2023-03-16

チェックシートの紹介と具体的な活用方法について

Amazon Web Services Japan G.K.
Startup Solutions Architect
Soh Ohara

尾原 颯
Ohara, Soh

アマゾン ウェブ サービス ジャパン合同会社
スタートアップ事業本部 技術統括部
ソリューションアーキテクト

- ヘルスケアの領域を中心に支援
- 好きなサービス:
  AWS Well-Architected, Amazon SageMaker

アジェンダ

- AWS Well-Architected Framework の紹介
- チェックシートの紹介
- チェックシートの具体的な活用例の紹介

この発表を通じて目指していただきたい姿

監基報 315 に基づく IT 全般統制対応を
適切なタイミングで計画的に行っている

IT 全般統制対応が計画的に行えないとどうなるか

上場の時期がずれてしまうリスクが高まる

上場前に IT 全般統制の対応に追われ、
対応期間前向きな開発に工数を割くことが難しくなる

このようなケースを見かけます

IT 全般統制を計画的に実行するために必要なこと

エンジニアの皆さんが上場に向けたタスクや
セキュリティの要件を把握し実装する

エンジニアと CFO や監査担当者が
同じ目線で意思疎通すること

悩みの解決のためのサポートツール

チェックシート

X

AWS Well-Architected Framework

AWS Well-Architected Framework

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

10年以上に渡り数多くのお客様の

アーキテクチャ設計および検証を

お手伝いしてきた経験から作成した、

クラウドアーキテクチャ設計・運用の

クラウドベストプラクティス集

AWS Well-Architected Framework の構成要素

一般的な設計原則

柱	柱	柱	柱	柱	柱
					
運用上の優秀性	セキュリティ	信頼性	パフォーマンス効率	コスト最適化	持続可能性
設計原則	設計原則	設計原則	設計原則	設計原則	設計原則
質問	質問	質問	質問	質問	質問
BP	BP	BP	BP	BP	BP
⋮	⋮	⋮	⋮	⋮	⋮
		…			

BP = ベストプラクティス

ホワイトペーパー

各種ベストプラクティスの詳細を記載
実装のガイダンスやリスクレベルに言及

SEC01-BP01 アカウントを使用してワークロードを分ける:

PDF | RSS

セキュリティとインフラストラクチャを念頭に置いて、ワークロードが増大するにつれて組織が共通のガードレールを設定できるようにします。このアプローチによって、ワークロード間の境界と制御が確立します。開発環境およびテスト環境から本番環境を分離する場合、または外部コンプライアンス要件 (PCI-DSS や HIPAA など) で定義されている機密レベルの異なるデータを処理するワークロードとそうでないワークロードとの間に強力な論理的境界を設ける場合は、アカウントレベルの分離を強くお勧めします。

このベストプラクティスが確立されていない場合のリスクレベル: 高

実装のガイダンス

- AWS Organizations を使用する: AWS Organizations を使用し、複数の AWS アカウント にポリシーベースの管理を一元的に適用します。
  - AWS Organizations の開始方法
  - サービスコントロールポリシーを使用して、AWS Organization のアカウント間にアクセス許可ガードレールを設定する方法
- AWS Control Tower を考慮する: AWS Control Tower では、ベストプラクティスに基づいて、新しいセキュアなマルチアカウントの AWS 環境を容易にセットアップおよび管理できます。
  - AWS Control Tower

リソース

https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/framework/welcome.html

上場後にも参照してほしいベストプラクティス

上場後にも（上場後こそ）セキュリティや

その他の観点は高く保たれる必要がある

AWS Well-Architected Framework は

スタートアップから大企業を含む一般化されたベストプラクティス集で

上場後も常に参照できる

AWS Well-Architected Framework の構成要素

一般的な設計原則

柱	柱	柱	柱	柱	柱
運用上の優秀性	セキュリティ	信頼性	パフォーマンス効率	コスト最適化	持続可能性
設計原則	設計原則	設計原則	設計原則	設計原則	設計原則
質問	質問	質問	質問	質問	質問
BP	BP	BP	BP	BP	BP
⋮	⋮	⋮	⋮	⋮	⋮
		…			

BP = ベストプラクティス

AWS Well-Architected Framework の構成要素

一般的な設計原則

柱

運用上
優秀

可能性

300 以上のベストプラクティス

設計

設計原則

質問

BP

質問

BP

質問

BP

…

質問

BP

質問

BP

質問

BP

BP = ベストプラクティス

AWS Well-Architected Framework の構成要素

一般的な設計原則

柱

運用上
優秀

可能性

300 以上のベストプラクティス
→ いきなり全ての網羅は困難

設計

設計原則

質問

BP

質問

BP

質問

BP

質問

BP

質問

BP

質問

BP

BP = ベストプラクティス

チェックシート

チェックシートとは

ブリッジコンサルティンググループ株式会社さまが作成した、
AWS Well-Architected Framework のベストプラクティスの中から
IPO 準備の中で監査対応で
必要な部分と判断したものを抜き出し整理したもの

チェックシートでのベストプラクティスとのマッピング

チェックシートの構成

- 説明: チェックシートについての説明
- 監基報 315:「 監基報 315」→ W-A へのマッピング
- 実施基準:「財務報告に係る内部統制の評価及び監査に関する実施基準」
  → W-A へのマッピング
- セキュリティ: W-A についての参考情報
- オペレーショナルエクセレンス: W-A についての参考情報
- 信頼性: W-A についての参考情報

チェックシートの構成

- 説明: チェックシートについての説明
- 監基報 315:「 監基報 315」→ W-A へのマッピング
- 実施基準:「財務報告に係る内部統制の評価及び監査に関する実施基準」
  → W-A へのマッピング
- セキュリティ: W-A
- オペレーショナルエク
- 信頼性: W-A につ

この 2 つのシートからまずはチェック

チェックシートの中身

監査基準委員会報告書 315（2023年1月12日最終改正） 付録6 IT全般統制を理解するための考慮事項　　SEC：セキュリティ、OPS：オペレーショナルエクセレンス、REL：信頼性

ITプロセス	ITの利用から生じるリスク	分類	内部統制（例）	AWS Well-Architected
アクセス管理のプロセス	システムへの不適切なアクセスを制限するように、適切に環境設定がされていない又はシステム設定がアップデートされていない。	認証	ＩＴアプリケーションやその他のＩＴ環境にアクセスする利用者が、利用者自身のログイン資格情報を使用している（すなわち、利用者が別の利用者の資格情報を使用していない。）ことを保証する内部統制 ユーザーのシステムへのアクセスを承認する仕組みとして、固有のユーザーIDとパスワード又は他の方法による認証がある。パスワードのパラメータは会社や業界の基準を満たしている（例えば、パスワードの必要最低限の長さと複雑性、有効期限並びにアカウントのロック）。	SEC：強力なサインインメカニズムを使用する
		セキュリティの環境設定	情報システムには、一般的に、IT環境へのアクセスを制限する、主要な環境設定がある。 セキュリティの環境設定の主要な属性が適切に実施されている。	SEC：一時的な認証情報を使用する SEC：シークレットを安全に保存して使用する
	利用者が担当業務の遂行に必要以上のアクセス権を有す	権限の付与	利用者が職責に必要な情報にアクセスし、それ以外の情報にはアクセスできないようにする内部統制。これにより、適切な職務分離が促進される	SEC：アクセス要件を定義する

チェックシートの中身

監査基準委員会報告書 315（2023年1月12日最終改正） 付録6 IT全般統制を理解するための考慮事項　　SEC：セキュリティ、OPS：オペレーショナルエクセレンス、REL：信頼性

ITプロセス	ITの利用から生じるリスク	分類	内部統制（例）	AWS Well-Architected
アクセス管理のプロセス	システムへの不適切なアクセスを制限するように、適切に環境設定がされていない又はシステム設定がアップデートされていない。	認証	ＩＴアプリケーションやその他のＩＴ環境にアクセスする利用者が、利用者自身のログイン資格情報を使用している（すなわち、利用者が別の利用者の資格情報を使用していない。）ことを保証する内部統制 ユーザーのシステムへのアクセスを承認する仕組みとして、固有のユーザーIDとパスワード又は他の方法による認証がある。パスワードのパラメータは会社や業界の基準を満たしている（例えば、パスワードの必要最低限の長さと複雑性、有効期限並びにアカウントのロック）。	SEC：強力なサインインメカニズムを使用する
		セキュリティの環境設定	情報システムには、一般的に、IT環境へのアクセスを制限する、主要な環境設定がある。 セキュリティの環境設定の主要な属性が適切に実施されている。	SEC：一時的な認証情報を使用する SEC：シークレットを安全に保存して使用する
	利用者が担当業務の遂行に必要以上のアクセス権を有す	権限の付与	利用者が職責に必要な情報にアクセスし、それ以外の情報にはアクセスできないようにする内部統制。これにより、適切な職務分離が促進される	SEC：アクセス要件を定義する

監査基準報告書 315 の中身

チェックシートの中身

監査基準委員会報告書 315（2023年1月12日最終改正） 付録6 IT全般統制を理解するための考慮事項　　SEC：セキュリテ、OPS：オペレーショナルエクセレンス、REL：信頼性

ITプロセス	ITの利用から生じるリスク	分類	内部統制（例）	AWS Well-Architected
アクセス管理のプロセス	システムへの不適切なアクセスを制限するように、適切に環境設定がされていない又はシステム設定がアップデートされていない。	認証	ＩＴアプリケーションやその他のＩＴ環境にアクセスする利用者が、利用者自身のログイン資格情報を使用している（すなわち、利用者が別の利用者の資格情報を使用していない。）ことを保証する内部統制 ユーザーのシステムへのアクセスを承認する仕組みとして、固有のユーザーIDとパスワード又は他の方法による認証がある。パスワードのパラメータは会社や業界の基準を満たしている（例えば、パスワードの必要最低限の長さと複雑性、有効期限並びにアカウントのロック）。	SEC：強力なサインインメカニズムを使用する
		セキュリティの環境設定	情報システムには、一般的に、IT環境へのアクセスを制限する、主要な環境設定がある。 セキュリティの環境設定の主要な属性が適切に実施されている。	SEC：一時的な認証情報を使用する SEC：シークレットを安全に保存して使用する
	利用者が担当業務の遂行に必要以上のアクセス権を有す	権限の付与	利用者が職責に必要な情報にアクセスし、それ以外の情報にはアクセスできないようにする内部統制。これにより、適切な職務分離が促進される	SEC：アクセス要件を定義する

マッピングされた W-A のベストプラクティス

（ホワイトペーパーの該当箇所へのリンクも）

チェックシートの活用例

これからチェックシートを使ったコミュニケーションの実践例は
あくまでイメージを掴むためのものです

例で紹介した方法で監査が通るかについてはケースバイケースのため
保証できません。最終的な確認は内部統制担当の方か監査法人の
方までお願いします。

[再掲] IT 全般統制を計画的に実行するために必要なこと

エンジニアの皆さんが上場に向けたタスクや
セキュリティの要件を把握し実装する

エンジニアと CFO や監査担当者が
同じ目線で意思疎通すること

チェックシート活用の流れ（例）

監査基準委員会報告書 315（2023年1月12日最終改正）　付録6 IT全般統制を理解するための考慮事項　　SEC：セキュリティ、OPS：オペレーショナルエクセレンス、REL：信頼性

ITプロセス	ITの利用から生じるリスク	分類	内部統制（例）	AWS Well-Architected
アクセス管理のプロセス	システムへの不適切なアクセスを制限するように、適切に環境設定がされていない又はシステム設定がアップデートされていない。	認証	ＩＴアプリケーションやその他のＩＴ環境にアクセスする利用者が、利用者自身のログイン資格情報を使用している（すなわち、利用者が別の利用者の資格情報を使用していない。）ことを保証する内部統制 ユーザーのシステムへのアクセスを承認する仕組みとして、固有のユーザーIDとパスワード又は他の方法による認証がある。パスワードのパラメータは会社や業界の基準を満たしている（例えば、パスワードの必要最低限の長さと複雑性、有効期限並びにアカウントのロック）。	SEC：強力なサインインメカニズムを使用する 証情報を使用する トを安全に保存して使用する 件を定義する
	利用者が担当業務			

一番上の項目でマッピングされている
「強力なサインインメカニズムを使用する」から
確かめよう

技術部門

→ ホワイトペーパーで該当項目を確認

会社で提供しているサービスを使用するユーザーにも MFA とかやった方が良いのかな？

技術部門

aws

SEC02-BP01 強力なサインインメカニズムを使用する

PDF | RSS

パスワードに最小の長さを設定し、よくあるパスワードや再利用を避けるようにユーザーを教育します。ソフトウェアまたはハードウェアのメカニズムを使用した Multi-Factor Authentication (MFA) を強制して、検証を追加します。例えば、IAM アイデンティティセンターをアイデンティティソースとして使用する場合、MFA の「コンテキストアウェア」または「常時オン」設定でユーザーに独自の MFA デバイスの登録を許可すると、すばやく使用開始できます。外部の ID プロバイダー (IdP) を使用する場合は、IdP を MFA 用に設定します。

このベストプラクティスを活用しない場合のリスクレベル: 高

実装のガイダンス

- MFA サインインを強制するアクセス管理 (IAM) ポリシーを作成する: ユーザーが [マイセキュリティ資格情報] ページでロールを引き受け、自分の認証情報を変更し、MFA デバイスを管理できるようにするものを除いて、すべての IAM アクションを禁止するカスタマー管理 IAM ポリシーを 作成します.
- ID プロバイダーで MFA を有効にする: MFA を、アイデンティティプロバイダーや使用する AWS IAM Identity Center (successor to AWS Single Sign-On)などのシングルサインオンサービスで有効にします。
- 強力なパスワードポリシーを設定する: 強力なパスワードポ

監査基準委員会報告書 315（2023年1月12日最終改正）　付録6 IT全般統制を理解するための考慮事項　　SEC：セキュリティ、OPS：オペレーショナルエクセレンス、REL：信頼性

ITプロセス	ITの利用から生じるリスク	分類	内部統制（例）	AWS Well-Architected
アクセス管理のプロセス	システムへの不適切なアクセスを制限するように、適切に環境設定がされていない又はシステム設定がアップデートされていない。	認証	ＩＴアプリケーションやその他のＩＴ環境にアクセスする利用者が、利用者自身のログイン資格情報を使用している（すなわち、利用者が別の利用者の資格情報を使用していない。）ことを保証する内部統制 ユーザーのシステムへのアクセスを承認する仕組みとして、固有のユーザーIDとパスワード又は他の方法による認証がある。パスワードのパラメータは会社や業界の基準を満たしている（例えば、パスワードの必要最低限の長さと複雑性、有効期限並びにアカウントのロック）。	SEC：強力なサインインメカニズムを使用する
		セキュリティの環境設定	情報システムには、一般的に、IT環境へのアクセスを制限する、主要な環境設定がある。 セキュリティの環境設定の主要な属性が適切に実施されている。	SEC：一時的な認証情報を使用する SEC：シークレットを安全に保存して使用する
	利用者が担当業務の遂行に必要以上のアクセス権を有す	権限の付与	利用者が職責に必要な情報にアクセスし、それ以外の情報にはアクセスできないようにする内	SEC：アクセス要件を定義する

技術部門

監査法人の方に聞いてみよう

監査基準委員会報告書 315（2023年1月12日最終改正）　付録6 IT全般統制を理解するための考慮事項　　SEC：セキュリティ、OPS：オペレーショナルエクセレンス、REL：信頼性

ITプロセス	ITの利用から生じるリスク	分類	内部統制（例）	AWS Well-Architected
アクセス管理のプロセス	システムへの不適切なアクセスを制限するように、適切に環境設定がされていない又はシステム設定がアップデートされていない。	認証	ＩＴアプリケーションやその他のＩＴ環境にアクセスする利用者が、利用者自身のログイン資格情報を使用している（すなわち、利用者が別の利用者の資格情報を使用していない。）ことを保証する内部統制 ユーザーのシステムへのアクセスを承認する仕組みとして、固有のユーザーIDとパスワード又は他の方法による認証がある。パスワードのパラメータは会社や業界の基準を満たしている（例えば、パスワードの必要最低限の長さと複雑性、有効期限並びにアカウントのロック）。	SEC：強力なサインインメカニズムを使用する
		セキュリティの環境設定	情報システムには、一般的に、IT環境へのアクセスを制限する、主要な環境設定がある。 セキュリティの環境設定の主要な属性が適切に実施されている。	SEC：一時的な認証情報を使用する SEC：シークレットを安全に保存して使用する
	利用者が担当業務の遂行に	権限の付与	利用者が職責に必要な情報にアクセスし、それ以外の情報にはアクセスできないようにする内	SEC：アクセス要件を定義する

技術部門

そうなると両方の観点から
対策しておく必要がありそうですね。

チェックシート活用の流れ（例）

監査基準委員会報告書 315（2023年1月12日最終改正）　付録6 IT全般統制を理解するための考慮事項　　SEC：セキュリティ、OPS：オペレーショナルエクセレンス、REL：信頼性

ITプロセス	ITの利用から生じるリスク	分類	内部統制（例）	AWS Well-Architected
プログラムや他のIT環境への変更を管理するためのプロセス	データベースの構造やデータ間の関連付けに不適切な変更が行われる。 システムソフトウェアに対して不適切な変更が行われる（例えば、オペレーティング・システム、ネットワーク、変更管理ソフトウェア、アクセス制限ソフトウェア）。	本番環境への移行に関する職務の分離	プログラムの変更と本番環境への移行に対するアクセス権の分離の内部統制 アプリケーションの本番環境における変更権限が適切に管理され、また開発環境から分離されている。	SEC：アカウントを使用してワークロードを分ける
		システムの開発、取得又は導入	ITアプリケーション又はその他のIT環境に関連する、当初の開発又は導入に対する内部統制	承認行為でありAWS Well-Architected外

本当にアカウントを分けるだけで十分なのだろうか？

技術部門

チェックシートによる解決

エンジニアの皆さんが上場に向けたタスクや
セキュリティの要件を把握し実装する

→ チェックシートにマッピングされた
W-A のベストプラクティスからまずは取り組む

エンジニアと CFO や監査担当者が
同じ目線で意思疎通すること

→ 対応を進めていく中で出てきた疑問を
チェックシートベースに会話を進める

パートナーによる支援

AWS パートナーがセキュリティ対策を全面サポート可能

連携パートナー：株式会社ジェーエムエーシステムズ（JMAS）

- ✓ 2014 年より継続的に AWS パートナーとしてお客様を多方面でご支援
  - ✓ **1,000 以上**にわたる AWS プロジェクトの支援実績
  - ✓ **Well-Architected パートナー認定**取得済み
  - ✓ **200 名以上**の AWS 認定資格取得者数

- ✓ スタートアップのお客様に対しても、インフラからアプリケーションにいたるまで幅広い領域をご支援

スタートアップ専用の IT 統制支援パッケージをご用意

■：必須対応項目　□：オプションとして追加対応可

分類	対応項目	PLAN-A	PLAN-B	PLAN-C
システム診断	Well-Architected レビュー	■	■	■
	アーキテクチャレビュー		■	■
	セキュリティ診断			■
	ペネトレーションテスト			■
システム改善	システム改善(含ハイリスク対応)	□	■	■
システム文書管理	アセスメント		■	■
	ドキュメント作成		□*	□*
			□	□
			□	□
			80万円～	300万円～
			50万円～	270万円～

PLAN-B 以上をご活用のお客様には、**最大 $4,500 のキャッシュをAWSから提供する Fund Program** もご案内可能です。
詳細は JMAS 様、または AWS 担当営業までご連絡ください。

*ドキュメントが無い場合は追加対応となります（必須）

まとめ

まとめ

- チェックシートは IT 全般統制と AWS W-A のベストプラクティスとを対応づけている
- チェックシートをベースに監査担当の方と適切にコミュニケーションをとりながら IT 全般統制対策を進めていきましょう

チェックシートはイベント参加されたみなさまに

後日ご案内いたします。

参考リンク AWS W-A Framework ホワイトペーパー

オペレーショナルエクセレンス

https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/operational-excellence-pillar/welcome.html

セキュリティ

https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/welcome.html

信頼性

https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/welcome.html

パフォーマンス効率

https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/performance-efficiency-pillar/welcome.html

コスト最適化

https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/cost-optimization-pillar/welcome.html

持続可能性

https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/sustainability-pillar/sustainability-pillar.html

Thank you!

Soh Ohara

Appendix

AWS Well-Architected Tool (WA Tool) の紹介

Well-Architected レビュー時に活用できるサービス

- 各質問毎に**ベストプラクティスの適用状況**を記録
- レビューした結果をレポートとして出力でき、

リスクレベルを可視化

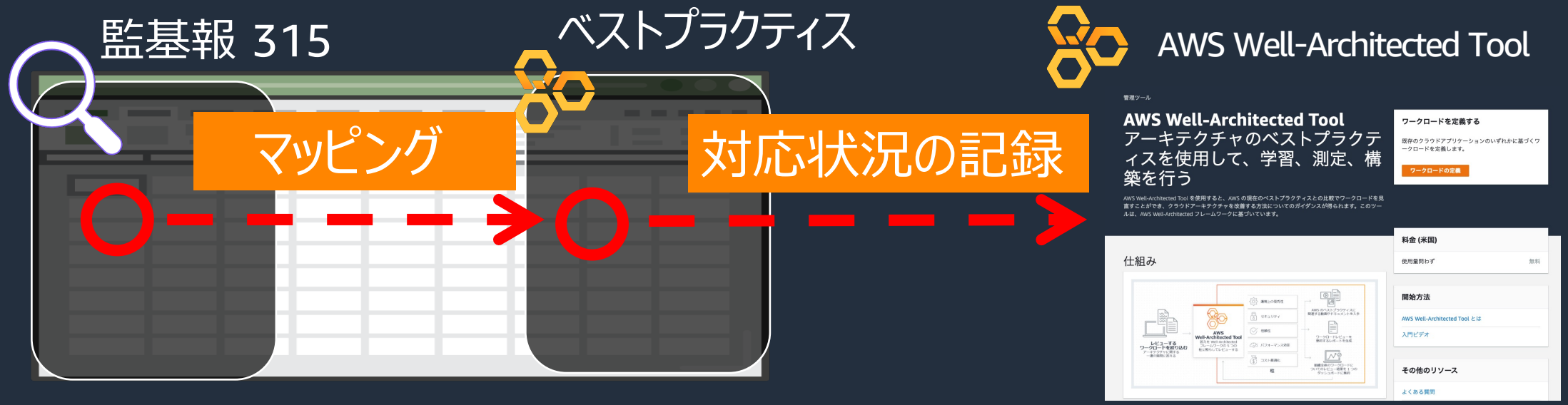
Well-Architected レビュー: AWS Well-Architected Framework で紹介されているベストプラクティスの適用状況を分析するプロセス

AWS Well-Architected Tool 使用例

STARTUP FM 2023/03

ベストプラクティスに関する説明やリソースの表示

チェックシートとの併用イメージ



マイルストーンの作成で、
その時の対応状況を保存