JANOG 45 Meeting 「常識が変わる責任共有のカタチ」

責任共有モデルとWell-Architectedの取り組み

中島 智広
セキュリティソリューションアーキテクト
アマゾン ウェブ サービス ジャパン株式会社
2020/01/24

自己紹介

中島　智広（Tomohiro Nakashima）

AWS Security Solutions Architect
お客様のセキュリティの取り組みをクラウド利活用の視点からご支援

Background

前職時代にASやデータセンターネットワーク等、オンプレミスのインフラ設計・運用に従事、JANOGとはその頃からのご縁

本発表の目的

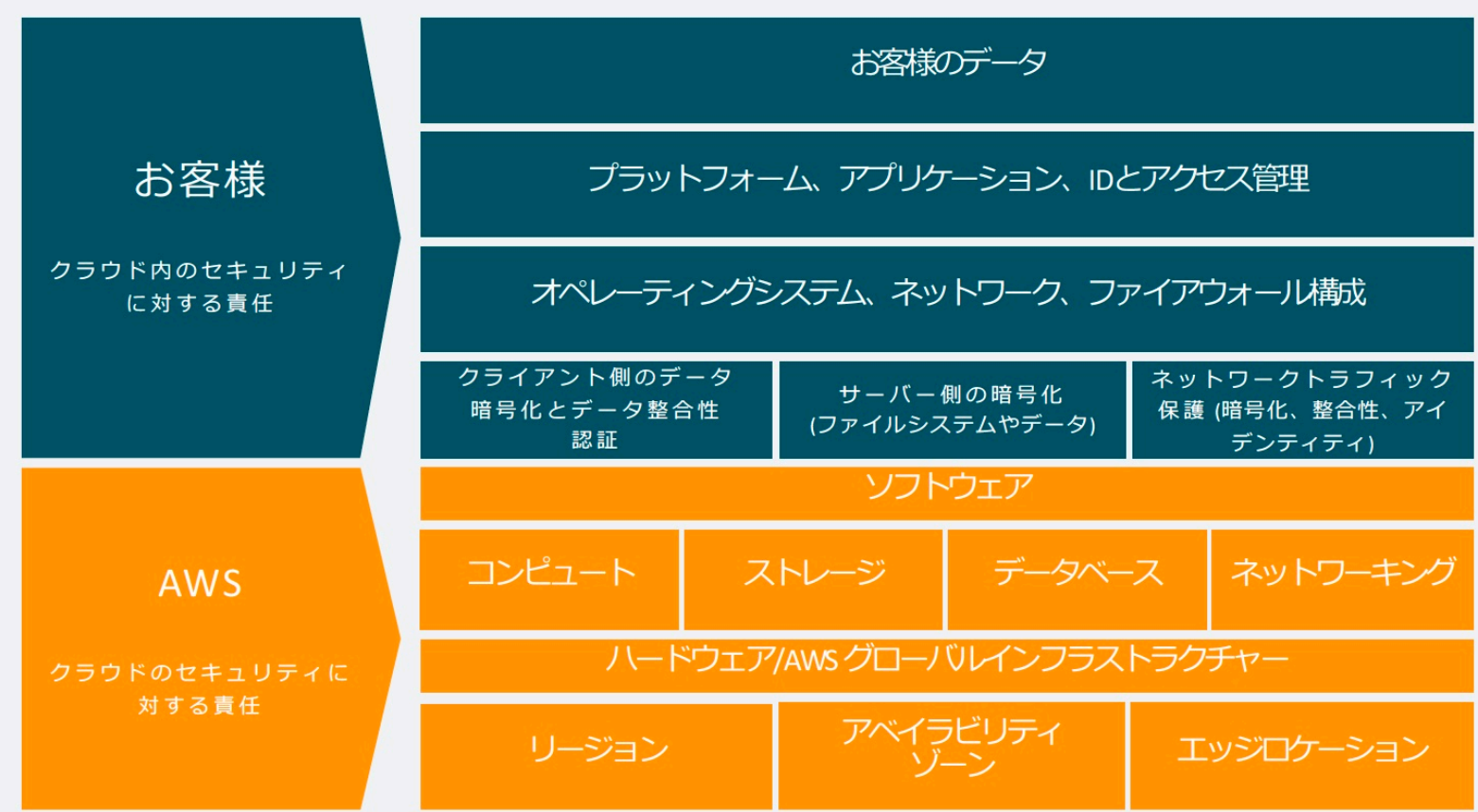
クラウドが前提としている
“責任共有モデル”の考え方を理解する

クラウドの設計・運用で取り組まれている
Well-Architectedの取り組み概要や効能を理解する

(これらを理解した上で、設計・構築・運用を行うことで…)
オンプレミスやハイブリッド環境における
事業者と利用者のよりよい関係を考えるきっかけ作り

責任共有モデル

責任共有モデル



前提となる重要なこと

“Everything fails all the time.”

すべてのものはいつでも壊れうる

—Werner Vogels, CTO AWS

責任共有モデルの下では、たとえば

複数のアベイラビリティゾーンにアプリケーションを配置することによって自然災害やシステム障害に備えるのは？

データのバックアッププランを管理するのは？

責任共有モデルの下では、たとえば

複数のアベイラビリティゾーンにアプリケーションを配置することによって自然災害やシステム障害に備えるのは？

データのバックアッププランを管理するのは？

いずれもお客様の責任です。
（そしてそのことを繰り返しお伝えしています）

aws

責任共有は効果的

- Facilities
- Physical security
- Compute infrastructure
- Storage infrastructure
- Network infrastructure
- Virtualization layer (EC2)
- Hardened service endpoints
- Rich IAM capabilities

+

- Network configuration
- Security groups
- OS firewalls
- Operating systems
- Application security
- Proper service configuration
- AuthN and account management
- Authorization policies

=

単一の事業体よりも、より安全で堅牢なシステムが構築可能

すなわち

Design for Failureを前提として
事業者/利用者のやるべきことへの集中をもたらす
これが**責任共有モデル**です。

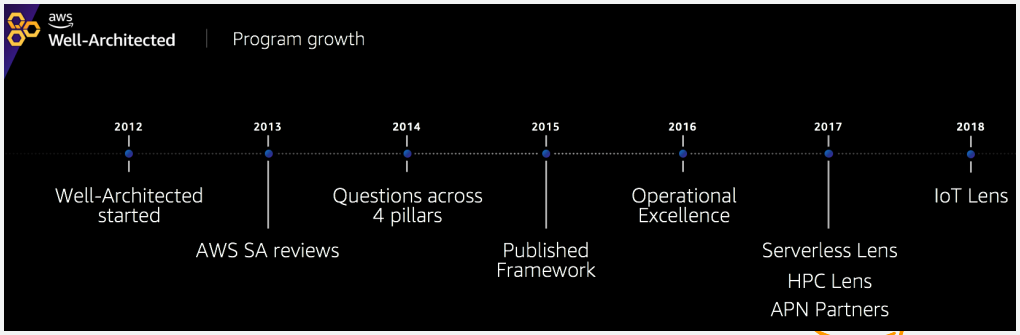
Well-Architectedの取り組み

AWS Well-Architected Framework(W-A)とは?

システム設計・運用の”大局的な”考え方と
ベストプラクティス集

- AWSのソリューションアーキテクト(SA)と**お客様**が
  長年にわたり**数多くの経験**から作り上げたもの

- AWSと**お客様**と共に、
  W-Aも**常に進化し続ける**



Well-Architected 5つの柱

運用の優秀性

セキュリティ

信頼性

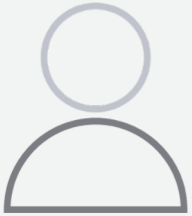
パフォーマンス効率

コストの最適化

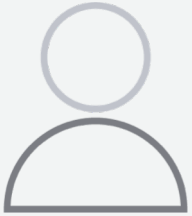
あくまでも設計”原則“なので、実装の詳細や
アーキテクチャパターンは扱っていない

aws

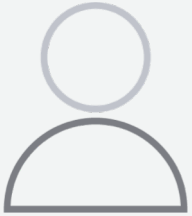
レビューに取り組まれたユーザーの声



網羅的なチェックリストにより、**サービス開始前に**
セキュリティや信頼性のリスクを発見できて非常によかった



オンプレミスからの移行だったが「**漠然とAWSを100%活用できてない。なんとかしないと…**」とは思っていた。
最適化や改善すべきポイントが明確になってよかった



自社の設計に対して、**AWSのベストプラクティスとの**
答え合わせが出来てよかった。自信を持てた

Well-Architected レビューのさらなる効能

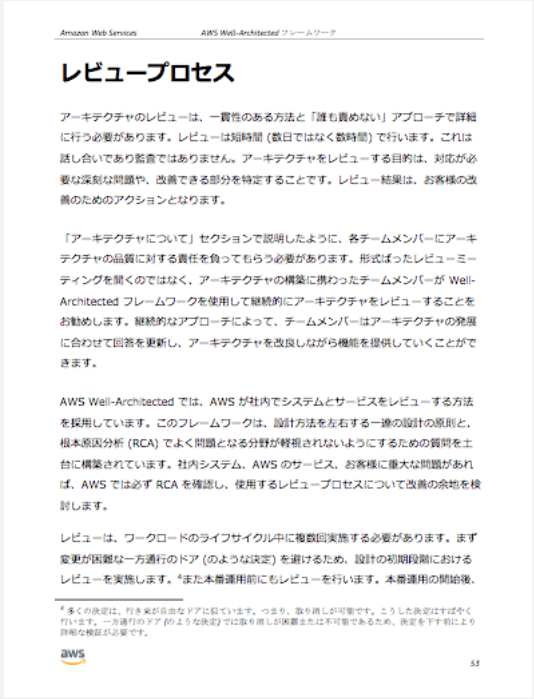
一度だけではなく、定期的な取り組みにより…

- システムの脆弱性やベストプラクティスとの乖離について、お客様と定期的に認識を共有（＝定期健康診断）

- 障害が生じる前に予防的対策に取り組むきっかけ
- 障害が生じた際にも発展的な会話をしやすくなる
- 障害を予防するノウハウがお客様社内に蓄積される

レビューの進め方に秘訣あり

重要なのでホワイトペーパーでは3ページも解説しています



Amazon Web Services　AWS Well-Architected フレームワーク

レビュープロセス

アーキテクチャのレビューは、一貫性のある方法と「誰も責めない」アプローチで詳細に行う必要があります。レビューは短時間 (数日ではなく数時間) で行います。これは話し合いであり監査ではありません。アーキテクチャをレビューする目的は、対応が必要な深刻な問題や、改善できる部分を特定することです。レビュー結果は、お客様の改善のためのアクションとなります。

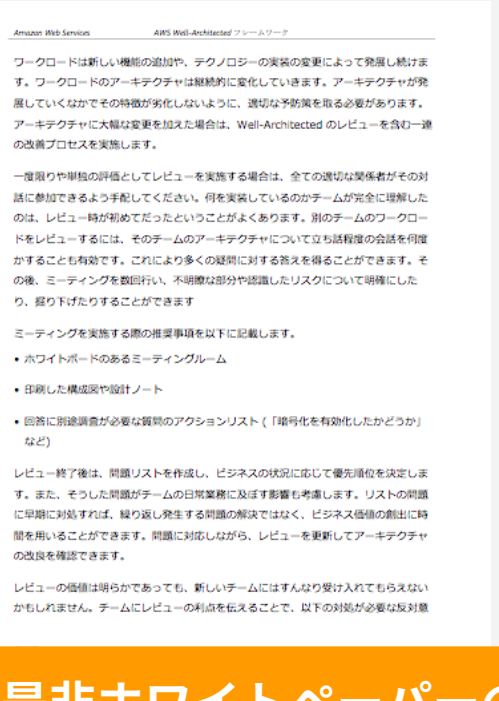
「アーキテクチャについて」セクションで説明したように、各チームメンバーにアーキテクチャの品質に対する責任を負ってもらう必要があります。形式ばったレビューミーティングを開くのではなく、アーキテクチャの構築に携わったチームメンバーが Well-Architected フレームワークを使用して継続的にアーキテクチャをレビューすることをお勧めします。継続的なアプローチによって、チームメンバーはアーキテクチャの発展に合わせて回答を更新し、アーキテクチャを改良しながら機能を提供していくことができます。

AWS Well-Architected では、AWS が社内でシステムとサービスをレビューする方法を採用しています。このフレームワークは、設計方法を左右する一連の設計の原則と、根本原因分析 (RCA) でよく問題となる分野が軽視されないようにするための質問を土台に構築されています。社内システム、AWS のサービス、お客様に重大な問題があれば、AWS では必ず RCA を確認し、使用するレビュープロセスについて改善の余地を検討します。

レビューは、ワークロードのライフサイクル中に複数回実施する必要があります。まず変更が困難な一方通行のドア (のような決定) を避けるため、設計の初期段階におけるレビューを実施します。[4]また本番運用前にもレビューを行います。本番運用の開始後、

[4] 多くの決定は、行き来が自由なドアに似ています。つまり、取り消しが可能です。こうした決定はすばやく行います。一方通行のドア (のような決定) では取り消しが困難または不可能であるため、決定を下す前により詳細な検証が必要です。

aws　53



Amazon Web Services　AWS Well-Architected フレームワーク

ワークロードは新しい機能の追加や、テクノロジーの実装の変更によって発展し続けます。ワークロードのアーキテクチャは継続的に変化していきます。アーキテクチャが発展していくなかでその特徴が劣化しないように、適切な予防策を取る必要があります。アーキテクチャに大幅な変更を加えた場合は、Well-Architected のレビューを含む一連の改善プロセスを実施します。

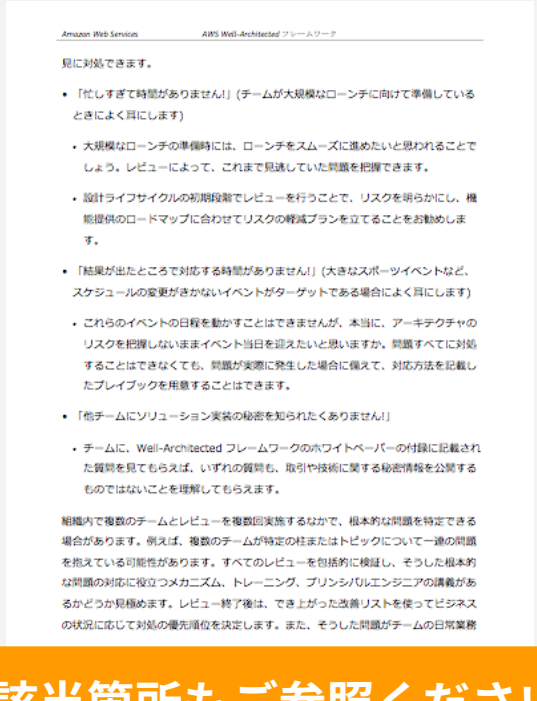
一度限りや単独の評価としてレビューを実施する場合は、全ての適切な関係者がその対話に参加できるよう手配してください。何を実装しているのかチームが完全に理解したのは、レビュー時が初めてだったということがよくあります。別のチームのワークロードをレビューするには、そのチームのアーキテクチャについて立ち話程度の会話を何度かすることも有効です。これにより多くの疑問に対する答えを得ることができます。その後、ミーティングを数回行い、不明瞭な部分や認識したリスクについて明確にしたり、掘り下げたりすることができます

ミーティングを実施する際の推奨事項を以下に記載します。

- ホワイトボードのあるミーティングルーム
- 印刷した構成図や設計ノート
- 回答に別途調査が必要な質問のアクションリスト (「暗号化を有効化したかどうか」など)

レビュー終了後は、問題リストを作成し、ビジネスの状況に応じて優先順位を決定します。また、そうした問題がチームの日常業務に及ぼす影響も考慮します。リストの問題に早期に対処すれば、繰り返し発生する問題の解決ではなく、ビジネス価値の創出に時間を用いることができます。問題に対応しながら、レビューを更新してアーキテクチャの改良を確認できます。

レビューの価値は明らかであっても、新しいチームにはすんなり受け入れてもらえないかもしれません。チームにレビューの利点を伝えることで、以下の対処が必要な反対意



Amazon Web Services　AWS Well-Architected フレームワーク

見に対処できます。

- 「忙しすぎて時間がありません!」(チームが大規模なローンチに向けて準備しているときによく耳にします)
  - 大規模なローンチの準備時には、ローンチをスムーズに進めたいと思われることでしょう。レビューによって、これまで見逃していた問題を把握できます。
  - 設計ライフサイクルの初期段階でレビューを行うことで、リスクを明らかにし、機能提供のロードマップに合わせてリスクの軽減プランを立てることをお勧めします。
- 「結果が出たところで対応する時間がありません!」(大きなスポーツイベントなど、スケジュールの変更ができないイベントがターゲットである場合によく耳にします)
  - これらのイベントの日程を動かすことはできませんが、本当に、アーキテクチャのリスクを把握しないままイベント当日を迎えたいと思いますか。問題すべてに対処することはできなくても、問題が実際に発生した場合に備えて、対応方法を記載したプレイブックを用意することはできます。
- 「他チームにソリューション実装の秘密を知られたくありません!」
  - チームに、Well-Architected フレームワークのホワイトペーパーの付録に記載された質問を見てもらえば、いずれの質問も、取引や技術に関する秘密情報を公開するものではないことを理解してもらえます。

組織内で複数のチームとレビューを複数回実施するなかで、根本的な問題を特定できる場合があります。例えば、複数のチームが特定の柱またはトピックについて一連の問題を抱えている可能性があります。すべてのレビューを包括的に検証し、そうした根本的な問題の対応に役立つメカニズム、トレーニング、プリンシパルエンジニアの講義があるかどうか見極めます。レビュー終了後は、でき上がった改善リストを使ってビジネスの状況に応じて対処の優先順位を決定します。また、そうした問題がチームの日常業務

是非ホワイトペーパーの該当箇所もご参照ください

Well-Architected レビューのポイント

ホワイトペーパーより抜粋①

- レビューは「誰も責めない」アプローチで行う必要があります。
  これは話し合いであり、監査ではありません

- レビューはワークロードのライフサイクル中に複数回実施する必要があります。まず変更が困難な一方通行のドア (のような決定) を避けるため、設計の初期段階におけるレビューを実施します。

是非ホワイトペーパーもお読みください

Well-Architected レビューのポイント

ホワイトペーパーより抜粋②

- レビューを実施する場合は、全ての適切な関係者がその対話に参加できるよう手配してください。何を実装しているのかチームが完全に理解したのは、レビュー時が初めてだったということがよくあります。

是非ホワイトペーパーもお読みください

Well-Architected レビューのポイント

ホワイトペーパーより抜粋③

- アーキテクチャの構築に携わったチームメンバーが W-Aフレームワークを使用して継続的にアーキテクチャをレビューすることをお勧めします

- また本番運用前にもレビューを行います。本番運用の開始後、ワークロードは新しい機能の追加や、テクノロジーの実装の変更によって発展し続けます。ワークロードのアーキテクチャは継続的に変化していきます。

すなわち

クラウドではWell-Architectedの取り組みにより
責任共有モデルに基づくお客様ワークロードの
設計・運用の継続的改善を推進しています。

まとめにかえて

これまでを振り返ってみませんか？

お客様のワークロードのアーキテクチャをどのくらい詳細に把握できているでしょうか？

また、どのくらい踏み込んでその改善提案や情報提供できているでしょうか？

さらには適切なコンセンサスを形成、維持できているでしょうか？

本日のお持ち帰りワード

責任共有モデル
&
Well-Architected

参考資料

クラウドはまったく新しい価値観の世界

クラウドでの一般設計原則(Design Principles)

- 必要なキャパシティ を**勘に頼らない**
- **本番規模**でのシステム**テスト**を行う
- アーキテクチャ**試行の回数を増やす**ために**自動化**を取り入れる
- **発展的なアーキテクチャ**を受け入れる
- **データ計測に基づいて**アーキテクチャを決定する
- 本番で想定されるトラブルを**あらかじめテストし、対策する**

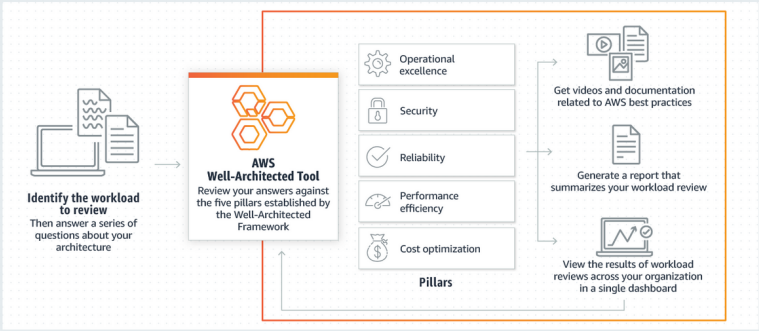
aws

Well-Architected レビューの方法

① AWSのソリューションアーキテクト(SA)と実施

- AWSのSAは、全世界で毎年数千件のW-Aレビューをお手伝いしています
- お気軽にお声がけください

② AWS Well-Architected toolを活用して、セルフサービスでレビューを実施



AWS Well-Architected 個別技術相談会

毎週”W-A個別技術相談会”を実施中

- AWSのソリューションアーキテクト(SA)に対策などを相談することが可能

- 申込みはイベント告知サイトから

  (https://aws.amazon.com/jp/about-aws/events/)

AWS イベント で[検索]

References

責任共有モデル
https://aws.amazon.com/jp/compliance/shared-responsibility-model/

AWS Well-Architected – 安全で効率的なクラウド対応
https://aws.amazon.com/jp/architecture/well-architected/