CSS2025 DEMO-23

日大理工

システムコール系列に基づく クリプトジャッキング検知の回避攻撃耐性評価

○ 嶋根 蛍太郎[1], 依田 みなみ[1], 松野 裕[1]
[1]日本大学

背景

- クリプトジャッキング攻撃におけるホスト型検知では、プロセスの**システムコール系列を入力**とし，**機械学習モデルで判定する手法**が研究されている
- 一方で，**検知回避を狙う攻撃に対して脆弱**となる可能性が指摘されている[1]

目的

- 検知回避攻撃に対する検知の耐性を定量化
- ノイズによるハッシュレート低下を定量化
- 検知回避攻撃に対して有効な防御戦略の指針を得る

脅威モデル

想定する回避攻撃
マイニング処理と軽量ノイズスレッドを並行実行させ、系列に無害なシステムコールを混在させる

目的
システムコール系列のパターンをノイズで崩し、検知を回避する（Recall 低下）

方法

データ処理の流れ

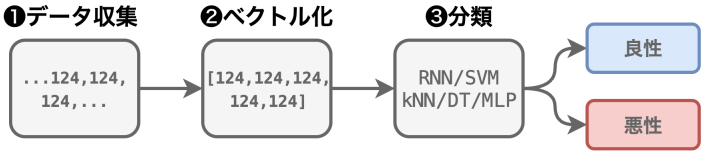

図1. データ処理フロー

観測
一定時間で採掘を行い，システムコール系列とハッシュレート(H/s) を収集

ベクトル化／分類
系列を n-gram 特徴量に変換（n=5/10/35/40/50）
RNN / SVM / kNN / DT / MLP で二値分類

ノイズ制御
ノイズスレッドを並行実行し無害なシステムコールを混在
ノイズ挿入率（0%, 10%, … ,90%）を変化させて評価

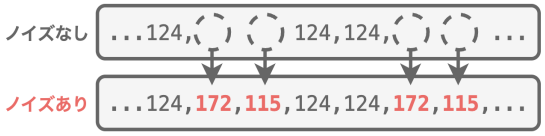

図2. システムコールのノイズ挿入例

総収集時間
約7時間30分（15分 × ノイズ挿入率0-90% × 各3ラン）

実験結果などの詳細はこちら

評価

- ノイズ挿入率を10%刻みで変化させて評価（0-90%）
- 検知性能は **再現率（Recall）**で比較
- 採掘効率は**ハッシュレート (H/s)** で相対評価

結果

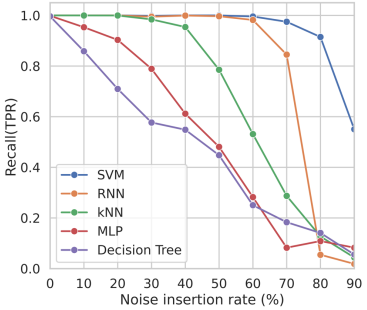

図3. ノイズ挿入率と Recall（モデル別）

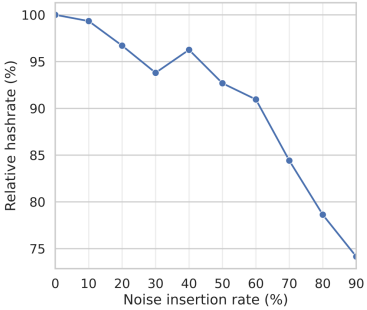

図4. ノイズ挿入率と相対ハッシュレート

表1. ノイズ挿入率 50% におけるモデル別性能（Recall／FPR／Precision／F1）

Model	Recall (TPR)	FPR	Precision	F1
Decision Tree	44.79%	0.01%	99.99%	61.85%
MLP	48.08%	0.57%	98.82%	64.69%
kNN	78.55%	0.00%	100.00%	87.98%
RNN	99.68%	0.00%	100.00%	99.84%
SVM	99.99%	0.00%	100.00%	100.00%

- SVM/RNN は高ノイズ挿入率でも Recall の低下が小さい
- DT/MLP/kNN はノイズ増加に伴い Recall が顕著に低下
- ハッシュレートはノイズ増加で概ね単調に低下

考察

ノイズ挿入下でも RNN の Recall 低下は比較的緩やかであり，時系列モデルとして局所的ノイズの影響を受けにくいことがその一因と考えられる．
ノイズ挿入率を90%まで高めても，採掘効率はベース比で約75%を維持しており，性能低下と収益確保の両立という観点で攻撃者にとって有効な回避策となり得る．

まとめ・今後の課題

ノイズ挿入は採掘効率を大きく落とさずに検知性能を低下させる有効な回避手段（特に DT/kNN/MLP）である．一方で，高いノイズ挿入率下でも高い Recall を保てる検知モデルの設計は今後の課題である．

[1] Riyeong Kim et al : “Detecting Cryptojacking Containers Using eBPF-Based Security Runtime and Machine Learning”, Electronics, vol. 14, Article 1208, 2025. doi:10.3390/electronics14061208

応用情報工学科