ブート整合性の可視性

- ブート整合性の可視性について （1 ページ）
- ソフトウェアイメージとハードウェアの確認 （3 ページ）
- プラットフォーム ID とソフトウェア整合性の確認 （3 ページ）
- イメージ署名の検証 （7 ページ）
- ブート整合性の可視性に関する追加情報 （8 ページ）
- ブート整合性の可視性の機能履歴 （8 ページ）

ブート整合性の可視性について

ブート整合性の可視性によって、シスコのプラットフォーム ID とソフトウェアの整合性情報が可視化され、実用可能になります。プラットフォーム ID は、プラットフォームの製造元でインストールされた ID を提供します。ソフトウェアの整合性ではブート整合性の測定値が明らかになり、それを使用してプラットフォームが信頼できるコードを起動しているかどうかを評価できます。

ブートプロセス中に、ソフトウェアはブートローダーアクティビティの各ステージのチェックサムレコードを作成します。

このレコードを取得して、シスコ認定レコードと比較し、ソフトウェアイメージが正規かどうかを確認できます。チェックサム値が一致していない場合は、シスコによって認定されていない、または未承認パーティによって改ざんされているソフトウェアイメージを実行している可能性があります。

イメージ署名とブートアップ

シスコの構築したサーバーが Cisco IOS XE イメージを生成します。Cisco IOS XE イメージの場合、Abraxas イメージ署名システムを使用して、シスコの秘密 RSA キーでイメージに安全に署名できます。

Cisco IOS XE イメージを Catalyst 9000 シリーズ スイッチにコピーすると、シスコの ROMMON ブート ROM がシスコのリリースキーを使用してイメージを検証します。これらのキーは、

Abraxasサーバーに安全に保存されているシスコのリリース秘密キーに対応する公開キーです。リリース秘密キーはROMMONに保存されます。

Catalyst 9000シリーズスイッチは、ブート整合性の可視性機能をサポートしています。ブート整合性の可視性は、ROMMONソフトウェアが改ざんされていないことを確認するために、ROMMONソフトウェアを検証するハードウェア トラスト アンカーとして機能します。

Cisco IOS XEイメージは、構築時にデジタル署名されます。バイナリイメージファイル全体に対してSHA-512ハッシュが生成され、このハッシュがシスコのRSA 2048ビット秘密キーで暗号化されます。ROMMONは、シスコの公開キーを使用して署名を検証します。このソフトウェアがシスコの構築したシステムによって生成されたものではない場合、署名の検証は失敗します。デバイスのROMMONはイメージを拒否し、起動を停止します。署名の検証に成功すると、デバイスはイメージをCisco IOS XE ランタイム環境で起動します。

ROMMONは、ブートアップ中に署名付きCisco IOS XEイメージを検証する際、次の手順を実行します。

1. Cisco IOS XE イメージを CPU メモリにロードします。
2. Cisco IOS XE パッケージのヘッダーを調べます。
3. イメージに対して非セキュア整合性チェックを実行し、ディスクまたは TFTP で意図しないファイル破損が生じていないことを確認します。これは非セキュアSHA-1ハッシュを使用して実行されます。
4. シスコの RSA 2048 ビット公開リリースキーを ROMMON ストレージからコピーし、シスコの RSA 2048 ビット公開リリースキーが改ざんされていないことを検証します。
5. パッケージのヘッダーからコード署名用署名（SHA-512 ハッシュ）を抽出し、シスコの RSA 2048 ビット公開キーを使用して検証します。
6. Cisco IOS XEパッケージのSHA-512ハッシュを計算してコード署名の検証を実行し、コード署名用署名と比較します。これで署名付きパッケージの検証が実行されたことになります。
7. Cisco IOS XEパッケージのヘッダーを調べて、プラットフォームタイプとCPUアーキテクチャの互換性を検証します。
8. Cisco IOS XE パッケージから Cisco IOS XE ソフトウェアを抽出して起動します。

（注） 上記のプロセス中、手順3はイメージの非セキュアチェックであり、ディスクエラー、ファイル転送エラー、またはコピーエラーによる偶発的な破損に関してイメージを確認することを目的としています。これはイメージコード署名の一環ではありません。このチェックは、意図的なイメージの改ざんを検出するためのものではありません。

イメージコード署名の検証は、手順 4、5、および 6 で行われます。これは、2048 ビット RSA キーで暗号化された SHA-512 ハッシュを使用した、イメージのセキュアコード署名チェックです。このチェックは、意図的なイメージの改ざんを検出することを目的としています。

ソフトウェアイメージとハードウェアの確認

このタスクでは、スイッチの起動時に作成されたチェックサムレコードを取得する方法について説明します。特権 EXEC モードで次のコマンドを入力します。

（注） 次のコマンドを実行した後で、メッセージ **% Please Try After Few Seconds** が CLI に表示されることがあります。これはCLIの障害を示すものではありませんが、必要な出力を取得するために必要な基盤となるインフラストラクチャの設定を示します。数分間待機して、コマンドを再度試すことをお勧めします。

メッセージ **% Error retrieving SUDI certificate** および **% Error retrieving integrity data** は、実際の CLI 障害を示します。

手順

	コマンドまたはアクション	目的
ステップ 1	**show platform sudi certificate** ［**sign** ［**nonce** *nonce*］］ **例**： `Device# show platform sudi certificate sign nonce 123`	特定の SUDI のチェックサム レコードを表示します。 • （オプション）**sign**：署名を示します • （オプション）**nonce**：ナンス値を入力します
ステップ 2	**show platform integrity** ［**sign** ［**nonce** *nonce*］］ **例**： `Device# show platform integrity sign nonce 123`	ブート段階のチェックサム レコードを表示します。 • （オプション）**sign**：署名を示します • （オプション）**nonce**：ナンス値を入力します

プラットフォーム ID とソフトウェア整合性の確認

プラットフォーム ID の確認

次に、PEM形式でセキュアな固有デバイス識別子（SUDI）チェーンを表示する例を示します。SUDIにエンコードされるのは、個々のデバイスの製品IDとシリアル番号であり、何千ものデバイスからなるネットワーク上でデバイスを一意に識別できます。最初の証明書は Cisco Root CA 2048 で、2 番目はシスコの下位 CA（ACT2 SUDI CA）です。どちらの証明書も、

https://www.cisco.com/security/pki/ で公開されているものと一致しているかを確認できます。3 番目は SUDI 証明書です。

```
 Device# show platform sudi certificate sign nonce 123
-----BEGIN CERTIFICATE-----
MIIDQzCCAiugAwIBAgIQX/h7KCtU3I1CoxW1aMmt/zANBgkqhkiG9w0BAQUFADA1
MRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENB
IDIwNDgwHhcNMDQwNTE0MjAxNzEyWhcNMjkwNTE0MjAyNTQyWjA1MRYwFAYDVQQK
Ew1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwNDgwggEg
MA0GCSqGSIb3DQEBAQUAA4IBDQAwggEIAoIBAQCwmrmrp68Kd6ficba0ZmKUeIhH
xmJVhEAyv8CrLqUccda8bnuoqrpu0hWISEWdovyD0My5jOAmaHBKeN8hF570YQXJ
FcjPFto1YYmUQ6iEqDGYeJu5Tm8sUxJszR2tKyS7McQr/4NEb7Y9JHcJ6r8qqB9q
VvYgDxFUl4F1pyXOWWqCZe+36ufijXWLbvLdT6ZeYpzPEApk0E5tzivMW/VgpSdH
jWn0f84bcN5wGyDWbs2mAag8EtKpP6BrXruOIIt6keO1aO6g58QBdKhTCytKmg9l
Eg6CTY5j/e/rmxrbU6YTYK/CfdfHbBcl1HP7R2RQgYCUTOG/rksc35LtLgXfAgED
o1EwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJ/PI
FR5umgIJFq0roIlgX9p7L6owEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQEF
BQADggEBAJ2dhISjQal8dwy3U8pORFBi71R803UXHOjgxkhLtv5MOhmBVrBW7hmW
Yqpao2TB9k5UM8Z3/sUcuuVdJcr18JOagxEu5sv4dEX+5wW4q+ffy0vhN4TauYuX
cB7w4ovXsNgOnbFp1iqRe6lJT37mjpXYgyc81WhJDtSd9i7rp77rMKSsH0T8lasz
Bvt9YAretIpjsJyp8qS5UwGH0GikJ3+r/+n6yUA4iGe0OcaEb1fJU9u6ju7AQ7L4
CYNu/2bPPu8Xs1gYJQk0XuPL1hS27PKSb3TkL4Eq1ZKR4OCXPDJoBYVL0fdX4lId
kxpUnwVwwEpxYB5DC2Ae/qPOgRnhCzU=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEPDCCAySgAwIBAgIKYQlufQAAAAAADDANBgkqhkiG9w0BAQUFADA1MRYwFAYD
VQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwNDgw
HhcNMTEwNjMwMTc1NjU3WhcNMjkwNTE0MjAyNTQyWjAnMQ4wDAYDVQQKEwVDaXNj
bzEVMBMGA1UEAxMMQUNUMiBTVURJIENBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEA0m5l3THIxA9tN/hS5qR/6UZRpdd+9aE2JbFkNjht6gfHKd477AkS
5XAtUs5oxDYVt/zEbslZq3+LR6qrqKKQVu6JYvH05UYLBqCj38s76NLk53905Wzp
9pRcmRCPuX+a6tHF/qRuOiJ44mdeDYZo3qPCpxzprWJDPclM4iYKHumMQmqmgmg+
xghHIooWS80BOcdiynEbeP5rZ7qRuewKMpl1TiI3WdBNjZjnpfjg66F+P4SaDkGb
BXdGj13oVeF+EyFWLrFjj97fL2+8oauV43Qrvnf3d/GfqXj7ew+z/sXlXtEOjSXJ
URsyMEj53Rdd9tJwHky8neapszS+r+kdVQIDAQABo4IBWjCCAVYwCwYDVR0PBAQD
AgHGMB0GA1UdDgQWBBRI2PHxwnDVW7t8cwmTr7i4MAP4fzAfBgNVHSMEGDAWgBQn
88gVHm6aAgkWrSugiWBf2nsvqjBDBgNVHR8EPDA6MDigNqA0hjJodHRwOi8vd3d3
LmNpc2NvLmNvbS9zZWN1cml0eS9wa2kvY3JsL2NyY2EyMDQ4LmNybDBQBggrBgEF
BQcBAQREMEIwQAYIKwYBBQUHMAKGNGh0dHA6Ly93d3cuY2lzY28uY29tL3NlY3Vy
aXR5L3BraS9jZXJ0cy9jcmNhMjA0OC5jZXIwXAYDVR0gBFUwUzBRBgorBgEEAQkV
AQwAMEMwQQYIKwYBBQUHAgEWNWh0dHA6Ly93d3cuY2lzY28uY29tL3NlY3VyaXR5
L3BraS9wb2xpY2llcy9pbmRleC5odG1sMBIGA1UdEwEB/wQIMAYBAf8CAQAwDQYJ
KoZIhvcNAQEFBQADggEBAGh1qclr9tx4hzWgDERm371yeuEmqcIfi9b9+GbMSJbi
ZHc/CcCl0lJu0a9zTXA9w47H9/t6leduGxb4WeLxcwCiUgvFtCa51Iklt8nNbcKY
/4dw1ex+7amATUQO4QggIE67wVIPu6bgAE3Ja/nRS3xKYSnj8H5TehimBSv6TECi
i5jUhOWryAK4dVo8hCjkjEkzu3ufBTJapnv89g9OE+H3VKM4L+/KdkUO+52djFKn
hyl47d7cZR4DY4LIuFM2P1As8YyjzoNpK/urSRI14WdIlplR1nH7KNDl5618yfVP
0IFJZBGrooCRBjOSwFv8cpWCbmWdPaCQT2nwIjTfY8c=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDezCCAmOgAwIBAgIEAc+JiTANBgkqhkiG9w0BAQsFADAnMQ4wDAYDVQQKEwVD
aXNjbzEVMBMGA1UEAxMMQUNUMiBTVURJIENBMB4XDTE3MDgxOTEwNDMzOVoXDTI3
MDgxOTEwNDMzOVowZzEmMCQGA1UEBRMdUElEOkM5MzAwLTI0VVggU046RkNXMjEz
NEwwMEMxDjAMBgNVBAoTBUNpc2NvMRgwFgYDVQQLEw9BQ1QtMiBMaXRlIFNVREkx
EzARBgNVBAMTCkM5MzAwLTI0VVgwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQDav5txv4THsqXwWC7AxzHm5MZ28Feqk8FA3tXAv0tV8RXtY4Z9I9XgRzwz
Yw8chknh8LuDMCmGmk8DP+ct++vAF4nkVeIeBeOHnx2RuC9rcR8tuKjCimamDk0M
JHk12w/9+TbdKdNBEy6Sueh1RPVbuSk1oQLQcOYW7CsYC5tI1GkJkfk1nGEK3ni3
ztIpsi7QHyp6k59yccnbzXSdwoBrtbpIIYEk/iHWFRQdlMUunnfIshI7yPneo7V0
NnPc08wk+CA+8XeXk/fnDeGAswKRK1tW9jDP/sY1YubBJNJ4ToqQpG6W/hbNvu3Y
NyS24osSvnn5Bp7on3Rf7eHq9hNjAgMBAAGjbzBtMA4GA1UdDwEB/wQEAwIF4DAM
BgNVHRMBAf8EAjAAME0GA1UdEQRGMESgQgYJKwYBBAEJFQIDoDUTM0NoaXBJRD1V
WUpPVkVZNEZRT0xSbkpwSUUxaGNpQXhNQ0F4Tnpvd05Eb3hNeUFiY1FjPTANBgkq
hkiG9w0BAQsFAAOCAQEASXX+iZLMvHQIR1/s1Pobm0kP/bYeHsgDTRQPRHbCM1HH
```

```
ROfjjDaJMHCspB17XtcLkNNFOwyUEkjoepyHjpxxhekGIqgD6Xt4rW6v/058Haw6
QbAhJFGZriVxFoBvW20VQ4ezyaGoqA+0I2GZqD/ZggUy6zsVwKmMe6inoEgXcYap
5GqF4weEoty9u+OKqr3ppWU475lxnNm/h+WHbNtunL6r7wZfe5dFQIxR5QP5gwRa
svpSsCoKm6PiwIUhw25CvtZ9NTg0tu5t5D7aVcxLeR8XbA1pjfgxw/RtSsjNse3+
ZkOgJUESqlxwzxcGUlY+vDINYRQ/sP6y7cT+niT00A==
-----END CERTIFICATE-----

Signature version: 1
Signature:
[redacted]
```

オプションの RSA 2048 署名は、3 つの証明書、署名のバージョンおよびユーザーにより提供されるナンスに対するものです。

```
RSA PKCS#1v1.5 Sign {<Nonce (UINT64)> || <Signature Version (UINT32)> || <Cisco Root CA
 2048 cert (DER)> ||
<Cisco subordinate CA (DER)> || <SUDI certificate (DER)> }
```

シスコの管理ソリューションには、上記の出力を解釈する機能が装備されています。しかし、OpenSSL コマンドを使用した簡単なスクリプトを使用してプラットフォームの ID を表示して署名を確認することもでき、それによってシスコの一意のデバイス ID を確保できます。

```
[linux-host:~]openssl x509 -in sudicert.pem -subject -noout
subject= /serialNumber=PID:C9300-24P SN:FDO1946BG05/O=Cisco/OU=ACT-2 Lite SUDI/CN=C9300-24P
```

ソフトウェア整合性の確認

次に、ブート段階のチェックサム レコードを表示する例を示します。ハッシュ測定値は、連続してブートされたソフトウェアの 3 つの段階それぞれについて表示されます。これらのハッシュをシスコが提供する基準値と比較できます。出力に署名するオプションを使用すると、出力は正規であり改ざんされていないことを保証する機能が検証ツールに付与されます。リプレイ攻撃から保護するために、ナンスを提供できます。

（注） ブート整合性ハッシュはMD5ハッシュではありません。バンドルファイルに対して**verify/md5 cat9k_iosxe.16.10.01.SPA.bin** コマンドを実行すると、ハッシュは一致しません。

次に、インストールモードでの **show platform integrity sign nonce 123** コマンドの出力例を示します。この出力には、インストールされている各パッケージファイルの測定値が含まれます。

```
Device# show platform integrity sign nonce 123
Platform: C9300-24P
Boot 0 Version: MA0081R06.1307262016
Boot 0 Hash: A99EF9F31CE3F3F8533055407F1C88C62176E667E4E1DA0649EAA7A1282F205E0A
Boot Loader Version: System Bootstrap, Version 16.8.0.3, RELEASE SOFTWARE (P)
Boot Loader Hash:
F8282651465805C3993AB95F53512341BF20F3CC7D4083C980450EA6CD84608EE636B5B15D13414203CED35603F01974B8676C6AC6F9DC45B25CD1039E686C40A
OS Version: 16.10.01
OS Hashes:
cat9k-cc_srdriver.16.10.01.SPA.pkg :
D0D155C1DEFDB03EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0
cat9k-espbase.16.10.01.SPA.pkg :
3EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFDB03EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEF43
cat9k-guestshell.16.10.01.SPA.pkg :
```

```
B0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFDB03EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03E
cat9k-rpbase.16.10.01.SPA.pkg :
4057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFDB03EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C6
cat9k-rpboot.16.10.01.SPA.pkg :
AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFDB03EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057
cat9k-sipbase.16.10.01.SPA.pkg :
9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFDB03EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A
cat9k-sipspa.16.10.01.SPA.pkg :
E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFDB03EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673
cat9k-srdriver.16.10.01.SPA.pkg :
4FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFDB03EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E211
cat9k-webui.16.10.01.SPA.pkg :
CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFDB03EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7
cat9k-wlc.16.10.01.SPA.pkg :
AA7ED0AE935CB0BD84E0D0D155C1DEFDB03EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7CCCA
PCR0: 9745B571B66D79F0936F4D292B5672B50F50FD1E56E74248D48A33582E992574
PCR8: 1CC295C233DA41BD3530A6F09C21991E8406BFFC88249D7778CA4BB0B9E71EB7
Signature version: 1
Signature:
[redacted]
```

次に、バンドルモードでの **show platform integrity sign nonce 123** コマンドの出力例を示します。この出力には、バンドルファイルとインストールされている各パッケージの測定値が含まれます。

```
Device# show platform integrity sign nonce 123
Platform: C9300-24P
Boot 0 Version: MA0081R06.1307262016
Boot 0 Hash: A99EF9F31CE3F3F8533055407F1C88C62176E667E4E1DA0649EAA7A1282F205E0A
Boot Loader Version: System Bootstrap, Version 16.8.0.3, RELEASE SOFTWARE (P)
Boot Loader Hash:
F8282651465805 5C3993AB95F53512341BF20F3CC7D4083C980450EA6CD84608FE636B5B15D13414203CED35603F01974B8676C6AC6F9DC45B25CD1039E686C40A
OS Version: 16.10.01
OS Hashes:
cat9k_iosxe.16.10.01.SPA.bin :
F4CAD08BE1EF841C3A2E3ED8540829F08F3CBA9336F38E45669D4D8B15AD15E365B922AC8B4DC0D5B63E2806D6A1BDAB7839DD9DC8CD7E366A49ED648C113440
cat9k-cc_srdriver.16.10.01.SPA.pkg :
D0D155C1DEFDB03EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0
cat9k-espbase.16.10.01.SPA.pkg :
3EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFDB03EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEF43
cat9k-guestshell.16.10.01.SPA.pkg :
B0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFDB03EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03E
cat9k-rpbase.16.10.01.SPA.pkg :
4057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFDB03EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C6
cat9k-rpboot.16.10.01.SPA.pkg :
AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFDB03EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057
cat9k-sipbase.16.10.01.SPA.pkg :
9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFDB03EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A
cat9k-sipspa.16.10.01.SPA.pkg :
E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFDB03EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673
cat9k-srdriver.16.10.01.SPA.pkg :
4FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFDB03EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E211
cat9k-webui.16.10.01.SPA.pkg :
CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFDB03EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7
cat9k-wlc.16.10.01.SPA.pkg :
AA7ED0AE935CB0BD84E0D0D155C1DEFDB03EB0C64057AD6A9673E2114FA7CCCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7CCCA
PCR0: 9745B571B66D79F0936F4D292B5672B50F50FD1E56E74248D48A33582E992574
PCR8: 1CC295C233DA41BD3530A6F09C21991E8406BFFC88249D7778CA4BB0B9E71EB7
Signature version: 1
Signature:
[redacted]
```

イメージ署名の検証

次に、SHA-512ハッシュを使用した、ブートアップ中のイメージに対するセキュアコード署名チェックの例を示します。

```
switch:boot flash:packages.conf
boot: attempting to boot from [flash:packages.conf]
boot: reading file packages.conf
#
Performing Integrity Check ...
boot: parsed image from conf file: cat9k-rpboot.17.02.01.SSA.pkg
##########################################################################################################################################################################


Loading image in Verbose mode: 1



Image Base is: 0x100099000
Image Size is: 0x2C83487
Package header rev 3 structure detected
Package type:30001, flags:0x0
IsoSize = 0
Parsing package TLV info:
000: 000000090000001D4B45595F544C565F -         KEY_TLV_
010: 5041434B4147455F434F4D5041544942 - PACKAGE_COMPATIB
020: 494C4954590000000000000090000000B - ILITY
030: 4652555F52505F545950450000000009 - FRU_RP_TYPE
040: 000000184B45595F544C565F5041434B -     KEY_TLV_PACK
050: 4147455F424F4F544152434800000009 - AGE_BOOTARCH
060: 0000000E415243485F693638365F5459 -     ARCH_i686_TY
070: 50450000000000009000000144B45595F - PE          KEY_
080: 544C565F424F4152445F434F4D504154 - TLV_BOARD_COMPAT
090: 00000009000000010424F4152445F6361 -         BOARD_ca
0A0: 74396B5F545950450000000900000018 - t9k_TYPE
0B0: 4B45595F544C565F43525950544F5F4B - KEY_TLV_CRYPTO_K
0C0: 4559535452494E470000000900000004 - EYSTRING

TLV: T=9, L=29, V=KEY_TLV_PACKAGE_COMPATIBILITY
TLV: T=9, L=11, V=FRU_RP_TYPE
TLV: T=9, L=24, V=KEY_TLV_PACKAGE_BOOTARCH
TLV: T=9, L=14, V=ARCH_i686_TYPE
TLV: T=9, L=20, V=KEY_TLV_BOARD_COMPAT
TLV: T=9, L=16, V=BOARD_cat9k_TYPE
TLV: T=9, L=24, V=KEY_TLV_CRYPTO_KEYSTRING
TLV: T=9, L=4, V=none
TLV: T=9, L=11, V=CW_BEGIN=$$
TLV: T=9, L=17, V=CW_FAMILY=$cat9k$
TLV: T=9, L=74, V=CW_IMAGE=$cat9k-rpboot.17.02.01.SSA.pkg$
TLV: T=9, L=20, V=CW_VERSION=$17.2.01$
IOS version is 17.2.1
TLV: T=9, L=53, V=CW_FULL_VERSION=$17.2.01.0.869.1580816579..Amsterdam$
TLV: T=9, L=52, V=CW_DESCRIPTION=$Cisco IOS Software, IOS-XE Software$
TLV: T=9, L=9, V=CW_END=$$
Found DIGISIGN TLV type 12 length = 392
RSA Self Test Passed

Expected hash:
DDAF35A193617ABACC417349AE204131
12E6FA4E89A97EA20A9EEEE64B55D39A
```

```
2192992A274FC1A836BA3C23A3FEEBBD
454D4423643CE80E2A9AC94FA54CA49F

Obtained hash:
DDAF35A193617ABACC417349AE204131
12E6FA4E89A97EA20A9EEEE64B55D39A
2192992A274FC1A836BA3C23A3FEEBBD
454D4423643CE80E2A9AC94FA54CA49F
Sha512 Self Test Passed
Found package arch type ARCH_i686_TYPE
Found package FRU type FRU_RP_TYPE
Performing Integrity Check ...

RSA Signed DEVELOPMENT Image Signature Verification Successful.
```

ブート整合性の可視性に関する追加情報

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	*Command Reference (Catalyst 9300 Series Switches)*

ブート整合性の可視性の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Fuji 16.8.1a	ブート整合性の可視性	ブート整合性の可視性によって、シスコのプラットフォームIDとソフトウェアの整合性情報が可視化され、実用可能になります。プラットフォームIDは、プラットフォームの製造元でインストールされたIDを提供します。

Cisco Feature Navigatorを使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigatorには、http://www.cisco.com/go/cfn [英語] からアクセスします。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。