資料２－４

情報セキュリティに係る検討

消防庁防災情報室

令和3年3月25日

情報セキュリティ等に関する検討方針

〇消防指令システムの情報セキュリティ対策については、「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」（令和２年１２月改定、総務省）に基づき実施することを原則としつつ、円滑に災害対応を行う観点から必要に応じて代替策等を検討。

〇指令システムが扱う情報の内容や求められる可用性の水準、外部システムとの接続シーンなどを整理し、指令システム全体もしくは機能別に情報セキュリティ対策を検討。

〇消防ＯＡシステムの一部など、指令システムと関わりが深い周辺システムについても合わせて検討。

＜検討の観点（例）＞

（１）機密性・完全性

- 指令システムでは事案情報等の個人情報を扱うが、ガイドラインと照らしてどのようなセキュリティ対策が求められるか。（どのようなネットワークに接続するかを含む。）
- 一方で、火災・救急事案等への極めて迅速な対応が求められる消防本部の業務特性を考慮し、場合によっては代替措置による対応が必要ではないか。（接続シーン別の整理が必要か。）

※現状として、やむを得ず情報セキュリティポリシーの例外措置を適用している事例も複数存在。

（２）可用性

- 指令システムは、国民からの緊急通報を常時受信できるようにするため高い可用性が求められるが、どの程度の水準が必要か。

※「非機能要求グレード（地方公共団体版）」（J-LIS）の区分を参照すると、災害発生時の初動対応に必要であり、社会的影響も大きいシステムに区分され、高い水準の非機能要件が求められる。

- システム障害発生時に縮退運転が行われること等も踏まえ、指令システムの中で特に高い可用性が求められる機能について、整理が必要ではないか。

参考

〇 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

- 総務省において、平成１３年３月に初版が策定された後、適宜改定され、最新版は令和２年１２月に改定。
- 各地方公共団体が情報セキュリティポリシーの策定や見直しを行う際の参考として、情報セキュリティポリシーの考え方及び内容について解説したもの。「三層の対策」として、システムをマイナンバー利用事務系、ＬＧ－ＷＡＮ接続系、インターネット接続系に分ける情報セキュリティ対策が示されている。

〇 情報セキュリティの定義（JIS Q 27000）

- 機密性：情報へのアクセスを認められた者だけが、その情報にアクセスできる状態を確保すること
- 完全性：情報が破壊、改ざん又は消去されていない状態を確保すること
- 可用性：情報へのアクセスを認められた者が、必要時に中断することなく、情報及び関連資産にアクセスできる状態を確保すること