国の行政機関における情報セキュリティ対策に関する実態調査

― 職員の情報セキュリティ教育の取組状況 ―

このレポートは、国の行政機関における情報セキュリティ対策に関する体制の整備状況及び情報セキュリティ教育の実施状況（サイバー攻撃や情報セキュリティインシデントを認知した際に取るべき行動についての一般職員に対する教育に関するもの）について令和2年11月に行った調査の結果をまとめたものである。

なお、調査は、内容の検討及び実施について政府情報セキュリティ・IT人材対策WG事務局の協力を、回答について24府省庁の協力を得て行った。

＜調査結果からみた主なポイント＞

1　標的型攻撃メールへの備え

○　標的型攻撃メールに係る情報セキュリティ教育については、

①　偽の標的型攻撃メールを職員に送信する模擬訓練

（令和元年度以降、調査時点までに21府省庁で実施済み）（図1）

②　職員に対する標的型攻撃メールに関する最新動向・手口等の情報提供

（定期的に情報提供：6府省庁、可能な限り細やかに情報提供：14府省庁）（図5）

が、一般的に行われている。

○　模擬訓練については、

①　各府省庁は、模擬訓練における不審メールの添付ファイルの開封率やURLのクリック率を注視

②　ただし、不審メールの受信や開封について「情報セキュリティ業務の統括部局（以下「セキュリティ部局」という。）等に必要な報告をしたか」というインシデント発生後の行動までを訓練の中に位置付けているのは、約4割にとどまる（図2）。

2　職員の情報セキュリティ業務の経験と研修・演習

○　各府省庁の CSIRT（注 1）、セキュリティ部局に加え、一般的な業務を行う本省内部部局と地方支分部局等（以下「一般部局」という。）からそれぞれ一つ（注 2）を選定し、これらの職員について、IT・情報セキュリティ関係の業務経験、研修・演習の受講状況を調べたところ、次のような状況がみられた（表 1）。

（注）1　組織において発生した情報セキュリティインシデントに対応するため設置された体制。Computer Security Incident Response Team の略

2　どちらも職員数の多い部局、さらに地方支分部局については原則として関東地方に所在する機関から各府省庁が選定

①　IT・情報セキュリティ関係の業務経験については、CSIRT 及びセキュリティ部局には、業務経験を有する者が比較的多く配置されているが、一般部局にまでは人数を配置しきれていない。

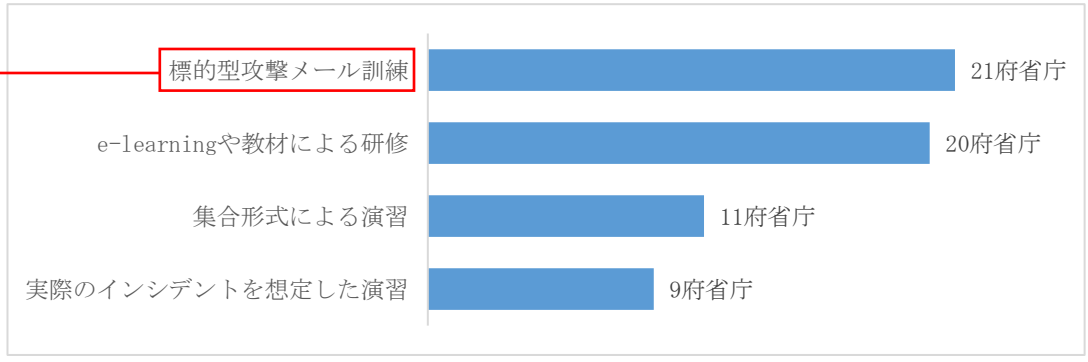
②　政府統一的に実施している IT・情報セキュリティ関係の研修・演習の受講状況については、CSIRT 及びセキュリティ部局では受講経験ありとする職員の割合は比較的高く、一般部局ではその割合は低い（表 1）。

他方、一般部局の情報セキュリティ責任者に対しては、各府省庁は独自の研修を行っている（図 6～8）。

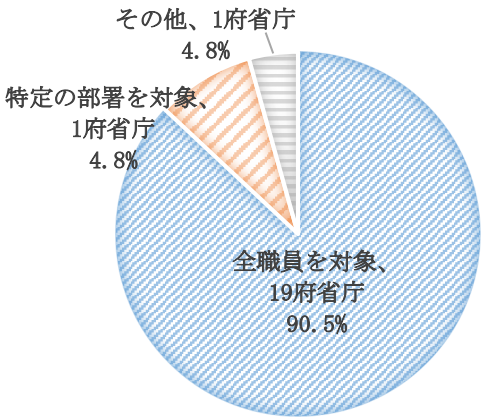
調査結果１「標的型攻撃メールへの備え」

図１　標的型攻撃メールに関する情報セキュリティ教育の実施状況（教育の類型別）

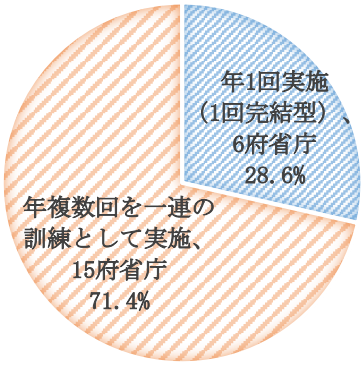
（n＝24 府省庁、複数回答あり）



【標的型攻撃メール訓練の実施対象】(n=21 府省庁)



【標的型攻撃メール訓練の実施頻度】(n=21 府省庁)

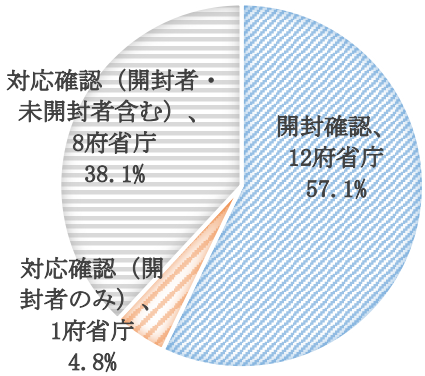


（注）１　標的型攻撃メール訓練を実施していると回答した 21 府省庁のうち、全職員及び特定の部署を対象に実施していると回答した府省庁がみられたため、当該府省庁を「その他」と整理している。

２　割合は、少数点第二位を四捨五入しているため、合計が 100 にならない場合がある。

図２　標的型攻撃メール訓練の訓練内容

（n＝21 府省庁）



（注）

1　図２は、標的型攻撃メール訓練を令和２年 11 月時点で実施している 21 府省庁が、令和２年又は元年に実施した訓練結果を組織内にフィードバック等を行った内容について、各府省庁から提供を受け、当局で分析・分類したものである。

2　図２のグラフの分類は以下のとおり。

・　開封確認
…訓練対象者のうち、訓練メールの開封率（添付ファイルの開封率、URL のクリック率）又は開封者数を把握するもの

・　対応確認（開封者のみ）
…訓練対象者のうち、訓練メールを開封した者で、規定の報告先に不審なメールを受信した旨を報告した人数等を把握するもの

・　対応確認（開封者・未開封者含む）
…訓練対象者のうち、規定の報告先に不審なメールを受信した旨を報告した人数等を把握するもの

図 3　標的型攻撃メール訓練の内容見直し状況

（n＝21 府省庁、複数回答あり）

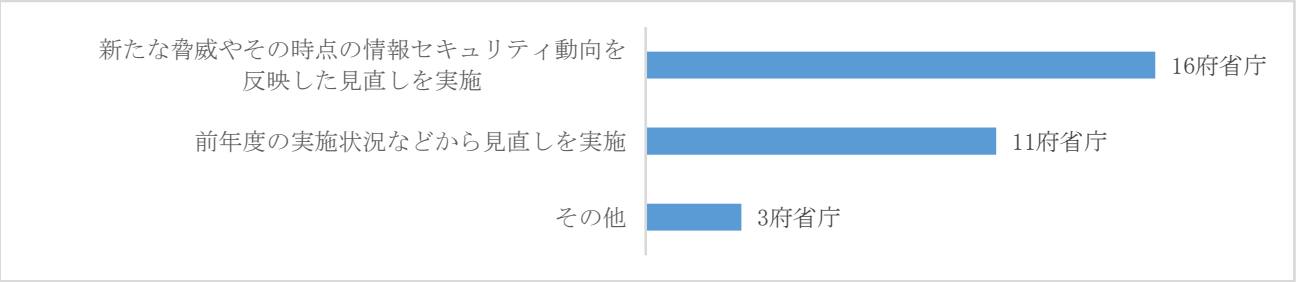
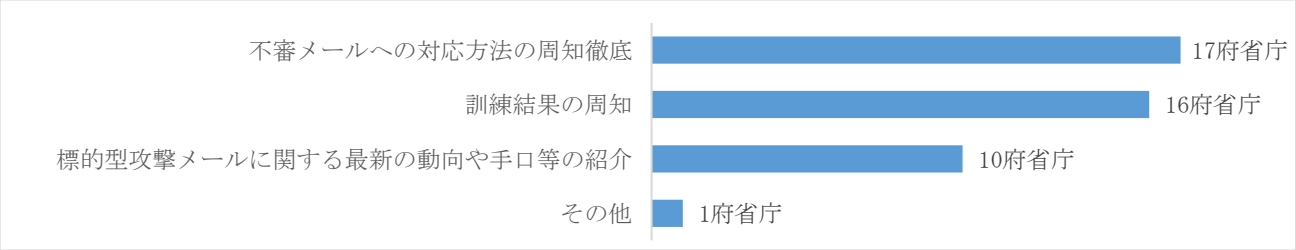


図 4　標的型攻撃メール訓練結果のフィードバック内容

（n＝21 府省庁、複数回答あり）



【事例 1：訓練結果を組織内にフィードバックした内容の例】

○　3 回連続して訓練メールを開封した者に対して、部局情報セキュリティ責任者を通じて注意喚起を個別に実施

○　訓練メール開封者に開封した際の心理などを聴くアンケートを実施

○　訓練結果の分析や結果に対する所見を周知

○　最近の標的型攻撃メールの実例を紹介

【事例 2：職員が標的型攻撃メールの脅威をより切実に受け止められるような工夫の例】

○　実際に受信した標的型攻撃メールを使用して見分けるポイント等を周知

○　職員向け電子掲示板において、実際に職員が受信した標的型攻撃メールの内容を実例として掲示するなど、職員の誰もが攻撃を受ける可能性があることが伝わるように意識した内容を掲載

○　ポータルサイトへ「重要周知」として掲載するとともに、幹部会においても副 CIO から発言

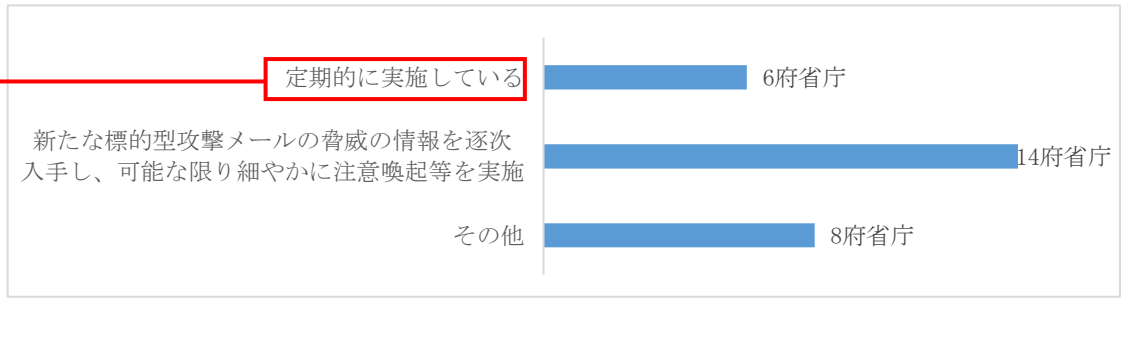
○　実際に受信したメールを用い、速やかに全職員に注意喚起。また、特定の分野を標的としているようなケースでは、当該分野に関連する部署に注意喚起

○　不審メールとして受信したメールそのものの内容を基に例示を立てて注意喚起

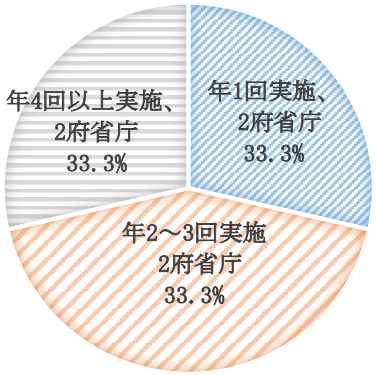
○　職員からの質問に対し回答できるよう CSIRT 内での情報共有を実施

図５　標的型攻撃メールに関する最新の動向・手口等の紹介や注意喚起状況

（n＝24 府省庁、複数回答あり）



【実施頻度】（n＝6 府省庁）

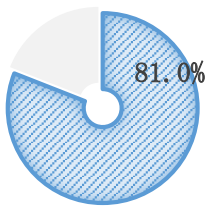
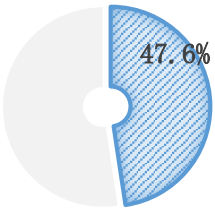
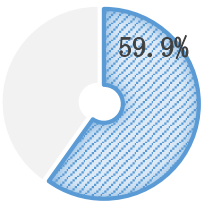
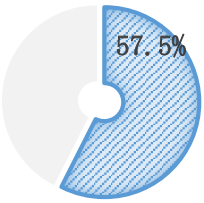
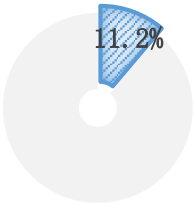
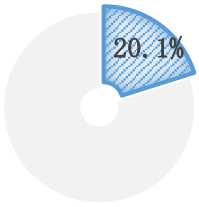
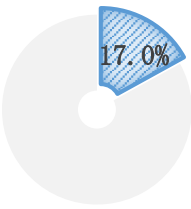
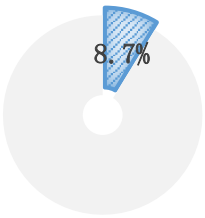
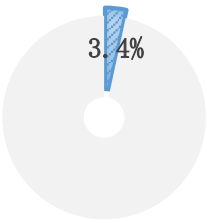
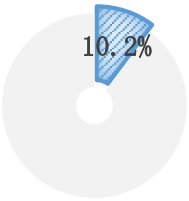
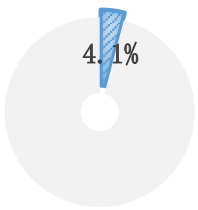
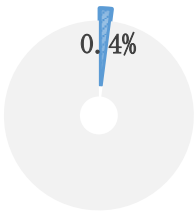


（注）　割合は、少数点第二位を四捨五入しているため、合計が 100 にならない。

調査結果２「職員の情報セキュリティ業務の経験と研修・演習」

職員の業務経験、総務省やNISC（内閣サイバーセキュリティセンター）等が実施する研修等の受講状況

表１　24府省庁の情報セキュリティ体制に関わる職員の業務経験や研修等受講状況

業務経験・研修等受講状況 ＼ 職員の区分	IT・情報セキュリティ関係業務の経験ありとする人数の割合	総務省が実施する政府の情報セキュリティ等に関する情報システム統一研修（以下「統一研修」という。）の修了経験ありとする人数の割合	NISC等が実施するIT・情報セキュリティ関係演習の受講経験ありとする人数の割合	【参考】特定の対象者に対して、独自に研修を企画実施している府省庁数（n＝24）（詳細：図6～8）
情報セキュリティインシデントに対処するCSIRT体制の責任者等				（CSIRTに属する職員向け） 
省内のセキュリティ部局の責任者等				（情報セキュリティ責任者向け） 
一般的な業務を行う本省内部部局の情報セキュリティ責任者等				（課室情報セキュリティ責任者向け） 
一般的な業務を行う地方支分部局等の情報セキュリティ責任者等				（注）各情報セキュリティ責任者は、組織の業務特性や課室単位を踏まえて置かれるため、左表と同区分となっていない。

（注）1　本表は、24府省庁を対象に、各府省庁の情報セキュリティポリシーや内規に基づき、調査の時点で配置されている情報セキュリティ責任者等を抽出して把握した業務経験や研修等受講状況の回答結果を整理したもの
2　情報セキュリティ関係の体制状況を明らかにすることは、情報セキュリティ上のリスクがあるため、回答のあった人数の割合を示している。

3　各府省庁が回答した業務経験や研修等受講状況は、各課室の本調査の担当者等が当該職員本人に照会し記憶の範囲での回答となっている場合、課室担当者が当該職員の人事記録等の記録の範囲での回答となっている場合など、府省庁により把握方法が異なる。

4　調査対象、表の項目等は以下のとおり

（調査対象）

・　CSIRT 体制
…各府省庁内の情報セキュリティインシデントに対処する CSIRT 体制の責任者等の状況を把握（セキュリティ部局との重複あり）

・　セキュリティ部局
…各府省庁のセキュリティ部局の責任者等の状況を把握

・　本省内部部局
…一般的な業務を行う本省内部部局のうち、府省共通システム及び府省重点システムを所管していない部局から、最も職員数（実員）の多い 1 部局の責任者等の状況を把握

・　地方支分部局等
…関東地方にある一般的な業務を行う地方支分部局等のうち、下位機関を有する機関の責任者等の状況を把握（該当機関が複数ある場合は、最も職員数（実員）の多い機関を選定。また、下位機関にも情報セキュリティ責任者が配置されている場合は、最も職員数（実員）の多い下位機関の責任者についても調査）

（表の項目等）

・　IT・情報セキュリティ関係業務の経験
…システムの企画・要件定義・設計・開発・テスト・運用・業務改革等や PMO（注）、また、情報セキュリティに関する施策の企画・立案などの業務経験
（注）　PMO とは、情報システムに関する府省内全体管理組織のこと。Portfolio Management Office の略字

・　統一研修の修了経験
…総務省行政管理局が実施している情報セキュリティ基礎、情報セキュリティ管理などの統一研修の修了経験

・　IT・情報セキュリティ関係演習の受講経験
…NISC 等が実施している NISC 勉強会、CSIRT 訓練などの演習受講経験

（参考）情報セキュリティに関する体制についての制度の概要

政府は、政府機関等におけるサイバーセキュリティに関する対策の基準として「政府機関等の情報セキュリティ対策のための統一基準（平成 30 年度版）」（平成 30 年 7 月 25 日サイバーセキュリティ戦略本部。以下「統一基準」という。）を策定し、情報セキュリティ対策の項目ごと（責任体制、実施体制、対策の内容等）に機関等が遵守すべき事項を規定している。

統一基準において設置が必須となっている役割等

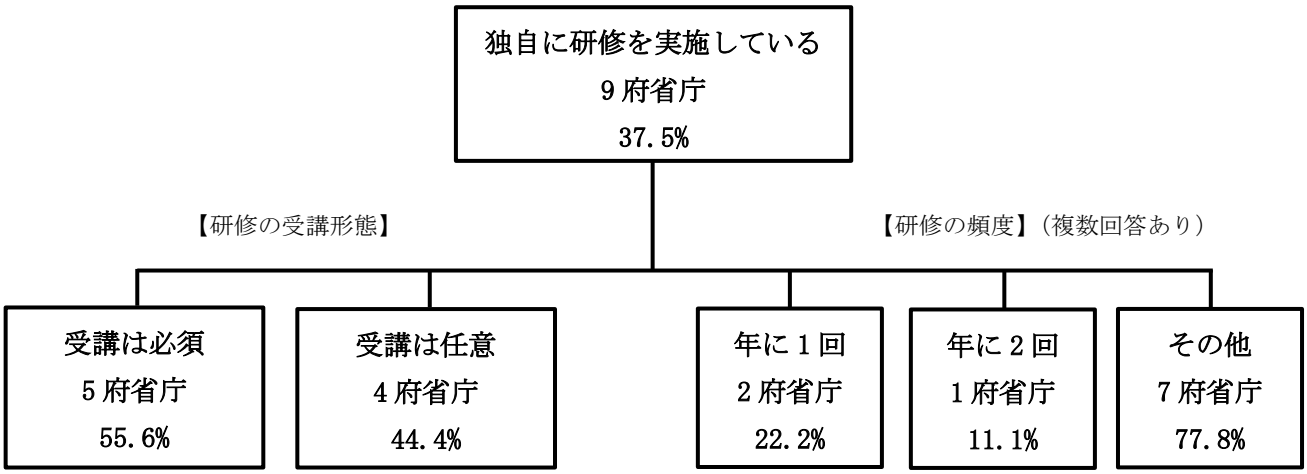
役割の名称	役割の内容
最高情報セキュリティ責任者	情報セキュリティに関する事務の統括
情報セキュリティ監査責任者	監査に関する事務の統括
統括情報セキュリティ責任者	情報セキュリティ責任者の統括、最高情報セキュリティ責任者及び最高情報セキュリティ副責任者の補佐
情報セキュリティ責任者（等）	業務の特性等から同質の情報セキュリティ対策の運用が可能な組織のまとまりごとに、情報セキュリティ対策に関する事務の統括
課室情報セキュリティ責任者	課室ごとの情報セキュリティ対策に関する事務の統括
情報システムセキュリティ責任者	所管する情報システムに対する情報セキュリティ対策に関する事務の責任を負う
最高情報セキュリティアドバイザー	情報セキュリティについて専門的な知識及び経験を有する者として、最高情報セキュリティ責任者への助言等を実施
CSIRT（Computer Security Incident Response Team）	機関等において、情報システム等にセキュリティ上の問題が発生していないか監視するとともに、万が一問題が発生した場合にその原因解析や影響範囲の調査等を実施

（注）　上記のほか、情報セキュリティ委員会、区域情報セキュリティ責任者等も設置が必須となっている。

各府省庁が独自に企画実施している研修の状況

図 6　各府省庁が独自に企画実施している研修の状況（CSIRT に属する職員向け）

（n＝24 府省庁）



（注）1　CSIRT に属する職員については、NISC 等が実施している NISC 勉強会、CSIRT 訓練などの研修・演習の受講経験者が多く（6 ページ表 1 参照）、独自の研修ではなく、政府における統一的な教育によって代替しているとする府省庁も存在する。

2　独自に研修を実施していると回答した 9 府省庁のうち、年に 1 回及び適宜のタイミングで実施していると回答した府省庁がみられたため、【研修の頻度】については、複数回答ありと整理している。

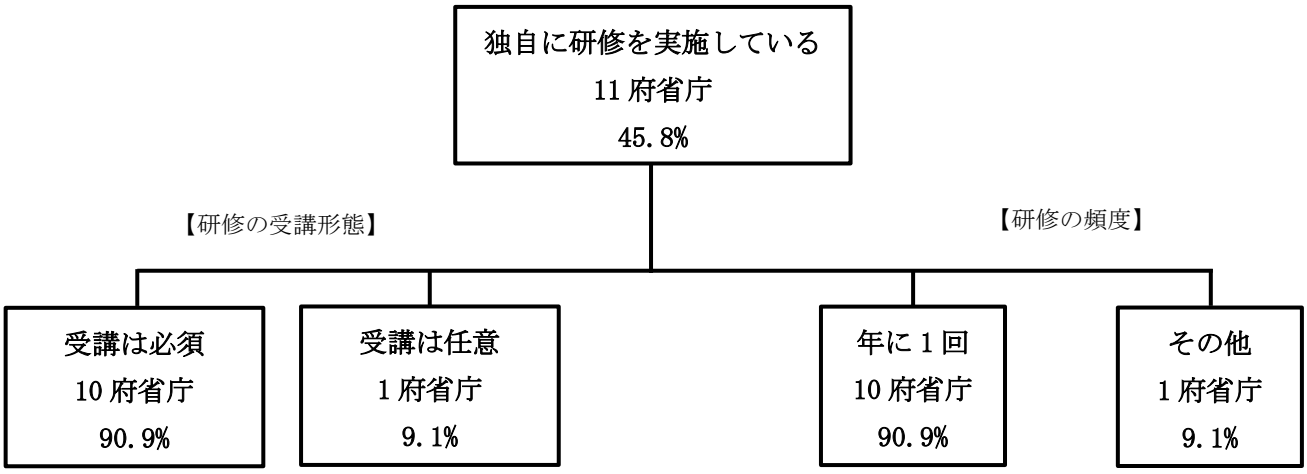
【独自に行っている研修の具体的内容】

- 民間研修により、インシデント発生時の対応や、技術的知識について、教育を実施している。
- 「CSIRT 教育」と題して、CSIRT 体制、最近のサイバー攻撃手法・事案、インシデント発生時の CSIRT としての対応等を講義形式で取り上げるとともに、インシデント発生時における外部委託事業者・CSIRT 管理者等への連絡訓練を実施している。
- CSIRT 及び Web システム等を個別に運用している原課との間で、初動対応や連携強化のために、Dos 攻撃（注）や不正アクセス等におけるインシデント対処について机上訓練を実施するとともに、人的ミスによるインシデント（メール誤送信、書類・端末紛失及び盗難）を取り上げた対応訓練を実施している。

（注）　Dos（Denial of Service）攻撃とは、特定のサーバに対して一度に大量のデータを送出し、通信路やサーバの処理能力をあふれさせるなどのサービス不能攻撃をいう。

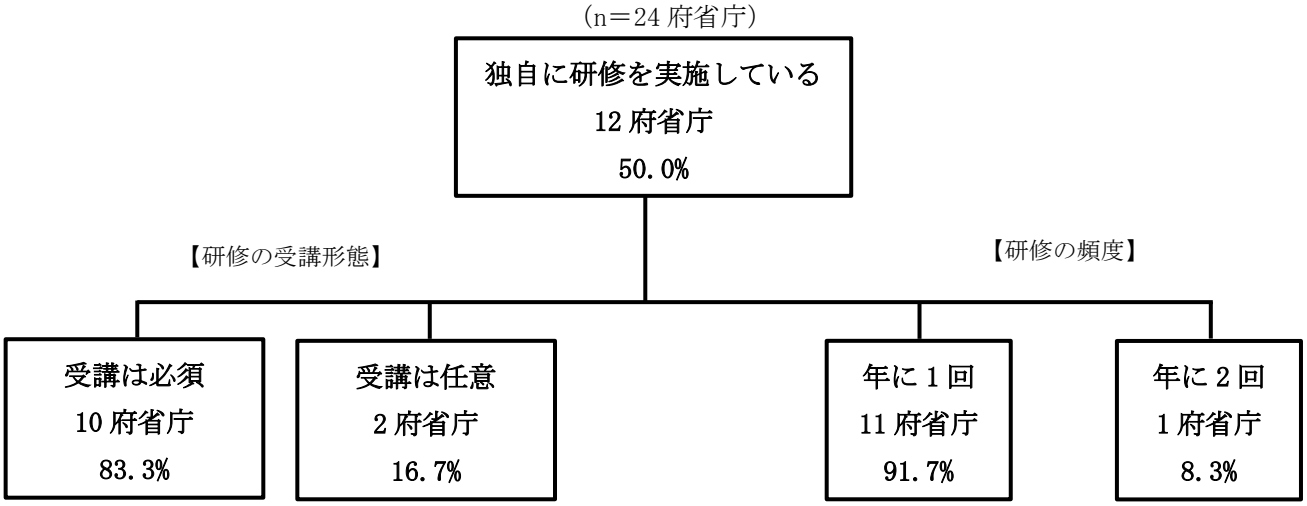
図 7　各府省庁が独自に企画実施している研修の状況（情報セキュリティ責任者向け）

（n＝24 府省庁）



【独自に行っている研修の具体的内容】
- 情報セキュリティの最新の動向や、当該府省庁及び関係法人で発生したインシデント事例を基に、情報セキュリティポリシーにおける情報システムセキュリティ責任者の役割などを理解するための研修を実施している。
- 情報セキュリティ関係規定、事故や障害時の対処、諸手続、情報セキュリティの最新動向等について、研修を実施している。

図 8　各府省庁が独自に企画実施している研修の状況（課室情報セキュリティ責任者向け）



【独自に行っている研修の内容】
- 課室情報セキュリティ責任者に特に依頼したい事項、情報セキュリティ監査等を踏まえた留意事項、外部委託に当たっての依頼事項等について実施している。
- 危機管理の一つとして、近年のサイバー・情報セキュリティの現状と課室情報セキュリティ責任者に求められる役割、インシデント対応を体験するワークショップを行っている。

表 2　各府省庁が独自に行う研修等の実施時期の工夫例（一般職員向け）

区分	具体的な工夫例
一般職員を対象としたもの	○　教材を掲示板等に掲載して実施する。 ○　e-learning により実施する。未受講者については、業務基盤システムのアカウント停止等の措置を行う。受講期間は随時（令和 3 年 1 月初旬～3 月中旬を集中受講期間）としている。 ○　管理職、留学・海外赴任予定者等に対する研修の一環として、情報セキュリティ対策に関する講義を行う。 ○　役職段階別等の研修により情報セキュリティに関する知識の習得を促進する。研修においては、ワークショップ形式の実施、外部講師の活用等による研修内容の充実に取り組む。
特に新規採用者等を対象としたもの	○　新規採用職員向けの集合研修の中で、座学での講義方式で情報セキュリティに係る講義を実施する。 ○　新規採用者（新卒、中途採用者）向け集合研修は、新卒、中途採用者向けを令和 2 年 4 月、中途採用者向けを 2 年 9 月及び 3 年 1 月を基準に実施する。

	○　新規採用者のほか、他府省庁からの転入者、育児休業等からの復帰者等に対し、着任又は異動後3か月以内に、e-learningによる研修を実施する。 ○　新規異動者を対象とした情報セキュリティ教材を第一四半期早期に配布する。 ○　新規異動者に対する研修を、随時、紙面で実施する。

（注）　本表は、各府省庁から提供を受けた情報セキュリティ教育実施計画等の記述内容に基づき、当局で整理を行ったものである。

（参考）テレワークに係る情報セキュリティ対策の周知状況

○　新型コロナウイルス感染症を契機にした新たな働き方として、テレワークや遠隔会議システム（Web 会議システム）の積極的な活用が進む中、NISC が示した情報セキュリティ上留意すべき点については、全府省庁が様々な手段で周知を図っている。
○　今後も新たな働き方については継続して実施されることが想定されるため、情報セキュリティ上の留意事項の最新動向を把握し、今回の調査結果を参考に、継続的な注意喚起や教育を充実していく必要がある。

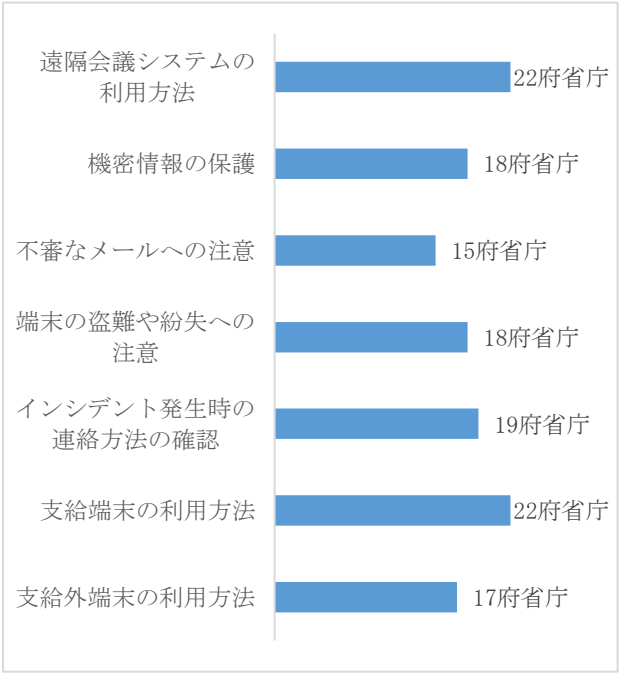
図①　テレワーク実施の際の情報セキュリティ対策に関する周知内容

（n＝24 府省庁、複数回答あり）

図②　テレワーク実施の際の情報セキュリティ対策の周知方法別周知内容

（n＝24 府省庁、複数回答あり）

【事務連絡等による周知】



【e-learning や教材による周知】