（７）研究開発イメージ図

平成２３年度「マルウェア対策ユーザサポートシステムの研究開発」の研究開発目標・成果と今後の研究計画

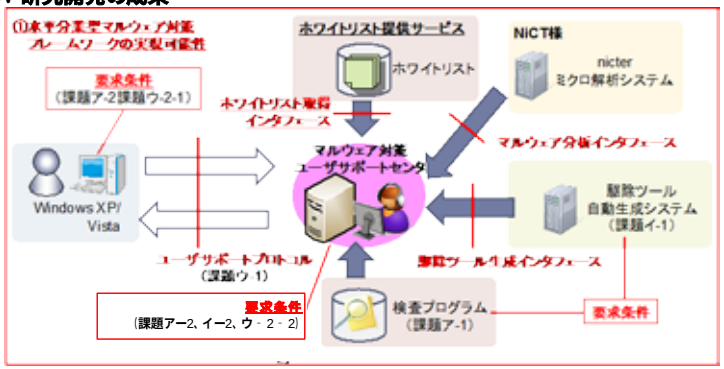
１．実施機関・研究開発期間・研究開発費

◆実施機関　　株式会社日立製作所（幹事者）、KDDI株式会社
◆研究開発期間　平成２１年度から平成２３年度（3年間）
◆研究開発費　　総額６６９百万円（平成２３年度　２０９百万円）

２．研究開発の目標

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。

３．研究開発の成果



研究開発成果：不正プログラム基本探索アルゴリズム（課題ア―１）
・プロセスの起動を捉え、実行元プログラムの擬陽性判定を行う
リアルタイムスキャン機能を実現

研究開発成果：ホワイトリスト化等を用いた高能率探索手法（課題ア―２）
・フィールド実験を通じ、構築したマスタホワイトリストフィルタが、ユーザPCから送られた検体のうち35%をフィルタリングすることを確認

研究開発成果：マルウェア駆除ツール自動生成システム（課題イ―１）
・フィールド実験を通じ、開発した駆除ツールが、nicterミクロ解析システムがマルウェアと判定した実行ファイルを全て駆除出来ることを確認

研究開発成果：マルウェア駆除ツール検証システム（課題イ―2）
・駆除ツールの正常性及び安全性の検証を、平均5分程度で完了する機能を実現

研究開発成果：クライアントサーバプロトコル（課題ウ―1）
・フィールド実験において、クライアントエージェントのログをサーバエージェントに送信するプロトコルを設計・開発

研究開発成果：クライアントエージェント（課題ウ― ２ ― １）
・フィールド実験において、ユーザPC内のログを収集し、サーバエージェントに送信する機能を設計
・リアルタイムスキャン機能の実行を制御する機能を実現

研究開発成果：サーバエージェント（課題ウ― ２ ― ２）
・フィールド実験において、ユーザPCから収集したログを保管・分析する機能を実現
・ユーザPCから送信された検体を、既存アンチウイルスソフトウェアを用いて自動的にスキャンする機能を実現

研究開発成果：課題ア～ウの実環境での有効性確認（課題エ）

課題ウ-2-1で研究開発したクライアントエージェントを実装したコンピュータをユーザの実環境において使用し、課題ア～ウの研究成果である各システムと連携し問題なく動作することを確認

ユーザPCから送られた実行コードが本研究で開発したシステムでマルウェアと判定された場合、駆除ツールが平均4分40秒（最大11分）で配信されることを確認

PCを配布したユーザの利用から得られた実験結果を基に、ユーザが数十万規模となった場合のシステムスケーラビリティをシミュレーションし算出

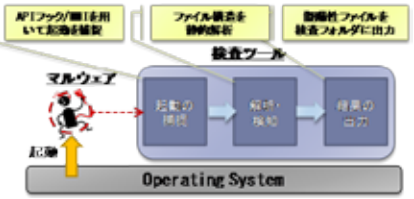
PCを配布したユーザへのアンケートおよび個別ヒアリングにより得られた情報を基に、ユーザビリティや利用上の問題点、課題について情報を収集

ユーザから送信された実行コードによる動作を解析し、Microsoft Security Essentialの定義ファイルが対応する3週間前に検知したマルウェアを確認

課題アー1・課題イ―2・課題エ　研究開発内容詳細

課題アー1：不正プログラム基本探索アルゴリズムの研究開発

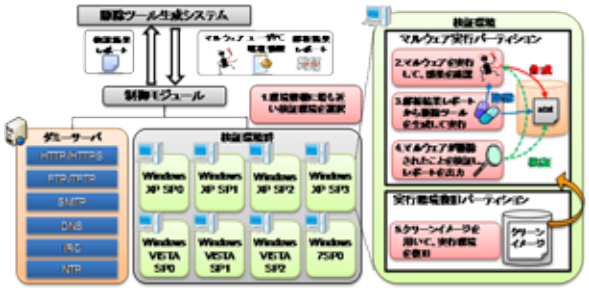
p リアルタイムスキャン機能を開発
- Ø APIフック及びWindows Management Instrumentation(WMI)を利用して**プロセスの起動を捕捉し、**ファイル構造を分析して擬陽性ファイルを発見する静的解析を行うことで、軽量で効率的な解析処理を実現
- Ø 安定性及びアンチウイルスソフトとの親和性を検討し、WMI方式をフィールド実験で使用



	APIフック方式	WMI方式
方式	IATを書き換え、全プロセスのCreateProcess系のAPIをフック	WMIを利用し、新規プロセス起動時に通知を受ける
安定性	低い	高い
アンチウイルスソフトとの親和性	低い	高い
実行ファイルの捕捉率	実行ファイルの起動を確実に補足	起動後に自身を削除するファイルの捕捉に失敗する場合がある

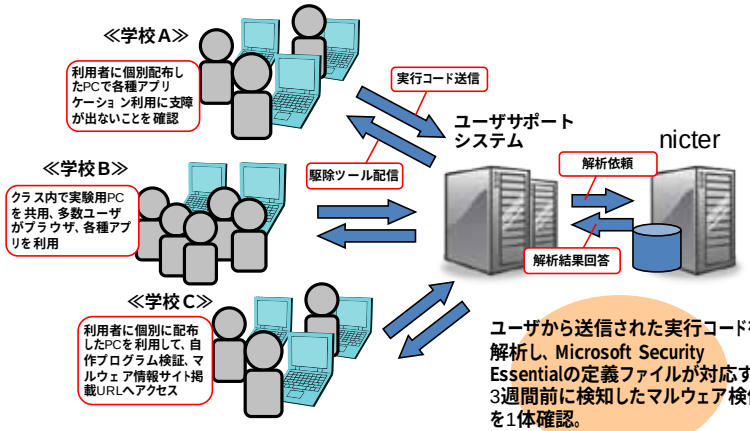
課題イー2：マルウェア駆除ツールの安全性の高速検証手法の研究開発

p マルウェア駆除ツール検証システムを開発
- Ø 環境情報を基に、ユーザPCに**最も近い検証環境を選択する**機能を開発
- Ø 駆除ツール実行後のPC環境とマルウェア解析結果レポートを比較して、**マルウェアの駆除が正常・安全に完了することを検証**する仕組みを開発
- Ø 正常性・安全性が検証済みの駆除ツールのみをユーザPCに返却し、**駆除ツールによる悪影響を防止**



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

課題ウ-2-1で開発したクライアントエージェントを実装したPCを大学、専門学校5校の実験主旨を理解いただいたユーザに配布、課題ア～ウの各研究で開発したシステムと連携し問題なく動作することを確認した。
また、各協力先においてはそれぞれ異なる方向での検証アプローチを行った。
・多数ユーザでの共用 または 個別ユーザでの専用
・非マルウェア系各種アプリケーションの積極的なダウンロード、インストール
・自作プログラムの検証
・マルウェア情報系サイト掲載URLへのアクセス
上記の各種検証の中で、実行コードが検出され検査⇒マルウェア判定⇒駆除ツール配信までの一連の動作を確認した。駆除ツール配信までの時間は平均4分40秒（最大11分）で、駆除ツール配信前に動作の確認を行う検証ツールを実装後も平均10分（最大15分）であった。
また、実験対象ユーザから取得したアンケートにより、システムのユーザビリティに関する情報を収集した。また、ユーザへの個別ヒアリングも実施し、より詳細な利用上の課題等について確認を行った。



ユーザから送信された実行コードを解析し、Microsoft Security Essentialの定義ファイルが対応する3週間前に検知したマルウェア検体を1体確認。

2

4．これまで得られた成果（特許出願や論文発表等）＊成果数は、累計件数と（ ）内の当該年度件数です。

	国内出願	外国出願	研究論文	その他研究発表	プレスリリース	展示会	標準化提案
マルウェア対策ユーザサポートシステムに関する研究開発	10 (6)	6 (6)	4 (3)	16 (11)	1 (1)	5 (5)	3 (3)

5．研究成果発表会等の開催について

国内外の学会や会議の場での研究発表等を通じて、研究成果を広く一般に周知、広報した。特に、マルウェア検知に関する代表的な国際会議であるRAID2011にて、開発したマルウェア対策ユーザサポートシステムの紹介を行い、この分野をリードしている著名な研究者と議論を行った。

6．今後の研究開発計画

・研究成果の実用化・事業化への取り組み
- ü本研究成果であるユーザサポートシステムの公共分野への適用・展開を目指す。
- ü本研究成果で得られた検査ツールや駆除ツールなどの要素技術、知見をセキュリティベンダに展開し、各ベンダ製品への適用を検討する。
- ü今回開発したマルウェア検知・駆除技術の標的型マルウェア、およびクラウドや制御システム分野のマルウェア対策への応用を図る。

・研究成果の標準化への取り組み
- üマルウェアに関する学会、標準化団体などの動向に注意し、ITU-Tなどを対象に標準化提案を実施する
（ITU-T SG17へ3件の標準化提案を実施）

・研究成果の普及・啓発への取り組み
- ü今回実証実験でご協力を頂いた大学様などの教育機関と連携し、説明会・セミナーでの紹介や、教育教材としての活用などにより、本研究成果の普及・展開を目指す。