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

1　検査の背景

サイバーセキュリティ基本法によれば、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、個人番号(注1)(以下「マイナンバー」)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」)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などとされている。

地方公共団体等の情報システムにおいて、平成28年1月からマイナンバー利用事務が実施され、29年11月から情報提供ネットワークシステム等を通じて特定個人情報(マイナンバーをその内容に含む個人情報)の照会及び提供である情報連携が行われており、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(注3)がそれぞれ改修されて活用されている。

27年5月に、日本年金機構が外部から標的型攻撃(注4)を受けて、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が発生した。

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、同年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」)を設置している。

検討チームは、同年8月に中間報告(以下「8月報告」)を取りまとめて、組織体制の再検討等の3項目について総務省に提言している。そして、同年11月に、次の①から③までの三層から成る対策(以下「三層の構え」)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」)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端末からの情報持出し不可設定(これらを「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

②　LGWAN接続系とインターネット接続系の分割

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」)と、Web閲覧やインターネットメール等のシステム(以下「インターネット接続系」)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

総務省は、11月報告を受けて、各地方公共団体に対して同年12月に通知を発し、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、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1/2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。そして、平成27年度補正予算に強化対策費補助金として254億9859万円が計上され、その交付額は、46都道府県及び1,727市区町村の計1,773地方公共団体に対し計233億4588万円となっていた。強

化対策費補助金は、「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」)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」)に要する経費を補助の対象としており、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、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。

強じん性向上事業は、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り、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いる。また、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事業である。

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、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ることなどができる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」)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。また、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。

(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

(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

(注4)　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

2　検査の着眼点

本院は、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、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。

3　検査の状況

(1) 強化対策費補助金の交付状況

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、このうち10都道府県は強じん性向上事業にも交付を受けていた。また、223市区町村の全てが強じん性向上事業を実施し、このうち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。

(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

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

マイナンバー利用事務系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の状況をみたところ、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。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、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市区町村のうち、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、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が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。

マイナンバー利用事務系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をみたところ、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。

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解除する運用を行っているものが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。上記の62市区町村及び27市区町村の純計87市区町村について、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、44市区町村では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としており、情報を持ち出す際の持出物等の記録については、77市区町村が記録していないとしていた。さらに、81市区町村は暗号化の実施を職員が任意で行っており、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。

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

223市区町村の領域間で行われている通信(以下「領域間通信」)についてみたところ、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において、通信経路の限定又は通信プロトコルの限定(注5)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おり、このうち3市区町村の延べ4件はマイナンバー利用事務系とインターネット接続系との間の領域間通信となっていた。

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、無害化することなくメール本文を転送しているのが4市区町村等、添付ファイル等を転送又は収受しているのが49市区町村等となっていた。

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、30年5月末時点で、更新プログラムを適用していないのが26市区町村から54市区町村へ、ウイルス対策ソフトの更新データを適用していないのが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。

(注5)　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

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

自治体情報セキュリティクラウドにおける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(注6)について1都道府県で集約化のための設備を整備していないなどしていた。また、自治体情報セキュリティクラウドへ接続している237地方公共団体のうち、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地方公共団体で集約及び監視が行われていないなどしていた。そして、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「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サーバにおける6地方公共団体等となっていた。

また、自治体情報セキュリティクラウドがインシデント発生を検知した際、「端末等を特定するために事業者等の支援等が必要」とする77地方公共団体のうち11地方公共団体は支援等を行う事業者等との間での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いなどしていた。

(注6)　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

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

情報セキュリティ対策基準(以下「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等をみたところ、対策基準を策定していなかったものが3地方公共団体、30年11月末時点で強じん化を踏まえた対策基準の改定の予定を未定としていたものが40地方公共団体となっていた。

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(注7)を設置した130地方公共団体のうち16地方公共団体はCSIRTの要員及び機能について文書化していないなどしていた。また、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、緊急時対応訓練を実施したのは28地方公共団体にとどまっていた。

(注7)　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

オ　支援PFの利活用の状況

支援PFに登録された情報の登録件数は、インシデント関連の掲示板機能が45件となっていて、自治体の掲示板機能については、質問の投稿が全くないなどとなっていた。また、利用等の状況を確認したところ、28年11月以降は毎月100ユーザー未満にとどまっており、68地方公共団体は「支援PFの存在を知らなかった」とし、「支援PFの存在を知っていた」地方公共団体でも「全く利用したことがない」とするものが74地方公共団体となっていた。

4　所見

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。

(1) 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状況を十分に把握するとともに、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　領域間通信において、本来意図しない通信や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　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、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、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

(2) 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が情報セキュリティ対策向上に寄与するよう、地方公共団体へ重ねて周知するとともに、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

本院としては、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。