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16回）

議事概要　要旨版

開催日時：令和７年１月 31 日（金）13:15～15:15
開催場所：Teams による遠隔会議

議　　事：
１．検討の方向性について
２．直近のインシデントについて
３．マイナンバー利用事務系に係る無線 LAN 利用及び画面転送の方式について
４．自治体情報セキュリティクラウドについて

○：構成員　●：総務省（事務局）

１．検討の方向性について

＃資料１　検討会の方向性について＃

２．直近のインシデントについて

＃資料２　直近のインシデントについて＃

○ EDR の定義をもう少し明確化すべきと考える。「不正な侵入の検知」、「データの持ち出し」「外部への通信」についても記載してはどうか。

○ マネージドサービスの評価基準を設け、その上で自治体が判断するという方が現実的と思われる。

○ 「セキュリティ専門家によるマネージドサービスの運用により」という記載は、必ずマネージドサービスはつけた状態で EDR の運用を行うことを意味しているのか。

○ EDR の定義をマネージドサービス込みとする考えは良いと思うが、マネージドサービスの運用に関する評価基準が非常に重要と考える。例えば、SOC の場所、監視している人物がどのような資格保持者か、守秘義務はどうなっているのか等、そのような注意が必要である旨を記載する必要があるのではないかと考える。

● EDR の定義に「不正な侵入の検知」、「データの持ち出し」「外部への通信」についても追記する。

● 自治体職員だけでは即座に検知及び対応が難しいため、「セキュリティ専門家」という言葉

でマネージドサービスについて言及している規定である。

● SOC によるファイルの国外送信や、SOC の場所等マネージドサービス選定時の評価基準については、検討会後、構成員の皆様へ相談し評価基準を決定後追記する。

○ 色々な対策の実施が求められているが実際に対策が実施できるのか、地方自治体への意見照会時に確認するようにしていただきたい。

● 対策実施の実現可能性についても意見照会時に確認する。

○ 緊急度や CVSS の値が高いパッチのみを選び適用したとしても、適用しなかったパッチが原因で攻撃を受ける可能性は否定できない。そのため、可能な限りセキュリティパッチは全て当てる方向とし、上手く実務と合うような形で進めていけるようにしていただきたい。

○ 財政的な問題から全てのパッチを適用することは難しいと思われる。全てのパッチを適用することは重要だと思うが、例えば「インターネットとの境界においては」などとする方が、比較的自治体側も受け入れやすいと考える。

○ パッチを適用しなくても緩和策で回避できる場合も多々あるため、緩和策で代替できる場合はそれも良しとする旨を記載しても良いのではと考える。

● 可能な限り全てのパッチを適用すべきことが伝わるような文章に修正する。
ただ、予算に限りがあることを考慮し、優先順位のつけ方として「インターネットとの境界のある機器」については、特に重要である旨が伝わるような文章に修正する。

● パッチ適用が緩和策で代替できる旨も補足する。

○ NDA 締結に 1 週間程日数がかかる場合がある。事前に NDA を結んでおかないとインシデント対応が遅れる可能性がある。

● NDA を事前に締結し、相談先とは情報共有をする旨を追記する。

３．マイナンバー利用事務系に係る無線 LAN 利用及び画面転送の方式について

＃資料３　無線 LAN 利用に係るガイドライン改定案等について＃
＃資料４　（別紙）マイナンバー利用事務系に係る画面転送の方式について（案）＃
＃資料４－１～８　マイナンバー利用事務系の画面転送に係るリスク分析結果(1)～(8)＃

○ 資料３の 15 頁「原則、接続先が信頼される特定先及び画面転送技術を利用する場合を除いて LGWAN 接続系やインターネット接続系と特定通信として接続してはならない。」の「原則」が文章全体にかかるため、文章を修正した方が良いと考える。

○ セキュアブラウザは製品によってセキュリティレベルが高いものから低いものまで存在する。最低限実装すべき機能を提示した方が良いのではないか。少なくとも、リスク分析時に使用したセキュアブラウザの基本機能については示す必要があるのではと考える。

● 「原則」を削除し、文章も「画面転送技術により信頼される特定先と接続する場合」のみ許容している旨が伝わるよう修正する。

● リスク分析を行った前提となるセキュアブラウザの要件について規定する。また最低限、セキュアブラウザの要件に記載すべき機能はあるか。

○ リスク領域の分離、メモリ領域の分離、ローカルと分離環境との間の通信の禁止、仮想ブラウザ自身の正常性の維持、仮想ブラウザ自身の脆弱性対応、任意プログラム実行禁止等は入れるべきではと考える。

● ご指摘を踏まえて追記させていただこうと思う。

○ 資料４の４頁「リスク値を考慮し、首長を含めた自団体の幹部まで」という記載をもう少し強調し、ハイリスクな仕組みを利用しようとしている旨を説明するようにしていただきたい。

● ハイリスクであることを組織的に認識し意思決定をしていただくことが必要だと総務省としても考えているため、より、その旨が伝わるようにしていきたい。

４．自治体情報セキュリティクラウドについ

＃資料５　自治体情報セキュリティクラウドについて＃

○この自治体セキュリティクラウドがうまく機能しているようで良かった。

以上