2013 年 4 月 26 日

独立行政法人情報処理推進機構（IPA）

重要情報インフラ防護（CIIP）の観点から見たクラウド

本概要は、欧州ネットワーク情報セキュリティ庁（ENISA：European Network Information Security Agency）が発行する、“Critical Cloud Computing – A CIIP perspective on cloud computing services”の主にエグゼクティブ・サマリーの抄訳となります。

内容の詳細につきましては、原文をご参照ください。（※本文中のリンク先は全て英文となります）

URL：http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/critical-cloud-computing

クラウドコンピューティング（以下、クラウド）の浸透に関する市場調査会社等の公表データによれば、数年後には約 80%の組織がクラウドを利用していることが見込まれている。重要情報インフラ防護（CIIP）の観点から見ると、クラウドにおける IT 資源の集約は、最先端のセキュリティ対策とレジリエンスが期待される一方で、障害やサイバー攻撃が発生した場合、影響が非常に広範囲に及ぶ可能性があり、諸刃の剣と言える。

重要情報インフラ（CII）は、国の経済活動や社会活動に不可欠な情報通信技術（ICT）システムを指すが、欧州委員会（EC）では CII を、a) 当該システム自身が重要インフラである ICT システム、または b) 他の重要インフラの運用に不可欠な ICT システム、と定義している。欧州連合（EU）加盟国は、EC の CIIP に関する行動計画に基づき CII の防護に取組むことを表明しており、CIIP の観点から見たクラウドのガバナンス戦略を検討している。本資料は、検討の参考として、CIIP の観点から、クラウドに対する脅威やサイバー攻撃によるサービス停止の影響などを、公開情報を基に調査したものである。

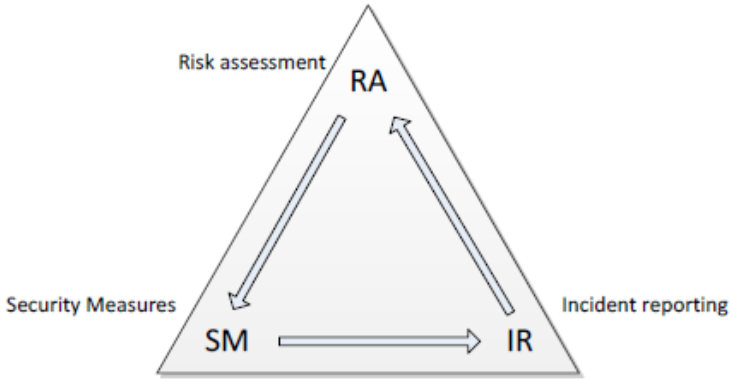
以下に、調査結果の主要点をまとめる。

- **クラウド自身の重要インフラ化**
  クラウドの利用は増加しており、近い将来大多数の組織が何かの形でクラウドに依存している状態になることが見込まれる。金融業界やエネルギー業界などの重要インフラでも利用が始まっており、そのうちにクラウド自身が重要インフラとなる。
- **クラウドと自然災害**
  クラウドの大きな利点として、従来のような IT システムの配備や単一のデータセンタでは提供することが困難な、局地的な停電や自然災害に直面した場合に提供されるレジリエンス（resilience）がある。
- **クラウドと過負荷／サービス妨害（DoS）攻撃**
  クラウドの大きな利点として、弾力性（elasticity）がある。これにより、使用量がピークに達した時や DDoS 攻撃を受けた際の負荷にも対処することができる。
- **サイバー攻撃**
  IT 資源を集約していることで、ソフトウェアの弱点を利用したサイバー攻撃に遭った場合には、非

常に大規模なデータ漏洩を起こす可能性がある。

- **IssS／PaaS が最重要**
  クラウドの中でも、他の IT ベンダにクラウドサービスを提供する Infrastructure as a Service（IaaS）と Platform as a Service（PaaS）は影響力が大きいため、最も重要となる。
- **行政訴訟／法的訴訟**
  クラウドサービスプロバイダ、または、そのユーザが関係する行政訴訟や法的訴訟が発生した場合、全ユーザ（のデータ）に影響を及ぼす可能性がある。
  - *例 1* ：Megaupload 社が提供していたオンラインストレージサービスが著作権法違反の疑いで米司法省によって閉鎖され、1 億 8 千万ユーザの 25 ペタバイトデータが失われた。
  - *例 2* ：Linkup 社が提供していたオンラインストレージサービスで、一部のユーザのデータへのアクセスが出来なくなった。その直後にサービス自体が閉鎖され、2 万人の有料サービスユーザのデータが失われた。

CIIP に関する行動計画では、クラウドに係わるガバナンス戦略の検討が要求されている。CIIP の観点から言えば、目標は大規模なセキュリティインシデントの防止であり、セキュリティガバナンスは「リスク評価（RA）」「セキュリティ対策（SM）」「インシデント報告（IR）」の 3 つのプロセスに大別される。



以下に、各プロセスにおける対策の勧告を記す。

- **リスク評価（RA）**
  リスク評価は、セキュリティガバナンスの基本を為す。
  - *範囲* ：実際的なアプローチを取り、最も重要なクラウドサービスから取り組む必要がある。影響度で言えば、IaaS/PaaS の優先度が最も高くあるべきと言える。
  - *依存性* ：多くの国では電力と通信の名があがるが、大規模なクラウドサービスについても検討すべきである。
  - *物理的・論理的依存性の透明性* ：クラウドはレジリエンスを提供すると同時に、1 つ間違えると IaaS/PaaS を通じて本来無関係なサービスにも障害の連鎖（cascading failure）を引き起こす可能性がある。どの重要インフラサービスがどのクラウドサービスに依存しているのか、主要な物理的・論理的依存性について全て明確にしておくことが重要となる。
- **セキュリティ対策（SM）**
  適切なセキュリティ対策を実施することは、セキュリティガバナンスの焦点となる。

- *ベストプラクティスの共有促進* :プロバイダにおける適切なセキュリティ対策実施のため、政府はセキュリティ対策に関する議論と共有を奨励するオープンな文化を育てる必要がある。また、特定のセキュリティ対策を指定するような柔軟性のない施策を取ってはならない
- *論理的冗長性* :多層防御を敷き、システム同士を異なる論理的構造で区切る。
- *標準化* :特定のプロバイダやプラットフォームに依存するのを抑制する。特に IssS/PaaS の場合、1 つのプロバイダに何かあった場合にも、ユーザが別のクラウドサービスに移れるようにする。
- *モニタリング*、*監査*、*テスト*、*演習* :情報セキュリティでは、監査とテストの重要性が説かれている。プロバイダは社内監査やテストを頻繁に行うほか、適宜外部監査やテストを行う。ガバナンスについては、しばしば独立した外部の監査組織による認証の必要性が論じられるが、外部の監査組織が複雑かつ常に変化しているシステムのセキュリティを年に 1 度の監査で評価するのは困難である。プロバイダおよび政府は、継続的なモニタリング、監査、テストおよび演習を実施すべきである。

- **インシデント報告(IR)**

  インシデント報告は、セキュリティ対策のクロスチェック、リスク評価の改善、ガバナンスプロセス全体へのフィードバックを得る機会を提供する。
  - *報告の義務付け* :インシデントの報告無くしては、セキュリティインシデントの影響を理解するのは困難であり、セキュリティ対策の優先度付も難くなる。結果的に、セキュリティガバナンスが非効率的になり、更には無効化してしまう。政府およびプロバイダは、報告の基準と報告対象のサービス範囲に関してきちんと同意することが重要である。
  - *法的結果* :ある種の攻撃はステルス性が高く、自社のクラウドシステムを熟知している管理者でも攻撃の痕跡に気づくのが難しい場合もある。また、叱責や法的結果を恐れて上層部や当局にインシデントを報告しない可能性は常に存在する。加盟国は、プロバイダがセキュリティインシデントを報告するインセンティブを検討すべきである。
  - *障害およびセキュリティインシデント* :クラウドサービスのセキュリティインシデントに関してはそれなりな情報が多少存在する一方で、障害に関する情報は存在しない。また、インシデント情報は存在するとは言え、話題となった事件であっても影響を受けたユーザの数や継続時間といった基本的な情報は明らかにされない場合が多い。全体的なリスクや対策の有効性を把握するためにも、幅広いクラウドサービスプロバイダから報告を得ることが必須となる。

以上