特　集

IT・ICTと営業秘密の保護

――クラウドコンピューティングとの関係を中心に――

岡　村　久　道*

抄　録　営業秘密を取り巻く環境は，いま激変の渦中にある。その主因は，グローバル化の進展とともに，IT（情報技術）・ICT（情報通信技術）（以下，この両者を「IT等」と総称する）の急速な進歩である。非正規雇用の増加による企業帰属意識の減少，アウトソーシングの増大等の点が，それに拍車を掛けている。他方でIT等は，もはや企業活動にとって不可欠なインフラとなっており，中でも近時におけるクラウドコンピューティングの普及はめざましい。本稿は，このような観点から，IT等と営業秘密保護との関係について，クラウドコンピューティングとの関係を中心に考察を試みるものである[1)]。

目　次

1．実際に発生した重要事件

最初に，営業秘密をめぐる現状を把握するために，実際に我が国で発生した近時の主な重要情報漏えい事件を概観し，その傾向を分析しておくことにする。

このような事件を時系列順に並べると，①国内大手電機企業が世界を対象に運営するゲーム関係のネットワークからサイバー攻撃によって大量の個人データを漏えいさせた事件（2011年発覚），②国内大手重工企業が防衛関連情報を狙ったサイバー攻撃を受け，ウイルス感染被害を受けた事件（同年発覚），③宇宙航空研究開発機構（JAXA）及び提携先の国内大手重工企業がサイバー攻撃を受け，ウイルス感染被害を受けて宇宙技術関連情報を漏えいさせた事件（2012年発覚），④国内大手教育企業の委託先従業員が大量の顧客データを漏えいさせて多数の名簿屋に流れた事件（2014年発覚），⑤日本年金機構がサイバー攻撃によるウイルス感染が原因で大量の年金情報を漏えいさせた事件（2015年発覚），⑥国内大手製鉄企業の元従業員が当該企業の提携先であった外国の製鉄企業に電磁鋼板の製造プロセス等の技術情報を漏えいし，当該情報が当該国外企業から別の国の企業に二次流出した事件（2015年に東京地裁で和解），⑦国内大手企業のフラッシュメモリ技術情報

* 弁護士，京都大学大学院医学研究科講師（非常勤）
Hisamichi OKAMURA

を，業務提携先の元技術者が，付与されたアクセス権を濫用してネットを介してデータベースから端末にコピーした上，これを可搬型記録媒体にコピーして持ち出し，外国企業に不正漏えいさせた事件（不正競争防止法違反で有罪とした刑事判決として東京地判平成27年３月９日判時2276号143頁）等がある。

以上の事件では，いずれも重要な技術情報もしくは大量の顧客情報が対象となっている。

これらのうち，①②③及び⑤はネットを介した外部からのサイバー攻撃によるものであり，国外からの攻撃である可能性が強い点では，同時にグローバルな事件といえよう。④⑥及び⑦は内部不正と呼ばれる類型のものであるが，⑥及び⑦はグローバルな事案である一方，少なくとも④及び⑦は内部者によるアクセス権濫用によるものであるという点で，やはりIT等に関連した事件である。

このようにして，企業の情報資産が，内部者の不正行為（いわゆる内部不正），もしくは外部からのサイバー攻撃によって，国内外への流出の危機にさらされているという傾向が近時は見受けられており，いずれにしても前記要因によるリスクの増大が現実化したものといえよう。

2．情報資産の法的保護－オープン・クローズ戦略

ここでは前提問題として，情報資産の法的保護に関する近時における制度面の動向について概説しておきたい。

情報資産を経営資源として利活用するためには，これを適正な法的保護の対象にすることが不可欠となる。その方法として，自社の情報資産の管理を他社に委託する場合のように，当事者間における契約法理による保護を図るべき場合もある。しかし，そうした場合を含め，第三者との関係で法的保護を及ぼそうとすれば，当該情報資産を保有する企業としては，知的財産権に頼らざるをえない。

こうした方法として情報資産の特許化は有用である。譲渡可能な排他的独占権を一定期間取得しうる等の利点を有するからである。しかし，特許化による保護にも限界がある。法定の保護期間が限定されている上，出願した技術情報の内容がオープン化されるため，競合企業に開発動向が明らかになるからである。さらに周辺特許を取得されて事業展開に支障を生じるおそれもある。したがって，情報資産を特許化することなく，秘匿化（クローズ化）して不正競争防止法上の営業秘密として保護することが，企業にとって得策である場合が多い。技術標準化等のため自社技術を特許化しようとする場合でも，出願公開までの間は秘匿化を要し，特許化が認められた場合でも，実際には秘匿化したパラメータ等の周辺的な技術ノウハウが製品差別化にとって重点となる場合が多い。これらの点が，両者の適正な使い分けという「オープン・クローズ戦略」が強調されている理由である。

さらに，新製品の販売開始予定時期，他社から預かっているデータ，顧客情報のような非技術情報については，特許化することができないだけでなく，不正漏えいした場合には，逆に企業として契約違反，プライバシー侵害その他の法令違反等の責任を問われる場合もあるから，自社を守るためには営業秘密保護に頼らざるをえない。例えば個人情報保護法は，顧客情報を保有する企業を保護するものではなく，当該顧客の権利利益を保護しようとするものである。同法の下では，自社が保有する顧客情報の漏えい元となった企業は加害者的立場となり，被害者たる当該顧客から非難を受け，個人情報保護委員会から処分を受けるべき地位に立たされるにすぎない（但し，個人情報保護法2015年改正によって，顧客名簿は個人情報データベース等不正提供罪の対象となった）。さらに当該顧客からプライバシー権侵害として損害賠償責任等

を問われることもある。

以上の諸点を踏まえ，企業としては，保有する情報資産の積極的・消極的価値を把握・評価した上，保護の必要性が認められるときは，どちらの方法で保護すべきか等の点を先に分類して，それに即した方策を講じておく必要がある。一種のアセスメントといえよう。

3．不正競争防止法2015年改正による保護強化

有用性のある情報資産を秘匿化する場合には，営業秘密として不正競争防止法による保護を受けるべきことになる（但し，営業秘密による保護は，製品のリバースエンジニアリングの前には無力であるという限界をわきまえる必要がある）。

これまで同法による営業秘密保護は1990年の立法化以降，数次にわたる改正を経て強化されてきたが，営業秘密保護の有する重要性は増加の一歩をたどる半面，それに対するリスクも前述のとおり増大している現在，不正競争防止法の2015年改正による営業秘密のさらなる保護強化は，時宜を得たものといえよう。

この改正は，抑止力の向上（営業秘密の価値上昇・侵害懸念の増大）と処罰範囲の整備（IT環境の変化）を目的とするものとされている。

前者（抑止力の向上）として，法定刑の引上げ（実行行為者及びその背後の主犯たる法人に対し，罰金の引き上げ，不当な収益の没収，非親告罪化等の措置），賠償請求等の容易化（立証負担の軽減），侵害品の譲渡・輸出入禁止（特許権侵害品と同様に，他人の営業秘密を侵害した製品の悪意・重過失の譲渡・輸出入を禁止），除斥期間の20年への延長が図られた。

後者（処罰範囲の整備）として，未遂行為の処罰化，情報の転売行為の処罰範囲拡大（営業秘密の転売利用を処罰対象に追加），インターネット上の情報の窃取行為の処罰化（インターネット上に保管された情報の窃取を処罰対象として明確化）が図られている。情報の転売行為の処罰範囲拡大は，前掲事件④で流出した情報が名簿屋に転売されたことへの対策であった。インターネット上の情報の窃取行為の処罰化は，前掲事件①②③及び⑤のような，ネットを介した外部からの越境サイバー攻撃に対処しようとするものである。

4．営業秘密管理指針の全面改訂

営業秘密として保護を受けようとする場合には，秘密管理性要件を満たす必要がある。

営業秘密に関する秘密管理性要件の解釈について，最近では一部の下級審判例で混乱が見受けられた。これまで経済産業省が策定してきた「営業秘密管理指針」には，秘密管理性要件を満たすために有用な各種の手法が網羅的に例示されていた。ところが，当該手法はベストプラクティスにすぎないにもかかわらず，少しでも欠けている点があれば秘密管理性を認めることができず，営業秘密として保護が受けられないとする誤解が一部に存在していたのである。

しかし，秘匿されている情報資産を故意に不正流出させた者が，いわば「戸締まり」に一部不備が存在したことを主張して責任を免れることができるとするのでは不合理きわまりない。そのため，かかる誤解を解消すべく，2015年に同指針が全面改訂され，それによって前記手法の大半を削除してシンプル化が図られるとともに，前記手法すべてを満たすことを要しない旨の行政解釈が示された。これによって，今後は司法においても過度に厳格な解釈が緩和方向へと是正されることが期待されている。

5．未然防止策としての「秘密情報の保護ハンドブック」の策定

このように不正競争防止法による事後的な責任追及は重要であるとしても，不正漏えいを未

然に防止するために企業の自主的な管理策の強化が有用であることに変わりはない。しかもIT等に関連した脅威が増加している現在，前記取組みはIT等に対応したものでなければならない。現にサイバーセキュリティ基本法の制定によって，民間部門を含めて我が国のセキュリティの基本的枠組みが規定され，前掲事件⑤を重視して，2016年の同法一部改正によって保護の枠組みの強化・拡大も図られている。このような情勢を踏まえ，同指針とは別に，経済産業省は「秘密情報の保護ハンドブック～企業価値向上にむけて～」を2016年２月に策定し，IT等への対応も含めて，秘密管理のために有用なベストプラクティスとなる手法を示している。「営業秘密」ではなく「秘密情報」という言葉を用いているのは，このハンドブックに記載された管理策すべてを講じなければ秘密管理性要件を満たさないという誤解を受けることを回避するためである。

6．クラウドコンピューティングの利用による保護

ところで，IT等の利活用とサイバーセキュリティ保護の双方を図るものとして，クラウドコンピューティングの利用が脚光を浴びてきた。

クラウドコンピューティングとは，インターネット等を介して設置されたサーバその他の機器に接続して利用する形態をいうが，ネットの彼方にあるサーバ等を「雲」に見立て，このように呼ばれている。

というのも，従来のように各企業が自前でサーバを構築・設置する方法では，サイバー攻撃から身を守って安全に運用することに大きな困難が伴う。高度なセキュリティ機能を有するハードウェア・ソフトウェアの設置・更新，スキルの高い要員の確保，それらの措置に伴う高額な維持経費や手間を要するからである。これに対し，十分なセキュリティ対策が施されたクラウドサービスを利用する方法は，安全面だけでなく，コスト面でも有用であるとされてきた。企業それ自体の事件ではないが，現に総務省は，市区町村のセキュリティに関するリソースが必ずしも十分といえないことから，「自治体情報セキュリティクラウド」政策を打ち出し，「自治体情報セキュリティ対策検討チーム」の中間報告「自治体情報セキュリティ緊急強化対策について」（2015年８月12日），報告「新たな自治体情報セキュリティ対策の抜本的強化に向けて」（同年11月24日）によって，インターネットからのネットワーク分離等とともに，都道府県にサーバ等の機能を集約させるべきものとしている。都道府県が設置するサーバ等は，専門のセキュリティベンダに監視させているケースが多い。

こうしたクラウドへの集約化という手法は，企業としても，小規模な地方の支店・支社，子会社のセキュリティ対策を検討する上で，大きな参考となるはずである[2)]。大企業であっても，本社においては万全の管理策が講じられているのに対し，地方の支店・支社，子会社においては人的･物的リソースの問題もあって，必ずしも十分な措置を独力で講じることは容易ではなく，情報資産の利活用という観点からも，全グループのクラウドへの集約が合理的であるといえよう。

クラウドサービスは，IaaS型（いわば仮想レンタルサーバであって，それにユーザーが自らOSをインストールしてアプリケーションを構築して利用する形態），PaaS型（事前にクラウドベンダ側が用意したツールを利用してユーザーが仮想レンタルサーバ上にアプリケーションを構築して利用する形態），及びSaaS型（事前にクラウドベンダ側が用意したアプリケーションをユーザーが利用する形態であり，ASPと呼ばれてきたもの）に大別することができる。

クラウドのサイバーセキュリティに関する指針として，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」，総務省「地方公共団体におけるASP･SaaS導入活用ガイドライン」，総務省「ASP・SaaS事業者が医療情報を取り扱う際の安全管理に関するガイドライン」等がある。

その場合でも，ユーザーによる管理策はクラウドベンダ側が許容した範囲に限られてしまう。例えば，クラウドベンダ側がSSLのような暗号通信に対応していなければ，それをユーザー側が実装しようとしても不可能である。おまけにクラウドベンダが自ら開発を委託される場合も少なくなく，その場合には開発委託契約に基づいて責任を負うことになる。以下，クラウドコンピューティングの特徴を分析した後，それを利用・管理する際に留意すべき点を解説することにする。

7．クラウドコンピューティングの特徴

クラウドコンピューティングに共通する特徴として，（ａ）データの越境性（ボーダレス性），（ｂ）データの所在の不明確性，（ｃ）サービスの重層性という諸点を指摘しうる。こうした特徴を踏まえ，クラウドコンピューティングの利用には，限界をわきまえる必要があることも事実である。

第１に，上記（ａ）（ボーダレス性）に起因する問題がある。従来の純然たる専用線接続と異なり，インターネットを用いたクラウドコンピューティングの場合には，ユーザーが接続に要する通信コストはデータセンター設置地との距離に比例しないので，利用料金が安い国外のクラウドを利用することが可能となる。これに伴い，ユーザーのデータも越境して国外に置かれることが多い。その結果，何らかの法律紛争が生じた場合，どこの国の裁判所で（国際裁判管轄），どこの国の法令を適用して（準拠法），どこの国の執行機関が法律を執行するのかという問題等が発生する。

刑事手続の点でも，漏えい等の事故発生時に，国外のクラウドサーバには日本の捜査権が及ばないという問題がある。営業秘密の侵害については民事的救済も用意されているが，企業は強制捜査権を有しておらず，漏えい原因調査の技術的スキルという点でも限界がある。そのような場合には捜査機関による刑事的救済に頼らざるをえない。これに対し，国内のクラウドサーバを選定すれば，こうした問題は回避しうる。とはいえ，国外からのサイバー攻撃には攻撃元に対する直接的な捜査が困難であることに変わりはない。

第２に，上記（ｂ）（データの所在の不明確性）がもたらす問題がある。クラウドでは，コンピュータリソースが仮想化されているので，必要に応じて，異なる国のデータセンター間をフレキシブルに移動させることが可能となる。しかし，それによってデータの所在国は不明確とならざるをえない。それに加えて，データセンターの具体的所在地は，クラウドベンダ（クラウドサービス提供事業者）側のセキュリティ保持を理由に公表されていないことが多い。これらの理由によってデータの所在が不明確になれば，適用される法令が不明となる。事故が発生した場合に，その原因を調査することも困難となり，いきおいクラウドベンダ側の説明を鵜呑みにするほかなくなってしまうなど，多くの問題が生じうる。

第３に，上記（ｃ）（サービスの重層性）がもたらす問題がある。SaaS型サービスの提供は，他のベンダが運営するPaaS型，もしくはIaaS型のサービスを利用して行われることが多く，その場合には，重層的な構造を有するサービスが，ユーザーに提供されるという意味である。これによって，上記（ａ）及び（ｂ）の特徴は，さらに複雑性を増す。すなわち，ユーザ

ーのデータ等が，どこの国に所在するPaaS等のデータセンターで扱われているのか，ユーザーはもとより，上記SaaS型サービスベンダすら，正確に把握することが困難になっている。

8．クラウドベンダ・クラウドサービスの適正な選定

以上の諸点を踏まえて，適正なクラウドベンダを選定することが重要となる。クラウドサービスを運営するベンダごとにセキュリティ水準に高低差があり，現にクラウドサーバからの大規模な漏えい事件も発生している。クラウドサーバに障害が発生したときには，それに依存する自社の業務全体に対し直ちに多大な支障が及ぶおそれもある。クラウドベンダが倒産したときも同様であろう。その場合には，当該ベンダがバックアップしているはずのデータすら取り戻せなくなるおそれがある。当該ベンダが競合他社に買収されることもある。これらの点が示すように，ベンダの適正な選択は極めて重要である。

クラウドサービスの種類選定という問題もある。その内容次第では，カスタマイズの自由度が低いため自社業務への利用が不可能なケースも多い。ユーザーの要求水準とサービス仕様との「フィット＆ギャップ」といえよう。IaaS型，PaaS型，及びSaaS型の順序に比例して，クラウドの利点である導入・維持の手軽さが増す半面，カスタマイズの自由度は反比例する。ユーザーによる管理策はクラウドベンダ側が許容した範囲に限られてしまう。例えば，クラウドベンダ側がSSLのような暗号通信に対応していなければ，それをユーザー側が実装しようとしても不可能である。おまけにクラウドベンダが自ら開発を委託される場合も少なくなく，その場合には開発委託契約に基づいて責任を負うことになる。そのため，構築の自由度が高くなることに比例して，クラウドサーバ内に自前で構築したソフトウェア環境について脆弱性が残るおそれが増大するという矛盾が生じうる。

9．サービス提供契約の内容吟味

クラウドベンダとユーザー間の権利・義務は，両者間において締結されるべきクラウドサービス提供契約によって決せられる。自前サーバの場合には直接的な管理が可能であるのに対し，ユーザー企業とベンダは互いに独立した存在であるから，契約条項によって縛るほかない。したがって，サービス提供契約の内容を吟味しておくことが重要となる。もともとクラウドコンピューティングは，特定の有形的な成果物が納入されるような性格のものではなく，いわば形のないサービスを提供するものであるから，契約によって確定されるべき点が大部分である。

ところが，クラウドサービスでは大量の契約処理が必要となることから，クラウドベンダ側が事前に統一的な契約約款を用意しておくことが通常である。いわば個々のユーザーは，それを全体として受け入れるかどうかを決定する自由は有していても，個々の契約条項を協議によって決定する自由を有しないことが一般的であろう。クラウドサービス提供契約は有償双務契約であるから，クラウドベンダはクラウドサービスの提供に際し，提供契約に明文規定がなくとも，もともと理論的にはユーザーに対する善管注意義務を負っているものと考えるべきである。さらに，クラウドの前記特質を併せて考慮すると，それにはサービスを安全に管理すべき義務が含まれていることも当然であろう[3)]。

このような観点から，再委託の扱い，ベンダによる二次利用禁止，インシデント発生時の役割分担，責任の境界に関する線引きについての契約条項を事前に確認しておく必要がある。サービス仕様が提供契約によって定められていても，提供契約締結後に，クラウドベンダによる一方的変更が許されることになれば，ユーザー

が予期しなかった事態が発生しうる。ところが，実際には，一定の予告期間を付けることを条件に，サービスの仕様をクラウドベンダ側が一方的に変更しうる旨の規定が，提供契約に盛り込まれていることが多い。IT等の技術革新は急速であること，クラウドベンダ側が迅速にバージョンアップを講じることによってセキュリティや利便性向上が図られるとともに，それに関係するユーザー側の運用負担が軽減される点で，ユーザー側にも利点が存在すること，一般にクラウドが多数のユーザー向けの継続的なサービス提供であるから，いちいち全ユーザーから個別同意を得ることは非現実的であることなどを考えると，前記規定には一定の合理性が存在している。しかし，その場合，仕様変更によって，それまで正常に稼働していたアプリケーションが稼働しなくなるなどの異常が発生することになって，逆にセキュリティが損なわれるおそれがある（同様の事態はセキュリティパッチの適用によっても生じうる）。さらにはサービスレベルが一方的に切り下げられてしまう危険もある。そもそも全く自由に一方的変更が可能であるとすると，契約締結時に仕様を定めた意味が減殺される。そのため，仕様の一部については変更にユーザーの同意を要するものとしているケースもある。したがって，提供契約において，どのような範囲で仕様変更が許容されるのか，ユーザーとしては確認しておき，不都合な部分があることが判明した場合には，契約条項の変更が可能であれば，変更に向けて協議する必要がある。契約条項の事前確認に関連して，免責約款も吟味する必要がある。クラウドサービス利用契約の大半には，クラウドベンダ側に有利な免責約款を入れているからである。消費者契約法の適用はないが，こうした免責約款の有効性については争いがあるところであり，ユーザー企業側としても，事前確認しておくことが重要であろう[4)]。上記（ａ）（ボーダレス性）に関連して，準拠法及び合意裁判管轄条項についても事前確認が重要である。

10．ベンダに対する監査

ユーザーによるクラウドベンダに対する監査の困難性という問題がある。国外ベンダの場合には地理的問題がある上，内外を問わずベンダはセキュリティ保護の見地からデータセンターへの立入りを厳しく制限している場合が多い。そのため，ユーザー企業による監査に代わるべきものとして，クラウドサービスに求められるセキュリティ要求事項を明確化するISO/IEC 27017（クラウドセキュリティ認証）が提唱されてきた。

11．ベンダロックイン

ベンダロックイン（vender lock-in）という問題もある。より適切なクラウドベンダを発見して移行しようとしても，当該ベンダ特有のフォーマットの特殊性等が移行の障害になる。

クラウドの利点として，より条件が良い他のサービスに乗り換えることが容易であることが指摘されている。ところが，互換性に乏しい仕様とすることなどを手段に，自由な乗り換えを阻止しようとするベンダも少なくない。そのため，単に契約内容を形式的にチェックするだけでなく，データ形式，データの書き出しの可否や費用負担などの点で，乗り換えが可能か，容易かについても，事前調査が重要となる。

12．その他の問題

送信路上の脅威という問題もある。しかし，純然たる専用線接続は高コストであることから，通信経路を暗号化する仮想プライベートネットワーク（VPN：Virtual Private Network）が利用されることが多く，特に外国のクラウドベンダである場合には，バックボーンにインターネットが用いられている。したがって，送信

手順についても注意を要する。

接続回線の障害による可用性喪失のリスクもあり，それは越境の場合において拡大する。現に，東日本大震災の際には，我が国と国外を結ぶ海底ケーブルの大半が切断された。クラウドのメリットとして大規模災害に強いことは事実であるが，自前のシステムに比べて，こうしたリスクが生じることも認識しておかなければならない。同様にサーバ所在地国のカントリーリスクという問題もある。したがって，クラウドを導入しようとするユーザーとしては，クラウドサービスに委ねるべき業務領域と，委ねる場合に，どのようなサービスを選択すべきかについて事前に検討するため，当該クラウドベンダの信頼性，当該契約内容を個別に吟味しつつ，契約外の要因によって左右されることを認識する必要がある。

最大の課題は端末管理である。クラウドサービスの利用によってサーバ管理の負担が軽減されても，端末管理の重要性という点では，自前サーバかクラウドサーバかによって差異はないからである。重要性に鑑み，項を改めて解説する。

13．端末側の管理等

漏えい事件の大半は，端末機器側に属する原因によって発生している。クラウドサーバそれ自体のセキュリティが如何に強固に保たれていても，ユーザーの端末機器側についてセキュリティが保たれていなければ，漏えいの危険は解消しない。サーバへの正当なアクセス権限を有する内部者が，当該権限を濫用してサーバから端末機器側へ情報をダウンロードして流出させるという内部不正のようなケースの防止には役立たない。前掲事件②③及び⑤はネットを介した外部からの標的型メール攻撃による端末機器のウイルス感染に起因する漏えい事例であった。この点は，サーバが自前のものであるか，クラウドサーバであるかということと無関係の問題である。さらに，漏えい事故の根絶は不可能に近いので，事故発生時に対応可能な社内体制の整備等による被害の拡大防止の重要性についても付け加えておきたい。このような見地から，各企業ではシーサート（CSIRT：Computer Security Incident Response Team）活動が進められている[5)]。

14．おわりに

少子高齢化に悩む我が国の産業界にとって，IT等を新製品・サービス開発に用いることによって国際競争力の回復に努めることは急務といえよう。IoT（Internet of Things：モノのインターネット）、ビッグデータを用いたディープラーニングによるAI（Artificial Intelligence：人工知能）への対応が，その具体例である。

これらのケースにおいて，営業秘密保護がどのような役割を果たすことができるか，オーバーザトップと呼ばれる外国の巨大IT企業によるデータの独占を不当に強化することがないよう留意しつつ，今後の踏み込んだ検討作業が待たれるところである。

注　記

1）著者は現在，産業構造審議会知的財産部会の営業秘密の保護・活用に関する小委員会の座長を務めているが，本稿はそれと関係なく，純然たる私見であることをあらかじめお断りしておく。

2）但し，そのためにはグループ内において各種帳票類等のフォーマットや外字フォントを統一するなど，別途，必要となる点は少なくないことに留意すべきである。

3）東京地判平成13年９月28日別冊NBL79号16頁も，インターネット接続プロバイダが，自己の提供するレンタルサーバ内に保管していたユーザーのコンテンツを，誤って消失させたという事案で，「物の保管を依頼された者は，その依頼者に対し，保管対象物に関する注意義務として，それを損壊または消滅させないように注意すべき

義務を負う」が，「この理は，保管の対象が有体物ではなく電子情報から成るファイルである場合であっても……異ならない。」として，前記プロバイダの契約責任を認めた。本判決はクラウドそのものに関するケースではないが，クラウドの場合に異なった考え方を採用すべき理由はないはずである。

4) 参考事例として，前掲注３）東京地判平成13年９月28日では，約款上の責任制限規定に関する適用の可否も争点となったが，裁判所は約款を厳格解釈することによって，本件には適用されないとしており，必ずしも責任減免条項が適用されるとは限らないことが示されている。

5) CSIRTは，コンピュータセキュリティにかかるインシデントに対処するための組織の総称である。インシデント関連情報，脆弱性情報，攻撃予兆情報を常に収集，分析し，対応方針や手順の策定などの活動をする。これを推進するものとして日本シーサート協議会が設けられており，我が国のメガバンクその他の著名大企業の多くが名前を連ね，新たなサイバー攻撃の脅威や対策について情報交換等を行っている。

（原稿受領日　2017年１月13日）