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11回）

議事概要　要旨版

開催日時：令和６年２月１日（木）13:15～15:00

開催場所：オンライン会議

議　　事：

１.LGWAN 接続系のローカルブレイクアウト（α’モデル）の検討について

○：構成員　●：総務省（事務局）

１.LGWAN 接続系のローカルブレイクアウト（α’モデル）の検討について

○マルウェア対策ソフトの定義として、「パターンマッチング方式、不審な動作を行うことが含まれていることを検出するヒューリスティック方式を行う」と書かれているが、「及び」なのか「または」なのかを明確にしていただきたい。自治体間には知識の差があり、両方やらなければならないのか否かというようなところを明確化しておいた方が、後からトラブルが少ないと思われる。

○マルウェア対策ソフトは、検知方式で性能が決まるというよりは、他の様々な要因で性能が決まるところがあり、どの製品であれば問題ないのかという判断がとても難しい製品である。現状、Windows 標準でマルウェア対策をできてしまうということもあり、マルウェア対策というものであればいいのか等、言葉尻だけを取られないよう書きぶりには注意をした方が良いかと思う。

○資料の、いわゆる三層分離の図において、分割（無害化通信）はファイアウォールを通じて LGWAN 接続系とインターネット接続系は繋がっているかのような書き方をしている。現実は、繋がらないというのが大前提であり、無害化通信については、通信というより単にファイルの授受が最初の話だったはずである。この絵の描き方だと限定通信であれば通信してもいいというふうに見えてしまう。一方、マイナンバー利用事務系と LGWAN 接続系間では限定通信している場合があり、インターネット接続系と LGWAN 接続系の壁より低いイメージを持ちかねない。そのため、図を公表する場合には書き方には気をつけた方が良いと思う。

○インシデントが発生した際自治体の責任になるということを改めて留意する必要がある。このように多量なセキュリティ対策をガイドラインに規定すると、自治体にとっては、全部解釈しきれないだろうということが心配される。「業者が対応」する際でも問題が起きたら「自治体の責任である」と記載していると思われるが、自治体側が業者に頼んだ時点、クラウドに頼んだ時点、あるいは自治体ガイドラインや ISMAP に載っている時点で手離れしてしまうようなことになりかねないと非常に危惧している。難しい話であればあるほど、最終的な判断が自治体側ではできないため、「我々の責任ではない」と言われないよう、折にふれて強調していくような資料、あるいはガイドラインの構成にしておかなければならないと思う。

●一部資料は、LGWAN 接続系の攻撃ルートが判明してしまうため、非公表としている。構成員の

ご指摘を踏まえると、資料１にはLGWAN接続系とインターネット接続系の間は分割、マイナンバー利用事務系とLGWAN接続系の間は分離という境界を作るような形で3パターンの模式図の方を用意している。資料1に載っている図をガイドラインの改定案に反映させるため、構成員のご懸念については払拭されると思う。

●自治体の責任になるということを改めて留意する必要については、非常に重要な観点だと思う。ガイドライン36ページにも記載しており、特に今回のα´では、設定を事業者に依頼するというところはあるため、まず契約で担保することを記載しており、その前段に、基本的な考え方ということで、「自らが責任を持ってセキュリティを確保するべきもの」ということを改めて認識すべきである。インシデントが発生した場合は、「保有する情報資産を守る立場にあり、セキュリティ確保の責務も有する地方公共団体が責任を負うことになる」ことを改めて理解する形にしている。

●構成員からあったヒューリスティック方式については、IPAのガイドラインから持ってきており、そのまま使っているが、地方公共団体の今回改定するガイドラインでは、振舞い検知や不審な行動等の言葉に置き換え、分かりやすい表現にする。「または」なのか「且つ」なのかについても注意したいと思う。

○LGWAN接続系からα´モデルとしてローカルブレイクアウトを想定したケースと、インターネット接続系からβ´モデルを比較してもらったが、すべての関係において確実に設定され、かつ対策が充分であれば、このような結果になるのだろうと思っている。

○インターネット接続において三層の分離をした時に、セキュリティクラウドという都道府県単位で設置した機能というものは、すべての自治体がやりきれないであろうことや、色々なセキュリティの状態効果を考えると非常に効果があったと評価できたと思う。

○α´モデルの１番の問題は、セキュリティクラウドをないがしろにしているという思いが若干あり、そこで担保していたものを「自治体の責任においてセキュリティ対策を施す」というところで、やはり自治体に降りかかってくるのだなというところが大きい。セキュリティクラウドの今後や考え方をどのようにするのかが、今回は課題として投げられたという風に感じている。

●リスクアセスメントで定量的な評価を踏まえての対策を提示しているが、おっしゃるように本来は、セキュリティクラウドでインターネット接続口を１つにするというところから例外的な状況を作っている形になっている。今までセキュリティクラウドで担ってきた、インターネットに対するセキュリティの機能について、今回のα’のように、サービス側の変更により、利便性の不都合を生じ、自治体側で勝手にブレイクアウトしてしまう、という現状があるのをどうようにしていくかが重要。今後の話になるが、セキュリティクラウドをどう見直していくか、という議論も含め、担当としては、また検討会で議論させていただきたいと考えている。

○アセスメントをやったように、どのような対策を確実に実施しなければならないのかを、βモデルβ´モデルのように明確にする必要があると思う。

○マルウェア対策ソフトが必須となっているが、その場合、マルウェア対策ソフトもその会社それぞれの製品によって良し悪しがあると思う。一定のセキュリティの認証をパスしたようなソフトを使うということを義務付けることなのか、そこまでは求めないのか、この点について、リスクアセスメントの元になっている IPA のセキュリティリスク分析ガイドではどのように言っているのか、また、国際的なサイバーセキュリティの水準からするとどうなのか、という言った点は如何か。

●マルウェア対策ソフトに関しては、過去にベンダー等とも議論をしている。結果、99.9%の検知・0.1%程度誤検知があり、その中でそれぞれのベンダーで違いがあると言うことを議論しても、意味がないという話になっている。パターンマッチングだけでは、機能として十分ではないと認識されており、振舞い検知等の機能が充実してきている。ひとまず、今の世の中で一般的に使われているものを入れていただくことを想定している。

○今回のアセスメントの元にした IPA の分析ガイドラインでは、そういった特定の認証をパスしたソフトである必要がある、ということまでは求めていないのか。

●ご認識のとおり。

○マルウェア対策だけではなくてパッチ適用等が必須となっている。例えばパッチ適用において、パソコンは適用しているが、ネットワーク機器は未適用という部分が散見されている。この辺りをきちんと自治体に分かりやすく周知していただくためにも、具体的な製品名を出すわけにはいかないかもしれないが、運用の中で組み込んでいく旨も出していただけるとありがたいと思う。

○「外部の指摘を踏まえて J-LIS に報告する」というのが、資料１のガイドラインの改定案の中にあるが、現在、例えばβ、β´の自治体はこれを対応できているのか、総務省や J-LIS が確認する方法というのが確立されているのか、発出するにあたり、今一度、整理し直すとよいのではないかと思う。

●正確な数字は出てこないが、β´の団体が多いので、β´の方は監査を受けたらその都度 J-LIS に提出しているということを事実として把握している。事実上は J-LIS 側や総務省側のマンパワーもあり、β´の団体における監査の有無、J-LIS への監査報告書提出の有無をフォローできていない状態である。監査の趣旨がそもそも LGWAN に影響を与えないようにするための措置ではあるため、丁寧に自治体に対してお願いしていくしかないと思う。J-LIS とも必要な調整を実施する。

○今回のリスクアセスメント非常に意欲的にやっていただいた。普通のやり方だと、資産ベースで広くやり、その中で重要なところを事業被害ベースでやるが、今回は資産ベースのところを非常に精緻にやり、事業被害ベースで作るシーケンスをあらかじめリストアップしたため、おそらく資産ベースだけでやれたのかなと思っている。

○必要な対策を必須にするか、それとも推奨にするかは難しいと感じており、リスクだけではなくて、コストや使い勝手等が入ってくるため、使い勝手、コスト、リスクのバランスをとるということについて、今後も検討していかなければならないだろうと思う。今後、マイナンバー利用事務系に対する画面転送の時に、使い勝手とリスクとのバランスが非常に重要になってくるため、引き続き総務省にて認識を持って重要視していただければと思う。

●ご指摘の通り、使い勝手とかコストの観点は重視しないと、結局、利便性を重視して抜け道が作られやすくなってしまうので、知見のある事業者の力を借りながら、来年度以降、リスクアセスメント実施の際に、先生のご指摘を踏まえて取り組んでいく。

○資料１のガイドライン改定案の右列に接続先のクラウドサービスにおける設定に誤りがないか、定期的な確認を行うことが必要と書いてあるが、ご存知の通り定期的な確認のみでは足りない。アップデートに伴う仕様変更との間で齟齬ができ大騒ぎになったことがあったので、その点も明記をできればしておいていただけたらありがたい。

●追加して反映する。

○外部監査の実施について、適正に外部監査を実施するため、「地方公共団体における情報セキュリティ監査に関するガイドライン」の「監査人の実績等」に具体的な資格を明記すべきと思う。特に監査メンバーについてはより具体的なものが望ましい。

●ご指摘を踏まえて整理し、周知する際に留意する。

●次回が今年度最後の検討会になる。

以上