SCIS 2017 2017 Symposium on
Cryptography and Information Security
Naha, Japan, Jan. 24- 27, 2017
The Institute of Electronics,
Information and Communication Engineers

「安心・安全電子メール利用基盤（SSMAX）」構想
Safe and Secure E-mail Exchange Framework(SSMAX)

才所 敏明* 五太子 政史* 辻井 重男*
Toshiaki Saisho Masahito Gotaishi Shigeo Tsujii

あらまし 基礎的・共通的コミュニケーション基盤として利用されているインターネットメールは、標的型攻撃メール、フィッシングメールなど、さまざまの悪用に晒され、その信頼性が揺らいでいる。本稿では、メールの悪用の手口を整理し、そのような悪用を許してしまう現在の電子メール利用基盤の脆弱性を分析、脆弱性を悪用する悪意のあるメールによる攻撃への効果的な対策を考察する。更に、暗号化によるメール内容の保護とメールによる情報の不正持出検出やメール内のマルウェア検出が可能な対策を検討、その実現のための暗号技術利用方式を考察する。以上の考察・対策検討の結果を踏まえ、我が国の今後の産業活動の活発化・発展、国民一人一人の社会活動の促進を支えることが期待できる、現在の電子メール利用基盤の脆弱性の克服を目指した「安心・安全電子メール利用基盤（SSMAX）」を提案する。

キーワード 標的型攻撃メール、フィッシングメール、電子メール利用基盤、SPF、DKIM、S/MIME、組織暗号、SSMAX、Safe-and-Secure-Email-Exchange-Framework

1 電子メール利用の現状

インターネットメール（以降、電子メールあるいは単にメールと表記）は、インターネットの歴史の当初から利用され現在に至っている。我が国でも約 30 年の歴史がある。

技術進歩の激しいICT、新たなコミュニケーションツールが数多く出現し、多くの方々がそれぞれの特徴を活かし利用している。しかし、現状でも約 30 年の歴史があるメールが最も多くの利用者を抱えており、依然として基礎的・共通的コミュニケーション基盤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 2016」（[1]）によると，ビジネスマンの業務上の通信手段は，メール 98.22%，電話 91.06%，会う 75.97%などが主要なものであり，LINE15.93%，Facebook10.01%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．個人通信の場合は、若干事情は異なると思われるが、それでも新たなコミュニケーション手段がメールに変わって基礎的・共通的コミュニケーション基盤の地位を得ることは考えにくい。業務通信・個人通信を問わず、メールが基礎的・共通的コミュニケーション基盤であることは間違いない。

一方、メールが高度情報化社会の基礎的・共通的コミュニケーション基盤であるがゆえに、攻撃者にとっても格好の攻撃ツールとして利用されることになる。組織を攻撃対象とし業務通信をなりすました標的型攻撃メール、個人を攻撃対象とし信頼できる組織をなりすましたフィッシングメールなど悪意のあるメールの氾濫は周知の通りである。もちろん我が国でもこのような悪意のあるメールへの人的対策、技術的対策が推進されてはいるが、減少の傾向は見えない。標的型攻撃メールやフィッシングメールなどの悪意のあるメールの氾濫は、基礎的・共通的コミュニケーション基盤としてのメールへの信頼性を揺るがせているのも事実である。

我が国の高度情報化社会の基礎的・共通的コミュニケーション基盤としてのメールへの信頼性の低下は、それを活用して展開される組織の業務活動や個人の社会活動の効率を大きく低下させ、我が国の産業活動や個人の社会的・文化的活動を停滞させかねない大きな問題である。

*中央大学研究開発機構，〒112-8551 東京都文京区春日 1-13-27,
Research & Development Initiative, Chuo University,
1-13-27,Kasuga, Bunkyo-ku, Tokyo 112-8551, Japan

2　「悪意のあるメール」の分類

悪意のあるメールの送付は、図１に示すように、使用される送信メールアドレスにより三つのパターンに分類される。

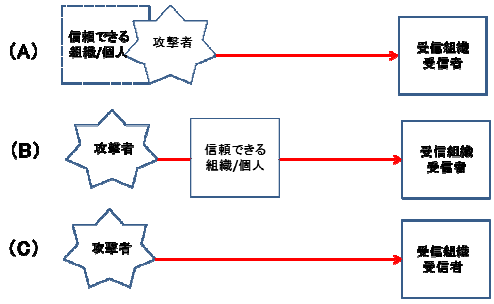

図１．悪意のあるメール送付のパターン

（A）は、送信組織のドメインや送信者のメールアカウントは使用しないが、送信組織の推定に使用されるメールアドレスのドメインや送信者の推定に使用されるメールアカウントを詐称し、あるいは酷似するドメイン、メールアカウントを使用し、信頼できる送信組織/送信者からのメールであるように思わせ、不信感を持たせずメールを処理させる、という手口の悪意のあるメールである。

（B）は、受信組織/受信者が信頼する送信組織のメールサーバを不正に利用し、あるいは信頼する送信者のメールアカウントを不正に利用し悪意のあるメールを送付することにより、信頼できるメールであるように思わせ、不信感を持たせずメールを処理させる、という手口の悪意のあるメールである。

（C）は、送信メールアドレスから推定できる送信組織/送信者に心当たりが無い、受信組織/受信者にとっては信頼できるかどうかわからない未知の送信組織/送信者からのメールである。送信メールアドレスにより受信組織/受信者の信頼感を得る代わりに、送信者の名前やメールのタイトル・本文の内容で、受信組織/受信者を信頼させる、興味を持たせる、あるいは緊急対応が必要と思わせる脅しの文言により即時メール対応へ駆り立てる、という手口の悪意のあるメールである。

3　「悪意のあるメール」対策

3.1　（A）パターン対策

このパターンの送信メールアドレス詐称メールの特徴は、送信メールアドレスに示された組織のメールサーバから送信されていないこと、送信メールアドレスに示されたメールアカウントから送信されていないこと、である。

送信メールアドレスに示された組織のメールサーバから送信されていないこと（送信組織の詐称）は、現在、推奨されている技術対策である、SPF（Sender Policy Framework [9]）およびDKIM（DomainKeys Identified Mail [10]）にて検知可能である。しかし、送信メールアドレスに示されたメールアカウントから送信されていないこと（メールアカウントの詐称）は、SPFおよびDKIMでは検知できない。

（A）パターンの悪意のあるメールの検知対策としては、S/MIME（Secure/Multipurpose Internet Mail Extensions [11]）では提供されている機能であるが、送信メールアドレス全体の正当性を確認できる**「送信メールアドレスの認証」**機能が必要であり、この機能により送信メールアドレスの、ドメイン、メールアカウントあるいは両方の詐称を検知し排除できる。

送信メールアドレス酷似メールに対しては、一般に上述の詐称メール対策は有効では無い。悪意のあるメール送信者が自らが酷似ドメインを立ち上げ、任意にメールアカウントを登録できるため、SPF、DKIM、またS/MIMEも酷似メールを検知できない。対策としては、ドメインが酷似しているが本来の信頼できる送信組織のドメインと異なることを自動的に確認できることが必要であり、このことは後述する**「送信組織の信頼性」**確認機能を利用し検出可能である。

3.2　（B）パターン対策

このパターンのメールは、「送信メールアドレスの認証」機能だけでは検知できない。送信組織のメールサーバや送信者のメールアカウントが不正利用され悪意のあるメールを送信された場合、受信組織/受信者では現在提案されている技術対策では受信組織/受信者は検知できず、適切な対応ができない。

このパターンの悪意のあるメールを許してしまうのは、送信者が送信組織の一員であるかどうか、送信者が本人かどうかの、送信組織の確認が不十分な場合である。

対策としては、まずは送信組織における厳密な**「送信者の本人確認」**機能が必要である。次に、受信組織/受信者が、受信メールが悪意のあるメールであるリスクの大きさを判断できるためには、送信組織が厳密な「送信者の本人確認」を行っている信頼できる組織であることを確認できる**「送信組織の信頼性」**確認機能、あるいは個々の受信メールごとにどのような「送信者の本人確認」を行ったかどうかを確認できる**「送信者の本人確認方法の通知」**機能、が必要である。

このような機能により、受信組織/受信者は受信メールが悪意のあるメールであるリスクの大きさを判断でき、ポリシーに応じ対応できる。

3.3　（C）パターン対策

このパターンのメールも、「送信メールアドレスの認証」機能だけでは検知できない。悪意のある送信組織/送信者の場合や送信組織のメールサーバあるいは送信者のメールアカウントが不正利用された場合、現在提案されている技術対策では受信組織/受信者は検知できず、適切な対応

ができない。

対策としては、まずは（B）と同様、送信組織における厳密な**「送信者の本人確認」**機能が必要である。次に、厳密に本人確認を実施していることを含め、信頼できる送信組織であることを、受信組織/受信者が何らかの方法で確認する仕組み**「送信組織の信頼性確認」**機能が必要である。

このような対策により、信頼できるかどうかわからない未知の送信組織/送信者からのメールであっても、受信組織/受信者は受信メールが悪意のあるメールであるリスクの大きさを判断でき、ポリシーに応じ対応できる。

4　対策を実現する四つの仕組み

前節の対策の整理から、受信組織/受信者が悪意のあるメールを誤って受け入れてしまうリスクを下げるには、次の三つの仕組みが必要であることがわかる。

①「送信メールアドレスの認証」に関する仕組み
②確実な「送信者の本人確認」に関する仕組み
③「送信組織の信頼性」確認に関する仕組み

さて、このような対策により、たとえ悪意のあるメールが氾濫している状況下でも、受信組織/受信者の被害の大幅な減少が期待できる。

しかし、我が国の産業活動や個人の社会的・文化的活動の基礎的・共通的コミュニケーション基盤であるメールに対しては、悪意のあるメールそのものの流通を許さない、悪意のあるメールの大幅な減少に向けた、より積極的な対策が必要である。そのためには、悪意のあるメールを野放しにせず、送信者を特定・追跡し、責任を追及する、というような悪意のあるメールの送信源を除去する仕組みが必要であり、実現できれば現在の悪意のあるメール氾濫を解消あるいは大幅に減少できる可能性がある。「悪意のあるメール対策」としては、次の四つ目の仕組みが大変重要である。

④「送信者の特定・追跡性」に関する仕組み

我々が提案する「安心・安全電子メール利用基盤（SSMAX）」では、以上の四つの仕組みの実装を予定している。個々の仕組みの内容・実装方法について以下具体的に示す。

4.1　送信メールアドレスの認証

SSMAX では、S/MIME と同様の送信メールアドレスの認証機能を有する。S/MIME との違いは、S/MIME では受信者がメールアカウント所有者により送信されたメールかどうかの確認を行う方式であるのに対し、SSMAX では送信組織、受信組織、受信者が連携し、メールアカウント所有者が送信したメールかどうか、送信組織のメールサーバから送信されたメールかどうかを確認する方式を採用している点である。

SSMAX での送信メールアドレスの認証手順は以下の通り。

①送信者は、送信メールアドレスに対応した秘密鍵により送信メールに署名を付与し、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、送信メールに付与された署名の検証により、送信メールアドレスを認証する。送信メールサーバは送信メールアドレス認証後、送信組織の秘密鍵により送信メールへ署名を付与し、受信組織のメールサーバへ送信する。

③受信組織のメールサーバは、送信組織の署名を検証後、特定した送信組織が送信メールアドレスの認証を行っている信頼できる組織かどうかを確認する。受信組織は、信頼できる送信組織であることを確認後、受信組織の秘密鍵により受信メールへ署名を付与し、受信者へ送信する。

④受信者は、受信組織の署名を確認し、信頼できる（受信者が属する）受信組織かどうかを確認の上、メールを処理する。

以上の手順により、受信者は受信メールの送信メールアドレスが認証されていることを確認できる。

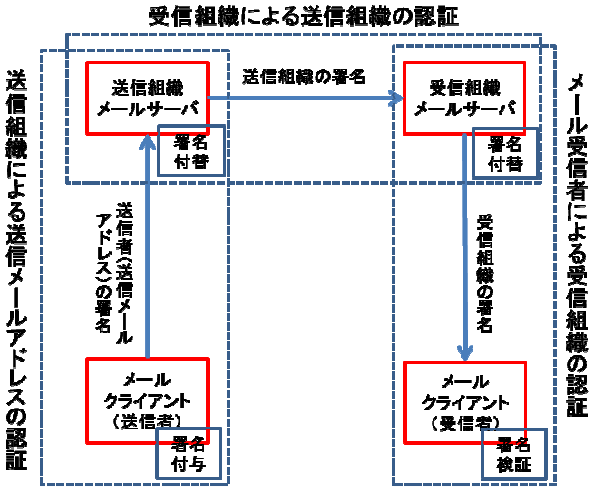

図２．認証の連鎖による送信メールアドレスの認証

4.2　送信者の本人確認

4.1 で述べた仕組みによる送信メールアドレスの認証が、正当な送信者（送信メールアドレスの正当な所有者）による送信メールであることを示しているわけではない。悪意のある第３者による送信組織のメールサーバや送信者のメールアカウントの不正利用によりメールが送信される危険性もある。そのため、送信者の確実な本人確認が必要である。

SSMAX では、組織がメール利用者（送信者/受信者）を登録する際、社員・職員カードや個人の場合はマイナンバーカードを提示させ、しっかりとした本人確認を行い、メールアドレス証明書を発行する。メールアドレス証明書内の公開鍵に対応する秘密鍵は、社員・職員カード・マイナンバーカード、あるいは同等の耐タンパー性のあるリムーバブルデバイスへの格納を想定している。

メール送信時の送信者の本人の確認は、社員・職員カード・マイナンバーカードや所定のリムーバブルデバイスを保有していることによる（所有物による）本人確認、およ

び社員・職員カード・マイナンバーカードやリムーバブルデバイスのアクセスのためのパスワードを知っていることによる（記憶による）本人確認の、2-way 認証を想定している。

送信メールアドレスの認証のための署名作成処理は、耐タンパー性のある社員・職員カード・マイナンバーカードやリムーバブルデバイス内で実施されることを想定しており、秘密鍵がクライアント PC をはじめ外部には一切開示されない運用を想定している。

以上のようなメール送信者がその送信メールアドレスの正当な所有者であることを送信組織が確認できる仕組みの運用を前提とすれば、4.1 で述べた送信メールアドレスの認証の仕組みとの組合せにより、受信者は受信したメールがメールアドレスの正当な所有者が送信したメールであることを確認できる。

なお、送信メールアドレスの正当な所有者かどうかの本人確認の仕組みは、SSMAX で想定している方式には拘らず、同程度の確実な本人確認方法による代替は可能とする。

4.3　送信者の特定・追跡性

4.1、4.2 の仕組みにより、受信者は受信メールが正しく送信メールアドレスが示す送信組織のメールサーバ、メールアカウントから送信されたこと、および送信メールアドレスの正当な所有者が送信したことが確認できる。しかし、もし受信したメールに悪意が含まれていたことが分かった場合は、4.1、4.2 の仕組みだけでは、メールアドレスの所有者の特定・追跡に必要な名前、住所等の情報が確認できる保証は無い。

悪意のあるメールの氾濫を防ぐには、悪意のあるメールの送信メールアドレスの所有者を特定・追跡し、原因追究と是正措置による再発防止を要求する必要があり、そのためには送信者を特定・追跡できる、名前、住所等の情報の確保が不可欠である。

SSMAX では、メールアドレス所有者の特定・追跡に必要な情報の確認は、メールアドレスを発行する組織が責任を持って行うことを想定している。

4.2 で述べたように、組織がメール利用者を登録する場合、本人確認のため社員・職員カードや個人の場合はマイナンバーカードを提示させるが、その際に、マイナンバーと何らかの形でリンクしている社員・職員番号等とメールアドレス証明書との対応情報を保管・管理することとしている。万一、組織内の送信者の送信メールが悪意のあるメールと判断された場合、そのメールの送信者を特定・追跡でき、原因追究と是正措置の指示・確認が可能となる。なお、意図的に悪意のあるメールを送信した場合、組織は懲戒免職等の措置も可能となるし、万一、犯罪に絡むメールの場合は必要に応じ捜査協力も可能となる。

個人の場合は組織の役割を果たす ESP（E-mail Service Provider）が、マイナンバーと何らかの形でリンクしている契約者・利用者番号等とメールアドレス証明書との対応情報を保管・管理することとしている。万一、組織内の送信者の送信メールが悪意のあるメールと判断された場合、そのメールの送信者を特定・追跡でき、原因追究と是正措置の指示・確認が可能となる。なお、意図的に悪意のあるメールを送信した場合、ESP は契約解除等の措置も可能となるし、万一、犯罪に絡むメールの場合は必要に応じ捜査協力も可能となる。

このような送信者の特定・追跡性の確保により、悪意のあるメールの氾濫を解消できるものと期待している。

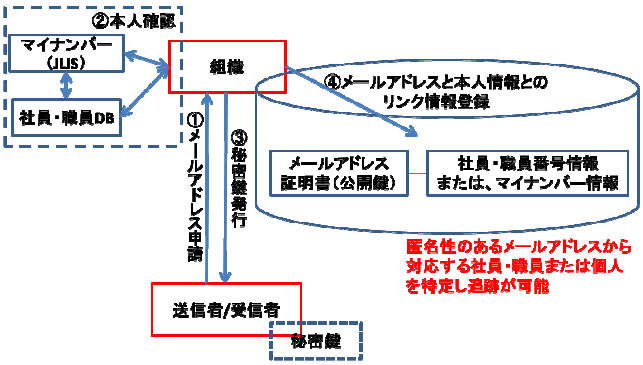

図３．メールアドレス証明書と本人情報のリンク

4.4　送信組織の信頼性

4.1～4.3 の仕組みにより、送信メールアドレスの正当性の確認、送信者の正当性の確認、送信者の特定・追跡が可能となる。しかし、これらの仕組みが正しく機能するには、送信組織が SSMAX 仕様の役割・責任を確実に遂行する必要があり、メール受信者が受信したメールを安心して処理できるかどうかは送信組織の信頼性に大きく依存する。

我々が提案する「安心・安全電子メール利用基盤（SSMAX）」では、SSMAX で規定している仕組みを確実に安全に遂行している組織を確認し、組織向けに公開鍵証明書を発行する管理組織の存在を想定している。受信組織は、SSMAX の管理組織から発行された公開鍵証明書を保有している送信組織かどうかで、SSMAX 仕様の役割・責任を確実に遂行する信頼に足る組織かどうかの判断が可能となる。

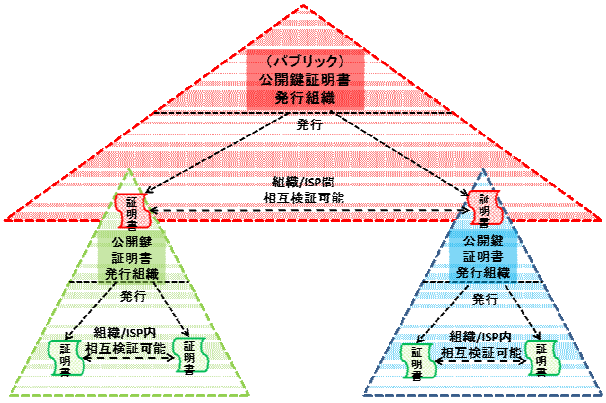

図４．PKI の階層・連携

5　「送信メールの改ざん・情報漏洩」対策

「悪意のあるメール」の氾濫は、4 節で述べた対策により、かなり改善されることが期待されるが、送信者のメール内容の改ざんや盗聴の対策も必要である。基礎的・共通的コミュニケーション基盤として今後も活用されるメールには、組織の機密情報や個人のプライバシ情報などを含めての自由なコミュニケーションへの期待も大きく、改ざんや盗聴への対策はますます重要となる。

メール内容の改ざんについては、4.1 で述べた送信メールへの署名の連鎖（認証の連鎖）により、同時に検知可能であり、改ざんメールを鵜呑みにすることによる被害は回避可能である。

メール内容の盗聴については、別途の対策が必要である。一般に情報の保護には暗号技術が利用される。我々が提案する「安心・安全電子メール利用基盤（SSMAX）」においても、暗号技術を利用する。ただし、暗号技術の利用には注意を要する。一般に受信組織では、受信メールのマルウェア等の悪意が仕込まれていないことを確認の上、組織内の受信者へ送信する。暗号化されたメールにおいても、このような検査機能を通過せずの組織内送信は許されない。また、一般に送信組織では、送信メールに組織の機密情報が含まれていないことを確認の上、受信組織へ送信する。暗号化されたメールにおいてもこのような検査機能を通過せずの組織外送信は許されない。

IETF にて標準化されている S/MIME は暗号化機能を有しているが、End-to-End の暗号化方式で、送信組織/受信組織でのセキュリティ検査機能の障害となり、S/MIME の組織での導入・活用は難しい。

SSMAX では、送信組織が外部へメールを送信する際、および受信組織が外部からメールを受信した際、暗号化されていても、一旦復号し、平文メールと同様の検査を受けさせ、その上で送信/受信の判断を可能とする方式を想定している。

具体的には、次のような暗号化/復号の手順により、受信者への安全な到達を実現している。

①送信者は送信組織の公開鍵により暗号化し、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、検査サーバへ送信メールに組織の機密情報が含まれていないかどうかの確認を依頼する。検査サーバは、鍵管理サーバの支援を受け送信メールを復号し検査を実施、検査結果を送信組織のメールサーバへ連絡する。検査の結果、送信メールに組織の機密情報が含まれていない場合、送信組織のメールサーバは鍵管理サーバの支援を受け、受信組織の公開鍵で暗号化されたメールへ変換し、受信組織のメールサーバへ送信する。

③受信組織のメールサーバは、検査サーバへ受信メールにマルウェア等の悪意が仕込まれていないかどうかの検査を依頼する。検査サーバは、鍵管理サーバの支援を受け受信メールを復号し検査を実施、検査結果を受信組織のメールサーバへ連絡する。検査の結果、マルウェア等の悪意が仕込まれていない場合は、受信組織のメールサーバは鍵管理サーバの支援を受け受信者の公開鍵で暗号化されたメールへ変換し、受信者へ送信する。

④受信者は、自身の秘密鍵により受信メールを復号し処理する。

このような暗号化の連鎖により、送信組織、受信組織での検査時には一旦復号されるが、それ以外では送信メールは暗号化されており、送信メールの情報保護と送信組織/受信組織での検査可能性を両立できる。

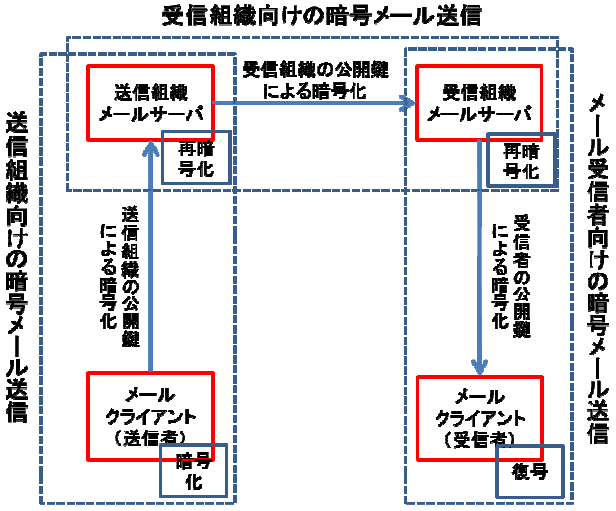

図５．暗号化の連鎖による情報漏洩防止と
秘密情報不正流出・マルウェア流入防止の両立

なお、送信者/受信者が個人の場合、SSMAX における組織の役割は ESP が担当するが、送信組織/受信組織における復号しての検査は、個人のプライバシ保護の観点から行わないことを想定している。

6　安心・安全電子メール利用基盤（SSMAX）

4 節、5 節の仕組みを組み込んだ、我々が提案する「安心・安全な電子メール利用基盤（SSMAX）」の全体像を図６に示す。

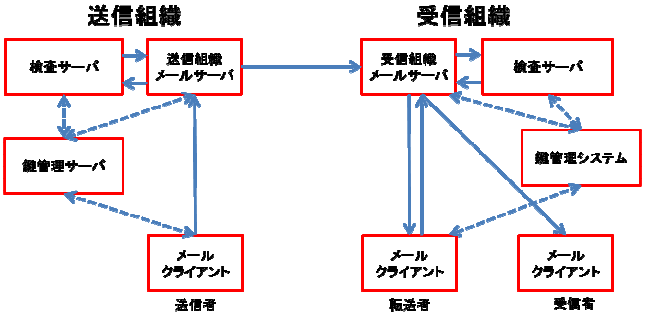

図６．SSMAX 全体構成

以下、想定している SSMAX の利用・運用手順を説明する。

(1)組織（送信組織/受信組織）の登録手続き

SSMAX へ参加を希望する組織は、SSMAX 運用基準を遵守していることを、SSMAX 管理組織の確認のもと、SSMAX 準拠組織として（グローバルな）公開鍵証明書の交付を受ける。

(2)メール利用者の登録手続き

組織が組織内のメール利用者（送信者/受信者）の登録を担当する。

登録においては、まずマイナンバーとリンクしている社員・職員カードや個人の場合はマイナンバーカードにより確実な本人確認、本人の特定・追跡性の確認を行うこととする。その上で、メールアドレスの登録およびメールアドレスと対応する公開鍵に対し（プライベートな）メールアドレス証明書を発行する。

メールアドレス証明書の公開鍵に対応する秘密鍵は、組織の公開鍵証明書と共に、メール利用者の社員・職員カードやマイナンバーカードあるいは同等の耐タンパー性を有するリムーバブルデバイスに格納するものとする。

組織は、発行したメールアドレス証明書と本人の特定・追跡が可能なマイナンバーを確認できる社員・職員番号や契約者・利用者番号と関連付け、管理するものとする。

(3)メール送信者の送信処理

保護すべき送信情報は関連する情報ごとにファイルにまとめ、送信組織の公開鍵により暗号化を実施し、メールに添付する。また、メール本文に暗号化した添付ファイルの内容説明をメール本文に記載する。

次に、メール全体に対し、送信者の秘密鍵を利用し署名を付与し、送信組織のメールサーバへ送信する。

(4)送信組織メールサーバの受信処理

送信者からのメールに対し、送信メールアドレスに対応する公開鍵証明書を利用し署名を検証する。署名検証に成功後、検査サーバへメールを送信し、検査を依頼する。なお、送信者が個人の場合は、メール内容の検査は行わないことを想定している。

(5)送信組織検査サーバの検査処理

検査対象のメールに組織の秘密情報が不正に含まれていないかどうか検査する。暗号化された添付ファイルの場合は、鍵管理サーバの支援を受け復号の上、検査を実施する。検査の結果をメールサーバへ伝える。

(6)送信組織メールサーバの送信処理

検査の結果、問題の無いメールの場合は、送信組織の公開鍵で暗号化されている添付ファイルを、すべて受信組織の公開鍵で暗号化されている添付ファイルへ変換（再暗号化）する。再暗号化は、鍵管理サーバの支援を受け実施する。

最後に、メール全体に対し、送信組織の秘密鍵による署名を付与し、受信組織のメールサーバへ送信する。

(7)受信組織メールサーバの受信処理

受信したメールに対し、SSMAX 管理組織から入手できる送信組織の公開鍵証明書を利用し署名を検証する。署名検証に成功後、検査サーバへメールを送信し、検査を依頼する。なお、受信者が個人の場合（受信組織が ESP の場合）は、メール内容の検査は行わないことを想定している。

(8)受信組織検査サーバの検査処理

検査対象のメールにマルウェア等の悪意が仕込まれていないかどうか検査する。暗号化された添付ファイルの場合は、鍵管理サーバの支援を受け復号の上、検査を実施する。検査の結果をメールサーバへ伝える。

(9)受信組織メールサーバの送信処理

検査の結果、問題の無いメールの場合は、受信組織の公開鍵で暗号化されている添付ファイルを、すべて受信者の公開鍵で暗号化されている添付ファイルへ変換（再暗号化）する。再暗号化は、鍵管理サーバの支援を受け実施する。

最後に、メール全体に対し、受信組織の秘密鍵による署名を付与し、受信者へ送信する。

(10)メール受信者の受信処理

受信組織のメールサーバからのメールに対し、受信組織の公開鍵証明書を利用し署名を検証する。署名検証成功後、自身の秘密鍵を使用し復号、メール処理を行う。

(11)メール受信者の転送処理

受信組織のメールサーバからのメールに対し、受信組織の公開鍵証明書を利用し署名を検証する。署名検証成功後、メール本文の内容を確認の上、転送先ごとに不要な添付ファイルを削除する。残された転送対象となる暗号化された添付ファイルは、受信組織の公開鍵で暗号化されたファイルへ変換し、全体に受信者の秘密鍵で署名を付与し、受信組織のメールサーバへ送信する。以降は、受信者が送信した新規のメールとして処理される。

(12)受信組織/受信者による悪意のあるメール受信処理

SSMAX の仕組みで悪意のあるメールのリスクが少ない送信組織/送信者からのメールであることを確認した上での受信であったとしても、送信組織の SSMAX 運用上の不備、送信者の悪意、あるいは送信者のクライアントの乗っ取り等による悪意のあるメールを受信するリスクは残る。

万一、受信組織/受信者が悪意のあるメールを受信した場合は、受信組織は SSMAX の管理組織へ連絡、送信組織には原因追究と是正措置を要請することになる。要請を受けた送信組織は自身の SSMAX 運用の確認・見直しや、必要があれば送信者を特定・追跡し原因追究と是正措置を要請する。万一、犯罪に絡むメールの場合は必要に応じ捜査への協力も可能である。

(13)組織の評価処理

SSMAX 参加組織の信頼性は、加入時に SSMAX 管理組織により評価され、その評価結果に応じ加入の是非が判断される。その後、SSMAX 運用開始後の悪意のあるメールの発生状況に応じ再評価される仕組みを想定している。

また、組織が SSMAX 運用基準に従った運用を実施し

ているかどうかの点も組織の情報セキュリティに関する監査項目に付加されることを想定、情報セキュリティ監査報告書の評価結果も、SSMAX 管理組織による組織の信頼性の再評価に活用されることを想定している。

このような組織の再評価の仕組みにより、SSMAX 参加組織の信頼性評価の確かさを高めていくことができる。

7　おわりに

本稿では、インターネットの歴史と共に活用されてきた電子メール（インターネットメール）における悪意のあるメールの氾濫の現状を憂慮し、その原因である電子メールの脆弱性を分析、脆弱性を悪用する攻撃への効果的な対策を考察の上、その対策を組み込んだ「安心・安全電子メール利用基盤（SSMAX）」を提案した。

電子メールシステムは多様なコミュニケーション手段が提供される現在においてもそして今後も、組織間の緊密な業務通信や個人の自由闊達な意見交換のための基礎的・共通的コミュニケーション基盤としての活用が期待されており、安定した「安心・安全電子メール利用基盤」の整備は、我が国の産業活動の活発化・発展、国民一人一人の社会活動の促進に大きく貢献するものと考えている。

また、本稿で述べた電子メールの脆弱性を悪用する攻撃への対策の基本的な考え方、あるレベルの匿名性は可能とするものの、情報送信・提供者の特定・追跡性の保証は、SNSやWebベースのコミュニケーション手段を悪用する攻撃に対しても有効であり、応用展開が可能と考える。

参考文献

[1] “ビジネスメール実態調査 2016” http://www.sc-p.jp/news/pdf/160701PR.pdf, (参照 2016-07-10).

[2] “国内標的型サイバー攻撃分析レポート 2016 年版“. トレンドマイクロ(株). http://www.trendmicro.co.jp/cloud-content/jp/pdfs/doc-dl/wp-apt2016-20160510.pdf, (参照 2016-07-09).

[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] “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）”. 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）”. http://www.nisc.go.jp/active/kihon/pdf/jseval_2013.pdf, (参照 2016-07-10).

[9] “Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1”. RFC7208. https://tools.ietf.org/html/rfc7208, (参照 2016-07-11).

[10] “DomainKeys Identified Mail (DKIM) Signatures”. RFC6376. https://tools.ietf.org/html/rfc6376, (参照 2016-07-11)

[11] “Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification”. RFC5751. https://tools.ietf.org/html/rfc5751 (参照 2016-07-12)

[12] “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”. http://www.soumu.go.jp/main_content/000227896.pdf (参照 2016-07-12).

[13] 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.

[14] 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.