の参考にできる
  - プロ向けのサービスのガイドラインを参考にできる
  - 製品だけでなく運用コストの根拠にできる

3. これまでの活動

2009年12月10日　統合ログWG発足説明会
2010年 1月28日　第1回WG開催
- 取り扱うログの種類の議論

2月12日　第2回WG開催
- ログの種類の意識合わせ
- サービスイメージの議論

3月12日　第3回WG開催
- サービスイメージの議論

4月22日　第4回WG開催
- ガイドラインの叩き台提示

8月24日　0.9版公開、パブコメ開始
2011年 2月21日　1.0版公開

6. 今後の予定

・WGとしての活動はいったん終了

・ガイドラインの普及促進

・他のコミュニティとの連携の模索

  ・フォレンジック方面

  ・クラウドサービス事業者方面