Vol.2015-DPS-162 No.41
Vol.2015-CSEC-68 No.41
2015/3/6

セキュアマルチパーティ秘密計算法におけるユーザ安心感定量化の試み
～情報システムの「安信性理論」の確立を目指して～

宮西洋太郎[†1]　韓嘯公[†2]　金岡晃[†3]　佐藤文明[†3]　北上眞二[†2]　浦野義頼[†2]　白鳥則郎[†2]

クラウドコンピューティングを利用する場合，ユーザはプログラムもデータもクラウド事業者に保管，管理，実行を委ねることになる．プログラム（情報処理のノウハウが具現したもの）やデータは企業競争力の源泉であり，企業は競争相手から，厳しく秘密を守りたい．このような点からユーザはセキュリティに関してクラウドに対して不安を払拭できないのが現状である．この対策として，従来から，セキュアマルチパーティ法による秘密分散法，秘密計算法が研究され，実用化されている．本稿では，その安全性の評価方法について提案する．すなわち，ユーザの安心感を定量化する試みである．さらに，この評価方法を一般化して，一般的な情報システムに対してユーザが安心して信頼できる度合い（安信性と仮称）を理論化することを目指している．

A Trial to Quantify about User's Sense of Safety in Multi Party Calculation
- Toward establishing "Safely Dependability Theory" of Information Systems-

Yohtaro Miyanishi[†1]　Xiaogong Han[†2]　Akira Knaoka[†3]
Fumiaki Sato[†3]　Shinji Kitagami[†2]　Yoshiyori Urano[†2]　Norio Shiratori[†2]

Users of cloud computing could not wipe away the anxiety about the data and programs may be abused or leaked, because users submit their almost whole data and programs to a cloud provider. Those data and programs usually embody the company's stored knowledge. Then they shall be key elements of core competences of the user's company. The countermeasures have been studied against the abuse or leakage of data and programs caused by cloud providers' careless or intentional crime. As one of those countermeasures, Secure Multi-party Calculation (SMC) method has been studied and used practically in some applications. We propose an evaluation method about how the SMC method is secure. And then we are aiming to establish a safety dependability theory about general information systems .

1. はじめに

近年，クラウドコンピューティングが普及しつつある．クラウドコンピューティングは計算能力を柔軟に拡大，縮小でき(scale out/in)，総合的に情報システムのコストを下げうるなどの長所がある反面，データの保管や情報処理ノウハウ(プログラム)を外部企業(クラウド事業者)に委託することに起因して，データや処理方法の不正使用や漏洩のリスクをもつという短所がある．この短所ゆえに，委託するデータやプログラムの性質によっては，ユーザは十分な安心感をもって利用することができない．

このユーザの不安感を軽減する方策として，従来は主にユーザとクラウド提供者との間で締結する SLA(Service Level Agreement)や各種のセキュリティガイダンスの遵守といった人間的要素（約束ごとや管理手法）に依存しており，技術的解決策とは言いがたかった．

一方，技術的解決策として，保存データの秘密を保持するためには，古くからデータの秘密分散法[1]が提案されている．また近年，計算結果の秘密を保持するためには，秘密計算法が提案されている．

秘密計算法には，準同型暗号を用いる方法[2]とセキュアマルチパーティによる方法[3]がある．本稿では，セキュアマルチパーティ秘密計算法(Secure Multi-party Calculation 略称 SMC)について，安全性の定量的評価方法について，提案する．ユーザの安心感は，システムの安全性の定量的指標によって評価できるという考えにたっている．

将来は，さらに，この評価方法を一般化して，一般的な情報システムに対してユーザが安心して信頼できる度合いについての理論（本稿では，安信性理論と仮称する）を確立することを目指している．

2. 技術課題

セキュアマルチパーティ秘密計算法(SMC)が研究され実用化されつつある[3]．我々も軽量型のセキュアマルチパーティ秘密計算法を提案した[4][5].

SMC は，ユーザの求める計算結果の秘密をクラウド提供者から守るために，システムの構成（ハードウェア，ソフトウェア）に，特別の仕掛けを必要とする．そのため，通常のクラウドコンピューティングシステムに比べ，追加のコストを発生する．追加のコストとは，マルチパーティを構成するためのシステム構築コスト，複数のクラウド提供者を利用するための運用コスト，またある計算をおこなう際の計算時間や通信のコストなどである．

それらのコストが，安全性の向上に見合うものかどうかユーザとして判断する必要がある．そのためには，SMC によって，どの程度の安全性を確保できるかを定量的に評価する必要がある．そこで本稿では，SMC の安全性を評価する方法を提案する．

Vol.2015-DPS-162 No.41
Vol.2015-CSEC-68 No.41
2015/3/6

提案方法の骨子は，従来の信頼性理論(Reliability Theory)は「動作中(alive)」,「故障停止(down)」といったシステムの動作状態について確率統計を用いて評価している．これに倣い，システムの「安全(safe)」と「非安全(unsafe / unsecured)」の状態について，確率統計を用いて評価する．

評価指標の例として，信頼性理論では，どの程度の期間動作中が継続するかといった指標が「平均故障間隔 MTBF(Mean Time Between Failure)」であるが，それに対応する指標として,「平均破断間隔 MTBB(Mean Time Between Break of Safety)」といった指標を提案する．この指標（次元は時間）の大きい,小さいによって安全性を評価できる．

このような理論体系を我々は「安信性理論」と仮に称することとした．どの程度安心して，信頼できるかという意味をこめている．

既存研究の調査は十分ではないが，信頼性理論に倣い安全性を定量評価する本稿のような取り組みは見当たらなかった．

3. 関連する研究

主な関連する研究を以下に述べる．

3.1 秘密分散法(secret sharing)

秘密分散法の 1 つに(k, n)閾値法がある[1]. この方法は，データを秘匿するため，秘密にすべきデータを k–1 次多項式によって変換して秘密データ（「シェア」と称される）とし，n 個のサーバに分散配置する．復元は，k 個のサーバからデータを得て，連立方程式を解くことによりなされる．

秘密分散法は個人情報(プライバシー情報)の匿名化や電子投票に応用されている．またセキュリティ問題に応用したシステムも実用化されている[6].

3.2 秘密計算法(secure computation)

秘密計算法の 1 つに，完全準同型暗号を使用した秘密計算法がある[2]. この方法では，クラウド側は暗号化されたデータをそのまま演算処理して，暗号化された計算結果を返答する．この返答を受けて，ユーザ側で暗号化された計算結果を復号して，平文の計算結果とする．よってクラウド側での，利用者データの秘密が保たれる．

上記の方法は，１つの数値データをビット列として表現するなど，通常よりも長いビット長を必要とし，まだ実用のシステムに適用するレベルには達していない[3]とされているが IBM 社からライブラリ提供の広報もなされている[7]. 今後に注目したい．

秘密計算法は，上記の完全準同型暗号を用いる方法のほかにセキュアマルチパーティによる計算法もある[3]. SMC は現時点では限定された機能で実用化されている[8].

SMC において，k out of n とは，秘密分散法に類似し，n 個のサーバのうち，k 個のサーバからの計算結果が得られれば，最終的計算結果が得られる，を意味する．

4. 前提事項

4.1 システムの安全な状態

本稿では，システムが「安全な状態(Safe State)」にあるということは，システム内に保存されているデータやプログラムが漏洩や，不正使用されないで，正常に運転を継続している状態であるものとする．今回は，特に内部犯罪者を想定し,内部犯罪者がデータやプログラムを漏洩したり，不正使用したりすることによって，システムの安全が破断(Break of Safety)されるものと想定する．したがって，安全が破断された状態が「非安全の状態(Not Safe State)」である．もちろん外部からの攻撃によってもシステムの安全性は脅かされるが，その問題は今後の検討事項とする．

SMC において，安全が破断される場合は，当該 SMC に関係する複数のクラウドの内部犯罪者が結託して，漏洩や不正使用の犯罪行為にいたる場合である．例えば 2 out of 3 の SMC において関係する 3 つのクラウド提供者のうち，2 つのクラウド提供者の内部犯罪者が悪事を結託したとき，安全が破断される．

4.2 ユーザの安心感とシステムの安全性

クラウドコンピューティングにおけるユーザの安心感は，委託する情報システムの安全性に依存するものと考える．すなわち，情報システムが安全であるほどユーザは安心して，その情報システムを利用できる．

ユーザの安心感を直接的に，定量的に表現し,「安心度(Degree of Trustable)」といった指標を得ることが望ましいが，本稿では，情報システムの安全性を定量評価すること（「安全度(Degree of Safety)」）により，それに代えている．

ユーザの安心度と情報システムの安全度との間には，単調関数的な関係があるものと考えるが，本稿では，取り扱わない．従来の信頼性理論においても，ユーザがどの程度信頼するか，といった人的感覚の定量評価の観点よりも，システムがどの程度の信頼性を有しているかという定量評価の観点であり，これに倣っている．

なお，本稿では,「安全性」という用語を一般的な意味で用いているが，具体的な議論の場合には,「安信性」といった本稿特有の用語を用いる場合がある．

4.3 関連する既存の知見

本稿に関連する既存の工学分野，あるいは知見，学問領域として，信頼性理論，待ち行列理論，犯罪心理学の分野を挙げることができる．

信頼性理論は，主にハードウェアが正常動作か故障停止かを確率過程として数理的に扱う理論である．待ち行列理論は，顧客の到着，サービスの完了，待ち時間を確率過程として数理的に扱う理論である．信頼性理論における故障の発生，修理は，待ち行列理論における顧客の到着，サービス完了にそれぞれ対応させれば，類似の学問領域とみなせる．犯罪心理学は，主に犯罪者が犯罪にいたる心理過程

Vol.2015-DPS-162 No.41
Vol.2015-CSEC-68 No.41
2015/3/6

を扱う定性的な学問領域である.

4.4 検討の方針

前記の既存分野（信頼性理論，犯罪心理学）の知見を活用して，本稿では，次の方針をとることとした.

- 情報漏洩や不正使用をおこなう内部犯罪者がシステムの安全性を破断する.
- 犯罪者が犯罪にいたる過程をシステムのハードウェアが故障する過程に対応させる.
- 犯罪の発生を確率過程と考える[9].
- 信頼性理論の各種概念を類推して適用する.

信頼性理論という用語に対応して，本稿では「安信性理論」と仮称する.

5. 信頼性理論からの類推（アナロジー）

本稿では，前述のように，犯罪者が犯罪を犯す過程をハードウェアが故障する過程から類推している．信頼性理論の諸概念が安信性理論にどのように対応づけできるかを，ここで検討する.

5.1 取り扱う対象の状態

(1) 信頼性理論の場合

信頼性理論が扱う状態は，「正常動作」と「故障停止」である．図 1 に信頼性理論が扱う状態について示す.

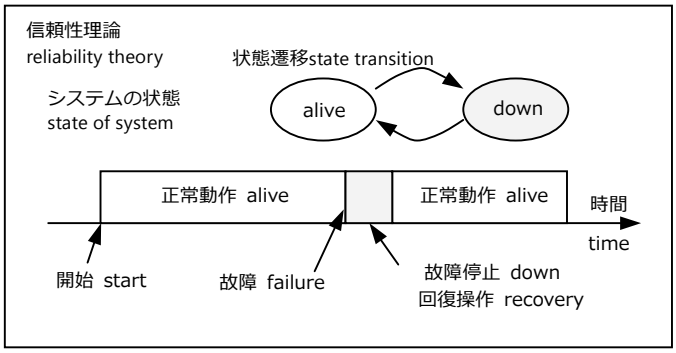

図 1 信頼性理論が扱う対象の状態
Figure 1 The state of an objective in reliability theory.

(2) 安信性理論の場合

安信性理論が扱う状態は「安全」と「非安全」である．図1に対応し,図2に安信性理論が扱う状態について示す.

(3) 両者の比較

図 1 と図 2 の比較をすることによって，信頼性理論における諸概念が安信性理論における諸概念に対応していること示すことができる.

特に信頼性理論における故障(failure)に相当する概念を，安信性理論では，内部犯罪(inside crime)に相当させている．さらに，一般化を意図して，安全の破断(break of safety)という概念を導入している.

両者に共通しているのは，時間という概念が欠かせないという点である．単純な確率事象ではなく，時間軸上での確率事象，すなわち，確率過程(stochastic process)であるという点である.

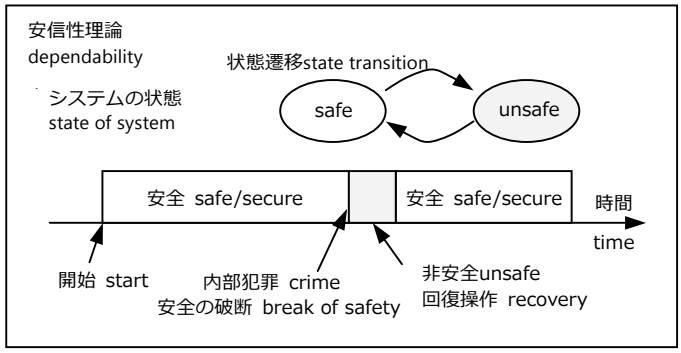

図 2 安信性理論が扱う対象の状態
Figure 2 The state of an objective in dependability theory.

5.2 状態変化の要因（正常→異常状態）

信頼性理論において，正常動作の状態から故障停止の状態に遷移する要因は故障である．他方，安信性理論において安全な状態から非安全な状態に遷移する要因は上記のように，内部犯罪である．ここでは，これらの考察を行う.

(1) 信頼性理論の場合

システム（主にハードウェア）において，システム外部から，時々刻々，刺激(stimulation)が入力される．外部刺激には, 温度, 湿度などの連続的な刺激(continuous stimulation)や機械的または電気的衝撃などのパルス的な刺激(impulsive stimulation)がある．これらの刺激，あるいは刺激の蓄積が，ある特定の因果関係が成立したとき，故障が発生すると考えられる.

このような因果関係を個別に把握することは困難であるので，故障の発生を確率事象としてマクロ的に把握するというのが信頼性理論の考え方である．実際の業務では，ミクロ的な個別の故障解析は必要に応じて行われている.

図 3 に故障発生について模式的に表す.

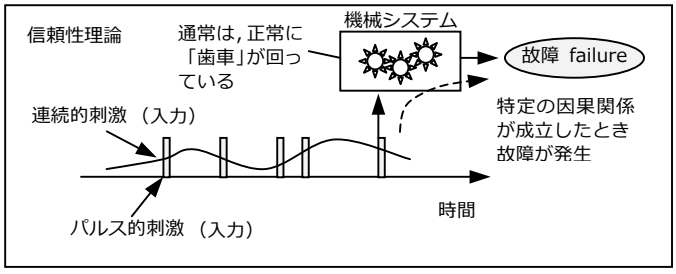

図 3 故障発生メカニズムの模式図
Figure 3 The mechanism model about occurrence of a failure.

次に時間の経過について，考察する.

- 上記の刺激が時間の経過とともに，次々と到来する.
- ある時間経過すると，上記の故障への因果関係が成立する場合が発生し，故障となる.
- その発生の度合いは，単位時間あたりの故障発生率 λ である（上記のマクロ的な把握）.
- すなわち，単位時間あたりの故障確率すなわち故障率 λ（単位は時間の逆数）によってシステムの信頼性が表現できる．λ の逆数が平均故障間隔 MTBF(Mean Time Between Failure)である．MTBF は信頼性(reliability)の基

本的な指標である.

(2) 安信性理論の場合

システム（主に人間系）において，システム外部から，時々刻々，犯罪誘因が到来する．それらの誘因は，世の中の世相のように，常日頃，連続的にもたらされるものと，ある特定の誘因のように，パルス的にもたらされるものがある．犯罪心理学の知見では，犯罪は，単純に A ならば，B であるといった論理で行われるものではなく，連続的またはパルス的な誘因が，ある時点で，犯罪の決行に及ぶものとのことである[9]. その点でもハードウェアの故障に類似している．このようにして，犯罪誘因，および蓄積されている犯罪誘因のうち，ある特定の決行条件が成立したとき，犯罪が発生するものと考えられる．この場合も，信頼性理論の立場に倣い，特定の決行条件を把握するのは困難なので，犯罪の発生をマクロ的に確率事象で把握することとする.

図 4 に犯罪発生について模式的に表す.

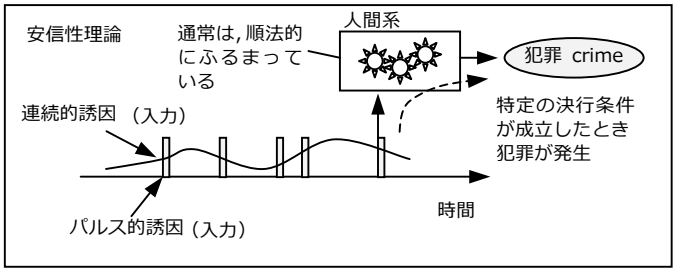

図 4 犯罪発生メカニズムの模式図
Figure 4 The mechanism model about occurrence of a crime.

次に，同様に時間の経過について考察する.

- 上記の誘因が時間の経過とともに，次々と到来する.
- ある時間経過すると，上記の犯罪への決行条件が成立する場合が発生し，犯罪となる.
- その発生の度合いは，単位時間あたりの犯罪発生確率 λである（上記のマクロ的な把握）.
- すなわち，単位時間あたりの犯罪発生確率すなわち犯罪率 λ（単位は時間の逆数）によってシステムの安信性が表現できる．λの逆数を本稿では，平均犯罪間隔 MTBC(Mean Time Between Crime)と名づける．さらに，内部犯罪に限らず概念を広げるため，平均破断間隔 MTBB(Mean Time Between Break of safety)と名づける．MTBB を安信性の基本的指標とみなす.

5.3 状態変化の要因（異常→正常状態）

多くのシステムでは，異常になったからといって即システムの廃棄というわけにはいかない. 故障なら修理を行い，犯罪なら取り除き，再びシステムを正常の状態に復帰する必要がある.

(1) 信頼性理論の場合

信頼性理論の場合には，次のステップで異常状態から正常状態に復帰する.

- 故障箇所の特定.
- 故障箇所の切り離し，取り出し.
- 故障箇所の修理または交換.
- 修理されたまたは交換された故障箇所をシステムに組み入れる.
- 上記のステップに要する時間が平均修復時間 MTTR(Mean Time To Repair)である．MTTR の逆数 μ は修復率である.

(2) 安信性理論の場合

安信性理論の場合には，次のステップで異常状態から正常状態に復帰する.

- 内部犯罪者の特定（安全破断要因の特定）.
- 内部犯罪者の除去.
- 代替要員の任用.
- 代替要員の投入（システムへの組み入れ）.
- 上記のステップに要する時間を MTTS(Mean Time To Safe state)と名づける．MTTS の逆数 μ は回復率である.

5.4 評価指標のまとめ

(1) 信頼性理論の場合

信頼性理論では従来から, 故障率 λ, 平均故障間隔 MTBF, 平均修理時間 MTTR，可用性 Availability によって，定量的な信頼性評価がなされている．信頼性は MTBF で，可用性は次式で表される.

$$MTBF = 1/\lambda \tag{1}$$

$$Availability = \frac{MTBF}{MTBF + MTTR} \tag{2}$$

(2) 安信性理論の場合

信頼性理論での故障率 λに対応する指標として，犯罪率 λを，MTBF に対応する指標として，平均破断間隔 MTBB を, MTTR に対応する指標として MTTS を前記で定義した. 信頼性理論における可用性に対応する指標として,「安信可用性(Safe_availability)」略して「安用性」を定義する．安信性は MTBB で，安用性は以下の式で表される.

$$MTBB = 1/\lambda \tag{3}$$

$$Safe\_availability = \frac{MTBB}{MTBB + MTTS} \tag{4}$$

5.5 直列配置

図 5 のように，要素を直列に配置する場合を考える.

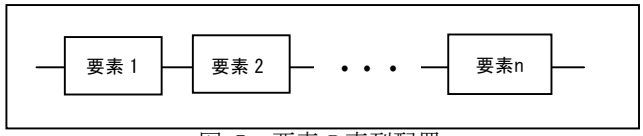

図 5 要素の直列配置
Figure 5 Serial connection of elements.

(1) 信頼性理論の場合

信頼性理論では，図 5 のように，要素を直列に配置すると, 故障率は各要素の故障率の和となり, 故障率は増加し，信頼性（MTBF=1/λ），可用性は低下する．ただし，ここ

での直列配置とは，物理的に直列に配置するという意味ではなく，すべての要素が正常動作（稼動）していれば，全体として正常動作するという意味での直列配置である．どれかの要素が故障停止すれば,全体として故障停止となる．各要素の故障率をλi，各要素の可用性を Avi とすると，全体の故障率λ,全体の可用性 Av は以下の式で計算できる．

$$\lambda = \sum_{i=1}^{n} \lambda_i \quad (5)$$

$$Av = \prod_{i=1}^{n} Av_i \quad (6)$$

(2) 安信性理論の場合

信頼性理論では，図 5 のように，要素を直列に配置することは，各要素をチェック要素（犯罪阻止要素）として機能させることにより，すべての要素で通過（阻止失敗）した場合，全体として非安全となる．どれかの要素が阻止成功すれば，安全となる．すなわち，要素を直列配置することにより，安信性，安用性は向上する．各要素の安用性(Safe_availability)を SAvi とすると，全体としての安用性 SAv は，次式となる．

$$SAv = 1 - \prod_{i=1}^{n} (1 - SAv_i) \quad (7)$$

5.6 並列配置

図 6 のように，要素を並列に配置する場合を考える．

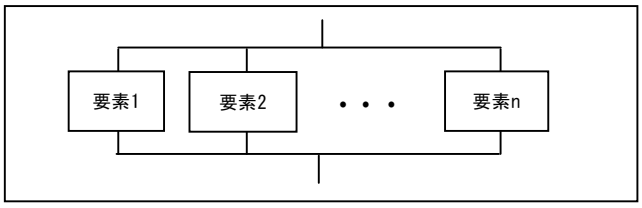

図 6 要素の並列配置
Figure 6 Parallel connection of elements.

(1) 信頼性理論の場合

信頼性理論では，図 6 のように，要素を並列に配置すると，どれかの要素が正常動作（稼動）していれば，全体として正常動作の状態であり，すべてが故障停止している場合には，全体として故障停止となる．すなわち，冗長系となっていて，可用性は向上する．各要素の可用性を Avi とすると全体の可用性は以下の式で計算できる．

$$Av = 1 - \prod_{i=1}^{n} (1 - Av_i) \quad (8)$$

(2) 安信性理論の場合

安信性理論では，図 6 のように，要素を並列に配置することは，各要素をチェック要素（犯罪阻止要素）として機能させているが，どれかの要素で通過（阻止失敗）した場合，全体として非安全となる．すべての要素が阻止成功すれば，安全となる．すなわち，要素を並列配置することにより，安信性（MTBB=1/λ），安用性は低下する．各要素の犯罪率をλi，安用性(Safe_availability)を SAvi とすると，全体の犯罪率λ，全体の安用性 SAv は，次式となる．

$$\lambda = \sum_{i=1}^{n} \lambda_i \quad (9)$$

$$SAv = \prod_{i=1}^{n} SAv_i \quad (10)$$

5.6 相互の対応と双対性

5.5 および 5.6 から信頼性理論と安信性理論における諸概念の対応をまとめると次のようになる．

- 故障率λ⇔犯罪率λ (時間の要素を含むことが重要)
- 信頼性：平均故障間隔（MTBF）
  ⇔安信性：平均破断間隔(MTBC または MTBB)
- 修復性μ⇔回復性μ
- 可用率(Availability)⇔安用性(Safe availability)

また，5.5 および 5.6 から

- 直列⇔並列
- (5) ⇔ (9)
- (6) ⇔ (10)
- (7) ⇔ (8)

の関係で，双対性(duality)のような関係を観測することができる．この考察は，今後の課題である．

6. SMC システムの安全性評価

ユーザが利用しているクラウド業者内の悪人によって惹き起こされる内部犯罪の発生率，その逆数の MTBB によって，SMC システムの安全性を評価する．すなわち，本稿の安全性に関わる定義から，SMC システムの「安信性」を評価するということになる．

6.1 SMC システムの安全が破断されるメカニズム

以下のメカニズムによって SMC システム（ここでは 2outof 3 を想定し，クラウド i，i＝0，1，2 を想定する）の安全が破断され非安全となる．

(1) クラウド i に，悪人が存在する．その確率を Pei とする（時間的要素をもたないものとする）．
(2) その悪人が犯行を決意する．その確率を Phi とする（時間的要素をもつことが重要，単位時間あたりの発生確率）．犯罪率に相当する．
(3) その悪人が別のクラウド j に悪事結託を呼びかける．その確率を Pcij とする（時間的要素をもたないものとする）．
(4) クラウド j に悪人が存在する．その確率を Pej とする（時間的要素をもたないものとする）．
(5) クラウド j の悪人がクラウド i からの悪事結託の呼びかけに合意する．その確率を Paji とする（時間的要素を

もたないものとする).

(6) 以上でクラウド i で安全破断の犯罪が発生する. その確率を Pi とする(時間的要素は(2)から継承される).

(7) クラウド 0，1，2 のいずれかで犯罪が発生する．その確率を P とする．この P は時間的要素をもち，5.2(2)で述べた犯罪率に相当する.

これらの要素の相互関係を図 7 に表す.

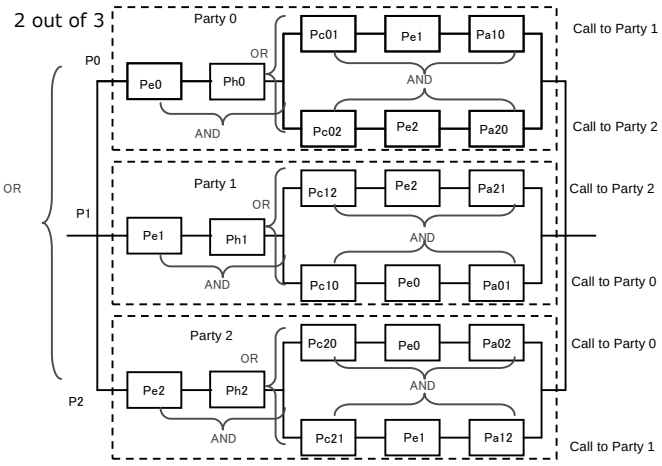

図 7　要素の関係
Figure 7　Relation of elements.

6.2　SMC システムの安信性の計算

図 7 の要素の AND，OR の関係から確率計算を行い，全体としての犯罪率 P を計算し，この逆数が安信性の代表的指標の平均破断間隔 MTBB である.

$$P_i = P_{ei} \cdot P_{hi} \cdot (1 - \prod_{j=i+1|\mathrm{mod}3}^{i+2|\mathrm{mod}\backslash 3} (1 - P_{cij} \cdot P_{ej} \cdot P_{aji})) \qquad (11)$$

$$P = 1 - \prod_{i=0}^{2} P_i \qquad (12)$$

$$MTBB = 1/P \qquad (13)$$

上記の計算は，2 out of 3 の場合であるが，2 out of 2 や 3 out of 3 の場合についても計算ができる.

なお，非安全状態から安全状態への復帰については，すなわち，回復率 μ，平均回復時間 MTTS=1/μ，安用率 SAv については，ここでは言及しない.

6.3　SMC システムの安信性の数値計算例

具体的に，どの程度の安全性が向上するかを数値例で示す．ちなみに我々の提案した軽量型 SMC は，任意の数のパーティで構成することができる．表 1 は数値例の計算結果である．表 1 の数値例において，単独クラウドでは，10 年に 1 回の安全破断が発生する. 一方, SMC を構成すれば, 160 年に 1 回よりも少ない安全破断の発生となる.

6.4　SMC システムの基礎データの取得

計算の基となる基礎データは，次の考えで取得する.

- 各種のセキュリティガイドライン[10]からチェックリストを作成し，それに基づき各クラウド提供者のレイティングを行う．そして定性的に，数値を定める.
- 数年にわたり安全破断の事案の実績を分析し，レイティングと各数値の関係を見直す.

6.5　SMC システムの安全性評価の意義

クラウド提供者が自ら,「わが社の MTBB は 10 年です」, とか「30 年です」と表明することは考えがたい．にも関わらず安全性を定量的に評価する意義は次の点である.

- 安全性を高めるためのシステム構成案の比較.
- クラウド提供者間での比較.
- 2.で述べたユーザにおけるコスト対効果の観点.

表 1　安信性（平均破断間隔 MTBB）の数値計算例
Table 1　Numerical Examples of MTBB.

	単独クラウド (1 out of 1)	SMC 2 out of 3	SMC 2 out of 2	SMC 3 out of 3
Pei	1/10	1/10	1/10	1/10
Phi	1/1 [1/hear]	1/1 [1/hear]	1/1 [1/hear]	1/1 [1/hear]
Pcij	-	1/5	1/5	1/5
Paji	-	1/2	1/2	1/2
P	0.1	0.005958128	0.001999	0.00014993
MTBB	10　[year]	167.8 [year]	500 [year]	6667 [year]
times	1	16.7	50.0	666.7

7.　おわりに

本稿の研究は緒に着いたところであり，今後，様々な場合の安全脅威に対して,「安信性理論」の考えが適用可能かどうかを研究していきたい.

参考文献

1) Shamir, A.: How to share a secret, Comm. ACM, Vol.22, No.11, pp.612-613, (1979)
2) Gentry, C.: Fully Homomorphic Encryption Using Ideal Lattices, STOC2009, pp.169-178 (2009)
3) 千田浩司, 安全な情報処理を目指す秘密計算技術の研究動向と実用化に向けた取り組み, 情報処理 Vol.54 No.11 pp.1130-1134 Nov. 2013
4) 宮西洋太郎他，クラウドサービス利用者の安心感を高める簡易的秘密計算法の提案， 信学技報，Vol.114 No.49 SWIM2014-4 pp19-24，2014/5
5) 金岡晃他，実数演算可能な軽量秘密計算法の一考察,CSS2014(Computer Security Symposium 2014)，Oct. 2014 Sapporo pp682-687
6) NRI セキュア，データセンターを活用した情報漏洩防止策 http://cloud.watch.impress.co.jp/epw/docs/news/20100301_351998.html
7) IBM，完全準同型暗号ライブラリをオープン化, http://news.mynavi.jp/news/2013/05/09/094
8) NTT，医療統計処理における秘密計算技術を世界で始めて実証, http://www.ntt.co.jp/news2012/1202/120214a.html#6
9) 越智啓太，犯罪心理学的観点からの内部犯行の分析と対策，日本セキュリティマネジメント学会第 27 回学術講演会「内部犯罪・不正のリスクマネジメント」資料，2014/11/22
10) 組織における内部不正防止ガイドライン http://www.ipa.go.jp/files/000041054.pdf