サイバー攻撃に対応するセキュリティマイスター育成のためのサイバーレンジCYBERIUM

Cyber Range CYBERIUM for Training Security Meisters to Deal with Cyberattacks

原　和宏

あらまし

今日，お客様のシステムは，常にサイバー攻撃の脅威にさらされている。このような時代においてお客様の業務を守るためには，お客様のシステムがサイバー攻撃に遭ったときに被害を最小限に抑えられる対応力が鍵となる。富士通では，サイバー攻撃への対応力を備えた人材であるセキュリティマイスターを育成することで，この課題に対応している。サイバー攻撃への対応力を向上させるためには，仮想空間で擬似的にサイバー攻撃を体験できるサイバーレンジを用いた訓練が適している。しかし，既存のサイバーレンジでは，多様なシステムを再現することと，全国各地のSEがオンデマンドで利用することが難しかった。そこで，仮想環境で多様なシステムを再現し，オンラインで時間や場所にとらわれずに学習できるサイバーレンジ，CYBERIUM（サイベリウム）を開発した。

本稿では，CYBERIUMの有用性について述べる。

Abstract

Customers' systems today are constantly exposed to the threat of cyberattacks. To protect customers' business in this age, the response capabilities to minimize the damage in the event of cyberattacks on customers' systems are key. Fujitsu addresses this issue by training security meisters, human resources capable of responding to cyberattacks. To improve response capabilities against cyberattacks, training in a cyber range—a virtual space allowing trainees to experience simulated cyberattacks—is useful. With existing cyber ranges, however, it was difficult to reproduce various systems and for systems engineers in various parts of the country to use them on demand. Accordingly, we have developed CYBERIUM, a cyber range in which various systems can be reproduced in a virtual environment where trainees can learn online without time or location constraints. This paper describes the usefulness of CYBERIUM.

1. まえがき

近年，企業ではサイバー攻撃への懸念が高まっており，様々なセキュリティ対策を実施している。それにも関わらず，被害を受ける企業は増加している。[(1)] サイバー攻撃を受けたときは，被害を最小限に抑えるための対応を正しく選択するスキル，すなわちサイバー攻撃への対応力が必要となる。しかし，サイバー攻撃への対応力を身につけることは難しい。サイバー攻撃は，システムのOSやミドルウェアの種類，システム構成，運用の実態に合わせて手法が巧妙化している。そのため，システムで何が起きているかを特定し，有効な対策を講じる必要があるが，あらかじめ決められた手順の対応だけで被害を抑制できるとは限らない。セキュリティ対策とサイバー攻撃の手法に対する知見や，限られた時間と環境の中で臨機応変に対応できるスキルが求められる。

富士通では，サイバー攻撃への対応力を身につけた人材をセキュリティマイスターとして育成および認定している。[(2)] セキュリティマイスターの育成には，全国各地で活動するSEが，お客様の環境で起こり得るサイバー攻撃を体験できる場が必要となる。そこでお客様の環境を柔軟に再現でき，オンラインで遠地からでも学習できるサイバーレンジCYBERIUM（サイベリウム）を開発した。

本稿では，既存のサイバーレンジの特徴をまとめた上で，開発したCYBERIUMのポイントを述べる。

2. サイバーレンジに求められる要件

何かを学ぶためには，体験しながら実践を重ねていくことが最も効果的である。体験することが困難な事象への対応を学ぶためには，シミュレーターを使用してその事象を疑似体験することが有効である。例えば，ドライブシミュレーター，フライトシミュレーター，月面活動シミュレーション，軍事通信シミュレーションシステムのようなシミュレーターが実用化されており，様々な分野で活用されている。

サイバーセキュリティ分野のシミュレーターには，サイバーレンジがある。サイバーレンジは，国家間のサイバー戦争に対応できるサイバーセキュリティの専門家を育成するための軍事用途を起源としており，国防としてサイバーセキュリティに力を入れているイスラエルや米国で発展した。富士通でも既存のサイバーレンジの活用を試みたが，以下の二つの点でセキュリティマイスターを育成する用途には適していないことが分かった。

(1) お客様システムの再現が困難

既存のサイバーレンジでは，平均的な企業の社内ネットワークを再現した仮想環境で訓練を行う。そこでは，高度で緻密に設計された演習シナリオに基づくサイバー攻撃が行われ，そこで起きる事象とその対応を学ぶことができる。この体験は非常にリアリティがあるが，一つの演習シナリオを整備するためには相応の費用と時間が掛かる。そのため，その種類は限られており，カスタマイズも難しい。

富士通は，様々な業種のお客様のシステムを構築・運用している。対象となるシステムは，事業やサービス用途から社内用途と幅広い。セキュリティマイスターを育成するためには，このような多様なお客様のシステムに合わせて演習シナリオをカスタマイズする必要がある。しかし，既存のサイバーレンジではそれが難しかった。

(2) 受講環境の整備が困難

既存のサイバーレンジでは，セキュリティの高度な専門知識を有する講師がフォローしながら訓練を行う。そこでは，本物のウイルスに感染している，攻撃ツールをインストールしているなど，誤って操作すると危険な仮想マシンを扱うこともある。そのため，外部のネットワークを攻撃しないよう，ほかのネットワークから隔離された仮想環境を使用した集合教育で学習することを前提としている。

富士通は，セキュリティマイスターを育成するための集合教育を，国内の89拠点で活動する全てのSEが受講できる規模で展開しようとした。ところが，ほとんどの地域では，講師や環境，会場の確保，および必要な受講者数を集めることが難しかった。そのため，東京以外では，名古屋と大阪の2拠点での開催にとどまっていた。

以上のことから，既存のサイバーレンジは，セキュリティマイスターの育成には不向きであること

が判明した。

3. CYBERIUMによる解決

富士通では，サイバー攻撃への対応力を備えたセキュリティマイスターを育成する独自のサイバーレンジCYBERIUMを開発した。開発に当たっては，以下の要件を定義して取り組みを開始した。

・お客様の多様なシステムを再現した仮想環境と演習シナリオで学ぶことができる。
・講師が居なくても学ぶことができる。
・オンラインで安全に学ぶことができる。

本章では，CYBERIUMの特長的な機能について述べる。

3.1 入れ替え可能なチャプター

既存のサイバーレンジでは，複雑で大規模な演習シナリオに合わせた仮想環境を構築する必要がある。このため，お客様の多様なシステムを再現するには膨大な費用と時間が必要であった。そこで，CYBERIUMでは演習シナリオを複数の小シナリオであるチャプターに分割するとともに，チャプター同士を入れ替えられるようにした（図-1）。

チャプターに分割することによって，最小限の構成を持つチャプターを複数組み合わせて複雑な演習シナリオの構成が可能になる。これによって，お客様のシステムで起こり得る様々なサイバー攻撃を再現できる。

また，チャプターのインターフェースを統一させることによって，演習シナリオのチャプターをほかの演習シナリオのチャプターと入れ替えて再利用することが容易になった。このことは，演習シナリオを整備するための時間短縮にもつながる。

例えば，メールサーバとWebサーバの両方をLinuxで構築しているお客様と，メールサーバはLinuxだがWebサーバはWindowsで構築しているお客様がいたとする。前者のシステムを担当するセキュリティマイスターには，Linuxで構築したメールサーバを用いたチャプターとLinuxで構築したWebサーバを用いたチャプターを組み合わせた演習シナリオを提供する。一方，後者のシステムを担当するセキュリティマイスターには，メールサーバのチャプターは変更せずに，Webサーバのチャプターのみを Windowsで構築したチャプターに差し替えた演習シナリオを提供できる。

3.2 直観的なユーザーインターフェース

CYBERIUMは，それぞれのチャプターの中で仮想環境とオンライン教材をひも付けて管理している。これによって，ユーザーが学習している仮想環

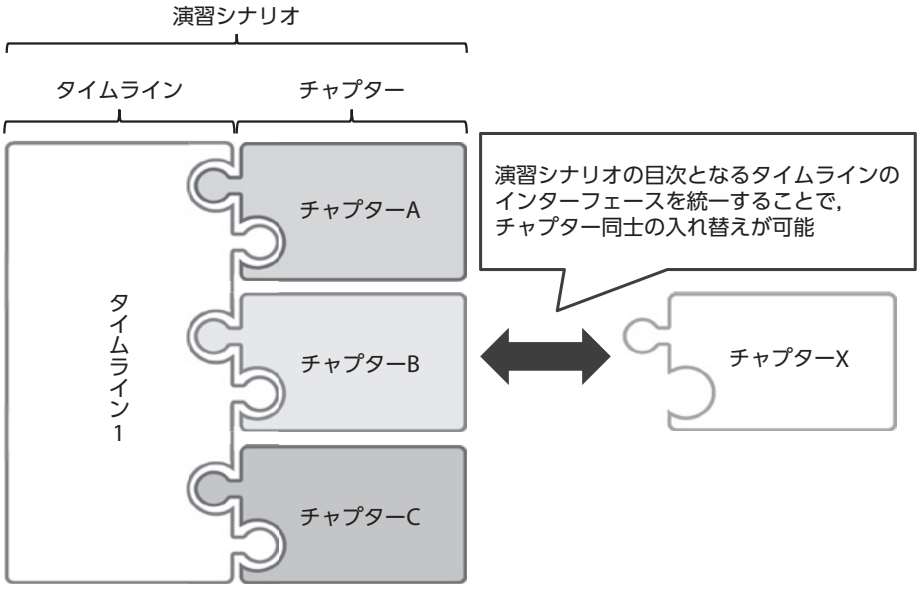

図-1　CYBERIUMにおける演習シナリオの構成

境において必要な学習内容を必要なタイミングで表示できるため，ユーザーが次に何をすれば良いのか，操作した結果のどこに着目すれば良いのかをきめ細やかに誘導できる。

また，ユーザーは演習の状況に合わせて仮想環境にオンライン教材をオーバーレイ表示させたり，不要な場合はオンライン教材を隠したり，これらの要素の大きさを変えたりすることができる。更に，ユーザーが演習を進める中で仮想環境へのアクセスを要求すると，CYBERIUMが発行するユーザーアカウントごとに用意した専用の仮想環境のコンソール画面を提供するようにした。これによって，同じ仮想環境の中にある複数の仮想マシンをメニューから切り替えられるようになり，ユーザーは今どの仮想マシンを操作しているかひと目で分かる（図-2）。

CYBERIUMのインターフェースの開発は，富士通デザイン株式会社の協力を得て，ユーザーの行動や体験を重視したユーザーエクスペリエンスを採り入れた。これによって，ユーザーがストレスなく，モチベーションを維持しながらサイバー攻撃への対応を学べるようになった。

3.3 隔離されたネットワークへの安全なアクセス

遠地から学べるようにするには，仮想環境をオンラインで操作することと，ほかのネットワークから隔離することの両立が必要になる。これは，演習で扱うウイルスや攻撃を誤って流出させてしまうと，外部のシステムに被害を与えてしまうリスクがあるためである。また，ユーザーがVPN（Virtual Private Network）を使って仮想環境へアクセスする場合，ユーザーのパソコンがウイルス感染や攻撃を受けてしまうリスクがある。

このようなリスクを防ぐための技術として，画面転送によるVDI（Virtual Desktop Infrastructure）がある。VDIでは，クライアントは画面情報を受信し，キーボードや操作情報を送信することで仮想マシンを操作する。

通常，VDIではVDIのユーザーと仮想マシンのユーザーは同一のユーザーアカウントを使用する。つまり，VDIのログイン認証で使用したユーザーアカウントが，そのまま仮想マシンのログインにも使用される。しかしこの方法は，1台の仮想マシンだけにアクセスする用途では有用であるが，1台の仮

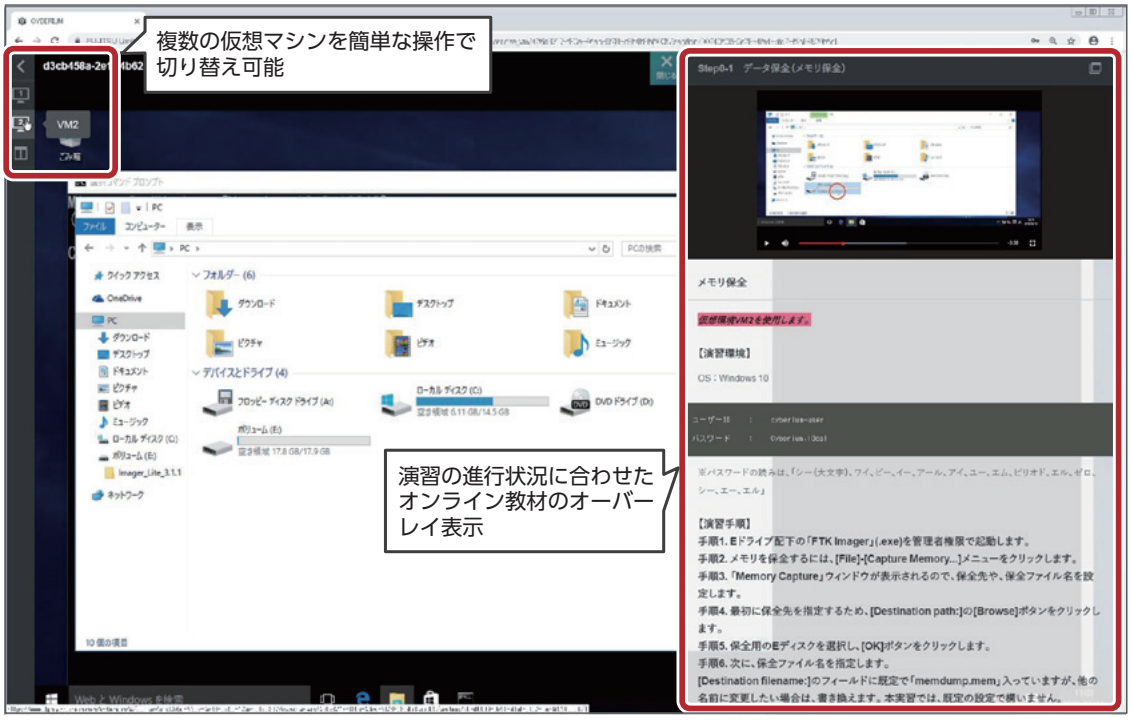

図-2　CYBERIUMのインターフェース

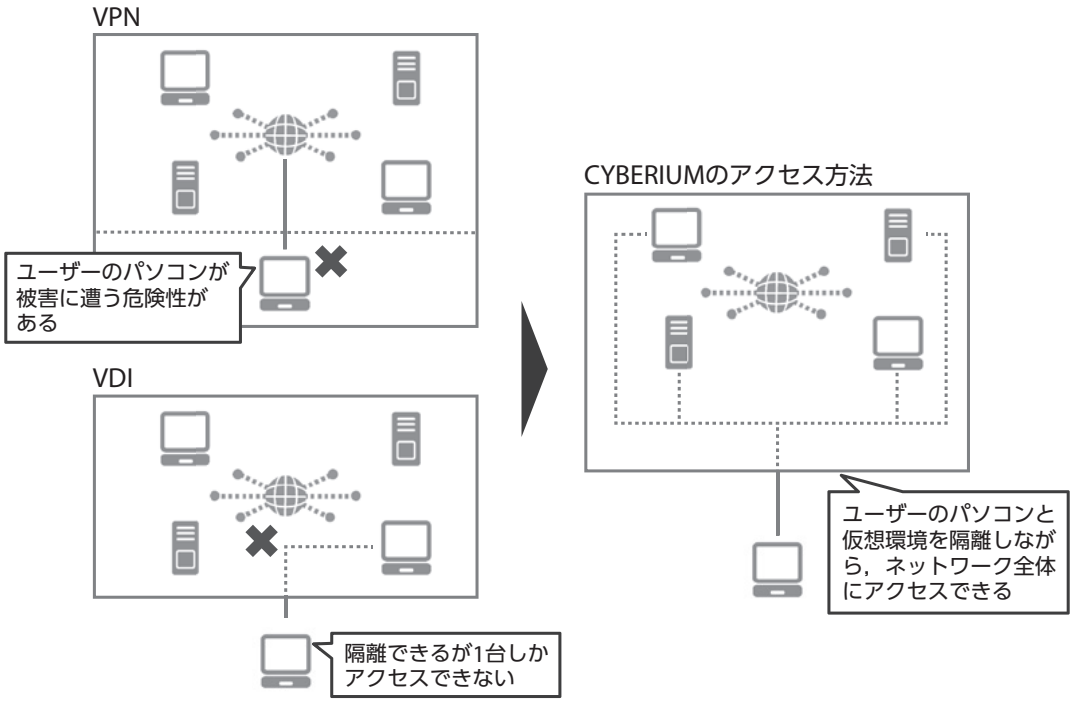

図-3　仮想環境へのアクセス方法

想マシンで複数のアカウントを扱ったり，複数の仮想マシンを扱ったりする場合には不向きである。

そこで，ネットワークに接続された全ての仮想マシンに対するコンソール接続を，一つの画面からアクセスできるようした（図-3）。これによって，ユーザーはネットワークにアクセスしながら，隔離された仮想環境を安全に操作できる。

4. CYBERIUMの効果

CYBERIUMでは，再現できるシステムを増やすために，演習シナリオを構成するチャプターを充実させる取り組みを進めている。

2018年6月からの半年間で，350人がCYBERIUMを用いてサイバー攻撃の対応演習を学習し，サイバー攻撃への対応力を備えたセキュリティマイスターとして認定されている。また，このうち100人は遠地の拠点から受講しており，これまで育成が難しかった地域で活動するセキュリティマイスターの認定にもつながっている。

演習以外の取り組みでは，セキュリティのスキルを問うクイズ形式の問題をチャプターとして構成し，サイバー攻撃の対応力を測るセキュリティコンテストの開催が挙げられる。教育とは異なる形態のイベントを開催することで，新たな人材を発掘するという副次的な効果も得られた。

2018年10月に開催したセキュリティコンテスト[3]では，2週間の開催期間を通じて富士通グループ全体で530人が参加し，このうち120人はセキュリティマイスターではない新たな人材であった。

5. むすび

本稿では，サイバー攻撃への対応力を備えたセキュリティマイスターを育成する取り組みとして，富士通が独自に開発したサイバーレンジであるCYBERIUMの特長について述べた。

富士通では，セキュリティマイスターを2021年度までに1万1,000人体制にすることを計画している。[4] CYBERIUMの活用によって，この計画を着実に進め，お客様のあらゆるシステムをセキュリティマイスターが守ることのできる体制を整える。今後もCYBERIUMの更なる強化を図り，お客様の安心・安全を支えるパートナーとなれるよう貢献し

ていきたい。

参考文献

(1) 総務省：平成30年版情報通信白書.
http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h30/html/nd252130.html
(2) 富士通：セキュリティマイスター.
http://www.fujitsu.com/jp/solutions/business-technology/security/secure/concept/security-meister/
(3) 富士通クラウドテクノロジーズ：富士通サイバーセキュリティーワークショップ（FCSW）2018参戦記.
https://tech.fjct.fujitsu.com/entry/2018/12/18/095449
(4) 富士通：経営方針進捗レビュー説明会（2018年10月26日実施）.
http://pr.fujitsu.com/jp/ir/library/presentation/pdf/20181026-03.pdf

著者紹介

原　和宏（はら　かずひろ）
富士通（株）
サイバーセキュリティ事業戦略本部
CYBERIUMを中心としたサイバーセキュリティ技術者人材の育成推進業務に従事。

©2019 富士通株式会社