



# ファイル署名の検証

## Cloud Volumes ONTAP

NetApp  
June 27, 2024

# 目次

ファイル署名の検証 .....	1
ファイル署名の検証 .....	1
Linuxでのファイル署名の検証 .....	2
Mac OSでのファイル署名の検証 .....	3

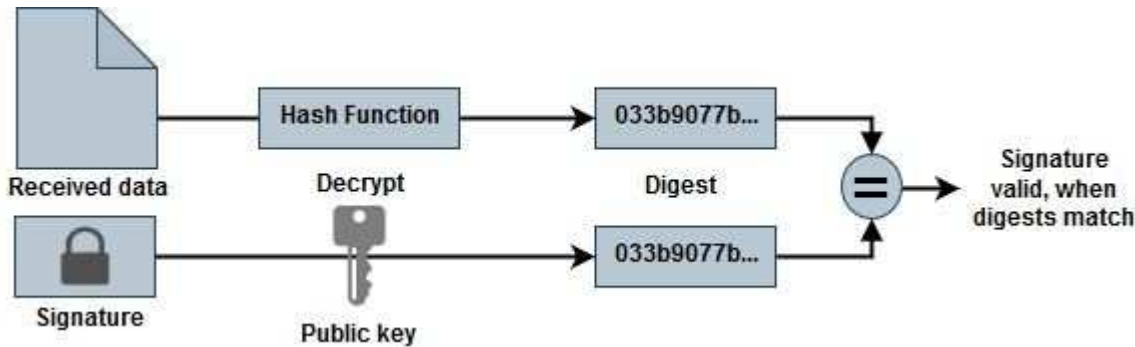
# ファイル署名の検証

## ファイル署名の検証

Azureイメージ検証プロセスでは、先頭に1MB、末尾に512Bのハッシュ関数を使用してストライプされたVHDファイルからダイジェストが生成されます。署名手順と照合するために、SHA256を使用してハッシュが作成されます。先頭の1MBと末尾の512BをVHDファイルから削除し、VHDファイルの残りの部分を確認する必要があります。

### ファイル署名検証ワークフローの概要

次に、ファイル署名検証のワークフロープロセスの概要を示します。



- からAzure Image Digestファイルをダウンロードします。 ["NetApp Support Site"](#) そして、ダイジェストファイル (.sig)、公開鍵証明書ファイル (.pem)、チェーン証明書ファイル (.pem) を展開します。

を参照してください ["Azureイメージダイジェストファイルをダウンロード"](#) を参照してください。

- 信頼チェーンを検証します。
- 公開鍵証明書 (.pem) から公開鍵 (.pub) を抽出します。
- 抽出された公開鍵は、ダイジェストファイルの復号化に使用されます。結果は、画像ファイルから作成された一時ファイルの新しい暗号化されていないダイジェストと比較され、先頭の1MBと末尾の512バイトが削除されます。

この手順は、次のopensslコマンドを使用して実行します。

- 一般的なCLI文は次のように表示されます。

```
openssl dgst -verify <public_key> -keyform <form> <hash_function>  
-signature <digest_file> -binary <temporary_file>
```

- OpenSSL CLIツールでは、両方のファイルが一致する場合は「Verified OK」メッセージが表示され、一致しない場合は「Verification Failure」というメッセージが表示されます。

# Linuxでのファイル署名の検証

LinuxでエクスポートされたVHDファイルのシグネチャを確認するには、次の手順を実行します。

手順

1. からAzure Image Digestファイルをダウンロードします。 ["NetApp Support Site"](#) として、ダイジェストファイル (.sig)、公開鍵証明書ファイル (.pem)、チェーン証明書ファイル (.pem) を展開します。

を参照してください ["Azureイメージダイジェストファイルをダウンロード"](#) を参照してください。

2. 信頼チェーンを検証します。

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. 先頭の1MB（1048576バイト）と末尾の512バイトのVHDファイルを削除します。

'tail'を使用した場合、オプション'-c + K'は指定されたファイルのKTHバイトから始まるバイトを出力します。したがって、1048577は'tail -c'に渡されます。

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. opensslを使用して証明書から公開鍵を抽出し、署名ファイルと公開鍵でストライプされたファイル (sign.tmp) を確認します。

入力ファイルが検証に合格すると、コマンドは次のように表示されます。  
「検証OK」。それ以外の場合は、「Verification Failure」と表示されます。

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verification OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. ワークスペースをクリーンアップします。

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

## Mac OSでのファイル署名の検証

エクスポートしたVHDファイルの署名をMac OSで確認するには、次の手順に従います。

手順

1. からAzure Image Digestファイルをダウンロードします。 ["NetApp Support Site"](#) そして、ダイジェストファイル (.sig) 、公開鍵証明書ファイル (.pem) 、チェーン証明書ファイル (.pem) を展開します。

を参照してください ["Azureイメージダイジェストファイルをダウンロード"](#) を参照してください。

2. 信頼チェーンを検証します。

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. 先頭の1MB (1048576バイト) と末尾の512バイトのVHDファイルを削除します。

'tail'を使用した場合、オプション'-c + K'はKTHバイトから始まるバイトを出力します。をクリックします。したがって、1048577は'tail -c'に渡されます。所要時間は約13mです。Mac OSでtailコマンドを完了します。

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. opensslを使用して証明書から公開鍵を抽出し、署名ファイルと公開鍵を含むファイル (sign.tmp) 。

入力ファイルが検証に合格すると、コマンドは「検証OK」と表示されます。それ以外の場合は、「Verification Failure」と表示されます。

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verified OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

##### 5. ワークスペースをクリーンアップします。

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

## 著作権に関する情報

Copyright © 2024 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。