

「電子商取引における電子メールに関するセキュリティ上の課題」

平成 11 年 3 月

目次

1. 現状調査	4
現在、電子決済を行っている企業とそのサイトについて.....	4
電子商取引の販促サービス.....	5
国内の電子商取引に対する個人的な考察.....	6
海外の電子メールの電子商取引における活用について.....	7
AMAZONE.COM に関して.....	7
THISCO.COM に関して.....	7
SSL 等が使用出来ないサイトの問題.....	8
2. X.509 電子証明書の問題調査	9
X.509 の解説.....	9
SSL の解説.....	13
S/MIME の解説.....	17
SSL と S/MIME で、電子証明書を引き継ぐことの技術的可能性について.....	20
X.509 電子証明書の互換性.....	23
ユーザー(消費者)利用者の観点からの課題.....	25
3. 商用電子メールのプライバシーの問題	28
電送路上でデータの盗聴の可能性について.....	28
電送路上の暗号化の必要性について.....	29
電子商取引サイト.....	29
DNS MX レコードについて.....	30
エラーメールのプライバシー問題.....	32
対策技術の紹介.....	33
電子商取引サーバの運用上の課題.....	34
4. 他人になりすました商取引電子メールの問題	35
サイトになりすました商取引電子メールの消費者への問題.....	35
商取引電子メールによる電子商取引サイトにおける影響.....	36
他人になりすました消費者による購入の問題.....	37
対策.....	38
5. 大量の商業宣伝メール(UCE)配信の問題	39
意図しない不正中継による問題.....	39
ORBS について.....	40

IP アドレス割当てと ORBS について.....	40
サーバの意図しない不正中継の問題.....	41
ユーザー(消費者)側での対策.....	43
スパマーによる電子メール・アドレスの収集方法と対策.....	44
6. 添付資料.....	45
ORBS メール.....	45
7. 参考文献.....	47

1. 現状調査

現在、電子決済を行っている企業とそのサイトについて

日本でも近年、電子商取引において電子決済を行なっているサイトが増えてきている。特に大手航空 3 社(ANA,JAS,JAL)では空席情報、予約、航空券の販売まで一連の手続きを WEB サーバを用いて行えるようになっている。しかし、クレジットカードを利用した電子決済(チケットレスサービス)までは 3 社とも事前に会員登録をすることが前提となっている。

これらのサイトで会員登録時の個人情報の入力、電子決済時のクレジットカード番号の入力などはいずれのサーバも SSL で暗号化をしている。

これら、航空 3 社のうち JAS だけが予約内容を電子メールで送付するシステムをとっている。しかしながら、ここでメールを送信するアドレスは予約時に任意に入力したメールアドレスに送信されるので、利用時の ID/パスワード等の情報が漏れ第三者に不正に利用された場合を考えると会員登録時に登録したメールアドレスへも同時に送信した方がより信頼性がある。また、このときに送信されてくる電子メールに電子署名等は一切行なわれないので十分になりすまし、改竄などが可能である。

また、セキュリティに関する対応も各社様々であり、SSL による暗号化を実際の取引のどの部分から行うかに大きな違いがある。これらを表 1-1 にまとめた。

表 1-1

航空会社名	会員登録時SSL	会員LOGIN時のSSL	個人情報入力時のSSL	クレジットカード入力時のSSL
ANA	なし	なし	なし	必須
JAS	選択可(SSL優先)	選択可(SSL優先)	選択可(SSL優先)	必須
JAL	必須	なし	なし	必須

会員登録時SSL：航空券を購入するための会員登録(個人情報の入力)がSSL化されているか

会員LOGIN時のSSL：航空券予約時システムにLOGINする際のID/パスワード入力にSSL化されているか

個人情報入力時のSSL：航空券購入時の氏名などの登録(個人情報入力)がSSL化されているか

クレジットカード入力時のSSL：航空券購入(電子決済)時のクレジットカード番号の入力がSSL化されているか

この表からわかるように各社 SSL による暗号化通信の使用 방법에それぞれ違いがみられる。

できれば、なんらかの基準を設け個人情報に対する保護が必要ではないかと思われる。

特に ID/パスワードの入力が暗号化されていない場合があるのでこのとき、経路上でデータの盗聴が行なわれると他人になりすまされて予約をされる可能性がある。

電子商取引の販促サービス

電子商取引によるショッピングモールを運営しているサイトのサービスでは、掲載商品を「友達にメールですすめる」という機能が用意されている、この機能は商品の購入等を行わなくても WEB サーバを利用して掲載商品への URL とメッセージを電子メールで送信する事ができる。他のサイトやグリーティングカードのサイト等でも WEB サーバから電子メールを出す機能を持っているものがあるが、サイトによっては、簡単に電子メールを「なりすまし」をして送信することができる。

機能としては WEB サーバから掲載商品の「友達にメールですすめる」を選択すると、電子メール送信画面が表示され、ここで送信先のメールアドレス、本文、送信元(From:)メールアドレスを入力して送信することができる。

これらの入力が行われた後にメールを送信することができる。

ここで、問題なのは送信された電子メールの From:等の送信者アドレスに電子商取引サイトの情報は一切なく WEB 上で指定された、送信元(From:)メールアドレスしか受信者には表示されないことにある。仮に、送信元(From:)アドレスに他人のメールアドレスを指定して送信した場合には完全に「なりすまし」を行なうことができる。またこのシステムはここで送られる電子メールは送信先と送信元のメールアドレスにもカーボンコピー(Cc:)で送信されるので送信元アドレスを、なりすまされた場合には自分が出した覚えのないメールが送信されてくるために疑問には思うかもしれないが、電子メールの Received:ヘッダーに対する知識、MTA の配送に関する知識や電子メールのヘッダー情報等に関して知識のない一般利用者にとってはこのメールがどこから発信された電子メールであることを知ることは非常に難しいと思われる。

このような電子商取引サイトで販売促進等に効果がありそうな機能であるが、利用方法によっては電子メールの「なりすまし」といったことが容易にできてしまうので問題であると言える。

また、ここで使用された送信先メールアドレス、送信元メールアドレスについての扱いが不明確であり、ここで入力されたメールアドレスをこのサイトが独自に収集しているのか、データは破棄されているのかといった個人情報に対する扱いが明確になっていない。

これらの個人情報にの取り扱いに関しては明確にする必要がある。

国内の電子商取引に対する個人的な考察

以下の情報は個人的な見解として参考にして頂きたい。

「現状調査」で航空 3 社を比較したのは鉄道などと違い、航空会社は早い時期からインターネットでの情報発信、チケット予約などに力を入れていたこと、基本的なサービス、仕様に関しては 3 社とも同じなので純粋に 3 社のセキュリティに対する考え方などがわかるのではないかと思います。比較した。

この比較の中で JAS だけが全ての情報を SSL を使用した通信を選択できる。JAS の場合は会員登録、予約等を選択した時点から全てのセッションで SSL を使用する事が可能であり、特に 3 社の中では唯一会員の ID/パスワード入力時から SSL を使用する事が可能で、情報の盗聴には十分配慮されていると言える。また、SSL を使用しない場合でも実際の航空券発行時のクレジットカード番号入力が必要な場合は SSL は必須となっている。

また、予約の確認を電子メールで送信しているのは JAS だけあるが、この場合電子署名等はされていないが、WEB のシステムだけでなく電子メールを利用して個人に対して確認を行っているところには、配慮がみられる。前述したが可能であればこのときに電子メールを送信先は会員登録時のアドレスに対しては必須とし、さらに電子署名をし改竄、なりすましなどに対処するのが望ましいと思われる。

JAL の場合は会員登録時個人情報の入力は SSL を使用しているので安全の様に思えるが実際には予約時に氏名電話番号等の情報が必要となるのでこれらの個人情報を守っているとは言えない。

ANA の場合に関してはクレジットカード番号の通信時だけが SSL で暗号化されてそれ以外の個人情報に関して SSL は使用されていない。

また、この 3 社のなかで会員登録後のパスワードの変更が可能なのも JAS のみでそれ以外は再登録となっている。JAS の場合は会員 ID、氏名、登録時の電話番号、生年月日のチャレンジを行ない、パスワードを変更することができる。

電子商取引ではここで紹介した SSL で暗号化した通信を使用する以外にもクレジットカード会社が推奨する SET(Secure Electronic Transaction)があるが、システムが複雑になること、初期導入コストが高いことなどから現時点で SET を利用している電子商取引サイトはほとんどない。

全般的に電子商取引ではクレジットカード番号の通信等実際の決済情報に関してのみ SSL を用いた暗号化が行われているが、クレジットカード番号等と同様に保護が必要な、個人情報に関しては取扱いに明確なガイドラインがないこともあり、十分な配慮がなされていない。これに関しては電子商取引サイトのみならず、インターネット上で個人情報を収集する場合の収集方法、収集後のデータの扱い(保存場所等)、データの使用等に対して何らかしらのガイドラインが必要と思われる。また、販促を目的とした電子メールの利用に関しても「なりすまし」等が可能なシステムがあるので、これらのシステムを作成する場合のセキュリティ上のガイドライン、また広告メール等に対するなんらかのガイドラインが必要と思われる。

海外の電子メールの電子商取引における活用について

米国ではインターネットを用いた電子商取引が盛んに行われている。特に書籍等の販売を目的とした amazon.com が近年有名である。また通信販売以外にもホテル予約などが行われている。

amazone.com に関して

amazone.com は書籍などの通信販売で有名である。このサイトでは商品の購入を選択した時点で SSL による経路の暗号化が行われる。ただし、他のサイトでも見られることであるが一部のファイアウォールでは SSL による経路の暗号化が出来ないサイトがあるため、これらのサイト用に SSL を使用しないで接続可能な方法も残してある。ただし、基本的には SSL での接続に誘導するようにコンテンツは構成してある。

このサイトで商品を購入すると連絡用の電子メールアドレスの入力が求められ、商品購入後に電子メールで住所、氏名、電話番号、購入商品、購入金額などの個人情報を含む電子メールで送付されてくる。その後、購入商品の発送時に前回の電子メールの内容にくわえて国際宅配便のトラックナンバー等の情報が送られてくる。また、これらの電子メールに対しては電子署名などは行われておらず、十分になりすましが可能な状態にある。

thisco.com に関して

thisco.com はホテル、航空券の予約が可能なサイトである。このサイトでの予約可能なホテルは米国国内だけでなく登録されている世界各国のホテルの予約が可能である。Hyatt, Westin 等の世界的なホテルチェーンもこのサイトのシステムを使用しているようである。

このサイトにでも予約者の個人情報の入力、クレジットカード番号等の入力時は基本的に SSL での接続が行われるが、同様の URL を HTTPS から HTTP へ変更してみると同様の処理が行なえるのでやはり、SSL が使用できないサイトへの配慮が見られる。

SSL 等が使用出来ないサイトの問題

現在、電子商取引を行っているサイトのほとんどが住所、氏名などの個人情報、決済のためのクレジットカード番号などの入力には SSL 等を使った暗号化通信が行われている。この SSL 等による暗号化は従来の TCP/IP の 80 番ポートを使用した HTTP 通信ではなく、443 番ポートを使用した HTTPS を使用して通信が行われる。最近では SSL 等による暗号化通信が一般的になってきたが 2、3 年前はそれほど使用されていなかったため古いバージョンのファイアウォール等では 443 番のポートを使用した通信が出来ないものもあった。また、製品が対応していたとしても実際は 443 番のポートでの通信を許可していない場合もある。これには 3 つの理由が考えられる。第一には古いバージョンのファイアウォール等を使用していて HTTPS に対応していない場合。第二に使用しているファイアウォールは HTTPS に対応しているがこれを適切に使用できるような設定が行われていない場合。第三に明示的に外部へ HTTPS による通信を禁止したい場合。が考えられる。現在のインターネットの利用状況などから考えると第三の HTTPS による通信を明示的に禁止している場合は少ないと思われる。ほとんどの場合は第一、第二の原因による場合がほとんどと思われる。これは、ファイアウォール等の導入は行うがその後ファイアウォールに対して適切な保守(設定変更、バージョンアップなど)を行っていないことが原因として考えられる。

2. X.509 電子証明書の問題調査

X.509 の解説

インターネットの普及に伴い公開鍵暗号方式は必須の技術となってきた。公開鍵暗号方式を利用するには、暗号化・署名の検証などを行うために事前に正しい公開鍵が配布されていることが前提となる。

少数の限られた範囲内での利用であれば、直接対面などの手段により安全に公開鍵を流布することが可能であるが、インターネットのような多数で広範囲に渡る通信においては不可能である。

そこで個人、組織、サーバに対する公開鍵の正当性を保証する信用のおける第 3 者機関 (trusted third party) である認証局 (Certificate Authority) という概念が生まれた。

認証局では利用者と公開鍵の対を認証局(の秘密鍵)によるデジタル署名した「公開鍵証明書」を発行する。公開鍵証明書を検証する側では公開鍵証明書の(認証局による)署名を検証して、公開鍵が正当なものであるかどうか確認することができる。

公開鍵証明書は認証書、証明書などと呼ばれることがある。

このようなしくみを実現した公開鍵証明書の規格の 1 つに X.509 がある。X.509 は ITU (International Telecommunication Union) や ISO (International Organization for Standardization) で標準化されており、ディレクトリに関する一連の規格である X.500 シリーズの 1 つに該当する。

そのためエンティティを識別するために X.500 に基づいた名前空間(X.500 識別名)を利用するのが特徴である。

その他の公開鍵証明書フォーマットとしては SPKI (Simple Public Key Infrastructure) や SDSI (Simple Distributed Security Infrastructure) などが存在するが、S/MIME や SSL などの多くのセキュリティプロトコルが X.509 をベースにしているためデファクトスタンダードとなっている。

X.509 公開鍵証明書は複数のバージョンがある。1988 年に公開されたバージョン 1 は基本的な必須項目が定義され、1993 年に公開されたバージョン 2 ではエンティティの一意性を表わすためのオプションな固有識別子が追加された。

更に 1996 年にはさまざまな情報を埋め込めることのできる追加領域を定義したバージョン 3 が発行されている。現在はこの X.509 v3 公開鍵証明書はよく利用されている。

X.509 は ASN.1 (Abstract Syntax Notation One) と呼ばれる表記法で定義されている。通常 X.509 証明書を保持するには DER (Distinguished Encoding Rules) と呼ばれるコーディング規則にのっとりエンコーディングされたものを利用する。

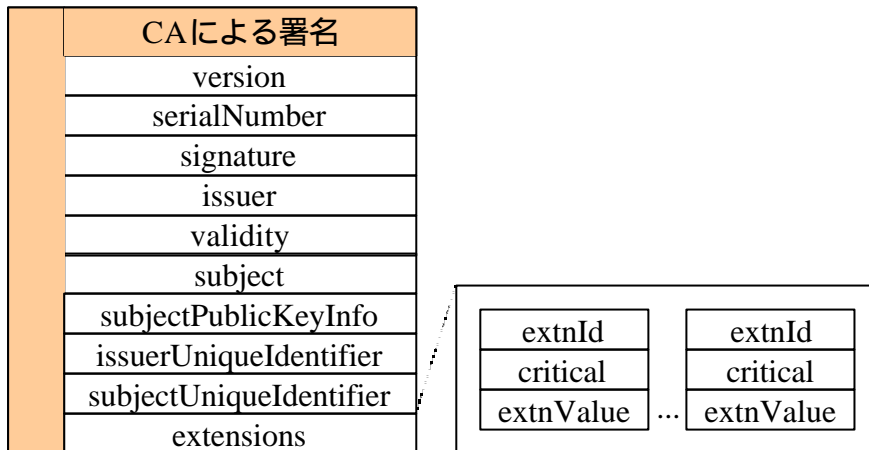


図 1 X.509 v3 フォーマット

それぞれのフィールドに表示される情報を説明する。(図 1 X.509 v3 フォーマット)

version は X.509 のバージョンが入る。このフィールドはオプションであり、省略された場合は v1 を表す。

serialNumber は認証局がユニークに割り当てるシリアル番号が入る。後述する CRL で利用される。

signature は公開鍵証明書の署名方式が入る。

issuer は公開鍵証明書の発行者である認証局の X.500 識別名が入る。

validity は公開鍵の有効期限(開始日時と終了日時)が入る。

subject は本証明書内に含まれる公開鍵に対応する秘密鍵の所有者の X.500 識別名が入る。

subjectPublicKeyInfo は証明する公開鍵が入る。

issuerUniqueIdentifier 及び subjectUniqueIdentifier は v2 から追加されたオプションなフィールドであり、それぞれ認証局の固有識別子, 所有者の固有識別子が入る。

extensions は v3 で追加されたオプションなフィールドであり、拡張型 (extnId)、拡張値 (extnValue) 及びクリティカルビット (critical) の 3 つ組の集合が入る。

X.509 で定められた拡張型には keyUsage(公開鍵の利用目的), subjectAltName(所有者の別名), basicConstraints(認証局かどうかを記入) などがある。

v3 拡張フィールドは X.509 で定められた標準の拡張型だけでなく、独自の新しい拡張型も組み込むことが可能である。

そのため v3 拡張型をどう認識するかはアプリケーション側に依存することとなる。クリティカルビットはその拡張型が必須であるかまたは無視可能かを表わすものである。

X.509 では公開鍵証明書だけではなく廃棄証明書リスト (CRL, Certificate Revocation List) のフォーマット(図 2 CRL v2 フォーマット)も定義されている。X.500 識別名の変更や秘密鍵の漏洩などの理由により公開鍵証明書を通常の有効期限内で無効にする機構を実現する。

CRL には v1 と v2 の 2 つのバージョンが存在する。v2 では CRL の配布場所や廃棄証明書ごとの廃棄理由などを埋め込むことができるようになった。

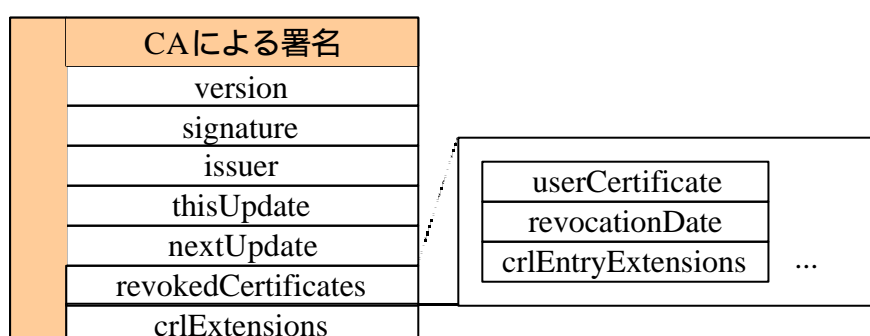


図 2 CRL v2 フォーマット

それぞれのフィールドに表示される情報を説明する。(図 2 CRL v2 フォーマット)

version は CRL のバージョンが入る。v1 ではこのフィールドは定義されていないため存在すれば v2 である。

signature は CRL の署名方式が入る。

issuer は CRL の発行者の X.500 識別名が入る。

thisUpdate は本 CRL の発行日時が入る。

nextUpdate はオプションなフィールドであり、次回の CRL 発行予定の日時が入る。

revokedCertificates は廃棄する証明書のシリアル番号 (userCertificate) と廃棄日時 (revocationDate) の対の集合が入る。

更にオプションで各組に対して拡張情報 (crlEntryExtensions) を入れることができる。例えば CRLReason 拡張型は廃棄理由が入る。

crlExtensions はオプションなフィールドであり CRL に対する拡張が入る。

cRLNumber (CRL の発行通し番号) cRLDistributionPoints (CRL の配布場所や扱う CRL の種類などが入る) などがこれにあたる。

また X.509 では属性証明書 (Attribute Certificate) と呼ばれる公開鍵証明書に類似したフォーマットも定義されている。

公開鍵証明書が公開鍵とその利用者を結びつけるしくみを提供するのに対し、属性証明書は所持者の属性や権限をあらわす証明書であり、属性情報を公開鍵証明書と結び付ける役割を持つ。

現在も標準化が進められている X.509 v3 拡張に対する FPDAM (Proposed Draft Amendment) では X.509 属性証明書に関する部分で大幅な改変が行われており、属性証明書のフォーマットだけでなく各フィールドの詳細やモデルについても触れられている。なおこのドキュメントが正式な形で公開されるのは 2000 年 3 月の予定である。

IETF では PKIX Working Group で X.509 公開鍵証明書を用いた公開鍵インフラの標準化作業が進行中である。1999 年 1 月に RFC Standard Track として RFC 2459 が公開されたほか現在の多くのドラフトが標準化の最終段階に入っている。

RFC 2459 では X.509 公開鍵証明書と CRL のプロファイルが紹介されているだけでなく PKIX WG 独自の拡張型も定義されている。そのほかにもマネージメントプロトコル、オンライン有効性確認プロトコル (Online Certificate Status Protocol) などの標準化が行われている。

SSL の解説

SSL(Secure Socket Layer) は Netscape Communications 社が提案するセキュリティプロトコルであり、暗号化、認証、完全性(改竄防止)を提供する。

OSI 参照モデルでは第 5 層のセッション層に位置し、アプリケーション層から透過的であるため HTTP, FTP, TELNET などのアプリケーション層のプロトコルの下で対応することが可能である。

同様のプロトコルとして EIT (Enterprise Integration Technology) の設計による S-HTTP (Secure HTTP) があるが、HTTP に特化したアプリケーション層のプロトコルであったため汎用性に欠けている。

また 2 大ブラウザである NetscapeCommunicator と InternetExplorer が SSL に対応したこともあり S-HTTP は影を潜め、SSL が WWW で最も利用されるセキュリティプロトコルとなった。

SSL には複数のバージョンが存在する。SSL 1.0 は実装されることはなく、初期の Netscape Navigator (1.0 から 2.x) で SSL 2.0 が組み込まれた。しかし乱数ジェネレータの実装上のバグがあったため、1996 年 3 月と 11 月にこの問題を解決した SSL 3.0 のドラフトが発表される。現在の NetscapeCommunicator では SSL 2.0 と SSL 3.0 の両者が使えるようになった。実装はされたが RFC などへの標準化作業は行われなかった。

SSL と同様のプロトコルとしては Microsoft 社が発表した PCT (Private Communication Technology) という対抗プロトコルがある。PCT は InternetExplorer で実装されたが、SSL が既に普及していたこともあり InternetExplorer 3.0 からは SSL 3.0 もサポートされるようになった。

IETF の TLS Working Group が 1996 年 6 月の 36th IETF 会議で活動を開始し、SSL 3.0 をベースに標準化が進められ、現在 RFC2246 として TLS 1.0 が公開されている。TLS 1.0 ではバージョン番号に 3.1 が使用されており、事実上の SSL 3.1 とも言える。

TLS では PCT 独自機能の付加、Fortezza のサポート中止などの変更点が見られる。

SSL プロトコルは 2 つのレイヤ上に構成される。トランスポート層の直上に SSL Record Protocol が、更に上位層を SSL Handshake Protocol が担当する。

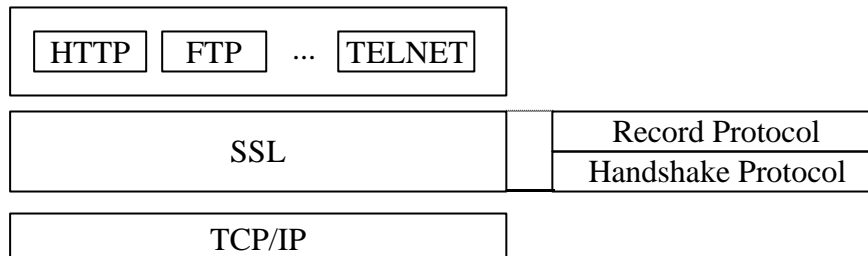


図 3 Leyer

SSL Record Protocol は 2^{14} バイト以下の SSLPlaintext レコードに分割し、データ圧縮、メッセージ認証子(MAC)の生成、データの暗号化などの処理がされ、上位の SSL Handshake Protocol には透過的に行われる。

SSL v3 での SSL Handshake Protocol は次のような処理が行われる。

ClientHello メッセージにてクライアント側でサポートしている暗号化・圧縮アルゴリズムが送信される。サーバ側でその中から選択したあと ServerHello メッセージで送信される。このとき双方でランダムに生成した値も交換しておく。

Certificate メッセージでサーバ自身の公開鍵証明書を送信する。公開鍵証明書が存在しない場合には ServerKeyExchange メッセージで RSA 公開鍵又は Diffie-Hellman 公開鍵が送信される。SSL で使用される公開鍵証明書は X.509 v3 が採用されている。

CertificateRequest メッセージはクライアントに公開鍵証明書の提示を求める場合に用いられる。

ServerHelloDone メッセージで ServerHello メッセージからの一連の送信が終了したことをクライアントに伝える。

クライアントは CertificateRequest メッセージを受け取った場合に限り Certificate メッセージを送信する。クライアントが公開鍵証明書を持っていない場合にはここで Alert を返却する。

クライアントは 48 ビットの PreMasterSecret データを生成し ClientKeyExchange メッセージで送信する。

CertificateVerify メッセージはクライアントの公開鍵証明書の検証を行う際に利用される。

Finished メッセージは SSL Handshake Protocol が終了するときに送信される。

ChangeCipherSpec メッセージは使用する暗号化・圧縮アルゴリズムを変更する際に送信される。
新規セッション確立時の SSL Handshake Protocol 中にも利用される。

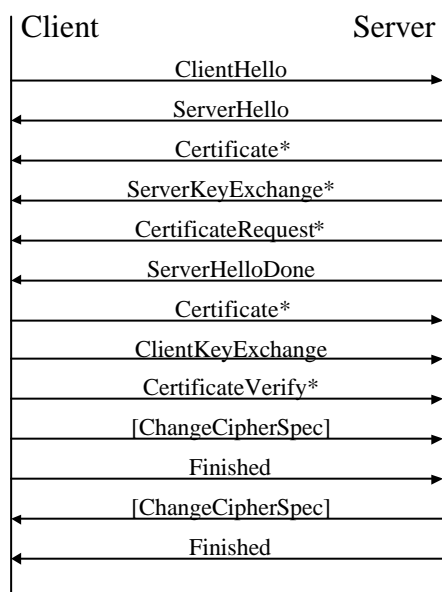


図 4 SSL Handshake

つぎに SSL 2.0/3.0 にて RSA とともに使用可能な暗号アルゴリズムとハッシュアルゴリズムの組 (cipher suite と呼ばれる) を紹介する。

Cipher suite		SSL 2.0	SSL 3.0
3DES_EDE_CBC_SHA			
DES_CBC_MD5			×
DES_CBC_SHA		×	
IDEA_CBC_MD5			×
IDEA_CBC_SHA		×	
RC4_128_MD5			
RC4_128_SHA		×	
RC2_CBC_128_MD5			×
輸出用	DES_CBC_40_SHA	×	
	RC4_40_MD5		
	RC2_CBC_40_MD5		
暗号化 なし	NULL_MD5	×	
	NULL_SHA	×	

図 5 RSA cipher suite 一覧

SSL 3.0 ではセッション鍵交換用として Diffie-Hellman 及び Fortezza が、認証用として DSS/DSA がサポートされている。

S/MIME の解説

S/MIME (Secure Multipurpose Internet Mail Extensions) は RSA Data Security 社が提案する PKCS (Public Key Cryptography Standards) という暗号技術標準を利用して MIME に対してデジタル署名や暗号化を施すための 1 規格である。

2 大ブラウザである NetscapeCommunicator と InternetExplorer に付随するメーラが S/MIME に対応したことにより急速に広まった。日本ではその他に S/Goma (オレンジソフト)、魔法便 (NTT エレクトロニクス)、SecureMessenger (株式会社アイフォー)、AT 承認メール (アライドテレシス) などのメーラ/プラグインソフトが対応している。

また S/MIME 対応 InternetFAX (松下電送システム) が製品化されている。

同様に MIME に対するデジタル署名及び暗号化の規格としては MOSS (MIME Object Security Services) が RFC 1848 で規定されているが現在はほとんど利用されていない。実装としては FEAL for EUDORA PRO (NTT アドバンステクノロジー) というプラグイン製品がある。

その他の暗号化電子メールの規格としては RFC 1421 から 1424 で規定された PEM (Privacy Enhanced Mail)、PGP (Pretty Good Privacy) を MIME 対応した PGP/MIME (RFC 2015) などがある。

PGP では公開鍵に対する信用の輪 (web of trust) をユーザ自身が形成していく方式に対し PEM 及び S/MIME では、公開鍵の認証する信用のおける第 3 者機関である認証局 (Certificate Authority) が公開鍵を保証する。

S/MIME における公開鍵の配布には認証局のデジタル署名が施された X.509 v3 公開鍵証明書が用いられる。

S/MIME は 1995 年に RSA Data Security 社を中心としたベンダーのコンソーシアムの手により生まれた。その後 IETF の S/MIME Working Group で議論され、現在は S/MIME version 2 として RFC 2311 (S/MIME v2 のメッセージ規約)、RFC 2312 (S/MIME v2 における証明書処理の規約) の 2 つの RFC が標準化された。

これらの RFC では上で紹介したように PKCS に準拠しているため、同時期に次の 3 つの仕様が参考文書として公開されている。

RFC 2313 (PKCS#1, RSA 暗号化規約)、RFC 2314 (PKCS#10, 公開鍵証明書を発行要求するためのフォーマット規定) そして RFC 2315 (PKCS#7, メッセージのデジタル署名と暗号化を施すためのフォーマット規定) である。

しかしこれらの仕様はすべて Informational RFC であるが Standard RFC ではない。

その理由として RSA は米国での特許が RSA Data Security 社に属しているが、S/MIME v2 は公開鍵暗号方式として RSA が必須となっている点が挙げられる。

また S/MIME v2 では共有鍵暗号方式としては RC2, RC2/40 (以上、必須) や DES, Triple-DES(EDE3 CBC, 168bits) が利用され、ハッシュアルゴリズムとしては MD5, SHA-1 のサポートが必須となっている。

このような背景のもと S/MIME Working Group では現在 S/MIME v3 の標準化が進められており、RSA 暗号や 40 ビットの弱い秘密鍵暗号を利用しない方式が採用され Standard RFC として公開されると言われている。

実際 S/MIME v3 では Diffie-Hellman/DSS を暗号化、署名アルゴリズムとして SHA-1 をセキュアハッシュ関数として採用する方向で標準化が進められている。

RFC 2315 (PKCS#7) では異なる 6 つのコンテンツタイプを規定しているが、S/MIME で利用されるのは SignedData (デジタル署名)、EnvelopedData (暗号化)、SignedAndEnvelopedData (デジタル署名 & 暗号化) の 3 つである。

RFC 2311 で新たに application/pkcs7-mime, application/pkcs7-signature, application/pkcs10 の 3 つの MIME タイプが導入された。

application/pkcs7-mime は添付ファイルの拡張子を .p7m にすることで SignedData 及び EnvelopedData タイプの PKCS#7 オブジェクトを送信することができる。

application/pkcs7-signature は multipart/signed MIME タイプ (RFC 1847) に入れ子で SignedData タイプの PKCS#7 オブジェクトを組み込む場合に用いられ、拡張子は .p7s となる。

application/pkcs10 は RFC 2312 に基づいた証明書発行要求フォーマットである PKCS#10 オブジェクトを送信する際に用いられる。その返答には application/pkcs7-mime で拡張子を .p7c にしたものが用いられ、公開鍵証明書や CRL を含んだ SignedData を送信される。

MIME タイプ		拡張子
application/ pkcs7-mime	signedData, envelopedData	.p7m
	signedData(certs-only)	.p7c
application/pkcs7-signature		.p7s
application/pkcs10		.p10

図 6 MIME タイプ一覧

SSL と S/MIME で、電子証明書を引き継ぐことの技術的可能性について

PKCS#12 は秘密鍵や公開鍵証明書のバックアップや他のマシンへの移行するために適した規格である。NetscapeCommunicator 4.04 以降と InternetExplorer 4.0 以降でインポート/エクスポートともに PKCS#12 が使用されている。

PKCS#12 が公開される以前に Microsoft PFX0.020 という規格が存在していた。

PFX (Personal Exchange Syntax and Protocol Standard) は秘密鍵や公開鍵証明書などに限らず、クレジット番号などの個人情報を格納するための規格である。

Microsoft の仕様であったが NetscapeCommunicator 4.03 以前でのみ実装が行われなかった。当時は PKCS#12 が存在していなかったため PFX に基づいて実装されていたようである。

その後 PFX をベースに PKCS#12 の標準化が行われた。

相互運用性を考慮して NetscapeCommunicator 4.04 以降及び InternetExplorer 4.0 以降はインポートする場合に限り PFX がサポートされている。これらのバージョンにおいてはエクスポートする場合に PFX は利用されず PKCS#12 が用いられる。

そのため NetscapeCommunicator 4.04 以降及び InternetExplorer 4.0 以降のブラウザから PKCS#12 でエクスポートした PKCS#12 ファイルは NetscapeCommunicator 4.03 以前では利用できない。また Netscape 3.x 及び InternetExplorer 3.x はこのようなインターフェイスは存在していない。

ブラウザの種類		PFX		PKCS#12	
		import	export	import	export
Netscape Communicator	4.03 以前	×	×		
	4.04 以降				×
Internet Explorer4.0 以降					×

図 7 PFX/PKCS#12 対応一覧

PKCS#12 は 秘密鍵格納のために PKCS#8 を利用する。しかし RSA の鍵しか対応していないため DH/DSS などに適用するためには PKCS#8 を拡張した PKCS#11 が利用されている。

PKCS#12 で使用されるハッシュアルゴリズムは SHA-1 であり、秘密鍵暗号方式は RC4/128, RC4/40, Triple-DES(2key), Triple-DES(3key), RC2/128 及び RC2/40 であるが、暗号輸出規制により使用できるアルゴリズムが制限されている。

InternetExplorer においては、インポートする場合はすべてのアルゴリズムにサポートしているが、米国内版/輸出版ともにエクスポートする場合は RC2/40 のみサポートしている。

NetscapeCommunicator においては、米国内版/輸出版ともにエクスポートする場合には証明書の暗号化には RC2/40 が、秘密鍵の暗号化には Triple-DES(3key) が使用される。

インポートする場合、米国内版ではすべてのアルゴリズムにサポートしているが、輸出版の証明書の暗号化には RC4/40 と RC2/40 しかサポートしていない。

ブラウザの種類		証明書の暗号化	秘密鍵の暗号化
Internet Explorer	import	すべて可	すべて可
	export	RC2/40	RC2/40
Netscape Communicator	import	すべて可	すべて可
	import (輸出版)	RC2,RC4/40	RC2/40
	export	RC2/40	Triple-DES

図 8 使用アルゴリズム一覧

InternetExplorer から NetscapeCommunicator に PKCS#12 で証明書/秘密鍵を移行した場合、インポート作業は成功するが S/MIME や SSL を利用する際に不都合が生じることがある。

NetscapeCommunicator では X.509 v3 証明書の独自拡張として nsCertType が用いられており証明書の用途に関する情報が組み込まれている。

そのため SSL client(bit-0) や S/MIME(bit-2) のビットが立っていない場合に Netscape では SSL や S/MIME 機能が利用できない。

InternetExplorer から NetscapeCommunicator に移行する場合には公開鍵証明書の v3 拡張における nsCertType が必要となる。

PKCS#12 に対応している実装は NetscapeCommunicator や InternetExplorer のほかフリーの暗号ライブラリである OpenSSL が存在する。

X.509 電子証明書の互換性

現在公開鍵証明書を利用するセキュリティプロトコルやアプリケーションは X.509 バージョン 3 がよく用いられている。v3 では extensions というオプションなフィールドが設けられ、アプリケーション又はプロトコル独自の新しい拡張型を組み込むことが可能となった。

X.509 では標準的な v3 拡張型がいくつか定義されている。電子メールアドレスや IP アドレスを subjectAltName に別名として組み込むことができる。また CA の証明書では、CA かどうかを示すフィールドとして basicConstraints が利用される。

独自の拡張型だけでなく、これらの標準的な拡張型の利用もアプリケーションやプロトコルに依存しており、クリティカルビットの有無により検証などの動作が異なっている。

SET では標準 v3 拡張として authorityKeyIdentifier, keyUsage, privateKeyUsagePeriod, certificatePolicies, subjectAltName, issuerAltName, basicConstraints, cRLNumber が、また SET 独自として hashedRootKey, certificateType, merchantData, cardCertRequired, tunneling, setExtensions が規定されている。

これらのうち keyUsage, basicConstraints, hashedRootKey, certificateType にクリティカルビットが必須ということになっている。

Netscape Communicator では authorityKeyIdentifier, basicConstraints, cRLDistributionPoints, extKeyUsage, keyUsage, subjectAltName, subjectKeyIdentifier が用いられている。これらのうち subjectAltName が証明書の subject フィールドが空である場合に限りクリティカルビットが必須となっている。

そのほか extKeyUsage ではクリティカルビットがマークされているかどうかで解釈が異なる。マークされている場合には、証明書は表示されている目的の一つでしか利用できない。マークされていない場合では忠告として扱うだけで証明書の目的を制限することはない。

Netscape Communicator では更に独自拡張として netscape-cert-type, netscape-comment が利用されている。これらの拡張型は 1997 年 8 月に Netscape 社の Jeff Weinstein がドラフトとして公開された。このドラフトでは上の 2 つのほか netscape-base-url, netscape-revocation-url, netscape-ca-revocation-url, netscape-cert-renewal-url, netscape-ca-policy-url, netscape-ssl-server-name が定義されているが、これらは廃止 (obsolete) されている。

netscape-cert-type は証明書の利用を制限するために設けられておりビット列により 0: SSL クライアント, 1: SSL サーバ, 2: S/MIME クライアント, 3: オブジェクトサイン, 4: 予約済, 5: SSL 認証局, 6: S/MIME 認証局, 7: オブジェクトサイン認証局 という定義がされている。

この netscape-cert-type 拡張は extKeyUsage や basicConstraints 拡張に取って変わられているが Navigator 3.x では必須となっている。

この拡張が存在する場合は指定用途以外の利用は制限される。また、この拡張が存在しない場合でもオブジェクトサインとしての利用は制限される。

認証局の証明書としての利用を目的で付けられる拡張としては `netscape-cert-type` と `basicConstraints` 拡張の 2 つが存在することになるため、次のように定められている。この 2 つのうち片方のみ組み込まれている場合には、その拡張型どおりに動作する。仮に 2 つの拡張型ともに存在しない場合には、認証局の証明書として利用しない。

また 2 つとも含まれていた場合には、2 つとも解析してどちらかに認証局の表示があれば認証局証明書として利用する。

Netscape Communicator では CRL にも X.509 で定義された標準的な拡張型が利用されている。CRL 拡張として `authorityKeyIdentifier`, `CRLNumber`, `deltaCRLIndicator`, `issuerAltName`, `issuingDistributionPoint` が、また CRL Entry 拡張として `certificateIssuer`, `holdInstructionCode`, `invalidityDate`, `reasonCode` が利用されている。

ユーザー(消費者)利用者の観点からの課題

現在インターネットにおいては電子商取引が活発に行われており、即時注文決済を行うバーチャルショップも登場している。消費者であるユーザ側では、インターネットがオープンな場であることの認知度が高まり「インターネットは危険」という意識も広まりつつある。

ユーザのこれらの不安を解消するためにモールではあらゆる方法でセキュリティを確保していることを宣言してユーザの安心感を得ている。実際には暗号技術を駆使することで実現されるが、ユーザからはブラックボックス化されているためどのくらい安全なのかについての尺度を持つことはできないかもしれない。

これまでに紹介した SSL や S/MIME などのセキュリティプロトコルだけでなく SET (Secure Electronic Transaction) などの電子決済に特化したプロトコルも提案されており、安全な商取引を可能にする仕組みは提供され整備されつつある。

SSL, S/MIME 及び SET といったプロトコルの安全性の根拠となる大前提として、認証局を信用する必要がある。

Internet Explorer や Netscape Communicator ではこの信用の基点となる認証局の証明書がいくつか組み込まれており、デフォルトで信用するというフラグをつけて配布されている。ユーザ側では SSL でセキュリティサイトにアクセスしていることさえわかりづらい状況である。

電子商取引を行う際にはスケーラビリティが要求される。すなわちモール側では不特定多数に対して商取引を行いたいのである。そのためにこのようにブラウザに認証局の証明書を組み込む方法が取られている。

電子商取引などのような広い範囲での利用ではなく、ある閉じた範囲内で有効であればよい場合もある。実際プライベート CA などと呼ばれる社内 CA の構築がこの一例である。

社内で稟議書をまわすなどの社内業務でのセキュリティ(認証と暗号化)を確保する目的で利用するのであればこの方法で十分である。しかし閉じた世界(=社内)でしか通用しない公開鍵証明書であるため、社外では何の効力も持たないこととなる。

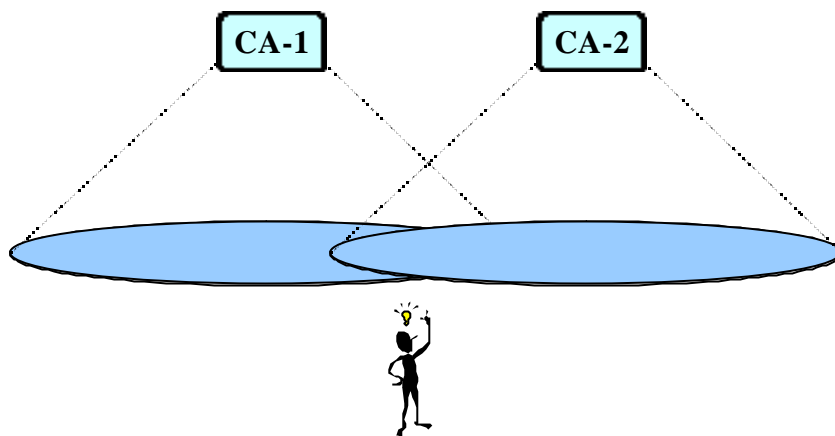


図 9 認証局

これは証明書の検証者が証明書の発行主体つまり認証局を信用するかどうか依存しているためである。現在も複数の認証局が乱立しており、公開鍵証明書の形式や検証方法は同じでも、主体も運営方針も異なっている。

認証局は信用の基点となる役割を持つ。ユーザは多くの認証局の中から自分の信用のおけるものを選択し、信用せねばならない。どの認証局の傘下に入るかどうかを決めるのは個人に任せられている。しかし Internet Explorer や Netscape Communicator の製品に既に組み込まれているように、この作業を怠っているのである。

先に述べた社内認証局の応用例として相互認証を紹介しておく。A社、B社ではそれぞれA社CA、B社CAが運用されている。A社の社員aはB社の社員bの証明書を検証したいがB社CAから発行された証明書であるため検証できない。

そこでA社CAではA社CA → B社CAという証明書を発行し、A社内に流布しておけば、B社内でもしか通用しなかったB社証明書がA社内でも効力をもつことができる。

B社でも同様の操作をすることで相互にやりとりすることができ、企業間取引などの用途で有効である。

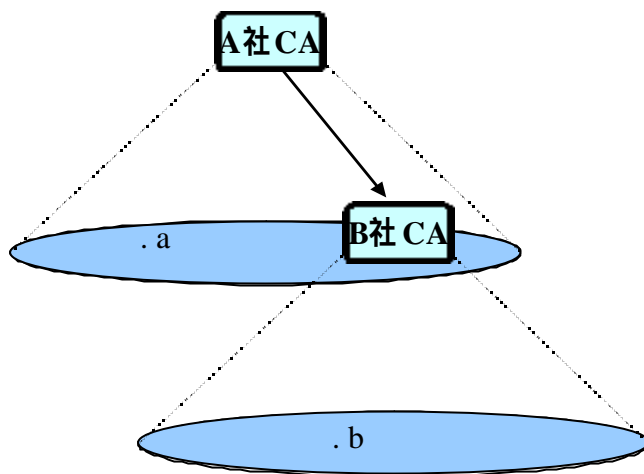


図 10 相互認証の例

しかし1社1社ごとにこのような作業を行うこと方式は煩雑かもしれない。つまり企業間でのやり取りの際には同業種で信用のポイントとなる認証局を立ち上げて利用するという少し大きなスケールビリティを持ったインフラが有効である。

このように認証局の傘の大きさ(有効範囲)によって用途を変えた運用が必要である。

暗号技術を用いることで、仕組みとしては安全にクレジット番号などの個人情報を安全に守ることができたとしても、ユーザが伝える相手すなわちモール側で適切な利用がされているかについては保証されない。

途中の経路は安全に守ってもプライバシー情報の流出は防ぐことができず運用・体制の仕組みでカバーする必要がある。

このようなプライバシー保護問題を解決するためにプライバシーマーク制度が存在するが、世間への認知度は低い。これもユーザ側の意識が低いためと思われる。

セキュリティを確保するためには、ユーザ側の煩雑さと安全性の確保は相反するところがある。しかし使いやすさ・わかりやすさを追求するのではなくユーザの意識を高めることが先決であり、このような啓蒙活動は重要である。

3. 商用電子メールのプライバシーの問題

電送路上でデータの盗聴の可能性について

インターネット上の電子メールの配送には一般的に SMTP(RFC821)を使用し MTA 間で転送が行われる。この MTA 間でのメール転送時は現状ではデータの暗号化及び認証は一切行われていない。したがってこの電送路上で第三者による盗聴される可能性がある。

特にネットワーク上のデータの盗聴に関しては今までは一部の管理者等しか使用する権限を持っていなかった障害調査を行うためのネットワークモニタリングツール(tcpdump 等)を、近年の PC-UNIX の普及(Linux,FreeBSD 等)により、これらのオペレーティングシステムをインストールすれば誰(だれ)でも管理者権限を得ることができるのでこれらのツールを容易に使用することができる。

したがって悪意を持ってこれらのツールを使用すればネットワーク上のデータを盗聴することが可能となる。

これらのツールによる盗聴はインターネットを介して行われる場合と内部から行われる場合がある。一般的にインターネットを介した外部からのネットワークの盗聴に関しては外部に公開されているサーバマシン等を適切に設定あるいはファイアウォール等を使用して外部からの侵入を防御することで対策することは可能であるが、内部にこれらのマシンを設置され盗聴を行われた場合は無防備な場合が多い。

これらを物理的に対策するには基本的に以下の 2 点の対策を行なう事が必要と思われる。

1. サーバマシン等を設置してある部屋への入室制限及び入室管理。
2. サーバマシンが接続されている HUB を SwitchingHUB を用い、ポート単ぐらいいで接続できる機器の MAC アドレスを登録し許可された機器以外の接続を拒否する。

最低限上記のような方法を用いれば、内部からの盗聴に対する可能性は完全とはいえないが低くなる。

電送路上の暗号化の必要性について

特に電子商取引を行ううえで電子メールを利用する場合、電子メールにクレジットカード情報等が記述されていなくても、一般的に電子商取引内容の確認のために利用者(消費者)の住所、氏名、電話番号等の個人情報及び購入商品名等が記述されている。

これら情報は利用者(消費者)の個人情報であり、電子商取引サイトから利用者(消費者)に通知する場合は第三者への漏洩に関しては十分に注意する必要がある。

また、配送経路上において盗聴の可能性の他にインターネットで電子メールを配送する場合には DNS¹ の MX レコード(図 11 MX による配送参照)が使用される、これは MTA² が当該の電子メールを配送する際にどの MTA に配送するべきかを知るための情報である。この MX レコードは自組織の MTA がなんらかのトラブルで電子メールの配送が受け付けられない場合に備えてセカンダリーを指定してあるのが一般的であるし、また推奨されている。このセカンダリーには一般的(広く)に自組織が契約している ISP(Internet Service Provider)のメールサーバを指定している。この場合の電子商取引サイト、利用者(消費者)の所属するサイト両方の場合の問題点を考察する。

電子商取引サイト

利用者(消費者)から電子商取引サイトに電子メールが送信されたが、なんらかの理由により電子商取引サイトで電子メールの受信が出来ないで DNS の MX でセカンダリーにしていされているメールサーバに配信される場合がある。

この場合、電子商取引サイトとしてメールシステムも含めセキュリティに配慮して構築した場合でもセカンダリーとして指定されているメールサーバに配信されたデータに関しては、セカンダリーとして指定されたメールサーバのセキュリティが適用されるので注意が必要である。

例えばセカンダリーサーバとなっているサーバが第三者に侵入可能な場合以下の様な事が考えられる。

攻撃対象のサーバの SMTP ポート(25 番ポート)に DoS³を送り受信不能にしセカンダリーサーバに転送させ、セカンダリーサーバないの情報を改竄する。

この場合、電子商取引サイトに残る記録は SMTP に対する DoS のみであり、利用者(消費者)からの電子メールの改竄が行われた痕跡は発見されない。また、DoS に関しても Syn Flood⁴によるハーフオープンによって攻撃された場合は記録に残らない場合が多い。

¹ DNS: Domain Name System

ホスト名と IP アドレスの対応、IP アドレスとホスト名の対応等を行なう。

Unix の bind が一般的に使用されている。Unix の bind ではバージョン 4.x の実装ではセキュリティホールがあることが知られているので、バージョン 8.x 以上を使用するのが望ましい。

² MTA Mail Transfer Agent

電子メールの配送を行なうプログラムをいう。Unix の sendmail 等が一般的に使われている。

³ DoS: Denial of Service

一般的に相手のサーバのサービスを使用できなくする攻撃をいう。

また「なりすまし」を行う場合は電子商取引サイトのメールサーバに直接配送するのではなく、組織外のセカンダリーとして指定されていた場合はセカンダリーサーバに配送し、セカンダリーサーバより電子商取引サイトに配送させた方が残される記録が少なくなる。

これらのことから、電子商取引サイトではMXに指定するセカンダリーサーバも含めて自組織で運営していれば、これらの対策も行うことが可能であり、またログの解析もできるので外部組織で運営するのではなく自組織で運営するほうが望ましい。

これらのことから電子メールの盗聴、改竄が行われる可能性は配送系路上だけでも複数に渡る可能性があるためこれらの情報は適切な暗号化による盗聴対策又は電子署名等による改竄の防止策が必要である。

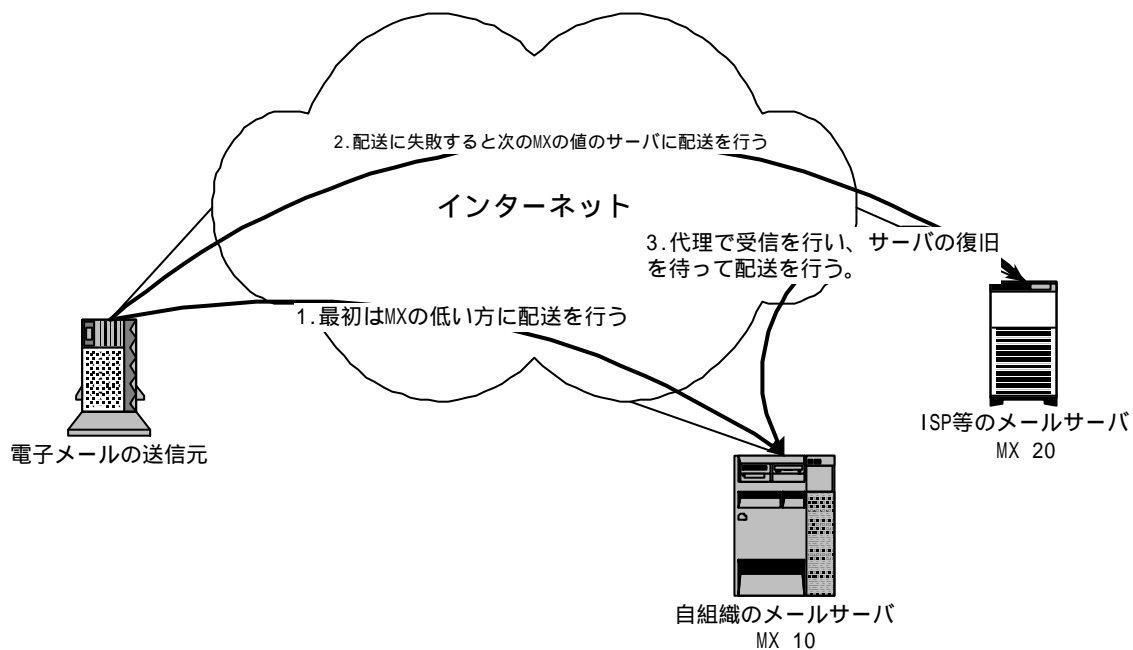


図 11 MX による配送

DNS MX レコードについて

現在いくつかの企業のMXを調査するとMXとして登録してあるサーバが1台のところも見られる。これに関して従来はメールサーバがダウンしている場合などを考慮して複数台のメールサーバで受信できるようにしていたが、現在は1台で運用されているところが見られる。

⁴ Syn Flood

TCPの3ウェイハンドコネクションを悪用した攻撃で初期のセッション開始要求のデータを大量に送信し、相手のサーバのサービスを停止させる攻撃。

これは、ファイアウォールが組織宛のメールを一括して受信して内部(ファイアウォール内)に転送している場合があるのでこの様な運用を行なっているものと思われる。

この運用に関してはほとんどの組織でファイアウォールを二重化するなどの冗長な構成を取ってはいないので組織のファイアウォールがダウンすると電子メールの送受信が不可能になる可能性がある。また、ファイアウォールでDNSも運用している場合はファイアウォールがダウンすることでその組織の Internet 上でサービスが停止することが考えられる。

エラーメールのプライバシー問題

商取引サイトから利用者(消費者)に送られる電子メールに限らず、電子メールは配送経路上でなんらかの理由で配送不能となり発信者アドレス及び配送系路上通過した MTA の管理者に通知される場合がある。

この場合の問題点は配送不能となった電子メールが発信者が本来意図していない、MTA の管理者(場合によっては組織外部の管理者)に送信されることである。また、MTA の管理者が組織内であったとしても MTA 管理者が該当する電子メールの内容を閲覧可能な権限(マシンの権限ではなく組織内の情報閲覧の権限)を持たない場合があることである。

したがって、電子商取引を行うサイトでは、自組織内でこれらのエラーメールを誰が受信(管理)しているか、どのような管理、対応が行なわれているかを把握しておくことが必要である。

対策技術の紹介

インターネットを利用した電子商取引における電子メールの利用において盗聴、なりすまし足しに対する危険性はインターネット構造的(複数のネットワーク事業者の集合)な問題である。

このような状況で電子商取引を行う場合にはデータのやり取りを SSL 等を利用して暗号化した通信が行なわれるが、電子メールの場合も、暗号化、電子署名などを行なうことでこれらの危険性がから電子メールの内容を守ることができる。

電子商取引サイトにおける、電子商取引メールを利用する場合、いくつかの技術が考えられるが通信の暗号化において X.509 証明書を用いた認証が用いられているので電子メールの場合にも同様に X.509 を用いた S/MIME による電子署名、暗号化を行うのがサーバの X.509 証明書と同じ証明書を使用できるので、利用者は同じ X.509 証明書で認証できるので、利用者が複数の証明書を使用する等の混乱がないので望ましいと思われる。

現状では、電子メールに電子署名等の技術を使う人は少ないのでこれらの技術の発展、電子メールの「なりすまし」防止のためにも啓蒙が必要と思われる。

電子商取引サーバの運用上の課題

電子商取引を行うサーバではサーバマシン、そのものへの不正アクセス対策と蓄積されたデータの運用管理(保存期間等)の2点を考える必要がある。

電子商取引を行うサーバには利用者(消費者)の個人情報や、クレジットカード情報等の重要な情報をサーバ上に蓄積することになる。したがって、電子商取引を行うサーバの運用管理を行う場合にはいかに、これらの個人情報を不正アクセス等から保護するかが課題となる。

また、運用としては既に取引の終了したクレジットカード情報、個人情報等をどの時点でサーバから削除するか等の運用規定を明確にする必要がある。

また、これらのデータは特にインターネットに公開されたサーバ又はインターネットからアクセス可能なサーバに蓄積しておくことは常に第三者による不正アクセスにさらされているので取引が終了したデータはなるべく早くインターネットからアクセス可能なサーバからは削除すべきである。

しかし、実際には電子商取引を行ううえでは過去の顧客の購入履歴などを利用したサービスは重要な顧客サービスとなるので兼ね合いが難しいところである。

電子商取引を行うサイトを構築する場合には一般的に利用者(消費者)の情報を格納するデータベースサーバとWEBサーバを分けて運用したほうが望ましい。

電子商取引サーバにはSSL等による暗号化通信のための秘密鍵/公開鍵が保存される。電子商取引サーバにおいてこの秘密鍵の管理は厳重に管理する必要がある。

電子商取引を行うサーバのみに関することではないが、これらのサーバに関しては不必要なサービス(デーモン)を起動しない、不要なポートに対してフィルタリングを行う等の侵入対策を適切に行う必要がある。

また、これら侵入対策だけでなくDNSサーバに対する侵入、DNSなりすまし等にも注意をする必要がある。WEBサーバなどをいくらガードしてもDNSサーバのデータを改竄されてしまっている意味がない。

4. 他人になりすました商取引電子メールの問題

サイトになりすました商取引電子メールの消費者への問題

電子メールを利用した広告は利用者を特定して効果的に情報が伝えられる、PUSH型の広告として効果の高い広告方法として利用されている。特に電子メールを利用した広告は従来の郵便を利用した広告よりも、費用及び即時性においても非常に手軽で有利な広告媒体として利用されている。

電子商取引サイト又は電子メールを利用した広告(電子メール新聞等含む)を送信する側は前項のような電子メールの改竄、「なりすまし」の可能性に関しては可能性を考慮、検討、対策は行われていないのが現状である。

電子メールの改竄、なりすましに関して検討が対策が行われていない問題としては、S/MIME等の、暗号、電子署名技術が一般に認識がされていない点と、これらの技術を用いるには特別な(専用ソフト等)が必要かのような誤った認識がある。

しかし、インターネットで利用されている電子メールソフトは Netscape, Outlook Express 等のシェアが大きく、これらのソフトは標準で S/MIME 機能をサポートしているので電子署名を検証することができる。

したがって「なりすまし」等による大きな被害、事件等が発生する前に、これらの技術の使用を啓蒙する活動が必要あり、そのためにはこれらの技術の実証実験等も必要と思われる。

商取引電子メールによる電子商取引サイトにおける影響

電子商取引サイトにおいて利用者(消費者)との連絡は電話等による通信手段を用いるよりも電子メールを用いたほうが、電子商取引サイト、利用者共に効率的であり特に電子商取引サイトにおいては電話等による、一対一の対応よりも効率化がよいことから電子商取引サイトにおいては電子メールのを利用するのが一般的となっている。

電子商取引サイトにおける電子メールの利用には一般的に以下の3種類が考えられる。

1. 商品購入時に利用者に確認のためにシステムが自動的に送信する電子メール。
2. 商品に対する問い合わせあるいは購入後の問い合わせなど人間が対応(作成)する電子メール。
3. 顧客リストに対する広告として電子メール。

これらの電子メールが改竄、盗聴、なりすましが行なわれる可能性が十分にある。実際に改竄、盗聴、なりすましが行なわれた場合のどのような影響が考えられるであろうか。

商品購入時に利用者に確認のためにシステムが自動的に送信する電子メールが成り済まされた場合。

電子商取引では、商品購入時(商品発送時ではない)に利用者に確認の意味も含めて、取引の内容を電子メールで送信している。この電子メールが盗聴されると個人情報漏洩することになる。一方、このメールが改竄等が行われた場合、決済に銀行振り込み等が用いられていた場合に危険性が高くなる、仮にこのときの振込先口座番号や名義人等が改竄され本来の電子商取引サイト以外の銀行口座に書き換えられた場合に、利用者が不正に改竄された銀行口座に振り込む可能性がある。

商品に対する問い合わせあるいは購入後の問い合わせなど人間が対応(作成)する電子メールがなりすましや、改竄が行われた場合は、これは本来、電子商取引サイトが伝えようとしている商品に対する情報や、取引方法等が改竄される可能性がある。これらの内容が改竄されると商品、電子商取引サイトの信用の低下及び特定商品等への中傷等も考えられる。いずれにしても、これらの情報が改竄されると不正に改竄を行った第三者によって企業の信用が低下させられることは明らかである。

顧客リストに対する広告として電子メールがなりすまし、改竄が行われた場合は、前述の問い合わせメールの場合と同様のことが考えられるが、それ以外に広告メールの場合は前述の問い合わせメールが基本的に1対1のメールであるのに対して、広告メールは1対多に対して送信されるので、なりすましにより不正な情報が送信された場合の企業における信用の低下は大きな問題となると思われる。特に、これらの問題は企業の知名度が高ければ高いほど企業に与える影響、社会に与える影響が多きのではないかと思われる。

他人になりすました消費者による購入の問題

一般に電子商取引サイトは WEB サーバを使用する場合がほとんどである。この場合に WEB を利用したシステムでは一般的に個人認証を行うことは難しい。特に不特定多数をターゲットとする、電子商取引サイトでは事前に個人を特定するためのユーザ登録等を行わないので、取引時に入力された個人情報を信用する以外に方法がない。

電子商取引サイトでは購入後の連絡なども電話やファクシミリ、郵送などを使用した連絡は行わず、電子メールを利用して利用者(消費者)と連絡を取ることが一般的である。この場合に問題になるのは実際に個人情報として入力された電子メールアドレスが本人のものか確認する手段がないことある。これは、電子メールアドレスは任意に指定することが出来るので、提示された電子メールアドレスが利用者(消費者)本人の電子メールアドレスであるか否かを調べる手段がない。特に ISP 等の接続サービスを利用している場合は、提示された電子メールアドレスが本人のものであるかの確認は契約している ISP に確認する必要がある。これは電子商取引サイトに限らずインターネット一般に言われる匿名性の問題と同じである。

また、上記以外の場合でも本来の電子メールアドレス利用者本人が気付かない間に、第三者により不正に利用されている可能性もある。

これをやるためには登録局(RA)⁵, 認証局(CA)⁶を利用した X.509 証明書を利用する方法くらいしか現状は考えられない。

⁵ 登録局(RA : Registration Authority)

証明書を発行可能か否かを与信する機関、RA により証明書発行者の存在や本人確認を行なう。現在、日本国内で運用されている認証局(CA)では認証局が代行している場合が多い。

⁶ 認証局(CA : Certification Authority)

電子署名に署名を行ない、その電子署名に対し署名を行ない証明した期間を認証局という。

対策

これらの問題に対策するためには何らかの方法で、利用者(消費者)を特定することが必要であり、これにはいくつかの方法が考えられるが現時点では決定的な方法はない。

ユーザ登録行(会員限定)

従来から行われている典型的な方法である。利用者を商品を購入する以前に、住所、氏名、連絡先等の情報を登録し、電子商取引サイトに登録を行う。電子商取引サイトでは登録された情報から電話、郵送等を使用して本人確認を事前に行うことができるの電子メールアドレスやその他情報の「なりすまし」を防止することができる。

しかし、この方法は利用者(消費者)にとっては商品を購入する際にユーザ登録するまでの時間が必要となるために、購入したいときにすぐに購入できないために利用者にとって不便である。また、電子商取引サイトを取っても商品、決済等のほかにユーザ情報の管理も行う必要性がでてくるので、その分コストが増加してしまう。

X.509 証明書を利用する

この場合は自サイトで認証局を運用する方法と、第三者認証機関が発行した証明書を利用する方法がある。

自サイトで認証局を運用すると前述のユーザ登録以上に運用コストがかかってしまう。

現時点では第三者認証機関が発行する証明書を用いた個人認証が電子商取引サイトの運用面からは望ましいのではないだろうか。

しかし、問題は現時点で信頼できる第三者認証機関に関する定義等がないことである。

今後、第三者認証機関に対する議論、定義等も必要である。

5. 大量の商業宣伝メール(UCE⁷)配信の問題

電子メールは年齢、性別、趣味等の個人情報により、送信者を特定することができる PUSH 型の広告媒体として利用されている。

しかし、一方ではこれら商業宣伝メールを大量に送信する場合に以下のような問題が発生している。

意図しない不正中継による問題

インターネットの普及によって日本国内にもインターネットに接続されているコンピュータの数が飛躍的に増えてきている。特に Microsoft 社製 Windows NT 等 GUI を持った OS の普及、昨今の Linux ブームにより、各種入門書、解説書などを参照して手軽にインターネットに接続したサーバを構築することが可能になった。

これらの方法でインターネットに接続可能なサーバマシンを構築した場合、基本的な機能に関しては動作するようにできるもののセキュリティに対する配慮などはほとんど行われていないのが現状である。

特に MTA を第三者に不正に使用され UCE 等の中継に使用される場合がある。

このスパム・メールの中継に使用されると一度に数千から数万単位のメールの配送に利用される場合がある。これらの不正中継に使用されるとサーバマシンの CPU 等の資源の殆んどを消費されてしまい、本来のそのサーバが行なう処理に支障がでる。また、サーバマシンの処理に問題が発生するだけでなく、中継に使用されたマシンの管理者に対して苦情のメールが届くなどの問題が発生する。それ以外も後述する MTA オープンリレーデータベース ORBS 等へ登録が行われ特定のサイトからは当該のサーバマシンから発信された電子メールの受取りを拒否される可能性がある。

また、これら不正中継可能なサーバマシンの情報はスパム・メール発信ソフトの中に組み込まれる可能性がある。このソフトの中継可能リストに登録されると不正中継を拒否する設定を行っても後から後から際限なく不正中継を行なう接続要求がくる。そのため、その要求をチェックして確認する処理にサーバマシンの CPU 資源が消費され結局本来の業務に使用できない事になり、対策としてはサーバマシンの IP アドレスを変更する以外方法がなくなってしまう。

このような事態になる前に事前に適切に設定を行なうのが望ましい。特に電子商取引を行うサイトの場合にはこのような不正中継に使用されることによってサイト自体の信用を落とす可能性がある。

電子商取引を行うようなサイトでは WEB サーバ等の構築だけに注意が注がれがちだが、MTA の不正中継またその他のセキュリティ対策にも十分な配慮が必要である。

⁷ UCE: Unsolicited Commercial Electronic mail
予期しない商業宣伝電子メールをいう。俗にスパムメールという。

ORBS について

前述の不正中継を許可しているサイトからの電子メールを拒否するためには有効な情報であるが、<http://www.orbs.org/> の団体自体の存在が不明あるためこのサイトの情報を信用し利用するか否かの判断は利用する側の判断である。

特に、ORBS のサイト自体が米国内で運営されていることもあり全ての情報は英語で発信されてる。これは現状の日本国内でのインターネットの普及から考えるとなんらかの形で ORBS に登録されてしまったサイトが ORBS のシステムを理解、対策を施し登録を削除することは難しいと思われる。したがってこのサイトの情報を利用することは特に日本国内で電子商取引に電子メールを利用しようと考えた場合は適切ではないと思われる。具体的な例としては ORBS のデータ登録されたメールサーバが ISP のものであった場合は ISP のメールサーバの設定、運用に問題があるのであって、その ISP の利用者がスパム・メールを送信しているとは限らないからである。また、ISP のメールサーバではなく、企業のメールサーバが登録された場合でもほとんどの企業では ORBS の存在すら知ることがなく、ORBS よりブラックリストデータベースに登録されたむねの電子メールを受信した場合でも内容を理解できないで無視している場合が多い。

添付資料に ORBS に登録された場合に ORBS より送信されてくる電子メールの例を示す。

IP アドレス割当てと ORBS について

現在の日本国内における IP アドレスの割当ては JPNIC から委任された JPNIC 会員(ISP)が顧客に対して IP アドレスを割り当てる運用方法が用いられている。この場合なんらかの理由により、ISP を変えた場合に IP アドレスが変わることになる。このとき、新たに ISP より割り当てられた IP アドレスが既に ORBS に登録されていた場合、IP アドレスを割り当てられたユーザとしては割り当てられた IP アドレスが ORBS に登録されているか否かは ISP からは連絡されないの知ることができない。このような場合に利用者側で対処しようと思った場合は新たに割当てが行われた IP アドレスを使用する前に ORBS のデータベースを参照し登録されていないことを確認する作業が必要となるが、これらの作業を ISP がやるべきなのか、ユーザがやるべきなのかといった事は明確になっていない。

サーバの意図しない不正中継の問題

電子メールサーバ(MTA)が利用者が意図しない、中継(中継時の文字コードの変換等)を行なった場合にどのような影響があるだろうか。

インターネットで電子メールを交換するときの文字コードは電子メールを配送するときに使用される、配送コードと端末で表示するときに使用する内部コードの二つに分けられる。

配送コードは MUA,MTA 間、MTA,MTA 間で使用される文字コードであり、日本国内では一般に ISO-2022-JP コードが用いられている。

内部コードはコンピュータが内部で処理するために使用する文字コードである。一般的にはパソコンでは ShiftJis、Unix 等のワークステーションでは EUC が使用される場合が多い。

ここで、問題になるのは配送コードと内部コードが異なることである、この問題は配送コードを実際に表示、メッセージ作成等の処理を行うコンピュータが配送コードを直接処理できないことである。内部コードはコンピュータのオペレーティングシステムやアーキテクチャによって異なるので、複数の文字コードが存在する。

このため、一部の古い、MTA では配送コードを内部コードに変換する MTA も存在したが、現在ではそれほど数は多くないと思われる。

現在問題になるのは MUA から送信されたメッセージを MTA が Q エンコーディング、B エンコーディング等を行ってしまう問題である。

具体的には MUA が MTA に対して ShiftJis コードでメッセージを送信したとすると、MTA では、配送時に 7bit コードで配送しようとして ShiftJis の文字コードを Q エンコーディングに変換してしまう場合がある。また、このときに MUA が MIME の Content-Type: charset: に対して正しく charset を指定して入れば問題は発生しないが、この charset を正しく設定していない場合は MTA が標準としている charset を自動的にセットさせる可能性がある。このような処理が行われると、受信した側では元の電子メールの文字コードが何であったのか判断がつかないために表示できないといった問題が発生する。

このような場合でも仮にメッセージが日本語だけと限定されていれば比較的、元の文字コードを推測することは容易であるが現在のインターネットのコミュニティを考えると文字コードを日本語だけと限定することは危険である。

また、これらの文字コードの変換やエンコーディング方式の変更が行われると、先に説明した電子署名を行なった場合に内容の改竄とみなされ正しく検証できない。

この問題は電子署名は内部コードではなく、配送コードに対してハッシュ値を求め署名を作成されるので、エンコーディング方式の変換だけでなく、実際には MUA が受信したメッセージをハードディスクに保存する際に配送コードから内部コードに変換して保存した場合にも発生する。この問題は日本語でも以下の場合に発生するので MUA では極力文字コードの変換は行うべきではない。

現在日本でも一般的に電子メールでは ISO-2022-JP コードが使用されている。

このコードはいわゆる JIS コードで ESC から、はじまる 3byte で使用するコードの状態推移を行なっている。

以下の ESC からはじまるシーケンスが使用されている。

ESC (B ASCII

ESC (J JIS X 0201-1976

ESC \$ @ JIS X 0208-1973

ESC \$ B JIS X 0208-1983

内部コードに ShiftJis コードを使用しているパソコンを使用している場合、JIS X 0208-1973 を使用して作成されたメッセージに対して電子署名がされていた場合にこの JIS X 0208-1973 コードを ShiftJis コードに変換してしまうと、メッセージに持ってた、JIS X 0208-1973 への推移コード ESC \$ @ の情報が失われてしまうために、このメッセージが本来、JIS X0208-1973 で作成されていたのか、JIS X 0208-1983 で作成されていたのかの情報が失われてしまい、電子署名が正しく検証できなくなってしまう。

この問題は内部コードに EUC 等、他の文字コードを使用してる場合でも同様の問題が発生するので注意が必要である。

ユーザー(消費者)側での対策

電子商取引における電子メールの利用、企業からの広告、アンケートなどの電子メールは「なりすまし」等が行われている可能性があるため、これらの電子メールに対して返信等を行う場合には十分に注意が必要である。特に電子メール本文内で名のっている企業名と電子メールアドレスの From: 行に記述されている電子メールに関しては基本的に「なりすまし」と思って間違いはない。このような電子メールに対しては十分な注意が必要であり、もし、この電子メールが個人情報等を求める内容であれば、送信元(名のっている企業名)に対して電子メール以外の方法で確認を行ったほうがよい。

また、電子メールの本文中の企業名と、From: で指定された電子メールアドレスの企業名が一致している場合でもなりすまされている可能性があるため、このような場合は最低でも電子メールの Received: ヘッダにより電子メールの配送経路を確認する等の作業が必要である。しかし、現実敵はこの Received: ヘッダも偽造が可能であるため、一概に Received: ヘッダの配送経路情報を信用する事はできない。

また、一般的な電子メールの利用者(インターネットの利用者)にはこれらの配送経路の情報をみても「なりすまし」等の可能性を発見することは不可能と思われる。

これらのことを考えるとユーザ(消費者)側での対策はアンケート等に対して個人情報を送信する場合は必要最低限のみに留めること、必要であれば企業に対して電子メール以外の手段内容の確認を求める等の対策が考えられるが、これら方法は現在のインターネットの普及率から考えると本質的な対策とは思えない。

先にも述べているように基本的には企業側でこれらの電子メールには対しては S/MIME 等の技術を使用して電子署名を行ない、「なりすまし」改竄を防ぐことが必要である。

また、アンケート等の個人情報を送信する場合には、電子署名だけは盗聴等には無防備であるため暗号化を行ない、個人情報を保護することが必要である。

これらの電子署名、暗号化による対策をユーザ(消費者)の側からも企業に求めていき、ユーザ(消費者)側でのこれら個人情報等に関する重要性を伝えることも必要であると思われる。

電子署名、暗号化等を使用するには複数の企業が違った技術を使用する等の統一性がなくなるとユーザ(消費者)が混乱し、実質的にこれらの技術は使えない技術になってしまう可能性があるため、何らかの形でこれらの技術を使用する場合のガイドライン及び、様々なプロダクト間での互換性なども十分に調査する必要があるが、これらを各企業間で行なうのも、作業料が膨大になるため何れかの団体等でこれらの互換性、相互接続性、ガイドラインを作成するのが適切と思われる。

スパマーによる電子メール・アドレスの収集方法と対策

スパムメールと呼ばれる無差別広告メールが問題になっているがこの様な無差別広告メールを送信するスパマーとはどのようにして電子メールアドレスを収集しているのだろうか。

以前はネットニュースへの投稿されたアドレスを使用するケースが目立ったが最近ではネットニュースの利用者自体が少なくなったこともあり、ネットニュースからの収集は少なくなったのではないだろうか。

その代わりに企業の特定のアドレス、例えば webmaster.info 等に対して送信してくるケースが増えている。これはドメイン情報は一般に公開されているために簡単に入手でき、これらのアドレスは簡単に推測できるのでこれらのアドレスに安易に送信される。またこれらのアドレスに送信している側は特にスパムメールを送信しているという意識が内容にも思える。

これら企業の特定のメールアドレスに送信されるの以外に特定個人のアドレスに送信されるメールもある。個人のメールアドレスに直接送信されてくる場合は、俗に言うロボットを使いホームページから”mail to: “タグを検索してメールアドレスを収集しているケースが考えられる。

これ以外にはメーリングリストからメーリングリストのコントロールコマンドを利用してメーリングリストの参加者アドレスを取り出す方法も使用されている。最近のメーリングリストを構築するプログラムでは参加者アドレスの取得を制限する機能があるが、2年から3年ほど前のこれらスパム等のメールが一般的な問題になる前のメーリングリストソフトではこれらに対する対策が行なわれない場合があるので、そのようなバージョンのソフトを使用している場合は新しいバージョンに入れ替えた方がよい。

また、このメーリングリスト自体がスパムメールの対象となる事もある。

これは、メーリングリスト自体が参加者を限定していない、自動登録形式の場合や、参加申し込みに対してメーリングリストから確認を出さない場合等に発生する。このようにメーリングリスト自体がスパムメールの対処になってしまうとスパマーは容易にそのメールの参加者に対してスパムメールを送信することができるのでメーリングリストの管理者はこの様なことが発生しないように十分注意を持って運用する必要がある。

6. 添付資料

ORBS メール

Date: Tue, 11 May 1999 08:43:19 +1200
Message-Id: <199905102043.IAA05531@mail2.manawatu.net.nz>
To: postmaster@goma.xxx.co.jp, postmaster@goma.xxx.co.jp
From: The Open Relay Behaviour-modification System <listings@orbs.org>
Reply-To: ORBS listings <listings@orbs.org>
Subject: Network security problem: 203.nnn.nnn.nnn is an open email relay

Please read this entire message carefully before replying

If you are not the technical contact for your organisation, please forward this to the person who is.

203.nnn.nnn.nnn has been detected as an open email relay and has been added to the ORBS database.

An open email relay is a SMTP server that accepts E-mail from anywhere on the Internet and forwards it to anywhere else on the Internet

Someone nominated 203.nnn.nnn.nnn for testing, probably because they received unwanted junkmail which was delivered via the server. Inspection of your mailserver logs will reveal more information.

ORBS (<http://www.orbs.org>) has confirmed this by sending an automated test message through 203.nnn.nnn.nnn. Delivery of that message back to the testing program has triggered this warning message.

Being an open relay used to be a desirable thing in the past, as the Internet operated in an atmosphere of trust and servers weren't normally abused. As such, almost all older SMTP transport software defaults to this behaviour. Almost all SMTP server software has changed this policy in recent releases because of rapidly escalating levels of abuse.

An open relay is a "Bad Thing" in the modern net environment, because they are used extensively by junkmailers to bypass filters and offload costs. Many admins have decided they won't accept mail from known open relays because of this. Many refer to the ORBS database to assist in detection and rejection of connections from such machines.

If you are happy for your machine to remain an open relay and be included in ORBS, you need do nothing, however you probably want to secure it. Apart from losing connectivity to hosts subscribing to the ORBS system, you may be breaching your supplier's terms and conditions.

The ORBS database is not downloadable. The only way anyone can "see" that the machine is included is to make a special DNS query or visit our website and make a specific query about 203.nnn.nnn.nnn

Please check the ORBS website (<http://www.orbs.org/>) or the Mail Abuse Prevention System's Transport Security Initiative (MAPS TSI) website (<http://maps.vix.com/tsi/>) for links to other sites that may be able to help you close your relay. The TSI website contains links covering most known Mail Transport Agents (MTAs), with the information on securing each MTA usually written by the MTA author, or user support group. Most mail transport agents can be secured quickly by the operator, usually for no cost other than the time take to read the appropriate instructions for your software.

To be removed from the ORBS database, you need to disable the external relay features of your mail server and then report the IP address 203.nnn.nnn.nnn to our web site at <http://www.orbs.org/closed1.cgi>. We will immediately remove your site's entry, then re-test it for third-party relay capabilities.

ORBS is an automated testing system, if your mailserver has multiple

IP interfaces, it is likely that you will receive multiple copies of this message. You should only receive one notice per IP number

Thank you for your attention to this matter.

Sincerely,

listings@orbs.org

7. 参考文献

ITU-T Recommendation X.500, X.509

ITU-T 勧告の X.500 及び X.509

<http://www.ietf.org/html.charters/pkix-charter.html>

IETF の PKIX (Public-Key Infrastructure X.509) WG のホームページ

<http://www.imc.org/ietf-pkix/>

Internet Mail Consortium による PKIX WG のホームページ

<http://www.cs.auckland.ac.nz/~pgut001/pubs/x509guide.txt>

Peter Gutmann 氏による X.509 の解説

<http://csrc.nist.gov/pki/welcome.html>

NIST の PKI に関するページ

<http://www.ietf.org/html.charters/spki-charter.html>

IETF の SPKI (Simple Public Key Infrastructure) WG のホームページ

<http://www.clark.net/pub/cme/html/spki.html>

SPKI に関する解説

<http://theory.lcs.mit.edu/~cis/sdsi.html>

SDSI (Simple Distributed Security Infrastructure) に関する解説

<http://devedge.netscape.com/docs/manuals/security/sslin/index.htm>

Netscape Communications 社による SSL の概要解説

<http://home.netscape.com/eng/ssl3/ssl-toc.html>

SSL ver 3.0 のドラフト

<http://jnetcom.jeida.or.jp/ec/papers/1-05/>

SSL 及び SHTTP の仕様と実装

<http://robin.sl.cae.ntt.co.jp/~motoda/SSL/>

元田氏による SSL 関連情報ページ

<http://www.ietf.org/html.charters/tls-charter.html>

IETF の TLS (Transport Layer Security) WG のホームページ

RFC 2246

TLS Version 1.0 の仕様

<http://www.fortify.net>

Fortify のホームページ

OpenDesign No.31 第5章

稲村氏による Linux 版 Apache での HTTPS サーバ構築

http://www.netscape.com/eng/security/SSL_2.html

SSL ver 2 のドラフト

<http://home.netscape.com/eng/ssl3/>

SSL ver 3.0 のダウンロードページ

<http://www.rsa.com/smime/>

RSA 社提供の S/MIME 解説

<http://www.rsa.com/smime/html/faq.html>

RSA 社提供の S/MIME に関する FAQ ページ

<http://www.imc.org/ietf-smime/>

Internet Mail Consortium による S/MIME WG のホームページ

<http://www.imc.org/smime-pgpmime.html>

S/MIME と OpenPGP の比較

<http://www.fujitsu.co.jp/hypertext/Products/Software/tswks/taka/mail.html#3>

S/MIME の製品動向に関するページ

RFC 1421-1424

PEM (Privacy Enhancement for Internet Electronic Mail) の仕様

RFC 1847

MIME セキュリティ

RFC 1848

MOSS (MIME Object Security Services) の仕様

RFC 2015

PGP による MIME セキュリティ

RFC 2311

S/MIME version 2 の仕様

RFC 2312

S/MIME version 2 における証明書の処理

RFC 2313

PKCS#1, RSA 暗号化規約

RFC 2314

PKCS#10, 公開鍵証明書を発行要求するためのフォーマット規定

RFC 2315

PKCS#7, メッセージのデジタル署名と暗号化を施すためのフォーマット規定

RFC 2459

X.509 証明書と CRL のプロファイル

http://www.ipa.go.jp/SECURITY/rfc/RFC_2311_index.html

RFC 2311 の日本語訳 (IPA 提供)

http://www.ipa.go.jp/SECURITY/rfc/RFC_2312_index.html

RFC 2312 の日本語訳 (IPA 提供)

<http://www.ietf.org/internet-drafts/draft-ietf-smime-cms-13.txt>
CMS (Cryptographic Message Syntax) の仕様

<http://www.ietf.org/internet-drafts/draft-ietf-smime-ess-12.txt>
S/MIME のためのより高いセキュリティサービス

<http://www.ietf.org/internet-drafts/draft-ietf-smime-msg-08.txt>
S/MIME version 3 の仕様

<http://www.ietf.org/internet-drafts/draft-ietf-smime-cert-08.txt>
S/MIME version 3 における証明書の処理

<http://www.ietf.org/internet-drafts/draft-ietf-smime-x942-07.txt>
S/MIME での Diffie-Hellman 鍵交換プロトコル利用の際の仕様

OpenDesign No.14 第5章
稲村氏による暗号化電子メールの解説

<http://www.rsa.com/rsalabs/pubs/PKCS/html/pkcs-12.html>
PKCS#12 仕様

<http://www.drh-consultancy.demon.co.uk/pkcs12faq.html>
Stephen Henson 氏による PKCS#12 実装の FAQ ページ

<http://home.netscape.com/eng/security/comm4-cert-exts.html>
Netscape 独自の X.509 v3 拡張の仕様

<http://www.drh-consultancy.demon.co.uk/nscertype.html>
Netscape 独自の X.509 v3 拡張の解説

<http://www.ecom.or.jp>
電子商取引実証推進協議会 (ECOM) のホームページ

<http://www.visa.com/nt/ecom/et/setprot.html>
SET の仕様書ダウンロードページ

<http://www.verisign.com/set/>
Verisign 社による SET 解説

<http://www.jipdec.or.jp/security/privacy/>
プライバシーマーク制度