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改定等に係る検討会（第10回）

開催日時：令和５年 12 月 19 日（火）10:15～11:45
開催場所：オンライン会議
議　　事：
１．各検討項目の改定方針
２．NISC 政府統一基準（令和５年度）の改定に係る対応について

○：構成員　●：総務省（事務局）

１．各検討項目の改定方針

＜機密性分類＞

○　通常は、個人情報で「機微な」という表現を用いた場合、個人情報保護法の要配慮個人情報を想起することが多いと思う。機密性３B の例として想定しているものは、要配慮個人情報の話ではなくて、「マイナンバー利用事務系の住民情報を束ねたリスト」というような形であり、「機微な」について、あまり重視はされていないような気がする。この点、事務局の方で「機微な」ということと、要配慮個人情報との関係について、どのような関係を想定しているのか伺いたい。

●　ご指摘の通り、基本的にマイナンバー利用事務系で扱われる情報を想定している。なぜ、要配慮個人情報ではなく、マイナンバー利用事務系で扱う情報を想定したかというと、これは自治体の実務に沿ってということになる。マイナンバー利用事務系のところ、ここは番号法にかかってくるところであるため、一段上に上げて実務に沿った形で定義している。
●「機微な」という言葉は避けて、書き方を見直せればと思う。

○　「機微な」は取った方が逆に誤解を招かずにいいと思う。

○　個人情報保護法に関しては「機微な」と言うのは要配慮個人情報を想起させる。
○　一方で、これまで運用されていた個人情報保護条例のうち、多くの個人情報保護条例では「機微な」という言葉を定義しているケースが少なからずあり、この場合、「機微な」に関していくつかの定義があり、よく言われていたのは、いわゆる差別の原因になる個人情報および思想信条の自由にかかる個人情報と言うような括りであるため、誤解を招かないようにするためにも、「機微な」を取った方がいいと強く思う。
○　マイナンバー利用事務系に置く、置かないというのは、歴史的経緯があり、一般的には住基システムに直結する必要があるシステムといったシステム上の都合で置かれてきた。この辺は実際実務に近い構成員の方々にご意見いただければと思う。
○　また、マイナンバー利用事務系の「住民情報」とは何を指すのか、やや定義の揺らぎが生じてくるのではないかと疑問に思っている。また「束ねたリスト」という言い方と、いわゆる

個人情報ファイルとの関係性というのもクリアではない。個人情報ファイルだと言い切って書いてしまってもよいと思う。あるいは、散在情報ではないことを明確にするのであれば、そのように書いた方がよいと思う。

○　「職員としての属性に基づく個人情報」について気になっている。人給システムには、職員の個人情報の中に特定個人情報も含まれている。マイナンバーの観点と職員としての属性からの観点のどちらを優先するのか考え方を整理した方がよいと思う。

● 資料１にあるように、現行のガイドラインで規定されているβ’モデルでは、職員のマイナンバー情報については、必要なセキュリティ対策を課すことを前提にインターネット接続に置いてもよいとしており、実際、人事給与システムをインターネット接続に置いているβ’モデル採用自治体も存在する。

● したがって、特定個人情報を番号法にあわせて機密性３Ｂにしてしまうと、実務上、支障が生じるため、職員の属性に基づく個人情報は機密性３Ｃに設定している。

● ご指摘の通り、用語の定義については、個人情報保護法の定義を鑑みて整理する必要があると認識。

● 情報資産の例示については、自治体の実務に詳しい構成員の方々から意見を伺えればと思う。

○　旧のホストコンピューターで行われていた業務がマイナンバー利用事務系に含まれている。

○　基本的には住基システムに紐づく業務システムがマイナンバー利用事務系になると思うが、自治体によっては、マイナンバー利用事務系ではなくLGWAN接続系で業務を行っているものもあるため、マイナンバー利用事務系の情報は機密性３Bが主体であるということを明確にし、機密性３Bはマイナンバー利用事務系の情報のみが該当すると誤解されないように表現を考えた方がよいと思う。

○　自治体の現場からという話ですが、マイナンバー利用事務系というのは三層分離の時の表現。当時はマイナンバー制度が始まろうとしている時で、ホストコンピューターを使った自治体もかなり多く、基幹系業務という形で住民登録等の業務を中心にマイナンバー利用事務系が使用されていた。

○　機密性３Ｂの情報をクラウドサービス上に乗せるという観点によって、機密性が担保出来ているサービスでなければまずいと思う。

○　ISMAPに登録されているサービスの中には、一般に広く公開するようなシステムを構築できるものもあり、そのようなサービスに機密性３Ｂの情報を乗せることで、利用形態によっては機密性３Ｂの情報がインターネットに公開されてしまうシステムを構築することが出来てしまう。その配慮が必要だということを検討し述べさせて頂く。

● 住民の情報が公開するのが前提で構築されるシステムの例があるため、ISMAPに登録されているため利用可能ということではなく、セキュリティ対策も併せて規定するという趣旨と認識した。

○　ISMAP に登録されているサービスの中には、利用方法によっては情報漏えいに繋がる可能性のあるものもある。ISMAP の登録だけではなく、当該サービスがどのような管理策を取っているかまで確認しないと安全性が確認できないのではないかと思っている。
○　自治体によっては、いわゆる住民情報として集めているマイナンバー利用事務に関する情報を、機密性３Ｂとしてマイナンバー利用事務系に配置していて、マイナンバー関係事務に関しては、機密性３Ｃとしてインターネット接続系に、暗号化などの対策を行い、データを配置している。
○　機密性３Ｃに関しては、ファイルサーバ等に市民から集めた一部の個人情報を置くことがあるため、システム化されていないファイルサーバであっても暗号化やアクセス制御が徹底されていれば、住民情報を含んだファイルをインターネット接続系に配置しても良い、という表現があると望ましいと思う。

●　ISMAP に登録されているだけでは不十分であり、その管理策まで確認する必要があるということや、アクセス制御や暗号化も重要であり、システムに保存されていなくても暗号化等のセキュリティ対策をとれていれば、機密性３Ｃであってもインターネット接続へ配置可能であるというルールが望ましく、現実的だという意見だと認識。
●　事例として受け止めて、引き続き検討させていただきたいと思う。

○　機密性３Ｃに関して、情報資産の例示の中に、住民本人から同意を得て収集している個人情報と太字で記載があるが、法令で認められていれば住民本人からの同意を得ずに、個人情報を収集、取得することができる。何か理由があって、この住民本人からの同意を得て収集しているという限定が付けられているのか。

●　個人情報保護法との整理が必要と認識。
●　オンラインの施設の予約システムなどにおいて、住民に個人情報を入力してもらう際に、入力フォームにおいて同意を得る等の場面を想定している。ご指摘の通り、個人情報保護法の中で同意を得ずに集めることもできるような情報がある中で、例示の記載が混乱を生じさせる恐れがあるため、機密性３Ｃの例示は見直す。

○　機密性３Ｂと機密性３Ｃの差別化を図るために、個人情報の中で「３Ｂ以外の」と明記すると、混乱を避けられるのではないかと思う。

○チャットのところにいくつか、コメントが書いてあるので、こちらも見ていただきたい。

＜情報システムの品質管理＞
○　ガイドラインの契約不適合責任に関する新しい追記は、法務のリソースが充実している自治体では、当然押さえた上でベンダーと協議し、然るべき契約条件を定めているため、必要性はさほど高くないと思う。他方、小規模自治体には法務のリソースが少ないところが多く、ベンダーが作成した契約ひな型にそのまま同意することが多々あり、その結果、問題が生じた時に権利行使ができず泣き寝入りということが報告されている。そのため、そういった自

治体が契約条件の検討の参考に供するために契約不適合責任に関するデフォルトルールである民法上の要件を記載しているほか、経産省・IPA 作成のひな型案の規定についての情報も記載したものと理解できる。

○　技術的セキュリティに関する解説に係るガイドラインの改定の方向性について、「個人情報漏えい防止の観点」と記載があるが、個人情報に限定すると誤解を招く恐れがある。

●ご指摘を踏まえ、「機密性の高い情報の漏えいを防止する観点」に修正する。

○　コンビニ交付のトラブルにおける業務委託あるいはソフトウェア調達の対応は、観点が情報漏えいだけではないと思う。
○　また対策基準の内容がスクラッチ（個別開発）を想定した記載と読み取れるが、パッケージ利用を前提とした場合の考慮も必要である。
○　パッケージであれば、他団体でも使用実績があり、中身まで細かく調べないので済まされているケースが多いかと思う。

●　ガイドラインの中で、個別のパッケージに必要な対策を記載するのは、公平性の観点や検証に係る時間やコストの観点から難しい。ただ、自治体にとって、パッケージ製品の詳細を１つ１つ調べて安全性やリスクを全部検証して導入するのは難しいという実態は理解した。
●　パッケージソフトの調達時のリスクや不具合、留意点として加筆する対応はありうるかと思う。

＜マイナンバー利用系と他の領域との画面転送の検討＞
○リスク観点の接続要件の中に特定通信とあるが、特定通信の定義が一応なされたことは良いことだと思うが、特定通信の定義が緩すぎると思う。
○また IP アドレスの限定かつポート番号のみで通信制限をしていいのか、という話にもなり、IP アドレスの限定かつポート番号の限定だけでいいように読めてしまうことが気になる。
○MAC アドレス（レイヤー２）で制御するケースは無いように思うため、記載を削った方がいいと思う。

●　現行のガイドラインの記載を採用しているが、おっしゃる通り、確かに特定通信は、最低限必要なもので、十分条件ではないことを、誤解を与えないように留意する。

○　レイヤー４までしか想定していないような書きぶりであり、その上位レイヤーも想定した内容とした方がよい。「とにかく特定通信さえすればよい」とならないようご注意いただきたい。

○　β’モデルを採用した自治体ではマイナンバー利用事務系との通信を必要としないのではないか。リスクアセスメントの前にニーズがあるか調べた方がよいと思う。
○　また観点４は、リスクアセスメントに関する観点というよりは、どのような運用であれば問

題ないか検討していただければと思う。

● β’モデルとマイナンバー利用事務系との通信について、詳細な調査は実施していないが、ニーズがあることを把握している。リスクアセスメントのパターン等について、構成の皆様との間でご意見をいただければと考えている。
● リスクアセスメントのプロセス自体は、総務省も事務方で技術的な知見が不足していることもあり、例えば来年度のガイドラインの改定に係る事業者をシステム的な知見のある事業者にご協力を得てということを想定している。

２．NISC 政府統一基準（令和５年度）の改定に係る対応について

○ 政府統一基準では、ソフトウェアに限らず、機器を対象として情報システムの構成要素の中にサーバ装置端末、通信回線装置に複合機、特定機器等などを含めての総称を言うというような定義になっている。ハードウェアに脆弱性や悪意ある仕様になっている場合もあるので、それらを含めて 23 ページで選定基準としている点は賛成する。
○ それに伴い、23 ページの標題も「ソフトウェア利用時の対策強化」ではなく、「機器等利用時の対策の強化」と、より幅広にしたほうがより適合的になるのではないかと考えるので、検討いただきたい。

● ご指摘を踏まえ、表題を修正させていただく。

● 本日いただいた皆様からの意見、特に機密性に係る部分をもう一度整理し、ご提示させていただき、意見をいただければと思う。

○ 意見については、メール等でも是非ご連絡いただければと思う。
○ 本日の会議はこれにて終了とさせていただく。

以上