Vol.2012-CSEC-58 No.37
Vol.2012-SPT-4 No.37
2012/7/20

電子メールの特徴情報を用いた 標的型メールへのクライアント対策技術の提案

吉岡 孝司[†] 片山 佳則[†] 津田 宏[†] 森永 正信[†] 深澤 亮太[††]

近年，特定企業や個人を標的に，機密情報の窃取を目的としてメールを送りつける標的型メール攻撃が急増している．標的型メール攻撃では，送信者を詐称したり，件名，本文の巧妙な記述によって細工されるため，受信者はうっかり添付ファイルを開いてしまうことで感染する．攻撃者は，受け手に合わせて，攻撃手法を変化させるため，迷惑メールフィルタやウイルス対策ソフトウェア等の一般的な対策では解決困難である．本論文では，メールヘッダや本文の中で，攻撃者が詐称することが困難な送信者固有の特徴情報を利用した，標的型メールへのクライアント対策技術を提案する．また，本技術を適用し，メールを開く前に，標的型メールの可能性を端末側でリアルタイムに検知・警告するプロトタイプを開発したので，その実装報告を行う．

A Client-side Solution for Protection Against Targeted Email Attacks Using Email Feature Information

TAKASHI YOSHIOKA[†] YOSHINORI KATAYAMA[†] HIROSHI TSUDA[†]
MASANOBU MORINAGA[†] RYOTA FUKASAWA[††]

As the first step to steal confidential information from targeted organization, targeted email attacks are increasing rapidly. By impersonating a legitimate sender with falsified "From" field, and carefully crafted email title, message body, signature, and attachments, the attacker sends an email which the receiver opens unwittingly and infects the victim with malware. As the attacker changes his tactics and tricks adaptively for each receiver, it is extremely difficult for current mass-market protections such as spam email filter and anti-virus software protect from such attacks. This paper proposes a client-side solution to protect email receivers from such attacks by utilizing email features which is difficult for attackers to forge. Based on this proposal, we have implemented a prototype, which warns an email receiver of potential email attacks before she opens the emails and its implementation details are given in this paper.

1. はじめに

近年，機密情報の窃取を目的に，特定企業や組織，個人のコンピュータを標的として攻撃を執拗に仕掛ける「標的型攻撃」が問題となっている．この標的型攻撃においては，マルウェアと呼ばれる不正なコードを仕掛けた文書ファイル等を，電子メールに添付して相手に送りつける攻撃（標的型メール攻撃）が一般的な手法となっている．

標的型メール攻撃は，迷惑メールのように，無差別，かつ大量に一括送信される不特定多数への攻撃ではなく，ある特定の対象を定めて攻撃が行われる特徴を有する．

例えば，実在の組織や個人の発信元を詐称し，正当な業務や依頼であるかのように見せかけ，件名や本文を作成する等，巧妙に細工されたメールを送りつけ，添付ファイルを開くように誘導する．このため，受信者は一見しただけでは怪しいメールだと判断できず，うっかり添付ファイルを開いてしまう．その結果，ソフトウェアの脆弱性等が悪用され，不正コードによるウイルス感染や，特定サイトへの誘導によるウイルス送信を誘発させ，機密情報が漏えいする事態となっている．

標的型攻撃への対策としては，ソフトウェアを最新状態に維持することや，ウイルス対策ソフトウェアの適切な運用が挙げられる．しかしながら，修正プログラムが未だ提供されていないソフトウェアの脆弱性（ゼロデイ脆弱性）を悪用して行われる攻撃は防ぐことができない．

このように，標的型メール攻撃では，既存パターンで検知できない新しいマルウェアを仕掛ける等，その手法を巧みに変化させるため，迷惑メールフィルタやウイルス対策ソフトウェアによる一般的な対策では解決困難である．

さらに，個々の受信メールに対して，差出人アドレスや配送経路等を記録したメールヘッダや，本文，添付ファイルを参照し，その整合性を受信者が逐一チェックし，怪しいメールか否かを判別するのには限界がある．

このため，メーラーによるメール受信前に，標的型メールの可能性を自動的に判定し，受信者に対して，注意喚起の警告を発する仕組みを導入することが望ましい．

本論文では，メールヘッダや本文の中で，攻撃者が詐称することが困難な送信者固有の特徴情報を利用し，送受信での連携による検知の高精度化技術と，受信履歴を用いた送信者特徴のソーシャル分析技術を提案する．

また，本技術を適用し，メールを開く前に，標的型メールの可能性をリアルタイムに検知・警告するプロトタイプを開発したので，その実装報告を行う．

[†] (株)富士通研究所
FUJITSU LABORATORIES LTD.
[††] (株)富士通ソーシアルサイエンスラボラトリ
FUJITSU SOCIAL SCIENCE LABORATORY LIMITED

2. 標的型メール攻撃

本章では，標的型メール攻撃についてまとめる．

2.1 標的型メール攻撃の概要

標的型メール攻撃は，特定企業や個人を狙い，送信者の詐称や件名，本文の巧妙な記述によって，添付ファイルを開かせたり，記載 URL をクリックさせることで，機密情報の窃取を行うことを目的とした攻撃である．

2005 年 10 月に，実在する官公庁職員を詐称して複数の官公庁職員宛に送られた標的型メールが確認されて以来，多数確認され，被害も報告されている．

また，マルウェアを仕掛ける文書ファイルとして，PDF や Microsoft Word/Excel のような業務で利用されやすいアプリケーションで作成した文書が多く，ウイルス対策ソフトウェアでも検知されない事例も多い．

2.2 標的型メール攻撃の特徴

不特定多数に送られるマスメール型ウイルスメールと，標的型メールの違いについて，表 1 にまとめる 1)．

表 1　マスメール型ウイルスメールと標的型メールの比較

	攻撃者の目的	件名	本文	送信者	添付ファイル
マスメール型	社会混乱	一般的な用件	一般勧誘指示	個人名や不明組織	実行形式
標的型	特定組織からの情報窃取	自分に関係ありそうな用件	関心事	官公庁・大企業を詐称	文書形式

特に，送信元を実在する信頼できそうな組織や個人を装い，自分に関係がありそうな件名や関心のある本文，時事ネタにして受信者の関心を引き付け，添付ファイルを開くように誘導する手口が主流である．

3. 関連研究

本章では，標的型メールに対する検知・防御のための関連研究についてまとめる．主に，メールヘッダの蓄積・解析による対策技術 2)や，送信元サーバ認証による対策技術 3), 4)に分類できる．

2)では，受信のたびにメールヘッダの特徴を蓄積しておき，今回受信したメールヘッダと過去に受信したメールヘッダとを比較することで，標的型攻撃である可能性を判定・評価する研究が行われている．

3)，4)は，送信メールサーバの正当性や送信経路の証跡をサーバベースで実現する，送信ドメイン認証に関連する技術である．また，4)に対する機能拡張の研究として，5)が提案されている．

送信ドメイン認証は，メールアドレスのドメインをチェックし，そのメールが正規のサーバから発信されているか否かを検証し，送信者のアドレスが正規のものであることを証明する技術である．

送信ドメイン認証の種類として，IP アドレスによる認証（SPF/Sender ID）と，電子署名による認証（DKIM）がある．SPF/Sender ID は，メールサーバのドメインと送信者の IP アドレスの関連（SPF Record）を DNS サーバに公開し，受信時に送信者 IP アドレスを DNS サーバに問合せ，送信者のアドレスが正規のものであることを確認する．

DKIM は，PKI ベースの送信ドメイン認証技術である．メールサーバの公開鍵を DNS サーバに登録し，秘密鍵で電子署名を行ってメール送信．受信時に公開鍵を DNS サーバに問合せ，送信者のアドレスが正規のものであることを確認する．

標的型メール攻撃では，送信者の詐称が行われる場合が多く，標的型攻撃の成立を難しくする緩和策としての利用が考えられる．しかしながら，送信ドメイン認証を導入した正規サーバを利用して攻撃される場合も考えられ，その場合，本人性を担保することができない．

また，サーバベースで行う対策では，導入コストや電子証明書の発行・運用コスト，多くの受信端末から解析・検証処理依頼が発生することが予想され，負荷が大きくなるという課題が残る．

4. 標的型メール対策技術

本章では，標的型メールへの対策技術について述べる．

4.1 提案方式

3 章で述べたとおり，送信ドメイン認証のように，サーバベースで行う対策がほとんどである．また，技術的な対策に加え，メール受信の際，標的型メールの可能性があれば受信者に対して警告を発し，注意喚起を促す施策が必要であり，最終的には，メール受信可否の判断を受信者に要求する人間系の対策も必要である．また，利用者にとっては，既存のメール環境を変えずに，低コストで簡単に対策が図れることが望ましい．

そこで，本論文では，サーバの導入コストや処理性能の課題，受信者への注意喚起の即時確認を考慮し，個々の端末において，メーラーによるメール受信前に，標的型メールの可能性をリアルタイムに検出し，受信者に対して，注意喚起の警告を発する仕組みを提案する．

具体的な対策として，メールヘッダや本文の中で，攻撃者が詐称することが困難な送信者固有の特徴情報を利用することで，標的型メールの可能性を判定･検知する技術を提案する．

本論文では，送受信での連携による検知の高精度化技術と，受信履歴を用いた送信者特徴のソーシャル分析技術を提案する．

4.2 送受信での連携による検知の高精度化技術

4.2.1 提案方式

標的型メールへの対策として，送信端末と受信端末が対策ツールを導入し，送信端末での出口対策と，受信端末の入口対策で互いに連携することで，攻撃に対する抑止，な

りすましを防止する．

具体的には，送信端末と受信端末が同じ対策ツールを導入することを前提として，送信端末でメールヘッダや本文等の情報から識別情報を自動生成し，メールに追加して送信．受信端末では，その識別情報の整合性を検証することで，攻撃者によるなりすましを防止する（図 1 参照）．

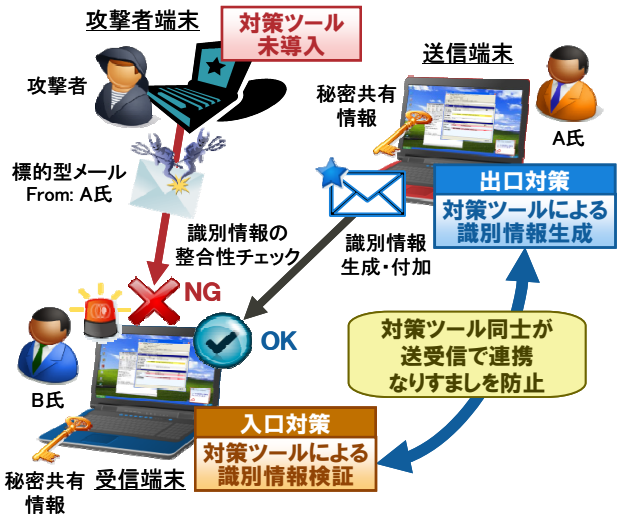

図 1　送受信での連携による検知の高精度化技術

識別情報の生成には，送信端末と受信端末の双方で，共通鍵やキーワード等，攻撃者が知りえない情報を共有し，この秘密共有情報を用いて，識別情報を生成することで，攻撃者が識別情報を容易に生成・偽装できない仕組みとする．例えば，社内や関連会社，委託先，協業他社等の間でメールをやりとりする際は有効であり，組織内メンバーや協業メンバーになりすました攻撃に対して，耐性を持つと考えられる．このように，組織間で予め秘密共有情報を外部に漏えいしない形で共有・管理しておき，メール送信の際，この秘密共有情報を用いて識別情報を生成する．

この仕組みによれば，攻撃者端末に対策ツールが未導入の場合には，識別情報の有無チェックを行うことで判定可能である．また，攻撃者によるメールヘッダの偽装・改変，および何らかの手段で識別情報付きメールが漏えいし，そのメールに記載された識別情報がそのまま引用されたとしても，識別情報の整合性を受信端末で検証することにより，怪しいメールか否かの判定を行うことが可能である．

このように，送信端末と受信端末でお互いにしか知り得ない秘密共有情報を用いて，識別情報を生成・検証することにより，攻撃者はその秘密共有情報を知らなければ識別情報を作ることができないという防御が可能になる．

4.2.2 識別情報の生成方式

本節では，送信端末で処理する識別情報の生成方式について述べる．

秘密情報を受信端末と共有する必要があるが，本論文では，その方法については特に言及しない．秘密共有情報は，外部に漏えいしないよう安全管理が行われていることを前提とする．また，識別情報の生成アルゴリズム，および後述する対象ヘッダ項目も送受信端末で共有する．

送信端末では，メール送信前に，識別情報の生成処理を行う（図 2，図 3 参照）．

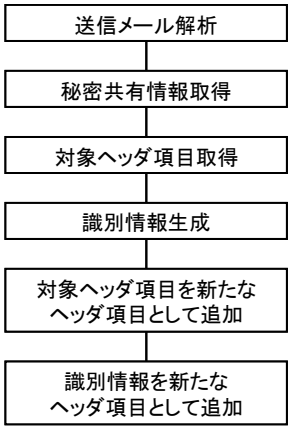

図 2　識別情報の生成処理の流れ

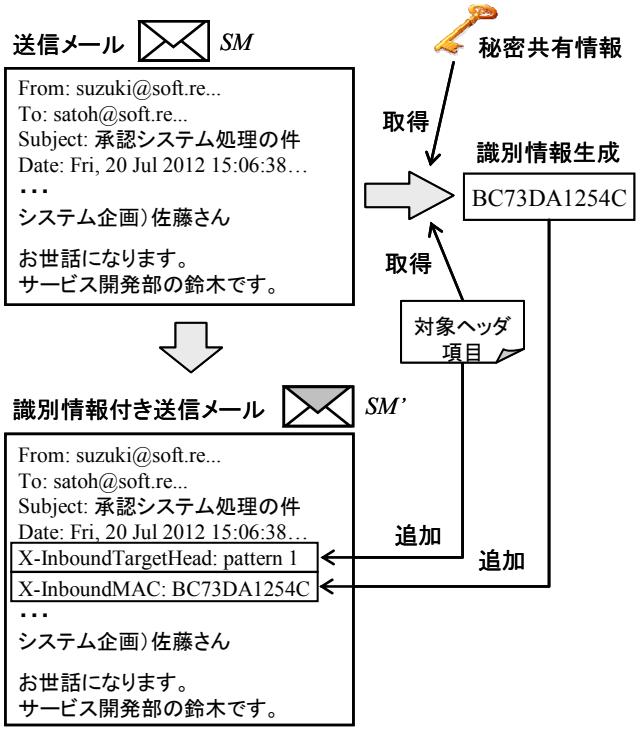

図 3　識別情報の生成処理の概要

送信メール *SM* の解析を行い，識別情報を生成するために必要な秘密共有情報と生成アルゴリズム，対象ヘッダ項目の取得を行う．

識別情報の生成アルゴリズムとして，一方向性ハッシュ関数や，HMAC 6)等が利用可能である．

対象ヘッダ項目とは，送信メールのヘッダ項目や本文，添付ファイルを対象とし，どの項目を識別情報の生成対象とするかを示す情報である．例えば，複数のヘッダ項目や，本文の全文，もしくは一部，添付ファイル等を対象ヘッダ項目とすることができる．

対象ヘッダ項目は，運用環境のセキュリティ強度に応じ，あらかじめ複数のパターンを用意し，例えば，管理者が任意に選択して使用する．また，メール本文の内容やその重要度によって，メール単位でその対象の選択肢，識別情報の生成方法をポリシー制御する．

SM から，対象ヘッダ項目の情報を抽出し，秘密共有情報を含めて，対象ヘッダ項目に対する識別情報を生成する．

対象ヘッダ項目と，生成した識別情報は，*SM* の新たなヘッダとして，識別情報ヘッダに追加し，識別情報付き送信メール *SM'*とする．識別情報ヘッダとは，対象ヘッダ項目と，識別情報の 2 つを指し，それぞれ *X-InboundTargetHead* と，*X-InboundMAC* として追加する．*SM'*を送信対象とする．

4.2.3 識別情報の検証方式

本節では，受信端末で処理する識別情報の検証方式について述べる．秘密共有情報，生成アルゴリズム，対象ヘッダ項目を送信端末と共有する必要がある．

受信端末では，メール受信前に，識別情報の検証処理を行う（図 4，図 5 参照）．

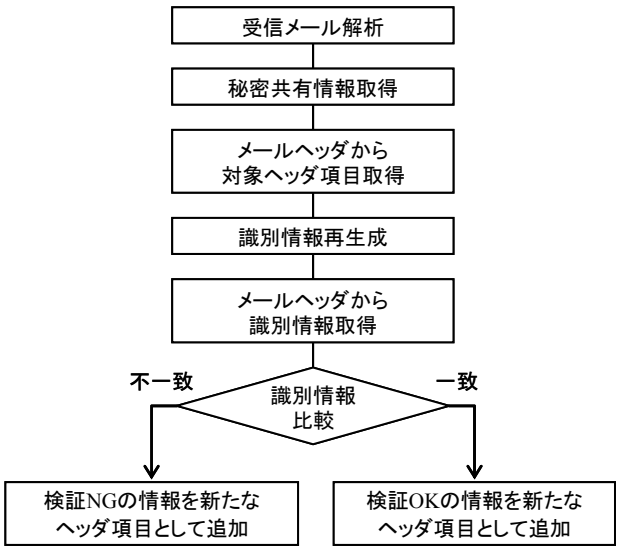

図 4　識別情報の検証処理の流れ

識別情報付き受信メール *RM* の解析を行い，識別情報の再生成を行うために必要な秘密共有情報と生成アルゴリズム，対象ヘッダ項目の取得を行う．対象ヘッダ項目は，*RM* のヘッダから取得する．

識別情報ヘッダ（*X-InboundTargetHead*，*X-InboundMAC*）を除く *RM* から，秘密共有情報を含めて，対象ヘッダ項目に対する識別情報を再生成する．この生成方法は，送信端末と共有した生成アルゴリズムと同じとする．

RM のヘッダ（*X-InboundMAC*）から，識別情報を取得し，再生成した識別情報と比較を行い，一致するか否かの確認を行う．この検証結果は，*RM* の新たなヘッダとして，識別情報検証結果ヘッダ（*X-InboundMACCheck*）に追加する．一致した場合は検証成功とし，*X-InboundMACCheck: OK* を追加し，識別情報検証結果付き受信メール *RM'*とする．

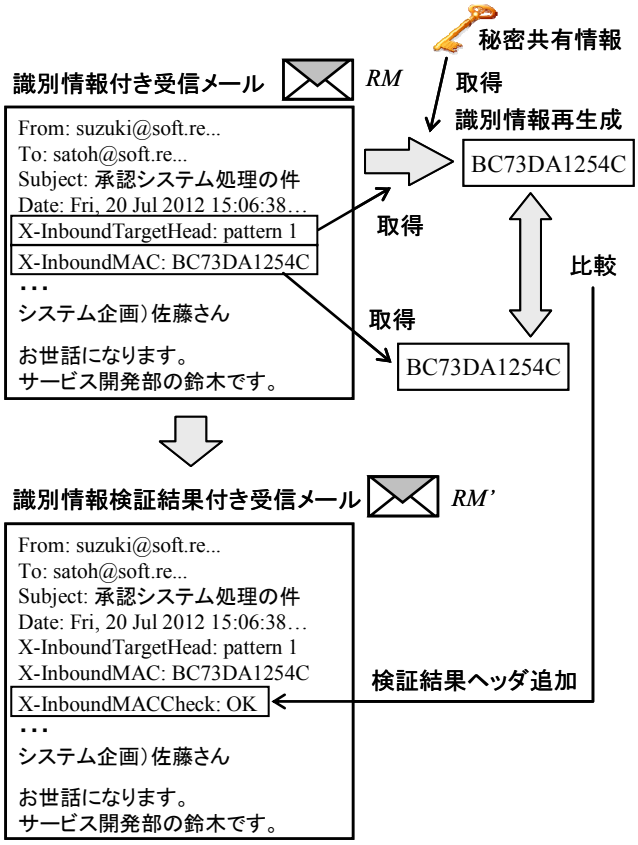

図 5　識別情報の検証処理の概要

4.3 受信履歴を用いた送信者特徴のソーシャル分析技術

4.2 節では，送受信端末で対策ツールを導入し，識別情報による連携を行うことで，攻撃に対する抑止，およびなりすましを防止した．しかしながら，送信端末に必ずしも対策ツールが導入されているとは限らず，相手側に対策ツールを導入してもらわなければならないという制約が残る．よって，対策ツールを導入していない相手からでも，標的型メールの可能性を判定できる仕組みが必要である．

そこで，さらなる強化対策として，受信履歴を用いた送信者特徴のソーシャル分析技術を提案する（図 6 参照）．

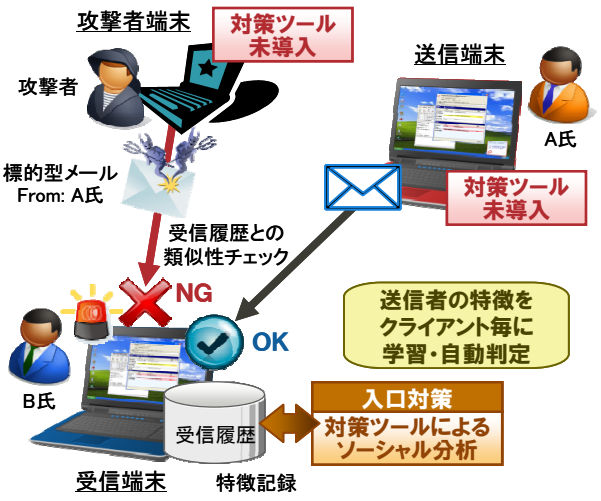

図 6　受信履歴を用いた送信者特徴のソーシャル分析技術

具体的には，これまでのメール受信履歴を，差出人アドレスごとに整理して，データベースとして蓄積しておき，新規の受信メールと，この蓄積データベースの情報との類似性を確認することで，差出人になりすました標的型メールか否かを判定する．この類似性確認においては，差出人アドレスごとに受信履歴を単純に蓄積して比較するのではなく，送信者の特徴をこれまでの履歴情報から，より明確に抽出させるために，送信者ごとの重み情報を採用する．

重み情報とは，受信履歴から，送信者の特徴情報を複数選択・抽出し，独自の算出アルゴリズムによって得られる情報である．この重み情報により，各送信者の特徴を堅実に捕えて，その類似性を判定する（図 7，図 8 参照）．データベースへの蓄積と類似性確認は,受信端末ごとに行う．

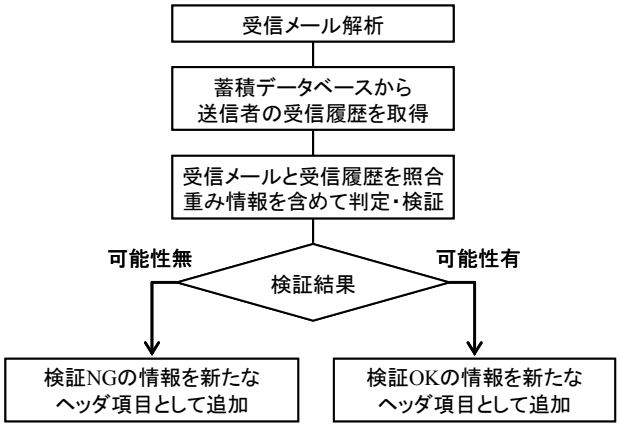

図 7　特徴情報検証処理の流れ

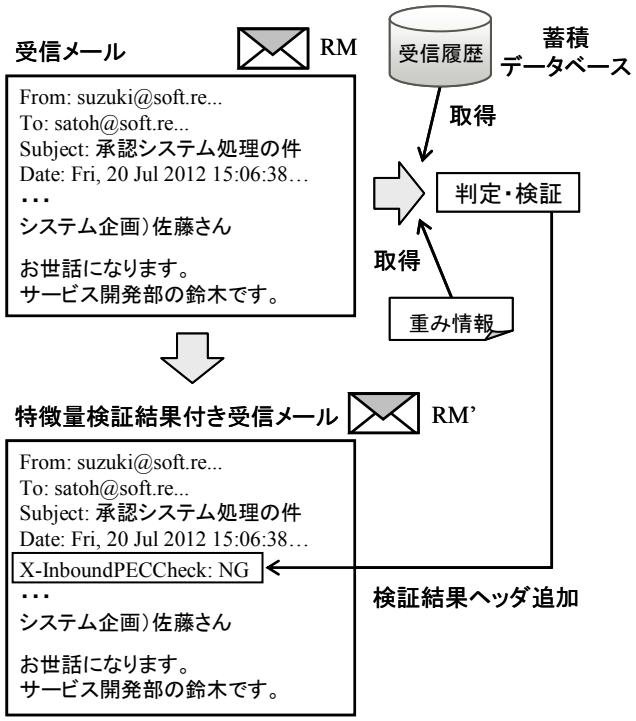

図 8　特徴情報検証処理の概要

受信メール *RM* の解析を行い，差出人アドレスを検索キーに，蓄積データベース内の受信履歴を検索・取得する．受信メールと受信履歴を照合し，重み情報を含めて標的型メールの可能性があるか否かの判定を行う．この検証結果は，*RM* の新たなヘッダとして，特徴情報検証結果ヘッダ（*X-InboundPECCheck*）に追加する．

この判定処理で標的型メールの可能性がある場合は，*X-InboundPECCheck: NG* を追加し，特徴情報検証結果付き受信メール *RM'*とする．

4.4 提案方式による判定方法

本節では，4.2 節，4.3 節で提案した技術による，標的型メールの判定方法について述べる．図 9 に，提案方式による判定処理の流れを示す．

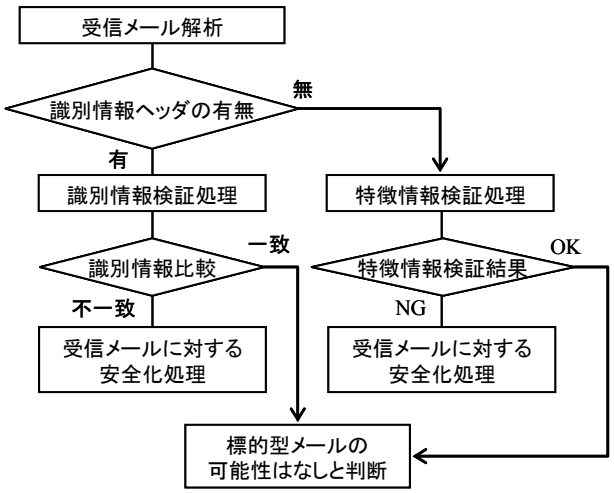

図 9　識別情報と特徴情報による判定処理の流れ

メール受信時，受信メールの解析を行い，識別情報ヘッダが存在するか否かの確認を行う．これは，*X-InboundTargetHead*，*X-InboundMAC* を参照することで存在確認が可能である．

識別情報ヘッダが存在する場合は，4.2.3 節で述べた識別情報検証処理を行い，不一致の場合は，受信メールに対する安全化処理を行う.識別情報ヘッダが存在しない場合は，4.3 節で述べた特徴情報検証処理を行う．標的型メールの可能性があれば，識別情報検証処理同様，受信メールに対する安全化処理を行う．

なお，高速化のために，添付ファイルや記載 URL を含まない受信メールに関しては，上記処理を省略することも考えられる．

4.5 効果

提案方式により，運用コスト等で課題となっていた，サーバでの対策（SPF/Sender ID，DKIM 等）を取らなくても，クライアントベースで標的型メールの可能性を判定・検知することが可能になる．

送受信での連携による検知の高精度化技術では，予め送信端末と受信端末で共有した，秘密共有情報，生成アルゴリズム，対象ヘッダ項目を用いて，秘密共有情報を含む識別情報を生成・検証を行うため，これら共有情報が攻撃者

に漏えいしない限り，ヘッダを偽装して識別情報を生成することができなくなる．よって，識別情報は付加されているが，整合性が確認できない受信メールに関しては，標的型メールの可能性があると判断することができる．

また，対策ツールを導入していない相手からでも，受信履歴を用いた送信者特徴のソーシャル分析技術を採用することで，過去の受信履歴から送信者の特徴を重み情報と共に判定し，類似性確認することで，標的型メールの可能性の有無をより確実に判断することができる．

これら技術を利用し，判定・検知を行うことで，標的型メールの受信確率を軽減させることが可能になる．

5. 試験実装

プロトタイプ実装により，識別情報生成・検証機能，および特徴情報検証機能の実現可能性検証を行った．

本章では，プロトタイプシステムの構成と，実装機能について述べる．

5.1 プロトタイプシステム

送受信端末とメールサーバの間に，送受信メールの解析・制御による標的型メールの判定・安全化処理を行うプロトタイプシステムを開発した（図 10 参照）．

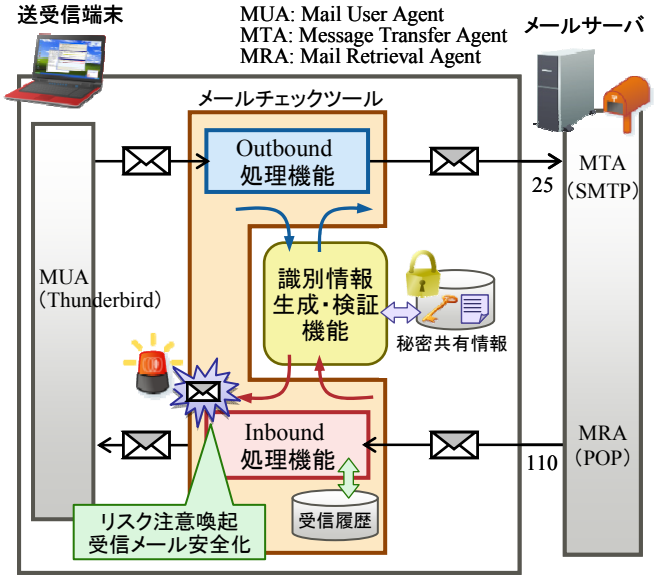

図 10　プロトタイプシステムの構成

送信メールに対して，識別情報の生成制御を行う Outbound 処理機能と，受信メールに対して，識別情報の検証制御，および特徴情報検証を行う Inbound 処理機能を開発した．

識別情報生成・検証機能は，今後の機能拡張・応用展開を考慮し，各処理機能とは別に外部コマンド（Java 実装）として用意し，各処理機能から呼び出して実行する仕組みとした．

これら機能をメールチェックツールとして統合し，送受信端末上に常駐させ，SMTP 中継機能，および POP 中継機能として動作させた．送受信メーラー（MUA）として，Mozilla Thunderbird を使用した．

5.2 識別情報生成機能の実装

添付ファイル付きの送信メールに対して，Outbound 処理機能からの要求を受け付け，送信メールの解析処理，および識別情報の生成機能を実装した．

秘密共有情報，生成アルゴリズム，対象ヘッダ項目を，受信端末と共有し，同一の情報，アルゴリズムを利用した．

対象ヘッダ項目として，ヘッダの一部と本文，および添付ファイルを選択した．識別情報の生成アルゴリズムには，HMAC-SHA256 を使用し，秘密共有情報を鍵情報として，対象ヘッダ項目と組み合わせてハッシュ値を算出．このハッシュ値を識別情報とした．

Outbound 処理機能は，送信端末上の常駐プロセスとして動作させ，MUA からの SMTP 接続要求を待機する．Outbound 処理機能は，MUA との接続を確立後，送信メールを取得し，それを入力として，識別情報生成機能を呼び出し，識別情報の生成・取得を行う．

対象ヘッダ項目，および取得した識別情報は，識別情報ヘッダ（*X-InboundTargetHead*，*X-InboundMAC*）として，送信メールヘッダに追加した．識別情報ヘッダを付加したメールを，MTA へ送信する．

5.3 識別情報検証機能の実装

添付ファイル付きの受信メールに対して，Inbound 処理機能からの要求を受け付け，受信メールの解析処理，および識別情報の検証機能を実装した．

秘密共有情報，生成アルゴリズム，対象ヘッダ項目を，送信端末と共有し，同一の情報，アルゴリズムを利用した．

Inbound 処理機能は，受信端末上の常駐プロセスとして動作させ，MUA からの POP 接続要求を待機する．Inbound 処理機能は，MUA との接続を確立後，MRA との接続を確立し，受信メールを取得する．

識別情報ヘッダを確認し，受信メールを入力として，識別情報検証機能を呼び出し，識別情報の検証を行う．識別情報が一致した場合，識別情報検証結果ヘッダとして，*X-InboundMACCheck: OK* を受信メールヘッダに追加した．

識別情報が一致しない場合，識別情報検証結果ヘッダとして，*X-InboundMACCheck: NG* を追加し，受信メールに対する安全化処理を行う機能を実装した．

具体的には，標的型メールの可能性がある旨を受信者に明示するため，識別情報の不整合を示す警告画面を，送信端末の画面に表示した．また，件名ヘッダ（*Subject:*）への警告表示の追加に加え，警告ヘッダ（*X-InboundAnalyze: Warning*），およびメール本文の先頭に標的型メールの可能性がある旨の警告メッセージを追加した．

さらに，添付ファイルを強制的に削除する機能，および所定のフォルダに強制隔離する機能を実装した．Inbound 処理を行った旨を受信者に通知するため，入口通過ヘッダ

（*X-InboundPolicyCheck: OK*）も追加した．

最後に，識別情報検証結果ヘッダと，入口通過ヘッダを追加した安全化処理メールを，MUA へ送信する．

5.4 特徴情報検証機能の実装

識別情報ヘッダが付加されていない受信メールの場合，差出人アドレスごとに特徴情報を整理した受信履歴をもとに，類似性確認を行う Inbound 処理機能を実装した．

受信履歴のある差出人アドレスからの場合，受信メールの特徴情報検証処理を行う．

標的型メールの可能性がない場合，特徴情報検証結果ヘッダとして，*X-InboundPECCheck: OK* を受信メールヘッダに追加した．標的型メールの可能性がある場合，特徴情報検証結果ヘッダとして，*X-InboundPECCheck: NG* を追加し，受信メールに対する安全化処理を行う機能を実装した．

また，受信履歴のない，初めて受信する差出人アドレスからの受信においては，標的型メールの可能性があると判定し，警告画面を表示した．

6. 試験実装の評価

実際に，正常メールと偽装メールを作成して，メール送受信し，プロトタイプで本提案方式の検証を行うことで，試験実装の評価を行った．

6.1 動作概要

まず，以下 3 種類の送信メールを作成した．（A）は，正規送信者が作成する通常メール，（B），（C）は，攻撃者が作成する標的型メールに相当する．添付ファイルは，任意の PDF ファイルを用意した．

また，指定の差出人アドレスから受信したメールの特徴情報を，予め受信履歴として保存した上で評価した．

（A） 5.2 節の方法で，送信メールから識別情報ヘッダを追加して作成した，添付ファイル付き送信メール

（B） 正規の識別情報付きメールから，メールヘッダのみコピーして作成した，添付ファイル付き送信メール

（C） 受信履歴のない特徴情報で作成した，添付ファイル付き送信メール

（A）は，Thunderbird でメール作成し，送信ボタンを押下することで，メールチェックツールの Outbound 処理機能を介して，メール送信する．

（B），（C）は，テキスト形式で偽装メールを作成し，メールチェックツールを介さず，sendmail コマンドを用いてメール送信する．

（A），（B），（C）のメール受信処理は，Thunderbird で行う．受信ボタンを押下することで，メールチェックツールの Inbound 処理機能を介して，メール受信する．

（A），（B），（C）のメール受信時の判定結果は，以下のとおりである．まず，（A）では，識別情報の検証結果が正常となり，Thunderbird の受信トレイに受信メールが格納される．また，識別情報ヘッダ（*X-InboundTargetHead*，*X-InboundMAC*），入口通過ヘッダ（*X-InboundPolicyCheck: OK*），および正常結果を示す識別情報検証結果ヘッダ（*X-InboundMACCheck: OK*）が追加される．

（B），（C）では，判定結果が異常となり，警告画面が表示される．（B）では，受信メールに付加された識別情報ヘッダは，正規メールから単純にコピーされた情報であるため，受信メールから再生成された識別情報と一致しない結果となり，警告画面が表示される（図 11 参照）．

（C）では，予め保存した受信履歴の特徴情報と，受信メールの特徴情報が異なる結果となり，（B）同様に警告画面が表示される．

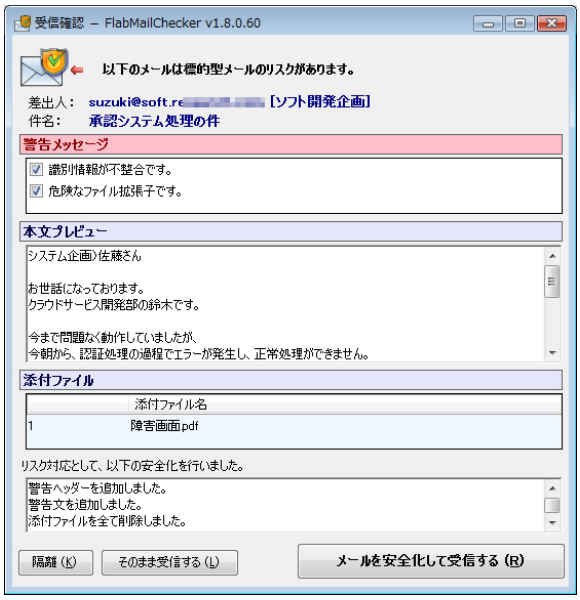

図 11 識別情報不整合による標的型メールの警告画面

警告画面の警告メッセージの項目を，受信者がすべてチェックすることで，“メールを安全化して受信する”ボタンの押下が有効になる．押下のタイミングで，安全化処理されたメールが，Thunderbird の受信トレイに格納される．

MRA に蓄積されているすべてのメールの受信が完了すると，警告画面を表示した（リスクを検知した）標的型メールの可能性のある受信メールに対して，安全化処理の確認画面が表示される（図 12 参照）．

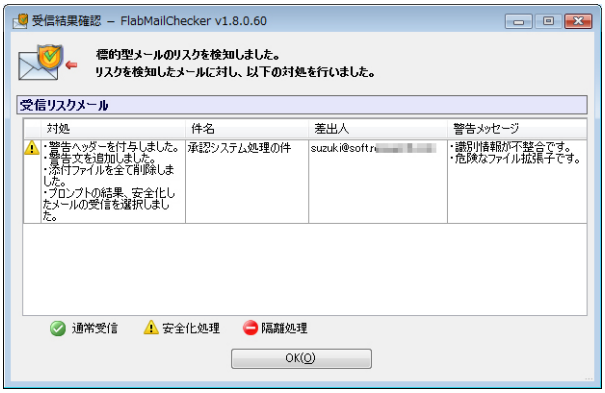

図 12 標的型メールへの安全化処理確認画面

（B），（C）の場合は，受信メールの件名ヘッダ（*Subject:*）先頭に【警告】が追加され，メール本文先頭には，警告メッセージが追加される．また，異常結果を示す警告ヘッダ（*X-InboundAnalyze: Warning*），および識別情報検証結果ヘッダ（*X-InboundMACCheck: NG*）が追加される．さらに，添付ファイルも強制的に削除される（図 13 参照）．

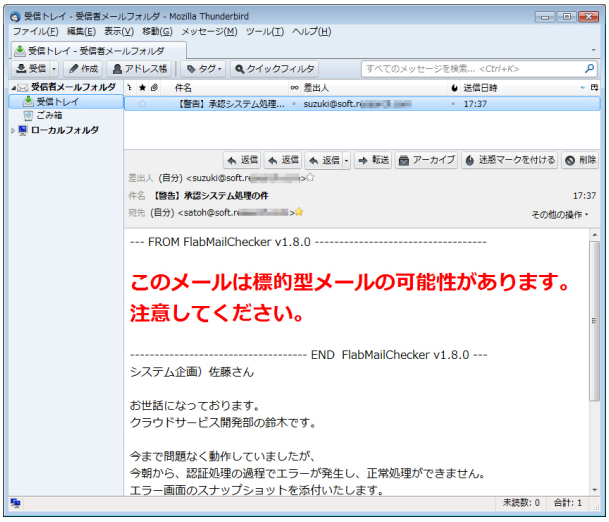

図 13　Thunderbird での安全化受信メールの確認画面

6.2 性能評価

識別情報生成・検証処理の性能評価を行った．表 2 の測定環境と条件で，以下処理時間を測定し，表 3 の結果が得られた．

（I）　メール送信時の識別情報生成処理時間
（II）　メール受信時の識別情報検証処理時間
（III）　メール受信時の識別情報検証処理開始から警告画面が表示されるまでの時間

表 2　測定環境と条件

試験使用のメールサイズ	メールサイズ: 165KB, 769KB, 1470KB 添付ファイルサイズ: 120KB, 560KB, 1070KB
測定環境（PC, メーラー）	OS: Windows XP Professional Version 2002 SP3 CPU: Intel Core 2 Duo T8100 2.10GHz メモリ: 3.23GB RAM メーラー: Mozilla Thunderbird 12.0.1
測定方法・条件	処理ごとに複数のメールサイズで測定．Java VM 等，起動に時間がかかる初回分は除外して平均値を算出

識別情報の生成・検証処理，警告画面の表示処理共に，メールサイズが大きくなる程，処理時間を要した．利用者にとっては，送受信に影響のない範囲での測定値が得られ，処理時間は実用的と考えられる．

表 3　測定結果

メールサイズ [添付ファイルサイズ]	測定結果（単位: ms）		
	(I)	(II)	(III)
165KB [120KB]	571	563	648
769KB [560KB]	797	789	969
1470KB [1070KB]	1094	1094	1375

7. まとめ

本論文では，送受信での連携による検知の高精度化技術と，受信履歴を用いた送信者特徴のソーシャル分析技術を利用し，標的型メールへのクライアント対策技術を提案した．提案方式により，運用コスト等で課題となっていた，サーバでの対策を取らなくても，クライアントベースで標的型メールの可能性を判定・検知することが可能になる．

さらに，メール受信前に，標的型メールの可能性をリアルタイムに検出し，受信者に対して注意喚起の警告を発するプロトタイプシステムを開発し，提案方式の評価を行った．提案方式による標的型メール判定方法で，利用者に影響のない範囲で，負荷なく検知できることを実証した．

提案方式によれば，既存のメール環境を変えることなく，受信者に対して注意喚起の気付きを与え，標的型メールによる感染を軽減させることが可能になる．

また，組織内のメールセキュリティ統制の徹底や，関連会社や委託先等，社内外のメンバーと安全なメール環境を簡単に構築することが可能となる．

今後，標的型メールの訓練と組み合わせて，提案方式の試行評価・検証を行っていく予定である．

参考文献

1) IPA テクニカルウォッチ,「標的型メールの分析に関するレポート～だましのテクニック事例 4 件の紹介と標的型攻撃メールの分析・対策～」, 2011 年 10 月 3 日, 独立行政法人情報処理推進機構, http://www.ipa.go.jp/about/technicalwatch/20111003.html
2) 梅田, 上原, 水谷, 武田. 電子メールヘッダの特徴情報を用いた標的型攻撃の検知, CSS2010, pp.109-114, 2010.10.
3) Sender Policy Framework Project Overview, http://www.openspf.org/
4) IETF, "DomainKeys Identified Mail (DKIM) Signatures", RFC 4871, May 2007. http://www.ietf.org/rfc/rfc4871.txt
5) 東角, 伊豆, 武仲, 吉岡. 部分完全性保証技術 PIAT: 送信ドメイン認証への適用, 電子情報通信学会技術研究報告. pp.129-132, 2007.7.
6) Mihir Bellare, Ran Canetti and Hugo Krawczyk, "Keying Hash Functions for Message Authentication", CRYPTO'96, pp1-15, 1996.