ブロックチェーンを用いた情報漏えいを未然に防ぐ警告システム

201403853　于　子鈞

背景と問題点

- 近年インターネットのユーザが劇的に増え続けている反面、ユーザーが情報漏えいの危険性を認識せず、個人情報をネットにアップしているため、情報漏えいが発生しやすくなっている。

- 個人情報が漏えいした際、ユーザが自分の個人情報が漏えいした事実を知らされず、詐欺などの被害に遭ってしまう。

先行研究

- ブロックチェーンを利用しアクセス履歴を記録する。
- ユーザがアクセスするたびに、ブロックチェーンに記録されたアクセス履歴をもとに推論規則を使って、情報漏えいの可能性があるかを判断する。
- もしあるようであれば、アクセスを拒否するシステムがあった。

目的

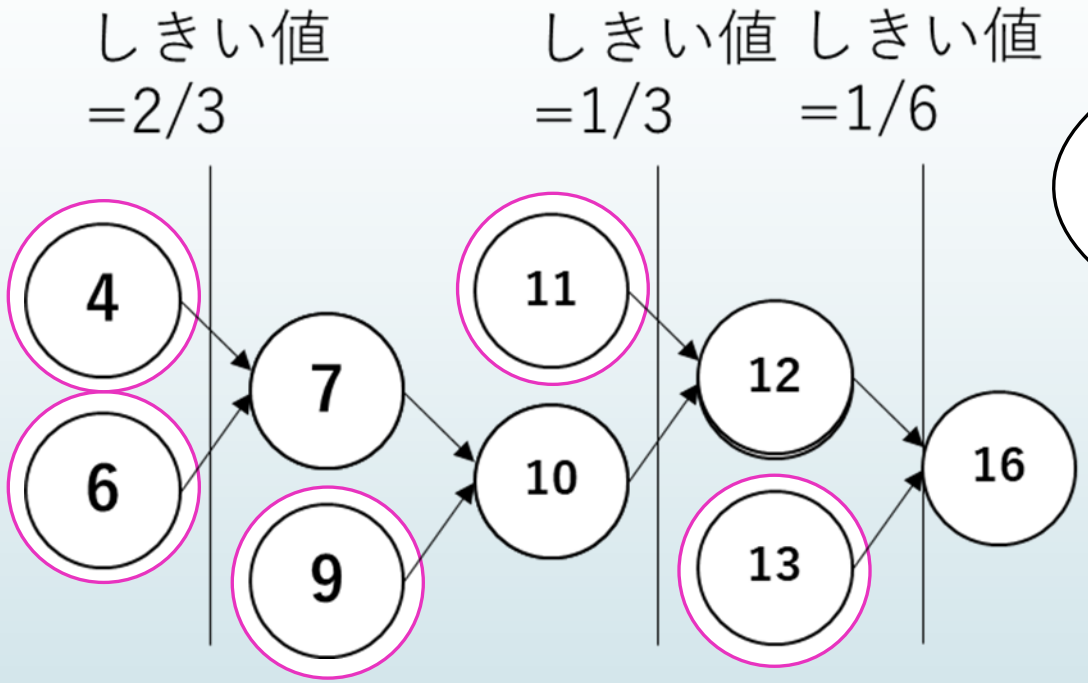
- あらかじめ推論径路を算出し、ユーザーからのアクセスによって推論攻撃のリスクがある場合、推論径路の一端を開放することによって、情報漏えいを未然に防ぐ。

- 個人情報の持ち主に情報漏えいが可能性があると警告を出すことによって、ユーザーが自分の情報について把握でき、詐欺などに遭ったときに、対応できる。

本研究のオリジナリティ

- あらかじめ推論規則を使って、推論径路を分析し、推論径路に長さという概念を付加する。
- 警報が出るしきい値を変更することによってさまざまな状況に対応できる。
- ユーザが自身の情報が漏えいする可能性があるのを知ることで、個人情報の不正利用に対処できる。

推論径路の長さとしきい値の定義

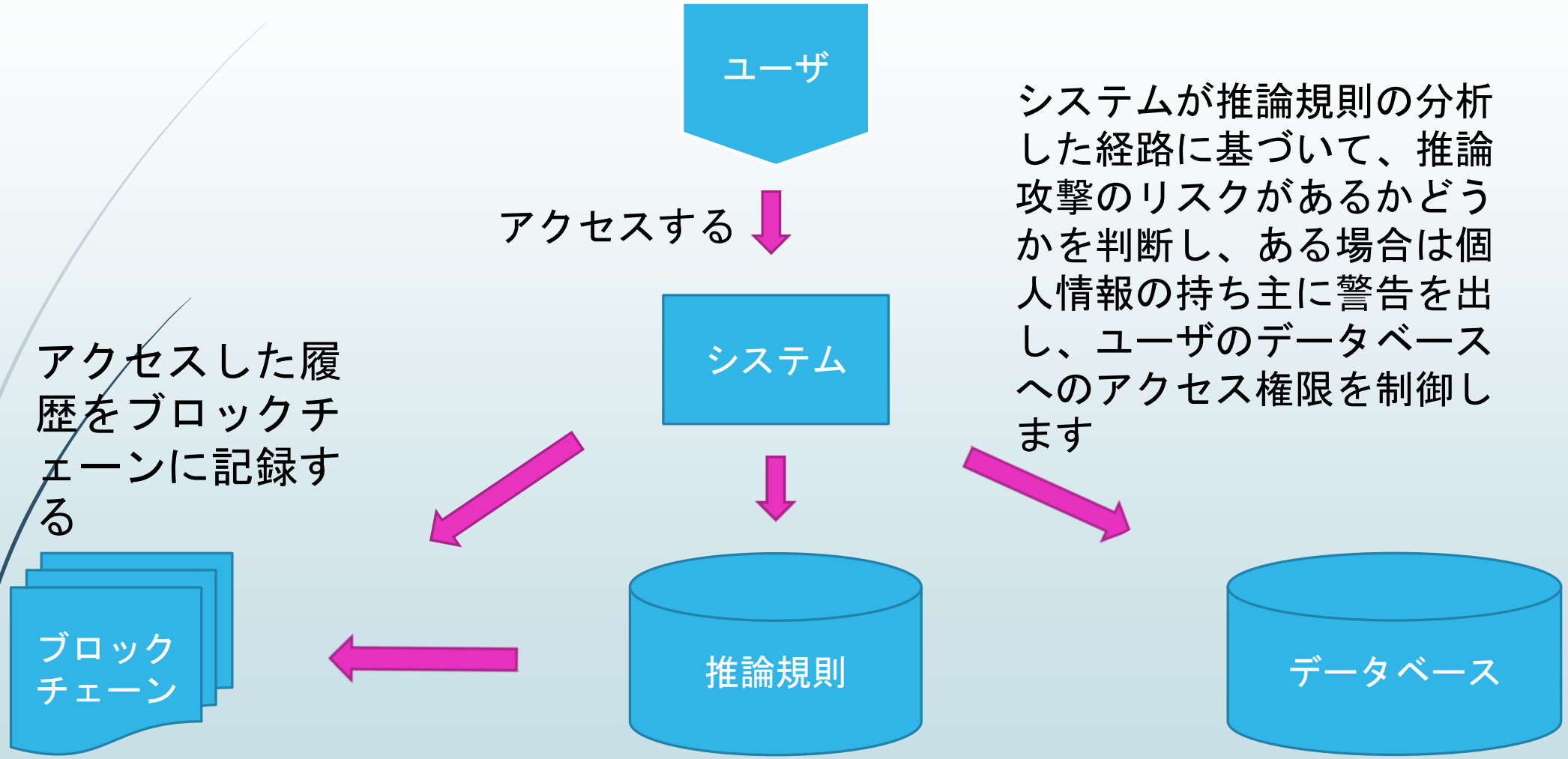


赤い丸に囲まれたオブジェクトは推論が完成する（o16が推論される）ための最小限に必要な情報

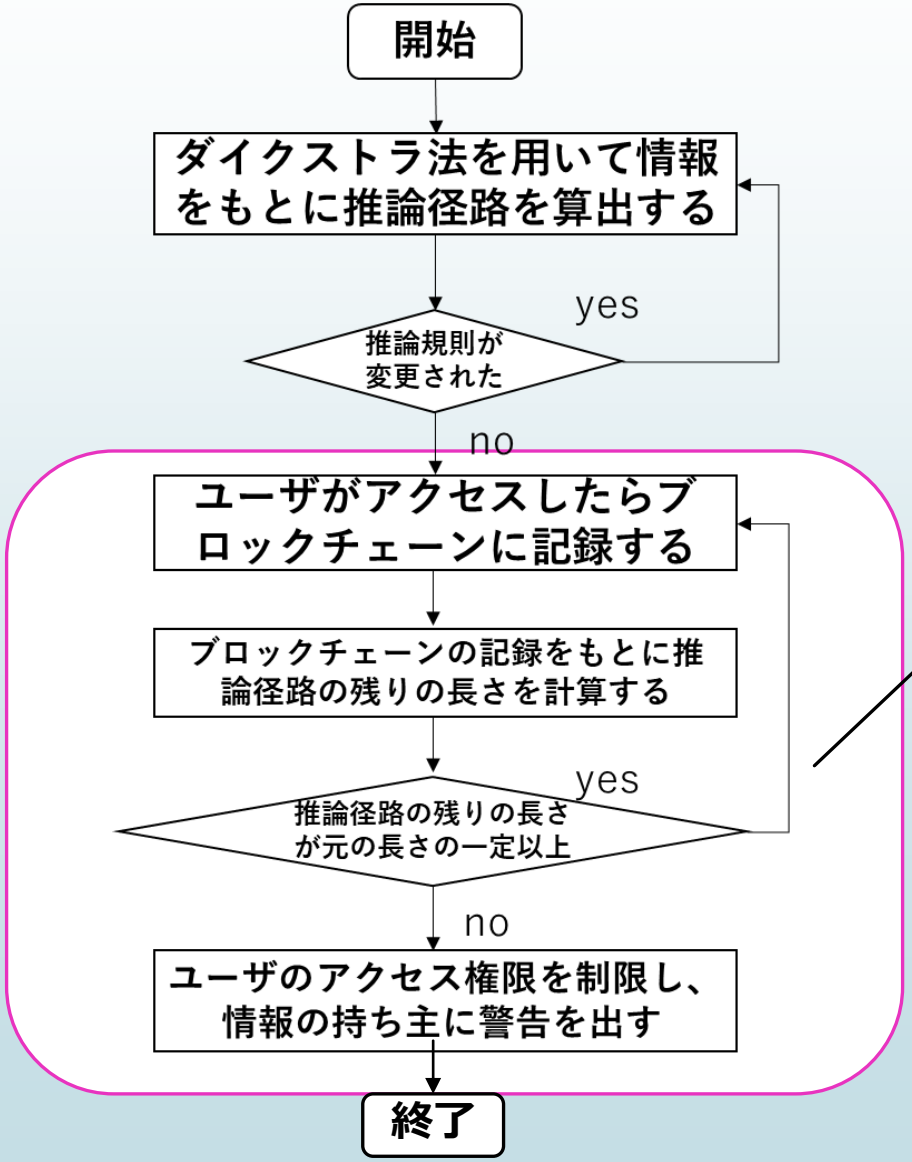
推論径路の元の長さを推論が完成するために必要な最小限のオブジェクトの数×２とする（オブジェクトへの書き込みと読み込みの長さをそれぞれ１とする）

経路の長さが元の長さ×ｎ以下となったときに警告を出すが、このｎをしきい値とする。

提案モデル


ユーザ
アクセスする
システム
システムが推論規則の分析した経路に基づいて、推論攻撃のリスクがあるかどうかを判断し、ある場合は個人情報の持ち主に警告を出し、ユーザのデータベースへのアクセス権限を制御します
アクセスした履歴をブロックチェーンに記録する
ブロックチェーン
推論規則
データベース
ブロックチェーンの記録に照らしてアクセス経路を分析する

提案モデルのフローチャート



この部分を実装し、シミュレーションした。

提案モデルの一回のシミュレーションの概要

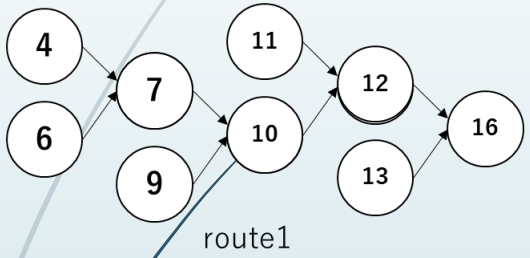
- アクセス行列を生成する。

	s1	s2	s3	s4	s5	s6	s7	s8	s9	s10	s11	s12	s13	s14	s15	s16
o1	1	3	2	0	1	0	2	2	2	0	1	1	1	3	1	3
o2	3	2	3	0	3	0	2	1	0	2	1	0	2	3	3	2
o3	3	2	1	0	3	3	3	2	3	3	2	1	1	0	1	3
o4	1	0	3	0	2	1	1	3	3	1	1	2	0	3	2	2
o5	0	2	0	2	0	0	2	1	2	1	2	2	2	1	1	0
o6	1	3	0	2	0	0	2	0	3	0	0	3	2	3	1	2
o7	2	2	1	1	1	3	3	2	0	2	1	2	1	2	1	1
o8	0	0	2	1	1	1	1	0	2	2	1	0	3	3	3	2
o9	3	0	2	2	1	0	2	2	3	3	3	1	1	3	1	3
o10	1	1	1	2	1	0	2	2	2	2	1	0	0	3	2	3
o11	2	3	0	1	0	3	3	1	2	2	3	0	2	0	0	1
o12	0	3	0	0	1	2	1	3	2	2	0	0	3	3	0	1
o13	0	3	3	1	2	1	1	2	1	0	3	3	0	1	3	0
o14	2	3	0	0	0	1	1	2	3	1	1	3	3	3	2	3
o15	0	0	2	2	0	0	2	1	1	2	1	1	0	2	2	0
o16	2	3	2	1	2	3	3	0	0	3	2	2	0	3	0	2

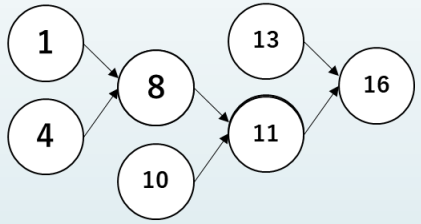
シミュレーションごとにアクセス行列は変更しないものとする。

提案モデルの一回のシミュレーションの概要

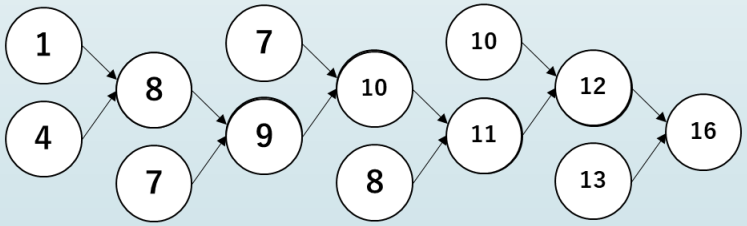
- 推論規則を生成する。



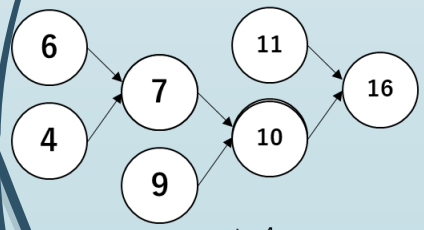
route1



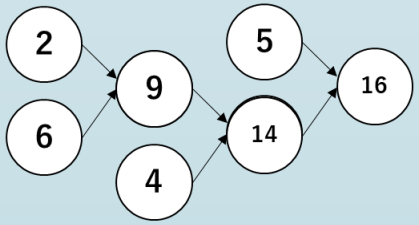
route2



route3



route4

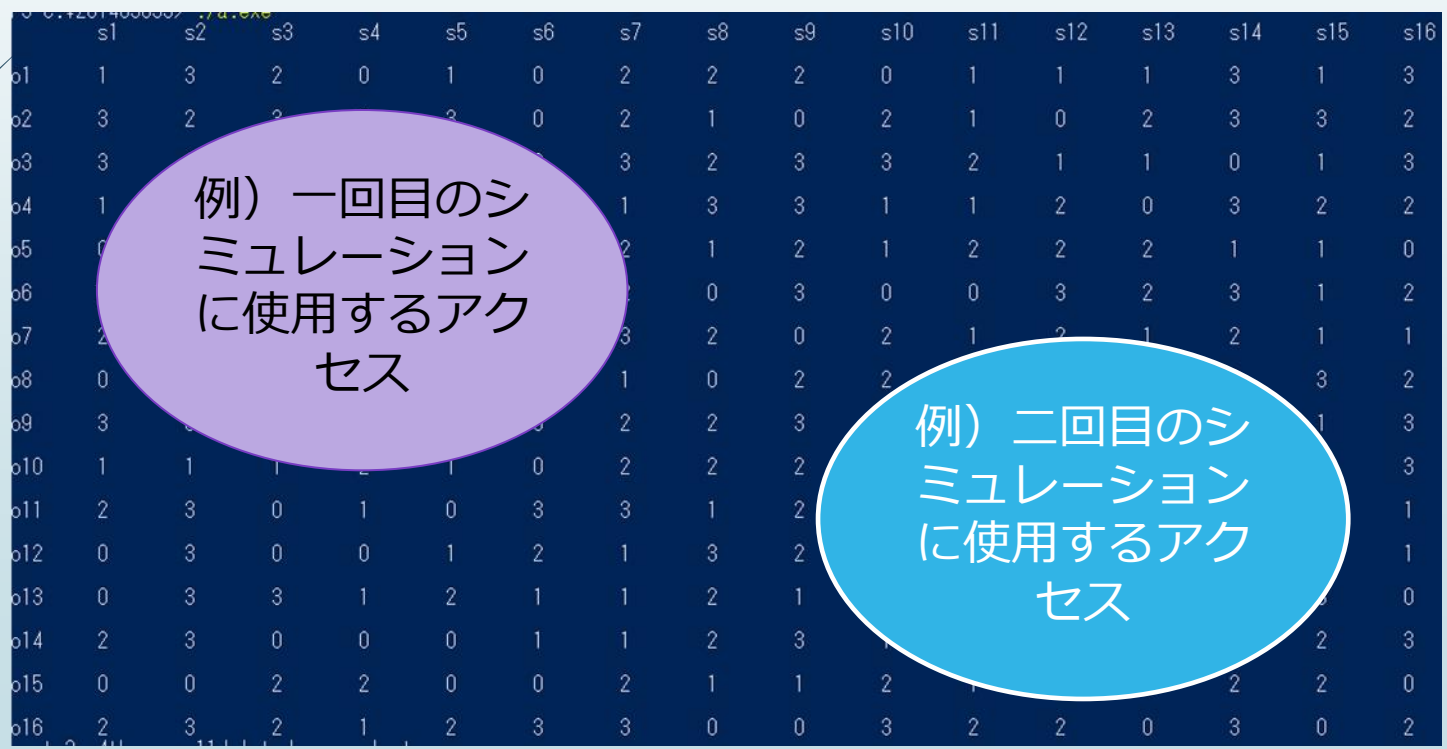


route5

今回のシミュレーションは生成された推論規則に基づき、この五つの経路を対処とする。

提案モデルの一回のシミュレーションの概要

- アクセス行列からシミュレーションごとに異なる100個のアクセスを異なる順番で行い、提案モデルの動作を検証する。



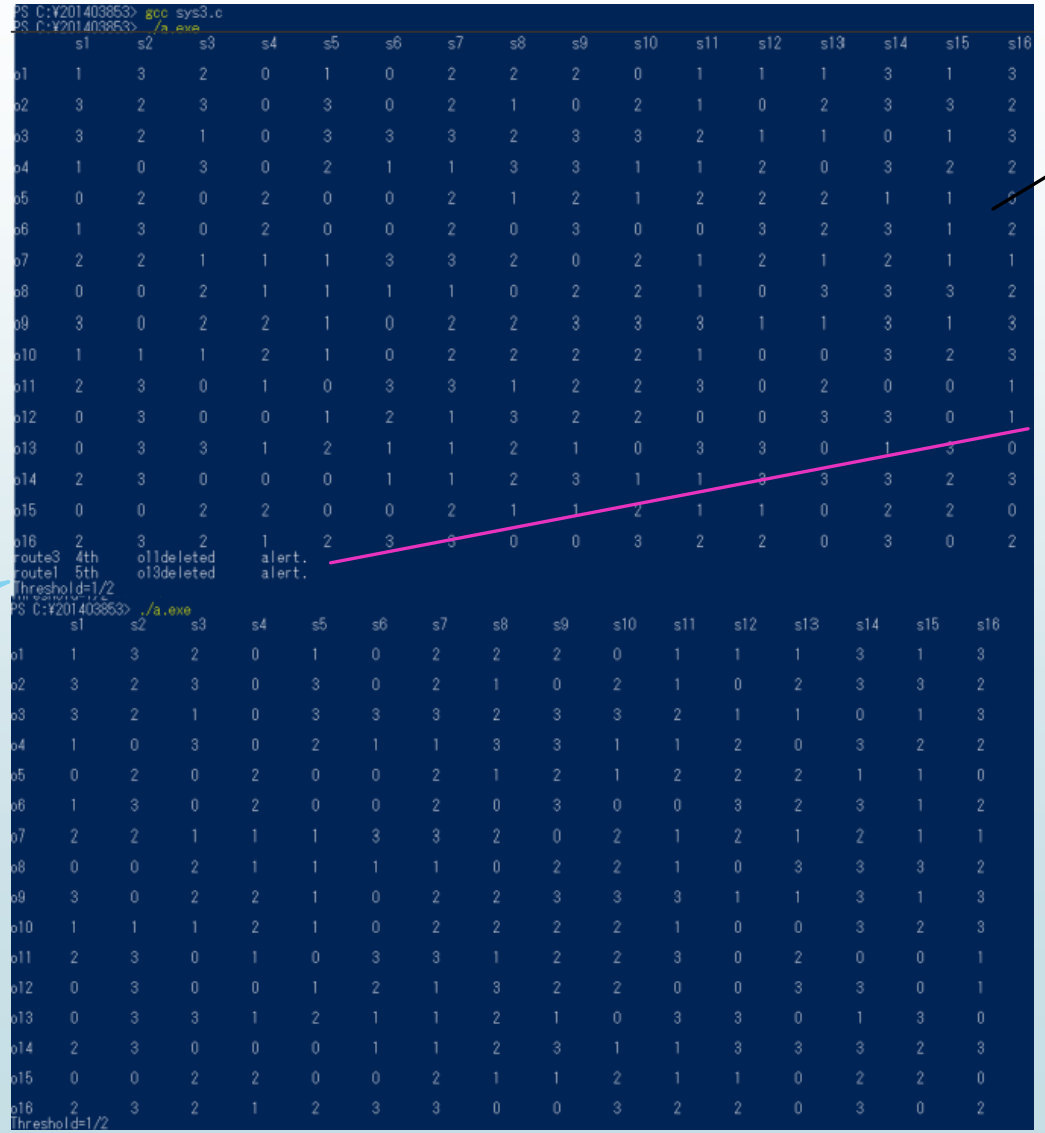
アクセス行列

提案モデルをシミュレーションした結果

しきい値が1/2の場合

シミュレーションごとに、アクセス行列は変更せず、アクセス行列からランダムに行われる100個のアクセスを変える

二つのシミュレーションの結果をピックアップしたが、警報が出るときと出ないときある。

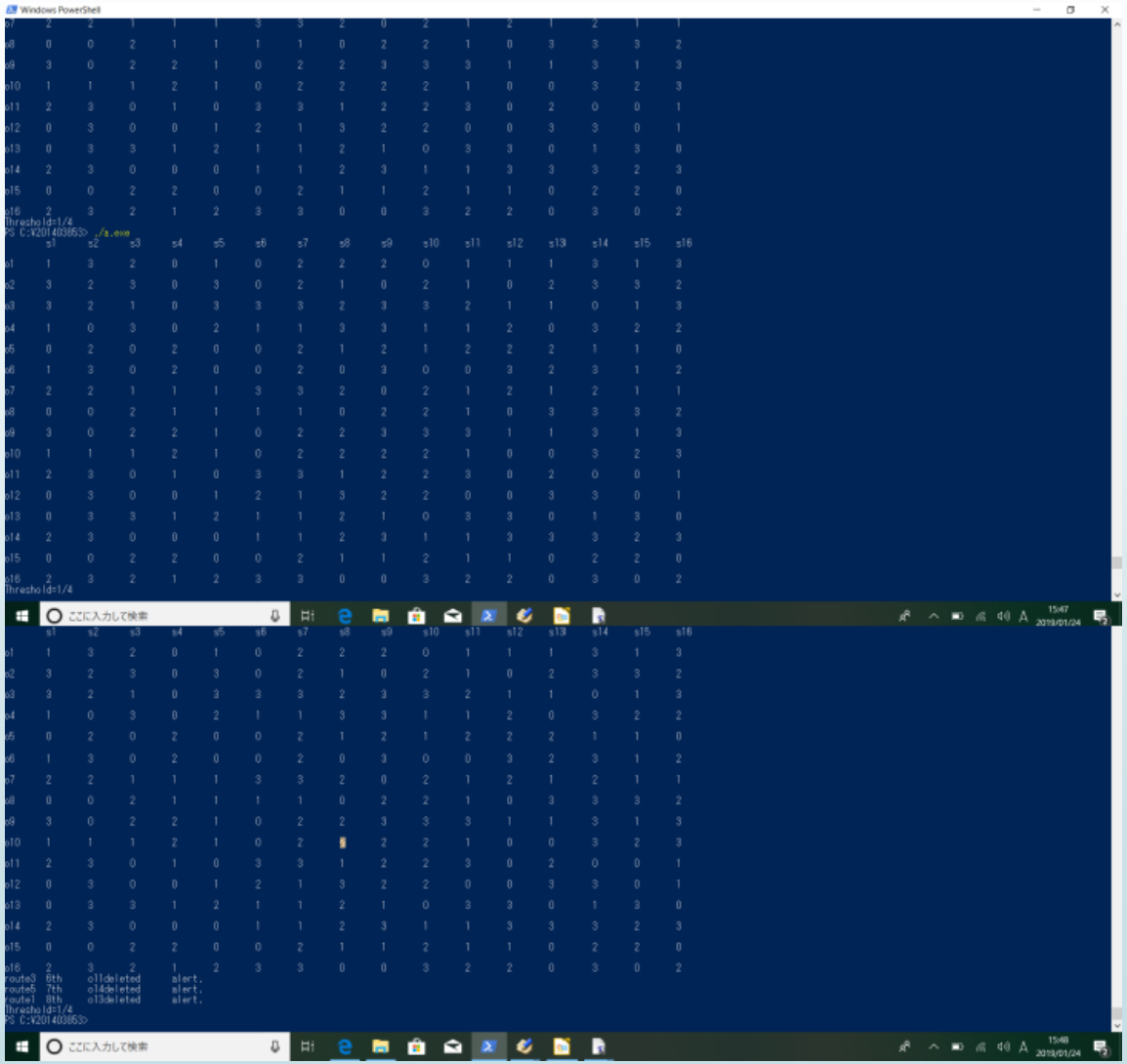


アクセス行列

route3 4th o11deleted alertは三番目の推論径路が4回目のアクセスで情報漏えいの可能性があり、o11へのアクセスを制限し、ユーザに警告を出すという意味

提案モデルをシミュレーションした結果

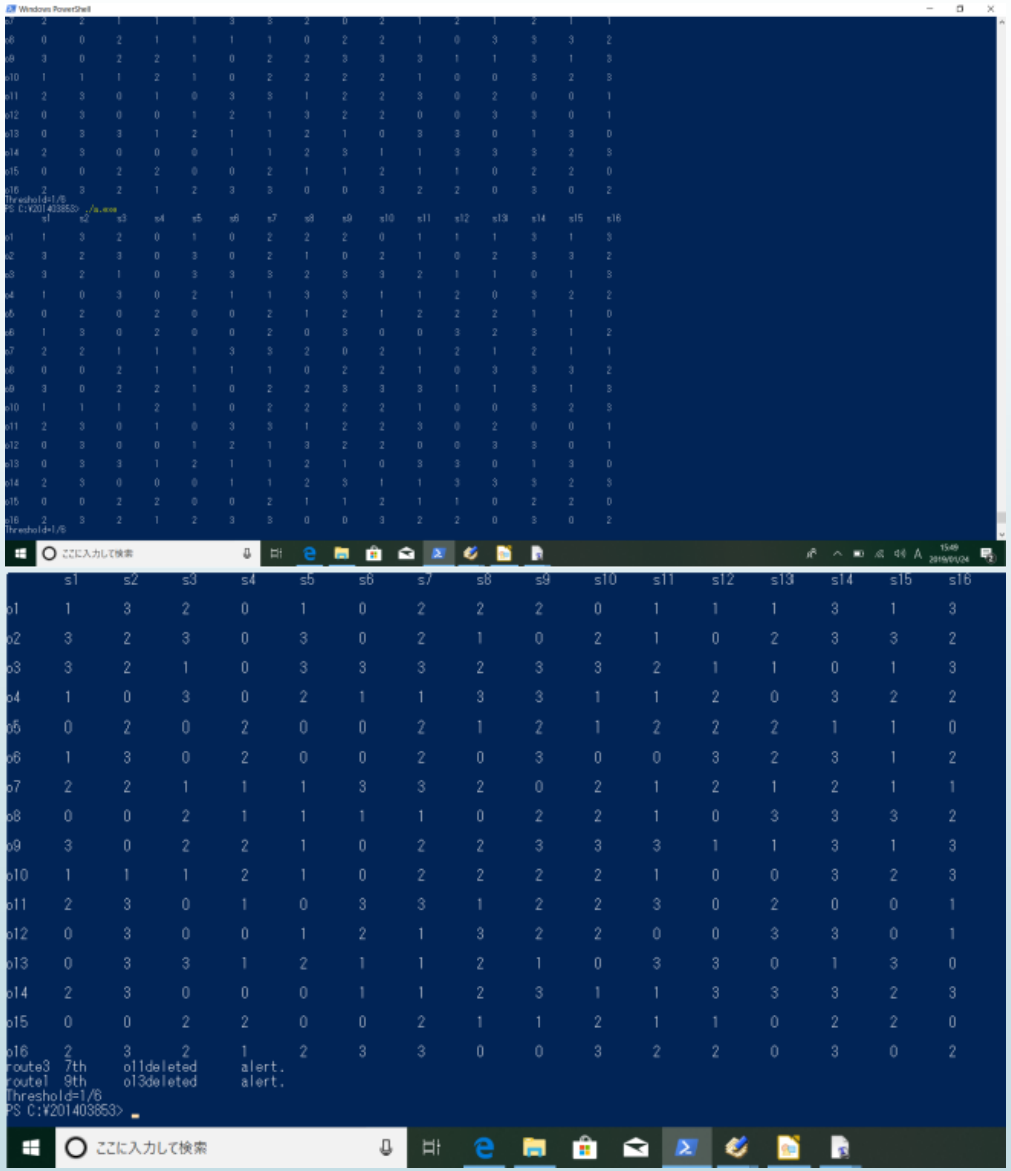
しきい値が1/4の場合



しきい値の分母が大きくなれば、警報が出るが出る頻度が低くなる。

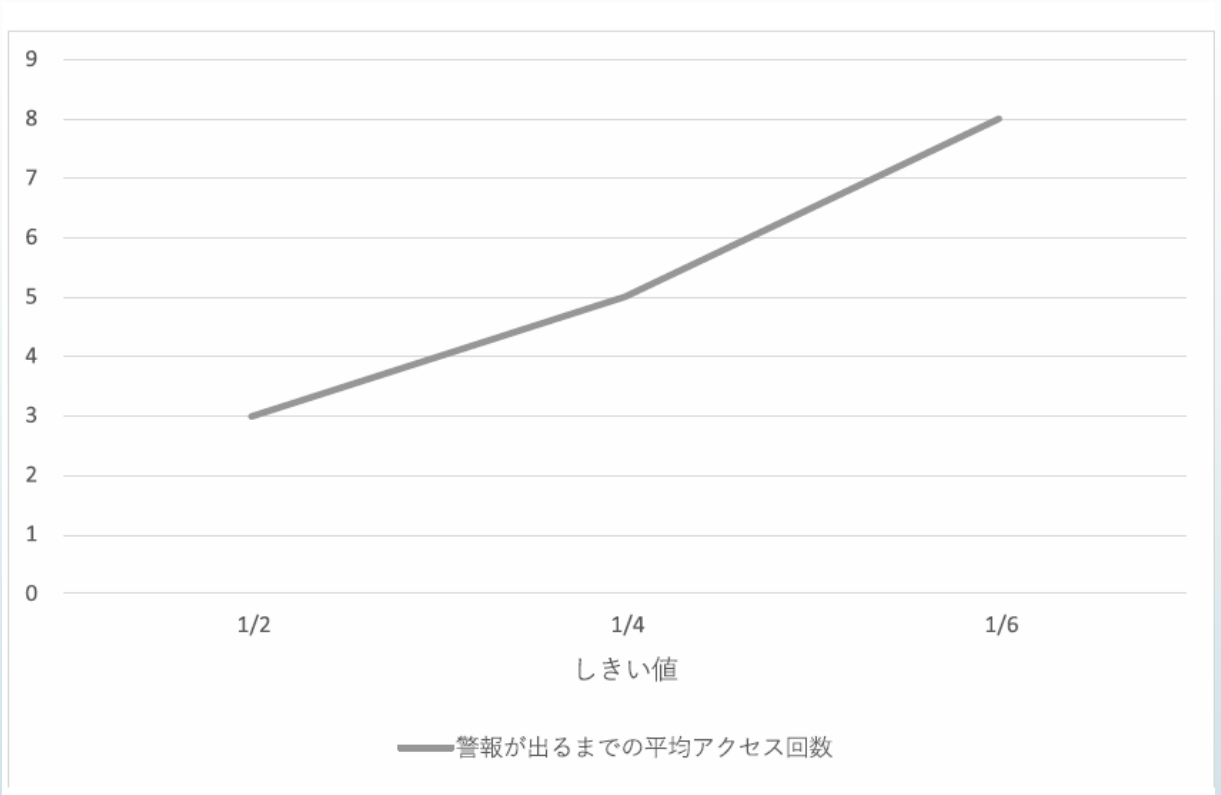
提案モデルをシミュレーションした結果

しきい値が1/6の場合



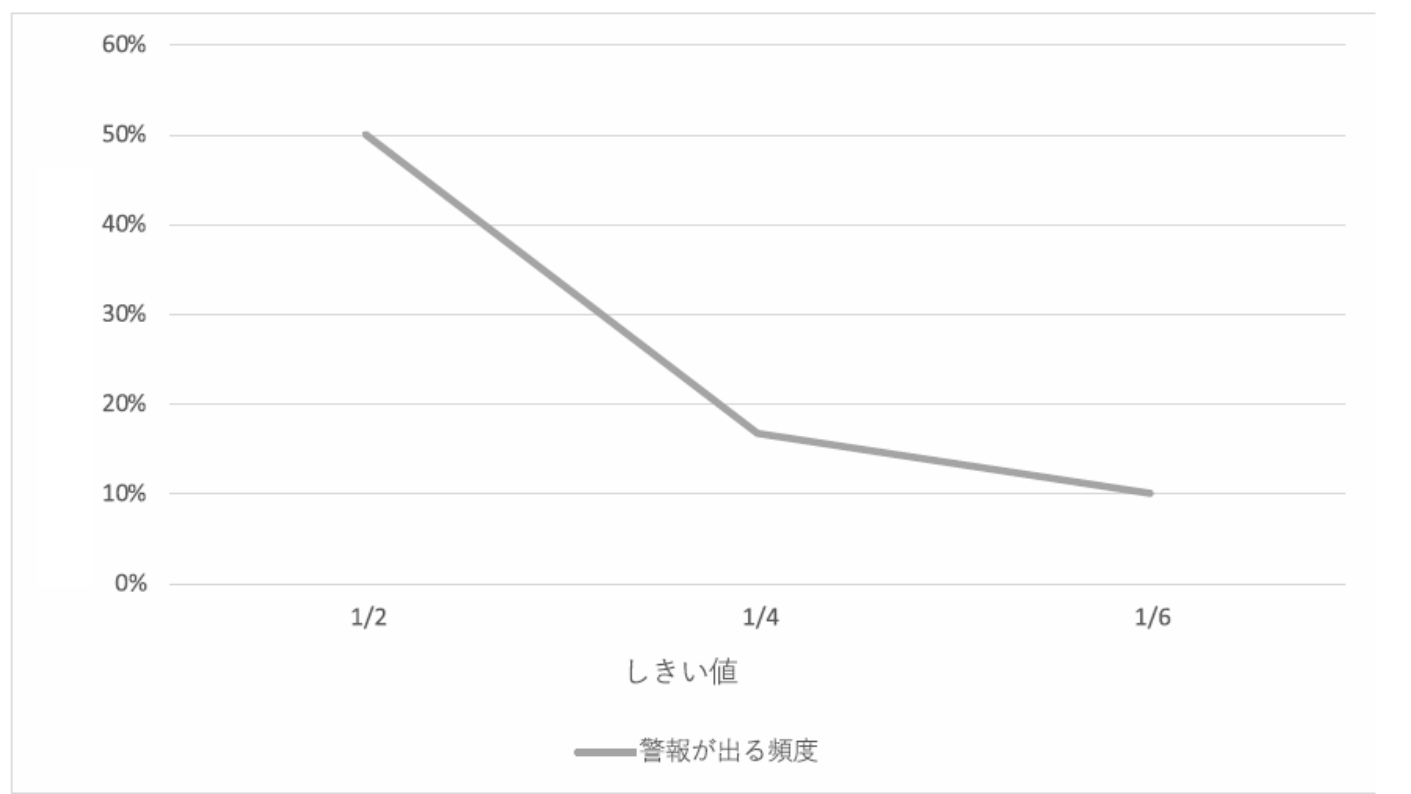
しきい値が1/6の場合でも、情報漏えいの可能性がある場合、アクセス制限がちゃんと行われている。

警報が出る場合のしきい値とアクセスの関係



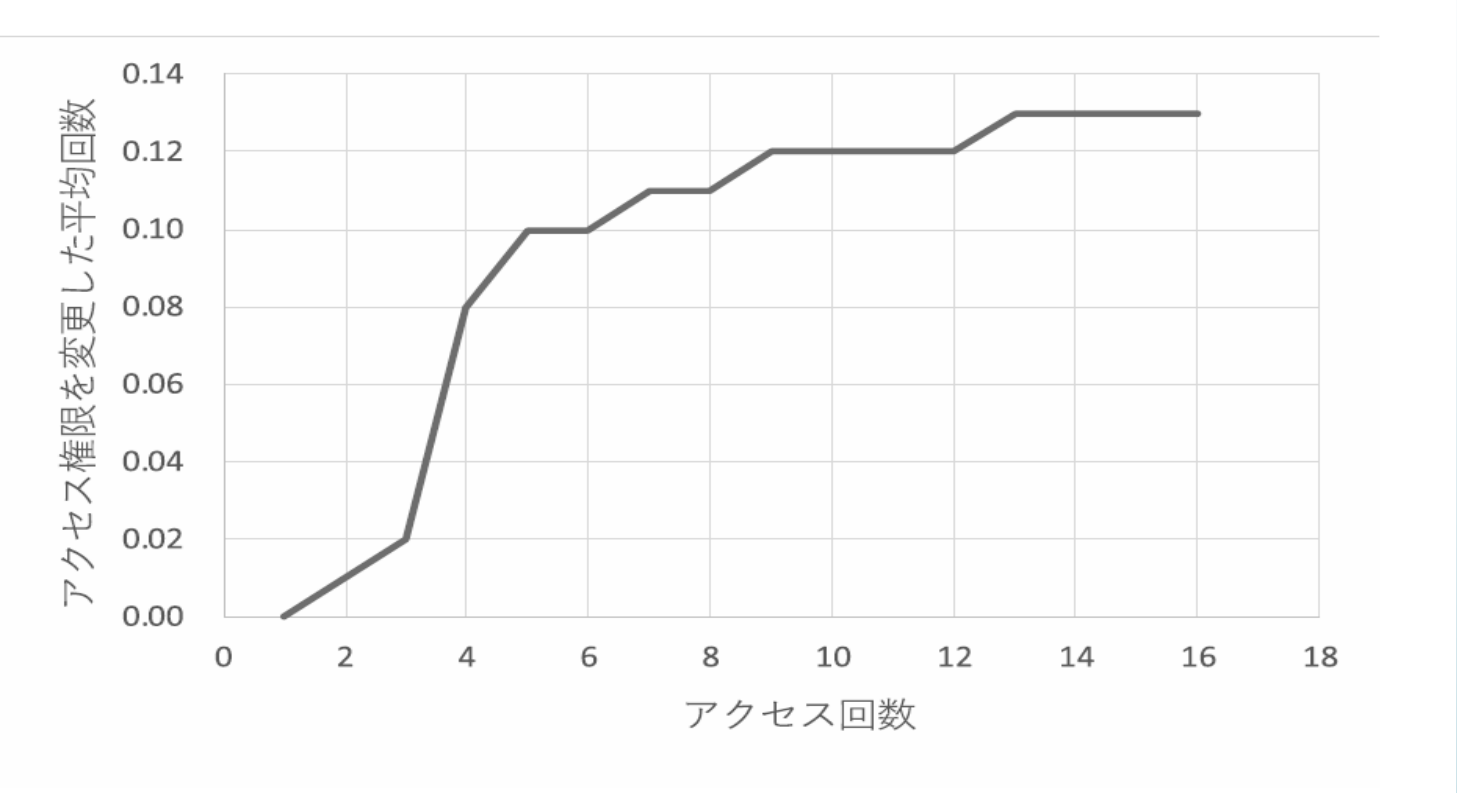
30回シミュレーションした中の、警報が出た回の結果を統計した。グラフからしきい値の分母が小さいほど、早い段階で警報がでる。

しきい値と警報が出る頻度との関係



グラフからしきい値の分母が大きいほど、警報が出る頻度が減ることがわかる。

アクセス回数と警告が出る回数の推移グラフ（しきい値＝1/6）の場合



グラフから、アクセス回数によらず、警報が出る回数が低い水準で安定している。というのは、情報漏えいの可能性がある場合、早い段階でアクセス制限を行っているから。したがって、情報漏えいの可能性がないにもかかわらず、一定数のアクセスが行われた場合、どの情報にもアクセスできなくなることはない。

考察

- シミュレーションの結果から、推論攻撃のリスクがある場合、推論径路の一端を開放を開放することによって、その推論径路から情報漏えいが発生しているのを未然に防げる。
- 一つの推論径路を開放しても、ほかの推論径路からの情報漏えいのリスクが起こる。
- しきい値の分母が大きいほど、警告が出ないシミュレーションの回数が増える。
- グラフにより、警告が出る頻度がアクセス回数が大きくなっても、低い水準で安定しているので、アクセス回数が極限に大きくなってもどのオブジェクトにもアクセスできなくなる心配はない。

まとめ

- どのタイミングでアクセスを制限するのか、また情報をどれくらい保護したいのかによって、しきい値を変更することで、様々な状況（アプリ）に対応できる。
- 個人が自分の情報が漏えいする可能性があると認識することによって、情報の不正利用（詐欺や架空の請求書など）に対応できる。
- 以上より、本システムは情報漏えいを未然に防ぎ、情報が漏えいすることによって発生する詐欺などの情報の不正利用を減らすのに役立つと結論付ける。
- 今後の課題としては、本システムに適した推論規則やすべての推論径路に対応したプログラムの開発がある。