

# 進化ゲーム理論に基づくマルウェア感染拡散対策モデルの検討

三浦 秀芳<sup>†</sup> 平田 孝志<sup>††</sup>

<sup>†</sup> 関西大学 大学院理工学研究科 システム理工学専攻 〒564-8680 大阪府吹田市山手町 3-3-35

<sup>††</sup> 関西大学 システム理工学部 電気電子情報工学科 〒564-8680 大阪府吹田市山手町 3-3-35

E-mail: <sup>†</sup>{k846996, hirata}@kansai-u.ac.jp

**あらまし** 感染ホストの計算資源を利用した分散機械学習によりホストの脆弱性を発見し、その脆弱性を用いた攻撃によりホストを感染させることで自律的に進化する自律進化型ボットネットの概念が提唱されている。本稿では、そのような新たなボットネットマルウェアの感染拡散に対抗するための感染対策モデルの提案を行う。提案モデルでは、対策ホストで構成される対策グループが、それら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ボットネットマルウェアよりも先に発見し、脆弱なホストを保護することを想定する。本稿では提案モデルにおいて、対策グループを構成するホスト数や脆弱、感染、保護といった各状態におけるホスト数の変化を進化ゲーム理論に基づく常微分方程式を用いて表現する。また、数値計算によりその感染ダイナミクスを明らかにする。

**キーワード** マルウェア, 感染モデル, 感染ダイナミクス, 感染対策モデル, 進化ゲーム理論

## Countermeasure model against malware spreading with an evolutionary game theory

Hideyoshi MIURA<sup>†</sup> and Kouji HIRATA<sup>††</sup>

<sup>†</sup> Graduate School of Science and Engineering, Kansai University, Suita 564-8680, Japan

<sup>††</sup> Faculty of Engineering Science, Kansai University, Suita 564-8680, Japan

E-mail: <sup>†</sup>{k846996, hirata}@kansai-u.ac.jp

**Abstract** The literature has suggested the appearance of self-evolving botnets that discover vulnerabilities of hosts by performing distributed machine learning using the computational resources of infected zombie computers. The self-evolving botnets are incomparably more powerful than existing botnets. In this paper, we propose a countermeasure model against the spread of the self-evolving botnets. In the proposed model, a countermeasure group consisting of countermeasure hosts discovers new vulnerabilities prior to the botnets by performing distributed machine learning using their computational resources. By doing so, they can protect non-infected hosts. In this paper, the average number of hosts that join and leave the countermeasure group, and the time variation of the number of hosts in respective states are represented by ordinary differential equations based on an evolutionary game theory. In addition, we clarify the dynamics by numerical calculations.

**Key words** Malware, epidemic model, infection dynamics, countermeasure model, evolutionary game theory