標的型サイバー攻撃の事例分析と対策レポート

2012 年 1 月

独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

概要

2011 年は、国内の大手重工メーカや衆議院・参議院が情報窃取型の標的型サイバー攻撃を受け、世間の注目を集めた。これらの攻撃は、標的型攻撃メールにより送付されたウイルスがシステム内部に侵入し、スパイ活動をすることで、システム内部の情報が抜き取られてしまうものである。例えれば、現実世界における、産業型スパイ、国家型スパイがインターネット空間で活動を行っていると言える。日本国内は、この脅威が現実のものとなった事件のため報道等で大きく取り上げられたこともあり、新しい攻撃の印象を受けるが、攻撃手法は数年前より問題となっており、海外でも攻撃事例が複数報告されている。
本レポートでは、標的型サイバー攻撃の事例分析、その課題と考察、標的型攻撃メールの分析と対応、標的型サイバー攻撃への技術的対策に加え、対策の新しい試みである情報共有のアプローチについて紹介する。

目次

1. 標的型サイバー攻撃の事例分析と考察

2011 年に多く報道された大手重工メーカが被害を受けた標的型サイバー攻撃の例を取り上げるが、当該事件は単独の問題と捉えるべきではなく、以前から対策が施しにくいと考えられているこのような攻撃に対して、今後の更に深い分析と必要な対策立案における参考の事案として取り上げている。

1.1. 大手重工メーカで発生した標的型攻撃の事例

大手重工メーカで発生した標的型サイバー攻撃に関しては様々な報道があった。これらの報道情報をつなぎ合わせ、情報が足りない個所は他先行事例も踏まえて一部推測を交えて攻撃の流れを再構成し、分析する。

大手重工メーカで発生した標的型サイバー攻撃については、次のような大きく 2 段階における攻撃が行われた。

【事前攻撃活動】

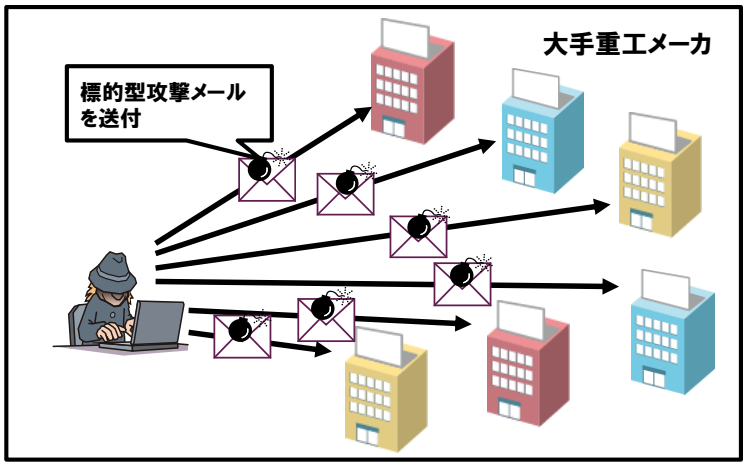
① ３月以降、様々な標的型攻撃メールが各組織で確認されている。その中には、

・社会的な事故を騙ったもの

・信頼できる組織を騙ったもの

・関心の高い話題を騙ったもの

などが挙げられる。今回の事件の攻撃の端緒がどれであったのかは明確になっていないが、巧みな組織への侵入の試みが行われたものと考えられる。



② そうした攻撃の中の一つとして、攻撃者が業界団体から盗んだメールの情報を使い、複数の企業へ送られた標的型攻撃メールが確認されている。業界団体の職員が送付した正規メールの約 10 時間後に、標的型攻撃メールへ悪用されていた。

本件の標的型攻撃メールで使用されたウイルスは、Adobe Reader/Adobe Flash の脆弱性(CVE-2011-0611)を悪用したものであった。これは 2011 年４月に修正プログラムが公開された脆弱性であり、攻撃がそれ以降に行われたものであれば、事前に IPA の公開している「MyJVN バージョンチェッカ」や脆弱性対策情報データベース「JVN iPedia」を活用して対策をしていれば攻撃を回避できた可能性が高い（5.1 節参照）。「MyJVN バージョンチェッカ」はよく使われるソフトウェア製品のバージョンが最新であるかを一括して確認できるツールであり、「JVN iPedia」はソフトウェアの脆弱性対策情報を収集・公開しているデータベースである。

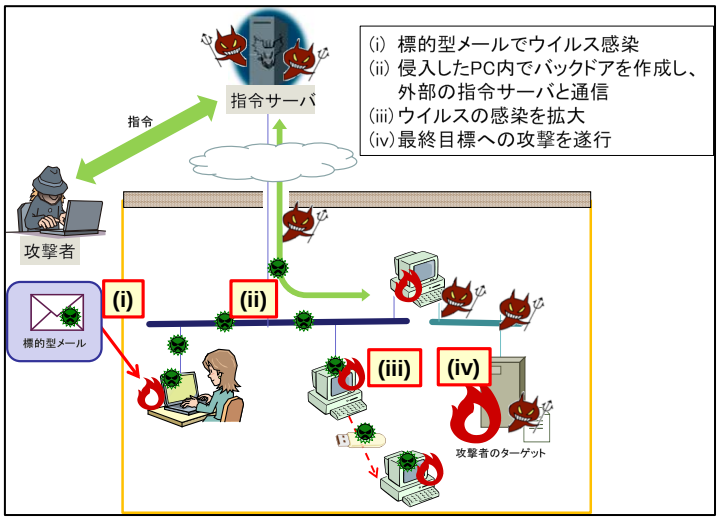
なお、大手重工メーカを狙った標的型攻撃で利用されたウイルスそのものではないが、CVE-2011-0611 を悪用している類似のウイルスの解析を本レポートの５章の付録にて紹介しており、具体的な回避策等も記載している。このウイルスに感染すると、外部通信による新たなウイルスのダウンロードやシステム内情報の外部送信（情報漏洩）の被害が発生することが推測される。

【大手重工メーカへの攻撃】

③　大手重工メーカ内において、標的型攻撃メールに添付されたウイルスファイルを開封してしまい、ウイルスに感染した。これにより、攻撃者が外部からの通信を用いて感染した端末を制御できる状態になったと推測される。

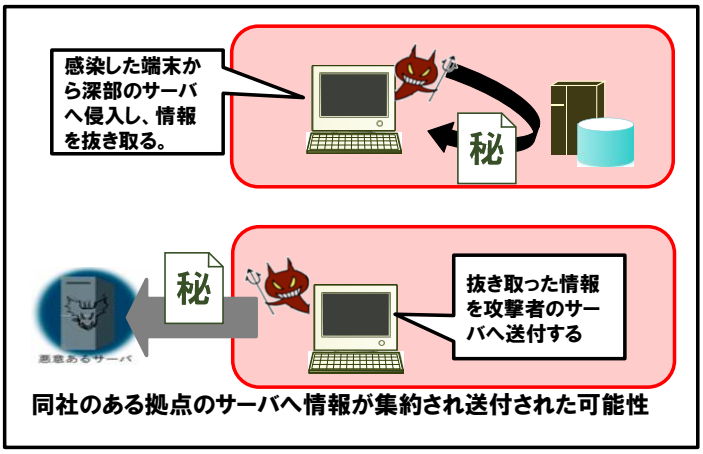
④　攻撃者が制御できるようになった端末は、攻撃者の操る指令サーバーの通信を介して、以下の攻撃が行われたと推測される。

- 新しいウイルスのダウンロード
- 攻撃の見えない化
- 内部拡散
- 情報探査



⑤　多数（報道では 8 種類以上）のウイルスが組織内に持ち込まれ、組織内で感染した PC やサーバーは 11 の事業拠点で、83 台（PC38 台、サーバ 45 台）にのぼった。

⑥　PC やサーバーに感染したウイルスは、PC やサーバー内の情報や周囲の内部ネットワークを介した情報を窃取し、ある拠点の事務所にあるサーバーに集約させた。集約させた理由として考えられるのは、多くの端末から外部の同じ指令サーバーへ集中的にアクセスさせるより、一つの拠点から指令サーバーへアクセスさせるほうが、発覚を遅らせることができる可能性があるという点がある。



⑦　ある拠点の事務所にあるサーバーから、米国にあるサーバーへ、集約させた情報が送信（窃取）された。

⑧　あるサーバーがウイルスによって異常な動作をすることから本件が発覚した。

⑨　システムログの分析などから、大手重工メーカからは防衛の「保護すべき情報」の流出は確認されなかったと発表が行われている。

1.2.　標的型サイバー攻撃の課題と考察

前章では、国内で初めて脅威が現実のものとなった事例を説明したが、これまで報道されている様々な標的型サイバー攻撃に関する事件、事故事例等も踏まえ、いかにこうした新しいタイプの攻撃[1]に備えていくのか、課題を整理する。標的型攻撃メールの組織への送付から、攻撃の進行は概ね以下のように行われる。

【攻撃準備】
・攻撃対象組織や、狙うべき弱い部分の事前調査

[1] 新しいタイプの攻撃は、海外等で一部 APT(Advanced Persistent Threats)とも呼ばれる。

【事前攻撃活動】

①信頼できる組織や個人を騙った巧妙な標的型攻撃メールの送付

②特定の情報窃取を目的とした業種や組織への執拗な攻撃

【本攻撃】

③メールの添付ファイルの開封や URL のクリックによるウイルスの一次感染。ウイルスは普段使っているアプリケーションソフトウェアの脆弱性（ゼロデイを含む）を悪用しているケースが多い。

④感染ウイルスによる外部の攻撃指令サーバーとの通信

⑤ウイルスの増強、変身や、新たな攻撃プログラムのダウンロード

⑥組織システム内での潜伏、拡散、侵攻、探索

⑦機密情報や個人情報等の窃取

⑧外部の攻撃者への窃取情報の送出

この脅威の特徴は以下である。

- 実メールの悪用や信頼できる実組織を騙るなど、攻撃を見分けることが困難である。
- 一般ユーザ環境の脆弱性をついて、初期侵入をしかけてくる
- 侵入（一時感染）後、組織に潜伏し、外部サーバーと連携し、隠密裏に時間をかけて目標となる情報を探索し、情報を窃取する。

これらに対して、最終の重大被害である⑦⑧に至る前のどの時点で攻撃を回避、検知、防御、遮断等ができるかが大きな課題である。可能ならば、攻撃活動の上流で回避できることが望ましいが、巧みなソーシャルエンジニアリングや人間の心理等もついた標的型攻撃メールに対しては、回避できないケースが生じうる。そうしたケースを踏まえ、本攻撃に対して検知、防御、遮断するための技術的な対策も不可欠となる。

以降の章では、２章において①に対する分析と対応を、３章において③～⑧に対する技術的な対策を説明する。１章の事例で挙げたように正しいメールを窃取して悪用された場合などを含め、①～③に対する対応として、類似の攻撃を受けている組織間で攻撃情報を共有して早期の対応、対策をすることが有効な手段と考えられる。４章では、そのアプローチに関して紹介する。

2. 標的型攻撃メールの分析と対応[2]

2.1. 標的型攻撃メールの分析

IPA へ届出のあった標的型攻撃メール群の分析の概要を説明する。

攻撃者はメールを開かせるための騙しのテクニックを駆使している。攻撃者がメールを開かせるために使用する騙しのテクニックは主に次の 3 点が挙げられる。

[2] 『標的型攻撃メールの分析』に関するレポート : http://www.ipa.go.jp/about/technicalwatch/20111003.html

1). メールの件名や本文に業務に関係あるものや関心を抱かせるものを記載する
2). 送信元を実在の組織のメールアドレスに偽装する
3). 添付されたウイルスを正常なファイルに見せかける
この 3 点それぞれの騙しのテクニックについて説明をする。

1).メールの件名や本文に業務に関係あるものや関心を抱かせるものを記載する

図 2. 1 は、実際に標的型攻撃で使用されたメール文面の一例である。「守秘」情報であることや「時事ネタ」等を絡ませている。図 2.1 の件名が「無償化関連記事」のメールは、2010 年当時に送付されたもので、当時高等学校の無償化のニュースが頻繁に報道されていた時期である。今年では、東日本大震災に便乗した標的型メールの事例も報告されている。

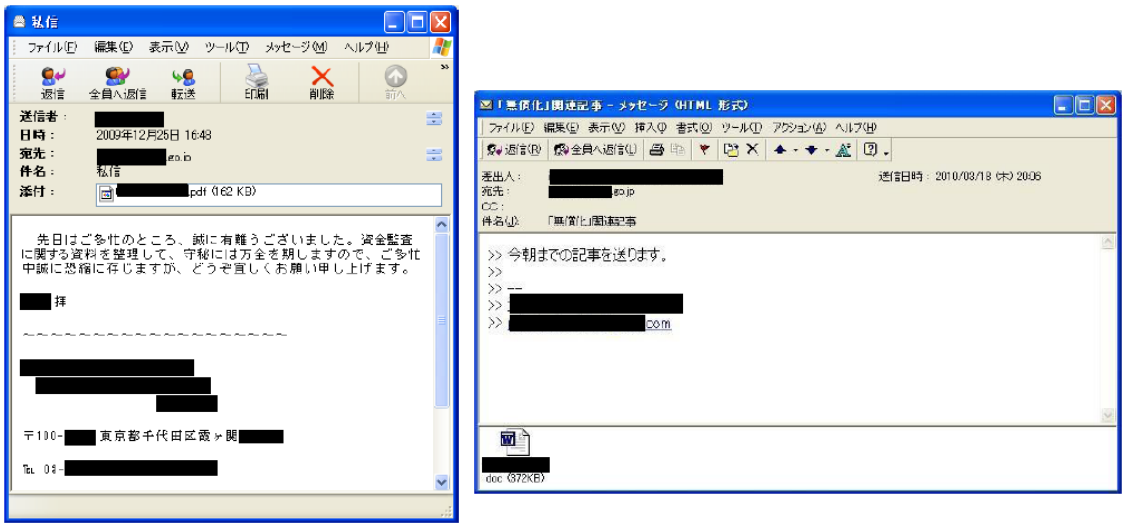


図 2.1：左：官公庁を装った標的型メール 右：件名が「無償化」関連記事の標的型メール

2).送信元を実在の組織のメールアドレスに偽装する

攻撃者はメールの送信元を、宛先に応じた信頼される組織を騙ったメールアドレスに変更して送付する。図 2.2 のグラフは、IPA に届出があった標的型攻撃メールにおける詐称された送信元の主体の属性の割合を示す。

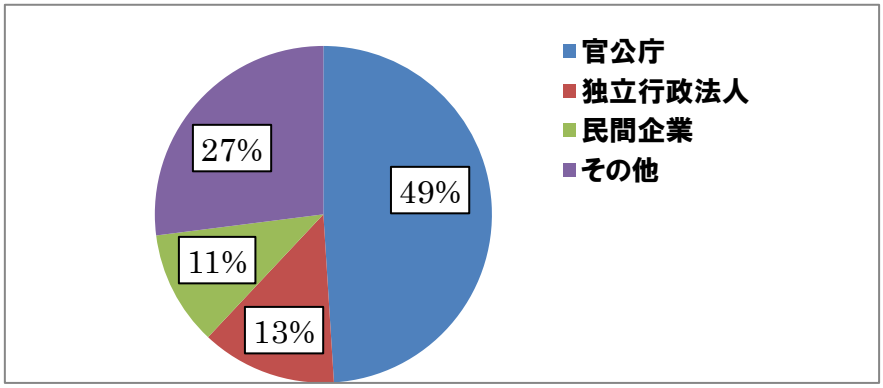


図 2.2：標的型攻撃メールの送信元メールアドレスにおける詐称された送信元

3).添付されたウイルスを正常なファイルに見せかける

拡張子を偽装して正常なファイルに見せるような手口と、ソフトウェアの脆弱性を悪用した手口である。ここでは、後者について触れる。ソフトウェアの脆弱性とは、ソフトウェアに内在する弱点のことである。脆弱性は、本来ソフトウェアが想定していない動作を起こさせる攻撃に使われる。例えば、Microsoft Word や Adobe Reader のようなソフトウェアに脆弱性があった場合、本来ソフトウェアが持ち合わせていない攻撃者の悪意ある任意のコードを実行されてしまう場合がある。図 2.3 のグラフは、標的型攻撃メールで悪用された脆弱性のあったソフトウェアの割合を示している。

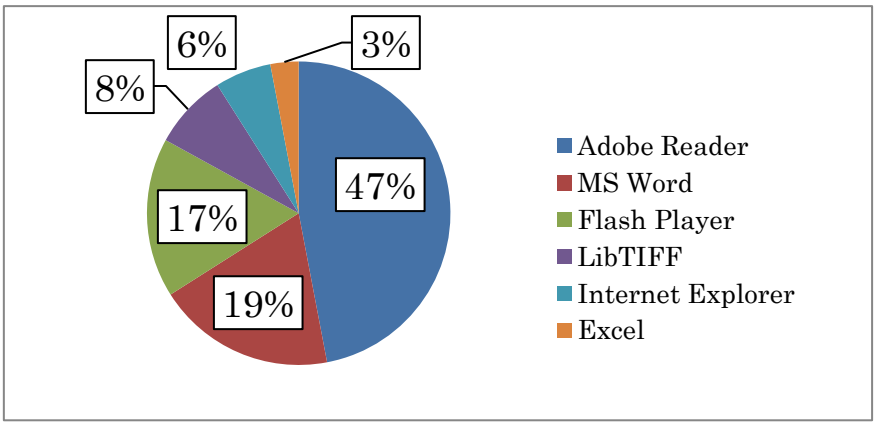


図 2.3：標的型攻撃メールで悪用された脆弱性のあったソフトウェア

2.2. 標的型攻撃への対応

以下、標的型攻撃メールにおける基本的な対応方法について説明する。

1). 標的型攻撃メールの見分け方

標的型攻撃メールの全てに対してではないが、下記のことに注意をすることで標的型メールか否かについて見分けることが可能になる。

- 普段メールをやりとりしていない人から、添付ファイル付きのメールが届いた
- そのメールを何故自分に送ってきたのか心当たりがない

- ファイル拡張子が exe のような実行形式(圧縮ファイルの場合は、その中身)
- ファイル名が文字化けしている

2). 標的型攻撃メールが届いた場合の対応

上記方法等で、標的型攻撃メールを実際に受信したことが分かった場合、次のような対応を取ることが好ましい。

- 電話番号案内(104)やウェブから、メール送信者の連絡先を調べ、そのメールを送ったか直接確認する。
- メール送信者がなりすましと判明した場合、組織内の情報システム部門などセキュリティ対策部門に報告し、指示を仰ぐ。
- 組織内のセキュリティ対策部門は、当該メールにウイルス感染の仕掛けがあるか調べるとともに、同様の攻撃メールが他の人に届いていないか調査し、注意喚起する。

3). 関係機関への届出

- 同じ攻撃者から他の組織に対して同様の攻撃メールが届いている可能性があるので、IPA の相談窓口[3]に連絡する。

3. 標的型サイバー攻撃に対する技術的対策

本章では商用の製品やサービス等で実現できる対策に加え、IPA で公開している対策についても紹介する。

3.1. トータルセキュリティ

標的型サイバー攻撃において、対策を施さなければならない対象は、個々の PC だけではなく、組織の重要サーバーを含んだネットワークシステム全体の対策が必要となる。組織においては、それぞれの組織の状況に応じて、必要な対策と組織でできる対策とを検討し、選択して採用する必要がある。

1). システムへの入口での防御

これらの対策の目的は、主に外部から直接内部のシステムを攻撃されないことを目的としている対策である。内部へアクセスすることが必要なものとそうではないものを分別するために施す対策である。

- ファイアウォール
- 最新のウイルス対策ソフト（ネットワーク、サーバー、クライアント）
- 侵入検知システム／防止システム

[3] 情報セキュリティ安心相談窓口：http://www.ipa.go.jp/security/anshin/

2). **脆弱性対策**

これらの対策の目的は、1) では防げなかった場合や、外部に曝されているシステムへの攻撃から守るための対策である。クライアントやサーバーの既知の脆弱性を悪用した攻撃から守るものである。特にクライアントで用いるソフトウェアは最新のバージョンを使うこと、脆弱性の修正プログラムは公開から遅延なく適用することが、標的型攻撃への事前対策として有効である。

主な対策項目を以下に示す。

- OS やサーバーソフトウェアの定期的な脆弱性診断
- OS やサーバーソフトウェアに関する脆弱性情報の、時期を逸しない収集と修正プログラムの適用
- ウェブアプリケーションへの脆弱性の作り込みの回避
- ウェブアプリケーションファイアウォール（WAF）

これらを実現するための環境として、IPA では、「MyJVN バージョンチェッカ」、脆弱性対策データベース「JVN iPedia」を公開している。

3). **標的型攻撃ルートでの対策**

標的型攻撃のルートとなるスパムメール等の排除、不要あるいは危険なウェブサイトへのアクセスの抑止、外部メディアによるウイルス感染や情報漏えいの防止を実施するものである。これらの対策はリスクを低減するには有効であるが、業務の性質やフロー上、採用できない場合もあり、慎重に導入を検討すべき対策である。

また、メールに対しては SPF (Sender Policy Framework) や DKIM (DomainKeys Identified Mail)等の送信側の身元保証をするためのドメイン認証等の技術が挙げられるが、送信側が対応している必要があり、これらの技術の導入を社会全体で対応していくことで、標的型攻撃メールの防止にも有効になる。

主な対策項目を以下に示す。

- スパムフィルタ
- URL フィルタ
- 外部メディア利用規則、強制利用抑止

4). **ウイルス活動の阻害および抑止 (出口対策)**

これらの対策の目的は、1) ～ 3)の対策を乗り越えてウイルス等が侵入してしまった場合でも、組織への実害を最小限に留めるための対策である。

主な対策項目を以下に示す。

- 端末間、他部署間のネットワーク通信の制限（ウイルスの組織内蔓延抑止）
- 組織の端末からの外部通信はプロキシを経由させる等の経路制御
- 組織内ネットワーク量の監視（異常さを早期に検知しウイルスの蔓延を早期に発見）
- 知財等のある重要なサーバーはインターネットから隔離

5). **アクセス制御**

ユーザ認証を実施する対策の目的は、主に元々重要サーバー等へのアクセスを最低限の従業員に絞るための対策である。このことは、たとえある端末がウイルスに感染したとしても重要サーバーへアクセス権がなければ、その端末から情報を窃取させることはないことになる。また、アクセスするプログラムの特定は、ウイルスからのアクセスを防ぐための対策である。

主な対策項目を以下に示す。

- ユーザ認証
- アクセスするプログラムの特定（ホワイトリスト化）

6). **情報の暗号化**

これらの対策は、たとえ情報を窃取されたとしても内容を解読させないことを目的とした対策である。

主な対策項目を以下に示す。

- 通信路の暗号化（Virtual Private Network などの利用）
- ファイルの暗号化
- 暗号鍵管理

7). **システム監視、ログ分析**

これらの対策は、ログを分析し、自組織への攻撃やウイルス感染や不正アクセスを早期に検知することが目的である。また、どのシステムが攻撃されているかどうかをログから分析し、被害状況等を把握するためにも重要である。

主な対策項目を以下に示す。

- ネットワークログ取得・分析
- サーバログ取得・分析
- アクセスログの監査（DB 監査ツールなど含む）

8). **管理統制およびコンテンジェンシープラン (事前準備・事後対応)**

これらの目的は、組織全体として、どのようなセキュリティポリシーの下に、どのような体制で運用管理するかを設定しておくことである。また、仮に攻撃が成功してしまった場合、どのような体制を組み、どのような行動を取るかということを定めておくものである。

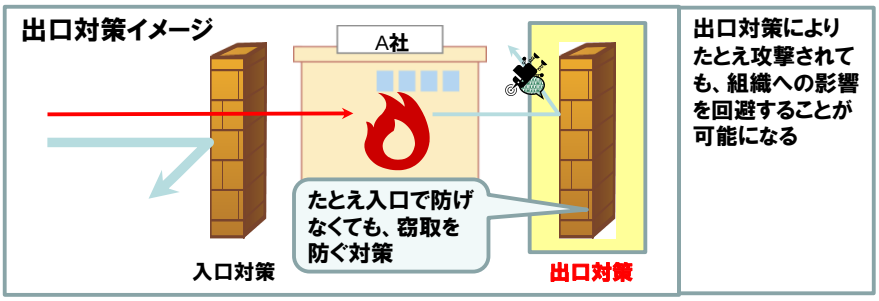
主な対策項目を以下に示す。

- セキュリティポリシーの徹底
- 海外を含むグループ会社間でのセキュリティガバナンス
- 危機対応体制の整備

これらの対策の中でも、標的型サイバー攻撃のような巧妙な攻撃においては、他の入口での対策をすり抜けてしまう可能性があるため、特にポイントとなる４）の出口対策を次節で取り上げる。

3.2. 出口対策[4]

多くの組織では、対策の幾つかの対応を既にしているだろう。その対策を施していることで数多くの攻撃から守ることができている。しかし、標的型攻撃は巧妙に作成されており、ウイルスが入り込んでしまうことを完全に防ぎきれるものではないのが現状である。そのため、たとえウイルス等が侵入してしまったとしても組織への実害を被らないことが重要である。



出口対策の具体的な方法は次のとおりである。

（水色）はバックドア通信を止める対策
（緑色）はシステム内拡散等を止める対策

対策	実装手法
① サービス通信経路設計	1.ファイアウォールの外向き通信の遮断ルール設定 2.ファイアウォールの遮断ログ監視
② ブラウザ通信パターンを模倣するhttp通信検知機能の設計	1.httpメソッド利用バックドア通信の遮断
③ RATの内部proxy通信（CONNECT接続）の検知遮断設計	1.RATのCONNECT確立通信の特徴を利用した、内部proxyログでの監視
④ 最重要部のインターネット直接接続の分離設計	最重要部がインターネットへ直接接続しないようにVLAN等で設計
⑤ 重要攻撃目標サーバの防護	1.ADを管理する管理セグメントを防護する。 2.利用者から見えるADのサービスに対するパッチ当て。
⑥ SW等でのVLANネットワーク分離設計	利用者セグメントと管理セグメントを分離設計する等
⑦ 容量負荷監視による感染活動の検出	スイッチ等の負荷やログ容量等における異常検知を行い、セキュリティ部門と連携する
⑧ P2P到達範囲の限定設計	③④の対策に加え、不要なRPC通信の排除を目的としたネットワーク設計

これら出口対策の詳細については、「『新しいタイプの攻撃』の対策に向けた設計・運用ガイド」で紹介をしている。詳細については同書を参考にして欲しい。
http://www.ipa.go.jp/security/vuln/newattack.html

[4] 「『新しいタイプの攻撃』の対策に向けた設計・運用ガイド」：
http://www.ipa.go.jp/security/vuln/newattack.html

4. 標的型サイバー攻撃に対する IPA の取組み

4.1. IPA の公開する対策情報とツールの紹介

近年、標的型サイバー攻撃が大きな脅威になってきていることに対応するため、IPA ではこの一年だけでも、表４．１に示すように、「事前対応」から、「早期警戒」、「システム対策」、「事案発生対応」に至るトータルな対策を策定、提案してきている。

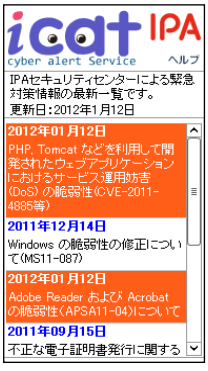
表 4.1：標的型サイバー攻撃に対するトータルな対応活動

フェーズ	項目	IPAの対応、施策、トピックス
事前対応	注意喚起	・'11.11.25：サイバーセキュリティ注意喚起サービス「icat」の公開 http://www.ipa.go.jp/about/press/20111125_2.html
	バージョンチェック	・'11.11.29： MyJVNバージョンチェッカ 機能強化 http://www.ipa.go.jp/about/press/20111129.html
	脆弱性対応	・JVNiPedia脆弱性対策DB（12,000件突破）：'12.01現在
	ユーザリテラシー向上	・'11.10.3：「テクニカルレポート『標的型攻撃メールの分析』 http://www.ipa.go.jp/about/technicalwatch/20111003.html
早期警戒	サイバー情報共有パートナーシップ（J-CSIP）	・'11.10.25 発足 ＜3月の本格運用に向け、鋭意推進中＞
システム対策	出口対策 標的型統合対策	・'11.8.3：「『新しいタイプの攻撃』の対策に向けた設計・運用ガイド」を公開、'11.11.30：改訂第二版 http://www.ipa.go.jp/about/press/20111130.html ・'11.10.18：プレス： 脅威を増す標的型のサイバー攻撃に関する注意喚起 ～セキュリティ対応状況の確認と対策の徹底を～ ＜チェックリスト＞ http://www.ipa.go.jp/about/press/20111018.html
事案発生対応	安心相談窓口 届出制度	・'11.10.25：「標的型サイバー攻撃の特別相談窓口」の設置 http://www.ipa.go.jp/about/press/20111025.html

「事前対応」では、２章で述べた標的型攻撃メールへの対応を、「システム対策」では、３章で述べた標的型サイバー攻撃を受けた際の防御のための技術的対策と IPA の提案する出口対策について挙げている。

３章で説明した対策を実現する上で、多くは商用の製品やサービス等で実現されるが、以下では、安全なネット社会を実現する重要な仕掛けとして、IPA で公開しているこの対策に関連する主なツールやサービスについて、紹介する。

(1) サイバーセキュリティ注意喚起サービス「icat」[5]



IPA では、これまで国内ベンダーや海外のセキュリティ機関のセキュリティに関する情報を日々収集し、影響度の大きなセキュリティ上の問題については、「緊急対策情報」または「注意喚起」としてホームページ上で広く一般に周知と対策を促してきました。サイバーセキュリティ注意喚起サービス icat（アイキャット）は、問題の周知と一層の対策促進を目的に、IPA が公開した注意喚起情報をリアルタイムに配信するもので、本ツールを企業のポータルサイトや団体の会員向けウェブサイトに設置することで、IPA が公開した最新の「緊急対策情報」の一覧を自動的に取得・表示することができます。

[5] http://www.ipa.go.jp/security/vuln/icat.html

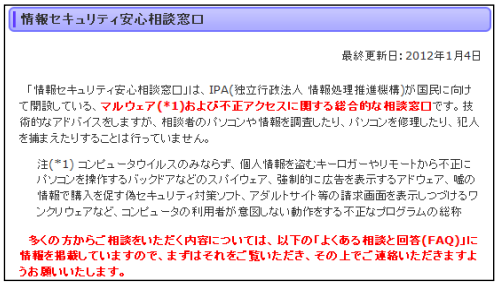
(2) MyJVN バージョンチェッカ[6]

「MyJVN バージョンチェッカ」は、PC やサーバーにインストールされているソフトウェアが最新のバージョンであるかを簡単な操作で確認することができるツールです。本ツールは、2009 年 11 月から公開しており、脆弱性対策を推進するツールとして広く利用されています。最新のバージョンを使うことで、既知の脆弱性に対する攻撃を回避することができます。

(3) 脆弱性対策データベース JVNiPedia[7]

脆弱性対策情報データベース「JVN iPedia」は、日本国内で使用されているソフトウェアの脆弱性対策情報を収集・公開することにより、脆弱性関連情報を容易に利用可能とすることを目指しています。1）国内のソフトウェア開発者が公開した脆弱性対策情報、2）脆弱性対策情報ポータルサイト JVN[8]で公表した脆弱性対策情報、3）米国国立標準技術研究所 NIST[9]の脆弱性データベース「NVD[10]」が公開した脆弱性対策情報の中から情報を収集、翻訳し、2007 年 4 月 25 日から公開しており、11,000 件を超える情報が登録されています。また、2011 年第 4 四半期より、NVD から日々公開される脆弱性対策情報の全てを 1 両日中に翻訳・公開しており、 対象製品のスコープや公開情報の即時性を高めたことにより、システム運用者にとって、幅広くかつ迅速に情報を取得することが可能となっています。

(4) 事案発生対応：安心相談窓口、届出制度[11]



「情報セキュリティ安心相談窓口」は、IPA が国民に向けて開設している、マルウェアおよび不正アクセスに関する総合的な技術上の相談窓口です。IPA は、1990 年 4 月に通商産業省が告示した「コンピュータウイルス対策基準」に基づき、国内のウイルス被害届を受付、国内のウイルス被害状況を発表するとともに、ウイルス対策の注意喚起や啓発活動を行なっています。また、1996 年 8 月に通商産業省が告示した「コンピュータ不正アクセス対策基準」に基づき、国内の不正アクセス被害届を受付、国内の不正アクセス被害状況を発表するとともに、注意喚起や啓発活動を行なっています。

---

6 http://jvndb.jvn.jp/apis/myjvn/
7 http://jvndb.jvn.jp/
8 http://jvn.jp/
9 http://www.nist.gov/
10 http://nvd.nist.gov/
11 http://www.ipa.go.jp/security/vuln/report/

4.2. 情報共有のアプローチ （J-CSIP の活動）[12]

情報窃取等を目的とした標的型サイバー攻撃に対して、メールが着信して組織内での危害や被害におよぶ前に、そのことをいち早く組織が検知して除去や対策をすることができれば、有効な手段の一つとなる。１章の事故事例で挙げたように、業界団体を騙って標的型攻撃メールを送ってきている例も示すように、ある特定分野の機密情報や個人情報等を狙ってくるケースも想定され、同業の業界全体で、ある組織が検知した標的型攻撃メールの情報を共有することができれば、被害の回避や早期の対応を打てることが期待できる。そうした業界全体での防御、ひいては国家としての防御の施策の試みが、「早期警戒」に挙げているサイバー情報共有イニシアティブ（J-CSIP）である。この情報共有の重要性は各国でもしきりに議論されている。[13]

J-CSIP の活動は、2011 年 10 月 25 日に経済産業省の主導の下に発足し、IPA が情報ハブとなって、まず重工業９社に対して、攻撃情報の共有を実現する試みである。その目的は、

・情報共有による攻撃の早期検知と回避策の実施
・標的型サイバー攻撃の実体調査と共有情報による効果的な対策の推進

である。そのスキームの概要を、標的型サイバー攻撃を例として図 4.1 を用いて説明する。

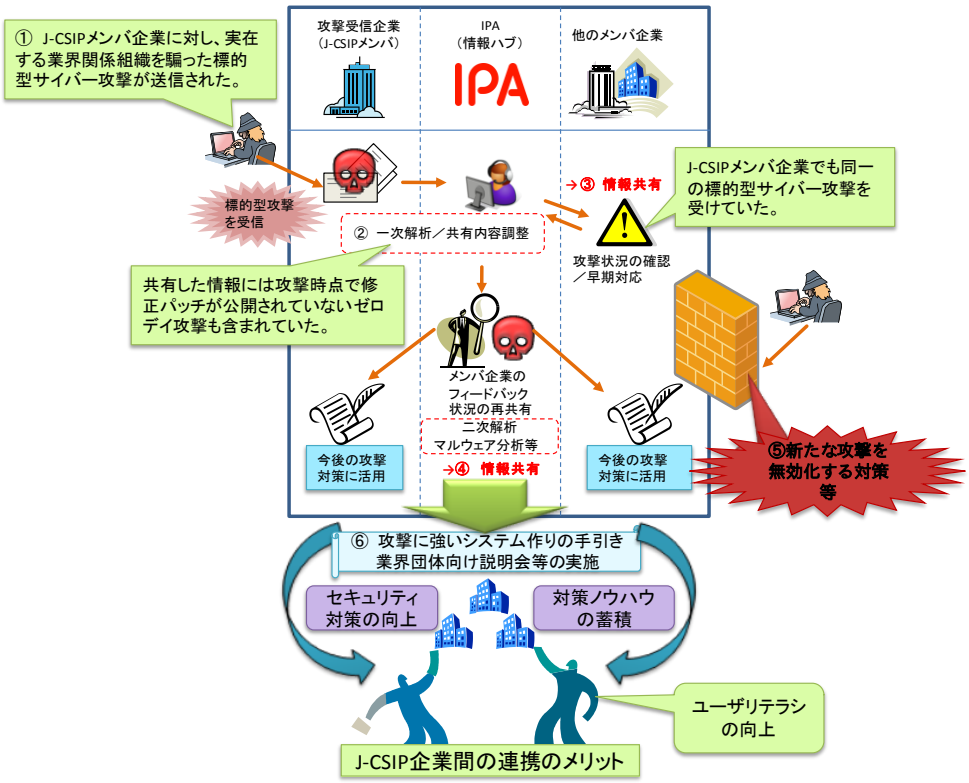


図 4.1：J-CSIP での標的型サイバー攻撃情報共有の取組みのスキーム

[12] サイバー情報共有イニシアティブ（J-CSIP）：http://www.ipa.go.jp/security/J-CSIP/
[13] National Public Private Partnerships：
http://www.enisa.europa.eu/act/res/other-areas/national-public-private-partnerships-ppps/

①メンバ企業の一社がサイバー攻撃の受信を検知
②攻撃受信企業からの情報提供を IPA が受け、その企業と協力して一次解析とメンバ間での共有情報の調整の実施
③メンバ企業への情報共有の実施
　共有情報を元に、メンバ企業は自組織への同様の攻撃の検知、メール削除や組織内周知等の早期対応
④IPA にて、攻撃、マルウェアの解析を実施し、対策情報を抽出しメンバ間での情報共有の実施
⑤メンバ企業のシステムにて、マルウェアの活動による新たな攻撃を無効化する対策等を実施
⑥サイバー攻撃情報群を分析し、攻撃に強いシステム作りのノウハウを策定

　この情報共有にあたっては、以下の要件が満たされることが重要な課題である。
(1)情報の匿名化：　共有される情報は、その標的型攻撃メールが着信した情報提供元企業（グループ企業含む）の固有情報が推定できない情報とする。
(2)情報の有効性：　共有される情報には、メンバ企業がその標的型攻撃メールと類似の攻撃の有無等を調査・検知するにあたり必要となる情報を最大限含むものとする。
(3)共有の即時性：　攻撃の早期検知や対応、次いで対策の実施等にタイムリーに活用できる情報を、段階を追って可能な限り迅速な情報共有を実現する。
　対象なる情報は、メールヘッダを構成する情報群、メール本文、使用言語・文字コード、添付ファイル、マルウェアの解析情報など、30 近い項目から構成されることになる。

　この J-CSIP の活動では、これらの課題を克服するため、引き続き有効性の検証を実施し、将来的には、共有メンバの拡大や情報共有する新たな集合体（業種、事業体など）への展開を検討していく予定である。

5. 付録 CVE-2011-0611 を悪用したウイルスの概要「PDF-Exploit-m」の解析レポート(対策情報)

5.1. PDF-Exploit-m の流行情報

2011 年 9 月に、日本の大手重工メーカが標的型のサイバー攻撃被害に遭い、複数のサーバーやパソコンが本ウイルスに感染する被害が発生したと報じられた(被害に遭ったのは同年 8 月)。今回解析する PDF-Exploit-m は、そのウイルスの亜種と思われる PDF ファイルである。

この標的型攻撃は、他の国内メーカに対しても同様の攻撃が仕掛けられたことが判明、また日本だけでなく、イスラエル、インド、米国の防衛産業の企業に対しても同種の標的型攻撃が行われていることが確認されている。

5.2. ウイルス概要

(1) 動作概要

PDF-Exploit-m は PDF タイプのウイルスであり、メールに添付された PDF-Exploit-m をユーザが開くことで、もしくは PDF-Exploit-m を公開した URL リンクがメール本文に記載してあり、それをユーザがクリックすることで感染すると推測される。

PDF-Exploit-m は、内部に難読化を施した不正な JavaScript や Flash ファイルを組込み、複数の脆弱性 CVE-2009-0927、CVE-2007-5659(CVE-2008-0655)、CVE-2011-0611 を悪用して、ユーザの環境に沿った感染を実現している。また、感染後は、それぞれ機能の異なる 2 つの dll ファイル（AdobeARM.dll、googlesetup.dll）と、googleservice.exe という実行ファイルを作成し、エクスプローラ(explorer.exe)および Internet Explorer(iexplorer.exe)に注入する。作成された googleservice.exe が、ボットであり、インターネット上の特定のサーバーの指令を受信する。

(2) 想定される被害(PC 内被害、漏洩情報等)

PDF-Exploit-m 自身が、直接 PC に被害を与える機能を有していない。しかしながら、PDF-Exploit-m により感染するボットは、外部から PC を操作され、ファイルのダウンロードおよび実行機能を有しているため、次の被害が想定される。

- 端末内の情報を外部に送信される（情報漏洩）。
- ボットがダウンロードした別のウイルスに感染する。それにより、PC 内被害や情報漏洩等の被害が想定される。

(3)　事前の回避策

事前の回避策は次のような方法が挙げられる。

- PDF-Exploit-m は PDF 内に組込まれた JavaScript を利用して感染を実現する。したがって、PDF-Exploit-m を開くアプリケーション（Adobe Reader）の JavaScript 機能を OFF(下記の図参照)にすることで、ボットの感染を防ぐことが可能である。
- 常に Adobe Reader 等のソフトウェアを最新にする。
- メールの添付ファイルをむやみに開かない。
- メール本文の URL をむやみに開かない。

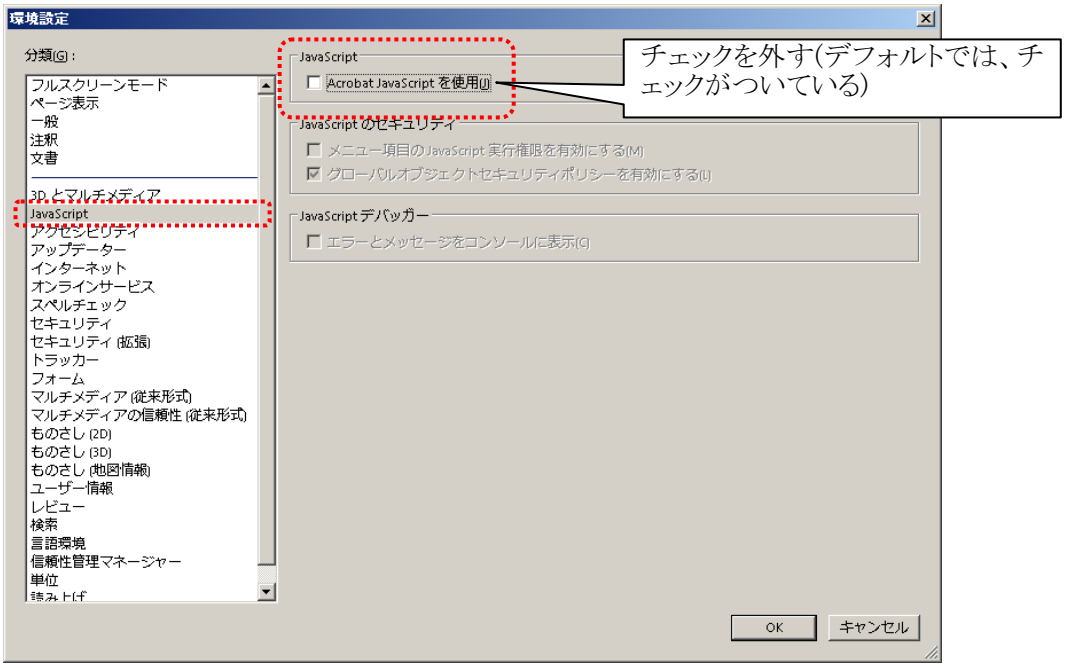


図 5.1：Adobe Reader の[編集]集 o 環境設定]画面

(4)　簡易的な感染判断方法

PDF-Exploit-m は次の方法で確認できる。

（1） ウィンドウが存在しないのに InternetExplorer のプロセス(iexplorer.exe)が存在する。

（2） 環境変数%CommonAppData%、または環境変数%AppData%の示すフォルダに、googlesetup.dll が存在する。

（3） 環境変数%CommonStartup%、または環境変数%Startup%の示すフォルダに、googleservice.exe が存在する。

(5)　感染した場合の復旧策

PDF-Exploit-m は次に示すファイルの削除を行う事で、システムを復旧する事が出来る。なお、PDF-Exploit-m 本体である PDF ファイルは、実行時に害の無い PDF ファイルに書き換えられているため、削除の必要はない。

（1） 環境変数%CommonAppData%、または環境変数%AppData%の示すフォルダに存在する”googlesetup.dll”を削除する。
（2） 環境変数%CommonStartup%、または環境変数%Startup%の示すフォルダに存在する”googleservice.exe”を削除する。
（3） 環境変数%temp%の示すフォルダに存在する、AdobeARM.dll および googlesetup.dll を削除する。

今回解析を行ったウイルスの概要一覧を表 5-1 に示す。

表 5-1：ウイルス概要一覧

NO.2011-03	
ウイルス名称	PDF-Exploit-m
ウイルス俗称 （2011 年 8 月 16 日時点）	トレンドマイクロ社　TROJ_PIDIEF.EED マカフィー社　Heuristic.BehavesLike.Exploit.PDF.CodeExec.FFLG シマンテック社　Trojan.Gen.2 その他　Exploit.JS.Pdfka.epp（カスペルスキー社）
起源	2011 年 9 月 19 日　(トレンドマイクロ社)
発見日	2011 年 9 月 30 日
動作環境	【Application】 ・ Adobe Reader and Adobe Acrobat 9 ～ 9.1 より前のバージョン ・ Adobe Reader and Adobe Acrobat 8 ～ 8.1.3 より前のバージョン ・ Adobe Reader and Adobe Acrobat 7 ～ 7.1.1 より前のバージョン ・ Adobe Reader and Acrobat 8.1.1 より前のバージョン ・ Adobe Reader and Acrobat before 8.1.2 より前のバージョン ・ Adobe Flash Player before 10.2.154.27 on Windows ・ Authplay.dll (aka AuthPlayLib.bundle)を利用する Adobe Reader 9.x ～ 9.4.4 より前のバージョンと 10.x t から 10.0.1
感染条件	上記動作環境に一致した環境下で当該 PDF タイプウイルスを実行することで感染する。当該ウイルスは複数の脆弱性を悪用する。脆弱性番号（CVE）と、その脆弱性が存在するアプリケーションおよびバージョンを以下に列挙する。 ■ CVE-2009-0927 ・ Adobe Reader and Adobe Acrobat 9 ～ 9.1 より前の

<table>
<tr><td></td><td>バージョン
・ Adobe Reader and Adobe Acrobat 8 ～ 8.1.3 より前のバージョン
・ Adobe Reader and Adobe Acrobat 7 ～ 7.1.1 より前のバージョン
■ CVE-2007-5659（CVE-2008-0655）
・ Adobe Reader and Acrobat before 8.1.2 より前のバージョン
■ CVE-2011-0611
・ Adobe Flash Player before 10.2.154.27 on Windows
・ Authplay.dll (aka AuthPlayLib.bundle)を利用する Adobe Reader 9.x ～ 9.4.4 より前のバージョンと 10.x t から 10.0.1</td></tr>
<tr><td>感染経路</td><td>メールに添付された PDF-Exploit-m をユーザが実行することで、もしくはメールに記載された PDF-Exploit-m をアップロードした URL をユーザがクリックすることで感染したと推定される。</td></tr>
<tr><td>タイプ</td><td>標的型攻撃＋ボット</td></tr>
<tr><td>ウイルス概要</td><td>PDF-Exploit-m は標的型攻撃を目的とした PDF タイプのウイルスである。前述の感染条件に合った PC で PDF-Exploit-m を開くと、ボット(※1)に感染する。ボットに感染後は、インターネットを通じて指示を受け、他のウイルスをダウンロードするなどの感染活動を行う可能性がある。

※1：ボットについては下記 URL を参照のこと
http://www.ipa.go.jp/security/antivirus/bot.html</td></tr>
<tr><td>ウイルス評価指標

※次頁に評価指標の説明を記す</td><td><table>
<tr><td>(1) 感染力</td><td>■■□</td></tr>
<tr><td>(2) 脆弱性悪用力</td><td>■■□</td></tr>
<tr><td>(3) 自己隠ぺい力</td><td>■■□</td></tr>
<tr><td>(4) 破壊力</td><td>■□□</td></tr>
<tr><td>(5) 影響力</td><td>■■■</td></tr>
<tr><td>(6) 感染拡大力</td><td>■□□</td></tr>
</table></td></tr>
</table>

※ウイルス評価指標について

（1） 感染力（感染のしやすさ）

■□□ … 実行形式ファイルで、開かなければ感染しないタイプ。
■■□ … ファイルを偽装することでファイルを開かせるタイプ。
■■■ … ファイルを開く行為をしなくても感染するタイプ。

（2） 脆弱性悪用力（感染のしやすさ）

■□□ … 脆弱性を悪用しない。
■■□ … 修正プログラムが公開されている脆弱性を悪用する。
■■■ … 修正プログラムが未公開の脆弱性を悪用する。

（3） 自己隠ぺい力（発見のしにくさ）

■□□ … 何らかの感染を疑うような症状がある。
■■□ … 表立った症状は無いがユーティリティの操作等で感染を確認できる。
■■■ … ルートキット等の技術が使われており、感染の確認が困難である。

（4） 破壊力（修復の難しさ）

■□□ … PC 等の通常利用にほとんど支障が無い。
■■□ … 実害はあるが、復旧は困難ではない。
■■■ … システムファイルや PC 等内のデータファイルが破壊され、復旧が困難である。

（5） 影響力（外部への影響の大きさ）

■□□ … 感染した PC 等から外部に対して何もしない。
■■□ … ネットワーク上の他の PC 等に対して DoS 攻撃や spam メール発信等を行う。
■■■ … 感染した PC 等から収集した情報を外部に送信または公開する。

（6） 感染拡大力（外部への影響の大きさ）

■□□ … 感染機能なし。
■■□ … LAN 内の他の PC 等に感染拡大する。
■■■ … インターネット上の他の PC 等に感染拡大する。

※ さらに詳しい説明は、下記ファイルを参照。
http://www.ipa.go.jp/security/virus/report/virus_evaluation_index.pdf