ISP連携によるスパムメールへの技術的対策

記事のポイント

サマリー　米国の大手ISPを中心メンバーとするスパムメール対策組織ASTAは、6月22日、スパムメールの送信元詐称を防ぐ対策技術などに関する提言書を発表した。また、米国連邦取引委員会（FTC）は、6月15日、米国議会への「Do Not E-mail」リストの有効性に関する報告書の中で、スパムメール対策として当該リストは効果無しと結論付け、送信元認証の必要性を訴えるなど、送信元認証技術を望む声が大きくなっている。本稿では、ASTAの提案するスパムメール送信元認証技術のしくみを概観し、その課題について考察する。

主な登場者　ASTA　Earthlink　Yahoo!　Microsoft　AOL　FTC

キーワード　スパムメール　送信元認証　ASTA　Earthlink　Yahoo!　Microsoft　AOL　FTC　SPF　Sender ID　DomainKeys

地　域　米国

執筆者　KDDI総研　調査2部　嶋田　実（mi-shimada@kddi.com）

1　経緯・背景

世界的にスパムメールの悪影響がますます大きくなっている。セキュリティソフトベンダーのSymantecによると、本年5月における全世界で行き交うEメールトラヒックに占めるスパムメールの比率は約64%に達するという。Eメールユーザの中には、受信メールボックスが、ほとんどスパムメールで埋め尽くされているケースもあり、状況はさらに悪化する傾向を示している。こうしたEメール機能を麻痺させるスパムメールというIT社会の共通の問題に対処するための業界連携の動きが具体化しつつある。

大手ISPのEarthlink、Yahoo!、Microsoft、AOLは、2003年4月、スパム対策組織Anti-Spam Technical Alliance（以下、「ASTA」）を結成し、スパムメールに対する技術的対策を検討してきた。その結果、本年6月22日、ASTAは、スパムメールの送信元詐称を防ぐ対策技術などに関する提言書を発表した。これまで各社とも、スパム

メール対策において送信元認証技術が重要との認識では一致していたものの、独自の技術にこだわっていたため、統一化が危ぶまれていた。ここにきて共同提言を行なうに至ったのは、現状が危機的状況にあり、「小異を捨てて大同につく」必要があるとの認識の下、歩み寄ったものと考えられる。

スパムメールへの技術的対策としては、従来からフィルタリングやブラックリストなど様々な方法が提案され実施されているが、スパムメールの勢いを食い止めるには至っていない。電子メール転送プロトコルとして広く普及しているSMTP（Simple Mail Transfer Protocol）はメールヘッダに含まれる送信元アドレスを任意に書き換えることが可能であり、このことを利用して、スパマーは送信元アドレスを詐称し（いわゆる「なりすまし」）（【図表1】参照）、送信元アドレスを用いたフィルタリングやブラックリストなどのスパムメール対策を逃れていることが、大きな要因の一つである☞（脚注）。

また、最近、米国を中心に、ネットオークション大手のebayや金融機関などを詐称したスパムメール（これらは送信元ドメイン名も詐称している）を個人に送りつけて偽造サイトに誘導し、クレジットカード番号などをかすめ取るいわゆるphishing詐欺が猛威を振るっている。送信元詐称は、従来のフィルタを欺く目的に加え、ユーザを欺く目的で行なわれるようになってきている。

【図表1】スパマーの送信元として使われたドメインのトップ10（2004年5月）

ドメイン	比率
Yahoo.com	6.46%
Hotmail.com	4.81%
MSN.com	4.30%
Attbi.com	1.78%
AOL.com	1.28%
Canada.com	0.38%
Excite.com	0.23%
Comcast.com	0.22%
Netscape.com	0.22%
Earthlink.com	0.21%

（Comtouchのホームページ掲載のデータを元にKDDI総研作成）

☞（脚注）

スパマーが送信元ドメインを詐称する理由としては、この他に、ありそうなメールアドレスに手当たり次第に送りつけるいわゆる辞書攻撃を行なう際、スパマーのメールサーバーに宛先不明の大量のバウンスメッセージが戻るのを避けるという目的もある。

一方、本年6月15日、米国FTCは、議会に対し「Do Not E-mail」リスト（脚注1）の有効性に関する報告書を提出した。その中で、当該リストへのユーザアドレスの登録は、却ってスパマーの格好のターゲットになることが明らかであるとし、リスト化は現時点では行なうべきでないと述べている。さらにEメールに送信元認証の機能がないことが、スパマーによるEメールの濫用を許しているとし、スパムメール対策としては、まず送信元認証技術の確立に努力を集中すべきとしている（脚注2）。これにより、フィルタリングや違法スパマーの特定が一層効果的になると述べている。

このように、送信元認証技術は、スパムメール対策として中心的なものになっている。ASTAの今回の提言書は、送信元認証技術として「IPアドレスによるアプローチ」、および「コンテンツ署名によるアプローチ」の二つを提案しており、いずれも送信元ドメイン名（送信元メールアドレスの@の右側）の詐称を判定するしくみである。これらの方式について、以下に、そのしくみの概要を紹介する。

2　IPアドレスによるアプローチ　－ SPF －

Eメールの届く基本的なしくみの概要ついては、コラム1を参照いただきたい。

「IPアドレスによるアプローチ」は、TCP/IP上で送られてくる送信元サーバーのIPアドレスを信頼して、エンベロープ上の送信元ドメイン名の詐称を判定しようとするものである。

この方式は、Eメールの転送サービスなどを行なう米国のベンチャー企業であるPobox.comのCTOであるMeng Weng Wong氏が「SPF（Sender Policy Framework）」

（脚注1）

リストに登録されたユーザアドレスに対し、広告メールの送信を禁じるものである。本年1月、スパムメールを規制する米連邦法CAN-SPAM ACTが施行されたが、その中で、当該リストの有効性に関する調査報告書を議会に提出するよう、FTCに要請していた。
（KDDI総研R&A 2004年3月号「米国連邦政府による迷惑メール規制法が成立」参照）

（脚注2）

FTCは、標準的な認証技術が、オープンな環境の下で開発され、小規模ISPなどにも簡単に採用できるようにするため、今年秋に、FTCのスポンサーの下、認証サミット（Authentication Summit）を開催するとアナウンスしている。ISPの技術者、メールサーバーの運営者、コンピュータ科学者などを招待して議論を交わし、標準的な認証方式について、参加者などに広範なテストの実施と、その結果を踏まえた大規模な導入を奨励するとしている。

【コラム1】Eメールの届くしくみ

Eメールの届く基本的なしくみを以下に示す（【図表2】参照）。

① 送信元PCから受信先メールアドレス（AAA@XXX.com）を入力してメッセージを送信すると、ユーザの契約した送信メールサーバーに転送される。

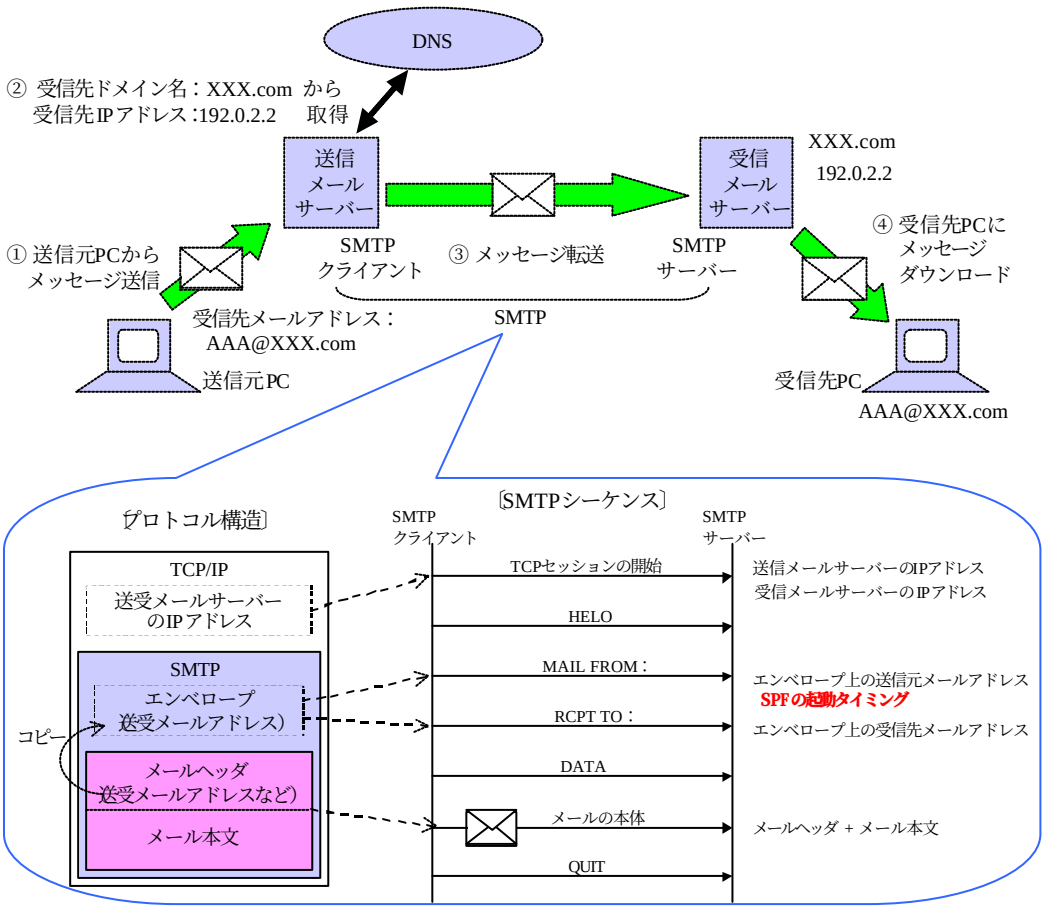
② 送信メールサーバーは、受信先メールアドレスのドメイン名（メールアドレスの@の右側の部分）に基づき、ドメイン名とIPアドレスの組合わせを管理するDNS（Domain Name Server）から、受信メールサーバのIPアドレスを取得する。

③ 受信メールサーバのIPアドレス宛に、SMTPにより、メッセージを転送する。受信メールサーバでは、図のSMTPシーケンスに示すように、TCP/IPをとおして「送受メールサーバーのIPアドレス」を、次にSMTPをとおして「エンベロープ上の送信元および受信先メールアドレス※」、「メールヘッダおよび本文」を順に受信する。

④ 受信メールサーバーに届いたメッセージは、受信メールボックスに保存され、受信先PCからのダウンロード要求によって、受信先PCにダウンロードされる。

※：SMTP上で記憶している送受メールアドレスであり、メールヘッダ上の同情報がコピーされている。

【図表2】Eメールの届くしくみ



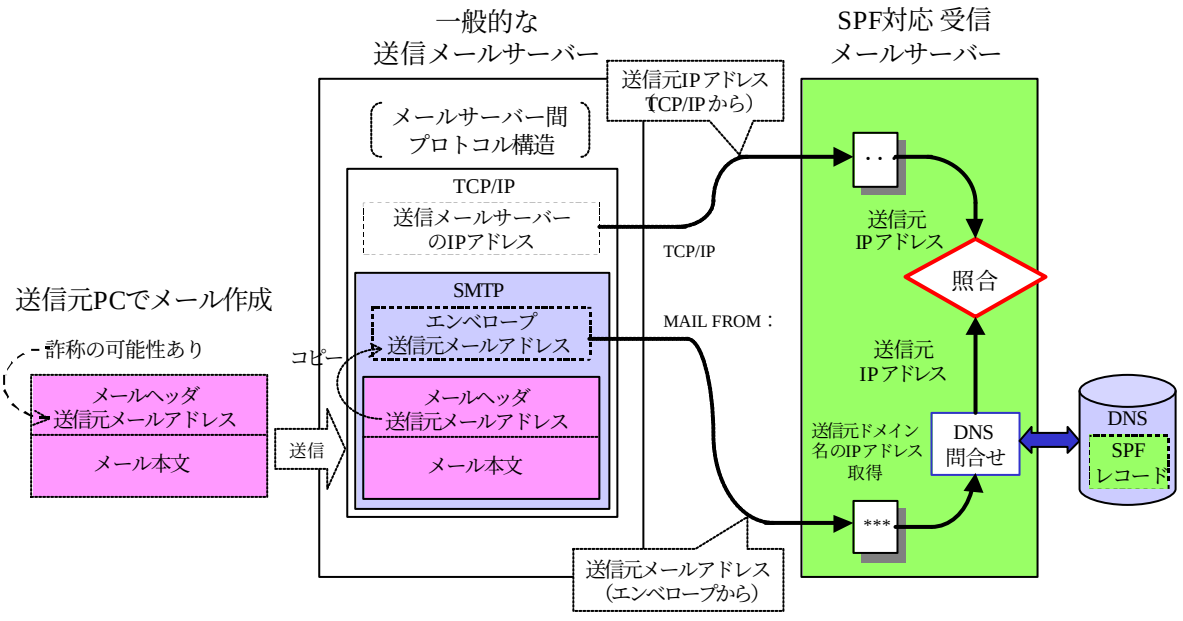
として開発した。SPFは、ASTAのメンバーであり世界最大のISPであるAOLが採用を検討して試験を行なってきた。同様のしくみは、Microsoftからも「Caller ID for E-mail」として提案されていたが、本年6月24日、両者の仕様を統合して「Sender ID」という名称に統一し、MicrosoftとPobox.comの共同で、インターネットの標準化推進団体のIETF（The Internet Engineering Task Force）に仕様書が提出された。仕様の競合よりも、統合により広く普及させることを優先したもの言えよう。これらの基本的なしくみは大きく変わるものでないため、本節では、統合前のSPFについて、そのしくみをみることとする。

SPFによる送信元認証のしくみを【図表3】、【図表4】に示す。

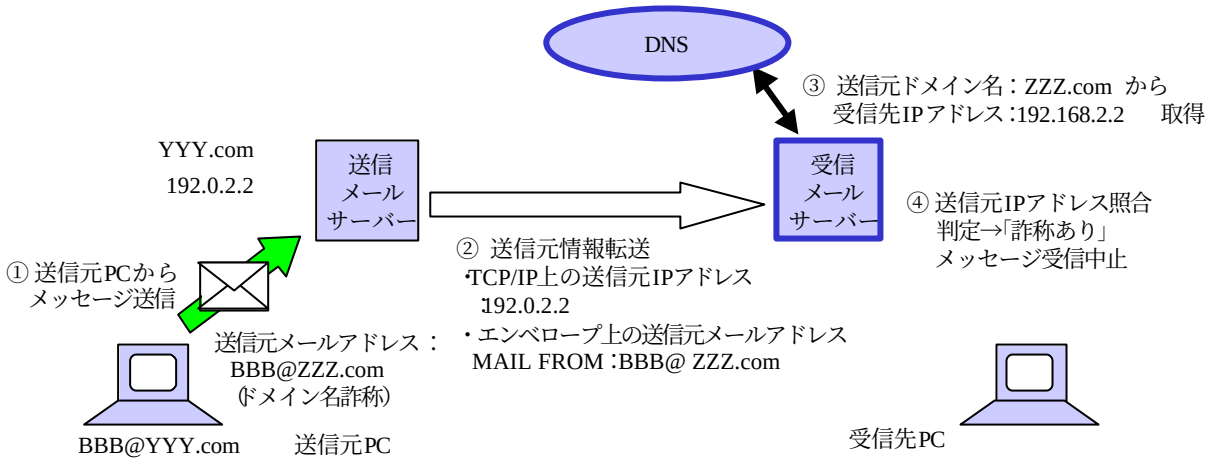
DNSは、受信先メールアドレスのドメイン名から、そのIPアドレスを引き出す機能をもつが、SPFでは、送信元ドメイン名（詐称の可能性のあるエンベロープ上の送信元ドメイン名）から、そのIPアドレスを引き出すためにもDNSを用いる。SPFに対応した受信メールサーバーでは、エンベロープの送信元ドメイン名に基づきDNSから得られた送信元IPアドレスを、詐称が困難なTCP/IP上で得られた送信元IPアドレスと照合する。両者が一致すれば、当該ドメイン名は詐称がなかったものとして、メッセージ受信処理をすすめる。一致しない場合、詐称ありとして、メッセージ受信を中止する。判定は、受信メールサーバーがメッセージ本体（ヘッダーおよび本文）を受信する前に行なえるため、スパムメール転送によるネットワークへの負荷を軽減できることが特徴である。

DNSは、受信メールサーバーを特定するためのしくみだが、SPFでは、送信メールサーバーを特定するためにも利用するため、DNSのドメイン情報のテーブルに「SPFレコード」という情報を追加する必要がある。

【図表3】SPFによる送信元認証のしくみ



【図表4】SPFによる送信元詐称の判定の流れ



SPFでは、SPF判定結果をメールヘッダに貼り付けることが推奨されている。これにより、受信先PCなどにおいて、「送信元詐称無し」、「送信元詐称あり（受信中止）」のほか、SPFレコード未発行のドメインから送られたものであること（すなわち「未判定」）の区別が見分けられるようになる。仮に、将来ほとんどのISPがSPFを採用するような場合には、SPFレコード未発行のドメインを怪しげな送信ドメインとみなし、受信先PCでフィルタリングすることも可能となる。また、こうしたユーザ行動が想定されれば、各ISPは、自分のドメインから送信したメールがユーザに怪しまれてフィルタで受信拒否されることのないよう、積極的にSPFの採用に向かうとも考えられる。

SPFは、既存のSMTPとDNSを巧みに利用し、対策に要する既存のインフラへの影響を最小限にとどめながら、送信元ドメインの詐称を防ぐしくみと捉えられ、大手ISPが後押ししていることもあり、普及が期待される現実的な解決策と言えよう。

3　コンテンツ署名によるアプローチ　－ DomainKeys －

「コンテンツ署名によるアプローチ」は、Eメールシステムにデジタル署名を導入しようとするものである。デジタル署名については、コラム2を参照されたい。

ASTAのメンバーのYahoo!は、DomainKeysという名称で、この方式を開発、提唱してきた。DomainKeysによる送信元認証のしくみを【図表5】、【図表6】に示す。

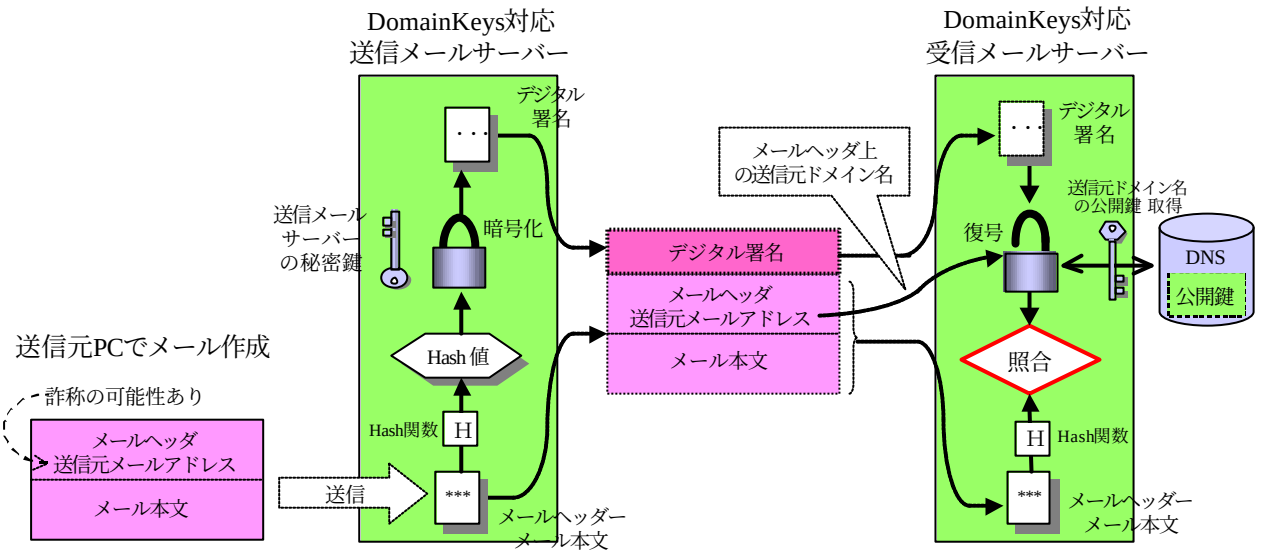
DomainKeysでは、各送信メールサーバーに、サーバー固有の秘密鍵が保管され、そのドメイン名を管理するDNSに、それぞれのペアとなる公開鍵が保管される。

ドメイン内のあるユーザからメッセージが送信されると、DomainKeys対応送信メールサーバーは、保管する秘密鍵を用いて、そのメッセージに自動的にデジタル署

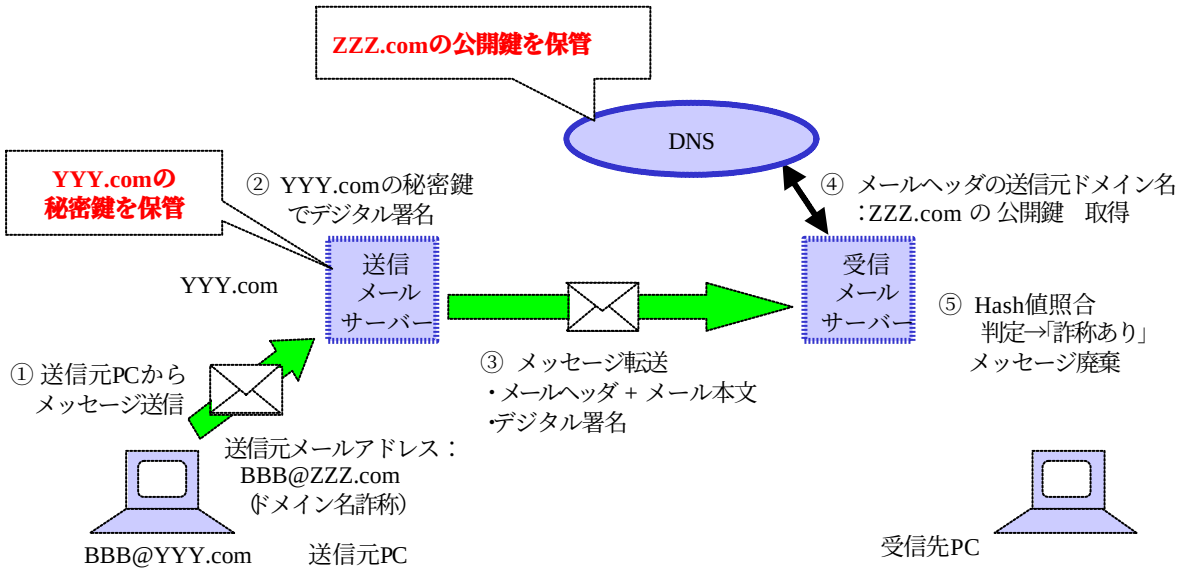
名を施し、メールヘッダに貼り付けて受信メールサーバーに送る。

DomainKeys対応受信メールサーバーは、デジタル署名されたメッセージを受信すると、メールヘッダ上の送信元メールアドレスのドメイン名に対応する公開鍵をDNSから取得する。その公開鍵を用いてデジタル署名を復号し、その結果とメッセージ本体（メールヘッダ＋メール本文）から得られたHash値と照合して、そのドメイン名が詐称されたものかどうかを判定する。

【図表5】DomainKeysによる送信元認証のしくみ



【図表6】 DomainKeys による送信元詐称の判定の流れ



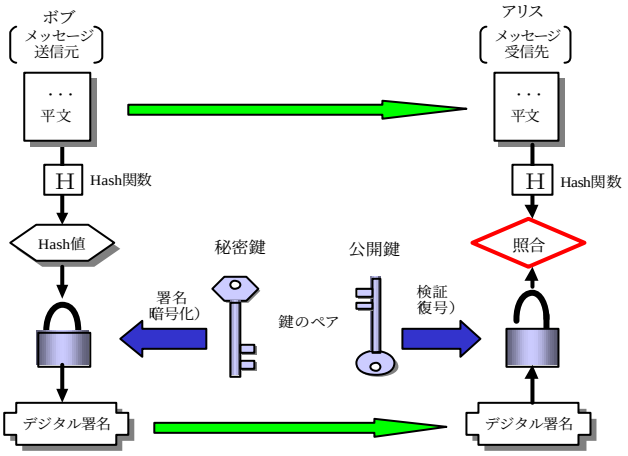
【コラム2】デジタル署名

デジタル署名とは、オンラインで送信元から受信先にデジタルデータを送る際、送信元の本人証明（「認証」）、および送信途上でのデータの改竄やすり替えなどの検出（「完全性」）を目的とするしくみである（【図表7】参照）。

平文を、ボブからアリスに送る場合を考える。まずボブは、デジタルデータを送る際、デジタルデータ全体をHash関数☞（脚注）へ入力し、Hash値を出力する。得られたHash値をボブの秘密鍵で暗号化することでデジタル署名が生成される。生成されたデジタル署名を平文といっしょにアリスに送る。アリスは、デジタル署名をボブの公開鍵で復号して、元のHash値を得る。また、並行して受信した平文をボブと同じHash関数へ入力してHash値を求め、両者を照合する。公開鍵がボブのものであることが明らかであるとすると、両者の値が一致すれば「認証」と「完全性」は満足されるが、一致しない場合は、ボブ以外の秘密鍵がデジタル署名に使用されたか、途中で平文が改竄されたかのいずれかと推定される。

ここで、公開鍵が本当にボブのものかどうかが問題になる。公開鍵が何らかの方法ですり替えられる可能性があるからだ。そこで公開鍵が送信元のものであることを証明する電子証明書を発行する信頼ある第三者機関として認証局、すなわち公開鍵基盤（Public Key Infrastructure：PKI）の構築が必要となる。

【図表7】 デジタル署名のしくみ



☞（脚注）

Hash関数とは、元データの長さに関係なく、Hashアルゴリズムの出力値（Hash値）は必ず決められた長さ（128ビットや160ビット）になるもので、元データが少しでも異なれば、Hash値は大きく異なるものになるという特徴をもつ。通常、暗号化処理の効率化のため、平文から一旦Hash値を求め、そのHash値を暗号化する。

一般にデジタル署名は、公開鍵がメッセージ送信者のものであることを証明する認証局を必要とするが、Yahoo!によれば、DomainKeysでは、認証局は特に必要ない。DNSが公開鍵の配送システムとして機能していること、またドメイン所有者のみがDNSに公開鍵を発行できることから、鍵のすり替えはありえないことをその理由とする。

DomainKeysは、前節でみたSPFと比較し、暗号化や復号に伴う複雑な処理が必要であり、またメールの本体を受信しなければ送信元認証の判定ができないなどの点を考えると、普及へのハードルはやや高いように思われる。ただし、デジタル署名をサーバー間で導入することで、認証局を不要とするなど、普及への配慮もなされている。

📖 執筆者コメント

受信側だけで対策を行なう受信フィルタリングなどの技術と異なり、本稿でみたように、送信元認証技術は、送信側および受信側のそれぞれが同じしくみの元で動作することでその機能を実現しようとするものである。ところが送信メールサーバー（または送信ドメインを管理するDNS）と受信メールサーバーは、一般に異なるISPなどの管理下にあることから、送信元認証技術は、特定のISPのメールサーバーやDNSだけが対応していても効果は薄く、多くのISPが同じ方式の導入に足並みを揃えることで、初めてその効果を生み出すものである。こうした協調システムによるスパムメール対策は、これまでにない新たな試みであると考えられ、いかに多くのISPが協調できるかが、その成否を左右する大きな課題と言えよう。

ASTAの提言はこの点を強調し、「短期間に広範な採用を確実にするリーダーシップを提供したい」と述べる。提案された送信元認証技術のうち、特にSPF（統合後の名称で言えば、Sender ID）は、世界最大のISPであるAOLの強力なバックアップがあることと、導入の容易さや、スパムメールの無駄なトラヒックが減少することなどのメリットにより、普及の可能性は高いと考えられる。

この動きは、現在、米国を中心としたものであるが、スパムメール対策ソフトベンダーのComtouchの調査によると、スパムメール発信元は、米国発のものが3月の60%から、5月の55.7%と次第に米国以外に広がりつつある。米国のみならず世界的規模での協調が必要となることは明らかであろう。偏狭なナショナリズムや技術的覇権主義の枠などを超えて、国際社会や企業がスパムメール対策に協調していけるか、送信元認証技術は、現代のIT社会に突きつけられた一つの試金石と言えるかもしれない。そこでは、各国大手ISPなどによる世界的な協調に向けたリーダーシップが特に重要になると考えられる。

【コラム3】送信元認証という新たな規制

インターネットのハードウェアやソフトウェアの「しくみ」そのものが、インターネットユーザの行為を規制する場合があり、こうした「しくみ」は、サイバー空間のいわば「法律」であるとする見方がある☞（脚注）。本稿にみる送信元認証技術も、これまでのインターネットに、大手ISP主導の下、新たな規制を導入しようとするものとの見方ができる。

ASTAの提言書は、この点を配慮し、「（送信元を明らかにする）送信元認証の導入は、プライバシーや法的な問題を孕み、特に言論の自由への潜在的影響を真摯に考慮する必要がある」とし、「慎重にこれらの問題に対処しつつ、『表現の自由』を許容する技術やアプローチを追及しなければならない」と述べる。一方、既存のEメールの柔軟性を維持しつつ、スパムメールを減らす新技術を育てることが目的であるが、送信元認証技術は「Eメールの配信、安全性、認証についての新しい考え方を要求する重大な挑戦である」として、一般社会への理解を求めている。

📖 出典・参考文献

ASTA, “Anti-Spam Technical Alliance Technology and Policy Proposal”, 22 June 2004

FTC, “National Do Not Email Registry　A Report To Congress”, June 2004

Pobox.comのホームページ　http://spf.pobox.com/mechanisms.html

INTERNET DRAFT ‘ Sender Policy Framework（SPF）　A Convention to Describe Hosts Authorized to Send SMTP Traffic ’, Mark Lentczner, Meng Weng Wong, Pobox.com, May 2004

LINUX Journal, APRIL 2004

LINUX Journal, MAY 2004

📖

☞（脚注）

スタンフォード大学ロースクールのレッシング教授は、こうした「しくみ（アーキテクチャー）」を「コード」と呼び、法律による規制に比べ、サイバー空間への「コード」の導入は、民主的プロセスを経ずに進みやすいことを危惧する。（ローレンス・レッシング著 山形、柏木訳『CODE』翔泳社　など参照）

Microsoftのホームページ
http://www.microsoft.com/presspass/press/2004/jun04/06-24SIDSpecIETFPR.asp

Yahoo！のホームページ　http://antispam.yahoo.com/domainkeys

INTERNET DRAFT ‘ Domain-based Email Authentication Using Public-Keys Advertised in the DNS（DomainKeys）’, Mark Delny, Yahoo! INC, May 2004

トム・オースティン著、㈱ニューコム訳『PKI公開鍵基盤』日経BP企画