「安心・安全電子メール利用基盤（SSMAX）」

才所 敏明[†1]　五太子 政史[†1]　辻井 重男[†1]

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共に，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，個人のプライバシー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やウイルスチェック等の内容検査の困難さなど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．

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，安心・安全電子メール利用基盤，SSMAX，認証，暗号，組織暗号，　楕円エルガマル暗号

Secure and Safe E-mail Exchange Framework(SSMAX)

Toshiaki Saisho[†1]　Masahito Gotaishi[†1]　Shigeo Tsujii[†1]

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.

Keywords: Targeted-attack-mail, Phishing-email, Slander-e-mails, Intimidation- e-mails,
SSMAX, Secure-and-Safe-E-mail-Exchange-Framework, Authentication, Encryption, Cryptosystems-for-social-organizations

1. はじめに

インターネットの歴史と共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%などが主要なものであり，LINE19.42%，Facebook10.06%など，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，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必定である．「安心・安全電子メール利用基盤（SSMAX）」は，メールシステムの安全性を更に高め，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，我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．

2. サイバー攻撃に悪用されない電子メール利用基盤を目指して

メールは，組織や国民の活動で最も良く利用されているコミュニケーション手段であり，それが故に，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取り，送信者・送信組織の名前やメールアドレス，更にメール内容を，受信者にとっての信憑性の度合いを高めた上で，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

†1　中央大学研究開発機構
Research and Development Initiative, Chuo University

クへの侵入手段としては，業務上のメールのやりとりが多い組織間の通信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たメール（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「安心・安全電子メール利用基盤（SSMAX)」(以下，単に SSMAX と略記）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（サイバー攻撃）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り，更にメールに含まれる個人情報や秘密情報の漏洩を防止できる仕組みの導入により組織や個人の緊密で活発なコミュニケーションに利用可能な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，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および送信内容の非改ざん性の検証を実施する．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/ISP（インターネット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/ISP 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/ISP 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/ISP 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/ISP に送信する．

③受信組織/ISP のメールサーバは，送信組織/ISP の署名検証により，送信者の認証を実施した送信組織/ISP 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/ISP のメールサーバが送信組織/ISP 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/ISP の署名は受信組織/ISP の署名に付け替えられ，受信者へ送信する．

④受信者は，受信組織/ISP の署名検証により，送信者の認証を実施した送信組織/ISP を更に認証した受信組織/ISP 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/ISP 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（図１）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．

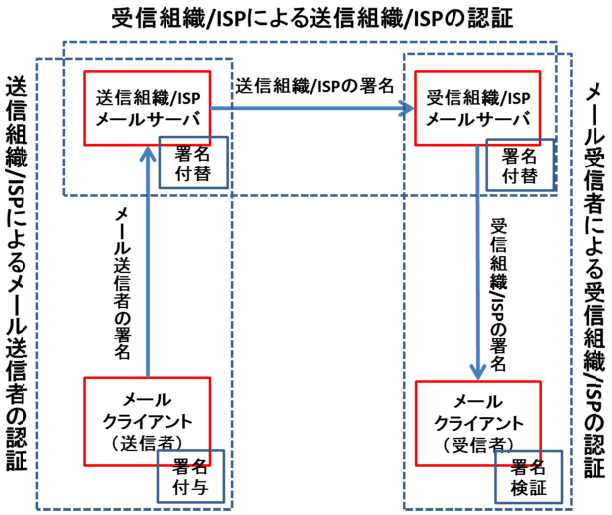

図１　認証の連鎖

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．

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横行は，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横行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，一定レベル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 SSMAX を目指している．

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/ISP 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/ISP がメール利用者を登録する際，組織/ISP 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ー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．その上で，組織/ISP 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．マイナンバー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/ISP 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マイナンバー制度を利用し，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/ISP が一定の役割を果たすことを想定している．組織/ISP が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，また，メールアドレス証明書内の所有者名としても，マイナンバー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，一定レベルの匿名性を実現することができる．

SSMAX にて，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/ISP へ連絡する．連絡を受けた受信組織/ISP は，受信したメールに付与された署名により送信組織/ISP を特定し対応を要請する．要請を受けた送信組織/ISP は，その組織/ISP のポリシーに準じ，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/ISP 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ーとの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，マイナンバーまで特定できる．更に必要があれば地方公共団体情報システム機構（JLIS）への問い合わせにより 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ーや 4 情報まで確認の上，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，ガイドラインなどが必要となろう．

SSMAX では，以上のような方法により，メール送信者の一定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想定している．なお，SSMAX で想定している匿名性の安全性については，本稿の最後に補足説明を付記している．

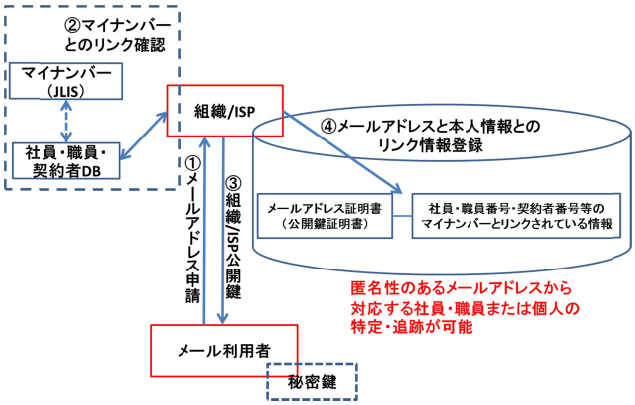

図 2　組織/ISP におけるメール利用者登録

なお，SSMAX ではメール送信者の特定・追跡性をマイナンバー制度の利用により実現するが，日本に限らず多くの国ではマイナンバー制度に類似した国民 ID 制度を導入しており，各国独自の国民 ID 制度を利用することにより SSMAX と同様のメール送信者の特定・追跡性の実現が可能であろう．

3. 情報漏洩を防止できる電子メール利用基盤を目指して

高度情報化時代，メールが今後も基礎的・共通的コミュニケーション基盤としての役割を果たすのは必定である．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ー情報のやり取りも多くなり，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取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メールには，暗号技術を活用した個人のプライバシー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など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踏まえ，「安心・安全電子メール利用基盤（SSMAX）」では，秘密情報の保護のみならず，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，メール送信者の認証および送信内容の非改ざん性の検証に使用する楕円エルガマル暗号をメール内容の秘匿にも利用する．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の流入の防止を両立可能な仕組みを，次のステップで実現する．

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 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無いことを確認後，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 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．

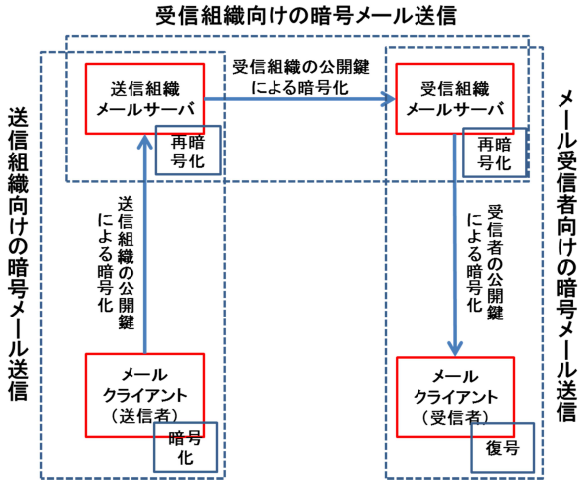

図 3　暗号化の連鎖

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よう暗号化された情報を，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された情報への変換）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ことを想定している．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]～[6]）．

SSMAX で想定している再暗号化の具体的手順を，特定の秘密鍵 a でしか復号できない暗号化情報 C_A を，異なる秘密鍵 b でしか復号できない暗号化情報 C_B への変換（再暗号化）を例に，図 4 に示す．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無いので，メールサーバおよび鍵管理サーバをそれぞれ独立した（結託の無い）管理主体が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．

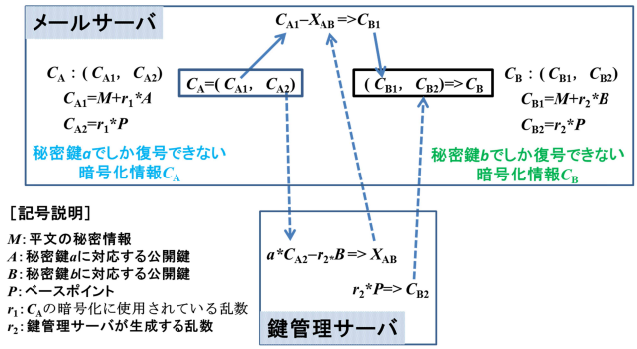

図 4　再暗号化手順

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，一旦復号した上での検査が必要である．そこで，SSMAX では，安全な環境での復号および検査を可能とする検査サーバを利用することとし，また鍵管理サーバで管理している復号に使用する秘密鍵を検査サーバへ開示することなく復号を可能とする仕組みにより，復号に使用する秘密鍵（送信組織の秘密鍵）の安全性を高めている．

送信組織側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無いかどうかなど，送信組織のポリシー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，送信組織のポリシー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．

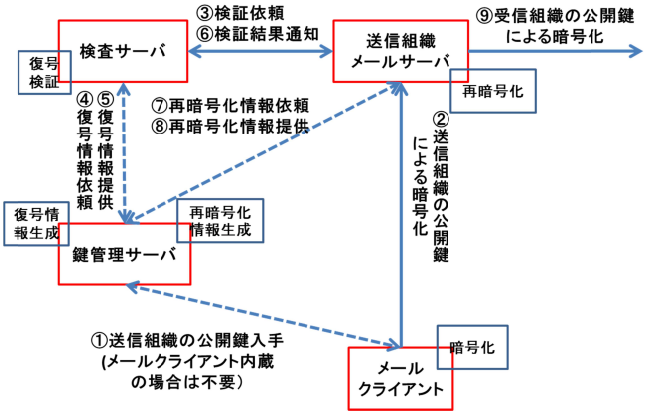

図 5　送信組織における情報漏洩検知・防止方式

さて，このように検査サーバでは鍵管理サーバの支援を受け，送信組織向けに暗号化されたメールを一旦復号する必要がある．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．具体的には図 6 に示す手順で，検査サーバは送信組織の公開鍵で暗号化された秘密情報 C_A を復号することが可能である．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無いので，検査サーバおよび鍵管理サーバをそれぞれ独立した（結託の無い）管理主体が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．

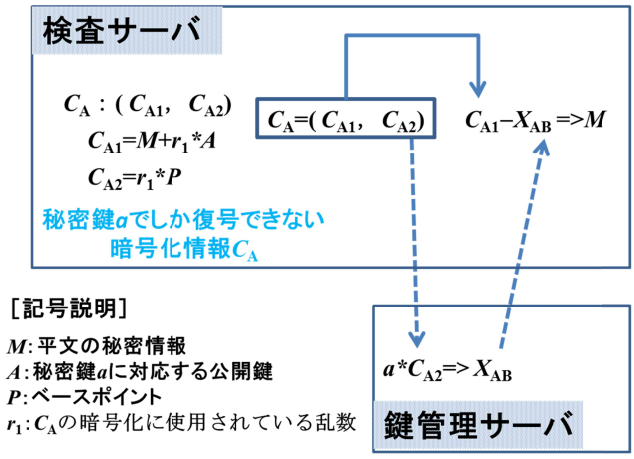

図 6　復号手順

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，一旦復号した上での検査が必要である．そこで，SSMAX では，安全な環境での復号および検査を可能とする検査サーバを利用することとし，また鍵管理サーバで管理している復号に使用する秘密鍵を検査サーバへ開示することなく復号を可能とする仕組みにより，復号に使用する秘密鍵（送信組織の秘密鍵）の安全性を高めている．

受信組織側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など，受信組織のポリシー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，受信組織のポリシー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など）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．

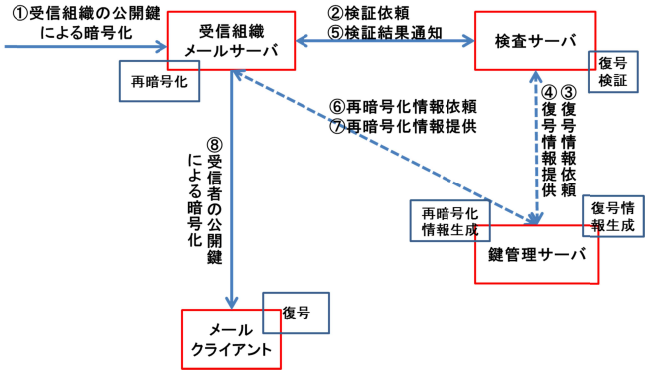

図 7　受信組織における悪意のある情報の流入防止方式

さて，このように検査サーバでは鍵管理サーバの支援を受け，受信組織向けに暗号化されたメールを一旦復号する必要がある．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 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，組織暗号の特性を活かし，鍵管理サーバが受信組織の秘密鍵を検査サーバに開示することなく復号を実施できるため，受信組織の秘密鍵の安全性を高める効果と共に，検査サーバおよび鍵管理サーバはそれぞれ単独では暗号化された秘密情報を復号できず，秘密情報の安全性を高める効果が期待できる．もちろん，検査サーバおよび鍵管理サーバをそれぞれ独立した（結託の無い）管理主体が運用することが，その前提である．

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．

その前提として，SSMAX では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ているものとし,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,という運用を想定している.メール受信者は,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,メール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,メール受信者の秘密鍵による署名を付与した上で，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上で，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無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属さない個人の場合のメール内容の秘匿方式

SSMAX では，メール送信者が個人の場合，その個人が所属する送信 ISP のメールサーバでは，個人のプライバシー情報保護のため，暗号化されたメールの検査は行ず，またメール受信者が個人の場合，同様にメール受信者が所属する受信 ISP では，個人のプライバシー情報保護のため，暗号化されたメールの検査は行わない．但し，メール利用者個人の同意（希望）があれば，メール送信時の検査（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)，メール受信時の検査（ウイルスなどの悪意の秘められたメールではないかどうか等）が，暗号化されたメールに対しても実施可能な構成を想定している．

4.　鍵ペアの生成・管理およびメールアドレス証明書/公開鍵証明書の発行・管理

「安心・安全電子メール利用基盤（SSMAX)」の全体像は以下の通りである．

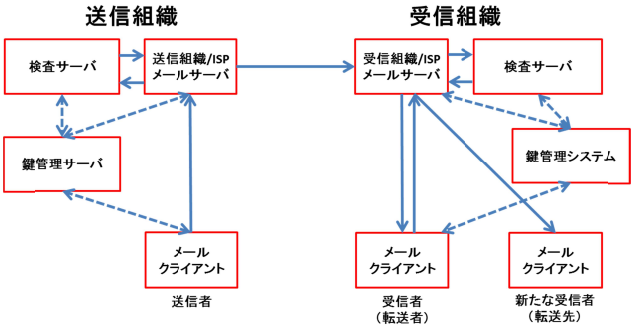

図 8　SSMAX 全体像

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/ISP，受信組織/ISP 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 章にて記載している通り、組織/ISP 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/ISP 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。

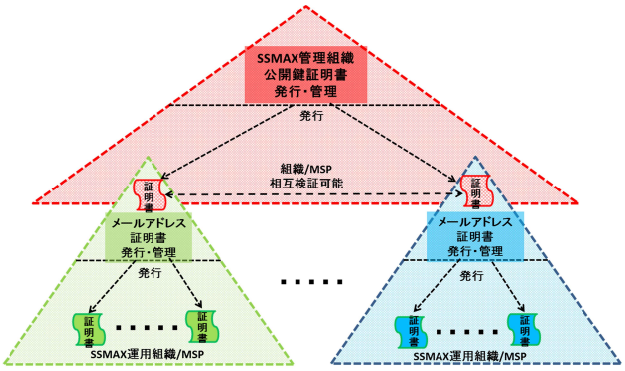

図 9　SSMAX における PKI の階層

SSMAX を構成するメール利用者、組織/ISP、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/ISP 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ー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、マイナンバーとのリンクが確認されている ISP との契約番号の提示を想定しているが、マイナンバー（マイナンバーカード）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/ISP 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/ISP 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 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/ISP］

組織/ISP 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/ISP 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ーとリンクされた情報の組合せを鍵管理サーバにて管理する.

組織/ISP 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・公開鍵証明書の他，所属する組織/ISP の公開鍵証明書を管理する.

組織/ISP 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全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構わない．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.

［SSMAX 管理組織］

SSMAX 管理組織は，SSMAX を運用する組織/ISP に対し SSMAX の運用状況を確認し，組織/ISP 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/ISP の実在性を審査の上で発行される 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、代替はできない。

組織/ISP 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/ISP が通信相手の組織/ISP 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/ISP かどうかの判定基準」は，関係機関の合意を得た上で具体的かつ明確に規定しておく必要がある．また，その判定は定期的に更新される必要があり，更新に値する組織/ISP かどうかの判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/ISP 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，情報セキュリティ監査の結果等を参考に、判断することになろう。

5.　おわりに

「安心・安全電子メール利用基盤（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（サイバー攻撃）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り，更にメールに含まれる個人情報や秘密情報の漏洩を防止できる仕組みの導入により組織や個人の緊密で活発なコミュニケーションに利用可能な電子メール利用基盤を目指したものである.

本稿では，SSMAX を構成する技術・管理の枠組について紹介した．我々は今後，SSMAX の社会実装に向け，関係機関・専門家のご理解・ご協力が得られるよう，また国民的コンセンサスが得られるよう，紹介活動を展開する予定である.

参考文献

[1]“ビジネスメール実態調査 2017 http://www.sc-p.jp/news/pdf/170602PR.pdf (参照 2017-07-31).

[2]“国内標的型サイバー攻撃分析レポート 2017 年版“. トレンドマイクロ(株). 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.

[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 56 巻 9 月号.

[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―”. 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―”. https://c-faculty.chuo-u.ac.jp/~tsujii/_userdata/my_number.pdf (参照 2016-07-14)

[7] 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.

[8] 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.

[9] 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.