Vol.2012-DPS-150 No.11
Vol.2012-CSEC-56 No.11
2012/2/29

PC 内のファイル改ざんを行うマルウェアの検知手法

澤 村 隆 志[†1]　ベッド B. ビスタ[†1]　高 田 豊 雄[†1]

近年，マルウェア検知は，従来のパターンマッチング法の弱点を補うために，振る舞い検知を行うビヘイビア法の研究が盛んに行われている．これにより，未知のマルウェアに対しても対応することが可能である．しかし，これらの手法を利用しても 100%検知可能ではなく，検知を免れる手法も考案されている．そこで，我々は，ビヘイビア法の補完として，従来のセキュリティツールを突破された後，ユーザの PC への被害から，マルウェアの存在を検知し，被害を最小限に抑えることが可能なのではないかと考えた．本稿では，数多くのマルウェアの中から，近年，被害が増加しているランサムウェアに注目し，このマルウェアが，PC 内に進入した後の挙動から，検知する手法を提案する．

A Proposal of Detection Method of Malware that Modifies Files inside PC.

Takashi Sawamura,[†1] Bhed Bahadur Bista[†1]
and Toyoo Takata[†1]

Recently, in order to cover a weak point of pattern matching method for malware detection, many researches have paid attention to behavior method. Though behavior method could be applicable to unknown malware, it cannot completely detect malwares. Additionaly, a number of techniques to evade behavior method are proposed and actually employed. We focus on actual behavior of malwares after evading conventional anti-virus software for supplementing conventional behavior method, in order to reduce actual damages by such malwares as small as possible. In this paper, specifically, we consider ransomware detection, whose damage are increasing considerably, by observing their activity after intruding PCs.

†1 岩手県立大学大学院ソフトウェア情報学研究科
Graduate School of Software and Information Science

1. はじめに

近年のマルウェア検知は，対象のプログラムに特徴的なコードの有無を調べることで検知を行うパターンマッチング法により，既知のマルウェアに対しては，90%以上の検知率[1)]がある．しかし，パターンが登録されていない未知のマルウェアに対しては，マルウェアの発見からパターンの作成，更新という一連の作業が完了しなければ検知ができない．そのため，未知のマルウェアに対しては，対象のプログラムを実際に実行し，その振る舞いを監視するビヘイビア法の研究が盛んに行われている．動的ヒューリスティック法とも呼ばれるこの手法では，仮想環境内で，対象のプログラムを実行し，危険な行動（書き込み動作，複製動作，例外ポート通信，通信量の異常増加など）を検出することでマルウェアを検知する．現在のアンチウィルスソフトウェアでは，パターンマッチング法とビヘイビア法を組み合わせることで，様々なマルウェアに対処している．しかし，これらの手法を利用しても，検知率は 100%とはならない．例えば，ビヘイビア法の場合，仮想環境で解析を行うが，マルウェアに実環境と仮想環境とを判別する機能が備わっていた場合，検知を免れてしまう．それ以外にも，解析や検知への耐性強化を目的として，実行時の挙動を様々に変異させているポリモルフィック型マルウェアなども存在する．パターンマッチング法が通用しないポリモルフィック型マルウェアに仮想環境を判別する機能が備われば，アンチウィルスソフトウェアでは感染を防ぐことはできない．このように，既存のセキュリティツールがすべてのマルウェアを検知し安全を保つことは困難である．このことから，ビヘイビア法の補完として，マルウェアがセキュリティツールの解析，検知を免れた場合に，その後の PC への挙動からマルウェアを検知することを考える．そこで本稿では，PC 内のファイルをユーザの承諾なしに暗号化し，その復号化の代償に金銭を要求するマルウェアである，ランサムウェアに注目する．ランサムウェアは，近年，その被害が増加しており，対策を考案することは実用上も重要である．このマルウェアが，PC 内に侵入した後の動作から検知する手法について述べる．

本稿では，まず 2 章で，ランサムウェアについての関連研究と， 様々なセキュリティベンダのランサムウェアに対する対応などを述べる．3 章では，多くのランサムウェアに見られる大まかな仕組みと近年の動向について述べる．そして，4 章では，ランサムウェアを検知するために利用する技術と，その検証について述べ，5 章では，その技術を採り入れた検知システムの評価と，その結果について述べる．最後に，本稿のまとめと，今後の課題を 6 章で述べる．

Vol.2012-DPS-150 No.11
Vol.2012-CSEC-56 No.11
2012/2/29

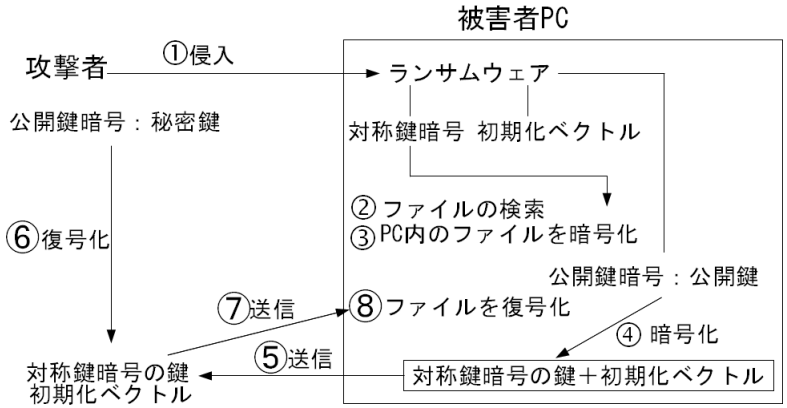

図 1 ランサムウェアの大まかな仕組み
Fig. 1 Overview of Ransomware activity

2. 関 連 研 究

ランサムウェアに関した関連研究には，Liao らの研究[2)3)] がある．この研究では，ランサムウェアの侵入，暗号化アルゴリズム，暗号化のための鍵の生成，攻撃対象のファイル，金銭の要求方法などのランサムウェアの挙動を解析している．セキュリティベンダでは，近年，ランサムウェアの被害が増加していることから，挙動に関する記事[4)5)] を掲載している．これらでは，ランサムウェアの挙動についてのみ述べられており，対策としては，“ 信頼できないサイトへのアクセス，ソフトウェアのインストールを行わない ”,“ セキュリティベンダに連絡する ”,“ セキュリティツールを常に最新にする ”,“ 企業内で教育し，未然に防止する ”,“ バックアップを取る ”，などが重要とされており，実効的な対策については一切述べられていない．そのため，セキュリティツールで侵入を未然に防ぐことができなかった場合，一般ユーザでは，的確に対処することができず，被害に遭う可能性がでてくる．

3. ランサムウェア

3.1 ランサムウェアの動作の概略

ここでは，多くのランサムウェアに見られる大まかな仕組みと，近年に発見されているランサムウェアについて述べる．**図 1** は，大まかな仕組みを示したものである．以下に，その詳細を述べる．

(1) 侵入
ランサムウェアは，トロイの木馬型に分類されるマルウェアで，近年の典型的なパターンとして，Web ページを介してユーザの PC に侵入する．このタイプは，性質上，被害者にサーバとなるファイルを実行してもらう必要がある．当然，一見して危険を察知されるような怪しげなファイル名やアイコンは使用されない．ほとんどの場合，動画の再生コーデックのインストーラ，アンチウイルスウェア，メディアプレイヤーなどの名に偽装し，被害者にダウンロード及びインストールを促す．それ以外にも，様々なソフトウェアの脆弱性を利用したり，検知や解析への耐性強化を目的として，実行時の挙動を様々に変異させている．攻撃者は，このように，様々な手段を使用して，ランサムウェアを侵入させる．

(2) ファイル検索
侵入したランサムウェアは，最初に何らかの方法で，攻撃対象となるファイルを検索する．近年のランサムウェアは，一般ユーザを対象としていることが多く，マイドキュメントや，デスクトップ上などの，Microsoft 社の Office 系のファイル，Adobe Systems 社の PDF ファイル，動画，画像，音楽など，様々な拡張子のファイルを対象としている．具体的な攻撃対象となるファイルの拡張子，フォルダ，ファイル数などは，ランサムウェアの種類によって異なる．

(3) PC 内のファイルを暗号化
ランサムウェアは，対称鍵暗号と，初期化ベクトルを生成し，これらを使用して，ファイルを暗号化する．初期化ベクトルは，同じ暗号鍵を使用しても，毎回異なる結果を生成するために必要とされる．これにより，毎回暗号鍵を替えるといった時間のかかる作業を省くことができる．

(4) 鍵の暗号化
ここでは，ファイルの暗号化に使用した，対称鍵暗号の鍵と初期化ベクトルを合わせたものを，攻撃者の公開鍵暗号の公開鍵で暗号化する．ここでは，強力な暗号化アルゴリズムが使われているため，ユーザ独力でのリカバリは実質不可能とされている．

(5) 攻撃者に鍵を送信
公開鍵暗号で暗号化された鍵を攻撃者に送信する．その後，ユーザに対して，何らかの方法で，ファイルが暗号化され，使用できないことと，その復号化に必要な金銭の額及び，金銭の受け渡し方法を伝える．支払い方法は様々だが，過去の事例として

Vol.2012-DPS-150 No.11
Vol.2012-CSEC-56 No.11
2012/2/29

は，指定した口座に振り込まない限り，30 分毎にファイルを 1 つ消去する，と宣言し，被害者を脅す，指定のウェブサイトから商品を購入させる，プレミアム SMS の送信を促す，などが挙げられる．

(6) 鍵の復号化
攻撃者は，公開鍵暗号の秘密鍵を使って，受信した暗号化後の鍵を復号化する．

(7) 被害者に鍵を送信
攻撃者は，金銭を受け取った後，復号化された対称鍵暗号の鍵を再び送信する．

(8) ファイルを復号化
ユーザは，受信した，対称鍵暗号の鍵を使って，暗号化された PC 内のファイルを復号化する．

3.2 ランサムウェアの近年の動向

次に，ランサムウェアの近年の動向について述べる．2010 年 11 月には，ユーザのメディアファイルと Office ファイルを暗号化するランサムウェアが報告[6] されている．2011 年にも様々な亜種[7][8] が登場しており，独力でのリカバリが実質不可能であるため，唯一の対策手段としては，ファイルのバックアップしかないのが現状である．一方，2010 年 1 月には，ランサムウェアとスケアウェアを組み合わせた新たなマルウェアが報告[9] されている．スケアウェアとは，偽のセキュリティツールのことである．このマルウェアは，まず，書類や動画，画像などのファイルを暗号化し，そのファイルが破損したかのように偽装する．次に，OS からのメッセージのように偽装したポップアップメッセージを表示させ，Windows が推奨するリカバリソフトと称した，スケアウェアのダウンロードと実行をユーザに促す．その後，ダウンロードしたスケアウェアで，ファイルの修復を試みると，“ このソフトは，無料版であるため，修復できるファイルは 1 つのみである ”というメッセージが表示され，完全に修復する場合は，89.95 ドルの製品版を購入するように誘導する．

このように，近年では，ランサムウェアでファイルを人質に取り，スケアウェアで金銭を要求するという一連の攻撃手法が確立されつつある．攻撃者にとっては，金銭を得た後，確実にファイルを復号化することは，次への攻撃に繋がることになるが，被害者側は，要求さえ飲めば，復号化の手段を得られる，という根拠のない手段に頼るのは，非常に危険である．また，このマルウェアの特徴としては，偽物だと判断しにくいインタフェースにすることで，スケアウェアを本物のリカバリソフトと信じさせ，詐欺の被害に遭っていることに気づかせないことである．そのため，偽のリカバリソフトである，スケアウェアを信頼したまま運用し続けたり，他人にスケアウェアを薦めてしまうことで，被害が増加する恐れもある．このような場合，ランサムウェアの被害に遭っている可能性をユーザに通知することで，その被害を抑える必要がある．そのために，1 章で述べた通り，ビヘイビア法の補完として，既存のセキュリティツールが突破された後にランサムウェアの挙動から検知を行う手法を提案する．主な挙動である，侵入，鍵の生成，ファイルの暗号化は，ランサムウェアの種類によって様々であるが，“ 暗号化されたファイルの生成 ”という部分の挙動は共通しているため，この特徴を利用して検知を行う．

4. 検知に用いる技術

4.1 BFA アルゴリズム

次に，暗号化されたファイルを検知するために用いる技術について述べる．本研究では，McDaniel らが行った未知のファイルのタイプを分析する研究[10] で使われている，BFA（Byte Frequency Analysis）アルゴリズムを参考にしたアルゴリズムにより検知を行う．BFA アルゴリズムは，ファイルのバイト配列から特徴となるパターンを生成し，未知のファイルのパターンと比較することで，ファイルタイプを識別する．従来では，このファイルタイプの判別は，拡張子とマジックナンバーで行なっていた．しかし，拡張子，マジックナンバーは，共に，偽装することが容易であり，悪意を持ったファイルは，必然的に，自身の性質を隠蔽しようとする．ファイルの真の性質を自動的に認識することは，PC を保護する上で重要である．そのために考案されたのが，この BFA アルゴリズムである．このアルゴリズムでは，ファイルの先頭と後尾の特定の場所に現れるバイト値に注目し，各ファイルのパターンとパターンの出現頻度の違いを特定する．そして，そのパターンと出現頻度の違いをシグネチャとして用いて未知のファイルを分析する．この手法では，ファイルタイプ毎にシグネチャを作成しなければならないため，ファイルタイプが追加されるたびに，大量の分析作業が必要となる．また，実験結果から，一度のパターン分析でファイルのタイプを必ず識別できるわけではなく，複数のシグネチャに当てはまるパターンを持っているケースも確認されているため，繰り返し分析を行う必要がある．本稿の提案手法は，ランサムウェアの暗号化に迅速に対応するため，一定値以上の速度で動作することが求められる．このことから，BFA アルゴリズムをこのまま本研究に用いることはできない．よって，本稿の提案手法に適した，暗号化されたファイルの識別に特化した新たなアルゴリズムを構築する必要がある．

次に，BFA アルゴリズムを参考にした，暗号化されたファイルの検知を行うためのパターン抽出方法について述べる．

Vol.2012-DPS-150 No.11
Vol.2012-CSEC-56 No.11
2012/2/29

表 1 スコア算出の例
Table 1 Example of calculate the score

要素数 5	454e4
”0”の出現数	0
度数分布（スコア）	0 = 0 / 5
要素数 10	5259505445
”0”の出現数	1
度数分布（スコア）	0.1 = 1 / 10
要素数 15	42042592056332e
”0”の出現数	2
度数分布（スコア）	0.133 = 1 / 15
・	・
・	・
・	・
要素数 160	7f98c672a4770736468bd6c145eaf3efe761f849a9895b8997e63a12b 186e75426a9615da603b9af43ea21097239acd939e91af49702d3dc44 79753e3192cee279a32bbd22986afd73b83a34d8f6cf06
”0”の出現数	5
度数分布（スコア）	0.031 = 5 / 160

4.2 本研究でのパターン抽出方法

まず最初に，ファイルのパターン抽出方法を述べる．

（1） パターン抽出対象のファイルの先頭から 4bit を 1byte（以下 4bit を 1byte（1 文字）とする）とした，16 進数で 2640 文字分抽出する．それらの文字の単位および数値は，事前調査により，そのファイルの特徴となるパターンを得るために最適と判断した数値である．

（2） 抽出された，2640 文字を先頭から長さ l_i（$1 \leq i \leq 32$）の 32 個の部分文字列 S_i に分割する．文字列 S_i の長さ l_i は $l_i = i \times 5$ である．l_i は事前調査により，そのファイルの特徴となるパターンを得るために最適な文字数と判断した数値である．

（3） 特定の一文字の度数 f_i を，分割した各文字列 S_i 毎に算出する．特定の一文字には，事前の調査から，文字 0 の度数分布を算出することとする．今後，この度数分布 $\{f_i | 1 \leq i \leq 32\}$ をスコアとし，そのファイルのパターンとして用いる．算出例を**表 1** に示す．

4.3 パターン抽出結果

抽出対象となるファイルは，近年のランサムウェアの攻撃対象となり易いとされるファイルタイプの中から，Microsoft 社の Word ファイル，音声ファイル，Adobe Systems 社の PDF ファイル（以後，doc ファイル，wmv ファイル，pdf ファイル）を選択した．また，ファイルタイプ毎に，暗号化後のファイルも用意する．暗号化アルゴリズムには，AES（Advanced Encryption Standard）に採用された Rijndael，AES 選考の最終 4 候補の 1 つであり，フリーウェア暗号化アルゴリズムでしばしば用いられている Twofish，強度は低いものの，通常の使用には問題は少ないとされている GOST 28147-89（以下 GOST），これらの 3 種類のアルゴリズムを使用する．対象としたファイルは，インターネット上から無作為に取得した，暗号化前のファイル 3 種（doc，pdf，wmv）を 10 個ずつ，それらを 3 種のアルゴリズム（Rijndael，Twofish，GOST）で暗号化したファイルを 10 個ずつ，計 120 個である．この 120 個のファイルを用いて，パターンを抽出する．

図 2 ～ **図 5** は，パターンの典型的な例を示したものである．x 軸は分割した各文字列 S_i の長さ l_i を表しており，y 軸は度数 f_i を表している．図 2 と**図 3** は，異なる暗号化アルゴリズムを用いた doc ファイルと pdf ファイルのパターンを示したものであるが，類似の傾向を示していることがわかる．他の暗号化後ファイルもすべて同様のパターンである．**図 4** と 図 5 は，暗号化前の doc ファイルと pdf ファイルのスコアを示したものであるが，暗号化後ファイルのパターンである，図 2，図 3 とは異なった傾向を示していることがわかる．すべてのパターンの相関係数を算出したところ，暗号化後ファイル同士では，0.921 以上になり，暗号化後ファイルと，暗号化前のファイルとでは，−0.644～0.503 となった．このことから，暗号化されたファイルと，暗号化されていないファイルとでは，本稿で述べた抽出法により抽出されたパターン抽出に，大きく差があることがわかる．よって，暗号化されたファイルには，シグネチャとして利用可能なパターンが存在することがわかる．また，このパターンは，元のファイルタイプと暗号化アルゴリズムに関係なく，一定であることを示すため，すべての暗号化後ファイルのパターンを平均化したものを，リファレンスパターンとし，このリファレンスパターンと，新たに用意した様々な暗号化後ファイル計 150 個との相関係数を算出した結果を**図 6** に示す．x 軸は新たに用意したファイルのナンバーを表しており，y 軸は相関係数を表している．暗号化アルゴリズムには，今までと同じ，Rijndael，

Vol.2012-DPS-150 No.11
Vol.2012-CSEC-56 No.11
2012/2/29

Twofish，GOST を用いている．この図からわかるように，このリファレンスパターンは，どのタイプのどの暗号化アルゴリズムを使ったファイルとでも，高い正の相関関係にあると言える．このことから，このリファレンスパターンを用いることで，暗号化後ファイルを検知することが可能であることがわかる．今後の評価では，このリファレンスパターンを用いて，暗号化後ファイルの検知を行う．

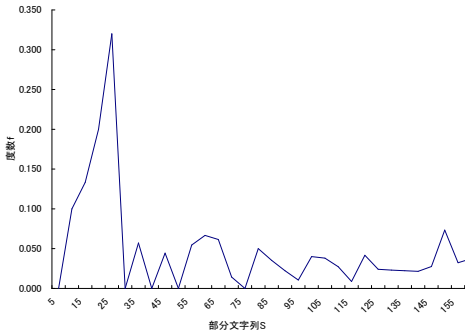

図 2 Rijndael で暗号化された doc ファイルのパターン
Fig. 2 Pattern of the doc file encrypted by Rijndael

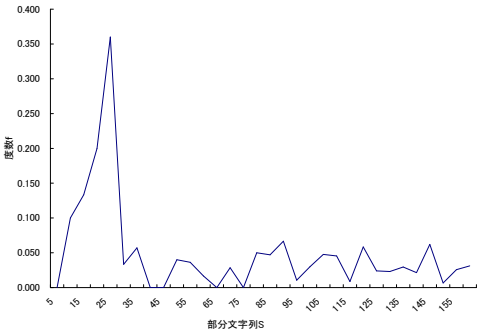

図 3 Twofish で暗号化された pdf ファイルのパターン
Fig. 3 Pattern of the pdf file encrypted by Twofish

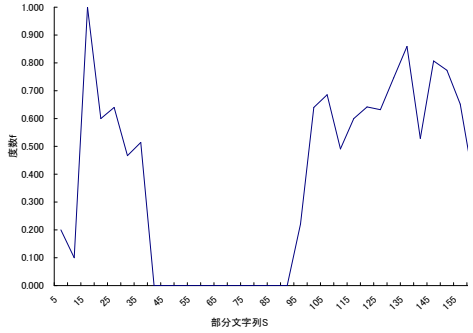

図 4 暗号化されていない doc ファイルのパターン
Fig. 4 Pattern of the doc file unencrypted

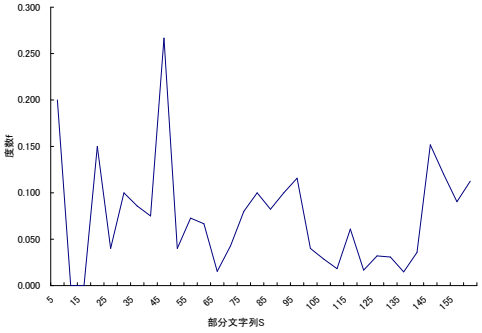

図 5 暗号化されていない pdf ファイルのパターン
Fig. 5 Pattern of the pdf file unencrypted

4.4 評価に用いるプログラムについて

評価では，検知システム，擬似ランサムウェアの 2 つを用いる．以下に，各プログラムの詳細を述べる．

- 検知システム
  前節で述べたリファレンスパターンを用いた，この検知システムには，以下の 3 つの機能がある．
  (1) Microsoft 社の ProcessMonitor によるファイルへのアクセス監視
  ProcessMonitor は，特定のフォルダやファイルに，どのようなプログラムが，いつ，どのような目的で，アクセスしているのかをリアルタイムに監視することができるソフトウェアである．このソフトウェアを用いることで，予めホワイトリストに登録してある正規の暗号化を行うソフトウェアを，監視の時点で除外することができる．
  (2) 生成されたファイルからパターンを抽出照合
  ホワイトリストに登録されていないプログラムにより，何らかのファイルが生成された場合，そのファイルからパターンを抽出する．その後，予め用意されたリファレンスパターンと照合する．
  (3) 暗号化されたファイルと判定された場合にユーザに通知
  相関係数が一定値以上だった場合には，ファイル生成を行ったプログラムの停止とユーザへの通知を行う．
- 擬似ランサムウェア
  ランサムウェアの詳細な侵入，暗号鍵の生成，ファイルの暗号化までの挙動は，ランサムウェアの種類によって様々である．しかし，暗号化されたファイルの生成という挙動は共通しており，この特徴を用いて検知を行うため，ファイルの検索と暗号化のみを実装し，評価で用いる．この擬似ランサムウェアは，特定のフォルダ内の攻撃対象となるファイルをすべて，1 個ずつ暗号化を行う．

5. 検知システムの評価

次に，リファレンスパターンを用いた，検知システムの評価について述べる．

5.1 ランサムウェア検知の流れ

図 7 は，検知の流れを表している．まず，検知システムは，攻撃対象となりうるフォルダを監視する．フォルダ内のファイルへのアクセスは，ProcessMonitor も監視しており，ホワイトリストに予め登録されている正規のソフトウェアによるアクセスであった場合は，検知システムはパターン抽出を行わない．登録されていないソフトウェアが，ファイルにアクセスし，フォルダ内に新たにファイルが生成された場合，検知システムは，生成されたファ

Vol.2012-DPS-150 No.11
Vol.2012-CSEC-56 No.11
2012/2/29

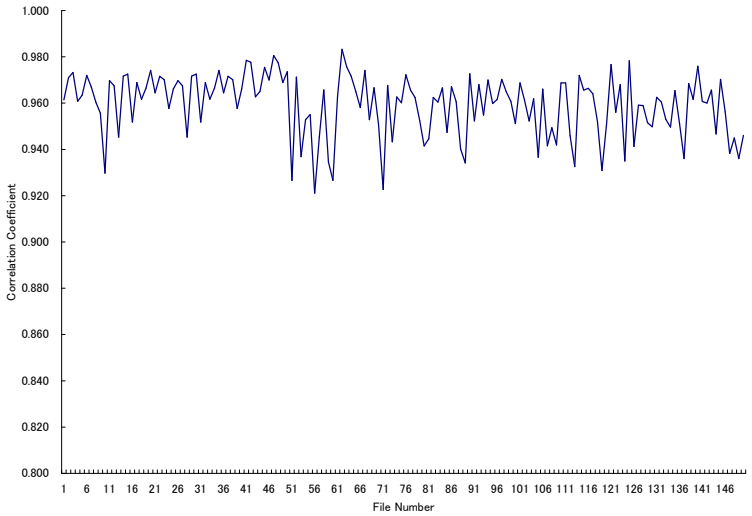

図 6 リファレンスパターンと新たに用意した暗号化ファイルのパターンとの相関係数
Fig. 6 Correlation coefficient of reference pattern and pattern derived by encrypted files newly provided

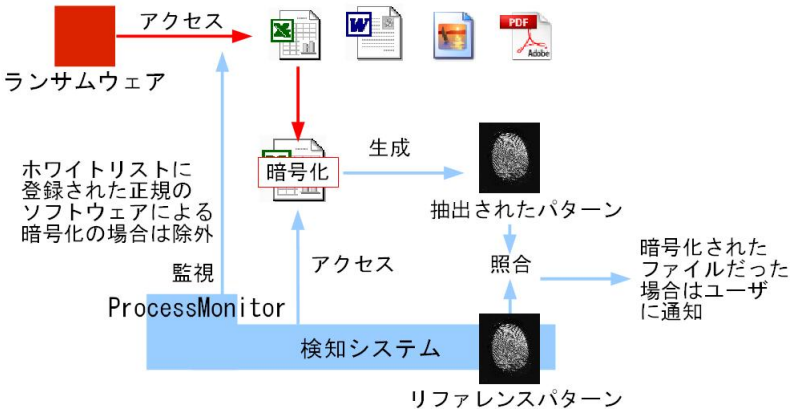

図 7 ランサムウェア検知の流れ
Fig. 7 Flow of detection process of Ransomware

イルにアクセスし，パターンの抽出とリファレンスパターンとの照合を行う．尚，この照合では，4 章のパターン抽出結果の，リファレンスパターンと様々な暗号化後のファイルとの相関係数を求めたもののうち最も相関係数が低かった，0.921 以上だった場合に，そのファイルは暗号化されていると判定を行うように設定されている．そして，その照合で暗号化されたファイルと判定された場合は，暗号化を行ったプログラムの停止と，ユーザへの通知を行う．

5.2 評価環境

次に，評価環境について述べる．評価は，1 つのフォルダ内を仮想環境とし，その中には，予め攻撃対象となり得るファイルが，100 個用意されている．ファイルのタイプは，実際に，近年のランサムウェアの攻撃対象[4] となっている，doc，docm，docx，otm，dotx，jpeg，jpg，mdb，mp3，pdf，png，potm，potx，ppam，ppsm，ppsx，ppt，pptm，pptx，pst，wma，xlam，xls，xlsb，xlsm，xlsx，xltm，xltx を拡張子とするファイルである．ファイルサイズは，小さいサイズから，動画などの大きいサイズまで，様々なファイルが攻撃対象になると考えられるため，30KB〜300MB のサイズのファイルを用意した．暗号化アルゴリズムには，様々な暗号化に対応可能できることと，暗号化との速度の差を検証するため，AES（Rijndael）と，AES よりも高速なトリプル DES を使用し，50 個ずつに分けて暗号化を行う．

また，この検証は，CPU が，Intel（R）Core（TM）i5-2500 Processor（6M Cache, 3.30GHz），OS が，Microsoft Windows XP Home Edition Service Pack 3，メモリ容量 3.6GB の PC で行われている．

5.3 評価方法

仮想環境内で，擬似ランサムウェアによる暗号化（100 個）と，それ以外のファイル生成（100 個）を同じ環境下で，10 回繰り返し，その際の，検知システムの検知率，パターン抽出と照合までの時間，パターン抽出から照合までに，擬似ランサムウェアに，攻撃（暗号化）されるファイル数，検知システムによる負荷を評価する．

5.4 評価結果

評価結果を**表 2** に示している．最初に，抽出から照合までの時間に関しては，4KB，30MB で，差はほとんど見られないため，ファイルサイズに左右されないことがわかる．次に，暗号化速度に関しては，トリプル DES の結果を示している．4KB では，約 0.002 秒で，これが最高であり．最低は，300MB の約 20 秒である．AES では更に多くの暗号化時間を要する．次に，検知率に関しては 100%であり，すべての暗号化ファイルを検知している．誤検

Vol.2012-DPS-150 No.11
Vol.2012-CSEC-56 No.11
2012/2/29

知率に関しても，0%であり，本稿で，使用したファイルタイプでは，リファレンスパターンと高い正の相関係数になるパターンは見られなかった．次に，抽出から照合までに擬似ランサムウェアに攻撃（暗号化）されるファイル数に関しては，10 回の評価で，最大 2 個のファイルが暗号化されことがわかった．この数値は，暗号化速度によって増減する．この検知システムは，仕様上，ファイルの暗号化が終了し，ファイルにアクセス可能になったことを確認してからパターンの抽出を行う．よって，ファイルへのアクセス可否の確認作業を行う際にプログラム内で遅延が発生しており，2 番目，3 番目に攻撃（暗号化）されるファイルのサイズが 4KB 程度の場合は，暗号化速度が極端に速く，パターンの抽出，照合が間に合わないと考えられる．最後に，PC への負荷に関しては，パターンの抽出から照合までの瞬間のみに，CPU 使用率が約 8%上昇した．この上昇に関しては，抽出，照合が極めて短い時間に行われるため，ファイルの生成など，他の原因による CPU 使用率の変動と重なってしまい，正確な数値とは言えない．しかし，上昇するのはわずかな時間であるため，CPU の平均使用率（全稼動時間に対する CPU を実際に使用している時間の割合）で考えれば，CPU 使用率は低いと考えられる．

表 2 評価結果
Table 2 Evaluation results

抽出から照合までの時間: 2KB	約 0.002 秒
抽出から照合までの時間: 30MB	約 0.003 秒
暗号化速度: 4KB	約 0.002 秒
暗号化速度: 30MB	約 20 秒
検知率（%）	100%
誤検知率（%）	0%
抽出から照合までに，暗号化されてしまうファイル数	最大で 2 個
PC への負荷	CPU 使用率が平均 8%上昇

6. おわりに

本稿では，BFA アルゴリズムを参考にした，ファイルのパターン抽出手法により，暗号化されたファイルの検知を行った．評価結果から，ファイルのタイプ，サイズに関係なく，一定の速さで正確な検知を行うことができた．このことから，暗号化されたファイルの生成が行われれば，様々なタイプのマルウェアに対して検知することが可能であることを示した．

今後の課題としては，抽出から照合までに，擬似ランサムウェアに攻撃（暗号化）されるファイル数が，攻撃を受けるファイルのサイズによって増減してしまうことから，サイズの小さいファイルのみが狙われた場合に対応できないため，検知速度と誤検知率のトレードオフに関する検討を行い，パターン抽出手法の調整などを行うことが挙げられる．

参考文献

1) AV-comparatives: Anti-Virus Comparative No.25, Febuary 2010, AV-comparatives, (online), available from ⟨http://www.av-comparatives.org/images/stories/test/ondret/avc_report25.pdf⟩ (accessed 2012-1-30).
2) Luo, X. and Liao, Q. Y.,: Awareness Education as the Key to Ransomware Prevention, Information Systems Security, pp. 195–202 (online), DOI:10.1080/10658980701576412 (2007).
3) Liao, Q. Y. : Ransomware: A Growing Threat to SMEs, Southwest Decision Science Institutes Annual Conference, Houston, (online), (2008).
4) Trend Labs：ランサムウェア（身代金要求型不正プログラム）のアプローチ手法, Trend Labs（オンライン），入手先⟨http://blog.trendmicro.co.jp/archives/2899⟩（参照 2012-1-30）.
5) kaspersky: GpCode-like Ransomware Is Back, kaspersky (online), available from ⟨http://www.securelist.com/en/blog/333/GPCode_like_Ransomware_Is_Back⟩ (accessed 2012-1-30).
6) Sophos: Drive-by Ransomware Attack Demands $120, Sophos (online), available from ⟨http://nakedsecurity.sophos.com/2010/11/26/drive-by-ransamware-attack-demands-120/⟩ (accessed 2012/1/30).
7) kasperskylab: データ返却に 125 ドル要求する GPCode 新亜種を検知, kasperskylab（オンライン），入手先⟨http://www.kaspersky.co.jp/news?id=207582698⟩（参照 2012-1-30）.
8) Symantec: ランサムウェアの猛威, Symantec（オンライン），入手先⟨http://www.symantec.com/connect/blogs-138⟩（参照 2012-1-30）.
9) F-Secure: Ransomware - Buy Back Your Own Files, F-Secure (online), available from ⟨http://www.f-secure.com/weblog/archives/00001850.html⟩ (accessed 2012-1-30).
10) McDaniel, M., Hossain Heydari, M. : Content Based File Type Detection Algorithm, Proceedings of the 36th Annual Hawaii International Conference on System Sciences, (online), (2003).