

AWS をはじめよう

mochikoAsTech 著

2018-10-08 版 mochikoAsTech 発行

はじめに

2018年10月mochikoAsTech

この本を手に取ってくださったあなた、こんにちは、あるいははじめまして。「AWSをはじめよう」の筆者、mochikoAsTechです。

前作の「DNSをはじめよう」では、お名前.comでドメインを買って、AWSのアカウントを作り、Route53をネームサーバとして使うところまでをやってみました。そして本書「AWSをはじめよう」では、そのそのドメインを使って自分のサイトを作ります。

AWSでウェブサーバを立てたり、DBサーバを立てたり、WordPressをインストールしたりして、ブラウザで自分のサイトが見られるところまで一緒に頑張ってやっていきましょう！

え、この本って別の本の続きなの？そっちを先に読んだ方がいい？と思ったあなた、ぜひ「DNSをはじめよう」を先に読んでください。

ケーキのデコレーションはスポンジを焼いてからでないと出来ないように、いきなり「AWSをはじめよう」から読み始めると「え、これを先にやっておかなければいけないの？」、「なにこれ、こんなの用意していない」となってさまざまな手戻りが発生します。はじめようシリーズ1作目となる「DNSをはじめよう」を読んでから、「AWSをはじめよう」を読み始める強くお勧めします。

想定する読者層

本書は、こんな人に向けて書かれています。

- AWSがなんなのかよく分かっていない人
- ブログやポートフォリオサイトを独自ドメインで作ってみたい人
- JavaScriptやHTMLやCSSなら書けるけどサーバは分からなくて苦手という人
- プログラミングの勉強がしたいけど環境構築でつまづいて嫌になってしまった人
- これからシステムやプログラミングを学ぼうと思っている新人
- ウェブ系で開発や運用をしているアプリケーションエンジニア

- ・ インフラやサーバになんとなく苦手意識のある人
- ・ AWS、EC2、RDS、ELB、Auto Scaling、IAM、CloudTrail、Route53などの単語に興味がある人
- ・ クラウドってなんだろう？ サーバってなんだろう？ という初心者

本著の特徴

本著では前作「DNS をはじめよう」で買ったドメインを使って、実際に WordPress で自分のサイトを作つてみます。手を動かして AWS でサーバを立てたりロードバランサーの設定をしたりしながら学べるので理解がしやすく、インフラ初心者でも安心して読み進められる内容です。

また実際にありがちなトラブルをとり上げて、

- ・ 上手くいかないときは原因をどう調べたらいいのか？
- ・ 問題をどう解決したらいいのか？
- ・ どうしたら事前に避けられるのか？

を解説するとともに、実際にコマンドを叩いて反復学習するためのドリルもついています。

本著のゴール

本著を読み終わると、あなたはこのような状態になっています。

- ・ WordPress のおしゃれなサイトができあがっている
- ・ 使うも壊すも自由な勉強用の Linux サーバ環境が 1 台手に入る
- ・ 物理サーバと仮想サーバの違いが説明できるようになっている
- ・ オンプレミスとクラウド、それぞれのメリットデメリットが分かるようになっている
- ・ 読む前より AWS やサーバや黒い画面が怖くなくなっている

免責事項

本著に記載されている内容は筆者の所属する組織の公式見解ではありません。

また本著はできるだけ正確を期すように努めましたが、筆者が内容を保証するものではありません。よって本著の記載内容に基づいて読者が行った行為、及び読者が被った損害

について筆者は何ら責任を負うものではありません。

不正確あるいは誤認と思われる箇所がありましたら、電子版については必要に応じて適宜改訂を行いますので筆者までお知らせいただけますと幸いです。

目次

はじめに	3
想定する読者層	3
本著の特徴	4
本著のゴール	4
免責事項	4
第 1 章 インフラとサーバってなに？	11
1.1 AWS を理解するには先ずインフラを知ろう	12
1.2 インフラとは？	12
1.3 サーバとは？	13
1.3.1 サーバの姿を見てみよう	16
1.3.2 サーバはデータセンターにいる	18
1.3.3 物理サーバと仮想サーバ	22
1.4 オンプレミスとクラウド	24
1.4.1 クラウドのメリットとデメリット	25
1.4.2 AWS がやっているクラウド	26
1.4.3 パブリッククラウドとプライベートクラウド	27
1.4.4 AWS 以外のクラウド	28
第 2 章 AWS を使い始めたら最初にやること	29
2.1 AWS 無料利用枠を使おう	30
2.2 AWS のアカウント作成	31
【コラム】「DNS をはじめよう」はどこで買える？	32
2.3 マネジメントコンソールにサインイン	32
2.3.1 【ドリル】AWS の管理画面はなんて名前？	34
2.4 IAM でユーザの権限管理	35
2.4.1 ルートユーザーの普段使いはやめよう	35

2.4.2	IAM ユーザを作ろう	36
2.4.3	MFA（多要素認証）で不正利用から IAM ユーザーを守る	48
2.4.4	ルートユーザーも MFA を有効にする	61
2.5	リージョンの変更	63
2.6	CroudTrail でいつ誰が何をしたのか記録	65
第 3 章	AWS でウェブサーバを立てよう	69
3.1	EC2 でサーバを立てる	70
3.2	SecurityGroup	70
3.3	VPC	70
3.4	EC2	70
3.4.1	請求アラート	70
3.4.2	SSH の鍵認証	70
3.4.3	鍵の変換	70
3.4.4	ElasticIP	70
3.4.5	Bastion	70
第 4 章	サーバのバックアップを取っておこう	71
4.1	AMI	71
第 5 章	ELB でバランシングやサーバの台数を管理しよう	73
5.1	ELB	73
5.2	Auto Scaling	73
5.2.1	スケーリングに使える	73
5.2.2	サーバが 1 台死んでも自動で 1 台立ち上がる	73
第 6 章	DB サーバを立てよう	75
6.1	RDS	75
6.2	Amazon Aurora	75
第 7 章	ネームサーバの設定をしよう	77
7.1	Route53	77
第 8 章	AWS をやめたくなったらすること	79
8.1	無料の 1 年が終わる前にすべきこと	79
8.1.1	【ドリル】サンプル	79

付録 A　本当の Git	81
A.1　Git - ぎゅつと言えないトウインクル	82
あとがき	83
Special Thanks:	83
レビュー	83
参考書	83
著者紹介	85

第 1 章

インフラとサーバってなに？

この章では AWS とはなにか？ そもそもクラウドとは何か？ サーバとは何か？ という基本を学びます。

1.1 AWS を理解するには先ずインフラを知ろう

AWS とは Amazon Web Services の略で、欲しいものをぽちっとな！ すると翌日には届くあの Amazon がやっているクラウドです。

「AWS は Amazon がやっているクラウドです」と言われても、「クラウド」が分からないと結局 AWS が何なのかよく分からないままでですよね。

クラウドって何なのでしょう？

クラウドだけではありません。よくクラウドと一緒に並んでいるサーバやインフラという言葉がありますが、こちらも何だか分かりますか？ IT 系で働いていても、その辺って「なんか・・・ふんわり・・・なんか雲の向こう側にある・・・ウェブサイト作るための何か・・・？」という程度の認識で、クラウドってなに？ とか、サーバってなに？ と聞かれたときに、ちゃんと説明できる人は意外と少ないのでと思います。

なので、先ずは「AWS は Amazon がやっているクラウド」という文章の意味が分かるよう、インフラ周りから順を追って学んでいきましょう。

1.2 インフラとは？

インフラという言葉は知っていますか？

はじめて聞いたという人も、「なんとなくは分かるけど、説明してと言われたらうーん・・・」な人も、いま自分が考える「インフラ」についての説明をここに書いてみましょう。いきなり正解を聞かされるより、自分で答えを考えて書き出してみてからの方が、正解を聞いたときにきっと自分の中へより染み渡ってくるはずです。

インフラとは



では答え合わせをしてみましょう。

インフラとはサーバやネットワークのことです。

そもそもインフラこと「Infrastructure」は、直訳すると基盤や下部構造といった意味です。ですので「生活インフラ」と言うと一般的には上下水道や道路、そしてインターネットなど、生活に欠かすことの出来ない社会基盤のことを指します。

そして技術用語としては、インフラはシステムやサービスの基盤となる「設備」のことをいいます。なので、分かりやすく言うと「インフラとはサーバやネットワークのこと」なのです。

これでもう会社で後輩に「インフラってなんですか？」と聞かれても、堂々と「サーバとかネットワークのことだよ」と答えられますね！

でも後輩に、続けて「え、サーバってなんですか？」と聞かれたらどうしましょう？

1.3 サーバとは？

後輩から「サーバってなんですか？」という直球の質問を投げつけられたら、しっかりとホームランで打ち返せますか？

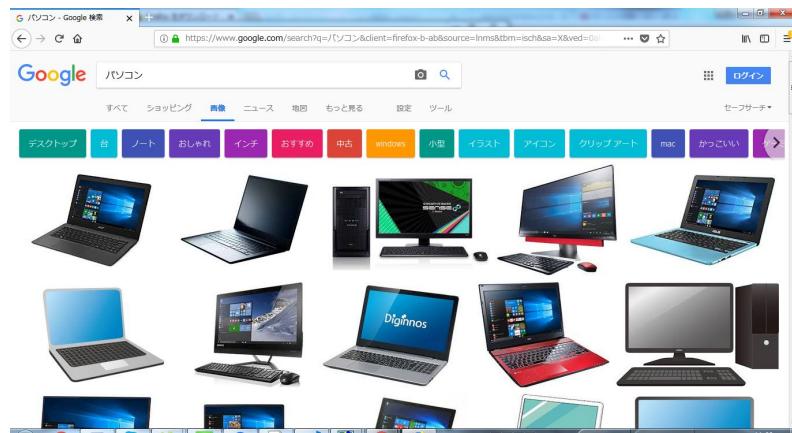
しっかりと答えられるか不安な人も、自信のある人も、ちょっと頭の中でサーバの姿を思い浮かべてみてください。できればイラストじゃなくて実写でお願いします。



▲図 1.1 サーバの姿を思い浮かべて描いてみよう

思い浮かびますか？ あんまり浮かばないですよね。サーバの姿がくっきり思い描ける人の方が少ないのでないかと思います。

でもこれが「パソコンの姿を思い浮かべてください」なら、きっとすぐに浮かんでくるはずです。（図 1.2）



▲図 1.2 パソコンの姿ならすぐに思い浮かぶ

でもサーバの姿は？ と考えるとなかなか思い浮かびません。
ではサーバの姿をお見せしたいと思います。

1.3.1 サーバの姿を見てみよう



▲図 1.3 サーバの姿（HPE ProLiant DL360）

これは Hewlett Packard Enterprise（ヒューレット・パッカード エンタープライズ）の HPE ProLiant DL360^{*1}というラックマウント型のサーバです。DL360 は 15 年以上前から愛されているシリーズ^{*2}で、日本でもっとも売れたラックマウント型のサーバと言っても過言ではないかも知れません。定価で 1 台おおよそ 50 万円以上します。

そして本は本棚に収めるように、サーバはサーバラック（図 1.4）^{*3}という専用の棚に収めることが多いです。

*1 HPE ProLiant DL360 <https://www.hpe.com/jp/ja/product-catalog/servers/proliant-servers/pip.hpe-proliant-dl360-gen10-server.1010007891.html>

*2 2018 年 8 月時点で発売されているのは HPE ProLiant DL360 Gen10 です。末尾の「Gen10」は世代（Generation）を表しているので、10 世代目ということです。

*3 写真のサーバラックは HPE Advanced G2 シリーズ <https://www.hpe.com/jp/ja/product-catalog/servers/server-racks/>



▲図 1.4 サーバを収めるためのサーバラック

先ほどの HPE ProLiant DL360 のようなサーバは、ラック (=棚) にマウントする (=乗せる) ことができる形状のため「ラックマウント型サーバ」、略してラックサーバと呼ばれています。

ラックマウント型のサーバは 1U (ワンユー)・2U・4U のように厚みが異なり、1U ならこのサーバラックの 1 ユニット (1 段) 分、2U なら 2 ユニット (2 段) 分を使うことになります。そのためラックマウント型サーバは 1U サーバという名前で呼ばれることもあります。サーバラックは 42U サイズが多く、その名前のとおり 1U サーバを 42 台収めることができます。^{*4}

^{*4} 但しラックに供給される電源の量や放熱の問題もあるため、実際は 42U サイズのラックにサーバ 42 台をぎちぎちに詰めることは少ないので、と思います。



▲図 1.5 タワー型サーバとブレードサーバ

「ラックマウント型サーバ」だけでなく、デスクトップパソコンのような「タワー型サーバ」(図 1.5)^{*5}や、シャーシやエンクロージャーと呼ばれる箱の中に何本も差し込んで使う省スペースな「ブレードサーバ」^{*6}など、サーバには色々な形があります。

こうしたラックマウント型サーバ、タワー型サーバ、ブレードサーバのように、手で触れる実体があるサーバのことを**物理サーバ**といいます。物理的な実態があるから物理サーバです。

そもそもですが、人がウェブサイトを作る時には土台となるサーバが必ず必要となります。たとえばてなブログで無料のブログを作ったときでも、ameba owned で無料のホームページを作ったときでも、あなた自身はサーバのことなど気にも留めないと思いますが、どこかしらに必ずそのブログやサイトが乗っかっているサーバは存在しています。

ではサーバはいったいどこにいるのでしょうか？

1.3.2 サーバはデータセンターにいる

前述のサーバラックや、その中に詰まったラックサーバを実際に見たことはありますか？

どんなウェブサイトも、世界中のどこかにあるサーバの中で稼動しているはずなのですが、インフラエンジニアでなければサーバを見る機会はなかなかないかも知れません。

サーバはほとんどの場合、**データセンター**と呼ばれる場所に設置されています。^{*7}

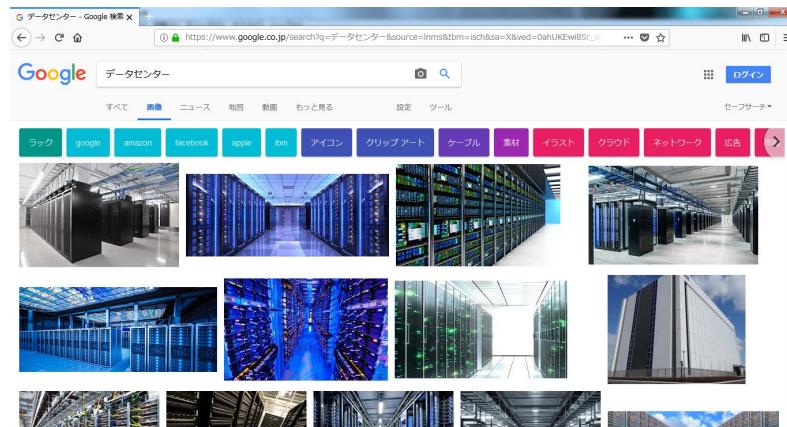
カラオケをするには防音や音響設備の整ったカラオケルームが適しているように、サー

^{*5} <https://www.hpe.com/jp/ja/product-catalog/servers/proliant-servers/pip-hpe-proliant-m110-gen10-server.1010192782.html>

^{*6} <https://www.hpe.com/jp/ja/integrated-systems/bladesystem.html>

^{*7} 企業によっては、オフィス内にサーバルームがあつてサーバはそこにいるかも知れません。

バを動かすためのさまざまな設備が整った場所のことをデータセンター、略して DC^{*8}といいます。先ほどのラックサーバがたくさん並んでいますね。（図 1.6）



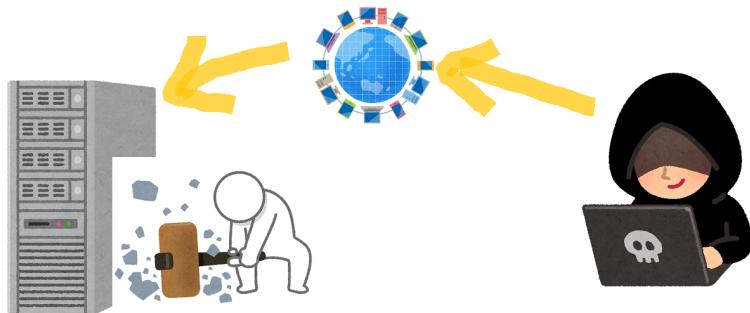
▲図 1.6 データセンターはサーバのための設備が整っている

しかし「サーバを動かすための設備」と言われても、「電源取れればそれでいいんじゃないの？ 専用の建物なんか要る？」と思われるかも知れません。サーバを動かすのに適した設備とはどんなものなのでしょう？

〈サーバに適した設備〉 1. 防犯設備

もし悪い誰かが「この企業が気に食わないから商品のウェブサイトを落としてやろう」と思ったとき、あるいは「このネットショップの顧客情報を根こそぎ盗んでやろう」と思ったとき、ネット越しにサイトを攻撃したり侵入したりするだけでなく、そのサイトが動いているサーバのところまで行って物理的に破壊したり、ハードディスクを引っこ抜いて盗んだり、という手段があります。

^{*8} データセンター（Data Center）の頭文字を取って DC ですが、の中でもインターネット用途向けのデータセンターはインターネットデータセンター、略して iDC と呼ばれたりします。「逆にインターネット用途以外のデータセンターってなに？」となりますが、メインフレーム（インターネット以前の時代の大型コンピュータ）向けということのようです。



▲図 1.7 攻撃や窃盗はインターネット越しでも物理的にでもできる

データセンターは後者の「物理的な攻撃や侵入」からサーバを守るための設備を整えています。

堅牢さはデータセンターによって異なりますが、たとえば次のような防犯対策が取られています。

- 所在地を一般に公開しない^{*9}
- 建物自体に侵入経路となる窓がない
- 事前予約をした上で顔写真つきの身分証を提示しないと建物に入れない
- エントランスで空港と同じような手荷物チェックや金属探知機チェック、静脈認証がある
- 上着や荷物、携帯電話、カメラなどは持ち込み禁止
- 借りているサーバラックがある階にしかエレベータが止まらない
- サーバルームへの入退室は監視カメラと静脈認証で記録
- 入るときと出るときで体重が違うと出られない

また「うちは弱小サイトだから誰かのうらみも買わないし、盗まれるような個人情報もないよ」という場合でも、防犯だけでなく天災や熱の対策も必要です。

^{*9} 2018年7月、都内で建築現場の火災が発生した際に「この建物はAWSのデータセンターとして建築していた可能性が高い」というニュースが出ており、断定はしていなかったものの「それは報道していいの？周知の事実になってしまったら、もう一度同じ場所に立てるの無理なのでは・・・？」とちょっと気になりました。

〈サーバに適した設備〉 2. 地震・火事対策設備

ウェブサイトはサーバ上で稼動しているため、サーバが止まればもちろんサイトも見られなくなってしまいます。^{*10}

もし地震などの天災があったときにも絶対にサーバを止めないため、データセンターの建物は耐震構造になっていることはもちろん、次のような電力供給対策もされています。

- 変電所から電力を受ける受電設備は複数用意して冗長化している
- もし停電があっても電力が途絶えないよう、電力は複数の変電所から引いている
- 両方の変電所が止まって完全に電力が途絶えたら UPS（無停電電源装置）が自動稼働
- さらに数十秒以内に自家発電機が稼動し、最低数日間は追加の燃料給油なしで稼動可能
- 燃料（重油やジェット燃料）は販売元業者と有事の優先供給の契約をしており、供給が続く限りは自家発電で稼動し続けることが可能

電源がなくなればパソコンも落ちてしまうように、サーバも、その上で稼動しているウェブサイトも、電力が供給されなければ落ちてしまいます。仮にサーバを2台用意して「1台壊れても、もう1台でサイトは見られる！ 大丈夫！」と安心していても、データセンターの電力そのものが止まってしまえば、どちらのサーバも電源が切れてサイトは見られなくなります。電気は使って当たり前と思いがちですが、311の輪番停電のように「当たり前が崩れたとき」にも、いつもどおり稼動できる環境がデータセンターには求められているのです。

さらに万が一火事が起きても、サーバにじゃんじゃん水をかけて消火するわけにはいきません。火は酸素をエネルギーにして燃えるので、多くのデータセンターでは酸素以外のガスで部屋を満たして消火するガス消火設備を備えています。

〈サーバに適した設備〉 3. 空調設備

そして一生懸命稼動しているサーバはとても熱くなります。皆さんのパソコンにもファンなどの冷却機構が付いていて、使っていると熱を冷まそうとしますよね。サーバも同じで、たくさんのサーバが詰まったサーバラックの裏側には、熱い空気がいっぱい吐き出されてきます。

^{*10} 冗談のようですが「こちらのサーバを停止して削除しますね」「はい、使ってないのでいいです」という会話をした後で、実際にサーバを削除したら「サイトが見られなくなつたんですけど！」という連絡が来た、という話も聞きます。サーバがなければサイトは見られない、というのは決して万人にとって当たり前のことではないのです。

暑い部屋ではサーバが故障したり落ちてしまったりする^{*11}ため、データセンター内のサーバルームの空調はとても強く、人間が過ごすにはちょっとつらい寒さです。

このように防犯、地震・火事対策、空調といった設備が整ったデータセンターで、サーバは日々元気に稼動しているのです。

1.3.3 物理サーバと仮想サーバ

部屋を借りるとき、「1DK の部屋なら 12 万、2LDK の部屋なら 20 万」のように広いほうが家賃は高くなります。データセンターを借りるときもまったく同じで「1/2 ラックなら 12 万、1 ラックまるごとなら 20 万」のように、ラックサイズによって月額の費用が変わってきます。

そして 2LDK の部屋に 1 人で住むと、1 人で 20 万負担しなければなりませんが、シェアハウスにして 10 人で住めば 1 人当たりの家賃コストは 2 万円に下がります。

サーバラックも同様に、42U のラックに 1U サーバを 1 台しか乗せないより、42 台詰め込んだ方が 1 台当たりのコストは下がります。

2000 年代前半、インターネットが盛り上がりってきてサーバが必要になってきた頃、42U のラックになんとかもっとたくさんのサーバを詰め込めないか？ と試行錯誤した結果、前述の省スペースなブレードサーバや、1U の半分サイズで奥と手前に 2 台収納できる 1U ハーフサイズのサーバなどが台頭してきました。

しかし 1 つのラックに割り当てられた電源の量には上限があるため、42U にぎちぎちに詰め込むと今度は電源が足りなくなってしまいます。^{*12}データセンターによっては、電源容量を増やせるオプションを提供しているところもありますが、それはそれで「10A 増やしたら 3 万円」のように月額費用に跳ね返ってきます。

ラックのスペースは決まっている、使える電源の容量も決まっている。でもそこに置けるサーバの台数を増やしたい！ そこで「物理サーバのサイズを小さくする」とは別のアプローチで生まれてきたのが仮想サーバです。

物理サーバが一軒家だとすれば、仮想サーバはマンション（図 1.8）です。

^{*11} アニメ映画のサマーウォーズで、冷却用の氷が部屋からなくなったことでスーパーコンピュータが熱暴走し、主人公が大事なゲームに負けてしまうシーンを思い出してください。

^{*12} ぎちぎちに詰め込んでなんとか稼動していたものの、ある日データセンターで停電が起きて全台停止。電源はすぐに復旧して自動で全台いっせいに起動しようとしたが、サーバは起動時がいちばん電源を食うため、ラックのブレーカーが落ちて再度全台停止。いっせいに起動しようとしてはブレーカーが落ちて全台停止、をずっと繰り返していた・・・という怪談を聞いたことがあります。本当に怖い話ですね。



▲図 1.8 物理サーバは一軒家、仮想サーバはマンション

一軒家には 1 世帯しか住めません^{*13}}が、マンションにすれば土地のサイズは同じままで 10 世帯住むことができます。1 台の物理サーバをそのまま使うのではなく、物理サーバ上に何台もの仮想サーバを作ることで、サーバラックのサイズはそのままでサーバ台数を増やすことができたのです。

このときマンションの建物にあたる物理サーバをホストサーバ、101 号室や 201 号室のような各部屋にあたる仮想サーバをゲストサーバと呼んだりします^{*14}。

物理的な実体があるのが物理サーバですが、その逆で手で触れる物理的な実態がないのが仮想サーバです。手で触れられるのはあくまでホスト OS のサーバであり、ゲスト OS のサーバはその中で仮想的にしか存在しないため、手で触ることはできません。

同じ広さのラックスペースに、今までよりたくさんのサーバが詰め込めるなんて仮想サーバ素晴らしい！ と思いますが、一軒家よりマンションの方が建築コストが高いのと同じで、仮想サーバを立てるにはホストサーバとなる物理サーバのスペックも高くなればならないため、初期投資額がぐっと高くなります。

データセンターで借りるラックスペース代も高いし、物理サーバだって何十万もします。スペースを切り詰めるために仮想サーバにしたいと思っても、ホストサーバとなる物理サーバはスペックが高いのでさらに高額・・・となると中小企業やスタートアップ企業が自社で物理サーバや仮想サーバを所有・管理するのはなかなか大変なことです。

そこで資本力のある会社が大きなホストサーバをたくさん立てて、その上の仮想サーバ(ゲストサーバ)を他の人に貸すような仕組みが生まれました。

お分かりでしょうか？ 勘のいい方はもうお気づきのことだと思いますが、ここでようやく「クラウドとは何か？」という話と繋がってきます。

^{*13} 一軒家で 2 世帯同居だってあるでしょ！ みたいな突っ込みは心にしまってください。

^{*14} ホスト OS、ゲスト OS という呼び方をすることもあります。

1.4 オンプレミスとクラウド

昔々は、企業が「そろそろ自社のウェブサイト作りたいなあ・・・だからサーバが必要だ！」と思ったら、「サーバを買う」という選択肢しかありませんでした。

サーバを買うと言っても、お店に行ってぱっと買って持ち帰れる、という訳ではありません。

「どのメーカーのサーバにしよう？ EHP かな？ それとも IBM かな？ DELL がいいかな？」と各社の見積もりをとり、値引き交渉をして、それでも数十万から数百万するので社内の裏議を通してやっと購入。購入してもすぐ届くわけではなく、数週間待ってやっと届きます。そして届いたらサーバを段ボールから出して、データセンターもしくは自社のサーバルームにあるサーバラックのところまで持つて行って、がっちゃんこと設置。設置できたら今度は同じく自前のネットワーク機器から LAN ケーブルを繋ぎ、電源も繋ぎます。そして OS のインストールディスクを用意したらサーバに OS をインストールして・・・以下省略しますが、要は「ただ自社のウェブサイトが作りたいだけなのに、サーバを用意するのがすごく大変だった」ということです。

自分でサーバを買って、何もかも自分で用意しないといけないため、* 初期投資のサーバ代が高い* サーバを置くのに適した場所も必要* 「欲しい！」と思ってから使い始めるまでに時間がかかるという状況でした。このようにインフラを自前で用意して、自社で所有・管理するのがいわゆる**オンプレミス**です。

これに対してクラウドは、オンプレミスと違ってサーバを買うのではなく、サービスとして「使う」だけです。

クラウドなら「自社のウェブサイト作りたいなあ・・・だからサーバが必要だ！」と思ったら、ブラウザを開いて、クラウド事業者のサイト上で使いたいサーバのスペックを選んでぽちっとなすだけで、すぐにサーバを立てることができます。しかも AWS なら課金も 1 秒単位の従量課金なので、たとえばサーバを 5 分使ったら 5 分ぶんの費用しかかかりません。こんな簡単にサーバを使い始めたりやめたりできるのは、クラウド事業者が物理サーバそのものを提供しているのではなく、大きなホストサーバをたくさん用意しておいて、その上に立てた仮想サーバ（ゲストサーバ）を提供しているからです。

オンプレミスはサーバを買って使う、クラウドはサービスとして使う、ということですね。でもまだちょっとわかりにくいと思うので、お店を例にオンプレミスとクラウドの違いを確認してみましょう。

1.4.1 クラウドのメリットとデメリット

たとえば私が突然ピザ作りに目覚めて、もうインフラエンジニアなんかやってる場合じゃない！ ピザ屋を始めるんだ！^{*15}と思いついたとします。

ピザ屋さんをオープンすべく、土地を買って、そこに店舗となる建物を建てて、電気とガスと水道を通して、床板や壁紙を貼って・・・からやると、お金も場所も時間もたくさん必要です。しかも準備が整ってやっとオープンしたと思ったら、たった1か月で資金が足りなくなってしまってお店がつぶれることになったとしても、今度は建物の取り壊しや土地の処分など、止めるときは止めるときでやることがたくさんあります。このように全部自分で買って、自分で所有・管理するオンプレミスだと、「ちょっと気軽にピザ屋さんをやってみよう」はなかなか厳しいことが分かります。

一方クラウドは、フードコートへの出店に似ています。「ピザ屋をはじめたい！ だからフードコートの一区画を借りてやってみよう！」という感じです。

これだと建物はもうあって、電気ガス水道ももう用意されています。フードコート内の一区画を契約して使わせてもらうだけなので、すべて自分で準備するオンプレミスと違ってすぐに始められます。しかも数か月やってみて「もうピザ焼くの飽きたわー！」と思ったら、その区画を借りるのを止めるだけでいいのです。前述のとおり AWS なら使い始めるとの初期費用もなく1秒単位の従量課金なので「ピザ屋さんもうやめたいけど、この先30年のローン支払いが残ってるからやめるにやめられない・・」ということはありません。「前月の25日までに契約終了を申し出る必要がある」といった制限すらないので、本当にいつでもやめられます。

クラウドならとても簡単に出店できる（つまりサーバを用意できる）ので、私は本来やりたかった「美味しいピザを焼いて売る」（ウェブサイトを作り自社を宣伝する）という本業に注力できます。

さらに、もしピザ屋さんが大繁盛したら、フードコート内で自店の隣の区画も借りて、お店を広くすることも簡単にできるので、初めから広い区画を借りておく必要もありません。つまり、ウェブサイトへのアクセスが増えてきてサーバのスペックが足りなくなったら、後から増強したり好きなだけサーバの台数を増やしたりもできるので、最初から高スペックなサーバを借りておく必要がありません。

クラウドなら初期投資額が少なく、すぐに始められて、すぐにやめられる。よく「クラウドはスマールスタートに向いている」と言われますが、その理由はまさにこういうところにあるのです。

但し、長い目で見るとフードコートにテナント料を払い続ける方が、土地や建物を買う

^{*15} そしたら「AWS をはじめよう」の続編として「ピザ屋をはじめよう」という本が書けますね。

よりも最終的には高くなるかも知れません。前述のとおり初期投資は少なくて済むのですが、クラウドのいいところは、決して「コストが安くなる」ということではありません。実際、AWSは他社の共有レンタルサーバやVPS^{*16}と比べると高額です。

クラウドのよいところは、たとえばショッピングセンター内でフードコートが入っている南館が地震で崩れてしまっても、すぐに北館に移ってピザ屋の営業を再開できる、といった冗長性です。

この冗長性を自力で確保しようとしたら大変です。ピザ屋さんを常に営業し続けておくために、いつ来るか分からない地震に備えて最初から予備の店舗も確保しておかなければならぬとしたら、相当なコストがかかります。オンプレミスのサーバなら、ただ自社サイトを作りたいだけなのに、品川と渋谷の2か所でデータセンターを借りて両方に1台ずつホストサーバを用意しておき、品川のデータセンターが使えなくなったらその上で動いていたゲストサーバを渋谷のホストサーバに移動させる、というような大仰な話です。これを勝手にやってくれるクラウドはすごいですよね。

ここまでクラウドの良さを色々お話ししてきましたが、もちろんデメリットもあります。

もし何かトラブルがあってフードコート全体がお休みになるときは、問答無用でピザ屋さんもお休みになってしまいます。つまり使っているクラウドで大規模障害が起きたら、一利用者である私たちにできることはなく復旧までひたすら待つしかない、ということです。AWSでも広範囲にわたる障害は定期的に起きています。たとえば2016年には豪雨による電源障害でサーバに接続できなくなる事象が発生^{*17}しました。こうした障害の際にも、AWSが発表してくれる内容がすべてですので、原因が分かるまで自分で徹底的に調べる、あるいは自力で何とかする、ということはできません。

また通路やトイレ、駐車場といった共有スペースはフードコート内の他店舗（ドーナツ屋さんやラーメン屋さんなど）と共有していますので、フードコート内で他のお店が混んでくると、駐車場が満杯になってピザ屋さんに来たかったお客様が入れなかったり、人波が自分の店の方まで押し寄せてきたりとマイナスな影響も受けます。つまり同じクラウド^{*18}を使っているウェブサイトにアクセスが集中すると、たとえば回線がひっ迫したりして自分のサイトまで繋がりにくくなる、ということです。

1.4.2 AWSはAmazonがやっているクラウド

たくさんお話ししてきたので、一度おさらいをしましょう。

*¹⁶ Virtual Private Server の略。先ほど出てきた仮想サーバのことだと思ってください。

*¹⁷ Amazonクラウドのシドニーリージョン、豪雨による電源障害でEC2などに一部障害。現在は復旧－Publickey <https://www.publickey1.jp/blog/16/amazonec2.html>

*¹⁸ 具体的には、同じホストサーバを使っている他のゲストサーバ上のサイト。あるいは同じインターネット回線を使っている他のサーバ上のサイト、ということです。

企業が「自社のウェブサイト作りたいなあ・・・だからサーバが必要だ！」と思ったとき、自分でサーバを買って自分で管理しなければいけないのがオンプレミスです。そして「自社のウェブサイト作りたいなあ・・・だからサーバが必要だ！」と思ったとき、従量課金ですぐ使えて、性能や台数の増減も簡単にできるのがクラウドです。

そしてようやく最初の話に戻ると、AWS とはアマゾン ウェブ サービス (Amazon Web Services) の略で、欲しいものをぽちっとな！ すると翌日には届くあの Amazon がやっているクラウドです。

AWS がなんなのか、お分かりいただけましたでしょうか？

1.4.3 パブリッククラウドとプライベートクラウド

ところでパブリッククラウドやプライベートクラウド、という言葉は聞いたことがありますか？

AWS のようなクラウドは、パブリッククラウドと呼ばれることもあります。みんなでホストサーバという資源（リソース）を共有して使うので、「公共の」という意味の「パブリック」が付いています。

クラウドが少しずつ使われるようになった頃に「クラウドって便利そうだけど、みんなで共有するのってちょっと抵抗あるな・・・」と思った人たちを安心させるため、「プライベートクラウド」という言葉が生まれました。プライベートクラウドとはいったい何なのでしょう？

たとえばオンプレミスの環境で「高スペックな物理サーバを買ってホストサーバにして、その上でゲストサーバ（仮想サーバ）を立てられるようにしたぞ！ ホストサーバのスペックが足りる限りという制限はあるものの、好きなときに好きなだけゲストサーバを立てたり、増強したりできるのでこれはクラウド！ プライベートなクラウドだ！」と言うこともできます。また「クラウド事業者が提供しているホストサーバを1台まるまる占有する契約をしたぞ！ 自社で物理サーバを所有している訳ではないのでこれはクラウドだ。しかも他の人はこのホストサーバ上のゲストサーバを使えないから、プライベートなクラウドだ！」と言うこともできます。定義は曖昧なのですが、このようにみんなで共有せず、自社だけで専有できるクラウドをプライベートクラウドと呼ぶようです。

このプライベートクラウドだと「初期投資額が少ない」「サーバの性能や台数を後から好きなだけ増強できる」といった、クラウド本来のメリットが享受できないように思えますが、これもクラウドなのでしょうか？

このようにクラウドという言葉はとても曖昧です。結局「クラウド」という言葉の定義がはっきりしていないため、その人が言っている「クラウド」という言葉がなにを指して

いるのかは、よくよく聞いてみないと分からない、ということです。^{*19}

1.4.4 AWS 以外のクラウド

ところでクラウドは AWS 以外にも Google の Google Cloud Platform^{*20}、Microsoft の Azure（アジュール）^{*21}、その他にも国内クラウドとしてさくらインターネットがやっているさくらのクラウド^{*22}、GMO クラウド^{*23}などたくさんあります。

その中でもなぜ AWS なのでしょう？

2018 年時点、クラウド市場では AWS がシェア 33% でトップを独走中^{*24}です。そのため他のクラウドと比べて、使ったことがあって対応可能なエンジニアも多いし、何か困ったときに調べて出てくる情報も多い、というのが、私が AWS を選ぶいちばんの理由です。それ以外だと、利益が出た分だけどんどん投資されてサービスが改良されていくため、細かな使い勝手がどんどん良くなっていく^{*25}ところもポイントです。

クラウドを選ぶ理由、の中でも AWS を選ぶ理由というのは、普遍的な何かがあるわけではなく、本来は使う人やその上で動かすサイトによって異なるはずです。あなたが動かしたいサイトによっては、AWS ではなく他の VPS の方がいいケースだってもちろんあるはずです。これから使ってみて、あなた自身が AWS の良いところを発見できたらいいですね。

*19 実際、オンプレミス環境にある仮想サーバをクラウドサーバと呼んでいるケースも多々あります。

*20 <https://cloud.google.com/>

*21 <https://azure.microsoft.com/ja-jp/>

*22 <https://cloud.sakura.ad.jp/>

*23 <https://www.gmocloud.com/>

*24 2018 年第 1 四半期、クラウドインフラ市場で AWS のシェアは揺るがず 33 %前後、マイクロソフト、Google が追撃、IBM は苦戦中。Synergy Research – Publickey https://www.publickey1.jp/blog/18/20181aws33googleibmsynergy_research.html

*25 画面や機能もどんどん変わっていくので、この後出てくる設定画面も皆さんのが手を動かしてやってみる頃にはキャプチャと違っているかも知れません。AWS のいいところでもあり、マニュアルなどを作つて説明する側にとってはつらいところでもあります。

第 2 章

AWS を使い始めたら最初にやること

この章では AWS の管理画面にサインインして、最初に行うべき設定をします。

2.1 AWS 無料利用枠を使う

AWS を初めて使用する場合、AWS アカウントを作成してから 1 年間は利用料が無料となります。但し、無料利用枠の範囲は決まっており、何をどれだけ使っても無料という訳ではありません。何もかも全部無料だと思ってサーバをバカスカ立てると、あとでクレジットカードにしっかり請求が来ますので注意してください。

どのサービスをどれくらい無料で使えるのか？は「AWS 無料利用枠の詳細 (<https://aws.amazon.com/jp/free/>)」(図 2.1) に「Amazon EC2 は t2.micro インスタンスが月に 750 時間無料」、「Amazon EBS は 30GB 無料」のように細かく書かれていますので、そちらを参照してください。^{*1}



▲図 2.1 AWS 無料利用枠の詳細

なお本著で使用する AWS のサービスは、基本的にこの無料利用枠の範囲内に収まるようになっています。但し、Route53 というネームサーバのサービスについては無料利用枠の対象外であるため、毎月 50 セント程度かかりますのでその点はご留意ください。

うっかり請求が来ても筆者が代わりに支払うことはできません^{*2}ので、後ほど「利用金額が〇円を超えたたらメールで知らせる」という請求アラートの設定をしっかりとおきましょう。

^{*1} EC2 ってなに？ EBS ってなに？ は後述します。

^{*2} できませんできません、人間にはこんなこと絶対にできません。

2.2 AWS のアカウント作成

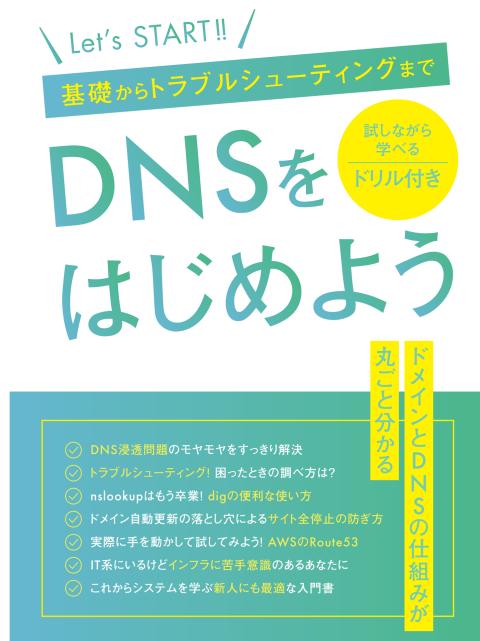
AWS を使うには、先ず AWS アカウントを作成する必要があります。

AWS アカウントの作成は「DNS をはじめよう」(図 2.2)*3 の「第 3 章 AWS のネームサーバ (Route53) を使ってみよう」で済ませていますので、本著でもその AWS アカウントを引き続き使用していきます。

まだ AWS アカウントを持っていない！ 作っていない！ という人は、先に「DNS をはじめよう」で、

- ドメインを買う
- AWS のアカウントを作る
- ネームサーバとして AWS の Route53 を使う

という 3 つのステップを踏んでから、この先へ進むようにしてください。



▲図 2.2 DNS をはじめよう

*3 <https://mochikoastech.booth.pm/>

【コラム】「DNS をはじめよう」はどこで買える？

「AWS をはじめよう」の前作である「DNS をはじめよう」（通称 DNS 本）は書籍版、PDF ダウンロード版とともに BOOTH^aで購入できます。

BOOTH はピクシブ株式会社^bが運営している同人誌の通販、及びダウンロード販売ができるサイトで、書籍版を購入すると 1~2 営業日以内に BOOTH 倉庫からネコポスで本が送られてきます。技術書典で頒布されている同人誌の多くは BOOTH でも購入できますので、気になる方は「技術書典」のタグで検索^cしてみることをお勧めします。

「DNS 本、Amazon で売ってくれないかな？」と思われる方も多いと思うのですが、そもそも Amazon では同人誌が販売できないため、Amazon で売るためには先ずは ISBN コード（商業誌の裏表紙にあるバーコードとその下の番号）を頑張って取らねばなりません。そこに労力を割くよりは、いい本を書く方で頑張ろうと思いますのでどうぞご理解ください。

ちなみに「DNS をはじめよう」は、ただの DNS 好きである筆者が、DNS へのあふれんばかりの愛を早口で詰め込んだ本ですが、技術書典 4 当日に 750 冊、その後もダウンロード販売で売れ続けて累計 1300 冊以上（2018 年 8 月現在）という驚きの頒布数となりました。手にとって、買って、読んでくださった皆さん、ありがとうございます。

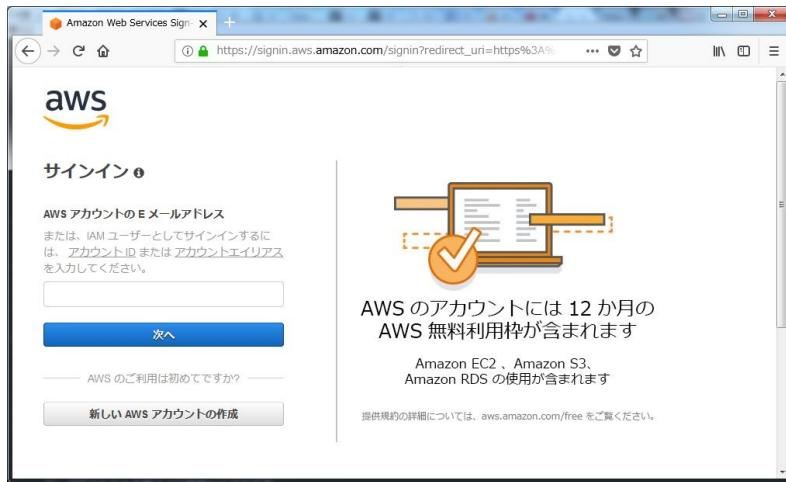
^a <https://mochikoastech.booth.pm/>

^b イラストを投稿できる SNS、pixiv でお馴染み。<https://www.pixiv.net/>

^c <https://booth.pm/ja/search/技術書典>

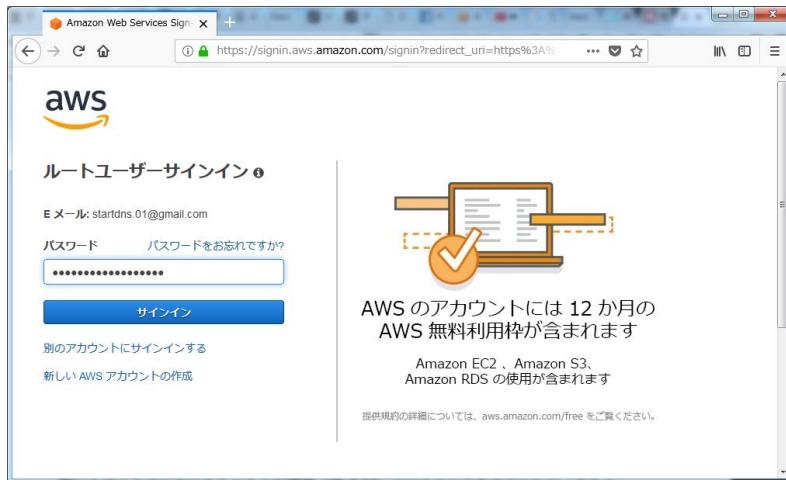
2.3 マネジメントコンソールにサインイン

それでは早速、マネジメントコンソールへのサインイン画面 (<https://console.aws.amazon.com/>) を開いて（図 2.3）、マネジメントコンソールにサインインしましょう。サインインという言葉に馴染みがないかも知れませんが、「ログイン」と同じ意味です。



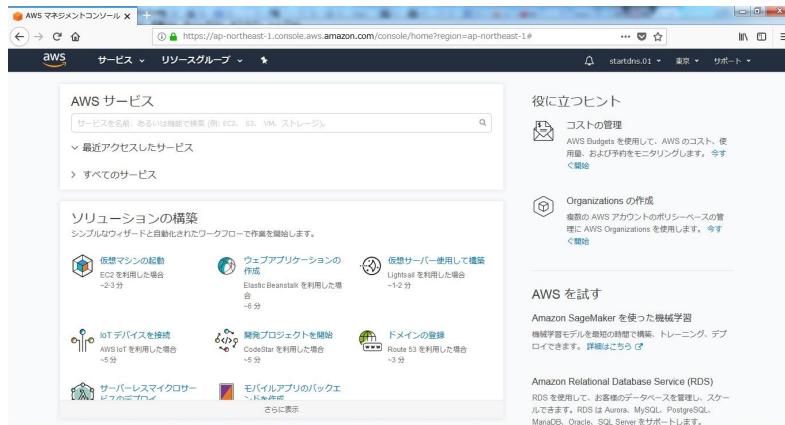
▲図 2.3 マネジメントコンソールのサインイン画面

先ずは AWS アカウントの E メールアドレスを入力して「次へ」、続いてルートユーザー サインインの画面（図 2.4）でパスワードを入力して「サインイン」ボタンを押します。



▲図 2.4 E メールアドレスを入力後、パスワードを入力してサインイン

無事にサインインできたら、マネジメントコンソール（図 2.5）が表示されます。皆さんもサインインできましたか？



▲図 2.5 マネジメントコンソール (AWS の管理画面)

このマネジメントコンソールが、AWS の管理画面となります。これからサーバを立てたりする作業は、すべてこの画面で行っていきます。

2.3.1 【ドリル】AWS の管理画面はなんて名前？

問題

AWS の管理画面はなんと呼ばれているでしょう？

- A. コントロールパネル
- B. マネジメントコンソール
- C. クラウドコンソール

答え _____

解答

正解は B のマネジメントコンソールです。マネジメントコンソールへのサインイン画面 (<https://console.aws.amazon.com/>) からサインインします。AWS を使うときは、このマネジメントコンソールで色々な操作をしますので、サインイン方法をおぼえておいてください。

2.4 IAM でユーザの権限管理

2.4.1 ルートユーザーの普段使いはやめよう

さて、皆さんがあなたのアカウントに使ったのは「ルートユーザー」と呼ばれるユーザです。ルートユーザーは全権を持っていてなんでもできるユーザなので、普段からこのユーザを使って色々な操作をするのはお勧めしません。

「ルートユーザーってなんでもできるユーザなんですよ？ 大は小を兼ねるっていうし、便利なんだからそれ使えばいいじゃない」と思われるかも知れませんが、最寄のスーパーまで晩御飯の買い物に行くだけなのに、1,000万円と利用上限額なしのクレジットカードが詰まったアタッシュケースを持っていく人は居ないですよね？ 子供の財布なら1,000円くらい、自分の財布なら20,000円くらい、のように使う人によって使える金額を制御しておくことで、財布を落としたり盗まれたりしたときのダメージを少なくしておくのは、誰しも無意識にやっているセキュリティ対策だと思います。

AWSのユーザにはクレジットカードを紐付けているのですから、お財布もルートユーザーも等しく扱いには気をつけなければいけません。たとえば悪い人があなたのルートユーザーのEメールアドレスとパスワードを盗んで、こっそりマネジメントコンソールにサインインしたとします。ルートユーザーならなんでもできるので、景気良きいちばん高いサーバ^{*4}を100台立てた^{*5}としましょう。その場合、1日で180万なので、1ヶ月後には5,400万の請求があなたのところへやってきます。（図2.6）

^{*4} EC2のd2.8xlargeというサーバは、東京リージョンだと1時間あたり6.752ドル。日本円にすると1日でおおよそ18,000円です。もちろん大量に立てられないように台数制限はありますが、ルートユーザーならその制限を緩和するリクエストを出すことだって可能です。

^{*5} 悪い人たちは他人のアカウントで高スペックのサーバを大量に立てて、ビットコインを生み出すためのマイニング（採掘）をするのです。



▲図 2.6 「AWS 不正利用」で検索すると不正利用による請求で青ざめた体験記がたくさん

このようにルートユーザーだとなんでもできてしまうため、必要以上に権限のあるルートユーザーを普段使いするのは大変危険です。繰り返しになりますが、1,000万円とクレジットカードが詰まったアタッシュケースを持って、うっきうきでスーパーマーケットに行くのは危ないのでやめましょう。

2.4.2 IAM ユーザを作ろう

という訳でルートユーザではなく、必要な作業ができる権限だけを持った自分用の「IAM ユーザ」というユーザを作つて普段はそちらを使いましょう。

IAM ユーザは 1 人に 1 つ

本著では1人だけで作業をする想定なので、IAM ユーザーも1人しか作りません。ですがもし業務などで複数名でマネジメントコンソールにサインインする場合は、IAM ユーザーは必ず1人につき1つずつ作成してください。まったく同じ作業をするから開発チーム内の A さんと B さんは同じ IAM ユーザを共有すればいいのでは? と思われる場合でも、必ず A さん B さんそれぞれに別々の IAM ユーザーを用意することをお勧めします。

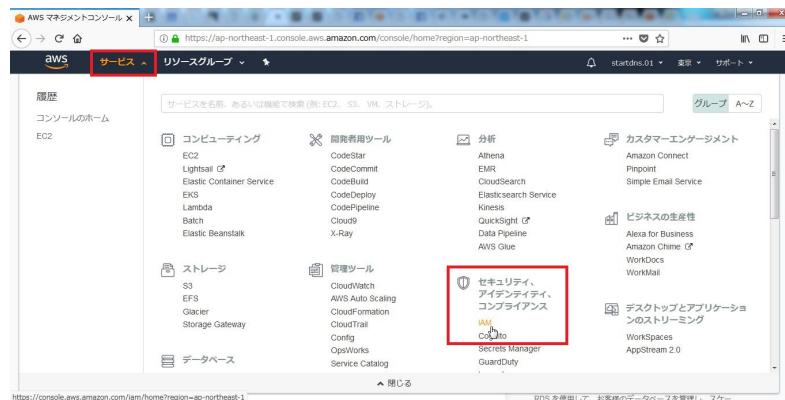
なぜならば AWS では「いつ・どの IAM ユーザーが・なにをしたのか」をすべて記録していて、後から調べることができるのですが、仮に A さんと B さんが1つの IAM ユーザーを共用していた場合、何か重大なトラブルが起きたとき^{*6}に「結局、誰がやらかした

^{*6} 想像もしたくないですが、たとえば誰かがすべてのサーバをバックアップ含めてすべてきれいに削除してしまった、とか。IAM ユーザーを共用していると、使っていた人全員に疑いがかかつてしまます。

のか？」を人単位で追いかけることができなくなってしまうからです。

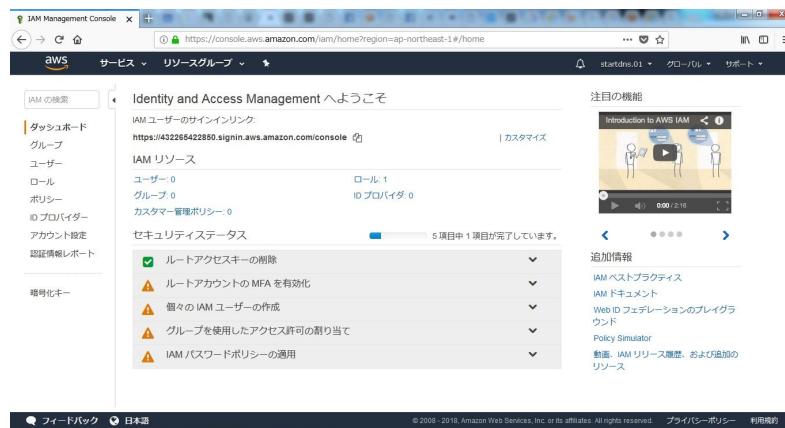
IAM ダッシュボード

それではマネジメントコンソールの左上にある「サービス」から、「セキュリティ、アイデンティティ、コンプライアンス」の下にある「IAM」(図 2.7) をクリックしてください。



▲図 2.7 サービス>セキュリティ、アイデンティティ、コンプライアンス> IAM

「IAM」をクリックすると、IAM のダッシュボード (図 2.8) が表示されます。IAM は Identity and Access Management の略で、AWS の利用を安全に管理するためのサービスです。



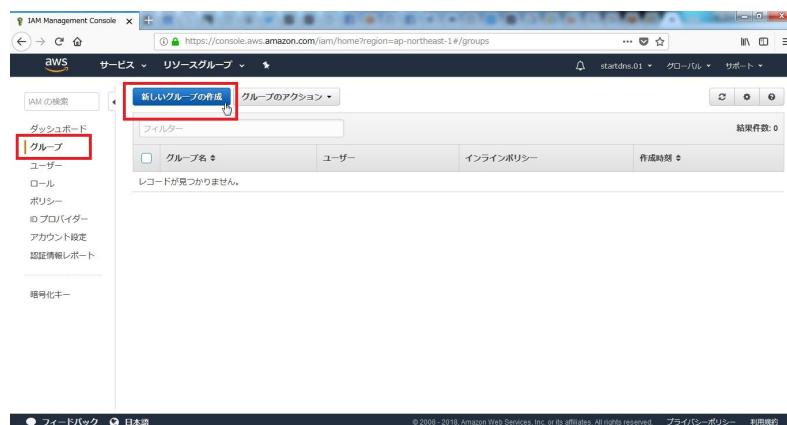
▲図 2.8 IAM ダッシュボード

IAM のグループを作成

では先ず IAM ダッシュボードの左メニューから「グループ」を選んでください。

IAM ではグループを作成して、そのグループに対して権限を設定し、個々の IAM ユーザはグループに所属させることでアクセス権限を管理できます。たとえば前述のような「開発チームの A さんと B さんにはまったく同じ権限を付与したい」という場合に、先に developers というグループを作って、developers グループに権限を付与しておけば、A さん B さんの IAM ユーザは developers グループに所属させるだけで必要な権限を渡すことができます。

今はまだ IAM にグループが 1 つもないため、先ずはグループを作りましょう。左上の「新しいグループの作成」をクリック（図 2.9）します。



▲図 2.9 左メニューの「グループ」>「新しいグループの作成」をクリック

ここから 3 つの手順で新しいグループを作成していきます。

先ずは手順 1 の「グループ名」です。本著では IAM のグループは「start-aws-group」にします。グループ名の欄に「start-aws-group」と入力して、右下の「次のステップ」をクリック（図 2.10）してください。



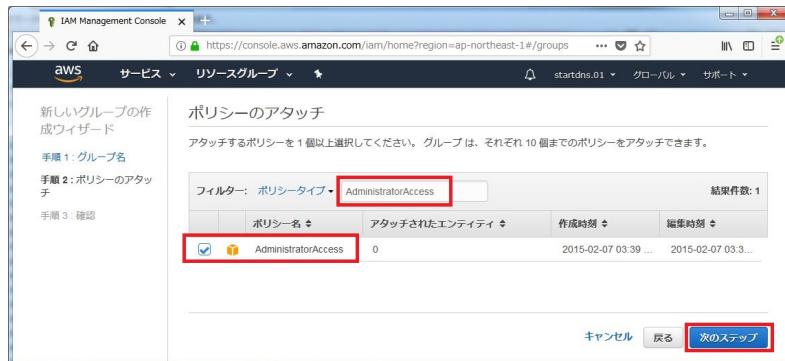
▲図 2.10 グループ名に「start-aws-group」と入力して「次のステップ」をクリック

続いて手順 2 の「ポリシーのアタッチ」でグループに対してポリシーを紐付けます。なんだかものすごくたくさん並んでいますが、それぞれ「どのサービスでどんな操作を許可する」というポリシー（方針）ですので、そこから必要なポリシーを選択してグループにアタッチ（紐付け）していきます。

たくさんあるのでここでは 2 つだけ紹介します。先ほどのルートユーザーと同様に何でもできる 1 番権限の強いポリシーが「AdministratorAccess」です。そして「AdministratorAccess」から IAM に関する権限だけを引いたのが「PowerUserAccess」という、2 番目に権限の強いポリシーです。

本来は必要最小限の権限だけを付与するべきですが、今回は細かな設定はせずにこの 1 番強力な「AdministratorAccess」というポリシーを「start-aws-group」にアタッチします。^{*7} フィルターに「AdministratorAccess」と入力して、下に表示された「AdministratorAccess」にチェックを入れたら、右下の「次のステップ」をクリック（図 2.11）してください。

^{*7} え、大金の詰まったアタッシュケース持って買い物に行っちゃうの？！と思ったあなたは正しいです。ですが、ここでは「普段はルートユーザーではなく IAM ユーザーを使うべき」「本来は IAM ユーザーには必要最小限の権限だけを付与すべき」ということだけ覚えておいて先へ進みましょう。



▲図 2.11 「AdministratorAccess」にチェックを入れて「次のステップ」をクリック

最後に手順 3 の「確認」です。グループ名とポリシーを確認したら、右下の「グループの作成」をクリック（図 2.12）します。

- グループ名 : start-aws-group
- ポリシー : arn:aws:iam::aws:policy/AdministratorAccess



▲図 2.12 グループ名とポリシーを確認して右下の「グループの作成」をクリック

IAM のグループ一覧に、今作ったばかりの「start-aws-group」というグループが表示（図 2.13）されたらグループの作成は完了です。



▲図 2.13 「start-aws-group」というグループが作成できた

IAM のユーザを作成

IAM のグループが作成できたので、続いて IAM ユーザーを作成しましょう。左メニューから「ユーザー」を選ぶと、ユーザーの一覧画面（図 2.14）が表示されます。まだ IAM ユーザーが 1 つも存在しないため、「IAM ユーザーが存在しません。」と表示されています。それでは左上の青い「ユーザーを追加」をクリックしてください。



▲図 2.14 左メニューの「ユーザー」>「ユーザーを追加」をクリック

ここから 3 つのステップで IAM ユーザーを追加していきます。

まずはステップ 1（図 2.15）です。IAM のユーザー名を入力してください。本著では IAM のユーザ名は「start-aws-user」にします。IAM のユーザー名はこの後もサインイン時に使用しますので、もし別のユーザー名にした場合は、しっかりメモしておいてください。

続いてこの IAM ユーザーで AWS にアクセスする方法を選択します。たとえば AWS で「サーバを立てる」「サーバを削除する」などの操作をするには、

1. プログラムから AWS の API を叩いて操作する方法
2. ブラウザでマネジメントコンソールを開いて画面上で操作する方法

の 2 つがあります。本著ではマネジメントコンソールからしか操作しないため、「アクセスの種類」は「AWS マネジメントコンソールへのアクセス」にのみチェックを入れてください。

ユーザー名を入力して、アクセスの種類を選択したら「次のステップ: アクセス権限」をクリックします。



▲図 2.15 ユーザー名を start-aws-user にして、AWS マネジメントコンソールへのアクセスにチェック

続いてステップ 2 (図 2.16) です。先に作っておいた「start-dns-group」というグループに、ユーザーを追加します。「start-dns-group」にチェックを入れたら、「次のステップ: 確認」をクリックしてください。



▲図 2.16 「start-aws-group」にチェックを入れて、「次のステップ: 確認」をクリック

最後にステップ 3 です。次の 4 つを確認して、問題なければ「ユーザーの作成」をクリック（図 2.17）してください。

- ユーザー名が「start-aws-user」であること
- AWS アクセスの種類が「AWS マネジメントコンソールへのアクセス - パスワードを使用」であること
- グループが「start-aws-group」であること
- 管理ポリシーが「IAMUserChangePassword」であること



▲図 2.17 確認して問題なければ「ユーザーの作成」をクリック

「成功」と表示されたら IAM ユーザーの作成は完了です。(図 2.18)



▲図 2.18 「成功」と表示されたら IAM ユーザーの作成完了

この画面で表示される URL の数字 (図 2.19) とパスワード (図 2.20) は、この後サインインするときに使用しますので必ずメモ (表 2.1) しておいてください。



▲図 2.19 URL の数字をメモしておこう

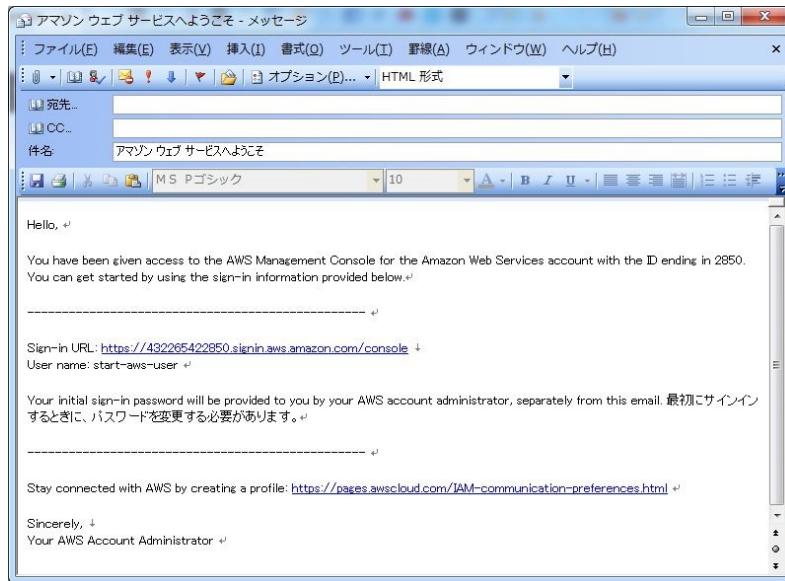


▲図 2.20 パスワードの「表示」をクリックして、パスワードもメモしておこう

メモができたら、続けて右下の「E メールの送信」をクリック (図 2.21) します。サインイン URL や IAM のユーザー名は忘れやすいので、メールでも自分自身宛てに送っておくことをお勧めします。

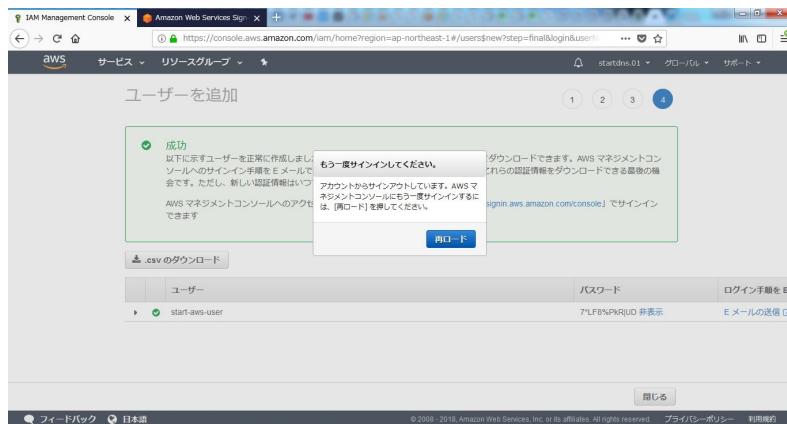
▼表 2.1 IAM ユーザの情報

IAM ユーザー情報	例	自分の IAM ユーザー情報をここにメモ
AWS アカウント (URL の数字)	432265422850	
ユーザー名	start-aws-user	
パスワード	7*LF8%PkR UD	



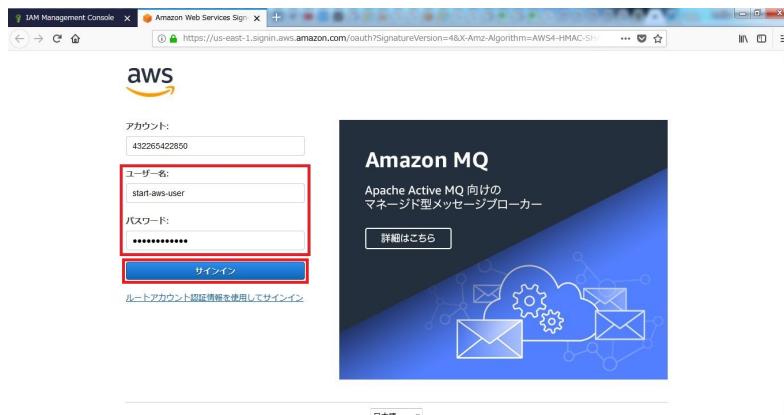
▲図 2.21 サインイン URL や IAM ユーザー名をメールで自分自身宛てに送っておこう

しつかりメモをしてメールも送ったら、画面の「https://*****.signin.aws.amazon.com/console」と書いてある URL をクリックします。するとブラウザの別タブで IAM ユーザーのサインイン画面が開いて、自動的に元のタブのルートユーザーはサインアウト（図 2.22）させられます。サインアウトしてしまったタブは閉じてしまって構いません。



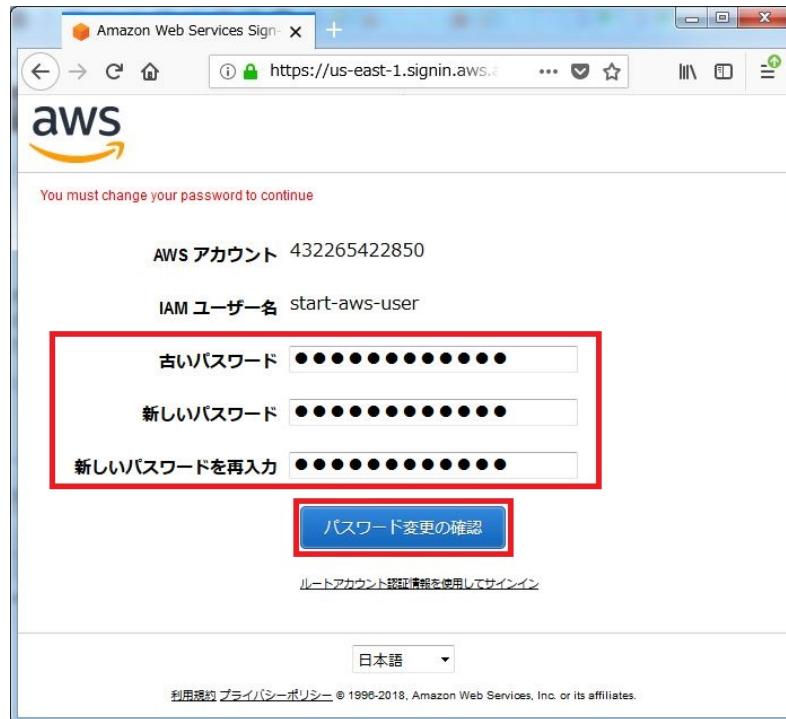
▲図 2.22 ルートユーザーでサインインしていた画面は自動的にサインアウトされる

別タブで開いた IAM ユーザーのサインイン画面（図 2.23）で、先ほどメモしたユーザー名とパスワードを入力して「サインイン」をクリックします。



▲図 2.23 ユーザー名とパスワードを入力して「サインイン」をクリック

サインインすると、新しいパスワードの設定画面（図 2.24）が表示されます。「古いパスワード」に先ほどメモしたパスワードを、「新しいパスワード」には自分で考えたパスワードを入力してください。すべて入力したら「パスワード変更の確認」をクリックします。



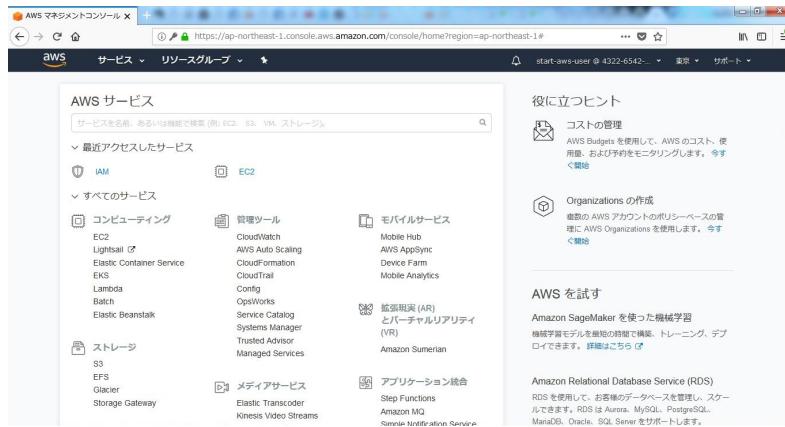
▲図 2.24 新しいパスワードを入力して「パスワード変更の確認」をクリック

ここで再び AWS アカウント、ユーザー名、新しいパスワードをメモ（表 2.2）しておきましょう。

▼表 2.2 IAM ユーザーの情報

IAM ユーザー情報	例	自分の IAM ユーザー情報をここにメモ
AWS アカウント (URL の数字)	432265422850	
ユーザー名	start-aws-user	
新しいパスワード	自作のパスワード	

IAM ユーザーで無事にサインインできたら、マネジメントコンソール（図 2.25）が表示されます。皆さんもサインインできましたか？



▲図 2.25 IAM ユーザーでサインインできた！

右上の IAM ユーザー名をクリック（図 2.26）すると、IAM ユーザー名と AWS アカウントが表示されるので、ルートユーザーではなく IAM ユーザーでサインインしていることが確認できます。



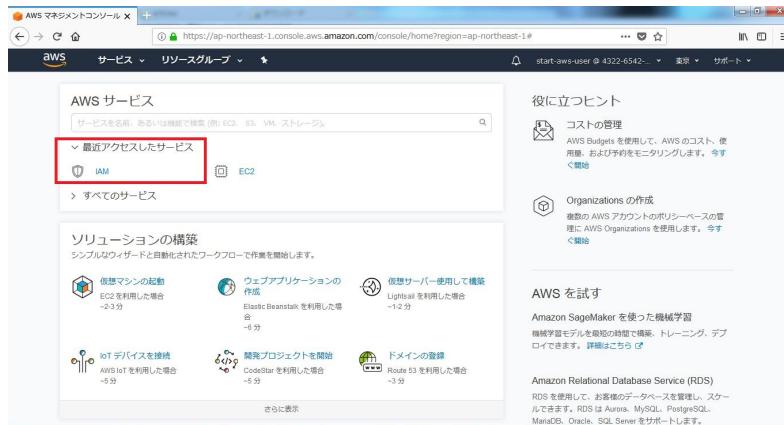
▲図 2.26 IAM ユーザーでサインインしていることを確認

これでルートユーザーではなく、IAM ユーザーでマネジメントコンソールにサインインできるようになりました。

2.4.3 MFA（多要素認証）で不正利用から IAM ユーザーを守る

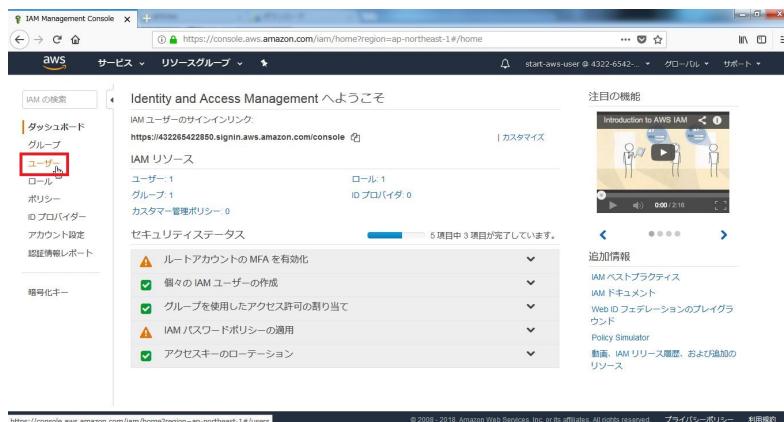
無事に IAM ユーザーでサインインできたら、再び左上にある「サービス」から「IAM」をクリックしてください。もしくは「最近アクセスしたサービス」から「IAM」をクリック

ク（図 2.27）でも構いません。



▲図 2.27 「最近アクセスしたサービス」から「IAM」をクリック

IAM のダッシュボードが表示されたら、左メニューの「ユーザー」をクリック（図 2.28）します。



▲図 2.28 左メニューの「ユーザー」をクリック

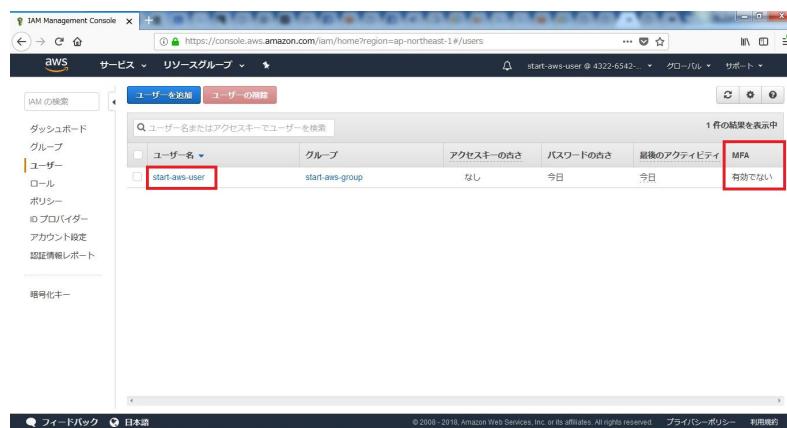
現状は、

- AWS アカウント（12 桁の数字）
- ユーザー名

- パスワード

3つがあれば、IAM ユーザーでサインインできてしまいます。ですが MFA（多要素認証）^{*8}を有効にすると「AWS アカウントとユーザー名とパスワード」に加えて、ユーザーが持っているスマホの認証アプリなど別の要素を使って本人か確認することになるため、より安全にアカウントを管理できます。

今はまだ MFA が有効になっていない（図 2.29）ため、有効にしてみましょう。ユーザー名の「start-aws-user」をクリックします。



▲図 2.29 ユーザー名の「start-aws-user」をクリック

「認証情報」タブの「MFA デバイスの割り当て いいえ」の横にあるエンビツマークをクリック（図 2.30）します。

^{*8} AWS Multi-Factor Authentication の略。

The screenshot shows the IAM Management Console interface. On the left, there's a sidebar with navigation links like 'Dashboard', 'Groups', 'Users', 'Roles', 'Policies', 'AWS Providers', 'Account Settings', and 'Audit Reports'. The main area has a breadcrumb trail: 'Users' > 'start-aws-user'. The 'Overview' tab is selected. It displays the user's ARN (arn:aws:iam:432265422850:user/start-aws-user), a password field, and a creation date (2018-08-13 23:47 UTC+0900). Below this, there are tabs for 'Access Permissions', 'Groups (1)', 'Identity Federation', and 'Access Advisor'. Under 'Identity Federation', it shows a 'Console Login Link' (https://432265422850.sigin.aws.amazon.com/console) and a 'Last Used' date (2018-08-14 21:16 UTC+0900). The 'MFA Device Allocation' section is highlighted with a red box around the '分配' button next to the text '分配済み' (Allocated). At the bottom, there are links for 'Feedback', 'Japanese', and copyright information (© 2008-2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.).

▲図 2.30 「MFA デバイスの割り当て いいえ」の横にあるエンピツマークをクリック

多要素認証をするときは、キーホルダーやカードの形をした専用の MFA デバイス（図 2.31）^{*9}を買って使うか、もしくは「Google 認証システム（Google Authenticator）」というスマホの認証アプリを擬似的な MFA デバイスとして使用します。



▲図 2.31 キーホルダータイプの MFA デバイス

言葉で説明しても分かりにくいと思うので実際にやってみましょう。有効にする MFA デバイスタイプは「仮想 MFA デバイス」を選択（図 2.32）して「次のステップ」をクリックしてください。

^{*9} <https://www.amazon.co.jp/dp/B019THYZGE>



▲図 2.32 「仮想 MFA デバイス」を選択して「次のステップ」をクリック

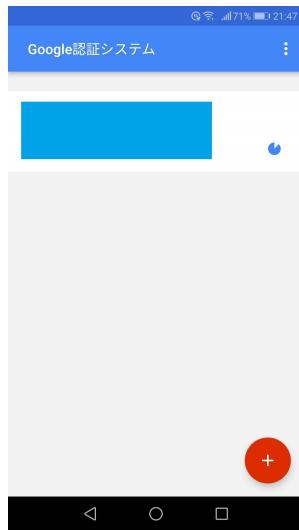
お手元のスマホに「Google 認証システム（Google Authenticator）」をインストール^{*10}したら「次のステップ」をクリック（図 2.33）します。



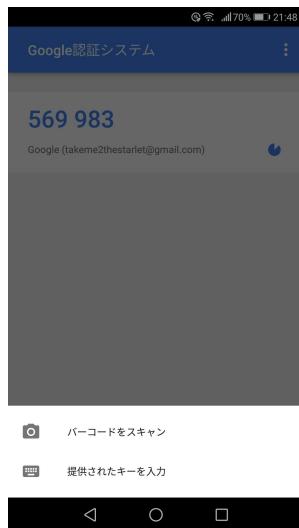
▲図 2.33 スマホに認証アプリをインストールしたら「次のステップ」をクリック

スマホで「Google 認証システム」のアプリを起動したら右下の赤い+ボタンをタッチ（図 2.34）して、「バーコードをスキャン」を選択（図 2.35）します。

^{*10} Android なら <https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2>、iPhone なら <https://itunes.apple.com/jp/app/google-authenticator/id388497605> からインストールできます。Android の場合は元々入っているかも知れません。

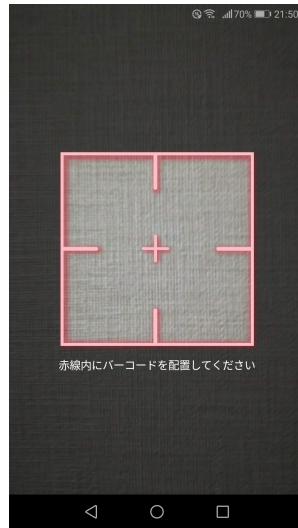


▲図 2.34 「Google 認証システム」のアプリを起動したら右下の赤い+ボタンをタッチ



▲図 2.35 「バーコードをスキャン」を選択

「赤線内にバーコードを配置してください」(図 2.36) と表示されるので、マネジメントコンソールに表示されたバーコード (図 2.37) がスマホの赤枠内に收まるようにします。

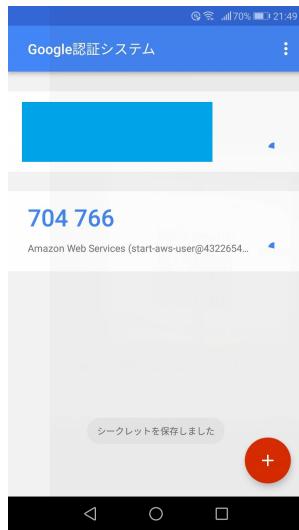


▲図 2.36 「赤線内にバーコードを配置してください」と表示される



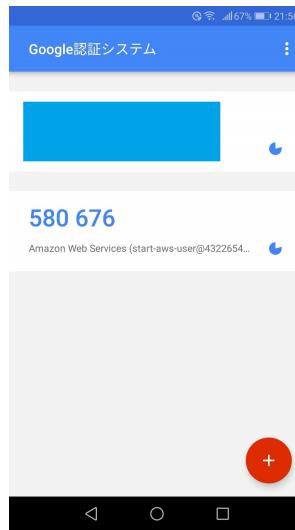
▲図 2.37 マネジメントコンソールに表示されたバーコードをスマホで撮る

すると「Google 認証システム」のアプリで「start-aws-user」用の認証コード（6桁の数字）が表示（図 2.38）されるようになります。



▲図 2.38 「start-aws-user」用の認証コード（6桁の数字）が表示されるようになる

この認証コードは 30 秒ごとに次々と切り替わっていきます（図 2.39）。表示されている認証コードをマネジメントコンソールの「認証コード 1」に入力（図 2.40）したら切り替わるのを待って、次の認証コードを「認証コード 2」に入力します。どちらも入力できたら「仮想 MFA の有効化」をクリックしましょう。

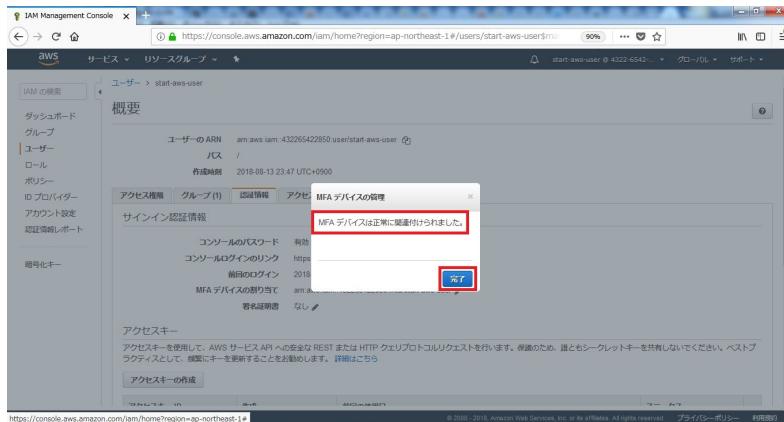


▲図 2.39 認証コードは 30 秒ごとに次々と切り替わる



▲図 2.40 「認証コード 1」と「認証コード 2」を入力して「仮想 MFA の有効化」をクリック

「MFA デバイスは正常に関連付けられました。」と表示（図 2.41）されたら「完了」をクリックしてください。



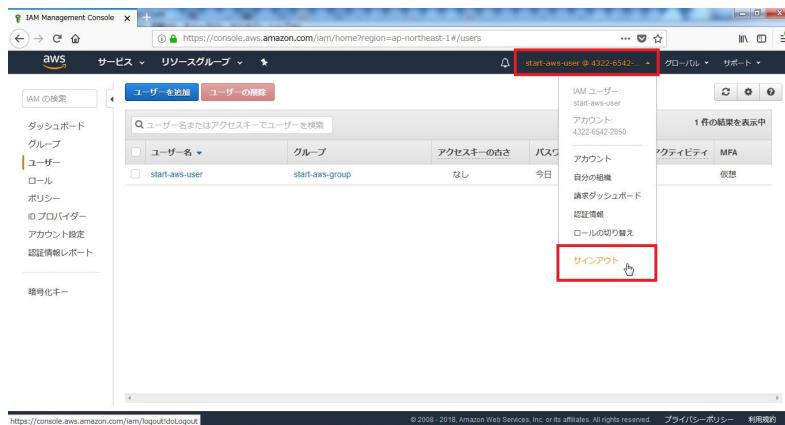
▲図 2.41 「MFA デバイスは正常に関連付けされました。」と表示されたら「完了」をクリック

再び左メニューの「ユーザー」をクリック（図 2.42）してから、右上の更新マークをクリックします。先ほどは「有効でない」になっていた MFA が「仮想」に変わっていたら MFA の設定は完了です。

ユーザー名またはアクセスキーでユーザーを検索	グループ	アクセスキーの古さ	パスワードの古さ	最後のアクティビティ	MFA
start-aws-user	start-aws-group	なし	今日	今日	仮想

▲図 2.42 MFA が「有効でない」から「仮想」に変わっていたら MFA の設定完了

それでは MFA を使ったサインインを試してみましょう！ 右上の IAM ユーザー名から「サインアウト」をクリック（図 2.43）します。



▲図 2.43 「サインアウト」をクリック

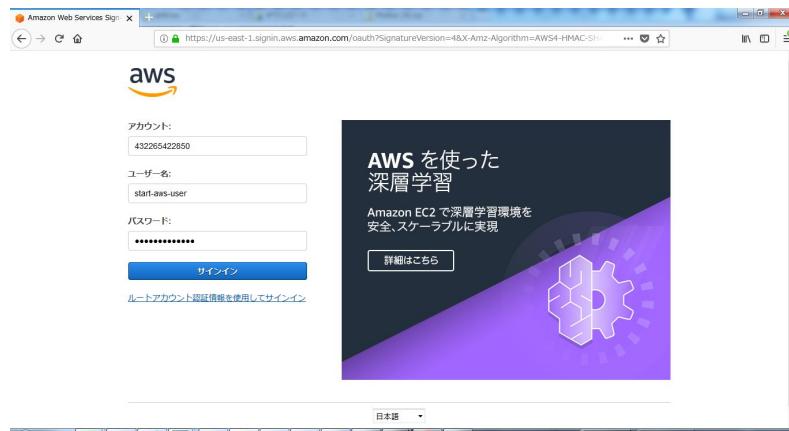
右上の「コンソールへログイン」をクリック（図 2.44）します。



▲図 2.44 「コンソールへログイン」をクリック

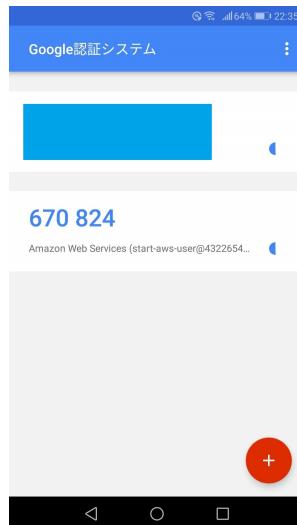
- アカウント（12桁の数字）
- ユーザー名
- パスワード

の3つを入力したら「サインイン」をクリックします。



▲図 2.45 「サインイン」をクリック

今までではこれだけでサインインできていましたが、MFA（多要素認証）が有効になったことで、さらに認証コードも確認されるようになりました。スマホで「Google 認証システム」のアプリを起動（図 2.46）して、表示されている認証コードを「MFA コード」（図 2.47）のところへ入力したら「送信」をクリックしてください。

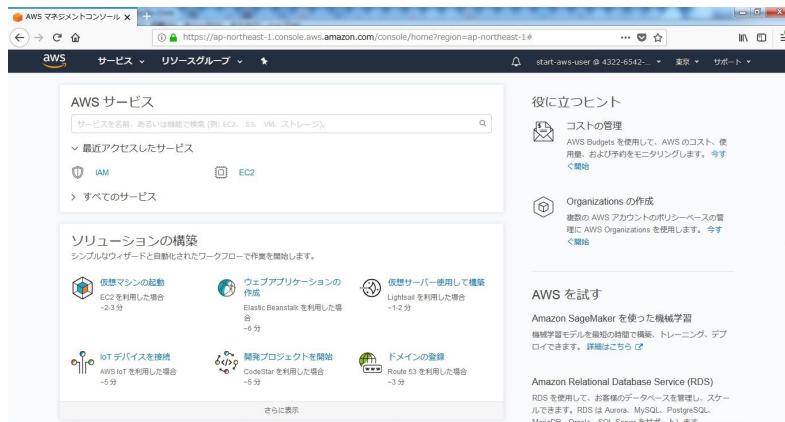


▲図 2.46 スマホで「Google 認証システム」を起動



▲図 2.47 認証コードを「MFA コード」に入力して「送信」をクリック

マネジメントコンソールが表示されたら MFA を用いたサインインは成功です！今後、サインインするときには必ず「Google 認証システム」のアプリが必要になるため、もし IAM ユーザのパスワードが盗まれてしまっても、それだけではサインインできないので安心ですね。

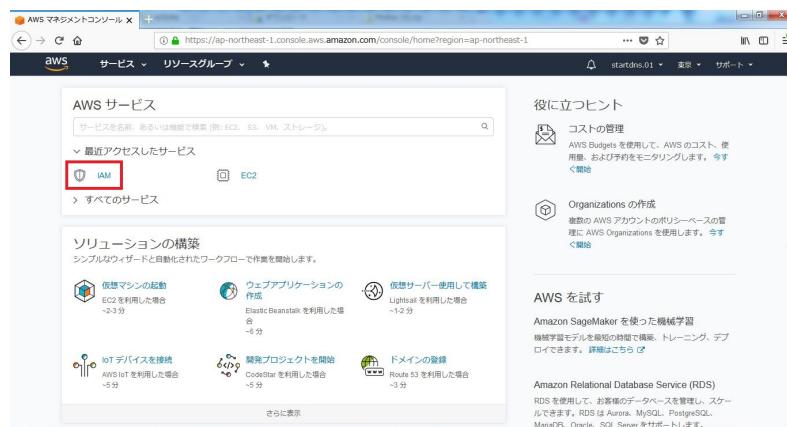


▲図 2.48 MFA を用いたサインインができるようになった！

2.4.4 ルートユーザーも MFA を有効にする

これで IAM ユーザーの「start-aws-user」は MFA が有効になりましたが、ルートユーザーはまだ MFA が有効になっていません。

いったん「start-aws-user」でサインアウトしたら、今度はルートユーザーでサインインしなおしてください。そしてマネジメントコンソールの「最近アクセスしたサービス」から「IAM」をクリック（図 2.49）して IAM のダッシュボードを開きます。



▲図 2.49 ルートユーザーで「最近アクセスしたサービス」から「IAM」をクリック

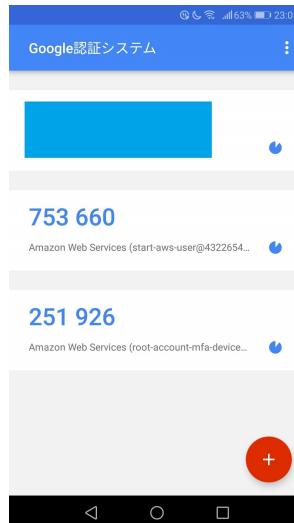
IAM のダッシュボードで「ルートアカウントの MFA を有効化」（図 2.50）^{*11}を開いて「MFA の管理」をクリックします。

^{*11} 突然「ルートアカウント」という言葉が出てきましたがルートアカウントとルートユーザーは同じものです。他にもサインインとログインで揺れでていたりと、AWS では表記揺れはままあることです。日本語の翻訳がおかしいところもあるので、マネジメントコンソールの言語を英語にした方がいいぞ分かりやすいかも知れません。英語が苦手な方は隨時脳内補完しながら頑張りましょう。



▲図 2.50 「ルートアカウントの MFA を有効化」を開いて「MFA の管理」をクリック

ここからは先ほどと同じ手順でルートユーザーでも仮想 MFA を有効にして、サインイン時は「Google 認証システム」を使うようにしておいてください。設定完了すると、Google 認証システムでもルートユーザー用の認証コード（図 2.51）が表示されるようになるはずです。



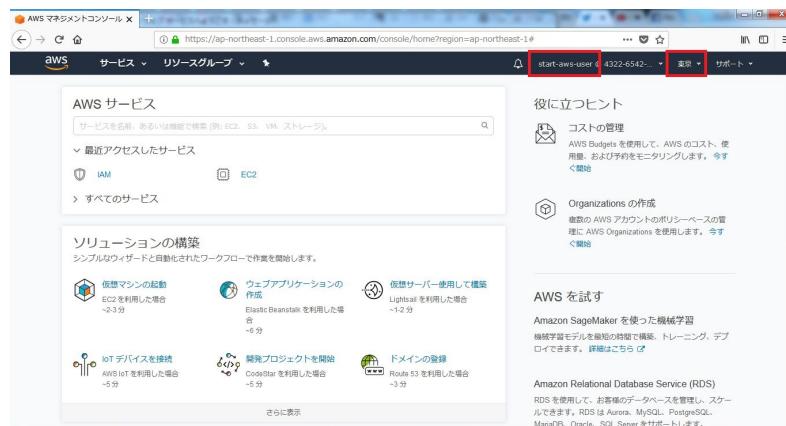
▲図 2.51 ルートアカウント用の認証コード（6桁の数字）も表示されている

ルートアカウントでも MFA が有効になったら、再び「start-aws-user」でサイ

シングしなおして先へ進みましょう。もしもこの URL からサインインするのか分からなくなってしまったら、先ほど送っておいたメールに「Sign-in URL: https://*****.signin.aws.amazon.com/console」という URL があるはずですので、そこをクリックしてサインインしましょう。MFA コードを聞かれたらスマホの Google 認証システムを起動して、表示されている 6 衔の数字を入力します。

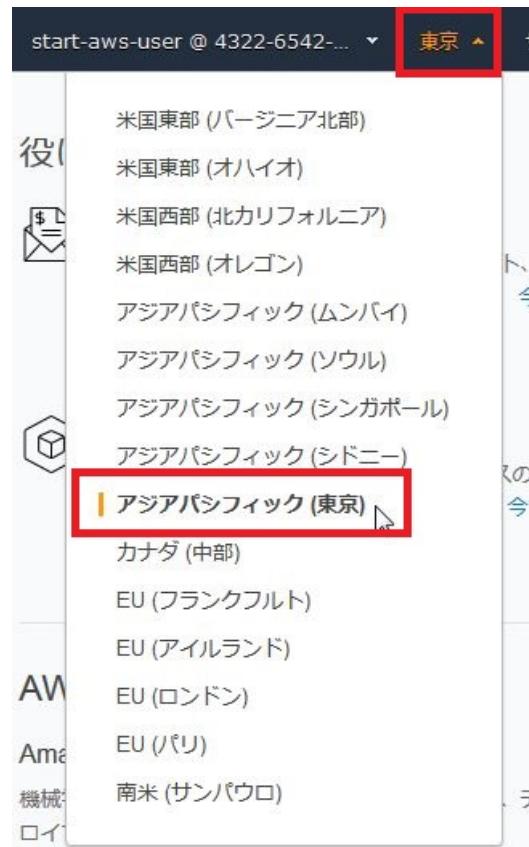
2.5 リージョンの変更

再び「start-aws-user」でサインインしなおして、マネジメントコンソールへ戻ってこられましたか？



▲図 2.52 右上に「start-aws-user」「東京」と表示されていたら OK

マネジメントコンソールの右上（図 2.52）に表示されているユーザー名が「start-aws-user」であること、そしてその右側に表示されているリージョンが「東京」であることを確認してください。ここがもし「東京」以外になっていたら、クリックして「アジアパシフィック（東京）」を選択（図 2.53）してください。選択後、右上が「東京」に変わったらリージョンの変更は完了です。



▲図 2.53 「東京」以外のときはクリックして「アジアパシフィック (東京)」を選択

AWS はバージニア、カナダ、ロンドン、シンガポール、東京など世界の各地域にデータセンターを所有しており、第1章「インフラとサーバってなに？」で詳しくお話ししたようにサーバはそのデータセンターの中にいます。

右上に表示されている「リージョン」とはその各地域の中でどこを使うか？を指定するものです。ウェブサイトにアクセスするとき、パソコンのある場所からサーバまで物理的に距離が遠いと、それだけ通信にも時間がかかるので応答時間も遅くなりますので、日本国内向けにウェブサイトを開設する場合は基本的にこの「東京」リージョンを選びましょう。ただし AWS のサービスによって、まだ東京リージョンが使えないものもあります。その場合は次点として「米国東部 (バージニア北部)」を選択してください。

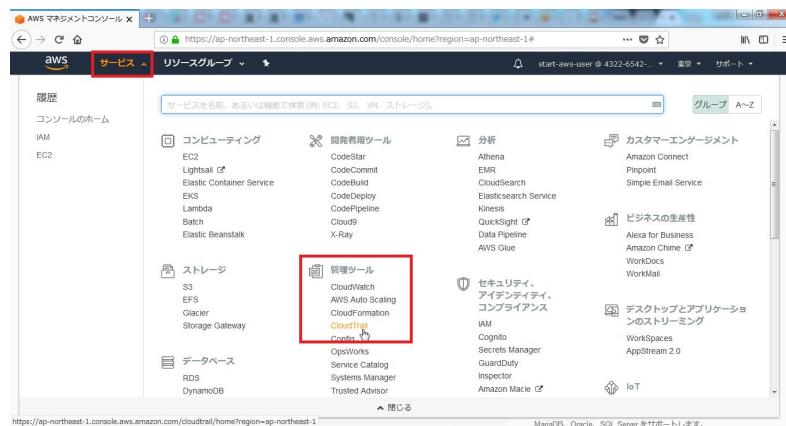
さらにリージョンという地域ごとの区分の下に、さらにアベイラビリティゾーン^{*12}という区分があります。アベイラビリティゾーンの場所は公開されていませんが、たとえば東京リージョンの下に、池袋アベイラビリティゾーンと品川アベイラビリティゾーンがある、というようなイメージです。それぞれのアベイラビリティゾーンは異なる場所に存在し、異なる変電所から電力を供給しています。そのため、もし東京リージョン内でどこかのアベイラビリティゾーンが局地的な災害に遭ったとしても、他のアベイラビリティゾーンは問題なく稼動しているので東京リージョン全体が止まってしまうことはありません。

この後、サーバを立てる際に誤って「東京」以外のリージョンでサーバを立てないように注意をしてください。

2.6 CloudTrail でいつ誰が何をしたのか記録

リージョンの確認が済んだら、続いて CloudTrail（クラウドトレール）を設定へ進みましょう。

それではマネジメントコンソールの左上にある「サービス」から、「管理ツール」の下にある「CloudTrail」（図 2.54）をクリックしてください。



▲図 2.54 サービス>管理ツール>CloudTrail

「CloudTrail」をクリックすると、CloudTrail のダッシュボード（図 2.55）が表示されます。CloudTrail は AWS のマネジメントコンソールや、プログラムを通じて行われた API呼び出しの履歴を保存してくれるサービス・・・と書くと難しいですが、要は「いつ

*12 アベイラビリティゾーンはよく AZ と略されます。

誰が何をしたのか」を記録しておいてくれるサービスです。

The screenshot shows the CloudTrail Management Console dashboard. On the left, there's a navigation menu with 'CloudTrail' selected, and 'イベント履歴' (Event History) is highlighted with a red box. The main area displays a table titled '最近のイベント' (Recent Events) with the following data:

イベント時間	ユーザー名	イベント名	リソースタイプ
2018-08-19, 12:03:08 AM	start-aws-user	DescribeConfigurationRecorder...	
2018-08-19, 12:03:08 AM	start-aws-user	DescribeConfigurationRecorders	
2018-08-19, 12:03:08 AM	start-aws-user	LookupEvents	
2018-08-19, 12:03:00 AM	start-aws-user	DescribeConfigurationRecorder...	
2018-08-19, 12:03:00 AM	start-aws-user	DescribeConfigurationRecorders	

At the bottom of the table, there's a link 'すべてのイベントを表示' (View all events). The right side of the dashboard has a sidebar with '最新情報' (Latest Information) and links like '料金表' (Billing), 'トキュメント' (Documentation), 'フォーラム' (Forum), and 'よくある質問' (FAQ).

▲図 2.55 CloudTrail ダッシュボード

CloudTrail ダッシュボードの左メニューにある「イベント履歴」をクリックして、イベントの一覧を確認してみましょう。CloudTrail はデフォルトで有効になっているため、今まで行ってきた「サインイン」や「IAM ユーザーの作成」などもすべてイベントとして記録されています。たとえばフィルターを「ユーザー名」にして「start-aws-user」で検索（図 2.56）してみると、いつサインインしたのか、いつ MFA（多要素認証）のチェックをしたのか、などが確認できます。^{*13}

^{*13} 表示されているイベント時間は UTC ですので日本時間とはずれています。

2.6 CloudTrail でいつ誰が何をしたのか記録

イベント時間	ユーザー名	イベント名	リソースタイプ	リソース名
2018-08-18, 11:59:23 PM	start-aws-user	DescribeTrails		
2018-08-18, 11:17:08 PM	start-aws-user	ConsoleLogin		
2018-08-18, 11:17:02 PM	start-aws-user	CheckMfa		
2018-08-18, 11:16:56 PM	start-aws-user	ConsoleLogin		
2018-08-18, 11:16:15 PM	start-aws-user	CheckMfa		

▲図 2.56 start-aws-user がいつ何をしたのかすべて表示される

このように CloudTrail では何も設定しなくても、デフォルトで過去 90 日間^{*14}のイベントが無料で記録されています。もし「消した覚えがないのにサーバが跡形もなく消え去っている！」というようなことがあったら、先ず CloudTrail を開いていつ誰がサーバを削除したのか確認してみましょう。

これで「AWS を使い始めたら最初にやるべきこと」はひととおり完了しました。準備万端！ それでは次章でサーバを立てていきましょう！

^{*14} 業務で使うので 90 日よりももっと前の記録も取っておきたい、という場合は「証跡（しょうせき）の作成」を行ってください。

第 3 章

AWS でウェブサーバを立てよう

この章では実際に AWS の EC2 を使ってウェブサーバを立てます。

3.1 EC2でサーバを立てる

いよいよサーバを立てましょう！

3.2 SecurityGroup

3.3 VPC

3.4 EC2

3.4.1 請求アラート

3.4.2 SSHの鍵認証

3.4.3 鍵の変換

3.4.4 ElasticIP

3.4.5 Bastion

第 4 章

サーバのバックアップを取ってお
こう

4.1 AMI

第 5 章

ELB でバランスシングやサーバの台数を管理しよう

5.1 ELB

5.2 Auto Scaling

5.2.1 スケーリングに使える

5.2.2 サーバが 1 台死んでも自動で 1 台立ち上がる

第 6 章

DB サーバを立てよう

6.1 RDS

6.2 Amazon Aurora

第7章

ネームサーバの設定をしよう

7.1 Route53

第 8 章

AWS をやめたくなったらすること

8.1 無料の 1 年が終わる前にすべきこと

8.1.1 【ドリル】サンプル

問題

問題問題

- A. Route53
- B. お名前.com

答え _____

解答

正解は B です。

付録 A

本当の Git

またしても何を言っているのかわからないと思いますが、「Git 用語だけでアイドルソングを作って架空のアイドルに歌わせたい」そんな気持ちで作詞をしてしまいました。大切な事が厳しい時ほど才能が花開いてしまう傾向にある、と言い訳をしたいのですが、本著を書くにあたって最初に着手したのがこの付録だったということは、GitHub でコミットログを見れば一目瞭然です。それでは聞いてください。

A.1 Git - ぎゅっと言えないトウインクル

いま何してる？ リモートのあなた

ガマンできずに フェッチして

髪型変えたの 知ったの

あなたへの気持ち 切なくて

思わずスタッショ したまま ずっと埃つもってる

下駄箱に入れた プルリクエスト

変わっていくわたしを ちゃんとプルして抱きしめて

分かれてしまった ふたりのプランチ

コミットログ読めば あの日の気持ちも分かるはず

たくさんのライバル わたしだけをチェリーピックして

きっとわたし あなたのクローン

フォークしたあの日から ずっとあなたを見つめてる

ステージに上がったら もうコミット逃げられない

ためらわないので オリジンにプッシュ

リバートしたって 過去がなくなるわけじゃない

ただ逆の気持ちで 打ち消しただけ

別々に歩んだ ふたりの過去も

リベースすれば ひとつになれるわ

ねえ いますぐ抱きしめて

ぎゅっと言えない トウインクル

あとがき

2018年10月
mochikoAsTech

Special Thanks:

- プロッコリー好きな茶色い猫に捧ぐ

レビュアー

-

参考書

-

著者紹介

mochiko / @mochikoAsTech

Web 制作会社のシステムエンジニア。モバイルサイトのエンジニア、SIer とソーシャルゲームの広報を経て、2013 年よりサーバホスティングサービスの構築と運用を担当。現在は再び Web アプリケーションエンジニアとしてシステム開発に従事。「分からぬ気持ち」に寄り添える技術者になれるように日々奮闘中。

<https://mochikoastech.booth.pm/> <https://twitter.com/mochikoAsTech>

Hikaru Wakamatsu

表紙デザインを担当。「DNS をはじめよう」の名付け親。

Shinya Nagashio

挿絵デザインを担当。

AWS をはじめよう

2018年10月8日 技術書典5版 v1.0.0

著 者 mochikoAsTech

デザイン Hikaru Wakamatsu / Shinya Nagashio

発行所 mochikoAsTech

印刷所 日光企画

(C) 2018 mochikoAsTech