Amazon MWS
アプリケーションの保護

インシデント対応

amazonservices

通知

Amazonの出品者および開発者は、この文書の情報について独自の評価を行う責任があります。この文書は、(a)情報提供のみを目的として、(b)現在の慣行を示しており、これらは予告なく変更されることがあります。また、(c)Amazon.com Services LLC(Amazon)およびその関連会社、サプライヤー、ライセンサーのコミットメントまたは保証を発生させるものではありません。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 Selling Partner API開発者契約、Amazon Selling Partner APIライセンス契約など)によって管理されており、この文書はAmazonと第三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。

目次

データ保護ポリシーの要件

開発者は、セキュリティインシデントを検知して対処するための計画を作成して、維持する必要があります。その計画では、インシデント対応の役割と責任を明記し、Amazonに影響する可能性のあるインシデントのタイプを定義し、定義したインシデントタイプごとにインシデント対応手順を定め、Amazonにセキュリティインシデントをエスカレーションするためのエスカレーションパスと手順を定義する必要があります。開発者は、6か月ごと、およびインフラストラクチャやシステムの大幅な変更後に、この計画の見直しと検証を行う必要があります。開発者は、各セキュリティインシデントを調査し、(該当する場合)今後の再発を防ぐために、インシデントの説明や修復アクション、および実装された関連する修正プロセスやシステムコントロールを文書化する必要があります。開発者は、収集されたすべての証拠や記録について、証拠保全を維持する必要があります。また、該当する場合はリクエストに応じて、Amazonにたその文書を入手できるようにする必要があります。

開発者は、セキュリティインシデントの検出から24時間以内にAmazon(メールで security@amazon.com宛て)に通知する必要があります。開発者は、Amazonから開発者に書面によるリクエストがない限り、または法律で義務付けられていない限り、Amazonに代わって規制当局や購入者に通知することはできません。Amazonは、あらゆる通知について、その通知が第三者に提供される前に、通知のフォームと内容を確認し、承認する権利を有します。ただし、その通知が法律で義務付けられているものである場合は、Amazonは通知のフォームと内容を確認する権利のみを有します。開発者は、法的手続きまたは適用法に従ってデータが求められた場合、24時間以内にAmazonに通知する必要があります。

インシデント対応

開発者は、セキュリティのインシデント対応(IR)プロセスを理解し、セキュリティスタッフはセキュリティに関する問題への対応方法を理解する必要があります。専任のセキュリティチームを持たない開発者は、1)組織の一部がIRの十分なトレーニングを受け、ツールを備えるようにする、および/または2)その導入を検討してください。成熟したセキュリティチームを作りたい開発者は、次のベストプラクティスを検討してください。セキュリティイベントと調査結果のフローを通知とワークフローのシステムに組み込みます。このシステムには、チケットシステムやバグ/問題システムなどのセキュリティ情報イベント管理(SIEM)システムが含まれます。

開発者は、簡単なことから開始して、Runbookを開発し、機能を活用し、インシデント対応メカニズムのライブラリーを作成して、反復処理と改善を行ってください。これには、法務部門などのセキュリティに関与していないチームも参加する必要があります。開発者はこのようにして、IRがビジネス目標に与える影響を理解していきます。

開発者は、NISTのSP 800-61R2: コンピューターセキュリティインシデント対応ガイドのような業界ガイドラインの使用を検討してください。このNISTのガイドには、インシデント中に実行する主な手順が記載されたチェックリストが記載されています。開発者は計画を作成する際に、このチェックリストをテンプレートとして使用できます。組織の機能、目標、リスク、緩和措置を反映させた、組織固有の計画を作成できます。これらはいずれも、組織とそのシステムの規模と複雑さに応じて異なります。

このホワイトペーパーの全体にわたって、米国国立標準技術研究所（NIST）の「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（特別刊行物800-53 Rev 5）」（一般に「NIST 800-53」と呼ばれる）を参考にしています。この開発フレームワークは、セキュリティとプライバシーの脅威から組織を保護するための柔軟なコントロールを提供します。開発者は、このフレームワークを使用して組織のコントロールを実装し、強化することを検討してください。

インシデント対応の基盤

インシデント対応計画は、プロシージャやRunbookと呼ばれることが多く、インシデントを調査して修復するための手順を定義します。インシデント対応プログラムを実装するには、セキュリティイベントに対処する前に、経験と教育が不可欠です。

イベントとは、許容可能なイベント（例：既知のユーザーがコンピューターにログインしている）から有害イベント（例：未知のユーザーがコンピューターにログインしている）まで、システムやネットワークで発生するあらゆることを言います。このような有害イベントは、コンピューターのセキュリティポリシー違反、利用規約違反、契約要求事項違反などのインシデントにつながる可能性があります。

NIST 800-53を使用してIR計画を作成したい開発者には、「**IR-8**：**インシデントレスポンスプラン**」セクションが参考になります。IR-8では、IR計画の実装に必要な構成要素について詳しく説明しています。このような要素には以下が含まれます。

- 必要なリソースと管理サポートを定義すること。
- 定義された頻度で計画を見直して承認すること。
- 適切な要員にIRの責任を指名すること。

開発者は、このコントロールを実装すると、Amazon MWS DPPの要件に準拠できます。これには、6か月ごとに計画を確認して検証し、インシデントを検出してから24時間以内にAmazonに通知することが含まれます。

セキュリティイベント

明確に定義されたインシデント対応計画には、さまざまなタイプのセキュリティイベントの対応メカニズムが含まれています。開発者は、ダイアグラムを使用して、脅威とその適切な対応メカニズムとの関係をマッピングすることを検討してください。たとえば、1955年にジョセフ・ルフトとハリントン・インガムによって作成された「ジョハリの窓」は、以下に示すような、4つの枠からなるグリッドです。

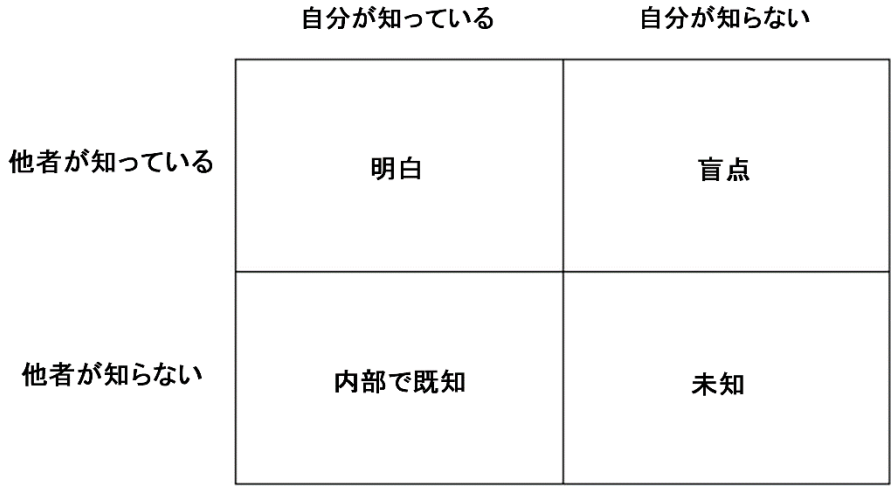

図1 – ジョハリの窓

セキュリティイベントのタイプ

「ジョハリの窓」の目的は情報セキュリティではありませんでしたが、開発者が組織の脅威を評価する方法を理解するのに役立ちます。インシデント対応ベースの概念で、この4つの窓は、明らかな脅威、内部で既知の脅威、盲点の脅威、未知の脅威です。開発者は、インシデントタイプごとに、インシデント対応手順を定義して、インシデント対応が適切であることを確認する必要があります。開発者はこれらのタイプを定義する際に、パートナーとサプライヤーの両方に関連する脅威を考えてください。連絡先情報を含めて、ツールやシステムが組織内の担当者に通知する連絡窓口を特定します。これは、Amazonを含む規制および契約上の義務におけるSLAに適合するために必要です。

明らかな脅威

明らかな脅威は、開発者とそのパートナー（Amazonなど）の両方が認識しているリスクです。たとえば、悪意のある攻撃者は通常、組織に対するサービス拒否（DoS）攻撃を利用します。DoS攻撃では、悪意のある攻撃者が一時的または無期限に、インターネットに接続するアプリケーションの機能を妨害します。開発者は、意図的な悪意のある中断からサービスを保護するメカニズムを採用する必要があります。開発者は、DoS攻撃に対する最小限のダウンタイム回復目標を定義することを検討してください。

悪意のある攻撃者は通常、アプリケーションに侵入して組織を侵害し、さらには制御しようとします。開発者は、侵入防止システム（IPS）と侵入検知システム（IDS）を導入することで、侵入の試みを軽減できます。このシステムは、ネットワークのトラフィックフローを調べて、侵入者がシステムへのアク

セスを試みていれば検知します。IPSのシステムでは、権限のないユーザーが侵入するのを防止します。それでも侵入が成功した場合は、IDSが通知を送信して、対応がトリガーされます。

内部で既知の脅威

内部で既知の脅威は、開発者がよく知っていても、Amazonなどのパートナーにあまり知られていない脅威です。これには、内部の専門知識やグループ内の知識が含まれます。たとえば、開発チームで、文書化されていないけれど構成の変更を管理する方法が確立されている場合があります。
ただし、文書化されていないプロセスを持つことにはリスクがあります。たとえば、以下のようなリスクです。

- チームは、すべての変更がテストされ承認されたと確信できません。
- コードのリリースが意図したとおりに動作しなかった場合に、チームにロールバックのメカニズムがないこともあります。
- チームは、新しい運用リリースのバグをスキャンできない可能性もあります。

開発者は、このようなシナリオを考慮して、内部で既知の脅威を軽減してください。

さらに、従業員の悪意のある、または意図しない行動などのインサイダーリスクは、環境に悪影響を及ぼす可能性があります。アクセス管理コントロールとデータ損失防止メカニズムは、このような行動の防止や検出に役立ちます。内部と外部の両方からの不正なデータアクセスを制限することは、データのセキュリティの確保と保護における重要なステップです。開発者は最小権限の原則を採用して、タスクを完了するために必要なアクセス権だけを個人またはプログラムに付与してください。既定のアクセスアカウントを削除し、共有アカウントの使用を制限することをお勧めします。必要に応じて、開発者は共有アカウントを監視し、必要な場合にのみ使用されていることを確認する必要があります。共有アカウントは、適切な管理者が使用を承認した場合のみ共有されるようにしてください。開発者は、このような監視にデータ損失防止コントロールを加えることができます。これにより、許可されていない相手と機密情報や重要な情報を共有してしまうのを防げます。このような情報には、制御を回避できる暗号化キーやアプリケーションの資格情報も含まれます（コードに埋め込まれ、GitHubで公開されている場合など）。

盲点の脅威

盲点の脅威は、パートナーがよく知っていても、開発者にあまり知られていないリスクです。適切な専門知識を持つパートナーは、その知識を共有できます。このようなリスクは、所有者が知らないうちにアプリケーションに影響を与える共通脆弱性識別子（CVE）である場合があります。開発者は明らかな脅威のリスクをよく知っているかもしれませんが、パートナーは、開発者がよく知らないコントロールとソリューションを推奨する可能性があります。パートナーはまた、内部で既知の脅威のリスクを軽減するために、きめ細かく調整された制御を確認するように備えることもできます。

その他の盲点は、規制環境の変化などです。欧州連合（EU）の一般データ保護規則（GDPR）は、世界中の企業に影響を及ぼしており、カリフォルニア州消費者プライバシー法（CCPA）など、同様の規制が急速に生まれています。このような規制は、応答メカニズムや通知方法に影響を与える可能性があります。

外部環境の監視は、このようなリスクを軽減するのに役立ちます。特に、脆弱性情報データベース（NVD）は、組織が最新の脆弱性とそのリスクスコアを理解するのに役立ちます。このようなスコアは、共通脆弱性評価システム（CVSS）によって導き出され、バグの重大度が、その複雑さと影響を考慮して示されます。開発者は、業界の更新、規制の変更、契約上の要件を常に把握しておいてください。要件は頻繁に変更されるため、準拠を維持するために内部プロセスを改善する必要がある場合があります。開発者は定期的にパートナーと会い、盲点を理解して、それを緩和してください。開発者は改善内容を評価する際に、Amazonサービスサポートページ からAmazonに連絡して、Amazon MWSアプリケーションの保護に関する専門的なアドバイスを受けることができます。

未知の脅威

未知の脅威は、開発者もパートナーもよく知らないリスクです。監視メカニズムの実装と見直しにより、セキュリティイベントのインジケーターを特定できます。

セキュリティイベントのインジケーター

開発者は、すべてのセキュリティイベントを調査して、セキュリティインシデントに発展しないようにしてください。開発者は以下のようなセキュリティイベントの可能性があるインジケーターについて考慮してください（すべてを網羅するものではありません）。

- **ログと監視**。監視ツールとログが示すコンピューティングアクティビティの急激な変化は、セキュリティイベントを示している可能性があります。
- **異常な請求活動**。請求活動の急激な増加は、セキュリティイベントを示している可能性があります。このような請求活動は、ビットコインマイニングなど、コンピューターに負荷がかかる侵入者が仕掛けたプロセスから発生する可能性があります。
- **脅威インテリジェンスフィード**。貴社がサードパーティの脅威インテリジェンスフィードに登録している場合は、その情報を他のログツールと監視ツールに関連付けて、潜在的なイベントのインジケーターを特定してください。
- **データの整合性**。サービスまたはアプリケーションのデータが、予期しない値を返します。
- **データの露出**。機密データが、許可されていないまたは想定外の第三者に公開されます。
- **可用性の欠如**。アプリケーションまたはサービスが、その機能を実行できません。
- **一般向けのセキュリティ連絡メカニズム**。セキュリティチームに連絡するという広く知られた方法で、開発者にインシデントを通知できます。顧客、開発チーム、または他のスタッフが、異常に気づいて報告する場合があります。一般の人々と連携する開発者は、連絡先のメールアドレスやウェブフォームなど、一般向けのセキュリティ連絡メカニズムを作成する必要があるかもしれません。

- **システムアラート**。異常な、悪意のある、またはコストのかかるアクティビティが発生した場合に、内部システムが警告する通知を作成できます。開発者は、たとえば予想される時間枠外に発生するアクティビティの通知を作成できます。
- **機械学習**。開発者は機械学習を活用して、特定の組織または個人の複雑な異常を特定できます。ネットワーク、ユーザー、およびシステムの正常な特性をプロファイリングすることで、異常な動作を識別しやすくなります。

役割と責任の定義

インシデント対応スキルとメカニズムは、新規または大規模なイベントに対処する際に不可欠です。不明瞭なセキュリティイベントに対処するには、組織をまたがる規律、断固とした行動に対する支持、結果を出す能力が必要です。

開発者は、関係者、法律顧問、組織のリーダーシップと協力して、インシデントに対応するための目標を特定してください。一般的な目標として、問題の抑止と軽減、影響を受けるリソースの回復、フォレンジクス用データの保存、帰属などがあります。開発者は、これらの役割と責任、および第三者が関与すべきかどうかを考える必要があります。

セキュリティ関係者の一覧を以下に示します。

- **アプリケーションの所有者**。開発者は情報やコンテキストを提供できるSME（領域の専門家）であるため、影響を受けるアプリケーションまたはリソースの所有者に連絡する必要があるかもしれません。アプリケーションの所有者またはSMEは、不慣れな環境、予期した以上に複雑な環境、または対応者がアクセスできない状況での対処を求められる場合があります。SMEは、IRチームとの連携作業に慣れてください。
- **情報セキュリティ**。イベントまたはインシデントが特定されると、情報セキュリティチームが主要な連絡先となります。インシデントを調査して修復し、発生を防止することで対応できます。
- **法務**。法務チームは、セキュリティインシデントがもたらす可能性のある法的な影響を理解するためのガイダンスを提供します。これには、請負業者、サービスプロバイダー、顧客、規制当局など、影響を受けるすべての当事者に対するコミュニケーションの形成も含まれます。
- **最高情報セキュリティ責任者、ビジネス情報セキュリティ責任者**。最高情報セキュリティ責任者（CISO）を含む情報セキュリティのリーダーは、開発者のセキュリティ正常性を常に把握する必要があります。CISOは、情報セキュリティチームおよび法務チームと連携して、法律とベストプラクティスに従ってインシデントの阻止、検出、修復を行い、その対応を周知するように組織を指揮します。
- **組織のその他の人員**。組織全体が、潜在的なリスクと適切な報告メカニズムを認識する必要があります。情報セキュリティ認識トレーニングは、スタッフ（技術者および非技術者）がセキュリティイベントの発生を防ぎ、インシデントのインジケーターを特定し、潜在的なインシデントをセキュリティチームに報告するのに役立ちます。
- **サードパーティ**。信頼できるパートナーは、調査と対応を支援して、さらなる専門知識と貴重な調査を提供します。このようなパートナーには、契約によりインシデントが発生したことを通知する義務があるサードパーティが含まれます。特にAmazonは、セキュリティインシデントの検出から24時間以内に、security@amazon.com宛てにEメールでAmazonに通知するよ

う開発者に義務付けています。また、サービスプロバイダーが、責任を負っている情報セキュリティ分野を契約条件に含める場合があります。そのようなプロバイダーまたはパートナーには、環境内のセキュリティ責任の一部を負うクラウドサービスプロバイダー（CSP）が含まれる場合があります。*図2*は、AWSに適用される一般的な共有責任モデルを示しています。AWSはクラウドのセキュリティを所有し、可能な限り最高レベルのセキュリティを提供します。お客様はクラウド内のリソースのセキュリティに責任を負い、コンテンツの安全性とコンプライアンスを維持します。

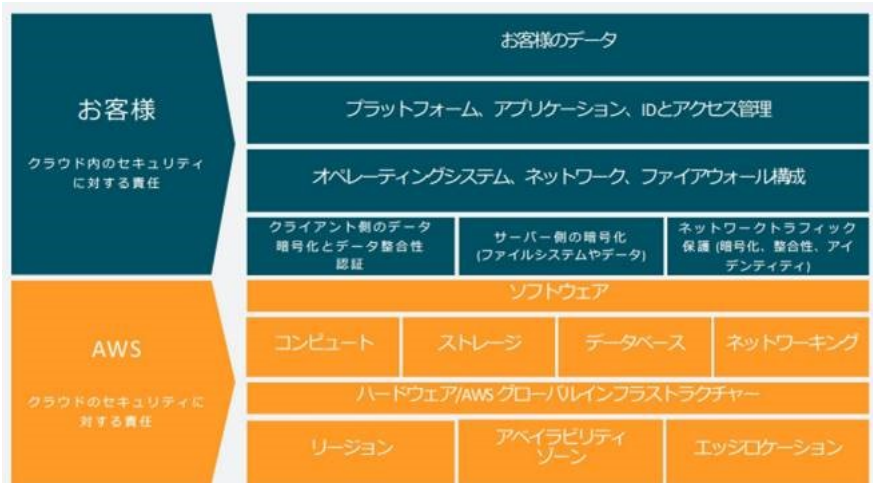

図2 – AWS共有責任モデル

通知と応答

Amazonなどの該当する当事者は、プロセスに従って対応できるように、イベント発生の通知を受け取る必要があります。そうしなければ、イベントが検知されず、システムが受けるダメージが大きくなります。

開発者は、イベント発生後に自動的に警告できる監視システムを導入する必要があります。一般的な通知メカニズムには、Eメール、チケットシステム、ページャー、アラーム、ショートメッセージサービス（SMS）などがあります。開発者には、対応目標に従ってインシデントに対応するための十分なツールが必要です。

開発者は、イベントが発生したときに対応パターンを実装する必要があります。インシデントの文書化は非常に重要です。これにより、インシデントの説明、修復アクション、および今後の再発を防ぐために実装されたコントロールなどの関連情報が保持されます。開発者はAmazon DPPに従って、（該当する場合は）今後の再発を防ぐために、インシデントの説明や修復措置、および実装された関連する修正プロセスやシステムコントロールを文書化する必要があります。さらに、文書を作成すると、社内の関係者、パートナー、および影響を受ける当事者に問題をエスカレーションするのに役立ちます。

NIST 800-53を使用している開発者は、「**IR-4**：**インシデントハンドリング**」を参照してください。効果

的なインシデント対応は、ベストプラクティスと社内計画に従ってインシデントを処理することです。インシデント処理計画とインシデント対応計画は、相互に関連しています。開発者がインシデント処理と対応能力を強化する際に、一方がもう一方をサポートします。これはコントロールIR-4でサポートされているため、このコントロールの各部分に従うことで、開発者はAmazon MWS DPPに準拠しやすくなります。必須ではありませんが、このドメインのコントロール強化の実装を検討することを開発者にお勧めします。この機能強化により、開発者はさまざまなタイプのインシデントに対応し、オペレーションの正常性と成功を保証することに備えられます。

NISTコントロール「**IR-6: インシデントレポーティング**」は、エスカレーションパスで担当者を指定するのに役立ちます。これは、インシデントが発生した場合に情報を得なければならない人々の鎖です。開発者は、重要な関係者と法律顧問がインシデントについて常に通知されて、セキュリティチームによるアクションの実行を支援できるように、エスカレーションパスを定義する必要があります。関連する関係者には、インシデントと、その影響およびステータスについて引き続き通知されます。このすべてが、開発者が法的にまたは契約上、外部の当事者に通知する義務がある場合に必要です。開発者は、インシデントをだれにいつ報告するか、法的要件と契約上の要件を理解してください。また、これらの要件を満たすための目標を策定してください。開発者は、エスカレーションパスと通知手順に、法的または契約上の知る権利を持つすべての当事者が含まれていることを確認してください。

開発者は、エスカレーションパスと通知手順に、法的または契約上の知る権利を持つすべての当事者が含まれていることを検証する必要があります。たとえば、GDPRでは、特定のタイプの個人データの侵害が発生したことを確認してから72時間以内に、データ管理者が、関連する監督当局に通知する必要があると義務付けています。同様に、Amazon MWSデータ保護ポリシーでは、インシデントを検出してから24時間以内に、security@amazon.com宛てにEメールでAmazonに通知するよう開発者に義務付けています。

証拠の保持

開発者は、環境内のすべての重要なアクションをキャプチャするログの収集、保存、保護を行っていることを確認する必要があります。これらのログには、少なくとも以下の情報が必要です。

- イベントが成功したか失敗か。
- 日付と時刻。
- アクセス試行の回数。
- データの変更内容。
- システムエラー。

Amazonの情報にアクセスできる開発者は、ログに個人を特定できる情報が含まれないようにする必要があります。セキュリティインシデントの場合、ログを参照できるように90日以上保持する必要があります。

開発者は、必要な人だけにアクセス権が付与された安全な場所にログを保存することで、偶発的または意図的な削除からログを保護してください。ログ情報は、システムの何が、どのように、いつ危害を受けたのかを理解するために不可欠です。開発者は、ログやドライブなどの証拠を一元化されたアカウントにコピーして保存してください。開発者は情報の整合性を維持するために、情報にアクセスした人や情報が提供された人、そして実行されたすべてのアクションを記録することにより、証拠保全を作成して維持する必要があります。このようなやり方により、開発者は、影響を受けるシステムが変更されたかどうかをアサートし、調査の結果が正確であることを保証できます。NIST 800-53フレームワークに従う開発者は、コントロール「**AU-10(3)：否認防止 | 生産物流管理**」を参照してください。監査と説明責任（AU）はIRドメインにはありませんが、このコントロールは、証拠保全プロセスの定義と維持に役立ちます。証拠保全はAmazon MWS DPPの遵守を維持できるだけでなく、必要に応じて、侵入者に対して訴訟を提起するのに役立ちます。

ログと監視について詳しく知りたい場合は、Amazon MWSのログと監視に関するホワイトペーパーを読んで、ポリシーに準拠したログの実装方法を確認してください。

継続的な見直し

開発者は、インシデント対応計画を徹底的にテストして見直し、定期的に更新する必要があります。そうしなければ、開発者はセキュリティインシデントに迅速に対応して解決することができません。Amazonでは、開発者に6か月ごと、およびインフラストラクチャやシステムの大幅な変更後に、この計画の見直しと検証を依頼しています。このような変更には、以下のようなものがあります。

- **システム**。新しいソフトウェアの開発、新しいツールの使用、既存ツールの廃止などのシステム変更により、問題発生の可能性が高くなります。
- **コントロール**。新しいコントロールを実装したり、コントロール障害が起きたりすると、開発者の露出が影響を受ける場合があります。
- **運用環境**。オンプレミス環境からクラウド環境に、またはその逆に移行すると、システムに新たな複雑さが生じる可能性があります。開発者は、このような変化がもたらす可能性のある新しいリスクを知るために、リスク評価を実行してください。
- **サプライチェーン**。ハードウェアプロバイダーの変更や請負会社の変更など、サプライチェーンの変更により、新たなリスクが生じる可能性があります。たとえば、特定のハードウェアプロバイダーが顧客にバグパッチを迅速に通知すると知られていても、低コストの競合他社はそのサービスを提供できない場合があります。この場合、後者の顧客は、SQLインジェクションなどの一般的なウェブエクスプロイトからインフラストラクチャを積極的に保護し、それらのパッチを実装する必要があるでしょう。
- **リスクレベル**。リスクレベルは、前述の要因により変動します。開発者は、ビジネスに許容可能なレベルのリスクを実装し、そのリスクがしきい値に達した場合はインシデント対応計画を見直してください。

頻繁に見直すことも重要です。開発者が通常のオペレーション中にプロセスやツールのギャップを確認した場合は、その修正を計画してください。このようなギャップは、自分で特定する可能性や、大きなシステム変更やインシデントの後に発生する可能性があります。開発者は、修正のプロセスやコントロールを実装して、今後のインシデントを検出して防止してください。その後、インシデント対応計画を更新して、得られた経験と実装したプロセスを反映する必要があります。

インシデント対応計画を設計して作成した後、実際にイベントが発生する前にそれをテストする必要があります。セキュリティチームがセキュリティインシデントをシミュレートし、それに応じてプロセスをテストできるように、開発者は頻度を設定してください。シミュレーションすることは、リスクベクトルを見つけてコントロールとプロセスを強化するための安全な方法です。このようなシミュレーションは、6か月ごとにインシデント対応計画を見直して検証するというAmazonの要件も満たします。

開発者は説明された各シナリオに従って対応計画を更新し、変更が生じた場合は関係者に通知する必要があります。

その他のリソース

- Amazon MWSの概要
- Amazon MWS利用規約
- Amazon MWSデータ保護ポリシー
- AWS共有責任モデル
- AWSセキュリティインシデント対応ガイド

業界の参考資料

- NIST SP 800-61R2: コンピューターセキュリティインシデントハンドリングガイド
- 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
- ナショナルバルネラビリティデータベース(NVD)
- コモンバルネラビリティスコアリングシステム(CVSS)

文書の変更履歴

改訂日	内容
2020年1月	初版