

要配慮者名簿データベースに対するアクセス制御

1170327 杉野良樹 【ネットワーク信号処理研究室】

1 はじめに

災害時に一時避難や応急手当を目的として災害救護拠点が開設される。災害救護拠点には要配慮者を含む被災者が多く集まることが予想される。要配慮者とは高齢者など災害時に避難支援が必要な人のことである。要配慮者の情報は名簿として自治体で管理されている。また、災害救護拠点では、今後の災害対策や安否確認のため被災者名簿の作成が義務づけられている。災害救護拠点での名簿作成の負担を軽減するために被災者名簿作成システムの研究が行われた [1]。災害救護拠点において被災者名簿作成システムから要配慮者名簿を活用することで要配慮者への柔軟な対応を行うことができる。しかし、災害救護拠点では多くの人が活動しており、すべての人が個人情報である要配慮者名簿を閲覧することは望ましくない。

本研究では、自治体で管理されている要配慮者名簿を災害救護拠点で活用するためにデータベース化し、閲覧可能な人を制限するためにアクセス制御を行う。また、データベースを運用する上ですべての権限を持つ管理者アカウントの不正利用のリスクを軽減するためにアカウント管理者と要配慮者名簿データベース管理者に権限を分けてデータベースの運用を行う。

2 要配慮者名簿データベースに対するアクセス制御

被災者名簿作成システム [1] から要配慮者名簿の情報にアクセスする上での問題点として、被災者名簿は災害救護拠点内で公開するのにに対して、要配慮者名簿は許可のある人しか閲覧させることができない点がある。要配慮者名簿データベースに対してアクセス制御を行うことで適切に情報を扱うことができる。

本研究では、要配慮者名簿データベースに対してアクセス制御を行う。また、要配慮者名簿データベース管理者はデータベースに対してすべての権限を持つため、不正利用されることで要配慮者名簿のデータを自由に参照することが出来てしまう。そのため、要配慮者名簿データベース管理者とアカウント管理者に権限を分けてデータベースの管理を行う。

表 1 要配慮者名簿データベースに対するアクセス権限

権限	参照	削除	更新	追加
ボランティア	×	×	×	×
医療従事者	○ (制限)	×	×	×
被災者名簿作成データベース管理者	○	×	×	×
要配慮者名簿データベース管理者	○	○	○	○
アカウント管理者	×	×	×	×

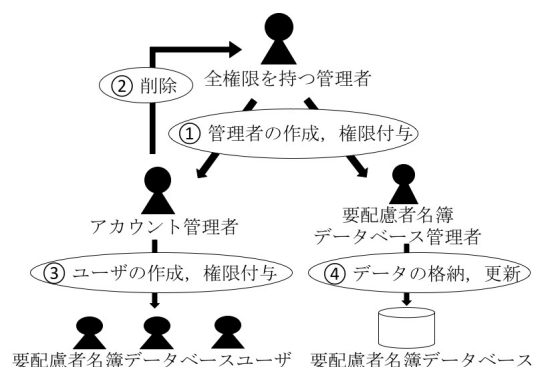


図 1 管理者アカウントの不正利用対策

2.1 アクセス制御

要配慮者名簿データベースのユーザとして 3 つのアカウントを作成し、データベースを運用するための管理者として 2 つのアカウントを作成する。各アカウントの要配慮者名簿データベースに対するアクセス権限を表 1 に示す。医療従事者は要配慮者の対応に必要なデータに対してのみ閲覧可能にするため、カラムレベルでの参照権限を与える。

2.2 データベース管理者権限

すべての権限を持つ管理者アカウントの不正利用対策を図 1 に示す。全権限を持つ管理者がアカウント管理者と要配慮者名簿データベース管理者を作成し、権限の付与を行う。アカウント管理者が全権限を持つ管理者を削除し、要配慮者名簿データベースにアクセスするユーザの作成及び権限付与を行う。要配慮者名簿データベース管理者がデータの格納及び更新を行う。

3 まとめ

本研究では、災害救護拠点において要配慮者名簿を活用するために要配慮者名簿データベースに対してアクセス制御を行った。これによって要配慮者名簿データベースの個人情報へのアクセスを制限することが可能となる。また、2 つの管理者に分けることで、管理者アカウントの不正利用のリスクを軽減することができる。

今後は、災害救護拠点において被災者名簿作成システムからの電子カルテの活用も検討していくことで被災者に対してより柔軟な対応を行うことができる。

参考文献

- [1] 那須裕太, “災害医療拠点における被災者名簿作成データベース,” 平成 27 年度高知工科大学プロジェクト研究報告書, 2016.