「OT サイバーセキュリティの原則」に基づくチェックリスト

国際文書「OT サイバーセキュリティの原則」の内容を抜粋し、チェックリストを作成しました。
自組織の OT セキュリティ対策が 6 つの原則に沿っているかを点検する際などに、参考としてご活用ください。

項番	チェック項目	実施状況
原則 1：安全が第一		
1-1	OT 環境に導入されているサイバーセキュリティシステム、プロセス、サービスは、障害時でも予測可能・管理可能であるか	
1-2	エンジニアはシステムの弱点を深く理解しているか	
1-3	OT 環境に導入されているサイバーセキュリティシステム、プロセス、サービスはブラックスタート（完全に電力が失われた場合でも、他のシステムへの最小限の依存で遅滞なく運用および復旧できる）に準拠しているか	
原則 2：ビジネスの知識が重要		
2-1	組織が重要なサービスを継続的に提供するために不可欠なシステムやプロセスを特定し、保護しているか	
2-2	OT システムの設計、運用、保守の責任者は、OT システムに接続されている物理的な設備とプロセス、および OT システムが利害関係者にサービスを提供する方法など、OT システムが動作するビジネスコンテキストを理解しているか	
2-3	OT サイバーセキュリティ担当者は、プラントの操業に関する実用的な知識を持ち、物理プラントを担当する組織内の担当者との実務的な関係を維持しているか	
2-4	OT 固有のインシデント対応計画および手順書が、組織のその他の緊急・危機管理計画、事業継続計画、手順書および必須のサイバーインシデント報告要件と統合されているか	
2-5	全てのインシデント対応計画、手順書、第三者向けの情報パッケージは、定期的に実行され、法務を含む全ての関係者によって更新され、保護されているか	
原則 3：OT データは極めて貴重であり、保護する必要あり		
3-1	重要な OT データ（ネットワーク構成図、動作シーケンスに関する文書、論理図、回路図などの技術的構成データや、組織の活動・OT システムの機能を推定可能な電圧の一時的データなどを含む）の保存場所・保存方法を定義・設計しているか	
3-2	外部ネットワークが OT からデータを取得するのではなく、OT ネットワークから外部にデータをプッシュする形になっているか	

3-3	OT データが閲覧または流出したときに警告が発せられるようになっているか	
3-4	デフォルトのパスワードが変更された場合は、失敗したログイン試行をキャプチャして調査する方法があるか	
原則 4：OT を他のネットワークから分離・隔離する		
4-1	OT ネットワークは、インターネットおよび IT ネットワークからセグメント化して分離されているか	
4-2	ベンダーから OT ネットワークを保護し、制限しているか	
4-3	安全性に不可欠なものなど、より重要な OT ネットワークを、それほど重要でない OT ネットワークから分離しているか	
4-4	OT ネットワークを、同業者や上流・下流の OT ネットワーク・サービスから保護し、制限しているか	
4-5	OT 環境におけるネットワークセキュリティ、認証・アクセス制御、仮想化、バックアップなどの管理・運用のシステム・サービスは、IT から適切に分離されているか	
原則 5：サプライチェーンは安全でなければならない		
5-1	OT にアクセスできる、機器やソフトウェアのサプライヤー、ベンダー、マネージドサービス プロバイダー（MSP）向けに、サプライチェーンのセキュリティを保証する施策・制度はあるか	
5-2	プリンター、ネットワーク機器、RTU、HMI、EWS 等を含むあらゆるデバイスのサプライチェーンが考慮されているか	
5-3	相互接続がある場合や、OT が正しく機能するために必要なシステム（ビル管理システム、空調、消火システムなどを含む）がある場合、それらのサプライチェーンも考慮されているか	
5-4	デバイスのファームウェアのアップデートにおいて、ファームウェアが信頼できる場所から受信され、暗号署名され、署名がチェックされていることを確認しているか	
5-5	ファームウェアの更新、設定の変更、ライセンス更新などにおいて、ベンダーが OT サイバーセキュリティの原則を破ることを要求する場合、ベンダーのセキュリティの成熟度に対してネガティブな評価をしているか	
原則 6：OT のサイバーセキュリティには人材が不可欠		
6-1	OT サイバーセキュリティの実践のために、さまざまなバックグラウンド、スキル、知識、経験、セキュリティ文化を持つ人材（インフラチーム、サイバーセキュリティチーム、制御システムエンジニア、現場の運営担当者、資産管理者など）の組み合わせが行われているか	
6-2	エンジニアリングの背景を持たないチームメンバーが、「安全が第一」などの OT の考え方・課題を理解しているか	

6-3	サイバーの安全性に関する観察力を高めるプロセスを導入し、観察力が評価される文化を醸成しているか	
6-4	安全性評価、工場受入試験（FAT）、サイト受入試験（SAT）、およびエンジニアリング変更管理プロセスにサイバーセキュリティに組み込んでいるか	
6-5	運用上の障害が特定された場合、サイバー侵害の可能性を考慮するよう現場のオペレーターを教育しているか	

Principles of operational technology cyber security（© Commonwealth of Australia 2024、クリエイティブ・コモンズ・ライセンス（表示 4.0 国際））を改変して PwC が作成