

AWS公共パートナーネットワーク(PSN)セミナー

Claude Mythos 時代の AWS セキュリティ対策

～ AWS Security Agent ご紹介 ～

2026年7月

アマゾン ウェブ サービス ジャパン合同会社
パブリックセクター技術統括本部
パートナーソリューションアーキテクト
市崎 洋平



アジェンダ

AWS が観測している脅威傾向 (Claude Mythos 前夜)

Anthropic Mythos / Project Glasswing と AWS の対応

今後の予想される脅威

AWS が提案する対応策

AWS Security Agent のご紹介

まとめ

AWS が観測している脅威傾向 (Claude Mythos 前夜)

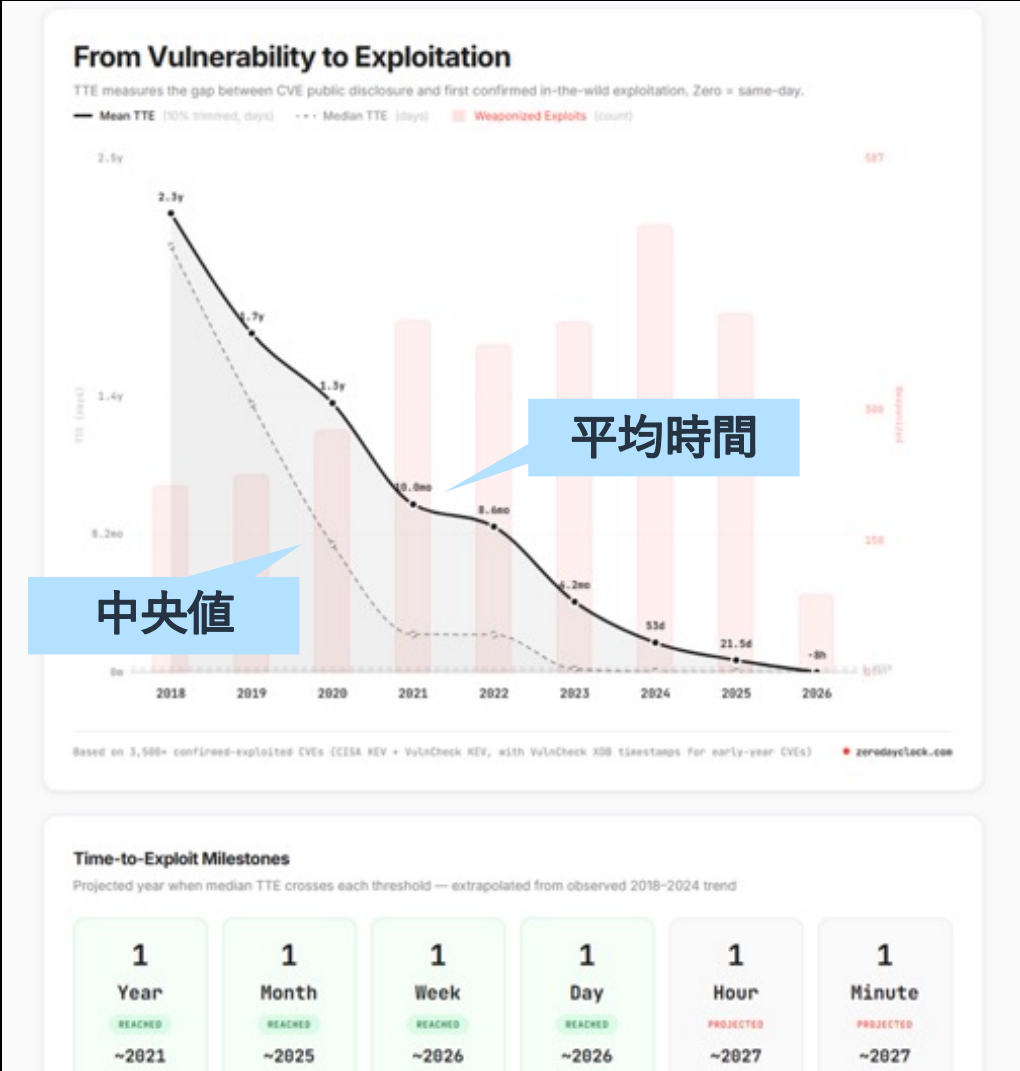


脆弱性公表からエクスプロイトまでの時間は短縮

CVE 公開からエクスプロイト（悪用）が実際に行われるまでの平均時間が、各閾値を下回った時期

平均値	状況	到達時期
1 年	到達済み	～2021年
1 ヶ月	到達済み	～2025年
1 週間	到達済み	～2026年
1 日	到達済み	～2026年
1 時間	予想値	～2026年
1 分	予想値	～2028年

出典：
Zero Day Clock
<https://zerodayclock.com/>



AI がサイバー攻撃の参入障壁を破壊

高度な技術を持たない攻撃者でも生成 AI を使えば大規模なサイバー攻撃を実行できる時代に

特徴： 基本的なセキュリティの不備が狙われる

- 高度な脆弱性ではない
- 従来は大規模チームが必要だった攻撃を、AI が少人数でも可能にした



ツール開発

- カスタム攻撃ツールを AI で自動生成
- 技術力がなくても高度なツールを入手可能



攻撃計画

- 段階的な侵入手順・成功率・所要時間まで AI が策定
- 人間の判断を AI が代替



大規模自動化

- 55 か国・600 台超のデバイスを少人数で同時攻撃
- 公開管理ポート + 弱いパスワード + 単一要素認証

事例

- 2025 年 8 月 . . . Nx パッケージ侵害
- 2025 年 9 月 . . . Chalk ・ Debug 改ざん
- 2025 年 10-11 月 . . . 偽パッケージ大量混入



出典：Amazon Web Services ブログ

AI で強化された脅威アクターによる FortiGate デバイスへの大規模な不正アクセス

<https://aws.amazon.com/jp/blogs/news/ai-augmented-threat-actor-accesses-fortigate-devices-at-scale/>

最近の npm サプライチェーン攻撃への対応から AWS Security が学んだこと

<https://aws.amazon.com/jp/blogs/news/what-aws-security-learned-from-responding-to-recent-npm-supply-chain-threat-campaigns/>

攻撃の「質的变化」 — 3 つの変質

- 攻撃側も AI の活用が進んでいる
- 攻撃のスピードと規模を上回る、自動化された検知・防御の仕組みとして AI による防御対策も必要に



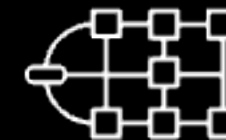
国家支援型の高度化

- ゼロデイ開発力と国家レベルのリソース
- 脆弱性公開から数時間で武器化
- 数年単位の長期潜伏
- **金融・エネルギーが主要標的**



AI による攻撃の大衆化

- 技術力不問で大規模攻撃が可能に
- ツール開発、攻撃計画、大規模自動化を AI が代替
- **基本的な不備が狙われる**



サプライチェーンの武器化

- 信頼の仕組みが攻撃経路に
- 正規の開発プロセスを悪用
- 正常な行為と区別がつかない
- **開発環境そのものがリスク**

AWS のスケールを活用した脅威インテリジェンスと防御

60 秒ごとに
エクサバイトの
データを分析

1日あたり 1,000 億件以上の
リクエストを
AWS マネージドルールで処理

毎日何千件もの
DDoS 攻撃を軽減

世界中に数万台のハニーポットを設置

新規脆弱性検出も AI を活用して 336% 迅速化

悪性 IP アドレスなどは、3 分で AWS クラウドに対策実装

世界 184 か所で
合計約 5,000 の
ネットワークと接続

6,600万
所有IPアドレス

26億/日
IPアドレスと通信

Claude Mythos / Project Glasswing と AWS の対応



ANTHROPIC: Project Glasswing

AWS はローンチパートナー

- **Claude Mythos Preview** を活用した業界横断コンソーシアム
- 2026年4月7日に約 50 の組織で開始 ⇒ 6 月には 15ヶ国以上・約 200 組織へ拡大

Mythos を世界の重要ソフトウェアを
防御するために活用

- 対象は、OS ・ブラウザ ・金融システムを含む重要インフラ、重要なオープンソース
- Anthropic が最大 1 億ドルのモデル使用クレジット提供
- **90 日以内に公開レポートとして共有 (予定)**
- Amazon Bedrock、Google Vertex AI、Microsoft Foundry、Claude API 等を経由してパートナーに提供

ローンチパートナー (12社)

AWS

Anthropic

Apple

Google

Microsoft

Cisco

CrowdStrike

Palo Alto

NVIDIA

Broadcom

Linux Foundation

JPMorganChase



Claude Mythos Preview とは

Anthropic 社が 2026 年 4 月に公開(限定公開)、サイバー能力に特化したフロンティア AI モデル

限定リリース

- Project Glasswing
- 12 パートナー
- 重要インフラ組織のみ
- 40 以上の組織(当初)

完全自律

- 人間の介入なしに、脆弱性発見からエクスプロイト開発まで

数千件

- Anthropic が数週間で主要OS・ブラウザの脆弱性の検出
- 人間と自動ツールが見逃してきたバグを発見

3 つの実例： 長年見逃されてきたバグを発見

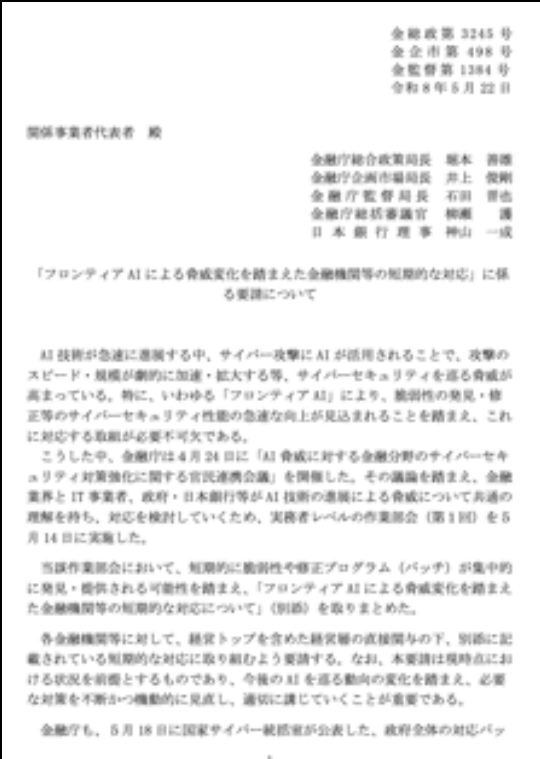
- OpenBSD . . . 27年間潜伏していた脆弱性を発見
- FFmpeg . . . 16年間テストツールも見逃してきた
- Linux Kernel . . . 複数の脆弱性を自律的に発見・連続接続



参考) 日本政府: 金融庁・日銀から金融機関等への要請

「フロンティアAIによる脅威変化を踏まえた金融機関等の短期的な対応」に係る要請について (令和8年5月22日)

- フロンティア AI への対応を経営課題として扱う
- 優先的に対応すべきサービス/IT システムを特定する
- 特定した資産の技術負債を解消しておく
- パッチ適用に係る人的リソースを追加する
- ベンダーとの維持保守契約の内容を確認する
- パッチ適用プロセスをリスクベースにする
- パッチ適用以外の対策も強化する
- 優先サービス/IT システムの停止に備える
- 外部との連携を維持・強化する



Project Glasswing の成果 (2026年6月2日時点)

Glasswing パートナーが発見

10,000 件超

- 深刻度 High 以上の脆弱性
- 発見速度は多くで 10 倍以上に向上

Anthropic 自身が発見

23,019 件

- 発見した全脆弱性
- 1,000 以上のOSSプロジェクトを調査

6,202 件

- 深刻度 High 以上の脆弱性
- 1,000 以上のOSSプロジェクトを調査

具体例 — 公式に報告された成果（抜粋）

- **Cloudflare** 重要システムで 2,000 件（うち高・重大 400 件）を発見。誤検知率は人間のテスターより低いと評価
- **オープンソース** 1,000 以上のプロジェクトをスキャン。インターネットを支える重要 OSS を点検
- **Microsoft** 「パッチ数は当面増え続ける」と表明
- **Palo Alto Networks** 最新リリースに通常の 5 倍のパッチを収録
- **銀行** Mythos Preview が 150 万ドルの不正送金を検知・阻止（メール乗っ取り + なりすまし電話）



ご参考) Claude Mythos 関連最新情報

2026年 5月 ～ 7月の主要なタイムライン

5/22 Glasswing パートナー約50組織で10,000件超の高/重大脆弱性を発見

- 出典: Project Glasswing has uncovered 10,000 vulnerabilities (CSO Online)
 - <https://www.csoonline.com/article/4176865/project-glasswing-has-uncovered-10000-vulnerabilities-anthropic.html>

6/2 Project Glasswing を15カ国以上・150組織に拡大

- 出典: Expanding Project Glasswing
 - <https://www.anthropic.com/news/expanding-project-glasswing>

6/9 Claude Mythos 5 + Claude Fable 5 リリース

- 出典: Claude Fable 5 and Claude Mythos 5 (Anthropic):
 - <https://www.anthropic.com/news/claude-fable-5-mythos-5>

6/12 米国政府の輸出規制により全アクセス停止

- 出典: Redeploying Claude Fable 5 (Anthropic)
 - <https://www.anthropic.com/news/redeploying-fable-5>

7/1 規制解除、Fable 5 / Mythos 5 アクセス復活

- Claude Mythos - Announcements (Anthropic)
 - <https://www.anthropic.com/claude/mythos>



AWS の Project Glasswing への取り組み

AWS はすでに AI を活用してセキュリティ対応を高度化

- AI と自動化で 1 日 400 兆のネットワークフローを分析・監視
- AI によるログ分析：6 時間 → 7 分に短縮（50 倍の生産性向上）
- 2025 年だけで S3 バケットへの不正暗号化試行を 3 億件ブロック

Glasswing でさらに先手を打つ

- 自社の重要コードベースに Mythos をいち早く適用し継続スキャン
- 十分にテスト済みの環境でも、新たな脆弱性を発見
- 得られた知見はお客様の防御にも還元

**AWS は脅威が出現する前に AI を活用し大規模なセキュリティ防御を構築
発見から修正までお客様に影響を与えることなく完了**



AWS インフラストラクチャーは迅速・無停止でパッチを適用

単一の技術ではなく、インフラの設計思想・規模・権限構造の組み合わせ

責任共有モデルによる即時実行権限

- AWS の管理責任範囲のため AWS の責任で実施
- 発見から**数時間～数日**で全フリートに展開可能

完全自動化された CI/CD パイプライン

- 自動ビルド → 自動テスト → 段階デプロイ → 自動ロールバック判定
- **お客様環境に影響がないことをテストで担保**した上でリリース

大規模フリートによるローリング更新

- 数千～数万ノードに段階的に適用
常にどこかがパッチ中だが、**全体としては無停止**
- サーバーレス環境は置き換え方式

ハードウェアレベルの分離 (Nitro System)

- 仮想化のハイパーバイザーに関しては、パッチ対象とワークロード実行が**物理的に別のチップ上**
- ホスト更新時もお客様ワークロードは継続稼働
- パッチ中もダウンタイムゼロを保証する構造

AWS インフラストラクチャ

- **自動的に常にパッチが適用されている**
- **アプリケーションは何も変わらず動き続けている**

事例: Log4Shell — 動いている JVM をライブパッチ

CVE-2021-44228 — 2021 年 12 月 世界中の Java アプリが即座に影響、AWS は新技術を開発し対応

- 世界中の数百万の Java アプリケーションが即座に影響を受ける重大脆弱性 (CVSS 10.0)
- ライブラリ更新には再ビルド・再デプロイ・再起動が必要 → 通常、**数日～数週間かかる**

Amazon Corretto (AWS が提供する OSS の Java 実行環境) チームが週末返上で新技術を開発
→ **2021年12月12日にオープンソース公開**

仕組み

- 稼働中の JVM に Java Agent を動的にアタッチ。
- ロード済みクラスの脆弱なメソッドをバイトコードレベルで書き換え。

特徴

- 再起動なし・デプロイなし・コネクション切断なし。
- shaded jar / 複数インスタンスにも対応。
- 冪等 (何度実行しても安全)。

AWS がなぜ出来たのか

- JVM 内部を熟知した Corretto チームが社内に。
- 各基盤に組み込み顧客アクション不要で適用。
- 数百万 JVM に数日で全フリート展開。

対応 AWS サービスの一例

AWS Lambda

AWS Fargate

Amazon EKS / Amazon ECS

適用方法

AWS 側で基盤更新。顧客アクション不要

プラットフォームレベルで自動 hotpatch。顧客コンテナ内の JVM にまで AWS が対応

DaemonSet / SSM Association で全ノード自動適用

結果： 発見から数日で全フリートに緩和策を展開、お客様環境はダウンタイムゼロ



今後の予想される脅威



予想される 2 つの脅威

管理された脅威

(Mythos / Project Glasswing への対応)

特徴

- Glasswing による知見は 90 日以内に公開 (予定)
- 参加組織企業より、脆弱性情報と修正パッチが大量に出てくることが予想される

リスク

- 大量の脆弱性とパッチがリリース
- 攻撃者は迅速に武器化をして攻撃 (Nデイ攻撃)

対策の方向性

- 迅速なパッチ適用によるリスク極小化
- 迅速なパッチの優先度付け

未知の脅威

(高度化する AI によるサイバー攻撃)

特徴

- 生成 AI の高度化によるサイバー能力の急激な向上
- 最先端 AI に追従するオープンウェイトモデル
- Mythos 相当の能力の一般化
- 攻撃者がゼロデイ脆弱性を見つけて独自に武器化

リスク

- 攻撃者は、パッチが存在しない未知の脆弱性について攻撃

対策の方向性

- 多層防御による被害の最小化
- AI 活用によるソフトウェア脆弱性の極小化

管理された脅威 の対策

脆弱性が「大量に公開」されれば、攻撃者はそれを使って武器化と攻撃の可能性

脆弱性の大量発見

- Project Glasswing が Mythos を使って世界の重要ソフトウェアで大規模に脆弱性を探索中
- 発見と同時にパッチも提供され、90 日以内に公開 (予定)

CVE 公開・パッチ配布

- 企業・組織はパッチをテスト・適用が求められる
- この間に「脆弱性情報」が世界に出回る
- パッチがあっても、当てるまでは脆弱性が残っている

数時間で武器化

- 大規模な攻撃グループは脆弱性公開から数時間で武器化することで知られている
- パッチ未適用のシステムが標的になる

- パッチ適用を日常業務化できる体制や仕組みが必要
 - 今までの「四半期ごとに当てる」「テスト後に当てる」のようなフローでは追いつかない可能性あり
- 迅速な脆弱性管理が重要な対策のひとつに
- 加えて、万が一のインシデントレスポンス対応の強化

未知の脅威 の対策

3つの考え方の転換が必要

① 防御の前提

今までは

「侵入を防ぐ」

これからは

「侵入される前提で被害最小化」

- 多層防御、ID 管理、通信制御、ネットワーク分離、データ暗号、ゼロトラストアーキテクチャ
- 検知と対応能力の強化

② 脆弱性レビュー

今までは

「人間によるレビュー」

これからは

「AI で先回りする」

- 最新 LLM による自社コードベースの脆弱性スキャン
- OSやソフトウェアの迅速な脆弱性発見

③ パッチ運用

今までは

「四半期ごとに当てる」

これからは

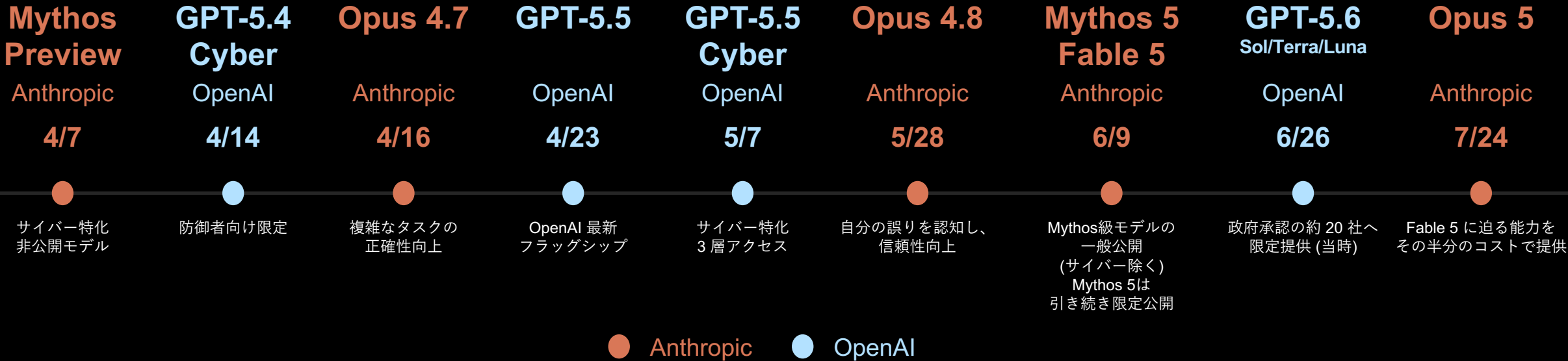
「日常業務として運用」

- モダナイズによるマネージドサービス活用により、パッチ対象自体を削減
- パッチ適用の自動化を目指す

背景) フロンティア AI のサイバー能力競争が加速

3 ヶ月の間に Anthropic と OpenAI がサイバー防御モデルを交互に投入

※ 米国時間基準



短期間に多くの高性能モデルがリリース

- 2026/5/28 Mythos 級のモデルを全ての顧客へ数週間以内に公開を予告
- 2026/6/9 Mythos 級でサイバー機能を制限した Fable 5 を全顧客提供
- 2026/6/12 米政府が輸出管理指令を発出。Anthropic は Mythos 5 と Fable 5 の提供を停止
- 2026/6/26 米政府の許可を受け、Anthropic が Mythos 5 を「信頼できる」米組織 (100 社超) へ限定再提供
- 2026/6/26 OpenAI が GPT-5.6 (Sol/Terra/Luna) を発表。政府要請で承認済み約 20 社へ限定提供

出典：
<https://www.anthropic.com/glasswing>
<https://www.anthropic.com/research/claude-opus-4-7>
<https://openai.com/index/scaling-trusted-access-for-cyber-defense/>
<https://openai.com/index/introducing-gpt-5-5/>
<https://openai.com/index/gpt-5-5-with-trusted-access-for-cyber/>
<https://www.helpnetsecurity.com/2026/05/29/anthropic-claude-opus-4-8/>
<https://www.reuters.com/business/anthropic-roll-out-claude-mythos-coming-weeks-launches-opus-48-2026-05-28/>
<https://www.anthropic.com/news/claude-opus-5>



AWS が提案する対応策



AWS が提案する対応策

AWS セキュリティの全体像

AWS の責任共有モデル

<https://aws.amazon.com/jp/compliance/shared-responsibility-model/>

お客様

クラウド内のセキュリティに対する責任
SECURITY 'IN' THE CLOUD

お客様のデータ

プラットフォーム、アプリケーション、IDとアクセス管理

オペレーティングシステム、ネットワークとファイアウォール構成

クライアント側データ暗号化
データ整合性認証

サーバー側暗号化
(ファイルシステムやデータ)

ネットワークトラフィック保護
(暗号化、整合性、アイデンティティ)

AWS

クラウドのセキュリティに対する責任
SECURITY 'OF' THE CLOUD

ソフトウェア

コンピューート

ストレージ

データベース

ネットワーキング

ハードウェア/AWSグローバルインフラストラクチャー

リージョン

アベイラビリティ
ゾーン

エッジロケーション



マネージド型サービスの選択によるセキュリティ強化

お客様のセキュリティ対応の範囲をさらに削減

お客様の管理範囲

AWS の提供範囲

オンプレミス
サービスの利用
スケーラビリティ
可用性の確保
バックアップ
ミドルウェアのパッチ適用
ミドルウェアの導入
OSのパッチ適用
OSの導入
サーバーメンテナンス
ラック導入管理
電源・ネットワーク

仮想マシン (Amazon EC2)
サービスの利用
スケーラビリティ
可用性の確保
バックアップ
ミドルウェアのパッチ適用
ミドルウェアの導入
OSのパッチ適用
OSの導入
サーバーメンテナンス
ラック導入管理
電源・ネットワーク

マネージド型サービス
サービスの利用
スケーラビリティ
可用性の確保
バックアップ
ミドルウェアのパッチ適用
ミドルウェアの導入
OSのパッチ適用
OSの導入
サーバーメンテナンス
ラック導入管理
電源・ネットワーク

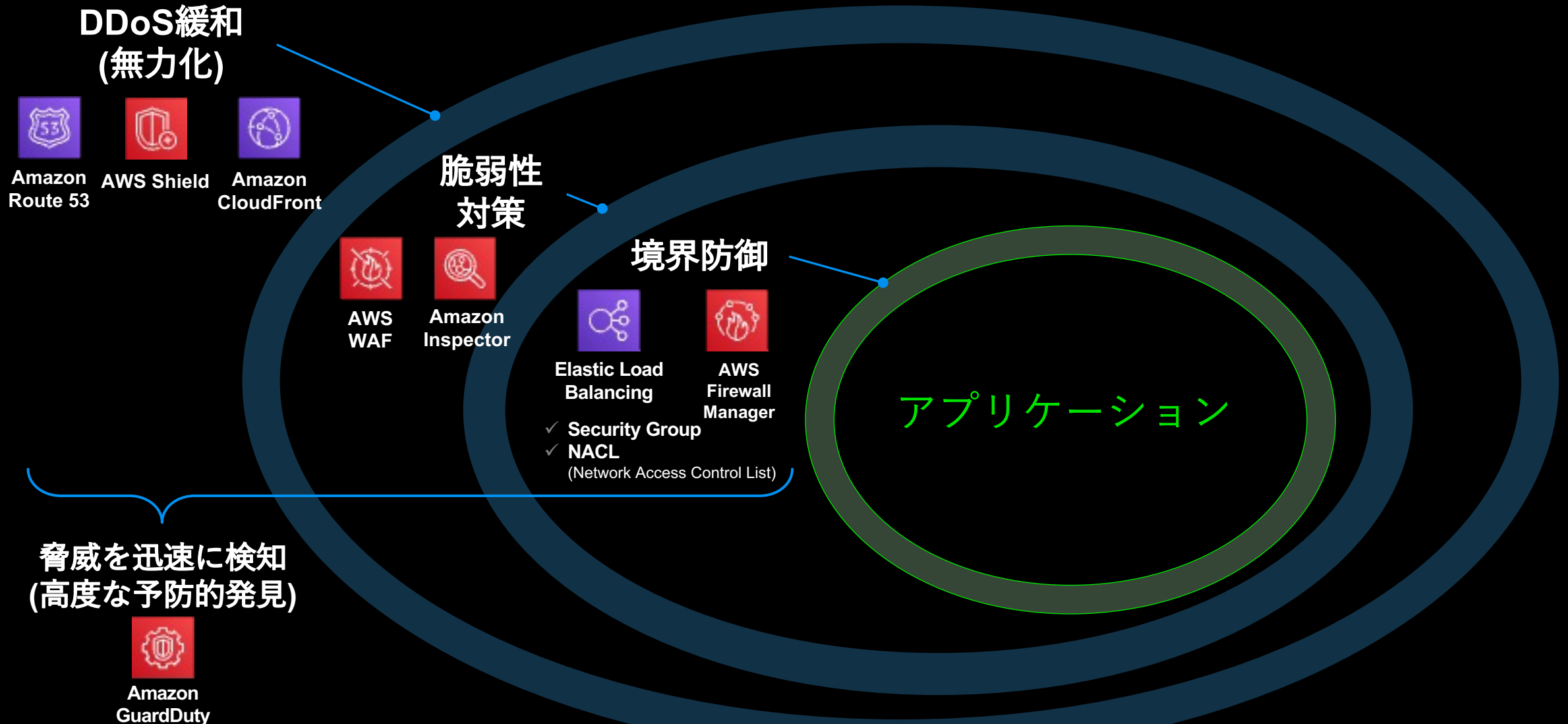
AWS 上のシステムのセキュリティ対策整理

	OS / アプリケーションレイヤー (お客様が作成)	基盤レイヤー (AWS サービス, お客様が設定)
代表的な攻撃	- DDoS 攻撃 - SQL インジェクション攻撃 - ブルートフォース攻撃 - ソフトウェア脆弱性をついた攻撃、等	- AWS アカウント侵害 (ソーシャルエンジニアリング含む) - クレデンシャル漏洩 - 権限管理が不十分 - 設定・設計の不備、等
主な対象	- カスタムビルドアプリケーション - ミドルウェア (商用 / OSS) - OS、等	- AWS 構成そのもの - クレデンシャル情報、等

**AWS の豊富なセキュリティ関連ソリューションにて
高度な対策が可能**



AWS セキュリティサービスによる外部脅威対策例



AWS セキュリティ関連サービス全体像



IDとアクセス管理

- ✓ AWS Identity & Access Management (IAM)
- ✓ AWS IAM Identity Center
- ✓ AWS Directory Service
- ✓ AWS Secrets Manager
- ✓ Amazon Cognito
- ✓ AWS Organizations
- ✓ AWS Control Tower



検出

- ✓ AWS Security Hub
- ✓ Amazon GuardDuty
- ✓ AWS CloudTrail
- ✓ AWS Config
- ✓ Amazon CloudWatch
- ✓ VPC Flow Logs
- ✓ Amazon Fraud Detector
- ✓ AWS Trusted Advisor



インフラ セキュリティ

- ✓ AWS Shield
- ✓ AWS Web Application Firewall (AWS WAF)
- ✓ Amazon Inspector
- ✓ AWS Systems Manager
- ✓ Amazon Virtual Private Cloud (VPC)



データ保護

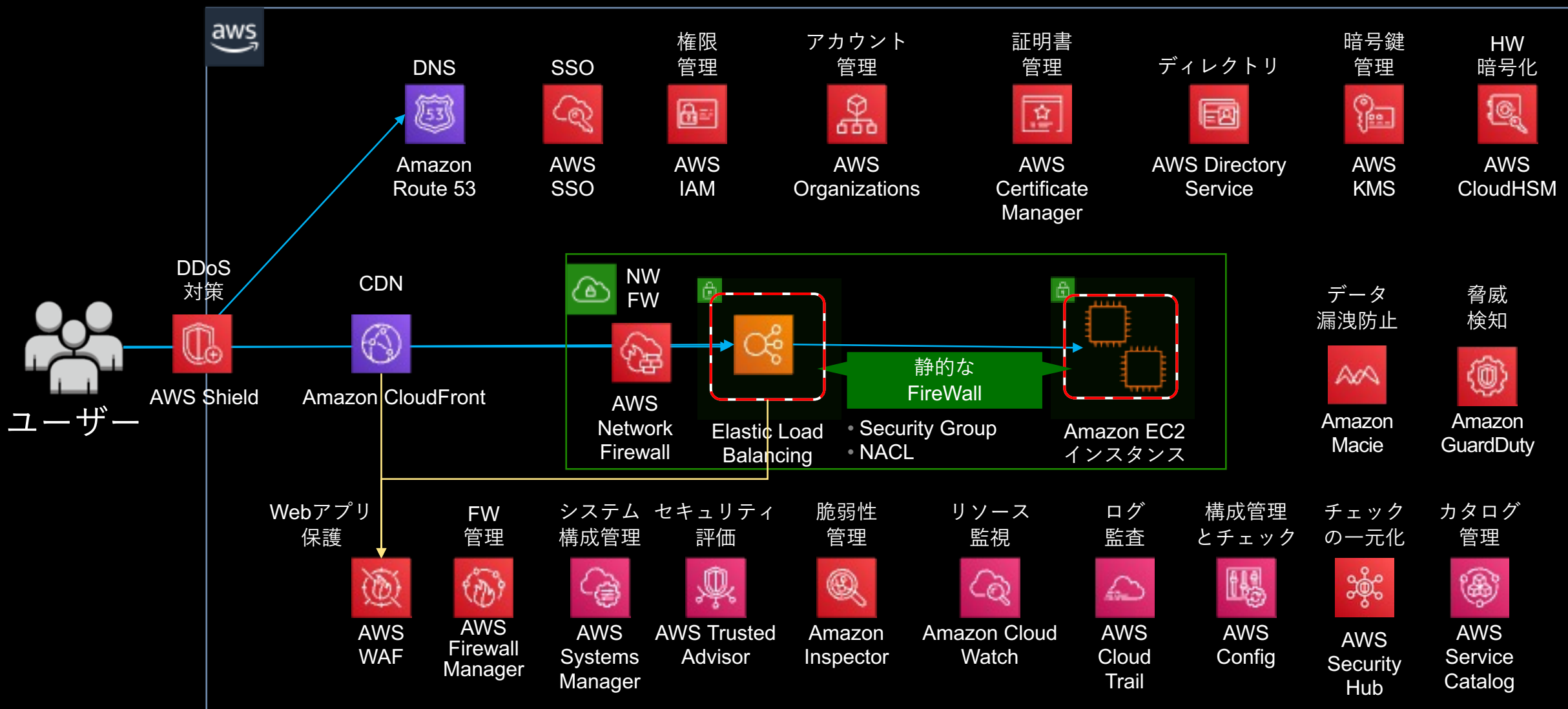
- ✓ AWS Key Management Service (KMS)
- ✓ AWS CloudHSM
- ✓ Amazon Macie
- ✓ AWS Certificate Manager
- ✓ Server-Side Encryption



インシデント レスポンス

- ✓ AWS Lambda
- ✓ Amazon EventBridge
- ✓ AWS Config Rules

AWS セキュリティ関連サービス全体像



AWS が提案する対応策

Mythos 時代の脅威への対策

Mythos 時代のサイバーセキュリティ

AWS アーキテクティングの観点

- システムが侵害されることを前提にしたアーキテクチャ
- 基本的なセキュリティ対策を確実に実施
- AI を活用した先進の対策

	短期的な取り組み例		+ 中長期的な取り組み例 (短期に加えて)	
	ソフトウェア・ アーキテクチャ	運用面	ソフトウェア・ アーキテクチャ	運用面
<u>管理された脅威</u>	- 迅速な脆弱性検出 - WAF の活用による多層防御	パッチ適用の日常業務化	マネージドな AWS サービスを活用したモダナイゼーション	検知と対応能力強化
<u>未知の脅威</u>	- 迅速な脆弱性検出 - AI を活用した脆弱性スキャンとレビュー	パッチ適用の日常業務化	多層防御の徹底による攻撃影響の最小化	検知と対応能力強化

管理された脅威への対策

Glasswing 後のパッチ大量公開に備える、二つの AWS アプローチ

短期的な取り組み例

脆弱性管理、パッチ適用の高度化

- 脆弱性の検出と優先度付け
- パッチ適用の自動化
- アプリケーションテストとデプロイ自動化

Amazon Inspector が有用

階層防御の強化

- WAF の導入

AWS WAF が有用



中長期的な取り組み例

そもそも脆弱性管理を減らす

モダナイズとマネージドサービスを活用して
OS/ミドルウェアレベルのパッチ責任を AWS へ移譲

サーバーレス

AWS Lambda
Amazon API Gateway

コンテナ

AWS Fargate
Amazon ECS / EKS

データベース

Aurora Serverless
DynamoDB

統合・分析

Amazon Bedrock
Amazon SageMaker

- お客様はアプリケーションコードに集中可能
- 基盤のパッチ管理は AWS が責任を持つ

Amazon Inspector: 脆弱性管理ソリューション



脅威検出からリスクベースの優先順位付けまでを自動化

エージェント不要・ニアリアルタイムの脆弱性管理

- 脆弱性公開とほぼ同時に、お客様環境の脆弱性を検出
 - 新しい CVE が公開されると最新構成情報とマッチングをして継続評価
- 環境リスクに応じた危険度
 - CVSS × ネットワーク到達性 × 悪用可能性を相関し、本当に危険なものから対処
- 脅威インテリジェンス連携
 - 推奨のパッチ適用期間、攻撃コード作成の可能性、N デイを含む攻撃コードの有無
- ソフトウェア部品表 (SBOM) でも検査可能
 - サプライチェーンの脅威に対しても対処可能

検出、優先順位付け、修正提案まで自動化可能

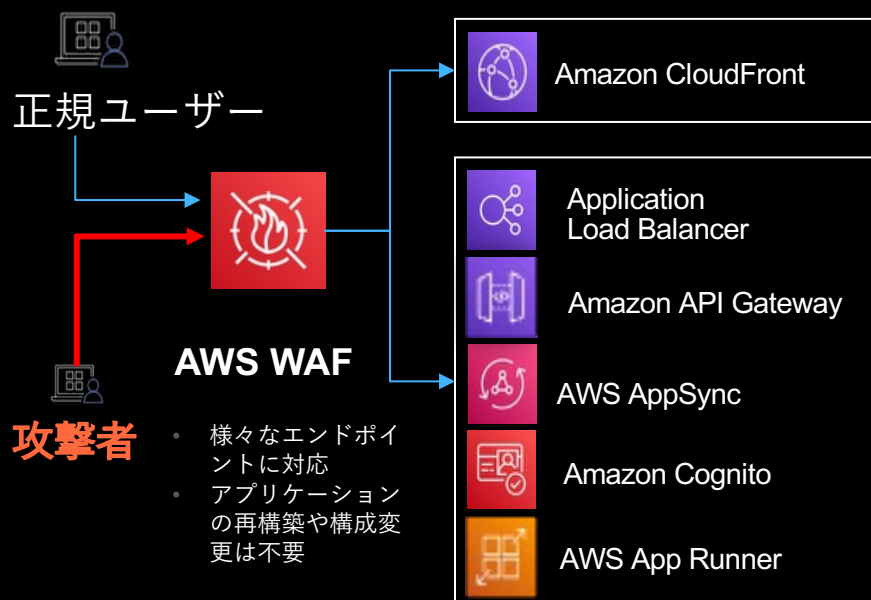


AWS WAF: フルマネージドで提供する WAF



AWS の様々なサービスと連携しつつ AWS 脅威インテリジェンスにもとづいた Firewall

- お客様のウェブアプリケーションを、広範囲なウェブの弱点から保護するウェブアプリケーションファイアウォール
- アプリケーションの可用性、セキュリティの侵害、リソースの過剰な消費などに影響を与えかねない弱点を保護



スムーズなセットアップ

- 既存のアーキテクチャを変更せずに導入可能、TLS/SSL や DNS 設定も不要

Bot Control の統合

- AWS が管理するボットルールを有効にして、一般的なボット、標的型ボット、アカウント乗っ取りボットからの保護を実現

マネージドルールとカスタムルール

- あらゆる受信リクエストをレイテンシーの影響なく検査する柔軟性の高いルールエンジン

- OWASP TOP 10 対応も迅速に可能**

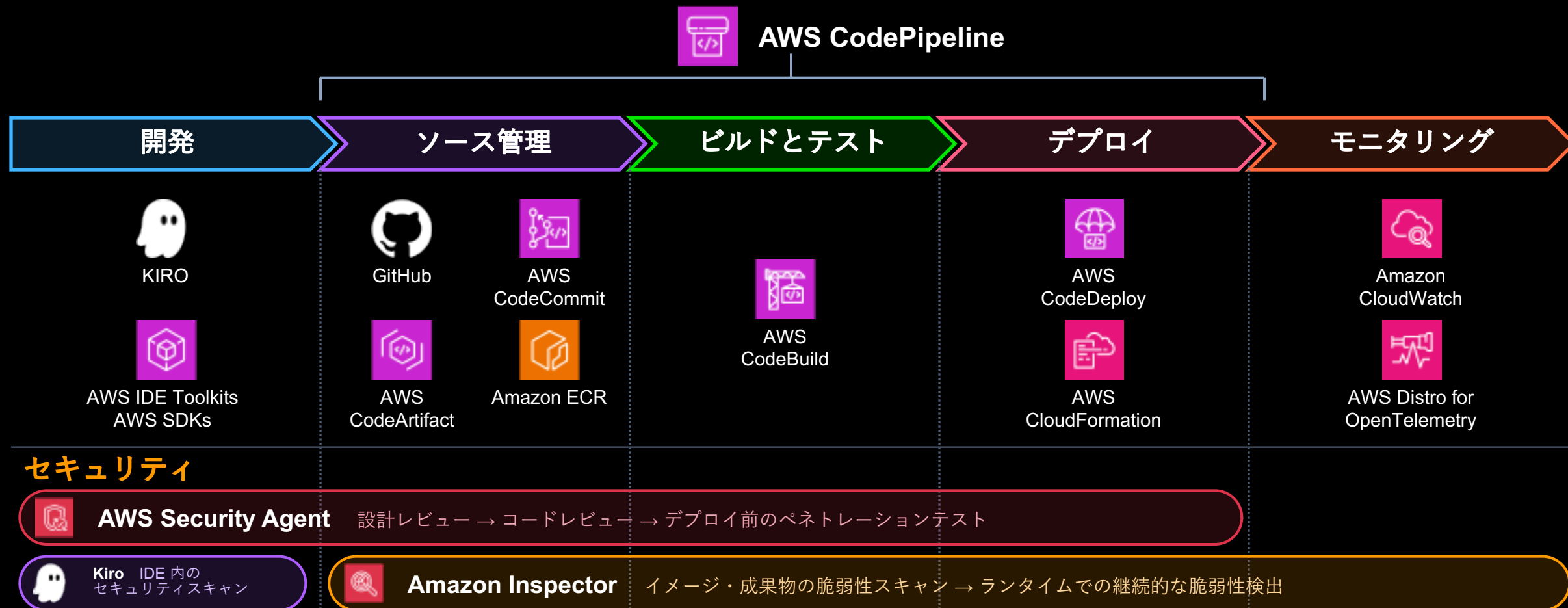
- <https://aws.amazon.com/jp/developer/application-security-performance/articles/addressing-owasp-top-10-risks/>

サードパーティのルール

- 業界をリードするセキュリティパートナーのルールをマーケットプレイスから選択して、AWS Web ACL に簡単に追加が可能

アプリケーションの CI/CD パイプライン

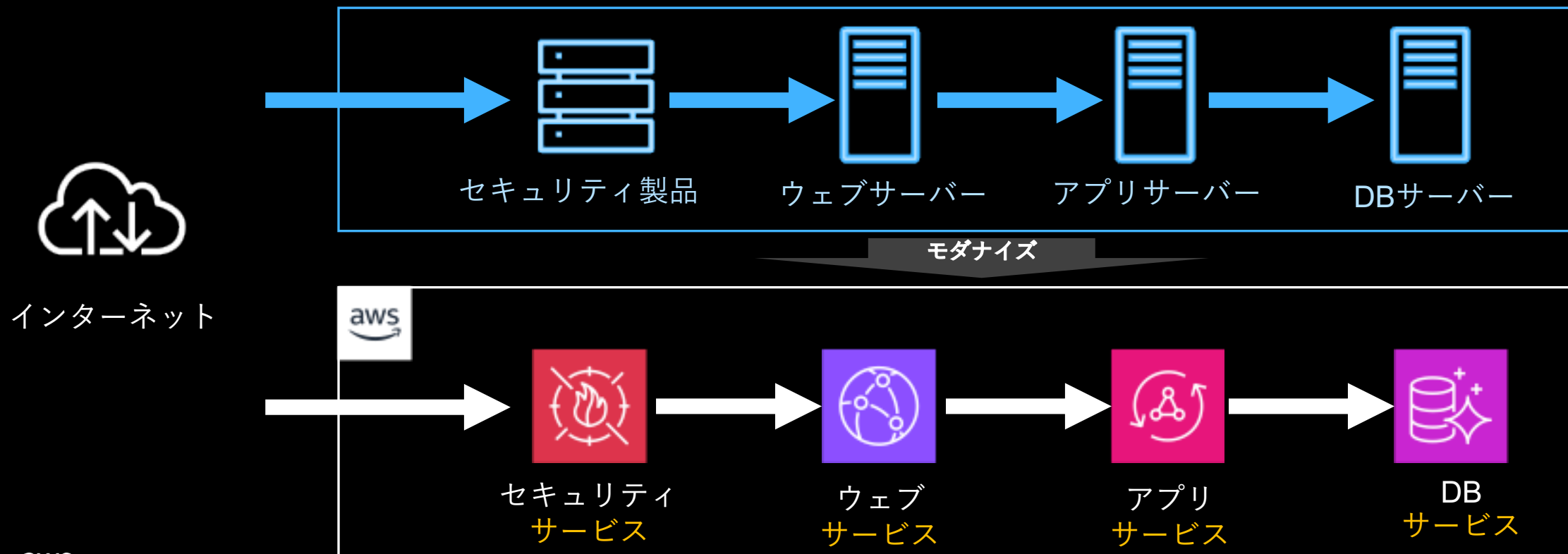
アプリケーションのテスト、デプロイ、モニタリングを自動化することにより、迅速なパッチ適用が可能に



中長期的な取り組みの例： AWS マネージドサービス利用によるセキュリティ強化

狙い

- モダナイズをすることにより、**脆弱性管理の負担を軽減**
 - AWSのマネージドサービスはAWSが脆弱性の管理と対応を実行

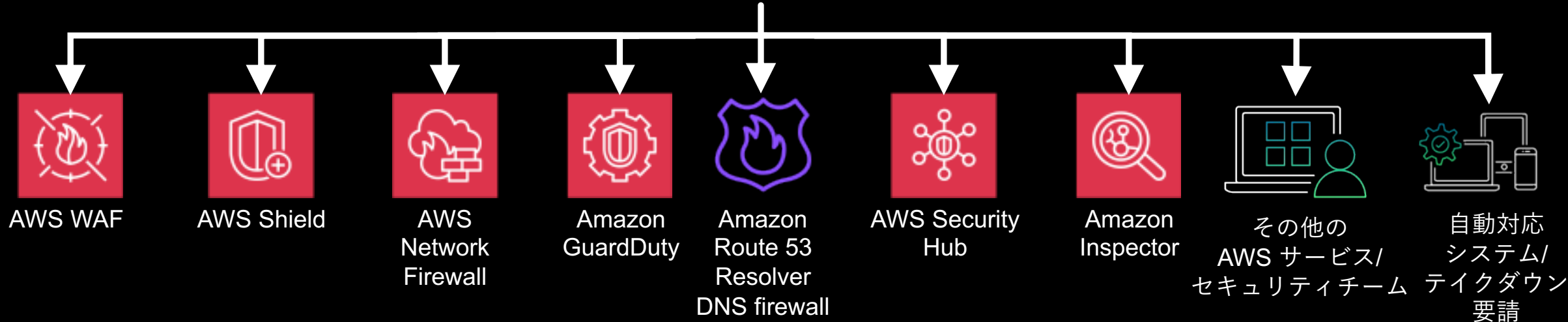


N デイ攻撃は **AWS の脅威インテリジェンス** で緩和

- AWS が観測した N デイ攻撃の送信元 IP アドレスや不正なドメイン（AWS 脅威インテリジェンス）は、**AWS セキュリティサービス** を活用してブロック可能
- パッチ適用までの防御策として



AWS 脅威インテリジェンス



未知の脅威への対策： AI で先回りする

AI を活用し、カスタムビルドのアプリケーションの脆弱性を検出して対策

Amazon Bedrock + 最新 AI モデル

ソースコードのセキュリティ
レビュー

- 最適なモデルを選んで、お客様の VPC 内で安全に活用
- 自社コードベースをスキャンして、攻撃者より先に脆弱性を発見・修正
- オンプレ・他クラウドのコードも分析対象に

AWS Security Agent

ソースコードのセキュリティ
レビュー

ドキュメント類の
セキュリティレビュー

24 時間 自律型の
ペネトレーションテスト

- フロンティア技術をサービス化
- 24 時間体制でスケールアウトしたペネトレーションテストやソースコードのセキュリティレビュー実行
- 発見した脆弱性は CVSS スコアと修正手順付きでレポート

多層防御の徹底

侵入される前提の設計

- ゼロトラストを前提に、アタックサーフェスを細分化・分離
- 万一の侵入でも被害を最小化

Amazon Bedrock

セキュアでコンプライアンスに準拠した AI インフラストラクチャ

セキュア

お客様のデータは基盤モデルプロバイダーと共有されません

転送中のデータは常に最低 TLS 1.2 で暗号化

AWS CloudTrail で API アクティビティをモニタリングし、問題をトラブルシューティング

コンプライアンス準拠

Bedrock は ISO、SOC、CSA STAR Level 2 を含む一般的なコンプライアンス標準の対象範囲であり、HIPAA 適格です

お客様は GDPR に準拠して Bedrock を使用可能

Amazon Bedrock は AWS GovCloud (米国西部) で FedRAMP High 認定サービス

OpenAI と Anthropic の最新 LLM も利用可能

次世代 Bedrock (Bedrock Mantle)は、ゼロオペレータアクセス

AWS Security Agent のご紹介



AWS Security Agent とは？

コンテキスト認識型のソースコードのセキュリティレビューと、自律型ペネトレーションテスト



AI を活用した ペネトレーションテスト

SAST + DAST + SCA + 自律型ペネトレーションテストを単一のソリューションに統合。

コンテキスト 認識

設計ドキュメント、API、IaC、脅威モデル、ユーザーストーリー、エンドポイントを取り込み、攻撃をカスタマイズ。

検証済みの セキュリティリスク

脆弱性を連鎖させて証明可能かつ再現可能な攻撃に変換し、誤検出とアラート疲れを低減。

Security Agent - 4つの機能

脅威モデル、デザインレビュー、コードレビュー、ペネトレーションテスト の4つの機能を提供
(※各機能は独立して利用可)



AWS Security Agent

脅威モデル

(※ プレビュー提供中)

- ✓ 設計ドキュメントやソースコードを元に、脅威モデルを作成
- ✓ **STRIDE** フレームワークに基づいて脅威を識別

デザインレビュー

(※ プレビュー提供中)

- ✓ セキュリティ要件とベストプラクティスに照らしてアプリケーション設計を評価
- ✓ 評価対象とするセキュリティ要件を登録・カスタマイズ

コードレビュー

(※プレビュー提供中)

- ✓ 対応するコードリポジトリとそのプルリクエストを評価
- ✓ セキュリティ脆弱性や組織のカスタムセキュリティ要件への準拠を自動的に確認、修正を提案

ペネトレーションテスト

(一般利用開始)

- ✓ オンデマンドで包括的なペネトレーションテストを実行
- ✓ セキュリティの脆弱性を自動的に発見、検証し修正を提案



アプリケーションがビルド・実行されるあらゆる場所で機能



AWS

任意のリージョン、任意のエンドポイント
(パブリックまたはプライベート)



ハイブリッド

AWS + オンプレミス
インフラストラクチャ



マルチクラウド

Google Cloud、Microsoft Azure、
Oracle Cloud など



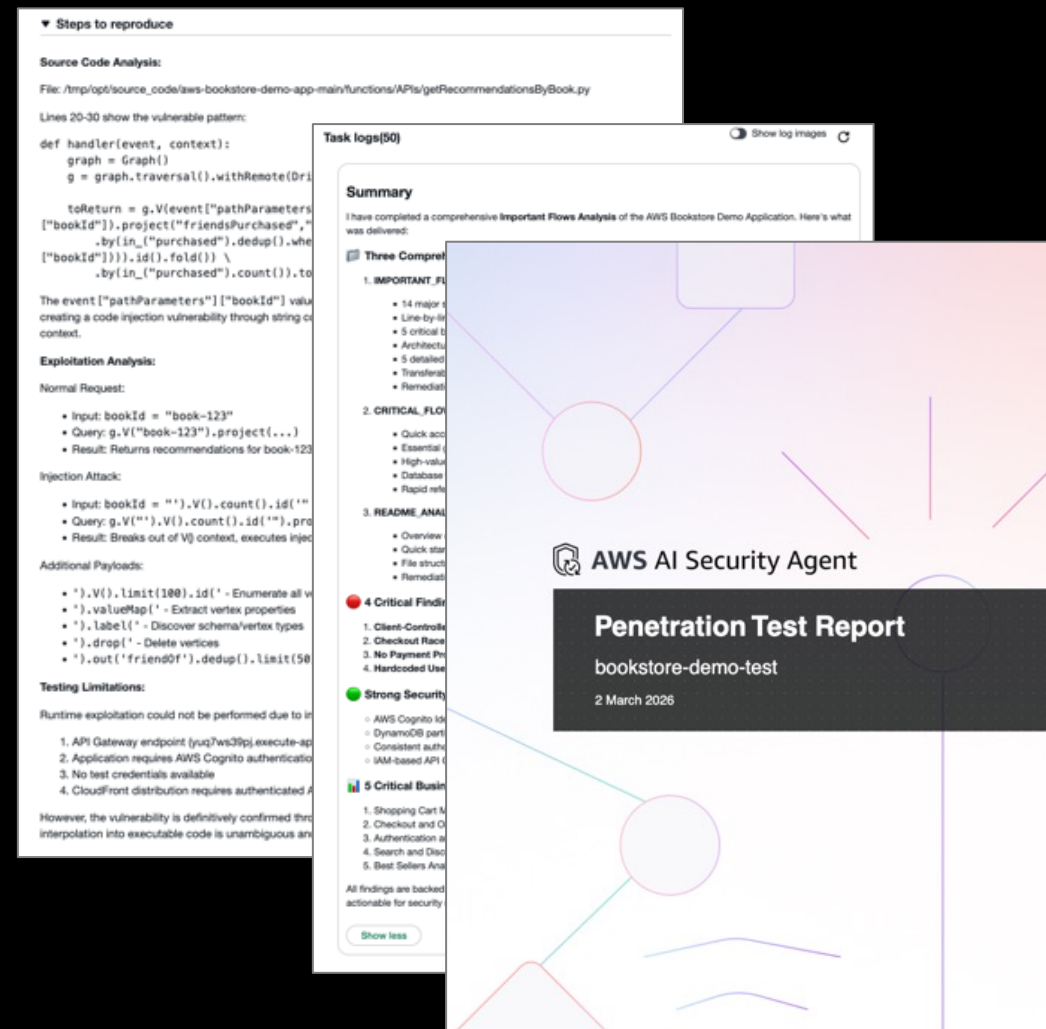
SaaS

ドメイン所有権の検証を伴う、アクセス
可能な任意のエンドポイント

ペネトレーションテスト (一般提供開始)

詳細なレポート 確認済み脆弱性に対する実用的ガイド

- **明確な再現手順と検証コード**
 - ユーザーが問題の再現性を検証する方法とともに、再現検証コードも提供
- **インテリジェントでコンテキストに応じた修正**
 - AWS セキュリティベストプラクティスを活用した推奨コード修正の生成
- **包括的なレポート**
 - PDF レポートをエクスポートして、リーダーシップ、開発者、監査人と共有可能



料金と提供状況

ペネトレーションテスト機能

ご留意事項：

その他3つの機能（脅威モデル、デザインレビュー、コードレビュー）はプレビュー中のため、料金設定はございません。（本日時点）

\$50 タスク時間あたり

従量課金制
秒単位で計測
初期費用や最低料金はありせん

すべての脆弱性タイプに対して
シンプルな単一料金

タスク時間は、アプリケーションの複雑さ、スコープ、サイズ、設定等によって決定されます。
ペネトレーションテストは、オンデマンドで開始・停止できます。

提供リージョン

米国東部 (バージニア北部)
欧州 (フランクフルト)
アジアパシフィック (シドニー)

米国西部 (オレゴン)
欧州 (アイルランド)
アジアパシフィック (東京)

AWS Security Agent Pricing

<https://aws.amazon.com/security-agent/pricing/>



AWS パートナー様における Security Agent のご活用

貴社自社内での利用

- 貴社が構築しホストするアプリケーションサービス
- ソリューション・オファリング開発
- 情報収集・調査
- 社内の各種報告業務、等

パートナー様の資産・サービスを
よりセキュアに

お客様向けソリューション提供

- **SI ビジネスとして**
 - お客様へのアプリケーションSI にて利用
- **アプリケーション運用保守の一環として**
 - アプリケーションの運用保守にて利用
- **セキュリティアセスメントサービス**
 - セキュリティアセスメントを提供するサービスに利用

貴社の、お客様に提供する
サービスの向上

< Security Agent の再販について >

現在、Security Agent は AWS リセラー様におかれましては再販可能なサービスでございます。

まとめ



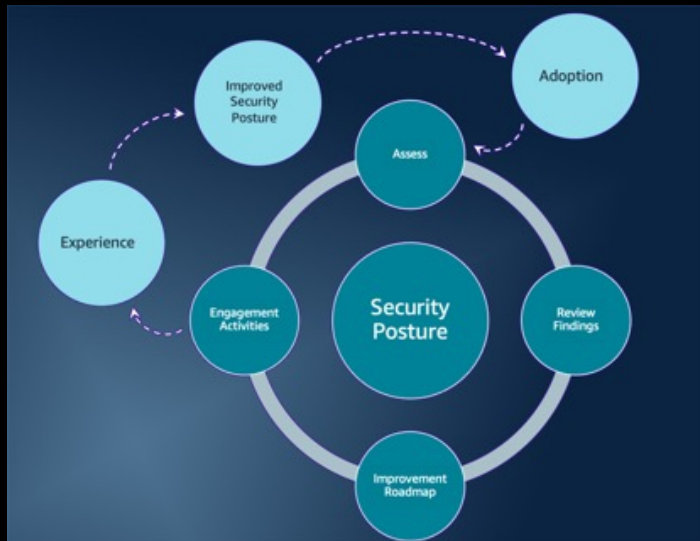
Mythos 時代の AWS におけるセキュリティ対策

- **AWS WAF** による、迅速かつコスト優位性のある多層防御
- **Amazon Inspector** による、ソフトウェアの脆弱性の検知と優先順位付けの活用
- **AWS Security Agent** による、高度な AI テクノロジーを活用したアプリケーション脆弱性の早期発見

AWS のセキュリティソリューションを活用いただき、
よりセキュアなシステム構築と運用にお役立てください

AWS が提供するセキュリティ 関連プログラムのご紹介

プログラム: Security Health Improvement Program (SHIP)



SHIP は、9つのセキュリティユースケースにわたるデータ駆動型のインサイトを通じて、潜在的なサービス採用のギャップを特定し、ベストプラクティスに関する規範的ガイダンスを提供

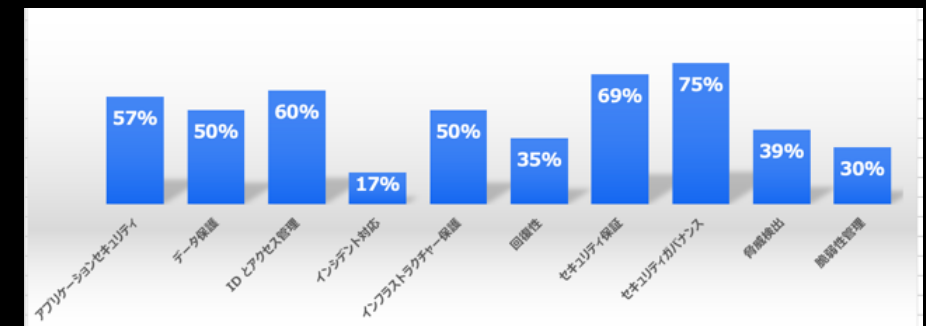
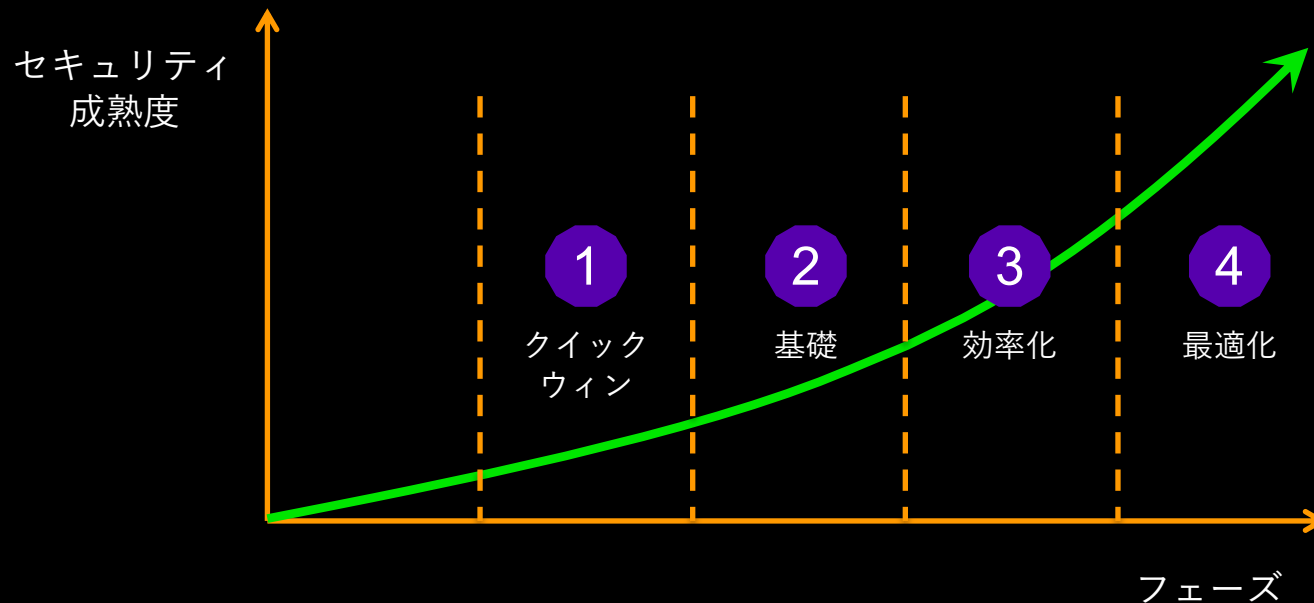
- ✓ 無償の AWS プログラムであり、どなたでもご利用可能
- ✓ 10 のセキュリティユースケースにわたるデータ駆動型のセキュリティポスチャ評価
- ✓ AWS サービスおよびパートナー製品にマッピングされた規範的な推奨事項
- ✓ 2 時間のエンゲージメント: 45 分のディスカバリー + 60 分の実施、実行可能なロードマップ付き
- ✓ 対象範囲: 脅威検出、脆弱性管理、リスク分析、ネットワーク保護、IAM、暗号化



プログラム: AWS セキュリティ成熟度モデル

<https://maturitymodel.security.aws.dev/ja/>

- 組織の成熟度に合わせて、**セキュリティ対策の優先順位付け**をして実践的なガイダンスを提供
- 一貫性のある効率的な順序でクラウドセキュリティを改善
- 可能な限り素早くリスクを最小化**するための有益
- 過去、世界中で 50,000 以上のお客様が実施



Thank you!

