信州大学における疑似体験型攻撃メール訓練の開発

内山　巧，永井　一弥，浅川　圭史，長田　和宏，不破　泰

大学をターゲットとするメールによる標的型攻撃の激化に伴い，大学の全構成員を対象とするメール利用に関する教育の必要性が増している．このことを背景として，本学を含む多くの大学では疑似標的型攻撃メールを送付する方式によるセキュリティ訓練を行っている．本稿では本学における訓練について説明するとともに，そこで明らかとなった複数の課題を述べる．そのうえで，これらの課題解決を目指し，現在開発中の疑似体験型の訓練システムについて述べるとともに，訓練の実施状況と今後の方針を紹介する．

キーワード：セキュリティ教育，標的型攻撃，疑似体験

1. はじめに

2018 年，大学で利用するウェブメールサービスをターゲットとしたフィッシングにより，情報漏洩や迷惑メール送信などの被害が相次いで発生した [1]．信州大学においてもその脅威は例外ではなく，フィッシングや標的型攻撃への対策は喫緊の課題となっている．特に標的型攻撃においては，大学構成員の一人が標的型攻撃メールを開封してマルウエアに感染してしまうと，その PC を踏み台に攻撃が進行し，学内ネットワークに接続されたさまざまなシステムに影響がおよび，大きな損害の発生に発展してしまう．

セキュリティ製品などによるシステム的な対策に取り組んでいたとしても，メール開封の最後の判断は個人に委ねられるため，これらのサイバー攻撃を完全に防ぐことは不可能であると考える．しかしながらセキュリティ訓練を通して攻撃の特徴や手法を学び，大学組織の構成員一人ひとりの情報セキュリティに対する当事者意識を高めることで，セキュリティインシデント発生のリスクを低減させることは可能である．

本学ではメールを悪用したさまざまな攻撃事例を知り，適切にメールを利用できるようになることを目標として，2015 年度から 2 年間，疑似標的型攻撃メールを用いた訓練を実施した．2018 年度には，2015, 2016 年度の訓練で明らかになった課題を改善した疑似体験型セキュリティ訓練のシステムを開発し，実施した．2018 年度に実施した疑似体験型セキュリティ訓練のシステムは，攻撃の手口や手法，マルウエア感染時の挙動などを体験することができる点が特徴である．

本稿では，実施した疑似体験型セキュリティ訓練の実施方法と結果を示し，信州大学におけるセキュリティ訓練の取り組みを紹介する．

2. 従来の標的型攻撃メール訓練

2015 年，訓練実施スタッフが訓練対象者へ標的型攻撃メールを模した疑似標的型攻撃メールを送付する形式で，標的型攻撃メール訓練を実施した．

具体的には，ファイルを開封すると Web サーバへアクセスする Web ビーコンと呼ばれる機能を組み込んだ Microsoft Word ファイルを訓練スタッフが作成し，同ファイルを電子メールへ添付し，訓練対象者へ送付した．Web サーバのアクセスログを調べることで，添付ファイルがどれくらい開封されたかを確認することができるようになっている．

ただし本訓練は，メールに関する注意喚起を通し，訓練対象者の情報セキュリティに対する当事者意識向上を目的としたため，添付ファイルを開封した対象者には注意喚起の文章が表示され，また添付ファイルの開封率は評価のために計測するが，誰が開封したかのログは取らないこととした．

2.1 標的型攻撃メール訓練の流れ

訓練の流れを表 1 に示す．

2.2 訓練詳細

2.2.1 訓練計画と役員承認

訓練であったとしても，疑似標的型攻撃メールを突然大学内へ送付することは大学の正常業務を侵害することにつながりかねないため，学長・理事・学部長から構成される役員部局長会議へ訓練計画を提出し，承

うちやま　たくみ，ながい　かずや，あさかわ　よしふみ，ながた　かずひろ，ふわ　やすし
信州大学総合情報センター
〒 390–8621 長野県松本市旭 3–1–1
iic-staff@shinshu-u.ac.jp

Copyright ⓒ by ORSJ. Unauthorized reproduction of this article is prohibited.

表 1　疑似標的型攻撃メール訓練の流れ

順	内容
1	訓練計画と役員承認
2	対象組織との NDA 締結
3	訓練実施日程の選択
4	添付ファイルとシステムの準備
5	事前教育
6	予行演習とシステムの準備
7	訓練対象者の選定
8	疑似標的型攻撃メールの送信
9	訓練実施の事後通知（種明かし）
10	訓練対象者へのアンケート実施
11	アンケート集計結果の報告

図 1　Word 添付ファイルの内容

認を得た．

2.2.2　日程の調整と事前説明

現場における混乱とトラブルを未然に防止する観点から，訓練対象部局の情報担当者へ訓練概要の説明を行い，協力を得ることにした．

また，訓練に関する情報が事前に訓練対象者へ知れ渡ってしまうと訓練の効果が低下するため，訓練対象者へは知らせないように依頼した．

2.2.3　添付ファイルとシステムの準備

添付ファイルの開封確認を行うため，Word の添付ファイルに URL を埋め込み，ファイルを開封すると同 URL へアクセスが発生する Web ビーコンの仕組みを組み込んだ．なお Word ファイル開封時に訓練メールであることを認識できるよう，Word ファイルへ訓練の内容と標的型攻撃メールへの対応方法の説明を記載した（図 1）．

あわせて学内に Web ビーコンを受信するための Web サーバを構築し，Word 添付ファイルに埋め込んだ URL に相当する 1 × 1 ピクセルの JPG ファイルを設置し，アクセスログの形でアクセス形跡が残る仕組みを準備した．

Web ビーコンの手法によってはメール開封者を特定する形式も実現できたが，開封者の特定は本学の目的ではなかったため，アクセスログは誰が開封したか特定できない形で取得する形式とした．

表 2　事前教育として送付した注意喚起メール

【重要】メール攻撃に関する注意喚起

平素より情報セキュリティ対策にご協力いただきまして，誠にありがとうございます．
最近「標的型メール攻撃」「フィッシングメール攻撃」の脅威が多くの大学や国の機関で問題となっています．信州大学においても「標的型メール攻撃」「フィッシングメール攻撃」がいつあってもおかしくない状況となっております．皆様におかれましては，下記に不審なメールの特徴を示しますので，十分に注意していただきますようお願い致します．

不審なメールの特徴
・身に覚えのないメール
・件名，本文，添付ファイルの日本語がつたないメール
・件名に「緊急」など，添付ファイルの開封を促す言葉があるメール
・知らない URL のリンク付きのメール
・出会い系や商売を紹介するメール
・ID やパスワードの情報入力を要求するメール
標的型メール攻撃においては，受信者が不審をいだかないように，高度な騙しのテクニックが用いられ，ウイルス対策ソフトなどのセキュリティソフトでは対応出来ない場合がほとんどです．
もし，少しでも怪しいと疑ったら，すぐに身近な同僚などへ相談し，総合情報センターまでご連絡をお願いします．

2.2.4　事前教育

標的型攻撃の存在を知り，訓練の疑似標的型攻撃メールに気づくことができるよう，訓練対象者へ事前教育を実施した．教育には集合教育や e-Learning 形式などさまざまな形態があるが，本訓練では標的型攻撃メールに対する注意を喚起するメール（表 2）を訓練対象者へ送付することで事前教育とした．

2.2.5　予行演習

訓練における課題や問題点を洗い出すことを目的とし，訓練対象者へ疑似標的型攻撃メールを送付する前

 Copyright © by ORSJ. Unauthorized reproduction of this article is prohibited.

表 3　予行演習のメール文面の例

表題	＜緊急＞情報漏洩事故に関するお知らせ
差出人	個人情報保護対策委員会 <kojinjoho@shinshu-u.jp>
本文	○○○○さんへ，重要なお知らせです． 平成 27 年 6 月 25 日　個人情報保護対策委員会 個人情報に関する重要なお知らせ． このたび，あなたのクレジットカード情報が漏洩した可能性があるとの通報を受けましたので，個人情報保護対策委員会として学内の状況確認を行っています． お心当たりのある方もない方も，万一に備えて確認をされた方がよろしいかと思いますので，添付の用紙に必要事項をご記入の上，至急ご返送いただきますようにお願い致します． クレジットカード番号を悪用されてしまうと金銭的被害にもつながりかねませんので，お急ぎください．
添付	038-カード情報 f.doc
要点	・差出人が実在しない組織である． ・差出人のアドレスが大学のアドレスに酷似している． ・被害の可能性を提示し，添付ファイルを開かせようとしている． ・「至急」「お急ぎください」など，急がせている． ・署名（発信者の記載）がない

表 4　訓練で用いたメール文面の例

表題	＜緊急＞パスワードに関するお知らせ
差出人	総合情報基盤対策委員会 <s-center@shinshu-u.jp>
本文	○○○○さんへ，重要なお知らせです． 平成 27 年 7 月 総合情報基盤対策委員会 パスワード関する重要なお知らせ． このたび，総合情報基板対策委員会にて，ID とパスワードを一括管理することになりましたので，お知らせします． つきましては，添付ファイルにある，情報を記入の上，至急ご返信いただくようお願いします． ○月○日，までにご返信いただけない場合，システムが利用できなくなりますので，お急ぎください．
添付	038-パスワード.doc
要点	・差出人が実在しない組織である． ・差出人のアドレスが大学のアドレスに酷似している． ・被害の可能性を提示し，添付ファイルを開かせようとしている． ・「至急」「お急ぎください」など，急がせている． ・署名（発信者の記載）がない

に，訓練スタッフが所属する信州大学総合情報センターのスタッフへ表 3 に示す疑似標的型攻撃メールを送付し，予行演習を実施した．

メール文面がクレジットカード情報漏洩という旨の内容であったため，予行演習では実際にクレジットカード会社へ連絡を取ろうとする者が出るという問題が発生した．これを反省点とし，訓練対象者へ送付するメールの内容は，大学組織外に影響が発生しづらい文面へ変更した（表 4）．

2.2.6　訓練の実施と種明かし・アンケート

本訓練は 2015 年度と 2016 年度の 2 回実施した．この両年度の訓練内容は用いたメール文面が違うのみで基本的に同じ手法であるため，本稿では 2015 年を例に説明する．2015 年度の訓練では，信州大学の教職員約 2,500 人が利用する全メールアドレス 6,795 アドレスを対象に，疑似標的型攻撃メールを送付した．

加えて疑似標的型攻撃メール送付の 7 日後に，標的型攻撃メール訓練であった旨を示す種明かしメールと，訓練に対するアンケートの協力依頼のメールを，対象のメールアドレスへ送付した．

なお種明かしメールでは，訓練対象者の不安を払拭するために，次の 2 点について強調して送付した．

・疑似標的型攻撃メールは訓練であり，実害はない
・今回の結果について各個人を評価するものではない

表 5　訓練対象メールアドレス数と開封数

対象メールアドレス数	初日開封数（重複あり）	7 日後開封数（重複あり）
6,795	982	1,065

2.3　訓練結果

訓練における添付ファイルの開封数を表 5 に，訓練に対するアンケートの集計結果を図 2 に示す．正確な開封率を得ることは目的としていなかったため，開封数は Web サーバへ届いた Web ビーコン数をカウントしたものであり，1 人の訓練対象者が複数回添付ファイルを開封した場合も，開封数は複数回カウントしている．

訓練初日の開封数は 982 件となり，これは当初の想定よりも低い値であった．

一方，アンケートの結果から標的型攻撃メール訓練で「それなりに効果がある」以上と答えた訓練対象者が 89％にのぼった．また「今後も訓練すべき」との前向きな回答も得られたことから，訓練対象者の情報セ

Copyright © by ORSJ. Unauthorized reproduction of this article is prohibited.

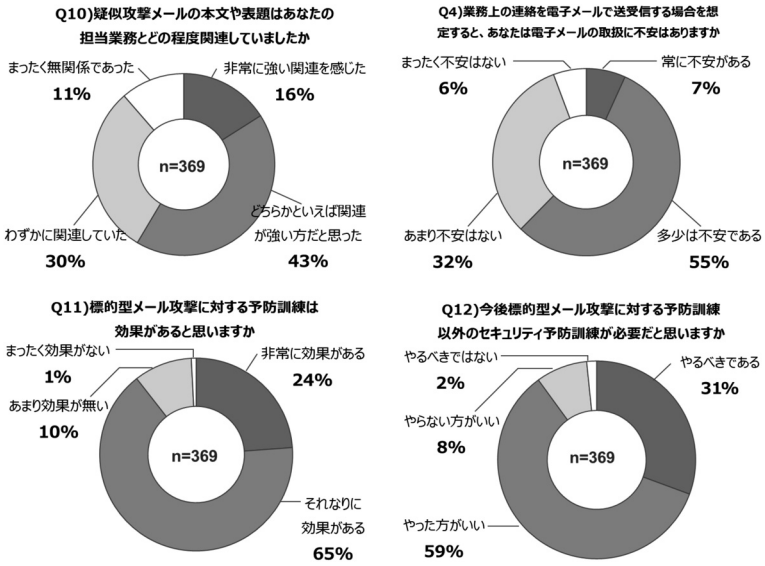

図 2　標的型攻撃メール訓練アンケート結果（抜粋）

キュリティに対する当事者意識向上の目的はおおよそ達成できたものと判断する．

2.4　訓練における課題点

一方，標的型攻撃メール訓練における課題も複数浮き彫りになった．

一つ目として，総合情報センタースタッフを対象にした予行演習では，クレジットカード会社へ連絡を行おうとする者が出るという問題が発生し，訓練実施によって組織外部を巻き込んだ問題やトラブルに発展する可能性があることがわかった．訓練実施前にこれらの危険性を十分調査し，万一の問題発生時に対応するための体制を整える必要がある．

二つ目として，業務への影響と訓練対象者の心理的不安の問題が挙げられる．訓練は，業務で利用している本番のメール環境上で実施しており，かつ訓練対象者は届いたメールが訓練メールであるか断定できないため，メールの調査やウイルススキャンを実施するなど，対応のために業務が一時的に滞ってしまったり対応に混乱が生じてしまったりすることがあった．またアンケートの結果に，本当に被害や影響がないのか心理的な不安を覚えるという意見もあった．容易に訓練であることを確認できる方法を準備するなど，対象者の心理的負担を軽減する方法も十分に考えなければならない．

三つ目として，本来の注意喚起と当事者意識向上という目的が，狙いどおりに行き渡らなかったという点である．一部の訓練対象者や管理職層において，メールおよび添付ファイルの開封率が主たる話題となってしまい，訓練の意図が十分に伝わらない部分があった．また添付ファイルを開かないと注意喚起内容を確認することができない形式であったため，添付ファイルを開封しないという正しい行動をとった者や，メールを確認する前にほかの者からメールの内容を聞いてしまった者など，添付ファイルを開封しなかった訓練対象者に対して注意喚起が届かない結果となってしまった．

最後に，メールを用いた攻撃ではさまざまな文面や手法が用いられるが，一度の訓練で 1 種類の攻撃メールしか体験できない点である．詳細な解説を添付ファイルの中に記載しても，三つ目の課題と同じく添付ファイルを開かなかった場合は注意喚起が届かない結果になってしまう．

3.　疑似体験型セキュリティ訓練の構築

3.1　開発のコンセプト

2 節で挙げた標的型攻撃メール訓練の課題を解決するため，2018 年度，Web ベースの疑似体験型セキュリティ訓練基盤を開発した．本基盤のコンセプトは次のとおりである．

- 疑似空間で体験することにより，大学外への影響や訓練対象者の業務に影響せず，学外へのトラブルや心理的不安を低減する
- 訓練対象者の都合のよいときに受講できるオンデマンド形式を採用することで，業務を妨害せず受講できるようにする
- 実際に疑似攻撃メールを開封して疑似的な被害を経験することで，情報セキュリティに対する関心

 Copyright © by ORSJ. Unauthorized reproduction of this article is prohibited.

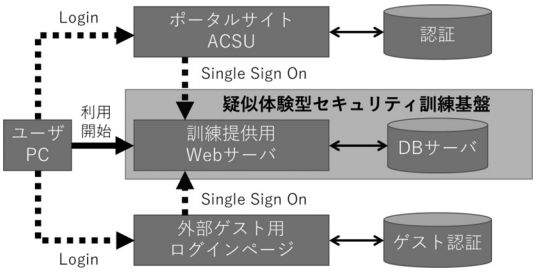

図 3　疑似体験型セキュリティ訓練基盤

を深め，当事者意識のより高い向上効果を得る

・容易にサイバー攻撃のシナリオ（テーマ）を増やせるようにするため，基盤部分とシナリオ部分を分割する構成を用いる

3.2　疑似体験型セキュリティ訓練の基盤

疑似体験型セキュリティ訓練基盤は，訓練を提供する訓練提供用 Web サーバに加えて，各対象者の訓練進捗状況を管理し，統計を取るための DB サーバを構築し，Web サーバと連動させた．

訓練対象者の識別および認証には，本学の認証基盤である ACSU (Active Campus for Shinshu University) を用いた．ACSU と訓練提供用 Web サーバはシングルサインオンでログインできるようになっており，訓練対象者の認証における負担の低減を実現している．

あわせて ACSU の ID を有しない外部ゲスト向けの研修としても活用することができるよう，外部ゲスト用ログインページも準備し，シングルサインオンでログインできるようにした（図 3）．

3.3　訓練フローとインタフェース

疑似体験型セキュリティ訓練基盤において訓練を受けるときの訓練フローを図 4 に示す．実際に疑似攻撃メールを開封して疑似的な被害を経験することをコンセプトとしているため，メールを開くという誤った操作を行わないとシナリオが進まないようになっている．

3.3.1　シナリオ選択・実施履歴画面

訓練対象者がシステムへログインすると図 5 に示す画面が表示され，体験可能なシナリオ一覧と，各シナリオの実施履歴状況が表示される（図中では「テーマ」と表現されている）．DB サーバの中へ訓練の進捗状況が記録されるようになっており，訓練対象者はどのシナリオを受講したか，また各シナリオがどこまで進んでいるか，進捗を確認することができるようになっている．

なお体験できる攻撃は主にメールを介したものであり，2018 年は次の四つのシナリオを準備した．

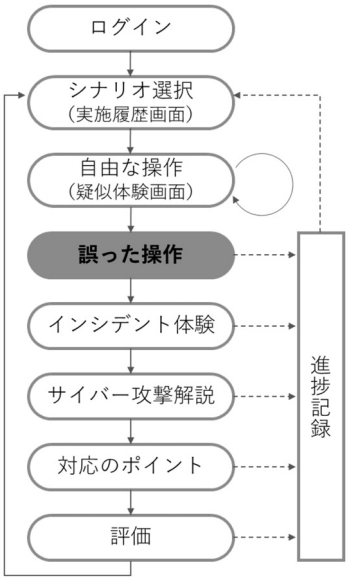

図 4　シナリオフロー

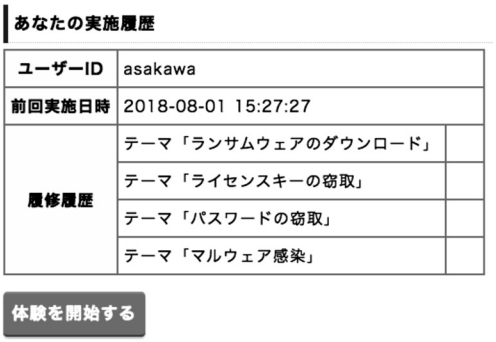

図 5　実施履歴画面

シナリオの種類

・ランサムウエアのダウンロード（添付ファイル）

・ライセンスキーの窃取

・ID・パスワードの窃取

・マルウエア感染（添付ファイル）

3.3.2　疑似体験画面

実施履歴画面から受講したいシナリオを選択すると，疑似体験画面が表示される（図 6）．本学では主にメールシステムに Google 社のクラウド型 Web メールの Gmail を利用している．訓練対象者が日常と同等の操作感を得ることができるよう，訓練基盤の疑似体験画面も Gmail と似たインタフェース構成を採用した．

疑似体験画面は Web メールサービスを模したもので従来のメール機能は有しておらず，メールの送受信などは実際に行うことはできないが，訓練対象者は疑似体験画面上で自由な操作が可能であり，疑似的にメー

Copyright © by ORSJ. Unauthorized reproduction of this article is prohibited.

図 6　疑似体験画面（画像を一部加工しています）

図 7　被害の体験を促すメッセージ

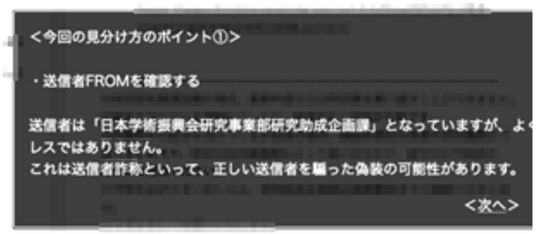

図 8　注意点やポイントを示すメッセージ（画像を一部加工しています）

表 6　疑似体験セキュリティ訓練の受講者数

対象者数	受講者数（ログイン数）	一つ以上シナリオを完了した対象者数
約 2,500	764	674

ルを開く，添付ファイルを開封するなど，本物の Gmail に近い操作を行うことができる．

3.3.3　誤った操作と対応のポイント

テーマを選択すると，サイバー攻撃の体験を促すようなメッセージが表示される（図 7）．

添付ファイルを開封する，メール本文中の URL をクリックするなど，わざと誤った操作を実施すると，ランサムウエアを模してファイルが暗号化される画面が表示されたり，ID が窃取される画面が表示されたりするなど，サイバー攻撃の被害を体験できる画面が出力される．

その後，シナリオの内容に合わせ，添付ファイルの拡張子の確認，送信者メールアドレスの確認など，被害に遭わないようにするための注意点やポイントの解説画面が表示される（図 8）．

3.4　訓練結果

2018 年度のセキュリティ訓練として，2018 年 5 月 18 日から 7 月 31 日実施までの 75 日間，疑似体験型セキュリティ訓練を開催した．この訓練の結果を表 6 へ示す．あわせて訓練受講者へ実施したアンケート結果の一部を図 9 に示す．

訓練対象者は所属や権限単位で一括してシングルサインオンの設定を行ったため正確な対象者数を把握できていないが，全教職員宛てに訓練開催とログイン方法を記載したメールを送信して訓練の受講を通知した．しかし，今回は初めての疑似体験型セキュリティ訓練であることから，受講に要する時間やシナリオのレベルなど訓練受講者への負担が未知数であったため，受講を強制せず，任意で受講するものとした．そのため訓練の受講者数（ログイン数）は少ない数にとどまった．これは比較的セキュリティ意識の高い教職員のみが受講した結果であると考える．限られた範囲での訓練であったが，アンケートの結果から，90%以上の訓練受講者が 30 分以内に受講できており，訓練に係る負担も高くないという結果が得られ，訓練受講者の負担軽減の目的は達成することができたと評価する．

一方，実業務との関連性について，四つのシナリオを平均して 96%以上がわずかにでも業務に関連していると回答し，評価も 96%が「役に立った」と回答した．

このことから，訓練受講者の負担を低減しつつ，サイバー攻撃の特徴や手法を知り，情報セキュリティに対する当事者意識を高めるという目標達成のために，疑似体験型セキュリティ訓練は有効であったと評価する．2019 年以降は部分的に受講を必須化させたり，未受講者に対して受講の催促を行ったりなど，受講対象者の拡大を検討する．

3.5　訓練における課題点

組織のセキュリティレベルを高めるため，組織の全構成員がセキュリティ訓練を受講することができるよう，さらに受講者の負担を軽減しかつ訓練の内容が理解しやすいものになるよう，疑似体験型セキュリティ訓練の環境を改善していく．

3.5.1　機能分割部分の改良

基盤部分の変更を行わずにシナリオの追加や削除ができるよう，基盤部分とシナリオ部分を分割させることで管理の容易化を実現することをコンセプトにしている．しかし現時点ではまだシナリオごとに基盤部分へ修正を加えている箇所があり，システム開発者側でシナリオを実装している状態である．

今後，信州大学側でシナリオを管理できるように機

 Copyright © by ORSJ. Unauthorized reproduction of this article is prohibited.

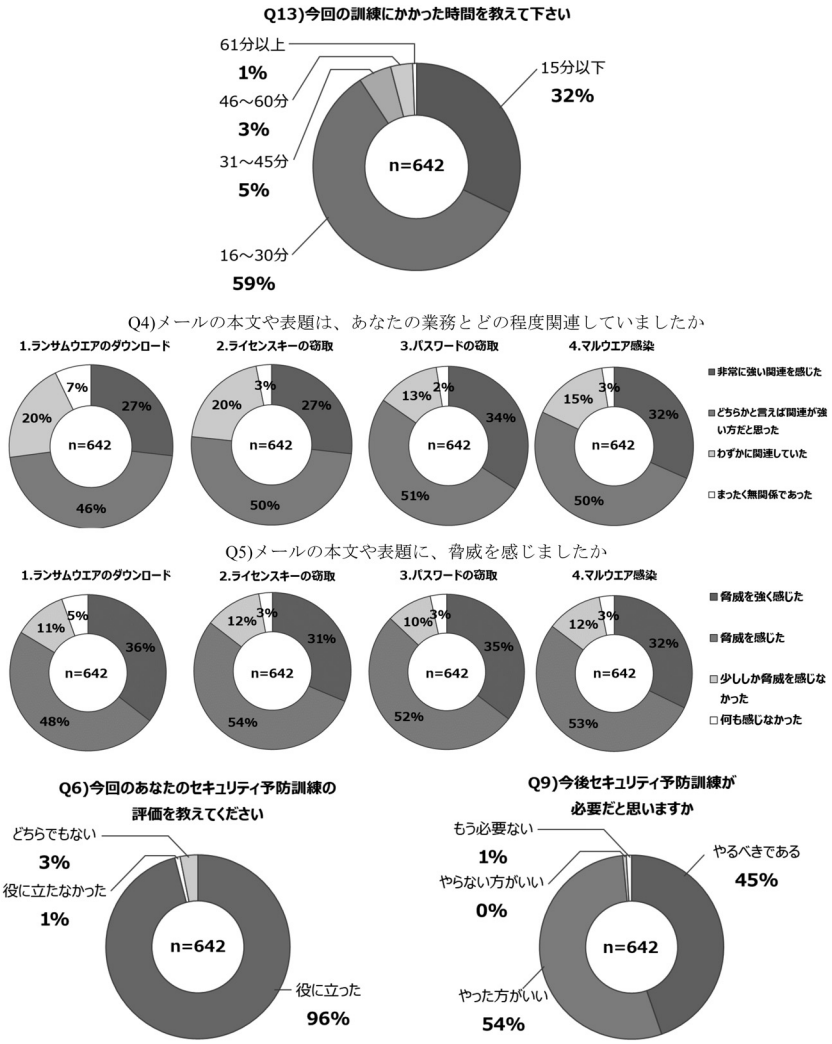

図 9　疑似体験型セキュリティ訓練アンケート結果（抜粋）

能分割を改良することに加え，メール以外の疑似環境も追加できるよう，開発を進めていく．

3.5.2　事後対応策

近年のサイバー攻撃の高度化に伴い，攻撃を完全に予防することは困難になりつつあり，予防だけでなく被害を最小限にとどめるための事後対応策も重要である．本訓練の中で被害に遭わないようにするための注意点やポイントの解説を行っているが，これに加え，異常発生時の対応も体験できる仕組みを検討し，機能として組み込んでいくことを計画している．

3.5.3　多言語化

将来，本訓練の対象を学生にまで広げることを検討している．留学生も訓練を受講することができるよう，多言語対応も今後の課題とする．

4.　おわりに

疑似体験を通したセキュリティ訓練も一度実施しただけでは時間の経過とともにその効果は減少してしまう．サイバー攻撃に関する最新の動向を更新しつつ，継続的にセキュリティ訓練を実施していくことが，大学組織の構成員一人ひとりの情報セキュリティに対するモチベーションを維持し，セキュリティインシデント発生のリスクを低減させるために重要である．

信州大学では，引き続き疑似セキュリティ訓練を活用した構成員のセキュリティ意識向上による「人の強化」に取り組むとともに，規程・運用ルール見直しやセキュリティシステムによる「仕組みによる強化」，インシデント発生時に被害を最小限に抑えるための「対応の強化」を合わせた三つの対策を軸に，情報セキュ

Copyright © by ORSJ. Unauthorized reproduction of this article is prohibited.

リティの強化と維持を進めていく.

謝辞　疑似体験型セキュリティ訓練基盤はベルケンシステムズ鈴木氏に多大なるご協力を得た．また，NICO藤沢氏にプロトタイプの開発を担当していただいた．この場を借りて感謝の意を表す.

参考文献

[1] 独立行政法人情報処理推進機構,「大学におけるウェブメールサービスを狙ったフィッシングメールに注意〜フィッシングの基本の手口を知って，継続的な対策を〜」，https://www.ipa.go.jp/security/anshin/mgdayori20181031.html（2019 年 5 月 23 日閲覧）

 Copyright © by ORSJ. Unauthorized reproduction of this article is prohibited.