安全なクラウド連携のためのデータセキュリティ

Inter-Cloud Data Security for Secure Cloud-Based Business Collaborations

● 津田　宏　　● 松尾昭彦　　● 阿比留健一　　● 長谷部高行

あらまし

クラウド時代になると，外部サービスの利用によって社内外の境界があいまいになるため，情報漏えい対策においても，従来のように社外との境界のゲートウェイで機密情報の流出をブロックするという考え方だけでは不十分になる。また，今後クラウドの利用形態が多様化するにつれ，オンプレミスや複数のクラウドが連携した環境で，プライバシー情報や機密情報を安全に利活用する技術やソリューションが求められている。

今回開発したクラウド情報ゲートウェイおよびアクセスゲートウェイ技術では，社内の機密情報からプライバシー情報を秘匿してクラウドで処理したり，クラウド側にある処理アプリケーションを社内に移動させ安全に実行したりすることが可能である。本技術により，ユーザ環境・サービス・情報の三つの多様な条件で，クラウドをまたがって安全に機密情報を利用することができ，異業種間での協業や分業などの新たなクラウド利用を促進する。

本稿では，情報ゲートウェイおよびアクセスゲートウェイの概要と利用シーンについて述べる。

Abstract

With the advent of cloud computing, the boundary separating internal and external data has become increasingly blurred due to the utilization of external services. As a result, existing methods of preventing data leakage, such as only using a gateway to block the outflow of confidential data, have become insufficient. Therefore, there is increased demand for new security technology to allow confidential data to be safely used even in the cloud. We have developed new cloud information gateway and access gateway technologies that can mask confidential information contained within data before it is processed in the cloud. They can also transfer applications from the cloud to inside the company for internal processing. In this way, they make it possible to utilize cloud services without transmitting actual data. These technologies enable users to safely utilize confidential data in the cloud, encouraging new uses of cloud computing, such as cross-industry collaborations and specialized uses in specific industries.

まえがき

クラウドコンピューティング（以下，クラウド）の活用形態は急速に多様化しており，セキュリティに対する要件も様々である。利用者は情報の機密性と，クラウドのセキュリティ機構，さらにクラウド活用による利便性を判断して，適切な情報を適切な形式でクラウドに預ける場面が増えてくる。クラウドや外部サービスの利用によって社内外の境界があいまいになっていくため，ここでのセキュリティは，従来のように社外との境界のゲートウェイで機密情報の流出をブロックするという情報漏えい対策手法だけでは十分ではない。そこで，プライバシー情報や機密情報を，オンプレミスやパブリッククラウド，ハイブリッドクラウド，さらに他社SaaSも含めて安全に利活用するための新たなセキュリティ技術が求められている。

本稿では，これらの課題を解決するクラウド間の新たなデータセキュリティ技術について述べる。

パートナクラウドとその課題

北米における今後のクラウドの利用形態について，独自の調査を行ったところ，ビジネスコラボレーションへの期待が大きいことが分かった。例えば，新製品共同開発，協業，ソフトウェア開発，業務アウトソース，情報の交換などである。このように一つまたは複数のクラウドサービスを，異なった会社で協業などに利用する形態を著者らは「パートナクラウド」と呼んでいる。

パートナクラウドのニーズは，小売，CPG（コンシューマ向け商品），医薬，ヘルスケアといった業界で高いことも分かった。例えば小売やCPG業界では，従来のサプライチェーンに加えて，他社や顧客との新製品の共同開発にクラウドを利用したいという要望がある。また，ヘルスケア業界ではホームドクター，病院，薬局，検査機関などが連携するHIE（Health Information Exchange）においてクラウドへの移行が望まれている。

こうしたパートナクラウドにおいては，クラウド間でやり取りされる情報のセキュリティがユーザの大きな懸念となる。カルテのように法的に規制されている情報や，共同開発における知財のような情報を，パートナクラウドでいかに守るかが大きい課題となる。このような形態では，単純に機密情報をブロックしたり，暗号化したりしてはサービスを利用できない。また，クラウドで複数の企業が連携して互いの情報を安全に利活用するといった場合にも不十分である。他社のクラウド上のSaaSアプリケーションで情報活用することまで考えると，ユーザ環境・サービス・情報の三つの条件を自由に組み合わせて，クラウド間での情報を制御できる必要がある。

情報ゲートウェイ

そこで，社内とクラウドの間や，クラウド間でやり取りされる情報を，情報の内容と相手サービスに合わせて柔軟に制御できるクラウド情報ゲートウェイ技術を新たに開発した。情報ゲートウェイのパートナクラウドへの適用例を**図-1**に示す。

この情報ゲートウェイでは，従来のファイアウォールのように通信データをブロックすることでセキュリティを保つのではない。以下の三つの技術により，クラウド間で流れるデータの中身まで見た処理や，実行環境機能を提供することで，社内およびクラウドを経由した他組織との情報連携など，様々な利用シーンに対して安全な情報の利活用を可能にしている。

（1）情報秘匿化

機密情報をクラウドに送信する際に自動的に秘匿化を行い，クラウドから処理結果を受信した際に自動的に復元する。

（2）情報トレーサビリティ

クラウドをまたがる情報の利用ログや内容から，利用状況を見える化する。

（3）安全実行サンドボックス

クラウド上のアプリケーションを社内の実行環境に配置して実行し，機密情報の処理を行う。

情報秘匿化

機密情報を単に暗号化してクラウドに置くだけだと，クラウド上に鍵がない限り情報を処理することはできない。そこで，著者らは機密情報に含まれる機密部分を落としたり，特別な暗号技術などで安全化した情報に置き換えて，クラウドで処理をすることが可能な情報秘匿化技術を開発した。(1)

例えば，健康診断の結果を業界クラウドで活用

するのに，氏名や住所などをいったん仮の名前に置き換えて外部の業界クラウドに送り，専門医が診断した結果を受け取る際には再び復元するといったことが，利用者やクラウドアプリケーション作成者は意識せずに行うことができる。

また，企業が持っている地域別の感染者数のような表形式の情報は，そのまま利用すると特定地域に患者が多いというような機微情報をクラウドの他社に渡してしまう。そこで，図-2に示すスクランブル集計の技術を開発した。オンプレミスでもとの数値が分からないよう特別な乱数を加算してクラウドに送り（①），なおかつ複数の数値をそのまま縦横に正しく集計できる（②）。集計結果は各利用者が持っている復号キーのレベルに応じた

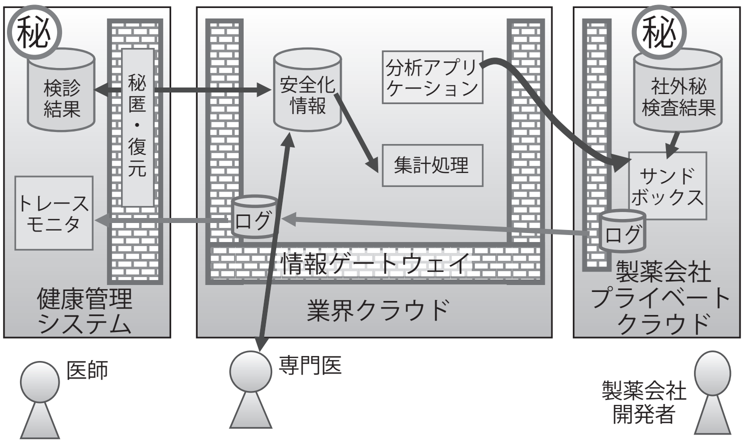
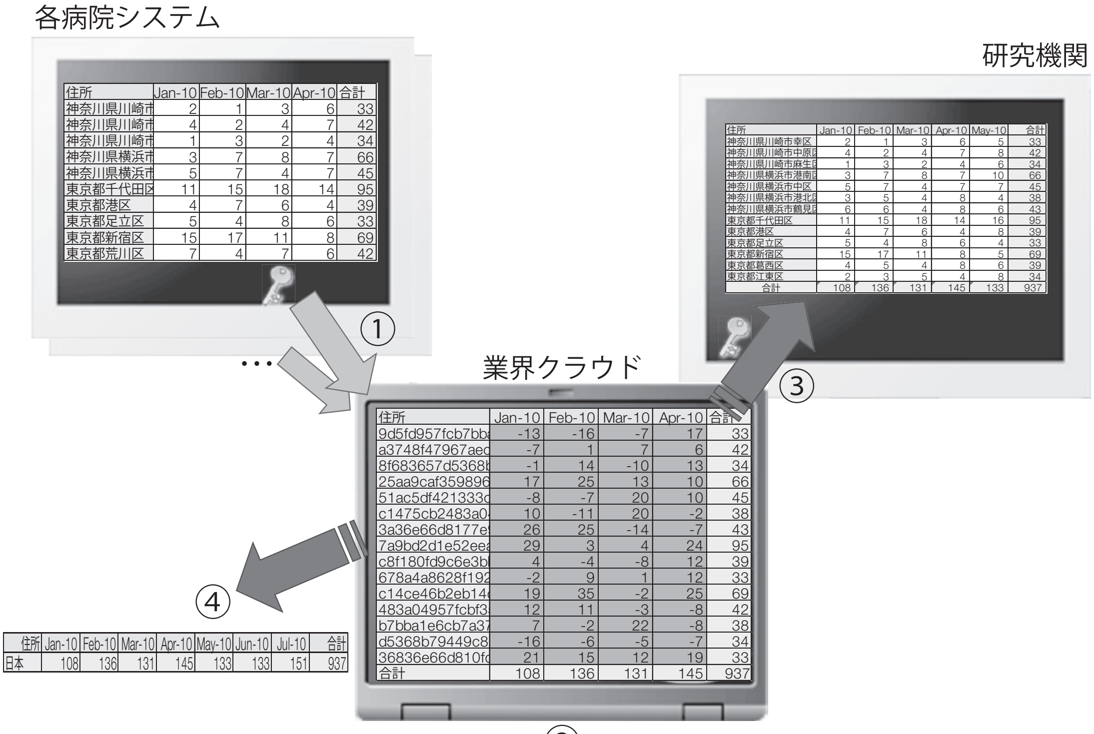


図-1　情報ゲートウェイのパートナクラウドへの適用例
Fig.1-Application of information gateway to partner cloud.



住所	Jan-10	Feb-10	Mar-10	Apr-10	合計
神奈川県川崎市	2	1	3	6	33
神奈川県川崎市	4	2	4	7	42
神奈川県川崎市	1	3	2	4	34
神奈川県横浜市	3	7	8	7	66
神奈川県横浜市	5	7	4	7	45
東京都千代田区	11	15	18	14	95
東京都港区	4	7	6	4	39
東京都足立区	5	4	8	6	33
東京都新宿区	15	17	11	8	69
東京都荒川区	7	4	7	6	42

住所	Jan-10	Feb-10	Mar-10	Apr-10	合計
9d5fd957fcb7bb	-13	-16	-7	17	33
a3748f47967ae	-7	1	7	6	42
8f683657d5368	-1	14	-10	13	34
25aa9caf359896	17	25	13	10	66
51ac5df421333	-8	-7	20	10	45
c1475cb2483a0	10	-11	20	-2	38
3a36e66d8177e	26	25	-14	-7	43
7a9bd2d1e52ee	29	3	4	24	95
c8f180fd9c6e3b	4	-4	-8	12	39
678a4a8628f192	-2	9	1	12	33
c14ce46b2eb14	19	35	-2	25	69
483a04957fcbf3	12	11	-3	-8	42
b7bba1e6cb7a37	7	-2	22	-8	38
d5368b79449c8	-16	-6	-5	-7	34
36836e66d810f	21	15	12	19	33
合計	108	136	131	145	937

住所	Jan-10	Feb-10	Mar-10	Apr-10	May-10	合計
神奈川県川崎市幸区	2	1	3	6	5	33
神奈川県川崎市中原	4	2	4	7	8	42
神奈川県川崎市麻生	1	3	2	4	6	34
神奈川県横浜市港南	3	7	8	7	10	66
神奈川県横浜市中区	5	7	4	7	7	45
神奈川県横浜市港北	3	5	4	8	4	38
神奈川県横浜市鶴見	6	6	4	8	6	43
東京都千代田区	11	15	18	14	16	95
東京都港区	4	7	6	4	8	39
東京都足立区	5	4	8	6	4	33
東京都新宿区	15	17	11	8	5	69
東京都葛西区	4	5	4	8	6	39
東京都江東区	2	3	5	4	8	34
合計	108	136	131	145	133	937

住所	Jan-10	Feb-10	Mar-10	Apr-10	May-10	Jun-10	Jul-10	合計
日本	108	136	131	145	133	133	151	937

図-2　スクランブル集計の例
Fig.2-Example of scrambled data aggregation.

詳細度（県レベル，市町村レベルなど）で入手できる（③）。クラウドには基となる表情報や元に戻すためのキーを置かずに処理することができ，さらに一つの集計結果を基に複数の利用者のレベルに対応可能なため，データベースの管理が容易という特徴がある。なお，キーを持たない人でも，全体の合計値のみを知ることができる（④）。

これら情報の秘匿化ポリシーは，オンプレミスやクラウドに配置した情報ゲートウェイで，管理者がXSLT（XML Stylesheet Language Transformations）により，相手クラウド上のサービスに合わせて，タグ単位で細かい秘匿・復元ルールを定義できる。また，このルールに合致しない情報はブロックすることで，クラウド間に流れる情報とその秘匿レベルを確実に制御できる。

関連する他社技術として，トークン化がある。(2) これは，例えばサブシステムに渡す情報に含まれるクレジットカード番号をマスクすることで，PCIDSS（Payment Card Industry Data Security Standard）における監査の手間を省く技術である。これに対して，本技術は，復元まで含めて柔軟なルールの記述ができ，また秘匿したまま特定の分析（集計）ができる点が特徴である。このほか，キーを使わずに多様な演算を行うことのできる準同型暗号もあるが，(3) 計算量が膨大で実用にはまだ時間がかかると考えられる。一方，本技術はデータ構造を限定した現実的なアプローチと言える。

情報トレーサビリティ

前述の北米での調査において，パートナクラウドで特に要望が高かったのが，クラウドに預けた情報のアクセスや変更を追跡する技術である。第三者の運営するクラウドで，協業他社がアクセスする状況だと，秘匿化した情報であっても契約に従った使い方をしているのかを監査したいという要望がある。

そこで，情報ゲートウェイを通じてクラウドをまたがった情報の移動を追跡し見える化する情報トレーサビリティ技術を開発した（**図-3**）。情報ゲートウェイによりクラウドのすべての入出力ログを記録できる。また，テキスト文書については，クラウドの入力時に，テキストに含まれるキーワードの出現特徴を独自のフィンガプリント技術（コンテンツシグネチャ）で記録しておき，クラウドから出るデータに機密テキストの一部が流用されていないかをチェックしたり，見える化したりすることができる。(1)

情報のトレーサビリティとして従来，電子透かしを使って情報を追跡する方法があるが，それに対して本技術はテキスト中のキーワード出現特徴を基にしているため，特別なアプリケーションは不要で，わずかな量のテキストでも検出可能とい

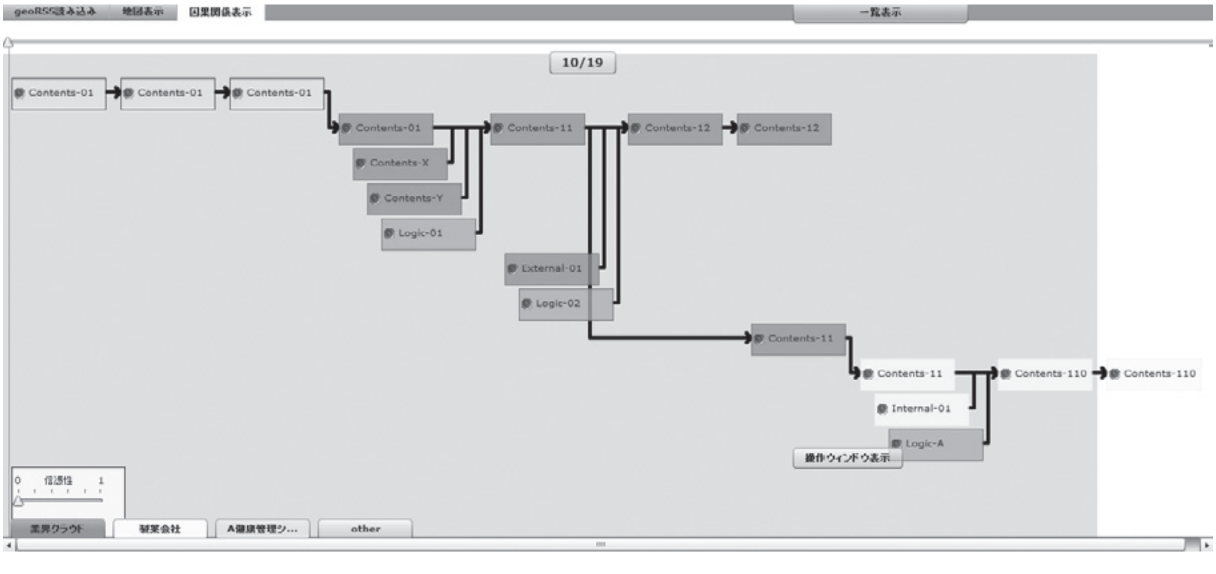


図-3　情報トレーサビリティの画面
Fig.3-Screenshot of information traceability.

う特徴がある。

情報ゲートウェイによるクラウド間の入出力チェックに加えて，後述のサンドボックスによるクラウド内のデータ利用状況のモニタリングを組み合わせることで，例えば共同開発において，クラウドに預けた文書の一部流用を含めてどのように利用されたか，不適切な利用がないかなどを確認することができる。

安全実行サンドボックス

SaaSアプリケーションなど，パブリッククラウド上で提供されるサービスを社内から利用する場合，データがクラウド側に渡って処理が行われる。このため，情報漏えいリスクを考慮すると，社外秘の機密情報やプライバシー情報を含むようなデータを社外のアプリケーションで扱うことは難しくなっていた。今後，パブリッククラウド上での優れたサービスが多く提供され，それらを社内からも安心して利用したいというニーズが強くなってくると考えられるため，情報を社外に出さずにクラウド上のサービスを利用する技術が求められている。

そこで，パブリッククラウド上の処理ロジックで社外秘のデータを扱う際には，処理ロジックを社内プライベートクラウド上の実行環境で動かし，情報を社外に出さずに処理を行う技術を新たに開発した。この技術では，情報ゲートウェイから制御されるアプリケーション実行環境を社内に用意し，情報の配置ポリシーに基づいて，社外に出せない情報を処理する場合にはクラウド上の処理ロジックをこの環境内に配置して実行するようにしている。この実行環境はサンドボックスと呼ばれる，不正な操作ができないように保護された環境になっているため，クラウド上から持ち込んだ処理ロジックに悪意のあるコードが含まれていたとしても，情報漏えいなどのリスクがなく，安全に実行することができる。この安全実行サンドボックスと情報ゲートウェイの連携の様子を**図-4**に示す。

アクセスゲートウェイ

クラウドにある情報を利用する形態としては，ほかのクラウドのサービスを経由して利用する形態も考えられる。例えば，印刷サービスやプロジェクト管理などのSaaSアプリケーションを，社内やお客様先などユーザ環境に合わせて機密情報を秘匿し，文書の必要な部分だけ見せるなどの利用シーンが考えられる。

このような，情報ゲートウェイを配備することができないほかのクラウドのサービスを経由するクラウド間連携に向けた技術として，情報を預けたクラウドの情報ゲートウェイと連携し，クラウド間のデータアクセス制御を実現するアクセスゲートウェイ技術を開発した。(4) 開発したアクセスゲートウェイと情報ゲートウェイの連携の様子を**図-5**に示す。

クラウドに預けた機密情報を，ほかのクラウドに渡す際には，ほかのクラウドからのデータアク

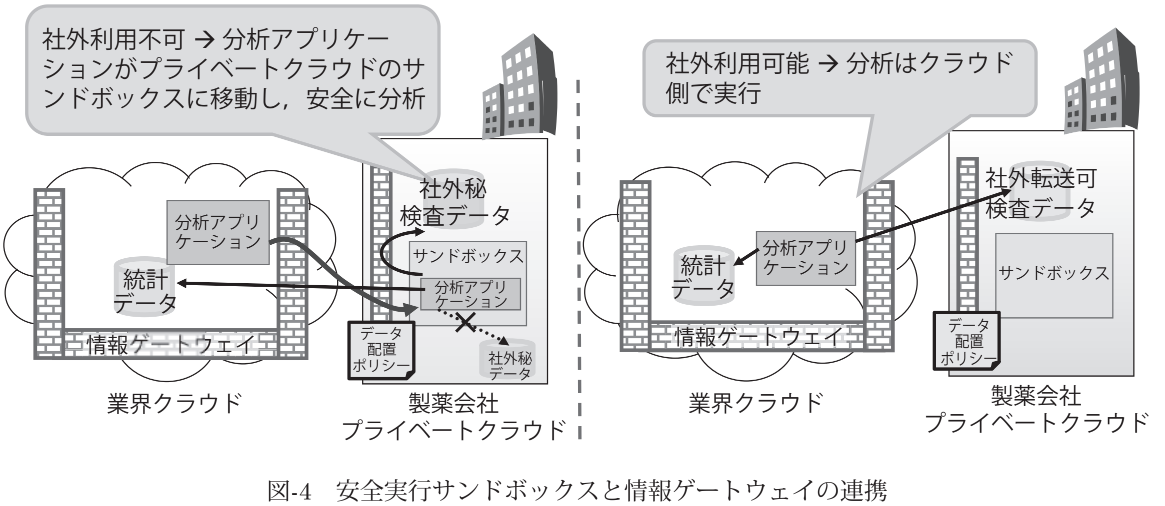


図-4　安全実行サンドボックスと情報ゲートウェイの連携
Fig.4-Combination of secure sandbox and information gateway.

セス要求が正当か否かを判断した上で渡す必要がある。例えば，既存インターネット上のWebサービス間では，ユーザにデータの受渡しの可否を確認する仕組みとしてOAuth(5)の利用が広がっている。しかし，企業ユースとして利用する場合には，個々のデータ提供可否を個々のユーザが行うのではなく，あらかじめ定めた企業ユーザの属性（部署，役職など）に応じた利用サービスや預けたデータについてのアクセス権限に応じて，アクセス制御を行うことも求められる。

そこで，ネットワークに置いたアクセスゲートウェイを利用し，情報ゲートウェイと連携することで，ほかのクラウドに渡すデータへのアクセス可否を判断した上で，ユーザの属性だけでなく利用環境にも応じて，秘匿レベルを自動的に変更するなどの制御を可能にした。

アクセスゲートウェイでは，ネットワークサービスへのログインを行う際に，ユーザの利用環境（社内や社外の区別）や利用属性（役職，所属）に基づいて利用者の権限を判断することができる。また，利用者の代わりにそれぞれのサービスに代理ログインすることで，OAuthのほかのクラウドのサービスへのデータ受渡し可否の確認フェーズを検出して，利用者の権限の判断結果も同時に通知できるようOAuthを拡張し，ユーザ利用環境やユーザの属性などを，情報ゲートウェイに通知できるようにしている。

様々なクラウドサービス利用のため，各事業者と契約するたびに，通信プロトコル，認証方式などが異なるとその設定が大変になるが，このようにネットワークサービスのアクセスゲートウェイでまとめて制御することで，企業側の対応を軽減できる効果がある。

ポリシー制御

クラウド上の情報に対して適切なポリシーを情報ゲートウェイで適用することで，情報が誤ってクラウドから取り出されるなどの危険を排除し，安心して情報をクラウドに預けることが可能になる。また，クラウドに預けた状況を活用するという観点から，これまでの情報に対してのアクセス制御に加えて，情報をどのような形で提供するかといった観点が必要になってきている。

このため，情報ゲートウェイでは，クラウドに預けた情報に対する出力の制御として，「どの情報を」「誰が（ユーザ属性，ユーザ環境などを含む）」「どこで利用するために（渡す先のサービス，アプリケーション，クラウドサービスなど）」「どのような形式」で提供するかに応じた制御を行う必要がある。これらのパラメータに応じて，情報の出力の可否判断や，秘匿領域の決定，秘匿化のレベルの変更などを行う必要がある。これらのパラメー

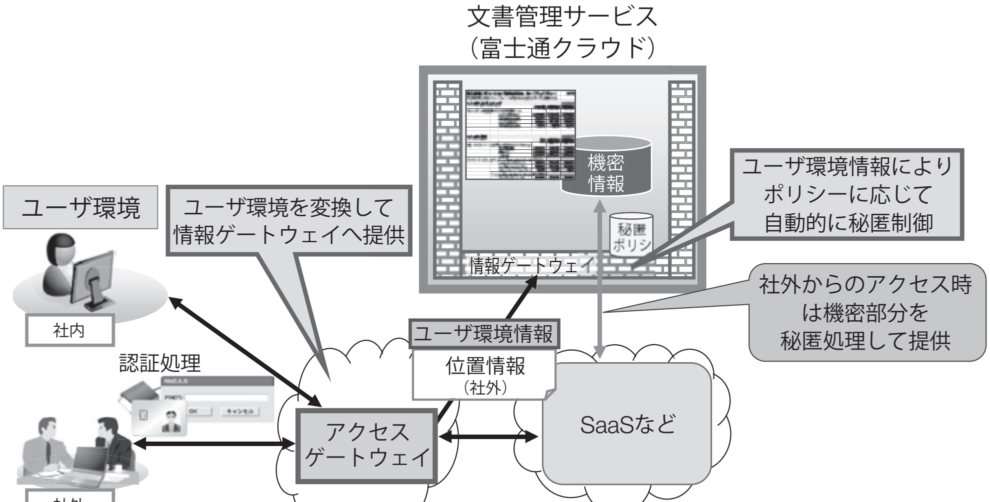


図-5　アクセスゲートウェイと情報ゲートウェイの連携
Fig.5-Combination of access gateway and information gateway.

タは様々であり，また利用のたびに異なることが考えられ，これを個別に設定しなくても制御を行えるようにするため，ポリシーが必要となる。アクセスゲートウェイと情報ゲートウェイと連携して，秘匿化のレベルを自動的に切り替えて出力を行うなどが可能である。

ポリシー管理では，クラウドに預けた情報に対するポリシーの設定は，情報の保有者である情報を預けたユーザが情報単位に行い，設定されたポリシーは情報ゲートウェイに設定され，設定されたポリシーに応じた制御が自動的に行われる。これにより，アクセスゲートウェイから渡されたユーザ環境情報や，ユーザ属性，サービスに応じて，秘匿化のレベルを変えて出力するといった，きめ細やかな制御を実現している。

む　す　び

今回開発したクラウド情報ゲートウェイ技術およびアクセスゲートウェイ技術により，ユーザ環境・サービス・情報の三つの条件を自由に組み合わせて，クラウドとやり取りする情報の機密度に応じた制御が可能になる。また，クラウド側の処理アプリケーションを社内のサンドボックス環境で安全に実行することで，社内の機密情報を外に渡さず，アプリケーションを利用することが可能になる。さらに，アクセスゲートウェイにより，他社のサービスを利用する場合にも，社内・社外・国外などユーザのアクセス環境に応じた秘匿化なども可能になる。

これらの技術は，オンプレミスとクラウド間，クラウドとクラウド間，またクラウドと他社サービス間，クライアントとクラウド間など，多様なデータ連携の場面で，情報漏えい対策技術として活用することが可能である。今後はこれらの技術を利用し，異業種間での協業や分業などの新たなクラウド利用を開拓していく予定である。

参考文献

(1) 伊藤孝一ほか：クラウドにおけるデータ秘匿化および追跡技術．電子情報通信学会IN研究会招待講演，IN2010-129，2011.

(2) RSAセキュリティ株式会社. トークナイゼーション. http://japan.rsa.com/

(3) C. Gentry：Fully Homomorphic Encryption Using Ideal Lattices. ACM Symposium on Theory of Computing（STOC2009），2009.

(4) 小倉孝夫ほか：他社クラウドを含めた安全なデータ・サービス連携方式の提案. 電子情報通信学会IN研究会，IN2011-57，2011.

(5) E. Hammer-Lahav, Ed.：The OAuth 1.0 Protocol. IETF RFC5849，April 2010.

著者紹介

津田　宏（つだ　ひろし）
ソフトウェアシステム研究所 所属
現在，セキュアナレッジ処理技術の研究開発に従事。

阿比留健一（あびる　けんいち）
ITシステム研究所 所属
現在，ネットワークサービス提供技術の研究開発に従事。

松尾昭彦（まつお　あきひこ）
ソフトウェアシステム研究所 所属
現在，クラウド間連携技術およびソフトウェア保守効率化技術の研究開発に従事。

長谷部高行（はせべ　たかゆき）
ソフトウェアシステム研究所 所属
現在，情報セキュリティシステム関連の研究に従事。