

標的型攻撃メール対策を目的とした送信者認証の提案

青山 尚史^{1,a)} 折茂 潤一² 金井 敦^{1,2}

概要：特定の人物に対して知人を騙り、情報窃取や破壊活動を行う標的型攻撃メールが問題になっている。攻撃に利用するメールにはファイルが添付されており、受信者がファイルを開くことでシステムの脆弱性などを突き、任意のコードを実行する。メールの内容は、不審に感じ難く、防御は非常に難しい。そこで本稿では、現在利用されているメールの認証方法と比較して、導入や利用が容易な ID ベース暗号と手持ちの IC カードを用いたメール送信者認証システムを提案し、プロトタイプにより動作を確認した。

1. はじめに

特定の軍事産業、化学産業、政府機関など機密性の高い組織を対象に情報窃取や破壊的な活動等を行う標的型攻撃が近年多くなっている。不特定多数ではなく特定の対象を狙って攻撃が行われることから標的型攻撃と呼ばれている。中でもメールを使用した標的型攻撃メール [1] はソーシャルエンジニアリングの手口を使っていて、メールの受信者は非常に騙されやすくなっている。標的型攻撃メールでは、悪意のある迷惑メールのように添付ファイルやメール本文の URL を経由してウイルスに感染させる攻撃パターンを含み、なおかつ、あたかも正当な業務連絡や依頼であるかのように見せかける件名や本文でメールを送りつけ、受信者が騙されやすいような仕掛けになっている。特に昨今は、受信者に関係のある実在の発信元を詐称するケースが増加しており、被害に遭いやすくなっている。

攻撃者にとっての利点は、情報を窃取することで依頼者から報酬を得たり、自らの政治的なものを含めた欲求を満たすことにある。ビジネスとして成立している場合は、依頼内容を完遂するまで手法を変えながら攻撃を繰り返す。

標的型攻撃メールによる被害として以下のものが挙げられる。

- 標的型攻撃メールの判別に時間を取られ、業務の妨げになる
- 偽装された添付ファイルによって受信したパソコンがウイルスに感染する
- メール本文の URL に誘導されて、ウイルスに感染

させられる、詐欺に巻き込まれる（フィッシング、ワンクリック詐欺等）

- 標的型攻撃メールによる被害を受けた端末の情報が、次への標的型攻撃メールによる攻撃を成功させる情報を悪用される

このような被害を防ぐためには、送信元が改ざんされていない、なりすまされているかどうかを検証できればよい。送信者がウイルスに感染していない限り同時に添付ファイル等の安全性も保証される。

そこで本稿では、新たに ID ベース暗号と手持ちの IC カードを利用して受信者が送信者を検証できるメールの認証システムを提案する。

2. 既存の認証方法・技術

既存の認証方法として S/MIME(Secure/Multipurpose Internet Mail Extensions)[2] や PGP(Pretty Good Privacy)[3] が挙げられる。

商品化されているものでは、メールサーバーの直前に対標的型攻撃メールサーバーを設置し、直前で添付ファイルを画像ファイルに変換し、無害化する。受信者が添付ファイルを開いても任意のコードを実行されることなく、添付ファイルの内容を確認することができるシステムが販売されている。[4]

これらの方法では、CA(Certificate Authority, 認証局)の利用や公開鍵サーバーなどの設置が必須になる。メール送信の対象規模が大きいほど有効な手段であるが、規模が小さい個人などで利用する場合は非効率である。

また、標的型攻撃メールの予防対策 [5] に関する研究もされている。接種直後であれば免疫力が上がっていて攻撃への耐性も高くなるが、完全な防御法では無い上に、時間とともに耐性が低くなる可能性が高く、定期的に予防対策

¹ 法政大学大学院 工学研究科 情報電子工学専攻
東京都小金井市梶野町 3-7-2

² 法政大学 理工学部 応用情報工学科
東京都小金井市梶野町 3-7-2

^{a)} hisashi.aoyama.4g@stu.hosei.ac.jp

を行う必要がある。

送信者がメールアドレスを偽装している場合はドメイン認証である, Sender ID や SPF(Sender Policy Framework), DomainKeys, DKIM(DomainKeys Identified Mail) などとも有効であるが, 標的化攻撃メールはメールアドレス偽装の確率は低いと思われる。これは送信元 IP アドレスを参照し問い合わせを行い送信元を検証したり, 電子署名を付与して送信元を検証する認証技術である。送信者のアドレスが正規なものであることを証明する(なりすましを防ぐ)技術で, 主にスパムの根本的な対策として利用されている。

3. 提案手法

本手法では, 以下を満たすシステムを提案する。

- 互いが既に知人であり, メールにて通常のコミュニケーションをとっている相手を対象とする。(メールのみで, 面識のない相手は対象としない。)
- S/MIME や PGP と比較して導入が容易である
- 送信者は受信者に正当性を証明できる
- システムを導入する相手は悪意がなく, 信頼出来る知人である
- 送信者のなりすましを防ぐ
- 既存の認証方法と比較して導入が容易であるか
- 再送攻撃対策をしているか

3.1 導入

本システムでは IC カード, ID ベース暗号 (IBE)[6] を使用する。IC カードは Suica や IC 免許証など特に新規に用意する必要はなく, IC カードの内部にある製造番号など不変の情報を用いる。独自に IC カードを用意して, IC カード内部のブロックに独自の情報を書き込んで良いが一般に普及しているもので十分である。

ID ベース暗号とは, 公開鍵暗号の一種であり識別子を利用した暗号方式である。この暗号では, 利用者の公開鍵として, 利用者の識別子を利用者の公開鍵として用いる。今回は ID ベース暗号に基づいて署名を作成・添付し, その署名を受信者が検証を行う。

また, 実装はスマートフォンである Android 端末上で動作するアプリケーションを作成し, 評価を行う。近年, スマートフォンの性能向上はめざましく, 様々な機能が増えており, IC カードの読み取りを行える NFC 搭載端末が増加している。そういった背景から特に事前準備が必要なく行えるため, 今回は Android 上で実装を行う。もちろん, IC カードリーダー搭載ノートパソコンや IC カードリーダーを用意すればコンピューター上でも実現可能である。

3.2 認証手順

メールの送信者を Alice, 受信者を Bob とする。PKG (秘密鍵生成局) を送信側に設置する。本稿では PKG と役

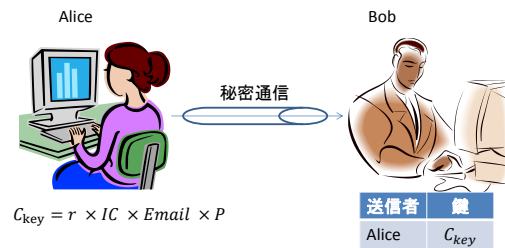


図 1 認証セットアップ 1

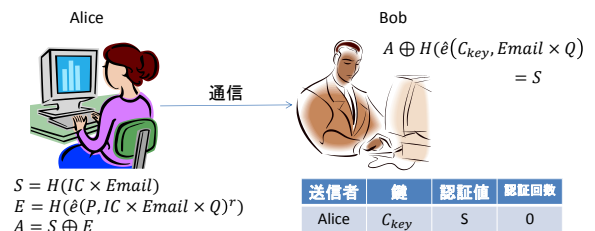


図 2 認証セットアップ 2

割上, 分けてと記してはいるが, 基本的に動作環境は全てスマートフォン上である。

3.2.1 パラメータの定義

PKG は以下のものを生成する。

- 楕円曲線の群のセット (G_1, G_2, G_T)
- 楕円曲線上の点 $P \in G_1, Q \in G_2$
- ペアリング (双曲線写像) $\hat{e}(\cdot, \cdot) : G_1 \times G_2 \rightarrow G_T$
- ハッシュ関数 H

送信者 Alice は ID(IC カード情報: IC) と受信者 Bob の Email アドレス (Email) を持つ。また, 乱数 $r(\in \mathbb{Z}/p\mathbb{Z})$ を生成する。 p は素数である。

3.2.2 認証セットアップ 1

図 1 に認証セットアップ 1 の概要を示す。送信者 Alice は PKG から楕円曲線上の点 P を受け取る。 $C_{key} = r \times IC \times Email \times P$ を計算する。受信者 Bob へ秘密通信を用いて C_{key} を送信する。ここでは, 事前の秘密の共有無しに盗聴の可能性のある通信路を使用して, 暗号鍵の共有を可能にする暗号プロトコルである, ディフィー・ヘルマン鍵共有 [7] などを用いて送信すると良い。また, 受信者は信頼出来る知人であるので, 直接受け渡しを行っても良い。

3.2.3 認証セットアップ 2

図 2 に認証セットアップ 2 の概要を示す。送信者 Alice は以下の 2 つを計算する。

- (1) $S = H(IC \times Email)$
- (2) $E = H(\hat{e}(P, IC \times Email \times Q)^r)$

そして, $A = S \oplus E$ を認証データとして受信者 Bob に送

信する。ここで S をシード認証値と呼ぶ。

受信者 Bob は A を受信し、ペアリングの双線形性より以下の計算を行う。

$$\begin{aligned} & A \oplus H(\hat{e}(C_{key}, Email \times Q)) \\ &= H(IC \times Email) \oplus H(\hat{e}(P, IC \times Email \times Q)^r) \oplus H(\hat{e}(r \times IC \times P \times Email, Q)) \\ &= H(IC \times Email) \oplus H(\hat{e}(P, Q)^{IC \times Email \times r}) \\ &\quad \oplus H(\hat{e}(P, Q)^{IC \times Email \times r}) \\ &= H(IC \times Email) \\ &= S \end{aligned}$$

受信者 Bob はシード認証値 S と送信者 Alice, 認証回数 (初期値は 0) の対応付けを行い, 記録する。

3.2.4 メール送信

送信者 Alice はシード認証値 S にハッシュ関数をかけて暗号化した A_1 をメールに添付する。

$$\begin{aligned} S_1 &= H(S) \\ E &= H(\hat{e}(P, IC \times Email \times Q)^r) \\ A_1 &= S_1 \oplus E \end{aligned}$$

二度目以降の送信時では

$S_2 = H(H(S), S_3 = H(H(S))), \dots$
とシード認証値 S にハッシュ関数を数珠つなぎに計算し, E で暗号化する。これは再送攻撃対策となる。通信路において認証情報 A を盗聴されたとしても, 再利用も次の認証情報の予測もできないため安全である。また, 送信者 Alice は受信者 Bob とのメール送信回数を対応付けし, 記録する必要がある。

3.2.5 メールの認証

受信者 Bob は, 認証情報が添付されたメールを受信したら, 認証セットアップ 2 と同様に C_{key} を用いて次の式で検証を行う。

$$\begin{aligned} & A_n \oplus H(\hat{e}(C_{key}, Email \times Q)) \\ &= H(\dots H(IC \times Email) \dots) \oplus H(\hat{e}(P, IC \times Email \times Q)^r) \oplus H(\hat{e}(r \times IC \times P \times Email, Q)) \\ &= H(\dots H(IC \times Email) \dots) \oplus \\ &\quad H(\hat{e}(P, Q)^{IC \times Email \times r}) \oplus H(\hat{e}(P, Q)^{IC \times Email \times r}) \\ &= H(\dots H(IC \times Email) \dots) \\ &= S_n \end{aligned}$$

同時に, 保持していた送信者 Alice のシード認証値 S に認証回数分のハッシュ計算を行い S'_n とする。

$S'_n = H(H(\dots H(S) \dots))$
 $S_n = S'_n$ が成立すれば送信者が認証され, 受理される。不成立ならば不正なメールと判断することが出来る。認証が受理された場合は, 送信者との認証回数を 1 増やす。

4. 実装

実装は Android 用にプロトタイプをアプリとして作成する。アプリの機能として, 鍵の生成・IC カードの読み取り・署名の生成・署名の検証・鍵共有機能を持たせる。

ペアリングの計算はペアリング暗号ライブラリである PBC ライブラリの Java 移植で, Android でも使用できる jPBC(Java Pairing-Based Cryptography) ライブラリを用いる。計算方法は, 前述のとおりである。

アプリでは IC カード情報を読み取って署名を生成し, インテント (他のアプリやデバイスから簡単に情報を受け渡す機能) を用いて常用しているメーカーへ署名データを受け渡す。受信側では, 逆に添付ファイル開く際にインテントで署名データを本アプリへ受け渡す。この方法を取ることで, ユーザの普段の環境を変えることなく署名の作成・添付が可能にしている, 尚且つ汎用性を高めている。

5. 評価と考察

5.1 評価

(1) 導入が比較的容易である

従来の S/MIME や PGP は事前に公開鍵サーバーを用意するなど準備の手順が多く手間がかかるが, 本システムではユーザーの個人間のみで完結しているため少ない手順で認証システムの構築が可能である。図 3 に本稿の認証概要図, 図 4 に S/MIME 概要を示す。一見, 図 4 の署名メールと近い処理をしているように見えるが, 証明書を用意する手順が本システムでは必要ない。ID ベース暗号がそれを可能にしている。

(2) 楕円曲線の離散対数問題に帰着するので安全である

一般に, 楕円曲線上の点 P , 任意の整数 k に関して $N = k \times P$ と乗算を行った場合, N から k を特定することは困難である。また, 署名長を従来より短くすることが出来る。

(3) なりすましが出来ない

メール送信に IC カードを必要としているため, 送信者を騙られても判別することが出来る。また, 送信

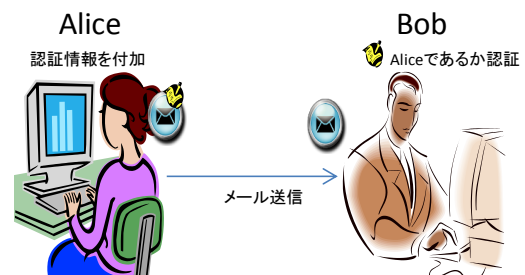


図 3 本稿の認証

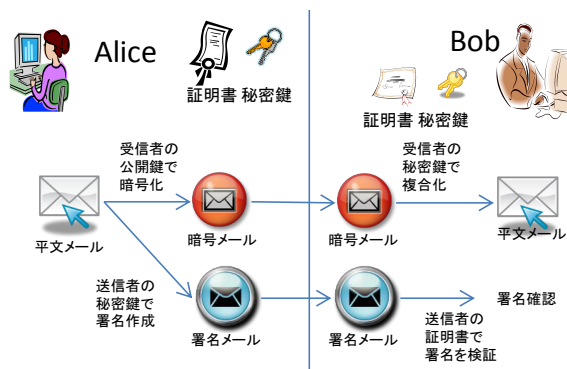


図 4 既存の認証

者のシステム内に侵入された場合でも、この認証システムを導入している相手にメールを送信されたとしても不正なメールとして拒否することが出来る。仮に、ICカードを紛失しても、送信者で無い限り同じ C_{key} は計算出来ないため安全である。鍵の更新も容易であり、セットアップ1・2を再び行えば良い。

5.2 課題

- 物理的なICカードを使っているためユーザーの手順が増加する
 手順は増加するが、必要な手順になっているので自然な流れとしてシステムに組み込みたい。
- 受信者の管理する鍵 C_{key} の管理が重要である
 近年ではスマートフォンを狙ったウイルスも存在しており、必ずしも安全とはいえないためシステムの保護をはじめ、鍵の管理は非常に重要である。
- シード認証値 S を数珠つなぎにハッシュ関数をかける時間

nexus7上で数珠つなぎにハッシュ関数SHA256を用いると平均で表1の時間だけかかることがわかった。表1から分かるように、ハッシュ関数をかけただけ計算時間は概ね線形的に増加するが、現実的なメールのやり取りの回数を考慮すると通常使用する上で極端に計算時間が長くなることはない。また、スマートフォンの機種によってCPUの性能が変わってくるため計算時間もそれぞれ変化するが、CPUの性能も次第に高くなっている傾向からどのような機種でも動作に影響することは少ない。しかし、効率が良いとは言えないので、効率がよく、尚且つ同期が取れる方法があればそれと入れ替えたい。

表 1 ハッシュ関数SHA256を使用した時の平均時間

回数	1回	10回	100回	1000回
時間	1.56ms	13.46ms	140.96ms	1349.73ms

6. おわりに

本稿では標的型攻撃メール対策として、IDベース暗号とICカードを利用した送信者を認証するためのシステムを提案、プロトタイプの実装をした。S/MIMEやPGPとは異なるメール認証として導入・利用ができるのではないだろうか。

謝辞

本稿の作成にあたり、ご協力頂いた研究室の皆様に深く感謝いたします。

参考文献

- [1] IPA: “IPA テクニカルウォッチ『標的型攻撃メールの分析』に関するレポート”, <http://www.ipa.go.jp/about/technicalwatch/20111003.html>, 2011
- [2] B Ramsdell, Brute Squad Labs, S. Turner ほか: “S/MIME Version 3.2 Message Specification”, RFC5751, 2010
- [3] J. Callas, PGP Corporation, L. Donnerhacke ほか: “OPEN PGP Message Format”, RFC4880, 2007
- [4] ネットエージェント株式会社: “標的型攻撃メール対策 防人”, <http://www.netagent.co.jp/product/sakimori/>, 2012
- [5] 伊藤史人, 高見澤秀幸, 佐藤郁哉: “標的型攻撃メールの予防対策”, 学術情報処理研究 No.16 p100-110, 2012
- [6] CRYPTREC: “IDベース暗号に関する調査報告書”, <http://www.cryptrec.go.jp/report/c08.idb2008.pdf>, 2008
- [7] W. Diffie, M. E. Hellman: “New Directions in Cryptography”, IEEE Transactions on Information Theory, vol.IT-22, No.6, pp.644-654, 1976.