コンピューターウィルス生態学序説

フェリス女学院大学文学部コミュニケーション学科
高 田 明 典

1. はじめに

コンピューターウィルス[1)]をどう考えるかということは、情報の電子化が進んだ現代の状況においては、きわめて重要な懸案事項であると言える。もちろんそれらは「善悪」の基準からすれば、「悪」に分類されるものである。しかしながらそれらの「悪」がこれほどまでに我々の社会に浸透し、脅威を与えているという現実を、深く認識しなくてはならない。

コンピューターウィルスの存在は、たとえそれに感染・発症しなくても甚大な損失をもたらしている。たとえば、ウィルス防護ソフトを購入する場合には経済的負担が発生する。

また、ウィルス防護ソフトは常駐監視型のソフトウェアである場合が多く、「コンピューター資源」をかなり消費する。つまり、「ウィルス防護ソフトを機能させる」ための「マシン性能」が必要となる。常駐型のウィルス防護ソフトを組み込んで使用しているマシンにおいて、「組み込んでいない」状態と同程度のパフォーマンスを得るためには、かなりの「CPU 性能のグレードアップ」「外部記憶へのアクセス速度の向上」「通信回線性能の向上」が必要となってしまう。ウィルス防護は、それらの性能の一部を「犠牲」にして実行されているのが現状である。もちろん、「ウィルス防護ソフトを組み込んでいない状態」と同程度の性能を実現しようとするならば、さらなる出費が必要となる。

また、通信時に「現有技術において使用することが可能であるにもかかわらず、その使用によって便益が供与される類の機能」の一部は、「コンピュータウィルス」の存在によって「使用不可」もしくは「使用しないことが望ましい」という状況が存在する。たとえば、JavaScript や ActiveX、JavaApplet などは、「通常使用」に関しては問題ないと思われるが、「地下系 (UG 系)」サイトを訪れる場合には「オフ」にすることが望ましい。もしも「コンピューターウィルス」の心配がなければ、それらを「常時オン」に設定したままでの閲覧が可能となる。現状、「通常使用」に関してはほぼ問題ないが、逆に言えば「リスク」と「リターン」を秤にかけて、「リターン」に重きをおいている状態である。当然のことながら、その場合においては「リスクは承知の上」で使用していることになるが、実際に被害を受けている事例は少なくない。

コンピューターウィルスは、単なるバグでも、単なる不正行為でもない。それらを生産する製作者の「不断の努力」によってこの世界に存在しつづけ、今この瞬間にも、どこかのサーバーやユーザーの「情報伝達」を阻害している。彼ら「コンピューターウィルス」の製作者には、明らかな「意図」「悪意」が存在している。本研究は、コンピューターウィルスの諸様相に関して包括的な議論の場を構築することをその主たる目的としている。議

論が行われるためには、共通認識が必要かつ不可欠である。一つの用語を同じ意味で使用する二者の間でしか、有効な議論は成立しない。しかしながら、コンピューターウィルスの諸様相に関しての用語や概念に関しては、その使用者によってかなりの偏差が存在し、それがコンピューターウィルスを考え、議論するうえで、障害となっているという現状が存在する。したがって、本書では、まず第一の段階として必要なのは概念の整理であるという認識のもと、定義および分類に十分な紙幅を費やした。さらに、コンピューターウィルスに付随して発生する様々な現象に関しても、同様の共通認識を形成することを企図している。

さらにその際、認識の基盤をどこに置くかという問題に遭遇する。これまで、コンピューターウィルスは「単なる不正プログラム」として認識され分類されてきた。それが間違いであったわけではないが、この問題に対処するためには「新しい認識の枠組み」が必要であると考えられる。コンピューターウィルスの「流行」を可能な限り少ないものとし、その被害を最小限に抑えるためには、その本質を捉える必要があると考える。本論では、以下に示す基本的な認識を定置する。

1) コンピューターウィルスを、ウィルス学・疫学・予防医学の視点から捉える。
2) コンピューターウィルスの実体を、「アルゴリズム」と考える。

上記 1) を定置する理由は、既存の、成功した学問分野における知見を最大限に利用することが、この問題を解決するための近道であると考えることによる。ウィルス学・疫学・予防医学は、「医学的ウィルス」の感染防止や治療に関して、確固たる実績を上げている。もしもその分野の知見を活用 / 内挿することが可能であれば、問題解決の労力を著しく軽減することができる。特に、現在における「コンピューターウィルス対策」は、「発生し、蔓延しつつあるコンピューターウィルス」から電子機器などで構成されるシステムをどのように防護するかという意味で「対症療法的」なものとなっているが、本来「予防医学」「疫学」的に考えるならば、その産生 / 発生の頻度などを減衰させることを考えなくてはならない。

上記 2) は、1) を定置したことによって付随的に発生する「概念の見直し」である。進化・感染・発症の各段階をくまなく網羅しつつ「医学的ウィルス学」における知見を援用しようと考える場合には、上記 2) のような「概念の変更」が必要となる。なぜなら、コンピューターウィルスの「進化 (もしくは亜種の発生) は、それを作成する「ハッカー」の脳内で起こる事象だからである。コンピューターウィルスは「宿主 (しゅくしゅ)」であるハッカーに論理的に感染し、そこで「進化」し、さらにそこから他へと「感染」していく。そのとき、コンピューターウィルスの「実体」は、電子的情報として記述されたプログラムではなく、「アルゴリズム」であると考える必要が生じる。その際、「コンピューターウィルスのアルゴリズムを知る」ことが「中間宿主への感染 [2)] 」となると考えられる。

2. コンピューターウィルス生態学における要素概念の定義の提案

2.1. 概念の整理

コンピューターウィルスを「自然ウィルス(医学的ウィルス)」と相同の構造のもとに把握しようとする本論における試みには、一部に困難が存在する。それは、コンピューターウィルスが2つの異なる様相を有していることによる。まず、コンピュータウィルスは「アルゴリズム」である。これは、すべてのコンピューターウィルスが何らかの「プログラム」として顕在化することに由来する。「プログラム」とは、ある人間の脳内に存在している「アルゴリズム」の顕在形である。したがって、プログラムが存在するところには、かならずその前段階としてのアルゴリズムが存在する。アルゴリズムとは「演算手順」であり、それによって「プログラム」が生成される。

したがって、コンピューターウィルスを考える段階においては、この「アルゴリズムの伝播」と「コンピューターウィルスの伝播」を別として考える必要が存在する。しかしながら、さらに問題を複雑にしているのは、この二つ(アルゴリズムの伝播と、コンピューターウィルスの伝播)が、不可分である場合を想定できるからである。たとえば、ある「コンピューターウィルスの実行形式のコード」が存在する場合、それを逆アセンブルもしくは逆コンパイルすることによって、その「アルゴリズム」を知ることができる(多くの「ハッカー」はそのような手順を踏むことによって、そのアルゴリズムを学ぶ)。したがって、コンピューターウィルスの伝播そのものが、「アルゴリズムの伝播」を惹起する場合がある。

しかし当然のことながら、純粋な感染者においては、「アルゴリズム」そのものは伝播せず、使用しているマシンが「感染する」のみである。

本論においては、それらの違いを前提としつつ、自然ウィルス学における「自然宿主」「中間宿主」「感受性宿主」「媒介宿主」「終宿主」という要素概念を、コンピューターウィルスを考えるために再定義することを試みる。

①自然宿主

コンピューターウィルスの「アルゴリズム」を脳内に知識として有している人間のうち、そのアルゴリズムを用いて実際に「悪意のあるプログラム」を作成しない人間のことを指す。もちろん、実験的に作成する場合を想定することができるが、その場合の位置づけは難しくなる。たとえば筆者はここでいう「自然宿主」であるが、現状においてはウィルスを作る可能性は皆無であるものの、過去においては実験的に作成したことがある。端的に言うならば「たとえ作成したとしても、使用しない」という場合に「自然宿主」であるとする。一般に自然宿主は通信系の研究者もしくはエンジニアである。

②中間宿主

コンピューターウィルスの「アルゴリズム」を、他から伝播され、それを実際に実装する(プログラムとしてコード化し、実際に使用すること)者のことを指す。この中間宿主

において、「自然宿主においてはアルゴリズムでしかなかったもの」が、実装され、現実に被害をもたらす「プログラム」もしくは「システム」となる。したがって、中間宿主は「人」である。中間宿主は、「プログラミング」を遂行しうる技術を有するエンジニアである場合が多いが、昨今の事例では「さほどの技量を有していなくても」コンピューターウィルスのプログラムを作成することは可能なので、必ずしもエンジニアや研究者に限られるわけではない。

③感受性宿主

後に説明する「終宿主」「媒介宿主」を含んだ概念である。中間宿主によって生成されたコンピューターウィルスに感染し、何らかの「発症」をするシステム／ハードウェアもしくは人を指す[3)]。ここで言う「発症」とは、単に破壊活動のみならず、潜伏して他のハードウェアへの感染の媒介となるものも含む。また、感受性宿主が発症するとき、その発症の原因となる要素を「病原性」と呼ぶ。

④媒介宿主

感染したシステム／ハードウェア／人においては「被害」を発生せず、単に別のシステムなどへの感染の足がかりとなっている場合のことを指す。近年では、bot における潜伏感染などが代表例である。

⑤終宿主

コンピューターウィルスに感染することによって、何らかの被害を蒙るシステムやハードウェアのことを指す[4)]。多くの場合、検知され、除去される。もしくは、システムそのものが破壊されることよって、感染が終了する。もちろん、終宿主から新たな感染が広がることもある。

上記のように、自然宿主に端を発するコンピューターウィルスは、中間宿主を経由して、感受性宿主・媒介宿主へと至り、最終的には終宿主へと到達する。そのような様態を本論では「コンピューターウィルスのライフサイクル」と呼ぶ。

2.2. コンピューターウィルスの定義

コンピューターウイルスに関する定義には様々なものが存在している。computer virus という用語を学術的な文脈において最初に使用したのは Fred Cohen であるとされる[5)]。Cohen(1984) によれば、コンピューターウィルスとは、

「第三者が作成したプログラムに、それ自身のコピーを含ませるために、それらのプログラムを修正することによって伝染することが出来るプログラム」

であるとされる[6)]。しかしながらこれは少々あいまいな定義である。日本においては、これを少々改変したものが使用されている。すなわち、

「第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、感染機能、潜伏機能、発症機能の一つ以上有するもの。」
という定義である[7]。

これは、コンピューターウィルスの定義というよりは、むしろ「悪質ソフト=malware」の定義であるというべきであるが、本書においては、この定義をもって「広義のコンピューターウィルス」とする。したがって、
広義のコンピューターウィルス　=　悪質ソフト (malware)
となる。

しかしこの定義も十分なものであるとはいえない。なぜなら、この定義においては、コンピューターウィルスの製作者を認識しえないからである。コンピューターウィルスとは、上記で定義されているように「作られたプログラム」である。本書の基本的立脚点は、「インフルエンザウィルス」などのような「自然ウィルス」の研究分野において培われてきた手法や知見を「コンピューターウィルス」に応用することである。

ここでは、まず以下の 2 種類の定義を定置する。

1)「広義の」コンピューターウィルス

本論における「広義の」コンピューターウィルスとは、コンピューターの使用を媒介として伝播・感染する、「情報の疎通を阻害する情報因子」のことを指す。この定義においては、bot、ワーム、ブラウザークラッシャー、サービス妨害プログラム (DOS) なども含まれる。

つまり、「コンピューターによる電子的な情報の受け渡しによって感染する」ものであるにもかかわらず、「コンピュータによる電子的な情報の受け渡しを阻害する」ものである。この「矛盾した構成」が、コンピューターウィルスの「広義」の定義として重要である。自らは電子的伝播媒体によって拡散しつつも、その「情報のやりとり」を阻害することを目的とするものであるという「矛盾」を持っている。この意味においての「コンピューターウィルス」は、必ずしも「電子的な形態」を保持していなくともかまわない。「情報の疎通を阻害するための何らかの意志」がそこに存在し、それが実際に「情報の疎通を阻害しうる」形をもった時点で、それは「コンピューターウィルス」であるといえる。ただし、当然ではあるが、単に「人為的な妨害活動」や「妨害行為」は、コンピューターウィルスではない。コンピューターウィルスは、「電子的に、単独で」活動しうる形態を持っている必要がある。「広義」の場合には、その潜在的形式も含むものの、最終的には、何らかの「電子的媒体」としての表現形を持つ必要がある。

本論においては「コンピューターウィルス」という場合、特にことわりの無い場合、それは「広義の」コンピューターウィルスを指す。それは最終的には「電子的なプログラム」などの形態を示すものの、必ずしもその形態を伴っているものばかりではない。
「広義のコンピューターウィルス」は、「自己増殖機能あり」と「自己増殖機能なし」の二つに大きく分類されている。「自己増殖機能」とは、コンピューターウィルスが自らの複

製を作り、さらに別のシステムなどへと感染していくことを示す。

広義のコンピューターウィルス			
自己増殖機能あり			自己増殖機能なし
感染・増殖・発症に際して、感受性宿主を必要とする	感染・増殖・発症に際して、媒介宿主を必要とするが、感受性宿主を必要としない	ファイル感染・ブートセクター感染せず、単体で動作し、増殖・発症する	トロイの木馬 論理爆弾
狭義のコンピュータウィルス※1	ワーム※2	バクテリア	

図1　広義のコンピューターウィルス

2)「狭義の」コンピューターウィルス

「狭義の」コンピューターウイルスとは、コンピューターの使用を媒介として伝播・感染する「コンピュータ用に作成された不正なプログラム」のことを指す。ここで「不正」とは、その使用者の本来の意図とは異なるという意味である。あるマシンの使用者が「不正なプログラム」によって、その意図とは別の動作を余儀なくされたとき、それが「狭義の」コンピューターウィルスとなる。この定義ではそのプログラム作成者の意図や目的などが問題なのではなく、使用者の意図を阻害するプログラムであることが重要となっている。

※1　狭義のコンピューターウィルス				
ファイル感染型			ブートセクター感染型	複合感染型
プログラムファイル感染型		マクロ感染型	（ブートセクターに感染するウィルスのうち、マクロによって実行されるもの以外）	
追記感染型	上書き感染型	マクロウィルス		

図2　狭義のコンピューターウィルス

※2　ワーム					
電子メール型					ネットワーク型
添付型	スクリプト型				特定のポート経由で直接に攻撃を行い、感染する
添付ファイルを経由して感染する	VBA Script 型	Java Script 型	Java アプレット型	ActiveX コントロール型	

図3　ワーム

3. コンピューターウィルス生態学における要素概念の概略

コンピューターウィルスは、通常ハッカーの脳内で情報因子として発生し、プログラミングなどの方法によって電子的な形を得る。また、それは情報因子であるために、その表現形式はかならずしも「電子的」な形をとっている必要はない。文字として表現される場合もあれば、図として表現される場合もある。しかしながら、それが実際に活動する場合には、電子的な形をとる必要がある 。

3.1. 自然宿主における生態

自然宿主におけるコンピューターウィルスの生態に関しては、特に多くを語る必要は感じられない。それは単に通信系のハードウェア・ソフトウェア関連の知識や技術であり、コンピューターウィルスとは言っても、それらの既存知識および技術の上に成立している

ものは明らかだからである。

ここで、「インフルエンザウィルス」と「コンピューターウィルス」を比較検討してみる。インフルエンザウィルスに代表される「自然ウィルス」は通常の場合、害をなすことはなく平和に生物と共存している。前述のとおり、ウィルスが「自然に」かつ「害をなさず」に存在している場合の宿主を自然宿主(しぜんしゅくしゅ)と呼ぶ。

自然ウィルスにおいては、人間が自然を破壊したり、未知の領域に踏み込んだ場合に、自然宿主内に存在していた「ウィルス」が人間に感染する。自然宿主においては害を形成しなかったウィルスが、「人間」の宿主に感染すると、害を形成するようになる。

そして、これと同じ状況が「コンピューターウィルス」においても発生しうる。エンジニアは、その意味で「特殊」な存在である。鳥インフルエンザウィルスにおける「鴨」のような状態であるといえる。

コンピューターウィルスは、多くのエンジニアを自然宿主として存在しているものであるが、彼らの多くは発症しない。彼らエンジニアから、何らかの経路で「ハッカー[9)]」と呼ばれる人間たちに感染することがある。もしくは、何らかの原因で「自然宿主」である「エンジニア」が「人間社会」に対して被害感情を持ったり、疎外感を感じたりした場合、「感染源」となることもある。ただしその場合においても「発症」はしない。ハッカーは、「優秀な」エンジニアである場合が多い。もちろん彼らは(ハッカーであれ、通常のエンジニアであれ)「自然宿主」であるので、発症することはない。この二種類の自然宿主の違いは「感染源となるか否か」である。

実際には、いくつかの種類の「自然宿主」を想定する必要がある。

1) 他への感染源にならない自然宿主
2) 自然宿主への感染源となる自然宿主
3) 中間宿主への感染源となる自然宿主

3.2. 中間宿主における生態

コンピューターウィルスは、単独では進化できない。コンピューターウィルスは、ハッカーを宿主として再生産される過程において進化し、その進化形は「亜種」と呼ばれる。また、電子機器によって増殖する場合もある。このとき、ハッカーなどの宿主を「中間宿主」と呼び、電子機器もしくはそのユーザーを「感受性宿主」と呼ぶ。「中間宿主」による増殖は、以下の経路で行われる。

①ハッカーがコンピューターウィルスに接触

このとき、ハッカーの使用している電子機器そのものは、コンピューターウィルスに感染しない場合が多い。なぜなら、中間宿主として正常に機能するためには、その使用機器が「正常に動作している」ことが必要であり、また、一般的に言って「ハッカー」は、比

較的高いレベルの「ウィルス防護」を自らの電子機器に施している場合が多いことによる。したがって、「中間宿主」としてのハッカーがウィルスに接触するということは、ハッカーが「あるコンピューターウィルスの情報を知る」ということに等しい。

②ハッカーが論理的[10]にコンピューターウィルスに感染

中間宿主は、情報破壊因子としてのコンピューターウィルスの「何らかの要素」によって感染する。この「何らかの要素」については後に検討するが、中間宿主の種類や性質などによって「感染する要因」は異なる。このとき中間宿主は「物理感染しない」ことに注意が必要である[11]。

③ハッカーにおいて、コンピューターウィルスが進化を遂げる

一般に、ハッカーは「知識」として多数の情報破壊因子を有している。つまり「論理感染」している状態である。それらが「融合」され、進化した形式のコンピューターウィルスが「情報」として発生する。どのようなコンピューターウィルスが発生するかは、その中間宿主の脳内にどのような「情報破壊因子」がすでに存在していたかに大きく依存する[12]。

④論理感染したハッカー(中間宿主)が、コンピューターウィルスを電子的媒体へと移植する

これは、中間宿主の自発的行動として行われる場合が多い。もちろん、このとき、中間宿主の「プログラミング技術」「ソフトウェアエンジニアとしての技量」「通信技術者としての技術力」などが影響し、それらによって、実際に発生するコンピューターウィルスは、強い感染力や破壊力もしくは病原性を有するようになる。

あるコンピューターウィルスに論理感染した中間宿主は、そのウィルスを「進化」させ、亜種を産生する場合がある。そのとき大量の亜種が発生するウィルスと、そうでないものが存在することが知られているが、それは「論理感染」しやすいものと、そうでないものが存在することによる。また、論理感染したものであっても、亜種が産生されない類のウィルスが存在する。それは、論理感染の帰結としてのコードの生成の難易度などによって多分に左右されていると考えられる。最近流行しているbotなどにおいては、コーディングが容易であるスクリプト系の言語で書かれているものが多く、大量の亜種の発生の原因となっていると考えられる。

中間宿主としてのハッカーの生態に関しては、未知の部分も多く、彼らがどのようなものに論理感染しやすいのか、もしくは彼らがどのようなものに触手を伸ばしやすいのかについては、今後さらに精査しなくてはならない。

3.3. 感受性宿主における生態

すべてのコンピューターウィルスは、自然宿主である研究者やエンジニアの脳内で発生し、中間宿主であるハッカーの脳内で変性され、さらに電子的媒体を経由して、その他の電子機器やそのユーザーに対して伝染・感染していく。そのとき、感染先となる電子機器およびユーザーを「感受性宿主」と呼ぶ。感受性宿主が電子機器であるかユーザー(人)であるかによって、その様態は異なる。

①感受性宿主が人である場合

感受性宿主という場合の「感受性」とは、何らかの病原性の影響を受けるという意味を持っている。病原性の種類によって、どのような行動が惹起されるかは様々であるが、多くの場合には「情報の送出」となる。もしくは、コンピューターウィルスの実行形式ファイルそのものを「媒介する」という場合もある。感染の結果として「媒介」が発生するという場合、「媒介性宿主」との違いが明確ではなくなるとも思われるが、人である感受性宿主における「媒介」とは、論理感染したユーザーの能動的な行為によって媒介が行われる場合のことを指す。

感受性宿主においてコンピューターウィルスが進化することはなく、表面的には単に潜伏し、他の感受性宿主に対しての感染活動や破壊活動を行うこととなる。もちろん、「感受性」を有する電子機器やユーザーにおいては、病原性が発生し、発症する。たとえば、フィッシング詐欺において、個人情報を送出してしまったり、ID や PW を送信してしまったりする場合などがそれに該当する。さらには、それと気づかずにウィルスを含んだ添付ファイルを開いてしまって感染する場合なども「感受性宿主」の様態と考えることができる。この「感受性」をより広くとるのであれば、チェーンメールなどの文言も「病原性」を有しているものと考えられる。チェーンメールを送信してしまうことが「発症」であり、すなわち感受性宿主としての性質を有していたと定義することもできる。

また、感受性宿主であるユーザーが論理感染することにより、コンピュータウィルスが「論理的に潜伏する」こともある。このとき、その感受性宿主は「中間宿主」となる。中間宿主においては「病原性」は効果を持たない。つまり、「感受性宿主」が病原性に対しての「感受性」を失うことが、感受性宿主が中間宿主(= ハッカー)になるための条件であると言える。つまりそれは、「コンピューターウィルスの被害を受けない状態になる」ことを指す。

②感受性宿主が電子機器である場合

感受性宿主として電子機器を想定する場合、一般に、感染経路の種類によってコンピューターウィルスを分類する場合が多い。感受性宿主を通しての感染経路は以下のように多種存在する。

1) ファイル経由 (トロイの木馬)
　1-1) アプリケーションファイル経由
　1-2) 電子メール添付ファイル経由

2) 通信ポート経由
　2-1)P2P ポート経由
　2-2)Telnet ポート経由

3)Web 経由
　3-1)JavaScript 経由
　3-2)ActiveX 経由
　3-3)CSS 経由
　3-4) ヘルパーアプリケーション (プラグイン) 経由
　3-5) ブラウザー (HTML) 経由 (ブラクラ)

4) アプリケーション経由
　4-1) メーラー経由
　4-2) プレイヤー経由
　4-3)GDI 経由
　4-4) マクロ経由 (マクロウィルス)

　上記分類のうち、特に 1) を Torojan(トロイの木馬) と呼び、また 2) をワームと呼ぶ。また、3) には、「ブラウザークラッシャー」が含まれるが、正確には「ウィルス」に分類される類のものとは一線を画する必要がある。これらのうちには、感受性宿主としてのユーザーを想定しているものが含まれているが、本来、厳密に分類しておくべきである。

3.4. 媒介宿主における生態

　コンピューターウィルスに感染しても、その感染者 (感染機器) が発症しない場合がある。そのようなとき、その感染者 (感染機器) を「媒介宿主」と呼ぶ。
媒介宿主の存在は、非常に奇妙なものであるように見える。感染したのみで発症せず、単に他の感染者 (感染機器) に対して、ウィルスを感染させることを目論むものだからである。そのようなものの代表としてワームがあげられる。ワームは、感染対象が発症しないまま、感染対象を足がかりとして別の感染対象へと拡散していく。もちろん、感染対象が発症することもある。媒介宿主として振舞うことと、感受性宿主であることは両立しうる。端的に言うならば、潜伏期においては媒介宿主として振る舞い、後に発症するという場合などを想定することができる。

また、bot においては、媒介宿主が重要な役割を担う。bot は、初期の段階においては純然たる「媒介宿主」として振る舞う。なぜなら「より多くの宿主に感染すること」が bot の初期の目的だからである。十分な数の感染者 (感染機器) を得た時点で、bot は何らかの経路で「指示」を受け、それによって発症する。

このようなタイプのウィルスや寄生虫は、自然界には存在しない。したがって、bot は「コンピューターウィルス」に分類されにくいものであるともいえるが、明らかに malware ではあり、「広義のコンピューターウィルス」には分類されるべきものである。

bot や一部のワームは、媒介宿主である段階と、感受性宿主である段階の二つを持つ「特殊なコンピューターウィルス」であると言える。bot は、何らかの「指示」によって、感染者である媒介宿主を「感受性宿主」へと変化させる。bot の感受性とは、「他の電子機器への攻撃開始」となる場合が多く、宿主機器においては病原性が発現されない場合が多い。被害は、宿主機器が攻撃対象とした機器において発生する。このとき、「宿主」において発症する病原性は「他者への攻撃」となる。

3.5. 終宿主における生態

終宿主は、「感受性宿主」の一形態である。感受性宿主のうち、感染したコンピューターウィルスの破壊活動などによって、システムそのものがダウンするなどの「動作不全」を発生する場合、その宿主を「終宿主」と呼ぶ。当初から終宿主の存在が想定されていないコンピューターウィルスも存在する。つまり、終宿主とは、あるコンピューターウィルスが「最終的な工作対象」として想定している電子機器がある場合の、その「対象となる電子機器」のことを指す。

4. おわりに

コンピューターウィルスの産生 / 発生を減弱させるのは、単に「防護的な措置」のみでは難しい。現在までのウィルス防護においては、本論における感受性宿主および媒介宿主における対策のみが検討されている。しかしながら、コンピューターウィルスのライフサイクルに鑑みれば、中間宿主における対策が効果的であることを指摘しうる。自然ウィルスとコンピューターウィルスの最も大きな相違点は、「コンピューターウィルスは、人が作成するもの」であるという点にある。コンピューターウィルスが本論で提案したようなライフサイクルを有し、進化し、発生し、伝播していくということを考慮に入れた対策を練らない限り、その発生数を低下させることは難しいと考えられる。そのためには、本論で述べた概念のうち、とくに「中間宿主における生態」を精査し、その段階における効果的な対策を立案する必要があると考えられる。この分野の研究は端緒であるが、今後の発展が望まれる。

【注】

注 1) 本論とはあまり関係がないことではあるが、本論においては computer の邦訳語として「コンピューター」を用いる。これを「コンピュータ」というように最後の音引きを省略した訳語を使う事例を多数見ることができるが、明らかに「奇妙な訳語」であり、まったく許容できない。ちなみに「サーバー (server)」を「サーバ」とするのも奇妙であり、それを許容しうるというのであれば、「セーター」は「セータ」に、「ハンバーガー」は「ハンバーガ」に、また、「メーター」は「メータ」に、「メーカー」は「メーカ」にすべきであろう。

注 2) 「自然宿主」とは、ウィルス学の用語であり、「自然界に普通に存在しているウィルスを保持しつつ、発症をしない状態」のことを指す。

注 3) ここで「人」を感受性宿主の一要素としてとらえる必要がある。「人」は、運用されていいるシステムの「一要素」である。たとえば、メール経由での感染の場合、「人」が誤操作をすることによって感染が広がる場合があるが、そのような誤操作を誘導するようなコンピューターウィルスである場合、「人」を感受性宿主と考える必要がある。

注 4) 終宿主には「人」が含まれないとする。もちろん、何らかの被害を被るのはつねに「人」であるが、それは「論理感染したこと」によって発生する被害ではなく、「物理感染したシステムでの被害」を経由しての間接的な被害である。さらに言えば、「物理感染したシステム」を使用していたユーザーの大半は「論理感染」していない。これには議論が必要であるが、現状では、この定義を採用する。

注 5)Cohen, F. 1984. Experiments with Computer Viruses. http://www.all.net/books/virus/part5.html (accessed January 29, 2006).

ただし論文中では、"virus" という言葉の使用を考えたのは Len Adleman であるとされている。

注 6)Cohen,F. 1984.Computer Viruses - Theory and Experiments. http://vx.netlux.org/lib/afc01.html(accessed January 29, 2006).

注 7) 独立行政法人情報処理推進機構 (IPA) の「コンピュータウイルス対策基準」における定義による。http://www.ipa.go.jp/security/antivirus/kijun952.html(accessed January 29, 2006)

注 8) 本論においては、「電子機器上の存在するファイル・ブートセクターへの感染やウィルス本体の複製」を「物理感染」と呼び、「情報として感染すること」を「論理感染」と呼ぶ。

注 9)「ハッカー (hacker)」とは、hack という動詞の派生形である。hack とは本来、何らかのシステムやプログラムを「上手に解析したり改造したりする」という程度の意味で使われてきたが、現在においては「システムの裏をかいたり、システムの脆弱性をつくことによって、何らかの不正行為を行う」という意味で使われるようになりつつある。本論では、この解釈の変遷を採用し、「ハッカー」を、従来の意味での「クラッカー (cracker)= 破壊者」や「インヴェーダー (invader)= 侵入者」という意味で用いている。筆者はそのような意味の変遷を決して快くは思わないものの、インターネット上での用語法においても、これらの「意味の変遷」が主流となりつつあることを勘案した。

注 10) 本論においては、「人間が、情報因子しての (広義の) コンピューターウィルスに感染する

こと」を論理感染と呼び、「電子機器などが(狭義の)コンピューターウィルスに感染すること」を物理感染と呼ぶ。

注 11) より正確に言えば、「中間宿主」となりえるのは「人」のみであるので、物理感染しないのは当然である。

注 12) まだ、どのような「情報破壊因子」にも感染していないハッカーが初めて「感染する」経緯に関しては、未だ研究は端緒であると言える。多くの場合、「社会に対する不満」「過度な承認欲求」「自己評価の高さ」などの共通した要素が存在していると考えられているが、それのみではなく、より決定的な「因子」の存在が指摘されるべきであると思われる。