学習指導要領

文部科学省
成長分野等における中核的専門人材養成の戦略的推進事業

実践クラウドセキュリティ

情報セキュリテイ分野の中核的専門人材養成の
新たな学習システム構築推進プロジェクト

学習指導要領

文部科学省
成長分野等における中核的専門人材養成の戦略的推進事業

実践クラウドセキュリティ

情報セキュリティ分野の中核的専門人材養成の
新たな学習システム構築推進プロジェクト

目　　次

はじめに

クラウドコンピューティング技術は、様々な要素技術の集合体ともいえるものです。その要素技術としては、ハードウェアアーキテクチャー、ソフトウェアアーキテクチャー、ネットワーク、サーバー、ストレージ、Web、モバイル、セキュリティ、ITサービスマネジメント等が挙げられます。そのため、クラウドコンピューティング技術を理解するためには、これらの要素技術の基本的な知識が前提となります。できる限り、事前に学習をしておくか、これらの関連技術を事後に補完のために学習をさせるようにしてください。

また、講義をする際は受講者がこれらの前提知識の所有の程度を予め調べておき、それにより、説明を工夫してください。前提知識がある場合にはそれをおさらいとして確認しながら、ない場合にはそれを補足しながら柔軟に進めてください。これにより、受講者の理解はより体系的になることでしょう。

第 1 章

クラウドコンピューティングとは

1-1 クラウドコンピューティングの概念、基本的な定義と特徴

履修目標

クラウドコンピューティング及びその情報セキュリティの知識習得のために、クラウドコンピューティングの基本的な定義を習得する。

- クラウドコンピューティングの基本的な定義を説明できる。
- クラウドコンピューティングの5つの基本的な特徴を説明できる。

標準学習時間 45～50分

※授業時間が90分の場合は、1-2.と併せて実施してください。

指導のポイント

ここでは、NIST（NationalNational Institute of Standards and Technology；米国国立標準技術研究所）のNIST SP800-145「NISTによるクラウドコンピューティングの定義」を使って、クラウドコンピューティングの基本的な定義と特徴を説明します。

単に定義を読み上げるのではなく、コンピューターやソフトウェアのアーキテクチャー、従来のインターネットサービスのモデルや技術などに当てはめ、比較しながら説明することが望ましいと思われます。

そのためにも、NIST SP800-145は事前に何度か目を通しておく必要があります。

また、（NIST SP800-145にも書かれている通り）これらの定義や特徴はあくまで概念的なものであり、今後もクラウドコンピューティングの技術は進化を続け、この定義や特徴が変わっていくことは間違いありません。今から半年後には、違った説明をしなければならないかもしれません。定義や特徴を、ただ暗記させるのでは、概念的に意味を理解させられるように説明をしましょう。

そのような旨を、必ず強調するようにしましょう。

1-2 クラウドコンピューティングのサービスモデルと利用の形態

履修目標

ここでは、NIST SP800-145「NISTによるクラウドコンピューティングの定義」を使って、クラウドコンピューティングの3つのサービスモデルについて説明します。

- SaaS(Software as a Service)について、説明できる。
- PaaS(Platform as a Service)について、説明できる。
- IaaS(Infrastructure as a Service)について、説明できる。
- 従来のサービスモデルとクラウドコンピューティングのサービスモデルの違いについて、説明できる。

標準学習時間 45～50分

※授業時間が90分の場合は、1-1.と併せて実施してください。

指導のポイント

ここに挙げている3つのサービスモデルの概要とその違いを図にあるように4つの階層で説明してください。説明する際には、2-5に書かれている概要（類似するサービスとの違い）を説明したり、場合によっては一緒に説明したりするのもよいでしょう。講義をする側の説明のシナリオや受講する側の前提知識などによって調整してください。

そして、この3つのサービスモデルはNISTにおける定義によるものであり、最近ではこれ以外の概念的な用語も使われ始めています。その例としては、DaaS（Desktop as a Service）、CaaS（Crimeware as a Service）、BPaaS（Business Process as a Service)などが使われています。

近年、クラウドコンピューティングのサービスは多様化しており、サービスモデルも変化することが予想されます。今後も、様々なXaaSという概念的な用語やサービスが登場してくると思われますので、そのような動向もあわせて説明しておくと良いでしょう。

1-3 クラウドコンピューティング導入による変化と効果（1）

Information security

履修目標

- クラウドコンピューティング導入により変わることが説明できる。
  （業務、生活、システムライフサイクル）
- クラウドコンピューティングの導入の主要なメリットや効果を説明できる。

標準学習時間 45～50分

※授業時間が90分の場合は、1-4.と併せて実施してください。

指導のポイント

ここでは、クラウドコンピューティングの導入による変化とその効果について説明します。

「所有するIT」から「利用するIT」に変わることにより、様々な変化が起こります。ここでは、その変化をネットワークやシステム、業務や生活、システムライフサイクルの3つの視点から説明しています。それぞれ、導入前と導入後を比較することによって、具体的な変化が受講者に想像できるように説明してください。

実際にクラウドサービスを使っている受講者がいた場合には、その人が感じている変化や効果を答えさせることで、講義を進めるのも効果的な方法です。

1-4 クラウドコンピューティング導入による変化と効果(2)

履修目標

- クラウドコンピューティング環境における提供者と利用者の管理責任の範囲を理解し、説明することができる。
- クラウドコンピューティングサービス利用の考慮点が説明できる。
- クラウドコンピューティングサービス利用の際の検討事項を説明できる。
- クラウドコンピューティングのこれからの変化や展望について説明できる。

標準学習時間 45～50分

※授業時間が90分の場合は、1-3.と併せて実施してください。

指導のポイント

ここでは、クラウドコンピューティングの利用者(ユーザー)と提供者(プロバイダー)の責任とその範囲について説明します。

事業者の責任は、クラウドサービスを提供している内容によっても異なります。

導入の効果に関しては、以下にあげるIPAセキュリティセンターの「クラウドサービス 安全利用のすすめ」と経済産業省の「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」を参照しています。この2つの文書に予め目を通しておくのもよいでしょう。

○「クラウドサービス 安全利用のすすめ」～IPAセキュリティセンター

http://www.ipa.go.jp/files/000011594.pdf

○「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年度版」

～経済産業省

http://www.meti.go.jp/press/2013/03/20140314004/20140314004-2.pdf

○「クラウドセキュリティガイドライン活用ガイドブック 2013年度版」

～経済産業省。

第 2 章

クラウドコンピューティングサービス

2-1 クラウドコンピューティングを支える技術（1）

履修目標

クラウドコンピューティングを支える技術要素である、ネットワーク技術、Web技術、ストレージ技術、認証技術を習得します。

- ネットワーク（分散処理、QoS、エミュレータ）、グリッドコンピューティング、Webアプリケーション、データストレージ（分散ストレージ、RAID、NAS/SAN）、ID管理

標準学習時間 45～50分

※授業時間が90分の場合は、2-2.と併せて実施してください。

指導のポイント

クラウドコンピューティングでは、ネットワークやストレージ、アプリケーションなどの様々な技術が使われています。ここでは、ネットワーク技術、Web技術、ストレージ技術、認証技術を扱います。

単なる技術の解説ではなく、実際にネットワークやクラウドコンピューティングのどこでどう使われているかを説明するようにしてください。

また、ここではこれらの技術の概要の解説に留めています。ここでの内容だけでは、十分な理解が得られないと思われる場合には、他の科目や参考書籍などを提示してください。

ネットワークやストレージ、アプリケーションなどの基本的な理解が前提となります。これらの知識が不十分な場合は、予めその項目の学習を促すか、後からその項目の学習をするように指導してください。

2-2 クラウドコンピューティングを支える技術（2）

履修目標

ククラウドコンピューティングを支える技術要素である、モバイル通信技術、ネットワークやシステムの運用技術を習得します。

- モバイル通信、冗長化技術・フォールトトレラントシステム、キャッシング・負荷分散

標準学習時間 45～50分

※授業時間が90分の場合は、2-1.と併せて実施してください。

指導のポイント

単なる技術の解説ではなく、実際にネットワークやクラウドコンピューティングのどこでどう使われているかを説明するようにしてください。

また、ここではこれらの技術の概要の解説に留めています。ここでの内容だけでは、十分な理解が得られないと思われる場合には、他の科目や参考書籍などを提示してください。

ネットワークやモバイル、システム管理などの基本的な理解が前提となります。これらの知識が不十分な場合は、予めその項目の学習を促すか、後からその項目の学習をするように指導してください。

2-3 ITサービスマネジメント

Information security

履修目標

ククラウドコンピューティングを支える技術要素である、ITサービスマネジメントのフレームワークとマネジメントシステムを習得します。

- ITサービスマネジメント、ITIL V2/V3、ITSMS

標準学習時間 45～50分

※授業時間が90分の場合は、2-4.と併せて実施してください。

指導のポイント

単なる規格の解説ではなく、実際に何のためにクラウドコンピューティング事業者を含めたITサービス事業者で使われているのかを説明するようにしてください。

また、ここではこれらの規格とフレームワークの概要の解説に留めています。ここでの内容だけでは、十分な理解が得られないと思われる場合には、他の科目や参考書籍などを提示してください。

○ITサービス管理に関しては、以下の資料を予め目を通しておくと良いでしょう。

「ITSMSユーザーズガイド-JIS Q 20000(ISO/IEC 20000)対応-」

～一般財団法人日本情報経済社会推進協会

「ITSMSユーザーズガイド～導入のための基礎～」

一般財団法人日本情報経済社会推進協会

※ITSMS適合性評価制度としてではなく、ITSMSのフレームワークや要素技術を理解し、説明できるようにしましょう。

2-4 ITサービスマネジメントの主要技術(1)

履修目標

クラウドコンピューティングを支える技術要素である、ITサービスの管理技術13のうち、サービス提供プロセスの6つの管理技術の知識を習得します。

- サービスレベル管理、サービスの報告、サービスの継続及び可用性管理、サービスの予算業務及び会計業務、容量・能力管理、情報セキュリティ管理

標準学習時間 45～50分

※授業時間が90分の場合は、2-3.と併せて実施してください。

指導のポイント

2-3. と同様に単なる技術の解説ではなく、実際に何のためにクラウドコンピューティング事業者を含めたITサービス事業者で使われているのかを説明するようにしてください。

2-5 ITサービスマネジメントの主要技術(2)

履修目標

クラウドコンピューティングを支える技術要素である、ITサービスの管理技術13のうち、関係プロセス、解決プロセス、統合的制御プロセス、リリースプロセスの7つの管理技術の知識を習得します。

- 事業関係管理、供給者管理、インシデント及びサービス要求管理、問題管理、構成管理、変更管理、リリース及び展開管理

標準学習時間 45～50分

※授業時間が90分の場合は、2-6.と併せて実施してください。

指導のポイント

2-3. 2-4. と同様に単なる技術の解説ではなく、実際に何のためにクラウドコンピューティング事業者を含めたITサービス事業者で使われているのかを説明するようにしてください。

2-6 ネットワーク管理の技術

Information security

履修目標

クラウドコンピューティングを支える技術要素である、ネットワークの運用技術を習得します。

- 耐障害性、性能管理、バックアップ、ログ管理、施設・設備の管理

標準学習時間 45～50分

※授業時間が90分の場合は、2-5.と併せて実施してください。

指導のポイント

単なる技術の解説ではなく、実際にネットワークやクラウドコンピューティングのどこでどう使われているかを説明するようにしてください。

また、ここではこれらの技術の概要の解説に留めています。ここでの内容だけでは、十分な理解が得られないと思われる場合には、他の科目や参考書籍などを提示してください。

ネットワークやモバイル、システム管理などの基本的な理解が前提となります。これらの知識が不十分な場合は、予めその項目の学習を促すか、後からその項目の学習をするように指導してください。

2-7 仮想化技術（1）

Information security

履修目標

クラウドコンピューティングの中核的な技術としての「仮想化技術」を理解する。

- 仮想化の概念や定義、パターン（分割、統合、模倣）、仮想化のメリットとデメリットを説明できる。

標準学習時間 45～50分

※授業時間が90分の場合は、2-8.と併せて実施してください。

指導のポイント

仮想化技術は、クラウドコンピューティングを構成する中核的な技術です。まずは、仮想化の概念や定義、パターン（分割、統合、模倣）を説明し、それを当てはめながら、様々な仮想化技術を説明しましょう。その際に、2-1.及び2-2.で学習した内容もおさらいしながら、これらを組み合わせて説明することで、受講者の理解をさらに進めることができます。

2-8 仮想化技術（2）

Information security

履修目標

ネットワークの仮想化（仮想ルータ、VLAN、VPN）について理解する。

標準学習時間 45～50分

※授業時間が90分の場合は、2-7.と併せて実施してください。

指導のポイント

2-3.と同様に、2-1.及び2-2.で学習した内容もおさらいしながら、これらを組み合わせて説明することで、受講者の理解をさらに進めることができます。

ここでは、ネットワーク技術やネットワーク機器の機能や特徴もおさらいしながら、説明をすることで、受講者はさらに理解をすることができるでしょう。

ネットワーク技術や通信技術の分野では、新しい技術や規格、プロトコルなどが既に策定されていたりするため、最新動向なども把握しておくとよいでしょう。

2-9 SaaS、PaaS、IaaS

Information security

履修目標

クラウドコンピューティングの3つのサービス提供形態「SaaS」「PaaS」「IaaS」について、詳細を理解し、サービスの選択や提案・提供などが適切に実施できるようにする。

- SaaS
- PaaS
- IaaS

標準学習時間 45～50分

※授業時間が90分の場合は、2-10.と併せて実施してください。

指導のポイント

1-3.で学習した内容を簡単におさらいしながら、従来のサービスとの比較でできる限り具体的に説明してください。

特に、SaaSは「ASP(Application Service Provider)の呼び方が変わっただけ」というような誤解をされていることが多いようです。サービスの提供と利用（クラウドコンピューティングサービスは、オンデマンドの課金と支払いであること）において、明確に違うことを説明してください。

PaaSやIaaSも、同じようにその違いを説明してください。

2-10 商用クラウドコンピューティングサービスの種類と特徴及び考慮点

履修目標

2-9.「SaaS、PaaS、IaaS」の学習内容に基づき、実際に提供されているサービスを学習することにより、さらに具体的にクラウドコンピューティングのサービスを理解する。

標準学習時間 45～50分

※授業時間が90分の場合は、1-3.と併せて実施してください。

指導のポイント

1-3、2-9.で学習したことをもとに、実際に提供されているサービスを例として、さらに具体的に説明してください。

ここでは、クラウドコンピューティングの3つのサービスモデル（SaaS/PaaS/IaaS）と4つの実装モデルのうちのプライベートクラウドを除くモデル（パブリッククラウド、コミュニティクラウド、ハイブリッド）を、ここに挙げたような実際提供されているサービスを用いて説明していきます。

サービス説明のサイトや、実際のサービスの画面を見せたり、使わせたりしながら説明するとさらに理解が深まるでしょう。

第 3 章

クラウドサービスにおける情報セキュリティ

3-1 クラウドサービスのセキュリティ上の課題

Information security

履修目標

- クラウドサービスを導入しない理由と導入する理由の両方で情報セキュリティが大きな関心事であることを理解する。
- クラウドサービスを選定するためには、自社のセキュリティ要件を定めそれを基準にして評価することを理解する。
- クラウドサービスすることで発生する新たなリスクを説明できる。

標準学習時間 20～30分

※3-1は3-2-1～3-2-2と合わせて実施することを推奨します。3-1と3-2-1～3-2-2で45～50分の学習時間となります。

指導のポイント

3-1-1（1）で使用しているグラフは総務省の「平成24年通信利用動向調査」から囲繞しています。国の機関が公開する情報は中立な印象を受けることから、資料として用いやすい。情報は常に更新するように、経済産業省、総務省、内閣サイバーセキュリティセンター等が公表する新しい情報を入手できるように情報源は周期的に確認することが望まれます。

3-1-1（1）の図3-1、3-2において、クラウドサービスを導入しない理由の2番目が機密性（情報漏えい）に対する不安であり5番目の「ネットワーク安定性に不安がある」も可用性に対する不安で、情報セキュリティに関する不安が導入の阻害要因となっていることが分かります。その一方で導入する理由の4番目が「安定運用、可用性が高くなるから」、5番目が「情報漏えい等に対するセキュリティが高くなるから」とセキュリティの向上を期待する意見が挙げられており、クラウドサービス導入において情報セキュリティが関心事であることを理解しておきます。数字だけでは分からないものの、導入しない理由に情報セキュリティに対する不安を抱えているのは具体的な根拠があるというより、社外にデータを置くことやデータの所在が利用者から見えないといったイメージだけで”漠然とした不安”によるものと想像できます。対して導入した理由に情報セキュリティの向上を挙げているのは、導入する際に具体的に調査したところ自社の現状に比較してクラウドサービスの方が高い情報セキュリティレベルを実現できると評価したと想像することができます。

正しくリスクを分析し客観的な評価ができれば、クラウドサービスに対する情報セキュリティ上の不安の多くは払拭できるものと思われます。

客観的な評価をするためには何らかの物差しをもって測る必要があり、その物差しのひとつがここで述べているセキュリティ要件です。3-1-1（2）では、自分たちが期待するセキュリティを求めるのであれば自社の確固たる基準としてのセキュリティ要件を定義する必要があることを理解させます。

セキュリティ要件はシステム要件の一部であるため、セキュリティ要件を検討するためには、システムの導入・運用プロセスやタスクに関する事項について概要を知っておくことが望まれます。セキュリティ要件定義の参照元としてはITILやISO 20000が代表的です。

セキュリティ要件はシステム要件の一部であり、セキュリティだけがクラウドサービス選定の唯一の基準ではないことを伝えます。まずは、クラウドに何をさせるのか、それが実現できるか否かが選定基準の第一義であり、その上でセキュリティが期待通りかを評価します。したがって、セキュリティ要件がすべて満たされなくてもシステム要件全体での評価が良ければ、セキュリティ上の不足も受容するという判断もあることを理解させます。

3-1-2（1）では、セキュリティ要件を“実装”“維持・運用管理”利用“”開発・変更工程“という区分で考えると説明していますが、組織によってシステム要件、セキュリティ要件の定義方法は異なるため、実際に勤務する先により区分や定義手順がここでの説明と異なることに言及してください。

3-1-2（1）で、“実装”“維持・運用管理”利用“について例を挙げていますが、他の例も用意しておいて説明すると理解の助けになると思われます。

3-1-2（2）の図3-3は、いくつかの情報を独自に解釈したものです。講師により情報を付加する等変更しても良い。

今まで社内システムで実施していたことがクラウド環境に置き換わった場合に変化することによるリスクが発生すること（直接管理できない範囲の発生に伴うリスク）、また、今までのシステムには存在しなかった利用形態が新たに付加されることで新たなリスクが発生すること（新たな機能や新たな環境に関連する新たなリスクの発生）を説明します。

3-2 リスクアセスメントに基づくセキュリティ要件の策定

Information security

履修目標

- セキュリティ要件に記載するセキュリティ対策はリスクアセスメントを根拠に検討することを理解する。
- リスクアセスメントの流れを説明できる。
- クラウドサービスにおけるインシデントの原因と傾向を説明できる。
- クラウドサービス利用における代表的な脅威が説明できる。
- クラウドサービスにおける責任分界点が説明できる。
- ガバナンス、マネジメント、個々の管理策、サプライチェーンの概要が説明できる。

標準学習時間 60～70分

※3-2-1～3-2-2は3-1と合わせて実施することを推奨します。3-1と3-2-1～3-2-2で45～50分の学習時間となります。

※3-2-3～3-2-4は、3-3と合わせて実施することを推奨します。3-2-3～3-2-4と3-3で45～50分の学習時間となります。

指導のポイント

セキュリティ要件を形成するセキュリティ対策は、リスクアセスメントを根拠に特定する必要があります。リスクアセスメント（分析・評価）の結果に基づかなければセキュリティ対策に過不足が発生することを説明します。

リスクアセスメントは様々な手順が存在します。実際に勤務する先によりリスクアセスメント手順が異なることに言及してください。ここでの説明はリスクアセスメントの一例であることに留意ください。

3-2-1（1）は、リスクアセスメントの流れを解説しています。（2）～（6）は（1）で提示したリスクアセスメントの各段階を個々に解説したものとなります。（5）のリスク対応について、受容、低減、移転、回避のそれぞれの考え方を補足説明することが望まれます。

本教科書ではリスクアセスメント方法の詳細には触れていません。講師は、ISO/IEC 27001及びISO 31000でリスクアセスメントの枠組みを理解し、ISO/IEC 31010で代表的なリスクアセスメント手法を学んでおくことが望まれます。また、自身でリスクアセスメントを実施し経験しておくこととより理解が深まると思われます。

3-2-2は、経済産業省「クラウドセキュリティガイドライン活用ガイドブック」から引用したクラウドサービスにおけるインシデントの傾向です。クラウドサービスにおける事故・障害の多くはシステム環境とシステム運用に関するものが多いことが分かります。ただし、(2)に挙げたインシデント事例を見ると、システム障害以外にヒューマンエラーも多いことが分かります。また、システム障害発生時に対応を誤る等、システム障害とヒューマンエラーが重なる事故も発生していることも留意点です。

また、原因がどうであれ、マルチテナント環境で仮想化により利用者環境集積することで、サービス停止などの事故が発生した場合の影響範囲が大きいことを説明します。

インシデントは日々発生していますので、常に情報を収集し教科書に記載されていない最新の事例を盛り込むようにすることが望まれます。特に国内の事例には注目しておく必要があります。

3-2-3では、リスクを招く原因である脅威を特定している。教科書では、脅威の存在を"クラウド利用者内""クラウド事業者内""利用者と事業者間のインフラ"という3つの区分で表記しています。3-1で解説した通りクルドサービス選定に際し自社のセキュリティ要件を洗い出す必要性に言及しました。クラウドサービス選定といってもクラウド事業者内のセキュリティだけではなく前述の3つの区分全てを包括して考えなければ自社のセキュリティ要件は定義できないことを説明します。

3つの区分の内"クラウド事業者内"のリスクの多くは利用者が直接関与してコントロールできないという認識も説明する必要があります。

脅威をもたらす要因については、以下のように整理すると洗い出しやすいことを補足説明します。脅威は人がもたらすものと災害や電源不良など環境によるものがあり、それぞれ組織の内部要因と外部要因があり、さらに人的脅威は故意か偶発(ミス)があります。

人的脅威	内的要因		外的要因	
	故意	偶発	故意	偶発
環境的脅威	内的要因		外的要因	

脅威に対するセキュリティ対策を検討する時、3-2-3(2)に記述した通り責任分界点が重要であることを解説します。自組織が自らの責任でセキュリティ対策を実施すべき範囲は責任分界点によって明らかになります。

3-2-3(3)の仮想環境におけるリスクは事業者の責任範囲ですが、クラウドを利用する上で利用者も知っておく事項であることを理解させます。

表3-2は、クラウドセキュリティ推進協議会　公開資料「付表:リスクとコントロールの整理」から引用したもので、経済産業省の事業の中でENISAが定義したリスクを整理して再構成したものです。クラウドサービスに関するリスクについては、クラウドセキュリティ推進協議会の公開資料(http://www.jasa.jp/jcispa/documents/)を参考にして最新情報を得ると良いでしょう。

3-2-4を説明するために、講師はガバナンスとマネジメントのサイクルと各フェーズの実施事項の概要を知っておく必要があります。

（1）図3-8は、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」から引用しています。

（http://www.meti.go.jp/press/2013/03/20140314004/20140314004.html）

（2）ガバナンスは、セキュリティ要件の定義には直接関連しませんが、セキュリティの目的が経営陣の示す方向付けと整合が取れていることを意識しておく必要があります。また、セキュリティの運用が経営陣にモニタリングできるようにしておく必要があります。講義の中で詳細は触れないまでもガバナンスの要素である“方向付け”“評価”“モニタリング”の概要程度は理解しておくことが望まれます。

（3）マネジメントは、情報セキュリティの確立と運用のためのフレームワークで、Plan・Do・Check・Actのサイクルで一般に説明されます。情報セキュリティの分野ではISO/IEC 27001（JIS Q 27001）が標準として用いられます。

（4）個々の管理策（対策）では、情報セキュリティの実施のガイドであるISO/IEC 27002（JIS Q 27002）の内容を把握します。ISO/IEC 27002はクラウドコンピューティングに限らず情報セキュリティ全般に適用できるため、組織における情報セキュリティ要件の基礎を定義する際に参考にします。その上でクラウドサービスを導入する範囲について、クラウドサービスのための実施ガイドであるISO/IEC 27017（JIS Q 27017）を参照しクラウド固有の要件を追加します。ISO/IEC 27017については、4-1-1（1）で取り上げるので、ここでは内容に踏み込む必要はありません。

この他、情報セキュリティの管理策の参照元として、以下の情報元に当たっておくと良いでしょう。

・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」「SaaS向けSLAガイドライン」
・IPA（独立行政法人 情報処理推進機構）「クラウド・コンピューティング社会の基盤に関する研究会 報告書」「中小企業のためのクラウドサービス安全利用の手引き」
・総務省「スマート・クラウド研究会報告書」「ASP・SaaSにおける情報セキュリティ対策ガイドライン」「地方公共団体におけるASP・SaaS導入活用ガイドライン」
・海外「Cloud Security Alliance」「ENISA」「NIST SP800-144,145,146」

サプライチェーンについて、他の事業者が提供するIaaSの上にPaaSやSaaSを構築する等事業者間で「事業者－利用者」という関係が構築されサプライチェーンの関係が築かれることを説明します。サプライチェーンにおいて、例えばSaaSを採用する際、利用者は採用するSaaSの基盤を構築するPaaS事業者、IaaS事業者の責任範囲を知り、場合によっては、SaaS事業者以外にPaaS事業者、IaaS事業者のセキュリティ対策を確認する必要があることを説明します。

顧客や取引先によっては、自社の情報がクラウド環境に置くことを許可しない方針を持つ場合があります。自社と情報を交換あるいは共有する外部組織（顧客や取引先等）が、そのような方針を持つ場合は、その組織の情報についてクラウド環境を介して交換・共有ができない可能性があります。その場合は、クラウドを介さない情報交換・共有の方法を検討し合意しておく必要があります。

3-3 クラウドサービスの選定

Information security

履修目標

- クラウドサービス選定において自社のセキュリティ要件と照らし合わせる公開情報（SLA、約款、ホワイトペーパー等）が説明できる。
- 自社のセキュリティ要件と公開情報にGAPがあったときの選択肢（受容、特約、代替策、不採用）が説明できる。

標準学習時間 20～30分

※3-3は、3-2-3～3-2-4と合わせて実施することを推奨します。3-3と3-2-3～3-2-4で45～50分の学習時間となります。

指導のポイント

3-3-1（1）では、自社のセキュリティ要件と照らし合わせる公開情報（SLA、約款、ホワイトペーパー等）の例を挙げ、どのような内容が記述されているかを解説してください。

実際のクラウドサービスのホームページを表示しSLA、約款、ホワイトペーパー等を例示しながら説明すると良いでしょう。

3-3-1（2）では、クラウドサービス選択においてセキュリティ要件以外にも「コスト」「事業者の健全性」「ISMS等第三者認証」も評価要件であることを説明します。

コストは、自社にシステム持つ場合のコスト（買い取り、リース等と保守、運用人件費などランニングコスト）に対しクラウドサービスのコスト（初期導入費用、課金、運用人件費などランニングコスト）の比較が提示できることが望まれます。

事業者の健全性は、クラウドサービスを提供する事業者の主要事業、財務状態、実績等を知るためにどのような情報を見るのかを説明します。6章にも記載されていますが、一般財団法人マルチメディア振興センター「クラウドサービスの安全・信頼性に係る情報開示認定制度」（http://www.fmmc.or.jp/cloud-nintei/）が参考になることを伝えます。

事業者のセキュリティ上の信頼性をはかる目安の一つに第三者認証があります。特に2016年に国内で運用が始まったISMSクラウドセキュリティ認証が事業者選定の目安として有効です。ISMSクラウドセキュリティ認証は、ISO/IEC 27001の認証制度を基盤にISO/IEC 27017の管理策を適用することによりクラウドサービスの情報セキュリティに確立・運用情報セキュリティマネジメントが定着していることを裏付ける認証制度です。ISMSクラウドセキュリティ認証の詳細については、6-1-2（4）で解説します。

また、個人情報を取り扱う業務を展開しているのであれば、個人情報保護のマネジメントの確立・維持を裏付けるプライバシーマークも重要な認証制度です。この他にも参考にできる認証制度も紹介してください。

第 4 章

クラウドサービスのセキュリティの要件

4-1 クラウドセキュリティの検討

Information security

履修目標

- 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」（以下「経済産業省ガイドライン」という。）の箇条5～15に何が記述されているか概要が説明できる。
- 経済産業省ガイドラインの管理策を自社の構成に合わせて対応付け編集できる。

標準学習時間 20～30分

※4-1-1～4-1-2は4-2-1と合わせて実施することを推奨します。4-1-1～4-1-2と4-2-1で45～50分の学習時間となります。

指導のポイント

4-1-1を説明するにあたり、講師はISO/IEC 27017（JIS Q 27017）を一読し、構成や記載内容を把握し、クラウドサービス固有の情報について説明してください。さらに、ISO/IEC 27017の箇条5～15及び附属書Aに記載された管理策の概要とそれらを用いて組織独自のセキュリティ要件に編集する方法を説明してください。

4-1-1（1）ISO/IEC 27017は2015年12月に制定されました（日本では2016年12月にJIS Q 27017として規格化）。ISO/IEC 27017の制定に際しては、日本が中心的な役割を果たしました。ISO/IEC 27017の管理策の原案になったのは経済産業省「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」です。

（2）ISO/IEC 27017の箇条4は、クラウドサービスの特徴である供給者関係やリスクについての解説及びこの規格の構成について記述されていますので理解の助けになります。箇条5～15に管理策が記載されていますが、ISO/IEC 27002の箇条5～15と対応しています。クラウドサービスであっても一般の管理策の適用で良い箇条については、ISO/IEC 27002の記述のままになっていて、特にクラウドサービス固有の対応が必要な管理策については、「実施の手引き」や「関連情報」が記述されています。また、ISO/IEC 27002の箇条では不足するクラウドサービス固有の管理策が附属書Aとして追記されています。

「実施の手引き」はクラウド利用者と事業者の両者に向けたガイドとなっています。本教科書はクラウド利用者のセキュリティ要件を定義することを主題にしていますが、クラウド事業者に確認すべき要件を検討するための参考になるため、クラウド事業者に向けた実施の手引きも一読し、自分なりに解釈しておくことが必要です。

（3）に記述した管理項目の編集方法は、例示であり、組織によってシステム管理の定義方法は異なるため、実際に勤務する先により管理分類がここでの説明と異なることに言及してください。

ISO/IEC 27017の箇条5～15及び附属書Aの管理策の並び順はそのままでは利用し難い場合があります。4-1-2（1）では、ISO/IEC 27017の管理策の箇条を4-1-1（3）に記述した管理項目に合わせて編集するために対応付けした表です。必ず対応表を作成しなければならないわけではありませんが、規格文書を自社の管理項目を適用する場合はこのような対応表を作っておくと管理策の漏れや見落としが防げます。

なお、4章では、3-1-2（1）に挙げた“利用”“開発・変更工程”に関する要件には触れていません。“利用”は業務フローの中で検討する事項であり、“開発・変更工程”は手順や手続きとして定義すべきことであるためです。しかし、PaaSやIaaSを利用する場合は“開発・変更工程”も考慮する必要があることを説明してください。。

4-2 クラウドセキュリティ要件

Information security

履修目標

- クラウドセキュリティ要件の各要件の「目的」「クラウド利用者が要件定義で検討すること」「クラウド事業者に確認する事項」の概要が説明できる。
- セキュリティ要件をチェックリストに編集できる。

標準学習時間 200～230分

※4-2-1は4-1-1～4-1-2と合わせて実施することを推奨します。4-2-1と4-1-1～4-1-2で45～50分の学習時間となります。

※4-2-2～4-2-4で45～50分の学習時間となります。

※4-2-5～4-2-7で45～50分の学習時間となります。

※4-2-8～4-2-10で45～50分の学習時間となります。

※4-2-11～4-2-14で45～50分の学習時間となります。

指導のポイント

4-2-2クラウドで利用する情報資産の特定と管理方針のポイントは以下の通りです。

・クラウド上で処理保存するデータを明らかにする。

・当該データの重要度を明らかにする。

・リスクアセスメントは当該データを対象に行う。（情報セキュリティで情報資産を洗い出す目的の一つがリスクアセスメントの対象を特定することにあります）

・リスクの算定ではデータ重要度を考慮する。

・リスクアセスメントの結果によりデータの開示範囲、利用範囲を決定する。

・データの重要度が認識できるようにラベリングやマーキングを行わなければ、重要度に合わせて期待通りの取り扱いをしてもらえない。

4-2-3装置のセキュリティのポイントは以下の通りです。

・装置のセキュリティとは設備を物理的、環境的脅威から保護すること。

・装置の破壊、持ち去り、装置の未許可接続、装置の未許可操作、装置内データ・プログラムの保護を行うために装置設置区画への侵入、覗き見、盗聴、災害の対策を行う。

・対策は“境界の設定”“境界内への入退制限”“入退および境界内活動の記録”が基本である。

・ここでは、ケーブルの保護、サポートシステム（電源、空調等）の保護も含めている。

・クラウド設備の保護は事業者の管理に依存するため、利用者が行えることはモニタリングが中心になる。
・廃棄されるクラウド設備内に利用者の資産（プログラムやデータ）が残留することも考慮し、設備の廃棄や再利用に際しての手順にも留意する。

講師は、入退室認証技術（暗証番号、ICカード認証、生体認証）についての基礎的な知識を持っておくことが望まれます。

4-2-4ネットワークのセキュリティのポイントは以下の通りです。

・ネットワークのセキュリティは、ネットワーク経由の侵入、伝送路上の盗聴、伝送路からのデータ流出、伝送遅延を防ぐことが目的になる。
・対策は “セグメント化”“セグメント間の伝送制限、伝送路制御”“伝送記録”が基本になる。
・ネットワークの仮想化による、物理環境と仮想環境の不整合が通信障害を招く。
・マルチテナント環境においては、他の利用者とのネットワーク環境の分離の方法は確認ポイントとなる。
・クラウド環境はネットワークへの依存度が高まることから、ネットワーク管理が重要である。ネットワークにおけるクラウド利用者、通信業者、クラウド事業者の責任分界点を理解し、各組織の責任範囲を明確にする。

講師は、制御装置（ファイアウォール、IDP）、経路制御装置（VLAN、Proxy）、監視装置（IDS/IPS）についての基礎的な知識を有しておくことが望まれます。

4-2-5アクセス制限のポイントは以下の通りです。

・アクセス制限は、セキュリティの基礎です。システム上のデータの窃取、流出、改ざん、消失、誤操作、利用不可を防ぐことが目的になる。
・対策は、本人認証によるアクセス制限が基本になる。
・アクセス権の見直しや利用者によるパスワード管理等、属人的な運用に依存する範囲が多い対策である。
・クラウド環境においては、他の利用者からの侵害、事業者からの侵害が利用者の関心事である。

講師は、本人認証技術（安全なパスワード、ICカード認証、ワンタイムパスワード、生体認証）についての基礎的な知識を基礎的な知識を持っておくことが望まれます。また、UNIX、Windowsのパーミッション（「読み込み」「書き込み」「実行」）の考え方を理解しておくことが望まれます。

4-2-6モニタリングのポイントは以下の通りです。

・自社が直接コントロールできないクラウド環境ではモニタリングは重要な要素である。
・モニタリングとは、各種記録に基づく状態管理のこと。監視もそれに含む。
・記録はコンピュータ、ネットワーク機器、監視カメラ等に残される。

・記録から何を読み取るのか、評価方法を事前に決めておく。
・記録データの権限者からの隔離。（権限の分離）
・クラウド事業者が利用する第三者が提供するサービスについてのモニタリングに留意する。

講師は、コンピュータ、ネットワーク機器にどのような記録が残されるかを概要で良いので把握しておくことが望まれます。また、いずれかのクラウドサービスをサンプルに、実際のクラウドからのアラートの内容やダッシュボード等で確認できる記録を見ておくことが望まれます。

4-2-7バックアップのポイントは以下の通りです。

・バックアップの責任範囲を知っておくこと。（利用者の責任、SaaS事業者の責任、PaaS、IaaS事業者の責任）
・クラウド上で取得されるバックアップ内容の把握。
・クラウドサービス側で付加したメタデータや生成した実行ファイル等の有無とそれらもバックアップ対象になるかを確認する。
・バックアップからの復旧手順と責任範囲。
・バックアップデータの保護。（アクセス制限、遠隔保存等）
・異なる事業者のクラウドサービスをバックアップ先にする構成も考えられる。

講師は、一般的なバックアップの概要（目的、内容、手法）を知っておくことが望まれます。また、データの実態がデータセンターやIaaSのストレージに存在する時、それらデータのバックアップが誰の責任で行われるのか、明らかにする必要があることを強調して説明してください。

4-2-8技術的脆弱性管理のポイントは以下の通りです。

・技術的脆弱性管理とはOSやプログラム、ネットワーク機器に存在するセキュリティホールの対策をいう。マルウェア対策も含む。
・アップデートやパッチ適用の、事業者と利用者の責任範囲を明確にする必要がある。
・クラウド側設備のアップデートが、利用者のプログラムに影響を与える可能性がある。場合によっては利用者のプログラムの動作が不安定になる。
・マルチテナントの場合、クラウド利用者によるクラウド環境への脆弱性検査（ペネトレーションテスト）が許可されないことがある。

講師は、アップデートやパッチの運用とマルウェア対策の基礎的な知識を持っておくことが望まれます。また、脆弱性検査（ペネトレーションテスト）の概要を知っておくことが望まれます。

4-2-9容量、パフォーマンス管理のポイントは以下の通りです。

・容量とはストレージの使用量と空き容量をいう。パフォーマンスはシステムの処理速度とネットワーク応答性をいう。
・ネットワークの応答性はSLAに記述されているケースが多い。

・クラウドコンピューティングにおけるシステムの処理能力の標準的想定方法等はまだ整理されていない。

講師は、いずれかのクラウドサービスをサンプルに、実際のクラウドのダッシュボード等で確認できる容量、パフォーマンスを見ておくことが望まれます。

4-2-10システム障害対応のポイントは以下の通りです。

・システム障害はクラウド側設備より利用者側設備の方に起因する可能性の方が高い。
・クラウド環境におけるシステム障害の対応は、切り分けから復旧まで事業者との連携が重要である。
・クラウド側設備で障害が発生した場合、どのようなタイミングでどのような警告が利用者に通知されるのか知っておく必要がある。
・障害復旧目標がSLAに明記されている場合がある。

講師は、3-2-2に挙げたインシデント事例を参考にクラウドにおける障害の要因等を把握しておくことが望まれます。ニュース等に注意し日々公表される障害の情報を知っておくことも必要です。また、クラウドに繋がらない等の事象が発生した時に、利用者側の切り分け手順を決めておくことの必要性を伝えてください。

4-2-11事業継続のポイントは以下の通りです。

・ここでは、システムの継続利用を確保するための冗長性と、クラウドを提供する事業者の事業継続を対象としている。
・事業継続を考える時、事業への影響度を考慮した最大許容停止時間を決定し、それを維持するための対策を適用する。
・ネットワークの依存度が大きいクラウド環境において、ネットワークの冗長化は重要である。利用者側で検討すべき冗長化対策は、利用者～事業者間の多重化とネットワーク機器の冗長化である。

講師は、回線の多重化、ネットワーク機器の冗長化について基礎的な知識を持っておくことが望まれます。また、いくつかの規約等を読み、事業者の都合でサービス提供を停止する条件の例を知っておく必要があります。

4-2-12クラウドサービス終了・解約の手続きのポイントは以下の通りです。

・クラウドサービスの終了・解約に際して、利用者が実装したプログラム、保存したデータ等を利用者側への回収できなければベンダロックインにつながる。
・クラウドサービスの終了・解約の条件や手続き、およびプログラム・データの回収について、サービス選定時に確認しておく必要がある。
・クラウドサービス側で付加したメタデータや生成した実行ファイル等の有無とそれらも回収対象になるかを確認する。

講師は、いくつかの規約等を読み、サービス終了・解約の手続きの例を知っておく必要があります。

4-2-13法令・契約上の責任のポイントは以下の通りです。

・グローバル展開しているクラウド環境において、利用者のプログラムやデータの実態がどの国に存在するか特定できないことに留意する。場合によっては事業者自身にも特定できない。

・他国にプログラムやデータが置かれている場合は、その国の法令の制約を受ける。

・特に、プライバシー保護関連法規、データ保護関連法規、暗号技術輸出入規制に注意する。

・捜査機関への協力で他利用者のデータと混在して自社のデータが差し押さえられる可能性がある。

講師は、代表的な国のプライバシー保護関連法規、データ保護関連法規、暗号技術輸出入規制について基礎的な知識を持っていることが望まれます。また、国内の代表的な業界ガイドラインについても基礎的な知識を持っていることが望まれます。

4-2-14チェックリストについて、講師は自分でいくつか作成してみてください。それにより4章の章末問題のバリエーションが作れます。

第 5 章

クラウドサービスのSLA、規約の解釈

5-1 セキュリティ要件と規約等の対応

Information security

履修目標

- セキュリティ要件とクラウドサービスのSLA、約款、規約等の対応付けができる。

標準学習時間 15～20分

※5-1-1は5-2-1と合わせて実施することを推奨します。5-1-1と5-2-1で45～50分の学習時間となります。

指導のポイント

5-1-1を理解するため、講師はいくつかの実際のクラウドサービスのSLAや規約等とセキュリティ要件の対応付けを試すことが望まれます。

5-2 クラウドサービス規約等の解釈

Information security

履修目標

- SLAの概念が説明できる。
- 月間非稼働率が算定できる。
- SLAを読んで責任分界点が説明できる。
- 規約等を読んでアカウント管理についての事業者と利用者の責任範囲が説明できる。
- 規約等を読んでデータ保護についての事業者と利用者の責任範囲が説明できる。
- 規約等を読んでプライバシー保護の対象範囲が説明できる。
- 規約等を読んでバックアップについての事業者と利用者の責任範囲が説明できる。
- 規約等を読んで事業者都合によるサービス停止の条件が説明できる。
- 規約等を読んでサービス解約手続きが説明できる。
- 規約等を読んでサービス終了・解約時のデータ回収および残留データ消去の条件が説明できる。
- 代表的な国のプライバシー保護関連法規、データ保護関連法規、暗号技術輸出入規制について説明できる。

標準学習時間 120～130分

※5-2-1は5-1-1と合わせて実施することを推奨します。5-2-1と5-1-1で45～50分の学習時間となります。

※5-2-2～5-2-5で45～50分の学習時間となります。

※5-2-6～5-2-8で45～50分の学習時間となります。

指導のポイント

5-1-2～5-1-8はサンプルであるため、講師はいくつかの実際のクラウドサービスのSLAや規約等を参照し、自分なりに解釈を試みてください。

4章のセキュリティ要件を想定した時、SLAや規約等から読み取れないことを洗い出し、事業者に何を確認すべきか検討してみてください。同様の検討を学生に試させることもできます。

月間稼働率の算定式から月間非稼働率を逆算し、想定した業務においてその非稼働率が許容できるか否かをシミュレーションして、指導の参考にしてください。

第 6 章

クラウドセキュリティの標準化等の動向

6-1 クラウドサービスのセキュリティガイドライン等

6-1 クラウドサービスのセキュリティガイドライン等

履修目標

- クラウドセキュリティに関する国内・国外の代表的な規格やガイドラインの概要が説明できる。
- クラウドサービスのセキュリティを裏付ける制度の動向が説明できる。

標準学習時間 45～50分

指導のポイント

6-1-1に挙げたガイドライン等は、クラウドセキュリティだけではなくクラウドコンピューティングやクラウドサービスの様々な面を定義し解説する文書です。講師は、各ガイドライン等を読み、その中でも特にセキュリティに関連する文章を理解することが望まれます。また、文書によって同じ事柄について異なった表現がされていることもあるため、文書間の差異についても注意を払う必要があります。利用者に向けた事項と事業者に向けた事項が明確ではない個所もあるので、自分なりに整理して理解する必要があります。

6-1-2は、クラウドサービスの安全性・信頼性を裏付けるための代表的な制度です。特に、認証制度は、クラウドサービス選定の目安として利用できます。

（1）は、クラウドサービスのセキュリティについての評価項目もありますが表面的な評価に留まっているため、安全性評価というよりサービス母体である事業者組織の健全性や信頼性を見る目的で利用すると良いでしょう。

（2）で紹介したSTARという制度は現時点（2014年2月）において、申請や審査は英語で実施されます。

（3）のクラウドセキュリティ監査制度は、2013年にパイロットが実施され、2014年に本格運用が始まりました。セキュリティに特化した制度であり、また、クラウドの事業体ではなくサービスのセキュリティを裏付ける制度であるため、クラウドサービス選定の目安に利用できます。

（4）は国際標準ISO/IEC 27017に基づく認証制度です。ISO/IEC 27001のマネジメントフレームワークを基盤にISO/IEC 27017の管理策が実装・運用されていることを審査し認証します。国内では、2016年8月に一般財団法人日本情報経済社会推進協会（JIPDEC）がISMSクラウドセキュリティ認証制度として認証が開始されました。クラウドに特化した範囲が対象となりますので、クラウドの事業体の情報セキュリティマネジメントやクラウド以外の一般的なシステムセキュリティについては従来のISMS制度を適用します。クラウド事業者がISMSクラウドセキュリティ認証を取得しようとするとき、適用範囲にクラウドサービスを含め、ISO/IEC27002だけではなくISO/IEC27017に記述されているクラウド固有の管理策を選択し適用しなければなりません。

おわりに

クラウドコンピューティングは変化し続けるパラダイムであり、技術です。この資料に示した様々な概念や定義、技術、サービスも非常に速いスピードで変化し続けることでしょう。それらの変化に対応できるようにするため、講義をする側は最新動向を把握しておくことが重要になります。

また、本資料はワールドワイドで提供されているベンダーニュートラルな認定試験である「CompTIA Cloud Essentials」及び「CompTIA Cloud+」の出題範囲を参照して作成されました。

より深い理解や、今後のクラウドコンピューティング関連技術の理解のために、これらの情報に触れておくこともよいでしょう。

〇CompTIA Cloud Essentials出題範囲

http://www.comptia.jp/pdf/CloudEssentials_jp_ver1.pdf

〇CompTIA Cloud+出題範囲

http://www.comptia.jp/pdf/cloudplus_jp_ver3.0_20131101.pdf

著作・制作　情報科学専門学校
編集責任　川上　隆　　柿本圭介
執筆者　**第1章～第2章**
長谷川　長一　株式会社ラック

第3章～第6章／ケーススタディ（別冊）
山田英史　株式会社ディアイティ

ケーススタディ（別冊）
吉田雄哉　一般社団法人クラウド利用推進機構

協力者（以下、氏名 50 音順）
植田　威　特定非営利活動法人 NPO 情報セキュリティフォーラム
宇津宮修二　札幌情報未来専門学校
金井　敦　法政大学
後藤厚宏　情報セキュリティ大学院大学
永宮直史　JASA- クラウドセキュリティ推進協議会
武藤幸一　情報科学専門学校
山崎展宏　専門学校穴吹コンピュータカレッジ

協力機関（以下、機関名 50 音順）
アマゾンユーザグループ横浜支部
一般社団法人神奈川県情報サービス産業協会
CompTIA 日本支局
独立行政法人情報処理推進機構（IPA）　技術本部セキュリティセンター
一般社団法人全国専門学校情報教育協会
ニッポンクラウドワーキンググループ

実践クラウドセキュリティ【学習指導要領】

平成 26 年3月（初版第一刷）

平成 27 年2月（改訂版第一刷）

Information security