



Cisco Intrusion Prevention System 5.1 コマンド リファレンス



このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。見当たらない場合には、代理店にご連絡ください。

シスコが採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB (University of California, Berkeley) パブリック ドメイン パーミッションとして、UCB が開発したプログラムを最適化したものです。All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、すべてのマニュアルおよび上記各社のソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよび上記各社は、商品性や特定の目的への適合性、権利を侵害しないことに関する、または取り扱い、使用、または取り引きによって発生する、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその代理店は、このマニュアルの使用またはこのマニュアルを使用できないことによって起こる制約、利益の損失、データの損傷など間接的で偶発的に起こる特殊な損害のあらゆる可能性がシスコまたは代理店に知らされていても、それらに対する責任を一切負いません。

CCSP、CCVP、Cisco Square Bridge のロゴ、Follow Me Browsing、および StackWise は、Cisco Systems, Inc. の商標です。Changing the Way We Work, Live, Play, and Learn および iQuick Study は、Cisco Systems, Inc. のサービスマークです。Access Registrar、Aironet、ASIST、BPX、Catalyst、CCDA、CCDP、CCIE、CCIP、CCNA、CCNP、Cisco、Cisco Certified Internetwork Expert のロゴ、Cisco IOS、Cisco Press、Cisco Systems、Cisco Systems Capital、Cisco Systems のロゴ、Cisco Unity、Empowering the Internet Generation、Enterprise/Solver、EtherChannel、EtherFast、EtherSwitch、Fast Step、FormShare、GigaDrive、GigaStack、HomeLink、Internet Quotient、IOS、IP/TV、iQ Expertise、iQ のロゴ、iQ Net Readiness Scorecard、LightStream、Linksys、MeetingPlace、MGX、Networkers のロゴ、Networking Academy、Network Registrar、Packet、PIX、Post-Routing、Pre-Routing、ProConnect、RateMUX、ScriptShare、SlideCast、SMARTnet、StrataView Plus、TeleRouter、The Fastest Way to Increase Your Internet Quotient、および TransPath は、米国および一部の国における Cisco Systems, Inc. とその関連会社の登録商標です。

このマニュアルおよび Web サイトで言及されているその他の商標はすべて、それぞれの所有者のもです。「パートナー」という語の使用は、シスコと他社の提携関係を意味するものではありません。(0502R)

Cisco Intrusion Prevention System 5.1 コマンド リファレンス

Copyright © 2005 Cisco Systems, Inc.

All rights reserved.



| | |
|---|------------|
| このマニュアルについて | vii |
| 概要 | viii |
| 対象読者 | viii |
| 表記法 | ix |
| 関連資料 | x |
| 技術情報の入手方法 | x |
| Cisco.com | x |
| Product Documentation DVD (英語版) | x |
| マニュアルの発注方法 (英語版) | xi |
| シスコシステムズマニュアルセンター | xi |
| シスコ製品のセキュリティの概要 | xii |
| シスコ製品のセキュリティ問題の報告 | xii |
| テクニカル サポート | xiii |
| Cisco Technical Support & Documentation Web サイト | xiii |
| Japan TAC Web サイト | xiii |
| サービス リクエストの発行 | xiv |
| サービス リクエストのシビラティの定義 | xiv |
| その他の資料および情報の入手方法 | xv |

CHAPTER 1

| | |
|----------------|------------|
| CLI の概要 | 1-1 |
| ユーザ ロール | 1-2 |
| CLI の動作 | 1-3 |
| コマンドライン編集 | 1-5 |
| IPS コマンド モード | 1-6 |
| 正規表現の構文 | 1-7 |
| 汎用 CLI コマンド | 1-9 |
| CLI キーワード | 1-9 |

CHAPTER 2

| | |
|------------------------|------------|
| 使用可能なコマンド | 2-1 |
| banner login | 2-3 |
| clear denied-attackers | 2-4 |

| | |
|--------------------------|------|
| clear events | 2-5 |
| clear line | 2-6 |
| clock set | 2-8 |
| configure | 2-9 |
| copy | 2-10 |
| display serial | 2-13 |
| downgrade | 2-14 |
| end | 2-15 |
| erase | 2-16 |
| exit | 2-17 |
| iplog | 2-18 |
| iplog-status | 2-20 |
| more | 2-21 |
| more begin | 2-23 |
| more exclude | 2-25 |
| more include | 2-27 |
| packet | 2-28 |
| password | 2-30 |
| ping | 2-32 |
| privilege | 2-33 |
| recover | 2-34 |
| reset | 2-35 |
| service | 2-36 |
| setup | 2-39 |
| show begin | 2-45 |
| show clock | 2-47 |
| show configuration | 2-48 |
| show events | 2-48 |
| show exclude | 2-51 |
| show history | 2-53 |
| show include | 2-54 |
| show interfaces | 2-55 |
| show inventory | 2-57 |
| show privilege | 2-58 |
| show settings | 2-59 |
| show ssh authorized-keys | 2-63 |
| show ssh server-key | 2-64 |
| show ssh host-keys | 2-65 |

| | |
|------------------------|------|
| show statistics | 2-66 |
| show tech-support | 2-69 |
| show tls fingerprint | 2-71 |
| show tls trusted-hosts | 2-72 |
| show users | 2-73 |
| show version | 2-75 |
| ssh authorized-key | 2-77 |
| ssh generate-key | 2-78 |
| ssh host-key | 2-79 |
| terminal | 2-81 |
| tls generate-key | 2-82 |
| tls trusted-host | 2-83 |
| trace | 2-85 |
| upgrade | 2-86 |
| username | 2-87 |

APPENDIX A

非推奨コマンドおよびコマンドとプラットフォームの依存関係 A-1

非推奨コマンド A-2

コマンドとプラットフォームの依存関係 A-2

APPENDIX B

CLI エラー メッセージ B-1

GLOSSARY

用語集

INDEX

索引



このマニュアルについて

この章には、次の項があります。

- [概要 \(P.viii\)](#)
- [対象読者 \(P.viii\)](#)
- [表記法 \(P.ix\)](#)
- [関連資料 \(P.x\)](#)
- [技術情報の入手方法 \(P.x\)](#)
- [シスコ製品のセキュリティの概要 \(P.xii\)](#)
- [テクニカル サポート \(P.xiii\)](#)
- [その他の資料および情報の入手方法 \(P.xv\)](#)

概要

このマニュアルでは、Cisco Intrusion Prevention System 5.1 で使用可能なコマンドの参照情報について説明します。

このマニュアルは、次の章で構成されています。

- [第 1 章「CLI の概要」](#): サポートされるユーザ ロール (アカウント アクセス)、CLI の動作、コマンドライン編集、IPS CLI のモード、CLI に関連する正規表現の構文について説明します。
- [第 2 章「使用可能なコマンド」](#): コマンドのアルファベット順の一覧に続いて、各コマンドの説明 (構文説明、サポートされるモード、使用上のガイドライン、および例) を示します。
- [付録 A「非推奨コマンドおよびコマンドとプラットフォームの依存関係」](#): IPS 5.1 では推奨されなくなった前バージョンのコマンドと、特定のプラットフォームでだけ有効なコマンドの一覧を示します。
- [付録 B「CLI エラー メッセージ」](#): CLI に関連するエラー メッセージの一覧を示します。

このガイドには用語集も付属しています。用語集では、よく使用される略語と IPS に関連する専門用語が定義されています。

このガイドは、Cisco Intrusion Prevention System 5.1 に関するマニュアル セットの一部です。P.x の[「関連資料」](#)に記載されているマニュアルと併せてお読みください。

対象読者

このマニュアルは、Cisco Intrusion Prevention System (IPS) センサーを設定および管理する経験豊富なネットワーク セキュリティ管理者を対象としています。IPS には、サポートされている IPS アプリアンスおよびモジュールを含みます。

表記法

このマニュアルでは、次の表記法を使用しています。

| 項目 | 表記法 |
|--|--|
| 手順の実行中に選択する必要があるコマンド、キーワード、専門用語、およびオプション | 太字 |
| ユーザが値を指定する変数、および新しい用語や重要な用語 | イタリック体 |
| セッション情報、システム情報、パス、およびファイル名の表示出力 | <code>screen</code> フォント |
| ユーザが入力する情報 | 太字の <code>screen</code> フォント |
| ユーザが入力する変数 | イタリック体の <code>screen</code> フォント |
| メニュー項目およびボタン名 | 太字 |
| メニュー項目の選択順序 | Option > Network Preferences |



(注)

注釈です。作業を続行する前に確認すべき重要な情報や役立つ情報、このマニュアル以外の参照資料などを紹介しています。



注意

「要注意」の意味です。機器の損傷、データの損失、またはネットワークセキュリティの侵犯を予防するための注意事項が記述されています。



ヒント

ご使用の製品を有効活用するために役立つヒントを示しています。



警告

怪我、ソフトウェアの破壊、または機器の損傷を防止するために留意すべき情報を示しています。この記号がある場合、記載されている情報に従って慎重に作業しないと、明らかなセキュリティ侵犯につながります。

関連資料

下に示すマニュアルは、Cisco Intrusion Prevention System 5.1 に対応しています。次の URL からアクセスできます。

http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/tsd_products_support_series_home.html

- *Documentation Roadmap for Cisco Intrusion Prevention System 5.1*
- *Release Notes for Cisco Intrusion Prevention System 5.1*
- *Regulatory Compliance and Safety Information for the Cisco Intrusion Detection and Prevention System 4200 Series Appliance Sensor*
- *Installing and Using Cisco Intrusion Prevention System Device Manager Version 5.1*
- *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*
- *Installing Cisco Intrusion Prevention System Appliances and Modules 5.1*

技術情報の入手方法

シスコの製品マニュアルやその他の資料は、Cisco.com でご利用いただけます。また、テクニカルサポートおよびその他のリソースを、さまざまな方法で入手することができます。ここでは、シスコ製品に関する技術情報を入手する方法について説明します。

Cisco.com

次の URL から、シスコ製品の最新資料を入手することができます。

<http://www.cisco.com/techsupport>

シスコの Web サイトには、次の URL からアクセスしてください。

<http://www.cisco.com>

また、シスコの Web サイトの各国語版へは、次の URL からアクセスできます。

http://www.cisco.com/public/countries_languages.shtml

シスコ製品の最新資料の日本語版は、次の URL からアクセスしてください。

<http://www.cisco.com/jp>

Product Documentation DVD (英語版)

シスコ製品のマニュアルおよびその他の資料は、製品に付属の Product Documentation DVD パッケージでご利用いただけます。Product Documentation DVD は定期的に更新されるので、印刷資料よりも新しい情報が得られます。

Product Documentation DVD は、技術情報を包含する製品マニュアルをポータブルなメディアに格納した、包括的なライブラリです。この DVD を使用することにより、シスコ製の各ハードウェアやソフトウェアのインストール、コンフィギュレーション、およびコマンドに関する複数のバージョンのマニュアルにアクセスし、技術情報を HTML で参照できます。また、この DVD を使用すると、シスコの Web サイトで参照できるのと同じマニュアルに、インターネットに接続せずにアクセスできます。一部の製品については、PDF 版のマニュアルもご利用いただけます。

Product Documentation DVD は、1 回単位で入手することも、または定期購読することもできます。Cisco.com 登録ユーザ (Cisco Direct Customers) の場合、Ordering ツールまたは Cisco Marketplace から Product Documentation DVD (Product Number DOC-DOCDVD=) を発注できます。

Cisco Ordering ツール :

<http://www.cisco.com/en/US/partner/ordering/>

Cisco Marketplace :

<http://www.cisco.com/go/marketplace/>

マニュアルの発注方法 (英語版)

2005 年 6 月 30 日以降、Cisco.com 登録ユーザの場合、Cisco Marketplace の Product Documentation Store からシスコ製品の英文マニュアルを発注できるようになっています。次の URL にアクセスしてください。

<http://www.cisco.com/go/marketplace/>

Ordering ツールを使用したマニュアル発注も引き続きご利用いただけます。

- Cisco.com 登録ユーザ (Cisco Direct Customers) の場合、Ordering ツールから英文マニュアルを発注できます。次の URL にアクセスしてください。

<http://www.cisco.com/en/US/partner/ordering/>

- Ordering ツールを使用した英文マニュアル発注の手順については、次の URL を参照してください。

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

- Cisco.com に登録されていない場合、製品を購入された代理店へお問い合わせください。

シスコシステムズマニュアルセンター

シスコシステムズマニュアルセンターでは、シスコ製品の日本語マニュアルの最新版を PDF 形式で公開しています。また、日本語マニュアル、および日本語マニュアル CD-ROM もオンラインで発注可能です。ご希望の方は、次の URL にアクセスしてください。

<http://www2.hipri.com/cisco/>

また、シスコシステムズマニュアルセンターでは、日本語マニュアル中の誤記、誤植に関するコメントをお受けしています。次の URL の「製品マニュアル内容不良報告」をクリックすると、コメント入力画面が表示されます。

<http://www2.hipri.com/cisco/>

シスコ製品のセキュリティの概要

シスコでは、オンラインの Security Vulnerability Policy ポータル (英文のみ) を無料で提供しています。URL は次のとおりです。

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

このサイトは、次の目的に利用できます。

- シスコ製品のセキュリティ脆弱性を報告する。
- シスコ製品に伴うセキュリティ事象についてサポートを受ける。
- シスコからセキュリティ情報を受け取るための登録をする。

シスコ製品に関するセキュリティ勧告および注意事項の最新のリストには、次の URL からアクセスできます。

<http://www.cisco.com/go/psirt>

勧告および注意事項がアップデートされた時点でリアルタイムに確認する場合は、次の URL から Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) フィードにアクセスしてください。

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

シスコ製品のセキュリティ問題の報告

シスコでは、セキュアな製品を提供すべく全力を尽くしています。製品のリリース前には内部でテストを行い、すべての脆弱性を早急に修正するよう努力しています。万一、シスコ製品に脆弱性が見つかった場合は、PSIRT にご連絡ください。

- 緊急の場合 : security-alert@cisco.com (英語のみ)
緊急とは、システムがアクティブな攻撃を受けている場合、または至急の対応を要する重大なセキュリティ上の脆弱性が報告されている場合を指します。これに該当しない場合はすべて、緊急でないと見なされます。
- 緊急でない場合 : psirt@cisco.com (英語のみ)

緊急の場合は、電話で PSIRT に連絡することもできます。

- 1 877 228-7302 (英語のみ)
- 1 408 525-6532 (英語のみ)



ヒント

シスコに機密情報をお送りいただく際には、PGP (Pretty Good Privacy) または互換製品を使用して、暗号化することをお勧めします。PSIRT は、PGP バージョン 2.x から 8.x と互換性のある暗号化情報に対応しています。

無効になった、または有効期限が切れた暗号鍵は、絶対に使用しないでください。PSIRT に連絡する際に使用する正しい公開鍵には、Security Vulnerability Policy ページの Contact Summary セクションからリンクできます。次の URL にアクセスしてください。

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

このページ上のリンクからは、現在使用されている最新の PGP 鍵の ID にアクセスできます。

テクニカル サポート

Cisco Technical Support では、24 時間テクニカル サポートを提供しています。Cisco.com の Cisco Technical Support & Documentation Web サイトでは、多数のサポート リソースをオンラインで提供しています。また、シスコと正式なサービス契約を交わしているお客様には、Cisco Technical Assistance Center (TAC) のエンジニアが電話でのサポートにも対応します。シスコと正式なサービス契約を交わしていない場合は、代理店にお問い合わせください。

Cisco Technical Support & Documentation Web サイト

Cisco Technical Support & Documentation Web サイトでは、シスコ製品やシスコの技術に関するトラブルシューティングにお役立ていただけるように、オンラインでマニュアルやツールを提供しています。この Web サイトは、24 時間、いつでも利用可能です。URL は次のとおりです。

<http://www.cisco.com/techsupport>

Cisco Technical Support & Documentation Web サイトのツールにアクセスするには、Cisco.com のユーザ ID とパスワードが必要です。サービス契約が有効で、ユーザ ID またはパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

<http://tools.cisco.com/RPF/register/register.do>



(注)

Web または電話でサービス リクエストを発行する前に、Cisco Product Identification (CPI) ツールを使用して製品のシリアル番号を確認してください。CPI ツールには、Cisco Technical Support & Documentation Web サイトから、Documentation & Tools の下の **Tools & Resources** リンクをクリックするとアクセスできます。アルファベット順の索引ドロップダウン リストから **Cisco Product Identification Tool** を選択するか、Alerts & RMAs の下の **Cisco Product Identification Tool** リンクをクリックします。CPI ツールには、3 つの検索オプションがあります。製品 ID またはモデル名による検索、ツリー表示による検索、show コマンド出力のコピー アンド ペーストによる特定製品の検索です。検索結果では、製品が図示され、シリアル番号ラベルの位置が強調表示されます。ご使用の製品でシリアル番号ラベルを確認し、その情報を記録してからサービス コールをかけてください。

Japan TAC Web サイト

Japan TAC Web サイトでは、利用頻度の高い TAC Web サイト (<http://www.cisco.com/tac>) のドキュメントを日本語で提供しています。Japan TAC Web サイトには、次の URL からアクセスしてください。

<http://www.cisco.com/jp/go/tac>

サポート契約を結んでいない方は、「ゲスト」としてご登録いただくだけで、Japan TAC Web サイトのドキュメントにアクセスできます。Japan TAC Web サイトにアクセスするには、Cisco.com のログイン ID とパスワードが必要です。ログイン ID とパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

<http://www.cisco.com/jp/register>

サービス リクエストの発行

オンラインの TAC Service Request Tool を使用すると、S3 と S4 のサービス リクエストを短時間でオープンできます (S3: ネットワークに軽微な障害が発生した、S4: 製品情報が必要である)。状況を入力すると、その状況を解決するための推奨手段が検索されます。これらの推奨手段で問題を解決できない場合は、シスコのエンジニアが対応します。TAC Service Request Tool には、次の URL からアクセスできます。

<http://www.cisco.com/techsupport/servicerequest>

S1 または S2 のサービス リクエストの場合、またはインターネットにアクセスできない場合は、Cisco TAC に電話でお問い合わせください (S1: ネットワークがダウンした、S2: ネットワークの機能が著しく低下した)。S1 および S2 のサービス リクエストには、シスコのエンジニアがすぐに割り当てられ、業務を円滑に継続できるようサポートします。

Cisco TAC の連絡先については、次の URL を参照してください。

<http://www.cisco.com/techsupport/contacts>

サービス リクエストのシビラティの定義

シスコでは、報告されるサービス リクエストを標準化するために、シビラティを定義しています。

シビラティ 1 (S1): ネットワークが「ダウン」した状態か、業務に致命的な損害が発生した場合。お客様およびシスコが、24 時間体制でこの問題を解決する必要があると判断した場合。

シビラティ 2 (S2): 既存のネットワーク動作が著しく低下したか、シスコ製品が十分に機能しないため、業務に重大な影響を及ぼした場合。お客様およびシスコが、通常の業務中の全時間を費やして、この問題を解決する必要があると判断した場合。

シビラティ 3 (S3): ネットワークの動作パフォーマンスが低下しているが、ほとんどの業務運用は継続できる場合。お客様およびシスコが、業務時間中にサービスを十分なレベルにまで復旧させる必要があると判断した場合。

シビラティ 4 (S4): シスコ製品の機能、インストレーション、コンフィギュレーションについて、情報または支援が必要な場合。業務の運用には、ほとんど影響がありません。

その他の資料および情報の入手方法

シスコの製品、テクノロジー、およびネットワーク ソリューションに関する情報について、さまざまな資料をオンラインおよび印刷物で入手できます。

- Cisco Marketplace では、シスコの書籍やリファレンス ガイド、マニュアル、ロゴ製品を数多く提供しています。購入を希望される場合は、次の URL にアクセスしてください。

<http://www.cisco.com/go/marketplace/>

- Cisco Press では、ネットワーク全般、トレーニング、および認定資格に関する出版物を幅広く発行しています。これらの出版物は、初級者にも上級者にも役立ちます。Cisco Press の最新の出版情報などについては、次の URL からアクセスしてください。

<http://www.ciscopress.com>

- 『Packet』はシスコシステムズが発行する技術者向けの雑誌で、インターネットやネットワークへの投資を最大限に活用するために役立ちます。本誌は季刊誌として発行され、業界の最先端トレンド、最新テクノロジー、シスコ製品やソリューション情報が記載されています。また、ネットワーク構成およびトラブルシューティングに関するヒント、コンフィギュレーション例、カスタマー ケース スタディ、認定情報とトレーニング情報、および充実したオンラインサービスへのリンクの内容が含まれます。『Packet』には、次の URL からアクセスしてください。

<http://www.cisco.com/packet>

日本語版『Packet』は、米国版『Packet』と日本版のオリジナル記事で構成されています。日本語版『Packet』には、次の URL からアクセスしてください。

<http://www.cisco.com/japanese/warp/public/3/jp/news/packet/>

- 『iQ Magazine』はシスコシステムズの季刊誌で、成長企業が収益を上げ、業務を効率化し、サービスを拡大するためには技術をどのように利用したらよいかを学べるように構成されています。本誌では、実例とビジネス戦略を挙げて、成長企業が直面する問題とそれを解決するための技術を紹介し、読者が技術への投資に関して適切な決定を下せるよう配慮しています。『iQ Magazine』には、次の URL からアクセスしてください。

<http://www.cisco.com/go/iqmagazine>

デジタル版には、次の URL からアクセスできます。

<http://ciscoiq.texterity.com/ciscoiq/sample/>

- 『Internet Protocol Journal』は、インターネットおよびイントラネットの設計、開発、運用を担当するエンジニア向けに、シスコが発行する季刊誌です。『Internet Protocol Journal』には、次の URL からアクセスしてください。

<http://www.cisco.com/ipj>

- シスコシステムズが提供するネットワーキング製品、および各種のカスタマー サポート サービスは、次の URL から入手できます。

<http://www.cisco.com/en/US/products/index.html>

- Networking Professionals Connection は対話形式の Web サイトです。このサイトでは、ネットワーキング製品やテクノロジーに関する質問、提案、および情報をネットワーキング担当者がシスコの専門家や他のネットワーキング担当者と共に共有できます。次の URL にアクセスしてディスカッションに参加してください。

<http://www.cisco.com/discuss/networking>

- シスコは、国際的なレベルのネットワーク関連トレーニングを実施しています。最新情報については、次の URL からアクセスしてください。

<http://www.cisco.com/en/US/learning/index.html>



CLI の概要

IPS 5.1 の CLI では、Telnet、SSH、およびシリアル インターフェイス接続を使用してセンサーにアクセスできます。

この章は、次の内容で構成されています。

- [ユーザ ロール \(P.1-2\)](#)
- [CLI の動作 \(P.1-3\)](#)
- [コマンドライン編集 \(P.1-5\)](#)
- [IPS コマンド モード \(P.1-6\)](#)
- [正規表現の構文 \(P.1-7\)](#)
- [汎用 CLI コマンド \(P.1-9\)](#)
- [CLI キーワード \(P.1-9\)](#)

ユーザロール

IPS 5.1 の CLI を使用すると、複数のユーザが同時にログインできます。ローカル センサーからユーザを作成および削除することも可能です。一度に変更できるユーザ アカウントは1つだけです。各ユーザはロールに関連付けられ、そのロールによって各ユーザの変更できる範囲が制御されます。

CLI では、管理者、オペレータ、ビューア、およびサービスの4つのユーザロールがサポートされています。各ロールの権限レベルが異なるので、メニューおよび使用可能コマンドも各ロールで異なります。

- **管理者**：このユーザロールは、最高レベルの権限を持っています。管理者には無制限の表示アクセス権があり、次の機能を実行できます。
 - ユーザの追加とパスワードの割り当て
 - 物理インターフェイスおよび仮想センサーの制御の有効または無効化
 - 仮想センサーへの物理センシングインターフェイスの割り当て
 - エージェントの構成または表示時における、センサーに接続可能なホストのリストの変更
 - センサー アドレス コンフィギュレーションの変更
 - シグニチャの調整
 - 仮想センサーへのコンフィギュレーションの割り当て
 - ルータの管理
- **オペレータ**：このユーザロールには、2番目に高い権限があります。オペレータには無制限の表示アクセス権があり、次の機能を実行できます。
 - 自分のパスワードの変更
 - シグニチャの調整
 - ルータの管理
 - 仮想センサーへのコンフィギュレーションの割り当て
- **ビューア**：このユーザロールには、最低位レベルの権限があります。ビューア ユーザはコンフィギュレーションおよびイベント データを表示でき、自分のパスワードを変更できます。



ヒント モニタリングアプリケーションには、センサーに対するビューアアクセス権のみが必要です。CLI を使用してビューア権限を持つユーザ アカウントをセットアップし、その後イベント ビューアを構成してこのアカウントでセンサーに接続できます。

- **サービス**：このユーザロールには CLI への直接アクセス権はありません。サービス アカウント ユーザは、bash shell (Bourne-again shell) に直接ログインします。このアカウントは、サポートおよびトラブルシューティングの目的でのみ使用します。許可のない変更はサポートされていません。許可のない変更を行うと、適切な操作を保証するために、デバイスのイメージの再作成が必要となります。サービス ロールを持つユーザを1つだけ作成できます。

サービス アカウントにログインすると、次の警告が表示されます。

```
***** WARNING *****
UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED.
This account is intended to be used for support and troubleshooting purposes only.
Unauthorized modifications are not supported and will require this device to be
re-imaged to guarantee proper operation.
*****
```



(注) サービス ロールは、必要に応じて CLI をバイパスできる特別なロールです。管理者権限を持つユーザだけがサービス アカウントを編集できます。

CLIの動作

IPSのCLIを使用するときは、次のヒントに従ってください。

プロンプト

- CLIコマンドに表示されるプロンプトは変更できません。
- システムが質問を表示して、その答えの入力を待つ場合は、ユーザ対話型プロンプトとなります。デフォルトの入力は大カッコ[]内に表示されます。デフォルトの入力を受け入れるには、Enterキーを押します。

ヘルプ

- コマンドのヘルプを表示するには、コマンドの後に?を入力します。

次の例で、?の機能を示します。

```
sensor# configure ?
terminal      Configure from the terminal
sensor# configure
```



(注) ヘルプの表示からプロンプトに戻ると、前に入力したコマンドが?なしで表示されません。

- 不完全なトークンの後に?を入力して、コマンドを完成させる有効なトークンを参照することもできます。トークンと?の間にスペースがあると、ambiguous command エラーが表示されません。

```
sensor# show c ?
% Ambiguous command : "show c"
```

スペースなしでトークンを入力すると、それを完成させるために選択可能なトークンが表示されます(ヘルプ説明なし)。

```
sensor# show c?
clock configuration
sensor# show c
```

- 現在のモードで使用できるコマンドだけが、ヘルプで表示されます。

タブ補完

- 現在のモードで使用できるコマンドだけが、タブ補完およびヘルプで表示されます。
- コマンドの完全な構文が不明な場合は、コマンドの一部を入力してTabを押すと、コマンドを完成できます。
- タブ補完に複数のコマンドが一致する場合は、何も表示されません。

再呼び出し

- モードで入力したコマンドを再呼び出しするには、上または下矢印キーを使用するか、Ctrl+PキーまたはCtrl+Nキーを押します。



(注) ヘルプおよびタブ補完の要求は、再呼び出しリストには表示されません。

- 再呼び出しリストの最後に、ブランクのプロンプトが表示されます。

大文字小文字の区別

- CLI は大文字小文字を区別しませんが、入力と同じ大文字小文字の型でテキストをエコーバックします。たとえば、次のようになります。

```
sensor# CONF
```

Tab を押すと、センサーに次のように表示されます。

```
sensor# CONFigure
```

表示オプション

- `-More-` は、対話型プロンプトで、端末出力が割り当てられた表示スペースを超えたことを示します。残りの出力を表示するには、**スペースバー**を押して次ページの出力を表示するか、または **Enter** キーを押して一度に 1 行ずつ出力を表示します。
- 現在行の内容をクリアして、ブランクのコマンドラインに戻るには、**Ctrl+C** キーを押します。

コマンドライン編集

表 1-1 は、CLI で使用できるコマンドライン編集機能を示しています。

表 1-1 コマンドライン編集

| キー | 説明 |
|------------------|---|
| Tab | 部分的なコマンド名入力を補完します。コマンドを 1 つに特定できるところまで文字を入力して、Tab を押すと、コマンド名が補完されます。複数のコマンドを示す可能性がある文字を入力すると、警告音が鳴ってエラーが示されます。部分的なコマンドの直後 (スペースなし) に疑問符 (?) を入力してください。その文字列で始まるコマンドのリストが表示されます。 |
| Backspace | カーソルの左側の文字を消去します。 |
| Enter | コマンドラインで、Enter を押すとコマンドが処理されます。端末画面の ---More--- プロンプトで Enter キーを押すと、行が下にスクロールします。 |
| スペースバー | 端末画面で、追加の出力を表示できます。画面に ---More--- 行が表示されているときにスペースバーを押すと、次画面が表示されます。 |
| 左矢印 | カーソルを 1 文字左に移動します。1 行を超えるコマンドを入力した場合、左矢印キーを繰り返し押し続けると、システム プロンプトの方にスクロールバックし、コマンド入力の開始部分を検証できます。 |
| 右矢印 | カーソルを 1 文字右に移動します。 |
| 上矢印または Ctrl+P キー | 履歴バッファ内のコマンドを、最新のコマンドから再呼び出しします。より古いコマンドへと順に連続して再呼び出しするには、キー シーケンスを繰り返します。 |
| 下矢印または Ctrl+N キー | 上矢印または Ctrl+P キーでコマンドを再呼び出した後、履歴バッファ内のより新しいコマンドに戻ります。より新しいコマンドへと順に連続して再呼び出しするには、キー シーケンスを繰り返します。 |
| Ctrl+A | カーソルを行の先頭に移動します。 |
| Ctrl+B | カーソルを 1 文字後に移動します。 |
| Ctrl+D | カーソルの位置の文字を削除します。 |
| Ctrl+E | カーソルをコマンドラインの末尾に移動します。 |
| Ctrl+F | カーソルを 1 文字前に移動します。 |
| Ctrl+K | カーソル位置からコマンドラインの末尾までのすべての文字を削除します。 |
| Ctrl+L | 画面を消去して、システム プロンプトとコマンドラインを再表示します。 |
| Ctrl+T | カーソルの左側の文字をカーソル位置の文字で置き換えます。 |
| Ctrl+U | カーソル位置からコマンドラインの先頭までのすべての文字を削除します。 |
| Ctrl+V | コードを挿入して、直後の入力を編集キーではなく、コマンド入力として処理することをシステムに指示します。 |
| Ctrl+W | カーソルの左側の語を削除します。 |
| Ctrl+Y | 削除バッファ内の最新のエントリを再呼び出しします。削除バッファには、削除または切り取りをした最新の 10 項目が格納されています。 |
| Ctrl+Z | コンフィギュレーション モードを終了して、EXEC プロンプトに戻ります。 |
| Esc+B | カーソルを 1 語後に移動します。 |
| Esc+C | カーソル位置の語を大文字にします。 |
| Esc+D | カーソル位置から語の末尾までを削除します。 |
| Esc+F | カーソルを 1 語前に移動します。 |

表 1-1 コマンドライン編集(続き)

| キー | 説明 |
|-------|-------------------------|
| Esc+L | カーソル位置の語を小文字に変更します。 |
| Esc+U | カーソル位置から語の末尾までを大文字にします。 |

IPS コマンド モード

IPS の CLI には、次のコマンド モードがあります。

- 特権 EXEC : CLI インターフェイスにログインすると、このモードになります。
- グローバル コンフィギュレーション : 特権 EXEC モードから `configure terminal` と入力すると、このモードになります。
コマンド プロンプトは `sensor(config)#` です。
- サービス モード コンフィギュレーション : グローバル コンフィギュレーション モードから `service service-name` と入力すると、このモードになります。
コマンド プロンプトは `sensor(config-ser)#` です。ここで、`ser` はサービス名の先頭の 3 文字です。
- マルチインスタンス サービス モード : グローバル コンフィギュレーション モードから `service service-name log-instance-name` と入力すると、このモードになります。
コマンド プロンプトは `sensor(config-log)#` です。ここで、`log` はログインスタンス名の先頭の 3 文字です。システムのマルチインスタンス サービスは、シグニチャ定義とイベントアクション ルールのみです。

正規表現の構文

正規表現は、文字列の照合に使用されるテキストパターンです。正規表現には平文テキストと特殊文字が混在し、どのような照合をするかを指定します。たとえば、数字を検索する場合の正規表現は「[0-9]」です。大カッコは、比較される文字が大カッコで囲まれたいずれか1つの文字と一致することを示します。0と9の間のハイフン(-)は、0から9までの範囲であることを示します。したがって、この正規表現は0から9のいずれかの文字（つまり、数字）と一致します。

特定の特殊文字を検索するには、特殊文字の前に\記号を使用する必要があります。たとえば、単一文字の正規表現「*」は、単一のアスタリスク(*)と一致します。

この項で定義されている正規表現は、POSIX Extended Regular Expression 定義のサブセットと類似しています。特に、「[...]」および「[==]」および「[::]」表現は、サポートされていません。ただし、単一文字を表すエスケープ表現はサポートされています。文字は16進値で表現できます。たとえば、\x61は「a」に相当するため、\x61は文字「a」を表すエスケープ表現になります。

表 1-2 に、特殊文字の一覧を示します。

表 1-2 正規表現の構文

| 文字 | 説明 |
|----|---|
| ^ | 文字列の先頭。「^A」表現は、文字列の先頭でだけ「A」と一致します。 |
| ^ | 左大カッコ([)の直後。対象の文字列との照合から大カッコ内にある文字を除外します。「^[0-9]」表現は、対象文字が数字ではないことを示します。 |
| \$ | 文字列の末尾との照合。「abc\$」表現は、文字列の一部「abc」が文字列の末尾にある場合のみ一致します。 |
| | 両側の表現を対象の文字列と照合します。「a b」表現は、「a」および「b」と一致します。 |
| . | 任意の文字と一致します。 |
| * | 表現内のアスタリスクの左側にある文字が0個以上一致することを示します。 |
| + | アスタリスク(*)の場合と似ていますが、表現内の+記号の左側の文字が1つ以上一致する必要があります。 |
| ? | その左側の文字が0または1回一致します。 |
| () | パターン評価の順序に影響し、また一致した文字列の一部を別の表現に置換するとき使用されるタグ付き表現としても機能します。 |
| [] | 文字セットを囲む大カッコ([および])は、囲まれた文字のいずれかが対象の文字と一致することを示します。 |
| \ | この記号が使用されない場合に特別に解釈される文字の指定を可能にします。 \xHH は、その値が(HH)、つまり16進数値[0-9A-Fa-f]で表現される値と同じであることを示します。値はゼロ以外にする必要があります。 BELは\x07と同じで、BSは\x08、FFは\x0C、LFは\x0A、CRは\x0D、TABは\x09、そしてVTは\x0Bと同じです。 他の文字「c」の場合、「\c」は「c」と同じで、特別に解釈されることはありません。 |

次に、特殊文字の例を示します。

- a* は、任意の数の文字 a と一致します（なしも含む）
- a+ では、少なくとも1つの文字 a が一致する文字列に存在する必要があります。

- `ba?b` は、文字列 `bb` または `bab` と一致します。
- `**` は、任意の数のアスタリスク (`*`) と一致します。

複数文字のパターンの乗数を使用するには、パターンをカッコで囲みます。

- `(ab)*` は、任意の数の複数文字列 `ab` と一致します。
- `([A-Za-z][0-9])+` は 1 つ以上の英数字の組み合わせと一致します。ただし、なしは対象としません (つまり、空の文字列は一致しない)。

乗数 (`*`、`+`、または `?`) を使用した照合の順序は、最も長い指定文字列が最初になります。ネスト化された指定文字列は、外側から内側に照合されます。連結された指定文字列は、その左側から照合されます。したがって、正規表現は `A9b3` とは一致しますが、`9Ab3` とは一致しません。文字が数字の前に指定されているためです。

単一または複数文字のパターンをカッコで囲み、正規表現の別の場所で使用するパターンをソフトウェアに覚えておくように指示することもできます。

以前のパターンを再呼び出しする正規表現を作成するには、カッコを使用して特定のパターンのメモリを指定し、`\` 記号の後に数字を続けてどの記憶されたパターンを再使用するかを指定します。数字は、正規表現パターン内のカッコの出現位置を指定します。正規表現に複数の記憶されたパターンがある場合、`\1` は最初に記憶されたパターン、`\2` は 2 番目に記憶されたパターン (以降も同様) を示します。

次の正規表現は、再呼び出しにカッコを使用しています。

- `a(.)bc(.\1)\2` は、`a` とそれに続く任意の文字、その後 `bc` と任意の文字が続き、さらに最初の任意の文字が再度続き、2 番目の任意の文字が再度続きます。

たとえば、正規表現は `aZbcTZT` と一致します。最初の文字は `Z` で、2 番目の文字は `T` であることがソフトウェアで記憶され、その後 `Z` と `T` が再度、正規表現に使用されます。

汎用 CLI コマンド

次の CLI コマンドは、IPS 5.1 で汎用的に使用されます。

- **configure terminal** : グローバル コンフィギュレーション モードに入ります。
グローバル コンフィギュレーション コマンドは、1つのプロトコルやインターフェイスだけでなく、システム全体に影響を及ぼす機能に適用されます。

```
sensor# configure terminal
sensor(config)#
```

- **service** : 次のコンフィギュレーション サブモードに入ります。analysis-engine、authentication、event-action-rules、host、interface、logger、network-access、notification、signature-definition、ssh-known-hosts、trusted-certificates、および web-server。



- (注) event-action-rules サブモードと signature-definition サブモードは、マルチインスタンスサービスです。それぞれ1つの事前定義されたインスタンスのみがサポートされます。event-action-rules では、サポートされるインスタンスは rules0 だけです。signature-definition では、サポートされるインスタンスは sig0 だけです。

```
sensor# configure terminal
sensor(config)# service event-action-rules rules0
sensor(config-rul)#
```

- **end** : コンフィギュレーション モードまたは任意のコンフィギュレーション サブモードを終了します。最上位の EXEC メニューに戻ります。

```
sensor# configure terminal
sensor(config)# end
sensor#
```

- **exit** : 任意のコンフィギュレーション モードを終了、またはアクティブなターミナルセッションを閉じて、EXEC モードを終了します。直前のメニューセッションに戻ります。

```
sensor# configure terminal
sensor(config)# service event-action-rules rules0
sensor(config-rul)# exit
sensor(config)# exit
sensor#
```

CLI キーワード

一般的に、機能を無効にするには、コマンドの **no** 形式を使用します。キーワード **no** を指定しないでコマンドを使用すると、無効になっている機能を有効にできます。たとえば、`ssh host-key ipaddress` コマンドを入力すると既知のホスト テーブルにエントリが追加され、`no ssh host-key ipaddress` コマンドを入力すると既知のホスト テーブルからエントリが削除されます。そのコマンドの **no** 形式の動作の詳細については、個々のコマンドを参照してください。

サービス コンフィギュレーション コマンドには、**default** 形式も使用できます。**default** 形式のコマンドを使用すると、コマンド設定をデフォルトに戻すことができます。このキーワードは、アプリケーションのコンフィギュレーションに対して使用する **service** サブメニュー コマンドに適用されます。コマンドで **default** を指定すると、パラメータがデフォルト値にリセットされます。コマンドで **default** キーワードを指定できるのは、コンフィギュレーション ファイルにデフォルト値を指定できるコマンドのみです。



使用可能なコマンド

この章では、IPS 5.1 のコマンドをアルファベット順に示します。

次の項があります。

- [banner login \(P.2-3 \)](#)
- [clear denied-attackers \(P.2-4 \)](#)
- [clear events \(P.2-5 \)](#)
- [clear line \(P.2-6 \)](#)
- [clock set \(P.2-8 \)](#)
- [configure \(P.2-9 \)](#)
- [copy \(P.2-10 \)](#)
- [display serial \(P.2-13 \)](#)
- [downgrade \(P.2-14 \)](#)
- [end \(P.2-15 \)](#)
- [erase \(P.2-16 \)](#)
- [exit \(P.2-17 \)](#)
- [iplog \(P.2-18 \)](#)
- [iplog-status \(P.2-20 \)](#)
- [more \(P.2-21 \)](#)
- [more begin \(P.2-23 \)](#)
- [more exclude \(P.2-25 \)](#)
- [more include \(P.2-27 \)](#)
- [packet \(P.2-28 \)](#)
- [password \(P.2-30 \)](#)
- [ping \(P.2-32 \)](#)
- [privilege \(P.2-33 \)](#)
- [recover \(P.2-34 \)](#)
- [reset \(P.2-35 \)](#)
- [service \(P.2-36 \)](#)
- [setup \(P.2-39 \)](#)
- [show begin \(P.2-45 \)](#)
- [show clock \(P.2-47 \)](#)

- show configuration (P.2-48)
- show events (P.2-48)
- show exclude (P.2-51)
- show history (P.2-53)
- show include (P.2-54)
- show interfaces (P.2-55)
- show inventory (P.2-57)
- show privilege (P.2-58)
- show settings (P.2-59)
- show ssh authorized-keys (P.2-63)
- show ssh server-key (P.2-64)
- show ssh host-keys (P.2-65)
- show statistics (P.2-66)
- show tech-support (P.2-69)
- show tls fingerprint (P.2-71)
- show tls trusted-hosts (P.2-72)
- show users (P.2-73)
- show version (P.2-75)
- ssh authorized-key (P.2-77)
- ssh generate-key (P.2-78)
- ssh host-key (P.2-79)
- terminal (P.2-81)
- tls generate-key (P.2-82)
- tls trusted-host (P.2-83)
- trace (P.2-85)
- upgrade (P.2-86)
- username (P.2-87)

banner login

端末画面に表示するバナーメッセージを作成するには、グローバル コンフィギュレーション モードで **banner login** コマンドを使用します。ログイン バナーを削除するには、このコマンドの **no** 形式を使用します。バナー メッセージは、ユーザが CLI にアクセスしたときに、ユーザ名プロンプトとパスワード プロンプトの前に表示されます。

banner login

no banner login

構文説明

引数 CLI にログインする前に表示されるテキスト。メッセージの最大長は 2500 文字です。改行または疑問符(?)を入力する場合は、その前にキーストローク **Ctrl+V** を入力する必要があります。

デフォルト

デフォルトの動作または値はありません。

コマンドモード

グローバル コンフィギュレーション

サポートされるユーザロール

管理者

コマンド履歴

| リリース | 修正 |
|--------|------------|
| 5.0(1) | このコマンドを導入。 |

使用上のガイドライン

banner login コマンドによって、端末画面に表示される 2500 文字までのテキストメッセージを作成できます。このメッセージは、CLI にアクセスしたときに表示されます。**Ctrl+V** を入力してから改行または疑問符(?)を入力することによって、改行または疑問符をメッセージに含めることができます。改行は、作成したテキストメッセージでは ^M と表示されますが、ユーザに対してメッセージが表示されるときは、実際の改行として表示されます。

Message プロンプトで **Ctrl+C** を入力すると、メッセージの要求がキャンセルされます。



(注) このコマンドの形式は、Cisco IOS 12.0 の実装とは異なります。

例

次の例は、ログイン時に端末画面に表示されるメッセージを作成します。

```
sensor(config)# banner login
Banner[: This message will be displayed on login. ^M Thank you!
```

ログイン時に、次のメッセージが表示されます。

```
This message will be displayed on login.
```

```
Thank you!
password:
```

clear denied-attackers

現在の拒否 IP アドレスのリストを削除するには、特権 EXEC モードで `clear denied-attackers` を使用します。

`clear denied-attackers`

構文説明 このコマンドには、引数またはキーワードはありません。

デフォルト デフォルトの動作または値はありません。

コマンドモード EXEC

サポートされるユーザロール 管理者

| コマンド履歴 | リリース | 修正 |
|--------|--------|------------|
| | 5.0(1) | このコマンドを導入。 |

使用上のガイドライン `clear denied-attackers` コマンドによって、拒否する攻撃者のリストをクリアし、以前拒否した IP アドレスとの通信を復元できます。このリストの IP アドレスを個別に選択し、削除することはできません。拒否する攻撃者のリストをクリアすると、リストからすべての IP アドレスが削除されます。



(注) このコマンドは、Cisco IOS 12.0 以前にはありません。

例 次の例は、拒否する攻撃者のリストからすべての IP アドレスを削除します。

```
sensor# clear denied-attackers
Warning: Executing this command will delete all addresses from the list of attackers
currently being denied by the system.
Continue with clear? []: yes
sensor#
```

| 関連コマンド | コマンド | 説明 |
|--------|---|--------------------|
| | <code>show statistics denied-attackers</code> | 拒否する攻撃者のリストを表示します。 |

clear events

イベントストアをクリアするには、特権 EXEC モードで `clear events` コマンドを使用します。

`clear events`

構文説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトの動作または値はありません。

コマンドモード

EXEC

サポートされるユーザロール

管理者

コマンド履歴

| リリース | 修正 |
|--------|------------|
| 4.0(1) | このコマンドを導入。 |

使用上のガイドライン

このコマンドを使用すると、イベントストアからすべてのイベントをクリアできます。



(注) このコマンドは、Cisco IOS 12.0 以前にはありません。

例

次の例は、イベントストアをクリアします。

```
sensor# clear events
Warning: Executing this command will remove all events currently stored in the event
store.
Continue with clear? []:yes
sensor#
```

clear line

別の CLI セッションを終了するには、特権 EXEC モードで `clear line` コマンドを使用します。

```
clear line cli-id [message]
```

構文説明

| | |
|----------------------|---|
| <code>cli-id</code> | ログインセッションに関連付けられている CLI ID 番号。 <code>show users</code> コマンドを参照してください。 |
| <code>message</code> | (オプション) <code>message</code> を選択した場合、メッセージを受信するユーザに送信する内容を入力するように求めるプロンプトが表示されます。 |

デフォルト

デフォルトの動作または値はありません。

コマンドモード

EXEC

コマンド履歴

| リリース | 修正 |
|--------|------------|
| 5.0(1) | このコマンドを導入。 |

サポートされるユーザロール

管理者、オペレータ、ビューア



(注) オペレータとビューアは、現在のログインと同じユーザ名の回線のみをクリアできます。

使用上のガイドライン

`clear line` コマンドを使用して、別の回線で実行中の特定のセッションをログアウトさせます。終了しようとするログインセッションの端末に表示するメッセージ(オプション)を指定するには、`message` キーワードを使用します。Ctrl+C では要求がキャンセルされ、改行によって指定したメッセージとともに要求が送信されます。メッセージの最大長は 2550 文字です。Ctrl+V の後に改行を入力すると、メッセージテキストに改行を含めることができます。

`clear line` コマンドを使用して、サービスアカウントのログインをクリアすることはできません。



(注) `message` キーワードは、このコマンドの Cisco IOS 12.0 バージョンではサポートされていません。

例 次の例は、最大セッション数に達した後、管理者権限を持つユーザがログインしようとしたときに表示される出力を示します。

```
Error: The maximum allowed CLI sessions are currently open, would you like to
terminate one of the open sessions? [no] yes
CLI   ID      User Privilege
1253  admin1  administrator
1267  cisco   administrator
1398  test    operator

Enter the CLI ID to clear: 1253
Message: Sorry! I need access to the system, so I am terminating your session.
sensor#
```

次の例は、admin1 の端末に表示されるメッセージを示します。

```
sensor#
***
***
Termination request from Admin0
***
Sorry! I need access to the system, so I am terminating your session.
```

次の例は、最大セッション数に達した後、オペレータまたはビューア権限を持つユーザがログインしようとしたときに表示される出力を示します。

```
Error: The maximum allowed CLI sessions are currently open, please try again later.
```

関連コマンド

| コマンド | 説明 |
|------------|-------------------------------|
| show users | CLI にログインしているユーザに関する情報を表示します。 |

clock set

アプライアンスのシステム クロックを手動で設定するには、特権 EXEC モードで `clock set` コマンドを使用します。

```
clock set hh:mm[:ss] month day year
```

構文説明

| | |
|-------------------------|--------------------------|
| <code>hh:mm[:ss]</code> | 時 (24 時形式)、分、および秒形式の現在時間 |
| <code>month</code> | 現在月 (月名) |
| <code>day</code> | 月の現在日 (日) |
| <code>year</code> | 現在年 (省略なし) |

デフォルト

デフォルトの動作または値はありません。

コマンドモード

EXEC

サポートされるユーザロール

管理者

コマンド履歴

| リリース | 修正 |
|--------|------------|
| 4.0(1) | このコマンドを導入。 |

使用上のガイドライン

次の場合、システム クロックを設定する必要はありません。

- システムが、NTP または VINES クロック ソースなど、有効な外部タイミング機構と同期化されている場合
- カレンダー機能を持つルータを使用している場合

どの時刻源も使用できない場合に、`clock set` コマンドを使用します。このコマンドで指定する時間は、設定した時間帯での相対時間です。

例

次の例は、システム クロックを手動で 2002 年 7 月 29 日午後 1 時 32 分に設定します。

```
sensor# clock set 13:32 July 29 2002
sensor#
```

configure

グローバル コンフィギュレーション モードに入るには、特権 EXEC モードで `configure terminal` コマンドを使用します。

`configure terminal`

構文説明

`terminal` 端末からコンフィギュレーション コマンドを実行します。

デフォルト

デフォルトの動作または値はありません。

コマンド モード

EXEC

サポートされるユーザロール

管理者、オペレータ、ビューア

使用上のガイドライン

`configure terminal` コマンドを実行すると、グローバル コンフィギュレーション モードに入ることができます。

例

次の例は、モードを特権 EXEC モードからグローバル コンフィギュレーション モードに変更します。

```
sensor# configure terminal
sensor(config)#
```

copy

IP ログおよびコンフィギュレーション ファイルをコピーするには、特権 EXEC モードで **copy** コマンドを使用します。

```
copy [/erase] source-url destination-url
```

```
copy iplog log-id destination-url
```

構文説明

| | |
|------------------------|--|
| /erase | (オプション) コピーする前に宛先ファイルを消去します。このキーワードは現行のコンフィギュレーションだけに適用され、バックアップ コンフィギュレーションは常に上書きされます。このキーワードが宛先の現行のコンフィギュレーションに対して指定されると、ソース コンフィギュレーションがシステムのデフォルト コンフィギュレーションに適用されます。宛先の現行のコンフィギュレーションに対して指定されない場合、ソース コンフィギュレーションは現行のコンフィギュレーションとマージされます。 |
| source-url | コピーされるソース ファイルの場所。URL またはキーワードが一般的です。 |
| destination-url | コピーされる宛先ファイルの場所。URL またはキーワードが一般的です。 |
| log-id | コピーするファイルのログ ID。 iplog-status コマンドを使用して、log-id を取得します。 |

デフォルト

デフォルトの動作または値はありません。

コマンドモード

EXEC

サポートされるユーザロール

管理者、オペレータ(copy iplog または packet-file のみ) ビューア(copy iplog または packet-file のみ)

コマンド履歴

| リリース | 修正 |
|--------|------------|
| 4.0(1) | このコマンドを導入。 |

使用上のガイドライン

ソースおよび宛先 URL の正確なフォーマットは、ファイルにより異なります。次の有効なタイプがサポートされています。

| プレフィックス | ソースまたは宛先 |
|---------|---|
| ftp: | FTP ネットワーク サーバのソースまたは宛先 URL。このプレフィックスの構文は、次のとおりです。 ftp://[username@] location[/relativeDirectory]/filename ftp://[username@]location//absoluteDirectory/filename |
| scp: | SCP ネットワーク サーバのソースまたは宛先 URL。このプレフィックスの構文は、次のとおりです。 scp://[username@] location[/relativeDirectory]/filename scp://[username@] location//absoluteDirectory/filename |

| プレフィックス | ソースまたは宛先 |
|---------|--|
| http: | Web サーバのソース URL。このプレフィックスの構文は、次のとおりです。 http://[username@]location/directory/filename ソース URL のみを使用できます。 |
| https: | Web サーバのソース URL。このプレフィックスの構文は、次のとおりです。 https://[username@]location/directory/filename ソース URL のみを使用できます。 |

センサーのファイルの場所を指定するには、キーワードを使用します。次のファイルがサポートされています。

| キーワード | ソースまたは宛先 |
|----------------|--|
| current-config | 現在実行中のコンフィギュレーション。このコンフィギュレーションは、Cisco IOS 12.0 の場合と異なり、コマンドが入力されると固定になります。ファイルフォーマットは CLI コマンドです。 |
| backup-config | コンフィギュレーション バックアップの保管場所。ファイルフォーマットは CLI コマンドです。 |
| iplog | システムに組み込まれている iplog。IP ログはログ ID を基に検索されます。 iplog-status コマンドの出力を参照してください。IP ログはバイナリで保存され、ログビューアで表示されます。 |
| license-key | 加入ライセンス ファイル。 |
| packet-file | packet capture コマンドを使用してキャプチャされ、ローカルに保管されている libpcap ファイル。 |

選択したプロトコルが FTP または SCP の場合、パスワードのプロンプトが表示されます。FTP セッションにパスワードが必要でない場合は、何も入力しないで Return キーを押します。

コマンドラインですべての必要なソースおよび宛先 URL 情報とユーザ名を入力するか、または **copy** コマンドを入力して、不足している情報をセンサーからプロンプトで要求させることができます。



警告

システム センシング インターフェイスと仮想センサーのコンフィギュレーションが異なる場合、別のセンサーからコンフィギュレーション ファイルをコピーすると、エラーが発生することがあります。



(注) Cisco IOS バージョン 12.0 の **copy** コマンドはさらに柔軟性があり、異なる宛先間でコピーできます。

例 次の例は、IP アドレスが 10.1.1.1 のセンサーのディレクトリ / ファイル名 ~csidsuser/configuration/cfg から現行のコンフィギュレーションにファイルをコピーします。ディレクトリとファイルは、csidsuser のホーム アカウントからの相対パスです。

```
sensor# copy scp://csidsuser@10.1.1.1/configuration/cfg current-config
Password: *****
WARNING: Copying over the current configuration may leave the box in an unstable
state.
Would you like to copy current-config to backup-config before proceeding? [yes]:
csidsuser@10.1.1.1's password:
cfg                               100%
|*****| 36124
00:00
sensor#
```

次の例は、IP アドレスが 10.1.1.1 のセンサーのディレクトリ / ファイル名 ~csidsuser/iplog12345 に ID 12345 の iplog をコピーします。ディレクトリとファイルは、csidsuser のホーム アカウントからの相対パスです。

```
sensor# copy iplog 12345 scp://csidsuser@10.1.1.1/iplog12345
Password: *****
iplog                               100%
|*****|
36124      00:00
sensor#
```

関連コマンド

| コマンド | 説明 |
|--------------|------------------------------------|
| iplog-status | 使用可能な IP ログの内容の説明を表示します。 |
| more | 論理ファイルの内容を表示します。 |
| packet | インターフェイス上のライブトラフィックを表示またはキャプチャします。 |

display serial

すべての出力をシリアル接続に転送するには、グローバル コンフィギュレーション モードで **display serial** コマンドを使用します。 **no display-serial** コマンドを使用すると、ローカル端末への出力をリセットします。

display-serial

no display-serial

構文説明 このコマンドには、引数またはキーワードはありません。

デフォルト デフォルトの設定は、no display-serial です。

コマンドモード EXEC

サポートされるユーザロール 管理者、オペレータ

| コマンド履歴 | リリース | 修正 |
|--------|--------|------------|
| | 4.0(1) | このコマンドを導入。 |

使用上のガイドライン **display-serial** コマンドによって、ブート処理中にリモート コンソール(シリアルポートを使用)でシステムメッセージを参照できます。このオプションが有効である限り、ローカル コンソールは使用できません。シリアルポートに接続したときに、このオプションが設定されていないと、Linux が完全に起動してシリアル接続のサポートが有効になるまで、フィードバックを得られません。

例 次の例は、出力をシリアルポートにリダイレクトします。

```
sensor(config)# display-serial
sensor(config)#
```

downgrade

最新のアップグレードを削除するには、グローバル コンフィギュレーション モードで **downgrade** コマンドを使用します。

downgrade

構文説明 このコマンドには、引数またはキーワードはありません。

デフォルト デフォルトの動作または値はありません。

コマンド モード グローバル コンフィギュレーション

サポートされるユーザロール 管理者

| コマンド履歴 | リリース | 修正 |
|--------|--------|------------|
| | 4.0(1) | このコマンドを導入。 |

例 次の例は、システムから最新のアップグレードを削除します。

```
sensor(config)# downgrade
Warning: Executing this command will reboot the system and downgrade to
IDS-K9-sp-4.1-4-S91.rpm. Configuration changes made since the last upgrade will be
lost and the system may be rebooted.
Continue with downgrade?: yes
sensor#
```

downgrade コマンドが使用できない場合(たとえば、アップグレードが適用されていない場合) 次のメッセージが表示されます。

```
sensor# downgrade
Error: No downgrade available
sensor#
```

| 関連コマンド | コマンド | 説明 |
|--------|---------------------|--|
| | show version | すべてのインストール済み OS パッケージ、シグニチャ パッケージ、およびシステムで実行中の IPS プロセスのバージョン情報を表示します。 |

end

コンフィギュレーション モードまたはコンフィギュレーション サブモードを終了するには、グローバル コンフィギュレーション モードで **end** コマンドを使用します。このコマンドは、最上位の EXEC メニューに戻ります。

end

構文説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトの動作または値はありません。

コマンド モード

すべてのモード

サポートされるユーザロール

管理者、オペレータ、ビューア

コマンド履歴

| リリース | 修正 |
|--------|------------|
| 4.0(1) | このコマンドを導入。 |

例

次の例は、コンフィギュレーション モードを終了する方法を示します。

```
sensor# configure terminal
sensor(config)# end
sensor#
```

erase

論理ファイルを削除するには、特権 EXEC モードで `erase` コマンドを使用します。

```
erase { backup-config | current-config | packet-file }
```

構文説明

| | |
|-----------------------|--|
| current-config | 現在実行中のコンフィギュレーション。このコンフィギュレーションは、Cisco IOS 12.0 の場合と異なり、コマンドが入力されると固定になります。ファイルフォーマットは CLI コマンドです。 |
| backup-config | コンフィギュレーションバックアップの保管場所。ファイルフォーマットは CLI コマンドです。 |
| packet-file | packet capture コマンドを使用してキャプチャされ、ローカルに保管されている libpcap ファイル。 |

デフォルト

デフォルトの動作または値はありません。

コマンドモード

EXEC

サポートされるユーザロール

管理者

コマンド履歴

| リリース | 修正 |
|--------|------------|
| 4.0(1) | このコマンドを導入。 |

使用上のガイドライン

このコマンドの Cisco IOS 12.0 バージョンでは、ファイル システム全体を削除できます。IPS では、この概念はサポートされません。

例

次の例は、現行のコンフィギュレーション ファイルを削除してすべての設定をデフォルトに戻します。このコマンドは、センサーのリポートを必要とする場合があります。

```
sensor# erase current-config
Warning: Removing the current-config file will result in all configuration being reset
to default, including system information such as IP address.
User accounts will not be erased. They must be removed manually using the "no
username" command.
Continue? []: yes
sensor#
```

exit

コンフィギュレーション モードを終了、またはアクティブなターミナル セッションを閉じて、特権 EXEC モードを終了するには、`exit` コマンドを使用します。

`exit`

構文説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトの動作または値はありません。

コマンド モード

すべてのモード

サポートされるユーザロール

管理者、オペレータ、ビューア

コマンド履歴

| リリース | 修正 |
|--------|------------|
| 4.0(1) | このコマンドを導入。 |

使用上のガイドライン

`exit` コマンドを使用すると、直前のメニュー レベルに戻ります。中に含まれるサブモードで変更を行った場合、変更を適用するかどうかを尋ねられます。`no` を選択すると、親サブモードに戻ります。

例

次の例は、直前のメニュー レベルに戻る方法を示します。

```
sensor# configure terminal
sensor(config)# exit
sensor#
```

iplog

仮想センサーの IP ロギングを開始するには、特権 EXEC モードで **iplog** コマンドを使用します。このコマンドの **no** 形式を使用すると、仮想センサーのすべてのロギング セッション、log-id に基づく特定のロギング セッション、またはすべてのロギング セッションがディセーブルになります。

```
iplog name ip-address [ duration minutes ] [ packets numPackets ] [ bytes numBytes ]
```

```
no iplog [log-id log-id | name name ]
```

構文説明

| | |
|-------------------|--|
| <i>name</i> | ロギングを開始および終了する仮想センサー。 |
| <i>ip-address</i> | 指定された IP アドレスが含まれるログ パケットのみをロギングします。パラメータの詳細については、 setup コマンドを参照してください。 |
| <i>minutes</i> | ロギングがアクティブな期間（分単位）。有効範囲は 1 ~ 60 です。デフォルトは 10 分です。 |
| <i>numPackets</i> | ロギングするパケットの合計数。有効範囲は 0 ~ 4294967295 です。デフォルトは 1000 パケットです。値 0 は、無制限を意味します。 |
| <i>numBytes</i> | ロギングする合計バイト数。有効範囲は 0 ~ 4294967295 です。値 0 は、無制限を意味します。 |
| <i>log-id</i> | 停止するロギング セッションのログ ID。ログ ID は、 iplog-status コマンドを使用することで取得できます。 |

デフォルト

「構文説明」の表を参照してください。

コマンドモード

EXEC

サポートされるユーザロール

管理者、オペレータ

コマンド履歴

| リリース | 修正 |
|--------|------------|
| 4.0(1) | このコマンドを導入。 |

使用上のガイドライン

パラメータを設定しないでこのコマンドを **no** 形式で使用すると、すべてのロギングが停止します。期間、パケット数、およびバイト数を入力すると、ロギングは最初のイベントが発生したときに終了します。



(注) このコマンドは、Cisco IOS 12.0 以前にはありません。

例 次の例は、仮想センサー vs0 で、ソースまたは宛先アドレスに 10.2.3.1 を含むすべてのパケットのロギングを開始します。

```
sensor# iplog vs0 10.2.3.1
Logging started for virtual sensor vs0, IP address 10.2.3.1, Log ID 2342
WARNING: IP Logging will affect system performance.
sensor#
```

関連コマンド

| コマンド | 説明 |
|---------------------------|------------------------------------|
| <code>iplog-status</code> | 使用可能な IP ログの内容の説明を表示します。 |
| <code>packet</code> | インターフェイス上のライブトラフィックを表示またはキャプチャします。 |

iplog-status

使用可能な IP ログの内容の説明を表示するには、特権 EXEC モードで **iplog-status** コマンドを使用します。

iplog-status

構文説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトの動作または値はありません。

コマンドモード

EXEC

サポートされるユーザロール

管理者、オペレータ、ビューア

コマンド履歴

| リリース | 修正 |
|--------|--------------------------|
| 4.0(1) | このコマンドを導入。 |
| 4.0(2) | このコマンドに Status フィールドを追加。 |

使用上のガイドライン

ログが作成されたときのステータスは `added` です。最初のエントリがログに挿入されると、ステータスは `started` に変更されます。パケット数の上限に達するなどの条件によってログが終了すると、ステータスは `completed` に変更されます。



(注) このコマンドは、Cisco IOS 12.0 以前にはありません。

例

次の例は、すべての IP ログのステータスを表示します。

```

sensor# iplog-status
Log ID:          2425
IP Address:      10.1.1.2
Virtual Sensor:  vs0
Status:          started
Start Time:      2003/07/30 18:24:18 2002/07/30 12:24:18 CST
Packets Captured: 1039438

Log ID:          2342
IP Address:      10.2.3.1
Virtual Sensor:  vs0
Status:          completed
Event ID:        209348
Start Time:      2003/07/30 18:24:18 2002/07/30 12:24:18 CST
End Time:        2003/07/30 18:34:18 2002/07/30 12:34:18 CST
sensor#

```

関連コマンド

| コマンド | 説明 |
|--------------|------------------------|
| iplog | 仮想センサーで IP ロギングを開始します。 |

more

論理ファイルの内容を表示するには、特権 EXEC モードで **more** コマンドを使用します。

more *keyword*

構文説明

| | |
|-----------------------|--|
| current-config | 現在実行中のコンフィギュレーション。このコンフィギュレーションは、Cisco IOS 12.0 の場合と異なり、コマンドが入力されると固定になります。ファイルフォーマットは CLI コマンドです。 |
| backup-config | コンフィギュレーション バックアップの保管場所。ファイルフォーマットは CLI コマンドです。 |

デフォルト

デフォルトの動作または値はありません。

コマンドモード

EXEC

サポートされるユーザロール

管理者、オペレータ (current-config のみ)、ビューア (current-config のみ)

コマンド履歴

| リリース | 修正 |
|--------|------------|
| 4.0(1) | このコマンドを導入。 |

使用上のガイドライン

IPS では、論理ファイルのみを表示できます。

パスワードなどの非表示フィールドは、管理者の場合にのみ表示されます。



(注) Cisco IOS バージョン 12.0 のこのコマンドでは、デバイス内のさまざまなパーティションに格納されたファイルの内容を表示できます。

例

次の例は、**more** コマンドの出力を示します。

```

sensor# more current-config
! -----
! Version 5.0(0.26)
! Current configuration last modified Thu Feb 17 04:25:15 2005
! -----
display-serial
! -----
service analysis-engine
exit
! -----
service authentication
exit
! -----
service event-action-rules rules0
exit
! -----
service host
network-settings
host-ip 10.89.147.31/25,10.89.147.126
host-name sensor
access-list 0.0.0.0/0
login-banner-text This message will be displayed on user login.
exit
time-zone-settings
offset -360
--MORE--

```

関連コマンド

| コマンド | 説明 |
|---------------------|---|
| more begin | more コマンドの出力を検索し、指定した文字列が最初に出現した位置から表示します。 |
| more exclude | more コマンドの出力をフィルタ処理して、特定の正規表現を含む行を排除します。 |
| more include | more コマンドの出力をフィルタ処理して、特定の正規表現を含む行のみを表示します。 |

more begin

more コマンドの出力を検索するには、特権 EXEC モードで **more begin** コマンドを使用します。このコマンドは、指定された正規表現を含む最初の行で **more** コマンドの出力を開始します。フィルタ処理は行いません。

```
more keyword | begin regular-expression
```

構文説明

| | | |
|----------------|-----------------------|--|
| <i>keyword</i> | current-config | 現在実行中のコンフィギュレーション。このコンフィギュレーションは、Cisco IOS 12.0 の場合と異なり、コマンドが入力されると固定になります。ファイルフォーマットは CLI コマンドです。 |
| | backup-config | コンフィギュレーション バックアップの保管場所。ファイルフォーマットは CLI コマンドです。 |
| / | | 縦棒は、出力処理指定が続くことを意味します。 |
| <i>正規表現</i> | | more コマンド出力に存在する任意の正規表現。 |

デフォルト

デフォルトの動作または値はありません。

コマンドモード

EXEC

サポートされるユーザロール

管理者、オペレータ (**current-config** のみ)、ビューア (**current-config** のみ)

コマンド履歴

| リリース | 修正 |
|--------|---------------------------------------|
| 4.0(1) | このコマンドを導入。 |
| 4.0(2) | more コマンドの begin 拡張を導入。 |

使用上のガイドライン

正規表現 の引数は大文字小文字を区別し、複雑な照合の要件を指定できます。

例 次の例は、**more** コマンドの出力を検索して、正規表現「ip」以降を表示する方法を示します。

```

sensor# more current-config | begin ip
host-ip 10.89.147.31/25,10.89.147.126
host-name sensor
access-list 0.0.0.0/0
login-banner-text This message will be displayed on user login.
exit
time-zone-settings
offset -360
standard-time-zone-name CST
exit
exit
! -----
service interface
exit
! -----
service logger
exit
! -----
service network-access
user-profiles mona
enable-password foobar
exit
exit
! -----
service notification
--MORE--

```

関連コマンド

| コマンド | 説明 |
|---------------------|---|
| more exclude | more コマンドの出力をフィルタ処理して、特定の正規表現を含む行を排除します。 |
| more include | more コマンドの出力をフィルタ処理して、特定の正規表現を含む行のみを表示します。 |
| show begin | 特定の show コマンドの出力を検索し、指定した文字列が最初に出現した位置から表示します。 |
| show exclude | show コマンドの出力をフィルタ処理して、特定の正規表現を含む行を排除します。 |
| show include | show コマンドの出力をフィルタ処理して、特定の正規表現を含む行のみを表示します。 |

more exclude

more コマンドの出力をフィルタ処理して、特定の正規表現を含む行を排除するには、特権 EXEC モードで **more exclude** コマンドを使用します。

```
more keyword | exclude regular-expression
```

| | | | |
|------|----------------|-----------------------|--|
| 構文説明 | <i>keyword</i> | current-config | 現在実行中のコンフィギュレーション。このコンフィギュレーションは、Cisco IOS 12.0 の場合と異なり、コマンドが入力されると固定になります。ファイルフォーマットは CLI コマンドです。 |
| | | backup-config | コンフィギュレーション バックアップの保管場所。ファイルフォーマットは CLI コマンドです。 |
| | / | | 縦棒は、出力処理指定が続くことを意味します。 |
| | 正規表現 | | more コマンド出力に存在する任意の正規表現。 |

デフォルト デフォルトの動作または値はありません。

コマンド モード EXEC

サポートされるユーザロール 管理者、オペレータ (**current-config** のみ)、ビューア (**current-config** のみ)

| コマンド履歴 | リリース | 修正 |
|--------|--------|---|
| | 4.0(1) | このコマンドを導入。 |
| | 4.0(2) | more コマンドの exclude 拡張を追加。 |

使用上のガイドライン *正規表現* の引数は大文字小文字を区別し、複雑な照合の要件を指定できます。

例 次の例は、**more** コマンドの出力を検索して、正規表現「ip」を排除して表示する方法を示します。

```

sensor# more current-config | exclude ip
! -----
! Version 5.0(0.26)
! Current configuration last modified Thu Feb 17 04:25:15 2005
! -----
display-serial
! -----
service analysis-engine
exit
! -----
service authentication
exit
! -----
service event-action-rules rules0
exit
! -----
service host
network-settings
host-name sensor
access-list 0.0.0.0/0
login-banner-text This message will be displayed on user login.
exit
time-zone-settings
offset -360
standard-time-zone-name CST
--MORE--

```

関連コマンド

| コマンド | 説明 |
|---------------------|---|
| more begin | more コマンドの出力を検索し、指定した文字列が最初に出現した位置から表示します。 |
| more include | more コマンドの出力をフィルタ処理して、特定の正規表現を含む行のみを表示します。 |
| show begin | 特定の show コマンドの出力を検索し、指定した文字列が最初に出現した位置から表示します。 |
| show exclude | show コマンドの出力をフィルタ処理して、特定の正規表現を含む行を排除します。 |
| show include | show コマンドの出力をフィルタ処理して、特定の正規表現を含む行のみを表示します。 |

more include

more コマンドの出力をフィルタ処理して、特定の正規表現を含む行のみを表示するには、特権 EXEC モードで **more include** コマンドを使用します。

```
more keyword | include regular-expression
```

構文説明

| | | |
|----------------|-----------------------|--|
| <i>keyword</i> | current-config | 現在実行中のコンフィギュレーション。このコンフィギュレーションは、Cisco IOS 12.0 の場合と異なり、コマンドが入力されると固定になります。ファイルフォーマットは CLI コマンドです。 |
| | backup-config | コンフィギュレーション バックアップの保管場所。ファイルフォーマットは CLI コマンドです。 |
| / | | 縦棒は、出力処理指定が続くことを意味します。 |
| 正規表現 | | more コマンド出力に存在する任意の正規表現。 |

デフォルト

デフォルトの動作または値はありません。

コマンドモード

EXEC

サポートされるユーザロール

管理者、オペレータ (**current-config** のみ)、ビューア (**current-config** のみ)

コマンド履歴

| リリース | 修正 |
|--------|---|
| 4.0(1) | このコマンドを導入。 |
| 4.0(2) | more コマンドの include 拡張を追加。 |

使用上のガイドライン

正規表現の引数は大文字小文字を区別し、複雑な照合の要件を指定できます。

例

次の例は、**more** コマンドの出力を検索して、正規表現「ip」を含む行のみを表示する方法を示します。

```
sensor# more current-config | include ip
host-ip 10.89.147.31/25,10.89.147.126
sensor#
```

関連コマンド

| コマンド | 説明 |
|---------------------|---|
| more begin | more コマンドの出力を検索し、指定した文字列が最初に出現した位置から表示します。 |
| more exclude | more コマンドの出力をフィルタ処理して、特定の正規表現を含む行を排除します。 |
| show begin | 特定の show コマンドの出力を検索し、指定した文字列が最初に出現した位置から表示します。 |
| show exclude | show コマンドの出力をフィルタ処理して、特定の正規表現を含む行を排除します。 |
| show include | show コマンドの出力をフィルタ処理して、特定の正規表現を含む行のみを表示します。 |

packet

インターフェイス上のライブトラフィックを表示またはキャプチャするには、特権 EXEC モードで **packet** コマンドを使用します。**display** オプションを使用すると、ライブトラフィックまたは以前にキャプチャしたファイル出力を画面に直接ダンプできます。**capture** オプションを使用すると、libpcap の出力をローカル ファイルにキャプチャできます。ローカル ファイルの保管場所は 1 か所だけなので、後続のキャプチャ要求によって既存のファイルは上書きされます。**copy** コマンドと **packet-file** キーワードを使用して、ローカル ファイルをマシンからコピーできます。ローカル ファイルを表示するには、**display packet-file** オプションを使用します。ローカル ファイルに関する情報がある場合は、**info** オプションを使用して表示できます。

```
packet display interface-name [snaplen length] [count count] [verbose] [expression expression]
```

```
packet display packet-file [verbose] [expression expression]
```

```
packet display iplog id [verbose] [expression expression]
```

```
packet capture interface-name [snaplen length] [count count] [expression expression]
```

```
packet display file-info
```

構文説明

| | |
|-----------------------|---|
| <i>interface-name</i> | インターフェイス名、インターフェイス タイプ (GigabitEthernet、FastEthernet、Management) とその後続くスロット / ポート。システムに存在する有効なインターフェイス名のみを入力できます。 |
| <i>id</i> | 表示する既存の IP ログ ID。 |
| file-info | 保管されているパケット ファイルに関する情報を表示します。 |
| verbose | (オプション) 1 行の要約ではなく、各パケットのプロトコル ツリーを表示します。 |
| <i>length</i> | (オプション) スナップショットの長さ。デフォルトは 0 です。有効範囲は 0 ~ 1600 です。 |
| <i>count</i> | (オプション) キャプチャするパケット数。指定しない場合は、最大ファイル サイズをキャプチャすると、キャプチャは終了します。有効範囲は 1 ~ 10000 です。 |
| <i>expression</i> | (オプション) パケット キャプチャ フィルタ式。この式が tcpdump に直接渡されます。tcpdump 式の構文と一致する必要があります。 |

デフォルト

「構文説明」の表を参照してください。

コマンドモード

EXEC

サポートされるユーザロール

管理者、オペレータ、ビューア (表示のみ)

コマンド履歴

| リリース | 修正 |
|--------|------------|
| 5.0(1) | このコマンドを導入。 |

使用上のガイドライン

ストレージは、1つのローカルファイルで使用可能です。このファイルのサイズは、プラットフォームによって異なります。可能な場合、要求したパケットカウントをキャプチャする前に最大ファイルサイズに達すると、メッセージが表示されます。**packet capture interface-name** コマンドは、同時に1ユーザのみが使用できます。2番目のユーザが要求すると、キャプチャを実行しているユーザに関する情報が含まれたエラーメッセージが表示されます。インターフェイスに関わるコンフィギュレーションの変更を行うと、そのインターフェイスで実行中の **packet** コマンドが異常終了することがあります。



(注) このコマンドは、Cisco IOS 12.0 以前にはありません。



警告

このコマンドを実行すると、パフォーマンスが大幅に低下します。

ライブ表示またはファイルキャプチャを終了するには、**Ctrl+C** を押します。

式の構文については、**ethereal-filter** の **man** ページを参照してください。

file-info の表示は、次のとおりです。

Captured by: *user:id*, Cmd: *cliCmd*

Start: *yyyy/mm/dd hh:mm:ss zone*, End: *yyyy/mm/dd hh:mm:ss zone* or *in-progress*

ここで

user = キャプチャを開始したユーザのユーザ名

id = ユーザの CLI ID

cliCmd = キャプチャを実行するために入力したコマンド

例

次の例は、**fastethernet 0/0** で発生するライブトラフィックを表示します。

```
sensor# packet display fastethernet0/0
Warning This command will cause significant performance degradation.
Executing command: tethereal -i fastethernet0/0
0.000000 10.89.147.56 -> 64.101.182.20 SSH Encrypted response packet len=56
0.000262 64.101.182.20 -> 10.89.147.56 TCP 33053 > ssh [ACK] Seq=3844631470
Ack=2972370007 Win=9184 Len=0
0.029148 10.89.147.56 -> 64.101.182.20 SSH Encrypted response packet len=224
0.029450 64.101.182.20 -> 10.89.147.56 TCP 33053 > ssh [ACK] Seq=3844631470
Ack=2972370231 Win=9184 Len=0
0.030273 10.89.147.56 -> 64.101.182.20 SSH Encrypted response packet len=224
0.030575 64.101.182.20 -> 10.89.147.56 TCP 33053 > ssh [ACK] Seq=3844631470
Ack=2972370455 Win=9184 Len=0
0.031361 10.89.147.56 -> 64.101.182.20 SSH Encrypted response packet len=224
0.031666 64.101.182.20 -> 10.89.147.56 TCP 33053 > ssh [ACK] Seq=3844631470
Ack=2972370679 Win=9184 Len=0
0.032466 10.89.147.56 -> 64.101.182.20 SSH Encrypted response packet len=224
0.032761 64.101.182.20 -> 10.89.147.56 TCP 33053 > ssh [ACK]
```

次の例は、保管されているキャプチャファイルに関する情報を表示します。

```
sensor# packet display file-info
Captured by: raboyd:5292, Cmd: packet capture fastethernet0/0
Start: 2004/01/07 11:16:21 CST, End: 2004/01/07 11:20:35 CST
```

関連コマンド

| コマンド | 説明 |
|---------------------------|--------------------------|
| <code>iplog</code> | 仮想センサーで IP ログインを開始します。 |
| <code>iplog-status</code> | 使用可能な IP ログの内容の説明を表示します。 |

password

ローカル センサーのパスワードを更新するには、グローバル コンフィギュレーション モードで `password` コマンドを使用します。管理者は、`password` コマンドを使用して既存のユーザのパスワードを変更することもできます。管理者は、コマンドの `no` 形式を使用して、ユーザ アカウントをディセーブルにできます。

password

管理者用の構文：`password [name [newPassword]]`

`no password [name]`

構文説明

| | |
|-----------------|--|
| <i>name</i> | ユーザ名を指定します。有効なユーザ名の長さは 1 ~ 64 文字です。ユーザ名の先頭は、英数字にする必要があります。その他の文字には、スペース以外のすべての文字を使用できます。 |
| <i>password</i> | このコマンドを入力すると、パスワードを要求されます。ユーザのパスワードを指定します。有効なパスワードの長さは 6 ~ 32 文字です。スペースおよび「?」以外のすべての文字を使用できます。 |

デフォルト

cisco アカウントのデフォルト パスワードは cisco です。

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザロール

管理者、オペレータ（現行ユーザのパスワードのみ）、ビューア（現行ユーザのパスワードのみ）

コマンド履歴

| リリース | 修正 |
|--------|------------|
| 4.0(1) | このコマンドを導入。 |

使用上のガイドライン

`password` コマンドを使用すると、現行ユーザのログイン パスワードを更新できます。管理者は、このコマンドを使用して既存のユーザのパスワードを変更できます。この場合、管理者に現行パスワードのプロンプトは表示されません。

最後の管理者アカウントをディセーブルにしようとする、エラーが発生します。`password` コマンドを使用して、ディセーブルにしたユーザ アカウントを再びイネーブルにし、ユーザ パスワードをリセットします。

パスワードは IPS で保護されます。



(注) Cisco IOS バージョン 12.0 の password コマンドでは、パスワード行にクリア テキストで新規パスワードを入力できます。

例

次の例は、現行ユーザのパスワードの変更方法を示します。

```
sensor(config)# password
Enter Old Login Password: *****
Enter New Login Password: *****
Re-enter New Login Password: *****
sensor(config)#
```

次の例は、ユーザ `tester` のパスワードを変更します。このコマンドは、管理者のみが実行できます。

```
sensor(config)# password tester
Enter New Login Password: *****
Re-enter New Login Password: *****
sensor(config)#
```

関連コマンド

| コマンド | 説明 |
|-----------------------|----------------------|
| <code>username</code> | ローカル センサーのユーザを作成します。 |

ping

基本的なネットワーク接続を診断するには、特権 EXEC モードで **ping** コマンドを使用します。

```
ping address [count]
```

構文説明

| | |
|----------------|--|
| <i>address</i> | ping の対象のシステムの IP アドレス。 |
| <i>count</i> | 送信するエコー要求数。値を指定しない場合、4 要求が送信されます。有効範囲は、1 ~ 10000 です。 |

デフォルト

「構文説明」の表を参照してください。

コマンドモード

EXEC

コマンド履歴

| リリース | 修正 |
|--------|------------|
| 4.0(1) | このコマンドを導入。 |

サポートされるユーザロール

管理者、オペレータ、ビューア

使用上のガイドライン

このコマンドは、オペレーティング システムで用意されている **ping** コマンドを使用して実装されます。コマンドからの出力は、オペレーティング システムにより若干異なります。

例

次の例は、Solaris システムでの **ping** コマンドの出力を示します。

```
sensor# ping 10.1.1.1
PING 10.1.1.1: 32 data bytes
40 bytes from 10.1.1.1: icmp_seq=0. time=0. ms
40 bytes from 10.1.1.1: icmp_seq=1. time=0. ms
40 bytes from 10.1.1.1: icmp_seq=2. time=0. ms
40 bytes from 10.1.1.1: icmp_seq=3. time=0. ms

----10.1.1.1 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 0/0/0
sensor#
```

次の例は、Linux システムでの **ping** コマンドの出力を示します。

```
sensor# ping 10.1.1.1 2
PING 10.1.1.1 from 10.1.1.2 : 32(60) bytes of data.
40 bytes from 10.1.1.1: icmp_seq=0 ttl=255 time=0.2 ms
40 bytes from 10.1.1.1: icmp_seq=1 ttl=255 time=0.2 ms

--- 10.1.1.1 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 0.2/0.2/0.2 ms
sensor#
```

次の例は、到達不能アドレスに対する出力を示します。

```
sensor# ping 172.21.172.1
PING 172.21.172.1 (172.21.172.1) from 10.89.175.50 : 56(84) bytes of data.

--172.21.172.1 ping statistics--
5 packets transmitted, 0 packets received, 100% packet loss
sensor#
```

privilege

既存のユーザの権限レベルを変更するには、グローバルコンフィギュレーションモードで **privilege** コマンドを使用します。 **username** コマンドでユーザを作成するときに、権限を指定することもできます。

```
privilege user name [ administrator | operator | viewer ]
```

構文説明

| | |
|-------------|--|
| <i>name</i> | ユーザ名を指定します。有効なユーザ名の長さは1～64文字です。ユーザ名の先頭は、英数字にする必要があります。その他の文字には、スペース以外のすべての文字を使用できます。 |
|-------------|--|

デフォルト

デフォルトの動作または値はありません。

コマンドモード

グローバルコンフィギュレーション

サポートされるユーザロール

管理者

コマンド履歴

| リリース | 修正 |
|--------|------------|
| 4.0(1) | このコマンドを導入。 |

使用上のガイドライン

このコマンドを使用すると、ユーザの権限を変更できます。



(注) このコマンドは、Cisco IOS 12.0 以前にはありません。

例

次の例は、ユーザ「tester」の権限をオペレータに変更します。

```
sensor(config)# privilege user tester operator
Warning: The privilege change does not apply to current CLI sessions. It will be
applied to subsequent logins.
sensor(config)#
```


関連コマンド

| コマンド | 説明 |
|-----------------|---------------------|
| username | ローカルセンサーのユーザを作成します。 |

recover

回復パーティションに保存されているアプリケーション イメージでアプリケーション パーティションのイメージを再作成するには、特権 EXEC モードで **recover** コマンドを使用します。センサーは複数回リブートされて、ほとんどのコンフィギュレーション（ネットワーク パラメータ、アクセス リスト パラメータ、時間パラメータ以外）がデフォルトの設定にリセットされます。

recover application-partition

| 構文説明 | application-partition アプリケーション パーティションのイメージを再作成します。 | | | | |
|---------------|--|------|----|--------|------------|
| デフォルト | デフォルトの動作または値はありません。 | | | | |
| コマンドモード | グローバル コンフィギュレーション | | | | |
| コマンド履歴 | <table border="1"> <thead> <tr> <th>リリース</th> <th>修正</th> </tr> </thead> <tbody> <tr> <td>4.0(1)</td> <td>このコマンドを導入。</td> </tr> </tbody> </table> | リリース | 修正 | 4.0(1) | このコマンドを導入。 |
| リリース | 修正 | | | | |
| 4.0(1) | このコマンドを導入。 | | | | |
| サポートされるユーザロール | 管理者 | | | | |
| 使用上のガイドライン | <p>回復を続行する質問への有効な応答は、yes または no です。Y または N は、有効な応答ではありません。</p> <p>コマンドを実行後、すぐにシャットダウンが開始されます。シャットダウンに少し時間がかかるため、CLI コマンドへのアクセスを続行できますが（アクセスは拒否されない）、アクセスは警告なしで終了します。必要であれば、アプリケーションがシャットダウンしている間、画面にピリオド（.）を 1 秒ごとに表示して進行を示すことができます。</p> <p> (注) このコマンドは、Cisco IOS 12.0 以前にはありません。</p> | | | | |

例 次の例は、回復パーティションに保存されているバージョン 4.0(1)S29 のイメージを使用して、アプリケーション パーティションのイメージを再作成します。

```
sensor(config)# recover application-partition
Warning: Executing this command will stop all applications and re-image the node to
version 5.0(1)Sx. All configuration changes except for network settings will be reset
to default.
Continue with recovery? []:yes
Request Succeeded
sensor(config)#
```

reset

センサーで実行中のアプリケーションをシャットダウンし、アプライアンスをリブートするには、特権 EXEC モードで `reset` コマンドを使用します。`powerdown` オプションを使用した場合は、アプライアンスの電源がオフ（可能な場合）、または電源をオフにできる状態になります。

```
reset[powerdown]
```

構文説明

`powerdown` このオプションを指定すると、アプリケーションのシャットダウン後、センサーにより電源がオフになります。

デフォルト

デフォルトの動作または値はありません。

コマンドモード

EXEC

コマンド履歴

| リリース | 修正 |
|--------|------------|
| 4.0(1) | このコマンドを導入。 |

サポートされるユーザロール

管理者

使用上のガイドライン

リセットを続行する質問への有効な応答は、`yes` または `no` です。`Y` または `N` は、有効な応答ではありません。

コマンドを実行後、すぐにシャットダウンが開始されます。シャットダウン中の CLI コマンドへのアクセスは拒否されませんが、開いているセッションは、シャットダウンが完了すると同時に、警告なしに終了します。必要であれば、アプリケーションがシャットダウンしている間、画面にピリオド (.) を 1 秒ごとに表示して進行を示すことができます。



(注) このコマンドは、Cisco IOS 12.0 以前にはありません。

例

次の例は、センサーをリブートします。

```
sensor# reset
Warning: Executing this command will stop all applications and reboot the node.
Continue with reset? []:yes
sensor#
```



service

さまざまなセンサー サービスのコンフィギュレーション メニューに入るには、グローバル コンフィギュレーション モードで `service` コマンドを使用します。このコマンドの `default` 形式を使用すると、アプリケーションのコンフィギュレーション全体が、工場出荷時のデフォルトにリセットされます。

```
service { authentication | analysis-engine | event-action-rules name | host | interface | logger |
network-access | notification | signature-definition name | ssh-known-hosts | trusted-certificate |
web-server }
```

```
default service { authentication | analysis-engine | host | interface | logger | network-access |
notification | ssh-known-hosts | trusted-certificate | web-server }
```

構文説明

| | |
|-----------------------------|---|
| authentication | ユーザの認証に使用する方式の順序を設定します。 |
| analysis-engine | グローバル分析エンジン パラメータを設定します。このコンフィギュレーションによって、仮想センサーを作成し、シグニチャ定義、イベントアクション ルール、およびセンシング インターフェイスを仮想センサーに割り当てることができます。 |
| event-action-rules | イベント アクションルール コンフィギュレーションのパラメータを設定します。このコンフィギュレーションは、4.X アラーム チャネルのコンフィギュレーションを置き換えます。 |
| host | システム クロック設定、アップグレード、および IP アクセス リストを設定します。 |
| interface-config | 物理インターフェイスとインライン インターフェイスのペアを設定します。 |
| logger | デバッグ レベルを設定します。 |
| network-access | ARC に関するパラメータを設定します。 |
| |  <p>(注) Network Access Controller は、現在は Attack Response Controller (ARC) と言います。サービスは新しい名称になっていますが、変更は IPS 5.1 の CLI には反映されていません。CLI 全体にわたって <code>network-access</code> および <code>nac</code> と表示されます。</p> |
| notification | 通知アプリケーションを設定します。 |
| signature-definition | シグニチャ定義コンフィギュレーションのパラメータを設定します。 |
| ssh-known-hosts | システムの既知のホスト キーを設定します。 |
| trusted-certificate | 信頼できる認証機関の X.509 証明書のリストを設定します。 |
| web-server | Web サーバ ポートなど、Web サーバに関するパラメータを設定します。 |
| <i>name</i> | イベント アクション ルールまたはシグニチャ定義コンフィギュレーションの論理名。 |
| |  <p>(注) 有効な名前は、イベント アクションルール用の <code>rules0</code> と、シグニチャ定義用の <code>sig0</code> の 2 つだけです。</p> |

デフォルト

デフォルトの動作または値はありません。

コマンドモード グローバル コンフィギュレーション

サポートされるユーザロール 管理者、オペレータ、ビューア（表示のみ）

| コマンド履歴 | リリース | 修正 |
|--------|--------|--------------------------------------|
| | 4.0(1) | このコマンドを導入。 |
| | 5.0(1) | default キーワードを追加。通知アプリケーションのサポートを追加。 |

使用上のガイドライン このコマンドで、サービス固有のパラメータを設定できます。このコンフィギュレーションの項目とメニューはサービスによって異なり、コマンドが実行されたときにサービスから取得したコンフィギュレーションに基づいて動的に作成されます。



注意

このモードおよびその中に含まれるすべてのサブモードで行われた変更は、サービス モードを終了するときにサービスに適用されます。

コマンドモードは、コマンドプロンプトに表示されるサービス名で示されます。たとえば、service authentication では、次のプロンプトが表示されます。

```
sensor(config-aut)#
```

このコマンドは IPS 固有です。



(注) このコマンドは、Cisco IOS 12.0 以前にはありません。

service event-action-rules および service signature-definition モードでは、変数を作成し、イベントをフィルタ処理するルールを設定できます。フィルタで変数を使用する場合は、変数の前にドル記号（\$SIG1）を使用して、入力した文字列が変数であることを指定する必要があります。

複数の IP アドレスを入力する場合は、アドレスの間にカンマを使用します（スペースではありません）。IP アドレスの範囲は、A.B.C.D/b の形式で表します。ここで A.B.C.D は IP アドレスで、b は範囲を指定するために IP アドレスのマスクとなる下位ビット数です。たとえば、値 10.1.0.0/8 は、IP アドレスが 10.1.0.0 で、下位 8 ビットがマスクでオフにされ、範囲が 10.1.0.0 ~ 10.1.0.255 になります。allowPartialInput 属性が true に設定されている場合、部分 IP アドレスは IPv4 アドレスの範囲の一部として使用できます。範囲の値は包括的なので、10.2-10.3 は 10.2.0.0-10.3.255.255 と同じ値となります。範囲タイプのデータには、範囲のセットを使用することもできます。範囲のセットはカンマで区切られた複数の範囲で構成されます。たとえば、10.1.9.20-10.1.9.30,10.1.10.40-10.1.10.50,10.2-10.3 です。

コンフィギュレーションは、仮想センサーに割り当てられていない場合にだけ削除できます。



(注) このコマンドは、Cisco IOS 12.0 以前にはありません。

例

次のコマンドは、認証サービスのコンフィギュレーション モードに入ります。

```
sensor(config)# service authentication  
sensor(config-aut)#
```

次のコマンドは、分析エンジン サービスのコンフィギュレーション モードに入ります。

```
sensor(config)# service analysis-engine  
sensor(config-ana)#
```

次のコマンドは、イベント アクション ルール サービスのコンフィギュレーション モードに入ります。

```
sensor(config)# service event-action-rules rules0  
sensor(config-rul)#
```

次のコマンドは、ホスト サービスのコンフィギュレーション モードに入ります。

```
sensor(config)# service host  
sensor(config-hos)#
```

次のコマンドは、インターフェイス サービスのコンフィギュレーション モードに入ります。

```
sensor(config)# service interface  
sensor(config-int)#
```

次のコマンドは、ロギング サービスのコンフィギュレーション モードに入ります。

```
sensor(config)# service logger  
sensor(config-log)#
```

次のコマンドは、ARC サービスのコンフィギュレーション モードに入ります。

```
sensor(config)# service network-access  
sensor(config-net)#
```

次のコマンドは、SNMP 通知サービスのコンフィギュレーション モードに入ります。

```
sensor(config)# service notification  
sensor(config-not)#
```

次のコマンドは、シグニチャ定義サービスのコンフィギュレーション モードに入ります。

```
sensor(config)# service signature-definition sig0  
sensor(config-sig)#
```

次のコマンドは、SSH 既知のホスト サービスのコンフィギュレーション モードに入ります。

```
sensor(config)# service ssh-known-hosts  
sensor(config-ssh)#
```

次のコマンドは、信頼できる認証サービスのコンフィギュレーション モードに入ります。

```
sensor(config)# service trusted-certificate  
sensor(config-tru)#
```

次のコマンドは、Web サーバ サービスのコンフィギュレーション モードに入ります。

```
sensor(config)# service web-server  
sensor(config-web)#
```


setup

基本的なセンサー コンフィギュレーションを構成するには、特権 EXEC モードで **setup** コマンドを使用します。

setup

構文説明

このコマンドには、引数またはキーワードはありません。

デフォルト

hostname : sensor

IP interface : 10.1.9.201/24,10.1.9.1

telnet-server : disabled

web-server port : 443

summer time : disabled

ユーザが summer time を enabled にした場合、デフォルトは次のとおりです。

- Summertime type : Recurring
- Start Month : april
- Start Week : first
- Start Day : sunday
- Start Time : 02:00:00
- End Month : october
- End Week : last
- End Day : sunday
- End Time : 02:00:00
- Offset : 60

システムの時間帯のデフォルトは、次のとおりです。

- Timezone : UTC
- UTC Offset : 0

コマンドモード

EXEC

サポートされるユーザロール

管理者

コマンド履歴

| リリース | 修正 |
|--------|--|
| 4.0(2) | アクセス リストおよび時間設定のコンフィギュレーションを追加。 |
| 5.1(1) | インライン VLAN ペアおよび仮想センサー設定のコンフィギュレーションを追加。 |

使用上のガイドライン

setup コマンドを使用すると、システム コンソール画面に System Configuration Dialog と呼ばれる対話型ダイアログが表示されます。System Configuration Dialog によって、コンフィギュレーション プロセスの手順が示されます。

各プロンプトの横のカッコ内に示される値が、最後に設定されたデフォルト値です。

System Configuration Dialog を終了してから、項目の変更に移る必要があります。変更しない項目についてデフォルトの設定を受け入れるには、Enter を押します。

変更せず、また System Configuration Dialog を終了せずに EXEC プロンプトに戻るには、Ctrl+C を押します。

この機能には、各プロンプトに関するヘルプ テキストも用意されています。ヘルプ テキストにアクセスするには、プロンプトで疑問符 (?) を入力します。

変更が完了すると、セットアップ セッションで作成されたコンフィギュレーションが表示されます。このコンフィギュレーションを保存するかどうかを尋ねるプロンプトが表示されます。yes と入力すると、コンフィギュレーションはディスクに保存されます。no と入力すると、コンフィギュレーションは保存されず、処理が再開されます。このプロンプトに対するデフォルトはありません。yes または no と入力する必要があります。

構成可能パラメータの有効な範囲は、次のとおりです。

IP Address/Netmask/Gateway : X.X.X.X/mn,Y.Y.Y.Y。ここで、

X.X.X.X は、ピリオドで区切られた 4 オクテットの 32 ビット アドレスとしてセンサーの IP アドレスを指定します。X = 0 ~ 255 です。

mn は、ネットマスクのビット数を指定します。

Y.Y.Y.Y は、ピリオドで区切られた 4 オクテットの 32 ビット アドレスとしてデフォルト ゲートウェイを指定します。Y = 0 ~ 255 です。

Host Name : 最大 256 文字の大文字小文字を区別する文字列。数字、「_」、および「-」は有効ですが、スペースは使用できません。

システムが NTP を使用しない場合のみ、setup モードでクロック設定を入力します。NTP コマンドは、別に用意されています。

夏時間は、recurring モードまたは date モードで設定できます。recurring モードを選択した場合、開始日と終了日は、週、曜日、月、時間に基づいて入力します。date モードを選択した場合、開始日と終了日は、月、日、年、時間に基づいて入力します。disable を選択すると、夏時間がオフになります。

表 2-1 に、クロック設定パラメータを示します。

表 2-1 クロック設定パラメータ

| | |
|----------|--|
| DST zone | サマータイムが有効なときに表示される時間帯の名前。 |
| week | 週 (1 ~ 5 または last) |
| day | 曜日 (Sunday、Monday など) |
| date | 日 (1 ~ 31) |
| month | 月 (January、February など) |
| year | 年。省略なし (2001 ~ 2035) |
| hh:mm | 開始 / 終了 DST (24 時形式) の時間と分。 |
| offset | (オプション) サマータイム中に加算する時間 (分)。デフォルトは 60 です。 |
| timezone | 標準時が有効なときに表示される時間帯の名前。 |
| hours | UTC からの時間差。 |
| hh:mm:ss | 時 (24 時形式)、分、および秒形式の現在時間。 |

デフォルトの仮想センサー vs0 の編集もできます。仮想センサーに、混合 / インラインのペアとインライン VLAN のペア（または、どちらか一方）を割り当て、割り当てたインターフェイスをイネーブルにできます。セットアップが完了すると、仮想センサーはトラフィックを監視するように設定されます。

例

次の例は、**setup** コマンドと System Configuration プログラムを示します。

```
sensor# setup

--- System Configuration Dialog ---

At any point you may enter a question mark '?' for help.
User ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '['].

Current Configuration:

service host
network-settings
host-ip 172.21.172.25/8,172.21.172.1
host-name sensor
telnet-option disabled
access-list 10.0.0.0/24
access-list 172.0.0.0/24
ftp-timeout 300
login-banner-text
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option disabled
ntp-option disabled
exit
service web-server
port 443
exit
service interface
physical-interfaces GigbitEthernet0/0
admin-state enabled
exit
exit
physical-interfaces GigbitEthernet1/0
admin-state enabled
subinterface-type inline-vlan-pair
subinterface 3
description Created via setup by user cisco
vlan1 5
vlan2 6
exit
exit
exit
service analysis-engine
virtual-sensor vs0
```

```

physical-interface GigabitEthernet0/0
physical-interface GigabitEthernet1/0 subinterface-number 3
exit
exit

```

Current time: Wed May 5 10:25:35 2004

Setup Configuration last modified: Mon May 3 15:34:30 2004

```

Continue with configuration dialog?[yes]:
Enter host name[sensor]:
Enter IP interface[172.21.172.25/8,172.21.172.1]:
Enter telnet-server status[enabled]:
Enter web-server port[8080]: 80
Modify current access list? [no]: yes
Current access list entries:
  [1] 10.0.0.0/24
  [2] 172.0.0.0/24
Delete: 1
Delete:
Permit: 173.0.0.0/24
Permit:

Modify system clock settings? [no]: yes
  Use NTP? [yes] no
  Modify summer time settings? [no]: yes
    Recurring, Date or Disable[recurring]:
    Start Month[apr]:
    Start Week[1]:
    Start Day[sun]:
    Start Time[02:00:00]:
    End Month[oct]:
    End Week[last]:
    End Day[sun]:
    End Time[02:00:00]:
    DST Zone[]: CDT
    Offset[60]:
  Modify system timezone? [no]: yes
    Timezone[UTC]: CST
    GMT Offset[-360]
Modify virtual sensor "vs0" configuration?[no]: yes
Current interface configuration
  Command control: GigabitEthernet0/1
  Unused:
    GigabitEthernet1/1
    GigabitEthernet2/0
    GigabitEthernet2/1
  Promiscuous:
    GigabitEthernet0/0
  Inline:
    None
  Inline Vlan Pair:
    GigabitEthernet1/0 : 3; Vlans: 5, 6
Delete Promiscuous interfaces?[no]:
Delete Inline Vlan Pairs? [no] yes
Inline Vlan Pair Interfaces:
  [1] GigabitEthernet1/0
Interface to modify: 1
Inline Vlan Pairs for GigabitEthernet1/0:
  [1] Subinterface: 3; Vlans: 5, 6
Delete: 1
Delete:
Delete Inline Vlan Pairs?[no]:
Add Promiscuous interfaces?[no]:
Add Inline pairs?[no]: yes

```

```
Pair name: test
Description[Created via setup by user cisco]:
Interface1[]: GigabitEthernet2/0
Interface2[]: GigabitEthernet2/1
Pair name:
Add Inline Vlan Pairs?[no]: yes
Available Interfaces:
  [1] GigabitEthernet1/0
  [2] GigabitEthernet1/1
Interface to modify: 2
Inline Vlan Pairs for GigabitEthernet1/1:
  None
Subinterface number: 1
Description[Created via setup by user cisco]:
Vlan1[]: 1
Vlan2[]: 2
Subinterface number:
Add Inline Vlan Pairs?[no]:
```

The following configuration was entered.

```
service host
network-settings
host-ip 172.21.172.25/8,172.21.172.1
host-name sensor
telnet-option enabled
access-list 172.0.0.0/24
access-list 173.0.0.0/24
ftp-timeout 300
login-banner-text
exit
time-zone-settings
offset -360
standard-time-zone-name CST
exit
summertime-option recurring
offset 60
summertime-zone-name CDT
start-summertime
month april
week-of-month first
day-of-week sunday
time-of-day 02:00:00
exit
end-summertime
month october
week-of-month last
day-of-week sunday
time-of-day 02:00:00
exit
ntp-option disabled
exit
service web-server
port 80
exit
service interface
physical-interfaces GigabitEthernet0/0
admin-state enabled
exit
physical-interfaces GigabitEthernet1/1
admin-state enabled
subinterface-type inline-vlan-pair
subinterface 1
description Created via setup by user cisco
```

```
vlan1 1
vlan2 2
exit
exit
exit
physical-interfaces GigabitEthernet2/0
admin-state enabled
exit
physical-interfaces GigabitEthernet2/1
admin-state enabled
exit
inline-interfaces test
description Created via setup by user cisco
interface1 GigabitEthernet2/0
interface2 GigabitEthernet2/1
exit
exit
service analysis-engine
virtual-sensor vs0
physical-interface GigabitEthernet0/0
physical-interface GigabitEthernet1/1 subinterface-number 1
logical-interface test
exit
exit
```

```
[0] Go to the command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit.
```

```
Enter your selection [2]:
Configuration Saved.
Modify system date and time? [no] yes
  Local Date[]: 2003-01-18
  Local Time[4:33:49]: 10:33:49
System Time Updated successfully
sensor#
```

show begin

show コマンドの出力を検索するには、特権 EXEC モードで **show begin** コマンドを使用します。このコマンドは、指定された正規表現を含む最初の行で show コマンドの出力を開始します。フィルタ処理は行いません。

```
show [configuration | events | settings | tech-support] | begin regular-expression
```

構文説明

/ 縦棒は、出力処理指定が続くことを意味します。
regular-expression show コマンド出力に存在する任意の正規表現。

デフォルト

デフォルトの動作または値はありません。

コマンドモード

EXEC

サポートされるユーザロール

管理者、オペレータ (current-config のみ)、ビューア (current-config のみ)

コマンド履歴

| リリース | 修正 |
|--------|-------------------------|
| 4.0(1) | このコマンドを導入。 |
| 4.0(2) | show コマンドの begin 拡張を追加。 |
| 5.1(1) | tech-support オプションを追加。 |

使用上のガイドライン

正規表現の引数は大文字小文字を区別し、複雑な照合の要件を指定できます。

例

次の例は、正規表現「ip」から始まる出力を示します。

```
sensor# show configuration | begin ip
host-ip 10.89.147.31/25,10.89.147.126
host-name sensor
access-list 0.0.0.0/0
login-banner-text This message will be displayed on user login.
exit
time-zone-settings
offset -360
standard-time-zone-name CST
exit
exit
! -----
service interface
exit
! -----
service logger
exit
! -----
service network-access
user-profiles mona
enable-password foobar
exit
exit
! -----
service notification
--MORE--
```

■ show begin

関連コマンド

| コマンド | 説明 |
|---------------------------|---|
| <code>more begin</code> | <code>more</code> コマンドの出力を検索し、指定した文字列が最初に出現した位置から表示します。 |
| <code>more exclude</code> | <code>more</code> コマンドの出力をフィルタ処理して、特定の正規表現を含む行を排除します。 |
| <code>more include</code> | <code>more</code> コマンドの出力をフィルタ処理して、特定の正規表現を含む行のみを表示します。 |
| <code>show exclude</code> | <code>show</code> コマンドの出力をフィルタ処理して、特定の正規表現を含む行を排除します。 |
| <code>show include</code> | <code>show</code> コマンドの出力をフィルタ処理して、特定の正規表現を含む行のみを表示します。 |

show clock

システムクロックを表示するには、特権 EXEC モードで `show clock` コマンドを使用します。

```
show clock [detail]
```

構文説明

detail (オプション) クロックソース (NTP またはシステム) および現行のサマータイム設定 (設定されている場合) を示します

デフォルト

デフォルトの動作または値はありません。

コマンドモード

EXEC

サポートされるユーザロール

管理者、オペレータ、ビューア

コマンド履歴

| リリース | 修正 |
|--------|------------|
| 4.0(1) | このコマンドを導入。 |

使用上のガイドライン

システムクロックは「保証」フラグを保持して、時間が保証されるか (正確と見なされるか) どうかを示します。システムクロックが NTP などのタイミングソースで設定された場合、このフラグがセットされます。表 2-2 に保証フラグを示します。

表 2-2 保証フラグ

| 記号 | 説明 |
|--------|-------------------------|
| * | 時間は保証されない。 |
| (ブランク) | 時間は保証される。 |
| . | 時間は保証されるが、NTP は同期化されない。 |

例

次の例は、設定され、同期化された NTP を示します。

```
sensor# show clock detail
12:30:02 CST Tues Dec 19 2002
Time source is NTP
Summer time starts 03:00:00 CDT Sun Apr 7 2003
Summer time ends 01:00:00 CST Sun Oct 27 2003
sensor#
```

次の例は、時刻源が設定されていないことを示します。

```
sensor# show clock
*12:30:02 EST Tues Dec 19 2002
sensor#
```

次の例は、時刻源が設定されていないことを示します。

```
sensor# show clock detail
*12:30:02 CST Tues Dec 19 2002
No time source
Summer time starts 02:00:00 CST Sun Apr 7 2003
Summer time ends 02:00:00 CDT Sun Oct 27 2003
```

show configuration

more コマンドの `more current-config` コマンドを参照してください。

コマンド履歴


| リリース | 修正 |
|--------|------------|
| 4.0(2) | このコマンドを追加。 |

show events

ローカル イベント ログの内容を表示するには、特権 EXEC モードで `show events` コマンドを使用します。

```
show events [ { [alert [ informational ] [ low ] [ medium ] [ high ] [include-traits traits] [exclude-traits
traits] | error [ warning ] [ error ] [fatal ] | log | NAC | status } ] [hh:mm:ss [ month day [ year ] ] | past
hh:mm:ss ]
```

構文説明

| | |
|-----------------------|--|
| alert | アラートを表示します。侵入攻撃が行われている、または試みられた可能性のある動作を通知します。アラート イベントは、IPS シグニチャがネットワーク アクティビティでトリガーされると、常に分析エンジンによって生成されます。レベル(情報、低、中、高)が選択されていない場合、すべてのアラート イベントが表示されます。 |
| include-traits | 指定された <i>traits</i> のあるアラートを表示します。 |
| exclude-traits | 指定された <i>traits</i> のあるアラートを表示しません。 |
| traits | 10 進 (0 ~ 15) の特性ビット位置。 |
| error | エラー イベントを表示します。エラー イベントは、エラー条件が発生したときにサービスによって生成されます。レベル(警告、エラー、重大)が選択されていない場合、すべてのエラー イベントが表示されます。 |
| log | ログ イベントを表示します。これらのイベントは、トランザクションが受信され、アプリケーションによって応答されたときに常に生成されます。要求、応答、およびトランザクションの成功または失敗についての情報が含まれます。 |
| NAC | ARC 要求(ブロック要求)を表示します。 |
| |  <p>(注) Network Access Controller は、現在は Attack Response Controller(ARC) と言います。サービスは新しい名称になっていますが、変更は IPS 5.1 の CLI には反映されていません。CLI 全体にわたって <code>network-access</code> および <code>nac</code> と表示されます。</p> |
| status | 状況イベントを表示します。 |
| hh:mm:ss | 時(24 時形式)、分、および秒形式の開始時間。 |
| day | 月の開始日(日)。 |
| month | 開始月(月の名前)。 |
| year | 開始年(省略なし)。 |
| past | 今までに開始したイベントを表示します。 <i>hh:mm:ss</i> に表示を開始する過去の時間を指定します。 |

デフォルト デフォルトの動作または値はありません。

コマンドモード EXEC

サポートされるユーザロール 管理者、オペレータ、ビューア

| コマンド履歴 | リリース | 修正 |
|--------|--------|--|
| | 4.0(1) | このコマンドを導入。 |
| | 4.0(2) | 複数のエラー イベント レベルを同時に選択できる機能を追加。 |
| | 4.1(1) | include-traits 、 exclude-traits 、および past オプションを追加。 |

使用上のガイドライン `show events` コマンドを使用すると、要求された開始時間に始まる要求イベント タイプを表示できます。開始時間が入力されていない場合、現行時間に開始する選択されたイベントが表示されます。イベント タイプが入力されていない場合、すべてのイベントが表示されます。イベントは、ライブフィードとして表示されます。ライブフィードをキャンセルするには、**Ctrl+C** を押します。

`show events` コマンドで正規表現 | **include shunInfo** を使用すると、イベントのソース アドレスなどのブロッキング情報を表示できます。



(注) このコマンドは、Cisco IOS 12.0 以前にはありません。

例 次の例は、2004 年 12 月 25 日 10 時に開始したブロック要求を表示します。

```
sensor# show events NAC 10:00:00 Dec 25 2004
```

次の例は、現行時間に開始するエラーおよび重大エラー メッセージを表示します。

```
sensor# show events error fatal error
```

次の例は、2004 年 12 月 25 日 10 時に開始したすべてのイベントを表示します。

```
sensor# show events 10:00:00 Dec 25 2004
```

次の例は、過去 30 秒に開始したすべてのイベントを表示します。

```
sensor# show events past 00:00:30
```

次の出力は、XML コンテンツから取得されます。

```
evAlert: eventId=1025376040313262350 severity=high
  originator:
    deviceName: sensor1
    appName: sensorApp
  time: 2002/07/30 18:24:18 2002/07/30 12:24:18 CST
  signature: sigId=4500 subSigId=0 version=1.0 IOS Embedded SNMP Community Names
  participants:
    attack:
      attacker: proxy=false
      addr: 132.206.27.3
      port: 61476
    victim:
      addr: 132.202.9.254
      port: 161
  protocol: udp
```

show exclude

`show` コマンドの出力をフィルタ処理して、特定の正規表現を含む行を排除するには、特権 EXEC モードで `show exclude` コマンドを使用します。

```
show [configuration | events | settings | tech-support] | exclude regular-expression
```

構文説明

`/` 縦棒は、出力処理指定が続くことを意味します。
`regular-expression` `show` コマンド出力に存在する任意の正規表現。

デフォルト

デフォルトの動作または値はありません。

コマンドモード

EXEC

サポートされるユーザロール

管理者、オペレータ (`current-config` のみ)、ビューア (`current-config` のみ)

コマンド履歴

| リリース | 修正 |
|--------|---|
| 4.0(1) | このコマンドを導入。 |
| 4.0(2) | <code>show</code> コマンドの <code>exclude</code> 拡張を追加。 |
| 5.1(1) | <code>tech-support</code> オプションを追加。 |

使用上のガイドライン

正規表現の引数は大文字小文字を区別し、複雑な照合の要件を指定できます。

例

次の例は、正規表現「ip」を排除した出力を示します。

```
sensor# show configuration | exclude ip
! -----
! Version 5.0(0.26)
! Current configuration last modified Thu Feb 17 04:25:15 2005
! -----
display-serial
! -----
service analysis-engine
exit
! -----
service authentication
exit
! -----
service event-action-rules rules0
exit
! -----
service host
network-settings
host-name sensor
access-list 0.0.0.0/0
login-banner-text This message will be displayed on user login.
exit
time-zone-settings
offset -360
standard-time-zone-name CST
--MORE--
```

関連コマンド

| コマンド | 説明 |
|---------------------------|---|
| <code>more begin</code> | <code>more</code> コマンドの出力を検索し、指定した文字列が最初に出現した位置から表示します。 |
| <code>more exclude</code> | <code>more</code> コマンドの出力をフィルタ処理して、特定の正規表現を含む行を排除します。 |
| <code>more include</code> | <code>more</code> コマンドの出力をフィルタ処理して、特定の正規表現を含む行のみを表示します。 |
| <code>show begin</code> | 特定の <code>show</code> コマンドの出力を検索し、指定した文字列が最初に出現した位置から表示します。 |
| <code>show include</code> | <code>show</code> コマンドの出力をフィルタ処理して、特定の正規表現を含む行のみを表示します。 |

show history

現行のメニューで入力したコマンドのリストを表示するには、すべてのモードで **show history** コマンドを使用します。

```
show history
```

構文説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトの動作または値はありません。

コマンドモード

すべてのモード

サポートされるユーザロール

管理者、オペレータ、ビューア

コマンド履歴

| リリース | 修正 |
|--------|------------|
| 4.0(1) | このコマンドを導入。 |

使用上のガイドライン

show history コマンドでは、現行メニューで入力したコマンドの記録が表示されます。履歴バッファに記録されるコマンド数は 50 です。

例

次の例は、**show history** コマンドで表示されるコマンドの記録を示します。

```
sensor# show history
show users
show events
sensor#
```

show include

show コマンドの出力をフィルタ処理して、特定の正規表現を含む行のみを表示するには、特権 EXEC モードで show include コマンドを使用します。

```
show [ configuration | events | settings | tech-support ] | include regular-expression
```

構文説明

| | |
|--------------------|--------------------------|
| / | 縦棒は、出力処理指定が続くことを意味します。 |
| regular-expression | show コマンド出力に存在する任意の正規表現。 |

デフォルト

デフォルトの動作または値はありません。

コマンドモード

EXEC

サポートされるユーザロール

管理者、オペレータ (current-config のみ)、ビューア (current-config のみ)

コマンド履歴

| リリース | 修正 |
|--------|---------------------------|
| 4.0(1) | このコマンドを導入。 |
| 4.0(2) | show コマンドの include 拡張を追加。 |
| 5.1(1) | tech-support オプションを追加。 |

使用上のガイドライン

正規表現の引数は大文字小文字を区別し、複雑な照合の要件を指定できます。

show settings コマンドの出力では、照合要求のヘッダー情報も表示され、照合コンテキストを判別できます。

例

次の例は、正規表現「ip」を含む行のみの出力を示します。

```
sensor# show configuration | include ip
host-ip 10.89.147.31/25,10.89.147.126
sensor#
```

関連コマンド

| コマンド | 説明 |
|--------------|--|
| more begin | more コマンドの出力を検索し、指定した文字列が最初に出現した位置から表示します。 |
| more exclude | more コマンドの出力をフィルタ処理して、特定の正規表現を含む行を排除します。 |
| more include | more コマンドの出力をフィルタ処理して、特定の正規表現を含む行のみを表示します。 |
| show begin | 特定の show コマンドの出力を検索し、指定した文字列が最初に出現した位置から表示します。 |
| show exclude | show コマンドの出力をフィルタ処理して、特定の正規表現を含む行を排除します。 |


show interfaces

すべてのシステム インターフェイスの統計情報を表示するには、特権 EXEC モードで `show interfaces` コマンドを使用します。このコマンドでは、`show interfaces management`、`show interfaces fastethernet`、および `show interfaces gigabitethernet` を表示します。

```
show interfaces [clear]
```

```
show interfaces {FastEthernet | GigabitEthernet | Management} [slot/port]
```

構文説明

| | |
|------------------------------|--|
| <code>clear</code> | 診断をクリアします。 |
| <code>FastEthernet</code> | FastEthernet インターフェイスの統計情報を表示します。 |
| <code>GigabitEthernet</code> | GigabitEthernet インターフェイスの統計情報を表示します。 |
| <code>Management</code> | Management インターフェイスの統計情報を表示します。 |
| |  (注) このキーワードは、Management とマークされた外部ポートを持つプラットフォームでのみサポートされます。その他のプラットフォームの管理インターフェイスは、インターフェイスの種類（通常、FastEthernet）に基づいて、 <code>show interfaces</code> の出力で表示されます。 |
| <code>slot/port</code> | スロットとポートの情報については、適切なハードウェア マニュアルを参照してください。 |

デフォルト

デフォルトの動作または値はありません。

コマンド モード

EXEC

サポートされるユーザロール

管理者、オペレータ、ビューア

コマンド履歴

| リリース | 修正 |
|--------|--|
| 5.0(1) | <code>show interfaces group</code> 、 <code>show interfaces sensing</code> 、および <code>show interfaces command-control</code> を削除。 |

使用上のガイドライン

このコマンドは、コマンド、コントロール、およびセンシング インターフェイスに関する統計情報を表示します。clear オプションで統計情報をクリアしてリセットすることもできます。

例

次の例は、インターフェイス統計情報を示します。

```
sensor# show interfaces
Interface Statistics
  Total Packets Received = 0
  Total Bytes Received = 0
  Missed Packet Percentage = 0
  Current Bypass Mode = Auto_off
MAC statistics from interface GigabitEthernet0/0
  Media Type = TX
  Missed Packet Percentage = 0
  Inline Mode = Unpaired
  Pair Status = N/A
  Link Status = Down
  Link Speed = N/A
  Link Duplex = N/A
  Total Packets Received = 0
  Total Bytes Received = 0
  Total Multicast Packets Received = 0
  Total Broadcast Packets Received = 0
  Total Jumbo Packets Received = 0
  Total Undersize Packets Received = 0
  Total Receive Errors = 0
  Total Receive FIFO Overruns = 0
  Total Packets Transmitted = 0
  Total Bytes Transmitted = 0
  Total Multicast Packets Transmitted = 0
--MORE--
```

show inventory

PEP 情報を表示するには、特権 EXEC モードで `show inventory` コマンドを使用します。このコマンドは、センサーの PID、VID および SN で構成された UDI 情報を表示します。

```
show inventory
```

構文説明 このコマンドには、引数またはキーワードはありません。

デフォルト デフォルトの動作または値はありません。

コマンドモード EXEC

サポートされるユーザロール 管理者、オペレータ、ビューア

| コマンド履歴 | リリース | 修正 |
|--------|--------|------------|
| | 5.0(1) | このコマンドを導入。 |

使用上のガイドライン これは、Cisco PEP ポリシーで要求される `show inventory` Cisco IOS コマンドと同じです。`show inventory` の出力は、ハードウェアによって異なります。

例 次の例は、`show inventory` コマンドの出力例を示します。

```
sensor# show inventory
NAME: "Chassis", DESCR: "Chasis-4240"
PID: 4240-515E , VID: V04, SN: 639156

NAME: "slot 0", DESCR: "4 port I/O card"
PID: 4240-4IOE , VID: V04, SN: 4356785466
sensor#
```

show privilege

現行の権限レベルを表示するには、特権 EXEC モードで `show privilege` コマンドを使用します。

```
show privilege
```

構文説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトの動作または値はありません。

コマンドモード

EXEC

サポートされるユーザロール

管理者、オペレータ、ビューア

コマンド履歴

| リリース | 修正 |
|--------|------------|
| 4.0(1) | このコマンドを導入。 |

使用上のガイドライン

このコマンドを使用して、現行の権限レベルを表示します。権限レベルは、管理者だけが変更できます。詳細については、`username` コマンドを参照してください。

例

次の例は、ユーザの権限を示します。

```
sensor# show privilege
Current privilege level is viewer
sensor#
```

関連コマンド

| コマンド | 説明 |
|-----------------------|----------------------|
| <code>username</code> | ローカル センサーのユーザを作成します。 |

show settings

現行のサブモードに含まれるコンフィギュレーションの内容を表示するには、サービス コマンドモードで `show settings` コマンドを使用します。

```
show settings [ terse ]
```

| | | |
|------|--------------|--------------|
| 構文説明 | <i>terse</i> | 出力を簡潔に表示します。 |
|------|--------------|--------------|

| | | |
|-------|---------------------|--|
| デフォルト | デフォルトの動作または値はありません。 | |
|-------|---------------------|--|

| | | |
|---------|--------------------|--|
| コマンドモード | すべての サービス コマンド モード | |
|---------|--------------------|--|

| | | |
|---------------|---------------------------------|--|
| サポートされるユーザロール | 管理者、オペレータ、ビューア（最上位コマンドツリーの表示のみ） | |
|---------------|---------------------------------|--|

| コマンド履歴 | リリース | 修正 |
|--------|--------|------------------------------|
| | 4.0(1) | このコマンドを導入。 |
| | 4.0(2) | <code>terse</code> キーワードを追加。 |

| | | |
|------------|-------------------|--|
| 使用上のガイドライン | このコマンドは IPS 固有です。 | |
|------------|-------------------|--|



| | |
|-----|-----------------------------------|
| (注) | このコマンドは、Cisco IOS 12.0 以前にはありません。 |
|-----|-----------------------------------|

| | | |
|---|---|--|
| 例 | 次の例は、ARC コンフィギュレーション モードでの <code>show settings</code> コマンドの出力を示します。 | |
|---|---|--|



| | |
|-----|---|
| (注) | Network Access Controller は、現在は Attack Response Controller (ARC) と言います。サービスは新しい名称になっていますが、変更は IPS 5.1 の CLI には反映されていません。CLI 全体にわたって <code>network-access</code> および <code>nac</code> と表示されます。 |
|-----|---|

```
sensor# configure terminal
sensor(config)# service network-access
sensor(config-net)# show settings
  general
  -----
    log-all-block-events-and-errors: true <defaulted>
    enable-nvram-write: false <defaulted>
    enable-acl-logging: false <defaulted>
    allow-sensor-block: true default: false
    block-enable: true <defaulted>
    block-max-entries: 250 <defaulted>
    max-interfaces: 250 <defaulted>
    master-blocking-sensors (min: 0, max: 100, current: 0)
    -----
    never-block-hosts (min: 0, max: 250, current: 0)
    -----
    never-block-networks (min: 0, max: 250, current: 0)
    -----
    block-hosts (min: 0, max: 250, current: 0)
    -----
    block-networks (min: 0, max: 250, current: 0)
    -----
    user-profiles (min: 0, max: 250, current: 0)
    -----
    cat6k-devices (min: 0, max: 250, current: 0)
    -----
    router-devices (min: 0, max: 250, current: 0)
    -----
    firewall-devices (min: 0, max: 250, current: 0)
    -----
sensor(config-net)#
```

次の例は、シグニチャ定義サブモードでの `show settings terse` の出力を示します。

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# show settings terse
  variables (min: 0, max: 256, current: 2)
-----
  <protected entry>
  variable-name: WEBPORTS
  variable-name: user2
-----
application-policy
-----
  http-policy
-----
  http-enable: false <defaulted>
  max-outstanding-http-requests-per-connection: 10 <defaulted>
  aic-web-ports: 80-80,3128-3128,8000-8000,8010-8010,8080-8080,8888-8888,
24326-24326 <defaulted>
-----
  ftp-enable: true default: false
-----
fragment-reassembly
-----
  ip-reassemble-mode: nt <defaulted>
-----
stream-reassembly
-----
  tcp-3-way-handshake-required: true <defaulted>
  tcp-reassembly-mode: strict <defaulted>
--MORE--
```

次の例は、フィルタ処理された `show settings` の出力を示します。このコマンドは、HTTP が含まれる行のみを出力します。

```

sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# show settings | include HTTP
Searching:
  sig-string-info: Bagle.Q HTTP propagation (jpeg) <defaulted>
  sig-string-info: Bagle.Q HTTP propagation (php) <defaulted>
  sig-string-info: GET ftp://@@:@@@/pub HTTP/1.0 <defaulted>
  sig-name: IMail HTTP Get Buffer Overflow <defaulted>
  sig-string-info: GET shellcode HTTP/1.0 <defaulted>
  sig-string-info: ..%c0%af..*HTTP <defaulted>
  sig-string-info: ..%c1%9c..*HTTP <defaulted>
  sig-name: IOS HTTP Unauth Command Execution <defaulted>
  sig-name: Null Byte In HTTP Request <defaulted>
  sig-name: HTTP tunneling <defaulted>
  sig-name: HTTP tunneling <defaulted>
  sig-name: HTTP tunneling <defaulted>
  sig-name: HTTP tunneling <defaulted>
  sig-name: HTTP CONNECT Tunnel <defaulted>
  sig-string-info: CONNECT.*HTTP/ <defaulted>
  sig-name: HTTP 1.1 Chunked Encoding Transfer <defaulted>
  sig-string-info: INDEX / HTTP <defaulted>
  sig-name: Long HTTP Request <defaulted>
  sig-string-info: GET \x3c400+ chars>? HTTP/1.0 <defaulted>
  sig-name: Long HTTP Request <defaulted>
  sig-string-info: GET .....?\x3c400+ chars> HTTP/1.0 <defaulted>
  sig-string-info: /mod_ssl:error:HTTP-request <defaulted>
  sig-name: Dot Dot Slash in HTTP Arguments <defaulted>
  sig-name: HTTPBench Information Disclosure <defaulted>

--MORE--

```


show ssh authorized-keys

現行ユーザの公開 RSA キーを表示するには、特権 EXEC モードで `show ssh authorized-keys` コマンドを使用します。

```
show ssh authorized-keys [ id ]
```

| | | |
|-------------|-----------|---|
| 構文説明 | <i>id</i> | 許可されたキーを一意に特定する 1 ~ 256 文字の文字列。数字、「_」および「-」は有効ですが、スペースと「?」は使用できません。 |
|-------------|-----------|---|

デフォルト デフォルトの動作または値はありません。

コマンドモード EXEC

サポートされるユーザロール 管理者、オペレータ、ビューア

| | | |
|---------------|-------------|------------|
| コマンド履歴 | リリース | 修正 |
| | 4.0(1) | このコマンドを導入。 |

使用上のガイドライン オプションの ID を指定せずにこのコマンドを実行すると、システムで設定済みの ID のリストが表示されます。特定の ID を指定してコマンドを実行すると、その ID に関連付けられたキーが表示されます。このコマンドは、IPS 固有です。



(注) このコマンドは、Cisco IOS 12.0 以前にはありません。

例 次の例は、SSH 認証キーのリストを表示します。

```
sensor# show ssh authorized-keys
system1
system2
system3
system4
```

次の例は、system1 の SSH キーを表示します。

```
sensor# show ssh authorized-keys system1

1023 37
66022272955660983338089706716372943357082868686000817201780243492180421420781303592082
95091017013584805250399939321125031474527683786209111899866537160898131479220860447399
113413696428706823193619281485218640945574163061387864683351158359104049402131369543353
39616344979349705016792583146548622146467421997057
sensor#
```

| | | |
|---------------|---------------------------------|---|
| 関連コマンド | コマンド | 説明 |
| | <code>ssh authorized-key</code> | 現行ユーザに公開キーを追加し、クライアントが RSA 認証を使用してローカル SSH サーバにログインできるようにします。 |

show ssh server-key

SSH サーバのホスト キーとホスト キーのフィンガープリントを表示するには、特権 EXEC モードで `show ssh server-key` コマンドを使用します。

```
show ssh server-key
```

構文説明 このコマンドには、引数またはキーワードはありません。

デフォルト デフォルトの動作または値はありません。

コマンドモード EXEC

サポートされるユーザロール 管理者、オペレータ、ビューア

| コマンド履歴 | リリース | 修正 |
|--------|--------|------------|
| | 4.0(1) | このコマンドを導入。 |

使用上のガイドライン このコマンドは IPS 固有です。



(注) このコマンドは、Cisco IOS 12.0 以前にはありません。

例 次の例は、`show ssh server-key` コマンドの出力を示します。

```
sensor# show ssh server-key
1024 35 144719237233791547030730646600884648599022074867561982783071499320643934
48734496072779375489584407249259840037709354850629125941930828428605183115777190
69953460097510388011424663818234783053872210554889384417232132153750963283322778
52374794118697053304026570851868326130246348580479834689461788376232451955011
MD5: F3:10:3E:BA:1E:AB:88:F8:F5:56:D3:A6:63:42:1C:11
Bubble Babble: xucis-hehon-kizog-nedeg-zunom-kolyn-syzec-zasyk-symuf-rykum-sexyx
sensor#
```

| 関連コマンド | コマンド | 説明 |
|--------|-------------------------------|-----------------------------------|
| | <code>ssh generate-key</code> | センサーで SSH サーバが使用するサーバホストキーを変更します。 |

show ssh host-keys

センサーが接続に使用できるリモート SSH サーバの公開キーを含む既知のホスト テーブルを表示するには、特権 EXEC モードで `show ssh host-keys` を使用します。

```
show ssh host-keys [ ipaddress]
```

| | | |
|-------------|------------------|--|
| 構文説明 | <i>ipaddress</i> | ピリオドで区切られた 4 オクテットの 32 ビット アドレス。X.X.X.X、ここで X は 0 ~ 255。 |
|-------------|------------------|--|

デフォルト デフォルトの動作または値はありません。

コマンドモード EXEC

サポートされるユーザロール 管理者、オペレータ、ビューア

| | | |
|---------------|-------------|--------------------------------------|
| コマンド履歴 | リリース | 修正 |
| | 4.0(1) | このコマンドを導入。 |
| | 4.1(1) | コマンドへの Bubble Babble および MD5 の出力を追加。 |

使用上のガイドライン オプションの IP アドレス ID を指定せずにこのコマンドを実行すると、公開キーで設定済みの IP アドレスのリストが表示されます。特定の IP アドレスを指定してコマンドを実行すると、その IP アドレスに関連付けられたキーが表示されます。このコマンドは IPS 固有です。



(注) このコマンドは、Cisco IOS 12.0 以前にはありません。

例 次の例は、`show ssh host-keys` コマンドの出力を示します。

```
sensor# show ssh host-keys 10.1.2.3
1024 35 144719237233791547030730646600884648599022074867561982783071499320643934
48734496072779375489584407249259840037709354850629125941930828428605183115777190
69953460097510388011424663818234783053872210554889384417232132153750963283322778
52374794118697053304026570851868326130246348580479834689461788376232451955011
MD5: F3:10:3E:BA:1E:AB:88:F8:F5:56:D3:A6:63:42:1C:11
Bubble Babble: xucis-hehon-kizog-nedeg-zunom-kolyn-syzec-zasyk-symuf-rykum-sexyx
sensor#
```

| | | |
|---------------|---------------------------|-------------------------|
| 関連コマンド | コマンド | 説明 |
| | <code>ssh host-key</code> | 既知のホスト テーブルにエントリを追加します。 |

show statistics

要求した統計情報を表示するには、特権 EXEC モードで `show statistics` コマンドを使用します。

```
show statistics {analysis-engine | authentication | denied-attackers | event-server | event-store | host
| logger | network-access | notification | sdee-server | transaction server | transaction-source |
virtual-sensor | web-server} [clear]
```

構文説明

`clear` 統計情報が取得された後、統計情報をクリアします。



(注) このオプションは、分析エンジン、ホスト、またはネットワーク アクセスの統計情報には使用できません。

`analysis-engine` 分析エンジン統計情報を表示します。

`authentication` 許可および認証統計情報を表示します。

`denied-attackers` 拒否する IP アドレスおよび各攻撃者からのパケット数のリストを表示します。

`event-server` イベントサーバ統計情報を表示します。

`event-store` イベントストア統計情報を表示します。

`host` ホスト（メイン）統計情報を表示します。

`logger` ログ機能統計情報を表示します。

`network-access` ARC 統計情報を表示します。



(注) Network Access Controller は、現在は Attack Response Controller (ARC) と言います。サービスは新しい名称になっていますが、変更は IPS 5.1 の CLI には反映されていません。CLI 全体にわたって `network-access` および `nac` と表示されます。

`notification` 通知統計情報を表示します。

`sdee-server` SDEE サーバ統計情報を表示します。

`transaction server` トランザクションサーバ統計情報を表示します。

`transaction-source` トランザクションソース統計情報を表示します。

`web-server` Web サーバ統計情報を表示します。

`virtual-sensor` 仮想センサー統計情報を表示します。

`name` 仮想センサーの論理名。

デフォルト

デフォルトの動作または値はありません。

コマンドモード

EXEC

サポートされるユーザロール

管理者、オペレータ、ビューア

コマンド履歴

| リリース | 修正 |
|--------|--|
| 4.0(1) | このコマンドを導入。 |
| 5.0(1) | analysis-engine 、 virtual-sensor 、および denied-attackers を追加。 |



(注) このコマンドは、Cisco IOS 12.0 以前にはありません。

例

次の例は、認証統計情報を表示します。

```
sensor# show statistics authentication
General
  totalAuthenticationAttempts = 9
  failedAuthenticationAttempts = 0
sensor#
```

次の例は、イベントストア統計情報を表示します。

```
sensor# show statistics event-store
Event store statistics
  General information about the event store
    The current number of open subscriptions = 1
    The number of events lost by subscriptions and queries = 0
    The number of queries issued = 1
    The number of times the event store circular buffer has wrapped = 0
  Number of events of each type currently stored
    Debug events = 0
    Status events = 129
    Log transaction events = 0
    Shun request events = 0
    Error events, warning = 8
    Error events, error = 13
    Error events, fatal = 0
    Alert events, informational = 0
    Alert events, low = 0
    Alert events, medium = 0
    Alert events, high = 0
sensor#
```

次の例は、ログ機能統計情報を表示します。

```
sensor# show statistics logger
The number of Log interprocessor FIFO overruns = 0
The number of syslog messages received = 27
The number of <evError> events written to the event store by severity
  Fatal Severity = 0
  Error Severity = 13
  Warning Severity = 35
  TOTAL = 48
The number of log messages written to the message log by severity
  Fatal Severity = 0
  Error Severity = 13
  Warning Severity = 8
  Timing Severity = 0
  Debug Severity = 0
  Unknown Severity = 26
  TOTAL = 47
sensor#
```

次の例は、ARC 統計情報を表示します。

```
sensor# show statistics network-access
Current Configuration
  LogAllBlockEventsAndSensors = true
  EnableNvramWrite = false
  EnableAclLogging = false
  AllowSensorBlock = false
  BlockMaxEntries = 250
  MaxDeviceInterfaces = 250
State
  BlockEnable = true
sensor#
```

show tech-support

現行システムの状況を表示するには、特権 EXEC モードで `show tech-support` コマンドを使用します。

```
show tech-support [page] [password] [destination-url destination url]
```

構文説明

| | |
|------------------------------|---|
| <code>page</code> | (オプション) 出力は一度に 1 ページの情報が表示されます。Enter キーを押して次の出力行を表示するか、スペースバーを押して次ページの情報を表示します。 <code>page</code> を使用しない場合、出力は改ページなしで表示されます |
| <code>password</code> | (オプション) 出力にパスワードとその他のセキュリティ情報が表示されません。 <code>password</code> を指定しない場合、パスワードとその他のセキュリティ機密情報は、 <code><removed></code> (デフォルト) というラベルで置き換えられます |
| <code>destination-url</code> | (オプション) 情報を HTML でフォーマット化し、このタグに続く宛先に送信することを示すタグ。このオプションを選択した場合、出力は画面に表示されません。 |
| <code>destination url</code> | (オプション) レポート ファイルの宛先。URL を指定すると、出力は HTML ファイルにフォーマット化されて、指定された宛先に送信されます。指定しない場合は画面に表示されます |

デフォルト

「構文説明」の表を参照してください。

コマンドモード

EXEC


サポートされるユーザロール

管理者

コマンド履歴

| リリース | 修正 |
|--------|------------|
| 4.0(1) | このコマンドを導入。 |

使用上のガイドライン

 (注) Cisco IOS バージョン 12.0 では、このコマンドの宛先部分はサポートされません。

宛先 URL の正確なフォーマットはファイルにより異なります。ファイル名を選択できますが、.html で終了する必要があります。

次の宛先タイプを指定できます。

- **ftp:** : FTP ネットワーク サーバの宛先 URL。このプレフィックスの構文は、`ftp:[[/username@location]/relativeDirectory]/filename` または `ftp:[[/username@location]//absoluteDirectory]/filename` です。
- **scp:** : SCP ネットワーク サーバの宛先 URL。このプレフィックスの構文は、`scp:[[/username@]location]/relativeDirectory]/filename` または `scp:[[/username@]location]//absoluteDirectory]/filename` です。

レポートには、次のコマンドからの HTML リンク出力が含まれています。

- **show interfaces**
- **show statistics network-access**
- **cidDump**

例 次の例は、tech-support の出力を `~csidsuser/reports/sensor1Report.html` ファイルに保存します。パスは、csidsuser のホーム アカウントを基準とします。

```
sensor# show tech support destination-url  
ftp://csidsuser@10.2.1.2/reports/sensor1Report.html password:*****
```

次の例は、tech-support の出力を `/absolute/reports/sensor1Report.html` ファイルに保存します。

```
sensor# show tech support destination-url  
ftp://csidsuser@10.2.1.2//absolute/reports/sensor1Report.html password:*****
```


show tls fingerprint

サーバの TLS 証明書のフィンガープリントを表示するには、特権 EXEC モードで `show tls-fingerprint` を使用します。

```
show tls fingerprint
```

構文説明 このコマンドには、引数またはキーワードはありません。

デフォルト デフォルトの動作または値はありません。

コマンドモード EXEC

サポートされるユーザロール 管理者、オペレータ、ビューア

| コマンド履歴 | リリース | 修正 |
|--------|--------|------------|
| | 4.0(1) | このコマンドを導入。 |

使用上のガイドライン このコマンドは IPS 固有です。



(注) このコマンドは、Cisco IOS 12.0 以前にはありません。

例 次の例は、`show tls fingerprint` コマンドの出力を示します。

```
sensor# show tls fingerprint
MD5: 1F:94:6F:2E:38:AD:FB:2C:42:0C:AE:61:EC:29:74:BB
SHA1: 16:AC:EC:AC:9D:BC:84:F5:D8:E4:1A:05:C4:01:BB:65:7B:4F:FC:AA
sensor#
```

| 関連コマンド | コマンド | 説明 |
|--------|-------------------------------|----------------------------|
| | <code>tls generate-key</code> | サーバの自己署名 X.509 証明書を再生成します。 |

show tls trusted-hosts

センサーの信頼できるホストを表示するには、特権 EXEC モードで `show tls trusted-hosts` コマンドを使用します。

```
show tls trusted-hosts [ id ]
```

| | |
|-------------|---|
| 構文説明 | <i>id</i> 許可されたキーを一意に特定する 1 ~ 32 文字の文字列。数字、「_」、および「-」は有効ですが、スペースと「?」は使用できません。 |
|-------------|---|

デフォルト デフォルトの動作または値はありません。

コマンドモード EXEC

サポートされるユーザロール 管理者、オペレータ、ビューア

| コマンド履歴 | <table border="1"> <thead> <tr> <th>リリース</th> <th>修正</th> </tr> </thead> <tbody> <tr> <td>4.0(1)</td> <td>このコマンドを導入。</td> </tr> </tbody> </table> | リリース | 修正 | 4.0(1) | このコマンドを導入。 |
|---------------|---|------|----|--------|------------|
| リリース | 修正 | | | | |
| 4.0(1) | このコマンドを導入。 | | | | |

使用上のガイドライン オプションの ID を指定せずにこのコマンドを実行すると、システムで設定済みの ID のリストが表示されます。特定の ID を指定してコマンドを実行すると、その ID に関連付けられた証明書のフィンガープリントが表示されます。

このコマンドは IPS 固有です。



(注) このコマンドは、Cisco IOS 12.0 以前にはありません。

例 次の例は、`show tls trusted-hosts` コマンドの出力を示します。

```
sensor# show tls trusted-hosts 172.21.172.1
MD5: 1F:94:6F:2E:38:AD:FB:2C:42:0C:AE:61:EC:29:74:BB
SHA1: 16:AC:EC:AC:9D:BC:84:F5:D8:E4:1A:05:C4:01:BB:65:7B:4F:FC:AA
sensor#
```

| 関連コマンド | <table border="1"> <thead> <tr> <th>コマンド</th> <th>説明</th> </tr> </thead> <tbody> <tr> <td><code>tls trusted-host</code></td> <td>信頼できるホストをシステムに追加します。</td> </tr> </tbody> </table> | コマンド | 説明 | <code>tls trusted-host</code> | 信頼できるホストをシステムに追加します。 |
|-------------------------------|--|------|----|-------------------------------|----------------------|
| コマンド | 説明 | | | | |
| <code>tls trusted-host</code> | 信頼できるホストをシステムに追加します。 | | | | |

show users

現在 CLI にログインしているユーザに関する情報を表示するには、特権 EXEC モードで `show users` コマンドを使用します。

```
show users [ all ]
```

| | |
|------|--|
| 構文説明 | <code>all</code> (オプション) ログイン状況に関係なく、システムで構成されているすべてのユーザアカウントのリストを表示します。 |
|------|--|

デフォルト デフォルトの動作または値はありません。

コマンドモード EXEC

サポートされるユーザロール 管理者、オペレータ、ビューア (自分のログインの表示のみ)

| コマンド履歴 | リリース | 修正 |
|--------|--------|--|
| | 4.0(1) | このコマンドを導入。 |
| | 4.1(1) | ロックされたアカウントを表示するようにアップデート。 <code>show users all</code> でのビューアの表示を制限。 |

使用上のガイドライン CLI でこのコマンドを使用すると、ID、ユーザ名、および権限を表示できます。説明の横の「*」は現行ユーザを示します。カッコ「()」で囲まれたユーザ名は、アカウントがロックされていることを示します。アカウントは、ユーザが連続して X 回、不正なパスワードを入力するとロックされます。ロックされたユーザのパスワードを `password` コマンドでリセットすると、アカウントのロックが解除されます。

同時にログインできる CLI ユーザの最大数は、プラットフォームによって異なります。



(注) このコマンドの出力は、Cisco IOS 12.0 コマンドの場合とは異なります。

例 次の例は、`show users` コマンドの出力を示します。

```
sensor# show users
```

```

      CLI ID      User           Privilege
-----
      1234        notheruser     viewer
*      9802        curuser        operator
      5824        tester         administrator

```

次の例は、tester2 のユーザ アカウントがロックされていることを示します。

```
sensor# show users all

      CLI ID      User           Privilege
-----
      1234        notheruser     viewer
*     9802        curuser        operator
      5824        tester         administrator
                        (tester2)      viewer
                        foobar          operator
```

次の例は、ビューアに対する show users all の出力を示します。

```
sensor# show users all

      CLI ID      User           Privilege
-----
*     9802        tester         viewer
      5824        tester         viewer
```

関連コマンド

| コマンド | 説明 |
|------------|---------------------|
| clear line | 別の CLI セッションを終了します。 |

show version

すべてのインストールされている OS パッケージ、シグニチャパッケージ、およびシステムで実行している IPS プロセスに関するバージョン情報を表示するには、特権 EXEC モードで **show version** コマンドを使用します。

show version

構文説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトの動作または値はありません。

コマンドモード

EXEC

サポートされるユーザロール

管理者、オペレータ、ビューア

コマンド履歴

| リリース | 修正 |
|--------|------------|
| 4.0(1) | このコマンドを導入。 |

使用上のガイドライン

show version コマンドの出力は IPS 固有で、Cisco IOS コマンドの出力とは異なります。

シリアル番号の後ろに、次のいずれかのライセンス情報が表示されます。

No license present

Expired license: <expiration-date>

Valid license, expires: <expiration-date>

Valid demo license, expires: <expiration-date>

<expiration-date> の形式は *dd-mon-yyyy* です (04-dec-2004 など)。



(注)

アップグレード履歴パッケージ名の前の * は、ダウングレードが実行された後の残りのバージョンを示します。* のマークが付いたパッケージがない場合、ダウングレードはできません。

例

次の例は、**show version** コマンドの出力を示します。

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 5.0(0.1)S91(0.1)

OS Version 2.4.26-IDS-smp-bigphys
Platform: IDS-4235
No license present
Sensor up-time is 6 days.
Using 701513728 out of 922509312 bytes of available memory (76% usage)
Using 527.6M out of 15.9G bytes of available disk space (3% usage)
Using 192.0k out of 31.0M bytes of available disk space (1% usage)

MainApp          2004_Aug_16_03.00  (Release)  2004-08-16T03:19:41-0500  Running
AnalysisEngine  2004_Aug_16_03.00  (Release)  2004-08-16T03:19:41-0500  Running
CLI              2004_Aug_16_03.00  (Release)  2004-08-16T03:19:41-0500

Upgrade History:

No upgrades installed

Recovery Partition Version 5.0.1.S91.0.1

sensor#
```

ssh authorized-key

現行ユーザに公開キーを追加し、クライアントが RSA 認証を使用してローカル SSH サーバにログインできるようにするには、グローバル コンフィギュレーション モードで `ssh authorized-key` コマンドを使用します。このコマンドを `no` 形式で使用すると、システムから許可されたキーを削除できます。

```
ssh authorized-key id key-modulus-length public-exponent public-modulus
```

```
no ssh authorized-key id
```

構文説明

| | |
|---------------------------------|---|
| <code>id</code> | 許可されたキーを一意に特定する 1 ~ 256 文字の文字列。数字、「_」、および「-」は有効ですが、スペースと「?」は使用できません。 |
| <code>key-modulus-length</code> | 511 ~ 2048 の範囲の ASCII 10 進整数。 |
| <code>public-exponent</code> | 3 ~ 2 ³² の範囲の ASCII 10 進整数。 |
| <code>public-modulus</code> | ASCII 10 進整数。(2 ^x (キーモジュラス長)) < x < (2 ^x (キーモジュラス長)) の x 値。 |

デフォルト

デフォルトの動作または値はありません。

コマンドモード

グローバル コンフィギュレーション

サポートされるユーザロール

管理者、オペレータ、ビューア

コマンド履歴

| リリース | 修正 |
|--------|------------|
| 4.0(1) | このコマンドを導入。 |

使用上のガイドライン

このコマンドにより、現行ユーザの既知のホスト テーブルにエントリが追加されます。キーを変更するには、エントリを削除し、再作成する必要があります。

このコマンドは IPS 固有です。



(注) このコマンドは、Cisco IOS 12.0 以前にはありません。

例

次の例は、既知のホスト テーブルにエントリを追加する方法を示します。

```
sensor(config)# ssh authorized-key system1 1023 37
66022272955660983338089706716372943357082868686000817201780243492180421420781303592082
95091017013584805250399939321125031474527683786209111899866537160898131479220860447399
11341369642870682319361928148521864094557416306138786468335115835910404940213136954353
39616344979349705016792583146548622146467421997057
sensor(config)#
```

関連コマンド

| コマンド | 説明 |
|----------------------------------|------------------------|
| <code>ssh authorized-keys</code> | 現行ユーザの公開 RSA キーを表示します。 |

ssh generate-key

センサーで SSH サーバが使用するサーバ ホスト キーを変更するには、特権 EXEC モードで `ssh generate-key` コマンドを使用します。

```
ssh generate-key
```

構文説明 このコマンドには、引数またはキーワードはありません。

デフォルト デフォルトの動作または値はありません。

コマンド モード EXEC

サポートされるユーザロール 管理者

| コマンド履歴 | リリース | 修正 |
|--------|--------|------------|
| | 4.0(1) | このコマンドを導入。 |

使用上のガイドライン 表示されるキーのフィンガープリントは、このセンサーと今後接続されるリモート SSH クライアントが SSH プロトコルバージョン 1.5 を使用している場合、リモートクライアントで表示されるフィンガープリントと一致します。

このコマンドは IPS 固有です。



(注) このコマンドは、Cisco IOS 12.0 以前にはありません。

例 次の例は、新しい SSH サーバ ホスト キーを生成する方法を示します。

```
sensor# ssh generate-key
MD5: 49:3F:FD:62:26:58:94:A3:E9:88:EF:92:5F:52:6E:7B
Bubble Babble: xebiz-vykyk-fekuh-rukuh-cabaz-paret-gosym-serum-korus-fypop-huxyx
sensor#
```

| 関連コマンド | コマンド | 説明 |
|--------|----------------------------------|--|
| | <code>show ssh server-key</code> | SSH サーバのホスト キーとホスト キーのフィンガープリントを表示します。 |

ssh host-key

既知のホスト テーブルにエントリを追加するには、グローバル コンフィギュレーション モードで `ssh host-key` コマンドを使用します。モジュラス、指数、および長さを指定しない場合、要求された IP アドレスの MD5 フィンガープリントおよび Bubble Babble がシステムに表示されて、テーブルにキーを追加できます。このコマンドを `no` 形式で使用すると、既知のホスト テーブルからエントリを削除できます。

```
ssh host-key ipaddress [ key-modulus-length public-exponent public-modulus ]
```

```
no ssh host-key ipaddress
```

構文説明

| | |
|---------------------------|--|
| <i>ipaddress</i> | ピリオドで区切られた 4 オクテットの 32 ビット アドレス。X.X.X.X、ここで X は 0 ~ 255。 |
| <i>key-modulus-length</i> | 511 ~ 2048 の範囲の ASCII 10 進整数。 |
| <i>public-exponent</i> | 3 ~ 2^{32} の範囲の ASCII 10 進整数。 |
| <i>public-modulus</i> | ASCII 10 進整数。 $(2^{\text{キーモジュラス長}}) < x < (2^{\text{キーモジュラス長}})$ の x 値。 |

デフォルト

デフォルトの動作または値はありません。

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザロール

管理者、オペレータ

コマンド履歴

| リリース | 修正 |
|--------|------------|
| 4.0(1) | このコマンドを導入。 |

使用上のガイドライン

`ssh host-key` コマンドを使用すると、既知のホスト テーブルにエントリを追加できます。IP アドレスのキーを変更するには、エントリを削除し、再作成する必要があります。

モジュラス、指数、および長さを指定しない場合、指定された IP アドレスの SSH サーバに接続して、要求されたキーをネットワーク経由で取得します。指定するホストは、コマンドを発行した時点でアクセス可能である必要があります。

このコマンドは IPS 固有です。



(注) このコマンドは、Cisco IOS 12.0 以前にはありません。

例

次の例は、10.1.2.3 の既知のホスト テーブルにエントリを追加する方法を示します。

```
sensor(config)# ssh host-key 10.1.2.3
1024 35
13930621354183524038533292225396881468568452352006413199783990511364012021781686969670
87217046313228442920738517305650448790826706775541579370584852039955721146312966045521
61309712601068614812749969593513740598331393154884988302302182922353335152653860589163
651944997842874583627883277460138506084043415861927
sensor(config)#
```

次の例は、10.1.2.3 の既知のホスト テーブルにエントリを追加する方法を示します。

```
sensor(config)# ssh host-key 10.1.2.3
MD5 fingerprint is 49:3F:FD:62:26:58:94:A3:E9:88:EF:92:5F:52:6E:7B
Bubble Babble is xebiz-vykyk-fekuh-rukuh-cabaz-paret-gosym-serum-korus-fypop-huxyx
Would you like to add this to the known hosts table for this host? [yes]
sensor(config)#
```

関連コマンド

| コマンド | 説明 |
|-------------------|--|
| show ssh host-key | センサーが接続できるリモート SSH サーバの公開キーを含む既知のホスト テーブルを表示します。 |

terminal

ログインセッションのターミナルプロパティを変更するには、特権 EXEC モードで `terminal` コマンドを使用します。

```
terminal [length screen-length]
```

構文説明

| | |
|----------------------|---|
| <i>screen-length</i> | 画面の行数を設定します。マルチ画面出力時に一時停止する行数を指定するには、この値を使用します。値ゼロの場合は、出力が画面長を超えても一時停止しません。デフォルトは 24 行です。この値は、ログインセッション間で保存されません。 |
|----------------------|---|

デフォルト

「構文説明」の表を参照してください。

コマンドモード

EXEC

サポートされるユーザロール

管理者、オペレータ、ビューア

コマンド履歴

| リリース | 修正 |
|--------|------------|
| 4.0(1) | このコマンドを導入。 |

使用上のガイドライン

`terminal length` コマンドを使用すると、`--more--` プロンプトが表示される前に、表示される行数を設定できます。

例

次の例は、マルチ画面表示の画面間で一時停止しないように CLI を設定します。

```
sensor# terminal length 0
sensor#
```

次の例は、マルチ画面表示の各画面について 10 行表示するように CLI を設定します。

```
sensor# terminal length 10
sensor#
```

tls generate-key

サーバの自己署名 X.509 証明書を再生成するには、特権 EXEC モードで `tls generate-key` を使用します。ホストで自己署名証明書を使用しない場合は、エラーが返されます。

```
tls generate-key
```

構文説明 このコマンドには、引数またはキーワードはありません。

デフォルト デフォルトの動作または値はありません。

コマンドモード EXEC

サポートされるユーザロール 管理者

| コマンド履歴 | リリース | 修正 |
|--------|--------|------------|
| | 4.0(1) | このコマンドを導入。 |

使用上のガイドライン このコマンドは IPS 固有です。



(注) このコマンドは、Cisco IOS 12.0 以前にはありません。

例 次の例は、サーバの自己署名証明書を生成する方法を示します。

```
sensor(config)# tls generate-key
MD5: 1F:94:6F:2E:38:AD:FB:2C:42:0C:AE:61:EC:29:74:BB
SHA1: 16:AC:EC:AC:9D:BC:84:F5:D8:E4:1A:05:C4:01:BB:65:7B:4F:FC:AA
sensor(config)#
```

| 関連コマンド | コマンド | 説明 |
|--------|-----------------------------------|-------------------------------|
| | <code>show tls fingerprint</code> | サーバの TLS 証明書のフィンガープリントを表示します。 |

tls trusted-host

信頼できるホストをシステムに追加するには、グローバル コンフィギュレーション モードで `tls trusted-host` コマンドを使用します。このコマンドを `no` 形式で使用すると、信頼できるホスト証明書を削除できます。

```
tls trusted-host ip-address ip-address [port port]
```

```
no tls trusted-host ip-address ip-address [ port port ]
```

```
no tls trusted-host id id
```

構文説明

| | |
|-------------------|---|
| <i>ip-address</i> | 追加または削除するホストの IP アドレス。 |
| <i>port</i> | (オプション) 接続するホストのポート番号。デフォルトはポート 443 です。 |

デフォルト

「構文説明」の表を参照してください。

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザロール

管理者、オペレータ

コマンド履歴

| リリース | 修正 |
|--------|---|
| 4.0(1) | このコマンドを導入。 |
| 4.0(2) | オプションのポートを追加。ID に基づいた削除をサポートするため <code>no</code> コマンドを追加。 |

使用上のガイドライン

このコマンドを使用すると、要求されたホスト / ポートの現行のフィンガープリントを取得して、その結果を表示できます。追加が要求されているホストから直接取得した情報に基づいて、フィンガープリントを受け入れるか拒否するかを選択できます。

各証明書は、ID フィールド付きで保存されます。IP アドレスおよびデフォルト ポートの ID フィールドは *ipaddress* で、IP アドレスおよび指定ポートの ID フィールドは *ipaddress:port* です。



(注) このコマンドは、Cisco IOS 12.0 以前にはありません。

例

次のコマンドは、信頼できるホスト テーブルに、IP アドレス 172.21.172.1、ポート 443 のエンTRIES を追加します。

```
sensor(config)# tls trusted-host ip-address 172.21.172.1
Certificate MD5 fingerprint is D4:C2:2F:78:B5:C6:30:F2:C4:6A:8E:5D:6D:C0:DE:32
Certificate SHA1 fingerprint is
36:42:C9:1B:9F:A4:A8:91:7F:DF:F0:32:04:26:E4:3A:7A:70:B9:95
Would you like to add this to the trusted certificate table for this host? [yes]
Certificate ID: 172.21.172.1 successfully added to the TLS trusted host table.
sensor(config)#
```



(注) コマンドが正常に終了すると、要求された証明書に関して保存された証明書 ID が表示されます。

次のコマンドは、IP アドレス 172.21.172.1、ポート 443 の信頼できるホスト エントリを削除します。

```
sensor(config)# no tls trusted-host ip-address 172.21.172.1
sensor(config)#
```

または、次のコマンドを使用して、IP アドレス 172.21.172.1、ポート 443 の信頼できるホスト エントリを削除できます。

```
sensor(config)# no tls trusted-host id 172.21.172.1
sensor(config)#
```

次のコマンドは、信頼できるホスト テーブルに、IP アドレス 10.1.1.1、ポート 8000 のエントリを追加します。

```
sensor(config)# tls trusted-host ip-address 10.1.1.1 port 8000
Certificate MD5 fingerprint is D4:C2:2F:78:B5:C6:30:F2:C4:6A:8E:5D:6D:C0:DE:32
Certificate SHA1 fingerprint is
36:42:C9:1B:9F:A4:A8:91:7F:DF:F0:32:04:26:E4:3A:7A:70:B9:95
Would you like to add this to the trusted certificate table for this host? [yes]
Certificate ID: 10.1.1.1:8000 successfully added to the TLS trusted host table.
sensor(config)#
```



(注) コマンドが正常に終了すると、要求された証明書に関して保存された証明書 ID が表示されます。

次のコマンドは、IP アドレス 10.1.1.1、ポート 8000 の信頼できるホスト エントリを削除します。

```
sensor(config)# no tls trusted-host ip-address 10.1.1.1 port 8000
sensor(config)#
```

または、次のコマンドを使用して、IP アドレス 10.1.1.1、ポート 8000 の信頼できるホスト エントリを削除できます。

```
sensor(config)# no tls trusted-host id 10.1.1.1:8000
sensor(config)#
```

関連コマンド

| コマンド | 説明 |
|-------------------------------------|----------------------|
| <code>show tls trusted-hosts</code> | センサーの信頼できるホストを表示します。 |

trace

IP パケットが宛先に送信されるルートを表示するには、特権 EXEC モードで **trace** コマンドを使用します。

```
trace address [count]
```

構文説明

| | |
|----------------|------------------------------------|
| <i>address</i> | ルートをトレースするシステムのアドレス。 |
| <i>count</i> | 使用するホップ数。デフォルトは4です。有効な値は1 ~ 256です。 |

デフォルト

「構文説明」の表を参照してください。

コマンドモード

EXEC

Command Types

管理者、オペレータ、ビューア

コマンド履歴

| リリース | 修正 |
|--------|------------|
| 4.0(1) | このコマンドを導入。 |

使用上のガイドライン

trace コマンドには、コマンド割り込みはありません。コマンドは完了するまで実行する必要があります。

例

次の例は、**trace** コマンドの出力を示します。

```
sensor# trace 10.1.1.1
traceroute to 172.21.172.24 (172.21.172.24), 30 hops max, 40 byte packets 1
171.69.162.2 (171.69.162.2) 1.25 ms 1.37 ms 1.58 ms 2 172.21.172.24 (172.21.172.24)
0.77 ms 0.66 ms 0.68 ms
sensor#
```

upgrade

サービスパック、シグニチャアップデート、またはイメージアップグレードを適用するには、グローバルコンフィギュレーションモードで **upgrade** コマンドを使用します。

```
upgrade source-url
```

| | |
|------|-----------------------------------|
| 構文説明 | <i>source-url</i> 取得するアップグレードの場所。 |
|------|-----------------------------------|

| | |
|-------|---------------------|
| デフォルト | デフォルトの動作または値はありません。 |
|-------|---------------------|

| | |
|---------|------------------|
| コマンドモード | グローバルコンフィギュレーション |
|---------|------------------|

| | |
|---------------|-----|
| サポートされるユーザロール | 管理者 |
|---------------|-----|

| コマンド履歴 | リリース | 修正 |
|--------|--------|------------|
| | 4.0(1) | このコマンドを導入。 |

使用上のガイドライン コマンドラインから、すべての必要なソースおよび宛先 URL 情報とユーザ名を入力できます。コマンド (**upgrade**) の後にプレフィックス (ftp: または scp:) だけを入力した場合は、適用されるパスワードを含む、不足している情報についてのプロンプトが表示されます。

ディレクトリは、必要なファイルへの絶対パスで指定する必要があります。アップグレードを繰り返す場合は、ファイル名を指定しないでください。指定した曜日の指定した時間に、繰り返しアップグレードを行うようにセンサーを設定できます。または、最初のアップグレードから指定した時間が経過した後で繰り返しアップグレードを行うように設定できます。

ソースを指定する場合は、次のガイドラインに従います。

- **ftp:** : FTP ネットワーク サーバのソース URL。このプレフィックスの構文は、
ftp:[[/username@]location]/relativeDirectory/filename または
ftp:[[/username@]location]//absoluteDirectory/filename です。
- **http:** : Web サーバのソース URL。このプレフィックスの構文は、
http:[[/username@]location]/directory/filename です。
- **https:** : Web サーバのソース URL。このプレフィックスの構文は、
https:[[/username@]location]/directory/filename です。



(注) HTTPS プロトコルを使用するには、TLS を使用する信頼できるホストをセットアップする必要があります。詳細については、コマンドを参照してください。

- **scp:** : SCP ネットワーク サーバのソース URL。このプレフィックスの構文は、
scp:[[/username@]location]/relativeDirectory/filename または
scp:[[/username@]location]//absoluteDirectory/filename です。



(注) このコマンドは、Cisco IOS 12.0 以前にはありません。

例 次の例は、センサーに対して、指定されたアップグレードをすぐに確認するよう指示します。ディレクトリとパスは tester のユーザ アカウントを基準とします。

```
sensor(config)# upgrade scp://tester@10.1.1.1/upgrade/sp.rpm
Enter password: *****
Re-enter password: *****
```

username

ローカル センサーのユーザを作成するには、グローバル コンフィギュレーション モードで `username` コマンドを使用します。ユーザを作成するには、管理者になる必要があります。このコマンドを `no` 形式で使用すると、センサーからユーザを削除できます。この場合、ユーザは CLI と Web アクセスの両方から削除されます。

```
username name [password password] [privilege privilege]
```

```
no username name
```

構文説明

| | |
|------------------|---|
| <i>name</i> | ユーザ名を指定します。有効なユーザ名の長さは 1 ~ 64 文字です。ユーザ名の先頭は、英数字にする必要があります。その他の文字には、すべての文字を使用できます。 |
| <i>password</i> | ユーザのパスワードを指定します。有効なパスワードの長さは 6 ~ 32 文字です。スペースおよび「?」以外のすべての文字を使用できます。 |
| <i>privilege</i> | ユーザの権限レベルを指定します。使用できるレベルは、サービス、管理者、オペレータ、ビューアで、デフォルトはビューアです。 |

デフォルト

「構文説明」の表を参照してください。

コマンドモード

グローバル コンフィギュレーション

サポートされるユーザロール

管理者

コマンド履歴

| リリース | 修正 |
|--------|------------|
| 4.0(1) | このコマンドを導入。 |

使用上のガイドライン

`username` コマンドを使用すると、ログインだけを目的としたユーザ名またはパスワード、またはその両方を認証できます。このコマンドを実行しているユーザは、自分自身を削除できません。

コマンドラインでパスワードを指定しなかった場合は、プロンプトが表示されます。`password` コマンドを使用すると、現行ユーザまたはシステムの既存のユーザのパスワードを変更できます。`privilege` コマンドを使用すると、システムの既存のユーザの権限を変更できます。

■ username

例 次の例は、ビューアレベルの権限とパスワード testpassword を持つユーザ tester を追加します。

```
sensor(config)# username tester password testpassword
```

次の例は、入力パスワードが保護されていることを示します。

```
sensor(config)# username tester
Enter Login Password: *****
Re-enter Login Password: *****
```

次の例は、ユーザ「tester」の権限をオペレータに変更します。

```
sensor(config)# username tester privilege operator
```

関連コマンド

| コマンド | 説明 |
|-----------|------------------------|
| password | ローカル センサーのパスワードを更新します。 |
| privilege | 既存のユーザの権限レベルを変更します。 |



非推奨コマンドおよびコマンドとプラットフォームの依存関係

この付録では、推奨されなくなったコマンドと、特定のプラットフォームに適用されないコマンドの一覧を示します。

この付録には、次の項があります。

- [非推奨コマンド \(P.A-2\)](#)
- [コマンドとプラットフォームの依存関係 \(P.A-2\)](#)

非推奨コマンド

表 A-1 に、IPS 5.1 で推奨されなくなったコマンドの一覧を示します。

表 A-1 非推奨コマンド

| コマンド | 置換コマンド |
|--------------------------------------|---|
| hostname | service host – network-settings – host-name |
| ip address | service host – network-settings – host-ip |
| ip default-gateway | service host – network-settings – host-ip |
| interface command-control | service host |
| telnet-sensor | service host – network-settings – telnet-option |
| interface group | service analysis-engine – virtual-sensor |
| interface sensing | service interface-config – physical-interfaces |
| interface sensing shutdown | service interface-config – physical-interfaces – state |
| sensing-interface | service analysis-engine – virtual-sensor – sensing-interface |
| service virtual-sensor-configuration | service signature-definition |
| service alarm-channel-configuration | service event-action-rules |
| reset-signatures | 置換はありません。個々のシグニチャまたはすべてのシグニチャをリセットするには、default キーワードを使用します。 |
| show interfaces command-control | show statistics host |
| show interfaces group | show statistics virtual-sensor。このコマンドは、仮想センサー統計情報のみを表示します。コンフィギュレーションを表示するには、more current-config または show configuration を使用します。 |
| show interfaces sensing | show interface fastethernet および show interface gigabitethernet |
| tune-micro-engines | 置換はありません。service signature-definition コマンドは、シグニチャ編集を直接開始します。 |
| tune-alarm-channel | 置換はありません。service event-action-rules コマンドは、ルール編集を直接開始します。 |

コマンドとプラットフォームの依存関係

表 A-2 は、特定のプラットフォームに無効なコマンドの一覧を示しています。

表 A-2 コマンドとプラットフォームの依存関係

| コマンド | プラットフォーム |
|----------------------------|--|
| display-serial | IDSM-2、NM-CIDS、IDS-4215、AIP SSM 10、AIP SSM 20、IPS-4240、IPS-4255 |
| clock set | IDSM-2、NM-CIDS、AIP SSM 10、AIP SSM 20 |
| show inventory | IDSM-2、NM-CIDS、IDS-4210、IDS-4235、IDS-4250、AIP SSM 10、AIP SSM 20 |
| show interfaces management | IDSM-2、NM-CIDS、IDS-4210、IDS-4215、IDS-4235、IDS-4250、AIP SSM 10、AIP SSM 20 |



CLI エラー メッセージ

この付録では、CLI エラー メッセージについて説明します。

表 B-1 は、CLI エラー メッセージを示しています。

表 B-1 CLI エラー メッセージ

| エラー メッセージ | 理由 | コマンド |
|---|--|-----------------------------------|
| Invalid command received. | .conf ファイルおよびコードが非同期です。これは実際に発生してはならない事態です。 | すべてのコマンド |
| Invalid port number was entered. | 範囲外のポート番号が URL に入力されました。 | copy、upgrade show tech-support |
| Invalid scheme was entered. | 内部テーブルが非同期です。これは実際に発生してはならない事態です。 | copy、upgrade show tech-support |
| Unknown scheme was entered. | 無効な方式が URL に入力されました。 | copy、upgrade show tech-support |
| The filename <file> is not a valid upgrade file type. | — | upgrade |
| Invalid instance name. "rules0" is currently the only instance name allowed. | サービス イベントアクションのルールに対して、無効な論理インスタンス名が入力されました。 | service event-action-rules |
| Invalid instance name. "sig0" is currently the only instance name allowed. | サービス シグニチャ定義に対して、無効な論理インスタンス名が入力されました。 | service signature-definition |
| User does not exist. | 管理者が、システムに存在しないユーザ名のパスワードの変更を試みています。 | password |
| Incorrect password for user account. | ユーザが、パスワードの変更を試みる際に無効なパスワードを入力しました。 | password |
| Empty user list. | curUserAccountList.xml ファイルにエントリが含まれていません。これは実際に発生してはならない事態です。 | username |
| User already exists. | システムにすでに存在するユーザの作成が試行されました。 | username |
| Cannot communicate with system processes. Please contact your system administrator. | 1 つ以上の必須アプリケーションが制御トランザクションに応答していません。 | すべてのコマンド |

表 B-1 CLI エラー メッセージ (続き)

| エラー メッセージ | 理由 | コマンド |
|--|--|------------------------------------|
| Source and Destination are the same. | — | copy |
| Backup config was missing. | ユーザがバックアップ コンフィギュレーション ファイルのコピーまたは消去を試みましたが、バックアップ コンフィギュレーション ファイルは生成されていません。 | copy erase |
| Could not load CLI configuration files, can not complete request. | .conf ファイルが見つかりませんでした。これは実際に発生してはならない事態です。 | copy |
| Error writing to <URL>. | 宛先に指定された URL に書き込みできませんでした。 | copy |
| Error reading from <URL>. | ソースに指定された URL から読み取りできませんでした。 | copy |
| Packet-file does not exist. | ユーザがパケット ファイルのコピーまたは消去を試みましたが、パケット ファイルは取り込まれていません。 | copy erase |
| No downgrade available. | ユーザが、アップグレードされていないシステムのダウングレードを試みました。 | downgrade |
| No packet-file available. | ユーザがファイル情報またはパケット ファイルの表示を試みましたが、パケット ファイルは存在しません。 | packet |
| Log file exists but an error occurred during read. | ユーザが、上書きされた iplog ファイルを表示またはコピーしました。一部のファイル内容は表示できます。 | packet |
| Another user is currently capturing into the packet-file.Please try again later. | — | packet capture |
| Another CLI client is currently displaying packets from the interface. | 他の CLI セッションでの表示が終了するまで、ユーザはこのコマンドを使用できません。複数のユーザがコマンド制御インターフェイスを同時に表示することがあります。 | packet display |
| Log does not exist. | ユーザが、存在しない iplog のコピーまたは表示を試みました。 | copy iplog packet display iplog |
| The requested IPLOG is not complete.Please try again after the IPLOG status is 'completed.' | ユーザが、完了していない iplog のコピーまたは表示を試みました。 | copy iplog |
| Could not create pipe /usr/cids/idsRoot/tmp/pipe_cliPacket.<pid>.tmp | iplog ファイルを送信するためのパイプを開けませんでした。これは、スペースまたはリソースの制限を示します。これは実際に発生してはならない事態です。 | copy iplog |
| The log file was overwritten while the copy was in progress.The copied log file may be viewable but is incomplete. | iplog がセンサーからコピーされている間に上書きされました。 | copy iplog |
| Could not read license file. | ライセンス ファイルはコピーされましたが、開くことができません。 | copy license-key |

表 B-1 CLI エラー メッセージ (続き)

| エラー メッセージ | 理由 | コマンド |
|--|--|------------------|
| Could not write the temporary license file location used to copy the file off the box. | 一時保管場所 /usr/cids/idsRoot/tmp/ips.lic を開くことができませんでした。これは、スペースの問題を示し、実際には発生してはならない事態です。 | copy license-key |
| Can not create an IP log.\\"vs0\" is currently the only virtual sensor allowed. | ユーザが、無効な仮想センサーに対して iplog の作成を試みました。 | iplog |
| Can not stop an IP log.\\"vs0\" is currently the only virtual sensor allowed. | ユーザが、無効な仮想センサーに対して iplog の停止を試みました。 | iplog |
| You do not have permission to terminate the requested CLI session. | オペレータまたはビューア ユーザが、別のユーザに属する CLI セッションの終了を試みました。 | clear line |
| Invalid CLI ID specified, use the 'show users all' command to view the valid CLI session IDs. | ユーザが、存在しない CLI セッションのキャンセルを試みました。 | clear line |
| The maximum allowed CLI sessions are currently open, please try again later. | オペレータまたはビューア ユーザがログインを試みましたが、最大数の CLI セッションがすでに開いています。 | initial login |
| The maximum allowed CLI sessions are currently open, would you like to terminate one of the open sessions? | 管理者ユーザがログインを試みましたが、最大数の CLI セッションがすでに開いています。 | initial login |
| Can not communicate with system processes.Please contact your system administrator. | CLI はセンサー上のアプリケーションに接続して起動情報を取得できません。これは発生してはならない重大なエラーです。サービス アカウントにログインして、手動でセンサーをリポートする必要があります。 | initial login |



GLOSSARY

A

- aaa** 認証、認可、アカウントिंग (authentication, authorization, and accounting)。Cisco IOS ソフトウェアと PIX ファイアウォールのコマンドで、ユーザがルータまたは PIX ファイアウォールにログインする方法を制御します。
- AAA** 認証、認可、アカウントING (authentication, authorization, and accounting)。「トリプルエー」と発音します。
- ACE** アクセス コントロール エントリ (Access Control Entry)。ACL 内のエントリで、指定されたアドレスまたはプロトコルに関して実行するアクションを記述します。センサーは、ACE を追加または削除してホストをブロックします。
- ACK** 確認応答 (acknowledgement)。何かのイベントが発生した場合に、1 つのネットワーク デバイスから別のネットワーク デバイスに送信される通知です (メッセージの受信など)。
- ACL** アクセス コントロール リスト (Access Control List)。ルータ経由のデータ フローを制御する ACE のリストです。ルータ インターフェイスごとに、受信データ用と送信データ用の 2 つの ACL があります。1 つの方向で同時にアクティブにできる ACL は 1 つだけです。ACL は、番号または名前で識別されず。ACL は、標準、強化、拡張のいずれかになります。センサーで ACL を管理するように設定できます。
- AIC エンジン** Application Inspection and Control エンジン。Web トラフィックの詳細な分析を行います。HTTP プロトコルの不正利用を防止するために、HTTP セッションを精密に制御します。インスタントメッセージやトンネリング アプリケーション (例 : gotomypc) など、特定のポート上でトンネリングを行うアプリケーションに対する管理制御を行います。また、FTP トラフィックを検査し、発行されるコマンドを制御します。
- AIP SSM** Advanced Inspection and Prevention Security Services Module。Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスの IPS プラグイン モジュール。「ASA」を参照。
- API** アプリケーション プログラミング インターフェイス (Application Programming Interface)。アプリケーション プログラムが通信ソフトウェアと対話を行うために使用するインターフェイス。標準化された API を使用すると、基盤となる通信方法に依存しないでアプリケーション プログラムを開発できます。コンピュータのアプリケーション プログラムは、標準的なソフトウェアの割り込み、コール、およびデータ形式のセットを実行して、他のデバイスとの接続を開始します (たとえば、ネットワーク サービス、メインフレームの通信プログラム、または他のプログラム間の通信)。一般に、API によって、ソフトウェア開発者はアプリケーションがオペレーティング システムまたはネットワークと通信するために必要なリンクを容易に作成できます。
- ARC** Attack Response Controller。以前の名称は、Network Access Controller (NAC)。IPS のコンポーネントの 1 つ。適用可能な場合にブロックおよびブロック解除の機能を提供するソフトウェア モジュール。
- ARP** アドレス レゾリューション プロトコル (Address Resolution Protocol)。IP アドレスを MAC アドレスにマッピングするために使用されるインターネット プロトコル。RFC 826 で定義されています。
- ASA** 適応型セキュリティ アプライアンス (Adaptive Security Appliance)。ASA は、ファイアウォール、VPN コンセントレータ、侵入防御ソフトウェアの機能を 1 つのソフトウェア イメージに結合します。シングルモードまたはマルチモードのいずれでも ASA を設定できます。

| | |
|--------------------------|---|
| ASDM | Adaptive Security Device Manager。ASA の設定と管理が可能な Web ベースのアプリケーションです。 |
| Atomic エンジン | ATOMIC エンジンは、2 種類あります。ATOMIC.IP は IP プロトコルおよび関連付けられているレイヤ 4 のトランスポート プロトコルを検査し、ATOMIC.ARP はレイヤ 2 の ARP プロトコルを検査します。 |
| AuthenticationApp | IPS のコンポーネントの 1 つ。ユーザが、CLI、IDM、または RDEP のアクションを実行するための適切な権限を持っていることを確認します。 |

B

| | |
|-------------|---|
| BIOS | Basic Input/Output System。センサーを起動し、センサー内のデバイスとシステムとの間で通信するプログラムです。 |
| BO2K | BackOrifice 2000。TCP および UDP 上で実行される Windows のバック ドア型トロイの木馬。 |
| Bpdu | ブリッジ プロトコル データ ユニット (Bridge Protocol Data Unit)。ネットワーク内のブリッジ間で情報を交換するために設定可能な間隔で送出される、スパニングツリー プロトコルの hello パケット。 |

C

| | |
|------------------|--|
| CA | 認証局 (certification authority)。デジタル証明書 (特に X.509 証明書) を発行し、証明書内のデータ項目間のバインディングを保証する機関です。センサーは、自己署名証明書を使用します。 |
| CA 証明書 | 別の CA によって発行された、CA の証明書。 |
| cidDump | 大量の情報を取り込むためのスクリプト。この情報には、IPS プロセスリスト、ログ ファイル、OS 情報、ディレクトリ リスト、パッケージ情報、コンフィギュレーション ファイルなどがあります。 |
| CIDEE | Cisco Intrusion Detection Event Exchange。Cisco IPS システムが使用する SDEE への拡張を指定します。CIDEE 標準は、Cisco IPS システムがサポートする可能性のあるすべての拡張を指定します。 |
| CIDS ヘッダー | IPS システム内の各パケットに付けられるヘッダー。これには、パケットの分類、パケットの長さ、チェックサムの結果、タイムスタンプ、および受信インターフェイスが含まれます。 |
| Cisco IOS | CiscoFusion アーキテクチャのすべての製品に対して、共通の機能、スケーラビリティ、およびセキュリティを提供するシスコのシステム ソフトウェア。Cisco IOS は、中央集中型で統合され自動化されたインストレーションおよびインターネットワークの管理を可能にするだけでなく、多様なプロトコル、メディア、サービス、およびプラットフォームをサポートします。 |
| CLI | コマンドライン インターフェイス (command line interface)。センサーに付属のシェルで、センサー アプリケーションの設定と制御に使用されます。 |

D

| | |
|---------------------------|---|
| Database Processor | 「DBP」を参照。 |
| DBP | データベース プロセッサ (Database Processor)。シグニチャ状態とフロー データベースを管理します。 |
| DCE | データ回線終端装置 (data circuit-terminating equipment)(ITU-T 拡張)。ユーザからネットワークへのインターフェイスのネットワーク終端を構成する、通信ネットワークのデバイスおよび接続。DCE はネットワークへの物理的接続を提供し、トラフィックを転送し、DCE デバイスと DTE デバイスとの間のデータ伝送の同期に使用するクロック信号を提供します。DCE には、モデムやインターフェイス カードなどがあります。 |

| | |
|-------------------------------|--|
| DDoS | 分散 DoS (Distributed Denial of Service)。脆弱性が生じた複数のシステムが単一の対象を攻撃した結果、対象になったシステムのユーザがサービスを拒絶されること。対象システムが受信する大量のメッセージによってシステムが強制的にシャットダウンすることにより、正当なユーザのシステムへのサービスが拒絶されます。 |
| Deny Filters Processor | 「DFP」を参照。 |
| DES | データ暗号規格 (Data Encryption Standard)。アルゴリズムではなく 56 ビット キーを基盤とする、強力な暗号化方式。 |
| DFP | Deny Filters Processor。拒否攻撃者機能を処理します。拒否された送信元 IP アドレスのリストを管理します。 |
| DIMM | デュアル インライン メモリ モジュール (Dual In-line Memory Modules)。 |
| DMZ | 非武装地帯 (demilitarized zone)。プライベート ネットワーク (内部) とパブリック ネットワーク (外部) との間の中立地帯にある別個のネットワーク。 |
| DNS | ドメイン ネーム システム (Domain Name System)。インターネット全体にわたるホスト名と IP アドレスのマッピングです。DNS を使用すると、人間が読める形式の名前を、ネットワーク パケットで必要とされる IP アドレスに変換できます。 |
| DoS | サービス拒絶 (Denial of Service)。特定のシステムまたはネットワークの操作を混乱させることを目的とする攻撃です。 |
| DRAM | ダイナミック ランダム アクセス メモリ (dynamic random-access memory)。キャパシタに情報を保存する RAM のことで、定期的リフレッシュする必要があります。DRAM がコンテンツをリフレッシュするときは、プロセッサがアクセスできないため、遅延が発生します。ただし、DRAM は SRAM に比べて複雑ではなく、容量も大きくなっています。 |

E

| | |
|-------------------|--|
| ESD | 静電放電 (electrostatic discharge)。静電放電は、1 つの物体から別の物体への急速な電荷の移動により、数千ボルトの電荷が発生することを指します。電気的コンポーネントやサーキット カード アセンブリ全体に重大なダメージを引き起こす場合があります。 |
| Ethereal | Ethereal は、フリーの UNIX および Windows 用ネットワーク プロトコル アナライザです。これを使用すると、稼働中のネットワークのデータ、またはディスク上のキャプチャ ファイルのデータを検査できます。対話的にキャプチャ データをブラウズし、各パケットの要約情報と詳細情報を表示できます。Ethereal には、機能豊富な表示フィルタ言語や TCP セッションの再構築されたストリームの表示機能など、いくつかの強力な機能があります。詳細については、 http://www.ethereal.com を参照してください。 |
| evIdsAlert | イベントストアに書き込まれる、アラートを表す XML エンティティ。 |

F

| | |
|--------------------------------------|---|
| false negative | 不正なトラフィックが検出されたときにシグニチャが起動されない状態。 |
| false positive | 正常なトラフィックまたは良好なアクションによってシグニチャが起動される状態。 |
| Flood エンジン | ホストおよびネットワークを宛先とする ICMP および UDP フラッドを検出します。 |
| Fragment Reassembly Processor | 「FRP」を参照。 |

| | |
|----------------|--|
| FRP | Fragment Reassembly Processor。フラグメント化された IP データグラムを再構成します。センサーがインライン モードの場合、IP フラグメントの正規化も処理します。 |
| FTP | ファイル転送プロトコル (File Transfer Protocol)。TCP/IP プロトコル スタックの一部であるアプリケーション プロトコルで、ネットワーク ノード間のファイル転送に使用されます。FTP は、RFC 959 で定義されています。 |
| FTP サーバ | ファイル転送プロトコル (File Transfer Protocol) サーバ。ネットワーク ノード間のファイルの転送に FTP プロトコルを使用するサーバ。 |
| FWSM | Firewall Security Module。Catalyst 6500 シリーズ スイッチにインストールできるモジュール。ブロックするには <code>shun</code> コマンドを使用します。シングルモードまたはマルチモードのいずれでも FWSM を設定できます。 |

G

| | |
|------------|---|
| GMT | グリニッジ標準時 (Greenwich Mean Time)。経度 0 の時間帯。現在では、世界標準時 (UTC) と呼ばれます。 |
|------------|---|

H

| | |
|----------------|---|
| H.225.0 | H.225.0 セッションの確立とパケット化を規定する ITU 標準。実際に、H.225.0 は RAS、Q.931 の使用、RTP の使用など、いくつかの異なるプロトコルを定めています。 |
| H.245 | H.245 エンドポイントの制御を規定する ITU 標準。 |
| H.323 | 異種の通信デバイスが、標準化された通信プロトコルを使用して、相互に通信できます。H.323 は、CODEC の共通セット、コール セットアップとネゴシエーションの手順、および基本的なデータ転送方法を定義します。 |
| HTTP | ハイパーテキスト転送プロトコル (Hypertext Transfer Protocol)。IPS アーキテクチャでリモート データ交換に使用される、ステートレスな要求 / 応答メディア転送プロトコルです。 |
| HTTPS | 標準 HTTP プロトコルを拡張したもので、Web サイトからのトラフィックを暗号化することによって機密保持を可能にします。デフォルトでは、このプロトコルは TCP ポート 443 を使用します。 |

I

| | |
|------------------|---|
| ICMP | インターネット制御メッセージ プロトコル (Internet Control Message Protocol)。ネットワーク層のインターネット プロトコルで、エラーを報告し、IP パケット処理に関するその他の情報を提供します。RFC 792 で定義されています。 |
| ICMP フラッド | プロトコルの実装で処理可能な数を超える多数の ICMP エコー要求 (ping) パケットをホストに送信する DoS 攻撃。 |
| IDAPI | 侵入検知アプリケーション プログラミング インターフェイス (Intrusion Detection Application Programming Interface)。IPS アーキテクチャ アプリケーション間に単純なインターフェイスを提供します。IDAPI はイベント データを読み書きし、制御トランザクションのメカニズムを提供します。 |
| IDCONF | Intrusion Detection Configurariion。侵入検知システムおよび侵入防御システムの設定に使用される操作メッセージを定義するデータ形式の規格です。 |
| IDIOM | Intrusion Detection Interchange and Operations Messages。侵入検知システムによって報告されるイベントメッセージ、および侵入検知システムの設定と制御に使用される操作メッセージを定義するデータ形式の規格です。 |

| | |
|------------------------|---|
| IDM | IPS Device Manager。センサーの設定と管理が可能な Web ベースのアプリケーションです。IDM の Web サーバはセンサーに常駐します。この Web サーバには、Netscape または Internet Explorer などの Web ブラウザでアクセスできます。 |
| IDMEF | Intrusion Detection Message Exchange Format。IETF Intrusion Detection Working Group による標準草案です。 |
| IDS-2 | 侵入検知システム モジュール (Intrusion Detection System Module)。Catalyst 6500 シリーズ スイッチで侵入検知を実行するスイッチング モジュールです。 |
| IDS MC | Management Center for IDS Sensors。Web ベースの IDS マネージャで、最大 300 台のセンサーのコンフィギュレーションを管理できます。 |
| IP アドレス | TCP/IP を使用しているホストに割り当てられる 32 ビットのアドレス。IP アドレスは、5 つのクラス (A、B、C、D、または E) のいずれかに属し、ピリオドで区切られた 4 つのオクテット (ドット付き 10 進形式) で記述されます。各アドレスは、ネットワーク番号、サブネットワーク番号 (オプション) およびホスト番号で構成されます。ネットワーク番号とサブネットワーク番号は、ともにルーティングに使用され、ホスト番号はネットワークまたはサブネットワーク内の個々のホストのアドレス指定に使用されます。サブネット マスクは、IP アドレスからネットワーク情報およびサブネットワーク情報を取り出すために使用されます。 |
| IP スプーフィング | IP スプーフィング攻撃は、ネットワーク外の攻撃者が信頼されたユーザになりすますことによって発生します。攻撃者は、ネットワークの IP アドレス範囲内の IP アドレスを使用するか、信頼され、ネットワーク上の指定されたリソースへのアクセスが可能な、許可された外部 IP アドレスを使用して、このなりすましを行います。攻撃者が IPSec セキュリティ パラメータにアクセスした場合は、その攻撃者が企業ネットワークへのアクセスを許可されたリモート ユーザを偽装する可能性があります。 |
| iplog | 指定されたアドレスとの間でやり取りされるバイナリ パケットのログ。iplog は、シグニチャに log EventAction が選択されている場合に作成されます。iplog は、Ethereal または TCPDump で読み取り可能な libpcap 形式で格納されます。 |
| IPS | 侵入防御システム (Intrusion Prevention System)。ネットワーク トラフィックの分析技術を使用して、ネットワークへの侵入の存在をユーザに警告するシステムです。 |
| IPS データまたはメッセージ | IPS アプリケーション間でコマンド / コントロール インターフェイスを介して転送されるメッセージ。 |
| IPv6 | IP version 6。現在のバージョンの IP (version 4) に置き換えられます。IPv6 では、パケットヘッダー内のフロー ID がサポートされます。これは、フローを識別するために使用されます。以前の名称は、IPng (next generation) です。 |

L

| | |
|--------------------------|--|
| L2P | Layer 2 Processor。レイヤ 2 関連イベントを処理します。また、異常形式のパケットを識別し、処理パスから削除します。 |
| Layer 2 Processor | 「L2P」を参照。 |
| Logger | IPS のコンポーネントの 1 つ。 |
| LOKI | リモート アクセスのバック ドア型トロイの木馬。ICMP トンネリング ソフトウェア。コンピュータが感染すると、悪質なコードによって、小さなペイロードの ICMP 応答を送信するために使用する ICMP トンネルが作成されます。 |

M

| | |
|-------------------|--|
| MainApp | IPS のメイン アプリケーション。オペレーティング システムのブート後、センサーで最初に起動するアプリケーションです。 |
| MD5 | Message Digest 5。128 ビット ハッシュを作成する単方向のハッシュ アルゴリズム。MD5 と Secure Hash Algorithm (SHA) は、MD4 のバリエーションで、MD4 ハッシュ アルゴリズムのセキュリティを強化したものです。シスコでは、IPSec フレームワーク内の認証にハッシュを使用しています。また、SNMP v.2 のメッセージ認証にも使用します。MD5 は、通信の整合性を確認し、発信元を認証して、適時性をチェックします。 |
| MEG | Mega Event Generator。META エンジンに基づいたシグニチャ。META エンジンは、アラームをパケットではなく入力と見なします。 |
| Meta エンジン | スライドする時間間隔内で、関連する方法で発生するイベントを定義します。このエンジンは、パケットではなくイベントを処理します。 |
| MIB | 管理情報ベース (Management Information Base)。SNMP や CMIP などのネットワーク管理プロトコルによって使用および保守される、ネットワーク管理情報のデータベース。MIB オブジェクトの値は、SNMP コマンドや CMIP コマンドを使用して、通常は GUI ネットワーク管理システムを通じて変更または取得できます。MIB オブジェクトは、public (標準) ブランチおよび private (独自仕様) ブランチを含むツリー構造で構成されています。 |
| MIME | 多目的インターネットメール拡張 (Multipurpose Internet Mail Extension)。インターネットメールで非テキストデータ (プレーン ASCII コードでは表現できないデータ) を伝送する場合の標準。たとえば、バイナリ、外国語テキスト (ロシア語、中国語など)、オーディオ、ビデオなどのデータがあります。MIME は、RFC 2045 で定義されています。 |
| MSFC、MSFC2 | Multilayer Switch Feature Card。Catalyst 6000 スーパーバイザ エンジンのオプションカードで、スイッチの L3 ルーティングを実行します。 |
| MSRPC | マイクロソフト リモート プロシージャ コール (Microsoft Remote Procedure Call)。 |

N

| | |
|-------------------------|---|
| NAC | Network Access Controller。「ARC」を参照。 |
| NAT | Native Address Translation。ネットワーク デバイスが外部ネットワークに対してホストの実際の IP アドレスとは異なる IP アドレスを提示できるしくみ。 |
| NBD | 翌営業日 (Next Business Day)。シスコとのサービス契約に従って交換のハードウェアを配送します。 |
| never block アドレス | ブロックされることのないように指定したホストおよびネットワーク。 |
| never shun アドレス | 「never block アドレス」を参照。 |
| NIC | ネットワーク インターフェイス カード (Network Interface Card)。コンピュータ システムとの間でやり取りされるネットワーク通信機能を提供するボード。 |
| NM-CIDS | IPS の機能を支社のルータに統合するネットワーク モジュール。 |
| NMS | ネットワーク管理システム (network management system)。ネットワークの少なくとも一部分の管理に責任を負うシステム。一般に NMS には、エンジニアリング ワークステーションなどの比較的高性能、高機能のコンピュータが使用されます。NMS はエージェントと通信して、ネットワークの統計情報やリソース情報を把握します。 |
| Normalizer エンジン | IP および TCP の NORMALIZER がどのように機能するかを設定し、IP および TCP の NORMALIZER に関連するシグニチャ イベントの設定を行います。 |

| | |
|------------------------|---|
| NSDB | Network Security Database。IPS が使用するシグニチャと、そのシグニチャの根拠となっている脆弱性を説明したセキュリティ情報のデータベースです。NSDB には、センサーで検出可能な各攻撃シグニチャの説明が含まれます。 |
| NTP | ネットワーク タイム プロトコル (Network Timing Protocol)。TCP 上に構築されたプロトコルで、インターネット上にあるラジオおよびアトミック クロックを参照して正確なローカル タイムを維持します。このプロトコルでは、分散されたクロックを長期にわたりミリ秒以内のレベルで同期させることができます。 |
| NTP サーバ | ネットワーク タイム プロトコル (Network Timing Protocol) サーバ。NTP を使用するサーバ。NTP は、TCP 上に構築されたプロトコルで、インターネット上にあるラジオおよびアトミック クロックを参照して正確なローカル タイムを維持します。このプロトコルでは、分散されたクロックを長期にわたりミリ秒以内のレベルで同期させることができます。 |
| NVRAM | 不揮発性読み取り / 書き込みメモリ (Non-Volatile Read/Write Memory)。RAM は、ユニットの電源が切られた後も内容を保持します。 |
| <hr/> | |
| O | |
| OIR | 活性挿抜 (online insertion and removal)。システムの電源を切ったり、コンソール コマンドを入力したり、他のソフトウェアまたはインターフェイスをシャットダウンしないで、カードの追加、交換、または取り外しを可能にする機能です。 |
| <hr/> | |
| P | |
| PASC ポートスプーフィング | ファイアウォールを通過し、保護された FTP サーバを経由して FTP 以外のポートに接続しようとする試み。これは、認証されていない接続を開始することにより、ファイアウォールが FTP 227 (パッシブモードに入る) コマンドを誤って解釈した場合に発生します。 |
| PAT | ポート アドレス変換 (Port Address Translation)。NAT より制限された変換方式で、1 つの IP アドレスと複数の異なるポートを使用してネットワークのホストを表します。 |
| PCI | 周辺コンポーネント インターフェイス (Peripheral Component Interface)。Intel ベースのコンピュータで、最も一般的に使用されている周辺拡張バス。 |
| PDU | プロトコル データ ユニット (protocol data unit)。OSI の用語で、パケットを表します。「BPDU」、「パケット」も参照。 |
| PEP | Cisco Product Evolution Program。センサーの PID、VID、および SN から構成される UDI 情報です。PEP は、電子的なクエリー、製品ラベル、および出荷項目などを通じて、ハードウェア バージョンおよびシリアル番号を示します。 |
| PER | 圧縮符号化規則 (packed encoding rules)。PER は、一般的なスタイルを使用して同じ方法ですべてのタイプを符号化するのではなく、日付タイプに基づいて符号化し、よりコンパクトな表現を生成します。 |
| PFC | ポリシー フィーチャ カード (Policy Feature Card)。Catalyst 6000 スーパーバイザ エンジンのオプションカードで、VACL パケットのフィルタリングをサポートします。 |
| PID | Product Identifier。注文可能な製品の識別番号。UDI の 3 つの部分の 1 つです。UDI は、PEP ポリシーの一部です。 |
| PING | packet internet groper。ICMP の echo メッセージとその応答。ネットワーク デバイスへの到達状況をテストするために、IP ネットワークでよく使用されます。 |
| PIX ファイアウォール | Private Internet Exchange Firewall。シスコのネットワーク セキュリティ デバイスで、プログラミングによってネットワーク間でアドレスとポートをブロックしたり使用可能にしたりできます。 |

| | |
|-----------------|---|
| PKI | 公開鍵インフラストラクチャ (Public Key Infrastructure) 。クライアントの X.509 証明書を使用した HTTP クライアントの認証です。 |
| POST | パワーオンセルフテスト (Power-On Self Test) 。デバイスに電源が投入されたときに、ハードウェア デバイスで実行されるハードウェア診断のセット。 |
| Post-ACL | ARC が ACL エントリを読み取り、ブロックされているアドレスのすべての拒否エントリの後ろにエントリを入れる ACL を指定します。 |
| Pre-ACL | ARC が ACL エントリを読み取り、ブロックされているアドレスのすべての拒否エントリの前にエントリを入れる ACL を指定します。 |

Q

| | |
|--------------|--|
| Q.931 | ISDN ネットワーク接続の確立、保持、および終了のシグナリングを行う ITU-T の仕様。 |
|--------------|--|

R

| | |
|---------------|--|
| RAM | ランダムアクセス メモリ (random-access memory) 。マイクロプロセッサによる読み取りと書き込みが可能な揮発性メモリ。 |
| RAS | Registration, Admission, and Status プロトコル。管理機能を実行するために、エンドポイントとゲートキーパーの間で使用されるプロトコル。RAS シグナリング機能は、登録、許可、帯域幅の変更、ステータス、および VoIP ゲートウェイとゲートキーパー間の接続解除手順を実行します。 |
| RDEP2 | Remote Data Exchange Protocol version 2。コマンド / コントロール ネットワーク上で HTTP と TLS を使用してリモート データ交換を行うための公開仕様です。 |
| regex | 「正規表現」を参照。 |
| ROMMON | Read-Only-Memory Monitor。復旧のためにシステム イメージをセンサーに TFTP 転送できます。 |
| RPC | リモート プロシージャ コール (remote-procedure call) 。クライアント / サーバ コンピューティングの技術的基盤。RPC は、クライアントで生成または指定されるプロシージャ コールで、サーバで実行され、結果はネットワーク経由でクライアントに返されます。 |
| RR | リスク評価 (Risk Rating) 。RR は、ネットワーク上の特定のイベントに関連付けられたリスクを、0 から 100 の間の数値で表した評価です。 |
| RSM | Router Switch Module。Catalyst 5000 スイッチにインストールされているルータ モジュール。スタンドアロン ルータとまったく同様に機能します。 |
| RTP | リアルタイム転送プロトコル (Real-Time Transport Protocol) 。一般に、IP ネットワークで使用されます。RTP は、アプリケーションがリアルタイムにデータを転送できるように、エンドツーエンドのネットワーク転送機能を提供することを目的に設計されています。RTP は、オーディオ、ビデオ、シミュレーション データなどのリアルタイム データをマルチキャストまたはユニキャストのネットワーク サービスとして転送します。RTP は、ペイロード タイプの識別、シーケンス番号付け、タイムスタンプの付加、およびリアルタイム アプリケーションへのモニタリング送信などのサービスを提供します。 |
| RU | ラック単位 (rack unit) 。ラックはラック単位で測定されます。1 RU は 44 Mm または 1.75 インチに相当します。 |

S

| | |
|--|---|
| SAP | Signature Analysis Processor。ストリーム ベースでなく、処理中のパケットのために設定されているインスペクタにパケットを送信します。 |
| SCEP | Simple Certificate Enrollment Protocol。PKCS#7 および PKCS#10 の使用によって既存のテクノロジーを活用した、シスコシステムズの PKI 通信プロトコルです。SCEP は進化した登録プロトコルです。 |
| SDEE | Security Device Event Exchange。セキュリティ デバイス イベントの通信を行うための、製品に依存しない標準。RDEP の拡張です。各種のセキュリティ デバイスによって生成された通信イベントに必要な拡張機能を追加します。SDEE プロトコルの詳細については、 http://www.icsalabs.com/html/communities/ids/sdee/index.shtml を参照してください。 |
| SDP | Slave Dispatch Processor。 |
| SEAF | シグニチャ イベント アクション フィルタ (signature event action filter)。シグニチャ イベントのシグニチャ ID、アドレス、および RR に基づいてアクションを削除します。SEAF へ入力するのは、SEAO によって追加される可能性のあるアクションを持つシグニチャ イベントです。 |
| SEAH | シグニチャ イベント アクション ハンドラ (signature event action handler)。要求されたアクションを実行します。SEAH から出力されるのは、実行中のアクションだけでなく、イベントストアに書き込まれる <evIdsAlert> である可能性があります。 |
| SEAO | シグニチャ イベント アクション オーバーライド (signature event action override)。RR 値に基づいて、アクションを追加します。SEAO は、設定済みの RR しきい値の範囲に該当するすべてのシグニチャに適用されます。各 SEAO は独立しており、各アクション タイプには別個の値が設定されています。 |
| SEAP | シグニチャ イベント アクション プロセッサ (Signature Event Action Processor)。イベント アクションを処理します。イベント アクションはイベント リスク評価 (RR) しきい値と関連付けできます。アクションが実行されるには、このしきい値を超える必要があります。 |
| Security Monitor | Monitoring Center for Security。ネットワーク デバイスに、イベントの収集、表示、およびレポート実行の機能を提供します。IDS MC とともに使用されます。 |
| SensorApp | IPS のコンポーネントの 1 つ。パケットの取り込みと分析を実行します。SensorApp はネットワークトラフィックを分析して悪意のあるコンテンツを探します。パケットは、プロセッサのパイプラインを通過します。このパイプラインは、設計者がセンサー上のネットワーク インターフェイスからパケットを収集するように設計します。Sensorapp は、分析エンジンを実行するスタンドアロンの実行ファイルです。 |
| Service エンジン | DNS、FTP、H255、HTTP、IDENT、MS RPC、MS SL、NTP、RPC、SMB、SNMP、および SSH など、特定のプロトコルを処理します。 |
| session コマンド | ルータとスイッチに対して使用されるコマンドで、ルータまたはスイッチ内のモジュールに対して Telnet またはコンソールのいずれかによるアクセスを提供します。 |
| shun コマンド | 新しい接続を防止し、既存の全接続からのパケットを許可しないことにより、攻撃中のホストへの動的な対応を可能にします。PIX Firewall によるブロッキング時に ARC によって使用されます。 |
| Signature Analysis Processor | 「SAP」を参照。 |
| signature event action filter | 「SEAF」を参照。 |
| signature event action handler | 「SEAH」を参照。 |
| signature event action override | 「SEAO」を参照。 |

| | |
|---|--|
| signature event action processor | 「SEAP」を参照。 |
| Slave Dispatch Processor | 「SDP」を参照。 |
| SMB | サーバメッセージブロック (Server Message Block)。データをパッケージ化し、他のシステムと情報を交換するために LAN マネージャおよび同様の NOS が使用するファイルシステム プロトコル。 |
| SMTP | シンプル メール転送プロトコル (Simple Mail Transfer Protocol)。電子メール サービスを提供するインターネット プロトコル。 |
| SN | シリアル番号 (Serial Number)。UDI の一部。SN は、ご使用のシスコ製品のシリアル番号です。 |
| SNMP | 簡易ネットワーク管理プロトコル (Simple Network Management Protocol)。TCP/IP ネットワークでほとんど独占的に使用されているネットワーク管理プロトコル。SNMP は、ネットワーク デバイスのモニタリングおよび制御、コンフィギュレーション、統計情報の収集、パフォーマンス、セキュリティの管理を行う手段を提供します。 |
| SNMP2 | SNMPv2。ネットワーク管理プロトコルのバージョン 2。SNMP2 は、中央集中型および分散型のネットワーク管理戦略をサポートし、SMI、プロトコル操作、管理アーキテクチャ、およびセキュリティにおいて改善されています。 |
| SP | Statistics Processor。パケット カウントおよびパケット到着率などのシステム統計情報を追跡します。 |
| SPAN | スイッチド ポート アナライザ (Switched Port Analyzer)。Catalyst 5000 スイッチの機能。既存のネットワーク アナライザの監視機能をスイッチ型イーサネット環境に拡張します。SPAN は、1 つのスイッチド セグメントのトラフィックを事前定義済みの SPAN ポートにミラーリングします。SPAN ポートに接続されたネットワーク アナライザで、その他の任意の Catalyst スイッチド ポートからのトラフィックを監視できます。 |
| SQL | 構造化照会言語 (Structured Query Language)。リレーショナル データベースの定義およびアクセスに使用する国際的な標準言語。 |
| SRAM | RAM の一種。電源が供給されている限り、内容を保持します。SRAM は、DRAM のように定期的なリフレッシュは必要ありません。 |
| SRP | Stream Reassembly Processor。さまざまなストリームベース インспекタでパケットが適切な順序で到着するよう、TCP ストリームを並べ替えます。また、TCP ストリームの正規化も行います。正規化エンジンを使用すると、アラートおよび拒否アクションを有効または無効にできます。 |
| SSH | Secure Shell。強力な認証と安全な通信を使用してネットワーク上の別のコンピュータにログインするユーティリティ。 |
| SSL | Secure Socket Layer。e- コマースにおけるクレジットカード番号の転送など、安全なトランザクションを提供するために使用されるインターネット用暗号化テクノロジー。 |
| Stacheldraht | ICMP プロトコルに依存する DDoS ツール。 |
| State エンジン | HTTP スtring のステートフル検索。 |
| Statistics Processor | 「SP」を参照。 |
| Stream Reassembly Processor | 「SRP」を参照。 |
| String エンジン | シグニチャ エンジン の 1 つ。正規表現ベースのパターン検査、および TCP、UDP、ICMP などの複数の転送プロトコルのアラート機能を提供します。 |
| SYN フラッド | プロトコルの実装で処理可能な数を超える多数の TCP SYN パケット (接続開始時に使用されるシーケンス番号の同期化要求) をホストに送信する DoS 攻撃。 |

T

| | |
|--------------------------|---|
| TAC | Cisco Technical Assistance Center。TAC は、世界中に 4 箇所にあります。 |
| TACACS+ | Terminal Access Controller Access Control System Plus。シスコが強化した専用の Terminal Access Controller Access Control System (TACACS)。認証、認可、アカウントングに追加サポートを提供します。 |
| TCP | 伝送制御プロトコル (Transmission Control Protocol)。信頼性の高い全二重データ伝送を可能にする、コネクション型トランスポート層プロトコル。TCP は、TCP/IP プロトコル スタックの一部です。 |
| tcpdump | tcpdump コーティリティは、フリーの UNIX および Windows 用ネットワーク プロトコル アナライザです。これを使用すると、稼働中のネットワークのデータ、またはディスク上のキャプチャ ファイルのデータを検査できます。さまざまなオプションを使用して、各パケットの要約情報と詳細情報を表示できます。詳細については、 http://www.tcpdump.org/ を参照してください。 |
| TCP リセット インターフェイス | TCP リセットを送信できる、IDS-4250-XL および IDSM-2 上のインターフェイス。ほとんどのセンサーでは、パケットが監視されるセンシング インターフェイスと同じインターフェイスで TCP リセットが送信されますが、IDS-4250-XL と IDSM-2 では、センシング インターフェイスを TCP リセットの送信に使用することができません。IDS-4250-XL では、オンボードの 10/100/100 TX インターフェイスが TCP リセット インターフェイスになります。このインターフェイスは、通常、XL カードが存在しない場合に IDS-4250-TX アプライアンスで使用されます。IDSM-2 の場合、TCP リセット インターフェイスは、Catalyst ソフトウェアでポート 1 として指定され、Cisco IOS ソフトウェアのユーザには表示されません。TCP リセット アクションは、TCP ベースのサービスに関連するシグニチャ上のアクションとして選択したときだけ有効なアクションとなります。 |
| Telnet | TCP/IP プロトコル スタックにおける標準の端末エミュレーション プロトコル。Telnet はリモート端末接続に使用され、ユーザはこれを使用してリモート システムにログインし、そのリソースを、ローカル システムに接続されているかのように使用することができます。Telnet は RFC 854 で定義されています。 |
| TFN2K | Tribe Flood Network 2000。一般的なタイプの DoS 攻撃。偽造した送信元 IP アドレスを利用するか、または送信元 IP アドレスを素早く変更して、攻撃の特定やフィルタリングを攻撃者が阻止できます。 |
| TFTP | Trivial File Transfer Protocol。FTP の単純なバージョンで、1 つのコンピュータから別のコンピュータに、通常はクライアント認証 (ユーザ名とパスワードなど) を使用せずにネットワークを介してファイルを転送できます。 |
| Time Processor | 「TP」を参照。 |
| TLS | Transport Layer Security。ピアの ID をネゴシエートし、暗号化通信を確立するために、ストリーム転送で使用されるプロトコル。 |
| TP | Time Processor。タイムスライス カレンダーに格納されたイベントを処理します。主なタスクは、古いデータベース エントリを有効期限切れにすること、および時間に依存する統計情報を計算することです。 |
| TPKT | パケット内のメッセージのマーキングを解除するための RFC 1006 によって定義された方式。 |
| traceroute | パケットが宛先に到達するまでに通過するパスをトレースするプログラムのことで、多数のシステムで使用可能です。主に、ホスト間のルーティング問題をデバッグする際に使用されます。traceroute プロトコルは、RFC 1393 でも定義されています。 |
| Traffic ICMP エンジン | TFN2K、LOKI、および DDOS など、非標準のプロトコルからのトラフィックを分析します。 |
| Trojan エンジン | BO2K および TFN2K など、非標準のプロトコルからのトラフィックを分析します。 |

U

- UDI** Unique Device Identifier。シスコの各製品を一意に識別できます。UDI は、PID、VID、および SN から構成されています。UDI は、Cisco IPS ID PROM に保存されています。
- UDP** ユーザ データグラム プロトコル (User Datagram Protocol)。TCP/IP プロトコル スタックにおけるコネクションレス型トランスポート層プロトコル。UDP は、確認応答や配信保証を行わずにデータグラムを交換するシンプルなプロトコルで、エラー処理や再送信は他のプロトコルによって行う必要があります。UDP は RFC 768 で定義されています。
- UPS** 無停電電源 (Uninterruptable Power Source)
- UTC** 世界標準時 (Coordinated Universal Time)。経度 0 の時間帯。以前は、グリニッジ標準時 (GMT) およびズールー時 (Zulu time) と呼ばれていました。

V

- VACL** VLAN ACL。スイッチを経由して渡されるすべてのパケット (VLAN 内および VLAN 間) をフィルタリングする ACL。セキュリティ ACL とも言います。
- VID** バージョンの識別番号 (Version identifier)。UDI の一部。
- VLAN** バーチャル LAN (Virtual Local Area Network)。1 つまたは複数の LAN 上にある設定済みのデバイスのグループ (管理ソフトウェアを使用して設定)。VLAN によって、これらが実際は複数の異なる LAN セグメントに配置されていても、同一のワイヤに接続されているかのように通信できます。VLAN は物理接続ではなく論理接続に基づいており、非常に柔軟です。
- VMS** CiscoWorks VPN/Security Management Solution。さまざまな Web ベース ツールを組み合わせた、ネットワーク セキュリティ アプリケーション スイート。これらのツールは、エンタープライズ VPN、ファイアウォール、ネットワーク侵入検知システム、およびホストベースの侵入防御システムを構成、管理、およびトラブルシューティングするために使用できます。
- VoIP** Voice over IP。通常のテレフォニー型音声を、POTS に類似した機能、信頼性、および音声品質を保持して、IP ベースのインターネットで伝送する機能。VoIP は、IP ネットワーク上でルータが音声トラフィック (たとえば、電話による通話やファックス) を伝送できるようにします。VoIP では、DSP が音声信号をフレームにセグメント化し、2 つからなるグループにカップリングしてボイス パケットに格納します。これらのボイス パケットは、ITU-T 仕様 H.323 に準拠する IP を使用して伝送されます。
- VPN** バーチャル プライベート ネットワーク (Virtual Private Network(ing))。ネットワークからネットワークへのすべてのトラフィックを暗号化することにより、IP トラフィックが安全にパブリック TCP/IP ネットワーク上を送信されるようにします。VPN は「トンネリング」を使用して IP レベルのすべての情報を暗号化します。

W

- WAN** ワイドエリア ネットワーク (wide-area network)。広い地域にいるユーザ間を接続するデータ通信ネットワークで、多くの場合コモン キャリアによって提供される伝送デバイスを使用します。WAN の例としては、フレームリレー、SMDS、および X.25 などがあります。
- Web サーバ** IPS のコンポーネントの 1 つ。

X

| | |
|-------|---|
| X.509 | 証明書に含まれる情報を定義する規格。 |
| XML | eXtensible Markup Language。異種ホスト間のデータ交換に使用されるテキスト ファイル形式。 |

あ

| | |
|-----------------|--|
| アーキテクチャ | コンピュータまたは通信システムの全体的な構造。アーキテクチャは、システムの機能と制限に影響を与えます。 |
| アクション | イベントに対するセンサーの応答。アクションは、イベントがフィルタ処理されない場合にだけ発生します。可能なアクションには、TCP リセット、ホストのブロック、接続のブロック、IP ロギング、アラートトリガー パケットの取り込みなどがあります。 |
| アクティブ ACL | ARCによって作成、管理される ACL。ルータのブロック インターフェイスに適用されます。 |
| 宛先アドレス | データを受信するネットワーク デバイスのアドレス。 |
| アトミック アタック | 1 つのパケット内に組み込まれた不正利用を表します。たとえば、「ping of death」攻撃は、異常に大きな単一の ICMP パケットです。 |
| アプリケーション | Cisco IPS 環境で動作するように設計された任意のプログラム (プロセス)。 |
| アプリケーション インスタンス | IPS 環境の特定のハードウェアで動作する特定のアプリケーション。アプリケーション インスタンスには、その名前と、ホスト コンピュータの IP アドレスによってアドレス可能です。 |
| アラート | 厳密には IPS のイベント タイプの 1 つを指し、evidsAlert としてイベントストアに書き込まれます。一般に、アラートは、ネットワークの不正利用が進行中であるか、潜在的なセキュリティの問題が発生していることを示す IPS メッセージです。アラームとも言います。 |
| アラーム チャネル | インスペクタによって生成されたすべてのシグニチャ イベントを処理する IPS ソフトウェア モジュール。主な機能は、受け取った各イベントのアラートを生成することです。 |
| 暗号化 | データに特殊なアルゴリズムを適用してそのデータの外見を変更し、その情報を読む許可を与えられていないユーザには理解できないようにすること。 |
| 暗号化キー | クリア テキストと暗号文の間の変換に使用されるシークレット バイナリ データ。暗号化と復号化に同じ暗号化キーが使用される場合を対称と言います。暗号化キーが暗号化と復号化のいずれかに使用される (両方ではない) 場合を非対称と言います。 |

い

| | |
|---------------|---|
| イベント | アラート、ブロック要求、ステータス メッセージ、またはエラー メッセージを含む IPS メッセージ。 |
| イベント サーバ | IPS のコンポーネントの 1 つ。 |
| イベントストア | IPS のコンポーネントの 1 つ。IPS イベントの格納に使用される、固定サイズのインデックス付きストア。 |
| インターフェイス グループ | センシング インターフェイスの論理的なグループ。1 つの論理インターフェイス グループに複数のセンシング インターフェイスを割り当てることができます。シグニチャのパラメータは、論理インターフェイス グループごとに調整されます。 |
| インライン モード | ネットワークに出入りするすべてのパケットは、センサーを経由する必要があります。 |

う

- ウイルス** コンピュータ ソフトウェアの隠された自己複製可能なセクション。通常は悪意のあるロジックになっており、感染により増殖します。感染とは、自身のコピーを挿入して、別のプログラムの一部になることです。ウイルスは、それ自体では実行不可能です。ウイルスをアクティブにするには、ホスト プログラムが実行されている必要があります。
- ウイルス アップデート** 特にウイルスに対処するシグニチャ アップデート。

え

- エスケープ表現** 正規表現で使用されます。文字は 16 進値で表現できます。たとえば、\x61 は「a」に相当するため、\x61 は文字「a」を表すエスケープ表現になります。
- エンジン** センサーのコンポーネントの 1 つ。特定の 1 つのカテゴリで多数のシグニチャをサポートするように設計されています。各エンジンには、シグニチャの作成や既存のシグニチャの調整に使用できるパラメータがあります。
- エンタープライズ ネットワーク** 企業などの組織内で大部分の主要ポイントを接続する、大規模で多様なネットワーク。プライベートに所有および管理されるという点で、WAN とは異なります。

か

- 仮想センサー** シグニチャ エンジンのセンシング インターフェイスとコンフィギュレーション ポリシー、およびシグニチャ エンジンに適用するアラーム フィルタの論理グループ。つまり、それぞれが異なるシグニチャの動作とトラフィック供給で設定された、同一アプライアンス上で動作する複数の仮想センサーです。IPS 5.x では、1 つの仮想センサーだけがサポートされます。

き

- ギガビット イーサネット** 高速イーサネットの標準。1996 年に、IEEE (Institute of Electrical and Electronics Engineers) 802.3z 標準化委員会で承認されました。

く

- クッキー** Web サーバから Web ブラウザに送信される情報で、ブラウザによって保存されます。ブラウザは、Web サーバに対して追加要求を行うときに、Web サーバにこの情報を送り返します。

こ

- 攻撃** 知的脅威から発生するシステム セキュリティへの攻撃。セキュリティ サービスを回避してシステムのセキュリティ ポリシーを妨害するために、(特に方法や技術に関して) 用意周到に計画したうえで試みられた知的行為を意味します。
- コマンドおよびコントロール インターフェイス** IPS マネージャなどのネットワーク デバイスと通信する、センサー上のインターフェイス。このインターフェイスには IP アドレスが割り当てられています。
- コミュニティ** SNMP において、同一の管理ドメイン内にある管理対象デバイスと NMS の論理グループ。

| | |
|--------------------|--|
| 混合モード | ネットワーク セグメントのパケットを監視する受動インターフェイス。センシング インターフェイスには IP アドレスが割り当てられていないので、攻撃者には表示されません。 |
| コンソール | センサーの監視と制御に使用される端末またはラップトップ コンピュータ。 |
| コンソールポート | センサーでコンソール デバイスへの接続に使用される、RJ45 シリアルポートまたは DB9 シリアルポート。 |
| コンポジット アタック | 単一セッションで複数のパケットにまたがる攻撃です。たとえば、FTP、Telnet、およびほとんどの Regex ベース攻撃などの大部分の対話型攻撃が、これに該当します。 |

さ

| | |
|-----------------|--|
| サービス パック | 新しい機能強化を伴わないバグ フィックスのリリースに使用されます。サービス パックは、ベースバージョンのリリース (マイナーまたはメジャー) の後で、複数のプログラムが累積した形で提供されるものです。 |
| 再構成 | 送信元または中間ノードのいずれかでフラグメント化された IP データグラムを、宛先でまとめること。 |
| サブシグニチャ | 一般のシグニチャより細分化されたシグニチャ。通常は、広い範囲のシグニチャをさらに詳しく定義します。 |

し

| | |
|---------------------|---|
| しきい値 | アラームが送信されるまでに許容される最大 / 最小の条件を定義する、上限または下限の値。 |
| シグニチャ | シグニチャは、ネットワーク情報を抽出して、一般的な侵入アクティビティを示した規則セットと比較します。 |
| シグニチャ アップデート | IPS のシグニチャ分析エンジン (SensorApp) と NSDB をアップデートする実行可能イメージ。IPS シグニチャ アップデートの適用は、ウイルス スキャン プログラムでのウイルス定義の更新と似ています。シグニチャ アップデートは単独でリリースされ、独自のバージョン体系になっています。 |
| シグニチャ エンジン | センサーのコンポーネントの 1 つ。特定のカテゴリで多数のシグニチャをサポートします。エンジンは、パーサーとインスペクタで構成されています。各エンジンには規定のパラメータのセットがあり、パラメータには使用可能な範囲や値のセットがあります。 |
| システム イメージ | センサー全体のイメージの再作成に使用される、IPS アプリケーションとリカバリの完全なイメージ。 |
| 出トラフィック | ネットワークから出るトラフィック。 |
| 証明書 | ユーザまたはデバイスの属性をデジタルに表現したもの。認証可能な秘密鍵とともに署名される公開鍵などがあります。 |
| 侵入検知システム | 不正な方法によるシステム リソースへのアクセスの試みを発見し、リアルタイムまたはそれに近い形で警告を与えることを目的として、システム イベントの監視と分析を行うセキュリティ サービス。 |
| 信頼できる鍵 | ユーザが信頼する公開鍵。特に、認証パスで最初の公開鍵として使用される公開鍵。 |
| 信頼できる証明書 | 検証テストを行わずに証明書ユーザが有効であることを示す証明書。特に公開鍵証明書は、認証パスの最初の公開鍵を提供するために使用されます。 |

す

| | |
|----------------|---|
| スイッチ | 各フレームの宛先アドレスに基づいて、フレームをフィルタリング、転送、およびフラッドするネットワーク デバイス。このスイッチは、OSI モデルのデータリンク層で動作します。 |
| 据え置き | 平らな面に設置する場合は、センサー底部にゴム製脚を取り付けます。ゴム製脚を使用すると、センサーの周りに適正なエアフローが確保され、振動を吸収するので、ハードディスク ドライブへの衝撃が軽減されます。 |
| スニファ インターフェイス | 「センシング インターフェイス」を参照。 |
| スパニング ツリー | ネットワーク トポロジのループフリーのサブセット。 |
| スリーウェイ ハンドシェイク | 接続を確立する間に、2つのプロトコル エンティティが同期するプロセス。 |

せ

| | |
|----------------|---|
| 正規表現 | データ ストリームまたはファイル内で指定された文字シーケンスを検索する方法を定義できるメカニズム。正規表現は高機能かつ柔軟な表記法で、テキストを表現するためのミニプログラミング言語のようなものです。パターン照合では、正規表現によりあらゆる任意のパターンを簡潔に表記できます。 |
| 制御インターフェイス | ARC では、ネットワーク デバイスで Telnet セッションまたは SSH セッションを開くときに、そのデバイスのルーティング インターフェイスの 1 つがリモート IP アドレスとして使用されます。これが制御インターフェイスです。 |
| 制御トランザクション | 特定のアプリケーション インスタンスに対して出されたコマンドを含む IPS メッセージ。制御トランザクションには、 <i>start</i> 、 <i>stop</i> 、 <i>getConfig</i> があります。 |
| 脆弱性 | コンピュータやネットワークの悪用パターンが開始されやすい状況を許す、当該コンピュータやネットワークの 1 つ以上のアトリビュート。 |
| セキュアシェル プロトコル | Transmission Control Protocol (TCP; 伝送制御プロトコル) アプリケーションを通じて、ルータに安全なリモート接続を提供するプロトコル。 |
| 接続ブロック | ARC による、特定の送信元 IP アドレスから特定の宛先 IP アドレスおよび宛先ポートへのトラフィックのブロック。 |
| センサー | 侵入検知エンジンのことです。不正行為の兆候を探してネットワーク トラフィックを分析します。 |
| センシング インターフェイス | 目的のネットワーク セグメントを監視する、センサー上のインターフェイス。センシング インターフェイスは、混合モードです。つまり、IP アドレスを持たず、監視対象セグメント上では見えません。 |
| 全二重 | 送信端末と受信端末との間で、同時にデータを伝送する機能。 |

そ

| | |
|---------|---------------------------|
| 送信元アドレス | データを送信するネットワーク デバイスのアドレス。 |
|---------|---------------------------|

た

| | |
|-----------|--|
| ターミナル サーバ | 他のシリアル デバイスに接続された複数の低速な非同期ポートを搭載したルータ。ターミナル サーバは、センサーを含むネットワーク機器をリモートで管理する場合に利用できます。 |
|-----------|--|

ち

調整 シグニチャ パラメータを調整して既存のシグニチャを変更すること。

て

データグラム 事前にバーチャル サークットを確立することなく、伝送メディアを介してネットワーク レイヤ単位として送信される情報を論理的にグループ化すること。IP データグラムは、インターネットの主な情報単位です。また、セル、フレーム、メッセージ、パケット、およびセグメントという用語は、OSI 参照モデルやさまざまな技術領域の各種レイヤで、論理的にグループ化した情報を説明するために使用されます。

と

トポロジ エンタープライズ ネットワーク構造内のネットワーク ノードおよびメディアの物理的な配置。

トラップ 決められた条件に合致したり、しきい値を超えたりするような重大なイベントがエージェントに発生したことを示すメッセージ。SNMP エージェントから NMS、コンソール、あるいは端末に送られます。

トラフィック分析 データが暗号化されている場合、または直接使用可能でない場合にも、データ フローの観測可能な特徴から情報を推理すること。このような特徴には、送信元と宛先 (複数の場合もある) の ID と場所や、事象の存在、回数、頻度、期間などがあります。

トランク ネットワーク トラフィックが通過する 2 つのスイッチ間の物理的および論理的接続。バックボーンは、複数のトランクによって構成されています。

トランザクション サーバ IPS のコンポーネントの 1 つ。

トランザクション ソース IPS のコンポーネントの 1 つ。

トリプル DES トリプル データ暗号規格 (Triple Data Encryption Standard)、DES をより強力にしたバージョンで、SSH バージョン 1.5 のデフォルトの暗号化方式。センサーと SSH セッションを確立するときに使用されません。センサーでデバイスを管理しているときに使用できます。

に

認証 ユーザがシステムを使用する権限を持っていることを確認する処理。通常はパスワード キーまたは証明書によって行われます。

ね

ネットワーク デバイス ネットワーク上の IP トラフィックを制御し、攻撃中のホストをブロックする機能を持つデバイス。ネットワーク デバイスには、Cisco ルータや PIX ファイアウォールなどがあります。

の

ノード コマンド/コントロール ネットワーク上の物理的な通信要素。たとえば、アプライアンス、IDS/IPS、またはルータを指します。

は

バイパス モード センサーに障害が発生した場合でも、センサーを通じてパケットのフローを継続するモード。バイパスモードは、インラインで組み込まれたインターフェイスに対してのみ適用されます。

パケット 制御情報および(通常は)ユーザ データを含むヘッダーなどの情報を論理的にグループ化したもの。パケットは、ネットワーク レイヤ単位のデータを参照するために最も多く使用されます。また、データグラム、フレーム、メッセージ、およびセグメントという用語は、OSI 参照モデルやさまざまな技術領域の各種レイヤで、論理的にグループ化した情報を説明するために使用されます。

バックプレーン シャーシ内でのインターフェイス プロセッサまたはカードと、データ バスおよび電源供給バスとの間の物理的な接続。

パッシブフィンガープリント ネットワークのインタラクションを受動的に監視することにより、システムで使用可能な OS またはサービスを判別する動作。

ハンドシェイク 複数のネットワーク デバイス間で、確実に転送を同期化するために交換する一連のメッセージ。

半二重 送信端末と受信端末との間で、一度に 1 つの方向だけにデータを伝送する機能。BSC は、半二重プロトコルの例です。

ふ

ファーストイーサネット 100 Mbps イーサネット仕様の任意の数値。ファーストイーサネットは、10BaseT イーサネット仕様の 10 倍の速度を提供し、フレーム形式、MAC メカニズム、および MTU などの品質を維持します。このように 10BaseT と類似しているため、既存の 10BaseT アプリケーションやネットワーク管理ツールをファーストイーサネット ネットワークで使用できます。IEEE 802.3 仕様の拡張をベースにしています。

ファイアウォール ルータまたはアクセス サーバ、あるいは複数のルータまたはアクセス サーバ。接続されている任意のパブリック ネットワークとプライベート ネットワーク間のバッファとして指定されます。ファイアウォール ルータは、アクセス リストや他の方法を使用して、プライベート ネットワークのセキュリティを確保します。

フラグメンテーション 元のサイズのパケットを維持できないネットワーク メディア上を伝送する際に、より小さい単位にパケットを分割する処理。

フラグメント 大きなパケットの一部で、より小さい単位に分割されます。

フラッドینگ スイッチおよびブリッジが使用するトラフィック転送技術のことで、あるインターフェイスで受信されたトラフィックは、そのデバイスにおいて情報を最初に受信したインターフェイス以外のすべてのインターフェイスに送出されます。

ブロック 指定されたネットワーク ホストまたはネットワークから入ってくるすべてのパケットをネットワーク デバイスが拒否するように指定するセンサーの機能。

ブロック インターフェイス センサーが管理する、ネットワーク デバイス上のインターフェイス。

ブロック解除 それまで適用されていたブロックを削除するようにルータに指示すること。

分析エンジン センサーのコンフィギュレーションを処理する IPS ソフトウェア モジュール。インターフェイスをマップし、またシグニチャおよびアラーム チャネル ポリシーを設定済みインターフェイスにマップします。パケット分析とアラート検知を実行します。

へ

ベースバージョン サービス パックやシグニチャ アップデートなどの後続リリースをインストールするために、事前にインストールしておく必要のあるソフトウェア リリース。メジャーおよびマイナー バージョン アップグレードは、ベースバージョン リリースです。

ほ

ホスト ブロック ARC が特定 IP アドレスからのすべてのトラフィックをブロックすること。

ま

マイナー アップデート 製品ラインへの小規模な機能強化を含むマイナー バージョン。マイナー アップデートはメジャー バージョンに対する差分であり、サービス パックのベースバージョンです。

マスター ブロッキング センサー 1 つ以上のデバイスを制御するリモート センサーです。ブロッキング転送センサーがブロッキング要求をマスター ブロッキング センサーに送信し、マスター ブロッキング センサーがブロッキング要求を実行します。

マニファクチャリング イメージ イメージ センサーに対するマニファクチャリングで使用される IPS システムの完全なイメージ。

め

メジャー アップデート 製品の主要な新機能または大きなアーキテクチャ上の変更を含むベースバージョン。

メンテナンス パーティション イメージ IDSM-2 のメンテナンス パーティションのイメージの再作成に使用される IPS の完全なイメージ。

も

モジュール スイッチ、ルータ、またはセキュリティ アプライアンス シャーシの取り外しできるカード。AIP SSM、IDSM-2、および NM-CIDS は、IPS モジュールです。

モニタリング インターフェイス 「センシング インターフェイス」を参照。

ら

ラックマウント センサーを装置ラックに搭載すること。

り

リカバリパーティションイメージ アプリケーションの完全なイメージとインストーラを含む IPS イメージ ファイル。センサーで復旧に使用されます。

良性トリガー シグニチャは正しく起動されているが、トラフィックの送信元には悪意がない状態。

ろ

ロギング ログ ファイル内に、発生したアクションを収集します。セキュリティ情報のロギングは、イベント (IPS のコマンド、エラー、およびアラート) のロギングと、個々の IP セッション情報のロギングという 2 つのレベルで実行されます。

わ

ワーム 単独で実行可能なコンピュータ プログラムで、完全に動作するバージョンのプログラムを、ネットワークの他のホストに増殖させることができ、コンピュータ リソースを非常に多く消費します。



B

banner login

- 構文 2-3
- 使用方法 2-3
- 説明 2-3
- 例 2-3

C

clear denied-attackers

- 使用方法 2-4
- 説明 2-4
- 例 2-4

clear events

- 使用方法 2-5
- 説明 2-5
- 例 2-5

clear line

- 構文 2-6
- 使用方法 2-6
- 説明 2-6
- 例 2-7

CLI

- default キーワード 1-9
- エラー メッセージ B-1
- コマンド モード 1-6
- コマンドライン編集 1-5
- 正規表現の構文 1-7
- 汎用コマンド 1-9

CLI セッションの終了 2-6

CLI の動作 1-3

- 大文字小文字を区別 1-4
- 再呼び出し 1-3
- タブ補完 1-3
- 表示オプション 1-4
- プロンプト 1-3

ヘルプ 1-3

clock set

- 構文 2-8
- 使用方法 2-8
- 説明 2-8
- 例 2-8

configure

- 構文 2-9
- 使用方法 2-9
- 説明 2-9
- 例 2-9

copy

- 構文 2-10
- 使用方法 2-10
- 説明 2-10
- 例 2-12

Ctrl+N 1-3

Ctrl+p 1-3

D

default キーワード

- 使用方法 1-9

display-serial

- 使用方法 2-13
- 説明 2-13
- 例 2-13

downgrade

- 説明 2-14
- 例 2-14

E

end

- 説明 2-15
- 例 2-15

- erase
 構文 2-16
 使用方法 2-16
 説明 2-16
 例 2-16
- exit
 使用方法 2-17
 説明 2-17
 例 2-17
- I
- IP パケット
 ルートの表示 2-85
- IP ロギングの開始 2-18
- iplog
 構文 2-18
 使用方法 2-18
 説明 2-18
 例 2-19
- iplog-status
 使用方法 2-20
 説明 2-20
 例 2-20
- M
- more exclude
 構文 2-25
 使用方法 2-25
 説明 2-25
 例 2-26
- more include
 説明 2-27
- P
- packet
 構文 2-28
 使用方法 2-29
 説明 2-28
 例 2-29
- password
 更新 2-30
 構文 2-30
 使用方法 2-30
 説明 2-30
 変更 2-30
 例 2-31
- PING
 構文 2-32
 使用方法 2-32
 説明 2-32
 例 2-32
- privilege
 構文 2-33
 説明 2-33
 変更 2-33
 例 2-33
- R
- recover
 構文 2-34
 使用方法 2-34
 説明 2-34
 例 2-34
- reset
 構文 2-35
 使用方法 2-35
 説明 2-35
 例 2-35
- S
- service
 analysis-engine 2-36
 authentication 2-36
 certificate-authority 2-36
 event-action-rules 2-36
 host 2-36
 interface 2-36
 logger 2-36
 network-access 2-36
 notification 2-36
 signature-definition 2-36
 ssh-known-hosts 2-36
 trusted-certificate 2-36
 web-server 2-36
 構文 2-36
 使用方法 2-37

- 説明 2-36
- 例 2-38
- service event-action-rules
 - 使用方法 2-37
- setup
 - クロック設定パラメータ (表) 2-40
 - 使用方法 2-40
 - 説明 2-39
 - 例 2-41
- show begin
 - 構文 2-45
 - 使用方法 2-45
 - 説明 2-45
 - 例 2-45
- show clock
 - 構文 2-47
 - 使用方法 2-47
 - 説明 2-47
 - 保証フラグ 2-47
 - 例 2-47
- show events
 - 構文 2-48
 - 使用方法 2-49
 - 説明 2-48
 - 例 2-49
- show exclude
 - 構文 2-51
 - 使用方法 2-51
 - 説明 2-51
 - 例 2-51
- show history
 - 使用方法 2-53
 - 説明 2-53
 - 例 2-53
- show include
 - 使用方法 2-54
 - 説明 2-54
 - 例 2-54
- show interfaces
 - 構文 2-55
 - 使用方法 2-55
 - 説明 2-55
 - 例 2-56
- show inventory
 - 使用方法 2-57
 - 説明 2-57
- 例 2-57
- show privilege
 - 使用方法 2-58
 - 説明 2-58
 - 例 2-58
- show settings
 - 構文 2-59
 - 説明 2-59
 - 例 2-59
- show ssh authorized-keys
 - 構文 2-63
 - 使用方法 2-63
 - 説明 2-63
 - 例 2-63
- show ssh host-keys
 - 構文 2-65
 - 使用方法 2-65
 - 説明 2-65
 - 例 2-65
- show ssh server-key
 - 説明 2-64
 - 例 2-64
- show statistics
 - 構文 2-66
 - 説明 2-66
- show tech-support
 - 使用方法 2-69
 - 説明 2-69
 - 例 2-70
- show tls trusted-hosts
 - 構文 2-72
 - 使用方法 2-72
 - 説明 2-72
 - 例 2-72
- show tls-fingerprint
 - 説明 2-71
 - 例 2-71
- show users
 - 構文 2-73
 - 使用方法 2-73
 - 説明 2-73
 - 例 2-73
- show version
 - 使用方法 2-75
 - 説明 2-75
 - 例 2-76

- ssh authorized-key
 - 構文 2-77
 - 使用方法 2-77
 - 説明 2-77
 - 例 2-77
- ssh generate-key
 - 使用方法 2-78
 - 説明 2-78
 - 例 2-78
- ssh host-key
 - 構文 2-79
 - 使用方法 2-79
 - 説明 2-79
 - 例 2-80
- System Configuration Dialog 2-40

- T
- terminal
 - 構文 2-81
 - 使用方法 2-81
 - 説明 2-81
 - 例 2-81
- tls generate-key
 - 説明 2-82
 - 例 2-82
- tls trusted-host
 - 構文 2-83
 - 使用方法 2-83
 - 説明 2-83
 - 例 2-83
- trace
 - 使用方法 2-85
 - 説明 2-85
 - 例 2-85

- U
- upgrade
 - 構文 2-86
 - 使用方法 2-86
 - 説明 2-86
 - 例 2-87
- username
 - 構文 2-87
 - 使用方法 2-87

- 説明 2-87
- 例 2-88

- あ
- アクティブなターミナルセッションの終了 2-17
- アプリケーションパーティション
 - イメージの再作成 2-34
- アラート
 - 表示 2-48

- い
- イベント
 - クリア 2-5
 - 削除 2-5
- イベントストア
 - イベントのクリア 2-5
- イベントログ
 - 内容の表示 2-48

- え
- エラー イベント
 - 表示 2-48
- エラー メッセージ B-1

- お
- オペレータ
 - 権限 1-2

- か
- 管理者
 - 権限 1-2

- き
- キーワード
 - no 1-9
 - デフォルト 1-9
- キャプチャ
 - ライブトラフィック 2-28

- 拒否する攻撃者
 - 削除 2-4

- こ
- 攻撃者の IP アドレス
 - 拒否 IP アドレスのリストからの削除 2-4
- 構文
 - 大文字小文字を区別 1-4
- コピー
 - IP ログ 2-10
 - コンフィギュレーション ファイル 2-10
- コマンド
 - 最近使用されたリストの表示 2-53
 - 推奨されなくなった A-2
 - プラットフォーム依存関係 A-2
- コマンド モード 1-6
 - EXEC 1-6
 - イベント アクション ルール コンフィギュレーション 1-6
 - グローバル コンフィギュレーション 1-6
 - サービス モード コンフィギュレーション 1-6
 - シグニチャ定義 コンフィギュレーション 1-6, 1-7
 - 特権 EXEC 1-6
- コマンドとプラットフォームの依存関係 A-2
- コマンドライン編集 (表) 1-5

- さ
- サービス
 - 権限 1-2
- サービス アカウント
 - 権限 1-2
- サービス ロール 1-2
- 最新のアップグレードの削除 2-14
- 再呼び出し
 - 使用方法 1-3
 - ヘルプおよびタブ補完 1-3
- 作成
 - バナー メッセージ 2-3
 - ユーザ 2-87

- し
- システム
 - 状況の表示 2-69
- システム クロックの設定 2-8
- システム情報
 - FTP または SCP サーバへのエクスポート 2-69
- システムのアップグレード 2-86
- 終了
 - コンフィギュレーション モード 2-15, 2-17
 - サブモード 2-15
- 出力
 - 現在の行をクリア 1-4
 - 表示 1-4
 - 表示する行数の設定 2-81
- 出力をシリアル接続に転送 2-13
- 状況イベント
 - 表示 2-48

- せ
- 正規表現の構文 1-7
- 正規表現の構文 (表) 1-7
- 生成
 - X.509 証明書 2-82
 - サーバ ホストキー 2-78
- センサーの初期化 2-39

- た
- タブ補完
 - 使用方法 1-3

- つ
- 追加
 - 既知のホスト テーブルにエント리를 2-79
 - 公開キー 2-77
 - 信頼できるホスト 2-83

- て
- 適用
 - サービス パック 2-86
 - シグニチャ アップデート 2-86

テクニカル サポート

表示

- 現行のコンフィギュレーション情報 2-69
- デバッグ ログ 2-69
- トランザクション応答の制御 2-69
- バージョン 2-69

と

統計情報

- クリア 2-66
- 表示 2-66

ね

ネットワーク接続

- テスト 2-32

は

入る

- グローバル コンフィギュレーション 2-9
- サービス コンフィギュレーション モード 2-36
- パスワードの更新 2-30
- パスワードの変更 2-30
- バナー メッセージ
 - 作成 2-3
- 汎用コマンド 1-9

ひ

非推奨コマンド A-2

ビューア

- 権限 1-2

表記法 ix

表示

- IP パケットのルート 2-85
- IP ログの内容 2-20
- IPS プロセス 2-75
- PEP 情報 2-57
- SSH サーバのホスト キー 2-64
- アラート 2-48
- インターフェイスの統計情報 2-55
- エラー イベント 2-48
- オペレーティング システム 2-75

画面の行数の指定 2-81

既知のホスト テーブル 2-65

現行システムの状況 2-69

現行の権限レベル 2-58

公開 RSA キー 2-63

サーバの TLS 証明書のフィンガープリント 2-71

シグニチャ パッケージ 2-75

システム クロック 2-47

状況イベント 2-48

センサーの信頼できるホスト 2-72

統計情報 2-66

バージョン情報 2-75

ブロック要求 2-48

ユーザ情報 2-73

ライブトラフィック 2-28

ローカル イベント ログの内容 2-48

ふ

ブロック要求

- 表示 2-48

プロンプト

- デフォルトの入力 1-3

へ

ヘルプ

- 疑問符 1-3
- 使用方法 1-3

変更

- 権限レベル 2-33
- ログイン セッションのターミナル プロパティ 2-81

も

モニター

- ビューア権限 1-2

ゆ

ユーザ ロール

- オペレータ 1-2, 1-3
- 管理者 1-2, 1-3

サービス 1-2, 1-3
ビューア 1-2, 1-3

る

ルート

IP パケットの表示 2-85

ろ

論理ファイルの削除 2-16