# nicterと連携したマルウェア対策技術の紹介

株式会社日立製作所
KDDI株式会社

本研究は、(独)情報通信研究機構(NICT)委託研究
「マルウェア対策ユーザサポートシステムの研究開発」の一部です。

# アウトライン

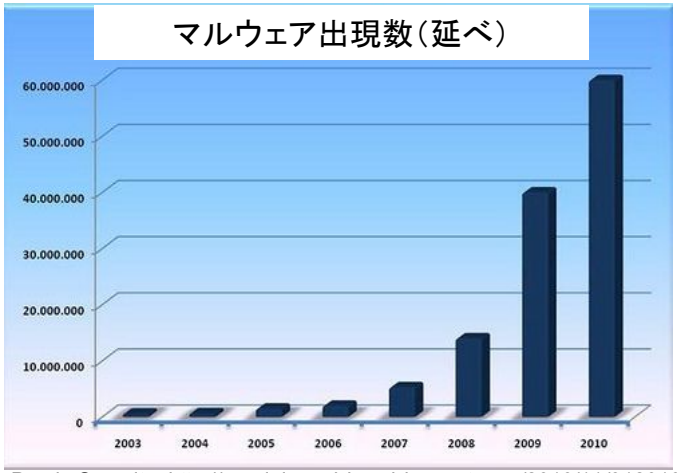
- １．研究開発概要
- ２．研究開発成果概要
- ３．実証実験
- ４．まとめ

# 1.研究開発概要

# 研究開発の背景

既存アンチウイルスソフト ⇨ マルウェアのデータ構造を記述した定義ファイルを用いて検知・駆除

- 1日に数千から数万に上る、大量の新種マルウェアが発生




Panda Security, http://pandajapanblogs.blogspot.com/2010/11/31201010.html

- データ構造を変えながら増殖を繰り返す、「自己変貌型マルウェア」の出現
- 多くのPCリソースを使用
  （CPU使用率20~60%、100%になる場合も）

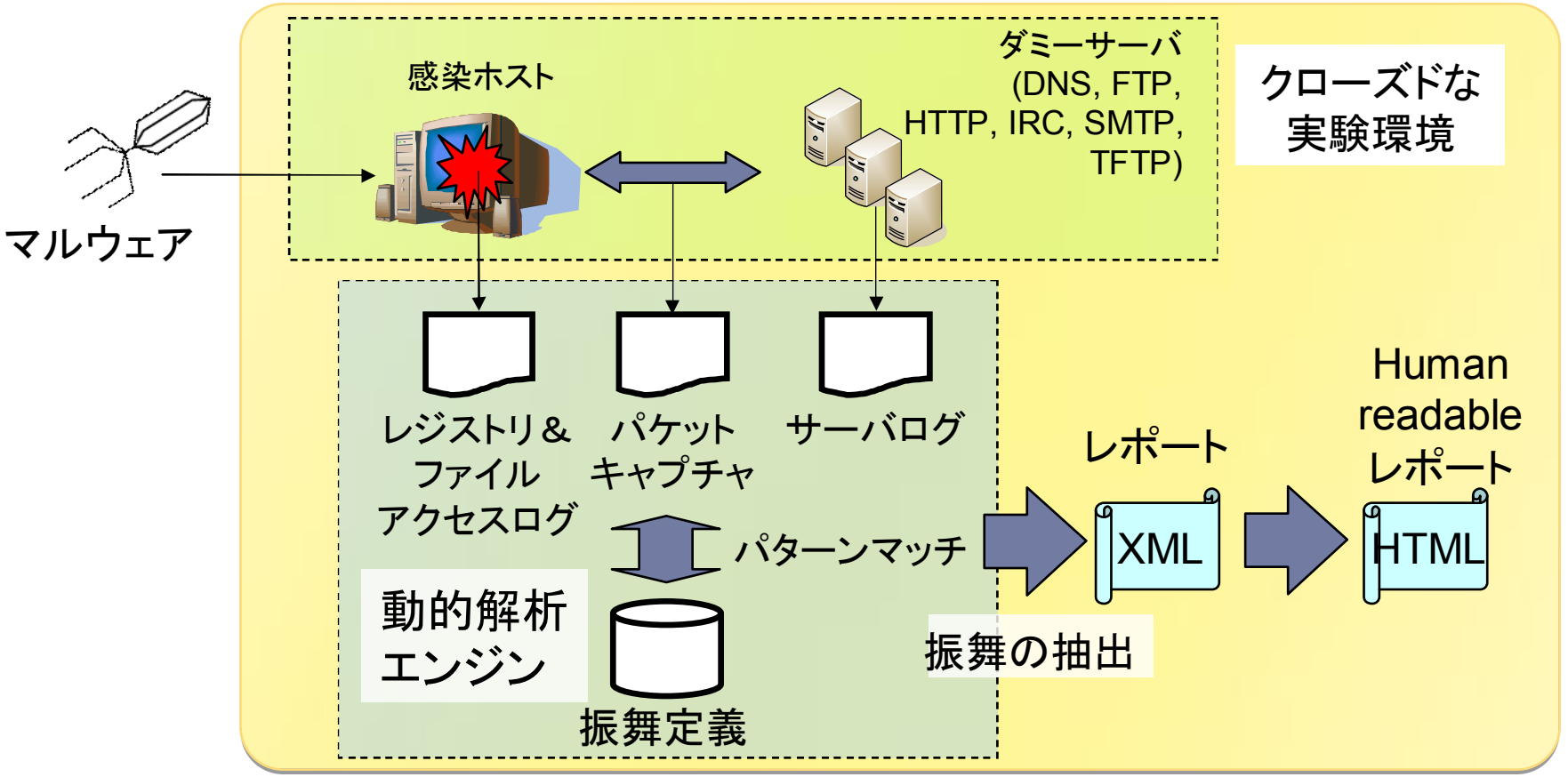
http://www.symantec.com/business/support/index?page=content&id=TECH101254

⇩

- 定義ファイルが対応しないマルウェアの効率的な検知・駆除が困難
- ユーザPCの利便性を損なう

# nicterミクロ解析システム+

- NICTが研究開発を行っているマルウェア動的解析システム
- 実行環境内でプログラムを実行し、挙動を基にマルウェアを検知




+D.Inoue, et.al, “Malware Behavior Analysis in Isolated Miniature Network for Revealing Malware’s Network Activity,” IEEE International Conference of Communications 2008 Proceedings, pp.1715-1722, 2008.

# 研究開発の目的

- nicterミクロ解析システムと連携し、既存アンチウイルスソフトが対応しないマルウェアの検出および自動駆除の仕組みを実現

- ユーザPCに負荷のかからないマルウェア対策を実現

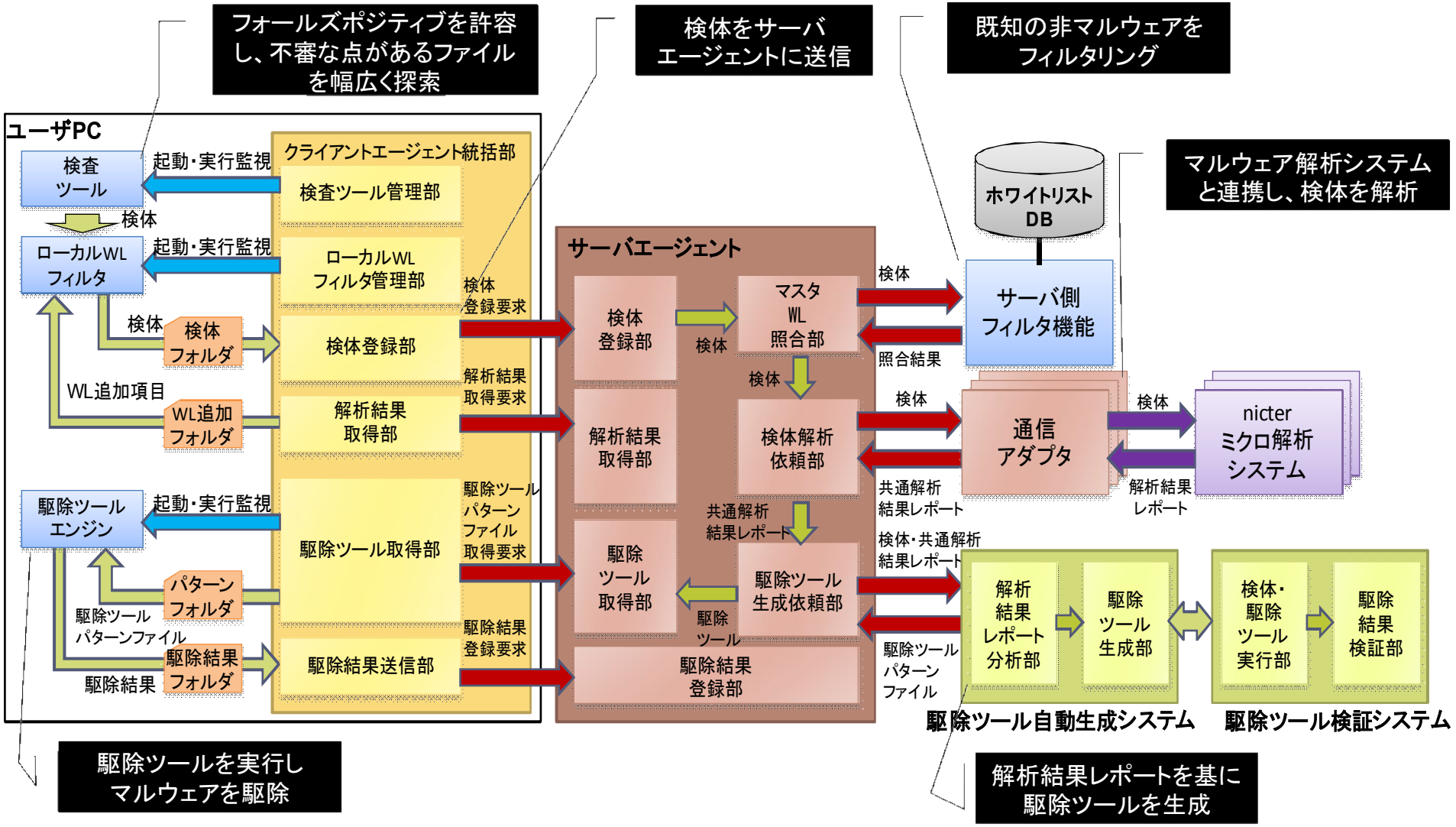
# 研究開発の最終目標

- マルウェア対策ユーザサポートフレームワークの確立
  1. ユーザPCに負荷をかけずに、擬陽性ファイルを発見
  2. 擬陽性ファイルをサポートセンタで解析、マルウェアを検知
  3. マルウェア駆除ツールを自動的に生成、マルウェアを駆除

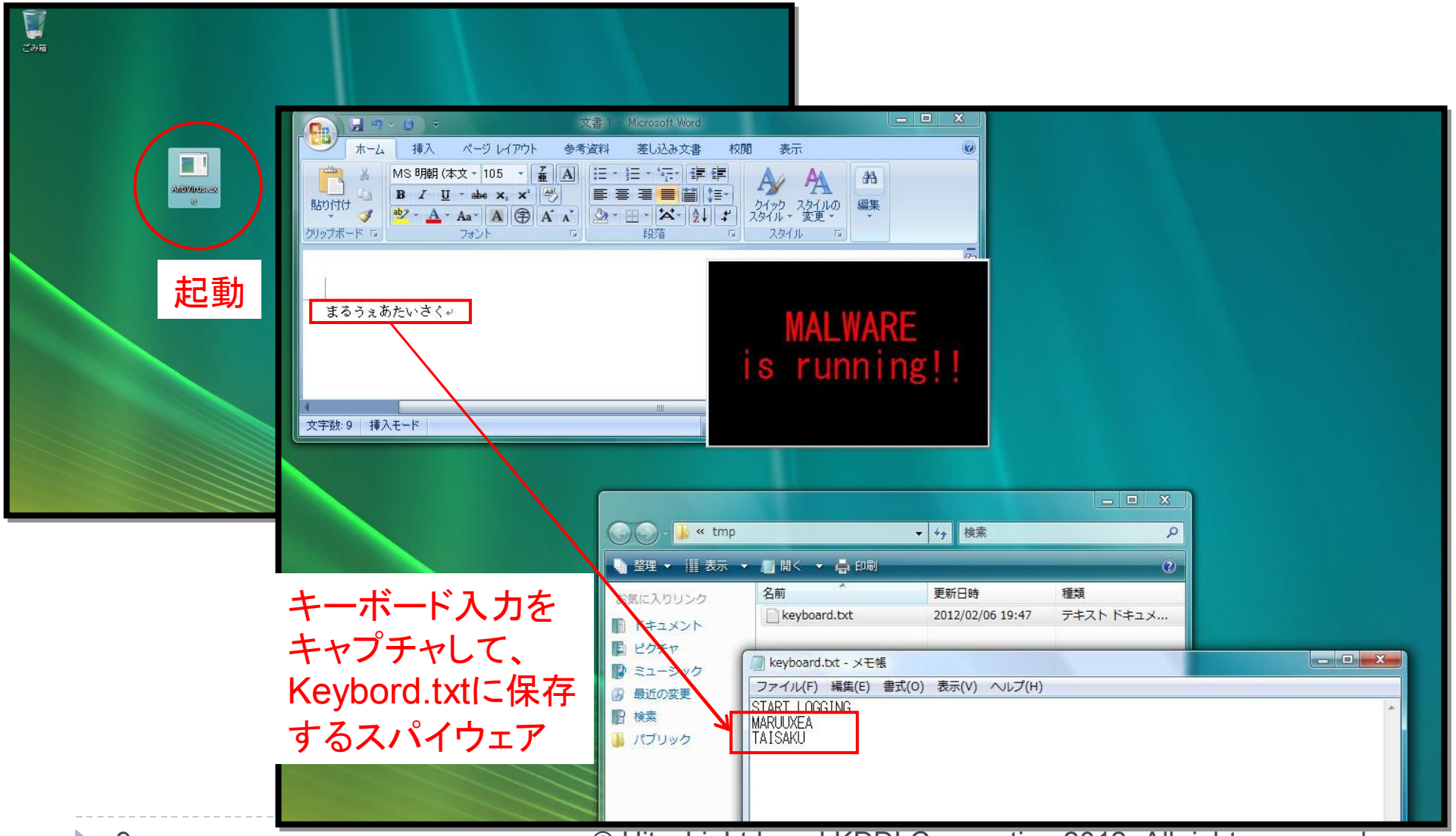
- 擬陽性ファイル発見～駆除ツール提供≒10分

# 2.研究開発成果概要

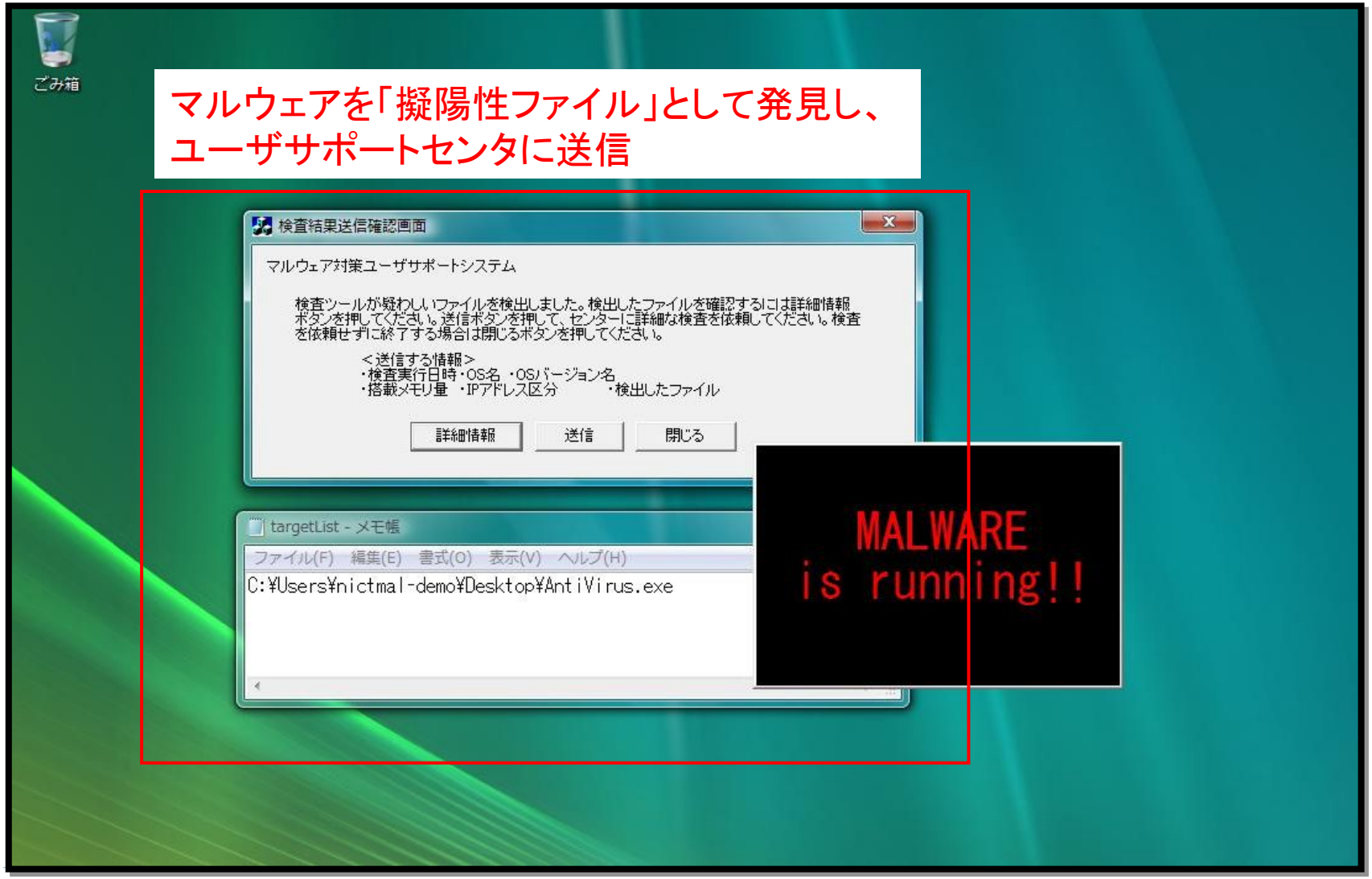
# 開発したユーザサポートシステムの構成



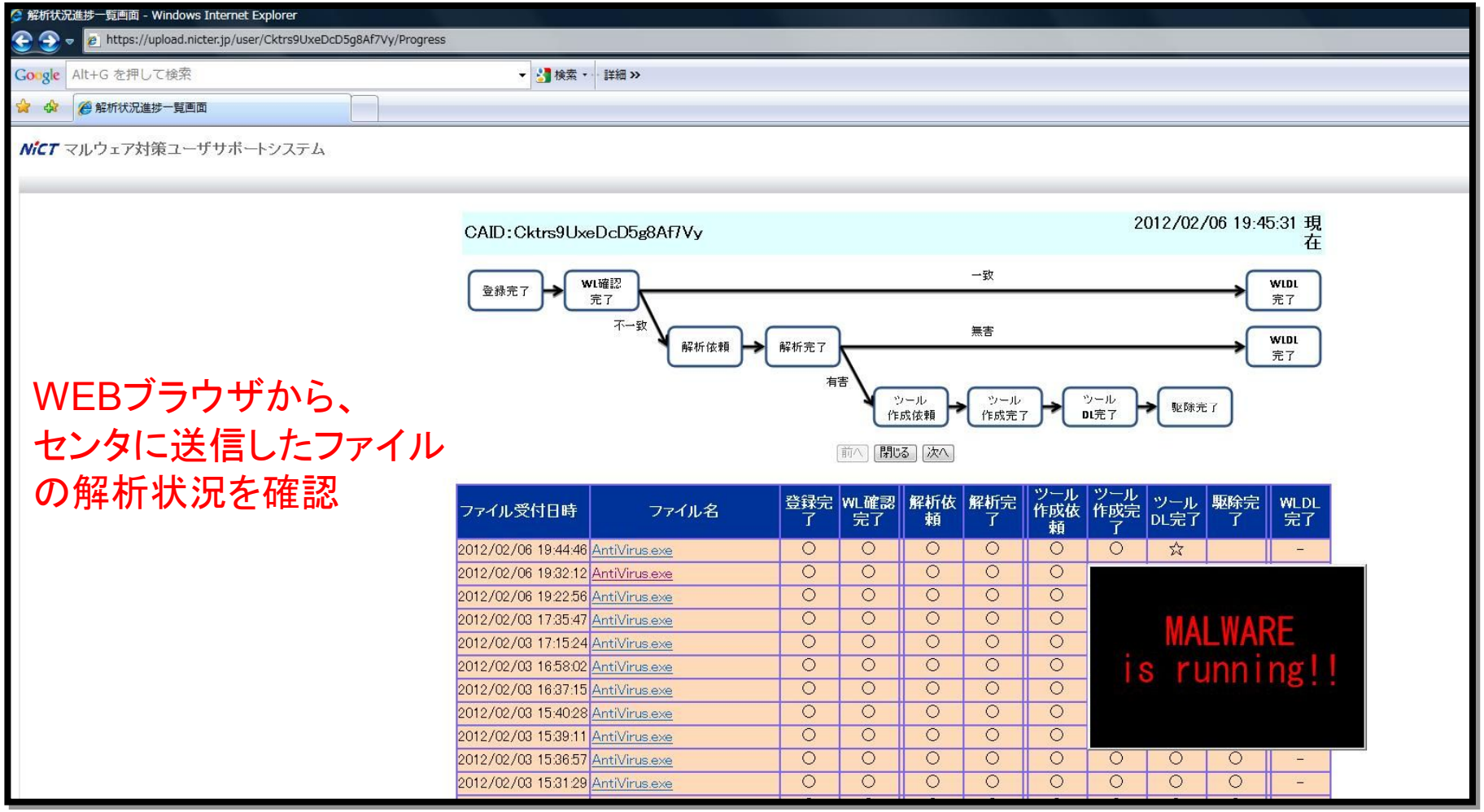
# 実行例：マルウェアの起動



# 実行例：擬陽性ファイルの発見・送信



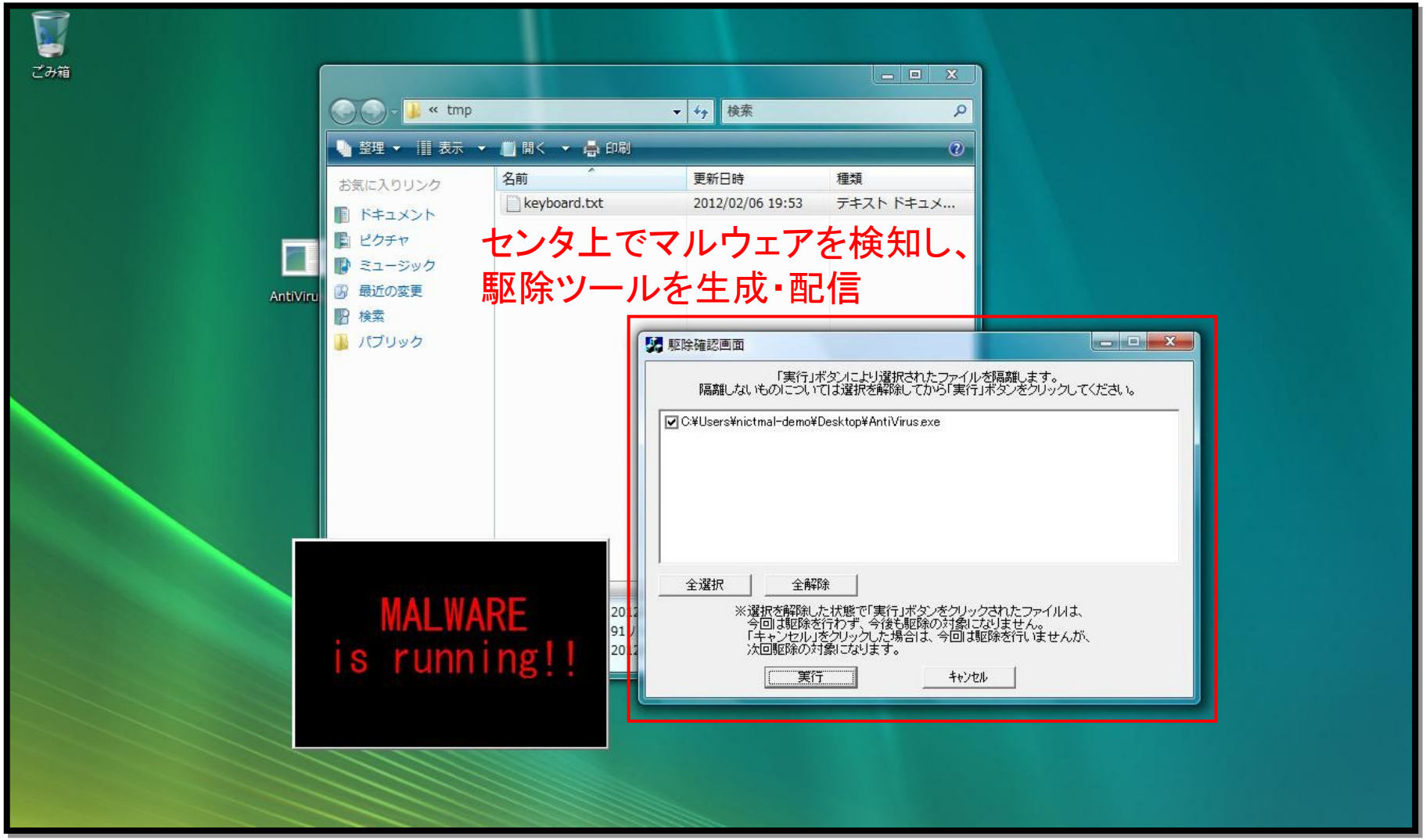
# 実行例：解析状況確認画面



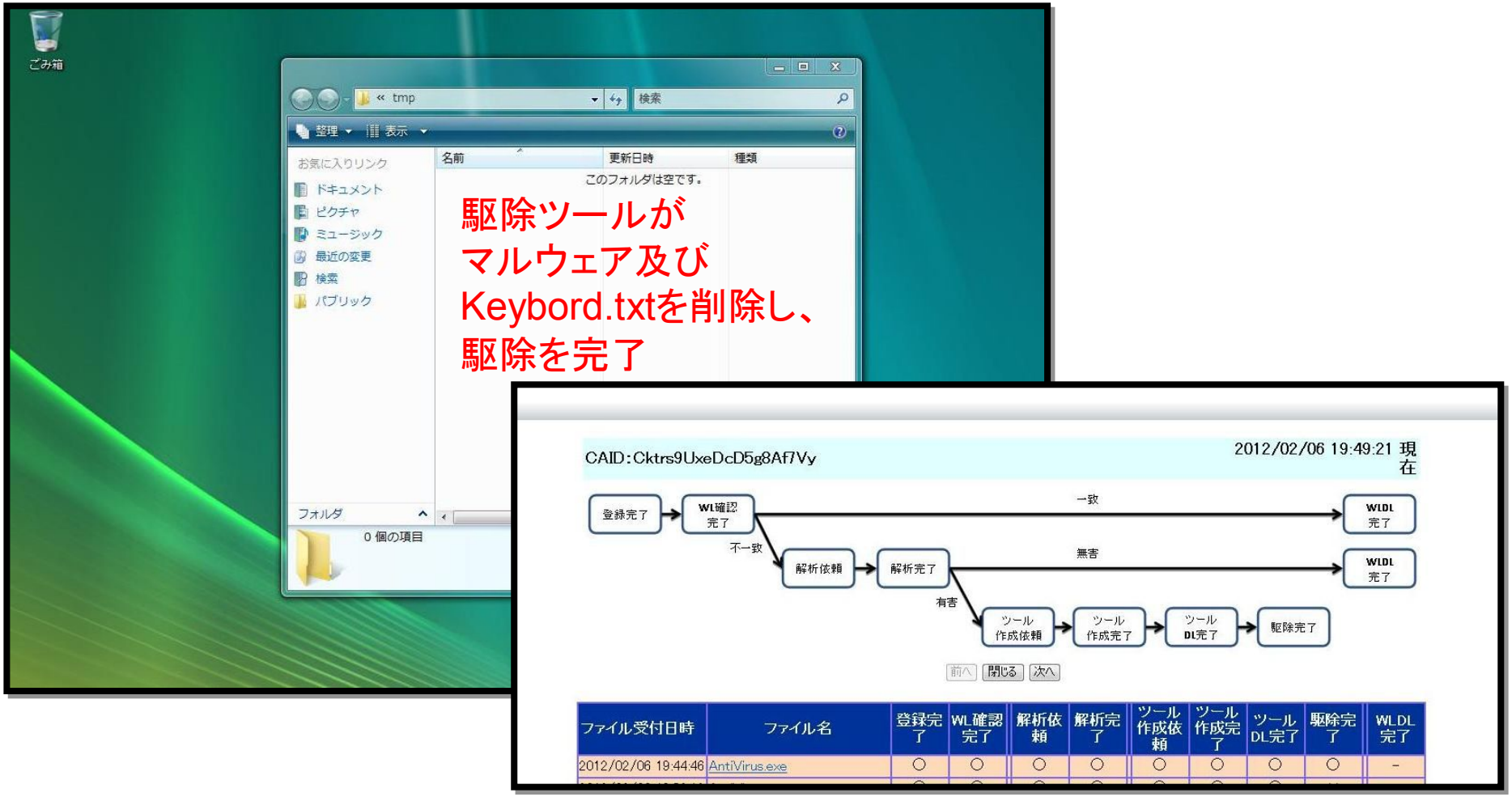

| ファイル受付日時 | ファイル名 | 登録完了 | WL確認完了 | 解析依頼 | 解析完了 | ツール作成依頼 | ツール作成完了 | ツールDL完了 | 駆除完了 | WLDL完了 |
|---|---|---|---|---|---|---|---|---|---|---|
| 2012/02/06 19:44:46 | AntiVirus.exe | ○ | ○ | ○ | ○ | ○ | ○ | ☆ | | - |
| 2012/02/06 19:32:12 | AntiVirus.exe | ○ | ○ | ○ | ○ | ○ | | | | |
| 2012/02/06 19:22:56 | AntiVirus.exe | ○ | ○ | ○ | ○ | ○ | | | | |
| 2012/02/03 17:35:47 | AntiVirus.exe | ○ | ○ | ○ | ○ | ○ | | | | |
| 2012/02/03 17:15:24 | AntiVirus.exe | ○ | ○ | ○ | ○ | ○ | | | | |
| 2012/02/03 16:58:02 | AntiVirus.exe | ○ | ○ | ○ | ○ | ○ | | | | |
| 2012/02/03 16:37:15 | AntiVirus.exe | ○ | ○ | ○ | ○ | ○ | | | | |
| 2012/02/03 15:40:28 | AntiVirus.exe | ○ | ○ | ○ | ○ | ○ | | | | |
| 2012/02/03 15:39:11 | AntiVirus.exe | ○ | ○ | ○ | ○ | ○ | | | | |
| 2012/02/03 15:36:57 | AntiVirus.exe | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | - |
| 2012/02/03 15:31:29 | AntiVirus.exe | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | - |

WEBブラウザから、
センタに送信したファイル
の解析状況を確認

# 実行例：駆除ツールの生成・配信



# 実行例：駆除完了



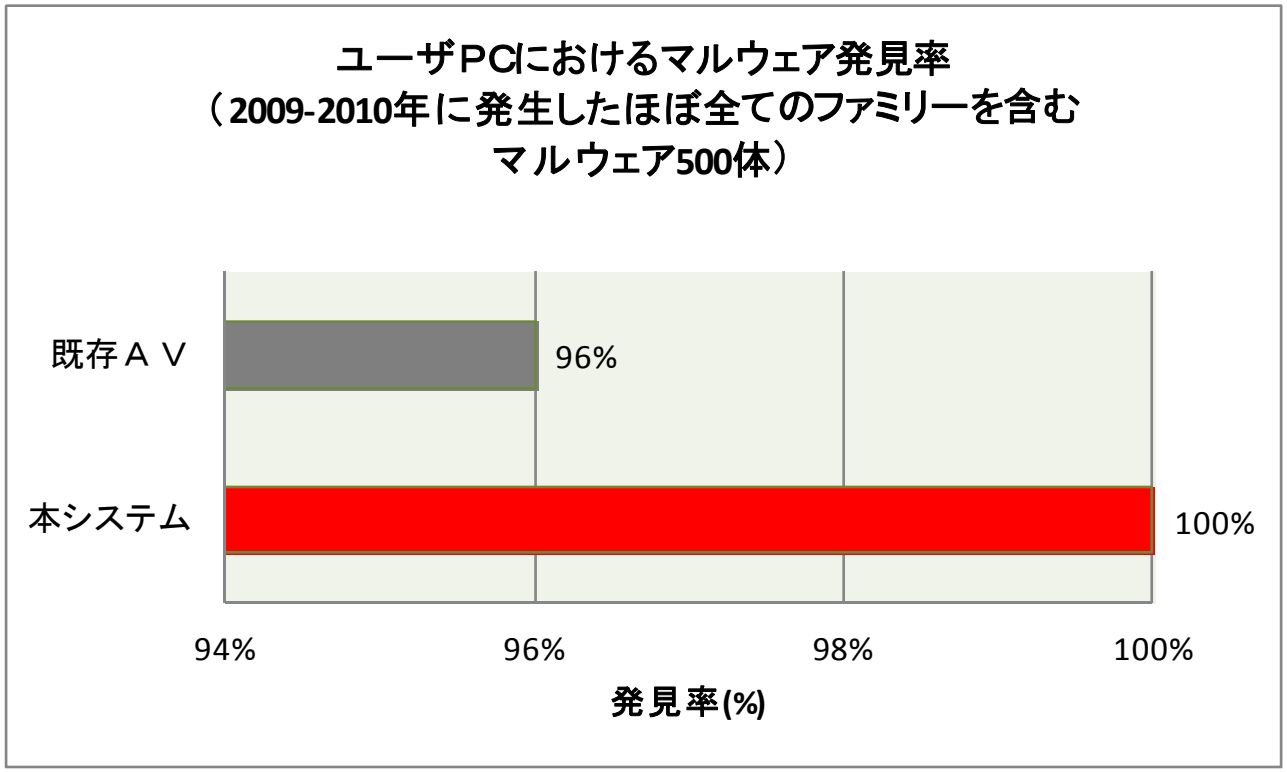
# システムの性能指標

プロジェクトの最終目標を基にシステムの性能指標を導出

- マルウェア対策ユーザサポートフレームワークの確立 →(1)(2)(4)(5)
- 擬陽性ファイル発見～駆除ツール提供≒10分 →(3)

- (1)マルウェア発見率
  - PCに侵入したマルウェアを、漏れなく発見できるか？
- (2)マルウェア駆除性能
  - 検知されたマルウェアを自動駆除し、影響を無害化できるか？
- (3)処理時間
  - 被害が拡大する前に、マルウェアの検知・駆除処理を完了できるか？
- (4)ユーザPCの負荷
  - PC側に負荷がかからないか？
- (5)スケーラビリティ
  - 多数のユーザを収容可能な、スケーラブルなシステムが実現できるか？

# マルウェア発見率




| 既存AVが見逃したファミリーの一例 |
|---|
| Agobot |
| Drefier |
| Dsbot |
| FlyAgent |
| Frag |
| Gamania |
| HakagIan |
| Ircbot |
| Magania |
| MarioF |
| Virut |

既存AVが対応しないものを含む、全てのマルウェアを擬陽性ファイルとして発見

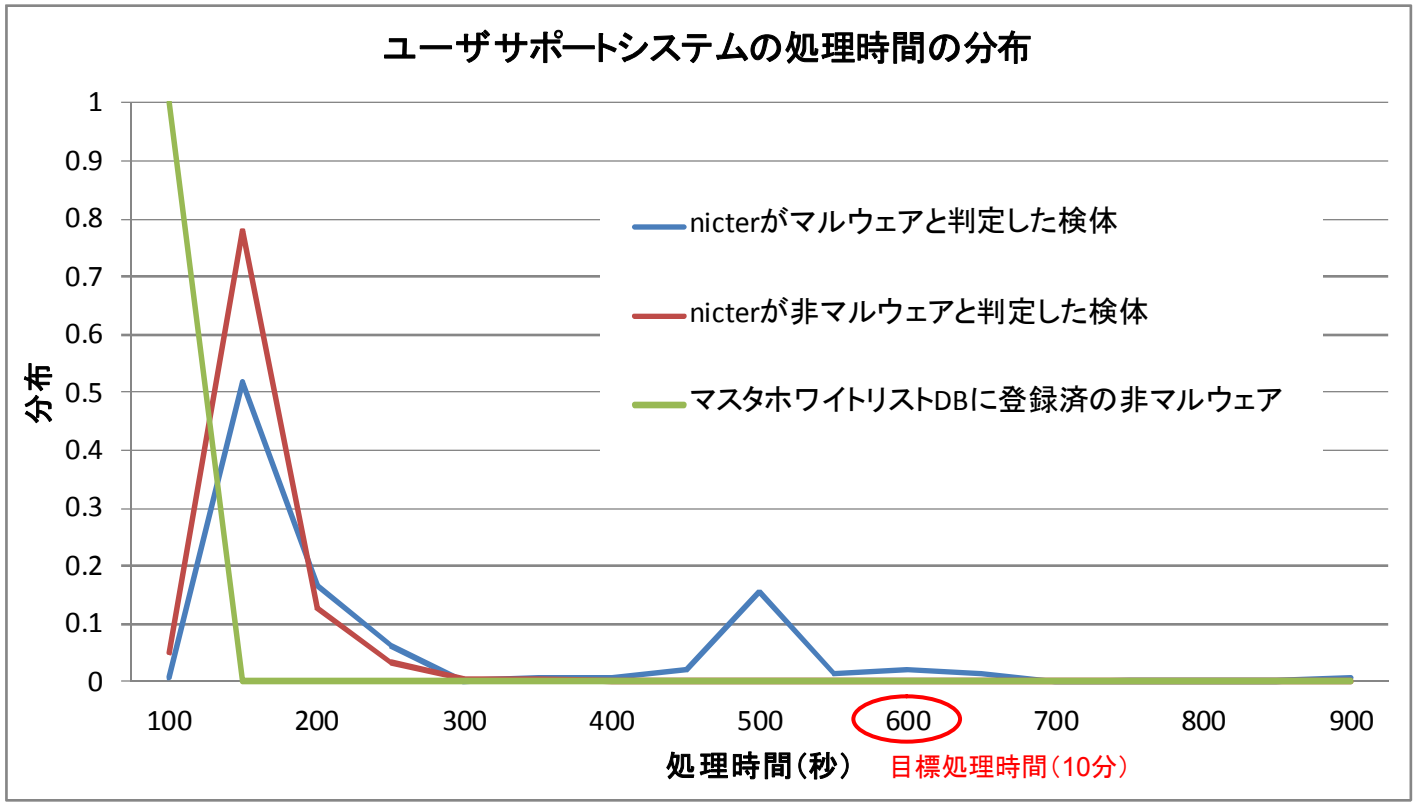
# マルウェア駆除性能

| 項目 | 駆除対象マルウェア | 本システム | 既存AV |
|---|---|---|---|
| 設定ファイルの削除 | Trojan.win32/Ircbrute （マルウェア本体） | ○ | ○ |
| | 作成 → C:¥RECYCLER¥...¥acleaner.exe | ○ | ○ |
| | 作成 → C:¥RECYCLER¥...¥Desktop.ini | ○ | × |
| レジストリの削除 | VirTool:WIn32/DelfInject.gen!BI （マルウェア本体） | ○ | ○ |
| | 作成 → C:¥Users¥...¥Roaming¥Reader_sl.exe | ○ | ○ |
| | 作成 → HKLM¥Software¥Microsoft¥...¥¥Run,patches | ○ | × |
| 実行モジュールの削除 | TrojanDropper:Win32/Lukicsel.B （マルウェア本体） | ○ | ○ |
| | 作成 → C:¥windows¥system32¥cryptnet32.dll | ○ | ○ |
| | 作成 → C:¥windowws¥sytem32¥shimg.dll | ○ | × |

（○:駆除成功　×:駆除せず）

挙動解析結果を利用してマルウェアを駆除するため、本体に加えて、マルウェアが作成したファイル・レジストリを、きめ細かく削除

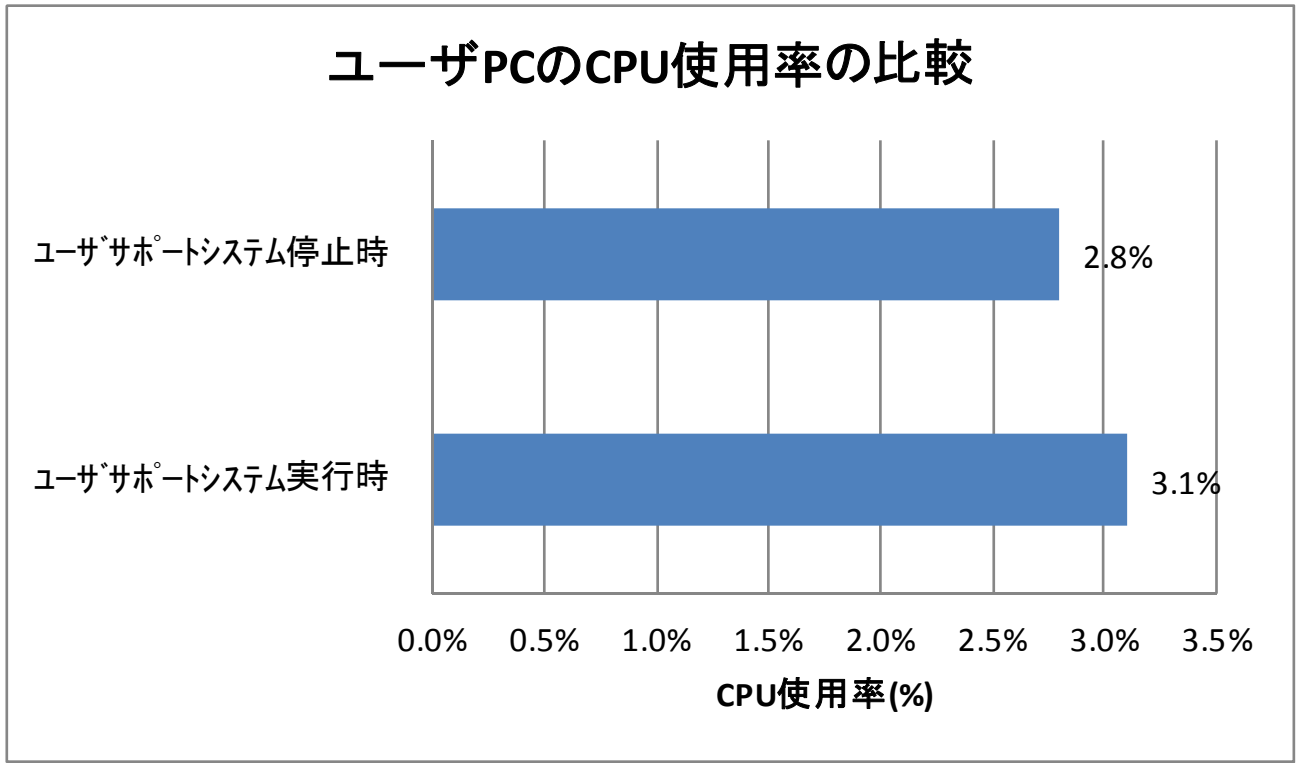
# 処理時間




※処理時間・・・検体受信から解析完了(マルウェアの場合は駆除ツール生成完了)までにかかる時間

10分以内に98%のマルウェア検体の処理を完了
(マルウェア検体の平均処理時間:4分42秒)

# ユーザPCの負荷



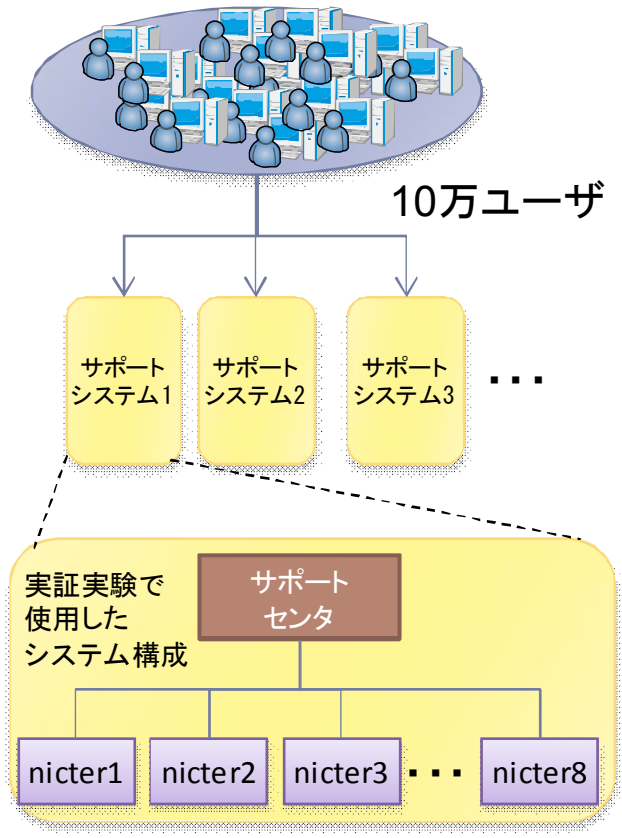

ユーザPCのCPU使用率の上昇は0.3%程度

# スケーラビリティ(1/2)

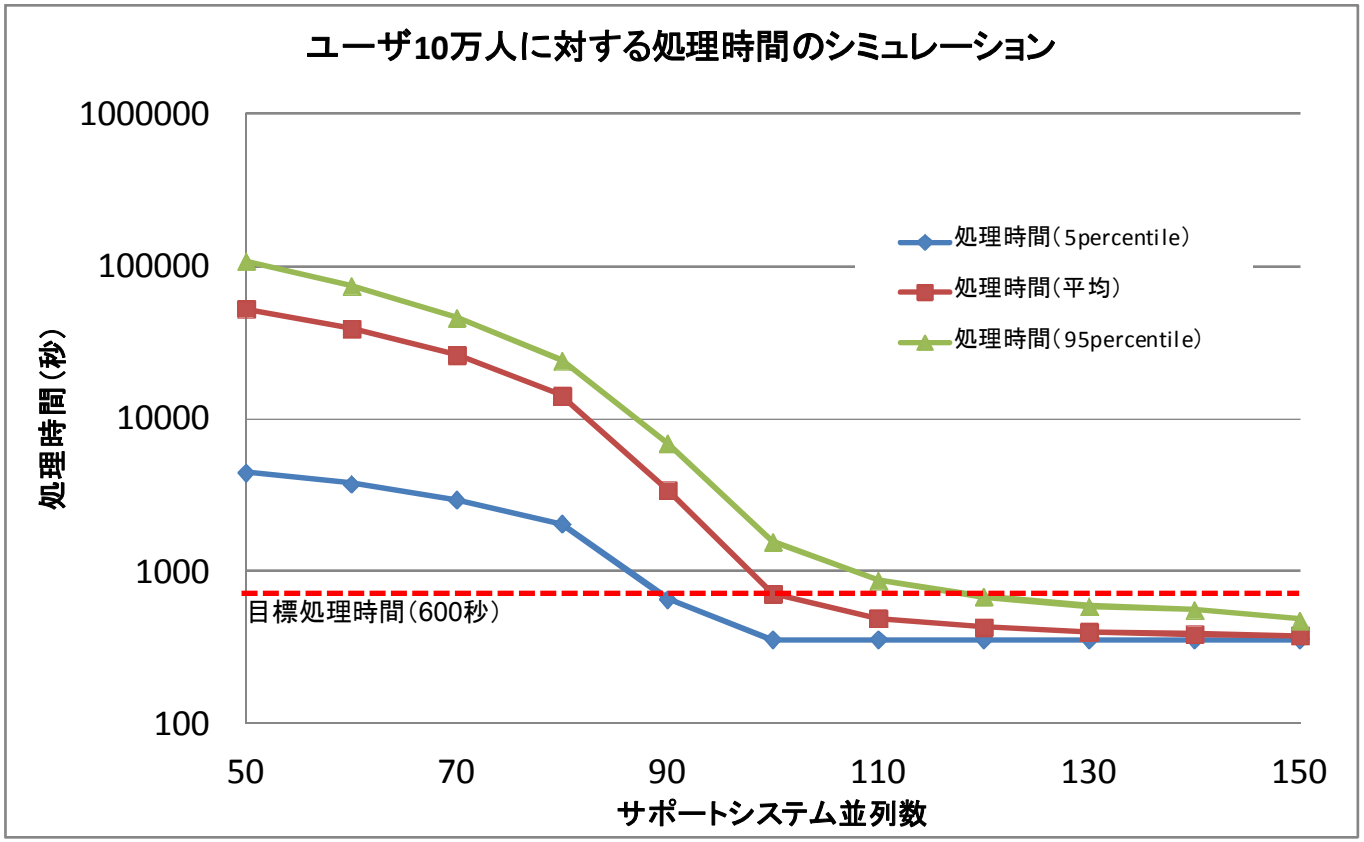
10万ユーザがマルウェアを送信した場合に、待ち時間無く処理するためには、
実証実験で用いた規模のサポートシステムが何台必要かを算出

・待ち行列網理論を用いて、ユーザサポートシステムの処理をモデル化
・シミュレーションパラメータ（実証実験で得られた値を基に設定）

| パラメータ | 値 |
|---|---|
| ユーザ数（人） | 100,000 |
| nicter解析時間（秒） | 300 |
| nicter実行環境復旧時間（秒） | 300 |
| その他処理時間（秒） | 60 |
| 1秒あたりに送信される検体数 | 6.2 |
| Nicterミクロ解析システム並列数 | 8 |
| 検体がマルウェアである確率 | 100%<br>（システムに最も負荷がかかる状況を想定） |



# スケーラビリティ(2/2)

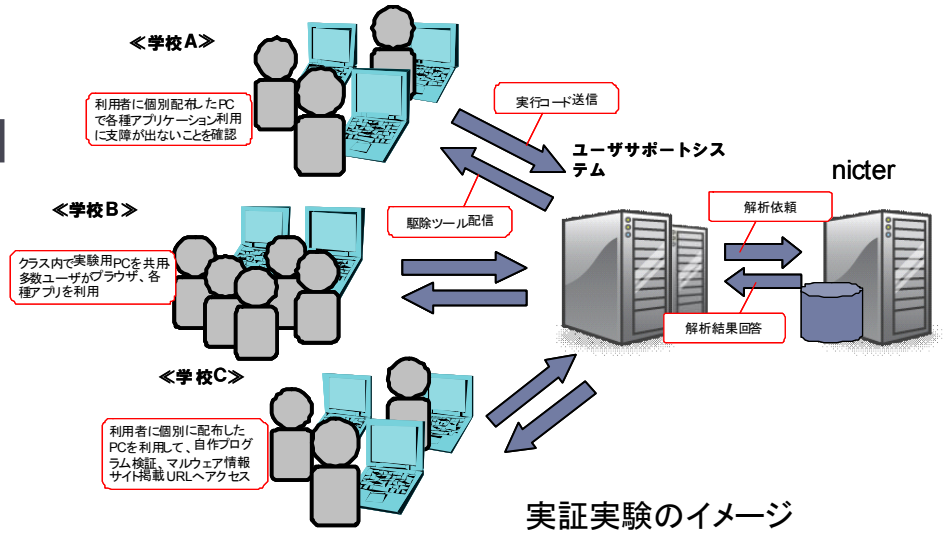



ユーザ数の0.8%程度の解析システム数(約100並列)で、
10万ユーザが送信したマルウェア検体を、目標処理時間内に処理

# 3.実証実験

# 実証実験の概要

- 実験期間
  - 2011年9月6日～12月31日



実証実験のイメージ

- 実験協力先機関
  - 玉川大学工学部（PC10台専用）
  - 宮城教育大学　情報処理センター（PC10台専用）
  - 鳴門教育大学　情報処理センター（PC10台専用）
  - 大阪情報コンピュータ専門学校（PC6台専用）
  - 大阪日本コンピュータ専門学校（PC4台50人で共用）

# 実証実験内容

- 各協力先へシステム概要・実験趣旨の説明会を実施
  - ✓ 実験結果については、協力先へ伺い、直接教員および学生から詳細なヒアリングを実施。定期的なゼミへも参加（玉川大学）
- 実験アプローチ
  - ✓ PC総数45台、利用者数50～80人で実験を実施
    - 共用PCではより多様な利用者環境での動作検証を、専用PCではより専門的で高度な実験を行っていただいた。
    - 実験によってマルウェア感染などのリスクも想定されるため、直接利用者をサポート可能な実験規模とした。
  - ✓ 積極的な非マルウェア系ソフトウェアのインストール
    - システムの処理性能や動作の正常性などを総合的に検証
  - ✓ マルウェア情報系サイトなどからの被疑検体取得
    - マルウェアの検知精度、駆除ツールの動作などを検証
    - 授業の課題による自作プログラムによる動作検証も実施

# 実験データ集計

全実験期間(2011. 9. 6～2011. 12. 31)の処理結果

| | |
|---|---|
| 送信された検体数 | 1985 |
| nicterが解析した検体数　※1 | 998 |
| nicterがマルウェアと判定した検体数　※2 | 144 |
| 駆除ツール実行数　※3 | 125 |
| 駆除成功数　※4 | 122 |
| マスタホワイトリスト・フィルタ率　※5 | 総合：38%、デフォルト時：31% |
| マルウェア検知・駆除実行時間 | 平均：282秒、最大：980秒、最少：146秒 |

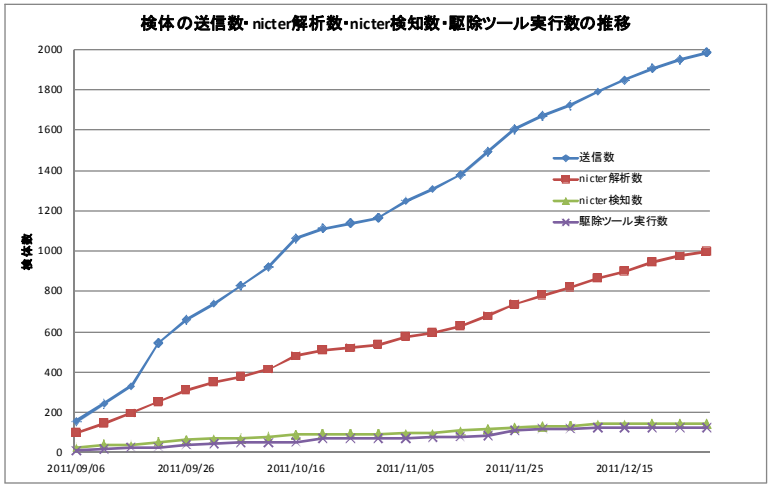
※1：ホワイトリスト内、あるいは既に解析済みの検体については解析を行わないため、送信された検体数より少なくなる

※2：FalsePositiveを含む

※3：ユーザによる駆除キャンセルあり

※4：一部設定ファイルの削除失敗(実行ファイルについては削除)

※5：ホワイトリストの学習によりフィルタ率が7%向上



# マルウェア検知結果

- 本システムで既存ウイルス対策ソフト未対応のマルウェアを検出
  - ✓ 本システムでマルウェアと判定した検体について、ウイルス対策ソフト（Microsoft Security Essentials）で継続的にスキャンしたところ、本システム検出の約3週間後にマルウェアとして検知された検体（1体）を確認
  - ✓ 検体の概要

| | |
|---|---|
| 検体名 | TrojanSpy:Win32/Bancos.AEQ |
| 説明 | オンラインバンキングのIDやパスワードなどを窃取するトロイの木馬の1種 |
| 本システム検出日 | 2011-9-24 |
| MSE検出日 | 2011-10-18 |
| 本システムでの判定根拠 | 動的解析により、同検体がPC内のMicrosoft Phonebookファイルを検索している活動等からマルウェアと判定 |

nicter解析レポート

```
<MaliciousCodeXML output="JP">
  <MaliciousCode>
    <Name>24603.exe</Name>
  <threat>
    <threat_type>WORM</threat_type>
  </threat>
・・・
<judgment>1</judgment>
  <Action>
    <showwindow>・・・
    <createFile>・・・
    <search>・・・
      <classification type="WORM"/>
        <file><![CDATA[ ・・・¥*.pbk]]></file>
        <file><![CDATA[ ・・・¥*.pbk]]></file>
        ・・・
    </search>
    <openFile>
    ・・・・
```

  - ✓ トロイの木馬は亜種が膨大なため、ウイルス対策ソフトでの対応が遅れたと考えられる。
  - ✓ 既存ウイルス対策ソフトより3週間早くマルウェアを検出できたことで、本システムでのパターンファイルに依存しないマルウェア検知手法の有効性を確認することができた。

# ユーザビリティ

**協力先ユーザからアンケート、ヒアリングで寄せられたご意見**

◆ほとんど違和感を感じずに利用でき、これで効果が見込めるのならばスタンダードになってもよいのではと感じた。実用化されれば利用したい。

◆実用しているソフトウェアのファイルが検知されたが、駆除されては困るので駆除を行わなかった。選択できるのはよいと思う。

◆怪しいものをはっきりと知らせてくれて、問題があればすぐに駆除もできるので有効である。誤検出があれば訂正（駆除対象外）もできるのでよいと思う。（誤検出が出ないほうがよいが）

◆普段遊んでいるゲームや、ネットワーク系パフォーマンス監視ソフト、LibreOfficeという事務系ソフトでもマルウェア判定された。もう少し正確にならないか。

◆ホワイトリスト一覧を参照したり、設定できたら、と感じた。

◆想像していたよりもスムーズに起動し、使いやすかった。また、マルウェアの被害を受けてもすぐに対応できるという安心感があった。

# 4.まとめ

# まとめと今後の課題

- 既存アンチウイルスソフト
  - ✓ 新種マルウェアへの対策の遅れ、ユーザPCへの負荷
- nicterミクロ解析システム
  - ✓ 挙動解析を行い、マルウェアを検知
- マルウェア対策ユーザサポートシステム
  - ✓ nicterと連携し、ユーザPCに侵入したマルウェアを検知
  - ✓ 解析結果レポートに基づき、マルウェアを自動駆除
- 実証実験
  - ✓ 既存アンチウイルスソフトが対応する3週間前に、未知のマルウェアを検知
  - ✓ 検知・駆除処理を平均4分42秒で完了
- 今後の課題
  - ✓ 特定のPC操作（例：ユーザが金融サイトにアクセス）に連動して活動を活性化するマルウェアが増えており、効率的な解析手段の確立が必要