ゼロトラスト環境の実現フレームワークの開発

Development of a framework for realizing a zero-trust environment

東京工科大学　コンピュータサイエンス学部　コンピュータサイエンス学科
サービスシステムデザイン研究室
宮田 陸杜
細野 繁

キーワード：ゼロトラスト,ブロックチェーン,分散

１．背景

従来のセキュリティモデルは社内ネットワークからのアクセスを完全に信用していた.しかしテレワークやクラウドの普及によりアクセスポイントの多様化が進んでいることからデータの漏洩やなりすましによる不正アクセスが多発しており,これらは企業の社会的信用が低下し,イメージを損なう原因になるため従来のセキュリティモデルが見直され,そこで注目されているのがゼロトラストというセキュリティモデルである.

２．課題

データの保証を実現させるゼロトラストを利用するための方法はまとめられていない為ゼロトラストを利用するための最小構成を考えパッケージングすることが必要であるが,いきなり完全なサーバレスにすると構成変更が多くなる為,ステップ 1 で認証サーバなし,認可サーバありステップ 2 で認証及び認可サーバなしと段階的にサーバレスにする.

３．ゼロトラスト

ゼロトラストとは社内ネットワークなど閉鎖的な場所であっても常に正しいアクセスであるかを検証するセキュリティモデルのこと.[1]

ゼロトラストを実現させる構成要素について次に述べる

３.1. 認証,認可

認証とはユーザが誰であるかを特定する行為がであり,認可とはユーザに何らかの権限を付与する行為である.[2]

３.２．ブロックチェーン

改ざんが非常に困難で取引履歴を消すことができないシステムのこと.取引履歴は鎖のように繋がり,データを相互に参照させていることで改ざんを防ぐことが出来る.[3]

図 1 ブロックチェーンのイメージ図

３.３．分散型台帳

端末同士で連携し,各自のデータベース(台帳)を同じ情報になるように共有する.コンセンサスアルゴリズムという方法で二重支払いや嘘の支払いなどが起きないように監視し合い,管理が分散されているためダウンしたとしても他のユーザがノードの一部として役割を果たしているので、残りのユーザでシステムの維持が可能である.

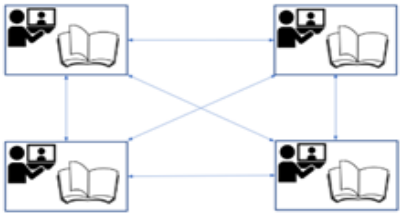

図 2 分散型台帳のイメージ図

３.４．分散型アイデンティティ(分散型 ID)

分散型台帳に個人の ID を書き込み,BC で情報の

改ざんを防ぐ方法のことで,企業が最も攻撃される要因としてユーザの ID 管理を企業が管理しており,年齢や購入履歴など個人情報を収集,保管している.そのため企業を攻撃すれば一度に大量の個人情報を盗むことができるため攻撃の的になりやすい.分散型 ID 管理では管理者が不在のため攻撃の的を作らず.ユーザは ID 管理を自分自身でることができる.[4]

5. 提案手法

ゼロトラストを利用するための必要な最小構成を考え実装していく.まず認証をサーバレスにし,ユーザ自身が ID を管理できる状態にする.BC には Hyperledger iroha を使用し,認可サーバには keycloak を使用する.

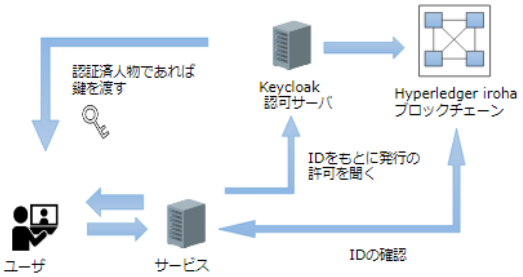

図 3 ゼロトラストの構成図

5.1 Hyperledger iroha

個人の ID を管理するのにあたって Hyperledger iroha を利用する.iroha は日本のソラミツ株式会社で開発されたオープンソースの BC フレームワークであり,ID やデジタルアセットの管理などが得意である.[5]

5.2 keycloak

認証や認可制御を実現させるオープンソースの ID アクセス管理ソフトウェアであり,ユーザ毎に属性や役職などを与えて管理することができる為ある役職のみに認可を与えるなど細かい設定を実現させるために使う.[6]

6. 検証

iroha を同一のマシン内に 3 台用意し各端末を連携させ BC ネットワークを作成する.3 台に分散された iroha がデータを共有できているかを確認し,テストアカウントに情報を書き込み,keycloak が情報をもとに認可を制御出来るか試す.

はじめに iroha が連携できているかを確認する.

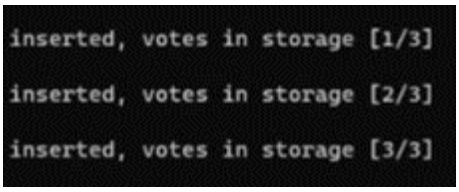

図 4 iroha が 3 台に分散している図

図 4 では 3 台の端末の連携できていることがわかる.更にこの状態から名前や年齢のデータを 1 つの端末から書き込み他の端末で確認できた為データベースの連携もできていることがわかった.

7. 考察

ゼロトラスト環境構築のための提案を考えたが認可制御の検証が終わっていないためまずは keycloak と iroha の連携を目指していく.

8. 今後の計画

Iroha のデータを json 形式で keycloak に渡し,そのデータから keycloak が認可制御を行えるようにする.

9. 参考文献

[1]Evan Gilman,Doug Barth,鈴木研吾(翻訳),ゼロトラストネットワーク―境界防御の限界を超えるためのセキュアなシステム設計,オライリー・ジャパン,2019 年 10 月 25 日,283 ページ

[2]認証と認可の違いとは | セキュリティの強化について説明,かもめエンジニアリング,かもめエンジニアリング株式会社,参照 2022 年 7 月 12 日,https://onl.bz/bjL2tdb

[3]tradeshift,
ブロックチェーンの仕組みとは？図解で知る基礎知識,2018 年 6 月 20 日,参照 2022 年 10 月 17 日,
https://jblog.tradeshift.com/blochkchain-zukai/

[4]https://diacc.ca/faq/,diacc,
Digital ID & Authentication Council of Canada,参照 2022 年 8 月 21 日,
https://diacc.ca/

[5]コネクト (監修), 佐藤 栄一,Hyperledger Iroha 入門:ブロックチェーンの導入と運営管理,オーム社.2020 年 2 月 12 日,288 ページ

[6]中村雄一,和田広之,田畑義之,田村広平,青柳隆,認証と認可 Keycloak 入門,リックテレコム 2022 年 1 月 31 日,464 ページ