Cisco IT@Work 事例研究:
E-コマースサーバを DDoS 攻撃から保護する Cisco Guard

Cisco Information Technology

March 31, 2006

概要

- 課題

  広範な偽装アドレスからの低帯域幅 DDoS 攻撃を遮断する

- ソリューション

  Cisco Guard をシスコのインターネット POP（Point of Presence）とインターネットクラウド内に設置

- 成果

  DDoS 攻撃やその他の攻撃を軽減することに成功

- 次のステップ

  サービスプロバイダーと共同で、サービスプロバイダー拠点に Cisco Guard を設置する「クリーンパイプ」ソリューションを他の企業顧客にも提供する。

課題: DDoS 攻撃を遮断する

- シスコのITは、ネットワーク攻撃に対処するために複数の手法を利用

  ネットワーク エッジに配置したアクセス コントロール リスト（ACL）、別名ブラックホールは、シスコのアドレスになりすましたサーバからのトラフィックや、ウィンドウズコントロールポートに向かうトラフィックを大まかにフィルタリング

  より細かい粒度のACLによりCisco Connection Online を保護

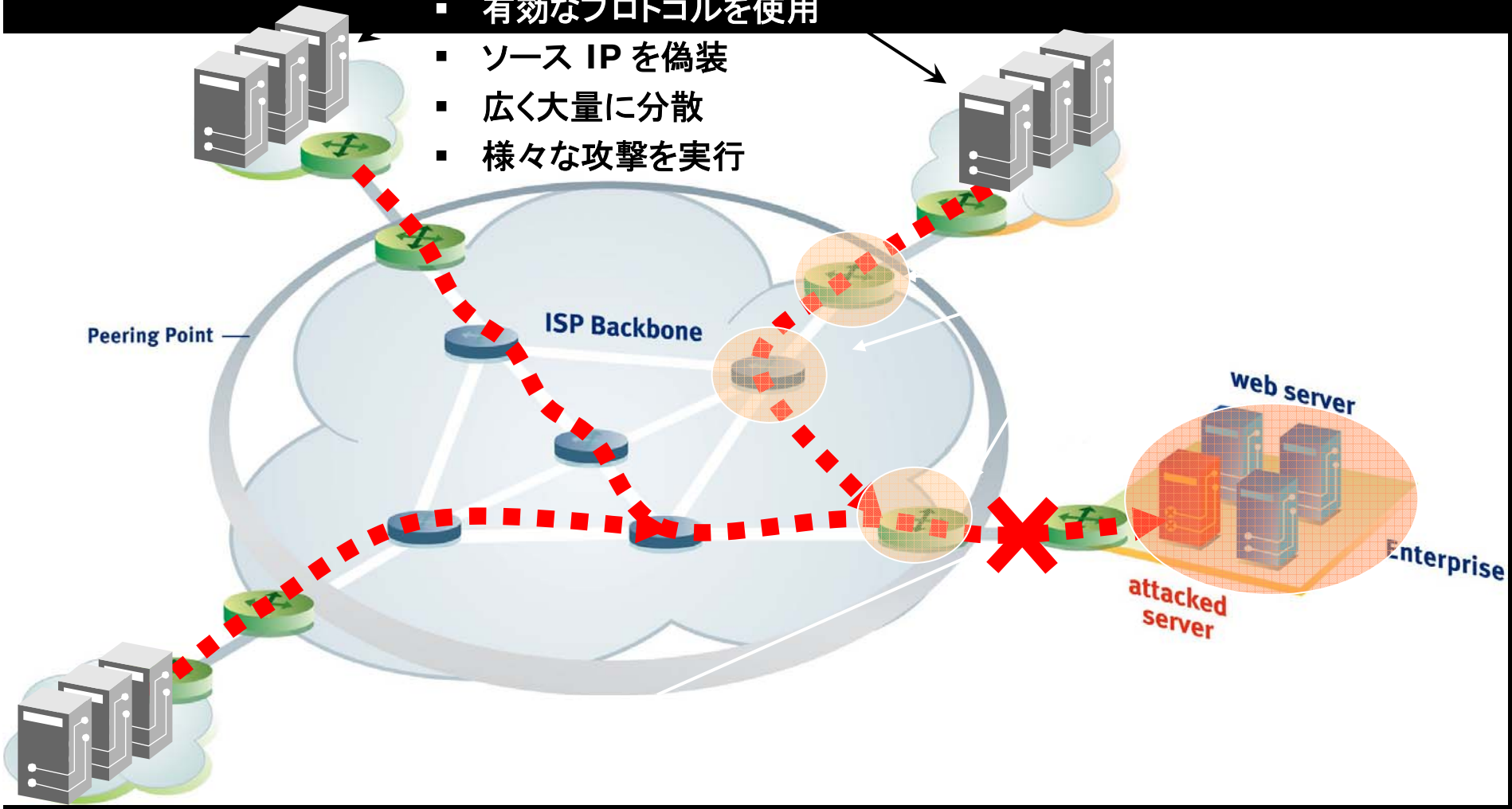
課題: DDoS 攻撃を遮断する

- シスコ IT では、広範な偽装アドレスからの低帯域幅 DoS 攻撃という、新しいタイプの脅威に対抗するために、新たな手法が必要となった
  - ACL は、悪意あるトラフィックと共に適正トラフィックも遮断してしまう
  - ACLでは、攻撃を遮断するために、IT が攻撃元の変化を追跡し続ける必要がある
  - ACL はネットワーク アドレス変換（NAT）を利用しているサイトからの DoS 攻撃に対応するほど洗練されていない

課題: DDoS 攻撃を遮断する

ゾンビによる攻撃

- 有効なプロトコルを使用
- ソース IP を偽装
- 広く大量に分散
- 様々な攻撃を実行



ソリューション: Cisco Guard

- E-コマースなどのミッションクリティカルなサーバを保護するための追加レイヤーを提供
- 全世界の主要なシスコ IPS POP（Point of Presence）とインターネットクラウド内に設置
- トラフィック経路上に設置
- 通常運用の間、トラフィックはネットワーク内の通常経路を通過

ソリューション: Cisco Guard が始動

いったん攻撃が始まると...

- シスコ IT は攻撃の可能性を、Cisco NetFlow データを解析する Arbor PeakFlow DoS システムからのアラートなど様々な方法で察知
- シスコ IT は DDoS 攻撃への対処方法を選択

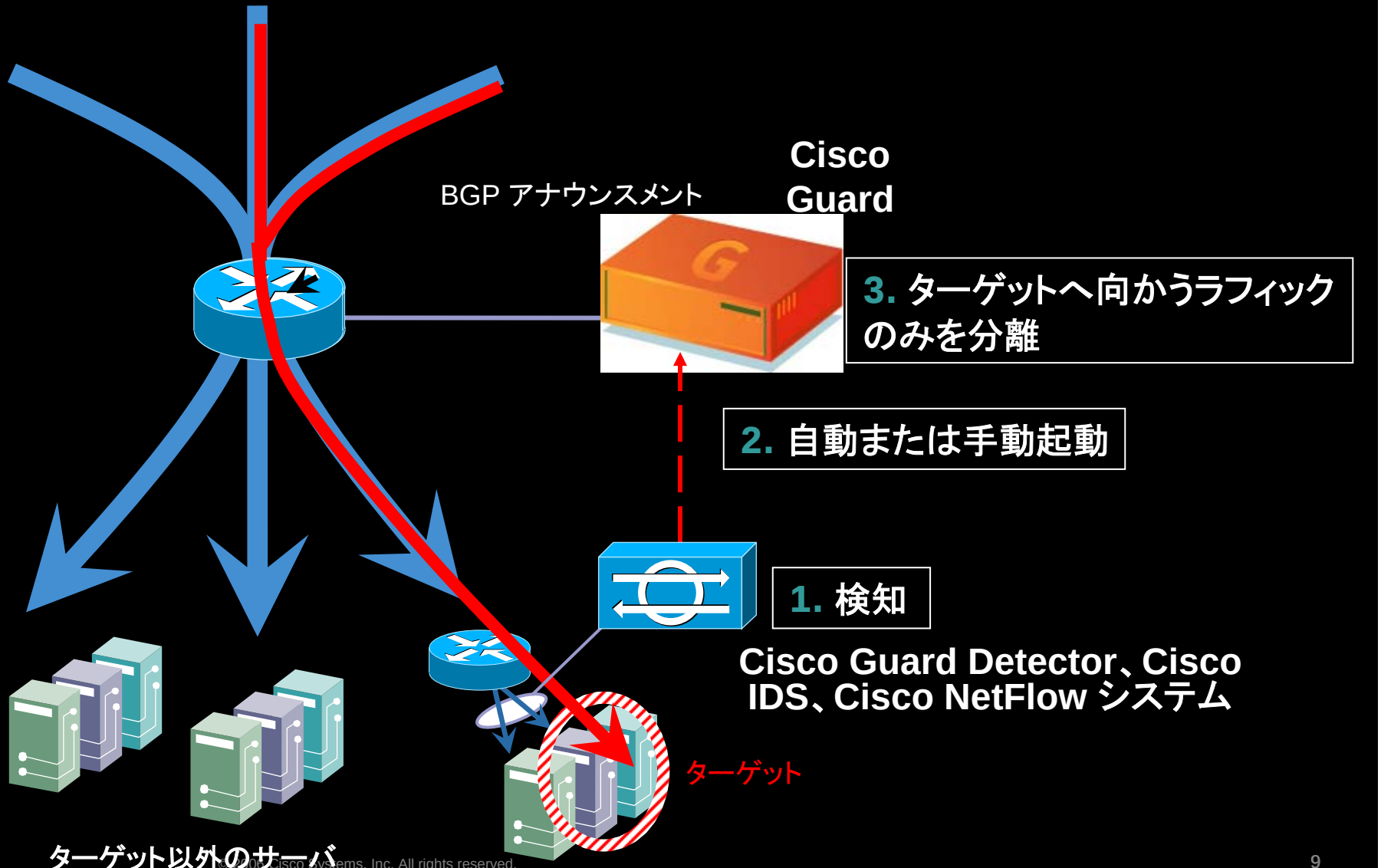
  限られた IP アドレスからの小規模な攻撃に対しては、ブラックホールテクノロジーを使うか、攻撃されているデバイスの電源を切る

  数多くの IP アドレスからの大規模な攻撃に対しては、Cisco Guard などの対策を講じる

ソリューション: Cisco Guard が始動

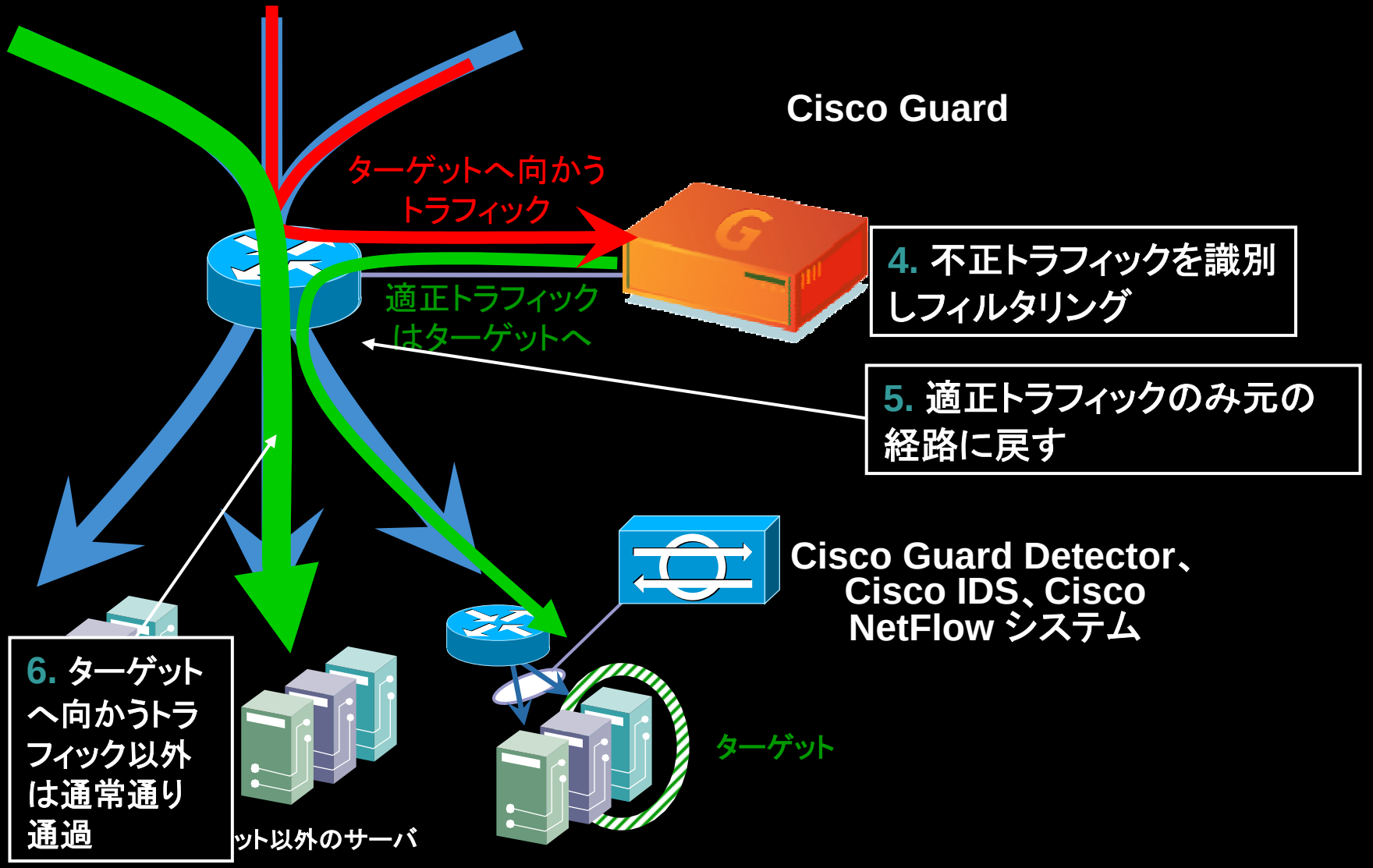
- Cisco Guardは、ダイナミック ルーティング機能を用いて、保護資産へ向かうトラフィックの経路を変更
- サーバへ向かうトラフィックを通常のトラフィック プロファイルと比較することで、適正トラフィックと不正トラフィックを識別
  - 適正トラフィックは通過
  - 不正トラフィックは排除

ソリューション: Cisco Guard（対処手順 1-3）



ソリューション: Cisco Guard（対処手順 4-6）

Cisco.com



ソリューション: ISP 上の Cisco Guard

世界中のシスコ ISP 上にも展開される Cisco Guard

Cisco POP 内の Cisco Guard	インターネットクラウド内のCisco Guard
シスコのネットワークに接続されたコンピュータを起点に実行される DDoS 攻撃からシスコサーバを保護	シスコのネットワーク外の拠点を起点に実行される大規模 DDoS 攻撃からシスコサーバとアップストリーム帯域幅を保護

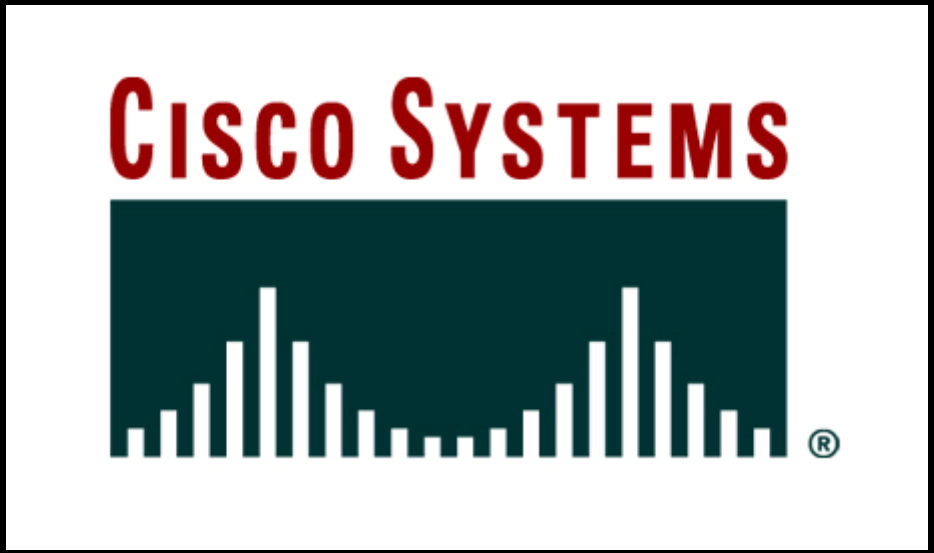
成果: DDoS 攻撃を効果的に軽減

- Cisco Guard によって、シスコ IT が軽減させることに成功した攻撃
  - 大規模 DDoS 攻撃
  - SYN フラッド攻撃
  - ICMP 攻撃
- Cisco Guard が収めたその他の成功例
  - SYN フラッド攻撃の可能性を否定
  - 潜在攻撃がクオーターエンドの業務に影響を与えないことを保証
  - 顧客のウェブサイトがスパム元となることを阻止
  - DNS 攻撃を阻止

次のステップ: IPS へのクリーンパイプ ソリューション

- サービスプロバイダーと共同で、他の法人顧客にCisco Guard ソリューションを提供する
- 目標: DDoS 攻撃を ISP サイト内に封じ込めることにより、ターゲットとなった企業へのインターネット接続に攻撃の影響が出ないようにする

その他、各ビジネスソリューションに対する Cisco IT の事例研究は、
Cisco IT @ Work をご覧ください
http://www.cisco.com/jp (シスコシステムズ→ Cisco IT @ Work)



この文書に記載されている事例は、シスコが自社製品の展開によって得たものであり、
この結果には様々な要因が関連していると考えられるため、
同様の結果を別の事例で得られることを保証するものではありません。

この文書は、明示、黙示に関わらず、商品性の保証や特定用途への適合性を含む、
いかなる保証をも与えるものではありません。

司法権によっては、明示、黙示に関わらず上記免責を認めない場合があります。
その場合、この免責事項は適用されないことがあります。