ブート整合性の可視性

ブート整合性の可視性

ブート整合性の可視性は、ROMMON ソフトウェアを検証して完全性を確保することにより、ハードウェア トラストアンカーとして機能します。

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のプラットフォーム ID とソフトウェアの整合性情報の両方が可視化され、実用可能になります。プラットフォーム ID とは、製造時に割り当てられた一意の ID であり、これによって各デバイスを確実に識別できます。ソフトウェア整合性には、ブート整合性測定値のキャプチャを伴います。これは、プラットフォームが、信頼できるコードを使用してブートしているかどうかを判断するのに役立ちます。

お使いのシスコデバイスでは、ブート整合性の可視性機能がサポートされています。

ブート整合性の可視性の仕組み

process_summary

Cisco IOS XE ソフトウェアイメージをシスコデバイスにコピーすると、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。このリリースキーは、シスコのビルドサーバーに安全に保存されているリリース秘密キーに対応する公開キーです。公開リリースキーは ROMMON 内に埋め込まれているため、デバイスはブートに Cisco IOS XE ソフトウェアイメージの真正性と完全性を検証できます。

process_workflow

ROMMON は、デバイスをブートする際に、次の手順に従って署名付き Cisco IOS XE ソフトウェアイメージを検証します。

1. Cisco IOS XE ソフトウェアイメージを CPU メモリにロードします。
2. Cisco IOS XE ソフトウェア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て、ディスクまたは TFTP でファイル破損が生じていないことを確認します。このチェックでは、非セキュア SHA-1 ハッシュが使用されます。

（注） この手順では、ディスク、ファイル転送、またはコピーのエラーによる不注意の破損がチェックされます。これはイメージコード署名の一部ではないため、意図的なイメージ改ざん性は検出されません。

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 公開リリースキーを使用して検証します。
6. Cisco IOS XE ソフトウェアパッケージの SHA-512 ハッシュを計算してコード署名の検証を行い、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 ソフトウェア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 アーキテクチャの適合性を検証します。
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ソフトウェアをブートします。

Result

（注） イメージコード署名の検証は、ステップ 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。

このソフトウェアがシスコのビルドサーバーによって生成されたものではない場合は、署名の検証が失敗します。デバイスの ROMMON がイメージを拒否してブートを停止します。

署名の検証に成功すると、デバイスはイメージをブートして Cisco IOS XE ランタイム環境に入ります。

イメージ署名

シスコのビルドサーバーが Cisco IOS XE ソフトウェアイメージを生成します。Cisco IOS XE ソフトウェアイメージは、ビルド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。

ソフトウェアイメージとハードウェアの確認

ここでは、スイッチのブート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。

表 *1:* チェックサムレコードを取得するコマンド

コマンド	説明
show platform sudi certificate [**sign** [**nonce** *nonce*]]	特定の SUDI のチェックサム レコードを表示します。 • （任意）**sign**： 署名を表示します。 • （任意）**nonce**： ナンス値を入力します。
show platform integrity [**sign** [**nonce** *nonce*]]	ブート段階のチェックサム レコードを表示します。 • （任意）**sign**： 署名を表示します。 • （任意）**nonce**： ナンス値を入力します。

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 であり、
- 2 つ目はシスコの下位 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。

（注） 次のコマンドを実行すると、CLI に「**% Please Try After Few Seconds**」というメッセージが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。数分間待ってから、コマンドをもう一度試します。

```
Device# show platform sudi certificate sign nonce 123
-----BEGIN CERTIFICATE-----
MIIDITCCAgmgAwIBAgIJAZozWHjOFsHBMA0GCSqGSIb3DQEBCwUAMC0xDjAMBgNV
BAoTBUNpc2NvMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwOTkwIBcNMTYwODA5
MjA1ODI4WhgPMjA5OTA4MDkyMDU4MjhaMC0xDjAMBgNVBAoTBUNpc2NvMRswGQYD
VQQDExJDaXNjbyBSb290IENBIDIwOTkwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQDTtuM1fg0+9Gflik4axlCK1I2fb3ESCL8+tk8kOXlhfrJ/zlfRbe60
xRP0iUGMKWKBj0IvvWFf4AW/nyzCR8ujTt4a11Eb55SAKXbXYQ7L4YMg+lmZmg/I
v3GJEc3HCYU0BsY8g9LuLMvqwiNmAwM2jWzNq0EPArt/F6RiQKq6Ta3e7VIfDZ7J
65OA2xASA2FrSe9Vj97KpQReDcm6G7cqFH5f+CrdQ4qwAa4zWNyM3kOpUb637DNd
9m+n6WECyc/IUD+2e+yp21kBZIKH7JvDpu2U7NBPfr52mFX8AfCZgkXV69bp+iYf
saH1DvXIfPpNp93zGKUSXxEj4w881t2zAgMBAAGjQjBAMA4GA1UdDwEB/wQEAwIB
BjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBQ4lVcPNCNO86EmILoUkcdBiB2j
WzANBgkqhkiG9w0BAQsFAAOCAQEAjeKZo+4xd05TFtq99nKnWA0J+DmydBOnPMwY
lDrKfBKe2wVu5AJMvRjgJIoY/CHVPaCOWH58UTqfji95eUaryQ/s36RKrBgMMlwr
WNItxE625PHuaN6EjD1WdWiRMZ2hy8F4FCKz5hgUEvN+PUNZwsPnpU6q3Ay0+11T
4TriwCV8kJx3cWu0NvTypYCCXMscSfLFQR13bo+1z6XNm30SecmrxkmQBVMqjCZM
VvAxhxW1iGnYdPRQuNqt0xITzCSERqg3QVVqYnFJUkNVN6j0dmmMVKZh17HgqLnF
PKkmBlNQ9hQcNM3CSzVvEAK0CCEo/NJ/xzZ6WX1/f8Df1eXbFg==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEZzCCA0+gAwIBAgIJCmR1UkzYYXxiMA0GCSqGSIb3DQEBCwUAMC0xDjAMBgNV
BAoTBUNpc2NvMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwOTkwIBcNMTYwODEx
MjAyODA4WhgPMjA5OTA4MDkyMDU4MjdaMDExHzAdBgNVBAMTFkhpZ2ggQXNzdXJh
bmNlIFNVREkgQ0ExDjAMBgNVBAoTBUNpc2NvMIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEAvdzeSWdDI6lRZDYRvA6JqaRvQyy6Dx1WaqI82UeKR4ZRn0ef
xMGvp4c88/VMS8WSjQO1qolMfMxqHkcSiFBOULx6Trquw4TrEf9sIuzvgJvDaEa8
IllXPwtPtNqZEIWi8jlinz2uGam93KuGPcioHfruzbDKWHL/HWFGYMgz+OKwhD3J
4NRySknQvUovfV8eWLeVOqW8rbnG3TZxv5VexOiK4jL3ObvsQPuAWUwUoo7nuFlE
GTG/VCeyCe/H8+afIScbZOkI9xejtckflnBYFVCyFxzm2H3YZatb6ohbyRXLtOPj
T3SJ+OOoYMlSLd28z727LpRbFFLGYhyWxEXDuQIDAQABo4IBgjCCAX4wDgYDVR0P
AQH/BAQDAgEGMBIGA1UdEwEB/wQIMAYBAf8CAQAwfwYIKwYBBQUHAQEEczBxMEEG
CCsGAQUFBzAChjVodHRwczovL3d3dy5jaXNjby5jb20vc2VjdXJpdHkvcGtpL2Nl
cnRzL2NyY2EyMDk5LmNlcjAsBggrBgEFBQcwAYYgaHR0cDovL3BraWN2cy5jaXNj
by5jb20vcGtpL29jc3AwHwYDVR0jBBgwFoAUOJVXDzQjTvOhJiC6FJHHQYgdo1sw
UgYDVR0gBEswSTBHBgorBgEEAQkVAR4AMDkwNwYIKwYBBQUHAgEWK2h0dHA6Ly93
d3cuY2lzY28uY29tL3NlY3VyaXR5L3BraS9wb2xpY2llcy8wQwYDVR0fBDwwOjA4
oDagNIYyaHR0cDovL3d3dy5jaXNjby5jb20vc2VjdXJpdHkvcGtpL2NybC9jcmNh
MjA5OS5jcmwwHQYDVR0OBBYEFOpro7nBE5d+G/s6jWhgBzlfh0j6MA0GCSqGSIb3
DQEBCwUAA4IBAQBcqYEOgAHhGWKndwM901XX2Enh4hjXR5avDg7G/f6Tb9H509dt
QW+AeZGEghhwUrw1EeG79tHkncAe+m+64xMC1ttyI1RSyn8rBqQYkXnnCRbtF/Nw
pQe5fjvdeIFWJhUI16TOt/ZlkNnWnLsUU1alZmN+J/FhSr8VTJWGRM9gY8hefH8f
5U7LMiDXxsFVHB7R6KGNjvtawrl6W6RKp2dceGxEIIvMahgMWWHHiWOQAOtVrHuE
NEjYR/7klLLwdgQF/NNCA2z47pSfMFnBcr8779GqVIbBTpOP2E6+1pBrE2jBNNoc
uBG1fgvh1qtJUdBbTziAKNoCo4sted6PW2/U
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIFQzCCBCugAwIBAgIKCFlwlokGmWc/RzANBgkqhkiG9w0BAQsFADAxMR8wHQYD
VQQDExZIaWdoIEFzc3VyYW5jZSBTVURJIENBMQ4wDAYDVQQKEwVDaXNjbzAgFw0y
NTA1MDgxMTM1NDJaGA8yMDk5MDgwOTIwNTgyNlowazEmMCQGA1UEBRMdUElEOkM5
MzUwLTQ4VFggU046RlZIMjkxOUw4TVIxDjAMBgNVBAoTBUNpc2NvMRgwFgYDVQQL
Ew9BQ1QtMiBMaXRlIFNVREkxFzAVBgNVBAMTDlE1Q0ItRTVYOS1QRkpRMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA10Xb/EGY8VGXQcgLCgML0yMoR8bx
9cqgHYZ594RkxUt+qO3xvvxgXVPZmK4t+6h4z5/up0hXkZD1UYlXDeOVmQ8Z5rFV
```

```
gRAAr1a8LUWo5pSympQ8kP6Dl3WT9RM9Mu42S7O41W91e59cyTszRMoTUZGqQV9X
UkL8TWLd4ZnM56ZP0l7O9VP3573tGYmNQhlhvZbFQWE3Yx7FkcNPQOZc+PopAjxW
9/s7iFeUy/yGeotYHKbMa5dch1XdbEwttskof6+BZNIS7nc5FSN70+Y2lLy36eCU
Om2xRLixTgWsZIbYXDSld2oeODcDUIgu/eS5klKXUme9yBoWULvYp0mYFQIDAQAB
o4ICHzCCAhswDgYDVR0PAQH/BAQDAgXgMAwGA1UdEwEB/wQCMAAwHwYDVR0jBBgw
FoAU6mujucETl34b+zqNaGAHOV+HSPowggG5BgNVHREEggGwMIIBrKBQBgorBgEE
AQkVAwQCoEITQDhCQzZEQTQzQkVFOUEzMUY2RkVCQUIxRDk3NERBMEZFNDFEMTMy
RjM2ODhFNTA4QkU2MzhGQTU3QjU1NjlFRjKgcAYKKwYBBAEJFQMEBKBiE2AwRkQw
QTAzNzA4MDUyODMxREM2RThGRkE1MzE1NjhCMEFGM0ZFQTRENEIxMTgwRUFFRUZF
MUQ4RjVBODlGNkVGOTQxMDE3MThGNjBBNkM1MDUwODgzNkY1MTlGOTFFMEOgUAYK
KwYBBAEJFQMEA6BCE0AwMjRCNENDNDgwRjE4Njg4MDAwMDAwMDAwMDAwMDAwMDAw
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAw
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAw
MDAwMDAwMDAwMDAwMDAwMKBCBgkrBgEEAQkVAgOgNRMzQ2hpcElEPWhtVzVXR2hu
STRVZWpNSTRIeFRSaXdBQUFBQUFBQUFBQUFBQUFBQUE9MB0GA1UdDgQWBBQF
WtZgjSA/BQT55wuhOk6qq2vGyjANBgkqhkiG9w0BAQsFAAOCAQEAOtAl+Cxyn/lO
h2QDbW6Ors4xPrxADdWDgpdaH6q3qTmU/HRx6mv5T5/y0KRyrwCkFSQRTYBw1/De
7MPV9XXBhUWDAolWN4eqYTMZQF9KTdthmfmTZMQlRZpRTWWYWASfVyt0eObi/RNK
lGKlKyDA+uSfOyKUj6+Yays/bF4A5Bc0bORyCZ0asy4URQ9es6niS6/YuX/FAVrl
xl0BMuiSs83kXxk3lyIUbalN6xz4U17m83m58OWV1sTykRuS58NDyxhmtaWOFLYj
Zap4lJvzu7Dnk0pAgKvwxeUDT1wOJGij/NemwMgXzZEJ7tKgNCaMOpoYGWDPVIZz
pHF1L0A1eQ==
-----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 cisco9k_iosxe.17.18.01.SPA.bin** コマンドを実行すると、ハッシュは一致しません。

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以下に示します。

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: C9350-48TX
Boot 0 Version: MA1007R07.1012142023
Boot 0 Hash: 6F213D15A4E5FAE794A18DF5984F2D1BC79FA6092B624974179C7FD106B97D8D
Boot Loader Version: System Bootstrap, Version 17.15.0.14r, DEVELOPMENT SOFTWARE
Boot Loader Hash: 7A237F1AD265BAE9BFE72741E7BA8231D67984F86D87382A29FC11BCC47CF30C
OS Version: 17.18.01
OS Hashes:
cisco9k_iosxe.17.18.01.SPA.bin:
63249C93EC1531C85D1DDB77886DB97336A35FFFC3B80C048C17442F0363AE8CCBB43F4178B88FE4611F1AC764BFD6CC9F4084CE8098663666B926AE6CB11709
cisco9k-wlc.17.18.01.SPA.pkg:
5FA17640BE34A0627588F21086FD0D0FC9FF4246266CF3A3E902EB3EF5D80BB566211771B72EB55D7C2BBFE2FEC8C2F9A9B9FAD28BB67E16B2095372D2A857AE
cisco9k-lni.17.18.01.SPA.pkg:
6A4A400A26BB3E5B6962CA4624EBBCF86871359077EBDFAF60D7331DF8E8AA7293F108322E6EDD8201CB816D074F1368BF6FD7779FC8EE0A68527D4E9B0D6AE6
cisco9k-guestshell.17.18.01.SPA.pkg:
5C0E5ED9876B8A1DBF9AD945C4D600308AF2312CB540173DDD0F262E363DC944B5A202C0D27731473311983748770DCCA2895B1C8CAEFB64F0BBF69720F6E084F
cisco9k-cc_srdriver.17.18.01.SPA.pkg:
263445E41F41A6867D1B7851E1F8CA0950C5F4347062A5850618C883A07C9CD81B8748BB4236C2EF15A71D4BD1F3E86F79EBACF5EFD18708BF0A1FB48547410D
cisco9k-webui.17.18.01.SPA.pkg:
AC669D965058EC7C708DA1FE396E292157A9151A08CBD42C4FC9C6FC1DE00FAFF1CE1735CCC87CAF4C19E615227FA0360B8FFC9B7C91A29C8F480752BD86A7CA
cisco9k-srdriver.17.18.01.SPA.pkg:
E371A47E8C315A2AEA55C086A2D0A13FB08C60F63853CFC192E71523C75C29BA9A3BF4478DA49648692DBF18144FAA8593EA07D39AAA387D45F8E59A5FBB60E4
cisco9k-rpbase.17.18.01.SPA.pkg:
2AB27567D8DE97623A2EE73E92519BD1DC2BFFAB9511B0CBC9A0FC60871E336E1E9FCB512005C7A5FD0468EEE8EB6C86219BC62B9939B96E50BC624498128093
PCR0: 72E291B753C405FAC5857969F1414DF0265F3BF6AA697E1A3EF67166DB5F8E6D
PCR8: 89AE6C797F6222869E389D2A4625EA854816FD432F501CB6091D4C467BEE8B49
Signature version: 1
Signature:
[redacted]
```

イメージ署名の確認

次の例は、SHA-512 ハッシュを使用した、ブートアップ時のイメージのセキュアコード署名チェックを表しています。

```
switch: boot
system has been configured to boot from device configuration.
boot: attempting to boot from [flash:cisco9k_iosxe.17.18.01.SPA.bin]
boot: reading file cisco9k_iosxe.17.18.01.SPA.bin
[redacted]


Loading image in Verbose mode: 1



Image Base is: 0x100000000
Image Size is: 0x45556D0D
Package header rev 3 structure detected
Package type:30000, flags:0x0
IsoSize = 1103171584
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: 5045000000000009000000144B45595F - PE          KEY_
080: 544C565F424F4152445F434F4D504154 - TLV_BOARD_COMPAT
090: 0000000900000012424F4152445F6369 -         BOARD_ci
0A0: 73636F396B5F5459504500000000009 - sco9k_TYPE
0B0: 000000184B45595F544C565F43525950 -     KEY_TLV_CRYP
0C0: 544F5F4B4559535452494E4700000009 - TO_KEYSTRING

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=18, V=BOARD_cisco9k_TYPE
TLV: T=9, L=24, V=KEY_TLV_CRYPTO_KEYSTRING
TLV: T=9, L=10, V=EnCrYpTiOn
TLV: T=9, L=11, V=CW_BEGIN=$$
TLV: T=9, L=19, V=CW_FAMILY=$cisco9k$
TLV: T=9, L=41, V=CW_IMAGE=$cisco9k_iosxe.17.18.01.SPA.bin$
TLV: T=9, L=21, V=CW_VERSION=$17.18.01$
TLV: T=9, L=50, V=CW_FULL_VERSION=$17.18.01.0.163.1754452537..IOSXE$
TLV: T=9, L=52, V=CW_DESCRIPTION=$Cisco IOS Software, IOS-XE Software$
TLV: T=9, L=9, V=CW_END=$$
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
CiscoRommonBootValidateTlv: Arch
Found package arch type ARCH_i686_TYPE
CiscoRommonBootValidateTlv: Fru
Found package FRU type FRU_RP_TYPE
CiscoRommonBootValidateTlv: Sha1
Performing Integrity Check ...
Returning default key storage: TAM

RSA Signed RELEASE Image Signature Verification Successful.
!
!
!
<<output truncated>>
```

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。