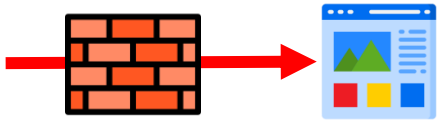
2022年度未踏IT人材発掘・育成事業

内部処理分析を基にしたWebアプリケーションのセキュリティSaaSの開発
ー　内部処理分析による新たな攻撃検知　ー

赤松 宏紀（大阪大学大学院情報科学研究科）大迫 勇太郎（大阪大学大学院情報科学研究科）

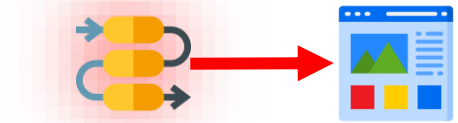
背景：従来の攻撃検知の課題

WAFでのパターンによる攻撃検知



WAFで設定されたルールを回避する攻撃や
ルール化されていない未知の攻撃の検知は困難

OSSのサプライチェーン攻撃の検知



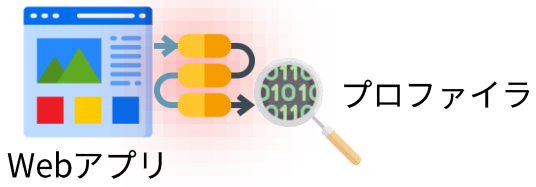
ライブラリ配布元への攻撃・改ざんや
開発者が意図せず導入してしまった
不審なライブラリの検知は困難

提案：内部処理分析による攻撃検知

Phrude

Profiling History-based Runtime Detection System

プロファイラで内部処理を記録し、不審な関数
呼び出しを**即座に検知**



内部処理分析で不審な関数呼び出しを検知し
その原因となるライブラリを**追跡**

2022年度未踏IT人材発掘・育成事業

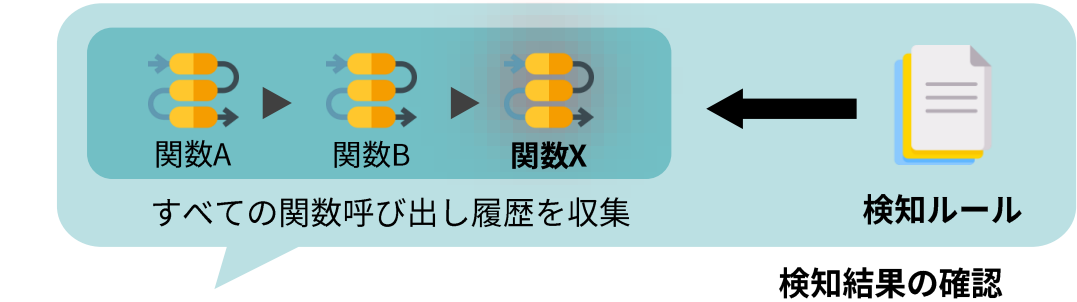
内部処理分析を基にしたWebアプリケーションのセキュリティSaaSの開発
ー　内部処理分析による新たな攻撃検知　ー

赤松 宏紀（大阪大学大学院情報科学研究科）大迫 勇太郎（大阪大学大学院情報科学研究科）

内部処理分析による攻撃検知SaaS

Phrude

https://phrude.com



内部処理である関数呼び出し履歴から攻撃に特有な関数を検知

```
...
関数名 :  call
ファイル : /usr/local/lib/python3.10/site-packages/jinja2/runtime.py
引数 :  {
    "args": "('CLOUD_SECRET_KEY',)",
    "kwargs": "{}",
    "_Context__obj": "CLASS:method-wrapper",
    "_Context__self": "CLASS:Context"
}

関数名 :  getenv
ファイル :  /usr/local/lib/python3.10/os.py
引数 :  {
    "key": "CLOUD_SECRET_KEY",
    "default": null
}
...
```

収集した内部処理の例

Webアプリケーションへの攻撃検知の
新たな情報源として内部処理を用いる

↓

既存の攻撃検知手法では検知不可能な
攻撃が検知可能になった