三重大学における標的型攻撃メール訓練の実施について

三重大学工学部技術部
〇深澤　祐樹
fukazawa@arch.info.mie-u.ac.jp

三重大学自然科学系技術部
松原　伸樹
matsubara@cc.mie-u.ac.jp

1. はじめに

近年，特定の個人や組織を対象に，個人情報や，業務機密などの情報資産を狙った標的型攻撃メールが増加傾向にある．これらは受信者心理の隙を突くソーシャルエンジニアリングという手法で，特定のサイトなどへの誘導を仕向ける方式などがみられる．三重大学では情報セキュリティ対策基本計画にて職員の自衛意識を高めるべく，標的型攻撃メール訓練の実施を掲げている．本発表では本学にて実施した標的型攻撃メール訓練について報告する．

2. 標的型攻撃メールとは

一般に迷惑メールは，スパムメール，フィッシングメール，標的型攻撃メールの 3 つに分類される．スパムメールやフィッシングメールは不特定多数の宛先に送られるもので，前者は通販サイトへの誘導やウィルスへの感染，後者は銀行や通販サイトのログイン情報などを狙うもので金銭などの獲得が目的である．一方，標的型攻撃メールは特定の個人や企業を狙うことに特化し，個人情報や業務機密などの奪取のため周到かつ執拗な攻撃を仕掛けるという特徴がある．

国内では，2005 年の標的型攻撃メールの初観測以後，個人や官公庁，公的機関だけでなく大学や企業を狙った標的型攻撃メールが増加傾向にあり，個人情報の流出などで多くの損害が発生している[*1]．

ここでは標的型攻撃メールの分類，受信者心理を利用した攻撃手法などを説明する．

2.1 標的型攻撃メールの分類

標的型攻撃メールは大きくわけて 3 通りに分類される．

・悪意のあるプログラムに感染させるための Web サイトなどへ誘導するもの

ウェブブラウザやプラグインなどの脆弱性を利用し，改ざんされたウェブページを閲覧させることで不正プログラムに感染させる手法などがある．一例として，ドメインの偽装や表示と異なる偽装リンクへ誘導などの手法がある．

・文書ファイルなどに見せかけた悪意あるプログラムを添付し，開封させようとするもの

これは業務で利用する書類などに偽装し，悪意あるプログラムを実行させようとする手法である．ファイルのアイコンなどを偽装し，一見では判断しづらいものが多い．

・有名なソフトウェアなどのアップデートなどを称し，インストールさせようとするもの

誰もが知っているソフトウェアなどを偽装し，メール受信者の警戒心を低下させ，悪意あるプログラムをインストールさせる．

標的型攻撃メールはこれらの手法を利用して攻撃者への個人情報・業務機密流出や業務システムの閲覧ロックによる金銭奪取などにより，攻撃を行う．

2.2 ソーシャルエンジニアリング

標的型攻撃メールは，悪意のある URL への誘導などのきっかけを作るため，標的となったメール受信者の心理の隙を突くソーシャルエンジニアリングという手法を利用している．この手法は，メール送信者が親しい人物や上司，お客様など確認や返信をしないことが失礼に当たる心理を狙うもの，高額商品当選などの特典や有名人情報などで受信者の興味を引くなどの手法がある．これらのほかにも急を要する確認事項や，回答の〆切時間が間近に迫るなど受信者の判断力や余裕を低下させることで，URL クリックや悪意あるプログラムの実行へ誘導する手法もある．標的型攻撃メールは，メール受信者に対してメールを開封したい，添付ファイルを確認したいという意識を働かせ，受信者を被害へと導く．

2.3 標的型攻撃被害の連鎖

近年は，標的型攻撃メールに対してわずかな人のリンククリックなどの損害を及ぼす行為を発端に，攻撃者の利益となる被害のさらなる拡大が発生するケースが増加している．これはリンククリックなどをきっかけに組織内部の人間関係などの情報が攻撃者に漏れ，攻撃者が人間関係を活用したより巧妙なりすましメールの送信や悪意ある業務命令の送信，機密情報の遠隔操作などのより深い活動に移行するケースがあげられる．

このように標的型攻撃メールはより巧妙に，より見分けがつきづらいように進化を遂げ，より被害が拡大している．

3. 三重大学における標的型攻撃メール訓練の実施概要

3.1 2017 年度における三重大学の標的型攻撃メール訓練方針

三重大学では情報セキュリティ対策基本計画にて，今後数年に渡って年に 1 度程度の標的型攻撃メール訓練実施を掲げている．本年度の訓練では初回の訓練であることから，訓練メールの内容を熟読すれば，業務関連のメールではないと容易に気付くことが可能な低難易度の訓練を実施することとした．

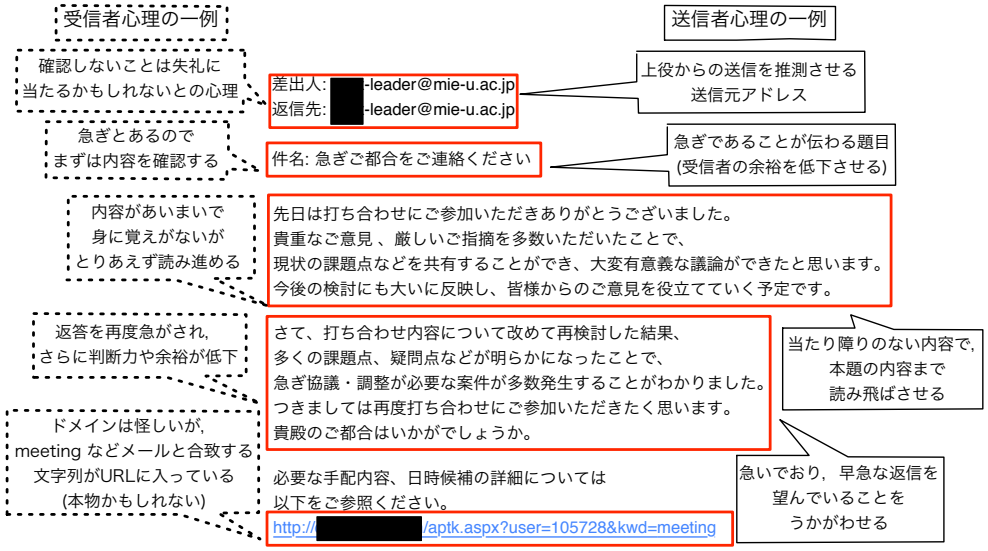

図 1 訓練において送信したメールとメール送信者および受信者心理の例

本訓練において送信したメールの内容と送受信者の心理の一例を図 1 に示す．本年度は標的とする訓練対象者をメール本文内の URL へ誘導するリンククリック型の標的型攻撃メールを採用した．メールの送信アドレスには leader という学内上役を推測させるワード入りのアドレスを利用した．またクリック用の URL には三重大学 (www.mie-u.ac.jp) と異なる訓練専用のドメインを設定した．

受信者心理として，上役からのメールを確認しないことに対する引け目，急いで次の打ち合わせに対する返答を要求することで受信者の余裕や判断力を低下させるような題目および本文，URL に meeting などのメール本文と合致するキーワードが含まれているなど，具体性のない怪しいメール内容ではあるが業務の遂行のため確認を取りたくなる内容としている．

初年度の本訓練では訓練メールに対する絶対的なクリック率の数値よりも，全職員に迷惑メールなどに対する安易なリンククリックを行わないなど自衛意識を高めてもらうことを重視し，メール本文などをしっかり確認すれば被害を防ぐことが可能である訓練メールを準備した．

3.2 標的型攻撃メール訓練用キット利用による訓練実施の容易化

リンククリック型の標的型攻撃メール訓練を実施するには全職員に訓練用メールを送信，かつ URL クリック者を特定する必要がある．このうち，クリック者の特定には通常 Web サーバのアクセス解析などが必要であり，対象者が数千人におよぶ本学ではこれらの解析にかなりの労力を要すると想像される．

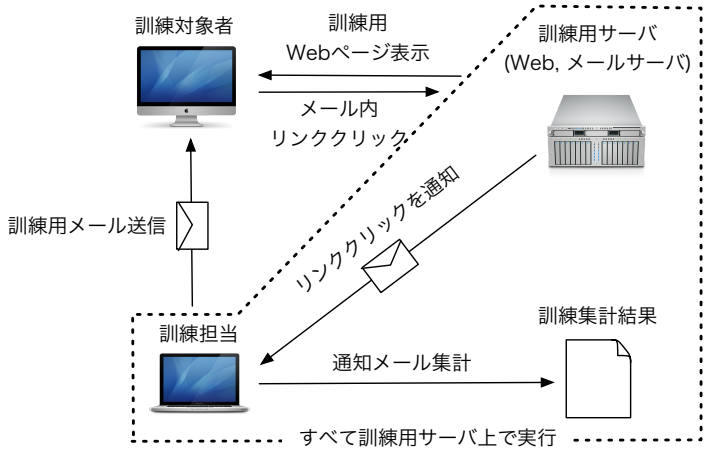

図 2 訓練の実施概要

そこで，縁マーケティング研究所[*2]より発売されている標的型攻撃メール訓練キットを利用することとした．このソフトウェアは不正プログラム添付型，リンククリック型などの多くの標的型攻撃メール訓練に対応するほか，Windows，Linux と複数の OS に対応したメール一斉送信ツールやアクセス解析ツールなどを標準で備えている．本訓練では訓練専用サーバとして WindowsServer 2012R2 に Microsoft Office，IIS，ASP.NET モジュールおよび SMTP サーバ機能をインストールした構成を利用した．

図 2 に本訓練の実施概要を示す．まずは訓練担当者がツールを用いて，図 1 に示す訓練用メールを全教職員に一斉送信する．このメール内には 1 通毎に異なる user 番号が入った URL が記載され，この URL を利用してクリック者との 1 対 1 の対応付けを行う．メール受信者が URL をクリックすると，集計用メールアドレスに通知メールが送信され，訓練担当へ通知される仕組みとなっている．

訓練は表 1 に示すスケジュールに沿って準備を進め，ソフトウェアの設定などを行った．11 月 8 日の 40 名程度を対象とした訓練の事前テストを経たのち，12 月 6 日 13 時過ぎより本番用メール送信を開始し，1 週間経過後の 12 月 13 日の集計を予定している．

表 1 標的型攻撃メール訓練実施スケジュール

3/30	情報セキュリティ対策基本計画策定 (標的型攻撃メール訓練を実施することを明記)
8/6-10/3	標的型攻撃メール訓練用ソフトウェア選定
9 月	工学部技術部と総合情報処理センターとの 協力による訓練実施を決定
9/13	標的型攻撃メール訓練実施の周知
10/6	初回打ち合わせ・今後のスケジュール調整
10/10-11/6	訓練用サーバの構築・ソフトウェアの設定
11/8	標的型攻撃メール訓練事前テストの実施
11 月	訓練用メール送信リスト作成
12/6	訓練用の標的型攻撃メールを送信
12/7-	結果集計・分析

表 2 訓練実施後の集計結果の一例

所属部署名	対象者数	開封者数	開封率
医学部	300	54	18.00%
教育学部	100	17	17.00%
工学部	200	23	11.50%
事務局	130	16	12.31%
人文学部	90	15	16.67%
生物資源学部	80	14	17.50%
各種センター	30	9	30.00%
管理職	100	20	20.00%
合計	1030	168	16.31%

※ 本学の訓練実施結果ではありません．

3.3 標的型攻撃メール訓練実施結果の集計

本訓練では，訓練実施後にリンククリック者情報の記載された通知メールをアクセス解析ツールによって訓練の実施結果を取りまとめた．訓練用ソフトウェアでは，アクセス解析ツール内に予め訓練対象者をそれぞれ集計したい項目でタグ付けすることで，所属先や役職に応じた集計データを得られる．なお訓練の集計結果は非公開のため，表 2 に本訓練における集計結果の一例を示す．表 2 に示すように所

属先に応じたリンククリック率(開封率)や，開封者の絶対数などが表示されていることがわかる．アクセス解析ツールでは同一 URL への複数回アクセスやアクセス日時も表示可能であり，訓練対象者の振る舞いの分析が可能である．また集計は所属だけでなく，役職などの他の項目でも実行可能である．

3.4 標的型攻撃メール訓練におけるリンククリック者への不審なメールに対する注意喚起

本訓練では，リンククリック者に対して注意喚起を促すため，メール内リンクのクリック後，図 3 に示す注意喚起のページへ自動ジャンプするよう設定した．注意喚起のページ内では標的型攻撃メールの被害について認識いただき，今後の参考となるよう不正なメールの見分け方などを記載して，職員の自衛意識を高める手助けとなるようなページを作成した．

また，訓練実施結果の集計後に集計結果の公表と不審なメールの見分け方などの周知を改めて実施し，全職員の自己防衛意識をより高めるほか，Windows10 Enterprise (Fall Creators Update 以降) にて実装された Microsoft Edge の Windows Defender Application Guard をはじめとした仮想ブラウザ環境の利用により，物理環境から分離された仮想環境によって標的型攻撃の被害を防ぐことが可能となることの周知も行っていきたい．

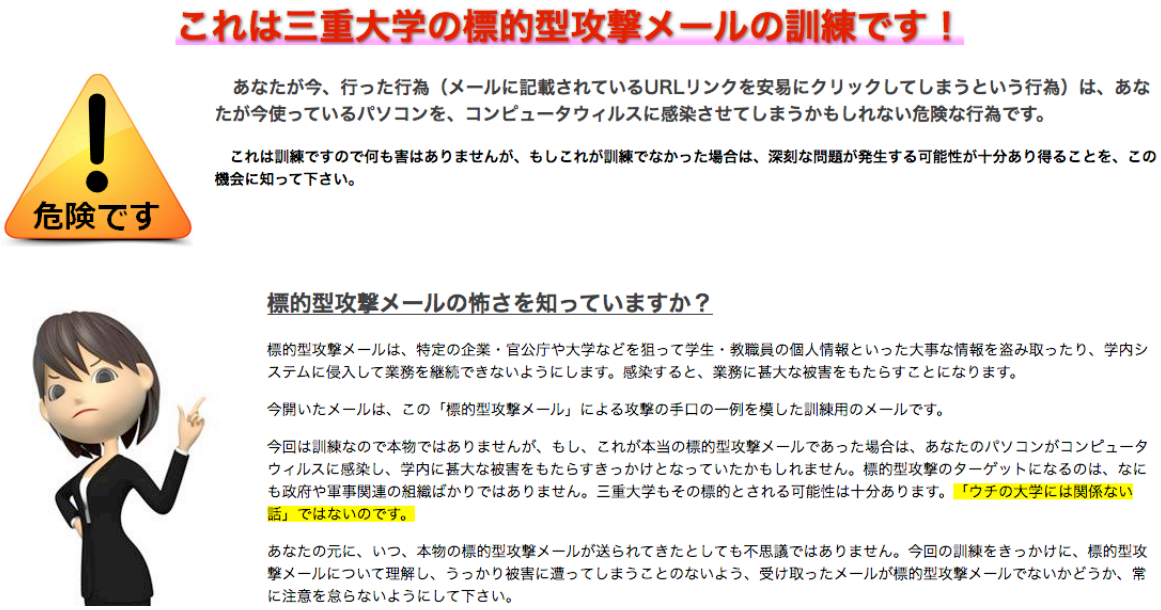

図 3 訓練メール内のリンククリック後に表示される注意喚起用 web ページ

4. まとめ

本発表では，三重大学における標的型攻撃メールに対する訓練実施について報告した．訓練用キットの利用により，アクセスログ解析などの作業を容易としたことで，本来の訓練実施や訓練実施後の分析にリソースを割くことができ，初年度としては十分な訓練が実施できた．今後，訓練実施結果の公表とともに，あらためての標的型攻撃メールの脅威・対策に関する周知を行う予定である．

謝辞

本学における標的型攻撃メール訓練実施のために総合情報処理センター，情報基盤室をはじめとした本学構成員の皆様方に数多くのご協力・ご支援をいただきましたことをここに深く感謝申し上げます．

参考文献

1) 独立行政法人 情報処理推進機構 「標的型攻撃メールの傾向と見分け方～サイバーレスキュー隊（J-CRAT の活動を通して）～」https://www.ipa.go.jp/files/000052612.pdf 2015 年
2) 縁マーケティング研究所 https://kit.happyexcelproject.com/