クラウド利用における管理課題とセキュリティの法的側面

日本クラウドセキュリティアライアンス 運営委員
株式会社ITマネー 内部監査室 室長
山崎 英人

日本クラウドセキュリティアライアンス 監事
駒澤綜合法律事務所代表 弁護士
高橋 郁夫

日本クラウドセキュリティアライアンス 運営委員
弁護士法人向原・川上総合法律事務所 弁護士
吉井 和明

この稿では、クラウドを利用する立場における、セキュリティ管理、その説明責任、法的問題について、管理上の課題について、概要を述べる。

1. クラウドコンピューティングを導入する利用者の視点

クラウドコンピューティングの導入は進んでおり、プライベートクラウド、パブリッククラウド、更にはパブリッククラウド環境下に自社専用のプライベートクラウドを構築するデディケーテッドプライベートクラウドなどが浸透してきている。

その背景には、クラウド技術を導入すると比較的簡単に可用性の向上や資源利用の効率化が図られるという期待がある。図1は、マイボイスコム社が2014年7月に発表したアンケート調査結果[1]である。ハードウェアコストの削減、運用・メンテナンスコストの削減、業務効率の向上といった項目が上位を占めていることが確認できる。

一方、クラウドの利用を躊躇する層では、図2[2]に示すように、クラウド利用のデメリット・心配事項として、セキュリティやデータの破壊・損失に対する懸念が強いことが、同調査から見てとれる。

2. クラウドコンピューティングに対する懸念をもたらす背景

クラウドの基礎技術としては仮想化という要素が最も大きな役割を果たす。仮想化技術により、単一のハードウェア構成の上に仮想的に複数のコンピュータ機能を生成し

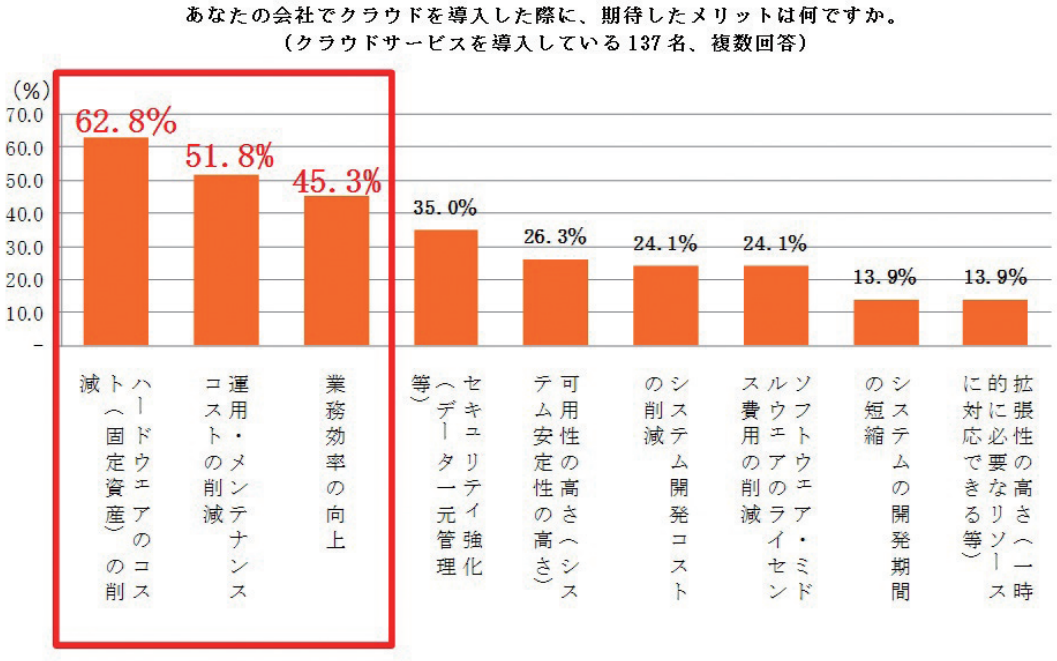

図1. クラウド化のメリット

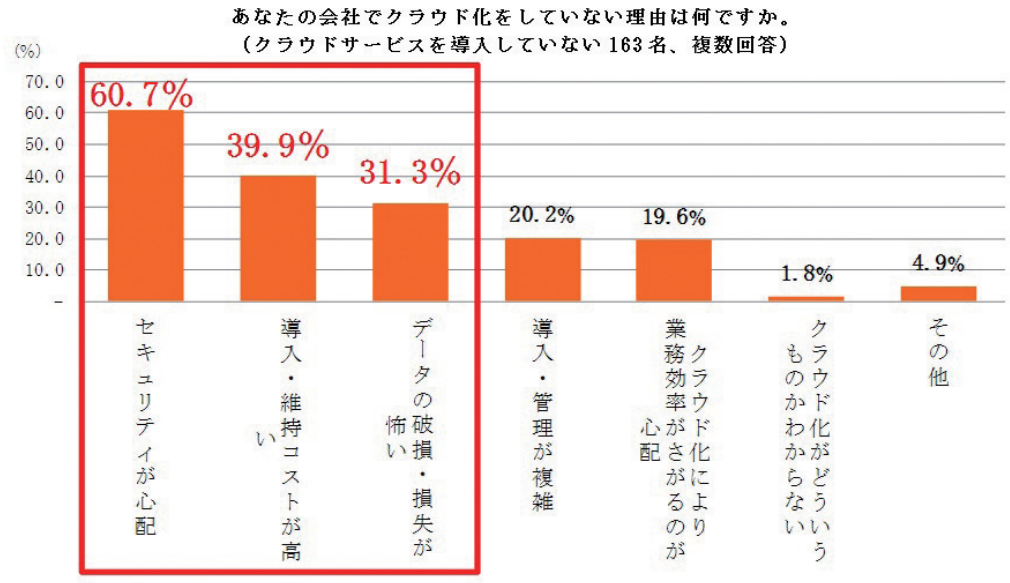

図2. クラウドサービスを導入していない理由

て、複数のユーザまたは複数の用途に提供することができる。その結果、仮想化技術により物理構成に関係無く論理構成が組めることとなった。利用者は物理的に所有・管理することなくコンピュータ機能の利用だけを享受することも可能となった。これが、コンピュータを「所有しなくても利用できる」ことやその運用・保守負担からの解放によるコスト削減や業務効率向上をもたらす。

クラウドサービスを提供する環境では、逆に、複数の、分散したハードウェアを束ねて、仮想的に単一のハードウェア構成のように見せる技術も多用されている。複数の物理的場所にまたがる環境を、一体化して利用できるのである。その結果、ユーザが利用している仮想的コンピュータと、それが物理的に存在している場所の間に対応関係が特定できないという問題が生じている。

利用に際してハードウェアの手当てを意識しなくてよいことは、ユーザにとって大きなメリットである。自分のマシンが今どこで動いているのかを認識せず、また何台のマシンを利用するのかを意識することなく、瞬時に構成変更が行える。これは変動の大きいコンピューティング負荷を管理する上で重要かつ便利な機能である。

一方、このことは、利用者から見ると今、自分のシステムがどこでどのように稼働し、誰にどのように管理されているのか、確認が取れなくなることを意味する。

実際に物理的セキュリティは大丈夫なのか? バックアップはどこにどのような形で取られているのか? データ削除をした場合バックアップ等も含めてちゃんと削除されているのか? これらの質問に、クラウドの利用者は自ら直接確認できる答えを持っていない。それは、クラウドサービス事業者の説明責任に依存せざるを得ない。

3. クラウド事業者の管理責任としてのGRC

事業者における説明責任は、クラウドをサービスとして提供し、それを利用するという商取引における、利用契約の重要な一要素となる。説明責任は、事業者の管理責任に裏打ちされて初めて意味を持つ。従い、クラウドの利用に際して、利用者は事業者の管理がいかに行われているか、その責任はいかにマネジメントされているか、に大きな関心が行くし、また、その点を踏まえて事業者及びサービスの選定をする必要がある。

ITシステムの管理体系として、近年RGCという概念がよく取り上げられるようになってきた。GRCとは、G（Corporate Governance）、R（Enterprise Risk Management）、C（Compliance & Audit Assurance）の三つの要素の頭文字をとったものである。**図3**にその概念図[3]を示す。

このうちガバナンスは経営陣が全体のマネジメントを把握し、経営管理の目標が組織に貫徹していることを確認し保証する経営活動であり、リスクマネジメントは、それに基づき経営リスクを総体的に管理しコントロールするプロセスである。そしてコンプライアンスは、これらすべての

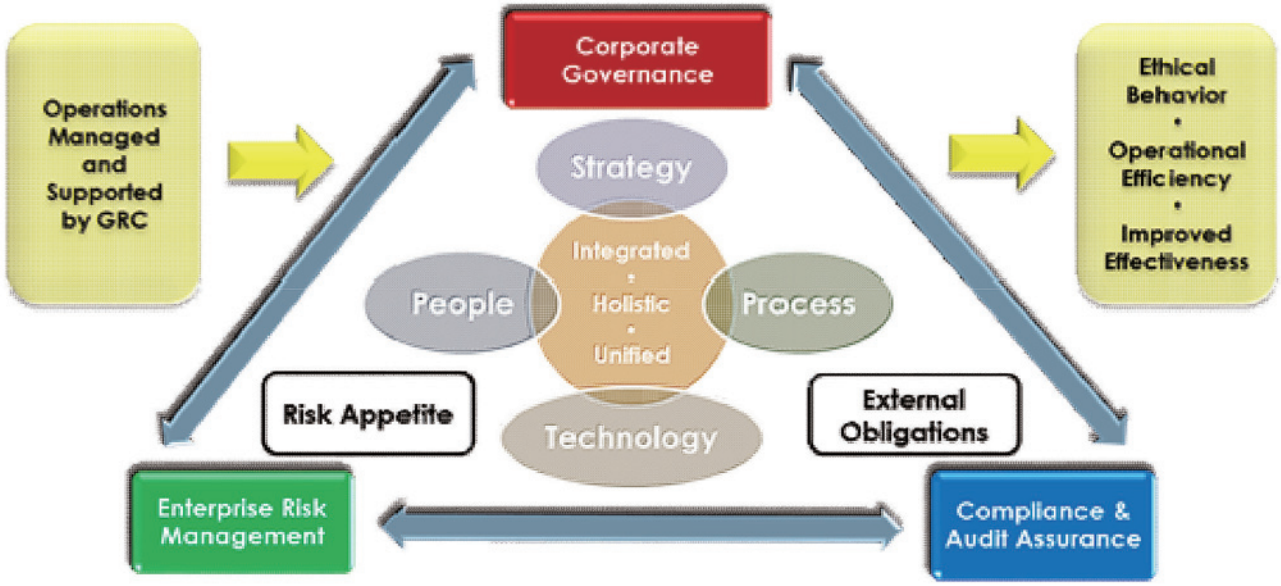

図3. GRCの概念図

経営・管理活動が法令及び社会規範上の企業の責務を満たしていることを担保するための取組みであり、それを支えるために、また経営・管理活動が正しく機能していることを確認・検証するために、監査という手続きが定義され、経営に組み込まれている。

GRCの実践上、特に日本の経営環境において問題になる要素に、セキュリティ管理がある。セキュリティ管理はGRCのうちR、すなわちリスクマネジメントの一環と位置付けられる。日本の企業の多くでは、経営陣に情報セキュリティ担当役員が定義されない結果、経営視点での情報セキュリティ戦略が描かれず、セキュリティ管理はセキュリティ担当者レベルで行われ、いわば戦術レベルでの局地戦の段階にとどまっている傾向がある。経営管理に通じた上で、情報セキュリティについてもその本質と真の課題を理解し、戦略に基づいてセキュリティ対策を実現できる人材の配置が必要になってくるのである。

4. クラウドのセキュリティ監査

経営管理の一環としての監査の面では、特にいわゆるJ-SOX法の導入以降、内部統制の実効管理の一環としての委託先管理が大きな課題となってきている。自社の内部統制と同等のセキュリティ管理が、委託先において実装され実施されていることを、委託元がいかに確認し第三者に対して担保するかという課題である。

特にパブリッククラウドを利用する場合、委託先管理はクラウドサービス事業者という外部組織に対するマネジメントを意味する。ここで、個別委託契約においては、個別に委託先の管理責任を契約上で規定し、その実装・実施に対する監査手続きについても相互に合意できる内容で取り決めることができる。（少なくともそのような交渉の機会が確保できる。）しかし、パブリッククラウドは一般的に、そのような個別的契約交渉を前提とせず、事業者が示す約款に利用者が（多くの場合ブラウザ上でボタンをクリックするだけで）同意することによって利用契約が成立する仕組みなので、委託先におけるセキュリティ管理についての監査は、契約上担保することが極めて困難になる。

その結果、事業者のセキュリティ管理の内容と程度について、利用者がどこまで確認できるか、事業者にどこまで確認させてもらえるかという綱引きが生じる。軽微な情報から経営を左右するような重要な情報まで、利用者がパブリッククラウド上に置く情報については重要度が分散している。重要度に応じたセキュリティ管理は、パブリッククラウドの上で可能なのか、可用性や完全性はどのように管理され、どのように担保されるのか。

例えば、アクセス管理は重要性に応じて決めるが、認証のためのパスワードが英数8桁と英数特殊文字を含む10桁の二つの強度が有ったとして、それをどの資産に適用するかは利用者が決める。そのため、事業者がどの程度の脅威を想定してパスワード等のセキュリティ対策の強度を決めているか、利用者にとって自社で扱う情報の重要度に見合った対策なのか確認する必要がある。事業者がこの点を開示しない場合には、利用者は自社のセキュリティポリシーがクラウド上で実現できるか確認できないことになり、管理上並びに監査上の管理責任が全うできないという問題が生じてくる。

このために、標準に基づく、あるいは共通のセキュリティ管理尺度を設け、それに基づいて事業者のセキュリティ管理内容を評価し、その評価結果を公表し、あるいは利用者と共有することで、個別のセキュリティ管理契約やセキュリティ監査に代替しようとする考え方が出てくる。この考え方に沿って、ISO/IECではセキュリティマネジメント標準にクラウド固有の体系を付加する取組み（ISO/IEC27017の制定）が進められている。これは日本が経済産業省の策定した「利用者のためのクラウドセキュリティマネジメントガイドライン」を基に国際標準化を提唱したもので、それを受けてクウラドセキュリティアライアンス（CSA）をはじめとする各国代表が検討する作業が続けられている。また同様の意味で、CSAの提供する「クラウドセキュリティガイダンス」や「Cloud Control Matrix」に基づく評価が浸透しつつある。更に、CSAではそれを体系化したSTAR[4]という仕組みを整備して、クラウド事業者の利用を促している。

このような標準に基づく評価に際して、それを評価する人、一般には監査人と呼ばれる機能または立場の存在が必要となる。まずは事業者内部での監査・評価が必要であるが、そのための組織や人材の整備が十分に進んでいないという問題がある。また、第三者評価を行うための独立した監査人については、その資質を保証するための資格制度が必要である。

まず、企業内での監査に従事する人材については、独立性と専門性の問題がある。最新のセキュリティ対策を理解した監査人が少ない問題や、企業が十分にコストを掛けない問題、人材不足のためにセキュリティやクラウドを十分に理解した人材が内部監査要員として配置されていない、などの問題がある。

日本では、日本セキュリティ監査協会[5]がクラウドのセキュリティ監査ができる情報セキュリティ監査人の育成に取り組んでいるが、クラウドを理解できる監査人はまだごく限られているのが実情である。CSAでは、直接監査のための資格ではないが、クラウドのセキュリティについて十分知識と理解を持った人材を認定する、CCSK[6]という資格認定制度を設け、世界で資格認定を行っている。日本でも日本語で受験[7]可能な体制が整っている。

5. クラウドコンピューティングにおける法的諸問題

クラウドコンピューティングについては、そのサービスの提供に関連する場所が、複数の国に及ぶことも多いために、どこの国の法律が適用されるのか、ということが議論されることも多い。しかしながら、この問題は、一筋縄ではいかない問題である。どこの裁判所で、どのような問題が論じられるのか、ということで場合分けをしなければ正確な回答にはならないからである。しかも、問題となるのは、裁判所での判断が問われる場合のみではない。そこで、具体的な問題に集中して、論じることにしよう。具体例として、日本に所在する会社Xが、米国に所在するクラウド提供者Y（データ処理も米国でなされる）に、電子商取引を依頼しており、そのクラウド提供者が、脆弱性対応を怠り、日本の顧客Aの情報を流出させ、それにより顧客Aに損害が発生した場合を考える。

このような場合、まず、どこの裁判所で論じられるのかということが問題になる。我が国の裁判所が管轄権を有するかどうか、という点については、民事訴訟法３条の２によって定められる（例外として法の適用に関する通則法３条の９）。一方、米国の裁判所が管轄権を有するかというのは、米国の連邦法の管轄の定めによる。一般論としては、米国のほうが、管轄権としては、広いものといえ、本件では、認められるであろう。すると、双方の裁判所がともに管轄権を有しうることになる。

それらの場合にそれぞれ、どこの法律が適用されるか、というのは、別の話である。例えば、X社とY社との間の法律関係であれば、基本的に当事者の合意による（この理は、日米において、差異はない）。それに対して、顧客Aが、被害を受けたとして不法行為を根拠にY社に対して損害賠償の請求訴訟を提起した場合に、どこの法律で過失や損害が評価されるのか、という具体的な問題が起こりうる。単なる個人情報の流出を根拠とする場合であっても、日本においては、日本法のもとで、損害を構成しうるとするのが一般であろうが、米国においては、かかる流出自体

を損害とするのは、一般的ではない。一方、損害が認められると、その評価は、米国で金額的に高く評価される傾向があるという問題もある。また、純粋に、日本法の見地から見ても、不法行為地として、被害をうけた顧客Aの法を適用するのか、不法行為者である会社Yの所在地の法を適用することになるのか、というのも明確な解釈が存在するとも思えないことになる。

また、クラウドの関係する法律問題は、上述のような民事紛争に限られるものではないということは重要である。このような場合、国家主権が、民事紛争における法律問題と比較して、より直接的な影響を及ぼすことに留意が必要である。この影響としては、データの域外移転禁止、コントロールしうるデータに対するアクセス、証拠の収集に関する規定などの問題がある。

データの移転禁止問題には、個人情報保護に基づく移転禁止（EUデータ保護指令25条の定めが例）、行政庁の監督が望ましい分野における移転禁止（医療情報については、法令に基づく資料を円滑に提出できるように国内法の適用が及ぶ場所に設置することとされている）、国家安全保障からする情報の移転禁止（外為法25条が例）などがある。

上記の情報流出の例を考えたときに、米国所在のY社に対して、法執行のために、データの提出を求める法的な命令等がなされた場合に、Y社は、これに応じなければならないことになる。このような法執行のための命令等がなされる要件は、各国によって異なる。通信の途上のデータを法執行機関が取得するのには、我が国においては、通信の秘密との関係があるため裁判所の発布する令状が必要とされるが、そのような例は、必ずしも、一般的なものではないということは、留意しておくべきである。また、X社に対して適法に発せられた令状に対して、データの記録されているのが外国であるとして、開示を拒絶しうるわけではないことも重要である。

クラウドの法適用に関する国際的な側面については、上述のようにきわめて複雑であり、法適用に関係するリスクの評価・対策を重要にしているものということができる。

6. クラウドコンピューティングにおけるデジタル･フォレンジックの問題

クラウドコンピューティングの法的課題に関しては、更にもう一つ、デジタル・フォレンジックという課題がある。法廷で争うような場合における電子的証拠に関わる手続きや考え方の問題であるが、対象となるデータがクラウド上にあり、クラウド事業者の管理下にあることが、問題を複雑にしている。

デジタル・フォレンジックは、「インシデントレスポンス……や法的紛争・訴訟に際し、電磁的記録の証拠保全及び調査・分析を行うとともに、電磁的記録の改ざん・毀損等についての分析・情報収集等を行う一連の科学的調査手法・技術」だが[8]、インシデント発生時の損害拡大の防止の為の原因究明、義務として[9]、あるいは任意の事故情報の公開、刑事事件となった場合の捜査、民事上の請求の基礎としての事実把握や、証拠の信用性確保などの場面で重要となる。

デジタル・フォレンジックが必要となる最たる例は、民事、刑事上の裁判において電子情報を証拠として提出し、あるいは義務として開示するような場合である。インシデントの予防や、裁判となる前段階で問題を解決することも、重要な役割であるが、その際も、当該インシデントに対してどのように向き合うかについて、最終的な法的帰結を意識せざるを得ない。

裁判において提出する証拠は、要証事実を立証するに十分なものである必要があり、また、その証拠が改ざんや変更などがされた疑いのない、信用に足るものである必要がある。

そこで、信用性を損なうことなく、十分な証拠としてのデータを収集するべく、デジタル・フォレンジックにおいては、「事故や不正行為、犯罪といったインシデントに関わるデジタル機器に残されたデータの中から、電磁的証拠となり得るものを、確実に、そのまま（As-is）で、収集（Collection）･取得（Acquisition）し､保全（Preservation）しておくこと」が最も重要とされる[10]。

クラウド環境では、仮想化技術が用いられる（多くの場合）と共に、システムの管理権限が事業者側にあるため、利用者がコントロールできる範囲は制限され、オンプレミス環境で行うことのできた、上述のような適切なフォレンジックを行うことができなくなる[11]。

例えば、収集・取得に関し、自身でログなどの必要な情報に接触することは困難であるかもしれないし、事前の利用契約やSLAでの合意なしに、利用者がクラウド提供業者に対してログの開示を求めることも困難となることも考えられる。

また、クラウドコンピューティングにおいて、利用者は、物理的な設備そのものを管理していないことから、保全の点でも、例えば、証拠の信頼性を確保し、あるいは後日の

検証に備えるために、完全物理複製を行うような方法は、採ることができない可能性が高い。

特に、互いを知らない利用者同士がマルチ・テナントにおいて共存しているパブリッククラウドの場合などは、ある利用者がフォレンジックを必要とした場合でも、他の利用者の情報に触れることになりかねないフォレンジックの実行を許すことはできないだろう。

データの保存される環境がオンプレミスではなく、クラウドであるからといって、信用性の担保された証拠としての情報を提出しなくてもよいことにはならず、提出することのできないことによるツケは、結局のところ、データを保存した利用者に返ってくることになる。

例えば、米国における裁判では、事実審理前に双方当事者より情報を開示しあう制度であるdiscoveryの一種であるe-discoveryの制度において、膨大な電子情報の開示を求められることとなるが、不開示があれば、不利な事実が認定され、あるいは不利な判決が下されるなど厳しい制裁が課されることとなる。

日本においても、当事者間での開示を求める当事者照会制度（同法163条）、裁判所への申立てにより行う文書提出命令制度があり（同法19条、220条）、これらの開示の範囲はdiscoveryのそれと比べてかなり限定的であるものの、電子情報が準文書として提出するよう求められる場合があり、提出がない場合に不利な認定がなされる場合がある[12]。

そのため、利用者は、クラウド提供業者に対して、自分の触れることのできない情報の開示を求める必要が生ずることを考え、自身のクラウドの利用方法によっては、クラウド提供業者との契約上、インシデント発生時には、これらの情報を取得できるよう規定が置かれているかを確認すること、これらの情報に関する保管期間を確認しておくことが望ましいものと思われる。また、利用者自身で情報の仕分けをし、事前に情報毎の保管方法やクラウドの利用方法について検討しておく必要もあるだろう[13]。

なお、Cloud Security Allianceでは、一般的なデジタル証拠の特定、収集、取得、保全のためのガイドラインであるISO/IEC27037:2012をクラウド環境にマッピングすることを目的とする文書である「Mapping the Forensic Standard ISO/IEC 27037 to Cloud Computing」をリリースしており[14]、クラウド環境でのデジタル・フォレンジックに対する備えをする上で、参考となるものと思われる。

以上、利用者の立場から見た、セキュリティ面における管理課題を概観した。このように、コンピューティングが複数の主体と複数の物理的場所（法管轄も異なることを意味する）にまたがることに伴う問題は多岐にわたり、かつ極めて複雑である。しかし、クラウドがもたらすメリットを考える時に、それら課題の前で立ち止まることは賢明でなく、実践の中で実際的な解を積み重ね、経験・事例の共有と共通理解を進めることにより、クラウドがより容易に、より広く、より高度に利用できるようになることを期待したい。

注

[1] マイボイスコム株式会社『企業のクラウド化について』2014年7月発表

[2] マイボイスコム株式会社『企業のクラウド化について』2014年7月発表

[3] クラウドコンピューティングのためのセキュリティガイダンス V3.0 http://www.cloudsecurityalliance.jp/j-docs/csaguide.v3.0.1_J.pdf

[4] Security and Trust Assurance Registry

[5] http://www.jasa.jp/

[6] Certification of Cloud Security Knowledge

[7] http://www.cloudsecurityalliance.jp/ccsk_j.html

[8] デジタル・フォレンジック研究会ウェブサイト「デジタル・フォレンジックとは」<https://digitalforensic.jp/home/what-df/>

[9] 例えば、個人情報保護法20条の安全管理措置としてのインシデントの公開など。

[10] 特定非営利活動法人デジタル・フォレンジック研究会「技術」分科会ワーキンググループ「証拠保全ガイドライン第3版」<https://digitalforensic.jp/wp-content/uploads/2014/06/5b0f6b0e93f42b5b3fd27a290d977a681.pdf>2頁

[11] CSAガイダンスでは、「第3章//法律問題：契約と電子的証拠開示」において、「3.3　電子的証拠開示での特別な問題点」として、フォレンジックと開示の問題を取扱っている。同ガイダンスの日本語版は、http://www.cloudsecurityalliance.jp/guidance.htmlよりダウンロードできる。

[12] 日本の民事訴訟における各制度とdiscoveryの違いを検討したものとして町村泰貴・小向太郎編著「実践的eディスカバリ　米国民事訴訟に備える」(NTT出版,2010.3)がある。

[13] 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2013年版」<http://www.meti.go.jp/press/2013/03/20140314004/20140314004-2.pdf>72～73頁。なお、同ガイドラインでは、外部の継続的証拠保全サービスの利用も、方法として存在すると述べている。

[14] https://cloudsecurityalliance.org/download/mapping-the-forensic-standard-isoiec-27037-to-cloud-computing/