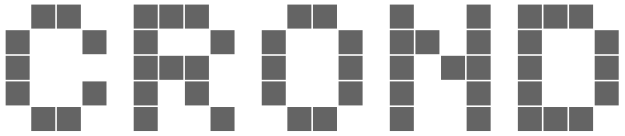
JAIST 型サイバーレンジ構成法
— JAIST CROND 活動紹介 —

知念 賢一

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 サイーバレンジ構成学
Cyber Range Organization and Design,
Security and Networks Area,
Japan Advanced Institute of Science and Technology

アウトライン

- 話者
- JAIST、CROND
- サイバーレンジ
  - ◇ 必要性
  - ◇ 構成法
  - ◇ 人材育成
- CROND の演習システム実装例、CyTrONE など
- 今後の活動



話　者 知念　賢一

所　属	北陸先端科学技術大学院大学 セキュリティー・ネットワーク領域 サイバーレンジ構成学
専　門	'90 サーバプログラム ＜開発・性能評価＞ 大規模WWWサーバ、プロキシサーバ '00 ネットワーク実験 StarBED Project 開発担当 '10 サイバーレンジ

JAIST: Japan Advanced Institute of Science and Technology
北陸先端科学技術大学院大学

- 1990年開学、大学院（修士・博士課程）のみ
- 人員（2017年5月1日現在）
  - ◇ 教職員: 292名
  - ◇ 学生: 1076名（うち留学生 513名、47%）
- 所在地
  - ◇ 石川県能美市旭台
    （金沢と小松の中間、手取川南岸の山側）

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（2017年11月1日現在）
  - ◇ 専任教員 2名＋担当教員 2名
  - ◇ 学生 12名（修士課程 12、博士課程 0）

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

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

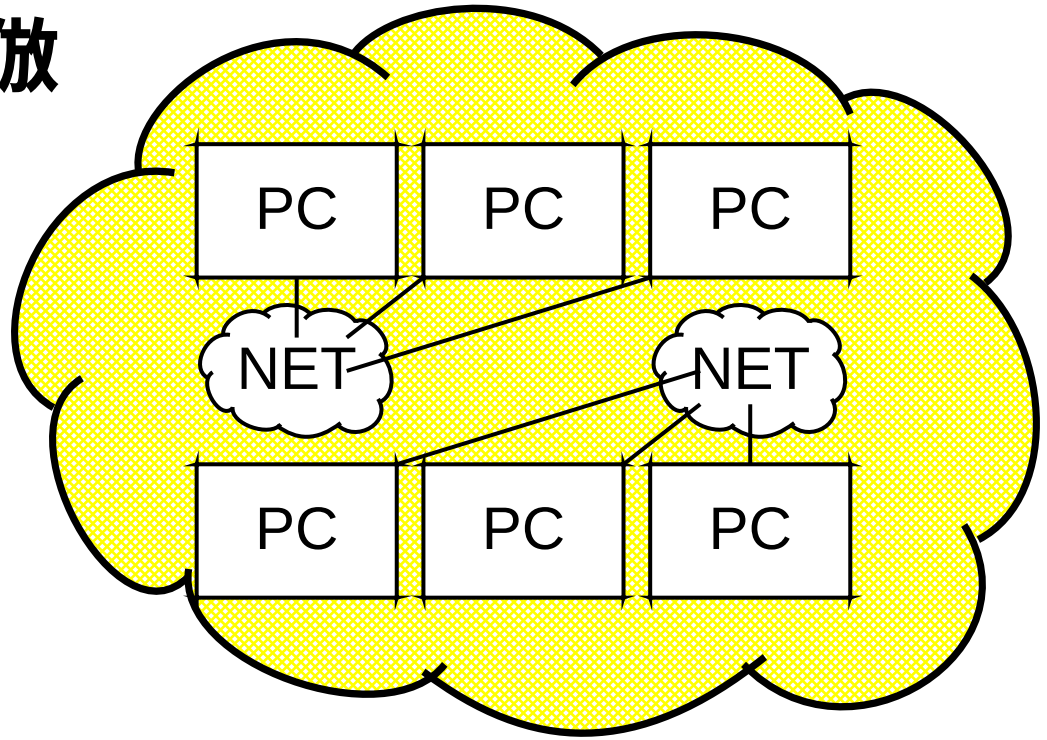
つまり、
コンピュータネットワーク上の演習場を
「サイバーレンジ」と呼ぶ。

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:

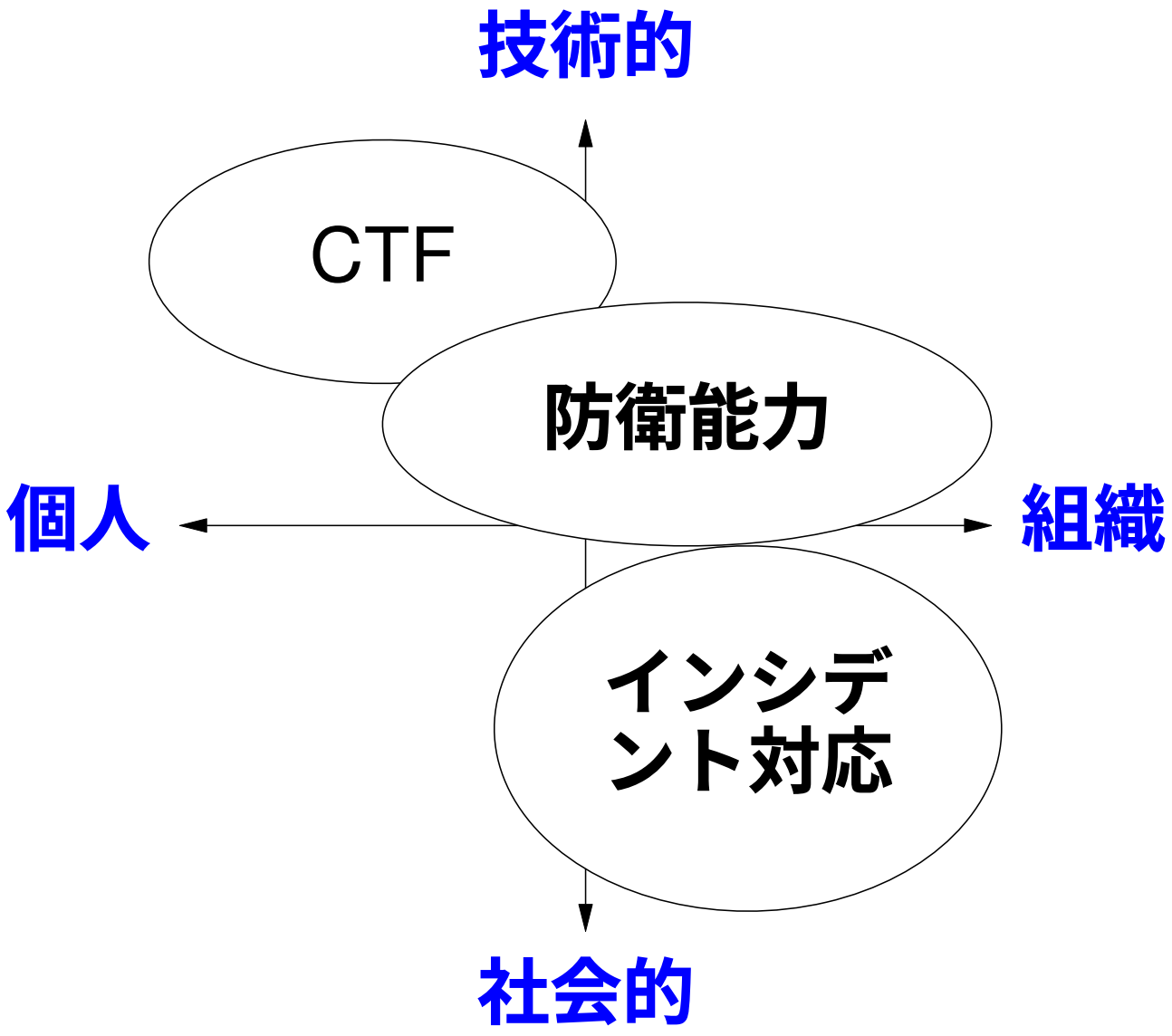
  - **相手の情報を奪う**
  - **相手へ情報を書き込む**
  - **拠点の制圧や占有率を競う**

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

対比: 従来教育

- 比較的少数のセキュリティ技術者間の共有
  - ◇ 養成される側も少数
  - ◇ 徒弟制に似た状況
  - ◇ 体系的/網羅性乏しい
- 遭遇経験ベースの知識獲得
  - ◇ 広い知識の獲得困難
  - ◇ 再現性低い
  - ◇ 比較的小規模中心
    - ⋆ 構築に時間的・経済的コストがかかる

対比: 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

従来・典型的サイバーレンジ

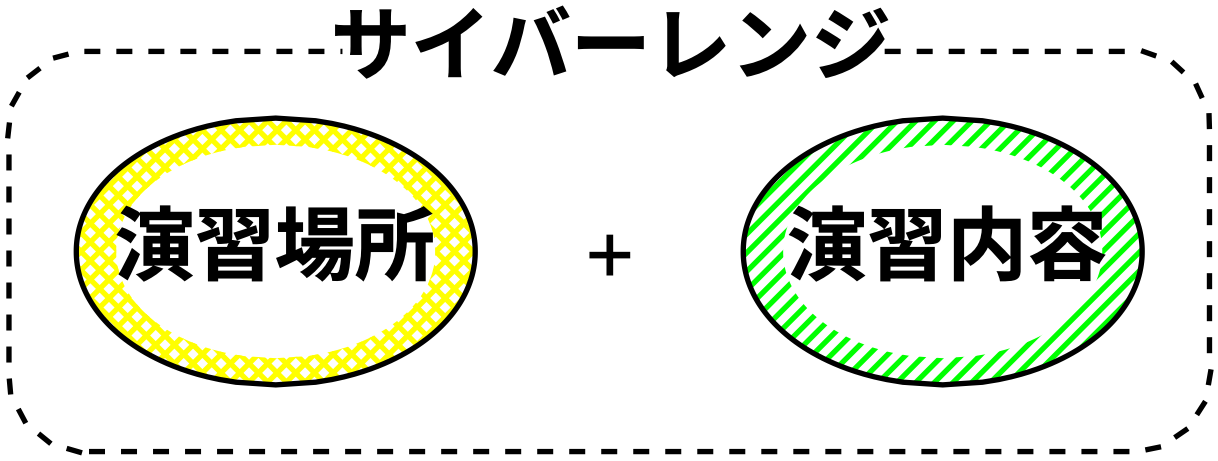
a) サイバーレンジの設備を販売
- 軍事・防衛由来が多い
- 数千万から数億円
- 内容固定
  - ◇ カスタムすると別料金

b) 設備を使ったセミナー
- 数日、数十万円/人

「プロ中のプロ」の養成はともかく、
大多数への適用は困難、一般人の啓蒙には程遠い

（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

JAIST型サイバーレンジ方針

- 汎用 . . . . . 演習内容記述方式
  - ◇ 記述を切り替えることで多用途に
  - ◇ 講師が独自に内容を記述可能に
- 自動化 . . . . . 容易かつ高速に
  - ◇ 構築・撤去を繰り返し、回転を早める
  - ◇ 複数内容切り替え
- オープンソフト
  - ◇ ハードウェアは別途必要
    - ⋆ 汎用ハードウェアを中心に

JAIST型とそれ以外の対比

	JAIST型	従来・典型的
用　途	汎　用 講師変更可能 複数内容、切替可能	固　定（製造者作成） または別用途を別料金で
費　用	オープンソフト ハードウェア別途必要	多くが有料

演習システムの開発

主な機能

- 場所構築、内容切替を自動化

用途・スタイル

- CTF のクイズ形式

構成要素

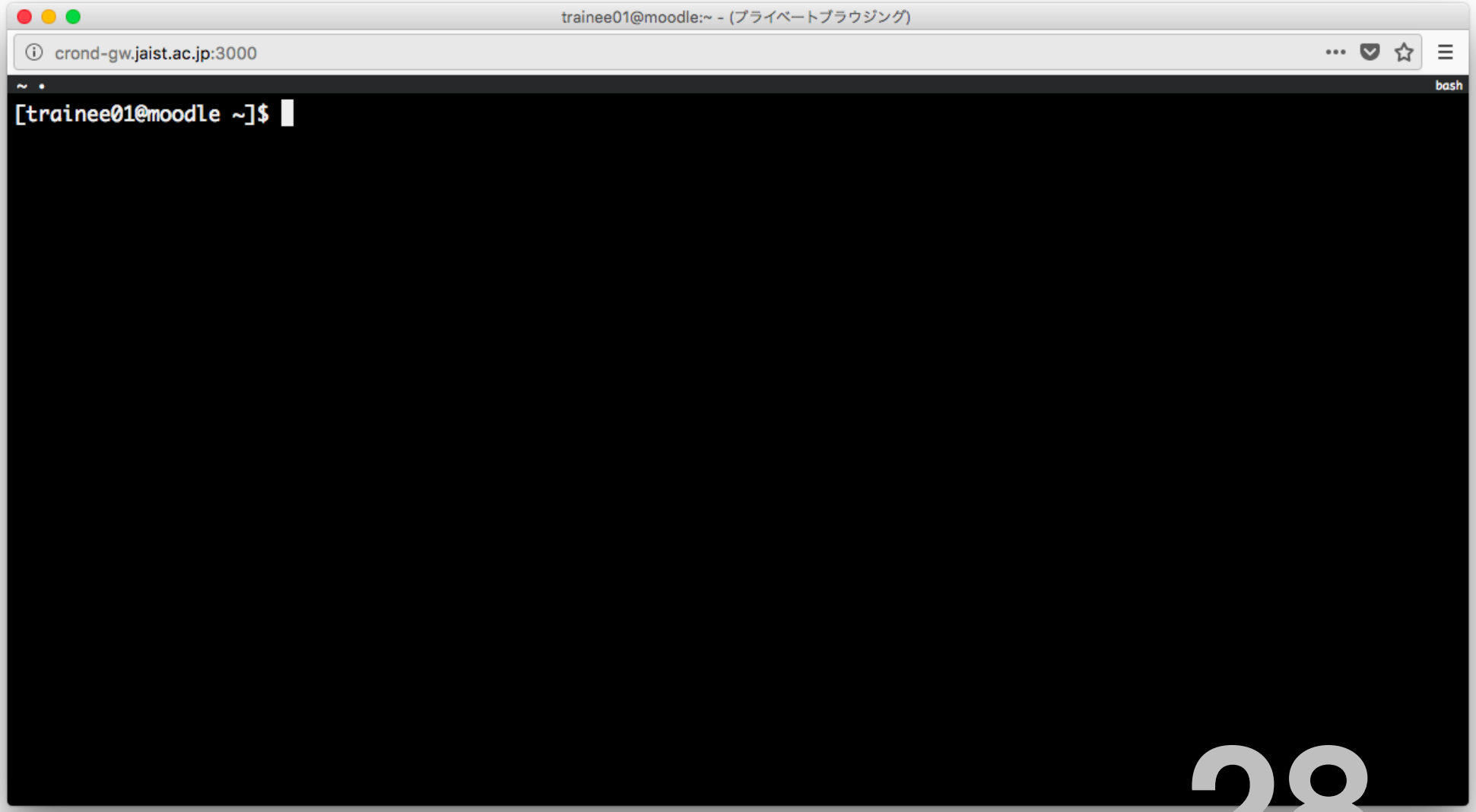
- 演習進行・内容管理
  - クイズ出題・回答の機構
- 演習場所構築
  - 情報が隠されたコンピュータとネットワーク

参加者 UI (LMS; Moodle) — カバー

参加者 UI — 設問


Navigation
Administration
CyTrONE Security Training
Dashboard ▶ CyTrONE ▶ Information Security Testing and Assessment ▶ Sample: レベル 1 （イージー）
Exit activity
Sample: レベル 1 （イージー）
Information Security Testing and Assessment
Questions Level 1
<
Click below button to connect to CyTrONE, investigate and answer the questions in textbox of each question. Good luck !
OPEN TERMINAL
Question 1
オペレーティングシステムとカーネルリリース番号はコンピュータにどの脆弱性の可能性があるか伝えることができます。マシンのカーネルリリース番号を探してください。（例： 3.4.56-789）
Click to show hint
Question 2
あなたのコンピュータが接続しているネットワークを理解するために、そのパソコンの詳細を知る必要があります。1つめのネットワークインターフェースに設定されたIPv4アドレスを探してください。

参加者 UI — サイバーレンジ操作



参加者 UI — ヒント

Question 1

オペレーティングシステムとカーネルリリース番号はコンピュータにどの脆弱性の可能性があるか伝えることができます。マ
ンのカーネルリリース番号を探してください。（例： 3.4.56-789）

Click to show hint

Hint 1: あなたは<code>uname</code>コマンドを使ってOSの詳細を

Hint 2: $ uname -r

Hint 3: 別の方法として，$ cat /proc/version ファイルから必要な情報を探

Question 2

あなたのコンピュータが接続しているネットワークを理解するために、そのパソコンの詳細を知る必要があります。1つめの
ネットワークインターフェースに設定されたIPv4アドレスを探してください。

演習進行・内容管理

- 内容説明・設問の提示、回答の受付
- LMS (Learning Management System) を採用
  - 遠隔教育で広く使われている
  - 今回は Moodle を採用
  - 他への互換性のためデータ形式は SCORM
- 設問と正解は自由に書き換え可能

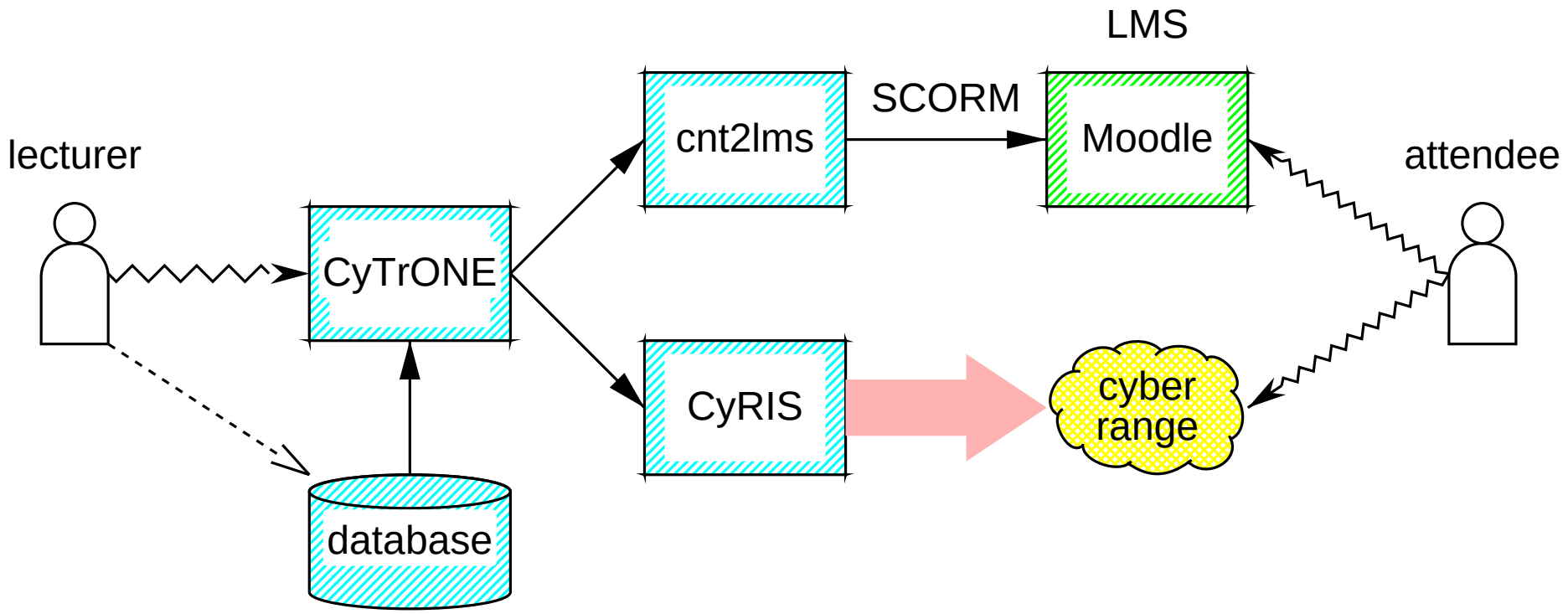
演習場所の構築

場所を状況を記述する形式を策定
PCやネットワーク、それらの部品を表現可能に

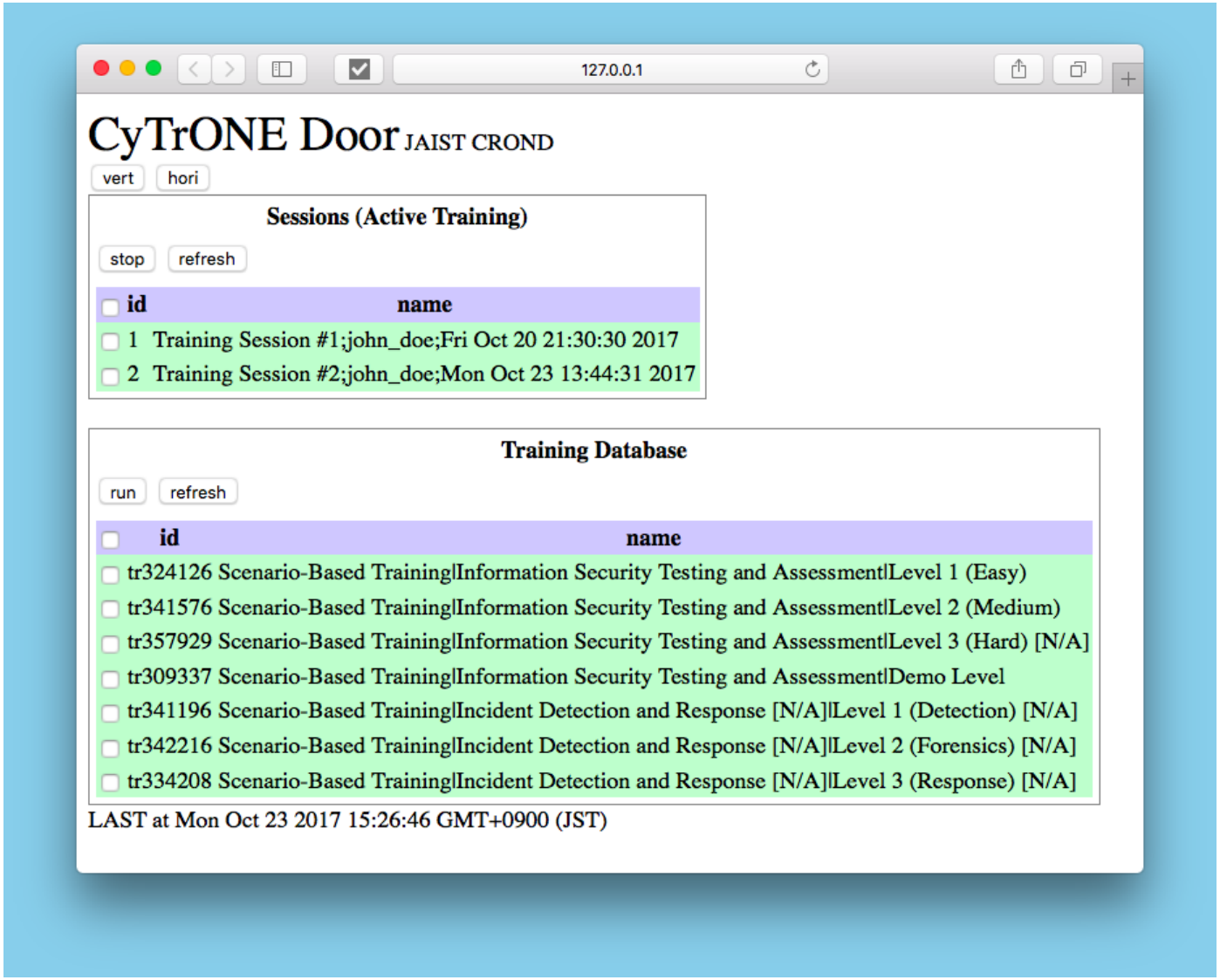
記述に応じて...

- PC **設置**
  - ◇ **仮想化技術（仮想マシン）で対応**
  - ◇ PC **に** OS**、アプリをインストール**
  - ◇ **セキュリティ的痕跡作成**
- **ネットワーク構築**
  仮想化技術（仮想マシン）で対応

演習システム構成


LMS
SCORM
cnt2lms
Moodle
lecturer
attendee
CyTrONE
CyRIS
cyber
range
database

講師向け制御UI


127.0.0.1
CyTrONE Door JAIST CROND
vert
hori
Sessions (Active Training)
stop
refresh
id
name
1 Training Session #1;john_doe;Fri Oct 20 21:30:30 2017
2 Training Session #2;john_doe;Mon Oct 23 13:44:31 2017
Training Database
run
refresh
id
name
tr324126 Scenario-Based Training|Information Security Testing and Assessment|Level 1 (Easy)
tr341576 Scenario-Based Training|Information Security Testing and Assessment|Level 2 (Medium)
tr357929 Scenario-Based Training|Information Security Testing and Assessment|Level 3 (Hard) [N/A]
tr309337 Scenario-Based Training|Information Security Testing and Assessment|Demo Level
tr341196 Scenario-Based Training|Incident Detection and Response [N/A]|Level 1 (Detection) [N/A]
tr342216 Scenario-Based Training|Incident Detection and Response [N/A]|Level 2 (Forensics) [N/A]
tr334208 Scenario-Based Training|Incident Detection and Response [N/A]|Level 3 (Response) [N/A]
LAST at Mon Oct 23 2017 15:26:46 GMT+0900 (JST)

参考性能

- NICT StarBED で規模性実験
  - ◇ 物理ホスト 30 台
    - ⋆ CPU (dual) Xeon X5670 2.93GHz 6core
    - ⋆ メモリ 128GB
  - ◇ 簡単な例、20 仮想マシン/物理ホスト
    - ⋆ KVM で仮想化
    - ⋆ 合計 PC 600 台相当
    - ⋆ 構築時間、約 14分（847.6秒）

※ まだまだ事例が少ない

将来展望

- 演習内容充実
  - ◇ CROND 自ら制作（できることは限られる）
  - ◇ 演習事例から変換
  - ◇ 協力者から収集
- 普及活動
- サイバーレンジ記述標準化、コンソーシアム設立
- 演習内容の交換が普及（草の根）
- 演習内容市場の醸成（ビジネス）

将来展望 *(cont.)*

- 開発項目
  - ◇ 不正回答防止、回答複数化・問題シャッフル
  - ◇ 攻撃模倣
- 様々な事例で性能計測
- 「CTFクイズ形式」以外の用途も実現

将来展望（野望）

- マルチプラットホーム化
  - Raspberry Pi など
- 物理ホスト、物理スイッチ制御
- 類似システムからの変換機構
- 資料解析による自動生成
  - インシデント報告から生成できれば...

公開場所

ソース公開場所:

https://github.com/crond-jaist/

連絡先:

crond-sec@jaist.ac.jp

まとめ

我々 CROND は...

- **JAIST の研究部署**
- **サイバーレンジ構成に取り組んでいる**
  - **モデル、構成法**
- **具体的な演習システムを開発している**
- **開発物は GitHub で公開している**
- **セキュリティ教育に貢献していきたい**

最後に...

以下のようなご協力を求めています

- 演習システムを使っていただける方
- 演習内容を考えていただける方
- 一緒にシステムを開発していただける方

興味がある方はお知らせください

□対 外 発 表

[1] D. Tang, C. Pham, K. Chinen, R. Beuran, ”Interactive Cyber Attack Emulation for Facilitating Security Training”, poster, Internet Conference (IC 2016), Tokyo, Japan, October 11-12, 2016.

[2] C. Pham, D. Tang, K. Chinen, R. Beuran, ”CyRIS: A Cyber Range Instantiation System for Facilitating Security Training”, International Symposium on Information and Communication Technology (SoICT 2016), Ho Chi Minh, Vietnam, December 8-9, 2016.

[3] R. Beuran, C. Pham, D. Tang, K. Chinen, Y. Tan, Y. Shinoda, ”CyTrONE: An Integrated Cybersecurity Training Framework”, International Conference on Information Systems Security and Privacy (ICISSP 2017), Porto, Portugal, February 19-21, 2017.

□対 外 発 表 *(cont .)*

[4] D. Tang, C. Pham , K. Chinen and R. Beuran: ”Interactive Cybersecurity Defense Training Inspired by Web-based Learning Theory”, IEEE 9th International Conference on Engineering Education (ICEED 2017), pp.103–108, Kanazawa, Japan, November, 2017

□これまでの活動 — 2015年度

- 若年層向けコンテンツの検討
- CTF 風課題提示・採点システム Cyclone実装
- 関連組織・イベントとの情報交換、及び参加

□これまでの活動 — 2016年度

- 演習システム実装、CyTrONEなど
- NIST技術ガイドに沿ったコンテンツ作成
- 都立高専と共同研究
  インターン: 高専生がコンテンツを作成（3/21-24）
- 国際会議2件、国内会議1件
- 関連組織・イベントとの情報交換、及び参加

□これまでの活動＋現在進行中 — 2017年度

- GitHub で CyTrONE 0.1 ＜ベータ＞公開
- INTEROP デモ展示
- 国際会議1件
- 関連組織・イベントとの情報交換、及び参加

- 都立高専と共同研究
- アライドテレシスアカデミーと共同研究
- 年度末、CyTrONE 1.0 公開予定

□関連組織・イベント

都立高専	共同研究、 インターン
アライドテレシスアカデミ	共同研究
国立高専機構	情報交換
NICT StarBED 技術センター	共同研究、施設利用
NICT セキュリティ人材 育成研究センター	情報交換
NEC 北陸ソリューションイノベータ	情報交換、開発協力

イベント: CYDER、Hardening、SECCON、セキュリティ・ミニキャンプ

□設問例

```
---
- training:
  - id: L1-JA
    title: デスクトップコンピュータのセキュリティ調査
    overview: |
      <p>本日はシステム管理者として初めての仕事の日です。あなたの上司は、誰かがあなたの会社のネットワークに攻撃しようとしたことを疑っており、あなたにダニエル・グレイグと呼ばれる男が管理者だった頃に起こった可能性のあるサイバー攻撃を調査するよう頼みました。上司は前任のシステム管理者のコンピュータの前にあなたを座らせて、上手くいくことを望んでいます。</p>
      <p>あなたはパソコンを見て、渋々仕事に取り掛かります。</p>
    level: 1
    questions:
    - id: L1-JA-001
      body: オペレーティングシステムとカーネルリリース番号はコ
```

□設 問 例 *(cont.)*

ンピュータにどの脆弱性の可能性があるか伝えることができます。マシンのカーネルリリース番号を探してください。(例:3.4.5-6.7.8.abc.x86_64

```
answer: 3.10.0-514.21.1.el7.x86_64
hints:
  - あなたは<code>uname</code>コマンドを使ってOSの詳細を探すことができます。
  - <code>$ uname -r</code>
  - 別の方法として，<code>/proc/version</code>ファイルから必要な情報を探すことができます。
```

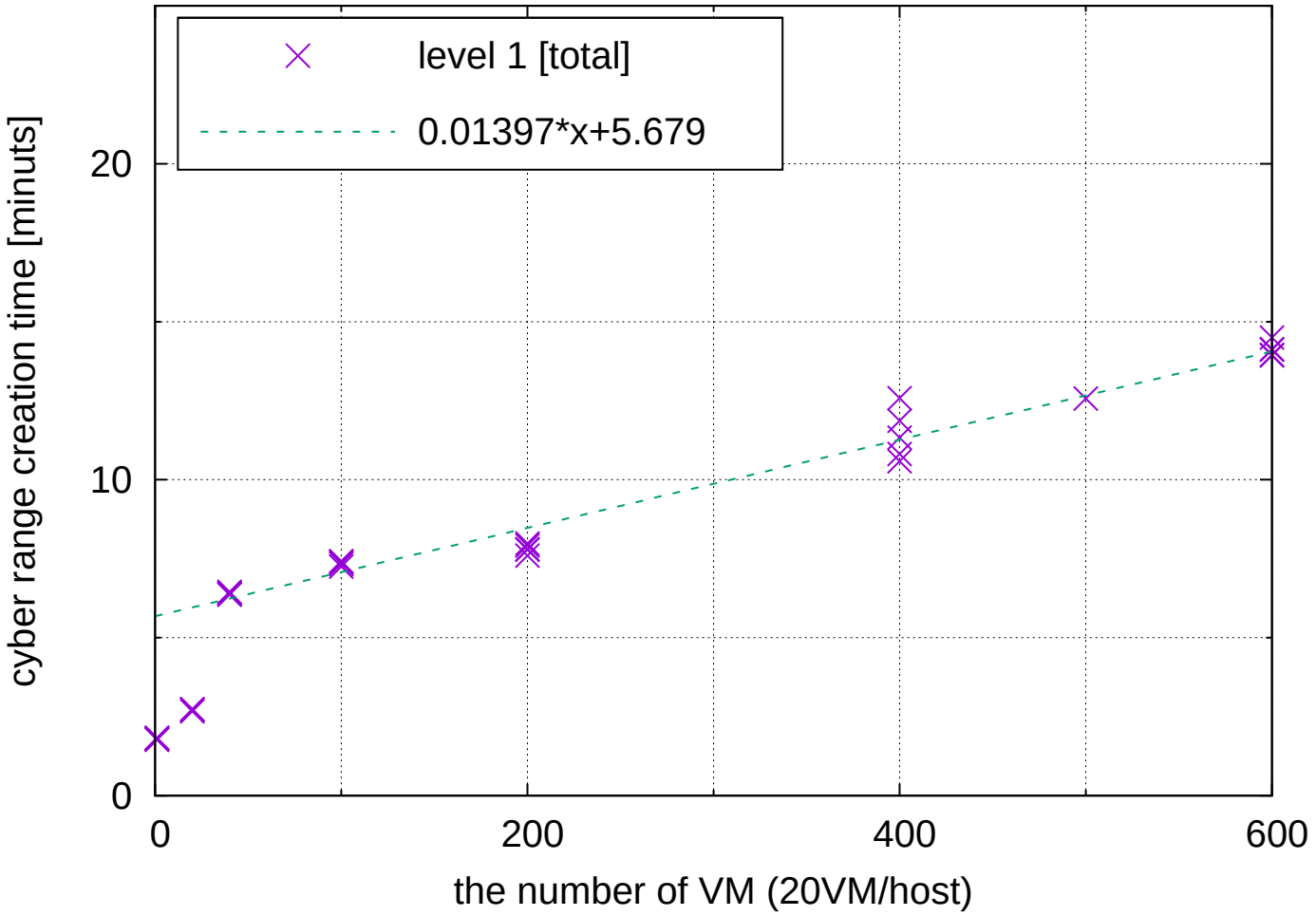
□場所記述例

```
---
- host_settings:
  - id: host_1
    mgmt_addr: {{ host_mgmt_addr }}
    virbr_addr: {{ host_virbr_addr }}
    account: {{ host_account }}
- guest_settings:
  - id: desktop
    basevm_host: host_1
    basevm_config_file: /home/cyuser/images/basevm_small.xml
    basevm_type: kvm
    tasks:
    - add_account:
      - account: daniel
        passwd: JamesBond
        full_name: Daniel Craig
    - install_package:
```

□場所記述例 *(cont.)*

```
    - package_manager: yum
      name: wireshark
- emulate_attack:
  - attack_type: ssh_attack
    target_account: daniel
    attempt_number: 54
    attack_time: 20170328
```

□性能グラフ


level 1 [total]
0.01397*x+5.679
cyber range creation time [minuts]
0
10
20
0
200
400
600
the number of VM (20VM/host)