Amazon MWS
アプリケーションの保護

ログ記録と監視

amazonservices

お知らせ

Amazonの出品者と開発者には、このドキュメントの情報を独立評価する責任があります。このドキュメントは、(a)情報提供のみを目的としており、(b) 現行の業務を説明するもので(ただし、現行の業務は予告なく変更されることがあります)、(c) Amazon.com Services LLC (Amazon) およびその関連会社、サプライヤー、またはライセンサーからのいかなる確約や保証も伴いません。Amazonマーケットプレイスwebサービス(Amazon MWS)の商品またはサービスは、明示または黙示を問わず、いかなる種類の保証、表明、条件もなく、「現状のまま」提供されます。Amazon MWSに関するAmazonの責任は、AmazonのMWS契約(Amazon出品パートナーAPI開発者契約、Amazon出品パートナーAPIライセンス契約など)によって管理されており、このドキュメントはAmazonといかなる当事者間の契約の一部ではなく、それを修正するものでもありません。

1 目次

データ保護ポリシーの要件

開発者は、ログを収集して、アプリケーションおよびシステムに対するセキュリティ関連イベント（アクセスや承認、侵入行為、設定の変更など）を検出する必要があります。開発者は、このログメカニズムをAmazonの情報へのアクセスを提供するすべてのチャネル（サービスAPI、ストレージレイヤーAPI、管理ダッシュボードなど）に実装する必要があります。すべてのログには、そのライフサイクルを通じて不正アクセスや改ざんを防止するためのアクセス制御が必要です。ログそのものにPIIを含めることはできません。また、セキュリティインシデントの場合、ログを90日間以上保持して参照できるようにする必要があります。開発者は、ログとすべてのシステム活動を監視するメカニズムを構築して、不審なアクション（複数の不正な呼び出し、予期しない要求率とデータ取得量、カナリアデータレコードへのアクセスなど）に対する調査アラームをトリガーする必要があります。開発者は、監視アラームのトリガーに応じて調査を行い、開発者のインシデント対応計画に記録する必要があります。

ログ記録と監視の基礎

ログは、組織のシステムおよびネットワーク内で発生したイベントのレコードです。ログはログエントリで構成されます。各エントリには、システムまたはネットワーク内で発生した特定のイベントに関連する情報が含まれます。ログは、主に問題のトラブルシューティング用として登場しましたが、現在では、システムおよびネットワークのパフォーマンスの最適化、ユーザーのアクション記録、悪意のあるアクティビティ調査へのデータ提供など、組織内で機能を提供できるようになりました。組織内では、コンピューターセキュリティに関連するレコードを含むログが必要です。コンピューターセキュリティログの一般的な例には、ユーザー認証の試行を追跡する監査ログと、潜在的な問題を記録するセキュリティデバイスログがあります。このガイドでは、コンピューターのセキュリティ関連情報を含むログのみを取り扱います。

ログ記録と監視の必要性

ログ管理により、一定の期間にわたってレコードを安全に保持し、十分な量の詳細データを保存できます。定期的なログレビューと分析は、セキュリティインシデント、ポリシー違反、不正行為、および運用上の問題を発生直後に特定するのに役立ちます。また、このような問題の解決に役立つ情報も提供します。ログは以下で役立ちます。

- 監査とフォレンジック分析の実行。
- 組織の内部調査のサポート。
- ベースラインの確立。
- 運用動向と長期的な問題の特定。

たとえば、侵入検知システムは、外部ホストからサーバーに発行された悪質なコマンドが記録された後、イベント情報の主要なソースとなります。インシデント対応者は、イベント情報の二次的なソースであるファイアウォールログをレビューし、同じ送信元IPアドレスからの他の接続試行を探します。開発者は、感染したホストからのログ精度に特に注意する必要があります。不安定な転送メカニズムなど、適切に保護されていないログソースは、ログ構成の変更やログ変更の影響を受けやすくなります。

ログ記録と監視のベストプラクティス

ログの分散、一貫性のないログ形式、およびログ数はすべて、ログの生成、保存、分析の管理を困難にします。組織がこれらの課題を回避し、解決するために、従うべき主なアクションがいくつかあります。以下の4つの対策は、このような問題の解決策について簡単に説明しています。

- **ログ管理に適切な優先順位を付け、その要件と目標を定義する。**組織は、ログ記録と監視のメカニズムが、適用法、規制、契約上の要件、および組織内の既存のポリシーに準拠しているか確認する必要があります。
- **ポリシーと手順を確立する。**適切なポリシーと手順により、組織全体で統一されたアプローチが確保されます。また、法規制要件を確実に満たせます。定期的な監査、テスト、および検証は、組織全体でログ記録標準とガイドラインが順守されているかを確認するメカニズムです。
- **安全なログ管理インフラストラクチャーを構築し、維持する。**組織にログ管理インフラストラクチャーを実装し、コンポーネントの相互作用を決めておくと、とても役立ちます。これは、偶発的または意図的な変更や削除からログデータの整合性を保ち、ログデータの機密性を維持するのに役立ちます。マルウェアインシデントの頻発など、極限状況でのピーク数などのログデータ予測数、侵入テスト、脆弱性スキャンを十分に処理できるよう、堅牢なインフラストラクチャーを構築することが不可欠です。
- **ログ管理を担当する全スタッフに適切なサポートとトレーニングを提供する。**サポートには、ログ管理ツールおよび関連ドキュメントの提供、ログ管理活動に関するテクニカルガイダンスの提供、ログ管理スタッフへの情報発信などがあります。

国立標準技術研究所（NIST）では、ログ記録管理策を監査と説明責任（AU）ドメインで定義する一方、監視管理策をシステムと情報の整合性（SI）ドメインで定義しています。ログは、このセクションで説明する管理策のほか、Amazon MWS DPPのアクセス制御、最小権限、暗号化、ストレージ要件に準拠している必要があります。

セキュリティ監視

API 呼び出しのログ記録と監視は、セキュリティおよび運用上のベストプラクティスであるとともに、業界および規制の順守要件の重要なコンポーネントです。組織では、ログ記録と監視を実行する要件と目標を定義する必要があります。要件には、適用法、規制、およびデータ保持ポリシーなどの既存の組織ポリシーがすべて含まれている必要があります。

開発者システムには、セキュリティログのソースが複数ある場合があります。さまざまなネットワークコンポーネントでログファイルが生成されます。コンポーネントには、ファイアウォール、IDP、情報漏洩対策（DLP）、オーディオ/ビジュアル（AV）システム、オペレーティングシステム、プラットフォーム、アプリケーションなどがあります。ログの多くはセキュリティに関連しており、ログファイル戦略の一部である必要があります。セキュリティ以外のログは、セキュリティ戦略から除外するようお勧めします。ログには、ユーザーアクティビティ、例外、セキュリティイベントがすべて含まれ、今後の調査のため、90日間以上保存する必要があります。

NIST 800-53を使用する開発者は、以下の管理策を参照できます（**SI-4**：**情報システムの監視**）。この管理策の目的は、開発者が環境を適切に監視し、異常なアクティビティの検知時に通知を受け取ることです。予期せぬコスト上昇や計算量の増加など、セキュリティ関連以外と思われるメトリクスは、検知されていないセキュリティイベントを示すことがあります。監査メトリクスを定義する際は、このような指標を必ず考慮してください。開発者が新しい指標を特定した場合、何度も発生するイベントを検出して対応する監視をすべて更新する必要があります。対応に関するガイダンスについては、このドキュメントの「インシデント対応」のセクションを参照してください。

さらに、開発者は環境をさらに保護できるよう、管理強化に細心の注意を払う必要があります。たとえば、**SI-4（1）システム全体にわたる侵入検知システム**は、侵入が発生するとすぐに通知を生成します。

一般的な要件

- 各サービスに関連するログへアクセスし、ログをレビュー、オフロードする方法を定義する。
- 購入者または出品者の氏名、住所、メールアドレス、電話番号、ギフトメッセージの内容、アンケートの回答、支払い詳細、購入、クッキー、デジタル指紋（ブラウザ、ユーザーのデバイスなど）、IP アドレス、場所、インターネットに接続されたデバイスの製品コードなど、Amazon の購入者の個人を特定できる情報（PII）を記録しない。
- 本番環境の顧客データやトラフィックを処理するシステムでは、デバッグレベルのログ記録を有効にしない。
- セキュリティインシデントの場合、ログは参照用に90日間以上保持する。
- 監査可能なイベントを年一度、または大幅な変更があった場合にレビューする。

- ログは、一元的かつ安全に保存する。
- すべてのシステムは、同じ日時で設定する。各システムの時間設定が異なると、インシデントが発生した場合に、エンジニアが追跡可能性テストを実行するのが困難になります。

識別

ログ情報が不十分だと、フォレンジック調査に悪影響が及び、エンジニアがインシデントの根本原因を突き止めることができなくなります。開発者は、ログに記録されたシステムの全領域を特定する必要があります。Amazon では、これらのログに捕捉されたパラメーター、API 呼び出し、syslog を文書に記録するようお勧めします。

セキュリティの監視は、次の質問に答えることから始まります。

- 測定すべきパラメーターは何か？
- どのように測定すべきか？
- これらのパラメーターのしきい値は何か？
- エスカレーションプロセスはどのようなものか？
- ログはどこに保存されるか？

ログファイル設計時に考慮すべき事項

開発者は、ログファイル設計時に次の点を考慮する必要があります。

- **収集。**ログファイルの収集方法に注意します。通常は、オペレーティングシステム、アプリケーション、またはサードパーティ/ミドルウェアエージェントがログ情報を収集します。
- **保存。**複数のインスタンスからのログファイルを一元的に管理すると、ログの保持、分析、関連付けに役立ちます。
- **転送。**分散ログを、安全で、信頼性が高く、タイムリーに集中管理できる場所に転送します。
- **分類。**分析に適した形式で、さまざまなカテゴリーのログファイルを提示します。
- **分析/関連付け。**ログ内のイベントを分析し、関連付けると、ログからセキュリティインテリジェンスを得ることができます。リアルタイム、または定期的にログを分析します。
- **保護/セキュリティ。**ログファイルは機密情報です。ネットワーク制御、ID、アクセス管理、暗号化、データ整合性認証、改ざん防止のタイムスタンプによりこれらを保護します。

計画作成と実装

組織は、運用ホスト上の、認証を受けたオペレータによるアクション、Amazonの情報を含むシステム内のすべての依存関係を記録する必要があります。

開発者は、以下に準じてログ記録された詳細な追加情報を検索できます（NIST管理策**AU-2**: **監査イベント**）。この管理策により、開発者は組織に影響を与えるセキュリティイベントを定義することができます。この管理策の名前は「監査イベント」ですが、ログ記録は開発者がイベントを捕捉してレビュー（監査）できるメカニズムなので、ログ記録を重視しています。Amazon MWS DPP順守には、最低限でも、アクセスと承認、侵入の試み、設定変更などのアクションがログに記録されている必要があります。

さらに、管理策**AU-3**: **監査記録の内容**には、ログに記録する内容が定義されています。特に、Amazon MWS DPPに必要な項目が取り上げられているため、補足ガイダンスには注意してください。その他の推奨項目のうち、タイムスタンプ、送信元および送信先アドレス、ユーザー/プロセス識別コード、イベントの説明、成功/失敗表示、関連するファイル名、アクセス制御またはフロー制御ルールをメモしておきます。イベント結果には、イベントの成功または失敗のインジケーター、およびイベント発生後のシステムのセキュリティおよびプライバシー状態などのイベント固有の結果が含まれます。セキュリティイベントが発生した場合、これらの項目は、イベントが発生したシステムに適切に対応する際に役立ちます。

開発者は、Amazonの情報へのアクセスを提供するアプリケーションとシステムに関連するすべてのログについて、次の質問に答える必要があります。

- ロググループの構成は？ 捕捉するイベントと関連のメタデータは何か？
- 保管時および輸送中のログの保護方法は何か？
- ログの保存期間は？
- ログの監視方法とアラームの生成方法は？
- 機密の内容（パスワード、認証情報、PII）を電信ログやサービスログからスクラブしているか。
- 違反通知やインシデント対応のサポートにどのログを使い、関連付けているか。
- ログに顧客対応アクションがすべて捕捉されているか。
- ログに内部（サービス内）および外部（サービス間）API呼び出しがすべて捕捉されているか。
- ログにAmazon購入者のPII（読み取り、書き込み、権限の変更、削除など）に関する監査証跡が捕捉されているか。

重要なトランザクションのログ管理

Amazonの情報を含む重要なトランザクションでは、追加、変更、削除アクティビティ、またはトランザクションすべてにログエントリを生成する必要があります。各ログエントリには、以下の情報が必要です。

- ユーザー識別情報。
- イベントのタイプ:
  - アカウント管理イベント。
  - プロセスの追跡。
  - システムイベント/エラー。
  - 認証/承認チェック。
  - データの削除、アクセス、変更、権限の変更。
  - ログの作成、保存、および分析に使用されるものなど、監査機能を実行するシステムへのアクセス試行。
  - エンドポイントおよび管理ダッシュボードにサービスを提供する API リクエスト。
  - 侵入の試行。
- 日付と時刻のスタンプ。
- 成功または失敗の表示。
- イベントの起点。
- 影響を受けるデータ、システムコンポーネント、またはリソースのIDまたは名前。

監視とアラーム

MACDイベントの監視のほか、ソフトウェアまたはコンポーネントの障害を監視します。障害は、ハードウェアまたはソフトウェアの障害によるもののほか、サービスおよびデータの可用性の影響によることがありますが、セキュリティインシデントとは関係がない場合もあります。あるいは、サービス障害がDoS攻撃など、計画的な悪意のあるアクティビティが原因の可能性があります。いずれの場合でも、障害によりアラートが生成される必要があります。これを受けて、開発者はイベント分析および相関技術を使用して障害の原因を特定し、セキュリティ対応をトリガーすべきか判断する必要があります。

監視とアラームの設計時には、開発者は以下を実施する必要があります。

- システム操作すべてのログを監視するメカニズムを構築し、不審な操作に対して調査アラームをトリガーする。
- 複数の不正な呼び出し、予期しない要求率、データ取得量、カナリアデータレコードへのアクセスなど、不審なイベントのログに対して、必ずアラームを設定する。
- アラーム別にプロセスを定義し、定期的に見直す。これには、チケット、オペレーターへの通知などが含まれます。

運用の監視とこれに付随するインシデント対応計画は、定期的に見直す必要があります。監視アラームのトリガーに応じて、開発者は調査を実施し、開発者のインシデント対応計画に記録する必要があります。詳細については、Amazon MWSインシデント対応ホワイトペーパーを参照してください。

Amazon CloudWatchアラームを利用した通知

ビジネスに不可欠なアプリケーションを開発、導入、サポートする場合、サービスを確実に稼働させるには、タイムリーなシステム通知が欠かせません。たとえば、チームがAmazon Chimeを使って積極的に連携している場合、重要なシステム通知をチームのチャットルーム内で直接受信したいことがあります。Amazon Chimeの着信ウェブフック機能を使えば、これが可能になります。

Amazon CloudWatchアラームを使うと、メトリクスのしきい値を設定し、Amazon Simple Notification Service（SNS）にアラートを送信できます。メール、HTTP（S）エンドポイント、ショートメッセージサービス（SMS）メッセージを使用して、SNSより携帯電話に通知を送信できます。また、Lambda関数のトリガーも可能です。現在SNSでは、Amazon Chimeチャットルームに直接メッセージを送信できないため、その間にLambda関数を挿入できます。以上の代替として、SNSからLambda関数をトリガーすると、CloudWatchアラームからイベントデータを取り込み、Amazon Chimeに送信する前に、ヒューマンフレンドリーな形式でメッセージを作成することができます。

以下に、さまざまなコンポーネントが連携してこのソリューションが機能する仕組みを示す簡単なアーキテクチャ図を示します。

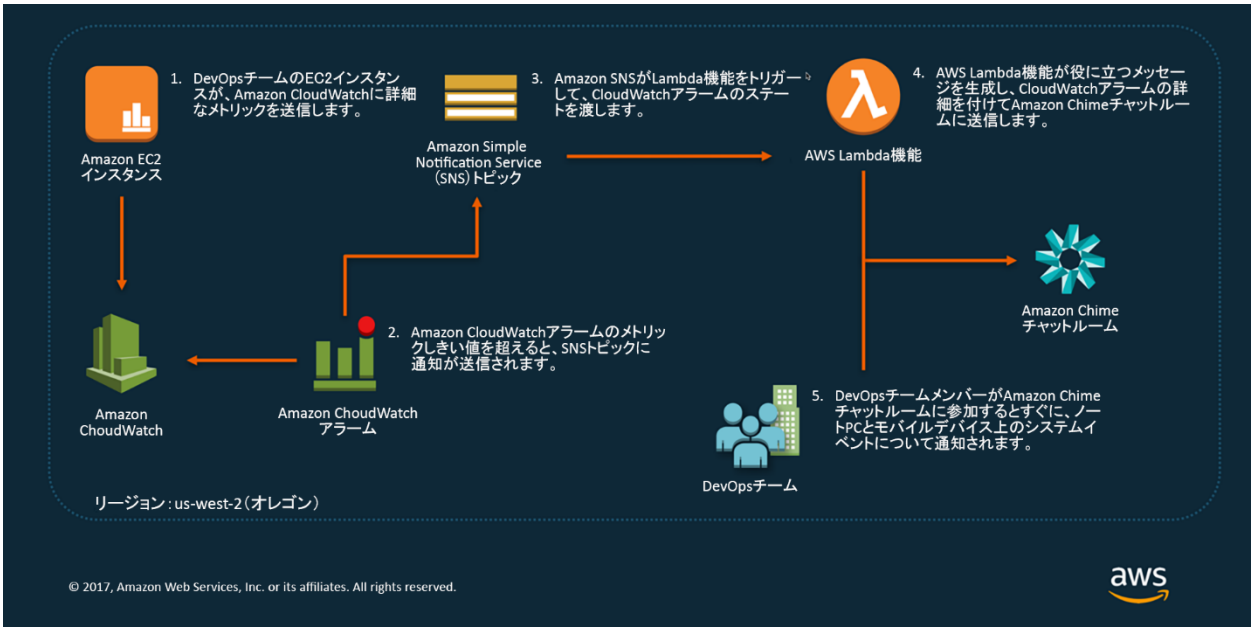

図 1：リアルタイムのAmazon CloudWatchアラーム通知設定

詳細については、各サービスの設定方法に関する AWS ドキュメントを参照してください。AWS ブログページも、使用開始時に役立つリソースです。

ログ情報の保護

ログ記録機能とログ情報は、改ざんや不正アクセスから保護する必要があります。アクティビティ痕跡の消去では、管理者ログとオペレータログが共通の対象です。

ログ情報の保護には、以下のような共通の管理策があります。

- システムコンポーネントの監査証跡が有効で、アクティブであることを確認する。
- 業務に必要な者以外、監査証跡ファイルを表示できないようにする。
- 最新の監査証跡ファイルが、アクセス制御メカニズム、物理的な分離、ネットワーク分離により、不正な変更から保護されていることを確認する。
- 最新の監査証跡ファイルが、一元的に管理されるログサーバー、または変更が困難なメディアに速やかにバックアップされるよう図る。
- 外部接続テクノロジー（ワイヤレス、ファイアウォール、DNS、メールなど）のログがセキュリティで保護され、一元的に管理される内部ログサーバーまたはメディアにアンロードまたはコピーされていることを確認する。
- システム設定や監視対象ファイルを調査する変更検出ソフトウェア、またはファイル整合性監視を使用して、監視アクティビティの結果をレポートする。
- セキュリティポリシーと手順を取得して調査し、セキュリティログを1日1回以上確認する手順が含まれており、例外へのフォローアップが義務付けられていることを確認する。
- システムコンポーネントすべてを対象に、定期的なログレビューが実行されていることを確認する。
- セキュリティポリシーと手順に監査ログ保持ポリシーが含まれており、ビジネス要件とコンプライアンス要件の定義により、一定期間、監査ログ保持が義務付けられていることを確認する。

AWSでの一元的な保存とレポート作成

運用とセキュリティの観点から、ユーザーの行動を分析し、特定のイベントを理解するために必要なデータとコンテキストがAPI呼び出しログより提供されます。API呼び出しとITリソース変更ログを使用して、権限のあるユーザーのみがコンプライアンス要件に準じて、環境内で特定のタスクを実行したことを示すこともできます。ただし、各種システムからのログ数と変動を考慮すると、オンプレミス環境では、ユーザーが実施したアクティビティとITリソースへの変更を明確に把握するのが困難なことがあります。

AWSは、複数のアカウントとAWSリージョンからAWSログを収集、分析、表示するための一元的なログソリューションを提供します。このソリューションには、Amazon Elasticsearch Service（Amazon ES）が採用されています。Amazon ESとは、AWSクラウドのElasticsearchクラスターの導入、運用、スケーリングを簡素化するマネージドサービスです。また、Amazon ESに統合された分析および可視化プラットフォームのKibanaも採用されています。このソリューションを他のAWSマネージドサービスと組み合わせると、カスタマイズ可能なマルチアカウント環境が実現し、購入者のAWS環境とアプリケーションのログ記録と分析を開始できます。

以下の図は、一元管理のログ記録アーキテクチャを示しています。このアーキテクチャは、一元管理のログ記録のAWS実装ガイドと付属のAWS CloudFormationテンプレートを使用して、自動的に導入できます。

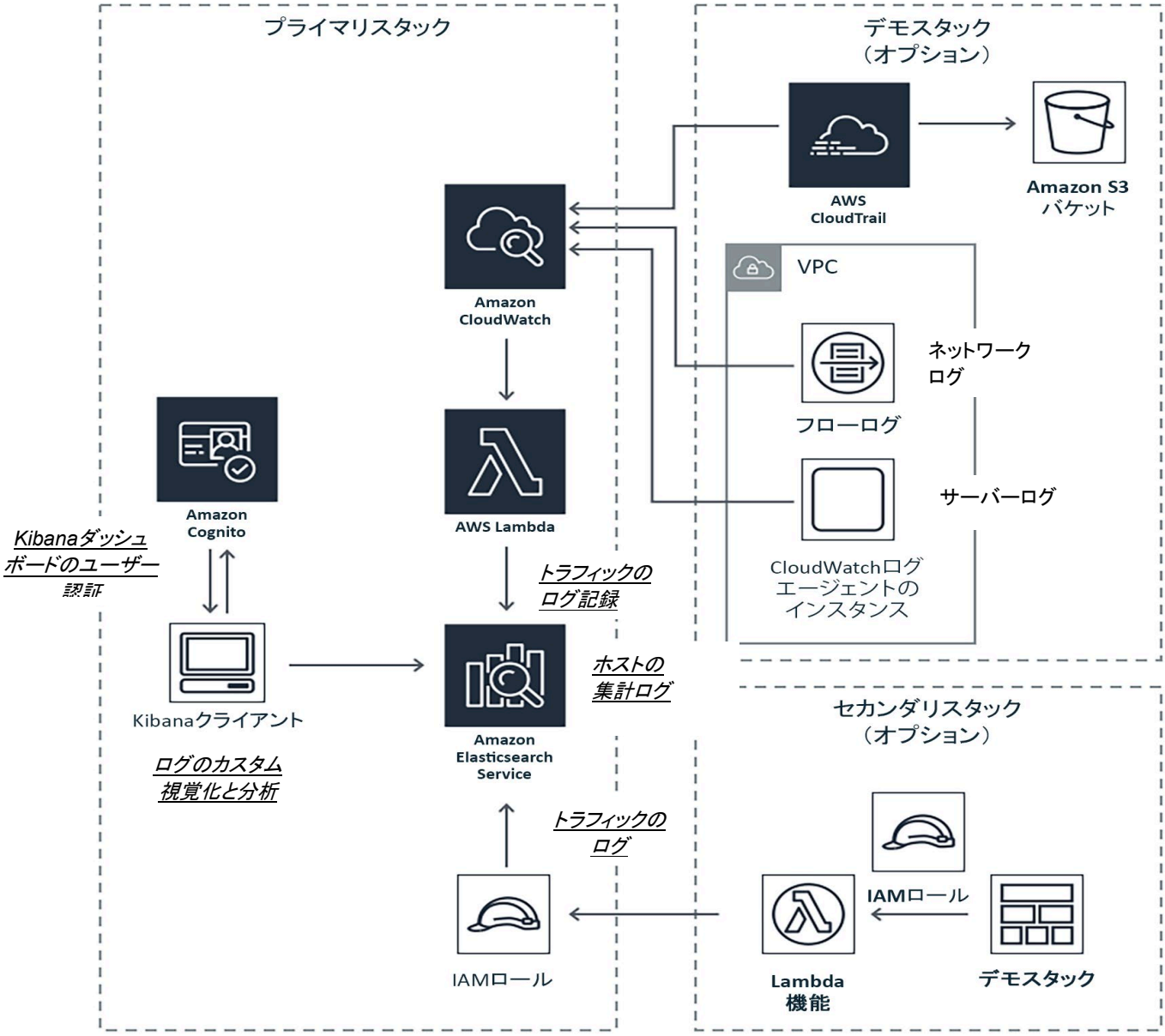

図2：AWSの一元管理のログ記録ソリューションアーキテクチャ

この一元管理のログ記録ソリューションの詳細については、AWSウェブサイトをご覧ください。AWSでのログ記録のベストプラクティスについては、以下を参照してください（「規模に応じたセキュリティ：AWSのログ記録に関するホワイトペーパー」）。

その他のリソース

- 規模に応じたセキュリティ: AWSのログ記録に関するホワイトペーパー
- AWSセキュリティのベストプラクティス
- 一元管理のログ記録
- 一元的にログを記録するAWS実装ガイド
- AWSブログ
- MWSデータ保護ポリシー
- MWS利用規約

業界の参考資料

- NIST 800-53 Rev.5（ドラフト）: 情報システムと組織のセキュリティ&プライバシーコントロール
- コンピューターセキュリティログ管理のNISTガイド

ドキュメントの変更履歴

改訂日	内容
2020年1月	初版