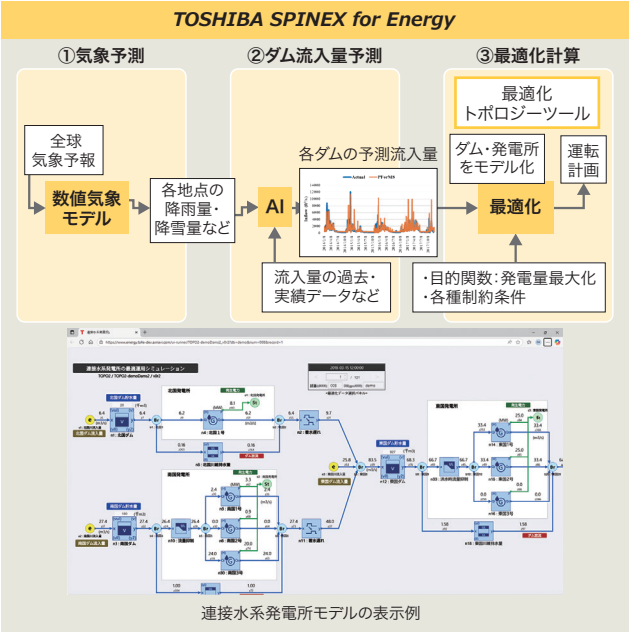
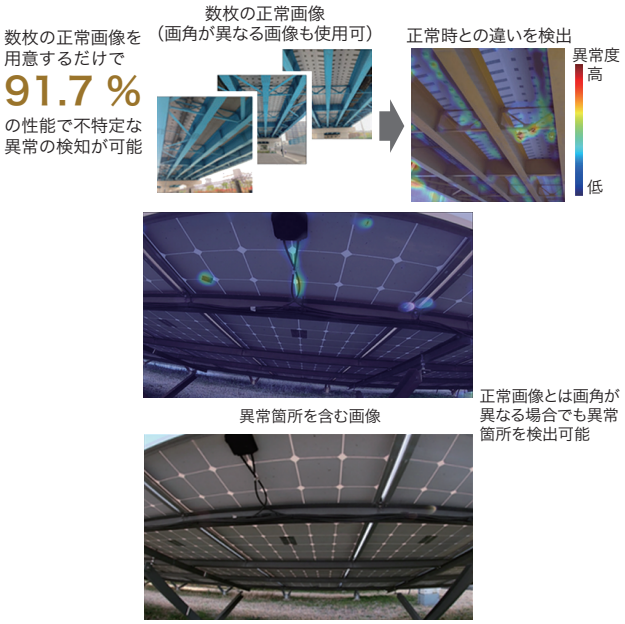
TOSHIBA SPINEX for EnergyのAI機能強化



連接水系発電所モデルの表示例

最適化トポロジーツールの水力発電所への適用事例

Example of application of topology optimization tool to hydroelectric power station



点検画像AI分析サービス

AI-based inspection image analysis service

電力事業者・製造業向けデジタルサービス TOSHIBA SPINEX for Energyは，2024年2月の基本機能リリースの後，2025年3月に新機能の提供を開始した。AIを活用したサービスを強化しており，その代表として，エネルギー運用の最適化計算ツール（最適化トポロジーツール）と，点検画像AI分析サービスがある。

最適化トポロジーツールは，発電所の運用計画や工場のエネルギーマネジメントなどの最適化問題を直感的に記述し，最適解を見つけ出すツールである。設備情報や運用課題を基にした計算モデルの作成や，設備の更新・増設に応じた計算モデルの変更を，設備メーカー以外が行うことは難しかったが，新たに顧客自ら実施できる機能を追加した。また，様々な設備を持つ清掃工場の二酸化炭素排出量削減評価なども可能である。更に，水力発電所向けに，気象予測・ダム流入量予測などのAIと組み合わせたサービスも準備している。

点検画像AI分析サービスは，現場の点検画像をAIで分析し，異常箇所を自動検出するサービスである。当社研究所が開発した独自アルゴリズムにより，数枚の正常画像から現場の点検画像の異常箇所を自動検出する。特定条件下で，91.7 %という世界最高精度(注)での異常検出が可能である。

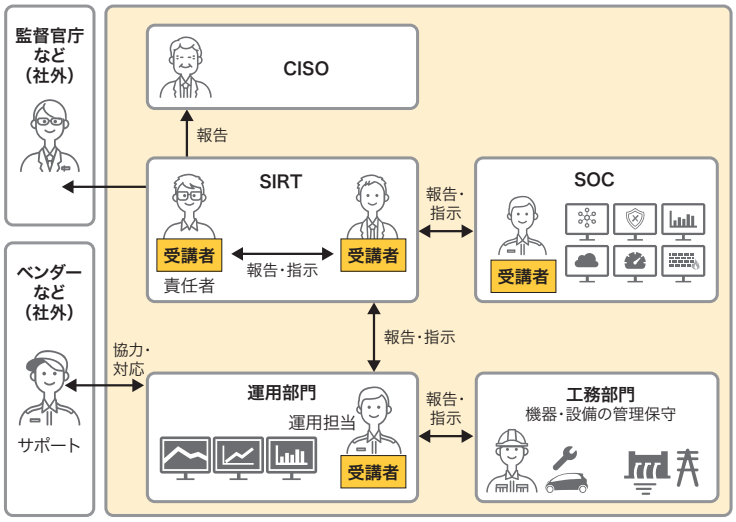
ほかに，様々な業界で広く導入されている株式会社シムトップス製の現場帳票システム i-Reporterとのデータ連携機能や，現場の安全パトロール業務を効率化する機能，Webブラウザーだけで社内外の関係者とセキュアに情報共有できるWebチャット機能などを追加した。また，データ保存周期の細分化（1分周期→1秒周期）など，データ収集・処理の機能も拡充した。

更に，生成AIを活用し，発電プラントに関連する大量の設計・運用ドキュメント群や過去のトラブル対応記録などを基に，新たなトラブル発生時の対応時間を削減する取り組みを試行・検証中である。エネルギー分野以外を含めた技術継承問題の解決手段の一つとして，サービス提供を予定している。

（注）　2022年5月現在，当社調べ。

東芝エネルギーシステムズ（株）

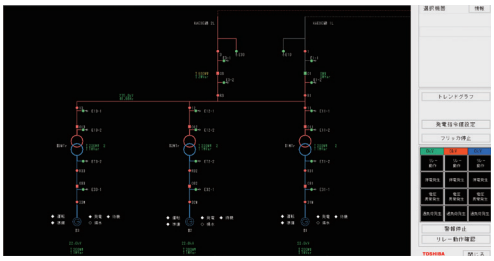
エネルギー事業者用サイバーセキュリティー訓練サービスの適用拡大



CISO : Chief Information Security Officer（最高情報セキュリティー責任者）

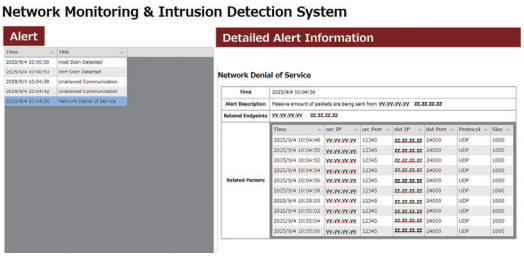
セキュリティー訓練時の組織構成例

Example of organizational structure for security training



再エネ向け訓練での監視制御画面の例

Example of supervisory control interface for renewable energy system cybersecurity training



SOCの調査解析ツールの表示画面例

Example of investigation and analysis tool for security operation centers

近年，制御システムでは，情報通信・デジタル技術の進歩や汎用の通信プロトコルの適用拡大により，サイバー攻撃の脅威が高まっている。制御システムへの攻撃を未然に防止することが重要であるが，攻撃を受けた場合にはその影響を最小限に抑えるとともに，迅速にシステム復旧することが求められる。これに対応するため，当社は，制御システムへのサイバー攻撃に備えるセキュリティー訓練サービスを提供している。今回，電力系統や発電システムを対象とした訓練サービスに加えて，重要性が高まる再生可能エネルギー（以下，再エネと略記）分野での訓練サービスを開始した。

訓練は，シミュレーターを用いたシナリオベースのロールプレイング方式で行う。受講者は，運用部門，リスク管理部門（SIRT：Security Incident Response Team），情報システム部門（SOC：Security Operation Center）を担当し，SIRTが運用部門及びSOCを統括してサイバー攻撃の検知・認識から対応・復旧までを体験する。シミュレーターを用いることで，攻撃時の現地機器の状態・挙動を正確に再現できる。これは特に，水力発電のように遠隔・無人で運用され，現地機器の直接確認に時間を要する場合にも実践的な訓練が可能となり，運用部門は，事故・故障・サイバー攻撃を迅速に判断する能力を習得できる。SOCは，侵入検知システムの警報，通信データ・サーバーログの調査解析を通して，多様なログや通信パターンから異常を判定する分析スキルや，大量のログを迅速かつ的確に処理・判断する能力を習得できる。

当社は，セキュリティー訓練を人財育成の教育カリキュラムとして体系的に提供しており，受講者はサイバー攻撃に対する的確かつ組織的な対応能力を向上させることができる。今回新たに，訓練対象の部門ごとに訓練での評価指標を作成し，必要な対応能力を定量的に評価する仕組みを導入した。PDCA（Plan-Do-Check-Act）サイクルを活用し，難易度や攻撃手法が異なる訓練シナリオを段階的かつ継続的に実施することで，評価指標に沿って受講者の対応能力の向上を支援する。当社は，今後もエネルギー事業者の人財育成に貢献していく。

関係論文：東芝レビュー，2025，80，4，p.16–19.

東芝エネルギーシステムズ（株）