SECURITY REPORT

2021 OCT

CyberFortress

このレポートは、株式会社サイバーフォートレスの独自の調査にて収集されたデータに基づき作成しています。

クラウドコンピューティングインシデント分析

01. 概要

新型コロナウィルスを機に始まった前例のない経済沈滞と不安定な国内・外のビジネス環境は産業全般に影響を及ぼしている。特にテレワークの需要急増がデジタル経済への移行の加速化と、経済・社会構造の大転換迎えることになった。こうしたパラダイムは柔軟なビジネス運用のためのITインフラ運用方法にも影響を及ぼしている。消費者及びお客に提供するサービスを運用するためのサーバ、ネットワーク、ストレージなどのITインフラは直接構成するオンプレミス(On-premise)環境から離れ、必要なだけ即時使用できる資源に対して費用を支払うクラウドへの移行が加速化されている。

オンプレイミス環境からクラウド環境への変化の理由は大きく便宜性、柔軟性、経済性などの向上がある。クラウドサービス環境はオンプレミス環境のように導入された情報資産を構築するための物理的な設置空間が必要なく、使用者が好きなだけ情報資産の増設と減少が簡単で、情報資産運用に必要な時間だけ起動し不要に所要される費用節減の効果がある。

そんなクラウドコンピューティング環境でも既存のオンプレミスの環境と類似したセキュリティインシデントは発生している。2018年11月にはAWSのソウルリージョン(Region)でEC2インスタンスが内部DNSサーバ設定エラーによって84分間DNS機能を使えなくなったインシデントが発生したり、2019年アメリカの大手銀行であるCapital OneではAWS(Amazon Web Service)に保存されていたお客の個人情報が漏出されるなど企業が運用するサービスの環境は変わってもセキュリティインシデントは相変わらず発生している。

このようにクラウドコンピューティング環境でもセキュリティインシデントが頻繁に発生している。インシデントを予防したり処理するためにはクラウドサービス提供業者と使用者はどのように対処すべきかについて説明したいと思う。

02. クラウドサービスの共有責任モデルとセキュリティ認証制度

1) クラウド環境に共有責任モデル

クラウドサービスは使用者が好きなサービスタイプを選択し、提供者がどのようなサービスモデルを提供するかによってサービスのクラウドコンピューティングモデルとクラウドサービスモデルとが区分される。

クラウドコンピューティングモデルはパブリッククラウド、コミュニティクラウド、プライベートクラウド、ハイブリッドクラウドなど総計4つで区分される。そしてクラウドサービスモデルはIaaS(Infrastructure-as-a-Service), PaaS(Platform-as-a-Service), SaaS(Software-as-a-Service)に区分されていて最近はサーバの直接管理がいらないサーバレス(Serverless)モデルであるFaaS(Function-as-a-Service)とBaaS(Backend-as-a-Service)のサービスモデルが存在する。

このようなクラウドサービスモデルは提供業者が管理すべきの資源と、使用者が管理すべき資源が区分され、区分された資源によって情報セキュリティ管理モデルの主体が分かれる、これを「責任共有モデル(Shared Responsibility Model)」と言う。使用者が管理すべきの資源が多いサービスのタイプはIaaSでOS、ミドルウェア、アプリケーション及びデータのような資源の管理が必要です。

クラウド提供業者が管理すべきの資源が多いサービスのタイプはSaaSで、提供業者はクラウドサービスから提供している多数のサービスに対して管理主体となる。

区分		IaaS (Infrastructure-as-a-Service)	PaaS (Platform-as-a-Service)	SaaS (Software-as-a-Service)
特徴		・拡張性が高く、自動化されたコンピューティングリソースを仮想化して提供 ・お客様にサーバ、ネットワーク、OS、ストレージなどを仮想化して提供、管理	・サービスは主に応用プログラムを開発、ときに必要なプラットフォーを提供 ・お客様にOS、ミドルウェア、ランタイムのようなソフトウェア作成のためのプラットフォームを仮想化して提供、管理	・使用者に提供されるソフトウェアを仮想化して提供 ・お客様の代わりにソフトウェアとデータを提供、管理
管理主体	提供業者	サーバ、ネットワーキング、仮想化及びストレージを管理	サーバ、ネットワーキング、仮想化及びストレージ、OS、ミドルウェアのような資源を管理	サーバ、ネットワーキング、仮想化及びストレージだけではなく、OS、ミドルウェア、アプリケーション、データのような資源を管理
	使用者	OS、ミドルウェア、アプリケーション及びデータのような資源を管理	データ、アプリケーションを管理	-

【▲ クラウドサービスモデルの特徴】

クラウドコンピューティングインシデント分析

2) クラウドセキュリティ認証制度

クラウドサービス提供業者とサービスの利用者は、クラウド環境の中で利用中の情報資産を安全に管理し運用するためには、認証機関が評価・認証するクラウドセキュリティ認証制度がある。

クラウドセキュリティ認証制度は国際認証制度と国内認証制度が存在する。
国内ではJIS Q 27001:2014(ISO/IEC 27001:2013)に基づくISMS(情報セキュリティマネジメントシステム)クラウドセキュリティ認証制度がある。

国際認証制度はISO 27017/27018とCSA STARが存在する。国際認証制度はクラウドサービスを提供する業者だけではなく使用者も適用される。

区分	適用対象	特徴
ISO 27017	クラウドサービス 提供者及び利用者 (IaaS, PaaS, SaaS)	・クラウド情報セキュリティのためにISO 27002にクラウドサービスに特化された具現指針と統制項目7つを追加 ・14の領域、114個の項目で構成
ISO 27018	クラウドサービス 提供者及び利用者 (IaaS, PaaS, SaaS)	・ ISO 27002から規定した制御装置に対した11個の具現指針を保安したガイドを提供 ・14の領域、114個の項目で構成
CSA STAR	クラウドサービス 提供者及び利用者 (IaaS, PaaS, SaaS)	・ 1段階自己診断、2段階サードパーティーからSTAR認証成熟度評価、3段階リアルタイムモニタリングモデル具現の順で進行 ・16の領域、133個の項目で構成

【▲ 国際クラウドセキュリティ認証制度】

クラウドコンピューティングインシデント分析

クラウドセキュリティ認証制度は企業の情報保護活動を体系的に遂行するように支援し、情報セキュリティインシデントを予防し、被害を最小化することができる。

しかし、このような認証制度を導入していなかったり、一部だけ規定して使用する場合、使用者がいくら気を付けていてもセキュリティインシデントは発生する。

このようなセキュリティインシデントに対処するために国際認証制度(ISO 27017)からは統制項目「16. 情報保護インシデント管理」から確認できる。

認証制度	統制分野	統制項目		認証類型		
				IaaS	PaaS	SaaS
ISO 27017	16. 情報保護インシデント管理	16.1. 情報保護インシデント管理及び改善	16.1.1 責任及び手順	○	○	○
			16.1.2 情報セキュリティインシデント報告	○	○	○
			16.1.3 情報セキュリティ脆弱性報告	○	○	○
			16.1.4情報セキュリティインシデントに対する評価及び決定	○	○	○
			16.1.5 情報セキュリティインシデント対応	○	○	○
			16.1.6 情報セキュリティインシデント学習	○	○	○
			16.1.7 証拠収集	○	○	○

【▲ クラウドセキュリティ認証制度セキュリティインシデント関連統制分野】

クラウドコンピューティングインシデント分析

03. クラウドインシデント分析段階

1) インシデント前の準備段階(Incident Response Preparations)

セキュリティインシデントが発生する場合、迅速で対処するためにインシデント対応の手順の確立が必須的である。一般的にインシデント対応の手順はインシデント前の準備段階、インシデント検知及び識別、エビデンス収集及び分析、レポート作成でオンプレミス環境とクラウド環境が同一であるとみられる。しかし、クラウド環境ではクラウドサービスのどのような技術を使用しているかによってデータの収集及び分析の可否が異なる。

クラウドサービス提供業者は多様な技術要素が求められている。その中で仮想化技術がは必ず要求され、大量のデータを分散処理したり、保存、管理でできる技術、ネットワーク環境を通じてサービスを利用したり情報共有をサポートするインターフェース技術、そして敏感な情報を外部環境に安全に保存したり保管する技術などが要求される。

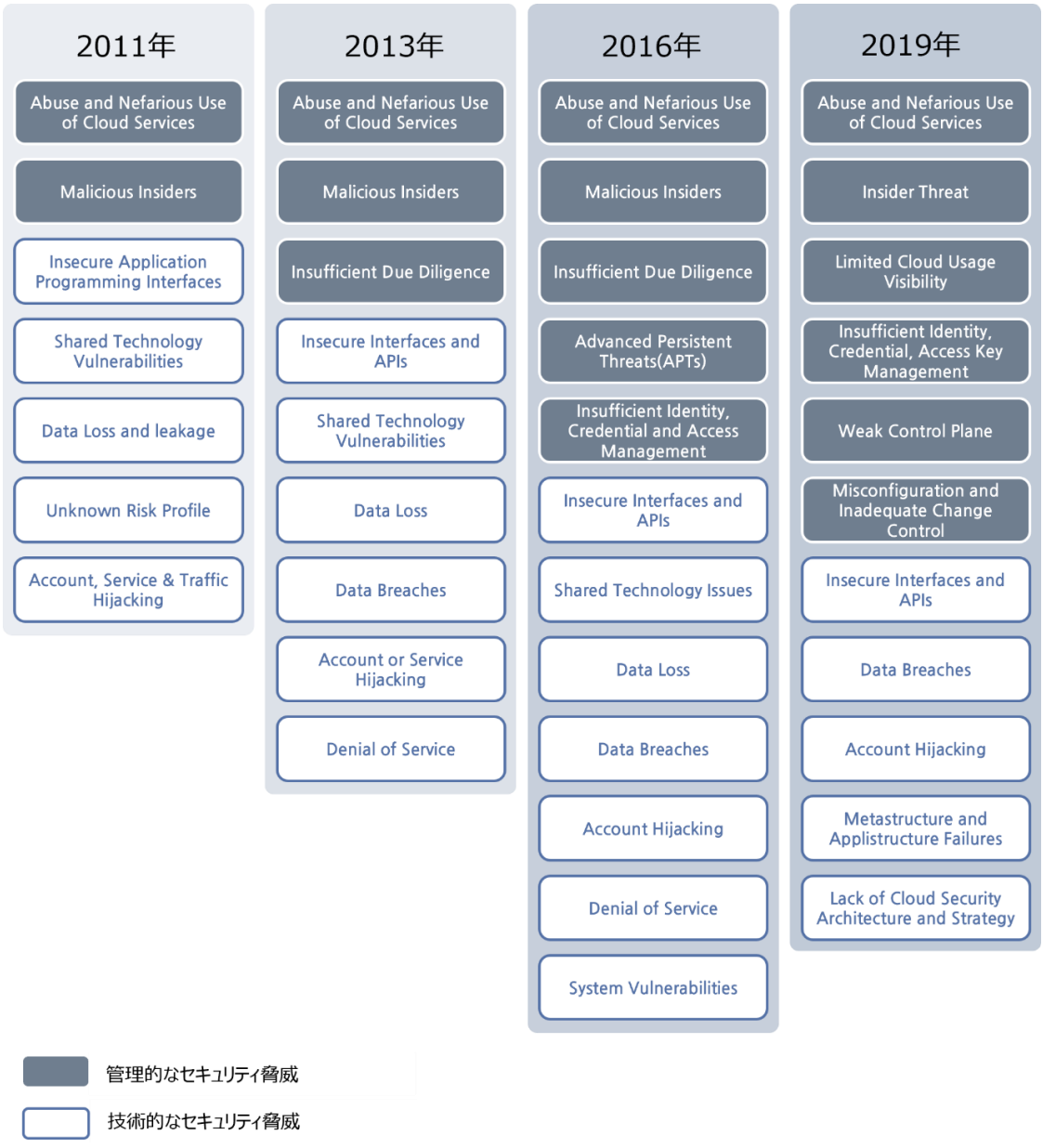
構成要素	技術要素
仮想化技術	・Resource Pool, Hypervisor(サーバ仮想化), Partition Mobility, VLAN, ストレージ仮想化など
大規模分散処理	・分散データ保存技術(CODA, Andrew, Apache, Hbase HyperTableなど)
オープンインターフェース	・SOA, Open API, Web Serviceなど
サービスプロビジョニング	・クラスター管理技術、プロビジョニング及びスケジューリングなど
資源ユーティリティ	・使用量測定、課金、ユーザーアカウント管理など
セキュリティ及び個人情報管理	・プラットフォームセキュリティ技術(DAC, MAC, RBACなど), ネットワークセキュリティ技術(SSL, IPSEC, VPN)、 端末セキュリティ技術(TPM, CryptoCellなど)

【▲ クラウドコンピューティング技術要素(参考：KOCCA)】

インシデントが発生する前に使用者はインシデント類型とインシデント定義、クラウドセキュリティ脅威などに対して整理する必要がある。インシデントは一般的に情報システムを使用していればどこでも不正アクセス、情報漏洩、マルウェア流布などのセキュリティインシデントが発生しうる。同じくクラウドコンピューティング環境から、使用者はクラウドサービスを利用する中で、第三者の悪意的な侵入またはクラウドサービス提供者・利用者のセキュリティ管理問題、多様な端末機器のアクセスなど様々なセキュリティ脅威が発しうる。

クラウドコンピューティングインシデント分析

このようなクラウドセキュリティ脅威はクラウドコンピューティングを使用する大勢の利用者が大容量のインフラを共有し、データを中央集中式で管理及びアクセスするために発生する。クラウドセキュリティ脅威は、クラウドセキュリティ協会(Cloud Security Alliance, CSA)から2年ごとにクラウドサービスを利用する業界従事者を対処にアンケート調査を行って2010年から持続的に発表している。その資料によるとクラウドサービス利用が増加することによって管理的・技術的セキュリティ脅威の範囲も次第に広がっている。

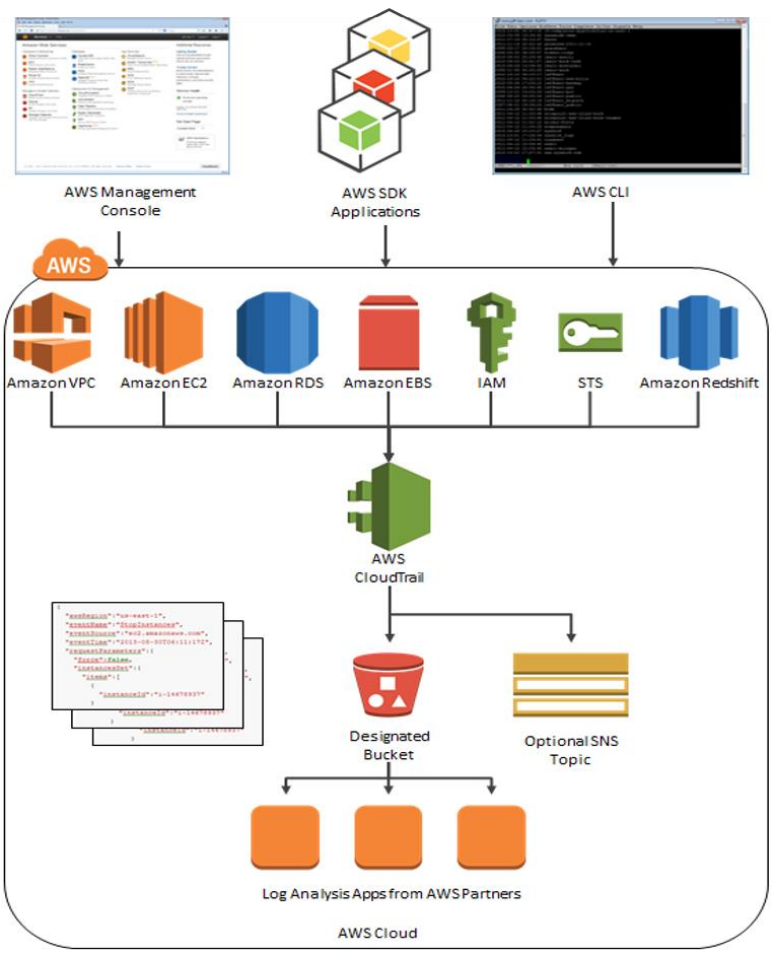


【▲ クラウドセキュリティ脅威要素(参考：Cloud Security Allianceセキュリティ脅威再構成)】

クラウドコンピューティングインシデント分析

このようなセキュリティ脅威に備えるためにクラウド使用者はセキュリティ設定の適用も重要だが、使用している主要システムのロギングと異常兆候のモニタリングが必要である。クラウド提供者は自主的にロギングとモニタリングサービスを提供しており、クラウドの市場占有率が一番高いAWSではAWS CloudTrailサービスとAWS CloudWatchサービスが主に使用される。

AWS CloudWatchはAWSのリソース及びアプリケーションに対してのモニタリングサービスであり、 AWS CloudTrailはAWS管理コンソール、AWS SDK Command lineツールとその他AWSサービスで実行されたものを含めた全てのAPI呼び出しに関するAWSアカウント活動を記録し、モニタリングすることができる。主なシステムロギングとモニタリングを円滑にするためには提供されたサービスのデフォルト設定はなく、セキュリティ設定を変更すると非認可行為やハッキング試しを検知することができる。



【▲ AWS CloudTrail Architecture(参考：Amazon Web Service)】

クラウドコンピューティングインシデント分析

セキュリティ変更の1番目は、すべてのリージョン(Region)に対しCloudTrailとAWS Configを有効化する必要がある。CloudTrailはAWSの全てのAPI呼び出しに対する履歴を残し、AWS Configはサービス設定の変更に対する履歴を保存しているため、すべてのリージョンから呼び出し及び作業履歴をロギングする必要がある。
2番目は、CloudTrailのログファイルを保存するS3 Bucketに対して認可されていない使用者がアクセスできないように変更が必要で、最後にCloudTrailのログファイルが改ざんできないように有効性チェックを有効化し、保存されるログは暗号化して保存されるように設定が必要である。

Category	推奨セキュリティ設定	説明
Logging	すべてのリージョン(Region)に CloudTrailを有効化する。	CloudTrailはAWSの全てのAPIの呼び出しに対する 全ての履歴を残すように設定する。
	CloudTrailのログファイルの 有効性チェックを有効化する。	ログファイルの整合性の確認のために 有効性チェックを有効化する。
	CloudTrailログを保存するS3 Bucket に対してPublicアクセスができないように 設定する。	保存されたログの整合性及び機密性のために Public権限が付与されないように設定する。
	すべてのリージョン(Region)に AWS Configを有効化する。	AWS Configはサービスの設定変更に対する履歴を 保管しており、監査及びイシュー分析のために保存する。
	CloudTrailログを保存するS3 Bucket に対してAccessログをEnableする。	Trailログのデータに対するアクセス履歴の確認のため Accessログを活用する。
	CloudTrailのTrailが CloudWatchログと 連携されるように設定する。	TrailのログはCloudWatchのようなモニタリングツールを利用してモニタリングされるべきで、SIEMから関連事項をモニタリングする場合は当該の設定を適用しない。
	KMS CMKを使用して CloudTrailログを保存する時 暗号化する。	CloudTrailログはSSE(サーバ側暗号化)及びKMS CMK(御客作成マスターキー)を活用してCloudTrailログを追加的に保護されるように構成することができ、SSE-KMSを使用してCloudTrailを構成する必要がある。

【▲ AWSサービス主要ロギング設定チェック項目(参考：CIS Benchmarks)】

クラウドコンピューティングインシデント分析

セキュリティ設定の適用が終わったら主要イベント項目に対してのモニタリングが必要である。モニタリングは上記で説明したAWS CloudTrailとCloudWatchサービスを活用して確認できる。サービスごとに記録されるイベントが存在するが、主に「認可されていない使用者によるAPI呼び出しによるアラート」、「rootアカウントモニタリング」、「IAMポリシー変更による情報アラート」、「AWSコンソールアクセス失敗によるアラート」などのように最高権限のアカウントのアクセス試しやポリシー変更などのようなイベントの確認が必要で、その他のモニタリングの推奨項目は下記になる。

Category	推奨モニタリング設定	説明
Monitoring	認可されていないAPI呼び出しに対する情報収取及びアラート	頻繁な認可されていないAPI呼び出しは悪意的なアクセス試しが疑われるため、臨界点を設定して担当者に知らせる。
	MFAを使用しないAWSコンソールログインに対する情報収集及びアラート	AWSコンソールのログイン時、追加認証(MFA)を使用するように推奨している。
	「root」アカウント使用に対する情報収取及びアラート	一般的な業務で「root」アカウント使用を推奨しないため「root」アカウントの使用に対してモニタリングが必要である。
	IAMポリシー変更に対する情報収取及びアラー	IAMポリシー変更で使用者のアクセス権限が変更される可能性があるため、ポリシー変更に対するモニタリングが必要である。
	CloudTrail設定変更に対する情報収取及びアラート	CloudTrailは全体API呼び出しに対する重要なログデータで無効化されないようにモニタリングが必要である。
	AWSコンソールアクセス失敗に対する情報収取及びアラート	認可されていないコンソールのアクセス失敗の発生回数によるアラート及び確認が必要である。
	S3 bucketポリシー変更に対する情報収取及びアラート	S3ポリシー変更時、データのアクセス権限が変更される可能性があるため確認が必要である。
	AWS Config設定変更に対する情報収取及びアラート	AWS Config設定変更によってAWSサービスの変更履歴が常時収取できるようにモニタリングが必要である
	Security group変更に対する情報収取及びアラート	ネットワークアクセスポリシー変更モニタリングが必要である

【▲ AWSサービス主要モニタリングチェック項目(参考：CIS Benchmarks)】

2) インシデント検知及び識別(Incident Detection and Identification)

インシデント検知はシステム及びネットワーク使用者、管理者によって検知される。侵入検知システム、ファイアウォールのようなセキュリティ機器からや、詳細な記録の確認から検知ができる。これはクラウドコンピューティング環境でも同一である。但し、クラウドコンピューティング環境は中央集中式で管理及びアクセスするため、攻撃の対象がサーバだけではなくクラウドサービスにアクセスするアカウントに対しても確認が必要である。

クラウドサービスを提供する業者はセキュリティ機器以外にも自主的にログを記録するサービスを提供している。

体表的なのが世界中一番使用されているクラウドサービスであるAWS(Amazon Web Service)からはAWS CloudTrailとCloudWatchサービスが提供されている。当該のサービスにで記録されるログを活用して異常兆候が検知できる。

インシデント異常兆候	Service	AWS CloudTrail EventName(API)
複数回のログイン失敗 期限切れ及びデフォルトアカウントへのログイン試し	Event	ConsoleLogin
管理者が作成していないアカウントの発見	IAM	CreateUser
説明できない権限変更	IAM	DeleteRolePolicy DeleteUserPolicy PutGroupPolicy PutRolePolicy PutUserPolicy
ログファイル・内容の削除	CloudTrail	DeleteTrail
	CloudWatch	DeleteLogStream DeleteLogGroup
	EC2	DeleteFlowLogs
サービス未提供時間の間のシステム活動	EC2	RunInstances StartInstances

【▲ AWS CloudTrail EventName】

クラウドコンピューティングインシデント分析

3) 証拠収集及び分析(Evidence Collection and Analysis)及びレポート作成(Reporting)

クラウドコンピューティング環境で異常兆候が発見された場合、これと関連するログを収集し、仮想環境の動作を中止したり、別途保存する必要がある。万が一クラウドサービスのログと被害システムの仮想環境を保存せずにそのまま動作することになると被害の規模や性格、インシデント原因の分析が難しく、2次、3次攻撃の経路として悪用され、利用するサービスの問題が発生する可能性が高い。

クラウド環境から運用中の情報システム(サーバ、データベース、セキュリティ機器など)は仮想環境から動作している。そのため、動作中の仮想環境を保存するために一時停止したりExport機能を利用して仮想イメージに変換してデータが変質しないように保存する必要がる。

AWS CloudTrailは使用者が利用したクラウドサービスログを保存している。当該サービスから確認できる詳細情報は時間、使用者、イベント名、ソースIPアドレスなどの情報が確認でき、90日間の管理イベントが記録されている、90日が過ぎたログは別途バックアップをしないと確認ができない。そのため、別途バックアップ環境を構築していないのであればAWS CloudTrailのダウンロード機能を利用して異常兆候のログを保存する必要がある。

最後に異常兆候が発見された時点の前後で収集・保存された、ログと環境を対象に分析を行った後、レポートの作成が必要である。レポート作成はオンプレミス環境のインシデントレポートと同様で、クラウドコンピューティング環境だけ確認できる内容を確認して事実関係を中心に作成すべきである。

04. 結論

クラウドコンピューティング環境への変化はゲーム、メディア産業企業を超えて一般企業と医療界、そして金融業界まで拡大されている。

クラウドコンピューティングの導入は単純に物理的な空間、初期設置費用の削減だけを考慮して導入するのではなく、なぜクラウドの導入が必要で、どこまで適用するべきかというのを工夫して正確な目標と方向性を設定するのが大事である。それによる管理的、物理的、技術的な対策方法を備えなければならない。

区分	処置事項
管理的対策	・情報保護専担組織を構成し、情報保護最高責任者を任命 ・情報保護政策及び政策施行文書の履歴管理手順を樹立 ・クラウドサービス導入による関連法律の規定の違背事項発生有無を把握し、処理 ・クラウドコンピューティングサービスの運用、開発など役職員を主要職務者と指定して管理 ・クラウドコンピューティングサービスで使用された資産の変更などが必要な場合セキュリティ影響評価を通じて変更 ・運用中のクラウドコンピューティングサービスがネットワーク障害で切断されないように持続的にモニタリング実施 ・インシデント手順確立及び発見された脆弱性を関連組織及び役職員と共有して処理
物理的対策	・重要情報及び情報処理施設を保護するためにセキュリティエリアの指定 ・物理的なセキュリティエリアに認可された人のみ入出 ・セキュリティエリアの出入り及び入出履歴を周期的に検討 ・外部機器の搬出入手順を確立し、記録及び管理
技術的対策	・仮想資源の変更(修正、移動、削除、コピー)に対してモニタリング実施 ・PC、無線端末などクラウドサービスにアクセスするIT資源を安全に管理 ・クラウドシステムアクセスに対する使用者認証、ログイン回数制限、使用者権限区分などセキュリティ設定適用 ・個人情報、企業の重要情報は事前に暗号化して保存管理 ・システムアカウント管理は安全なパスワード設定規則を適用して周期的に変更 ・クラウドサービス障害時、情報損失に備えて重要情報は定期的にバックアップ

【▲ クラウド情報保護管理的・物理的・技術的な対応方法】

クラウドコンピューティングインシデント分析

04. 結論

クラウドコンピューティング環境への変化はゲーム、メディア産業企業を超えて一般企業と医療界、そして金融業界まで拡大されている。

クラウドコンピューティングの導入は単純に物理的な空間、初期設置費用の削減だけを考慮して導入するのではなく、なぜクラウドの導入が必要で、どこまで適用するべきかというのを工夫して正確な目標と方向性を設定するのが大事である。それによる管理的、物理的、技術的な対策方法を備えなければならない。

区分	処置事項
管理的対策	・情報保護専担組織を構成し、情報保護最高責任者を任命 ・情報保護政策及び政策施行文書の履歴管理手順を樹立 ・クラウドサービス導入による関連法律の規定の違背事項発生有無を把握し、処理 ・クラウドコンピューティングサービスの運用、開発など役職員を主要職務者と指定して管理 ・クラウドコンピューティングサービスで使用された資産の変更などが必要な場合セキュリティ影響評価を通じて変更 ・運用中のクラウドコンピューティングサービスがネットワーク障害で切断されないように持続的にモニタリング実施 ・インシデント手順確立及び発見された脆弱性を関連組織及び役職員と共有して処理
物理的対策	・重要情報及び情報処理施設を保護するためにセキュリティエリアの指定 ・物理的なセキュリティエリアに認可された人のみ入出 ・セキュリティエリアの出入り及び入出履歴を周期的に検討 ・外部機器の搬出入手順を確立し、記録及び管理
技術的対策	・仮想資源の変更(修正、移動、削除、コピー)に対してモニタリング実施 ・PC、無線端末などクラウドサービスにアクセスするIT資源を安全に管理 ・クラウドシステムアクセスに対する使用者認証、ログイン回数制限、使用者権限区分などセキュリティ設定適用 ・個人情報、企業の重要情報は事前に暗号化して保存管理 ・システムアカウント管理は安全なパスワード設定規則を適用して周期的に変更 ・クラウドサービス障害時、情報損失に備えて重要情報は定期的にバックアップ

【▲ クラウド情報保護管理的・物理的・技術的な対応方法】

クラウドコンピューティングインシデント分析

最近までクラウドセキュリティインシデントはクラウド使用者の管理不備で発生し、代表的なものとしてクラウド環境にアクセスできるアカウントの設定や、ファイアウォールのようなセキュリティ機器に間違った設定などがあった。

クラウド環境を提供する業者が多様な機能とサービスを提供しても、これを使用者が上手く活用できないと意味がないので、使用者は提供されるセキュリティ機能とサービスを適切に活用してセキュリティインシデントが発生しないように努力する必要がある。

05. 参考資料

[1] 클라우드 보안 체계 수립 및 보안 모니터링 방안
(https://blog.lgcns.com/2134?category=604440)
[2] Global cloud services market Q1 2021
(https://www.canalys.com/newsroom/global-cloud-market-Q121?ctid=2048-939228c2c091da7d8a36c60eb59020ec)
[3] 클라우드 정보보호 안내서
(https://www.cisp.or.kr/wp-content/uploads/2019/12/%ED%81%B4%EB%9D%BC%EC%9A%B0%EB%93%9C-%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8-%EC%95%88%EB%82%B4%EC%84%9C-KISA-2017.pdf)
[4] Amazon Web Services:Overview of Security Processes
(https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf)
[5] 클라우드컴퓨팅서비스 정보보호에 관한 기준
https://www.law.go.kr/%ED%96%89%EC%A0%95%EA%B7%9C%EC%B9%99/%ED%81%B4%EB%9D%BC%EC%9A%B0%EB%93%9C%EC%BB%B4%ED%93%A8%ED%8C%85%EC%84%9C%EB%B9%84%EC%8A%A4%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8%EC%97%90%EA%B4%80%ED%95%9C%EA%B8%B0%EC%A4%80
[6] CIS Amazon Web Services Foundations
(https://d1.awsstatic.com/whitepapers/compliance/AWS_CIS_Foundations_Benchmark.pdf)