実践報告

2023年度標的型攻撃メール訓練実施報告

学術情報事務局情報推進グループ　川　邉　　剛

概要

関西大学では、2022年度から標的型攻撃メール訓練を実施している。前回（2022年度）は事務職員を対象にメール訓練を実施し、今回（2023年度）は大学教員及び事務職員に対象を広げてメール訓練を実施した。本稿では、今回のメール訓練及びアンケート結果について紹介する。

1　はじめに

2022年、関西大学は DX 推進計画の一環として、DX 情報セキュリティプロジェクトにおいて、関西大学 CSIRT[1)]（以下、CSIRT）を発足させた。CSIRT は、IT 政策専門部会の下で CISO[2)]（IT センター所長）をリーダーとし、IT センター副所長、学術情報事務局長、学術情報事務局次長（IT 担当）、総務課長、法務課長、学長課長、情報推進グループ長、情報基盤グループ長をメンバーとしている。

CSIRT の主な役割は、危機管理責任者や事案担当組織からの情報セキュリティインシデントに関する相談や被害報告を受け、その状況を把握・分析することを担っている。また、平時の活動として情報セキュリティ向上のための施策の検討および実施を行っており、その一環として、標的型攻撃メール訓練（以下、メール訓練）を実施しており、2022年度は事務職員を対象に、2023年度は大学教員および事務職員を対象に訓練を実施した。

本稿では、2023年度に実施された大学教員および事務職員を対象としたメール訓練とそのアンケート結果について紹介する。

2　メール訓練概要

本メール訓練は、セキュリティ対策ソフトでの防御が難しい標的型攻撃への啓発訓練として、模擬標的型攻撃メール（以下、模擬メール）を送付し、本訓練を通じて実践的な模擬体

1）Computer Security Incident Response Team
2）Chief Information Security Officer

験を提供することにより、実際に攻撃者が利用する可能性のある手法や、それに対する適切な対応策についての理解を深め、標的型攻撃メールに対する認識を高めることで、情報漏洩などのリスクを減らし、本学の構成員の情報セキュリティ意識を高めることを目的としている。

2022年度に実施した事務職員を対象としたメール訓練が有意義だったことを受け、IT 政策専門部会において、情報セキュリティの啓発活動としてのメール訓練対象者を大学教員および事務職員に拡大することが提案された。その後、関連する各種会議にて報告および検討が行われ、2023年度メール訓練を実施することとなった。

メール訓練の内容やスケジュールの検討については、メール訓練対象者を大学教員および事務職員に広げるにあたり、CSIRT 会議及び IT センター所員会議で意見交換や提案を受けながら、前回のメール訓練の文面およびアンケート内容を見直し、昨年同様に外部のメール訓練サービスを利用した。

3　メール訓練実施方法

3.1　メール訓練対象者数

役員、専任職員、大学教員（専任及び専任に準ずる大学教育職員）の計1481名をメール訓練対象者とした。

3.2　模擬メール文面

2022年に警察庁、文部科学省、内閣サイバーセキュリティセンターより発出「学術関係者・シンクタンク研究員等を標的としたサイバー攻撃について（注意喚起）」[1] を参考に、模擬メールの文面は、文中に模擬サイトへの URL リンクを記載し、学内関係部署からの取材を装った文面を作成した。

また、日本年金機構の不正アクセスによる情報流出事案に関する調査結果報告[2] によると、文面中に担当部署に実在する職員の苗字が記載されていたことから、模擬メールの文面中に宛名として名前を差し込むこととした。

なお、模擬メールの文面は、実際の攻撃に悪用されるリスクを考慮して、本稿では掲載を差し控えることとする。

3.3　メール訓練実施手順

メール訓練の実施にあたっては、1. 事前啓発、2. 事前テスト（メール送信テスト）、3. メール訓練本番、4. 事後のアンケート実施の順に行い、メール訓練実施日を、日本政府が主導するサイバーセキュリティ月間内とした。

1．事前啓発

事前啓発として、資料「標的型攻撃メールの見分け方」（38ページ A）を作成した。この資料には、今回模擬メールの文面の基となった「関係者からの取材の依頼を偽装しているケース」を例として記載している。2024年 1 月11日には、本学の構成員向けポータルサイト（インフォメーションシステム）において、標的型攻撃メールに関する注意喚起とともに本資料を参考資料として掲載した。

2．事前テスト（メール送信テスト）

メール訓練本番時に模擬メールが各種セキュリテイ装置でブロックされたり、迷惑メールにならないようにするため、ファイアウォールやメールサーバ等へメール訓練サービス提供元の IP アドレスや From 情報をもとに設定変更を実施した。メール送信テストでは、CSIRT メンバーの協力を得ながら、メール訓練本番と同様の模擬メールをメンバー宛に送信及び確認テストを繰り返し行い、訓練本番の際に訓練対象者に届くよう確認した。

3．メール訓練本番

日本政府が主導するサイバーセキュリティ月間中にあたる2024年 2 月20日㈫にメール訓練を開始した。メール文面中に記載の URL リンクから模擬サイトにアクセスがあった場合には、メール訓練の趣旨と対処方法が表示されるようにし、2024年 2 月27日㈫迄の模擬サイトへのアクセスを集計した。

4．事後のアンケート

2024年 2 月27日㈫にメール訓練対象者宛に先日のメールが訓練であったことをメール及びインフォメーションシステムのお知らせの掲示を行うとともに、2024年 3 月 5 日㈫迄の期間、アンケートを実施した。

4　結果と考察

4.1　模擬サイトへのアクセス者数結果

模擬サイトへのアクセス者数は、表 1 のとおりとなった。単純な比較はできないが、前回結果（14.1%）より高い結果となった。

要因として、今回のメール訓練では、前回の添付ファイルを開けるタイプの方法とは違い、より実践的なメール文面中の URL リンクをクリックするタイプの方法に変更したこと、メールの内容を取材のお願いという、大学教員にとってはよくある依頼メールの内容に変更したことにより、前回のメール訓練よりも標的型攻撃と気づかれにくくなったと考える。

一方、前回のメール訓練を経験した人に限ると、アクセス率は11.4%となり、前回の結果（14.1%）より改善が見られた。

表１　模擬サイトへのアクセス者数結果

	人数	割合
模擬サイトへアクセスした	526名	35.5%
模擬サイトへアクセスしなかった	995名	64.5%

4.2　アンケート回答数結果

アンケート回答者数は、表２のとおりとなった。アンケートへの回答と模擬サイトへのアクセスとの関係は、表３となり、模擬サイトへのアクセスの有無とアンケートへの回答の有無に関係は低いと見られる。

表２　アンケート回答者数結果

	人数	割合
アンケートに回答	322名	21.7%
アンケートに未回答	1,159名	78.3%

表３　アンケートへの回答と模擬サイトへのアクセスとの関係

	模擬サイトへアクセス有	模擬サイトへアクセス無
アンケートに回答	108名（7.3%）	214名（14.4%）
アンケートに未回答	415名（28.0%）	744名（50.2%）

4.3　各アンケート項目と回答結果

各アンケート項目に対する回答は表４の結果となった。訓練用メールを受信した際の最初の反応として、（表４：Q1, Q2）88.9%の方が、「かなり怪しい」「少し怪しい」と感じており、怪しいと感じた点についての回答としては、送信者アドレス、メール内容の怪しさを挙げていた。不審なメールに対しての行動として（表４：Q4）、「メール文面のリンクをクリックしなかった」が52.4%で多く、次に「メール文面のリンクをクリックした」が24.3%であった。その他回答のうち、周囲へ相談、エスカレーション、削除や迷惑メールフォルダへ移動した等の適切な行動を取られていた。

表４　アンケート項目と回答

Q1	今回の標的型攻撃メール訓練（以下。訓練メールという）を受信した際の最初の反応で最も近いものは次のどれでしたか？（１つ選択）		
	選択肢	回答数	割合
	かなり怪しいと感じた	177	55.0%
	少し怪しいと感じた	109	33.9%
	怪しくないと感じた	36	11.1%

次のページに続く

表４　アンケート項目と回答（続き）

Q２	Q１で「かなり怪しいと感じた」「少し怪しいと感じた」を選んだ方へ：怪しいと感じた理由は何でしたか？（複数選択可）		
	選択肢	回答数	割合
	送信者のアドレス	179	33.2%
	メールの内容	237	44.0%
	リンク	83	15.4%
	メールソフトウェア等の迷惑メールフィルタによる検索結果	11	2.0%
	その他	29	5.4%
Q３	Q２で「その他」を選んだ方へ、具体的に記入してください（自由記述）		
Q４	今回の訓練メールを受信した後。どのような対応をしましたか？（複数選択可）		
	選択肢	回答数	割合
	メール文面のリンクをクリックした	92	24.3%
	メール文面のリンクをクリックしなかった	198	52.4%
	IT センターサポートデスクに報告した	25	6.6%
	その他	63	16.7%
Q５	Q４で「その他」を選んだ方へ：具体的に記入してください。（自由記述）		
Q６	１月11日インフォメーションシステム掲載のお知らせ「標的型攻撃メールに関する注意喚起」をご覧いただきましたか？（１つ選択）		
	選択肢	回答数	割合
	はい	116	36.0%
	いいえ	206	64.0%
Q７	標的型攻撃メールについて、どの程度理解していましたか？（１つ選択）		
	選択肢	回答数	割合
	よく理解していた	92	24.3%
	どちらかというと理解していた	198	52.4%
	あまり理解していなかった	25	6.6%
	全く理解していなかった	63	16.7%
Q８	普段から情報セキュリティに関するニュースや情報をどの程度チェックしていますか？（１つ選択）		
	選択肢	回答数	割合
	週に１回はチェックしている	22	6.8%
	月に１回はチェックしている	85	26.4%
	ほとんどチェックしていない	201	62.5%
	全くチェックしていない	14	4.3%
Q９	今回の訓練で、標的型攻撃メールに関するあなたの知識や意識は向上しましたか？（１つ選択）		
	選択肢	回答数	割合
	大幅に向上した	38	11.8%
	やや向上した	188	58.3%
	あまり変わらなかった	81	25.2%
	全く変わらなかった	15	4.7%
Q10	標的型攻撃メールを見分ける際に、最も重要だと思うポイントは何ですか？（自由記述）		

次のページに続く

表4　アンケート項目と回答（続き）

Q11	お使いのメールソフトは次のどれですか？		
	選択肢	回答数	割合
	Microsoft Outlook（ウェブ版）	185	45.1%
	Microsoft Outlook（デスクトップ版）	114	27.8%
	Mozilla Thunderbird	36	8.8%
	Gmail	42	10.2%
	Apple Mail	18	4.4%
	その他	15	3.7%
Q12	Q11で「その他」を選んだ方へ：具体的なソフト名を記入してください（自由記述）		
Q13	訓練メールの頻度はどの程度が適切だと思いますか？（１つ選択）		
	選択肢	回答数	割合
	もっと頻繁に必要（年に数回）	73	22.7%
	現在の頻度で十分（年に１回）	184	57.1%
	あまり頻繁でなくて良い（数年に１回）	46	14.3%
	必要ない	19	5.9%

4.4　事前の注意喚起の効果について

事前のメール訓練予告にあたるインフォメーションシステム上でのお知らせ「標的型攻撃メールに関する注意喚起」を閲覧の有無について（表４：Q6）36.0%が「はい」と回答している。模擬サイトへアクセスの有無との関係は表５の結果となり、模擬サイトにアクセスしなかったグループは、アクセスしたグループに比べて、「標的型攻撃メールに関する注意喚起」を閲覧している割合が高くなっていることから、注意喚起の情報を閲覧している人は標的型攻撃メールに対する耐性が高いことがわかった。

また、普段から情報セキュリティに関するニュースや情報をどの程度チェックしているかについては、（表４：Q8）66.8%の方が「ほとんどチェックしていない」「全くチェックしていない」状況であることから、注意喚起の情報共有やアクセシビリティの向上が、標的型攻撃メールに対する意識及び耐性の向上につながる可能性があると考える。

表５　事前の注意喚起が模擬サイトへのアクセスに与える影響

	模擬サイトへアクセス有	模擬サイトへアクセス無
注意喚起を見た	58名（18.0%）	148名（46.0%）
注意喚起を見てない	50名（15.5%）	66名（20.4%）

4.5　メール訓練実施前の標的型攻撃メールについての理解度について

メール訓練実施前の標的型攻撃メールについての理解度と模擬サイトへのアクセスとの関係は表６のとおりとなった。模擬サイトにアクセスしたグループは、アクセスしなかったグループに比べて、標的型攻撃メールについて「あまり理解していなかった」または「全く理

解していなかった」と回答した割合が高くなっており、標的型攻撃メールに対する理解度の向上が耐性の向上に有益であることがわかる。

表 6　事前の標的型攻撃メールについての理解度と模擬サイトへのアクセスとの関係

	模擬サイトへアクセス			
事前の標的型攻撃メールについての知識や意識	有		無	
よく理解していた	73名（22.7%）	14名（4.3%）	187名（58.1%）	45名（14.0%）
どちらかというと理解していた		59名（9.3%）		142名（44.1%）
あまり理解していなかった	35名（10.9%）	31名（9.6%）	27名（8.4%）	27名（8.4%）
全く理解していなかった		4 名（1.2%）		0 名（0 %）

4.6　模擬サイトへのアクセスとメール訓練後の標的型攻撃メールについての知識や意識の向上との関係

今回のメール訓練を受けて、（表 4 ：Q9 ）70.1%の方は知識や意識が「大幅に向上」「やや向上」したと回答しており、メール訓練実施の有効性が確認できた。模擬サイトへのアクセスとメール訓練後の標的型攻撃メールについての知識や意識の向上との関係について、表 7 の結果となり、模擬サイトへアクセスしなかった方にも、知識や意識向上に有効であったことがわかった。

また、メール訓練後の振り返りとして「標的型攻撃メールを見分ける際のポイント」への問いには、大半の方がメールアドレスやリンクの怪しさと回答されており、不審なメールと見抜く力として耐性を付けられている事が確認できた。

表 7　模擬サイトへのアクセスとメール訓練後の標的型攻撃メールについての知識や意識の向上との関係

	模擬サイトへアクセス			
標的型攻撃メールについての知識や意識	有		無	
大幅に向上した	87名（27.0%）	24名（7.5%）	139名（43.1%）	14名（4.3%）
やや向上した		63名（19.6%）		125名（38.8%）
あまり変わらなかった	21名（6.5%）	18名（5.6%）	75名（23.3%）	63名（19.6%）
全く変わらなかった		3 名（0.9%）		12名（3.7%）

4.7　メール訓練の頻度について

メール訓練の頻度については、（表４：Q13）「年に数回」が22.7％、現状と同じ「年に１回」が57.1％と、80％以上を占めていたが、「必要ない」との回答が5.9％と、一定数いることがわかった。

5　課題

今回、大学教員および事務職員を対象に実施されたメール訓練では、多くの参加者が事前通知を見逃しており、注意喚起を意識されないまま、メール訓練に臨んだ状態であったと思われ、情報セキュリティに関する定期的な情報収集が不足していることが明らかになった。今後の課題として、メール訓練の頻度や方法、参加者への事前通知の改善、および教育プログラムの見直しに検討が挙げられる。

今回のメール訓練は、ほぼ一斉に対象者へ訓練用メールを配信する方法を採用した。そのため、事務職員の場合、部署の人数や部署内での情報共有により、アクセス率が低下したと見受けられるところもあった。この場合、一般的なスパムメールへの耐性は向上するが、実際の標的型攻撃メールのようにターゲットを絞った攻撃には対応しきれない可能性がある。この点を踏まえ、今後はランダムに訓練対象者を抽出して訓練用メールを配信する方法や、複数の訓練用メール文面を用意して配信する方法の検討が必要である。

技術面の課題として、現在 IT センターでは複数のセキュリティ機器を用いた多層的な対策を進めており、次回のメール訓練時にはこれらのセキュリティ装置が動作して訓練が予期せぬ形で失敗する可能性がある。通常の運用ではセキュリティ装置によるブロックは望ましいことだが、訓練時には予期せぬブロックが起きないように、今後は慎重に送信テストを行う必要がある。

6　おわりに

本訓練は、普通のセキュリティソフトでは防ぎにくい標的型攻撃メールへの対処方法を学ぶための模擬訓練であり、実際に標的型訓練メール（怪しいメール）を受け取った際の対応を練習し、適切な対処法を理解することが目的である。これにより、情報の誤送信リスクを低減し、本学の構成員が情報セキュリティにより一層注意を払うことを期待している。

各部署や職種ごとに、模擬サイトへのアクセス者数やアクセス率が競争の対象になることがある。しかし、訓練メールの内容によっては、特定の部署や職種でアクセス率が高くなることがあり得るため、単純にアクセス者数やアクセス率を比較するだけでは実際のリスクを見落とす恐れがある。

アンケートの結果から、標的型攻撃メールに関する知識が不足する中でのメール訓練実施

となる中、今回実施した URL クリック型の標的型攻撃メールの模擬訓練によって、情報セキュリティへの意識を高め、実際に起こり得る攻撃に対する警戒心も強化された。今後も、定期的な訓練と教育を充実させることにより、一人ひとりがセキュリティを重視する文化を築いていくことが重要である。

攻撃者の手法は絶えず進化しており、世間ではフェイク動画やフェイク画像を用いた SNS 型投資詐欺[3] や PC サポート詐欺[4] などの被害額が増加傾向となり、社会問題となっている。今後は生成 AI を用いたものが増え、フェイク情報、フェイクニュースや標的型攻撃メールを見抜く力を個々がしっかりと身につけることが大切である。今後も組織全体で情報セキュリティを重視する文化の醸成が求められると考える。

参考文献

［1］ 内閣サイバーセキュリティセンター. “学術関係者・シンクタンク研究員等を標的としたサイバー攻撃について（注意喚起）”. 内閣サイバーセキュリティセンター. 2023-11-30. https://www.nisc.go.jp/pdf/press/20221130NISC_press.pdf,（参照 2024-04-27）.

［2］ 日本年金機構 不正アクセスによる情報流出事案に関する調査委員会. “不正アクセスによる情報流出案件について”. 日本年金機構. 2016-01-04. https://www.nenkin.go.jp/oshirase/topics/2016/0104.files/F.pdf,（参照 2024-04-27）p. 2-3.

［3］ 警察庁 捜査第二課 組織犯罪対策第二課. “SNS 型投資・ロマンス詐欺の被害発生状況等について”. 警察庁. 2024-03-13. https://www.npa.go.jp/bureau/criminal/souni/sns-romance/sns-romance20240311.pdf,（参照 2024-04-27）.

［4］ 大阪府警察. “サポート詐欺の手口及び対処法”. 大阪府警察. 2024 https://www.police.pref.osaka.lg.jp/seikatsu/tokusyusagi/14206.html,（参照 2024-05-01）.

A　事前啓発資料（標的型攻撃メールの見分け方）

標的型攻撃メールの見分け方

2023年6月27日
情報推進グループ

スパムメールやフィッシングメールとの違い

本物のメールと見分けがつきにくい上、ウイルス対策ソフトウェアのチェックをすり抜けることも多く、標的者まで届いてしまいます。

4

標的型攻撃メールとは

1

標的型攻撃メールの手口

5

まずは、標的型攻撃について

本学や個人を標的にして、重要情報の搾取等を目的とした攻撃です。

悪の組織の思惑は・・・

標的とした本学のシステムに侵入して
個人情報や重要情報を搾取したい。

不正に動作させるために作られた悪意のあるソフトウェアのこと。
ウイルスやワームなどが含まれる。

そのためには、あなたのパソコンにマルウェアをインストールさせて、パソコンを遠隔操作したい。

2

標的型攻撃メールの手口

実在する信頼できそうな人名や組織名に差出人を偽装している。

- 友人・知人
- 実在する組織の社員・職員

知らない人からのメールであるが開封せざるを得ない内容である。

- 報道関係・出版社などからの取材申請・公演依頼
- 就職活動に関する問い合わせ
- 学外、近隣からのクレーム
- アンケート調査

6

標的型攻撃メールとは

- 本学や個人等、特定の標的に対して送信されるメールのことです。
- 攻撃者はパソコンやスマートフォンなどの端末をマルウェアに感染させようと、標的者の知り合いや関係先のように送信者を偽装して、悪意のあるファイルを添付したり、悪意のあるサイトに誘導するためのURLリンクを貼り付けたメールを送信してきます。
- そのため、標的型攻撃メールにより、気づかないうちにマルウェアに感染して、重要な情報が盗まれる事件が発生しています。

3

標的型攻撃メールの手口（続き）

誤って自分宛てに送られたメールのようだが興味をそそられる内容に偽装している。

- 人事、給与に関する内部文書
- 議事録、講演原稿などの内部文書
- 成績に関する情報
- 有名人の訪問に関する情報

公的機関からのお知らせに偽装している。

- 情報セキュリティに関する注意喚起
- 新型コロナウイルス流行情報
- 災害情報

7

標的型攻撃メール対策

標的型攻撃メールは1つの対策で防げるものではなく、
多層の防御対策が必要です。

8

標的型攻撃メール対策

OSやアプリケーションを最新に保つ。

- OS、Webブラウザ、電子メールソフト、Officeアプリケーション、PDFソフトウェアなどのソフトウェアを最新の状態に保つこと。
- 脆弱性対応をせずに放置していると、マルウェアに感染したり、悪意のあるホームページを見ただけでパソコンの中のシステムが破壊されたりすることがあります。

ウイルス対策ソフトウェア等を導入する。

- ウイルス対策ソフトウェア等のセキュリティ対策ソフトウェアを導入し、定義ファイル（パターンファイル）を更新して最新の状態に保つことでマルウェア等のリスクを軽減することができます。
- ただし、ウイルス対策ソフトウェアのチェックをすり抜けることも多く、過信は禁物です。

9

標的型攻撃メール対策（続き）

不審なメールに記載されているリンクを辿らない。

メール本文のリンク先のWebサイトが本物とそっくりの偽サイトである可能性があります。不審なメール本文中のリンクを安易に辿らないようにしてください。

不審なメールの添付ファイルを開封しない。

標的型攻撃に利用されるウイルスには、実行形式のものや、組織でよく利用されるソフトウェアの脆弱性を突くものが多くあります。不審なメールに添付ファイルが付いていたら要注意です。

10

標的型攻撃メール対策（続き）

WordやExcelファイルを開いた際に、マクロを有効化、コンテンツの有効化をしない。

有効化すると、ウイルスがダウンロードされる恐れがあります。

不審なメールのパスワード付きZIPファイルに注意する。

パスワードにより暗号化されているため、メール配送経路上でセキュリティ製品の検知・検疫をすり抜ける可能性が高く、ZIPファイルにマルウェアが入っている恐れがあります。

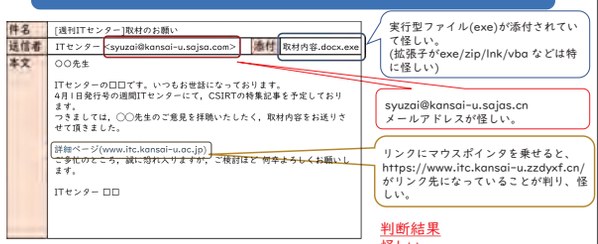
11

標的型攻撃メールの見分け方

判断が難しいですが、メールの内容を総合的に判断して見分けるようにしましょう。
別の連絡手段で相手に確認する等も有効です。

12

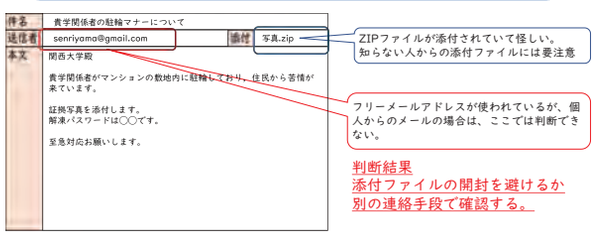
例：関係者からのメールに偽装しているケース



判断結果
怪しい

13

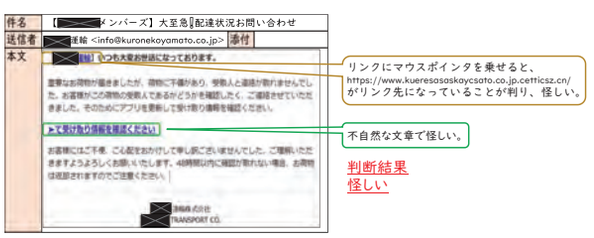
例：開封せざるを得ないメールに偽装しているケース



判断結果
添付ファイルの開封を避けるか
別の連絡手段で確認する。

14

例：運送会社からの問い合わせに偽装しているケース



判断結果
怪しい

15

例：誤って自分宛てに送られたメールで、興味をそそられる内容に偽装しているケース

件名	［要機密情報］VIPの来校について		
送信者	［実在するメールアドレス］	添付	詳細.zip
本文	○○課 ○○様 平素より大変お世話になっております。 映画のPRのため、俳優の○○さんがキャンパスに来られます。 詳細は添付資料をご確認ください。 以上です。 よろしくお願いします。		

判断結果
自分宛てではないメールの添付ファイルは開封しない。

16

標的型攻撃メールの見分け方（その他）※

不自然な日本語の使用や、日本語では使用されない漢字やカタカナが使用されていないかを確認する。

［例］
・皆様→皆様
・文字化けが発生している場合

メール署名の妥当性を確認する。

署名の人物・所属組織が実在するか正確性を確認する。

差出人（送信元）のメールアドレスを確認する。

フリーメールアドレスが使われている場合がある。

※ただし、最近ではこの方法で見分けられないメールも増えています。

17

怪しいと感じた際に実行すべき事項

18

怪しいと感じた際に実行すべき事項

1. 別の手法で送信者へ確認する。

送信者として知人の名が記載されたメールであっても、怪しいと感じた際には、当該メールへの返信以外の方法で送信者に内容を確認してください。

メール本文に記載されている連絡先も怪しいため、企業や組織からのメールの場合、インターネット等で公式Webサイト等から連絡先を確認してください。

2. セキュリティ対策ソフトウェアでフルスキャンする。

念のためセキュリティ対策ソフトウェアを最新の状態にして、フルスキャンを実施してください。

19

問い合わせ

20

ITセンターサポートデスク

パソコンやスマートフォンの利用に関するさまざまな相談を受け付けています。

- 外線：[redacted]　内線：[redacted]
- [redacted]
- サポート時間：9:00-17:00（土・日・祝日、大学休業日を除く）

21

Thank you.

22