＜基本計画書＞

情報の来歴管理等の高度化・容易化に関する研究開発

1. 目的

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。

2. 政策的位置付け

「ＩＴ新改革戦略」（平成１８年１月１９日　ＩＴ戦略本部決定）において、『２０１０年度までに、ユビキタス端末等における瞬時に安全かつ確実に認証を行う技術や相手に応じて適切な情報のみを提供可能とするプライバシー保護技術を実現する。』こと、及び『２００８年度までに、「ＩＴ利用に不安を感じる」とする個人を限りなくゼロにする。』ことが目標として掲げられている。また、「第１次情報セキュリティ基本計画」（平成１８年２月２日　情報セキュリティ政策会議決定）において、『急速に拡大するＩＴの利用・活用に対応し、次から次へと発生する新しい情報セキュリティの脅威に、対症療法的ではなく対応するためには、常に最先端の研究開発・技術開発の要素を取り入れた情報セキュリティ対策を推進していくことが必要である。』と提言されている。

また、「セキュア・ジャパン２００６」（平成１８年６月１５日　情報セキュリティ政策会議決定）において、『情報通信ネットワークの安定運用を継続的に確保するため、新たな情報セキュリティ脅威に対し、即時かつ的確な対応を図るための状況調査を実施するとともに、必要な研究開発・技術開発等を推進する。』と提言されている。さらに、「分野別推進戦略」（平成１８年３月２８日　総合科学技術会議）において、『セキュリティ領域の【課題１】情報セキュリティ技術の高度化、【課題２】技術を補完しより強固な基盤を作るための管理手法の研究が重要である。したがって、これら

の研究開発課題の中核部分を戦略重点科学技術として選定する。』と提言されている。

3. 目標

（１）政策目標

大規模な情報流出事件は、情報の無断持ち出しや不正流用といった、悪意の情報漏えい行為に起因しており、情報の適切な管理を高度化・容易化するための基盤技術の早期実現が求められている。そのため、本研究開発では、情報の流通経路を正確かつ容易に把握可能とする技術を確立し、悪意の情報漏えい行為を抑止するとともに、必要以上の情報開示を防止する技術により、開示情報の悪用を防止し、適切な情報流通を促進する。これらを実現することにより、前記分野別推進戦略が掲げる「ＩＴ利用に不安を感じる個人を限りなくゼロに近づけ、誰もが安心してインターネット上のサービスを利用できる環境を整備する」という目標の達成に大きく寄与し、組織における情報管理など様々な社会・経済活動の更なる活性化への貢献を行う。

また、来歴管理技術の相互接続性・運用性を確保するように、技術仕様の共通化・標準化を実現することを目指す。

（２）研究開発目標

情報の流通経路を把握可能とし、情報漏洩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。

4. 研究開発内容

（１）メディアシームレス対応来歴管理技術

① 概要

現在、情報の来歴を管理するためには、サイバー空間もしくは物理空間の何れかのみを流通する情報しか管理できなかったり、組織外に送信された情報を管理することが困難である等の技術面、運用面での制限がある。

このため、組織間を流通するコンテンツの来歴（誰が・いつ・どこで・どの情報に・何をした）をメディアフォーマット（電子／物理媒体）に応じて統一的に管理する技術の研究開発を実施する。

また、併せてこれらの技術については、標準獲得に向け、幅広い意見を集約する場を設け、議論のために技術を公開して早期に IETF 等へ標準化提案を行い、勧告化、規格化されることを目標とする。

② 技術課題

ア） 組織シームレス来歴管理技術

複合企業体の業務や、業務のアウトソーシング等で起こりうる他組織を経由した情報漏えいの検知を可能とするため、組織内の重要情報の来歴を管理するだけではなく、組織外に送信された重要情報の来歴管理を容易に実現する組織シームレス来歴管理技術の研究開発を実施する。

具体的には、組織ごとの来歴管理システムを連携させる来歴情報連携システムを構築することにより、組織を跨った来歴管理を可能とする基盤技術の研究開発を実施する。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追跡可能とするために、プライバシー保護に対応したシステム間のセキュアな通信プロトコル、各組織における来歴情報の管理方式、及び、組織間でシームレスに来歴情報を追跡可能とする来歴情報の連携方式を実現する「セキュア来歴管理技術」の研究開発を実施する。また、第三者に対して来歴情報の信頼性を証明可能とする「来歴情報信頼性保証技術」の研究開発を実施する。

イ） メディアシームレス来歴情報付与・検知技術

サイバー空間と物理空間を行き来するコンテンツを対象とした来歴管理を可能とするため、メディアフォーマットに依存せず来歴管理が可能となる技術の研究開発を実施する。

具体的には、サイバー空間と物理空間を複数回行き来するコンテンツの来歴を統一的に管理するため、特定のデータ形式やメディアフォ

ーマット（電子／物理媒体）に依らず、また、白黒二値や多値カラー表現などのデータの表現形式に依らずに識別 ID が付与・検知可能となる「メディアシームレス来歴情報付与・検知技術」の研究開発を実施し、管理対象となるメディアフォーマット（電子／物理媒体）に応じて、コンテンツ品質を維持しながら、識別 ID またはそれに付随する来歴をメディアの品質を維持しながらコンテンツに不可分な形で対応付けるメディア品質維持来歴情報付与技術、および、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付与した情報が一貫して正しく検出可能な高耐性・高精度来歴情報検出技術の研究開発を実施する。上記技術の研究開発にあたり、コンテンツのメディアフォーマットに応じて、来歴情報をコンテンツ自身に付与する多重来歴記録技術、およびユーザに意識させることなく自動的に来歴管理を行うため、識別 ID に基づいて、コンテンツの来歴（誰が・いつ・どこで・どの情報に・何をした）を自動記録する来歴管理サーバ連携技術の研究開発も併せて実施する。

③　到達目標

ア）　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、機密情報の漏洩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。

イ）　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。

（２）グループ電子署名技術

①　概要

情報の責任主体を明確にするため電子署名技術が用いられている。

現在の電子署名技術は、「誰が」その情報の責任主体かを明確に証明できる者であるが、組織内、組織間での情報の管理を行う場面で使用する際には、作成組織、部署など「どの組織」が作成したものかが証明できれば、「誰が」に該当する署名者の氏名等の個人情報は必ずしも必要ではなく、場合によっては不必要となる個人の情報を公開してしまうことにもつながる。

このため、コンテンツの作成者（署名者）個人の特定を防止し、署名元組織や所属のみを証明可能とすることで、必要以上の個人情報開示を防止するグループ電子署名技術を確立する。

②　技術課題

同一組織のメンバで公開鍵を共有することで、署名者が属する組織内部においては、署名者個人を検証可能とし、組織外部に対しては、署名者の組織や所属のみを証明可能とする電子署名技術の研究開発を

実施する。

現状の技術では、署名者の個人情報保護を運用だけで行う場合、オペレータの操作ミスやソフトウェアのバグ等により、個人情報を流出させる危険性がある。一方、個人情報保護を優先させた運用を行った場合、匿名性を利用した不正行為が可能となる、といった問題がある。

そこで、現状の署名技術におけるこれらの課題を技術的に解決するために、署名者の匿名性を保証し、かつ特定の管理者からは必要に応じて署名者を追跡可能とする、グループ電子署名技術の研究開発を実施する。具体的には、計算量的安全性を有し、かつリソース使用量が少ない等の実装性に優れているアルゴリズムを開発・実装することにより、匿名性、非改竄性、およびユーザの利便性を向上する技術の研究開発を実施する。また、鍵および証明書の失効方式の研究開発を実施し、組織のメンバの所属を無効にした際、メンバに意識させることなく、無効化されるメンバの鍵および証明書の失効処理技術の研究開発を実施する。更にメンバが複数の組織に所属する場合、署名者個人の検証を組織ごとに可能とするグループ電子署名方式の研究開発を実施する。

③　到達目標

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。

5. 実施期間

平成１９年度から平成２１年度までの　３年間

6. その他　特記事項

①　「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」との連携

本研究開発に関して、別途公募中である「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」と連携した研究開発が推進され、２つの研究開発が連携した統合的な実験・評価等によって実用的な成果を導出することが必要である。

そのため、提案者は、「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」との連携方針について、できるだけ具体的に提案書に記載すること。また、提案の採択後、上記方針に従い、総務省および「情報の来歴管理等の容易化・高度化に関する研究開発」の採択者と協議を行い、具体的な連携方法等を定めることとする。

②　「テンプレート保護型生体認証技術」に係る参考資料の提出

政府予算の状況等により、本研究計画の２年目以降、「テンプレート保護型生体認証技術」（別紙を参照）の研究開発を追加実施して頂く可能性がある。

そのため、提案者は、上記技術の研究開発が追加されることを考慮した全体計画、実施体制を検討するとともに、上記同技術の研究開発に係る参考資料を提出すること。総務省は、採択者の選定に際して参考資料の内容についても参照することとする。

なお、参考資料はあくまで採択者の選定を行う際の参考として提出して頂くものであり、上記技術の追加実施について何ら保証するものではないので留意すること。

③　その他

本研究開発を実施するにあたっては多彩なアイデアに基づく新技術の研究開発に積極的に取り組むこととし、提案に当たってもその内容を明記すること。また、本研究開発内容を、広く普及・啓発させるとともに技術仕様の標準化を推進するための体制整備方法についても提案書に記載すること。

別紙

「テンプレート保護型生体認証技術」に係る参考資料の提出について

（１）研究開発内容

①　概要

情報漏洩の抑止においては、情報の操作者を確実に特定・記録することが重要である。異なる組織間において情報操作者を確実に特定するためには、運用レベルに依存しない本人確認技術である、生体認証技術の適用が必要となる。

このため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、なりすましを防ぐのはもちろん、システムに登録された利用者の生体情報（テンプレート）が安全に利用されることが保証できるテンプレート保護型生体認証技術の研究開発を実施する。

②　技術課題

ア）　セキュアテンプレート生成・照合技術

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する。具体的には、通常のテンプレートから変換テンプレートを生成し、変換テンプレート同士を照合する、生成・照合技術の研究開発を実施する。

イ）　セキュアテンプレート配布・利用技術

ア）で生成された変換テンプレートを登録した組織外に配布する場合の再変換方式、再変換における安全性の検討、再変換時の利用者の認可方式を検討する。また、変換テンプレートを配布された組織における、利用者の認証方式、認証における安全性の検討、変換テンプレート漏洩時の対策方式の研究開発を実施する。

③　到達目標

ア）　セキュアテンプレート生成・照合技術

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。

イ） セキュアテンプレート配布・利用技術

変換テンプレートを安全に複数組織に配布・利用するための基本方式を検討し、再変換された変換テンプレートの配布・利用の安全性に関して、テンプレート漏洩リスクを定量化することで安全性を明確化し、さらに、漏洩時の対策により漏洩リスクを低減できることを定量的に示すことを目標とする。また、上記で検討した方式を元に、少なくとも三つ以上の異なる組織において、それぞれの組織で生成した変換テンプレートの登録と配布による相互利用を可能とする技術の研究開発を実施する。

（２）参考資料の作成要領

「平成１９年度　情報通信技術の研究開発に係る提案公募　提案書作成要領」（平成 19 年 2 月　総務省）に準じ、上記技術に係る以下の書類を作成の上、提案書とともに提出すること。

・ ［様式 2］研究開発内容説明書

・ ［様式 3a］研究開発実施計画書
・ ［様式 3b］研究開発実施計画書

・ ［様式 5a］実施体制説明書
・ ［様式 5b］実施体制説明書

（注）「２．経理責任者」については記載不要です。

（注）「３．研究開発体制図」には予定される研究リーダーまでを記載し、個々の研究者については記載不要です。

・ ［様式 6］研究者経歴説明書

（注）［様式 5a］又は［様式 5b］に記載された「研究代表者」および「研究リー

ダー」についてのみ提出して下さい。

なお、参考資料の作成に際しては、以下の点に留意すること。

① 基本計画書に掲げた「自動転送型ファイル共有ソフトトラヒック制御技術」および「流出情報の検知・削除技術」に係る研究開発との連携方法について具体的に記述すること。
② 資料右上に参考資料と明記すること。