AWS Artifact

ユーザーガイド

AWS Artifact: ユーザーガイド

Table of Contents

AWS Artifact とは?

AWS Artifact では、AWS ISO 認定、Payment Card Industry (PCI)、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。AWS Artifact は、AWS に関するドキュメントのみを提供しています。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。

AWS Artifactの開始方法

AWS Artifact は、AWS セキュリティおよびコンプライアンスレポートの中心的なリソースを提供します。AWS Artifact で使用可能なアーティファクトには、Service Organization Control (SOC) レポート、Payment Card Industry (PCI) レポート、および AWS セキュリティコントロールの実装と運用効果を検証する認定機関からの認定が含まれます。AWS Artifact を使用すると、Business Associate Addendum (BAA) などの法的な契約を受諾および管理できます。AWS Organizations を使用すると、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。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: AWS にサインアップする

AWS アカウント をお持ちでない場合は、以下の手順を実行してアカウントを作成してください。

AWS アカウント にサインアップするには

1. https://portal.aws.amazon.com/billing/signup 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、電話のキーパッドを用いて確認コードを入力するように求められます。

ステップ 2: レポートをダウンロードする

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 (p. 4)」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コンソール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. (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。
4. 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。
5. 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、[I have read and agree to all the terms (すべての条件を読み、同意します)] を選択し、[Accept terms and download (規約に同意してダウンロードする)] を選択します。
6. Adobe Acrobat Reader を使用して、ダウンロードしたファイルを開きます。「規約」セクションを読みます。完了したら、指示に従って、ダウンロードしたレポートを表示します。

ステップ 3: 契約の管理

契約を締結する前に、AWS Artifact 機密保持契約 (NDS) の条件をダウンロードして同意する必要があります。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。

AWS との契約を受諾するには

1. を開くAWS Artifactコンソールhttps://console.aws.amazon.com/artifact/。
2. AWS Artifact ナビゲーションペインで [Agreements (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 (p. 6)を参照してください。

AWS Artifact にレポートをダウンロードする

AWS Artifact コンソールからレポートをダウンロードできます。AWS Artifact からレポートをダウンロードすると、レポートは特にお客様用に生成され、各レポートには一意のウォーターマークが含まれます。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 WorkDocs などのセキュアな共有サービスを使用します。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 (p. 10)」を参照してください。

AWS Artifact にサインアップすると、アカウントに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。リスト内の別のレポートへのアクセスをリクエストする場合は、指定の形式を使用して AWS からのアクセスをリクエストします。

レポートをダウンロードするには

1. を開くAWS Artifactコンソール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. (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。
4. 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。
5. 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、[I have read and agree to all the terms (すべての条件を読み、同意します)] を選択し、[Accept terms and download (規約に同意してダウンロードする)] を選択します。
6. Adobe Acrobat Reader を使用して、ダウンロードしたファイルを開きます。「規約」セクションを読みます。完了したら、指示に従って、ダウンロードしたレポートを表示します。

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、常に安全に保護する必要があります。AWS Artifact は、そのドキュメントに対して AWS 責任共有モデルを使用しています。このため、AWS は、AWS クラウドにある間はドキュメントを安全に保護しますが、ダウンロード後に安全に保護するのはお客様の責任になります。 AWS Artifactでは、ドキュメントをダウンロードする前に規約への同意が要求される場合があります。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 WorkDocs などのセキュア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、またはエラーメッセージが表示される場合は、AWS Artifact のよくある質問の「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。

内容

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、「Identity and Access Management (p. 10)」を参照してください。

AWS との契約を受諾するには

1. を開くAWS Artifactコンソールhttps://console.aws.amazon.com/artifact/。
2. AWS Artifact ナビゲーションペインで [Agreements (契約)] を選択します。
3. [Account agreements (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 (p. 9)」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、「Identity and Access Management (p. 10)」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. を開くAWS Artifactコンソールhttps://console.aws.amazon.com/artifact/。
2. AWS Artifact ナビゲーションペインで [Agreements (契約)] を選択します。
3. [Account agreements (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] 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。`describeOrganizations` 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:CreateRole
iam:AttachRolePolicy
```

詳細については、「Identity and Access Management (p. 10)」を参照してください。

組織の契約を受諾するには

1. を開くAWS Artifactコンソールhttps://console.aws.amazon.com/artifact/。
2. AWS Artifact ダッシュボードで、[Agreements (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 (p. 9)」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:CreateRole
iam:AttachRolePolicy
```

詳細については、「Identity and Access Management (p. 10)」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. を開くAWS Artifactコンソールhttps://console.aws.amazon.com/artifact/。

2. AWS Artifact ダッシュボードで、[Agreements (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] 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:CreateRole
iam:AttachRolePolicy
```

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、Identity and Access Management (p. 10)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。

IAM ユーザーを作成し、AWS Artifact へのアクセス権を付与する

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 1: IAM ポリシーを作成する (p. 10)
- 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 (p. 11)
- ステップ 3: IAM ユーザーを作成してグループに追加する (p. 11)

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] (ポリシーの作成) 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 (p. 11) 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、Policy Validator によってレポートされます。
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. [Create policy] (ポリシーの作成) 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 access (アクセス)] の横にあるチェックボックスをオンにします。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: (次へ:)] を選択します アクセス許可.
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: (次へ:)] を選択します タグ 必要に応じて、ユーザーにタグを追加できます。
7. [Next: (次へ:)] を選択します 確認. 準備が完了したら、[ユーザーの作成] を選択します。

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。単一のアカウントまたは組織に代わって、ユーザーが AWS Artifact レポートにアクセスすること、および契約の受諾およびダウンロードを行うことを許可できます。

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。

- レポートを管理するポリシーの例 (p. 12)

Example レポートを管理するポリシーの例

次のポリシーは、すべての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:Get"
            ],
            "Resource": [
                "arn:aws:artifact:::report-package/*"
            ]
        }
    ]
}
```

次のポリシーは、SOC、PCI、および ISO レポートのみ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: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/*"
            ]
        }
    ]
}
```

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 AWS Organizations と統合するポリシーの例

次のポリシーは、AWS Organizations と統合する AWS Artifact ユーザーの IAM ロールを作成するアクセス許可を付与します。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:CreateRole",
            "Resource": "arn:aws:iam::*:role/service-role/AWSArtifactAccountSync"
        },
        {
            "Effect": "Allow",
            "Action": "iam:AttachRolePolicy",
            "Resource": "arn:aws:iam::*:role/service-role/AWSArtifactAccountSync",
            "Condition": {
                "ArnEquals": {
                    "iam:PolicyARN": "arn:aws:iam::aws:policy/service-role/
AWSArtifactAccountSync"
                }
            }
        }
    ]
}
```

次のポリシーは、AWS Organizations を使用するアクセス許可を AWS Artifact に付与します。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:CreateRole",
            "Resource": "arn:aws:iam::*:role/service-role/AWSArtifactAccountSync"
        },
        {
            "Effect": "Allow",
            "Action": "iam:AttachRolePolicy",
            "Resource": "arn:aws:iam::*:role/service-role/AWSArtifactAccountSync",
            "Condition": {
                "ArnEquals": {
                    "iam:PolicyARN": "arn:aws:iam::aws:policy/service-role/
AWSArtifactAccountSync"
                }
            }
        },
        {
            "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": "*"
        }
    ]
}
```

サービス間での不分別な代理処理の防止

混乱した代理問題とは、あるアクションを実行する許可を持たないエンティティが、より多くの特権を持つエンティティにアクションの実行を強制できることで生じるセキュリティ上の問題です。EclipseAWSでは、サービス間でのなりすましが、不分別な代理処理の問題が発生する可能性があります。サービス間でのなりすましは、1 つのサービス (呼び出し元サービス) が、別のサービス (呼び出し先サービス) を呼び出す場合に発生します。呼び出し元サービスが操作され、それ自身のアクセス許可を使用して、本来アクセス許可が付与されるべきではない方法で別の顧客のリソースに対して働きかけることがあります。これを防ぐために AWS では、お客様のすべてのサービスのデータを保護するのに役立つツールを提供しています。これには、アカウントのリソースへのアクセス権が付与されたサービスプリンシパルを使用します。

間の信頼されたアクセスを有効にするとAWS ArtifactそしてAWS Organizationsでは、そのロールを引き受けることができるユーザーを制限するポリシーを使用して、アカウントにロールを自動的に作成します。

を使用しますaws:SourceArnそしてaws:SourceAccount信頼ポリシーのグローバル条件コンテキストキー。アカウントで作成するサービスロールを引き受けることができるエンティティを制限します。グローバル条件コンテキストキーを使用すると、aws:SourceAccountの値とアカウントaws:SourceArn同じポリシーステートメントで使用する場合は、同じアカウント ID を使用する必要があります。

以下に、次の間で信頼されたアクセスを有効にしたときにロールを使用して作成するポリシーの例を示します。AWS ArtifactそしてAWS Organizations。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "aws-artifact-account-sync.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "ArnEquals": {
                  "aws:SourceArn": "arn:aws:artifact:us-west-2:00117294401"
                },
                "StringEquals": {
                  "aws:SourceAccount": "00117294401"
                }
            }
        }
    ]
}
```

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。

update-history-change	update-history-description	update-history-date
セキュリティ (p. 18)	混乱した代理人防止のための「アイデンティティとアクセス管理」ページにセクションを追加しました。	2021 年 12 月 20 日
レポート (p. 18)	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 (p. 18)	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 (p. 18)	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 (p. 18)	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 (p. 18)	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 (p. 18)	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。