社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE.

劣通信環境におけるモビリティを考慮したマルウェア感染拡散モデルの考察

三浦　秀芳† 　虻川　翔哉† 　木村　共孝†† 　平田　孝志†††

† 関西大学大学院 理工学研究科　〒564–8680 大阪府吹田市山手町 3–3–35
†† 同志社大学 理工学部　〒610–0321 京都府京田辺市多々羅都谷 1–3
††† 関西大学 システム理工学部　〒564–8680 大阪府吹田市山手町 3–3–35
E-mail: †{k846996,k507593,hirata}@kansai-u.ac.jp, ††tomkimur@email.doshisha.ac.jp

あらまし　本稿では，劣通信環境におけるモバイル端末の移動性を考慮したマルウェア感染拡散モデルを提案する．近年，スマートフォン等のモバイル端末に感染するマルウェアが出現している．さらに，モバイル端末の Bluetooth 接続を悪用した攻撃が深刻な問題となっている．このような背景のもと，本稿では，劣通信環境上のモバイル端末を伝播する新たなマルウェアの挙動を明らかにするための感染モデルを提案する．提案モデルでは，感染症数理モデルである SIR モデルに基づき，マルウェアの感染ダイナミクスをエリア内のホストの移動を考慮した微分方程式で表現する．本稿では，微分方程式に基づく数値計算が，シミュレーション実験で得られた結果と近似することを示す．
キーワード　劣通信環境，マルウェア，SIR モデル

Modeling of malware diffusion with mobile devices in intermittently connected networks

Hideyoshi MIURA†, Syoya ABUKAWA†, Tomotaka KIMURA††, and Kouji HIRATA†††

† Graduate School of Science and Engineering, Kansai University　3–3–35 Yamate-Suita, Osaka, 564–8680 Japan
†† Faculty of Science and Engineering, Doshisha University, 1–3, Kyotanabe, Kyoto, 610–0321, Japan
††† Faculty of Engineering Science, Kansai University　3–3–35 Yamate-Suita, Osaka, 564–8680 Japan
E-mail: †{k846996,k507593,hirata}@kansai-u.ac.jp, ††tomkimur@email.doshisha.ac.jp

Abstract　In this paper, we introduce an epidemic model of malware with mobile devices in intermittently connected networks. In recent years, malware that infects mobile devices such as smartphones has emerged. Furthermore, attacks exploiting Bluetooth connections of smartphones have become serious issues. Based on these facts, in this paper, we aim to reveal the infection dynamics of new malware propagating on mobile devices in intermittently connected networks, with the epidemic model. The epidemic model represents the dynamics of malware diffusion with ordinary differential equations, considering node mobility. Through numerical calculations, we show that our proposed epidemic model well approximates results obtained from simulation experiments.
Key words　intermittently connected networks, malware, SIR model

1. はじめに

近年，コンピュータウイルスやワーム，トロイの木馬といったマルウェアによるサイバー攻撃が深刻な脅威となっている [3], [7]．これらのサイバー攻撃の標的は，従来のデスクトップ PC やノート PC だけでなく，タブレット端末やスマートフォン等のモバイル端末にも及んでいる．モバイル端末へのサイバー攻撃としては，Bluetooth 接続の脆弱性を悪用した BlueBorne [5] などが存在する．また，文献 [2] では，モバイル端末間を広がる Bluetooth ワームの感染挙動を表す感染モデルを提案し，シミュレーション実験によりその感染ダイナミクスを分析している．このような感染モデルを用いることで，マルウェアの感染ダイナミクスを理解し，様々なシナリオや感染率等のパラメータの影響を分析することができる．

マルウェアの感染ダイナミクスを表す感染モデルは，決定論的モデルと確率論的モデルに分類することができる．決定論的モデルは，マルウェアの感染ダイナミクスを微分方程式で表現し，数値計算によりその特性を明らかにするものである [6]．決

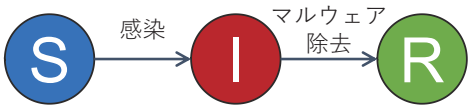


図 1: SIR モデル

定論的モデルでは，短時間で平均感染ホスト数の変化等の平均的な特性を取得することができる．一方，確率論的モデルはマルウェアの感染ダイナミクスを，感染モデルに基づく確率論的シミュレーション実験やマルコフ解析等により表現する方法である．確率的に発生するランダムな事象を観測することが可能であり，より詳細にマルウェア感染の挙動を分析することができる．文献 [2] の感染モデルは確率論的モデルの一種である．

本稿では，劣通信環境下において，モバイル端末間で感染拡散を行う新たなマルウェアに対する決定論的感染モデルの提案を行う．劣通信環境下では，エリア内を自由に移動できるモバイル端末がエリアのサイズに比べて少ない数で存在する．このとき，距離的に近いモバイル端末同士のみが通信を行えるため，ネットワークの接続性は確保されていない．さらに，モバイル端末は移動するため，移動に伴いモバイル端末間の接続は断続的に確立される．また，Bluetooth ワーム等のマルウェアは，近くに存在するモバイル端末を攻撃し感染を広げる．劣通信環境において広がるマルウェアの挙動分析は，モバイル端末の移動やモバイル端末間の接続性を考慮しなければならないことから，文献 [2] に示すような確率論的モデルに基づくシミュレーション実験が一般的である．しかし，確率論的モデルでは，平均的な特性を得るためにはシミュレーション実験を複数回繰り返す必要があり，想定するネットワークの規模やホスト数が増加する場合，計算時間が膨大となる．

本稿で提案する決定論的感染モデルでは，劣通信環境下でのマルウェア拡散の挙動を，ネットワークの構造やホストの移動性を考慮した微分方程式で表現する．提案手法における微分方程式に基づく数値計算が，短時間でシミュレーション実験の結果に近似できることを示す．

2. 劣通信環境におけるマルウェア感染モデル

提案モデルは，伝染病の伝播を表現する疫学モデルである SIR モデルに基づいている．一般的な SIR モデルは，ネットワークの構造やホストの移動性を考慮しておらず，各状態に存在するホスト数の割合のみに着目している．本稿では SIR モデルを拡張し，劣通信環境におけるホストの移動性とグリッド構造を考慮したマルウェア感染モデルを提案する．そこで，はじめに SIR モデルについて簡単に説明し，その後 SIR モデルを拡張した提案モデルの説明を行う．

2.1 SIR モデル

ネットワーク上に一種類のマルウェアと K 台のホストが存在すると仮定する．SIR モデルでは，図 1 に示すように，ネットワーク上の各ホストは脆弱状態（S），感染状態（I），回復状態（R）のいずれかの状態となる．状態 S，状態 I，状態 R はそれぞれ，ホストに脆弱性がありマルウェアに感染する可能性があること，マルウェアに感染していること，マルウェアが除去され以降感染しないことを表す．各状態間の遷移は以下のイベントに従う．

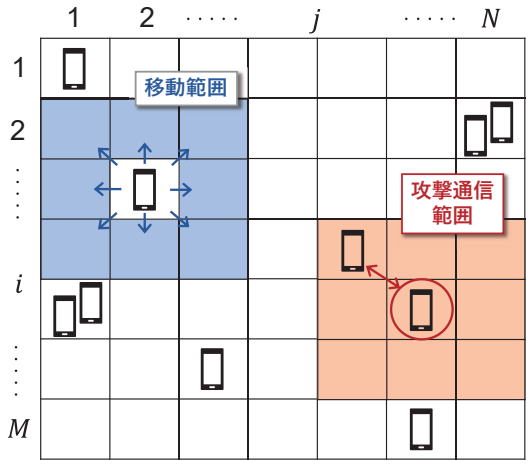


図 2: システムモデル

（1） 感染したホストとの接触により，脆弱性が存在するホストがマルウェアに感染し，状態 I に遷移する．

（2） 感染したホストは，自身からマルウェアを除去することで状態 R へと遷移する．

ここで，$S(t)$，$I(t)$，$R(t)$ をそれぞれ時刻 t（$t \geqq 0$）における状態 S，I，R に属するホスト数とし，$S(t)+I(t)+R(t)=K$ とすると，以下の常微分方程式によりマルウェアの感染拡散挙動を分析することができる．

$$\frac{d}{dt}S(t) = -\alpha S(t)I(t), \tag{1}$$

$$\frac{d}{dt}I(t) = \alpha S(t)I(t) - \beta I(t), \tag{2}$$

$$\frac{d}{dt}R(t) = -\beta I(t), \tag{3}$$

ただし，α，β はそれぞれ，マルウェア感染率，マルウェア除去率を表す．式 (1)，(2) 中の $\alpha S(t)I(t)$ は，単位時間あたりの平均感染ホスト数，式 (2)，(3) 中の $\beta I(t)$ は，単位時間あたりの平均回復ホスト数を表す．

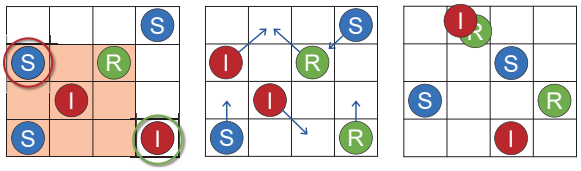
2.2 システムモデル

図 2 に本稿で想定するシステムモデルを示す．図に示すような，$M \times N$ 個のセルで構成される 2 次元空間グリッド $\mathcal{G}$ に K 台のモバイルホストが存在する劣通信環境を考える．ここで，モバイルホストの集合を $\mathcal{H}$ とし，セル $(i,j) \in \mathcal{G}$（$1 \leqq i \leqq M, 1 \leqq j \leqq N, i,j \in \mathbb{N}$）の接触セル $C_{(i,j)}$ を

$$C_{(i,j)} = \{(m,n) \mid |m-i| \leqq 1, |n-j| \leqq 1\}$$

とする．ここで，セル (i,j) は $C_{(i,j)}$ に含まれることに注意する．また，セル $(i,j) \in \mathcal{G}$ の隣接セルを $\mathcal{A}_{(i,j)} = C_{(i,j)} \setminus \{(i,j)\}$ とする．

モバイルホストは離散時間ステップ t_d（$t_d = 0,1,2,\ldots$）でグリッド上を移動する． ここで，$c_h(t_d) = (i,j)$ を時間ステップ t_d



(a) 状態遷移　(b) ホストの移動　(c) 次の状態

図 3: 各ステップにおけるそれぞれのホストの挙動

における ホスト $h \in \mathcal{H}$ の位置（セル）とする．各時間ステップにおいて，各セル $(i,j) \in \mathcal{G}$ 上の各ホストは，隣接セル $\mathcal{A}_{(i,j)}$ のうちの 1 つにランダムに移動する．各セル上の各ホストは，そのホストの通信範囲を表す接触セル $C_{(i,j)}$ 上の他のホストとのみ通信することができる．各ホストの状態遷移は，劣通信環境における SIR モデルに従う．具体的には，各ホストは S，I，R のいずれかの状態に属し，以下の仮定に基づき時間ステップごとに状態遷移する．

（1） 各セル $(i,j) \in \mathcal{G}$ 上の各感染ホストは各時間ステップにおいて，感染確率 α_d で接触セル $C_{(i,j)}$ 上の各脆弱ホストを感染させる．このとき，感染した脆弱ホストは次のステップで感染ホストとなる．

（2） 各感染ホストは各時間ステップにおいて，マルウェア除去確率 β_d で自身からマルウェアを除去する．このとき，感染ホストは次ステップで回復ホストとなる．回復ホストはマルウェアに再び感染することはない．

図 3 に状態遷移の一例を示す．この例では，感染ホストが接触セル上の脆弱ホストと接触することでマルウェアに感染させる（図 3(a)）．さらに，感染ホストが自身のマルウェアを除去する．これらのホストはそれぞれ状態 I と R に遷移する（図 3(b)）．その後，全てのホストが隣接セルのいずれかに移動する（図 3(c)）．この手順は時間ステップごとに行われる．

2.3 提案モデル

システムモデルで示したモバイルホストにおけるマルウェア感染挙動を，SIR モデルに基づく常微分方程式で表現する．ここでは，離散的な時間ステップではなく，連続的な時間環境を想定し，t_d，α_d，β_d はそれぞれ，t，α，β に対応させる．

ここで，$S_{(i,j)}(t)$ を時刻 t におけるセル (i,j) 上の脆弱ホスト数とする．同様に，$I_{(i,j)}(t)$ と $R_{(i,j)}(t)$ をそれぞれ，時刻 t におけるセル (i,j) 上の感染ホスト数，回復ホスト数とする．ただし，$S(t) = \sum_{(i,j)\in\mathcal{G}} S_{(i,j)}(t)$，$I(t) = \sum_{(i,j)\in\mathcal{G}} I_{(i,j)}(t)$，$R(t) = \sum_{(i,j)\in\mathcal{G}} R_{(i,j)}(t)$ である．以上より，各セル上の各ホスト数の変化量は以下の常微分方程式で与えられる．

$$\begin{aligned}\frac{d}{dt}S_{(i,j)}(t) = &-\alpha S_{(i,j)}(t)\left\{\sum_{(m,n)\in C_{(i,j)}} I_{(m,n)}(t)\right\}\\ &-\mu S_{(i,j)}(t)\\ &+\mu\sum_{(m,n)\in\mathcal{A}_{(i,j)}}\frac{1}{|\mathcal{A}_{(m,n)}|}S_{(m,n)}(t),\end{aligned} \tag{4}$$

$$\begin{aligned}\frac{d}{dt}I_{(i,j)}(t) = &\alpha S_{(i,j)}(t)\left\{\sum_{(m,n)\in C_{(i,j)}} I_{(m,n)}(t)\right\}\\ &-\beta I_{(i,j)}(t)-\mu I_{(i,j)}\\ &+\mu\sum_{(m,n)\in\mathcal{A}_{(i,j)}}\frac{1}{|\mathcal{A}_{(m,n)}|}I_{(m,n)}(t),\end{aligned} \tag{5}$$

$$\begin{aligned}\frac{d}{dt}R_{(i,j)}(t) = &\beta I_{(i,j)}(t)-\mu R_{(i,j)}(t)\\ &+\mu\sum_{(m,n)\in\mathcal{A}_{(i,j)}}\frac{1}{|\mathcal{A}_{(m,n)}|}R_{(m,n)}(t),\end{aligned} \tag{6}$$

ここで，μ はホストの移動率を表す．

式（4）において，第 1 項はセル (i,j) 上の脆弱ホストが，接触セル $C_{(i,j)}$ 上に位置する感染ホストとの接触により，マルウェアに感染する可能性があることを表す．第 2 項と第 3 項はそれぞれ，セル (i,j) から隣接セル $\mathcal{A}_{(m,n)}$ へ移動する脆弱ホストと，隣接セル $\mathcal{A}_{(m,n)}$ からセル (i,j) へ移動する脆弱ホストを表す．ここでは，システムモデルにおいて，ホストは時間ステップごとにランダムに隣接セル $\mathcal{A}_{(m,n)}$ に移動することを仮定している．従って第 3 項では，セル (m,n) から移動するホスト数を，(m,n) の隣接セル数 $|\mathcal{A}_{(m,n)}|$ で割ることでそれぞれのセルへの移動ホスト数を表している．同様に，式（5）において，第 1 項は脆弱ホストが感染することを表す．第 2 項は，感染ホストがマルウェアを除去し，回復状態へ遷移することを表す．第 3 項，第 4 項は感染ホストの移動の項を表す．式（6）も同様に，第 1 項は感染状態から回復状態，第 2 項および第 3 項は回復ホストの移動を表す．

3. 評　　価

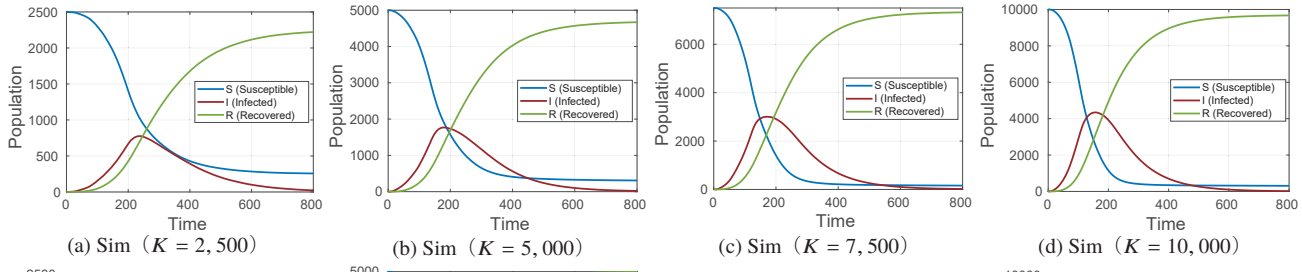
3.1 評価モデル

本章では，提案モデルの挙動を数値計算で検証する．常微分方程式 (4)-(6) の計算には MATLAB [1] を用いる．また，比較のために 2.2 節で説明したシステムモデルに基づく離散時間シミュレーションの結果を示す．これらの数値計算およびシミュレーション実験では，2.10 GHz CPU，16 GB メモリの Intel Xeon Silver 5110 を搭載した DELL Precision 5820 を使用し，OS には Ubuntu20.04 を用いる．

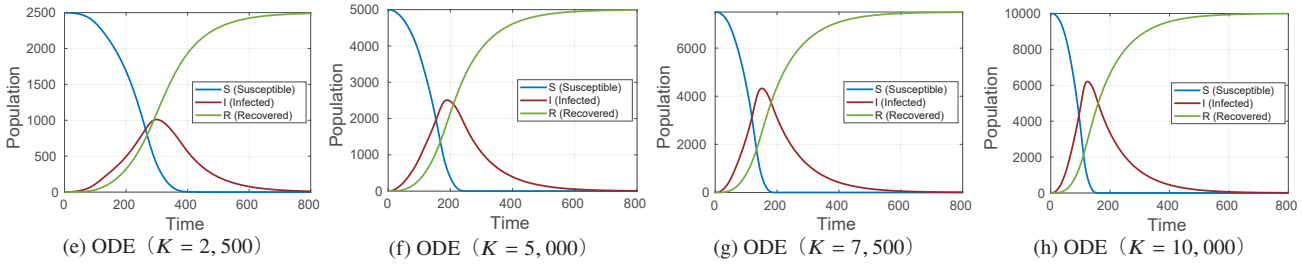
劣通信環境として，100×100（$M = N = 100$）のグリッドを考える．また，初期状態として感染ホストを 1 台，脆弱ホストを $K-1$ とする（$S(0) = K-1$，$I(0) = 1$，$R(0) = 0$）．初期感染ホストはセル $(1,1)$ または $(50,50)$ で実験を行い，脆弱ホストはグリッド上のセルにランダムに配置する．また，パラメータを $\alpha = \alpha_d = 0.05$，$\beta = \beta_d = 0.01$，$\mu = 1$ とする．

3.2 結　　果

図 4 に，初期感染ホストをセル $(1,1)$ 上に配置したときの，経過時間に対する各状態のホスト数を示す．図 4(a)-(d) と図 4(e)-(h) はそれぞれ，K の値を変化させたシミュレーション結果（Sim）と，提案モデルである常微分方程式の数値計算結果（ODE）である．シミュレーション結果は試行回数 100 回の標本平均を示す．これらの図からわかるように，感染ホスト数 $I(t)$ は時間の経過と共に急激に増加する．その後，回復ホスト

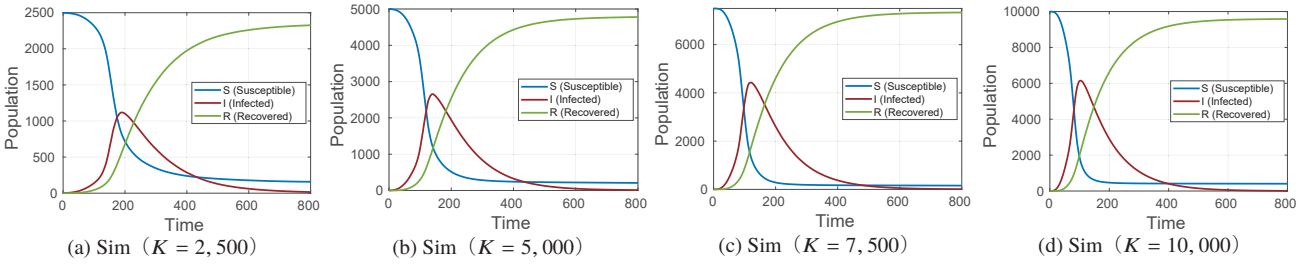


(a) Sim（$K = 2,500$） (b) Sim（$K = 5,000$） (c) Sim（$K = 7,500$） (d) Sim（$K = 10,000$）

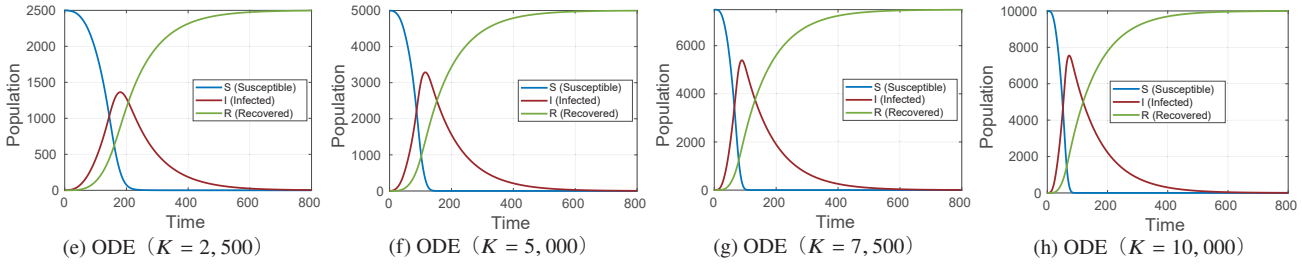


(e) ODE（$K = 2,500$） (f) ODE（$K = 5,000$） (g) ODE（$K = 7,500$） (h) ODE（$K = 10,000$）

図 4: 初期感染ホスト配置 $(1,1)$ のときの，経過時間に対するそれぞれの状態のホスト数



(a) Sim（$K = 2,500$） (b) Sim（$K = 5,000$） (c) Sim（$K = 7,500$） (d) Sim（$K = 10,000$）



(e) ODE（$K = 2,500$） (f) ODE（$K = 5,000$） (g) ODE（$K = 7,500$） (h) ODE（$K = 10,000$）

図 5: 初期感染ホスト配置 $(50,50)$ のときの，経過時間に対するそれぞれの状態のホスト数

はマルウェアに感染しないため感染ホスト数は減少し，最終的に 0 に近い値となる．また，マルウェアの感染速度は，全ホスト数 K に比例して増加することがわかる．これは，感染したホストが脆弱ホストに遭遇する確率が，全ホスト数 K が増加するにつれて高くなるためである．さらに，提案モデルはシミュレーション結果とよく近似していることが確認できる．

図 5 に，初期感染ホストをセル $(50,50)$ 上に配置したときの，経過時間に対する各状態のホスト数を示す．この図から分かるように，図 4 と比較してマルウェアの感染速度が相対的に大きくなっていることがわかる．これは，初期感染ホストがグリッドの中心に位置している場合，マルウェアがグリッド内で容易に拡散できるためである．また，提案モデルは初期感染ホストの初期位置によらず，シミュレーション実験の結果に近似することが分かる．

最後に，計算時間の比較を行う．図 6 に，モバイルホスト数 K に対する計算時間の結果を示す．図より，提案モデルの計算時間（ODE）は，シミュレーション実験の計算時間（Sim）より小さいことが分かる．シミュレーション実験の計算時間は，ホスト数が増えるにつれて大きくなる．一方で，数値計算の計算時間はホスト数に依存しない．したがって，提案モデルはシミュレーション実験に近い結果を，シミュレーション実験より短時間で取得できることがわかる．

4. 結　　論

本稿では，劣通信環境におけるモバイル端末間のマルウェア拡散を表現する感染モデルの提案を行った．提案モデルを用いることで，シミュレーション実験によって得られる結果と近い結果を，より短時間で取得できることが分かった．今後の課題として，SIR モデルのような単純なモデルではなく，実世界のモバイル端末の挙動を表現できるような具体的なモデルを検討する．

謝辞 本研究は日本学術振興会科学研究費補助金（基盤研究 (B)）第 20H04184 号の支援を受けています．

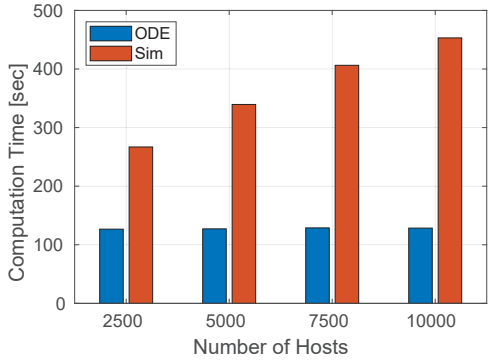


図 6: 計算時間の比較

文　　献

[1] MATLAB, https://jp.mathworks.com/products/matlab.html, accessed Sep. 3, 2022.

[2] G. Gonzalez, M. E. Larraga, L. Alvarez-Icaza, and J. Gomez, “Bluetooth worm propagation in smartphones: modeling and analyzing spatiotemporal dynamics,” *IEEE Access*, vol. 9, pp. 75265–75282, 2021.

[3] J. Jang-Jaccard and S. Nepal, “A survey of emerging threats in cyber security,” *Journal of Computer and System Sciences*, vol. 80, no.5, pp. 973-993, 2014.

[4] W. O. Kermack and A. G. McKendrick, “A contribution to the mathematical theory of epidemics,” in *Proc. the Royal Society of London Series A*, vol. 115, no. 772, pp. 700–721, 1927.

[5] A. M. Lonzetta, P. Cope, J. Campbell, B. J. Mohd, and T. Hayajneh, “Security vulnerabilities in Bluetooth technology as used in IoT,” *Journal of Sensor and Actuator Networks*, vol. 7, no. 3, 2018.

[6] B. K. Mishra and S. K. Pandey, “Dynamic model of worms with vertical transmission in computer network,” *Applied Mathematics and Computation*, vol. 217, no. 21, 2011.

[7] A. M. Rey, “Mathmatical modeling of the propagation of malware: a review,” *Security and Communication Networks*, vol. 8, no.15, pp. 2561-2579, 2015.