SCI-Tech Festival 2024

高信頼アクセス制御をベースとする知的侵入検出・防御方式

香川大学・創造工学部・情報システム・セキュリティコース 准教授　橋本正樹

1　研究目的とアプローチ

不正アクセスやマルウェアの悪性活動を高精度で検出し、抑制する手法を研究開発する。そのために、以下のアプローチを行う。

① 悪性活動を、詳細な要素活動の連結パターンとして記述し、攻撃の意図を推定する。

② セキュアOSに組み込んだセキュリティモジュールが、悪性活動パターンに合致する実行プロファイルを検出する。

2　具体的な研究内容と特徴

悪性活動の意図を要素活動から系統的に推測するルールを検討し、それを記述する専用言語を定義する。また、OSモジュールがルールを効率的に解釈・実行する処理系を開発した上で、セキュアOSに組み込み、攻撃活動データセットの上で有効性を検証する。本研究の特徴は以下の通りである。

① 個別マルウェアや大量ログの事前解析に依存せず、活動パターンから攻撃意図を推定する。

② リアルタイムでの検出と対処が可能である。

図1. プロセス活動のリンク付

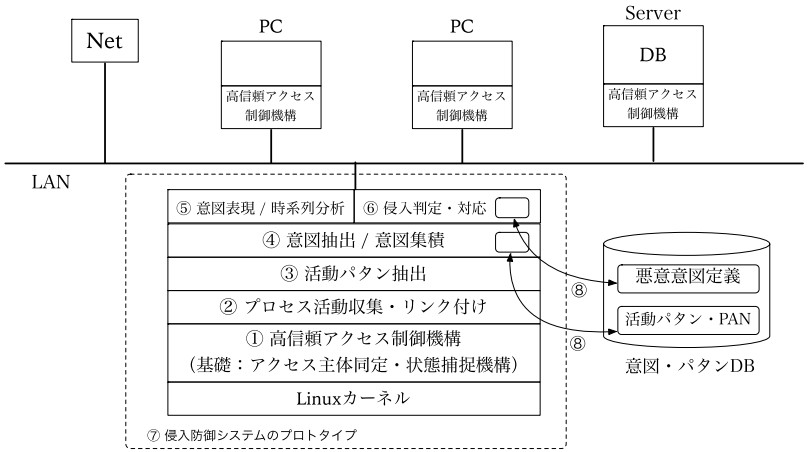

図2. 適応型知的侵入防御システム

分野：　情報工学　専門：　情報セキュリティ関連
（研）　電子・情報工学領域
E-mail: hashimoto.masaki@kagawa-u.ac.jp　Tel. 087-864-2221