SaaS/ASP 型の証跡管理システムにおける個人情報保護に関する考察

坂本 昌史　　廣田 啓一　　橋本 正一　　中原 慎一　　平田 真一

NTT 情報流通プラットフォーム研究所
180-8585 東京都武蔵野市緑町 3-9-11

{sakamoto.masanobu, hirota.keiichi, ,hashimoto.shoichi, nakahara.shinichi, hirata.shinichi}@lab.ntt.co.jp

あらまし 内部統制や個人情報保護に関する法整備や，関連するガイドラインの整備が進み，業務監査のための情報取得，情報漏洩の防止を目的とした，システムログ情報の証跡管理を行う仕組みが求められるようになっている．その中で個人情報を扱う業務システムでは，証跡情報に個人情報が含まれることも想定されるため，証跡生成や保管，閲覧に際して不適切な閲覧者から証跡情報を保護する必要がある．本稿では業務システムへ機能提供する SaaS/ASP 型の証跡管理システムモデルを定義し，証跡生成から閲覧までの過程において個人情報保護に関する課題を抽出し，現在の個人情報保護技術の適用評価を行う．

On the Personal Information Protection in the Digital Evidence Management Service System

Masanobu Sakamoto　　Keiichi Hirota　　Shoichi Hashimoto　　Shin'ichi Nakahara
Shin'ichi Hirata

NTT Information Sharing Platform Laboratories
3-9-11 Midori-Cho Musashino-Shi Tokyo 180-8585 Japan

{sakamoto.masanobu, hirota.keiichi, hashimoto.shoichi, nakahara.shinichi,hirata.shinichi,}@lab.ntt.co.jp

Abstract With the development of legislations and relevant guidelines for internal control and personal information protection, the consolidated framework and management system for trail information such as system logs and service logs are demanded from the both purpose of the collection for auditing services and the prevention of information leakage. In such situation, trail information from business systems which handle personal information may involve personal information within them, so it is necessary to protect these trail information from inapposite audiences when generating, transfering, storing and auditing them. In this paper, we define the SaaS/ASP model of the management system for trail information which provides several functionality to business systems. We also extract problems and requirements in each process of trail information management, and then assess the applicability of technologies from the viewpoint of personal information protection.

1　はじめに

近年，企業の IT 投資が進み，企業内の NW インフラの整備が充実するとともに，財務・税務関連文書といった企業文書の電子化が促進している．これに伴い，企業内の情報の活用流通が活発に行われるようになったが，その反面で情報漏洩や経済犯罪等の不正行為の増加も目立っており，内部統制や，監査対応の観点から情報管理の効率化と徹底が注目されるようになってきている [1].

これらの課題を解決する技術の一つとして，業務アプリケーションログを証跡として収集管理することで，後日第三者へ業務事実の存在を説明することができるようにする証跡管理製品への関心が高まっている [2].

証跡管理機能の実装方法は様々あるが，証跡管理自体は直接的な利益につながらないため，追加投資による既存システムの再開発よりも，SaaS/ASP サービスの形態で他事業者から機能提供を受ける需要も高く，サービス提供も始まりつつある [3][4].

個人情報を取り扱うシステムでも情報漏洩抑制のために SaaS/ASP サービスを利用する需要が想定で

きるが，証跡に個人情報が含まれる可能性を考慮すると個人情報保護法 [5] を遵守すべき立場からも不用意にサービスを利用することができない．

このことからも SaaS/ASP により提供される証跡管理機能を利用する場合は，証跡として意味のある情報の管理を委託しつつも，証跡に含まれる可能性のある個人情報を他事業者である証跡管理事業者から保護することを考慮しなければならない．

本稿では業務システムへ機能提供する SaaS/ASP 型の証跡管理システムモデルを定義し，証跡生成から利用までの各過程において個人情報保護をするための課題を抽出し，各課題に対して，現存する個人情報保護技術の適用評価を行う．

2　証跡管理システム

2.1　証跡管理機能

本章では最初に証跡管理システムモデルの定義を行う．証跡管理システムとは業務システム等のアプリケーションで発生した ”事実 ”を長期に渡ってその正当性を証明するシステムである．

モデル定義に先立って，まずアプリケーションシステムが ”事実 ”を記録したイベントログを生成しており，イベントログには「いつ」「誰が」「何を」「どうした」といった必要な情報が含まれていることを前提としておく．証跡管理システムはこのイベントログを事実の証跡として収集し，証明能力の付与を行い，長期の保管管理を行うシステムであり，保管されている証跡に対する閲覧要求に対しては証跡の正当性を示す情報とともに証跡に含まれる情報の提供を行うシステムと定めた．想定した証跡管理システムモデルを図 1 に示す．

このシステムが提供する基本的なサービス機能は下記の 4 機能とする．

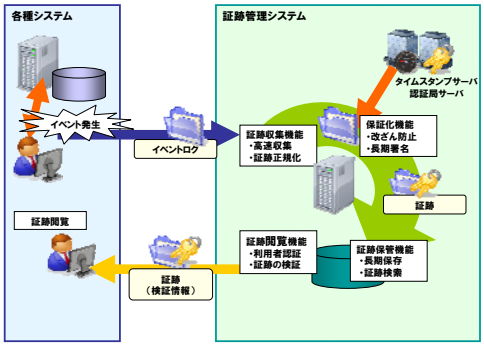

図 1: 証跡管理システム

証跡収集機能
対象となるアプリケーションシステム上で発生した事実の記録であるイベントログを証跡として収集する機能．

保証化機能
収集された証跡に対して署名付与を行うなど，証跡の改竄を防止するための処理を施し，証跡へ証明能力を付与し，後日第三者へ証明可能な状態にする機能．

証跡保管機能
保証化された証跡を証拠能力を保ったまま長期に渡り保管し，要求に応じて証跡を検索する機能．

証跡閲覧機能
証跡の閲覧要求に応じて，保管されている証跡の正当性を証明する情報とともに，証跡内容を提供する機能．

2.2　機能提供

次に証跡管理機能をネットワークを通して他のシステムへ機能提供する SaaS/ASP 型の汎用的な証跡管理システムモデルを想定する．

具体的には証跡管理システムの証跡収集機能と，証跡閲覧機能のインタフェースをネットワークを介して提供し，収集された証跡を一括して保管管理することを考える．

これによりサービス提供先のシステムではアプリケーションシステム上で発生した事実をイベントログとして記録，証跡管理システムに証跡として預けておくだけで，後日必要な時に発生事実を証明できるようになる．

尚，証跡管理システムの機能提供先として次の 2 つのシステムを想定している．

- サービス提供システム
  一般利用者を対象としてサービスを提供するシステム．サービス提供の事実を証跡として保管し，利用者への利用状況報告や，サービス提供事実の証明を行う．

- 企業内業務システム
  企業の内部で社員が業務のために利用する業務システム．業務記録を証跡として保管し，コンプライアンスや情報漏洩の抑制，監査報告の監査証跡に利用する．

3　個人情報の取扱いと課題

証跡には「誰が」という事実の行為者を特定する情報が含まれるため，特定するレベルにより，個人情報保護法の適用となる可能性が高く，その場合に

は個人情報保護の対策が必要となる．機能提供先システムにおいても，各種イベントログを証跡として証跡管理システムに収集するが，ここに利用者の情報や企業社員の社員情報が含まれるケースも十分に考えられる．

ここでは機能提供先のシステムが取り扱う証跡について，個人情報が含まれることを考慮しつつ，図2のようなユースケースの想定を想定した．このユースケースの中で個人情報漏洩につながる問題点を洗い出し，課題点を抽出する．

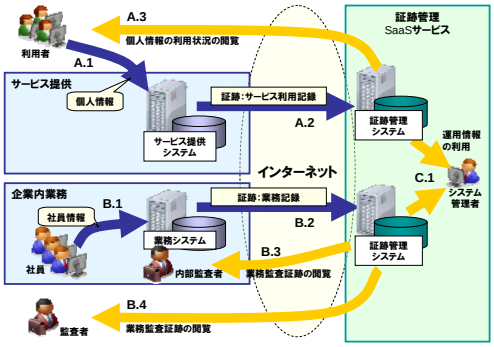

図 2: 証跡利用ユースケース

3.1 証跡利用のユースケース

定義したシステムモデルにおいて，個人情報が含まれる可能性のある証跡を取り扱う流れを各システム毎にユースケースを整理してみる．

A. サービス提供システム

1. サービスの利用と個人情報登録

   利用者はサービスの利用アカウントを取得するために個人情報の登録を行い，ログインした上で提供されるサービスを利用している．

2. サービス利用ログの証跡収集 (証跡を預ける)

   利用者が利用したサービスの利用履歴はアプリケーションイベントログとして記録されており，この情報が自動的にネットワーク先の証跡管理システムへ送付され，証跡として登録されている．

3. 本人個人情報の利用確認 (本人が閲覧)

   利用者は証跡管理システムに登録されている証跡を閲覧し，自分の利用したサービスの課金履歴等の確認を行う．

B. 企業内業務システム

1. 業務システムの利用

   各社員には業務システムを利用するための認証番号が払い出されており，社員は認証番号を用いてシステムへログインした上で各種業務を行っている．

2. 業務イベントログの証跡収集 (証跡を預ける)

   社員が実施した業務の内容は業務イベントログとし記録されており，この業務履歴は自動的にネットワーク先の証跡管理システムへ送付され，監査証跡として登録されている．

3. 内部監査 (組織内部関係者が閲覧する)

   企業内の監査者は定期的に証跡管理システムに登録されている監査証跡を閲覧し，各業務の内容の監査を実施する．

4. 第三者による監査 (組織外の者が閲覧する)

   企業外部の監査者は，証跡管理システムから監査対象とする企業の監査証跡を検索閲覧し，業務内容の監査を実施する．

C. 証跡管理システム

1. 証跡管理システムを運用する

   利用事業者の登録管理，ログや設定ファイル類のメンテナンス，バックアップ/ レストア等のシステム運用を定期的に行う．

3.2 個人情報保護の課題

個人情報を含む証跡の利用を想定したユースケースにおいて，個人情報保護の観点から個人情報漏洩と考えられる問題点を抽出し，解決すべき課題を設定する．

- サービス利用記録の証跡保管での問題点 [A.2]

  個人情報: 利用者の個人情報
  漏洩対象: 証跡管理事業者

  サービス提供システムにおいては，マーケティング情報をイベントログに出力することがある．サービス提供事業組織に閉じて利用する場合は問題ないが，組織外である証跡管理システムへ証跡として収集されると，証跡管理事業者に対する個人情報漏洩となる可能性がある．

- 本人の利用履歴の閲覧での問題点 [A.3]

  個人情報: 利用者の認証情報
  漏洩対象: 証跡管理事業者

  サービスの利用履歴の閲覧を行うためには，その履歴情報の所有者本人であることを認証する必要があるが，この時に用いられる認証情報は個人情報である．

  一方で証跡管理システムは利用者からの閲覧要求に対して認証を行う必要があるが，自身では認証情報を所有していないため，サービス提供システムへ代理認証を依頼することになる．この時，認証情報が証跡管理システム上を通過するため，証跡管理事業者に対する情報漏洩となる可能性がある．

- 監査証跡の閲覧での問題点 [B.4]

  個人情報: 社員を特定する情報 (社員番号)
  漏洩対象: 外部の監査者

  社内システムを利用するために認証が必要とされるが，この時入力する社員を特定する社員番号のような情報が監査証跡に含まれることが想定される．この情報を内部監査のように組織内部の者が閲覧することは問題ないが，組織外部の監査者による証跡の社員番号の閲覧は情報漏洩となる可能性がある．

- 証跡管理システムの運用での問題点 [C.1]

  個人情報: 証跡に含まれる全ての個人情報
  漏洩対象: 証跡管理システム運用者

  システム運用においては，システムが保管する全ての証跡情報に触れる可能性がある．アプリケーション機能により情報管理を徹底することで，システムに保管された証跡情報を保護することは可能だが，運用業務の一つである DB バックアップ/レストア作業においては，情報へ直接的に触れることができてしまうため，システム運用者に対する情報漏洩となる可能性がある．

以上から，想定した証跡管理システムモデルにおいて，個人情報が証跡に含まれる場合に解決しなければならない課題は下記の 4 点と考えられる．

1. 個人情報の抽象化

   証跡には事実の行為者を証明するための情報「誰が」を残す必要がある．従って，証跡の証明能力を失わない程度に，個人情報となる情報を抽象化する処理を施す必要がある．

2. 情報秘匿性の高い代理認証

   証跡の閲覧者の認証においては，証跡システム上に要求者の認証情報と閲覧の対象を結びつける情報を残さない工夫が必要である．

3. 閲覧者ごとに証跡情報粒度の制御

   組織内外で同じ証跡を利用する場合は，証跡の閲覧者の所属により，閲覧する証跡情報の情報量を制御する必要がある．

4. 情報保護を考慮した証跡保管

   証跡管理システムに保管される証跡は，証跡データ単体で閲覧者の目に触れても個人特定に至る情報が読み取れないことが必要である．

4 個人情報保護技術

前章に整理した個人情報管理の課題に対して，有用と考えられる個人情報保護技術の適用性などを評価することにより，SaaS/ASP 型の証跡管理システムにおける適用技術の検討を行う．

以下では，評価の対象とした個人情報保護技術についてその概要を列挙する．

暗号化
: 第三者に秘匿対象のデータの中身を知られることのないように，鍵情報を使ってデータを撹乱し，秘匿する処理を暗号化という．対象とする個人情報を含む証跡を，各種システムから証跡管理システムに送信する際に，共通鍵や公開鍵などにより暗号化することで，個人情報の不必要な漏えいを避けることができる．

開示制御 開示制御とは，対象のデータを保護し，権限を持つ利用者だけが閲覧できるように，秘匿対象のデータとその利用者の関係に基づいて，データの開示を制御する技術である．証跡管理システムにおいては，各種システムから送信された証跡を参照できる利用者を予め登録し，参照を希望する利用者がいる場合に，その利用者を認証し，証跡に対する参照権限があるかどうかを判断した上で，承認された参照である場合に証跡を開示することが考えられる．一方，利用者が証跡管理システムから証跡データを取得する際に，承認された利用者だけが参照できるように，証跡データをカプセル化し，参照するための鍵情報であるライセンスとともに配布する DRM 技術も，一種の開示制御技術である．

匿名化 個人情報を含む証跡を第三者に開示する際に，個人を特定可能な情報を取り除き，また情報としての粒度を粗くする一般化などのを行うことにより，個人の特定を防ぐように個人情報を処理する技術を，匿名化技術という．年齢や性別，住所といったデモグラフィック情報を個人情報として含む証跡の場合に，たとえば年齢を年代に置き換える，住所を都道府県のレベルに一般化するなどの処理を行うものである．各種のサービス・システムから証跡管理システムに証跡データを送る際に匿名化する場合と，証跡管理システムにおいて蓄積した証跡データを匿名化する場合の二通りが考えられる [6][7].

秘密計算 秘密計算技術は，秘匿対象のデータを暗号化したままで，分析者において任意の計算を実行することを可能とする技術である．一般に，秘密計算技術は複数の分析者が協力して演算処理を実行することにより，暗号化したデータを復号することなく，計算することが可能となる．そのため，複数の機関にまたがって証跡を管理する場合に有用であると考えられる [8].

匿名認証 匿名認証技術とは，利用者が誰であるかを明かすことなく，利用権限があることをサーバに対して証明することで，匿名のままで利用者を認証できる技術である．類似の技術として属性認証があり，こちらは利用者が利用者がある属性すなわち利用権限のあるグループなどに属していることを証明することにより，匿名の利用者を認証する技術である．また，これらの匿名認証技術においては，一定の条件を満たす場合に匿名性を剥奪し，利用者が誰であったかを後から追跡できる追跡性を持つものもある [9].

プライベート情報検索 (PIR) プライベート情報検索（Private Information Retrieval, PIR）とは，データベースに問合せを行う際に，利用者が何を検索したかをサーバ自体に明らかにすることなく，利用者が望む検索結果を得ることを可能とする技術である．証跡管理システムに蓄積された証跡に対して検索処理を行うことは，誰が誰の証跡にアクセスしたかの記録が残るため，こうしたプライベート情報検索により，誰の証跡を検索したかを秘匿することは利用者の個人情報保護に有用であると考えられる [10].

5 適用評価

最後に 3 章で設定した課題に対して，個人情報保護技術の有効性を検証する．そのためにまず証跡管理システムに対して技術の適用方法を検討し，各適用方法に関して課題に対する有効性の評価を行う．

5.1 証跡管理システムへの技術適用

まず証跡管理システムの機能「収集」「保証」「保管」「閲覧」が動作する部分に，改良を加える形で，個人情報保護技術の適用方法を考案した．加えた改良内容について下記の機能部分ごとに説明する．

収集：証跡生成元で証跡を収集する時の処理
保証：証跡管理システムで証跡保証化時の処理
保管：証跡を保管する時のインデックス情報
閲覧：保管された証跡を閲覧する時の処理

技術適用例

A. 証跡の**暗号化**

証跡生成元で証跡を暗号化した後に証跡管理システムへ送信する．

収集：証跡生成元の鍵で証跡を暗号化
保証：暗号化された証跡に対して署名
保管：保管日時
閲覧：閲覧者は証跡生成元から
　提供された鍵で証跡を復号化して閲覧

B. 証跡の個人情報の**匿名化**

証跡に含まれる個人情報部分を個人特定に至らない程度に抽象化する．

収集：証跡内の個人情報を匿名化
保証：匿名化された証跡に対して署名
保管：匿名化された証跡情報
閲覧：証跡をそのまま閲覧

C. **秘密計算**による閲覧制御

秘密計算用の秘密鍵を証跡生成元と証跡管理システムで所有し，署名や閲覧において，両者の合意する情報範囲で復号化を行う．

収集：公開鍵で証跡を暗号化
保証：秘密計算で復号化した証跡に署名
保管：証跡に含まれるメタ情報
閲覧：秘密計算で復号化した証跡情報を閲覧

D. **開示制御**による閲覧制御

証跡に含まれる個人情報を閲覧可能な対象者のみに閲覧を許可する．

収集：証跡をそのまま収集
保証：証跡内容の検証と署名
保管：証跡に含まれるメタ情報
閲覧:閲覧者に対して情報項目単位で開示制御

E. **匿名認証**による閲覧者認証

閲覧要求者の認証を匿名で行う．閲覧対象の証跡の秘匿は行わない．

閲覧：閲覧者を匿名のまま認証

F. **PIR** による認証情報保護

認証された閲覧要求者が行った閲覧対象証跡の秘匿を行う．

閲覧：PIR で閲覧対象証跡を秘匿

5.2 有効性評価

考案した技術適用例について，3 章で抽出した課題に対する有効性の評価を行い，まずは証跡自体の情報保護に関する課題 (1,3,4) について表 1 に示した．評価観点は課題に対して安全な対処であるかという安全性と，証跡管理システムが扱う証跡として証拠能力の程度を問う証拠性である．

表 1 の評価の結果，想定した証跡管理システムモデルにおいて，秘密計算技術の有効性が認められた．また，情報保護技術の適用は証跡に含まれる情報保護の安全性は高まる一方で，証跡の証拠性が失われる傾向があることが分かった．

次に証跡の閲覧時の認証における課題 (2) については表 2 に示した．評価観点は課題への対処の安全性である．

表 2 の評価の結果，想定した証跡管理システムモデルにおける本人閲覧サービスの課題に対して有効な技術を見出せなかった．

6 まとめ

本稿では，SaaS/ASP 型でサービス提供を行う証跡管理システムモデルを定義し，個人情報を含む証跡を取り扱う場合における課題の抽出を行い，課題に対する個人情報保護技術の有効性の評価を行った．

その結果，同システムモデルにおいては個人情報保護に関する課題があり，証跡に対する情報保護対策が必要であることを示した．対策技術の適用では，秘密計算技術に有効であることを示し，情報保護の

	1	3	4	証拠	証拠性の評価根拠
A	◎	×	◎	△	証跡内容の証明が困難
B	○	○	○	○	情報抽象化レベルにより 安全性と証拠性がトレードオフ
C	○	◎	◎	○	合意する証跡情報範囲により 安全性と証拠性がトレードオフ
D	×	◎	×	◎	証跡内容の証明が可能

表 1: 情報保護課題 (課題 1,3,4) に対する有効性

	課題 2	評価根拠
E	×	閲覧者の秘匿は行えるが，閲覧した対象から，個人特定に至る情報が残る可能性がある．
F	×	閲覧した対象を隠せるが，閲覧者が特定されており，個人特定に至る情報が残る．

表 2: 閲覧者認証課題 (課題 2) に対する有効性

安全性と証跡の証拠性がトレードオフ関係にあることを示した．閲覧者の認証において個人情報漏洩を完全に防止する有効な技術を見出すことはできなかった．

今回有効とした秘密計算技術は性能面での課題があるとされており，今後は技術の性能面も含めて検討を深めるとともに，安全性と証拠性の両方の条件を満たすための課題について検討を進めていく予定である．

参考文献

[1] IDC Japan，産業分野別 国内コンプライアンス市場，`http://www.idcjapan.co.jp/Press/Current/-20090421Apr.html`

[2] ITR，ITR Market View セキュリティ・ログ市場 2009，http://www.itr.co.jp/press_release/090811PR/

[3] NTT Communications，セキュアログ管理サービス，http://www.ntt.com/icto/security/data/security-log.html

[4] JIEC，Log Shelter，http://www.jiec.co.jp/service/logshelter/index.html

[5] 個人情報の保護に関する法律 (個人情報保護法) http://www5.cao.go.jp/seikatsu/kojin/houritsu/-index.html

[6] Willenborg, L. and de Waal, T., Statistical Disclosure Control in Practice, Lecture Notes in Statistics 111, Springer, 1996.

[7] Willenborg, L. and de Waal, T., Elements of Statistical Disclosure Control, Lecture Notes in Statistics 155, Springer, 2000.

[8] 千田浩司, 谷口展郎, 山本剛, 岡崎聖人, 塩野入理, 金井敦, エルガマル暗号に基づく秘匿回路計算の実装と応用, コンピュータセキュリティシンポジウム 2005 (CSS2005) 予稿集, pp. 475–480, 2005.

[9] J. Kilian and E. Petrank, “ Identity Esclow ”, In Proceedings of Crypto’98, LNCS1462, pp. 169–185, 1998.

[10] B. Chor, O. Goldreich, E. Kushilevitz and M. Sudan, “ Private Information Retrieval ”, Journal of the ACM 45 (6), pp. 965–982, ACM, 1998.