# 仮想化技術により検証精度向上と高効率化を実現するセキュリティー検証用制御システムテストベッド

## Control System Testbed to Improve Accuracy and Efficiency of Security Verification Using Virtualization Technology

丸地　俊也 MARUCHI Shunya　飯田　康隆 IIDA Yasutaka　金井　遵 KANAI Jun

デジタルトランスフォーメーションの推進に伴い，制御システムも遠隔保守のために外部ネットワークとの接続が必要になるなど，その運用形態が変化してきている。このような中，サイバー攻撃に備えて，制御システムのセキュリティー対策の強化が求められている。セキュリティー対策を導入する際は，その有効性の事前検証が不可欠であり，テストベッドと呼ばれる試験環境が用いられる。従来のテストベッドは，コストなどの理由で対象制御システムの一部を用いて構築していたため，実際の構成及び挙動を十分に模擬できないという問題があった。

東芝は，仮想化技術を活用して，仮想空間上に制御システムと同等の構成を実装できる検証用制御システムテストベッドを開発した。任意の時点におけるシステムの状態を記録する機能を備えており，容易に検証前の状態に戻せるので，繰り返しの検証も支障がない。テストベッド上に模擬制御システムを実装して評価を行い，セキュリティー対策の検証に有効であることを確認した。

As digital transformation progresses, control systems are being increasingly connected to external networks for remote maintenance, requiring enhancement of security against cyberattacks. A test environment called a testbed is generally used to verify the validity of security measures before they are incorporated into a control system. However, conventional testbeds cannot fully simulate the configuration and behavior of a control system for cost and other reasons.

To address this problem, Toshiba Corporation has developed a testbed capable of replicating a control system in a virtual space, drawing on its virtualization technology. This testbed can record the internal state of a system at any point of time, making it possible to bring a system back to its state prior to a simulation and thereby iterate simulations. We have used this testbed to simulate a control system and confirmed its effectiveness in incorporating security measures into control systems.

## 1. まえがき

発電所や，ビル，工場などの制御システムは，従来外部ネットワークとは隔離されていたため，セキュリティーについては情報システムほど意識されてこなかった。近年，デジタルトランスフォーメーションの進展などにより，制御システムも遠隔保守やデータ利活用を目的として外部ネットワークに接続する機会が増えている。このような中，サイバー攻撃のリスクは，制御系システムでも高まっており，侵入検知システム（IDS：Intrusion Detection System）や，ホワイトリスト機能といったセキュリティー対策の強化が求められている。

セキュリティー対策を制御システムに導入する際は，その有効性やシステムとの整合性について，模擬的なセキュリティー攻撃による動作検証を行う必要がある。しかし，実際の制御システムを用いた検証はシステムを停止させる必要があり，可用性を損なう懸念がある。そこで，制御システムを模擬したテストベッドの重要性が高まっている[(1)]。

従来のテストベッドでは，実際の制御機器の一部を用いた構成が一般的であり，対象とする制御システムとテストベッドの構成を一致させることが困難であった。このため，テストベッドに含まれない機器の検証ができず，制御システムで不具合が発生する可能性があった。また模擬的なセキュリティー攻撃による動作検証では，システムを攻撃前の状態に復旧させて，同一条件による試験を繰り返す必要がある。しかし，従来のテストベッドではシステム復旧が難しく，十分な検証ができなかった。

こうした問題を解決するため，東芝は仮想化技術を用いて，実際の制御システムと同等の構成を実装し，更に任意の時点のシステム状態を保存することで容易に復旧できるセキュリティー検証用制御システムテストベッドを開発した。ここでは，開発したテストベッドの概要と特長，及びその検証結果について述べる。

## 2. セキュリティー検証用制御システムテストベッド

**図1**(a)に，検証の対象となる制御システムの一例を示す。制御システムは，監視制御機器や，複数の表示機器，メンテナンスサーバー，PLC（Programmable Logic Controller），及び制御対象機器など多くの機器で構成されている。

### 2.1 従来のテストベッド

図1(b)に，従来のテストベッドによる制御システムの概念図を示す。従来のテストベッドは実機を使用していたので，検証対象の制御システムと同等の構成で実装することは導入コストの面で現実的ではなく，検証対象の一部だけで構成される。そのため，例えば検証対象の制御システムとは構成機器の台数が異なり，ネットワーク負荷や，制御周期を同じにできないので，制御システムの全ての機能を検証できないという問題があった。また，検証対象のシステム構成に変更があった際には，テストベッドもそれに合わせて変更する必要があり，一層コストや手間が掛かった。更に，検証の過程で繰り返し実行する模擬的なセキュリティー攻撃により制御機器内データの破損がその都度発生し，テストベッドを正常状態へ復旧させるために再インストールやシステム立ち上げの手間が掛かるという問題もあった。

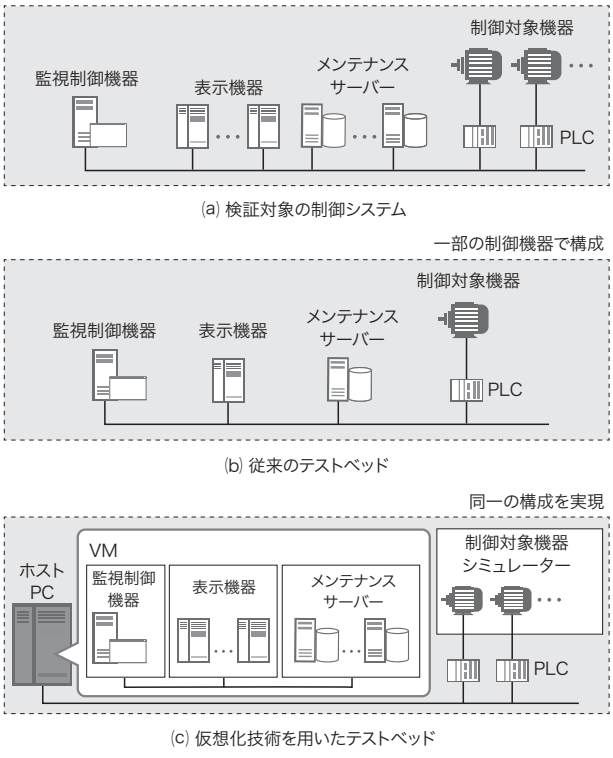



**図1. 従来のテストベッドと仮想化技術を用いたテストベッドの比較**

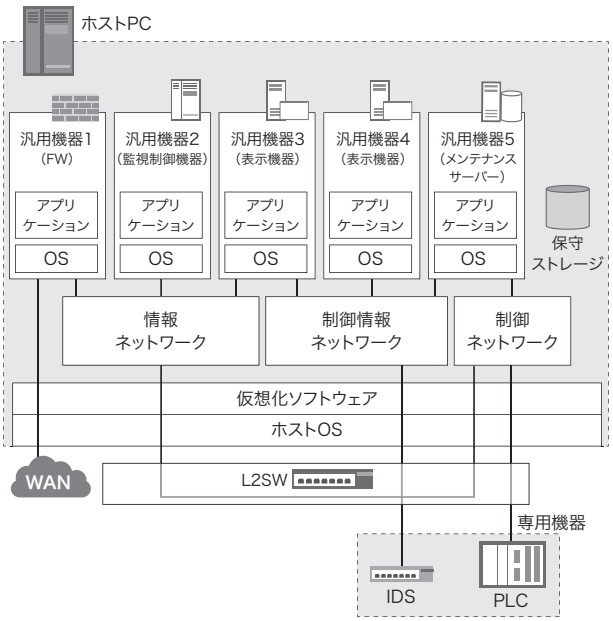
従来のテストベッドは検証対象のシステムの実機を部分的に使用していたので，同等の構成にすることや繰り返して検証することが難しかった。仮想化技術を用いたテストベッドでは制約がないため，検証対象と同等の構成にし，容易に特定の状態に復旧して繰り返し検証を実施できる。

Comparison of conventional testbed and newly developed testbed using virtualization technology

### 2.2 仮想化技術を用いたテストベッド

上記の問題を解決するため，仮想化技術を用いてホストPC（パソコン）上に複数の仮想機器（VM：Virtual Machine）を実装したテストベッドを開発した。図1(c)に，仮想化技術を用いたテストベッドの概念図を示す。検証対象の制御システムのうち，監視制御機器や，表示機器，メンテナンスサーバーなどの汎用アーキテクチャーを持つ制御機器（以下，汎用機器と呼ぶ）を，ホストPC上にVMとして実装している。また，制御対象機器もシミュレーターに置き換えており，これについては3章で述べる。

**図2**に，開発したテストベッドの構成を示す。このテストベッドは，汎用機器をVMとして実装するホストPC，専用アーキテクチャーを持つPLCやIDSなどの制御機器（以下，専用機器と呼ぶ），及びホストPCと専用機器を接続するL2SW（Layer 2 Switch）から構成される。




FW：ファイアウォール　OS：基本ソフトウェア　WAN：広域通信網

**図2. 開発したテストベッドの構成**

ホストPC上に汎用機器やネットワークをVMとして構成し，L2SWを通して専用機器に接続している。

Configuration of newly developed testbed using virtualization technology

VM同士は，ホストPC上に実装した仮想ネットワークを用いて相互に接続されている。仮想ネットワークとして，汎用通信プロトコルが動作する情報ネットワーク，OPC（Object Linking and Embedding for Process Control）-DA（Data Access）など制御用データ通信プロトコルが動作する制御情報ネットワーク，及び産業用プロトコルModbus/TCP（Transmission Control Protocol）やメンテナンス通信プロトコルが動作する制御ネットワークを実装した。これにより，実際の制御システムに用いられる3階層のネットワークを構成可能としている。

また仮想ネットワークにはVLAN（Virtual LAN）機能を実装している。3階層のネットワークは，VLAN機能を用いて論理的に別々のネットワークを構成したまま，ホストPCのEthernet端子経由でホストPC外のL2SWに接続される。専用機器は，L2SWを介して3階層のネットワークにそれぞれ接続できる。

VMはホストPC上にソフトウェアとして実装されるので，VMの台数及び構成はホストPCの処理能力以外の制約を受けない。このため，汎用機器として，実機を用いていた従来のテストベッドでは実現できなかった構成の自由度を提供できる。

また，VMとして仮想ネットワークの対応する通信プロトコルや，プロトコル変換機能を実装している。専用機器は，L2SWと仮想ネットワークのVLAN機能を介して，ホストPC内の任意のVMに接続できる。VMによる構成の自由度と，専用機器とVMとが混在できる仮想ネットワークにより，このテストベッドは実際の制御システムと一致した構成のシステムを，従来に比べて容易に実現できる。

このテストベッドのもう一つの特長として，ホストPC上のVMが，VMの全情報について，保存と復旧の機能を備える点が挙げられる。システムの構成情報や，運用中・停止中・メンテナンス中など制御システムにおける任意の動作状態，その時点でのメモリーやレジスターの状態などの情報をホストPC内の保守ストレージに保存できる。

模擬的なセキュリティー攻撃による動作検証では，制御システムの任意の動作状態において，同一条件による試験を繰り返す必要がある。また，模擬的なセキュリティー攻撃により度々発生する制御機器内データの破損に対して，都度テストベッドの復旧作業が求められる。このテストベッドでは，保存と復旧の機能により，容易に特定の状態に戻せるので，同一条件の試験を繰り返し実施できる。また，破損されたデータも，保守ストレージに保存したデータを用いて，復旧することが可能である。

## 3. テストベッドの有効性検証

### 3.1 制御システムの実装

テストベッドの有効性検証を目的として，テストベッド上に電力系統制御を対象とした遠隔監視制御システムを実装した（**図3**）。

ホストPC上に，VMの汎用機器として，ゲートウェイ機能を持つFW（ファイアウォール），制御対象機器の状態表示及び制御を行うEWS（Engineering Workstation），監視制御を行うSCADA（Supervisory Control and Data Acquisition）サーバー，及びプロトコル変換とPLCのメンテナンスを行うOPCサーバーを実装した。一方，専用機器のPLCには保護リレーの制御や電流値の取得を行う機能を実装した。制御システムは，電流や遮断器の状態を遠隔から監視し，遮断器に対して制御を行う。

セキュリティー検証においては，制御機器が攻撃を受けた際の制御対象機器に与える影響を確認する必要がある。このためテストベッド上に実装した制御システムでは，PLC上にも実機と同様の制御機能を実装している。

また，この制御システムでは，制御対象機器として実機を用いず，代わりにPLC内に制御対象機器の挙動を模擬する制御対象機器シミュレーターを実装している。**表1**にSCADAサーバー，OPCサーバー，PLCに実装した機能を示す。

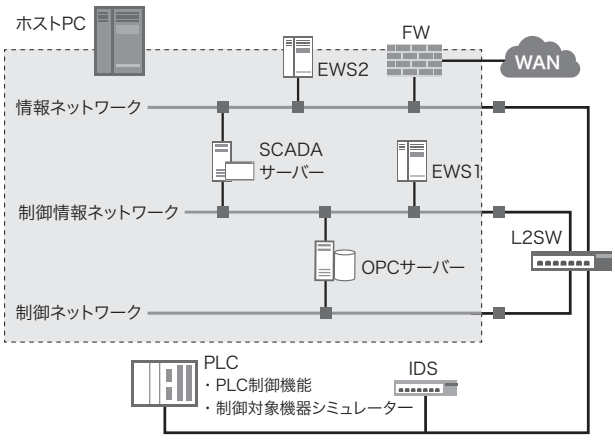



**図3. 検証用にテストベッド上に実装した遠隔監視制御システムの構成**

ホストPC上にEWSやSCADAをVMとして実装し，PLCやIDSといった実機の専用機器も接続して，電力系統制御の遠隔監視制御システムを構成した。

Configuration of remote observation and control system on testbed

**表1. SCADAサーバー，OPCサーバー，及びPLCに実装した機能**

Functions incorporated in supervisory control and data acquisition (SCADA) server, Open Platform Communications (OPC) server, and programmable logic controller (PLC)

| 機器名 | 機　能 |
|---|---|
| SCADAサーバー | 監視制御機能<br>（OPCサーバーとOPC-DAによるデータ送受信） |
| OPCサーバー | PLCメンテナンス機能 |
| PLC | PLC制御機能<br>・比率電流差動リレー機能<br>・自動系統連系・解列機能<br>・需給バランス異常時自動解列機能<br>・電流遠隔監視機能<br>・遮断器遠隔監視・制御機能 |
| | 制御対象機器シミュレーター<br>・保護リレー<br>・遮断器<br>・電流センサー |

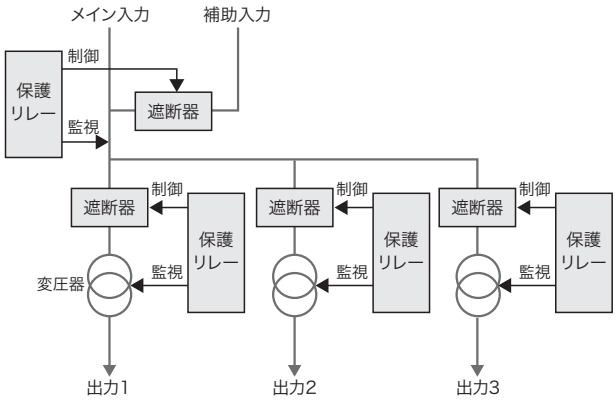



**図4. 変電所内の系統の配線及び機器の構成**

変電所を模擬して，2入力，3出力系統の構成とした。

Configuration of substation system and equipment

**図4**にPLCがシミュレートする変電所内系統の配線と機器構成を示す。各出力系統及び補助入力系統には遮断器が設けられており，遮断器ごとに保護リレーが変圧器などの異常を監視し，異常時には自動的に遮断操作が行われる。また，保護リレーはネットワーク接続されており，遠隔監視制御室で各系統の出力などの状況を監視するとともに，遮断器を制御する。制御システムの状態は，HMI（Human Machine Interface）画面及び各サーバーのログから確認ができる。

### 3.2　検証方法

テストベッド上に実装した制御システムを用いた，セキュリティー対策の有効性検証方法について述べる。

ここではセキュリティー対策として，制御システムに市販

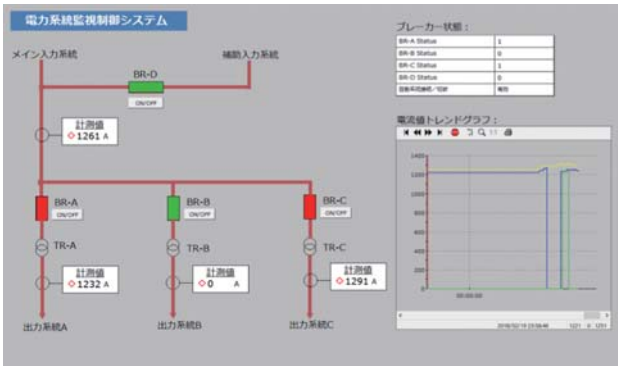



**図5. 電力系統監視用HMI画面**

遮断器の手動制御機能と状態監視機能，トレンドグラフ表示機能を実装したものである。

Human-machine interface (HMI) screen for power system monitoring

のIDSを導入することを仮定した。図2に示すように，IDSは2.2章で説明した情報ネットワーク，制御情報ネットワーク，制御ネットワークそれぞれに接続され，ネットワークに対する攻撃及び侵入を検知する機能を持つ。このIDSは，あらかじめ定常状態の制御システムを流れるパケットを学習し，非定常状態を区別して検出する。

次に，攻撃用PCを用いた模擬的なセキュリティー攻撃による動作検証を行った。攻撃用PCは，ホストPC上に実装されたFWに対して，ネットワークスキャンや不正ログインを繰り返すことで，情報ネットワークから制御ネットワークへ順次侵入を拡大し，最終的にPLCを停止させる多段侵入攻撃を実施した。攻撃結果は，SCADAサーバー上に構築したHMIのグラフィック画面とトレンドグラフ表示，及び攻撃PC上の画面表示で確認した（**図5**）。

### 3.3　検証結果

テストベッド上に実装した制御システムに対し，攻撃PCによる多段侵入攻撃を実施した。情報ネットワークから制御ネットワークへ順次侵入が拡大するのに応じて，IDSが，情報ネットワーク，制御情報ネットワーク，及び制御ネットワークの異常を検知することを確認した。

複数回実施した攻撃検証の中で，各VMは動作状態や権限の不正な変更，バックドアの設置などにより非定常状態に遷移した。検証の都度，テストベッドの備える復旧機能を使用することにより，数分程度で制御システムを正常状態に復旧できた。

これらの結果から，仮想化技術を用いたテストベッドが従来のテストベッドの問題を解決し，実際の制御システムと同

様の構成を実現できること，及びIDSなどのセキュリティー対策の有効性検証に利用できることを確認した。

## 4. あとがき

従来のテストベッドの問題と，開発したセキュリティー検証用制御システムテストベッドの特長，テストベッド上に構築した模擬制御システムの概要について述べ，模擬的なセキュリティー攻撃による動作検証により，開発したテストベッドがセキュリティー対策の検証に有効であることを確認した。

様々な制御システムに対してこのテストベッドの適用を進めることで，従来の検証手法に比べて，制御システムで不具合が発生する可能性をより低減することができる。引き続き，制御システムのセキュリティー確保と利便性拡大の取り組みを進めていく。

## 文　献

(1) 経済産業省．サイバーセキュリティテストベッド構想の概要．制御システムセキュリティ検討タスクフォース（第2回）- 配付資料．<http://www.meti.go.jp/committee/kenkyukai/shoujo/controlsystem_security/002_03_00.pdf>,（参照 2018-05-18）.



丸地　俊也　MARUCHI Shunya
研究開発本部 電力・社会システム技術開発センター
システム制御・ネットワーク開発部
System Control and Network R&D Dept.

飯田　康隆　IIDA Yasutaka
研究開発本部 電力・社会システム技術開発センター
システム制御・ネットワーク開発部
電気学会会員
System Control and Network R&D Dept.

金井　　遵　KANAI Jun, D.Eng.
研究開発本部 研究開発センター
コンピュータアーキテクチャ・セキュリティラボラトリー
博士（工学）　情報処理学会・電子情報通信学会会員
Computer Architecture & Security Systems Laboratory