Cisco Application Control Engine 4710

より速く、よりセキュアな仮想ロードバランサ・ソリューション
概要編

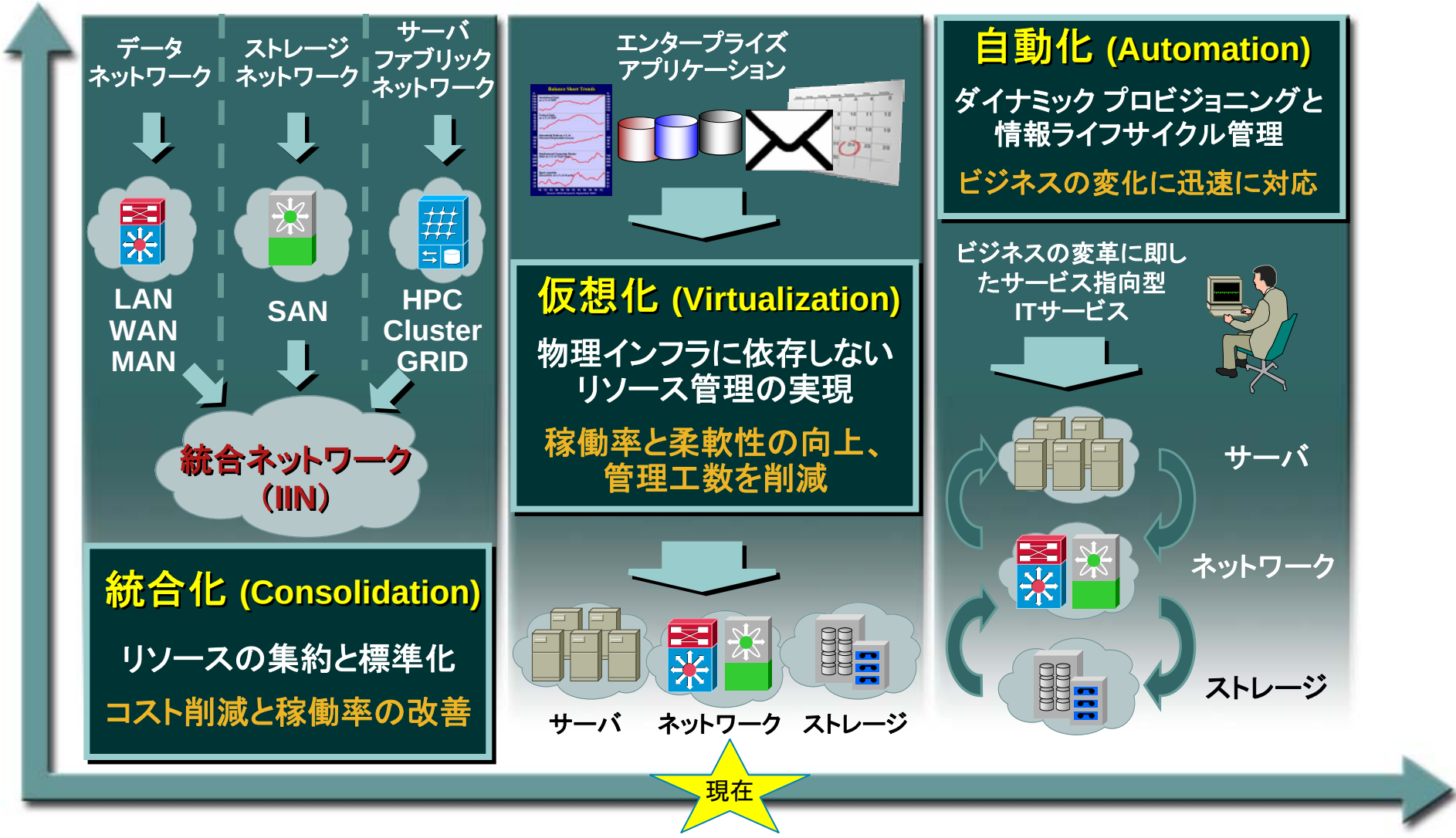
2009年6月

シスコシステムズ合同会社

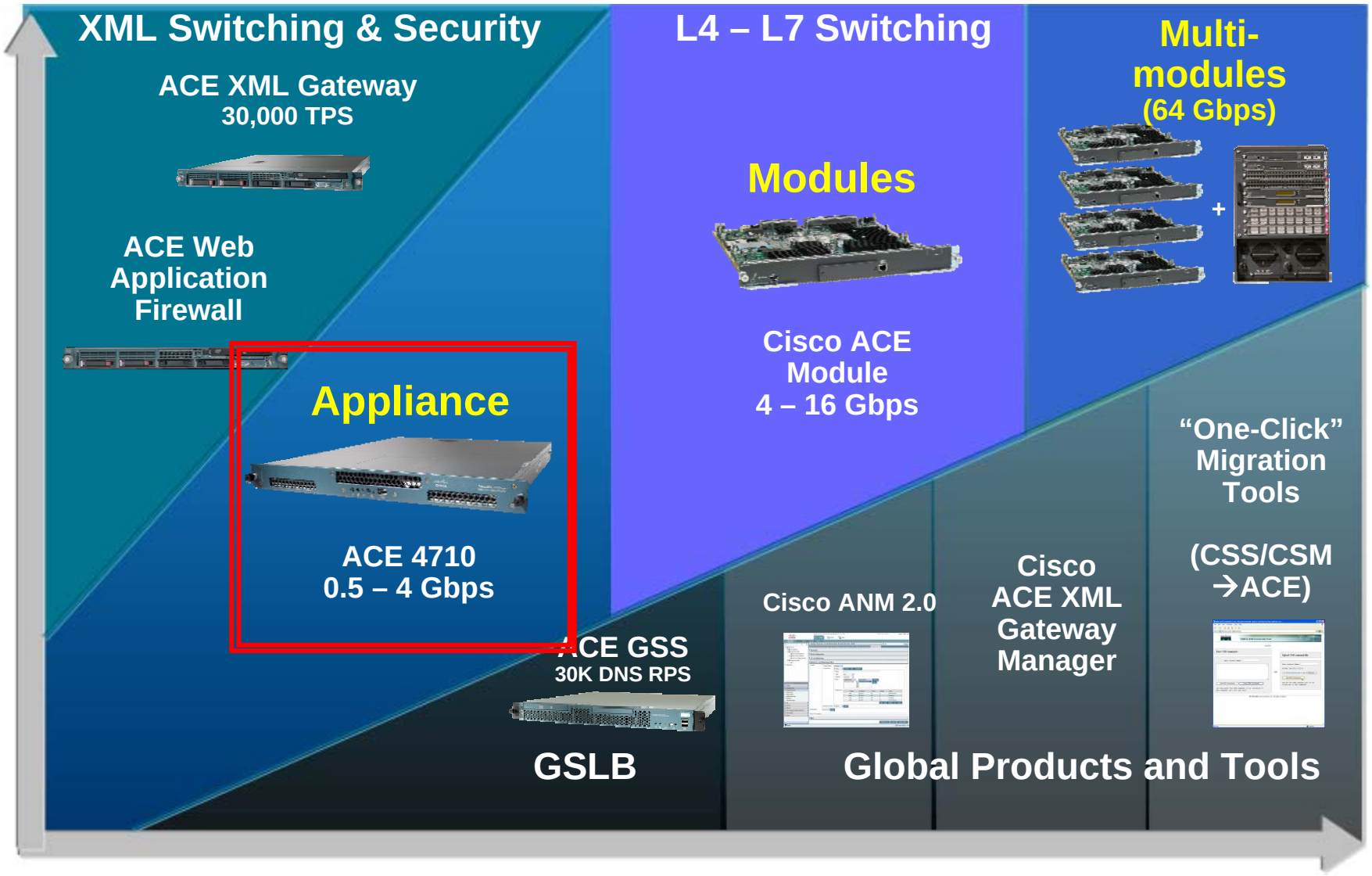
チャネルシステムエンジニアリング

大平　伸一

Cisco Data Center 3.0について



Application Control Engine製品ラインナップ



ACE 4710 ハードウェアについて

前面

背面

ハードウェア: 1 RU,　4 x 10/100/1000 Copper Ethernet Ports

デュアルコア、デュアルCPUアーキテクチャ

スループット: 500Mbps – 4Gbps (ライセンス拡張可)
HWベース圧縮: 最大2 Gbps (ライセンス拡張可)
SSL TPS 最大7500（ライセンス拡張可）
仮想デバイス 最大20 （ライセンス拡張可）

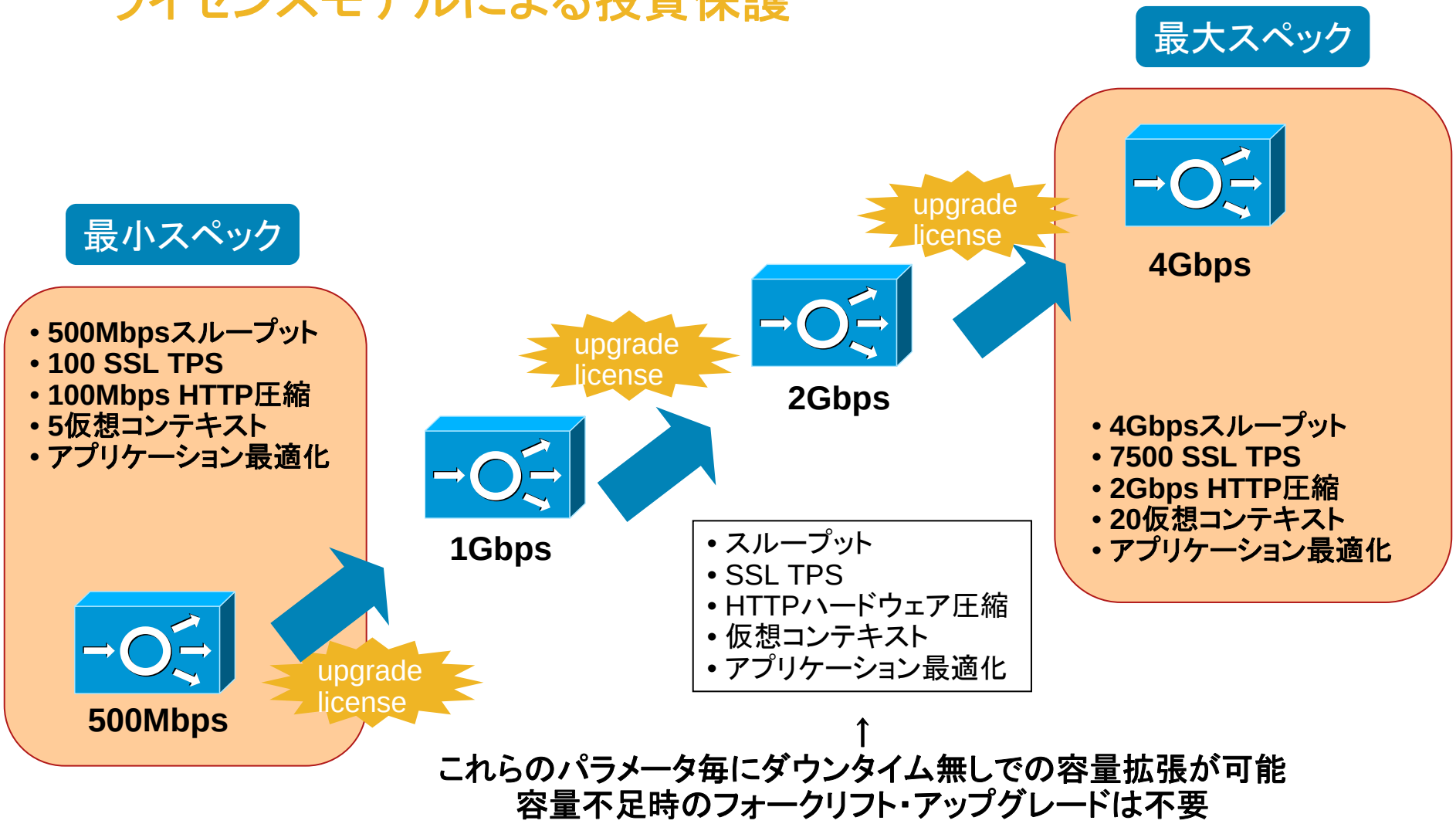
搭載メモリ: 6 GB (基本構成に含む)

デバイスマネージャGUI　標準搭載

ACL行数	:40,000以上
NATエントリー	:1Million
仮想デバイス	:デフォルト5、最大20
SSL Throughput	:1Gbps
CPS	:120,000/秒
仮想サーバ（VIP）	:1000

ACE 4710: L4-7機能統合の効果

ライセンスモデルによる投資保護



↑

これらのパラメータ毎にダウンタイム無しでの容量拡張が可能
容量不足時のフォークリフト・アップグレードは不要

ハードウェアの置換え不要、成長に合わせた投資が可能

バンドル型番構成について

Cisco ACE 4710 アプライアンス バンドル型番一覧表	
型番	説明
ACE-4710-0.5F-K9	ACE 4710 0.5 Gbps バンドル （0.5 Gbps パフォーマンス、100 TPS SSL、100 Mbps 圧縮、5 仮想コンテキスト、アプリケーション高速化（50 コネクション限定））
ACE-4710-1F-K9	ACE 4710 1 Gbps バンドル （1 Gbps パフォーマンス、5,000 TPS SSL、500 Mbps 圧縮、5 仮想コンテキスト、アプリケーション高速化（50 コネクション限定））
ACE-4710-2F-K9	ACE 4710 2 Gbps バンドル （2 Gbps パフォーマンス、7,500 TPS SSL、1 Gbps 圧縮、5 仮想コンテキスト、アプリケーション高速化（50 コネクション限定））
ACE-4710-4F-K9	ACE 4710 4 Gbps バンドル （4 Gbps パフォーマンス、7,500 TPS SSL、2 Gbps 圧縮、5 仮想コンテキスト、アプリケーション高速化（50 コネクション限定））
ACE-4710-BAS-2PAK	ACE 4710 1 Gbps 2 台パック バンドル （1 Gbps パフォーマンス、1,000 TPS SSL、100 Mbps 圧縮、5 仮想コンテキスト、アプリケーション高速化（50 コネクション限定））

ライセンス型番構成について

Cisco ACE 4710 アプライアンス 個別型番一覧表	
型番	説明
ACE-4710-K9	ACE 4710 アプライアンス 本体
ACE-AP-01-LIC	1Gbpsパフォーマンスライセンス
ACE-AP-02-LIC	2Gbpsパフォーマンスライセンス
ACE-AP-04-LIC	4Gbpsパフォーマンスライセンス
ACE-AP-04-UP1=	1Gbps から4Gbpsへのパフォーマンスアップグレード ライセンス
ACE-AP-04-UP2=	2 Gbps から 4 Gbps へのパフォーマンス アップグレード ライセンス
ACE-AP-C-500-LIC	500 Mbps 圧縮ライセンス
ACE-AP-C-1000-LIC	1 Gbps 圧縮ライセンス
ACE-AP-C-2000-LIC	2 Gbps 圧縮ライセンス
ACE-AP-C-UP1=	500 Mbps から 1 Gbps への圧縮アップグレード ライセンス
ACE-AP-C-UP3=	1 Gbps から 2 Gbps への圧縮アップグレード ライセンス
ACE-AP-OPT-LIC-K9	アプリケーション高速化機能ライセンス
ACE-AP-SSL-05K-K9	5,000 TPS SSL ライセンス
ACE-AP-SSL-7K-K9	7,500 TPS SSL ライセンス
ACE-AP-SSL-UP1-K9=	5,000 TPS から 7,500 TPS への SSL アップグレード ライセンス
ACE-AP-VIRT-020=	20 仮想コンテキスト ライセンス

ACE 高機能な負荷分散アルゴリズム

- **Adaptive Response Predictor（サーバレスポンスタイムベース）**
  サーバからのレスポンスタイムをベースにロードバランスを行う
  （サポート対象は HTTP ）

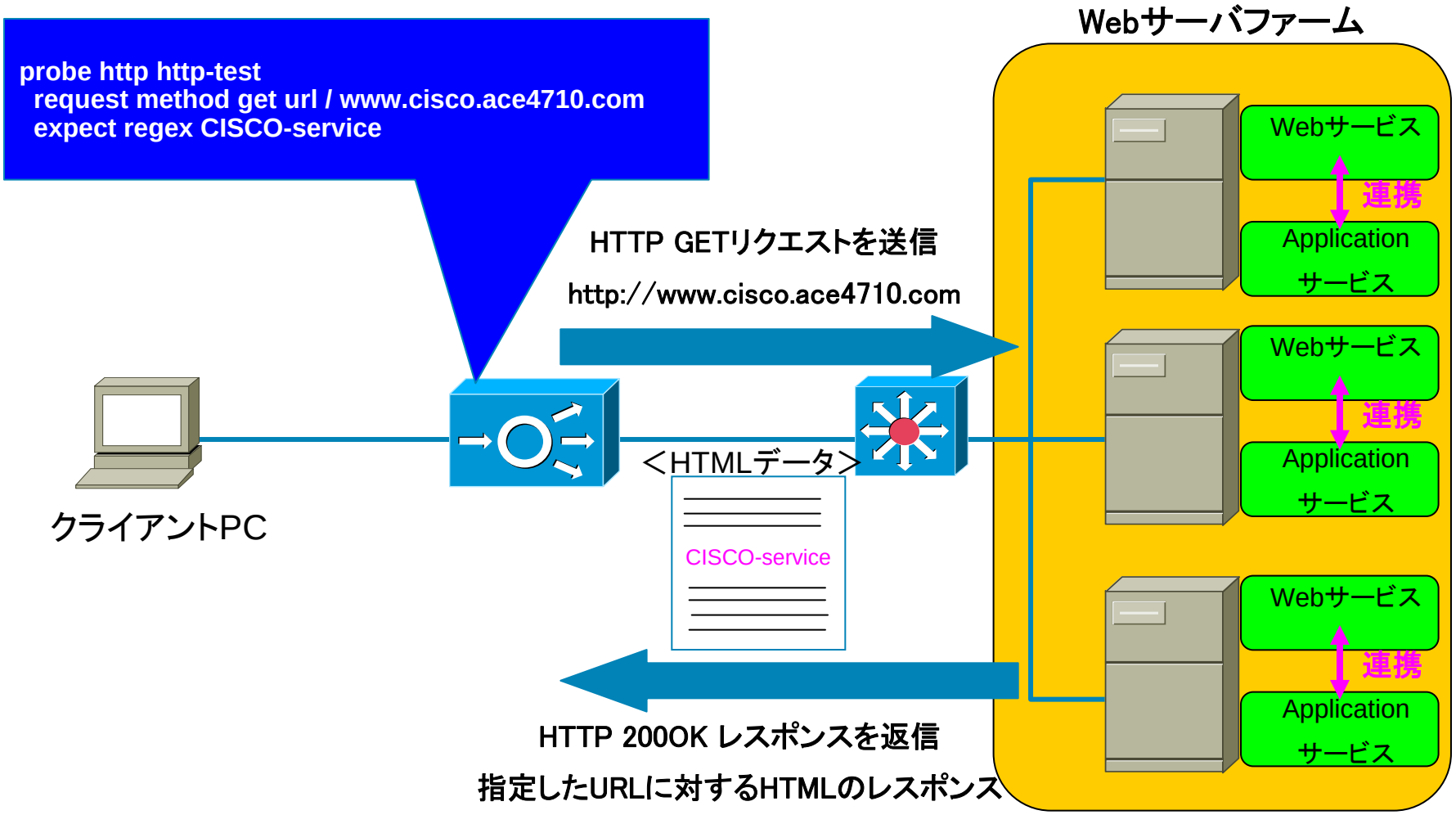
- **Least Loaded Predictor（サーバ MIB 値ベース）**
  SNMP Probeによる実サーバの SNMP オブジェクト ID の値を
  ベースにロードバランスを行う（例； CPU 使用率、メモリ空き容量）

- **Least Bandwidth Predictor（サーバ平均使用帯域ベース）**
  実サーバに対する双方向の平均使用帯域（Bytes/sec）をベースにロードバランスを行う

※上記以外にも標準的なロードバランスアルゴリズムである、ラウンドロビン（重付け可能）、最小コネクション（重付け可能）、IPアドレスやヘッダー、Cookie、URLのハッシュ関数などもサポート

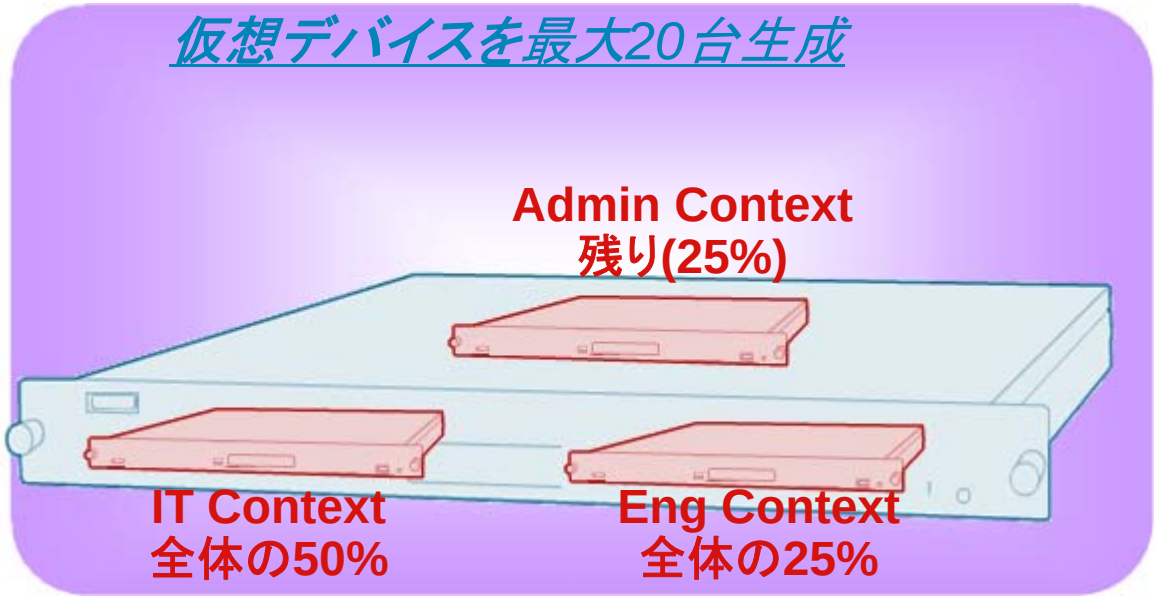
拡張負荷分散アルゴリズムは動的なサーバ負荷にも対応可能

アプリケーションレベルでのサーバヘルスチェック



面倒のスクリプトを作成することなく、HTTP ResponseのBODY部分に含まれるStringをチェックしサーバのヘルスチェックをL7レベルで容易に監視することが可能

ACE 仮想SLBソリューション



各仮想デバイスが個別管理

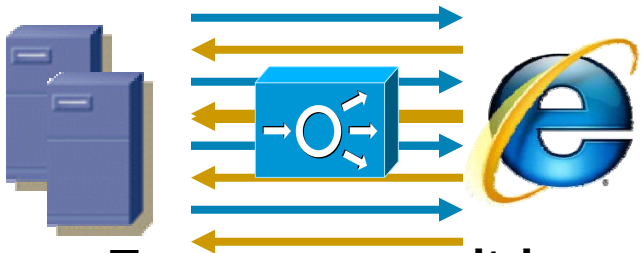
- Configurationファイル
- 専用のディレクトリストラクチャ
- ルーティングテーブル
- リソースクラス
- RBAC、ユーザアカウント等
- SLBポリシー

- 最大20台の仮想のデバイス(コンテキスト)とAdmin専用の仮想デバイス
- システム、アプリケーション、テスト用途に仮想デバイスを展開
- 仮想デバイス毎の多岐に渡る柔軟なリソース制御: bandwidth, CPS, SSL, sticky, ACL等
- 仮想デバイス毎のリソースのOversubscription設定も可能
- 仮想デバイス単位での冗長化やフェールオーバーが可能
- Router (NAT), Bridge, One-Armなど、多彩なデザインに柔軟に対応

**保証されたリソースを各コンテキストに割り当てることで
ACE仮想デバイスはプラットホームのリソース利用効率を最大に**

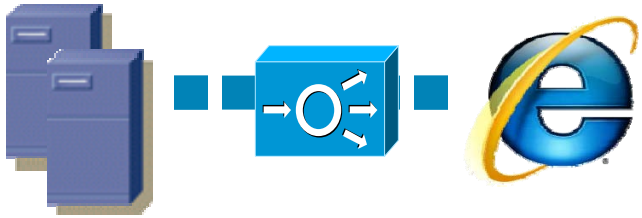
ACEのWebアプリケーションの最適化

Latency Reduction



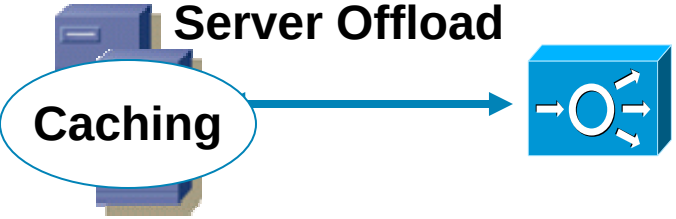
- **特許取得済の技術であるFlashForwarding機能**
  - ページダウンロード時間を高速化
  - ラウンドトリップタイムを最小限に抑制
  - 効率的なコネクション管理

Bandwidth Reduction



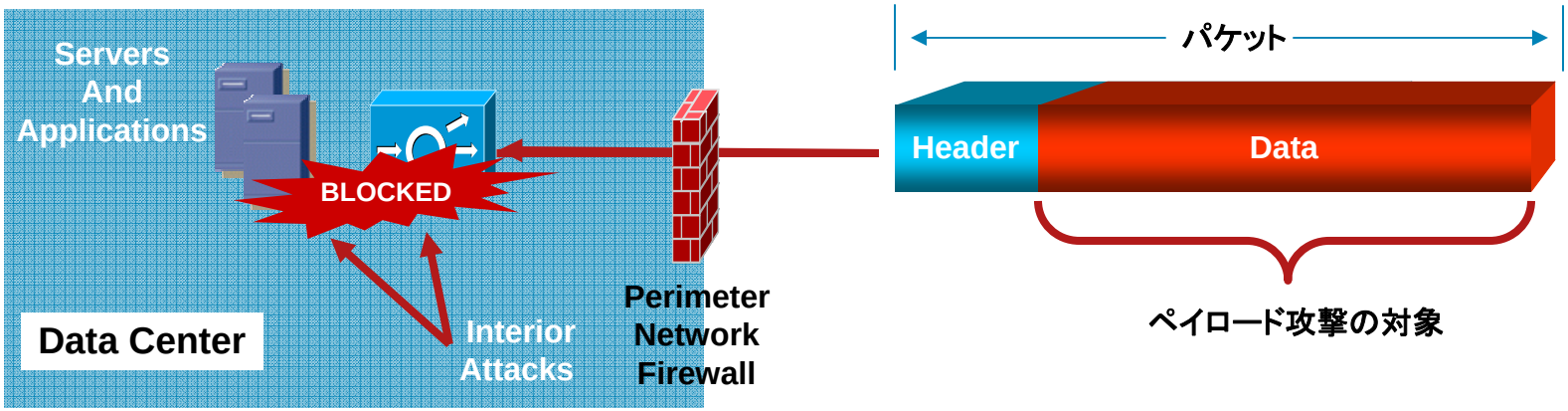
- **特許取得済の技術であるDelta Encoding機能**
  - Webページの差分データのみを返信
- **HTTP Compression機能**
  - Webコンテンツを専用HWでGzip圧縮

Unnecessary data
Required data only
Server Offload



- **ACE4710で終端することでサーバ負荷を軽減**
  - SSL termination
  - TCP Reuse
  - Static および Dynamic Caching

ACEのFirewall機能　ペイロード攻撃を回避
The Last Line Of Server Defense



- Deep Packet Attacks

  通常のFirewallだけではアプリケーションデータの保護という観点で不十分

  ACEはDPIを行い、アプリケーションへの攻撃をブロック

  『Generic Protocol Parsing』はDPIによる防御をどんなプロトコルにも適用可

- 内部からの攻撃: サーバの直前に位置するACEを活用する

  DDoS、プロトコル脆弱性、悪意あるアクセスからサーバファームを保護

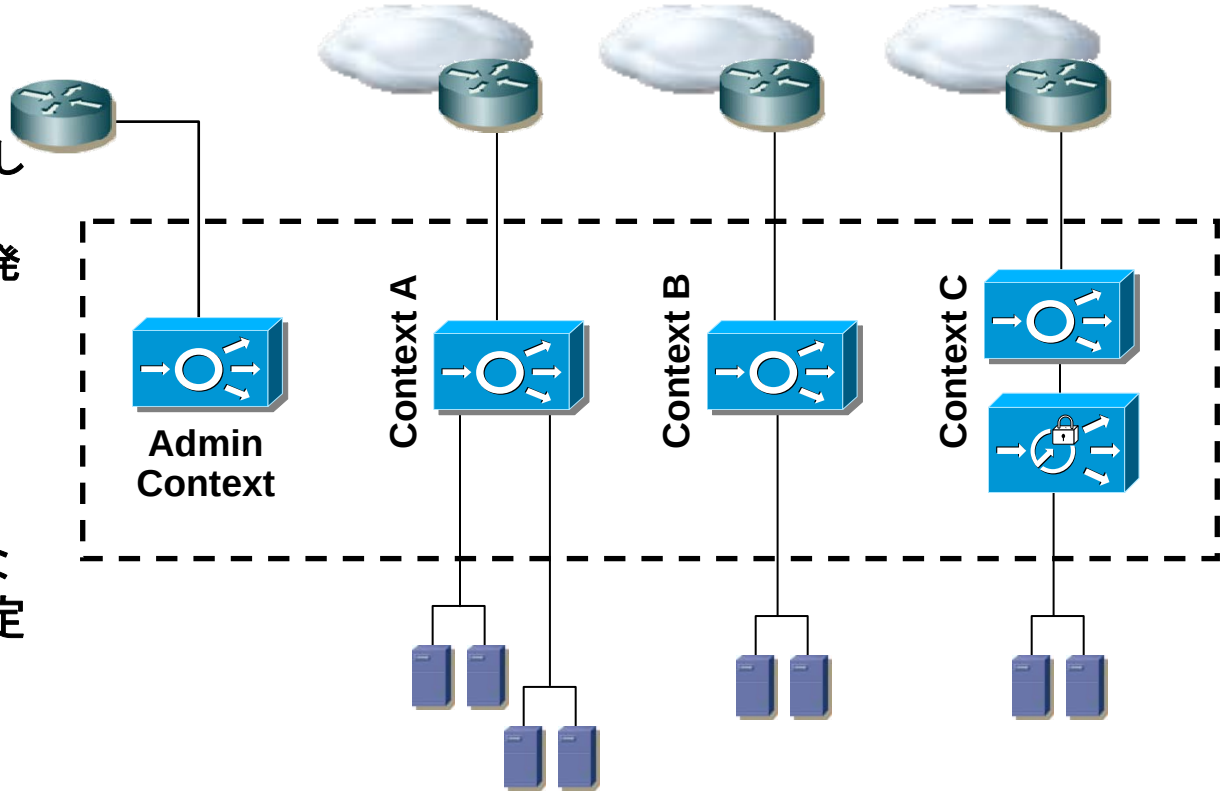
ACE4710のセキュリティ機能とパフォーマンス:
4Gbps, 64k NAT (1M PAT), 40K ACL エントリー, 1M SYN Blocks/sec

仮想化機能のACEユーザ活用例 1/2

設定の複雑さを排除し、管理対象を小さくする

“20,000行以上のconfigを管理していたが、変更箇所のチェックや設定エラー、不要な設定項目を発見するのは難しい”

仮想コンテキスト毎の容易なconfig管理、設定変更、設定のロールバック

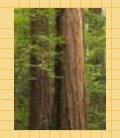


Configをより小さく管理し易くすることで、メンテナンスや変更も容易になり、アプリケーションを保護しながら設定エラーのリスクを回避できる

仮想化機能のACEユーザ活用例 2/2

仮想化機能の活用でGreen IT

例：仮想化機能を用いて一般的なロードバランサー（500Mbps）× 8 台を ACE4710（4Gbps）× 1 台へ統合して 1 年間運用した場合

	ロードバランサー× 8	ACE4710 × 1	ACE による削減量
動作時の消費電力（W）	143×8 = 1,144 W	128 × 1 = 128 W	**1,016 W**
年間 CO2 排出量（トン）	1.144 kW × 0.000425（※1）× 24 × 365 = 4.26 トン	0.128 kW × 0.000425（※1）× 24 × 365 = 0.48 トン	**約 3.78 トン / 年** 
杉の木が 1 年で吸収するために必要な本数	4.26t × 1,000kg ÷ 14（※2） = 304.3 本	0.48t × 1,000kg ÷ 14（※2） = 34.2 本	**約 270.1 本 / 年 = 約 0.34ha（58×58m）** 

（※1） 2007年度 東京電力のCO2 排出係数 0.000425（t-CO2/kWh）を元に計算
環境省：http://www.env.go.jp/press/press.php?serial=10574

（※2） 杉の木（50年杉）が 1 年平均で CO2 約 14kg を吸収する想定して計算
「地球温暖化防止のための緑の吸収源対策」環境省、林野庁資料

仮想化機能のACEユーザ活用例 2/2（続）

仮想化機能の活用でGreen IT

例：仮想化機能を用いて一般的なロードバランサー（500Mbps）× 8 台を ACE4710（4Gbps）× 1 台へ統合した場合

	ロードバランサー× 8	ACE4710 × 1	ACE による削減量
最大発熱量（BTU/hr）	1,025×8 = 8,200 BTU/hr	1,314 × 1 = 1,314 BTU/hr	**6,886 BTU/hr**

→ 約 84 % の発熱量を削減（＝ 冷却コストの削減）

（参考）6,800BTU/hr は、大型のスイッチを設置した程度の発熱量に相当 !!

ラックスペース	1RU × 8 = 8 RU + α（隙間）	1RU × 1 = 1 RU	**7 RU + α**

→ 約 88 % 以上の設置スペースを削減（＝ 設備コストの削減）

機器ごとに 0.5RU 空けていた場合、10.5RU のスペースを削減 !!

ACE4710 A3.x ソフトウェア機能概要

Available

Load Balancing Support
- SIP
- Extended RTSP
- Radius
- RDP
- Generic Protocol Parsing

Enhanced Predictors
- Adaptive Algorithms
- Least Loaded
- Least Bandwidth

General SLB
- Kal-AP
- HTTP Header Rewrite
- Partial Serverfarm Failover
- Application-based Probes
- SNMP-based Probes
- UDP Fast Age
- Port Inheritance for Probes

Fast

SSL Enhancements
- Session ID Stickiness
- Session ID Re-use
- SSL Queue Delay
- Client Authentication
- URL Rewrites for SSL
- SSL Cipher Load Balancing

Enhanced UDP
- UDP Booster

Licenses
- 0.5,1,2,4Gbps Throughput
- 2Gbps HTTP Compression

Management
- XML Tagged Configuration
- ANM 1.2
- HA Sync Improvements
- Source NAT Changes
- SNMP Enhancements

Secure

Protocol Inspection
- SIP
- ILS/LDAP
- Skinny

ACL Improvements
- Object Grouping

DoS Protection
- SYN Cookie per Interface

Rate-Limiting
- Connection-rate
- Bandwidth-rate

HTTP Firewall Features
- Inspect HTTP POST Body
- Inspect HTTP “Secondary cookies”


CISCO