ユーザーガイド

AWS Artifact

AWS Artifact: ユーザーガイド

Table of Contents

AWS Artifact の概要

AWS Artifact では、AWS ISO 認定、Payment Card Industry (PCI) レポート、Service Organization Control (SOC) レポートなどの AWS セキュリティおよびコンプライアンスドキュメントのオンデマンドダウンロードを実行できます。これらのセキュリティおよびコンプライアンスドキュメント (監査アーティファクトとも呼ばれます) を監査人や規制機関に送信し、使用中の AWS インフラストラクチャとサービスのセキュリティとコンプライアンスを示すことができます。また、これらのドキュメントは、独自のクラウドアーキテクチャを評価したり、会社の内部統制の有効性を評価したりするためのガイドラインとしても使用できます。

さらに AWS Artifact では、ISO 認証や AWS Marketplace で自社製品を販売している独立系ソフトウェアベンダーの Service Organization Controls (SOC)レポートなどの、セキュリティおよびコンプライアンスドキュメントのオンデマンドダウンロードを実行できます。詳細については、「AWS Marketplace ベンダーインサイト」を参照してください。

AWS のお客様による自社のセキュリティとコンプライアンスを示すドキュメントの作成または取得については、お客様の責任となります。詳細については、「責任共有モデル」を参照してください。

また、AWS Artifact を使用し、事業提携契約 (BAA) のような AWS 契約の状況を確認、受諾、追跡できます。BAA は通常、Health Insurance Portability and Accountability Act (HIPAA) の対象となる企業において必要なものであり、保護されるべき医療情報 (PHI) が適切に保護されていることを確認するものです。AWS Artifact を使用して、AWS との契約を受諾し、限定された情報を法的に処理できる AWS アカウントを指定できます。複数のアカウントに代わって契約を受諾できます。複数アカウントの契約を受諾するには、AWS Organizations を使用して組織を作成します。

詳細については、「AWS Artifact」を参照してください。

料金

AWS は AWS Artifact ドキュメントおよび契約を無料で提供しています。

の開始方法 AWS Artifact

AWS Artifact は、 の中央リソースを提供します。 AWS セキュリティおよびコンプライアンスレポート。で利用可能なアーティファクト AWS Artifact には、Service Organization Control (SOC) レポート、Payment Card Industry (PCI) レポート、および の実装と運用の有効性を検証する認定機関からの証明書が含まれます。 AWS セキュリティコントロール。さらに、 AWS Artifact は、 ISO 認定などのセキュリティおよびコンプライアンスドキュメント、および製品を販売する独立系ソフトウェアベンダー (SOC) のサービス組織コントロール (ISVs) レポートへのオンデマンドアクセスを提供します。 AWS Marketplace。 詳細については、「」を参照してください。 AWS Marketplace Vendor Insights

AWS Artifact では、事業提携契約 () などの法的契約を受諾および管理できますBAA。を使用する場合 AWS Organizationsでは、組織内のすべてのアカウントに代わって契約を受諾できます。受諾すると、すべての既存のメンバーアカウントおよび今後のメンバーアカウントはすべてこの契約の範囲内となります。

タスク

- ステップ 1: にサインアップする AWS
- ステップ 2: レポートのダウンロード
- ステップ 3: 契約の管理
- ステップ 4: 通知の管理

ステップ 1: にサインアップする AWS

をお持ちでない場合 AWS アカウントで、次の手順を実行して作成します。

にサインアップするには AWS アカウント

1. https://portal.aws.amazon.com/billing/サインアップ を開きます。
2. オンラインの手順に従います。

   サインアップ手順の一環として、通話呼び出しを受け取り、電話キーパッドで検証コードを入力するように求められます。

   にサインアップするとき AWS アカウント、 AWS アカウントのルートユーザー が作成されます。ルートユーザーはすべての にアクセスできます AWS のサービス アカウントの および リ

ソース。セキュリティのベストプラクティスとして、ユーザーに管理アクセスを割り当て、ルートユーザーのみを使用してルートユーザーアクセスが必要なタスクを実行してください。

ステップ 2: レポートのダウンロード

Adobe Acrobat Reader を使用してレポートをダウンロードできます。他のPDFリーダーはサポートされていません。詳細については、「レポートをダウンロードする」を参照してください。

レポートをダウンロードするには

1. を開く AWS Artifact の コンソールhttps://console.aws.amazon.com/artifact/。
2. で AWS Artifact ホームページで、レポートの表示 を選択します。
3. レポートページで、 を使用します。 AWS にアクセスするためのレポートタブ AWS は (例: SOC 1/2/3、、C5 など) を報告しPCI、サードパーティーレポートタブに移動して、製品を販売する独立系ソフトウェアベンダー (ISVs) のレポートにアクセスします。 AWS Marketplace.
4. (オプション) 検索フィールドにキーワードを入力して、レポートを検索します。レポートのタイトル、カテゴリ、シリーズ、説明など、個々の列に基づいてレポートのターゲット検索を実行できます。例えば、Cloud Computing Compliance Controls Catalogue (C5) レポートを検索する必要がある場合は、「contains」演算子と「C5」という用語を使用して「Title」列を検索できます。
5. レポートを選択し、[レポートのダウンロード] を選択します。
6. (オプション) サードパーティーレポートタブで、ISVレポートタイトルをクリックしてレポートの詳細ページにアクセスし、レポートの詳細を確認できます。
7. ダウンロードする特定のレポートに適用される規約に同意するよう求められることがあります。詳細に読むことをお勧めします。完了したら、[規約を読み、同意します] を選択し、[規約に同意してレポートをダウンロードする] を選択します。
8. ダウンロードしたファイルをPDFビューワー経由で開きます。同意に関する規約を確認し、下にスクロールして監査レポートを探してください。レポートにはPDF、ドキュメント内の添付ファイルとして追加情報が埋め込まれている可能性があるため、サポートドキュメントについては、 PDF ファイル内の添付ファイルを確認してください。添付ファイルを表示する方法については、こちらをご覧ください。

サードパーティーのレポートには、 でのみアクセスできます。 AWS にオンボーディングしたのお客様 AWS Marketplace Vendor Insights。詳細については、「」を参照してください。AWS Marketplace Vendor Insights

ステップ 3: 契約の管理

契約を締結する前に、 の条項をダウンロードして同意する必要があります。 AWS Artifact 非開示契約 (NDA) 。各契約は機密情報であり、社外のユーザーと共有することはできません。

との契約を受諾するには AWS

1. を開く AWS Artifact の コンソールhttps://console.aws.amazon.com/artifact/。
2. で AWS Artifact ナビゲーションペインで、契約 を選択します。
3. 自分のアカウントの契約を管理するには [アカウント契約] を選択します。組織の代わりに客を管理するには、[組織の契約] を選択します。
4. 契約書のセクションを展開します。
5. [Download and review] (ダウンロードしてレビュー) を選択します。
6. 規約を読みます。完了したら、[Accept and download] (同意してダウンロード) を選択します。
7. 契約書を確認し、チェックボックスを選択して同意することを示します。
8. [Accept] (同意する) を選択して契約を受諾します。

詳細については、「契約の管理」を参照してください。

ステップ 4: 通知の管理

新しいレポートや契約の入手、または既存のレポートや契約の更新に関する通知へのサブスクライブが可能です。AWS Artifact はAWSユーザー通知サービスを使用して通知を送信します。通知は、通知設定をセットアップする際にユーザーが指定した E メールアドレスに送信されます。

設定を作成するには

1. AWS ユーザー通知サービスの通知ハブページを開く
2. AWS ユーザー通知リソースを保存するリージョンを選択します (複数可) 。デフォルトでは、ユーザー通知データは米国東部 (バージニア北部) に保存され、選択される他のリージョンにも複製されます。詳細については、「通知ハブのドキュメント」を参照してください。
3. [設定を作成] をクリックします。
4. 契約の通知を受け取るには、AWS「契約の更新」のチェックボックスをオンにします。
5. レポートの通知を受け取るには、AWSレポートの更新 のチェックボックスをオンにします。特定のカテゴリとシリーズのレポートの通知のみを受け取るには、[レポートのサブセット] の

チェックボックスをクリックし、関心のあるカテゴリとシリーズのチェックボックスをクリックします。

6. 設定用の名前を入力します。
7. 通知を受信するメールのリストをコンマで区切って入力します。
8. (オプション) 通知設定にタグを割り当てるには、タグセクションを展開してキーと値のペアを入力します。注: タグは、 AWSリソースに割り当てることができるラベルであり、各タグは、定義できるキーとオプションの値で構成されます。タグは、リソースの管理、検索、フィルタリングに役立ちます。
9. 送信 をクリックします。
10. 指定された E メールアドレスに確認メールが送信されます。この場合、E メールの受信者は、送信された確認 E メールにある [E メールアドレスの認証] とあるリンクをクリックする必要があります。これにより、認証された E メールアドレスにのみ通知が届くことになります。

詳細については、「通知の管理」を参照してください。

でのレポートのダウンロード AWS Artifact

レポートは AWS Artifact コンソールからダウンロードできます。からレポートをダウンロードすると AWS Artifact、レポートがお客様専用に生成され、すべてのレポートに固有の透かしがあります。このため、レポートは信頼しているユーザーとのみ共有してください。添付ファイルとしてレポートを E メールで送信したり、オンラインで共有したりしないでください。レポートを共有するには、Amazon などの安全な共有サービスを使用します WorkDocs。一部のレポートでは、ダウンロードする前に規約に同意する必要があります。

内容

レポートをダウンロードする

レポートをダウンロードするには、必須のアクセス許可が必要です。詳細については、「AWS Artifact での Identity and Access Management」を参照してください。

にサインアップすると AWS Artifact、アカウントには一部のレポートをダウンロードするアクセス許可が自動的に付与されます。へのアクセスに問題がある場合は AWS Artifact、AWS Artifact 「サービス認証リファレンス」ページのガイダンスに従ってください。

レポートをダウンロードするには

1. で AWS Artifact コンソールを開きますhttps://console.aws.amazon.com/artifact/。
2. AWS Artifact ホームページで、レポートの表示 を選択します。
3. レポートページで、AWS レポートタブを使用して AWS レポート (SOC1/2/3、、C5 など) にアクセスしPCI、サードパーティーレポートタブに移動して、 で製品を販売する独立系ソフトウェアベンダー (ISVs) のレポートにアクセスします AWS Marketplace。
4. (オプション) 検索フィールドにキーワードを入力して、レポートを検索します。レポートのタイトル、カテゴリ、シリーズ、説明など、個々の列に基づいてレポートのターゲット検索を実行できます。例えば、Cloud Computing Compliance Controls Catalogue (C5) レポートを検索する必要がある場合は、「contains」演算子と「C5」という用語を使用して「Title」列を検索できます。

5. レポートを選択し、[レポートのダウンロード] を選択します。
6. (オプション) サードパーティーレポートタブで、ISVレポートタイトルをクリックしてレポートの詳細ページにアクセスし、レポートの詳細を確認できます。
7. ダウンロードする特定のレポートに適用される規約に同意するよう求められることがあります。詳細に読むことをお勧めします。完了したら、[規約を読み、同意します] を選択し、[規約に同意してレポートをダウンロードする] を選択します。
8. ダウンロードしたファイルをPDFビューワー経由で開きます。同意に関する規約を確認し、下にスクロールして監査レポートを探してください。レポートにはPDF、ドキュメント内の添付ファイルとして追加情報が埋め込まれている可能性があるため、サポートドキュメントについては、 PDF ファイル内の添付ファイルを確認してください。添付ファイルを表示する方法については、こちらをご覧ください。

PDF ドキュメントでの添付ファイルの表示

現在PDF添付ファイルの表示をサポートしている以下のアプリケーションをお勧めします。

Adobe Acrobat Viewer

1. Adobe Acrobat の最新バージョンは、こちらからダウンロードしてください。
2. Adobe Acrobat Viewer でファイルを開きます。
3. 添付ファイルパネルを開くには、PDFドキュメントの左側にあるペーパークリップアイコンをクリックします。または、表示 > 表示/非表示 > ナビゲーションペイン > 添付ファイルを選択します。
4. 添付ファイルパネルで、添付ファイルをダブルクリックしてドキュメントを表示します。

Firefox ブラウザ

1. Firefox ブラウザはこちらからダウンロードしてください
2. ファイルメニューからPDFファイルを開くオプションを使用して、Firefox ブラウザでファイルを開きます。
3. 添付ファイルを開くには、画面左上の Toggle サイドバーアイコンをクリックします。

ドキュメントのセキュリティで保護する

AWS Artifact ドキュメントは機密であり、常に安全に保つ必要があります。 は、ドキュメントの責任 AWS 共有モデル AWS Artifact を使用します。つまり、 AWS は AWS 、 クラウドにいる間はドキュメントを安全に保つ責任を担いますが、ダウンロード後はドキュメントを安全に保つ責任があります。 では、ドキュメントをダウンロードする前に利用規約に同意 AWS Artifact する必要があります。各ドキュメントのダウンロードには一意のトレース可能なウォーターマークが含まれます。

機密とマークされているドキュメントは、企業内、規制機関、およびお客様の監査人とのみ共有できます。これらのドキュメントをお客様の顧客またはウェブサイト上で共有することは許可されていません。Amazon などの安全なドキュメント共有サービスを使用して、他のユーザーとドキュメントを共有することを強くお勧め WorkDocsします。ドキュメントは E メール経由で送信したり、セキュアでないサイトにアップロードしたりしないでください。

トラブルシューティング

ドキュメントをダウンロードできない場合やエラーメッセージが表示される場合は、「」の「トラブルシューティング」を参照してください AWS Artifact FAQ。

AWS Artifact での契約の管理

AWS Artifact Agreements を使用すると、AWS Management Console でアカウントや組織の契約を確認、受諾、管理できます。たとえば、事業提携契約 (BAA) は通常、Health Insurance Portability and Accountability Act (HIPAA) の対象となる企業において必要なものであり、保護されるべき医療情報 (PHI) が適切に保護されていることを確認するものです。AWS Artifact を使用して BAA などの契約を AWS と結び、PHI を法的に処理できる AWS アカウントを指定できます。AWS Organizations を使用すると、AWS BAA などの契約を組織内のすべてのアカウントに代わって受諾できます。既存のメンバーアカウントおよび今後のメンバーアカウントはすべてこの契約の範囲内となり、PHI を法的に処理できます。

また、AWS Artifact を使用して AWS アカウントまたは組織が契約を受諾したことを確認したり、義務を理解するために受諾した契約の条項を確認したりすることもできます。アカウントや組織で受諾済みの契約書を使用する必要がなくなった場合は、AWS Artifact を使用して契約を終了できます。契約を終了しても、後で使用する必要が生じた場合は、再度有効にすることができます。

目次

AWS Artifact での単一アカウントの契約の管理

自分のアカウントが AWS Organizations の組織のメンバーアカウントの場合でも、自分のアカウントのみの契約を受諾できます。AWS Organizations の詳細については、「AWS Organizations ユーザーガイド」を参照してください。

AWS との契約の受諾

契約を受諾する前に、法務、個人情報、およびコンプライアンス担当部門に相談することをお勧めします。

必要なアクセス許可

アカウントの管理者は、1 つ以上の契約にアクセスし管理するロールアクセス権限を IAM ユーザーおよびフェデレーティッドユーザーに付与できます。デフォルトでは、管理者権限を持つユーザーし

か契約を受諾できません。契約を受諾するには、IAM ユーザーおよびフェデレーティッドユーザーに次のアクセス許可が必要です。

```
artifact:DownloadAgreement
artifact:AcceptAgreement
```

詳細については、「アイデンティティとアクセス権の管理」を参照してください。

AWS との契約を受諾するには

1. https://console.aws.amazon.com/artifact/ で AWS Artifact コンソールを開きます。
2. AWS Artifact ナビゲーションペインで [契約] を選択します。
3. [アカウント契約] タブを選択します。
4. 契約書のセクションを展開します。
5. [Download and review] (ダウンロードしてレビュー) を選択します。
6. 規約を読みます。完了したら、[Accept and download] (同意してダウンロード) を選択します。
7. 契約書を確認し、チェックボックスをオンにして同意することを示します。
8. [Accept] (同意する) を選択して自分のアカウントの契約を受諾します。

AWS との契約の終了

契約の受諾に AWS Artifact コンソールを使用した場合、コンソールを使用してその契約を終了できます。それ以外の場合は、「オフライン契約」を参照してください。

必要なアクセス許可

契約を終了するには、IAM ユーザーおよびフェデレーティッドユーザーに次のアクセス許可が必要です。

```
artifact:TerminateAgreement
```

詳細については、「アイデンティティとアクセス権の管理」を参照してください。

AWS とのオンライン契約を終了するには

1. https://console.aws.amazon.com/artifact/ で AWS Artifact コンソールを開きます。
2. AWS Artifact ナビゲーションペインで [契約] を選択します。

3. [アカウント契約] タブを選択します。
4. 契約を選択し、[Terminate agreement] (契約を終了) を選択します。
5. すべてのチェックボックスをオンにして、契約を終了することに同意することを示します。
6. [Terminate] (終了) を選択します。確認を求めるメッセージが表示されたら、[終了] を選択します。

AWS Artifact での複数アカウントの 1 つの契約の管理

AWS Organizations 組織の管理アカウントの所有者は、組織のすべてのアカウントに代わって契約を受諾できます。組織の契約を受諾または終了するには、正しい AWS Artifact アクセス許可を持つ管理アカウントにサインインする必要があります。`organizations:DescribeOrganization` アクセス許可を持つメンバーアカウントのユーザーは、お客様が代わりに受諾した組織の契約を表示できます。

アカウントが組織の一部でない場合は、AWS Organizations ユーザーガイドの「組織の作成と管理」の手順に従って、組織を作成または組織に参加できます。

AWS Organizations には、一括請求機能とすべての機能の 2 つの利用可能な機能セットがあります。組織で AWS Artifact を使用するには、所属する組織で、すべての機能を有効にする必要があります。組織が一括請求用にのみ設定されている場合は、AWS Organizations ユーザーガイドの「組織内のすべての機能の有効化」を参照してください。

メンバーアカウントが組織から削除されると、そのメンバーアカウントは組織契約の対象範囲ではなくなります。管理アカウントの管理者は、メンバーアカウントが必要に応じて新しい契約を用意できるよう、メンバーアカウントを組織から削除する前に、そのことをメンバーアカウントに通達するべきです。組織の有効な契約のリストは、AWS Artifact の組織契約で確認できます。

詳細については、AWS Organizations ユーザーガイドの「組織内の AWS アカウントの管理 」を参照してください。

組織の契約を受諾する

AWS Organizations の組織内のすべてのメンバーアカウントに代わって契約を受諾できます。契約を受諾する前に、法務、個人情報、およびコンプライアンス担当部門に相談することをお勧めします。

必要なアクセス許可

契約を受諾するには、管理アカウントの所有者に次のアクセス許可が必要です。

```
artifact:DownloadAgreement
artifact:AcceptAgreement
organizations:DescribeOrganization
organizations:EnableAWSServiceAccess
organizations:ListAWSServiceAccessForOrganization
iam:ListRoles
iam:CreateServiceLinkedRole
```

詳細については、「アイデンティティとアクセス権の管理」を参照してください。

組織の契約を受諾するには

1. https://console.aws.amazon.com/artifact/ で AWS Artifact コンソールを開きます。
2. AWS Artifact ダッシュボードで、[契約] を選択します。
3. [Organization agreements (組織契約)] タブを選択します。
4. 契約書のセクションを展開します。
5. [Download and review] (ダウンロードしてレビュー) を選択します。
6. 規約を読みます。完了したら、[Accept and download] (同意してダウンロード) を選択します。
7. 契約書を確認し、チェックボックスをオンにして同意することを示します。
8. [Accept (受諾)] を選択して組織内の既存および今後のすべてのアカウントの契約を受諾します。

組織契約の終了

AWS Artifact コンソールを使用して組織内のすべてのメンバーアカウントの代わりに契約を受諾した場合は、コンソールを使用してその契約を終了できます。それ以外の場合は、「オフライン契約」を参照してください。

必要なアクセス許可

契約を終了するには、管理アカウントの所有者に次のアクセス許可が必要です。

```
artifact:DownloadAgreement
artifact:TerminateAgreement
organizations:DescribeOrganization
organizations:EnableAWSServiceAccess
organizations:ListAWSServiceAccessForOrganization
iam:ListRoles
```

```
iam:CreateServiceLinkedRole
```

詳細については、「アイデンティティとアクセス権の管理」を参照してください。

AWS とのオンライン組織契約を終了するには

1. https://console.aws.amazon.com/artifact/ で AWS Artifact コンソールを開きます。
2. AWS Artifact ダッシュボードで、[契約] を選択します。
3. [Organization agreements (組織契約)] タブを選択します。
4. 契約を選択し、[Terminate agreement] (契約を終了) を選択します。
5. すべてのチェックボックスをオンにして、契約を終了することに同意することを示します。
6. [Terminate] (終了) を選択します。確認を求めるメッセージが表示されたら、[終了] を選択します。

AWS Artifact での既存のオフライン契約の管理

既存のオフライン契約がある場合、AWS Artifact にはオフラインで受諾した契約が表示されます。たとえば、コンソールに [Offline Business Associate Addendum (BAA) (オフライン事業提携契約)] が [Active (有効)] というステータスで表示されます。有効というステータスは契約が受諾されたことを示します。オフライン契約を終了するには、契約に含まれる終了のガイドラインおよび手順を参照してください。

アカウントが AWS Organizations 組織の管理アカウントである場合、AWS Artifact を使用してオフライン契約の条項を組織のすべてのアカウントに適用できます。オフラインで受諾した契約を組織および組織内のすべてのアカウントに適用するには、以下のアクセス許可が必要です。

```
organizations:DescribeOrganization
organizations:EnableAWSServiceAccess
organizations:ListAWSServiceAccessForOrganization
iam:ListRoles
iam:CreateServiceLinkedRole
```

お客様のアカウントが組織のメンバーアカウントである場合、オフラインの組織契約を表示するには、以下のアクセス許可が必要です。

```
organizations:DescribeOrganization
```

詳細については、「アイデンティティとアクセス権の管理」を参照してください。

AWS Artifact での通知の管理

AWS Artifact の通知では、E メール通知を設定することができます。通知設定ページでは、以下に説明するように、通知をサブスクライブしたり、その他の通知設定を管理したりすることができます。AWS Artifact は、AWS User Notifications サービスを使用して通知を送信します。AWS Artifact 通知を使用するには、AWS Artifact および AWS User Notifications サービスに必要なアクセス許可が付与されていなければなりません。詳細については、「アイデンティティとアクセス権の管理」を参照してください。

目次

通知の設定

通知の受信を開始する際は、あらかじめユーザー通知データを保存するリージョンを指定する必要があります。通知ハブをセットアップするには、以下の手順に従ってください。

通知ハブをセットアップするには

1. AWS User Notifications サービスの「通知ハブ」ページを開きます。
2. AWS User Notifications リソースの保存を希望するリージョンを選択します。デフォルトでは、ユーザー通知データは米国東部 (バージニア北部) に保存され、選択された他のリージョンにも複製されます。詳細については、「通知ハブのドキュメント」を参照してください。
3. 送信 をクリックします。

通知をサブスクライブするには

1. AWS Artifact 「通知設定」ページを開きます。
2. AWS Artifactの通知をサブスクライブするには、[Artifact 通知をサブスクライブ] トグルをクリックします。

通知のサブスクライブを解除するには

1. AWS Artifact 「通知設定」ページを開きます。
2. AWS Artifactの通知のサブスクライブを解除するには、[Artifact 通知をサブスクライブ] トグルをクリックします。

設定を作成するには

1. AWS Artifact 「通知設定」ページを開きます。
2. [設定の作成]をクリックします。
3. 契約の通知を受け取るには、[AWS 契約の更新] の横にあるチェックボックスをオンのままにします。
4. レポートの通知を受け取るには、[AWS レポートの更新] の横にあるチェックボックスをオンのままにします。
5. すべてのレポートの通知を受け取るには、[すべてのレポート] の横にあるチェックボックスをオンのままにします。
6. 特定のカテゴリーやシリーズのレポートのみの通知を受け取るには、[レポートのサブセット] のチェックボックスをクリックします。次に、関心のあるカテゴリとシリーズのチェックボックスをクリックします。
7. 設定用の名前を入力します。
8. 通知を受信するメールのリストをコンマで区切って入力します。
9. (オプション) 通知設定にタグを割り当てるには、タグセクションを展開してキーと値のペアを入力します。注：タグは AWS リソースに割り当てることができるラベルで、各タグはキーとユーザーが定義できるオプションの値で構成されます。タグは、リソースの管理、検索、フィルタリングに役立ちます。
10. [設定の作成]をクリックします。
11. 指定された E メールアドレスに確認メールが送信されます。この場合、E メールの受信者は、送信された確認 E メールにある [E メールアドレスの認証] とあるリンクをクリックする必要があります。これにより、認証された E メールアドレスにのみ通知が届くことになります。

設定を編集するには

1. AWS Artifact 「通知設定」ページを開きます。
2. 編集する設定の行をクリックします。

3. ページの右上にある [編集] ボタンをクリックします。
4. どのフィールドも編集できます。変更内容に問題がなければ、[変更内容の保存]を押します。
5. 新しい E メールアドレスを追加すると、各 E メールアドレスに確認メールが送信されます。確認メール内の [メールアドレスの認証] リンクをクリックします。

設定を削除するには

1. AWS Artifact 「通知設定」ページを開きます。
2. 編集する設定の行をクリックします。
3. [Delete (削除)] をクリックします。
4. 警告メッセージを読んだら、[削除] をクリックします。

設定にタグを割り当てる

タグとは、AWS リソースに付けるラベルです。タグはそれぞれ、1 つのキーとオプションの 1 つの値で設定されており、どちらもお客様側が定義します。タグは、リソースの管理、検索、フィルタリングに役立ちます。設定を作成または編集するときは、オプションでタグを設定できます。詳細については、「リソースのタグ付け」を参照してください。

トラブルシューティング

AWS Artifact 通知の使用中にエラーメッセージを受け取った場合は、AWS Artifact よくある質問の「トラブルシューティング」を参照してください。

AWS Artifact での Identity and Access Management

AWS にサインアップするときには、AWS アカウントに関連付けられた E メールアドレスとパスワードを提供します。これらは ルート認証情報であり、これらの情報を使用すると、AWS Artifact のリソースを始めとするすべての AWS リソースへの完全なアクセスが可能になります。ただし、日常のアクセスにはルートアカウントを使用しないことを強くお勧めします。また、他のユーザーとアカウント認証情報を共有して、アカウントへの完全なアクセスを提供しないことをお勧めします。

ルート認証情報を使用して AWS アカウントにサインインしたり、他のユーザーと認証情報を共有したりするのではなく、自分と、AWS Artifact 内のドキュメントまたは契約へのアクセスを必要とする可能性のあるユーザー用にIAM ユーザーと呼ばれる特別なユーザー ID を作成してください。この方法では、各ユーザーに個別のサインイン情報を提供し、各ユーザーが特定のドキュメントを使うために必要なアクセス許可のみを与えることができます。複数の IAM ユーザーに同じアクセス許可を付与するには、IAM グループにアクセス許可を付与して、IAM ユーザーをそのグループに追加します。

すでにユーザー ID を AWS の外で管理している場合、IAM ユーザーを作成する代わりに、IAM ID プロバイダーを利用できます。詳細については、 IAM ユーザーガイドの「ID プロバイダーとフェデレーション」を参照してください。

目次

AWS Artifact へのユーザーアクセスをセットアップする

以下のステップを完了して、必要なアクセスレベルに基づいて、AWS Artifact へのアクセス許可をユーザーに付与します。

タスク

- ステップ 2: IAM グループを作成してポリシーをアタッチする
- ステップ 3: IAM ユーザーを作成してグループに追加する

ステップ 1: IAM ポリシーを作成する

IAM 管理者は、AWS Artifact アクションとリソースへのアクセス許可を付与するポリシーを作成できます。

IAM ポリシーを作成するには

IAM ユーザーおよびグループにアクセス許可を付与するために使用できる IAM ポリシーを作成するには、以下の手順を使用します。

1. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. ナビゲーションペインで、ポリシー を選択します。
3. [Create policy] (ポリシーを作成) を選択します。
4. [JSON] タブを選択します。
5. ポリシードキュメントを入力します。独自のポリシーを作成するか、IAM ポリシーの例 のポリシーを使用することもできます。
6. [ポリシーの確認] を選択します。構文エラーがある場合は、ポリシーバリデータが報告します。
7. [ポリシーの確認] ページで、ポリシーの目的を示す一意の名前を入力します。説明を追加することもできます。
8. [ポリシーを作成] を選択します。

ステップ 2: IAM グループを作成してポリシーをアタッチする

IAM 管理者はグループを作成し、作成したポリシーをグループにアタッチできます。いつでも IAM ユーザーをグループに追加できます。

IAM グループを作成してポリシーをアタッチするには

1. ナビゲーションペインで、[Groups]、[Create New Group] の順に選択します。
2. [グループ名] にグループの名前を入力し、[次のステップ] を選択します。
3. 作成したポリシーの名前を検索ボックスに入力します。 ポリシーのチェックボックスを選択にし、[次のステップ] を選択します。
4. グループ名とポリシーを確認します。準備ができたら、[グループの作成] を選択します。

ステップ 3: IAM ユーザーを作成してグループに追加する

IAM 管理者は、いつでもユーザーをグループに追加できます。ユーザーを追加すると、グループに付与された権限がユーザーに付与されます。

IAM ユーザーを作成してグループに追加するには

1. ナビゲーションペインで、[Users] (ユーザー)、[Add user] (ユーザーを追加する) の順に選択します。
2. [ユーザー名] に 1 人または複数のユーザーの名前を入力します。
3. AWS Management Console アクセス の横にあるチェックボックスを選択します。自動生成されたパスワードまたはカスタムパスワードを設定します。必要に応じて、[ーザーは次回のサインインで新しいパスワードを作成する必要があります] を選択して、初回サインイン時にパスワードのリセットを要求できます。
4. [Next: Permissions] (次のステップ: アクセス許可) を選択します。
5. [ユーザーをグループに追加] をクリックし、作成したグループを選択します。
6. [Next: Tags] (次へ: タグ) を選択します。必要に応じて、ユーザーにタグを追加できます。
7. [Next: Review] (次のステップ: レビュー) を選択します。準備が完了したら、[ユーザーの作成] を選択します。

きめ細かな権限への移行

AWS Artifact により、お客様はきめ細かなアクセス許可を使用できるようになりました。これらのきめ細かなアクセス許可により、お客様は条件の承諾やレポートのダウンロードなどの機能へのアクセスをきめ細かく制御できます。

きめ細かなアクセス許可を使用してレポートにアクセスするには、AWSArtifactReportsReadOnlyAccess 管理ポリシーを使用するか、以下の推奨事項に従ってアクセス許可を更新できます。以前にきめ細かなアクセス許可の使用をオプトアウトしたことがある場合は、レポートコンソールで利用可能なAWS「アーティファクトレポートのきめ細かなアクセス許可へのオプトイン」リンクを使用してオプトインする必要があります。

新しいアクセス許可の更新に問題がある場合は、コンソールで利用可能なAWS「アーティファクトレポートのきめ細かなアクセス許可のオプトアウト」リンクから、古いアクセス許可を持つレポートにアクセスできます。

新しい権限への移行

リソース固有ではない権限の移行

ユーザーは、従来の権限を含む既存のポリシーを、きめ細かい権限を含むポリシーに置き換える必要があります

従来のポリシー:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:Get"
      ],
      "Resource": [
        "arn:aws:artifact:::report-package/*"
      ]
    }
  ]
}
```

きめ細かい権限を持つ新しいポリシー:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports",
        "artifact:GetReportMetadata",
        "artifact:GetReport",
        "artifact:GetTermForReport"
      ],
      "Resource": "*"
    }
  ]
}
```

リソース固有の権限の移行

ユーザーは、従来の権限を含む既存のポリシーを、きめ細かい権限を含むポリシーに置き換える必要があります。レポートリソースのワイルドカード権限は条件キーに置き換えられました。

従来のポリシー:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:Get"
      ],
      "Resource": [
        "arn:aws:artifact:::report-package/Certifications and Attestations/SOC/*",
        "arn:aws:artifact:::report-package/Certifications and Attestations/PCI/*",
        "arn:aws:artifact:::report-package/Certifications and Attestations/ISO/*"
      ]
    }
  ]
}
```

きめ細かい権限と条件キーを含む新しいポリシー。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReportMetadata",
        "artifact:GetReport",
        "artifact:GetTermForReport"
```

```
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "artifact:ReportSeries": [
            "SOC",
            "PCI",
            "ISO"
          ],
          "artifact:ReportCategory": [
            "Certifications and Attestations"
          ]
        }
      }
    }
  ]
}
```

IAM ポリシーの例

IAM ユーザーにアクセス許可を付与するアクセス許可ポリシーを作成できます。 AWS Artifact レポートへのアクセス権と、単一のアカウントまたは組織に代わって契約書を承諾およびダウンロードする権限をユーザーに付与できます。

次のサンプルポリシーは、必要なアクセスレベルに基づいて IAM ユーザーに割り当てることができるアクセス許可を示します。

- AWS きめ細かい権限でレポートを管理するポリシーの例
- サードパーティレポートを管理するポリシーの例
- 契約を管理するポリシーの例
- 統合するポリシーの例 AWS Organizations
- 管理アカウントの契約を管理するポリシーの例
- 組織的な契約を管理するポリシーの例
- 通知を管理するポリシーの例

Example AWS きめ細かい権限でレポートを管理するポリシーの例

> **Tip**
> 独自のポリシーを定義するのではなく、AWSArtifactReportsReadOnlyAccess 管理ポリシーの使用を検討してください。

以下のポリシーは、 AWS きめ細かい権限を通じてすべてのレポートをダウンロードする権限を付与します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports",
        "artifact:GetReportMetadata",
        "artifact:GetReport",
        "artifact:GetTermForReport"
      ],
      "Resource": "*"
    }
  ]
}
```

次のポリシーでは、詳細な権限を通じて AWS SOC、PCI、ISO レポートのみをダウンロードする権限を付与します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports",
        "artifact:GetReportMetadata",
        "artifact:GetReport",
        "artifact:GetTermForReport"
      ],
```

```
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "artifact:ReportSeries": [
            "SOC",
            "PCI",
            "ISO"
          ],
          "artifact:ReportCategory": [
            "Certifications And Attestations"
          ]
        }
      }
    }
  ]
}
```

Example サードパーティレポートを管理するポリシーの例

> **Tip**
>
> 独自のポリシーを定義するのではなく、AWSArtifactReportsReadOnlyAccess 管理ポリシーの使用を検討してください。

サードパーティレポートは IAM リソースの `report` で示されます。

次のポリシーは、すべてのサードパーティレポート機能に対しアクセス許可を付与します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports",
        "artifact:GetReportMetadata",
        "artifact:GetReport",
        "artifact:GetTermForReport"
      ],
      "Resource": "*"
```

```
    }
  ]
}
```

次のポリシーは、サードパーティレポートをダウンロードするアクセス許可を付与します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReport",
        "artifact:GetTermForReport"
      ],
      "Resource": "*"
    }
  ]
}
```

次のポリシーは、サードパーティレポートを一覧表示するアクセス許可を付与します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReport"
      ],
      "Resource": "*"
    }
  ]
}
```

次のポリシーは、すべてのバージョンのサードパーティレポートの詳細を閲覧する権限を付与します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
      "Effect": "Allow",
      "Action": [
        "artifact:GetReportMetadata"
      ],
      "Resource": [
        "arn:aws:artifact:us-east-1::report/report-jRVRFP8HxUN5zpPh:*"
      ]
    }
  ]
}
```

次のポリシーは、特定のバージョンに関するサードパーティレポートの詳細を閲覧する権限を付与します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReportMetadata"
      ],
      "Resource": [
        "arn:aws:artifact:us-east-1::report/report-jRVRFP8HxUN5zpPh:1"
      ]
    }
  ]
}
```

Example 契約を管理するポリシーの例

次のポリシーは、すべての契約をダウンロードするアクセス許可を付与します。IAM ユーザーが契約を受諾するには、このアクセス許可も必要です。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:DownloadAgreement"
```

```
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

次のポリシーは、1 つの契約を受諾するアクセス許可を付与します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:AcceptAgreement",
        "artifact:DownloadAgreement"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

次のポリシーは、1 つの契約を終了するアクセス許可を付与します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:TerminateAgreement"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

次のポリシーは、1 つアカウント契約を管理するアクセス許可を付与します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:AcceptAgreement",
        "artifact:DownloadAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": [
        "arn:aws:artifact::*:customer-agreement/*",
        "arn:aws:artifact:::agreement/*"
      ]
    }
  ]
}
```

Example と統合するポリシーの例 AWS Organizations

以下のポリシーは、 AWS Artifact AWS Organizationsとの統合に使用する IAM ロールを作成する権限を付与します。組織的な契約を開始するには、組織の管理アカウントにこれらのアクセス許可が必要です。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:ListRoles",
      "Resource": "arn:aws:iam::*:role/*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    }
  ]
}
```

次のポリシーは、 AWS Artifact AWS Organizations使用するアクセス権限を付与するアクセス権限を付与します。組織的な契約を開始するには、組織の管理アカウントにこれらのアクセス許可が必要です。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

Example 管理アカウントの契約を管理するポリシーの例

次のポリシーは、管理アカウントの契約を管理するアクセス許可を付与します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:AcceptAgreement",
        "artifact:DownloadAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": [
        "arn:aws:artifact::*:customer-agreement/*",
        "arn:aws:artifact:::agreement/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "iam:ListRoles",
      "Resource": "arn:aws:iam::*:role/*"
```

```
    },
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:EnableAWSServiceAccess",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

Example 組織的な契約を管理するポリシーの例

次のポリシーは、組織的な契約を管理するアクセス許可を付与します。必要な権限を持つ別のユーザーが組織的な契約を設定する必要があります。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:AcceptAgreement",
        "artifact:DownloadAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": [
        "arn:aws:artifact::*:customer-agreement/*",
        "arn:aws:artifact:::agreement/*"
      ]
    },
    {
      "Effect": "Allow",
```

```
      "Action": [
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

次のポリシーは、組織的な契約を表示するアクセス許可を付与します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:DownloadAgreement"
      ],
      "Resource": [
        "arn:aws:artifact::*:customer-agreement/*",
        "arn:aws:artifact:::agreement/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

Example 通知を管理するポリシーの例

次のポリシーでは、 AWS Artifact 通知を使用するためのすべての権限を付与します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```
      "Action": [
        "artifact:GetAccountSettings",
        "artifact:PutAccountSettings",
        "notifications:AssociateChannel",
        "notifications:CreateEventRule",
        "notifications:CreateNotificationConfiguration",
        "notifications:DeleteEventRule",
        "notifications:DeleteNotificationConfiguration",
        "notifications:DisassociateChannel",
        "notifications:GetEventRule",
        "notifications:GetNotificationConfiguration",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListNotificationConfigurations",
        "notifications:ListNotificationHubs",
        "notifications:ListTagsForResource",
        "notifications:TagResource",
        "notifications:UntagResource",
        "notifications:UpdateEventRule",
        "notifications:UpdateNotificationConfiguration",
        "notifications-contacts:CreateEmailContact",
        "notifications-contacts:DeleteEmailContact",
        "notifications-contacts:GetEmailContact",
        "notifications-contacts:ListEmailContacts",
        "notifications-contacts:SendActivationCode"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

次のポリシーは、すべての設定を一覧表示するためのアクセス許可を付与します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetAccountSettings",
        "notifications:ListChannels",
```

```
        "notifications:ListEventRules",
        "notifications:ListNotificationConfigurations",
        "notifications:ListNotificationHubs",
        "notifications-contacts:GetEmailContact"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

次のポリシーは、設定を作成するアクセス許可を付与します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetAccountSettings",
        "artifact:PutAccountSettings",
        "notifications-contacts:CreateEmailContact",
        "notifications-contacts:SendActivationCode",
        "notifications:AssociateChannel",
        "notifications:CreateEventRule",
        "notifications:CreateNotificationConfiguration",
        "notifications:ListEventRules",
        "notifications:ListNotificationHubs",
        "notifications:TagResource",
        "notifications-contacts:ListEmailContacts"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

次のポリシーは、設定を編集するアクセス許可を付与します。

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetAccountSettings",
        "artifact:PutAccountSettings",
        "notifications:AssociateChannel",
        "notifications:DisassociateChannel",
        "notifications:GetNotificationConfiguration",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListTagsForResource",
        "notifications:TagResource",
        "notifications:UntagResource",
        "notifications:UpdateEventRule",
        "notifications:UpdateNotificationConfiguration",
        "notifications-contacts:GetEmailContact",
        "notifications-contacts:ListEmailContacts"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

次のポリシーは、設定を削除するアクセス許可を付与します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "notifications:DeleteNotificationConfiguration",
        "notifications:ListEventRules"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

次のポリシーは、設定の詳細を表示するアクセス許可を付与します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "notifications:GetNotificationConfiguration",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListTagsForResource",
        "notifications-contacts:GetEmailContact"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

次のポリシーは、通知ハブを登録または登録解除するアクセス許可を付与します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "notifications:DeregisterNotificationHub",
        "notifications:RegisterNotificationHub"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

AWS Artifact の AWS マネージドポリシー

AWS マネージドポリシーは、AWS が作成および管理するスタンドアロンポリシーです。AWS マネージドポリシーは、多くの一般的なユースケースで権限を提供できるように設計されているため、ユーザー、グループ、ロールへの権限の割り当てを開始できます。

AWS マネージドポリシーは、ご利用の特定のユースケースに対して最小特権の権限を付与しない場合があることにご注意ください。AWS のすべてのお客様が使用できるようになるのを避けるためです。ユースケース別にカスタマー管理ポリシーを定義することで、権限を絞り込むことをお勧めします。

AWS マネージドポリシーで定義したアクセス権限は変更できません。AWS が AWS マネージドポリシーに定義されている権限を更新すると、更新はポリシーがアタッチされているすべてのプリンシパルアイデンティティ (ユーザー、グループ、ロール) に影響します。新しい AWS のサービスを起動するか、既存のサービスで新しい API オペレーションが使用可能になると、AWS が AWS マネージドポリシーを更新する可能性が最も高くなります。

詳細については、「IAM ユーザーガイド」の「AWS マネージドポリシー」を参照してください。

AWS マネージドポリシー: AWSArtifactReportsReadOnlyAccess

`AWSArtifactReportsReadOnlyAccess` ポリシーは IAM ID に添付できます。

このポリシーは、レポートの一覧表示、表示、ダウンロードを許可する######権限を付与します。

権限の詳細

このポリシーには、以下の権限が含まれています。

- `artifact` — プリンシパルがレポートを一覧表示、表示、ダウンロードすることを許可します。AWS Artifact

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:Get",
```

```
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource": "*"
    }
  ]
}
```

Artifact での AWS マネージドポリシーの更新

Artifact の AWS マネージドポリシーの更新に関する詳細を、このサービスがこれらの変更の追跡を開始した以降の分について表示します。このページの変更に関する自動通知については、「Document history」ページの RSS フィードをサブスクライブしてください。

変更	説明	日付
Artifact が変更の追跡を開始しました	Artifact は、AWS マネージドポリシーの変更の追跡を開始し、AWSArtifactReportsReadOnlyAccess を導入しました。	2023-12-15

AWS Artifact のサービスリンクロールの使用

AWS Artifact では AWS Identity and Access Management (IAM) サービスにリンクされたロールを使用します。サービスにリンクされたロールは、AWS Artifact に直接リンクされる一意のタイプの IAM ロールです。サービスにリンクされたロールは、AWS Artifact で事前定義され、ユーザーの代わりに該当サービスから他の AWS サービスを呼び出すために必要なすべてのアクセス権限が付与されます。

サービスにリンクされたロールを使用すると、必要なアクセス許可を手動で追加する必要がないため、AWS Artifact を簡単にセットアップできます。AWS Artifact は、サービスにリンクされたロールのアクセス許可を定義します。特に定義されていない限り、AWS Artifact のみがそのロールを引き受けることができます。定義される許可には、信頼ポリシーとアクセス許可ポリシーが含まれており、そのアクセス許可ポリシーを他の IAM エンティティに添付することはできません。

サービスリンクロールを削除するには、まずその関連リソースを削除します。これにより、AWS Artifact リソースが保護されます。これは、リソースにアクセスする権限を誤って削除できないためです。

サービスにリンクされたロールをサポートする他のサービスについては、「IAM と連動する AWS のサービス」を参照し、[Service-linked roles(サービスにリンクされたロール)] の列内で [Yes (はい)] と表記されたサービスを確認してください。サービスにリンクされたロールに関するドキュメントをサービスで表示するには、[はい] リンクを選択します。

AWS Artifact のサービスリンクロールのアクセス権限

AWS Artifact は AWSServiceRoleForArtifact という名前のサービスにリンクされたロールを使用します。これにより、AWS Artifact は AWS Organizations サービスを通じて組織に関する情報を収集できます。

サービスにリンクされたロール AWSServiceRoleForArtifact は、次のサービスを信頼してそのロールを引き受けます。

- `artifact.amazonaws.com`

AWSArtifactServiceRolePolicy という名前のロール許可ポリシーにより、AWS Artifact は `organizations` リソースに対して次のアクションを実行できます。

- `DescribeOrganization`
- `DescribeAccount`
- `ListAccounts`
- `ListAWSServiceAccessForOrganization`

AWS Artifact のサービスリンクロールの作成

サービスリンクロールを手動で作成する必要はありません。組織管理アカウントの組織契約タブにアクセスし、AWS Management Console の [開始] リンクを選択すると、AWS Artifact によってサービスにリンクされたロールが作成されます。

このサービスリンクロールを削除した後で再度作成する必要が生じた場合は、同じ方法でアカウントにロールを再作成できます。組織管理アカウントの組織契約タブにアクセスし、 [開始] リンクを選択すると、AWS Artifact によってサービスにリンクされたロールが再度作成されます。

AWS Artifact のサービスリンクロールの編集

AWS Artifact では、サービスにリンクされたロールである AWSServiceRoleForArtifact を編集できません。サービスリンクロールを作成すると、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、IAM を使用したロールの説明の編集はできます。詳細については、IAM ユーザーガイドの「サービスにリンクされたロールの編集」を参照してください。

AWS Artifact のサービスリンクロールの削除

サービスリンクロールが必要な機能またはサービスが不要になった場合には、そのロールを削除することをお勧めします。そうすることで、使用していないエンティティがアクティブにモニタリングされたり、メンテナンスされたりすることがなくなります。ただし、手動で削除する前に、サービスリンクロールのリソースをクリーンアップする必要があります。

> **Note**
>
> リソースを削除する際に、AWS Artifact のサービスでロールが使用されている場合、削除は失敗することがあります。失敗した場合は、数分待ってから操作を再試行してください。

AWSServiceRoleForArtifact が使用している AWS Artifact リソースを削除するには

1. AWS Artifact コンソールの「組織契約」の表を参照してください
2. 有効な組織契約をすべて終了します。

サービスにリンクされたロールを IAM で手動削除するには

IAM コンソール、 AWS CLI 、または AWS API を使用して、サービスにリンクされたロールである AWSServiceRoleForArtifact を削除します。詳細については、IAM ユーザーガイド の サービスにリンクされたロールの削除 を参照してください。

AWS Artifact のサービスにリンクされたロールをサポートするリージョン

AWS Artifact は、サービスを利用できるすべてのリージョンで、サービスにリンクされたロールの使用をサポートしているわけではありません。AWSServiceRoleForArtifact ロールは、以下のリージョンで使用できます。

リージョン名	リージョン識別子	AWS Artifact でのサポート
米国東部 (バージニア北部)	us-east-1	はい
米国東部 (オハイオ)	us-east-2	いいえ
米国西部 (北カリフォルニア)	us-west-1	いいえ
米国西部 (オレゴン)	us-west-2	はい
アフリカ (ケープタウン)	af-south-1	いいえ
アジアパシフィック (香港)	ap-east-1	いいえ
アジアパシフィック (ジャカルタ)	ap-southeast-3	いいえ
アジアパシフィック (ムンバイ)	ap-south-1	いいえ
アジアパシフィック (大阪)	ap-northeast-3	いいえ
アジアパシフィック (ソウル)	ap-northeast-2	いいえ
アジアパシフィック (シンガポール)	ap-southeast-1	いいえ
アジアパシフィック (シドニー)	ap-southeast-2	いいえ
アジアパシフィック (東京)	ap-northeast-1	いいえ
カナダ (中部)	ca-central-1	いいえ
欧州 (フランクフルト)	eu-central-1	いいえ
欧州 (アイルランド)	eu-west-1	いいえ
欧州 (ロンドン)	eu-west-2	いいえ
欧州 (ミラノ)	eu-south-1	いいえ
欧州 (パリ)	eu-west-3	いいえ
欧州 (ストックホルム)	eu-north-1	いいえ

リージョン名	リージョン識別子	AWS Artifact でのサポート
中東 (バーレーン)	me-south-1	いいえ
中東 (アラブ首長国連邦)	me-central-1	いいえ
南米 (サンパウロ)	sa-east-1	いいえ
AWS GovCloud (米国東部)	us-gov-east-1	いいえ
AWS GovCloud (米国西部)	us-gov-west-1	いいえ

IAM 条件キーの使用

IAM 条件キーを使用すると、特定のレポートカテゴリとシリーズに基づいて、AWS Artifact のレポートにきめ細かくアクセスできます。

次のサンプルポリシーは、特定のレポートカテゴリとシリーズに基づいて IAM ユーザーに割り当てることができるアクセス許可を示します。

Example AWS レポートの読み取りアクセスを管理するポリシーの例

AWS Artifact レポートは IAM リソースの `report` で示されます。

次のポリシーは、`Certifications and Attestations` カテゴリのすべての AWS Artifact レポートを読み取るアクセス許可を付与します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
```

```
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "artifact:ReportCategory": "Certifications and Attestations"
        }
      }
    }
  ]
}
```

次のポリシーは、SOC シリーズのすべての AWS Artifact レポートを読み取るアクセス許可を付与します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "artifact:ListReports"
            ],
            "Resource": "*"
        },{
            "Effect": "Allow",
            "Action": [
                "artifact:GetReport",
                "artifact:GetReportMetadata",
                "artifact:GetTermForReport"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringEquals": {
                    "artifact:ReportSeries": "SOC",
                    "artifact:ReportCategory": "Certifications and Attestations"
                }
            }
        }
```

```
    ]
}
```

次のポリシーは、`Certifications and Attestations` カテゴリを除くすべての AWS Artifact レポートを読み取るアクセス許可を付与します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "artifact:ReportSeries": "SOC",
          "artifact:ReportCategory": "Certifications and Attestations"
        }
      }
    }
  ]
}
```

AWS Artifact による AWS CloudTrail API コールのログ記録

AWS Artifact は AWS CloudTrail と統合されています。このサービスは、ユーザーやロール、または AWS の AWS Artifact のサービスによって実行されたアクションを記録するサービスです。CloudTrail は、AWS Artifact の API コールをイベントとしてキャプチャします。キャプチャされた呼び出しには、AWS Artifact コンソールの呼び出しと、AWS Artifact API オペレーションへのコード呼び出しが含まれます。証跡を作成する場合は、AWS Artifact のイベントなど、Amazon S3 バケットへの CloudTrail イベントの継続的な配信を有効にすることができます 証跡を設定しない場合でも、CloudTrail コンソールの [Event history (イベント履歴)] で最新のイベントを表示できます。CloudTrail によって収集された情報を使用して、AWS Artifact に対して行われた要求、要求が行われた IP アドレス、要求を行った人、要求が行われた日時、および追加の詳細を判別できます。

CloudTrail の詳細については、「AWS CloudTrailユーザーガイド」を参照してください。

CloudTrail での AWS Artifact 情報

CloudTrail は、アカウント作成時に AWS アカウント で有効になります。AWS Artifact でアクティビティが発生すると、そのアクティビティは [Event history] (イベント履歴) の他の AWS のサービスのイベントとともに CloudTrail イベントに記録されます。最近のイベントは、AWS アカウント で表示、検索、ダウンロードできます。詳細については、「CloudTrail イベント履歴でのイベントの表示」を参照してください。

AWS Artifact のイベントなど、AWS アカウント のイベントの継続的な記録については、追跡を作成します。追跡により、CloudTrail はログファイルを Amazon S3 バケットに配信できます。デフォルトでは、コンソールで証跡を作成するときに、証跡がすべての AWS リージョン に適用されます 証跡は、AWS パーティションのすべてのリージョンからのイベントをログに記録し、指定した Amazon S3 バケットにログファイルを配信します。さらに、CloudTrail ログで収集したイベントデータをより詳細に分析し、それに基づく対応するためにその他の AWS のサービスを設定できます。詳細については、次を参照してください。

- 「追跡を作成するための概要」
- CloudTrail がサポートされているサービスと統合
- CloudTrail の Amazon SNS 通知の設定
- 「複数のリージョンから CloudTrail ログファイルを受け取る」および「複数のアカウントから CloudTrail ログファイルを受け取る」

AWS Artifact は、CloudTrail ログファイルのイベントとして以下のアクションのログ記録をサポートします。

- ListReports
- GetAccountSettings
- GetReportMetadata
- GetReport
- GetTermForReport
- PutAccountSettings

各イベントまたはログエントリには、リクエストの生成者に関する情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます。

- リクエストが、ルート認証情報と AWS Identity and Access Management (IAM) ユーザー認証情報のどちらを使用して送信されたか。
- リクエストがロールまたはフェデレーティッドユーザーのテンポラリなセキュリティ認証情報を使用して行われたかどうか。
- リクエストが、別の AWS のサービスによって送信されたかどうか。

詳細については、「CloudTrail userIdentity 要素」をご参照ください。

AWS Artifact ログファイルエントリの理解

追跡は、指定した Amazon S3 バケットにイベントをログファイルとして配信するように設定できます。CloudTrail のログファイルには、単一か複数のログエントリがあります。イベントはあらゆるソースからの単一のリクエストを表し、リクエストされたアクション、アクションの日時、リクエストのパラメータなどの情報が含まれます。CloudTrail ログファイルは、パブリック API コールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

次の例は、 GetReportMetadata アクションを示す CloudTrail ログエントリです。

```
{
  "Records": [
    {
      "eventVersion": "1.03",
      "userIdentity": {
```

```
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::999999999999:user/myUserName",
        "accountId": "999999999999",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "myUserName"
      },
      "eventTime": "2015-03-18T19:03:36Z",
      "eventSource": "artifact.amazonaws.com",
      "eventName": "GetReportMetadata",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "127.0.0.1",
      "userAgent": "Python-httplib2/0.8 (gzip)",
      "errorCode": "AccessDenied",
      "errorMessage": "User: arn:aws:iam::999999999999:user/myUserName is not
 authorized to perform: artifact:GetReportMetadata on resource: arn:aws:artifact:us-
east-1::report/report-f1DIWBmGa2Lhsadg",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "7aebcd0f-cda1-11e4-aaa2-e356da31e4ff",
      "eventID": "e92a3e85-8ecd-4d23-8074-843aabfe89bf",
      "eventType": "AwsApiCall",
      "recipientAccountId": "999999999999"
    },
    {
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::999999999999:user/myUserName",
        "accountId": "999999999999",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "myUserName"
      },
      "eventTime": "2015-03-18T19:04:42Z",
      "eventSource": "artifact.amazonaws.com",
      "eventName": "GetReportMetadata",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "127.0.0.1",
      "userAgent": "Python-httplib2/0.8 (gzip)",
      "requestParameters": {
        "reportId": "report-f1DIWBmGa2Lhsadg"
      },
      "responseElements": null,
```

```
      "requestID": "a2198ecc-cda1-11e4-aaa2-e356da31e4ff",
      "eventID": "20b84ce5-730f-482e-b2b2-e8fcc87ceb22",
      "eventType": "AwsApiCall",
      "recipientAccountId": "999999999999"
    }
  ]
}
```

AWS Artifact のドキュメント履歴

次の表では、AWS Artifact のリリースを説明しています。

変更	説明	日付
きめ細かいレポートアクセスと AWSArtifactReportReadOnlyAccess マネージドポリシー	Artifact レポートへのきめ細かいアクセスを有効にし、レポート条件キーを有効にして、AWSArtifactReportsReadOnlyAccess マネージドポリシーをリリースしました。	2023 年 12 月 15 日
「AWS Artifact のサービスにリンクされたロール」	サービスにリンクされたロールのドキュメントを追加し、AWS Artifact と AWS Organizations の統合に関するポリシーの例を更新しました。	2023 年 9 月 26 日
通知	通知の管理に関するドキュメントを公開し、API リファレンスガイド、CloudTrail ロギングドキュメント、および AWS Artifact Identity and Access Management ページに関連する更新を行いました。	2023 年 8 月 1 日
「サードパーティレポート - 一般提供を開始」	API リファレンスドキュメント、CloudTrail ロギングドキュメントを追加し、サードパーティレポートの一般提供を開始しました。	2023 年 1 月 27 日
「サードパーティレポート (プレビュー)」	AWS Marketplace で自社製品を販売する独立系ソフトウェアベンダーのコンプライ	2022 年 11 月 30 日

	アンスレポートを公開しました。また、サードパーティレポートの Identity and Access Management ページにポリシーの例を追加しました。	
セキュリティ	Identity and Access Management ページに、混乱した代理防止のためのセクションを追加しました。	2021 年 12 月 20 日
レポート	秘密保持契約書を削除し、レポートのダウンロードに関する利用規約を追加しました。	2020 年 12 月 17 日
ホームページと検索	レポートと契約ページにサービスホームページと検索バーを追加しました。	2020 年 5 月 15 日
GovCloud での提供	GovCloud リージョンで AWS Artifact の提供を開始しました。	2019 年 11 月 7 日
AWS Organizations 契約	組織の契約の管理に関するサポートを追加しました。	2018 年 6 月 20 日
契約	AWS Artifact 契約の管理に関するサポートを追加しました。	2017 年 6 月 17 日
初回リリース	このリリースでは AWS Artifact を導入しています。	2016 年 11 月 30 日

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。