Vol.2010-EIP-48 No.13
2010/5/28

クラウドコンピューティングのセキュリティ問題へのナッシュ均衡と確率モデル適用の最近の動向

金子 格†

クラウドコンピューティング上のマッシュアップはセキュリティの問題をより複雑にし、そこに含まれる一つのサービスの停止の影響範囲を拡大している。そして，システムが多数のユーザーにより構成されることにより炎上や DOS 攻撃など，新しいカテゴリーの障害の可能性も拡大している．このようなシステムの問題を予見的に分析することは喫緊の課題である。それにはナッシュ均衡と確率モデルが最も直截な手法と考える。同様の考えを持つと思われる他研究者の研究動向を紹介しつつ、手法の有効性を検討する。

Applying Nash equilibrium and probabilistic model on security problem of cloud computing

Itaru Kaneko†

Evolution and expansion of mash up applications in the cloud computing complicate security problems and increase the influence of the failure of single service within the system to other part. It is an urgent problem to establish the analysis method of the failure of such system. Nash equilibrium and probabilistic modeling are the possible tool to analyze such problem. We examine the effectiveness of those technique by reviewing research project using such techniques.

† 東京工芸大学 工学部コンピュータ応用学科

1. はじめに

クラウドコンピューティングの拡大はパソコン登場以来のパラダイムシフトをもたらしつつある．クラウドコンピューティングではサービス，インフラストラクチャー，プラットフォーム，ストレージがそれぞれ独立に提供され，標準インタフェースによる相互運用を可能とする．また相互運用が可能となった様々なサービスを自由に融合(マッシュアップ)し，次々と新しい応用が創出されている．クラウドコンピューティングとマッシュアップは今日，最新の否ターネットサービス実現手法のシンボルになっている．

このようにクラウドコンピューティングはすでに重要な社会基盤であり，このシステムに生じる様々な障害や問題を事前に予見し制御する手法の確立は，重要かつ緊急性の高い課題である．しかし，クラウドコンピューティングが複雑で大きなシステムになり，マッシュアップにより応用や利害関係者が多様化し安全性要件が複雑化する中で，その障害や問題を事前に予見，制御する手法が確立しているとは言い難い．

筆者等は従来より，多数の利害関係者や要素からなる複雑なセキュリティ問題を扱うために，ゲーム理論(特にナッシュ均衡モデル)と確率モデルの併用を提案してきた．これらの手法はクラウドコンピューティングにおけるセキュリティ問題の分析にも有効と考える．また実際，クラウドコンピューティングにこれらの手法を適用する提案が多くみられるようになってきた．本報告ではこれらの事例を紹介し，このようなアプローチの有用性を示す．

2. クラウドコンピューティングのセキュリティ

2.1 クラウドコンピューティングの定義

まずクラウドコンピューティングとは何かを確認しよう．

ウィキペディアによると，「「クラウド」（雲）は、ネットワーク（通常はインターネット）を表す。従来より「コンピュータシステムのイメージ図」ではネットワークを雲の図で表す場合が多く、それが由来と言われている」[1]．“Cloud computing”という呼称を含む最も古い文献を cinii および ACM のデジタルライブラリで調べると，cinii においては日経エレクトロニクスの記事[2]が，ACM デジタルライブラリにおいては Chellappa の INFORMS1997 の発表[3]が確認できる．日経エレクトロニクスの記事が SaaS に関するもので Chellapa の発表にも SaaS に類する言及があることから SaaS を主体とした構成であると解釈するのが適当と思われる．本報告ではクラウドの定義を，物理的な形態をあらわすものではなく，サービス，インフラストラクチャー，プラットフォーム，ストレージがそれぞれ分散独立管理される運用形態，ビジネスモデルとして定義することにする．

2.2 クラウドコンピューティング固有のセキュリティ問題

2009 年シカゴで開催された”ACM workshop on Cloud computing security”では 4 つのセッションでは計 14 件の発表があった．セッション 1 “Connecting to the web 2.0”では Spam および Abuse の問題, SSL とトラフィック管理の問題に関する発表等があった．セッション 2 “Clouds and data outsourcing”ではクラウド特有のデータアウトソーシングに関する発表があった．セッション 3” New challenges”ではリソース管理やデータアウトソーシングの問題，VM セキュリティ問題等に関する発表があった．セッション 4” Applications”では医療などの応用に関する発表があった．

これらの発表から，クラウドコンピューティングの分野で現在着目されている課題をいくつか抽出してみよう．以下にあげる要素がクラウドコンピューティング特有であると考えられるのではないか．

(1) サービス，インフラストラクチャー，プラットフォーム，ストレージが独立運用されることによる問題

(2) ネットワーク上を交錯する膨大なトランザクションの問題

(3) 多様な用途(たとえば医療情報)などを扱うことによる要求条件の多義性, 曖昧性

たとえば VM セキュリティに関する課題等は(1)のカテゴリーに含まれる課題と考えられる．また SPAM や DOS 攻撃等に関する問題は(2)のカテゴリーに含まれる課題と考えられる．医療用途などでは(3)が課題になると考えられる．

2.3 クラウドコンピューティングにおけるセキュリティ問題の特徴

次にクラウドコンピューティングのセキュリティ問題の特徴を形式的に記述する．

まずクラウドコンピューティングの構成を形式的に記述する．これまであげた構成から以下のように記述することができる．

(1) サービス(A), インフラストラクチャー(I), プラットフォーム(P), ストレージ(D)がそれぞれ独立な運営主体によって提供され得る．さらにこれらから最終的なサービスを受けるユーザ(U)が存在する．

(2) クラウドコンピューティングのには多数の S, I, P, D, U が含まれる．

構成要素: $C_i \in \{A_i, I_k, P_l, D_m, U_n\}$

各要素の状態: $Sc_i=\{sc_{i,j}\}$

全体の状態:$X=\Pi S_i,\ x \in X$

状態遷移: $t_{ij}=(x_i,x_j)$

と記述できる．

次にセキュリティに関する条件を形式的に記述する．

セキュリティが保たれていることは，セキュリティが保たれている状態から不良状態への遷移がない，と定義出来るだろう．f(x)をシステムのセキュリティが不良な場合に非零となる関数であるとすれば，以下のようにあらわすことが可能である．

$\forall t_{ij}=(x_i,x_j), f(x_i)=0 : f(x_j)=0$ -(式 1)

クラウドコンピューティングにおいては多様な用途，多様な利害関係者が存在する．たとえば医療情報であれば，公的ない医療情報へのアクセス権やプライバシーなど新しい利害関係が関係する．利害関係者毎に多様なセキュリティ条件を持ち得る．したがって，利害関係者を r とすると利害関係者毎にそれぞれ異なる安全性の要求条件があるので以下のようにあらわされる．

$f_r(x)$

したがって，すべての r にとってセキュアなシステムの条件は

$\forall t_{ij}=(x_i,x_j), f_r(x_i)=0 : f_r(x_j)=0$ -(式 2)

となる．

クラウドコンピューティングの構成要素$\{S_i,I_j,P_k,D_l,U_m\}$はそれぞれ独立に提供，運用，管理される．したがって T には利害関係者にとって直接確認できる部分とそうでない部分が含まれる．

T のうち利害関係者 r から見える部分を T の r から見た視野と呼ぶことにし T_{r+}であらわす．R から見えない部分を r からの死角と呼ぶことにして T_{r-}とあらわす．

$T= T_{r+} \cup T_{r-}$

である．

具体的には，利用者にとってオペレーティングシステムがある条件を満たすかどうか知る由もない．サービス提供者にとって，利用者のクライアントソフトウエアの挙動は特定できない．他の多くの部分についても同様である．また，積極的に多数のマッシュアップを利用している利用者にとって，利用しているサービスの品質や安定性にはかなりのばらつきがある．またサービス提供者からみると，利用者の挙動は予測がつかない．

クラウドコンピューティングのセキュリティの特徴は以下 2 点であると考えられる．

(1) $f_r(x)$が r をパラメータとし，かつ随時変化する

(2) $T= T_{r+} \cup T_r$ において T_rの部分が大きい

このような不確定要素の多い状況での安全性の議論は，たとえば初期の小規模なプログラムの機能保証の問題に慣れた読者にとっては異質で，違和感を持つかもしれない. しかしクラウドコンピューティングの状況下ではむしろ自然なことと考えられる．また，一般的なエンジニアリングの世界ではむしろ構成要素に一定のばらつきがある方が普通の状況である．機械工学においても建築学においても，また電気工学においても，構成要素や環境のばらつきは当然想定され，その中で満たすべき安全性の条件を保証することが求められる．筆者等が目指すのは，バラつきを前提としながら，全体としてはある数値的水準を満たすことが保証されるような分析，設計手法である．

Vol.2010-EIP-48 No.13
2010/5/28

3. ナッシュ均衡と統計モデル

本報告では，ナッシュ均衡と統計モデルの利用について検討する．これらはよく知られた概念であるが，簡単に説明する．

3.1 ナッシュ均衡

ナッシュ均衡はゲーム理論の非均衡モデルにおいて想定される安定解の一つである．

表 1　ナッシュ均衡の例
Table 1　An example of Nash equilibrium

B / A	選択 B1	選択 B2
選択 A1	4,5	0,5
選択 A2	3,1	3,4

(A1,B1)は A，B いずれかが戦略を変更しても戦略を変更した側にとって不利益になる．このような解をナッシュ均衡と言う．(A1, B1)は双方が最大の利得を得られる選択，すなわち最適解であるが，ナッシュ均衡は最適解である必要はない． (A2,B2)も A，B いずれかが戦略を変更すると戦略を変更した側の不利益になる．このような解もナッシュ均衡に含まれる．

クラウドコンピューティングにおいてナッシュ均衡は T の死角，T_rの推定と制御に利用できる．たとえば SaaS を利用したサービス事業者にサービスを受けている利用者にとって，SaaS の安全性もサービスの安全性も死角に含まれる．SaaS とサービス事業者の双方がお互いの信頼性についてある程度の基準を設けていれば，どちらかが基準を満たさなかった場合に不利益をこうむるから，利用者は間接的に安全性を期待できる．しかし SaaS 提供者の欠陥をサービス提供者があえて黙認するという状態もナッシュ均衡となるかもしれない．どうすればそのような可能性を減ずることが可能かもナッシュ均衡の分析により明らかになる．

3.2 確率モデル

T は膨大かつあいまいであるので，確率的に扱う必要が生じる．特に利用者の挙動は実際的には確率的にのみ扱うことができる．

崖を登り降りすることはほとんどの人にとって危険に見合う利益のない全く非合理な行動であるが，多数の人数が崖に接すれば，落ちる危険を冒して崖を登る人間が一定数あらわれる．人生いろいろ人それぞれである．

セキュリティを確率的に扱った場合に，達成すべき目標は確率的な数値目標になる．たとえばシステムの壊滅的な被害の確率はほぼ零でなければならない．また小さな被害であればある程度発生してもかまわないが，想定した範囲を超えた状態にシステムが陥ることは避ける必要がある．

4. ナッシュ均衡と確率モデルの適用

次に，ナッシュ均衡と確率モデルがどのように具体的にシステムの動作推定に応用できるかを簡単に説明する．以下の議論は[4]，[5]に詳しく述べている．

4.1 動的確率的 PL モデル

SNS のような環境で，特定の利用者がある試行を繰り返す場合を考える．

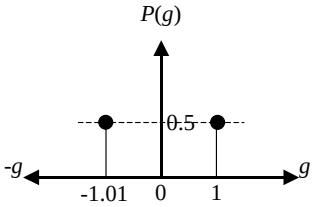

図 1　利得確率分布の例-
Figure 1　An example of a payoff probability distribution.

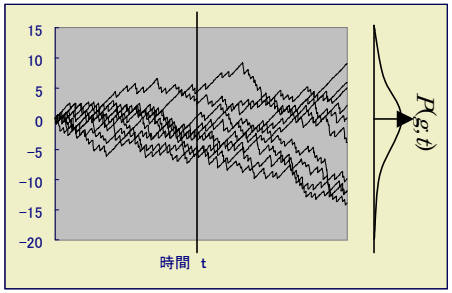

図 2　試行をくり返した場合の利得の推移
Figure 2　The trajectory of the payoff after repeating of series of the trial.

このような状況で利用者の行動をいかに予測するかについて考える．一つの手がかりとして，利用者が利得を最大化すると仮定することが考えられる．しかし，利得を最大化する行動がとられるとは限らない．

たとえば，例としてある行為を行った場合の利得が図 1 の示す確率分布になっている場合を考える．この試行の利得の期待値は-0.005 であるので，利用者が期待値に基づいて行動するのであれば，利用者はこの行動を一度もとらないと予想される．

一方，仮に利用者が数回試行をくり返した場合，利得の推移は図 2 のように推移し t 回の試行後の利得分布は P(g,t)のようになる．利用者が時刻 t まではとりあえず試行

を繰り返し，その時点での利得の累計によって利得の正負を判断するとすれば，利用者の約半数はこの行為が正の利得をもたらすと判断する．このような判断と戦略を単純回帰推定と呼ぶことにしよう．

SNS のような応用では，実際には多くの利用者が期待値が負の行為を繰り返し行う現象がみられる．したがってより多くの利用者が期待値ではなく，単純回帰推定値を採用しているとするとした方が，利用者の行動をより高精度に予測できるだろう．

4.2 交換可能性の効果

構成モジュールの交換費用と，「その部品に欠陥があった場合に確実に検査・交換されるか」，という運用上の信頼性の関係について考える．

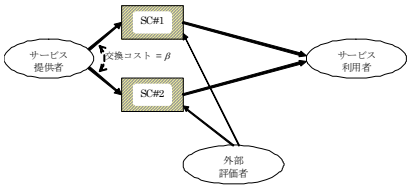

図 3　交換可能なセキュリティ部品(SC)
Figure 3　Effect of replaceable security component(SC).

図 3 においてサービス提供者は 2 種類のセキュリティ部品 SC#1 と SC#2 を交換できるものとする。2 つの SC は検査者 P により検査されている。セキュリティ不良に起因する利害のみに着目し、サービスそのものによる利益と損失は 0 としている。また、不良が発覚した場合の損失の期待値を α、SC モジュール交換の費用を β としている。この利得行列では、検査者 A は不良があった場合に報告を行わないとペナルティ $-\alpha$ を課せられるため、不良を発見するように動機付けられる。またサービス提供者 S は不良を報告された場合、通常は交換費用 β がセキュリティ不良による損失 α よりも小さいので SC モジュールの交換を行うよう動機付けられると期待される。

しかし発見された欠陥を報告しない場合に S が A に隠蔽の報償 γ を支払うとすると、ゲームマトリックスはに表 2 示すものになる。

もしも $-\alpha < -\beta$ であれば $\gamma > \alpha$ という値がナッシュ均衡となる。この均衡戦略に達すると A は a< g であるため、報告を行わない方が常に有利であり、S にとってもモジュールを交換しない方が有利となる。

この状況を避けるには交換費用が 0 であればよい．交換費用が 0 である場合の利得行列を表 4 に示す．交換費用が 0 だとモジュールを交換しない戦略はナッシュ均衡とならない．

表 2　不良のペナルティが α で交換費用が β の利得行列
Table 2　Game matrix with zero replacement cost

S＼A	報告する	報告しない
継続利用	$-\alpha$,0	0,$-\alpha$
交換	$-\beta$,0	$-\beta$, 0

表 3　協調因子が γ の利得行列
Table 3　Game matrix with zero replacement cost

S＼A	報告する	報告しない
継続利用	$-\alpha$,0	$-\gamma$,$-\alpha+\gamma$
交換	$-\beta$,0	$-\beta-\gamma$, γ

表 4　交換費用が 0 のゲームマトリックス
Table 4　Game matrix with zero replacement cost

S＼A	報告する	報告しない
継続利用	$-\alpha$,0-γ	0,$-\alpha+\gamma$
交換	0,0-γ	0,0+γ

5. クラウドにおけるナッシュ均衡と確率モデル適用の例

2010 年 4 月にダラスで開催された ICASSP2010 では，”Multimedia Social Networks: Behavior, Dynamics, Security and Beyond と題したワークショップにおいて多くの分析事例が紹介された．

W. Lin 等による P2P SNS に関する報告[6]ではビデオ共有サイトにおいてただ乗りを防止するためのインセンティブ条件をナッシュ均衡を用いて分析している．P2P SNS では資源を共有するため，参加者には他の参加者をだます選択があり，他の参加者にだまされないかという疑いがある．Lin 等はゲーム理論的な分析を行い，実現可能で参加者間の協調を支持できる利得行列を示している．

Yan Sun 等による Trust Modeling に関する報告[7]では Ad-hoc netowrk における信頼性を分散協調システム上で評価する方法を示している．信頼性を中心的な信頼性から伝搬するのではなく,情報理論的に評価することで Ad-hoc ネットワークの各ノードがそれぞれ独自に信頼性を確率的に評価することが可能となる．

W. Lin 等によるマルチメディア海賊行為における共謀の分析[8]では複数人が協調してすかし除去を行って画像を違法にアップロードする場合に協力が成立する条件に

ついて分析している．非協調ゲームの枠組みにより，共謀が起こりえる条件が示されている．

Niyato 等によるリソース管理に関する分析[9]では、クラウドコンピューティングにおけるリソース管理の問題に，ナッシュ均衡を適用している．

Reputation や Trust の評価問題はデータマイニングのタスクとして定義することもでき, コンペティションも盛んにおこなわれている. 表 5 にそのいくつかを示す. NetFlix のコンペティションでは賞金はなんと$1M(9 千万円)である．これらの課題でも本報告であげた手法を併用できそうである．

表 5　データマイニングコンペティション
Table 5　Data mining competition

Host	URL	賞金
UCSD	http://mill.ucsd.edu/	$8000
NetFlix	http://www.netflixprize.com/	$1M

6. まとめ

本稿ではクラウドコンピューティングにおけるセキュリティ問題の特徴を示し，ナッシュ均衡と確率モデルを適用する必要性と，どのような分析が可能かをを論じた．多くの不確定性を有し膨大な利用者，ツール提供者，問い合わせ処理を有するクラウドコンピューティングの分析において，ナッシュ均衡と確率モデルを利用した多くの分析事例がある．したがって，これらは有効なツールであると考えられる．

クラウドコンピューティングはすでに重要な社会基盤である．大規模な応用も多く，その障害は社会的にも重大なものとなり得る．一方でクラウドコンピューティングはいまだ急速に発展しつつある分野であり，物理的にも，運営システム上も，常にその形態は進化発展しつつあり，応用分野にもこれまでにない新しいものが次々と登場する．

このように新しい重要な応用が巨大なスケールで次々に登場する場合，社会システムを含めたその安定性や既存のシステムに対する影響を事前に高い精度で予見する必要性は高い．筆者はナッシュ均衡と確率モデルがその有力なツールになると考える．

クラウドコンピューティングにおいては今後も新しい課題が次々と生ずるだろう．これらの多くの問題に光があてられることを期待している．

参考文献

1)　「クラウドコンピューティング」『フリー百科事典　ウィキペディア日本語版』。2010 年 4 月 8 日 (木) 00:36　UTC、URL: http://ja.wikipedia.org
2)　“SaaS 最前線 クラウド・コンピューティングの正体”，日経コンピュ-タ (699), 34～37, 2008-03-15, 2008
3)　Chellappa R. Cloud computing---emerging paradigm for computing. In INFORMS 1997, Dallas, TX, 1997
4)　金子格，白井克彦，“高度デジタル AV フレームワークの多面的安全性とその特性”，情報処理学会論文誌 Vol 41, 3010-3018, 2000
5)　Itaru Kaneko, Katsuhiko Shirai, Mika Onishi,”　Probabilistic Multi-Lateral Security Model for Ubiquitous Multimedia Services”，ICDCSW04, Vol. 7, pp. 236-241,2004
6)　W. Lin et.al, “Incentive Cooperation Strategies for Peer-to-Peer Live Streaming Social Networks”, Special session on communication and Media Computing, IEEE Trans. on Multimedia, Vol. 11, No. 3, pp 396-412, April 2009
7)　Yan Sun et.al, “Information Theoretic Framework of Trust Modeling and Evaluation of ad-hoc network”, IEEE J. on Selected Area of Communications, Vol. 24, No. 2, pp. 305-317, February 2006
8)　W.Lin et.al, “Fairness Dynamics in Multimedia Colluders’ Social Network”, IEEE Int. Conf. on Image Processing (ICIP’07), San Diego, 2008
9)　Dusit Niyato, “Economic Analysis of Resource Market in Cloud Computing Environment”, Services Computing Conference, 2009. APSCC 2009，pp 156-162，　IEEE 2009