3D-7

クラウドサービスにおける 利用者の安心感を実現するセキュリティ確保方式

韓　嘯公†　　宮西　洋太郎‡　　北上　眞二†　　浦野　義頼†　　白鳥　則郎†

†早稲田大学大学院国際情報科学研究科　　‡(株)アイエスイーエム

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．計算能力を柔軟に拡大，縮小でき，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，データの保管や処理(プログラム)を外部企業(クラウド事業者)に委託することにより，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．

本研究では，データベースおよびプログラムを複数クラウド間に分割・配置し，個別に処理させる方式を提案する．これにより個別部分が不正使用や漏洩されたりしても，全体としてデータや処理方法の秘密を確保する．

2　技術的課題と研究の目的

企業において，(1)どのようなデータを使い，(2)どのような処理方法で，(3)どのようなデータを算出して，企業活動を行っているかは競争相手には秘密にしたい情報，すなわち企業秘密情報である．

クラウドを利用する場合，これらをクラウド事業者に委託することとなり，「クラウドに保管されているデータベースやプログラムがクラウド内部に起因して不正使用される，または漏洩される等のセキュリティリスク」(以下，「当該リスク」と略称する)の問題がある．

この問題に対して，「技術またはシステムによる解決策」を求めることが技術的課題であり，それによりクラウド利用者の安心感を高めることが本研究の目的である．

3　従来の利用者の対応

上記の不安に対して，利用者は現在では大略，次のような対策によっている．

(1)企業秘密であるデータやプログラムにはパブリッククラウドを利用しない(本稿の対象外)．

(2)クラウドを利用する場合には，信頼性の高いクラウド事業者を選択し，政府発行のガイドラインにそった利用，運用を行う[1][2]．

上記のガイドラインでは，クラウドにおけるデータの暗号化が推奨されている．データの暗号化は，クラウド外部から不正にデータを読み取ろうとする攻撃には有効な対策であるが，クラウド内でプログラム実行時，暗号化データは復号され，平文となり，クラウド事業者にはデータが明らかとなる．

さらには，データベースとプログラムが同一クラウドに配置されていれば，上記の復号時に使用した暗号鍵がクラウド事業者に知られることとなり，データベース全体が明らかとなってしまう．従って暗号化しても，「当該リスク」が存在することになる．

このリスクに対しては，SLA(Service Level Agreement)などの人間的な「約束ごと，契約」によって防止する対策はあるが，そのような方法では技術またはシステムによる十分な解決策とは言いがたい．

A Method to Ensure Security for realizing User's Sense of Safety in Cloud Services
Xiagong Han†, Yohtaro Miyanishi‡, Shinji Kitagami†, Yoshiyori Urano†, Norio Shiratori†
†Waseda University GITS, ‡ISEM,Inc.

4　関連する研究

「当該リスク」に対して「技術またはシステムによる解決策」として，有望な技術には，秘密分散法[3]および秘密計算法がある[4]．

4.1　秘密分散法(secret sharing)，電子的割符技術

秘密分散法の１つに(k, n)閾値法がある[5]．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とし，n個のサーバに分散配置する．復元は，連立方程式を解くことによりなされる．電子的割符技術は，あるデータをビットレベルで秘密データに加工する技術である．

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][7]．

4.2　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[8]．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[5]とされているがIBM社からライブラリの広報もなされている[9]．

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[5]．現時点では限定された機能で実用化されている[10]．

4.3　データ・プログラムの分割による方法

全体としてのデータやプログラムを分割し，別々のクラウドに配置することにより，部分的に秘密が破られても，全体としてのデータやプログラム(処理方法)の秘密を守るという提案もなされている[11]．

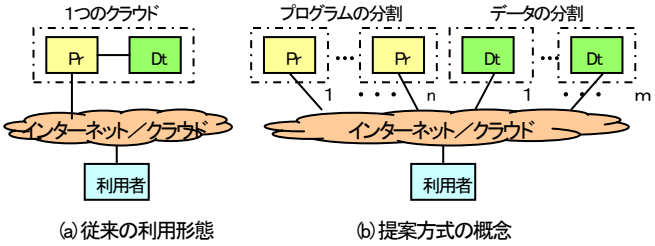
5　提案する方式

本研究では，パブリッククラウド，IaaS，PaaS を前提とし，4.3の考えに基づき，4.1や4.2の考え方を組み入れた方式を提案する．複数の方式案を提案し比較する．

「当該リスク」を回避するための本質的な解決策は，秘密計算法にあると考えるが，汎用的な用途としてはまだ十分な実用レベルにはない．さらには，この方法でもプログラムそのものはクラウド事業者に対し秘密にはできない．

そこで，本研究ではデータおよびプログラムを分割し，別々のクラウドに配置することにより，全体としての秘

密を確保するという方式を提案する．図 1 に従来の対応と本提案方式の概念を示す．一点鎖線は個別のクラウドを表す．以下，Pr はプログラム，Dt はデータを表す．



(a)従来の利用形態　　(b)提案方式の概念

図 1 従来の利用形態と提案方式の概念

この概念の下に，各種の組み合わせを考察する．Pr，Dt の分割数は任意の整数 n，m が考えられるが，本稿では n=m=2 以下とする．表 1 に各種の分割案を示す．

表 1　各種の分割方法　(表中の○は する，×は しないの意味)

		①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩
		Dt と Pr を別クラウドに配置	Pr 用クラウドの数	Dt 用クラウドの数	Dt を暗号化	Pr を暗号化	自己サーバを使用	秘密分散法使用	秘密計算法使用	安全性	コスト
現方式 E		×	1	0	×	×	×	×	×	E<D	E<D
現方式 E1(暗号)		×	1	0	○	×	×	×	×	E1>E	E1>E
A 群	A 案	×	2	0	×	×	○	×	×		
	A1 案	×	2	0	○	×	○	×	×	A1>A	A1>A
	A2 案	×	2	0	○	○	○	×	×	A2>A	A2>A
B 群	B 案	○	2	2	×	×	×	×	×	B<A	B<A
	B1 案	○	2	2	○	×	×	×	×	B1>B	B1>B
	B1a 案	○	2	1	○	×	×	×	×	B1a>B1	B1a<B1
	B2 案	○	2	2	○	○	×	×	×	B2>B1	B2>B1
C 群	C 案	×	2	0	×	×	×	×	×	C<B	C<B
	C1 案	×	2	0	○	×	×	×	×	C1>C	C1>C
D 群	D 案	○	1	1	×	×	×	×	×	D<A	D<A
	D1 案	○	1	1	○	×	×	×	×	D1>D	D1>D
X 群	X 案	○	2	2	×	×	×	○	×	X<A	X<A
	Xa 案	×	2	0	×	×	×	○	×	Xa<X	Xa<X
Y 群	Ym 案	×	3	0	○	×	×	○	○	Y>A	Y>A
	Ye 案	○	1	1	○	×	×	×	○	Y>A	Y>A

表 1 の列①～⑧の観点からの分割を考える．表 1 において，E 方式は，現在の一般的なクラウドの利用形態で，E1 方式は，データを暗号化する利用形態である．

提案の代表的な構成として，A 案と B 案を示す．データの要素を x_1，x_2 とし，全体の処理(プログラム)を $y=f(x_1,x_2)$ とする．

5.1 A 案

この案は，全体処理を(1)式のように分割できるものとし，分割・配置先のクラウドを Cpd_1，Cpd_2 とする(Dt と Pr は同一クラウドに配置)．

$$y=f(g_1(x_1),g_2(x_2),g_0(x_1,x_2)) \quad (1)$$

ここで，$g_1(x_1)$ はデータ x_1 を Cpd_1 で処理する部分，$g_2(x_2)$ はデータ x_2 を Cpd_2 で処理する部分，$g_0(x_1,x_2)$ はデータ x_1，x_2 をどうしても分割できない処理(例えば乗算，除算など)について，自社サーバで処理する部分である．

最後の合成処理 $f()$ も自社サーバで処理を行う．

5.2 B 案

この案は，自社サーバで処理を行わない案であり，全体処理を(2)式のように分割できるものと仮定する．

$$y=f(x_1,x_2)=f_2(x_1,x_2,f_1(x_1,x_2)) \quad (2)$$

ここで，$f_1(x_1,x_2)$ は全体処理 $f(x_1,x_2)$ の前半部分，$f_2(x_1,x_2,f_1(x_1,x_2))$ は後半部分である．

図 2 は B 案の構成図である．実線は処理制御のながれ，破線はデータの流れを表し，一点鎖線は個別のクラウドを表す．Pr はクラウド Cp_1，Cp_2 に，Dt はクラウド Cd_1，Cd_2 に配置する．

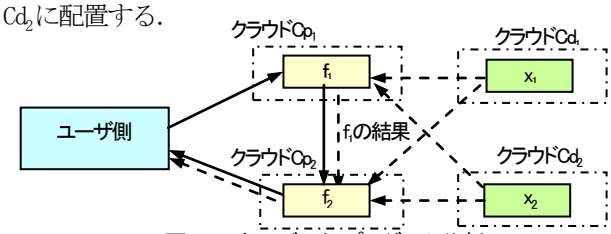


図 2 B 案のデータ･プログラム分割

6 実験システムと考察

提案方式の有効性を確認するために，実験的なクラウドシステムを構築する．4 つのクラウドサーバと 1 つの自社サーバを利用し，OS は Linux で実験環境を構築する．

適用例として，秘密情報(学生成績ランキング：名前，学籍番号，科目，点数，ウェート等)を想定する．実験は，(1)データと処理方法を想定し作成する．(2)データと処理方法の分割案を決定する．(3)各クラウドサーバに配置して，実験を行っており，結果は当日発表する予定である．クラウド間連携動作実行を確認し，実験方式と従来方式について，安全性，システム構築コスト，クラウド利用料，性能などの比較を考察する予定である．

7 おわりに

本研究では，クラウドサービスにおける利用者の安心感を実現するセキュリティ確保方式について，データとプログラムのクラウドへの分割・配置方式について複数の提案を行い，基本的な実験を行った．今後の課題は性能の検討，データ分割，プログラム分割の自動化や，簡易的な秘密計算法の適用についても検討していきたい．

参考文献

[1]経済産業省：クラウドサービス利用のための情報セキュリティマネジメントガイドラインの公表～クラウドサービスの安全・安心な利用に向けて～ (2011 年)
http://www.meti.go.jp/press/2011/04/20110401001/20110401001.html
[2]総務省：ASP・SaaS における情報セキュリティ対策ガイドライン (平成 20 年，2008 年)
http://www.soumu.go.jp/main_sosiki/joho_tsusin/policyreports/chousa/asp_saas/pdf/asp_saas_zentai.pdf
[3]千田浩司他，“照合匿名化クラウドの課題と対策，” 信学論 (A)，Vol.J96-A No.4 pp.149-156，2013/4
[4]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
[5]Shamir, A.：“How to share a secret,” Comm. ACM, Vol.22, No.11, pp.612-613, (1979)
[6]NRI セキュア，“データセンターを活用した情報漏えい防止策”
http://cloud.watch.impress.co.jp/epw/docs/news/20100301_351998.html
[7]ソリトンシステム，“電子割符技術 Tally-WariZen”
http://www.itmedia.co.jp/enterprise/articles/1310/07/news001.html
[8]Gentry, C.：“Fully Homomorphic Encryption Using Ideal Lattices,” STOC2009, pp.169-178 (2009)
[9]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
[10]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
[11]宮西洋太郎，“クラウドコンピューティングでの高度セキュリティ実現方式の提案～情報処理委託内容の秘匿方式～，” 信学技報，Vol.110 No.302 pp13-17，2010/10