社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2004－ＣＳＥＣ－26　(29)
2004／7／21

コンピュータウィルス拡散過程の数理モデル化と解析

内田　真人†　　佐藤　大輔†

† 日本電信電話株式会社 NTT サービスインテグレーション基盤研究所
〒 180–8585 東京都武蔵野市緑町 3–9–1
E-mail: †{uchida.masato, satoh.daisuke}@lab.ntt.co.jp

あらまし　ネットワークを介して伝播するウイルスが主流となった現在，コンピュータウィルスがネットワーク上をどのように伝播して感染規模を広めていくかを理解することは，コンピュータウィルスの危険性を評価する上で基本的かつ重要な問題である．そこで本稿では，ネットワークを介して感染するコンピュータウィルスを攻撃形態に応じて分類した上で，それぞれの攻撃形態について感染数の推移過程の数理モデルを提案し，感染数の推移と攻撃形態の関係を明らかにする．特に，ランダム IP 型（繰り返し攻撃型）・メール型（感染直後のみ攻撃型）コンピュータウィルスのそれぞれについて，その拡散過程を表現する差分方程式を確率論の視点から導出し，さらに，この差分方程式から得られる幾つかの解析結果を示す．

キーワード　コンピュータウィルス，拡散過程，数理モデル化

Modeling and Analysis of Computer Virus Diffusion Process

Masato UCHIDA† and Daisuke SATOH†

† NTT Service Integration Laboratories, NTT Corporation
3-9-11, Midori-Cho, Musashino-Shi, Tokyo 180–8585 Japan
E-mail: †{uchida.masato, satoh.daisuke}@lab.ntt.co.jp

Abstract　Almost all contemporary computer viruses spread through the network. Therefore, understanding how and how much a given computer virus will spread through the network is an essential and important problem in terms of evaluating the threat of computer viruses. The goal of this work is to reveal the relationship between the process of the spread of infection and the attack pattern. We start by classifying computer viruses that spread through networks in terms of their attack patterns, as either Random IP (attack repetitively after infection) Model or Mail (attack immidiately after infection) Model. We then propose mathematical models of the process of the spread of infection by viruses in each classes. We derive difference equations which explain the diffusion process in each case, and give some analysis result obtained by using these equations.

Key words　Computer Virus, Diffusion Process, Mathematical Modeling

1. まえがき

情報技術が生活を支える基盤となった現在，ネットワークを介して感染するコンピュータウィルスの脅威が増している．コンピュータウイルスは感染先で様々な被害を発生させ，さらに，その感染行為自体がネットワークに対する負荷となることもある．こうしたコンピュータウィルスによる被害はその感染規模（数）に依存する．そのため，コンピュータウィルスの感染規模（数）がどのように推移するかを把握することは基本的かつ重要な問題であると言える．また，コンピュータウィルスがどのように新たな感染を引き起こすのか（攻撃形態）によって感染規模は大きく影響を受けると考えられるため，感染規模の推移が攻撃形態とどのように関係しているかを明らかにする事も重要である．そこで本稿では，ネットワークを介して感染するコンピュータウィルスを攻撃形態に応じて分類した上で，それぞれの攻撃形態について感染数の推移過程の数理モデルを提案し，その特性を調べる．

ネットワークを介して感染するコンピュータウィルスの攻撃形態には幾つかの種類がある．例えば CodeRed では，ウィルスに感染した端末が，ランダムに IP アドレスを生成して攻撃先の端末を決定するという手順を繰り返して感染活動を行う（繰り返し攻撃型）．Slammer や Blaster も，CodeRed と同様の方法で感染を行うウィルスである．一方，Aliz や LoveLetter は電子メールを介した感染活動を行う．すなわち，ウィルスに

感染した端末は，メールアドレス帳に登録されている端末を新たな攻撃先とする．したがって，メールアドレス帳内の全てのアドレスに対して攻撃が終了するとその後は新規の感染が発生しない（感染直後のみ攻撃型）．本稿では，上記の二種類の攻撃形態を取り上げる．

これまでにも，コンピュータウィルスの拡散過程に関する以下のような研究結果が報告されている．[1] では，CodeRed, Slammer, Blaster のような繰り返し攻撃型のウィルス感染数の推移がロジスティック方程式で表現できることが報告されている．一方, [2] では，Aliz や LoveLetter のような感染直後のみ攻撃型のウィルス感染数の推移を表現する差分方程式が提案されている．しかし，これらの研究では，それぞれの方程式がどのような理論的背景から導出されるかという問題については触れられていない．そこで，本稿では，これらの方程式を確率論の視点から導出する．

2. モデル化

本稿では, [2] に従い，コンピュータウィルスの感染形態のモデルとして，以下の二種類を検討する．なお，以下では，ネットワークを構成する端末（ノード）の個数を N とおく．

繰り返し攻撃型（ランダム IP 型）モデル　時刻 n における累積感染ノードが互いに独立に，時刻 $n+1$ において，ランダムに選択した A $(1 \leqq A \leqq N-1)$ 個のノードを攻撃し，確率 p $(0 < p \leqq 1)$ で感染させる．

感染直後のみ攻撃型（メール型）モデル　時刻 n における新規感染ノードのみが互いに独立に，時刻 $n+1$ において，ランダムに選択した A $(1 \leqq A \leqq N-1)$ 個のノードを攻撃し，確率 p $(0 < p \leqq 1)$ で感染させる．

ここで，A は確率変数である．A が従う分布型は様々に設定可能であるが，時刻 n における攻撃先ノード数を固定（a 個）とするためには

$$\Pr\{A = a\} = 1$$

とすれば良い．なお，現実の感染形態においては，攻撃元ノードが互いに独立に攻撃を行うとは限らないと考えられるが，このことについては今後の課題とする．

3. 解　　析

3.1 差分方程式の導出

時刻 n における累積感染ノード数を表す確率変数を，繰り返し攻撃型モデル，感染直後のみ攻撃型モデルについてそれぞれ R_n，M_n とおく．なお，以下では，ある確率変数 X, Y について $\mathbb{E}[X]$ は X の期待値を表し，$\mathbb{E}[X|Y]$ は Y を条件とする X の条件付き期待値を表す．さらに，記法の簡単のため，ある確率変数 X, Y について $X = Y$, w.p.1 が成り立つ場合，誤解の恐れが無い限り単に $X = Y$ と書く事とする．

まず，M_n について解析する．N 個の要素からなるノード集合を V とおく．さらに，時刻 n における新規感染ノード数を表す確率変数を $\bar{M}_n = M_n - M_{n-1}$ とおき，新規感染ノード集合を $V_n = \{v_{n,1}, v_{n,2}, \cdots, v_{n,\bar{M}_n}\} \subset V$ とおく．ただし，一般性を失うことなく，V_n の各要素は $v_{n,1}, v_{n,2}, \cdots, v_{n,\bar{M}_n}$ の順に互いに独立に $A_{n,1}, A_{n,2}, \cdots, A_{n,\bar{M}_n}$ 個のノードに対してそれぞれ攻撃を行うとする．ここで，$A = A_{n,i}$ である $(i = 1, \cdots, \bar{M}_n)$．このとき，$v_{n+1,i}$ が攻撃した $A_{n+1,i}$ 個のノードについて，ウィルス未感染ノード数を表す確率変数を $\bar{M}_{n+1,i}$ とおき，$v_{n,i}$ の攻撃が終了した段階での累積感染ノード数を表す確率変数を $M_{n+1,i}$ とおけば，$M_{n+1,j} = M_n + \sum_{i=1}^{j} \bar{M}_{n+1,i}$ となる $(j = 1, \cdots, \bar{M}_n)$．なお，$M_{n+1} = M_{n+1,\bar{M}_n}$ である．

以上の定義より

$$\begin{aligned}&\mathbb{E}[M_{n+1,j}|M_n, \bar{M}_n, A_{n+1,j}] \\ &= \mathbb{E}[M_{n+1,j-1}|M_n, \bar{M}_n] + p\mathbb{E}[\bar{M}_{n+1,j}|M_n, \bar{M}_n, A_{n+1,j}]\end{aligned}$$

が成り立つ $(j = 1, \cdots, \bar{M}_n)$．また

$$\begin{aligned}&\Pr\{\bar{M}_{n+1,j} = \bar{m}|M_n, \bar{M}_n, \bar{M}_{n+1,1}, \cdots, \bar{M}_{n+1,j-1}, A_{n+1,j}\} \\ &= \begin{pmatrix} N - M_{n+1,j-1} \\ \bar{m} \end{pmatrix} \begin{pmatrix} M_{n+1,j-1} \\ A_{n+1,j} - \bar{s} \end{pmatrix} \Big/ \begin{pmatrix} N \\ A_{n+1,j} \end{pmatrix}\end{aligned}$$

であるので

$$\begin{aligned}&\mathbb{E}[\bar{M}_{n+1,j}|M_n, \bar{M}_n, \bar{M}_{n+1,1}, \cdots, \bar{M}_{n+1,j-1}, A_{n+1,j}] \\ &= \frac{A_{n+1,j}}{N}(N - M_{n+1,j-1})\end{aligned}$$

となる．（超幾何分布の期待値）．したがって，$\alpha = \mathbb{E}[A]/N$ $(0 < \alpha < 1)$ とおくと

$$\begin{aligned}&\mathbb{E}[\bar{M}_{n+1,j}|M_n, \bar{M}_n, \bar{M}_{n+1,1}, \cdots, \bar{M}_{n+1,j-1}] \\ &= \alpha(N - M_{n+1,j-1})\end{aligned}$$

が成り立つ．このことから

$$\mathbb{E}[\bar{M}_{n+1,j}|M_n, \bar{M}_n] = \alpha(N - \mathbb{E}[M_{n+1,j-1}|M_n, \bar{M}_n])$$

が成り立つ（$M_{n+1,j-1} = M_n + \sum_{i=1}^{j-1} \bar{M}_{n+1,i}$ に注意）．以上より

$$\begin{aligned}&\mathbb{E}[M_{n+1,j}|M_n, \bar{M}_n] \\ &= \mathbb{E}[M_{n+1,j-1}|M_n, \bar{M}_n] + p\alpha(N - \mathbb{E}[M_{n+1,j-1}|M_n, \bar{M}_n]) \\ &= N - (N - \mathbb{E}[M_{n+1,j-1}|M_n, \bar{M}_n])(1 - p\alpha)\end{aligned}$$

が成り立つ．これを再帰的に適用すると

$$\mathbb{E}[M_{n+1,j}|M_n, \bar{M}_n] = N - (N - M_n)(1 - p\alpha)^j$$

となる．さらに，$\bar{M}_n = M_n - M_{n-1}$ であるので

$$\mathbb{E}[M_{n+1}|M_n, M_{n-1}] = N - (N - M_n)(1 - p\alpha)^{M_n - M_{n-1}}$$

が成り立つ．R_n についても，ほぼ同様の議論を行うことで，以下の定理が導かれる．

定理 1. R_n，M_n について

$$\mathbb{E}[R_{n+1}|R_n] = N - (N - R_n)(1 - p\alpha)^{R_n} \quad (1)$$

$$\mathbb{E}[M_{n+1}|M_n, M_{n-1}] = N - (N - M_n)(1 - p\alpha)^{M_n - M_{n-1}} \quad (2)$$

が成り立つ $(n = 0, 1, 2, \cdots)$．　□

ここで

$$\mathbb{E}[R_{n+1}] = \mathbb{E}[R_{n+1}|R_n = \mathbb{E}[R_n]] \quad (3)$$

$$\mathbb{E}[M_{n+1}] = \mathbb{E}[M_{n+1}|M_n = \mathbb{E}[M_n], M_{n-1} = \mathbb{E}[M_{n-1}]] \quad (4)$$

と仮定すると，定理 1 より

$$\mathbb{E}[R_{n+1}] = N - (N - \mathbb{E}[R_n])(1-p\alpha)^{\mathbb{E}[R_n]} \quad (5)$$

$$\mathbb{E}[M_{n+1}] = N - (N - \mathbb{E}[M_n])(1-p\alpha)^{\mathbb{E}[M_n]-\mathbb{E}[M_{n-1}]} \quad (6)$$

が導かれる（$n = 0, 1, 2, \cdots$）．以下では，特に断わらない限り，上記の仮定の下で議論する．

式 (5)，(6) はそれぞれ

$$\mathbb{E}[R_{n+1}] - \mathbb{E}[R_n] = (N - \mathbb{E}[R_n])\{1 - (1-p\alpha)^{\mathbb{E}[R_n]}\}$$

$$\mathbb{E}[M_{n+1}] - \mathbb{E}[M_n] = (N - \mathbb{E}[M_n])\{1 - (1-p\alpha)^{\mathbb{E}[M_n]-\mathbb{E}[M_{n-1}]}\}$$

と変形できる．このことから，時刻 $n+1$ における新規感染数が，繰り返し攻撃型モデルでは時刻 n における累積感染数に依存し，感染直後のみ攻撃型モデルでは時刻 n における新規感染数に依存することが分かる．これは，繰り返し攻撃型モデル，感染直後のみ攻撃型モデルのそれぞれの特徴を良く反映していると言える．

3.2 感染数の収束値

式 (5)，(6) より，累積感染数の収束値に関する以下の定理が導かれる（証明は付録 1. 参照）．

定理 2. $\mathbb{E}[R_0] = 1$，$\mathbb{E}[M_0] = 1$，$\mathbb{E}[M_{-1}] = 0$ の時，M_n，R_n について

$$\lim_{n\to\infty} \mathbb{E}[R_n] = N$$

$$\lim_{n\to\infty} \mathbb{E}[M_n] = N - \frac{W((N-1)(1-p\alpha)^N \ln(1-p\alpha))}{\ln(1-p\alpha)}$$

が成り立つ．ただし，W は乗積対数関数である．なお，乗積対数関数とは $x\exp(x)$ の逆関数である（Lambert の W 関数とも呼ばれる）[3]. □

定理 2 より，感染直後のみ攻撃型モデルにおける平均累積感染数は全ノード数 N に収束しない場合があることが分かる．このことは，感染直後のみ攻撃型モデルにおいては，時刻 n における新規感染ノードのみが，時刻 $n+1$ において攻撃を行うことに起因する．すなわち，時刻 n における新規感染ノードが存在しない場合（時刻 $n-1$ における全ての攻撃対象が時刻 $n-1$ において既感染である場合）は，ウィルスの拡散が停止してしまうということである．このことに対し，繰り返し攻撃型モデルにおいては，時刻 n における累積感染ノードが，時刻 $n+1$ において攻撃を行う．そのため，仮に，時刻 n における新規感染ノードが存在しない場合であっても，ウィルスの拡散が継続し，最終的には全てのノードが感染するのである．

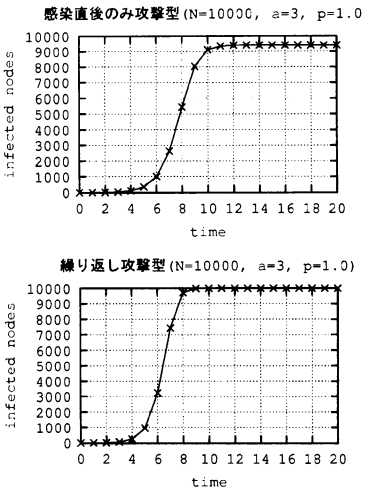

Fig 1 平均累積感染ノード数の推移（左：感染直後のみ攻撃型モデル，右：繰り返し攻撃型モデル，実線：理論値，×印：実験値）

3.3 差分方程式の連続化

式 (5)，(6) で与えられる差分方程式の連続化を行う．まず，$n = \frac{t}{\delta}$ と特殊化し，$R(t) = R_n$，$M(t) = M_n$ とおく．さらに，式 (5) で与えられる差分方程式について $1-p\alpha = (1-p\bar{\alpha})^{\delta}$ と特殊化し，式 (6) で与えられる差分方程式について $1-p\alpha = (1-p\bar{\alpha})^{\delta}$，$N = \bar{N} - \frac{1}{\delta \ln(1-p\bar{\alpha})}$ と特殊化すると，$\delta \to 0$ のとき，以下の定理が導かれる（証明は付録 2. 参照）．

定理 3. $R(t)$，$M(t)$ について

$$\frac{d\mathbb{E}[R(t)]}{dt} = -\{\ln(1-p\bar{\alpha})\}\mathbb{E}[R(t)](N - \mathbb{E}[R(t)]) \quad (7)$$

$$\frac{d^2\mathbb{E}[M(t)]}{dt^2} = -\{\ln(1-p\bar{\alpha})\}\frac{d\mathbb{E}[M(t)]}{dt}(\bar{N} - \mathbb{E}[M(t)]) \quad (8)$$

が成り立つ． □

式 (7)，(8) の解はそれぞれ

$$\mathbb{E}[R(t)] = \frac{NC}{C - (1-p\alpha)^{Nt}}$$

$$\mathbb{E}[M(t)] = \bar{N} + \tilde{N}\tanh\left(-\frac{1}{2}\tilde{N}(t + C_2)\ln(1-p\alpha)\right)$$

と与えられる．ただし

$$\tilde{N} = \sqrt{\frac{2C_1 - \bar{N}^2\ln(1-p\alpha)}{-\ln(1-p\alpha)}}$$

である．なお，C，C_1，C_2 は積分定数である．

4. シミュレーション

$N = 10000$，$a = 3$（すなわち，$\Pr\{A = 3\} = 1$）とし，感染直後のみ攻撃型モデル，繰り返し攻撃型モデルに基づくシミュレーションをそれぞれ 10000 回ずつ行い，時刻 n 毎に累積感染数の平均値を求めた．ただし，時刻 0 における感染ノード数を 1 とした．

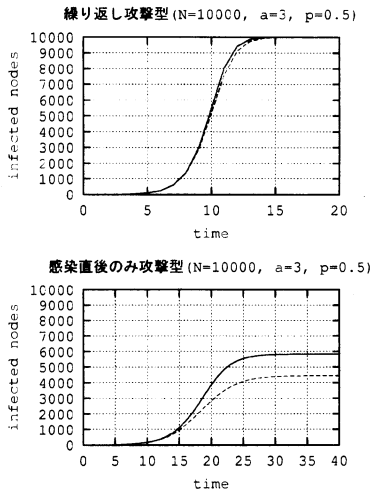

Fig 2 平均累積感染ノード数の推移（左：感染直後のみ攻撃型モデル，右：繰り返し攻撃型モデル，実線：理論値，点線：実験値）

図1は，上記のシミュレーションの結果，及び式(5)，(6)に $N = 10000$，$\alpha = a/N$，$p = 1.0$ を代入することにより求められる平均累積感染数をプロットしたものである．ただし，式(5)，(6)において，$\mathbb{E}[M_0] = 1$，$\mathbb{E}[M_1] = (N-1)p\alpha + 1$，$\mathbb{E}[R_0] = 1$ とした．この図より，式(5)，(6)は，それぞれの対応するシミュレーション結果を良く近似していることが分かる．また，定理2より累積感染ノード数の収束値は，9405（感染直後のみ攻撃型モデル），10000（繰り返し攻撃型モデル）と求められる．この収束値は，シミュレーション上の収束値（$n = 10$ の時の値）と一致している．

図2は，$p = 0.5$ とした点を除いて，図1と同様のプロットである．この図より，式(5)，(6)は，それぞれの対応するシミュレーション結果よりも大きな値となっていることが分かる．これは，式(3)，(4)の仮定の影響であるということが，以下の定理によって示される（証明は付録3.参照）．

定理 4. R_n，M_n について

$$\mathbb{E}[R_{n+1}] \leqq N - (N - \mathbb{E}[R_n])(1-p\alpha)^{\mathbb{E}[R_n]} \quad (9)$$

$$\mathbb{E}[M_{n+1}] \leqq N - (N - \mathbb{E}[M_n])(1-p\alpha)^{\mathbb{E}[M_n]-\mathbb{E}[M_{n-1}]} \quad (10)$$

が成り立つ（$n = 0, 1, 2, \cdots$）． □

上記の定理より，各種パラメータ（N, a, p 等）の値によっては，式(3)，(4)の仮定の妥当性が保障されない場合があることが分かる．このことについては今後の課題とする．

5. 関連研究

前節で導いた結果と，[1], [2] との関係について考察する．

二項定理を用いると，式(5)，(6)は，$p\alpha \ll 1$ のとき，それぞれ

$$\begin{aligned}\mathbb{E}[R_{n+1}] &\approx N - (N - \mathbb{E}[R_n])(1 - p\alpha\mathbb{E}[R_n]) \\ &= \mathbb{E}[R_n] + p\alpha\mathbb{E}[R_n](N - \mathbb{E}[R_n]) \quad (11)\end{aligned}$$

$$\begin{aligned}\mathbb{E}[M_{n+1}] &\approx N - (N - \mathbb{E}[M_n])\{1 - p\alpha(\mathbb{E}[M_n] - \mathbb{E}[M_{n-1}])\} \\ &= \mathbb{E}[M_n] + p\alpha(\mathbb{E}[M_n] - \mathbb{E}[M_{n-1}])(N - \mathbb{E}[M_n]) \quad (12)\end{aligned}$$

と近似できる．ここで，式(11)はロジスティック差分方程式である．したがって，この結果は[1]の主張と一致していることがわかる．また，式(12)は[2]で提案されている差分方程式に一致していることがわかる．一方，定理3の結果も[1], [2]に一致していることがわかる．なぜならば，式(7)はロジスティック微分方程式であり，式(8)は[2]で導出された微分方程式に（係数を除いて）一致しているからである．ただし，式(7)，(8)は $p\alpha \ll 1$ の条件を用いずに導出した結果であることに注意されたい．

6. むすび

本稿では，コンピュータウィルスの拡散過程について，確率論の視点から解析を行った．また，この解析によって得られた結果と[1], [2]との関係を明らかにした．今後の課題としては，式(3)，(4)により与えられる仮定の妥当性をより詳細に評価する事や，攻撃元ノードが互いに独立に攻撃を行わない場合の解析を行うことなどが挙げられる．

References

[1] S.Staniford, V.Paxson, N.Weaver, "How to 0wn the Internet in Your Spare Time", Proceedings of the 11th USENIX Security Symposium (Security '02), 2002.

[2] 佐藤, 内田, 石橋, 小林, "メール型コンピュータウィルス拡散モデル", 情報セキュリティ研究会, July 2004.

[3] R. M. Corless, et al., "On the Lambert W Function", Advances in Computatianal Mathematics, vol.5, 1996.

付　録

1. 定理2の証明

まず，R_n について証明する．

背理法を用いて証明するために $\lim_{n\to\infty}\mathbb{E}[R_n] \neq N$ と仮定する．このとき，式(5)より $\lim_{n\to\infty}(1-p\alpha)^{\mathbb{E}[R_n]} = 1$ となる．ここで，$p\alpha \neq 0$ であることから $\lim_{n\to\infty}\mathbb{E}[R_n] = 0$ となるが，これは $\mathbb{E}[R_n] \geqq 1$ に矛盾する．

次に，M_n について証明する．

式(6)より

$$\begin{aligned}N - \mathbb{E}[M_{n+1}] &= (N - \mathbb{E}[M_n])(1-p\alpha)^{\mathbb{E}[M_n]-\mathbb{E}[M_{n-1}]} \\ &= (N-1)(1-p\alpha)^{\mathbb{E}[M_n]}\end{aligned}$$

となる．ここで $\mathbb{E}[M_\infty] = \lim_{n\to\infty}\mathbb{E}[M_n]$ とおくと

$$\begin{aligned}&(N-1)(1-p\alpha)^N \ln(1-p\alpha) \\ &= \{\ln(1-p\alpha)\}(N - \mathbb{E}[M_\infty]) \\ &\quad \times \exp(\{\ln(1-p\alpha)\}(N - \mathbb{E}[M_\infty]))\end{aligned}$$

となるので，乗積対数関数の定義より

$$W((N-1)(1-p\alpha)^N \ln(1-p\alpha))$$
$$= \{\ln(1-p\alpha)\}(N - \mathbb{E}[M_\infty])$$

が成り立つ．

2. 定理 3 の証明

まず，$R(t)$ について証明する．

式 (5) より

$$\ln(N - \mathbb{E}[R(t+\delta)]) - \ln(N - \mathbb{E}[R(t)])$$
$$= \delta\{\ln(1-p\bar{\alpha})\}\mathbb{E}[R(t)]$$

が成り立つ．このとき，上式の全体を δ で割り，$\delta \to 0$ とすれば良い．

次に，$M(t)$ について証明する．

式 (6) より

$$-\{\ln(1-p\alpha)\}(N - \mathbb{E}[M(t)])(\mathbb{E}[M(t)] - \mathbb{E}[M(t-\delta)])$$
$$= -(N - \mathbb{E}[M(t)]) \ln\left(\frac{N - \mathbb{E}[M(t+\delta)]}{N - \mathbb{E}[M(t)]}\right) \qquad \text{(A·1)}$$

が成り立つ．ここで

$$1 - \frac{1}{x} \leqq \ln(x) \leqq x - 1, \quad \text{（等号は} x = 1 \text{ のときに限る）}$$

が成り立つことに注意すると，式 (A·1) より

$$-(N - \mathbb{E}[M(t)])\left(\frac{N - \mathbb{E}[M(t+\delta)]}{N - \mathbb{E}[M(t)]} - 1\right)$$
$$\leqq -\{\ln(1-p\alpha)\}(N - \mathbb{E}[M(t)])(\mathbb{E}[M(t)] - \mathbb{E}[M(t-\delta)])$$
$$\leqq -(N - \mathbb{E}[M(t)])\left(1 - \frac{N - \mathbb{E}[M(t)]}{N - \mathbb{E}[M(t+\delta)]}\right)$$

が成り立つ．さらに，$\bar{\alpha}$，$\bar{N}$ の定義より

$$(\mathbb{E}[M(t+\delta)] - \mathbb{E}[M(t)]) - (\mathbb{E}[M(t)] - \mathbb{E}[M(t-\delta)])$$
$$\leqq \delta\{\ln(1-p\bar{\alpha})\}(\bar{N} - \mathbb{E}[M(t)])(\mathbb{E}[M(t)] - \mathbb{E}[M(t-\delta)])$$
$$\leqq (\mathbb{E}[M(t+\delta)] - \mathbb{E}[M(t)]) - (\mathbb{E}[M(t)] - \mathbb{E}[M(t-\delta)])$$
$$+ \frac{(\mathbb{E}[M(t+\delta)] - \mathbb{E}[M(t)])^2}{\bar{N} - \frac{1}{\delta\ln(1-p\bar{\alpha})} - \mathbb{E}[M(t+\delta)]}$$

が成り立つ．このとき，上式の全体を δ^2 で割り，$\delta \to 0$ とすれば良い．

3. 定理 4 の証明

まず，式 (9) を証明する．このとき，式 (1) より

$$\frac{d^2}{d^2 R_n}\mathbb{E}[R_{n+1}|R_n]$$
$$= (1-p\alpha)^{R_n}\ln(1-p\alpha)\{2 - (N-R_n)\ln(1-p\alpha)\} < 0$$

となるので，$\mathbb{E}[R_{n+1}|R_n]$ は R_n に関して上に凸の関数であることが分かる．したがって，Jensen の不等式より

$$\mathbb{E}[R_{n+1}]$$
$$= \mathbb{E}[\mathbb{E}[R_{n+1}|R_n]]$$
$$\leqq \mathbb{E}[R_{n+1}|R_n = \mathbb{E}[R_n]]$$
$$= N - (N - \mathbb{E}[R_n])(1-p\alpha)^{\mathbb{E}[R_n]}$$

となる．

次に，式 (10) を証明する．このとき，式 (2) より

$$\frac{\partial^2}{\partial^2 M_n}\mathbb{E}[M_{n+1}|M_n, M_{n-1}]$$
$$= (1-p\alpha)^{M_n - M_{n-1}}\ln(1-p\alpha)$$
$$\times\{2 - (N-M_n)\ln(1-p\alpha)\} < 0$$
$$\frac{\partial^2}{\partial^2 M_{n-1}}\mathbb{E}[M_{n+1}|M_n, M_{n-1}]$$
$$= -(1-p\alpha)^{M_n - M_{n-1}}\{\ln(1-p\alpha)\}^2 < 0$$

となるので，$\mathbb{E}[M_{n+1}|M_n, M_{n-1}]$ は M_n および M_{n-1} に関して上に凸の関数であることが分かる．したがって，Jensen の不等式より

$$\mathbb{E}[M_{n+1}]$$
$$= \mathbb{E}[\mathbb{E}[M_{n+1}|M_n, M_{n-1}]]$$
$$\leqq \mathbb{E}[M_{n+1}|M_n = \mathbb{E}[M_n], M_{n-1} = \mathbb{E}[M_{n-1}]]$$
$$= N - (N - \mathbb{E}[M_n])(1-p\alpha)^{\mathbb{E}[M_n] - \mathbb{E}[M_{n-1}]}$$

となる．