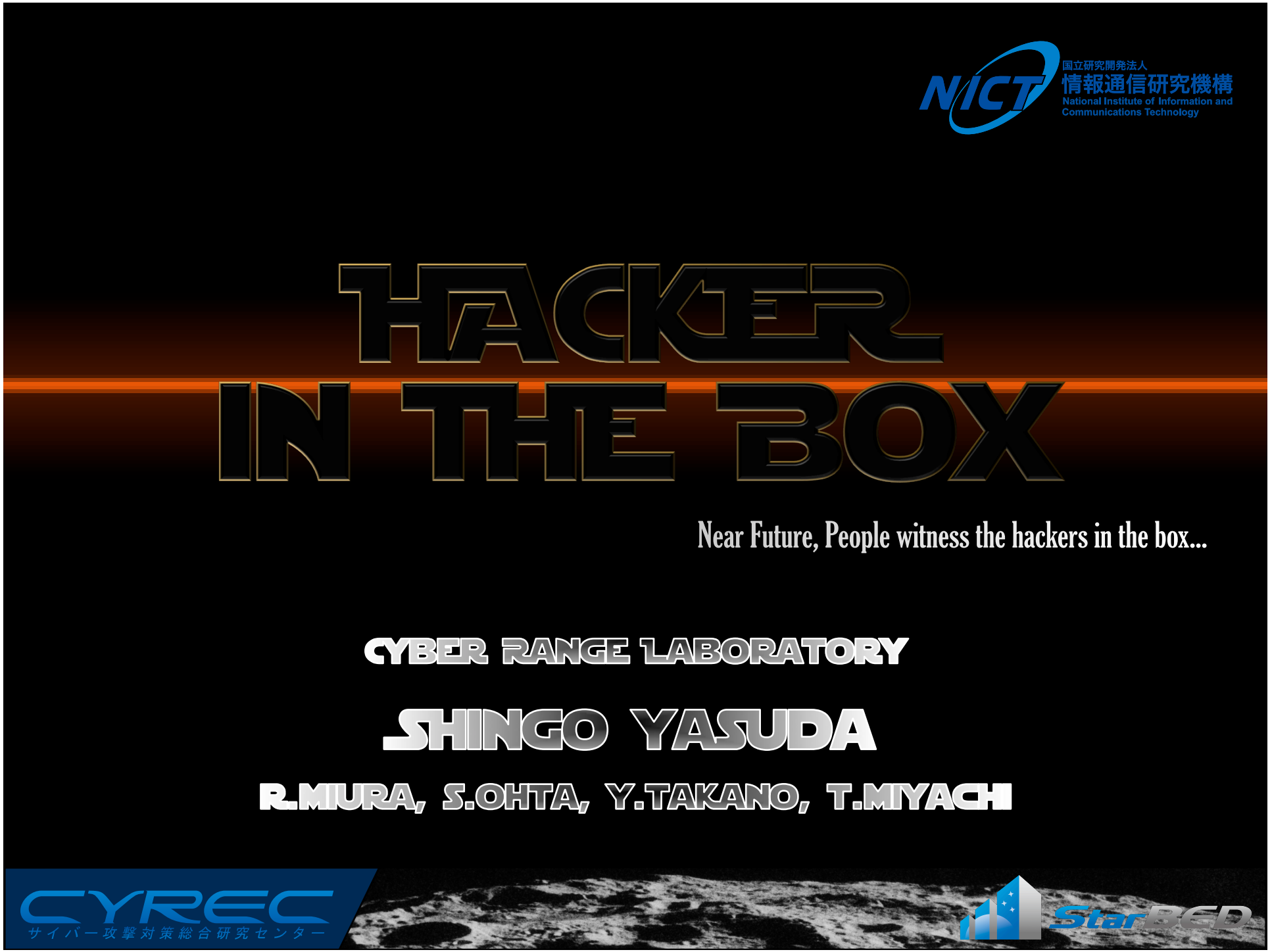

NICT
国立研究開発法人
情報通信研究機構
National Institute of Information and Communications Technology
HACKER IN THE BOX
Near Future, People witness the hackers in the box...
CYBER RANGE LABORATORY
SHINGO YASUDA
R.MIURA, S.OHTA, Y.TAKANO, T.MIYACHI
CYREC
サイバー攻撃対策総合研究センター
StarBED

標的型攻撃の増加

- サイバー攻撃の遭遇率=19.3%※
  - うち標的型攻撃=30.4%
  - 2014年度は2013年度に対して5.2倍

- ニュースな事例
  - 年金機構
  - 防衛系企業

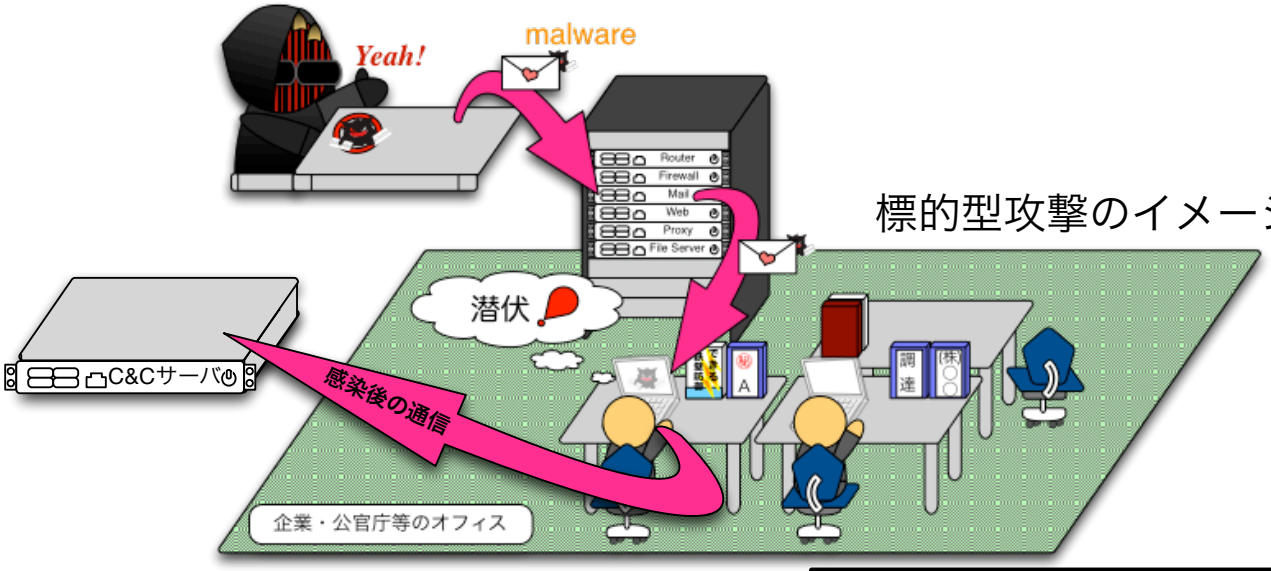
※IPA情報処理推進機構調査
調査対象　　：業種別・従業員数別に抽出した13,000企業
調査対象期間：2013年4月～2014年3月
調査方法　　：郵送調査法
回収結果　　：1,913件（有効回収率14.7%）
主な調査項目：回答企業の概要、情報セキュリティ体制・対策の現状、コンピュータウイルス・サイバー攻撃による被害状況

CYRECの発足

国立研究開発法人 情報通信研究機構 National Institute of Information and Communications Technology

- サイバー攻撃対策総合研究センター
  （CYREC：Cybersecurity Research Center）
  - 標的型攻撃等の新たなサイバー攻撃の抜本的な解決を目指し、NICTが主導的な役割を担って国内の英知を結集する体制を構築することで、当該サイバー攻撃の対策技術の研究開発及び開発された技術の速やかな社会展開を推進
- サイバー防御戦術研究室
  - nicterで培った基盤技術群を活用し、APTによる攻撃等に対する能動的かつ根本的な防御技術を確立・実現
- サイバー攻撃検証研究室
  - StarBEDとその基盤技術群を活用し、攻撃・防御の検証用模擬環境を用いたAPTによる攻撃等を実践的に検証
  - StarBED技術研究センター(テストベッド研究開発推進センター）と連携

標的型攻撃の概要



標的型攻撃のイメージ

標的型攻撃の段階
①情報収集
- ソーシャルハッキング等
②初期潜入
- メール添付ファイル等による感染
③攻撃基盤構築
- 初期感染マルウェアによるツールDL
④攻撃
- 自動/攻撃者によるデータ取得

セキュリティ人材不足

- セキュリティ人材育成が急務
  - セキュリティ人材8万人月不足
  - 現職のセキュリティ人材の6割がスキル不足

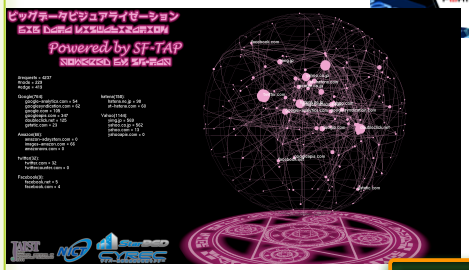
➢ 人材育成の裾野を広げ，官民の対応力の底上げ，一般市民への啓蒙活動による社会全体のリテラシーの向上

CYRECの取り組み

国立研究開発法人 情報通信研究機構 National Institute of Information and Communications Technology

対策・解析技術の研究開発

- StarBED/nicterで培った技術を応用



電網検証
Alfons

人材育成イベントへの技術協力

- 各種セキュリティイベントに協賛/後援，技術協力

SECCON

Hardening Project

enPiT Security SecCap

CYDER

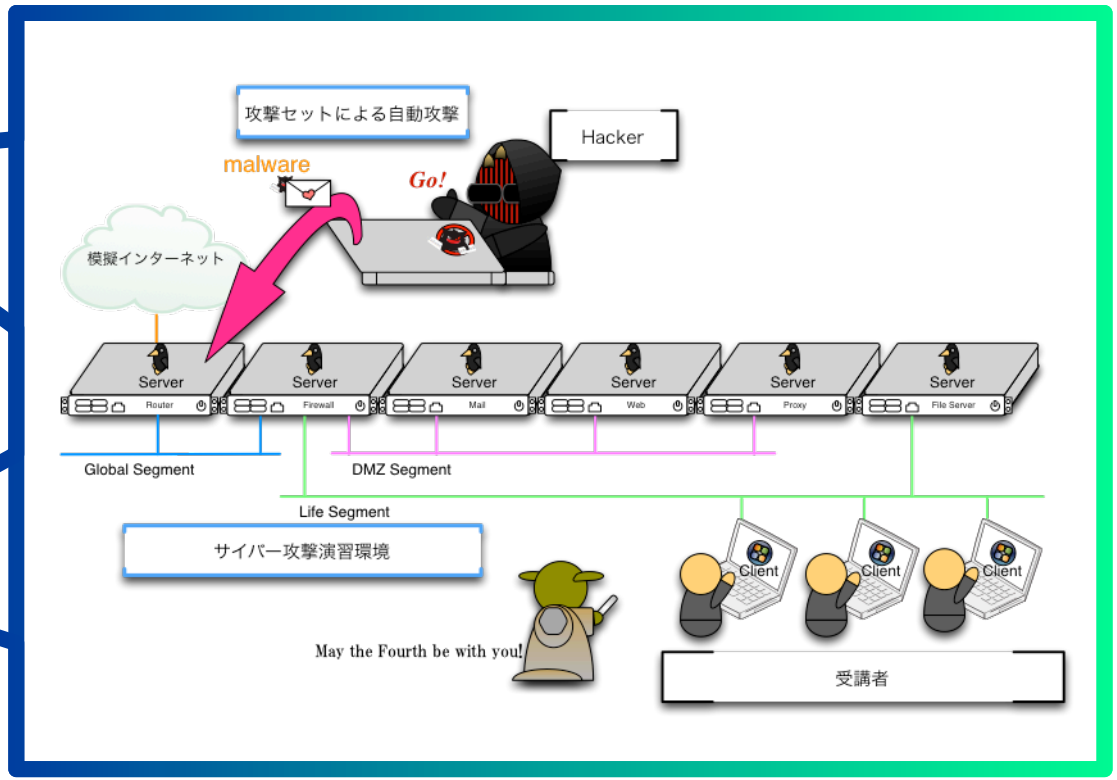
Hacker in the box

国立研究開発法人 情報通信研究機構 National Institute of Information and Communications Technology

- サイバー攻撃対策人材育成パッケージ
  - 演習環境構築システム
  - サイバー攻撃演習カリキュラム

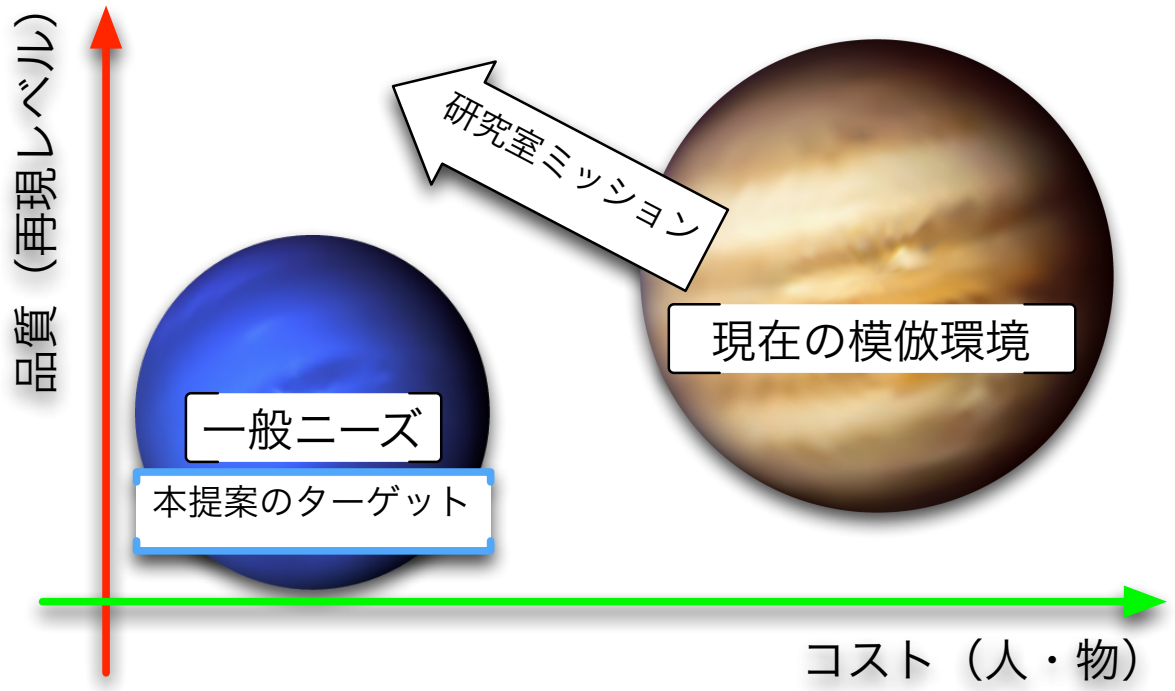
北陸StarBED技術センター

可搬型サイバー演習パック



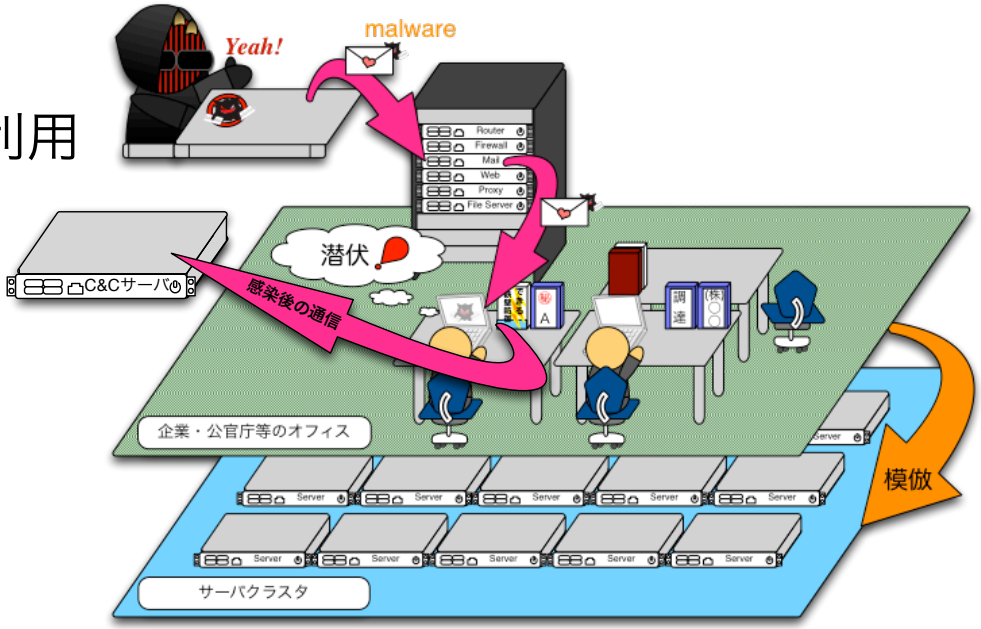
ターゲット

- 大学・高等学校での講義や交通安全教室のサイバー版を想定し，広く一般市民迄を対象



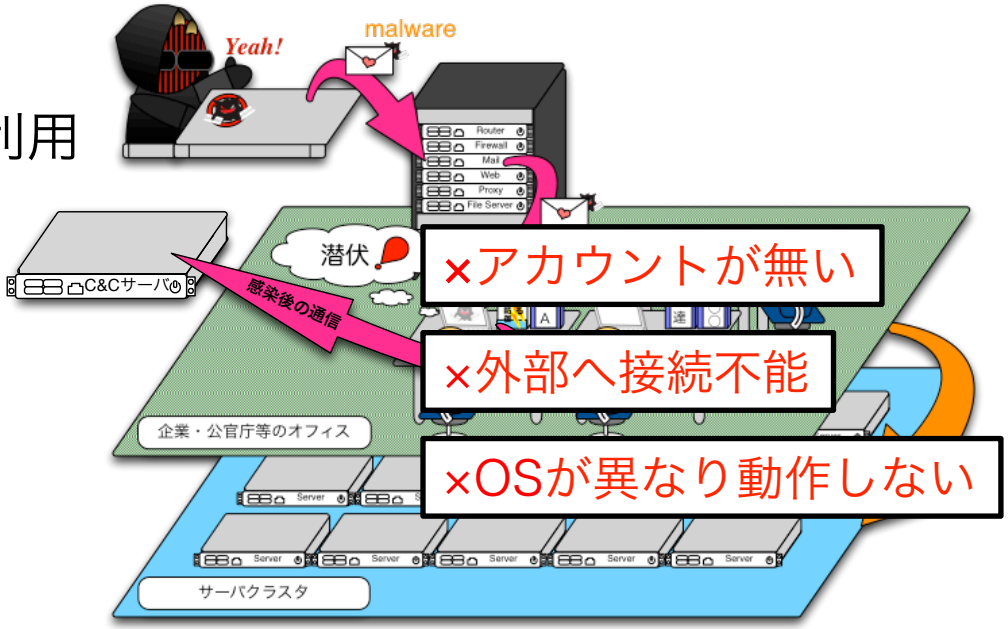
動的解析環境の研究開発

- 高詳細な模倣環境の必要性
  - 解析環境検知
    - 仮想環境検知
    - Sandbox検知
    - etc..
  - 想定外環境での不全
    - 攻撃対象の環境情報の利用
      - ユーザアカウント
      - Proxy Server IP
      - etc..



動的解析環境の研究開発

- 高詳細な模倣環境の必要性
  - 解析環境検知
    - 仮想環境検知
    - Sandbox検知
    - etc..
  - 想定外環境での不全
    - 攻撃対象の環境情報の利用
      - ユーザアカウント
      - Proxy Server IP
      - etc..



課題整理

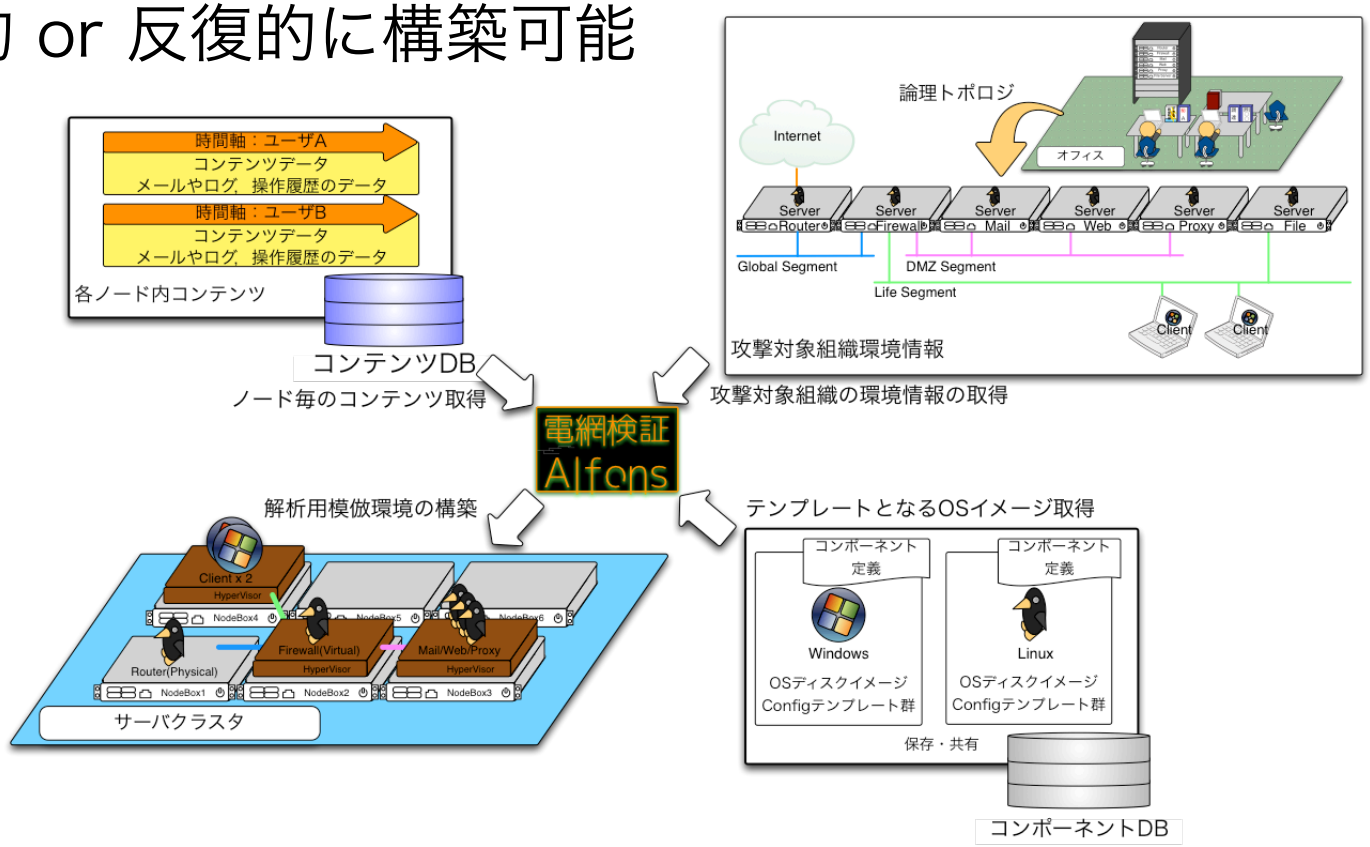
特殊な環境構築要件	
課題	**解決要件（研究開発）**
解析環境検知回避 - 仮想環境検知 - SandBox検知	物理・仮想混在環境の構築
	インスタンスの設定やコンテンツの模倣
	インスタンスの振る舞い模倣
	外部組織とのインタラクションの模倣
反復的な環境構築	構築したHoneynet環境の構成保存，再構築
必要な物理資源の削減	サービスの動的配置技術
	テンプレートと差分データによる実データ圧縮
コンテンツの模倣	シナリオからの自動生成技術
シナリオ作成	記述形式
中長期的な運用	時間，人材確保（連携先確保），運用の自動化

既存環境・ツール

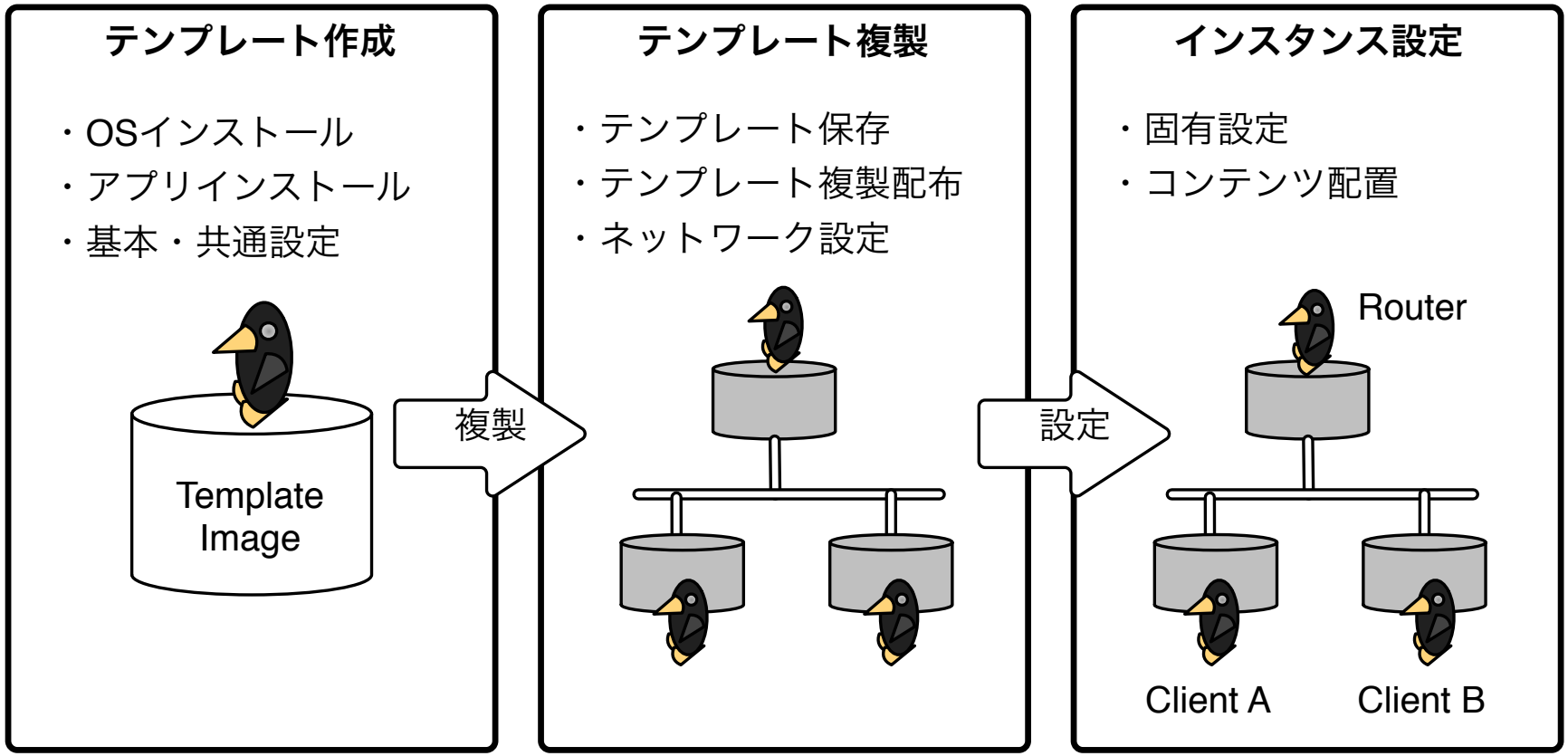
- StarBED/SpringOS
  - OSイメージの配布(物理ノード)
  - ネットワーク設定機構(VLAN)
  - 均一なノードを大規模に展開可能
  - ノードの多様性再現は困難
- Chef/Ansible
  - 同一の構成を多数のノードに適用するのが主な目的
  - 設定ファイルは手続き型記述が煩雑
  - SpringOSとの連携が困難
- クラウドコントローラ
  - ノードの複製とネットワーク設定
  - コンテンツの配置は不可

電網検証 Alfons

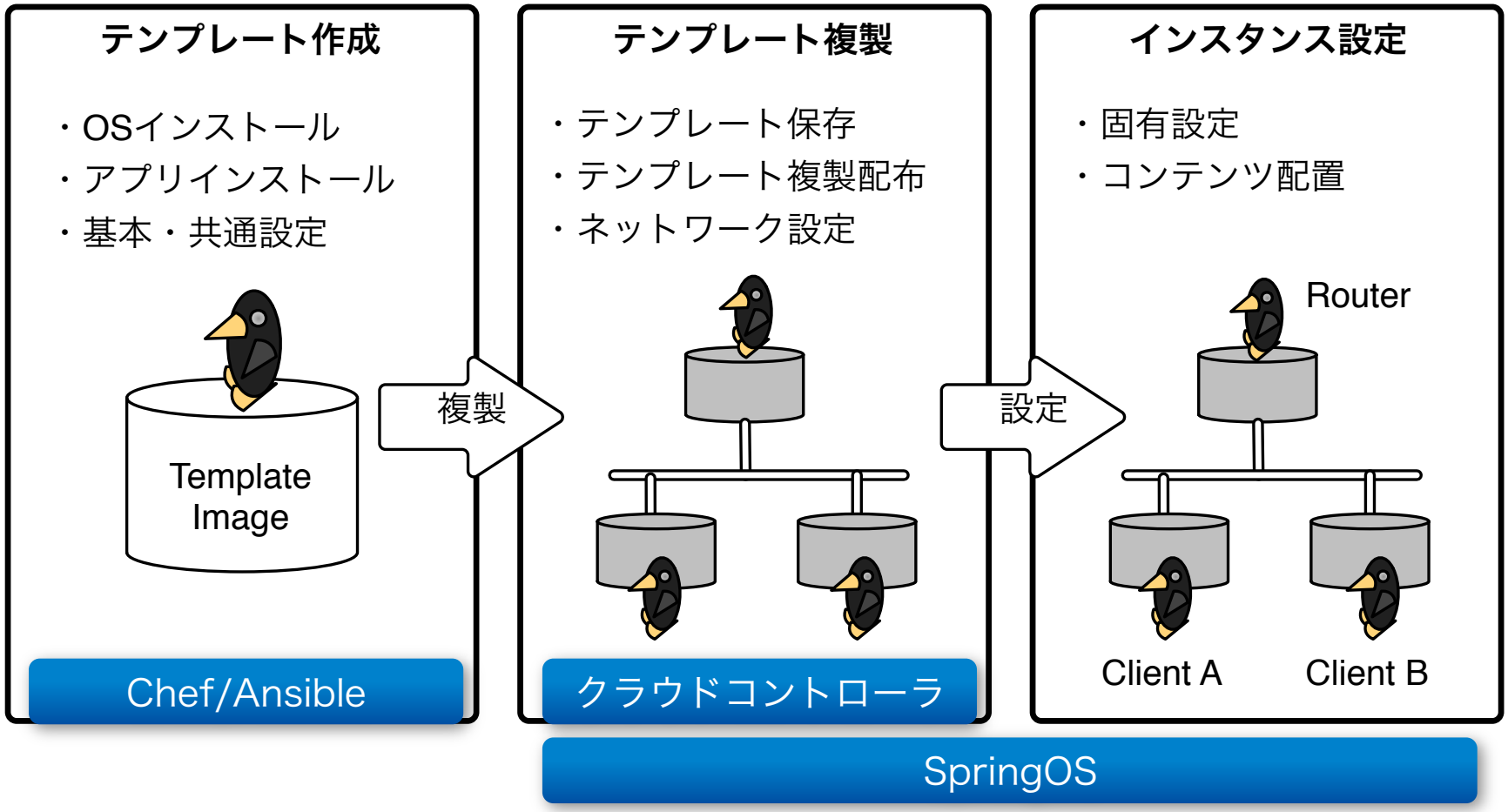
- 模倣環境構築システム
  - コンテンツ挿入型環境構築システム
  - 対話的 or 反復的に構築可能



インスタンス生成過程


テンプレート作成
・OSインストール
・アプリインストール
・基本・共通設定
Template Image
複製
テンプレート複製
・テンプレート保存
・テンプレート複製配布
・ネットワーク設定
設定
インスタンス設定
・固有設定
・コンテンツ配置
Router
Client A
Client B

インスタンス生成過程


テンプレート作成
・OSインストール
・アプリインストール
・基本・共通設定
Template Image
Chef/Ansible
複製
テンプレート複製
・テンプレート保存
・テンプレート複製配布
・ネットワーク設定
クラウドコントローラ
設定
インスタンス設定
・固有設定
・コンテンツ配置
Router
Client A
Client B
SpringOS

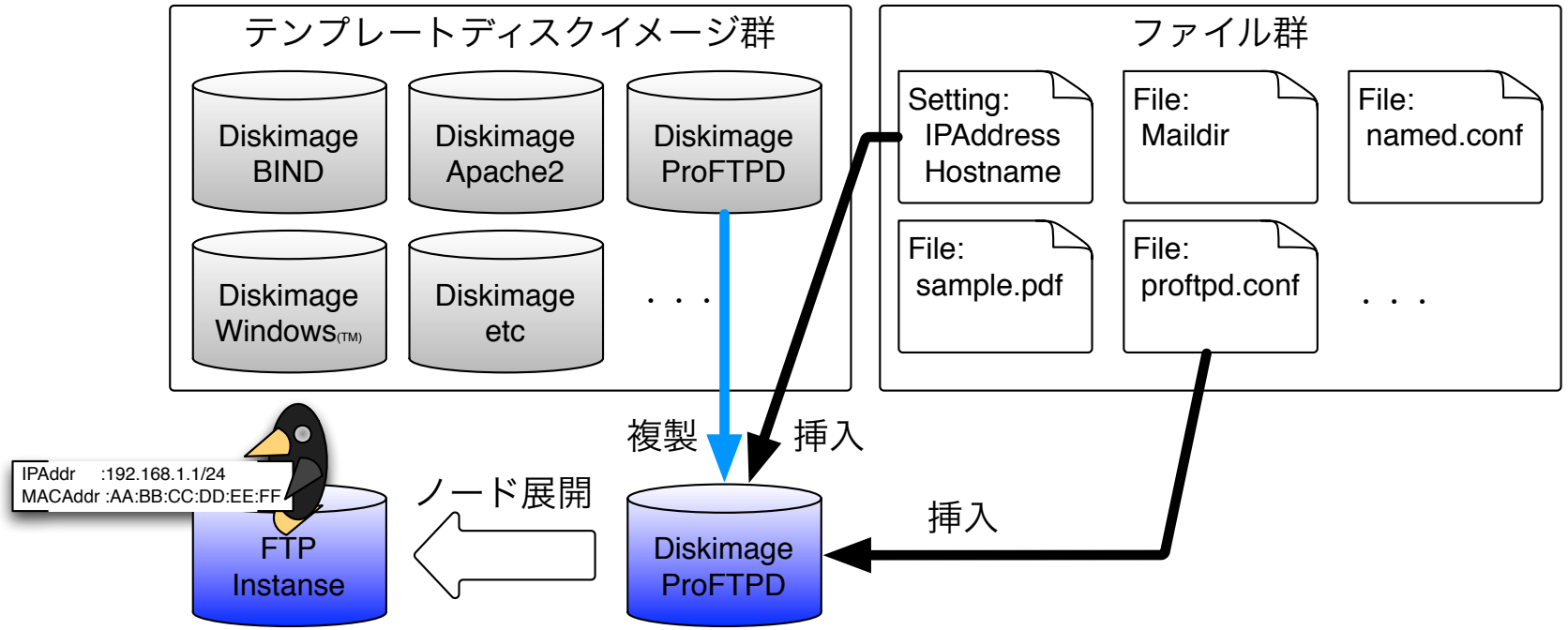
模倣環境の特徴

- 模倣対象が存在
  - 設定ファイル
  - コンテンツ
- サービスの同一性
  - 一般的な組織ネットワークのサービスは同一
    - Firewall,DHCP,Mail,Proxy,Web,AD,FTP,CIFS…etc
  - トポロジや設定のみ異なる

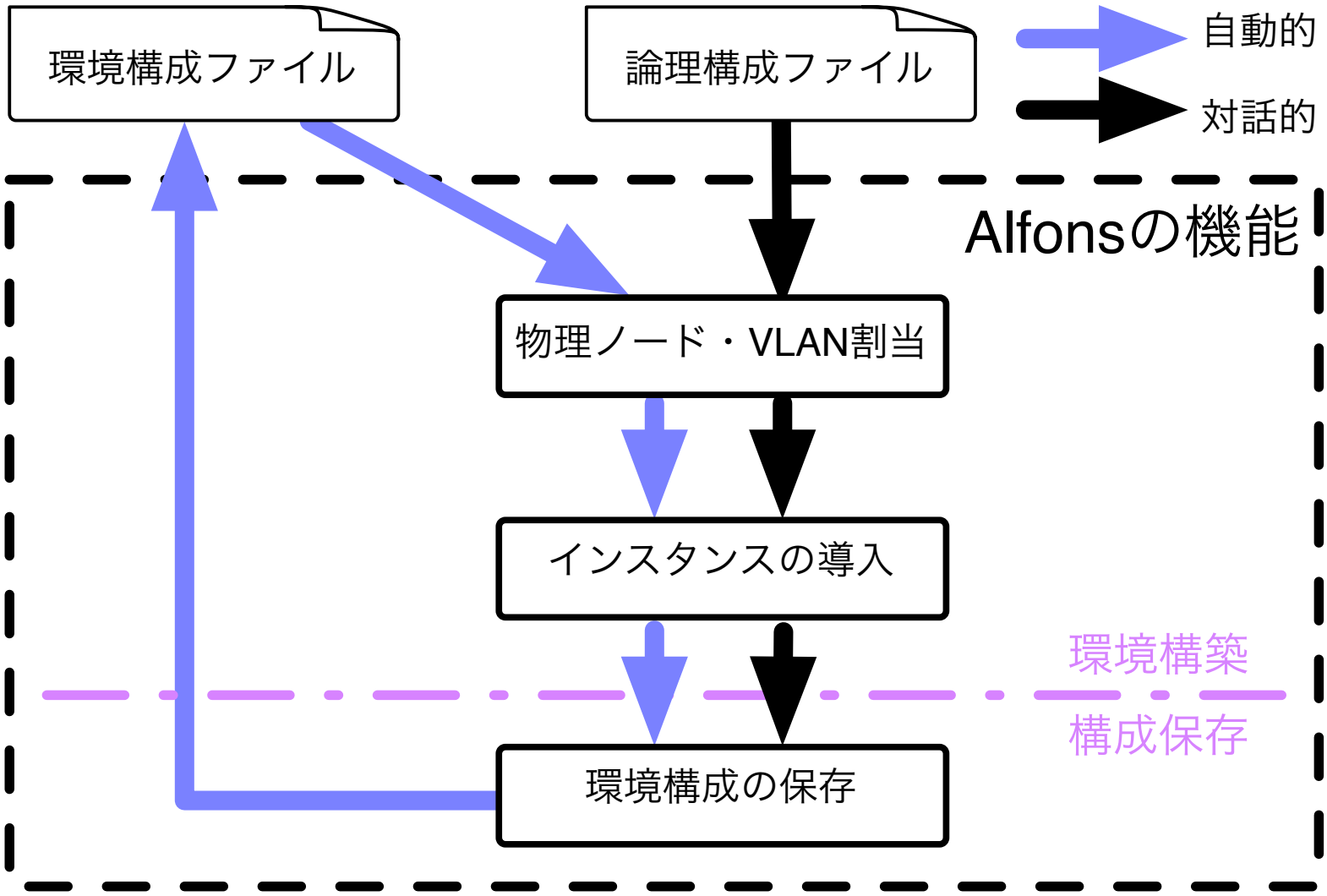
➢ 複製に特化した方が効率的
  - 実環境の設定ファイルの挿入
  - 実(模擬)コンテンツ挿入

ビルディングブロック型環境構築

- テンプレート＋設定・コンテンツファイル群
  - 置換によるファイル内容の置き換え(オプション)
- ネットワークは対象環境を模擬

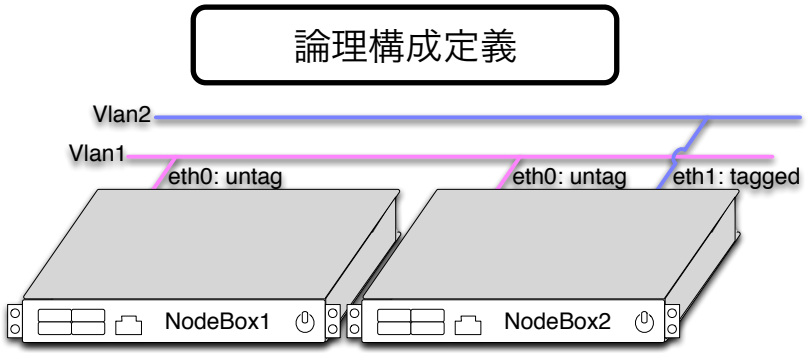


環境構築操作フロー


環境構成ファイル
論理構成ファイル
自動的
対話的
Alfonsの機能
物理ノード・VLAN割当
インスタンスの導入
環境構築
構成保存
環境構成の保存

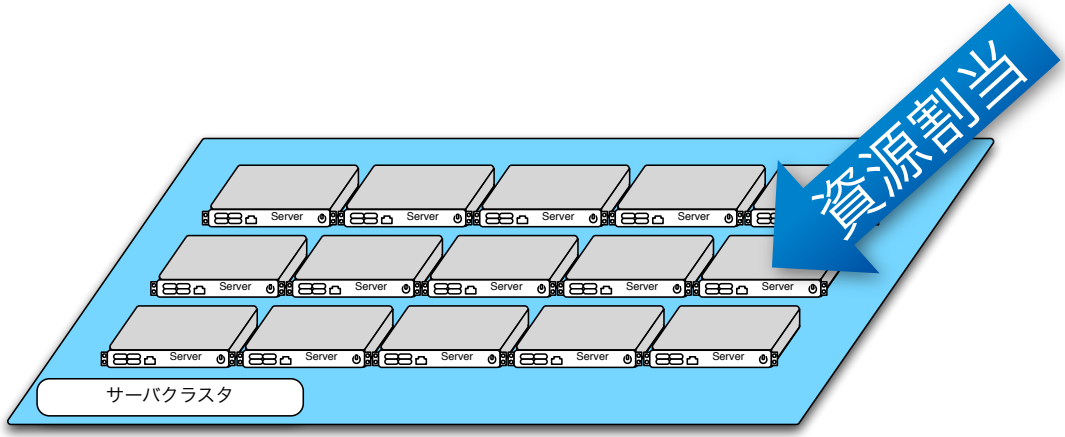
物理資源割当

- 論理構成定義
  - 物理資源と検証環境の分離
    - 環境移行・複製を実現
  - 用語
    - NodeBox：物理ノード



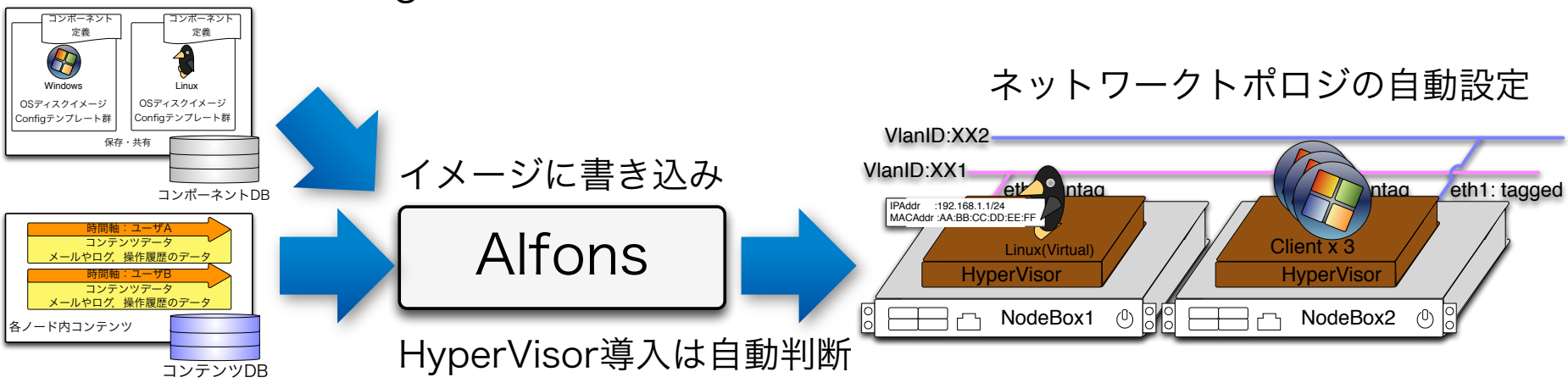
論理構成定義ファイル

```
nbs:
  nb1:
  nb2:
vlans:
  vl1:  {nb1: {etho: ut}, nb2: {etho: ut}}
  vl2:  {nb2: {eth1: tg}}
```



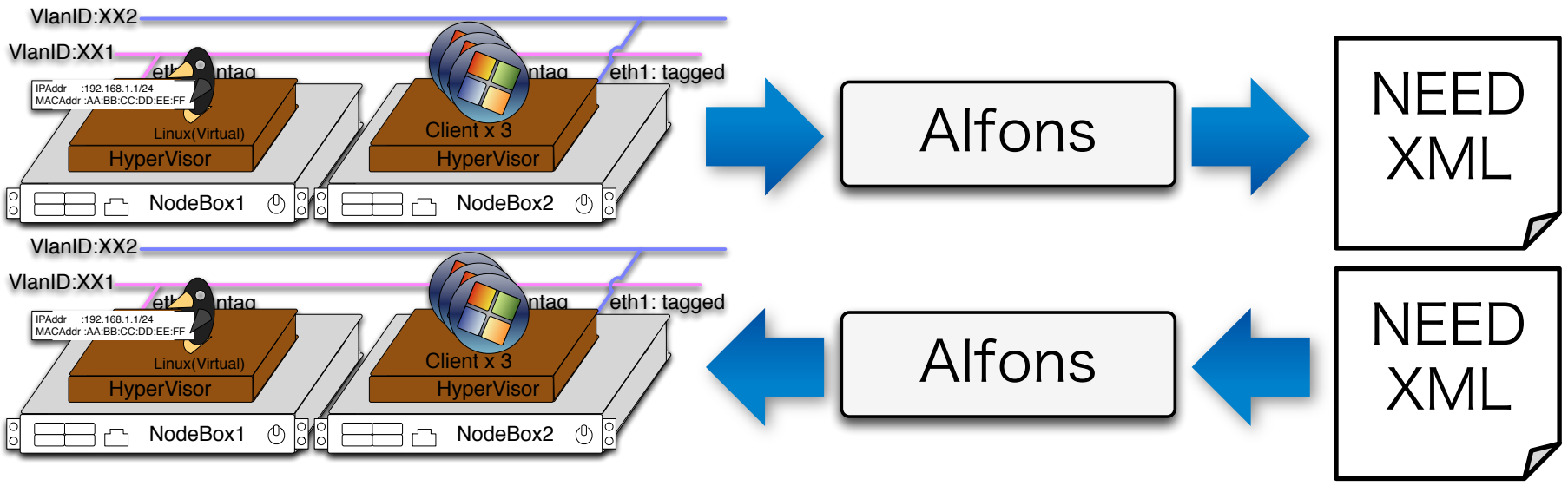
インスタンス導入

- インスタンス
  - テンプレートイメージ+設定ファイル+コンテンツ
    - OS毎の設定方法の差異を吸収
      - IPAddress
        - » Linux：/etc/network/interfacesの書き換え
        - » Windows：netshコマンドbatch処理をrun onceで起動
    - コンテンツはファイル単位でインスタンスに事前挿入
      - libguestfs



環境の保存・再構築

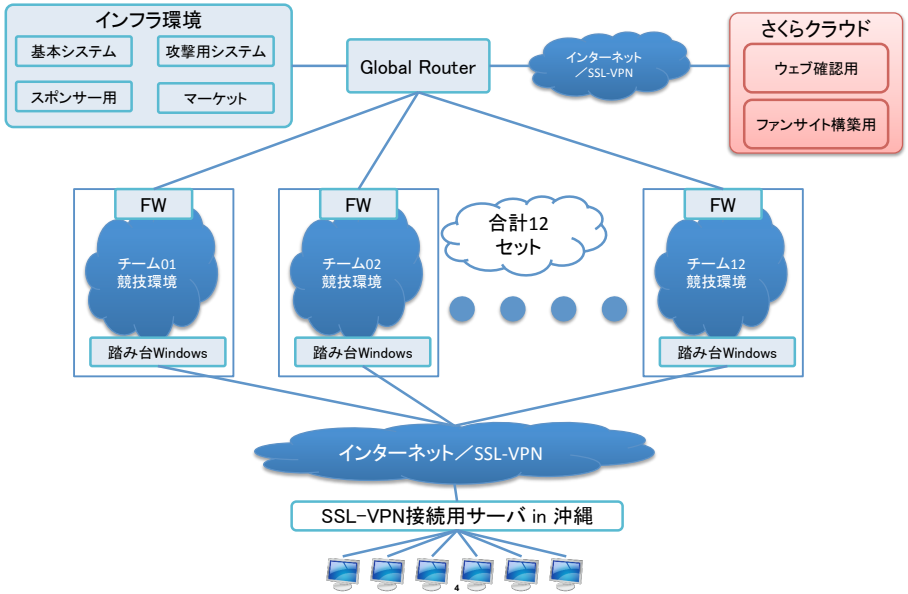
- 対話的に構築した環境構成情報を保存
  - XML形式
  - XMLから環境一括構築可能
    - 物理資源の変更可能(複製/並列)



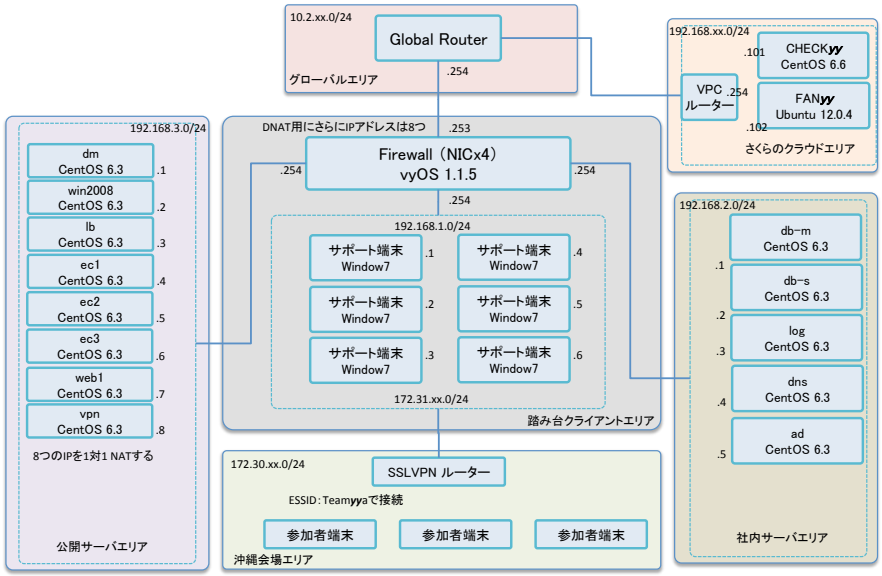
適用事例1

- Hardening 10 MarketPlace
  - 企画/実行： WASForum Hardening Project実行委員会
  - 脆弱性のあるECサイトのハードニング(堅牢化)力を競う
  - チーム対抗で8時間耐久競技

トポロジ全体



チーム環境



適用事例1

- 構成資源量
  - 80物理ノード(NodeBox)，100 VLAN利用
  - 335インスタンス作成

Server	CPU	Memory	DISK	Network IF
Alfons	Intel Xeon®E5-2620 v3 x2	64GB	FusionIO SX300 x 2	10Gbps
Group J	Intel Xeon®X5670 x2	48GB	SATA HDD x2	1Gbps
Group N	Intel Xeon®E5-2650 x2	128GB	SATA HDD x1/SSD x4	1Gbps

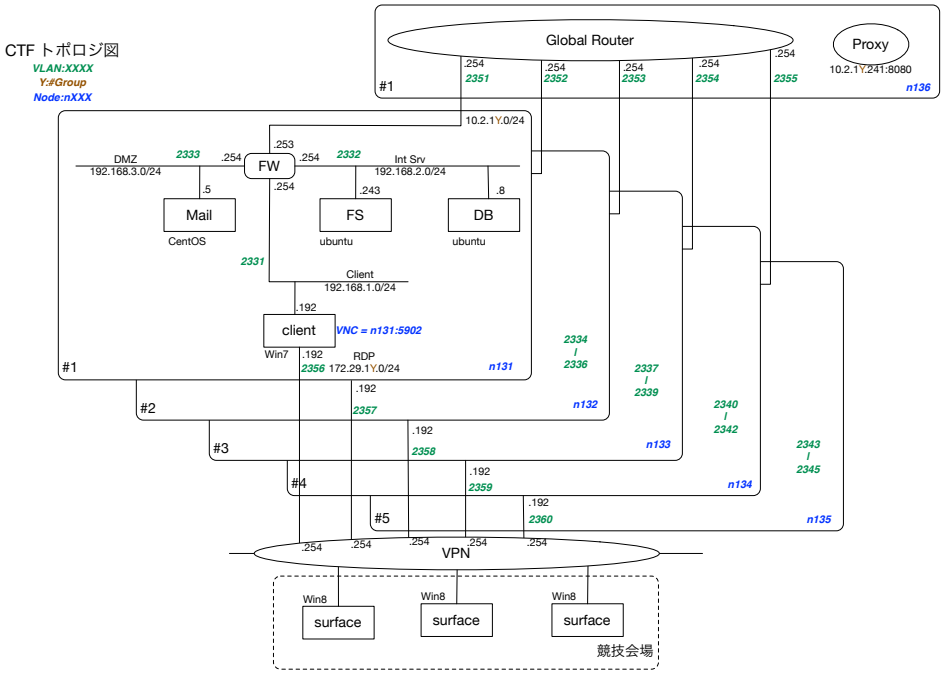
- 構築時間
  - 平均的なインスタンス１個の作成時間：約3分半

処理対象	処理段階	所要時間 [s]
ネットワーク	設定	66
ハイパーバイザ	ネットワーク転送	436
	設定	13
インスタンス	複製・ファイル挿入	146
	ネットワーク転送	62
合計		723

適用事例2

- CTF形式の競技体験
  - Windowsを一台乗っ取った想定で，NW環境上のどこかにあるDBの個人情報を奪取する.
  - 参加者にはトポロジ不開示も，最速達成者は25分

会場風景



今後の課題

- 攻撃パッケージ，演習シナリオなどの教材作成
  - 環境構築システムには目処

➢ StarBEDパッケージ
  - 一般的な組織ネットワーク環境とユーザ端末を模擬
  - 各種レベルの演習シナリオセット
  - 演習レベルにあわせた攻撃セット
  - StarBED環境を用いた大規模環境

➢ 可搬型パッケージ
  - セキュリティ演習パッケージを可搬型機材で実現
  - NW環境が準備出来ない会場でも演習可能
  - SDN技術を活用した安価な演習機材システム

EOF

May the 4th be with you!!