メールにおける信頼性

経済学部 鈴木　斉
sigh@net.nagasaki-u.ac.jp

はじめに

1995 年前後を境に、日本国内でも Internet 利用人口が年々爆発的に増えて来た。その結果、Internet も着実に一般的な通信媒体の一つとして世間に認知されることとなった。Internet を使用する電子メール等は、近年では携帯電話だけで利用可能となる商品が発売される等、かなり一般的な通信手段としての地位を獲得している。しかし、残念なことに 90 年代前半から世界的に関心が高くなって来た電子メールを使用する上でのプライバシー保護の仕方や、信頼出来る電子メールの作成方法等は未だ日本国内では広く認知されているとは言えない。そこでメールに信頼性を持たせることの意味と信頼性を持たせるための方法とについて述べる。

メールとは

個人が持っている情報を他人に伝える際、伝えるべき情報が具体的に提示可能な物体であれば、受信者にその情報を伝えることは簡単だ。また、情報を具体的に示すことが出来ない場合でも情報を何らかの手順で符号化し、その結果を受信者に伝えることで間接的に情報を伝えることが出来る。間接的な情報伝達では、伝えようとする情報を何らかのルールに基づき符号化し、その符号化の結果を相手に示す。受信者は、この結果を基に情報を復号化 (復元) する。この際、相手が符号化の結果を直接的に受け取ることが出来ない時は、さらに、符号化の結果を何らかの媒体に記録 (保存) し、この媒体をやり取りすることで情報を伝える。ここでは、相手に伝えようとする情報をメッセージと呼び、メッセージのうち標準的に符号化で保存した形式で利用されるものをメールと呼ぶ。

メールに対する信頼性とは

メールの信頼性を考える際、メッセージの信頼性も同時に扱う必要があると考えられる。しかし、メッセージの信頼性を検証する一般的な方法は存在しない。そのため、ここではメッセージをメールとした際の信頼性の変化について考察する。メッセージは保存されメールとなった瞬間から、期待される受信者へと配送されるまでの間、様々な理由により信頼性が低下する危険にさらされる。

メールが一切改変されていないと仮定した場合に受信者から見たメールの信頼性を分類すると、

1. メッセージ発信者が特定出来ないもの　　例) 落書き等
2. メッセージ発信者が特定出来る何らかの特徴を持つもの　　例) 手書き郵便物等
3. メッセージ発信者が完全に特定出来るもの　　例) 直接手渡されたメモ等

といった 3 段階に区分することが出来る。ここでは、番号が増えるにつれ、そのメールの信頼性が高まるものとする。メールが受信者のもとに到着するまでに、どの経路を通過して来たのか確認する手段が存在しない、かつ、メール中に発信者を特定させる特徴もないメールが 1 の「情報の発信者が特定出来ない」メールである。このメールでは、メール内容の確認を発信者から一切出来ないことが、メールの信頼性 (価値) を低下させている。2 の場合、別の第 3 者が情報発信者になりすまして、メールを発信することを防げない。ゆえに、改変は行われていなくとも、期待されるメッセージ発信者からのメールであると保証することも出来ない。その結果、3 と比べた際にはメールの信頼性が低下している。なお、3 に分類されるメールでは、メッセージのメール化に伴なう信頼性の低下が起きていないことを保証出来る。

実際には、メールが受信者に届くまでに改変される可能性があることを考慮する必要があるため、

① メッセージ発信者が特定出来ない、もしくは、改変されたことが確認出来るもの
② メッセージ発信者が特定出来る何らかの特徴を持ち、かつ、改変された可能性があるもの
③ メッセージ発信者が特定出来る何らかの特徴を持ち、かつ、改変されていないもの
④ メッセージ発信者が特定出来、かつ、改変された可能性があるもの
⑤ メッセージ発信者が特定出来、かつ、改変されていないもの

という5種類に分類する。④では、メールが作成されてから受信者に届くまでに第3者による改変可能な時間が存在する。つまり、メールを発信者から直接受け取ろうとも、メール作成直後に受信しない限り、ここに分類される。なお、②、④といった改変された可能性のあるメールであっても、メール自体にメールの完全性 (改変を受けていないこと) を証明する仕組みを組み込むことで、その一部を③、⑤と同等の信頼性を持ったメールとして扱うことが出来る。もちろん、改変が確認されたメールに信頼性は存在しない。なお、実社会における手書き郵便物や留守番電話への録音等は、他人がなりすましてメールを作成する可能性が存在するものの、筆跡や声質を完全に偽ることが難しいため、現在の所、まだ、③に分類されるメールの例として挙げることが出来る。

また、機密性が高いメールを扱う場合、いかにして関係のない第3者からメールを保護するのかといった問題が存在する。メール受信者がメールを受け取るまでの間はもちろん、メールを受信後もメール (または、その複製) が存在している間は秘密が漏れる恐れがある。重要なメッセージの場合、第3者に秘密が漏洩することを防ぐため、少なくともメッセージをメールに変換する時から、メッセージの機密性が必要なくなるまでの間、機密を保つ必要がある。このためには、メッセージを符号化してメールとする際に暗号化も併せて行い、かつ、その暗号化手法の強度が十分に強いことが必要になる。なお、暗号化手法の強度は暗号解読の難しさで示す。

なお、使用する通信路の信頼性だけに問題がある場合、つまり、メッセージの保存について考える必要が無く、伝達中のメッセージの信頼性だけが保護されれば良い場合には、通信路上を通る全てのメッセージを十分な強度を持った暗号化手法で符号化して伝達することで、信頼性の低下を避けることが出来る。しかし、メールは受信後そのまま保存しておく際の機密保持も必要であるため、ここでは、保存中のメールに適した別の方式による信頼性の保護方法について考えることとする。

標準的な電子メールに存在する信頼性

Internet経由の電子メールは実験的なサービスの一つとして開始した。その結果、当初から存在する最低限のルールでは発信者の身元確認といった基本的な認証が存在しない。また、手書きの手紙で存在していた筆跡といったメールの発信者を識別する手がかりもなく、文体や内容等に特徴がなければ全てが印刷された郵便物と同じく誰が実際のメール送信者であるか特定することは難しい。さらに、メールの内容は平文 (すぐに読める形式の文) で配送される。よって、標準的な電子メールは印刷された郵便葉書き程度の信頼性しか存在しない。また、電子メールは様々な理由により手書きの手紙以上に簡単に間違って配送され、その際に第3者の目にさらされることも考慮する必要がある。このような状況下でメールに信頼性を持たせるためには使用する各個人がメッセージの持つ重要度に応じて信頼性を保護する対策を取り、また、機密性に応じて暗号化を施す必要がある。

電子メールのしくみ

Internetを経由して電子メールを送るということは、

1. コンピュータ内部で使用しているメールの形式でもってメールを作成する。
2. Internetでメールを配送する際に使用するメールの形式へと変換を行う。

3. Internet 経由でメールを配送する (Mail Transfer Agent: MTA)に配送を依頼する。
4. MTA を経由し、相手先のコンピュータネットワークへとメールを配送する。
5. 相手がメールとして活用する前までに利用しているコンピュータ内部で使用しているメールの形式へと変換を行う。

といった手順を踏むこととなる([1])。以下、図 1で上述 3 番の動作を示す。

```
$ telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 localgate.* ESMTP
HELO localhost
250 localgate
MAIL FROM: <my@mail.address>
250 ok
RCPT TO: <recipient@somewhere>
250 ok
DATA
354 go ahead
Date: Tue, 16 Feb 1999 00:00:00
From: My name <my@mail.address>
To: Someone <recipient@somewhere>
Subject: This is the subject

Here is the beginning line for body.
Only one dot at beginning is the end mark.
To send an only '.' Line, put '..' instead.
And this line is the last line.
.
250 ok
QUIT
```

図 1: telnet でのメール配送

telnet でメール配送サービスを行っているポートに接続し、「HELO localhost」にて、メールの配送を依頼するホスト名を名乗る。なお、各入力に対し 3 桁数字による応答コードが返される。

- 「MAIL FROM: <my@mail.address>」で使われているメールアドレス「my@mail.address」はメールの配送中に配達不能等のエラーが発生した際にエラーメールを受け取るために使用される。
- 「RCPT TO: <recipient@somewhere>」で使われている「recipient@somewhere」がメールの配送先として使用され、「To: Someone <recipient@somewhere>」は実際のメールの配送に使われることはない。なお、この配送先の指定は 100 回まで繰り返すことが出来る。
- 「DATA」が電子メール本体を入力するための命令である。この命令が受け付けられた場合には、以後「.」だけで構成される行の直前までを電子メールとして先ほど示された相手に配送することになる。また、各行は 1000 文字までの ASCII テキスト文字で構成されるものとなっているため、最低限の仕様しか満たしていないエージェントを通過する際には漢字を使うことは許されていない。

なお、電子メールとしての本文に使用されるのは、「Here is the beginning line.」の行からであり、それ以前の部分はメールヘッダとなる。また、電子メールとして必須のメールヘッダを記述しなかった場合、通常はエージェントが適当に補ってくれる。

図 1 の例から理解出来るように、通常我々が発信者や宛て先の確認に使用しているメールヘッダでさえメール本体と同様、配送には一切影響を及ぼさない通常のテキストである。このため、標準的な電子メールではメール本文だけでなく発信者や宛て先等すべて、そのまま信頼することは出来ない。なお、電子メールの行末は、復帰 (0x0D) 改行 (0x0A) で正則化すること、また、別な規格で漢字は JIS コードで正則化してから Internet 経由のメール配送を依頼することが決められている。

暗号化によるセキュリティの向上

メールとはメッセージに何らかの符号化を実施したものであり、暗号化も符号化の一つである。既に符号化されているメールをさらに暗号で符号化することの目的とは、

1. メールに不正に変更が加えられた際に変更があったことを検出する

2. 第3者によってメールが不正に読み出されることを防ぐ
3. 期待する作成者によって作成されたメールであるか検証する

という3つが挙げられる。しかし、暗号化も万全ではないため、

1. 検出された改竄を完全に復旧することは出来ない
2. 暗号化に使用した手法に致命的な欠陥が発見された場合に効果は期待出来ない
3. 面識のない人がなりすまされた別人であると確認することはかなり難しい
4. 暗号化前のメール、復号化後のメールは保護出来ない
5. 復号化の方法を忘れた際にはメールを復元する手段を失うことになる

といった問題点がある。事実、単純な暗号化では総当たり法での復号化で適当な時間内に元のメールを取り出すことが出来る。コンピュータの処理速度は年々高速化し、価格も低下して来ているため、台数を集めた総当たり攻撃を行う環境が既に各所で整っていると考えるべきである。ゆえに、簡単な暗号化手法を信頼してはいけない。出来ることなら、自分が使おうとしている暗号化手法が「現在の」コンピュータで総当たり攻撃を受けた場合、どの程度の期間まで、平均的に安全であると考えることが出来るのか確認してから使用する暗号化手法の選択を行うことをお勧めする。

ただし、強力な暗号化手法を使用しているからといって安心しきってはいけない、なぜなら、どんなに強固な暗号化手法を使用していても、何らかのきっかけで暗号化ツールに細工をしかけられた場合、暗号を使用することによるセキュリティ向上効果は一切存在しない。複雑な暗号化手法を使用しているのだから安全などと間違った解釈をして油断している使用者等は悪意を持った攻撃者からみれば格好の的である。セキュリティを向上させるためには、物理的な安全 (使用するツールやユーザに対する攻撃を防御する等) を確保し、使用しているツールの危険性等を提供する環境を利用する人々に理解してもらうという運営者側の対策も必要であるが、それに伴ない、利用する各人でも自衛の手段を講じてもらう必要がある。たとえメッセージが暗号化で保護されていたとしても、使用する者がうかつな行動を起こせば (例えば、復号化に必要となる鍵をメモにしてコンピュータに貼り付けておく等) セキュリティは一瞬にして破綻してしまう。なお、一箇所でもセキュリティが破綻を起こせば、連動して関連している各人、各所のセキュリティも危険にさらされることになり、当事者一人だけの問題では済まなくなくなる。このことを忘れないでおいていただきたい。

暗号化方式の種類

暗号化方式は大別して、秘密鍵方式、および、公開鍵方式の2種類に分類される。秘密鍵方式は、メッセージの暗号化、復号化ともに同一の鍵を使用する方式であり、対称鍵暗号方式とも呼ばれる。DES (Data Encryption Standard)、RC5、IDEA といった暗号方式がこれに相当する。DES や RC5 等が持つ強度は RSA 社主催で開かれたコンテストや distributed.net による、このコンテストの世界的な協力体制による総当たり攻撃による解読[1]等の話を見てもらえばわかりやすい。この暗号化方式では暗号化にも復号化にも同じ秘密鍵を使用するため、鍵が他人に漏れることによる情報漏洩の可能性が発信、受信者双方に存在する。また、鍵に使用するビット数 (鍵の取り得る組み合わせ総数) が少ない秘密鍵方式では、既に総当たりで鍵を簡単に探し出し解読出来る時代となっている。

一方、公開鍵方式は、公開鍵と呼ばれるメッセージ暗号化に使用する鍵と秘密鍵と呼ばれる復号化に使用する鍵との鍵の組みを使用する暗号化方式であり、暗号化に使用する鍵、および、復号化に使用する鍵それぞれが異なるため非対称鍵暗号方式とも呼ばれる。Diffie-Hellman、RSA、ElGamal、DSA といった暗号方式がこれに相当する。これらの説明は参考文献[2-5]を参照しても

[1] http://www.distributed.net/rc5/

らうこととし、詳しい説明は割愛させていただく。これら公開鍵暗号方式の特徴として、暗号化を実施する人が知ることになる公開鍵では復号化出来ないため情報発信者サイドから公開鍵が他人に漏れることが、危険な行為とはならないことが挙げられる。なお、公開鍵方式では暗号化の強度を構成する部分に数学的な前提条件 (例えば、非常に大きな数の素因数分解には時間がかかる等) を使用することが多い。このため、使用している前提条件に問題がないか確認をする必要が出てくる。なお、暗号化手法の強度を示す根拠として暗号化に使用するアルゴリズムの非公開を挙げている暗号化手法等を信じてはいけないということを覚えておいていただきたい。なぜなら、信頼とは本質的には減点方式ではなく、積み上げ方式で高めることしか出来ないものと考えるべきだからである。

PGP (Pretty Good Privacy)

PGP[3,6] は公開鍵暗号方式を基本の暗号方式とし、部分的に秘密暗号方式を取り入れた暗号化を行う、メジャーなオペレーティングシステムの殆どで動作するプログラムである。この手のプログラムを入手する際に注意する点として、輸出入規制がある。アメリカ合州国のように強力な暗号は武器にあたると判断をする国もあるし、軍事国家等では全ての通信は平文、もしくは、暗号を使用する際には解読方法を政府に提出する必要がある国もある。PGP はアメリカ国内で作成されたため、当初、アメリカ国外への持ち出し方法に問題があるとか、他の特許を許可なく使用していた等の様々な問題を抱えていた。現在は[6]で述べられているとおり、世界各国で合法的に入手可能なバージョンが存在する。日本国内での入手も可能であるが、商用利用する目的であればフリーウェア版は使用出来ないため、使用する際には良く注意して選択していただきたい。PGP は、暗号化によるセキュリティの向上で示した 3 つの目的すべてに対して有効に利用可能なツールである。

不正に加えられた変更の検出

受け取った公開鍵を検証する場合、PGP では key's fingerprint が重要な役割を果たす。key's fingerprint とは、公開鍵に対してある特別な計算（メッセージ要約関数: md5）を行った結果であり、16 個の 16 進数だけで構成される。これは、メールや公開鍵と比べ非常に少量のデータである。しかし、同じ md5 値を持つ鍵が作成されることは、まずありえない。そこで、この md5 値を使用して、鍵の真贋を確認出来る。メールの受け取りに使用する経路が既に安全ではない場合を考え、別の信頼出来る経路（直接本人から受け取る等）を使い、key's fingerprint を受け取る。次に公開鍵の md5 値を算出し、それらを検査することで、受け取った公開鍵の真贋が確認出来る。

秘密鍵で暗号化したものは、その対となる公開鍵で復号化出来る。そこで、この仕組みを使用して電子署名が実現出来る。なお、公開鍵を検証したのと同様にメール自体も md5 値で検証することが出来る。検証が必要となるメールが持つ md5 値を発信者の秘密鍵で暗号化し、署名としてメールに添付する。メールに変更が加えられると、当然そのメールが持つ md5 値も変わる。もちろん、不正に変更を加えようとする者も発信者の公開鍵は入手出来る。このため、添付された署名から、本来のメールが持つ md5 値を取り出すことは出来る。しかし、改変を隠そうとして、変更後のメールが持つ md5 値で新たな署名を作成することを計画しても、署名作成に必要となる発信者の秘密鍵が入手できない限り改変後のメールに有効な署名が付くことはない。よって、発信者の秘密鍵が第 3 者に漏れていない限り、添付された署名でメール本来の md5 値で改変の有無が確認出来る。

不正な読み出しの防止

不正な読み出しを防ぐ際は発信者が受信者の公開鍵で暗号化し、受信者は受信者自身の秘密鍵で復号化する。ここで、PGP の使用している暗号化方式が前提としている数学的条件より、対となる

鍵以外では復号化出来ないこと、公開鍵から秘密鍵を特定しようとしても鍵作成者の生存中に総当たり法等の力技で鍵が発見されることはないことが現時点では予測されている。よって、この前提条件が現在でもまだ崩れていないこと、暗号化に使用する環境が悪意を持った第3者によって汚染されていないこと、復号化に使用する鍵が第3者に漏れていないことが確認できた場合、復号化鍵を使用する以外では不正な読み出しを防ぐことが出来る。

メール作成者の検証

前述の不正に加えられた変更の検出で述べたように、発信者の秘密鍵が第3者に漏れていない限り、発信者以外には有効な発信者の署名を作成することが出来ない。このため、添付された署名がメール作成者の公開鍵で復号化出来ること、また、その公開鍵の key's fingerprint を鍵作成者本人から入手し、発信者の公開鍵であることを検証してあること、さらに、発信者の秘密鍵が第3者に漏れていないことが保証される場合、期待している人物がメールの作成者であると確認出来る。ただし、これもPGPに致命的な欠陥が発見されるまでの間しか有効ではないことを忘れてはいけない。

PGPを電子メールに使用する際の問題点

PGPを電子メールと共に使うことを考えるとMail User AgentやMTA内にPGPが組み込まれていることが考えられる。電子メールのしくみで述べたように、Internetでは通常作成しているメールとは異なった形式で配送することが多い。このため、何時 PGP で暗号化や署名を実施するかという問題がある。PGPを使用して暗号化なり、署名なりした結果がすぐ電子メールで使用出来る形式をとる方式では、配送途中や、メールを受け取ると同時に機械的に署名の検査、復号化が行えるため都合が良い。ただし、電子メール用の正則化により、作成者が意図したとおりのデータを使用出来るわけではない。事実、各環境で使用出来る文字のセットには違いが存在し、これらは可換ではない。なお、メールに構造化を持ち込み、暗号化方式や使用する文字セット等を記述することも考えられている。こちらは、現在、標準化の最中であるため、しばらくの間は仕様が変更になるかもしれないことを考慮しておく必要があることをお伝えしておく。

まとめ

最後に、どのように技術が進歩し便利な世の中が来ようとも使用するツールの持つ危険性や利用していく上での注意事項をおろそかにすれば、ツールを使用しなかった時以上の危険性が待ち構えていることを忘れないでほしい。個人で専用端末等を利用していない場合には、セキュリティを高める必須条件となる物理的な安全確保、例えば、ネットワークに常時接続した共同利用マシン上に個人の秘密鍵を放置する等の危険を回避するために、これを期に所有することを考えてもらいたい。

参考文献

[1] 笠野 英松監修,「ポイント図解式インターネットRFC事典」, 株式会社アスキー, 1998

[2] Simson Garfinkel, Gene Spafford, 山口 英監訳,「UNIX & インターネットセキュリティ」第2版, オライリー・ジャパン, 1998

[3] Simson Garfinkel, 山本 和彦監訳,「PGP暗号メールと電子署名」, オライリー・ジャパン, 1996

[4] 菊地 豊彦,「インターネット世紀のコンピュータネットワーク暗号システム」, 株式会社NECクリエイティブ, 1995

[5] Brouce Schneier, 力武 健次監訳,「E-Mailセキュリティ」, オーム社開発局, 1995

[6] http://www.pgpi.com/, 「The International PGP Home Page」