ユーザの信用評価に基づく ゼロトラストネットワークの実装と評価

先端科学技術研究科 博士前期課程２年
河合 将隆 <kawai.masataka.kl6@is.naist.jp>

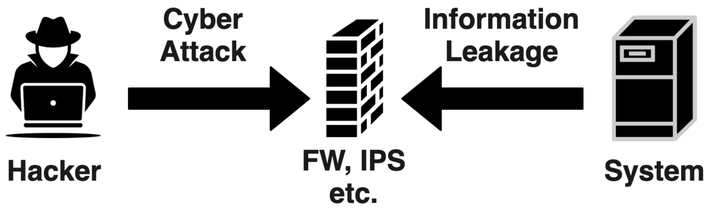
iplab Laboratory for Cyber Resilience

Nara Institute of Science and Technology NAIST

Background & Motivation

境界型セキュリティモデルの限界

➢ 組織の情報システム保護において，現行の主流である境界型モデルは様々な要因から弱点が指摘されている



- 境界での完璧な防御は不可能
  境界内部に脅威が存在しないことが前提であり，一度侵入を許せば他の端末に被害が拡大する
- テレワークによる外部アクセス需要の高まり
- 内部不正の脅威

ゼロトラストネットワーク(ZTN)とは

➢ 信用の概念を取り入れたセキュリティモデル
➢ 下記コンセプトから前述の問題が抑制できるとされている
1. 場所に関係なく全リソースに安全にアクセスできる
2. 最小特権の原則を採用する
3. 全ての通信を検証し，記録する
「認証を必須とし，たとえ認証されたユーザからのアクセス要求であったとしても，そのユーザが正しいことをしているか常に検証する」

➔ どのように通信の検証を行うのか，どのようなユーザが正しいことをしていると判断できるのかについては言及されていない

ZTNのコンセプトに基づくアクセス制御システム

➢ 通信の検証を行い信用できるアクセスのみを通すシステム
➢ ZTNを謳う殆どの先行研究では，システムの構築技術がメイン．通信の検証について言及しているものも，脆弱性情報などユーザに関連しない要素を使用している

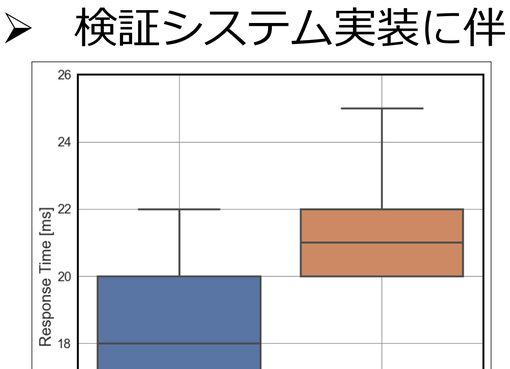
➔ ユーザが正しいことをしているかの検証(ユーザの信用評価)には至っておらず，内部不正等への対策として未だ不安が残る
➔ ユーザの信用評価を行うアクセス制御システムが実現すれば内部不正等を抑制できるという仮説のもと，このシステムの実現を試みる
対象範囲：社内システムからの機密情報の漏洩

Result

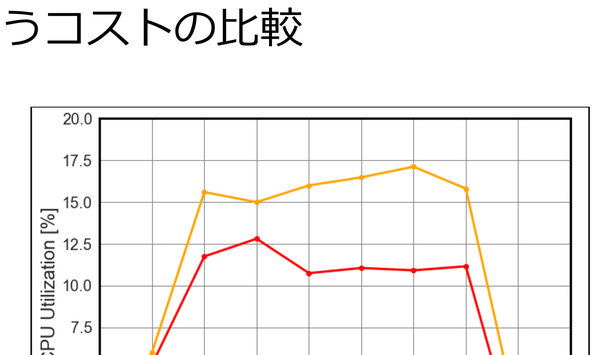
➢ 各ユースケースに基づくアクセス制御の検証

```
172.30.0.2 - - [10/Feb/2021 13:49:54] "POST / HTTP/1.1" 200 -
Request Data: {'X-Forwarded-For': '172.28.0.1', 'Request-Host': 'redmine'
, 'Request-Uri': '/projects/naist_project/dmsf?folder_id=4', 'User': 'Kim
uraMasao', 'Role': 'Development'}
Number of times accessed: {'rainloop': 0, 'idempiere': 0, 'redmine': 18}
Trust Score: 95.5
{'message': 'OK'}
```

➢ 検証システム実装に伴うコストの比較



サーバ応答時間の比較



CPU使用率の比較

Proposed Idea and Methodology

ユーザの信用を評価する上でどのような要素が必要か

➢ 企業のセキュリティ担当者47名に演習を実施．考え出されたユーザの信用要素の内，大勢に共通する要素を採用

接続元場所，ネットワーク
接続時の時間
・
・

ユーザの信用をどのように評価するか

➢ NISTの信用評価方法の定義に則りスコアベースの信用アルゴリズム(TA)を採用
➢ 各信用要素で異常と見られる場合に制限的なアクセスとなるよう，減算によるスコア算出

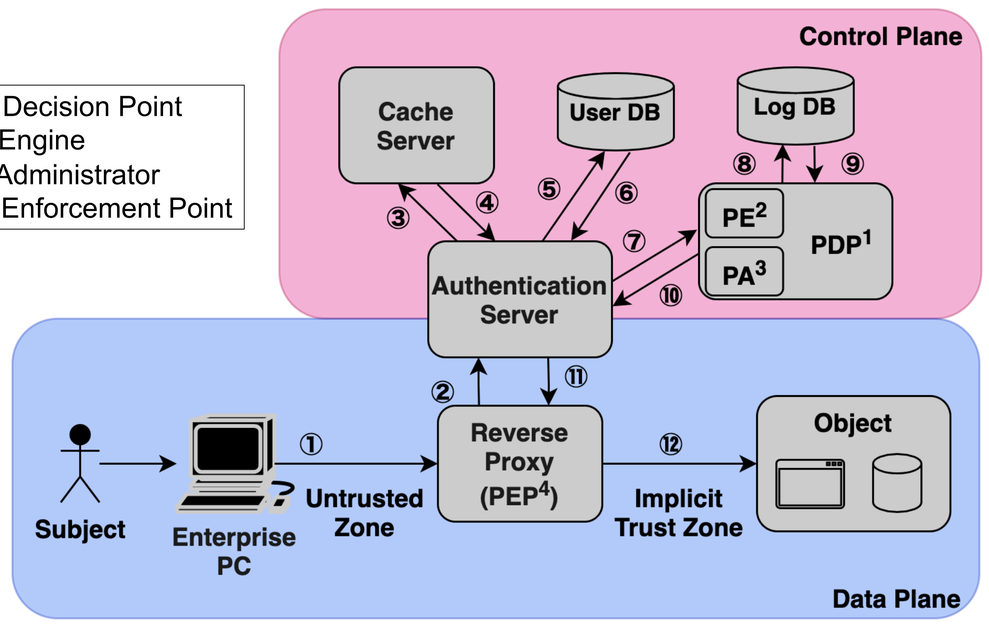
ユーザの信用評価方法をどのように有用性検証するか

➢ 仮想企業設定による各信用要素の具体化
➢ ユースケース設定による各信用要素の探索空間の網羅

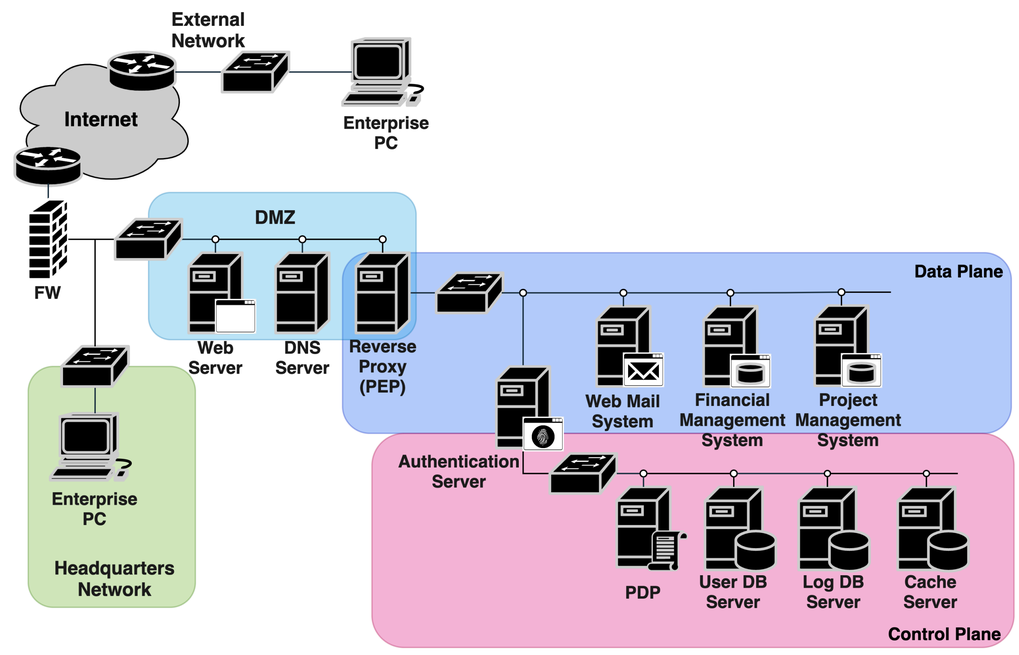
ZTN検証システムの設計と実装

➢ 検証に供することのできるシステムが存在しないため，先行研究を参考に論理構成を設計

[1]PDP: Policy Decision Point
[2]PE: Policy Engine
[3]PA: Policy Administrator
[4]PEP: Policy Enforcement Point

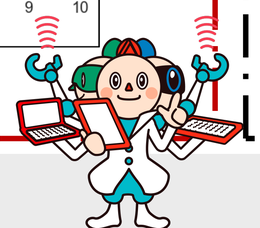


➢ 仮想企業の社内システムに対し検証システムを実装



Conclusion and Future Work

➢ 内部不正等抑制のために，ZTNのコンセプトに基づきユーザの信用評価を行うアクセス制御システムの実現を目指した．ユーザの信用要素，信用評価方法について検討し，ユースケースに基づく有用性検証を行った
➢ 検証の結果，想定した全てのユースケースでアクセス制御を達成した．しかし，本手法での適応限界等も見えた

今後の課題

➢ 新たな信用要素の追加
➢ 特異なユースケースへの対応
➢ Ajax等特定の実装方式を採用するWebシステムへの対応