情報処理学会論文誌 Vol.59 No.9 1545–1556 (Sep. 2018)

「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

才所 敏明[1,a)] 五太子 政史[1] 辻井 重男[1]

受付日 2017年10月5日, 採録日 2018年6月8日

概要：標的型攻撃メール，フィッシングメール，中傷や脅迫を目的としたメール等の悪意のあるメールの氾濫を抑止し，メール内容の改ざん検知・漏洩防止が可能な「安心・安全電子メール利用基盤（SSMAX）」を提案する．悪意のあるメール対策として，メール送信者の認証とともに，送信者の特定・追跡機能の重要性を示し，SSMAX における認証・特定・追跡機能の実現方式を示す．また，個人のプライバシや組織の秘密情報の漏洩防止にはメール内容の暗号化が有効であるが，秘密情報の不正持出しやウイルスチェック等の内容検査の困難さ等，暗号化の負の側面の克服も重要であることを示し，SSMAX におけるメール内容漏洩防止機能とメール内容検査機能の両立方式を示す．また，現在推進されている標的型攻撃メール対策（人的対策，技術的対策）の効果の限界や費用負担問題を指摘，さらにセキュアメール標準 S/MIME の現状・課題を示し，SSMAX の優位性を示す．最後に，「安心・安全電子メール利用基盤（SSMAX）」を，わが国の高度情報化社会を支える安心・安全な基礎的・共通的コミュニケーション基盤として社会実装するための課題を指摘し，その克服方策について考察する．

キーワード：標的型攻撃メール，フィッシングメール，中傷メール，脅迫メール，いじめメール，悪意のあるメール，SPF，DKIM，暗号メール，S/MIME，SSMAX，安心・安全電子メール利用基盤，認証，暗号，組織暗号，楕円エルガマル暗号，匿名性，連結可能匿名性

Secure and Safe E-mail Exchange Framework (SSMAX) Aiming at Eradicating Malicious Mail and Protecting Mail Content

Toshiaki Saisho[1,a)] Masahito Gotaishi[1] Shigeo Tsujii[1]

Received: October 5, 2017, Accepted: June 8, 2018

Abstract: We propose “Secure and Safe e-MAil eXchange framework (SSMAX)” which is effective as measures against malicious e-mails, such as targeted attack e-mails, phishing e-mails, slander e-mails and intimidation e-mails, and also is effective for falsification detection and leakage prevention of e-mail contents. As an anti-malicious e-mail countermeasure, we show the importance of the sender’s identification / tracking function and show its implementation method. Also, to protect personal privacy and organizational confidential information, we show an implementation method of encrypted e-mail system that can be introduced by organization. We show the superiority of SSMAX, comparing with the current defense methods which are being promoted within Japan, and comparing with the secure e-mail standard S/MIME. Finally, we describe the issues and overcoming policies for implementing “Secure and Safe e-MAil eXchange framework (SSMAX)” as a safe and secure fundamental / common communication infrastructure supporting Japan’s advanced information society.

Keywords: targeted-attack-mail, phishing-mail, slander-mail, intimidation-mail, bullying-mail, malicious-mail, SPF, DKIM, encrypted-mail, S/MIME, SSMAX, secure-and-safe-e-mail-exchange-framework, authentication, encryption, elliptical-elgamal-cryptosystem, cryptosystems-for-social-organizations, anonymity, linkable anonymity

1. はじめに

インターネットの歴史とともに発展してきた電子メール（以下，メールと略記）は，コミュニケーション手段の多様化が進む中でも基礎的・共通的コミュニケーション基盤として，依然として重要な役割を担っている．「ビジネスメール実態調査 2017」[1] によると，ビジネスマンの業務上の通信手段は，メール 99.08%，電話 90.10%，会う 74.07%等が主要なものであり，LINE 19.42%，Facebook 10.06%等，最近のツールも使われ始めているが，メールがネット経由の電子的通信手段の主役であるのは間違いない．しかし，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．

我々は，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，さら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（以下，SSMAX と略記）」を提唱する．高度情報化が進む中，新たなコミュニケーション手段が次々と出現する中でも，今後もメールが基礎的・共通的コミュニケーション基盤としての役割を果たすのは確実である．SSMAX は，メールシステムの安全性をさらに高め，その安全性に裏付けられたメールへの安心感の醸成により，わが国の生活や産業を支える安定した基礎的・共通的コミュニケーション基盤の確立を目指すものである．

まず，SSMAX の機能を実現するための悪意のあるメールの氾濫を抑止する仕組みを 2 章で，メールからの情報漏洩を防ぐ仕組みを 3 章で示し，SSMAX が安心・安全な電子メール利用基盤として維持されるために必要な運用・管理の仕組みを 4 章で示す．続く 5 章では現在展開されている標的型攻撃メール対策（技術的対策および人的対策）と比較した場合の，6 章ではセキュアメール標準 S/MIME と比較した場合の，SSMAX の優位性を示している．最後に，SSMAX の社会実装上の課題とその克服策について 7 章で考察している．

2. 悪意のあるメールの氾濫を抑止する仕組み

メールは，組織や国民の活動で最もよく利用されているコミュニケーション手段であり，それがゆえに，悪意を送り込む媒体として攻撃者に利用されることが多い．

一般に，メール受信者は，メールヘッダの送信者の名前・所属やメールアドレスにより，送信者や送信組織が信頼できるかどうか，メールの内容に心当たりがあるかどうか，を確認する．メール受信者は，このような確認で不審な点を感じなければ，メールを処理することになる．このようなメール受信者の判断基準を逆手にとり，送信者・送信組織の名前やメールアドレス，さらにメール内容を，受信者にとっての信憑性の度合いを高めたうえで，悪意を秘めてメールを送り込む，という攻撃が急増している．

昨今の大きな社会問題となっている組織を狙った標的型攻撃においても，その攻撃対象とする組織のネットワークへの侵入手段としては，業務上のメールになりすましたメール（標的型攻撃メール）が利用されることが圧倒的に多い [2]．また，やはり大きな社会問題になっている個人を狙ったフィッシング詐欺においても，偽サイトへの誘導を目的としたメール内容の信憑性を高めるため，信頼できる送信組織や知人の名前を送信者として利用したなりすましメール（フィッシングメール）が利用されることが多い．

本稿で提唱する SSMAX は，メール送信者およびメール内容を確実に認証できる仕組みの導入により，なりすましメール・改ざんメールを検出でき，また送信者個人を確実に特定・追跡可能とする仕組みの導入により，悪意が秘められたメールの送信者を特定・追跡でき，匿名性を悪用した犯罪に利用されない電子メール利用基盤を目指したものである．

2.1 メール送信者の認証および送信内容の非改ざん性の検証方式

SSMAX では，電子署名を利用した認証の連鎖（**図 1**）により，メール送信者の認証および送信内容の非改ざん性の検証を実施する．SSMAX では，メールサーバでの再暗号化（暗号化鍵の付替え）および検査サーバでの復号で暗号化情報や秘密鍵の安全性を高めることを目的として楕円エルガマル暗号ベースの組織暗号の利用を想定（3 章で説明）しており，認証の連鎖の実現においても楕円エルガマル暗号による電子署名の利用を想定している．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

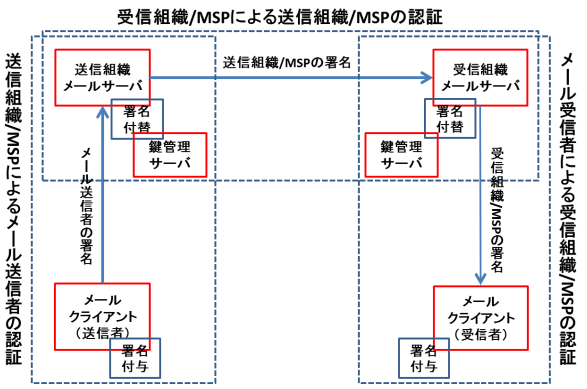

図 1 認証の連鎖
Fig. 1 Chain of certification.

[1] 中央大学研究開発機構
Research & Development Initiative, Chuo University, Bunkyo, Tokyo 112–8551, Japan
[a)] toshiaki.saisho@advanced-it.co.jp

れるメール全体に送信者の署名を付与し，送信者が所属する組織/MSP（メールサービスプロバイダ）のメールサーバへ送信する．

② 送信組織/MSP 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．送信組織/MSP のメールサーバ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送信組織/MSP の署名に付け替えられ，メール受信者が所属する受信組織/MSP に送信される．

③ 受信組織/MSP のメールサーバは，送信組織/MSP の署名検証により，送信者の認証を実施した送信組織/MSP の認証と同時に送信内容の非改ざん性を検証する．受信組織/MSP のメールサーバが送信組織/MSP 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組織/MSP の署名は受信組織/MSP の署名に付け替えられ，受信者へ送信される．

④ 受信者は，受信組織/MSP の署名検証により，送信者の認証を実施した送信組織/MSP をさらに認証した受信組織/MSP の認証と同時に送信内容の非改ざん性を検証する．受信者が受信組織/MSP 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．

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）に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・排除できるとともに，メール内容の改ざんも検知可能となる．

2.2 メール送信者の特定・追跡性と匿名性の両立方式

悪意のあるメールの氾濫は，現在幅広く利用されているメールシステムではメール送信者の特定・追跡が難しいことに根本的な原因がある．送信者を何らかの手段で確実に特定・追跡できることが保証されているメールシステムの場合，悪意のあるメールの送信者への注意喚起や法的手段を講じることが可能となり，悪意に満ちた誹謗中傷や犯罪目的のメールの氾濫を抑止することが可能である．

SSMAX では，送信者を確実に特定・追跡できることが保証されているメールシステムを目指しているが，個人は通信相手と共有する世界に応じたニックネームやメールアドレスを使用する場合も多く，匿名性も多様なメール文化を支える重要な要素である．このようなメール文化の発展を阻害しないように，一定の範囲の匿名性を保証しつつも，社会的に許されない悪意に満ちた誹謗中傷や犯罪目的のメールの場合は，送信者を特定・追跡し注意喚起や法的手段を講じることが可能な仕組みの実現を，SSMAX では目指している．

メール送信者の特定・追跡性の実現においては，SSMAX では送信組織/MSP が一定の役割を果たすことを想定している．具体的には，組織/MSP がメール利用者を登録する際，組織/MSP は利用者が提示する職員・社員番号や契約者番号等のあらかじめマイナンバとのリンクが確認されている情報および本人確認により，利用者の特定・追跡性を確認する．そのうえで，組織/MSP は利用者を登録しメールアドレス証明書（公開鍵証明書）を発行する．マイナンバとのリンクが確認されている情報とメールアドレス証明書との対応を組織/MSP が保持することにより特定・追跡性を実現する（**図 2**）．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マイナンバ制度を利用し，SSMAX におけるメール送信者の特定・追跡性を実現する．

一方，メール送信者の匿名性の実現においても SSMAX では送信組織/MSP が一定の役割を果たすことを想定している．組織/MSP がメール利用者に対し発行するメールアドレスや利用者名として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，また，メールアドレス証明書内の所有者名としても，マイナンバとリンクされているが利用者の実名を推測できない社員・職員番号・契約者番号あるいは新たに付与したコード等の利用により，一定の範囲の匿名性を実現することができる．

SSMAX で，悪意のあるメールが発見された場合，悪意のあるメールの受信者は所属する受信組織/MSP へ連絡する．連絡を受けた受信組織/MSP は，受信したメールに付与された署名により送信組織/MSP を特定し対応を要請する．要請を受けた送信組織/MSP は，その組織/MSP のポリシに準じ，メール送信者への対応を行う．一般に，軽い警告あるいは是正勧告が相当と判断されれば，メール等で行うことになろう．メール送信者自身が悪意のあるメールを送信していない場合は，メール送信者が使用する PC 等のウイルス感染が疑われ，その時点で解消されることが期待される．もし，警告あるいは是正勧告への対応がなされない場合は，送信組織/MSP が管理しているメール利用者登録情報よりメールアドレスに対応するマイナンバとの

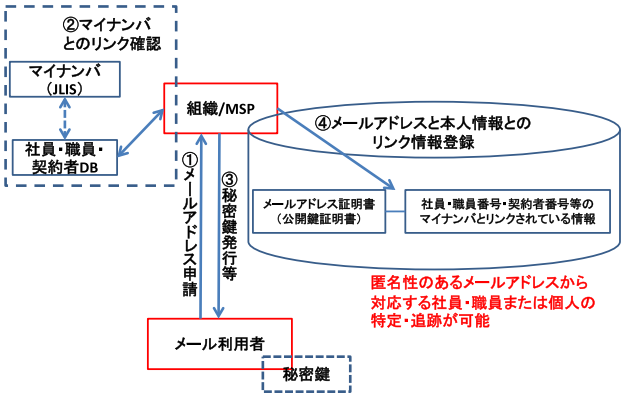

図 2　組織/MSP におけるメール利用者登録
Fig. 2　Mail user registration at organization / MSP.

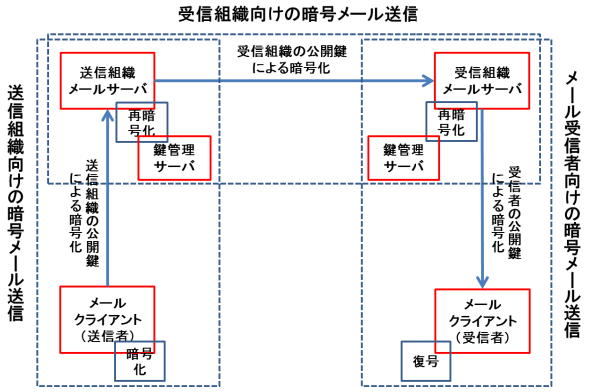

図 3　暗号化の連鎖
Fig. 3　Chain of encryption.

リンクが確認されている情報を特定し，その情報のリンクをたどることにより，マイナンバまで特定できる．さらに必要があれば地方公共団体情報システム機構（JLIS）への問合せにより 4 情報（氏名・住所・生年月日・性別）まで特定でき，悪意のあるメール送信者の確実な追跡が可能である．なお，このようなマイナンバや 4 情報まで確認のうえ，メール送信者に対応を要請するかどうかは，悪意のあるメールの内容や被害の状況に応じた判断が必要であり，国民的なコンセンサスに基づいたルール，ガイドライン等が必要となろう．

SSMAX では，以上のような方法により，メール利用者へ一定の範囲の匿名性を保証しながら，特定・追跡性を保証する仕組みの実現を目指している．

3.　メールからの情報漏洩を防ぐ仕組み

高度情報化時代，メールによるコミュニケーション内容も多様・多岐に広がりつつあり，個人の日常生活を支えるコミュニケーション手段としての役割が増すにつれプライバシ情報のやりとりも多くなり，また組織の業務活動を支えるコミュニケーション手段として活発に利用されるようになるにつれ必然的に秘密情報のやりとりも多くなることが想定される．今後も基礎的・共通的コミュニケーション基盤としての役割を期待される電子メール基盤には，暗号技術を活用した個人のプライバシ情報や組織の秘密情報の保護機能が不可欠である．

しかし，組織が送受信するメールへの暗号技術の応用には課題もある．送信組織にとってみれば，組織内の送信者が組織の秘密情報を受信者向けに暗号化したメールに含めていたとしても，暗号化されているため組織の秘密情報が含まれているかどうかの検査は送信組織では困難であり，メールによる秘密情報の不正な持出，情報漏洩を未然に防ぐことはできない．また受信組織にとってみれば，受信者向けに暗号化されたメールにウイルス等の悪意が秘められていたとしても，暗号化されているためウイルス等の悪意の有無の検査は受信組織では困難であり，組織内へのウイルス等のマルウェアの流入・感染を未然に防ぐことはできない．このように組織にとっては暗号技術が両刃の刃的存在であることをふまえ，SSMAX では，秘密情報の保護だけでなく，組織からの情報漏洩や組織への悪意のある情報の流入を防止可能な仕組みの実現を目指している．

3.1　メール送受信者が組織に所属する場合のメール内容の秘匿方式

SSMAX では，メール送受信者が組織に所属する場合に課題となる，メール内容の秘匿と組織からの情報漏洩や組織への悪意のある情報流入の防止を両立させるため，またメール受信者の公開鍵の送信者による管理を不要とするため，暗号化の連鎖方式（**図 3**）を採用している．具体的には以下のステップで，送信者により送信組織向けに暗号化されたメールは受信者向けに暗号化されたメールへ変換され，受信者へ送信される．

① 送信者は，送信者が所属する組織の公開鍵によりメールの暗号化を実施し，送信組織のメールサーバへ送信する．
② 送信組織のメールサーバは，(3.2 節に記載する方法により）送信するメールに秘密情報の不正持出がないことを確認後，送信組織の公開鍵で暗号化されているメールを，受信組織の公開鍵で暗号化されたメールへ変換（暗号化鍵の付替え，以下再暗号化と略記）し，受信者が所属する受信組織へ送信する．
③ 受信組織のメールサーバは，(3.3 節に記載する方法により）受信したメールにウイルス等の悪意が秘められていないことを確認後，受信組織の公開鍵で暗号化されているメールを受信者の公開鍵で暗号化されたメールへ変換（再暗号化）し，受信者へ送信する．
④ 受信者は，受信したメールを自身の秘密鍵により復号し，メール処理を行う．

以上のような “暗号化の連鎖” で必要となる再暗号化（特定の秘密鍵でしか復号できない暗号化情報を，復号することなく，他の秘密鍵でしか復号できない暗号化情報への変

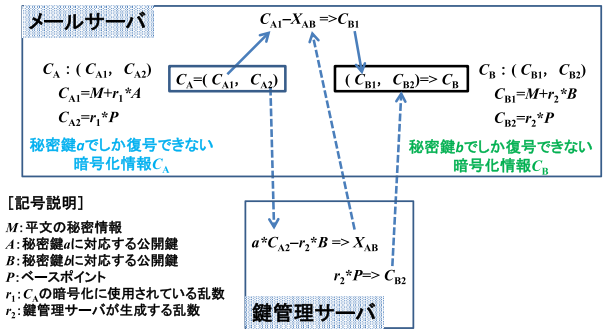

図 4　再暗号化手順

Fig. 4　Re-encryption procedure.

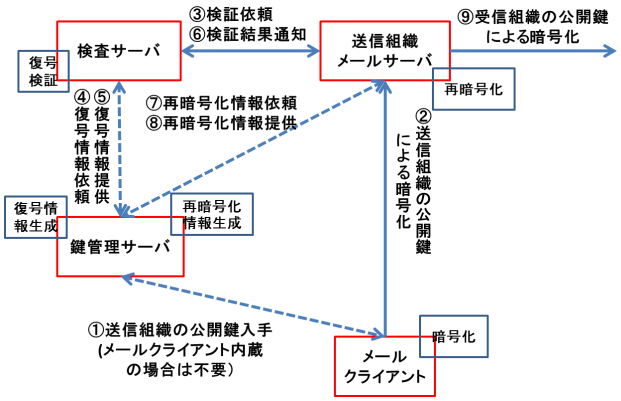

図 5　送信組織における情報漏洩検知・防止方式

Fig. 5　Detection/prevention method of information leak in mail sending organization.

換）は，筆者らが開発した楕円エルガマル暗号ベースの組織暗号方式を利用し実現する．組織暗号方式は，独立研究開発法人情報通信研究機構（NICT）における高度通信・放送研究開発委託研究課題「組織間機密通信のための公開鍵システムの研究開発–クラウド環境における機密情報・パーソナルデータの保護と利用の両立に向けて」の下に行った研究の成果である [3], [4], [5], [6].

送信組織のメールサーバが，送信組織向けに暗号化されたメール C_A を受信し，受信組織向けに暗号化されたメール C_B へ変換（再暗号化）する場合を例に，具体的再暗号化手順を以下に示す（図 4）．

① メールサーバは，送信組織の秘密鍵 a でしか復号できない暗号化情報（送信組織向けに暗号化されたメール）C_A の第 2 項 C_{A2} のみを鍵管理サーバへ送信する．

② 鍵管理サーバは，受信した C_{A2} とともに，管理している送信組織の秘密鍵 a，受信組織の公開鍵 B，ベースポイント P，および新たに生成した乱数 r_2 を使用し，変換鍵 X_{AB} および受信組織の秘密鍵 b（受信組織の鍵管理サーバが管理）でしか復号できない暗号化情報（受信組織向けに暗号化されたメール）C_B の第 2 項 C_{B2} を導出し，メールサーバへ送信する．

③ メールサーバは，受信した変換鍵 X_{AB} および管理している送信組織の秘密鍵 a でしか復号できない暗号化情報（送信組織向けに暗号化されたメール）C_A の第 1 項 C_{A1} を使用し受信組織の秘密鍵 b でしか復号できない暗号化情報（受信組織向けに暗号化されたメール）C_B の第 1 項 C_{B1} を導出し，鍵管理サーバより受信した C_{B2} と組み合わせ，受信組織の秘密鍵 b でしか復号できない暗号化情報（受信組織向けに暗号化されたメール）C_B を導出する．

このような手順による再暗号化では，暗号化情報を保持するエンティティ（メールサーバ）と秘密鍵を保持するエンティティ（鍵管理サーバ）はお互いに保有する暗号化情報および秘密鍵を開示する必要がないので，メールサーバおよび鍵管理サーバをそれぞれ独立した（結託のない）管理主体が十分なセキュリティ対策を施したうえで運用することにより，秘密情報および秘密鍵の安全性を高めることができる．

3.2　送信組織における暗号化送信メールの検査方式

メール送信者が組織に所属している場合，送信組織としては外部へ送信するメールに組織の秘密情報が不正に（許可を得ず）含まれていないかどうかの検査が不可欠である．送信メールが暗号化されていても例外ではない．暗号化されているメールに組織の秘密情報が含まれているかいないかの検査は，将来的には暗号化状態での検査技術の開発を期待したいが，現状では，いったん復号したうえでの検査が必要である．

送信組織での暗号化されたメールの具体的な処理内容・手順を図 5 に示している．このように送信組織のメールサーバは，送信組織の公開鍵で暗号化されたメールを受信する．送信組織のメールサーバは，秘密情報の不正な持出がないかどうか等，送信組織のポリシに応じた検査を検査サーバへ委託する．検査サーバは，鍵管理サーバの支援を得て暗号化されているメールを復号し，送信組織が別途用意したポリシに応じた検査を担当する専用ソフトウェアを利用し検査を実施，その結果を送信組織のメールサーバへ通知する．送信組織のメールサーバは検査サーバからの検査結果を確認後，送信組織の公開鍵で暗号化されたメールを受信組織の公開鍵により暗号化されたメールへ変換（再暗号化，図 4）し，受信組織へ送信する．

なお，検査サーバでの復号には，一般には鍵管理サーバで管理されている送信組織の秘密鍵が必要となるが，SSMAX では組織暗号の特性を活かし，鍵管理サーバが送信組織の秘密鍵を開示することなく検査サーバでの復号を可能とする方式を採用している．

送信組織の検査サーバが，送信組織向けに暗号化されたメール C_A を受信し，鍵管理サーバが管理する送信組織の秘密鍵 a の開示を受けることなく復号しメールの平文 M を得る場合を例に，具体的復号手順を以下に示す（図 6）．

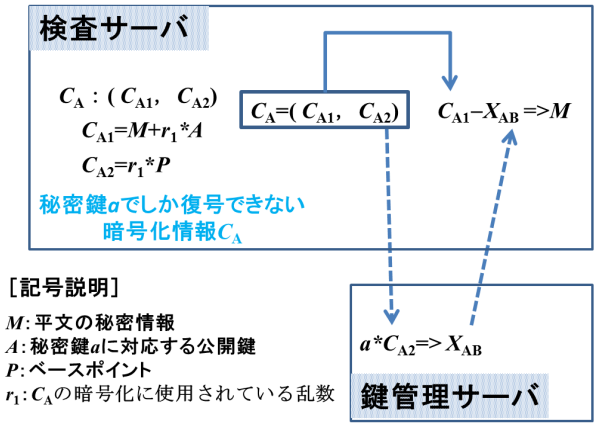

図 6　検査サーバでの復号手順

Fig. 6　Decoding procedure at the inspection server.

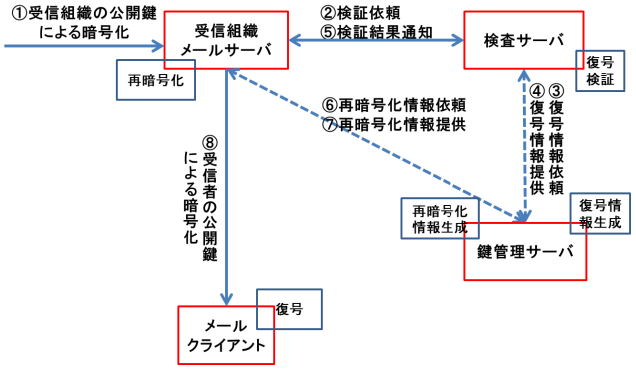

図 7　受信組織における悪意のある情報の流入防止方式

Fig. 7　Detection/prevention method of malicious information flow in mail receiving organization.

① 検査サーバは，送信組織の秘密鍵 a でしか復号できない暗号化情報（送信組織向けに暗号化されたメール）C_A の第 2 項 C_{A2} のみを鍵管理サーバへ送信する．

② 鍵管理サーバは，受信した C_{A2} および管理している送信組織の秘密鍵 a を使用し変換鍵 X_{AB} を導出し，検査サーバへ送信する．

③ 検査サーバは，受信した変換鍵 X_{AB} および管理している送信組織の秘密鍵 a でしか復号できない暗号化情報（送信組織向けに暗号化されたメール）C_A の第 1 項 C_{A1} を使用し，メールの平文 M を導出する．

このような手順による復号では，暗号化情報を保持するエンティティ（検査サーバ）と秘密鍵を保持するエンティティ（鍵管理サーバ）はお互いに保有する暗号化情報および秘密鍵を開示する必要がないので，検査サーバおよび鍵管理サーバをそれぞれ独立した（結託のない）管理主体が十分なセキュリティ対策を施したうえで運用することにより，秘密情報および秘密鍵の安全性を高めることができる．

以上の手順での復号により検査サーバでの検査が可能となり，SSMAX では秘密情報の保護機能を極力維持しつつも，秘密情報の組織からの不正な持出の検知および防止が可能となる．

3.3　受信組織における暗号化受信メールの検査方式

メール受信者が組織に所属している場合，受信組織としては外部から受信するメールにウイルス等の悪意が秘められていないかどうかの検査が不可欠である．送信メールが暗号化されていても例外ではない．暗号化されているメールにウイルス等の悪意が秘められていないかどうかの検査は，将来的には暗号化状態での検査技術の開発を期待したいが，現状では，いったん復号したうえでの検査が必要である．

受信組織での暗号化されたメールの具体的な処理内容・手順を**図 7** に示している．このように受信組織のメールサーバは，受信組織の公開鍵で暗号化されたメールを受信する．受信組織のメールサーバは，ウイルス等の悪意が秘められていないかどうか等，受信組織のポリシに応じた検査を検査サーバへ委託する．検査サーバは，鍵管理サーバの支援を得て暗号化されているメールを復号し，受信組織が別途用意したポリシに応じた検査を担当する専用ソフトウェア（ウイルスチェックソフト等）を利用し検査を実施，その結果を受信組織のメールサーバへ通知する．受信組織のメールサーバは検査サーバからの検査結果を確認後，受信組織の公開鍵で暗号化されたメールを受信者の公開鍵により暗号化されたメールへ変換（再暗号化，図 4）し，メール受信者へ送信する．

検査サーバでの復号方式は，送信組織の場合と同様，鍵管理サーバの支援を受け実施される．具体的な手順は 3.2 節で示した手順とほぼ同一でありここでは割愛するが，このような手順による復号では，暗号化情報を保持するエンティティ（検査サーバ）と秘密鍵を保持するエンティティ（鍵管理サーバ）はお互いに保有する暗号化情報および秘密鍵を開示する必要がないので，検査サーバおよび鍵管理サーバをそれぞれ独立した（結託のない）管理主体が十分なセキュリティ対策を施したうえで運用することにより，秘密情報および秘密鍵の安全性を高めることができる．

このような手順による検査サーバでの復号により受信メールの確実な検査が可能となり，SSMAX では秘密情報の保護機能を極力維持しつつも，悪意のある情報の流入検知および防止が可能となる．

3.4　受信組織内での暗号化受信メールの転送方式

一般に組織向けのメールは，メール受信者がメール内容の最終利用者ではなく適切な利用者への転送が発生する場合も多い．SSMAX では，秘密情報が含まれる暗号化されたメールの安全な転送の仕組みを用意している．

SSMAX における暗号化メールは，秘匿すべき情報（秘密情報）は暗号化されたファイルとしてメールに添付され，暗号化されている添付ファイルの説明はメール本文に

平文で記載されている，という形式を想定している．暗号化メールの受信者は，メール本文を確認し，必要な場合は適切な転送先へ対象となる (暗号化された) 添付ファイルを転送する．

転送にあたっては，受信者の公開鍵により暗号化されている情報 (添付ファイル) を受信組織の公開鍵により暗号化されている情報へ変換 (再暗号化) し，受信者の秘密鍵による署名を付与したうえで，メールを送信する．そのメールを受け取った受信組織のメールサーバは，受信組織の公開鍵により暗号化されている情報 (添付ファイル) を新たなメール受信者 (転送先) の公開鍵により暗号化されている情報へ変換 (再暗号化) し，受信組織の秘密鍵による署名を付与したうえで，メールを新たな受信者 (転送先) へ送信する．

このように，SSMAX ではメール受信者の手元で扱う必要のない秘密情報が格納されている（暗号化された）添付ファイルについては，組織暗号の特性を活かし，メール受信者の手元では復号せず暗号化状態で転送されるため，秘密情報の安全性を高める効果が期待できる．

3.5 メール送受信者が組織に所属しない個人の場合のメール内容の秘匿方式および暗号化メールの検査方式

SSMAX では，メール送信者が組織に所属せず MSP を利用する個人の場合でも，その個人が所属する送信 MSP の公開鍵により暗号化し，送信 MSP のメールサーバまでの経路でのメール内容の秘匿を実現する．しかし，個人のプライバシ情報保護のため送信 MSP では暗号化されたメールのいったん復号しての検査は行わず，再暗号化を実施し受信組織/MSP 宛に送信するものとする．

また，メール受信者が組織に所属せず MSP を利用する個人の場合も，メール受信者が所属する受信 MSP は，送信組織/MSP から受信した暗号化されたメールは，再暗号化を実施し受信者へ送信，受信 MSP のメールサーバから受信者のクライアントまでの経路でのメール内容の秘匿を実現する．しかし，個人のプライバシ情報保護のため，受信 MSP での暗号化されたメールのいったん復号しての検査は行わないものとする．

ただし，メール利用者個人の同意（希望）があれば，暗号化されたメールに対しても，送信 MSP によるメール送信時のいったん復号しての検査（送信メールにウイルス等の悪意が混入していないかどうか等），受信 MSP によるメール受信時のいったん復号しての検査（ウイルス等の悪意の秘められたメールではないかどうか等）は，MSP の判断により実施可能とする．

4. 安心・安全な電子メール利用基盤維持の仕組み

サイバー攻撃に悪用されない，しかもメール内容の漏洩を防止できる安心・安全な電子メール利用基盤を目指した SSMAX のシステム構成は図 8 のとおりである．

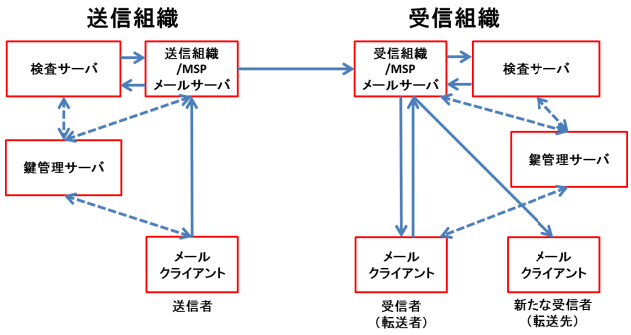

図 8 SSMAX のシステム構成
Fig. 8 System configuration of SSMAX.

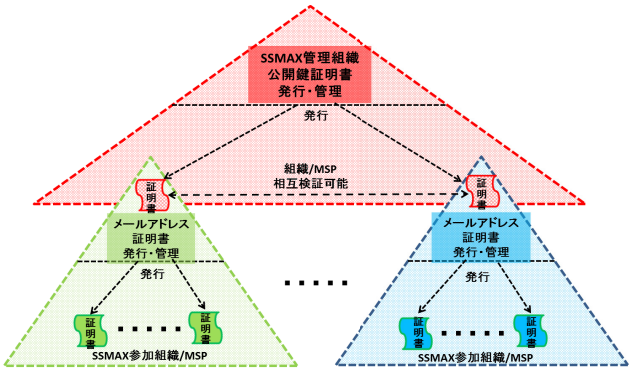

図 9 SSMAX における PKI の階層
Fig. 9 Hierarchy of PKI in SSMAX.

SSMAX では，メール送受信者の認証およびメール内容の非改ざん性検証，メール内容の漏洩防止等のため，メール送受信者（利用者），送信組織/MSP，受信組織/MSP の楕円エルガマル暗号による署名付与・検証および暗号化・再暗号化・復号のメカニズムを利用している．具体的には，2 章および 3 章で記載しているとおり，組織/MSP が所属するメール利用者へ発行・管理するメールアドレス証明書，および SSMAX 管理組織が参加組織/MSP へ発行・管理する公開鍵証明書により実現している．図 9 に SSMAX における PKI の階層を示している．

SSMAX を構成するメール利用者，組織/MSP，および SSMAX 管理組織の役割・作業としては，以下のような内容を想定している．

［メール利用者］

メール利用者は，自分自身の秘密鍵に対応する公開鍵，メールアドレスや所有者名，メール利用者を特定・追跡可能な情報等を所属する組織/MSP へ提示し，メール利用を申請する．本人確認および特定・追跡性確認のためには，組織に所属する職員・社員の場合は，あらかじめマイナンバとのリンクが確認されている職員・社員番号（職員・社員カード）の提示を行う．組織に所属しない個人の場合は，マイナンバとのリンクが確認されている MSP との契約番

号の提示を想定しているが，マイナンバ（マイナンバカード）そのものの提示の可能性も想定している．

メール利用申請が受理されると，プライベートなメールアドレス証明書および所属する組織/MSP のパブリックな公開鍵証明書が配布され，メール利用が可能となる．

メール利用者が管理すべき情報は，自身の秘密鍵・メールアドレス証明書 1 組と，所属する組織/MSP の公開鍵（証明書）1 個のみである．メール送受信者全員のメールアドレス証明書を管理する必要があるセキュアメール標準 S/MIME（6 章）に比べ，メール利用者の管理作業は大幅に軽減可能である．

［組織/MSP］

組織/MSP はメール利用申請者の本人確認および特定・追跡性の確認後，メールアドレス証明書を発行する．組織/MSP は，所属するメール利用者のメールアドレス証明書および特定・追跡のためのマイナンバとリンクされた情報の組合せを鍵管理サーバ等で管理する．

組織/MSP はまた，メールサーバおよび検査サーバより提示される公開鍵に対し公開鍵証明書を発行し，公開鍵証明書を鍵管理サーバで管理する．

メールサーバおよび検査サーバは，自身の秘密鍵・公開鍵証明書のほか，所属する組織/MSP の公開鍵証明書を管理する．

組織/MSP が発行するメール利用者向けのメールアドレス証明書およびメールサーバ/検査サーバ向けの公開鍵証明書はすべて組織内でのみ利用されるのでプライベートな証明書でかまわない．パブリックな証明書利用に比べ，費用負担・運用負担は大幅に軽減できる．

なお，小規模な組織の場合は，証明書の発行・更新費用負担減に比べ，プライベートな証明書を発行する鍵管理サーバ等の運用・管理やセキュリティ維持のための費用・作業負担が上回る可能性もある．このような小規模な組織では，SSMAX 参加 MSP のサービスを受けるとか，社内 SSMAX 運用・管理を外部業者に委託する等により，費用・作業負担の軽減を図ることも選択肢となるであろう．

［SSMAX 管理組織］

SSMAX 管理組織は，SSMAX を運用する組織/MSP に対し SSMAX の運用状況を確認し，組織/MSP の公開鍵（鍵管理サーバの公開鍵）に対しパブリックな公開鍵証明書（SSMAX 証明書）を発行する．なお，現在でも組織/MSP の実在性を審査のうえで発行される EV 証明書が存在するが，SSMAX 証明書は SSMAX の適切な運用状況も審査の対象であるため，EV 証明書による代替は難しい．

組織/MSP に対し発行される SSMAX 証明書は，SSMAX 管理組織が管理するが，それぞれの組織/MSP が通信相手の組織/MSP の SSMAX 証明書を鍵管理サーバで管理することも可能である．

SSMAX 管理組織が使用する「SSMAX を適切に運用している組織/MSP かどうかの判断基準」は，関係機関の合意を得たうえで具体的かつ明確に規定しておく必要がある．また，その判断基準に基づく組織/MSP の認定は定期的に更新される必要があり，更新に値する組織/MSP かどうかの認定の手続きも規定しておく必要がある．

SSMAX 管理組織の参加あるいは継続を希望する組織/MSP の評価にあたっては，悪意のあるメールの発生頻度および発生した場合の対応状況や，SSMAX 向けに監査項目の追加が必要であるが情報セキュリティ監査制度の報告書等を参考に，判断することになろう．

5. 現在の標的型攻撃メール対策に対する SSMAX の優位性

SSMAX は，大きな社会問題となっている組織を狙った標的型攻撃，その侵入手段としての主役である標的型攻撃メール対策としても大変有効である．本章では，まず標的型攻撃メール対策の現状と課題をまとめ，次に SSMAX の標的型攻撃メール対策としての優位性を示す．

5.1 技術的対策の現状と課題

組織を対象とした標的型攻撃メールの対策として，わが国で推奨されている技術的対策は SPF [10]，DKIM [11] の 2 つであるが，両方の対策とも，DNS サーバを利用した送信メールサーバの認証（送信メールアドレスのドメインに対応する送信組織/MSP の DNS サーバに登録されている正規のメールサーバかどうかの確認）の仕組みである．この仕組みにより，送信メールアドレスのドメインに対応する送信組織/MSP の DNS には登録されていない不正なメールサーバから送信された（不正な）メールを検出可能である．

ところが，攻撃者が独自のドメインを立ち上げた場合，DNS サーバも攻撃者の管理下にあるため攻撃に使用するメールサーバの IP アドレスや公開鍵も DNS サーバに登録することができ，独自ドメインを利用した攻撃サイトからの標的型攻撃メールの検出は SPF および DKIM では難しい．

また，メール送信時にメールクライアントと送信メールサーバ間で使用される通信プロトコル SMTP は，SMTP auth や POP before SMTP 等の利用によりメール送信者認証機能の一定の強化は可能であるが，確実なメール送信者認証は難しく，送信メールアドレスのドメインに対応する送信組織/MSP の DNS サーバに登録されている正規のメールサーバからの正規の送信者になりすまして送信された不正なメールの検知は難しい．

5.2 人的対策の現状と課題

現在の技術的対策効果が不十分なため，標的型攻撃メールの現状やその特徴，見分け方の説明や教育，訓練用の標

的型攻撃メールを実際に送付しての訓練等により，メール利用者1人1人に標的型攻撃メールを見分ける能力を付与し，標的型攻撃メールの被害を回避させようとする，人的対策が多くの組織で実施されている．

しかし，教育・訓練で行われている模擬標的型攻撃メール配布実験の結果 [7], [8] では，受信した職員の10%程度が開封しており，一定の効果は期待されるものの，標的型攻撃メールに対する人的対策効果の限界も明らかである．

また，教育・訓練で得た知識・ノウハウをベースに毎日多数受信するメールが標的型攻撃メールかどうかの判断を求められる社員・職員の人件費負担は膨大であることが容易に推定できる．たとえば，「ビジネスメール実態調査2017」[1] によると，99%以上のビジネスマンがメールを主たる通信手段として利用，1日に平均13通のメールを送信し，平均39通のメールを受信している，と報告されている．社員・職員が，1日に受信するメール39通が標的型攻撃メールかどうかの判断，そのためのチェック・確認の時間が必要となる．その時間を仮に5分程度/日とすると，また平均給与が月額40万円程度の公務員一般職約120万人 [9] に限って試算すると，年間600億円程度の人件費を人的対策に投入していることになる．わが国では従業員が300人以上の民間企業に所属する社員が約1800万人であることを考えると，人的対策に対するわが国全体の費用負担がじつは膨大であろうことは容易に推定できる．

5.3 SSMAXの優位性

本節では，現在実施されている標的型攻撃メール対策に対するSSMAXによる対策の優位性を，標的型攻撃被害の回避効果およびそのための作業・費用負担の両面で示す．

[標的型攻撃被害の回避効果]

現在のSPF，DKIM等の技術対策および人的対策は一定の効果はあるものの抜本的な対策にはほど遠い．実際，現実に多くの標的型攻撃事件が発生しており，その初期侵入手段として標的型攻撃メールが使用されている．

4章で示したSSMAX運用・管理の仕組みにより，SSMAXでは標的型攻撃メールを含む悪意のあるメールの送信を行わないであろうという一定レベル信頼できるSSMAX参加組織/MSPからのメールであることを確認のうえの受信となり，標的型攻撃メールの被害を人的対策によらず，より確実に回避できる．万一，SSMAX参加組織/MSPから標的型攻撃メールを含む悪意のあるメールが送られてきた場合は，2章で示したメール送信者の認証および特定・追跡の仕組みにより，ただちに送信組織/MSPへ連絡，発信を止めさせることができ，SSMAX参加組織/MSP間での標的型攻撃メールの流通・氾濫は抑止できる．

[作業・費用負担]

5.2節で示したように，現在の人的対策では受信メールが標的型攻撃メールかどうかの判断が受信のつど必要で，メール受信者の大きな作業負担，所属する組織の大きな人件費負担となっている．わが国の産官組織の人的対策費用は年間数百億～数千億円にのぼると推定できる．

SSMAXでは，4章で示したSSMAXの運用・管理の仕組みを導入するSSMAX参加組織/MSPが増加するにつれ受信メールごとの受信者の判断作業は限りなく0に近づけることができ，年間数百億～数千億円にものぼるであろうわが国の産官組織の人的対策費用は大幅に削減可能である．なお，新たな仕組みの運用・管理のためのSSMAX参加組織/MSPやSSMAX管理組織での作業・費用負担が別途必要となるが，期待される人的対策費用削減に比べはるかに少額と見込まれ，標的型攻撃メール対策として必要な作業・費用負担は大幅な軽減が期待される．

上述のようにわが国社会全体としてのSSMAXによる作業・費用負担の大幅な軽減は現在の技術的対策および人的対策に対する揺るぎない優位性であるが，個々の組織，特に人的対策費用負担の少ない小規模な組織にとってはSSMAX導入により作業・費用負担増の可能性もある．わが国の高度情報化社会を支える安心・安全な基礎的・共通的コミュニケーション基盤SSMAXの重要性に対する社会のコンセンサスを得つつ，わが国が目指すべき社会実現のための費用負担の在り方を議論する必要があろう．

6. セキュアメール標準S/MIMEに対するSSMAXの優位性

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 [12] がある．S/MIMEは，1995年に発表され，IETFにより標準化が進められており，MIMEでカプセル化したメールの公開鍵暗号方式による暗号化とデジタル署名に関する標準規格である．

本章では，まずS/MIMEの現状・課題をまとめ，次にわが国の高度情報化社会を支える安心・安全な基礎的・共通的コミュニケーション基盤としてのSSMAXの優位性を示す．

6.1 S/MIMEの現状と課題

S/MIMEの署名機能により，メール送信者の認証（なりすましメールの排除）が可能となり，また暗号化機能により，機密情報の安全な送信にメールが利用可能となる．このような特徴を有するS/MIMEが，標的型攻撃メール対策として有効なのは，多くの報告書に記されているとおりである [13]．しかし，現実にはS/MIMEが広く普及し活用されている状況ではない．

S/MIMEが広く活用される状況にならないのには大きく3つの課題がある．

第1の課題は，メールアドレス証明書の費用負担問題である．S/MIMEでは，原則，すべてのメール送受信者が

パブリックなメールアドレス証明書を保有していることが前提となっている．パブリックなメールアドレス証明書の発行サービスを提供している事業者は多いが，一般的に1メールアドレスあたり年間数千円の費用負担が必要となる．多数の社員・職員をかかえる組織にとっては大きな負担を強いられることになる．

第2の課題は，利用者の作業負担問題である．S/MIMEでは，1人1人のメール利用者が通信するすべての相手のメールアドレス証明書を入手・保管する必要があり，しかも通信相手のメールアドレス証明書が更新されるつど，あらためて入手し更新する必要がある．

第3の課題は，S/MIMEの暗号化機能である．S/MIMEの暗号化では，メール受信者の公開鍵を使用する．そのため，メール受信者しか復号できず，送信組織での秘密情報の不正持出しの有無の検査や，受信組織によるウイルス等の悪意の有無の検査ができず，組織での導入は難しい暗号化機能となっている．

S/MIMEは現在，必要性に差し迫った組織（一部の団体や金融機関）において，メール送信組織の認証（なりすましのメールではないことを示す）目的に限って，利用されている．

6.2 SSMAXの優位性

第1の課題については，4章の［組織/MSP］で示したように，SSMAXでは利用者（個人や社員・職員）に対し所属する組織/MSPが発行するのはプライベートなメールアドレス証明書であり，パブリックなメールアドレス証明書を利用するS/MIMEに比べ，費用負担を大幅に軽減させることが可能である．

第2の課題については，4章の［メール利用者］で示したように，SSMAXでは利用者が管理する情報は自身の秘密鍵・メールアドレス証明書1組と，所属する組織/MSPの公開鍵（証明書）1個のみである．通信相手の数に応じた多数のメールアドレス証明書の管理・更新が必要なS/MIMEに比べ，作業負担を大幅に軽減させることが可能である．

第3の課題については，3章で示したように，SSMAXではメール内容の保護と同時に，送信組織での秘密情報の不正持出しの有無の検査や受信組織によるウイルス等の悪意の有無の検査が可能な暗号化方式を採用しており，S/MIMEでは難しかった組織への導入も可能な暗号化機能を実現している．

一方，SSMAXがS/MIMEの第1の課題（メールアドレス証明書の費用負担問題）克服のために送信組織/MSPでの署名の付替えを行う「認証の連鎖」方式を採用したがゆえに，その署名の付替えに関与するメールサーバおよび鍵管理サーバが外部からの攻撃により被害を受けた場合に，S/MIMEでは発生しない送信メールの送信者/送信先/送信内容等の改ざんが発生する可能性がある．SSMAXでは，S/MIMEと同等のメール送信者/メール内容の認証機能を安価に実現する代償として，サーバ側での処理に高い安全性が求められセキュリティ対策が重要となる．

また，SSMAXがS/MIMEの第2の課題（利用者の作業負担問題）および第3の課題（暗号化機能の問題）克服のために送信組織/MSPでの復号/再暗号化を行う「暗号化の連鎖」方式を採用したがゆえに，その復号/再暗号化に関与するメールサーバ，検査サーバ，鍵管理サーバが被害を受けた場合に，S/MIMEでは発生しない暗号化された送信メールからの情報漏洩が発生する可能性がある．SSMAXでは，S/MIMEで必要な利用者による送信相手のメールアドレス証明書の管理・更新作業負担をなくし，組織では受け入れられないS/MIMEの暗号化機能を組織でも活用可能な暗号化機能へ置き換える代償として，サーバ側での処理に高い安全性が求められセキュリティ対策が重要となる．

S/MIMEとSSMAXの大きな相違点は，S/MIMEがメール送信者のメールアドレスの認証までの機能であるのに対し，SSMAXでは悪意のあるメール発信を止めるため，メール送信者本人を特定・追跡できる機能まで実現していることである．SSMAXでは，メール送信者本人を特定・追跡を可能とするために組織/MSPに対し所属する利用者に対する管理責任を負わせることになる．また，そのような管理責任を適切に果たしている組織/MSPかどうかを確認し他の組織/MSPへ情報提供するSSMAX管理組織が必要となる．社会全体としてそれなりの費用負担増となろうが，メール送信者本人の特定・追跡性は，将来のわが国の高度情報化社会を支える基礎的・共通的コミュニケーション基盤として不可欠な機能であろう．

7. 「安心・安全電子メール利用基盤（SSMAX）」の社会実装上の課題

本章では，SSMAXの社会実装を進めるにあたって想定される，主要な課題とその克服策について考察する．

［研究開発・実証実験］

SSMAXの全体システム構成，主要な構成要素の実装方式，適切な運用のための留意点等，2章から4章で報告したとおりである．SSMAXの社会実装を目指すにあたり，まずは実際にSSMAXを開発し機能検証を行うとともに，実際の組織活動へ適用した実証実験等を実施，有用性・実用性を具体的に示し，SSMAXの社会実装推進に対する産業界・国民のコンセンサスを得る必要があろう．

SSMAXはわが国の高度情報化社会の発展を支える安心・安全なコミュニケーション基盤を目指すものであり，政府主導での研究開発・実証実験の推進を期待したい．

［社会実装展開］

SSMAXが十分普及した段階でのSSMAXの新規導入の場合は投資効果の算定や投資後の効果の測定や実感は容易だが，普及の初期フェーズでのSSMAX導入の場合は難し

く，各組織/MSP の個々の経営判断に任せても，SSMAX の普及は進展しない恐れがある．

そこで，SSMAX を普及させるにあたっては，まずは中央省庁，地方自治体等，官公庁や関連機関が先行導入し，有用性・有効性を実業務で示すのが効果的であろうし，SSMAX の一定範囲の普及環境を創出することも効果的であろう．官公庁や関連機関とのメール送受信が多い組織/MSP への波及効果も期待される．

SSMAX は，多くの組織/MSP に普及すればするほど，その効果は大きくなるため，一般の組織/MSP での早期導入を推進・支援する施策も必要であろう．特に小規模な組織においては，SSMAX 導入が費用負担増となる可能性もあり，4 章の［組織/MSP］で示したように小規模組織が SSMAX 運用・管理を外部業者へ安全で安価に委託できるための環境整備等も検討が必要であろう．また，5.3 節で示したように安心・安全な電子メール利用基盤を実現する社会全体としての費用負担の在り方の議論の中で，小規模組織に対する支援策（たとえば税制面での支援等）の検討も必要であろう．

SSMAX 普及は，組織/MSP に所属しメールを直接送受信する社員・職員や個人の協力も不可欠である．一般に，使い慣れたメールクライアントを変更することには抵抗を感じるものである．安心・安全電子メール利用基盤 SSMAX 導入の必要性に対する理解を得るとともに，SSMAX に特化したメールクライアントの開発においても既存のメールクライアントの利用者に操作上の違和感を極力与えないような配慮が必要であろう．また，使い慣れた従来のメールクライアントへの最小限の変更で SSMAX を利用できる仕組みの検討も SSMAX 普及の初期段階では必要であろう．

なお，SSMAX の普及には時間がかかることも予想される．SSMAX 普及の中途段階では，SSMAX 未導入組織/MSP からのメールの完全な排除が難しく何らかの例外的な対応が必要となる場合も想定される．受信者へ警告付きで配信する利便性を重視した対応から，悪意が秘められていたとしても受信組織に影響を与えないような環境（サンドボックス等）でのみ開封させる利便性よりも安全性を重視した対応まで，様々の対応が想定されるが，原則，受信組織/MSP のポリシに応じた対応となろう．いずれにせよ，SSMAX の普及を急ぎ，多くの組織/MSP でリスクのある例外的な対応を不要にするのが望ましい．

SSMAX が社会の安心・安全な電子メール利用基盤として維持され続けるためには，SSMAX 参加組織/MSP が SSMAX の仕組みを適切に運用・管理する必要がある．SSMAX の仕組みを不適切に運用・管理する SSMAX 参加組織/MSP が発生した場合，その組織/MSP から発信されるメールには悪意のあるメールが混入する恐れもあり，受信組織/MSP 側で悪意のあるメールを早期に検知できれば発信組織/MSP を特定でき対応を要請できるが，被害発生後の検知となる場合も想定され好ましくない．そこで，組織/MSP を SSMAX へ（継続）参加させるかどうかの判断（SSMAX 参加組織/MSP としての認定）を行う SSMAX 管理組織の役割・責任が重要である．SSMAX 管理組織が採用する判断基準は社会のコンセンサスを得て決定すべきであろうが，2 章から 4 章に示している SSMAX の仕組みの運用・管理の状況および情報セキュリティ対策内容を確認できる情報セキュリティ監査等の報告書や悪意のあるメールの発生・対応状況等を利用した判断基準が想定される．SSMAX 管理組織は，わが国の社会を支える安心・安全なコミュニケーション基盤を支える組織であり，社会のコンセンサスを得つつ，その維持・高度化に努めることが期待されている．

［海外展開］

SSMAX が提供する「安心・安全電子メール利用基盤」はわが国だけでなく，多くの国で基礎的・共通的コミュニケーション基盤として活用が期待される．「世界一安全な日本」を目指すわが国は，世界に先駆け「安心・安全電子メール利用基盤（SSMAX）」を実現し，世界一安全なサイバー空間の実現においても世界を先導する役割を担うべきであろう．

海外展開を図るには，SSMAX の国際標準化を進める必要がある．国際標準化は，S/MIME の仕様を議論している Internet Engineering Task Force（IETF）で進めるのが適切であろう．なお，わが国特有のマイナンバ制度の活用を想定している SSMAX のメール送信者の特定・追跡機能については，海外では各国の国民 ID 制度の利用が想定され，各国の国民 ID 制度にも対応可能な標準仕様を検討することになろう．

また，「安心・安全な電子メール利用基盤」を各国内に限定せず，世界全体に広げることも重要であろう．そのためには，技術仕様の国際標準化と同時に，組織/MSP に期待される役割と責任の考え方・具体的実施方式・基準，管理組織に期待される組織/MSP 認証方式・基準，相互認証の仕組みおよび各国で運用されるシステムの相互運用性等について，各国と協議を行う必要があろう．

8. おわりに

本稿では，サイバー攻撃への悪用を抑止可能で，メール内容の漏洩防止が可能な「安心・安全電子メール利用基盤（SSMAX）」を提案した．

また SSMAX では，標的型攻撃メール対策として現在展開されている技術的対策・人的対策に比べ，被害回避効果も大きく，作業・費用負担も大幅な削減が可能であることを示した．さらに，現在国際標準で定められているセキュアメール仕様 S/MIME に比べても，SSMAX が悪意のあるメール対策として効果的であり，S/MIME では普及が難しいメール内容の保護機能についても，SSMAX のメール

内容保護機能が社会実装可能であることを示した．

ネット依存が高まる現代社会に様々の混乱・不安を与えるメールのセキュリティ上の課題を克服できるSSMAXによる安心・安全な基礎的・共通的コミュニケーション基盤の確立は，産業界の業務活動，国民の生活活動の活発化・緊密化・効率化を促進させ，わが国の高度情報化社会のさらなる発展に貢献するものと考える．

産官学の主要組織およびキーマンの協力を得，SSMAXの早期実現，社会実装を目指したい．

参考文献

[1] ビジネスメール実態調査2017，入手先 ⟨http://www.sc-p.jp/news/pdf/170602PR.pdf⟩（参照 2017-07-31）．
[2] トレンドマイクロ（株）：国内標的型サイバー攻撃分析レポート2017年版，入手先 ⟨http://www.trendmicro.co.jp/cloud-content/jp/pdfs/doc-dl/wp-apt2017-20170508.pdf⟩（参照 2017-07-31）．
[3] 才所敏明，近藤 健，庄司陽彦，五太子政史，辻井重男：自治体における組織暗号実証実験報告，*CSS2015* (2015).
[4] 才所敏明，近藤 健，庄司陽彦，五太子政史，辻井重男：組織暗号の構成と社会的実装—個人情報の安全な利活用を目指して，情報処理学会論文誌，Vol.56, No.9 (2015).
[5] 「組織暗号」の実用化と利用に向けて—情報漏洩とマイナンバー導入に備えた自治体・医療機関における実証実験報告，入手先 ⟨https://c-faculty.chuo-u.ac.jp/˜tsujii/_userdata/organization_code.pdf⟩（参照 2016-07-14）．
[6] マイナンバー情報環境における組織通信と組織暗号—サイバー攻撃・情報漏洩に備えて，入手先 ⟨https://c-faculty.chuo-u.ac.jp/˜tsujii/_userdata/my_number.pdf⟩（参照 2016-07-14）．
[7] 政府機関における情報セキュリティに係る年次報告（平成24年度），入手先 ⟨http://www.nisc.go.jp/active/general/pdf/h24_report.pdf⟩（参照 2016-07-10）．
[8] サイバーセキュリティ政策に係る年次報告（2013年度），入手先 ⟨http://www.nisc.go.jp/active/kihon/pdf/jseval_2013.pdf⟩（参照 2016-07-10）．
[9] 国家公務員給与の概要，入手先 ⟨http://www.jinji.go.jp/kyuuyo/kou/27gaiyou.pdf⟩（参照 2016-07-10）．
[10] Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1, RFC7208, 入手先 ⟨https://tools.ietf.org/html/rfc7208⟩（参照 2016-07-11）．
[11] DomainKeys Identified Mail (DKIM) Signatures, RFC6376, 入手先 ⟨https://tools.ietf.org/html/rfc6376⟩（参照 2016-07-11）．
[12] Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification, RFC5751, 入手先 ⟨https://tools.ietf.org/html/rfc5751⟩（参照 2016-07-12）．
[13] 標的型攻撃に対抗するための通信規格の標準化動向に関する調査結果，入手先 ⟨http://www.soumu.go.jp/main_content/000227896.pdf⟩（参照 2016-07-12）．
[14] 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 (2016).
[15] 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* (2016).

才所 敏明 （正会員）

1947年生．1970年東京大学工学部計数工学科卒業，同年（株）東芝入社，企業情報活動基盤の高度化企画・推進および情報セキュリティ技術の研究企画・開発活動に従事，2007年（株）IT企画代表取締役社長，2013年より中央大学研究開発機構・研究員．電子情報通信学会，IEEE，ACM各会員．

五太子 政史

1959年生．1984年東京大学農学部農芸化学科卒業．2011年中央大学大学院理工学研究科博士後期課程修了（情報セキュリティ科学専攻）．ソフトウェアベンダでセキュリティソフトの販売および技術サポートに従事した後，中央大学研究開発機構で情報セキュリティ・ネットワークセキュリティの教育，暗号技術の研究に従事．現在，中央大学研究開発機構准教授．

辻井 重男 （正会員）

1933年生．1958年東京工業大学工学部電気工学科卒業．同年日本電気（株）入社．山梨大助教授．東京工業大学教授．中央大学教授を経て，2004年情報セキュリティ大学院大学長．1998年一般財団法人マルチメディア振興センター理事長等を歴任．現在，放送セキュリティセンター理事長，マルチメディア振興センター顧問，東京工業大学名誉教授．中央大学研究開発機構フェロー．工学博士．電子情報通信学会功績賞，NHK放送文化賞，内閣官房「情報セキュリティの日」功労者表彰，2009年春瑞宝中綬章，2014年C&C賞等を受賞．電子情報通信学会会長，総務省電波監理審議会会長，日本学術会議会員等を歴任．日本ペンクラブ会員．