ScanMonster 管理者マニュアル

株式会社NTTドコモ

2020/02/04

はじめに

本マニュアルはScanMonsterの管理者向けのマニュアルです。利用者向けのマニュアルはScanMonsterのHelpページをご参照ください。

ScanMonsterとは

ScanMonsterはNTTドコモが開発したAWS上に構築したシステムを自動的にアセスメントするツールです。NTTドコモでは長年AWSを大規模に運用してきた経験をノウハウ化し、AWSを利用するにあたって必要となる考え方やAWS上でのセキュリティ対策方法などをガイドラインやセキュリティデザインパターンとしてまとめ、ドコモ・クラウドパッケージとして展開してきました。 これらのガイドラインやセキュリティデザインパターンを利用することで、AWSを効率的に、かつ考慮漏れを防止しながら利用することが可能です。

- クラウド開発ガイドライン
- セキュリティデザインパターン
- インシデント対応ガイドライン
- IAMデザインパターン
- 共通基盤化ガイドライン
- システム移行ガイドライン

一方で基本的な考え方を理解し、考慮漏れを防止しながらAWSを利用しているつもりでも、システムの規模が増大したり、複数のアカウントを管理する必要がでたり、またメンバーの交代などが発生すると、システムの運用管理も複雑化します。これにより、システムの設定や構成に思わぬ不備がでたり、考慮漏れが再び発生するなどの自体が発生する可能性があります。これらの事態はシステムの規模が大きくなったり、長い間運用しているシステムほど、発生しやすく、人手による運用対処は難しくなります。

ScanMonsterではこれらの思わぬ不備や考慮漏れを**早期に発見し、対策する**ために、実際に運用しているシステムに対して、ガイドラインやデザインパターンで言及している対策事項が実施できているかを自動的に監査するツールです。ScanMonsterを利用することで、システム運用者はAWSのコンソール画面を切り替えながら、システムの設定状況などを確認する必要がなくなり、ScanMonsterの統一した画面上で対策状況を確認することができるようになります。
ScanMonsterには下記のような代表的な特徴があります。

1. **各種ガイドライン/デザインパターンに準拠**
   ドコモ社内で長年AWSを利用して蓄積してきたノウハウを元にした各種ガイドラインやデザインパターンに準拠したアセスメントを実施
2. **自動アセスメント**
   アセスメントはAWS APIを利用して自動的に実施されるため、利用者は複雑な操作は必要ありません。
3. **アカウント横断でアセスメント**
   複数のアカウントを管理している場合でもScanMonsterの統一した画面からアセスメント対象のアカウントを切り替えるだけでアセスメントが可能です。
4. **チュートリアル完備**
   各アセスメント項目に対して、アセスメントの概要やアセスメント結果がNGだった場合の対応策案をチュートリアルとして完備しています。

5. **利用開始が簡単**
   アセスメント対象アカウントは事前に準備されたCloudFormationテンプレートを利用して、アセスメント用のIAMロールを作成するだけで、アセスメントが開始できます。
6. **運用費用が安価**
   ScanMonsterはAWS上でサーバーレス構成で構築されます。そのため、ScanMonster自体の運用費用も安価であり、インフラの運用は必要ありません。

ご利用に際して

ScanMonsterは30日間無償でご利用いただけるトライアル期間を設けています。トライアル期間終了後も継続してご利用いただく場合は、契約に関して下記**お問い合わせ**までご連絡ください。

- トライアルユーザー
  ScanMonsterを構築するAWSアカウント1つにつき30日間無償で利用可能です。セットアップしたScanMonsterに初めてログインした日から起算されます。
- ライセンスユーザー
  ご契約後ScanMonsterにライセンスキーを登録し、1年間毎の契約にてお使いいただけます。
  ライセンスキーの登録については「ライセンスキーの登録」を参照ください。

お問い合わせ

導入やご契約その他ご質問など下記のメールアドレス宛にご連絡ください。

```
株式会社NTTドコモ ScanMonster担当
dcm-cloudconsulting-ml@nttdocomo.com
```

注意事項

- AWSコンソールの操作をする際はリージョンの選択にご注意ください。ScanMonsterをご利用になるリージョンで操作しているかご確認ください。
  選択中のリージョンは、AWSコンソールの上部ナビゲーション右側で確認できます。

各種マニュアル

- ScanMonster セットアップガイド
- ScanMonster アップデートマニュアル
- ScanMonster 管理者オペレーションマニュアル
- ScanMonster 管理者トラブルシューティング

ScanMonster セットアップガイド

ScanMonsterはCloudFormationを利用してセットアップします。ScanMonsterのセットアップ手順を示します。

事前準備

- **AWSアカウントの作成**

  ScanMonsterのセットアップにはAWSアカウントが必要です。AWSアカウントを作成していない場合は、下記の手順で作成してください。

  1. https://aws.amazon.com/を開き、「**アカウント作成**」または「**Create an AWS Account**」をクリックします。
  2. オンラインの手順に従い、アカウントを作成します。

- **IAMユーザの作成**

  ScanMonsterをセットアップするためにはIAMユーザが必要です。AWSマネージメントコンソールにログインしてセットアップを行いますので、マネージメントコンソールにログインできるIAMユーザを準備してください。

- **IAMユーザの権限**

  IAMユーザでは必要最小限の権限を付与することが推奨されています。ただしScanMonsterのセットアップではCloudFormationを利用してIAMロールを含むリソースを作成するため、IPアドレス等によるアクセス制限を実施している場合、セットアップが失敗する可能性があります。

  CloudFormationテンプレートにて作成されるリソースは下記です。

  - API Gateway
  - Cognito
  - CloudFront
  - CloudFormationスタック
  - DynamoDB
  - IAM
  - Lambda
  - S3
  - WAF

  これらのサービスの作成権限があるユーザまたはAWSサービスロールを利用して環境のセットアップを実施してください。

  （参考）AWS CloudFormation サービスロール

  https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-iam-servicerole.html

- **CloudWatchログのアクセス権限**

CloudFormationで作成されるAPI GatewayではCloudWatchログのアクセス許可設定が必要です。

1. ScanMonsterをセットアップするAWSアカウントにログインした状態でこちらをクリックし、API Gatewayの **設定** をクリックしてください。
2. **CloudWatch ログのロール ARN** にIAMロール名が入力されていない場合、必要な権限が付与されたIAMロールのARNを入力してください。

CloudFormationスタックの作成

CloudFormationを利用してScanMonsterのセットアップに必要なコンポーネントをデプロイします。

1. ScanMonsterをデプロイするアカウントにログインします。
2. こちらをクリックしてください。

   Note

   CloudFormationテンプレートはネスト構造になっているため、セットアップ用のテンプレートでスタックを作成すると、その他のテンプレートによるスタックも自動的に作成されます。

3. スタックの名前とパラメータを入力します。

   スタックの名前 （必須）

   作成するスタックの名前を入力します。（例：「ScanMonsterSetUp」）

   AdminUserEmail （必須）

   ScanMonsterの初期ユーザのメールアドレスを入力します。セットアップ完了後、ここで指定したEメールアドレスにログイン用の初期パスワードが通知されます。

   CognitoUserPoolName （任意）

   空欄のままで問題ありません。ScanMonsterのユーザ管理で利用するCognito User Poolの名前を指定したい場合のみ入力してください。

   CrossAccountRoleName （必須）

   アセスメント対象となるAWSアカウントに作成するクロスアカウント用のIAMロールの名前を指定します。デフォルトのままでも問題ありません。

   LambdaExecutionRoleName （任意）

   空欄のままで問題ありません。アセスメント実行時に必要なIAMロールの名前を指定したい場合のみ入力してください。

   S3ContentsBucketName （任意）

   空欄のままで問題ありません。ScanMonsterのWebコンテンツを配信するためのS3バケットの名前を指定したい場合のみ入力してください。その場合でも**あらかじめS3バケットを作成する必要はありません。**S3バケットは新規作成されます。入力する場合は、S3バケットの命名規則に従ってください。

S3LogsBucketName（任意）

空欄のままで問題ありません。ScanMonsterのアクセスログ等を格納するS3バケットの名前を指定したい場合のみ入力してください。その場合でも**あらかじめS3バケットを作成する必要はありません。**S3バケットは新規作成されます。入力する値は、S3バケットの命名規則に従ってください。

TemplateHostS3Url（必須）

別途指定がない限りはデフォルト値のままにしてください。

UpdateDate (必須)

別途指定がない限りはデフォルト値のままにしてください。

WebFunctionHostS3Bucket（必須）

別途指定がない場合はデフォルト値のままにしてください。

WhiteCidr（必須）

ScanMonsterのWebページはセットアップ時はIPアドレス（グローバルIPアドレス）によるアクセス制限をしています。ここではセットアップ時にアクセスを許可するアクセス元のCIDRを入力します。入力できるのは、/8もしくは、/16から/32までの任意のIPv4レンジです。この設定はセットアップ後に変更することが可能です。セットアップ時にアクセス元が決定していない場合はデフォルト値のままにします。

LicenseKey（任意）

ScanMonsterを試用される場合は入力不要です。
ScanMonsterのライセンスキーをお持ちの場合はご入力ください。ライセンスキーについての詳細は、ライセンスキーの登録でご確認ください。

ScanMonsterは30日間無償で利用可能なトライアル期間を設けています。トライアルユーザーとしてご利用になる場合は当項目に何も入力しないでください。

4. **次へ** をクリックします。

5. オプションの画面が出るので、そのまま **次へ** をクリックします。

6. 確認画面が出るので、「**AWS CloudFormation によって IAM リソースがカスタム名で作成される場合があることを承認します。**」と「**AWS CloudFormation によって、次の機能が要求される場合があることを承認します: CAPABILITY_AUTO_EXPAND**」にチェックを入れて、**スタックの作成** をクリックします。

7. スタックの状況が「**CREATE_COMPLETE**」になったら完了です。下記のスタックが作成されます。

    - [*スタック名*]
    - [*スタック名*]-Api-[*ランダム文字列*]
    - [*スタック名*]-Auth-[*ランダム文字列*]
    - [*スタック名*]-AssessmentExecutionRole-[*ランダム文字列*]
    - [*スタック名*]-ContentsDelivery-[*ランダム文字列*]

- [*スタック名*]-WebContetns-[*ランダム文字列*]

クロスアカウント用のIAMロール作成

アセスメント対象のAWSアカウントに、アセスメントに必要なクロスアカウントロールを作成します。

1. CloudFormationスタックの作成 の手順で作成したCloudFormationスタックの出力タブに記載されている*QuickCreateLinkForAssessmentRole*の値をメモします。

   Note

   *QuickCreateLink*はScanMonsterのユーザ招待メールにも記載されます。ユーザがクロスアカウントロールを作成する場合は招待メールか、*QuickCreateLink*を使用して作成ください。

2. アセスメント対象アカウントにログインした状態で、1でメモした*QuickCreateLinkForAssessmentRole*のURLへアクセスします。

3. **AWS CloudFormation によって IAM リソースがカスタム名で作成される場合があることを承認します。** にチェックを入れ、「スタックの作成」をクリックして完了です。

> クロスアカウント用のIAMロールの作成は、アセスメント対象の全てのAWSアカウントで必要です。

ScanMonsterへのアクセス

1. CloudFormationスタックの作成 で作成したスタックの出力タブに表示されている*ScanMonsterUrl* にアクセスしてScanMonsterのログイン画面が出力されれば、セットアップ完了です。

   Note

   URLにアクセスした際にS3のURLにリダイレクトされる場合は、AWS側でDNSの反映に時間がかかっている場合があります。しばらく時間をおいてから再度アクセスしてください。

(オプション) カスタムドメインの設定

ScanMonsterのドメインはデフォルトではCloudFrontのドメイン名が使用されています。カスタムドメインを利用したい場合は、下記の手順で設定することができます。

1. CloudFormationスタックの作成にて作成されたCloudFrontディストリビューションにて、代替ドメイン名（CNAME）の追加とカスタムドメインの設定をします。

   代替ドメイン名 (CNAME) を追加してカスタム URL を使用する

   https://docs.aws.amazon.com/ja_jp/AmazonCloudFront/latest/DeveloperGuide/CNAMEs.html

2. AWSコンソールからCloudFormationスタックの作成で作成されたCognito User Poolの設定画面を開き、「全体設定」から「メッセージのカスタマイズ」を開きます。

3. 設定画面下部の「Eメールのメッセージ」に記載されているScanMonster URLを設定したカスタムドメインのURLに変更します。以上でカスタムドメインの設定は完了です。

ライセンスキーの登録

ScanMonsterのご契約後、ライセンスキーが発行されてから必要な作業です。
※30日間の無償期間で利用される場合は不要な作業です。

ScanMonsterをご契約される場合は下記のメールアドレス宛にご契約希望の旨をご連絡ください。

```
株式会社NTTドコモ ScanMonster担当
dcm-cloudconsulting-ml@nttdocomo.com
```

- **ライセンスキー登録方法**
  - 既にCloudFormationスタックの作成でScanMonsterを作成している場合
    ScanMonster アップデートマニュアルの手順に沿い、**LicenseKey**欄を入力しCloudFormationスタックを更新します。
  - CloudFormationスタックの作成を完了していない場合
    スタックパラメータの**LicenseKey**欄を入力しスタックを作成します。

ScanMonster アップデートマニュアル

ScanMonsterのアップデートはCloudFormationスタックの更新で実施します。アップデートを実施する際は、下記の手順で実施してください。

1. AWSコンソールにログインし、CloudFormationスタックの作成 で作成したCloudFormationスタックを選択して「**更新する**」をクリックします。

   > CloudFormationスタックはネスト構造になっているため、ルートのスタックを選択してください。

2. 「既存テンプレートを置き換える」を選択し、テンプレートソースとして「Amazon S3 URL」を指定した上で「https://cloudformation-for-scan-monster.s3-ap-northeast-1.amazonaws.com/setup-scan-monster.yaml」を入力して「**次へ**」をクリックします。

3. パラメータ指定画面にて、下記のパラメータを変更します。

   - UpdateDate
     更新を実施する日付(yyyyMMdd)を入力してください。値を変更しない場合、Webコンテンツが更新されません。同一日に複数回更新が必要な場合は、時間も含めて値を設定(yyyyMMddHHmm)をしてください。

   - LicenseKey
     ライセンスキーをお持ちで未入力の場合、またはライセンスキーを変更する場合は入力してください。トライアルユーザーは未入力のまま次の手順へ進んでください。

4. 「**次へ**」をクリックします。

5. オプション指定画面にてそのまま「**次へ**」をクリックします。

6. 確認画面が出るので、「**AWS CloudFormation によって IAM リソースがカスタム名で作成される場合があることを承認します。**」 と「**AWS CloudFormation によって、次の機能が要求される場合があることを承認します: CAPABILITY_AUTO_EXPAND**」にチェックを入れて、**スタックの作成** をクリックします。

ScanMonster 管理者オペレーションマニュアル

本マニュアルではScanMonsterの運用において、管理者が必要な操作を示します。

ユーザー管理

ScanMonsterのユーザー管理に必要なオペレーションの説明を行います。

ユーザー作成

ScanMonsterのユーザーはCognito User Poolで管理されているため、Cognito User Pool上でユーザー作成を行います。

1. Cognitoコンソールにログインします。
2. **ユーザープールの管理** をクリックします。
3. ユーザープールの一覧が表示されますので、ScanMonsterで利用しているユーザープールを選択します。
4. **ユーザーとグループ** タブをクリックします。
5. **ユーザーの作成** をクリックします。
6. ユーザーの作成画面で下記の通り、項目を入力します。

   ユーザー名(必須)
   ユーザー名を入力します。

   この新規ユーザーに招待を送信しますか?
   項目にチェックを入れ、**Eメール** にチェックを入れます。

   仮パスワード
   仮パスワードを指定したい場合は入力します。空白の場合、自動的にランダムな初期パスワードが設定されます。

   電話番号
   何も入力しません。

   電話番号を検証済みにしますか?
   チェックを外します。

   Eメール
   利用者のEメールアドレスを入力します。

   Eメールを検証済みにしますか?
   項目にチェックをいれます。

7. **ユーザーの作成** をクリックして作成完了です。

グループ作成

ScanMonsterの各AWSアカウントへのアセスメント権限はCognito User Poolで作成したユーザーをグループに所属させることで付与します。
ここではグループの作成を行います。

1. Cognitoコンソールにログインします。
2. **ユーザープールの管理** をクリックします。
3. ユーザープールの一覧が表示されますので、ScanMonsterで利用しているユーザープールを選択します。
4. **ユーザーとグループ** タブをクリックします。
5. **グループ** タブを開きます。
6. **グループの作成** をクリックします。
7. グループの作成画面で下記の通り、項目を入力します。

   名前（必須）
   グループ名を入力します。
   グループ名は必ずAWSアカウントID(12桁の数字)としてください。 ユーザーは所属しているグループのグループ名のAWSアカウントをアセスメントする権限を持ちます。

   説明
   グループの説明を入力します。

   IAMロール
   何も選択しません。

   優先順位
   何も入力しません。

8. **グループの作成** をクリックして作成完了です。

Note
ユーザープールごとに作成できるグループの最大数はデフォルトで25になっています。 グループの最大数は制限緩和申請にて緩和することが可能です。

ユーザーをグループに所属させる

ScanMonsterにAWSアカウントのアセスメント権限を付与するためには、ユーザープールで作成したユーザーをグループに所属させます。

1. Cognitoコンソールにログインします。
2. **ユーザープールの管理** をクリックします。
3. ユーザープールの一覧が表示されますので、ScanMonsterで利用しているユーザープールを選択します。

4. **ユーザーとグループ** タブをクリックします。
5. ユーザー一覧からグループに所属させるユーザーを選択します。
6. **グループに追加** をクリックします。
7. 所属させるグループ（権限を付与したいAWSアカウントIDのグループ名）を選択します。
8. **グループに追加** をクリックして完了です。

アクセス制限管理

ScanMonsterはアクセス制限を実施することが可能です。ここではアクセス制限のオペレーションについて説明します。

IPアドレス制限

IPアドレスによるアクセス元制限を行います。IPアドレス制限はCloudFrontを経由して配信されるWebコンテンツのアクセス制限と、ScanMonsterのAPIのアクセス制限があります。
IPアドレス制限では双方の設定を行う必要があります。

Note

IPアドレス制限はScanMonsterのSettingから変更可能です。特別な事情が無い限り、ScanMonsterのSettingより変更ください。使用方法はScanMonsterのヘルプを参照ください。

1. Webコンテンツ側の設定を行います。WebコンテンツはAWS WAFにてIPアドレス制限を実施しているので、AWS WAF コンソールを開きます。
2. **Conditions** の **IP addressess** タブを選択します。
3. **ScanMonsterAllowedIPSet** を選択します。
4. アクセスが許可されているアクセス元のCIDR一覧が表示されるため、適宜追加/更新します。
5. 続いてAPI側の設定を行います。CloudFormationスタックの作成で作成した`[*スタック名*]-Auth-[*ランダム文字列*]`スタックの`AuthenticatedRole`で表示されているロールでAPIのアクセス制限を実施しています。このロールのポリシーを更新することでIPアドレスの更新を行います。
6. IAM コンソールを開きます。
7. 「ロール」タブのロール一覧から`AuthenticatedRole`で確認したロールを開きます。
8. アクセス制限のインラインポリシーから`InvokeScanMonsterAPI`を開き、「ポリシー編集」をクリックします。
9. 「JSON」タブから`Condition` -> `IpAddress` -> `aws:SourceIp` エンティティの許可するCIDRのリストを更新してください。
10. 「Review policy」をクリックし、「Save changes」をクリックしてポリシーを保存して完了です。IPアドレス制限が反映されていることを確認してください。

ScanMonster 管理者トラブルシューティング

エラー発生時の対処法

ScanMonsterを操作中にエラーメッセージが表示された場合、以下の対処方法を参照してください。

```
AWS account ID must be registered. Please contact the administrator.
```

アセスメント可能なアカウントが登録されていない状態です。 ScanMonster 管理者オペレーションマニュアル内にあるグループの作成、ユーザをグループに所属させるを参照しアカウントの追加を行ってください。

```
ScanMonster is not authorized to access AWS Account [AWS AccountID]
```

クロスアカウント用IAMロールの見直し再設定をお願いします。 新しくロールを作成する場合はScanMonster セットアップガイドよりクロスアカウント用のIAMロール作成 を行ってください。

```
Response ID ([Response ID]) is invalid
```

DynamoDBのキャパシティの上限値を超えている可能性があります。

- Amazon DynamoDB「読み込み/書き込みキャパシティーモード」
  キャパシティーモードを「プロビジョンド」で運用している場合は、 AWSコンソールよりキャパシティーモードを「オンデマンド」に変更ください。

```
The requested URL was not found
```

リクエストURLが存在しないか異なる可能性があります。 ScanMonster アップデートマニュアルより CloudFormationスタックの更新を行い、 問題が解消するかご確認ください。
※ 変更の反映に時間がかかる場合があるため時間を置いてから確認ください。

```
Not authorized to modify IP Address.
```

IP制限設定に必要な権限が許可されていません。 ScanMonster アップデートマニュアルに従って CloudFormationスタックの更新を実施してください。

```
Not found '[Key Name]' key in Environment variable.
```

Lambda関数の環境変数が不足しています。 最新のCloudFormationテンプレートを適用するため、ScanMonster アップデートマニュアルの**CloudFormationスタックのアップデート方法**に従ってアップデートを実施してください。

```
Unregistered license key is requested
- - - -
Requested license key is Denied
```

ライセンス認証で許可されていません。入力されているライセンスキーに誤りがないかご確認ください。

```
License key is expired
```

ご契約期間の有効期限を過ぎています。引き続きご利用になる場合は契約について下記**ライセンス契約のお問い合わせ**宛にご連絡ください。

```
The trial license for [AWS AccountID] is expired.
```

トライアル期間が終了しています。引き続きご利用になる場合は契約について下記**ライセンス契約のお問い合わせ**宛にご連絡ください。ご契約後ライセンスキーの登録については「ライセンスキーの登録」を参照ください。

ライセンス契約のお問い合わせ

下記メールにご連絡ください。

```
株式会社NTTドコモ ScanMonster担当
dcm-cloudconsulting-ml@nttdocomo.com
```