アンラボ・セキュリティレター

Press Ahn

2019.5　Vol.65

クラウド環境の到来に備えよ

クラウド環境の到来に備えよ

IT環境の急速な変化と共に、最近はクラウド環境がトレンドとなっている。多くの企業がクラウド環境への移行を検討しているが、様々な理由により導入を躊躇う場合も多い。企業の懸念事項はクラウド専門人材の不足、コスト管理、セキュリティなどがある。昨年末 A社の DNS設定エラーによって発生したインシデントで、多くのサービスがストップしたケースもあり、クラウドサービスへの不安が高まったことも企業の悩みを深くさせている。

今回のコラムでは、韓国におけるクラウドサービスのコンプライアンス要件とセキュリティ脅威を分析し、クラウドサービスの利用者とサービス提供者の要件を反映したアンラボのクラウド情報保護コンサルティングを紹介する。

コンプライアンス観点のクラウドセキュリティ

韓国のクラウド関連主要法令には『クラウドコンピューティング発展と利用者保護に関する法律（略称：クラウドコンピューティング法）』と『クラウドコンピューティング発展と利用者保護に関する法律施行令（略称：クラウドコンピューティング法施行令）』がある。同法の行政規則としては、『クラウドコンピューティングサービスの情報保護に関する基準』と『クラウドコンピューティングサービス品質・性能に関する基準』がある。

区分	規制名称	主な内容
法令	クラウドコンピューティング発展及び利用者保護に関する法律と施行令	標準契約書の作成、インシデント通知、利用者情報保護などのサービス安全性確保に関する内容規定
行政規則	クラウドコンピューティングサービス情報保護に関する基準	クラウドサービスの信頼性を確保するための管理的、物理的、技術的な保護措置の内容規定
	クラウドコンピューティングサービス品質・性能に関する基準	クラウドサービスの品質・性能基準、品質測定方法及び手順内容規定

[表1] クラウドコンピューティング法及び行政規則の主な内容

クラウドコンピューティング法及び行政規則の主な内容では標準契約書の作成、インシデント通知、利用者の情報保護などのサービス安全性の確保に関して法令で定めており、サービス信頼性を確保するための保護措置の詳細内容とサービスの品質と性能基準、品質測定方法及び手順について行政規則で明示している。また、クラウド環境でもオンプレミス（On-premise）環境の情報保護の要求事項を遵守する必要があり、電子金融監督規定等の一部法令でクラウド関連の要件を追加で定めているため、業種別に関連法令の確認が必要だ。

区分	規制名称	主な内容
公共分野	クラウドコンピューティング発展及び利用者保護に関する法律と施行令	民間クラウドは、セキュリティ認証（IaaS、SaaS）を受けたサービスのみ利用可能 ※但し、安全保障、捜査・裁判、敏感な情報処理、若しくは個人情報影響評価対象は、民間クラウド利用不可
金融分野	電子金融監督規定	金融会社は、クラウドサービス提供者を対象に、健全性・安全性の評価後に情報保護委員会の審議及び金融監督院に報告
その他	医療法等の業種別関連法規	各業種別の関連法規の要件を遵守する 例）医療：バックアップ、可用性の確保、医療情報の暗号化、アクセス制御が必要

[表2] 業種別クラウド規制の主な内容

クラウド情報保護認証制度は、韓国国内認証の『クラウドサービスセキュリティ認証制』と、海外認証の『ISO27017/27018』、『CSA STAR』などがある。

認証	適用対象	特徴
クラウドサービスセキュリティ認証制度（CSAP）	クラウドサービスプロバイダー（IaaS、SaaS）	•公共機関にクラウドサービスを提供する民間クラウド事業者は義務 •金融分野のクラウドサービス自己評価で「クラウドサービスセキュリティ認証制度項目+金融部門の追加保護措置」を適用 •IaaSは14領域117項目、SaaSは13領域78項目で構成
ISO27017	クラウドサービスプロバイダー及び利用者（IaaS、PaaS、SaaS）	•クラウド情報保護のため、ISO27002にクラウドサービスに特化した実装ガイドラインと制御7項目を追加 •制御項目別のクラウドサービスプロバイダーと利用者の実装ガイド •14領域114項目で構成
ISO27018	クラウドサービスプロバイダー及び利用者（IaaS、PaaS、SaaS）	•クラウドの個人情報保護のために ISO27002と ISO2100をもとに作成 •クラウドの個人情報保護実装ガイドラインと個人情報ライフサイクル関連の拡張制御項目を追加 •14領域114項目で構成
CSA STAR	クラウドサービスプロバイダー及び利用者（IaaS、PaaS、SaaS）	•ステップ1-自己診断、ステップ2-3rdPartyで STAR認証成熟度評価、ステップ3-リアルタイム監視モデル実装の順序で進行 •IaaS、PaaS、SaaSの事業者別の項目を明示 •16領域133項目で構成

[表3] クラウド情報保護の認証制度

クラウドセキュリティの脅威

クラウド環境における主な脅威は管理者やスタッフのミスなど、インサイダー管理ミスが大半を占めた。また SWの脆弱性ハッキング、認証及び権限への脅威など、オンプレミス環境で発生するインシデントタイプとほぼ似ていた。クラウドセキュリティ脅威は従来の IT環境で発生したセキュリティ脅威が、クラウド環境でもそのまま継承されている部分と、クラウド環境の特性によって発生する脅威に区分することができる。

米国標準技術研究所（National Institute of Standards and Technology、NIST）、ガートナー（Gartner）、CSA（Cloud Security Alliance）などの関連機関で定義した従来のセキュリティ脅威とクラウドのセキュリティ脅威にまとめると次のようになる。

分類	脅威	関連機関					
		Gartner	RSA	CSA	NIST	ITU-UX.1601	ENSIA
既存の脅威	データ損失及び流出（データバックアップ管理、外付記憶装置管理、削除管理不十分）	○		○	○	○	○
	データ改ざん（データ暗号化及び鍵管理不十分）	○	○			○	○
	認証及び権限（ユーザーアカウント情報の流出、管理者権限の管理不十分）	○	○	○	○	○	○
	システム及びネットワークセキュリティの脆弱性（マルウェア、OSセキュリティの脆弱性、仮想ネットワーク脆弱性）		○	○	○	○	
	サービス障害（災害管理、クラウドサービスプロバイダの廃業と合併）	○	○		○	○	○
	インサイダー管理ミス（統合ポリシー管理不十分、法令及び規定の遵守不十分）	○	○	○	○	○	○
	システム悪用（クラウドリソースを活用したフィッシング、ボットネット悪用）	○	○	○			
クラウド固有のセキュリティ脅威	ハイパーバイザー脆弱性（脆弱なハイパーバイザーを活用VM被害）	○		○	○	○	
	VM内部攻撃（VM間のパケットスニッフィング、マルウェア拡散、内部領域の侵入検知が困難）	○		○	○	○	
	安全でないAPI（CSPで提供されたAPIに脆弱性が存在する場合、情報漏えい、サービス障害発生）			○	○	○	

* ITU-U X.1601 : International Telecommunication Union Telecommunication Standardization Sector国際電気通信連合の電気通信標準化部門。
X.1601は、ITU-Tで発行した『クラウドコンピューティング・セキュリティフレームワーク（Security framework doud computing）』標準文書。
* ENSIA : 欧州連合ネットワークと情報セキュリティ機構（European Union Agency for Network and Information Security）

[表4] 既存のセキュリティ脅威とクラウドセキュリティ脅威

クラウドサービスのインシデントケースと国内外の関連機関で定義された脅威をベースに選定したセキュリティ課題 Top5 は以下の通りだ。

1. **インサイダー管理ミス**

クラウド環境の運用プロセスを含む内部対策の確立及び関連業務担当者の役割を定義

2. **ユーザー認証とアクセス制御**

クラウドサービスの業務別アカウント及び権限管理ポリシーの適用とサービス別アクセス制御ポリシーの適用

3. **データ損失及び流出**

重要なデータの暗号化と定期的なバックアップ実行

4. **システム及びネットワーク脆弱性**

仮想サーバーのハードニングされた標準 OSの選択及び、サーバ、ネットワークなどの情報システムに対する技術的な保護対策を適用

5. **安全でないAPI**

APIの整合性を定期的にチェック及び監視強化

クラウドサービスの利用者観点

セキュリティ上の脅威が実際のインシデントに繋がるリスクを最小化するための利用者視点におけるチェックポイントを、サービスの導入段階と運用段階に分けて見てみよう。クラウドサービスの導入プロセスは、大きく状況分析、導入対象選定、分析/設計、サービス移管の段階で行われる。
導入段階ではオンプレミス環境との違いを区別して、安全なサービス運営のためのポリシーとクラウドサービスを担当する組織を構成する。

クラウドサービス導入時の主なチェックポイントは次の通りだ。

- 情報保護組織の再構成とR&R定義
  - 既存のITシステムの構築と運用からサービス運用を中心にシフト
- 情報保護方針策定
  - クラウドサービス運用の観点からポリシー改正及び関連法規に反映
- クラウドセキュリティ・アーキテクチャ確立
  - クラウド環境に必要とされるセキュリティ要素を識別してセキュリティアーキテクチャを確立
- クラウドサービスプロバイダとの契約管理
  - クラウドサービス標準契約書を作成して関連法規に反映

クラウドサービス構築の終了後、運用段階ではオンプレミス環境と同じ情報保護要件を適用する必要があり、加えて仮想リソース管理などのクラウド環境の特性に応じた要求事項を考慮する。クラウドサービス運用の際に考慮する点は次の通りだ。

- アクセス制御
  - クラウドサービスリソース管理アカウント及び VMサーバーOSアカウントの管理
  - ユーザー接続時に認証手順適用及び業務別の権限付与
- ネットワークセキュリティ
  - Security Groupなど CSPが提供するネットワークアクセス制御機能を活用してトラフィック制御
  - 通信区間の暗号化
- データ保護とバックアップ
  - 安全な暗号化アルゴリズムでデータ暗号化と鍵管理
  - データバックアップポリシーによる定期的バックアップ
- システム開発と導入
  - 新規システム設計時に監査証跡の確保などセキュリティ要件を反映
  - クラウドシステムの容量モニタリングで追加システム導入計画
- 仮想化
  - 仮想リソースの変更内容（修正、移動、削除、コピー）を監視
  - 仮想化実行履歴をスナップショットなどの画像形式で保存管理

クラウドサービスのプロバイダー観点

クラウドサービスプロバイダーが遵守するセキュリティ要件は、コンプライアンス要件と CSPセキュリティ要件に分類される。

コンプライアンスセキュリティ要件は、情報保護関連の法律準拠性の確保、CC認証取得などの既存オンプレミス環境と同じ要件が存在し、クラウドサービスのセキュリティ認証と同様のクラウド環境の特性に応じた要件がある。

CSPセキュリティ要件は、AWS、Azure、Google Cloud、IBM Cloudのような IaaSクラウド事業者マーケットに SaaSサービスなどを登録する場合に遵守しなければならない事項である。

AWSを例に挙げると『AWS Marketplace販売者ガイドライン』では次のセキュリティ要件に準拠するように定めている。

- 不要なサービスやプログラムは無効にするか削除
- ネットワークトラフィックにエンドツーエンド暗号化技術を適用
- Security Groupを使用してインスタンスの受信トラフィック制限
- 定期的な侵入テストを実行
- OWASP Top10 脆弱性に注意

コンプライアンス要件とCSPセキュリティ要件をもとに選定した、クラウドサービスプロバイダが遵守する主なセキュリティ事項は次の通りだ。

■ クラウドサービス開発などの運用前に考慮するポイント

- コンプライアンスセキュリティ要件を反映
- サービス関連資産の識別及び保護措置の適用
- ソースコード管理、運用環境の移管管理など開発セキュリティ強化
- システム及びソースコードの脆弱性診断の実行

■ クラウドサービス運営時に考慮するポイント

- インシデントの試みモニタリング
- 安全なアップデート及びメンテナンス対策
- インターフェイス及び APIの脆弱性を定期的に分析
- サービス継続性を確保すること

クラウド環境の特性による情報保護

市場調査会社 IDCの『クラウド及び AI導入に関する調査（2018 Cloud and AI Adoption Survey）』によると、アンケート回答者のうち「単一のクラウドを使用する」という回答は28%に過ぎず、ほとんどの回答者が「マルチクラウド（64 %）を使用する」、「ハイブリッドクラウド（7%）を使用する」と答えた。これらの結果は AWSのようなクラウドサービスプロバイダに対する依存から脱し、サービス可用性の確保、クラウドサービス提供企業別の技術特性の活用によるものと分析される。しかしハイブリッドやマルチクラウドを使用する場合、管理対象の区間が増えてしまう点によってセキュリティソリューションの構成とポリシー管理、統合監視などの課題が発生する。

ハイブリッドとマルチは、単一のパブリッククラウドをオンプレミスや他のパブリッククラウドと繋ぐ特徴があるため、ネットワークセキュリティ・ポリシー管理・モニタリングなどの共通のセキュリティ要件に加えて各環境の特性によるセキュリティ要件がある。

■ ハイブリッドクラウド及びマルチクラウドの共通セキュリティ要件

- VPN、専用線などのネットワーク区間の暗号化
- セキュリティソリューション統合管理対策が必要（異なる環境で同じ製品を使用することを推奨）
- 統合監視対策が必要

■ ハイブリッドクラウドのセキュリティ要件

- オンプレミス又はプライベート（Private）クラウドの網分離要件を満足

■ マルチクラウドのセキュリティ要件

- 複雑なクラウド管理を考慮したサービス配分

アンラボのクラウド情報保護コンサルティング

アンラボは前述した様々なセキュリティ脅威と要件に対応しながらクラウドサービスの安全性を確保するために**「C3（Cloud Compliance Consulting）サービス」**を提供している。C3サービスは「P（Privacy）」、「D（Diagnostic）」、「C（Compliance）」、「A（Assurance）」で構成されており、各項目で提供する内容は以下の通りである。

- **P（Privacy）**
  - 個人情報影響評価コンサルティング/ GDPR対応コンサルティング
  - 個人情報受託社実態チェックコンサルティング
  - 個人情報保護マスタープラン策定コンサルティング
- **D（Diagnostic）**
  - AWSなど CSP利用顧客の情報保護要件に対応する専門的なコンサルティングを提供
  - CSPと協力してクラウド環境に特化した応用情報保護コンサルティングを提供
- **C（Compliance）**
  - 主要情報通信インフラの脆弱性分析評価コンサルティング
  - 電子金融インフラ脆弱性分析評価コンサルティング
  - 金融会社クラウドサービス情報保護コンサルティング
- **A（Assurance）**
  - クラウド情報保護システム確立
  - クラウドセキュリティ認証/ ISO27017、ISO27018、CSA STAR認証
  - ISO27001、ISMS-Pなど

アンラボはオンプレミス環境に提供している情報保護コンサルティングをクラウド環境に最適化して提供し、クラウドサービスセキュリティ認証などのコンプライアンス遵守のためのコンサルティングサービスを提供している。特に、AWSなど CSPと協力してクラウド環境に特化した情報保護要件に関する専門コンサルティングサービスを提供する。

今回のコラムでは、クラウドサービスにおけるコンプライアンス・セキュリティ脅威・クラウドサービスの利用や提供企業、クラウド構成環境の観点からの情報保護要件を紹介した。クラウドは環境構成と対象サービスに応じて様々なセキュリティ要件が発生するため、クラウド環境への移行計画段階からセキュリティ要件を識別・対応してこそサービスの安全性を確保できる。特に多くの企業がハイブリッドやマルチクラウド環境を採用して様々なサービスを導入しており、管理ポイントも増加している。よって事前にクラウドサービスのを活用対策を明確に把握し、セキュリティ要件を識別してこそ安全なクラウドサービス環境を構築することができる。

アンラボはクラウド以前のステップから運用段階までお客様の様々なサービス運用環境に特化したC3（Cloud Compliance Consulting）サービスを提供しており、クラウド環境で発生するリスクを事前に特定・対応することで情報保護コンプライアンスなど、多様なセキュリティ上の懸念事項を解消することが期待されている。

http://jp.ahnlab.com/site/main.do

http://global.ahnlab.com/site/main.do

http://www.ahnlab.com/kr/site/main.do

アンラボとは

株式会社アンラボは、業界をリードする情報セキュリティソリューションの開発会社です。
1995年から弊社では情報セキュリティ分野におけるイノベーターとして最先端技術と高品質のサービスをご提供できるように努力を傾けてまいりました。今後もお客様のビジネス継続性をお守りし、安心できるIT環境づくりに貢献しながらセキュリティ業界の先駆者になれるよう邁進してまいります。
アンラボはデスクトップおよびサーバー、携帯電話、オンライントランザクション、ネットワークアプライアンスなど多岐にわたる総合セキュリティ製品のラインナップを揃えております。どの製品も世界トップクラスのセキュリティレベルを誇り、グローバル向けコンサルタントサービスを含む包括的なセキュリティサービスをお届け致します。

AhnLab

〒108-0014 東京都港区芝4丁目13- 2 田町フロントビル3階 | TEL: 03-6453-8315 (代)