学習項目に応じた訓練用標的型メールの自動生成および個別配信システムの実装と評価

板倉 健将　依田みなみ　五味 悠一郎

標的型メール攻撃はシステム面の対策だけでは防ぎきれないため，従業員一人ひとりのセキュリティ意識向上を目的とした標的型メール訓練が有効な人的対策として求められている．しかし，外部訓練サービスの利用はコスト負担が大きく，自社での訓練環境構築には専門的な技術やノウハウを要するため，特に中小企業では十分な実施に至っていない．本稿の目的は，このような課題を踏まえ，組織における運用負荷を抑えつつ，教育効果の高い実践的な標的型メール訓練を実施できる環境を構築することである．先行研究では Gemini を用いたメール自動生成と配信制御を行うシステムを開発したが，学習項目に応じたプロンプトの手動変更にかかる工数や，訓練者ごとに適したメールを自動配信する機能に課題があった．これらの課題を解決するため，本稿では IPA，総務省，警察庁が公開しているセキュリティ脅威レポートおよび対策ガイドラインに基づき，11 の学習項目を定義した．その上で，選択した学習項目に応じたプロンプトを自動生成するシステム Ver.3.1 と，スプレッドシートのデータに基づき訓練者ごとに適切な学習項目のメールを自動選択・配信する配信システムを開発した．評価として，300 通の機能テストを行った結果，学習項目に対応したメールの生成および正常な送受信が確認でき，運用の自動化と実践的な訓練の両立に寄与するシステムを実装した．

1　はじめに

標的型攻撃は，サイバー攻撃の代表的な手法のひとつである．独立行政法人情報処理推進機構（IPA）が毎年公表する情報セキュリティ10 大脅威では，組織向け脅威として「機密情報等を狙った標的型攻撃」が 2016 年の初選出以来 2026 年まで [2]11 年連続でランクインしており，企業が優先的に取り組むべき脅威として位置づけられている．なかでも，メールを介して標的組織ネットワークへ初期侵入を図る手法は，標的型メール攻撃とよばれる．

標的型メール攻撃は，不特定多数ではなく特定の組織や個人を対象に送付される点に特徴があり，受信者の端末をマルウェアに感染させる，あるいはフィッシングサイトへ誘導して認証情報を窃取することを主な目的とする．送信元を詐称したり，本文中で URL へのアクセスや添付ファイルの開封を誘導したりする文面が多く用いられる．こうした攻撃はシステム面の対策だけでは防ぎきれないため，従業員一人ひとりのセキュリティ意識向上を含めた人的対策を並行して講じる必要がある．

人的対策のひとつとして標的型メール訓練が挙げられるが，訓練実施には，外部の訓練サービスを利用する方法と，訓練環境を自社で構築する方法が考えられる．前者はコスト面の負担が大きく，特に中小企業では十分な実施に至っていない．後者は専門的な技術や運用ノウハウが求められるため，導入は容易ではない．

先行研究 [6] [7] では，生成 AI を用いて訓練用標的型メールを自動生成する仕組みと，生成したメールを訓練者へ配信するシステムがそれぞれ開発され，低コ

Implementation and Evaluation of an Automated Generation and Individualized Delivery System for Spear-Phishing Training Emails Corresponding to Learning Items

Kensuke Itakura, 日本大学理工学部応用情報工学科, Department of Computer Engineering, College of Science and Technology, Nihon University.

Minami Yoda, 日本大学理工学部, College of Science and Technology,Nihon University.

Yuichiro Gomi, 日本大学理工学部, College of Science and Technology,Nihon University.

[企業名]
[氏名] 様

いつも[送信者名]をご利用いただき、誠にありがとうございます。この度、[送信者名]では、[年月日]に東京ソラマチにてイベントを開催いたします。[氏名]様には、本イベントに特別にご招待させていただきます。
詳細につきましては、下記 URL をご確認ください。
[URL]
ご多忙中とは存じますが、ぜひご参加ください。

[送信者名]
電話番号: [電話番号]
メールアドレス: [送信者メールアドレス]

図 1　自動生成した訓練用標的型メール文章

ストな訓練環境の構築が図られてきた．しかし，学習項目に応じたプロンプトの手動変更にかかる工数や，訓練者ごとに適したメールを自動配信する機能には課題が残されていた．

本稿では，これらの課題を解決し，学習項目に応じてメールを自動生成・配信できるシステムを開発することで，企業が低コストかつ手軽に実践的な標的型メール訓練を実施できる環境の実現を目指す．

2　先行研究

2.1　訓練用標的型メール自動生成システム Ver.3.0

徳野ら [6] は，Google が提供する生成 AI である Gemini の API を利用し，Google Colaboratory 上で動作する訓練用標的型メールの自動生成プログラムを開発した．このプログラムは，メール文章に URL へのアクセスを誘導する記述を含める点と，文中の固有名詞を後から入力内容へ置き換えられるよう伏字化しておく点を，あらかじめ生成条件として組み込んだ．

利用者が生成したいメールの概要を入力欄に記述することで，多様な訓練用標的型メールを出力できる．生成モデルには gemini-1.5-flash を採用した．開発したこのプログラムを，訓練用標的型メール自動生成システム Ver.3.0 と命名した．自動生成したメール文章の例を図 1 に示す．

2.2　訓練用標的型メール配信システム Ver.3.0

山口 [7] は，訓練用標的型メール自動生成システム Ver.3.0 で生成したメール文章を訓練者へ配信するシステムを開発した．このシステムは Google Apps Script（GAS）上に構築して，URL クリックの検知処理を GAS へ統合することで，システム構成を単純化するとともに，HTML 形式のファイルをメールに添付送信する機能と，Web ビーコンの原理を用いて添付ファイルの開封を検知する機能を開発した．

URL のクリックや添付ファイルの開封を検知した際には，訓練者本人へ検知結果を通知するメールを自動送信する機能を開発した．この通知機能に加え，訓練者間での情報共有や，一斉送信によるメールサーバ側でのブロックを避けるため，配信先をランダムに抽出する機能と，送信時刻をずらす機能を開発した．

中小企業基本法が定める常時使用する従業員の数の基準 [1] に基づき，訓練対象者数の上限を 300 人とした．訓練用標的型メール配信システム Ver.3.0 における，メール送信機能のシーケンス図を図 2 に示す．

このシステムを用いた機能テストでは，10 個のメールアドレス宛てにそれぞれ 30 通ずつ，合計 300 通の訓練用標的型メールを送信して，添付ファイルを含めて全てのメールが正常に送受信できること，および URL クリックや添付ファイル開封の検知・通知が正常に動作することを確認した．

2.3　先行研究の課題

訓練用標的型メール配信システム Ver.3.0 は，送信先ごとに異なるメール文章を割り当てる機能を備えておらず，全員に同一のメール文章を送信する仕様であった．この仕様では，受講者の特性や過去の履歴を踏まえて内容を個別化する場合，添付するファイルの ID を一人ずつ手作業で差し替える必要があり，運用負担が大きいという課題があった．

訓練用標的型メール自動生成システム Ver.3.0 においても，メールに含める内容をその都度入力欄へ記述する方式を採っていたため，訓練者に習得させたい脅威の類型に応じてプロンプトを手動で書き換える必要があり，特定の学習内容を反映したメールを効率的に生成する仕組みを備えていないという課題があった．

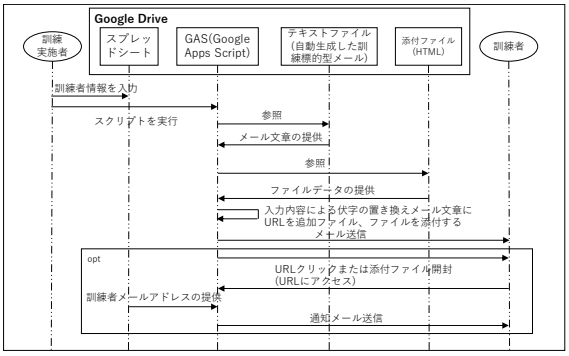

図 2　訓練用標的型メール配信システム Ver.3.0 におけるメール送信機能シーケンス図

表 1　学習項目

No.	学ばせたいこと	出典
1	不必要な URL クリックや添付ファイル開封の誘導を識別できること	[3]
2	URL や添付ファイルを開かざるを得ない内容に潜む不自然さを識別できること	[3]
3	日本語の不自然な言い回しを識別できること	[3]
4	パスワード変更や振込先変更をメールで求める不審さを識別できること	[3] [4]
5	海外の銀行口座を振込先として指定している不審さを識別できること	[4]
6	ソーシャルエンジニアリング（緊急性・重要性を装う手口）への不審さを識別できること	[5]
7	普段やりとりしない企業や組織からのメールを不審と識別できること	[3] [5]
8	取引先や自社の経営者層を装ったなりすましを識別できること	[4]
9	ID やパスワードの入力を要求する不審さを識別できること	[3]
10	日本語では通常使われない漢字（繁体字・簡体字）の混在を識別できること	[3]
11	署名の内容が誤っている（実在しない）ことを識別できること	[3]

これらの課題を解決するため，本稿では「学習項目に応じたプロンプトの自動追加」と「訓練者ごとの学習項目に基づくメールの自動選択・配信」を課題として設定する．

3　目標

本稿の目標は，標的型メール訓練における学習項目を制御基準として定義し，訓練者に習得させるべき学習項目に応じたメールを効率的に生成・配信できるシステムを構築することである．具体的には，選択した学習項目に応じてプロンプトを自動的に追加を行い，メール文章を生成する訓練用標的型メール自動生成システム Ver.3.1 を開発するとともに，スプレッドシートに設定した学習項目に基づき，訓練者ごとに対応するメール文章を自動的に選択して配信する訓練用標的型メール配信システム Ver.3.1 を開発する．これらのシステムにより，プロンプトやファイル ID の手動変更を必要とせず，訓練者の部署や個人の特性および過去の訓練履歴に応じた学習項目に基づき，実践的な標的型メール訓練の実施を可能にする．

4　学習項目に基づく訓練用標的型メールシステム

4.1　標的型メール訓練における学習項目

標的型メール訓練においてメール文章から学んでほしい内容を，11 項目の学習項目として表 1 のとおり定義した．学習項目の選定にあたっては，IPA が公開する「標的型攻撃メールの例と見分け方」[3] が示す標的型攻撃メールの着眼点を主要な枠組みとして採用した．同資料が示す着眼点は，差出人のメールアドレス・本文の日本語表現・添付ファイルの拡張子や実行形式・署名の内容など，メールを構成する要素ごとに，標的型攻撃メールに特徴的な不審点を整理した一覧である．これらの不審点のうち，メール本文の記述のみで訓練用メールとして再現可能な着眼点を学習項目 3，10，11 とし，添付ファイルや URL への誘

導に関する着眼点を学習項目 1，2，9 とした．

IPA の着眼点に加えて，警察庁 [4] および総務省 [5] で指摘されている，取引先や経営者層へのなりすまして，振込先の変更要求，緊急性を装う心理的誘導といった，より高度なソーシャルエンジニアリングの観点を学習項目 4，5，6，7，8 として追加した．これら 11 の学習項目の追加により，メール本文の技術的な不審点を見分ける基礎的な着眼点から，攻撃者の心理的な誘導手口を見抜く高度な着眼点までを，訓練者が段階的に習得できるよう構成した．

各情報源で重複する着眼点はひとつの学習項目に統合しており，本稿の項目は各情報源の着眼点を過不足なく網羅する形で設定した項目数である．学習項目は，不審な URL クリックや添付ファイル開封の誘導に対する識別力といった基本的な着眼点から，ソーシャルエンジニアリングやなりすましへの耐性といった高度な着眼点までを含む，11 項目で構成した．

4.2 訓練用標的型メール自動生成システム Ver.3.1

訓練用標的型メール自動生成システム Ver.3.0 は，特定の学習項目を反映したメール文章を生成する際，その都度プロンプトを手動で書き換える必要があるという課題があった．この課題を解決するため，本稿では Google Colaboratory 上で Gemini API を利用し，学習項目に応じたプロンプトを自動的に追加するプログラムを開発した．利用者が「メール文章に含めたい学習項目の番号」を入力すると，あらかじめ定義した標的型メールの特徴や，配信システムにおける固有名詞の置き換え前表現を踏まえたプログラムがプロンプトを自動的に構成して，訓練用標的型メールを生成する．生成モデルには gemini-2.5-flash を採用した．本稿ではこのプログラムを追加したシステムを，訓練用標的型メール自動生成システム Ver.3.1 と命名した．メール文章自動生成の流れを図 3 に示す．

4.3 訓練用標的型メール配信システム Ver.3.1

訓練用標的型メール配信システム Ver.3.0 は，送信先ごとに異なるメール文章を割り当てる機能を備えておらず，訓練者の特性に応じた訓練を行うには，添

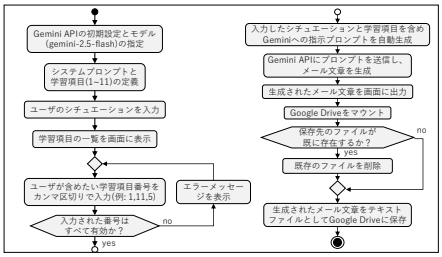

図 3　自動生成システム Ver.3.1 におけるメール文章生成のアクティビティ図

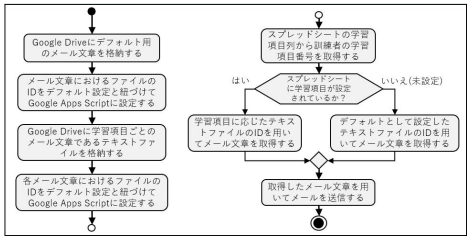

図 4　訓練用標的型メール配信システム Ver.3.1 のアクティビティ図

付するファイルの ID を手動で切り替える必要があるという課題があった．この課題を解決するため，スプレッドシート上の学習項目列に基づき，訓練者ごとに対応するメール文章を自動的に選択して送信するプログラムを開発した．このプログラムは，訓練者ごとに設定された学習項目番号を読み取り，対応するテキストファイルの ID を用いてメールを送信する．学習項目が未設定の場合は，あらかじめ設定したデフォルトのテキストファイルを用いて送信する．このプログラムを追加したシステムを，訓練用標的型メール配信システム Ver.3.1 と命名した．配信システム Ver.3.1 における処理の流れを図 4 に示す．

5　テスト方法

訓練用標的型メール自動生成システム Ver.3.1 について，学習項目番号 1〜11 のそれぞれを単独で 1 回ずつ入力すると，プログラムが対応する学習項目のプロンプトを追加し，正常にメール文章を生成することを確認する機能テストを行った．学習項目 1 と 6 を組み合わせて 1 回入力した場合についても，それ

ぞれに対応する学習項目のプロンプトを追加し，正常にメール文章を生成することを確認した．

訓練用標的型メール配信システム Ver.3.1 について，スプレッドシート上の学習項目列に，学習項目番号 1〜11 および未設定をそれぞれ 25 人ずつ設定した計 300 人の訓練者に対し（※以降「訓練者」は実際の人間の被験者ではなく，機能テスト上の送信対象データを指す），各学習項目に対応する異なるメール文章を送信する機能テストを行った．

送信するメールには，2.2 節と同様に URL クリック検知機能をもつ URL，および添付ファイル開封検知機能をもつ添付ファイルを含め，10 個のメールアドレスに対して各 30 通ずつ計 300 通を送信する方法でテストを行った．1 個のメールアドレスには複数の学習項目区分に対応するメールを割り当て，同一アドレス宛に異なる内容のメールを送信する構成とした．

学習項目が未設定の訓練者に対しては，あらかじめ設定したデフォルトのメール文章を送信することもあわせて確認した．本テストでは 2.2 節で述べた送信時間をずらす機能は使用せず，300 通を一括して送信した．

6　結果と考察

訓練用標的型メール自動生成システム Ver.3.1 を用いた機能テストでは，学習項目番号 1〜11 をひとつずつ入力した場合，および複数の学習項目番号を組み合わせて入力した場合のいずれにおいても，プログラムが対応する学習項目のプロンプトを自動的に追加し，正常にメール文章を生成することを確認した．学習項目 6 であるソーシャルエンジニアリングへの不審さの識別を入力して，生成したメール文章の例を図 5 に示す．このテストの結果から，訓練用標的型メール自動生成システム Ver.3.1 は，学習項目に応じたプロンプトの手動変更を必要とせず，多様な学習項目を反映した訓練用標的型メールを効率的に生成できるといえる．

訓練用標的型メール配信システム Ver.3.1 を用いた機能テストでは，スプレッドシート上の学習項目列に学習項目番号 1〜11 および未設定をそれぞれ設定した計 300 人の訓練者に対し，各学習項目に対応する

[氏名]様

平素よりお世話になっております。[送信者名]でございます。

【重要なお知らせ】新業務システム移行に伴う設定確認のお願い
この度、[企業名]では業務効率化を目的として、[年月日]より新業務システムへの移行を実施いたします。これに伴い、全従業員の皆様に至急、新システムへのアクセス設定と利用マニュアルの確認をお願いしております。
期日までに必要な設定が完了していない場合、新システムへのログインや業務の継続に支障が生じる可能性がございます。

つきましては、下記 URL より詳細な手順とマニュアルをご確認の上、速やかにご対応いただけますようお願い申し上げます。

[URL]

ご多忙の折、大変恐縮ですが、何卒ご理解ご協力のほど、よろしくお願い申し上げます。

[送信者名]
[電話番号]
[送信者メールアドレス]

図 5　学習項目 6 を入力して生成されたメール文章

異なるメール文章 300 通を正常に送受信できることを確認した．学習項目を設定したスプレッドシートの例を図 6 に示す．図 6 中の「訓練者メアド」は，大学ドメインのテスト用メールアドレスであり，実際の訓練対象ではない．学習項目が未設定の訓練者に対しては，あらかじめ設定したデフォルトのメール文章を送信することも確認した．

本テストにおける 300 人の訓練者データは 10 個のメールアドレスに均等に対応させており，1 アドレスあたり学習項目ごとに約 2〜3 人分の計 30 人で訓練者データを割り当てている．この割り当てから，訓練用標的型メール配信システム Ver.3.1 は，訓練者ごとにファイル ID を手動で切り替えることなく，学習項目に応じたメールを自動的に選択・配信できるといえる．

本稿で開発した訓練用標的型メール自動生成システム Ver.3.1 および訓練用標的型メール配信システム Ver.3.1 により，学習項目の設定負荷を増大させることなく，訓練者ごとに適した項目を反映し，実践的な標的型メール訓練を実施できる仕組みを実装した．訓練者の部署や個人の特性，あるいは過去の訓練履歴に応じて異なる学習項目を割り当てられるようになったことで，画一的な訓練内容では得にくい教育効果の向上も期待できる．

7　まとめと今後の課題

本稿では，標的型メール訓練における学習項目を制御基準として定義し，学習項目に応じたプロンプトを自動的に追加する訓練用標的型メール自動生成システム Ver.3.1 と，スプレッドシートに設定した学習項

	A	B	C	D
1	氏名	訓練者メアド	No.	学習項目
2	佐藤	@g.nihon-u.ac.jp	1	
3	鈴木	@g.nihon-u.ac.jp	2	1
4	高橋	@g.nihon-u.ac.jp	3	2
5	田中	@g.nihon-u.ac.jp	4	3
6	渡辺	@g.nihon-u.ac.jp	5	4
7	伊藤	@g.nihon-u.ac.jp	6	5
8	山本	@g.nihon-u.ac.jp	7	6
9	中村	@g.nihon-u.ac.jp	8	7
10	小林	@g.nihon-u.ac.jp	9	8
11	加藤	@g.nihon-u.ac.jp	10	9
12	吉田	@g.nihon-u.ac.jp	11	10
13	山田	@g.nihon-u.ac.jp	12	11
14	佐々木	@g.nihon-u.ac.jp	13	
15	松本	@g.nihon-u.ac.jp	14	1
16	井上	@g.nihon-u.ac.jp	15	2

図 6　学習項目を設定したスプレッドシートの例

目に基づき訓練者ごとに対応するメール文章を自動的に選択・配信する訓練用標的型メール配信システム Ver.3.1 を開発した．機能テストの結果，自動生成システム Ver.3.1 ではプログラムが学習項目に応じたプロンプトを正常に追加し，メール文章を生成することを確認し，配信システム Ver.3.1 では，学習項目を設定した 300 人の訓練者に対して，対応するメール文章 300 通を正常に送受信できることを確認した．

これらの結果から，訓練者ごとにプロンプトやファイル ID を手動で変更する必要がなくなり，手間のかからない実践的な標的型メール訓練の実施が可能になったといえる．

今後の課題として，以下が挙げられる．

1 つ目は，各学習項目に対して最適なメール生成手法を明らかにすることである．本稿では Gemini API を用いた生成手法のみを対象としたが，学習項目によっては，マルコフ連鎖や再帰型ニューラルネットワーク等，他の生成手法がより適している場合もある．盲検法を用いた被験者実験により，学習項目ごとに最適な生成手法を検証する必要がある．

2 つ目は，本稿で定義した学習項目が，訓練者に実際の気づきを与えられるかを検証することである．本稿では機能テストに留まっているため，生成・配信したメールを用いた被験者実験を行い，学習項目として意図した内容への気づきが得られるかを確認する必要がある．

3 つ目は，1 通のメール文章に複数の学習項目を組み合わせた場合の妥当性を検証することである．本稿で開発した自動生成システム Ver.3.1 は複数の学習項目を同時にプロンプトへ追加できるが，それらの学習項目が 1 通のメール文章の中で両立して反映されるかどうかは十分に検証できていない．

4 つ目は，実際の企業環境における動作検証である．本稿における機能テストは，企業のネットワーク環境や利用するソフトウェアの影響を考慮していないため，実際の環境下でシステムが問題なく動作するかを検証する必要がある．本稿の機能テストでは 10 個のメールアドレスに対して重複して送信したが，重複しない 300 個のメールアドレスを用いた検証も今後の課題である．

これらの課題を解決することで，学習項目に基づく訓練用標的型メールシステムは，より実践的な標的型メール訓練の実現に資すると考える．

謝辞 本稿の作成にあたり協力いただいた山口智誠氏に感謝いたします．

参 考 文 献

[1] 中小企業庁: 中小企業基本法, https://www.chusho.meti.go.jp/faq/faq/faq01_teigi.html. (参照 2026-08-03).

[2] 独立行政法人情報処理推進機構 (IPA): 情報セキュリティ10 大脅威 2026, https://www.ipa.go.jp/security/10threats/10threats2026.html. (参照 2026-08-03).

[3] 独立行政法人情報処理推進機構 (IPA): 標的型攻撃メールの例と見分け方, https://warp.da.ndl.go.jp/info:ndljp/pid/12446699/www.ipa.go.jp/files/000043331.pdf. (参照 2026-08-03).

[4] 警察庁: ビジネスメール詐欺に注意！, https://www.npa.go.jp/bureau/cyber/countermeasures/bec.html. (参照 2026-08-03).

[5] 総務省: 標的型攻撃への対策, https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/security/business/staff/04/. (参照 2026-08-03).

[6] 徳野響, 五味悠一郎: 自動生成した標的型メールを用いた訓練用標的型メール配信システムの開発と評価, コンピュータソフトウェア, Vol. 42, No. 2(2025), pp. 252–257.

[7] 山口智誠, 五味悠一郎: 学習項目に基づく訓練用標的型メール自動生成システムおよび実践的配信システムの開発と評価, 日本ソフトウェア科学会第 42 回大会投稿原稿（未採択）, 2025.