



サイバーセキュリティ対応

脆弱性対応とPSIRT支援で、製品セキュリティを強化

サービス概要

製品セキュリティ要求の整理、脆弱性管理、インシデント対応準備を通じて、サイバーセキュリティ対応を支援します。
セキュリティリスクの可視化と対応フロー整備により、継続的な製品セキュリティ運用を支えます。

① 主な支援内容

-  セキュリティ要求整理
-  資産・脅威・脆弱性分析
-  脆弱性監視 / トリアラージ支援
-  インシデント対応フロー整備
-  対策立案・レビュー支援

② 想定成果物

-  セキュリティ要求一覧
-  脆弱性管理表
-  対応フロー図
-  報告テンプレート

③ お客様の主な課題

-  脆弱性情報の監視ができない
-  役割分担が曖昧
-  セキュリティ要求が整理できない
-  報告フローが未整備

④ 提供価値

-  リスク低減
-  対応迅速化
-  運用品質向上
-  顧客信頼性向上

主な対象



ネット接続製品



産業機器



ロボット



欧州輸出品



継続的な脆弱性対応で、製品セキュリティを強化

サイバーセキュリティサービス

1

セキュリティ要求整理・リスク分析

製品のビジネス要件・法規制・脅威を整理し、対策方針を策定します。



セキュリティ要求整理
(規格・法規・顧客要求)



脅威・脆弱性分析
(TARA)



リスク評価



対策方針の立案

分析イメージ

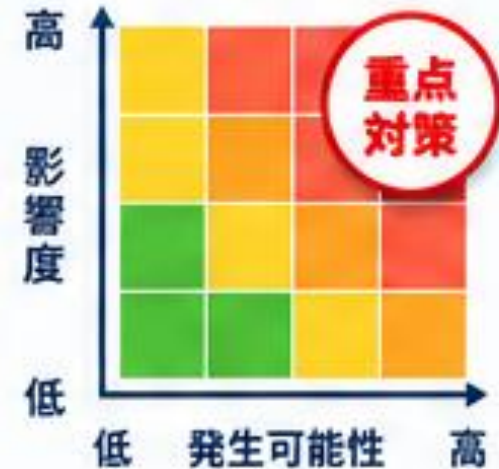
製品・システム
(アセット)



脅威
(Threat)

TARA
(脅威分析・リスク評価)

リスクマップ



サイバーセキュリティサービス

2

脆弱性管理・監視支援

製品のライフサイクルを通じた脆弱性管理と継続的な監視を支援します。



脆弱性情報の収集・分析
(CVEs 等)



自社/サードパーティ
ソフトウェアの脆弱性管理
(SBOM活用)



脆弱性対応計画の策定
(修正・回避・緩和)



定期モニタリング・
アラート対応支援

脆弱性管理フロー

収集

分析

評価

対応

監視



脆弱性情報
(CVE・JVD等)



影響分析
優先度付け



対応方針
の検討



修正・緩和
対策実施



継続監視
再発防止

製品ライフサイクル全体で継続的に支援

サイバーセキュリティサービス

3

インシデント対応準備支援

インシデント発生時に迅速・的確に対応できる体制・プロセスを整備します。



インシデント対応体制の構築
(役割・連絡体制)



対応フロー・手順書の整備



フォレンジック・
原因調査支援



訓練・演習の実施
(テーブルトップ演習)



再発防止策の提案

インシデント対応フロー（例）

検知・
通報



アラート受信
インシデント検知

初動対応
(封じ込め)



CSIRT対応
関係者連携

調査・分析
(原因特定)



ログ解析
原因調査

復旧・
対策実施



修正・復旧
対策展開

報告・
再発防止



レポート作成
改善提案

インシデントの影響を最小化し、迅速な復旧を支援

サイバーセキュリティサービス

4

PSIRT運用・運用支援

製品セキュリティ窓口（PSIRT）の立ち上げから運用までを包括的に支援します。



PSIRT組織・運用プロセス構築



脆弱性情報の受付・管理
(公開ポリシー策定支援)



外部との連携支援
(顧客・研究者・ベンダー)



セキュリティアドバイザリ
の作成支援



教育・運用定着支援

PSIRT運用イメージ



顧客・ユーザー



セキュリティ
研究者



ベンダー・
パートナー



情報の評価・対応



アドバイザリ公開



製品改善・
アップデート

信頼性の高い情報開示と継続的な製品セキュリティ運用を実現