Technology Reports（特集）
セキュリティ　クラウド　ガバナンス
パブリッククラウド活用特集

パブリッククラウドの利用に特化したセキュリティチェックツールの開発

イノベーション統括部　中村（なかむら）　拓哉（たくや）

世界中でパブリッククラウドの利用が加速する中，多くの企業がパブリッククラウドを利用して自社サービスや基幹システムのワークロードを実行している．パブリッククラウド上では，機密性の高い情報も扱われている場合があり，その際にセキュリティが非常に重要となる．

本稿では，パブリッククラウドを利用する上でのセキュリティに関する基本的な考え方について解説するとともに，ドコモにおける対策や取組みについて述べる．

1. まえがき

2021年現在，世界中の多くの企業がAWS（Amazon Web Services）[*1]やMicrosoft Azure[*2]（以下，Azure），GCP（Google Cloud Platform）[*3]などのパブリッククラウド[*4]を利用して，自社サービスや基幹システムのワークロード[*5]を実行している．パブリッククラウド上では，機密性の高い情報も扱われている場合があり，その際にセキュリティが非常に重要となる．

実際に，パブリッククラウドを利用して構築したシステムにおいて大規模な情報流出やサービスの停止などの情報事故が発生している．特に大規模な事例として，米国Capital One社がパブリッククラウド上に構築したシステムから1億人以上の個人情報が流出した事故［1］が注目を集めた．これらの事故の中には，パブリッククラウドを利用していたからこそ発生したものも多い．しかしながら，ビジネスを大きく加速させることができるなど，パブリッククラウドを利用することのメリットも数多く，もはや2021年現在において，セキュリティだけを理由にしてパブリッククラウドを利用しないという選択肢を取ることは，企業経営において適切ではないと考えられる．

ドコモでも，2009年ごろからパブリッククラウドを活用しており，2021年現在では数多くのワークロードをパブリッククラウド上で実行し，その間セキュリティに関するノウハウを蓄積してきた．本稿

＊1　AWS：Amazon Web Services社が提供するクラウドコンピューティングサービス．
＊2　Microsoft Azure：Microsoft社が提供するクラウドコンピューティングサービス．
＊3　GCP：Google社が提供するクラウドコンピューティングサービス．

では，パブリッククラウドを利用する上でのセキュリティに関する基本的な考え方について解説する．さらに，セキュリティ事故を起こさないためのドコモにおける対策や取組み事例について述べるとともに，取組みの中で開発したセキュリティチェックツール『ScanMonster』の特徴や構成について解説する．

2. クラウドセキュリティの考え方

パブリッククラウドが普及する以前は，自社でデータセンタやサーバを用意することが多かった．現在この方法はオンプレミスと呼ばれる．オンプレミスとパブリッククラウドの一番の違いは，オンプレミスでは目の前で見えるサーバを管理できていたことに対し，パブリッククラウドではデータセンタの存在すら我々から隠匿されてしまう点であろう．直接目に見えず，直接管理することもできないサーバ上に構築されたパブリッククラウドをうまく活用していく上で，非常に重要かつ基本的な考え方が，次に述べる責任共有モデルである（AWSの場合，文献［2］参照）．

2.1 責任共有モデル

パブリッククラウドでは，クラウド事業者がホストOSや仮想化レイヤからサービスが運用されている施設の物理的なセキュリティまで，さまざまなコンポーネントを運用，管理，統制している．これにより，利用者の運用上の負担が軽減するというメリットを提供しつつ，クラウド事業者はその提供の責任を負っている．

一方で，クラウド事業者がいくら対策を実施していたとしても，利用者側の設定次第では非常に危険な状態を作り出してしまう可能性がある．そのため，クラウド事業者とその利用者がそれぞれ責任を負う範囲を明確化して分担し，協力して対策を行っていく必要がある．このような考え方が責任共有モデルである．

パブリッククラウドにおける責任共有モデルでは，サービスの種類によって利用者およびクラウド事業者の責任範囲が異なる（**図1**）．IaaS（Infrastructure as a Service）[*6]と呼ばれる仮想マシン[*7]を提供するサービスであれば，クラウド事業者は主にデータセンタなどの物理的なファシリティから，物理マシンやネットワークなどのハードウェア，ホストOSや仮想化レイヤの管理までを実施する一方で，ゲストOSやその上で動作するアプリケーションは利用者側が責任をもって管理を行う必要がある．PaaS（Platform as a Service）[*8]やFaaS（Function as a Service）[*9]のようにマネージドサービス[*10]と呼ばれているサービスでは，利用者側が責任を負う範囲がより狭くなっており，多くの管理をクラウド事業者側に任せる事が可能である．このようなサービスを適宜利用していくことで，付加価値の高いアプリケーションやビジネス領域に集中して企業のリソースを投下することができる．

2.2 クラウド事業者評価

前述した責任共有モデルにおいて，利用者はクラウド事業者と責任を共有することになるため，逆に言うと責任の一部を任せなければならず，利用者はクラウド事業者が責任を全うできると信頼をする必要がある．しかし，本当にそのクラウド事業者が責任を共有する相手にふさわしいのであろうか．例えば，クラウド事業者が本当に安定的にサービスを提供できるのか，どのようにしてセキュリティを担保しているのか，あるいは利用者がパブリッククラウドへアップロードしたデータが内部で不正にアクセスされることがないだろうか，といった点が懸念される．では，信頼の置ける事業者かどうかをどのようにして評価すればよいのだろうか．

パブリッククラウドやクラウド事業者の評価方法

＊4 パブリッククラウド：インターネットを介して誰でも利用ができるクラウドコンピューティングサービス．
＊5 ワークロード：CPU使用率などのシステムの負荷の大きさを表す指標．特にパブリッククラウドの分野では，クラウド上で実行されるOSやアプリケーションコードなどを含めたシステム自体を表すこともある．本稿では後者の意味で用いる．
＊6 IaaS：サーバ，ネットワークなどのハードウェアを仮想的に貸し出すサービス．利用者は借りたサーバやネットワーク上にOSやアプリケーションソフトウェアを設定して利用する．
＊7 仮想マシン：ソフトウェアによって仮想的に構築されたサーバなどのコンピュータ．

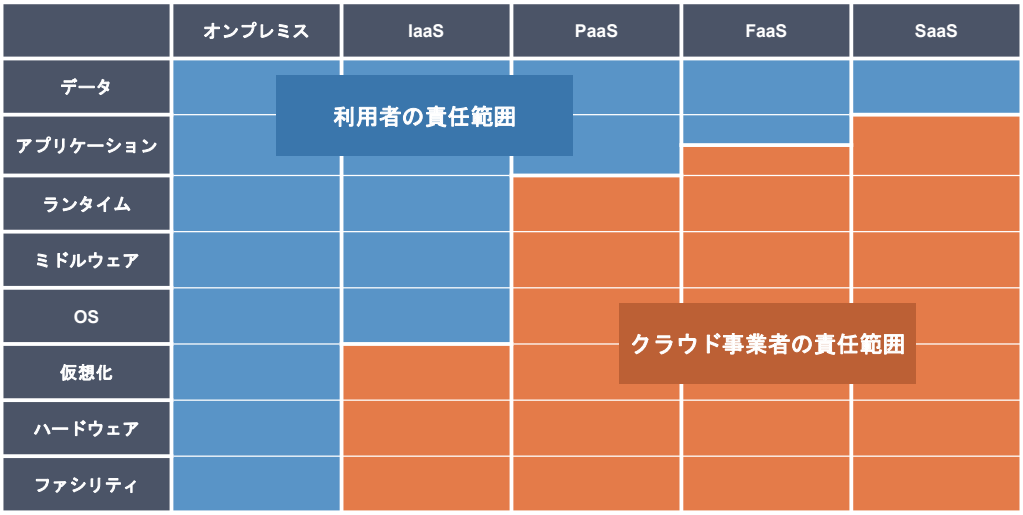

図1　パブリッククラウドのサービス種別ごとの責任範囲の違い

については，機能要件と非機能要件に大きく分けて考える必要がある．

機能要件については，クラウド事業者が提供するドキュメントやホワイトペーパー，サービスレベルアグリーメント（SLA：Service Level Agreement）*11を事前に確認することが非常に重要である．特にサービスの可用性やパフォーマンスといった項目は，ドキュメントに数値として明示的に記載されていることが多いため，具体的なシステム要件と照らし合わせて評価を行うことが可能である．

次に，非機能要件について評価する上で重要な判断材料として，公的機関による認定証や監査法人によるコンプライアンスレポートを活用することが有効である．これらの各種文書は，クラウド事業者が一般公開しているものもあれば，個別に秘密保持契約を結んで取得しなければならないものもある．多くのクラウド事業者は，下記のような国際機関による監査を受けており，その認証やレポートを入手することが可能である．

・ISO（International Organization for Standardization）*12 27017：2015 Certification
・PCI DSS（Payment Card Industry Data Security Standard）*13 AOC（Attestation of Compliance）*14 and Responsibility Summary
・SOC（Service Organization Controls）*15 2 Report

また，これらのレポートは，当該クラウド事業者が各種業界でのセキュリティ基準を満たしているかを判断するのにも役立つ．例えば，金融業界では公益財団法人金融情報システムセンター（FISC：The Center for Financial Industry Information Systems）によって安全対策基準が示されており，多くのクラウド事業者はこういった基準にどのように対応しているかという情報を公開している．

また，近年ではEUにおいて一般データ保護規則（GDPR：General Data Protection Regulation）が制定されたように，利用者のプライバシーを守るための法令の制定が活発である．これらの各地域や国で定められた法令を遵守したサービスをパブリック

＊8　PaaS：アプリケーションを実行するためのOSやミドルウェアを含むプラットフォームをクラウド上で貸し出すサービス．利用者は借りたプラットフォームの上でアプリケーションソフトウェアを作成して利用する．
＊9　FaaS：イベント駆動型のアプリケーション実行サービス．リソースの管理が不要のため，利用者はコードの記述に専念できる．一般的には実行時間に応じた課金モデルが採用されている．
＊10　マネージドサービス：クラウドサービスのうち，リソースのプロビジョニングや運用の大半をクラウド事業者の責任で実施しているサービス．クラウドコンピューティングサービスのうち，特にPaaSやSaaSを指す．

クラウド上で実装するために，パブリッククラウドでは物理的なデータセンタを，一般的にリージョンと呼ばれる国や地域ごとに分離し，それぞれのデータセンタにおいてサービスを提供している．これにより，データレジデンシー＊16を明確化できるとともに，各国や地域において求められる法令遵守要件に応じてサービスをカスタマイズして提供することが可能となっている．

2.3 利用者側での対策

パブリッククラウドにおける利用者側の対策は，基本的にはオンプレミスで行っていた対策と同様のものが求められる．例えば，ソフトウェアに内在する脆弱性の管理や通信の暗号化を行うなどの対策はもちろんのこと，IaaSを利用する上ではゲストOSのセキュリティパッチを管理することや，ネットワークレベルでの攻撃を防ぐためにファイアウォールを設定することなどが必要である．

ところで，パブリッククラウドのメリットは，物理的なデータセンタやサーバの保守運用をクラウド事業者に任せられることだけなのであろうか．パブリッククラウドがここまで広く使われるようになった大きな要因に，PaaSと呼ばれるプラットフォームを提供する形態が挙げられる．PaaSであれば，IaaSで必要だった利用者側でのOSの管理も不要となる．さらに，PaaSの中でも特にFaaSと呼ばれるコードのみを管理する形態では，利用者側はミドルウェア＊17の管理からも開放される．このように，オンプレミス（やIaaS）と比較して利用者が管理する部分が減少することは，セキュリティ対策として利用者が分担しなければならない責任が減少したことを意味する．つまり，PaaSやFaaSを活用すること自体が利用者側のセキュリティリスクを軽減させる効果がある．

逆に，クラウドならではのインシデント事例もある．クラウドではすべてのインフラストラクチャ＊18はソフトウェア化されている．これまではサーバルームへ入室し，LANケーブルを抜き差ししなければ外部ネットワークと繋がらなかったものが，ボタンの押下1つで簡単に公開できてしまうようになったのである．このように，保守用の端末からボタン1つでインフラストラクチャを素早く大胆に変更できるようになったことはビジネス上の優位点となるが，一方でセキュリティにおいては大きな懸念となる．

クラウド事業者は，利用者の責任領域におけるセキュリティ対策に有用なサービスをいくつも提供している．例えば，AWSはAWS Well Architected フレームワーク＊19というベストプラクティス集を公開している．また，AWS Trusted AdvisorやAWS Security Hubのように，利用者の責任領域において，ベストプラクティスに則ったかたちでシステムが運用されているかどうかをチェックするツールを活用することが非常に重要となっている．

3. ドコモにおけるセキュリティ統制

ここでは，ドコモにおけるセキュリティ統制の考え方や体制について述べる．

3.1 セキュリティ統制の体制

クラウドを利用する上でのセキュリティ統制の体制は**図2**のようなものとなっている．本図の情報セキュリティ部とは，セキュリティポリシーを作成・管理し，また，各システムがそのセキュリティポリシーを満たしたものかどうかを審査し，助言を行う全社的な組織である．

ドコモでは，通信ネットワークを構成する設備や通信サービスを提供する設備を自社で多く保有しており，また，これら以外にも依然として多くのワークロードをオンプレミス上で実行している．これらワークロードの実行に対しては，セキュリティ事故を避けるため厳格なセキュリティポリシーが適用さ

＊11 サービスレベルアグリーメント（SLA）：提供するサービスの品質保証．
＊12 ISO：国際標準化機構．情報技術分野の標準化を行う組織であり，電気および電気通信分野を除く全産業分野に関する国際規格を作成する．
＊13 PCI DSS：クレジットカード利用者の会員情報や取引情報を保護するために策定されたセキュリティ基準．
＊14 AOC：準拠証明書．PCI-DSSに準拠していることを示す証明書．
＊15 SOC：米国公認会計士協会により策定されたセキュリティ基準．System＆Organization Controlとも言う．
＊16 データレジデンシー：データの保管場所．

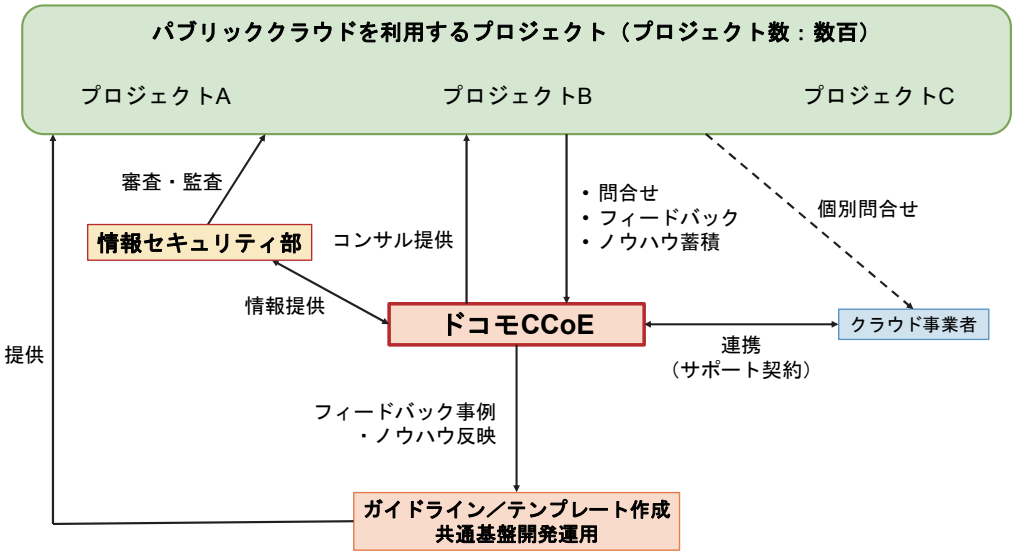

図2　ドコモ社内のクラウド統制の体制

れている．ただし，セキュリティポリシーはパブリッククラウドを利用したことにより緩和されるものではなく，パブリッククラウドを利用するかどうかに関係なく社内で構築されるすべてのシステムを対象として制定された一般的なものとなっている．そこで，パブリッククラウドの利用にあたっても，責任共有モデルなど特有の仕組みを理解し，その特性に応じたセキュリティ対策が必要とされるようになっている．

3.2　CCoEの役割と課題

前述のように，パブリッククラウドを利用する上で特有の考え方や対策を実施する必要性がある．そこでドコモでは，CCoE（Cloud Center of Excellence）というクラウド利用の支援に特化した部隊を発足させ，情報セキュリティ部へ情報提供を行うとともに，各プロジェクトに対してノウハウを提供したり，アーキテクチャやセキュリティに関するコンサルティングを行ったりしている．

しかしながら，パブリッククラウドを利用したシステムやプロジェクトの数は近年急速に拡大してきており，CCoEがすべてのシステムの構成を把握することが困難となってきた．また，パブリッククラウドを利用することの目的の1つとして，ビジネスを加速させることが挙げられるが，情報セキュリティ部やCCoEの統制強化が，各プロジェクトがサービスをいち早く市場に投入し，短いサイクルで機能を追加・改修していくことを阻害してしまう．したがって，ビジネス要件とシステム構成を各プロジェクトメンバが自身で把握し，セキュリティのリスクを自主的に判断する必要が出てきた．

そこで，CCoEから提供しているのが，ノウハウ集であるドコモ・クラウドパッケージとセキュリティチェックツールのScanMonsterである．

なお，CCoEの取組みについては本特集別記事を参照されたい［3］．

＊17 ミドルウェア：複数のアプリケーションから共通に利用される機能を提供するソフトウェア．
＊18 インフラストラクチャ：アプリケーションを実行するのに必要な物理的もしくは仮想的なデータセンタやサーバ，ネットワークなどの総称．
＊19 AWS Well Architected フレームワーク：AWSが公開している設計や運用に関するベストプラクティス．

4. 可視化とチェックツールの提供

各プロジェクトの開発者は，プロジェクトの開始にあたって，まずはドコモ・クラウドパッケージを用いてパブリッククラウド特有のノウハウを習得し，それを活用してシステムを構築する．しかし，各プロジェクトに対してヒアリングすると，「どのノウハウを適用すればよいのか分からない」「構築後にポリシーを満たせているかどうかがわからない」という声が多く聞かれた．このような課題に対して，CCoEではAWS環境を自動アセスメントするツール「ScanMonster」を開発した．

4.1 ScanMonsterの機能

ScanMonsterでは，AWS環境に対する70項目以上のアセスメントを実行することができる．アセスメント項目は，ドコモ・クラウドパッケージに記載されている内容や，CIS（Center for Internet Security）Benchmark*20，AWS Well Architected フレームワークなどいくつかの指標を参考に作成されている．例えば，「Root Account MFA」というアセスメント項目では，ルートユーザ*21に対してMFA（Multi-Factor Authentication）*22が設定されていないAWSアカウントをチェックすることができる．チェック結果を利用して，利用者はMFAが設定されていないルートユーザに対して設定を促すといった取組みが可能となる．また，「ACM Validation Method」は，AWS Certificate Manager*23において証明書発行時のドメイン検証に，DNS（Domain Name System）*24が利用されているかどうかを監査するためのアセスメント項目である．これはドコモ・クラウドパッケージへ記載している内容が基となっており，ドコモでのパブリッククラウド活用ノウハウを活かしたオリジナルの項目である．

ScanMonsterのアセスメント実行画面を**図3**に示す．利用者は，アセスメント項目を任意に選択し，ボタンを押すことでアセスメントを実行することができる．結果は「○」または「×」の2値で示され，利用者はひと目でアセスメント結果を判別できる．複数のアセスメント項目，または，すべてのアセス

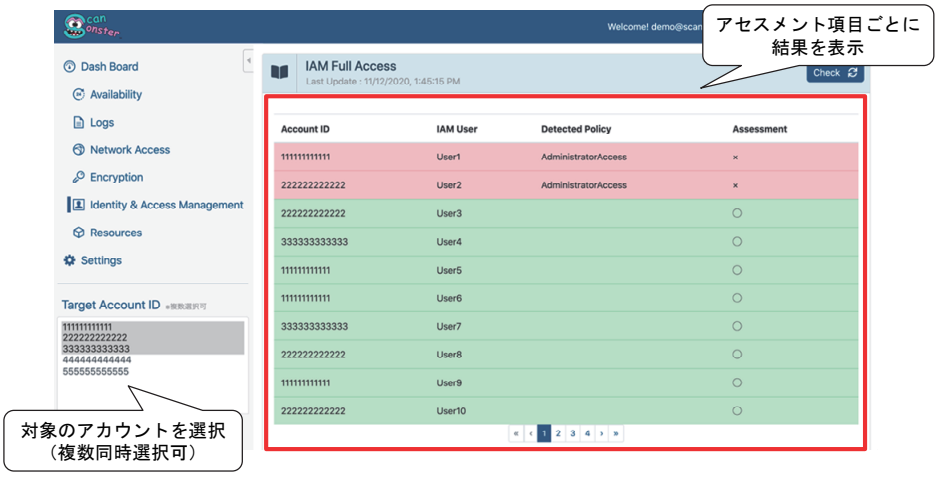

図3　ScanMonsterのアセスメント実行画面イメージ

＊20 CIS Benchmark：米CISが策定しているセキュリティ基準．
＊21 ルートユーザ：AWSアカウントへの完全なアクセスをもつアイデンティティ．MFAを設定して厳重に保護することがベストプラクティスとされている．
＊22 MFA：多要素認証．複数の種類の要素により本人確認を行う認証方式．
＊23 AWS Certificate Manager：AWSサービスで利用するSSL/TLS証明書を簡易に発行し管理できるサービス．
＊24 DNS：インターネット上でドメイン名とIPアドレスの対応付けを管理し，相互に変換するサービスを提供する仕組み．

メント項目を同時に実行することも可能である．また，ユーザごとにあらかじめ設定されたアセスメント可能なAWSアカウントのうちから，複数のアカウントを選択して同時にアセスメントを実行することも可能である．

多くのアセスメント項目には，それが何を目的としたものか，アセスメントがOK/NGとなる条件，アセスメントをOKとするための対応手順などを記載したチュートリアルを用意している．ScanMonsterにおけるチュートリアルの表示画面を**図4**に示す．AWSに不慣れな利用者であっても，チュートリアルを読むことでアセスメント結果の理解と，ビジネス上のリスクの見積もり，対応を実施するかの判断が容易に行える．

4.2 ScanMonsterの構成

(1)サーバレスアーキテクチャの採用

ScanMonsterは，**図5**に示すようにそれ自体がAWS上で構築されている．また，構成要素にはAmazon EC2などのIaaS製品を使用せず，AWS Lambda[*25]やAmazon S3[*26]，Amazon DynamoDB[*27]，Amazon Cognito[*28]，Amazon CloudFront[*29]，AWS WAF（Web Application Firewall）[*30]といったサービスを採用してサーバレスの構成とした．

サーバレス構成としたことにより，2つの大きな特長が生まれた．

1つ目は，サーバレスの名前が示すとおりで，インフラストラクチャの管理が不要であるという点である．すべてのサービスがマネージドサービスであるため，サーバの死活監視や負荷に応じたプロビジョニング[*31]が不要である．

2つ目は，運用コストが非常に安価という点である．利用時間による料金が発生するのは，フロントエンドのデータを格納したAmazon S3とエンドポイントのアクセス制御のためのAWS WAF，ユーザの管理とアクセス許可のためのAmazon Cognitoのみである．AWS LambdaとAmazon DynamoDBについては，アセスメントを実行した際にのみ利用料が課金されるため，ScanMonsterを利用中でもアセスメントを行っていない期間，あるいは夜間など誰

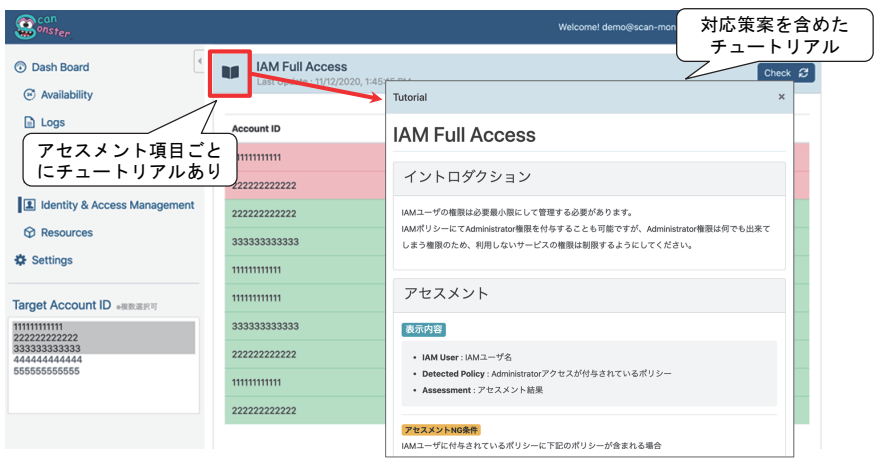

図4　ScanMonsterのチュートリアル表示画面イメージ

＊25 AWS Lambda：AWSが提供するPaaSの1つ．アプリケーションコードの実行環境が提供されており，利用者は作成したソースコードを登録してアプリケーションが実行できる．

＊26 Amazon S3：AWSが提供するオブジェクトストレージサービス．99.999999999％のデータ耐久性を実現するように設計されている．

＊27 Amazon DynamoDB：AWSが提供するNoSQLデータベースサービスの1つ．多量のリクエストを低遅延で処理可能なように設計されている．

＊28 Amazon Cognito：AWSが提供するPaaSの1つ．ウェブアプリケーションやモバイルアプリケーションに対して認証や認可，ユーザ管理機能を提供する．

もScanMonsterへアクセスしていない時間帯などは一切利用料がかからない．ドコモでの月当りのコストの実績は，数十円から数百円となっている（**図6**）．

(2)クロスアカウントアクセスによる複数AWSアカウントへのアセスメント

複数のAWSアカウントへの同時アセスメントは，IAM（Identity and Access Management）ロール*32

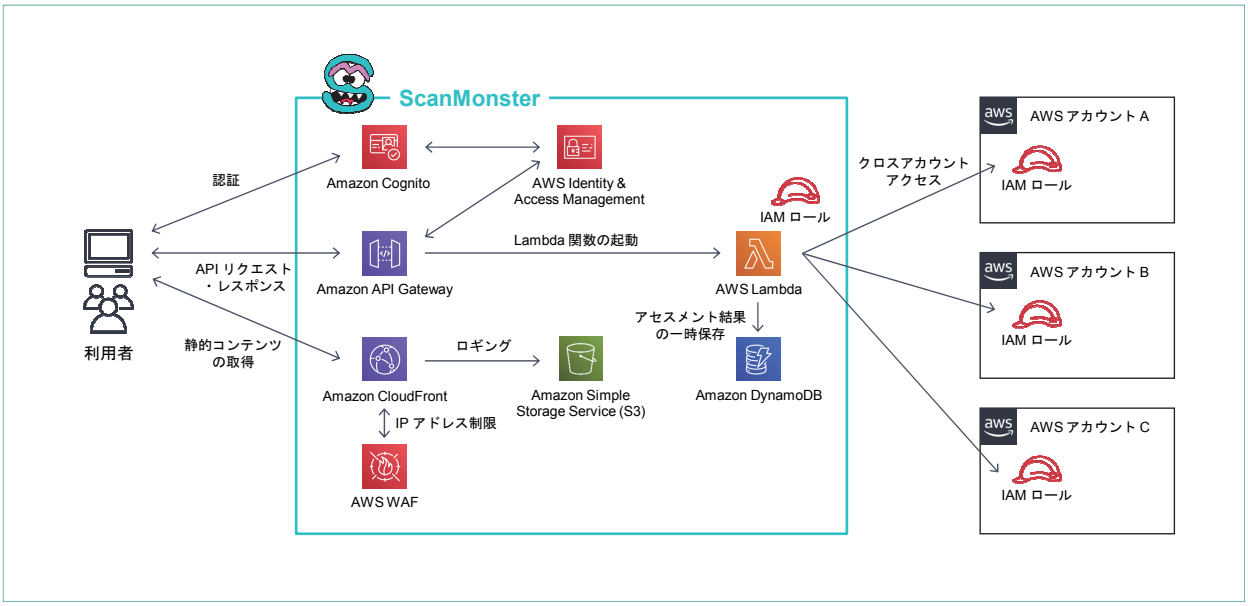

図5　ScanMonsterのアーキテクチャ図

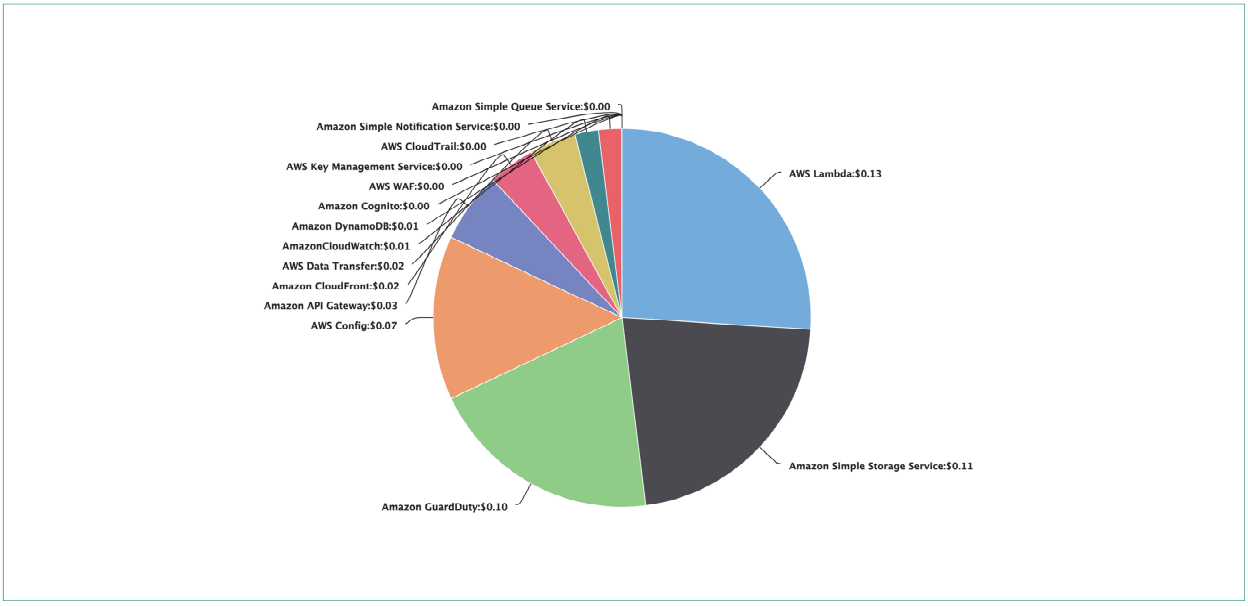

図6　ScanMonsterのコスト実績図

*29 Amazon CloudFront：AWSが提供するCDN（Content Delivery Network，コンテンツ配信ネットワーク）サービス．

*30 AWS WAF：AWSが提供するWebアプリケーション向けのファイアウォールサービス．

*31 プロビジョニング：アプリケーションを実行するために必要となるサーバやネットワークなどのリソースの確保やそれらを動作させるための各種設定作業．

*32 IAMロール：AWSにおけるアイデンティティリソースの1つ．任意の許可されたユーザ，アプリケーション，サービスなどにAWSリソースに対するアクセス権限を委任するために利用する．

の引受けによるクロスアカウントアクセスを利用している．アセスメント対象のAWSアカウント内に，ScanMonsterをデプロイしたAWSアカウントを信頼するIAMロールを設定することにより，ScanMonsterへのアクセス許可を行う．これにより，明示的にアクセス許可を与えたAWSアカウントのみがアセスメントを受け入れることを担保している．IAMロールの権限はアセスメントの実行に必要最低限の読取り権限のみとし，ScanMonsterをデプロイしたAWSアカウントからの不正な攻撃を防止している．さらに，ScanMonster内でもAmazon Cognitoのユーザを管理することで，利用者ごとにアセスメントが可能なAWSアカウントを設定することが可能である．

⑶IaC（Infrastructure as Code）＊33による簡易なScanMonsterデプロイ

また，ScanMonsterは構成されるすべてのAWSリソースをAWS CloudFormation＊34のテンプレートで記述しており，瞬時にScanMonsterをデプロイすることが可能である．これにより，アプリケーション開発時のテストや品質管理に，ScanMonsterの新しい環境を都度自動的に作成することが可能となっている．また，ScanMonsterは社外のお客様向けにも提供している製品であるが，この特長によりお客様自身の保有するAWSアカウント内にScanMonsterを簡単にデプロイすることができる．これにより，自社のAWS環境のアセスメント結果という非常に機密性の高いセキュリティ情報を，ドコモに開示することなく保管・利用ができる．

5. あとがき

本稿では，クラウドセキュリティの基本的な考え方と，ドコモでのセキュリティ統制の取組み内容について解説した．パブリッククラウドは今もなお進化を続けており，クラウドセキュリティの考え方や世の中の攻撃手法も刻一刻と変化をしている．大事なのは，パブリッククラウド上で一度システムを作ったらそれで終わりではなく，日々セキュリティアセスメントを行うとともに，そのアセスメントの内容も時代に合わせて日々アップデートすることである．アップデートを行うにあたって，クラウド事業者それ自身が提供するサービスを利活用するのはもちろんのこと，CCoEのようにクラウド活用の促進や，セキュリティ統制を行う専任の組織をつくって運用していくことは，進化のスピードが早いパブリッククラウドをうまく利用していく上で非常に重要である．

ドコモでは，数多くの社内プロジェクトで自律的にセキュリティアセスメントができるツールとしてScanMonsterを開発した．ガイドラインと併せてこういったツールを活用することで，ビジネスの速度を緩めることなく安全にパブリッククラウドを利用していける体制を確立した．今後は，ScanMonster自体の機能拡張としてアセスメント内容のカスタマイズ機能やガイドラインとの紐付け，現在のAWSに加えてGCPやAzureなどのマルチクラウド対応を検討している．また，アセスメント結果の情報セキュリティ部への集約や，定期的にアセスメントを実行するような仕組みの検討など，社内の体制やポリシーの改善にも取り組んでいきたい．

文　献

［1］ Bloomberg：“Capital One Says Breach Hit 100 Million Individuals in U.S.,” Jul. 2019. https://www.bloomberg.com/news/articles/2019-07-29/capital-one-data-systems-breached-by-seattle-woman-u-s-says

［2］ AWS：“責任共有モデル.” https://aws.amazon.com/jp/compliance/shared-responsibility-model/

［3］ 守屋，ほか：“ドコモのパブリッククラウド活用とCCoEの果たす役割，”本誌，Vol.29，No.1，pp.6-12，Apr. 2021.

＊33 IaC：サーバやネットワーク，ストレージなどのインフラストラクチャの構成をコードとして記述して管理するという考え方．設定やプロビジョニングの作業を自動化できる．

＊34 AWS CloudFormation：AWSサービスの1つ．IaCを実現するために，テンプレートに記述されたAWSリソースのプロビジョニングや管理機能を提供する．