会計検査院法第30条の2の規定に基づく報告書

「国による地方公共団体の情報セキュリティ対策の強化について」

令　和　2　年　1　月

会　計　検　査　院

我が国では、インターネット等の高度情報通信ネットワークの整備及び情報通信技術の活用の進展に伴って世界的規模で生じているサイバーセキュリティに対する脅威の深刻化等に伴い、情報の自由な流通を確保しつつ、サイバーセキュリティの確保を図ることが喫緊の課題となっている。

また、行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号）の成立により、マイナンバー利用事務並びに国、地方公共団体等の各機関の間でマイナンバーをその内容に含む個人情報（特定個人情報）について情報照会及び情報提供を行う情報連携が行われることとなっており、地方公共団体の情報セキュリティ対策の強化は公的機関全体にとって重要な課題となっている。

このような中、マイナンバー制度の施行を控えた平成27年5月に日本年金機構が外部から標的型攻撃を受け、日本年金機構内のＬＡＮシステム上の共有フォルダに保存されていた個人情報が外部に流出する事案が発生したことは、多くの住民情報を扱う地方公共団体にとって重大な警鐘となった。

上記の事案等を踏まえ、総務省は、同年12月に各地方公共団体に通知を発出して、三層から成る対策を講ずることにより情報セキュリティ対策の抜本的強化を図るよう要請するとともに、27、28両年度に地方公共団体へ、情報セキュリティ対策の強化を目的とする補助金を交付している。また、マイナンバー利用事務が28年1月から、情報連携が29年11月から行われている。

本報告書は、以上のような経緯等を踏まえて、地方公共団体における情報セキュリティ対策強化等の状況について検査を実施し、その状況について取りまとめたことから、会計検査院法（昭和22年法律第73号）第30条の2の規定に基づき、会計検査院長から衆議院議長、参議院議長及び内閣総理大臣に対して報告するものである。

令　和　2　年　1　月
会　計　検　査　院

目　次

・本文及び図表中の数値は、表示単位未満を切り捨てている。

・上記のため、図表中の数値を集計しても計が一致しないものがある。

事 例 一 覧

国による地方公共団体の情報セキュリティ対策の強化について

検　査　対　象	総務省、241地方公共団体（18都道府県、223市区町村）
地方公共団体における情報セキュリティ対策の強化に係る補助事業の概要	二要素認証及び情報持出し不可設定の導入、ＬＧＷＡＮ接続系とインターネット接続系の分割並びに自治体情報セキュリティクラウドの構築の三層から成る対策を講ずることにより地方公共団体の情報セキュリティ対策の抜本的な強化を図るもの
上記の補助事業に係る検査対象の241地方公共団体に対する国庫補助金交付額	61億3920万円（平成27、28両年度）
自治体情報セキュリティ支援プラットフォームの概要	ネットワークシステム上で地方公共団体の担当者がセキュリティ専門家からの助言を受けたり、他の地方公共団体との事例の共有を行ったりするもの
上記の構築等に係る支払額	4752万円（平成27年度）

1　検査の背景

(1) 情報セキュリティ対策に係る制度等の概要

ア　国及び地方公共団体における情報セキュリティ対策に係る制度等の概要

我が国では、インターネット等の高度情報通信ネットワークの整備及び情報通信技術の活用の進展に伴って世界的規模で生じているサイバーセキュリティに対する脅威の深刻化等に伴い、情報の自由な流通を確保しつつ、サイバーセキュリティの確保を図ることが喫緊の課題となっている。

このような課題に対処するため、平成26年に、サイバーセキュリティに関する施策を総合的かつ効果的に推進し、もって経済社会の活力の向上及び持続的発展並びに国民が安全で安心して暮らせる社会の実現を図るとともに、国際社会の平和及び安全の確保並びに我が国の安全保障に寄与することを目的として、サイバーセキュリティ基本法（平成26年法律第104号。以下「基本法」という。）が制定されている。

基本法によれば、国は、サイバーセキュリティに関する総合的な施策を策定し、及び実施する責務を有するとされており、地方公共団体は、国との適切な役割分担

を踏まえて、サイバーセキュリティに関する自主的な施策を策定し、及び実施する責務を有するとされている。そして、政府は、サイバーセキュリティに関する施策の総合的かつ効果的な推進を図るために、サイバーセキュリティに関する基本的な計画として、サイバーセキュリティ戦略を定めなければならないとされている。

27年9月に定められたサイバーセキュリティ戦略（平成27年9月4日閣議決定）によれば、地方公共団体は、取り扱う情報の機微性等の事情を踏まえて、政府機関等と同様のセキュリティを確保することが求められるとされている。そして、個人番号(注1)（以下「マイナンバー」という。）の導入に伴い、政府としても、サイバーセキュリティが確保されるよう基本法等に基づき必要な支援を実施していくとともに、地方公共団体の情報システムについて、社会保障・税番号制度（以下「マイナンバー制度」という。）の運用に係るセキュリティを強化する観点から必要な対策を検討し、講じていくとされている。また、行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号。以下「マイナンバー法」という。）に規定されたマイナンバー利用事務(注2)において使用するシステムについて、インターネットから独立するなどの高いセキュリティ対策を踏まえたシステム構築や運用体制の整備を含めて検討した上で、必要な措置を講ずるとともに、関係機関が連携して専門的・技術的知見を有する監視・監督体制を整備するとされている。

そして、マイナンバー利用事務は、マイナンバー法に基づき28年1月から行われている。

（注1）　個人番号　　国民一人一人に付与された唯一無二となる12桁の番号。国民の氏名、住所、性別及び生年月日と関連付けられている。
（注2）　マイナンバー利用事務　　行政機関等、地方公共団体等その他の者が、法令に基づき行う社会保障、税及び災害対策に関する特定の事務において、保有している個人情報の検索や管理のためにマイナンバーを利用する事務

イ　地方公共団体における情報システム、情報セキュリティ対策等の概要

(ｱ) 情報セキュリティ対策の強化以前の地方公共団体における情報システム等の概要

地方公共団体は、独自に情報システム及び情報通信ネットワークを構築して、住民に対して行政サービスを提供している。そして、地方公共団体が構築している情報システムは、大別して、住民基本台帳ネットワークシステム（以下「住基ネット」という。）に接続して戸籍事務等に使用する情報システム（以下「基幹

系システム」という。）、ＬＧＷＡＮ(注3)に接続して地方公共団体の事務を行う情報システム、インターネットに接続してメール、Ｗｅｂ閲覧等に使用する情報システム等となっている。

（注3）　ＬＧＷＡＮ　地方公共団体内のネットワークを相互に接続する総合行政ネットワーク

(ｲ) マイナンバー制度における地方公共団体等の情報連携の概要

地方公共団体等は、マイナンバー制度の導入に当たり、情報システムの整備（既存システムの改修を含む。）を行っている。そして、それらの情報システムにおいて、マイナンバー法に基づき28年1月からマイナンバー利用事務が実施され、29年11月から総務省が管理する情報提供ネットワークシステム（以下「情報提供ＮＷＳ」という。）(注4)等を通じて相互に特定個人情報を照会し、又は提供する情報の連携が行われている（以下、特定個人情報の照会及び提供を合わせて「情報連携」という。）。また、情報連携の仕組みの構築に当たっては、国の行政機関の組織内のネットワークを相互に接続する政府共通ネットワーク及びＬＧＷＡＮがそれぞれ改修されて活用されている。

（注4）　特定個人情報　マイナンバー（マイナンバーに対応し、当該マイナンバーに代わって用いられる番号、記号その他の符号であって、住民票コード以外のものを含む。）をその内容に含む個人情報

(ｳ) 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の概要

地方公共団体は、法令等に基づき、住民の個人情報（住民基本台帳に記載された住民の氏名、住所、生年月日、性別の情報や特定個人情報等。以下「住民情報」という。）等の重要な情報を多数保有するなどしている。そして、地方公共団体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、住民生活等を保護するために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。

総務省は、各地方公共団体が情報セキュリティポリシーの策定や見直しを行う際の参考として、13年3月に、「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」（平成30年9月最終改定。以下「セキュリティポリシーガイドライン」という。）を策定している。

セキュリティポリシーガイドラインによれば、情報セキュリティ対策を徹底するためには、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、

地方公共団体は、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とされている。そして、基本法第5条において、地方公共団体がサイバーセキュリティに関する自主的な施策を策定して実施することが責務規定として法定化されたことを踏まえて、地方公共団体において情報セキュリティポリシーを策定することが必須となり、策定済みの地方公共団体においても適時適切に見直しを行うことなどが重要であるとされている。

また、セキュリティポリシーガイドラインによれば、情報セキュリティポリシーとは、組織内の情報セキュリティを確保するための方針、体制、対策等を包括的に定めたものとされている。そして、情報セキュリティポリシーは、各地方公共団体の情報セキュリティ対策における基本的な考え方を定めた「情報セキュリティ基本方針」（以下「基本方針」という。）と、基本方針に基づき全ての情報システムに共通の情報セキュリティ対策の基準を定めた「情報セキュリティ対策基準」（以下「対策基準」という。）で構成されるものとされている。

(2) 情報セキュリティ対策の強化の概要等

ア　地方公共団体の情報セキュリティ対策の強化の経緯

(1)イ(ｱ)のとおり、地方公共団体は、独自に情報システム及びネットワークを構築して住民に対して行政サービスを提供しており、総務省は、サイバー攻撃が急速に複雑・巧妙化している中で、地方公共団体の情報セキュリティ対策を強化することが喫緊の課題であるとしている。特に、マイナンバー法の成立によりマイナンバー利用事務及び全国の地方公共団体等の情報システムの情報連携が行われることとなったため、各地方公共団体においては、より一層情報セキュリティを強化することが必要とされた。

このような中、マイナンバー制度の施行を控えた27年5月に、日本年金機構が外部から標的型攻撃(注5)を受けて、同機構内のＬＡＮシステム上の共有フォルダに保存されていた約125万件（対象者約101万人分）の基礎年金番号、氏名等の個人情報がインターネットを通じて不正に外部に流出したとされる事案（以下、この標的型攻撃による個人情報流出を「年金情報流出事案」という。）が発生した。年金情報流出事案の原因の究明、再発防止策の検討等を行った同機構の調査委員会の報告書等によれば、年金情報流出事案を発生させた直接的な要因は、標的型攻撃を受けた場合における対応としてＬＡＮケーブルの抜線以外に具体的な定めがなく、事態の確認が

遅れて有効な対策が講じられなかったことであるとされている。また、流出した個人情報には、所要のアクセス制限やパスワードの設定が行われていないものが多数あったとされている。

（注5）　標的型攻撃　　特定の組織に狙いを絞り、その組織の業務習慣等の内部情報について事前に入念な調査を行った上で、様々な攻撃手法を組み合わせ、その組織に最適化した方法を用いて行われる攻撃

また、会計検査院は、年金情報流出事案について、会計検査院法第30条の2の規定に基づき、28年12月に、「年金個人情報に関する情報セキュリティ対策の実施状況及び年金個人情報の流出が日本年金機構の業務に及ぼした影響等について」を国会及び内閣に報告している。同報告において、年金情報流出事案の発生に対応するための経費として日本年金機構が見込んだ支出額が27年度決算額で計10億8379万余円となるほか、年金情報流出事案が発生したことにより支出されたと考えられる経費が計9418万余円（厚生労働省分4687万余円、日本年金機構分4730万余円）となるなどしていることや、年金個人情報流出者に対する対応等に集中して取り組む必要が生じたことなどを理由に国民年金保険料の未納者に対する督促状等を送付しなかったことで、消滅時効期間が経過した国民年金保険料が債権額にして1億2115万余円（会計検査院試算）となることなどを記述している。

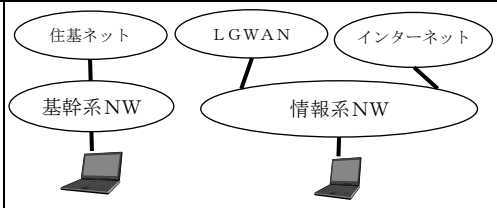
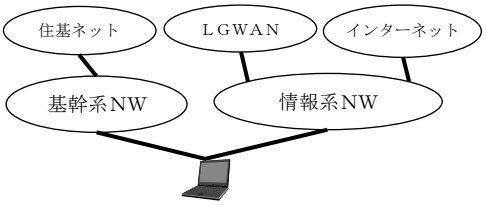
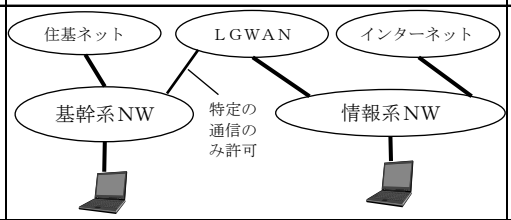
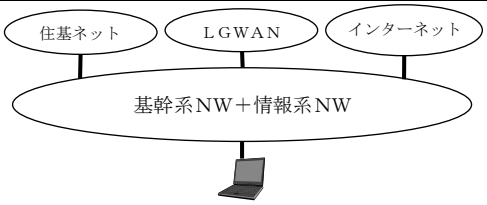
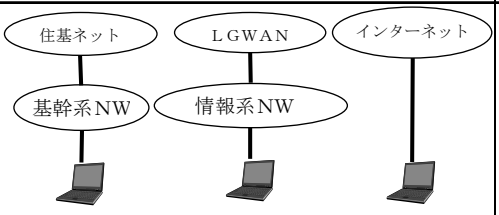
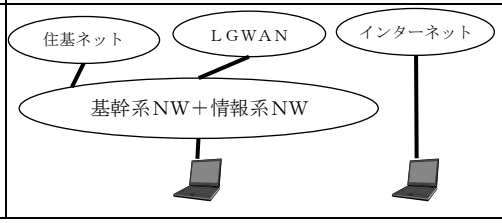
そして、地方公共団体においても、年金情報流出事案から間もない27年6月に、日本年金機構と同様の標的型攻撃を受けて基幹系システムをネットワークから切断することを余儀なくされるなどの事案が発生している。

年金情報流出事案等を受けて、総務省は、同月に、地方公共団体におけるネットワークの接続形態の現状を確認するために、①基幹系システムが接続する内部ネットワーク（以下「基幹系ＮＷ」という。）、②①以外の地方公共団体の事務を行う上で必要なシステムが接続する内部ネットワーク（以下「情報系ＮＷ」という。）、③①及び②以外のネットワークで各種情報の検索、住民や企業からのメールの受信等を行う外部のインターネットと接続しているネットワークそれぞれの構成について調査した（以下「6月調査」という。）。

6月調査によれば、地方公共団体におけるネットワーク接続形態は、図表0-1のとおり、基幹系ＮＷと情報系ＮＷを分離して、インターネットを情報系ＮＷに接続している形態（図表の1番から3番まで）や、基幹系ＮＷと情報系ＮＷを統合してインターネットにも接続している形態（同4番）が大半を占めており、多くの地方公共団

体において、住民情報を扱う基幹系システムやＬＧＷＡＮに接続するシステムがインターネットに接続するネットワーク内にある状況となっていた。また、インターネットに接続しているネットワークは独立しているが、基幹系ＮＷと情報系ＮＷを統合している形態（同6番）も見受けられた。

図表0-1　地方公共団体におけるネットワーク接続形態

番号	ネットワーク接続形態	概念図	地方公共団体数	割合
1	①基幹系ＮＷと②情報系ＮＷが分離（インターネットは情報系ＮＷに接続）		696	38.9%
2	①基幹系ＮＷと②情報系ＮＷが分離されているが、端末は共用（インターネットは情報系ＮＷに接続）		194	10.8%
3	①基幹系ＮＷと②情報系ＮＷが分離されているが、特定の業務に対して、通信ができるように設定（インターネットは情報系ＮＷに接続）		432	24.1%
4	①基幹系ＮＷと②情報系ＮＷを統合（インターネットにも接続）		341	19.0%
5	①基幹系ＮＷ、②情報系ＮＷ、③インターネットに接続しているネットワークがそれぞれ独立		37	2.0%
6	①基幹系ＮＷと②情報系ＮＷが統合、③インターネットに接続しているネットワークが独立		88	4.9%
計			1,788	100.0%

イ　総務省による地方公共団体への助言等

年金情報流出事案等を踏まえて、総務省は、地方公共団体の情報セキュリティに係る抜本的な対策を検討するために、27年7月に、情報システムに関する専門家等で構成する「自治体情報セキュリティ対策検討チーム」（以下「検討チーム」という。）を設置している。

総務省は、検討チームの会合において、6月調査の結果、地方公共団体において住民情報を扱うシステムやＬＧＷＡＮ、インターネットに接続しているシステムが分かれていない状況が確認されたことなどについて報告している。

検討チームは、同年8月に中間報告（以下「8月報告」という。）を取りまとめて、①組織体制の再検討、職員の訓練等の徹底、②インシデント即応体制の整備及び③インターネットのリスクへの対応の3項目について総務省に提言している。

そして、総務省は、各地方公共団体に対して、8月報告を参考に情報セキュリティ対策に積極的に努めるよう通知するとともに、同月に、検討チームにおける議論を踏まえた地方公共団体の情報セキュリティ対策の強化に係る留意事項について通知を発出して、助言等を行っている（以下、これらの通知を合わせて「8月通知」という。）。

8月報告及び8月通知の主な内容は次のとおりとなっている。

①　組織体制の再検討、職員の訓練等の徹底

・　最高情報セキュリティ責任者（ＣＩＳＯ）を設置し、その任務を明らかにするとともに、ＣＩＳＯを支えて自治体情報セキュリティ対策を推進する組織（ＣＳＩＲＴ等）(注6)を構築すること

・　インシデント発生時の国までの連絡ルートを再構築（多重化）(注7)すること

・　特に標的型攻撃に対する緊急時対応計画の見直しと緊急時対応訓練を逐次実施すること

（注6）　ＣＳＩＲＴ　　情報システムに対するサイバー攻撃等のインシデントが発生した際に、当該インシデントを正確に把握して分析し、被害の拡大防止、復旧、再発防止等を迅速かつ的確に行うことを可能にするための機能を有する体制

（注7）　多重化　　本報告書では、国及び庁内ＣＩＳＯ（市区町村においては都道府県を含む。）へ一斉同報することを指している。

②　インシデント即応体制の整備

・　都道府県ごとに都道府県ＣＳＩＲＴと市区町村ＣＳＩＲＴの連携体制を構築

しておくこと

・　アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を点検し、不正通信の監視機能を強化すること

・　インシデント事例、情報セキュリティＱ＆Ａ等を掲載する自治体情報セキュリティ支援プラットフォームを創設すること

③　インターネットのリスクへの対応

・　マイナンバー制度が施行されるまでに、庁内の住民基本台帳システム（既存住基）(注8)がインターネットを介して不特定の外部との通信を行うことができないようになっていることを確認すること

・　機密性(注9)はもとより、可用性(注10)や完全性(注11)の確保にも十分配慮された攻撃に強い内部ネットワーク等の構築（システムの強じん性の向上）を図ること

・　より高い水準のセキュリティ対策を講ずるため、インターネット接続ポイントの集約化やセキュリティ監視の共同利用等（自治体情報セキュリティクラウドの構築）の検討を進めるべきこと

(注8)　既存住基　住基ネット導入以前から使用されている住民基本台帳システム

(注9)　機密性　情報にアクセスすることを認められた者だけが情報にアクセスできる状態を確保すること

(注10)　可用性　情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保すること

(注11)　完全性　情報が破壊、改ざん又は消去されていない状態を確保すること

ウ　検討チームによる総務省への11月報告

検討チームは、8月報告で提言されていたシステムの強じん性の向上及び自治体情報セキュリティクラウドの構築について、次の①から③までの三層から成る対策（以下「三層の構え」という。図表0-2参照）を講ずることにより、同年11月に地方公共団体の情報セキュリティ対策を抜本的に強化することが必要であるとの報告（以下「11月報告」という。）を取りまとめて、総務大臣に報告している。

①　二要素認証及び情報持出し不可設定の導入

マイナンバー利用事務系(注12)（既存住基、税、社会保障、戸籍事務等）においては、原則として、他の領域との通信ができないように分離を徹底した上で、端末への二要素認証(注13)や端末からの情報持出し不可設定(注14)（以下、二要素認証と情報持出し不可設定を合わせて「二要素認証等」という。）の導入等を図ることにより、住民

情報の流出を徹底して防ぐこと

（注12）　マイナンバー利用事務系　　主に、従来は基幹系システムとして整理されてきた、マイナンバー利用事務、既存住基と密接に関わる戸籍事務等に供する情報システム（ハードウェア、ソフトウェア、ネットワーク等）及びデータ。代表的なシステムには、既存住基、税、社会保障、戸籍事務等がある。

（注13）　二要素認証　　本人確認の精度と安全性を高めるために、正規の利用者かどうかをシステムが判断する認証手段の三要素である知識（例：暗証番号）、所持（例：ＩＣカード）及び存在（例：静脈）のうち二つを併用するもの

（注14）　情報持出し不可設定　　ネットワーク上の情報持出しを制御するソフトウェア等により、ＵＳＢメモリ等の外部記憶媒体による端末からの情報持出しができないように設定すること

② ＬＧＷＡＮ接続系とインターネット接続系の分割

マイナンバーによる情報連携に活用されるＬＧＷＡＮ環境のセキュリティ確保に資するために、財務会計等のＬＧＷＡＮを活用する業務用システム（以下「ＬＧＷＡＮ接続系(注15)」という。）と、Ｗｅｂ閲覧やインターネットメール等のシステム(注16)（以下「インターネット接続系」という。）との通信経路を分割すること。なお、ＬＧＷＡＮ接続系とインターネット接続系との間で通信する場合には、ウイルス感染のない無害化通信を図ること

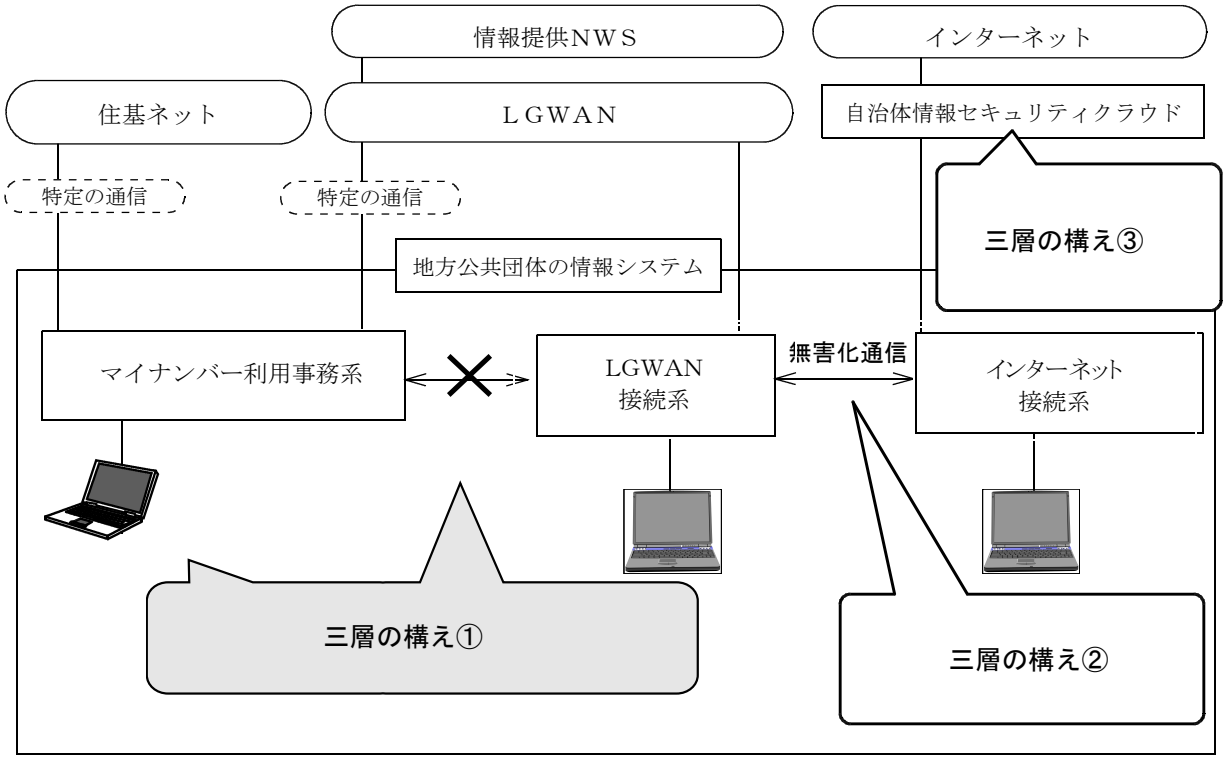
③ 自治体情報セキュリティクラウドの構築

インターネット接続系においては、都道府県と市区町村が協力してインターネット接続口を集約した上で、自治体情報セキュリティクラウドを構築し、高度なセキュリティ対策を講ずること

（注15）　ＬＧＷＡＮ接続系　　主に、従来は情報系システムとして整理されてきた、マイナンバー関係事務（法令に基づき、職員等のマイナンバーを必要な書類に記載して行政機関等に提出する事務）等に供する情報システム（ハードウェア、ソフトウェア、ネットワーク等）及びデータ。代表的なシステムには、人事給与、財務会計、文書管理等がある。

（注16）　インターネット接続系　　主に、従来は情報系システムとして整理されてきた、インターネットメール、Ｗｅｂ閲覧等に利用する情報システム（ハードウェア、ソフトウェア、ネットワーク等）及びデータ

図表0-2　三層の構えの概念図



エ　強化対策費補助金による補助事業等の概要

総務省は、11月報告を受けて、各地方公共団体に対して「新たな自治体情報セキュリティ対策の抜本的強化について」（平成27年12月総務大臣通知。以下「12月通知」という。）を発し、三層の構えを講ずることにより情報セキュリティ対策の抜本的な強化を図るよう要請するとともに、地方公共団体が行うこれらの対策に要する経費を総額510億円と見積もり、その2分の1を地方公共団体情報セキュリティ強化対策費補助金（以下「強化対策費補助金」という。）として、平成27年度補正予算により地方公共団体に交付することとした。また、残りの地方負担額については、原則として、地方負担額の100％まで地方債で充当できることとし、後年度における元利償還の財源は、地方財政計画の策定及び地方交付税の算定を通じて確保することとされた。

そして、平成27年度補正予算に強化対策費補助金として254億9859万余円が計上され、総務省は、27年度及び28年度に地方公共団体に対し強化対策費補助金を交付している。その交付額は、図表0-3のとおり、46都道府県及び1,727市区町村の計1,773地方公共団体に対する計233億4588万余円となっている。その内訳は、都道府県に

対する交付額が67億8538万余円（29.0%）、市区町村に対する交付額が165億6050万円（70.9%）となっている。

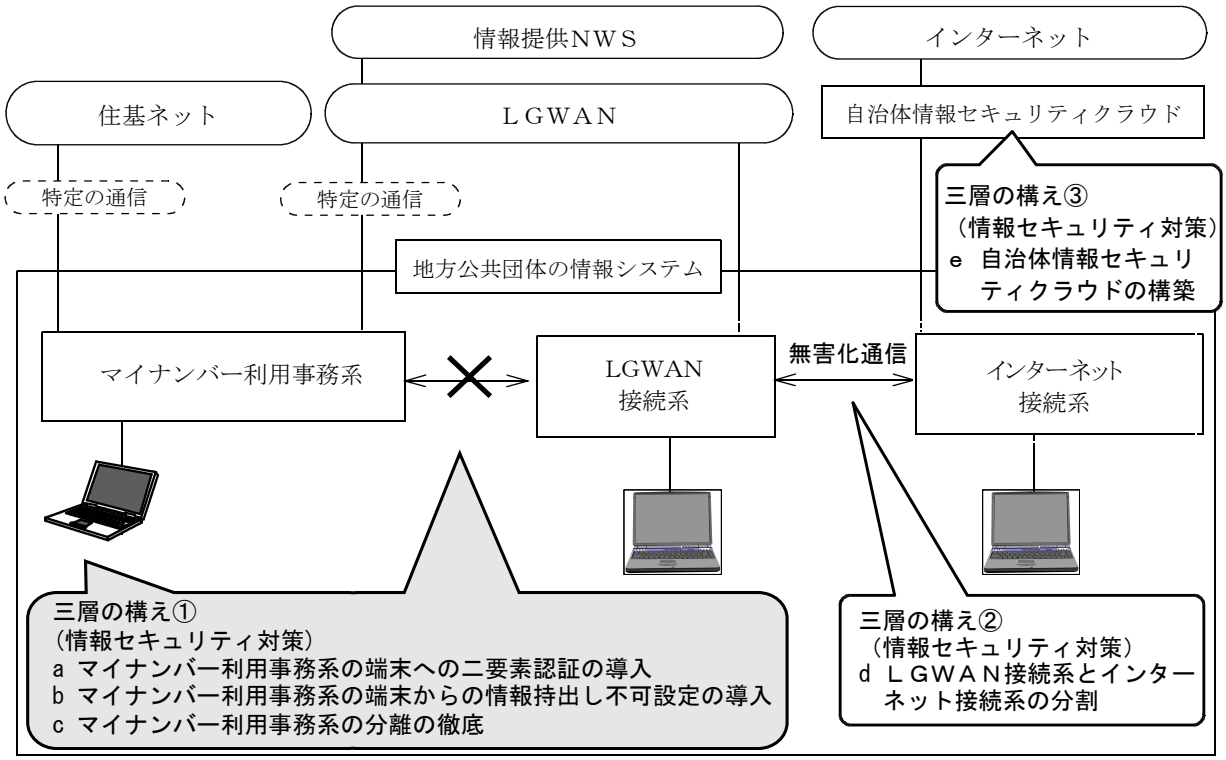
図表0-3　強化対策費補助金の交付実績額等

区分	地方公共団体数	交付対象地方公共団体数	交付実績額（千円）			交付実績額の合計に占める割合（%）
			平成27年度	28年度	計	
都道府県	47	46	－	6,785,389	6,785,389	29.0
市区町村	1,741	1,727	60,901	16,499,599	16,560,500	70.9
合計	1,788	1,773	60,901	23,284,988	23,345,889	100.0

強化対策費補助金の交付要綱等によれば、強化対策費補助金は、地方公共団体の情報セキュリティ対策の強化を図ることを目的として、「自治体情報システム強じん性向上モデル」の構築（以下「強じん性向上事業」という。）及び「自治体情報セキュリティクラウド」の構築（以下「セキュリティクラウド事業」という。）に要する経費を補助の対象としている。そして、原則として、自治体情報セキュリティクラウドは都道府県が市区町村におけるインシデントの初動対応を支援するためのツールであることから、都道府県に対してはセキュリティクラウド事業に要する経費を補助の対象としている。また、市区町村はマイナンバーの管理等を行うシステムである既存住基を保有していることから、市区町村に対しては強じん性向上事業に要する経費を補助対象としている。一方、都道府県がセキュリティクラウド事業の実施後に行う自庁の強じん性向上事業に要する経費を、また、市区町村が強じん性向上事業の実施後に行うセキュリティクラウド事業に要する経費を、それぞれ補助対象とすることを妨げないとされている。そして、人口規模等によって算定した補助基準額を上限とした額又は各地方公共団体からの申請額のうち補助対象経費として認められる額のいずれか低い額の2分の1について強化対策費補助金を交付することとされている。

三層の構え及び情報セキュリティ対策と強化対策費補助金との関係を示すと図表0-4及び図表0-5のとおりである。

図表0-4　三層の構え及び情報セキュリティ対策の概念図



図表0-5　三層の構え及び情報セキュリティ対策と強化対策費補助金との関係

三層の構え		情報セキュリティ対策		強化対策費補助金		「3 検査の状況」における記述箇所
				事業の名称	主な事業主体	
①	二要素認証及び情報持出し不可設定の導入	a	マイナンバー利用事務系の端末への二要素認証の導入	強じん性向上事業	市区町村	(2)ア
		b	マイナンバー利用事務系の端末からの情報持出し不可設定の導入			
		c	マイナンバー利用事務系の分離の徹底			(2)イ
②	LGWAN接続系とインターネット接続系の分割	d	LGWAN接続系とインターネット接続系の分割			
③	自治体情報セキュリティクラウドの構築	e	自治体情報セキュリティクラウドの構築	セキュリティクラウド事業	都道府県	(2)ウ

それぞれの事業及び経費の内容は次のとおりとなっている。

(ｱ) 強じん性向上事業

強じん性向上事業は、マイナンバー利用事務系の端末への二要素認証等の導入、ＬＧＷＡＮ環境とインターネット環境等の分割等により、地方公共団体の庁内の

ネットワークの強じん性の向上を図る事業である。

強じん性向上事業の対象となる経費は、二要素認証等に必要なサーバや認証装置等の購入経費や端末設定に要する経費等となっている。

総務省は、強化対策費補助金の実施要領及び「地方公共団体情報セキュリティ強化対策費補助金執行Ｑ＆Ａ」（以下「補助金Ｑ＆Ａ」という。）において、強じん性向上事業については、マイナンバー利用事務系の他の領域からの分離を徹底した上で、①マイナンバー利用事務系の端末への二要素認証の導入、②マイナンバー利用事務系の端末からの情報持出し不可設定及び③ＬＧＷＡＮ接続系とインターネット接続系の分割の情報セキュリティ対策を必須要件としており、これらの項目を実施せずに行った情報セキュリティ対策に要した経費は強化対策費補助金の交付対象とはならない（ただし、上記の項目を既に実施している場合や他の事業により実施予定の場合は交付対象となる）としている。

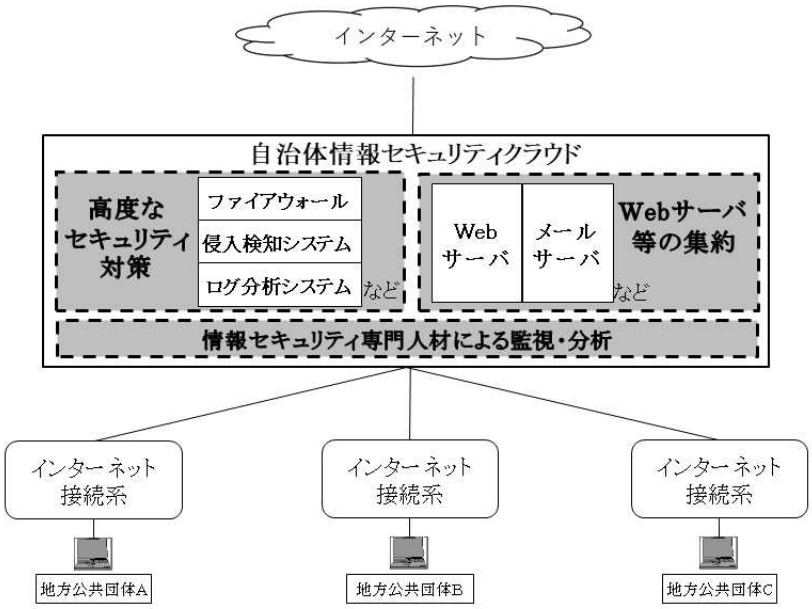
(ｲ) セキュリティクラウド事業

セキュリティクラウド事業は、都道府県と市区町村が協力してインターネット接続系において高度な情報セキュリティ対策を講ずるために、インターネット接続口を集約した上で、自治体情報セキュリティクラウド（図表0-6参照）を構築し、高度なセキュリティ対策を講ずる事業である。

強化対策費補助金の実施要領によれば、セキュリティクラウド事業においては、各市区町村が個別に設置しているＷｅｂサーバ等を都道府県が構築する自治体情報セキュリティクラウドに集約し、監視を始め高度なセキュリティ対策を実施するとされている。

セキュリティクラウド事業の対象となる経費は、都道府県にＷｅｂサーバ等を集約するための機器やファイアウォール等のセキュリティ対策ツールの購入経費やそれらの構築等に要する経費となっている。

図表0-6　自治体情報セキュリティクラウドの概念図



オ　セキュリティポリシーガイドラインの改定

総務省は、検討チームの報告及び30年7月に改定された「政府機関等の情報セキュリティ対策のための統一基準群」の内容等を踏まえて、同年9月にセキュリティポリシーガイドラインを改定している。この改定により、自治体情報セキュリティ対策の抜本的強化に当たり、マイナンバー利用事務系、ＬＧＷＡＮ接続系及びインターネット接続系において、情報システム全体の強じん性の向上（以下「強じん化」という。）のための措置を講ずることについて、その方法等が具体的に記載された。

カ　総務省による支援ＰＦの構築等

総務省は、8月報告を受けて、地方公共団体における情報セキュリティ対策向上に寄与することを目的として自治体情報セキュリティ支援プラットフォーム（以下「支援ＰＦ」という。）を事業費3780万円で構築等し、27年9月から運用を開始している。

支援ＰＦは、ネットワークシステム上で地方公共団体の担当者が情報セキュリティの専門家から助言を受けたり、他の地方公共団体との事例の共有を行ったりすることができるものである。また、地方公共団体からの要望により、地方公共団体の担当者が質問を投稿して他の地方公共団体に回答を依頼することができる掲示板機能等を事業費972万円で追加整備し（上記の構築等を合わせた事業費計4752万円）、28年3月から運用している。

2　検査の観点、着眼点、対象及び方法

(1) 検査の観点及び着眼点

前記のとおり、総務省は、年金情報流出事案等を踏まえて、各地方公共団体に対し、27年12月に情報セキュリティ対策として三層の構えを講ずるよう要請するとともに、平成27年度補正予算において強化対策費補助金を交付している。そして、地方公共団体は、上記の要請を受けて、情報セキュリティ対策の強化等を行い、27年度以降順次、その運用を開始している。

強化対策費補助金は、強じん性向上事業及びセキュリティクラウド事業におけるハードウェア及びソフトウェアの購入等を補助の対象としており、これらは、情報セキュリティ対策のうち、物理的セキュリティ及び技術的セキュリティを向上させるものである。一方、情報セキュリティは、ハードウェア及びソフトウェアの整備だけではなく、それらの運用や人的セキュリティに係る対策等を講ずることも必要である。総務省においても、年金情報流出事案等を踏まえて、地方公共団体に8月通知を発出して、組織体制の再検討、職員の訓練等の徹底等について助言等を行っている。そして、これらの体制整備等が適切に行われることにより、強化対策費補助金の交付の目的である情報セキュリティ対策の強化が実現することとなる。また、マイナンバー法におけるマイナンバー利用事務が28年1月から行われ、全国の地方公共団体等の情報システムの情報連携が29年11月から行われているが、マイナンバー制度の情報連携の効果がもたらされるためには、地方公共団体の情報セキュリティ対策が着実に実施される必要がある。

そこで、会計検査院は、強化対策費補助金等による情報連携開始前後の地方公共団体の情報セキュリティ対策の強化の状況について、合規性、経済性、効率性、有効性等の観点から、次の点に着眼して検査した。

ア　強化対策費補助金の交付状況はどのようになっているか。

イ　二要素認証等の導入、ＬＧＷＡＮ接続系とインターネット接続系との分割及び自治体情報セキュリティクラウドの構築といった強化対策費補助金等による地方公共団体の情報セキュリティ対策の強化は、補助金の交付目的に照らして適切に実施されているか、また、補助金の交付目的を実現し、効果を持続させるための体制等は整備されているか。

ウ　総務省は、強化対策費補助金で強化された情報セキュリティ対策の実効性を確保

するためどのような支援を行っているか、支援ＰＦは有効に機能しているか。

(2) 検査の対象及び方法

検査に当たっては、27、28両年度に強化対策費補助金が交付された46都道府県及び1,727市区町村の計1,773地方公共団体のうち18都道府県及び管内223市区町村の計241地方公共団体に交付された強化対策費補助金計61億3920万余円、並びに支援ＰＦの構築等に係る支払額4752万円を対象として、総務省及び241地方公共団体において、情報セキュリティ対策の実施状況について、関係資料を確認するなどして会計実地検査を行うとともに、241地方公共団体から調書を徴するなどして調査分析を行った。

3　検査の状況

(1) 強化対策費補助金の交付状況

1(2)エのとおり、強化対策費補助金の補助の対象は、強じん性向上事業及びセキュリティクラウド事業に要する経費となっている。しかし、両事業をいずれも実施した場合に、事業ごとの契約金額や強化対策費補助金の交付額を実績報告書において明らかにすることとなっていなかった。そこで、調書を徴するなどして、都道府県及び市区町村における両事業の交付状況を確認したところ、次のようになっていた。

ア　都道府県への強化対策費補助金の交付状況

1(2)エのとおり、強化対策費補助金の交付要綱によれば、強化対策費補助金は、原則として、都道府県に対してはセキュリティクラウド事業に要する経費を補助の対象としているが、セキュリティクラウド事業の実施後に行う自庁の強じん性向上事業等に要する経費を補助対象とすることを妨げないとされている。

そこで、18都道府県に対して交付された強化対策費補助金計27億2938万余円を補助対象事業別にみると、図表1-1のとおり、18都道府県の全てがセキュリティクラウド事業を実施して計22億5145万余円（交付実績額の合計に占める割合82.4%）の交付を受けていた。また、このうち10都道府県は強じん性向上事業も補助対象事業として実施して計4億7793万余円（同17.5%）の交付を受けていた。

図表1-1　18都道府県への強化対策費補助金の交付実績額等の状況

事業名	都道府県数	交付実績額（千円）			交付実績額の合計に占める割合（%）
		平成27年度	28年度	計	
強じん性向上事業	10	－	477,935	477,935	17.5
セキュリティクラウド事業	18	－	2,251,451	2,251,451	82.4
合計	18	－	2,729,387	2,729,387	100.0

(注) 強じん性向上事業とセキュリティクラウド事業の両方を実施した都道府県があるため、両事業の都道府県数を合計しても合計欄と一致しない。

イ　市区町村への強化対策費補助金の交付状況

223市区町村に対して交付された強化対策費補助金計34億0981万余円を補助対象事業別にみると、図表1-2のとおり、223市区町村の全てが強じん性向上事業を実施して計33億8299万余円（交付実績額の合計に占める割合99.2%。事業別に分離できない交付実績額計1638万余円を除く。）の交付を受けていた。また、このうち27市区町村はセキュリティクラウド事業も補助対象事業として実施して計1043万余円（同0.3%。事業別に分離できない交付実績額計1638万余円を除く。）の交付を受けていた。

図表1-2　223市区町村への強化対策費補助金の交付実績額等の状況

事業名	市区町村数	交付実績額（千円）			交付実績額の合計に占める割合（%）
		平成27年度	28年度	計	
強じん性向上事業	223	21,100	3,361,896	3,382,996	99.2
セキュリティクラウド事業	27	－	10,435	10,435	0.3
事業別に分離できないもの 注(1)	12	－	16,382	16,382	0.4
合計　注(2)	223	21,100	3,388,714	3,409,814	100.0

注(1) 強じん性向上事業及びセキュリティクラウド事業の両方を実施した市区町村のうち、交付実績額を事業別に分離できない市区町村に係る分である。また、市区町村数は、強じん性向上事業及びセキュリティクラウド事業の各欄にもそれぞれ計上している。

注(2) 強じん性向上事業とセキュリティクラウド事業の両方を実施した市区町村があるため、市区町村数を合計しても合計欄と一致しない。

(2) 三層の構えによる情報セキュリティ対策の強化の実施状況等

（注17）
会計実地検査時点における強化対策費補助金等による地方公共団体の情報セキュリティ対策の強化の実施状況を、三層の構えの対策ごとに着目するなどしてみると、次のとおりとなっていた。

（注17）　会計実地検査時点　　検査の対象とした18都道府県及び223市区町村の241地方公共団体に対する会計実地検査は、平成29年10月から30年3月までの間に実施している。

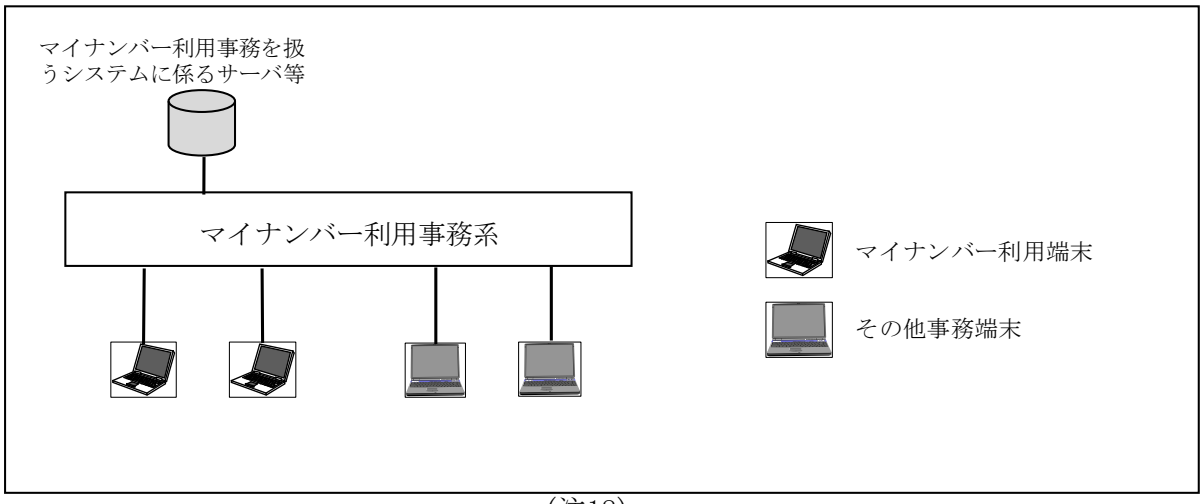
ア　マイナンバー利用事務系の端末等の二要素認証等の実施状況等

(ｱ) マイナンバー利用事務系における端末等の配置状況

1(2)ウのとおり、11月報告において、マイナンバー利用事務系（既存住基、税、社会保障等）においては、原則として、他の領域との通信ができないように分離を徹底した上で、端末への二要素認証等の導入等を図ることにより、住民情報の流出を徹底して防ぐこととされている。そして、強化対策費補助金の実施要領等によれば、マイナンバー利用事務系とは、マイナンバー利用事務、住民基本台帳と密接に関わる戸籍事務等に供する情報システム及びデータであり、既存住基、税、社会保障、戸籍事務等の従来は主に基幹系システムとして整理されてきたインターネットに接続する必要がない情報資産であるとされている。

そこで、検査の対象とした241地方公共団体における情報システムのネットワーク構成をみると、ＬＧＷＡＮ接続系やインターネット接続系の各領域と通信ができないように分離されたマイナンバー利用事務系の領域の中には、既存住基、税、社会保障、戸籍事務等のマイナンバー利用事務等を行っている情報システムがあることなどから、図表2-1のとおり、地方公共団体によってマイナンバー利用事務で使用する端末とそれ以外の事務で使用する端末が配置されるなどしていた（以下、マイナンバー利用事務系の領域に配置された端末のうちマイナンバー利用事務で使用する端末を「マイナンバー利用端末」、それ以外の事務で使用する端末を「その他事務端末」という。）。

図表2-1　マイナンバー利用事務系の端末に係る概念図



（注18）

また、これらとは別に、仮想化技術を用いて、マイナンバー利用事務系の領域にマイナンバー利用事務系のシステムに係るサーバとは異なるデータを処理するサーバを新たに設けるなどして、新たに設けるなどしたサーバとマイナンバー利用事務系以外の領域に配置した端末との間で通信経路の限定等を行った上で領域間の通信を行うことにより、マイナンバー利用事務に係るデータを表示したり、変更したりすることができるようにしている地方公共団体も見受けられた（以下、マイナンバー利用事務系以外の領域に置かれたこのような端末を「マイナンバー仮想利用端末」という。）。

（注18）　仮想化技術　　ソフトウェア技術等の活用によりコンピュータやハードディスク等を実際の物理的構成によらずに柔軟に分割したり、統合したりする技術。１台のものを複数台であるかのように利用することなどができる。

18都道府県及び223市区町村の計241地方公共団体のマイナンバー利用事務系の端末及びマイナンバー仮想利用端末の配置状況をみると、図表2-2のとおり、マイナンバー利用事務系の端末のみを配置しているのは、16都道府県及び198市区町村の計214地方公共団体、マイナンバー仮想利用端末のみを配置しているのは、1都道府県及び4市区町村の計5地方公共団体、マイナンバー利用事務系の端末とマイナンバー仮想利用端末を併用しているのは、1都道府県及び21市区町村の計22地方公共団体となっていた。

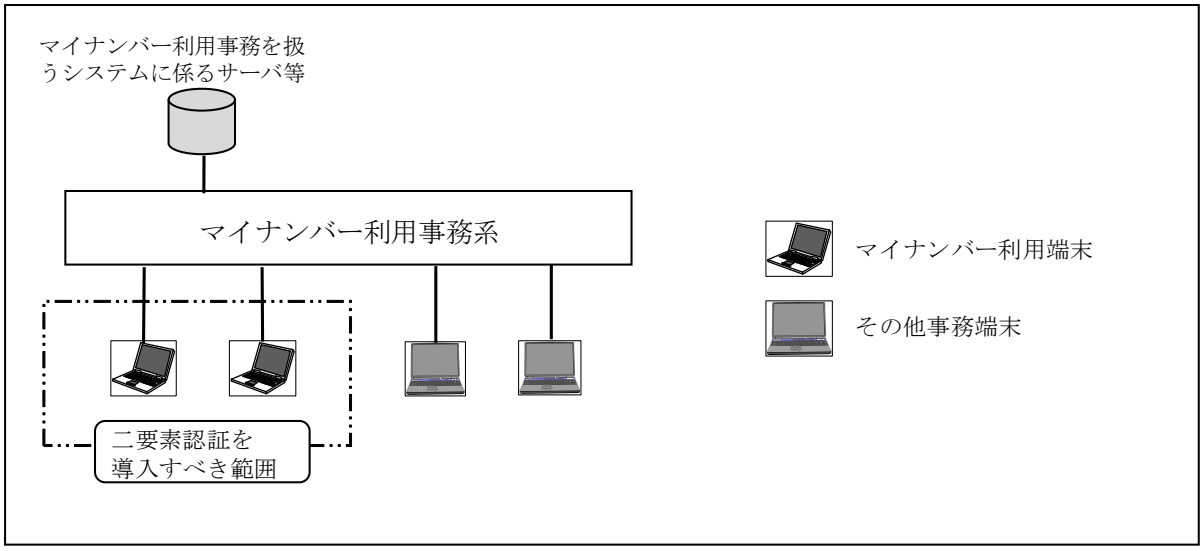
図表2-2　マイナンバー利用事務系の端末及びマイナンバー仮想利用端末の配置状況

区分	都道府県数	市区町村数	計
マイナンバー利用事務系の端末のみ	16　(88.8%)	198　(88.7%)	214　(88.7%)
マイナンバー利用事務系の端末とマイナンバー仮想利用端末を併用	1　(5.5%)	21　(9.4%)	22　(9.1%)
マイナンバー仮想利用端末のみ	1　(5.5%)	4　(1.7%)	5　(2.0%)
計	18 (100.0%)	223 (100.0%)	241 (100.0%)

(ｲ) マイナンバー利用事務系の端末への二要素認証の導入等の状況

1(2)ウのとおり、11月報告では、マイナンバー利用事務系においては、住民情報の流出を徹底して防ぐために、端末への二要素認証等の導入等を図ることとされている。そして、1(2)エ(ｱ)のとおり、総務省は、11月報告を踏まえて、強化対策費補助金の実施要領及び補助金Ｑ＆Ａにおいて、マイナンバー利用事務系の端末への二要素認証の導入を強じん性向上事業の必須要件としている。一方、マイナンバー利用事務系にはその他事務端末が配置されている場合もあることから、総務省に、その他事務端末への導入も必須となるのか確認したところ、同省は、強じん性向上事業として導入が必須となるのはマイナンバー利用端末であるとしていた（図表2-3参照）。

図表2-3　二要素認証を導入すべき範囲の概念図



また、総務省は、二要素認証の導入を必須要件とするのは市区町村が実施する強じん性向上事業のみであり、都道府県が実施する場合には適用しないとしている。18都道府県のうちマイナンバー利用事務系の端末を配置している17都道府県の二要素認証については、強じん性向上事業で実施した7都道府県を含む全ての都

道府県が、マイナンバー利用端末に導入していた。

一方、総務省では、二要素認証の導入は市区町村が実施する強じん性向上事業の必須要件としているが、既に実施している場合や他の事業により実施する予定の場合には、適用しないとしている。また、(1)のとおり、他の事業により実施する場合の実施の時期については、事業計画書や実績報告書において必ずしも明らかにすることとなっていない。

そこで、223市区町村のうちマイナンバー利用事務系の端末を配置している219市区町村における二要素認証の導入状況をみたところ、会計実地検査時点において、全部又は一部の端末に二要素認証を導入していたのは217市区町村となっていた。なお、残りの2市区町村は、令和元年5月末現在において、他の事業により導入済みとなっている。

そして、上記の217市区町村について、会計実地検査時点における二要素認証を導入した端末の範囲や二要素認証の運用等の状況をみたところ、次のとおりとなっていた。

a　二要素認証を導入した端末の範囲

217市区町村におけるマイナンバー利用端末への二要素認証の導入の状況をみたところ、図表2-4のとおり、マイナンバー利用端末の全てに導入しているのが205市区町村、一部の端末に導入していないのが12市区町村となっていた。そして、これらの12市区町村のうち、2市区町村はマイナンバー利用端末の全てに導入する予定があるとしていたが、残りの10市区町村は導入する予定があるとしていなかった。なお、平成31年3月末現在において、上記の10市区町村のうち2市区町村は、マイナンバー利用端末の全てに二要素認証を導入しており、3市区町村は令和元年度内に、3市区町村は2年度内に導入する予定であるとしていた。残りの2市区町村は、入退室管理がされた、正規の権限を持った者のみが立ち入ることのできるセキュリティを確保したサーバ室等で使用される限られた端末についてのみ一要素で認証できるようにしていた。

図表2-4　マイナンバー利用端末への二要素認証の導入の状況

導入状況	市区町村数	
全ての端末に導入している市区町村	205	
一部の端末に導入していない市区町村	12	
	マイナンバー利用端末の全てに導入する予定があるとしているもの	2
	マイナンバー利用端末の全てに導入する予定があるとしていないもの	10
計	217	

二要素認証をマイナンバー利用端末の一部に導入しておらず、マイナンバー利用端末の全てに導入する予定があるとしていない市区町村においては、マイナンバー利用端末に一要素による認証でログインでき、正規の権限を持たない職員等が、正規の権限を持つ職員になりすましてログインして、特定個人情報に不正にアクセスすることが、二要素認証を導入した端末に比べて容易な状況となっていた。

しかし、総務省は、二要素認証をマイナンバー利用端末の一部に導入しておらず、マイナンバー利用端末の全てに導入する予定があるとしていない市区町村があることを十分に把握していなかった。

したがって、マイナンバー利用端末の一部に二要素認証を導入していない場合は、特定個人情報に不正にアクセスすることが二要素認証を導入した端末に比べて容易であることから、総務省は、マイナンバー利用端末への二要素認証の導入状況を十分に把握するとともに、対策が十分でない地方公共団体に対して助言を行う必要がある。

b　導入した二要素認証の種類及び手段の組合せ

総務省は、地方公共団体の情報セキュリティ対策の参考資料として、同省が平成28年1月に11月報告を踏まえて作成し、地方公共団体に配布した「「新たな自治体情報セキュリティ対策の抜本的強化に向けて」における主な論点」（以下「論点集」という。）の中で、二要素認証とは、図表2-5に示した認証の手段のうち二種類を併用するものであるとしている。

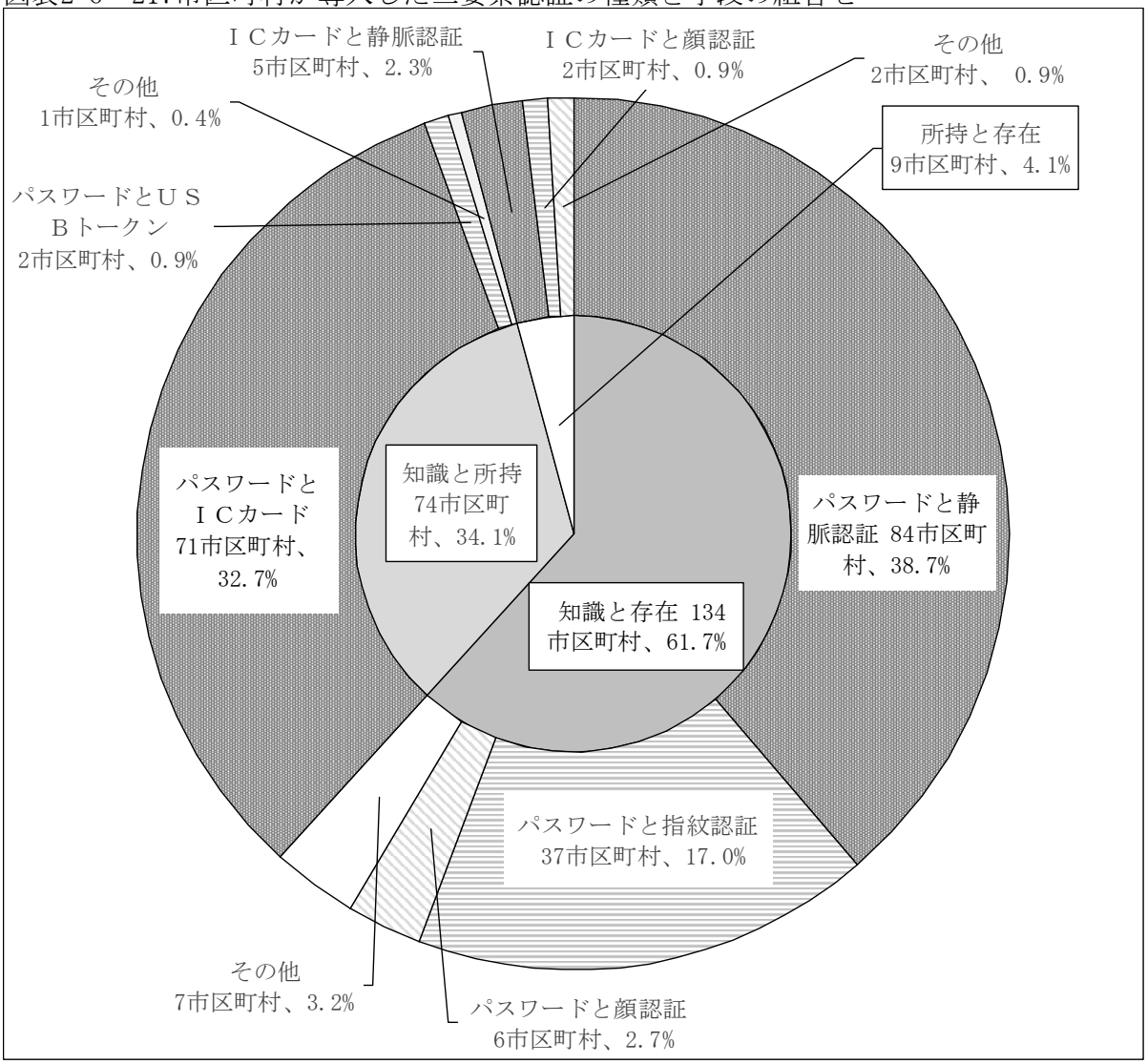
図表2-5　二要素認証の種類、手段及び具体例

種類	認証の手段	具体例
知識	正規の利用者“だけが知っている情報（知識）”をその人が知っているか否かで判断	パスワード、暗証番号
所持	正規の利用者“だけが持っているモノ（所持品）”をその人が持っているか否かで判断	ＩＣカード、ＵＳＢトークン
存在	正規の利用者の“身に備わっている特徴（利用者自身の存在）”でその人か否かを判断	指紋、静脈

前記の217市区町村について、導入した二要素認証の要素の種類の組合せをみると、図表2-6のとおり、「知識」と「存在」を採用していたものが134市区町村（217市区町村に占める割合61.7%）、「知識」と「所持」を採用していたものが74市区町村（同34.1%）、「所持」と「存在」を採用していたものが9市区町村（同4.1%）となっていた。

また、認証の手段の組合せをみると、「知識」と「存在」の組合せの内訳は、パスワードと静脈認証が84市区町村（同38.7%）、パスワードと指紋認証が37市区町村（同17.0%）、「知識」と「所持」の組合せの内訳は、パスワードとＩＣカードが71市区町村（同32.7%）、パスワードとＵＳＢトークンが2市区町村（同0.9%）、「所持」と「存在」の組合せの内訳は、ＩＣカードと静脈認証が5市区町村（同2.3%）、ＩＣカードと顔認証が2市区町村（同0.9%）等となっていた。

図表2-6　217市区町村が導入した二要素認証の種類と手段の組合せ



（注）システムによって異なった組合せを採用している市区町村については、当該市区町村の端末の中で最も多い組合せにより集計している。

c　導入した二要素認証の運用等の状況

(a) 認証エラーとなった際等の代替手段

二要素認証の種類のうち、ＩＣカード等の「所持」や指紋等の「存在」が認証エラーとなった際等の代替手段となるパスワードがあらかじめ設定され、かつ、通常の操作のみで当該パスワード入力画面に遷移することができる場合、当該パスワードを不正に取得すれば、正規の権限を持たない職員等でも正規の権限を持つ職員になりすまして、二要素認証を回避して「知識」の一要素のみによる認証でログインし、特定個人情報に不正にアクセスすることが、二要素認証でログインする場合に比べて容易となる。

そこで、「所持」又は「存在」による認証がエラーとなった際等の代替手段の状況をみたところ、217市区町村のうち27市区町村は、認証の代替手段となるパスワードをあらかじめ設定する運用を行っており、かつ、職員がシステムを管理する職員に別途依頼するなどの特別な手続を必要とすることなく、通常の操作のみで当該パスワード入力画面に遷移することができる状況となっていた。

(b) 端末及び業務システムの認証の手段の共有

端末及び業務システムにログインするために必要となる認証の手段を職員の間で共有していて、共有している認証の手段のみで端末及び業務システムにログインが可能な場合には、業務システムを通じて特定個人情報にアクセスした実際の利用者を識別できないため、不正アクセスや情報漏えいが発生した場合に不正アクセスを行った者等の特定が困難になるおそれがある。

そこで、端末及び業務システムにログインするために必要となる認証の手段を職員の間で共有しているかをみたところ、217市区町村のうち7市区町村は、一部のアカウントについて、「知識」及び「所持」の認証の手段を職員の間で両方とも共有していて、共有している認証の手段のみで端末及び業務システムにログインが可能な状況となっていた。

(c) 端末のローカルドライブ等に特定個人情報を保存している場合のリスク

特定個人情報を端末のローカルドライブ及び複数の端末からアクセスできるファイルサーバ等の共有フォルダ（以下、これらを合わせて「端末のローカルドライブ等」という。）に保存している場合で、①共有している認証の手段のみで端末にログインできたり、②端末に一要素による認証でログインし、その後、マイナンバー利用事務に係る業務システムにログインする際に別の一要素又は二要素で認証する方法（以下「段階的な認証方法」という。）を採用していたりする場合には、導入した二要素認証の効果が十分に発現しないおそれがある。また、同様に、③ファイルサーバ等へのアクセス制御の設定により、正規の権限を持たない職員でもファイルサーバ等の共有フォルダにアクセスできる場合にも、導入した二要素認証の効果が十分に発現しないおそれがある。

また、セキュリティポリシーガイドラインにおいても、各地方公共団体の

情報セキュリティポリシーを策定等する際の例として、住民情報や人事記録等の特定の職員等しか取り扱えないデータについては、同一課室等であっても、担当職員以外の職員等が閲覧及び使用できないようにしなければならないことなどとされている。

217市区町村について、特定個人情報を端末のローカルドライブ等に保存しているかをみたところ、図表2-7のとおり、59市区町村ではマイナンバー利用端末へログインすることによりアクセスできる当該端末のローカルドライブに、113市区町村ではログインした複数のマイナンバー利用端末からそれぞれアクセスできるファイルサーバ等の共有フォルダに、それぞれ特定個人情報を保存しており、これらの市区町村は純計で122市区町村となっていた。

そこで、上記の122市区町村について、端末のローカルドライブ等への特定個人情報の保存状況をみたところ、次のとおりとなっていた。

① 特定個人情報を保存していた端末のローカルドライブ等にアクセスできる端末に共有している認証の手段のみでログインできるかみたところ、15市区町村では、全部又は一部のアカウントについて共有している認証の手段のみで端末にログインできる状況となっていた（15市区町村には(b)の共有している認証の手段だけで端末及び業務システムにログインが可能な状況となっていた7市区町村のうち5市区町村を含む。）。

図表2-7 端末のローカルドライブ等への特定個人情報の保存状況等

特定個人情報を端末のローカルドライブ等に保存している市区町村数		端末のローカルドライブ	ファイルサーバ等の共有フォルダ	計
		59	113	122
①全部又は一部のアカウントについて共有している認証の手段のみで端末にログインできる		9	14	15
②段階的な認証方法を採用している		7	16	16
③ファイルサーバ等へのアクセス制御の設定により、正規の権限を持たない職員でもファイルサーバ等の共有フォルダにアクセスできる		－	7	7
①から③までの純計		14	28	29
	保存期間が1年以上	9	19	19
	保存期間が不明	2	8	8

（注）端末のローカルドライブとファイルサーバ等の共有フォルダの両方に保存している市区町村があるため、各欄を合計しても計と一致しないものがある。

上記の共有している認証の手段のみで端末にログインできる15市区町村に認証の手段を共有している理由を確認したところ、「窓口対応業務で職員が交代した際の端末へのログインをスムーズに行えるようにするため」等としていた。しかし、これらの15市区町村では、不正アクセスや情報漏えいが発生した場合に不正アクセスを行った者等の特定が困難になるおそれがある。

② 段階的な認証方法を採用しているかみたところ、図表2-7のとおり、16市区町村が採用していた。このため、これらの16市区町村では、特定個人情報が保存された端末のローカルドライブ等にアクセスできる端末にログインする正規の権限を持つ職員に課されているログインするための一要素を不正に取得するなどすれば、正規の権限を持たない職員等でも、この職員になりすまして、一要素による認証で端末にログインし、端末のローカルドライブ等に保存された特定個人情報に不正にアクセスできる状況となっていた。

上記の事態について、事例を示すと次のとおりである。

＜事例1＞ 一要素による認証で端末にログインした職員等が、マイナンバー利用事務系の端末のローカルドライブ等に保存された特定個人情報のデータにアクセスできる状況となっていたもの

市区町村Ａは、平成28年度に、強化対策費補助金の交付を受けて、強じん性向上事業を実施している。
市区町村Ａは、導入した二要素認証について、会計実地検査時点において、マイナンバー利用端末に一要素（ＩＣカード）による認証でログインし、その後、マイナンバー利用事務に係る業務システムにＩＣカードとパスワードによる二要素でログインする段階的な認証方法を採用していた。そして、市区町村Ａは、業務システムに認証する際に二要素とすることで、安全性が確保されているとしていた。
しかし、市区町村Ａでは、業務システムの特定個人情報をマイナンバー利用事務系の端末のローカルドライブ等に保存しており、当該端末のログインに必要なＩＣカードを不正に取得するなどすれば、正規の権限を持たない職員等でも、この職員になりすましてマイナンバー利用事務系の端末にログインし、端末のローカルドライブ等に保存された特定個人情報のデータにアクセスできる状況となっていた。
なお、市区町村Ａは、会計実地検査の結果を踏まえて、30年11月に、マイナンバー利用端末への認証方法をＩＣカードとパスワードによる方法に変更する対策を講じている。

③ ファイルサーバ等へのアクセス制御の設定により、正規の権限を持たない職員でもファイルサーバ等の共有フォルダにアクセスできるか、特定個人情報を共有フォルダに保存している113市区町村についてみたところ、図表2-7のとおり、7市区町村は課室単位でアクセス制御しているが、特定個人情報を含むデータにパスワードを設定するなどはしておらず、同じ課室内に所属する正規の権限を持たない職員でも共有フォルダに保存されてい

る特定個人情報にアクセスできる状況となっていた。そして、7市区町村において、そのような取扱いとしている理由としては、「正規の権限がなくても、同じ課室等に所属する職員であれば問題ないと認識しているため」とするものが3市区町村、「個人単位での権限設定の作業が煩雑であるため」とするものが3市区町村、「原則正規の権限を持たない職員は閲覧又は使用を不可としているが、定期監査等が徹底していないことなどにより例外がある状況となっているため」とするものが1市区町村となっていた。

そして、上記の①の15市区町村、②の16市区町村、③の7市区町村の純計である29市区町村のうち19市区町村では、図表2-7のとおり、端末のローカルドライブ等への特定個人情報の保存期間が1年以上の長期にわたっていたり、8市区町村では、保存期間が不明であるとしたりしていて、特定個人情報への不正なアクセスにつながる可能性がより高まる運用が行われている状況となっていた。

以上のように、二要素認証の運用等の状況によっては、その効果が十分に発現しないおそれがある状況が見受けられた。

しかし、総務省は、このような状況について十分に把握していなかった。

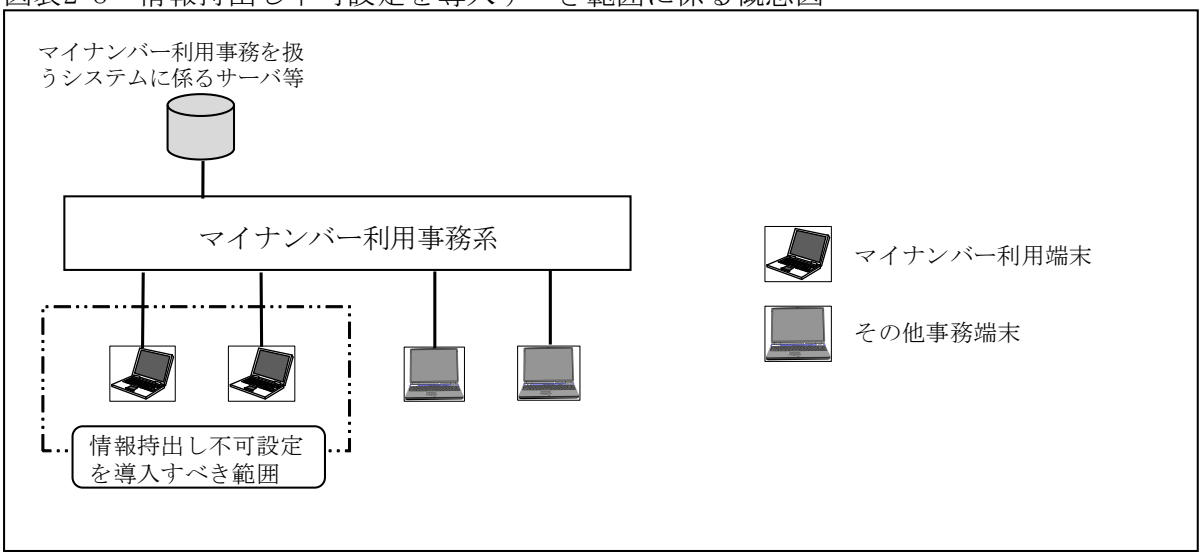
したがって、総務省は、補助事業実施後の状況を十分に把握した上で、共有している認証の手段だけで端末のローカルドライブ等に保存された特定個人情報にアクセスできるなどの望ましくない運用方法を具体的に示すなどして、特定個人情報の情報漏えいなどのリスクが低減されるよう、地方公共団体に対して助言を行う必要がある。

(ｳ) マイナンバー利用事務系の端末からの情報持出し不可設定の導入等の状況

1(2)エ(ｱ)のとおり、総務省は、11月報告を踏まえて、強化対策費補助金の実施要領及び補助金Ｑ＆Ａにおいて、マイナンバー利用事務系の端末からの情報持出し不可設定の導入を強じん性向上事業の必須要件としている。一方、マイナンバー利用事務系にはその他事務端末が配置されている場合もあることから、総務省に、その他事務端末への導入も必須となるのか確認したところ、同省は、強じん性向上事業として導入が必須となるのはマイナンバー利用端末であるとしていた

（図表2-8参照）。

図表2-8　情報持出し不可設定を導入すべき範囲に係る概念図



また、総務省は、情報持出し不可設定の導入を必須要件とするのは市区町村が実施する強じん性向上事業のみであり、都道府県が実施する場合には適用しないとしている。

18都道府県のうちマイナンバー利用事務系の端末を配置している17都道府県の情報持出し不可設定については、強じん性向上事業で実施した5都道府県を含む全ての都道府県が、マイナンバー利用端末に導入していた。

一方、総務省では、情報持出し不可設定の導入は市区町村が実施する強じん性向上事業の必須要件としているが、既に実施している場合や他の事業により実施する予定の場合には、適用しないとしている。また、(1)のとおり、他の事業により実施する場合の実施の時期については、事業計画書や実績報告書において必ずしも明らかにすることとなっていない。

そこで、223市区町村のうちマイナンバー利用事務系の端末を配置している219市区町村における情報持出し不可設定の導入状況をみたところ、会計実地検査時点において、全部又は一部の端末に情報持出し不可設定を導入していたのは218市区町村となっていた。なお、残りの1市区町村は、31年3月末現在において、他の事業により導入済みとなっている。

そして、上記の218市区町村について、会計実地検査時点における情報持出し不可設定を導入した端末の範囲や情報持出し不可設定の運用等の状況をみたところ、次のとおりとなっていた。

a　情報持出し不可設定を導入した端末の範囲

218市区町村におけるマイナンバー利用端末への情報持出し不可設定の導入の状況をみたところ、図表2-9のとおり、マイナンバー利用端末の全てに導入しているのが205市区町村、一部に導入していないのが13市区町村となっていた。そして、これらの13市区町村のうち、1市区町村は、マイナンバー利用端末の全てに導入する予定があるとしていたが、残りの12市区町村は導入する予定があるとしていなかった。なお、31年3月末現在において、上記の12市区町村のうち3市区町村は、マイナンバー利用端末の全てに情報持出し不可設定を導入しており、2市区町村は令和元年度内に、1市区町村は元年度以降にマイナンバー利用端末の全てに情報持出し不可設定を導入する予定であるとしていた。残りの6市区町村は、入退室管理がされた、正規の権限を持った者のみが立ち入ることができるセキュリティを確保したサーバ室等で使用される限られた端末についてのみ情報を持ち出せるようにしていた。

図表2-9　マイナンバー利用端末への情報持出し不可設定の導入の状況

導入状況	市区町村数	
全ての端末に導入している市区町村	205	
一部の端末に導入していない市区町村	13	
	マイナンバー利用端末の全てに導入する予定があるとしているもの	1
	マイナンバー利用端末の全てに導入する予定があるとしていないもの	12
計	218	

情報持出し不可設定をマイナンバー利用端末の一部に導入しておらず、マイナンバー利用端末の全てに導入する予定があるとしていない市区町村においては、特定個人情報を持ち出す正当な理由のない職員が、情報持出し不可設定を導入していない端末から不正に特定個人情報を持ち出すことが、情報持出し不可設定を導入した端末に比べて容易な状況となっていた。

上記の事態について、事例を示すと次のとおりである。

＜事例2＞　マイナンバー利用端末の一部に情報持出し不可設定を導入しておらず、マイナンバー利用端末の全てに導入する予定があるとしていないもの

市区町村Ｂは、平成28年度に、強化対策費補助金の交付を受けて、強じん性向上事業を実施している。
しかし、市区町村Ｂは、会計実地検査時点においてマイナンバー利用端末63台に情報持出し

不可設定を導入しておらず、職員等が不正に特定個人情報を持ち出すことが、情報持出し不可設定を導入した端末に比べて容易な状況となっていた。そして、これらの端末に情報持出し不可設定を導入する予定があるとしていなかった。
　そして、市区町村Ｂによれば、情報持出し不可設定を導入していなかったのは、外部の機関とのデータのやり取りを行う業務が月に数回定期的にあり、業務上データの持出しが必要になるためであるとしている。
　なお、市区町村Ｂは、会計実地検査の結果を踏まえて、31年3月に、マイナンバー利用端末の全てについて、情報持出し不可設定を導入し、やむを得ない場合のみ情報持出し不可設定を解除する運用にしている。

しかし、総務省は、情報持出し不可設定をマイナンバー利用端末の一部に導入しておらず、マイナンバー利用端末の全てに導入する予定があるとしていない市区町村があることについて十分に把握していなかった。

したがって、マイナンバー利用端末の一部に情報持出し不可設定を導入していない場合は、特定個人情報を不正に持ち出すことが情報持出し不可設定を導入した端末に比べて容易であることから、総務省は、マイナンバー利用端末への情報持出し不可設定の導入状況を十分に把握するとともに、対策が十分でない地方公共団体に対して助言を行う必要がある。

b　導入した情報持出し不可設定の運用等の状況

(a) 例外的な情報持出しの運用状況

総務省は、地方公共団体に配布した論点集の中で、情報持出し不可設定における例外的な取扱いとして、納付書等の大量帳票のアウトソーシングや指定金融機関に対する口座振替情報の提供等のやむを得ない場合においては、管理者権限を持つ職員によってその都度情報持出し不可設定を解除するか、又は管理者権限を持つ職員のみに持出しを許可する設定とすることとしている。しかし、長期間又は期間を設けることなく情報持出し不可設定を解除する運用を行い、かつ、情報を持ち出す際に情報セキュリティ管理者による許可がなくても情報を持ち出すシステム操作ができたり、情報セキュリティ管理者に許可を得る運用をしていなかったりする場合には、内部不正等による情報漏えいのリスクが高まり、情報持出し不可設定の効果が十分に発現しないおそれがある。

また、セキュリティポリシーガイドラインにおいても、職員等が情報資産を不正に利用したり、適正な取扱いを怠ったりした場合には、情報漏えいなどの被害が発生し得ることから、情報資産等を外部に持ち出す場合には、情

報セキュリティ管理者の許可を得なければならないとされている。

前記の218市区町村における例外的な情報持出しの運用状況をみたところ、図表2-10のとおり、203市区町村では端末からの例外的な情報持出しを認めており、このうち、40市区町村では管理者権限を持つ職員等のみに情報持出しを許可する運用を、3市区町村では情報システム担当部署内の端末等からのみ情報持出しを許可する運用を、160市区町村では管理者権限を持つ職員等が職員からの申請に基づいて情報持出し不可設定を解除する運用を行っていた。

しかし、管理者権限を持つ職員等が職員からの申請に基づいて情報持出し不可設定を解除する運用をしている160市区町村のうち、期限を設けることなく情報持出し不可設定を解除する運用をしているものが62市区町村において見受けられた。また、一度の申請で一定の期間を定めて情報持出し不可設定を解除する運用を行っているものが33市区町村あり、このうち解除期間を1か月以上としているものが27市区町村となっていた。

図表2-10　例外的な情報持出しの運用の状況

<table>
<tr><th colspan="4">例外的な情報持出しの内容</th><th>市区町村数</th></tr>
<tr><td colspan="4">例外的な情報持出しを全面的に禁止している市区町村</td><td>15</td></tr>
<tr><td rowspan="6">例外的な情報持出しを認めている市区町村</td><td colspan="3">管理者権限を持つ職員等のみに情報持出しを許可している市区町村</td><td>40</td></tr>
<tr><td colspan="3">情報システム担当部署内の端末等からのみ情報持出しを許可している市区町村</td><td>3</td></tr>
<tr><td rowspan="4">管理者権限を持つ職員等が職員からの申請に基づいて情報持出し不可設定を解除している市区町村</td><td colspan="2"></td><td>160</td></tr>
<tr><td colspan="2">一定の期間を定めて解除</td><td>33</td></tr>
<tr><td>1か月以上</td><td>27</td></tr>
<tr><td colspan="2">期限を設けることなく解除</td><td>62</td></tr>
<tr><td colspan="3">小計</td><td>203</td></tr>
<tr><td colspan="4">計</td><td>218</td></tr>
</table>

(注)「管理者権限を持つ職員等が職員からの申請に基づいて情報持出し不可設定を解除している市区町村」については、事務の内容に応じて情報持出し不可設定を解除する期間が異なる市区町村がある。また、情報持出し不可設定の解除には、端末からの情報の持出しを可能にするＵＳＢキーを貸与する場合を含めている。

そこで、期限を設けることなく解除する運用をしている62市区町村及び情報持出し不可設定の解除期間を1か月以上としている27市区町村の純計87市区町村について、情報を持ち出す場合の情報セキュリティ管理者の許可の実施状況をみたところ、全ての市区町村において情報セキュリティ管理者による

許可がなくても情報を持ち出すシステム操作ができるようになっており、このうち29市区町村では情報セキュリティ管理者に許可を得る運用もしていない状況となっていた。

上記の事態について、事例を示すと次のとおりである。

＜事例3＞　期限を設けることなく情報持出し不可設定を解除する運用を行っていたもの

市区町村Ｃは、平成28年度に、強化対策費補助金の交付を受けて、強じん性向上事業を実施している。
市区町村Ｃは、導入したマイナンバー利用端末14台に係る情報持出し不可設定について、情報持出しを制御するソフトウェアにより、原則として情報持出しができないように設定している。そして、例外的な情報持出しの運用として、原課の職員から情報持出しの申請があった場合は、管理者権限を持つ情報システム担当課の職員が情報持出し不可設定を解除し、原課の職員がＵＳＢメモリ等により情報の持出しを行っている。
しかし、市区町村Ｃは、会計実地検査時点において、日常的に情報の持出しが必要な業務があることを理由として、全ての情報持出しについて、申請があれば期限を設けることなく持出し不可設定を解除する運用を行っていた。また、情報を持ち出す際に情報セキュリティ管理者による許可がなくても持ち出すシステム操作ができるようになっていた。このため、一度申請するだけで、時間的な制約がなく情報持出しができることになり、全ての情報持出しについてその都度持出し不可設定を解除している場合等と比べると、内部不正等による特定個人情報の持出しのリスクが高い状況となっていると認められた。現に、市区町村Ｃでは、会計実地検査時点において、上記14台のうち11台について情報持出し不可設定を解除しており、解除期間が1年以上3年未満のものが7台、5年以上のものが4台となっていた。
なお、市区町村Ｃは、会計実地検査の結果を踏まえて、31年2月に、全ての情報持出しについて、その都度持出し不可設定を解除する運用に変更している。

(b) 例外的な情報持出しに係る記録等の状況

情報を持ち出す際に、情報持出しに係るログを保存したり、台帳等により記録したりするなどしていない場合には、外部記憶媒体による情報持出しによる情報漏えいや内部不正等のリスクが高まることとなる。

また、セキュリティポリシーガイドラインにおいても、職員等が情報資産を不正に利用したり、適正な取扱いを怠ったりした場合には、情報漏えいなどの被害が発生し得ることから、外部記憶媒体等の持出しについては、所属課室名、氏名、日時、持出物等の記録を作成して保管しなければならないとされている。そして、ネットワークや情報システム等の管理が不十分な場合には、情報漏えい、内部不正等の被害が生ずるおそれがあることから、各種ログ及び情報セキュリティの確保のために必要な記録を取得し、一定の期間保存しなければならないとされている。

そこで、前記の203市区町村について、情報持出しに係る記録等の実施状況をみたところ、情報持出しに係るログの保存については、図表2-11のとおり、159市区町村ではログを一定の期間保存しているとしていたが、44市区町村で

は全部又は一部の媒体についてログを保存していないとしていた。

また、情報を持ち出す際の氏名、日時、持出物等の台帳等への記録については、ログを保存している159市区町村のうち58市区町村、ログを保存していない44市区町村のうち19市区町村の計77市区町村が記録していないとしていた。

図表2-11　情報持出しに係るログの保存及び台帳等による記録の状況

実施内容	市区町村数	左のうち情報を持ち出す際に台帳等により記録していない市区町村数
情報持出しに係るログを保存している	159	58
全部又は一部の媒体について情報持出しに係るログを保存していない	44	19
計	203	77

(c) 例外的な情報持出しに係るデータの暗号化等の状況

情報を持ち出す際に、暗号化機能を備える外部記憶媒体を使用するなどしていない場合には、外部記憶媒体による情報持出しによる情報漏えいや内部不正等のリスクが高まることとなる。

また、セキュリティポリシーガイドラインにおいても、職員等が利用する外部記憶媒体等が適正に管理されていない場合には、不正利用、紛失、盗難、情報漏えいなどの被害を及ぼすおそれがあることから、これらの被害を防止するために、データ暗号化機能を備える外部記憶媒体を使用しなければならないなどとされている。

そこで、前記の203市区町村について、データ暗号化機能を備える外部記憶媒体の使用等の状況についてみたところ、図表2-12のとおり、147市区町村では暗号化機能を備える外部記憶媒体を使用するなどしており、このうち66市区町村は暗号化しなければ情報を持ち出せない仕組みにしていたが、81市区町村は暗号化の実施を職員が選択でき、任意で行っている状況となっていた。そして、56市区町村は、そもそも暗号化機能を備える外部記憶媒体を使用するなどしていなかった。

図表2-12　情報持出しに係るデータの暗号化の状況

実施内容		市区町村数
暗号化機能を備える外部記憶媒体を使用するなどしている		147
	暗号化しなければ情報を持ち出せない仕組みにしている	66
	暗号化の実施を職員が選択できる	81
暗号化機能を備える外部記憶媒体を使用するなどしていない		56
計		203

以上のように、情報持出し不可設定の運用等の状況によっては、その効果が十分に発現しないおそれがある状況が見受けられた。

しかし、総務省は、このような状況を十分に把握していなかった。

したがって、総務省は、補助事業実施後の状況を十分に把握した上で、長期間又は期間を設けることなく情報持出し不可設定を解除する運用を行い、かつ、情報セキュリティ管理者に許可を得る運用をしていないなどの望ましくない運用方法を具体的に示すなどして、特定個人情報の情報漏えいなどのリスクが低減されるよう、地方公共団体に対して助言を行う必要がある。

イ　マイナンバー利用事務系等の分離、分割等の実施状況等

1(2)ウのとおり、11月報告では、マイナンバー利用事務系においては、原則として、他の領域との通信ができないように分離するなどして住民情報の流出を徹底して防ぐこととなっている。また、マイナンバーによる情報連携に活用されるＬＧＷＡＮ環境のセキュリティの確保に資するために、ＬＧＷＡＮ接続系とインターネット接続系との通信経路を分割することとなっている。

(ｱ) マイナンバー利用事務系の他の領域からの分離及びＬＧＷＡＮ接続系とインターネット接続系との通信経路の分割の状況

総務省は、マイナンバー利用事務系等の分離、分割等を必須要件とするのは市区町村が実施する強じん性向上事業のみであり、都道府県が実施する場合には適用しないとしている。そして、18都道府県の領域間の分離及び分割の状況については、強じん性向上事業で実施した10都道府県を含む全ての都道府県がマイナンバー利用事務系と他の領域の分離を行っていたものの、ＬＧＷＡＮ接続系とインターネット接続系の分割については、強じん性向上事業を補助対象とした2都道府

県を含む計3都道府県が実施していなかった。なお、これらの3都道府県では、平成31年3月末現在において、これらの分割を既に実施し、又は実施する予定としている。

一方、総務省は、マイナンバー利用事務系等の分離及び分割は市区町村が実施する強じん性向上事業の必須要件としているが、既に実施している場合や他の事業により実施する予定の場合には、適用しないとしている。また、(1)のとおり、他の事業により実施する場合の実施の時期については、事業計画書や実績報告書において必ずしも明らかにすることとなっていない。

そこで、223市区町村における領域間の分離及び分割の状況をみたところ、マイナンバー利用事務系と他の領域の分離及びＬＧＷＡＮ接続系とインターネット接続系の分割については、31年3月末現在において全ての市区町村で分離及び分割を行っていた。

(ｲ) マイナンバー利用事務系等の分離及び分割後の領域間通信の状況

11月報告において、マイナンバー利用事務系と他の領域を分離した上で、マイナンバー利用事務系と他の領域との間で通信を行う場合には、住基ネット等の十分にセキュリティが確保された特定通信先と限定的に接続することとなっている。また、強化対策費補助金の実施要領において、ＬＧＷＡＮ接続系とインターネット接続系については、一旦通信環境を分離した上で、必要な通信だけを許可できるようにすることとなっている。

そして、総務省は実施要領において、強じん性向上事業を行う場合に参照すべき手法の例として、マイナンバー利用事務系、ＬＧＷＡＮ接続系及びインターネット接続系との間で通信を行う場合には、Ｌ３スイッチ(注19)等による通信経路の限定、ファイアウォール(注20)による通信プロトコルの限定等を行うことで、通信を制限することとしている。また、地方公共団体に配布した論点集において、マイナンバー利用事務系と他の領域との間で特定の通信に限定する際は、通信経路の限定に加えて、アプリケーションプロトコル(注21)のレベルでの限定も行うこととしている。

そこで、223市区町村において、領域間で行われている通信（以下「領域間通信」という。）について、通信内容の種類別及び領域別にみたところ、図表2-13のとおり、217市区町村において延べ1,672件の領域間通信が行われていた。そして、マイナンバー利用事務系と他の領域との間の領域間通信の通信制御の状況を

みたところ、図表2-13のとおりとなっており、59市区町村の延べ247件において、通信経路の限定又は通信プロトコルの限定のうち少なくともいずれか一つが行われていない状態で領域間通信が行われていた。このうちマイナンバー利用事務系とインターネット接続系の領域間の通信制御の状況についてみたところ、3市区町村の延べ4件において、通信経路の限定又は通信プロトコルの限定のうち少なくともいずれか一つが行われていない状態で領域間通信が行われていた。

なお、ＬＧＷＡＮ接続系とインターネット接続系の間の通信についても上記の考え方に準じて確認したところ、61市区町村の延べ174件において、通信経路の限定又は通信プロトコルの限定のうち少なくともいずれか一つが行われていない状態で領域間通信が行われていた。

(注19)　Ｌ３スイッチ　　ＬＡＮの中核を構成する機器であり、データを転送する際の制御を主な機能とし、ＩＰアドレスによりアクセスを制限するなどネットワークを分割したり、端末をグループ化したりするなどの機能を有するもの

(注20)　通信プロトコルの限定　　通信規約（通信する上での約束事や手続）により通信を限定すること

(注21)　アプリケーションプロトコルのレベルでの限定　　通信規約の分類の一つで、具体的な用途やソフトウェア、サービス等の種類に応じて個別に制定されたものにより通信を限定すること

図表2-13　領域間通信の状況

領域間通信の対象	領域間通信の総数	通信経路の限定又は通信プロトコルの限定のうち少なくともいずれか一つが行われていないもの
マイナンバー利用事務系とＬＧＷＡＮ接続系	185市区町村　延べ784件	58市区町村　延べ243件
マイナンバー利用事務系とインターネット接続系	12市区町村　延べ23件	3市区町村　延べ4件
計	188市区町村　延べ807件	59市区町村　延べ247件
ＬＧＷＡＮ接続系とインターネット接続系	204市区町村　延べ865件	61市区町村　延べ174件
合　計	217市区町村　延べ1,672件	―

注(1) 市区町村数は領域間通信の対象ごとに計上していて重複があるため、各項目を合計しても計と一致しない。

注(2) 会計実地検査時点においてＬＧＷＡＮ接続系とインターネット接続系の分割が行われていない1市区町村は、マイナンバー利用事務系と他の領域（ＬＧＷＡＮ環境を含む領域）について、マイナンバー利用事務系とＬＧＷＡＮ接続系の欄に状況を記載している。

しかし、通信経路の限定が行われない場合には、本来意図しない端末等間において領域間通信が行われるおそれがある。また、通信プロトコルの限定が行われ

ない場合には、本来意図しないサービス（アプリケーション等）について領域間通信が行われるおそれがある。

強じん性向上事業における各種の施策は、マイナンバー利用事務系と他の領域との通信が原則としてできないようにすることを前提としており、マイナンバー利用事務系と他の領域との間で通信する場合でも通信先のサーバや端末もインターネットとの通信がないこと、ＬＧＷＡＮ接続系とインターネット接続系についても必要な通信だけを許可できるようにすることとしていて、例外的に認められる通信については、その設定に不備等がある場合、住民情報の流出につながるおそれがあることから、セキュリティの確保に十分に留意する必要がある。

したがって、総務省は、マイナンバー利用事務系の他の領域からの分離及びＬＧＷＡＮ接続系とインターネット接続系との通信経路の分割後の領域間通信において、本来意図しない通信を防止するための方策を改めて明示するなど、地方公共団体に対して助言を行う必要がある。

(ｳ) ＬＧＷＡＮ接続系とインターネット接続系との通信経路の分割後のインターネット接続系からＬＧＷＡＮ接続系への無害化通信の状況

11月報告及び論点集によれば、標的型攻撃においてはマルウェアをメールに添付された文書ファイル等に仕込まれて侵入されることが多いため、インターネット接続系で受信したメールをＬＧＷＡＮ接続系に転送する必要がある場合には、メールを無害化することとされている。そして、メールの無害化の方法は、ＨＴＭＬ形式で記述されたメール本文をテキスト化したり、添付ファイルを削除したりすることなどとされている。また、添付ファイルをインターネット接続系からＬＧＷＡＮ接続系へ転送する場合の方法としては、画像ファイルに変換したり、その他の添付ファイルを無害化するサービスを利用したりするなどして転送することが望ましいとされている。そして、業務上必要な添付ファイルに限っては、インターネット接続系の端末でウイルスチェックを行った上で、上司等の利用許可の下、専用の外部記憶媒体を利用するなどして収受することが考えられるとされている。

また、添付ファイル以外の業務上必要なファイルについても、マルウェアに感染しているファイルをＬＧＷＡＮ接続系に取り込むことを防止するという観点から、上記と同様にウイルスチェックを行うなどした上で収受することが重要であ

る。

そこで、会計実地検査時点においてＬＧＷＡＮ接続系とインターネット接続系の分割が行われている222市区町村について、メール本文及び添付ファイルその他の業務上必要なファイル（以下、これらを合わせて「添付ファイル等」という。）の転送又は収受に当たり、強じん性向上事業により整備した機器等により無害化が行われているか確認したところ、図表2-14のとおりとなっており、インターネット接続系からＬＧＷＡＮ接続系へメール本文を無害化することなく転送しているのが4市区町村等となっていた。そして、添付ファイル等の転送又は収受における無害化の状況についてみると、無害化した添付ファイル等を転送又は収受する仕組みを構築した上で無害化のサービスが対応していないなどの一部の添付ファイル等の無害化を行わずに転送又は収受しているのが159市区町村、上記のような無害化を行うことなく転送又は収受しているのが49市区町村等となっていた。

標的型攻撃は大きな脅威となっており、メール本文や添付ファイル等を無害化しないままＬＧＷＡＮ接続系との間で転送又は収受している市区町村においては、住民情報の流出につながるおそれがある。一方、メール本文や添付ファイル等が無害化のサービスに対応していないものであったり、無害化することにより本来の機能が損なわれたりすることなどにより、無害化が業務の効率性を著しく損なう場合がある。このため、メール本文や添付ファイル等をやむを得ず無害化を行うことなく転送又は収受する場合には、マルウェアに感染している添付ファイル等をＬＧＷＡＮ接続系に取り込むことなどを防止するため、オペレーティングシステム（以下「ＯＳ」という。）等の更新プログラム（以下「更新プログラム」という。）及びウイルス対策ソフトの更新データ（以下「更新データ」という。）を最新の状態に保つなどしてウイルスチェック等を確実に実施するための措置を講ずる必要がある。

図表2-14　インターネット接続系からＬＧＷＡＮ接続系へのメール本文及び添付ファイル等の転送又は収受における無害化の状況

（単位：市区町村数）

転送又は収受の対象	転送又は収受している市区町村				転送又は収受していない市区町村	計
		無害化（テキスト化）したもののみ転送	一部を無害化（テキスト化）しないまま転送	常に無害化（テキスト化）しないまま転送		
メール本文	152	147	1	4	70	222
添付ファイル等	218	10	159	49	4	222

(ｴ) ＬＧＷＡＮ接続系とインターネット接続系との通信経路の分割後のＬＧＷＡＮ接続系におけるＯＳの更新プログラム等の適用の状況

セキュリティポリシーガイドラインによれば、情報システムにコンピュータウイルス等の不正プログラム対策が十分に行われていない場合、システムの損傷、情報漏えいなどが発生するおそれがあるため、更新プログラム及び更新データの適用等を確実に実施することが基本であるとされている。従来、市区町村は、情報セキュリティを維持するために、これらの更新プログラム等を随時インターネットからダウンロードして端末等に適用するなどしていた。しかし、ＬＧＷＡＮ接続系とインターネット接続系を分割したことから、ＬＧＷＡＮ接続系においては、地方公共団体情報システム機構(注22)（以下「Ｊ－ＬＩＳ」という。）が運営するＬＧＷＡＮ－ＡＳＰ(注23)から購入してダウンロードしたり、職員等が手作業により外部記憶媒体を利用してオフラインでのインストールをしたりして更新プログラム等を適用することが必要となる。

(注22)　地方公共団体情報システム機構　　地方公共団体情報システム機構法（平成25年法律第29号）に基づき、地方公共団体が共同して運営する組織として、マイナンバー法等の規定による事務等を地方公共団体に代わって行うとともに、地方公共団体に対してその情報システムに関する支援を行い、もって地方公共団体の行政事務の合理化及び住民の福祉の増進に寄与することを目的とする法人

(注23)　ＬＧＷＡＮ－ＡＳＰ　　ＬＧＷＡＮを介して、利用者である地方公共団体の職員に各種行政事務サービスを提供するもので、アプリケーション及びコンテンツサービス並びに通信サービス等の5種類のサービスにより構成されている。

そこで、前記の222市区町村について、ＬＧＷＡＮ接続系とインターネット接続系の分割前後におけるＬＧＷＡＮ接続系に配置された端末等への更新プログラム等の適用状況を確認したところ、図表2-15のとおりとなっており、ＬＧＷＡＮ接続系とインターネット接続系の分割後である30年5月末時点において、更新プログラムを適用していないのが、分割前の26市区町村から54市区町村へ、更新データ

を適用していないのが、分割前の9市区町村から14市区町村へと増加していた。そして、これら54市区町村及び14市区町村の分割前における更新プログラム等の適用頻度についてみると、それぞれ29市区町村及び9市区町村は、分割前には1か月以内の頻度で適用していたのに、分割後に適用を行わなくなっていた。

図表2-15　ＬＧＷＡＮ接続系における更新プログラム及び更新データの適用状況

（単位：市区町村数）

ファイルの種類＼適用頻度		未適用	7か月以上	1か月～6か月	1か月以内	計
更新プログラム	分割前の適用状況	26(20)	10(5)	9(0)	177(29)	222
	分割後の適用状況	54	6	17	145	222
更新データ	分割前の適用状況	9(5)	1(0)	0(0)	212(9)	222
	分割後の適用状況	14	1	4	203	222

（注）括弧書きは、分割後の適用状況で未適用であった54市区町村及び14市区町村の分割前の状況である。

総務省は、更新プログラム等を適用していない市区町村においては、強じん性向上事業等で実施した対策の効果が十分に発現しないおそれがあることから、更新プログラム等の適用を適時に行い、マイナンバー利用事務系等へのコンピュータウイルスの感染を防止するための方策を改めて明示等する必要がある。

ウ　自治体情報セキュリティクラウドによる高度なセキュリティ対策の実施状況等

1(2)ウのとおり、11月報告では、インターネット接続系において、都道府県と市区町村が協力してインターネットの接続口を集約した上で、自治体情報セキュリティクラウドを構築し、高度なセキュリティ対策を講ずることとされている。総務省は、11月報告を踏まえて、強化対策費補助金の実施要領及び補助金Ｑ＆Ａにおいて、セキュリティクラウド事業の実施に当たり、都道府県は市区町村と十分協議の上、必要となる高度なセキュリティ対策を講ずることとしている。

そこで、241地方公共団体について、自治体情報セキュリティクラウドの構築及び高度なセキュリティ対策の実施状況等をみたところ、次のとおりとなっていた。

(ｱ)　自治体情報セキュリティクラウドへの接続状況

1(2)エ(ｲ)のとおり、強化対策費補助金の実施要領によれば、セキュリティクラウド事業においては、各市区町村が個別に設置しているＷｅｂサーバ等を都道府県が構築する自治体情報セキュリティクラウドに集約し、監視を始め高度なセキュリティ対策を実施するとされている。そして、監視対象とする機器等や高度なセキュリティ機器等を自治体情報セキュリティクラウドに集約することで、特に、専門的な担当者の確保等が困難と思われる市区町村においても、必要な対策を講

ずることが可能となる。また、総務省は、都道府県についても自治体情報セキュリティクラウドに接続することとしている。

そこで、前記の18都道府県が構築した自治体情報セキュリティクラウドについて、241地方公共団体の自治体情報セキュリティクラウドへの接続状況をみたところ、会計実地検査時点において、237地方公共団体が自治体情報セキュリティクラウドに接続していた。自治体情報セキュリティクラウドに接続していない4地方公共団体のうち2地方公共団体は、従前所有していたデータセンター機能を持った施設を有効活用するために近隣市区町村が別途構築したセキュリティクラウドに接続して共同利用しており、他の2地方公共団体は、31年3月末現在において、自治体情報セキュリティクラウドに接続している。

(ｲ) 自治体情報セキュリティクラウドに接続する地方公共団体における監視対象機器等の集約状況等

強化対策費補助金の実施要領によれば、監視については、自治体情報セキュリティクラウドに集約した機器等を対象とするとされており、補助金Ｑ＆Ａでは、Ｗｅｂサーバ、メールリレーサーバ(注24)（メールサーバを含む場合もある。）、プロキシサーバ(注25)及び外部ＤＮＳサーバ(注26)を集約の対象として挙げ、ＬＧＷＡＮ接続ファイアウォール(注27)のログについても自治体情報セキュリティクラウド上のログ分析システムにログを転送することにより、併せて監視対象とすることが望まれるとされている。また、論点集によれば、自治体情報セキュリティクラウドにおける監視について、インシデントに対して迅速かつ適切に対応するために、予兆を含めた早期検知と常駐する専門人材による早期判断が重要であり、そのため、自治体情報セキュリティクラウドにおいては、情報セキュリティ専門人材による24時間365日の監視が必要であると考えられるとされている。

(注24)　メールリレーサーバ　　メールの中継を行うサーバ
(注25)　プロキシサーバ　　インターネットと内部ネットワークとの境界で、内部ネットワーク内の端末等の代理としてインターネットとの通信を行うサーバ
(注26)　外部ＤＮＳサーバ　　サーバ等の情報をインターネットに公開するためのサーバ
(注27)　ＬＧＷＡＮ接続ファイアウォール　　各地方公共団体の内部のネットワークとＬＧＷＡＮ接続ルータとの間にあるファイアウォール

そこで、18都道府県が構築した自治体情報セキュリティクラウドについて、上記監視対象機器等の集約化のための設備の整備状況をみたところ、図表2-16のと

おり、Ｗｅｂサーバ、メールリレーサーバ及びプロキシサーバについては全ての都道府県が整備していた一方、外部ＤＮＳサーバについては1都道府県、ＬＧＷＡＮ接続ファイアウォールのログについては8都道府県が、それぞれ集約化のための設備を整備していないなどして、監視対象から除かれていた。

そして、自治体情報セキュリティクラウドに接続している237地方公共団体について、自治体情報セキュリティクラウドにおける集約及び監視状況をみたところ、Ｗｅｂサーバについては26地方公共団体、外部ＤＮＳサーバについては44地方公共団体、ＬＧＷＡＮ接続ファイアウォールのログについては116地方公共団体において、集約化のための設備が自治体情報セキュリティクラウドに整備されていなかったり、整備されていても接続している地方公共団体がこの設備を利用した集約をしていなかったりして、集約及び監視が行われていなかった。

図表2-16　監視対象機器等の集約化の状況

（単位:地方公共団体数）

集約化の対象機器等	18都道府県の集約化のための設備の整備状況			237地方公共団体の集約化の状況 注(1)		
	整備している	整備していない	計	集約している	集約していない 注(2)	計
Webサーバ	18	－	18	211	26	237
メールリレーサーバ	18	－		232	5	
プロキシサーバ	18	－		234	3	
外部DNSサーバ	17	1		193	44	
LGWAN接続ファイアウォールのログ	10	8		121	116	

注(1) 241地方公共団体のうち、会計実地検査時点において自治体情報セキュリティクラウドに接続済みの237地方公共団体について集計している。

注(2) 「集約していない」地方公共団体数には、当該機器を集約するための設備が自治体情報セキュリティクラウドにおいて整備されていないため、監視対象から除かれている地方公共団体数を含む。

なお、情報セキュリティ専門人材による監視の状況についてみると、自治体情報セキュリティクラウドに集約されている監視対象機器等については、情報セキュリティ専門人材による24時間365日の監視・分析等が行われているとされていた。

一方、自治体情報セキュリティクラウドに集約されておらず、各地方公共団体において別途管理されている上記の機器等についての監視の状況をみたところ、図表2-17のとおりとなっており、Ｗｅｂサーバについて、「情報セキュリティ専門人材による監視・分析を行っていない地方公共団体」が6地方公共団体、「情報

セキュリティ専門人材による監視・分析が行われているかを把握していない地方公共団体」が3地方公共団体、外部ＤＮＳサーバについて、「情報セキュリティ専門人材による監視・分析を行っていない地方公共団体」が11地方公共団体、「情報セキュリティ専門人材による監視・分析が行われているかを把握していない地方公共団体」が3地方公共団体、ＬＧＷＡＮ接続ファイアウォールのログについて、「情報セキュリティ専門人材による監視・分析を行っていない地方公共団体」が63地方公共団体、「情報セキュリティ専門人材による監視・分析が行われているかを把握していない地方公共団体」が5地方公共団体等となっていた。

図表2-17 監視対象機器等に対する監視の状況

（単位:地方公共団体数）

監視対象機器等	自治体情報セキュリティクラウドに集約していないために、セキュリティクラウドの監視・分析の対象外となっている地方公共団体	左記のうち各地方公共団体における監視の状況				
		情報セキュリティ専門人材による監視・分析の対象としていて、24時間365日監視しているとする地方公共団体	情報セキュリティ専門人材による監視・分析の対象としているが、24時間365日は監視していない、又は、24時間365日監視されているかを把握していない地方公共団体	情報セキュリティ専門人材による監視・分析が行われているかを把握していない地方公共団体	情報セキュリティ専門人材による監視・分析を行っていない地方公共団体	その他
Webサーバ	26	13	4	3	6	－
メールリレーサーバ	5	2	1	1	1	－
プロキシサーバ	3	2	1	－	－	－
外部DNSサーバ	44	25	4	3	11	1
LGWAN接続ファイアウォールのログ	116	28	20	5	63	－

注(1) 会計実地検査時点において自治体情報セキュリティクラウドに接続済みの237地方公共団体について集計している。

注(2) 「その他」は、当該機器等が24時間365日監視されているものの分析の対象ではないものである。

以上のように、自治体情報セキュリティクラウドに集約することとされている機器等が、自治体情報セキュリティクラウドにおいて一部整備されていなかったり、整備されていても接続している地方公共団体が集約をしていなかったりして、自治体情報セキュリティクラウドと同等の情報セキュリティ専門人材による監視・分析が行われていない機器等があることから、監視・分析の必要な機器等が都道府県に集約されていない場合には、総務省において、その状況を十分把握した上で、都道府県にできる限り集約されるなどして専門人材による監視・分析が行われるよう、必要に応じて助言を行う必要がある。

(ｳ) 自治体情報セキュリティクラウドに接続する地方公共団体におけるインシデント対応体制

市区町村のインターネット通信については、都道府県のセキュリティクラウドに集約した接続口を対象として、自治体情報セキュリティクラウドにおいて、情報セキュリティ専門人材が監視を行い、インシデントの発生を検知した際は、該当する市区町村等に通報することになっている。インシデントへの対応としては、不正な通信を行っている端末等をそのＩＰアドレス等により速やかに特定し、必要に応じて、自治体情報セキュリティクラウドや接続している地方公共団体においてネットワークから遮断するなどの迅速な措置を執ることが求められている。しかし、通報を受けた地方公共団体において必要とされる対応体制が整っていない場合、自治体情報セキュリティクラウドによる通報等を十分にいかせないこととなるおそれがある。

そこで、前記の237地方公共団体について、不正な通信を行っている端末等のＩＰアドレス等の特定や遮断等の対応が可能かをみたところ、図表2-18のとおり、標的型攻撃によるインシデント発生時に、自治体情報セキュリティクラウドに接続している地方公共団体において実施することとなっている対応の「全てを職員だけで実施可能」としているのは47地方公共団体となっていて、190地方公共団体は端末の特定等の対応の一部又は全部に事業者等の「他の組織の支援等を必要とする要素あり」としていた。

そして、不正な通信を行っている端末等の特定については、上記の190地方公共団体のうち70地方公共団体は「全ての端末等について自治体情報セキュリティクラウド側で特定が可能」としていて、残りの120地方公共団体は接続している地方公共団体側で端末特定に係る作業を要する状況となっていた。そして、120地方公共団体のうち77地方公共団体は「端末等を特定するために事業者等の支援等が必要」としているが、このうち11地方公共団体は支援等を行う事業者等との間で役割の確認を行っていなかったり、役割の確認を踏まえた内容で契約を締結していなかったり、必要な内容で契約が締結されているかの確認を行っていなかったりしていた。

また、自治体情報セキュリティクラウド側で不正な通信等を検知した場合のネットワークの遮断については、前記のとおり、自治体情報セキュリティクラウド

側で実施する場合と抜線等による物理的な遮断や仮想環境における遮断等の接続する地方公共団体側で実施する場合とがある。上記190地方公共団体のうち160地方公共団体は自らにおいてネットワーク遮断を実施することがあるとしていて、このうち129地方公共団体は遮断を実施するために事業者等の支援等を必要としている。しかし、このうち23地方公共団体は支援等に係る役割の確認及びそれを踏まえた契約の締結等を行っていなかった。

図表2-18　自治体情報セキュリティクラウドに接続している地方公共団体のインシデント発生時における対応体制の状況

<table>
<tr><th colspan="5">標的型攻撃によるインシデント発生時の地方公共団体の対応</th><th>地方公共団体数</th></tr>
<tr><td colspan="5">一連の対応の全てを職員だけで実施可能</td><td>47</td></tr>
<tr><td colspan="5">一連の対応について他の組織の支援等を必要とする要素あり</td><td>190</td></tr>
<tr><td rowspan="5">不正な通信を行っている端末等の特定</td><td colspan="4">全ての端末等について自治体情報セキュリティクラウド側で特定が可能</td><td>70</td></tr>
<tr><td colspan="4">一部又は全ての端末等について自治体情報セキュリティクラウド側での特定が不可能等</td><td>120</td></tr>
<tr><td rowspan="3"></td><td colspan="3">端末等を特定するために事業者等の支援等が必要</td><td>77</td></tr>
<tr><td colspan="2">支援等に係る事業者等との役割の確認等が未済</td><td>11</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td rowspan="5">ネットワーク遮断</td><td colspan="4">接続している地方公共団体側でネットワーク遮断を実施する場合なし</td><td>30</td></tr>
<tr><td colspan="4">接続している地方公共団体側でネットワーク遮断を実施する場合あり</td><td>160</td></tr>
<tr><td rowspan="3"></td><td colspan="3">ネットワークを遮断するために事業者等の支援等が必要</td><td>129</td></tr>
<tr><td colspan="2">支援等に係る事業者等との役割の確認等が未済</td><td>23</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td colspan="5">計</td><td>237</td></tr>
</table>

さらに、インシデント発生時に自治体情報セキュリティクラウドが実施するネットワーク遮断について、遮断の判断主体をみたところ、図表2-19のとおり、ネットワークの遮断を判断する際に、接続している地方公共団体側において遮断を判断することとしている12都道府県（場合によって判断主体が異なる10地方公共団体を含む。）の自治体情報セキュリティクラウドに接続する160地方公共団体のうち76地方公共団体及び判断主体が決まっていない1都道府県の自治体情報セキュリティクラウドに接続する7地方公共団体のうち5地方公共団体は、遮断の判断に至る手順を策定していなかったり、文書化していなかったりしていた。

図表2-19　ネットワーク遮断の判断主体に係る状況

ネットワーク遮断の判断主体と判断に係る手順の策定等	地方公共団体数
ネットワーク遮断の判断を自治体情報セキュリティクラウド側において行うこととなっている地方公共団体	70
ネットワーク遮断の判断を接続している地方公共団体側において行うこととなっている地方公共団体	160（注）
接続している地方公共団体側において、遮断の判断に係る手順の策定や文書化が未済である地方公共団体	76
自治体情報セキュリティクラウド側と接続している地方公共団体側のどちらがネットワーク遮断の判断を行うか決まっていない地方公共団体	7
接続している地方公共団体側において、遮断の判断に係る手順の策定や文書化が未済である地方公共団体	5
計	237

（注）接続する地方公共団体において遮断を判断することとしている2都道府県の自治体情報セキュリティクラウドに接続する28地方公共団体と、自治体情報セキュリティクラウド側と接続している地方公共団体側のどちらが判断主体となるかは場合により異なる10都道府県の自治体情報セキュリティクラウドに接続する132地方公共団体の合計

このように、インシデント発生時に必要となる不正な通信を行っている端末等の特定やネットワーク遮断等の一連の対応の際に事業者等の支援等が必要であるにもかかわらず、当該支援等に係る事業者等との役割の確認等が未済であったり、ネットワーク遮断の判断に至る手順を策定するなどしていなかったりしている地方公共団体においては、インシデント発生時の対応に漏れや誤りが生じたり、判断等を迅速に行えなかったりするなどの事態により、自治体情報セキュリティクラウドによる通報等を十分にいかせないこととなるおそれがある。

したがって、総務省においては、自治体情報セキュリティクラウドに接続する地方公共団体に対して、そのネットワーク遮断等を支援する事業者等と役割の確認をすることの必要性を明示するなどして、インシデント発生時に適切にネットワークを遮断することなどができるよう、必要に応じて助言を行う必要がある。

エ　情報セキュリティ対策の実効性を確保するための体制整備等

(ｱ) 情報セキュリティポリシーの策定及び強じん化に係る改定等の状況

1(1)イ(ｳ)のとおり、セキュリティポリシーガイドラインによれば、情報セキュリティ対策を徹底するためには、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とされており、情報セキュリティポリシーは、基本方針と対策基準から構成されるものとされている。また、情報セキュリティ対策は、情報セキュリティに関する脅威や技術等の変化に応じて、必要

な対策が変化するものであり、情報セキュリティポリシー等は、定期的に見直しを行い、情報セキュリティ対策の実効性を確保するとともに、対策レベルを高めていくことが重要であるとされている。そして、情報セキュリティは、ハードウェア及びソフトウェアの整備だけではなく、それらの運用や人的セキュリティに係る対策等を講ずることも必要である。また、これらの体制整備等が適切に行われることにより、強化対策費補助金の交付の目的である情報セキュリティ対策の強化が実現することとなる。

そこで、前記の241地方公共団体について、会計実地検査時点における対策基準の策定及び強じん化を踏まえた改定等の取組の状況をみたところ、対策基準を策定していなかったものは3地方公共団体となっていた。また、強じん化を踏まえた対策基準の改定の取組については、対策基準に強じん化を踏まえた規定がないとしているものが178地方公共団体となっていた。

そして、強じん化を講ずる方法等が30年9月に改定されたセキュリティポリシーガイドラインにおいて具体的に記載されたことから、改定後の同年11月末時点の地方公共団体における対策基準の改定の予定についてみたところ、上記178地方公共団体のうち40地方公共団体が未定としていた。さらに、強じん化に係る対策基準の改定時期を未定としていた主な理由を40地方公共団体に確認したところ、「人員不足」「業務多忙」等としていた。

したがって、総務省は、補助事業で強化された情報セキュリティ対策の実効性を確保するために、強じん化を踏まえた対策基準の見直しについて、必要に応じて地方公共団体に対して助言を行う必要がある。

(ｲ) 強じん性向上事業実施後のセキュリティリスクへの組織的な対応

1(2)イのとおり、総務省は、8月通知において、地方公共団体は、インシデントの発生に備えて、ＣＩＳＯを設置するとともに、インシデントに関するコミュニケーションの核となる体制であるＣＳＩＲＴ等の組織を構築することが必要であるとしていて、地方公共団体に対して、インシデント発生時の国までの連絡ルートを再構築（多重化）することを要請するとともに、緊急時対応計画について、標的型攻撃が増加している現状に対応しているか見直すことが必要であるとして、その見直し後の内容に基づいた緊急時対応訓練を逐次実施することを要請している。

そして、強じん性向上事業等の実施により、マイナンバー利用事務系と他の領域との分離が徹底され、ＬＧＷＡＮ接続系とインターネット接続系が分割された地方公共団体においても、インターネット接続系からの添付ファイル等の転送又は収受や、外部記憶媒体によりコンピュータウイルスに感染するなどすれば、特定個人情報等の情報資産が破壊されるなどの被害を受けるおそれがあることから、強じん性向上事業の効果が持続的に発現するためには、インシデント発生時の体制が整備されていることが必要である。

そこで、241地方公共団体のインシデント発生時における対応体制の整備等の状況をみたところ、図表2-20のとおりとなっており、ＣＩＳＯは232地方公共団体（241地方公共団体に占める割合96.2%。ＣＩＯ等がＣＩＳＯの役割を担っているものを含む。）で設置していたが、ＣＳＩＲＴを設置していたのは130地方公共団体（同53.9%）にとどまっており、ＣＳＩＲＴを設置していない111地方公共団体に主な理由を確認したところ、「人員が足りない」「知見がない」等としていた。また、130地方公共団体のうち16地方公共団体では、ＣＳＩＲＴの要員及び機能について文書化していなかったり、37地方公共団体では緊急時対応計画を策定していなかったり、49地方公共団体ではインシデント発生時に国及び庁内ＣＩＳＯ等へ一斉同報する連絡ルートを構築していなかったりしていた。これらの地方公共団体では、インシデント発生時において講ずべき措置内容や連絡体制が明確となっていないことなどにより、ＣＳＩＲＴが迅速かつ的確に機能しないおそれがある。

さらに、緊急時対応計画における標的型攻撃に対応する内容の規定の整備状況及び緊急時対応訓練の実施状況をみたところ、図表2-20のとおりとなっており、緊急時対応計画において標的型攻撃に対応した内容を規定しているとしたのは66地方公共団体（同27.3%。別途標的型攻撃への対応について規定した文書を策定しているものを含む。）、緊急時対応訓練を実施したのは54地方公共団体（同22.4%）となっていた。そして、上記のいずれも実施したものは28地方公共団体（同11.6%）にとどまっており、特に、政令指定都市及び中核市を除く市町村では、182地方公共団体のうち6地方公共団体（182地方公共団体に占める割合3.2%）のみとなっていて、小規模な地方公共団体ほど、インシデントが発生した場合に即応できる十分な体制が構築できていないおそれがある状況となっていた。

一方、総務省は、近年の情報セキュリティ対策の高度化において、地方公共団体単独での対策には限界が生じており、専門的な知見に基づく対策が求められているとして、ネットワーク上で地方公共団体の担当者がセキュリティ専門家から助言を受けたり、他の地方公共団体との事例の共有を行ったりすることができるようにすることなどを目的として、支援ＰＦを構築している。

したがって、総務省は、補助事業で強化された情報セキュリティ対策の実効性を確保するために、インシデント発生時の体制整備等に係る緊急時対応計画の策定、連絡体制の構築等について、支援ＰＦを活用するなどして、必要に応じて地方公共団体に対して助言を行う必要がある。

図表2-20　地方公共団体の区分別のインシデント発生時における体制整備等の状況

区分	地方公共団体数	ＣＩＳＯを設置しているもの	ＣＳＩＲＴを設置しているもの	ＣＳＩＲＴの要員及び機能について文書化していないもの	緊急時対応計画を策定していないもの	インシデント発生時の国及び庁内ＣＩＳＯ等へ一斉同報する連絡ルートを策定していないもの	緊急時対応計画を策定しているもの	①8月通知を受けて標的型攻撃に対応した内容を規定しているもの	②8月通知を受けて緊急時対応訓練を実施したもの	①及び②ともに実施したもの
都道府県	18	17 (94.4%)	15 (83.3%)	2	1	3	16 (88.8%)	8 (44.4%)	11 (61.1%)	7 (38.8%)
政令指定都市・中核市・特別区	41	41 (100.0%)	33 (80.4%)	3	6	5	32 (78.0%)	19 (46.3%)	25 (60.9%)	15 (36.5%)
市町村（政令指定都市・中核市を除く。）	182	174 (95.6%)	82 (45.0%)	11	30	41	81 (44.5%)	39 (21.4%)	18 (9.8%)	6 (3.2%)
計	241	232 (96.2%)	130 (53.9%)	16	37	49	129 (53.5%)	66 (27.3%)	54 (22.4%)	28 (11.6%)

(3) 支援ＰＦの利活用の状況

総務省は、1(2)カのとおり、8月報告を受けて、地方公共団体単独での情報セキュリティ対策には限界が生じているとの認識の下、地方公共団体における情報セキュリティ対策向上に寄与することを目的として、支援ＰＦを27年9月から運用するとともに、28年3月から自治体の掲示板機能を追加しており、支援ＰＦの構築等に係る事業費は4752万円となっている。

支援ＰＦの主な機能は、図表3-1のとおりとなっている。

図表3-1　支援ＰＦの主な機能

機能名	内容
インシデント関連掲示板機能	過去に発生したインシデントの事例や情報セキュリティに関する注意喚起等、地方公共団体の情報セキュリティに関する情報を登録したり、表示したりする機能
Ｑ＆Ａ機能	地方公共団体が情報セキュリティに関する問合せを登録し、情報セキュリティ専門家がその問合せに対する回答を登録し、その登録された回答を問合せ元の地方公共団体が参照できるようにする機能。情報セキュリティ専門家が作成したＱ＆Ａ案件のサマリー情報は、問合せ元の地方公共団体が公開を承認しない場合を除き、全ての地方公共団体が参照できる。
ワーキンググループ機能	情報セキュリティ専門人材から構成されるワーキンググループで作成され、登録されたインシデント初動マニュアルや対処訓練マニュアル等の各種マニュアルを参照できる機能
その他関連情報機能	登録された自治体情報セキュリティの関連情報等を参照できるようにする機能
自治体の掲示板機能（平成28年3月に追加）	地方公共団体の担当者が専用の掲示板に質問を投稿し、他の地方公共団体への回答の依頼を行える機能

総務省は、支援ＰＦのＷｅｂサイトにログインするために必要なユーザーＩＤを各地方公共団体の情報システム担当部署に一つずつ配布しており、地方公共団体の担当者は支援ＰＦのＷｅｂサイトに適宜アクセスして、必要な情報を閲覧したり、セキュリティ専門家に問合せを行ったりなどすることになっている。また、支援ＰＦのユーザーＩＤの登録数は、30年5月末現在で、総務省5、セキュリティ専門家50、地方公共団体1,788となっている。

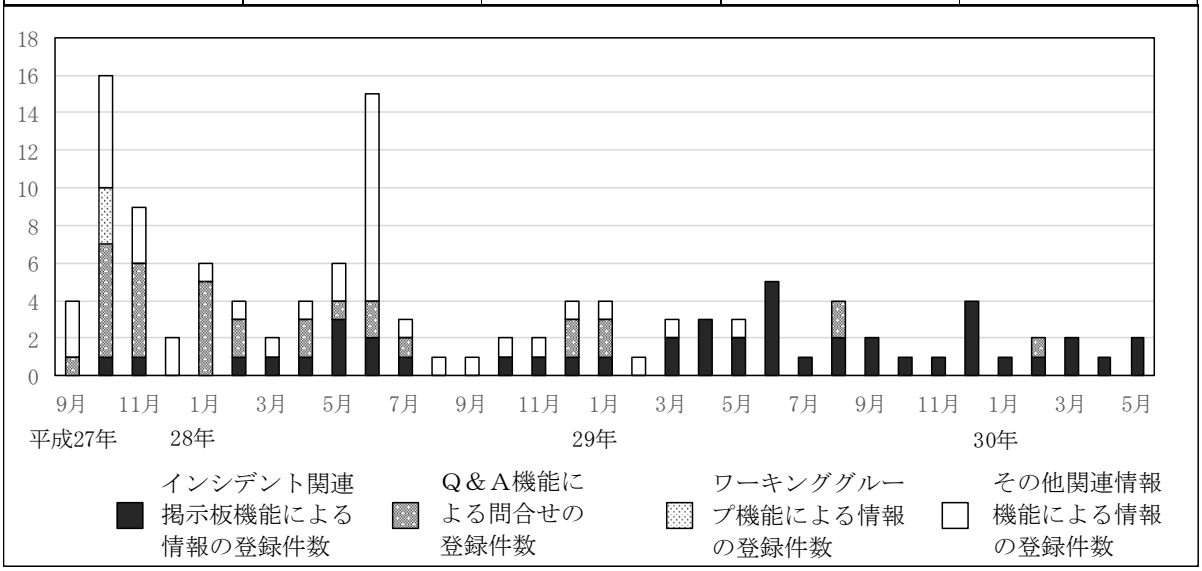
ア　支援ＰＦへの情報の登録等の状況

27年9月から30年5月までの2年9か月に、支援ＰＦに登録された情報セキュリティに関する情報等について、主な機能ごとに確認したところ、図表3-2のとおりとなっており、インシデント関連掲示板機能については、情報の総登録件数は45件で、登録が全くない月数が6月、1件しか登録がない月数が16月となっていた。Ｑ＆Ａ機能については、問合せの総登録件数は32件で、登録が全くない月数が20月、1件しか登録がない月数が4月となっていて、29年2月以降は3件にとどまっていた。ワーキング

グループ機能については、情報の総登録件数は27年10月に情報セキュリティ専門人材で構成されるワーキンググループで作成されたインシデント初動マニュアルの情報が3件掲載されたのみとなっていて、同年11月以降は情報の登録はなかった。その他関連情報機能については、情報の総登録件数は41件で、29年6月以降は情報の登録はなかった。自治体の掲示板機能については、当該機能が追加された28年3月以降、質問の投稿が全くなかった。

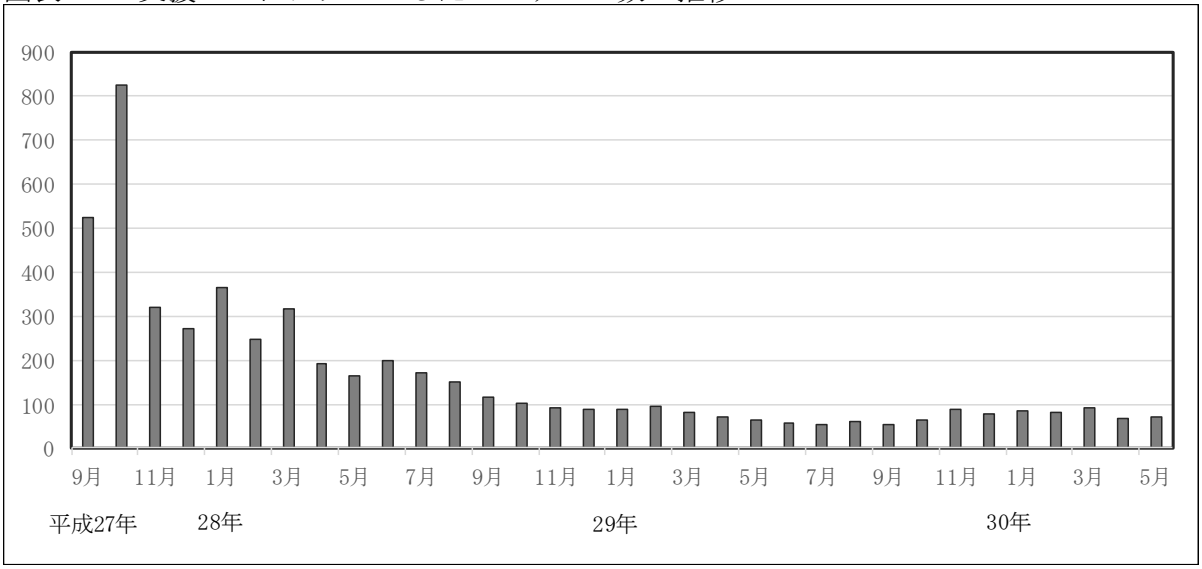
図表3-2　支援ＰＦの主な機能ごとのセキュリティに関する情報等の登録の状況

インシデント関連掲示板機能による情報の登録件数	Ｑ＆Ａ機能による問合せの登録件数	ワーキンググループ機能による情報の登録件数	その他関連情報機能による情報の登録件数	自治体の掲示板機能による質問の投稿件数
45	32	3	41	0



支援ＰＦの利用等の状況について、支援ＰＦにアクセスした個別のユーザーの月ごとの数を総務省に確認したところ、図表3-3のとおり、運用を開始した27年9月直後は一定数がアクセスしていたものの、28年11月以降は毎月100ユーザー未満となっていて、支援ＰＦにアクセスしているユーザー数は、同月以降、運用当初に比べて相当少数にとどまっていた。

図表3-3　支援ＰＦにアクセスしたユーザーの数の推移



イ　支援ＰＦの利用等の状況

241地方公共団体に支援ＰＦの利用等の状況を確認したところ、図表3-4のとおり、68地方公共団体は、会計実地検査の時点まで「支援ＰＦの存在を知らなかった」としており、全く利用していなかった。また、「支援ＰＦの存在を知っていた」とする173地方公共団体の利用状況を確認したところ、「毎日利用している」とするものが1地方公共団体（241地方公共団体に占める割合0.4%）、「時々利用している」とするものが12地方公共団体（同4.9%）とそれぞれ少数にとどまっていて、「ほとんど利用していない」（利用頻度が3か月に1回程度未満）とするものが49地方公共団体（同20.3%）、「ログインが初回実績のみ」とするものが37地方公共団体（同15.3%）、「全く利用したことがない」とするものが74地方公共団体（同30.7%）となっていた。

図表3-4　支援ＰＦの利用等の状況

支援ＰＦの利用等の状況	地方公共団体数	割合（%）
支援ＰＦの存在を知っていたもの	173	71.7
利用したことがあるもの	99	41.0
毎日利用しているもの	1	0.4
時々利用しているもの	12	4.9
ほとんど利用していないもの（利用頻度が3か月に1回程度未満）	49	20.3
ログインが初回実績のみ	37	15.3
全く利用したことがないもの	74	30.7
支援ＰＦの存在を知らなかったもの	68	28.2
計	241	100.0

228（94.6%）

このように、241地方公共団体のうち計228地方公共団体（同94.6%）が支援ＰＦを利用したことがない、又はほとんど利用していないことから、支援ＰＦの存在を知っていたもののほとんど利用していない49地方公共団体にその理由を確認したところ、図表3-5のとおり、「Ｊ－ＬＩＳからセキュリティ喚起情報を入手するなど別の方法で情報を得ているため」とするものが29地方公共団体（49地方公共団体に占める割合59.1%）、「情報の更新が少ないため」とするものが11地方公共団体（同22.4%）等となっていた。

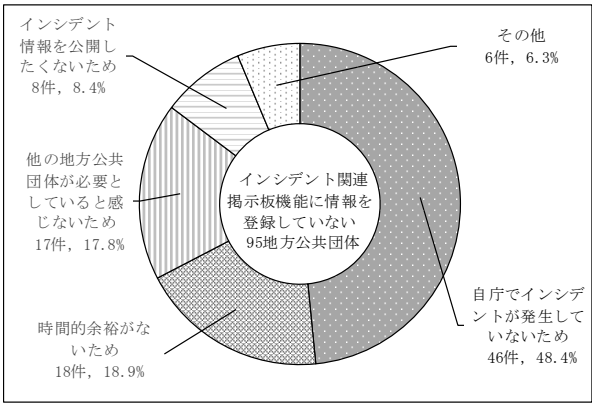
図表3-5　支援ＰＦをほとんど利用していない理由

理由	地方公共団体数	割合（%）
Ｊ－ＬＩＳからセキュリティ喚起情報を入手するなど別の方法で情報を得ているため	29	59.1
情報の更新が少ないため	11	22.4
有益な情報がないため	6	12.2
その他	3	6.1
計	49	100.0

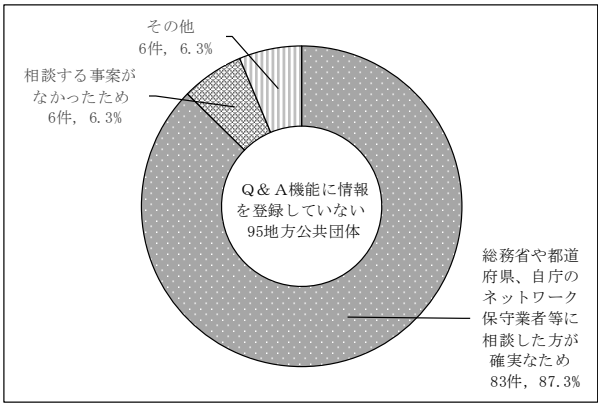
また、前記のとおり、支援ＰＦへの情報の登録が低調になっていることから、支援

ＰＦを利用したことがあるとした99地方公共団体のうち、支援ＰＦの各機能のうち主として地方公共団体が情報を登録することが想定されるインシデント関連掲示板機能、Ｑ＆Ａ機能及び自治体の掲示板機能にそれぞれ情報や質問等を登録したことがない地方公共団体（それぞれ、95地方公共団体、95地方公共団体及び99地方公共団体）に、それぞれその理由を確認したところ、図表3-6、同3-7、及び同3-8のとおりとなっており、Ｑ＆Ａ機能及び自治体の掲示板機能については、いずれも他の方法で対応しているためとしている地方公共団体が多くなっていた。

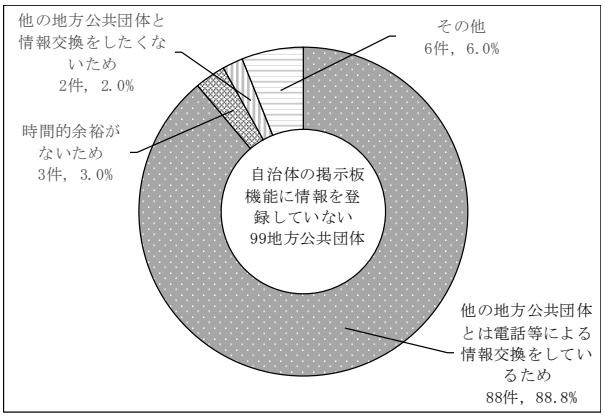
図表3-6　インシデント関連掲示板機能に情報を登録していない理由



図表3-7　Ｑ＆Ａ機能に情報を登録していない理由

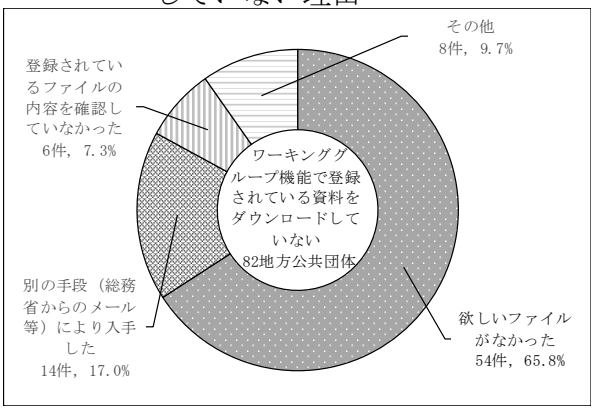


図表3-8　自治体の掲示板機能に情報を登録していない理由

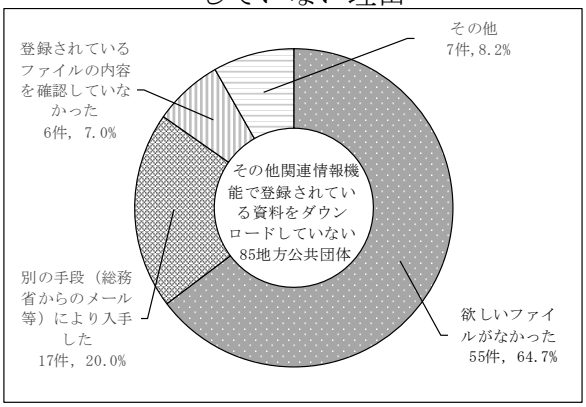


また、ワーキンググループ機能及びその他関連情報機能については、それぞれ、登録されている資料をダウンロードできることから、支援ＰＦを利用したことがあるとした99地方公共団体のうち、登録されている資料のダウンロードを行ったことがない地方公共団体（82地方公共団体及び85地方公共団体）に、それぞれその理由を確認したところ、図表3-9及び同3-10のとおりとなっており、いずれも欲しいファイルがなかったためとしている地方公共団体が多くなっていた。

図表3-9　ワーキンググループ機能で登録されている資料をダウンロードしていない理由



図表3-10　その他関連情報機能で登録されている資料をダウンロードしていない理由



以上のことから、支援ＰＦは、地方公共団体の情報セキュリティ対策向上のために十分に利活用されているとはいえない状況となっており、総務省における支援の需要の把握や、支援ＰＦが提供する情報や機能の見直しなどの検討も行われていない状況となっていた。

したがって、総務省において、支援ＰＦが地方公共団体における情報セキュリティ対策向上に寄与するよう、支援ＰＦの機能及び利活用の方法等について地方公共団体へ重ねて周知するとともに、支援の需要を把握して、支援ＰＦが提供する情報や機能の見直しなどについて検討する必要がある。

4　所見

(1) 検査の状況の概要

総務省は、年金情報流出事案等を受けて設置した検討チームから、11月報告において、三層の構えとして、①マイナンバー利用事務系においては、原則として、他の領域との通信ができないように分離を徹底した上で、端末への二要素認証や情報持出し不可設定の導入等を図ることにより、住民情報の流出を徹底して防ぐこと、②マイナンバーによる情報連携に活用されるＬＧＷＡＮ環境のセキュリティ確保に資するため、ＬＧＷＡＮ接続系とインターネット接続系との通信経路を分割した上で、両システム間で通信する場合には、ウイルスの感染のない無害化通信を図ること、③インターネット接続系においては、都道府県と市区町村が協力してインターネット接続口を集約した上で、自治体情報セキュリティクラウドを構築し、高度なセキュリティ対策を講ずることが提言された。総務省は、これを踏まえて、12月通知により地方公共団体に対し、三層の構えによる情報セキュリティ対策の強化を要請するとともに、平成27年

度補正予算において強化対策費補助金を交付した。そして、地方公共団体は、これを受けて、情報セキュリティ対策の強化等を行い、27年度以降順次、運用を開始するなどしている。また、総務省は、地方公共団体における情報セキュリティ対策向上に寄与することを目的として支援ＰＦを運用するなどしている。

そこで、会計検査院は、強化対策費補助金等の状況について、合規性、経済性、効率性、有効性等の観点から、①強化対策費補助金の交付状況はどのようになっているか、②強化対策費補助金等による地方公共団体の情報セキュリティ対策の強化は、補助金交付の目的に照らして適切に実施されているか、また、補助金交付の目的を実現し、効果を持続させるための体制等は整備されているか、③総務省は強化対策費補助金で強化された情報セキュリティ対策の実効性を確保するためどのような支援を行っているか、支援ＰＦは有効に機能しているかに着眼して検査したところ、次のような状況が見受けられた。

ア　強化対策費補助金の交付状況

(ｱ) 都道府県への強化対策費補助金の交付状況

18都道府県に対して交付された強化対策費補助金計27億2938万余円を補助対象事業別にみると、18都道府県の全てがセキュリティクラウド事業を実施して計22億5145万余円（交付実績額の合計に占める割合82.4%）の交付を受けており、10都道府県は強じん性向上事業にも交付を受けていた（16、17ページ参照）。

(ｲ) 市区町村への強化対策費補助金の交付状況

223市区町村に対して交付された強化対策費補助金計34億0981万余円を補助対象事業別にみると、223市区町村の全てが強じん性向上事業を実施して計33億8299万余円（交付実績額の合計に占める割合99.2%。事業別に分離できない交付実績額計1638万余円を除く。）の交付を受けており、27市区町村はセキュリティクラウド事業にも交付を受けていた（17ページ参照）。

イ　三層の構えによる情報セキュリティ対策の強化の実施状況等

(ｱ) マイナンバー利用事務系の端末等の二要素認証等の実施状況等

ａ　マイナンバー利用事務系における端末等の配置状況

18都道府県及び管内223市区町村の計241地方公共団体のマイナンバー利用事務系の端末等の配置状況について、マイナンバー利用事務系の端末のみを配置しているのは、16都道府県及び198市区町村の計214地方公共団体、マイナンバ

ー仮想利用端末のみを配置しているのは、1都道府県及び4市区町村の計5地方公共団体、マイナンバー利用事務系の端末とマイナンバー仮想利用端末を併用しているのは1都道府県及び21市区町村の計22地方公共団体となっていた（18～20ページ参照）。

b　マイナンバー利用事務系の端末への二要素認証の導入等の状況

223市区町村のうち、マイナンバー利用事務系の端末を配置し、全部又は一部の端末に二要素認証を導入していた217市区町村における導入した端末の範囲や運用等の状況をみたところ、マイナンバー利用端末の一部に二要素認証を導入していないのが12市区町村となっており、このうちマイナンバー利用端末の全てに導入する予定があるとしていないものが10市区町村となっていた。マイナンバー利用端末の一部に導入しておらず、マイナンバー利用端末の全てに導入する予定があるとしていない市区町村においては、マイナンバー利用端末に一要素による認証でログインでき、正規の権限を持たない職員等が、正規の権限を持つ職員になりすましてログインして、特定個人情報に不正にアクセスすることが、二要素認証を導入した端末に比べて容易な状況となっていた。

上記の217市区町村における、「所持」又は「存在」による認証がエラーとなった際等の代替手段の状況をみたところ、27市区町村は、認証の代替手段となるパスワードをあらかじめ設定する運用を行うなどしていた。また、7市区町村は、一部のアカウントについて、端末及び業務システムにログインするために必要となる「知識」及び「所持」の認証の手段を職員の間で両方とも共有していて、共有している認証の手段のみで端末及び業務システムにログインが可能な状況となっていた。さらに、特定個人情報を端末のローカルドライブ等に保存していた122市区町村について、特定個人情報を保存していた端末のローカルドライブ等にアクセスできる端末に共有している認証の手段のみでログインできるかみたところ、15市区町村では、共有している認証の手段のみで端末にログインできる状況となっており、不正アクセスや情報漏えいが発生した場合に不正アクセスした者等の特定が困難になるおそれがある状況となっていた。また、16市区町村では、段階的な認証方法を採用しているため、一要素による認証で端末にログインし、特定個人情報に不正にアクセスできる状況となっていた。そして、7市区町村では、同じ課室内に所属する正規の権限を持たない職員

でも共有フォルダに保存されている特定個人情報にアクセスできる状況となっていた（20～28ページ参照）。

c　マイナンバー利用事務系の端末からの情報持出し不可設定の導入等の状況

223市区町村のうち、マイナンバー利用事務系の端末を配置し、全部又は一部の端末に情報持出し不可設定を導入していた218市区町村における導入した端末の範囲や運用等の状況をみたところ、マイナンバー利用端末の一部に情報持出し不可設定を導入していないのが13市区町村となっており、このうちマイナンバー利用端末の全てに導入する予定があるとしていないものが12市区町村となっていた。マイナンバー利用端末の一部に導入しておらず、マイナンバー利用端末の全てに導入する予定があるとしていない市区町村においては、特定個人情報を持ち出す正当な理由のない職員が、情報持出し不可設定を導入していない端末から不正に特定個人情報を持ち出すことが、情報持出し不可設定を導入した端末に比べて容易な状況となっていた。

218市区町村における例外的な情報持出しの運用状況をみたところ、端末からの例外的な情報持出しを認めている203市区町村のうち、160市区町村では管理者権限を持つ職員等が職員からの申請に基づいて情報持出し不可設定を解除する運用を行っており、このうち、期限を設けることなく情報持出し不可設定を解除する運用をしているものが62市区町村、解除期間を1か月以上としているものが27市区町村となっていた。

期限を設けることなく解除する運用をしている市区町村及び情報持出し不可設定の解除期間を1か月以上としている市区町村の純計87市区町村について、情報を持ち出す場合の情報セキュリティ管理者の許可の実施状況をみたところ、全ての市区町村において情報セキュリティ管理者による許可がなくても情報を持ち出すシステム操作ができるようになっており、このうち29市区町村では、情報セキュリティ管理者に許可を得る運用もしていない状況となっていた。

また、情報持出しに係る記録等の実施状況をみたところ、44市区町村では全部又は一部の媒体についてログを保存していないとしていた。そして、情報を持ち出す際の氏名、日時、持出物等の台帳等への記録については、77市区町村が記録していないとしていた。さらに、データ暗号化機能を備える外部記憶媒体の使用等の状況についてみたところ、81市区町村は暗号化の実施を職員が任

意で行っている状況となっており、56市区町村は、そもそも暗号化機能を備える外部記憶媒体を使用するなどしていなかった（28～35ページ参照）。

(ｲ) マイナンバー利用事務系等の分離、分割等の実施状況等

a　マイナンバー利用事務系の他の領域からの分離及びＬＧＷＡＮ接続系とインターネット接続系との通信経路の分割の状況

223市区町村における領域間の分離及び分割の状況をみたところ、マイナンバー利用事務系と他の領域の分離及びＬＧＷＡＮ接続系とインターネット接続系の分割については、31年3月末現在において全ての市区町村が分離及び分割を行っていた（35、36ページ参照）。

b　マイナンバー利用事務系等の分離及び分割後の領域間通信の状況

223市区町村における領域間通信について、通信内容の種類別及び領域別にみたところ、217市区町村において延べ1,672件の領域間通信が行われていた。そして、マイナンバー利用事務系と他の領域との間の領域間通信の通信制御の状況をみたところ、59市区町村の延べ247件において、通信経路の限定又は通信プロトコルの限定のうち少なくともいずれか一つが行われていない状態で領域間通信が行われていた。このうちマイナンバー利用事務系とインターネット接続系の領域間の通信制御の状況についてみたところ、3市区町村の延べ4件において、通信経路の限定又は通信プロトコルの限定のうち少なくともいずれか一つが行われていない状態で領域間通信が行われていた（36～38ページ参照）。

c　ＬＧＷＡＮ接続系とインターネット接続系との通信経路の分割後のインターネット接続系からＬＧＷＡＮ接続系への無害化通信の状況

会計実地検査時点において、ＬＧＷＡＮ接続系とインターネット接続系の分割が行われている222市区町村について、メール本文及び添付ファイル等の転送又は収受に当たり、強じん性向上事業により整備した機器等により無害化が行われているか確認したところ、メール本文を無害化することなく転送しているのが4市区町村等となっていた。また、添付ファイル等の転送又は収受における無害化の状況についてみると、無害化を行うことなく転送又は収受しているのが49市区町村等となっていた（38～40ページ参照）。

d　ＬＧＷＡＮ接続系とインターネット接続系との通信経路の分割後のＬＧＷＡＮ接続系におけるＯＳの更新プログラム等の適用の状況

上記の222市区町村について、ＬＧＷＡＮ接続系とインターネット接続系の分割前後におけるＬＧＷＡＮ接続系に配置された端末等への更新プログラム等の適用状況を確認したところ、ＬＧＷＡＮ接続系とインターネット接続系の分割後である30年5月末時点において、更新プログラムを適用していないのが、分割前の26市区町村から54市区町村へ、更新データを適用していないのが、分割前の9市区町村から14市区町村へと増加していた。そして、これら54市区町村及び14市区町村の分割前における更新プログラム等の適用頻度についてみると、それぞれ29市区町村及び9市区町村は、分割前には1か月以内の頻度で適用していたのに、分割後に適用を行わなくなっていた（40、41ページ参照）。

(ｳ) 自治体情報セキュリティクラウドによる高度なセキュリティ対策の実施状況等

a　自治体情報セキュリティクラウドへの接続状況

18都道府県が構築した自治体情報セキュリティクラウドへの接続状況をみたところ、会計実地検査時点において、237地方公共団体が自治体情報セキュリティクラウドに接続していた。自治体情報セキュリティクラウドに接続していない4地方公共団体のうち2地方公共団体は、近隣市区町村が別途構築したセキュリティクラウドに接続して共同利用しており、他の2地方公共団体は、31年3月末現在において、自治体情報セキュリティクラウドに接続している（41、42ページ参照）。

b　自治体情報セキュリティクラウドに接続する地方公共団体における監視対象機器等の集約状況等

18都道府県が構築した自治体情報セキュリティクラウドについて、監視対象機器等の集約化のための設備の整備状況をみたところ、外部ＤＮＳサーバについては1都道府県、ＬＧＷＡＮ接続ファイアウォールのログについては8都道府県が、それぞれ集約化のための設備を整備していないなどして、監視対象から除かれていた。また、上記の自治体情報セキュリティクラウドに接続している237地方公共団体について、自治体情報セキュリティクラウドにおける集約及び監視状況をみたところ、Ｗｅｂサーバについては26地方公共団体、外部ＤＮＳサーバについては44地方公共団体、ＬＧＷＡＮ接続ファイアウォールのログについては116地方公共団体において、集約化のための設備が自治体情報セキュリティクラウドに整備されていないなどしていて、集約及び監視が行われていな

かった。そして、各地方公共団体において別途管理されている機器等についての監視の状況をみたところ、「情報セキュリティ専門人材による監視・分析を行っていない」とするのがＷｅｂサーバについては6地方公共団体、外部ＤＮＳサーバについては11地方公共団体、ＬＧＷＡＮ接続ファイウォールのログについては63地方公共団体等となっていた（42～44ページ参照）。

c　自治体情報セキュリティクラウドに接続する地方公共団体におけるインシデント対応体制

上記の237地方公共団体について、不正な通信を行っている端末等のＩＰアドレス等の特定や遮断等の対応が可能かをみたところ、190地方公共団体は端末の特定等の対応の一部又は全部に事業者等の「他の組織の支援等を必要とする要素あり」としていて、このうち70地方公共団体は「全ての端末等について自治体情報セキュリティクラウド側で特定が可能」としているものの、残りの120地方公共団体は、接続している地方公共団体側で端末特定に係る作業を要する状況となっていた。そして、このうち77地方公共団体は「端末等を特定するために事業者等の支援等が必要」としているが、このうち11地方公共団体は支援等を行う事業者等との間で役割の確認を行っていなかったり、役割の確認を踏まえた内容で契約を締結していなかったり、必要な内容で契約が締結されているかの確認を行っていなかったりしていた。

さらに、上記190地方公共団体のうち160地方公共団体は自らにおいてネットワーク遮断を実施することがあるとしていて、このうち129地方公共団体は遮断を実施するために事業者等の支援等を必要としている。しかし、このうち23地方公共団体は支援等に係る役割の確認及びそれを踏まえた契約の締結等を行っていなかった。

インシデント発生時に自治体情報セキュリティクラウドが実施するネットワーク遮断について、遮断の判断主体をみたところ、ネットワークの遮断を判断する際に、接続している地方公共団体側において遮断を判断することとしている12都道府県の自治体情報セキュリティクラウドに接続する160地方公共団体のうち76地方公共団体及び判断主体が決まっていない1都道府県の自治体情報セキュリティクラウドに接続する7地方公共団体のうち5地方公共団体は、遮断の判断に至る手順を策定していないなどしていた（45～47ページ参照）。

(ｴ) 情報セキュリティ対策の実効性を確保するための体制整備等

a　情報セキュリティポリシーの策定及び強じん化に係る改定等の状況

241地方公共団体について、対策基準の策定及び強じん化を踏まえた改定等の取組の状況をみたところ、対策基準を策定していなかったものは3地方公共団体、強じん化を踏まえた規定がないとしているのが178地方公共団体となっていた。そして、30年11月末時点の対策基準の改定の予定については、178地方公共団体のうち40地方公共団体が未定としていた（47、48ページ参照）。

b　強じん性向上事業実施後のセキュリティリスクへの組織的な対応

241地方公共団体のインシデント発生時における対応体制の整備等の状況をみたところ、ＣＳＩＲＴを設置していたのは130地方公共団体（241地方公共団体に占める割合53.9％）となっていて、このうち16地方公共団体では、ＣＳＩＲＴの要員及び機能について文書化していなかったり、37地方公共団体では緊急時対応計画を策定していなかったり、49地方公共団体ではインシデント発生時に国及び庁内ＣＩＳＯ等へ一斉同報する連絡ルートを構築していなかったりしていた。

緊急時対応計画における標的型攻撃に対応する内容の規定の整備状況及び緊急時対応訓練の実施状況をみたところ、緊急時対応計画において標的型攻撃に対応した内容を規定しているとしたのは66地方公共団体（同27.3％）、緊急時対応訓練を実施したのは54地方公共団体（同22.4％）、いずれも実施していたのは28地方公共団体（同11.6％）にとどまっていた（48～50ページ参照）。

ウ　支援ＰＦの利活用の状況

(ｱ) 支援ＰＦへの情報の登録等の状況

27年9月から30年5月までの2年9か月に、支援ＰＦに登録されたインシデント関連掲示板機能については、情報の総登録件数は45件となっていた。Ｑ＆Ａ機能については、問合せの総登録件数は32件で、29年2月以降は3件にとどまっていた。ワーキンググループ機能については、情報の総登録件数は、3件掲載されたのみとなっていて、27年11月以降は情報の登録はなかった。その他関連情報機能については、情報の総登録件数は41件で、29年6月以降は情報の登録はなかった。自治体の掲示板機能については、当該機能が追加された28年3月以降、質問の投稿が全くなかった。また、支援ＰＦの利用等の状況について、支援ＰＦにアクセスした個

別のユーザーの月ごとの数を確認したところ、28年11月以降は毎月100ユーザー未満にとどまっていた（51～53ページ参照）。

(ｲ) 支援ＰＦの利用等の状況

241地方公共団体に支援ＰＦの利用状況を確認したところ、68地方公共団体は、会計実地検査の時点まで「支援ＰＦの存在を知らなかった」としており、全く利用していなかった。また、「支援ＰＦの存在を知っていた」とする173地方公共団体の利用状況を確認したところ、「ほとんど利用していない（利用頻度が3か月に1回程度未満）」とするものが49地方公共団体（241地方公共団体に占める割合20.3％）、「ログインが初回実績のみ」とするものが37地方公共団体（同15.3％）、「全く利用したことがない」とするものが74地方公共団体（同30.7％）となっていた（53～56ページ参照）。

(2) 所見

基本法において、国は、サイバーセキュリティに対する脅威の深刻化等に伴い、サイバーセキュリティの確保に関する総合的な施策を策定し、及び実施する責務を有するとされており、地方公共団体は、国との適切な役割分担を踏まえて、サイバーセキュリティに関する自主的な施策を策定し、及び実施する責務を有するとされている。

また、マイナンバー制度の施行に伴い、国と地方公共団体等の各機関の特定個人情報等を取り扱う情報システムが相互に接続されたことで、マイナンバー利用事務を行う地方公共団体の情報セキュリティ対策は、公的機関全体にとってますます重要な課題となっており、政府としても必要な支援を実施していくことになっている。

ついては、総務省において、地方公共団体における情報セキュリティ対策について、今後、次の点に留意して取り組んでいく必要がある。

ア　地方公共団体における情報セキュリティ対策の強化等

(ｱ) マイナンバー利用端末への二要素認証等の導入について、二要素認証等の導入状況を十分に把握するとともに、マイナンバー利用端末の二要素認証等の運用について、補助事業実施後の状況を十分に把握した上で、望ましくない運用方法を具体的に示すなどして、特定個人情報の情報漏えいなどのリスクがより低減されるよう、地方公共団体に対して助言を行うこと

(ｲ) マイナンバー利用事務系と他の領域との分離及びＬＧＷＡＮ接続系とインターネット接続系との分割について、分離及び分割後に行われる場合がある領域間通

信において、本来意図しない通信やマイナンバー利用事務系等へのコンピュータウイルスの感染を防止するための方策を改めて明示するなどして、特定個人情報の情報漏えいなどのリスクがより低減されるよう、地方公共団体に対して助言を行うこと

(ｳ) 自治体情報セキュリティクラウドによる高度なセキュリティ対策について、補助事業実施後の状況を十分把握した上で、監視・分析の必要な機器等が都道府県にできる限り集約されるなどして専門人材による監視・分析が行われるよう、また、自治体情報セキュリティクラウドに接続する地方公共団体に対して、そのネットワーク遮断等を支援する事業者等と役割の確認をすることの必要性を明示するなどして、インシデント発生時に適切にネットワークを遮断することなどができるよう、必要に応じて地方公共団体に対して助言を行うこと

(ｴ) 補助事業で強化された情報セキュリティ対策の実効性を確保するために、強じん化を踏まえた対策基準の見直しや、インシデント発生時の体制整備等に係る緊急時対応計画の策定、連絡体制の構築等について、必要に応じて地方公共団体に対して助言を行うこと

イ　地方公共団体に対する情報セキュリティ等に係る支援等

支援ＰＦが地方公共団体における情報セキュリティ対策向上に寄与するよう、支援ＰＦの機能及び利活用の方法等について地方公共団体へ重ねて周知するとともに、支援の需要を把握して、支援ＰＦが提供する情報や機能の見直しなどについて検討すること

会計検査院としては、サイバーセキュリティに対する脅威が深刻化する中で、マイナンバー制度において情報連携が行われている情報システムの情報セキュリティ対策の実施状況等について、今後とも引き続き注視していくこととする。