対策推進計画策定マニュアル

令和５年７月４日

内閣官房

内閣サイバーセキュリティセンター

目次

1　本マニュアルの目的

本マニュアルは、「政府機関等のサイバーセキュリティ対策のための統一基準」（以下「統一基準」という。）の遵守事項2.1.3(4)(a)によって機関等が策定することとされている対策推進計画について、その策定に当たっての考え方や主眼点等を示し、もって機関等における当該計画の円滑な策定に資することを目的とするものである。

なお、統一基準の遵守事項（これに対応する「政府機関等の対策基準策定のためのガイドライン」（以下「対策基準策定ガイドライン」という。）の基本対策事項及び解説を含む。）を満たす限りにおいては、必要に応じて本マニュアルの記載と異なる手順や内容等で対策推進計画を策定しても差し支えない。

2　対策推進計画の位置付け等

(1)　対策推進計画の位置付け

対策推進計画は、情報セキュリティ対策に関する一連の取組を対象とした全体計画であり、情報セキュリティ対策に関する取組の全体方針のほか、対策基準策定ガイドラインの基本対策事項 2.1.3(4)-1 に掲げる情報セキュリティ対策に関する個々の取組について、全体方針に応じた個々の方針や重点、大まかな実施（予定）時期を設定するものである。（対策基準策定ガイドラインの遵守事項 2.1.3(4)(a)の解説参照）

したがって、対策推進計画は統一基準の適用対象となる機関等においてそれぞれ策定することとなるが、独立行政法人及び指定法人（以下「独法等」という。）の対策推進計画については、「国の行政機関に置かれる最高情報セキュリティ責任者においては、所管する独立行政法人及び指定法人に関し、当該法人を所管する部署との適切な連携や当該部署への必要な助言等を通じて、当該法人の情報セキュリティ対策が適切に推進されるようにすることについても、役割として求められる」（対策基準策定ガイドラインの遵守事項 2.1.1(1)(a)の解説参照）ことを踏まえ、当該法人を所管する国の行政機関は当該法人に提出を求めるなどし、その内容について把握しておくことが望ましい。

(2)　対策推進計画の対象期間と見直しの考え方

対策推進計画の対象期間は単年度とする場合と複数年度とする場合が考えられるが、対策推進計画は「「情報セキュリティ対策の運用及び自己点検、情報セキュリティ監査、本部監査等を総合的に評価するとともに、情報セキュリティに係る重大な変化等を踏まえ」た上で「定期的な見直しを行う」もの（統一基準の遵守事項2.4.1(3)(a)参照）」であり、同計画に含めることが求められている取組には単年度をサイクルとするものがあることから、少なくとも１年に１回は見直しを行うことが前提となる。また、ここでいう「見直し」とは、既存の計画に盛り込まれた各取組の実績等を踏まえて次期計画を策定することを含むものであることから、対象期間を単年度とする場合と複数

年度とする場合のいずれの場合においても、策定作業を行う年度（N年度）の翌年度（N＋１年度）における方針や重点については、明確に示す必要がある。

したがって、対策推進計画は、対象期間を単年度とし、複数年度に渡る取組を盛り込む際には、計画対象期間である翌年度（N＋１年度）に取り組む事項について、翌々年度（N＋２年度）以降に向けてどのように実施する予定であるのかを明確とすることを標準とする。また、単年度の対策推進計画における複数年度に渡る取組については、たとえば以下のように対応することが考えられる。

例：N年度に策定するN＋１年度計画に単年度の取組のほか、３か年の取組としてN＋１年度に全体構想の検討や調査を、N＋２年度に予算要求及び予算執行準備を、N＋３年度に実行・完了を予定している取組を盛り込む場合

○　N年度

策定するN＋１年度計画において、N＋２年度以降に予算要求等を予定していることを示しつつ、N＋１年度に実施する全体構想の検討や調査に関する方針や実施（予定）時期を設定する。

○　N＋１年度

N＋１年度計画の見直しとして策定するN＋２年度計画において、前年度と同様に、N＋２年度に実施する予算要求及び予算執行準備に関する方針や実施（予定）時期を設定する。また、N＋１年度の実績や情勢の変化等により、N＋２年度に実施する事項に変更が生じた場合は、それを反映する。

○　N＋２年度

前年度における対応と同様に、N＋３年度計画において、同年度における方針や実施（予定）時期を設定する。

なお、対策推進計画の対象期間を複数年度とする必要があると機関等において判断する場合は、単年度のサイクルで完了する取組に関しては複数回サイクルが回ることや、複数年度での実施を予定している取組にあっても取組ごとに期間が異なる場合が想定されることを踏まえ、対策推進計画の対象期間を決定する必要がある。

(3)　対策推進計画と個々の取組の詳細計画との関係

対策推進計画は、機関等が組織として、種々の情報セキュリティ対策をいかなる考え方や方向性に基づいて進めていくのかといった一連の取組全体の大枠について、最高情報セキュリティ責任者（CISO）があらかじめ総合的に定めるもの（対策基準策定ガイドラインの遵守事項 2.1.3(4)(a)の解説参照）である。

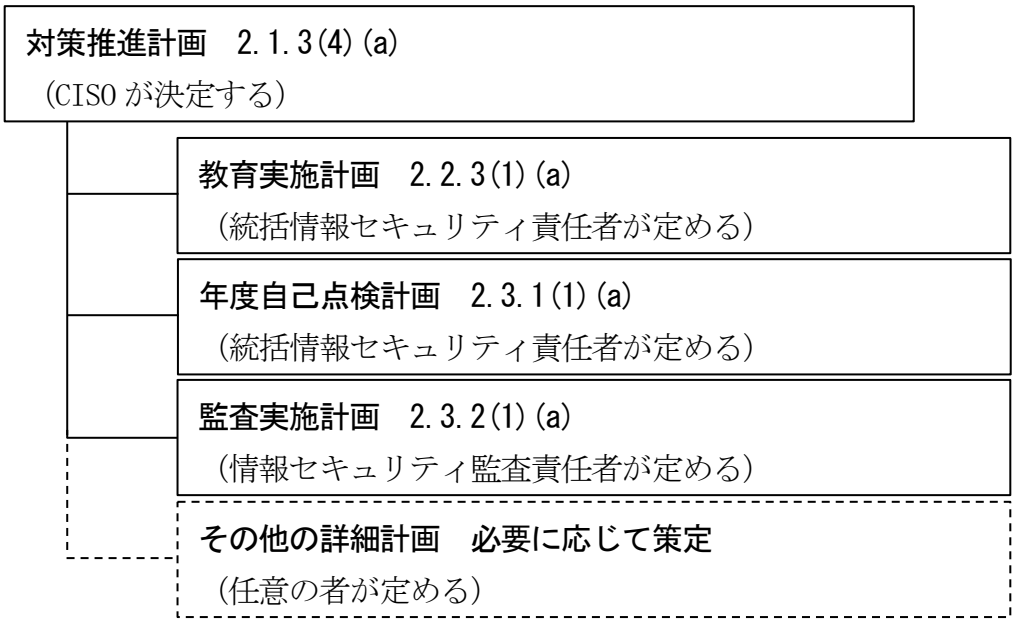
対策推進計画に含めることが求められている取組の中には、統一基準によって別途それらの詳細計画を策定することが定められているものがあるところ、対策推進計画は、それらの取組を含む複数の取組に横串を通すため、それぞれの取組の方針や重点、

詳細計画の策定時期等をあらかじめ定めるものであり、個々の詳細計画は、それぞれの取組の責任者がその権限の下に対策推進計画に則して策定することとなる。

なお、統一基準によって詳細計画の策定が定められている取組としては、情報セキュリティに関する教育（教育実施計画：遵守事項 2.2.3(1)(a)）、情報セキュリティ対策の自己点検（年度自己点検計画：遵守事項 2.3.1(1)(a)）及び情報セキュリティ監査（監査実施計画：遵守事項 2.3.2(1)(a)）がある。

また、詳細計画を策定する定めのない情報システムに関する技術的な対策を推進するための取組、所管する独法等のセキュリティ対策の評価及びその推進に資するための取組（独法等を所管する国の行政機関に限る。）並びにその他の情報セキュリティ対策に関する重要な取組については、詳細計画の策定の要否を含めて個別に検討し、その結果に応じて詳細計画の策定時期や推進体制も対策推進計画に含めることが考えられる。（対策基準策定ガイドラインの遵守事項 2.1.3(4)(a)の解説参照）

図 1 対策推進計画と個々の取組の詳細計画との関係



(4) 対策推進計画の公表等

国の行政機関の対策推進計画については、内閣官房内閣サイバーセキュリティセンター（NISC）へ提出するとともに、サイバーセキュリティ戦略に定める年次報告等を通じて公表できる情報の範囲内で公表する。具体的な公表方法等については、NISC からの事務連絡文書等を通じて別途行う。

３　対策推進計画の策定等の流れの例

対策推進計画は、情報セキュリティ委員会における審議を経て CISO が定めることとされているところ、その原案は適宜の担当者（以下「起案者」という。）が作成し、関係部署との調整を行った上で意志決定のプロセスに乗せていくことが一般的と考えられる。ここでは、機関等における情報セキュリティ対策推進体制に属する職員が起案者となり、情報システムの整備等を担当する課室等の関係者との調整を行った上で単年度を対象期間とする対策推進計画の策定又は見直し（以下「策定等」という。）を行う場合を想定した流れの一例を示す。また、策定等の時期としては、策定等の作業を行う年度（Ｎ年度）における各取組の完了又は相応の進ちょくが見込まれるとともに、翌年度（Ｎ＋１年度）の政府予算案の閣議決定後である第４四半期を想定している。

なお、ここで示す流れは飽くまでも一つの例であり、情報セキュリティ対策推進体制を含む情報セキュリティ関係部局からなるプロジェクトチーム等の体制を設けて原案を作成する、原案の作成段階から CISO や最高情報セキュリティアドバイザーが関与するなど、その他の手順によって対策推進計画の策定に当たることを妨げるものではない。また、対策推進計画の記載内容については、ここでは概要のみを記載しており、その詳細については本マニュアルの「４　対策推進計画の構成・記載事項」で示している。

(1)　全体方針（案）の作成等

ア　前年度の総合評価

起案者は、対策推進計画の全体方針（案）を作成するため、情報セキュリティ対策に関する各取組の担当者等を始めとした関係者と協力し、現在の年度（Ｎ年度）における対策推進計画（前年度（Ｎ－１年度）に策定したもの）に盛り込まれた各取組の実績（初年度を除く。）、情報セキュリティ対策に係る点検の結果、情報セキュリティインシデントの発生状況、その他の取組の状況等に関する情報の収集・分析を行い、当該年度の取組を総合的に評価するとともに、自組織における情報セキュリティに係るリスクや課題を把握する。

現在の年度（Ｎ年度）における対策推進計画（前年度（Ｎ－１年度）に策定したもの）に盛り込まれた各取組の実績に関する評価については、単に計画どおりのスケジュールで取組が実施されたかなどではなく、計画において設定した方針や重点に照らして実施した結果が妥当であったか、計画策定後に計画に影響を及ぼすような情勢の変化は生じたかなど、改善点や反省教訓の抽出に主眼を置き、対策推進計画の位置付けにかなう評価とするように留意する。

イ　全体方針（案）の作成・調整

起案者は、前年度の総合評価によって把握した自組織における情報セキュリティに係るリスクや課題に加え、政府機関全体としての動向その他の情報セキュリティを取り巻く情勢を踏まえ、策定する対策推進計画の対象期間となる翌年度（Ｎ＋１

年度)における全体方針(案)を作成する。また、全体方針(案)は「個別の取組の方針・重点及びその実施時期」（以下「個別の取組の方針・重点等」という。）を定める上での前提となるものであることから、情報セキュリティ委員会の構成員が所属する課室を始めとした関係課室や独法等については所管する国の行政機関に幅広く意見照会を行うなどの調整を行い、事前の合意形成を図る。

⑵　個別の取組の特定及び方針・重点等の設定

起案者は、調整を完了した全体方針(案)を自組織内に周知するとともに、対策推進計画に盛り込む個別の取組を特定するため、盛り込むべき取組やその方針・重点等について提出を依頼する。

該当する取組の担当者は、全体方針(案)を踏まえて自らが担当する取組の方針・重点及びその実施時期を含む必要な事項について検討し、起案者に回答する。

起案者は、各取組の担当者からの回答を取りまとめるとともに、全体方針(案)との整合性、各取組の実施(予定)時期や取組間の連携等を確認し、必要に応じて調整を行う。また、個別の取組の方針・重点等を具体的に検討・調整する過程で、全体方針(案)を修正する必要が生じた場合は、併せて全体方針(案)の修正案を作成する。

⑶　対策推進計画(案)の全体調整

起案者は、対策推進計画(案)として取りまとめた全体方針(案)及び個別の取組の方針・重点等について、情報セキュリティ委員会における審議に向けた全体調整を行う。また、個別の取組の特定及び方針・重点等の調整の過程において全体方針(案)の修正案を作成している場合には、修正点や修正理由を明らかにするとともに、新たに盛り込むべき取組の有無を確認し、該当がある場合は改めて調整を行う。

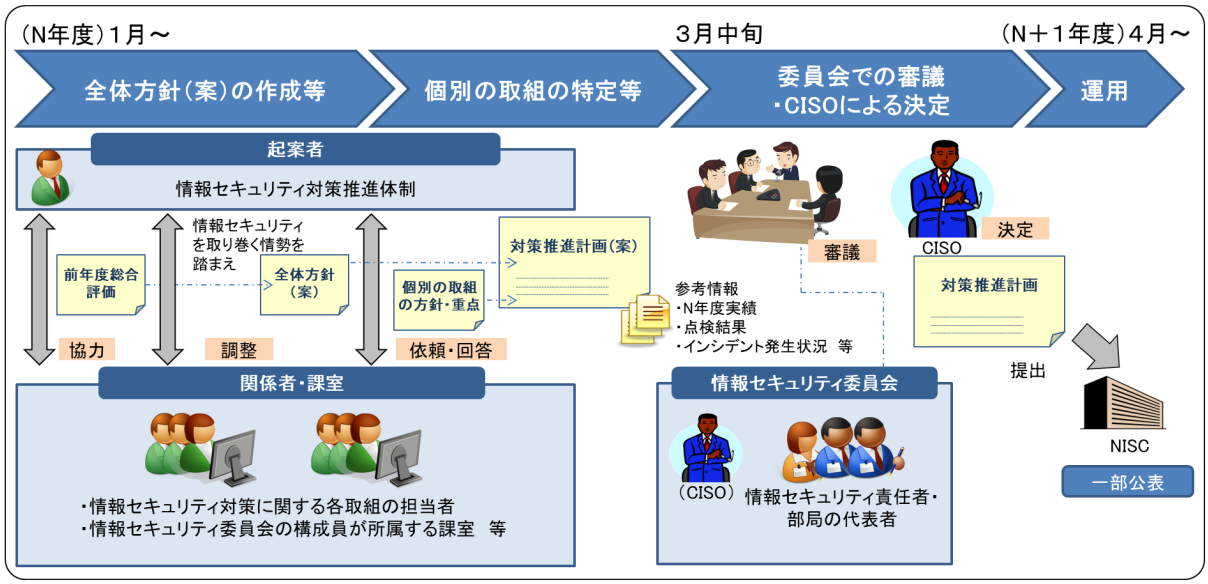
⑷　情報セキュリティ委員会における審議・CISO による決定

情報セキュリティ委員会による審議を行った上で、CISO が対策推進計画を決定する。

審議・決定に当たっては、必要に応じて、参考となる情報（現在の年度（N年度）における対策推進計画（前年度(N－１年度)に策定したもの）の実績、自己点検や情報セキュリティ監査等の結果、情報セキュリティインシデントの発生状況等）をまとめた資料を準備するなど、CISO 等が内容の妥当性等を判断できるように留意する。

なお、CISO が情報セキュリティ委員会の構成員である場合は、情報セキュリティ委員会における審議による了承をもって対策推進計画を決定しても差し支えない。

図　２　対策推進計画の策定等の流れ



４　対策推進計画の構成・記載事項

対策推進計画は、「全体方針」と「個別の取組の方針・重点等」により構成されるものである。また、個別の取組の実施時期については、対象期間における一連の取組の実施予定時期を全体として容易に把握できるようにするため、上述とは別に線表にまとめ、対策推進計画の別添とする。

「全体方針」及び「個別の取組の方針・重点等」の記載事項をそれぞれ(1)及び(2)に示す。

なお、ここでは単年度を対象期間とする対策推進計画の策定等を行う場合を想定した記述としている。

(1)　「全体方針」に係る記載事項

「全体方針」は、限られた予算や人的資源を最大限に活用して自組織及び所管する独法等における情報セキュリティ対策を推進するため、対策推進計画の対象期間となる年度における個々の取組の方向付けを行うものであることから、その前年度の総合評価によって把握した自組織における情報セキュリティに係るリスクや課題に加え、政府機関全体としての動向（例えば、新たな「サイバーセキュリティ戦略」の策定等）その他の情報セキュリティを取り巻く情勢を明記した上で、それらを踏まえた方針を記載する。

ア　前年度の総合評価

前年度（策定等の作業を行う年度）の対策推進計画に盛り込まれた各取組の実績、情報セキュリティインシデントの発生状況、その他の取組の状況等に関する情報の収集・分析を行い、現在の年度における取組を総合的に評価した結果を記載する。

なお、記載事項としては以下のものが挙げられる。

・　前年度の対策推進計画に照らした取組の実績

→　単に計画どおりのスケジュールで取組が実施されたかなどではなく、計画において設定した方針や重点に照らして実施した結果が妥当であったか、組織として新たに対応すべき課題が確認されたか、計画策定後に計画に影響を及ぼすような情勢の変化は生じたかなど、改善点や反省教訓の抽出に主眼を置いて記載する

・　前年度に発生した情報セキュリティインシデント

→　自組織において発生した情報セキュリティインシデントや、他組織において発生した情報セキュリティインシデントを踏まえて新たに対応すべき課題はないかなど、改善点や反省教訓の抽出に主眼を置いて記載する

・　その他の取組の状況等

→　情報セキュリティ対策推進会議（CISO 等連絡会議）における申合せ事項等への対応など、対策推進計画策定以降に生じた新たな取組に係る対応状況について記載する

イ　総合評価を踏まえた方針

総合評価によって把握した自組織における情報セキュリティに係るリスクや課題に加え、政府機関全体としての動向その他の情報セキュリティを取り巻く情勢を踏まえ、情報セキュリティ対策の方針を記載する。

なお、記載事項としては以下のものが挙げられる。

・　複数の取組の共通的な方向付けによる重要課題への対応

（例）　前年度に発生した情報セキュリティインシデントや本部監査において助言された事項がある場合､関係する情報システムに対する技術的な対策の強化、原因となった事象を重点とした教育、自己点検及び情報セキュリティ監査を推進するため、全体方針において、優先的に対応すべき事項や自組織で横断的に改善が必要な事項に位置付ける

・　最新の脅威・技術動向を踏まえた情報セキュリティ強化への対応

（例）　直近で統一基準の改定が行われている場合、自組織の現在の情報セキュリティ体制と同基準を照らし合わせ、新たに措置が必要となると考えられる事項（例えば、動的なアクセス制御の実装、サービス不能攻撃対策の強化、標的型攻撃メールへの適切な対処）を重点的に実施すべき取組に位置付ける

⑵　「個別の取組の方針・重点等」に係る記載事項

「個別の取組の方針・重点等」は、「全体方針」を踏まえて、計画対象期間における情報セキュリティ対策に関する個々の取組をどのような方針・重点により、どのようなスケジュールで実施するかについて、個々の取組ごとに記載する。

なお、実施(予定)時期を別途線表にまとめる場合は、本項目では取組の主な流れを把握できる程度の粒度で記載し、細部的事項は線表のみに記載するなどの対応としても差し支えない。

ア　情報セキュリティに関する教育

情報セキュリティに関する教育に係る実施方針や重点の検討に当たっての主眼点としては、以下の事項が挙げられる。

なお、統括情報セキュリティ責任者は、ここで定めた方針・重点等に則して教育実施計画を策定することとなる。

・　教材の充実・見直し

→　特定の事象や新たなリスク等（例えば、標的型攻撃メール、サプライチェーン・リスク、ソーシャルメディアの利用）に重点を置いた教材を作成する、事例（例えば、失敗事例・その際に取るべきであった対応等）をまとめた教材を作成するなど

・　教育の対象者ごとの重点化

→　幹部職員を対象とした情報セキュリティマネジメントに関する集合教育を実施する、CSIRT 要員を対象とした専門家による研修を実施するなど

・　教育機会の拡充

→　集合教育の実施回数を増加させる、ｅラーニングを整備・活用する、定期的な標的型攻撃メールに備えた訓練を実施するなど

イ　情報セキュリティ対策の自己点検

情報セキュリティ対策の自己点検に係る実施方針や重点の検討に当たっての主眼点としては、以下の事項が挙げられる。

なお、統括情報セキュリティ責任者は、ここで定めた方針・重点等に則して年度自己点検計画を策定することとなる。

・　点検項目の重点化

→　特定の事象や新たなリスク等に関する点検項目を詳細化するなど

ウ　情報セキュリティ監査及び過年度の監査結果を踏まえた取組

情報セキュリティ監査及び過年度の監査結果（本部監査の結果を含む。）を踏まえた取組に係る実施方針や重点の検討に当たっての主眼点としては、以下の事項が挙げられる。

なお、情報セキュリティ監査責任者は、ここで定めた方針・重点等に則して監査実施計画を策定することとなる。

・　情報セキュリティ監査の重点監査対象・重点監査テーマの設定

→　特定の組織（たとえば、内部部局、地方支分部局又はその一部）ごとに重点的に監査を行う、特定の要件に合致する対象（たとえば、機微な情報を取り扱

う部署や情報システム、インターネットからアクセスさせることを前提とする情報システム等）に対する監査を行う、特定の脅威や脆弱性への対策（たとえば、端末の盗難・紛失対策、情報システムの脆弱性対策（ソフトウェア更新・パッチ適用等）の実施状況）に関する監査を行う、過年度の監査結果を踏まえリスクが高いと考えられる事項に関する監査を行うなど

・　情報セキュリティ監査の強化・見直し

→　監査の実施体制を強化する、監査の方法（書面監査、実地監査、情報システムの脆弱性検査等）を充実させるなど

エ　情報システムに関する技術的な対策を推進するための取組

情報システムに関する技術的な対策を推進するための取組に係る実施方針や重点の検討に当たっての主眼点としては、以下の事項が挙げられる。

・　政府機関全体としての取組への対応

→　CISO 等連絡会議における申合せ事項、NISC からの注意喚起、高度サイバー攻撃対処のためのリスク評価等のガイドラインに基づく取組等にどのように対応するかなど

・　脆弱性検査やペネトレーションテスト等において検出された課題への対応

→　課題が検出された情報システム等においてどのように対処するか、検出された課題を踏まえて組織全体としてどのような対応を採るかなど

・　主要な情報システム（基幹 LAN システム等）のセキュリティ強化

→　新たなリスク等に対応していくためのセキュリティ強化(機能･体制の強化、運用の見直し等）にどのように取り組むかなど

オ　所管する独立行政法人及び指定法人のセキュリティ対策の評価及びその推進に資するための取組（独法等を所管する国の行政機関に限る。）

所管する独法等のセキュリティ対策の評価及びその推進に資するための取組に係る実施方針や重点の検討に当たっての主眼点としては、以下の事項が挙げられる。

・　情報セキュリティ対策が適切に推進されるために必要な自組織の体制の整備

→　所管する独法等の情報セキュリティ対策に関する目標の策定及び実施状況に関しての評価、指導等を当該法人所管部署が適切に行うために必要な自組織の体制の整備方針や対処方針など

カ　その他情報セキュリティ対策に関する重要な取組

ア～オに該当しない情報セキュリティ対策に関する重要な取組に係る実施方針や重点の検討に当たっての主眼点としては、以下の事項が挙げられる。

・　情報セキュリティ関係規程の整備・見直し

→　統一基準の改定その他の情勢の変化に応じた関係規程の見直しや、新たな IT サービスの利用等に関する規程の整備をどのような方針等で行うかなど

・　情報システムの調達・外部委託関連の取組

→　情報システム等に関する調達における仕様書のセキュリティ要件のチェックに係る制度・体制を確立するなど

・　情報セキュリティに係る体制整備

→　情報セキュリティ担当部署やCSIRT等の体制を強化する、それらの間の連携を強化する、業務委託契約により情報セキュリティに関する知見を有する外部の専門家等による必要な支援を得られる体制を整備するなど

・　監査結果に応じた対処

→　自組織内で横断的に改善が必要な事項や、組織特有の改善が必要な事項についての改善措置の実施、改善計画の推進など

・　機関等支給以外の端末の利用時の取組

→　業務の遂行に当たってやむを得ず、機関等支給以外の端末の利用を認める場合における、規程類の整備や安全対策措置等の整備・充実など

・　中長期的な情報セキュリティ対策の強化に係る取組

→　単年単位の計画だけではなく、複数年に渡って中長期的な目線で情報セキュリティの強化策の計画（例：ゼロトラストアーキテクチャ適用に向けた導入計画）を策定するなど