標的型メール攻撃に対抗する「組織通信向け S/MIME」

才所 敏明[†1]　五太子 政史[†1]　辻井 重男[†1]

概要：
多発する標的型メール攻撃への効果的な対策となる「組織通信向け S/MIME」を提案する．
標的型メール攻撃は，組織間の通信を装った送信者なりすましメールによる攻撃が大半である．「組織通信向け S/MIME」構想では，組織通信における標的型メール攻撃のリスクを軽減させるため，S/MIME に準じた署名付与・検証機能を導入し，送信者の確実な認証を可能とする．更に，組織暗号を利用した暗号化機能を導入し，組織通信に求められる機密情報保護機能と暗号化通信における機密情報漏洩検知やウイルスチェックなどの検査・監査機能の両立を可能とする．
「組織通信向け S/MIME」は，個人間の通信も含めた我が国の「安心・安全な次世代電子メール利用基盤」の第一歩となることを目指し，策定中の構想である．

キーワード：標的型攻撃，標的型メール攻撃，S/MIME，組織通信，組織暗号，認証，暗号化，安心・安全な電子メール利用基盤

The proposal of new email system based on S/MIME concept for protecting the email between organizations from the targeted-email-attack

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

Abstract: We propose new email system based on S/MIME concept for protecting emails between organizations from targeted-email-attacks.
Most of targeted-attack-mails are pretending regular staff of organizations by using the mail address of regular staff. Our proposing system can authenticate the email sender by using digital signature similar to S/MIME and can detect the targeted-attack-mails which are pretending regular staff.
Furthermore, our proposing system provides the function of confidential-information-protection by utilizing our Organizational-Cryptosystem and also provides the check function of confidential-information-leakage and virus-infection.
We expect that our proposing system will become the foundation of safe-and-secure email infrastructure in the near future.

Keywords: targeted-attack, targeted-email-attack, S/MIME, organizational-communication, organizational-cryptography, Authentication, Encryption, Safe-and-Secure-Email-infrastructure

1. 標的型攻撃および標的型メール攻撃

標的型攻撃は，サイバー攻撃の一種である．サイバー攻撃は，不特定多数を対象とした攻撃と，特定の組織を対象とした攻撃に分類される．後者の，特定の組織を狙った攻撃が，標的型攻撃である．

昨今，多くの企業が標的型攻撃を受け，情報漏洩等の被害を受けている．昨年の日本年金機構の情報漏洩事件や今年の（株）ジェイティービー（JTB）の情報漏洩事件等，枚挙にいとまがない．情報処理推進機構（IPA）の資料「情報セキュリティ 10 大脅威 2016」([1]）では，2015 年において社会的影響が大きかったセキュリティ上の脅威のランキングで「標的型攻撃による情報漏洩」が 1 位（組織にとっての最大の脅威）に位置付けられている．

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

さて，標的型攻撃は，一般に次のステップで実施される．

(1)事前調査
不正侵入に有益な，攻撃対象とした組織やシステムの情報を調査する．

(2)不正侵入
事前調査で得た情報を利用し，攻撃対象組織の内部へウイルス等のマルウェアを送り込む．

(3)情報収集
侵入に成功したマルウェアが，攻撃対象組織のネットワーク内の情報を探索し収集する．

(4)情報送出
収集した情報を攻撃者へ届けるべく，組織外へ送出する．

このように標的型攻撃では，まずは攻撃対象組織に侵入する（マルウェアを送り込む）必要がある．その侵入方法としては，以下の方法が報告されている．

(1)メールを利用する方法

これがいわゆる標的型メール攻撃である．事前調査で入手した社員・職員の名前・メールアドレス，担当業務内容，メール通信相手などの情報を利用し，日常的にメールをやりとりしている通信相手になりすまし，マルウェアを仕込んだメールを受信させ感染させる方法．

送信者名・メールアドレスが業務上の通信相手になりすまされたメールや，担当業務内容に即したメール内容など，受信した社員・職員がなりすまされたメールであることを検知するのが難しいように工夫され，しかも利用されるマルウェアは未公開のものであり，一般のウイルスチェックソフトでは検出されないよう工夫されていることが多い（ゼロデイアタック）．

(2)Web 参照を利用する方法

いわゆる水飲み場攻撃である．攻撃対象の組織の社員・職員の業務内容から，攻撃対象の組織の社員・職員が利用している可能性の高い（外部の）Web サイトにマルウェアを仕込み，社員・職員がその Web を参照するときに，マルウェアを送り込み感染させる方法．攻撃対象の組織の社員・職員が参照する場合にのみ，マルウェアを送り込むなど，マルウェアの存在の発覚を遅らせるよう工夫されていることが多い．

(3)ソフトウェアの更新を利用する方法

攻撃対象の組織の社員・職員の業務内容から，利用している可能性の高いソフトウェアの更新情報をよそおい，マルウェアを送り込む方法．この場合も，攻撃対象の組織の社員・職員が参照する場合にのみ，マルウェアを送り込むなど，マルウェアの存在の発覚を遅らせるよう工夫されていることが多い．

このような侵入手法の中でも，メールを利用した侵入，つまり標的型攻撃メールによる侵入が非常に多いことが，各種調査機関より報告されている．例えば，トレンドマイクロ(株)の「国内標的型サイバー攻撃分析レポート 2016 年版」によると，2015 年に行った標的型サイバー攻撃の調査において，侵入のきっかけが標的型メールであると特定された事例が，全体の 93%，Web 経由が 7%，と報告されている（[2]）．

標的型攻撃対策としては，様々の対策が必要ではあるが，以上のように多くの標的型攻撃による被害が，標的型攻撃メールによる侵入に端を発していることを考慮すると，標的型メール攻撃対策の重要性は明らかであろう．

2. 標的型メール攻撃対策の現状と課題

標的型メール攻撃への対策として，我が国では次の二つの対策が，現在，推進されている．

(1)人的対策

標的型メール攻撃に対する社員・職員の教育・訓練である．標的型攻撃メールの特徴や確認すべき事項を説明し，標的型攻撃メールを見分ける能力を一人一人の社員･職員に身につけさせる対策である．また，適宜，訓練用の標的型攻撃メールを社員・職員に送付，標的型攻撃メールを見分ける能力が不十分な社員・職員への注意喚起や再度の教育・訓練により，見分ける能力を高める，という対策である．

(2)技術的対策

我が国では，メール送信ドメイン認証技術である SPF : Sender Policy Framework（[3]），DKIM : Domainkeys Identified Mail（[4]）の利用が推奨されている．両技術とも，標的型攻撃メールの多くがメール送信ドメインの詐称であるという特徴を利用し，受信メールの送信者のメールアドレスに指定されたドメインと，そのメールが実際に発信されたメールドメインの不一致を確認することにより，メール送信ドメインの詐称（メールアドレスの詐称）を検出する技術である．

2.1 人的対策の現状と課題

標的型攻撃メールの現状やその特徴，見分け方の資料は数多く公開されており，多くの組織で社員・職員の教育も実施されている．また，実際に訓練用の標的型攻撃メールを社員・職員に送付，適切な対応ができるかどうかの訓練も広範に実施されており，その結果を踏まえて，再度の教育や訓練が繰り返されている.「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）」（[5]）によると，平成 24 年度，19 府省庁で約 12 万人に対し標的型メール攻撃に対する職員の教育・訓練が行われ，訓練のために配布した標的型攻撃メールの開封率は 14.6%（2 回目は 10.6%）と報告されている．また,「サイバーセキュリティ政策に係る年次報告（2013 年度）」（[6]）によると，平成 25 年度は 18 府省庁で約 18 万人に対し教育・訓練が行われ，訓練のために配布した標的型攻撃メールの開封率は 10.1%（2 回目は 16.3%）と報告されている．もちろん，民間企業でも，このような教育・訓練は実施されている．

このような社員・職員の教育・訓練は，社員・職員の情報セキュリティに対する危機意識を高めるのに効果はあるが，標的型メール攻撃対策としては限界もあり課題もある．

府省庁の訓練結果のように標的型攻撃メールの開封率が 10%程度の場合，攻撃者が攻撃対象の組織の 50 人の社員・職員に対し標的型攻撃メールを送ると，99%以上の確率で開封され攻撃者は侵入に成功することになる．もちろん，教育・訓練により標的型攻撃メールの開封率を下げる努力により侵入される確率を下げることは可能であろうが，標的型攻撃メール対策としての人的対策には限界がある．

また，教育・訓練は一時的だが，社員・職員は教育・訓練にて得た知識・ノウハウにより，毎日多数受信するメールが標的型攻撃メールかどうかを判断する必要がある．送信者の名前・メールアドレス，組織名称やタイトルや本文

の内容について信憑性を確認するために，インターネットや関係書類の調査，場合によっては送信者へ電話で送信メールの確認などが必要な場合もあろう．このような，受信メールが標的型攻撃メールかどうかの調査・確認に必要な社員・職員の時間に対する費用負担は，算出された例は無いが大きなコストとなっていることは間違いない.「ビジネスメール実態調査 2016」（[7]）によると，98%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 12 通のメールを送信し，平均 55 通のメールを受信している，という．社員・職員が，1 日に 55 通のメールを受信するとした場合, この 55 通のメールが標的型攻撃メールかどうかの判断, そのための調査･確認の時間が必要となる．その時間を仮に 15 分～30 分/日とすると，人件費の 1/32～1/16 が標的型攻撃メールへの人的対策コスト，となる．国家公務員の平均給与が月額 40 万程度（[8]），平成 25 年度の府省庁での標的型メール攻撃訓練を受けた 18 万人が同程度メール受信，同程度の標的型攻撃メールかどうかの調査・確認時間を消費したとすると，年間 270 億～540 億の標的型メール攻撃への人的対策費用を負担していることになる．もちろん，このような人的対策費用の負担は，国家公務員約 58 万人，地方公務員約 275 万人，従業員が 300 人以上の民間企業に属する社員約 1800 万人であることを考えると，人的対策に対する我が国全体の費用負担額が実は膨大であることがわかる．

標的型メール攻撃に対しても，教育・訓練による社員・職員の情報セキュリティ意識を高める人的対策が重要であることはもちろんだが，技術的対策で効果的に効率的に代替できる部分については，積極的に技術的対策に切り替える努力，技術的対策実用化への投資を行うべきであろう．

2.2 技術的対策の現状と課題

我が国で推奨されている技術的対策の一つ SPF は，あらかじめドメインを管理する DNS サーバに承認した送信メールサーバの IP アドレスを登録しておくことが前提であり，受信メールサーバが受信したメール内のメールアドレスに指定されているドメインの DNS サーバに, 受信メールを実際に送信した送信メールサーバの IP アドレスが登録されている（承認されている）ことをチェックすることにより，送信メールサーバがなりすまされていないことを確認する仕組みである．

我が国で推奨されているもう一つの技術的対策 DKIM は公開鍵暗号を利用しており，あらかじめ承認された送信メールサーバの DKIM 用の公開鍵は DNS サーバに登録しておくことが前提であるが，送信メールサーバはメールヘッダに秘密鍵を利用して署名を付与し，受信メールサーバはメールアドレスに指定されているドメインの DNS サーバから公開鍵を入手し署名を検証することで，受信メールを実際に送信した送信メールサーバがそのドメインを管理する DNS サーバに承認されていることを確認することにより，送信メールサーバかなりすまされていないことを確認する仕組みである．

このように，SPF，DKIM の両方とも，メールサーバ間の認証の仕組みである．受信メールサーバは，送信メールサーバの認証は行うが，その送信メールサーバが確実にメール送信者の認証を行っているかどうかについては確認するすべがない．

一般に，メール送信時にはメールクライアントと送信メールサーバ間では通信プロトコル SMTP が使用されているが，標準的な SMTP にはメール送信者の認証機能は無い．つまり，送信者になりすましてのメール送信は大変容易である．送信メールサーバの認証だけでは，送信者なりすましメール対策としては不十分である．なお，SMTP auth や POP before SMTP 等の仕組みにより，メール送信時のメール送信者の認証機能を強化する仕組みを導入している送信メールサーバも多いが，そこで利用されているメール送信者認証は，パスワードの長さ・複雑さ・有効期間などの運用ルール次第で安全性が大きく左右されるパスワード認証方式である. 実際, パスワードの認証方式の場合, 0.2~0.3%のパスワードが盗まれている，つまり 500 人に 1 人の割合でパスワードが盗まれている，という調査報告もあり，やはり送信者なりすましメール対策としては不十分である．

以上のように，SPF，DKIM は，メールサーバのなりすまし対策には一定の効果があるが，メール送信者のなりすまし対策としては不十分であり，SPF，DKIM では，人的対策の軽減，人的対策費用の負担軽減は期待できない，と思われる．

メール送信者なりすましのより確実な検出・排除のためには，送信組織側がメール送信者のより確実な認証を行う必要があり，かつ，受信組織側がそのことを確認できる仕組みが必要である．

3. 標的型メール攻撃対策としての S/MIME の可能性と課題

メール送信者の認証機能を有する技術に S/MIME：Secure / Multipurpose Internet Mail Extensions（[9]）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 でカプセル化した電子メールの公開鍵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．

S/MIME のデジタル署名により, メール送信者の認証（送信者の特定，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，標的型メール攻撃対策として大変有効なのは，多くの報告書に記されている通りである（[10]）．

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．現在，多くの金融機関は自らが送信する連絡メールがなりすまされたメールとの区別がつくように，

お客様への連絡メールには S/MIME を利用し署名を付与している．このように BtoC の通信で活用されてはいるが，標的型メール攻撃の攻撃対象となる BtoB（組織間）の通信ではほとんど利用されていないのが現状である．

なぜ，S/MIME が広く活用される状況にならないのか．それにはいくつかの課題がある．まずメールアドレス証明書発行費用の問題である．メールアドレス証明書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．第 2 に，利用者の煩わしさである．S/MIME メールの送受信には，通信相手のメールアドレス証明書の入手・管理が必要である．メールアドレス証明書の有効期間は 1 年～3 年程度であるから，適宜最新版を入手し保管中のメールアドレス証明書の更新が必要である．第 3 に，これが最大の課題ともいえるが，単独で S/MIME の導入・利用のための投資をしても，それだけでは投資に見合う効果をあげることができない，つまり標的型メール攻撃への有効な対策とはならないことである．S/MIME は，業務通信の多い組織グループで共通的に利用することにより，はじめて大きな効果を発揮する，という性質を有する技術である．

その他，S/MIME の暗号化機能についても課題がある．まず，組織の機密情報漏洩防止が難しい点である．メール送信者が S/MIME の暗号化機能を利用した場合，メール受信者以外は復号できないため，送信組織としては，機密情報がメールに含まれていないかどうかのチェックは難しい．第 2 に，ウイルスチェックが難しい点である．受信したメールが S/MIME の暗号化機能により暗号化されている場合，受信組織のメールサーバでの受信メールのウイルスチェックは難しい．

4. 「組織通信向け S/MIME」

“標的型メール攻撃に対抗する「組織通信向け S/MIME」”は，S/MIME の基本コンセプトは踏襲しつつも，組織通信のための機能の強化と同時に，組織通信へ限定するがゆえに実現可能な S/MIME の課題克服策を織り込んだ，組織通信向けの安心・安全な電子メール利用基盤構想である（図 1）．

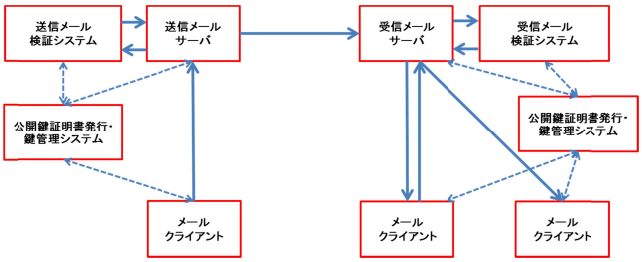

図 1　「組織通信向け S/MIME」システム基本構成図

以下，本構想における送信者認証機能，秘匿通信機能の実現方法を紹介し S/MIME が広く利用されない課題の多くが克服できることを示し，最後に **4.3** にて「組織通信向け S/MIME」が S/MIME と同様に抱えている普及上の課題の克服策について紹介する．

4.1 送信者認証機能の実現方法

S/MIME と同様，メール送信者の確実な認証の仕組みを導入する．また，そのような確実なメール送信者認証を行ったメールであることを，受信メールサーバで確認できる仕組みを導入する．本構想では，このような仕組みを次の三つのステップで実現する予定である．

(1)送信組織によるメール送信者の認証

メール送信者は，組織内で発行されたメールアドレス証明書内の公開鍵に対応する秘密鍵で，送信メールに署名を付与し，送信する．外部組織へメールを送信する送信メールサーバは，まず署名検証によりメール送信者の認証を行い，検証に成功したメールのみを外部送信対象とする．外部送信時には，メールに付与されているメール送信者の署名は送信組織の署名に付け替えられ送信される．

(2)受信組織による送信組織の認証

送信組織からメールを受信した受信組織の受信メールサーバは，送信組織の公開鍵証明書内の公開鍵により署名検証を行う．署名検証が成功し信頼できる組織からのメールであることを確認できたメールのみを内部転送対象とする．内部転送時には，メールに付与されている送信組織の署名は受信組織の署名に替えられ受信組織内部へ転送される．

(3)メール受信者による受信組織の認証

メール受信者は，受信組織の公開鍵証明書内の公開鍵により署名検証し，受信組織が認証済みのメールであることを確認し受信する．

図 2 は，転送プロセスを含めた，それぞれのエンティティ間で配信されるメールに付与される署名を示したものである．組織内の配信の場合の署名検証は，組織内で可能であるが，組織間の場合は信頼できる公開鍵証明書発行機関の存在，または信頼できる組織間での公開鍵証明書の交換・管理の仕組みが必要となる．

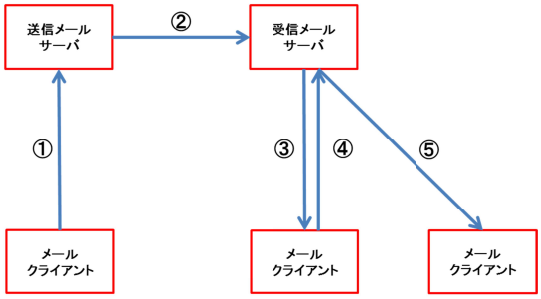

図 2　メールに付与される署名

このような，署名機能の連鎖によるメール送信者の認証を実現する方式の特徴・メリットは以下の通りである．

①S/MIME と同程度のメール送信者の認証

メール受信者はメールが(3)の署名検証に成功したかどうかを確認でき，その確認できたメールは(2)により受信組織が信頼できる送信組織からの送信メールであることを確認したメールであり，そのメールは(1)により送信組織がメール送信者の確実な認証を行ったメールであることを示している．

メール受信者は，メール送信者のなりすましの可能性（標的型攻撃メールの可能性）が極めて低いメールを選別でき，人的対策の時間を大幅に削減でき，効率的なメール処理が可能となる．

なお，メール送信者の秘密鍵管理や署名付与は，社員・職員カード内で行うなど，安全な管理・処理環境で行うことを想定している．

②メールアドレス証明書の費用負担低減

メール送信者のメールアドレス証明書は，本構想の場合，その有効範囲は送信組織内のみでよく，送信組織内での発行を想定している．

S/MIME の場合は，メール受信者が他の組織に属するメール送信者の署名検証を行う必要があり，その際に必要なメール送信者のメールアドレス証明書の検証が行えるよう，パブリックな公開鍵証明書である必要があり，１メールアドレスあたり年間数千円の費用負担を覚悟しなければならないが，本構想の場合は送信組織内のみで有効なメールアドレス証明書，プライベートな公開鍵証明書で構わないため，組織内で任意に発行でき，導入・運用費用の大幅な削減が見込まれる．

③メール送信者の公開鍵管理が不要

S/MIME では，メール受信者が受信メールの署名を検証するには送信者の公開鍵が必要であり，想定する送信者の公開鍵（メールアドレス証明書）を管理する必要がある．本構想では，送信者のいかんにかかわらず，受信メールは所属する組織の署名が付与されており，メール受信者は送信者の公開鍵を管理する必要が無い．

本構想では，S/MIME に比べメール受信者の鍵管理・鍵更新管理負担を劇的に削減できる．

4.2 秘匿通信機能の実現方法

本構想では，S/MIME の暗号化機能と異なり，“組織通信向け”のための機能，転送時の安全性を向上させうる暗号方式，組織暗号を導入する（[11]，[12]，[13]，[14]）．また，メールの外部送信時の機密情報漏洩チェックおよび外部からのメール受信時のウイルスチェックを可能とする仕組みを導入する．本構想では，このような仕組みを以下の方針で実現する予定である．

(1)メール送信者による暗号化

組織暗号は，受信者（転送者）のみが保有する秘密鍵でしか復号できない暗号化データを，その内容を示すラベル（暗号化データの内容の説明が記載された平文情報）を確認し，適切な利用者を判断できれば，その利用者のみが保有する秘密鍵でしか復号できない暗号化データへ，復号する（平文へ戻す）ことなく変換（鍵の付替え）できる暗号方式である．

本構想では，組織暗号による安全な転送実現のため，添付ファイルを個々に組織暗号による暗号化の対象とし，メール本文は個々の暗号化された添付ファイルの内容説明（ラベル）を記載する運用を想定している．

本構想ではまた，添付ファイルの暗号化には，送信組織の公開鍵を使用する．S/MIME では，メール受信者に応じその受信者の公開鍵で暗号化する必要があるが，本構想ではメール受信者に依存せず，常に送信組織の公開鍵で暗号化することを想定している．

(2)メールの外部送信時の検査および再暗号化

送信メールサーバが受信した外部への送信メールは，安全な検査環境が維持されている検査サーバへ転送される．検査サーバでは，暗号化添付ファイルも一旦復号され，機密情報の有無などの検査が行われ，その結果が送信メールサーバに通知される．送信メールサーバは，情報漏洩等，メールに問題が無いことを確認した上で，送信組織のために暗号化された添付ファイルを受信組織のための暗号化添付ファイルに変換（鍵の付替え）し，外部へ送信する．

(3)外部からのメール受信時の検査および再暗号化

受信メールサーバが外部より受信したメールは，安全な検査環境が維持されている検査サーバへ転送される．検査サーバでは，暗号化添付ファイルも一旦復号され，ウイルスチェックなどの検査が行われ，その結果が受信メールサーバに通知される．受信メールサーバは，ウイルス等，メールに問題が無いことを確認した上で，受信組織のために暗号化された添付ファイルをメール受信者のための暗号化添付ファイルに変換（鍵の付替え）し，受信組織内へ配送する．

(4)メール受信者による復号

メール受信者は，自身の秘密鍵により復号する．秘密鍵の管理および復号処理は，社員・職員カード内の安全な環境で管理・処理されることを想定している．

(5)メール受信者による再暗号化および転送

メール受信者は，平文のメール本文の情報から，暗号化添付ファイルの適切な転送先を判断，転送先のメールアドレスを指定し転送すると，メール受信者のために暗号化された添付ファイルは受信組織の公開鍵による暗号化添付ファイルへ変換（鍵の付替え）され転送される．

図３は，転送プロセスを含めた，それぞれのエンティティ間で配信されるメールの暗号化に使用される公開鍵を示したものである．暗号化および再暗号化に必要な送信先の公開鍵による暗号化は，送信先が組織内の場合は組織内で可能であるが，組織間の場合は信頼できる公開鍵証明書発行機関の存在，または信頼できる組織間での公開鍵証明書の交換・管理の仕組みが必要となる

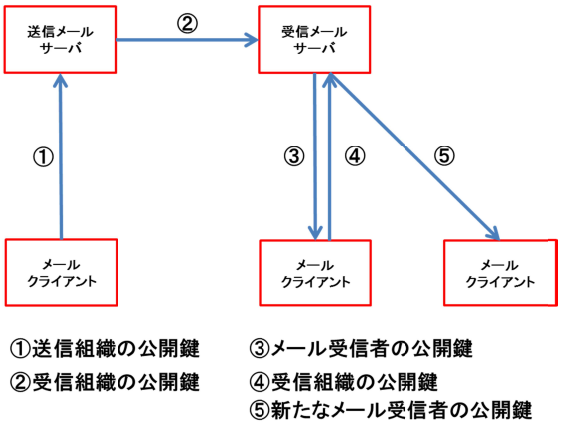

図３　暗号化に使用される公開鍵

このような，暗号化機能の連鎖による秘匿通信機能を実現する方式の特徴・メリットは以下の通りである．

①メール受信者の公開鍵管理が不要

本構想では，添付ファイルの暗号化には，送信組織の公開鍵を使用する．S/MIME では，メール送信者は想定する暗号化メール受信者の公開鍵を暗号化に使用するため，暗号化メール送信を想定する全ての受信者の公開鍵（メールアドレス証明書）を管理する必要があるが，本構想ではメール送信者はメール受信者の公開鍵を管理する必要が無い．

本構想では，S/MIME に比べメール送信者の鍵管理・鍵更新管理負担を劇的に削減できる．

②送信組織の機密情報漏洩等の検査が可能

S/MIME の暗号化機能の場合，組織の管理者といえども送信メールの暗号化データの内容を確認できず，組織としてのポリシー順守の確認が取れず，組織として暗号化機能を導入するのは困難であったが，本構想の秘匿通信機能では，平文メールと同等の検査・監査が可能となり，組織としての導入の大きな障害の一つをクリアできる．

③受信組織のウイルスチェック等の検査が可能

S/MIME の暗号化機能の場合，組織の管理者といえども受信メールの暗号化データの内容を確認できず，ウイルスチェック等ができず，組織として暗号化機能を導入するのは困難であったが，本構想の秘匿通信機能では，平文メールと同等のウイルスチェックが可能となり，組織としての導入の大きな障害の一つをクリアできる．

④転送時の機密情報の安全性向上

S/MIME の暗号化機能の場合，転送の際は暗号化された機密情報を一旦復号し，その上で新たに暗号化する必要があるが，本構想では，暗号化された機密情報を復号することなく転送先の新たなメール受信者のために暗号化された機密情報へ変換できる組織暗号を採用しているため，転送時の安全性を大きく向上させることができる．

4.3 普及上の課題克服策

3. で指摘した S/MIME の普及を阻害してきた課題については，**4.1** および **4.2** で示した，本構想の実現方針・方式により，以下の 1 点を除き克服される見通しを得ることができた．

残る課題は，投資効果の問題である．本構想も S/MIME と同様の課題に直面しており，標的型メール攻撃対策としての本構想に基づくシステム導入への投資が，自組織の標的型メール攻撃対策効果には必ずしも直結しない点である．本構想に基づく電子メール利用基盤が社会基盤として多くの組織が導入し運用している状況ではない現状では，単一組織の努力は実を結ばないことになる．一方，一つ一つの組織で導入を進めていただかない限り，社会基盤へ発展する可能性は無い．

このような状況を打開し，「組織通信向け S/MIME」構想が抱える課題を克服するためには，以下のような政府主導の施策が必要と考える．

(1)我が国の次世代電子メール利用基盤として開発推進

標的型メール攻撃対策として大きな効果が期待できる，組織間の安心・安全な電子メール利用基盤として，まずは政府主導で開発を推進し，実証実験等を通じ，機能性・実用性を社会に提示し，導入推進に対する社会のコンセンサスを得るのが望ましい．

(2)政府主導で目標・スケジュールを策定し推進

我が国の産業活動の安全性，効率性の向上策の一環として，システムの導入・運用目標・スケジュールを政府主導で策定，業界ごとに監督官庁がフォローする体制を整え，確実な普及を図ることが望ましい．

(3)府省庁が率先し導入・活用推進

標的型メール攻撃の対象となることが多い府省庁が率先し導入・活用し，産業界に範を示すことが望ましい．また，府省庁と産業界との組織通信は，本構想に基づくメール通信に限定するなどにより，産業界での導入・活用を促す施策を推進することが望ましい．

(4)産業界の導入に対する支援

産業界の導入を加速すべく，導入組織への税制面の優遇など，導入組織の費用負担軽減策などを検討することが望ましい．

以上のように，普及上の課題を克服するには，どうしても政府主導の施策が必要と考えるが，「組織通信向け

S/MIME」構想の必要性・効果に関するコンセンサスの醸成, および政府への具体的政策提言などを検討するための, コンソーシアム的な組織が必要ではないかと考え，その設立について検討中である.

5. 安心・安全な電子メール利用基盤に向けて

我々の最終目標は，個人も含めた我が国の安心・安全な次世代電子メール利用基盤の構築である．その第一歩として，組織通信向けに限定した新たな構想を「組織通信向け S/MIME」と称し，本論文で提案した.

個人を含めた安心・安全な電子メール利用基盤でのメールアドレス証明書（公開鍵証明書）の発行については以下のような方式を想定している．このようなメールアドレス証明書（公開鍵証明書）発行の枠組を前提に，我が国の安心・安全な次世代電子メール利用基盤構想を，現在策定中である.

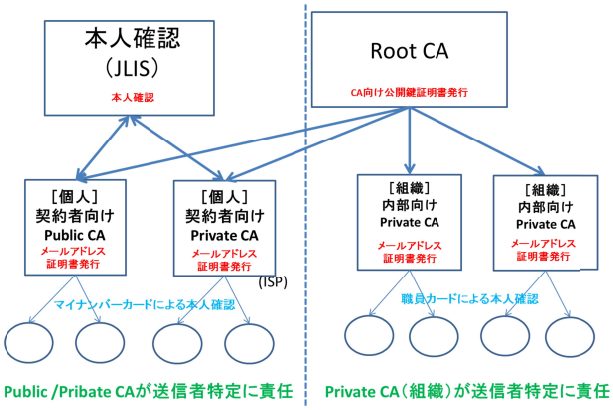

図４　メールアドレス証明書（公開鍵証明書）発行の枠組

なお，個人の場合のメールアドレス証明書発行時の本人確認にはマイナンバーカードによる本人確認を，署名付与には個人の場合はマイナンバーカード，組織の場合は社員・職員カードの利用を想定している.

6. おわりに

本論文では，我が国の高度情報化社会を支える安心・安全な次世代電子メール利用基盤構想，およびその第一歩として，標的型メール攻撃被害が多発している組織通信を対象とした構想を「組織通信向け S/MIME」と称し紹介した．なお,「標的型攻撃・サイバー戦争から日本を守る」という観点からの本構想の位置付け，重要性については，日本セキュリティ・マネジメント学会第 30 回全国大会にて報告済みである（[15]）．参照願いたい.

我々は,「組織通信向け S/MIME」構想，ひいては「安心・安全な次世代電子メール利用基盤」構想の実現に向け，引き続き活動する予定である.

関係各位の，ご協力・アドバイス等，いただければ幸いである.

参考文献

[1] “情報セキュリティ 10 大脅威 2016”. 情報処理推進機構. https://www.ipa.go.jp/security/vuln/10threats2016.html, (参照 2016-07-09).

[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] “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).

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

[5] “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).

[6] “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).

[7] “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).

[8] “国家公務員給与の概要”. http://www.jinji.go.jp/kyuuyo/kou/27gaiyou.pdf,（参照 2016-07-10）

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

[10] “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)

[11] 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.

[12] 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.

[13] “「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)

[14] “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)

[15] 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.