自律進化型マルウェアに対抗するアンチマルウェアシステムモデルの構築

代表研究者	平田 孝志	関西大学　システム理工学部　准教授
共同研究者	木村 共孝	同志社大学　理工学部　助教
	本仲 君子	関西大学　システム理工学部　助教

1 はじめに

近年のインターネットの急激な発展に伴い，コンピュータウイルス，ワーム，トロイの木馬といったマルウェアの被害が拡大してきている．中でも，これらのマルウェアに感染したコンピュータ（ゾンビコンピュータ）群がネットワークを形成するボットネットは，攻撃者の遠隔操作によって一斉にサーバ等の標的を攻撃するため，極めて大きな脅威となっている．大規模なボットネットは数百万台のゾンビコンピュータで構成されるものも存在し，それらのコンピュータの計算資源を利用した分散コンピューティングによりクレジットカード情報の詐取等を行ったという事例もある．一方，近年のコンピュータの性能上昇に伴い，機械学習が日々発展を遂げている．機械学習は入力されたデータを用いた学習により，アルゴリズムを進化させていく技術である．機械学習の応用範囲は広く，画像認識，音声認識，自然言語処理等の様々な分野で用いられている．さらには，機械学習によりソフトウェアのバグや脆弱性を発見するという研究も行われている．

このような背景のもと，これまでの研究において，ゾンビコンピュータ資源を利用した分散機械学習によりソフトウェアの脆弱性を発見し，その脆弱性に合わせ自らのコードを書き換えることで自律進化するような，自律進化型ボットネットと呼ばれる新種のボットネットの出現が予見されている[1]．また，この自律進化型ボットネットの感染力は従来のボットネットと比較にならないほど驚異的であることが数学的なモデル化によって示されている．マルウェアや機械学習が急速に進化している現状を考えると，このような自律的に進化するボットネットの近い将来における出現は想像に難くなく，早急な対策が必要不可欠である．

そこで本稿では，これまでの研究から得られた知見をもとに，この自律進化型ボットネットに対抗するアンチマルウェアシステムモデルの構築を行う．そのために，決定論的モデルおよび確率論的モデルの両者の側面から，課題の解決を狙う．決定論的モデルは将来の挙動を一意に予測することが可能であり，一方，確率論的モデルは短時間にランダムで発生するような事象を解析できる．このように多角的な視点により，その脅威をより深く考察する．本稿では，まず決定論的モデル化により，自律進化型ボットネットの感染ダイナミクスを表し，どのような条件において感染が拡大するのかを明らかにする．そしてその上で，未感染のコンピュータを利用して分散機械学習を行い，自律進化型ボットネットよりも先に未知の脆弱性を発見することであらかじめ感染を防ぐ，ボランティアモデルの提案を行う．計算機シミュレーション実験による評価により，ボランティアモデルの有効性を示す．

次に，確率論的モデル化により，より詳細な感染抑制の考察を行う．具体的には，確率論的感染モデルにゲーム理論の適用を検討する．ゲーム理論を用いることで，マルウェア感染を抑制できる可能性のある防御側の意思決定を見ることができる．本稿では，ホスト間の繋がりで構成されるネットワークを考慮した畳み込みニューラルネットワーク（Convolutional Neural Network: CNN）[2]を用いた感染拡散予測法の提案も行う．確率論的モデルにおける計算機シミュレーション実験ではネットワークの規模が大きくなるほど，計算時間が大幅に増加する問題がある．CNN を用いることで，短時間でボットネットの感染力の強さを推定することが可能となる．本稿では数値実験により感染拡散予測法の有効性を示す．

本稿の構成は以下のとおりである．2 節において，自律進化型ボットネットの概念及びその感染モデルを示す．3 節において，決定論的モデルによるアプローチの検討，評価，考察を行う．4 節においては，確率論的モデルに基づき，ゲーム理論の適用及び感染拡散予測法の提案を行い，その評価，考察を行う．5 節において，本稿をまとめる．

2 自律進化型ボットネット

2-1 概念

現在，ウイルスは日々進化しており，ボットネットのようにゾンビコンピュータ群でネットワークを形成

し大規模な攻撃を行うものや，変形性マルウェアのように，ホストに感染する度に自分自身のコードを書き換えることで難読化を行い，アンチウイルスソフトに検出されにくくするものが存在する[3]．また，[4] や [5] では，遺伝的アルゴリズムを用いて，既知のマルウェアのコードを組み合わせることで新たなマルウェアを生み出し，コードの難読化やソフトウェアへのマルウェア埋め込み等を行う手法が提案されている．マルウェアはホスト上で動作するソフトウェアの脆弱性を突くことでホストを感染させるが，[6] や[7] において，静的コード解析及び機械学習を用いてソフトウェアの脆弱性を検出する手法が提案されている．これらの手法では，ソフトウェアのソースコード中の文字列を分割し，それらを特徴とすることで機械学習を行う．既知の脆弱性を用いて学習することで，ソフトウェアのどの部分が未知の脆弱性を含むのかを予測することを可能としている．上記のようなマルウェアの進歩を考えると，これらの脆弱性検出手法が，将来的にマルウェアの機能の一部として用いられることは想像に難くない．

機械学習においては，深層学習の発展により，コンピュータが人間の手を借りずに自律的に人間や猫の顔を認識するに至った，というような目覚しい成果を上げている．深層学習では，多層ニューラルネットワークを用いた特徴量の自動抽出により，教師なしでの学習を行うことが可能である．深層学習では通常，扱うパラメータの数や学習量が膨大であるため，実用には非常に多くの計算資源を必要とする．そこで，深層学習において，多数の廉価なホストを用いて分散的に学習を行う手法がこれまでに提案されている[8]．これらの手法を用いると，ボットネットに属するゾンビコンピュータ上で学習を行うことが可能となり，悪意のある攻撃者によって，上述の脆弱性の検出に利用される恐れがある．以上のことを勘案すると，各ゾンビコンピュータの資源を用いて学習を行い，分散型静的コード解析によりソフトウェア脆弱性を自動的に検出し，それに合わせてコードを変異させるようなボットネットが出現する未来が十分に予測できる．さらにそのボットネットは，検出した脆弱性を用いて新たにホストを感染させ，より巨大なボットネットを形成し，また，その計算資源を利用して新たな脆弱性を発見するというような繰り返しの自律進化を行うことが考えられる．本稿ではこのようなボットネットを自律進化型ボットネットと呼ぶ．自律進化型ボットネットは，自律的に変異を繰り返しながら進化するため，通常のウイルスに比べ感染力が非常に高いと考えられ，そのため，ネットワークから完全に除去され難く，将来のインターネット社会の脅威となり得る．

2-2 感染モデル

我々は，自律進化型ボットネットの脅威を明らかにするために，その挙動を表す感染モデルを提案している．提案感染モデルでは，ネットワーク内に存在する各ホストの状態を，図 1 に示される SIRS（Susceptible-Infected-Recovered-Susceptible）モデルにより表す．「S」はホストが何らかの脆弱性がある状態（脆弱状態）を，「I」はホストがボットネットマルウェアに感染した状態（感染状態）を，「R」はホストが脆弱性を全く持たない状態（保護状態）を意味する．なお，保護状態は既知の脆弱性から保護されている状態であり，未知の脆弱性からは保護されていないことを想定している．図 1 に示すように，脆弱状態にあるホストは，ボットネットマルウェアに感染する可能性があり，感染ホストによる攻撃により感染状態に移行する．また，脆弱状態もしくは感染状態にあるホストは，例えばアンチウイルスソフトによるボットネットマルウェアの駆除や保護，もしくは OS のアップデート等により脆弱性が取り除かれることで，保護状態に移行することが可能である．さらに，自律進化型ボットネットが既知の脆弱性情報を用いた分散機械学習により新たな脆弱性を発見した場合，保護状態のホストは脆弱状態に戻る．以下に，提案感染モデルの動作をまとめる．

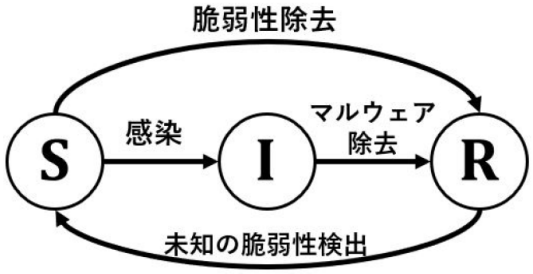


図 1 SIRS モデル

1）感染ホスト同士でボットネットを形成することで，分散機械学習を行い，新たな脆弱性を発見する．感染ホストが多いほど，発見する確率は高くなる．また，このとき，保護状態のホストは脆弱状態に遷移する．
2）脆弱状態にあるホストは，一定の確率で保護状態へ移行する．
3）脆弱状態にあるホストは，一定の確率でボットネットマルウェアに感染し，ボットネットに組み込まれる．一方，保護状態にあるホストは感染しない．

4）感染ホストは一定の確率でボットネットマルウェアが取り除かれ，保護状態へ移行する．このとき，脆弱性を区別せず，脆弱性は一度に全て取り除かれる．

3 決定論モデルによるアプローチ

3-1 感染ダイナミクスによるマルウェア拡散解析

（１）感染ダイナミクス

これまでの研究では，自律進化型ボットネットの脅威を明らかにするために，決定論的感染モデルの提案を行い，数値計算によりその脅威が示されているが，それは自律進化型ボットネットの感染力が非常に強いということのみ示しており，初期ホスト数に対する挙動の変化やボットネットマルウェア蔓延後の様子など詳細な解析が行われていなかった．そこで本研究では，自律進化型ボットネットの決定論的感染モデルに基づき，疫病の感染力や人口の増加減少の解析に一般的に用いられる基本再生産数の導出を行い，ボットネットマルウェアの拡散及び消滅の初期条件を明らかにする．さらに，ボットネットマルウェアが初期段階において拡散してしまったと仮定したときに,そのボットネットマルウェアが消滅に向かう条件を明らかにする．最後に，これらの条件に基づく数値計算により自律進化型ボットネットの感染拡散の振る舞いを調べる．

ネットワーク内の全ホスト数を N 台，時刻 t において脆弱状態にあるホスト数を$S(t)$，感染状態にあるホスト数を $I(t)$，保護状態にあるホスト数を$R(t)$ とする．このとき，各状態のホスト数の単位時間あたりの変化量は，以下の常微分方程式系により与えられる．

$$\frac{dS(t)}{dt} = -\alpha S(t)I(t) + \gamma(I(t)+1)R(t) - \delta S(t) \qquad (1)$$

$$\frac{dI(t)}{dt} = \alpha S(t)I(t) - \beta I(t) \qquad (2)$$

$$\frac{dR(t)}{dt} = \beta I(t) - \gamma(I(t)+1)R(t) + \delta S(t) \qquad (3)$$

ここで，α はマルウェア感染率，β はマルウェア除去率，γ は脆弱性検出率，δ は脆弱性除去率を表すシステムパラメータである．

（２）感染拡散解析

ここでは，自律進化型ボットネットの感染ダイナミクスにおける基本再生産数の導出及びそれに基づく解析により，自律進化型ボットネットの感染拡散及び消滅の初期条件を導く．基本再生産数は集団にいる全てのホストが感受性を有した状態（脆弱状態）で，一人の感染ホストが生み出す二次ホスト数を表すとされ，一般にR_0 と表記される. 式(1)において, 脆弱状態のホスト数の時刻 $t=0$ における初期値を $S(0)$ とする．ここで，少数のホストが感染したとすると，流行初期において以下の線形化方程式が成り立つ．

$$\frac{dI(t)}{dt} = (\alpha S(0) - \beta)I(t) \qquad (4)$$

これより，$I(t) = I(0)e^{(\alpha S(0)-\beta)t}$ となり，マルサスの法則に従い増減する．式(4)より，$I(t)$ が初期状態に近くにおいて時刻とともに増加するためには，$(\alpha S(0)-\beta)t > 0$ である必要がある．これを変形すると$\alpha S(0)/\beta > 1$ となる．一方，$(\alpha S(0)-\beta)t < 0$ の場合は，$I(t)$ は減少し，$\alpha S(0)/\beta < 1$と変形できる．これより自律進化型ボットネットの感染ダイナミクスにおける基本再生産数 R_0 は

$$R_0 = \frac{\alpha S(0)}{\beta}$$

で表されることがわかる．この R_0 の値が 1 より大きい時にボットネットマルウェアは初期状態において感染拡散し，一方，1 より小さい時はボットネットマルウェアが感染拡散せず，初期状態から自然消滅する．

次に，$R_0 > 1$ の場合に，自律進化型ボットネットがそのまま蔓延し続けるのか，もしくはある段階で消滅するのかを考察する．ここで，$t \to \infty$とした場合に，脆弱状態のホスト数 $S(t)$ と感染状態のホスト数 $I(t)$ がそれぞれ，S および I という定常状態に収束するものとする．このとき，式(1)および(2)より，

$$0 = -\alpha SI + \gamma(I+1)(N-S-I) - \delta S$$
$$0 = \alpha S I - \beta I$$

が成立し，$S=\frac{\beta}{\alpha}$ もしくは $I = 0$ であることがわかる．$x = \alpha S - \gamma N + \gamma S + \gamma$，$y = 4\gamma(\delta S - \gamma N + \gamma S)$ とし，$S=\frac{\beta}{\alpha}$ の場合の I および，$I = 0$ の場合の S を求めると，以下の式が導かれる．

$$(S,I) = \begin{cases} \left(\frac{\beta}{\alpha}, \frac{-x-\sqrt{x^2-y}}{2\gamma}\right), & x^2 - y \geq 0 \text{ のとき} \\ \left(\frac{\gamma N}{\gamma+\delta}, 0\right), & \text{その他} \end{cases} \qquad (5)$$

（３）評価

式(1)-(3)に基づいた数値計算により，自律進化型ボットネットの感染拡散の振る舞いを調べる．以下では，MATLAB を用いて数値計算を行った結果を示す．まず，基本再生産数によって，自律進化型ボットネットが初期状態から拡散，もしくは消滅に向かうことを確認する．式(1)-(3)における各種パラメータは$\alpha = 0.0001$，$\beta = 0.1$，$\gamma = 0.2$，$\delta = 0.05$とする．

図 2 に $R_0 = 0.5$ の場合の経過日数 t に対する感染ホスト数 $I(t)$ を示す．なお，このときの初期状態は $\big(S(0), I(0), R(0)\big) = (500,1,0)$ であり，$R_0 = (0.0001 \times 500)/0.1 = 0.5$ となる．図より，初期状態から感染ホスト数 $S(t)$ が増加せずに消滅に向かうことがわかる．つまり，脆弱性の発見能力に関わらず，感染率 α，除去率 β，初期状態での脆弱ホスト数 $S(0)$ により決定される R_0 が 1 より小さい場合に，初期状態の広がりは抑制されるといえる．図 3 に，$R_0 = 2$ の場合の経過日数 t に対する感染ホスト数 $I(t)$ を示す．このときの初期状態は $\big(S(0), I(0), R(0)\big) = (2{,}000,1,0)$ であり，$R_0 = (0.0001 \times 2{,}000)/0.1 = 2.0$ である．図より，初期状態から感染ホスト数が爆発的に増加し，おおよそ 1,000 台から増加も減少もしなくなっていることがわかる．

次に，数値計算により，感染拡散後の挙動の確認を行う．ここで，総ホスト数を 10,000 台，各種パラメータを $\alpha = 0.0001$，$\beta = 0.2$，$\delta = 0.05$ とする．初期状態を $\big(S(0), I(0), R(0)\big) = (9{,}999, 1, 0)$ とし，このときの基本再生産数は $R_0 \approx 5.0$ である．つまり，初期状態から感染ホスト数が増加していく状況を想定している．上記パラメータを与えた場合に，$I \geq 0$ となるためには，式(5)において，$\gamma \geq 4.0983 \times 10^{-5}$ である必要がある．図 4 に，$\gamma = 4.0 \times 10^{-5}$ のときの，経過時間 t に対する脆弱ホスト数，感染ホスト数，保護ホスト数の推移を示す．このとき，$\gamma < 4.0983 \times 10^{-5}$ であるため，感染ホスト数は一時的に増加するが，時間とともに減少し，最終的に 0 となることがわかる．また，ほとんどのホストが保護状態に遷移していることから，ボットネットマルウェアの流行は終息に向かうことが確認できる．図 5 に，$\gamma = 4.1 \times 10^{-5}$ のときの，経過時間 t に対する脆弱ホスト数，感染ホスト数，保護ホスト数の推移を示す．このとき，$\gamma > 4.0983 \times 10^{-5}$ であるため，感染ホスト数は一定の値に収束する．また，式(5)により，$(S, I, R) = (2{,}000, 1{,}636, 6{,}365)$と計算でき，図と一致することがわかる．つまり，ボットネットマルウェアの流行は終息に向かわず，常に感染ホストが存在し続けることがわかる．これらの結果により，自律進化型ボットネットに対抗していくためには，脆弱性検出率 γ を少しでも抑制することが重要となる．

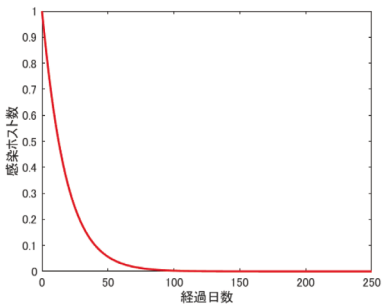


図 2　$R_0 = 0.5$ の場合

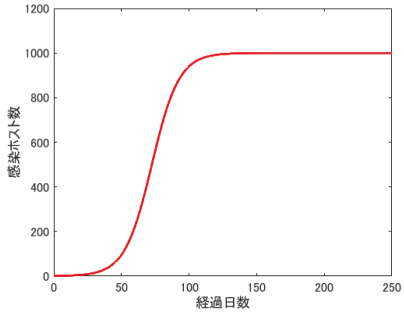


図 3　$R_0 = 2$の場合

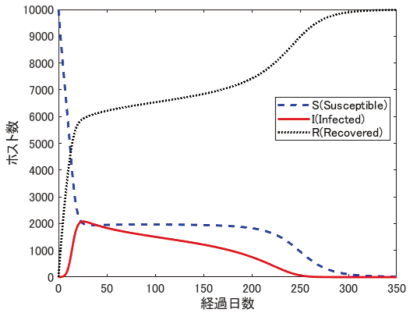


図 4　$\gamma = 4.0 \times 10^{-5}$ の場合

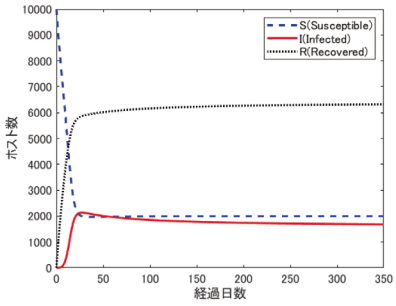


図 5　$\gamma = 4.1 \times 10^{-5}$の場合

3-2 ボランティアモデルによる感染対策

（1）ボランティアモデルの感染ダイナミクス

自律進化型ボットネットへの対抗手段として，脆弱性の発見を抑制することが考えられる．そこで本研究では，ボランティアのホスト群の計算資源を用いた分散機械学習により未知の脆弱性を自律進化型ボットネットよりも先に発見し，それを修復するボランティアモデルの提案を行う．本稿では以下の想定のもと，ボランティアモデルの決定論的モデル化を行う．

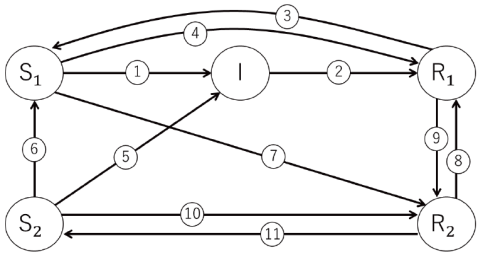


図 6　ボランティアモデル

1)　対象となるネットワーク内に，ボランティアグループが一つ存在する．

2)　脆弱状態もしくは保護状態のホストはボランティアホストになることが可能であり，ボランティアグループ内のホスト数が多いほど，ボランティアホストになりやすい．

3)　ボランティアグループは，脆弱性発見の情報をネットワーク内の全ホストに提供し，脆弱性を保護することが可能である．

4)　ボランティアホストは，グループから自由に抜け出すことが可能である．

図 6 に，これらを想定したボランティアモデルにおける各ホストの状態遷移を示す．図において，S_1 および S_2 はホストに既知の脆弱性がある状態（脆弱状態），I はホストが感染している状態（感染状態），R_1 および R_2 はホストに既知の脆弱性が無い状態（保護状態）であることを示す．また，S_1 および R_1 はホストがボランティアグループに属していないことを，S_2 および R_2 はホストがボランティアグループに属していることを表す．各ホストは以下のイベントに従い状態遷移する．

a)　脆弱状態のホストが感染する．(1，5)．

b)　感染状態のホストからマルウェアが取り除かれる（2)．

c)　脆弱状態のホストから脆弱性が除去される（4，10)．

d)　ボランティアグループから離脱する．(6，8)．

e)　ボランティアグループに参加する（7，9)．

f)　自律進化型ボットネットが脆弱性を発見する（3，11)．

ここで，時刻 t において脆弱状態 S_1 および S_2 にあるホスト数をそれぞれ $S_1(t)$ および $S_2(t)$，感染状態 I にあるホスト数を $I(t)$，保護状態 R_1 および R_2 にあるホスト数をそれぞれ $R_1(t)$ および $R_2(t)$ とする．このとき，各状態間の時間当たりの変化量は以下の常微分方程式系によって表される．

$$\frac{dS_1(t)}{dt} = -\alpha_1 S_1(t) I(t) + \frac{\gamma^2 I(t)^2 R_1(t)}{\psi\big(S_2(t) + R_2(t)\big) + \gamma I(t)} + \theta S_2(t) - \delta_1 S_1(t) - \epsilon S_1(t)(S_2(t) + R_2(t) + 1)$$

$$\frac{dS_2(t)}{dt} = -\alpha_2 S_2(t) I(t) + \frac{\gamma^2 I(t)^2 R_2(t)}{\psi\big(S_2(t) + R_2(t)\big) + \gamma I(t)} - \theta S_2(t) - \delta_2 S_2(t) R_2(t)$$

$$\frac{dI(t)}{dt} = \alpha_1 S_1(t)I(t) + \alpha_2 S_2(t)I(t) - \beta I(t)$$

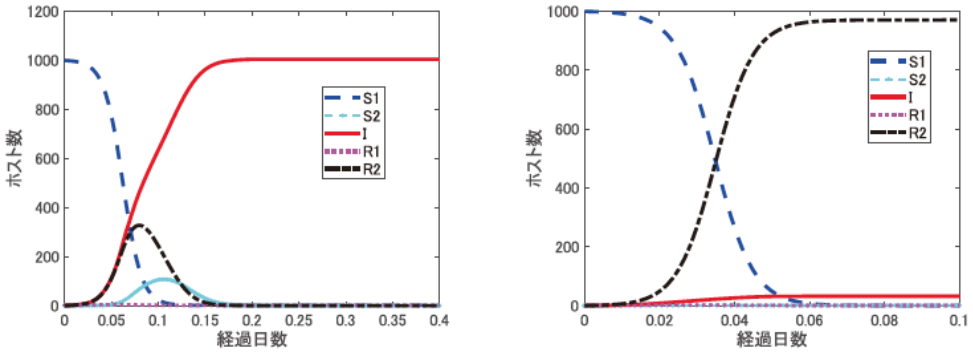
$$\frac{dR_1(t)}{dt} = \delta_1 S_1(t) - \frac{\gamma^2 I(t)^2 R_1(t)}{\psi\big(S_2(t)+R_2(t)\big)+\gamma I(t)} + \beta I(t) - \mu R_1(t)(S_2(t)+R_2(t)+1) + \lambda R_2(t)$$

$$\frac{dR_2(t)}{dt} = \delta_2 S_2(t)R_2(t) - \frac{\gamma^2 I(t)^2 R_2(t)}{\psi\big(S_2(t)+R_2(t)\big)+\gamma I(t)} - \lambda R_2(t) + \mu R_1(t)(S_2(t)+R_2(t)+1)R_2(t)$$
$$+ \epsilon S_1(t)(S_2(t)+R_2(t)+1)$$

ただし，α_1，α_2 はマルウェア感染率，β はマルウェア除去率，γ および ψ はそれぞれ自律進化型ボットネットおよびボランティアグループの脆弱性発見率，δ_1，δ_2 は脆弱性除去率，ϵ，μ はボランティアグループ参加率，θ，λ はボランティアグループ離脱率である．ボランティアモデルでは，自律進化型ボットネットの脆弱性発見能力 $\gamma I(t)$ が，ボランティアグループの脆弱性発見能力 $\psi\big(S_2(t)+R_2(t)\big)$ との比に応じて弱められることを想定している．

（２）評価

ボランティアモデルにおいて，全ホスト数を 1000 台としたときに，マルウェアが 1 台のホストからどのように拡散，消滅するかを調べる．システムの初期状態を $\big(S_1(0), S_2(0), I(0), R_1(0), R_2(0)\big) = (999,0,1,0,0)$ とする．また，$\alpha_1 = \alpha_2 = \beta = \gamma = \delta_1 = \delta_2 = \psi = \theta = \lambda = 0.1$ とする．図 7(a)および(b)にそれぞれ，ボランティアグループへの参加率が $\epsilon = \mu = 0.1$ および $\epsilon = \mu = 0.198$ のときの，経過時間に対する各状態のホスト数を示す．図 7(a)より，ボランティアグループへの参加率が低い場合は，初期段階においてボランティアグループに属するホスト数が少し増加するが，短時間でほとんどのホストがマルウェアに感染してしまうことがわかる．一方，図 7(b)より，ボランティアグループへの参加率が高い場合は，ボランティアグループに属するホスト数が効果的に増加し，その結果，マルウェアの感染拡散を抑制できていることがわかる．ボランティアモデルの課題としては，どのように各ホストにボランティアグループへ参加することを促すかということをゲーム理論等を使用して考察する必要がある．



(a) $\epsilon = \mu = 0.1$　　(b) $\epsilon = \mu = 0.198$

図 7　各状態のホスト数

4 確率論モデルによるアプローチ

4-1 ゲーム理論を用いたマルウェア感染拡散モデルの考察

（１）FLIPIT ゲームの適用

本研究では，自律進化型ボットネットの感染モデルのより詳細に考察するために，ゲーム理論の適用を行う．自律進化型ボットネットの感染モデルにおいては，ボットネットを使用してホストに攻撃を行うプレイヤを攻撃者，その脅威からホストを防御するプレイヤを防御者と考えることができる．ゲーム理論を用いる

ことで，相手がどのような意思決定をするか，その時自分自身がどのような意思決定，戦略を取るべきかを考察できる．また，その意思決定をした場合の利得はどのようになるかを分析でき，マルウェア感染を抑制できる可能性のある防御側の意思決定を見ることができる．本研究では，攻撃者，防御者に加え共有リソースを各ホストとし，共有リソースを奪い合う非協力，完備情報の 2 人戦略形ゲームを考える．このような共有リソースを奪い会う状況は FLIPIT ゲーム[9]と呼ばれるゲーム理論の枠組みを適用し分析することができる．

実際のマルウェア感染では，人間同士の繋がりや，よく見る WEB ページ，接続しているネットワーク環境といったように，マルウェアの感染のしやすさはホスト同士の接続関係に依存すると考えられる．このような接続関係を表現するために，ホストで構成されるオーバーレイネットワークを想定する．これは，感染ホストはオーバーレイネットワーク上の隣接ホストのみを感染させることができ，その他のホストを感染させることはできないというものである．そのうえで，シミュレーション実験により得られたデータを用いて，利得や挙動を分析することで，ボットネットマルウェア感染の拡大を抑制できる可能性のある防御側の意思決定を推測する．

FLIPIT ゲームは，2 人のプレイヤが共有リソースの完全制御を獲得するために競い合い，利得は共有リソースが自分の制御下にある時間などによって定義される．共有リソースを奪い合う状況を各ホストにおいて想定し，その時の各プレイヤの平均制御時間（各プレイヤがリソースを自身の制御下においた時間），FLIP が行われた（共有リソースを奪取した）回数により利得を算出する．ここで，プレイヤ 1 はマルウェア感染，脆弱性発見を行うことで各ホストを感染の脅威に晒し，プレイヤ 2 は脆弱性除去，マルウェア除去を行うことで各ホストをマルウェアなどの脅威から防御することを考えることから，プレイヤは SIRS モデルにおける各遷移に従い FLIP を行うものとする．つまり，本稿の FLIPIT ゲームでは攻撃者の戦略を脆弱性発見率 γ とマルウェア感染率 α の組で，防御者の戦略を保護率 δ とマルウェア除去率 β の組で表す．

ここで，ホスト数を N，ホスト集合を $\mathcal{N} = \{1,2,\dots,N\}$，プレイヤの集合 $\mathcal{I} = \{1,2\}$ とする．時刻 $t = 0$ からゲームが開始したとして，時刻 t までの各プレイヤの利得 $B_i(t)$ は，

$$B_i(t) = G_i(t) - C_i(t)$$

で与えられる．ただし，$G_i(t)$ は時刻 t までのプレイヤ i の獲得ポイントであり，$C_i(t)$ は時刻 t までにプレイヤ i が支払ったコストである．ホスト j における時刻 t までのプレイヤ i の制御時間の総和を $A_i^j(t)$ とすると，獲得ポイント $G_i(t)$ は以下の式で表すことができる．

$$G_i(t) = \frac{1}{N}\sum_{j=1}^{N} A_i^j(t) \times n_i$$

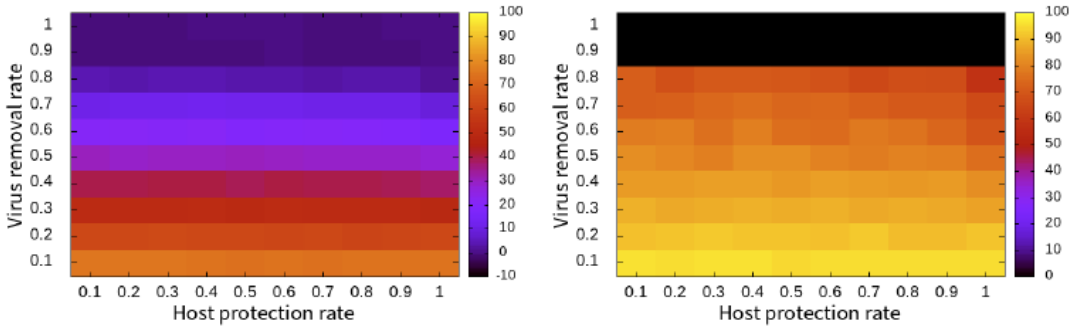
ただし，n_i はプレイヤ i が共有リソースを制御している場合に，単位時間あたりに獲得できるポイントを表す．また，プレイヤ 1（攻撃者）の支払いコスト $C_1(t)$ を

$$C_1(t) = T_\alpha(t)C_\alpha + T_\eta(t)C_\eta \frac{1}{I(t)+1}$$

で定義する．ここで $T_\alpha(t)$ は時刻 t までに攻撃者がボットネットマルウェアをホストに感染させた回数，$T_\eta(t)$ は時刻 t までに攻撃者が脆弱性を発見した回数を表す．また，C_α および C_η はそれぞれ，マルウェア感染および脆弱性発見あたりに攻撃者が支払う必要のあるコストである．また，$I(t)$ は時刻 t における感染ホスト数を表す．一方，プレイヤ 2（防御者）の支払いコスト $C_2(t)$を

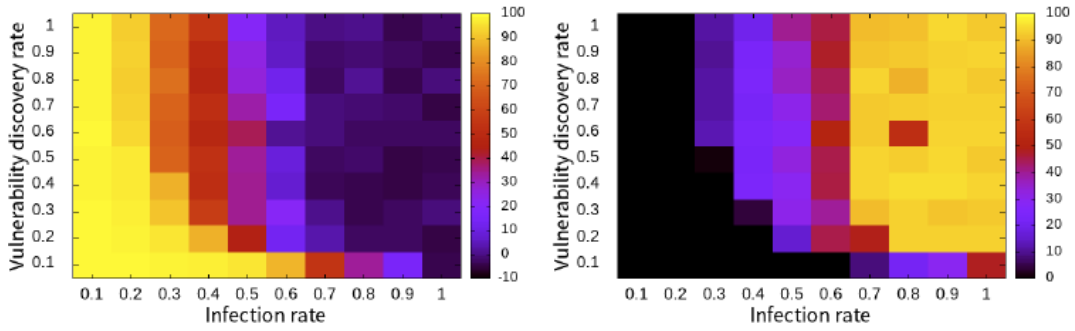
$$C_2(t) = T_{\delta_S}(t)C_{\delta_S} + T_{\delta_I}(t)C_{\delta_I}$$

と定義する．ここで，$T_{\delta_S}(t)$ は時刻 t までに防御者がホストの脆弱性を除去した回数を，$T_{\delta_I}(t)$ は時刻 t までに防御者がボットネットマルウェアをホストから除去した回数である．また，C_{δ_S} および C_{δ_I} はそれぞれ，脆弱性除去およびマルウェア除去あたりに防御者が支払う必要のあるコストを表す．



(a) 利得　　(b) 感染ホスト数

図 8　攻撃者の最適応答戦略



(a) 利得　　(b) 感染ホスト数

図 9　防御者の最適応答戦略

（２）評価

本研究では，シミュレーション実験により，自律進化型ボットネットの感染モデルに FLIPIT ゲームを適用し攻撃者および防御者の最適応答戦略や利得の考察を行う．ホストで構成されるオーバーレイネットワークとして，スモールワールド性とスケールフリー性の性質を持つ Barabasi-Albert モデル[10]に基づき作成した，全ホストを 100 台，平均次数 4 のネットワークを用いる．システムの初期状態を $\big(S(t),I(t),R(t)\big)=(99,1,0)$ とし，$n_1=n_2=1$，$C_\alpha=C_\eta=C_{\delta_I}=C_{\delta_S}=1$ として FLIPIT ゲームを適用する．

図 8(a)および(b)にそれぞれ，時刻 $t=100$ のときの保護率およびマルウェア除去率に対する，攻撃者の最適応答戦略時の利得および平均感染ホスト数を示す．同様に，図 9(a)および(b)にそれぞれ，時刻 $t=100$ のときの脆弱性発見率およびマルウェア感染率に対する，防御者の最適応答戦略時の利得および平均感染ホスト数を示す．図 8 より，マルウェア除去率の増加により，攻撃者の利得と感染ホスト数が減少することがわかる．一方，これらの値は保護率の変化に対してほとんど変動しない．図 9 より，防御者の利得と感染ホスト数は，マルウェア感染率および脆弱性発見率が増加することで高くなる．これらの結果には 2 つのナッシュ均衡点が存在する．一つ目は戦略 $\big((\alpha,\beta),(\gamma,\delta)\big)=\big((0.2,0.1),(1.0,0.9)\big)$ のときで，このとき攻撃者の利得は−0.336，防御者の利得は 98.765 である．二つ目は戦略 $\big((\alpha,\beta),(\gamma,\delta)\big)=\big((0.1,0.1),(1.0,1.0)\big)$ のときで，このときの攻撃者の利得は−0.135，防御者の利得は 98.923 である．

4-2 機械学習を用いたマルウェアの感染拡散予測

（１）データセットの作成

確率論的モデルに従う計算機シミュレーション実験によるマルウェア感染拡散解析では，ネットワークの規模が大きくなるほど，計算時間が大幅に増加する問題がある．そこでこの問題を解決するために，ネットワーク構造の情報を画像化し，畳み込みニューラルネットワーク(Convolutional Neural Network: CNN)を用いることで簡易的にマルウェアの感染拡散度合いを予測する手法を提案する．本手法では，規模の小さいネットワーク構造を用いた計算機シミュレーション実験の結果により CNN の学習を行い，それをもとに規模

の大きいネットワークの識別を行う．規模の大きいネットワークを画像化する際には，ネットワーク構造の情報を失わずに画像をリサイズし，学習データのサイズに合わせる．このようにすることで，小規模ネットワーク構造の情報から異なるネットワーク規模におけるマルウェアの感染拡散度合いを効率的に予測することが出来る．

提案予測手法では，オーバーレイネットワークを重み付き隣接行列で表現する．オーバーレイネットワークの構造を表す行列を $\boldsymbol{A}$ とする時，行列の要素は $a_{i,j}$ $(i,j = 1,2,\ldots,N)$ となる．$\boldsymbol{A}$ はホスト数が N の時，$N \times N$ の正方行列である．i 行目の各要素は，ホスト i と他の全てのホストとの接続状況を示している．ここで，各ホスト間の繋がりの強さを考慮するために，$a_{i,j}$ の値として，各ホスト間の感染率 $\alpha_{i,j}$ を用いる．

この重み付き隣接行列を用いて CNN の入力用の $N \times N$ サイズのグレースケール画像を作成する．具体的には，$a_{i,j}$ を 0 から 255 の値に正規化したうえで，行列の各要素が各ピクセルに対応するようにグレースケール画像を作成する．各要素は，繋がりが強いほど 255 に近くなり，繋がりが弱いほど 0 に近くなる．なおグレースケール画像の場合，行列の各要素は 255 に近いほど白く，0 に近いほど黒くなる．ただし，この CNN を用いた感染拡散予測法では，入力画像のサイズが，ネットワーク規模（ノード数）に依存する．通常 CNN では，画像を入力する際にバイリニア補間法というリサイズ方法により自動的にサイズの調整が行われる．その場合，ネットワーク構造の情報が失われる恐れがあり，予測精度の低下につながると考えられる．そのため，異なるネットワーク規模のマルウェア生存率を予測する場合は，画像のリサイズ方法を考慮しなければならない．そこで提案手法では，ネットワークの接続関係を維持しながら，画像の縮小を行い，それをテストデータとすることで，予測精度の向上を狙う．以下に，提案手法における画像の縮小手順について説明する．

i) 各ホストに対し，隣接ノードの感染率の合計を算出し，ネットワーク内で最も感染率の合計が小さいホストを選択する．
ii) i)で選択されたホストに接続しているホストの中で，最も感染率の合計が小さいホストを選択する．
iii) i)で選択されたホストが接続している各ホストを ii)で選択されたホストに接続する．
iv) i)で選択されたホストを削除する．
v) 目標値まで i)から iv)を繰り返す．

（２）評価

学習済み CNN を用いた評価実験により，提案手法の感染拡散予測性能を評価する．本稿では，学習データおよびテストデータとして，平均次数が 4，6，8，10 のオーバーレイネットワークの結果を用いる．各ホスト間の感染率 $\alpha_{i,j}$ は 0 から 1 の間でランダムに与える．また，学習データの画像のサイズを100×100ピクセル（ホスト数 100）とし，19,200 枚の学習データセットを用意する．テスト画像は各ピクセルのものをそれぞれ 4,800 枚ずつ用意し，画像のサイズを統一するために，ホスト数が 200 および 300 の画像は100×100ピクセルの画像に縮小する．また，画像の縮小方法の比較として，画像の拡大縮小に用いられる事が多いバイリニア補間法を用いる．

表 1 に提案手法で示した画像縮小法と既存の画像縮小法とを比較したテストデータの識別結果を示す．この識別結果とは，計算機シミュレーション実験により算出されたマルウェアの感染度合いと，CNN により予測されたマルウェアの感染度合いの差の絶対値を示している．そのため，値が小さいほど計算機シミュレーション実験により求められた結果と CNN により求められた結果に誤差がなく，正確に予測できているといえる．この結果より，既存の画像縮小法より，提案手法を用いた場合の方が平均絶対誤差が小さく，より正確に予測できていることが確認できる．

表 1　識別結果

ホスト数	100	200		300	
縮小方法	×	①	②	①	②
平均絶対誤差	0.090	0.143	0.236	0.144	0.238
標準偏差	0.109	0.174	0.277	0.183	0.307

①提案手法　　②バイリニア補間法

5 まとめ

本研究では，将来の情報通信社会の脅威となりうる自律進化型ボットネットに対抗するための，アンチマルウェアシステムモデルの構築を行った．まず決定論的モデル化により，自律進化型ボットネットの感染ダイナミクスを表し，どのような条件において感染が拡大するのかを明らかにした．さらに，未感染のコンピュータを利用して分散機械学習を行い，自律進化型ボットネットよりも先に未知の脆弱性を発見することであらかじめ感染を防ぐ，ボランティアモデルを提案した．次に，確率論的モデル化により，より詳細な感染抑制の考察を行った．まず，確率論的感染モデルにゲーム理論の適用を検討し，マルウェア感染を抑制できる可能性のある防御側の意思決定を確認した．さらに，ホスト間の繋がりで構成されるネットワークを考慮した CNN を用いた感染拡散予測法を提案した．本研究では，数値実験およびシミュレーション実験により，これらの提案手法の有効性を示した．

【参考文献】

[1] T. Kudo, T. Kimura, Y. Inoue, H. Aman, and K. Hirata, “Stochastic modeling of self-evolving botnets with vulnerability discovery,” *Computer Communications*, vol. 124, pp. 101-110, 2018.

[2] J. Gu, Z. Wang, J. Kuen, L. Ma, A. Shahroudy, and B. Shuai, “Recent advances in convolutional neural networks,” arXiv preprint arXiv:1512.07108, 2015.

[3] J. Borello and L. Me, “Code obfuscation techniques for metamorphic viruses,” *Journal in Computer Virology*, vol. 4, no. 3, pp. 211-220, 2008.

[4] A. Cani, M. Gaudesi, E. Sanchez, G. Squillero, and A. Tonda, “Towards automated malware creation: code generation and code integration,” in *Proc. Symposium on Applied Computing*, Mar. 2014.

[5] S. Noreen, S. Murtaza, M. Z. Shafiq, and M. Farooq, “Evolvable Malware,” in *Proc. Genetic and Evolutionary Computation Conference*, Jul. 2009.

[6] R. Scandariato, J. Walden, A. Hovsepyan, and W. Joosen, “Predicting vulnerable software components via text mining,” *IEEE Transactions on Software Engineering*, vol. 40, no. 10, pp. 993-1006, 2014.

[7] F. Yamaguchi, F. Lindner, and K. Rieck, “Vulnerability extrapolation: assisted discovery of vulnerabilities using machine learning,” in *Proc. USENIX conference on Offensive Technologies*, Aug. 2011.

[8] J. Dean et al., “Large scale distributed deep networks,” in *Proc. Neural Information Processing Systems*, Dec. 2012.

[9] M. Dijk, A. Juels, and A. Oprea, “FLIPIT: The Game of “Stealthy Takeover”,” *Journal of Cryptology*, vol. 26, no. 4, pp. 655–713, 2013.

[10] A. Barabasi and R. Albert, “Emergence of scaling in random networks,” *Science*, vol. 286, pp.509–512, 1999.

〈発　表　資　料〉

題　　名	掲載誌・学会名等	発表年月
決定論的モデルによる将来のマルウェア進化に対する感染対策の評価	電子情報通信学会コミュニケーションクオリティ研究会	2019 年 7 月
将来のマルウェア進化に対する感染対策モデルの検討	超知性ネットワーキングに関する分野横断型研究会	2019 年 11 月
FLIPIT ゲームを用いたマルウェア感染拡散モデルの考察	電子情報通信学会ネットワークシステム研究会	2020 年 3 月
数理モデルによる将来のボットネット感染ダイナミクスの考察	電子情報通信学会ネットワークシステム研究会	2020 年 3 月

ネットワーク規模を考慮したマルウェアの感染拡散予測法	電子情報通信学会ネットワークシステム研究会	2020 年 3 月
Consideration of a countermeasure model against self-evolving botnets	International Conference on Evolving Internet (INTERNET 2019)	2019 年 6 月
Evaluation of countermeasure against future malware evolution with deterministic modeling	Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC 2019)	2019 年 11 月