



ユーザーガイド

AWS Artifact



AWS Artifact: ユーザーガイド

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon の商標およびトレードドレスは Amazon 以外の製品およびサービスに使用することはできません。また、お客様に誤解を与える可能性がある形式で、または Amazon の信用を損なう形式で使用することもできません。Amazon が所有していない他のすべての商標は、それぞれの所有者の所有物であり、Amazon と提携、接続、または後援されている場合とされていない場合があります。

Table of Contents

とは AWS Artifact	1
料金	1
開始方法	2
前提条件	2
機能	2
レポートをダウンロードする	3
レポートをダウンロードする	3
PDF キュメント内の添付ファイルを表示する	4
ドキュメントのセキュリティで保護する	5
トラブルシューティング	5
契約の管理	6
アカウント契約の承諾	6
アカウント契約の終了	8
組織契約を受諾する	8
組織契約の終了	10
オフライン契約	11
通知の設定	12
前提条件	12
設定の作成	13
設定の編集	14
設定の削除	15
ID とアクセス管理	16
ユーザーアクセスの許可	16
ステップ 1: IAM ポリシーを作成する	17
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	17
ステップ 3: IAM ユーザーを作成してグループに追加する	18
商用 AWS リージョンの IAM ポリシーの例	18
の IAM ポリシーの例 AWS GovCloud (US) Regions	37
AWS 管理ポリシーの使用	47
AWSArtifactReportsReadOnlyAccess	48
AWSArtifactAgreementsReadOnlyAccess	48
AWSArtifactAgreementsFullAccess	49
ポリシーの更新	49
サービスにリンクされたロールの使用	51

のサービスにリンクされたロールのアクセス許可 AWS Artifact	51
のサービスにリンクされたロールの作成 AWS Artifact	52
のサービスにリンクされたロールの編集 AWS Artifact	52
のサービスにリンクされたロールの削除 AWS Artifact	52
AWS Artifact サービスにリンクされたロールでサポートされているリージョン	53
IAM 条件キーの使用	54
CloudTrail ログイン	58
AWS Artifact CloudTrail の情報	58
AWS Artifact ログファイルエントリについて	59
ドキュメント履歴	62
.....	lxvi

とは AWS Artifact

AWS Artifact は、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提供します。例えば、国際標準化機構 (ISO) 標準および Payment Card Industry (PCI) セキュリティ標準への準拠に関するレポート、および System and Organization Controls (SOC) レポートです。は、AWS セキュリティコントロールの実装と運用の有効性を検証する認証機関からの証明書のダウンロード AWS Artifact も提供します。

では AWS Artifact、製品を販売する独立系ソフトウェアベンダー (ISVs) のセキュリティおよびコンプライアンスドキュメントをダウンロードすることもできます AWS Marketplace。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。

さらに、AWS Artifact を使用して、と組織 AWS アカウント 内の複数の AWS のとの契約のステータスを確認、承諾 AWS アカウント、追跡できます。での契約の詳細については AWS Artifact、「」を参照してください [での契約の管理 AWS Artifact](#)。

使用する 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実証するために、監査アーティファクトとして監査人または規制当局に AWS Artifact ドキュメントを送信できます。これらの監査アーティファクトをガイドラインとして使用して、独自のクラウドアーキテクチャを評価し、会社の内部コントロールの有効性を評価することもできます。監査アーティファクトの詳細については、[AWS Artifact FAQs](#)」を参照してください。

Note

AWS のお客様は、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を作成または取得する責任があります。詳細については、「[責任共有モデル](#)」を参照してください。

料金

AWS は、ドキュメント AWS Artifact と契約を無料で提供します。

の開始方法 AWS Artifact

の使用を開始するには AWS Artifact、AWS Artifact コンソールで主要な機能を試してください。コンソールでは、AWS セキュリティおよびコンプライアンスレポートのダウンロード、法的契約のダウンロードと承諾、AWS Artifact ドキュメントに関する通知のサブスクライブを行うことができます。

前提条件

の機能を使用するには AWS Artifact、が必要です AWS アカウント。セットアップ手順については、[「の作成 AWS アカウント」](#)を参照してください。

機能

の機能を使用する手順については AWS Artifact、以下のトピックを参照してください。

- [レポートをダウンロードする](#)
- [契約の管理](#)
- [通知の設定](#)

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、レポートはお客様専用生成され、すべてのレポートに一意のウォーターマークがあります。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 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](#)
- [PDF キュメント内の添付ファイルを表示する](#)
- [ドキュメントのセキュリティで保護する](#)
- [トラブルシューティング](#)

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、「[での ID とアクセスの管理 AWS Artifact](#)」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。アクセスに問題がある場合は AWS Artifact、[AWS Artifact 「サービス認可リファレンス」](#) 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. <https://console.aws.amazon.com/artifact/> で AWS Artifact コンソールを開きます。
2. AWS Artifact ホームページで、レポートの表示を選択します。

レポートページのAWS レポートタブで、AWS レポート (SOC 1/2/3、PCI、C5 など) にアクセスできます。サードパーティーレポートタブでは、製品を販売する独立系ソフトウェアベンダー (ISVsからのレポートにアクセスできます AWS Marketplace)。

3. (オプション) レポートを検索するには、検索フィールドにキーワードを入力します。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することもできます。例えば、Cloud Computing Compliance Controls Catalogue (C5) レポー

トを検索するには、「Title」、「contains」演算子 (:、「C5」という用語 () を使用してタイトル列を検索できます**Title : C5**。

4. (オプション) レポートの詳細については、レポートのタイトルを選択して詳細ページを開きます。
5. (オプション) レポートの以前のバージョンをダウンロードする場合は、レポートタイトルを選択してレポートの詳細ページを開くことができます。詳細ページで、以前のバージョンセクションを探し、目的のバージョン行でダウンロードを選択してレポートの特定のバージョンをダウンロードします。
6. 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。
7. ダウンロードする特定のレポートの利用規約に同意するように求められる場合があります (レポートをダウンロードするには利用規約に同意する)。利用規約をよく読むことをお勧めします。読み終わったら、「I have read and agree to the terms」を選択し、「Accept terms and download report」を選択します。
8. PDF ビューワーを使用して、ダウンロードしたファイルを開きます。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、PDF ファイル内の添付ファイルをチェックして、サポートドキュメント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、「」を参照してください[PDF キュメント内の添付ファイルを表示する](#)。

PDF キュメント内の添付ファイルを表示する

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 Reader

Adobe ウェブサイト <https://get.adobe.com/reader/> から Adobe Acrobat Reader の最新バージョンをダウンロードします。

Acrobat Reader で PDF 添付ファイルを表示する方法については、Adobe Support ウェブサイトの「[PDF でのPDFs](#)」を参照してください。

Firefox ブラウザ

1. Mozilla ウェブサイト <https://www.mozilla.org/en-US/firefox/new/> から最新の Firefox ウェブブラウザをダウンロードします。

2. Firefox の組み込み PDF ビューワーで PDF ファイルを開きます。手順については、[「Firefox で PDF ファイルを表示する」](#)を参照するか、Mozilla サポートウェブサイトの「[別のビューワーを選択する](#)」を参照してください。
3. Firefox の組み込み PDF ビューワーで PDF 添付ファイルを表示するには、サイドバーの切り替え、添付ファイルの表示を選択します。

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、ドキュメントを安全に保つ責任がありますが、ダウンロードした後は、ドキュメントを安全に保つ責任があります。は、ドキュメントをダウンロードする前に、利用規約に同意する必要がある AWS Artifact 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。

での契約の管理 AWS Artifact

AWS Artifact を使用して、AWS アカウント または組織の契約を確認および管理できます。例えば、医療保険の相互運用性と説明責任に関する法律 (HIPAA) の対象となる企業では、保護対象の医療情報 (PHI) が適切に保護されるように AWS、通常、との事業提携契約 (BAA) が必要です。AWS Artifact コンソールでは、このような契約を確認して承諾し、PHI AWS アカウント を法的に処理できる を指定できます。

を使用する場合は AWS Organizations、組織 AWS アカウント 内のすべてのユーザー AWSに代わって BAA などの契約を受諾できます。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。

AWS Artifact を使用して、お客様 AWS アカウント または組織が契約を承諾したことを確認し、承諾された契約の条項を確認してお客様の義務を理解することもできます。アカウントまたは組織が承諾された契約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、後でその契約が必要であることに気付いた場合は、契約を再度アクティブ化できます。

内容

- [AWS アカウント での の契約への同意 AWS Artifact](#)
- [AWS アカウント での の契約の終了 AWS Artifact](#)
- [での組織との契約の受諾 AWS Artifact](#)
- [での組織の契約の終了 AWS Artifact](#)
- [でのオフライン契約 AWS Artifact](#)

AWS アカウント での の契約への同意 AWS Artifact

AWS Artifact コンソールを使用して、AWS のとの契約を確認して承諾できます AWS アカウント。

Important

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である場合は、IAM ユーザーとフェデレーテッドユーザーに、1 つ以上の契約にアクセスして管理するアクセス許可を付与できます。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 およびフェデレーテッドユーザーが必要な[アクセス許可](#)を持っている必要があります。

詳細については、「[での ID とアクセスの管理 AWS Artifact](#)」を参照してください。

との契約を受諾するには AWS

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. <https://console.aws.amazon.com/artifact/> で AWS Artifact コンソールを開きます。
5. ナビゲーションペインで、契約を選択します。
6. 契約ページで、次のいずれかを実行します。
 - アカウントに対してのみ契約を受諾するには、アカウント契約タブを選択します。
 - 組織に代わって契約を受諾するには、組織契約タブを選択します。
7. 契約を選択し、契約のダウンロードを選択します。

レポートをダウンロードするための NDA の承諾ダイアログボックスが表示されます。

8. 選択した契約をダウンロードする前に、まず秘密保持契約 (AWS Artifact NDA) AWS Artifact の条項に同意する必要があります。
 - a. NDA を承諾してレポートをダウンロードするダイアログボックスで、NDA AWS Artifact を確認します。
 - b. (オプション) NDA のコピーを印刷するには (または PDF AWS Artifact として保存するには)、 「NDA の印刷」 を選択します。
 - c. 選択 NDA のすべての条項を読み、同意します。
 - d. AWS Artifact NDA を承諾し、選択した契約の PDF をダウンロードするには、「NDA を承諾してダウンロードする」 を選択します。
9. PDF ビューワーで、ダウンロードした契約 PDF を確認します。
10. AWS Artifact コンソールで、契約を選択し、契約を承諾を選択します。
11. 「契約を承諾する」ダイアログボックスで、次の操作を行います。
 - a. 契約を確認します。

- b. 選択 これらのすべての利用規約に同意します。
- c. 「契約を承諾する」を選択します。

12. [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 アカウント での の契約の終了 AWS Artifact

AWS Artifact コンソールを使用して[単一の の契約を受諾 AWS アカウント](#)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[でのオフライン契約 AWS Artifact](#)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 およびフェデレーテッドユーザーが必要な[アクセス許可](#)を持っている必要があります。

詳細については、「[での ID とアクセスの管理 AWS Artifact](#)」を参照してください。

とのオンライン契約を終了するには AWS

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. 契約の終了に同意することを示すチェックボックスをすべて選択します。
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] を選択してください。

での組織との契約の受諾 AWS Artifact

AWS Organizations お客様が組織の管理アカウントの所有者である場合は、組織 AWS アカウント内のすべての AWS に代わって との契約を受諾できます。

Important

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。

AWS Organizations には、一括請求機能とすべての機能という 2 つの機能セットがあります。組織 AWS Artifact で を使用するには、所属する組織を [すべての機能](#) で有効にする必要があります。組織が一括請求用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。

組織契約を承諾または終了するには、適切な AWS Artifact アクセス許可で管理アカウントにサインインする必要があります。アクセス `organizations:DescribeOrganization` 許可を持つメンバーアカウントのユーザーは、ユーザーに代わって承諾された組織契約を表示できます。

詳細については、「AWS Organizations ユーザーガイド」の「[を使用して組織内のアカウントを管理する AWS Organizations](#)」を参照してください。

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必要な [アクセス許可](#) が必要です。

詳細については、「[での ID とアクセスの管理 AWS Artifact](#)」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. <https://console.aws.amazon.com/artifact/> で AWS Artifact コンソールを開きます。
5. ナビゲーションペインで、契約を選択します。
6. 契約ページで、次のいずれかを実行します。
 - アカウントに対してのみ契約を受諾するには、アカウント契約タブを選択します。
 - 組織に代わって契約を受諾するには、組織契約タブを選択します。
7. 契約を選択し、契約のダウンロードを選択します。

レポートをダウンロードするための NDA の承諾ダイアログボックスが表示されます。

8. 選択した契約をダウンロードする前に、まず秘密保持契約 (AWS Artifact NDA) AWS Artifact の条項に同意する必要があります。
 - a. NDA を承認してレポートをダウンロードするダイアログボックスで、NDA AWS Artifact を確認します。
 - b. (オプション) NDA のコピーを印刷するには (または PDF AWS Artifact として保存するには)、 「NDA の印刷」を選択します。

- c. 選択 NDA のすべての条項を読み、同意します。
 - d. AWS Artifact NDA を承諾し、選択した契約の PDF をダウンロードするには、「NDA を承諾してダウンロードする」を選択します。
9. PDF ビューワーで、ダウンロードした契約 PDF を確認します。
 10. AWS Artifact コンソールで、契約を選択し、契約を承諾を選択します。
 11. 契約を承諾ダイアログボックスで、次の操作を行います。
 - a. 契約を確認します。
 - b. 選択 これらのすべての利用規約に同意します。
 - c. 「契約を承諾する」を選択します。
 12. Accept を選択して、組織内のすべての既存アカウントと将来のアカウントの契約を承諾します。

での組織の契約の終了 AWS Artifact

の組織内のすべてのメンバーアカウントに代わって AWS Artifact コンソールを使用して契約を受諾した場合、コンソールを使用してその契約を終了できます。[AWS Organizations](#) それ以外の場合は[でのオフライン契約 AWS Artifact](#)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た場合、そのメンバーアカウントは組織契約の対象範囲が長くなります。管理アカウント管理者は、組織からメンバーアカウントを削除する前に、必要に応じて新しい契約を締結できるように、これをメンバーアカウントに伝える必要があります。アクティブな組織契約のリストは、AWS Artifact コンソールの「契約」ページの[「組織契約」](#)で確認できます。

詳細については AWS Organizations、「AWS Organizations ユーザーガイド」の[「を使用して組織内のアカウントを管理する AWS Organizations」](#)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必要な[アクセス許可](#)が必要です。

詳細については、「[での ID とアクセスの管理 AWS Artifact](#)」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. 契約の終了に同意することを示すチェックボックスをすべて選択します。
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] を選択してください。

でのオフライン契約 AWS Artifact

既存のオフライン契約がある場合、はオフラインで承諾した契約 AWS Artifact を表示します。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。

詳細については、「[での ID とアクセスの管理 AWS Artifact](#)」を参照してください。

での E メール通知の設定 AWS Artifact

Note

このページの内容は commercial AWS [Regions](#) にのみ適用され、現在は適用されません AWS GovCloud (US) Regions。

AWS Artifact コンソールを使用して、 の契約とレポートの更新に関する E メール通知を設定できます AWS Artifact。 は、 を使用してこれらの E メール通知 AWS Artifact を送信します AWS User Notifications。 E メール通知を受信する AWS Artifact には、まず User Notifications コンソールで AWS User Notifications 通知ハブを選択する必要があります。次に、 AWS Artifact コンソールで、通知の受信者と受信する通知を指定する通知設定を作成できます。

E AWS Artifact メール通知を設定するには、 AWS Artifact とに必要なアクセス許可が必要です AWS User Notifications。詳細については、「[での ID とアクセスの管理 AWS Artifact](#)」を参照してください。

内容

- [前提条件: で通知ハブを選択する User Notifications](#)
- [AWS Artifact 通知設定の設定の作成](#)
- [AWS Artifact 通知設定の設定の編集](#)
- [AWS Artifact 通知設定の設定の削除](#)

前提条件: で通知ハブを選択する User Notifications

E AWS Artifact メール通知を受信する前に、まず User Notifications コンソールを開き、データ AWS リージョン を保存する User Notifications の通知ハブを選択する必要があります。通知ハブの選択は AWS User Notifications、 AWS Artifact が通知を送信するために使用する が必要です。

通知ハブを選択するには

1. AWS User Notifications コンソールの[通知ハブ](#)ページを開きます。
2. AWS User Notifications リソース AWS リージョン を保存する の通知ハブを選択します。デフォルトでは、 User Notifications データは米国東部 (バージニア北部) リージョンに保存されます。 は、選択した他のリージョンに通知データを User Notifications レプリケートします。詳細

については、AWS User Notifications ユーザーガイドの[通知ハブのドキュメント](#)を参照してください。

3. [保存して続行] を選択します。

AWS Artifact 通知設定の設定の作成

Note

このページの内容は commercial AWS [Regions](#) にのみ適用され、現在は適用されません AWS GovCloud (US) Regions。

[User Notifications 通知ハブを選択](#)したら、AWS Artifact コンソールで通知設定の設定を作成できます。作成する設定で、AWS Artifact 通知を受信する受信者の E メールアドレスを指定します。また、AWS Artifact 契約の更新や、すべての (またはサブセットの) AWS Artifact レポートの更新など、受信者が通知を受け取る更新も指定します。

設定を作成するには

1. AWS Artifact コンソール[の通知設定](#)ページを開きます。
2. [設定を作成] を選択します。
3. 設定の作成ページで、次の操作を行います。
 - 契約の通知を受け取るには、契約の下で、AWS 契約の更新を選択したままにします。
 - レポートの通知を受信するには、レポートで更新 AWS を選択したままにします。
 - a. すべてのレポートの通知を受信するには、すべてのレポートを選択します。
 - b. 特定のカテゴリと系列のレポートについてのみ通知を受信するには、レポートのサブセットを選択します。次に、関心のあるカテゴリとシリーズを選択します。
 - 設定名に、設定の名前を入力します。
 - Eメールの受信者には、AWS Artifact 通知 Eメールを受信する Eメールアドレスのカンマ区切りリストを入力します。
 - (オプション) 通知設定にタグを追加するには、タグを展開し、新しいタグを追加を選択し、キーと値のペアとしてタグを入力します。User Notifications リソースのタグ付けの詳細については、「AWS User Notifications ユーザーガイド」の[AWS User Notifications 「リソースのタグ付け」](#)を参照してください。

- [設定を作成] を選択します。

User Notifications は、指定した各受信者の E メールアドレスに検証 E メールを送信します。E メールアドレスを検証するには、検証 E メールで、受信者は Eメールの検証を選択する必要があります。検証済みの E メールアドレスのみが AWS Artifact 通知を受け取ります。

AWS Artifact 通知設定の設定の編集

Note

このページの内容は commercial AWS [Regions](#) にのみ適用され、現在は適用されません AWS GovCloud (US) Regions。

AWS Artifact 通知[設定の設定を作成](#)したら、いつでも設定を編集して通知設定を変更できます。たとえば、受信者を追加または削除するには、受信者が受信する通知のタイプを変更し、タグを追加または削除します。

設定を編集するには

1. AWS Artifact コンソール[の通知設定](#)ページを開きます。
2. 編集する設定を選択します。
3. [編集] を選択します。
4. 設定の選択とフィールドを編集します。完了したら、[変更を保存] を選択します。

通知受信者として新しい E メールアドレスを追加した場合、AWS User Notifications はそれらの E メールアドレスを検証 E メールを送信します。E メールアドレスを検証するには、検証 E メールで、受信者は Eメールの検証を選択する必要があります。検証済みの E メールアドレスのみが AWS Artifact 通知を受け取ります。

AWS Artifact 通知設定の設定の削除

Note

このページの内容は commercial AWS [Regions](#) にのみ適用され、現在は適用されません
AWS GovCloud (US) Regions。

AWS Artifact 通知[設定用に作成した](#)設定が不要になった場合は、AWS Artifact コンソールで設定を削除できます。

設定を削除するには

1. AWS Artifact コンソールの[通知設定](#)ページを開きます。
2. 削除する設定を選択します。
3. [削除] を選択します。
4. 設定の削除ダイアログボックスで、削除を選択します。

での ID とアクセスの管理 AWS Artifact

にサインアップするときは AWS、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指定します。これらはルート認証情報であり、AWS リソースを含むすべてのリソースへの完全なアクセスを提供します AWS Artifact。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代わりに、IAM ユーザーと呼ばれる特別なユーザー ID を自分で作成し、のドキュメントや契約にアクセスする必要がある可能性のあるユーザーのために作成する必要があります AWS Artifact。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。

外部でユーザー ID をすでに管理している場合は AWS、IAM ユーザーを作成する代わりに IAM ID プロバイダーを使用できます。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。

内容

- [へのユーザーアクセスの許可 AWS Artifact](#)
- [商用 AWS リージョン AWS Artifact での の IAM ポリシーの例](#)
- [AWS Artifact での の IAM ポリシーの例 AWS GovCloud \(US\) Regions](#)
- [の AWS 管理ポリシーの使用 AWS Artifact](#)
- [のサービスにリンクされたロールの使用 AWS Artifact](#)
- [AWS Artifact レポートに IAM 条件キーを使用する](#)

へのユーザーアクセスの許可 AWS Artifact

必要なアクセスレベル AWS Artifact に基づいて へのアクセス許可をユーザーに付与するには、次の手順を実行します。

タスク

- [ステップ 1: IAM ポリシーを作成する](#)

- [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に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 を選択してください。
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、[商用 AWS リージョン AWS Artifact での の 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. ポリシーのレビュー 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 マネジメントコンソール 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、[ユ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: 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. [次へ: 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。

商用 AWS リージョン AWS Artifact での 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をユーザーに付与し、単一のアカウントまたは組織に代わって契約を受諾およびダウンロードすることができます。

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。

これらのポリシーは commercial AWS [Regions](#) に適用されます。適用可能なポリシーについては AWS GovCloud (US) Regions、[「の IAM ポリシーの例」を参照してください AWS Artifact](#)。AWS [GovCloud \(US\) Regions](#)

- [きめ細かなアクセス許可を持つ AWS 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](#)
- [と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 きめ細かなアクセス許可を使用して AWS レポートを管理するポリシーの例

i Tip

独自のポリシーを定義する代わりに、[AWSArtifactReportsReadOnlyAccess マネージドポリシー](#)の使用を検討してください。

次のポリシーは、きめ細かなアクセス許可を使用してすべての AWS 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:ListReports",
        "artifact:GetReportMetadata",
        "artifact:GetReport",
        "artifact:GetTermForReport",
        "artifact:ListReportVersions"
      ],
      "Resource": "*"
    }
  ]
}
```

次のポリシーは、きめ細かなアクセス許可を使用して AWS 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:ListReports"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReportMetadata",
        "artifact:GetReport",
        "artifact:GetTermForReport",
        "artifact:ListReportVersions"
      ],
      "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代わりに、[AWSArtifactReportsReadOnlyAccess マネージドポリシー](#)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:ListReports"
      ],
      "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ーレポート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": [
        "artifact:GetReportMetadata"
      ],
      "Resource": [
        "arn:aws:artifact:us-east-1::report/report-jRVRFP8HxUN5zpPh:*"
      ]
    }
  ]
}
```

次のポリシーは、特定のバージョンのサードパーティーレポート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": [
        "artifact:GetReportMetadata"
      ],
      "Resource": [
        "arn:aws:artifact:us-east-1::report/report-jRVRF8HxUN5zpPh:1"
      ]
    }
  ]
}
```

i Tip

独自のポリシーを定義する代わりに、[AWSArtifactAgreementsReadOnlyAccess](#) または [AWSArtifactAgreementsFullAccess](#) 管理ポリシーを使用することを検討する必要があります。

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。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
    }
  ]
}
```

```
    "Resource": [
      "*"
    ]
  },
  {
    "Sid": "AWSAgreementActions",
    "Effect": "Allow",
    "Action": [
      "artifact:GetAgreement",
      "artifact:AcceptNdaForAgreement",
      "artifact:GetNdaForAgreement"
    ],
    "Resource": "arn:aws:artifact::agreement/*"
  },
  {
    "Sid": "CustomerAgreementActions",
    "Effect": "Allow",
    "Action": [
      "artifact:GetCustomerAgreement"
    ],
    "Resource": "arn:aws:artifact::*:customer-agreement/*"
  }
]
}
```

次のポリシーは、すべての契約を受け入れるアクセス許可を付与します。

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

```
"Action": [
  "artifact:GetAgreement",
  "artifact:AcceptNdaForAgreement",
  "artifact:GetNdaForAgreement",
  "artifact:AcceptAgreement"
],
"Resource": "arn:aws:artifact:::agreement/*"
}
]
}
```

次のポリシーは、すべて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": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    }
  ]
}
```

次のポリシーは、アカウントレベルアグリーメントを表示および実行するアクセス許可を付与します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    }
  ]
}
```

Exampleと統合するポリシーの例 AWS Organizations

次のポリシーは、AWS Artifact が と統合するために使用する IAM ロールを作成するアクセス許可を付与します AWS Organizations。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": [
    {
      "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole",
        "iam:GetRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": [
            "artifact.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

次のポリシーは、 を使用するアクセス許可を付与するアクセス許可を付与 AWS Artifact します AWS Organizations。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:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource": "*"
    },
    {
      "Sid": "EnableServiceTrustForArtifact",
```

```
"Effect": "Allow",
"Action": [
  "organizations:EnableAWSServiceAccess"
],
"Resource": "*",
"Condition": {
  "StringEquals": {
    "organizations:ServicePrincipal": [
      "aws-artifact-account-sync.amazonaws.com"
    ]
  }
}
]
```

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": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
    }
  ]
}
```

```

    "Resource": "arn:aws:artifact::agreement/*"
  },
  {
    "Sid": "CustomerAgreementActions",
    "Effect": "Allow",
    "Action": [
      "artifact:GetCustomerAgreement",
      "artifact:TerminateAgreement"
    ],
    "Resource": "arn:aws:artifact::*:customer-agreement/*"
  },
  {
    "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
    "Effect": "Allow",
    "Action": [
      "iam:CreateServiceLinkedRole",
      "iam:GetRole"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact",
    "Condition": {
      "StringEquals": {
        "iam:AWSServiceName": [
          "artifact.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid": "EnableServiceTrust",
    "Effect": "Allow",
    "Action": [
      "organizations:ListAWSServiceAccessForOrganization",
      "organizations:DescribeOrganization"
    ],
    "Resource": "*"
  },
  {
    "Sid": "EnableServiceTrustForArtifact",
    "Effect": "Allow",
    "Action": [
      "organizations:EnableAWSServiceAccess"
    ],
    "Resource": "*"
  }
}

```

```
"Condition": {
  "StringEquals": {
    "organizations:ServicePrincipal": [
      "aws-artifact-account-sync.amazonaws.com"
    ]
  }
}
]
```

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": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
```

```
    "Effect": "Allow",
    "Action": [
      "artifact:GetCustomerAgreement",
      "artifact:TerminateAgreement"
    ],
    "Resource": "arn:aws:artifact::*:customer-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": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
  ],
}
```

```
{
  "Sid": "CustomerAgreementActions",
  "Effect": "Allow",
  "Action": [
    "artifact:GetCustomerAgreement"
  ],
  "Resource": "arn:aws:artifact::*:customer-agreement/*"
},
{
  "Effect": "Allow",
  "Action": [
    "organizations:DescribeOrganization"
  ],
  "Resource": "*"
}
]
```

Example 通知を管理するポリシーの例

次のポリシーは、AWS Artifact 通知を使用するための完全な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: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 での の IAM ポリシーの例 AWS GovCloud (US) Regions

これらのポリシーは にのみ適用されます AWS GovCloud (US) Regions。 commercial AWS [Regions](#) に適用されるポリシーについては、 [「商用 AWS リージョン AWS Artifact での の IAM ポリシーの例」](#) を参照してください。

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をユーザーに付与し、単一のアカウントまたは組織に代わって契約を受諾およびダウンロードすることができます。

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 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](#)
- [と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](#)

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

```
    }  
  ]  
}
```

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:ListReports"  
      ],  
      "Resource": "*"   
    },  
    {  
      "Effect": "Allow",  
      "Action": [  
        "artifact:GetReportMetadata",  
        "artifact:GetReport",  
        "artifact:GetTermForReport",  
        "artifact:ListReportVersions"  
      ],  
      "Resource": "*",  
      "Condition": {  
        "StringEquals": {  
          "artifact:ReportSeries": [  
            "SOC",  
            "PCI",  
            "ISO"  
          ],  
          "artifact:ReportCategory": [  
            "Certifications and Attestations"  
          ]  
        }  
      }  
    }  
  ]  
}
```

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:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact::*:customer-agreement/*"
    }
  ]
}
```

次のポリシーは、すべて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:ListAgreements"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact:::agreement/*"
    }
  ]
}
```

次のポリシーは、すべて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": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
```

```
"Sid": "CustomerAgreementActions",
"Effect": "Allow",
"Action": [
  "artifact:GetCustomerAgreement",
  "artifact:TerminateAgreement"
],
"Resource": "arn:aws-us-gov:artifact::*:customer-agreement/*"
}
]
}
```

次のポリシーは、アカウントレベルアグリーメントを表示および実行するアクセス許可を付与します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact::*:agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
```

```
    "artifact:GetCustomerAgreement",
    "artifact:TerminateAgreement"
  ],
  "Resource": "arn:aws-us-gov:artifact::*:customer-agreement/*"
}
]
}
```

Exampleと統合するポリシーの例 AWS Organizations

次のポリシーは、AWS Artifact が統合に使用する IAM ロールを作成するアクセス許可を付与します AWS Organizations。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": [
    {
      "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole",
        "iam:GetRole"
      ],
      "Resource": "arn:aws-us-gov:iam::*:role/aws-service-role/
artifact.amazonaws.com/AWSServiceRoleForArtifact",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": [
            "artifact.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

次のポリシーは、 を使用するアクセス許可を付与するアクセス許可を付与 AWS Artifact します AWS Organizations。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:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource": "*"
    },
    {
      "Sid": "EnableServiceTrustForArtifact",
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "organizations:ServicePrincipal": [
            "aws-artifact-account-sync.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

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": [
```

```
{
  "Sid": "ListAgreementActions",
  "Effect": "Allow",
  "Action": [
    "artifact:ListAgreements",
    "artifact:ListCustomerAgreements"
  ],
  "Resource": "*"
},
{
  "Sid": "AWSAgreementActions",
  "Effect": "Allow",
  "Action": [
    "artifact:GetAgreement",
    "artifact:AcceptNdaForAgreement",
    "artifact:GetNdaForAgreement",
    "artifact:AcceptAgreement"
  ],
  "Resource": "arn:aws-us-gov:artifact::agreement/*"
},
{
  "Sid": "CustomerAgreementActions",
  "Effect": "Allow",
  "Action": [
    "artifact:GetCustomerAgreement",
    "artifact:TerminateAgreement"
  ],
  "Resource": "arn:aws-us-gov:artifact::*:customer-agreement/*"
},
{
  "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
  "Effect": "Allow",
  "Action": [
    "iam:CreateServiceLinkedRole",
    "iam:GetRole"
  ],
  "Resource": "arn:aws-us-gov:iam::*:role/aws-service-role/
artifact.amazonaws.com/AWSServiceRoleForArtifact",
  "Condition": {
    "StringEquals": {
      "iam:AWSServiceName": [
        "artifact.amazonaws.com"
      ]
    }
  }
}
```

```

    }
  },
  {
    "Sid": "EnableServiceTrust",
    "Effect": "Allow",
    "Action": [
      "organizations:ListAWSServiceAccessForOrganization",
      "organizations:DescribeOrganization"
    ],
    "Resource": "*"
  },
  {
    "Sid": "EnableServiceTrustForArtifact",
    "Effect": "Allow",
    "Action": [
      "organizations:EnableAWSServiceAccess"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "organizations:ServicePrincipal": [
          "aws-artifact-account-sync.amazonaws.com"
        ]
      }
    }
  }
]
}

```

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": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [

```

```

        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
    ],
    "Resource": "*"
  },
  {
    "Sid": "AWSAgreementActions",
    "Effect": "Allow",
    "Action": [
      "artifact:GetAgreement",
      "artifact:AcceptNdaForAgreement",
      "artifact:GetNdaForAgreement",
      "artifact:AcceptAgreement"
    ],
    "Resource": "arn:aws-us-gov:artifact:::agreement/*"
  },
  {
    "Sid": "CustomerAgreementActions",
    "Effect": "Allow",
    "Action": [
      "artifact:GetCustomerAgreement",
      "artifact:TerminateAgreement"
    ],
    "Resource": "arn:aws-us-gov:artifact::*:customer-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": [
    {
      "Sid": "ListAgreementActions",

```

```
"Effect": "Allow",
"Action": [
  "artifact:ListAgreements",
  "artifact:ListCustomerAgreements"
],
"Resource": "*"
},
{
  "Sid": "AWSAgreementActions",
  "Effect": "Allow",
  "Action": [
    "artifact:GetAgreement",
    "artifact:AcceptNdaForAgreement",
    "artifact:GetNdaForAgreement"
  ],
  "Resource": "arn:aws-us-gov:artifact:::agreement/*"
},
{
  "Sid": "CustomerAgreementActions",
  "Effect": "Allow",
  "Action": [
    "artifact:GetCustomerAgreement"
  ],
  "Resource": "arn:aws-us-gov:artifact::*:customer-agreement/*"
},
{
  "Effect": "Allow",
  "Action": [
    "organizations:DescribeOrganization"
  ],
  "Resource": "*"
}
]
}
```

の AWS 管理ポリシーの使用 AWS Artifact

AWS 管理ポリシーは、によって作成および管理されるスタンドアロンポリシーです AWS。AWS 管理ポリシーは、ユーザー、グループ、ロールにアクセス許可の割り当てを開始できるように、多くの一般的なユースケースにアクセス許可を付与するように設計されています。

AWS 管理ポリシーは、すべての AWS お客様が使用できるため、特定のユースケースに対して最小特権のアクセス許可を付与しない場合があります。ユースケースに固有の [カスタマー管理ポリシー](#) を定義して、アクセス許可を絞り込むことをお勧めします。

AWS 管理ポリシーで定義されているアクセス許可は変更できません。が AWS 管理ポリシーで定義されたアクセス許可 AWS を更新すると、ポリシーがアタッチされているすべてのプリンシパル ID (ユーザー、グループ、ロール) に影響します。AWS は、新しい が起動されるか、新しい API オペレーション AWS のサービス が既存のサービスで使用できるようになったときに、AWS 管理ポリシーを更新する可能性が高くなります。

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 ポリシーを IAM アイデンティティにアタッチできます。

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。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- artifact – プリンシパルがレポートを一覧表示、表示、ダウンロードできるようにします AWS Artifact。

AWS マネージドポリシー: [AWSArtifactAgreementsReadOnlyAccess](#)

AWSArtifactAgreementsReadOnlyAccess ポリシーを IAM アイデンティティにアタッチできます。

このポリシーは **#AWS Artifact #####** アクセス権を付与します。また、組織の詳細を一覧表示および説明するアクセス許可も含まれています。さらに、このポリシーは、必要なサービスにリンクされたロールが存在するかどうかを確認する機能を提供します。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- `artifact` – プリンシパルがすべての契約を一覧表示し、承諾された契約を表示できるようにします AWS Artifact。
- `iam` – プリンシパルが、必要なサービスにリンクされたロールが存在するかどうかをチェックできるようにします。
- `organizations` – プリンシパルが現在の組織を記述し、その組織のサービスアクセスを一覧表示できるようにします。

AWS マネージドポリシー: [AWSArtifactAgreementsFullAccess](#)

`AWSArtifactAgreementsFullAccess` ポリシーを IAM アイデンティティにアタッチできます。

このポリシーは、AWS Artifact 契約を一覧表示、ダウンロード、承諾、終了するための###アクセス許可を付与します。また、AWS Organizations サービス内の AWS サービスアクセスを一覧表示して有効にし、組織の詳細を記述するアクセス許可も含まれています。さらに、ポリシーでは、必要なサービスにリンクされたロールが存在するかどうかを確認し、存在しない場合はロールを作成します。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- `artifact` – プリンシパルが契約を一覧表示、ダウンロード、承諾、および終了できるようにします AWS Artifact。
- `iam` – プリンシパルが、必要なサービスにリンクされたロールが存在するかどうかを確認し、存在しない場合は作成できるようにします。
- `organizations` – プリンシパルが現在の組織を記述し、その組織のサービスアクセスを一覧表示/有効化できるようにします。

AWS Artifact AWS 管理ポリシーの更新

このサービスがこれらの変更の追跡を開始 AWS Artifact してからの の AWS 管理ポリシーの更新に関する詳細を表示します。このページの変更に関する自動アラートについては、AWS Artifact [ドキュメント履歴](#) ページの RSS フィードにサブスクライブしてください。

変更	説明	日付
AWSArtifactReportsReadOnlyAccess – 既存のポリシーの更新	AWS Artifact は、レポートバージョンの一覧表示を許可するアクセスartifact:ListReportVersions 許可を追加しました。	2025-12-15
AWS Agreements 管理ポリシーの更新	AWSArtifactAgreementsFullAccess 管理ポリシーを更新し、organizations:EnableAWSServiceAccess アクセス許可 AWS Artifactをのサービスプリンシパルに限定しました。これは、管理ポリシーの機能には影響しません。	2025-10-16
AWS レポート管理ポリシーの更新	AWSArtifactReportsReadOnlyAccess 管理ポリシーを更新して artifact:get アクセス許可を削除しました。	2025-03-21
AWS Agreements 管理ポリシーを導入	AWSArtifactAgreementsReadOnlyAccess と AWSArtifactAgreementsFullAccess 管理ポリシーが導入されました。	2024-11-21
AWS Artifact が変更の追跡を開始しました	AWS 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

のサービスにリンクされたロールの使用 AWS Artifact

AWS Artifact 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、直接リンクされた一意のタイプの IAM ロールです AWS Artifact。サービスにリンクされたロールは によって事前定義 AWS Artifact されており、サービスがユーザーに代わって他の AWS サービスを呼び出すために必要なすべてのアクセス許可が含まれています。

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くなるため、 の設定 AWS Artifact が簡単になります。 は、サービスにリンクされたロールのアクセス許可 AWS Artifact を定義します。特に定義されている場合を除き、 のみがそのロールを引き受け AWS Artifact することができます。定義されるアクセス許可には、信頼ポリシーと許可ポリシーが含まれており、その許可ポリシーを他の IAM エンティティにアタッチ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 リソースへのアクセス許可が誤って削除されないため、リソースが保護されます。

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の詳細については、[AWS 「IAM と連携するサービス」](#)を参照し、「サービスにリンクされたロール」列で「はい」があるサービスを探してください。サービスリンク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、リンクで [はい] を選択します。

のサービスにリンクされたロールのアクセス許可 AWS Artifact

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。 が を介して組織に関する情報を収集 AWS Artifact できるようにします AWS Organizations。

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アクセス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

のサービスにリンクされたロールの作成 AWS Artifact

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移動し、の開始方法リンクを選択すると AWS マネジメントコンソール、はサービスにリンクされたロール AWS Artifact を作成します。

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ある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移動し、開始方法リンクを選択すると、はサービスにリンクされたロールを再度 AWS Artifact 作成します。

のサービスにリンクされたロールの編集 AWS Artifact

AWS Artifact では、AWSServiceRoleForArtifact サービスにリンクされたロールを編集することはできません。サービスリンクロールの作成後は、さまざまなエンティティがロールを参照す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 を使用してロールの説明を編集することはできます。詳細については、「IAM ユーザーガイド」の「[サービスリンクロールの編集](#)」を参照してください。

のサービスにリンクされたロールの削除 AWS Artifact

サービスリンクロールを必要とする機能やサービスが不要になった場合は、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

リソースを削除しようとしたときに AWS Artifact サービスがロールを使用している場合、削除が失敗する可能性があります。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 で使用される 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」テーブルにアクセスする
2. 有効な組織契約をすべて終了します。

サービスリンクロールを 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、AWSServiceRoleForArtifact サービスにリンクされたロールを削除します。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 サービスにリンクされたロールでサポートされているリージョン

AWS Artifact は、サービスが利用可能な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	でのサポート ト AWS Artifact
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

リージョン名	リージョン識別子	でのサポート ト AWS Artifact
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
中東 (バーレーン)	me-south-1	いいえ
中東 (UAE)	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	はい

AWS Artifact レポートに IAM 条件キーを使用する

IAM 条件キーを使用して、特定のレポートカテゴリとシリーズに基づいて AWS Artifact、レポートへのきめ細かなアクセスを提供できます。

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 リソースによって示されます report。

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"
        }
      }
    }
  ]
}
```

次のポリシーでは、SOCシリーズ内のすべての AWS Artifact レポートを読み取るアクセス許可を付与できます。

```
{
  "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"
      }
    }
  }
]
```

次のポリシーでは、Certifications and Attestationsカテゴリ、SOC系列のすべての AWS Artifact レポートを読み取るアクセス許可を付与できます。

```
{
  "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"  
}  
}  
]  
}
```

を使用した AWS Artifact API コールのログ記録 AWS CloudTrail

AWS Artifact は、ユーザー AWS CloudTrail、ロール、または のサービスによって実行されたアクションを記録する AWS サービスであると統合されています AWS Artifact。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 コンソールからの呼び出しと 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、イベントを含む 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 AWS Artifact。証跡を設定しない場合でも、CloudTrail コンソールの [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、リクエストの実行元の IP アドレス AWS Artifact、リクエストの実行者、リクエストの実行日時などの詳細を確認できます。

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。

AWS Artifact CloudTrail の情報

CloudTrail は、アカウントの作成 AWS アカウント 時に で有効になります。でアクティビティが発生すると AWS Artifact、そのアクティビティはイベント履歴の他の AWS サービスイベントとともに CloudTrail イベントに記録されます。で最近のイベントを表示、検索、ダウンロードできます AWS アカウント。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。

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 AWS Artifact、証跡を作成します。証跡により、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 パーティション内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 ログで収集されたイベントデータをさらに分析して処理するように他の AWS 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次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](#)
- [AcceptAgreement](#)
- [AcceptNdaForAgreement](#)
- [GetAgreement](#)
- [GetCustomerAgreement](#)
- [GetNdaForAgreement](#)
- [ListAgreements](#)
- [ListCustomerAgreements](#)
- [TerminateAgreement](#)

各イベントまたはログエントリには、誰がリクエストを生成したかという情報が含まれます。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または AWS Identity and Access Management (IAM) ユーザー認証情報を使用して行われたかどうか。
- リクエストがロールまたはフェデレーション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 サービスによって行われたかどうか。

詳細については、「[CloudTrail userIdentity エlement](#)」を参照してください。

AWS Artifact ログファイルエントリについて

「トレイル」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 のログファイルは、単一か複数のログエントリを含みます。イベントは、任意の出典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

ストパラメータなどに関する情報が含まれます。CloudTrail ログファイルは、パブリック API 呼び出し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-httpplib2/0.8 (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-httpplib2/0.8 (gzip)",
    "requestParameters": {
      "reportId": "report-f1DIWBmGa2Lhsadg"
    },
    "responseElements": null,
    "requestID": "a2198ecc-cda1-11e4-aaa2-e356da31e4ff",
    "eventID": "20b84ce5-730f-482e-b2b2-e8fcc87ceb22",
    "eventType": "AwsApiCall",
    "recipientAccountId": "999999999999"
  }
]
}
```

のドキュメント履歴 AWS Artifact

次の表に、AWS Artifact ユーザーガイドの AWS Artifact リリースと関連する変更の履歴を示します。

変更	説明	日付
ListReportVersions API のアクセス許可を更新しました	IAM ポリシーの例 、 GovCloud IAM ポリシーの例 、 AWSArtifactReportsReadOnlyAccess 管理ポリシーの例 を更新し、新しい ListReportVersions API に対応するためにレポートバージョンをダウンロードするための artifact: ListReportVersions アクセス許可とサポートを含むレポート手順をダウンロードしました。	2025 年 12 月 15 日
AWSArtifactAgreementsFullAccess 管理ポリシーを更新	AWSArtifactReportsReadOnlyAccess 管理ポリシー を更新し、organizations:EnableAWSServiceAccess アクセス許可 AWS Artifactを のサービスプリンシパルにスコープダウンしました。これは管理ポリシーの機能には影響しません。	2025 年 10 月 16 日
IAM アクション廃止通知の更新	AWS GovCloud (US) パーティションの artifact: DownloadAgreement およびの IAM アクション廃止通知	2025 年 7 月 1 日

を更新artifact:Get しました。

[AWS Artifact での のきめ
細かなアクセス許可 AWS
GovCloud \(US\) Regions](#)

AWS Artifact で を使用する
ためのポリシーを更新および拡
張しましたが AWS GovCloud
(US) Regions、 AWS Artifact
機能がすべてのリージョン
でより広く適用されるよう
になったため、制限に関する注
意事項を削除しました。

2025 年 3 月 31 日

[AWSArtifactReportR
eadOnlyAccess 管理ポリシー
を更新しました](#)

[AWSArtifactReports
ReadOnlyAccess](#) 管理ポリ
シーを更新して artifact:get ア
クセス許可を削除しました。

2025 年 3 月 21 日

[AWS Artifact の ポリシーの例
AWS GovCloud \(US\) Regions](#)

AWS Artifact で を使用す
るためのポリシーの例を追
加し AWS GovCloud (US)
Regions、 での の使用に
適用されないページを記録
AWS Artifact しました AWS
GovCloud (US) Regions。

2024 年 12 月 6 日

[契約実行、AWSArtifactAg
reementsFullAccess
、AWSArtifactAgreem
entsReadOnlyAccess 管理ポ
リシーのきめ細かなアクセス
許可](#)

AWS Artifact 契約実行の
ためのきめ細かなアクセ
スを有効にし、[AWSArtifa
ctAgreementsFullAccess](#)
と [AWSArtifactAgreeme
ntsReadOnlyAccess](#) AWS 管
理ポリシーを開始しました。

2024 年 11 月 21 日

きめ細かいレポートアクセスと AWSArtifactReportReadOnlyAccess マネージドポリシー	AWS Artifact レポートへのきめ細かなアクセスを有効にし、レポート 条件キー を有効にして、 AWSArtifactReportsReadOnlyAccess 管理ポリシー を起動しました。	2023 年 12 月 15 日
AWS Artifact 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ドキュメントを追加し、AWS Artifact および AWS Organizations 統合のポリシー例を更新しました。	2023 年 9 月 26 日
通知	通知を管理するためのドキュメントを公開し、AWS Artifact API リファレンス、CloudTrail ログ記録ドキュメント、および 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と CloudTrail ログ記録ドキュメントを追加し、サードパーティのレポートを一般公開しました。	2023 年 1 月 27 日
「サードパーティレポート (レビュー)」	製品を販売する独立系ソフトウェアベンダー (ISVs) のコンプライアンスレポートを起動しました AWS Marketplace。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。	2022 年 11 月 30 日

セキュリティ	混乱した代理防止のために、アイデンティティとアクセスの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	機密保持契約を削除し、レポートのダウンロードに関する利用規約を導入しました。	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
AWS GovCloud (US) 起動	AWS Artifact で起動した AWS GovCloud (US) Regions。	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 契約管理の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。