

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8回）

日 時：令和5年2月21日（火）10:00～11:15

形 式：オンライン会議

議 事：

1. 「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」の改定案について
2. 今後の地方公共団体の情報セキュリティ対策に係る検討事項について

○：構成員 ●：総務省（事務局） ■：J-LIS

1. 「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」の改定案について

○ガイドラインの改定と公表は3月末を予定しているとのことだが、その後のスケジュールは、どのように想定しているか。標準化対応など地方公共団体において、優先度が付けづらい状況になっていると感じている。今後の見通しのようなものがあると地方公共団体にとって良いのではないか。

●4月以降、地方公共団体向けに今回の改定に係るポイント等を説明する予定である。また、今後は、年に一度のガイドラインの改定を想定しているが、できる限り事前に改定の方向性を地方公共団体に示すことを検討していきたい。

○資料2の「iii-46」の記載について、図では、ローカルブレイクアウトが、セキュリティクラウドから分岐するように表現されているが、実際は地方公共団体のファイアウォールから分岐するイメージであると考えている。この記載では、通信の安全性を確保した上で、可用性を優先するというローカルブレイクアウトの趣旨とずれているのではないか。

●ご指摘のローカルブレイクアウトの記載は、今回の改定で新しい考え方をお示したものではなく、令和2年度の第2期のセキュリティクラウドに関する検討会の中で議論いただいた結果をガイドラインにも記載したところである。地方公共団体の要望として、ご指摘の内容は理解しているが、今回は第2期のセキュリティクラウドを前提に記載している。今後、ローカルブレイクアウトの考え方についてセキュリティクラウドの在り方と合わせて検討していく。

○今後、ローカルブレイクアウトを含めて新しい仕組みを導入する際は、リスクアセスメントを実施することをお願いしたい。

2. 今後の地方公共団体の情報セキュリティ対策に係る検討事項について

○セキュリティクラウドを通らずにローカルブレイクアウトを用いてクラウドサービスを利用する場合とLGWAN-ASPやLGWAN接続系の領域からインターネットへ抜けていく場合とで違いが

あるのか。

●LGWAN 接続系のローカルブレイクアウトは、今後、詳細を検討していくところである。現時点では、Web 会議サービス等、限定されたサービスに留めることを想定している。そのため、インターネット接続系のローカルブレイクアウトとはユースケースに応じて異なるものと考えている。問題意識としては、ローカルブレイクアウトを実施している地方公共団体において、様々なセキュリティレベルで LGWAN 接続系の領域とつないでいるため、しっかりとセキュリティ対策の考え方を示すことが必要と考えている。インターネット接続系でのクラウドサービスの利用、LGWAN-ASP の利用と整合性を図る形で今後検討していきたい。

■LGWAN-ASP は、J-LIS が安全性を審査しているため、地方公共団体側で個別にセキュリティ対策を講ずることなく利用いただいている。一方、ローカルブレイクアウトについては、地方公共団体側にセキュリティ要件を設け、個別に対策を求める必要があるかという点も含め検討していく必要があると考えている。

○ α モデルや β' モデルは、画一的なものではなく、地方公共団体が安全性又は利便性のどちらを重視するかに応じて選択するものと認識している。また、無害化処理による有効性は下がってきていると考えられる。以前は、マクロウイルス等の脆弱性による被害が多かったが、今はあまり発生していない。今は、エンドポイント対策として、EDRにより、端末でのふるまい検知で対応することができるようになってきている。加えて、サンドボックスも効果が薄いため、今後は端末側のセキュリティ対策に軸足を置き、無害化は原本性の確保を考慮して、対策を入れ替えることも検討すべきと考える。

●三層の対策の導入時は、全国の地方公共団体で統一的なモデルをお示ししたが、現在では、地方公共団体で様々な規模がある中で、それぞれの地方公共団体のニーズに応じた必要な支援を行う必要があると考えているところである。無害化については、令和2年度の改定において、インターネット接続系から LGWAN 接続系への無害化通信の際にサニタイズ以外の方法による処理も認めたとところであるが、今後も最新の動向を踏まえて検討していきたい。

■EDR を中心としたセキュリティ対策は、自治体のセキュリティ対策として考えられるが、LGWAN としては、特に小規模自治体では EDR 等の導入が厳しいため、次期 LGWAN でも閉域で境界防御を維持するしかないと考えている。なお、無害化については、多重スキャンやサンドボックスの組合せ等、無害化に代わる対策について、ご意見を踏まえて引き続き検討する。

○無害化に課題があると言われているが、無害化、多重スキャンはどうあるべきかを明確にしないと、地方公共団体は、事業者からの提案について内容を確認せずに導入してしまうのではないかと。そのため、J-LIS でベンチマークを示していただき、基準を満たしたもののだけが利用されるようにしないと実効性が確保されないのではないかと。また、ローカルブレイクアウトにも関連するが、閉域接続の先にあるサービスの信頼性が確保されなければ、特定通信といえども安心できない。サービスに関する安全管理基準が地方公共団体では判断できないため、何らか

の基準が必要になる。

- これまでもガイドラインでは地方公共団体が混乱しないようできる限り機能面でセキュリティ対策を記載することに留意している。今後もその点は注意するようにしたい。また、接続先の問題について国は ISMAP の指標を設けているが、どのように接続先を限定するかを考えていく必要があると感じている。
- 単にサンドボックスや多重スキャンという言葉を示すだけでなく具体的な基準を示したい。例えば、多重スキャンは、無害化処理と同等のセキュリティが確保されるものでなければならぬと考えている。また、今回検討案でお示しした接続先のサービスの安全性についても、具体的なセキュリティ要件の整理を進めており、それを示していきたい。
- 今後、地方公共団体はいつまでに何をやらなければならないのか、短期と中長期の両面でデジタル庁、総務省、J-LIS がどのように検討していくか地方公共団体に分かりやすく説明してほしい。
- 三層の対策を今後どうするかなどは、過去の経緯を踏まえて議論する必要があるため、時間がかかると思われる。総務省のほか、デジタル庁や関係機関と協力して検討する必要があると思うため、ぜひ協力してほしい。
- 境界型防御はやむを得ないと考えるが、大規模災害が発生した際にも対応できる LGWAN の仕組みを検討いただきたい。加えて、今後 5 年～10 年の間にまた新たな感染症の流行が発生することも考えられるため、地方公共団体の機能を維持するためにリモートワークを併用することが重要であるとする。
- LGWAN はコンビニ交付などの住民サービスでも使われており、次期 LGWAN では、災害時等を含め、一層安定して運用できるよう引き続き検討していきたい。
- 今後、地方公共団体への調査等を実施予定である。本日いただいたご意見を踏まえて検討していきたい。

以 上