Vol.2018-CSEC-83 No.1
2018/12/13

サイバーレンジ演習環境展開の高速化手法

村木 優太[1,a)]　上原 哲太郎[2]

概要：近年，サイバー攻撃の増加にともないセキュリティ人材の育成が急務となっている．しかし，現在のセキュリティ人材の教育は座学が中心となっており，教育現場と実務環境とでは隔たりがある．こういった背景から，実演習型のサイバー攻撃の学習が必要になっている．実務環境にを模した仮想的な環境でサイバー攻撃の実演習を行える場としてサイバーレンジがある．これにより実演習型のサイバー攻撃の学習が可能になる．しかし，サイバーレンジは，様々なサイバー攻撃の筋書きに応じた環境構築が必要となり，環境構築に長いな時間を要する．そこで，我々は演習環境展開の高速化手法を提案する．提案手法では，ZFS を用いた演習環境構築により，環境構築と演習環境切替の高速化を図っている．

キーワード：サイバーレンジ，環境構築高速化，ZFS，セキュリティ人材育成

A method of acceleration to deploy cyber-range experimental environments

Muraki Yuta[1,a)]　Uehara Tetsutaro[2]

1. 序論

近年，パソコン・スマートフォンの普及によりインターネットの利用率が大幅に増加した．それに伴いインターネット上で個人情報などの電子データのやり取りがされるようになり，この個人情報を狙った攻撃が生まれ攻撃が増加している．この攻撃はサイバー攻撃と呼ばれており現代ではこのサイバー攻撃が大きな問題となっている．しかし，サイバー攻撃が増加するなか情報セキュリティ分野の人材不足が問題となっている．IPO の情報セキュリティ 10 大脅威 2018[1] によると，脅威に対応するためのセキュリティ人材の不足が「組織」向け脅威の 5 位に位置している．

[1] 立命館大学 大学院情報理工学研究科
Graduate School of Information Science and Engineering, Ritsumeikan University
[2] 立命館大学 情報理工学部
College of Information Science and Engineering, Ritsumeikan University
[a)] muraki@cysec.cs.ritsumei.ac.jp

情報セキュリティ分野の人材が不足している現状から，現在日本では経済産業省が中心になって情報セキュリティ人材育成への力が注がれている．これらの人材育成は座学が中心に置かれ，実演習のないものも存在する．サイバー攻撃に対する対処として座学で学ぶ知識も必要ではあるが，実際のサイバー攻撃への対処は実対処の経験が必要となる [2]．現在サイバー攻撃の実演習を経験する場としてサイバーレンジがある．

サイバーレンジとは，サイバー攻撃を防ぎ・軽減させる方法を演習する実環境を模した擬似的な演習場で，座学だけでなく実演習を行うことができる．サイバーレンジはシナリオと呼ばれるサイバー攻撃の筋書きが存在し，サイバーレンジ演習者はシナリオに沿って演習を行う．サイバーレンジは実環境を模した擬似的な演習場上においてシナリオを考慮した機器設定・ネットワーク環境上で演習を行うという特徴から，シナリオに応じた演習環境構築が必要になる．この演習環境構築には多大な時間が要されている．演

表 1　2014 年における想定人材数

スキルレベル	人材数
トップガン	10 人以下
トップガン補佐	20 人
中間層エリート	300 人
中間層	3000 人
中間層の卵	300 人採用/年
基礎教育修了者	10,000 人輩出/年

習環境構築は人材育成の本質ではなく，サイバーレンジの演習環境構築時間を短縮する必要がある．

2. 研究背景

2.1 セキュリティ人材不足と人材育成の必要性

IPO の情報セキュリティ 10 大脅威 2018[1] に脅威に対応するためのセキュリティ人材の不足が「組織」向け脅威の 5 位に位置していることからもセキュリティ人材不足が問題になっていることがわかり，セキュリティ人材育成の必要性が考られる．

2.1.1 セキュリティ人材育成の対象

セキュリティ人材の不足からセキュリティ人材育成に力をいれる必要があるが，人材不足を解消するためには多くのセキュリティ人材を対象とする必要がある．サイバーセキュリティ人材像（7 階層）[3] があるが，区分は表 1 に示すスキルレベルによってわけられている．

表 1 の想定人数は，2014 年におけるサイバーセキュリティ人材をサイバーセキュリティ人材像にわけた場合の想定人材数である．想定人材数の算定方法は参考文献 [3] を参考にしている．

この 7 層のスキルレベルにおいて，「基礎教育修了者」と「中間層の卵」を育成することによって，毎年 10,300 人以上もセキュリティ人材を輩出できる可能性を秘めている．これら層を育成することでセキュリティ人材不足の解消につながると考えられる．

2.1.2 セキュリティ人材育成における問題点

「基礎教育修了者」と「中間層の卵」の層を育成することによってセキュリティ人材不足が解消される可能性があるが，これらの層は対象者が多く個人で大きくスキルが異なる．また，これらの層は大学の講義での演習が想定されるため，演習できる時間が限られてくる．したがって，時間制約下における個人のスキルに適した内容の育成内容が必要となる．

2.2 サイバーレンジ

サイバーレンジとは，サイバー攻撃を防ぎ・軽減させる方法を演習する実環境を模した計算機利用環境である．現在サイバー攻撃の学習は座学中心の教育であるが，サイバーレンジを用いた演習ではサイバー攻撃をシミュレーションした実際の環境を使用した専門的な育成が可能である [4]．一般企業のネットワークシステムを再現しサイバーレンジを用いて，実例に基づいて疑似攻撃によるトレーニングを行い，攻撃者がどういった視点でサイバー攻撃を行っているのかを学び，実際に発生しているサイバー攻撃の体験が模擬的に行える [5]．

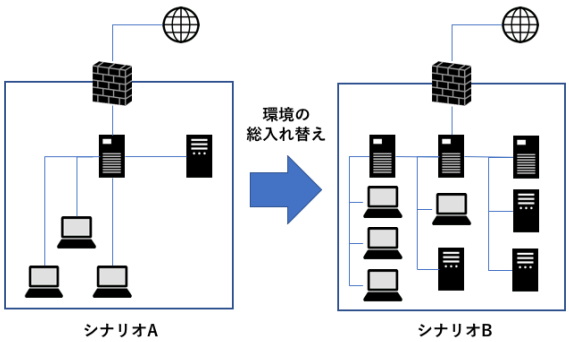

図 1　サイバーレンジ演習環境の総入れ替え 想定図

サイバーレンジはサイバー攻撃の筋書き（シナリオ）によって運用がされ，演習者はシナリオにそった対応をする．サイバーレンジの演習環境はサイバー攻撃が行われるという特徴から演習で利用する PC のシステムファイルが変更される可能性があり，サイバー攻撃の演習を行った環境で違うシナリオを実施した場合，前のシナリオにおける影響が出てしまう．したがって，図 1 に示すようにシナリオごとに演習環境の総入れ替えが必要となる．

2.2.1 時間制限下のサイバーレンジ実施

サイバーレンジを大学教育のような時間的制約のある教育現場に導入する際には，特有の問題がいくつか存在する．

1 つ目の問題として，生徒の能力によってシナリオを進める進度に差があり，サイバーレンジ演習環境の総入れ替え回数に影響があることである．サイバー攻撃への知識が乏しい生徒やプログラミングが苦手な生徒のレベルに合わせた解法を想定した場合，サイバー攻撃への知識が豊富な生徒やプログラミングが得意な生徒は短い時間でシナリオを解決し，次々と違うシナリオに取り組む．違うシナリオに取り組むに際に演習環境の総入れ替えが必要になるので，次々と多くのシナリオに取り組むとそのたびに演習環境の総入れ替えが必要になり，演習環境の総入れ替えにかかる時間の問題が大きくなる．

2 つ目の問題として，講義時間が固定されているため，演習環境の総入れ替えにかかる時間の問題が顕著に現れることである．一般的な大学における 1 回の講義時間は 90 分であり，この時間のなかで演習を行う．演習時間の中で取り組むシナリオの数は 1 つとは限らず，複数取り組むこともある．3 つのシナリオに取り組み，1 回の演習環境の

総入れ替えに 15 分かかると仮定した場合，演習環境構築に合計で 45 分の時間が取られ，実際に演習する時間は講義時間の半分になってしまう．

2.2.2 サイバーレンジ演習環境構築

一般にサイバーレンジにおいて，シナリオ間の演習環境の総入れ替えを行うことは長い時間を要する．この時間を大学講義間の休憩時間である 10 分以内におさめることで休憩時間内に演習環境総入れ替えが行え，演習時間圧迫の影響を小さくすることができる．本提案手法では，10 分以内という時間指標を演習環境切り替えの 1 つの目標としている．

学校教育におけるサイバーレンジを用いた演習を採用するにあたって問題となっている演習環境構築の時間を本提案手法を用いて解決することで，学校教育などの限られた時間下でのサイバーレンジを用いた演習が可能になる．

この演習環境の切り替えにおいて VM の複製（クローン）に 1 番時間がかかっている．これは複製の基となる VM（テンプレート VM）から数 GB〜数十 GB の VM イメージをコピーした後，数 GB〜数十 GB 分ディスク書き込みを行っているからである．本提案手法では，このディスク読み書きを少なくすることで高速化を図っている．

VM のクローン方法として，テンプレート VM のディスクイメージをすべてコピーすることで VM を複製する方法がある．このディスクイメージをすべてをコピーするクローン方法を FULL クローンと呼ぶ．また，ZFS と呼ばれるファイルシステムにはクローンという機能がある．この ZFS のクローン機能を使ったクローン方法を ZFS クローンと呼ぶ．ZFS や ZFS クローン方法については次節で説明する．

2.3 ZFS

ZFS とは，物理ストレージを管理するためにストレージプールという概念を使用しているファイルシステムであり，堅牢かつスケーラブルという特徴を備えている．ストレージプールはストレージの物理特性（デバイスのレイアウト，データの冗長性など）を記述したもので，ファイルシステムを作成する機能を持つ．ファイルシステムが個々のデバイスに制約されず，複数のディスク領域をプール内のすべてのファイルシステムで共有することができる [9]．

ZFS にはクローンの機能がある．ZFS のクローンはスナップショットと呼ばれるファイルシステムまたはボリュームの読み取り専用のコピーを基に複製する機能のことである．ZFS クローンの共通部分におけるディスク領域は基のスナップショットと共有されるためクローンは高速に行われる．

ZFS クローン後の VM は，ファイル読み出し時はスナップショットの基を参照する．一方で，ファイル書き込み時はスナップショットの参照先との差分をクローンで作成された VM のディスク容量に書き込み，スナップショットの参照先情報を書き換える．よって，ZFS は書き込み時に FULL クローンより時間が必要になる短所がある．本提案手法では，演習環境切替の高速化に ZFS クローンを利用している．

2.4 関連研究

サイバーレンジの研究では，Cuong Pham らがサイバーセキュリティのトレーニング環境として CyRIS というサイバーレンジのインスタンスシステム作成のためのツールを作成している．研究の内容としては，サイバーレンジのホスト環境のセキュリティ評価や VM 設定を設定ファイルを利用したスクリプト化などを行っている．しかし，サイバーレンジの演習環境構築において，2 台の仮想環境ホストで 8GB のイメージ 60 台の VM 複製に平均 672.1 秒かかっている [6]．これは我々が目標としている 10 分を超えている．

Beuran, Razvan らは CyTrONE というサイバーセキュリティトレーニングのフレームワークを作成した [7]．CyTrONE では，サイバーレンジ演習の環境構築の設定内容が YAML 形式で管理できるため，設定変更において高度なプログラミング技術を必要としない．また，演習において演習者のインターフェースとして e-Learning を使用している．e-Learing 上で演習の質問やヒントの参照，結果の統計などを行っている．

また，Lori Pridmore，Patrick Lardieri，Robert Hollister らはサイバーレンジを用いたネットワークの管理に関する研究をし環境の総入れ替えにサイバーレンジを用いることのメリットを述べている [8]．

サイバーレンジの有用性やサイバーレンジ演習を行う上で演習者のユーザビリティを向上させる提案はされているが，演習環境切り替え時間の高速化に注力している研究は少ない．演習切り替え時間は，限られた時間内で演習を行う大学などの機関において大きな問題である．本研究では演習環境切り替え時間の問題解決の手法を導入した．

3. 提案手法

本提案手法では，ZFS クローンによってサイバーレンジの演習環境展開の高速化を図る．高速化の指標として大学講義間の 10 分を目標とする．サイバーレンジの演習環境展開の高速化を実現することによって，シナリオ間の演習環境展開における待機時間の減少を実現する．

サイバーレンジ演習では，シナリオにそったネットワーク設定や時限式のマルウェア感染など，シナリオ通りに演習が行える設定済みの環境が必要となる．この設定済みの環境構築を 1 からすると時間がかかるので，シナリオに

必要なツールのインストールなどを事前に行い VM のクローンで短縮している．しかし，VM のクローンを行うとクローン後にクローンの基となる VM と同じ設定になってしまう．そこで，クローン後の VM の設定を変更するためにスクリプトを作成し，クローンが行われたあとに同一設定がされているクローン後の VM の設定を，サイバーレンジのシナリオにそった IP アドレスやマシン ID などに変更している．

仮想環境における VM のイメージは qcow2 や raw などであり，仮想環境ホストからは VM イメージ内のファイルに直接アクセスできない．そこで仮想環境ホストが VM イメージにアクセスできるようにイメージを変換しマウントする必要がある．マウントする流れを図 2 に示す．仮想環境ホストがアクセスできるように KVM のツールである qemu-nbd で VM のイメージを他のデバイスにおける記録領域として認識する NBD（Network Block Device）として振る舞うように変換する．NBD とは，ネットワーク経由で他のデバイスにおける記録領域を使用可能にするデバイスのことである．この NBD として振る舞っている VM イメージを，編集が行えるように仮想環境ホストのデバイスにマウントするためにボリュームグループの VM イメージを論理ボリュームに分割し，論理ボリュームを仮想環境ホストのデバイスにマウントしている．NBD として振る舞って VM イメージにおいて，複製の基が同一の VM イメージおいて UUID（Universally Unique Identifier）が重複し，仮想環境ホストが異なるディスクイメージへのアクセスを試みたとしても同一の VM イメージへアクセスを試みていると認識してしまう．UUID とはソフトウェア上でオブジェクトを一意に識別するための識別子である．そこで，複製した VM の個々のディスクイメージを異なるディスクイメージだと認識させるために UUID の変更を行う．これらの手順を経ることで，VM のディスクイメージへの編集を可能にしている．

本提案手法におけるサイバーレンジ演習を想定した VM の構成図を図 3 に示す．4 人の学生を 1 つのグループとしている．学生それぞれにクライアント端末となる VM を 1 台，ソフトウェアルータの VM を 1 台、ウェブサーバの VM を 1 台使うと想定し，6 グループ分 36 台の VM を準備している．

3.1 ZFS クローンによる環境構築

本手法では Proxmox VE（Proxmox Virtual Environment：以降「Proxmox」と表記）[10] を仮想環境ホストとして用いている．Proxmox は，Linux の KVM 機能と QEMU の技術を用いた仮想化ツールである．Proxmox は，CLI を使用することにより，コマンドラインでの仮想環境の操作が可能になる．また，ZFS をサポートしているので，提案手法を実現する上で新たに ZFS 環境を構築する必要がない．

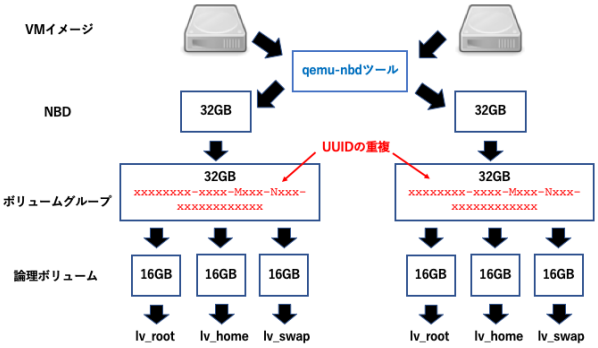

図 2　VM イメージ マウントの流れ

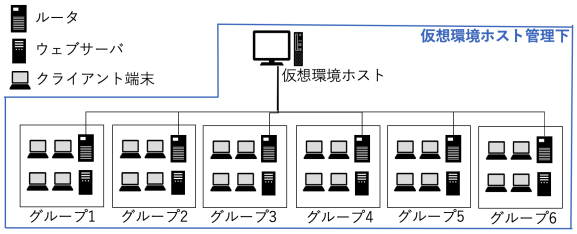

図 3　サイバーレンジ演習実験 想定図

ZFS クローン時にクローンの基となる VM のスナップショットの作成が必要となるが，スナップショットは VM を準備する段階で作成している．スナップショップが作られている状態で ZFS クローンを行っている．ZFS クローンの実行方法は，zfs clone コマンドで行っている．

3.2 スナップショット参照による環境構築

サイバーレンジ演習においてシナリオごとにサイバーレンジ演習環境の総入れ替えが必要と述べたが，これは 1 度演習に利用した VM は演習中に設定が変わっている可能性があり再利用できず破棄する必要があるという意味である．既存研究では FULL クローンを用いた環境構築行っているため，サイバーレンジで用いる演習環境を準備するためには大容量が必要となる．これは，演習利用する VM とテンプレート VM でディスク容量が必要になるからである．テンプレート VM のディスク容量が大きくなる理由として，Windows では SID と呼ばれる識別子の重複を解決する必要があげられる．SID とは Windows のユーザやファイルオブジェクトについている識別子のことでありユニークである必要がある．SID が重複すると Windows が動かなくなる可能性がある．SID の再付番は sysprep で行うがこれは多くの時間がかかり，サイバーレンジ演習環境展開時に行う時間的余裕はない．そこで本提案システムでは，SID が異なる端末を事前に利用する台数分用意する手法を取っている．利用する台数分用意するのでディスク容

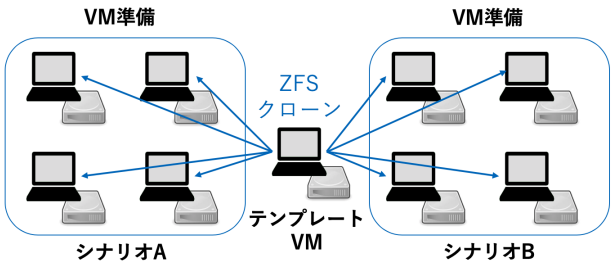

図 4　スナップショット参照による環境構築 (演習環境の準備)

量が必要となる．

ZFS クローンではクローン時にスナップショットリンクのみのディスク容量で済むため，クローン時にクローンの基となるテンプレート VM 分のディスク容量を必要としない．そのため演習環境構築時のディスク容量を大幅に削減することができ，サイバーレンジ演習環境を演習前にすべて準備しておくことが可能である．よって，演習時のシナリオ入れ替えは VM の停止と起動だけで済み，演習環境展開の時間がほぼかからない．

サイバーレンジ演習環境を演習前にすべて準備する手法の流れを図 4〜図 6 に示す．ここではシナリオ A, B 二つのシナリオを実施することを想定している．最初にシナリオ A を実施し，シナリオ A を終えるとシナリオ B に移行する流れになっている．

図 4 はサイバーレンジの演習環境を演習前にすべて準する想定図である．演習環境構築ではシナリオごとに使う VM をテンプレート VM を基に ZFS クローンで複製する．ZFS クローンを行うことでクローン時のディスク容量を多く必要としない．

図 5 はシナリオ A 実施時の想定図である．シナリオ A で使う VM を起動し演習で利用できるようにする．このときシナリオ B で使う VM は起動せず停止させたままにする．演習中のシナリオ A の VM は停止されているシナリオ B で使う VM にアクセスするのは容易でなく，シナリオ B で使う VM はシナリオ A の演習時に影響を受けない．

図 6 はシナリオ B 実施時の想定図である．シナリオ A で使った VM は起動したままでいるとシナリオ B 実施時に影響を与える可能性があるため，シナリオ移行時にシナリオ A で使った VM はすべて停止する．そして，シナリオ B で使う VM を演習で利用できるように起動する．

4. 実験結果

実験結果を関連研究と比較できるように，本提案手法で用いた機器を表 2 に，関連研究 CyRIS で用いられていた機器を表 3 に示す．

4.1 ZFS クローンによる環境構築

ZFS クローンを用いた演習環境の切り替えで，本提案手法では関連研究よりも多いイメージ容量と VM 台数において，関連研究と比較して大幅な時間短縮がみられた．関連研究と本提案手法との時間の比較を表 4 に示す．ZFS クローンを用いることによって，目標としていた 10 分以内の演習展開に成功している．

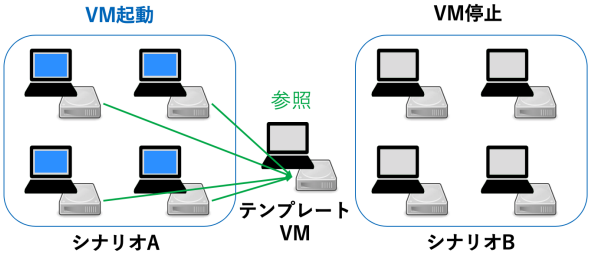

図 5　スナップショット参照による環境構築 (シナリオ A の実施)

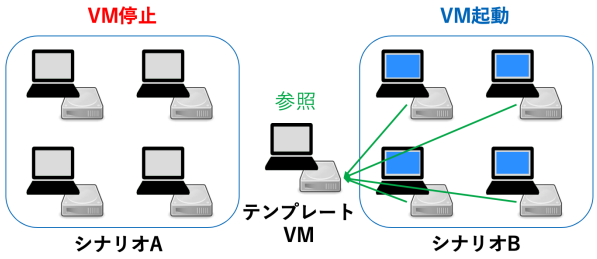

図 6　スナップショット参照による環境構築 (シナリオ B の実施)

表 2　本提案手法使用 PC 機器

部品名	仕様
CPU	3.5GHz(Cores=4/Threads=8/Cache=8MB)
メモリ	48GB(8GB * 2 + 16GB * 2)
ハードディスク	12TB(3TB/Cache 64MB)* 4

表 3　関連研究使用 PC 機器

部品名	仕様
CPU	2GHz(Cores=4/Threads=4/Cache=4MB)
メモリ	72GB
ハードディスク	400GB

表 4　関連研究との比較 1

	ZFS クローン手法	関連研究
イメージ量	32GB	8GB
VM 数	36 台	30 台
総イメージ量	1,152GB	240GB
クローン時間	195.6 秒	627.1 秒

4.2 スナップショット参照による環境構築

ZFS クローンによる環境構築を応用し，サイバーレンジ演習前にすべての演習環境を構築することに成功している．これはシナリオが 4 つあると仮定し，4 シナリオ分計 144 台の VM のクローンと VM の設定変更を行っている．関連研究と本提案手法との時間の比較を表 5 に示す．スナッ

表 5　関連研究との比較 2

	スナップショット参照手法	関連研究
イメージ量	32GB	8GB
VM 数	144 台	30 台
総イメージ量	4608GB	240GB
クローン時間	651.4 秒	627.1 秒

表 6　FULL クローンと ZFS クローンのディスク書き込み要求比較

ZFS クローン	FULL クローン
163.46 回	1017.29 回

プショット参照による環境構築では関連研究よりもクローン時間が長くなってしまっているが，これは 4 シナリオ分の演習環境構築をしているからである．シナリオの切り替えのみに焦点を当てると，スナップショット参照による環境構築では VM の停止と起動だけで済むので 1 分以内に演習環境展開に成功している．

5. 評価・考察

ZFS クローンとスナップショット参照を用いることによって演習環境切り替えの高速化に成功している．演習環境切り替え時間を短縮することによって，演習に割ける時間が増えるので大きな意味があると考える．しかし，本提案手法 2 つにおいて演習中にディスク IO が発生すると，FULL クローンで作った VM のディスク IO と比較して時間がかかってしまう．これは，スナップショットの内容から差分が発生すると差分の書き込みとスナップショットへの参照先書き換えが必要となるからである．よって，大量のディスク IO が発生するシナリオにおいては FULL クローンへの置き換えの方がシナリオ進行において弊害が少ない可能性があり，ZFS クローンと FULL クローンの併用を考える必要がある．大量のディスク IO が発生しないシナリオにおいては，FULL クローンと ZFS クローンとの差は感じられないアンケート結果がでている．

5.1 ZFS クローンによる環境構築

36 台の VM のセットアップを目標としていた 10 分以内の 3 分 16 秒で行うことに成功した．これは，FULL クローンにおける VM データの全コピーとディスクへの書き込み処理がなくなっているからである．FULL クローンと ZFS クローンのディスク書き込みを比較するために iostat コマンドの w/s の値を参照した結果を表 6 に示す．ZFS クローンと FULL クローンとで 6.22 倍の要求数の差がある．この要求数の差で FULL クローンの方が 3 倍も演習環境構築に時間がかかっているため，ディスク書き込みに大きな差が生まれている．ディスク書き込み処理を少なくすることよって，高速化に成功した．

5.2 スナップショット参照による環境構築

ZFS クローンで VM をクローンをした場合スナップショットの参照先を作成するだけで済むため新たに確保するディスク容量は少なく済む．Proxmox において ZFS クローン後の VM のディスク容量は，起動した場合で 8MB，以下起動しない場合で 1MB 以下に抑えられている．ほとんどディスク容量を確保しておらず，ディスク容量増加の心配を無視できる．

スナップショット参照の特徴を活かすことによって演習が行われる前にすべての演習環境を用意することに成功し，切り替え時を VM の停止と起動だけで済むことに成功した．

5.3 FULL クローンと ZFS クローンの違いアンケート

セキュリティ知識のある 7 名の大学院生と 1 名の大学生を対象に FULL クローンと ZFS クローンとの 2 パターンのサイバーレンジ演習環境構築を行い，それぞれの環境でサイバーレンジ演習の実施とそれにともなうアンケートを行った．サイバーレンジ演習のシナリオはランサムウェアの原因の究明と暗号化されたデータの復元を行う大量のディスク IO が発生しないシナリオであった．このシナリオにおいて，対象者 8 名全員が FULL クローンと ZFS クローンとの 2 つの環境構築方法の違いによる演習実施への影響の差を感じないと回答した．この結果から実演習に ZFS クローンを利用できることがわかった．

6. 結論

ZFS クローンによる環境構築で 36 台の VM 分のサイバーレンジ演習環境展開を，目標としていた大学講義間の 10 分以内である 3 分 16 秒で行い，高速化に成功している．また，スナップショット参照による環境構築で 144 台の VM の演習環境事前準備を 10 分 52 秒で行い，演習環境展開に 1 分以内で成功している．

しかし，ZFS クローンではディスク読み書きが発生すると FULL クローンのときと比較し大きな IO 負荷がかかるので演習に支障をきたす可能性がある．そこで今後の課題としては，ZFS クローンと FULL クローンの時間モデリングを行い，演習実施における IO 負荷を考慮したクローン選択のモデリングを作成する必要がある．これは，ZFS クローンで環境構築した方が構築時間が短くで済むが演習実施時 IO 待機時間が長く演習にきたす可能性があるからである．図 7 に示すように ZFS クローンと FULL クローン時間で待機時間の境界点が存在するので，境界点を導き出し IO 負荷のかかるシナリオでは FULL クローンを使うといった切り替えが必要となる．このモデリングを作成することによって，ZFS クローンの短所をカバーすることができる．

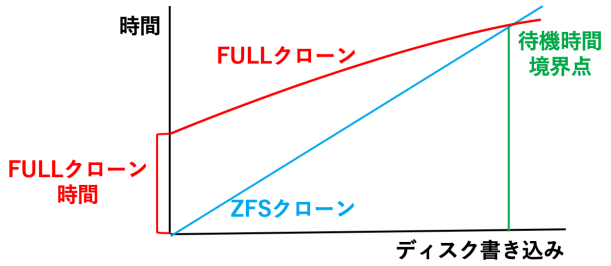

図 7　IO 負荷を考慮したクローン選択のモデリング

参考文献

[1] 情報セキュリティ 10 大脅威 2018：IPO 独立法人情報処理推進機構 セキュリティセンター，入手先 ⟨https://www.ipa.go.jp/files/000065376.pdf⟩（参照 2018-09-06）.
[2] 情報セキュリティ人材の育成・確保について：経済産業省，入手先 ⟨http://www.nisc.go.jp/conference/cs/jinzai/dai01/pdf/01shiryou0503.pdf⟩（参照 2011-09-15）.
[3] シスコ サイバーレンジ サービス：CISCO，入手先 ⟨http://www.cisco.com/web/JP/services/security/cyberrange.html⟩（参照 2011-09-15）.
[4] サイバーセキュリティ人材の発掘・育成・維持・レベルアップを社会全体で行うエコシステムの提言：OGC サイバーセキュリティ分科会，入手先 ⟨https://ogc.or.jp/wp/wp-content/uploads/2015/12/7_proposal_cyber_20150601.pdf⟩（参照 2017-01-07）.
[5] DNP、サイバーレンジの疑似攻撃で訓練するイスラエル製サービス：Security NEXT，入手先 ⟨http://www.security-next.com/061915⟩（参照 2011-09-15）.
[6] Pham, Cuong and Tang, Dat and Chinen, Ken-ichi and Beuran, Razvan.: *CyRIS: A Cyber Range Instantiation System for Facilitating Security Training*, SoICT (2016).
[7] Beuran, Razvan and Pham, Cuong and Tang, Dat and Chinen, Ken-ichi and Tan, Yasuo and Shinoda, Yoichi. : *CyRIS: A Cyber Range Instantiation System for Facilitating Security Training*, ICISSP (2017).
[8] National Cyber Range（NCR） Automated Test Tools: Implications and Application to Network-Centric Support Tools.: *Lori Pridmore, Patrick Lardieri, Robert Hollister*, AUTOTESTCON (Proceedings) (2010).
[9] ORACLE：Oracle Solaris の管理：ZFS ファイルシステム，入手先 ⟨https://docs.oracle.com/cd/E26924_01/html/E25824/zfsover-2.html⟩（参照 2011-09-15）.
[10] Proxmox VE：Proxmox Server Solutions GmbH., 入手先 ⟨https://www.proxmox.com/en/⟩（参照 2018-11-13）.