クラウドの発展と、安全・安心な社会へ向けて
Towards the Secure and Safe Society in the Development of “Cloud-based Anything”

東京大学名誉教授
日本クラウドセキュリティアライアンス会長
TM Forum Distinguished Fellow, Ambassador
吉田（よしだ）　眞（まこと）

ICT（Information and Communication Technology）の急速な進展が技術と社会の結びつきを一層強め、異なる多様な（技術）要素が相互に連携して大規模化しながら、市民生活、産業・社会活動を国内外で、またグローバルに担うようになっている。このグローバル規模の社会基盤への必須要件は、安心・安全、高信頼でカタストロフィに陥らないことである。このため、各要素と利用サービスに対して、定義の共通化と実現条件の共有（理解と合意）がグローバルとローカルなレベルで必要となる。このためには、個別の標準化・共通化だけではなく、総合的な視点と活動が必須であり、より複雑で高度な課題が存在する。本稿では、クラウドを中心とした最近の動向の概観から、特に安全・安心・セキュリティについて幾つかの視点と関連課題を述べ、関係者のグローバルな協働の必要性を示し、本特集の導入とする。

1．主要なキーワードと動向

キーワードは、IoT（Internet of Things）/M2M（Machine to Machine）、モバイル（mobile）、ビッグデータ（big data）、これらを総合化して価値を創出しサービス化を行う、クラウド（cloud（computing））、ソーシャル（social）である。物理面からのCPS（Cyber Physical System）[1]、人間にモノを付随させたMCS（Mobile Crowd Sensing）[2]といったパラダイムもこれらを基礎に議論されている（**図1**参照）。これらの要素とサービスが相互に絡み合って日々多様な新しい活動と分野が生まれており、学会や業界での関連セミナや国際会議の急増と、そこで扱われているキーワード、トピックの多種・多様化からも実感される。特に産業応用分野では、ドイツのIndustry 4.0[3]、米国でのIndustrial Internet[4]などが、具体的な活動を活発化している。

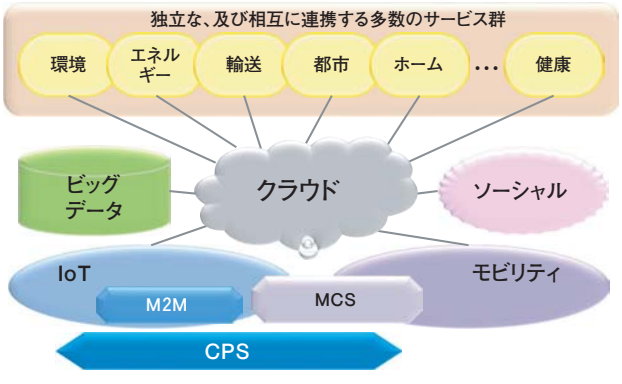

図1．最近の動向

これらが、将来の（及び既に先駆けが見られる）社会基盤の技術・サービス要素と考えられるが、中でも特に「クラウド」が、社会システムや各種サービスの処理・支援機能の中核として重要な役割を果たす。クラウドという言葉は、情報技術としてのcloud computingを意味するが、最近ではクラウドでのサービス、ビジネス、技術、運営単位など、広い概念で使われることも多く、本稿でも広い意味で用いる。クラウドは、ネットワーク化、特にインターネット（とワイヤレス）を前提にしているが、インターネットはベストエフォート、ワイヤレスの通信路はオープンエアである。このような“素性”を持つものを安全で高信頼な社会基盤としていくには、全ての個別要素（ハード、ソフト、ゲートウエイ、システムなど）に加えて、「要素間の総合連携」の観点から高度な課題の解決が必須である。利用目的によって、管理者・運用者の異なる複数のクラウドや複数のIoTが連携するので、これらの相互接続、相互運用も重要な要素である。

クラウドの基本思想は“所有から利用へ”であり、利用者からは所有に見えながらも実際には所有しない。利用者は、いわば“自己・自社の生活と管理”をクラウド環境に全て預けることになり、安全性、セキュリティ、プライバシの確保・保証が必須となることは言うまでもない。これらに関して、以下に幾つかの視点からの議論と課題を示す。

2．幾つかの視点から

情報の視点からは、「モノ」や「ヒト」自体の状態情報だけでなく、両者の組合せから得られる情報の分析によって、その周囲状況を判断することが可能となる。例えば、人間からの情報や動きから集中豪雨を判断する（例：「ゲリラ雷雨Ch.」[5]）、車の動きから渋滞を判断するなど、自然や社会的な変動を把握して即時や長期的な対応を取ることが可能と

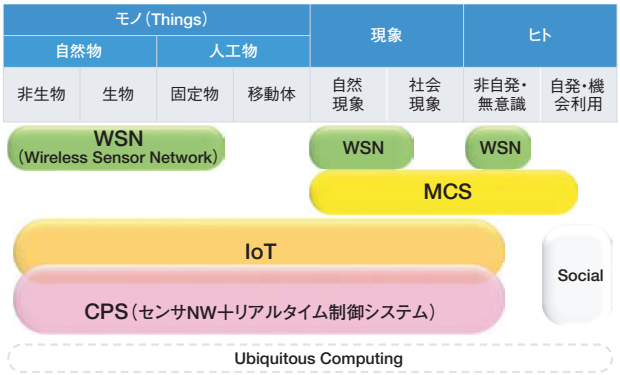

図２．要素の関係

なる。この分野は役に立つクラウドの応用サービスとして注目されており、研究・開発、試行が盛んに行われている。このようなシステムでは、対モノ・個人だけでなく、自然・社会全般への影響の観点から安全・セキュリティを検討しておく必要がある。人間とその動きの原情報を扱うことからプライバシへの対応、そのための原則・規定の確立と社会での共有も一層強調される（**図2**）。

「システムの視点」から見ると、システム化は「自動化」とほぼ同義として、個々の装置の個別監視・制御・運用から、技術の進展とともに関連システムへ、ネットワークの遠隔監視・制御・運用へと拡大し、さらには製造、金融、運輸等の産業応用・サービス全般へと、高度化し拡大してきた。システムが複数システムと組織を含む巨大システム化するとともに、近年ではさらに自己組織化、すなわち「システム・モノ」が自ら進化（少なくとも変化）する方向が志向されている。この場合、「自己組織化する複数の要素が互いに相手を損なうことのないこと」が基本であるが、相互に全く予期しない動作や複合事象が発生するおそれがある。これに対処するには、事前・事後の検証の役割が重要になる。特に、安全・セキュリティからは、このような動向を意識しながら、個別機能・組織に対して評価、認証、監査等を、広く認められた形で実施することとそのための仕組みの確立が有効な保証となる。

「標準化・共通化の視点」からは、これまでは基本標準と実装標準に加えて、コンソーシアムや業界団体で、共通開発手順、運用共通マップ、アプリケーション適用法等が開発され利用されてきた。技術分野間、業界・企業間の協力が必要な場合には、関係者が集まり共通枠組みを作る努力もされてきた。今後の多様なサービス環境でもこのような活動が必須となることは間違いないが、その規模と複雑性は今までにないレベルのものになる。その上に、元来標準化ではカバーできない/しない方がよいもの・ことが存在する。クラウド環境では、特にこれを意識する必要があり、正式標準化機関よりは、まずは広く多様な知を持ち寄れる場の方が効率的に議論できるであろう。

クラウドのサービスでは、複数の要素が相互連携して動くため、“各要素の個々のトラブルを解決しても、全体及び最終利用者のトラブルが解決されない”という問題が増える。これは、近代の分業化・専門分化により全体把握が困難になったこと、科学的に原理が解明されていなくとも技術的に実現できる（できてしまう）こと、多様な利用者・サービスの異なる価値観が混在するようになったこと、などによる。人間行動、技術、システム、規程、異分野連携などを織り込んだ、複合的な問題解決手法が必要となる。

3．セキュリティ対応でのネットワーク組織的な協力

セキュリティが暗号やウイルスというキーワードで語られていた時代には基本的な対策は「悪意に対抗する技術」であったが、クラウドに象徴される生活全般の基盤となると、人間がすること、機械がすること、自然現象で起きることを全てカバーするための思想、規範、方策が、国内だけでなく国際・グローバルに必要になる。原理的に攻撃側は防御側より常に有利なことから、防御側の組織的な協力が一層重要となる。

今後、グローバルな規範を形成していくには、関連する専門分野ごとの国際ネットワークの貢献が大きい。すなわち、市民社会、企業における関連分野の専門家、社会活動家が多極的なグローバル社会を形成する潜在的な力となる。要素開発者、サービス提供者だけでなく、利用者も参画して、既に発生している緊急問題に対処しながら、将来の事象に柔軟かつ確実に対応していく仕組み作りが望まれる。このための継続的な人材育成も重要な課題である。以上の観点から、安全・セキュリティ分野でも、本特集で紹介するCSA（Cloud Security Alliance）のような国際ネットワークの活動が大いに期待される。

4．クラウドの進展

クラウドは日々発展している。例えば、ビジネスモデルでは、中小企業ユーザと提供事業者の間を取り持つクラウドブ

ローカ[6]、アーキテクチャ・構成法としては、集中センタ型の問題点を解決するボトムアップ型のピア・ツー・ピア（peer-to-peer）クラウド[7]、などなど新しい動きは尽きない。このような常に変化していく環境では、常に新しい課題が発生する。人材育成についても、これまでにないスキルを有する人材の必要性が認識されており、2014年10月には、特にIoT、セキュリティで多様な分野間にまたがる人材の不足を補うために、米国で産・学・官が連携するコンソーシアムが設立された[8]。

一方で、クラウドが隆盛になる中、“世界の全てがクラウドだけに収束していく”という考えは、“多様性によって進化・発展がある”ということと相いれないことに注意する必要があろう。例えば、個々が自分のネットワークやサービスを創造し、それを適宜共有していくUCN（User Centric Networks）、UCP（User-Provided Networks）[9]も研究されている。

クラウドとこれらの個別的な構成がどう連携するかが、セキュリティ・安全性の総合保証の点からも課題となるであろう。

本特集では、以上の背景の下に、クラウドのセキュリティに影響する主要な要因について、基本となる四つの視点、すなわち、全般的な課題と枠組みの概観、技術面、利用の視点からの管理と法的側面、社会インフラの視点から、各記事で課題を挙げながら解説する。

クラウド、セキュリティという言葉を聞かない日はない。日本クラウドセキュリティアライアンス（CSA-JC）では、安全・安心・セキュリティの保証の観点から、基本的な要因についての知見の創出・集約機能となり、頼られる存在となることを目標に活動している。御協力と積極的な御利用をいただければ幸いである。

注

[1] 特集「サイバーフィジカルシステム」、Vol.55、No.9、2014年9月

[2] 特集 “Mobile Crowd Sensing: Part 1”, IEEE Com. Mag., Vol.52, No.8, Aug. 2014, “Mobile Crowd Sensing: Part 2”, IEEE Com. Mag., Vol.52, No.10, Oct. 2014

[3] “Recommendations for Implementing the Strategic Initiative INDUSTRIE 4.0”, Apr. 2014, http://www.plattform-i40.de/finalreport2013

[4] Industrial Internet Consortium, http://www.iiconsortium.org/

[5] http://weathernews.jp/guerrilla/

[6] Ian Scales: “Upcoming Business Models: Cloud Service Broker”, Telecom TV News, 5 Nov., 2014, http://www.telecomtv.com/articles/news/upcoming-business-models-cloud-service-broker-11905/

[7] Ozalp Babaoglu & Moreno Marzolla: “The People’s Cloud”, Oct. 2014, International, IEEE Spectrum, pp.44-49

[8] Bob Vavra: “Cisco Focuses on Skills, Security for Internet of Things”, 14 Oct., 2014, http://www.zdnet.com/cisco-focuses-on-skills-security-for-internet-of-things-7000034660/

[9] “User Centric Networking and Services: Part I”, IEEE Com. Mag., Vol.52, No.9, Sept. 2014

何が問題を複雑にしているのか

何のためか：クラウドもセキュリティもそれ自身で成立するものではない。すなわち、クラウドはそれによって「何を提供するか、実現するか」、セキュリティは「何を守るのか」を決めないと意味がない。クラウドサービスの安全・セキュリティは、本文にあるように個人、組織、社会、自然を含めた広い範囲を対象とする。標準化・共通化の検討には、これらの個々の視点と全体の複合視点の両者が必要である。一方、“グローバル・（グローカル）・ローカル”と、“国・社会・団体・個人”の関係についての議論が活発になっているが、単一の解釈、解は存在していない。このことは、議論を複雑にする一要因となっている。

将来が想像できるか：今眼前にある問題の解決法を考えると同時に、この解決法が将来どのような（考えもしなかった）ことを引き起こす可能性があるか、何にどう影響するか、何からどう影響されて連鎖を起こすか、について考えを巡らすことが大切である。特に社会・自然のインフラに関わることについては、“取り返しのつかないこと”が起きる危険性は避けるようにしなければならない。科学的・技術的な思考だけでなく、ある意味これを“超越した思考”が必要である。過去に経験のある「内なるリスク」に対しては統計的な算定が可能なため保険が用意できるが、「外から来る未来のリスク」には保険は用意できないからである。

人間の行動は理屈ではない：クラウドに限らないが、サービスの最終利用者は人間であるから、人間要因、社会共同体の要因（しきたりなど）が使い方・使い勝手や安心度を左右する。このため、近年、従来のQoS（Quality of Service）に、さらにQoE（Quality of Experience）の設計・実装・運用・評価が重要であるという認識がされるようになった。従来の取組は、人間工学、予測理論、管理工学などでの学問的なアプローチが主体であり、現実の実践面から確立した実現技術や保証方法とのギャップは大きい。これを埋める積極的な取組が望まれる。