Markovian Arrival Process と暗号通信

豊泉　洋

$M/M/\infty$ 待ち行列のダイナミックスに従う位相変化を持つ $BMAP/M/1$ 待ち行列の待ち時間を解析し，グループでの暗号通信のセキュリティを評価する．$M/M/1$ 待ち行列，$MAP/M/1$ 待ち行列との対比を行いながら，$BMAP/M/1$ 待ち行列の系内客数の上下限を，通常用いられる行列の反復計算を用いずに求める方法を示す．

キーワード：待ち行列，Markovian Arrival Process (MAP)，暗号通信，セキュリティ

1. 記憶へ

待ち行列理論では，$M/M/1$ 待ち行列と呼ばれるモデルを最初に学習する．最初の M は到着間隔が指数分布に従い，いわゆる Poisson 到着していることを示し，2番目の M はサービス時間が指数分布に従うことを表す．M は指数分布が無記憶 (Memoryless) と呼ばれる性質を持ち，過去 (例えば，ひとつ前の到着時点や今の系内数) によらずに，次の到着が起こることを示している．このことが $M/M/1$ 待ち行列全体が Markov 性を持つことを保証している．最後の1は，サービスを行う窓口が一つであることを指す．

$M/M/1$ 待ち行列では，時刻 t での系内数 $N(t)$ は，到着で一つ増え，退去で一つ減る．$N(t)=n$ という状態に着目し，確率の変化を考えよう．十分小さな時間区間 $I=(t, t+\Delta t]$ での $N(t)=n$ からの確率の流出は，

$$P\{N(t)=n, I\text{で変化あり}\}$$
$$=P\{I\text{で変化あり}\,|N(t)=n\}P\{N(t)=n\}$$

となる．到着レートを λ，サービスレートを μ とし，待ち行列の安定性条件より，$\mu>\lambda$ とする．到着間隔やサービス時間が無記憶なので，現在の客数 $N(t)$ と将来の区間 I での事象は独立である．このことに注意すれば，十分小さな区間 I で，$P\{I$ で変化あり $|N(t)=n\}$ は，$(\lambda+\mu)\Delta t$ で近似できる．したがって，長さ Δt の微小区間での確率の流出は，

$$(\lambda+\mu)\Delta tP\{N(t)=n\},$$

で表せる．今度は，流入について考える．十分小さな区間 I では，$N(t)=n-1$ で到着が起こったとき，または $N(t)=n+1$ で退去が起こったときに，$N(t)=n$ へ遷移する．したがって，$N(t)=n$ への流入は

$$\lambda\Delta tP\{N(t)=n-1\}+\mu\Delta tP\{N(t)=n+1\}$$

となる．定常状態では，確率の「出入り」はバランスしているはずである．定常状態確率を $\pi_n=P\{N(t)=n\}$ とすると，次のような状態方程式が成立する (図1の状態遷移図参照)．

$$0=-\lambda\pi_0+\mu\pi_1,$$
$$0=\lambda\pi_{n-1}-(\lambda+\mu)\pi_n+\mu\pi_{n+1}\ \text{for}\ n\geq 1. \quad (1)$$

π_n の z 変換を $\pi(z)=\sum_{n=0}^{\infty}\pi_n z^n$ とする．(1)の全体を z 変換すると，次のように $\pi(z)$ に対する定常状態方程式が得られる．

$$\mu\left(1-\frac{1}{z}\right)\pi_0+\pi(z)\left\{-\lambda+\lambda z-\mu\left(1-\frac{1}{z}\right)\right\}=0. \quad (2)$$

$\pi(z)$ について解くことも可能だが，ここは我慢して，z について一階微分し，$z\to 1$ の極限をとる．$\pi(z)$ の一階微分 $\pi'(z)$ の項はちょうど無くなり，

$$\mu\pi_0+\pi(1)(\lambda-\mu)=0, \quad (3)$$

が得られる．全確率保存により，$\pi(1)=1$ に注意すれば，$M/M/1$ 待ち行列の使用率 ρ は，

$$\rho=P\{N(t)>0\}=1-\pi_0=\frac{\lambda}{\mu}, \quad (4)$$

であることがわかる．(2)の二階微分を行い，$z\to 1$ の極限をとると，今度は二階微分 $\pi''(z)$ の項がなくなり，

$$\mu\pi_0+\pi'(1)(\lambda-\mu)+\mu=0, \quad (5)$$

という式が得られ，$M/M/1$ 待ち行列の平均系内数が

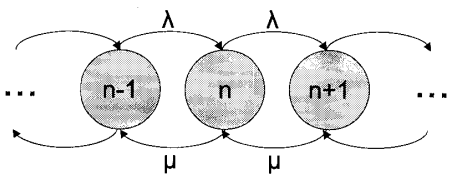

図1　$M/M/1$ 待ち行列の状態遷移図

とよいずみ　ひろし
早稲田大学 大学院会計研究科
〒169-8050 新宿区西早稲田 1-6-1

$$E[N(t)]=\pi'(1)=\frac{\rho}{1-\rho}, \tag{6}$$

となることがわかる．

さて，実際の到着間隔は無記憶なのであろうか？もちろん，無記憶としてモデル化できるケースも多々存在するが，記憶のある到着もモデル化したいのは当然である．Markovian Arrival Process (MAP) とは，Markov性を保持しつつ，記憶のある到着へPoisson到着を拡張したものである[2][9]．拡張の仕方は，いたって素直だ．次の到着の時点が，過去に依存して決まるようにする．ただし，過去は何でもいいわけではなく，計算のしやすさを保存するために，Markov過程にしておくのがポイントだ．

具体的には，系内数 $N(t)$ とは別に，過去を保持するプロセス $I(t)$ を用意する．$I(t)$ は，それ自体Markov過程をなし，ある特定の遷移が起こったときに，$N(t)$ へ到着を引き起こす．記憶を $I(t)$ の形で持つ到着過程の誕生だ．$I(t)$ は伝統的に到着過程の位相 (phase) と呼ばれる．

2. グループでの暗号通信

さて，いきなり話を変える．暗号通信である．言うまでもなく，現代は暗号通信の時代だ．SSL (Secure Socket Layer) [3]と呼ばれる公開鍵暗号方式無しでは，日々のインターネット上でのショッピングに必要な情報のやり取りすらできない．

公開鍵暗号方式は，公開鍵と秘密鍵を使った一対一の通信である．この方式は，大きなグループで暗号通信するのには，不向きだ．グループで情報を共有するためには，そのグループメンバーだけが知る秘密鍵の共有が効率的である[6][8]．

ところが，秘密鍵の共有は，グループの構成員の脱退に弱い．秘密鍵を持ったまま脱退するので，脱退者は容易に盗聴できる．盗聴を防ぐには，秘密鍵を更新すればよいが，それでも，鍵の更新がグループ全体に行き渡るまで，古い鍵を使用しなければならず，グループ内のセキュリティは低下する[4][5]．ちょっと人工的だが，各鍵の更新には，平均 $1/\mu$ の指数時間かかり，その更新中，さらに脱退が起こった場合の次の鍵更新処理は，待たされるとしよう．

鍵の更新処理を待ち行列でモデル化する．このとき，鍵の更新処理の発生は無記憶だろうか？

グループへの加入がレート ν のPoisson到着であり，滞在時間が平均 $1/\sigma$ の指数分布に従うとする．この形のダイナミックスは $M/M/\infty$ 待ち行列と呼ばれる．グループへ参加した瞬間，待たずにサービスされるので，あたかも，無限大のサービス窓口が存在すると考えることできる．

鍵の更新処理は，$M/M/\infty$ に従う位相 $I(t)$ を持つMAPに従って発生する．すなわち，$MAP/M/1$ 待ち行列としてモデル化できる．

3. あらためて $MAP/M/1$ 待ち行列

$MAP/M/1$ 待ち行列では，$(N(t), I(t))$ の組でMarkov過程である．定常状態確率を $\pi_{ni}=P\{N(t)=n, I(t)=i\}$ とする．位相にあたる i をまとめて，次のようにベクトル表記する．

$$\boldsymbol{\pi}_n=(\pi_{n0}, \pi_{n1}, \cdots). \tag{7}$$

(1)に相当する定常状態方程式を考えよう（図2の $MAP/M/1$ 待ち行列の状態遷移図参照）．$MAP/M/1$ 待ち行列では，$M/M/1$ 待ち行列と違い，ベクトルで確率の出し入れを考える．定常状態方程式は，

$$\begin{aligned}0&=\boldsymbol{\pi}_0\mathbf{D}_0+\mu\boldsymbol{\pi}_1,\\ 0&=\boldsymbol{\pi}_{n-1}\mathbf{D}_1+\boldsymbol{\pi}_n(\mathbf{D}_0-\mu\mathbf{I})+\mu\boldsymbol{\pi}_{n+1}\ \text{for}\ n\geq 1.\end{aligned} \tag{8}$$

となる．ここで，$\mathbf{D}_1$ は，$N(t)$ の到着を伴う位相 $I(t)$ の遷移レート行列で，$M/M/1$ 待ち行列での到着率 λ に相当する．$\mathbf{D}_0$ は，到着を伴わない変化を表し，$M/M/1$ 待ち行列での $-\lambda$ を拡張したものに相当する．2節でみた脱退時に更新処理が起こる暗号通信では，

$$\mathbf{D}_0=\begin{pmatrix}-\nu & \nu & & & \\ \sigma & -(\nu+\sigma) & \nu & & \\ & & -(\nu+2\sigma) & \nu & \\ & & & \ddots & \ddots\end{pmatrix},$$

$$\mathbf{D}_1=\begin{pmatrix}0 & & & & \\ \sigma & 0 & & & \\ & 2\sigma & 0 & & \\ & & 3\sigma & 0 & \\ & & & \ddots & \ddots\end{pmatrix},$$

となる（空白部分は0をあらわす）．メンバーは，ν のレートで新規参加するが，鍵の更新処理は起こらな

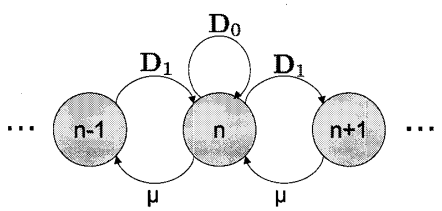

図2 $MAP/M/1$ 待ち行列の状態遷移図

い．脱退は，$i\sigma$のレートで起こり，こちらは鍵の更新を伴う．

$M/M/1$待ち行列と同様に，定常状態方程式のz変換を考える．ベクトルの形で$\boldsymbol{\pi}_n$のz変換を次のように定義する．

$$\boldsymbol{\pi}(z)=(\pi_0(z), \pi_1(z), \cdots, \pi_i(z), \cdots)=\sum_{n=0}^{\infty}\boldsymbol{\pi}_n z^n.$$

定常状態方程式(8)は，

$$\mu\left(1-\frac{1}{z}\right)\boldsymbol{\pi}_0+\boldsymbol{\pi}(z)\left\{\mathbf{D}_0+\mathbf{D}_1 z-\mu\left(1-\frac{1}{z}\right)\mathbf{I}\right\}=\mathbf{0}, \quad (9)$$

と変換される．微分する前に，とりあえずそのまま$z\to 1$としてみると，

$$\boldsymbol{\pi}(1)(\mathbf{D}_0+\mathbf{D}_1)=\mathbf{0}, \quad (10)$$

となる．$\mathbf{D}_0+\mathbf{D}_1$は，$M/M/\infty$待ち行列の遷移レート行列なので，$\boldsymbol{\pi}(1)$が，その定常周辺確率分布になっていることを示している．次に，(9)をzについて一階微分し，$z\to 1$の極限をとれば，

$$\mu\boldsymbol{\pi}_0+\boldsymbol{\pi}'(1)(\mathbf{D}_0+\mathbf{D}_1)+\boldsymbol{\pi}(1)(\mathbf{D}_1-\mu\mathbf{I})=\mathbf{0}, \quad (11)$$

が得られる．(3)と異なり，$\boldsymbol{\pi}'(1)$の項が残っているが，心配無用である．両辺に右側から$\mathbf{1}=(1, 1, 1, \cdots)^T$をかけると，$(\mathbf{D}_0+\mathbf{D}_1)\mathbf{1}=\mathbf{0}$となり，きちんと消滅する．また，$\boldsymbol{\pi}_0\mathbf{1}=P\{N(t)=0\}$，$\boldsymbol{\pi}(1)\mathbf{1}=1$に注意すれば，$M/M/1$待ち行列と同様に，$MAP/M/1$待ち行列の使用率$\rho$は，

$$\rho=P\{N(t)>0\}=\frac{\lambda}{\mu}, \quad (12)$$

で与えられることがわかる．ここで，$\lambda=\boldsymbol{\pi}(1)\mathbf{D}_1\mathbf{1}$は，暗号通信における鍵の更新レート（実は$\nu$に等しい）であり，$MAP/M/1$待ち行列へのジョブの到着レートに相当する．

さて，一階微分の次は，二階微分である．(9)を二階微分し，$z\to 1$の極限をとる．すると，

$$-2\mu\boldsymbol{\pi}_0+\boldsymbol{\pi}''(1)(\mathbf{D}_0+\mathbf{D}_1)+2\boldsymbol{\pi}'(1)(\mathbf{D}_1-\mu\mathbf{I})+2\boldsymbol{\pi}(1)\mu=\mathbf{0},$$

となる．さきほどと同様に右側から$\mathbf{1}$をかければ，$\boldsymbol{\pi}''(1)$の項は消滅する．整理すると，$M/M/1$待ち行列の(5)に相当する．

$$-\mu\boldsymbol{\pi}_0\mathbf{1}+\boldsymbol{\pi}'(1)(\mathbf{D}_1-\mu\mathbf{I})\mathbf{1}+\mu=0, \quad (13)$$

が得られる．ここから，$\boldsymbol{\pi}'(1)$について解いて，$N(t)$の期待値が得られそうだが，話は，そう簡単ではない．$\mathbf{D}_1-\mu\mathbf{I}$というやっかいなものが，$\boldsymbol{\pi}'(1)$と$\mathbf{1}$の間に挟まっている．とりあえず，もう少し整理すると，

$$\boldsymbol{\pi}'(1)\mathbf{D}_1\mathbf{1}=\mu(E[N(t)]-\rho) \quad (14)$$

が得られるが，やはり，余分な$\mathbf{D}_1$が挟まっている．

そこで，$MAP/M/1$待ち行列では，$M/M/1$待ち行列と違ったテクニックが必要となる．少し遡って，一階微分の(11)を書き換えると，

$$\boldsymbol{\pi}'(1)(\mathbf{D}_0+\mathbf{D}_1)=\mu(\boldsymbol{\pi}(1)-\boldsymbol{\pi}_0)-\boldsymbol{\pi}(1)\mathbf{D}_1, \quad (15)$$

となる．天下り的だが，両辺に$\boldsymbol{\pi}'(1)\mathbf{1}\boldsymbol{\pi}(1)$を加え，$\mathbf{A}=\mathbf{D}_0+\mathbf{D}_1+\mathbf{1}\boldsymbol{\pi}(1)$とおくと，

$$\boldsymbol{\pi}'(1)\mathbf{A}=\boldsymbol{\pi}'(1)\mathbf{1}\boldsymbol{\pi}(1)+\mu(\boldsymbol{\pi}(1)-\boldsymbol{\pi}_0)-\boldsymbol{\pi}(1)\mathbf{D}_1, \quad (16)$$

が得られる．$\mathbf{A}$は，ちょうど$\boldsymbol{\pi}(1)$を不動点とする行列で，逆行列も持つこともわかる．$\mathbf{A}$の逆行列$\mathbf{A}^{-1}$を両辺の右側からかけると，

$$\boldsymbol{\pi}'(1)=\boldsymbol{\pi}'(1)\mathbf{1}\boldsymbol{\pi}(1)+\{\mu\boldsymbol{\pi}(1)-\mu\boldsymbol{\pi}_0-\boldsymbol{\pi}(1)\mathbf{D}_1\}\mathbf{A}^{-1}, \quad (17)$$

となり，ようやく$\boldsymbol{\pi}'(1)$が得られた．しかし，このまま，右側から$\mathbf{1}$をかけても，残念ながら$\boldsymbol{\pi}'(1)$は消えてしまう．そこで，(17)の右側から$\mathbf{D}_1\mathbf{1}$をかける．すると，

$$\boldsymbol{\pi}'(1)\mathbf{D}_1\mathbf{1}=\lambda E[N(t)]+\{\mu\boldsymbol{\pi}(1)-\mu\boldsymbol{\pi}_0-\boldsymbol{\pi}(1)\mathbf{D}_1\}\mathbf{A}^{-1}\mathbf{D}_1\mathbf{1}, \quad (18)$$

となる．ここで，先ほどの(14)の出番だ．$\boldsymbol{\pi}'(1)\mathbf{D}_1\mathbf{1}$がうまく消去できる．まとめると，ちょっと複雑だが，平均系内数$E[N(t)]$に対して，次のような式が得られる．

$$E[N(t)]=\frac{\rho}{1-\rho}+\frac{1}{1-\rho}\left\{\boldsymbol{\pi}(1)-\boldsymbol{\pi}_0-\frac{1}{\mu}\boldsymbol{\pi}(1)\mathbf{D}_1\right\}\mathbf{A}^{-1}\mathbf{D}_1\mathbf{1}, \quad (19)$$

$M/M/\infty$を位相として持つ$MAP/M/1$待ち行列を例にとりながら，(19)を導いたが，ここまでは，どんな$MAP/M/1$待ち行列でも成立する．$M/M/\infty$を位相として持つ$MAP/M/1$待ち行列ならば，さらに先に進むことができる．

4. 記憶の失われた$MAP/M/1$待ち行列

さて，今更だが（鋭い読者ならば既にお気づきかもしれない），ここまで扱ってきた$M/M/\infty$を位相として持つ$MAP/M/1$待ち行列は，積形式解を持つ．ちょうど，$M/M/\infty+M/M/1$のタンデム待ち行列に相当している．$M/M/\infty$の入力レートνは，そのまま$M/M/1$の入力レートλと等しくなる．定常状態方程式(8)は，$M/M/\infty$と$M/M/1$の積形式解

$$\pi_{ni}=\frac{(\nu/\sigma)^i}{i!}e^{-\nu/\sigma}\times(1-\nu/\mu)(\nu/\mu)^n, \quad (20)$$

を持つ．z変換で表示すれば，

$$\boldsymbol{\pi}(z)=\frac{\mu-\nu}{\mu-\nu z}\boldsymbol{\pi}(1), \quad (21)$$

となる．$\boldsymbol{\pi}(1)$は，平均ν/σのPoisson分布を表すベ

クトルであり，具体的には，

$$\boldsymbol{\pi}(1)=e^{-\nu/\sigma}\left(1,\ \nu/\sigma,\ \frac{(\nu/\sigma)^2}{2!},\ \cdots\right) \tag{22}$$

である．また，$\boldsymbol{\pi}_0=(1-\rho)\boldsymbol{\pi}(1)$ である．実際，

$$\boldsymbol{\pi}(z)\mathbf{D}_0=-\nu\boldsymbol{\pi}(z),$$
$$\boldsymbol{\pi}(z)\mathbf{D}_1=\nu\boldsymbol{\pi}(z), \tag{23}$$

に注意すれば，積形式解(21)が(9)を満たすことは容易にわかる．さらに，$\boldsymbol{\pi}(1)\mathbf{A}^{-1}=\boldsymbol{\pi}(1)$ に注意すれば，

$$\boldsymbol{\pi}(1)\mathbf{D}_1\mathbf{A}^{-1}\mathbf{D}_1\mathbf{1}=\nu^2, \tag{24}$$
$$\mu\boldsymbol{\pi}_0\mathbf{A}^{-1}\mathbf{D}_1\mathbf{1}=\mu\nu(1-\rho) \tag{25}$$

がわかる．これらを代入すると，実は，複雑に見えた(19)の第2項は消滅し，$M/M/1$ 待ち行列の場合と同様に

$$E[N(t)]=\frac{\rho}{1-\rho}, \tag{26}$$

となっていることがわかる．

もったいぶって，Poisson 到着を MAP に拡張したのだが，このような $M/M/\infty$ の位相を持つ MAP は，記憶を持たない Poisson 到着と等価であることがわかった．

5. さらに *BMAP/M/1* 待ち行列

これまでは，グループ脱退時に鍵の変更ジョブが一つ生じることを，暗黙のうちに仮定していた．鍵の変更処理は，グループを構成する全員へ行うので，グループサイズ $I(t)$ のジョブが一斉に生じると考える方が自然であろう[4]．集団到着サイズの記憶を持つ集団到着へ MAP を拡張した Batch Markovian Arrival Process (BMAP) である．BMAP の場合には，一つのジョブの到着にあたる遷移レート行列 $\mathbf{D}_1$ だけではなく，i 個のジョブの集団到着にあたる遷移レート行列 $\mathbf{D}_i$ が新たにモデルに加わる（図3の *BMAP/M/1* 待ち行列の状態遷移図参照）．$\mathbf{D}_i$ は，グループサイズが $i+1$ のときに，レート $(i+1)\sigma$ で脱退が起こり，残りのグループ員への鍵の変更が生じることを表す．具体的には，$i\geq 1$ に対して，

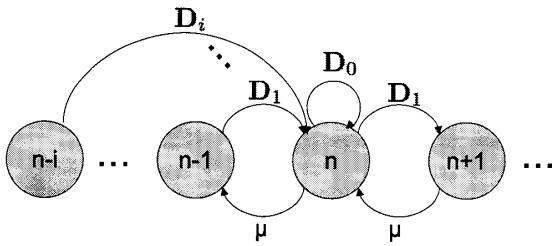

図3　*BMAP/M/1* 待ち行列の状態遷移図

$$\mathbf{D}_i=i+1\begin{pmatrix} & & i & \\ & & \vdots & \\ \cdots & & (i+1)\sigma & \end{pmatrix}, \tag{27}$$

であり，また $\mathbf{D}_0$ だけは，ちょっと特殊だが，

$$\mathbf{D}_0=\begin{pmatrix} -\nu & \nu & & & \\ \sigma & \nu-\sigma & \nu & & \\ & 0 & -\nu-2\sigma & \nu & \\ & & \ddots & \ddots & \ddots \end{pmatrix}, \tag{28}$$

となる．

BMAP/M/1 待ち行列であっても，基本的な取り扱いは $M/M/1$ 待ち行列，*MAP/M/1* 待ち行列となんら変わりない．z 変換型を微分するといろいろな情報が得られる．

MAP/M/1 待ち行列の定常状態方程式の z 変換(9)の $\mathbf{D}_0+\mathbf{D}_1 z$ が，

$$\mathbf{D}(z)=\sum_{i=0}^{\infty}z^i\mathbf{D}_i \tag{29}$$

に置き換わり，*BMAP/M/1* 待ち行列の定常状態方程式の z 変換は，下記のように拡張される．

$$\mu\left(1-\frac{1}{z}\right)\boldsymbol{\pi}_0+\boldsymbol{\pi}(z)\left\{\mathbf{D}(z)-\mu\left(1-\frac{1}{z}\right)\mathbf{I}\right\}=\mathbf{0}. \tag{30}$$

$\mathbf{D}(z)$ は，到着を表す遷移レート行列 $\mathbf{D}_i$ の z 変換であり，特に，

$$\mathbf{D}(1)=\sum_{i=0}^{\infty}\mathbf{D}_i \tag{31}$$

は，再び $M/M/\infty$ 待ち行列の遷移レート行列となる．$\boldsymbol{\pi}(1)$ は，位相 $I(t)$ の周辺確率分布だが，(30)で $z\to 1$ とすることで，$\boldsymbol{\pi}(1)\mathbf{D}(1)=\mathbf{0}$ を満たし，平均 ν/σ の Poisson 分布を表すベクトルとなることがわかる．ジョブの到着レート λ は，

$$\lambda=\boldsymbol{\pi}(1)\mathbf{D}'(1)\mathbf{1}=\boldsymbol{\pi}(1)\sum_{i=0}^{\infty}i\mathbf{D}_i\mathbf{1}=\frac{\nu^2}{\sigma}, \tag{32}$$

だが，これは，ちょうど「平均グループサイズ (ν/σ) ×脱退レート (ν)」に相当する．

(30)を一階微分して，$z\to 1$ とすると，

$$\mu\boldsymbol{\pi}_0+\boldsymbol{\pi}'(1)\mathbf{D}(1)+\boldsymbol{\pi}(1)(\mathbf{D}'(1)-\mu\mathbf{I})=\mathbf{0}, \tag{33}$$

となり，$\mathbf{D}(1)\mathbf{1}=\mathbf{0}$ に注意しながら，いつのものように両辺の右側から $\mathbf{1}$ をかけると，使用率 ρ が得られ，

$$\rho=P\{N(t)>0\}=\frac{\lambda}{\mu}=\frac{\nu^2}{\sigma\mu}, \tag{34}$$

となる．

さて，次は $E[N(t)]$ を求めよう．まず，(30)を二階微分する．*MAP/M/1* 待ち行列では，$\mathbf{D}''(1)$ に相当する項は消滅していたが，*BMAP/M/1* 待ち行列では生

き残り，

$$-\mu\boldsymbol{\pi}_0\mathbf{1}+\frac{1}{2}\boldsymbol{\pi}(1)\mathbf{D}'(1)\mathbf{1}$$
$$+\boldsymbol{\pi}'(1)(\mathbf{D}'(1)-\mu\mathbf{I})\mathbf{1}+\mu=0,$$

となる．整理すると，

$$\boldsymbol{\pi}'(1)\mathbf{D}'(1)\mathbf{1}=\mu(E[N(t)]-\rho)-\frac{1}{2}\boldsymbol{\pi}(1)\mathbf{D}''(1)\mathbf{1} \quad (35)$$

が得られる．一方，(33)で，$\mathbf{A}=\mathbf{D}(1)+\mathbf{1}\boldsymbol{\pi}(1)$ とすると，$\mathbf{D}_1$ の部分が $\mathbf{D}'(1)$ に拡張され，(18)とまったく同様に，

$$\boldsymbol{\pi}'(1)\mathbf{D}'(1)\mathbf{1}=\lambda E[N(t)]+\{\mu\boldsymbol{\pi}(1)-\mu\boldsymbol{\pi}_0$$
$$-\boldsymbol{\pi}(1)\mathbf{D}'(1)\}\mathbf{A}^{-1}\mathbf{D}'(1)\mathbf{1}, \quad (36)$$

が得られる．これら二つの式を使うと，$BMAP/M/1$ 待ち行列の $E[N(t)]$ が

$$E[N(t)]=\frac{\rho}{1-\rho}+\frac{1}{2\mu(1-\rho)}\boldsymbol{\pi}(1)\mathbf{D}''(1)\mathbf{1}$$
$$+\frac{1}{1-\rho}\left\{\boldsymbol{\pi}(1)-\boldsymbol{\pi}_0-\frac{1}{\mu}\boldsymbol{\pi}(1)\mathbf{D}'(1)\right\}\mathbf{A}^{-1}\mathbf{D}'(1)\mathbf{1}, \quad (37)$$

で与えられることがわかる．

前節で扱った積形式解が存在する $MAP/M/1$ 待ち行列の場合には，$\mathbf{A}^{-1}$ を陽に計算せず，うまく処理できたが，残念ながら，$BMAP/M/1$ 待ち行列ではうまくいかない．有限位相の $BMAP/M/1$ 待ち行列では，数値的に $\mathbf{A}$ の逆行列を求めるところであるが，$M/M/\infty$ という無限状態の位相を持つ $BMAP/M/1$ 待ち行列では難しい．そこで，$\boldsymbol{\pi}(z)=(\pi_0(z), \pi_1(z), \cdots, \pi_i(z), \cdots)$ を，さらにもう一度 z 変換して計算を進める．すなわち

$$\pi(z, y)=\sum_{i=0}^{\infty}\pi_i(z)y^i, \quad (38)$$

とする．この z 変換によって，$\mathbf{A}=\mathbf{D}(1)+\mathbf{1}\boldsymbol{\pi}(1)$ に，A というオペレータ，

$$Af(y)=\sigma(1-y)f_y(y)-\nu(1-y)f(y)+f(1)\pi(1, y) \quad (39)$$

が対応する．$\boldsymbol{\pi}(1)$ は Poisson 分布なので，対応して $\pi(1, y)=e^{\nu(y-1)/\sigma}$ である．さらに，オペレータ A の逆写像は，

$$A^{-1}g=\pi(1, y)\left\{g(1)-\int_y^1\frac{g(u)e^{-\frac{\nu}{\sigma}(u-1)}-g(1)}{\sigma(1-u)}du\right\}, \quad (40)$$

と陽に書き表せることがわかる．また，$\mathbf{D}'(1)$，$\mathbf{D}''(1)$ には，

$$D'(1)f(y)=\sigma y f_{y^{(2)}}(y), \quad (41)$$
$$D''(1)f(y)=\sigma y^2 f_{y^{(3)}}(y), \quad (42)$$

というオペレータがそれぞれ対応する．これらの対応関係を使うと，少し計算は大変だが[4]，結局(37)の未知項として

$$\boldsymbol{\pi}(1)\mathbf{D}''(1)\mathbf{1}=D''(1)\pi(1, y)|_{y=1}=\nu\left(\frac{\nu}{\sigma}\right)^2, \quad (43)$$

$$\boldsymbol{\pi}(1)\mathbf{D}'(1)\mathbf{A}^{-1}\mathbf{D}'(1)\mathbf{1}=D'(1)A^{-1}D'(1)\pi(1, y)|_{y=1}$$
$$=\nu(\nu-1)\left(\frac{\nu}{\sigma}\right)^2, \quad (44)$$

さらに，

$$\mu\boldsymbol{\pi}_0\mathbf{A}^{-1}\mathbf{D}'(1)\mathbf{1}=\mu D'(1)A^{-1}\pi(0, y)|_{y=1}$$
$$=\mu\rho(1-\rho)+\frac{1}{2}\left\{3\left(\frac{\nu}{\sigma}\right)^2-2\left(\frac{\nu}{\sigma}\right)\pi_y(0, 1)\right.$$
$$\left.-\pi_{y^{(2)}}(0, 1)\right\}, \quad (45)$$

が得られる．しかし，この計算も十分とはいえない．残念ながら，未知量 $\pi_y(0, 1)$ と $\pi_{y^{(2)}}(0, 1)$ が含まれてしまっている．通常の $BMAP$ の計算では，やはり行列に対する数値計算で $\boldsymbol{\pi}_0$ を求めるのだが，無限の位相を持つ $BMAP$ では使えない．ここでは，その代わりに，

$$0\leq\pi_y(0, 1)\leq E[I(t)]=\nu/\sigma, \quad (46)$$
$$0\leq\pi_{y^{(2)}}(0, 1)\leq E[I(t)(I(t)-1)]=(\nu/\sigma)^2 \quad (47)$$

というかなり大雑把な不等式を使う．すると，$BMAP/M/1$ 待ち行列におけるジョブの系内数の期待値の上下限が次のように得られる．

$$E[N(t)]\leq\frac{\rho}{1-\rho}+\frac{3\rho(\nu/\sigma)(1-\nu/\sigma)}{2(1-\rho)}, \quad (48)$$

$$E[N(t)]\geq\left[\frac{\rho}{1-\rho}+\frac{3(\nu/\sigma)\{\rho-(1-\rho)(\nu/\sigma)\}}{2(1-\rho)}\right]^+, \quad (49)$$

ここで，$x^+=max(x, 0)$ とする．

6. セキュリティの評価

すっかり，数学モデルの細部に時間をかけてしまったが，せっかくの暗号通信のモデルなので，セキュリティを評価してみよう．グループ内での暗号通信を，秘密鍵の共有方式で行う場合，鍵の更新ジョブが終了するまで古い鍵を使わざるを得ない．その時間 W が長ければ長いほど，盗聴などセキュリティ上の問題が生じる可能性がある．(48)と(49)で，鍵の更新ジョブの系内数の期待値の上下限が得られているので，Little の公式[1][7]を使えば，セキュリティ悪化時間の期待値 $E[W]$ の上下限が得られる．ジョブのサービスレートを $\mu=100,000$ とした場合の $E[W]$ の数値例を図4に示す．

グループへの参加レート ν が大きくなれば，鍵の更新レート $\lambda=\nu^2/\sigma$ が大きくなり，セキュリティの悪化時間が大きくなる．σ が大きくなれば，参加から脱退までの時間が短くなり，グループサイズが小さくなる．そのため，高い参加レートであっても，セキュリ

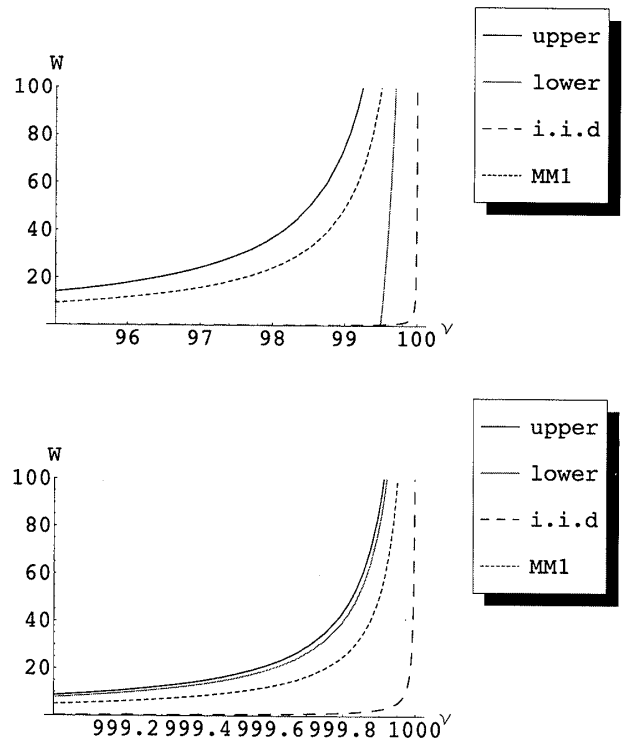

図4　セキュリティの悪化時間：上が $\sigma=1$，下が $\sigma=100$ の場合の $E[W]$．"upper" と "lower" はそれぞれ，$E[W]$の上限，下限を表す．"i.i.d" は独立なバッチサイズ X を持つ $M^{[X]}/M/1$ 待ち行列，MM 1 は，同じ使用率を持つ $M/M/1$ 待ち行列でモデル化した場合の $E[W]$ の推定値を表す．どちらも過小評価の傾向がみられる．

ティは悪化しない．また，この暗号通信を，もっと簡易な待ち行列である

1. 平均 ν/σ の Poisson 分布に従う i.i.d のバッチサイズ X を持つ $M^{[X]}/M/1$ 待ち行列（i.i.d）
2. 同じ使用率を持つ $M/M/1$ 待ち行列（MM1）

でモデル化した場合も比較している．記憶を持たない集団到着モデル $M^{[X]}/M/1$ 待ち行列や使用率だけ合わせた $M/M/1$ 待ち行列では，セキュリティの悪化時間を過小評価してしまい，きちんとセキュリティが評価できていないことが，図4からもわかる．

参考文献

[1] L. Kleinrock. *Queueing Systems Vol. 1.* John Wiley and Sons, 1975.

[2] G. Latouche and V. Ramaswami. *Introduction to Matrix Analytic Methods in Stochastic Modeling.* SIAM, 1999.

[3] S. A. Thomas. *SSL and TLS Essentials : Securing the Web.* John Wiley and Sons, 2000.

[4] H. Toyoizumi. An infinite phase-size BMAP/M/1 queue and its application to secure group communication. In *SECRYPT*, pp. 283-288, 2006.

[5] H. Toyoizumi and M. Takaya. Performance evaluation of secure group communication. *Journal of the Operations Research Society of Japan*, 47(1): 38-50, 2004.

[6] D. Wallner, E. Harder and R. Agee. Key management for multicast : Issues and architectures. *Request for Comments : 2627*, 1999.

[7] R. Wolff. *Stochastic modeling and the theory of queues.* Princeton-Hall, 1989.

[8] C. Wong, M. Gouda and S. Lam. Secure group communications using key graphs. *IEEE/ACM Trans. on Networking*, 8(1): 16-30, 2000.

[9] 牧本直樹．待ち行列アルゴリズム—行列解析アプローチ．朝倉書店，2001.