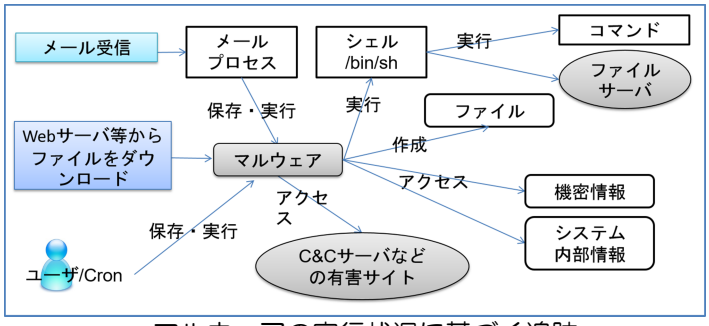
マルウェアの活動解析による検知手法の提案

Malware Detection based on Activity Analysis

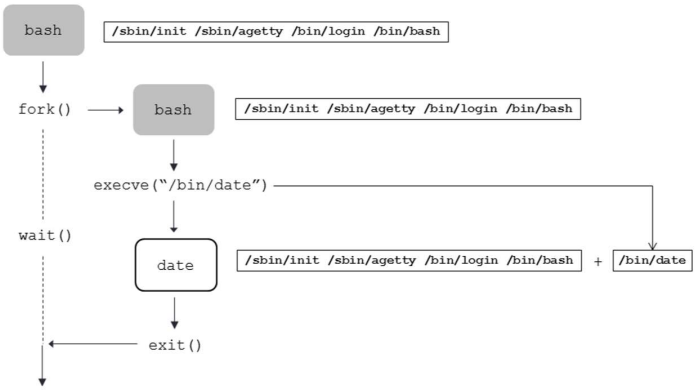
吉村豪康・ネットワーク分科会・情報セキュリティ大学院大学

Abstract：We propose a detection method to dynamically track the contents of processing executed by malware. Specifically, TOMOYO Linux which is a secure OS is applied as a malware dynamic analysis system. Because TOMOYO Linux can automatically record the execution history of all processes from system startup to termination, it is important to track all processes at the process level, including associated processes, of processes of interest such as malware based on the principle. By the proposed method, malware countermeasure that mechanically distinguishes malware activity becomes possible.

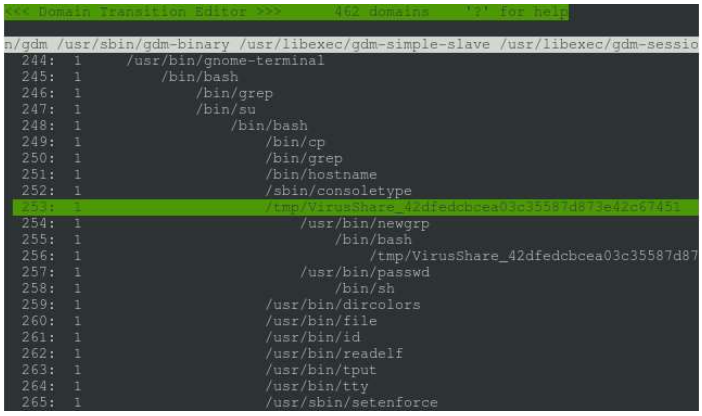
要旨：マルウェアが実行する処理の内容を動的に追跡する検知手法を提案する．マルウェアの動作を関連プロセスまで含めて，プロセスレベルで追跡および制御することが可能となる．



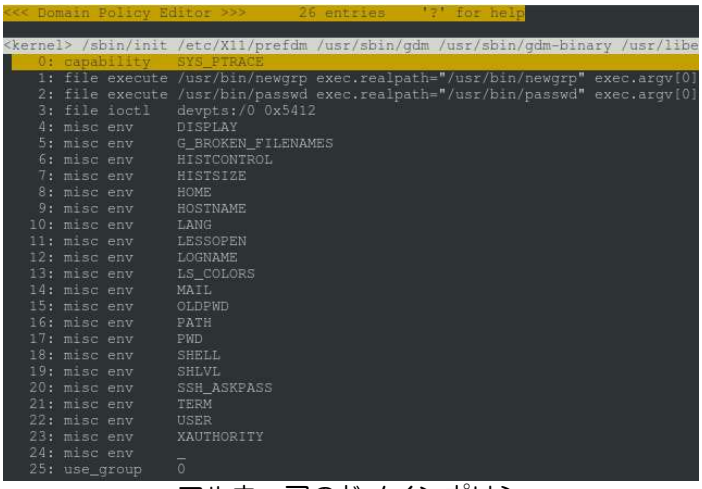
マルウェアの実行状況に基づく追跡



システムの起動から現在までのすべてのプロセスの実行履歴を自動的に記録することが可能．



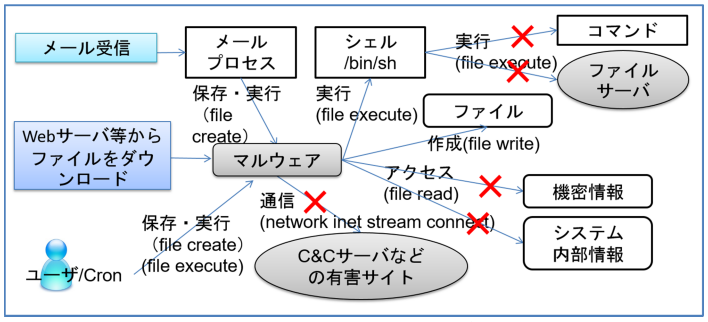
マルウェアのドメイン遷移



マルウェアのドメインポリシ

モード	内容	動作
disabled	無効	通常のカーネルと同様に動作する．
learning	学習	ポリシ違反が発生しても要求を拒否しない． ポリシ違反が発生しないようにするのに必要なアクセス許可をポリシに追加する．
permissive	確認	ポリシ違反が発生しても要求を拒否しない．
enforcing	強制	ポリシ違反が発生したら要求を拒否する．

すべてのプロセスについてプログラム実行履歴を記憶しておき，その属するドメインごとにアクセス許可を定義し，それに基づきアクセス制御を行う．



マルウェアの実行状況に基づく制御