組織内情報共有を支援する標的型メール攻撃対策システムの検討

半井 明大[†1]　澤谷 雪子[†1]　山田 明[†1]　村上 洸介[†1]　窪田 歩[†1]

概要：標的型メール攻撃では，新種のマルウェアや特定組織向けのメール本文，URL，添付ファイルを攻撃者が用いることが多いため，既存のメールフィルタや AV ソフトの検知では防ぎきれない事例がある．そのような場合，受信するメールの良性悪性に関する最終的な判断は利用者が行うことになるため，ヒト対策が重要となる．しかし，従来の標的型メール攻撃訓練や注意喚起といったヒト対策では，不審メールに気づけない組織構成員をゼロにすることは難しく，また訓練や注意喚起で示された確認作業等が組織構成員の負担となり確認漏れや確認怠りを助長していまいかねないといった問題点が存在する．

本稿では，組織内で不審メールに気づいた構成員の報告を組織内に配信し気づかなかった構成員の気づきを促す報告共有機能と，ホワイトリストにより本来確認すべき受信メールを絞ることを補助する標的型メール攻撃特徴検出機能を提供するシステムを提案する．また，組織構成員の不審メールへの気づき向上等の標的型メール攻撃の被害軽減効果に対する提案システムの貢献について論じる．

キーワード：標的型攻撃，標的型メール攻撃，セキュリティ教育

A Study on Information Sharing Support System for Mitigating Risk of Spear Mail Phishing Attack

Akihiro Nakarai[†1]　Yukiko Sawaya[†1]　Akira Yamada[†1]　Kosuke Murakami[†1]
Ayumu Kubota[†1]

Abstract: Attackers tend to use new computer viruses, texts, URL, attached files customized for a specific organization in their spear mail phishing. Thus, existing mail filters and antivirus software cannot completely prevent the suspicious messages. In this case, organization members who receive the suspicious messages must evaluate if they are benign or malignant by themselves, and as a result, “human-side measures” such as practical training or heads-up for internal members are important factors for countering spear mail phishing. However, existing human-side measures cannot totally remove the members who cannot find the suspicious messages. In addition, checking every incoming messages is very burdensome task for the members in their daily tasks and it may cause their oversight in checking by mistake or laziness.

In this paper, we propose a countermeasure system that provides suspicious mail reporting and result sharing function to share other members’ awareness with members who do not notice the suspicious messages by themselves and the characteristics detection function with whitelist for the specific organization. We also discuss the contributions for mitigating the risk of spear mail phishing in the viewpoint related to awareness of suspicious messages.

Keywords: Targeted attack, Spear mail phishing, Security training

1. はじめに

近年，特定の組織を狙った標的型攻撃が国内外問わず猛威を振るうようになった．標的型攻撃の中でも標的型メール攻撃は，広く業務で電子メールが利用される昨今被害リスクが高まっており，実際に国内でも複数の会社・官公庁・地方自治体での被害又は被害未遂の事例が見られるようになった．

標的型メール攻撃の特徴として，新種のマルウェアが用いられたり，特定組織の攻撃に特化したメール本文・URL・添付ファイルが用いられたりすることから，既存のシグネチャベースのファイヤーウォール，IDS，メールフィルタ等によるサーバ対策やウイルス対策ソフト等によるエンドポイント対策のみではその検知や被害軽減が難しい．

上述の理由から，現状標的型メール攻撃の対策においては，サーバサイド対策やエンドポイント対策をすり抜ける場合を想定し，攻撃メールに直面する受信者における「ヒト対策」が肝要であるといえる．

従来の「ヒト対策」においては，サーバサイド対策やエンドポイント対策で見逃された場合でも，組織構成員が自身で不審メールに気づけるようになることを目的とし，標的型攻撃の特徴を模擬演習・訓練等を通して教育する手法や，口頭・メールにより不審メールへの対処方法などを注意喚起することで組織構成員のセキュリティ意識向上を目指すような手法が取られる．

しかし，このような従来のヒト対策のアプローチにはいくつかの問題点が存在する．第一に，訓練や注意喚起によって自分で受信メールの正当性を判断できる人が増えても

†1 株式会社 KDDI 研究所
KDDI R&D Laboratories, Inc.

その効果にばらつきがあり，不審メールに気づかず標的型メール攻撃の被害を受けてしまう組織内人員をゼロにはできないという点がある．実際，昨今の標的型メール攻撃の事例においては，複数回にわたって別々のタイミングで標的型メール攻撃を受けた組織において，都度組織内全体に管理者が注意喚起を実施したのにもかかわらず，組織構成員は標的型メール攻撃に気づけず，メール内の URL へアクセス，または添付ファイルを開封してしまい，マルウェア感染に至ってしまった事例も存在する．第二に，訓練や注意喚起等で周知された確認手順を徹底するのが煩雑で日常業務の中で組織構成員の大きな負担となりうる点である．こうした不審メールの確認が負担となると，誤って不審点を見落としてしまったり確認を怠ってしまったりする組織構成員が現れることが予想され，組織としての被害リスクが高まる可能性がある．第三に，組織構成員に対する注意喚起や教育が画一的であり，個々人の標的型メール攻撃のリスクを軽減する内容が検討できない点である．例えば，単純な注意喚起を出すケースを考えたときに,「簡潔な警告か細かく事例ベースの説明をすべきか」,「誰からの注意喚起なのか」,「情報源はどこか」,「UI や図解はどうか」等検討の要素があり，これらの効果的な組み合わせは各人によって異なるが各人の実態を把握する枠組みは十分に整備されていないといえる．

本稿では，上述の問題点の解決を目指すべく組織内情報共有を支援する標的型メール攻撃対策システムを提案する．

提案システムでは，組織構成員が不審メールに気づいた際に管理者や組織構成員全体に報告を実施できる機能を設けることで，不審メールに気づかない組織構成員がいたとしてもシステムによって共有される「不審メールへの気づき」によって不審メールへの気づきを促すことできる．

また，組織特有のホワイトリストとのマッチング結果やメール内の URL・添付ファイル・メールヘッダの正当性判断に係る情報について，メール内の URL や添付ファイルに対する操作時に提示することで，人手で確認する負荷が低減でき，結果的に確認に注力すべき対象メールが絞られるため，訓練や注意喚起が十分に活かせることが期待できる．

加えて，本システムでは先に述べた組織内からの報告や確認すべき事項として提示した情報について，提示後の組織構成員の URL アクセス/添付ファイル開封や報告に関する振る舞いをロギングすることで，管理者がアドオンで提示された情報や警告がどれだけ組織構成員に対して効果があったかを知ることができ，将来の警告やダイアログのメッセージについて効果的な内容を検討する材料に活用できる．

提案システムは組織構成員の端末上で動作するクライアントソフトウェアであるメーラーアドオンと，当該メーラーアドオンと連携するメール情報管理サーバとから構成される．図 1 に提案システムの効果のイメージを示す．

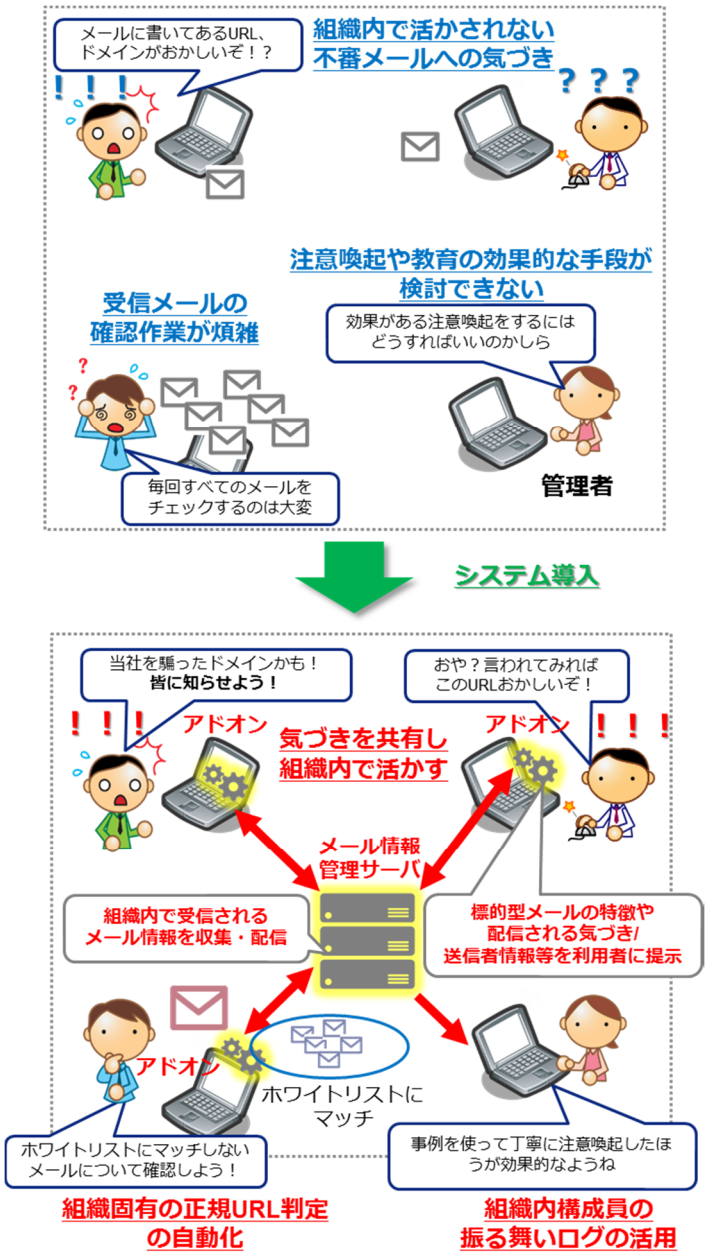

図 1　標的型メール攻撃対策の課題と提案手法の効果

本稿の構成は以下のとおりである．第 2 章では，標的型メール攻撃対策に関連する既存技術についてその課題を整理する．第 3 章では，本章ならびに第 2 章で述べた課題を解決することを目的とした「組織内情報共有を支援する標的型メール攻対策システム」について，詳細に述べる．第 4 章では，本提案に基づくプロタイプ実装について述べる．第 5 章では，組織構成員の不審メールへの気づき向上等の標的型メール攻撃被害軽減への貢献を論じる．第 6 章では，第 5 章の内容を踏まえ本稿の総括並びに今後の展望について述べる．

2. 既存の関連技術

本章では，標的型メール攻撃対策に係る既存の関連技術並びにその課題について論じる．

2.1 既存の技術・関連研究

標的型メール攻撃においては，第 1 章でも述べたように，新種のマルウェアや攻撃対象の組織用のマルウェアが用いられるケースもあることから，従来のシグネチャベースの検知では対応が難しいケースがある．従来の画一的なシグネチャベースではなく，ヒューリスティック検知により未知のマルウェアの検知を目指した FFRI Mr.F[1]や組織固有のマルウェアについても検知可能なサンドボックス製品である Wild Fire[2]等がある．

山田ら[3]は組織内ネットワークにおける内部攻撃の方法としての RAT，および Pass-the-hash 攻撃に関連するツールを調査，分析し，その結果から攻撃ツールによって発生する通信は通常業務に偽装され，攻撃との判別が難しい一方で，内部攻撃は RAT の機能と SMB 管理ツールの連携によって行われることを明らかにした．また，分析結果に基づいて,攻撃者ホスト，踏み台ホスト，標的ホストの間の一連の通信が順に連動して発生する通信シーケンスを検出することにより，内部攻撃を検知する方式を設計し評価を行い，標的型攻撃に関する新種や亜種の攻撃ツールであっても内部攻撃を検知できることを明らかにしている．

既述のマルウェア検知や被害検知が完全でないことから受信者へ標的型メール攻撃の特徴を提示し，ヒト対策を充実させるアプローチも近年盛んであり，既存製品として CipherCraft/Mail 標的型メール対策[4]や GUARDIANWALL [5]等が挙げられる．

吉岡ら[6]は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方式を提案している．吉岡らの提案で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．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．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ため，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．

2.2 既存の技術の問題点

標的型メール攻撃におけるマルウェアの検知や内部侵入後の検知技術は現状として完全に検知できるものはなく，これらのマルウェアの検体検知・活動検知等に加え，組織構成員が日頃から受信するメールの正当性を正しく判断するようヒト対策を実施することが肝要であると考えられる．

標的型メール攻撃の特徴を組織構成員に提示する既存製品は，組織固有のホワイトリスト・ブラックリストのカスタマイズの機能が提供されておらず，組織固有の URL・添付ファイル・メール本文等の攻撃対策には難がある．吉岡らの手法は，攻撃者の組織構成員なりすましの検知が可能ではあるが，類似性判定により普段の通信相手を装った外部犯は検知できるものの，組織外から到来する初出の特徴を有する標的型メールの検出が難しいといえる．

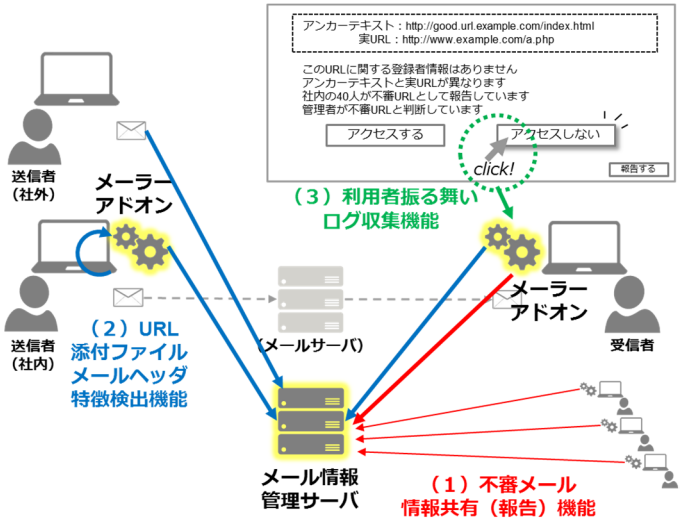

図 2　提案システムの基本構成

3. 提案手法：組織内情報共有を支援する標的型メール攻撃対策システム

3.1 設計指針

前項で述べたように，標的型メール攻撃対策においては，ヒト対策が肝要であり，標的型メール攻撃の特徴検出を提示するのが有効である一方，特定の組織を狙う未知の標的型メール攻撃に対しては，特徴検出並びに組織構成員への警告のみでは対応が遅れてしまう可能性がある．

そこで，本稿では組織構成員が受信メールに対して不審だと判断した気づきを各構成員が報告可能とすると共に報告内容が組織のセキュリティを管轄する管理者や組織全体へ自動的に情報展開される仕組みを導入することで，未知の特定組織を狙った標的型メール攻撃に対しても迅速な措置や被害拡大防止行動を取れるようすることを目指す．

また，第 1 章でも指摘したように，ヒト対策として実施

した訓練や注意喚起等で周知された確認手順の徹底が，日常業務の中で組織構成員の大きな負担となる可能性がある．特に高度な標的型メール攻撃の場合，メールの配送経路や特徴に基づく不審判定をシステムで確実に実施することは困難であり，受信メールの不審点の検知のみに焦点を当てたシステムでは組織構成員の負担軽減には結び付かないと考えられる．

提案システムでは上記背景から，社内メールや主要取引先からのメールといった組織固有の正規メールの情報をシステムで自動的に「正規メール」である旨を判定することで組織構成員の負担軽減を目指す．

さらに，情報や警告がどれだけ組織構成員に対して効果があったかを解析し，各構成員に応じた警告やダイアログのメッセージを検討する材料に活用するために，組織構成員に対して提示される情報とそれに対する組織構成員のアクションに関するログを収集する機構を設けることとする．

3.2 システム構成

提案システムの基本構成を図 2 に示す．本システムは，

(1) 不審メール・正規メール情報共有機能

(2) URL/添付ファイル/メールヘッダ特徴検出機能

(3) 利用者振る舞いログ収集機能

を有する「メーラーアドオン」と，先述のアドオンより受信したメール本文 URL や添付ファイルの情報，利用者からの報告情報，管理者が登録したブラックリスト・ホワイトリスト等を格納するデータベースを持ち，アドオンからの問い合わせに応答する機能を有する「メール情報管理サーバ」からなる．

3.3 本システムの主たる機能

3.3.1 不審メール情報共有機能

本機能は，組織構成員が受信メールについて不審な点への気づきを任意に管理者や組織全体へ報告・配信する機能である．

（1）不審メール情報報告機能

本機能の概要図を図 3 に示す．メーラーアドオンを利用する組織構成員は，メール本文内の URL へのアクセスや添付ファイルの開封操作時や受信メール本文上の右クリック操作等で対象の URL・添付ファイルへの報告を実施することができる．報告内容はアドオンからメール情報管理サーバへ送信される．

実際の報告においては，通常の報告に加え，緊急度が高く早急に管理者や組織構成員に情報共有が必要であるとメールを受信した組織構成が判断したケースの為に「緊急報告」のような枠組みを導入することが望ましいと考えられる．緊急度や重要度が付加されることで管理者が管理者フラグを立てる際の参考情報への活用や組織構成員が判断するときのヒントとなると考えられる．

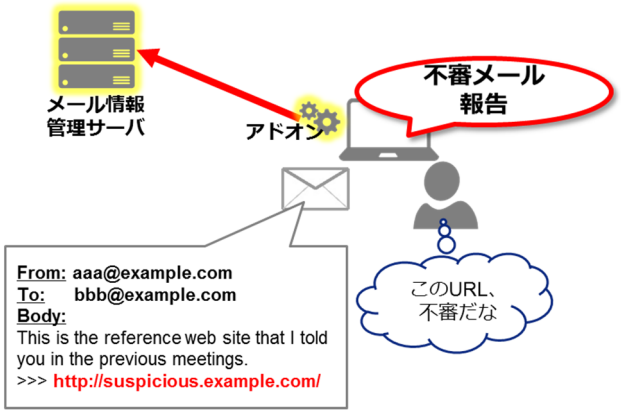

図 3　不審メール情報報告機能

（2）報告情報参照機能

本機能の概要図を図 4 に示す．上記報告機能においてアドオンから挙がった報告内容はメール情報管理サーバのデータベースにて管理する．また，収集された報告より「組織構成員からの報告数」「組織構成員からの緊急報告数」「管理者が付与したメールの正当性フラグ」を組織構成員が利用するアドオンへ配信する．配信された情報は，URL アクセス時/添付ファイル開封時のダイアログにて表示する．

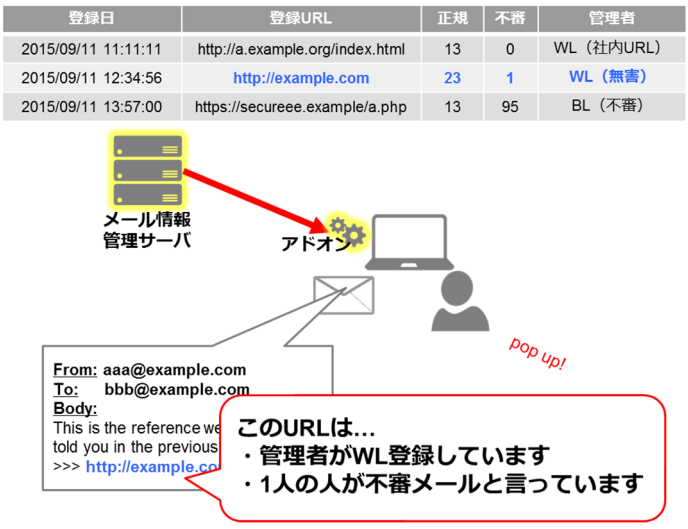

図 4　不審メール情報参照機能

3.3.2 URL/添付ファイル/メールヘッダ特徴検出機能

本機能は，受信メールに対して標的型メール攻撃の一般的または組織に特化した特徴を自動的に検出し，検出結果を受信者たる組織構成員に提示する機能である．

[検知する特徴について]

本機能で検知対象として取り上げる標的型メール攻撃の特徴として以下の様な項目がある．

（A）組織固有の URL の特徴

当該組織や関連会社，取引先等のドメインをホワイトリ

スト登録することで当該組織にとって「正規」の URL を明示する．期待される効果として，本システムを利用する組織構成員は組織固有の正規メールを確実に判断できるため，正当性判断に注力すべきメールの数を減らすことができ結果として確認作業の負荷軽減が見込めると考えられる．図 5 にホワイトリストによる確認作業の負荷軽減のイメージを示す．

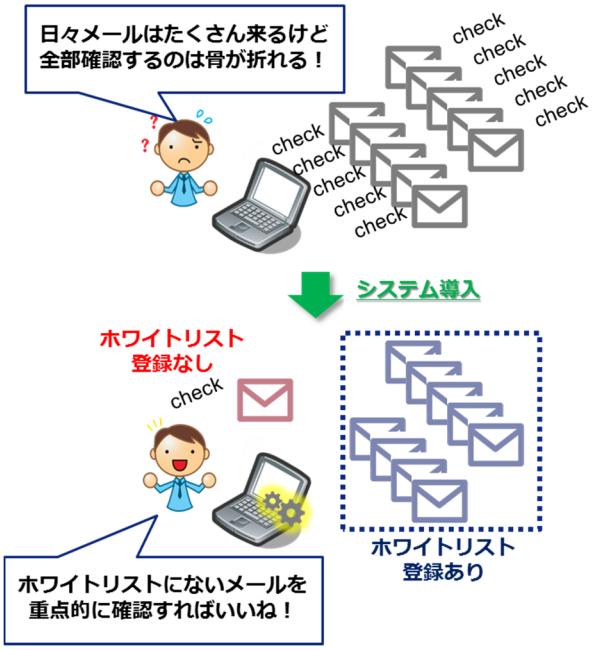

図 5　ホワイトリストによる確認作業の負荷軽減

（B）一般的な標的型メールの特徴

組織固有の特徴以外でも，一般的な標的型メールの特徴について警告表示を行う．一般的な標的型メール攻撃の特徴の例として以下の様なものが挙げられる．

例 1:アンカーテキストと URL のジャンプ先が異なる

例 2:不自然な空白や RLO をファイル名に含む添付物

（C）メールヘッダ情報の特徴

メールヘッダを解析し，メール配信時に経由したメールサーバの正当性をチェックする．例えば，メールアドレスと配送経路の組をシステムにて保持し，到来したメールに対して，過去と異なる配送経路を検知した際に警告する．

（D）URL・添付ファイルの登録者の正当性

標的型メール攻撃においては，組織構成員になりすまし，正常な社内メールを装って攻撃メールを送るケースが存在する．そこで本システムでは URL・添付ファイルの登録者について，アドオンを利用している場合にその登録者の情報を利用者に提示することで，組織構成員を騙る標的型メール攻撃かどうかの判断材料を提供する．

登録者情報の共有の流れを図 6　URL・添付ファイルの登録者情報共有に示す．

① まず，組織構成員がアドオンを利用している場合において送信メール内の URL ならびに添付ファイルと送信者の組をメール情報管理サーバへ送信する．メール情報管理サーバでは，アドオンより送られてきた URL/添付ファイルと送信者の組を DB に保持する．

② 通常通り，メールを送信する．

③ 受信者側で URL や添付ファイルにアクセスした際に該当の URL や添付ファイルが登録されているかメール情報管理サーバへ問い合わせる．

④ 問い合わせを受けたメール情報管理サーバは，自身の DB 内を URL または添付ファイルをキーに検索し，もし登録済みの場合は登録者情報を，登録がない場合は「登録者無し」の旨をアドオンに返答する．

⑤ アドオンはサーバからの情報を元に登録者情報を表示する．

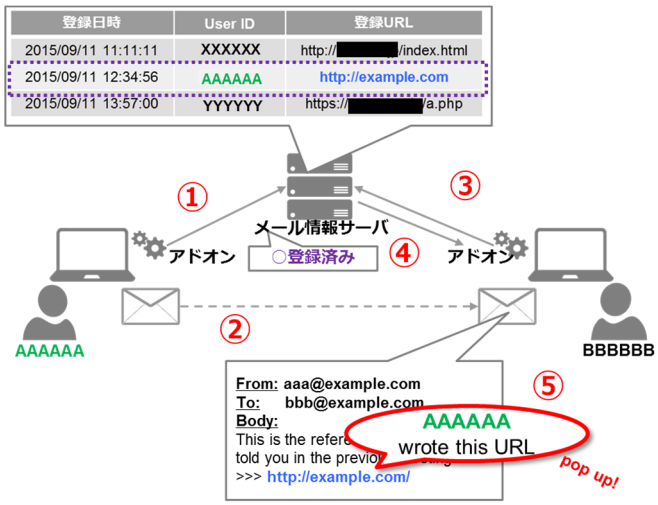

図 6　URL・添付ファイルの登録者情報共有

[利用者への警告について]

メール本文内に記載された URL へのアクセス操作や添付ファイルの開封操作の際，本システムではアドオンが既述の標的型メール攻撃の特徴に関する検出項目や後述の不審メール・正規メール情報共有機能による報告内容がダイアログで表示される．メール本文内 URL アクセス時ダイアログの例を図 7 に示す．組織構成員は，上述した検出項目や報告内容を確認した上でアクセスの実施を判断する．

3.3.3 利用者振る舞いログ収集機能

本機能は，組織構成員に対して提示される情報とそれに対してどのようなアクションを組織構成員がとったかの組み合わせを収集する機能である．本機能によって，管理者がアドオンで提示された情報や警告がどれだけ組織構成員に対して効果があったか知ることができ，将来の警告やダイアログのメッセージについて効果的な内容を検討する材料に活用できる．

提示される情報と組織構成員のアクションの例は以下

のような内容を想定する．

【提示される情報】

先述の（1）不審メール情報共有機能にて検出・共有された情報と（2）URL/添付ファイル/メールヘッダ特徴検出機能を指す．

・URL/添付ファイルの送信者情報

・URL/添付ファイル/メールヘッダのパターンマッチング

・組織内/管理者による不審判定情報

【組織構成員がとったアクション】

標的型メール攻撃に関連する情報を提示されたうえで組織構成員がとった行動について，ダイアログに対する操作イベントの取得をもってロギングする．

・対象 URL へのアクセス/添付ファイルの開封の有無

　ダイアログ上のボタンの押下イベントで取得する

・対象 URL・添付ファイルへの報告実施の有無

　報告画面での報告ボタンの押下イベントで取得する

・報告の内容

　受信メールの不審報告をしたか，また緊急報告等で報告事由が付加されていた場合はその内容を取得する

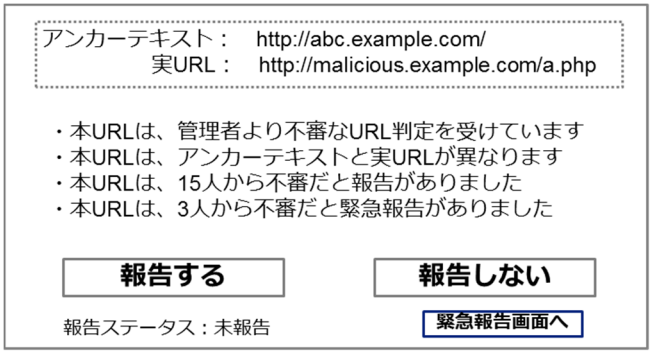

図 7　メール本文内 URL アクセス時ダイアログ

4. プロタイプシステムの実装

本章では，提案に基づくプロトタイプシステムについて，その実装内容を述べる．

プロトタイプシステムは，3.2 節でも述べたようにクライアントサイドの「メーラーアドオン」とサーバサイドの「メール情報管理サーバ」の 2 つからなる．

4.1　クライアントサイド（メーラーアドオン）

クライアントサイドの環境として Windows 7, 8, 8.1,10 または MacOS X の PC にて利用することを想定し，動作確認を行っている．また，アドオンは Mozilla Thunderbird のアドオンとして実装した．

4.2　サーバサイド（メール情報管理サーバ）

サーバサイドの環境として Ubuntu 14.04 が導入されたサーバをメール情報管理サーバとして用意した．メール内 URL・添付ファイルの登録者や不審・正規の報告情報については，PostgreSQL の DB にて管理する．また，管理者のメンテナンス画面も提供する為に HTTP サーバとして Apache を，Web UI には Bootstrap を用いた．

尚，メール情報管理サーバはクライアントサイドのアドオンからネットワーク的に到達可能である場所に設置した．

5. 考察

本章では，典型的な標的型メール攻撃シナリオを例に，提案システムを導入した場合の効果とその限界について考察する．

5.1 想定シナリオについて

本節では，想定する標的型メール攻撃のシナリオと想定シナリオにおける提案システムの効果について考察する．

5.1.1 想定するシナリオ

近年の標的型メール攻撃の特徴を参考に下記の様なシナリオを考える．想定する攻撃シナリオの全体イメージを図 8 に示す．

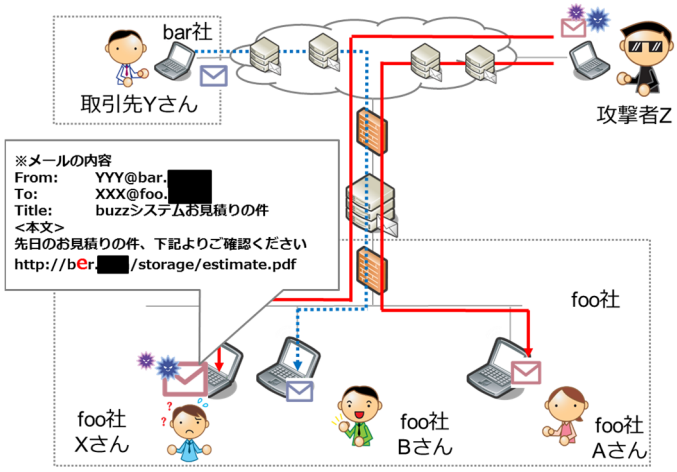

図 8　想定する攻撃シナリオ

総合商社 foo 社の社内システム担当の X さんは，社内システムの開発を bar 社に発注しており，bar 社担当者の Y さんとは開発に関して日常的にやり取りをしている．

ある日，取引先 Y さんの名前でメールが X さんを含む foo 社の数人届く．メールには foo 社が社内で利用している buzz システムの名前を含むタイトルがついており，本文内には bar 社の公開ファイルストレージを閲覧・ダウンロードを促す本文が含まれていたが，実際は Y さんからではなく攻撃者 Z が仕掛けた標的型メール攻撃であった．本標的型メールは送信元が Y さんのメールアドレスに偽装されており，メール本文内の URL へアクセスすると新種のマルウェアがダウンロードされ感染してしまう．

5.2 想定シナリオにおける懸念事項とその効果

5.2.1 一般的な攻撃の特徴確認を組織内で徹底できない

想定シナリオにおいては，foo 社で標的型メールを受信した X さんや A さんは自身で受信メールの正当性を判断することになるが，手動で正当性判断を行った場合に，セキュリティに関する知識や意識の差によって対応が分かれてしまい，組織として確実なリスク回避は困難であるといえる．

本提案システムでは，受信メール内の URL へアクセスしようとしたり，添付ファイルを開封しようとしたりしたタイミングで，操作を遮断し組織構成員に対してダイアログ表示する．このとき，URL，添付ファイル，メールヘッダについて，ブラックリストまたはホワイトリストとのマッチング結果の情報を合わせて表示するため，組織構成員の中で知識や意識に差があっても，正当性確認の徹底を促すことができる．

5.2.2 正規 URL 判断の煩雑さが増大する

図中の B さんのように Y さんから本物のメールを受信している人にとっても，常日頃から受信メールの正当性を気にかけたい場合,「正常メールであること」を確認する必要もあり，通常業務においても確認コストがかかるという副次的な懸念事項もある．

本提案システムでは，URL や添付ファイル，メールヘッダ等の情報についてホワイトリストを登録できるため，例えば図中の B さんのように Y さんから本物のメールを受信した場合に，ホワイトリストに登録されている旨がダイアログ上に表示されるため，正規メールに関する判断を確実かつ即座に実施でき煩雑さを軽減することができる．

5.2.3 各人の受信メールへの気づきが活かされない

仮に X さんが受信したメールの不審な点に気づいたとしても，A さんとコンタクトを取らない限りは不審点の気づきが共有されないため，A さん自身で気づけなかった場合の感染リスクが高まる．

管理者が早期に攻撃メールに気づければ，組織に対して注意喚起が行われる可能性があるが，早急にできることは保証できない上に，注意喚起がメールや口頭のみで行われた場合，受信メールの対する操作の際に注意喚起された内容が意識に上らず，結果的に注意喚起が活かされない危険性がある．

本システムでは，組織構成員が受信メールの URL や添付ファイルについて，不審か正規かの報告を行うことができる．加えて報告した結果はアドオンを利用しているほかの組織構成員に共有されるため，組織内で気づきが共有され，気づけなかった場合の感染リスクを提言することができる．

また，上述の報告は管理者に対しても行えるため，組織構成員をトリガーに早期警戒することも可能になる．また仮に管理者が注意喚起を早急に行えなかった場合でも，アドオンを利用している場合, 自動的に組織内の不審メール・正規メールの情報は配信されメール内の URL や添付ファイルに対する操作の流れの中で気づきが共有されるので注意喚起が活かされない可能性を低減することができる．

5.3 既存技術の課題に対する効果

前節で取り上げたシナリオは，日常的に連絡を取り合う人物を騙るタイプの標的型メール攻撃であった．しかしながら，標的型メール攻撃においては過去にやり取りがある人物を騙って攻撃してくるとは限らず，標的となった組織構成員が興味を持つような送信元や URL，添付ファイルの内容を用意し攻撃を仕掛けてくることは容易に想定できる．

その場合, 2.2 節で述べたように類似性判定による外部犯のなりすまし判定は困難であるが，我々の提案システムにおいては，組織外から来る未知の攻撃型メールに関しても疑わしい特徴の検出機能にての検知及び気づいた組織構成員の報告共有により攻撃を検知できる．

5.4 提案システムの限界と今後の課題

本節では，提案システムの限界とそれらに関する今後の課題について，考察する．

5.4.1 組織内及び通常メールをやり取りする外部端末がすでに感染していた場合について

仮に何らかのルートで組織内の端末が既に感染しており，乗っ取られていた端末から攻撃者が標的型攻撃を仕掛けた場合，経由するメールサーバや送信者情報等は正規の者となるため，組織構成員が判断する際に正しく正当性を判断できない場合がある可能性がある．

また，本稿の提案システムを構成するメール情報管理サーバが操作されてしまった場合，組織外部からの標的型メール攻撃もホワイトリストに入れることで回避されてしまう可能性がある．しかしながら組織内端末に関しては本提案システムにより感染を未然に防ぐことが期待できる．

5.4.2 報告の信頼性と重みづけについて

本稿の提案システムにおいては，システムを利用するすべての組織構成員が受信メールの URL や添付ファイルについて「不審メール」「正規メール」の報告を行う権利を有する．従って，各々の組織構成員のセキュリティに関する知識や意識付けが十分な人員も十分ではない人員も 1 票を持つことになり，場合によって不正確な組織内報告が組織内全体に配信される可能性がありその場合は組織構成員が判断を誤ることにつながると考えられる．

上記は，組織内の報告に対して適切な重みを付与した上で組織構成員に配信することで報告を基にした情報の信頼性を高めることができると考えられる．例えば，あらかじめ組織構成員のセキュリティに関する知識や意識についてアンケート調査やテストを実施し，その程度により重みづ

けを決定する方法や組織内の責任や役職を考慮して重みを調整する方法などが考えられる．

5.4.3 利用者に合わせた注意喚起について

本稿の提案システムにおいては，標的型攻撃メールの一般的/組織固有の特徴情報や組織内の報告状況をダイアログでメッセージを出力するが，表示のさせ方や文言については本来であれば各個人について効果的なものであるべきである．本システムでは効果的な注意喚起のための UI やメッセージを管理者が検討するうえで必要な利用者の振る舞いログを収集するようになっており，検討の指針や自動化等のサポート手法に関する検討は今後検討する予定である．

6. おわりに

本稿では，上述の課題に対してメール内の URL・添付ファイル・メールヘッダ等の良性悪性の根拠の提示に加え，組織構成員から実施する不審な受信メールの申告機能・並びに申告された内容の管理者・組織内への共有を以て，標的型メール攻撃のリスク軽減を狙う標的型メール攻撃対策システムを提案した．また，標的型メール攻撃の事例において，本提案がもたらすリスク軽減効果とその貢献について考察を行った．

提案システムは，組織構成員からの不審メールに係る報告をメール情報管理サーバから組織構成員のアドオンへ配信することで，自ら不審メールに気づけなかった組織構成員が不審メールの被害を受けるリスクの軽減に寄与できると期待する．また，組織固有のホワイトリストやメール内 URL/添付ファイル・メールヘッダの確認ポイントについて情報を提示することで，日々の受信メールに対する確認作業の負担を軽減し本当に判断に注力すべきメールを絞ることで，ヒト対策における教育や注意喚起の効果を十分に活かせる環境づくりにも効果があると期待する．加えて，組織構成員に提示した諸所の情報と組織構成員の振る舞いのログが本システムによって収集できるため，今後の組織構成員に対する教育や訓練，注意喚起の改善に役立つのではないかと考えられる．

今後は，本提案システムの実証実験を行うとともに，組織構成員からの報告に関する重みづけ手法や，組織構成員からの振る舞いログを活用した個々人に効果がある注意喚起の UI・メッセージのカスタマイズ手法や自動化手法について検討を進めていきたいと考えている．

謝辞 本研究成果は国立研究開発法人　情報通信研究機構(NICT) の委託研究「Web 媒介型攻撃対策技術の実用化に向けた研究開発」により得られたものである．ここに深謝する．

参考文献

[1] “FFRI Mr.F”. http://www.ffri.jp/online_shop/proactive/index.htm, (参照 2016-08-07)

[2] “Wild Fire”. https://www.paloaltonetworks.jp/products/technologies/wildfire.html, (参照 2016-08-07)

[3] 山田 正弘, 森永 正信, 海野 由紀, 鳥居 悟, 武仲 正彦. 組織内ネットワークにおける標的型攻撃の検知方式. 研究報告セキュリティ心理学とトラスト（SPT） 2013-SPT-6(53), 1-6, 2013-07-11

[4] “CipherCraft/Mail 標的型メール対策”. https://www.ntts.co.jp/products/ccraftmailtypeh/, (参照 2016-08-07)

[5] “GUARDIANWALL”. http://canon-its.jp/guardian/product/gw/, (参照 2016-08-07)

[6] 吉岡 孝司, 片山 佳則, 津田 宏, 森永 正信, 深澤 亮太. 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. 情報処理学会論文誌 55(10), 2290-2299, 2014-10-15