JAIST
JAPAN
ADVANCED INSTITUTE OF
SCIENCE AND TECHNOLOGY
1990

サイバーレンジ構成学
CRONO
Cyber Range Organization and Design

サイバーセキュリティ演習フレームワークCyTrONE

コンテンツ作成

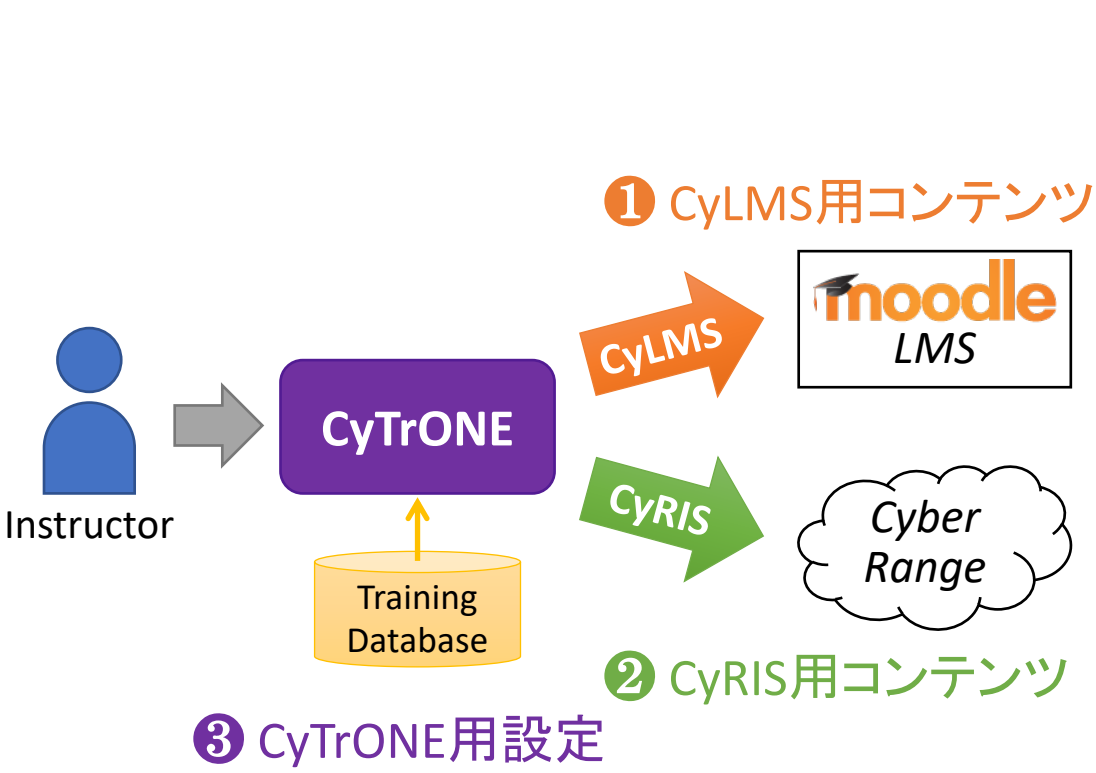
北陸先端科学技術大学院大学

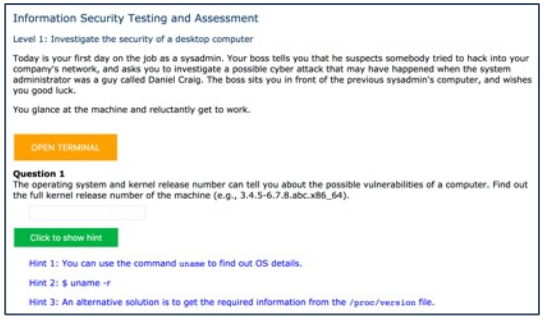
Razvan Beuran

概要

1. CyLMS用コンテンツ作成
2. CyRIS用コンテンツ作成
3. CyTrONE用設定
4. まとめ

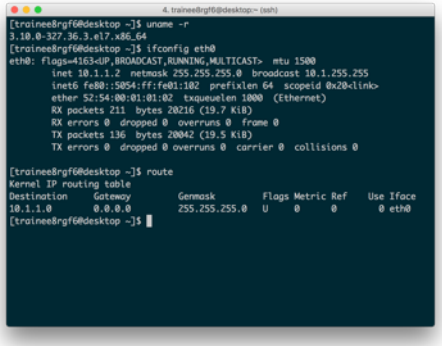
コンテンツ作成方法





Moodle UI

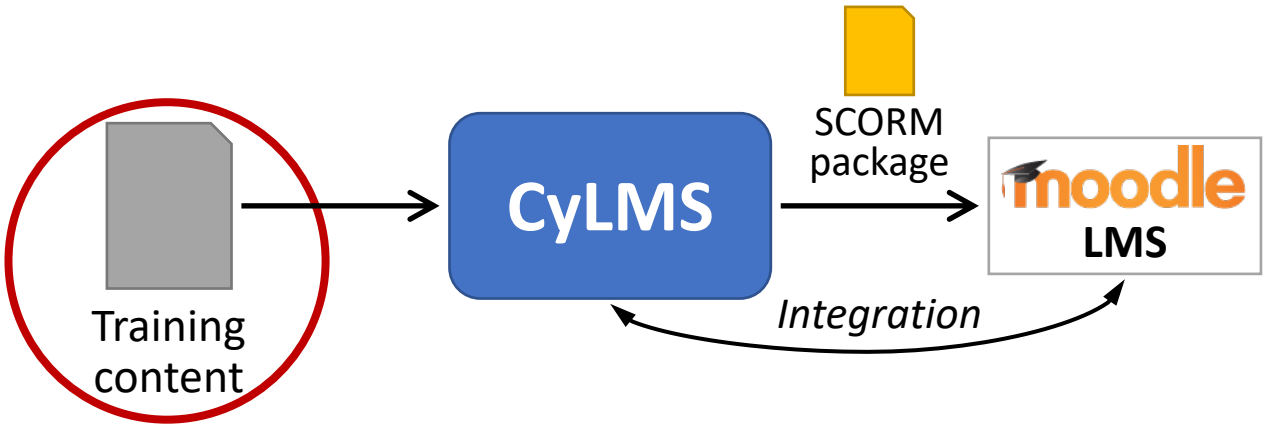
Trainees



SSH/VNCでアクセス

1. CyLMS用コンテンツ作成

Reference: *R. Beuran, D. Tang, Z. Tan, S. Hasegawa, Y. Tan, Y. Shinoda, "Supporting Cybersecurity Education and Training via LMS Integration: CyLMS", Springer Education and Information Technologies, vol. 24, no. 6, November 2019, pp. 3619-3643.*



CyLMS用の
記述ファイル ＋ CyTrONE用の設定

CyLMS用の記述ファイル

- CyTrONEのサンプルファイル: NISTレベル1
  - `cytrone/database/NIST-level1-content-ja.yml`
- 二つのセクション
  - `title`など: コンテンツのタイトルなど
  - `questions`: 問題の内容

titleなど

```
---
- training:
  - id: NIST-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
```

コンテンツのIDとタイトル

コンテンツの概要

レベル番号（省略可能）

questions

問題のID

問題の内容

```
- 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: 3.10.0-957.12.2.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。

    - id: L1-JA-002
      ...
```

問題の正解答

ヒントのリスト

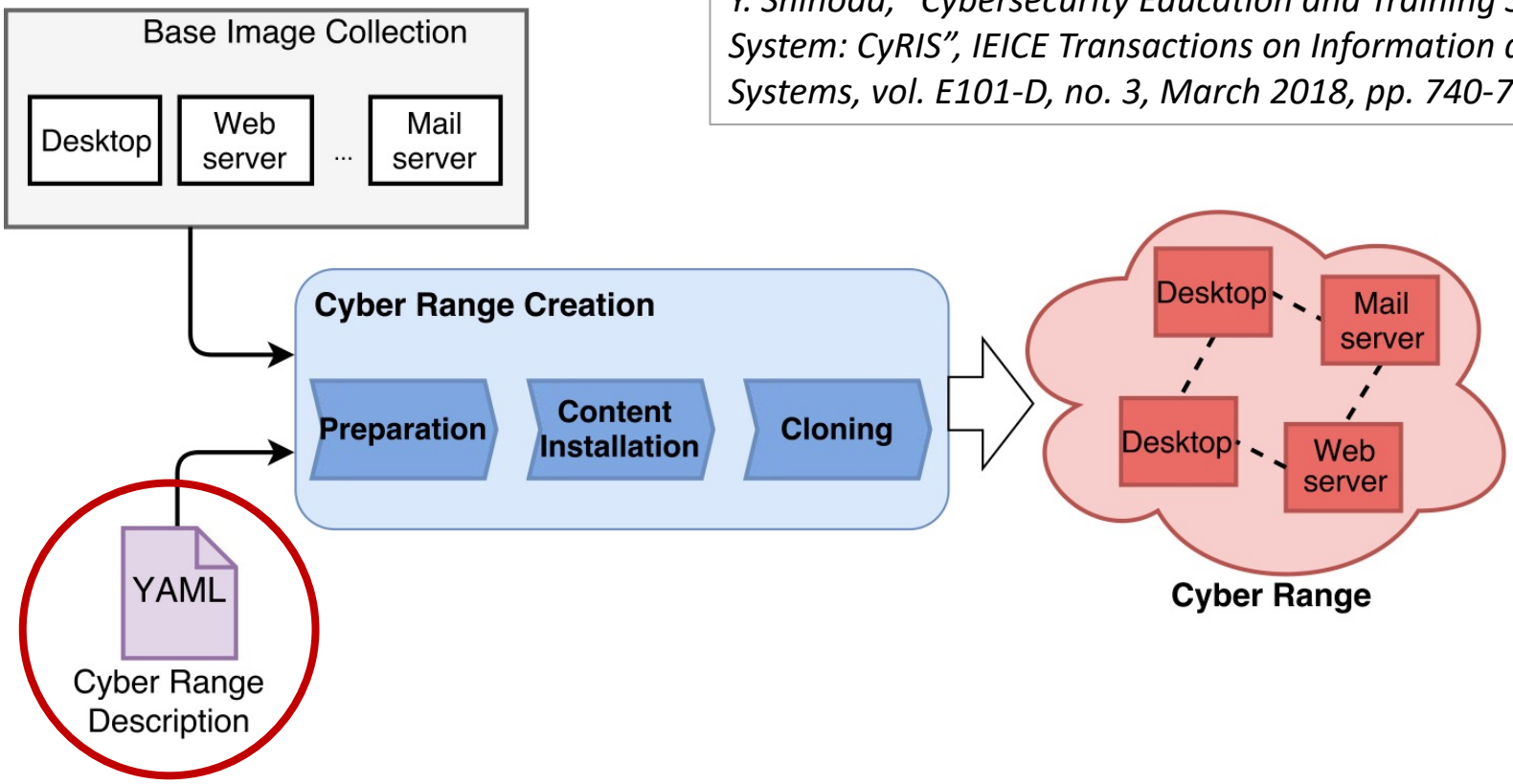
詳しい情報

- CyLMSユーザガイド
  - `title`など: pp. 5-7
  - `questions`: pp. 7-9
- CyLMSのサンプルファイル（cylms/）
  - `demo_quiz.yml`: 各種類の問題例

- 注意点：問題の解答をサイバーレンジの内容（CyRIS用コンテンツ）に合わせる必要がある

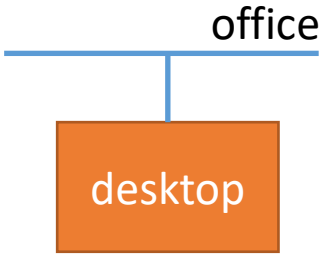
2. CyRIS用コンテンツ作成

Reference: *R. Beuran, C. Pham, D. Tang, K. Chinen, Y. Tan, Y. Shinoda, "Cybersecurity Education and Training Support System: CyRIS", IEICE Transactions on Information and Systems, vol. E101-D, no. 3, March 2018, pp. 740-749.*



CyRIS用の記述ファイル ＋ CyTrONE用の設定

CyRIS用の記述ファイル



- CyTrONEのサンプルファイル: NISTレベル1
  - `cytrone/database/NIST-level1-range.yml`
- 三つのセクション
  - `host_settings`: ホストPCの設定
  - `guest_settings`: ゲストVMの設定
  - `clone_settings`: VMクローニングの設定
- CyTrONEを利用する事を想定
  - 直接CyRISを利用する場合、`{{ VAR }}`の変数の代わりに値を使う必要がある

host_settings

```
---
- host_settings:
  - id: host_1
    mgmt_addr: {{ host_mgmt_addr }}
    virbr_addr: {{ host_virbr_addr }}
    account: {{ host_account }}
```

CyRISが利用するホストのID
（他のセクションで使用）

CyTrONE用の設定
ファイルに指定

guest_settings

```
- guest_settings:
  - id: desktop
    basevm_host: host_1
    basevm_config_file: /home/cyuser/images/basevm.xml
    basevm_type: kvm
    tasks:
    - add_account:
      - account: daniel
        passwd: JamesBond
        full_name: Daniel Craig
    - install_package:
      - package_manager: yum
        name: wireshark
```

ゲストVMのID

VMファイルが保存されているホストのID

VMファイル名

タスクのリスト

アカウントを追加するタスク

パッケージをインストールするタスク

問題6

問題4

問題8

guest_settings (2)

問題5

問題8

問題10

```
- emulate_attack:
  - attack_type: ssh_attack
    target_account: daniel
    attempt_number: 54
    attack_time: 20170328
- emulate_traffic_capture_file:
  - format: pcap
    file_name: /home/traffic.pcap
    attack_type: ssh_attack
    attack_source: 2.95.120.235
    noise_level: medium
- emulate_malware:
  - name: DAEMON
    cpu_utilization: 40
    mode: dummy_calculation
```

攻撃エミュレーションのタスク

PCAPファイル生成のタスク

マルウェアエミュレーションのタスク*

(*cpu_limitが必要)

clone_settings

CyTrONEが設定する

```
- clone_settings:
  - range_id: {{ clone_range_id }}
    hosts:
    - host_id: host_1
      instance_number: {{ clone_instance_number }}
      guests:
      - guest_id: desktop
        number: 1
        entry_point: yes
      topology:
      - type: custom
        networks:
        - name: office
          members: desktop.eth0
```

レンジ生成に使われるホストのID

使うゲストVMのIDとVM数

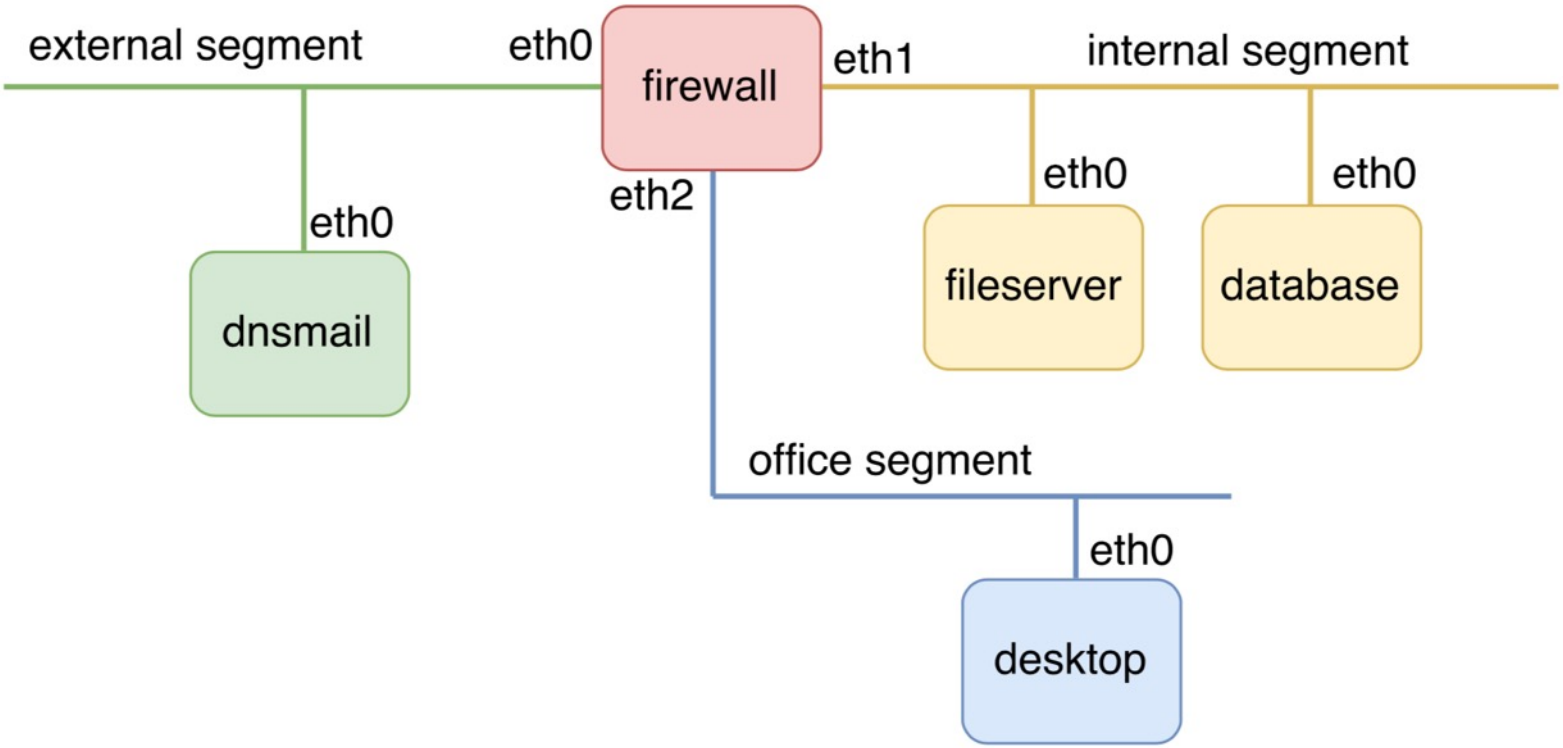
レンジの「入口」として指定

eth0をネットワークに設定

詳しい情報

- CyRISユーザガイド
  - `host_settings`: pp. 5-6
  - `guest_settings`: pp. 6-16
  - `clone_settings`: pp. 16-23
- CyRISのサンプルファイル（cyris/examples/）
  - `basic.yml`: 空のサイバーレンジ
  - `basic_multi-host.yml`: 空のサイバーレンジ（マルチホストバージョン）
  - `dmz.yml`: 複数VMのサイバーレンジサンプル（DMZ）
  - `full.yml`: 記述ファイルの説明

DMZサンプル


external segment
eth0
firewall
eth1
internal segment
eth0
eth2
eth0
eth0
dnsmail
fileserver
database
office segment
eth0
desktop

DMZのclone_settings：guests

```
guests:
- guest_id: firewall
  number: 1
  forwarding_rules:
  - rule: src=office,external dst=internal.dbsrv dport=3306
  - rule: src=office,external dst=internal.filesrv dport=139,445
  - rule: src=office dst=external dport=25,53
  entry_point: yes
- guest_id: dnsmail
  number: 1
- guest_id: filesrv
  number: 1
- guest_id: dbsrv
  number: 1
- guest_id: desktop
  number: 1
```

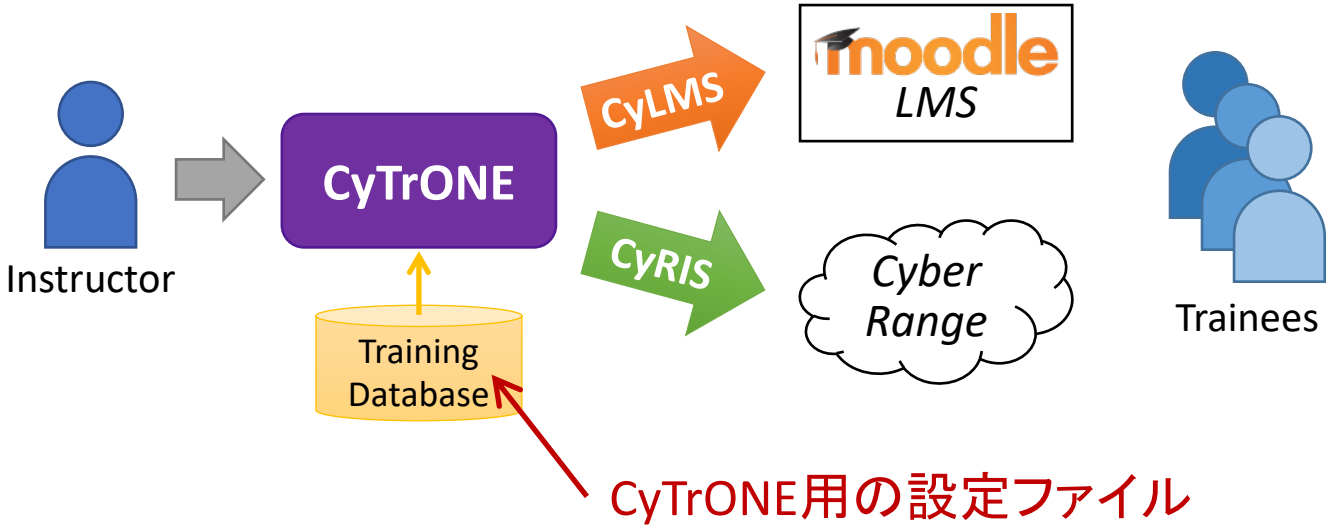
DMZのclone_settings：topology

```
topology:
- type: custom
  networks:
  - name: external
    members: dnsmail.eth0
    gateway: firewall.eth0
  - name: internal
    members: filesrv.eth0, dbsrv.eth0
    gateway: firewall.eth1
  - name: office
    members: desktop.eth0
    gateway: firewall.eth2
```

注意点

- ゲストのIPアドレスは、CyRISが自動的に設定 (p. 18)
  - <range id>.<instance id>.<segment no>.<guest id>
  - 生成されたサイバーレンジについての情報がファイルに保存される
    `cyris/cyber_range/ID/range_details-crID.txt`

3. CyTrONE用設定



Reference: *R. Beuran, D. Tang, C. Pham, K. Chinen, Y. Tan, Y. Shinoda, "Integrated Framework for Hands-on Cybersecurity Training: CyTrONE", Elsevier Computers & Security, vol. 78C, June 2018, pp. 43-59.*

設定ファイル

- 二つの設定ファイル
  - `users.yml`: ユーザ・ホストの設定
    - CyTrONEへのアクセス情報
    - CyRISが利用できるホスト情報
    - 詳しい情報：CyTrONEユーザガイド pp. 3-5
  - `training-LN.yml`: 演習コンテンツの登録
    - `training-en.yml`: 英語版コンテンツ
    - `training-ja.yml`: 日本語版コンテンツ
    - 詳しい情報：CyTrONEユーザガイド pp. 5-6

users.yml

```
---
- users:
   - name: John Doe
     id: john_doe
     password: $pbkdf2-sha256$29000$7x2jl…
     host_mgmt_addr: 172.16.1.7
     host_virbr_addr: 192.168.122.1
     host_account: cyuser
```

ユーザリスト

ユーザ名

ユーザID

パスワードハッシュ
(password.pyで生成)

CyRIS用の設定
（記述ファイルで使用）

training-ja.yml

```
---
- types:
  - name: シナリオに基づいた演習
    category: scenarios
  - name: トピックに基づいた演習 [N/A]
    category: topics
- scenarios:
  # Scenario based on the US National Institute of Standards and Technology
  # (NIST) Guide on Information Security Testing and Assessment
  - name: 情報セキュリティテスト＆評価
    levels:
      - name: レベル 1
        content: NIST-level1-content-ja.yml
        specification: NIST-level1-range.yml
      - name: レベル 2
        content: NIST-level2-content-ja.yml
        specification: NIST-level2-range.yml
```

シナリオリスト

シナリオ名

レベルリスト

レベル名

CyLMS用（content）と
CyRIS用（specification）
の記述ファイルを指定

新しいコンテンツの登録

4. まとめ

- CyLMS用記述ファイルの作成 → 演習コンテンツ（問題）の準備
  - `title`など: コンテンツのタイトルなど
  - `questions`: 問題の内容
- CyRIS用記述ファイルの作成 → サイバーレンジの設計
  - `host_settings`: ホストPCの設定
  - `guest_settings`: ゲストVMの設定
  - `clone_settings`: VMクローニングの設定
- CyTrONE用設定ファイル → ユーザ・ホストの設定と新コンテンツの登録
  - `users.yml`: ユーザ・ホストの設定
  - `training-LN.yml`: 演習コンテンツの登録