AWS Continuum とは

AI がセキュリティの穴を
見つける → 確認する → 直す まで手伝う、AWS の新サービス

発表: 2026年6月17日（AWS Summit New York）
作成: 2026年6月21日

一言で言うと

脆弱性を「検出して終わり」ではなく、
本当に危ないか確かめ、直すところまで AI が支援する。

ステップ	意味
FIND	既存ツール＋自前スキャンで穴を洗い出す
VERIFY	Sandbox で「本当に攻撃できるか」を再現
FIX	修正案を出し、承認後に修復へ進める

なぜ必要か

AI の進化で、脆弱性は **ますます速く、たくさん見つかる**。
しかし現場では、そのあとが人の手で止まりがち。

困りごと	具体例
どれが本当に危ない？	検出結果が数千件。全部は直せない
本当に悪用できる？	誤検知が多く、優先順位がつけにくい
誰が直す？	開発・インフラ・セキュリティが分断

> Continuum は、この **「見つけたあと」** を AI で自動化しようとするサービス。

何をしてくれるか（4 ステップ）

#	ステップ	内容
1	**発見**	既存ツールの結果＋自前スキャンで穴を洗い出す
2	**優先順位**	本番利用・外部到達性などで重要度を判断
3	**検証**	隔離環境で攻撃を再現し、本当に危ないか確認
4	**修復**	修正案を提示し、承認後にパッチや設定変更へ

> 単に「穴がある」と言うだけでなく、**自社環境を踏まえて「本当に直すべきもの」に絞る**。

Sandbox での検証とは

本番と切り離した安全なテスト環境 で、「本当に攻撃できるか」を再現する。

1. スキャンで「脆弱性の疑い」を検出
2. Sandbox に同様の環境を用意
3. その疑いを使って攻撃を再現
4. 結果で本物か誤検知かを判断

結果	判断
再現できた	本当に危ない → 優先して直す
再現できなかった	誤検知の可能性 → ノイズを減らせる

4 つの機能

機能	状態	内容
コード脆弱性の自動対応	限定プレビュー	発見→優先→検証→修復を一気通貫
ペネトレーションテスト	利用可能	擬似攻撃で穴を探す（週単位→時間単位）
コードスキャン	プレビュー	ソースコードのセキュリティ問題を分析
脅威モデリング	プレビュー	設計・コードから攻撃面を自動整理

> 以前の **AWS Security Agent** の機能は、Continuum に統合された。

人間の承認はどうなるか

いきなり全部を自動で直すわけではない。**段階的に自動化を広げる** 設計。

モード	動き
学習モード（最初）	AI が提案 → **人が確認して承認**
適用モード（慣れてから）	信頼できる範囲は **自動で対応**（ルールは自分で設定）

> 「AI に任せきり」ではなく、**人がコントロールしながら自動化を広げる**。

既存ツールとの関係

Continuum は **GuardDuty や Security Hub の代わりではない**。併用する。

サービス	役割
GuardDuty	不正アクセスなどの **脅威を検知**
Security Hub	セキュリティ情報を **一か所に集約**
Continuum	脆弱性を **見つけて・判断して・直す** まで支援

> 検知（既存ツール）＋ 対応自動化（Continuum）＝ セキュリティ運用の加速

発表・提供状況

項目	内容
発表日	2026年6月17日（AWS Summit New York 2026）
提供状況	**限定プレビュー**（招待制に近い段階）
申し込み	製品ページからアクセス申請

参考リンク

- AWS Continuum 製品ページ
- 公式発表（What's New）
- AWS セキュリティブログ（日本語）

まとめ

項目	内容
何か	AI で脆弱性を見つけ・判断・検証・修復するサービス
誰向けか	検出結果が増え、対応が追いつかないセキュリティ・開発チーム
特徴	自社環境を理解し、優先順位をつけ、誤検知を減らす
注意点	まだ限定プレビュー。既存ツールと併用する

> **一言:** 「見つけたあと」を AI が手伝う、セキュリティ運用の Continuum