

# マイナンバー制度におけるアクセス制御

木下研究室

伊藤圭祐 (201002666)

## 1 まえがき

近年、企業や個人が扱う情報量は増加しており、その情報が漏えいする可能性もまた増加している。情報漏えいを防止するために様々な研究が進められているが、個人情報漏えいが後を絶たない。情報漏えい対策で研究されている技術の一つがアクセス制御である。一つ一つは秘密情報として扱われなくても、ある条件下におけるとき推論によって本来は得ることができない情報として外部に流出してしまう可能性が出てきた。

また、2016年1月より「マイナンバー制度」の運用が開始される。国民一人一人に12桁の番号が割り当てられ、個人情報を番号で一元管理する制度である、しかしこの制度において推論による個人情報の漏えいが懸念されている。マイナンバー制度では行政間をまたいで情報をやり取りするため、自然に様々な情報が集まり、情報漏えいがされやすくなる問題がある。

例えば行政内部に情報漏えいを目論む者がいる場合、複数の書類上に同様の項目(住所等)が存在するとその情報をもとに他の情報を辿っていくことで秘密情報にも到達できてしまうと考えられる。本研究ではマイナンバー制度のもと、ハイパーグラフとダイクストラ法を用いて、推論されやすい経路の検出を目的とする。

## 2 提案手法

マイナンバー制度で扱う情報をグラフにし、辺にコストを重みとしてつけダイクストラ法で推論経路を検出する。複数の推論による経路を発見するために、ハイパーグラフを用いる。求めた経路が推論経路となるので、その経路に対し辺を開放除去することで推論を防ぐ。重みは  $w$  として設定し、 $w = C + p$  とする。ここで  $C$  を書類を閲覧する際の時間的コスト、 $p$  を情報の貴重さとする。

## 3 提案モデル

マイナンバー制度におけるオブジェクト間の辺の重みを設定することで、推論されやすい経路の定義は次のようになる。

時間的コストを重みとした場合、ダイクストラ法で求めた最短経路は最も推論に時間がかからない経路、すなわち推論されやすい経路となる。この求めた経路に対して、辺の開放除去を行い推論による情報漏えいを防ぐ。

辺の開放除去に関しては、最も重みの大きい辺を開放除去する。

また、三角形を頂点として扱う場合、三角形から三角形の向く方向にある頂点間の重みは時間的コストなどからは計算することができないため、隣接する辺の重みの平均をとり、 $E_j$  とする。

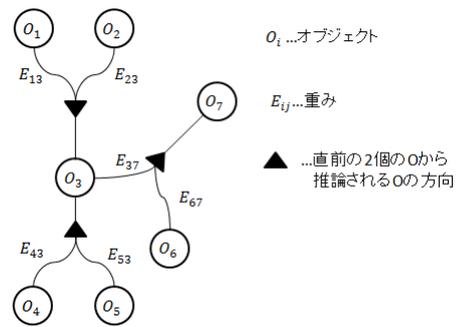


図 1: ハイパーグラフの重みづけ

実際にマイナンバー制度で扱う情報をハイパーグラフに当てはめ、推論経路を検出する。ここで扱う情報は、給与支払調査書、出生届、印鑑登録書、法定調査書とする。

またオブジェクト間の重みは時間的コストと貴重さから次のように置く。書類から書類へまたぐ場合、時間的コストを2、またがない場合1とする。情報から多くのことが推論できるオブジェクトの辺の貴重さは多くする。同じような名前のOからOへ向かう辺なら貴重さは0とする。

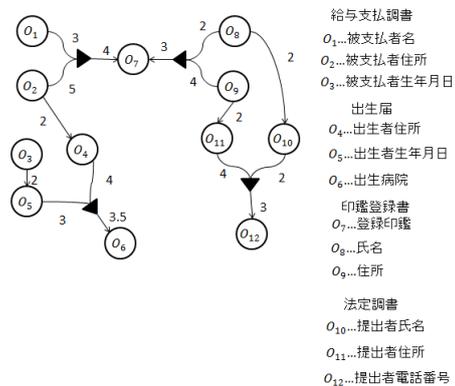


図 2: マイナンバー制度でのハイパーグラフ

このグラフにダイクストラ法を適用して推論されやすい経路を求める。例えば  $O_1$  から最も推論しやすいのは  $O_7$  の登録印鑑である。経路の辺に対して開放除去を行えば、推論を防ぐことができる。