クラウドセキュリティ概論受講報告

～全学技術センター専門技術研修～

○山田一成[A)]、大川 敏生[A)]

[A)] 共通基盤技術支援室　情報通信技術系

概要

クラウド環境を利用・構築する際のセキュリティ面での注意点を習得することを目的に、全学技術センター専門技術研修として、NEC マネジメントパートナー株式会社が開催する研修会「クラウドセキュリティ概論」に著者及び共著者の２名で受講する機会を得たのでその内容を報告する。

なお、本稿では、クラウドコンピューティングとは、「クラウドサービスを提供するためのシステム構成」のこととし、クラウドサービスとは「クラウドコンピューティングを利用して提供されるサービス」のこととする。

1　はじめに

研修は、次の日程で実施された。

研修日程

日　　時：平成 28 年 9 月 16 日（金）　AM 9:30 ～ PM 5:00

場　　所：大阪市中央区（松下 IMP ビル）

研修メニュー：

・クラウドセキュリティ概要

・クラウドセキュリティ ～利用者編～

・クラウドセキュリティ ～構築編～

・クラウド関連の法制度・ガイドライン

本稿では、研修メニューに従い、クラウドとして気をつけたい脅威や、利用者としてクラウドを利用する場合にクラウド事業者に対して確認する確認項目、提供者としてクラウドを提供する場合に必要な対策、およびクラウド関連の法制度やガイドラインを中心にまとめてみました。

2　クラウドセキュリティ概要

2.1　クラウドサービス

クラウドサービスのサービスモデルは一般的に表１のとおり 3 種類に分類される。

表１．サービスモデル

サービスモデル	概　　要	サービス（会社名）
SaaS	アプリケーションレイヤのサービスを提供	Google Apps(Google)など
PssS	ミドルウエアのサービスを提供	Microsoft Azure(Microsoft)など
IaaS	インフラストラクチャや OS の環境を提供	Amazon EC2(Amazon)など

クラウドサービスの提供モデルとしては、表２のとおり４種類に分類される。

表２．クラウド提供モデル

クラウド提供モデル	概　　要
プライベートクラウド	特定の組織のために単独で提供される。そして、当該組織あるいはサードパーティーにより管理され、自社運用型又は他社運用型で運用される。
コミュニティクラウド	いくつかの組織によって共有され、また、関心事を共有する特定のコミュニティのために提供される。そして、当該組織あるいはサードパーティーにより管理され、自社運用型又は他社運用型で運用される。
パブリッククラウド	不特定多数の人々や大規模な業界団体に提供され、対象となるクラウドサービスを販売する組織により所有される。
ハイブリッドクラウド	複数のクラウド提供モデルから2つ以上を組み合わせたもの。

2.2　クラウドセキュリティ

クラウド環境における脅威は次のとおり５種類に分類される。

① 外部からクラウド環境への攻撃

－＞例：DDos 攻撃など

② クラウド環境内部から他のクラウド利用者への攻撃

－＞例：内部犯など

③ クラウドを踏み台とした攻撃

－＞例：第三者がクラウドを踏み台とし、他を攻撃など

④ パスワード解析や暗号解読など

－＞例：コンピューティングパワーの悪用など

⑤ 攻撃以外の原因（停電、システム不具合など）でクラウドサービスが停止

－＞例：電柱が折れて停電となった

このうち、①～④に関しては、以下のように分類できる。

・クラウドへの攻撃・・・・・・①②

・クラウドを利用した攻撃・・・③④

クラウドセキュリティとして、サービスモデルや提供モデルを考慮し、これら①～⑤の脅威に備える必要がある。

3　クラウドセキュリティ～利用者編～

クラウドサービスのような外部サービスを利用する場合、サービスを提供する側のセキュリティ対策状況が重要となる。サービス利用前のクラウド事業者に対する確認項目は、SaaS,PaaS の場合、次のとおりである。

・データセンター自体のセキュリティ対策

－＞データセンター自体のセキュリティ対策が十分なものであるかを確認する。

① 物理的対策

－＞侵入、盗難、持込、災害、障害対策について確認する。

② 人的対策

－＞信頼できる運用者アサイン、管理、教育について確認する。

・構築システムの技術的対策

－＞システムの技術的対策が不可欠。システム面でのセキュリティ対策が十分なものであるかを確認する。

① ネットワーク

－＞暗号化、信頼性・品質について確認する。

② マルチテナント

－＞仮想化、マルチテナント間対策、シングルテナント対応について確認する。

③ サーバ

－＞サーバ要塞化について確認する。

④ アプリケーション

－＞パスワードポリシー設定について確認する。

⑤ データ

－＞暗号化、復元防止、分散処理、格納場所の確認について確認する。

⑥ ログ管理

－＞収集保管、定期監視・検知、時刻同期について確認する。

⑦ 脆弱性対策

－＞診断、最新脆弱性入手・ウイルス対策・改ざん検知について確認する。

⑧ バックアップ

－＞バックアップ、エキスポート、データ・媒体の安全対策について確認する。

・外部サービス事業者の適用的対策

－＞日々の運用、インシデント発生時の運用が適切なものである必要がある。各種運用が適切に行われている事を確認する。

① セキュリティポリシー

－＞セキュリティポリシーの開示がされているか確認する。

② インシデント対応

－＞連絡体制確立、ログ提供、立ち入り検査・監査対応について確認する。

③ 監査・認証・第三者評価

－＞ISMS,SAS70,WebTrust などの認証、第三者診断について確認する。

4　クラウドセキュリティ～構築編～

サービスを提供する側のセキュリティ対策としては、3. クラウドセキュリティ～利用者編～ にて記載した内容を利用者が求めてくる。その為には、

・技術的対策

・運用的対策

・情報開示指針

が必要である。

4.1　技術的対策

クラウドコンピューティングにおける技術的対策は、次の分類による対策が必要である。

① 仮想化機能 : サーバ、ストレージ、ネットワーク等の IT 資産について、物理的な性質や境界を取り除き、論理的な利用単位に変換して提供する機能。

－＞ハイパーバイザー型の利用が好ましい。

② プロビジョニング：ネットワーク設備やシステムリソース等を事前に準備しておき、ユーザの要求に応じてそれらを割り当てて迅速にサービスを提供する機能。

－＞リソースを効率的に利用することが可能である。

③ マイグレーション：アプリケーションやその動作に必要な環境を別のサーバに移行する機能。

－＞負荷の均一化を図ることが可能である。

④ 隔離：ある仮想マシンが使用するリソースを他の仮想マシンから利用されないようにする等、他のクラウド利用者とのリソース間でデータ・処理を混在させないようにする機能。

－＞情報漏洩の防止。

⑤ ユーザ認証：システム、アプリケーション等に対してユーザを識別認証し、正規のユーザであることを確認するための機能。

－＞内部犯、悪意を持ったクラウド利用者、及び第三者のクラウドサービスの不正利用を防止する。

⑥ アクセス制御：認証されたユーザやシステムに対して、リソースへのアクセス権を指定し、アクセス権に基づきリソースへのアクセスの可否を制御する機能。

－＞内部犯や第三者などの権限を持たないものによるクラウド利用者が所有する機密情報への不正アクセスを防止する。

⑦ ログ：ユーザが不正操作を行う、又は不正プログラムによりシステムが意図しない動作をする等の事象を検知するために、特定のイベントが発生した場合にその処理内容を記録する機能。

－＞問題の原因を追跡する。

⑧ 暗号通信：ネットワーク上を流れるデータを暗号化して通信を行う機能。

－＞内部犯や第三者によるクラウドサービス内の通信内容の盗聴を防止する。

⑨ データ暗号：文書や画像等のデータを決まった規則で変換する機能。

－＞内部犯、他のクラウド利用者、及び第三者によるクラウド利用者のデータの不正な読み取りを防止する。

⑩ データ完全消去：実データ領域に対して意味のない値を上書きすることで復元不可能な状態にする機能。

－＞ストレージ内に残存しているデータが内部犯や悪意を持ったクラウド利用者により復元されることを防止する。

⑪ バックアップ：障害等によるデータの喪失に備え、データのコピーを取って保存する機能。

－＞クラウド利用者のデータ喪失やクラウドサービスの運用停止を防止する。

⑫ 侵入検知：ネットワーク上への不正なアクセスの兆候を検知する機能。

－＞ファイヤーウオールや IPS を利用し、クラウドサービス、仮想マシンに対するアクセス制御を実施する。

4.2 運用的対策

クラウドコンピューティングにおける運用的対策は、次の分類による対策が必要である。

① アクセス管理：クラウド利用者やクラウド提供者による不正な操作を監視し、防ぐために行う。

－＞アカウントの不正利用などを予防、又は阻止する目的で行うアイデンティティ管理を行う。

② アプリケーション・セキュリティ：クラウドサービスを構成する各コンポーネントのセキュリティレベルを最適に保つために行う作業。

－＞脆弱性の有無を確認する作業や、パッチ・バージョン・構成管理を行う。

③ 可用性：クラウドサービスが稼働していることを正確に把握するための作業。

－＞システム稼働状況や負荷状況の監視を行う。

④ インシデントレスポンス：障害などのインシデントの発生前、発生中、発生後に行うべき作業。

－＞関係者への連絡、被害拡大の防止、原因の究明、及び復旧作業を行う。

⑤ 事業継続：クラウド利用者にとって重要な事業（業務）を中断しないこと、又は中断した場合でも早期に原状復帰するために行う作業。

－＞クラウド基盤への既存業務データの移行容易性の担保や各コンポーネントの代替管理、災害などの障害発生時のデータ保護のための作業を行う。

4.3　情報開示指針

クラウドコンピューティングにおける情報開示指針は、2011 年 4 月 IPA（独立行政法人情報処理推進機構）より「クラウド事業者による情報開示の参照ガイド」が公開されている。このガイドでは、以下のように開示項目を示している。

① 事業者の信頼性

－＞企業名、所在地、連絡先、創業の時期、クラウドサービスの開始時期・利用実績、販売代理店、制度にもとづいて開示される企業情報（情報セキュリティ監査報告書など）

② サービスの信頼性

－＞サービスの稼働状況・稼働率、計画停止や障害時の復旧に関する情報

③ セキュリティ対策

－＞システム、データ管理、ネットワーク、データセンターの運用に関するセキュリティ対策項目

④ 利用者サポート

－＞利用方法の説明書、ユーザマニュアル、サポート窓口の情報

⑤ 利用終了時のデータ保護

－＞利用終了時のデータの保存方法、保存できる形式、データの抹消についての保証

⑥ 契約条件の確認

－＞取引内容の規定

5　クラウド関連の法制度・ガイドライン

クラウド関連の法制度やガイドラインについては、次のとおりとなっている。

① データの保管場所

－＞国外でのデータ保存は現地の法制度の対象となる。

② 外国為替及び外国貿易法

－＞特定技術（国際的な平和及び安全の維持を妨げることになると認められるものとして政令で定める特定の種類の貨物の設計、製造又は使用に係わる技術）を内容とする情報の送信についても経済産業大臣の認可が必要となる。

③ 米国愛国者法

－＞米国内に存在するコンピュータであれば、そのコンピュータ上に保存されているデータに関して、米連邦捜査局等が調査権限を持つ。

④ EU データ保護指令

－＞欧州連合加盟国（EU）では、EU 内の住人の個人情報に関して、EU 保護指令が要求する十分なデータ保護レベルの水準を確保していない第三国へのデータ移動を禁止している。

⑤ 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

－＞総務省からガイドラインとして、災害時の非常時の対応における ASP・SaaS 事業者への要求事項が公開されている。要求事項は、監督官庁に対して法令に基づく資料を円滑に提出できるよう、ASP・SaaS サービスの提供に用いるアプリケーション、プラットホーム、サーバ・ストレージ等は国内法の適用が及ぶ場所に設置すること。となっている。

6　終わりに

今回、クラウドセキュリティ概論として、研修メニューに従いまとめてみましたが、2. クラウドセキュリティ概要では､クラウド環境における脅威として､｢外部からクラウド環境への攻撃｣のみだけではなく､｢クラウド環境内部から他のクラウド利用者への攻撃｣、さらには､｢クラウドを踏み台とした攻撃｣､｢攻撃以外の原因（停電など)｣など、ありとあらゆる脅威があることが分かった。

3. クラウドセキュリティ～利用者編～　では、サービス利用前のクラウド事業者に対する確認項目の中で、「セキュリティポリシーの開示がされているか確認する」がとても参考となった。

また、各クラウドサービスの提供者が提供する「性能等を評価するための項目とその値」を用いてクラウドサービスを比較判断している。

4. クラウドセキュリティ～構築編～ では、クラウド提供者として、技術的対策のみでなく、運用的対策や情報開示指針も重要であることが分かった。

最後に、本研修に参加の機会を与えて頂いた全学技術センターの皆様に感謝の意を表します。