成果概要書

マルウェア対策ユーザサポートシステムの研究開発

（１）研究の目的

本研究開発では、ユーザパソコンに負荷がかかる実行コードの解析をnicter(Network Incident analysis Center for Tactical Emergency Response)」等の解析機能を有する外部のシステムが担うことにより、効率的なマルウェアの検出および自動駆除の仕組みを実現することを目的とする。

（２）研究期間

平成２１年度から平成２３年度（３年間）

（３）委託先企業

株式会社　日立製作所＜幹事＞、KDDI 株式会社

（４）研究予算（百万円）

平成２１年度	２３７（契約金額）
平成２２年度	２２２（　〃　）
平成２３年度	２０９（　〃　）

（５）研究開発課題と担当

課題ア　：検査プログラムに関する研究開発

ア－１：不正プログラム基本探索アルゴリズムに関する研究開発
（株式会社　日立製作所）

ア－２：ホワイトリスト化等を用いた高能率探索手法に関する研究開発
（株式会社　日立製作所）

課題イ　：マルウェア駆除ツールの自動生成・最適化・高速検証手法の研究開発

イ－１：マルウェア駆除ツールの自動生成・最適化手法の研究開発
（株式会社　日立製作所）

イ－２：マルウェア駆除ツールの安全性の高速検証手法の研究開発
（株式会社　日立製作所）

課題ウ：ユーザサポートプロトコルに関する研究開発

ウ－１：クライアントサーバプロトコルの設計及び開発
（KDDI 株式会社）

ウ－２－１：クライアントエージェントの設計及び開発
（KDDI 株式会社）

ウ－２－２：サーバエージェントの設計及び開発　（KDDI 株式会社）

課題エ：課題ア～ウを実環境で有効に機能させるための実証実験
（KDDI 株式会社）

（６）これまでの主な研究成果

特許出願：　２件

外部発表：　２件

具体的な成果

①マルウェア対策ユーザサポートシステムのフレームワークを設計。PC 内からの擬陽性ファイルを発見し，マルウェア解析システムに解析依頼を行う機能を開発し，評価実験を実施

②ユーザパソコン内で稼働，あるいは常駐している実行コードを漏れなく検索・収集するための検査機能，検査機能で検索した実行コードがマルウェアの疑いがあるかを判定するマルウェア可能性判定機能，マルウェア可能性判定機能でマルウェアの可能性があると判定された実行コードをマルウェア解析機能で解析させるために必要な情報を収集する情報収集機能，を設計・開発。
マルウェア可能性判定機能が有する検出基準の策定にあたっては，マルウェアのファイル構造の特徴に基づき擬陽性ファイルを発見することで，高速・軽量化を実現

③センタ側で管理する市販のソフトウェアをリストアップしたホワイトリスト（マスタホワイトリスト）を管理し，ユーザのパソコンからアップロードされてきた実行コードが，市販のホワイトリストに記載されているかどうかを判定するサーバ型フィルタリング技術および，判定の結果，ホワイトリストに記載されている（＝マルウェアではない）と判断された場合にユーザのパソコンに結果をフィードバックし，ユーザのパソコン側で部分的なホワイトリスト（ローカルホワイトリスト）を作成する，クライアント型フィルタリング自動生成技術を開発。センタ・PC の連携により，既知の非マルウェ

アを効率的にフィルタリングを実現

④既存のマルウェア解析機能を有するシステム（nicter ミクロ解析システム，CWSandBox，Anubis,）の解析結果や，ユーザの利用環境に関連する情報の収集方法，自己変貌型マルウェアに関する分析に基づき，ユーザのパソコン上からマルウェアを駆除するマルウェア駆除ツールが備えるべき機能要件，駆除ツールを自動的に生成する自動駆除ツール生成システムが備えるべき機能要件，さらには自働駆除生成ツールに対する入力となる共通実行コード解析結果フォーマットの機能要件を策定。

⑤多種類のマルウェアを PC に感染させた場合の振る舞いの分析に基づき，検証環境をマルウェアに感染させるための機能要件，駆除ツールの正常性を検証するための機能要件，駆除ツールの安全性を検証するための機能要件，駆除ツールの効率性を検証するための機能要件，感染環境を高速に復元するための機能要件，を策定

⑥一般的な通信エラーに加えて，ユーザによる通信の切断やマルウェアによるファーミング等の意図的なエラーについて整理し，ユーザサポートプロトコルの要件を整理。エラー発生時に不安定状態に陥らない回復機能を備え，かつマルウェアを誤って入手した第三者が被害を受けないよう，アップロードする実行コードを無害化する機能を備えた，安全・効率的な検体登録，駆除ツール取得を実現する，3 層構造プロトコルを設計

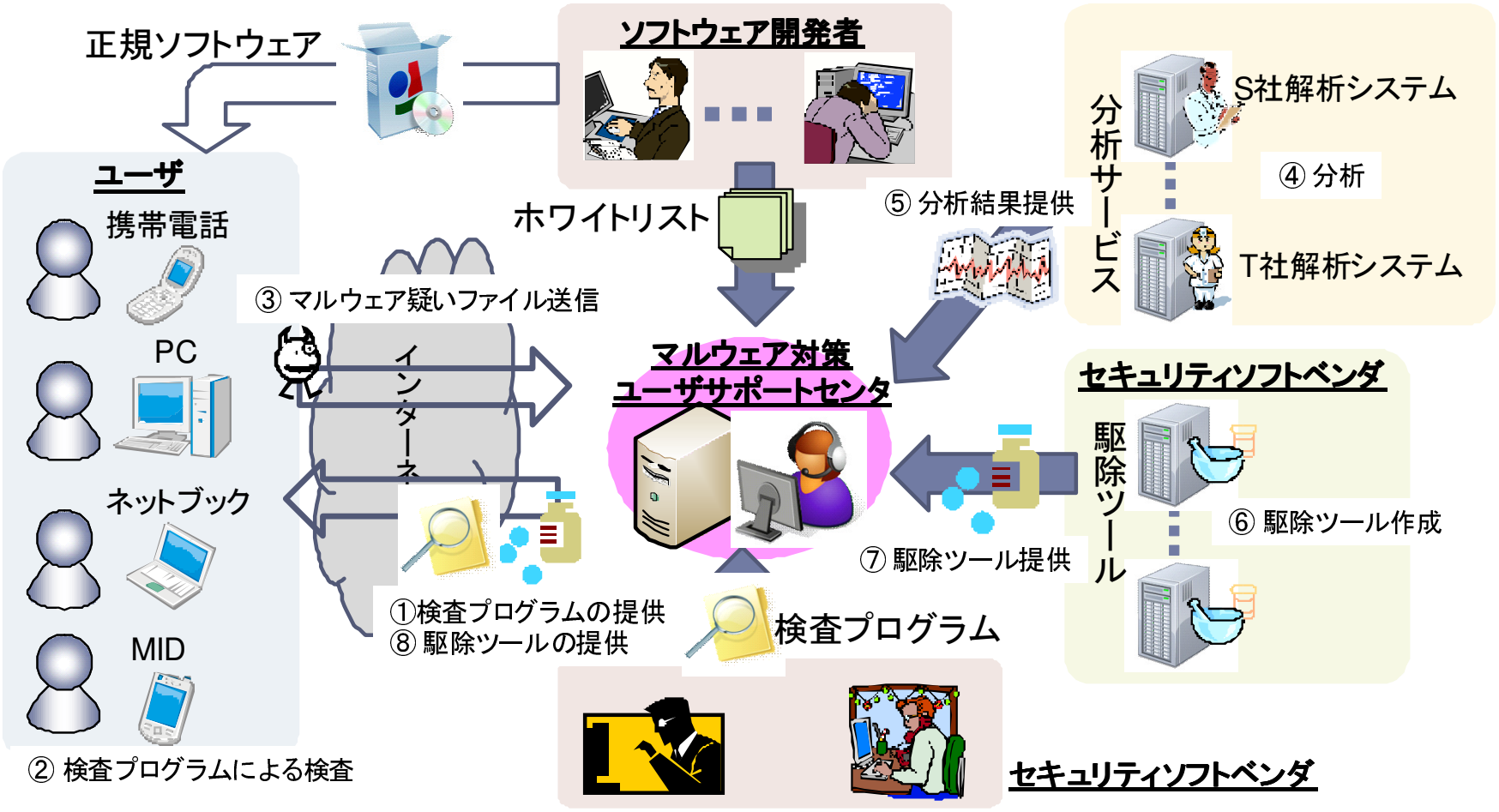
⑦マルウェアを探索モジュールとして誤認したり，ダウンロードした正しい探索モジュールおよび駆除プログラムモジュールを削除されたり，置き換えられたり等，ユーザ端末上でマルウェアが動作していると仮定した場合にクライアントエージェントがマルウェアから晒される脅威について整理し，クライアントエージェントが備えるべきセキュリティ要件を定義。また，策定した要件定義を満足するクライアントエージェントの基本仕様を策定。検査プログラムとフィルタプログラムを制御し，擬陽性ファイルをサポートセンタに転送する機能を開発

⑧サーバエージェントが晒される脅威について整理し，サーバエージェントが備えるべきセキュリティ要件を定義。ユーザのパソコンから実行コードを受信する機能，マルウェア駆除ツールのダウンロード要求をユーザのパソコンに通知する機能等，クライアントエージェントと連携するためのポータル機能から構成されるサーバエージェントを開発し，動作を確認

⑨nicter ミクロ解析システム等のマルウェア解析機能を有するシステムに提供すべき情報およびマルウェア解析機能を有するシステムから受信すべき情報を整理し，連携のためのインタフェース仕様を策定

⑩平成２２年度より開始する評価に向け，実証実験においてプロトタイプシステムの実用性・スケーラビリティについて評価を行うための評価項目を整理し，実証実験の実施委託先，実施環境，検証内容，検証方法について，必要条件の洗出しを実施

（７）**研究開発イメージ図**


正規ソフトウェア
ソフトウェア開発者
ユーザ
携帯電話
PC
ネットブック
MID
② 検査プログラムによる検査
ホワイトリスト
⑤ 分析結果提供
分析サービス
S社解析システム
④ 分析
T社解析システム
③ マルウェア疑いファイル送信
インターネット
マルウェア対策
ユーザサポートセンタ
セキュリティソフトベンダ
駆除ツール
⑥ 駆除ツール作成
⑦ 駆除ツール提供
①検査プログラムの提供
⑧ 駆除ツールの提供
検査プログラム
セキュリティソフトベンダ