第１回　地方公共団体における情報セキュリティ対策の向上に関する研究会
議事概要

１．　開催日時：平成 26 年 10 月 6 日（月）15：00 ～ 17：00

２．　開催場所：ＮＥＣ本社ビル　2Ｆ　242 会議室

３．　出席者

＜座長＞

佐々木良一（東京電機大学未来科学部教授）

＜構成員＞

今井　建彦（仙台市まちづくり政策局情報政策部長）
大木 榮二郎（工学院大学常務理事・情報学部教授）
大高　利夫（藤沢市総務部参事兼ＩＴ推進課長）
高橋　邦夫（豊島区政策経営部情報管理課長）

＜オブザーバ＞

石川 家継（地方公共団体情報システム機構情報化戦略部次長）

＜事務局＞

増田　直樹（総務省自治行政局地域情報政策室長）
須藤　正喜（総務省自治行政局地域情報政策室課長補佐）
大井　芳泰（総務省自治行政局地域情報政策室係長）
日本電気株式会社

４．議題

・地方公共団体における情報セキュリティ対策の向上に関する調査研究について
・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について

《外部委託（クラウド）について》

○　資料２－１の６ページに自治体によるデータセンターの立ち入り検査できることとの記載があり、それが出来ればある程度監査できると考える。ただし、サービス利用のような形態の場合、立ち入り検査は出来ないが、外部監査を受けているためよいという整理もあると考える。何を持ってよしとするかを決める必要がある。

○　サービス利用の形態の場合、委託元がガバナンスを利かせることは難しいため「外部委託」として取り扱うことは確かに違和感を感じるが、機密情報を取り扱う基幹系のクラウドがプライベートクラウド的なものということであれば、「外部委託」として取り扱うことも納得できる。ただし、プライベートクラウド的なクラウドと、それ以外については明確に分けた方が分かりやすい。

○　データセンターに自治体が行けるのかという点や、個人情報保護審議会でチェックできるのかという点が課題と考える。やはり基幹系のシステム、特に住民記録や税といったシステムをクラウドに預ける場合は、それなりのチェックができることが望ましい。ただし、それが行き過ぎとなりクラウドが進まないのも問題なので、それ以外はどこまで許されるのかというところは整理した方がよい。

○　立ち入り検査が不可であったとしても、第三者委員会などを設置して、そこが立ち入り検査しているから大丈夫だという仕組みがあればよいと思う。全ての外部サービスを自治体が立ち入り検査するというのは現実の運用上難しいものがあるため、第三者委員会が監査をしっかりしているという説明ができるのが望ましい。

○　J-LIS 等がどこのクラウドサービスであれば大丈夫というものを紹介したり認証制度等を利用するのが現実的ではないかと感じる。

《外部委託（サプライチェーンリスク・委託先管理）について》

○　サプライチェーンのリスクを自治体としてどこまで検討しなくてはならないのか疑問である。現実問題として外部委託先のさらに再委託先のコントロールは難しいのではないか。

○　調達仕様書に盛り込むべき委託先への要求事項を提案してはどうか。それを調達の際に利用する方が現実的である。

《ネットワークの利用・支給以外のスマートデバイスの業務利用について》

○　クラウドを利用する上でもインターネット上のＶＰＮでよいのか、専用回線がよいのか、その場合コストがネックになるという課題もあるので、どのレベル感であればどの回線がよいという基準があるとよいのではないか。

○　専用回線でも多くの攻撃方法があるため、そういう意味では安全性はインターネットＶＰＮでも専用回線でも同じくらいクリアできるものでなくてはならない。

○　業務利用にリモートアクセスを認めるかどうかは重要な問題と考える。私物の端末でリモートアクセスを認めるのは危険。私物利用を認めるとすれば仕様を厳しく固める必要があるが、そのようにすれば今度は私物が私物として利用しづらくなると思われる。

○　テレワークで使う端末は支給にするほうが良い。その方が運用もしやすいし安全性も高くなる。

○　新しい技術を否定するポリシーガイドラインはよくないと思うので、条件を満たせばリモートアクセスなどの新しい仕組みを使ってもかまわない程度のスタンスが良い。

○　職員全員に端末を支給するのではなく自分で管理して使える人に限定して支給すべき。

○　リモートアクセスによる個人情報などが入った基幹系のデータへのアクセスについては、物理的にアクセスできないよう分けているところもあるが、ルーティングでのみアクセスをコントロールしている場合もある。

○　私物パソコン等の端末持ち込みについて、現在のポリシーガイドラインは守れないルールになっている。本当はレベルを分けて対応できる方がよい。例えばスマートフォンの持ち込みを一律禁止しても守れないが、サーバー室への持ち込み禁止や撮影禁止等のルールであれば守れるだろう。

《SMS 業務利用について》

○　ツイッターの炎上防止マニュアルを作成する等の対策はとっている。利用時のルールを定め、職員啓発をすることが重要。

○　防災情報等の一方的に発言する性質のものと、観光や産業振興などくだけた形で盛り上がる必要があるものがあるので、注意することが大事である。

《情報セキュリティインシデント対策体制の強化について》

○　CSIRT の定義を明確にするとよい。CSIRT を作ることで具体的な対応策が分からない場合でも、周りの職員と相談できたり、他の CSIRT から情報をもらったりして、理解を深めていくことができると考える。

○　自治体内部でも情報システム部門が教育員会などの組織とは別れている場合もあるので、どこで問題を受けるのかの窓口を作ることは情報共有するために意味はあると思う。

○　名称にはこだわらないが、CISO や CSIRT がどのような機能をもち、役割を担うのかは明確にする必要がある。例えばインシデントが発生したときに何をすべきか（どのようなルートで警察に通報し、記者発表をするのか等）を明確にしておくべきである。

○　CIO と CISO は同じ人物が兼務してもいいと思う。ただし、その下に CIO の役割を担う人、CISO の役割を担う人が存在する必要がある。

《監査ガイドラインについて》

○　ISO27001 は既に ISO19011 を受けて改正されているため、ISO27001 としてどのような改正をしたのかということに着目してはどうか。

○　ISO27001 の変更点を中心に情報セキュリティポリシーガイドラインを見直すということはよいが、その場合 ISO27001 がきちんと ISO19011 をカバーしきれているかは念のため確認しておいた方がよい。

○　地方自治情報管理概要にて、監査の取組みが進んでいるか進んでいないかある程度確認できるため、その結果をもっと生かしていくべき。

○　監査のガイドラインはいい資料ではあるがあまり使われていない。どう使ってもらうかも含めて考える必要がある。
○　J-LIS から LGWAN 上にて監査の方法を示したものを自治体に提供されている。

○　民間企業においても監査の質が落ちているということを漏れ聞くことがあるので、監査がどの程度きちんと実施されているか心配である。

《その他》
○　小さい自治体を配慮した情報セキュリティポリシーにして欲しい。そのためにも J-LIS のサポートなど体制をしっかり整えて欲しい。