平成21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」の開発成果について

1. 施策の目標

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。

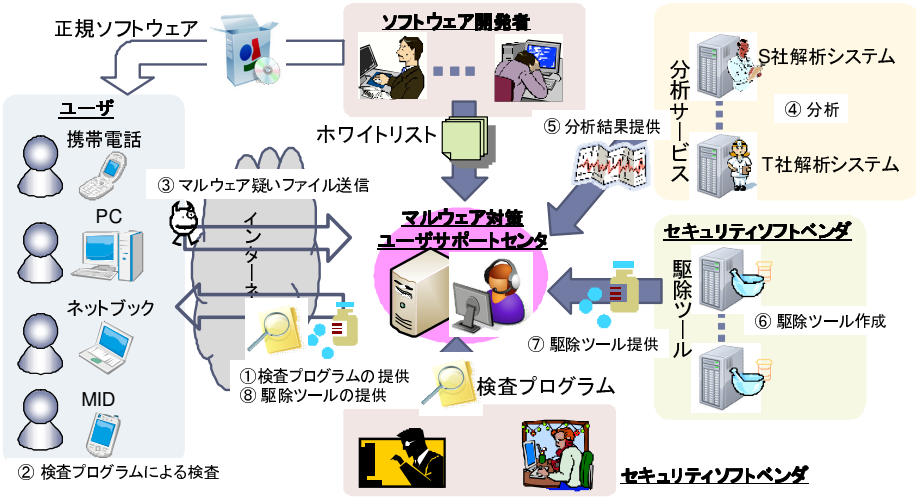
2. 研究開発の背景

コード難読化やコード自己変貌化に代表されるように、昨今、マルウェアの高度化・巧妙化が進展しており、未知のマルウェアや一定期間感染行動を見せないマルウェアの疑いのある怪しい実行コード等、アンチウィルスソフトによる対応では十分カバーし切れない領域が存在している。

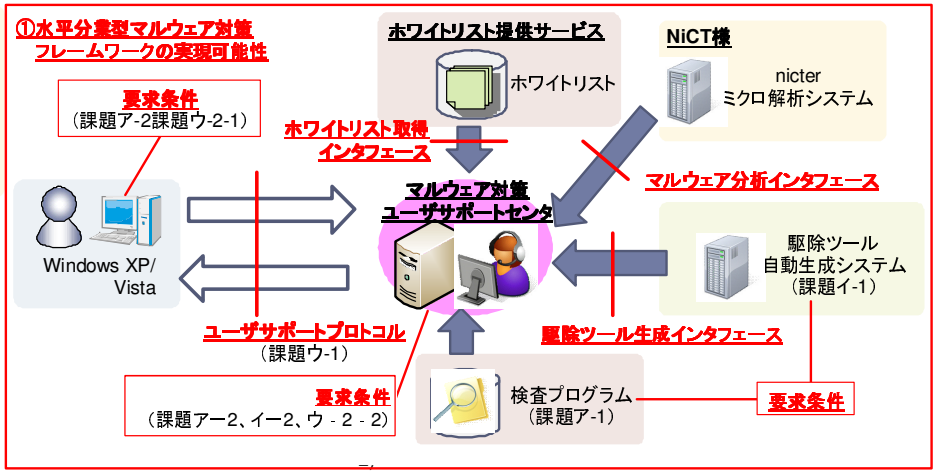
3. 研究開発の概要と期待される効果

本研究開発は、マルウェア対策に必要とされる、(1)ユーザのパソコンに負荷をかけない方法で怪しい実行コードを探索・収集する機能、(2)怪しい実行コードがマルウェアかどうかを解析・判断する機能、(3)マルウェアを駆除するツールを生成する機能、(4)(1)ー(3)の機能を連携させる機能、をモジュール化することで、各機能についての専門家がノウハウを提供しあい、高度なマルウェア対策を実現する、水平分業型マルウェア対策フレームワークの実現が期待できる。

水平分業型マルウェア対策フレームワーク



本研究開発での研究内容



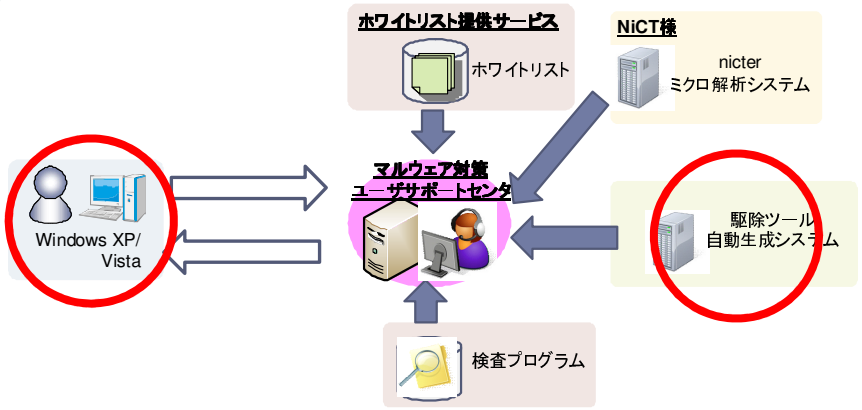
水平分業型マルウェア対策フレームワークのリファレンス実装を開発

4. 研究開発の期間および体制

平成21年度～23年度(3年間)

NICT委託研究(株式会社　日立製作所、KDDI株式会社)

検査プログラムに関する研究開発
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



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
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
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
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

課題ア－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

□マルウェアのファイル構造の特徴に基づき，PCから擬陽性ファイルを高速に発見する軽量なアルゴリズムを開発
- ✓500体のマルウェア検体を解析し，マルウェアの特徴を分析
- ✓19の静的解析エンジンと数百のルールから構成される，擬陽性ファイル発見プログラムを設計・実装。既存アンチウイルスソフトが検知できない58検体（500検体中）を検知
- ✓マルウェアの各特徴の出現頻度を元に，解析エンジンの実行順序を効率化することで，PCで実行中のプロセスを5秒以内に検査する，高速なスキャンを実現

開発した静的解析エンジン一覧

1. スキャン対象ファイルチェック	8. 電子署名検証	15. マーカ隣関解析
2. 文字列前処理	9. コードセクションヒューリスティック	16. 埋め込み画像ヒューリスティック
3. JAVA/RIFFスキャナ	10. IATヒューリスティック	17. エミュレーション
4. Win32ファイルフィルタ	11. 文字列量ヒューリスティック	18. セクション属性解析
5. ファイル名チェック	12. リソースブラックリスト	19. タイムスタンプ解析
6. 破損ファイルフィルタ	13. API・文字列検知	
7. セクションヘッダ解析	14. マーカ隣関ヒューリスティック	

課題イ－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

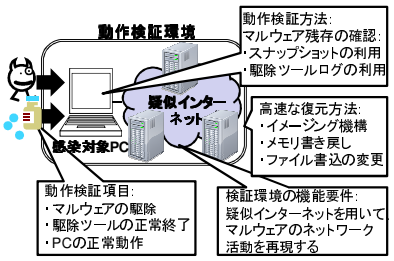
□マルウェア駆除ツール生成の要件を策定
- ✓ nicterミクロ解析システム、CWSandBox, Anubisの解析結果を調査し、マルウェア標準解析レポートフォーマットを策定
- ✓ マルウェアが行うPCの改変項目を調査
- ✓ 駆除ツールの機能要件を策定
- ✓ 自己変貌型マルウェアの検知・駆除ツール生成方法を考案

マルウェア標準解析レポート

```
<Reporter>・・・</Reporter>          ← 解析システム
<Environment>...</Environment>       ← 検出元PCの環境情報
<target>...</target>                 ← 検体及び検体から派生したプログラム
<Symptom>                            ← Targetsが行った、ファイル/レジストリ/プロセス/ネットワーク/サービスに関連した活動
  <Registry>...</Registry>
  <File>...</File>
  <Process>...</Process>
  <Network>...</Network>
  <Service>...</Service>
</Symptom>
```

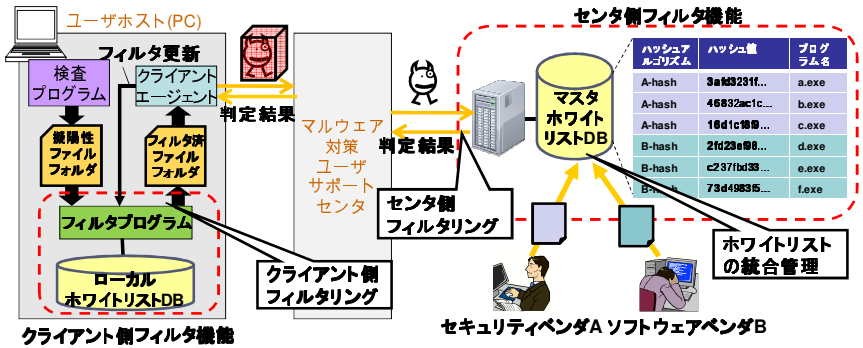
課題イ－2：マルウェア駆除ツールの安全性の高速検証手法の研究開発

□マルウェア駆除ツールの動作検証に必要な要件を策定
- ✓ 駆除ツール動作検証項目
- ✓ 駆除ツール動作検証方法
- ✓ 動作検証環境の機能要件
- ✓ 動作検証環境の高速な復元方法

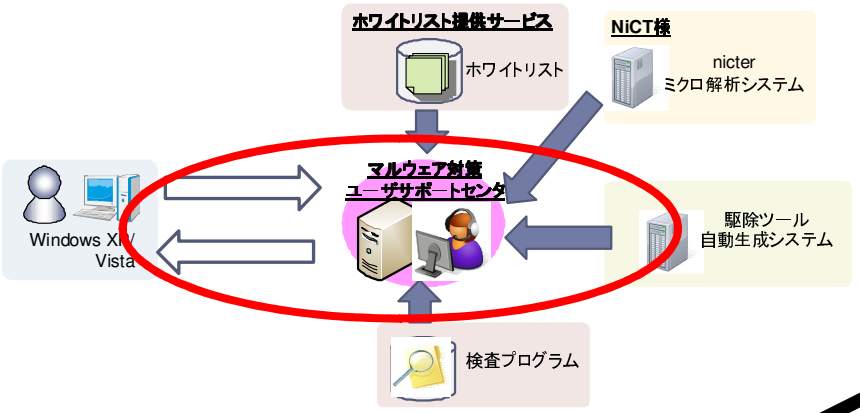


課題ア－２：ホワイトリスト化等を用いた高能率探索手法に関する研究開発

□センタ・PCの連携により，既知の非マルウェアの効率的なフィルタリングを実現
- ✓ センタ側で，大規模なマスタホワイトリストDBを一元管理することで，PC側でのホワイトリストの管理を容易化
- ✓ 非マルウェアと判定された検体のリストをPC側で管理することで，センタへの検体の不要な再送信を防止
- ✓ 様々な組織が提供する多様なホワイトリストを，統合管理する方式を開発



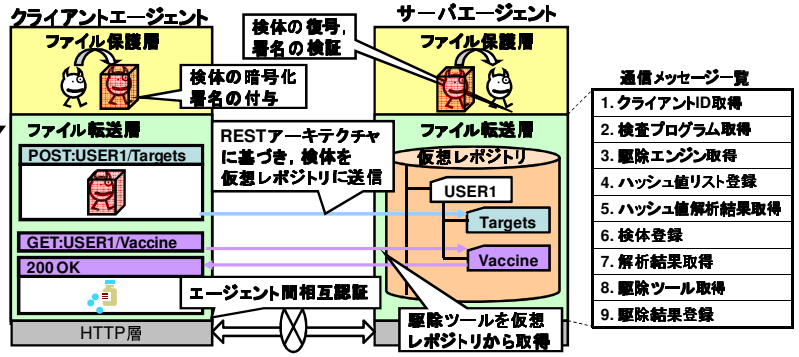
ユーザサポートプロトコルに関する研究開発



ウ－１：クライアントサーバプロトコルの設計及び開発
ウ－２－１：クライアントエージェントの設計及び開発
ウ－２－２：サーバエージェントの設計及び開発

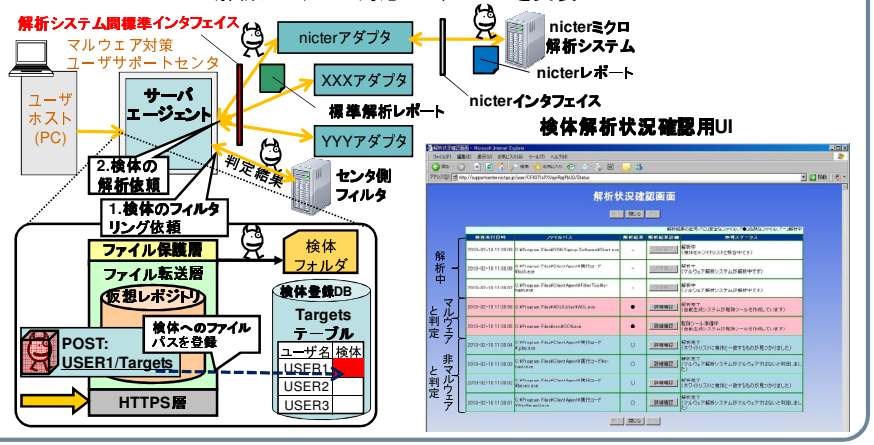
課題ウ－１：クライアントサーバプロトコルの設計及び開発

- 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
  - ✓ ファイル保護層：転送ファイルを、任意の暗号化方式と署名方式を用いてカプセル化することで，マルウェアがサーバエージェント以外に誤転送された場合の被害を防止
  - ✓ ファイル転送層：RESTアーキテクチャに基づくステートレスなプロトコル設計により，スケーラビリティの向上，通信エラー回復の容易化
  - ✓ HTTP層：エージェント間の相互認証，通信全体を暗号化



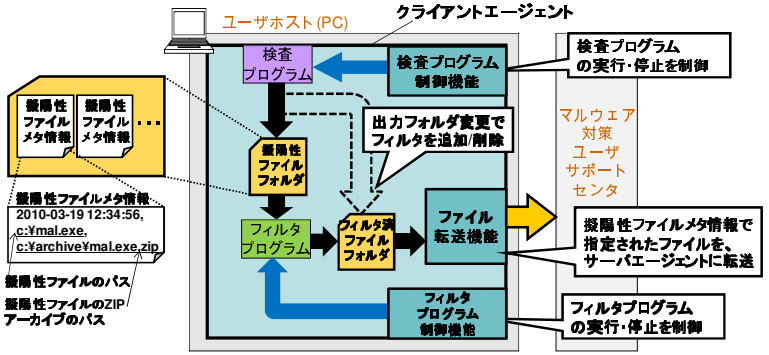
課題ウ－２－２：サーバエージェントの設計及び開発

- 解析システムとフィルタ機能と連携し，検体の解析・マルウェア判定を実現
  - ✓ 検体を管理し、解析依頼を行う機能を設計・開発
  - ✓ 様々な解析システムに対応する，解析システム間標準インタフェイスを策定
  - ✓ サーバエージェントと様々な解析システムを連携するアダプタを設計・開発。nicterミクロ解析システムに対応したアダプタを実装

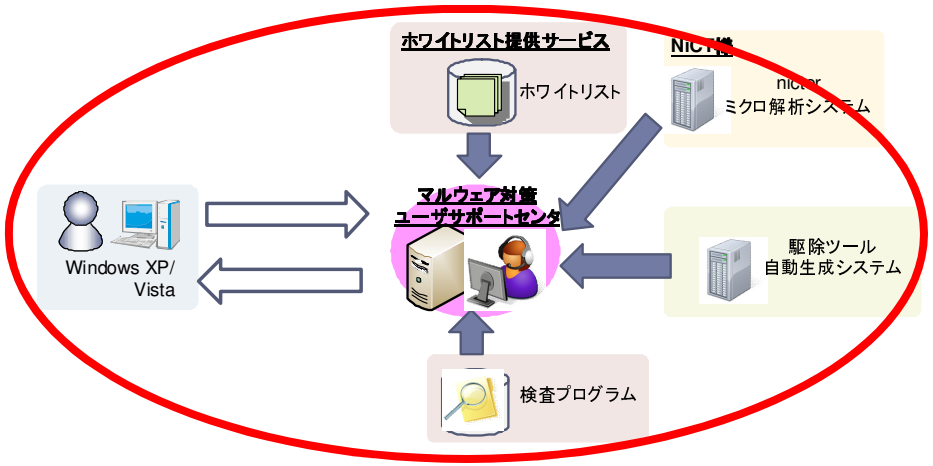


課題ウ－２－１：クライアントエージェントの設計及び開発

- 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実現
  - ✓ 擬陽性ファイルメタ情報フォーマットを策定
  - ✓ 検査プログラムとフィルタプログラムを疎結合するための、フォルダベースのファイル交換インタフェイスを設計・開発。プログラムの柔軟な入れ替え、フィルタの追加/削除を容易化
  - ✓ 3階層プロトコルを実装し、検体を安全・効率的に転送する機能を設計・開発



課題ア～ウを実環境で有効に機能させるための実証実験



2年目～3年目の実施にあたり、様々な条件、手法の検討を実施

実施環境

検証用システム

- NiCT様内に設置する検証システム⇒nicterと接続

教室、事務所など

▲委託先学校、団体のLAN環境

イベント会場

- イベント、セミナー会場に設置した端末

ネットカフェ 図書館等

- 起動する毎にユーザーデータ、環境がリセットされる端末 ＝重要データは扱わない端末

▲上記各評価を合計し、１０００以上のサンプル収集

実施委託先

研究機関

各種団体・企業

学校法人

◆本研究の主旨を説明し、エージェントのインストール、実行コードをサーバへ送信することを了解いただいたうえで委託

一般ユーザー

各種確認事項

- マルウェア検出動作
- 駆除ツール生成動作
- 駆除ツール生成～配信までの時間
- 正常な実行コードが誤検出されないこと
- 不正な実行コードが残存しないこと
- 既存セキュリティ製品との検出・駆除性能比較

▲ マルウェア検出・駆除動作のみならず、他の利用に影響を与えないことも十分に確認

検証方法

◆詳細な動作は課題ア～ウの内部検証で確認していることを前提とし、下記で問題が出ないことを確認する。

❶ レンタルPC：マルウェア検出動作を主体に検証

❷ 協力先または個人所有PC：クライアントエージェントをダウンロード/インストールして使用いただき。正常なアプリケーションがマルウェアとして検出されないことを主体に検証

❸ イベント会場にPC端末をオンラインで設置、「マルウェア探索コンテスト」のような形で来場者に積極的に検出テストを試行いただく

▲ログ解析、アンケート等により検証結果収集

平成21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」の開発成果について

1. これまで得られた成果（特許出願や論文発表等）

	国内出願	国外出願	研究論文	その他 研究発表	報道発表	展示会	標準化提案
マルウェアユーザサポート システムの研究開発	2件	0件	0件	2件	0件	0件	0件