情報処理学会論文誌 Vol.55 No.10 2290–2299 (Oct. 2014)

推薦論文

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[1,a)] 片山 佳則[2] 津田 宏[2] 森永 正信[2] 深澤 亮太[3]

受付日 2013年9月24日, 採録日 2014年7月11日

概要：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，ソーシャルエンジニアリングの手法により，標的対象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，標的型メール攻撃の可能性をクライアント側でメールを開く前に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．

キーワード：標的型攻撃，標的型メール，なりすまし，クライアント対策，標的型メール訓練

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

Takashi Yoshioka[1,a)] Yoshinori Katayama[2] Hiroshi Tsuda[2]
Masanobu Morinaga[2] Ryota Fukasawa[3]

Received: September 24, 2013, Accepted: July 11, 2014

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

Keywords: advanced persistent attack, targeted e-mail, spoofed e-mail, client-side defence, training for targeted e-mail attack

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，

[1] 富士通株式会社
FUJITSU LIMITED, Minato, Tokyo 105–0001, Japan
[2] 株式会社富士通研究所
FUJITSU LABORATORIES LTD., Nakahara, Kanagawa 211–8588, Japan
[3] 株式会社富士通ソーシアルサイエンスラボラトリ
FUJITSU SOCIAL SCIENCE LABORATORY LIMITED, Nakahara, Kanagawa 211–0063, Japan
[a)] takac@jp.fujitsu.com

本論文の内容は 2012 年 7 月の CSEC58 研究発表会にて報告され，同研究会主査により情報処理学会論文誌ジャーナルへの掲載が推薦された論文である．

最初にマルウェアを仕掛けたファイルを，電子メールに添付して攻撃対象に送りつける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・大量に送信される不特定多数への攻撃とは異なり，ある特定の対象を定め，ソーシャルエンジニアリングの手法を用い，対象に合わせて攻撃手法を変化させる．たとえば，実在する個人や組織，上司や知人になりすまし，正当な業務や依頼であるかのように件名や本文を巧妙に細工する．さらに，興味を引く言葉でマルウェアを仕掛けた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．結果，マルウェア感染により，攻撃者に情報窃取の入口を作られてしまうことになる．

標的型メール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，ウイルス対策の適切な運用があげられる．しかしながら，修正プログラムがいま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，既存パターンで検知不能な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，一般的な対策では解決困難である．

また，メールの送信者を詐称できること等は知識として知っていても，実際にメールヘッダ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，メールを開く前に，標的型メール攻撃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，送受信で連携して送信者固有の情報をチェックすることでなりすましを検知する技術と，受信履歴を基にした送信者の特徴分析技術により，メールを開く前に，標的型メール攻撃の可能性をリアルタイムに検知・警告する技術について，プロトタイプ評価も含めて述べる．

2. 標的型メール攻撃

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，マルウェアを仕掛けた添付ファイルや，本文中のURLリンクを開かせることで，機密情報の窃取を行うことを目的とした攻撃である．

2.2 標的型メール攻撃の特徴

不特定多数に送られる迷惑メール等のマスメール型メールと，標的型メールの違いについて，文献 [1] を基に，**表 1** にまとめる．

特に，送信元を実在する信頼できる組織や個人を装い，受信者の関心のある件名や本文，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標的型メール攻撃の特徴である．また，標的型メール攻撃では添付ファイルの形式としては，Word や Excel 文書に加え，実行形式のファイルを仕掛けた ZIP や LZH 等が増えてきている [2]．

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
Table 1 Comparison between mass e-mail virus and targeted e-mail.

	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，ZIP等

3. 関連研究

本章では，標的型メール攻撃に対する検知，防御技術に関する国内と海外の学術研究，ならびに標準仕様について調査したので，その内容と対策に向けた課題について述べる．大別して，メール解析で攻撃を検知する端末ベースの対策と，送信元サーバ認証によるサーバベースの対策に分類できる．

3.1 端末ベースの対策技術

メール解析で攻撃を検知する端末ベースの対策として文献 [3], [4], [5], [6] のような研究が行われている．

文献 [3] は，ベイジアンフィルタを利用し，メールの件名や本文中に出現するキーワードの出現頻度を学習することで，怪しいメールか否かの判定を行う技術である．現在のベイジアンフィルタは，無差別・大量に送信される迷惑メールには効果的とされている．

文献 [4] では，送信者のなりすましを検知するため，メールヘッダの特徴を蓄積し，受信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，標的型メール攻撃である可能性を判定・評価する手法が提案されている．受信者への警告表示による注意喚起を行うプロトタイプを試作している．

文献 [5], [6] は，S/MIME でメッセージ署名を付加・検証することで，なりすましを防止する技術である．S/MIME は，PKI のインフラを利用して機能する．送信側では，認証局（CA）が発行する電子証明書を取得し，送信者の秘密鍵を用いてメール本文に対する電子署名を付加する．受信側では，送信者の公開鍵証明書を取得し，電子署名の検証を行うことで，改ざんされていないことを確認可能とする．

3.2 サーバベースの対策技術

文献 [7], [8], [9] は，送信元サーバを認証するための研究であり，特に，文献 [8], [9] 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

ン認証技術である．具体的には，メールアドレスのドメインをチェックして，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，送信者アドレスの正当性を証明する．

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）[8] と，電子署名による認証（DKIM）[9] がある．

SPF 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 サーバに問い合せ，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付加してメールを送信する．受信時に公開鍵を DNS サーバに問い合せ，送信者のアドレスが正規のものであることを確認する．

3.3 標的型メール攻撃対策に向けた課題

なりすましによる標的型メール攻撃を困難にする対策として，送信ドメイン認証の技術の利用が考えられる．しかし，正規の電子証明書を用いたサーバから発信したり，送信ドメイン認証が成功する正規のメールサーバを経由して攻撃を仕掛けたりする場合も考えられる．また，送信ドメイン認証では，ドメインの正当性を保証するだけで，送信者が正当であるかは保証しない．さらに，正規の電子証明書を用いて S/MIME 署名した標的型メールを送りつける場合も考えられる．S/MIME は，送信者の識別と本文が改ざんされていないことを確認する技術であり，標的型メール攻撃か否かを判断できない．また，S/MIME は，電子証明書を取得するコスト等の要因で，十分に普及しているとはいえず，対策としての利用には限界がある．

ベイジアンフィルタは，迷惑メールのように独特の表現を使うものは検知しやすいが，個人ごとにカスタマイズされた一般の業務メールに似せた内容のメール攻撃には限界がある．サーバベースで行う対策では，導入・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. 標的型メール攻撃対策技術

本章では，提案する標的型メール攻撃対策技術について述べる．

4.1 アプローチ

現実的な標的型メール攻撃の対策として，メール受信の際，標的型メール攻撃の可能性があれば受信者に対して警告を発し，注意喚起を促す仕組みに加え，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や，警告と判断したメールを隔離する等の安全化対策も必要である．さらに，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．

本論文では，正規送信者と攻撃者の判別困難さや，サーバの導入コスト・処理性能の課題を解決し，受信者への注意喚起による即時確認や安全化対策を実現するために，個々の端末において，メールを開く前に，標的型メール攻撃の可能性を検知する技術について提案する．具体的な対策として，送受信での連携による検知の高精度化技術と，受信履歴を基にした送信者ごとの特徴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

標的型メール攻撃への対策として，送信端末と受信端末が連携することで，攻撃者が第三者になりすました標的型メール攻撃を防止する．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する．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）．

送信端末と受信端末の双方で，共通の鍵やキーワード等，攻撃者が知りえない情報を共有し，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．

本仕組みでは，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場合に有効である．送信ドメイン認証が成功する正規のメールサーバを経由した攻撃に対しても，送信者の正当性を確認することができるため，組織内メンバや協業メンバになりすました組織外からの攻撃に対して，耐性を持つと考えられる．

本仕組みによれば，対策ツールが未導入の端末からの攻撃には，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，攻撃者がメールヘッダを偽装・改変した場合，

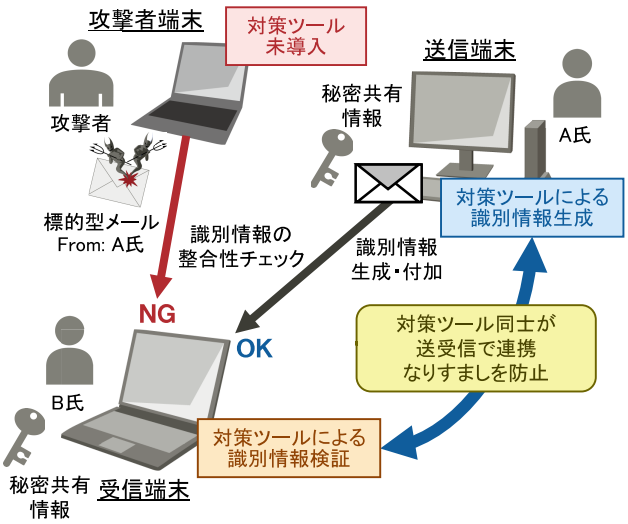


図 1 送受信での連携による検知の高精度化技術

Fig. 1 Accurate detection of spoofed e-mail by cooperating outbound and inbound software mechanism.

および攻撃者が何らかの手段で入手した過去の識別情報付きメールに記載された識別情報をそのまま引用したとしても，受信端末で識別情報の整合性を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．

4.2.2 識別情報の生成方式

本項では，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．本方式では，秘密共有情報を攻撃者に知られずに受信端末と安全に共有する仕組みが必要となる．この共有方法として，たとえば，組織内の情報セキュリティ部門の管理者が，本対策ツールのインストーラを用意して配布することを想定する．秘密共有情報そのもの，もしくは秘密共有情報の基となる情報をインストーラに埋め込み，組織内メンバに一斉配布し，共有する方法が考えられる．また，秘密共有情報は，送信端末で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 MAC 対象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．送信メールの解析を行い，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，MAC 対象項目の取得を行う．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 [10] 等が利用可能である．

MAC 対象項目とは，送信メール内の複数のヘッダ項目や本文，添付ファイル等を対象とし，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．たとえば，From，To，Subject，Date 等のヘッダや，本文の全文，もしくは一部，添付ファイル等を MAC 対象項目とする．MAC 対象項目は，運用環境のセキュリティ強度に応じ，管理者があらかじめ複数のパターンを用意し，たとえば，インストーラに埋め込んで配布する．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制御する．これにより，秘密共有情報とメール本文の特定の情報から単純計算した場合に比べ，識別情報の生成対象が定まらず，識別情報の捏造を抑止・防止できる．

送信メール *SM* の解析を行い，*SM* から MAC 対象項目の情報を参照し，秘密共有情報を含めて識別情報を生成する（**図 2**）．図 2 では，MAC 対象項目として，p1: From，To，Date，Body（本文），File（添付ファイル）を用いて，識別情報を生成している．

MAC 対象項目と生成した識別情報は，識別情報ヘッダとして，*SM* の新たなヘッダとして追加し，識別情報付き送信メール *SM'* とする．MAC 対象項目の情報は，*X-InboundTargetData* に追加し，識別情報は，*X-InboundMAC* に追加する．その他のヘッダ，添付ファイルを含む本文はいっさい加工しない．*SM'* を送信対象とする．

4.2.3 識別情報の検証方式

本項では，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，MAC 対象項目を送信端末と共有する必要がある．受信端末では，メールを開く前に，識別情報の検証処理を行う（**図 3**）．

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

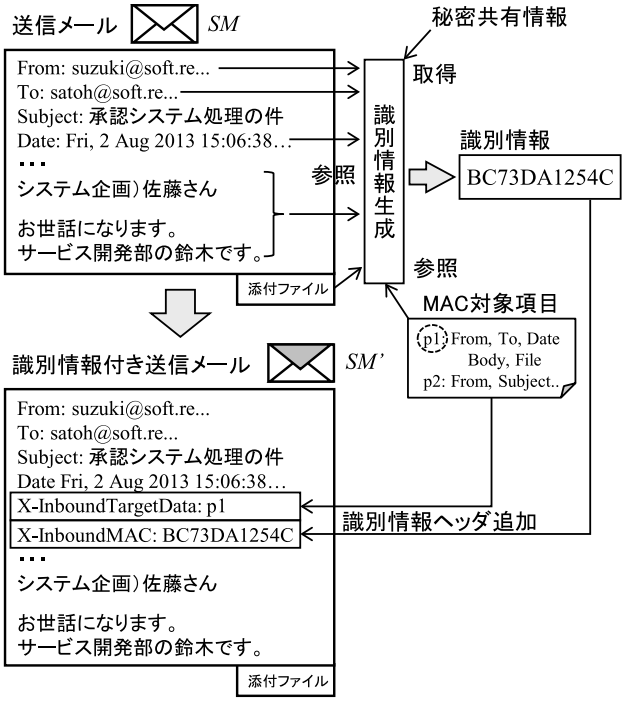


図 2 識別情報の生成処理の概要

Fig. 2 Generation process of e-mail identification information.

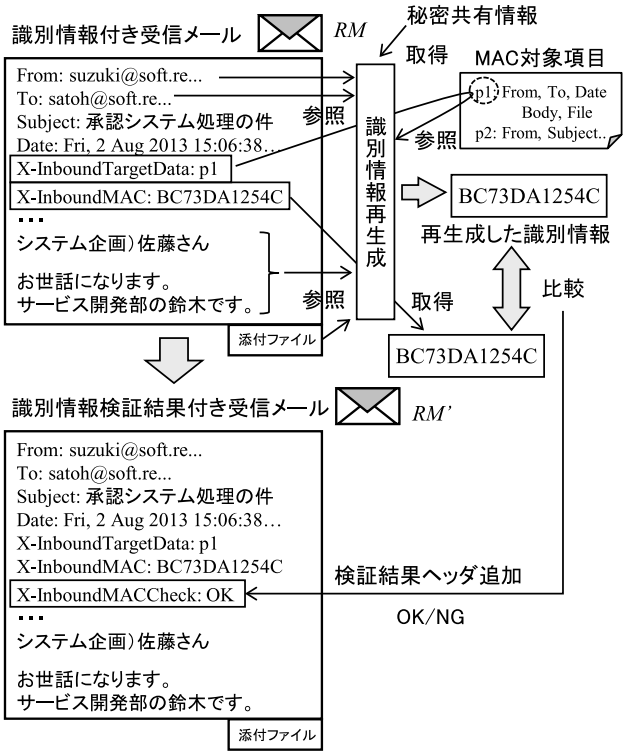


図 3 識別情報の検証処理の概要

Fig. 3 Verification process of e-mail identification information.

ム，MAC 対象項目の取得を行う．MAC 対象項目は，*RM* のヘッダ内の *X-InboundTargetData* から取得する．識別情報ヘッダを除く *RM* から，秘密共有情報を含めて，MAC 対象項目に対する識別情報を再生成する．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である．図 3 では，*X-InboundTargetData* から p1 を取得し，From，To，Date，Body（本文），File（添付ファイル）を用いて，識別情報を再生成している．

RM のヘッダ内の *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．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．識別情報が一致する場合は，*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．

4.3 受信履歴を基にした送信者ごとの特徴分析技術

組織外とのメールのやりとりやメールマガジン等，送受信で共通の対策ツールを導入できない場合には，4.2 節の手法は使えない．そこで，本節では，受信履歴を基に送信者ごとの特徴を分析し，第三者になりすました標的型メール攻撃を検知する技術を提案する（**図 4**）．

具体的には，受信端末ごとに，これまでの受信履歴から，送信者アドレスごとにその特徴をデータベースに蓄積し，受信メールの情報とデータベースの情報との類似性を確認することで，正規送信者になりすました標的型メール攻撃か否かを判定する．たとえば，送信経路の変化等，ふだんと特徴が異なるケースを識別することで，正規送信者になりすました怪しいメールか否かを検知する．

表 2 は，送信者特徴として判定に利用する情報の一部である．メールヘッダから取得可能な情報（たとえば，経路，使用メーラ，タイムゾーン等）やメール属性情報（たとえば，送信時間帯等）を対象とする．重みは，送信者ごとの値の変化度合に応じて，過去の受信履歴から算出する．これら類似判定項目と重み情報を組み合わせて，送信者の特徴をとらえ，なりすましをチェックする（**図 5**）．

受信メール *RM* の解析を行い，送信者アドレスをキーにして，データベース内の送信者別類似判定項目と重み情報を検索・取得する．受信メールと受信履歴を照合し，時間帯，タイムゾーン，ドメインの異なり等から，標的型メール攻撃の可能性があるか否かを判定する．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

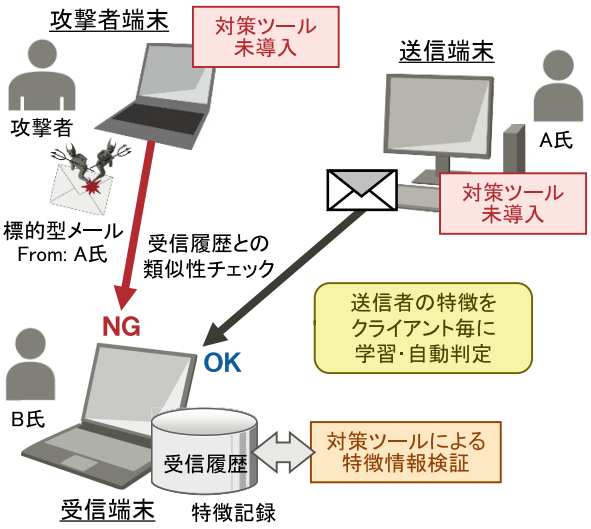


図 4 受信履歴を基にした送信者ごとの特徴分析技術

Fig. 4 Analyzing sender feature information from received e-mail log.

表 2 特徴情報対象

Table 2 Sources of sender feature information.

対象情報	項目名	チェック内容
経路ドメイン	Received	Fromドメインが含まれていない
		蓄積情報とIPが類似していない
タイムゾーン	Date	jpドメインだが+0900でない
		蓄積情報と異なる時間帯から送信
メーラ	X-Mailer	蓄積情報と異なる
メッセージID	Message-ID	Fromドメインと異なる
Returnドメイン	Return-Path	Fromドメインと異なる
・・・	・・・	・・・

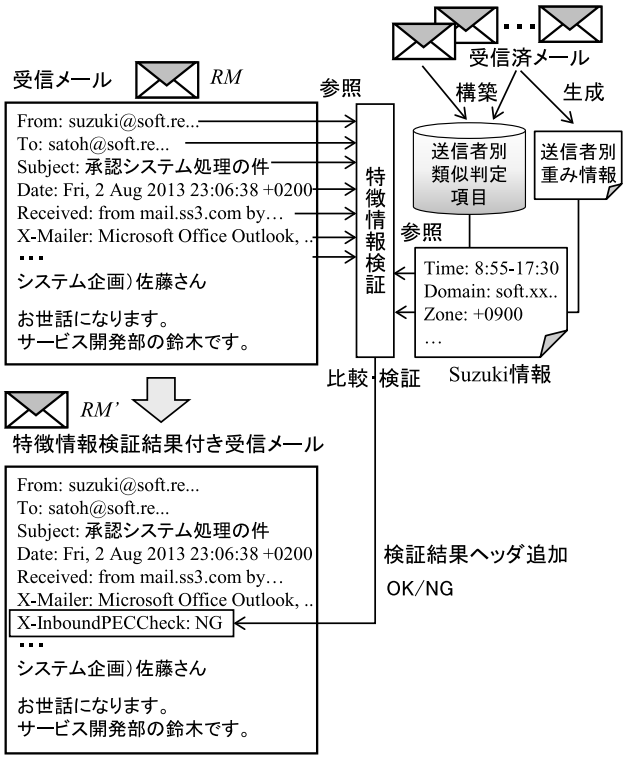


図 5 特徴情報検証処理の概要

Fig. 5 Verification process of sender feature information.

型メール攻撃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．この検証結果ヘッダの内容に基づき，利用者になりすましメールの警告を行う．

Received ヘッダによる経路情報からなりすましメールを判定する方式は一般的に知られている．しかしながら，単純に IP アドレスを経路として蓄積するだけでは，大手のニュース配信サービスやメールマガジン等の複数の送信元 IP アドレスで分散して配信しているメールには，毎回警告が出てしまうことになる．また，外部を含めたメーリングリストでは，メンバ登録が頻繁に発生することで同一メーリングリストが毎回検出対象になったりする等，送信者と経路の IP アドレスの単純な判別では過剰な警告を防ぐことができない．そのため，送信経路の IP アドレスは，完全一致ではなく一定範囲内かの柔軟なチェックを行う．また，経路に含まれるドメインが，From やメッセージ ID，Return-Path，本文中に含まれる URL 等に含まれるドメインと，どの程度一致するかのチェックも行う．これら複数の特徴情報を判定項目とすることで，過剰警告を減らす．

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，標的型メール攻撃の判定方法について述べる．**図 6** に，提案方式による判定処理の流れを示す．

受信メールの解析を行い，識別情報ヘッダ（*X-InboundTargetData*，*X-InboundMAC*）が存在するか否かの確認を行う．識別情報ヘッダが存在する場合は，4.2.3 項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警告・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．標的型メール攻撃の可能性があれば，識別情報検証処理同様，受信メールに対する警告・安全化処理を行う．

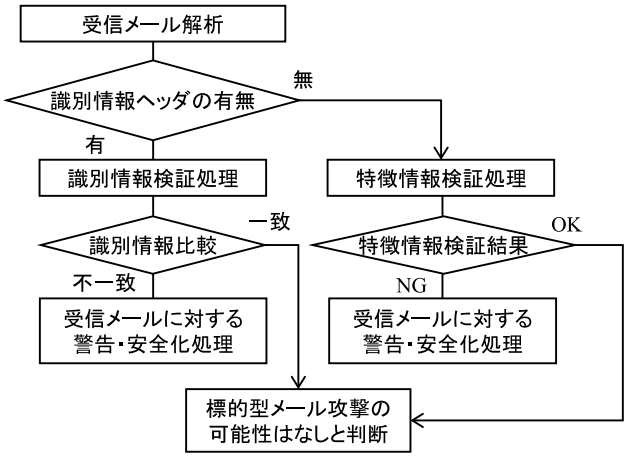


図 6 識別情報と特徴情報による判定処理の流れ

Fig. 6 Detection process of spoofed e-mail with identification information and sender feature information.

なお，高速化のために，添付ファイルや URL リンク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，クライアントベースで標的型メール攻撃の可能性を判定・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，あらかじ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，MAC 対象項目を用いて，秘密共有情報を含む識別情報を生成し，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，メール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，標的型メール攻撃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，受信履歴を基にした送信者ごとの特徴分析技術を採用することで，受信履歴から送信者の特徴を重み情報とともに判定し，類似性を確認することで，標的型メール攻撃の可能性の有無をより確実に判断することができる．本方式により，標的型メール攻撃による感染を軽減させることが可能になる．

5. 試験実装

プロトタイプ実装で，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

送受信メールの解析・制御による標的型メール攻撃の判定，および受信者への警告・安全化処理を行うプロトタイプシステムを開発した（**図 7**）．

メールチェックツールとして，送信メールに対して，識別情報の生成を行う Outbound 処理機能と，受信メールに対して，識別情報の検証，および特徴情報の検証を行う Inbound 処理機能を開発した．SMTP，および Microsoft Exchange に対応することで，既存の多くのメーラ（MUA）には依存しない構成となっている．MUA として，Microsoft Outlook（以降，Outlook）を使用する場合には，Outlook アドインによるメールチェックツールとの連携機能も開発した．以下，主として Outlook を対象にしたツール実装について述べる．

5.2 識別情報生成機能

送信メールに対する解析処理，ならびに識別情報を生成する機能をメールチェックツール上に実装した．秘密共有情報，生成アルゴリズム，MAC 対象項目を，受信端末と共有し，同一の情報，アルゴリズムを利用できる．MAC

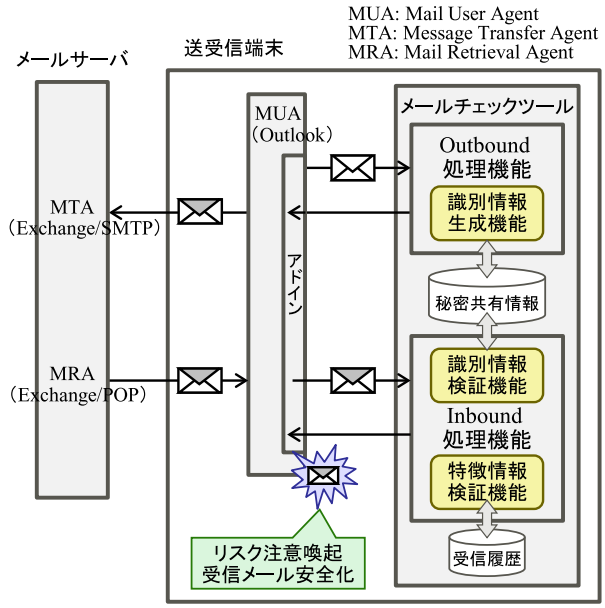


図 7 プロトタイプシステムの構成
Fig. 7 Outline of prototypic system.

対象項目として，メールヘッダの一部と本文，添付ファイルを選択可能とした．識別情報の生成アルゴリズムは，HMAC-SHA256 を使用し，秘密共有情報を鍵情報として，MAC 対象項目と組み合わせてハッシュ値を算出し，このハッシュ値を識別情報とした．

5.3 識別情報検証機能

受信メールに対する解析処理，ならびに識別情報を検証する機能をメールチェックツール上に実装した．秘密共有情報，生成アルゴリズム，MAC 対象項目を，送信端末と共有し，同一の情報，アルゴリズムを利用した．

5.4 特徴情報検証機能

識別情報ヘッダが付加されていない受信メールの場合，送信者アドレスごとに受信履歴から特徴情報を算出し，類似性確認を行う機能をメールチェックツール上に実装した．受信履歴のある送信者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．

5.5 受信者への警告・安全化機能

受信メールに対する受信者への警告・安全化機能として，標的型メール攻撃の可能性がある旨を受信者に対して，警告画面で表示する機能を実装した．また，攻撃の可能性のあるメールは，誤って添付ファイルを開封したりしないよう，迷惑メールフォルダに強制的に移動（隔離）する．さらに，標的型メールか否かの判定結果を受信者が視覚的に確認できるよう，Outlook のメール分類項目機能を用いて，判定結果や受信者による操作結果を表示した．

6. 試験実装の評価と課題

実際に正常メールからヘッダを偽装したメールを作成し，プロトタイプシステムで本提案方式の検証を行った．また，組織内利用者での試行により，試験実装の評価と課題抽出を行った．

6.1 試験実装の単体評価

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正規メール，(B)，(C) は，(A) を基にメールヘッダを偽装したメールで，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．(A)〜(C) は，同一の送信者（From）からのメールであり，その送信者アドレスからの正規メールをあらかじめ受信履歴として保存し，メール特徴情報を作成したうえで評価した．

(A) 5.2 節の方法で，識別情報ヘッダを追加した，添付ファイル付き送信メール
(B) (A) とは別の正規の識別情報付きメールから，ヘッダのみコピーして作成した，添付ファイル付き偽装メール
(C) 受信履歴のヘッダの特徴情報とは異なる特徴情報になるようヘッダを変更した，添付ファイル付き偽装メール

(A) は，Outlook でメールを作成し，メールチェックツールを介して送信する．(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 コマンドを用いて送信する．

メール受信処理は，メールチェックツールを介して判定処理を行う．判定結果は，以下のとおりである．

(A) は，識別情報の検証が正常となり，警告画面は表示されずに，そのままメールが読める状態となった．

(B) は，正規メールのヘッダを単純コピーしたため，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，標的型攻撃の可能性がある旨の警告を示す分類項目が追加された（**図 8**）．

(C) は，あらかじ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，警告を示す分類項目が追加された．

警告を示す分類項目のついた (B)，(C) は，メールを開くと同時に警告画面が表示された（**図 9**）．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，“安全なメールとして学習” ボタンが有効になる．本ボタンを押下することで，警告を示す分類項目から，そのまま受信したメールであることを示す分類項目に変更し（**図 10**），本メールの特徴情報を受信履歴として記録する．警告画面で，“迷惑メールフォルダへ隔離” ボタンを押下することで，本メールを迷惑メールフォルダへ強制移動する．このとき，標的型攻撃の可能性がある旨の警告を示す分類項目から，隔離

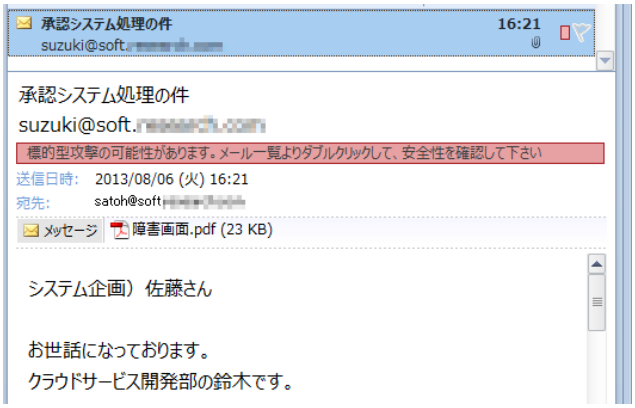


図 8 標的型メールの判定確認画面
Fig. 8 Alert message of detecting suspicious targeted e-mail.

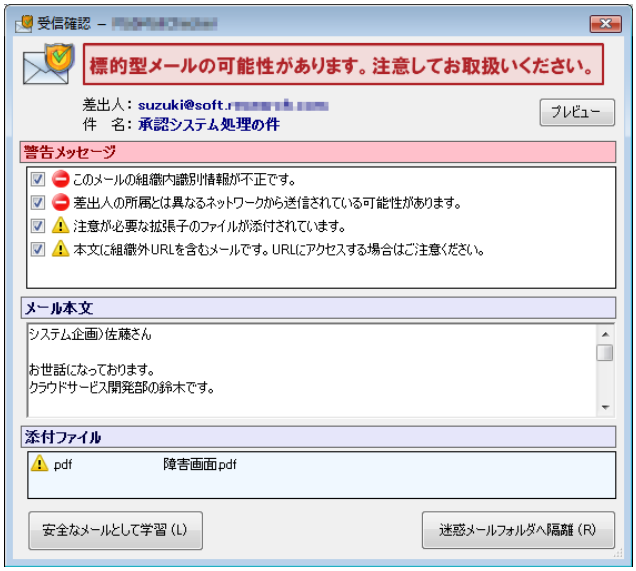


図 9 識別情報不正による標的型メール攻撃の警告画面
Fig. 9 Alert window for detecting wrong e-mail identification information.

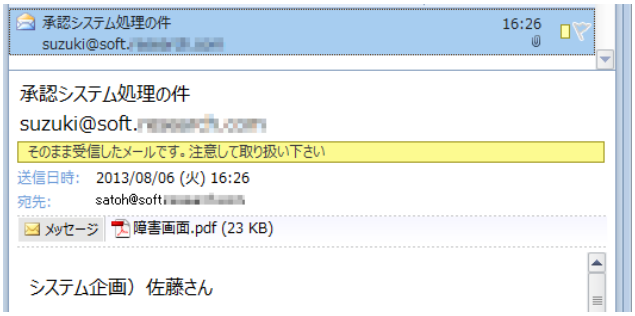


図 10 そのまま受信メールの確認画面
Fig. 10 Warning message for checked e-mail.

したメールであることを示す分類項目に変更する（**図 11**）．

なお，今回の実装・評価は，Outlook を使用して行ったが，対策ツールは MUA とは切り離して実装しているため，Mozilla Thunderbird や Becky! Internet Mail 等の主要なメーラへも容易に導入可能である．

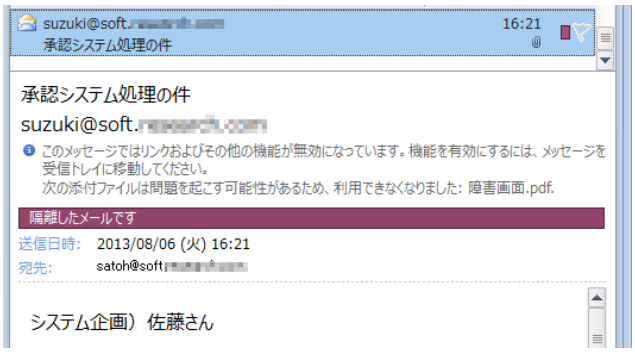


図 11 隔離メールの確認画面
Fig. 11 Warning message for isolated e-mail.

6.2 試験実装の試行評価と課題

今回試作したメールチェックツールを組織内利用者 20 名に配布して，日常的に利用してもらい，実際の業務メールを用いて，試験実装の試行評価を行った．

6.2.1 試行による試験実装の機能評価

組織内利用者に対して，人為的に以下のような評価メールを送付し，識別情報検証機能，ならびに特徴情報検証機能の動作評価を行った．

(1) 6.1 節の (B) 攻撃メールを組織外から送信
(2) 6.1 節の (C) 攻撃メールを組織外から送信
(3) S/MIME 署名の付いたメールを組織内から送信

結果，(1) は，識別情報の検証異常，(2) は，特徴情報の検証異常となり，警告画面が表示された．(3) は，S/MIME 署名検証，識別情報検証ともに正常となり，警告画面は表示されないことを確認した．これにより，組織内の正規利用者や S/MIME 署名の付いたメールでは，警告画面は表示されず，組織内利用者を騙った組織外からの攻撃メールでは，警告画面が表示されることを確認できた．

6.2.2 標的型メール訓練での開封率の低減効果検証

標的型メール訓練を以下の条件で実施し，開封率の効果を測定した．当社内にある部全員（男性 45 名，女性 8 名の計 53 名）を対象者とし，前述のメールチェックツールの導入者 20 名，および非導入者 33 名で，社外から，社内管理部門の送信者（From）を騙って，対象者全員に対して，同じ文面の添付ファイル付き疑似攻撃メールを 1 通送付した．なお，事前に訓練を行う旨と実施する週を周知した．また，導入者にはあらかじめ訓練を実施する週の 2 週間前にメールチェックツールを配布し，警告画面の出方，警告画面が出た際の対処方法について通知した．測定方法は，訓練メールの添付ファイル（Microsoft Word）を開くと，ビーコンが送信される仕組みにより，開封率を測定した．

本メール訓練の結果，メールチェックツールの非導入者におけるメール開封者は 11 名，導入者におけるメール開封者は 1 名となった（**表 3**）．フィッシャーの直接確率計算法による統計的検定を実施したところ，5%水準で有意であった（$P \fallingdotseq 0.016$）．よって，標的型メール訓練において

表 3 疑似攻撃メール開封結果
Table 3 Results on simulated e-mail attack.

	開封者	非開封者
導入者	1名	19名
非導入者	11名	22名

も，本ツールの効果があることが分かった．

6.2.3 試行評価による課題抽出

試験実装の試行評価を通じて，本ツールでの効果の確認とともに，いくつかの課題も明らかとなった．1つは，過剰警告である．受信履歴のない初回受信のメールには必ず警告が出てしまう．これに対しては個人だけではなく，組織として受信履歴を共有する等の対策も必要と考えられる．また，効果が出るまでの時間も課題である．

本ツールを長期利用することで，多くのパターンが学習され，過剰指摘が軽減されることも期待できる．実際，別に実施した数百名規模での標的型メール訓練では，本ツールの長期利用者の方が，短期利用者よりも開封率は低いという結果を得ている．学習により，過剰指摘が減り，利用者も良い意味で慣れてきたためと考えられる．

さらに，ユーザインタフェース上の課題である．標的型メール訓練においては，本ツールが警告画面を出しても，添付ファイルを開封してしまうケースがあった．セキュリティにも詳しくない利用者に対して，攻撃メールのリスクを端的に伝えるユーザインタフェースの改良が必要である．たとえば，「メールの送信経路が異なります」という技術的な警告メッセージよりも「普段と違う組織からメールが送られています」の方が一般利用者により分かりやすい．

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，受信履歴を基にした送信者ごとの特徴分析技術を利用し，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，サーバ等での対策をとらなくても，クライアントにメールチェックツールを導入するだけで，標的型メール攻撃の可能性を判定・検知することが可能になる．さらに，標的型メール攻撃の可能性をリアルタイムに検出し，メールを開く前に受信者への警告・安全化処理を行うプロトタイプシステムを開発し，提案方式の試行評価を行った．提案方式で標的型メール攻撃の可能性を検知できることを実証し，本ツール利用による開封率の軽減効果も示した．

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，標的型メール攻撃による感染を軽減させることが可能になる．

また，メールチェックツールを組織内で共通に利用することで，メールセキュリティ統制の徹底や，関連会社や委託先も含めて利用することで，社内外のメンバ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．

参考文献

[1] 独立行政法人情報処理推進機構：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，入手先 ⟨http://www.ipa.go.jp/about/technicalwatch/20111003.html⟩.

[2] 警察庁警備企画課・情報技術解析課：平成 25 年上半期のサイバー攻撃情勢について，入手先 ⟨http://www.npa.go.jp/keibi/biki3/250822kouhou.pdf⟩.

[3] Sahami, M., Dumais, S., Heckerman, D., et al.: A Bayesian Approach to Filtering Junk E-mail, AAAI Workshop on Learning for Text Categorization, AAAI Technical Report WS-98-05 (1998).

[4] 梅田昴翔，上原雄貴，水谷正慶ほか：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，コンピュータセキュリティシンポジウム（CSS2010）論文集，pp.109–114 (2010).

[5] IETF: Secure/Multipurpose Internet Mail Extensions (S/MIME), RFC3851, (2004), available from ⟨http://www.ietf.org/rfc/rfc3851.txt⟩.

[6] 総務省情報通信国際戦略局通信規格課：標的型攻撃に対抗するための通信規格の標準化動向に関する調査結果，入手先 ⟨http://www.soumu.go.jp/main_content/000227896.pdf⟩.

[7] 春名光一：ID-Based 暗号を用いたメール送信元サーバ認証に関する研究，筑波大学大学院博士課程システム情報工学研究科修士論文 (2006).

[8] Sender Policy Framework Project Overview, available from ⟨http://www.openspf.org/⟩.

[9] IETF: DomainKeys Identified Mail（DKIM）Signatures, RFC4871, (2007), available from ⟨http://www.ietf.org/rfc/rfc4871.txt⟩.

[10] Bellare, M., Canetti, R. and Krawczyk, H.: Keying Hash Functions for Message Authentication, *CRYPTO '96*, pp.1–15 (1996).

推薦文

本論文は，昨今被害が深刻となっている標的型メールを検知するための現実的な手法を提案している．提案手法を実システムとして実装，運用してその効果を評価している．今後の同研究分野の発展に有用であるため，推薦論文として推薦したい．

（コンピュータセキュリティ研究会主査　西垣正勝）

吉岡 孝司

1992 年富士通株式会社入社．株式会社富士通研究所で，電子データの原本性保証（電子署名応用），サイバー攻撃対策に関する研究に従事．1998 年東京工業大学像情報工学研究施設研究員．現在，富士通株式会社セキュリティイニシアティブセンターに所属し，サイバー攻撃対策を中心としたセキュリティビジネスの企画，推進に従事．

片山 佳則 （正会員）

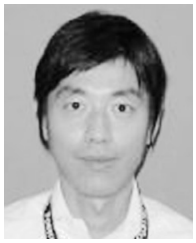
1985 年東京理科大学大学院理工学研究科経営工学専攻修士課程修了．同年富士通株式会社国際情報社会科学研究所入社．1990 年株式会社富士通研究所に編入，現在に至る．知識表現，ソフトウェア工学の研究を経て，現在，ソーシャルイノベーション研究所に所属し，サイバー攻撃対策や情報セントリックセキュリティに関する研究に従事．

津田 宏 （正会員）

1987 年東京大学理学部情報科学科卒業．1989 年東京大学大学院理学系研究科修士課程修了．同年株式会社富士通研究所入社．現在，ソーシャルイノベーション研究所主席研究員．1989〜95 新世代コンピュータ技術開発機構（ICOT）出向．Web マイニング，セマンティック Web，情報漏洩対策，プライバシ保護技術等の研究に従事．人工知能学会会員．博士（理学）．

森永 正信 （正会員）

1993 年九州大学大学院工学研究科電子工学専攻修士課程修了．同年株式会社富士通研究所入社．IP ネットワークにおける VoIP を主としたシステム・サービスの研究を経て，現在，ソーシャルイノベーション研究所に所属し，ICT システムにおけるセキュリティ技術に関する研究に従事．



深澤 亮太

1999 年株式会社富士通ソーシアルサイエンスラボラトリ入社．SI 分野において Web/DB 系業務アプリ開発，大規模決済システム開発に従事．2008 年より株式会社富士通研究所をはじめとした研究機関との連携によるセキュリティ，メディア処理，テキスト処理，組織マネジメント，ソーシャル分析，OSS 信頼性評価に関する研究開発，およびソリューションビジネスに従事．現在，SI ビジネス本部に所属し，SI ビジネスおよび新製品企画，開発，拡販推進に従事．