HITACHI
Inspire the Next

資料5

産業サイバーセキュリティ研究会 WG3

サイバーセキュリティ産業の振興に向けて

2024/10/29

株式会社 日立製作所
花見 英樹

HITACHI
Inspire the Next

Contents

１．製造業を取り巻く環境

1．　製造業を取り巻く環境

HITACHI
Inspire the Next

製造業のデジタル化・グローバル化に伴う「責任・義務」を果たしつつ「事業機会」を獲得して成長
［責任・義務］ 安全・安心や持続的社会実現に向けたサプライチェーン全体での社会的責任・義務
［事業機会］　信頼できるデータ、AI活用によるイノベーションと事業機会獲得・国際競争力強化

責任・義務

- **安全保障**
  セキュリティ強化
- **社会の要求**
  SDGs、環境、人権
- **法律・規制**
  セキュリティ、AI，データ関連

経済価値　社会価値　環境価値

グローバルサプライチェーン

サイバーセキュリティ

事業機会

- **デジタル化**
  効率化、価値創出
- **データ連携**
  産業データ活用
- **AI活用**
  AIを活用した製造業の効率化、高度化

２．日立におけるサイバーセキュリティの位置づけ

2-1. 現在のトレンド

HITACHI
Inspire the Next

サプライチェーンのデジタル化、グローバル化、ボーダレス化
➡ サプライチェーンのサイバーセキュリティ強化が国家・経済安全保障上の喫緊の課題へ

① サイバー攻撃の高度化・脅威の深刻化

社会インフラ、システム、サービスの安定稼働が脅かされている

② サプライチェーンを対象としたサイバー攻撃

サプライチェーンの脆弱性を悪用したサイバー攻撃が安全保障上、重大な脅威へ

③ サイバーセキュリティ関連法規制

サプライチェーン全体でサイバーセキュリティ要件を満たす責任をベンダー、製造元が負う
(安定供給に向けたリスク評価、対策、インシデント対応、報告義務など)

一企業では解決できない
『サプライチェーン全体での対応』、『国境を超えて影響する法規制』

2-2. 日立におけるサイバーセキュリティの位置づけ

HITACHI
Inspire the Next

社会インフラ・システム・サービスの安定稼働・品質を支える事業基盤

デジタルシステム＆サービス（DSSセクター）	グリーンエナジー＆モビリティ（GEMセクター）	コネクティブインダストリーズ（CIセクター）
金融・公共・電力・交通など	パワーグリッド・鉄道など	ファクトリー・ビル・ホームなど

サイバーセキュリティ

主要事業にセキュリティをAdd-On

- **開発**：ミッションクリティカルな製品・サービスの品質確保・セキュア開発
- **運用**：サイバー攻撃や脆弱性へ対応し、製品・サービスの安定稼働を維持

３．サイバーセキュリティ政策への期待

3-1. 課題認識

HITACHI
Inspire the Next

ライフサイクルを通じて、調達先を含めたセキュリティ確保・運用は、企業個別では解決不可
➡ ①～③に向けて、サプライチェーン全体にセキュリティを普及させることが産業界としての課題

① システム・サービスの安定稼働
従来：品質(競争領域、各社のノウハウ)
今後：品質(競争領域)＋**調達先を含むセキュリティ確保の仕組み・ルール(協調領域)**

② サプライチェーン全体でのセキュリティ確保は1社では対応できない
セキュリティ技術の差別化だけでは、サプライチェーンの脆弱性を悪用した脅威には対応不可
➡ 産業界にとって重要なことは、サプライチェーン全体のセキュリティレベルが上がること

③ セキュリティ関連法規制対応
セキュリティ確保、システム安定稼働について、企業がサプライチェーン全体の責任を負う
➡ 企業にとって法規制対応は経営リスクであるとともに、事業推進・拡大の前提条件

➡ サプライチェーン全体にセキュリティをいかに普及させていくか？

3-2. サイバーセキュリティ政策への期待

HITACHI
Inspire the Next

サプライチェーン全体にセキュリティを普及させるために『①実効性を高める施策』と『②受容可能なコスト負担』、受け皿となる『③セキュリティサービス産業の強化』を検討すべき

３つの施策を連携し、産業界全体の競争力強化とセキュア化を促進

①基準・ガイドラインの実効性向上

課題 ガイドライン・基準の実効性がない

施策 政府系調達、重要インフラなどへの調達要件化など市場で評価される仕掛け (可視化、認証など)
これらを実現するインセンティブ強化

②コスト負担のエコシステム

課題 セキュリティは企業にとってコストUPであり、市場原理に任せるだけではセキュリティ普及は困難

施策 サプライチェーンを構成する企業が受容可能なコスト負担の仕組み (エコシステム) 整備

③セキュリティサービス産業の強化

課題 実効性向上・コスト負担の施策を実現する仕組み

施策 運用をコアとしたセキュリティサービス産業化
(情報共有、SBOM(*)活用、第三者評価、
法規制対応サービス(運用、アセスメント)など)

(*)SBOM : Software Bill Of Materials

４．今後に向けた提言

4-1．ディスカッション　～ 施策①②の具体化 ～

HITACHI
Inspire the Next

■ 施策①②を具体化し、**業界の理解と支援を得て官民一体で推進**
■ 民間が**施策を持続的に機能させるためのエコシステム**を確立

① 基準・ガイドラインの実効性向上

論点：民間が自らセキュリティ強化のモチベーションを持つような持続的施策とは？

・政府系調達で調達要件化し、政府系システムで高いセキュリティレベルを実現
・民間、重要インフラへ範囲を拡大（調達要件化、補助金活用など）
・セキュリティレベルを可視化、市場原理で自立的にレベル向上（適合性評価など）

② コスト負担のエコシステム

論点：サプライチェーンを構成する企業が受容可能なコスト負担を実現するには？

・社会・産業界全体でコストを薄く広く負担するエコシステム、コミュニティー
・立場の弱い受注者に過度なコスト負担が行かない仕組み
　→ サービスの質・量を競争領域として高め、リーズナブルにサプライチェーン全体に普及

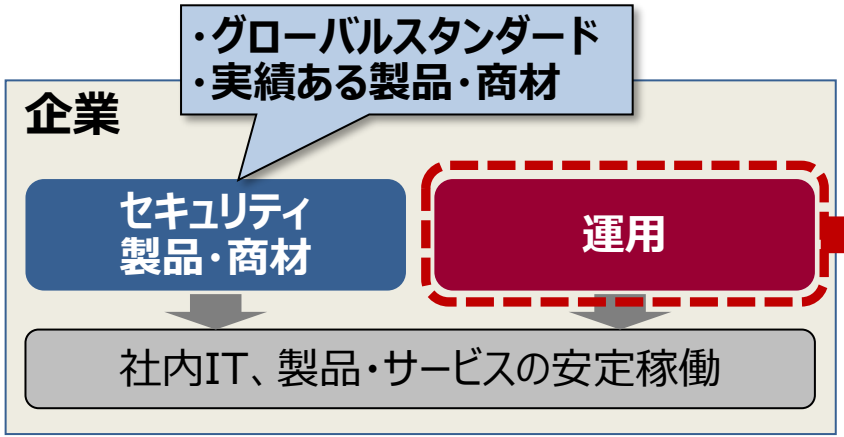
HITACHI
Inspire the Next

日本のサイバーセキュリティを『サービス産業』として育てる
～日本に信頼できるセキュリティサービサーを育て、セキュリティの「普及率」を高める～

受け皿として信頼できるサービサーを国内で育て、サプライチェーン全体に普及

① 基準・ガイドラインの実効性を高める機能、サービス（調達要件化、評価機関など）

② セキュリティサービス産業全体をエコシステムとして、受容可能なコストを実現



政策としての強化ポイント

(1)セキュリティ適合性評価基準・制度
→機器・組織・サービス品質の可視化と普及率向上

(2)オペレーション支援サービス
→情報共有、自動化・効率化、法規制対応など

(3)人材育成（資格制度・活用の仕組み）
→セキュリティ商材の知見、ツールの使いこなし、オペレーター（監視、インシデント対応など）

HITACHI
Inspire the Next

END

サイバーセキュリティ産業の振興に向けて

2024/10/29

株式会社 日立製作所
花見 英樹