



# **ARP** を有効にする

## ONTAP 9

NetApp  
February 01, 2026

# 目次

ARP を有効にする .....	1
ボリューム上でONTAP Autonomous Ransomware Protectionを有効にする .....	1
NASFlexVolボリュームでARPを有効にする .....	2
NAS FlexGroupボリュームでARPを有効にする .....	5
SANボリュームでARPを有効にする .....	7
関連情報 .....	8
新しいボリュームで ONTAP Autonomous Ransomware Protection をデフォルトで有効にする .....	9
ONTAP Autonomous Ransomware Protection のデフォルトの有効化をオプトアウトする .....	12

# ARP を有効にする

## ボリューム上でONTAP Autonomous Ransomware Protection を有効にする

ONTAP 9.10.1以降では、既存のボリュームに対して自律型ランサムウェア対策（ARP）を有効にすることも、新しいボリュームを作成してARPを最初から有効にすることもできます。

### タスク概要

環境が特定の要件を満たしていることを確認しますの後に、環境に合った手順に従ってARPを有効にします：

- [FlexVolを備えたNAS](#)
- [FlexGroupボリューム付きNAS](#)
- [SANボリューム](#)

ARP を有効にした後、環境と ONTAP バージョンによっては、ARP が移行期間に入る場合があります。

ボリューム タイプ	ONTAPのバージョン	有効化後の動作
NAS FlexGroup	ONTAP 9.18.1以降	ARP/AIは学習期間なしですぐにアクティブになります
	ONTAP 9.13.1 から 9.17.1	ARPは30日間学習モードで開始されます
NAS FlexVol	ONTAP 9.16.1以降	ARP/AIは学習期間なしですぐにアクティブになります
	ONTAP 9.10.1から9.15.1	ARPは30日間学習モードで開始されます
SANボリューム	ONTAP 9.17.1以降	ARP/AI は直ちにアクティブになり、初期の保守的なしきい値から移行する前に、適切なアラートしきい値を確立するための評価期間を開始します。

### 開始する前に

ARP を有効にする前に、環境に次の条件が満たされていることを確認してください：

#### NAS固有の要件

- NFSまたはSMB（またはその両方）プロトコルが有効になっているStorage VM（SVM）。
- クライアントが設定されたNASワークロード。
- ボリュームのアクティブな["ジャンクションパス"](#)。

#### SAN固有の要件

- iSCSI、FC、または NVMe プロトコルが有効になっているストレージ VM（SVM）。
- クライアントが設定されたSANワークロード。

### 一般要件

- ONTAPバージョンの["正しいライセンス"](#)。

- （推奨）マルチ管理者検証（MAV）が有効（ONTAP 9.13.1以降）。"[複数管理者による検証を有効にする](#)"を参照してください。

## NASFlexVolボリュームでARPを有効にする

System ManagerまたはONTAP CLIを使用して、NAS FlexVolボリュームでARPを有効化できます。手順はONTAPバージョンによって異なります。

## ONTAP 9.16.1以降

ONTAP 9.16.1 以降では、学習期間を必要とせず、ARP/AI がすぐにアクティブになります。

### System Manager

1. ストレージ > ボリューム を選択し、保護するボリュームを選択します。
2. \*ボリューム\*概要の\*セキュリティ\*タブで、\*ステータス\*を選択して、無効から有効に切り替えます。
3. \*ランサムウェア対策\*ボックスでボリュームのARP状態を確認します。

すべてのボリュームのARPステータスを表示するには：\*ボリューム\*ペインで\*表示/非表示\*を選択し、\*ランサムウェア対策\*ステータスがチェックされていることを確認します。

### CLI

既存のボリュームでARPを有効にする：

```
security anti-ransomware volume enable -volume <vol_name> -vserver  
<svm_name>
```

ARPを有効にして新しいボリュームを作成：

```
volume create -volume <vol_name> -vserver <svm_name> -aggregate  
<aggr_name> -size <nn> -anti-ransomware-state enabled -junction-path  
</path_name>
```

ARP状態を確認します：

```
security anti-ransomware volume show
```

```
`security anti-ransomware volume show`
```

の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/security-anti-ransomware-volume-show.html](https://docs.netapp.com/us-en/ontap-cli/security-anti-ransomware-volume-show.html) ["ONTAP コマンド リファレンス"] を参照してください。

## ONTAP 9.10.1から9.15.1

ONTAP 9.10.1～9.15.1では、ARPを初期状態**"学習モード"**（または「ドライラン」状態）で有効化する必要があります。システムはワークロードを分析し、正常な動作を特徴付けます。アクティブモードで開始すると、誤検知レポートが過剰に生成される可能性があります。

ARPを学習モードで少なくとも30日間実行することをお勧めします。ONTAP 9.13.1以降では、ARPは最適な学習期間を自動的に決定し、切り替えを自動化するため、30日未満で切り替えが行われる場合があります。

## System Manager

1. ストレージ > ボリューム を選択し、保護するボリュームを選択します。
2. \*ボリューム\*概要の\*セキュリティ\*タブで、\*ステータス\*を選択して、無効から有効に切り替えます。
3. \*Anti-ransomware\*ボックスで\*Enabled in learning-mode\*を選択します。



"関連付けられたStorage VMでアクティブモードへの自動学習遷移を無効にする"学習モードからアクティブモードへの移行を手動で制御する場合は、



既存のボリュームの場合、どちらのモードでも対象となるのは新しく書き込まれたデータだけで、ボリューム内の既存のデータは対象外です。それまでの正常なデータトラフィックの特性は、ボリュームのARPを有効にしたあとの新しいデータに基づいて推定されるため、既存のデータはスキャンも分析もされません。

4. \*ランサムウェア対策\*ボックスでボリュームのARP状態を確認します。

すべてのボリュームのARPステータスを表示するには：\*ボリューム\*ペインで\*表示/非表示\*を選択し、\*ランサムウェア対策\*ステータスがチェックされていることを確認します。

## CLI

既存のボリュームで**ARP**を有効にする：

```
security anti-ransomware volume dry-run -volume <vol_name> -vserver  
<svm_name>
```

```
`security anti-ransomware volume dry-run`
```

の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/security-anti-ransomware-volume-dry-run.html](https://docs.netapp.com/us-en/ontap-cli/security-anti-ransomware-volume-dry-run.html)["ONTAPコマンド リファレンス"]をご覧ください。

**ARP**を有効にして新しいボリュームを作成：

```
volume create -volume <vol_name> -vserver <svm_name> -aggregate  
<aggr_name> -size <nn> -anti-ransomware-state dry-run -junction-path  
</path_name>
```

自動切り替えを無効にする（オプション）：

ONTAP 9.13.1からONTAP 9.15.1にアップグレードし、関連付けられているすべてのボリュームの学習モードからアクティブモードへの切り替えを手動で制御する場合は、SVMから次の操作を実行できます：

```
vserver modify <svm_name> -anti-ransomware-auto-switch-from-learning-to-enabled false
```

**ARP状態を確認します：**

```
security anti-ransomware volume show
```

## NAS FlexGroupボリュームでARPを有効にする

System ManagerまたはONTAP CLIを使用して、NAS FlexGroupボリュームでARPを有効化できます。手順はONTAPバージョンによって異なります。

### ONTAP 9.18.1以降

ONTAP 9.18.1 以降では、FlexGroup ボリュームに対して ARP/AI は学習期間を必要とせず、すぐにアクティブになります。

#### System Manager

1. ストレージ > ボリューム を選択し、保護するFlexGroupボリュームを選択します。
2. \*ボリューム\*概要の\*セキュリティ\*タブで、\*ステータス\*を選択して、無効から有効に切り替えます。
3. \*ランサムウェア対策\*ボックスでボリュームのARP状態を確認します。

すべてのボリュームのARPステータスを表示するには：\*ボリューム\*ペインで\*表示/非表示\*を選択し、\*ランサムウェア対策\*ステータスがチェックされていることを確認します。

#### CLI

既存のFlexGroupボリュームでARPを有効にする：

```
security anti-ransomware volume enable -volume <vol_name> -vserver  
<svm_name>
```

ARPを有効にして新しいFlexGroupボリュームを作成します：

```
volume create -volume <vol_name> -vserver <svm_name> -aggr-list  
<aggregate name> -aggr-list-multiplier <integer> -size <nn> -anti  
-ransomware-state enabled -junction-path </path_name>
```

ARP状態を確認します：

```
security anti-ransomware volume show
```

### ONTAP 9.13.1 から 9.17.1

ONTAP 9.13.1～9.17.1の場合、FlexGroupボリュームは"学習モード"で始まります。システムはワークロードを分析して、通常の動作を特徴付けます。

ARP を学習モードで少なくとも 30 日間実行することをお勧めします。ARP は最適な学習期間間隔を自動的に決定し、切り替えを自動化します。切り替えは 30 日未満で実行される場合もあります。

#### System Manager

1. ストレージ > ボリューム を選択し、保護するFlexGroupボリュームを選択します。
2. \*ボリューム\*概要の\*セキュリティ\*タブで、\*ステータス\*を選択して、無効から有効に切り替えます。
3. \*Anti-ransomware\*ボックスで\*Enabled in learning-mode\*を選択します。





"アクティブモードへの自動学習遷移を無効にする"を使用すると、学習モードからアクティブモードへの移行を手動で制御できます。

4. \*ランサムウェア対策\*ボックスでボリュームのARP状態を確認します。

#### CLI

既存のFlexGroupボリュームでARPを有効にする：

```
security anti-ransomware volume dry-run -volume <vol_name> -vserver  
<svm_name>
```

ARPを有効にして新しいFlexGroupボリュームを作成します：

```
volume create -volume <vol_name> -vserver <svm_name> -aggr-list  
<aggregate name> -aggr-list-multiplier <integer> -size <nn> -anti  
-ransomware-state dry-run -junction-path </path_name>
```

自動切り替えを無効にする（オプション）：

学習モードからアクティブモードへの切り替えを手動で制御する場合：

```
vserver modify <svm_name> -anti-ransomware-auto-switch-from-learning-to  
-enabled false
```

ARP状態を確認します：

```
security anti-ransomware volume show
```

## SANボリュームでARPを有効にする

ONTAP 9.17.1以降では、SANボリュームでARPを有効にできます。ARP/AI機能は自動的に有効になり、"評価期間"中にSANボリュームのアクティブな監視と保護を直ちに開始すると同時に、ワークロードがARPに適しているかどうかを判断し、検出に最適な暗号化しきい値を設定します。

System Manager または ONTAP CLI を使用して、SAN ボリューム上で ARP を有効にすることができます。

## System Manager

### 手順

1. **Storage > Volumes** を選択し、保護する SAN ボリュームを選択します。
2. \*ボリューム\*概要の\*セキュリティ\*タブで、\*ステータス\*を選択して、無効から有効に切り替えます。
3. ARP/AIは自動的に評価期間に入ります。
4. ランサムウェア対策 ボックスで ARP の状態と評価ステータスを確認します。

すべてのボリュームのARPステータスを表示するには：\*ボリューム\*ペインで\*表示/非表示\*を選択し、\*ランサムウェア対策\*ステータスがチェックされていることを確認します。

### CLI

既存の**SAN**ボリュームで**ARP**を有効にする：

```
security anti-ransomware volume enable -volume <vol_name> -vserver  
<svm_name>
```

**ARP**を有効にした新しい**SAN**ボリュームの作成：

```
volume create -volume <vol_name> -vserver <svm_name> -aggregate  
<aggr_name> -size <nn> -anti-ransomware-state enabled
```

**ARP**の状態と評価ステータスを確認します：

```
security anti-ransomware volume show
```

```
`Block device detection  
status`フィールドをチェックして、評価期間の進行状況を監視します。
```

```
`security anti-ransomware volume show`  
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-  
anti-ransomware-volume-show.html["ONTAPコマンド リファレンス  
"^]を参照してください。
```

## 関連情報

- ["学習期間後のアクティブ モードへの切り替え"](#)

# 新しいボリュームで **ONTAP Autonomous Ransomware Protection** をデフォルトで有効にする

ONTAP 9.10.1以降では、ストレージVM (SVM) を設定して、新規ボリュームでAutonomous Ransomware Protection (ARP) がデフォルトで有効になるようにすることができます。この設定は、System ManagerまたはONTAP CLIを使用して変更できます。

ONTAP 9.18.1以降では、クラスタのアップグレードまたは新規インストール後、12時間の猶予期間が経過すると、["サポートされているシステム"](#)のすべての新規ボリュームでクラスタレベルでARPがデフォルトで有効化されます。クラスタレベルでARPの自動デフォルト有効化を無効にした場合でも、SVMレベルですべての新規ボリュームでARPをデフォルトで手動で有効化することができます。

ONTAP 9.17.1 以前では、新しいボリュームで ARP をデフォルトで有効にする唯一の方法は、SVM レベルでの設定です。

## タスク概要

デフォルトでは、新しいボリュームはARP機能が無効の状態で作成されます。SVMで作成される新しいボリュームでは、ARP機能を有効にし、デフォルトで有効になるように設定する必要があります。

ARPが有効になっていない既存のボリュームは、SVMのデフォルト設定を変更しても、ARPの有効化ステータスが自動的に変更されることはありません。この手順で説明するSVM設定の変更は、新しいボリュームにのみ影響します。["既存のボリュームに対してARPを有効にする"](#)方法については、こちらを参照してください。

ARP を有効にした後、環境と ONTAP バージョンによっては、ARP が移行期間に入る場合があります。

ボリューム タイプ	ONTAPのバージョン	有効化後の動作
NAS FlexGroup	ONTAP 9.18.1以降	ARP/AIは学習期間なしですぐにアクティブになります
	ONTAP 9.13.1 から 9.17.1	ARPは30日間学習モードで開始されます
NAS FlexVol	ONTAP 9.16.1以降	ARP/AIは学習期間なしですぐにアクティブになります
	ONTAP 9.10.1から9.15.1	ARPは30日間学習モードで開始されます
SANボリューム	ONTAP 9.17.1以降	ARP/AI は直ちにアクティブになり、初期の保守的なしきい値から移行する前に、適切なアラートしきい値を確立するための評価期間を開始します。

## 開始する前に

ARP を有効にする前に、環境に次の条件が満たされていることを確認してください：

### NAS固有の要件

- NFSまたはSMB（またはその両方）プロトコルが有効になっているStorage VM (SVM) 。
- ボリュームのアクティブな["ジャンクションパス"](#)。

### SAN固有の要件

- iSCSI、FC、または NVMe プロトコルが有効になっているストレージ VM (SVM) 。


#### 一般要件

- ONTAPバージョンの["正しいライセンス"](#)。
- （推奨）マルチ管理者検証（MAV）が有効（ONTAP 9.13.1以降）。["複数管理者による検証を有効にする"](#)を参照してください。

#### 手順

System ManagerまたはONTAP CLIを使用して、新しいボリュームに対してARPをデフォルトで有効にできます。

## System Manager

1. ストレージ または クラスター（環境によって異なります）を選択し、ストレージ **VM** を選択して、ARP で保護するボリュームが含まれるストレージ VM を選択します。
2. \*設定\*タブに移動します。\*セキュリティ\*の下にある\*ランサムウェア対策\*タイルを見つけて、 を選択します。
3. ランサムウェア対策（ARP）を有効にするには、チェックボックスをオンにします。ストレージVM 内のすべての対象ボリュームでARPを有効にするには、追加のチェックボックスをオンにします。
4. 推奨学習期間が設定されているONTAPバージョンの場合は、\*十分な学習後に学習モードからアクティブモードに自動的に切り替える\*を選択します。これにより、ARPが最適な学習期間を判断し、アクティブモードへの切り替えを自動化できます。

## CLI

既存の **SVM** を変更して、新しいボリュームで **ARP** をデフォルトで有効にする

ARPのバージョンで[学習期間](#)が必要な場合は `dry-run` を選択します。それ以外の場合は `enabled` を選択してください。

```
vserver modify -vserver <svm_name> -anti-ransomware-default-volume  
-state <dry-run|enabled>
```

新しいボリュームに対してデフォルトで**ARP**が有効になっている新しい**SVM**を作成します

ARPのバージョンで[学習期間](#)が必要な場合は `dry-run` を選択します。それ以外の場合は `enabled` を選択してください。

```
vserver create -vserver <svm_name> -anti-ransomware-default-volume  
-state <dry-run|enabled>
```

既存の**SVM**を変更して、アクティブモードへの自動学習遷移を無効にする

ONTAP 9.13.1からONTAP 9.15.1にアップグレードし、デフォルトの状態が `dry-run`（学習モード）の場合、アダプティブラーニングが有効になり、`enabled` 状態（アクティブモード）への切り替えが自動的に行われます。この自動切り替えを無効にすると、関連付けられているすべてのボリュームの学習モードからアクティブモードへの切り替えを手動で制御できます：

```
vserver modify <svm_name> -anti-ransomware-auto-switch-from-learning-to  
-enabled false
```

## ARP状態を確認する

```
security anti-ransomware volume show
```

## 関連情報

- ["学習期間後のアクティブ モードへの切り替え"](#)

## ONTAP Autonomous Ransomware Protection のデフォルトの有効化をオプトアウトする

ONTAP 9.18.1以降、AFF A-series、AFF C-series、ASA、ASA r2システムのすべての新規ボリュームでは、アップグレードまたは新規インストール後の12時間のウォームアップ期間後に、Autonomous Ransomware Protection (ARP) がデフォルトで自動的に有効化されます (ARPライセンスがインストールされている場合)。この12時間の猶予期間中または猶予期間終了後に、System ManagerまたはONTAP CLIを使用して、このデフォルトの有効化を解除できます。



既存のボリュームはARP用に"手動で有効化"する必要があります。

### タスク概要


この手順で選択した設定は後で変更できます。猶予期間後は、いつでもデフォルトの有効化をオンまたはオフにすることができます：

```
security anti-ransomware auto-enable modify -new-volume-auto-enable  
false|true
```

### 手順

System Manager または ONTAP CLI を使用して、ARP のデフォルト有効化オプションを管理できます。

## System Manager

1. \*Cluster > Settings\*を選択します。
2. 次のいずれかを実行します。
  - アクティブな猶予期間中に無効にする：
    - i. \*ランサムウェア対策\*セクションで、ARPが有効になるまでの残り時間を示すメッセージが表示されます。\*有効にしない\*を選択します。
    - ii. 次のダイアログ ボックスで 無効 を選択して、新しいボリュームのデフォルトの ARP 有効化がオフになっていることを確認します。
  - 猶予期間後に無効にする：
    - i. \*ランサムウェア対策\*セクションで、 を選択します。
    - ii. チェックボックスを選択して 保存 をクリックすると、新しいボリュームのデフォルトの ARP 有効化が無効になります。

## CLI

1. デフォルトの有効化ステータスを確認します：

```
security anti-ransomware auto-enable show
```

2. 新しいボリュームのデフォルトの有効化を無効にします：

```
security anti-ransomware auto-enable modify -new-volume-auto-enable  
false
```

## 関連情報

- ["個々のボリュームで ONTAP Autonomous Ransomware Protection を有効にする"](#)

## 著作権に関する情報

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

## 商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。