総行サ第１号
令和８年４月１日

各都道府県知事
各都道府県議会議長
各指定都市市長
各指定都市市議会議長
御中

総務省自治行政局長
（公印省略）

地方公共団体におけるサイバーセキュリティを確保するための方針の
策定又は変更に関する指針の策定について（通知）

地方自治法の一部を改正する法律（令和６年法律第６５号。以下「改正法」という。）は、令和６年６月２６日に公布され、地方公共団体等におけるサイバーセキュリティを確保するための方針等に係る規定（地方自治法（昭和２２年法律第６７号）第２４４条の６及び地方独立行政法人法（平成１５年法律第１１８号）第２４条の２）については、令和８年４月１日（以下「改正法施行日」という。）に施行されました。

本改正においては、普通地方公共団体、特別区、一部事務組合及び広域連合の議会、長（地方公営企業の管理者を含む。）、委員会及び委員並びに地方独立行政法人（以下「執行機関等」という。）は、サイバーセキュリティを確保するための方針（以下「方針」という。）を定め、及びこれに基づき必要な措置を講じなければならないものとされ（地方自治法第２４４条の６第１項）、総務大臣は、方針の策定又は変更について指針を示すこととされています（同法第２４４条の６第３項）。

今般、「地方公共団体におけるサイバーセキュリティを確保するための方針の策定又は変更に関する指針」を策定しましたので、お知らせします。（本指針は、令和７年４月１日付け総行サ第１号において通知した「地方公共団体におけるサイバーセキュリティを確保するための方針の策定又は変更に関する指針（案）」と同内容です。）

各都道府県知事におかれては、貴都道府県内の指定都市を除く市区町村長及び市区町村議会議長に対してもこの旨周知願います。また、その際には、一部事務組合、広域連合及び地方独立行政法人にも、対応に遺漏なきよう併せて周知願います。

なお、地域の元気創造プラットフォームにおける一斉通知・調査システムを通じて、各市町村に対して、本通知についての情報提供を行っていること、及び本通知は、地方自治法第２４５条の４第１項に基づく技術的な助言であることを申し添えます。

＜送付資料＞

別紙１　地方公共団体におけるサイバーセキュリティを確保するための方針の策定又は変更に関する指針

連絡先:
自治行政局住民制度課サイバーセキュリティ対策室
桑折、松崎、大野
TEL:03-5253-5333(直通)
E-mail:lg-security@soumu.go.jp

地方公共団体におけるサイバーセキュリティを確保するための方針の策定又は変更に関する指針

第１　本指針の位置付け

地方公共団体における情報セキュリティ対策に関しては、これまで総務省として地方公共団体における情報セキュリティポリシーに関するガイドライン（以下「ガイドライン」という。）を示し、各地方公共団体においては、ガイドラインを踏まえ、個別の団体の事情に応じた情報セキュリティ対策が自主的に講じられてきたところである。

昨今、国・地方公共団体・民間企業・住民の間のネットワークを通じた相互接続がますます進展していることに伴い、一つの地方公共団体の情報セキュリティ対策の不備や不適切なシステム利用が、他の地方公共団体や国の機関等の情報セキュリティにも脅威となり、その安全性や信頼性に影響を与える蓋然性が高くなっている。こうした情報セキュリティ対策の重要性の高まりを踏まえ、第33次地方制度調査会「ポストコロナの経済社会に対応する地方制度のあり方に関する答申」（令和５年12月21日）においては、「地方公共団体が講ずべき情報セキュリティ対策に係る指針を国が示すとともに、地方公共団体に対し、情報セキュリティ対策の方針の策定義務及びその方針に基づく措置の実施義務を課すこととすべき」とされた。これを受けて、地方自治法（昭和22年法律第67号）等が改正され、普通地方公共団体、特別区、一部事務組合及び広域連合（以下「地方公共団体」という。）の議会、長（地方公営企業の管理者を含む。）、委員会及び委員並びに地方独立行政法人（以下「執行機関等」という。）は、サイバーセキュリティを確保するための方針（以下「方針」という。）を定め、及びこれに基づき必要な措置を講じなければならないものとされるとともに、方針の策定又は変更について、総務大臣が指針（以下「指針」という。）を示すこととされた。

引き続き、地方公共団体等（地方公共団体及び地方独立行政法人をいう。以下同じ。）は、自らの責任において情報セキュリティ対策を講じていくことが原則となるが、今後、全ての執行機関等において指針に沿った形で方針が定められ、一定以上の水準の情報セキュリティ対策が講じられることが求められる。さらに、国においては、サイバー攻撃によるリスクの増大に対応するため、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である「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群」が順次改定されるとともに、DXの浸透、AIや量子技術の進展、複雑化する安全保障環境等、急速に変化するサイバー空間を巡るリスクを踏まえた情報セキュリティ対策の改善・強化がこれまで以上に重要になっている。ガイドラインには、こうした動きを適時に反映していくこととしているため、地方公共団体等においても、国の動向及びガイドラインを踏まえて方針を不断に見直し、必要な措置を確実に講じていくことが求められている。

これらを踏まえ、地方自治法第 244 条の 6 第 3 項の規定に基づき、指針を定めるものである。

第 2　地方公共団体等における情報セキュリティとその対策

1　地方公共団体等における情報セキュリティの考え方

地方公共団体等は、法令等に基づき、住民の個人情報や企業の経営情報等の重要情報を多数保有するとともに、ほかに代替することができない行政サービスを提供している。また、地方公共団体等の業務の多くが情報システムやネットワークに依存していることから、住民生活や地域の社会経済活動を保護するため、地方公共団体等は、情報セキュリティ対策を講じて、その保有する情報を守り、業務を継続することが必要となっている。

今後、各種手続のオンライン利用の本格化や情報システムの高度化等、電子自治体が進展することにより、情報システムの停止等が発生した場合、広範囲の業務が継続できなくなり、住民生活や地域の経済社会活動に重大な支障が生じる可能性も高まる。また、地方公共団体等は LGWAN（総合行政ネットワーク）等のネットワークにより相互に接続しており、一部の団体で発生した IT 障害がネットワークを介して他の団体に連鎖的に拡大する可能性は否定できない。

これらの事情から、全ての地方公共団体等において、情報セキュリティ対策の実効性を高めるとともに対策レベルを一層強化していくことが必要となっている。また、情報セキュリティの確保に絶対安全ということはないことから、情報セキュリティに関する障害・事故及びシステム上の欠陥（以下「情報セキュリティインシデント」という。）の未然防止のみならず、情報セキュリティインシデントが発生した場合の拡大防止・迅速な復旧や再発防止の対策を講じていくことが必要である。

なお、情報セキュリティ対策は、個人情報保護対策と内容的に重なる部分も多い。例えば、個人情報保護のための情報セキュリティ対策ともいえる安全管理措置については、個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「個人情報保護法」という。）第 66 条第 1 項において、地方公共団体等は、保有個人情報の漏えい、滅失又は毀損の防止その他の保有個人情報の安全管理のために必要かつ適切な措置を講じなければならないことが定められている。また、個人情報保護法第 66 条第 2 項各号において、地方公共団体等の委託先、指定管理者及び以上の者から当該各号に定める業務の委託（二以上の段階にわたる委託を含む。）を受けた者も、地方公共団体等と同等の安全管理措置を講じる義務を負う旨が定められており（同項第 1 号・第 2 号・第 5 号）、その点について地方公共団体等においても留意することが求められる。その上で、地方公共団体等においては、安全管理措置の一環として、委託先へ適切な監督や指導等を行うことが求められ、（参考：個人情報の保護に関する法律について

のガイドライン（行政機関等編）、個人情報の保護に関する法律についての事務対応ガイド（行政機関等向け）、個人情報の保護に関する法律についてのQ&A（行政機関等編））また、指定管理者に対しても、条例において個人情報の保護に関して必要な事項を指定管理者との間で締結する協定に盛り込むことを規定すること、必要に応じて地方自治法第 244 条の 2 第 10 項及び第 11 項に規定する監督権限を行使することなど、必要な措置を講ずる責務を負っていることから、これらの責務を果たすため、必要に応じて指定管理者において講ずる安全管理措置全体の状況について指導や監督等を行うことが考えられる。加えて、地方公共団体等において、保有個人情報の漏えい、滅失、毀損その他の保有個人情報の安全の確保に係る事態であって個人の権利利益を害するおそれが大きいものとして個人情報保護委員会規則で定めるものが生じたときは、個人情報保護法第 68 条第 1 項及び第 2 項により、個人情報保護委員会への報告を行わなければならないほか、原則として本人に通知を行う必要がある。なお、地方公共団体等から個人情報の取扱いの委託を受けた者が個人情報取扱事業者に該当する場合、当該事業者において個人情報保護委員会規則で定めるものが生じた際は同様の対応が必要となる。

自然災害時や感染症のまん延時における対応という意味では防災対策とも重なる。情報セキュリティを対策する部署とこれらを担当する部署は、相互に連携をとって、それぞれの対策に取り組むことが求められる。

また、地方公共団体は、自らの情報セキュリティを確保するとともに、地域全体の情報セキュリティの基盤を強化するため、地域における広報啓発や注意喚起、官民の連携・協力等に積極的に貢献することが望まれる。例えば、住民等への広報による啓発、IT 講習等による住民等への情報セキュリティに関する研修の実施、業務面で関係する団体に対する情報セキュリティポリシーの策定の働きかけなどの取組を行うことが考えられる。

2　情報セキュリティポリシーの必要性と構成

地方公共団体等においては、情報セキュリティ対策を徹底するには、対策を組織的に統一して推進することが必要であり、そのためには組織として意思統一し、明文化された文書として、情報セキュリティポリシーを定めなければならない。

情報セキュリティポリシーの体系は階層構造となっており、基本的な考え方を定めるものが「基本方針」、基本方針に基づき共通の情報セキュリティ対策の基準を定めるものが「対策基準」である。この「基本方針」と「対策基準」を総称して「情報セキュリティポリシー」という。さらに「対策基準」を具体的なシステムや手順、手続に展開して個別の実施事項を定めるものが「実施手順」である。

このように、情報セキュリティポリシーは、情報セキュリティ対策の頂点に位置するものであることから、地方公共団体等の長をはじめ、全ての職員等及び委託事業者は、業務の遂行に当たって情報セキュリティポリシーを遵守する

義務を負う。
　そのため、地方公共団体等は情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じることが必要である。また、委託事業者の情報セキュリティポリシーの遵守を担保するため、業務委託の際に、情報セキュリティ要件を明記した契約を締結の上、委託事業者における対策の実施を確認することも重要である。

3　策定を要する方針及び方針の公表

　すでに多くの地方公共団体等において、ガイドライン等を踏まえて情報セキュリティポリシーが定められており、当該ポリシーに沿って、体制が構築され、対策が講じられている。そのため、これまで情報セキュリティポリシーを策定している地方公共団体等においては、既存の情報セキュリティポリシーの基本方針について、指針を十分に踏まえて必要に応じて見直しを行ったものの策定をもって、地方自治法第 244 条の 6 第 1 項（地方独立行政法人法（平成 15 年法律第 118 号）第 24 条の 2 において準用する場合を含む。）に規定する方針に位置付けることとして差し支えない。
　情報セキュリティポリシーを未策定の執行機関等においては、令和 8 年 4 月 1 日の法施行までに情報セキュリティポリシー（少なくとも基本方針）を策定し、基本方針をもって方針とする等の対応をとることが必要であり、その際、ガイドラインを十分に参照して策定することが必要である。
　なお、情報セキュリティポリシーのうち、対策基準については、情報セキュリティを確保するために公表すべきでない情報が含まれる場合があることから方針には含めないが、未策定の執行機関等においては、個別の執行機関等の情報システムの利用の状況に応じて、基本方針の策定と併せて又は今後策定することを検討されたい。
　方針を策定又は変更した際は、住民に対し、どのように情報セキュリティの確保を図ろうとしているのかについての説明責任を果たすとともに、情報セキュリティ対策の質を確保し、実効性や透明性の維持・向上を図るため、公表を要することとされており（地方自治法第 244 条の 6 第 2 項)、対応に万全を期されたい。

4　方針を策定する必要がある主体

　執行機関等ごとに業務の内容・性質が異なり、必要となる情報セキュリティ対策も異なりうることから、方針はそれぞれの執行機関等が策定する必要がある。
　現在、個別の行政分野について、その所管省庁が情報セキュリティに関して個別にガイドラインや基準を定めている場合がある。このような行政分野を担任する執行機関等（議会を除く。）においては、
①　指針に基づき方針を定め、その方針のもとで、個別のガイドラインに基づ

き具体の対策を講じる
② 個別のガイドラインに基づき基本方針を定めるとともに、具体の対策を講じる
のいずれかの対応をとることとなる。②の場合に関しては、指針の対象範囲から、政令で定める執行機関が定めるものを除くことができることとされており（地方自治法第 244 条の 6 第 3 項)、当該政令において対象から除外する執行機関は、公安委員会とされているため、留意されたい。

なお、必要となる情報セキュリティ対策が概ね同様のものとなるなど別個の方針を定めることが非効率となるような場合に、一つの方針を複数の執行機関等で共同で策定する（委員会及び委員においては、地方自治法第 180 条の 7 の規定に基づき長の補助機関に委任する、その他の執行機関及び議会においては、長との連名により共同で策定すること等が考えられる）など、運用上の工夫を行うことも可能である。

5 情報セキュリティ対策の実施サイクル

情報セキュリティ対策の実施プロセスは、策定・導入（Plan)、運用（Do)、評価（Check)、見直し（Action）の 4 段階に分けることができ、この実施サイクル（PDCA サイクル）を繰り返すことによって情報セキュリティは確保される。この PDCA サイクルを定期的に繰り返すことで環境の変化に対応しつつ、情報セキュリティ対策の水準の向上を図らなければならない。

第 3 地方公共団体等における情報セキュリティの管理プロセス

1 策定及び導入

（1）策定及び導入の概要

方針の策定及び導入に当たっては、まず、策定のための組織体制を確立し、その組織体制の下で方針を策定し、正式に決定する。この後、職員等への周知、住民への公表を行うというプロセスになる。

（2）組織体制の確立

① 組織体制の確立

方針の策定には、幹部職員の関与が不可欠である。また、方針は、組織内の様々な部局の情報資産に係る問題を取り扱うことから、責任の所在を明確にするため、全ての部局の長、情報システムを所管する課室長及び情報セキュリティに関する専門的知識を有する者などで構成する組織又はこれに代わる組織（以下「情報セキュリティ委員会等」という。）が行う。

（注 1）小規模の団体の場合には、新たに組織を立ち上げるのではなく、「情報化推進委員会」等の既存の類似する組織が行う場合もあり

得る。
（注２）組織が有機的に機能するために全組織横断的な指示、連絡可能な役割及び権限を明確にすることが望ましい。

② 方針策定チームの編成

情報セキュリティ委員会等は、方針の策定作業の一部を下部の組織に行わせることができる。策定チームには、全ての部、課等の関係者が関与することが望ましいが、主たる関係部署に絞って構成する場合もある。

（３）方針の策定

方針においては、情報セキュリティ対策の目的、体系等、各執行機関等の情報セキュリティに対する基本的な考え方を示す。なお、ガイドラインにおいて、基本方針の策定例及び解説を示しているところであり、ガイドラインを十分に参照し、各執行機関等におけるネットワーク構成等の個別の事情に即して方針（基本方針）を策定することが重要である。

方針に規定すべき項目については、次のとおりである。(9 については、各執行機関等の情報システムの状況等にもよるため推奨事項とするが、対策基準・実施手順を策定する場合は、方針に規定すること。)

1. 方針の目的
2. 定義
3. 対象とする脅威
4. 適用範囲
5. 職員等の遵守義務
6. 組織体制の確立、情報資産の分類・管理、物理的・人的・技術的セキュリティ対策をはじめとした情報セキュリティ対策
7. 情報セキュリティ監査・自己点検の実施
8. 情報セキュリティポリシーの見直し
9. 情報セキュリティ対策基準・実施手順の策定

（４）方針の決定

情報セキュリティ委員会等が策定した方針について、執行機関等の長の決裁等により、当該執行機関等における方針として正式に決定する。

（５）方針の周知・公表

情報セキュリティ対策を最終的に実施するのは職員等であるため、実効性を確保するため方針の配布や説明会などにより、方針を職員等に十分に周知するとともに、住民に公表する。

2　運用

方針を確実に運用していくため、情報システムの監視や方針に従って対策が適正に遵守されているか否かを確認し、情報資産に対するセキュリティ侵害や方針違反に対し、適正に対応しなければならない。

3　評価・見直し

方針の実効性を確保するとともに、情報資産や情報システム等の変化、情報セキュリティに関する脅威や対策等の変化に対応していくためには、方針の評価・見直しを行い、前述の PDCA サイクルを繰り返すとともに、PDCA サイクルの有効性の確認のために監査・自己点検を活用し、情報セキュリティ対策を不断に強化し続けることが不可欠である。

（1）監査・自己点検

情報セキュリティ対策の実効性を確保するには、情報セキュリティ対策の実施状況を検証し、方針の見直しに反映させることが必要である。このため、独立かつ専門的知識を有する専門家（部内者であっても監査対象から独立した監査担当者等が行う場合を含む。）による検証である情報セキュリティ監査や情報システム等を運用する者自らによる検証である自己点検を行う。

（2）方針の見直し

方針の見直し作業は、情報セキュリティ委員会等の下で、方針の策定手順に準じて実施する。