OTセキュリティをワンストップで実現する統合コンサルティングプロセス手法

Integrated Consulting Process Development Method to Provide Customers with One-Stop OT Security Solutions

源島　朝昭 GENJIMA Tomoaki　　村田　　敦 MURATA Atsushi　　伊波　　俊 IHA Shun

製造業や社会インフラの設備であるOT（制御・運用技術）システムは，耐用年数を迎えたレガシー機器や，独自プラットフォームの利用，通信の可視性の欠如，システムの可用性や安全性の確保，及びセキュリティ規制厳守といった，OTシステム固有のセキュリティ上の制約がある。そのシステムのライフサイクル全体を通じて，効率的・効果的にセキュリティ対策を講じるための体系的な方法論が，これまで確立されていなかった。

そこで，東芝グループは，OTシステムにおける高度な制御技術と豊富な運用実績を基に，リスクアセスメントからセキュリティソリューションの導入・運用に至るまでを，体系的にワンストップで提供できるOTセキュリティの統合コンサルティングプロセス手法を開発した。この手法は，顧客への依頼事項や入出力用のテンプレート・サンプル文書，及びモデリング手法を提供することで，顧客のシステムに最適なOTセキュリティを導入し，持続的な安定運用を可能にする。

In production facilities and the social infrastructure domain, operational technology (OT) systems are subject to specific security restrictions including utilizing legacy equipment reaching the end of its service life, specific platforms, limited communication visibility, ensuring system availability and safety, and strict compliance with security regulations. However, there has previously been no established systematic methodology to efficiently and effectively implement security measures throughout the life cycle of OT systems.

With this in mind, the Toshiba Group has devised an integrated consulting process development method to systematically provide customers with a one-stop solution from risk assessment to security introduction and operation by making full use of its high-level control technologies cultivated through experience in OT system development and operations. This method makes it possible to introduce optimal OT security measures into existing systems using templates and sample documents to fill in requests to customers, and via modelling methods, helping achieve sustainable, stable system operations.

1. まえがき

DX（デジタルトランスフォーメーション）の推進に伴い，製造業の生産設備や社会インフラの設備であるOTシステムは，サイバー空間からのサイバー攻撃の脅威にさらされている。OTセキュリティは，その脅威に対応するために，次の三つの重要な役割を果たしている。

⑴　システム可用性の確保　　サイバー攻撃からOTシステムを防御し，設備の稼働を中断させることなく，安定した稼働を維持する。

⑵　安全性の確保　　OTシステムは，物理的なプロセスを制御しているため，サイバー攻撃が人命や環境に直接的な影響を及ぼすリスクがある。このリスクを，最小限に抑える。

⑶　セキュリティ規制の遵守　　多くの産業分野では，セキュリティに関する規制や標準の遵守が求められる。その対策の導入により，法的リスクを回避する。

このようにOTセキュリティは，OTシステムを保護し，サプライチェーン全体としてレジリエントな社会（危機に直面しても，迅速に回復し，適応する能力を持つ社会）の実現に貢献している。しかし，OTセキュリティを導入する場合，具体的に何から着手するべきか，効率的に効果的なセキュリティ製品やサービスをどのように選択すべきか分からないという顧客の声が多い。

そこで，東芝グループは，顧客に最適化されたOTセキュリティを提供するため，OTシステムのライフサイクル（設計・構築，運搬，運用，保管，廃棄などの総称）全体に関わるセキュリティ業務を分類し，ワンストップで提供できる統合コンサルティングプロセス手法を開発した[1]。開発した手法は，OTシステムのライフサイクルに関わるセキュリティ業務を四つのフェーズに分類し，体系的にワンストップで提供するものである。四つのフェーズは，“リスクアセスメント”，“セキュリティ計画”，“セキュア設計・構築”，“管理・体制・テスト”であり，各フェーズで実施すべき一連の作業プロセスをシームレスにつなぐ。

ここでは，開発した統合コンサルティングプロセス手法の

概要と特長について述べる。

2. 統合コンサルティングプロセス手法の概要

統合コンサルティングプロセス手法は，これまで多種多様なニーズに合わせて培ってきたOTシステムのリスクアセスメントやインテグレーション・運用のセキュリティコンサルティングの実績を基に，その業務を四つのフェーズに分け，それらをワンストップで提供できる（**図1**）。

その特長は，各フェーズを効率的に遂行するため，顧客への依頼事項や入出力用のテンプレート・サンプル文書，モデリング手法を提供している点である。これらは，これまでの社会インフラを中心としたセキュリティコンサルティングの実績を基に作成している。これにより，顧客において，各フェーズで何から着手するべきか，どのような意思決定が必要かといった理解の助けとなる。また，モデリング手法を使った可視化により，関係者間の認識レベルの差が少なくなり，議論が促進できる（**図2**）。更に，各フェーズのステップで得られた出力を次のステップの入力として使用することで，OTセキュリティの導入を効率的に進められる。

次に各フェーズの作業のステップ（(STEP1-1) ～ (STEP4-4)）について述べる。

2.1 リスクアセスメント

フェーズ1のリスクアセスメントでは，OTシステムとそのサプライチェーンのリスクを可視化し，優先するリスクを整理する。作業のステップは次のとおり実施する。

最初に，（STEP1-1）現状把握では，インタビューや既存資料の閲覧を通じて，リスクアセスメントの対象スコープやその業務目的，業務内容，情報資産，既存のセキュリティ対策を洗い出す。

次に，（STEP1-2）資産・構成パターンの分類化では，現状把握でヒアリングした結果に基づき，OTシステムを構成する機器のOS（基本ソフトウェア）やそのバージョン，設置場所といった付帯情報を整理する。

更に，（STEP1-3）リスクアセスメントの実施では，資産・構成パターン分類化の結果を基に，実施目的に応じたリスクアセスメント手法によりアセスメントを実施する[2]。

最後に，（STEP1-4）セキュリティ対策・優先度の整理では，リスクアセスメント結果を基に，リスクの対策優先度の方針を決定し，その方針に従って対策の優先度を決定する。

2.2 セキュリティ計画

フェーズ2のセキュリティ計画では，フェーズ1のリスクアセスメント結果を基に，OTシステムに対するセキュリティポリシーや対策基準の規程類を策定し，PDCA（Plan-Do-Check-Act）サイクルを維持する体制を整備する。作業のステップは，次のとおり実施する。

最初に，（STEP2-1）自主規程類の位置づけ整理では，

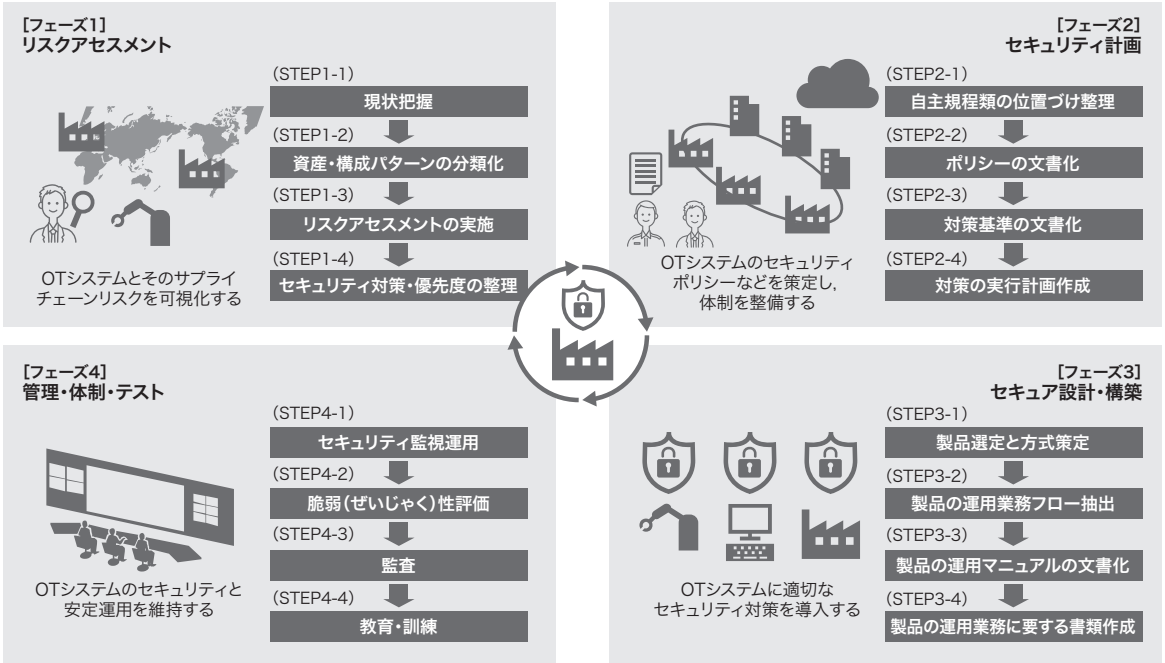


図1. 統合コンサルティングプロセス手法の概要
リスクアセスメントからソリューション導入・運用まで一括提供し，顧客に適したOTセキュリティを実現する。
Outline of integrated consulting process

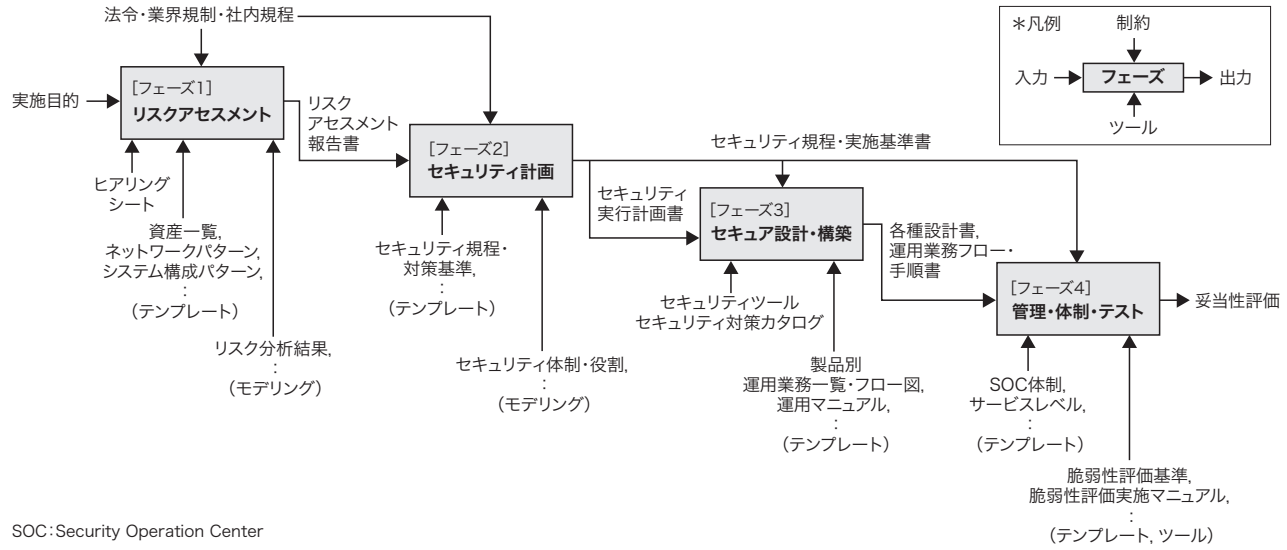


図2. 統合コンサルティングプロセスのモデリングの例

各フェーズの入出力テンプレートや文書サンプルなどを整備することで，確実な施策の実現を図る。

Example of integrated consulting process modeling

新たに文書化するセキュリティポリシーや対策基準が，既存規程にどのように関わるのかを整理する。

次に，(STEP2-2) ポリシーの文書化では，顧客の既存のセキュリティ規程とリスクアセスメント結果を基に，国や業界のセキュリティ規制の要件を整合させ，文書化する。

更に，(STEP2-3) 対策基準の文書化では，ポリシーを実現するための具体的なルールや対策基準を文書化する。

最後に，(STEP2-4) 対策の実行計画作成では，対策基準とリスクアセスメント結果を整合させ，具体的なセキュリティ対策の実行計画書を作成する。その作成時には，対策に掛かるコストや技術難易度，国や業界の規制要求も加味する。

2.3　セキュア設計・構築

フェーズ3のセキュア設計・構築では，OTシステムに適切なセキュリティを導入する。作業のステップは，(STEP3-1) 製品選定と方式策定，(STEP3-2) 製品の運用業務フロー抽出，(STEP3-3) 製品の運用マニュアルの文書化，(STEP3-4) 製品の運用業務に要する書類作成の順に実施する。導入する製品が複数ある場合は，製品ごとに (STEP3-1) から (STEP3-4) を繰り返す。

最初に，(STEP3-1) 製品選定と方式策定では，セキュリティ対策カタログから，OTシステムの制約条件を満たす組み合わせを選択し，その製品の運用を見据えた実現方式を策定する。

次に，(STEP3-2) 製品の運用業務フロー抽出では，そのセキュリティ製品が検知した脅威への対応と，その製品の維持管理に必要な運用業務フローを策定する。

更に，(STEP3-3) 製品の運用マニュアルの文書化では，セキュリティ対策基準書に従い，運用業務フローの遂行に必要な役割と実施内容を定めた運用マニュアルを文書化する。

最後に，(STEP3-4) 製品の運用業務に要する書類作成では，運用マニュアルに従って業務を遂行するために必要なチェックリストや作業報告書などを文書化する。

2.4　管理・体制・テスト

フェーズ4の管理・体制・テストでは，OTシステムのセキュリティと安定運用を維持する。作業のステップは，(STEP4-1) セキュリティ監視運用，(STEP4-2) 脆弱 (ぜいじゃく) 性評価，(STEP4-3) 監査，(STEP4-4) 教育・訓練の順であるが，これらは，それぞれのステップの入出力に因果関係がないため，既存の対策状況から実施順序を定める。ここでは，(STEP4-1) ～ (STEP4-4) の順番で概要を述べる。

(STEP4-1) セキュリティ監視運用は，セキュリティ製品の運用業務フロー内の一業務であり，その作業要員の体制を整備し，ログ監視項目やインシデントのレベルに応じた対応レベルとともに文書化する。

(STEP4-2) 脆弱性評価では，機器の脆弱性評価基準や脆弱性評価実施マニュアル，脆弱性評価報告書を文書化する。

(STEP4-3) 監査では，セキュリティ対策基準に従って対策が実施されているかを，定期的にセキュリティ監査するための体制を整備し，その実施マニュアル類を文書化する。

フェーズ3 セキュア設計・構築の作業の流れ

	(STEP3-1) 製品選定と方式策定	(STEP3-2) 製品の運用業務フロー抽出	(STEP3-3) 製品の運用マニュアルの文書化	(STEP3-4) 製品の運用業務に要する書類作成
主要作業	・最優先となるサイバーセキュリティ対策の製品選定と実現方式を策定	・導入した製品の運用業務一覧と運用業務フローを策定	・導入した製品の運用業務フローにおける詳細を取り決めた運用マニュアルを文書化	・導入した製品の運用業務フローで要するチェックリストや作業報告書などの書類を作成
顧客への依頼事項	・サイバーセキュリティ対策作業の役割調整 ・顧客側の導入計画の社内調整	・運用業務フローのレビュー ・既存の運用業務フローとの整合を調整	・運用業務フローの取り決め文書のレビュー ・既存の運用業務取り決めとの整合を調整	・運用業務フローに要する書類のレビュー ・既存の運用業務書類との整合を調整
入出力・文書テンプレート	・サイバーセキュリティ対策の実現方式	・運用業務一覧 ・運用業務フロー図	・運用マニュアル	・運用書類一式

図3. フェーズ3 セキュア設計・構築の作業の流れの例
顧客への依頼事項や入出力用のテンプレートなどを提供することで，適切なサイバーセキュリティ対策を導入する。
Example of secure design and development work process (phase 3)

また，(STEP4-4) 教育・訓練では，セキュリティ運用体制の役割別の教育定義や訓練の頻度，実施手順を文書化する。

3. 統合コンサルティングプロセス手法の適用例

統合コンサルティングプロセス手法は，その適用がリスクアセスメントから導入・運用まで広範囲に及ぶ。そのため，ここではフェーズ3のセキュア設計・構築フェーズの運用業務に限って適用例を述べる。その例を示す(**図3**)。

フェーズ3の(STEP3-1) 製品選定と方式策定において，ネットワーク型のIDS (Intrusion Detection System：侵入検知システム) の製品を導入する場合の運用業務フローを考える。

IDSは，ネットワーク上に流れる不正な通信を検知し，アラートを通知する機能を備えている。その運用としては，アラートの発生を常時監視し，アラートが発生した場合は，OTシステム運用管理者が原因究明，復旧を行う。アラートの一次分析や，ログの確認と分析を担うのがSOC (Security Operation Center) である。SOCは，一般的に24時間365日対応可能な運用体制を整備しており，システム規模を問わず最新のサイバー攻撃にも対応可能な高度な解析スキルを持つアナリストを保有する。このことからSOCの業務を，外部サービスに委託することが一般的である(**図4**)。

アラート監視とアラート発生時のログ分析は，基本的な運用業務の一つにすぎないが，そのほかにセキュリティ製品の維持管理に要する機器の構成管理や，リリース管理，変更管理などの運用業務もある。これらを最初から検討していては非効率である。よって，これまでのIDS導入・運用実績からベストプラクティスを形式知化した運用業務のテンプレート図などを使用することで省力化する。

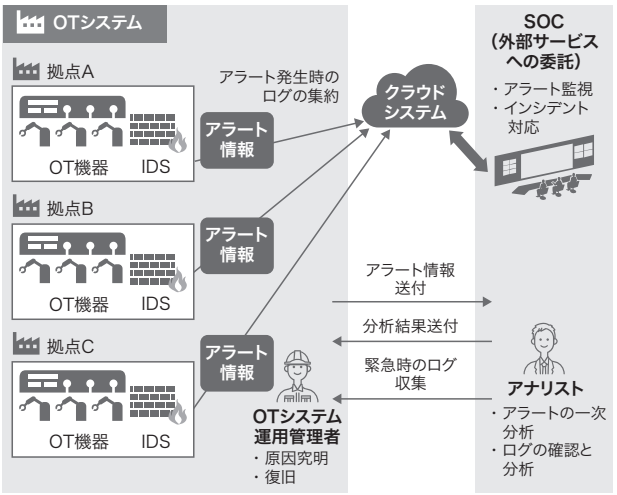


図4. クラウドシステム活用によるIDS製品のセキュリティ監視・運用例
複数拠点を持つOTシステムで，クラウドシステムを活用し，セキュリティ監視・運用をSOCで一元化した例である。
Example of security monitoring and operation of intrusion detection system (IDS) products using cloud computing

図5に，SOCの運用業務一覧とフロー図テンプレートを示す。このように各フェーズで，作業のノウハウが形式知化したテンプレートとしてまとめられていることで，その参照により関係者間の認識レベルがそろいやすくなり，早期の合意形成が得られる可能性が高くなる。これにより効率良くSOCの運用業務導入が進められ，文書化により運用定着化が図れる。

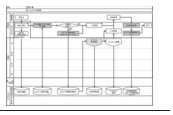
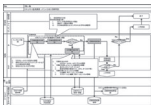
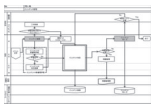
業務名	内　容	フロー図テンプレート
サービスデスク業務	問い合わせに対する初期対応，問い合わせの受け付けと記録，対応記録の管理及びアナリストへの引き継ぎを行う。	
セキュリティ監視業務	アナリストは24時間365日継続してIDSのアラートのモニタリングを実施する。アラートの重大度に応じて調査の優先度を設定し，イベント分析へ移行する。	
インシデント管理業務	インシデントと識別された事象の対応を実施し，インシデントの発生から解消までを適切に管理する。	
⋮	⋮	⋮

図5．SOCの運用業務一覧とフロー図テンプレート

運用業務の役割分担とそのフローを明示することで，効率良い導入と運用定着化を図る。

Tasks of security operation center (SOC) and templates for creating workflow charts

4．あとがき

持続的に安定運用できるOTセキュリティを提供するために，リスクアセスメントからセキュリティソリューションの導入・運用に至るまでを，体系的にワンストップで提供する統合コンサルティングプロセス手法の取り組みについて述べた。多種多様なOTシステムのセキュリティコンサルティングの実績を基に，ナレッジを形式知化したプロセスやツール類を整備することで，効果的なOTセキュリティの導入の効率性やスピードの向上が得られている。更に当該の手法を活用し，検証と改善を繰り返し，法規制の遵守，導入コスト削減，導入期間短縮，運用管理の負担軽減を目的に，随時改良を進めていく。

また，開発した手法の対象は，OTシステムのライフサイクル全体であり，これを俯瞰（ふかん）できるという特長がある。この手法の適用範囲の拡大を図っていくためには，自ら全てを行うのではなく，パートナーとの密接な連携により統合コンサルティングプロセスの改良を進めることが重要である。こうした取り組みにより，持続的に安定運用できるOTセキュリティの実現に貢献していく。

文　献

(1) 天野 隆，ほか．社会インフラや産業システムのCPSを支える東芝グループのサイバーセキュリティサービス・技術．東芝レビュー．2022，**77**，3，p.2–6．<https://www.global.toshiba/content/dam/toshiba/jp/technology/corporate/review/2022/03/a02.pdf>，（参照 2025-04-01）．

(2) 源島朝昭，ほか．CPSのセキュリティを担保するリスクアセスメント手法．東芝レビュー．2022，**77**，3，p.29–33．<https://www.global.toshiba/content/dam/toshiba/jp/technology/corporate/review/2022/03/a08.pdf>，（参照 2025-04-01）．

源島　朝昭　GENJIMA Tomoaki
東芝デジタルソリューションズ（株）
デジタルエンジニアリングセンター 制御セキュリティ事業推進部
Toshiba Digital Solutions Corp.

村田　　敦　MURATA Atsushi
東芝デジタルソリューションズ（株）
デジタルエンジニアリングセンター 制御セキュリティ事業推進部
Toshiba Digital Solutions Corp.

伊波　　俊　IHA Shun
東芝デジタルソリューションズ（株）
デジタルエンジニアリングセンター 制御セキュリティ事業推進部
Toshiba Digital Solutions Corp.