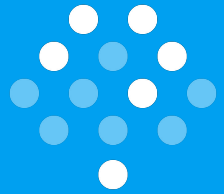
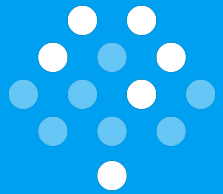


マルチアカウント環境に現代のベストプラクティスを取り入れていく話

株式会社 はてな
SRE 渡辺 道和 (id:nabeop)

2022/4/28
第十七回「アップデート紹介とちょっぴり Dive Deep する AWS の時間」春のセキュリティ編

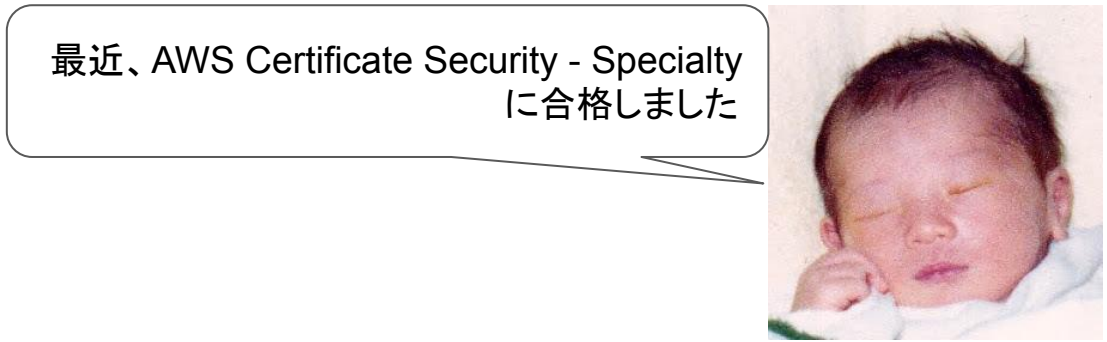


自己紹介

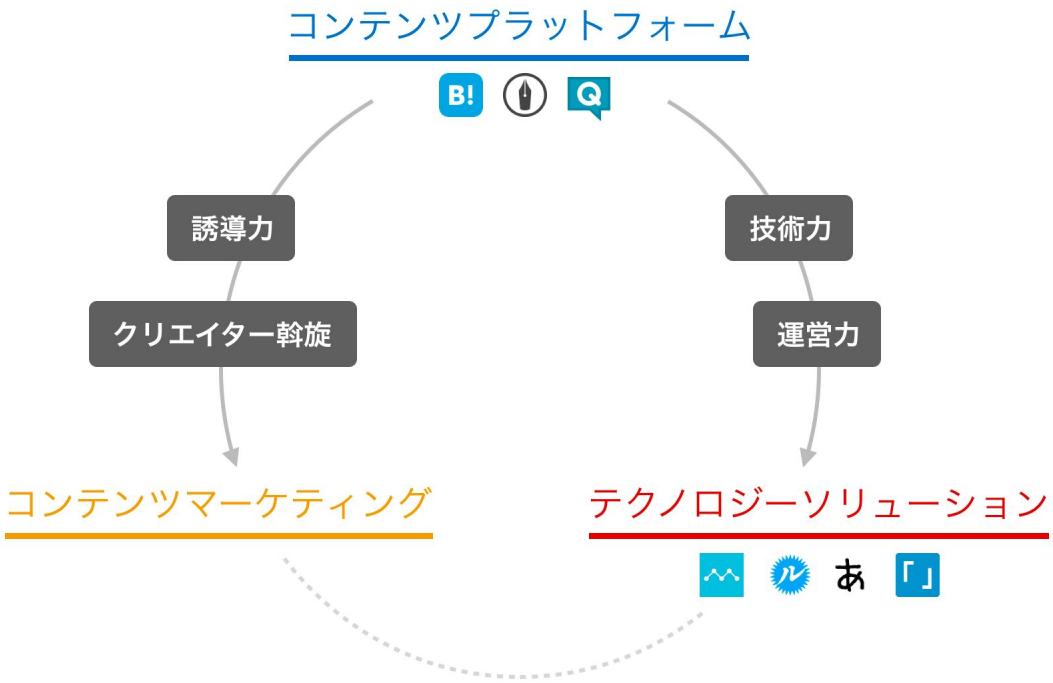
Hatena

株式会社 はてな
サービス・システム開発本部 システムプラットフォーム部
SRE 渡辺 道和 (id:nabeop)

Blog : nabeo がピーしているブログ (仮) / https://nabeop.hatenablog.com/
Twitter : @nabeo / https://twitter.com/nabeo



株式会社 はてな



https://hatenacorp.jp/information

本日の話題

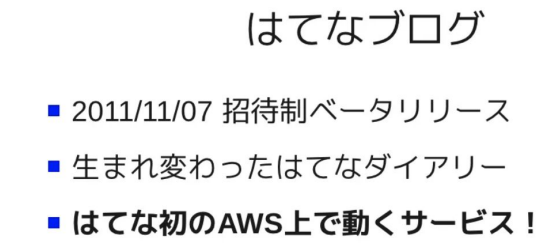
- AWS アカウント運用の再設計に着手した背景
- 再設計にあたり検討した内容
- AWS Control Tower のガードレール設計方針
- まとめ

本日の話題

- AWS アカウント運用の再設計に着手した背景
- 再設計にあたり検討した内容
- AWS Control Tower のガードレール設計方針
- まとめ

はてなにおける AWS アカウント運用の歴史

- はてなで最初に AWS を使用したサービスは
  はてなブログ
- はてなブログからオンプレとクラウドのハイブリッドクラウドでサービスを展開
- 2014年ごろからマルチアカウントを選択
  - ここ数年は積極的にマルチアカウント展開を実施



はてなブログの下側 (2011/11/10 JAWS-UG - Kyoto 勉強会第2回
渡辺 起 (id:wtatsuru)
https://www.slideshare.net/wtatsuru/jawsugkyoto2nd

はてなブログは2021年に10周年🎉

Hatena

https://hatenablog.com/10th

Hatena

つまり、10年モノの AWS アカウント

この10年間でリリースされた AWS サービス（抜粋）

Hatena

- AWS IAM（2011年5月3日 一般公開）
- Amazon VPC（2011年8月4日 リリース）
- AWS CloudTrail（re:Invent 2013 で発表）
- AWS Config（re:Invent 2014 で発表）
  - AWS Config Rule は 2015年10月7日にプレビュー公開
- AWS Organizations（2017年2月27日 一般公開）
- Amazon GuardDuty（re:Invent 2017 で発表）
- AWS Control Tower（2019年6月24日 一般公開）
- AWS Security Hub（2019年6月24 一般公開）

この10年間でリリースされた AWS サービス（抜粋）

Hatena

- AWS IAM（2011年5月3日 一般公開）
- Amazon VPC（2011年8月4日 リリース）
- AWS CloudTrail（re:Invent 2013 で発表）
- AWS Config（re:Invent 2014 で発表）
  - AWS Config Rule は 2015年10月7日にプレビュー公開
- AWS Organizations（2017年2月27日 一般公開）
- Amazon GuardDuty（re:Invent 2017 で発表）
- AWS Control Tower（2019年6月24日 一般公開）
- AWS Security Hub（2019年6月24 一般公開）

10年前には存在していた

追従したけど…

- AWS のベストプラクティスに完全に沿っているとは言いずらい状況
- 無法地帯ではないが、各所にほころびがあることは認識している

AWS アカウント運用の再設計に着手‼

本日の話題

- AWS アカウント運用の再設計に着手した背景
- 再設計にあたり検討した内容
- AWS Control Tower のガードレール設計方針
- まとめ

組織の作り直し or 既存の組織の再編成

Hatena

- 管理アカウントで一部のサービスが運用されている状態
  - 既存の組織をそのまま使うにはメンバーアカウントにサービスを移設する必要がある
  - 完全なサービスの移行は非現実的
- 既存組織の管理アカウントに構築されている一部のサービスをメンバーアカウントへ移設したとして…
  - 新組織に既存の全ての AWS アカウントを移設する工数とほぼ同じ
  - 新組織に既存の全ての AWS アカウントを移設した時と同等のメリットは得られない

組織の作り直しを選択

AWS Control Tower の採用

Hatena

- 今回の再設計のキモの部分
- AWS が推奨しているベストプラクティスに乗りやすい
  - AWS Organizations のメンバーアカウントをガードレールという形で保護できる
    - 管理アカウントはガードレールの適用範囲外ということに注意
  - Audit アカウントや Log Archive アカウントがセットで作成される
- 2021年4月のアップデートで ap-northeast-1 が利用可能になった
  - 後述のリージョン拒否ガードレールの導入でも助かった

re:Invent 2021 の発表内容

Hatena

- 地理的制限ガードレール
- Account Factory for Terraform
- Nested OU

地理的制限ガードレール

Hatena

- リージョン拒否ガードレールは採用
  - 現状で利用実績のあるリージョンと将来的に利用が見込まれるリージョンを管理対象にいれる
  - 想定外のリージョンでリソースが作成されることを防ぐ
- いくつかのガードレールは導入することにした

Account Factory for Terraform (AFT)

Hatena

- Account Factory でフォローされないプロビジョニングが Terraform で可能になる
- 専用の AWS アカウントが必要など仕組みが大掛かり
- AWS アカウント単位で適用されるため、意図したリソースが作られているかなどテストの仕組みを整えるコストが大きい
- AWS Organizations との連携が弱く、OU を移動したときに AFT によるプロビジョニングが実行されないように見える

現時点では時期尚早として採用は見送り

Nested OU

Hatena

- OU を階層化して実組織の構成を AWS Organizations の組織に反映できる
- 現状の AWS アカウント数では Nested OU を積極的に取り入れるメリットは少ない
- 想定しているユースケースと比較して機能的に取り回しが悪い
  - SCP 製のガードレールだけ伝播して、AWS Config 製のガードレールは OU ごとに適用する必要がある
  - SCP のガードレールでドリフトが発生したときは OU 全体に波及する

ユースケースが合わないため、採用は見送り

本日の話題

- AWS アカウント運用の再設計に着手した背景
- 再設計にあたり検討した内容
- AWS Control Tower のガードレール設計方針
- まとめ

AWS Well-Architected Tool FTR Lens

Hatena

- ゴールイメージの明確化
- AWS が考えるセキュリティや信頼性と運用性についてのベストプラクティス
  - AWS アカウント運用の再設計にあたり、FTR の取得は必須ではない
  - 設計時に FTR で求められる基準を意識することで、ベストプラクティスを効率よく取り込めると判断した
- 実際に FTR Lens の結果などを見つつ、ガードレールを選択する
  - **ガードレールを採用する ≠ FTR の認定を得られる** ということに注意!!
  - ガードレールだけではなく、他の AWS サービスを組み合わせたり、運用ドキュメントの整備などが必要

はてなにおける権限移譲の考え方

Hatena

- 最優先:
  - 各開発チームに技術選択の裁量と責任が任されており、自身のサービスで最適と思われるサービスや技術スタックを選択できる
- とはいえ…
  - AWS アカウントのセキュリティ周りについては最高の状態にしておきたい

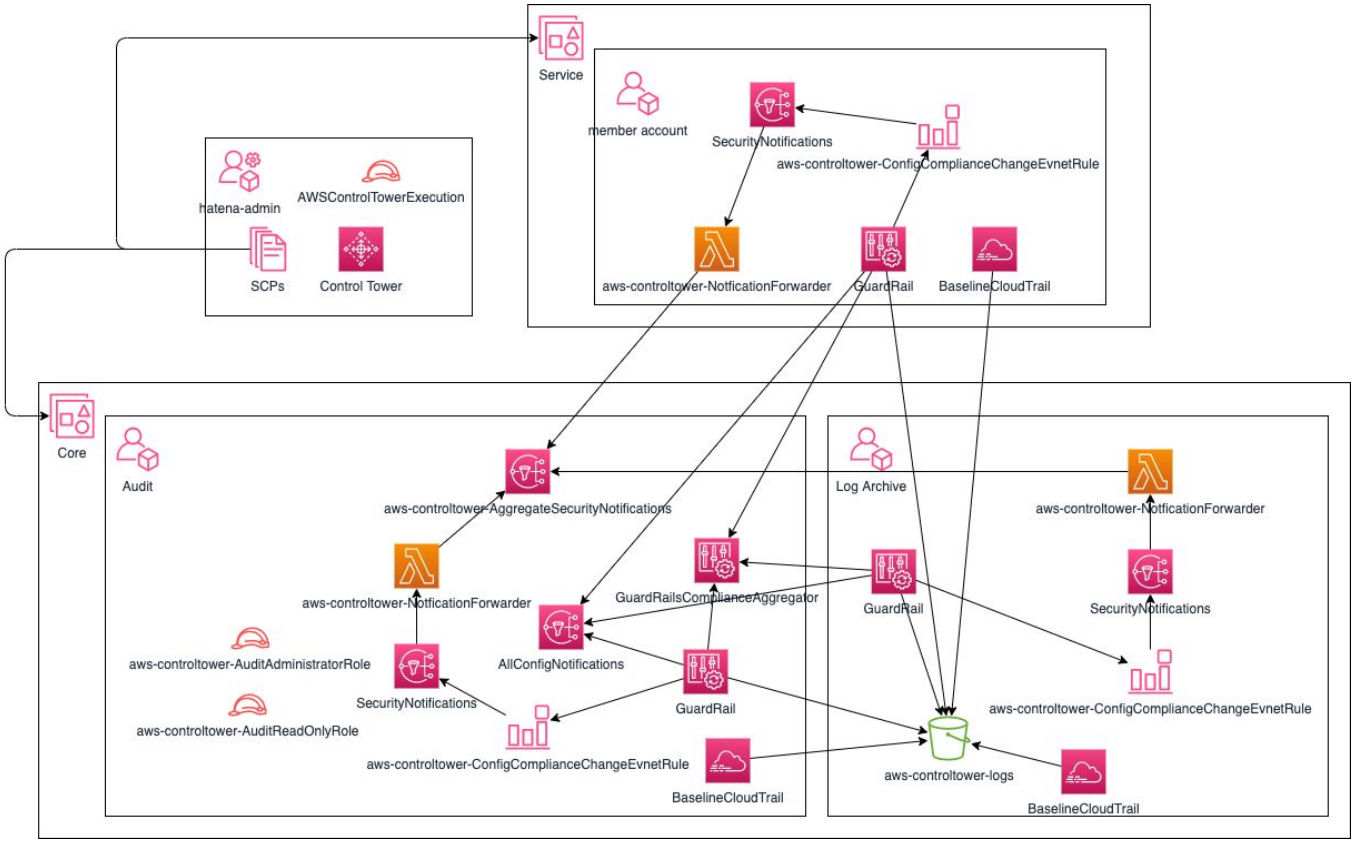
最高の状態 #とは

Hatena

- メンバーアカウントの管理者（開発チームのエンジニア）が意識せずに安全な状態で AWS アカウント内でリソースを作って運用できる
  - AWS Control Tower の「ガードレール」
    - なるべく強い権限を持つことはできるが、ガードレールを超えないことで AWS アカウントの基盤部分を安全な状態で保つ
  - ガードレールでカバーできない部分は AWS のセキュリティ系サービスの組み合わせやガイドラインの整備などで対応する

AWS Control Tower のガードレール概要

Hatena



ガードレールの選択方針

Hatena

- FTR Lens の内容とガードレールの内容、構築されている既存サービスとのバランス
- 予防的ガードレールと検出的ガードレール
  - 予防的ガードレールの適用は慎重に
  - 検出的ガードレールの適用は気軽に

ガードレールの選択方針

Hatena

- AWS アカウントをユースケースごとに分類
  - ユースケースごとに選択的ガードレールからいくつかピックアップしている
  - 後からガードレールの追加/削除できるようにしておく
- 意図していない場所にリソースを作らないようにする
  - 地理的ガードレールの採用
  - 新規のリージョンの使用を開始するときの手順の整備

AWS アカウントのユースケースの分類

Hatena

- ケース A : 組織の管理アカウント
  - AWS Organizations における管理アカウント
  - ガードレールは適用されない
- ケース B : 組織のセキュリティを確保するために必要なアカウント
  - Audit アカウントや Log Archive アカウント
- ケース C : サービスを構築しているアカウント
  - Workloads OU に所属する AWS アカウントが一番近い
- ケース D : 共通のリソースを構築しているアカウント
  - Infrastrastructure OU に所属する AWS アカウントが一番近い
- ケース E : その他
  - ケース C と似ているが、特定の開発チームに紐付かない
    - ex. ハンズオンなど期間限定で使用する

本日の話題

- AWS アカウント運用の再設計に着手した背景
- 再設計にあたり検討した内容
- AWS Control Tower のガードレール設計方針
- まとめ

まとめと今後の展望

Hatena

- AWS Control Tower は AWS が提唱するベストプラクティスに沿ったマルチアカウント運用を効率よく導入できそう
- AWS Organizations の組織移動には他にも考慮するべき内容がある

俺たちの戦いはこれからだ！！

nabeop 先生の次回作にご期待ください

SRE 積極採用中!!!