

2021年度修士論文等発表会  
2022/2/19

# ゼロトラストアーキテクチャにおける ブラウザフィンガープリントを利用した アクセス制御

大久保研究室 M2

高木祥一

# 目次

- 背景
- ゼロトラスト
- 先行研究
- 提案手法
- 提案手法の実装と評価
- まとめと今後の課題

- 背景
- ゼロトラスト
- 先行研究
- 提案手法
- 提案手法の実装と評価
- まとめと今後の課題

## ■ ゼロトラスト(2010年に提唱)

- 全てのリソースを検証して安全を確保
- アクセス制御を厳格に実施
- 全てのトラフィックを検査して記録

グローバル、モバイル、リモート、クラウドが主流な近年、  
更にセキュアにするための概念として注目を集めている

- ゼロトラストアーキテクチャに関する文書がNISTより発行
- 概念の定義が主であり、実装方法においては具体性が乏しい

## ゼロトラストの考え方

- 1 全てのデータソースとコンピューティングサービスをリソースとみなす
- 2 ネットワークの場所に関係なく、全ての通信を保護する
- 3 企業リソースへのアクセスは、セッション単位で付与する
- 4 リソースへのアクセスは、クライアントアイデンティティ、アプリケーション/サービス、リクエストする資産の状態、その他の行動属性や環境属性を含めた動的ポリシーにより決定する
- 5 全ての資産の整合性とセキュリティ動作を監視し、測定する
- 6 全てのリソースの認証と認可を動的に行い、アクセスが許可される前に厳格に実施する
- 7 資産、ネットワークインフラストラクチャ、通信の現状について可能な限り多くの情報を収集し、セキュリティ態勢の改善に利用する

## 企業リソースへのアクセスは、セッション単位で付与する

- 頻繁なアクセス元の信頼性評価が必要
- ユーザビリティの低下は防ぎたい
- ブラウザフィンガープリントに着目
  - ブラウザ識別の研究にて利用されている
  - JavaScriptで自動取得ができる
  - 継続して同じならば、同一環境利用の確度が高い

ブラウザフィンガープリントを用いたアクセス制御手法を提案

**Fingerprints.js2**

Get my fingerprint

Your browser fingerprint:  
**b30562e0dd23414123afd53df5d5e930**

Time took to calculate the fingerprint: 440 ms

Detailed information:

```
userAgent = Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:59.0) Gecko/20100101 Firefox/59.0
webdriver = false
language = ja
colorDepth = 24
deviceMemory = not available
hardwareConcurrency = 2
screenResolution = 1920,1080
availableScreenResolution = 1920,1080
timeZoneOffset = -540
timezone = Asia/Tokyo
sessionStorage = true
localStorage = true
indexedDB = true
addBehavior = false
openDatabase = false
cpuClass = not available
platform = Win32
plugins =
canvas = canvas (vendor:yes, canvas fp:data:image/png;base64,iVBORw0RGQoAAAN3UeUghp8AAANdCvYAAACGncB
webgl = data:image/png;base64,iVBORw0RGQoAAAN3UeUghp8AAANdCvYAAACGncB
webglVendorAndRenderer = Google Inc.-ANGLE (AMD Radeon(TM) RX Vega 10 Graphics DirectX3D11 vs_5_0 ps_5_0)
hasLiedLanguages = false
hasLiedResolution = false
hasLiedOs = false
hasLiedBrowser = false
touchSupport = 0, false, false
fonts = Arial, Arial Black, Arial Narrow, Book Antiqua, Bookman Old Style, Calibri, Cambria, Cambria Math, Century
audio = 35.7383295930922
```

# 目次

- 背景
- **ゼロトラスト**
- 先行研究
- 提案手法
- 提案手法の実装と評価
- まとめと今後の課題

## ■ ゼロトラスト

- ネットワークが侵害されている場合であっても、情報システムやサービスにおいて、各リクエストを正確かつ最小の権限となるようにアクセス判断する際の不確実性を最小化するために設計された概念とアイデアの集合体。

## ■ ゼロトラストアーキテクチャ(ZTA)

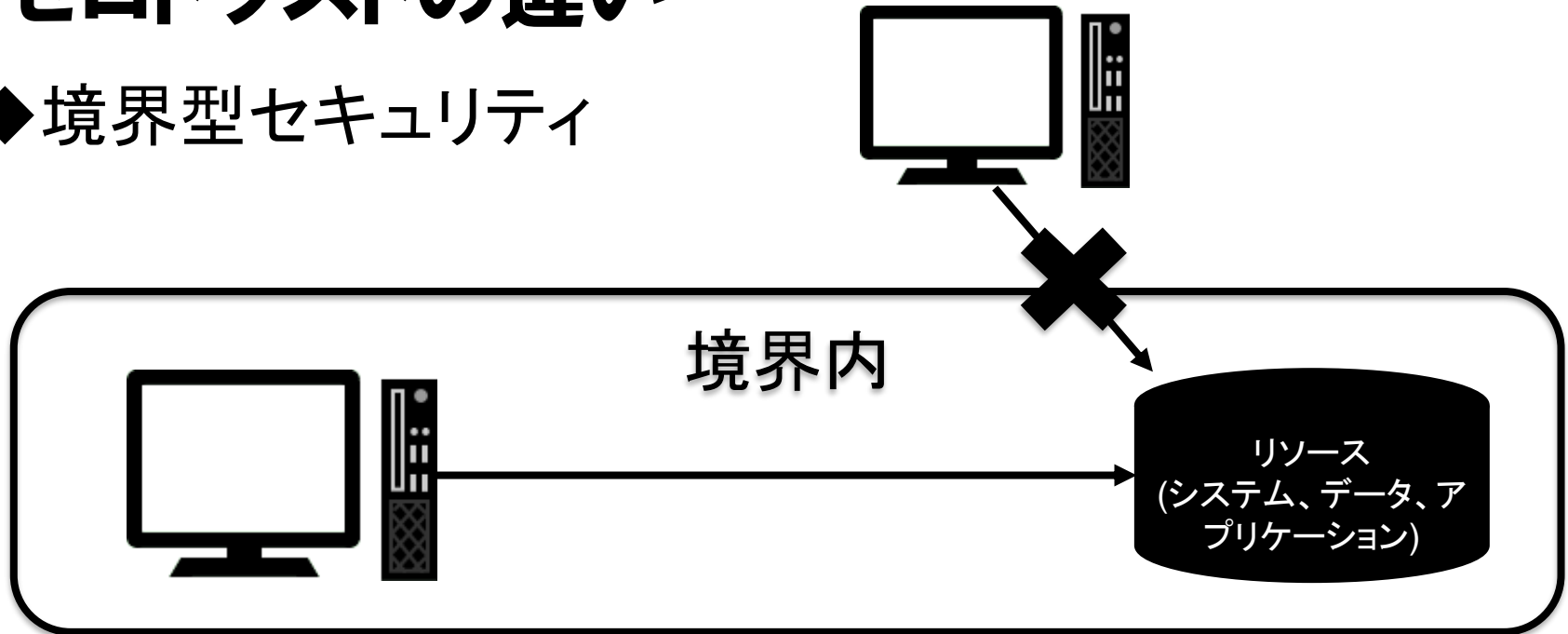
- ゼロトラストの概念を利用し、コンポーネントの関係、ワークフロー計画、アクセスポリシー等を含むサイバーセキュリティ計画。ゼロトラスト企業とは、ゼロトラストアーキテクチャ計画の産物として、組織のネットワークインフラストラクチャと運用ポリシーを指す。



# 境界型セキュリティと ゼロトラストの違い



## ◆境界型セキュリティ

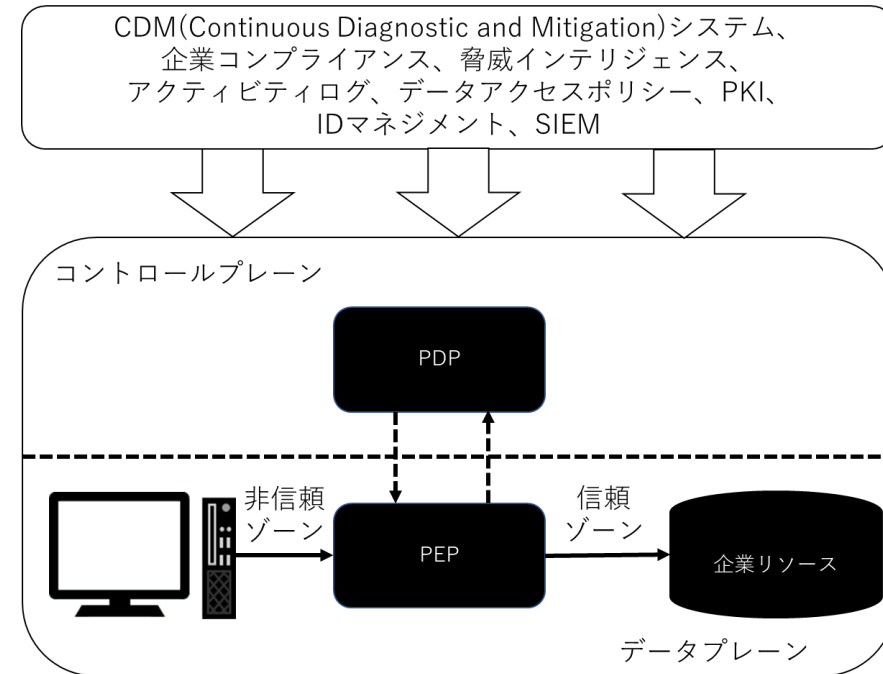


## ◆ゼロトラスト



# ZTAコンポーネント

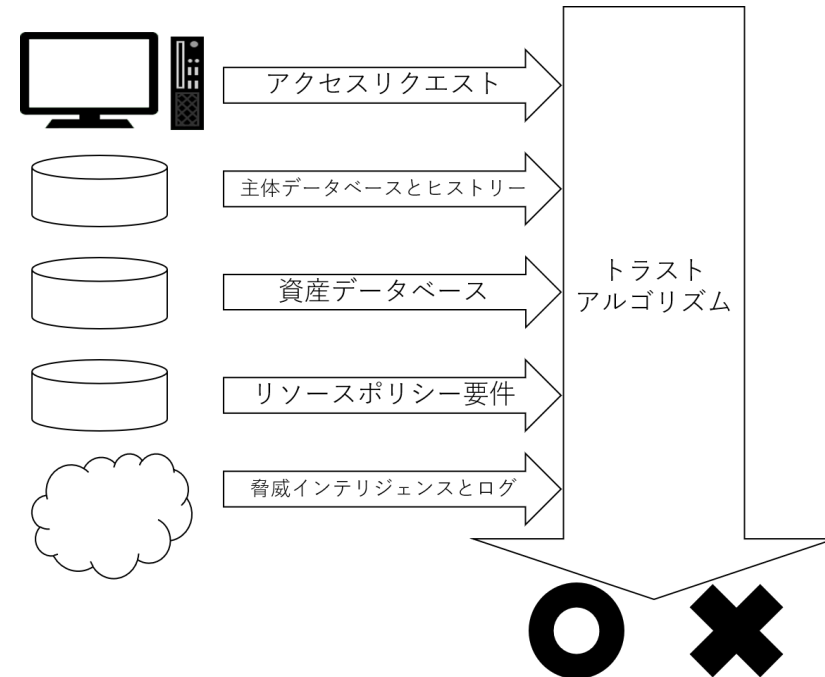
- ポリシー決定ポイント  
(Policy Decision Point: PDP)
  - ポリシーと外部ソースを入力としてリソースへのアクセス可否を判定。
- ポリシー実施ポイント  
(Policy Enforcement Point: PEP)
  - リソースへのアクセスを受け取り、PDPの結果を反映。



# トラストアルゴリズム

- リソースへのアクセスを最終的に判断するPDPのプロセス
- 複数ソースを入力として受け付ける

- 外部ソースや判定方法に具体的なものはなく, ZTAを構築する組織にゆだねられている
- ZTA実装難易度を引き上げる要因にもなっている



# 目次

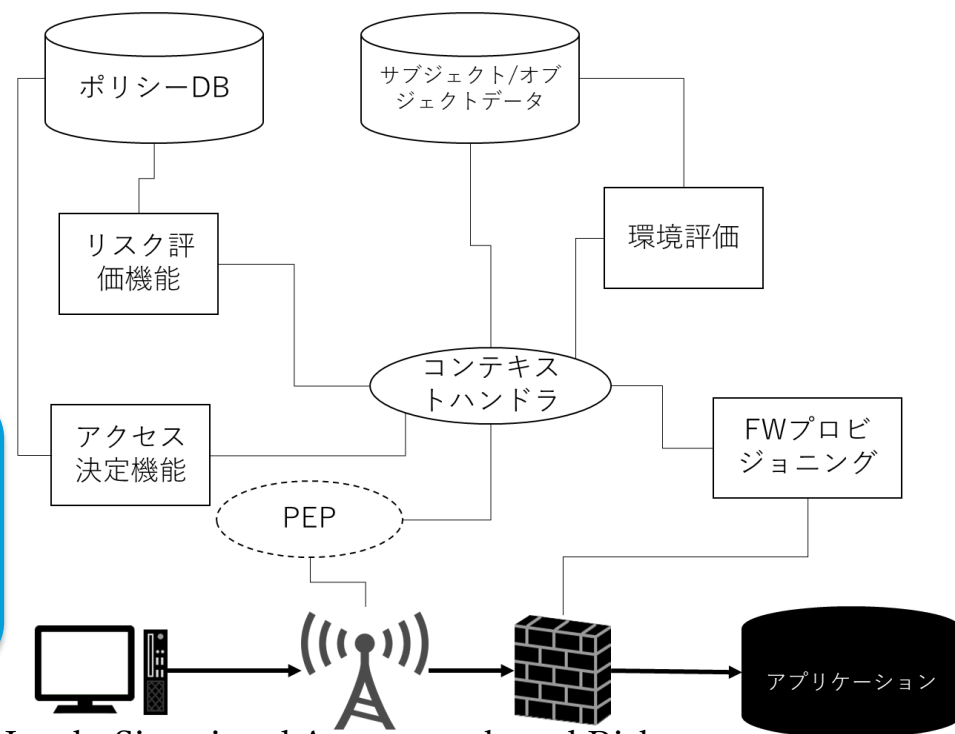
- 背景
- ゼロトラスト
- **先行研究**
- 提案手法
- 提案手法の実装と評価
- まとめと今後の課題

# 先行研究 (ゼロトラスト)

## ■ PDP/PEPにリスクベースアクセス制御を取り入れるための研究

- ポリシー実行  
フレームワークの提案
- ファジィ論理の採用
- ポリシー言語の設計

具体的な検討を行っているものの、フレームワーク実装の評価実験は行われていない。



Brian Lee, Roman Vanickis, Franklin Rogelio, and Paul Jacob. Situational Awareness based Risk-Adaptable Access Control in Enterprise Networks. pp. 400–405, 10 2017.

Romans Vanickis, Paul Jacob, Sohelia Dehghanzadeh and Brian Lee, "Access Control Policy Enforcement for Zero-Trust-Networking," 2018 29th Irish Signals and Systems Conference (ISSC), Belfast, 2018, pp.1-6

# 先行研究 (ゼロトラスト)

- リソースアクセス元の継続的な検証によるアクセス制御
- User Portraitを取得し続け、行動の乖離度を判定

乖離度のしきい値の設定には継続的な調整が必要

## User Portrait

動作タイプ	特定の動作
ログイン動作	ログイン方法
	ログイン時間
	ログイン間隔
	ログインデバイス
	ログインIP
ネットワーク動作	上りトラフィック
	下りトラフィック
	TCPコネクション密度
操作動作	アクセスリソース名
	操作履歴

- Eckersleyの研究 – How unique is your web browser? (2010年)  
ブラウザフィンガープリントを採取するサイトを構築し、83.6%がユニークである旨を発表
- 田邊らの研究 – Browser fingerprintingにおける特徴の組み合わせに関する考察 (2017年)  
ブラウザ識別精度が最良となる特徴量の組み合わせを検討
- 神らの研究 - ブラウザフィンガープリンティングを用いたVM上のブラウザによるアクセス識別の試み (2020年)  
仮想マシン上のブラウザからのアクセスを識別する手法の提案

ブラウザ識別に関する研究に利用されており、  
アクセス元の識別がしやすい特徴を持つ

# 目次

- 背景
- ゼロトラスト
- 先行研究
- **提案手法**
- 提案手法の実装と評価
- まとめと今後の課題



## ■ Webサイトとアクセス元の間でブラウザフィンガープリントの値 (BFP値) の検証を実施

- リクエストと共にBFP値を送信
- 検証済のリクエストのみをWebサイトへ転送

BFP値を利用した  
アクセス制御

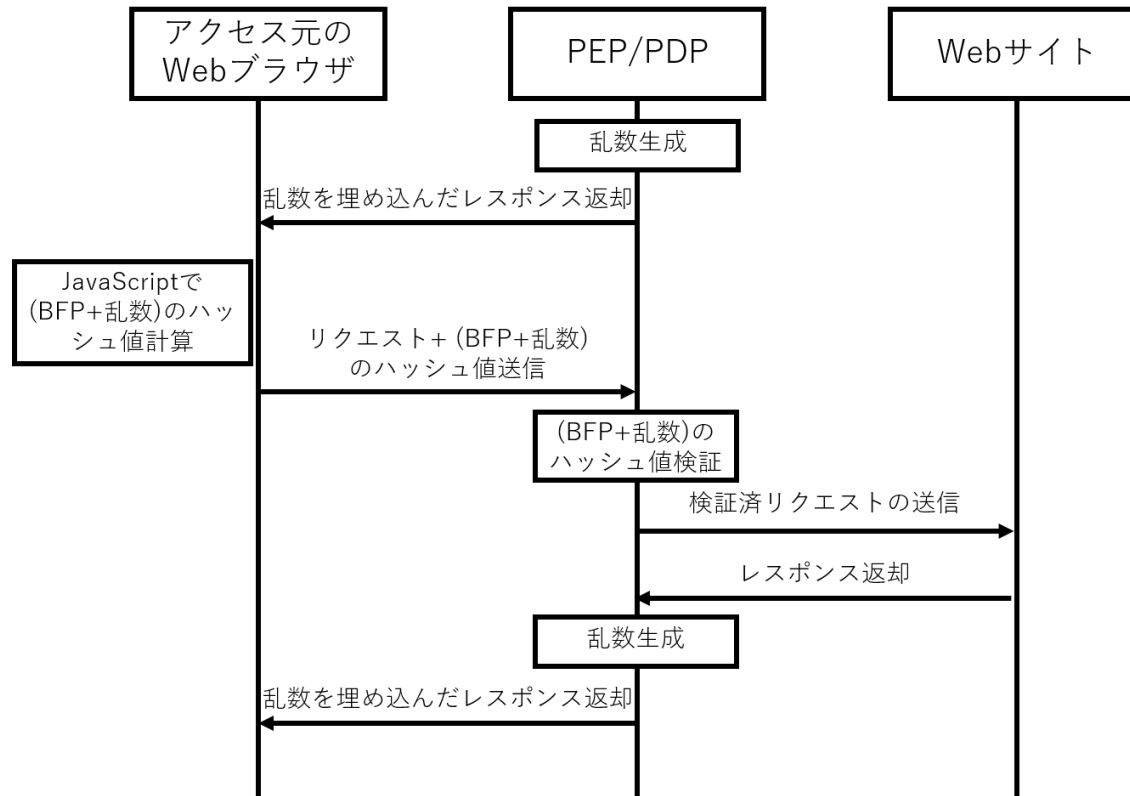


## ■ 提案手法の適用対象は、企業リソースを格納しているWebサイト

- JavaScript無効等の機能でBFP値の取得が阻害されないことが前提

# BFP値の偽装対策

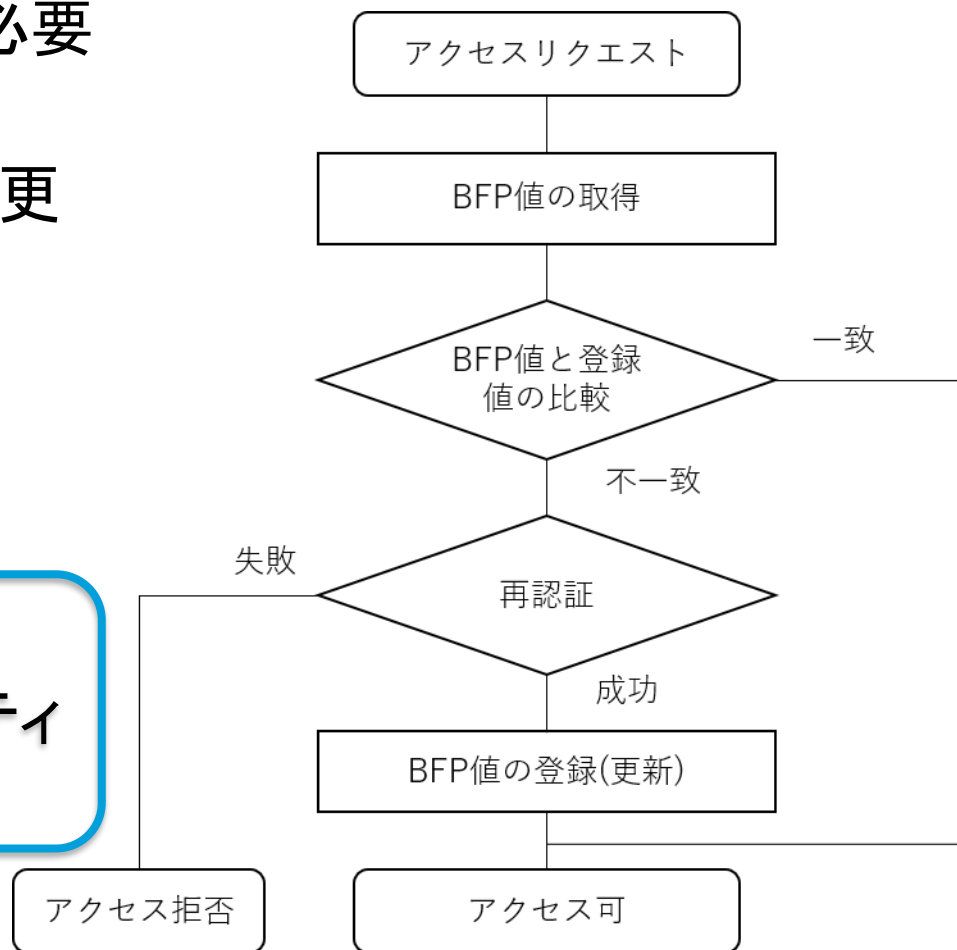
- BFP値の送信に，チャレンジレスポンス方式を導入
  - 乱数を利用することでBFP値を素のまま利用しない



# 提案手法による検証フロー

- BFP値は同じ値であり続ける保証がないため、更新可能である必要あり
- BFP値が不一致の場合、登録更新前に別の認証を実施
  - 別値の利用が必須
  - 別要素の利用は推奨

課題：BFP値が変化しやすい性質を持っているとユーザビリティに影響あり

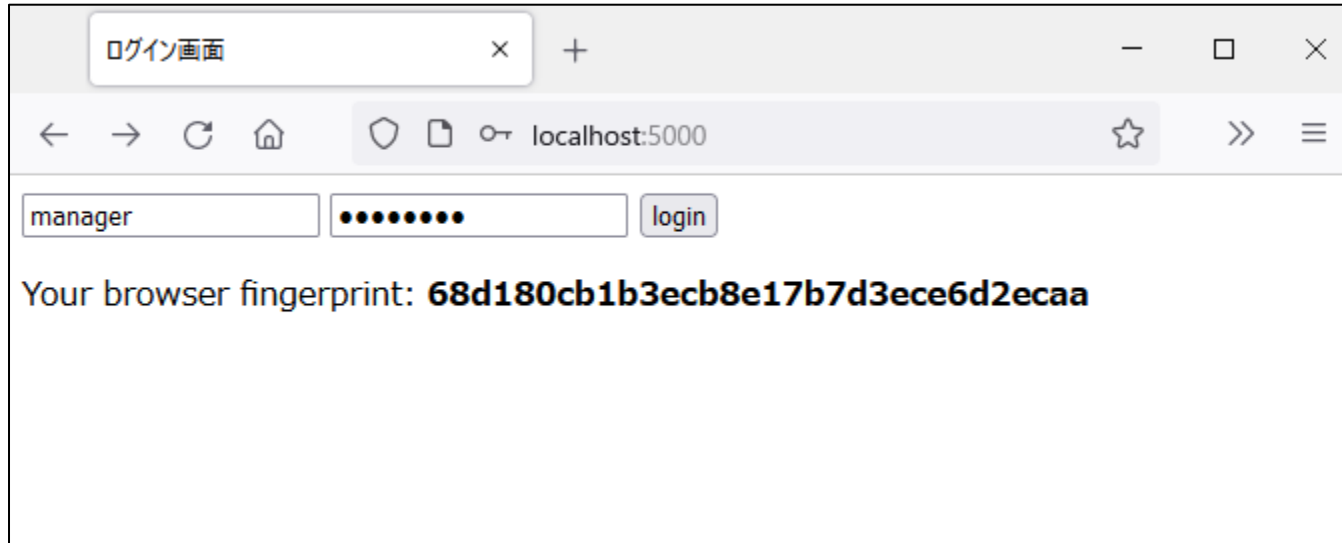


# 目次

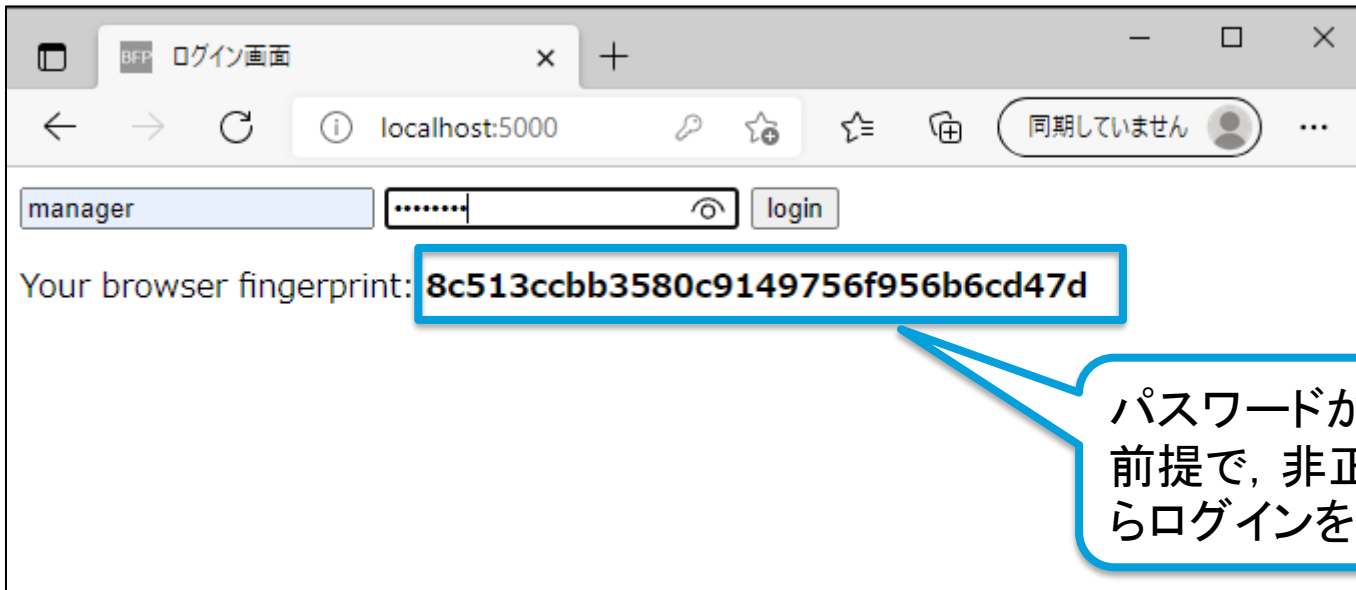
- 背景
- ゼロトラスト
- 先行研究
- 提案手法
- **提案手法の実装と評価**
- まとめと今後の課題

- Python, Flask, Flask-Login, SQLiteを用いて提案手法を実装したWebサイトを構築
- BFP値の取得にはFingerprintjs2を利用
  - Githubで公開されているオープンソース
  - 28種類の要素からBFP値を生成
- BFP値不一致の場合, ログイン時とは別パスワードを求める画面に遷移する設計
- 以下の不正アクセスによる検知を実証
  - クレデンシャルスタッフィング
  - Cookieハイジャック

# 不正アクセスの検知: クレデンシャルスタッフィング



# 不正アクセスの検知: クレデンシャルスタッフィング



manager  login

Your browser fingerprint: **8c513ccbb3580c9149756f956b6cd47d**

パスワードが漏えいした  
前提下で、非正規環境か  
らログインを実施

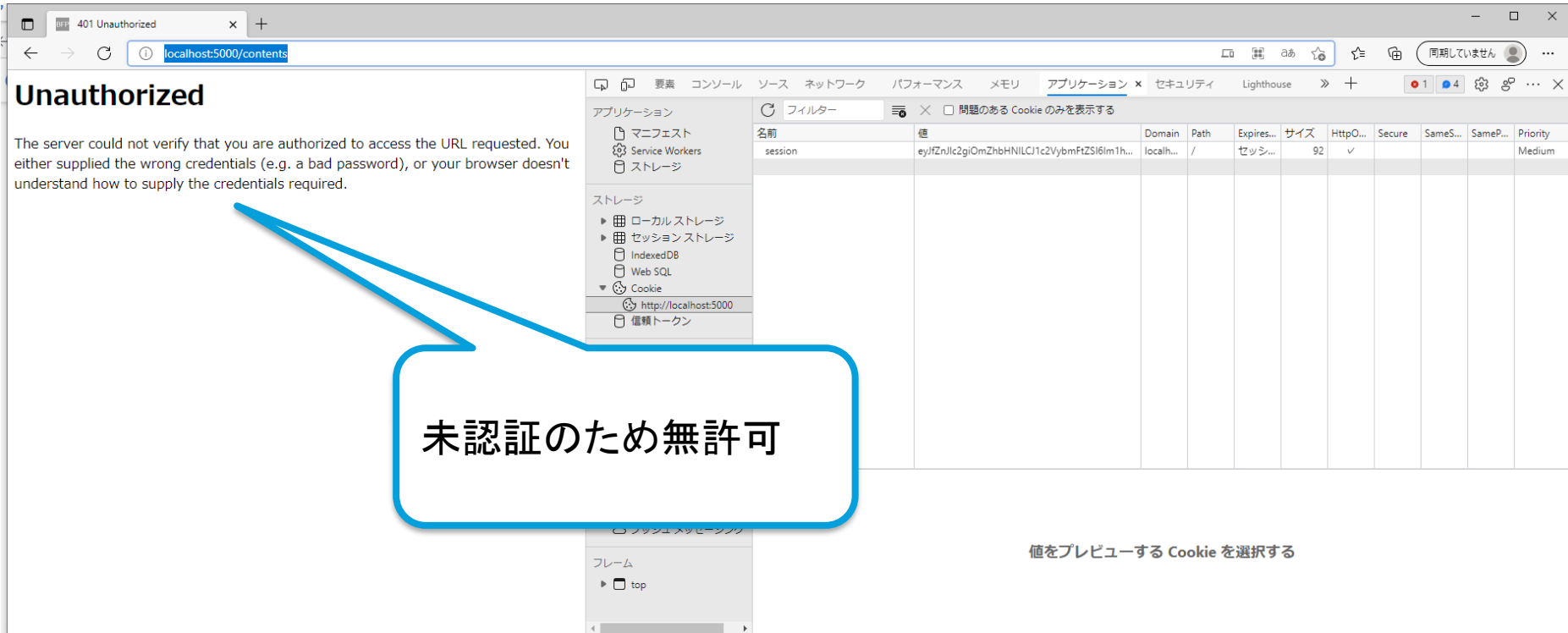


登録されていない環境からのアクセスを検知しました。第二要素のパスワードを入力してください。

Your second password  Submit

Your browser fingerprint: **8c513ccbb3580c9149756f956b6cd47d**

# 不正アクセスの検知: Cookieハイジャック



The server could not verify that you are authorized to access the URL requested. You either supplied the wrong credentials (e.g. a bad password), or your browser doesn't understand how to supply the credentials required.

未認証のため無許可

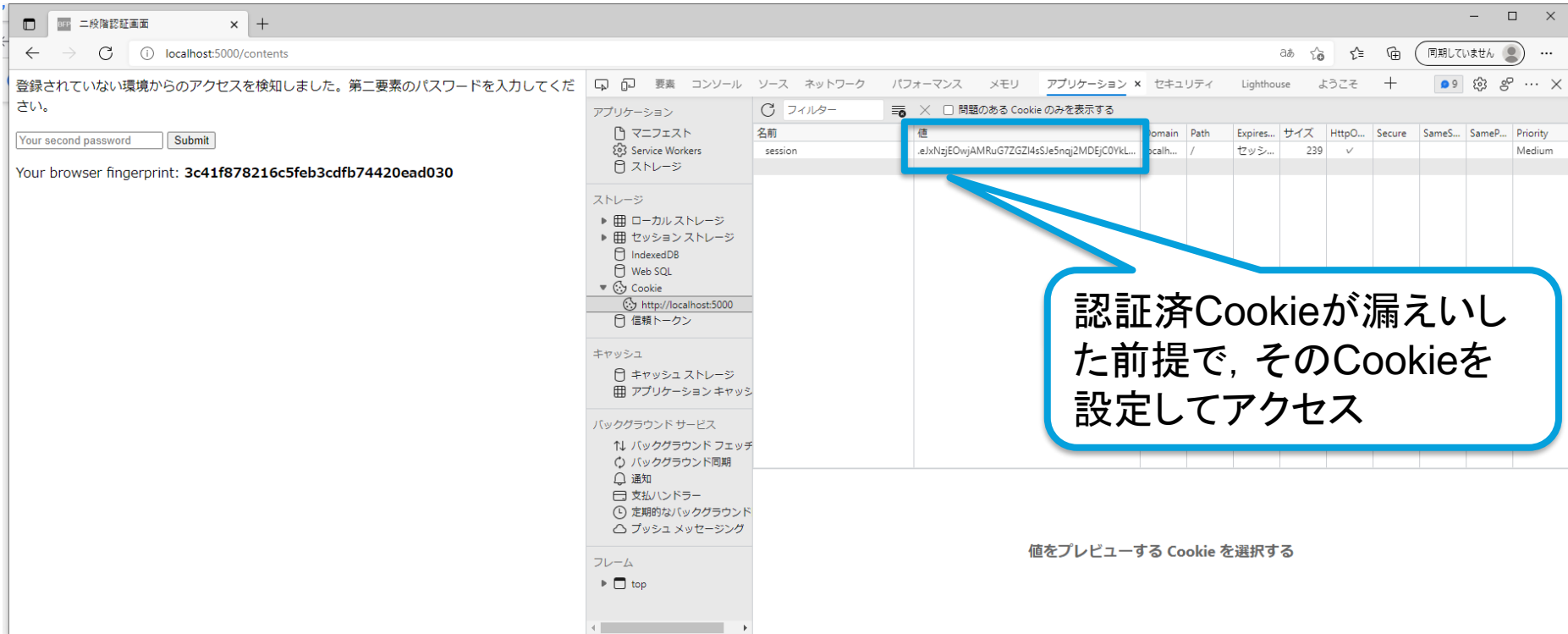
名前	値	Domain	Path	Expires...	サイズ	HttpO...	Secure	SameS...	SameP...	Priority
session	eyJfZnJlc2giOmZhbHNlLCJ1c2VybmFtZSI6Im1h...	localh...	/	セッシ...	92	✓				Medium

値をプレビューする Cookie を選択する

※Flask-LoginはCookieでログイン状態を管理



# 不正アクセスの検知: Cookieハイジャック



The screenshot shows a web browser window with a security warning: "登録されていない環境からのアクセスを検知しました。第二要素のパスワードを入力してください。" (Access detected from an unregistered environment. Please enter the second factor password). Below the warning is a form with "Your second password" and a "Submit" button. The browser's developer console is open, showing the "Application" tab with the "Cookie" section selected. A table of cookies is displayed, with one cookie selected and its value highlighted in a blue box. A blue callout box points to this value with the text: "認証済Cookieが漏えいした前提で、そのCookieを設定してアクセス" (Assuming a leaked authenticated cookie, access is performed by setting that cookie). Below the table, a note says "値をプレビューする Cookie を選択する" (Select a cookie to preview the value).

登録されていない環境からのアクセスを検知しました。第二要素のパスワードを入力してください。

Your second password

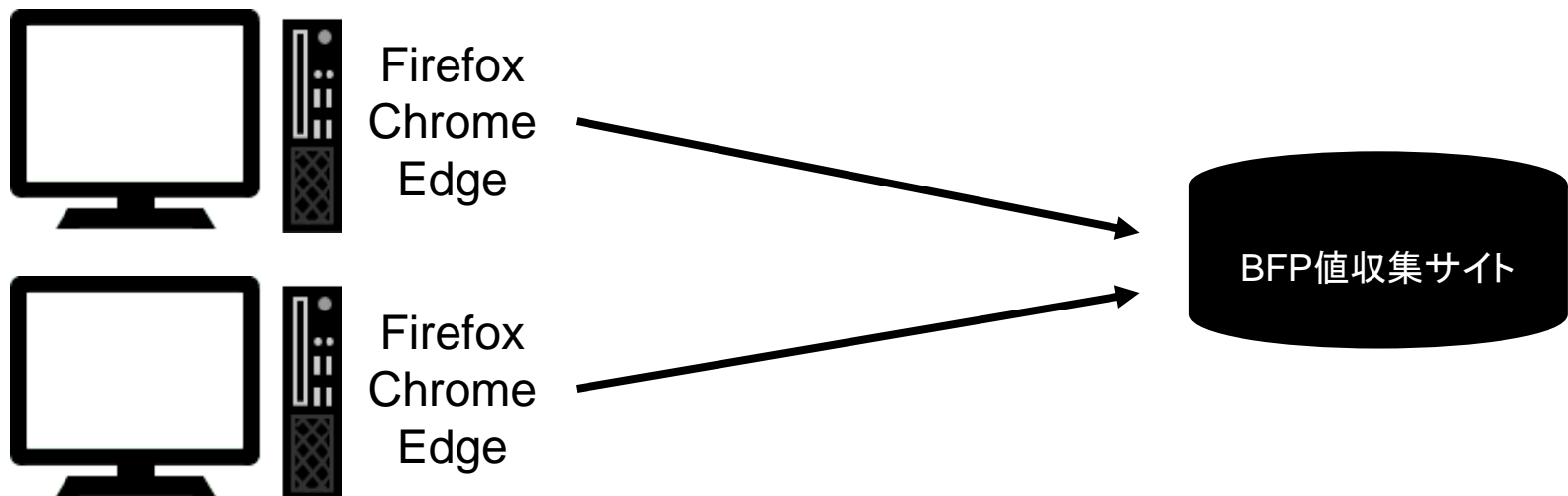
Your browser fingerprint: 3c41f878216c5feb3cdfb74420ead030

名前	値	ドメイン	パス	有効期限	サイズ	HttpOnly	Secure	SameSite	Priority
session	.eJkNzjEOwjAMRuG7ZGZl4s5Je5nqj2MDEjC0YkL...	localhost	/	セッション	239	✓			Medium

値をプレビューする Cookie を選択する

# BFP値の特性検証

- BFP値が頻繁に変化するとユーザビリティが低下する懸念あり
- BFP値を定期取得する実験を実施



# 実験結果 (週次)

- BFP値変化の頻度はブラウザ依存
- 詳細な解析の結果、変化はUserAgentの変化によるもの
  - つまりブラウザの更新が要因

	端末 1			端末 2		
	Firefox	Chrome	Edge	Firefox	Chrome	Edge
2021/4/23	f1_1	c1_1	e1_1	f2_1	c2_1	e2_1
2021/4/30	f1_1	c1_2	e1_2	f2_1	c2_2	e2_2
2021/5/7	f1_1	c1_2	e1_3	f2_1	c2_2	e2_3
2021/5/14	f1_1	c1_3	e1_4	f2_1	c2_3	e2_4
2021/5/21	f1_1	c1_3	e1_5	f2_1	c2_3	e2_5
2021/5/28	f1_1	c1_4	e1_6	f2_1	c2_4	e2_6
2021/6/4	f1_2	c1_4	e1_7	f2_2	c2_4	e2_7
2021/6/11	f1_2	c1_5	e1_7	f2_2	c2_5	e2_7

# 実験結果（日次・その他）

- Edgeに絞ってBFP値を日次取得
  - 日々の変化はなく、週一程度の変化

- 変化の頻度は高くないため、提案手法適用によるユーザビリティ低下の懸念は少ない

	端末 1 Edge
2021/5/25	e1_5
2021/5/26	e1_5
2021/5/27	e1_5
2021/5/28	e1_6
2021/5/29	e1_6
2021/5/30	e1_6
2021/5/31	e1_6
2021/6/1	e1_6
2021/6/2	e1_6
2021/6/3	e1_6
2021/6/4	e1_7
2021/6/5	e1_7
2021/6/6	e1_7
2021/6/7	e1_7
2021/6/8	e1_7

- その他、ブラウザのズーム機能の利用や、デュアルディスプレイ環境でのブラウザ移動によってBFP値が変化
  - BFPの要素に「スクリーンサイズ」「ディスプレイの有効領域」が含まれていることが原因
    - ⇒利便性のためにも、提案手法適用時は要素から取り除くべき

# 目次

- 背景
- ゼロトラスト
- 提案手法
- 提案手法の実装と評価
- **まとめと今後の課題**

# まとめと今後の課題

## ■ まとめ

- ゼロトラストの考え方の1つを実現するために、ブラウザフィンガープリントを利用してアクセス制御を行う手法を提案
- 提案手法を実装し、不正アクセス検知の実証実験を実施

## ■ 今後の課題

- BFP値が同じになりやすい環境における、不正アクセス検知に向けたBFP値要素の追加検討や提案手法へのロジックの追加