1 クラウドコンピューティングのリスクとガバナンスに関する調査・研究について

原田要之助 情報セキュリティ大学院大学

本稿は，クラウドコンピューティングに関するリスクとガバナンスの調査と研究について解説した．この解説では，クラウドコンピューティングの定義についてのコンセンサスがなされ，ビジネスが展開されてきた中における，さまざまなリスクやこれをどのように管理，運営していくかについて述べている．特に，海外の文献から紹介する．

クラウドの定義について

クラウドの定義と特徴については，以下の NIST（National Institute of Standards and Technology）の定義[1]をベースにしているので，この定義について紹介する．

(1) クラウドの特徴[1]

NIST ではクラウドについて，以下のような特徴を持つサービスとして定義している．

① On Demand and Self Service：ユーザ企業は，クラウドサービス事業者（以下では，CSP という）のコンピュータ能力（サーバの処理能力やストレージ容量など）をオンデマンドで利用できること．

② Broad Network Access：ネットワーク経由で CSP のコンピュータ能力（所在地は問わない）をノートパソコン，携帯電話，PDA などで利用できること．

③ Resource Pooling：CSP は，複数のユーザ企業に対して，要求があれば，コンピュータ能力を提供する．ただし，ユーザ企業は，CSP のコンピュータ能力を物理的にコントロールすることはできない．また，一般的には，地理的にどこから提供されているのかを特定できない（付加的に，CSP がコンピュータ能力を提供している地理情報を開示するサービスもある）．

④ Rapid Elasticity：CSP は，コンピュータ能力を，迅速に，かつ柔軟に，自動的に提供する．そのため，ユーザ企業からは，コンピュータ能力は無限にある（能力的な制限がない）ように見え，また，ニーズが発生した時点で，いつでも必要なコンピュータ能力を購入できる．

⑤ Measured Service：CSP は，ユーザ企業が利用しているコンピュータ能力の利用量を計測して，料金請求を行ったり，CSP のサービスを最適化する．

(2) クラウドのサービス提供形態による分類[1]

前項で述べた特性を実現するクラウドサービスは以下の 3 つの形態に分類されている．この分類には，さまざまな派生があるが，NIST による分類を紹介する．

① SaaS（Software as a Service）：CSP が，サービス提供にあたって，物理的なサーバやストレージだけでなく，インストールされる OS やデータベース，ミドルウェアに加え，ユーザ企業が最終的に利用するアプリケーションまでをサービスとして提供する形態を言う．

② PaaS（Platform as a Service）：SaaS が提供する形態からアプリケーションを除いた形態を言う．従来，ユーザ企業がアプリケーションを利用するために開発する場合は，サーバなどの物理的な機器を調達して，OS やデータベース，必要な開発環境などをインストールして，専門家が開発を行っていた．PaaS を利用する場合，機器の調達が不要になり，OS やデータベース，開発環境の準備

も不要になる．CSP の提供するコンピュータ能力に，ネットワークの経由でアクセスして，利用する．ただし，OS やデータベースのカスタマイズについては CSP の提供条件による．

③ IaaS（Infrastructure as a Service）：HaaS（Hardware as a Service）とも呼ばれる．CSP は，ユーザ企業にサーバやストレージのハードウェアを（意識できる形で）提供する．ユーザ企業は，自ら OS やデータベースなどを選択し，その上でアプリケーションを開発・導入する．ユーザ企業自らサーバを購入して設定を行ってから開発するという一連の手間をかけないで済む．実際にハードウェアを購入して，OS やデータベースを設定する必要がないため，アプリケーションの開発に専念できる．

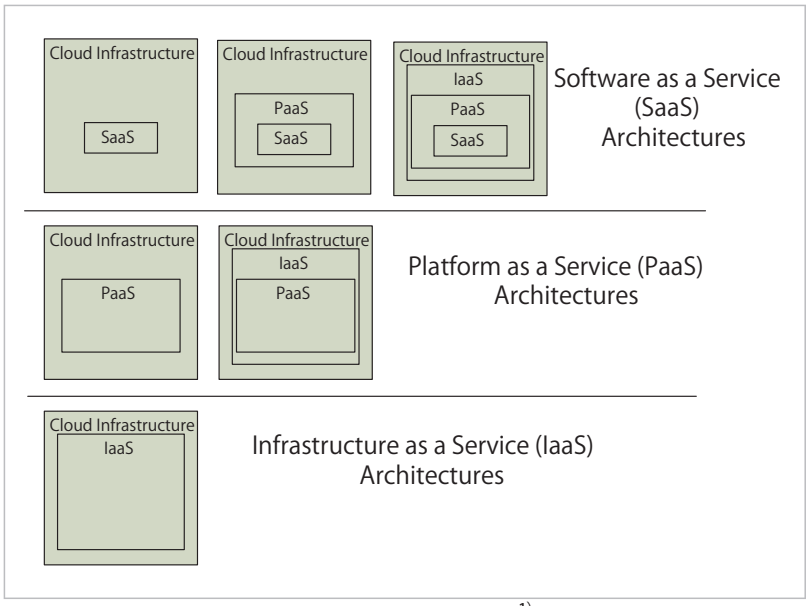

図 -1　NIST によるクラウドのサービス提供形態の分類 [1)]

以上で述べたのは，一般論であり，SaaS の場合，必ずしも陽に PaaS や IaaS が介在しない場合もある．これは，ユーザ企業にとっては，アプリケーションサービスが提供されればよいのであり，OS やデータベースなどのプラットフォームについてはどうでもよいことも多い．NIST では，図 -1 のように整理している [1)]．なお，NIST の図 -1 のモデルでは，SaaS の提供形態として，IaaS と PaaS を利用する形態，PaaS を利用して提供する形態，SaaS だけを提供する形態が（分類額的には）存在する．たとえば，ネットワークゲームを提供する CSP は特殊な環境を（開示しない場合も含めて）利用する．

クラウドのリスクについて

-- クラウドのリスクとは --

クラウドのリスクについて，最初に網羅的に整理したのは，Gartner の調査レポート [4)] である．このレポートでは，クラウドのリスクについて，次の 7 つの項目を挙げて解説している．特に，ビジネスモデルの観点から法的なリスクについてジャーナリスティックに述べているのが新しい．

① 特権ユーザのアクセスに対する管理が不明確になりがちである．

ユーザ企業は自社で機密情報を扱う場合，情報を取り扱う特権者や管理者を制限し，アクセスを監視して，不正が起きないよう管理し，事件が起きた場合のために犯人を追跡できるようにしている．したがって，ユーザ企業は，CSP に機密情報を処理する場合，同様のコントロールを CSP に要請する．しかし，CSP は，多数のユーザ企業の情報を一括で管理しているため，ユーザ企業は，CSP が希望するレベルのコントロール（アクセス制御など）を実施できないことを懸念する．

②コンプライアンス違反が起きたり外部監査が実施されないことがある．

CSP のビジネスモデルは，多数のユーザ企業にサービスを提供することであり，個々のユーザ企業が要求するようなコンプライアンスに対応できないこともある．たとえば，ユーザ企業が個人情報をクラウドに蓄積し，データベースとして参照するような場合，クラウド側が個人情報として

取り扱わない場合が想定される．

また，ユーザ企業は自社の情報が安全に取り扱われているか知るためにCSPに外部監査の実施を要請することがある．CSPによっては，個々のユーザ企業から，個別に監査を要請されると業務に支障が出るとして拒否するかもしれない．ユーザ企業は，CSPとの契約に，監査実施を陽に謳わない限り，監査報告を要請するのは難しい．

③データの(物理的な)保管や処理するサーバが他国の場合，適用される法令が異なるため，情報の管理や漏えい事故などの場合に不安がある．

CSPは，ユーザ企業から預かったデータが物理的にどこの国で保管され，処理されているかについて開示しない場合が多い．すなわち，ユーザ企業の情報が外国のサーバに保管されたり，処理されることもある．このような場合には，その国の法令が適用されることになり，事件の際には，自社の機密情報や顧客の情報が裁判のために開示されたり，証拠として押収されて，利用できなくなる可能性もある．さらに，個人情報の保護法や電子情報の証拠保全に関する法令は地域や国によって異なるため，自国では想定できない問題が発生する可能性がある．

④CSPが扱うデータがユーザ企業ごとに隔離されていないため，自社の機密情報が他社に漏れてしまう．

CSPでは，多数のユーザ企業がデータベースや処理システムを共有するビジネスモデルであるため，Gartnerは，「どのような方法で，保管しているデータを隔離しているのかを調べておく必要がある」[4]と述べている．CSPを利用する場合には，複数のユーザ企業を隔離する場合の脆弱性など，既存技術の不十分な点に注意すべきであろう．

⑤CSPは，事件や事故の有無や復旧時間などについて通知しない場合がある．ユーザ企業は利用するサービスが故障するなどの場合に備えた対策が必要である．

⑥裁判所命令などへの対応のために，必要な証拠が開示されるか分からない．

CSPは多数のユーザ企業の情報の保管や処理を並行で実施しており，個別のユーザ企業の処理の追跡やデータの変更履歴などへの調査や証拠開示が難しいことがある．サーバが外国に置かれている場合には，証拠保全が難しいこともある．

⑦CSPの事業継続

CSPは，災害時にユーザ企業のデータのバックアップやハードウェア障害への対応などについて開示されない場合もある．また，開示されていても，約束通りに事業継続が実施されるかの保証はない．さらに，CSPは，ビジネスであり，倒産やM&Aで所有者が変更になることもある．

Gartnerは，以上の7点を指摘したことから，CSPに対するリスクに対して注意が向けられるようになった．

--ENISAによるクラウドのリスク[3),9)] --

ENISA（European Network and Information Security Agency）[3]は，Gartnerの調査を受けて，クラウドのリスクをさらに深く分析している．以下では，ENISAのリスク分析について紹介する．

リスクの分析では，中小企業に対してアンケート調査（**付録1**参照）を行って，その結果をもとに，EUの太陽光発電関係の中小製造業（**付録2**参照）とオンラインサービス業（eHealth）のモデルで評価している．これらのモデルを対象に，詳細リスク分析(ISO/IEC 27005:2008)を実施している．最初に，リスク項目にかかわる情報資産を明確にする．次に，情報資産ごとに，関係する脆弱性を紐付ける．情報資産に想定される脆弱性がリスクとなる頻度および影響の大きさを評価して，総合的なリスクのレベル(0～9)を計算する．レベルは，0～2を低，3～5を中，6～9を高としている．

(1)リスクの分類

ENISAでは，クラウドのリスクを網羅的に調査して4つ(共通を区別した場合)に分類している．組織的なリスク，技術的なリスク，法的なリスク，共

通のリスク（必ずしもクラウドに限らない ICT リスクを共通のリスクとしている）．これを以下に示す．

①組織的なリスク（7 項目）☆1

ロックイン，ガバナンスの喪失，コンプライアンス対応，共同サービスの提供による企業価値の低下，CSP のサービス停止および障害，クラウド・プロバイダの買収，サプライ・チェーンのトラブル

②技術的なリスク（13 項目）☆1

リソースの問題（不足または過剰），独立性（サービスの共有からくる Public Cloud の問題点），内部者の悪意，管理者の特権濫用，管理者機能の悪用，データの妨害，データ漏えい，データの不確実な消去，DDoS への対応，EDOS への対応，暗号鍵の管理（紛失），悪意あるスキャン，サービス提供の欠陥，ユーザ企業と CSP でのセキュリティ対策の違いからくる問題

③法的なリスク（4 項目）☆1

法令による命令や証拠保全，裁判管轄の違いによるリスク，データ保護にかかわるリスク，ソフトウェアライセンスにかかわるリスク

④共通のリスク（11 項目）☆1

ネットワークのダウン，ネットワーク管理，ネットワークトラフィックの経路変更，権限奪取（root 権限を奪われる），ソーシャルエンジニアリング攻撃，運用ログの滅失または漏えい，セキュリティ・ログの滅失または漏えい，バックアップの毀損・盗難，構内への無権限アクセス，機器の盗難，災害

(2) 情報資産について

ENISA では，リスク分析の対象とする情報資産を，無形物と有形物に分けて，23 項目を列挙している．これを**表 -1** に示す．表 -1 では，情報資産のオーナー（管理責任者）が CSP のユーザ企業なのか CSP なのかに応じて，分類している（表 -1 中の○が相当する）．情報資産が両者にかかわる場合には，両方で評価する（表 -1 中のユーザ企業と CSP に○がついているもの，たとえば，A5 など）．

なお，表 -1 は，網羅的に作成されており，ユーザ企業は，自社の情報資産にあてはめて利用する．表 -1 を利用する場合，対象とする情報資産が自社に該当する場合には，その情報資産の重要度を決めることになる．

(3) リスクの分析

ENISA のリスク分析では，（1）の 35 項目のリスク候補について，**表 -2** のフォームを利用して評価することを勧めている．以下にこのプロセスを示す．

Ⅰ．（1）の 23 項目の中から分析する項目を選び①に記入する．

Ⅱ．①のリスクに関係する情報資産を表 -1 から選び，②に記入する．

Ⅲ．情報資産②に対応する脆弱性を③に列挙する（**付録 3** 参照）．

Ⅳ．②の情報資産と対応する③の脆弱性について，それぞれ発生頻度と重要度をもとに，④に発生頻度を記入する（高，中，低の 3 段階），⑤に影響度（高，中，低の 3 段階）を記入する．

Ⅴ．Ⅳの各項目の影響度を求めて，表 -1 をもとにして評価（最高，高，中，低，最低）して，その総合的な影響度を⑥に記入する．また，Ⅳと同様に，影響度の変化について⑦に記入する．

Ⅵ．④と⑥を評価して，最終的にリスクを評価する（高，中，低の 3 段階）．

なお，項目によって発生頻度を評価できないものについては，NA（対応なし）として，影響度のみによって評価する．

ENISA では，表 -2 のテンプレートを用いて，23 すべてのリスクについて分析結果を示している．ここでは，ロックイン（ユーザ企業が CSP のサービスに囲い込まれて，他の CSP のサービスに移れない状況のことを言う）についての評価例を**表 -3** に示す．

(4) リスク分析の結果

①組織的なリスク

組織的なリスクについての分析結果を**表 -4** に

☆1 個々のリスクの内容については，表 -4 ～ 7 の表中に示す．

対象とする情報資産（有形，無形）	クラウドユーザ企業	CSP	資産の重要度☆2
A1. コーポレートレピュテーション☆3（企業のブランドなど）	○		最高
A2. 顧客の信頼（顧客の評判）	○		最高
A3. 従業員の忠誠度と経験能力	○		高
A4. 知的財産	○		高
A5. 機微な個人情報（病歴や宗教など漏れると重大な不利益となる情報）	○	○	最高
A6. 一般的な個人情報（氏名，住所，性別などの個人情報）	○	○	中
A7. 企業の重要情報（企業が重要と識別している情報）	○	○	高
A8. 従業員情報（従業員の業績や人事評価に関する情報）	○		高
A9. 実時間サービスの提供状況の情報（リアルタイムで提供しているサービスの負荷や品質に関する情報）	○	○	最高
A10. サービスの提供状況の情報（サービス全体の品質に関する情報）	○	○	中
A11. アクセス制御，認証，権限付与に関する情報（root 権限や管理者に対するアクセス権限の情報）	○	○	高
A12. システムへのアクセスに関する認証情報や証明書（CSP の従業員に対するアクセス権限を付与するときに必要な情報）	○		最高
A13. ユーザ企業のディレクトリ情報（ファイルやデータの管理情報）	○		高
A14. クラウドサービスを受けるための管理インタフェース（ユーザ企業が CSP サービスを利用するときの Web などのインタフェース）	○	○	最高
A15. 管理用 API のインタフェース（CSP との API）	○	○	中
A16. CSP のネットワーク接続（CSP 間の接続および CSP 外部の接続を含む）	○	○	高
A17. 物理的ハードウェア	○	○	低／中☆4
A18. 施設情報（クラウドのサービスを提供している施設に関するロケーションなどの物理的な情報）	○	○	高
A19. CSP のアプリケーション（CSP が利用しているアプリケーションソフトウェアのソースコードなど）	○	○	高
A20. 取得した ISO，PCI DSS などの認証	○	○	高
A21. オペレーションログ情報（クラウドが運用やユーザ企業のログ情報．これらのログは，ビジネスの見直しや監査のために利用される）	○	○	中
A22. セキュリティログ情報（情報漏えいや事件のときの証拠保全に必要となるセキュリティに関するログ情報）	○	○	中
A23. バックアップやアーカイブデータ	○	○	中

表 -1　情報資産の分類，重要度と対象者　ENISA[3] より

リスク項目	①	
発生頻度	④	現状との比較：⑤
影響度	⑥	現状との比較：⑦
脆弱性の項目	③	
影響する情報資産	②	
リスクの評価値	⑨	

表 -2　リスク分析のテンプレート　ENISA[3] より

リスク項目	ロックイン	
発生頻度	H（高）	現状との比較：高い
影響度	M（中）	現状との比較：同等
脆弱性の項目	V13, V46, V47, V31	
影響する情報資産	A1, A5, A6, A7, A9, A10	
リスクの評価値	H（高）	

表 -3　ENISA によるリスク分析の例（ロックインの場合）ENISA[3] より

示す．

組織的なリスクとして扱っている項目では，「ロックイン」（表 -4 中の R1）と「ガバナンスの喪失」（表 -4 中の R2），「コンプライアンス対応」（表 -4 の R3）をリスクが高としている．また，「サービスを共有するためコーポレートレピュテーションを低下させる」リスクは，企業の競争優位を喪失するというリスクであり，「クラウドサービスの

☆2 重要度は，Very Low（最低），Low（低），Medium（中），High（高），Very High（最高）で評価している．
☆3 原文では，Company Reputation となっているがここでは，コーポレートレピュテーションとしている．
☆4 低（どの程度失うかによる），中（保護されていない状態で倒産された場合は深刻となることもある．

組織的なリスク		頻度	影響度	リスク
R1	ロックイン（ユーザが CSP のサービスに囲い込まれ，自由に CSP を変更できないリスク）	高	中	高
R2	ガバナンスの喪失（ユーザ企業が CSP に依存するため自分でコントロールできなくなるリスク）	最高	最高	高
R3	コンプライアンス対応（CSP のサービス条件が法令や認証などへの対応ができないため移行できない）	最高	高	高
R4	サービスを共用するためコーポレートレピュテーションを低下させる（同じ CSP のサービスを利用する他のユーザ企業の影響でリソースが使えなくなる）	低	高	中
R5	クラウドサービスのサービス停止および障害によるサービス中断	NA	最高	中
R6	CSP の買収（CSP が買収されて，拘束されない条件が変更されて，セキュリティ条件に適合しなくなる）	NA	中	中
R7	サプライ・チェーンのトラブル（CSP が依存する他の CSP のトラブルで，サービスが中断する）	低	中	低

表 -4　ENISA によるクラウドの組織的なリスク [3)]

技術的なリスク		頻度	影響度	リスク
R8	リソース過不足の問題（プロセッサやストレージ容量が不足したり，過剰な場合のリスク）	中 / 低	低 / 中	中
R9	サービスを共有するため，他のユーザ企業の影響を受けるリスク（プライベートクラウドの問題点）	低 / 中	最高	高
R10	内部者の悪意，管理者の特権濫用のリスク（CSP の内部者や管理者が特権濫用して，ユーザ企業の情報にアクセスしたり漏えいするリスク）	中	最高	高
R11	管理者機能の悪用によるリスク（管理者機能を悪用してユーザ企業のデータに不正アクセスするリスク）	中	最高	中
R12	データ通信経路途中におけるリスク（データ転送が増え，盗聴，なりすまし，中間者攻撃のリスクが増える）	中	高	中
R13	データ漏えい（ユーザ企業が CSP にデータ転送時にデータが漏えいする）	中	高	中
R14	CSP のデータ消去漏れのリスク（CSP がユーザ企業のデータを確実に消去しない場合のリスク）	中	最高	中
R15	DDoS のリスク	中 / 低	高 / 最高	中
R16	EDoS のリスク（CSP のリソースを消費することで料金請求されるなど）	低	高	中
R17	暗号鍵の喪失のリスク（CSP が管理ミスでユーザ企業の暗号鍵を紛失する）	低	高	中
R18	（ハッキングを目的とした第三者による）悪意ある CSP へのスキャンによるリスク	中	中	中
R19	ハイパーバイザなどの脆弱性（CSP のリソースの隔離ができないなど）	低	最高	中
R20	顧客とクラウドでのセキュリティ対策の違いからくるリスク	低	中	低

表 -5　ENISA によるクラウドの技術的なリスク [3)]

サービス停止および障害によるサービス中断」によって自社のサービスが停止して，企業への信頼の低下を招くことであり，リスクは中と評価している．一方，「CSP の買収」のリスクについては，リスクが中程度と分析している．なお，「サプライ・チェーンのトラブル」については，重要度は中と低く評価している．

②技術的なリスク

技術的なリスクを，表 -5 に示す．

技術的なリスクでは，「サービスを共有するため，他のユーザ企業の影響を受けるリスク」（表 -5 中 R9）と「内部者の悪意，管理者の特権濫用のリスク」（表 -5 中 R10）を高としている．その他の「リソース過不足の問題」（表 -5 中 R8），「管理者機能の悪用によるリスク」（表 -5 中 R11），「データ通信経路途中におけるリスク」（表 -5 中 R12），「データ漏えい」（表 -5 中 R13），「CSP のデータの消去漏れのリスク」（表 -5 中 R14），「DDoS のリスク」

法的なリスク		頻度	影響度	リスク
R21	召喚状や証拠保全のリスク	高	高	高
R22	司法権の違いによるリスク（企業の情報が海外のサーバに保存されているとその国の法令が適用される）	最高	高	高
R23	データ保護にかかわるリスク（個人情報保護法が地域・国によって異なるためのリスク）	高	高	高
R24	ライセンスにかかわるリスク（クラウドがサービス提供に利用するソフトウェアのライセンスについての権利関係によるリスク）	中	中	中

表 -6　ENISA によるクラウドの法的なリスク [3)]

（表 -5 中 R15），「EDoS のリスク」（表 -5 中 R16），「暗号鍵の喪失のリスク」（表 -5 中 R17），「悪意ある CSP へのスキャンによるリスク」（表 -5 中 R18），「ハイパーバイザなどの脆弱性」（表 -5 中 R19），は中程度のリスクと分析している．一方，「顧客とクラウドでのセキュリティ対策の違いからくるリスク」（表 -5 中 R20）はリスクを低と評価している．なお，Thomas [5)] は，技術的なリスクの中で，Availability of Service（サービスの可用性）が抜けていると述べている．この項目は，共通のリスク（表 -7）の R25 に含まれると解釈することもできるが，サーバなどのシステムを含めた総合的な可用性と考えられるので，追加すべきであろう．

なお，技術的なリスクの中で DDoS（Distribute Denial of Service）と EDoS（Economic Denial of Service）に関する問題点は，クラウドに特有の問題としてクローズアップされている．DDoS の場合，リソースを再配置できるため，影響を軽減することができる．一方，EDoS は，CSP のあるユーザ企業が DDoS 攻撃にさらされた場合，負荷が集中するため，異常と区別することができない．そのため，CSP からは，DDoS によるアクセスをも含めて料金を請求される．これらの問題は，リソースが共有されているために起きる．これらの現象については，Meiko Jensen ら [6)] が細かい分析をしている．

また，Thomas [5)] は，CSP のデータの中継に伴うリスクを取り上げており，暗号化が望ましいとしている．梶本と原田 [8)] は，悪意あるユーザ企業によって，CSP がデータロンダリングに使われるリスクを述べている．これは，不正な手段で入手した個人情報やコンテンツを複数の CSP のサービスを中継することで，入手経路を隠ぺいして正当なコンテンツに見せかけることをいう．マネーロンダリングは，複数の銀行間で資金を送受することで，犯罪にかかわるお金の入手経路を隠すものであり，厳しく規制されている．データロンダリングについても，同様な規制が必要と考えられる．

③法的なリスク

ENISA による法的なリスクの分析結果を，**表 -6** に示す．

ENISA では，法的なリスクを 4 つに分けて細かく述べている．特に，裁判所からの召喚状や証拠保全についてリスクが高としている（これは，米国の e-discovery 法を念頭に述べている．裁判所からの召喚状により，PC やサーバに保存したデータを提出する必要がある．たとえば，企業では PC のイメージをバックアップするなど対策を実施している）．また，企業が犯罪に関係したとき，裁判では訴追された国や地域での法律を適用することになる．たとえば，クラウドのデータが EU のサーバに蓄積されている場合，日本では有罪にならない Child Porno の保有は EU では犯罪となる．また，個人情報データが EU に存在すれば，EU のデータ保護法（EU の個人情報保護法）の適用を受ける．個人情報の場合，EU から域外に送信する場合には，データ保護法では，域外に個人情報を送付する場合，送信先を厳しく制限している．法的なリスクへの対応について**付録 4** にまとめる．

共通事項		頻度	影響度	リスク
R25	ネットワークがダウンしてサービス提供がされないリスク	低	最高	中
R26	ネットワークが運用のトラブルで正常に利用できないリスク（例，輻輳／誤接続／不適切利用）	中	最高	高
R27	ネットワークの経路情報が変更されて接続できなくなるリスク	低	高	中
R28	権限奪取（root 権限を奪われる）されて，不正に利用されたり，内容を見られてしまうリスク	低	高	中
R29	ソーシャルエンジニアリング攻撃を受けて，重要な情報を奪取されるなどのリスク	中	高	中
R30	企業の運用ログを滅失したりまたは漏えいさせるリスク	低	高	低
R31	セキュリティログの滅失または漏えいのリスク	低	中	低
R32	バックアップを失敗するリスク，および盗難されるリスク	低	高	中
R33	第三者が構内の設備にアクセスできてしまうリスク（装置やその他の施設への物理的アクセスを含む）	最低	高	低
R34	機器の盗難のリスク	最低	高	低
R35	災害のリスク	最低	高	低

表 -7　ENISA によるクラウドに共通的なリスク [3)]

④共通のリスク

共通のリスクを，表 -7 に示す．共通のリスクはクラウドではない IT サービスにも共通するリスク項目である．

表 -7 の「災害のリスク」（表 -7 中の R35）は，頻度が最低であり，影響度は高であるが，最終的なリスクとしては低という判断となっている．これは，「機器の盗難のリスク」と同程度と評価しており，ヨーロッパという条件からの結論と考えられる☆5．地震や自然災害が多いアジアや米国の西海岸では，この評価をそのまま利用することはできないであろう．また，Gartner がとりあげた 7 項目と共通する権限奪取（表 -7 中 R28）については，中と判定している．一方，ENISA が高としたネットワークの運用のトラブル（表 -7 中 R26）については Garter は触れていない．米欧で見解が異なっている．

--ENISA の総合リスク評価 --

ENISA では，R1 ～ R35 のリスクについて発生頻度と影響度から，リスクを以下の①～④を総合評価して，図 -2 にまとめている [3)]．

図 -2 の結果からは，総合リスクの高いものとして，R2：ガバナンスの喪失，R3：コンプライアンス対応，R22：司法権の違いによるリスクが，評価点 7 で高としている．次に，R9：サービスを共有するため，他のユーザ企業の影響を受けるリスク，R10：内部者の悪意，管理者の特権濫用のリスク，R11：管理者機能の悪用によるリスク，R14：CSP のデータ消去漏れのリスク，R26：ネットワークが運用のトラブルで正常に利用できないリスクの 5 項目が，評価点 6 で，高としている．これ以外の項目は，総合評価 5 から 3 のリスクが中程度と評価している．なお，この分析は，EU の観点で評価したものであり，同じ分析を日本で実施すれば，違った評価結果となると考えられる．

クラウドのガバナンスについて

ENISA のリスク分析からは，「ガバナンスの喪失」が最もリスクが高い項目の 1 つとして挙げられており，ガバナンスはクラウドの利用者，CSP の双方にとって重要なテーマである．なお，情報セキュリティ分野におけるガバナンスの研究は比較的新しい．また，大木・原田ら [7)] により，経済産業省の情報セキュリティガバナンス研究会の報告書をベー

☆5　ヨーロッパでは，2010 年 4 月の火山爆発の影響で航空が 1 週間ほどストップして企業の IT に多大な影響がでており，これをうけて ENISA の担当者は，頻度は中にすべきで，全体のリスクも中になると非公式に述べている．

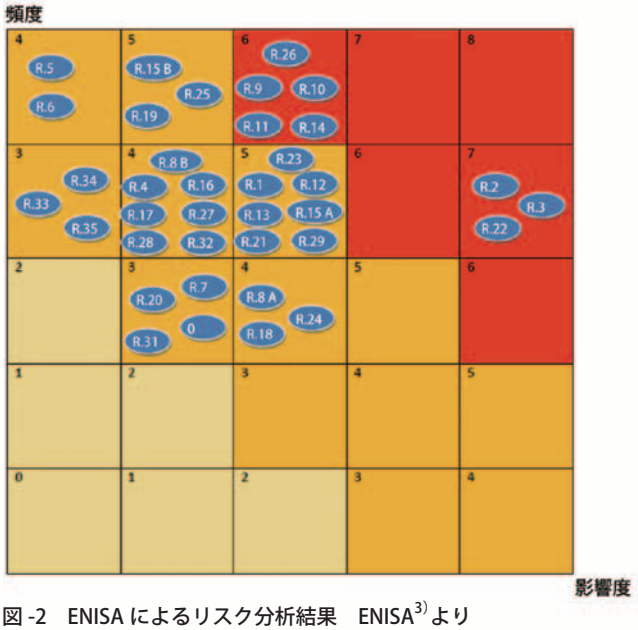

図 -2　ENISA によるリスク分析結果　ENISA[3] より

スに，ガバナンスモデルが検討されている．このモデルは，ISO の情報セキュリティガバナンス（ISO 27014 CD）の標準モデルともなっている．

クラウドのガバナンスについては，CSA[2] が，以下の項目からの分析を行っている．

①ガバナンスと ERM（Governance and Enterprise Risk Management）
②法的な課題と e-discovery 法（Legal and Electronic Discovery）
③コンプライアンスと監査（Compliance and Audit）
④情報のライフサイクル（Information Lifecycle Management）
⑤情報の移転可能性と相互運用性（Portability and Interoperability）

これらの項目について，クラウドの利用企業や CSP がどのように情報を管理し，サービスを提供するか，さらには，サービスについての法的な問題や監査について触れている．すなわち，CSA は情報セキュリティのガバナンスとして企業として必要なすべての項目を網羅している．しかし，文献 7）のモデルとは整合していない．今後，モデルについて整合していくことが望まれる．

まとめ

本稿では，クラウドの最近のリスクに関する調査・研究について述べた．クラウドについては，日本においても多くの事業者がサービスを提供しており，ここで述べたリスクやガバナンスについて，すでに考慮して，それなりに対応しているものもあり，ここで述べたことがすべて当てはまらないケースもあると考えられる．

謝辞　本稿をまとめるにあたって，貴重なアドバイスをいただいた工学院大学大木栄次郎教授，ISACA 関係者の皆さまに感謝いたします．

参考文献

1）Mell, P. and Grance, T : The NIST Definition of Cloud Computing, National Institute of Standards and Technology (2009).
2）Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1(Feb. 2010).
3）Catteddu, D. and Hogbeu, G.（監修）: Benefits, Risks and Recommendations for Information Security, ENISA (Nov. 2009).
4）Heiser, J. and Nicolett, M. : Assessing the Security Risks of Cloud Computing, Gartner Inc. (June 2, 2008), or Gartner, B. J. : Seven Cloud-computing Security Risks, InfoWorld（http://www.infoworld.com/d/security-central/ gartner-seven-cloudcomputing-security-risks-853）(July 2, 2008).
5）Betcher, Thomas J. : Cloud Computing Key IT-Related Risks and Mitigation Strategies for Consideration by IT Security Practitioners, University of Oregon Applied Information Management Program, (Feb. 2010).
6）Jensen, M., Schwenk, J., Gruschka, N. and Lo Iacono, L. L. : On Technical Security Issues in Cloud Computing, 2009 IEEE International Conference on Cloud Computing, pp.109-116.
7）Ohki, E., Harada, Y. et al. : Information Security Governance Framework, Proceedings of the First ACM Workshop on Information Security Governance, pp.1-6（Nov. 2009）.
8）Kajimoto, M. and Harada, Y. : SecureCloud 2010, Standardization for Cloud, SecurityBarcelona (Mar. 2010).
9）An SME Perspective on Cloud Computing Survey, ENISA (Nov. 2009).

（平成 22 年 9 月 6 日受付）

原田要之助（正会員）yo-harada@iisec.ac.jp

1979 年京都大学大学院工学部数理工学専攻を修了，電信電話公社（現 NTT）入社．1999 年情報通信総合研究所主席研究員．2010 年より情報セキュリティ大学院大学教授，大阪大学大学院工学研究科特任教授．

付録 1　ENISA による中小企業向けのクラウドに関する実態調査 [9)]

ENISA は，中小企業を対象に，以下に示すクラウドに関する 7 項目と企業規模，ロケーションの 2 項目を合わせた 9 項目の調査を実施している．調査では，74 社を対象に 2009 年 11 月 1 日に実施されている．

(1) クラウドコンピューティングを利用する場合の利用目的
(2) 自社に最も適しているクラウドのモデル（プライベート，パブリック，その他）
(3) 利用する可能性の高いクラウドサービスの種類（SaaS，PaaS，IaaS，その他）
(4) 複数のプロバイダに外部委託する意向の有無
(5) クラウドに災害復旧や BCM を依存するかどうか
(6) クラウドを利用するアプリケーションは何か
(7) クラウドを利用するにあたっての懸念事項

付録 2　中小企業向けのクラウドのリスク分析のための企業モデル

ENISA では，リスク分析をモデル企業を対象に実施している．なお，モデル企業を想定するにあたって，付録 1 の調査をもとに，以下のシナリオを作成している．

Clean Future work 社は，1999 年にドイツで，太陽光発電関連の製造と販売を始めた中小企業で，従業員数は 93 名（ドイツ 50 名，ポーランド 34 名，スペイン 5 名，イタリア 4 名）．主要な工場はドイツにあり，年率 20% で急速に成長している．2003 年にスペイン，2004 年にイタリアに事業所を開いた．2005 年には，反射防止ソーラーガラスの製造をポーランドに移し，2006 年に稼働させた．現在，米国への進出を検討している．取引先は，太陽光関係の 10 ～ 30 社ある．

Clean Future work 社は，競争の激化と 2008 ～ 2009 年の経済危機に対応するため，コスト削減と生産性向上を計画した．特に，IT サービスは改善余地が大きいと判断して，IT の変革を考えている．

付録 3　ENISA が分析した脆弱性評価項目

ENISA の調査では，リスクを分析するにあたって，情報資産に対する脆弱性をまとめた．付表 1 に示す．

付録 4　クラウドコンピューティングにかかる法的な課題のまとめ

① CSP との契約
• 契約をどこの国の法律で実施するのか．
• CSP が，国境をまたがってサービスしている場合，どこの国の法律で，紛争処理を行うか（国際的な仲裁機関が取り扱えるか）．
② 個人情報の保管
• どこの国の法律が適用となるのか：個人情報漏えいについて厳しい国であればよいが，未整備の国の場合，権利保護がなされない可能性がある．
• 個人情報の取り扱いに複数の異なる国の法制度が関係するときに，どの法律を適用するかを契約で決めておく．物理的ロケーションで法律が課せられる場合が多い．
• CSP の情報漏えいの際に，直接被害を受ける最終顧客をどのように保護するか，被害についての賠償責任をどこまで負うかを契約で決めておく必要がある．
③ 個人情報の移送
国境をまたがって個人情報を移送する場合，制限がある国，地域がある．この問題については，明確な対策はない．
④ CSP が倒産したり，M&A に巻き込まれたりしたときの最終利用者の保護をどのように担保するか決めておく必要がある．
⑤ 預託した個人情報が CSP の資産として扱われないように制限する仕組みが必要．
⑥ 捜査の観点からのエスクロー暗号の利用
CSP が犯罪に関係しているような場合，事業者自体が捜査対象となる．このような場合，扱っているデータが差し押さえされることが考えられる．国際的な犯罪が国境をまたぐ場合の CSP への捜査について国際的な取り決めは現在ない．通常の犯罪のように，犯人引き渡しなどによる手続きが必要となる．特に，CSP が扱っているデータを暗号化しその暗号鍵を秘匿した場合，捜査が不可能となる．このような場合に備えて，CSP が利用者や自身の運用ログなどについては，エスクロー型の暗号利用を義務づけることも必要になるかもしれない．
⑦ クラウドのユーザ企業のデータ保全
CSP の利用企業が裁判所からの召喚状で，扱うデータの消去の禁止や保全，提出を求められる可能性がある（米国のアメリカ連邦民事訴訟規則や e-Discovery（電子情報開示）法など）．特に，企業が脱税や破棄物違反などの違法行為をしている場合，ビジネスの全体を捕捉する必要があるため，取引のトランザクションを証拠として押収することになる．被疑企業が，これらのデータについて CSP を利用している場合には，CSP に協力を申し出て，当該企業のデータ（もしくは，そのコピー）を保全することが必要となる．このような場合に，当該企業の関連する情報が，海外の CSP に保管されている場合，法的な権限が及ばないため，当局が差し押さえられないかもしれない．悪質な場合には，この時間を利用して，証拠となるデータを消去するかもしれない．どのように，データを保全し，証拠とするかが今後，重要な課題となっている．また，クラウドに保存されたデータの元本性が保証されないこともあり，証拠とできるかの疑問もある（原本である証明．改ざんしたものでないことの証明が難しい）．
今後，クラウドの提供するサービスが，現在の法的な制約をついた形で悪徳企業や反社会的組織の取引に用いられないような国際的な枠組みを作る必要がある．

項目	内容
V1	CSP の認証，権限付与，課金処理にかかわる問題点
V2	ユーザ企業の必要に応じたサービスを提供する CSP のプロビジョニングが適切に実施されない問題点
V3	ユーザ企業がプロビジョニングを取り消すなどの場合に時間遅れが生じるなどの問題点
V4	CSP のメンテナンス用に遠隔から利用するインタフェースの問題点
V5	CSP のハイパーバイザー（物理的なリソースや VM を管理するレイヤ）の脆弱性による問題点
V6	CSP のハードウェアリソースでの隔離が不足している問題点
V7	顧客間のデータの隔離が不足している問題点
V8	CSP が通信に利用する暗号の脆弱性の問題点
V9	CSP がデータ保存や中継する際に，弱い暗号を利用する問題点
V10	CSP で暗号のままでデータを処理できない問題点
V11	CSP での暗号鍵の管理による問題点
V12	暗号カギの生成に用いる乱数発生の脆弱性の問題点
V13	標準的な技術とソリューションがない問題点
V14	CSP との間でエスクロー契約がなされない問題点（NO SOURCE ESCROW AGREEMENT）：ソフトウェアのライセンスの場合，第 3 者にソースコードを預託しておき，倒産した場合など，そのソースコードを利用できる権利
V15	CSP のリソースの利用のモデルが正確でない問題点
V16	脆弱性評価が正しく実施されていないため，CSP を信用できない問題点
V17	CSP の内部ネットワークでクラウド利用者が他の利用者へのポートスキャンなどができてしまう問題点
V18	CSP のリソースの隔離が不十分なため他の利用者にデータが漏れる問題点
V19	CSP からフォレンジック情報が提供されない問題点
V20	CSP でストレージなどが共用されていると，初期化できないため，情報漏えいにつながる問題点
V21	ユーザ企業に課せられる責任（や契約）に対して無頓着な問題点
V22	CSP が他の CSP を利用する場合の隠れた依存性の問題点
V23	CSP の SLA 条項が他の関係者の約束と矛盾する場合の問題点
V24	CSP の SLA 条項が（CSP が契約で無理をして）過剰なビジネスリスクを含んでいる場合の問題点
V25	CSP が利用者に対して監査を受けることを許可しない場合や認証を受けない問題点
V26	CSP のインフラストラクチャの特徴的なセキュリティコントロールが実施されていない問題点（それ以外は実施されている）
V27	CSP において，長期的なインフラストラクチャのリソースへの投資計画が策定されていない問題点
V28	CSP のリソース利用の上限設定がない問題点
V29	CSP のデータ提供の際のエンドポイントでのミラーリングやデータの複数の個所への保存で生じる法的な問題とデータ保存に際して透明性が確保できない問題点
V30	CSP のデータ処理についての法的な規制の情報がなく，データを没収されたりする問題点
V31	CSP 利用条件の完全性と透明性が不足している問題点
以下の V32 ～ V40 は，クラウドサービスに限らない共通する問題点	
V32	CSP やユーザ企業のセキュリティアウェアネスが不足していて，リスク対策を行わない問題点
V33	CSP では，高い特権の役割が必要となるため，スタッフに対する不適切な審査が重大な脆弱性となる問題点
V34	CSP における役割と責任の属性が不適切なために起きる問題点
V35	CSP 内部では，役割の分離のミスから，管理者が過剰な権限（1 人でクラウド全体のデータにアクセスできるなど）を持ち得る脆弱性がある問題点
V36	CSP で，役割と権限の分離がなされていない問題点
V37	CSP での入退室管理が十分でない問題や電磁漏えいによる盗聴が起きる問題点
V38	CSP での不適切なセキュリティ対策，物理的対策，ヒューマンエラー，アドミニストレータのトレーニング不足などの問題点
V39	CSP のシステムや OS が持つ脆弱性の問題点
V40	CSP の信用のできない（バグのある）ソフトウェアの問題点
V41	CSP の事業継続計画や災害復旧計画が不十分な問題点
V42	CSP の資産管理が不十分や不完全な問題点
V43	CSP の資産の分類が不十分や不完全な問題点
V44	CSP の資産のオーナーが不明確な問題点
V45	セキュリティや法的な要求事項を考慮しなかったり，ユーザ企業が関与しないシステムやアプリケーションを構築したり，ビジネスの要求条件が不明確なシステム設計の問題点
V46	不十分な CSP を選択する問題点
V47	CSP の代替がない問題点
V48	CSP のアプリケーションのバグなどの脆弱性と不十分なパッチ提供の問題点
V49	CSP のリソースを無駄に消費する問題点
V50	CSP の守秘義務協定違反の問題点
V51	CSP がデータを紛失する問題点
V52	CSP のログデータの収集と廃棄に関するポリシーや手順が欠如する問題点
V53	CSP がフィルタリングする際に起きる不十分な設定や設定ミスに伴う問題点

付表 1　ENISA による脆弱性評価項目 [3)]