SCIS 2021 2021 Symposium on Cryptography and Information Security
On-line, Jan. 19 — 22, 2021
The Institute of Electronics, Information and Communication Engineers

インターネット上のサービスにおける利用者の匿名性と特定・追跡性の両立
A method of achieving both anonymity and identifiability / trackability of users in services on the Internet

才所 敏明[*1] 辻井 重男[*2]
Toshiaki Saisho Shigeo Tsujii

あらまし インターネット社会の課題の一つに，利用者の高い匿名性がある．インターネット社会における確実な本人確認を目指し，筆者らはインターネット上の様々のサービスに対し確実な本人確認機能を提供する本人確認基盤 NAFJP を提案している．一方，インターネット社会では，利用者の匿名性も重要である．本稿では，提案している NAFJP の利用により，インターネット上の様々のサービスにおいて，利用者の匿名性を確保しつつ，同時に利用者の特定・追跡性を保証することが可能であることを示す．更に，筆者らが別途提案している確実な本人確認機能を内包する安心・安全な電子メール利用基盤 SSMAX に対し，確実な本人確認機能には NAFJP を利用することにより，個人情報である身元確認情報，当人確認情報等の管理が不要となる新たな SSMAX の構成案を示す．NAFJP の利用により，インターネット上の様々のサービスにおいて，利用者の個人情報の管理を回避しつつ，利用者の匿名性と特定・追跡性の両立が実現可能となる．

キーワード インターネット，匿名性，特定・追跡性，本人確認基盤，NAFJP，電子メール利用基盤，SSMAX

Abstract One of the issues in the Internet society is the high anonymity of users. Aiming for reliable authentication, the authors are proposing the National Authentication Framework in Japan NAFJP, which provides a reliable authentication for various services on the Internet. On the other hand, in the Internet society, the anonymity of users is also important. This paper shows that by using the proposed NAFJP, it is possible to ensure the anonymity of users and at the same time guarantee the identifiability and trackability of users in various services on the Internet. So far we have proposed “Secure and Safe eMAil eXchange framework SSMAX“ that have the reliable authentication function. In this paper, we propose new framework of SSMAX that utilize NAFJP for the reliable authentication and that is not need for managing user’s personal information.

Keywords Internet, anonymity, identifiability / trackability, national authentication framework, NAFJP, secure and safe e-mail exchange framework, SSMAX

1 インターネット社会の課題

インターネットの普及，応用の進展は目覚ましく，今や日常の生活活動，産業活動には欠かせないインフラとなっている．インターネットは人を動かし，社会を動かす時代となり，現在はインターネットに強く依存する社会，インターネット依存社会である．

*1 （株）IT 企画 http://advanced-it.co.jp/
mail : toshiaki.saisho@advanced-it.co.jp
*2 中央大学研究開発機構
mail: tsujii@tamacc.chuo-u.ac.jp

このように，社会を支える最重要インフラともいえるインターネットは，当初，利用者が他の利用者を攻撃するというようなことは想定されておらず，利用者の確実な本人確認や悪意のある利用者の特定・追跡性については考慮されていなかった．また，IPv4 から IPv6 への移行は経験したものの，セキュリティ機能はほとんど強化されていない．インターネットの普及，発展を支えたアプリケーション，電子メールやワールドワイドウエブ（WWW）もインターネットと同様の方針で利用者の確実な本人確認や悪意のある利用者の特定・追跡性につい

ては考慮されていなかった．このようなインターネットおよびインターネット上のアプリケーションにより形成されたインターネット社会では，匿名性が強いがゆえに，様々の不正・不法な利用，悪意のある利用への的確な対応が困難で，様々の技術・情報を駆使しての対応が実施されているが，不正・不法な利用，悪意のある利用の氾濫はますます増加する傾向にある．

インターネットの社会における位置づけ・役割はますます大きくなり，今後も社会はインターネット依存を強めることは必至である．インターネットの様々の不正・不法な利用，悪意のある利用を効果的に抑止できる基本的なセキュリティ機能の強化が，インターネットに依存する社会の安心・安全の維持・強化に不可欠であり，インターネット社会の健全な発展にも不可欠である．

筆者らはこのような認識の元，確実な本人確認がインターネット上の安心・安全なアプリケーションの必須要件であると認識し，インターネット上のアプリケーションが容易に確実な本人確認機能を組み込むことができるよう，日本の本人確認基盤 NAFJP（National Authentication Framework in Japan）の構築を提唱している．

本稿では，まず本人確認基盤 NAFJP の機能や構成を示し，更に NAFJP が利用者の特定・追跡性を保証する基盤となりうること，また利用者の一定レベルの匿名性の確保も実現可能であることを示す．

次に，筆者らが電子メール利用者の匿名性と特定・追跡性の両立を目指し提案している安心・安全な電子メール利用基盤 SSMAX の機能や構成を示し，更に SSMAX へ NAFJP を適用した SSMAX の新たな構成案を示し，NAFJP の利用により身元確認情報，当人確認情報等の個人情報の管理が不要にもかかわらず，確実な本人確認および特定・追跡性の両立ができる SSMAX の実現が可能なことを示す．

2　利用者の本人確認基盤 NAFJP

日本では，行政サービスのオンライン本人確認は住民基本台帳制度による身元確認をベースにマイナンバーカードによる当人確認へ集約される方向にある．しかし，民間サービスにおいては独立した本人確認サービスも一部では利用されてはいるが，それぞれのインターネット上のサービス事業者が個別に多様な本人確認方法を利用し本人確認を行っているのが実情である．このような個別サービスごとの本人確認の現状には多くの課題が存在する．

ア：利用者の課題

① サービス事業者ごとに，本人確認情報（個人情報・秘密情報等）を提供しなければならない，利用者の不安

② 多くの本人確認情報の安全・確実な管理のための，利用者の負担

③ サービス利用の都度，サービス事業者ごとに異なる本人確認情報の提示が求められる，利用者の利便性の悪さ

イ：事業者の課題

① 利用者の本人確認情報の安全・確実な運用・管理のための，事業者の負担

② インターネット上のサービスシステム開発時に求められる本人確認機能の個別実装のための，事業者の負担

ウ：社会の課題

① 本人確認関連技術の発展の成果である新たな本人確認手段の各サービス事業者での採用の遅れによる，社会におけるインターネット高度利用の遅れ

以上のような民間分野における個別のサービス事業者ごとの本人確認の課題を克服するために，本人確認機能をそれぞれのサービス事業者から切り離し，本人確認を専門事業者に委託する仕組み，日本の本人確認基盤 NAFJP の構築を提唱している．

2.1　インターネット上での本人確認

インターネット上のサービスシステムがサービス要求を受けた場合に，そのサービス要求者がサービスシステムに登録されている正規の利用者かどうかの判断（本人確認）が必要となる．正規の利用者であることが確認できれば，システムはその利用者の権限に応じた範囲での利用を認可する．本稿では，サービス要求者がシステムに登録されている登録仮想エンティティに紐づけられた当人確認情報に合致するかどうかを判定する機能を当人確認機能とする．また，登録仮想エンティティに対応する利用者の実名，住所等，実エンティティ（利用者）を特定できる情報の取得およびその情報の妥当性を検証する機能を身元確認機能とする．

本人確認機能は，身元確認機能および当人確認機能から構成され，身元確認の信頼レベルおよび当人確認の信頼レベルに応じ，本人確認の信頼レベルが決定される．

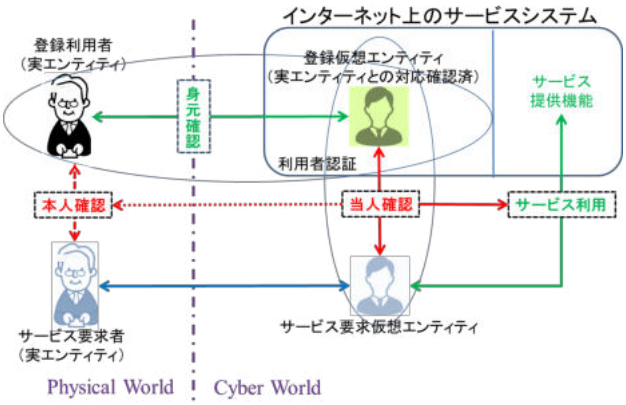

図１　本人確認基盤

2.2　日本の本人確認基盤 NAFJP の仕組み

インターネット経由の民間サービスでは，身元確認・当人確認は個別のサービス事業者が担当しているのが実情である．政府としては，民間分野においても，行政サービス部門と同様の仕組みによる本人確認が可能なように，J-LIS によるサービスの民間事業者への提供を進めているが，現実には活用は進んでいない．

そこで，身元確認には住民基本台帳制度/J-LIS のサービスを利用し，民間サービス向けの多様な当人確認を専門的に行う事業者を活用する，日本の民間サービス向け本人確認基盤（以降，特段の記載がない限り，単に NAFJP と略記）の構築を提案している．

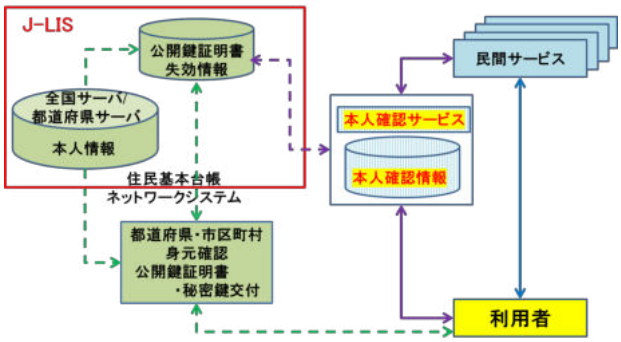

図 2　日本の民間サービス向け NAFJP（構想）

NAFJP における本人確認サービス事業者は，住民基本台帳制度/J-LIS サービスを利用しつつ利用者の身元確認を実施し，本人確認情報の登録を受け付ける本人確認情報登録事業者と，その本人確認情報（当人確認情報）を利用しインターネット経由の当人確認を実施する当人確認サービス事業者の二つの事業者グループから構成されるものとする．本人確認情報登録事業者および当人確認サービス事業者が採用する当人確認方式は，本人確認技術の開発・評価を行う専門機関の評価結果に基づき，安全な方式を採用するものとし，またそのような安全な当人確認方式を正しく実装し運用しているか，個人情報・プライバシー情報の管理等，適切なセキュリティ対策をとっているかどうかについて，本人確認サービス事業者認定機関による監査・認定を受ける仕組みにより，NAFJP における本人確認サービスの安全性・信頼性を担保する仕組みを想定している．

NAFJP の構成は，本人確認サービスと利用者，インターネット上の各サービスとの連携方法に応じ，二つの構成を想定している．それぞれの構成案を図 3～図 4 に示している．

図 3 に示す NAFJP/A は，利用者中継型であり，利用者側のシステムに負荷がかかるが，最もプライバシー保護に適した形態である．図 4 に示す NAFJP/B は，インターネット上のサービス事業者中継型であり，従来は事業者自身で行っていた本人確認をアウトソーシングする形態である．

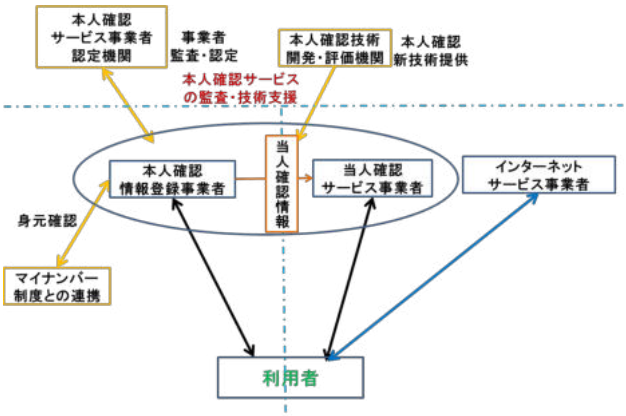

図 3　利用者中継型 NAFJP/A

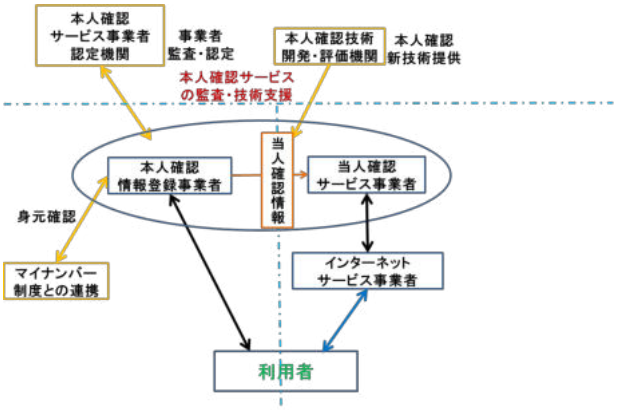

図 4　サービス事業者中継型 NAFJP/B

2.3　NAFJP における匿名性と特定・追跡性

インターネット上では，仮想エンティティが利用者の行為・発言を代行する．実際の利用者（実エンティティ）との対応が未確認の仮想エンティティの場合，その仮想エンティティの無責任な行為・発言の責任追及や抑止することが難しく，現在のインターネット上の不正・不法な行為・発言，誹謗・中傷やいじめに該当する行為・発言を誘発する大きな原因となっている．

NAFJP による本人確認と同時に，本人確認された仮想エンティティと実エンティティ（利用者）の対応を管理することにより，仮想エンティティの特定・追跡性を確保することが可能となる．

一方，仮想エンティティに紐づけられている実エンティティ（利用者）の情報を隠蔽することにより，利用者の一定レベルの匿名性を維持することが可能となる．

以上のように，本人確認基盤 NAFJP により，実エンティティ X（利用者）と仮想エンティティ A の対応付けの情報（連結情報）の秘匿と開示の制御により，利用者（実エンティティ X）の匿名性と特定・追跡性を両立させる仕組みが可能となる（図５）．

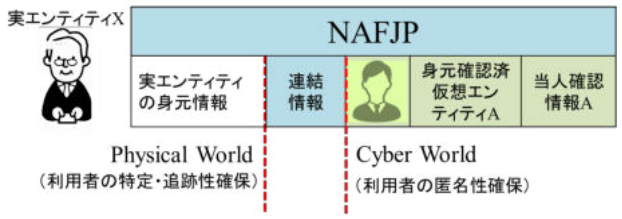

図５　NAFJP による匿名性と特定・追跡性の両立

インターネット上のサービスでは，このような NAFJP の仕組みを利用し本人確認の上，それぞれのサービス空間内で活動できる仮想エンティティを定義・登録し，利用者が当該サービス利用時には，NAFJP による本人確認結果をもとに，サービス提供の是非を判断することを想定している（図６）．

利用者（実エンティティ X）は，NAFJP を利用し本人確認の上，インターネット上のサービス S へ利用登録を行うと，NAFJP 登録エンティティ A と連結されたサービス S 空間での活動に必要な新たな仮想エンティティ A1 が定義される．

利用者（実エンティティ Y）がサービス S の利用を要求する場合，まずインターネット上の仮想エンティティ Y を通じ，NAFJP の仮想エンティティ A の当人確認情報 A を利用し当人確認を実施する．その当人確認に成功すると，仮想エンティティ Y は仮想エンティティ A と同一であり，実エンティティ Y も実エンティティ X と同一であること，実エンティティ Y が実エンティティ X 本人であることが確認される．このような本人確認の結果をサービス S が確認できれば，サービス S は仮想エンティティ Y に対し仮想エンティティ A1 としてのサービスを提供することを想定している．

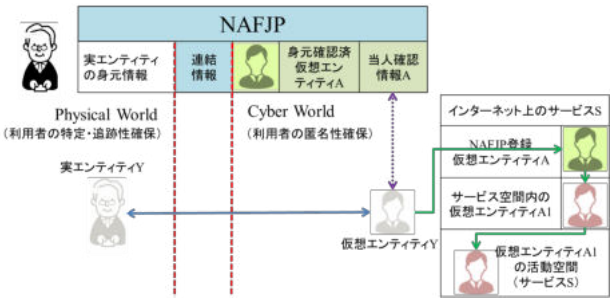

図６　インターネット上のサービス S での NAFJP 利用

3　安心・安全電子メール利用基盤 SSMAX への日本の本人確認基盤 NAFJP 適用案

現在の電子メール（インターネットメール）では利用者の確実な本人確認や悪意のある利用者の特定・追跡性については考慮されておらず，個人対象のフィッシングメールや組織対象の標的型攻撃メール等の悪意のあるメールの流通を安易に許す現在のメールシステムの脆弱性により，メールへの信頼性が失われつつある．

我が国では悪意のある電子メールへの技術的対策として，SPF（[19]），DKIM（[20]），DMARK（[21]）等が導入されているが，一定の効果はあるものの抜本的な対策には程遠い状況である．また，セキュリティ機能を強化したメールの技術仕様として S/MIME：Secure / Multipurpose Internet Mail Extensions（[22]）が規定されているが，①メールアドレス証明書の費用負担問題，②利用環境を維持する利用者の作業負担問題，③秘密情報の不正持出検査やウイルス等の悪意の有無の検査に対応できない S/MIME の暗号化機能問題により，普及・活用が進んでいない．

筆者らは，悪意のあるメールの流通を安易に許す現在のメールシステムの脆弱性を克服し，更に個人情報や秘密情報の安全な送受信が可能な「安心・安全電子メール利用基盤（SSMAX）」を提唱している．

本章では，まず安心･安全電子メール利用基盤 SSMAX を機能・特徴を紹介の上，本人確認および送信者の匿名性と特定・追跡性に関連する仕組みを説明する．次に，SSMAX への NAFJP の適用案を示し，NAFJP を利用した SSMAX における利用者（メール送信者）の匿名性と特定・追跡性の両立方式について考察する．

3.1　SSMAX 概要

［認証の連鎖による送信者・送信内容の真正性確認］

SSMAX では，楕円エルガマル暗号による電子署名を利用し，メール送信者の認証（本人確認）および送信内容の認証（非改ざん性）の検証を可能とする（図７）．具体的には，次のステップで実施する．

① メール送信者は，本文および添付ファイルから構成されるメール全体に送信者の署名を付与し，送信者が所属する MSP（メールサービスプロバイダ）や組織のメールサーバへ送信する．

② MSP/組織のメールサーバは，送信者の署名検証により送信者の認証と同時に送信内容の非改ざん性を検証する．MSP/組織が送信者認証および送信内容の非改ざん性検証に成功した場合，メールに付与されている送信者の署名は MSP/組織の署名に付け替えられ，メール受信者が所属する MSP/組織に送信する．

③ 受信者が所属する MSP/組織のメールサーバは，送信側の MSP/組織の署名検証により，送信者の認証を実施した送信側の MSP/組織の認証と同時に送信内容の非改ざん性を検証する．MSP/組織のメールサーバが送信側の MSP/組織の認証および送信内容の非改ざん性検証に成功した場合，メールに付与されている送信側の MSP/組織の署名は受信側の MSP/組織の署名に付け替えられ，受信者へ送信する．

④ 受信者は，所属する MSP/組織の署名検証により，送信者の認証を実施した送信側の MSP/組織およびその送信側の MSP/組織を認証した受信側の MSP/

組織の認証と同時に送信内容の非改ざん性を検証する．受信者が所属する MSP/組織の認証および送信内容の非改ざん性の検証に成功した場合，受信者はメール処理を行う．

以上のステップを通じ受信者が受信するメールは，SSMAX の適切な認証の連鎖を通過してきたメールであるため，送信者の認証および送信内容の非改ざん性が検証されたメールであることを，受信者は確認できる．

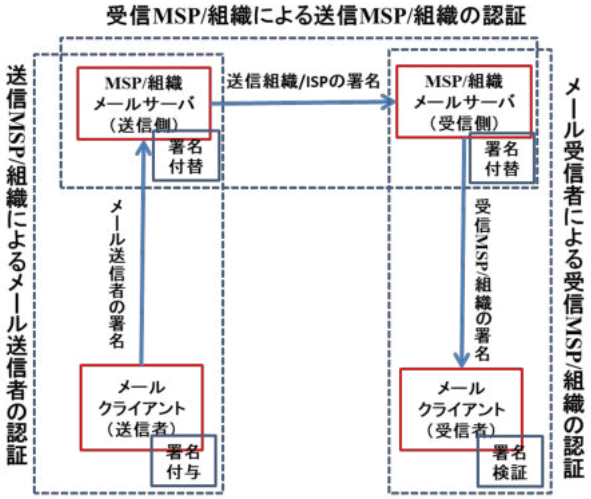

図７　認証の連鎖

組織を対象とした標的型攻撃メールは，受信者の業務通信相手（送信者/送信組織）をなりすましたメールが大半である．このようななりすましメールは，SSMAX では送信組織の正規の署名が付与されていないため拒否可能であり，標的型攻撃メールの被害を避けることができる．個人を対象としたなりすましメールの多くも，金融機関等の信頼できる組織からのメールのなりすましである．このようななりすましメールも，送信組織の正規の署名が付与されていないため拒否可能であり，フィッシング詐欺等の被害を回避することができる．

このように，SSMAX の認証の連鎖により，なりすましメールを検知・排除できると共に，メール内容の改ざんも検知可能となる．

［メール送信者の特定・追跡性］

送信者なりすましや送信内容の改ざん検知だけでは，悪意のあるメール，たとえば誹謗・中傷メールやいじめメール，様々のフェイクメールの横行の抑止は難しく，送信者を何らかの手段で確実に特定・追跡でき，送信者への注意喚起やメール利用停止等の措置がとれる仕組みが必要である．

SSMAX では，メール送信者の特定・追跡性の実現において，送信 MSP/組織が一定の役割を果たすことを想定している．MSP/組織がメール利用者を登録する際の手順を図８に示しているが，MSP/組織は住民基本台帳制度による利用者の確実な身元確認あるいは身元確認が既に実施された職員・社員番号や契約者番号等を確認の上，更に確実な当人確認により，利用者の特定・追跡性を確認する．その上で，MSP/組織は利用者を登録しメールアドレス，公開鍵証明書等を発行する．マイナンバーとのリンクが確認されている情報とメールアドレス，公開鍵証明書等との対応を MSP/組織が保持することにより特定・追跡性を実現する．このように，行政の効率化，国民の利便性の向上，公平・公正な社会の実現のための社会基盤として導入され活用が始まった住民基本台帳制度を利用し，SSMAX におけるメール送信者の特定・追跡性を実現する．

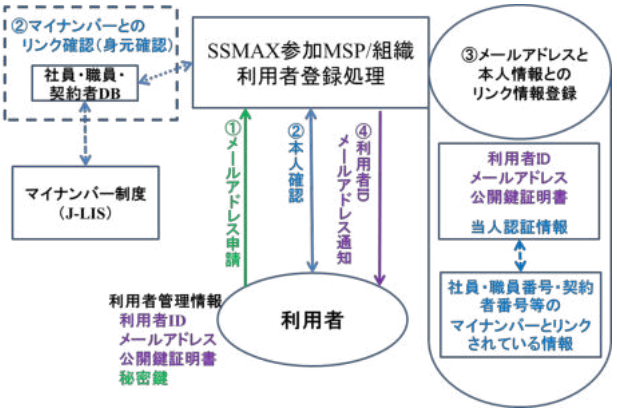

図８　利用者の MSP/組織への登録手順

［メール送信者の匿名性］

メール送信者の匿名性の実現においても SSMAX では MSP/組織が一定の役割を果たすことを想定している．メール送信時の手順を図９に示しているが，MSP/組織が送信者のメールアドレス，公開鍵証明書に対応する身元情報の安全・確実な管理により，またメール利用者に対し発行するメールアドレス，所有者名として，利用者の実名を推測できない仮名（ニックネーム等）の使用を認めることにより，一定レベルの匿名性の実現が可能である．

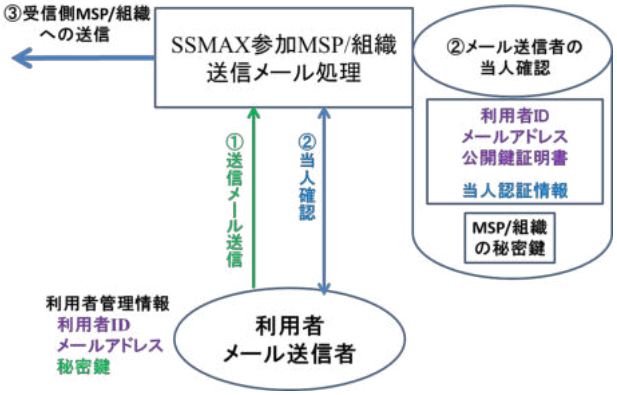

図９　SSMAX 利用者のメール送信手順

3.2　SSMAX への本人確認基盤 NAFJP 適用案

SSMAX の基本機能である［認証の連鎖による送信者・送信内容の真正性確認］を維持しつつ，［メール送信

者の特定・追跡性］および［メール送信者の匿名性］を実現できるよう NAFJP を適用した SSMAX/NAFJP の概要を示す.

［メール送信者の特定・追跡性］

NAFJP を利用した SSMAX においては，身元確認，当人確認は NAFJP 側で実施済みとし，MSP/組織は，利用者から送信される，NAFJP が発行する NAFJP-ID，公開鍵，有効期限あるいは発行日時等を含む本人確認証明書を使用し，利用者登録を行い，利用者 ID およびメールアドレスを発行する（図１０）.

万一，メール受信者が不正・不法あるいは悪意のあるメールを送信した場合は，図７に示す認証の連鎖を遡り，送信側の MSP/組織（送信者が利用者登録をしている MSP/組織）へ到達でき，その MSP/組織が管理する利用者 ID と NAFJP-ID の対応から送信者の NAFJP-ID を特定でき，NAFJP の協力により，送信者の特定・追跡が可能となる.

同時に，NAFJP の本人確認機能の利用により，MSP/組織は，利用者の本人確認に使用する個人情報・プライバシー情報の入手・管理，それらの情報を使用した当人確認機能の実装・維持が不要となる.

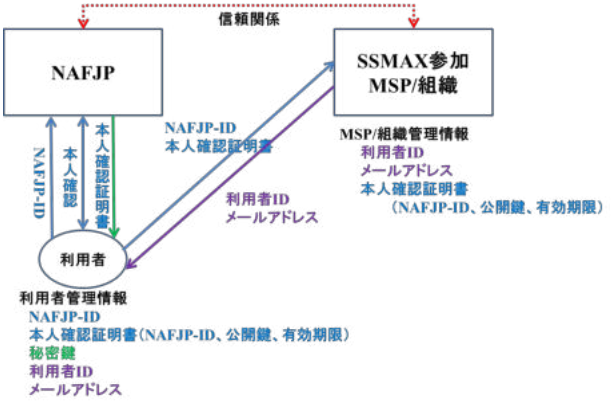

図１０　NAFJP 利用 SSMAX における利用者登録

［メール送信者の匿名性］

登録済みの利用者がメールを送信する場合の手順を図１１に示している.

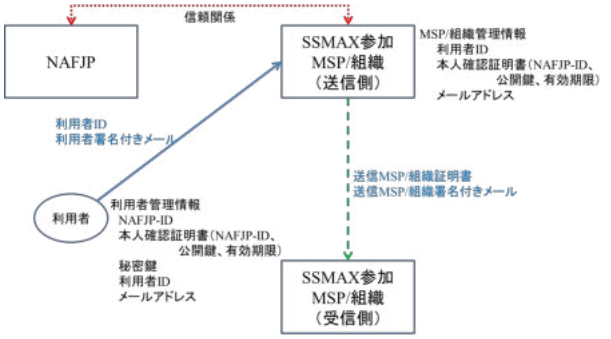

図１１　NAFJP 利用 SSMAX によるメール送信

送信者は利用者 ID と送信者の署名付きメール，必要に応じ本人確認証明書を MSP/組織へ送信する．メールを受信した MSP/組織は，本人確認証明書の有効性およびその証明書と利用者 ID およびメールに付与された署名の検証を行い，MSP/組織の署名へ付け替えたメールおとび送信 MSP/組織証明書と共に，受信側の MSP/組織へ送信する.

以上の手順で送信されたメールに含まれる送信者の情報はメールアドレスやニックネーム等のみで，送信者の特定・追跡に繋がらないようメールアドレスやニックネーム等を設定することにより，一定の匿名性が確保可能である.

3.3　NAFJP を利用した SSMAX のメリット

NAFJP を利用した SSMAX により，利用者の匿名性および特定・追跡性を含め SSMAX 本来の機能は維持できると共に，以下のような効果を期待できる.

ア：利用者の課題の克服

①複数の MSP 利用や組織へ所属している場合も，それぞれの MSP/組織ごとに本人確認情報（個人情報・秘密情報等）を提供する必要が無く，国のガイドラインや監査・認定等の制度で一定の信頼性が確認された NAFJP のみへの本人確認情報の提供により，利用者の不安を軽減

②NAFJP のみによる本人確認のため，保持しておくべき本人確認情報が整理・削減でき，その本人確認情報の安全・確実な管理のための，利用者の負担を軽減

③従来のサービス事業者ごとに求められる異なる本人確認情報の提示に対し，NAFJP の利用により提示すべき本人確認情報が整理・削減できることによる，利用者の利便性の改善

イ：事業者の課題の克服

①利用者の本人確認情報は NAFJP 側での運用・管理のため，SSMAX 側ではその安全な運用・管理の負担は不要

②NAFJP の利用により，本人確認技術に進展に応じた本人確認機能の実装のための SSMAX 側の負担は不要

ウ：社会の課題の克服

①NAFJP の適切な維持・管理による，本人確認関連技術の発展の成果である新たな本人確認手段のタイムリーな実装により，各サービス事業者での採用が促進され，社会における安心・安全なインターネットの高度利用が実現

4　おわりに

社会がインターネット依存を強める中，社会の安心・安全の確保には，インターネットの安心・安全の確保が不可欠である.

インターネットの安心・安全確保のためには，利用者の確実な本人確認，不正・不法あるいは悪意のあるイン

ターネット利用者のすみやかな特定・追跡が必要であるが，同時に，個人情報やプライバシー情報の保護のための匿名性もまた必要である．

本稿では，筆者らが提唱している日本の本人確認基盤 NAFJP においても，匿名性と特定・追跡性の両立が可能であることを示し，更に電子メールの送信者の匿名性および特定・追跡性を可能とする，筆者らが別途提唱している安心･安全な電子メール利用基盤 SSMAX に対し，NAFJP 適用モデルを示し，身元確認情報，当人確認情報等の個人情報の管理が不要にもかかわらず，確実な本人確認および特定・追跡性の両立ができる SSMAX の実現が可能なことを示した．このような NAFJP の利用により，インターネット上の様々のアプリケーションにおいても，特定・追跡性を保証しつつの匿名性実現が可能である．

日本のインターネット社会の安心・安全の維持強化のために，日本のインターネット社会の更なる発展のために，匿名性と特定・追跡性の両立が可能な本人確認基盤 NAFJP の早期の社会実装を期待したい．

謝辞

九州大学大学院・システム情報科学研究院の櫻井教授には，本研究の議論に参加いただき，有益な助言をいただいた．

参考文献

[1] 才所敏明，辻井重男，「インターネット時代の本人確認基盤に関する考察－ NAF から GAF へ －」，コンピュータセキュリティシンポジューム 2020（CSS2020），2020 年 10 月 26 日．

[2]才所敏明，「NAFJP における本人確認方法に関する考察 － National Authentication Framework in Japan －」，コンピュータセキュリティシンポジューム 2019（CSS2019），2019 年 10 月 21 日．

[3]才所敏明，辻井重男，「日本における本人確認基盤（NAFJA）の考察 － National Authentication Framework in Japan －」，情報処理学会・第 85 回コンピュータセキュリティ研究発表会，2019 年 5 月 24 日．

[4] 才所 敏明，五太子 政史，辻井 重男：“「安心・安全電子メール利用基盤（SSMAX）」悪意のあるメールの根絶とメール内容の確実な保護を目指して”，情報処理学会論文誌 59 巻 9 月号．

[5]才所 敏明，五太子 政史，辻井 重男：“「安心・安全電子メール利用基盤（SSMAX）」”，CSS2017．

[6]才所 敏明，五太子 政史，辻井 重男：”「安心・安全電子メール利用基盤（SSMAX）」構想”，SCIS2017．

[7]才所敏明，五太子政史，辻井重男：”標的型メール攻撃に対抗する「組織通信向け S/MIME」”，CSS2016．

[8]辻井重男，五太子政史，才所敏明：”標的型攻撃・サイバー戦争から日本を守るには”, JSSM 第 30 回全国大会．

[9]「2018 年度情報セキュリティの脅威に対する意識調査」報告書，独立行政法人情報処理推進機構，2018 年 12 月．
https://www.ipa.go.jp/files/000070256.pdf

[10]「行政手続におけるオンラインによる本人確認の手法に関するガイドライン」，各府省情報化統括責任者（CIO）連絡会議決定，2019 年 2 月．
https://cio.go.jp/sites/default/files/uploads/documents/hyoujun_guideline_honninkakunin_20190225.pdf

[11]「Society5.0 を見据えた個人認証基盤のあり方について」（報告），Society5.0 を見据えた個人認証基盤のあり方懇談会，2018 年 6 月．
http://www.soumu.go.jp/main_content/000560861.pdf

[12]「Developing Trust Frameworks to Support Identity Federations」，NISTIR 8149，January 2018.
https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8149.pdf

[13]「Be sure your users are who they say they are」，Government Digital Service，UK.
https://www.verify.service.gov.uk/

[14]「Yoti is the new way to prove your identity」，Yoti.
https://www.yoti.com/

[15]「Digital Identity Guidelines」，NIST Special Publication 800-63-3，June 2017.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

[16]「Digital Identity Guidelines: Enrollment and Identity Proofing Requirements」，NIST Special Publication 800-63A，June 2017.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf

[17]「Digital Identity Guidelines: Authentication and Lifecycle Management」，NIST Special Publication 800-63B，June 2017.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

[18]「Digital Identity Guidelines: Federation and Assertions」，NIST Special Publication 800-63C，June 2017.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63c.pdf

[19] “Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1”. RFC7208.
https://tools.ietf.org/html/rfc7208

[20] “DomainKeys Identified Mail (DKIM) Signatures”. RFC6376.
https://tools.ietf.org/html/rfc6376

[21] “Domain-based Message Authentication,

Reporting, and Conformance (DMARC)", RFC7489.
https://tools.ietf.org/html/rfc7489
[22] "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification", RFC8551.
https://tools.ietf.org/html/rfc8551
[23] 「What is Aadhaar」, Unique Identification Authority of India, Government of India.
https://uidai.gov.in/what-is-aadhaar.html
[20] 「Technology for 1.2 Billion Indians」, Unique Identification Authority of India, Government of India.
https://www.indiastack.org/
[21] 「Simple, secure access to government services online」, General Services Administration, USA.
https://www.login.gov/