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20回）

議事概要　要旨版

開催日時：令和８年１月 14 日（水）　13:00～15:00

開催場所：Teams による遠隔会議

議　　事：

１．電磁的記録媒体を使用しないデータ連携について、

２．機器の廃棄・データ消去について

３．今年度のセキュリティポリシーガイドラインの改定内容について、

４．地方公共団体のサイバーセキュリティ対策に関する地方財政措置の拡充について

○：構成員　●：総務省（事務局）

１．電磁的記録媒体を使用しないデータ連携について

＃資料１　電磁的記録媒体を使用しないデータ連携について＃

＃参考資料　電磁的記録媒体の利用に関するアンケート結果＃

○ 本来不必要なデータを、領域間を跨いで受け渡しをしている例もあるのではないか。自治体へのヒアリングを行い、セキュリティ上の観点からあるべき運用等を検討していくのはどうか。

● 地方公共団体へのヒアリングをしながら幅広く検討していく。

○ ガイドラインの改定案に「主体認証機能」や「暗号化機能の適切な使用」とあるが、具体的内容を示した方が分かり易いのではないか。

● 改定案の見直しを検討する。

○ リスクアセスメントを実施するにあたり、攻撃者の侵入経路、マルウェアの拡散方法等の攻撃シーケンスについては、現実的で地方公共団体にとって理解しやすいような表現にしてほしい。

○ クラウドを利用したデータ連携では、オブジェクトストレージを活用する以外にファイルサーバ等を用いる場合もある。

○ リスクアセスメントを行いモデルを評価する上で、効果（インセンティブ）についても明記されると良いのではないか。

○ リスクアセスメントにおいては、複数の視点での確認をしていくことで偏りを防ぐことにつながるのではないか。

● リスクアセスメントのモデルは、地方公共団体の意見を踏まえながら見直し、リスクアセスメントの計画書を来年度の初めの検討会で提示する予定である。

２．機器の廃棄・データ消去について

＃資料２　機器の廃棄・データ消去について＃

３．今年度のセキュリティポリシーガイドラインの改定内容について

＃資料３　今年度のセキュリティポリシーガイドラインの改定内容について＃

○ 物理破壊を行う専用機器について、地方公共団体が理解し易いように写真付きの例示があると良いのではないか。

○ 暗号化消去については、国際動向を踏まえ、統一基準群が改定された場合は、ガイドラインへ反映できるよう検討してほしい。

● 専用機器の写真などは、補足資料に盛り込むことを想定している。補足資料は、自治体に展開する予定である。

● 引き続き国際的な動向を注視していく。

○ 消去の残存リスクについては、OS から認識できない部分については復元できてしまうという表現とした方が良いのではないか。

○ USB メモリ、SSD の上書き消去を２回以上とするのは、フラッシュメモリのウェアレベリング機能のためである。２回以上とする必要性について注意書きを記載した方が良いのではないか。

○ 破壊作業委託時の履行の担保方法について、庁舎内で破壊する場合と委託先において破壊する場合を分けて記載した方が良いのではないか。

○ 機器の修理時のデータ抹消は、記録媒体の情報を消去できないときのみならず、故障により記録媒体を交換する場合も想定されるので、改定案の記載を見直した方が良いのではないか。

● ご指摘について確認し、改定案を見直す。

○ 暗号化消去は、鍵を使用できない状態にすることが重要である。鍵を確実に消去する具体的な手順についてガイドラインにて記載するのはどうか。

● 鍵を確実に消去する具体的手順については記載内容を含め検討する。

○ サブドメインテイクオーバーや NS テイクオーバーの背景には、地方公共団体における資産管理や業務委託先管理の徹底不足といった要因があるのではないか。

○ サービス終了後のドメイン設定の確認における地方公共団体と委託先の責任分界点について方向性を示した方が良いのではないか。

● 「lg.jp」を使うことはガイドラインに記載済であるが、ドメインに関する管理や委託先管理の徹底については、引き続き検討する。

○ DDoS 対策は、クラウドサービスや通信事業者側で実施した方が有効な場合がある。

● ご指摘を踏まえ、地方公共団体にとって分かり易い追記を検討する。

○ ガイドラインの情報量が増えて複雑になっている。ガイドラインの構成だけでなく、自治体

に対する情報展開など今後の課題としてほしい。

● 総務省側からの積極的な情報発信や説明会の実施など今後検討していく。

４．地方公共団体のサイバーセキュリティ対策に関する地方財政措置の拡充について

＃資料４　地方公共団体のサイバーセキュリティ対策に関する地方財政措置の拡充について＃

○ 不交付団体も視野に入れた財政支援をお願いする。

● 不交付団体についても念頭に置きつつ、来年度以降も財政支援を拡充できるように検討していく。

○ 総務省において、ガイドラインに記載されている対策内容の必要性を説明する担当者向け研修を丁寧に実施してほしい。また、地方公共団体共通の質問については FAQ を用意することも考えられるのではないか。

● J-LIS や自治大学校が実施する研修等と連携し、自治体職員向け研修等を拡充していく。

● 自治体からの質問に対しては、共有可能な仕組みなどを今後検討していきたい。

○ 予算措置をしていただいたことは非常に大きい。セキュリティ事業者が人手不足で、自治体からのニーズに対応できる事業者が少ない状況である。地域単位で自治体を支援できる事業者を増やす施策も必要となってくるのではないか。

● ご指摘の通り現状認識している。

○ 昨今のサイバー攻撃の現状を踏まえると、常時監視の有効性は高いと考える。

○ 地方公共団体が積極的に対策に取組めるよう、財政支援と併せて地方公共団体への周知を徹底してほしい。

● ご指摘を踏まえ、今後も尽力していく。

● 次回の検討会は 3 月中旬から下旬ごろを目途に開催予定。次回もどうぞよろしくお願い申し上げる。

以上