

サイバーレンジ構成学 + 知念研究紹介

知念

北陸先端科学技術大学院大学
セキュリティ・ネットワーク領域 サイバーレンジ構成学
Cyber Range Organization and Design,
Security and Networks Area,
Japan Advanced Institute of Science and Technology

サイバーレンジ構成学（NEC 寄付講座）

サイバーレンジ:

サイバー攻撃・防御の演習を行う場所のこと

⇒ 情報流出やセキュリティーホール調査

⇒ セキュリティー対策の教育

任務

1) サイバーレンジを構築する技術の研究開発

2) それを用いた教育プログラムの設計および開発

現状、サイバーレンジを直接扱う講義はない

サイバーレンジ構成学（NEC 寄付講座）(cont.)

研究分野

- OS やネットワークなどのシステム全般
- セキュリティと教育

開講

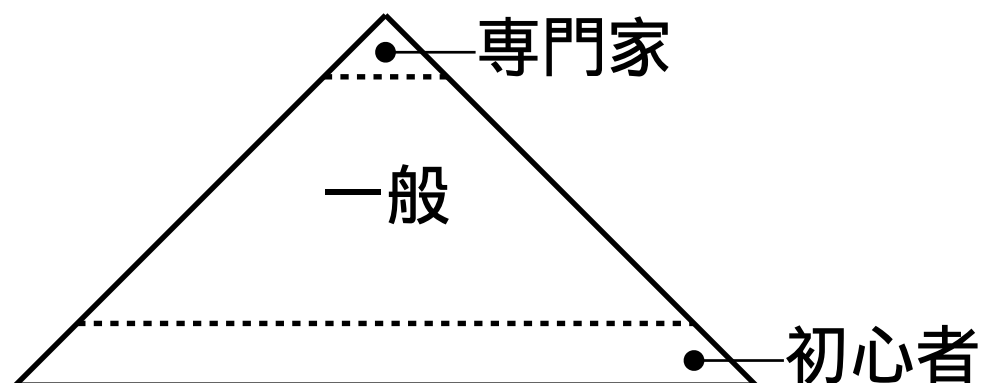
- 平成27年度、3年目

メンバー

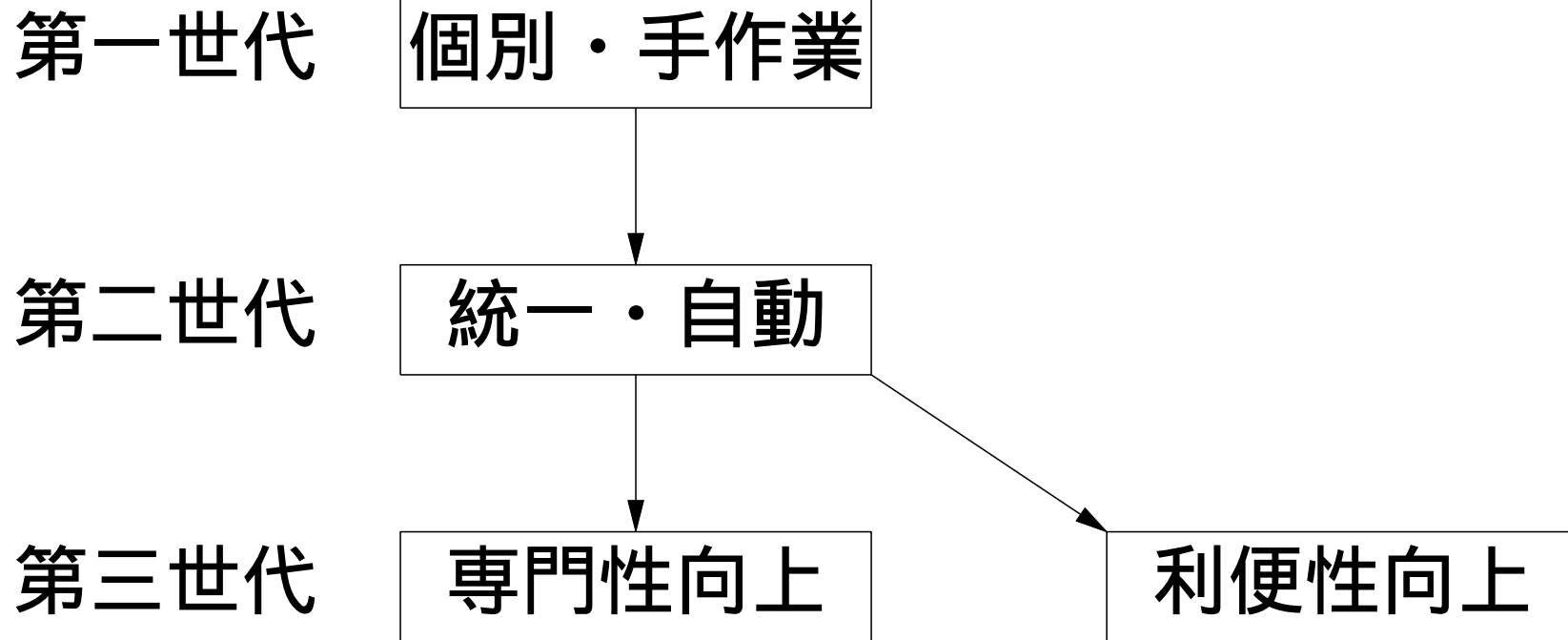
- 知念特任准教授 + 博士前期課程 4名
- ベウラン特任准教授 + 博士前期課程 4名

取り組んでいる研究テーマ

- サイバーレンジ構築技術の研究開発
 - ◇ 構成要素の速やかな配置・連携
 - ◇ 時間・順序の管理
- 学生・若者視点のセキュリティー教育、教材開発
 - ◇ H28年度から高専と共同研究

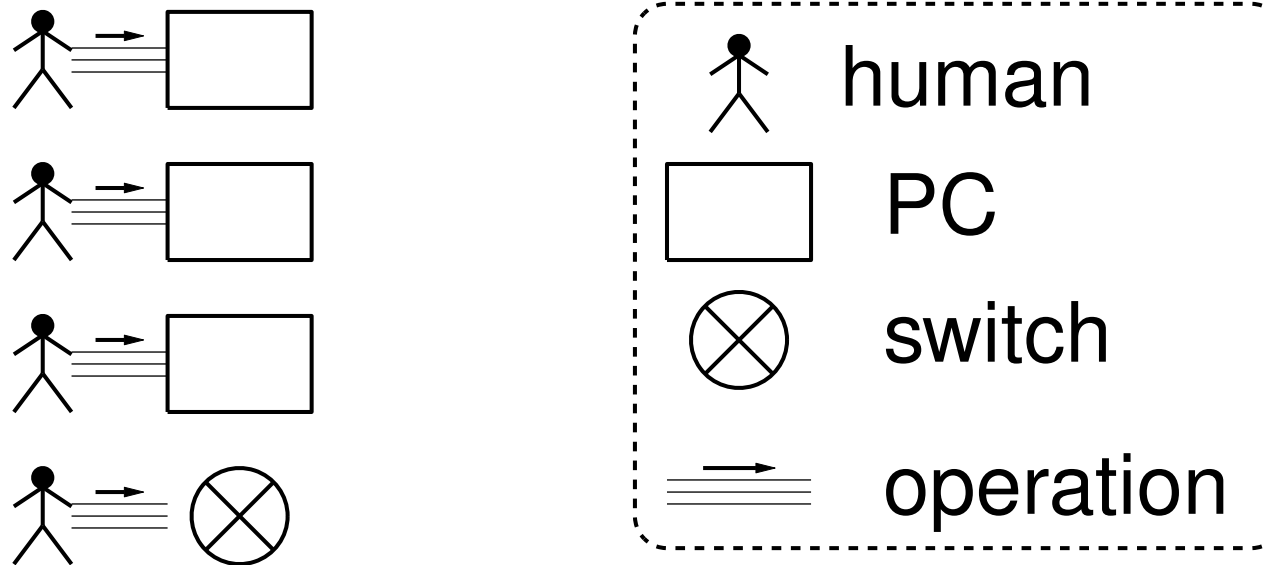


サイバーレンジ構築技術



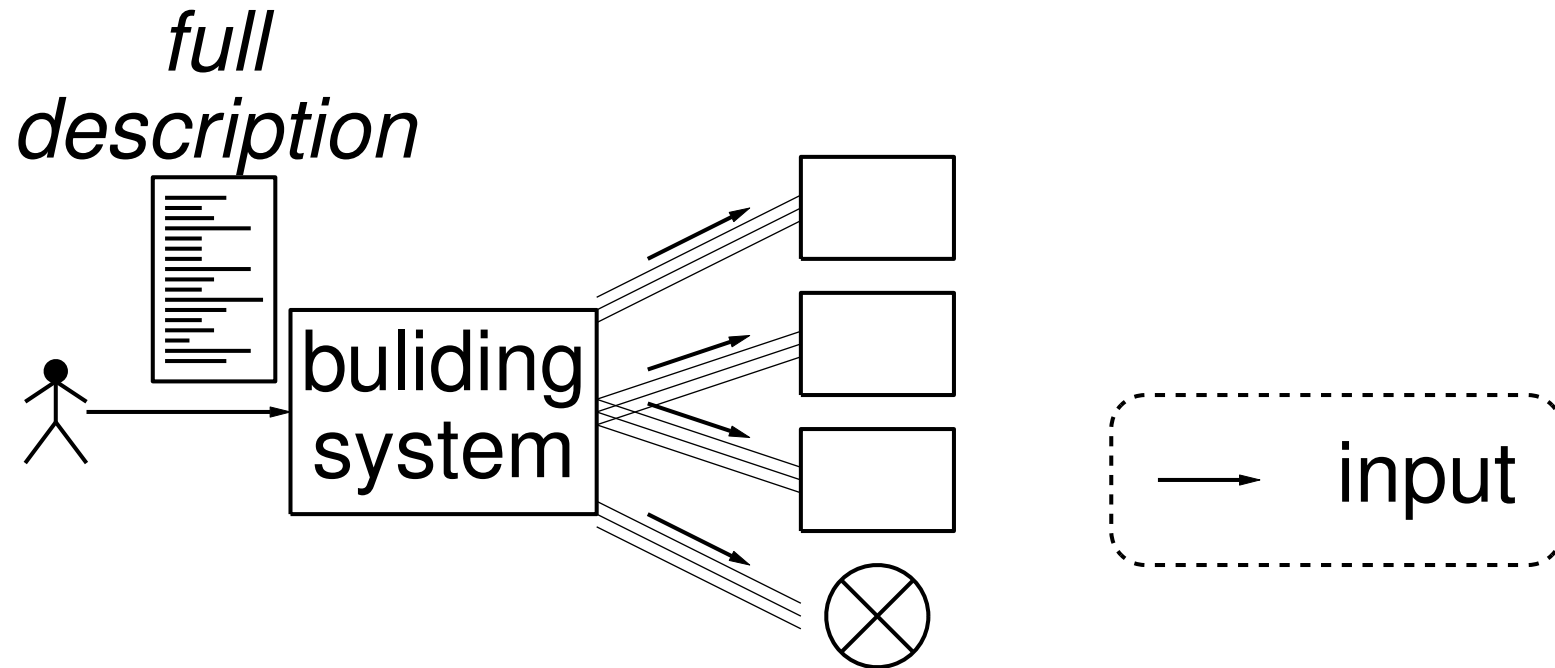
初期はクラスタ・クラウド構築システムとほぼ等価

第一世代：個別・手作業



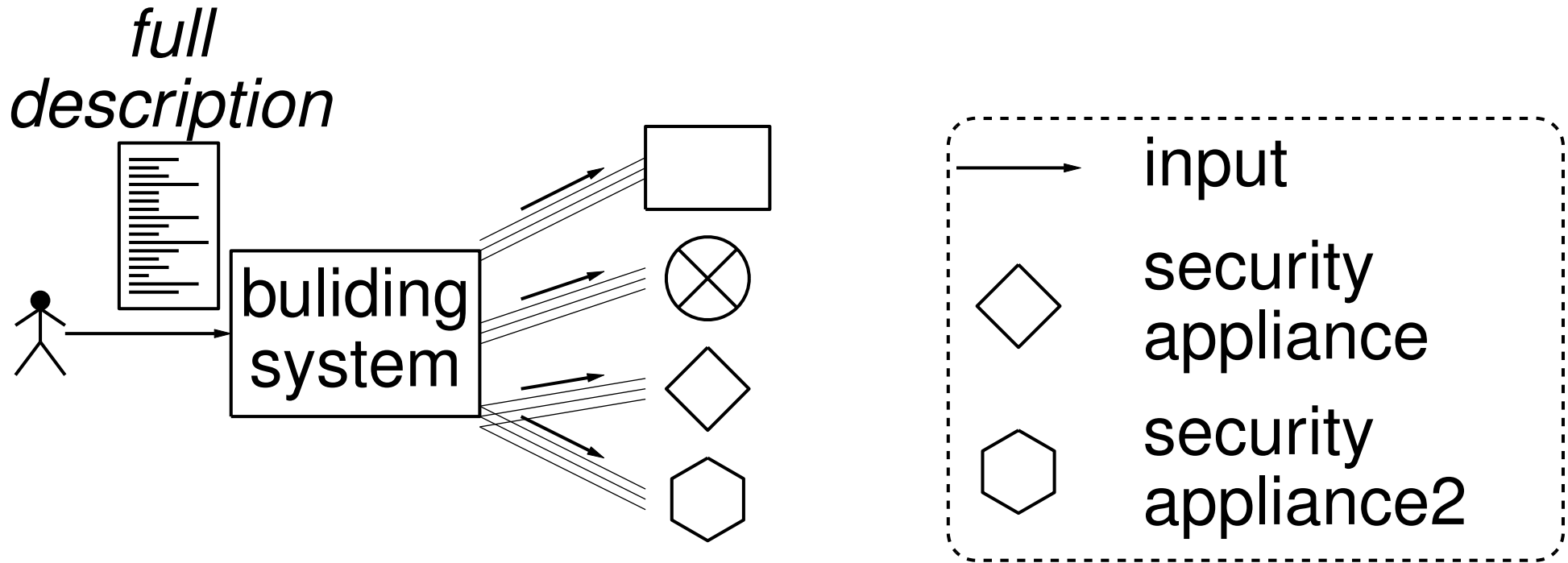
昔は全ての機材を個別に手作業
⇒ 煩雑、操作ミス誘発

第二世代：統一・自動



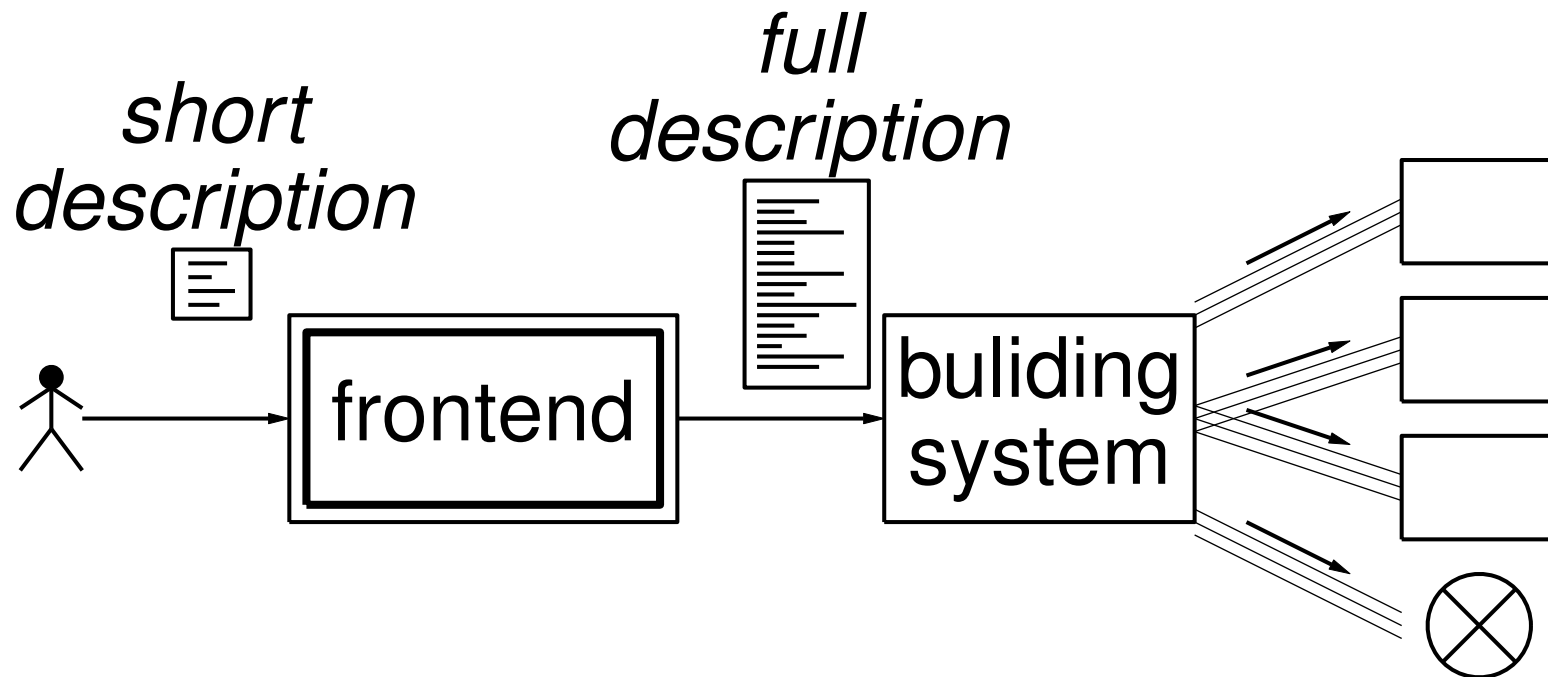
統一的な構築システムに全ての設定項目記述を与える
⇒ 手作業を削減、操作ミスも軽減

第三世代その1: 専門性向上



専門的な処理を施す、あるいは装置を操作する
⇒ フィッシング、マルウェア、ランサムウェアなど

第三世代その2: 利便性向上 — 高級化



要点を記述するだけで構築する

「良きに計らう」モジュールを設ける

⇒ 煩雑な記述が不要に、関心のある点だけ記述

第三世代その2: 利便性向上 — 高級化 (*cont.*)

「要点」の例

- マルウェア
- セキュリティーホール
- 事例

研究室の生活

- 関連（篠田、丹など）研究室と一緒にすすめる
- インターネットや UNIX の輪講
- 実際のネットワーク / サーバ機材を使った演習
- WIDE 等の研究コンソーシアムに参加

ただし書き

- ソフトウェア中心です
- 暗号は研究していません

知念 賢一 // Ken-ichi Chinen

1) ネットワーク実験

Network experiment; Network testbed

2) ネットワークサーバの開発・評価

Development and evaluation of network servers



研究分野1: ネットワーク実験

多くの産業と同様、ネットワーク産業も実験が必要

- 性能は？ ...自動車の燃費や最高速度測定
- 壊れ方は？ ...自動車の衝突実験

インターネットは広大 実験は大規模になりがち

- 機材の維持・管理は大変
- 機材を制御して実験を実施するのも大変
- 既存の枠組みでは制御できないことも

各種技術開発が必要

「規模」を考えてみよう

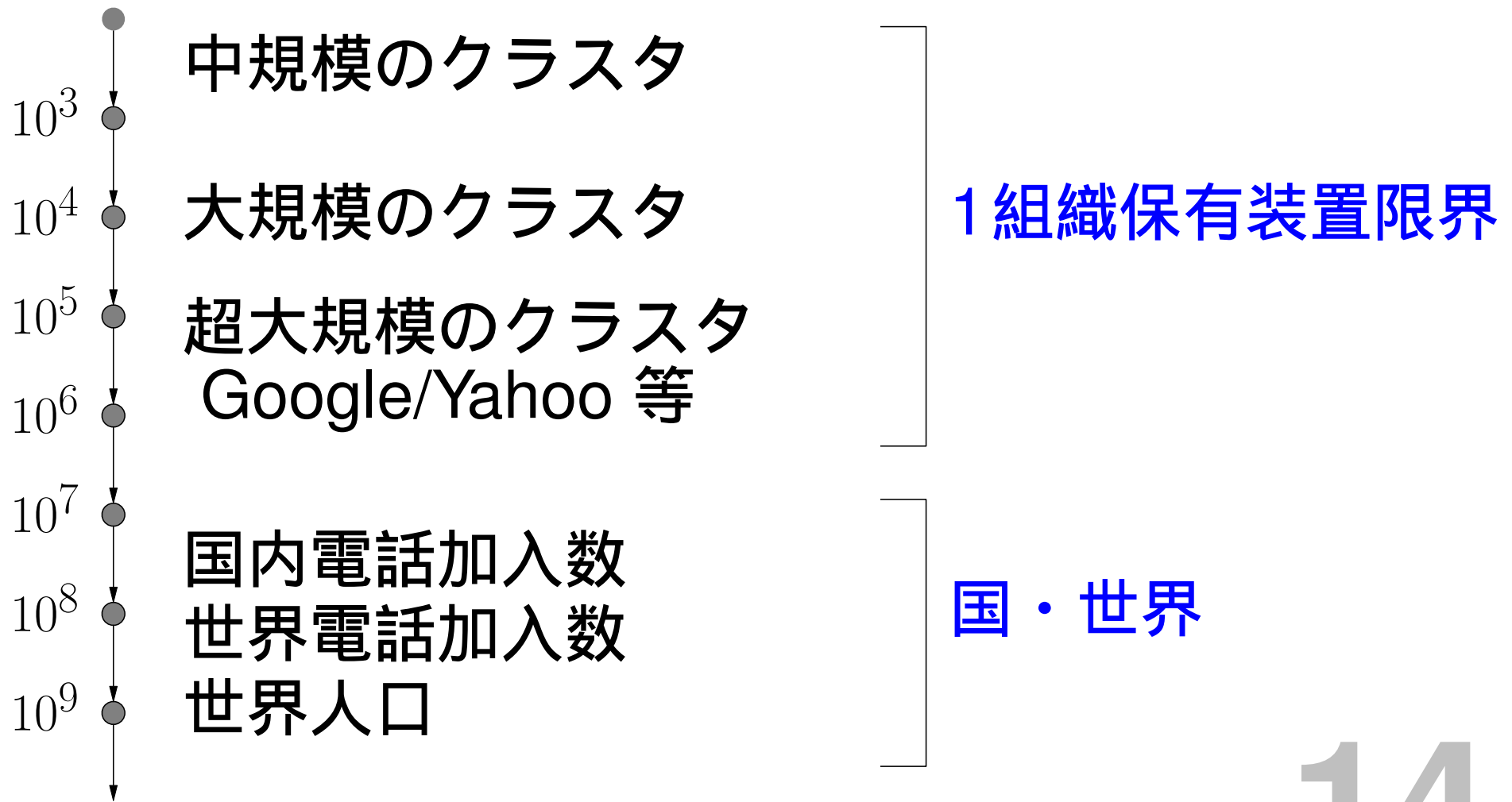
- 世界の人口は 70 億
- 国内携帯電話加入者数は 1.2 億 (2012 年 3 月)
- 国内固定電話加入者数は 4 千万 (2011 年)
- 32 ビットの IPv4 アドレスはほぼ枯渇
- WWW サーバ数 (Netcraft 調査)
6.7 億 (2013 May)
- Firefox のユーザは 3 億人

値の範囲

$10^7 - 10^9$

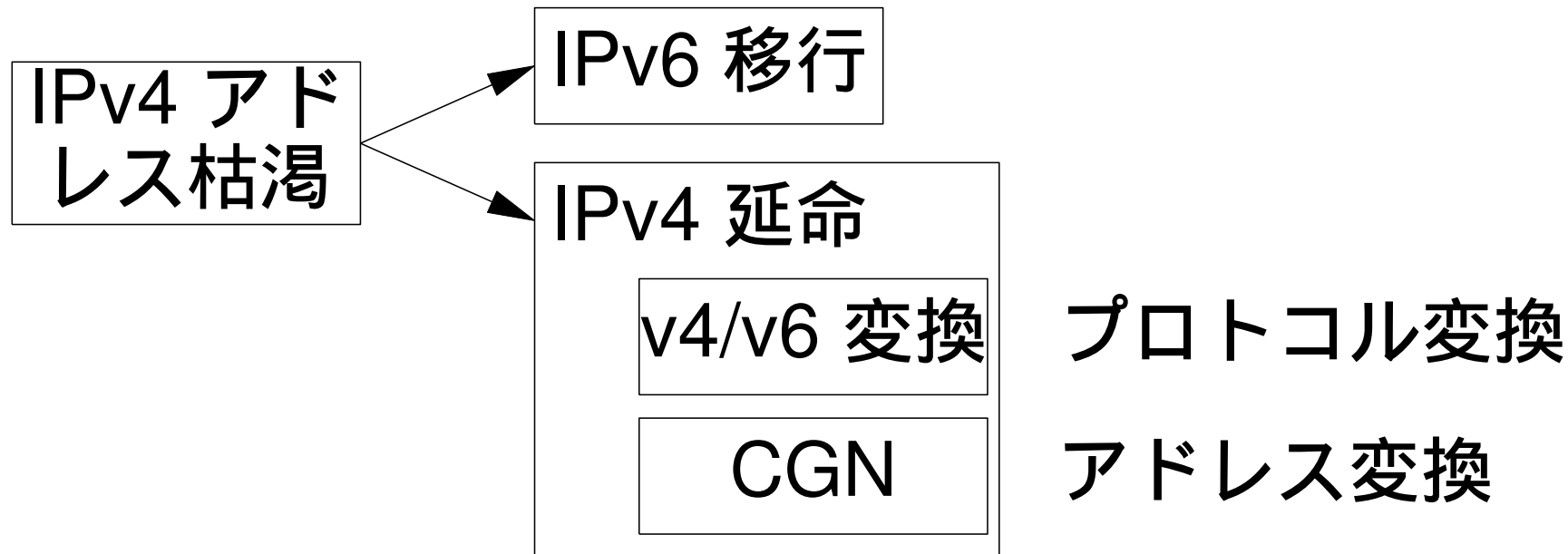
というような数字から考えると……

規模の隔たり



H25年度実験: CGN 負荷テスト

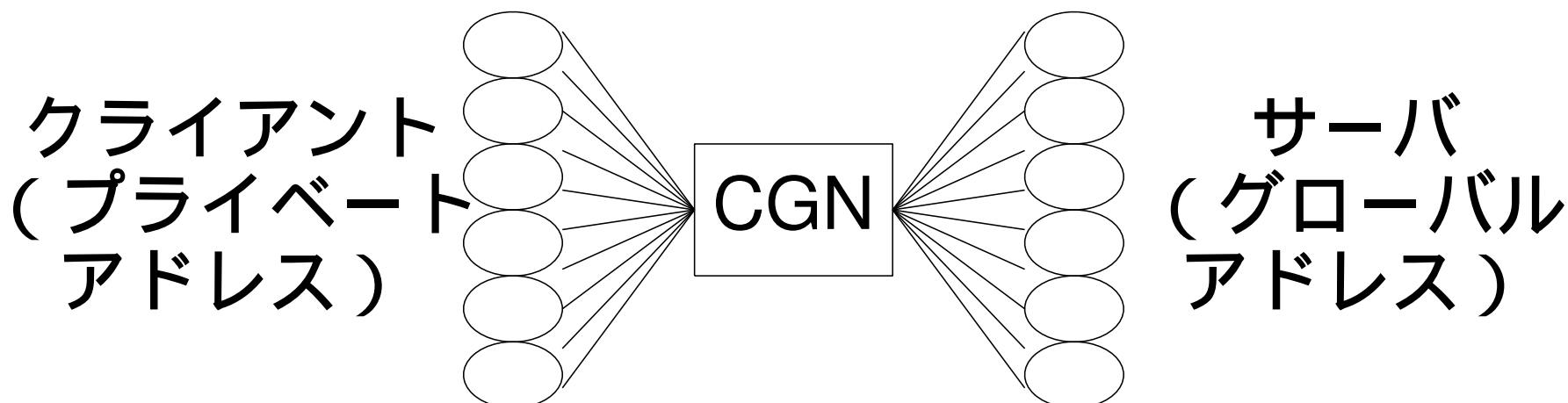
IPv4 アドレス枯渇に関する研究 — 延命策の一つ



NTTコミュニケーションズとの実験

Carrier-Grade NAT (a.k.a Large Scale NAT)

CGNが扱える同時接続数の実験
百万端末、一億接続向けの体制構築



使用した CGN が一億には至らず性能限界
ただし、数千万接続生成のノウハウは確立

H26年度実験: アップロードサーバ

- ビデオ向けクラウドの実現可能性検証
- コンテンツ中の重複を排除
 - ◇ 3.2万クライアント
 - ◇ クライアント毎、5秒間に10コンテンツ
 - ◇ コンテンツは 10MBのビデオ
 - ★ 重複排除なし 5.12Tbps
 - ★ 重複排除あり 300Mbps

1.7万分の1 に帯域改善

パナソニックとの共同研究

今後の実験（野望）

- 巨大規模実験の制御方法
 - ◇ 装置は数十万規模、将来は数億規模
 - ★ 仮想化技術を駆使
 - ◇ 通信数は数億規模、将来は数百億規模
- 複数施設にまたがった実験設備の構築方法
- 現実のプログラムを使ったトラヒック生成
 - ◇ FireFox 1000台など

得られるスキル

- ネットワークやコンピュータに関する知識
- システム全般に関する洞察力
- システム構築・管理・運用
- トラブルシューティング
- プログラミング



これまでの共同研究先

- パナソニック
- アラクサラ・ネットワーク
- NTT コミュニケーションズ
- ルネサス
- 情報通信研究機構
 - ◇ ネットワークテストベッド
 - ◇ セキュリティー

研究分野2: サーバ — 不可欠な存在

暮らしの中にコンピュータネットワークがとけ込む

- スマートフォン
- ネットワーク家電
- 音楽プレイヤー
- カメラ

ネットワークを使った通信販売が珍しくない
各種チケットもネットワークで手配

研究分野2: サーバ — 不可欠な存在 (*cont.*)

- クライアントの主流はスマートフォンに
 - それでもサーバは存在する
 - 「クラウド」もサーバの延長
- ⇒ サーバは現在社会を支えている

サーバの高度化・多機能化に取り組む

知念の研究分野

ネットワークサーバ

- サーバ単体の性能向上
- 複数サーバや支援装置による性能向上

派生して、ネットワーク実験

- ◇ 性能指標の考案、性能計測ツールの開発
- ◇ 実験設備の整備、実験支援ツールの開発

様々な技術やシステムを実際に計測する

サーバ単体性能

- I/O（入出力）性能
 - ◇ ネットワーク
 - ◇ ファイルシステム
- コンテキスト性能
 - ◇ プロセス
 - ◇ スレッド

その他、OS 近くの様々な性能向上を図る

研究はシステムプログラミング中心

複合サーバ性能

- 分散偏り平滑化
- 動的な台数増加・削減
 - ◇ リクエスト予測
 - ◇ コンテンツ同期
 - ◇ 負荷分散装置制御



研究はサーバ群構築や計測が中心

【最近の研究テーマ】

サーバ自体

- ビデオストリーム向けアップロードサーバ
 - ◇ 数Mbps × 数百本
 - ◇ メタ情報で重複省く
 - ◇ 映像内容で重複省く

【最近の研究テーマ】 (cont.)

実験技術

- 100万回線相当トラフィック生成 // CGNの実験
 - ◇ 1億 HTTP コネクション生成
対象装置の性能足りず実績 2600万
- 一定コネクション確立レート生成
 - ◇ 毎秒 25万コネクション
- 実験記述言語処理系開発
 - ◇ StarBED 型テストベッド向けスクリプト言語
 - ◇ 数百台規模の PC を制御

【最近の研究テーマ】 (cont.)

その他

- 計算ジョブディスパッチシステム
 - ◇ 汎用 PC 向け
 - ◇ 100万件以上のジョブを数百台 PC に分配
- トラフィック観測システム
 - ◇ セキュリティ的視点
 - ◇ 稀な通信を検出

学外設備: StarBED (共同研究組織)

情報通信研究機構 北陸 StarBED 技術センター

- JAIST のアイディアに基づいて設立
- JAIST 近く、徒歩 8分
- 1000 台以上の PC、多数のスイッチ

