メール訓練手引書

一般公開版 (ver. 1. 0)

2022 年 8 月 18 日

一般社団法人 日本コンピュータセキュリティインシデント対応チーム協議会
（日本シーサート協議会）

メール訓練手法検討サブワーキンググループ

◆メール訓練手引書一般公開版について

一般社団法人 日本コンピュータセキュリティインシデント対応チーム協議会（以下、日本シーサート協議会）は、協議会加盟チームで実施しているメール訓練に関する課題/問題を共有すると共に、効率的・効果的なメール訓練手法の検討を目的としたワーキンググループ活動（メール訓練サブワーキンググループ）に取り組んでいます。

メール訓練は、組織のもっとも大きい脅威である「標的型攻撃による被害」に対応するために、不審メールへの対応力向上を目的とした従業員向けの訓練になりますが、訓練方法や目標の設定、評価方法などの情報が少ない中で悩みながら行われていることが多い状況です。

このメール訓練手引書一般公開版は、メール訓練サブワーキンググループの活動成果であるメール訓練手引書第３版を、協議会加盟組織以外の企業にも広く役立てていただくことを目的に、再編集した手引書となっています。メール訓練の成果が不明確、マンネリ化している、また、これからメール訓練の導入を検討している企業などに、本手引書が参考になりましたら幸いです。

◆メール訓練手引書一般公開版の主な内容

１．メール訓練の計画
２．メール訓練の準備
３．メール訓練の実施
４．メール訓練の最適化に向けて
５．メール訓練委託の場合
６．メール訓練実施状況アンケート集計結果

※日本シーサート協議会加盟組織に向けたメール訓練手引書第３版では、以下の内容を追加しております。ぜひ協議会に加盟いただき、加盟組織限定情報もご活用ください。

◆加盟組織限定情報

１．メール訓練工夫点、改善点 14 チーム
２．訓練メール事例　66 事例（国内訓練メール 52 事例　海外訓練メール 11 事例）
※協議会加盟組織は掲載事例を自社訓練に 2 次利用可能としています。

・実施時期	・件名
・難度	・訓練での見破りポイント
・カテゴリ	・訓練メール概要、工夫点
・分類	・開封率（%）
・メール形式	・対象人数
・誘導形式	・訓練対象
・添付ファイル形式	・事前学習有無
・差出人種類	・事前周知有無
・差出人名	・訓練結果概要
・差出人偽装	・考慮事項、注意点

３．誘導先ページの事例　12 事例
４．教育資料の工夫点、改善点　4 事例
５．メール訓練報告書の工夫点、改善点　2 事例

◆本書の目的

独立行政法人情報処理推進機構（IPA）が公表している「情報セキュリティ 10 大脅威」によると、組織におけるセキュリティ脅威に「標的型攻撃による被害」があり、2021 年は 2 位、2020 年までは 5 年連続 1 位と組織として最も大きく、かつ、継続している脅威と言える。組織はこの脅威への対策としてメール訓練の実施を進めている。

日本シーサート協議会 訓練ワーキンググループ内で実施したアンケートからも、メール訓練を実施、または実施予定が８割以上となっており、多くの企業が取り組んでいる状況である。また、訓練に用いるメール文面立案などに苦戦していることがわかり、各 CSIRT 担当者は、課題を抱えながらメール訓練を実施しているのが現状となっている。

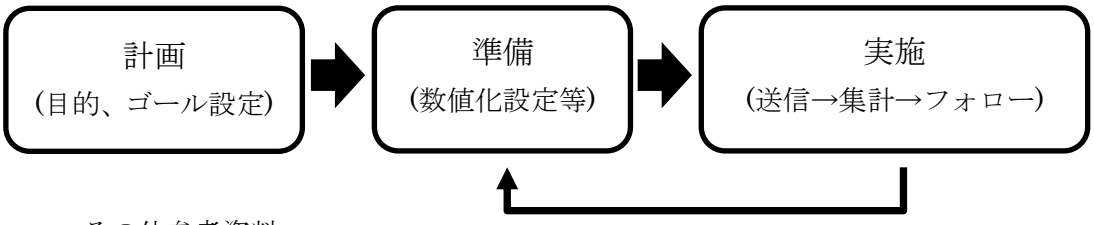
本手引書は、これらの課題を解決するためにメール訓練実施における必要な検討要素を明確にし、円滑かつ発展性のあるメール訓練の実施を支援することを目的とする。本手引書がメール訓練開始の手助け、また、実施中の CSIRT やセキュリティ担当者の工数削減、訓練最適化となり、最終的に標的型攻撃の防御につながることを期待する。

◆想定する読み手

メール訓練を実施中、並びにこれから訓練を開始する企業の CSIRT、または、セキュリティ担当者を想定として作成している。

◆手引書の構成

本手引書は以下の構成でまとめている。メール訓練は準備から実施を繰り返して行う。



・その他参考資料

ゴール達成の工夫点、訓練メール事例　等

メール訓練を繰り返す過程で課題を明確にし、ゴール達成に向けた工夫が必要である。すでに訓練を実施している CSIRT も「計画」の必要要素から再確認することが望ましい。

メール訓練手引書（メール訓練実施における検討要素）

目次

1　メール訓練計画
1.1　メール訓練の必要性
　メール訓練の将来的な必要性
1.1.1　メール訓練の役割
1.1.2　メール訓練の種類
1.1.3　メール訓練の流れ（概要）
1.2　訓練目的の明確化
1.3　ゴールの設定
1.4　要求する行動の設定
1.5　インシデント対応との関係確認
1.6　社内規程等との関係確認
1.7　訓練対象者個人情報の確認
1.7.1　個人情報利用目的の確認
1.7.2　海外対象者の個人情報取り扱い確認
1.8　実施要素の決定
1.9　メール訓練の運用方法の決定
1.10　担当役割の設定
1.10.1　役割分担
1.10.2　問合せ窓口

2　メール訓練の準備
2.1　訓練対象の選択
2.1.1　海外を対象とした訓練
2.1.2　社外の従業者を対象とした訓練の注意点
2.2　訓練回数の決定
2.3　訓練メール送信環境
2.4　誘導先ページ（リンク先ページ、添付ファイル）の用意
2.5　訓練用ドメインの用意
2.6　受信環境の調査
2.7　メール訓練の検知・数値化設定
2.7.1　リンク URL 型訓練の検知・数値化設定
2.7.2　添付ファイル型訓練の検知・数値化設定
2.7.3　通報訓練の数値化
2.7.4　数値化設定の注意点
2.8　ネットワーク環境の設定
2.8.1　受信環境ホワイトリスト登録
2.8.2　プロキシ設定の確認
2.9　実際の攻撃メール情報の収集
2.10　安定したメール訓練環境の維持

3　メール訓練実施
3.1　次回メール訓練に向けた方向性決定
3.2　次回訓練メール送信日の決定
3.3　次回訓練メール要素の決定

3.4　訓練対象の決定とメールアドレスリストの準備
3.5　訓練案内
3.6　メール訓練に関する教育
3.7　訓練メールの作成
3.8　体制、問い合わせ対応の再確認
3.9　リハーサルの実施
3.10　訓練メールの送信実施
3.11　送信直後の対応
3.12　トラッキング収集
3.13　通報の収集
3.14　事後対応
3.14.1　種明かし案内、訓練結果速報
3.14.2　全体アンケート
3.15　訓練結果集計
3.15.1　集計期間
3.15.2　トラッキング情報の集計
3.15.3　通報情報の集計
3.15.4　属性別の集計
3.16　全体アンケート集計
3.17　課題の明確化
3.18　フィードバック
3.19　フォロー
3.20　経営層への報告
3.21　メール訓練改善検討

4　メール訓練の最適化に向けて
4.1　学術連携「メール訓練と褒める文化について」(明治大学)
4.2　メール訓練の成熟度
4.2.1　モデル１：開封率、通報率を指標とした成熟度モデル
4.2.2　モデル２：訓練メールの難易度を指標とした成熟度モデル
4.3　テレワークにおけるメール訓練の工夫すべき点
4.3.1　テレワークにおけるメール訓練実施状況　調査結果
4.3.2　テレワークにおけるメール訓練の工夫点

5　メール訓練委託の場合
5.1　確認すべき事項
5.2　外部委託する場合の個人情報の取り扱い

以下（6.　7.　8.）は加盟組織限定情報となります。

6　ゴール達成の工夫点
6.1　メール訓練工夫点、改善点の取り扱いについて
6.2　メール訓練手法検討サブ WG 参加チームのメール訓練工夫点、改善点
6.3　その他の工夫点、改善点
（メール訓練サブ WG 内で検討した工夫点、改善点のまとめ）

7　関連資料
7.1　訓練メール事例

7.1.1　訓練メール事例の取り扱いについて
7.1.2　訓練メール事例の二次利用について
7.1.3　訓練メール一覧（国内訓練）
7.1.4　訓練メール一覧（海外訓練）
7.2　誘導先ページ（リンク先ページ内容、添付ファイル内容）の事例
7.2.1　誘導先ページ事例の取り扱いについて
7.2.2　誘導先ページ事例の二次利用について
7.2.3　誘導先ページ事例
7.3　教育資料の工夫点、改善点
7.3.1　教育資料の工夫点、改善点の取り扱いについて
7.3.2　教育資料の工夫点、改善点事例
7.4　メール訓練報告書の工夫点、改善点
7.4.1　メール訓練報告書の工夫点、改善点の取り扱いについて
7.4.2　メール訓練報告書の工夫点、改善点事例

6(8)　メール訓練実施状況アンケート　集計結果関連資料
アンケート項目一覧

・メール訓練手引書作成メンバー
・最後に
・お問い合わせ

メール訓練実施における検討要素

1　メール訓練計画

1.1　メール訓練の必要性

メールを使った標的型攻撃は、重要な情報を盗み出す手段として PC などにメールを使って侵入し、マルウェアに感染させる事などを目的としている。巧妙な騙しのテクニックを用いた攻撃メールを送信してくるため正規メールと区別がつかず、メールフィルタなどの技術的対策では完全に防ぐことはできない。したがって訓練メールによる事前の疑似体験と、繰り返し体験による習得が有効な対策となる。

NCA 訓練 WG を対象に実施したアンケートにおける「メール訓練実施有無」は以下となる。

メール訓練実施有無	第 1 回アンケート	第 2 回アンケート	第 3 回アンケート
有	85.7%	87.1%	79.1%
無:計画無し	9.5%	8.1%	14.3%
無:計画中	4.8%	4.8%	6.6%
	100.0%	100.0%	100.0%

※メール訓練の将来的な必要性について

NCA 訓練 WG 参加チームを対象に行った第２回アンケート（2019 年 10 月）から「メール訓練の将来的な必要性」を追加し、以下の結果となった。（将来的は５年後をイメージ。）

メール訓練の将来的な必要性	第２回アンケート	第３回アンケート
将来的にも必要と思う	90.3%	91.2%
将来的には不要と思う	9.7%	8.8%
	100.0%	100.0%

「将来的」として５年後をイメージしたアンケートであるが「メール訓練は将来的にも必要」の回答が９割を超えた。回答の理由として「５年後もメールを使用している」「スキルに依存する」が多い結果となった。

回答の理由（一例）

「将来的にも必要と思う」 回答の理由（第 3 回アンケートまでの一例）
5 年程度はコミュニケーションツールとしてのメールがなくならないだろう。
標的型メール攻撃は完全に防ぐことができず、最終的にはユーザーのスキルに依存するところが大きいため。
メール訓練と言うよりも詐欺対策教育訓練として残ると思っています。
巧妙な攻撃は増加すると思いますので、踏んでしまった後の初動がますます重要になると思います。

リテラシーの高くない従業員も入社（あるいは転入）してくるため、将来的にも必要である。
EMOTET のような実際のメールを利用した返信型メールなど、攻撃手法が変わってくるので、攻撃手法に合わせた訓練は必要。
どんな内容であれ、繰り返しの訓練は必要。社員はいつも同じとは限らず、入れ替わりは常に発生している。不審メールがいつ届くかもわからないそのため、常にアンテナを張り、意識を持つように全員がある程度の水準を保てるように継続的訓練が必要。
標的型メールはビジネスメール詐欺（BEC）へ発展する可能性があります。このような被害があることを知り、注意する意味でメール訓練の必要性を感じます。

「将来的には不要と思う」 回答の理由（第 3 回アンケートまでの一例）
現状では攻撃の手段として eMail を用いるケースが散見されるが、昨今の IoT 然り、eMail よりも攻撃者にとってコストパフォーマンスの良い別の媒体を利用した攻撃が主流となると考えられるため。
防御、無害化が進み、攻撃メールによる脅威が劇的に下がると思っています
現在やっている行動訓練としては、日々本物が届く状況下では不要と考える。但し、行動定着のための意識啓発は必須。一方で、実際に感染してしまったらどんな動きをするのか、イメージしやすい「感染体験プログラム」のようなものが必要と感じている。

1.1.1 メール訓練の役割

メール訓練は、入口対策で完全に防ぐことができない攻撃メールを疑似的に社員に送信し、攻撃メールへの対応を練習する役割となる。具体的には以下のような役割となる。

① 攻撃メールの体験

攻撃メールが届く可能性があることを事前に疑似体験する役割がある。

② 攻撃メールの見抜く能力の向上

攻撃メールに対して見抜く能力を向上させ攻撃メールのリンク URL をクリックしないようにし、攻撃メールからのマルウェア感染などのリスクを低減する役割がある。しかし実際の攻撃メールは巧妙で見抜くのが大変困難な場合がある。見抜くことが可能な難度を定めて行うことが望ましい。例えば”ばらまき型攻撃メール”などへの”うっかりクリック”の低減などである。

③ 攻撃メールへの対応練習

本物の巧妙な攻撃メールを多忙な業務の中で完全に見抜くのは困難であり、攻撃メールを通常のメールと認識しマルウェアのダウンロードサイトに誘導する URL をクリックした場合や、同様の誘導を忍ばせた添付ファイルを開封してしまうことが想定される。メール訓練では、このような行為後に不審に気が付いたときに、慌てずに通報や初期対応ができるよう練習することも重要な役割となる。

1.1.2 メール訓練の種類

メール訓練の種類は、測定と評価の違いから以下の 2 種類がある。

① 攻撃メールを見抜く能力の向上訓練（判別訓練）

攻撃メールの見抜く能力として、攻撃メールの特徴や手法の教育と疑似的な訓練メールの送信を繰り返し、見抜く能力を向上させる訓練である。見抜けず通常のメールと認識し、リンク URL のクリックや添付ファイルの開封を行った行動を数値的に評価する。

② 攻撃メールへの対応練習（通報訓練）

通報訓練は攻撃メールを見抜くことより、訓練メールのリンク URL のクリックや添付ファイルの開封後、通報の実行有無を評価する訓練である。リンク URL のクリックや添付ファイルの開封段階は、まだ通常のメールと認識している段階であるが、クリック後に無関係のページが表示されたり、言語が異なるなど、不審と感じる段階がある。通報訓練ではクリック先のページまたは添付ファイルの内容で訓練であることを伝える、もしくは直接的に伝えず不審に思わせ、迷わず通報できるよう練習する。

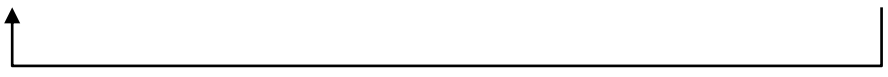
NCA 訓練 WG を対象に実施したアンケートにおける「メール訓練時の通報実施について」は以下となる。アンケート結果では、通報実施が減少しており、第 3 回アンケートにて 50%以下となった。

メール訓練時の通報実施について	第1回アンケート	第2回アンケート	第3回アンケート
実施(通報を求めている)	72.2%	63.6%	48.9%
未実施(通報を求めていない)	11.1%	29.1%	23.9%
計画中(通報を求める訓練を計画中)	11.1%	1.8%	5.4%
無回答	5.6%	5.5%	21.7%
	100.0%	100.0%	100.0%

1.1.3 メール訓練の流れ（概要）

メール訓練は、訓練メールの送信を繰り返せば対策になるわけでは無い。目的の明確化とゴール設定から始め、計画と準備を整えてからメール訓練を実施する必要がある。

訓練案内 → 訓練対象決定 → 訓練メール送信 → 測定 → 集計 → フォロー



1.2　訓練目的の明確化

メール訓練では目的を明確にすることが重要である。「他社が行っているから」などは目的にならず、以下の例などを参考に設定することが望ましい。メール訓練実施の目的は業種や企業規模、CSIRT 活動やメール訓練の成熟度などによって異なる。また、目的を 1 つに限定せず繰り返される訓練の過程で見直すことが必要である。

・メール訓練の実施目的例

（NCA 訓練 WG を対象に実施したアンケートで回答数の多い順）

訓練メール目的（複数回答可）	第 1 回アンケート	第 2 回アンケート	第 3 回アンケート
リテラシー教育の一環として	29	49	65
不審メールの開封率を下げるため	31	44	62
セキュリティ意識向上のため		43	61
開封後の初動（CSIRT への連絡等）を確認するため	21	34	47
インシデント通報の定着のため	25	33	42
攻撃メールに対する耐性（レジリエンス）を高めるため		31	40
不審メールが増えていることを定期的に気付かせるため		16	28
開封率の特に高い組織や人を特定するため	6	7	9
監督官庁や親会社からの実施依頼があったため	2	3	4
その他、自由記載	2	2	4

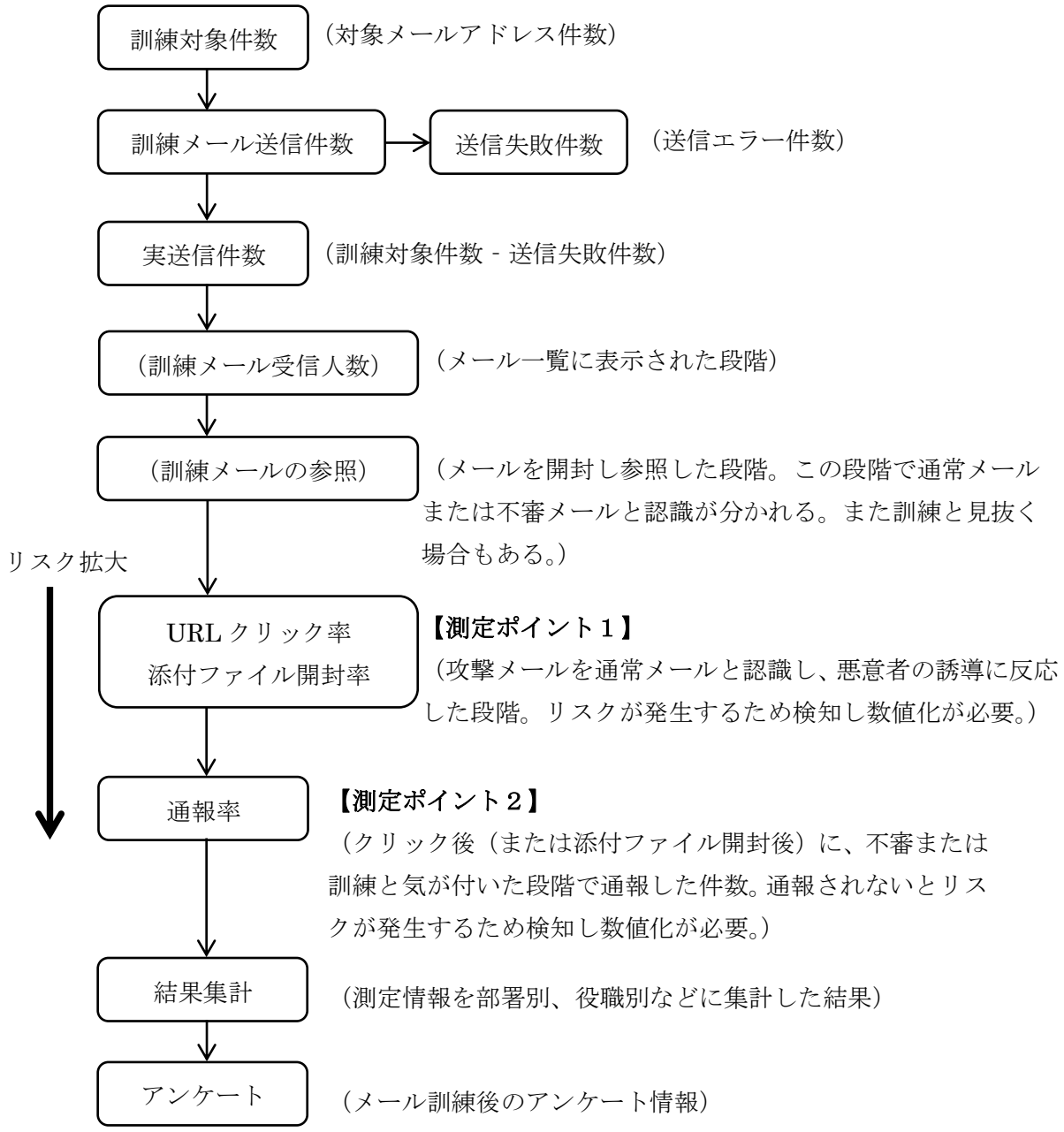
・メール訓練目的と有効となる訓練種類は以下となる。訓練種類は目的とゴールなど訓練詳細から選択する必要があり以下は一例である。

メール訓練目的例	判別訓練	通報訓練
不審メールの開封率を下げるため	○	
リテラシー教育の一環として	○	○
インシデント通報の定着のため	○	○
開封後の初動（CSIRT への連絡等）を確認するため	○	○
開封率の特に高い組織や人を特定するため	○	
監督官庁や親会社からの実施依頼があったため	○	○

1.3　ゴールの設定

メール訓練の目的に対し評価可能な数値的ゴールを設定することが望ましい。目的と連動しているため、目的を変更した場合にはゴールも変更する必要がある。ゴール設定は以下の「メール訓練における測定ポイントと数値化」が参考となる。

・メール訓練における測定ポイントと数値化



ゴール設定は URL クリック率（添付ファイル開封率）と通報率など複数設定する場合もある。また、訓練開始段階は URL クリック率（または開封率）とし、通報受付体制の整備後に通報率に移行するなど、体制との関係でゴールを変更するやり方もある。

ゴール設定例

・クリック率

判別訓練に必要な測定項目である。

内容：”リンク URL 型訓練メール”の場合の URL クリック人数比率

算出方法：クリック率＝クリック人数÷実送信件数×１００

クリック人数はリンク先アクセスログ等の集計から算出することができる。詳細は「2.7　メール訓練の数値化設定」に記載。

ゴール例：クリック率１０％以下

・添付ファイル開封率

判別訓練に必要な測定項目である。

内容：添付ファイル型の場合の添付ファイル開封人数比率

算出方法：添付ファイル開封率＝開封人数÷実送信件数×１００

開封人数は添付ファイルに設定したビーコンのアクセスログ集計から算出することができる。詳細は「2.7　メール訓練の数値化設定」に記載。

ゴール例：開封率１０％以下

※クリック人数と開封人数は、一人当たり複数クリック、開封しても 1 回とする。
※実送信数は送信リスト数から送信失敗メール数（バウンスメール数）を引いた数。

・通報率

通報訓練に必要な測定項目である。

内容：URL クリックまたは添付ファイル開封者内の通報人数比率

算出方法：通報率＝通報人数÷クリック人数（または開封人数）×１００

通報人数の把握には通報、連絡の受付が必要である。Web システムやスマートフォンアプリ、または、電話受付などがある、メール訓練では対象者人数に応じて受付方法の検討が必要である。受付キャパシティに問題がある場合は、訓練メールの送信を分散させ、受付集中を起きないようにする工夫も必要である。また、通報は遅滞なく実施される必要があるため、クリック時刻と通報時刻の差も測定する必要がある。

詳細は「2.7　メール訓練の数値化設定」に記載。

ゴール例：通報率９０％以上

※注意点

・訓練対象者毎の測定が必要（対象者一人ひとりの測定）

クリックや開封のアクションを訓練対象者毎に測定し、明確な「人数」の算出が必要である。リンク URL に訓練者コードを埋め込むなどのパーソナライズすることが望ましい。詳細は「2.7 メール訓練の検知・数値化設定」に記載。

・検知の精度

検知漏れや誤検知が発生する場合がある。クリックや開封があっても、検知できない場合や、逆にクリックしていないのに検知される場合もあり、誤検知発生を想定しておく必要がある。（「2.7.4 数値化設定の注意点」にて記載）

1.4 要求する行動の設定

訓練メールの URL クリックや添付ファイル開封を行ったときの行動を事前に設定する必要がある。

・受信時の行動例（訓練メールを不審メールと認識した場合の行動例）

例：掲示板などに不審メール受信として、差出人や件名などを投稿し他従業員に知らせる。

・訓練メールの URL をクリックした場合の行動例

例：LAN ケーブルの抜線、PC の利用中止、管理者への通報

NCA 訓練 WG を対象に実施したアンケートにおける「社内ルールで定められている初動対応」は以下となる。

社内ルールで定めている 初動対応(複数回答可)	第 1 回アンケート	第 2 回アンケート	第 3 回アンケート
通報	29	47	68
ネットワークからの切り離し	31	46	63
電源OFF	2	3	4
PC初期化/入れ替え	1	3	4
特になし		0	1
その他	5	3	6

1.5 インシデント対応との関係確認

社内で定められたインシデント対応手順とメール訓練時に要求する行動の関係を明確にする必要がある。不審メールの URL クリックや添付ファイル開封はインシデント発生となる。インシデント対応手順で定められた行動と連動したメール訓練時の行動要求事項を定める必要がある。

1.6　社内規程等との関係確認

インシデント対応に関する社内規程が定められている場合は、規程の則った行動を要求する必要がある。

・例：マルウェア対策規程類との連動

マルウェア感染時の初動等が定められている場合は、訓練メールの添付ファイル開封時に同じ初動を要求する。

・例：危機管理規程類との連動

インシデント発生時のエスカレーションフロー等が定められている場合は、訓練メールの受信、クリック、添付ファイル開封時に同じエスカレーションを要求する。

訓練の運営のため、メール訓練専用のエスカレーション先としてメール訓練事務局などに変更することは運営上の工夫となる。

NCA 訓練 WG を対象に実施したアンケートにおける「社内ルールにて通報を定めていますか」は以下となる。

社内ルールにて通報を定めていますか？	第 1 回アンケート	第 2 回アンケート	第 3 回アンケート
社内ルールで定めている	83.3%	77.8%	76.9%
定めていない	2.8%	1.6%	1.1%
定めていないが運用がある	5.6%	6.3%	6.6%
無回答	8.3%	14.3%	15.4%
	100.0%	100.0%	100.0%

※社内規程連動の注意点

メール訓練における社内規程との連動は「行動の連動」であり、制裁規定には関係しないこととなる。これを明確にするために訓練対象者に事前に周知することが有効である。メール訓練は制裁事項や人事考課に関係しない活動とすることが望ましい。また、メール訓練が「従業者のモニタリング」に当たらないことも関係部門とすり合わせしておくことが望ましい。

1.7　訓練対象者個人情報の確認

1.7.1 個人情報利用目的の確認

訓練メールの送信先となるメールアドレスは個人情報であり、従業員情報の利用目的について確認が必要である。また関連会社の場合は、従業員情報の利用目的確認に加え、共同利用に関する契約についても確認が必要である。

1.7.2 海外対象者の個人情報取り扱い確認

海外法令との関係性確認が必要である。メールアドレスなどの個人情報に加え、ＩＰアドレスなどの取扱いも注意が必要である。国内外の法務部門と連携し事前に確認することが望ましい。

1.8　実施要素の決定

メール訓練の必要要素は、訓練メールの「送信」を中心として「案内」から「フォロー」などがある。実施要素は訓練の段階により変更することも望ましい。また、訓練規模やCSIRT要員の負荷状況によっても実施要素を調整する必要がある。

例：段階別の実施要素例

	案内	教育	送信	結果集計	課題抽出	ﾌｨｰﾄﾞﾊﾞｯｸ	フォロー
現状把握	○		○	○		○	
初期段階	○	○	○	○	○	○	
育成段階	○	○	○	○	○	○	○
抜打訓練			○	○	○	○	○

1.9　メール訓練の運用方法の決定

メール訓練を自社運用するか外部委託するかの検討が必要である。

NCA訓練WGを対象に実施したアンケートにおける「訓練運用形態」は以下となる。

現在の訓練運用形態	第1回アンケート	第2回アンケート	第3回アンケート
自社(内部):内製ツール	51.2%	41.4%	33.0%
自社(内部):OSSや市販ソフト		19.0%	17.6%
外部委託	19.5%	19.0%	18.7%
ASP等外部サービス+自社運用	12.2%	13.8%	13.2%
無回答	9.8%	5.2%	16.5%
その他	7.3%	1.6%	1.1%
	100.0%	100.0%	100.0%

訓練運用はCSIRT要員の負荷、訓練対象人数、訓練回数、目的、ゴールにより検討が必要である。また、訓練段階的により変更することも検討が必要である。

運用形態の過去、今後の変更についてのアンケート回答は以下となる。

	第2回アンケート		第3回アンケート	
訓練運用形態の変更	過去の運用形態	今後の運用形態	過去の運用形態	今後の運用形態
変更なし、変更計画なし	51.6%	56.5%	48.4%	57.1%
自社(内部):内製ツール	4.8%	1.6%	5.5%	1.1%
自社(内部):OSSや市販ソフト	1.6%	3.2%	2.2%	2.2%
外部委託	14.5%	1.6%	13.2%	2.2%
ASP等外部サービス+自社運用	1.6%	4.8%	2.2%	3.3%
無回答	22.6%	25.8%	26.4%	28.6%
その他	3.2%	6.5%	2.2%	5.5%

現在の運用形態の約 50%が自社（内部）に対し、過去の運用が「外部委託」である回答が 10%以上あった。また、2018 年以降に訓練を開始したチームにおいて外部委託は 28%となり、訓練開始段階は外部委託を採用する傾向がある。（2019 アンケート（第 2 回）結果より）

1.10 担当役割の設定

メール訓練を進める上で担当役割を明確にする必要がある。役割は内部運営する場合と委託する場合とで異なる。

1.10.1 役割分担

実際の訓練実施では①案内から⑦フォローまでの複数要素を CSIRT が担当することとなる。

※役割設定の注意点

メール訓練の全要素を CSIRT が担当することも可能だが、以下を考慮し役割を決めることが望ましい。

・個人情報の取り扱い

メールアドレスは個人情報となるため社内規程に則り、取り扱うエリアや権限を考慮する必要がある。

・地区分散

教育とフォローは、訓練対象者に近い担当者が行うことが有効な場合がある。CSIRT 要員の負荷軽減も含め、職場地区分散の検討も必要である。

1.10.2 問合せ窓口

「案内」から「フォロー」の要素以外に問合せ担当を明確にすることが望ましい。訓練は問合せが発生するため、インシデント発生時のエスカレーションフローとは別に問合せ担当を明確にすることが望ましい。

2　メール訓練の準備

2.1　訓練対象の選択

メール訓練は標的型攻撃メールを受信する可能性があるメールアドレス付与者全員が対象となる。全員を一斉に訓練する場合の他に、役員と一般職層など役職別に分けて実施する場合もある。また、訓練結果から継続的な開封者を対象とする場合もある。

役職別に分けて実施する例として、役員層に「セミナー講師依頼」の訓練メールを採用し、一般層には「メールボックス容量超過」を装った訓練メールとするなど、対象者が被害に遭う可能性が高い内容に変えて訓練する。この場合、開封率や通報率を層別に評価することが必要である。

NCA 訓練 WG を対象に実施したアンケートにおける「訓練対象」は以下となる。

訓練対象(国内)	第 1 回アンケート	第 2 回アンケート	第 3 回アンケート
全員対象	70.7%	64.5%	65.9%
部分的	19.5%	24.2%	17.6%
無回答	7.3%	11.3%	16.5%
未実施	2.4%	0.0%	0.0%

部分的　訓練対象	第 1 回アンケート	第 2 回アンケート	第 3 回アンケート
役員	13	18	23
管理職	17	19	24
一般社員	16	20	25
新規採用者		17	21
派遣社員	12	11	17
協力会社	8	5	9
その他	1	4	7

2.1.1 海外を対象とした訓練

海外の従業員もメールアドレス付与者全員を対象にすることが望ましいが、訓練運用や現地協力などから検討する必要がある。

NCA 訓練 WG を対象に実施したアンケートにおける「海外訓練実施状況」は以下となる。

訓練対象(海外)	第 1 回アンケート	第 2 回アンケート	第 3 回アンケート
全員対象	12.2%	16.1%	14.3%
部分的	12.2%	11.3%	11.0%
未実施	41.5%	43.5%	40.7%
無回答	34.1%	29.0%	34.1%

2.1.2 社外の従業者を対象とした訓練の注意点

自社内に席を置く委託先社員や派遣社員も自社と同じネットワーク下で外部のメールを受信する場合は、訓練対象に加えることが望ましい。しかし以下について注意が必要である。

・契約内容、個人情報利用目的の確認が必要
・情報セキュリティ活動、社内規程等、全般の適用が必要
・メール訓練に関し、教育やインシデント対応、通報先など一連の適用が必要

2.2 訓練回数の決定

メール訓練はゴール達成に向けて繰り返して実施する必要があるため、訓練対象者は一定期間内に複数回訓練を受ける形となる。本手引書では訓練対象者一人当たり一年間に受ける訓練の回数を訓練回数とする。訓練回数は目的、ゴール、また、企業規模等により異なる。

NCA 訓練 WG を対象に実施したアンケートにおける「訓練回数」は以下となる。

実施回数(年間回数)	第 1 回アンケート	第 2 回アンケート	第 3 回アンケート
1 回	41.7%	40.7%	42.5%
2 回	36.1%	37.0%	34.2%
3 回	8.3%	3.7%	4.1%
4 回	8.3%	3.7%	5.5%
5 回	0.0%	1.9%	2.7%
6 回	0.0%	1.9%	1.4%
7 回	0.0%	3.7%	1.4%
8 回	0.0%	1.9%	0.0%
10 回	0.0%	3.7%	4.1%
11 回	6.1%	1.9%	2.7%
12 回	0.0%	0.0%	1.4%

訓練回数は、訓練運用工数や訓練費用にも関係するため、本手引書に記載されている必要要素全体から検討することが望ましい。

2.3 訓練メール送信環境

訓練メールを対象者に訓練メールを送信する環境が必要である。訓練メールの送信環境は以下などがある。

例　・外部レンタルサーバ環境
　　・メール送信外部サービス（ＡＳＰ等）
　　・メール訓練外部委託

訓練メール送信環境は訓練対象範囲と件数、訓練回数により環境を選択する必要がある。訓練メールは攻撃メールを疑似的に再現するもので、外部の環境を使うことが望ましい。メール送信サーバによっては差出人アドレスが限定される場合や、メール送信数に上限が定められている場合があり確認が必要である。

送信環境の機能として、以下の機能が必要となる。

・訓練対象者全員にメールを送信する機能
・訓練対象者アドレスを送信先に設定できること
・送信者アドレスは訓練用ドメイン（「2.5　訓練用ドメインの用意」が利用できること
・メール本文中のリンク URL に個人別コード（訓練コード）を挿入できること

2.4　誘導先ページ（リンク先ページ、添付ファイル）の用意

誘導用のリンク URL をクリックしたとき表示されるＷｅｂページと、添付ファイルを開いたとき表示される「誘導先ページ」が必要となる。誘導先ページは訓練であることを明らかにする「種明かしページ」の役割に加え、リンク URL のクリックと添付ファイル開封の数値化のためのトラッキング機能も必要となる。

（加盟組織限定情報：誘導先ページの内容は、本手引書の「6.2　誘導先ページ事例」を参考にすることができる。本手引書の誘導先ページ事例は NCA 加盟組織内にて二次利用を可能としている。）トラッキング機能については「2.7　メール訓練の検知・数値化設定」を参考にＷｅｂサーバの必要な機能を確認する必要がある。

2.5　訓練用ドメインの用意

メール訓練では、訓練メールの差出人とリンク URL にドメインが必要となり、訓練用にドメインを用意することが有効である。

①訓練メールの差出人アドレスのドメイン

メールの差出人アドレスはメール受信時に必ず確認する項目であるが、攻撃者は標的とする企業ドメインに類似したドメインを使って攻撃する場合がある。例えばドメインの文字の中の「o」(英文字) を数字の「0」にしたドメイン（類似ドメイン）などである。訓練ではその攻撃手法を再現するために訓練用ドメインとして用意することが有効である。

②リンク URL 用のドメイン

メール文章内に仕込まれたリンク URL も類似ドメインが使われることがあり、訓練用のドメインを使うことが有効である。

ドメインの取得と維持には費用がかかることを考慮する必要がある。また、訓練用のドメインではなく、自社の本物のドメインを使用する「なりすましメール訓練」の場合、外部サーバから自社ドメインのメールを送信するため届かない可能性があり、事前確認が必要である。

2.6　受信環境の調査

メール訓練の準備段階で訓練メールの受信環境の調査が必要である。メール訓練は外部からメールを受信する従業員全員を対象とすることが望ましいため、全員の環境として事務所内 PC だけでなく、モバイル PC、スマートデバイス、また、関連会社環境や派遣先環境も発生する場合がある。受信環境に加えメーラーの種類や関連会社でメールシステムが異なる場合なども確認が必要である。

2.7　メール訓練の検知・数値化設定

メール訓練ではゴール設定と連動した訓練結果の検知と数値化設定が必要である。

2.7.1 リンク URL 型訓練の検知・数値化設定

”リンク URL 型訓練メール”を用いたメール訓練では、クリック者を検知するためのリンク URL の設定が必要である。

このリンク URL は、訓練対象者が通常のメールと認識してメールを開き、メール本文内の「詳しくはリンク URL をクリックしてください」などの誘導通りにクリックしたことを検知し数値化する機能である。本手引書ではクリックを検知することをトラッキング、URL をトラッキング URL と記す。

・トラッキング URL の仕様

トラッキング URL は訓練対象者が特定できるコードを含める必要がある。

例：http://www.example.com?code=1234567

↑訓練コード（個人別コード）

訓練対象者の個別の訓練コードを採番する場合と、メールアドレスのアカウント部や従業員コードなど個人コードを使う場合もある。繰り返し訓練を行うことを想定し、いつの訓練であるかも判別できるよう「実施月」を追加するなどコードを工夫する必要がある。

例：http://www.example.com/?date=201905&code=1234567

↑実施年月　↑訓練コード（個人別コード）

※注意点

上記トラッキング URL 例は説明用であり、実際の訓練メールでは容易にコードが判別できないように工夫することが望ましい。

また、訓練コードが単純な連番であると、訓練対象者が故意にトラッキング URL の訓練コードを改ざんした場合に、他者のトラッキングとして記録されてしまう。訓練ではこの行為を回避する仕組みを導入することが望ましい。

例として、訓練対象者を特定するコードを連続したものや社員番号ではなく、ランダムな文字列を付加することで、正規でない他者トラッキングを軽減することが可能となる。

例：http://example.com/1.bmp?date=201905&code=LY0mz5j

2.7.2 添付ファイル型訓練の検知・数値化設定

”添付ファイル型訓練メール”を用いたメール訓練では、添付ファイルが開封されたことを検知する機能の設定が必要である。

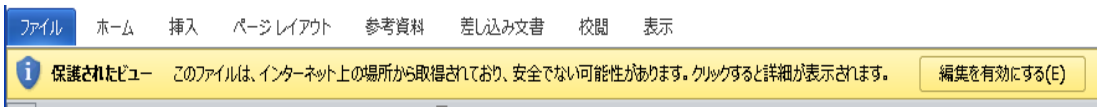
①Office ファイルの場合

Office ファイル（Word,Excel,PowerPoint）の添付ファイル型訓練では、開封者を検知する仕組みとして Web ビーコンを用いたトラッキングで集計を行う。Office ファ

イル内に小さな画像ファイルを埋め込み、Office ファイルを閲覧した際に発生する画像ファイルへのアクセスデータを基に開封者数を数値化する。Web ビーコンにはトラッキング URL と同様に訓練対象者を特定するコードを含める必要がある。

③ 添付ファイルに WORD ファイルを用いた場合の注意点

Web ビーコンを含めた WORD ファイルを開封すると以下の警告が表示される場合がある。



この状態は外部との通信が実施されないためトラッキングができない。トラッキングするためには開封した後に、訓練対象者に「保護されたビュー」の「編集を有効にする」をクリックしてもらう必要があるが、実際の訓練では徹底が難しい。したがって WORD ファイルの Web ビーコンを使った訓練は正しい数値化が難しい。(開封しても「編集を有効にする」を押さない人が発生する。)

WORD のセキュリティセンターの設定により表示状況が変わる為、事前の環境確認が必要である。

2.7.3 通報訓練の数値化

通報訓練数値化はクリックや添付ファイル開封の後に、訓練対象者が実施する通報行為を収集し数値化する。通報はインシデントエスカレーション手順と連動することが望ましく、「1.5　インシデント対応との関係確認」の連動も必要である。また、対象者のコードに加え「通報時刻」を収集する必要がある。クリック時刻と通報時刻の時間差は迅速なインシデント対応の妨げとなるため、遅滞なき通報が求められる。メール訓練においてはクリックから通報までの限界時間を定め、超えた場合は未通報として集計することも検討する必要がある。通報の収集方法は以下などがある。

・口頭、電話などによる通報受付

注意点：訓練規模により受付分散や訓練タイミングを分けるなど集中を防ぐ工夫が必要。口頭受付では通報者を特定する情報（部署名、氏名、メールアドレス、訓練コードなど）と通報時間をメモする運用を徹底する必要があるため、通報記録用紙を事前に用意することが望ましい。

・Web フォームやメールによる通報

注意点：ネットワーク経由による通報受付は自動的に数値化が可能であるが、「1.4　要求する行動の設定」と連動する必要がある。例えばインシデント初期対応で PC の LAN ケーブル抜線が定められている場合は、自分の PC でメール通報することはできない。口頭通報した上長からのメール通報やスマートフォンを活用するなど工夫が必要である。

2.7.4 数値化設定の注意点

リンク URL や Web ビーコンなどからの数値化設定は、訓練メールを受信するすべての環境でトラッキング可能であることが必要である。「2.6　受信環境の調査」の調査結果と「2.8

ネットワーク環境設定」などを参考に、設定段階からすべての環境で高精度に数値化できるよう準備が必要である。また、環境変化によりトラッキング不能にならないよう、環境変更に対応していく必要もある。

2.8　ネットワーク環境の設定

2.8.1 受信環境ホワイトリスト登録

訓練メールを受信するメールサーバの設定によっては、訓練メール送信時に以下の事象が発生する可能性がある。

・訓練メールが許可のない送信元からのメールとして拒否される
・訓練メールが迷惑メールと判定される
・同じ送信元から大量にメールを受信したことで迷惑メールや SPAM メール判定される

上記を回避するため、受信サーバにて下記情報のホワイトリスト登録を行うことが必要である。

・訓練メール送信元メールサーバのホスト名／IP アドレス
・訓練メールに使用する差出人メールアドレス

2.8.2 プロキシ設定の確認

社内からのインターネット接続においてプロキシ認証を行っている場合は、トラッキング通信のプロキシ認証について確認と対応方向を定める必要がある。

・トラッキング通信もプロキシ認証する設定
　実際の攻撃メールと同様の動きとなるが、プロキシ認証を行わないとクリック行動を検知できないため、クリック人数の評価に影響する。プロキシ認証まで行った人数として評価する形となる。
・トラッキング通信をプロキシ認証から除外する設定
　全てのクリック行動のトラッキングが可能となる。クリック行為に対するゴール設定を行った場合はプロキシ認証を除外した方が良い場合がある。訓練用ドメインを複数用意している場合は、全ての訓練用ドメインでプロキシ認証を除外するよう管理が必要である。

2.9　実際の攻撃メール情報の収集

最新のメール攻撃手法の把握と訓練メール文面の作成のために実際の攻撃メール情報の収集を行う必要がある。メール攻撃情報は以下などから入手することができ、継続した情報収集が望ましい。

・日本サイバー犯罪センター（JC3）
　犯罪被害につながるメール情報
　https://www.jc3.or.jp/topics/virusmail.html
・IPA 独立行政法人 情報処理推進機構
　標的型攻撃メールの例と見分け方
　https://www.ipa.go.jp/files/000043331.pdf

・一般財団法人 日本データ通信協会
迷惑メール相談センター
https://www.dekyo.or.jp/soudan/
・フィッシング対策協議会
緊急情報
https://www.antiphishing.jp/

2.10 安定したメール訓練環境の維持

自社で導入しているセキュリティ装置や利用しているメールクラウドサービスの迷惑メールフィルタ機能などが影響し、訓練メールが届かないことや、トラッキングができないことなど、メール訓練の不具合が多数発生する。準備段階で完全な環境準備は難しいため、継続した対応もメール訓練の必要要素であると認識すべきである。

メール訓練環境の不具合例として、以下などがある。

・不具合例：訓練メールが送信途中から迷惑メールに分類される
午前の送信は受信フォルダに届いたが、午後の送信は迷惑メールホルダに届いてしまう。学習型の迷惑メールフィルタによる影響の可能性がある。

・不具合例：HTML メールに変更すると迷惑メールに分類される
テキストメールから HTML メールに変更したところ、迷惑メールホルダに届いてしまう。HTML メールのリンク URL において、表現上の URL と実際にリンクする URL が異なる場合迷惑メールフィルタで迷惑メールに分類される場合がある。

3　メール訓練実施

メール訓練実施における送信準備と実施内容は以下となる。

3.1　次回メール訓練に向けた方向性決定

以下の再確認から次回メール訓練の方向性を決定する必要がある。

①メール訓練の目的、ゴールの再確認

繰り返し実施するメール訓練において、訓練実施の都度、目的とゴールを再確認する必要がある。

②ゴール達成の進捗再確認

前回の訓練結果、分析結果からゴールへの進捗度合を再確認する必要がある。

③前回メール訓練の課題の再確認

前回訓練の課題抽出から次回訓練における改善点を明確にする必要がある。改善点は訓練対象や訓練メール内容、さらに次回訓練の案内に反映させることが望ましい。

3.2　次回訓練メール送信日の決定

訓練方向性を踏まえ次回訓練メールの送信日を決定する必要がある。

①訓練メール送信日を中心として詳細スケジュールを策定することが望ましい。

②訓練メール送信日は訓練対象者に伝えないことが望ましいが、「○月下旬」など実施時期を案内に記載するやり方もある。

③訓練メール送信日は送信後の対応がスムーズに行えるよう、IT メンテナンスや重要イベントと重ならない設定が望ましい。実際の攻撃はいつ行われるかわからないが、訓練においては事後対応を考慮する形である。

④メール訓練よりインシデント対応の方が優先であり、もし送信日直前にインシデント対応が発生した場合は、送信日程を変更することが望ましい。またトラブル対応も優先することが望ましい。

3.3　次回訓練メール要素の決定

次回訓練方向性と改善点などから以下の訓練メール要素を検討することが望ましい。

① 訓練メールカテゴリの検討

（ばらまきメール、一般なりすましメール、業務なりすましメール、社内なりすましメール、広告宣伝メール、架空請求メール、フィッシングメール、脅迫メール、その他）

② 訓練メール分類の検討

（業務・周知系、業務・依頼系、社内・プライベート系、一般・プライベート系、その他）

③ 訓練メール難度の検討

（「株式会社ラック　標的型攻撃　対策指南書　第１版」より引用）

訓練メール難度	内容例
高難度	ウィルスを使って実際の業務メールを盗み出し、流用している 本文や件名は過去に送受信された業務メールであり、見分けることは困難。 添付書類もゼロデイが使用されるなど見極めは不可能。
中難度	業務に関連しているように見せかけたメールを攻撃者が作ったもの。 IPA などの Web サイトにある記述をそのままコピーして利用したもの。 自分に関わりの無い内容が書かれていた場合は、見分けられる可能性がある。 セミナーの案内等見分けが難しいものもあるが、添付書類は安易な実行ファイルレベル。
低難度	他国語が混ざっていたり、日本語の「てにをは」がおかしいなどの特徴を持つもの。 標的型攻撃に使われるなりすましメールの特徴をいくつか知っていれば、見分けられる可能性がある。
標的型メールではないもの	広告メールやフィッシングメールなど、不特定多数の人に送られたもの。 基本的なセキュリティリスクをいくつか知っていれば、見分けられる可能性がある。

NCA 訓練 WG を対象に実施したアンケートにおける、実施した訓練の「訓練メールの難度」は以下となる。

訓練メールの難度（複数回答可）	第 1 回アンケート	第 2 回アンケート	第 3 回アンケート
高難度	6	10	14
中難度	32	48	65
低難度	11	16	23

④ メール形式の検討（HTML メール、テキストメール）

HTML メール形式の場合、リンク URL をクリッカブルにすることで URL、訓練用ドメインをメール文面上見せない工夫ができる。HTML メールの場合はテキストメールも同時に送信する形（マルチパート）とする場合があり、その場合は html とテキストの両方の文面を用意する必要がある。

⑤ 導形式の検討（URL リンク型、添付ファイル型、URL フィッシング型）

NCA 訓練 WG を対象に実施したアンケートにおける「訓練メールの形式」は以下となる。

訓練メールの形式 （複数回答可）	第 1 回アンケート	第 2 回アンケート	第 3 回アンケート
リンク URL 型	28	47	64
添付ファイル型	23	33	50
フィッシングメール訓練（リンククリックだけでなく、アカウントを入力させるまで）	3	4	7
ランサムウェア型（身代金要求が表示されるもの）		1	0
その他		1	1

⑥ 差出人種類の検討

訓練メールの差出人は架空の差出人とする場合とホームページなどに公表している実在する人物を詐称する場合もある。組み合わせとしては以下となる。

	実在	架空
社内の人物	○※１	○
社外の人物	△※２	○

※１：社内の実在する人物の場合、事前に差出人実名使用の了解を得るとともに、問い合わせ対応を依頼する必要がある。

※２：「3.7　訓練用メールの作成」記載の訓練メール作成の注意点を考慮する必要がある。

⑦ 訓練メール種類数の検討

対象者全員に同じ訓練メールを送信する場合と、役職毎に変更する場合、また、ランダムに複数内容を送信することも有効である。同一の訓練メールを一斉に送信すると、訓練であることが周囲の行動から知ってしまうことがある。

3.4　訓練対象の決定とメールアドレスリストの準備

次回訓練方向性と改善点などから次回の訓練対象を決定し、対象となる最新のメールアドレスリストを入手する必要がある。

・メールアドレス収集の注意点

①メーリングリストなど複数アドレスに転送されるアドレスは除外することが望ましい。

②社員が直接受信する業務用アドレスや部署代表アドレスで、外部からのメールを受信する場合は「3.15.2 トラッキング 情報の集計」の注意点を考慮し、訓練に含めるかを決定する必要がある。

③1 名で複数のアドレスを持っている場合も、外部からメールを受信するアドレスは全て

訓練に含めることが望ましい。

④新入社員の訓練

最新のリストには新しい社員のアドレスが含まれており、初めての訓練となる。新しいアドレスを含めて訓練を行うか、別にするかを決定する必要がある。

⑤リスト入手から訓練メール送信までの新規採用者

メールアドレスの入手タイミングにより、訓練対象に含まれない社員が発生する。「部下に訓練メールが届いていない」などの問い合わせが発生する場合があり、問い合わせ担当と連携する必要がある。

⑥訓練を委託する場合のメールアドレスリストの取扱注意点

「4. メール訓練の委託の場合」に記載。

3.5 訓練案内

次回訓練に関する事前案内を行うことが有効である。主な事前案内例は以下となる。

案内対象	案内目的	案内内容	案内時期
訓練対象者（訓練目的によっては事前案内は不要）	訓練目的を理解し、円滑に訓練を進めるため	目的、対象組織、対象者（社員、役員、派遣社員、協力会社社員）、実施期間、開封時の訓練行動	訓練実施の１週前程度前
訓練対象者のセキュリティ部門担当者	対象組織のセキュリティ部門担当者訓練実施時に、訓練対象者からの問合せ対応のため （対象組織が大きい場合やグループ会社に対して実施する場合のみ）	訓練対象者への案内内容、訓練メールの内容、エスカレーション先、想定問答集	訓練実施の１ヶ月～１週前程度前
社内ユーザサポート部門	訓練実施時に、訓練対象者からの問合せ対応のため	同上	訓練実施の１週前程度
SOC、情報システム部門	訓練実施時に、実対応を阻害しないため メール送信元をセキュリティ機器のホワイトリスト登録をするため	メール送信期間、接続先 URL、送信元サーバ IP アドレス、エンベロープ From、ヘッダ From、メール件名、訓練対象組織、対象人数、メール送信間隔、メールタイプ（添付ファイル or URL リンク）、問合せ先	リハーサルの１週前程度前 ただし対象組織でのホワイトリスト設定が初めての場合は、余裕をもったスケジュールで事前案内することが望ましい

NCA 訓練 WG を対象に実施したアンケートにおける「訓練の事前案内実施状況」は以下となる。

訓練事前案内の実施	第 1 回アンケート	第 2 回アンケート	第 3 回アンケート
無	48.8%	59.7%	58.2%
有	34.1%	29.0%	24.2%
無回答	17.1%	11.3%	17.6%

3.6　メール訓練に関する教育

メール訓練には教育が必要である。教育は次回訓練方向性と改善点などから内容を追加・修正し、訓練実施前に実施することが望ましい。

実施時期は年間の情報セキュリティ研修に含める場合と、メール訓練の１ヶ月程度前に実施するやり方もある。また訓練実施時後に、開封者や未通報者に対し再度教育を実施することも有効である。

メール攻撃のベースとなる教育内容は以下などがある。

項目	内容	備考
教育の目的	標的型攻撃のリスクを理解し、不審なメールを開封しないこと。仮に不審なメールを開封しても適切な初動対応を行うことで、被害を最小限とすることが可能であること。	
標的型メール攻撃とは	標的型攻撃の仕組み、攻撃成功時の業務や会社への影響、近年の標的型メール攻撃による被害や実被害をうけた会社の例 人の脆弱性が狙われていることにも触れることが望ましい	IPA やセキュリティベンダが提供している資料を参考にするとよい
不審メールの添付ファイル開封時に要求する行動	「1.4　要求する行動の設定」の内容 行動はフロー化し、またイラスト等を用いることにより対象者が容易に理解できることが望ましい	NW 切離し方法は、無線 LAN 利用時についても触れる
利用者が気を付けるべき対策	不審なメールは開封しないこと、不審なメールの見分け方、不審なメールの実例。 業務上どうしてもメールを開く必要がある場合の方法（携帯のメールアプリを利用する等）	不審なメールの実例は、JC3（日本サイバー犯罪センター）で提供している情報を参考にするとよい

NCA 訓練 WG を対象に実施したアンケートにおける「事前教育実施状況」は以下となる。

事前教育の実施	第 1 回アンケート	第 2 回アンケート	第 3 回アンケート
無	46.3%	48.4%	44.0%
有	41.5%	38.7%	38.5%
無回答	12.2%	12.9%	17.6%

3.7　訓練メールの作成

次回訓練方向性と改善点、「3.3　次回訓練メール要素の決定」で決定した要素などから次回訓練メールを作成することが望ましい。訓練メール文面の作成は、「2.9　実際の攻撃メール情報収集」で収集した実際の攻撃メールを参考にする場合が多い。(加盟組織限定情報：また、本手引書の「6.1　訓練メール事例」を参考にすることもできる。本手引書の訓練メール事例は NCA 加盟組織内にて二次利用を可能としている。)

※訓練メール作成の注意点

IPA 独立行政法人 情報処理推進機構から「実在または酷似する組織名を使ったメールでの訓練は実施しないことが賢明」の注意喚起があり、詳細を確認する必要がある。

「組織における標的型攻撃メール訓練は実施目的を明確に」

https://www.ipa.go.jp/security/anshin/mgdayori20170731.html

3.8　体制、問い合わせ対応の再確認

決定した訓練メール要素、訓練メール内容から体制を再確認することが望ましい。実業務内容を訓練メールに採用した場合などは、実際の部署に問合せが発生るため対応依頼が必要となる。例えば訓練メールにインフルエンザ予防接種の案内を採用した場合、総務部門に問合せが発生するため、一次問合せ受付を依頼する必要がある。

3.9　リハーサルの実施

訓練メールの送信前にリハーサルが必要である。受信環境の変化により到着状況やトラッキングなどの技術的内容の再確認と、通報受付や問い合わせ対応など体制的な再確認を行うことが望ましい。確認範囲をカバーできるリハーサル対象者の選定とリハーサル案内、フィードバック協力も重要になる。

3.10　訓練メールの送信実施

準備が整った段階でスケジュール通り送信することが望ましい。

①送信開始時間、送信間隔、総送信時間

送信に必要な時間が送信対象件数、送信間隔に連動するため、訓練規模により送信監視時間を調整する必要がある。訓練メールを高速に一斉に送信すると、ほぼ全員が同時に受信し訓練であることが明確になってしまう。送信間隔（数秒）を持たせて送信することが有効である。

②送信に複数日数必要な場合

複数日で送信が行われる場合は、対応体制、工数など考慮し事業部単位や関連会社単位などで送信範囲を分けるやり方がある。

3.11 送信直後の対応

訓練メール送信直後から以下の対応を行うことが望ましい。

①受信状況、トラッキング状況の確認

リハーサルメンバーに受信状況の確認を行うことが望ましい。また、クリックまた添付ファイル開封を実施してもらい、トラッキング状況も確認することが望ましい。

②問い合わせ対応

「これは訓練ですか？」などの問い合わせが発生する。回答内容を決めておくことが望ましい。また、返答で訓練であることを明かす場合は、他訓練対象者への口外についても決めておくことが望ましい。

③社員への注意喚起対応

「1.6　社内規程等との関係確認」に従い、不審メールを社内で発見した際の注意喚起実施について決めておくことが望ましい。

3.12 トラッキング収集

「2.7 メール訓練の検知・数値化設定」の設定に基づきトラッキング情報を収集する。

※注意点

①転送による本人以外のトラッキング

業務に関連した内容の訓練メールの場合、上司が部下に転送する場合がある。その場合部下がクリックすると上司のクリックとしてトラッキングされる。

②人間以外のクリックの可能性

サンドボックスなどのセキュリティシステムがクリックと同じ動作をする場合もある。操作元のＩＰアドレスなどから判断し、除外する必要がある。

3.13 通報の収集

「2.7.3 通報訓練の数値化」に基づき通報情報を収集する。

※注意点

①通報必要事項の取り忘れ

口頭通報受付の場合、通報時刻の記録漏れが発生する場合があるため、通報記録用紙を定期的に確認し漏れのないよう収集することが望ましい。電話の場合は着信記録などを活用し、通報時刻を明確にすることも有効である。

②通報フロー途中の欠落

初期通報を上司、次に上司から事務局へ通報など通報フローが設定されている場合、途中で通報が滞る場合もある。「3.14 事後対応」のタイミングで役職者等、エスカレーション一時受付者に通報時刻の収集も含め、再確認することが望ましい。また途中で通報情報が滞っていいた場合は、フィードバック後に本人通報の確認をとり、集計値修正を行うことなどの対応がある。

3.14 事後対応

3.14.1 種明かし案内、訓練結果速報

訓練を実施したことをメールや社内掲示板などで案内する。種明かし案内や訓練速報などであり、今回のメール訓練の改善ポイントや訓練メール内容と見抜きポイントなども伝えることが望ましい。

NCA 訓練 WG を対象に実施したアンケートにおける「種明かしタイミング」は以下となる。

種明かしタイミング	第 1 回アンケート	第 2 回アンケート	第 3 回アンケート
開封時 ＆ 訓練終了時	19	23	36
開封時	11	20	22
訓練終了時	7	8	14
無回答	5	8	16
その他		3	3

3.14.2 全体アンケート

メール訓練実施後に訓練に関するアンケートを実施することも有効である。種明かし案内と同時にアンケートも実施するやり方がある。アンケート項目は訓練に気が付き、クリックしなかった対象者からの情報収集項目を含めることが望ましい。また、教育内容や課題からアンケート項目を追加することも必要である。

アンケート項目例

Q．メール訓練に関する教育を受けましたか？
Q．メール訓練があることを知っていましたか？
Q．訓練メールに気が付きましたか？
Q．不審なメール（訓練メール）をどの時点で気付きましたか？
Q．メール訓練の事前予告は必要ですか？
Q．メール訓練は役に立ちましたか？
Q．メール訓練の継続を希望しますか？

3.15 訓練結果集計

3.15.1 集計期間

メールを参照するタイミングは受信者で様々であり、トラッキング情報を集計する期間（送信日からトラッキング情報を集計に採用する日数）を定める必要がある。訓練対象者の規模や休日数なども関連するが、約 1 週間程度である。また種明かし案内までを集計期間にする場合もある。

3.15.2 トラッキング情報の集計

集計期間を過ぎた段階でトラッキング情報からクリック人数（または添付ファイル開封人数）を集計する。クリック情報（または添付ファイル開封情報）では同じ従業員が複数クリ

ックする場合もあるが、最初のクリック情報のみを重複しないように使用し、その時刻を集計に使う。最終的なトラッキング集計結果として、訓練対象者を特定できるコード（訓練コード）と検知時刻（クリック時刻）のクリック者リスト（添付ファイルの場合は開封者リスト）が作成されることが望ましい。

※トラッキング情報の集計の注意点

メーリングリストや業務用、部署代表アドレスに送信した訓練メールがクリックされた場合、クリックした従業者が特定できない場合がある。属性別集計とフィードバック、フォローに影響するため、他のログ情報を活用しクリック者を特定するか、または、代表アドレス類は集計から除外することが望ましい。

3.15.3　通報情報の集計

通報情報の集計は、以下の手順となる。

①クリック者リストの訓練コードをキーとして通報者情報を追加（消込）する。その際通報時刻も追加する。

②クリック時刻と通報時刻の差を算出する。インシデント発生時の手順で通報時間が定められている場合は、通報時間を超えた通報を未通報者扱いとする。

③通報情報のあるクリック者を通報者とし、通報情報のないクリック者を未通報者とする。

④通報者数を集計し、通報率を決定する。

通報率＝通報人数÷クリック人数（または開封人数）×１００

※通報情報集計の注意点

クリック者リストに無く通報のみ行われる場合がある。これは訓練メール参照しただけで通報された場合と、トラッキングができなかった場合などに発生する。この場合、クリックと通報の両方にリストに追加するか、両方とも追加しないか、集計方法を決定することが必要である。

3.15.4　属性別の集計

「クリック者リスト」（添付ファイルの場合は開封者リスト）と「通報者集計」が完了すると属性別集計に進むことができる。属性別集計方法は以下などがあるが、訓練目的とゴールなどにより集計方法を決定することが望ましい。また従業員属性を使う場合は、「1.7　訓練対象者個人情報の確認」を再確認する必要がある。

属性別集計例

・組織対象別、地区別集計　など
・役職別集計、入社年数別集計、雇用形態別集計、従業員種類別集計　など
・環境別集計（受信環境別など）
・行動別集計（クリックまでの時間、通報までの時間集計など）

属性別集計は訓練単位に行うことに加え、訓練対象者一人ひとりの履歴を管理し、継続した集計を行うことが望ましい。その中で複数回クリックや連続クリック、また、複数回未通報、連続未通報などを集計することができる。

3.16 全体アンケート集計

全体アンケートは訓練に気が付き、クリックしなかった対象者からの情報を集計することができる。例えば事前教育で「不審なメールの見分け方、不審なメールの実例」を強化し、その特徴を盛り込んだ訓練メールを採用した場合に、アンケートでその効果を測定することができる。アンケート回答は訓練を重ねることで変化するため基本質問は継続して集計することが望ましい。

3.17 課題の明確化

訓練結果集計とアンケート集計などから訓練ゴールの達成度を把握し、課題を明確にすることが望ましい。通報訓練の場合は「3.18　フィードバック」と「3.19　フォロー」の中で未通報者からの情報を収集した後に課題をまとめることが必要である。また訓練運用についても課題抽出することが望ましい。

3.18 フィードバック

フィードバックは設定したゴールを達成させるため、訓練対象者、対象組織に情報提供することである。フィードバックは以下などがある。

①基本情報のフィードバック

- 今回の訓練内容、訓練メール内容
- 判別訓練の場合は訓練メールの見抜きポイント
- 全体集計結果、推移、ゴール達成度、属性別集計
- 全体アンケート集計結果
- 課題

②個別フィードバック（改善を要する訓練対象者、対象組織）

（クリック率をゴール設定した場合）

- クリック者および管理者にクリック実施について（クリック時間等）
- クリック者に対し累積回数

（通報率をゴール設定した場合）

- 未通報者および管理者にクリック情報と未通報について
- 未通報者に対し累積回数、連続状況

③発生理由の確認

個別フィードバック時にクリック理由や未通報理由などの報告を求めることが有効である。

※個別フィードバックの注意点

フィードバック者から「クリックしていない」と苦情を受ける場合がある。トラッキング情報からクリック者を特定しているため誤検知の可能性があり、トラッキング

ログの再確認を行い、クリック行為を断定できない場合は、集計結果を修正することが必要である。

3.19 フォロー

フォローは設定したゴールを達成させるため、具体的な改善を行うことである。フォローには以下などがある。

・開封者フォロー
・未通報者フォロー
・複数回開封者フォロー
・複数回未通報者フォロー

改善内容は以下などがある。

・発生理由の報告内容から改善ポイント明確化と指導
・再教育

※フォローの注意点

「1.6　社内規程等との関係確認」の注意点にもあるが、改善指導において制裁事項や人事考課に関係させないことが重要である。また叱責することも避けるべきである。フォローは対象者の上司など身近な管理者が行うことが良いが、叱責など責めることのないよう、フォローする側への情報提供、教育も必要である。

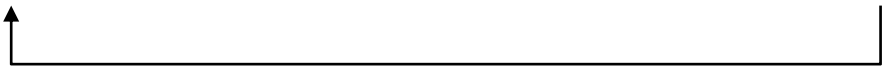
3.20 経営層への報告

CSIRT 活動として、また情報セキュリティ活動やリスクマネージメント活動としてメール訓練結果を経営層へ報告することが望ましい。標的型攻撃からのリスク軽減（低減）の進捗報告となることが望ましい。

3.21 メール訓練改善検討

メール訓練の概要は以下のサイクルとなるが、繰り返す中で改善検討が必要である。

訓練案内 → 訓練対象決定 → 訓練メール送信 → 測定 → 集計 → フォロー



また、改善は以下の段階別の実施要素から選択と各要素の改善を検討するのも効果的である。

例：段階別の実施要素例

	案内	教育	送信	結果集計	課題抽出	ﾌｨｰﾄﾞﾊﾞｯｸ	フォロー
現状把握	○		○	○		○	
初期段階	○	○	○	○	○	○	
育成段階	○	○	○	○	○	○	○
抜打訓練			○	○	○	○	○

4　メール訓練の最適化に向けて

4.1　メール訓練手法検討サブ WG 活動：学術連携

明治大学との学術連携活動において、企業文化とメール訓練の関係についてまとめていただきました。メール訓練の最適化に役立つ内容です。

標的型メール訓練と「褒める文化」

明治大学大学院経営学研究科　杉原大輔

（2020 年 2 月）

URL をクリックしてしまったり、開封してしまったことだけを取り上げて
過失やミス、さらには不審なメールを見極める能力不足として個人の責にすること
組織の対応として不適当
組織メンバーに期待される行動は「知らせること」
訓練の目標として考えるべきが「報告」

組織の情報セキュリティの向上に資するためには、「賞」を重視した訓練
*報告に**感謝**をしていますか？フィードバックはしていますか？*
報告が役に立ったという実感を持ってもらうことが、
次の報告行動につながります。

1）.「はじめに」

組織の情報セキュリティ推進において「褒める」こととの繋がりはあまりピンと来ないかもしれません。しかし、組織を構成するメンバーの人間的側面を考えれば非常に重要な役割を果たすものです。

企業組織における情報セキュリティは、システムとメンバーとが一体として展開される必要がありますが、メンバー全員がセキュリティ専門家になることはできないでしょう。しかし、専門家の手伝いをしてもらうことはできます。システムとメンバー、どちらに対しても期待されているのはインシデントを未然に防ぐことですが、完璧であることあり得ない以上、次善として期待されるのはインシデントに早期に対応できる「きっかけ」を提供することです。インシデントの予兆を専門家がいち早く知ることができれば、被害が小さいうちに対処し早期に復旧させることができます

組織の情報セキュリティを向上させるために、このきっかけをもたらす行動をいかに促進するかという点で、組織の文化としての「褒める」文化について標的型メール訓練を通して考えていきたいと思います。

2）.「企業文化」とは

企業組織の特徴を説明するために、それぞれの企業の持つ「文化」としてこれを紹介するビジネ

ス記事を目にしたことがあるのではないかと思います。

経営学においても多くの研究がなされていますが、そこでの企業の文化とは「企業組織（経営者）が標榜する価値（価値観）がメンバーに共有された状態」と説明されます。ここで言う「価値観」とは、何を重視しているかを示すもので、単純には、ある考え方やある行動が組織のメンバーとして「受け入れられる／受け入れられない」の判断基準のことを意味します。特に「受け入れられる」とはメンバーとして期待されている考え方や行動が取れているということです。そして「共有」とは、この価値観、すなわち何が受け入れられ、何が受け入れられないかが十分に理解され、個々人に内面化されていることです。

これらを踏まえれば、実務の上での企業文化とは、「会社が謳う理念やヴィジョンの達成において、何を重視しているのかが組織メンバーに理解され、それに沿った行動が当然のこととして現れている状態」と言えます。

価値観については、社是や理念、クレドといった呼び名において明文化されていることがあるかもしれません。しかし、共有についてはどうでしょうか。本当に重視しているものとしてメンバー個々人に内面化され、それが行動として現れているでしょうか。

3）.「セキュリティ重視を共有するためには」

会社が情報セキュリティを重視していることを共有するのならば、年頭の挨拶でそれを発信することも重要ですが、それだけでは不足です。メンバーに十分に共有されるためには、マネジメント層はそれを体現しなくてはなりません。たとえば、情報システムへの投資やセキュリティ人材の重用といったように、組織メンバーの目に見える形で示す必要があります。教育・訓練も投資の一つの形ですが、この文脈においては、マネジメント層も訓練に参加することや、訓練の結果に関心を持っていることを表現するといったことでしょうか。特に、訓練の結果に関心を示すことは重要です。これによって、訓練という投資に対するリターンをしっかりチェックしている姿勢が組織のメンバーに見えることになります。ここまですれば、年頭の挨拶で「言っていたこと」と実際に「やっていること」に一貫性を見出すことができ、「言っていること」を信用することができます。

ここで問題になるのが、何をリターンとしてチェックするかです。端的には訓練の目的となりますが、これもまた価値観のシグナルになります。そして、「チェックの後に何が待っているか」が重要です。これこそが、先に述べた価値観としての「何を重視しているのか」、すなわち「受け入れられる／受け入れられない」の線引きの理解を導き、これにより価値観の内面化の程度もまた変わることになります。

4）.「何をチェックするのか」：訓練の目的Ⅰ

さて、標的型メール訓練においては何を目的として、何をチェックするべきなのでしょうか。何を目的にするかについては、初めての訓練であれば、組織全体の健康診断が目的になるかもしれません。回数を重ねているのであれば前回との比較を通して事前の教育の効果の定着具合を測るといったように、訓練の頻度によっても変わり、訓練対象者の層や人数によっても変わります。もちろん複数の目的を持たせたせることもあるでしょう。

前提として、標的型メールについては、技術的なシステムを向上させても完全にシャットアウト

することは困難であり、本文の URL をクリックさせよう、添付ファイルを開かせようという攻撃者の技術と（悪）知恵のインセンティブが高い為、攻撃者側の意図が防御側の備えを常に上回る状態にあると言えます。そのため、標的型メールについての十分な知識と注意力を持っていたとしても、これを完全に避けることもまた難しいでしょう。

であるならば、URL をクリックしてしまったり、開封してしまったことだけを取り上げて過失やミス、さらには不審なメールを見極める能力不足として個人の責にすることは、組織の対応として不適当です。この点で、標的型メールであることを見極めることのみを訓練の目的とすることは不十分といえるでしょう。

5）.「チェックの後に何が待っているか」:訓練の目的Ⅱ

冒頭でも述べましたが、企業組織における情報セキュリティは、システムと人とが一体として展開される必要があり、どちらも完璧であることあり得ない以上、次善として期待されるのはインシデントに早期に対応できる「きっかけ」を提供することです。これに加えて、標的型メールは攻撃者側が常に優位であること、優れた人でもミスはあり得ることを前提とすれば、見抜く力の育成だけを目標にしても組織的なセキュリティの向上には限界があると言えます。であるならば、組織メンバーに期待される行動は「知らせること」であり、訓練の目標として考えるべきが「報告」となります。

ところが、本来の仕事に忙しいメンバーに、仕事よりも報告に優先順位をつけてもらうのはなかなか大変そうです。訓練であればなおさらかもしれません。しかし、本当のメール攻撃に遭遇した時のみならず、たとえ訓練であっても、メンバーには真剣に取り組んでもらわねばなりません。そのためには報告する側、訓練を受ける側にも何らかのインセンティブが必要です。

6）.「強化理論」と「誤った学習」

このインセンティブになるものが「チェックの後に何が待っているか」であり、組織のメンバーとして「受け入れられる／受け入れられない」ものを端的に示すものとしての「評価報酬」です。端的には「賞罰」ということになりますが、成功＝受け入れられることには報酬を、失敗＝受け入れられないことには罰を与えることで、その行動の制御をしようとする「強化理論」が原理であり、褒賞が与えられる行動は出現頻度が上がり、反対に罰が与えられる行動は出現頻度が減ることが期待されます。

では、多くのメンバーによって構成される企業組織においてはどうでしょうか。特にこの標的型メールや情報セキュリティの文脈においてはどうでしょうか。強化理論の基本に従えば、罰が与えられる行動は減少するはずです。であるならば、URL をクリックしたり、添付ファイルを開封することが罰の対象であるのならば、こういった対象に注意深くなり、減少することが期待できるかもしれません。

しかし、問題はもっと深層にあるのです。時々、罰を与えることが意図しない学習の成果を生むことがあります。それは、罰せられないようにミスをしないようにするのではなく、罰せられないようにミスを隠すようになることです。さらには、賞罰が発生する事由そのものを忌避したり、訓練の実施者を嫌悪するようになることもあり得ます。

クリックしてしまうこと、開封してしまうことが「個人のミス」として位置付けられているならば、ミスは恥ずかしい事であり他人には知られたくないと思うのは普通の事です。さらにミスがあれば罰せられるという図式が成立するのであれば、自らのミスを進んで開示することなど考えられません。それを隠そうとするのは人間の学習として自然なことです。

先ほど、インシデントへの早期の対処のための素早い報告の重要性について触れましたが、その反対に最も避けなければならないのは、クリックや添付ファイルの開封に気づかない、さらには気づいていても隠してしまうことです。気づかないことへの対処は、やはり知ってもらうしかないので、事前の教育研修が重要であることにかわりはありません。しかし、訓練を通じた意図しない学習として「隠すこと」はどのように防ぐことができるでしょうか。

7）．標的型メール訓練と「褒める」こと

訓練を通じた意図しない誤った学習を防ぎ、組織の情報セキュリティの向上に資するためには、「罰」の対象を再定義することと、「賞」を重視した訓練へと転換していく必要があるのではないでしょうか。

具体的には、クリックしてしまったこと、開封してしまったことそのものが個人のミスとして扱われることがないこと、問題となるのはそれを放置することであること、この反対に期待されることは早期に報告することである、ということを「訓練の結果をチェックすること」、すなわち賞罰を用いて示し、組織において「何が期待されているか」すなわち冒頭で述べた価値観の現れとしての「受け入れられる／受け入れられない」ものとしてコツコツ共有を図っていくしかありません。

しかし、訓練のたびに報奨金を用意するのは現実的ではありません。そこで登場するのが「褒める」ことです。人間集団において「褒める」こと、すなわち認知や承認は最も手軽な報酬といえます。この「褒める」ことは、教育やスポーツの分野でも重要なキーワードです。これらは、青少年に「自己効力感」を与え、自信を持たせることで自律的な行動を引き出すことにおいて有用であるとされるからです。そして、他者との関係において褒められることは「自己有用感」を与え、他者への貢献を引き出すことにつながります。これは大人の社会でももちろん同じです。

8）．「まとめ」

この賞罰と訓練の目的、冒頭の価値観との関連で整理するならば、

叱られること＝クリックや開封を隠すこと、報告しないこと＝期待されないこと
褒められること＝クリックや開封してしまっても早期に報告すること＝期待されること

という認識を明確に作ることであり、これを「訓練の結果をチェックすること」において「褒める」と「叱る」を明確に使い分けることで、組織にいかに定着させるかが重要なのです。

具体的には、ミスしたことではなく、報告しないことが罰の対象であり、これを叱らなくてはなりません。そして、ミスしたことを「褒める」のではもちろんありません。正直にミスを「報告す

ること」を「褒める」ことで引き出すことが求められます。
したがって、訓練の実務的な文脈では、「クリック率・開封率のゼロ」を訓練の目標として謳うことは、この達成を妨げるクリックや開封が叱責の対象と認識されやすくなるため、望ましくないといえるでしょう。むしろ標的型メールのバリエーションを知ってもらうには、工夫を凝らして開封率を上げることも一つの手段といえます。

であるならば、長期的に開封率の「低減」を目標とするとともに、「報告の 100%」を目標とすることが望ましく、これを「褒める」ことの徹底を通じて達成するのが早道なのです。
可能であれば、できるだけオフィシャルな場で、良好な結果であった部署や訓練実務を担う者を褒めてあげてください。そして報告しない者、不良な結果であった部署を叱咤激励してください。これこそが、経営者層が関心を持っているもの、重要視しているものをメンバーが理解する近道です。

先にも触れましたが、人間社会で生活する者にとって、他者から褒められること、認められること、堅い言い方をすれば認知や承認は社会的欲求を満たすものとして重要です。さらに、褒められている人、叱られている人を第三者として観ることも重要です。褒められていることは真似しようとし、叱られていることはやろうとしません。これを代理学習といいます。兄姉が両親に叱られているのを見て、弟妹は要領よく振舞うのです。（ちなみに筆者は長男です。）

9）.「終わりに」

これまで見てきたように、情報セキュリティが組織に十全に備わるために、特に早期のインシデント検知を人的に補完しようとするならば、そういった行動を引き出すために、その土台として「褒める」ことが組織に定着していることが重要です。「褒める」ことによって、情報インシデントに早期に対処する「きっかけ」を、組織メンバーに「報告」という振る舞いによってもたらしてもらうことを促進するのです。

コンプライアンスという言葉が当然のものとして用いられている社会環境である今、企業組織において何らかの不手際や不祥事を隠すことは、組織の信頼をより大きく毀損するものとして、もっとも避けなければならない行動であると考えます。標的型メール訓練において報告しないことが世間からの非難の対象になるとはもちろん思えません。しかし、一事が万事です。隠すことによって難を逃れようとする姿勢が組織のどこかにあるとすれば、後々大きな問題へと繋がっていく芽が放置されていることが懸念されます。

もちろん、問題が起きないように各所に配慮しながら物事を進めることが第一義ですが、仮に問題が発生した時でも、それが正直に報告されれば問題の芽を早期に摘むことが可能となります。組織の情報セキュリティと同じ構図です。正直な報告を「褒めること」で引き出すこと、そして正直な報告が組織にとって有用であったと「褒める」ことで次の報告行動につなげることが組織のマネジメントにおいて必要なのです。

このように、標的型メール訓練だけではなく組織活動全般においても、組織の将来にとってより望ましい振る舞いを引き出し、組織に定着させる前提として「褒める」ことを重視し、共有された状態、すなわち「褒める文化」を組織文化の下地として持つことはが求められているのではないでしょうか。

（要約）

①セキュリティが重要であることが、本当に共有されていますか？

・読む。聞く。だけでなく「実感する」ことが重要です。

・訓練の結果に経営者層は関心を示していますか？組織のメンバーは経営者層の行動をよく観察しています。一貫性のない行動はすぐ見透かされます。

②「報告」の優先順位を高くつけてもらうために

・報告の簡便さを備えることが必要です。

・面倒なことはしたくありません。そもそも、どうやって？誰に？が分からなければ報告のしようがありません。

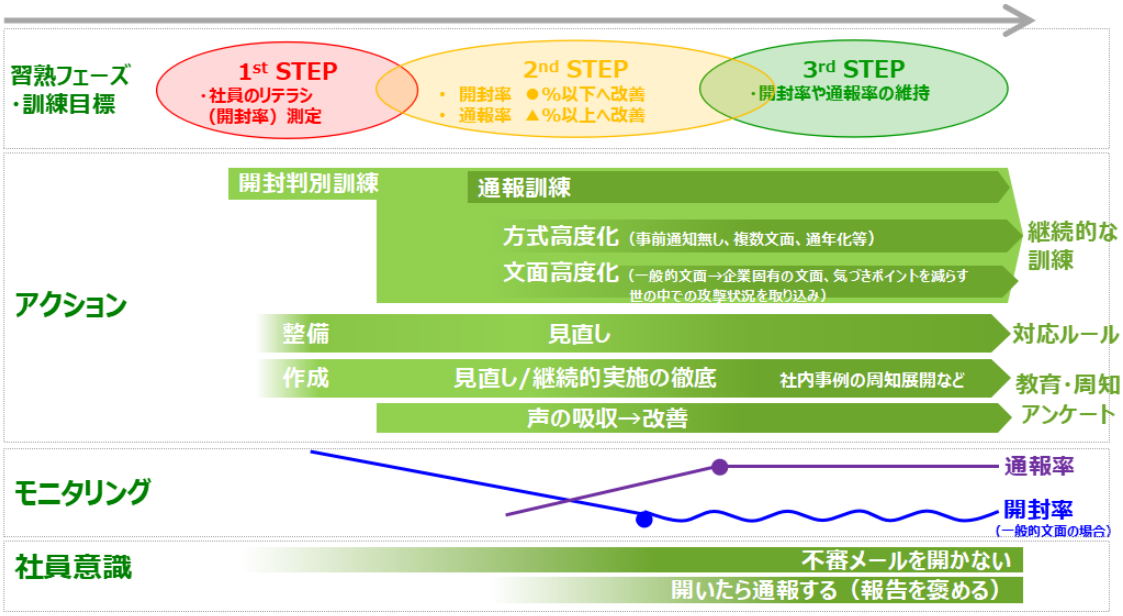
・報告に感謝をしていますか？フィードバックはしていますか？報告が役に立ったという実感を持ってもらうことが、次の報告行動につながります。

4.2　メール訓練の成熟度

メール訓練を繰り返し行う中で、難易度を高めて行くことや訓練を高度化するなどの「訓練の成長」が必要である。メール訓練サブ WG では訓練の成長を「メール訓練の成熟度モデル」として検討を重ね、2 つの成熟度モデルをまとめた。（モデル１、モデル２、それぞれの主担当者にてまとめ）

4.2.1　モデル１：開封率、通報率を指標とした成熟度モデル

メール訓練を実施した結果、訓練それ自身や、標的型メール攻撃に対応するためのさまざまな課題が浮き彫りになり対応が必要となる。それらの課題や対応事例について、メール訓練手法検討サブ WG での各社の訓練事例紹介や「8 メール訓練実施状況アンケート　集計結果関連資料」に記載のあるメール訓練実施状況アンケートの集計結果から、以下のようなメール訓練のモデルが浮かび上がる。



このモデルを活用することで、訓練実施各社のメール訓練における現状の立ち位置や、今後実施すべきメール訓練関連の施策の把握が可能となり、さらに経営層への状況報告や今後の施策説明にも活用が期待できる。

以下に上記モデルの説明を記す。

■ 習熟度

フェーズ	1st STEP	2nd STEP	3rd STEP
訓練目標	開封率の測定	開封率●%以下 通報率▲%以上	開封率や通報率の維持
説明	一時的な訓練を実施し、社員の標	1stSTEP の結果をうけて、**定期的に訓練を実施**	2nd STEP で訓練を継続的に実施した結果、開封

	的型メールに対する耐性、リテラシを測定する**現状確認のフェーズ。**	**し積極的に改善しているフェーズ。** 開封率や通報率に目標を設定し、アクションに記載する内容を実施し改善していく。	率や通報率が**目標達成後に、その状態を維持するフェーズ。** 今後もこの状態を維持し続けるためには、標的型攻撃メールに関する最新情報を入手し、それに対応していくことが重要である。

■ アクション

項目		解説
訓練	開封・通報	1stSTEP では社員の不審メールに対する判別能力（耐性）の現状を確認する。現状確認後、社内での不審メールの対応（通報を含む）ルールの整備や教育を実施したのち、通報を含めた訓練を実施していく。
	方式高度化	難易度を上げていくための訓練方式の高度化の方法としては、①訓練実施頻度、②複数文面の利用、③事前通知の有無があげられる。①については、はじめは非定期のイベントとして実施し、徐々に定期的な実施に切り替える。②については、例えば複数文面で訓練を実施することによりネタバレや最初の受信者が訓練であることを周りに展開してしまうことによる訓練効果の低下を防ぐことができる。③については、完全に事前通知をしない方法もあるが、事前通知はするが通知から訓練日までの時間をあけることで、難易度をあげる方法もある。
	文面高度化	はじめは一般的に世の中で出回っている文面で実施し、開封率が下がってきたことを確認したのち、文面を高度化していく（例：識別ポイントを減らす、企業固有の知識・用語をメール文面に含める） 参考：「3.3 次回訓練メール要素の決定」
対応ルール		訓練メールの添付ファイルやURLリンクを開いた場合の行動や、不審メール受信時の行動をルール化、文書化し社内イントラ等で周知する。 またルールは一度整備した後も、社内外の状況を見ながら、見直しをしていくことが重要である。 参考：「1.4 要求する行動の設定」

教育・周知	教育内容としては①標的型メールの手口と脅威、②メールの添付ファイルや URL リンクを開いた場合の行動、③不審なメールの見分け方　などがある。①、③については、はじめは IPA やセキュリティベンダなどが提供している一般的な教育資料で教育を実施し、徐々に社内外での最新の事例を取り入れて更新していくことが望ましい。 また教育もイベント的に非定期に実施するものから、徐々に定期的な実施に移行し、さらに新規参入者に対しても漏れなく確実に教育を実施する仕組みを整えることにより教育効果の向上が期待できる。 参考：「3.6 メール訓練に関する教育」
アンケート	メール訓練実施後に訓練に関するアンケートを実施することで、社員の訓練に対する意識や教育の効果などを確認できる。その際には訓練全体で気づいた点なども自由記入欄として設定することで、訓練の改善に関する声を収集することができ、今後の訓練の改善にフィードバックができる。 参考：「3.14.2 全体アンケート」

■ モニタリング

項目	解説
開封率	訓練開始当初は十数パーセントを超える開封率となることもあるが、訓練や教育を繰り返し実施していくことで１桁台（一般的には5%前後）まで抑えることが可能になる。 １桁台到達後の注意点としては、社員は業務多忙の中で、どうしても開封してしまう場合もあるため、無理な数値（開封者ゼロ＝開封率０％）などを目標にはせずに、その値を維持することを目標とするのがよい。 なお開封率はメールの難易度に大きく依存するので、モニタリングする際には、複数文面を用意し、そのうちの難易度を固定した文面の結果に対してモニタリングする必要がある。
通報率	通報率は開封率と違い、方式や文面の難易度には左右されず、また訓練や教育の効果があれば、値の着実な上昇がみられるので、重要なモニタリング指標である。

■ 社員意識

項目	解説
開封や通報に対する意識	訓練や教育を繰り返し実施していくことで、「不審なメールは開かない」「不審メールの添付ファイルや URL を開いた場合には通報する」という標的型メール攻撃に対応するための重要な行動が、社員の意識の中や、会社での基本的動作として定着していく。 そのためには訓練の運営組織においては、不審なメールを受信した、添付ファイルを開いてしまった場合の通報や報告に対し「褒める」ということを意識して運営していくことも重要である。 参考：「4.1 メール訓練手法検討サブ WG 活動：学術連携」

4.2.2　モデル２：訓練メールの難易度を指標とした成熟度モデル

今まで攻撃メール訓練は、『メール文面の難易度』が攻撃メール訓練レベルの評価基準、そして『開封率』が訓練結果に対する評価基準であった。訓練初期は攻撃メール訓練を行うことがゴールだったが、訓練を行うにつれ、より効果を高まる実践的な訓練を行うようになってきた。すると、訓練を多く行っている方が、開封率が上がる（訓練結果が悪くなる）という逆転現象が発生した。そこで、訓練結果に波及する訓練要因を定義し、『攻撃メール訓練成熟度』というモデルを新たに作成した。攻撃メール訓練の目的は、攻撃メール訓練の開封率を下げるだけでなく、訓練の事前・事後アクションを通じてセキュリティレベルを上げることである。このため、このモデルでは、CSIRT 等セキュリティ対策統括組織が行う訓練を対象としている。なお、訓練のみを実施する組織でも、監視や教育等を行うセキュリティ組織と連携すれば問題ない。

考え方：

（１）訓練成熟度の判定基準

①訓練メール

文面の種類、内容、文面の成熟度（文面の難易度）

②開封率収束値（参考値）

一般的な文面による訓練は、正常性バイアスにより５％程度と言われているが、目標はあくまでも０％

（２）推奨事項

①教育

②アクション

攻撃メール訓練ツールは期間限定で教育コンテンツにアクセスできるようになっているが、永続的に公開できるよう専用ページによる公開や、規則・ガイドライン作成を検討すること

（３）レベル終盤における問題点

掲載している事象に該当すれば、次のレベルへのステップアップを検討

補足事項：

・訓練実施者の反応（感想）を把握することにより、よりセキュリティを向上させることが可能になるため、アンケートは実施する方が良い。

・訓練メール開封時に警告画面（訓練であることを開示）を表示せず、各組織のインシデント対応(通報や報告)させるなど､組織の管理方法に従ったやり方で良い。

・セキュリティ機器などによりその環境で受信しないメールへの訓練は不要だが、教育は必要である。

攻撃メール訓練成熟度

攻撃メール訓練成熟度

レベル		1	2	3	4	5
		初めの一歩	初級	中級		上級
訓練メール	種類	**ばらまき型**		**標的型攻撃 （組織内なりすまし、業務関連）**		**標的型攻撃 （サプライチェーンなりすまし）**
	文面の内容	**一般 ※組織固有ではない**		**組織固有 組織内状況・特性を考慮した訓練**		**組織固有 サプライチェーン攻撃 ※要事前調整**
	文面の成熟度	**低 ※たどたどしい日本語（レガシー）**	**中 ※普通の日本語**	中 ※普通の日本語	**高 ※トレンド、組織内フォーマット活用**	高 ※トレンド、組織内フォーマット活用
	開封率収束値	5%			なし ※内容次第で開封率は高くなる	
インシデント対応		なし（開封警告画面表示）	なし（開封警告画面表示）		なし（開封警告画面表示） **or あり（開封警告画面表示なし）**	
対外組織連携		なし	なし	なし	なし	**あり** ※なりすまし先と要調整
教育		一般的知識（攻撃メールレガシー）	組織固有（人的・管理的対策）	組織固有（組織内環境）	組織固有（技術的対策）	ガイドライン（対策全般）
アクション	事後教育 ※暫定対策	**・訓練メールで気づくポイント 送信元詐称方法 ・一般知識 例）攻撃メールの特徴 被害事例**	・訓練メールで気づくポイント ・一般知識 ・組織固有有知識 ①人的対策 a.予防策 b.インシデント対応	・訓練メールで気づくポイント ・一般知識 ・組織固有有知識 ①人的対策 a.予防策 b.インシデント対応 **②組織内状況 a.環境 b.攻撃メール受信状況**	・訓練メールで気づくポイント ・一般知識 ・組織固有有知識 ①人的対策 a.予防策 b.インシデント対応 ②組織内状況 a.環境 b.攻撃メール受信状況 **③技術的対策 a.予防策 b.インシデント対応**	・訓練メールで気づくポイント ・一般知識 ・組織固有有知識 ①人的対策 a.予防策 b.インシデント対応 ②組織内状況 a.環境 b.攻撃メール受信状況 ③技術的対策 a.予防策 b.インシデント対応
	永続公開 ※恒久対策 ・CSIRTページ ・ガイドライン作成	―	**・組織固有有情報 ①人的対策 a.予防策 b.インシデント対応 ②管理的対策 規則・ガイドライン作成**	・組織固有有情報 ①人的対策 a.予防策 b.インシデント対応 ②管理的対策 規則・ガイドライン作成	・組織固有有情報 ①人的対策 a.予防策 b.インシデント対応 ②管理的対策 規則・ガイドライン作成 **③技術的対策 a.予防策 b.インシデント対応**	・組織固有有情報 ①人的対策 a.予防策 b.インシデント対応 ②管理的対策 規則・ガイドライン作成 ③技術的対策 a.予防策 b.インシデント対応
レベル終盤における問題点		・マンネリ化により、訓練をまじめに受けなくなる ・ユーザーがインシデント対応方法を知らない ・事後教育が一過性のページで公開されている ※知識が蓄積されない	・マンネリ化により、訓練をまじめに受けなくなる ・訓練メールが簡単すぎる。 **・この訓練を行う理由がわからない ※社内状況を把握していない**	**何度やっても、開封者が発生する ※人的対策の限界** 対策が訓練ごとに公開され、新規着任者は把握できない 例）過去に掲示板に掲載された前回訓練対策で公開された	**実際の攻撃の緊迫感がない**	

4.3　テレワークにおけるメール訓練の工夫すべき点

メール訓練サブ WG では、コロナ禍、テレワークにおけるメール訓練の実施について議論するとともに、第 3 回メール訓練実施状況調査にてテレワークにおけるメール訓練の実施について調査した。

4.3.1 テレワークにおけるメール訓練実施状況　調査結果（テレワーク調査回答数は 51 件）

①「コロナ禍にメール訓練を実施しましたか？」

コロナ禍にメール訓練を実施	第3回アンケート
実施した(実施予定含む)	60.8%
見送り中	15.7%
無回答	23.5%

②「テレワーク者をメール訓練の対象としていますか？」

テレワーク者をメール訓練の対象としているか	第3回アンケート
対象としている(対象とする予定含む)	70.6%
対象としていない	0.0%
無回答	29.4%

③「テレワーク時の不審メール対応について教育を行いましたか？」

テレワーク時の不審メール対応の教育実施	第3回アンケート
実施していない(テレワークによって教育内容を変えていない)	56.9%
実施した	23.5%
無回答	19.6%

④「テレワーク者のメール受信環境をお答えください。(複数回答可)」

テレワーク者のメール受信環境	第3回アンケート
仮想デスクトップ/VDI環境で受信	20
会社支給PCからVPN経由で受信	31
会社支給PCからインターネット経由で受信	12
会社支給スマホ	23
個人PC	2
個人スマホ	3
その他	0

⑤「テレワーク者が不審メールを受信した際に求めている行動を定めていますか？」

テレワーク者の不審メール受信時の行動	第3回アンケート
特に定めていない(通常勤務と同じ行動)	84.3%
テレワーク用の行動を定めている	0.0%
無回答	15.7%

⑥「テレワーク者が不審メールの URL をクリックした際に求めている行動を定めているか？」

テレワーク者が不審メールのURLクリックまたは添付ファイルを開封した際に求めている行動	第3回アンケート
特に定めていない(通常勤務と同じ行動)	78.4%
テレワーク用の行動を定めている	0.0%
無回答	21.6%

⑦「テレワーク時の通報手段を定めていますか？」

テレワーク時の通報手段	第3回アンケート
特に定めていない(通常勤務と同じ行動)	82.4%
テレワーク用の行動を定めている	0.0%
無回答	17.6%

4.3.2 テレワークにおけるメール訓練の工夫点

テレワーク時のメール訓練の工夫点として、アンケート結果と WG 内協議から以下が挙げられる。

① 特に工夫せず、従来通りメール訓練を継続する。

アンケート結果から分かったこととして、テレワーク者に特別な対応を求めることは行われていない。また、実際のメール訓練の結果においてテレワーク者に差は発生していない。したがってテレワーク者が含まれても特別な工夫は不要と言える。ただし、不審メール受信時の行動や通報手段など、テレワーク時にも実行できる内容が定められ、教育されている必要がある。

アンケート結果：「メール訓練結果において、テレワーク者に差がありましたか？」

メール訓練結果において、テレワーク者に差があったか	第3回アンケート
差はなかった	43.1%
差があった	0.0%
無回答(テレワーク者を区別できない)	56.9%

また、WG 内の協議ではコロナ禍、テレワーク中のメール訓練は実施すべきであるとの意見がまとまった。不審メールによる脅威は出勤時と同様、また高い場合もあり、メール訓練を継続して実施することで、テレワーク中においても攻撃メールに対する

耐性を向上することができる。

②コロナ禍特有の攻撃パターンを取り入れる。

テレワーク時のメール訓練の工夫点として、訓練メールにコロナ禍特有の攻撃パターンを取り入れることが有効である。

訓練に取り入れたコロナ禍特有の攻撃パターン（WG内意見およびアンケート調査結果）
オンラインミーティング関係のトピックスを取り入れる
コロナに関する打ち合わせを打診する内容を取り入れる
利用が増えているウェブ会議システムのアップデートに関するメールを題材にする
社内Web会議システム関連の通知を偽装する
給付金詐欺を想定したメール文面を取り入れる
WEB会議サービスの会議招集を模したメールを取り入れる
コロナの話題のメール文章に取り入れる

5　メール訓練委託の場合

5.1　確認すべき事項

メール訓練を外部に委託する場合に、契約前に確認すべき事項の例を以下に示す。メール訓練検討時には、以下の項目の提供可否やポイントについて外部委託先に確認し、訓練目的やシステム環境に最適な外部委託先を選定することが望ましい。

カテゴリ		確認ポイント
メールコンテンツ	メールヘッダ	差出人偽装が可能か
	メールタイプ	添付ファイル形式が可能か メール本文の URL リンク形式が可能か
	メール本文	本文中に組織名や名前などを動的に挿入が可能か 例：○○部　佐藤様
	添付ファイル形式の種類	Word(doc,docx)、Exel,pdf など 対応可能なファイル拡張子まで
	URL リンク形の偽装	html メール形式による､URL リンク偽装が可能か
	URL リンクのパラメータ	パラメータが推測不可のランダムな値であるか
	メール文面数	１回の訓練あたりに送信できるメール文面数
	サンプルコンテンツ	サンプルコンテンツの種類や数
開封コンテンツ	開封コンテンツのサンプル	開封時のコンテンツの種類 コンテンツの自由度（通報連絡先の URL などが記載できるか）
トラッキング方式	開封時のトラッキング方式	方式によっては､社内のセキュリティ機器や設定により､トラッキングのための通信が遮断される可能性もあるので､事前に確認しておく
ドメイン	送信元アドレスドメイン ビーコン送付先ドメイン	委託先が保有するデフォルトドメインの種類と数 新規取得が可能か（追加費用の有無）
リハーサル	実施時期	訓練本番前に余裕をもったリハーサルができるか
	ホワイトリスト設定	メールサービスやセキュリティ機器などでメールがブロックされる場を想定し､適切なアドバイスできるか､経験があるか
開封ログ	ログの形式	ログの項目、形式、複数
	提供タイミング	初報（例：翌日）～最終報告タイミング

報告書	内容	開封率、組織別開封率※、役職別開封率※、他社との比較など （組織データや役職データなどの提供する必要あり）
	提供タイミング	訓練終了後数日後～1 ヶ月程度。報告書の内容により期間が
	報告会の有無	単純な開封率だけでない詳細報告書を求める場合には、報告会を開催し、外部委託先からの意見を施策にフィードバックする方法もある

教育やアンケートについても、提供可能な外部業者があるので、外部委託する場合にあわせて確認するとよい。

5.2 外部委託する場合の個人情報の取り扱い

従業員のメールアドレスは個人情報となるため、委託先への受け渡しについて契約による明確化と安全性確認を行うことが望ましい。また訓練メール送信用のアドレス以外に、転送メールがバウンスした場合にスマートフォンのアドレスや個人アドレスなども委託先に渡る場合があり、目的外利用の禁止と安全対策を明確にすべきである。

6　メール訓練実施状況アンケート　集計結果

メール訓練サブ WG では NCA 訓練 WG 参加チームを対象としたメール訓練実施状況アンケートを実施している。以下がアンケート集計結果となる。(加盟組織限定情報では全結果を記載)

アンケート項目一覧

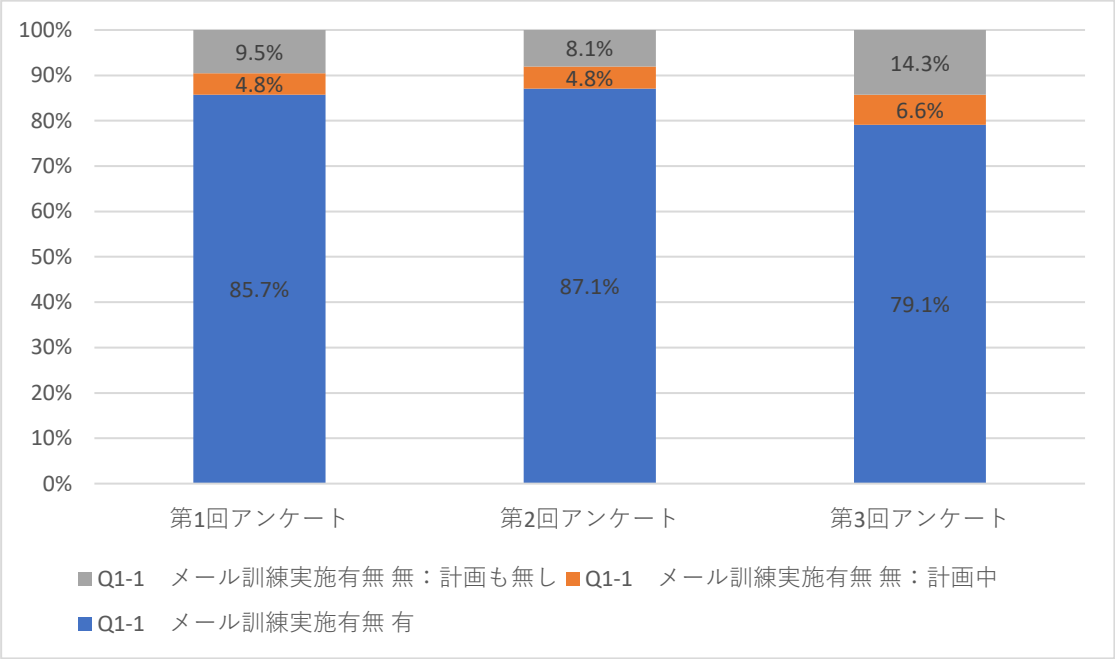
No.	アンケート項目
Q1-1	メール訓練実施有無
Q2	メール訓練実施回数
Q3-1	訓練対象（国内）
Q3-2	部分的 訓練対象
Q3-3	訓練対象 部分的
Q4-1	訓練対象（海外）
Q4-2	部分的 訓練対象
Q4-3	訓練対象 部分的
Q5	対象人数 年間の対象者数（実人数）
Q6	訓練事前案内の実施
Q7	事前教育の実施
Q8	訓練メールの形式（複数回答可）
Q8-2	訓練メールの難度
Q8-3	最も多く採用している難度
Q9	訓練メールの種明かしタイミング
Q10	訓練メールクリック者へのフォローアップ教育（添付ファイル開封者/URLクリック者/未通報者）
Q11-1	現在の訓練運用形態
Q11-2	運用形態の変更があった場合は、以前の運用形態をお聞かせください。
Q11-3	運用形態の変更を計画している場合、今後の運用形態をお聞かせください。
Q12-1	社内ルールにて通報を定めていますか？
Q12-2	通常時の通報方法（複数回答可）
Q12-3	社内ルールで定めている通知のタイミング（複数回答可）
Q12-4	社内ルールで定めている不審メールの添付ファイル開封/URLクリック時の初動対応（複数回答可）
Q12-5	不審メール受信時の運用（添付ファイル未開封/URL未クリック）（複数回答可）
Q13-1	メール訓練時の通報実施について
Q13-2	メール訓練時の通報方法（複数回答可）
Q13-3	メール訓練時の通知先（複数回答可）
Q14	訓練後アンケートの実施と対象（複数回答可）
Q15	結果集計・分析の実施（複数回答可）
Q16	訓練結果の報告内容（複数回答可）

Q21	訓練メールは何の為に行なっていますか。目的設定は何でしょうか。（複数回答可）
Q22-1	訓練のゴールを設定していますか？（クリック率〇〇%や通報率〇〇%など）
Q31-1	メール訓練の課題について
Q41-1	コロナ禍にメール訓練を実施しましたか？
Q42-1	テレワーク者をメール訓練の対象としていますか？
Q42-2	テレワーク時の不審メール対応について教育を行いましたか？
Q42-3	テレワーク者のメール受信環境をお答えください。（複数回答可）
Q42-4	テレワーク者が不審メールを受信した際に求めている行動を定めていますか？
Q42-5	テレワーク者が不審メールのURLクリックまたは添付ファイルを開封した際に求めている行動を定めていますか？
Q42-6	テレワーク時の通報手段を定めていますか？
Q43-1	メール訓練結果において、テレワーク者に差がありましたか？
Q43-2	どのような差がありましたか？（複数回答可）
Q43-3	メール訓練にコロナ禍特有の攻撃パターンを取り入れた場合は、概要をお聞かせください。
Q44-1	Emotetウイルスのメール攻撃に対する訓練を実施しましたか？
Q90	メール訓練の将来的な必要性についてどのようにお考えですか？

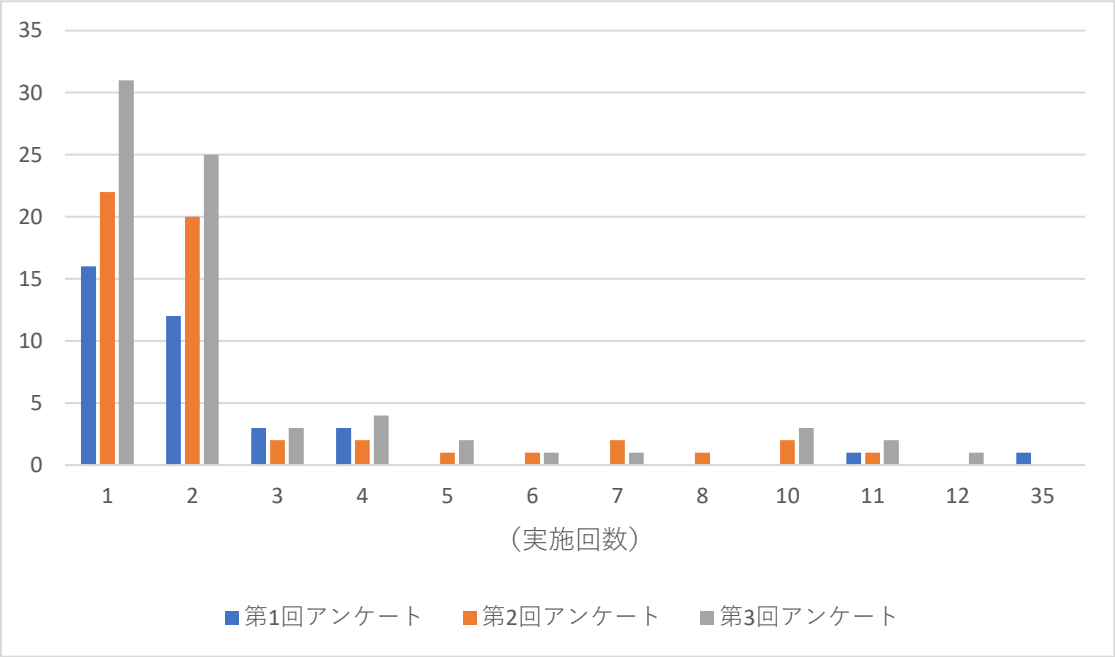
メール訓練実施状況調査結果

（傾向比較のため無回答を除いて再集計）

Q1-1　メール訓練実施有無

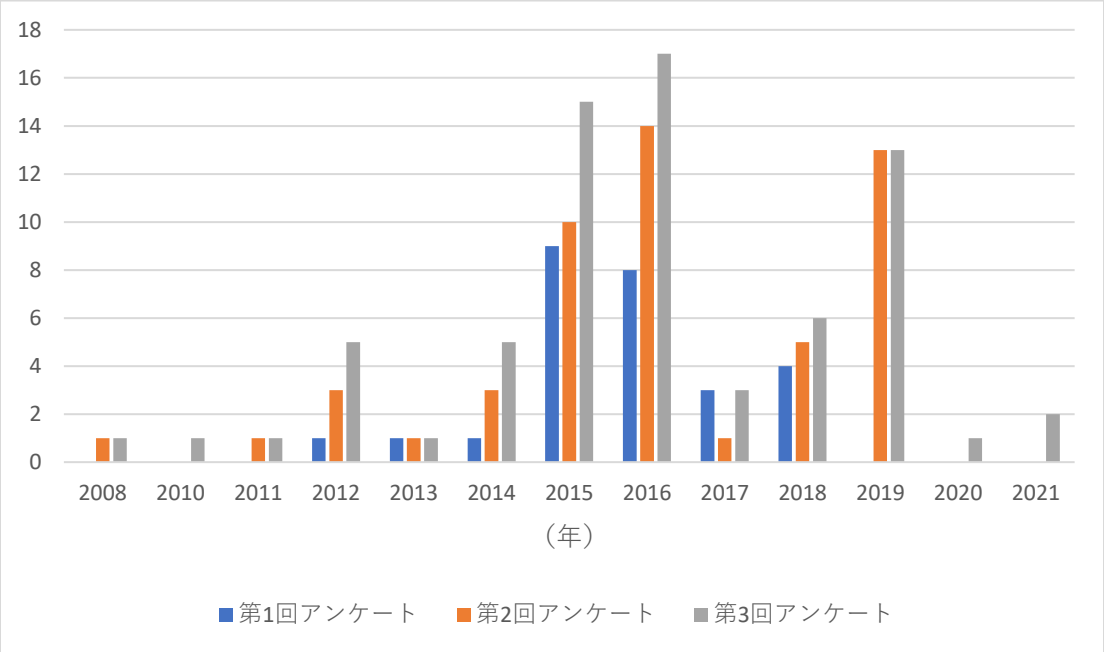


Q2　メール訓練実施回数

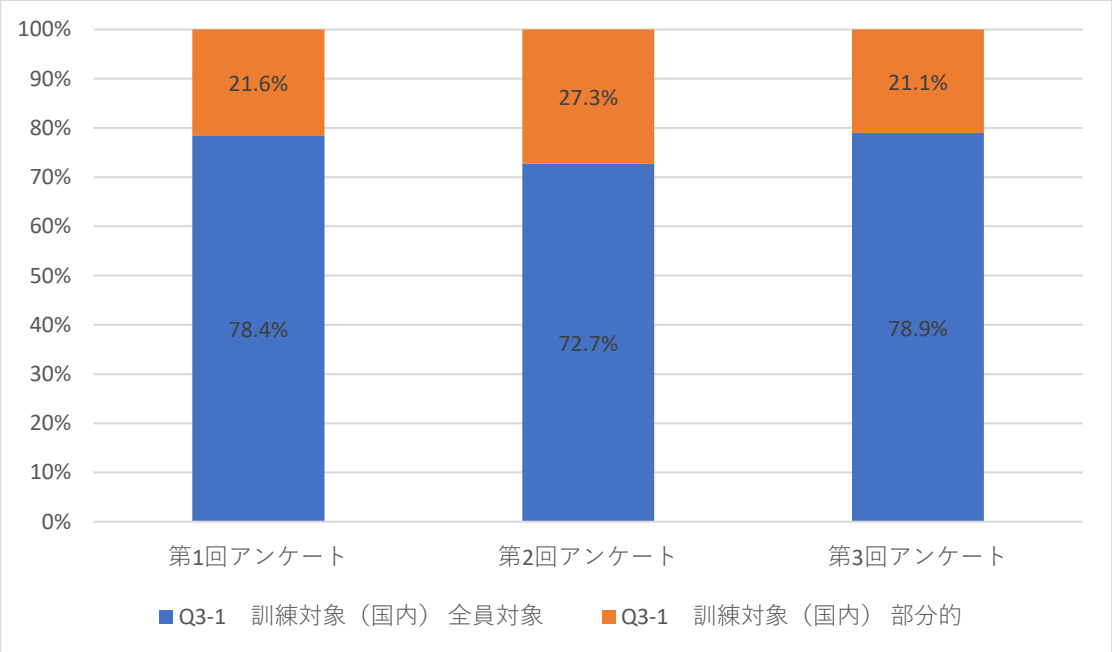


メール訓練実施状況調査結果

Q2-2訓練開始時期(年)

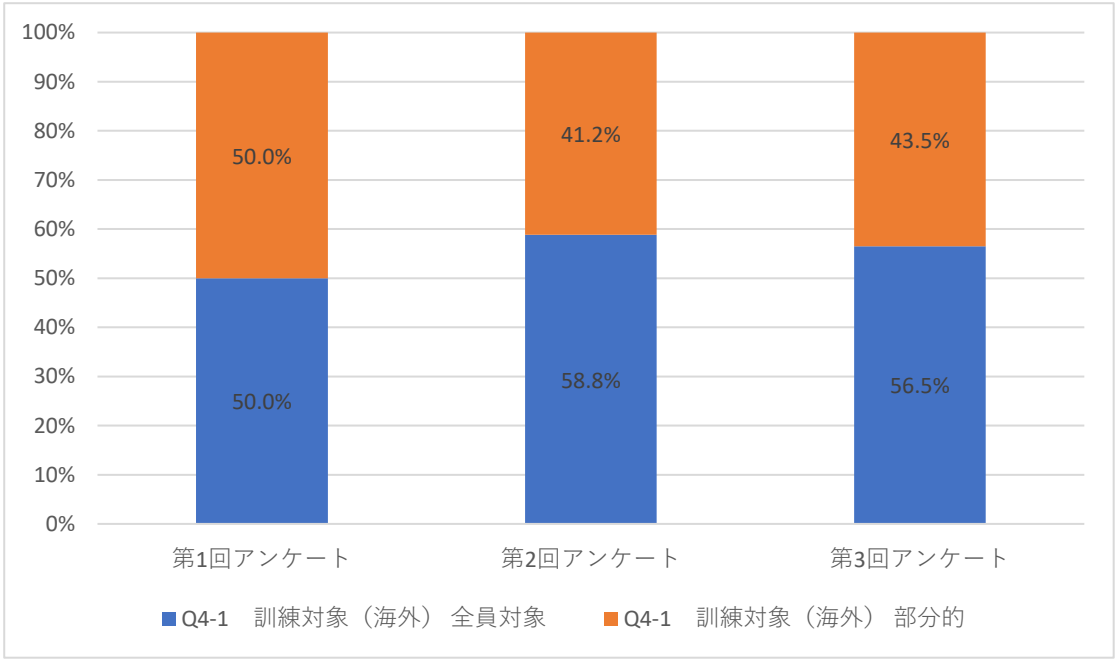


Q3-1　訓練対象(国内)

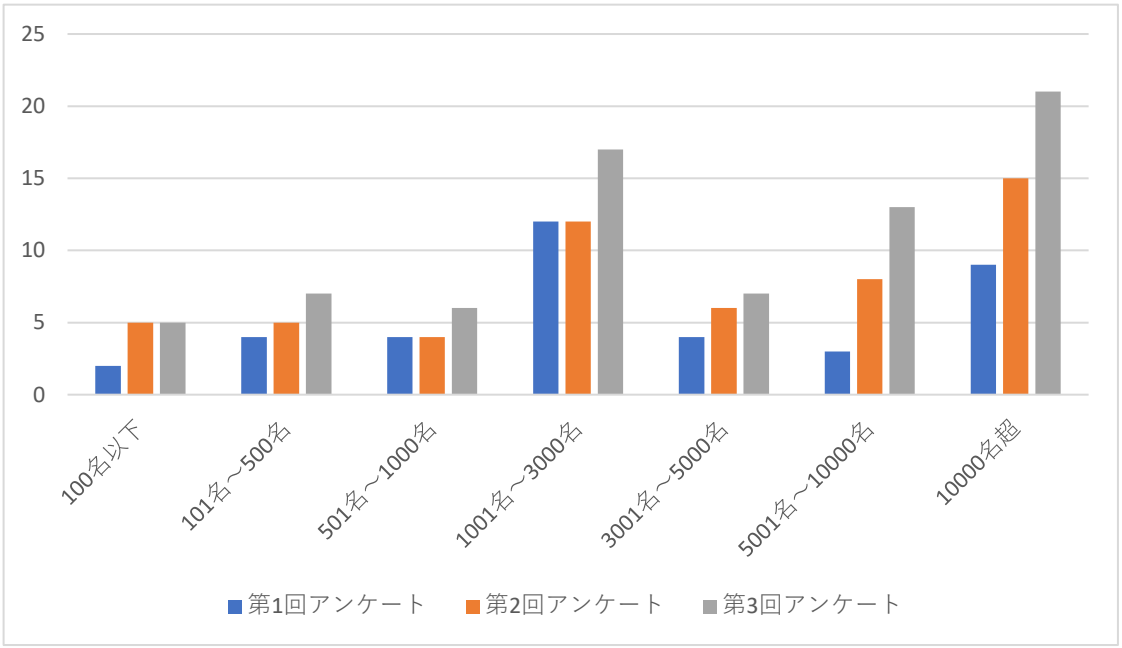


メール訓練実施状況調査結果

Q4-1　訓練対象（海外）

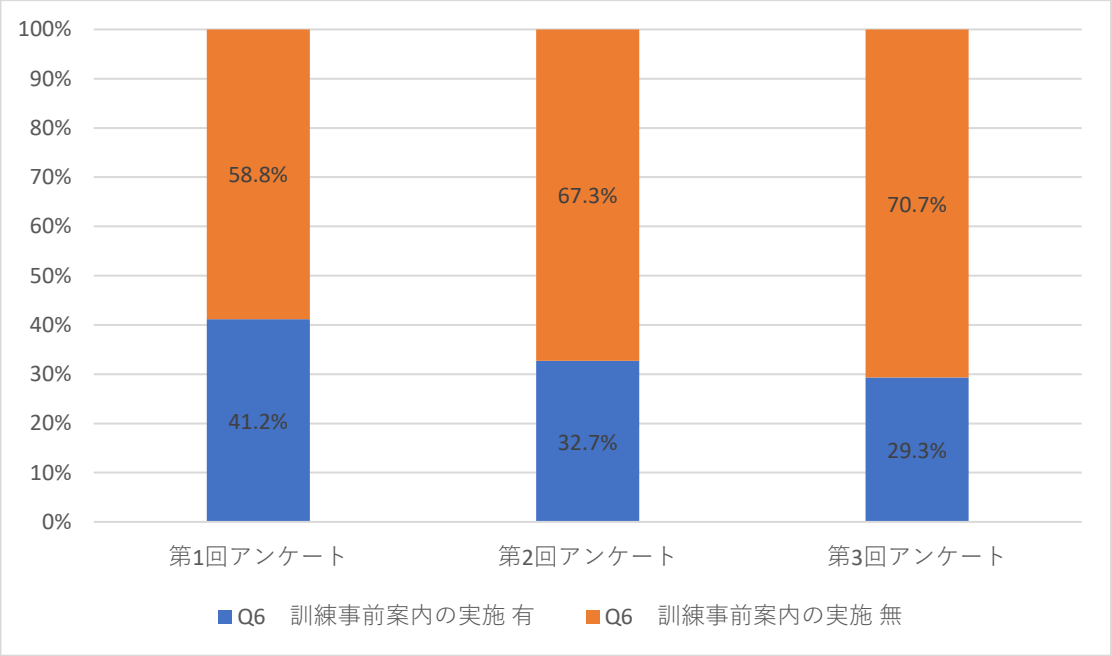


Q5　対象人数　　年間の対象者数（実人数）

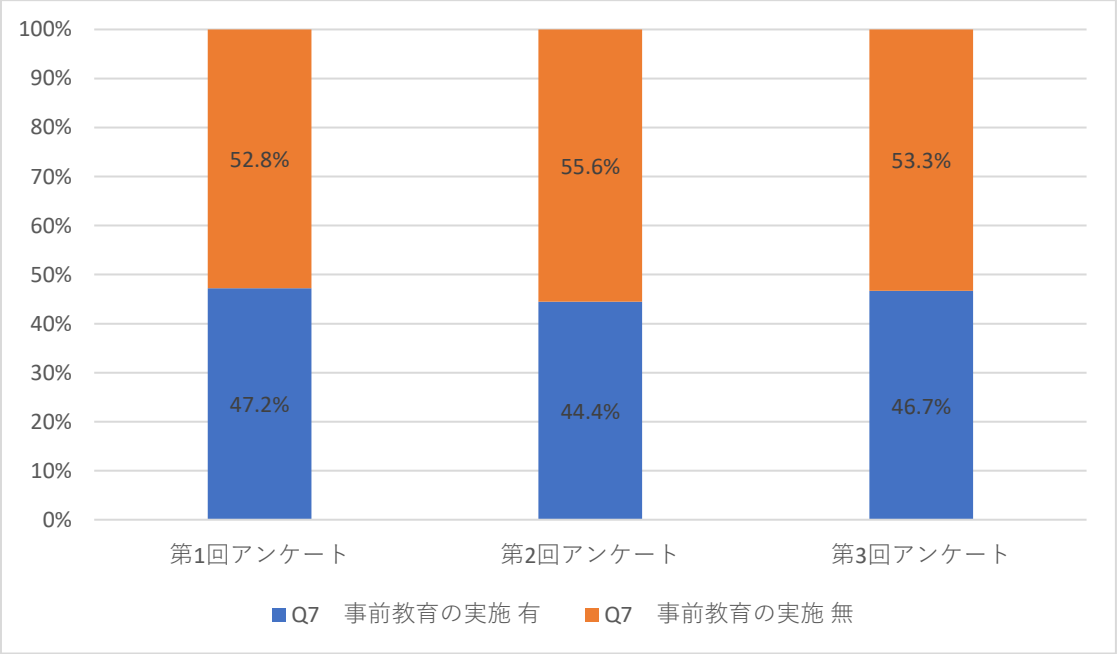


メール訓練実施状況調査結果

Q6　訓練事前案内の実施

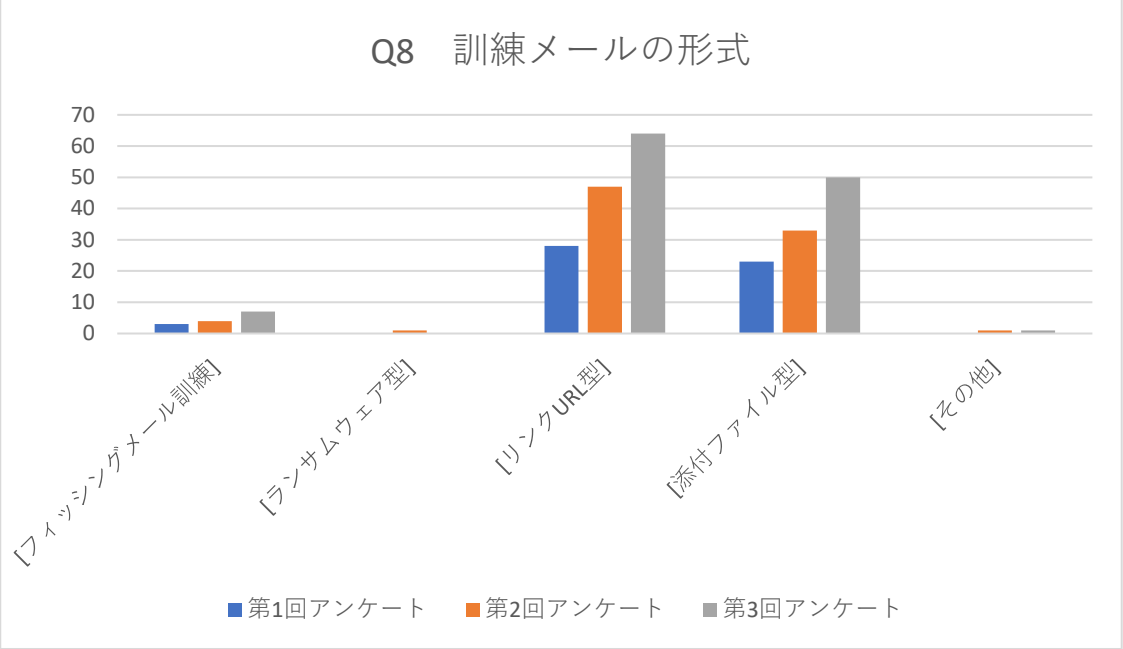


Q7　事前教育の実施

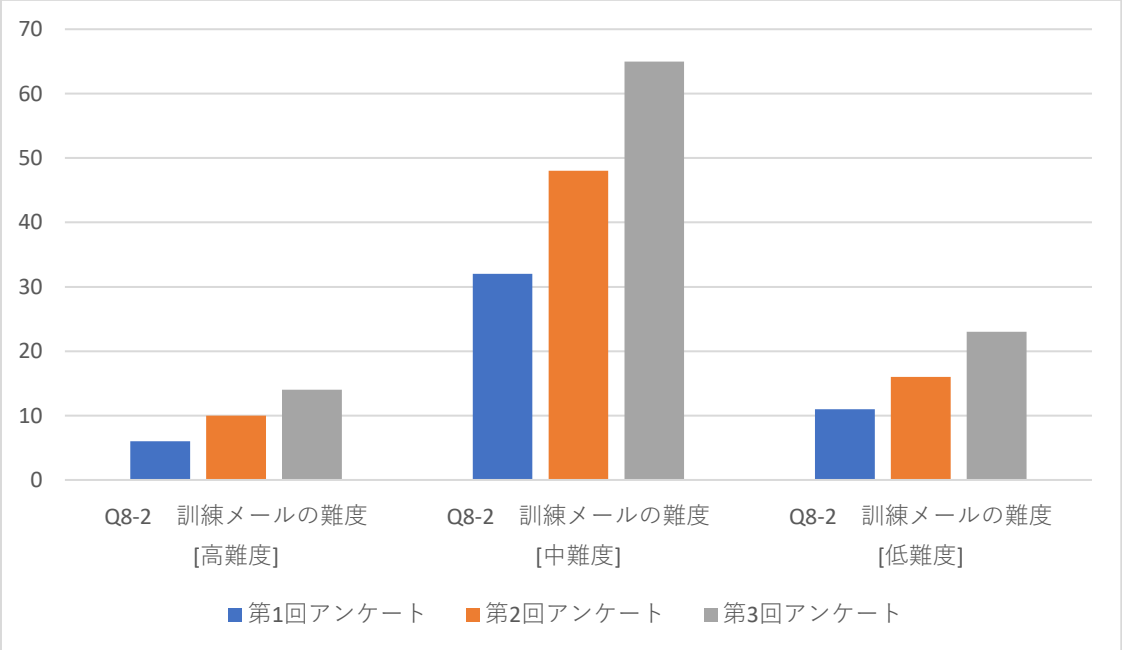


メール訓練実施状況調査結果

Q8　訓練メールの形式（複数回答可）

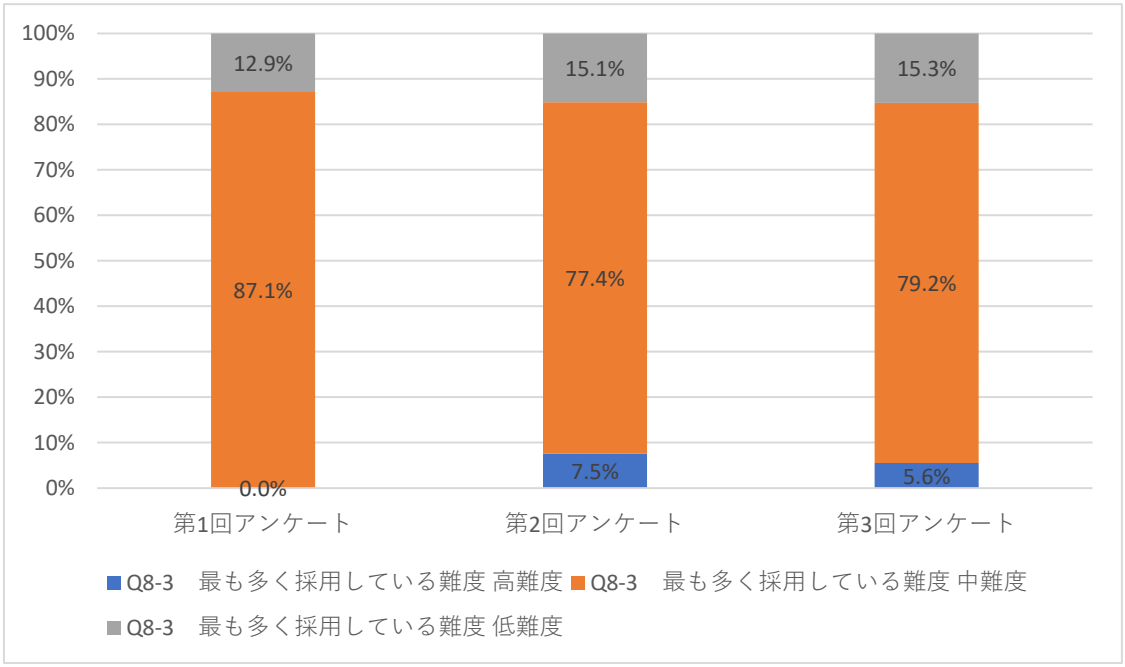


Q8-2　訓練メールの難度（複数回答可）

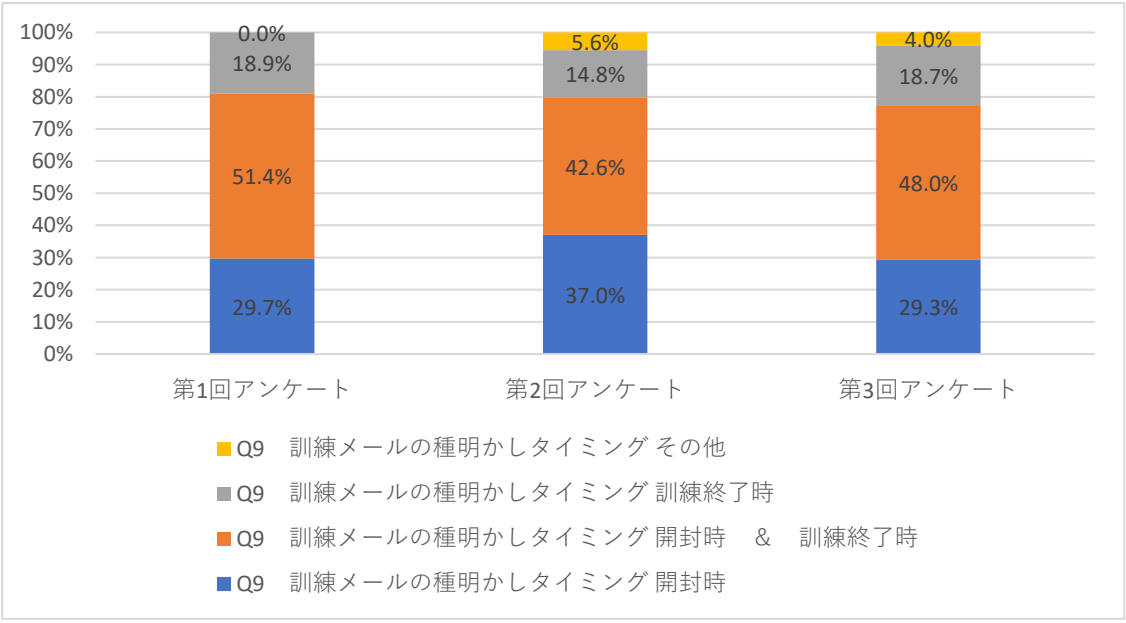


メール訓練実施状況調査結果

Q8-3　最も多く採用している難度

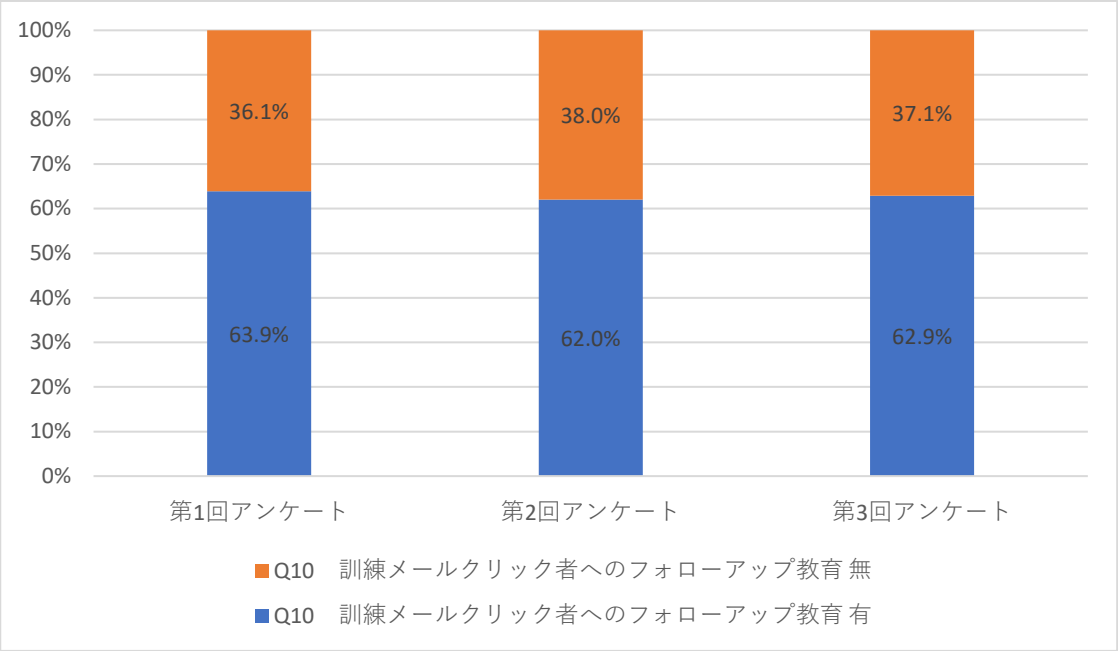


Q9　訓練メールの種明かしタイミング

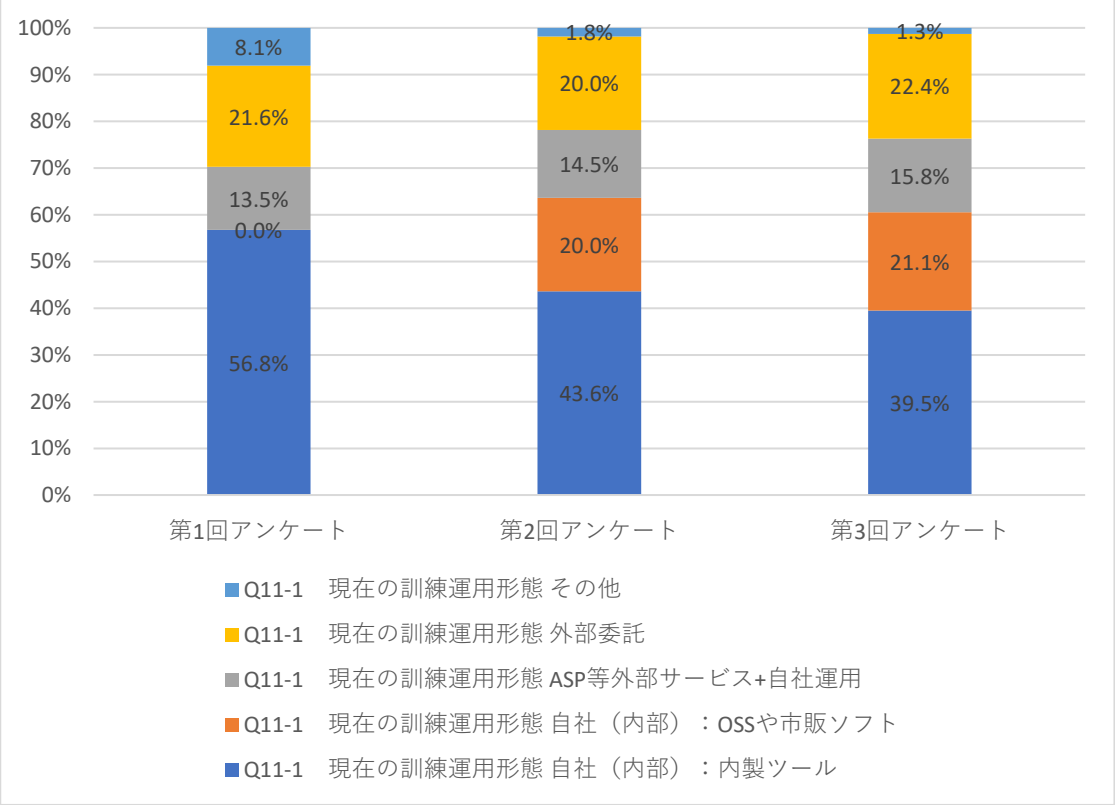


メール訓練実施状況調査結果

Q10　訓練メールクリック者へのフォローアップ教育

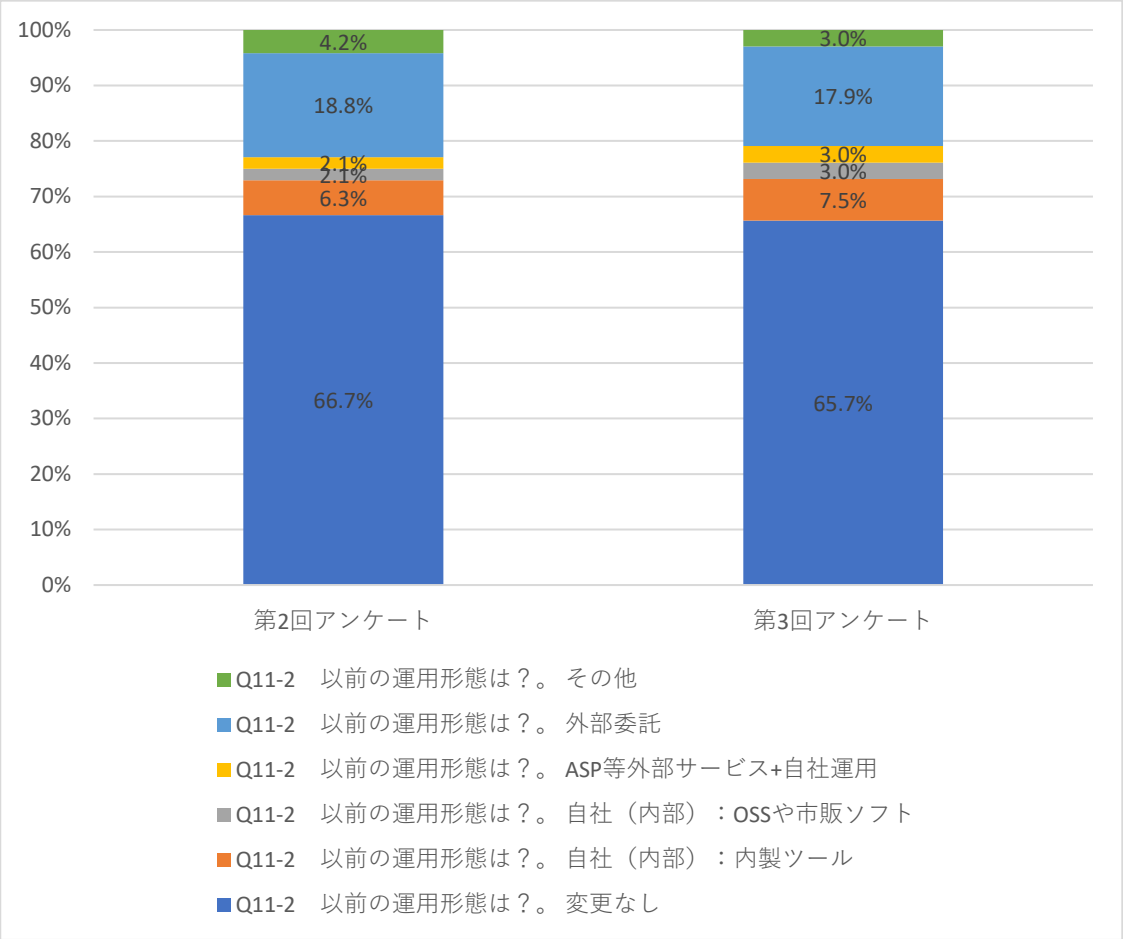


Q11-1　現在の訓練運用形態



メール訓練実施状況調査結果

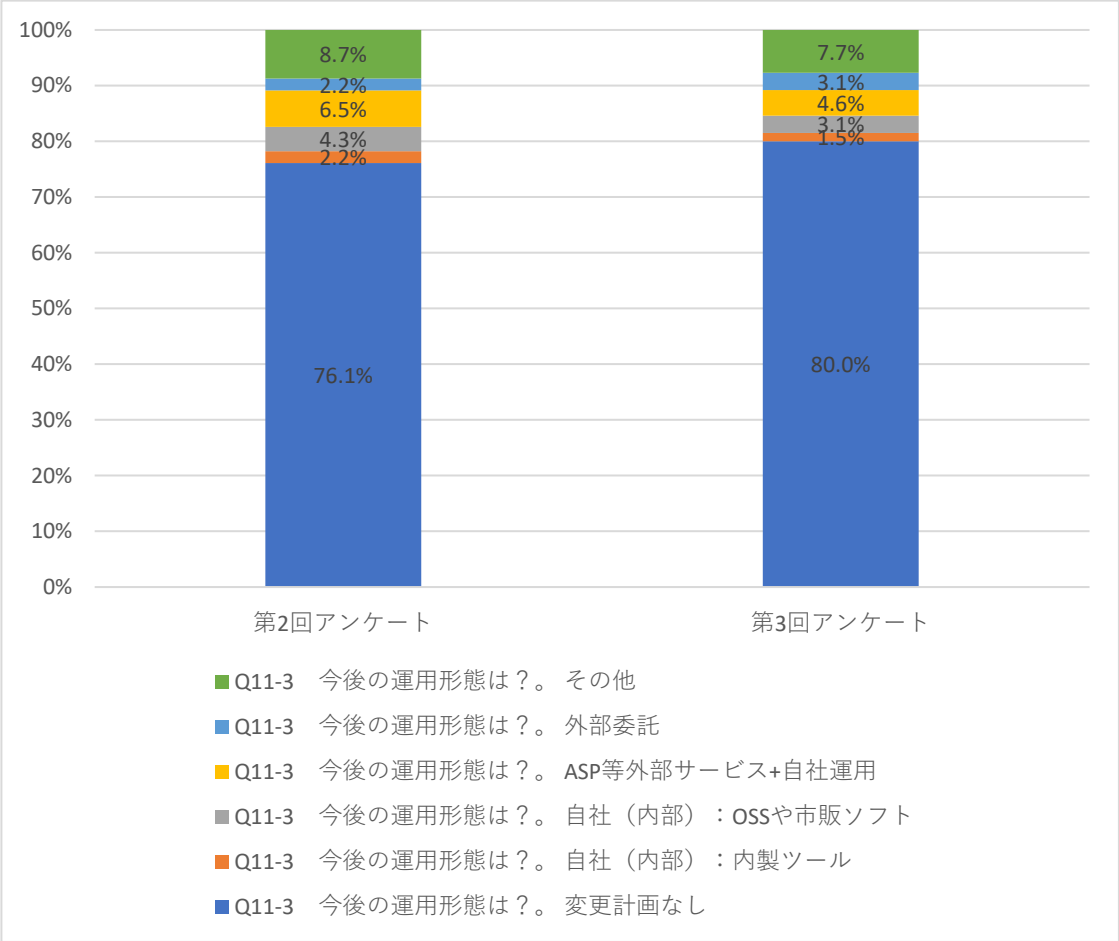
Q11-2　運用形態の変更があった場合は、以前の運用形態をお聞かせください。



		現在の訓練運用形態				
		自社(内部):内製ツール	自社(内部):OSSや市販ソフト	ASP等外部サービス+自社運用	外部委託	その他
Q11-2 運用形態の変更があった場合は、以前の運用形態をお聞かせください。	変更なし	38	5	13	18	2
	自社(内部):内製ツール	2	4		2	
	自社(内部):OSSや市販ソフト	2			1	
	ASP等外部サービス+自社運用		2	1		
	外部委託	5	13	3		
	その他	2			2	

メール訓練実施状況調査結果

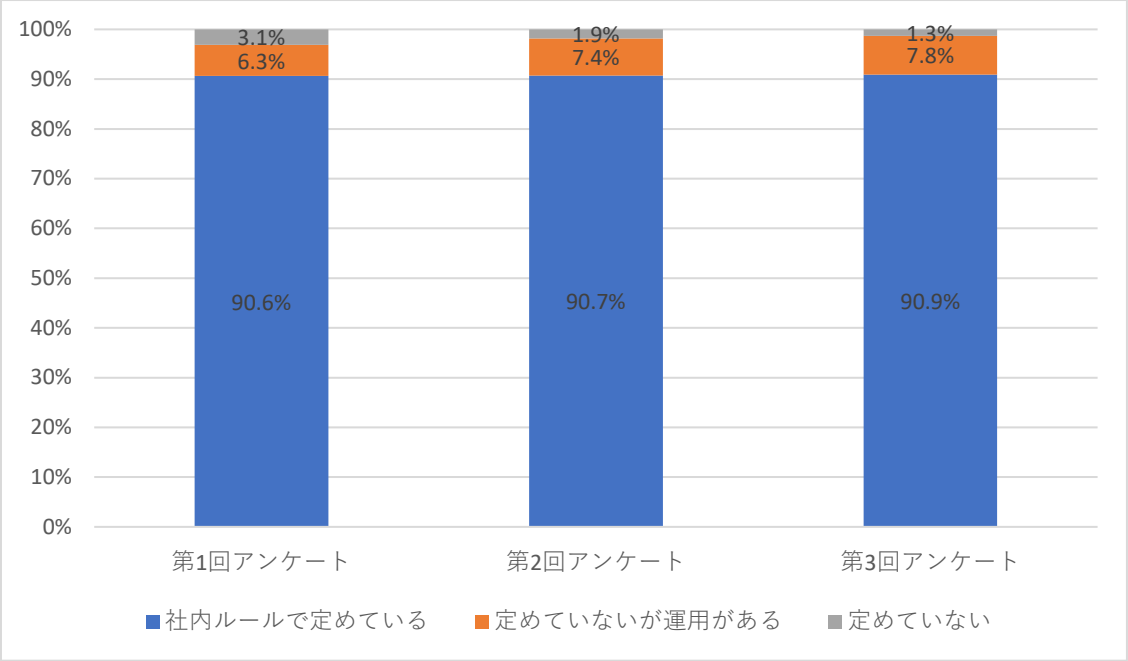
Q11-3　運用形態の変更を計画している場合、今後の運用形態をお聞かせください。



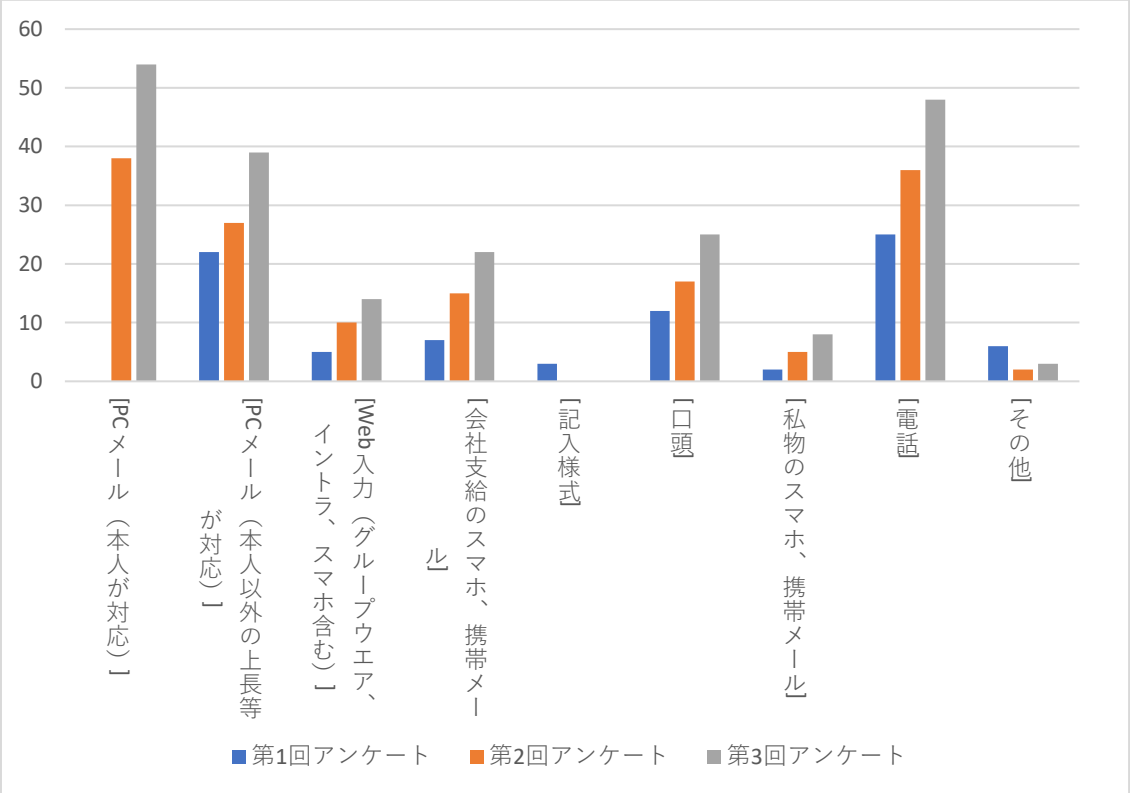
		Q11-3　運用形態の変更を計画している場合、今後の運用形態をお聞かせください。					
		変更計画なし	自社(内部):内製ツール	自社(内部):OSSや市販ソフト	ASP等外部サービス+自社運用	外部委託	その他
現在の訓練運用形態	自社(内部):内製ツール	35		2	6	2	
	自社(内部):OSSや市販ソフト	22					4
	ASP等外部サービス+自社運用	11					3
	外部委託	17	2	2		1	2
	その他	2					

メール訓練実施状況調査結果

Q12-1　社内ルールにて通報を定めていますか？

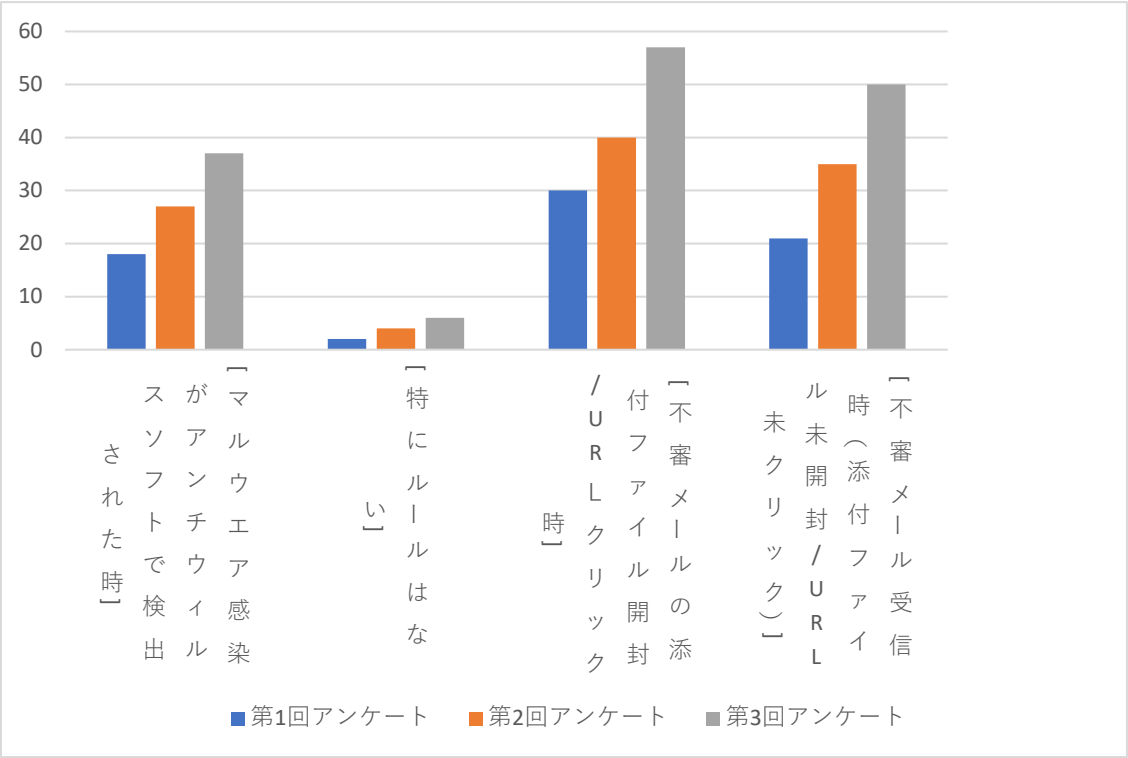


Q12-2　通常時の通報方法(複数回答可)

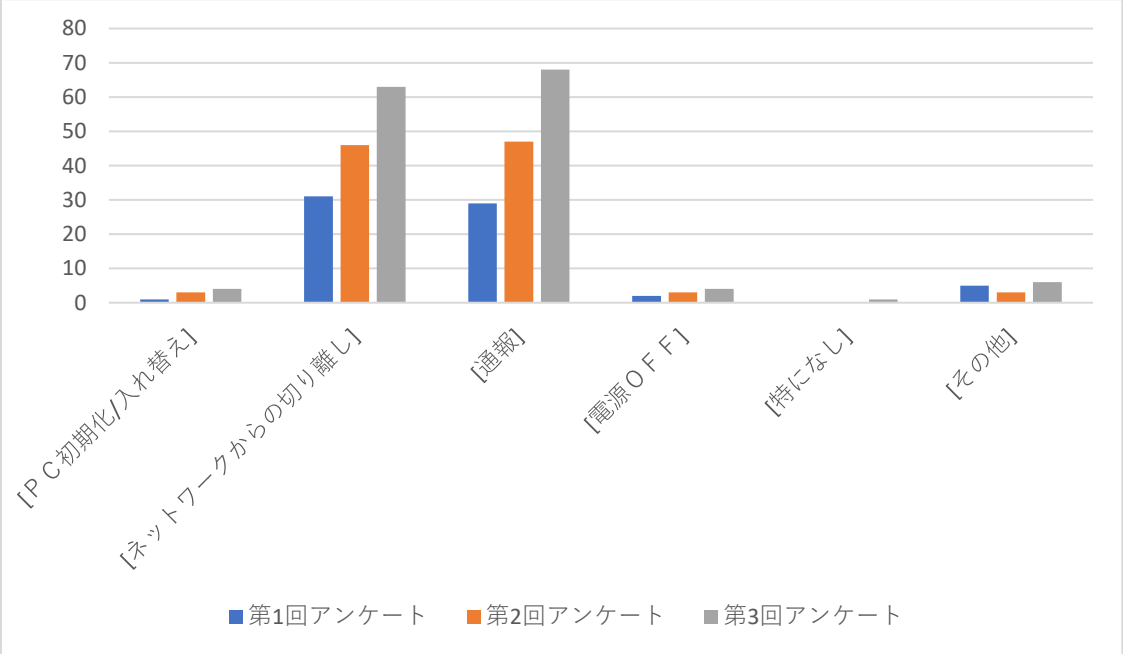


メール訓練実施状況調査結果

Q12-3　社内ルールで定めている通知のタイミング（複数回答可）

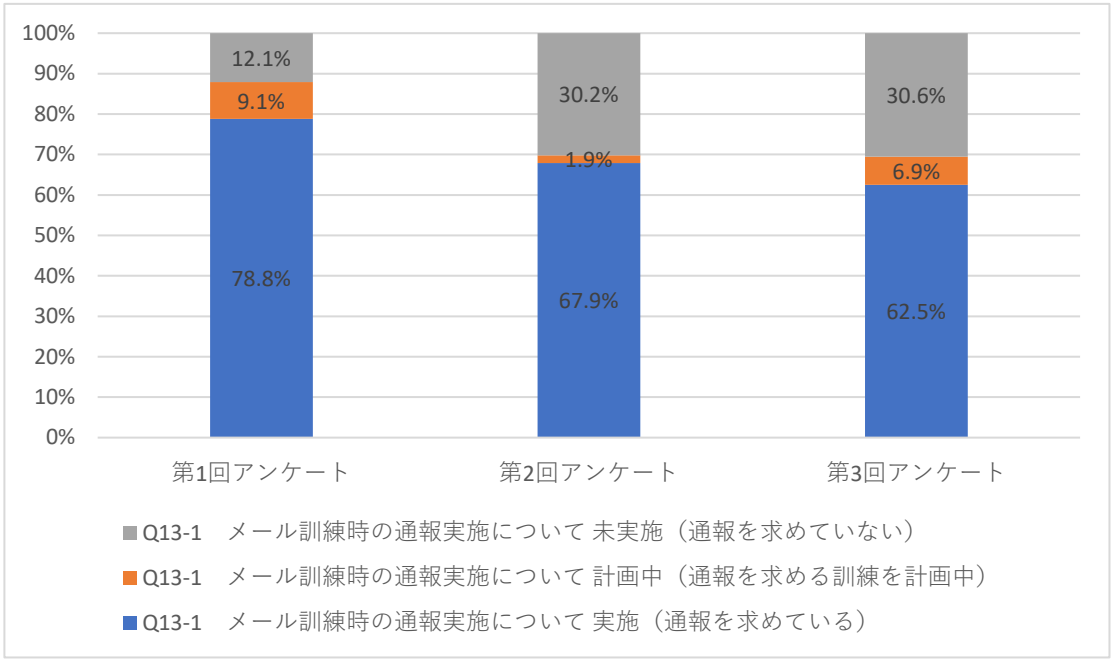


Q12-4　社内ルールで定めている不審メールの添付ファイル開封/URLクリック時の初動対応（複数回答可）

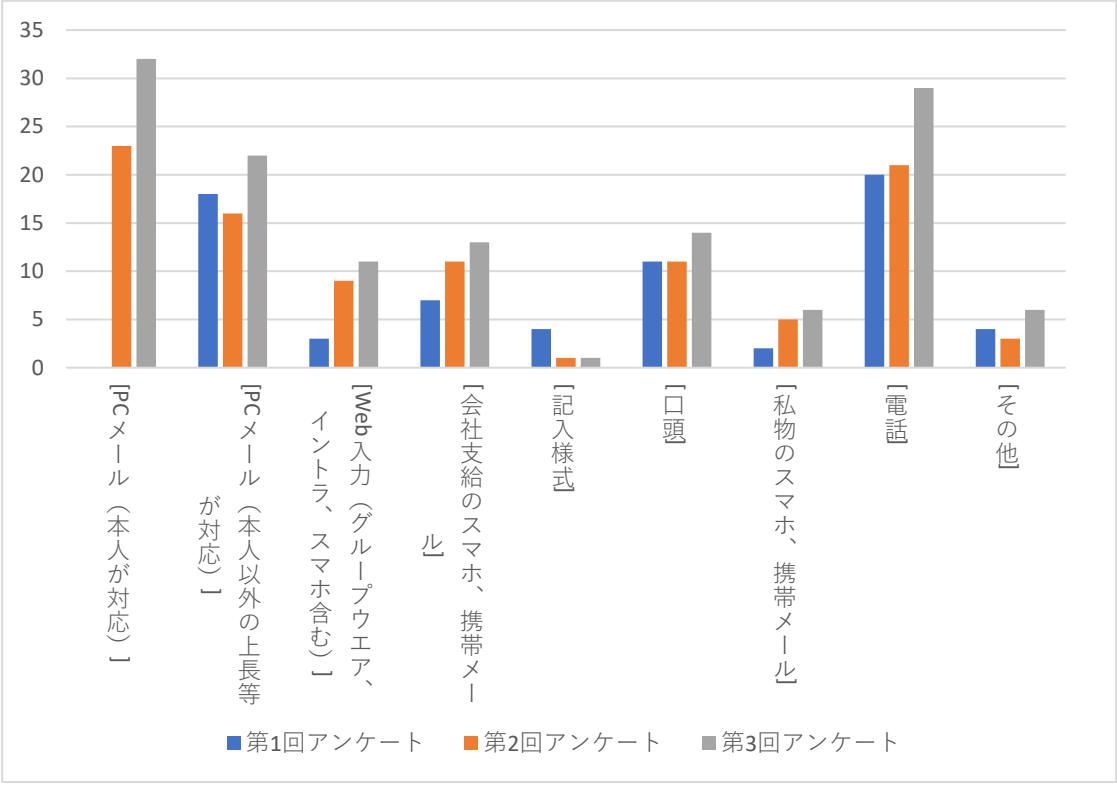


メール訓練実施状況調査結果

Q13-1　メール訓練時の通報実施について

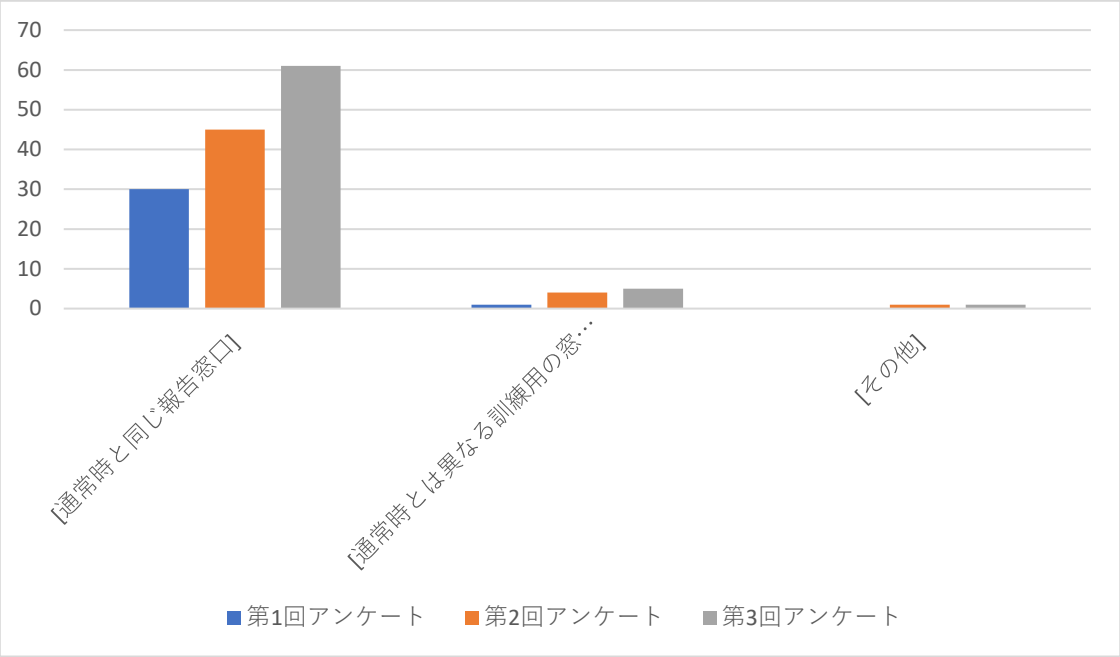


Q13-2　メール訓練時の通報方法(複数回答可)

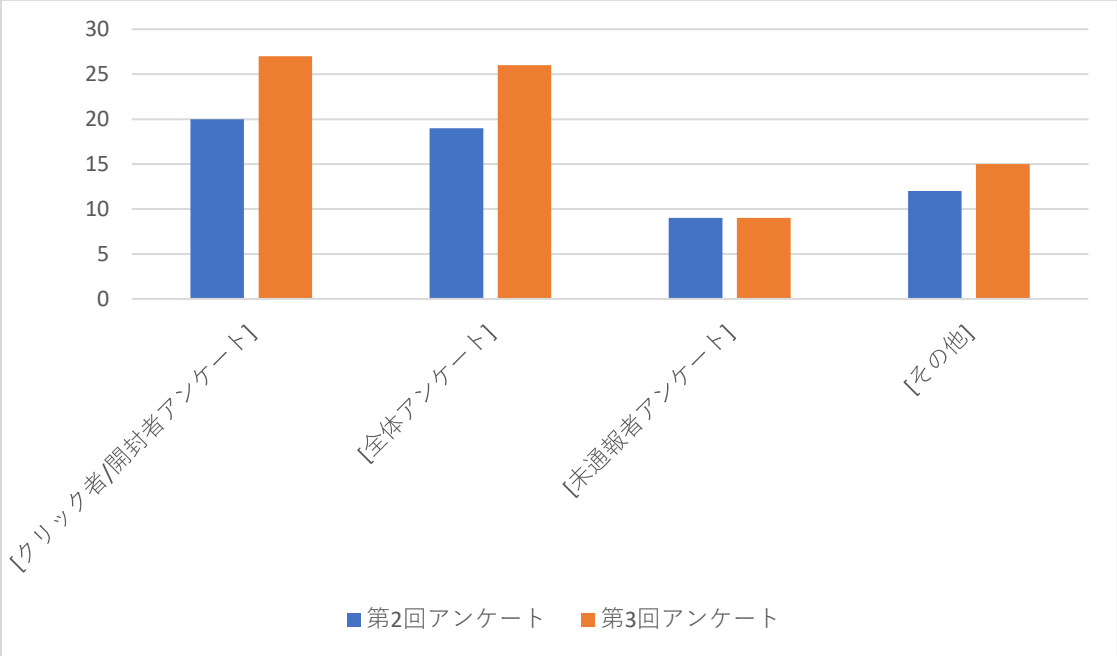


メール訓練実施状況調査結果

Q13-3　メール訓練時の通知先（複数回答可）

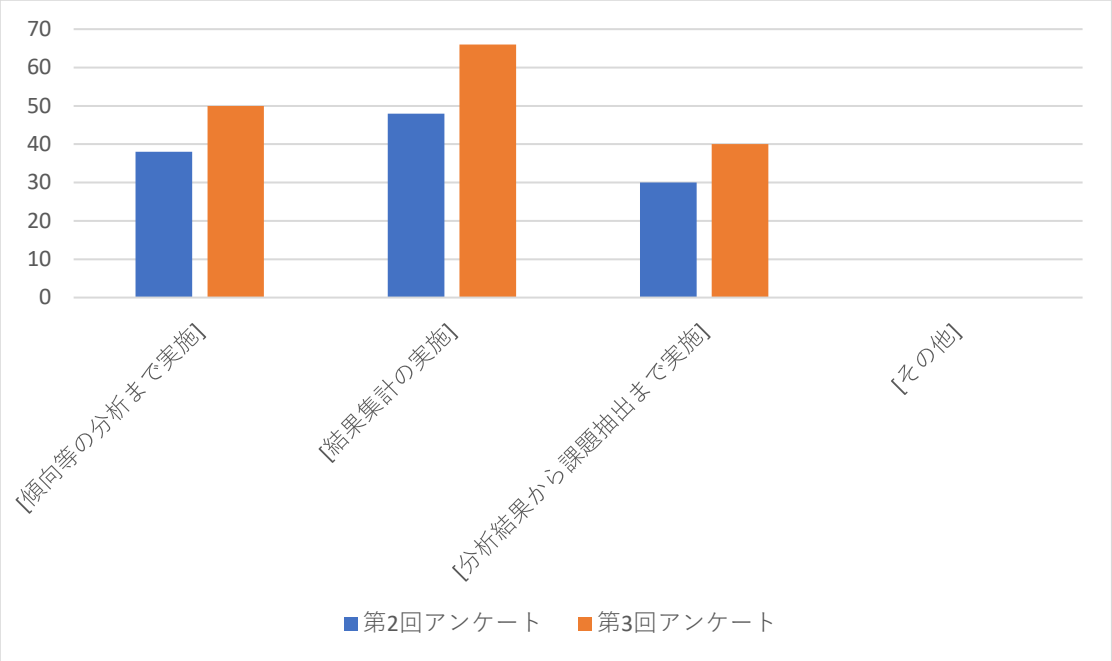


Q14訓練後アンケートの実施と対象（複数回答可）

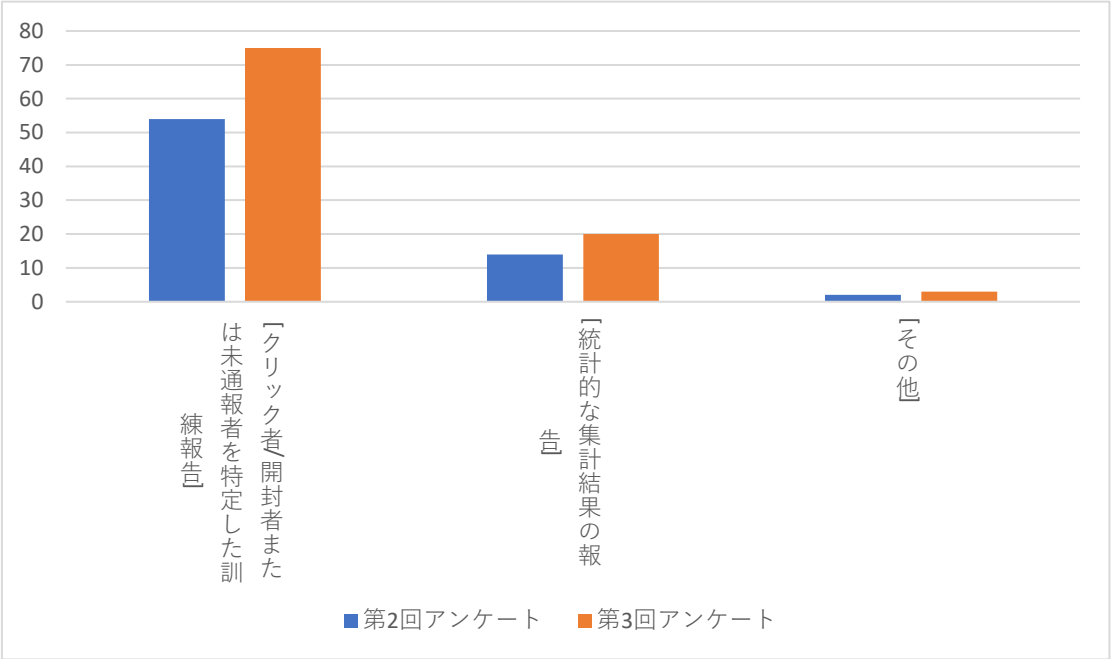


メール訓練実施状況調査結果

Q15結果集計・分析の実施（複数回答可）

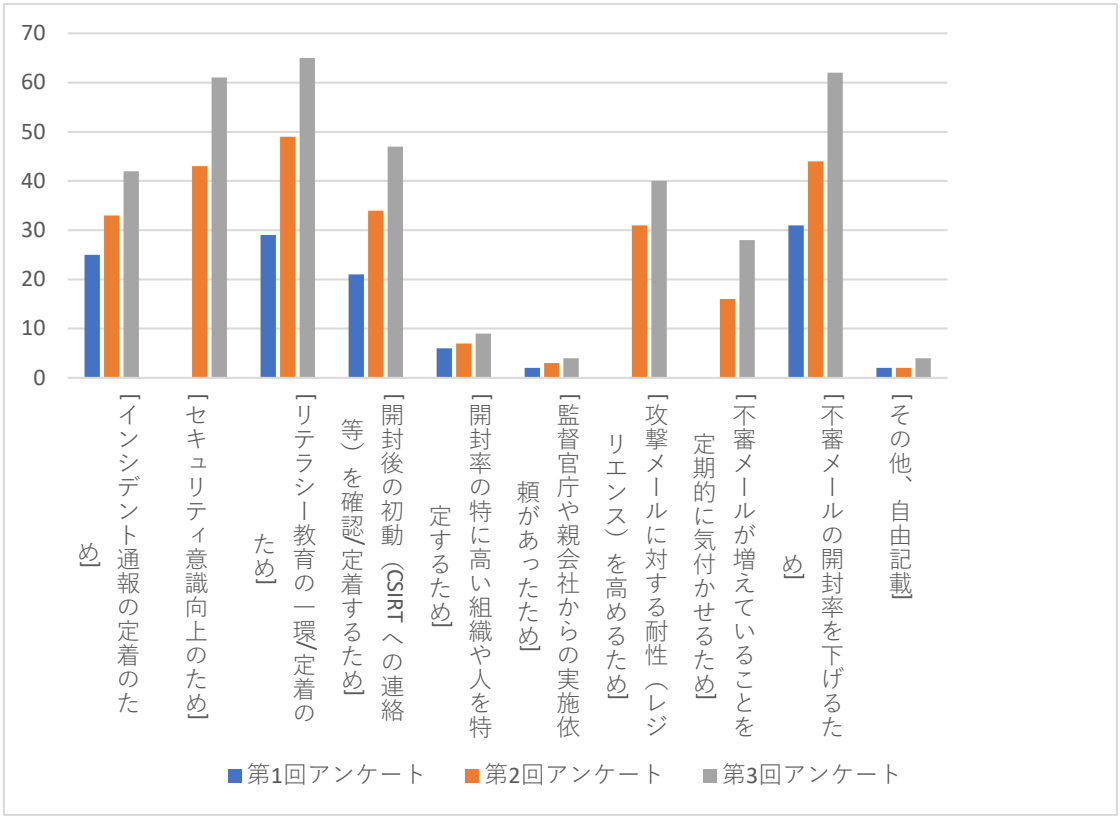


Q16訓練結果の報告内容（複数回答可）

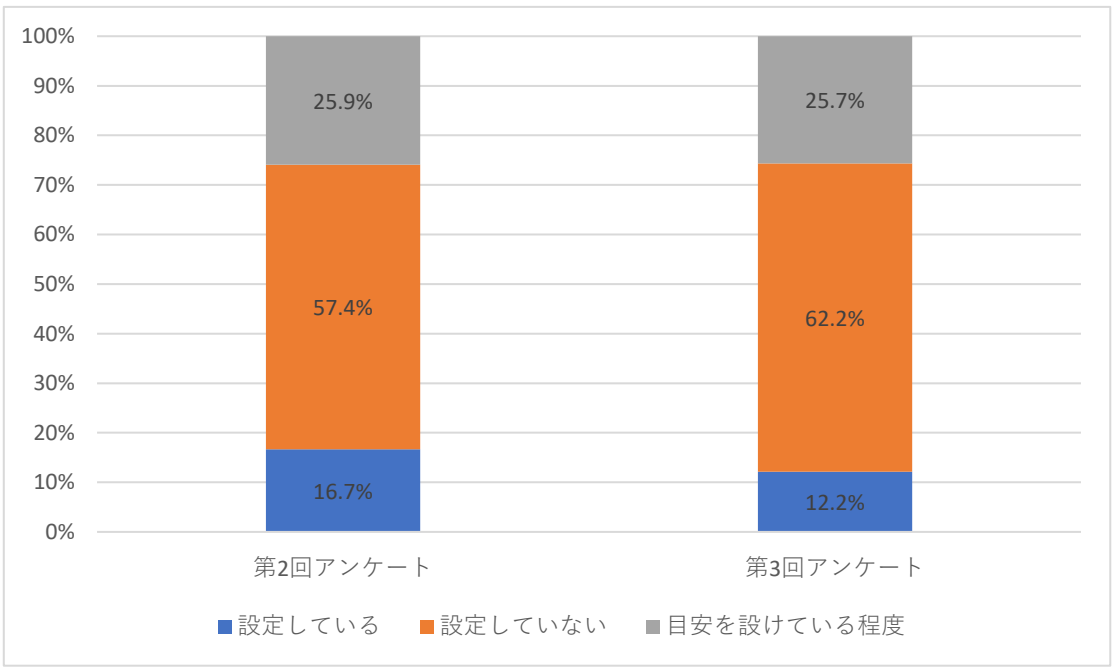


メール訓練実施状況調査結果

Q21　訓練メールは何の為に行なっていますか。目的設定は何でしょうか。（複数回答可）



Q22-1　訓練のゴールを設定していますか？（クリック率〇〇%や通報率〇〇%など）



メール訓練実施状況調査結果

Q22-1　訓練のゴールを設定していますか？（クリック率〇〇%や通報率〇〇%など）

①ゴール内容：URLクリック率、または、添付ファイル開封率

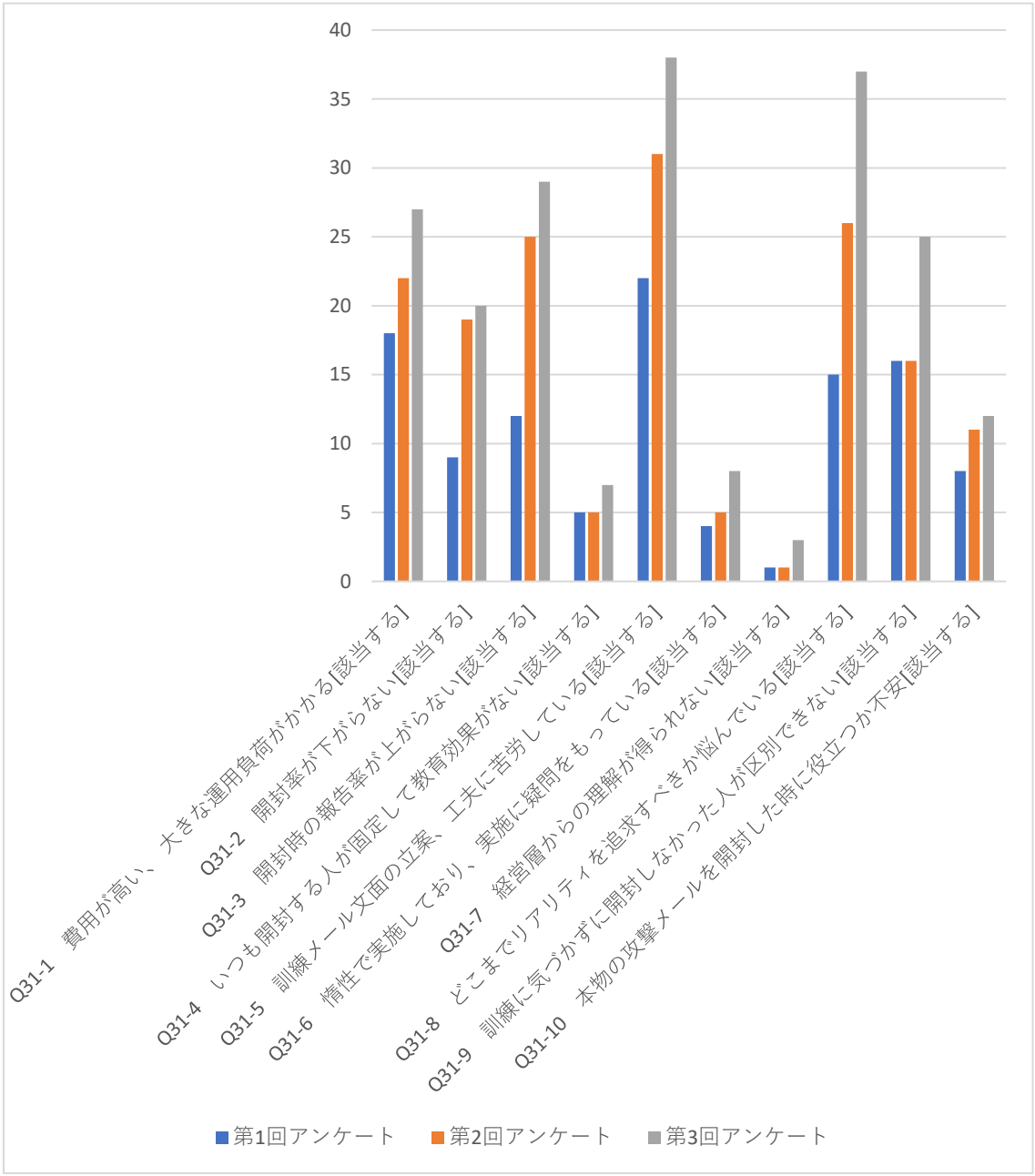
	設定していない	～3%	2%～9%	5%以上	5%	0～10%	5%～10%	10%
第2回アンケート	31	1		1	1	1	1	2
第3回アンケート	46	1	1	2	1	1	2	2

②ゴール内容：通報率

	設定無し	50%	50%～70%	50%～100%	60%	60%～100%	70%	80%～100%	90%～100%	100%
第2回アンケート	18		1		1	1	1		5	4
第3回アンケート	33	1	1	1	1	1		1	5	5

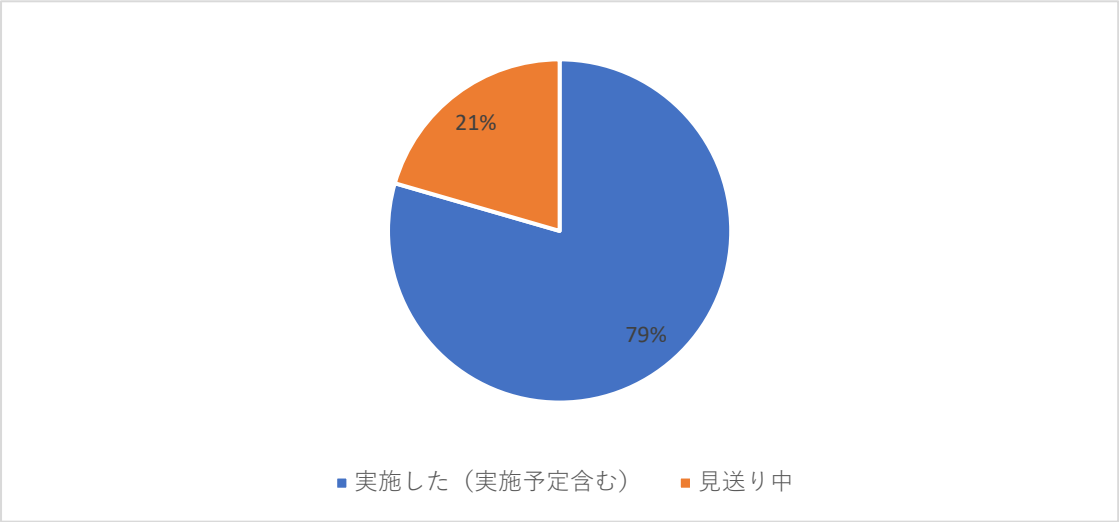
メール訓練実施状況調査結果

Q6　メール訓練実施上の課題



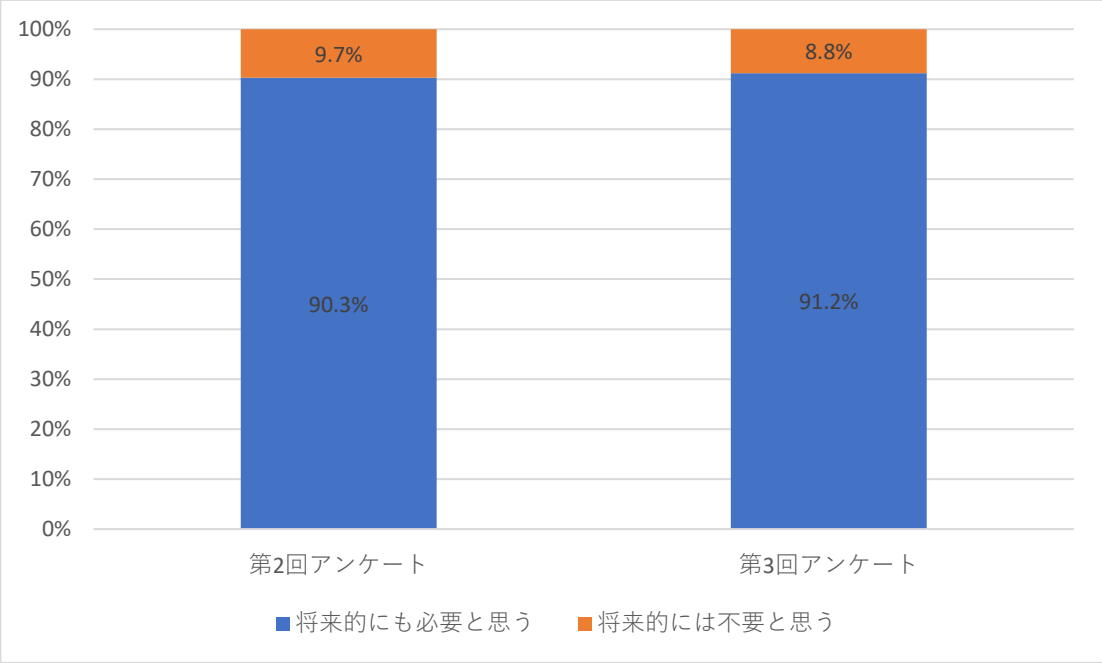
メール訓練実施状況調査結果

Q41-1　コロナ禍にメール訓練を実施しましたか？



※「4.3.1☑レワークにおけるメール訓練実施状況　調査結果」に他結果を記載

Q90　メール訓練の将来的な必要性についてどのようにお考えですか？



メール訓練手引書作成メンバー

	CSIRT 名	
主査	ToppanForms-CERT	トッパン・フォームズ株式会社
副主査	DOCOMO-CSIRT	株式会社 NTT ドコモ

（コアメンバー）

ASY-CSIRT	ＡＮＡシステムズ株式会社
Canon-CSIRT	キヤノン株式会社
FujiXerox-CERT	富士ゼロックス株式会社
PIRATES	東京海上ディーアール株式会社

（サブ WG メンバー）

CEC-SIRT	株式会社シーイーシー
Cy-SIRT	サイボウズ株式会社
glico-s	江崎グリコ株式会社
IIBC-SIRT	一般財団法人 国際ビジネスコミュニケーション協会
INES-SIRT	株式会社アイネス
INTEC-SIRT	株式会社インテック
JAST-SIRT	日本システム技術株式会社
JFE-SIRT	JFE ホールディングス株式会社
JRW-CSIRT	株式会社 JR 西日本 IT ソリューションズ
KIRIN-CSIRT	キリンビジネスシステム株式会社
KKCSIRT	株式会社カカクコム
LACERT	株式会社ラック
NetOne-CSIRT	ネットワンシステムズ株式会社
NSSOL-CSIRT	新日鉄住金ソリューションズ株式会社
PERSOL-SIRT	パーソルホールディングス株式会社
Rakuten-CERT	楽天グループ株式会社
RS-CIRT	株式会社ＪＭＣリスクソリューションズ
SANWA-CSIRT	三和シヤッター工業株式会社
Sky-SIRT	Sky 株式会社
SMMC	住友金属鉱山株式会社
SUMIBE-CSIRT	住友ベークライト株式会社
TEPSYS-SIRT	株式会社テプコシステムズ
TIS-CSIRT	TIS 株式会社
TOPPAN-CERT	凸版印刷株式会社

（表示順：CSIRT 名）

学術連携	明治大学大学院経営学研究科　杉原大輔

最後に

NCA メール訓練手法検討サブ WG ではメール訓練の必要要素に加え、進め方や評価方法、成熟度などについて協議を重ね、また新たな事例を追加し手引書を更新していく予定です。

お問い合わせ先

一般社団法人 日本コンピュータセキュリティインシデント対応チーム協議会
（日本シーサート協議会）
メール訓練手法検討サブワーキンググループ
nca-mail-exercise-swg-owner@nca.gr.jp

改定履歴

加盟組織限定　第１版作成　２０１９年６月２８日
加盟組織限定　第２版作成　２０２０年２月３日
・各項のアンケート結果に「第２回アンケート結果」を追加
・「1.1 メール訓練の必要性」にアンケート結果「将来的な必要性について」を追加
・「1.9 メール訓練の運用方法の決定」にアンケート結果「運用形態の変化」を追加
・4.「メール訓練の最適化に向けて」を追加
4.1メール訓練手法検討サブWG活動:学術連携「メール訓練と褒める文化について」
明治大学大学院経営学研究科　杉原大輔様
・「7.1.3　訓練メール一覧（国内訓練)」に事例を追加
・「7.1.4　訓練メール一覧（海外訓練)」を追加
・「7.3　教育資料の工夫点、改善点」を追加
・「8.2　メール訓練実施状況調査結果（2019 NCA 訓練 WG 内調査結果)」を追加
・「メール訓練手引書作成メンバー」を更新
加盟組織限定　第３版作成　２０２２年２月３日
・各項のアンケート結果に「第３回アンケート結果」を追加
・「4.2　メール訓練の成熟度」を追加
・「4.2.1　モデル１：開封率、通報率を指標とした成熟度モデル」を追加
・「4.2.2　モデル２：訓練メールの難易度を指標とした成熟度モデル」を追加
・「4.3　テレワークにおけるメール訓練の工夫すべき点」を追加
・「6.2　メール訓練手法検討サブ WG 参加チームのメール訓練工夫点、改善点」に事例を追加
・「6.3　その他の工夫点、改善点」を追加
・「7.1.3　訓練メール一覧（国内訓練)」に事例を追加
・「7.1.4　訓練メール一覧（海外訓練)」に事例を追加
・「7.2.3　誘導先ページ事例」に事例を追加
・「7.3.2　教育資料の工夫点、改善点事例」に事例を追加
・「7.4　メール訓練報告書の工夫点、改善点」を追加】
・「8.3　第３回メール訓練実施状況調査結果（2020 NCA 訓練 WG 内調査結果)」を追加
・「メール訓練手引書作成メンバー」を更新

一般公開版(ver.1.0)　２０２２年８月１８日

以上