主　論　文　要　旨

報告番号	㊙ 乙 第　　号	氏 名	嶋村 誠

主 論 文 題 目 ：

攻撃コードの振る舞いの自動解析に関する研究

（内容の要旨）

現在，インターネットは重要な社会基盤となっており，オンラインバンキングやオンラインショッピングをはじめとした様々なサービスが提供されている．一方で，サービスを提供するサーバに対する悪意あるリモート攻撃が後を絶たない．リモート攻撃によって，サーバの正常な稼働が妨げられ，大きな損失を受ける事例が数多く報告されている．このため，リモート攻撃への対策はセキュリティ上の重要な課題になっている．

リモート攻撃では脆弱性のあるサーバに攻撃メッセージを送信し，攻撃メッセージ中の攻撃コードと呼ばれる機械語命令列を実行させる．このようなリモート攻撃に対して，ネットワーク侵入検知システムやホスト侵入検知システムなどの防御システムが用いられている．こうした防御システムでは攻撃コードの生成するファイル名や攻撃コードの行う通信の内容など，個々の攻撃コードに特有な情報を防御のために利用している．攻撃コードに特有なこうした情報はシグネチャと呼ばれている．そのため，防御システムは攻撃コードごとにシグネチャを必要とし，シグネチャのない攻撃コードへの対処はできない．このため，防御システムのベンダーは新種の攻撃コードが現れるとその攻撃コードを解析し，解析結果を用いてシグネチャを作成している．

攻撃コード解析では，解析者は攻撃コードが計算機資源へのアクセスのために用いるシステムコールやAPI 呼び出しを抽出する．そして，この解析結果からシグネチャに必要となる情報を取り出す．現在，ベンダーの解析者は逆アセンブラやデバッガを用いて人手で攻撃コードを解析している．しかし，人手による解析は多くの時間を要し，間違いを起こしやすい．また，ベンダーでは新種の攻撃コードを迅速に発見するため一日に数万個の攻撃コードを収集しており，解析者は毎日大量の攻撃コードを解析する必要がある．そこで，解析者の負担を減らすため，攻撃コードの自動解析システムが利用されている．

しかし，最近では攻撃者が攻撃コードを工夫し，自動解析システムによる解析が困難になってしまっている．例えば，攻撃者は攻撃コードの主要部分を暗号化しておき，実行時に復号することで攻撃コードを逆アセンブルできないようにする．また，システムコールの実行結果を検査することでデバッガや自動解析システムを検出し，攻撃者の想定外の環境で動作しているときには攻撃を実行しないようにしている．

本研究では攻撃コードによる解析の回避が難しい自動解析システムである Yataglass を提案する．Yataglass では攻撃コードを機械語命令列として疑似実行することで解析を行う．これにより，暗号化された攻撃コードによって解析を回避されることはない．また，攻撃コードがシステムコールの結果を利用して Yataglass を検出することを防ぐために，Yataglass では Dynamic Taint Analysis を用いてシステムコールの実行結果を検査する条件分岐を発見し，その分岐の両方のパスを解析する．さらに，攻撃者による Yataglass の回避を難しくするため， 本研究ではメモリスキャン攻撃の対策を行う．メモリスキャン攻撃とは攻撃コードが攻撃対象サーバのデータを攻撃コードの一部として利用する攻撃であり，既存の自動解析システムを回避するための攻撃手法である．Yataglass は Symbolic Execution を用いて攻撃コードが利用するデータを推測することで，メモリスキャン攻撃を用いる攻撃コードの解析を可能にしている．

Yataglass のプロトタイプを実装し，攻撃コード生成ツール MetaSploit を用いて生成した攻撃コード，および実際の攻撃コードを解析する実験を行った．その結果，Yataglass がこれらの攻撃コードを正しく解析できることが確認できた．また，様々な回避手法を適用した攻撃コードを用いた実験により，既存の解析システムによる解析を回避できる攻撃コードであっても，Yataglass は正しく解析できることを確かめた．