サイバーレンジ構成学
サイバーレンジ紹介、活動報告

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

CROND: Cyber Range Organization aNd Design
サイバーレンジ構成学講座

- 2015年設置（NEC寄付講座）
- 設置目的
  サイバーレンジ構築技術、及びそれを用いた教育カリキュラムなどの研究
  - ◇ 研究開発中心（講義・授業の名称ではない）
- 人員（2018年4月1日現在）
  - ◇ 専任教員 2名＋担当教員 2名
  - ◇ 学生 9名（修士課程 8、博士課程 1）

サイバーレンジとは

- 「サイバー」はコンピュータネットワーク
  電脳と呼ぶ場合も…
- 「レンジ」は演習場

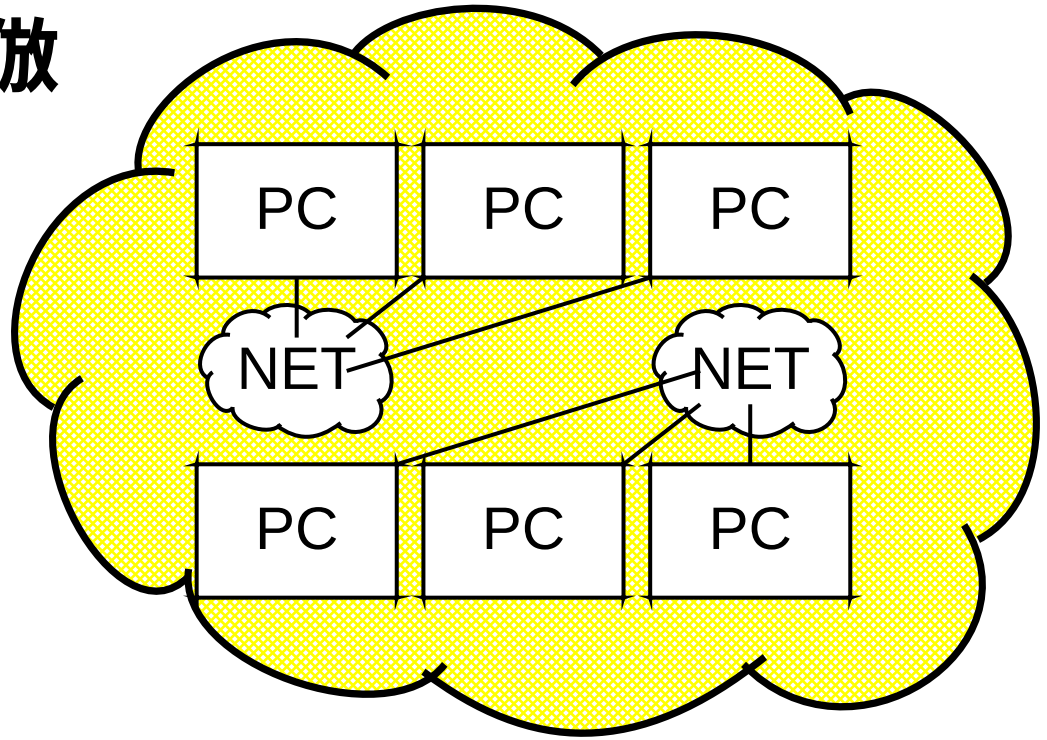
つまり、
コンピュータネットワーク上の演習場を
「サイバーレンジ」と呼ぶ。

セキュリティ分野の文脈で登場する例が多い

サイバーレンジとは *(cont.)*

- （現実とは分離した場所に…）
- 攻撃対象のコンピュータやネットワークを構築
  - ◇ 実物あるいは模倣物を設置
- 攻撃を実施あるいは模倣
- （被害が現れる）
- 解析や対策を実施

※ 仮想化技術の発展で模倣が容易に



サイバーレンジがあれば...

一般利用者・会社など組織:

- 直接被害を受けずに体験
- セキュリティ対策演習＜災害演習のように＞
- システム診断

研究者・開発者:

- 悪意あるプログラムの調査
- 対抗技術の研究開発

□想定される被害

- 個人情報流出
- 設備・装置・サービスの破壊・妨害
- 金融機関からの不正引出
- ネットワークを介した手術の事故
- 自動運転車の事故
- 交通網の麻痺
- 工場・発電所の麻痺

このような事象の研究や対策練習の場が必要

□サイバーレンジの必要性 — 脅威例

- インターネット接続後、短時間でウィルスに感染
  （2004年、20分）
  https://gcn.com/articles/2004/08/17/unprotected-pcs-can-expect-infection-in-minutes.aspx

  （2008年、4分）
  https://isc.sans.edu/diary/Survival+Time+on+the+Internet/4721
- 対策は進化しているが、ウィルス側も進化
- 対策の強化が必要 — 体制（人材）や技術

サイバーレンジ分類 — 代表的視点

演習スタイル（攻防）：

技術度:

演習対象組織:

典型的サイバーレンジ用途

- CTF (Capture The Flag) — **旗取り合戦**

  クイズ形式:

  - **隠された情報（Flag）を集める**
  - **集めた情報の数や正確さを競う**

  攻防形式:

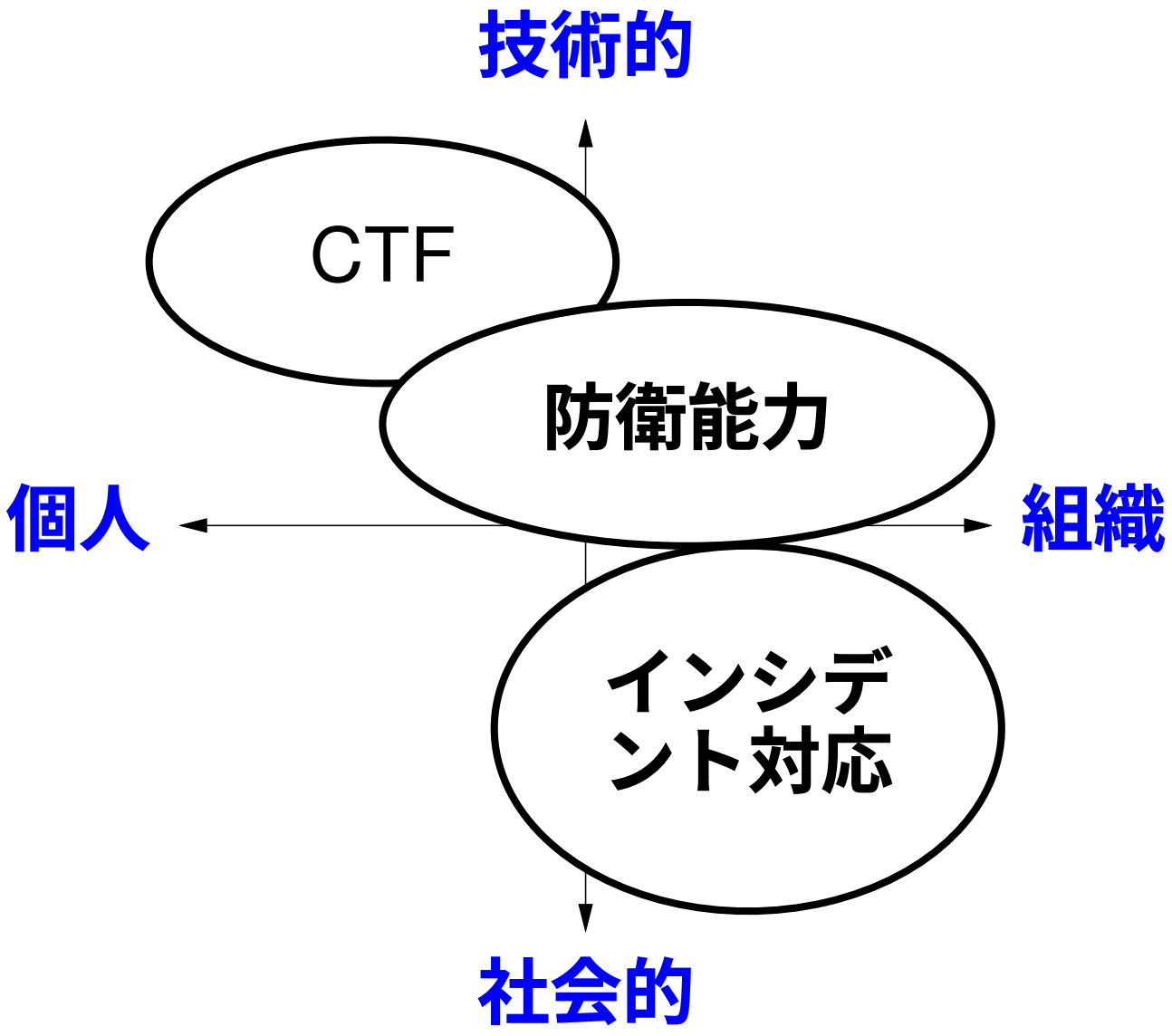
  - **相手の情報を奪う**
  - **相手へ情報を書き込む**
  - **拠点の制圧や占有率を競う**

典型的サイバーレンジ用途 *(cont.)*

- 耐久テスト
  - 攻撃に耐えられるか
  - ウィルス耐久時間や感染速度を計測
- 防衛能力テスト
  - 攻撃を受けつつ運用
  - システム・運用者の運用能力を評価
  - 停止時間（ダウンタイム）も重要

典型的サイバーレンジ用途 *(cont.)*

- 組織的サイバーインシデント対応演習
  - インシデント発見
  - 専門家への相談
  - 当局へ報告
  - 顧客や株主への対応
  - 営業判断: プレスリリース、サービス停止


技術的
CTF
防衛能力
個人
組織
インシデント対応
社会的

□サイバーレンジ — 問われる能力

- コンピュータの知識・技術
- ネットワークの知識・技術
- それ以外の機材の知識・技術
- 攻撃の知識・技術
- 防御の知識・技術
- 組織内の情報共有・意思決定
- 組織間の情報共有

□サイバーレンジの意義 — 人材育成

大別して 3つ

a) **一般教養としてのセキュリティー啓蒙**

b) **セキュリティーを配慮する研究開発人材の育成**

c) **セキュリティー専門人材の育成**

セキュリティー人材（上記ｃ）の調査
（IPA、2012年4月）

`https://www.ipa.go.jp/security/fy23/reports/jinzai/`

2.2万人不足、供給量も不足

□人材育成加速

- セキュリティー事件（インシデント）増加
- 人材不足、供給不足

⇓

育成手段の加速が必要

- 大規模化
- 育成内容の多様化

⇓

育成にはサイバーレンジが有効

- 大規模かつ多様な内容が扱えるとなお良い

□サイバーレンジを使った教育

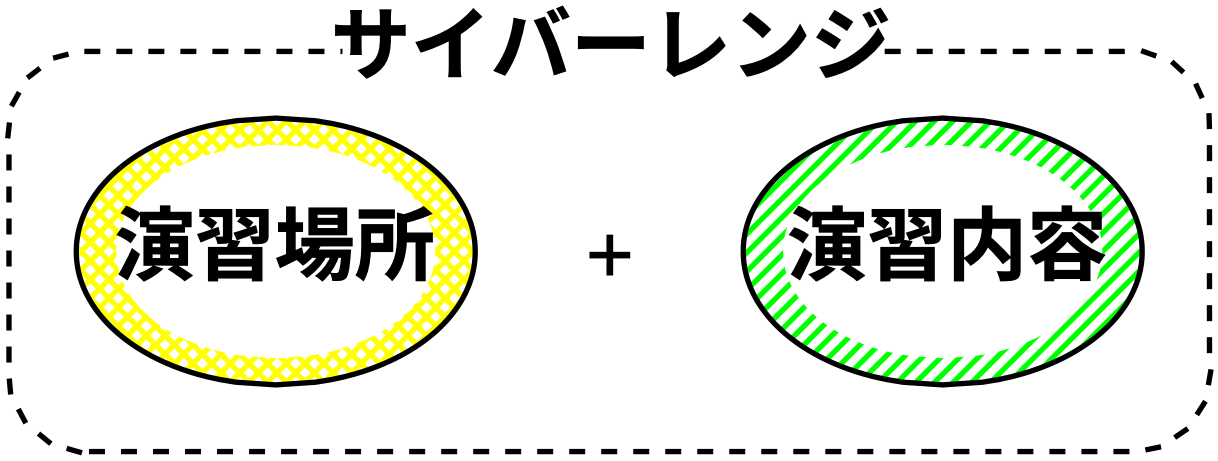
- 通常業務から切り離して実施可能
- 繰り返し実施可能
- 多種の内容（過去の遭遇以外）に対応可能
  - ◇ 体系的/網羅性も向上
- （自動化されれば）大人数に実施可能
- （自動化されれば）構築も容易

⇓

自動化こそ、有効性の鍵

（我々の考える）サイバーレンジ

設備（場所）だけでなく内容もセットで考える



演習場所: PC、ネットワーク機器

演習内容: 防衛・攻撃訓練、試験・解析

どちらも自由に切り替えられるべき

□CROND — ニュース紹介例

「優れものだが高価、
サイバー攻撃の疑似体験システムが無償に」

（日経BP社 ITpro 2017年10月10日）

http://itpro.nikkeibp.co.jp/atcl/
column/14/346926/100301150/?rt=nocnt

セキュリティ人材不足の方策の一例として、
サイバーレンジ無償化の点で紹介された

具体的な活動

- **サイバーレンジに関するシステム開発**
  - ◇ CyTrONE, CyRIS **など**
- **演習内容の調査・開発**
- **開発物の普及**
- **各種セキュリティイベントへの協力**

学生の活動

修士研究テーマ

- セキュリティ、あるいはセキュリティ教育
- OS やネットワーク技術

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
  - 例年、篠田研究室と輪講やセミナー
- 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

周りの活動

共同研究

- ネットワーク関連
  - アラクサラ、NTTコミュニケーション
  - 情報通信研究機構
- セキュリティ
  - NEC、アライドテレシスアカデミー
  - 東京都立産業技術高等専門学校（都立高専）
  - 国立高専機構
  - Hardening Project、その他イベント

過去の研究

- CGN（Carrier Grade NAT）性能評価
- 全録レコーダのクラウド化検討実験
- ネットワーク実験支援 . . . . . SpringOS
  - ◇ 各種支援サーバ群
  - ◇ 実験記述言語、自動実行 . . . . . Kuroyuri

- WWW サーバ、プロキシサーバ開発
- 大規模 WWW サーバサイト構築