

2008年7月9日
電子情報通信学会
インターネットアーキテクチャ研究会

パネル討論

ルータとサーバの運用管理技術 (NETCONFの現状と今後)

『OANによる新しい運用管理の現状と方向性』

アラクサラネットワークス 先端技術企画部

黒崎 芳行

樋口 秀光

飯島 智之

新 善文

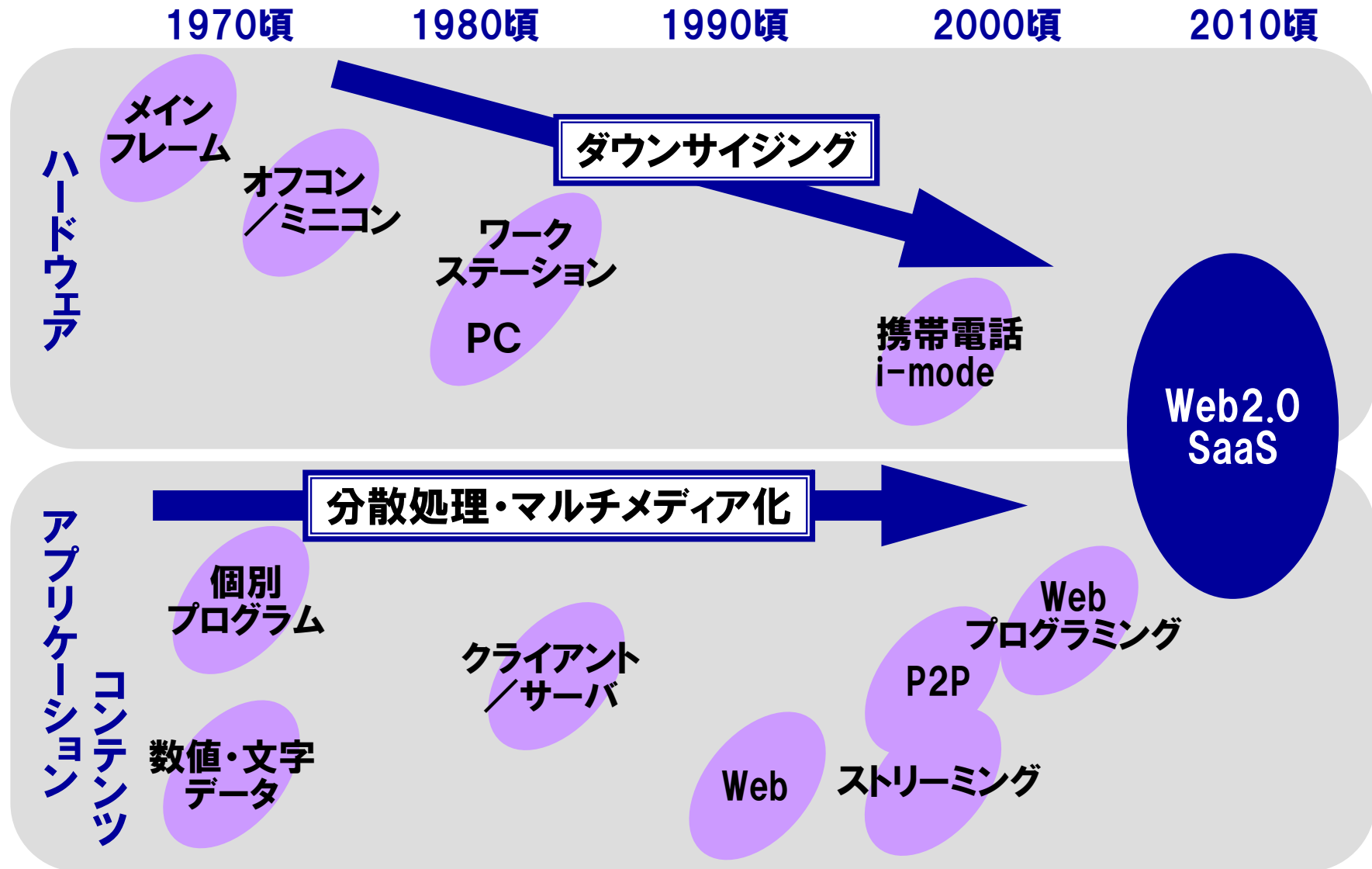
木村 浩康

木谷 誠

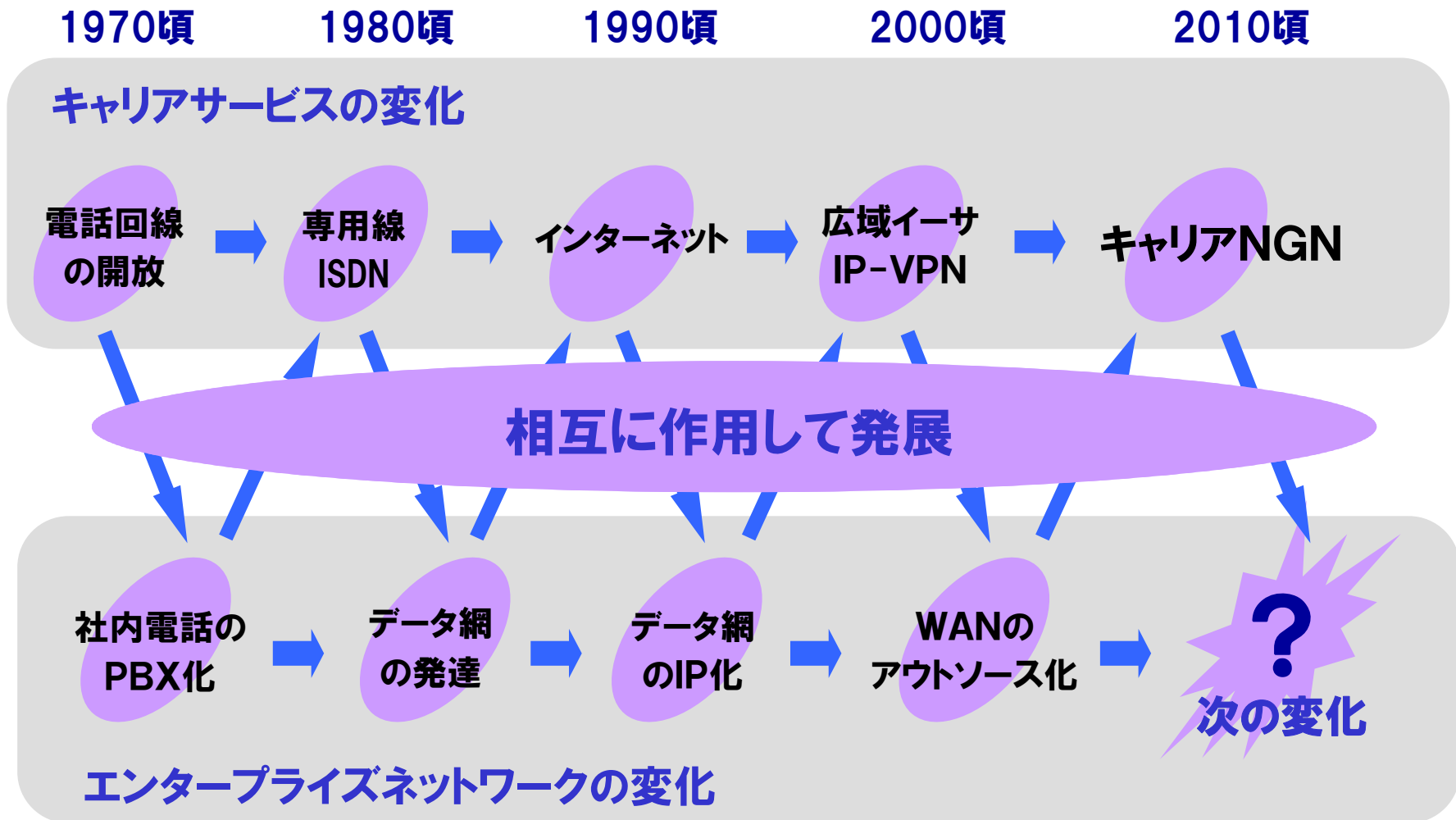
目次

- 1 OANの背景
- 2 OANの構造
- 3 標準化状況
- 4 ストレージでの実装状況
- 5 サーバでの実装状況
- 6 ON-API活用事例

1 OANの背景 (ITのイノベーション)



1 OANの背景(ネットワークのイノベーション)



1 OANの背景(アプリとネットの連携)

ICTシステムと共通のWebベース運用管理がトレンドに

業務
アプリケーション



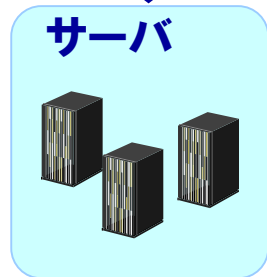
運用
アプリケーション



機器制御I/F

Webサービス
WSDL
HTTP/SOAP

ICTインフラ



1 OANの背景(運用の課題)

OANは、ネットワーク運用における課題を解決し、システムの安定稼働を支援します。

管理対象装置や機能が急速に増加・複雑化、24時間サービス提供、コスト削減など、ネットワーク管理者が絶対的に不足(人数、スキル)

運用管理が属人的なノウハウに支えられているため作業の一般化(継承、横展開)が出来ない。



単純なミス(設定ミス、コミュニケーション不足)が引き金となり、社会インフラ(金融、交通、行政などのサービス)の停止へと発展する事例が多発。

ビジネスの損害のみならず、社会的信頼の失墜、監督官庁からの指導など、企業の存続さえも左右する。

これからのICTシステムにおけるネットワークの役割は、従来の機能を踏襲し、...

突然のシステム変更にも対応出来る柔軟な構成管理



アプリケーションの動きに合わせた機動的なサービスの提供(動的な帯域割当等)

日々発生する新しいセキュリティ問題への対応



ネットワークの機能を公開し、ユーザの要望に沿った役務の提供を容易に行える

1 OANの背景(まとめ)

「人」は減るが「トランザクション」は増える

→トランザクションの形態も変化して増加
24Hr365Dayになり、止められないシステムへ

あらゆるところでのアウトソースが進む

→複数の企業との連携があたりまえに
システム間連携の為にインターフェイスはWeb技術へ

装置とアプリケーションの境界がドンドンなくなる

→Web技術が全てを包含する形で徐々に仮想化が浸透

2～3年経つと新技術もレガシーになる

→「今出来ない事がいつまでも出来ないという事ではない」が
時間の間隔が非常に短くなってきている

2 OANの構造

CLI、SNMPの問題を解消し、自動化を実現するAPIを実現

CLI、SNMPの問題点

- CLIはコマンドにリターンコード無し
- SNMPはUDPでロストが心配。MIBは細かすぎ

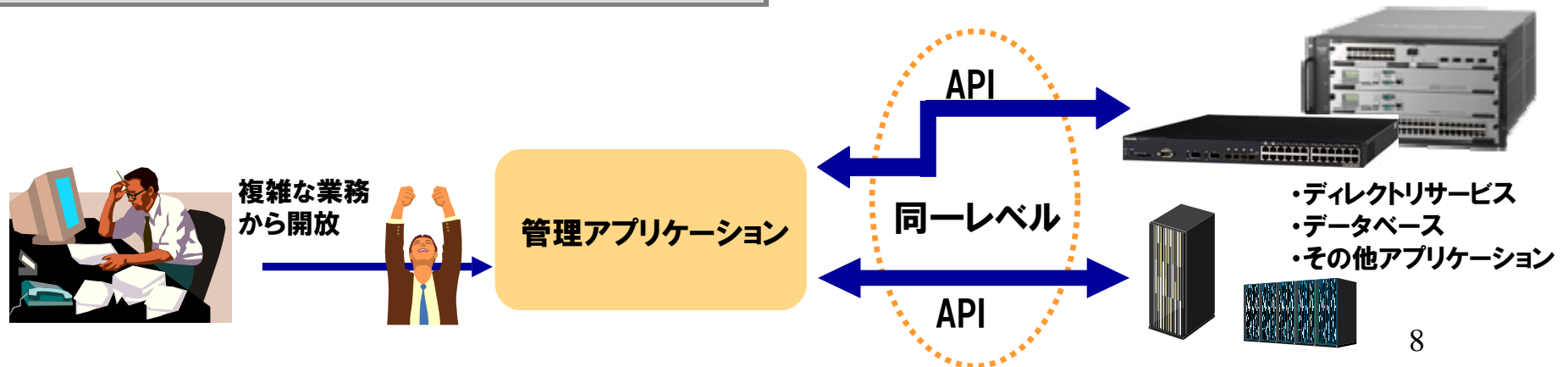
AX-ON-API-SDKによる新しい取組み

自動化による運用コストの低減

- リクエスト完結型のAPI
リクエスト完結型のAPIによりCLIの問題を解決
(結果確認の為のコマンドが不要です)
- ICTシステムとの親和性の拡大
Javaで記述するAPIのライブラリを提供
業務アプリケーションと同じ様にネットワーク機器を
制御可能

標準化技術の活用によるオープン性

- 標準準拠で相互接続性を確保
「NETCONF」(RFC4741~RFC4744。2006/12)
「MAXI-NM-1.0」(INTAP/OSMIC規格。2007/2)
に準拠。市場で広く採用される技術を先取り
- 通信基盤にHTTP/SOAPを利用
セキュリティの確保、通信品質の確保を実現



2 OANの構造

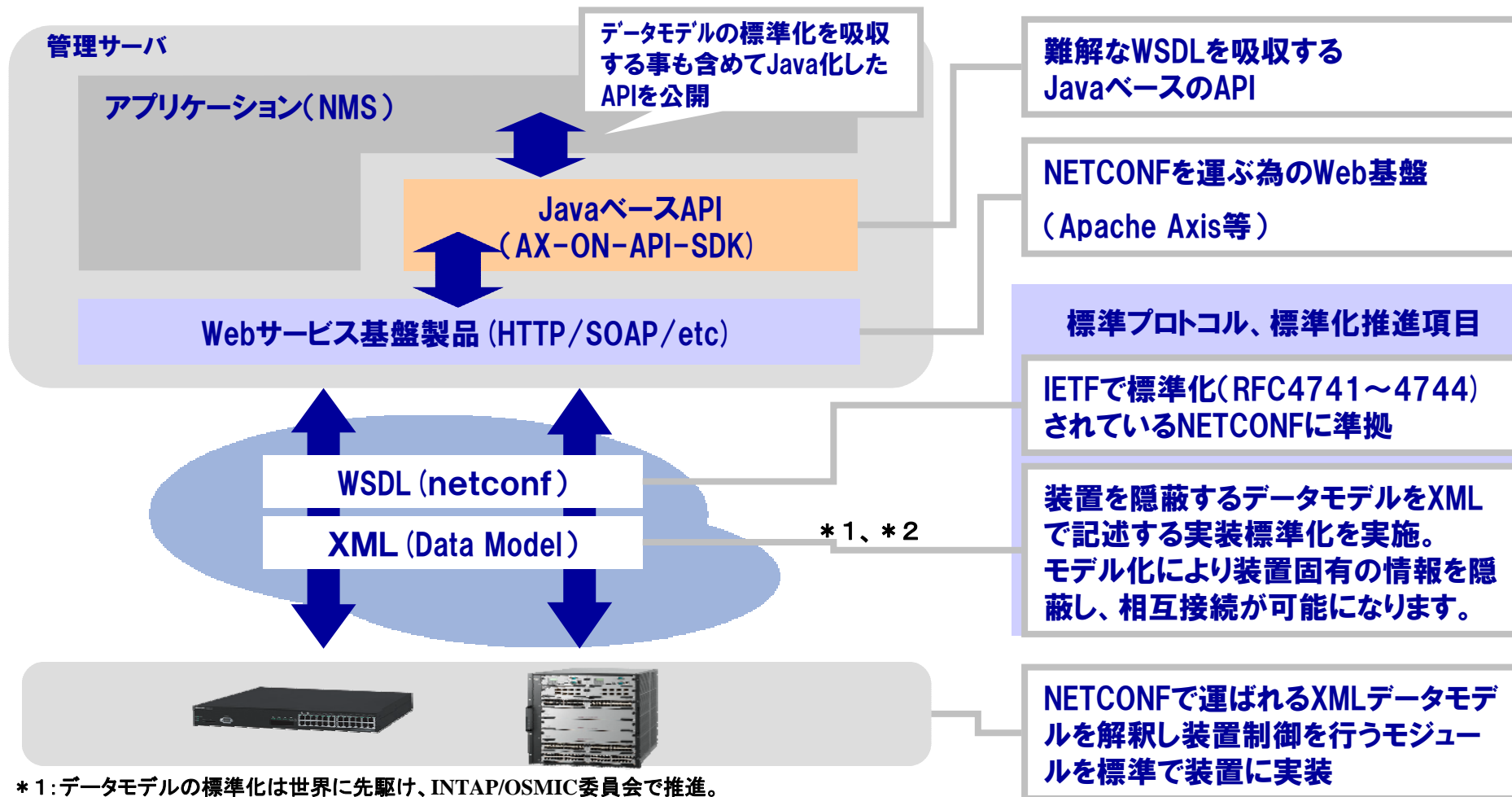
AX-ON-API-SDKで提供する機能 2008/5現在

	項目	内容
設定 (追加/ 削除/参 照)	装置情報	・装置名称、ループバックアドレス、FDB(収集のみ)など
	VLAN情報	・VLAN番号、VLAN名称 ・Trunk/Access/Protocol/MACの4種類のモードなど
	インタフェース情報	・物理情報(スロット番号/ポート番号、回線名称など) ・リンクアグリゲーション(LACP/Staticなど)
	フィルタ情報	・MACアドレス、IPアドレス(IPv4/IPv6)、TCP/UDPポート 番号の範囲指定など
	経路情報	・スタティックルート(ポーリングなど)
	コンフィグ情報	・スタートアップコンフィグ/ランニングコンフィグ
その他	NEW OS管理	・装置OSの入れ替え(イメージファイル配置、アップデート)

NEW : AX-ON-API-SDK Ver1.3

2 OANの構造

OANはWebサービスで装置制御が行える構造を採用
利用者の操作性を考慮し、JavaによるAPIで開発の容易性を訴求



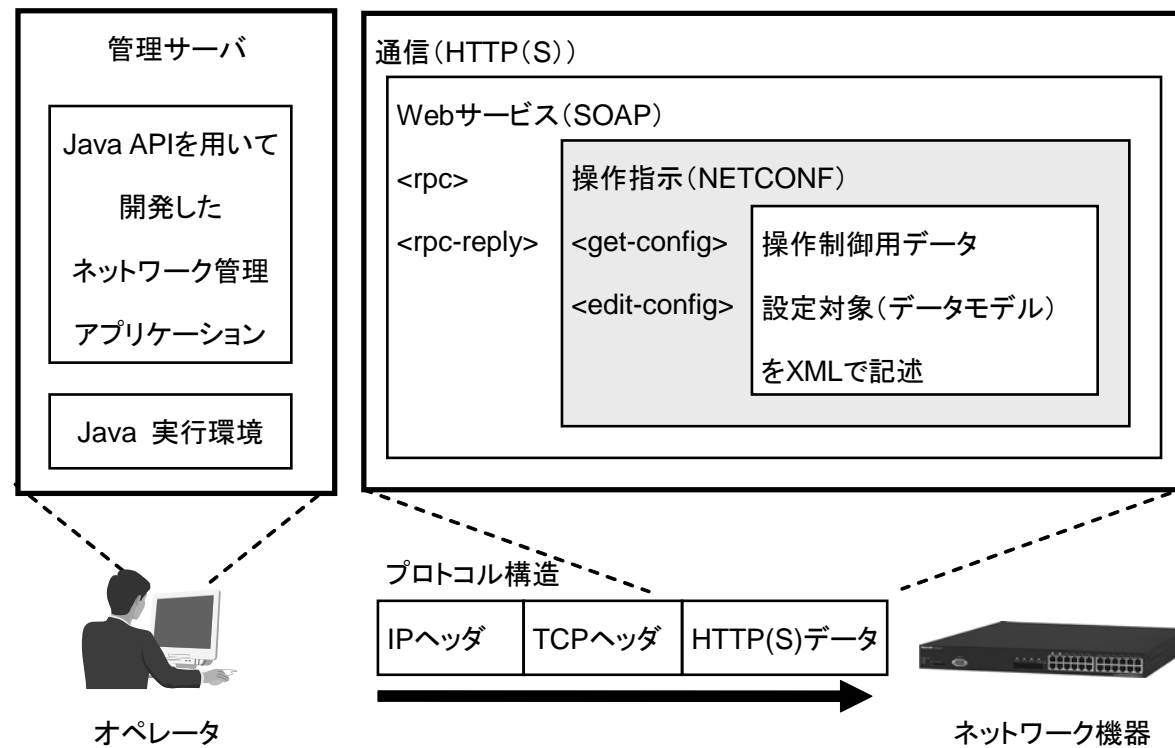
* 1: データモデルの標準化は世界に先駆け、INTAP/OSMIC委員会で推進。

2007/1にMAXI-NM-1.0として標準仕様の策定完了 (<http://www.net.intap.or.jp/INTAP/osmic/index.html>)

* 2: IETFにて標準化活動中 (draft-ijjima-ngo-vlandatamodel-00, draft-ijjima-netconf-soap-implementation-01など)

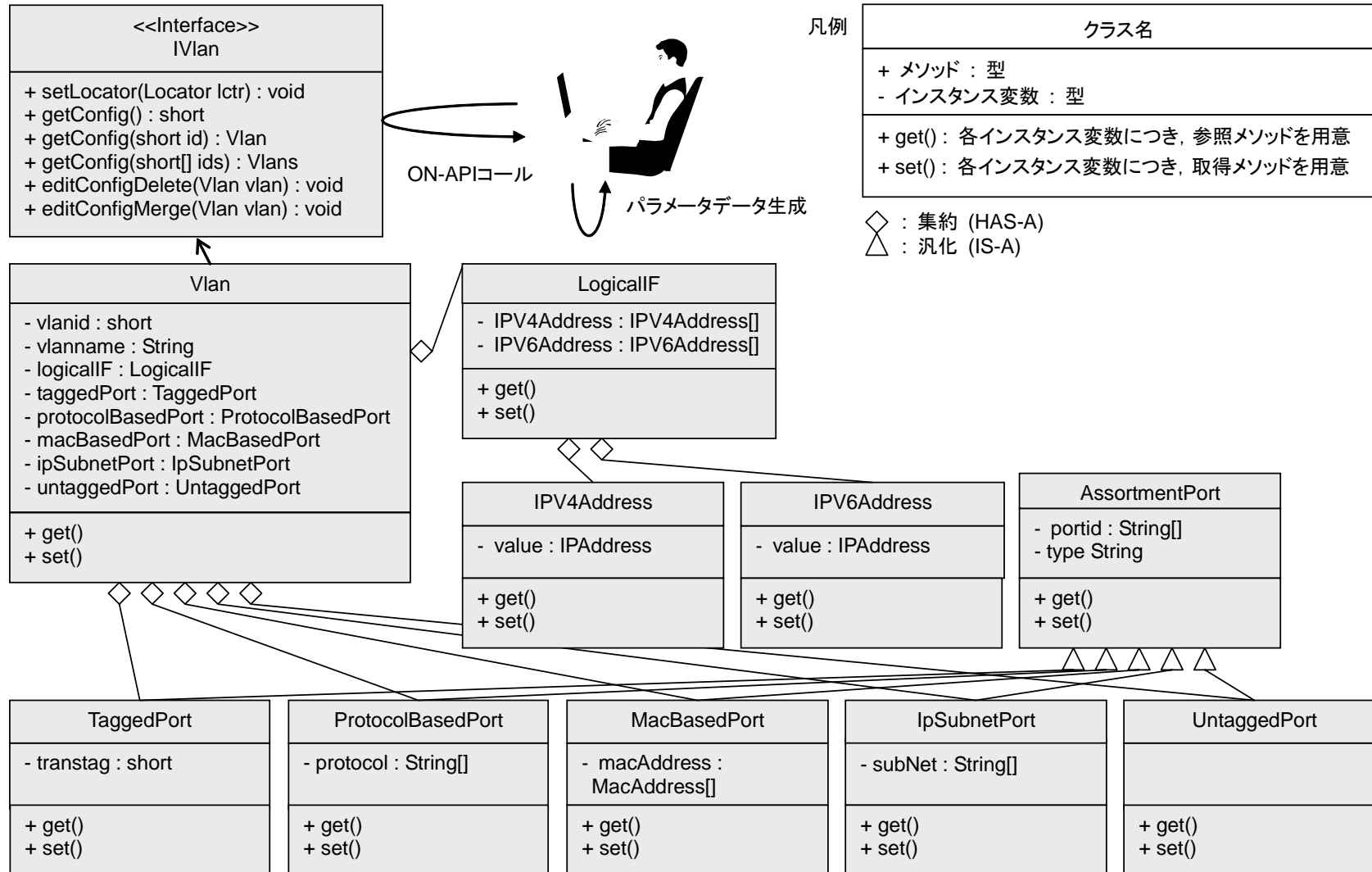
2 OANの構造

- 転送プロトコルとしてNETCONFを利用
- 機器操作のモデルはXMLで記述



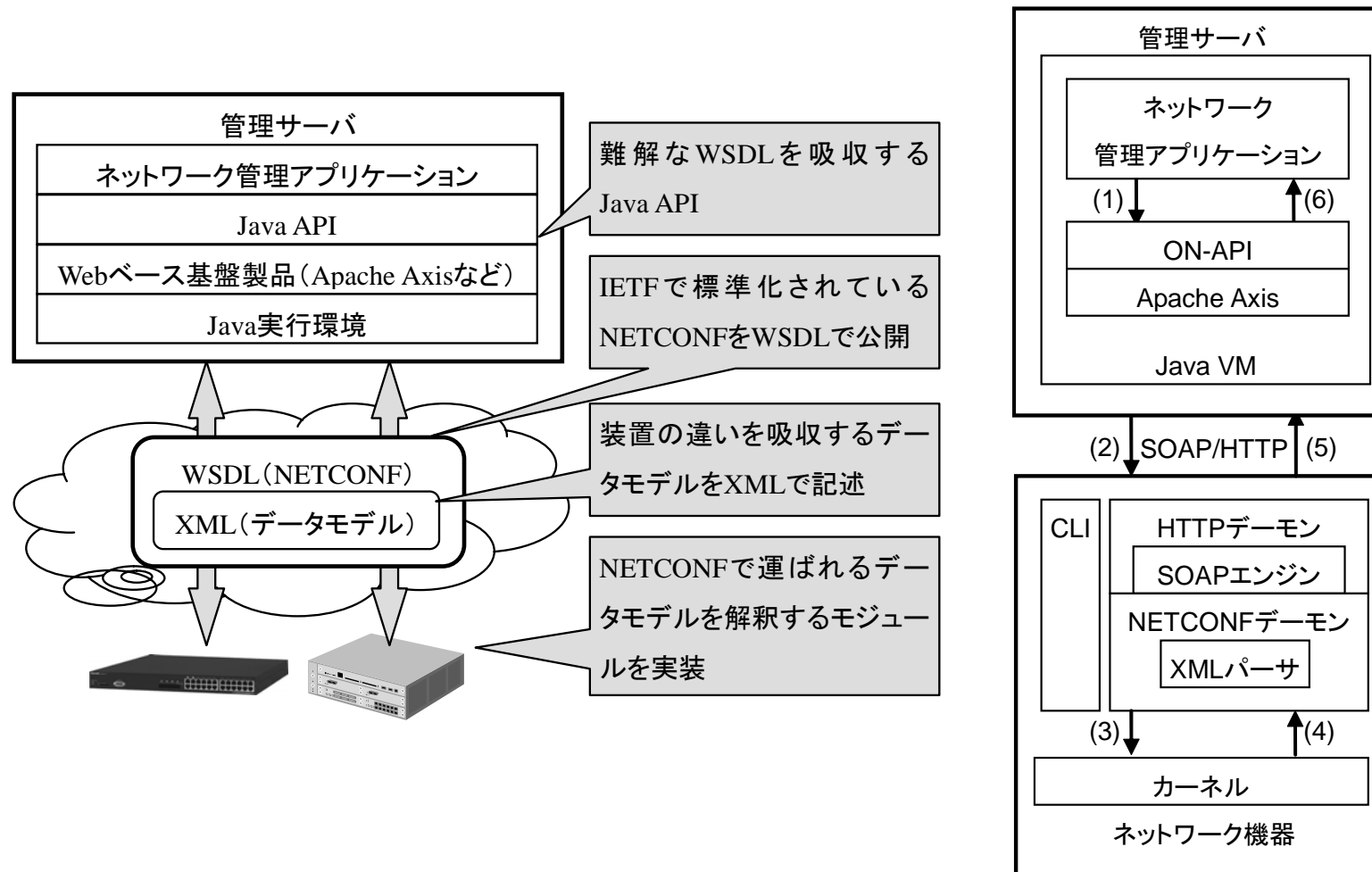
2 OANの構造

VLANのデータモデル図



2 OANの構造

- 管理アプリケーションインターフェイスをJavaで提供
- WSDLによる相互接続性をJavaで隠蔽



2 OANの構造

ON-APIを利用した定量的な評価の一部を以下に示します。

効果1 アクセスリストのフロー検出条件4000件設定の比較例

<測定方法>

CLI : TeraTermのMacroを用いて1コマンドずつ投入

API : APIで100件のフロー検出条件の配列を生成し、APIで100件一括設定を40回繰り返す

<測定結果>

CLI : 1時間10分(1コマンドの応答が約1秒)

API : 7分16秒

効果2 某ISV会社での操作アクセス頻度

<測定結果>

	APIベース	CLIベース
VLANへの1ポート追加	2.8秒/1メソッド	13秒/7CLI
VLANへの10ポート追加	2.9秒/1メソッド	114秒/61CLI

2 OANの構造

本資料は若干変わっています

OANを利用する事のメリットとデメリット

項目	メリット	デメリット
モデル化による 機種依存性の排除	機器/メーカーに依存した操作が不要	装置実装が重たくなる (Web技術の装置実装)
	アプリケーション開発の単純化	エンジニアの習熟 アプリの開発
ネットワーク操作の API化による効率 向上(自動化、高速 化)	自動化を容易に実現 (人為的ミスの低減が可能)	エンジニアの習熟 アプリの開発
	大量の変更作業が容易かつ高 速に変更が可能 (省エネ、クラウドコンピューティング、 仮想化、等への対応が可能)	
トランザクション型の 操作(結果が返る)	自動化を容易に実現	なし
既存資産への対応	メンテナンスが容易 機種追加でも修正量が少	新規に再作成

3 標準化状況 (INTAP/OSMICでの検討状況)

注意: 以下の資料はINTAP/OSMIC WG4で議論されている資料から抜粋しています。
正式な情報としては、INTAP/OSMIC委員会のから発行されている情報で確認をお願いします。

・経緯

IETFでネットワークの新しい管理技術標準 (netconf) の検討が加速。
サーバ系のDMTF、ストレージ系のSNIAと同様のWebサービスによる管理方式が広まる状況を踏まえて検討を開始した。

・INATP/OSMICでのnetconfネットワーク標準化の経緯

- ・2006年2月 OSMIC-WG1の場でnetconfの標準化動向の検討会実施
- ・2006年3月 H17年度第5回OSMIC企画委員会で今後のMAXI仕様の拡張の一部として検討する事について合意。
- ・2006年5月 準備会を開きnetconfをベースにしたモデル化技術による構成管理についての標準化方針を確認
- ・2006年7月 OSMIC企画委員会にてWG4の設置およびWG4での技術検討を決定
- ・2006年8月 第一回WG4会合から技術面の検討を開始
- ・2007年1月 MAXI-NM-1.0としてVLAN、Filter等を規格化

MAXI仕様書

<http://www.net.intap.or.jp/INTAP/osmic/business/MAXI-NM-10.pdf>

3 標準化状況 (IETFでの標準化状況)

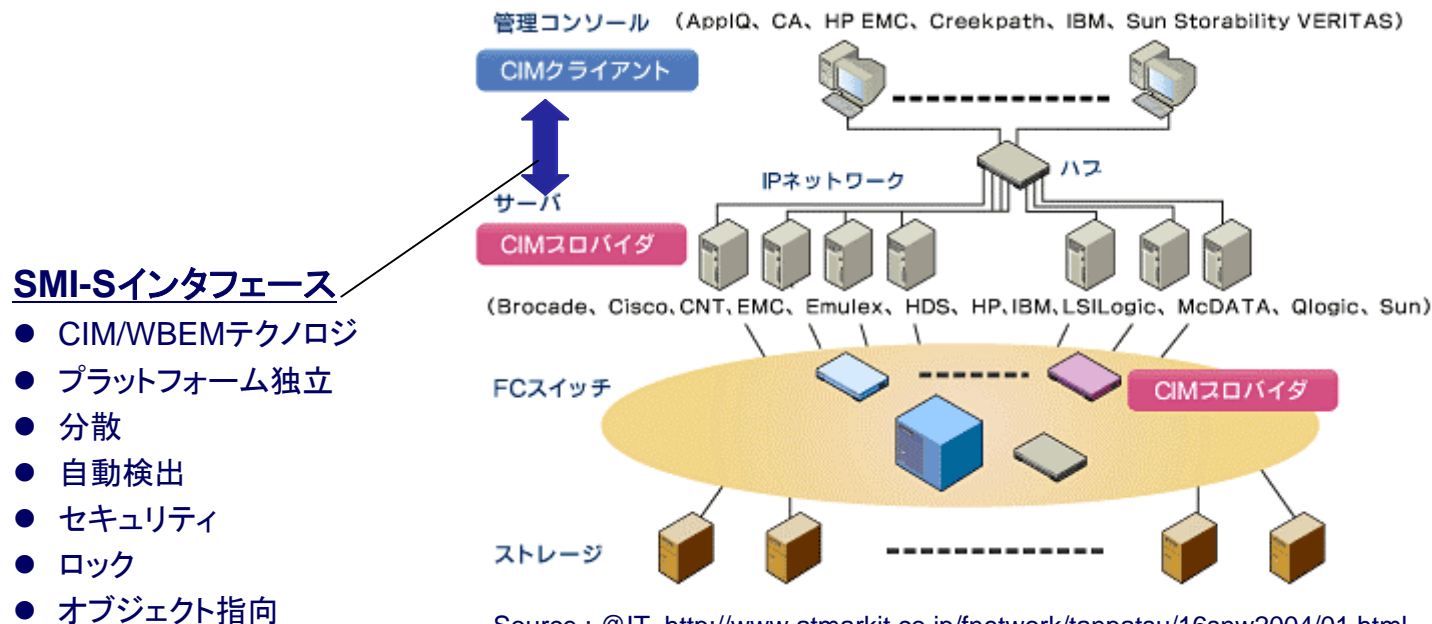
- 67th IETF @ San Diego (draft-iijima-netconf-soap-implementation-01)
 - NETCONF/SOAPアーキテクチャを提案
 - SOAPの利点として, Apache AxisによるAPIの自動生成機能が使用できること等を紹介
- 68th IETF @ Prague (draft-iijima-ngo-vlandatamodel-01)
 - AX-ON-API VLANデータモデルを提案
 - UML図, XMLスキーマを披露
 - VLANデータモデルのユースケースとして, INTEROP 2007のデモに使用したVLAN設定アプリケーションを紹介
- 69th IETF @ Chicago (draft-iijima-ngo-acldatamodel-00)
 - AX-ON-API VLANデータモデルを提案
 - UML図, XMLスキーマを披露
 - ACLデータモデルのユースケースとして, AMEL (AxMacListEditor)を紹介
- 70th IETF @ Vancouver (draft-iijima-netconf-soap-implementation-04)
 - NETCONF client & serverの簡単な実装デモを実施
 - Eclipse, Axis, Ant, Tomcatを用いれば, それらの環境設定, build.xmlと build.propertiesの作成, 10行のソースコード記述だけで動くことを紹介
 - NETCONF WG ChairのAndyから, Informational RFC化を目指すようにとのコメント
- 関連ドラフト
 - draft-atarashi-ngo-consider-architecture-01
 - サーバ, ストレージとの連携を考慮に入れたNETCONFアーキテクチャを提示

3 標準化状況 (Netconf関連の他社状況)

本資料は画面のみです

4 ストレージでの実装事例 (SNIAでのストレージ系実装例)

- SNIA (Storage Networking Industry Association)
 - ストレージベンダを中心とした業界団体. 技術標準化の取りまとめ等をしている
- SMI-S (Storage Management Initiative - Specification)
 - 相互運用を目的としてSNIAが策定した標準仕様
 - DMTF (Distributed Management Task Force)が定義したCIM (Common Information Model)やWBEM (Web-Based Enterprise Management)に基づく
 - CIM: プラットフォームやOSに依存しないコンピュータのオブジェクト指向管理モデル
 - WBEM: ネットワーク上のデバイスをWebベースで管理するための仕様



Source : @IT, <http://www.atmarkit.co.jp/fnetwork/tanpatsu/16snw2004/01.html>

4 ストレージでの実装事例

(SNIA SMI-S CTP (Conformance Testing Program) 結果)

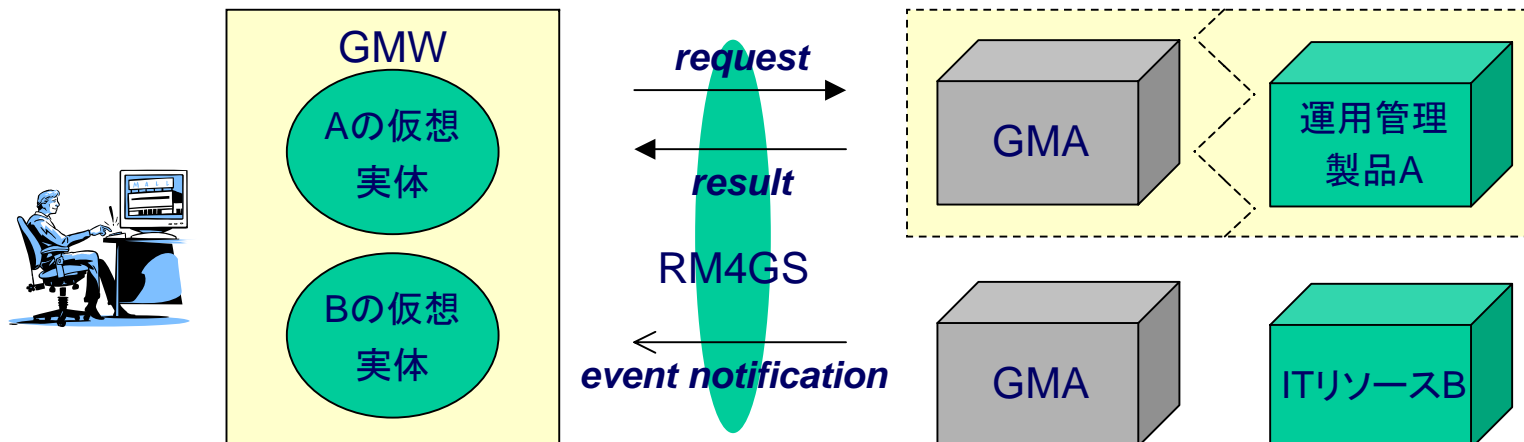
ベンダ名	製品名 ※斜字体:クライアント側製品	プロバイダ側テスト SMI-Sのバージョン	クライアント側テスト SMI-Clientのバージョン	最新テスト バージョン
EMC	CLARiiON, <i>EMC ControlCenter v6.0</i>	1.2	1.1	1.2.0.69
Hitachi Data Systems	Universal Storage Platform V, <i>HiCommand Storage Services Manager v5</i>	1.2	1.1	1.2.0.69
日立	SUNRISE, Universal Storage Platform	1.2	-	1.2.0.69
HP	StorageWorksDisk Array XP, <i>Storage Essentials v5.1</i>	1.2	1.1	1.2.0.50
IBM	Tivoli, <i>TotalStorage Productivity Center v3.3.2</i>	1.2	1.1	1.2.0.50
Brocade	Silkworm	1.1	-	1.1.0.98
Cisco	MDS 9000	1.1	-	1.1.0.45
Emulex	LightPulse FC HBA, LightPulse	1.1	-	1.1.0.85
富士通	ETERNUS	1.1	-	1.1.0.98
LSI Logic	Engenio Storage Systems	1.1	-	1.1.0.98
McDATA	Intrepid, Spherion,	1.1	-	1.1.0.98
NEC	NEC Storage, iStorage	1.1	-	1.1.0.94
QLogic	SANblade FC HBA 2300, SANbox2	1.1	-	1.1.0.85
CA	<i>BrightStor Resource Management v11.6</i>	-	1.1	
Symantec	<i>Veritas CommandCentral</i>	-	1.1	

4 ストレージでの実装事例（相互運用可能な機能（一部））

機能		内容	実績テストバージョン			
			EMC	HDS	HP	IBM
HTTP/SSL通信			1.2	1.2	1.2	1.2
SLP Discovery			1.2	1.2	1.2	1.2
Array管理	Volume Creation	ストレージ内に新規ボリュームを作成可能	1.2	1.2	1.2	1.2
	Volume-FC Target Port-HBA Initiator Allocation Creation					
	Volume-FC Target Port-HBA Initiator Allocation w/ Volume Addition					
Fabric管理	Zone Create		-	-	1.0	-
	Zone Add Member	Zoneに新規メンバ, ポート, WWNを追加可能				
	Zone Remove Member	Zoneからメンバ, ポート, WWNを削除可能				
	Zone Delete					
	Zoneset Create					
	Zoneset Add Member	ZonesetにZoneを追加可能				
	Zoneset Remove Member	ZonesetからZoneを削除可能				
	Zoneset Delete					
Zoneset Activate	不活性Zoneを活性化可能					
Switch管理	Port Enable	ポートを活性化可能	-	-	1.0	-
	Port Disable	ポートを不活性化可能				

5 サーバ系実装事例(ビジネスグリッド)

- ビジネスグリッドコンピューティングプロジェクト
 - 参画団体: 経産省, IPA(情報処理推進機構), 富士通, 日立, NEC
 - 2006年3月終了
 - 2006年5月より「ビジネスグリッド推進コンソーシアム」へ
 - 構成要素
 - GMW: Grid MiddleWare
 - GMA: Grid Management Agent
 - 運用管理製品, ITリソースごとにGMAを作成し, 異なる操作の違いを吸収
 - ITリソース: SystemWalker, JP1, VALUMOが管理するネットワーク, ストレージ, サーバ(Web, DB, AP)
 - GMA SDKによるJavaアプリケーション開発
 - RM4GS: Reliable Messaging for Grid Services
 - XMLベース



5 サーバ系実装事例 (GMA SDK)

- GMA (Grid Management Agent: グリッド管理エージェント) SDK
 - 「ビジネスグリッドコンピューティングプロジェクト」の一成果物
 - 他成果物は, RM4GS v1.1など
 - WSDM (Web Services Distributed Management) 1.0 準拠
 - OASISにて策定されたWebサービスによるハードウェア/ソフトウェア管理IF
 - 開発環境
 - OS: RedHatLinux2.1/3.0, Windows 2000 Server
 - Java: Java2 Runtime Environment 1.4.2
 - J2EE server (for RM4GS): J2EE RI 1.4
 - ライブラリ: Log4J 1.2.8, XML beans 2.0, RM4GSなど
 - 機能
 - GMWとのXMLメッセージ送受信
 - GMWへのイベント通知
 - 仮想実体のID管理機能
 - 「ITリソースの例えばIPアドレス」と「GMWにおける一意なID」とのマッピング
 - FTPを用いてGMWからの設定ファイル取得機能
 - FTPを用いてGMWへバックアップファイル転送機能
 - ログ管理機能

5 サーバ系実装事例 (Java API(機能の一部))

機能	Java API	内容
GMA実装	BGOperationAdapterFactory#getAdapter()	GMAを実装
	BGGmaOperation#start(BGOperationAdapterFactory adapterFactory, String gmwHost, String gmaHost, String gmaName, GmaLog gmaLog, Properties options)	GMAをスタートさせ, GMWからのリクエスト受付
メッセージ送受信	BGParseOperationRequest#getBodyXmlDocument()	GMWから送られるXMLメッセージのBody要素取得
	BGCreateResultMessage#setBody(String body)	GMWへ送るXMLメッセージのBody要素設定
イベント通知	GmaEvent#sendEventMessage(String gmaMsg)	GMWへイベント通知
ID管理	ObjectIDmanager#registerASID(in ASID, in ASProprietaryID)	IDマッピングテーブルにID登録
	ObjectIDmanager#removeASID(in ASID)	IDマッピングテーブルからID削除
File取得	BGFileTransferAgent#getFile(String from, String to)	GMWから設定ファイル取得
	BGFileTransferAgent#getFiles(String from, String to)	GMWから複数の設定ファイル取得
File転送	BGFileCollectorAgent#transferFile(BGGmaEndpointReference asURI, String FilePath, String HostingDirectory)	GMWへバックアップファイル送信
ログ管理	GmaLogForLog4J#error(Object message)	エラーレベルでログ出力

5 サーバ系実装事例 (ITリソースのオペレーション)

- BGOperationAdapter#invokeCommand(String operdata)
 - GMAの上記Java APIの引数operdata(XMLで記述)に, GMWから以下のWSDMオペレーションを渡すことによって, GMAは所望の設定をITリソースに対して実行

分類	オペレーション	内容
取得	<GetResourceProperty>	リソース内の指定されたプロパティの値を取得
	<GetMultipleResourceProperties>	リソース内の指定されたプロパティ群の値を取得
	<QueryResourceProperties>	Xpathを用いて, リソース内の指定されたプロパティドキュメントを取得
	<QueryRelationshipByType>	リソースの関連情報を取得
設定	<SetResourceProperties>	リソースが持つプロパティドキュメント内のプロパティを変更(insert, update, and delete)
通知	<Subscribe>	イベント通知を要求
	<GetCurrentMessage>	最後のイベントの通知を要求
	<PauseSubscription>	イベント通知の一時停止を要求
	<ResumeSubscription>	一時停止したイベント通知の再開を要求

6 InteropでみつけたON-API活用事例

本資料は画面のみです

認証・検疫ソリューション

InfoAge Empowered by Innovation NEC

Zoom

InfoCage PC検疫 イントラ制御 with IP8800

協調型セキュリティによるネットワークセキュリティ

InfoCage Networkシリーズ

特長

- シンククライアント端末と許可された通常端末のみを接続させることが可能
- 専用アプライアンスサーバ、データベースアプリケーション、エージェントソフトが不要
- 標準化が進められているNETCONFを利用し、安全、確実かつスピーディーに接続許可端末のみにアクセス許可

概要

InfoCage PC検疫 イントラ制御 with IP8800は、IPスイッチ UNIVERSE IP8800/Sシリーズと連携し、企業ネットワークで稼働している個人所有のPCの検出など、ポリシー違反のPCをネットワークに接続させない、次世代のセキュアなLANを提供します。

シンククライアント環境のネットワークセキュリティ対策をターゲットとして、シンククライアントの各種方式（仮想PC型、画面転送型、ネットワークアダプタ型）に合わせたセキュアなアクセス環境を提供し、接続の許可されていない端末の接続を防止することが可能です。

運用形態例: DivX Presentation Server (自動MetaFrame) シンククライアントサーバ
検疫PC型: VirtualPC Center
ネットワーク型: Arance

適用メリット

- サブネットワークに専用のアプライアンスサーバが不要のため容易に導入が可能
- データベースアプリケーション、エージェントソフトが不要なため安価な導入、容易な運用を実現
- 初期設定後、運用管理者の手を介さない自動運用が可能
- 未許可端末を接続させないことによるセキュアなLANを提供

入退出管理 & セキュリティ

PhoneAppliとAlaxala ONAPIによる個人認証/ネットワーク開通連携

Alaxala Empowered by Innovation NEC

オフィスセキュリティ & 社員管理ソリューション

PhoneAppli Serverを用いたトータルセキュリティ

各機能の説明

PhoneAppli Server	IP-PBX	UPnP-Action Control Server	ONAPI対応 L2 SWITCH
<ul style="list-style-type: none"> IP Phone用XMLアプリケーションサーバ 各種アプリケーション連携 	<ul style="list-style-type: none"> SIP, H323対応 TAPI対応 	<ul style="list-style-type: none"> Active Directoryと連携し、UPnPデバイス、ドア、書庫、キーボックスの検出管理・設定などを制御 	<ul style="list-style-type: none"> ONAPI機能搭載によって、リモートからのPort制御が可能

遠隔設定支援

Empowered by Innovation NEC

遠隔機器管理ソリューション

グローバル空間の管理サーバからNAT配下の機器を一元管理

<NTTコミュニケーションズ株式会社様との共同開発>

特長

- ネットワーク機器の自動設定と一元管理を実現
- NAT配下のプライベートネットワークに設置された機器管理も可能
- 複数のネットワーク機器管理ソリューションの一元管理を実現

概要

NAT配下のネットワーク機器に対する自動設定と一元管理

ネットワーク機器の自動設定、一元管理も可能なソリューションとして以下が挙げます。

- UNIVERSE IP8800/S3600シリーズ networkIPベースとした遠隔管理ソリューション
- UNIVERSE IP2000シリーズ SMF/SSL Management Frameworkソリューション
- NAT内側のプライベートネットワークに設置された機器に対して、NTTコミュニケーションズ株式会社様提供のm2m-x小形アダプタによるオンデマンドセキュリティの導入が可能。NAT越え機能と組み合わせることにより、グローバル空間の遠隔管理サーバからネットワーク機器の自動設定および一元管理も可能です。

自動設定 一元管理

管理対象 (IX2000) 小型アダプタ

管理対象 (IP8800/S3600) 小型アダプタ

遠隔機器管理センター

m2m-x NTTコミュニケーションズ株式会社様が提供するセキュアな遠隔管理を実現するプラットフォーム (machine-to-machine for anything, anytime and anywhere)

6 ON-APIを使ったアプリケーション

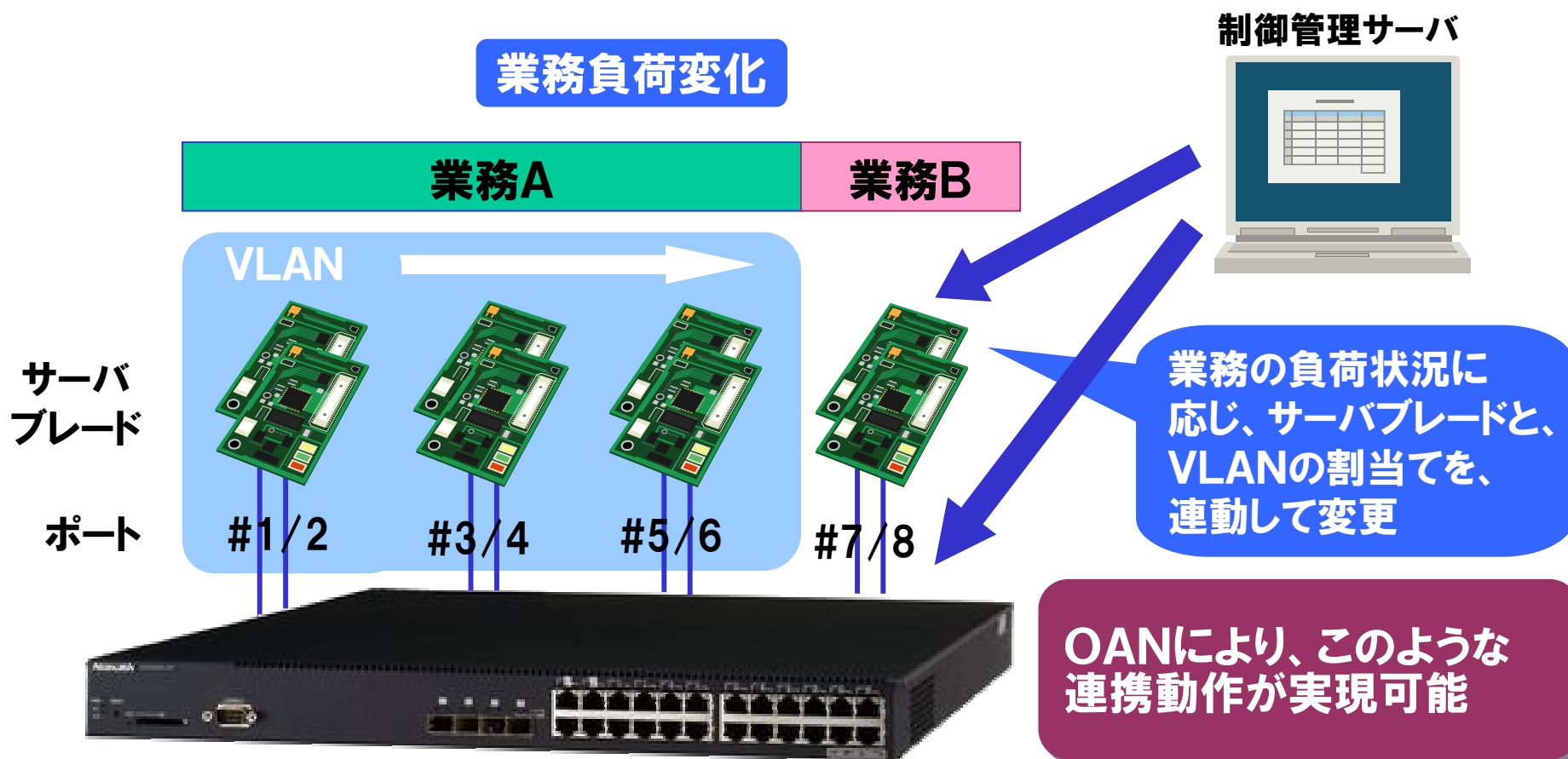
本資料は画面のみです

ON-APIを使ったアプリケーションのデモンストレーションを行います。

- 装置OSのアップデート
- 装置Configの自動収集
- ループ検知

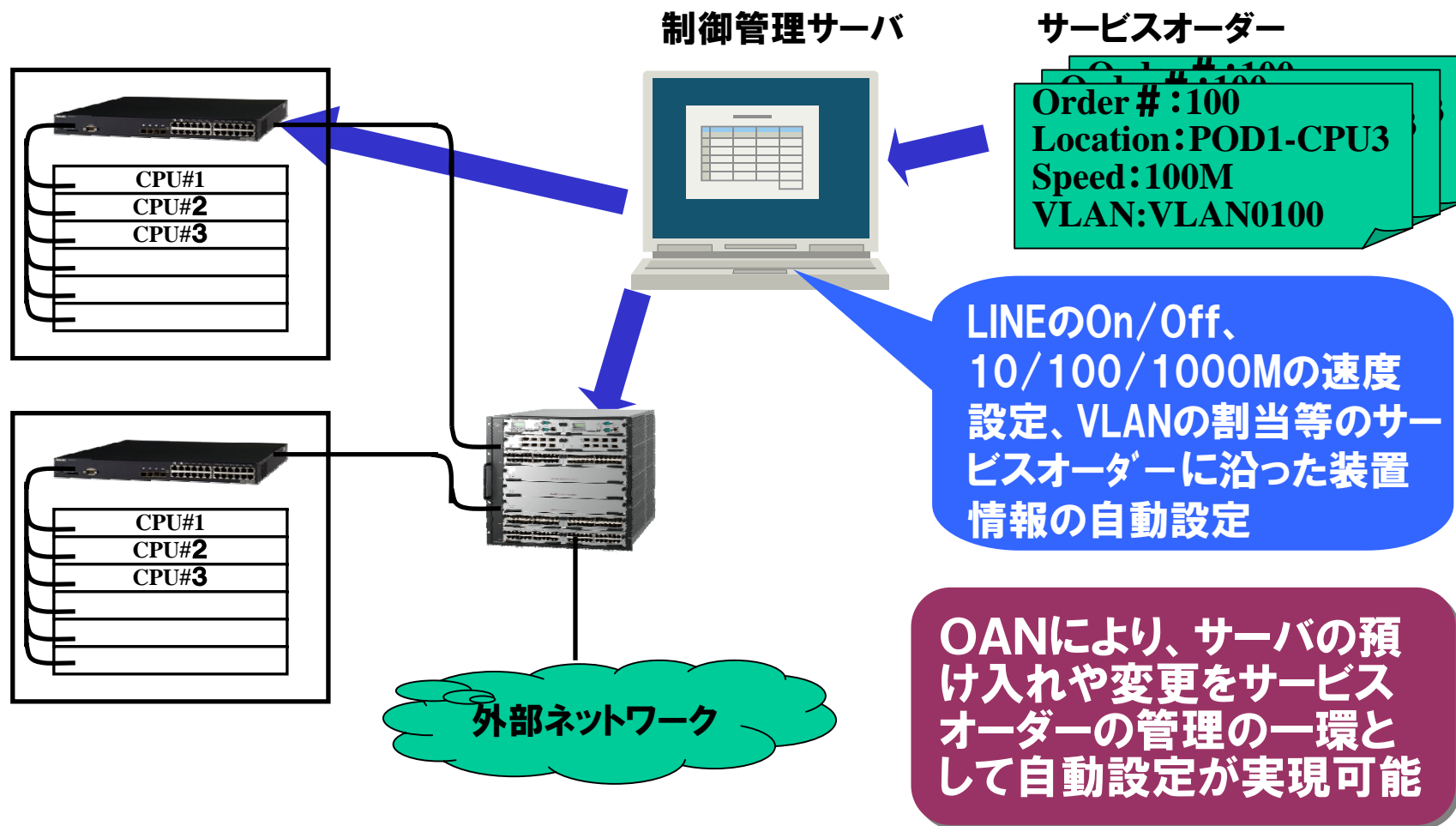
6 ON-API活用事例(適用例:1)

業務負荷に応じた、オンデマンドネットワーキング



6 ON-API活用事例(適用例:2)

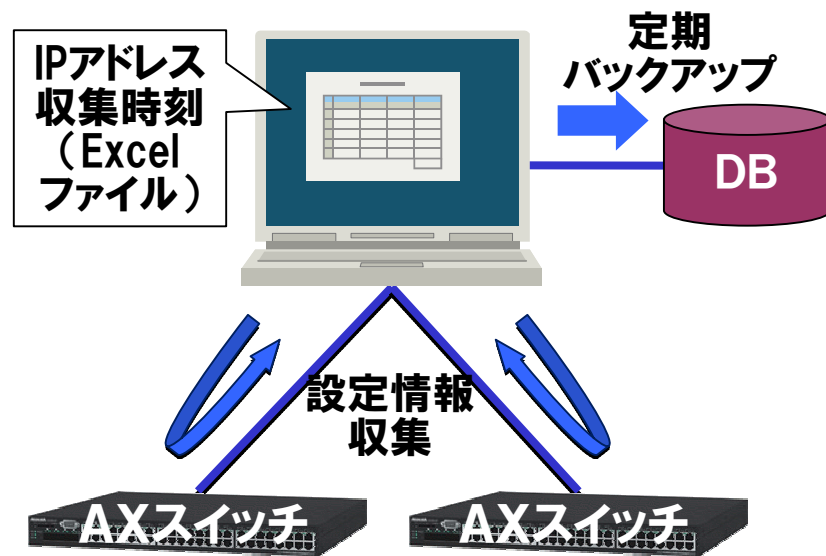
データセンターの自動構成設定支援



6 ON-API活用事例(適用例:3)

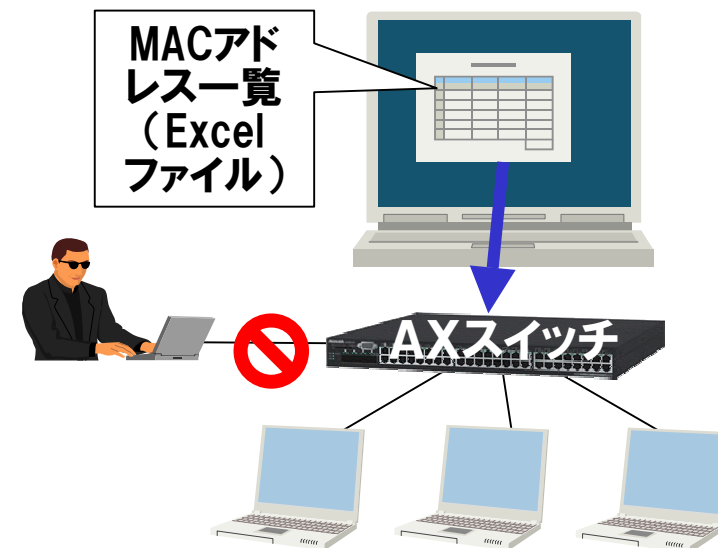
OANによる運用自動化

設定情報(コンフィグ)の自動収集と定期バックアップ



ExcelファイルでIPアドレスと収集時刻を指定して、各スイッチの設定情報を自動収集

MACフィルタの一括設定

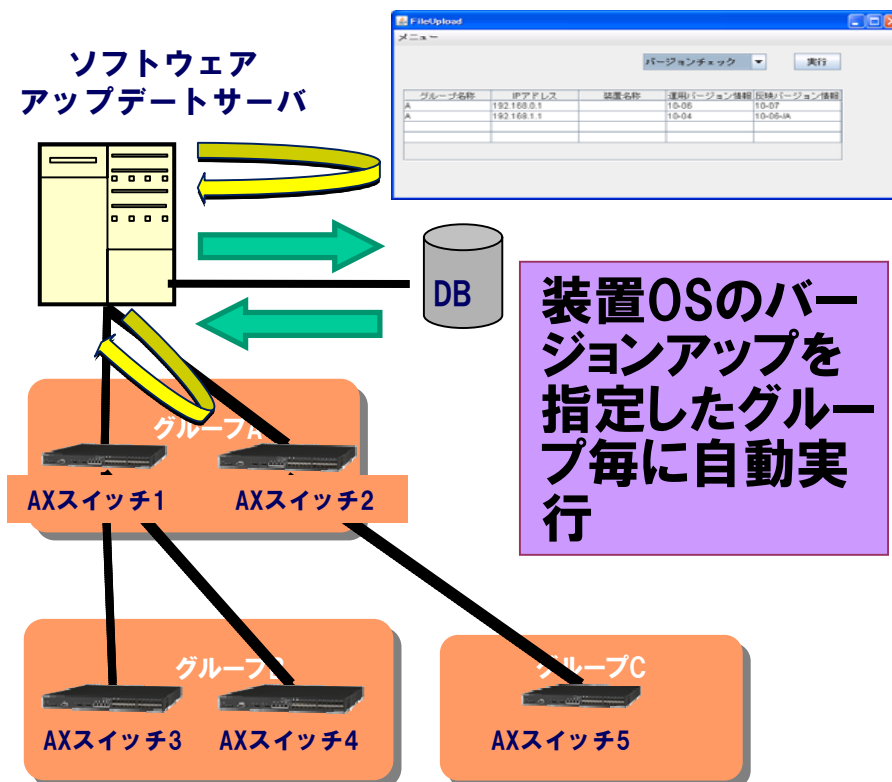


Excelファイルで指定されたMACアドレスのみを許可するフィルタを一括設定

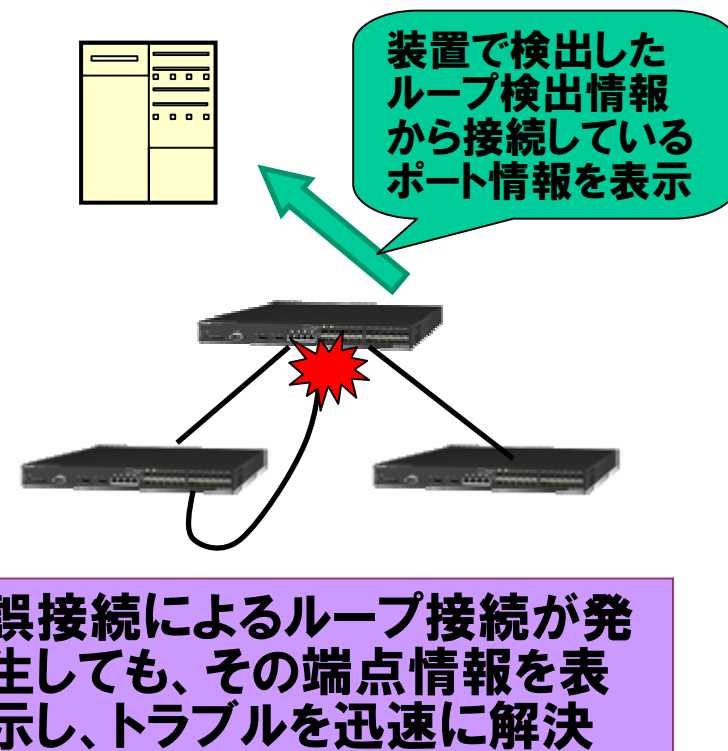
6 ON-API活用事例(適用例:4)

OANによる運用自動化

装置OSのバージョンアップ



ループ検知・表示



6 ON-API活用事例 (AX-Config-Master)

AXCMは、ネットワーク構成を管理し、装置の状態管理や構成の変更、稼働情報の表示等を一元的に行います。

ネットワーク構成の一元管理

- ネットワーク上の機器やPCを一元的に管理し、全体を見ながらの運用が可能

コンフィグ情報の一元管理

- 装置のもつコンフィグ情報を一元管理、障害時のダウンロードや機器での変更時のアップロードが可能

ネットワーク状態の一元管理

- 装置や回線の障害を検知し、ネットワークマップ上で表示
- 障害箇所の特定が容易
- VLANの状態を画面上で確認(見える化)可能

The screenshot displays the AX-Config-Master-View software interface. The top window shows a network topology diagram with nodes labeled 'Manager', 'E-Box-101', 'E-Box-102', and 'E-Box-103'. A dashed blue circle highlights a portion of the network, with a callout box labeled '状態管理' (Status Management). Another callout box labeled '構成管理' (Configuration Management) points to the network diagram. The bottom window shows a configuration management interface with a list of configuration files and a 'コンフィグ管理' (Config Management) callout box. The configuration files listed include 'Local Config', 'Manager Config', 'StartUp Config', and 'Running Config'. The interface also shows a list of network interfaces and their configurations, such as 'interface gigabitethernet 0/21' and 'interface vlan 1000'.

Thank You !!

Alaxala

<http://www.alaxala.com/>