国立大学法人　長岡技術科学大学　御中

令和４年度
標的型攻撃メール訓練
結果報告書

令和５年１月

株式会社ＩＴスクエア

目 次

1　実施概要

1.1　目的

標的型攻撃メールに対応できるよう、長岡技術科学大学様（以下、貴学）の教職員のセキュリティ意識の向上を図るとともに、標的型攻撃メールに対する現状の課題・不足点を洗い出す。また、全体で見たときの大きな課題だけではなく、所属別など絞った範囲での課題も洗い出し、今後的確な教育を行うための基礎的資料として活用できるようにすること目的に、標的型攻撃メール訓練を実施する。

1.2　実施期間

	送信日	送信時間	集計期間
第1回訓練	令和4年9月20日	10:00～11:00	令和4年9月27日まで
第2回訓練	令和4年11月21日	10:00～11:00	令和4年11月29日まで

2　訓練概要

2.1　訓練対象者数

	対象者数（名）
第 1 回訓練	517
第 2 回訓練	529

2.2　訓練メールの文面

2.2.1　第 1 回訓練

件名	不正なログインがブロックされました
送信者名	Google システムサポートセンター
送信者アドレス	system-support@ gogle-alert.info
添付ファイル	アクセス詳細.zip(zip の中に「アクセス詳細.docx」)
本文	最近、あなたのパスワードを知っている谁かがあなたの アカウントにログインしようとしたのでブロックしました。 アクセスがあった端末、时间等の情報につきましては、 添付いたしますファイルをご確認ください。 【ファイルパスワード：2022】 今後ともよろしくお願いいたします。 Google システムサポートセンター ※このメールアドレスは送信専用となっており、返信を受け付けません。
備考	【気付きのポイント】 ①「Google システムサポートセンター」は存在しない。 ②本文中に中国語の簡体字が含まれている。 ③システムからの自動返信を装っている。

2.2.2　第 2 回訓練

件名	Re:ミーティング ＩＤの送付
送信者名	田口 宏太
送信者アドレス	Tanaka_Kota@grnail.net
添付ファイル	会議の接続情報.zip(zip の中に「会議の接続情報.docx」)
本文	いつもお世話になっております。 田口です。 本日の Web 会議の接続情報を添付ファイルにて お送りいたします。 ご参加いただきますようお願いいたします。 添付ファイルのパスワードは下記となります。 パスワード：1121 ご確認のほど、宜しくお願いいたします。 // 長岡技術科学大学 総務センター局 田口 宏太 //
備考	【気付きのポイント】 ①件名に「Re:」とつけることで返信であると思わせる。 ②送信者名（田口）と送信者アドレス（Tanaka）で名前が異なる。 ③署名の「総務センター局」は存在しない。

2.3　訓練メール本文中 URL アクセス時の開封時コンテンツ

2.3.1　第 1 回訓練

このURLを開いた行為は、

不審なメールに対する不適切な対応です！！

長岡技術科学大学　情報セキュリティ専門部会　実施

本メールは、標的型攻撃メールの「対応訓練」として送付したものです。

標的型攻撃メールとは、特定の組織から重要な情報を盗むことなどを目的として送り付けられるウイルス付きメールを指します。組織内のたった１人が、標的型攻撃メールの添付ファイルを開封したりリンクをクリックしただけでもウイルスに感染し、機密情報が漏えいする恐れがあります。

以下の２点を熟読し、標的型攻撃メールに対する正しい対応を身に付けてください。

１．この標的型攻撃訓練メールの気付きのポイント

（１）「Google システムサポートセンター」は存在しない。

（２）本文中に中国語の簡体字が含まれている。

（３）システムからの自動返信を装っている。

２．標的型攻撃メールへの対応

（１）実在する組織や団体からのメールであっても、内容が自身に関わりがないなどの違和感がある場合、添付ファイルやＵＲＬをクリックせず、差出人に送信の有無を確認したり、総合情報課事務情報システム係に相談してください。また、同様のケースが発生していないか総合情報課事務情報システム係へ相談することも大事です。

（２）確認の結果、送信の事実がない場合は、該当メールを速やかに削除し、その旨を総合情報課事務情報システム係（joho-kiban@jcom.nagaokaut.ac.jp、内線 9266・9219）に連絡してください。

なお、今回は訓練ですので連絡は不要です。

2.3.2　第 2 回訓練

このURLを開いた行為は、

不審なメールに対する不適切な対応です！！

長岡技術科学大学　情報セキュリティ専門部会　実施

本メールは、標的型攻撃メールの「対応訓練」として送付したものです。

標的型攻撃メールとは、特定の組織から重要な情報を盗むことなどを目的として送り付けられるウイルス付きメールを指します。組織内のたった１人が、標的型攻撃メールの添付ファイルを開封したりリンクをクリックしただけでもウイルスに感染し、機密情報が漏えいする恐れがあります。

以下の２点を熟読し、標的型攻撃メールに対する正しい対応を身に付けてください。

１．この標的型攻撃訓練メールの気付きのポイント

（１）件名に「Re:」とつけることで返信であると思わせる。

（２）送信者名（田口）と送信者アドレス（Tanaka）で名前が異なる。

（３）署名の「総務センター局」は存在しない。

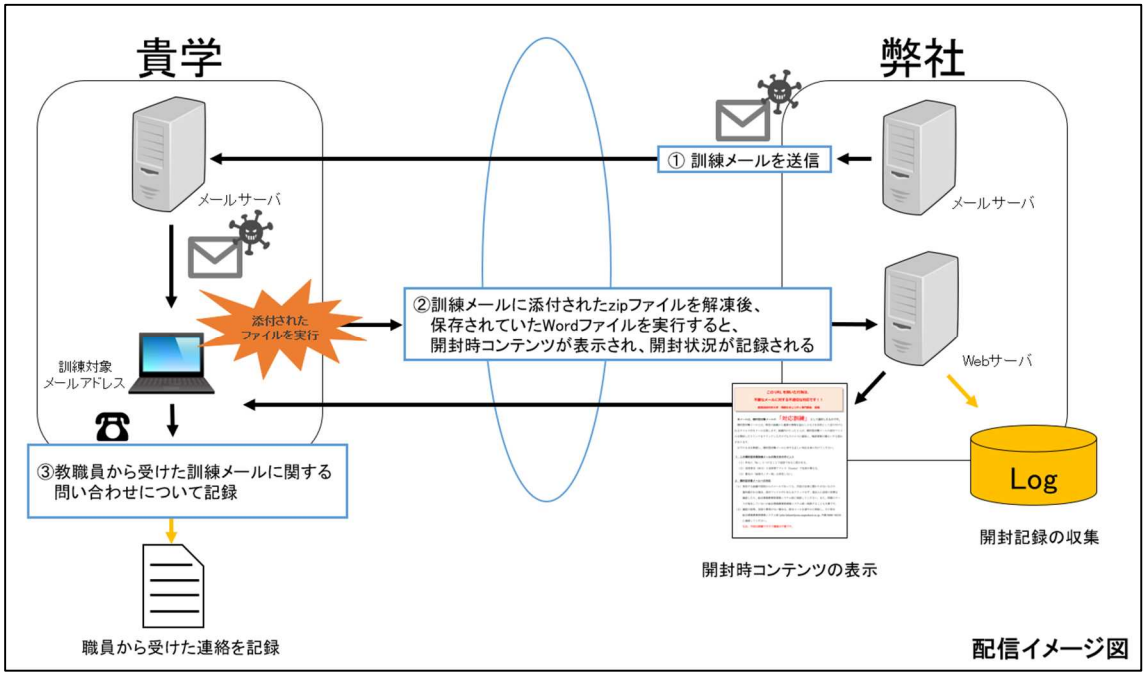
２．標的型攻撃メールへの対応

（１）実在する組織や団体からのメールであっても、内容が自身に関わりがないなどの違和感がある場合、添付ファイルやＵＲＬをクリックせず、差出人に送信の有無を確認したり、総合情報課事務情報システム係に相談してください。また、同様のケースが発生していないか総合情報課事務情報システム係へ相談することも大事です。

（２）確認の結果、送信の事実がない場合は、該当メールを速やかに削除し、その旨を総合情報課事務情報システム係（joho-kiban@jcom.nagaokaut.ac.jp、内線 9266・9219）に連絡してください。

なお、今回は訓練ですので連絡は不要です。

2.4　訓練実施方法



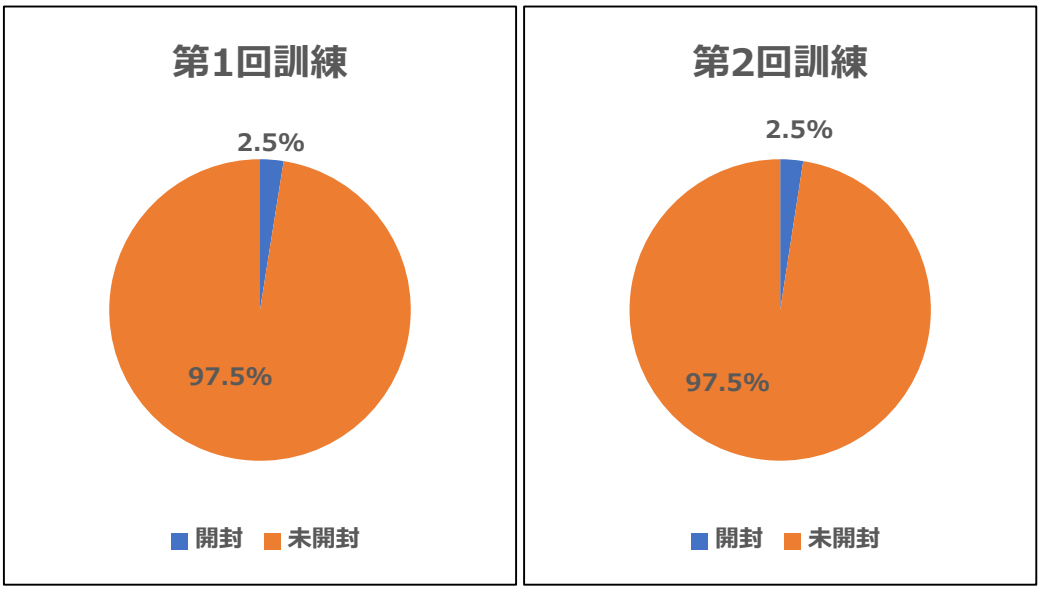
弊社メールサーバより、貴学訓練対象者宛てに訓練メールを送信した。訓練メールに添付された zip ファイルを解凍後、保存されていた Word ファイルを実行（以下、Word ファイルを実行した訓練対象者を「開封者」と表記。）すると、開封時コンテンツが表示されるとともに、弊社集計サーバに開封したというログが記録される。このログを元に開封結果の集計を行った。なお、開封率は以下の計算方法で算出している。

開封率（%）＝開封者数／訓練対象者数×100（%）
※小数点以下第 2 位を四捨五入

3　訓練結果

3.1　全体訓練結果

	対象者数（名）	開封者数（名）	開封率
第 1 回訓練	517	13	2.5%
第 2 回訓練	529	13	2.5%



システムからの通知を装ったメールを使用した第 1 回訓練において、訓練対象の 517 名のうち 13 名(2.5%)が添付ファイルを開封した。

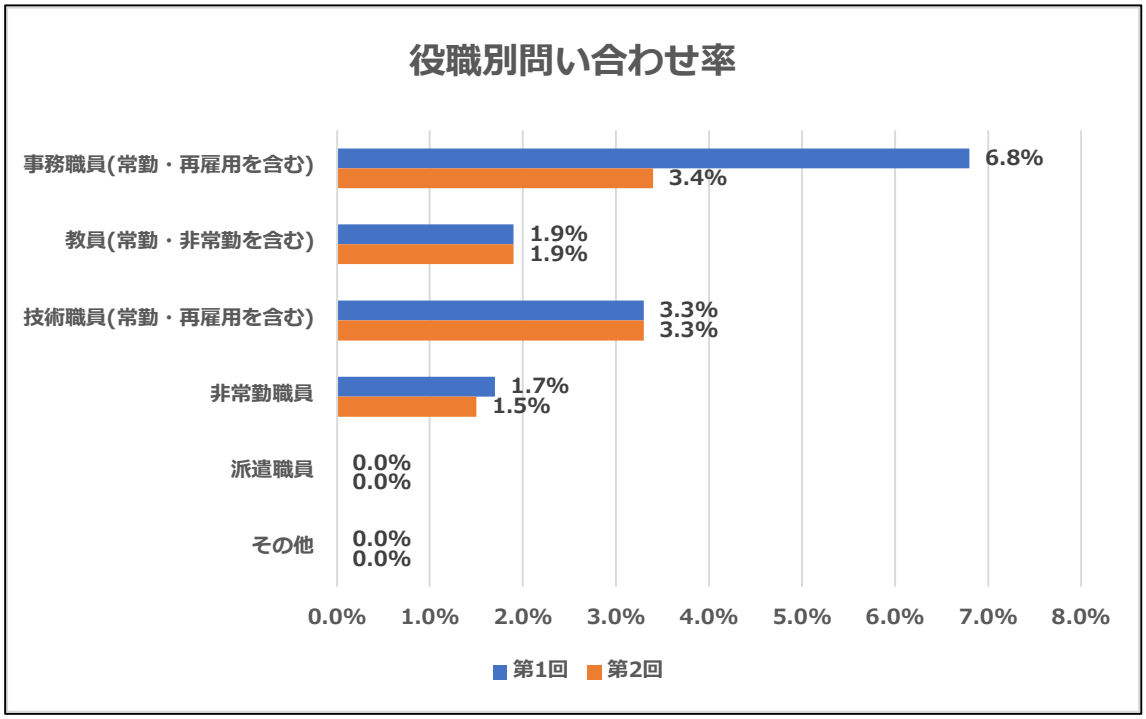
内部関係者から返信を装ったメールを使用した第 2 回訓練において、訓練対象の 529 名のうち 13 名(2.5%)が添付ファイルを開封した。

これは、弊社が昨年度（令和 3 年度）に教育機関を対象に訓練を実施した際の平均開封率 10.4%（添付ファイルまたは URL を開く行為を開封とする）と比べて低い開封率となっている。

3.2　訓練メール受信後の問い合わせ件数

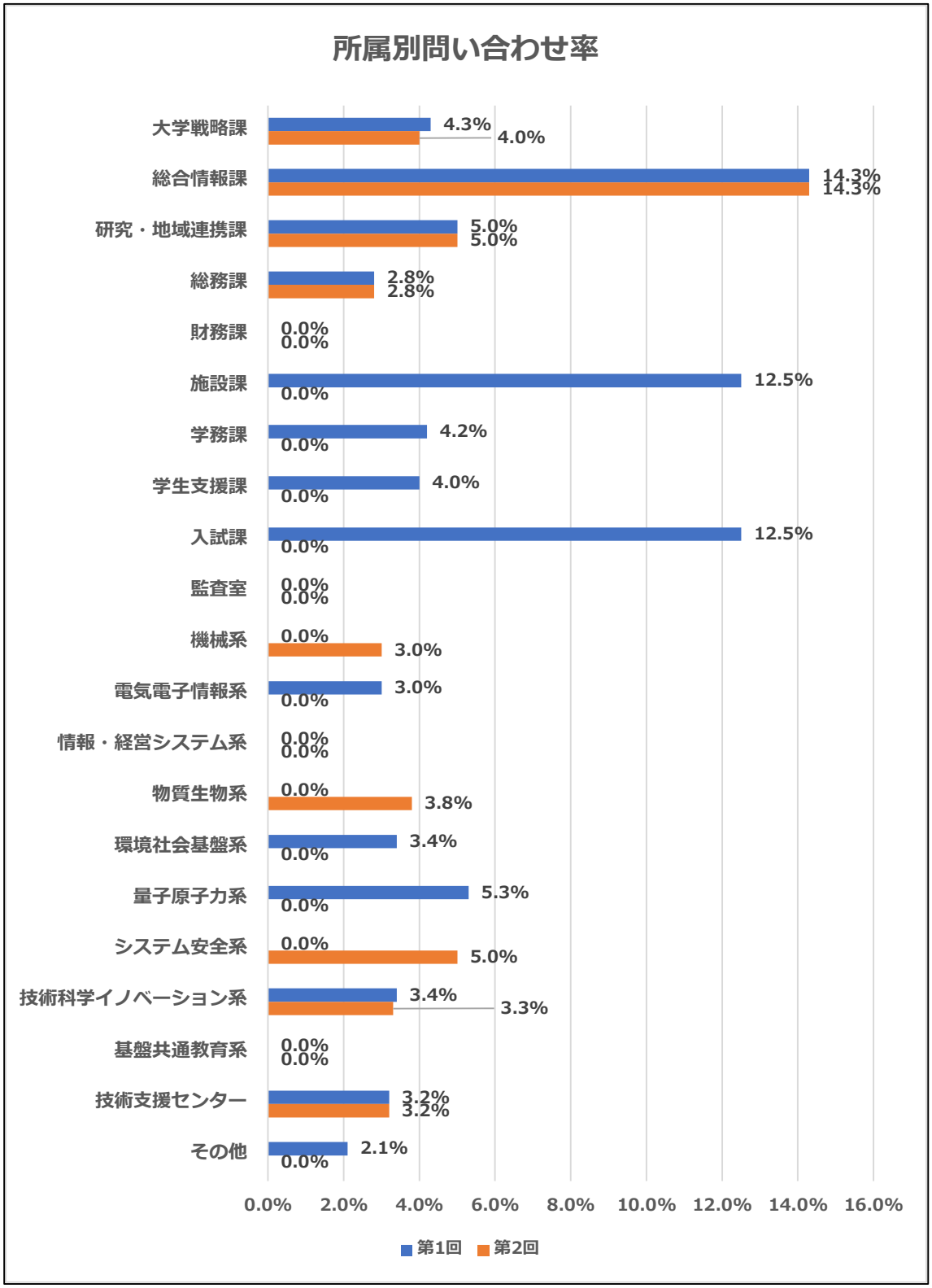
3.2.1　役職別問い合わせ件数

役職	対象者数（名）		問い合わせ件数（名）		問い合わせ率	
	第 1 回	第 2 回	第 1 回	第 2 回	第 1 回	第 2 回
事務職員(常勤・再雇用を含む)	117	118	8	4	6.8%	3.4%
教員(常勤・非常勤を含む)	211	211	4	4	1.9%	1.9%
技術職員(常勤・再雇用を含む)	30	30	1	1	3.3%	3.3%
非常勤職員	121	130	2	2	1.7%	1.5%
派遣職員	12	14	0	0	0.0%	0.0%
その他	26	26	0	0	0.0%	0.0%
計	517	529	15	11	2.9%	2.1%



3.2.2　所属別問い合わせ件数

所属	対象者数（名）		問い合わせ件数（名）		問い合わせ率	
	第1回	第2回	第1回	第2回	第1回	第2回
大学戦略課	23	25	1	1	4.3%	4.0%
総合情報課	14	14	2	2	14.3%	14.3%
研究・地域連携課	20	20	1	1	5.0%	5.0%
総務課	36	36	1	1	2.8%	2.8%
財務課	28	28	0	0	0.0%	0.0%
施設課	8	9	1	0	12.5%	0.0%
学務課	24	24	1	0	4.2%	0.0%
学生支援課	25	26	1	0	4.0%	0.0%
入試課	8	8	1	0	12.5%	0.0%
監査室	2	2	0	0	0.0%	0.0%
機械系	32	33	0	1	0.0%	3.0%
電気電子情報系	33	34	1	0	3.0%	0.0%
情報・経営システム系	24	24	0	0	0.0%	0.0%
物質生物系	50	52	0	2	0.0%	3.8%
環境社会基盤系	29	29	1	0	3.4%	0.0%
量子原子力系	19	20	1	0	5.3%	0.0%
システム安全系	18	20	0	1	0.0%	5.0%
技術科学イノベーション系	29	30	1	1	3.4%	3.3%
基盤共通教育系	16	16	0	0	0.0%	0.0%
技術支援センター	31	31	1	1	3.2%	3.2%
その他	48	48	1	0	2.1%	0.0%
計	517	529	15	11	2.9%	2.1%


所属別問い合わせ率
大学戦略課
4.3%
4.0%
総合情報課
14.3%
14.3%
研究・地域連携課
5.0%
5.0%
総務課
2.8%
2.8%
財務課
0.0%
0.0%
施設課
12.5%
0.0%
学務課
4.2%
0.0%
学生支援課
4.0%
0.0%
入試課
12.5%
0.0%
監査室
0.0%
0.0%
機械系
0.0%
3.0%
電気電子情報系
3.0%
0.0%
情報・経営システム系
0.0%
0.0%
物質生物系
0.0%
3.8%
環境社会基盤系
3.4%
0.0%
量子原子力系
5.3%
0.0%
システム安全系
0.0%
5.0%
技術科学イノベーション系
3.4%
3.3%
基盤共通教育系
0.0%
0.0%
技術支援センター
3.2%
3.2%
その他
2.1%
0.0%
0.0% 2.0% 4.0% 6.0% 8.0% 10.0% 12.0% 14.0% 16.0%
第1回
第2回

4　アンケート結果

対象者にアンケートを実施しその結果を以下に記載する。なお、役職別及び所属別の集計結果は「8　補則」にて記載している。

4.1　アンケート概要

4.1.1　アンケート回答者数

対象者：521 名（第 2 回配信後に在籍している教職員等）
回答者：153 名（回答率：29.4%）

4.1.2　アンケート実施方法

標的型攻撃メール訓練についてより深く分析することを目的とし、貴学のアンケートシステムを利用して対象者に対しアンケートを実施した。なお、回答率は以下の計算方法で算出している。

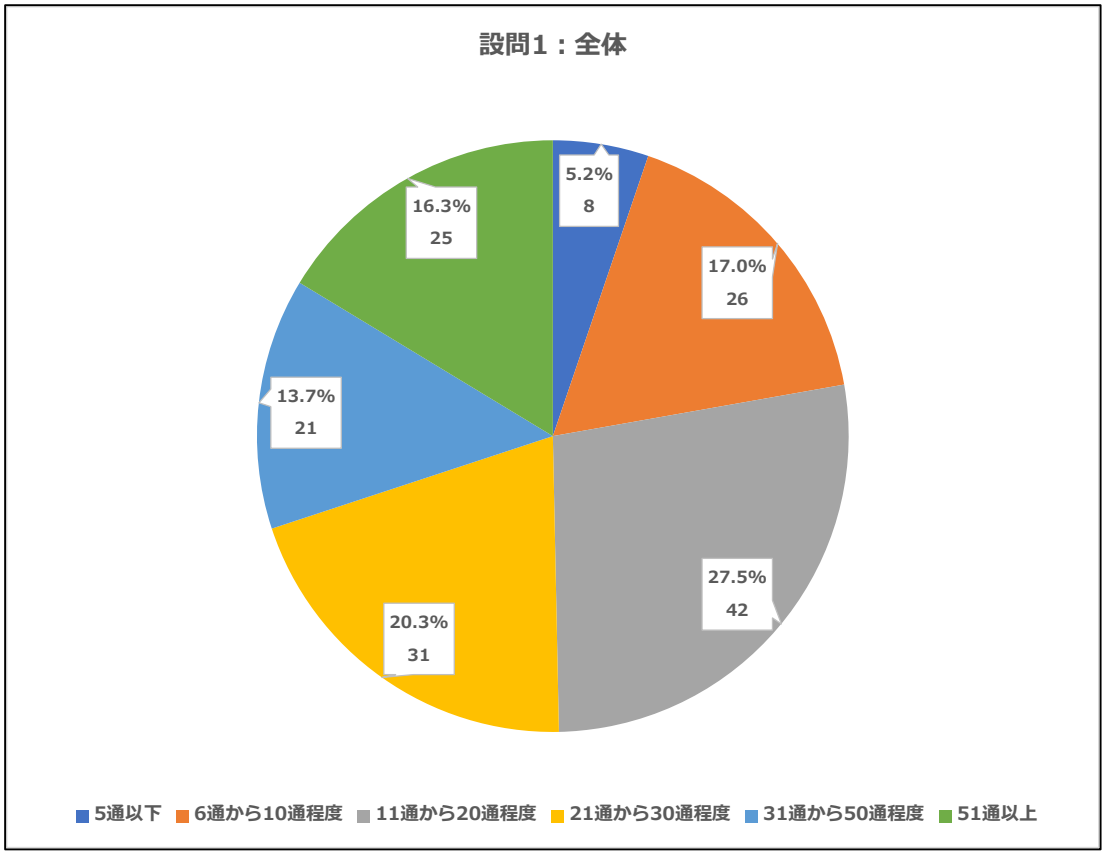
回答率（%）＝回答者数／回答対象者数×100（%）
※小数点以下第 2 位を四捨五入

4.2　アンケート回答

4.2.1　設問 1

一日当たりの平均的なメール受信数として近いものはどれですか。

選択肢	回答者数（名）	回答率
5 通以下	8	5.2%
6 通から 10 通程度	26	17.0%
11 通から 20 通程度	42	27.5%
21 通から 30 通程度	31	20.3%
31 通から 50 通程度	21	13.7%
51 通以上	25	16.3%
計	153	-



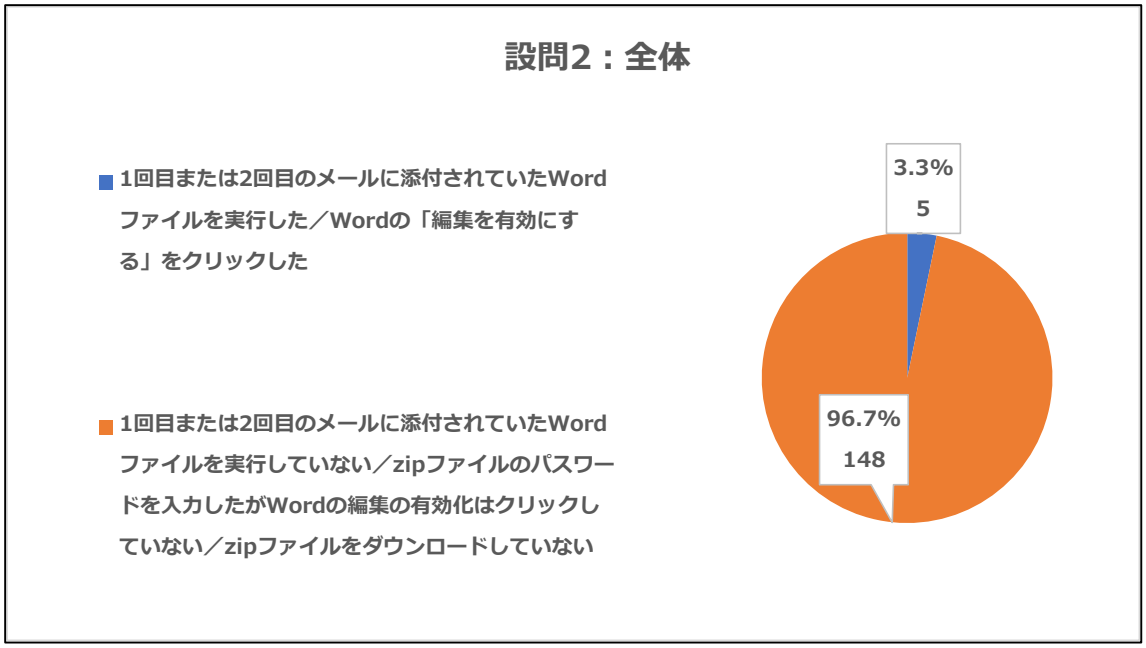
4.2.2　設問 2

本訓練では 9/20（火）と 11/21（月）にそれぞれ以下の 2 件の画像のメールを送信しました。いずれかの訓練メールの添付ファイル（zip）をダウンロードし、Word ファイルを実行しましたか。

【訓練メール 1】送信日 9 月 20 日（火）10:00～11:00
送信者アドレス：system-support@gogle-alert.info
件名：不正なログインがブロックされました

【訓練メール 2】送信日：11 月 21 日（月）10:00～11:00
送信者アドレス：Tanaka_Kota@grnail.net
件名：Re:ミーティング ＩＤの送付

選択肢	回答者数（名）	回答率
1 回目または 2 回目のメールに添付されていた Word ファイルを実行した／Word の「編集を有効にする」をクリックした	5	3.3%
1 回目または 2 回目のメールに添付されていた Word ファイルを実行していない／zip ファイルのパスワードを入力したが Word の編集の有効化はクリックしていない／zip ファイルをダウンロードしていない	148	96.7%
計	153	-

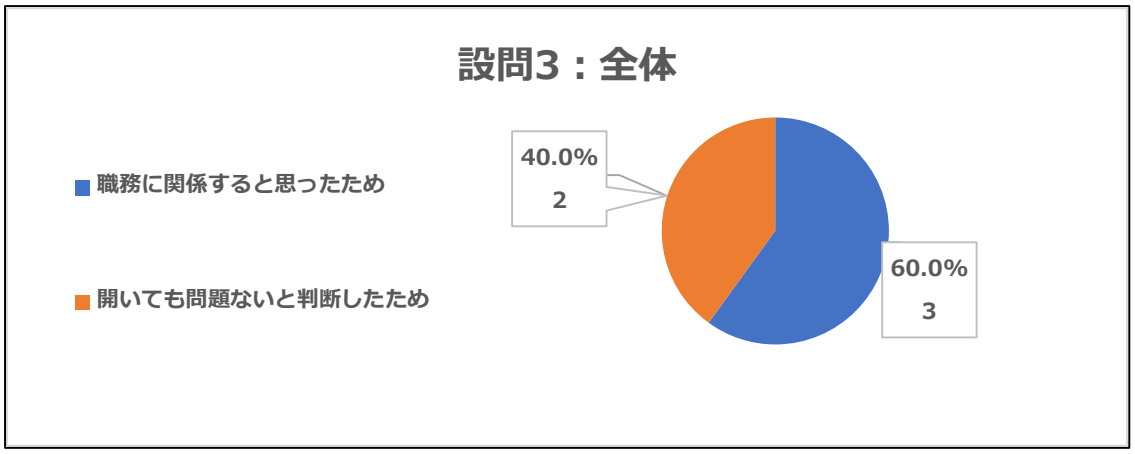


4.2.3　設問 3

【※設問 2 で「添付されていた Word ファイルを実行した／Word の「編集を有効にする」をクリックした」を選択した場合】

訓練メールの添付ファイルを開いた理由として最も近いものはどれですか。

選択肢	回答者数（名）	回答率
職務に関係すると思ったため	3	60.0%
内容を確認し重要だと判断したため	0	0.0%
開いても問題ないと判断したため	2	40.0%
個人的興味でアクセスした	0	0.0%
操作ミスでアクセスした	0	0.0%
訓練メールだとわかったため	0	0.0%
計	5	-

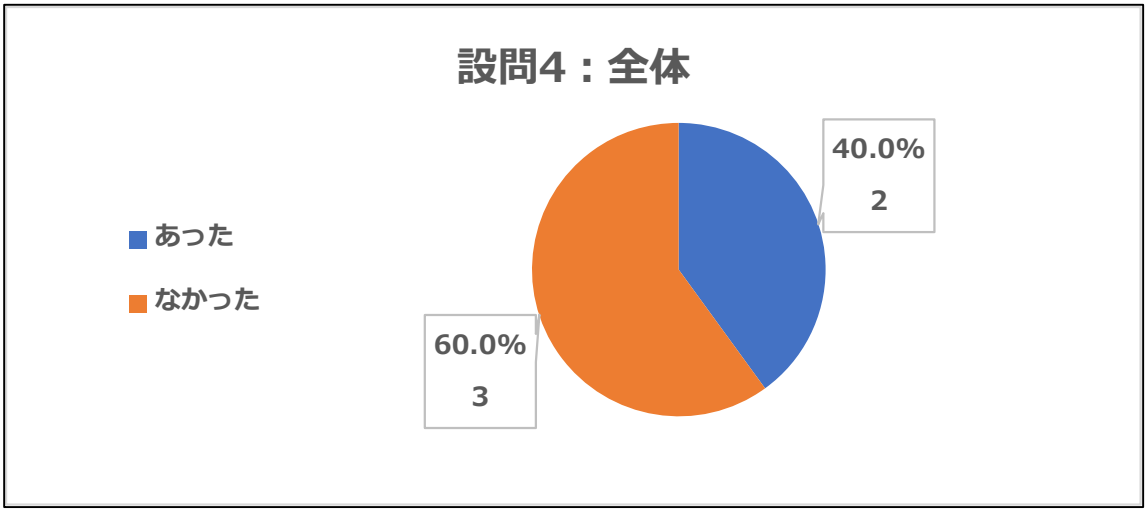


4.2.4　設問 4

【※設問 2 で「添付されていた Word ファイルを実行した／Word の「編集を有効にする」をクリックした」を選択した場合】

訓練メールで不審に感じた点はありましたか。

選択肢	回答者数（名）	回答率
あった	2	40.0%
なかった	3	60.0%
計	5	-

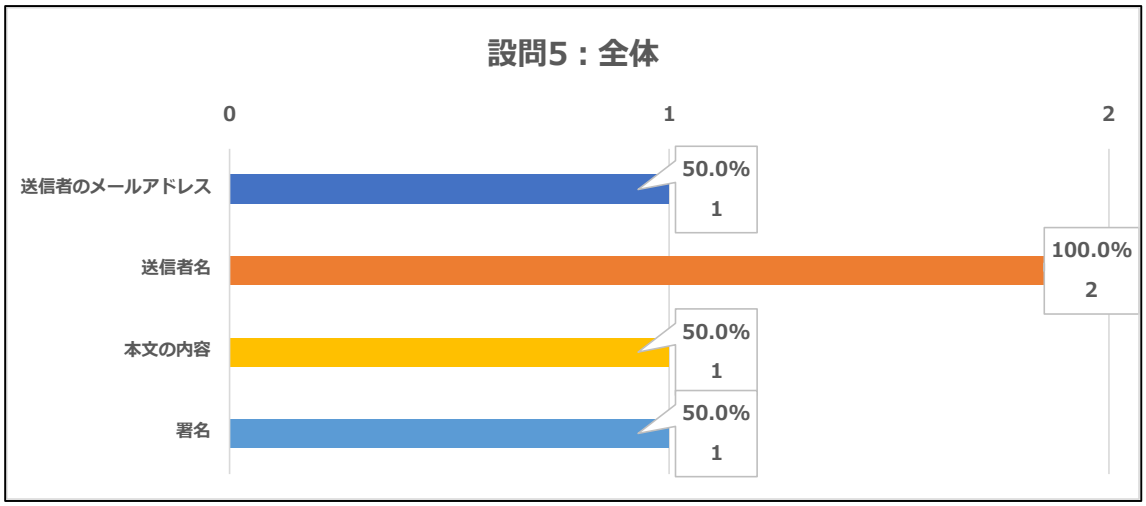


4.2.5　設問 5

【※設問 4 で「あった」を選択した場合】

訓練メールのどの点に不審さを感じましたか。（複数選択可）

選択肢	回答者数（名）	回答率
送信者のメールアドレス	1	50.0%
送信者名	2	100.0%
件名	0	0.0%
本文の内容	1	50.0%
署名	1	50.0%
添付ファイル	0	0.0%
その他	0	0.0%
※延べ回答数合計	5	-
回答者数合計	2	-

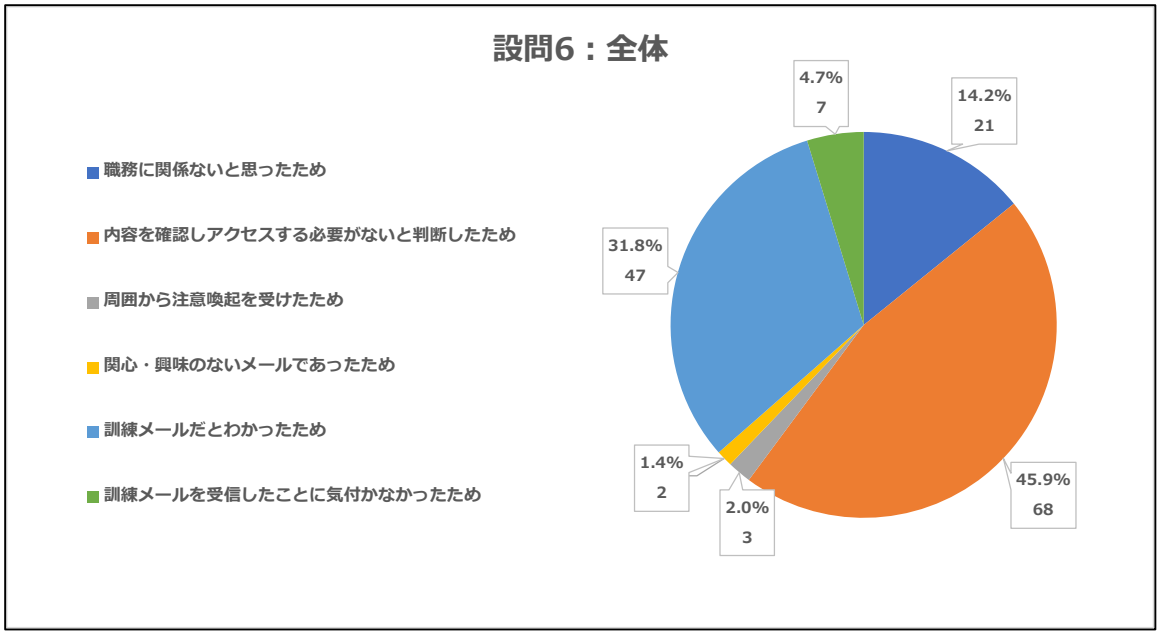


4.2.6　設問 6

【※設問 2 で「添付されていた Word ファイルを実行していない／zip ファイルのパスワードを入力したが Word の編集の有効化はクリックしていない／zip ファイルをダウンロードしていない」を選択した場合】

訓練メール本文中の URL にアクセスしなかった理由として最も近いものはどれですか。

選択肢	回答者数（名）	回答率
職務に関係ないと思ったため	21	14.2%
内容を確認しアクセスする必要がないと判断したため	68	45.9%
周囲からの注意喚起を受けたため	3	2.0%
関心・興味のないメールであったため	2	1.4%
訓練メールだとわかったため	47	31.8%
訓練メールを受信したことに気付かなかったため	7	4.7%
計	148	-

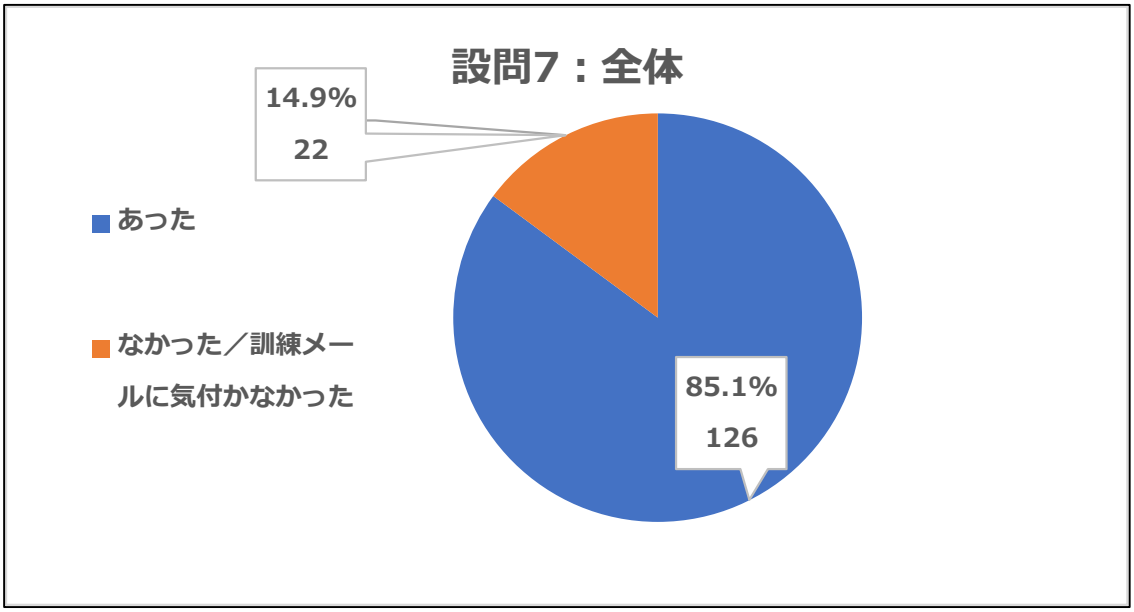


4.2.7　設問 7

【※設問 2 で「添付されていた Word ファイルを実行していない／zip ファイルのパスワードを入力したが Word の編集の有効化はクリックしていない／zip ファイルをダウンロードしていない」を選択した場合】

訓練メールで不審に感じた点はありましたか。

選択肢	回答者数（名）	回答率
あった	126	85.1%
なかった	22	14.9%
計	148	-

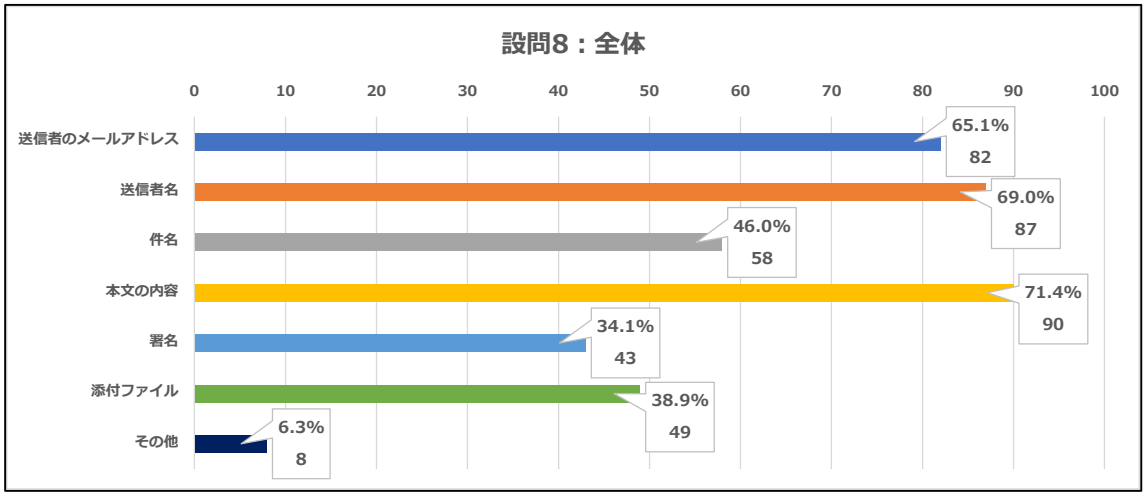


4.2.8　設問 8

【※設問 7 で「あった」を選択した場合】

訓練メールのどの点に不審さを感じましたか。（複数選択可）

選択肢	回答者数（名）	回答率
送信者のメールアドレス	82	65.1%
送信者名	87	69.0%
件名	58	46.0%
本文の内容	90	71.4%
署名	43	34.1%
添付ファイル	49	38.9%
その他	8	6.3%
※延べ回答数合計	417	-
回答者数合計	126	-



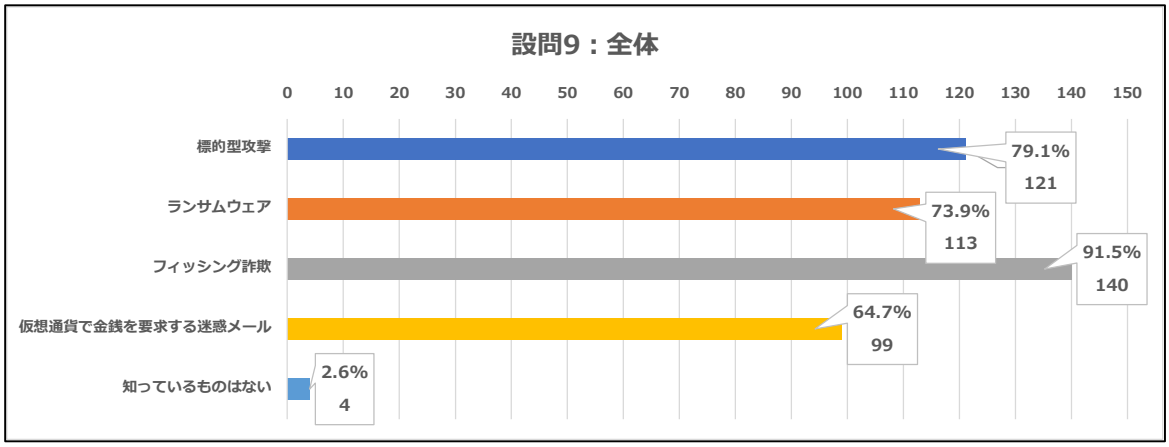
設問８で「その他」を選択いただいた職員の回答は下記となります。

項番	回答（原文ママ）
1	全体的にひっかけポイントが多くクオリティが高いので、不審メールと感じた
2	全てが不審であった、ばればれである
3	所属が当学にないものだった
4	職員名簿を確認し偽物と判断し、メールを直ちに削除した
5	最終的にヘッダファイルにて確認
6	不正ログインをされる心当たりがない。会議そのものに心当たりがなく、事務職員に対して届くメールの文面としては不自然だった。外部に公表されていて業務で日常的に使う係メールではなく、ほとんど表に出していないはずの個人アドレス宛に届く時点で不自然に思った
7	職務と関係のない内容が怪しかったため
8	Gmail のセキュリティ機能で警告が表示されたり自動で迷惑メール判定されたりしていました
計	８名

4.2.9　設問 9

次のインターネット上での攻撃・脅威について、概要を知っているものをすべて選択してください。(複数選択可)

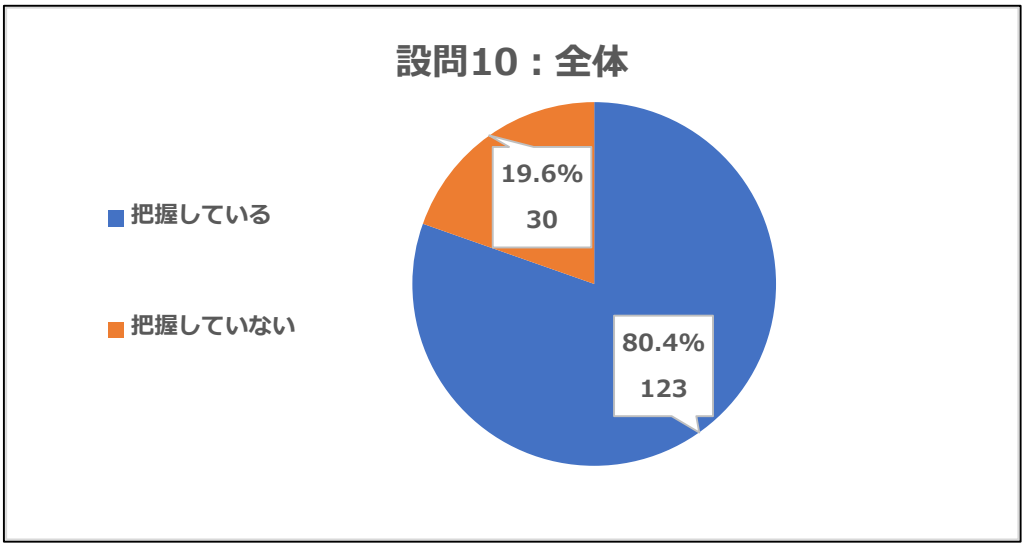
選択肢	回答者数（名）	回答率
標的型攻撃	121	79.1%
ランサムウェア	113	73.9%
フィッシング詐欺	140	91.5%
仮想通貨で金銭を要求する迷惑メール	99	64.7%
知っているものはない	4	2.6%
※延べ回答数合計	477	-
回答者数合計	153	-



4.2.10　設問 10

不審なメールの URL や添付ファイルを開いてしまった場合の対応手順や報告先を把握していますか。

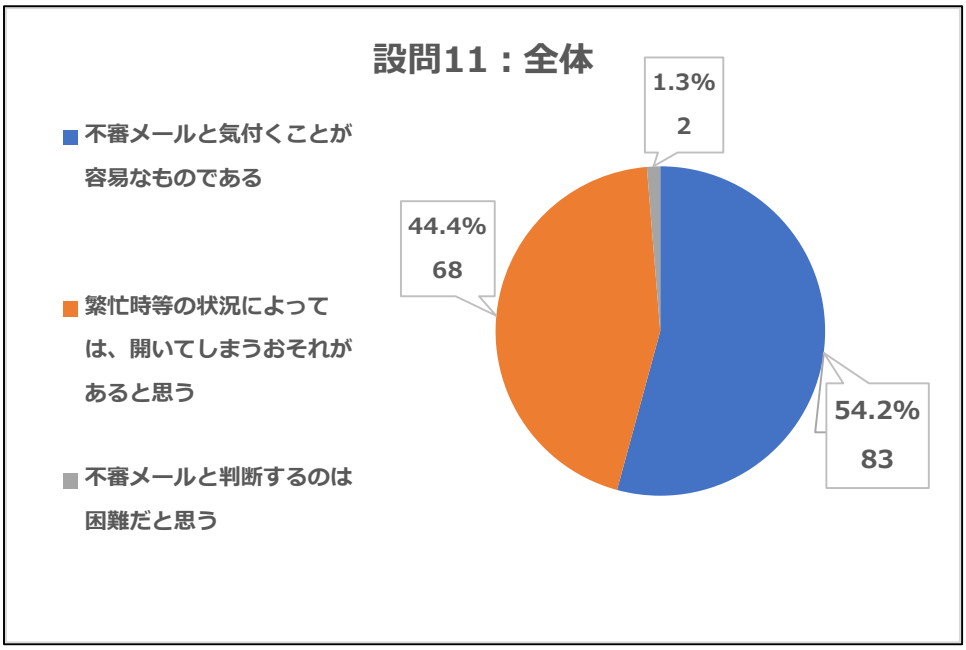
選択肢	回答者数（名）	回答率
把握している	123	80.4%
把握していない	30	19.6%
計	153	-



4.2.11　設問 11

訓練メールの難易度について、どのように感じましたか。

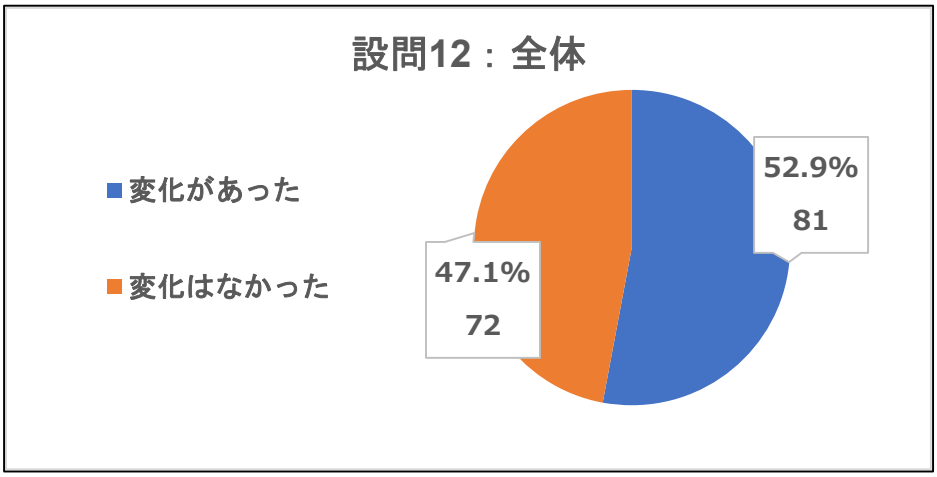
選択肢	回答者数（名）	回答率
不審メールと気づくことが容易なものである	83	54.2%
繁忙時など状況によっては、 開いてしまうおそれがあると思う	68	44.4%
不審メールと判断するのは困難だと思う	2	1.3%
計	153	-



4.2.12　設問 12

本訓練を体験してみて、あなたの情報セキュリティに対する意識や理解度に変化はありましたか。

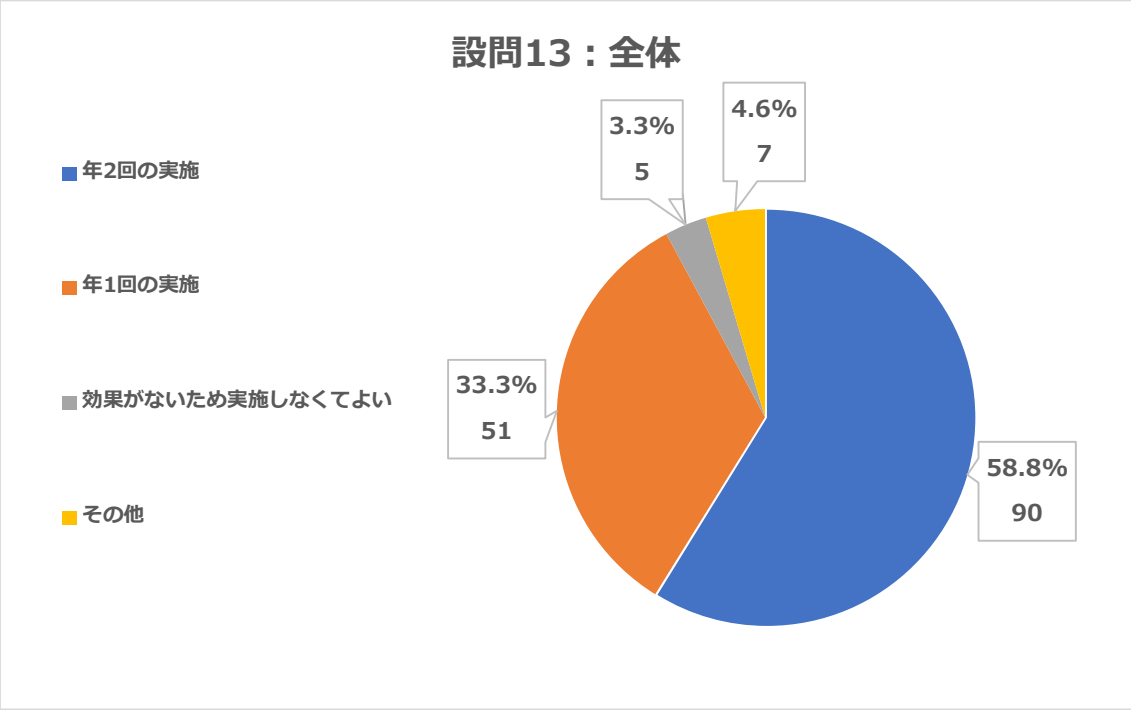
選択肢	回答者数（名）	回答率
変化があった （意識または理解度が高まった）	81	52.9%
変化はなかった	72	47.1%
計	153	-



4.2.13　設問 13

標的型攻撃メール訓練の実施について、学習効果がある頻度はどれぐらいだと考えますか。

選択肢	回答者数（名）	回答率
年 2 回の実施	90	58.8%
年 1 回の実施	51	33.3%
効果がないため実施しなくてよい	5	3.3%
その他	7	4.6%
計	153	-



4.2.14　設問 14

本訓練全体に関する御意見・御要望がありましたら、記入してください。

項番	回答（原文ママ）
1	セキュリティ確保と職務時間確保の合理的バランスを考慮してください
2	少々難易度を高めたほうが良いかと思います
3	怪しいメールは開かないという第一原則を習得できるため、訓練としては評価できる。加えて不審メールを発見した後の行動についても訓練に入れたほうが良いと考える。不審メール発見⇒開かないだけでなく、適切な部署へ報告するというフローを加えてはどうか。現状のままだと訓練だろうから報告しなくてもよいという層が出てきそうである
4	教職員だけでなく、学生も対象として訓練メールを送ってみてはどうでしょうか。学生の方が誤ってファイルを開いてしまう可能性は高いかもしれません。特に留学生の場合、日本語の文章が不自然であったも、不正なメールと気づかずにファイルを開いてしまう恐れがあります
5	これらメールは gmail にて迷惑メールにならないのか
6	大変参考になりました。自分は大丈夫と思っていたのに、こんなに簡単に引っ掛かったことに驚いています。今後も、このような実施型の注意喚起をお願いしたいです
7	実際にクリックした割合などを公表して欲しい。「結構みんな引っかかるんだ～」と変な安心が生まれる可能性もありますが
8	今回の訓練メールは「迷惑メール」に入っていて全く気づくことはありませんでした
9	受信したこと自体に気づきませんでした。確認したところ、11 月分は GMail で自動的に「迷惑メール」として隔離されていました。9 月分は、時間経過で削除されたのか、検索しても出てきませんでした
10	この様な「訓練」は１００％無駄です。こんなものに引っかかる人は、訓練などしてもしなくてもどうせ引っかかります。こんなことを「訓練はしていました」という「情報漏洩が起きた際の事務的な言い訳・アリバイ作り」のためにやるくらいなら、まずは事務局が「HTML 形式のメールを送信しない、テキスト形式で送信すること」という学内ルールを守るべきではないですか？このアンケートも含めて、アンケートに次ぐアンケート、講演会に次ぐ講演会、予算消化のためなのか短期間に次々と全部の部署があれやれこれやれ、そんな時間などあるわけがありません。事務局お得意の all_nut 送信での「全教職員にお送りしています」というメールも乱発するようになりましたが、情報セキュリテ

項番	回答（原文ママ）
	ィ的に極めてまずい仕事のやり方ではないでしょうか？担当部局には強く自省を求めます
11	特に 2 番目の訓練メールでは学内のユーザが乗っ取られたようにも見えるため念のため調査と連絡をしなければならず，不要な時間を費やしました．実際に訓練メールを送信するより，危険なメールの複数事例を講習するなどの方が役に立つような気がします．多くのユーザが使っている Thunderbird や Gmail など MUA の実際の画面を実演しながら対応方法を説明しても良いと思います
12	差出人が正しいメールでも学内インフォを経由しない学外 URL への誘導や不自然な添付ファイルは開かないようにしています。最近は減りましたが事務局からの依頼メールで外部のアンケートサイトなどに"直接"誘導するのは控えるようにお願いします
13	今回のメールは比較的不審なメールだとわかりやすかったと思いますが、最近はなかなか巧妙な内容のメールが届くこともあるので、もう少し難易度をあげてもよいかと思います
14	このメールの存在に全く気付きませんでした。あるいは覚えていない
15	訓練とは思わず、普通の迷惑メールと思っていた。(その割には「長岡技術科学大学」と入っていたので手が込んでいるな、と思った）訓練と知って驚いた
16	関連する講演を時間が空いた時に受講できるようにしていただきたい。特に、どのようなメールが届くのかという例示をしていただきたい
17	署名の「総務センター局」に違和感を感じたものの、ひとまず内容を確認してみようとファイルを開いてしまい、まんまと騙されました。この訓練を通して危機意識が高まりました。改めて注意しなければならないと思いました
18	本件は防災訓練のような位置づけですので，本学構成員が忘れないように意識づけするため定期的に実施したほうが良いと考えます．本学でもランサムウェア被害や，クレジットカードを入力してしまった事例などはありますので，添付ファイルを開いてしまった構成員に向けて,「過去にこのような被害が起きている」といったホラーストーリーを明確に提示する必要があるかと思います．本学の訓練はやりっぱなしのところがあって，PDCA サイクルがうまく回っていないようにも感じるので，最後の教育の部分にもう一工夫があると良いかと思っています
計	18 名

5　訓練結果まとめ

5.1　開封結果について

システムからの通知を装ったメールを使用した第 1 回訓練において、訓練対象の 517 名のうち 13 名（2.5%）が添付ファイルを開封した。また、内部関係者から返信を装ったメールを使用した第 2 回訓練において、訓練対象の 520 名のうち 13 名（2.5%）が添付ファイルを開封した。これは、弊社が昨年度（令和 3 年度）に教育機関を対象に訓練を実施した際の平均開封率 10.4%（添付ファイルまたは URL を開く行為を開封とする）と比べて低い開封率となっている。

5.2　訓練メールに関する問い合わせについて

訓練メールに関する問い合わせ率については、第 1 回訓練が 2.9%、第 2 回訓練が 2.1%であった。また、役職別の割合は全て 10%を下回る結果となった。所属別の割合を確認しても問い合わせを行った職員は少なく、第 1 回第 2 回ともに 10%を超えている所属は 1 所属のみとなっている。

不審メール対応手順や報告先の理解度についてアンケート（設問 10）で確認を行った。回答は「把握している」が 80.4%となっており、問い合わせ率と大きな差異があることがわかった。

5.3　訓練メールの添付ファイル開封及び未開封理由について

訓練メールの添付ファイルを開封及び未開封理由についてアンケート（設問 3、設問 7）で確認を行った。

開封した理由として「職務に関係すると思ったため」が 60.0%、「開いても問題ないと判断したため」が 40.0%であった。また、訓練メールで不審に感じた点があったと回答した 40.0%の開封者に、どの点に不審さを感じたかについてアンケート（設問 5）で確認を行った。開封者の不審に感じた点として多かった回答として「送信者名」が 100.0%、「送信者のメールアドレス」が 50.0%、「本文の内容」が 50.0%、「署名」が 50.0%、であった。

未開封者の未開封理由として多かった回答は「内容を確認しアクセスする必要がないと判断したため」が 45.9%、「訓練メールだとわかったため」が 31.8%、「職務に関係ないと思ったため」が 14.2%であった。また、訓練メールで不審に感じた点があったと回答した 85.1%の未開封者に、どの点に不審さを感じたかについてアンケート（設問 8）で確認を行った。「本文の内容」が 71.4%、「送信者名」が 69.0%、「送信者のメールアドレス」が 65.1%であった。

開封者、未開封者ともに「本文の内容」や「送信者名」を不審に感じた割合が高い結果となっている。開封者の理由として「職務に関係すると思ったため」と回答

した割合が高く、組織関係者になりすましたメールには特に注意が必要である。

訓練メールの難易度についてどのように感じたかアンケート（設問 11）で確認を行った。「不審メールと気づくことが容易なものである」と回答した割合は 54.2%となっており、パスワード付き zip ファイルが添付されているメールは比較的気づきやすかったのではないかと考える。しかし、そのようなメールでも「繁忙時など状況によっては、開いてしまうおそれがあると思う」と回答した割合は 44.4%いることから、業務状況によっては開封する可能性を感じていることがわかった。

5.4　インターネット上での攻撃・脅威の理解度について

インターネット上での攻撃・脅威の理解度についてアンケート（設問 9）で確認を行った。全ての攻撃・脅威について 50%以上理解しており、「フィッシング詐欺」が 91.5%、「標的型攻撃」が 79.1%、「ランサムウェア」が 73.9%、「仮想通貨で金銭を要求する迷惑メール」が 64.7%であった。昨今は、サイバー攻撃による被害や関連したニュースを見る機会が増えていることもあり割合が高くなっていると考える。

5.5　訓練体験後の情報セキュリティに対する意識変化について

本訓練を体験して、情報セキュリティに対する意識や理解度に変化があったかアンケート（設問 12）で確認を行った。「変化があった（意識または理解度が高まった)」が 52.9%となっており、訓練を通じておよそ半数の訓練対象者が情報セキュリティに対する意識や理解度が高まったことがわかった。

6　今後の課題及び対応策

6.1　不審メール受信時の情報共有

標的型攻撃メールなどの不審メールは、標的とする組織の複数のメールアドレスに届くことが多いという特徴がある。そのため、不審メールを発見した場合、自分に届いたメールを削除するのみでは、別の部署で被害が発生する可能性もあるため対策として不十分であるといえる。このような被害を防ぐためにも、不審メールを受信した際の連絡体制を教職員が理解していることが必要になる。

本訓練においては 80.4%の対象者が不審メールの対応手順や報告先を把握しているにも関わらず、役職別の割合は全て 10%を下回る結果となった。所属別の割合を確認しても問い合わせを行った職員は少なく、第 1 回第 2 回ともに 10%を超えている所属は 1 所属のみとなっている。

対応策として、不審メールの受信時には情報セキュリティ担当部署へその旨を連絡するとともに周囲の教職員と情報共有を行うといった連絡体制や、マルウェア感染時のリスクについて周知徹底を図ることを推奨する。また、教職員から報告のあった不審メール情報については随時、組織内メーリングリストや掲示板で通知を行うことで被害の拡散防止と予防が可能となる。

6.2　不審メールを見分ける判断力

標的型攻撃メールなどの不審メールに使用される添付ファイルや URL には最新のウイルス対策ソフトで検知できない、いわゆる「ゼロデイ」脆弱性が利用される場合がある。ウイルス対策ソフトによる防御は、マルウェアの巧妙化に対して後追いであるため、教職員への教育などにより意識を啓発することの被害防止効果は以前より高まっており、一人一人の不審メールを見分ける判断力が被害発生を大きく左右する要素となる。不審メールを開封しないことが標的型攻撃メールに対する最も有効な防御策になる。

第 2 回の訓練メールのように内部の関係者を装ったメールの場合、注意していないとうっかり開いてしまうことも考えられる。メールに添付ファイルがある場合、そのファイルは信頼できるものか、自分に必要なファイルなのかを開封する前に必ず確認することが大切である。

今回の訓練では添付ファイルを用いたものであったが、それ以外にも不審メールは存在する。不審メールの見分け方について情報セキュリティ研修の対象者及び受講機会の拡充を行っていくことを推奨する。

不審メールを判断する際の着眼点を以下に示す。

不審メールの着眼点	
メールの内容	・知らない人からのメールだが、開封せざるを得ない内容 【例】 ①新聞社・出版社からの取材申込・講演依頼 ②就職活動に関する問い合わせ・履歴書の送付 ③製品やサービスに対する問い合わせ・クレーム ④システムや端末のエラー通知
	・誤って自分宛に送られたメールのようだが、興味をそそられる内容 【例】 ①議事録・演説原稿などの内部文書送付 ②訪問や打合せに関する日程調整の連絡
	・組織全体への案内 【例】 ①人事情報 ②新年度の事業方針 ③資料の再送、差し替え ④製品、サービスの不具合や脆弱性情報
	・ID やパスワードなどの入力を要求するメール 【例】 ①メールボックス容量オーバーの警告 ②銀行からの登録情報確認
送信者	・フリーメールアドレスからの送信 ・差出人のメールアドレスとメール本文の署名に記載されたメールアドレスが異なる
メール本文	・言い回しが不自然な日本語 ・日本語では使用されない漢字（繁体字、簡体字）カタカナ ・正式名称を一部に含むような不審 URL ・HTML メールで、表示と実際の URL が異なるリンク ・署名の記載内容がおかしい、該当部門が存在しない

7　総評

今回の訓練では第 1 回、第 2 回ともに開封率が 2.5%となっており、弊社が昨年度（令和 3 年度）に教育機関を対象に訓練を実施した際の平均開封率 10.4%（添付ファイルまたは URL を開く行為を開封とする）と比べて低い開封率となった。また、アンケート結果からインターネット上での攻撃・脅威について理解度が高く、セキュリティに関する知識があることを確認できた。

貴学の課題としては、不審メールに対する対応が挙げられる。80.4%の対象者が不審メールの対応手順や報告先を把握しているにも関わらず、役職別の割合は全て 10%を下回る結果となった。所属別の割合を確認しても問い合わせを行った職員は少なく、第 1 回、第 2 回ともに 10%を超えている所属は 1 所属のみとなっている。また、第 1 回訓練で訓は見られなかったが、内部関係者を装った配信を実施した第 2 回訓練では、訓練メールに対する返信が 4 件あり、4 件とも差出人に訓練対象者の本名が表示されていた。また、その内の 3 名のメールには署名が記載されており、対象者の所属情報を返信メールから入手することができた。不審メールに対する返信は、更なる標的型攻撃につながる可能性があるため、返信はしないようお願いする。昨今の不審メールには、関係者になりすましたり、返信を装うといったメールが確認されている。そういったメールには、本文を確認するだけでなく送信者のメールアドレスが信頼できるものかを確認することも必要となる。

不審メールを「開かない（添付ファイルまたは URL）」、「気付いたら担当部署に連絡する（開いてしまった場合も同じ）」「怪しいメールには返信をしない」ということを訓練などの教職員教育により浸透させること、集合研修や資料配布で不審メールを見分ける判断力を培うなどの取り組みを、継続して実施していくことが推奨される。

参考情報

今回の訓練では Word ファイルにパスワードを設定し zip ファイル形式で配信を実施した。添付されているファイルを開いた際に「保護ビューの設定」をしていれば「編集を有効にする」が表示されと思う。しかし設定をしている場合でも、zip ファイルを開くために使用するアプリケーション※[1]や Windows のデフォルトの機能等による影響で表示されない場合がある。悪意のあるマクロが仕掛けられた添付ファイルを開いた際に「編集を有効にする」等のメッセージが出ない場合、即座にマクロが実行されてしまう危険があるため設定されていることをご確認ください。

※[1]「7-zip」のバージョン 22.00 以前で zip を展開した人は「編集を有効にする」が出ない可能性があります。
（https://news.mynavi.jp/techplus/article/20220624-2376319/）

以上