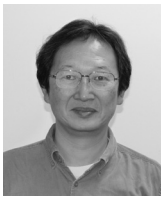
Amazon Web Servicesにおける監視・監査の管理手法

ICT営業本部
鹿谷　崇志

イノベーションビジネス本部
南雲　　仁

ICT営業本部
鈴木　成一


1. はじめに

1.1 IT環境の変遷

企業におけるITシステムは時代とともに進化を遂げてきており、今後も進化を続けることは容易に予測される。従来、ITサービスは必要なものは「作る」ことにより実現していた。その後、コモディティ化されたパッケージソフトウェアの出現により「買う」時代が到来した。さらに、ダウンサイジングやオープンシステム化、インターネットの普及を経て、現在は仮想化技術の進歩を背景とした「利用する」時代が到来している。

「作る」時代、「買う」時代において、提供されるITサービスはすべてシステム管理者の影響力の範囲内である自社設置またはデータセンターで提供されてきた。しかし、「利用する」時代のITサービスのホスト先は自社外が多数を占める傾向にある。また、この流れは今後さらに加速していく傾向が強く、企業ITには迅速に対応することが求められる。

1.2 オンプレミスとパブリッククラウドの違い

企業ITシステムにおけるオンプレミスとパブリッククラウドの違いについて表1−1に示す。

「利用する」時代においてはITシステムのホスト先としてはパブリッククラウドの利用が大きな割合を占めていくことになる。通常、企業がITシステムを構築する際には予算化された投資のもとサービスの拡充を行うが、パブリッククラウドでは企業の投資とは関係なく最新の技術、機能が随時拡充されている。利用する側にとっては少ない投資で新しい技術や機能を利用できる点は非常に魅力的である。

一方で、IT管理者がインフラ業務として対応する範囲は非常に狭くなる。自社でインフラ管理を行う場合には、ファシリティからアプリケーションまでIT管理者が自由に管理作業を行っていたが、パブリッククラウドでは複数の顧客が同居するホストOS部分をクラウドベンダーが管理する形態を取っているため、IT管理者が対応できる範囲が例外なくクラウドベンダーとの契約によって定められた非常に限定的な範囲となる。結果として、IT管理者は企業ITシステムの管理における責任範囲についての十分な理解が必要となる。

パブリッククラウドの活用においては、オンプレミスで実施してきた従来の管理手法とは異なる方法によって管理・運営することが求められる。

1.3 本稿のゴール

上述の通り、パブリッククラウドの導入には柔軟性や新技術・機能の活用など魅力的な側面がある一方、企業ITシステムにおける高い要件に適合した管理運営が行えるか不安を感じることも事実である。

本稿においてはパブリッククラウドサービス市場で圧倒的なシェアを誇るAmazon Web Services（以下、AWS）を利用した企業ITシステムの監視・監査における管理手法に焦点を当て、実証を行う。

表1-1　オンプレミスとパブリッククラウドの違い

#	名称	インフラ管理の主体	最新アーキテクチャ活用	課金体系の柔軟性	IT管理者の対応範囲
1	オンプレミス	自社	自社での調査・検証が必要	初期投資が必要	広い
2		ホスティングベンダー	ベンダーとの調整が必要		やや広い
3	パブリッククラウド	クラウドベンダー	新クラウドサービスとして利用が可能	従量課金によりスモールスタートが可能	狭い

2. 企業ITシステムの監視・監査

2.1 一般的な監視・監査対象

企業ITシステムにおける監視、監査の対象は広範囲にわたるケースがほとんどである。一般的な監視、監査対象について表2−1に示す。

2.2 オンプレミスとパブリッククラウドの監視・監査

オンプレミス上の企業ITシステムでは、上記の監視・監査項目に対する検討が必要であったが、パブリッククラウドを利用することにより、IT管理者による対応が必要な監視・監査項目に変化が生じている。オンプレミスとパブリッククラウドの監視・監査対象の違いについて表2−2に示す。

3. クラウドサービスの監視・監査

3.1 AWSにおける監視・監査機能

AWSのサービス提供が開始された当初は、AWSリソースの監視を行うためにオンプレミスのシステムと同様に、ゲストOSに監視エージェントを導入するなど、監視システムを構築する必要があった。

監査証跡（クラウドの構成変更、操作などの記録）に至っては、操作記録を取得する機能はなく、サポートへの問い合わせにより入手するといった状況が一般的であった。

しかし、ここ数年の間でAWSサービスのほとんどの監視項目（Metrics）の取得が可能となり、監査証跡に関しても、AWSサービスに対する操作/変更の履歴が記録できる機能が実装された。

このようにオンプレミスと同等以上の監視・監査の機能が装備されたことにより、現在では個人情報や機密情報を取り扱う企業ITシステムのクラウド利用拡大の一翼を担う状況となっている。

3.2 監視・監査機能の全体像

監視・監査の標準的な処理パターンについて、図3−1に示す。

表2-2　オンプレミスとパブリッククラウドの監視・監査対象の比較

#	監視・監査対象項目	オンプレミス	パブリッククラウド
1	ファシリティ	必要	不要 ※クラウドベンダーが対応
2	ネットワーク	必要	必要
3	ハードウェア	必要	不要 ※クラウドベンダーが対応
4-1	ホストOS	必要	不要 ※クラウドベンダーが対応
4-2	ゲストOS	必要	必要
5	ミドルウェア	必要	必要
6	アプリケーション	必要	必要
7	操作履歴	必要	必要

（1）ログ収集

ログ収集機能のほとんどは標準機能としてAWS管理コンソールから利用が可能である。例外として、ゲストOSのシステム、アプリケーションなどのログは、CloudWatch Logsエージェントを OSにインストールすることで、OS上のログが収集可能となる。

（2）保管

ログの保存先としては、S3ストレージへ保存するもの、CloudWatch Logsへ保存するもの、その両方を指定できるものに大分される。

（3）通知

CloudWatch Logsへ保管されたログは、Metrics Filterを定義しAlarm設定を行うことで、リアルタイムなログ監視を行うことができ、SNS経由でメール送信やアプリケーション連携が可能となっている。

あらかじめ用意されているAWSリソースの性能情報などの各種Metricsについても、Alarm設定を行うことで、同様のリアルタイム監視が可能となっている。

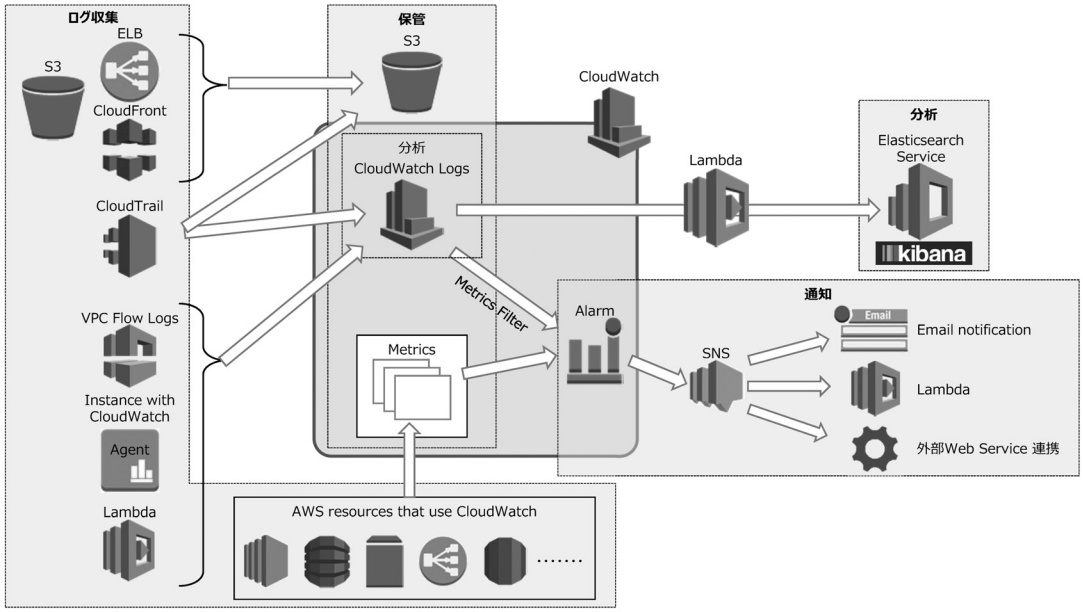
（4）分析

ログの長期的なトレンド分析やインシデント発生時のログの

表2-1　企業ITシステムにおける監視・監査対象

#	監視・監査対象項目	説明
1	ファシリティ	消費電力/温度の監視、入退室の管理
2	ネットワーク	ネットワークのスループット、不正パケットなどの監視
3	ハードウェア	ITシステムを構成する各種機器の監視
4	OS	OSが管理するプロセスの稼働状態・性能情報、出力ログなどの監視
5	ミドルウェア	各ミドルウェアのプロセスの稼働状態・性能情報、出力ログなどの監視
6	アプリケーション	アプリケーションのプロセス稼働状態、性能情報、出力ログなどの監視
7	操作履歴	アカウント管理、リソース操作の監視・管理

図3-1　標準的なログの処理パターン



監視・監査機能の処理は、大きく分けてログ収集、保管、通知、分析に分類できる。

調査には、多様なログを総合的に検索し、性能情報やイベントのトレンドをグラフ化するなど可視化にたけているElasticsearch Serviceを用いるのが効果的である。AWSでは、CloudWatch Logsに保管されたログを自動的にElasticsearch Serviceへ取り込むための処理コードのテンプレートとしてLambda Functionが提供されているため、容易に簡易な分析環境を構築することが可能となる。

図3−1の監視・監査を実現するためのAWSサービスについて、表3−1にまとめる。

3. 3 ログ収集機能を実行する主なAWSサービス

3. 3. 1 CloudTrail

AWSでは、クラウドサービスのすべての操作、設定、構成定義は、API経由で行う。

CloudTrailは、このAPIを通した操作に関しての記録を取るもので、AWS上のすべてのクラウドサービスに関する監査証跡を取得することが可能となっている。

CloudTrailは、S3およびCloudWatch Logsへ監査証跡を保存することができ、保存されたデータを基にリアルタイム通知や分析に利用することができる。

表3-1　AWSにおける監視・監査機能

#	機能	AWSサービス	説明
1	ログ収集	ELB	ELB(ロードバランサ)のアクセスログを収集
2		CloudFront	CloudFront(CDN)のアクセスログを収集
3		S3	S3へのサーバーアクセスに関するログを収集
4		CloudTrail	各種AWSサービスに対するAPIからのオペレーション記録を収集
5		VPC Flow Logs	VPCのネットワークインタフェースで発生するIPトラフィックに関する情報を収集 ※Firewallのログに相当
6		CloudWatch Logs Agent	イベントログ、Apache/IISなどのアクセスログ、アプリケーションログなどゲストOS上でテキスト形式で出力されるログを収集
7		Lambda	Lambda Functionに関するエラー出力、標準出力などのログを収集
8		CloudWatch(Metrics)	AWSの各種リソースのパフォーマンスデータ/キャパシティデータ/サービスステータスなどのデータをMetricsとして収集
9	保管	S3	ELB、CloudFront、S3、CloudTrailのログデータを保管
10		CloudWatch Logs	CloudTrail、VPC Flow Logs、CloudWatch Logs Agent、Lambdaで発生する各種ログを保管
11	検知	SNS	CloudWatch Logsに収集したデータから閾値を超えたデータを検知し、メール通知や次のアクションの実行などを行う
12	分析	CloudWatch Logs	簡易なログの確認、検索などで利用
13		Elasticsearch Service	パフォーマンスデータの傾向分析や総合的な特定文字列の確認などで利用

3. 3. 2 VPC Flow Logs

VPC上のEC2インスタンス(仮想サーバー)やクラウドサービスは、セキュリティグループ(ネットワーク接続許可ポリシー)によってEnd−To−Endで通信をきめ細かく制御することができる。これは、すべての仮想サーバー、サービスに各々ファイアウォールが用意されているような処理モデルとみなすことができる。VPC Flow Logは、セキュリティグループに従い、クラウド上のサービスの通信が許可されたか、拒否されたかを記録するものである。

VPC Flow Logsは、CloudWatch Logsへ収集されるので、通信拒否の件数や、重要なサービスへのアクセス件数などをMetrics Filterで定義することで、不正アクセスの兆候や、重要データへの不用意なアクセスなどをリアルタイムに監視することができる。また、Elasticsearch Serviceを用いることで、長期トレンドの分析や、他のログとの関連分析など行うことが可能である。

3. 3. 3 CloudWatch Logs Agent

EC2は仮想サーバーを提供するIaaSである。仮想サーバー上で稼働するOS、ミドルウェア(DBMS、Web Serverなど)、アプリケーションなどが出力するログは通常OS上のDISKに保管されるが、AWSで用意されたCloudWatch Logs Agentを用いることで、CloudWatch Logsへの収集が可能となる。CloudWatch Logs Agentでは、イベントログ(Windows)、テキスト形式のログファイル、CSV(カンマ区切り)のログファイルなどを取り込むことができる。VPC Flow Logと同様に、リアルタイムなログ監視や、Elasticsearch Serviceを用いた分析が可能である。

3. 3. 4 Lambda

Lambda FunctionはCloudWatch Logsへ直接ログを出力することが可能である。VPC Flow Logと同様に、リアルタイムなログ監視や、Elasticsearch Serviceを用いた分析が可能である。

CloudWatch Logs APIを用いたアプリケーションも同様にCloudWatch Logsへの出力が可能である。

3. 3. 5 CloudWatch(Metrics)

AWS上のほとんどのサービスには、多様なパフォーマンス情報を取得するためのCloudWatch Metricsが標準で提供されている。特定のパフォーマンス項目が閾値を超えた場合に通知メールを送るなどは、Alarm機能を用いることで簡単に実現することができる。

ただし、CloudWatch Metricsは、クラウドサービス内部のパフォーマンスデータであるため、例えば、エンドユーザー視点に立ったWebアプリケーションのレスポンスタイムの測定や、アプリケーションの正常性の確認などを直接行うことはできない。これらを監視するためにはオンプレミス環境で用いられてきた方法でもある、監視サーバーからの外部からの監視を行う必要がある。

3. 4 企業ITシステムへの適用

3. 4. 1 通知

企業環境に必要な通知機能は、サービス/サーバーの稼働状況の監視通知と、重要な構成要素の変更検知や、管理者アカウントのログイン検知などの監査通知がある。稼働状況の監視通知は、オンプレミスと同様にZabbixなどの監視ツールを導入し統合的に管理することが一般的だ。この場合でも、クラウド特有の監視項目(Metrics)を監視ツールに取り込むなどの連携が必要となる。

一方、監査通知に関してはクラウドならではの機能であり、クラウドの構成要素の変更/操作のすべてを記録することが可能であるため、監査ログにCloudWatch MetricsでAlarm設定することで、重要な構成要素への変更検知をリアルタイムで通知することが可能となる。オンプレミスではH/WやN/Wなどへの個々の構成変更を自動的に記録することは難しく、変更管理/構成管理手順で管理するにとどまっている。

通知の手段は、SNS機能を用いたE−Mailによる通知のほかに、Lambda/API Gatewayを組み合わせることで、電話通報(SaaS)との連携も可能となる。実際に検証した環境を図3−2に記す。

3. 4. 2 過去データの利用

企業環境においては、監査証跡(ログ)は長期間保管しておかなくてはならないことが多い。しかし、経済的な理由や検

表3-2 通知の一例

#	通知内容	ログソース	検知内容
1	セキュリティ設定の変更通知	Cloud Trail	セキュリティグループのルール変更 インスタンス、サービスへのセキュリティグループの設定/解除
2	データ持ち出し警戒	Cloud Trail	スナップショットからのEBS作成 スナップショットへのアクセス権の設定
3	不正アクセスの兆候	VPC Flow Log	Reject(通信拒否)回数の閾値超過
4	管理者ログインの監視	Cloud Trail	Rootアカウントの認証の監視

索/分析のパフォーマンスの理由から、CloudWatch Logsや Elasticsearch Serviceに長期保管することは現実的ではない。標準で提供されている処理パターンではElasticsearch Serviceに長期保管することになるが、今回はCloudWatch Logsから一旦S3(オブジェクトストア)へ保管し、そこから Elasticsearch Serviceへ取り込む処理パターンを検証した(図3−3)。

この処理パターンでは、S3上で長期保管を行う。S3には、ライフサイクル機能が備わっており、指定した期間を経過したファイルをより経済的なストレージへ自動的に移動したり削除することができる。また、分析ツールとして利用しているElasticsearch Serviceに関しても、分析対象期間分のデータを保管しておき、必要に応じてS3からデータを再投入することで、データ増によるパフォーマンス劣化を防ぐことができる。

3. 4. 3 リージョンを跨いだ監査

AWSは、世界中にクラウド拠点(リージョン)がありユーザーはどのリージョンでも利用可能である。グローバル企業の情報システムや、DRサイトの構築などの場合は、複数のリージョンを利用したシステム構成となることが一般的だ。このよう

図3-2　監査ログの電話通報検証イメージ

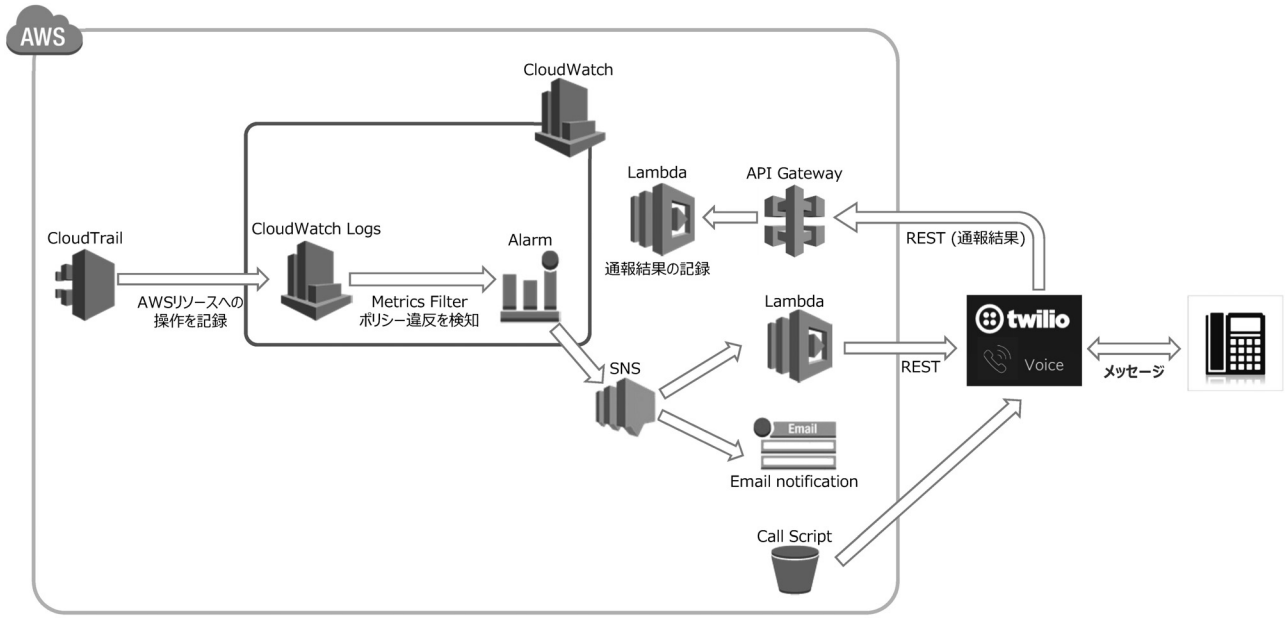


図3-3　監査ログの長期保管処理検証イメージ

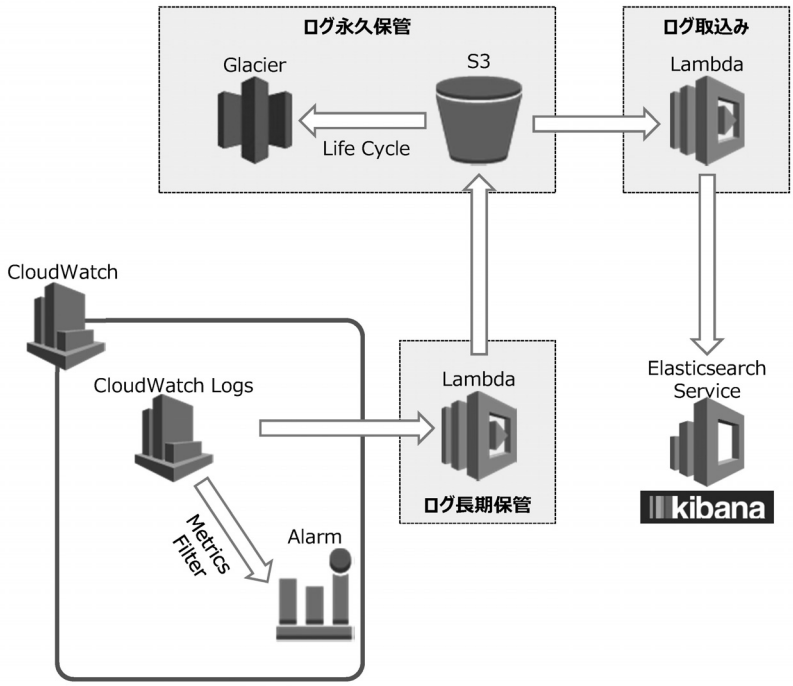
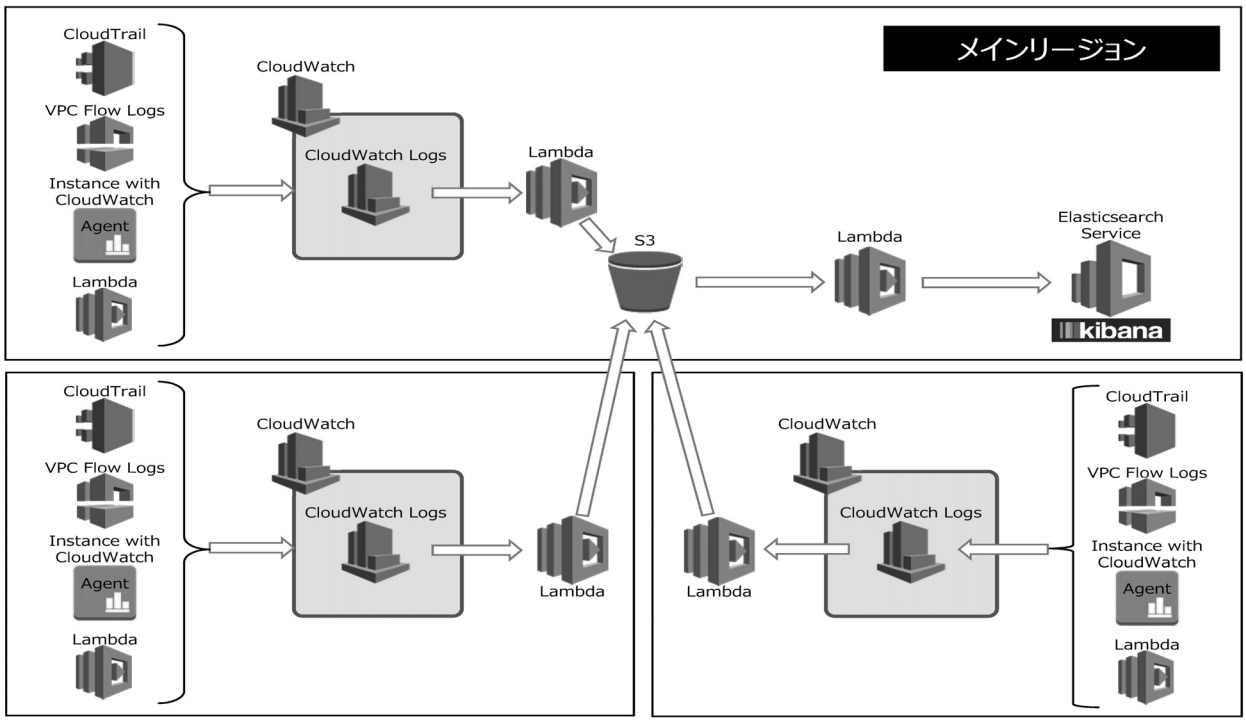


図3-4　リージョンを跨いだ監査ログの処理イメージ



なケースでは、監査ログを一か所に集中し統合的に分析可能な環境が求められる。この場合でも長期保管の処理モデルで検証したS3へのログ保管を応用し、メインリージョンのS3へログを集中し保管することが可能だ（図3−4）。

3. 4. 4 監査データの保全

企業環境においてもう一つ重要な項目が監査ログの保全である。監査ログの長期保管先として利用したS3には、バージョニング（オブジェクトの世代管理）機能があるため、ログの改ざんを行っても変更前のログを参照可能であり、改ざんに対しての耐性は高い。また、”Delete On MFA”機能を併用することで、S3オブジェクトの削除時に、指定されたMFA（スマートフォンまたは専用機器によるワンタイムパスワード生成装置）のパスワード入力が必要となる。このMFAを物理的に安全に管理（金庫に保管など）することで、S3に対して強力な権限を持っているアカウント（管理者など）による、監査ログの改ざん/削除を防ぐことができる。

4. まとめ

4. 1 AWSの監視・監査

本稿の目的であるAWSにおける監視・監査については、すべてのリソースに対して網羅的に「変更の証跡を出力するサービス（CloudTrail）」と「挙動のログを出力する各種サービス（CloudWatch、CloudWatch Logs Agent、ELB、CloudFrontなど）」が提供されていることを確認することができた。

また、網羅性とともに着目すべきはリソースに対して変更の証跡を出力するサービスの存在である。

オンプレミスのシステムで同様の機能を提供するためにはプログラム開発の際に要件の一部として開発を伴うことになるのに対して、AWSではフレームワークの中に機能が含まれているため、特に意識することなく高度な機能が提供される点は非常に大きなメリットである。

4. 2 今後の課題

4. 2. 1 監視の統合

本検証においては以下の観点から検証を行った。

- パブリッククラウドサービスの監視・監査の可能性についての検証
- 典型的な企業ITシステムにおいて、既存機能だけでは不足しているシナリオの検証

本稿の冒頭においても記載した通り、企業ITシステムは多様化している。その半面、多様性が増しても効率性を損なうことなくそれらを監視・監査することが求められる。現時点で想定されるIT基盤の監視・監査については、それらをどのように集約、統合するべきか検討する必要がある。以下に考慮すべき観点を挙げる。

- オンプレミスシステムとの監視統合
- 複数のパブリッククラウドの監視統合

監視の統合を行う際には監視結果データの親和性やデータそのもののセキュリティレベル、統合するためのデータの通信経路など様々な点を考慮する必要がある。その中で優先的に考慮すべきはシステム監視の集約先である。

稼働するシステムのサービスレベルはその特性によってさまざまであるが、システム監視はその中でも高いサービスレベルを求められる。

一般的にサービスレベルは投資する費用に応じて高くなる傾向にあり、オンプレミスに集約した場合は相応の初期投資が必要になり、構成の変更ごとに投資を行う必要性に迫られる。一方、クラウドサービスはもともと拠点災害を想定した構成となっているため、オンプレミスと同等のサービスレベルを実現しようとした場合は費用面で圧倒的に有利である。

一概にパブリッククラウドが集約先としての解ではないが、システム監視のサービスレベルを考えるとパブリッククラウドに統合することが多くのケースにおいて有効であると思われる。

4.2.2 必要に応じた各種ログの長期保管の考慮

今回、検証を行ったAWSで提供されるCloudWatch（Metrics）サービスでは、各種AWSリソースの使用状況の把握が可能である。しかし、提供された履歴は一定期間保存の後に削除される。長期間にわたって保持が必要となるリソースの履歴については既存機能を拡張し、データストア等に保持すべき項目である。要件に応じた対応になると思うが、監視・監査の観点においては実現することが望ましいと考える。

4.2.3 おわりに

パブリッククラウドはその機能や進化のスピードというこれまでに経験することのなかったメリットの反面、企業ITにとって提供するサービスレベルを保持するという副次的な問題が発生することは自明であるが、本検証を通じて、一定のレベルの監視・監査機能が提供され、必要な機能は開発することができる点を確認することができた。今後も継続して提供されていく新技術を採用し、企業ITシステムの糧とするためにはオンプレミス、パブリッククラウドの適切な組み合わせがより一層求められていくことは容易に想像できる。そのような潮流の中で本稿が一考に値することになれば幸いである。