

要配慮者名簿データベース に対するアクセス制御

2017年2月20日

1170327 杉野良樹

情報学群

ネットワーク信号処理研究室

研究の背景

- ・ 災害発生時，災害救護拠点が開設される

大勢の被災者



災害拠点病院



被災者
対応エリア

災害救護拠点

被災者名簿



総合受付

中重度受付

重症

軽傷

要医療

要介護

一時避難

軽傷エリア

医療対応

被災者対応エリア

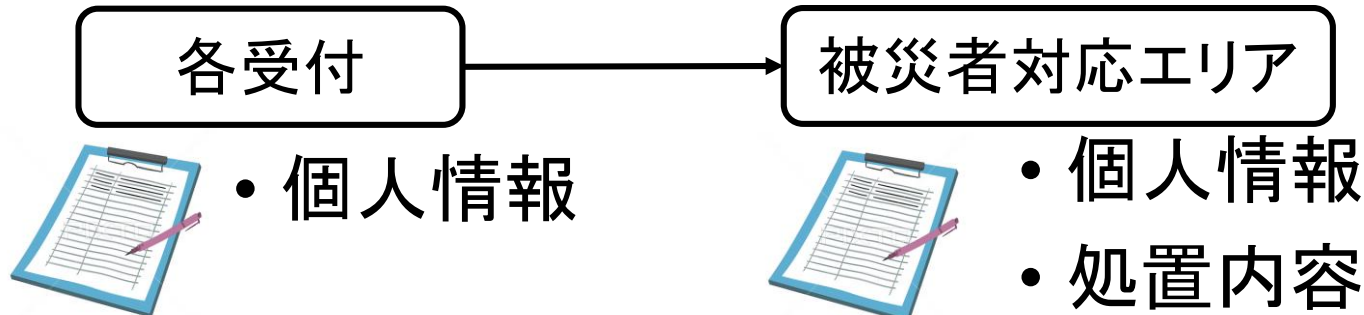
一時避難エリア

研究の背景

- 被災者名簿
 - 後の安否確認や情報共有にも活用



- 各エリアで名簿の保管が必要



個人情報の重複記入
各エリアで個別に名簿が存在する



- 被災者名簿作成データベース（那須裕太, 2016）
 - 紙の名簿が不要 → エリア間での名簿の共有

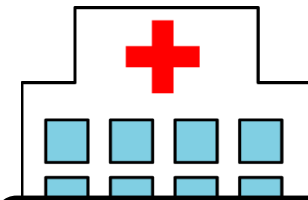
災害救護拠点

大勢の被災者

要配慮者



災害拠点病院



重症エリア

災害救護拠点

総合受付

中重度受付

重症

軽傷

要医療

要介護

一時避難

軽傷エリア

医療対応エリア

介護福祉エリア

一時避難エリア

要配慮者名簿

- 要配慮者
 - 災害時に避難支援が必要な人
- 要配慮者名簿
 - 要配慮者の情報を自治体が管理
 - 災害救護拠点での活用

要配慮者名簿データベース

要配慮者名簿DBの課題(1/2)

要配慮者名簿

- ・個別計画
 - 個人情報、避難方法
- ・医療情報
 - 治療中の病気、投薬履歴



要配慮者名簿データベース

- ・個別情報テーブル
 - 個別計画の一部
- ・医療情報テーブル
 - 治療中の病気、投薬履歴



職種によって閲覧可能な情報が異なる

要配慮者名簿DBの課題(2/2)

データベースの運用

- ・管理者アカウント
 - ユーザの作成・権限付与
 - データベース、テーブルの作成・データ格納

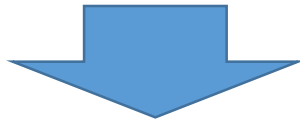


課題

- ・不正利用
 - データベースの情報を閲覧される

研究の目的

- 課題
 - 管理者アカウントの不正利用
 - 要配慮者名簿をすべての人が閲覧することは望ましくない



- 要配慮者名簿DBの管理者アカウントの権限を分け、要配慮者名簿DBに対してアクセス制御を行う

管理者アカウント

管理者アカウントの権限を用途別で分割



アカウント管理者

- ・要配慮者名簿DBユーザの作成
- ・ユーザ情報の管理
- ・全権限を持つ管理者アカウントの削除

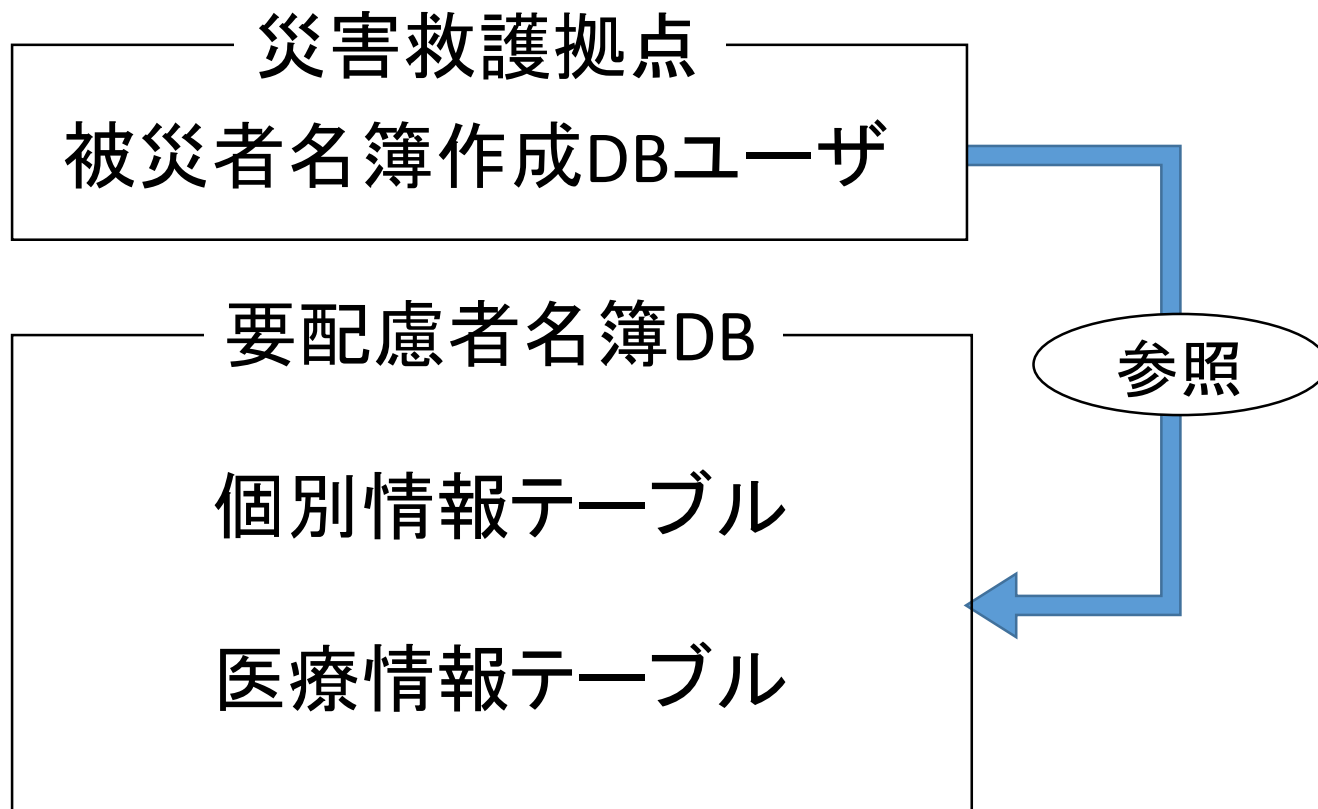


要配慮者名簿DB管理者

- ・要配慮者名簿DBへデータの格納・更新
- ・各ユーザへ参照権限の付与

それぞれ権限が制限されているため
不正利用のリスクの軽減

アクセス制御



要配慮者名簿を参照できる人を制限する

要配慮者名簿DBユーザ

- 被災者名簿作成DB
ボランティア、医療従事者、介護職員、
被災者名簿作成DB管理者
- 管理者アカウント
アカウント管理者、要配慮者名簿DB管理者
- 医療従事者
医師、薬剤師、看護師
- 介護職員
ケアマネージャ

アクセス制御

要配慮者名簿DBに対する参照権限

アカウント	個別情報テーブル	医療情報テーブル
ボランティア	×	×
医療従事者・介護職員	○	※
被災者名簿作成DB管理者	○	○
アカウント管理者	×	×
要配慮者名簿DB管理者	○	○

医療従事者と介護職員の アクセス制御

- 医療従事者、介護職員

医療情報テーブルへのアクセス

- 医師
- 薬剤師
- 看護師
- ケアマネージャ

二重でアクセス制御

- 職種別の医療従事者・介護職員の権限

- 現状は同じ権限
- 今後区別する可能性がある

要配慮者名簿データベースに対するアクセス制御

—— 災害救護拠点 ——

要配慮者名簿データベース

- ・管理者アカウントの不正利用のリスク軽減
- ・各ユーザの閲覧制限



分割した管理者同士の結託

管理者でも簡単にアクセスできない仕組みの検討

まとめ

- 管理者アカウント権限の分割
 - 管理者アカウントの不正利用対策
- 要配慮者名簿DBに対するアクセス制御
 - 要配慮者名簿を閲覧可能な人を制限
- 今後の課題
 - 災害時に必要なデータの整理
 - 管理者も簡単に閲覧できない仕組みの検討