情報の来歴管理等の高度化・容易化に関する研究開発
R&D for enhancing functionality and usability of information history management

研究代表者　小松 尚久　早稲田大学

研究期間　　平成 19 年度～平成 21 年度

【Abstract】

This paper presents the outcome of "R&D for enhancing functionality and usability of information history management".

The R&D is about the technologies for prevention of information leakage, especially for those who care the increased cost or inconvenience associated with traditional technologies. Using trace logs of classified information, we aim to achieve both the efficiency of end-users' work and security of information management within organizations irrespective of data media format, such as electronic files or paper documents, in which the classified information is recorded. The R&D consists of three fundamental technologies, Technologies for Information History Management among Multimedia, Technologies for Group Signatures, and Technologies for Cancelable Biometrics based on Protected Templates.

The R&D has completed its 3 years of research period (2007-2010) with many benefical and useful outcomes for a infrastructure platform to prevent information leakage. This paper also provides many intellectual properties, technical papers, and presentation materials that have been developed through the R&D.

1　研究体制

○　**研究代表者**　　小松 尚久（早稲田大学）

○　**研究分担者**　　舩曳 信生†（岡山大学†）

田代 勤††（株式会社日立製作所††）

佐古 和恵†††（日本電気株式会社†††）

島津 秀雄††††（ＮＥＣシステムテクノロジー 株式会社††††）

○　**研究期間**　　平成 19 年度～平成 21 年度

○　**研究予算**　　総額　949 百万円

（内訳）

平成 19 年度	平成 20 年度	平成 21 年度
441,030,127	255,701,224	252,292,391

2　研究課題の目的および意義

組織における職員等による重要情報の持ち出し等による情報漏えいの被害が社会問題として顕在化している。情報の無断持ち出しや不正流用などに起因する情報漏えいを抑止・防止し、被害を防止するため、情報の来歴管理を高度化・容易化するための技術を開発し、情報の来歴を管理するための基盤技術の確立を早期に進めることにより、安心・安全なＩＣＴ利用環境の整備に資することを目的とする。

具体的な研究開発目標としては、情報の流通経路を把握可能とし、情報漏えい行為の抑止および適切な情報流通の促進を図るため、本研究開発では、サイバー空間と物理空間の区別なく、組織間を流通する情報（電子／物理媒体）の来歴の統一的な管理を実現する「メディアシームレス対応来歴管理技術」、扱う情報に応じて適切なレベルでの情報開示を可能とする「グループ電子署名技術」、更に異なる組織間での本人認証においても、システムに登録された利用者の生体情報（テンプレート）の安全性が保証される「テンプレート保護型生体認証技術」の研究開発を行い、高度な来歴管理機能を有した基盤技術の確立を目標とする。

３　研究成果

３．１　メディアシームレス対応来歴管理技術

３．１．１　組織シームレス来歴管理技術

初年度は、大企業等の大規模組織を想定し、３組織以上の大規模組織間で、大量の来歴（数百ギガバイト以上）から効率良く必要な来歴を取得可能な管理技術を確立する。さらに、他組織の従業員等の情報を開示することなく、他組織に送信した機密情報の取り扱い状況を検証可能な技術の確立を目標とする。

２年目以降は、大量の来歴を管理した場合に、利用者に来歴管理を意識させないために、来歴の登録を実用化されている一般的なクライアントサービスと同程度の処理時間（１秒未満）で完了する技術の確立を目標とする。また、機密情報の漏えいが発生していないかを確認する管理者等の業務を効率化するために、来歴情報の取得、信頼性検証の性能を数秒以内に完了することを目標とする。

上記目標を達成するために、第一年目に公知技術の調査、基本アーキテクチャの設計を行い、第二年目にプロトタイププログラムの構築を行い、第三年目にプロトタイププログラムを大規模化・高性能化し、目標を達成するという研究開発マネジメントを原則として行った。以下、詳細について説明する。

(1) コンテンツを特定し来歴を管理するための ID 体系の研究開発

① コンテンツを管理している組織が複数存在する場合の ID 体系の基本アーキテクチャの確立

電子文書については、互いに連携しなくても各組織でユニークな識別子を生成可能な「UUID」（Universally Unique Identifier）などの既存の ID 体系について調査した。紙文書に対して電子透かしについて調査した。上記調査結果を基に、来歴管理に適した新しい ID 体系（来歴 ID）の基本アーキテクチャを確立した。

② コンテンツに対して ID を発行し、付与する基本手順の確立

上記アーキテクチャに準拠した 128 ビットの ID を発行するプログラムを実装した。紙文書に対しては、印刷時に印刷物に 128 ビットの QR コードを書き込む方式と、128 ビットの電子透かしを埋め込む方式 2 つを開発した。

特に印刷物に 128 ビットの電子透かしを埋め込む技術は、これまでない新しい方式である。公知の電子透かし技術は紙文書の背景部分にドット（地紋）を打つことで ID を埋め込む方式だが、

本研究で開発した技術は、文字の輪郭や画像の明るさを微妙に変更することで ID を埋め込む。従来このような方法では 128 ビットの ID を埋め込むことができなかったが、本研究で画像処理や誤り訂正を見直すことで、128 ビットの ID を埋め込むことが可能になった。

③ ID が付与されたコンテンツから ID を抽出する基本手順の確立

これまで開発した、電子透かし技術を用いた来歴 ID の発行手順、来歴 ID からコンテンツを特定する方式のプロトタイププログラムを高性能化し、電子ファイル、紙媒体を複数回行き来するようなメディア変換後でも、誤識別率 100 万分の 1 以下で正しく来歴を追跡可能な技術を実装した。

特に、数値計算および透かしの検出実験を行なうことで最適な誤り訂正符号を選定し、誤識別率 10^{-50} 以下を達成した。

(2) 組織間の来歴情報引継ぎ技術の研究開発

① 組織間の来歴情報引継ぎ体系の基本アーキテクチャの確立

組織シームレス来歴管理システムは、さまざまな組織をまたがって流通する物品に ID タグをつけて管理する「トレーサビリティシステム」に類似している。そこで、トレーサビリティの標準化団体「EPCglobal」の標準仕様を参考にすることで、組織シームレス来歴管理を実現するための全体構成を明確化した。また、メール、紙文書、外部記憶媒体など別の来歴管理組織に流通する可能性のあるコンテンツについて具体的にその来歴管理を考察し、問題点を明らかにした。上記考察結果をもとに、組織間の来歴情報引継ぎ体系の基本アークテクチャを確立した。

② 来歴情報交換プロトコルとそのメッセージフォーマットの策定

上記組織間の来歴情報引継ぎ体系の基本アークテクチャを基に、組織間来歴通信プロトコルを設計した。また、組織間を流通するコンテンツが引き起こす脅威と対策を洗い出し、来歴管理技術の有用性、カバー範囲を明確化した。これらの組織間流通による脅威の対策となるように、来歴情報交換プロトコルとそのメッセージフォーマットのプロトタイププログラムを開発した。このプロトタイププログラムを大規模化、高性能化し、3 組織以上にまたがって流通するコンテンツの来歴管理を確立した。

特に、本研究で開発した基本アーキテクチャ、およびプロトタイププログラムにおいては、大企業等の大規模組織での利用に耐えうるスケーラビリティの具備を目的として、複数の組織で来歴管理を分散しており、具体的には、3 組織以上の大規模組織間で、大量の来歴（300GB）から効率良く必要な来歴を取得可能である。

③ 異なる組織のコンテンツの ID を特定する処理手順の確立

上記組織間の来歴情報引継ぎ体系の基本アークテクチャを基に、組織間来歴検索プロトコルを設計した。また、組織間を流通するコンテンツが引き起こす脅威と対策を洗い出し、これらの脅威の対策となるように、組織間来歴検索プロトタイププログラムを開発した。このプロトタイププログラムを大規模化、高性能化し、3 組織にまたがった来歴の検索であっても、1.8 秒以内で検索処理が完了するシステムを確立した。

(3) 来歴情報から統一フォーマットへ変換・照合する技術の研究開発

① 来歴情報の統一フォーマットの策定

来歴管理への適用を念頭に、既存の電子署名技術について調査した。さらに、組織シームレス

来歴管理システムの脅威と対策について考察し、電子署名技術の適用方法を明確化した。上記考察を基に、来歴情報の真正性を保証し、かつ来歴情報自体からの情報漏えいを防止するための統一フォーマット及びプロトコルを確立した。

② 来歴情報を照合するための基本手順の確立

上記来歴情報の統一フォーマット等をもとに、来歴管理組織が複数存在し、それぞれ異なる管理をしている場合に、来歴情報を統一フォーマットに変換し、照合するためのプロトタイププログラムを開発し、基本手順を確立した。

特に、利用者に来歴の登録を意識させないよう、来歴の収集、変換、登録にかかる処理時間を 0.13 秒で完了する技術を確立した。

③ 来歴情報の真正性を保障するための基本方式の策定

来歴情報の真正性を保証し、かつ来歴情報自体からの情報漏えいを防止するためのプロトタイププログラムを、墨塗り署名技術、グループ署名技術を用いて開発した。しかし、墨塗り署名技術単体では署名者に関する情報が漏えいする、グループ署名技術単体では来歴情報自体に含まれている個人情報が漏えいするという問題があった。そこで、墨塗り署名とグループ署名の利点を併せ持つ「墨塗りグループ署名技術」を新たに設計・開発し、来歴情報の真正性を保障するための基本方式を確立した。

特に、「墨塗りグループ署名技術」は、来歴情報の真正性を保証し、かつ来歴情報自体からの情報漏えいを確実に防止することができる新しい電子署名方式であり、「３．２　グループ電子署名技術」とまたがる研究成果である。墨塗りグループ署名技術の研究は第二年目から着手したため、密に連携して作業を分担し、短期間で効率よく成果を出すことを目標とした研究開発マネジメントを行った。具体的には、第二年目に基本アーキテクチャの設計を共同して行い、第三年目にプロトタイププログラムの構築および高性能化を行うことで、目標を達成した。

(4) 組織シームレス認証技術の研究開発

① 利用者認証システムの基本アーキテクチャの確立

認証者である組織側の認証サーバが、利用者が正当な生体情報を提示していることを確認することのできる利用者認証システムの基本アーキテクチャの仕様策定および基本システムのプロトタイププログラムの開発と実験評価を行った。具体的には、第一年目に、利用者認証システムの基本アークテクチャを策定し、プロトタイププログラムを開発し、実証実験を行い、目標を達成した。

② 利用者登録・認証方式、プロトコル、およびデータフォーマットの策定

認証者に対して利用者の生体情報そのものを開示せずに利用者認証を可能にする認証方式に関して、有力な既存技術に関する詳細調査を実施した。また、既存技術の評価を目的としたプロトタイププログラムを開発した。具体的には第一年目に、利用者の生体情報そのものを開示せずに利用者認証を可能とする方法の調査を実施、評価目的のプロトタイププログラムを開発し、目標を達成した。

③ 利用者認証システムの運用方式の確立

第二年目以降、「３．テンプレート保護型生体認証技術の研究開発」に引き継ぎ、複数組織間において、安全に登録情報を移行し、認証することが可能な運用方式を確立した。

④ 機器認証システムの基本アーキテクチャの確立

耐タンパ性を有したデバイスを機器の一部に実装し、機器間相互認証を実現する、機器認証システムの基本アーキテクチャの仕様策定およびプロトタイププログラムの開発を行った。具体的には、第一年目に、耐タンパ性を有したデバイスを機器の一部に実装し、機器間相互認証を実現する、機器認証システムの基本アーキテクチャの仕様策定およびプロトタイププログラムを開発、第二年目に、機器認証デバイスを検証するための利用者 PC 向けの機器認証デバイス(USB メモリデバイス)検証システムを開発し、目標を達成した。

⑤ 機器の登録・認証方式、プロトコル、およびデータフォーマットの策定

高度な演算機能を必要とせずに署名付与を行うことのできる署名方式の調査および基本方式の仕様策定、およびプロトタイププログラムの開発を行った。具体的には、第一年目に高度な演算機能を必要とせずに署名付与を行うことのできる署名方式の調査および基本方式の仕様策定、およびプロトタイププログラムを開発し、第二年目に機器認証デバイス(USB メモリデバイス)に実装し、上記の認証システムに適用し、目標を達成した。

⑥ 機器認証システムの運用方式の確立

最終目標である組織シームレス認証技術を実現するため、プロトタイプを開発する。具体的には、第二年目までに策定、開発した単一組織内での機器認証デバイス検証システム（ＵＳＢメモリ認証システム）を基に、これを拡張し、複数の組織にまたがって情報をやり取りする可搬媒体の真正性を保証する機器認証システムの開発を行い、複数組織間で、組織をまたいで機器認証デバイスの登録と検証を行い、正当なデバイスのみの使用を可能とするシステムを確立し、目標を達成した。

３．１．２　メディアシームレス来歴情報付与・検知技術

メディアフォーマットに応じて柔軟に、識別ＩＤまたはそれに付随する来歴を情報に不可分に対応付けるため、初年度に、既存ファイルシステム、デバイスドライバ、プリンタドライバ等の機能特性の分析、および、例えば白黒二値文書のような情報を付与しにくいコンテンツに対しても、メディア品質を維持しながら、数百ビットの情報量を電子ファイル、紙文書に埋め込む技術の確立を目標とする。

2 年目以降では、サイバー空間と物理空間を複数回行き来するような多様なメディア変換後にも埋め込んだ情報が高精度で検出可能な技術を確立するとともに、電子媒体から紙文書などの物理媒体に変換し電子媒体に戻したときに異なった埋め込み情報を検出する確率を、工学的に信頼性を確保できる確率である 100 万分の 1 以下に抑えることを目標とする。さらに、ユーザに来歴管理を意識させないために、識別ＩＤ等の埋め込み、検出、および来歴の発行・管理ともに実用化されている一般的なクライアントサービスと同程度の処理時間（１秒未満）で完了することを目標にする。

また、組織シームレス来歴管理技術とともに、要素技術を確立するとともに、これらの技術を、ファイルシステム、デバイスドライバ、プリンタドライバ等に製品レベルの実装を行い、３組織以上に跨る来歴管理基盤として利用可能なことを担保するための実証実験を行うこととする。

上記目標を達成するために、第一年目に公知技術の調査、基本アーキテクチャの設計を行い、第二年目にプロトタイププログラムの構築を行い、第三年目にプロトタイププログラムを大規模化・高性能化し、目標を達成するという研究開発マネジメントを原則として行った。システムが大規模であるため、公知技術については綿密に実機調査を行って利用可否を判断し、無駄な新規開発をせず研究を加速できるように留意した。以下、詳細について説明する。

(1) 電子ファイルに対する来歴情報管理技術の研究開発

① 電子ファイルの来歴情報を管理するための基本アーキテクチャの確立

既存のログ収集ソフトウェアについて実機調査を行い、既存のソフトウェアで来歴情報を管理できる操作とそうでない操作を明確化した。具体的には、電子ファイルの生成に関する来歴情報の収集に課題があることが明らかとなった。この調査結果をもとに、電子ファイルの来歴情報を管理するための基本アーキテクチャを確立した。

② 電子ファイルの PC 内部での操作を監視するための基本手順の確立

上記基本アーキテクチャをもとに、既存の PC 内の操作ログ収集ソフトウェアをベースとし、PC 内の操作ログを整形して来歴 DB に登録する「来歴登録サービス」のプロトタイププログラムを開発した。また、電子ファイルの生成に関する来歴情報の収集を行うプロトタイププログラムを開発した。これらのプログラムにより、PC 内部での操作を監視するための基本手順を確立した。

③ 電子ファイルの PC 外部への送受信を監視するための基本手順の確立

上記基本アーキテクチャをもとに、ネットワークを介する PC 外部に渡る電子ファイルの操作を監視し、操作ログを収集する機構を設計した。既存のログ収集ソフトウェアをベースとして、電子メール、可搬媒体などといった PC 外部への送受信に関する操作ログを整形して来歴 DB に登録する「来歴登録サービス」のプロトタイププログラムを開発した。これらのプログラムにより、PC 内部での操作を監視するための基本手順を確立した。

(2) 物理メディアに対する来歴情報管理技術の研究開発

① 物理メディアの来歴情報を管理するための基本アーキテクチャの確立

紙文書の印刷・複写に関する処理はプリンタ・複写機の機種ごとに独自であるという現状を鑑みて、複写機ベンダの協力の下、紙文書の来歴情報を管理するための基本アーキテクチャを確立した。

特に複合機については仕様が公開されていないため複合機ベンダの協力（仕様公開）が必要である。まずは来歴管理複写機プログラムの基本アーキテクチャを策定し、これをもとに複合機の仕様を最小限開示してもらうことで、マルチベンダに紙文書の来歴情報を管理するための基本アーキテクチャを確立した。

② 電子ファイルから物理メディアに遷移したとき来歴情報の引継ぎ手順の確立

上記基本アーキテクチャをもとに、印刷元の電子ファイルを特定する機構を開発した。具体的には、「３．１．１　組織シームレス来歴管理技術」で研究した ID 付与・検知方式をベースに、印刷時に印刷物に 128 ビットの QR コードを書き込むプリンタドライバと、128 ビットの電子透かしを埋め込むプリンタドライバの 2 種類を開発した。プリンタドライバについては高速化につとめ、ユーザに来歴管理を意識させないように、ID の埋め込みなどといった印刷処理を通常の印刷の最大 1.35 倍（印刷開始まで 1 秒以内）におさえる方式を確立した。また、後者の電子透かしを埋め込むプリンタドライバについては信頼性の向上につとめ、電子ファイル、紙媒体を複数回行き来するようなメディア変換後でも、誤識別率 100 万分の 1 以下で正しく来歴を追跡可能な技術を確立した。

特に、これらのプリンタドライバについては、OS へのフック方法を工夫することで、既存のログ収集ソフトウェアでは収集できないような印刷元の電子文書に関する情報（フルパスおよび電

子ファイル内のテキスト情報）を取得できるようにした。これにより、電子ファイルから物理メディアに遷移したときに来歴情報を確実に引継げるようになった。

③ 物理メディアから別の物理メディアに遷移したとき来歴情報の管理手順の確立

上記基本アーキテクチャおよび開示された複合機の仕様をもとに、紙文書の複写に関する来歴管理を可能にする複合機連携プロトタイププログラムを、リコーおよびキヤノン複合機を用いて開発した。複写時に複合機から外部サーバに紙文書のスキャン画像を送信し、当該サーバで QR コードまたは電子透かしの方式で紙文書に付与された ID を読み取ることで、紙文書の複写に関する来歴管理が可能になった。

特に、紙文書の来歴管理と複合機内部で行う処理を分離することで高速化につとめ、通常の複写と遅延がほとんどなく紙文書の複写の来歴を管理できる方式を確立した。具体的には、ID の検出などといった複写処理を通常の 1.2 倍（複写開始まで 1 秒以内）におさえる方式を確立した。

また、紙文書をスキャナで読み取ってから裁断するスキャナ付きシュレッダとも連携して紙文書の廃棄の来歴管理を行うプロトタイププログラムを開発した。これにより、紙の生成から廃棄まで、紙文書のライフサイクルを管理できるようになった。

④ 物理メディアから電子ファイルに遷移したとき来歴情報の引継ぎ手順の確立

上記基本アーキテクチャおよび開示された複合機の仕様をもとに、紙文書の電子化に関する来歴管理を可能にする複合機連携プロトタイププログラムを、リコーおよびキヤノン複合機を用いて開発した。電子化時に複合機から外部サーバに紙文書のスキャン画像を送信し、当該サーバで QR コードまたは電子透かしの方式で紙文書に付与された ID を読み取ることで、紙文書の電子化に関する来歴管理が可能になった。ユーザに来歴管理を意識させないために、ID の検出などといった電子化処理を通常の 1.2 倍（電子化開始まで 1 秒以内）におさえる方式を確立した。

(3) 来歴管理サーバを統合管理する技術の研究開発

① 電子ファイル物理メディアそれぞれで管理している来歴情報を統合するための基本アーキテクチャの確立

上述の電子ファイルや紙文書の来歴管理システムをもとに、電子ファイル、物理メディアの来歴情報を管理しているサーバ間の通信プロトコル、および電子ファイル、紙文書それぞれで管理している来歴情報を紐付けるための基本アーキテクチャを策定した。

② 来歴情報統合プロトコルの策定

上記基本アーキテクチャをもとに、電子ファイル、物理メディアの来歴情報を管理しているサーバ間の通信プロトタイププログラム、および複数のログ関連付け方式を強化し、さまざまなコンテンツのログを一元管理する来歴 DB の開発を行った。

特に、利用者に来歴の登録を意識させないよう、来歴の発行・管理にかかる処理時間を 0.13 秒で完了する技術を確立した。

③ 統合来歴情報を探索するための基本手順の確立

上記基本アーキテクチャをもとに、来歴 DB から来歴情報を検索するためのプログラムを設計・開発した。既存のファイルを追跡するようなソフトウェアでは、操作元のファイルが複数である場合にはうまく追跡できないが、操作元を複数表示できるように、探索した来歴情報の表示形式を設計し、流出元の特定をより高信頼に行なうことができる基本手順を確立した。

特に、「３．３テンプレート保護型生体認証技術」と連携し、来歴情報検索プロトタイププログ

ラムに生体認証機能を追加して、管理者でなければ来歴情報を検索できないようにした。テンプレート保護型生体認証技術の研究は第二年目から着手したため、密に連携して作業を分担し、短期間で効率よく成果を出すことを目標とした研究開発マネジメントを行った。具体的には、第二年目に基本アーキテクチャの設計を共同して行い、第三年目にプロトタイププログラムの構築および高性能化を行うことで、目標を達成した。

④ 来歴管理技術の評価モデル設計

来歴管理技術の実際の運用場面を想定して、3 組織間における評価モデルを設計した。具体的には、実際に発生している情報漏えい事故の要因、形態を踏まえ、委託先・ビジネスパートナーに起因し漏えい事故を想定して評価モデルを設計した。

⑤ 来歴管理技術の評価

上記評価モデルに基づいて実証実験を行なった。具体的には、基本計画書にて研究課題毎に示された到達目標を、それぞれの研究課題単位でクリアしているかを検証するとともに、開発した技術を連携させ、統合システムとして機能させた際に、情報漏えい対策(予防)の基盤技術として有効であるかを、有識者に対するアンケートにより評価した。その結果、到達目標を達成することを実証するとともに、約 80%の有識者により来歴管理システムが有効であるとの評価が得られた。

また、総務省委託研究「ネットワークを通じた情報流出の検知及び漏出情報の自動流通停止のための技術開発」（P2P 情報漏えい対策プロジェクト）と連携するためのプロトタイププログラムを開発し、P2P ネットワークに流出してしまった情報に対し、漏えい経路を特定できることを実証した。

(4) サイバー空間での電子ドキュメントの中央集権型来歴制御技術に関する研究開発

① 来歴管理サーバのアーキテクチャと実現方式の確立

中央集権型サーバで実施される電子ドキュメントの権限譲渡、カプセル操作、アクセス権変更等の来歴関連事象を記録し、閲覧または追跡表示を行うことが可能なアーキテクチャの策定とプロトタイプを開発試作することで実現方式を確立した。

② 常時接続型カプセルサーバのアーキテクチャと実現方式の確立

電子ドキュメントの権限譲渡及び許諾情報管理を行う中央集権型カプセルサーバのアーキテクチャの策定とプロトタイプを開発試作することで実現方式を確立した。

③ カプセル運用エンジンのアーキテクチャと実現方式の確立

基本的なアクセス権管理を行う運用エンジンのアーキテクチャの策定とプロトタイプを開発試作することで実現方式を確立した。

上記３つの目標に対する技術を実現することで、一つのサイバー空間内で流通する電子ドキュメントの中央集権型来歴制御に関する技術を確立することで目標を達成した。

(5) 複数のサイバー空間でのプライバシ保持型電子ドキュメントの来歴制御技術に関する研究開発

① 多重認証サーバのアーキテクチャと実現方式の確立

組織内で流通している電子ドキュメントを組織外で流通可能な電子ドキュメントに変換することで組織外でも認証可能なアーキテクチャの策定とプロトタイプを開発試作し実現方式を確立した。

② 多重来歴管理サーバのアーキテクチャと実現方式の確立

組織内で来歴事象の記録と、組織外での来歴事象の記録をシームレスに連結活用可能なアーキテクチャの策定とプロトタイプを開発試作し実現方式を確立した。

③ 常時接続型多重カプセルサーバのアーキテクチャと実現方式の確立

組織内で流通している電子ドキュメントを組織外で流通可能な電子ドキュメントに変換することで組織外でも権限変更などを可能にするアーキテクチャの策定とプロトタイプを開発試作し実現方式を確立した。

④ 常時接続型多重カプセル運用エンジンのアーキテクチャと実現方式の確立

組織内で流通している電子ドキュメントを組織外で流通可能な電子ドキュメントに変換することで組織外でもアクセス権管理を行うことが可能なアーキテクチャの策定とプロトタイプを開発試作し実現方式を確立した。

上記４つの目標に対する技術を実現することで、複数のサイバー空間間での電子ドキュメントのシームレスかつ安全な流通を行える技術を確立することで目標を達成した。

(6) 任意のサイバー空間での電子ドキュメントの多重来歴追跡技術に関する研究開発

① 非接続型認証サーバのアーキテクチャと実現方式の確立

常時ネットワークに接続していない端末からでも電子ドキュメントへの操作認証が可能なアーキテクチャの策定とプロトタイプを開発試作し実現方式を確立した。

② 非接続型カプセルサーバのアーキテクチャと実現方式の確立

常時ネットワークに接続していない端末からでも電子ドキュメントのアクセス権限操作を行うことが可能なアーキテクチャの策定とプロトタイプを開発試作し実現方式を確立した。

③ 非接続型運用エンジンのアーキテクチャと実現方式の確立

常時ネットワークに接続していない端末からでも電子ドキュメントのアクセス権管理を行うことが可能なアーキテクチャの策定とプロトタイプを開発試作し実現方式を確立した。

上記３つの目標に対する技術を実現することで、複数のサイバー空間で、常にネットワークに接続していない環境においても権限制御を行った電子ドキュメントの利用を制御することを達成した。

④ 非接続型カプセル探索・収集エンジンのアーキテクチャと実現方式の確立

インターネット上に上記カプセル化を行った電子ドキュメントが流失した場合において、短期間に探索及び来歴情報を収集するアーキテクチャの策定とプロトタイプの開発試作し実現方式を確立した。

３．２　グループ電子署名技術

初年度は、大企業等の大規模組織を想定し、３組織以上の大規模組織間で、他組織からは、署名者の組織や所属のみを証明可能とし、組織内部では、署名者個人を証明可能とする署名方式の確立を目標とする。署名方式には、上記の現状の技術課題を克服するアルゴリズムを検討するとともに、計算量理論に基づいた安全性を短い署名長（数十キロビット以下）で実現する方式とする。また、鍵および証明書の失効方式を確立し、メンバの追加および削除に関して、組織の他メンバが行う処理を軽減させることを目標とする。

さらに 2 年目以降では、ユーザに署名付与、検証処理を意識させないために、任意のコンテンツに

対して、署名の付与および検証を実用化されている電子署名と同程度の処理時間（１秒未満）で完了することを目標とする。また、複数の組織に所属するメンバの署名の検証を組織ごとに署名者個人の検証を可能とする方式の確立を目標とする。さらに、複数組織に所属するメンバによる複数秘密鍵の管理の利便性向上を目標とする。

(1) 低コストを実現するグループ電子署名技術の研究開発

① 携帯端末向けグループ電子署名技術の確立

スマートフォン向けグループ電子署名プログラムを開発した。具体的には、スマートフォン上で有効となる演算高速化手法の複数検討を行い、その中で特に有効な 2 種類の高速化手法を適用した。実装したプログラムは、Willcom WS011SH 上で署名生成を 0.393 秒で行う。これにより、当初の目標である、低コスト端末において来歴ログにプライバシを保護しつつ署名を施す処理時間を 1 秒以内で完了を達成する技術を確立した。

② グループ電子署名向け演算チップ

グループ電子署名の生成・検証を行う演算チップを開発し、多様な機器でプライバシを保護しつつ来歴情報を流通させる技術を確立した。グループ電子署名演算チップの開発に向けて、初年度は FPGA プロトタイプを実装し、40MHz 駆動で署名生成・検証に 0.85 秒程度という結果を得た。2 年目は、初年度に作成したプロトタイプの最適化を行い、処理速度の向上と回路サイズの削減を行った。3 年目はグループ電子署名の ASIC 実装を行い、バックエンド工程で生じる各種の問題を解決し、100MHz 駆動したとき、署名生成に 0.135 秒、検証に 0.103 秒という処理性能を有するチップを開発した。

③ 署名者に大きな負荷をかけることなくユーザ無効化が可能となる失効技術の確立

署名者が失効処理に関与しない失効手法である検証者ローカル失効法(Verifier Local Revocation: VLR)を利用することにより、失効に関係しない署名者に大きな負荷をかけることなくユーザ無効化が可能となる失効技術を確立した。

本失効法は楕円曲線上で定義されるペアリングと呼ばれる演算を必要とするが、本研究以前は、RSA2000 ビット級のセキュリティレベルに対して効率なペアリング実装が存在しなかった。それに対して、本研究では通常の PC（CPU:Pentium4 3.0GHz）において 10ms 程度で動作する実装を完成させた。さらにペアリングの積であるマルチペアリング演算についても高速化を達成した。これらの技術を組み込むことにより、失効数に依存することなく、ノート PC（CPU:PentiumM 1.7GHz）なら 200ms 程度、スマートフォン(Wilcom, CPU: Marvell PXA270 520MHz)でも 1 秒未満で署名生成可能となる失効手法を確立した。

(2) グループ電子署名における署名者特定者指定技術の研究開発

① グループ電子署名における署名者特定者指定技術の確立

署名者特定者を柔軟に指定することができる署名者特定者指定型グループ電子署名技術を開発し、複数組織に渡る来歴情報の、適切な情報開示を可能にする技術を開発した。特に、複数の署名者特定者を指定可能な方式は、指定した署名者特定者の数 n に対して、署名生成にかかる時間および署名データ長が n 倍未満となった。具体的には、提案方式において署名者特定者を 10 人指定するとき、署名生成に 0.061 秒かかり、署名データ長は 9500 ビットとなり、単純に署名を 10 個作成する場合（署名生成に 0.25 秒、署名データ長 66200 ビット）と比較して、非常に効率的な方式であることが確認できた。

(3) グループ電子署名における鍵管理技術の研究開発

① 署名案件ごとに、どの秘密鍵ならびにパラメータを利用するかの選択が、署名者にとって簡便におこなえる鍵管理技術の確立

現在一般的に使用されている鍵管理技術、ID 管理技術の調査を行い、グループ電子署名特有の鍵管理機能を提供できることを確認した。具体的には、Windows CardSpace および Higgins の調査を行い、グループ電子署名の処理フローに、既存 ID 管理技術を組み込むことが可能であることを確認した。これにより、複数グループに所属する署名者が容易にグループ電子署名の鍵を管理、利用できることが分かった。

３．３　テンプレート保護型生体認証技術

３．３．１　セキュアテンプレート生成・照合技術の研究開発

変換テンプレートによる生体認証技術は、国際的にみても研究段階であり、最良の手法は確立されていない。本研究開発では、下記の基本方針にしたがって、セキュアテンプレート生成・照合技術の研究開発を実施する。

①実用化されている生体認証と同程度の認証時間（1 秒未満)、本人拒否率（数%未満)、他人受入率（10000 分の 1 未満）を維持すること。②単純攻撃により変換テンプレートから元のテンプレートを再構成する可能性が、現状の共通鍵暗号と同等（2 の 256 乗分の 1 未満）となること。③漏洩した変換テンプレートを入力データとして再利用する（リプライアタック）攻撃に対して、通信路の保護がなされていない環境においても耐性を有すること。

(1) 技術および標準化動向の調査

テンプレート保護型生体認証技術については、学会や標準化団体へ様々な提案がされており、本研究開発の意義を明確にするために、国内・国際学会の技術動向の調査や、ITU-T SG 17、および、ISO/IEC JTC 1/SC 27 などの国際標準化の動向調査をおこなった。具体的には、第一年目に、欧州 TURBINE プロジェクトの動向を調査し、ITU-T SG 17 、および、ISO/IEC JTC 1/SC 27/WG 5 で行われている関連する標準化動向を調査した。テンプレート保護型生体認証に関するプロジェクトの動向を得た。さらに、第三年目まで継続し、ICB2009、Biometric Consortium Conference 2009、BTAS2009、CSS2009、Biometrics 2009、WIFS2009、SCIS2010 に出張し、欧米の動向を調査し、ITU-T SG17　課題 9 テレバイオメトリクス、および、ISO/IEC JTC 1/SC 27/WG5 の Biometric Template Protection プロジェクトの動向を調査し、本研究開発の分野が活発に議論されており、本研究の位置づけを明確にし、また、ICB2009、BTAS2009 に本委託研究の成果の一部を発表し、本委託研究で進めているセキュアテンプレート生成･照合技術の有効性をアピールした。これらにより、目標を達成した。

(2) セキュアテンプレート生成・照合技術の確立

① セキュアテンプレート生成・照合技術の確立

利用者を登録する組織と認証する組織が異なる場合でも、システムに登録された利用者のテンプレートが安全に利用されることを保証するため、テンプレートを変換したまま照合を行う生体認証技術の研究開発を実施した。具体的には、第一年目に「メディアシームレス対応来歴管理技術の研究開発 組織シームレス認証技術の研究開発」にて開発した登録･認証方式･フォーマット･プロトコルを元に、第二年目に、認証時のクライアントからの生体情報漏えい防止を目的としたモデル検討の結果、セキュアテンプレートへの認証端末内変換モデルおよびセンサ内変換モデルを挙げ、リスク・コストの観点から比較を行い、変換処理をセンサに実装可能か検証するため、

画像制御を応用先とするマイコンの評価ボードに実装し、第三年目に、実際の指静脈センサと連携し動作するプロトタイプシステムを実現するための要件抽出を行い、指静脈センサを搭載した評価ボードを開発し、さらにセンサ制御ミドルウェアや GUI アプリケーションを評価ボード上で開発し、目標を達成した。

② セキュアテンプレート生成・照合スキームの確立

第一年目に「メディアシームレス対応来歴管理技術の研究開発 組織シームレス認証技術の研究開発」にて開発した利用者認証アーキテクチャに基づき、来歴管理基盤上のセキュアテンプレート生成・照合スキームを開発し、具体的には、第二年目に、非対称キャンセラブル指静脈認証の来歴管理基盤向けプロトタイプシステムの設計を行い、第一年目に開発したキャンセラブル指静脈認証アルゴリズムを非対称化するため、パラメータのゼロ知識証明アルゴリズムを開発し、非対称キャンセラブル指静脈認証プロトタイプシステムを開発し、第三年目に、一時的なテンプレートを用いることにより、複数の組織で互いに自身のテンプレートを秘匿しながら、同一特徴量に基づくが異なるパラメータで変換されたテンプレートを共有するプロトコルを確立し、本プロトコルを実装したプロトタイプシステムを設計・開発し、目標を達成した。

(3) セキュアテンプレート生成・照合技術の評価

① セキュアテンプレート生成・照合技術の安全性評価

生体情報を複数の組織で利用する場合、生体情報の漏えいに関する安全性が課題となる。そこで、同技術の安全性を評価するための指針・方式について検討する必要がある。具体的には、第二年目に利用者認証方式の安全性に関する評価方法に基づき、テンプレート保護型生体認証の安全性評価フレームワークに関する検討を行い、テンプレート保護型生体認証の安全性評価モデルを設計し、さらに代表的なテンプレート保護型生体認証の一つであるバイオメトリック暗号プログラムを試作した。

第三年目には、安全性評価フレームワークによる評価例として、前年度作成した指紋を用いたバイオメトリック暗号による評価を実施し、安全性評価手法の実現性を確認した。さらに、これらの知見をまとめ、ITU-T SG17 課題 9 に寄書提案を行った。なお、寄書提案は新規勧告案 X.gep: “A guideline for evaluating telebiometric template protection techniques” として採択された。また、実証実験におけるアンケート調査でも、本研究開発の成果であるテンプレート保護型生体認証技術の安全性評価手法に関しては、概ね肯定的な評価を得ることができ、これらにより、本研究の目標を達成した。

② セキュアテンプレート生成・照合技術の実用性評価

セキュアテンプレート生成・照合技術は、コンセプトが提案されてから数年しか経過されておらず、本技術の実用性を明確に評価する必要がある。具体的には(2)①について、第二年目に、マイコン評価ボードへ実装したキャンセラブル指静脈認証の変換処理の性能評価により、処理時間、メモリ使用量、テンプレートサイズともに実用的なレベルであること、上記変換処理の安全性評価においては、初年度に開発したアルゴリズムから変更はなく、安全性は保たれていること、認証精度は保たれていることを確認し、第三年目に、開発した専用評価ボードおよび認証ホスト(PC)上に実装したキャンセラブル指静脈認証の性能評価により、処理時間、メモリ使用量、テンプレートサイズともにプロトタイプシステムとして実用的なレベルであることを確認した。さらに(2)②について、第二年目に、来歴管理基盤向け非対称キャンセラブル指静脈認証プロトタイプシステムの性能評価により、処理時間、テンプレートサイズともに、実用的なレベルにあることを確

認し、第三年目に、来歴管理基盤向けに開発したテンプレート移行システムのプロトタイプの性能評価により、処理時間、テンプレートサイズともに、実用的なレベルにあることを確認した。また、実証実験におけるアンケート調査でも、本研究開発の成果であるテンプレート保護型生体認証技術に関しては、概ね肯定的な評価を得ることができ、これらにより、本研究の目標を達成した。

３．４　その他の研究実績

(1) 他プロジェクトのとの連携

総務省委託研究「ネットワークを通じた情報漏出の検知及び漏出情報の自動流通防止のための研究開発」と連携し検討を行った。

具体的には、上記プロジェクトが、自動転送型ファイル共有ソフトのネットワークを介した情報漏えいの未然の防止や、既に自動転送型ファイル共有ソフトのネットワークに流通してしまった漏えい情報の流通抑止を実現するものであることから、本来歴管理システムによって管理されている電子ファイルが故意もしくは過失により来歴管理システムの対象組織外へと漏えいし、そこからさらに自動転送型ファイル共有ソフトのネットワークへと流出してしまっている状況を想定し、それぞれのプロジェクトで開発した技術が連携し有効に機能することを確認した。

(2) 標準化活動

・テンプレート保護型生体認証技術の安全性評価について、ITU-T SG 17（2 月会合、および 9 月会合）に提案し、X.gep：A guideline or evaluating telebiometric template protection techniques として、標準化項目として採択された（2009 年 9 月）。

・グループ電子署名技術を用いた匿名認証フレームワークについて、ISO/IEC JTC1 SC27 WG5 に提案し、Requirements on partially anonymous unlinkable authentication として、標準化プロジェクトとして採択された（2009 年 5 月）。その後、本プロジェクトのエディタとして、WD1, WD2 を提出した。

・グループ電子署名技術をはじめとする匿名性をサポートするメカニズムについて、ISO/IEC JTC1 SC27 WG2 に新規プロジェクト提案を支援し、匿名エンティティ認証メカニズムと匿名デジタル署名として、標準化プロジェクトが成立した（2010 年 3 月）

(3) 実証実験の実施

これまでの研究成果が単独の研究技術として有効であることはもちろんのこと、これら開発技術を統合したシステムとして有効であるかを検証するため、実証実験を行った。

具体的には、来歴管理技術の評価モデルを大規模化、詳細化することにより、実際の運用場面に適した評価モデルを設計した上で、有識者を含め評価を行った。この結果、情報漏えいの抑止に有効な高度な来歴管理機能を有した基盤技術の確立を確認した。

４　研究成果の更なる展開に向けて

(1) 標準化活動

ITU-T、ISO 等の国際標準化機関において、引き続き標準化活動を行い、本技術の普及展開を図る。具体的には、下記を予定。

・テンプレート保護型生体認証技術の評価方法について、ITU-T SG 17 課題 9 の X.gep： A

guideline for evaluating telebiometric template protection techniques の勧告化プロジェクトのエディタとして、2012 年の勧告化に向けて活動する。

・グループ電子署名技術を用いた匿名認証フレームワークについて、ISO/IEC JTC1 SC27 WG5 の Requirements on partially anonymous unlinkable authentication プロジェクトのエディタとして、標準化文書の成立に向けて活動する。

・ISO/IEC JTC1 SC27 WG2 において、グループ電子署名技術をはじめとする匿名デジタル署名のメカニズムを扱うプロジェクト 20008-2 において、エディタとして、標準化文書の成立に向けて活動する。

(2) 本研究開発における成果の事業化

本研究開発の成果は、情報の無断持ち出しや不正流用などに起因する情報漏えいを抑止・防止し、被害を防止するための基盤技術として有効な技術である。この成果を、受託者他のセキュリティソリューション・製品に適用することで、上記標準化活動とあわせ本研究開発の成果展開・普及を図る。

５　査読付き誌上発表リスト

[1] アマンスダルソノ、中西透、野上保之、舩曳信生、”Anonymous IEEE802.1X Authentication System Using Group Signatures”、Journal of Information Processing、Vol.18 pp. 63-76 (2010 年 3 月 10 日)

[2] 大木哲史、披田野清良、小松尚久、笠原正雄、“Fuzzy Fingerprint Vault Scheme によるバイオメトリック暗号のロック情報作成手法”、情報処理学会論文誌、vol.50 no.9 pp.2077-2087（2009 年 9 月 15 日）

６　その他の誌上発表リスト

[1] 洲崎誠一、福沢寧子、藤井康広、仲小路博史、“社会イノベーションを支える先進セキュリティ技術”、日立評論 Vol.91 No.12 pp60-65（2009 年 12 月 1 日）

[2] 森岡澄夫、“動作合成で開けつつある新しい回路設計の世界”、CQ 出版社、Design Wave Magazine (2009 年 2 月 10 日)

７　口頭発表リスト

[1] 藤井康広、海老澤竜、本多義則、洲崎誠一、“マルチベンダ紙文書漏えい対策システムの一提案”、第 42 回　CSEC 研究発表会（福岡）（2008 年 7 月 24 日）

[2] 藤井康広、海老澤竜、冨樫由美子、山田隆亮、本多義則、洲崎誠一、“Third-party Approach to controlling Digital Copiers”、The 10th International Conference on Information Integration and Web Based Applications & Services (iiWAS2008)（Linz）（2008 年 11 月 25 日）

[3] 藤井康広、海老澤竜、甲斐賢、山田隆亮、本多義則、“High-Accuracy Text Search of Hardcopy Logs”、The 11th International Conference on Information Integration and Web Based Applications & Services (iiWAS2009)（Kuala Lumpur）（2009 年 12 月 16 日）

[4] 宮崎邦彦、“墨塗り署名技術の来歴管理技術への適用”、安心・安全インターネット推進協議会（東京）（2008 年 4 月 11 日）

[5] 藤井康広、“情報漏えい対策技術と来歴管理技術”、安心・安全インターネット推進協議会（東京）（2008 年 9 月 5 日）

[6] 森田光、“「情報の来歴管理」平成 21 年度　実証実験について”、安心・安全インターネット推進協議会（東京）（2009 年 7 月 31 日）

[7] 藤井康広、“メディアシームレス来歴管理３年間の研究成果と実証実験案”、安心・安全インターネット推進協議会（東京）（2009 年 9 月 4 日）

[8] 藤井康広、西村知也、尾花賢、中西透、大木哲史、比良田真史、情報の来歴管理等の高度化・容易化に関する研究開発　実証実験結果報告”、安心・安全インターネット推進協議会（東京）（2010 年 2 月 26 日）

[9] 洲崎誠一、“セキュリティ技術最前線”、日立製作所 uValue コンベンション（東京）（2008 年 7 月 17 日）

[10] 洲崎誠一、“セキュリティ技術最前線 2009”、日立製作所 uValue コンベンション（東京）（2009 年 7 月 22 日）

[11] 藤井康広、冨樫由美子、“来歴管理システム”、日立製作所 2008 年度春 TC 展示会（東京）（2008 年 6 月 6 日）

[12] 藤井康広、芹田進、“機密文書廃棄管理システム”、日立製作所テクノロジーコミュニティ 2009 秋（東

京）（2009 年 11 月 5 日）
[13] 披田野清良、大木哲史、小松尚久、笠原正雄、“Fuzzy Vault Scheme を用いた Biometric Encryption の安全性評価に関する一考察”、 第 13 回バイオメトリックシステムセキュリティ研究会、（東京）（2008 年 6 月 25 日）
[14] 大木 哲史、磯部 義明、小松 尚久、“テンプレート保護型生体認証の標準化動向と評価方法ガイドラインーITU-T SG17 課題 9：テレバイオメトリクスを取り巻く状況ー”、第 19 回バイオメトリックシステムセキュリティ研究会、2009 年 12 月
[15] 大木哲史、“テンプレート保護型生体認証の評価方法に関する標準化”、安心・安全インターネット推進協議会第 19 回 アプリケーション技術 WG（2009 年 12 月 14 日）
[16] 西村知也、島津秀雄、アヌラグ・グプタ“権限委譲型のコンテンツセキュリティ”情報処理学会第 70 回全国大会（筑波大学)(2008 年 3 月 13 日）
[17] 西村知也、島津秀雄“異なる組織間でのセキュア文書流通アーキテクチャ”情報処理学会第 71 回全国大会（立命館大学)(2009 年 3 月 10 日）
[18] 西村知也、島津秀雄“電子文書の保護流通と来歴の管理”情報処理学会第 72 回全国大会（東京大学)(2010 年 3 月 9 日）
[19] 高橋健太、“キャンセラブルバイオメトリクスの現状”、第 13 回バイオメトリクス研究会、2008 年 6 月 25 日
[20] 比良田真史､高橋健太､磯部義明､“キャンセラブル生体認証の変換処理を搭載したセンサの基礎開発”、SCIS 2009 (2009 年　暗号と情報セキュリティシンポジウム)、大津、2009 年 1 月 21 日
[21] 比良田真史、高橋健太、“Cancelable Biometrics with Perfect Secrecy for Correlation-based Matching”、ICB2009（The 3rd IAPR Int. Conference on Biometrics）、Alghero、2009 年 6 月 5 日
[22] 高橋健太、比良田真史、“Generating Provably Secure Cancelable Fingerprint Templates Based on Correlation-invariant Random Filtering”、BTAS 2009 (IEEE Third International Conference on Biometrics: Theory、 Applications and Systems)、Washington DC、2009 年 9 月 30 日
[23] 比良田真史、“テンプレート保護型生体認証技術の開発”、安心・安全インターネット推進協議会 第 19 回　アプリケーション技術 WG、2009 年 12 月 14 日
[24] 平雄太、加藤英洋、中西透、野上保之、舩曳信生、森川良孝、“署名者の負担を軽減した失効方式をもつペアリングを用いたグループ署名方式の実装”、 電子情報通信学会 ISEC 研究会（東京）(2007 年 9 月 7 日）
[25] 上村香菜子、舩曳信生、中西透、ターメルファラグ、”無線メッシュネットワークでの最大遅延の最小化を目的とした経路木生成アルゴリズムの提案”、 電子情報通信学会 NS 研究会（東京）(2007 年 10 月 19 日）
[26] 赤根正剛、加藤英洋、沖本卓求弥、野上保之、森川良孝、”Ate ペアリングに適した Barreto-Naehrig 曲線のパラメータ設定”、 コンピュータセキュリティシンポジウム 2007（CSS2007）（奈良）(2007 年 11 月 2 日）
[27] 赤根正剛、加藤英洋、沖本卓求弥、野上保之、森川良孝、” Barreto-Naehrig 曲線を用いた Ate ペアリングにおける Miller アルゴリズムの改良”、 コンピュータセキュリティシンポジウム 2007（CSS2007）（奈良）(2007 年 11 月 2 日）
[28] 舩曳信生、中西透、ワラアハサン、上村香菜子、”A Channel Configuration Problem for Access-Point

Communications in Wireless Mesh Networks”、 2007 International Conference on Networks (ICON2007) (Adelaide, Australia) (2007 年 11 月 19-21 日)
[29] 加藤英洋、赤根正剛、沖本卓求弥、野上保之、森川良孝、”ペアリングに適した拡大体の高速実装”、第 30 回情報理論とその応用学会(SITA2007)、(志摩) (2007 年 11 月 29 日)
[30] 三木康平、中西透、川島潤、舩曳信生、”モバイルホストの負荷を軽減した失効機能をもつ匿名 IEEE802.1X 認証の実装”、情報処理学会 CSEC 研究会（東京）(2007 年 12 月 14 日)
[31] ターメルファラグ、舩曳信生、中西透、 “A heuristic Algorithm for access point allocation in indoor environments for wireless mesh networks”、 電子情報通信学会 IN 研究会（広島) (2007 年 12 月 14 日)
[32] 加藤秀明、舩曳信生、 中西透、”無線メッシュネットワークでのコンテンションウインドウサイズ操作時のスループット測定結果”、 電子情報通信学会 NS 研究会（千葉) (2007 年 12 月 21 日)
[33] 赤根正剛、加藤英洋、沖本卓求弥、酒見由美、野上保之、森川良孝、”部分体計算を活用する高速な Ate ペアリングの提案”、 2008 年 暗号と情報セキュリティシンポジウム（SCIS2008）（宮崎）(2008 年 1 月 24 日)
[34] 沖本卓求弥、赤根正剛、古川潤、野上保之、佐古和恵、森川良孝、” 楕円曲線上の高速スカラー倍算を用いた効率的なグループ署名の高速実装” 、 2008 年 暗号と情報セキュリティシンポジウム（SCIS2008）（宮崎）(2008 年 1 月 24 日)
[35] 上村香菜子、舩曳信生、中西透、ターメルファラグ、”二階層無線メッシュネットワークへの経路木アルゴリズムの拡張”、 電子情報通信学会 NS 研究会（沖縄) (2008 年 3 月 7 日)
[36] 吉田知輝、加藤英洋、根角健太、野上保之、森川良孝、” ペアリング暗号に効果的な拡大体上べき乗算に関する一考察”、電子情報通信学会 ISEC 研究会（福岡) (2008 年 7 月 25 日)
[37] アマンスダルソノ、中西透、三木康平、舩曳信生、”An Implementation of Anonymous IEEE802.1X Authentication with User Revocation”, The 3rd Joint Workshop on Information Security (JWIS 2008) (Seoul, Korea) (2008 年 7 月 10 日)
[38] アマンスダルソノ、中西透、野上保之、舩曳信生、” An Implementation of Anonymous IEEE802.1X Authentication System for Wireless Networks”、The 10th Industrial Electronics Seminar 2008 (IES2008)、(Surabaya, Indonesia) (2008 年 10 月 30 日)
[39] 中西透、アマンスダルソノ、酒見由美、野上保之、舩曳信生、” A Group Signature Scheme with Efficient Verifier-Local Revocation Check”、 2009 年暗号と情報セキュリティシンポジム(SCIS2009) (大津) (2009 年 1 月 21 日)
[40] 酒見由美、竹内翔一、野上保之、森川良孝、”Multi Pairing on Cross Twisted Xate Pairing”、 2009 年暗号と情報セキュリティシンポジム(SCIS2009) (大津) (2009 年 1 月 22 日)
[41] 加藤英洋、根角健太、柳枝里佳、野上保之、森川良孝、” ペアリング計算での利用を考慮した拡大体上 2 乗算の改良”、 2009 年暗号と情報セキュリティシンポジム(SCIS2009) (大津) (2009 年 1 月 22 日)
[42] アマンスダルソノ、中西透、酒見由美、野上保之、舩曳信生、”An Implementation of a Group Signature Scheme with Efficient Verifier-Local Revocation Check”、(東京) (2009 年 5 月 22 日)
[43] 一色寿幸、森健吾、尾花賢、佐古和恵、“グループ署名のスマートフォンへの実装”、2008 年暗号と情報セキュリティシンポジウム（宮崎）(2008 年 1 月 24 日)
[44] 荒木俊則、一色寿幸、森岡澄夫、尾花賢、佐古和恵、寺西勇、“グループ署名の FPGA 実装”、2008 年暗号と情報セキュリティシンポジウム（宮崎）(2008 年 1 月 24 日)

[45] 森岡澄夫、“Architecture Optimization of a Group Signature Circuit”、電子情報通信学会コンピュータセキュリティ研究会（CSEC）（福岡）（2008 年 7 月 25 日）

[46] 荒木俊則、尾花賢、佐古和恵、寺西勇、森岡澄夫、“グループ署名のハードウェア実装に適したストレートライン抽出可能証明生成方法”、2009 年暗号と情報セキュリティシンポジウム（滋賀）（2009 年 1 月 20 日）

[47] 尾花賢、一色寿幸、佐古和恵、宮崎邦彦、藤井康広、本多義則、“プライバシを考慮した来歴管理を実現する墨塗りグループ署名”、2009 年暗号と情報セキュリティシンポジウム（滋賀）（2009 年 1 月 20 日）

[48] 森岡澄夫、荒木俊則、一色寿幸、尾花賢、佐古和恵、寺西勇、“ESL 設計法を活用したグループ署名アルゴリズムの ASIC 化”、2010 年暗号と情報セキュリティシンポジウム（香川）（2010 年 1 月 19 日）

[49] 一色寿幸、尾花賢、佐古和恵、“複数人のオープナーを指定可能なグループ署名方式”、2010 年暗号と情報セキュリティシンポジウム（香川）（2010 年 1 月 19 日）

[50] 森岡澄夫、荒木俊則、一色寿幸、尾花賢、佐古和恵、“二段階動作合成によるグループ署名 ASIC の実装と評価”、電子情報通信学会 VLSI 研究会（沖縄）（2010 年 3 月 12 日）

[51] 柏木希美、披田野清良、大木哲史、小松尚久、“Biometric Encryption を用いた話者照合用のテンプレート作成手法に関する一考察”、コンピュータセキュリティシンポジウム 2008(CSS2008)、(沖縄) (2008 年 10 月 10 日)

[52] 小松尚久、“Some Comments on Biometric Authentication and Introduction of Research Activities”、 BERC (Biometric Engineering Research Center 招待講演)、(Korea)（2008 年 6 月）

[53] 披田野清良、大木哲史、小松尚久、笠原正雄、“On Biometric Encryption using Fingerprint and it's Security Evaluation ”、 International Conference on Control, Automation, Robotics and Vision(ICARCV2008)、（ベトナム）（2008 年 12 月 18 日）

[54] 森岡澄夫、“サブシステム・クラスの IP コアを開発するための設計・検証戦略”、設計品質＆検証技法ワークショップ 2008 テクノロジーセミナー（東京）（2008 年 9 月 19 日）

[55] 尾花賢、“グループ電子署名 3 年間の研究成果と実証実験案”、安心・安全インターネット推進協議会アプリケーション技術 WG（東京）（2009 年 10 月 2 日）

[56] 谷幹也、“複数の組織間で共有する情報漏えい対策技術”、安心・安全インターネット推進協議会アプリケーションサービス部会活動報告（東京）（2010 年 1 月 29 日）

[57] 高山伸也、大木哲史、山崎恭、小松尚久、笠原正雄、“バイオメトリック暗号を用いた CELP 話者照合のテンプレート安全性対策”、電子情報通信学会　オフィスインフォメーションシステム研究会（神戸）（2007 年 11 月 21 日）

[58] 秋元良次、大木哲史、小松尚久、“Fuzzy Vault Scheme を用いた顔認証システムのテンプレート保護に関する一考察”、暗号と情報セキュリティシンポジウム(SCIS2008)（2008 年 1 月 23 日）

[59] 宿沢晃平、大木哲史、山崎恭、小松尚久、“共通テンプレートを用いたバイオメトリック暗号の構成に関する一検討”、バイオメトリックシステムセキュリティ研究会（長野）（2009 年 12 月 4 日）

8　出願特許リスト

[1] 藤井康広、海老澤竜、田川豊、森田光、楠拓也、“印刷物管理システムおよび方法”、日本、2008 年 1 月 7 日

[2] 藤井康広、海老澤竜、田川豊、森田光、楠拓也、“Print management system and method”、米国、2008

年 11 月 28 日
[3] 藤井康広、冨樫由美子、本多義則、森田光、“来歴管理システム、来歴管理サーバ及びその管理方法”、日本、2009 年 1 月 8 日
[4] 藤井康広、芹田進、本多義則、森田光、“紙文書来歴管理システム”、日本、2009 年 5 月 21 日
[5] 島津秀雄、“ファイル管理装置、ファイル管理システム、及びそのプログラム”、日本、2007 年 8 月 1 日
[6] 西村知也、“電子ファイルアクセス権管理装置、電子ファイルアクセス権管理方法およびプログラム”、日本、2008 年 8 月 19 日
[7] 島津秀雄、“電子ファイルアクセス権管理装置、電子ファイルアクセス権管理方法およびプログラム”、日本、2008 年 8 月 13 日
[8] 西村知也、“アクセス権管理システム、ファイル管理サーバ、クライアントマシン、アクセス権管理方法およびプログラム”、日本、2010 年 1 月 08 日
[9] 西村知也、“ファイル管理システム、ファイル管理装置、ファイル管理方法およびファイル管理プログラム”、日本、2010 年 2 月 19 日
[10] 一色寿幸、“署名生成装置、署名人特定装置、グループ署名システム、およびそれらの方法とプログラム”、日本、2009 年 7 月 16 日
[11] 森岡澄夫、荒木俊則、“署名生成装置、ならびに、署名検証装置”、日本、2008 年 7 月 2 日
[12] 寺西勇、“ゼロ知識証明システム、ゼロ知識証明装置、ゼロ知識検証装置、ゼロ知識証明方法およびそのプログラム”、日本、2008 年 12 月 11 日

9　取得特許リスト

該当なし

１０　国際標準提案リスト

[1] ITU-T Study Group 17 Working Party 2 Question 9 (Telebiometrics)、C28、“Proposal of the New Discussion item for Telebiometrics - Evaluation framework for techniques of biometric template”、February 2009
[2] ITU-T Study Group 17 Working Party 2 Question 9 (Telebiometrics)、C158、“Revision proposals and comments for TD178: A guideline for evaluating biometric protection techniques”、September 2009
[3] ITU-T Study Group 17 Working Party 2 Question 9 (Telebiometrics)、TD603、“X.gep: A guideline for evaluating telebiometric template protection techniques”、September 2009
[4] ISO/IEC JTC SC27 WG5、提案番号 29191、“Requirements on partially anonymous unlinkable authentication”、提案年月日 2008 年 10 月 8 日(N7106)、修正提案年月日 2009 年 5 月 6 日(preliminary WD1)、2009 年 7 月 15 日(WD1(N7745))、2010 年 1 月 15 日(WD2(N8277))
[5] ISO/IEC JTC SC27 WG2、提案番号 20008, 20009、“Mechanisms supporting anonymity”、提案年月日 2009 年 3 月 3 日(Response to N7680)
[6] ITU-T Study Group 17 Working Party 2 Question 8 (Telebiometrics)、C215、“Proposal of the Draft Question text for next study period”、September 2007

１１　参加国際標準会議リスト

[1] ITU-T Study Group 17 Meeting、Geneva、2007/09/19-28

[2] ITU-T Study Group 17 Meeting、Geneva、2008/04/07-18

[3] ITU-T Study Group 17 Meeting、Geneva、2008/09/15-19

[4] ITU-T Study Group 17 Meeting、Geneva、2009/02/11-20

[5] ITU-T Study Group 17 Meeting、Geneva、2009/09/16-25

[6] ISO/IEC JTC SC27 WG2, WG5、キプロス、2008 年 10 月 6 日～10 日

[7]]ISO/IEC JTC SC27 WG2, WG5、北京、2009 年 5 月 4 日～8 日（電話会議）

[8] ISO/IEC JTC SC27 WG2, WG5、レッドモンド、2009 年 11 月 2 日～6 日

１２　受賞リスト

該当なし

１３　報道発表リスト

（１）報道発表実績

[1] “「指静脈マネー」によるクレジット決済の実証実験を実施”、日立製作所 HP にてリリース、2007 年 7 月 23 日

[2] “複数の組織間で共有する情報の漏えい対策技術を開発 電子ファイルや印刷物などの漏えい経路を追跡可能に”、５社（早稲田大学、岡山大学、日立製作所、日本電気、NEC システムテクノロジー）の HP にて共同リリース、 2009 年 11 月 30 日

（２）報道掲載実績

[1] “「指静脈マネー」によるクレジット決済の実証実験を実施 9 月から 3 ヶ月間、日立システムプラザ新川崎の食堂・売店で実施”、livedoor ニュース、2007 年 7 月 23 日

[2] “指 1 本で買い物ができる「指静脈マネー」を日立が開発”、AFPBB News、2007 年 7 月 24 日

[3] “日立、社員食堂にカードも不要の指静脈認証システムを導入！実機を展示デモ”、RBB TODAY、2007 年 7 月 25 日

[4] “社員食堂に「指静脈マネー」，日立が実証実験”、日経 BP Tech-On!、2007 年 10 月 5 日

[5] “「指静脈マネー」ってなんだ？！”、J-Net21、2008 年 11 月 19 日

[6] “情報漏洩元追ソフト”、TV 東京ワールドビジネスサテライト、2009 年 11 月 30 日

[7] “データ流出元特定　早大など 5 者システム開発”、毎日新聞、2009 年 12 月 1 日

[8] “企業間共有情報漏洩経路を追跡　早大など機器に専用ソフト”、日経産業新聞、2009 年 12 月 1 日

[9] “企業間情報漏えい元特定　早大･日立などシステム共同開発”、日刊工業新聞、2009 年 12 月 1 日

[10] “来歴管理技術を共同開発　日立など情報漏えい対策”、電波新聞、2009 年 12 月 1 日

[11] “NEC、日立など、複数の組織間で共有する情報の漏えい対策技術を共同開発”、CNET Japan、2009 年 12 月 1 日

[12] “複数組織で共有する情報の漏洩を防ぐ技術を日立、早大らが実証実験開始”、マイコミジャーナル、2009 年 12 月 1 日

[13] “情報漏えい元が一目で分かる追跡システム、早大や日立などが開発”、ITPro、2009 年 12 月 1 日

[14]“紙媒体経由の情報流出も追跡「禁止ではなく抑止」、早稲田大らが来歴管理技術を共同開発”、atmarkIT、

2009 年 12 月 1 日
[15]“早大や日立ら、複数組織間での情報流通を可視化・追跡する技術を開発～漏洩経路を特定”、RBBToday、2009 年 12 月 1 日
[16]“早稲田大学など、複数組織で共有する情報の漏えい対策技術を開発”、Enterprise Watch、2009 年 12 月 1 日
[17]“犯人は誰？ 複数企業で共有する情報の流出経路を追跡する技術”、日経パソコン、2009 年 12 月 1 日
[18]“早大、日立、ＮＥＣなどで複数組織共有情報の漏洩を防ぐ技術開発”、知財情報局、2009 年 12 月 1 日
[19]“組織を跨いだ情報漏えいの経路を追跡する技術、早大らが実証へ”、ITMedia、2009 年 12 月 1 日
[20]“犯人は誰？ 複数企業で共有する情報の流出経路を追跡する技術”、ITPro、2009 年 12 月 1 日
[21]“技術ウオッチ　電子文書の伝達、安全確実に　日立、漏洩元の追跡ソフト”、日本経済新聞、2010 年 2 月 20 日
[22]“情報漏洩元追跡ソフト”、小学館 DIME、2010 年 3 月 16 日

１４　ホームページによる情報提供

[1] “指だけの簡単・便利なクレジット決済「指静脈マネー」”

[URL] http://www.hitachi.co.jp/products/it/veinid/case_studies/yubijomyaku_money/index.html

[掲載情報の概要] 日立は 2007 年 9 月から 3 ヵ月間、株式会社ジェーシービー（以下 JCB）の協力のもと、情報・通信システム関連の事業所である「日立システムプラザ新川崎（神奈川県川崎市）」の社員食堂と売店において、指静脈マネーの実証実験を実施。

[2] “紙文書来歴管理システム iiWAS2009 にて発表”

[URL] http://www.hitachi.co.jp/rd/sdl/conf/2010/iiwas/index.html

[掲載情報の概要] 日立は 2009 年 12 月 14 日から 16 日までの 3 日間、マレーシアのクアラルンプールで、The 11th International Conference on Information Integration and Web-based Applications & Services（iiWAS2009）が開催（採録論文数は 102、採択率は 23%）され、紙文書来歴管理システムの成果について成果発表模様のレポート。

研究開発による成果数

	平成 19 年度	平成 20 年度	平成 21 年度
査読付き誌上発表数	0 件（ 0 件）	0 件（ 0 件）	2 件（ 0 件）
その他の誌上発表数	0 件（ 0 件）	1 件（ 0 件）	1 件（ 0 件）
口頭発表数	14 件（ 1 件）	19 件（ 5 件）	18 件（ 2 件）
特許出願数	2 件（ 0 件）	5 件（ 1 件）	4 件（ 0 件）
特許取得数	0 件（ 0 件）	0 件（ 0 件）	0 件（ 0 件）
国際標準提案数	0 件（ 1 件）	1 件（ 1 件）	0 件（ 3 件）
国際標準獲得数	0 件（ 0 件）	0 件（ 0 件）	0 件（ 0 件）
受賞数	0 件（ 0 件）	0 件（ 0 件）	0 件（ 0 件）
報道発表数	1 件（ 0 件）	0 件（ 0 件）	1 件（ 0 件）
報道掲載数	5 件（ 0 件）	0 件（ 0 件）	17 件（ 0 件）

	合計	（参考） 提案時目標数
査読付き誌上発表数	2 件（ 0 件）	－件（－件）
その他の誌上発表数	2 件（ 0 件）	－件（－件）
口頭発表数	51 件（ 8 件）	－件（－件）
特許出願数	11 件（ 1 件）	20 件（－件）
特許取得数	0 件（ 0 件）	2 件（－件）
国際標準提案数	1 件（ 5 件）	－件（－件）
国際標準獲得数	0 件（ 0 件）	－件（－件）
受賞数	0 件（ 0 件）	－件（－件）
報道発表数	2 件（ 0 件）	3 件（－件）
報道掲載数	22 件（ 0 件）	－件（－件）
論文掲載数	－	9 件（－件）
研究発表数	－	30 件（－件）

注１： （括弧）内は、海外分を再掲。

注２： 「査読付き誌上発表数」には、論文誌や学会誌等、査読のある出版物に掲載された論文等を計上する。学会の大会や研究会、国際会議等の講演資料集、アブストラクト集、ダイジェスト集等、口頭発表のための資料集に掲載された論文等は、下記「口頭発表数」に分類する。

注３： 「その他の誌上発表数」には、専門誌、業界誌、機関誌等、査読のない出版物に掲載された記事等を計上する。