資料３－５

情報セキュリティに係る検討状況

消防庁防災情報室

令和3年7月19日

情報セキュリティ等に関する検討状況①

検討方針（第２回会合資料より抜粋）

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＞（以下「総務省ガイドライン」）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。

今回

〇まずは現状把握のため、一部の本部からヒアリングを実施。
〇引き続き情報収集を行い、論点整理を行った上で詳細検討を実施予定。※今回は論点（例）のみ提示。

現状把握の結果

①消防本部の情報セキュリティポリシーは、基本的に総務省ガイドラインをもとに作成されている

【ヒアリング結果】

・所属する地方公共団体のポリシーに準拠する場合や同ポリシーのもと消防本部が独自に情報通信規定を定めている場合、消防本部自らがポリシーを定めている場合などがあった。

・共同指令センターでは、指令センターで独自のポリシーを定めている場合と、構成本部（もしくは市町村）のポリシーにそれぞれ準拠している場合の両方があった。

⇨ 総務省ガイドラインをベースに検討を進める方針は、妥当と考えられる。

情報セキュリティ等に関する検討状況②

②外部から独立させることで指令システムのセキュリティを担保していることが多い

【ヒアリング結果】

・指令システムは、外部ネットワークとの接続を最小限に留めることで、システムの情報セキュリティを担保していることが多い。

・外部ネットワークと接続する場合は、接続点にファイヤウォール等のセキュリティ機器を設置する等の対策を実施。セキュリティ対策の参考として、総務省ガイドラインのLG-WAN接続系のセキュリティ対策を参照している等。

・システム内部のセキュリティについては、ログ管理等の一定の対策を行いつつも、対策強化の余地あり。厳しい対策を行うことで、安定稼働や緊急時の迅速な対応などに影響がでることを懸念する声。

⇨ 今後、指令システムと外部システムを接続させる場合、情報セキュリティ対策の考え方を変える必要。

③指令システムと接続している既存システムについて、引き続き整理が必要

【ヒアリング結果】

・指令システムと接続している既存システムとして挙げられたものは、以下のとおり。

・詳細が不明な項目もあり、追加の情報収集が必要。また、第２回会合にて提示したアンケート結果によると、これら以外にも接続しているシステムはあると推定。

⇨ 各システムとやり取りする情報の内容や、接続に用いるネットワークなどについて、引き続き整理が必要。

表　接続している既存システム（例）

名称	概要	取扱データ	接続回線	対策状況
メール指令	消防職団員に指令情報をメール送信	（出力）災害地点、種別等 （入力）参集可否	インターネット	今後整理
住民向け情報配信	住民向けに災害情報をメール配信	（出力）災害・防災情報	インターネット	
位置情報通知	電話事業者から位置情報等を受信	（入力）位置情報・契約者情報等	IP-VPN	
車載端末	部隊活動の支援・報告	（出力）災害地点、部隊動態等 （入力）活動状況	モバイル閉域網	
映像系	高所カメラ等の映像を受信	（入力）災害現場の映像	専用線、閉域網	
医療情報系	病院空床、搬送状況等の共有	（入力）空床、搬送状況等	IP-VPN等	

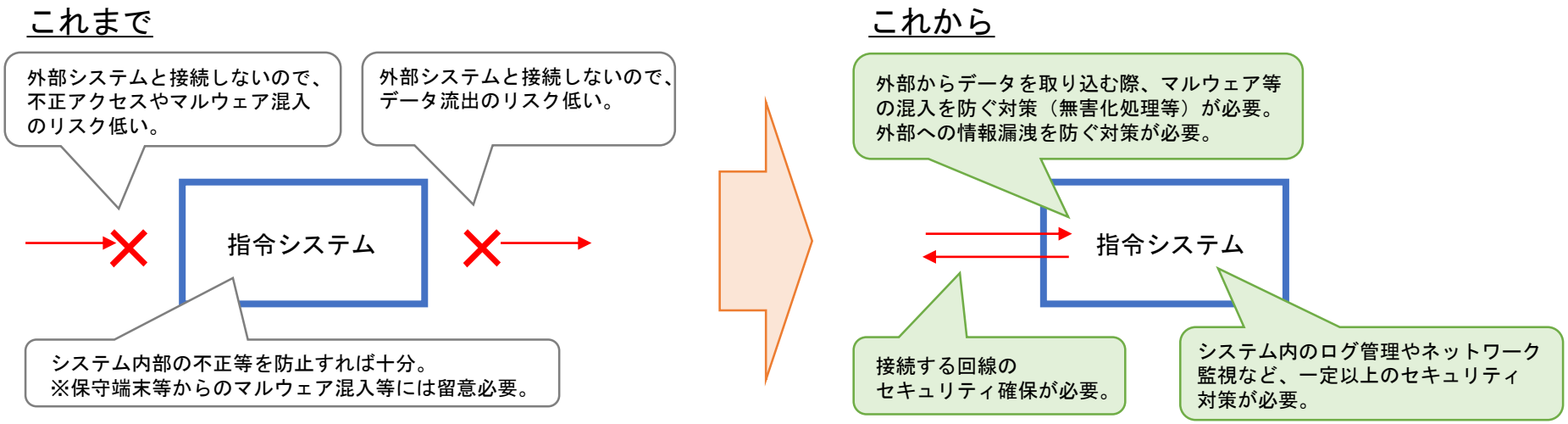
システムの洗い出し

さらに整理

情報セキュリティ等に関する検討状況③

論点（例）

★論点①　外部システムと接続する際の対策



★論点②　総務省ガイドラインとの比較検討

ポイント

○指令システムが扱うデータの内容や接続先の外部システムなどを踏まえ、総務省ガイドラインにおいて求められるセキュリティ水準はどの程度か。

○今後、総務省ガイドラインを始めとした地方公共団体のシステムについて、どのような検討が行われるか。
（議論動向を継続的に注視していく。）

・成長戦略フォローアップ（令和3年6月18日）

地方公共団体の業務システムの標準化・共通化を踏まえ、「三層の対策」の抜本的見直しを含め新たなセキュリティ対策の在り方を検討する。
さらに、地方公共団体のパブリッククラウドの利用について、ISMAPの運用状況等を踏まえ、必要なセキュリティ対策を検討する。

【参考】総務省ガイドラインの記載　※一部を例示として掲載

- LGWAN接続系とインターネット接続系は両環境間の通信環境を分離した上で、必要な通信だけを許可できるようにしなければならない。なお、メールやデータをLGWAN接続系に取り込む場合は、（中略）無害化通信を図らなければならない。
- ウェブサーバ等をインターネットに公開する場合、庁内ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続しなければならない。
- 機密性2以上の情報資産を取り扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適正な回線を選択しなければならない。
- クラウドサービスの特性を考慮した上で、クラウドサービス部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全体を見渡した形でセキュリティ設計を行った上でセキュリティ要件を定めなければならない。