# H.323メッセージ処理の脆弱性


アドバイザリーID : cisco-sa-20040113-h323
初公開日 : 2004-01-13 12:00
バージョン 1.4 : Final
回避策 : No Workarounds available
Cisco バグ ID :

CVE-2004-0056
CVE-2004-0054
CVE-2004-0097
CVE-2003-0819

日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

## 概要

複数のシスコ製品に、H.323メッセージの処理に関する脆弱性が存在します。これらのメッセージは通常、Voice over Internet Protocol(VoIP)またはマルチメディアアプリケーションで使用されます。このプロトコルを対象とし、脆弱性を特定するために、オウル大学によって開発されたテストスイートがあります。

H.323プロトコルのサポートは、Cisco IOS®ソフトウェアリリース11.3Tで導入されました。ソフトウェアに音声/マルチメディアアプリケーションのサポートが含まれている場合、リリース11.3T、およびそれ以降のすべてのCisco IOSリリースが影響を受ける可能性があります。脆弱性が存在するデバイスには、ネットワーク要素としてH.323のソフトウェアサポートが含まれているものや、IOS Network Address Translation（NAT；ネットワークアドレス変換）用に設定されているものや、IOS Firewall（別名Context-Based Access Control [CBAC]）用に設定されているものがあります。

Cisco IOSを実行していない他のCisco音声製品も影響を受ける可能性があります。

これらの脆弱性が繰り返し悪用されると、サービス拒否(DoS)が発生する可能性があります。

このアドバイザリは、
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20040113-h323で確認できます。

## 該当製品

このセクションには、該当製品に関する詳細が掲載されています。

## 脆弱性のある製品

Cisco IOSソフトウェアが稼働し、H.323パケット処理をサポートするすべてのシスコ製品が影響を受けます。これには、セッション開始プロトコル(SIP)またはメディアゲートウェイコントロールプロトコル(MGCP)用に設定されたデバイスが含まれます。これらのプロトコルのサポートにより、H.323のサポートが可能になるためです。「PLUS」機能セットを含むCisco IOSイメージは、設定に関係なく、脆弱性が存在する可能性があります。これは、デフォルトでH.323が有効になっており、プロトコルをオフにできないバグが原因です。

Cisco IOSソフトウェアが稼働していない他の該当製品には、次のものがあります。

- Cisco CallManagerバージョン3.0 ~ 3.3
- Cisco Conference Connection（CCC）
- Cisco Internet Service Node（ISN）
- Cisco BTS 10200 Softswitch
- Cisco 7905 IP Phone H.323ソフトウェアバージョン1.00
- バージョン2.16.1より前のH.323/SIPロードを実行するCisco ATA 18xシリーズ製品

注：Cisco ATA 18xシリーズ製品は、H.323用に設定されている場合にのみ脆弱です。SIP用に設定されている場合は脆弱性の影響を受けません。

Cisco 製品で稼働しているソフトウェアを確認するには、デバイスにログインし、show version コマンドを発行してシステム バナーを表示します。Cisco IOS ソフトウェアは「Internetwork Operating System Software」または単に「IOS」と表示されます。 出力の次の行では、イメージ名がカッコで囲まれて表示され、その後に「Version」とIOSリリース名が続きます。その他の Cisco デバイスには show version コマンドがないか、異なる出力が返されます。

次の例は、シスコ製品でCisco IOSソフトウェアリリース12.0(3)が稼働し、インストールされているイメージ名がC2500-IS-Lであることを示しています。リリーストレインラベルは12.0です。

```
Cisco Internetwork Operating System Software IOS (TM)
2500 Software (C2500-IS-L), Version 12.0(3), RELEASE SOFTWARE
```

次の例は、Cisco IOSソフトウェアリリース12.0(2a)T1が稼働し、イメージ名がC2600-JS-MZである製品を示しています。

```
Cisco Internetwork Operating System Software IOS (tm)
C2600 Software (C2600-JS-MZ), Version 12.0(2a)T1, RELEASE SOFTWARE (fc1)
```

Cisco IOSバージョンの命名に関する詳細については、
http://www.cisco.com/warp/public/620/1.htmlを参照してください。

Cisco IOSバージョン10.x、11.1、11.2以前を実行している場合は、この問題には該当しません。

Cisco IOSによるH.323トラフィックの処理

IOSが不正なH.323パケットに対して脆弱である可能性のある領域が3つあります。次のセクションを読んで、ご使用のルータが該当するかどうかを確認してください。TACケースをオープンする必要がある場合は、推奨される識別手順の出力をキャプチャして、ケースの解決を迅速化してください。

注：H.323トラフィックがルータに入るのを防ぐために、アクセスリストを使用してH.323トラフィックをブロックすることを選択した場合は、このアドバイザリで説明されている脆弱性からデバイスを保護することになり、以下に示す詳細は適用されません。この方法の詳細については、「回避策」のセクションを参照してください。シスコでは、お客様ができるだけ早く適切なIOSイメージにアップグレードすることを推奨しています。

Cisco IOSデバイスがH.323トラフィックを処理しており、脆弱である可能性があるかどうかを確認するには、Cisco IOSソフトウェアがH.323トラフィックを処理する3つの異なる方法を理解する必要があります。

1. H.323エンドポイント

これには、H.323ゲートウェイ、H.323ゲートキーパー、およびプロキシを使用するH.323ゲートキーパーが含まれます。また、設定しなくてもH.323プロセスをデフォルトで実行できるリリースも含まれます。次の手順に従って、お使いのデバイスが該当するかどうかを確認してください。

イネーブルプロンプトからshow process cpuコマンドを実行して、CCH323_CTというプロセスを探します。Cisco IOSソフトウェアの新しいバージョンでは、show process cpu | include CCH323コマンドを使用します。

<#root>

```
Router#
show process cpu | include CCH323
 112 Mwe 60F3E5E0       295112     239401    123220072/24000  0 CCH323_CT
```

注：「PLUS」機能セット（IP PLUS、ENTERPRISE PLUSなど）を持つイメージのみが音声をサポートし、CCH323_CTプロセスが実行されます。12.0では、「PLUS」機能セットには、

2600および3600プラットフォームでデフォルトで実行されるCCH323_CTプロセスがあります。12.1以降では、音声カードまたはdspカードが挿入されている場合、デフォルトでこのプロセスが実行されます。

- CCH323_CTというaプロセスが表示される場合、ルータが影響を受けています。使用しているデバイスに適したバージョンを確認するには、IOSの表を参照してください。すぐにアップグレードできない場合は、次の回避策が有効です
  – ネットワーク内でH.323を使用していない場合、TCPポート1720をブロックする着信アクセスリストによってルータが保護されますが、可能な限り早急にアップグレードすることをお勧めします。
  - H.323を使用している場合は、アクセスリストを設定して、TCPポート1720のトラフィックを既知の信頼できるIPアドレスに制限できます。繰り返しますが、可能な限り速やかにアップグレードすることをお勧めします。
- CCH323_CTプロセスが表示されない場合でも、脆弱性が存在する可能性があります。H.323ゲートキーパーの一部の設定には脆弱性が存在します。該当する設定は、H.323プロキシ用に設定されたゲートキーパーです。ゲートキーパーとして設定されているかどうかを確認するには、グローバル設定の行「proxy h323」の設定を確認します。「proxy h323」が設定されている場合、脆弱性が存在します。
  - GKプロキシ機能を使用していない場合は、次の設定を行ってプロキシ機能を無効にすることができます。

  注：ゲートキーパーで管理されているすべてのコールがドロップされます。ゲートキーパーの機能を安全に停止できる場合にのみ、これを実行してください。

  ```
  <#root>

  Router(config)#

  no proxy h323

  Router(config)#

  gatekeeper

  Router(config-gk)#

  shutdown

  Router(config-gk)#

  no shutdown
  ```

  - H.323プロキシを使用している場合、TCPポート1720のトラフィックを既知の信頼できるIPアドレスに制限するようにアクセスリストを設定するか、IOSバージョンをアップグレードします。

2. IOS Firewall（コンテキストベースアクセスコントロール）

IOSデバイスがIOSファイアウォール（IOS FWまたはContext-Based Access Control [CBAC]）を使用するように設定されている場合は、show ip inspect allコマンドを発行して、IOS FWがデバイスで実行されているかどうかを確認します。IOS FWがインターフェイスに適用されていることを示す次の行を探します。この場合、インスペクションルール「<NAME>」はインターフェイスFastEthernet0/0にインバウンドで適用されます。

```
Interface Configuration
 Interface FastEthernet0/0
  Inbound inspection rule is <NAME>
   tcp alert is on audit-trail is off timeout 3600
   h323 alert is on audit-trail is off timeout 3600
  Outgoing inspection rule is not set
```

- インターフェイスFastEthernet0/0で着信IOS FW(CBAC)をオフにするには、インターフェイス設定モードで次のコマンドを入力します。

  <#root>

  Router#

  **config t**

  Router(config)#

  **Interface FastEthernet 0/0**

  Router(config-if)#

  **no ip inspect**

  **in**

- アウトバウンドIOS FW(CBAC)がFastEthernet0/0に設定されている場合は、インターフェイスコンフィギュレーションモードで次のコマンドを入力します。

  <#root>

  Router#

  **config t**

  Router(config)#

  **Interface FastEthernet 0/0**

```
Router(config-if)#
no ip inspect
```

```
out
```

- 他のIOS FWの動作に影響を与えないまま、H.323メッセージのIOS FW(CBAC)処理だけをオフにするには、グローバルコンフィギュレーションモードで次のコマンドを入力します。

<#root>

```
Router(config)#
no ip inspect name
```

```
h323
```

シスコでは、できるだけ早くIOSをアップグレードすることを推奨しています。

3. IOSネットワークアドレス変換(NAT)

NATルールを設定し、いずれかのインターフェイスでNATがアクティブになっている場合は、show ip nat statisticsコマンドを発行して、デバイスでNATが設定され、アクティブになっているかを確認します。

<#root>

```
Router#
show ip nat statistics
```

```
Total active translations: 3 (3 static, 0 dynamic; 0 extended
Outside interfaces
Inside interfaces
Hits: 0  Misses: 0
Expired translations: 0
Dynamic mappings:
```

- 出力がない場合、または出力に（上の例のように）内部または外部インターフェイスがリストされない場合は、IOSデバイスがNATを実行していないため、NATによる脆弱性の影響を受けません。
- 出力にInsideまたはOutsideインターフェイスが表示される場合、NATが原因で脆弱性が存在する可能性があります。次に例を示します。

```
Total active translations: 3 (3 static, 0 dynamic; 0 extended
Outside interfaces:
  Serial3/0
Inside interfaces:
  Serial1/0
Hits: 0  Misses: 0
Expired translations: 0
Dynamic mappings:
```

- 設定にPort Address Translation（PAT；ポートアドレス変換）ステートメントだけが含まれており、PATステートメントでPAT変換にTCPポート1720が明示的に指定されていない場合、NATの影響を受けて脆弱性は存在しません。
  - PATのみを実行している場合は、overload、route-map、またはextendableキーワードを使用せずに、IOS NAT設定に次のNATルールのいずれかが含まれているかどうかを確認します。

```
ip nat outside source ...
ip nat inside destination ...
ip nat inside source ...
```

  キーワードoverload、route-map、またはextendableが設定されていない上記の行のいずれかが表示される場合、脆弱性が存在します。
  - H.323（TCPポート1720）に対してスタティックPATを実行しているかどうかを確認するには、次のパターンの行を探します。

```
ip nat (inside|outside) source static tcp
ip-addr (port|1720) ip-addr (1720|port)
```

  次の例は、脆弱性の影響を受ける可能性があります。

```
ip nat inside  source static tcp 10.1.0.1 1720 10.2.0.1 5834
ip nat outside source static tcp 10.15.12.1 6884 10.6.7.1 1720
ip nat inside  source static tcp 10.1.0.17 1720 10.33.14.1 1720
```

  次の例は、脆弱性の影響を受けません。

```
ip nat inside  source static tcp 10.1.0.17 53 10.33.14.1 53
ip nat outside source static udp 10.1.14.75 1720 10.131.1.1 6888
```

脆弱性が存在する設定行がある場合は、「回避策」セクションを参照してください。

特定のCisco IOSリリースに脆弱性があるかどうかを確認するには、次の「ソフトウェアバージョンと修正」セクションのリストを参照して、製品が該当するソフトウェアバージョンを実行しているかどうかを確認します。

## 脆弱性を含んでいないことが確認された製品

次のシスコ製品のリストは、これらの脆弱性に関してお客様が懸念する可能性のある製品のリストを示すために提供されています。次の製品は、脆弱性が存在しないか、H.323処理をサポートしていないため、影響を受けません。その他のシスコ製品は本脆弱性の影響を受けないと判断されているため、脆弱性が存在しないと判断された製品、または下記のリストから除外された製品は、脆弱性が存在しないと判断する必要があります。

- Cisco IP Phoneモデル7960、7940、7912、7910、7902、30VIP、および12SP+
- Cisco uOne（すべてのバージョン）
- VG248 Analog Phone Gateway
- Cisco Unityサーバ
- Catalyst 6000 WS-X6608 Voice Services ModuleおよびWS-X6624 FXS Analog Station Interface Module
- PGW2200、SC2200、VSC3000およびH.323シグナリングインターフェイス(HSI)
- Cisco IP/VC 3500シリーズ
- IP/TVシリーズ
- Catalyst 19xx、28xx、290x、292x、2948g、3000、3200、3900、4000、4912g、および5000シリーズスイッチ
- Catalyst 2900XL、2900XL-LRE、2940、2950、2950-LRE、2955、2970、3500XL、3550、および3750シリーズスイッチ
- Cache Engineシリーズ
- Content Engineシリーズ
- SN5400シリーズストレージルータ
- VPN 3000およびVPN 5000シリーズVPNコンセントレータ
- 音声インターワーキング サービス モジュール（VISM）
- VCO/4K
- Cisco Secure Intrusion Detection System(NetRanger)アプライアンスおよびIDSモジュール
- BR340、WGB340、AP340、AP350、およびBR350 Cisco/Aironetワイヤレス製品
- Cisco Aironet 1100シリーズ、1200シリーズ、および1400シリーズワイヤレス製品
- Cisco PIX ファイアウォール

- Cisco Catalyst 6500 シリーズ ファイアウォール サービス モジュール
- CBOSを実行しているCisco 6xxシリーズDSLモデム
- Cisco 7xxシリーズルータ
- Cisco 12000 シリーズ ルータ
- Cisco 10000 シリーズ ルータ
- 61xxおよび62xxシリーズDSLAM
- Cisco CSS11xxxシリーズ（SSLアクセラレータを含む）
- LocalDirector
- BPX、IGX、MGX WANスイッチ、およびサービス拡張シェルフ
- Cisco Intelligent Contact Management（ICM）
- Cisco ONS 15xxxプラットフォーム

# 詳細

H.323は、パケットベース(IP)ネットワークを介したリアルタイムマルチメディア通信および会議の国際電気通信連合(ITU)標準です。H.323標準のサブセットはH.225.0で、コールシグナリングプロトコルとIPネットワーク上のメディアストリームのパケット化に使用される標準です。

H.225.0標準は、抽象構文記法1(ASN.1)を使用して、コール設定、コール制御、および通信のメッセージ形式を定義します。ISDNネットワークでのコールシグナリング用に開発されたITU標準Q.931は、H.225.0内のコールセットアップメッセージの標準としても使用されます。

University of Oulu Secure Programming Group(OUSPG)は、H.323メッセージ、具体的にはH.225.0およびQ.931メッセージのテストスイートを作成し、H.323メッセージの処理における脆弱性の予防的な検出と解決をサポートしています。テストスイートは通常、プロトコルを分析し、プロトコルの実装内のさまざまな設計制限をプローブするメッセージを生成するために使用されます。H.323プロトコルデータユニット(PDU)のさまざまなフィールドに過度に長いまたは例外的な要素を含むテストパケットは、プログラムによって生成され、テスト対象のネットワークデバイスに送信されます。H.323用のPROTOSテストスイートは配布されており、約4500の個別のテストケースが含まれています。

H.323対応のOUSPG PROTOS Test Suiteを使用すると、該当製品で発見された脆弱性を簡単かつ繰り返し実証できます。このアドバイザリで説明されている脆弱性の最大のグループは、該当システムで受信および処理されるH.225.0メッセージの不十分なチェックによるものです。該当システムが受信した不正なH.225.0メッセージにより、さまざまな解析および処理機能が失敗し、ほとんどの状況でシステムクラッシュおよびリロード（またはリブート）が発生する可能性があります。

通常、H.323ネットワーク要素は、ポート1720でUDPとTCPの両方のトランスポートにコールシグナリングを実装します。OUSPGからのH.323テストスイートは、デフォルトではポート1720でのTCP実装のみをテストします。

Cisco IOS

| Cisco IOS ソフトウェア リリース | 脆弱性の説明 |
| --- | --- |
| 11.1、11.2、11.3、12.3 | 脆弱性なし |
| 11.3T、12.0、12.0S、12.0T、12.1、12.1T、12.1E、12.2、12.2S、12.2T | 脆弱性は、H.323ネットワーク要素トラフィックの処理に存在します。これには、H.323ゲートウェイ、H323ゲートキーパー、およびプロキシを使用するH.323ゲートキーパーが含まれます。 |
| 12.1、12.1E、12.2、12.2T、12.2S、12.3T | 脆弱性は、H.323 IOS NATトラフィックの処理に存在します。 |
| 12.0、12.1、12.1E、12.2、12.2T、12.2S | 脆弱性は、H.323 IOS Firewall(CBAC)トラフィックの処理に存在します。 |

H.323ダイヤルピアエンドポイントとして機能するデバイスに対するCisco IOSの脆弱性は、次のBug IDで文書化されています。CSCdt09262(登録ユーザ専用)、CSCdt54401（登録ユーザ専用）、CSCdw14262(登録ユーザ専用)、CSCdx76632（登録ユーザ専用）、CSCdx77253 CSCea19885（登録ユーザ専用）、CSCea32240（登録ユーザユーザ専用）、CSCea36231 CSCea33065（登録ユーザユーザ専用）、CSCea42826（登録ユーザのみ）、CSCea42527（登録ユーザのみ）、CSCea44227（登録ユーザのみ）、CSCea44309（登録ユーザのみ）、CSCea46342（登録ユーザのみ）、CSCec79541（登録ユーザのみ）。

プロキシが設定されたH.323ゲートキーパーとして機能するCisco IOSデバイスについては、脆弱性は次のBug IDで文書化されています。CSCea51076(登録ユーザ専用)、CSCea51030(登録ユーザ専用)、およびCSCea54851(登録ユーザ専用)。

H.323 v3/4トラフィックでNAT変換を実行するCisco IOSデバイスには脆弱性が存在する可能性があります。12.2Tに基づくリリースでは、12.2(11)T以降に基づくバージョンのIOSが稼働しており、隠しコマンドip nat service h323allが有効になっている必要があります。このコマンドのデフォルトの条件は無効です。12.1および12.1Eに基づくリリースでは、デバイスは外部インターフェイスから内部インターフェイスに送信されるパケットに対してのみ脆弱です。つまり、ネットワ

ークは、スタティック変換が設定され、ポート1720への接続を受け入れる場合にのみ脆弱になります。ポート1720でダイナミック変換を実行できますが、攻撃トラフィックは元のフローの宛先アドレスから戻る必要があり、変換がアクティブな間はルータを通過する必要があります。ダイナミック変換の危険を減らす方法については、「回避策」のセクションを参照してください。

IOS 12.1以降のH.323パケットでNATを実行するデバイスに対するCisco IOSの脆弱性は、次のBug IDで文書化されています。CSCdr48143(登録ユーザ専用)、CSCdx40184(登録ユーザ専用)、CSCea27536(登録ユーザ専用)、CSCec76694 CSCed28873(登録ユーザユーザ専用)。

12.1以降のIOSでH.323パケットのディープパケットインスペクションを実行するIOSファイアウォールフィーチャセットを実行しているデバイスに対するCisco IOSの脆弱性は、次のBug IDで文書化されています。CSCec76776(登録ユーザ専用)およびCSCec87533(登録ユーザ専用)。

Cisco CallManager

Cisco CallManagerの脆弱性は、Bug ID CSCdx82831（登録ユーザ専用）、CSCea46545(登録ユーザ専用)、およびCSCea55518(登録ユーザ専用)に記載されています。

3.1または3.2を実行しているCisco CallManagerが脆弱であるためには、発信側デバイスのIPアドレスがCallManagerのH.323ゲートウェイ、H.323クライアント、またはクラスタ間トランクとして設定されているか、CallManager設定のゲートキーパーセクションで「匿名コールを許可」が有効になっている必要があります。H.225.0デバイスとして設定されていないデバイスからH.323メッセージをCallManagerが受信すると、H.225.0メッセージが処理される前にTCPセッションが閉じられます。ゲートキーパー設定で「匿名コールを許可」が有効になっている場合、CallManagerサーバは発信元ソースからのH.225.0メッセージを解析しようとするため、脆弱です。

CallManager 3.3では、サーバは脆弱で、任意の発信元ソースから受信したH.225.0メッセージの解析を試みますが、CallManagerがTCP 1720以外のポートでリッスンしている可能性があります。匿名コールのポート番号はTCP 1720以外の番号であるため、潜在的な攻撃者は攻撃を成功させるために、CallManager H.323ゲートウェイがどのランダムポートをリッスンしているかを判断する必要があります。

Cisco Conference Connection

Cisco Conference Connection(CCC)のすべてのバージョンが影響を受けます。現在、Cisco Conference Connection(CCC)に対するソフトウェア修正は計画されていません。CCCを実行しているお客様は、信頼できるホストからのH.323トラフィックのみを制限する回避策を実装する必要があります。この問題の回避策は「回避策」セクションで説明されています。

Cisco Internet Service Node

すべてのバージョンのInternet Service Node(ISN)が影響を受けます。現在、Cisco Internet Service Node(ISN)に対するソフトウェア修正は計画されていません。ISNを実行しているお客様

は、信頼できるホストからのH.323トラフィックのみを制限する回避策を実装する必要があります。この問題の回避策は「回避策」セクションで説明されています。

Cisco 7905シリーズIP Phone

Cisco 7905 IP Phoneの脆弱性は、Bug ID CSCec77152(登録ユーザ専用)に記載されています。

Cisco ATA18xシリーズアナログテレフォニーデバイス

Cisco ATA18xデバイスの脆弱性は、Bug ID CSCea46231（登録ユーザ専用）、CSCea48726(登録ユーザ専用)、およびCSCef42352(登録ユーザ専用)に記載されています。

Cisco BTS 10200 Softswitch

Cisco BTS 10200ソフトスイッチの脆弱性は、Bug ID CSCea48755(登録ユーザ専用)に記載されています。

## 回避策

H.323エンドポイントおよびプロキシ設定の回避策

H.323を実行する必要がある該当デバイスには脆弱性が存在し、これらを保護するために使用できる特定の設定はありません。H.323トラフィックを受け入れないインターフェイスにアクセスリストを適用し、ファイアウォールを戦略的な場所に配置することで、アップグレードが実行できるまでのリスクを大幅に軽減できる可能性があります。

『Voice over IP SAFE』のホワイトペーパーでは、音声ネットワークをインターネットから隔離するためのベストプラクティスについて説明しています。これによりリスクが軽減されますが、ローカルネットワーク内からの攻撃は常に潜在的なリスクと見なす必要があります。

http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_papers_list.htm

許可されたネットワーク以外の場所からのH.323管理トラフィックをブロックするアクセスリストの例を次に示します。この例では、許可ネットワークは172.16.0.0/16です。

```
!--- Permit access from any IP address in the 172.16.0.0/16
!--- network to anywhere on port 1720.

access-list 101 permit tcp 172.16.0.0 0.0.255.255 any eq 1720

!--- Permit access from anywhere to a host in the
!--- 172.16.0.0/26 network on port 1720.

access-list 101 permit tcp any 172.16.0.0 0.0.255.255 eq 1720

!--- Deny all traffic from port 1720.
```

```
access-list 101 deny tcp any eq 1720 any

!--- Deny all traffic to port 1720.

access-list 101 deny tcp any any eq 1720

!--- Permit all other traffic.

access-list 101 permit ip any any
```

## H.323トラフィックでNATを実行するIOSデバイスの回避策

該当するバージョンの12.1または12.1Eコードが稼働し、スタティックNATを実行するように設定されているCisco IOSデバイスは、デバイスを介してNATによって処理される破損パケットによる攻撃に対して脆弱です。このような状況でリスクを軽減または削除する方法はいくつかあります。

- 外部インターフェイスのアクセスリスト
  H.323ディープパケットインスペクションは、送信元または宛先ポートが1720のパケットでのみ実行されます。これらのパケットを変換したり受け入れたりする必要がない場合は、ファイアウォールなどの外部デバイスか、NATを実行しているデバイスの外部インターフェイスに適用された入力アクセスリストによって、これらのパケットをブロックできます。

```
interface serial 0/0
 ip nat outside

 !--- This is used to indicate which interface
 !--- this configuration should be applied to.

 ip access-group 101 in
!
access-list 101 deny tcp any eq 1720 any
access-list 101 deny tcp any any eq 1720
access-list 101 permit ip any any
```

- スタティックNAT変換でポート1720トラフィックをブロックするポリシーベースルーティング
  シンプルなスタティック変換により、任意のポートでトラフィックの通過が可能です。スタティックNAT設定でH.323トラフィックを許可する必要がないものの、外部インターフェイスにアクセスリストを適用することが現実的でない場合は、ポリシーベースルーティング(PBR)を使用して、ポート1720宛てのトラフィックを再ルーティングできます。ポリシーベースルーティングはNATの前に処理されます。
  この例では、アドレス1.0.0.5は、ルータがローカルネットワークアドレスにNATを実行している外部ルーティング可能なアドレスです。

```
interface Null0
     no ip unreachables
```

```
!
interface Ethernet0/0
 ip address 10.0.0.8 255.255.255.0
 ip nat inside
!
interface Ethernet0/1
 ip address 11.0.0.8 255.255.255.0
 ip nat outside
 ip policy route-map block-h323

ip nat inside source static 10.0.0.5 1.0.0.5

access-list 102 permit tcp any host 1.0.0.5 eq 1720
access-list 102 permit tcp any eq 1720 host 1.0.0.5

route-map block-h323 permit 10
 match ip address 102
 set interface Null0
```

- ダイナミック変換を使用してポート1720をブロックする
  ダイナミック変換は、オープン変換を通過する元のフローの外部アドレスからの攻撃に対して脆弱ですが、ip nat translation port-timeout tcp 1720 2コマンドを使用すると、エクスポージャのリスクを減らすために迅速にタイムアウトすることができます。これにより、ポート1720の変換が2秒でタイムアウトし、必要なコールセットアップ要求を処理するには短すぎる可能性があります。
  NATは、アクセスリストの代わりにルートマップを使用してトラフィックを照合することにより、ポート1720を送信元または宛先とするトラフィックを変換しないように設定できます。次に示す設定例では、送信元ポートまたは宛先ポートが1720のトラフィックを除き、10.0.0.0/24ネットワークから送信されたトラフィックをNATプール「h323-test」内のアドレスに変換することを許可しています。

  注：これにより、ユーザはNetMeetingなどのPCデスクトップからH.323対応アプリケーションに対してNATを使用できなくなります。この種の回避策を適用する際には、ネットワークと、ネットワークで使用されているアプリケーションを理解することが重要です。

```
interface Ethernet0/0
 ip address 10.0.0.8 255.255.255.0
 ip nat inside
!
interface Ethernet0/1
 ip address 11.0.0.8 255.255.255.0
 ip nat outside

ip nat pool h323-test 1.0.0.5 1.0.0.15 prefix-length 24
ip nat inside source route-map h323-block pool h323-test

access-list 101 deny   tcp any any eq 1720
access-list 101 deny   tcp any eq 1720 any
access-list 101 permit ip host 10.0.0.0 0.0.0.255

route-map h323-block permit 10
```

```
        match ip address 101
```

ローカルで信頼できるホストからのH.323トラフィックを制限するためのWindowsベースのアクセスコントロールリストの定義

IPSec-H323.exeという名前の実行可能ファイルがあります。このファイルには、Microsoft Windows 2000ベースのサーバのアクセスリストの設定に役立つスクリプトが含まれています。

http://www.cisco.com/pcgi-bin/tablebuild.pl/cmva-3des?psrtdcat20e2

この回避策は、Cisco Conference Connection(CCC)とInternet Service Node(ISN)の両方で動作することがテストされており、潜在的に有害なH.323パケットをブロックします。スクリプトの詳細については、上記のリンクから入手可能なIPSec-H323-Readme.htmファイルを参照してください。

# 修正済みソフトウェア

Cisco IOS ソフトウェア

表の各行に、リリース群、および対象のプラットフォームまたは製品を示します。特定のリリーストレインに脆弱性が存在する場合は、修正を含む最初のリリースとそれぞれの提供予定日が「Rebuild」、「Interim」、および「Maintenance」の各列に表示されます。場合によっては、特定のリリースのリビルドが計画されていない場合があります。この場合、「Not scheduled」というラベルが付きます。 特定の列のリリースより前（最初の修正リリースより前）のトレインのリリースを実行しているデバイスは脆弱であることが確認されており、少なくとも示されたリリースまたは以降のバージョン（最初の修正リリースのラベルより後）にアップグレードする必要があります。

リリースを選択する際には、次の定義に注意してください。

- メンテナンス
  表の特定の行にあるラベルの、最も頻繁にテストされ、推奨されるリリース。
- リビルド
  以前のメンテナンスリリースまたはメジャーリリースから同じトレインで構築されており、特定の脆弱性に対する修正が含まれています。テストの回数は少なくなりますが、修復に必要な最小限の変更のみが含まれています。シスコでは、この脆弱性に対処するためにメイントレインのリビルドを数種類提供していますが、最新のメンテナンスリリースのみをメイントレインで実行することを強く推奨します。
- Interim
  メンテナンスリリース間で定期的に構築され、テストの頻度が少ない暫定イメージは、脆弱性に対処する適切なリリースが他にない場合にのみ選択し、可能な限り早急に次のメンテナンスリリースにアップグレードする必要があります。暫定リリースは製品としては提供されず、通常は、Cisco Technical Assistance Center（TAC）によって事前に手配されない限り

、CCO からダウンロードできません。

いずれの場合も、アップグレードする機器に十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新しいリリースで引き続き適切にサポートされていることの確認を十分に行ってください。情報が不明な場合は、次の表に示すように、Cisco TACに連絡して支援を求めてください。

注： 次の表の目的に従い、ID「Element」には、H.323エンドポイントとして動作するIOSデバイスと、プロキシが設定されたゲートキーパーに対する修正が含まれています。

| リリース群 | 脆弱性の存在するコンフィギュレーション | 修正済みリリースの入手可能性 | | |
|---|---|---|---|---|
| 10.xベースのリリース | | 脆弱性なし | | |
| 11.xベースのリリース | | リビルド | Interim | メンテナンス |
| 11.0 | | 脆弱性なし | | |
| 11.1 | | 脆弱性なし | | |
| 11.1AA | | 脆弱性なし | | |
| 11.1CA | | 脆弱性なし | | |
| 11.1CC | | 脆弱性なし | | |

| | | | | |
|---|---|---|---|---|
| 11.2 | | 脆弱性なし | | |
| 11.2P | | 脆弱性なし | | |
| 11.2SA | | 脆弱性なし | | |
| 11.3 | | 脆弱性なし | | |
| 11.3T | | 11.3(3)TでH.323機能を導入<br>Vulnerable<br>ソフトウェア修正は予定されていません<br>12.0 への移行が必要 | | |
| 12.0 ベースのリリース | | リビルド | Interim | メンテナンス |
| 12.0 | 要素 | | | 12.0(27) |
| | NAT | 脆弱性なし | | |
| | IPFW | 12.0(28) | | |
| 12.0D | | 脆弱性なし | | |
| 12.0DA | | 脆弱性なし | | |
| 12.0DC | | 脆弱性なし | | |
| 12.0S | 要素 | 2600/3600プラットフォームのみ | | 2600/3600プラットフォ |

| | | | | |
|---|---|---|---|---|
| | | 12.0(25)S1、<br>12.0(24)S2、<br>12.0(23)S3 | | ームのみ<br>12.0(26)S |
| | NAT | 脆弱性なし | | |
| | IPFW | 脆弱性なし | | |
| 12.0SC | | 脆弱性なし | | |
| 12.0SL | | 脆弱性なし | | |
| 12.0SP | | 脆弱性なし | | |
| 12.0ST | | 修正は予定されておらず、2600/3600プラットフォームのみに脆弱性が存在します。 | | |
| 12.0SX | | 脆弱性なし | | |
| 12.0SY | | 脆弱性なし | | |
| 12.0SZ | | 脆弱性なし | | |
| 12.0T | | Vulnerable.修正予定はありません。 | | |
| 12.0W5 | | 脆弱性なし | | |
| 12.0WC | | 脆弱性なし | | |
| 12.0WT | | 脆弱性なし | | |

| | | | | |
|---|---|---|---|---|
| 12.0XC | | Vulnerable.12.1(22) に移行 | | |
| 12.0XD | | Vulnerable.12.1(22) に移行 | | |
| 12.0XG | | Vulnerable.12.1(22) に移行 | | |
| 12.0XH | | Vulnerable.12.1(22) に移行 | | |
| 12.0XI | | Vulnerable.12.1(22) に移行 | | |
| 12.0XJ | | Vulnerable.12.1(22) に移行 | | |
| 12.0XK | | Vulnerable.12.2(19)bに移行 | | |
| 12.0XL | | Vulnerable.12.1(22) に移行 | | |
| 12.0XN | | Vulnerable.12.1(22) に移行 | | |
| 12.0XQ | | Vulnerable.12.1(22) に移行 | | |
| 12.0XR | | Vulnerable.12.2(19)bに移行 | | |
| 12.0XT | | Vulnerable.<br>移行パスなし | | |
| 12.1 ベースのリリース | | リビルド | Interim | メンテナンス |
| 12.1 | 要素 | | | 12.1(22) |

| | | | | |
|---|---|---|---|---|
| | NAT | | | 12.1(22) |
| | IPFW | | | 12.1(22) |
| 12.1AA | | Vulnerable.12.2(19)bに移行 | | |
| 12.1AX | | 脆弱性なし | | |
| 12.1AY | | 脆弱性なし | | |
| 12.1DA | | 脆弱性なし | | |
| 12.1DB | | 脆弱性なし | | |
| 12.1DC | | 脆弱性なし | | |
| 12.1E | 要素 | 12.1(20)E2 | | |
| | NAT | 12.1(13)E13、<br>12.1(20)E2<br>12.1(8b)E18、<br>12.1(11b)E14、<br>12.1(14)E10、<br>12.1(19)E6 - 2004年1月16日までに入手可能 | | |
| | IPFW | 12.1(8b)E16、<br>12.1(11b)E14、<br>12.1(13)E12、 | | |

| | | | | |
|---|---|---|---|---|
| | | 12.1(14)E9、<br>12.1(19)E6、<br>12.1(20)E2 | | |
| 12.1EA | | 脆弱性なし | | |
| 12.1EB | | 脆弱性なし | | |
| 12.1EC | | Vulnerable<br>移行パスなし<br>修正済みリリースなし | | |
| 12.1EV | | 脆弱性なし | | |
| 12.1EW | | 脆弱性なし | | |
| 12.1EX | | 脆弱性なし | | |
| 12.1EY | | 脆弱性なし | | |
| 12.1EZ | | Vulnerable<br>まだ移行されていません<br>再構築の予定なし | | |
| 12.1T | 要素 | 12.1(5)T17 | | 12.2(19)bに移行 |
| | NAT | 12.1(5)T17 | | 12.2(19)bに移行 |

| | | | | |
|---|---|---|---|---|
| | IPFW | 12.1(5)T17 | | 12.2(19)bに移行 |
| 12.1X(l) | 12.1Xリリースは通常、次に示すように12.1T、12.2、または12.2Tに移行します。移行パスの文書化については、具体的なトレインのテクニカルノートを参照してください。 | | | |
| 12.1XA | | Vulnerable.12.2(19)bに移行 | | |
| 12.1XB | | Vulnerable.12.2(15)T5に移行 | | |
| 12.1XC | | Vulnerable.12.2(19)bに移行 | | |
| 12.1XD | | Vulnerable.12.2(19)bに移行 | | |
| 12.1XF | | 脆弱性なし | | |
| 12.1XG | | Vulnerable.12.2(15)T5に移行 | | |
| 12.1XH | | Vulnerable.12.2(19)bに移行 | | |
| 12.1XI | | Vulnerable.12.2(19)bに移行 | | |
| 12.1XJ | | Vulnerable.12.2(15)T5に移行 | | |
| 12.1XL | | Vulnerable.12.2(15)T5に移行 | | |
| 12.1XM | | Vulnerable.12.2(2)XB15へ移行 | | |
| 12.1XP | | Vulnerable.12.2(15)T5に移行 | | |

| | | | |
|---|---|---|---|
| 12.1XQ | | Vulnerable.12.2(2)XB15へ移行 | |
| 12.1XR | | Vulnerable.12.2(15)T5に移行 | |
| 12.1XT | | Vulnerable.12.2(15)T5に移行 | |
| 12.1XU | | Vulnerable.12.2(4)T6に移行 | |
| 12.1XV | | Vulnerable.12.2(2)XB15へ移行 | |
| 12.1XW | | Vulnerable.12.2(15)T5に移行 | |
| 12.1YB | | Vulnerable.12.2(15)T5に移行 | |
| 12.1YC | | Vulnerable.12.2(15)T5に移行 | |
| 12.1YD | | Vulnerable.12.2(15)T5に移行 | |
| 12.1YE | | Vulnerable.12.2(15)T5に移行 | |
| 12.1YF | | Vulnerable.12.2(15)T5に移行 | |
| 12.1YH | | Vulnerable.12.2(15)T5に移行 | |
| 12.1YI | | Vulnerable.12.2(15)T5に移行 | |
| 12.1YJ | | 脆弱性なし | |
| 12.2 ベースのリリース | リビルド | Interim | メンテナンス |

| | | | | |
|---|---|---|---|---|
| 12.2 | 要素 | 12.2(10g)、<br>12.2(13c)、<br>12.2(16a) | | 12.2(17) |
| | NAT | 12.2(19b)<br>12.2(21a)<br>12.2(10g)、<br>12.2(13e)、<br>12.2(16f)、<br>12.2(17d):2004年1月16日までに入手可能 | | |
| | IPFW | 脆弱性なし | | |
| 12.2B | | 12.3(4)Tに移行 | | |
| 12.2BC | | 脆弱性なし | | |
| 12.2BW | | 12.2(15)T5に移行 | | 12.3(3e)に移行 |
| 12.2BX | | Vulnerable<br>移行パスなし | | |
| 12.2BZ | | 脆弱性なし | | |
| 12.2CX | | 脆弱性なし | | |
| 12.2CY | | 脆弱性なし | | |

| | | | | |
|---|---|---|---|---|
| 12.2DA | | 脆弱性なし | | |
| 12.2DD | | Vulnerable.12.3(3e)に移行 | | |
| 12.2DX | | Vulnerable.12.3(3e)に移行 | | |
| 12.2JA | | 脆弱性なし | | |
| 12.2MB | | 脆弱性なし | | |
| 12.2MC | | Vulnerable<br>リリース予定なし | | |
| 12.2MX | | Vulnerable.12.3(4)T1に移行 | | |
| 12.2S | 要素 | 12.2(14)S3 | | 12.2(18)S |
| | NAT | 12.2(14)S7（2004年2月23日に入手可能）<br>12.2(18)S3（2004年1月19日に入手可能） | | |
| | IPFW | 脆弱性なし | | |
| 12.2SX | 要素 | 12.2(17a)SXA | | |
| | NAT | 12.2(17a)SXA | | |
| | IPFW | TBD | | |

| | | | | |
|---|---|---|---|---|
| 12.2SY | | 12.2(14)SY3 | | |
| 12.2SZ | | 脆弱性なし | | |
| 12.2T | 要素 | 12.2(4)T6、<br>12.2(8)T10、<br>12.2(11)T9、<br>12.2(13)T5、<br>12.2(15)T2 | | 12.2T用のメンテナンストレインは今後予定されていません。最新の12.3メインラインリリースに移行してください。 |
| | NAT | 12.2(4)T6、<br>12.2(8)T10、<br>12.2(11)T8、<br>12.2(13)T3、<br>12.2(15)T5 | | 12.2T用のメンテナンストレインは今後予定されていません。最新の12.3メインラインリリースに移行してください。 |
| | IPFW | 12.2(4)T8 | | 12.2T用のメンテナンストレインは今後予定されていません。最新の12.3メインラインリリースに移行してくださ |

| | | | | |
|---|---|---|---|---|
| | | | | い。 |
| 12.2XA | | Vulnerable.12.2(11)T9に移行 | | |
| 12.2XB | 要素 | 12.2(2)XB14 | | |
| | NAT | 12.2(2)XB14 | | |
| | IPFW | 12.2(2)XB15 | | |
| 12.2XC | | Vulnerable.12.3(3e)に移行 | | |
| 12.2XD | | Vulnerable.12.2(15)T5に移行 | | |
| 12.2XE | | 脆弱性なし | | |
| 12.2XF | | 脆弱性なし | | |
| 12.2XG | | Vulnerable.12.2(8)T10に移行 | | |
| 12.2XH | | Vulnerable.12.2(15)T5に移行 | | |
| 12.2XI | | Vulnerable.12.2(15)T5に移行 | | |
| 12.2XJ | | Vulnerable.12.2(15)T5に移行 | | |
| 12.2XK | | Vulnerable.12.2(15)T5に移行 | | |
| 12.2XL | | Vulnerable.12.2(15)T5に移行 | | |

| | | | | |
|---|---|---|---|---|
| 12.2XM | | Vulnerable.12.2(15)T5に移行 | | |
| 12.2XN | | Vulnerable.12.2(11)T9に移行 | | |
| 12.2XQ | | Vulnerable.12.2(15)T5に移行 | | |
| 12.2XS | | Vulnerable.12.2(2)XB15へ移行 | | |
| 12.2XT | | Vulnerable.12.2(11)T9に移行 | | |
| 12.2XU | | Vulnerable.12.2(15)T5に移行 | | |
| 12.2XW | | Vulnerable.12.2(15)T5に移行 | | |
| 12.2YA | 要素 | 12.2(4)YA7 | | |
| | NAT | 脆弱性なし | | |
| | IPFW | 12.2(4)YA8 | | |
| 12.2YB | | Vulnerable.12.2(15)T5に移行 | | |
| 12.2YC | | Vulnerable.12.2(15)T5に移行 | | |
| 12.2YD | | Vulnerable.12.3(2)T3に移行 | | |
| 12.2YE | | Vulnerable.12.2(15)T5に移行 | | |
| 12.2YF | | Vulnerable.12.2(15)T5に移行 | | |

| | | |
|---|---|---|
| 12.2YG | | 脆弱性なし |
| 12.2YH | | Vulnerable.12.2(15)T5に移行 |
| 12.2YJ | | Vulnerable.12.2(15)T5に移行 |
| 12.2YK | | Vulnerable.12.2(13)ZCに移行 |
| 12.2YL | | Vulnerable.12.3(2)T3に移行 |
| 12.2YM | | Vulnerable.12.3(2)T3に移行 |
| 12.2YN | | Vulnerable.12.3(2)T3に移行 |
| 12.2YO | | 脆弱性なし |
| 12.2YP | | 脆弱性なし |
| 12.2YQ | | 脆弱性なし |
| 12.2YR | | 脆弱性なし |
| 12.2YS | | 脆弱性なし |
| 12.2YT | | Vulnerable.12.2(15)T5に移行 |
| 12.2YU | | Vulnerable.12.3(4)T1に移行 |
| 12.2YV | | Vulnerable.12.3(4)T1に移行 |

| | | | | |
|---|---|---|---|---|
| 12.2YW | 要素 | 12.2(8)YW3 | | |
| | NAT | 12.2(8)YW3 | | |
| | IPFW | 脆弱性なし | | |
| 12.2YX | | 12.2(S)リリース3に移行<br>または2004年3月12.2(14)SUに移行 | | |
| 12.2YY | | Vulnerable<br>12.3(2)T3に移行 | | |
| 12.2YZ | | Vulnerable.要求に応じてリビルドが利用可能 | | |
| 12.2ZA | | 脆弱性なし | | |
| 12.2ZB | | Vulnerable<br>12.3(2)T3に移行 | | |
| 12.2ZC | | Vulnerable<br>未計画 | | |
| 12.2ZD | | Vulnerable<br>移行パスなし<br>計画された修正はありません | | |
| 12.2ZE | | Vulnerable.12.3(3e)に移行 | | |

| | | | | |
|---|---|---|---|---|
| 12.2ZF | | Vulnerable.12.2(15)SL1に移行 | | |
| 12.2ZG | | Vulnerable<br>移行パスなし<br>計画された修正はありません | | |
| 12.2ZH | 要素 | 12.2(13)ZH3 | | |
| | NAT | | | |
| | IPFW | 脆弱性なし | | |
| 12.2ZJ | 要素 | 12.2(15)ZJ3 | | |
| | NAT | 12.2(15)ZJ2 | | |
| | IPFW | 脆弱性なし | | |
| 12.2ZL | 要素 | 12.2(15)ZL1 | | |
| | NAT | | | |
| | IPFW | 脆弱性なし | | |
| 12.2ZM | | 脆弱性なし | | |
| 12.2ZP | | 脆弱性なし | | |
| 12.3 ベースのリリース | | リビルド | Interim | メンテナンス |

| | | | | |
|---|---|---|---|---|
| 12.3 | | 脆弱性なし | | |
| 12.3T | 要素 | H.323エンドポイント/ゲートウェイ/ゲートキーパーの問題に対して脆弱でない | | |
| | NAT | 12.3(2)T3<br>12.3(4)T1 | | |
| | IPFW | IOS FWの問題に対して脆弱ではない | | |

Cisco ソフトウェア - 非IOS

すべての場合において、アップグレードするデバイスに十分なメモリが実装されており、現在のハードウェアおよびソフトウェアの構成が新しいソフトウェア リリースでも適切にサポートされていることを確認する必要があります。情報が明確でない場合は、「修正済みソフトウェアの取得」セクションに示されているように、Cisco TACに連絡して支援を求めてください。

- Cisco CallManager

| Cisco CallManager のバージョン | 最初の修正済み定期リリース |
|---|---|
| 3.1 | 3.1(4b)spD |
| 3.2 | 3.2(3) |
| 3.3 | 3.3(2)spC<br>3.3(3) |

- Cisco Conference Connection
  現在、Cisco Conference Connection(CCC)に対するソフトウェア修正は計画されていません。CCCを実行しているお客様は、信頼できるホストからのH.323トラフィックのみを制限する回避策を実装する必要があります。この問題の回避策は「回避策」セクションで説明されています。
- Cisco Internet Service Node
  現在、Cisco Internet Service Node(ISN)に対するソフトウェア修正は計画されていません。ISNを実行しているお客様は、信頼できるホストからのH.323トラフィックのみを制限する回避策を実装する必要があります。この問題の回避策は「回避策」セクションで説明されています。
- Cisco 7905シリーズIP Phone
  これらの不具合は、7905 H.323電話ファームウェアロードのバージョン1.0(1)で解決されて

います。修正を含むバージョン1.0(1)のイメージ名は、署名されたイメージの場合はcp790501001h323031212a.sbin、署名されていないイメージの場合はcp790501001h323031212a.zupです。

- Cisco ATA18xシリーズアナログテレフォニーデバイス
  これらの不具合は、ソフトウェアバージョン3.1.2で解決されています。
- Cisco BTS 10200
  Cisco BTS 10200には、バージョン4.1で利用可能なソフトウェア修正があります。BTS 10200を配備したお客様は、「修正済みソフトウェアの入手」セクションの指示に従ってTACに連絡し、修正済みソフトウェアバージョンを入手する必要があります。

## 推奨事項

$propertyAndFields.get("recommendations")

## 不正利用事例と公式発表

Cisco PSIRTでは、このアドバイザリに記載されている脆弱性のエクスプロイト事例は確認していません。

これらの脆弱性は、NISCC Vulnerability Management Team（英国政府のCERT）の協力を得て、フィンランドのオウル大学のOUSPGによって開発されたPROTOS H.323テストスイートを使用して発見されました。

これらの脆弱性は、シスコが提供していない他の製品にも存在します。また、このセキュリティアドバイザリは、影響を受ける他の組織からの発表と同時に公開されます。

## URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20040113-h323

## 改訂履歴

| | | |
|---|---|---|
| リビジョン1.4 | 2004年10月8日 | 「Cisco ATA18xシリーズアナログテレフォニーデバイス」の説明の「詳細」セクションにバグIDを追加。「Cisco ATA18xシリーズアナログテレフォニーデバイス」の説明の「ソフトウェアバージョンと修正」セクションのソフトウェアバージョンを変更。 |

| | | |
|---|---|---|
| リビジョン1.3 | 2004年1月16日 | show process cpuの構文を明確化 \| \| include CCH323コマンドを「該当製品」セクションで実行します。 |
| リビジョン1.2 | 2004年1月15日 | 「概要」および「該当製品」セクションで該当リリースの特性を明確化。12.2XB、12.0、12.1、12.2B、12.2S、および12.2EのIOSソフトウェアテーブルを更新。「回避策」セクションでIPSec-H323.exeのソフトウェアリンクを更新。 |
| リビジョン1.1 | 2004年1月14日 | 「該当製品」セクション：「AS5xxxシリーズプラットフォーム」を「IOSイメージ」に「PLUS」フィーチャセットに置き換え、「Cisco IOS Processing of H.323 Traffic」でAS5xxxプラットフォームの記載を削除、「H.323 Endpoints」セクションを更新、「Cisco IOS Processing of H.323 Traffic」セクションを更新、12.2XB、12.1E、12.0の2を0のIOSソフトウェアテーブルを更新。「12.2(19)に移行」のすべての参照を「12.2(19)Bに移行」に変更。「回避策」セクションの「ローカル信頼ホストからのH.323トラフィックを制限するWindowsベースのアクセスコントロールリストの定義」セクションを更新。「不正利用と公表」セクションの下で、「UNIRAS」の表記を「NISCC Vulnerability Management Team」に変更。 |
| リビジョン | 2004年1月13日 | 初回公開リリース |

| | | |
|---|---|---|
| 1.0 | | |

## 利用規約

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。 本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。 また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。