制御システムのサイバーレジリエンスを向上させるセキュリティ訓練サービス

Security Training Service to Enhance Cyber Resilience of Control Systems

黒田　英彦 KURODA Hidehiko　　大橋　健一郎 OHASHI Kenichiro　　辻　　尚志 TSUJI Hisashi

近年，制御システムでは，汎用プロトコルの適用拡大や情報通信技術の進歩により，サイバー攻撃の脅威が高まっている。制御システムは完全性と可用性の維持が重要であり，サイバー攻撃の防止に加え，攻撃を受けた場合には影響を最小限に抑えて迅速に復旧するレジリエンスが求められる。

東芝グループは，制御システム向けセキュリティ訓練システムを開発し，それを用いたサービスの提供を開始した。訓練は，ロールプレイング方式であり，制御システムのシミュレーターを用いてサイバー攻撃をリアルに体感でき，システム操作や通信データ・ログ解析を組織的に連携して行い，攻撃の検知・分析・対応からシステム復旧までを体験する。攻撃への的確かつ組織的な対応を習得でき，更には，訓練を教育の一つに取り入れることで組織の人材育成に貢献できる。

In recent years, control systems have faced growing threats from cyberattacks along with the spread of general-purpose protocols and advancing information and communication technologies. To maintain the integrity and availability performance of control systems, demand continues to grow for the prevention of cyberattacks, for greater resilience to minimize the effects on control systems, and for rapid recovery when encountering cyberattacks.

The Toshiba Group has developed a security training system for control systems and launched a security training service incorporating the following features: (1) a role-playing method using control system simulators allowing users to realistically experience pseudo cyberattacks, and (2) coverage of cyberattack handling processes, including detection, analysis, countermeasures, and system restoration, while tackling system operations and communication data and log analyses. The service equips users with proper systematic countermeasures against cyberattacks, contributing to training and educating personnel.

1. まえがき

電力などの重要インフラの制御システムは，物理的に分離されたクローズドなネットワークとされ，また独自の通信プロトコルが適用されることが多いため，サイバー攻撃とは無縁とされてきた。しかし，制御システムでの汎用プロトコルの利用拡大や情報通信関連の技術進歩で，サイバー攻撃の脅威が制御システムへ拡大している。この結果，近年では発電システムや石油パイプラインなどの重要インフラでサイバー攻撃の事例が報告されている[1), 2)]。

重要インフラの制御システムでは，システムの稼働を健全に継続して運転する完全性及び可用性が重要である。このため，サイバー攻撃に対して事前に備えて防御し，攻撃を受けた場合にはその被害や影響を最小限にとどめる対応が必要である。更に，一刻も早いシステム復旧が求められる。サイバー攻撃に対してシステムのパフォーマンスを高品質に維持する能力は，サイバーレジリエンスといわれる。

サイバーレジリエンスの概要を**図1**に示す。事前の備えと防御（Prepare領域）では，システムパフォーマンスの最大化とその維持が求められ，セキュリティ対策の製品・技術が有効である。一方，サイバー攻撃によるインシデント発生時（Mitigate領域からRespond & Recover領域）では，被害や影響を最小限にとどめる的確かつ迅速な対応とシステムパフォーマンスの早期復旧が求められ，セキュリティ訓

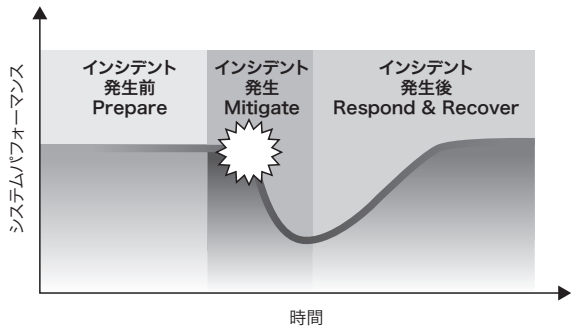

図1. サイバーレジリエンス

インシデントが発生した場合，システムパフォーマンスの低下を最小限にとどめるよう的確に対応し，迅速に復旧する必要がある。

Cyber resilience and security incident response processes

練を通じてサイバーレジリエンスを向上させて維持することが有効である。

セキュリティ訓練の種類には，座学で学習する基礎教育や，ロールに分かれてセキュリティインシデントを体験するロールプレイング方式の演習や訓練，実機での実践演習などがある。

東芝グループは，電力及び社会インフラのシステムとそれらのシミュレーターで製作・納入の実績がある利点を生かし，制御システム向けシミュレーターを用いたロールプレイング方式のセキュリティ訓練システムを開発し，これを用いたサービスの提供を開始した[3]。シミュレーターを用いることで，DoS（Denial of Service）攻撃やランサムウェア（身の代金要求型ウイルス）などのサイバー攻撃をリアルに体感できる。

ここでは，制御システム向けセキュリティ訓練システムと，それを用いたセキュリティ訓練サービスにおける訓練の実施状況について述べる。

2. セキュリティ訓練

送配電システムや遠隔の監視制御システムに関するセキュリティ訓練システムのうち，電力系統システムの例を述べる。

2.1 訓練対象

セキュリティ訓練の訓練対象を**図2**に示す。NIST（米国国立標準技術研究所）のサイバーセキュリティフレームワーク[4]では，サイバーセキュリティにおける要求機能として，全体の統治をベースに，識別・特定から復旧までが要求される。このうち，セキュリティ訓練は，検知・対応・復旧の範囲で，発電部門，系統運用部門や配電部門，工務部門を含めて，経営層のCISO（Chief Information Security Officer，最高情報セキュリティ責任者）からリスク管理部門に至るまでほぼ組織全体が対象になる。

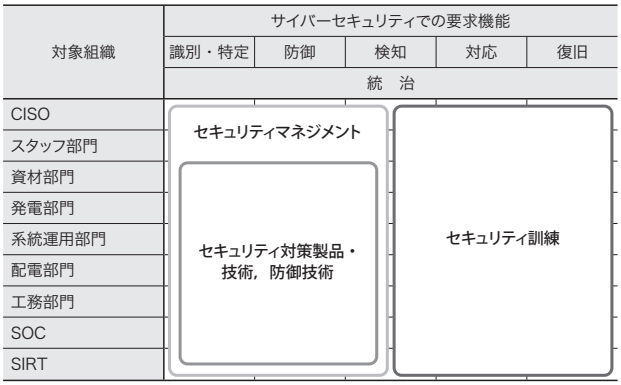

図2. セキュリティ訓練の対象

NISTのサイバーセキュリティフレームワークにおける要求機能へ対応することが重要である。

Security training target divisions

リスク管理部門はSIRT（Security Incident Response Team）と呼ばれ，セキュリティインシデントに対して中心的に対応する専門組織であり，主な役割は以下である。

(1) セキュリティインシデントの検知・対応
(2) 被害の拡大防止，システム復旧
(3) 情報収集・分析
(4) 報告・関連部門との連携
(5) フォレンジック(注1)対応

また，情報システム部門はSOC（Security Operation Center）とも呼ばれ，制御システムやそのネットワークの監視を担当する。サイバー攻撃やセキュリティインシデントを検知し，その解析を行う。

2.2 訓練システム

2.2.1 システム構成

訓練システムの構成を**図3**に示す。訓練システムはサーバー・クライアント方式で構成した。訓練サーバーでは，訓練対象となる制御システムのシミュレーターソフトウェアが動作する。クライアントPC（パソコン）は，運用部門（系統運用部門，配電部門など），SOC，SIRT，及び訓練シナリオの実行やサイバー攻撃を行うシミュレーター操作担当で構成する。なお，運用部門，SOC，SIRTは，実際を想定してそれぞれ異なる部屋に配置する。

シミュレーター操作担当は，訓練シナリオに従って制御システムのシミュレーターを運転し，実際の攻撃者の視点に

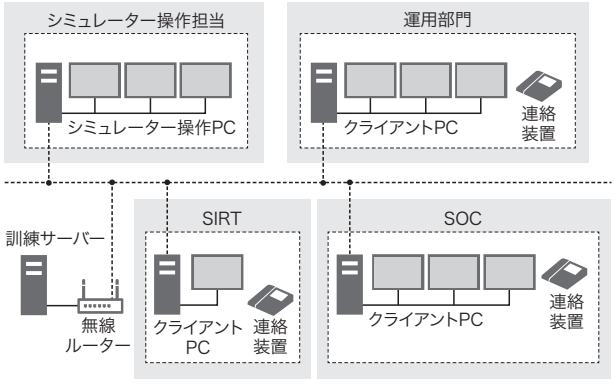

図3. セキュリティ訓練システムの構成

東芝グループのシステムは，訓練サーバーに実装するシミュレーターを変えることで，目的とする制御システムの訓練に対応できる。

Security training system configuration

（注1） セキュリティ事故に対して，原因究明のため，コンピューターに残された証拠を調査すること。

立って制御システムに模擬的なサイバー攻撃を行う。訓練では，レッドチームと呼ばれる。

これに対して運用部門は，シミュレーター上で動作する制御システムの監視制御を行い，サイバー攻撃の検知・対応を行う。SOCは，制御システムのネットワークにおける通信情報を模擬したログデータを得ることができ，このログデータを分析する。SIRTは，訓練で作成される報告書や記録などに関する時刻情報を正確に管理することを目的としてネットワークに接続している。なお，運用部門，SOC，SIRTなどは訓練では，ブルーチームと呼ばれる。

2.2.2　シミュレーター

運用部門が監視制御するシミュレーターの系統図画面の例を**図4**に示す[5]。運用部門は，系統図画面内の変電所や発電所について状態監視及び機器操作を行う。設備が監視のしきい値を逸脱した場合は警告を表示し，また系統での事故発生時には警告音を発する。運用部門は，警告表示や警告音，系統図画面やメッセージ画面の情報，更には保護リレー動作の有無などから状況を判断し，必要な対応を検討して機器を操作する。

一方，シミュレーター操作担当は，シミュレーター上の制御システムにサイバー攻撃を行う。具体的には，監視情報・操作指令の改ざんや，監視制御の不能化，更にランサムウェアなどによる機能不全，などが可能である。攻撃は，系統図画面内の設備の異常動作やメッセージとして系統図画面に現れる。

2.2.3　ネットワーク通信ログの生成機能及び検知・分析

訓練システムは，制御システム内で想定されるネットワーク通信の状態を模擬して，ログデータを生成する機能を備えている。そしてサイバー攻撃を行った場合，その攻撃による一連の通信パケットを模擬したデータをログデータへ付与する。ログデータから，攻撃による通信パケットを検知した画面を**図5**に示す。画面は，IDS（Intrusion Detection System：侵入検知システム）のアラート検知を示している。図5で左側のNetwork logが検知された通信パケットであり，右側のAlertがその通信パケットに関するアラート内容である。SOCは，アラート内容や，その通信パケットのIP（Internet Protocol）アドレス，ポート番号，などを分析してサイバー攻撃の原因・影響・対応を検討する。

3.　セキュリティ訓練の実施状況

電力系統システムにおけるサイバー攻撃を例に取り，セキュリティ訓練の実施状況を述べる。

訓練時の組織構成は**図6**に示すように，運用部門，工務部門，SIRT，SOC，CISO，ベンダーなどとする。それぞれの訓練受講生が分かれてロールを担当するが，工務部門は訓練主催側が担当する場合がある。工務部門は現地設備を管理保守する部門であるが，訓練では現地設備は必要なく，訓練主催側から工務部門へ訓練シナリオに応じて現地設備の状況を提示する。またベンダーは，訓練対象に含めず，訓練主催側で担当する。

サイバー攻撃による変電所機器の不正制御により停電が発生した場合，運用部門は，停電範囲や，原因と推定される機器の状態確認，これらの時間的な変化，などを系統図画面の監視・操作機能を使って把握する。そして運用部門は，この後すぐに工務部門へ現地確認を依頼し，系統事故や機器故障ではないことを再確認する。これを基に，運用部門はSIRTへサイバーインシデントの可能性と状況を報告する。事故や故障とサイバーインシデントを見極めるノウハウ・スキルは，非常に重要である。

同時にSOCは，IDSのアラート検知によってネットワーク

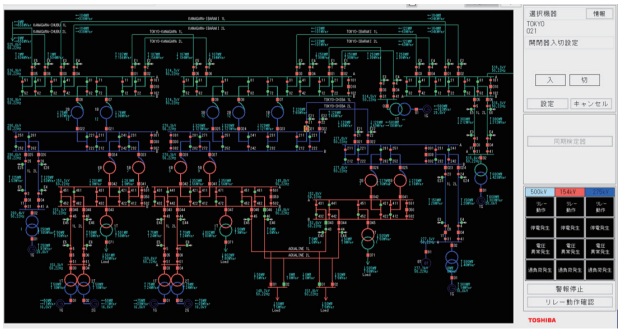

図4.　監視制御する系統図画面の例

シミュレーターソフトウェアは訓練サーバーで動作させ，監視制御画面を運用部門のクライアントPCに表示させる。

Training interface for power system monitoring and control

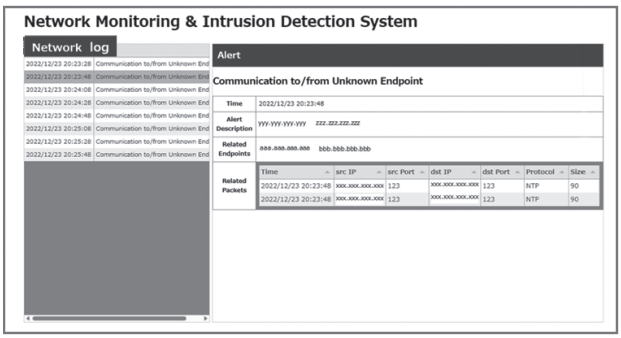

図5.　ネットワーク通信の監視画面

検出した通信パケットとそのアラート内容は，SOCのクライアントPCに表示させる。

Example of network monitoring display at time of alert detection

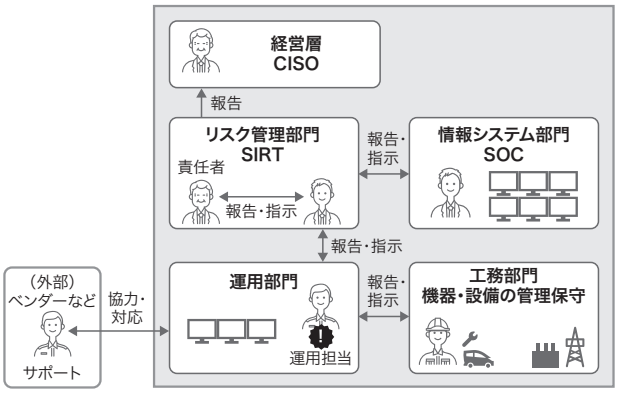

図6. セキュリティ訓練時の組織構成例

組織体制に従って職務分掌を設定し，部門間で連携してサイバーインシデントに対応する。

Example of organizational structure for security training

内に通常では見られない通信パケットを発見し，SIRTへ報告し，かつ，通信パケットの分析を開始する。IDSでは大量の通信パケットが検出される場合が多いため，SOCには迅速かつ的確な分析が求められる。SOCの分析力は，サイバー攻撃の原因や影響を把握するために重要である。

SIRTでは，運用部門及びSOCからの報告を論理的に思考し，サイバーインシデントを判定する。サイバー攻撃が判明した場合，SIRTは運用部門・SOCと協議して対策を決定し，指示を行う。そして対策を実行して，SOCの分析やベンダーのリモート調査によってマルウェアの感染設備を特定し，運用部門が感染設備の除去あるいは隔離を行う。またSIRTは，CISOへ状況報告を行う。状況報告は，SIRTの主要な任務の一つである。このようにSIRTは，サイバーインシデントを判断し，指示・報告する対応力が必要である。

システム復旧策は，SIRT・運用部門が中心となって立案し，SIRTで実施を最終決定する。そして運用部門・工務部門・SOCが連携して実施し，システム復旧を達成する。SIRTのガバナンスの下に，組織間でコミュニケーションを取り合いながら協力することが重要である。

ここでは訓練状況の一例を述べたが，シミュレーターを用いた訓練では，図4の系統図画面の例に示す設備を攻撃対象として，いろいろなサイバーインシデントを発生できる。またロールプレイング方式の訓練であり，図2に示す各部門を訓練対象にできるため，それぞれの部門で必要な技術やスキルを習得でき，サイバーインシデントへの効率的でかつ的確な組織連携を学べる。

4. あとがき

制御システムへのサイバー攻撃に対するレジリエンスの向上を目的として，送配電システムや遠隔の監視制御システム向けセキュリティ訓練システムを開発した。制御システムのシミュレーターを用いたロールプレイング方式の訓練であり，サイバー攻撃をリアルに体感でき，またいろいろな攻撃を再現できることから運用部門，SIRTやSOCを中心に実践的かつ効果的な訓練が可能である。

これによって受講生各人がセキュリティに関する技術力や知見を高め，的確かつ組織的な対応力を習得できる。組織内の各部門を訓練対象にできることから，教育の一環として組織の人材育成に広く貢献可能である。

今後も開発を継続し，最新のサイバー攻撃を取り入れたシナリオの追加や難易度が異なるシナリオの拡充を進め，セキュリティの対応力向上，更には人材育成に貢献していく。

文　献

(1) 山田秀和．制御システムのセキュリティリスク分析ガイド補足資料：制御システム関連のサイバーインシデント事例1～2015年 ウクライナ 大規模停電～．情報処理推進機構 セキュリティセンター，2019，18p．<https://www.ipa.go.jp/security/controlsystem/ug65p900000197wa-att/000076755.pdf>,（参照 2025-04-24）.

(2) 福原 聡．制御システムのセキュリティリスク分析ガイド補足資料：制御システム関連のサイバーインシデント事例9～2021年 米国最大手のパイプラインのランサムウェア被害～．情報処理推進機構 セキュリティセンター，2021，24p．<https://www.ipa.go.jp/security/controlsystem/ug65p900000197wa-att/000093825.pdf>,（参照 2025-04-24）.

(3) 東芝．サイバーセキュリティ報告書 2025．2025，26p．<https://www.global.toshiba/content/dam/toshiba/jp/cybersecurity/corporate/report/pdf/CyberSecurityReport2025_A3_rev02.pdf>,（参照 2025-07-09）.

(4) NIST. The NIST Cybersecurity Framework (CSF) 2.0. 2024, 31p. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>,（accessed 2025-04-24).

(5) 田中幸太郎，ほか．発電プラント及び電力系統向け運転訓練シミュレータの活用．ヒューマンファクターズ．2024，**28**，2，p.57–62.

黒田　英彦　KURODA Hidehiko
Nextビジネス開発部 GX事業推進室
電気学会会員
GX Business Promotion Dept.

大橋　健一郎　OHASHI Kenichiro
Nextビジネス開発部 GX事業推進室
GX Business Promotion Dept.

辻　　尚志　TSUJI Hisashi
Nextビジネス開発部 GX事業推進室
電気学会会員
GX Business Promotion Dept.