情報システムのサプライチェーンにおける情報セキュリティに関する調査

平成23年3月

(財)未来工学研究所

１．サプライチェーンの情報セキュリティ課題の概要①

１．米国におけるサプライチェーンの定義（NISTIR 7622による）

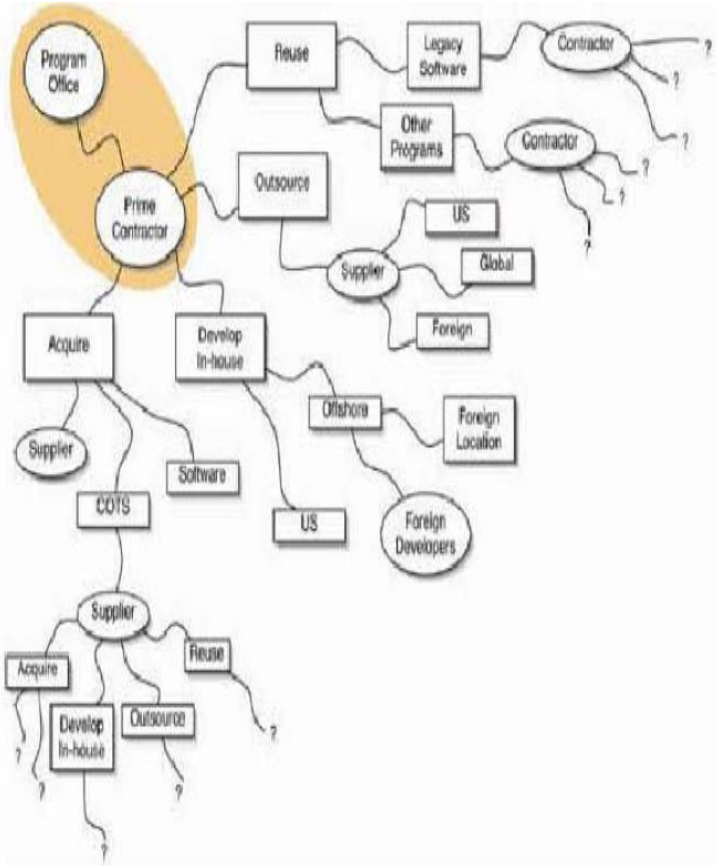
サプライチェーンとは、製品やサービス（サブエレメントを含む）を生産して動かして、サプライヤから組織の顧客に供給するための組織、人、活動、情報及び資源を意味する。

２．米国でサプライチェーンのセキュリティ課題が登場した背景

1980年代	COTS ＝Commercially off the Shelf）
1990年代	調達のグローバル化
1990年代後半	ハード・ソフトのIT調達のオープン化
2000年代	重要インフラのへのサイバー攻撃の頻発

1．サプライチェーンの情報セキュリティ課題の概要②

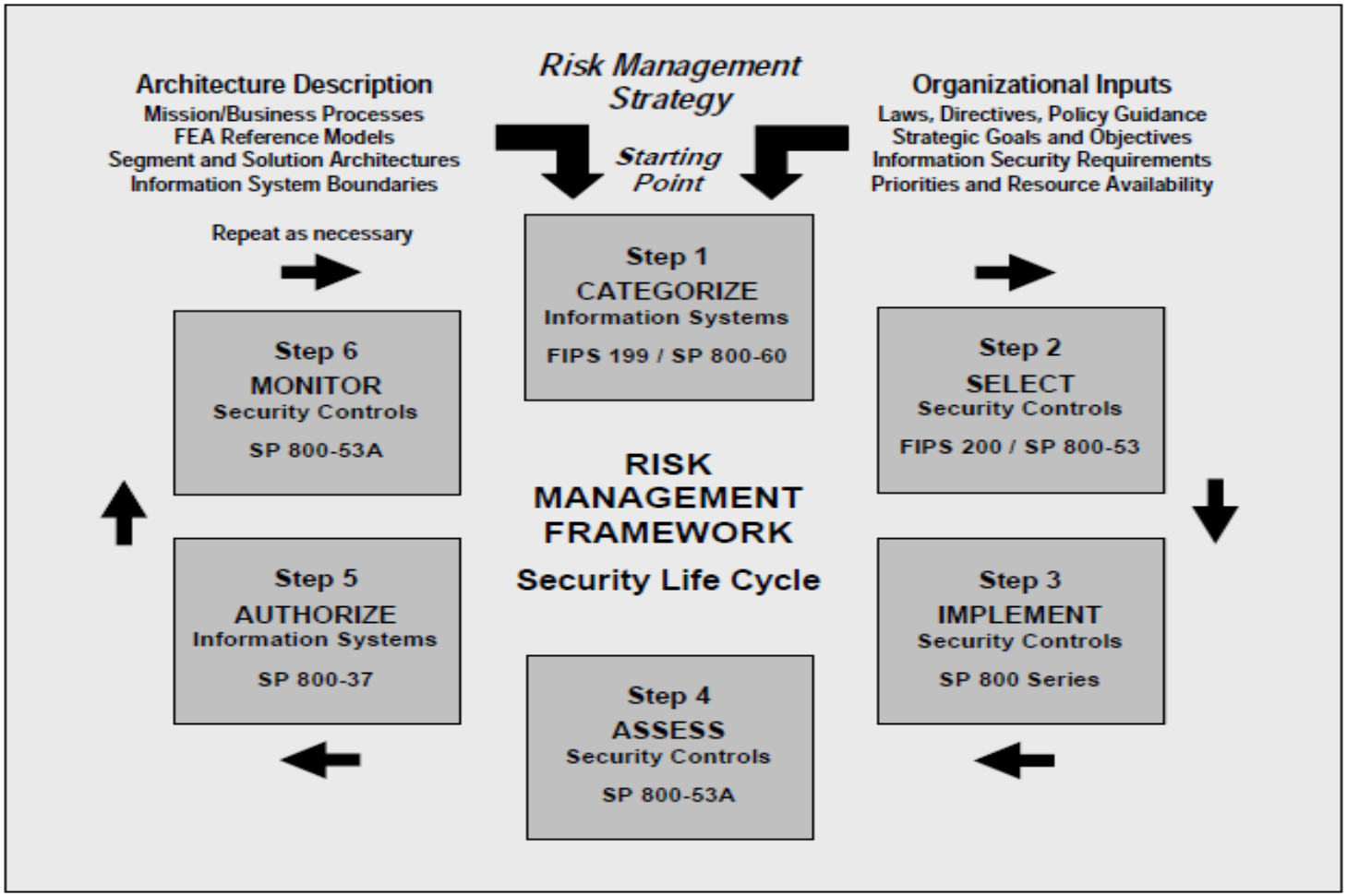
アメリカにおけるサプライチェーンの概念図（右図は翻訳）



プログラム・オフィス	プライム・コントラクタ	再使用	レガシーソフトウェア	コントラクター		不明のサプライヤ群
			その他のプログラム	コントラクター		不明のサプライヤ群
		外注	サプライヤ	米国内		
				グローバル		
				外国		
		内製	オフショア	外国に立地		
				外国の開発者		
			米国内			
		調達	ソフトウェア			
			サプライヤ			
			COTS	サプライヤ	再使用	不明のサプライヤ群
					外注	不明のサプライヤ群
					内製	不明のサプライヤ群
					調達	不明のサプライヤ群

2. サプライチェーンの情報セキュリティの最近の動向と将来予測（米国1）

NIST800-53が示すサプライチェーンのリスクマネジメント・フレームワーク



2. サプライチェーンの情報セキュリティの最近の動向と将来予測（米国2）

国土安全保障省（DHS）が示す調達ソフトウェアのスコアリング・サンプル

Categories	Priority	Product Score			Weighted Average			
		Product 1 Score (0–4)	Product 2 Score (0–4)	Product 3 Score (0–4)	Product 1	Product 2	Product 3	Average
					1.6	2.1	2.5	10.6
Software History & Licensing	5	2	2	3	8.4	11.4	13.0	10.9
Development Process Management	3	1	3	4	9.0	9.0	9.0	9.0
Software Security Awareness and Training	3	2	2	3	9.0	9.0	9.0	9.0
Concept and Planning	2				0.0	0.0	0.0	0.0
Architecture and Design	3				0.0	0.0	0.0	0.0
Software Development	3				0.0	0.0	0.0	0.0
Testing	4				0.0	0.0	0.0	0.0
Software Change Management	4				0.0	0.0	0.0	0.0
Built-in Software Defenses	2				0.0	0.0	0.0	0.0
Assurance Claims and Evidence	5				0.0	0.0	0.0	0.0
Timeliness of Vulnerability Mitigation	3				0.0	0.0	0.0	0.0
Security Track Record	4				0.0	0.0	0.0	0.0

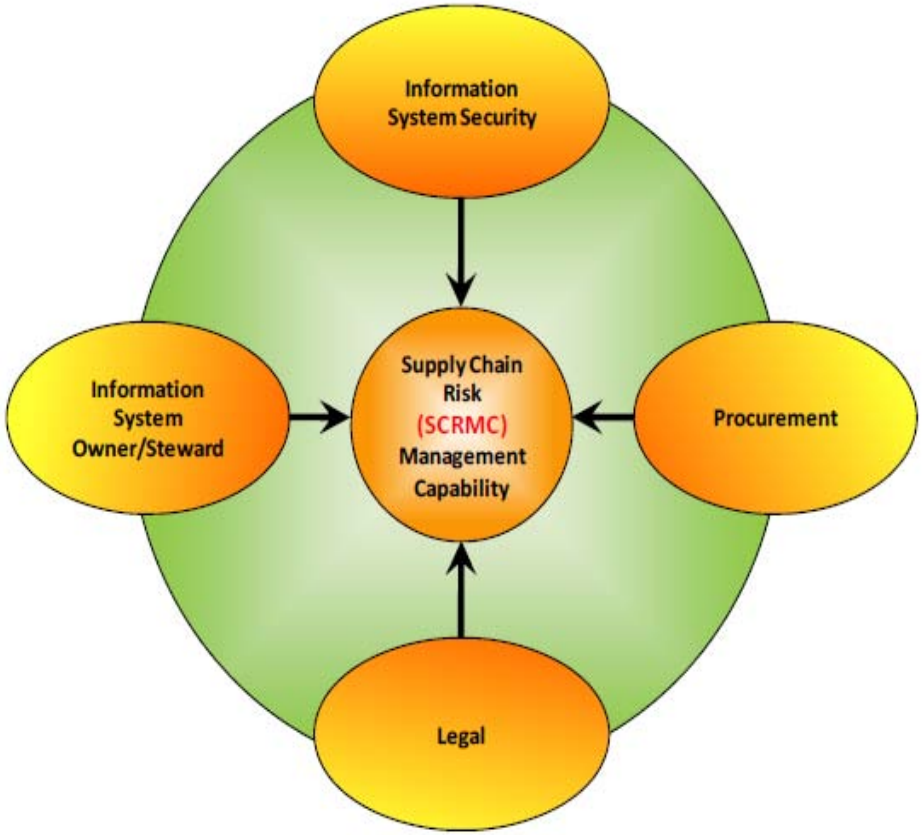
2. サプライチェーンの情報セキュリティの最近の動向と将来予測（米国3）

Comprehensive National Cybersecurity Initiative＝CNCIにおける12のR&D課題

#1	信頼できるインタネット接続を備えた単一の連邦政府ネットワークの管理
#2	連邦政府システム全体に及ぶセンサーによる侵入検出システムの展開
#3	連邦政府システム全体に及ぶ侵入防止システムの展開の追及
#4	研究開発（R&D）努力の調整と再指向
#5	状況認識力の強化のために現存するサイバー運用センターを結合させる
#6	政府全体に及ぶサイバー・カウンターインテリジェンス（CI）プランの開発と実施
#7	米国の機密ネットワークのセキュリティ強化
#8	サイバー教育の拡充
#9	耐久性のある「飛躍的」技術、戦略、計画を定義し開発する
#10	耐久性のある抑止の戦略と計画を定義し開発する
#11	**グローバルに多数に枝分かれしたサプライチェーンのリスク管理**
#12	重要インフラドメインへのサイバーセキュリティの拡大への連邦政府の役割の定義

2. サプライチェーンの情報セキュリティの最近の動向と将来予測（米国4）

NISTIR 7622（サプライチェーンに関する最新の重要文書）



サプライチェーンリスクマネジメント能力を構成する4つの要素

・情報システムセキュリティ

・調達

・法制

・情報システムの所有者と運用者

2　サプライチェーンの情報セキュリティの最近の動向と将来予測（欧州１）

ENISA におけるサプライチェーンリスクの7つの課題と4つのキーファクター

7つの課題

① グローバルに分散したサプライチェーン（人、プロセス。技術）の複雑な性格
② ICTサプライチェーンに共通したガイドラインの欠如
③ 統計的な確信レベルとITエコシステム全体を通じて統合性を認証するツール、プロセス、コントロールの欠如
④ エンドユーザにとっての非効果的な製品評価の方法論と技術
⑤ システムへの偽造や偽装による侵入を検出し打破できる、幅広く適用できるツール、テクニック、プロセスの欠如
⑥ 購入によって生産され運用・使用されている、異なったタイプの製品の統合を維持するための協同的アプローチの欠如。
⑦ ICTの各種の分野を越えた統合的要求の調和を引きだし得る、共通のビジネスモデルの欠如。

4つのキーファクター

① 生産、配送、購入、導入および導入された製品とシステムの維持などの全サプライチェーンの設計を通じて、継続的に実行され明確に定義された製品とサービスへの要求
② アップストリームの要求を遵守したコンポーネントの評価と実証のための方法論
③ ソルージョンの組立と導入時、及び製品の適切な（定義されるべき）ライフサイクル時期における、ハードウェアとソフトウェアのコンポーネント・パーツの出自（確認された起源）と真実性を評価する能力。
④ その元来の意図された利用モデル全体を通じた、システム、コンフィギュレーション、運用パラメータの統合性を防護し維持する手段

2　サプライチェーンの情報セキュリティの最近の動向と将来予測（欧州２）

EUの研究開発計画（PROCENT）における重要５項目と
「サプライチェーン統合」課題の登場

①クラウド・コンピューティング
②リアルタイム検出・診断システム
③将来型無線ネットワーク
④センサネットワーク
⑤サプライチェーンの統合

2 わが国におけるサプライチェーン課題の認識

わが国おけるサプライチェーン問題の認識は

①物流に係る問題

（「第２次情報セキュリティ基本計画」における認識）

または

②成長戦略の一部

（経済産業省サイバーセキュリティと経済研究会における認識）

であり、課題自体の重要性の認識は低かった。

即ち、サプライチェーンの情報セキュリティについて、

わが国はIT先進国とは言えない。

3.サプライチェーンが重要インフラの情報セキュリティにもたらす影響の考察（米国１）

Comprehensive National Cybersecurity Initiative＝CNCIにおけるサプライチェーンのセキュリティに関するＲ＆Ｄの方向性

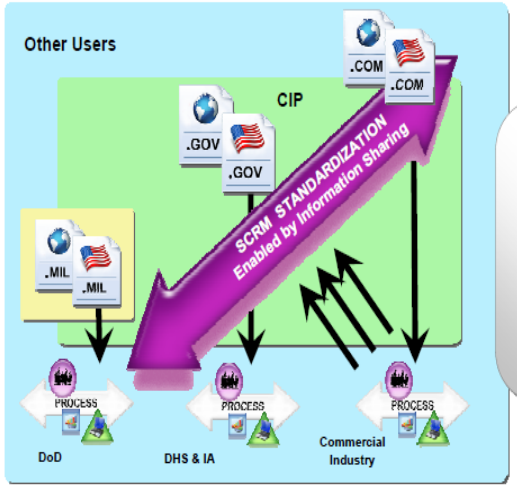
民間の情報通信技術市場は、サプライチェーンへの侵入を通じて、データへの非正統的なアクセスの入手、データの改変、通信の妨害などを試みる者たちに、増大する機会を提供している。国内外のサプライチェーンから由来するリスクは、製品の全ライフサイクルに亘って、戦略的で包括的な方法で管理されなければならない。このリスク管理は、調達決定、に関連した脅威、脆弱性、その結果についてのより大きな認識を要請している。それらは、ライフサイクル全般（設計から退役まで）に亘って技術的にも運用面でもリスクを軽減するツールとリソースの開発と採用、複雑なグローバル市場を反映した新しい調達政策とその実行、サプライチェーンとリスクマネジメントの標準とベストプラクティスを開発、採用するための産業界との協力を要請している。このイニシアティブは、彼らのシステムやネットワークの重要性とリスクに相応するレベルで、サプライチェーンのリスクをよりよく管理し緩和するロバストなツールセットを各省庁に提供し、連邦政府の技能、政策、プロセスを強化する。

3.サプライチェーンが重要インフラの情報セキュリティにもたらす影響の考察（米国2）

米国国防総省におけるサプライチェーンリスク管理の標準モデルと標準化の開発と実施の予定

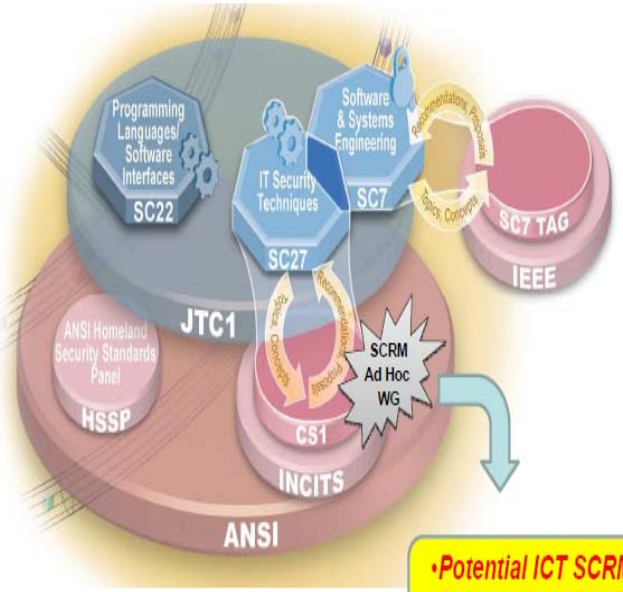
SCRM Stakeholders

US (CNCI) has vital interest in the global supply chain.



SCRM "commercially acceptable global standard(s)" must be derived from Commercial Industry Best Practices.

SCRM Standardization Requires Public-Private Collaborative Effort



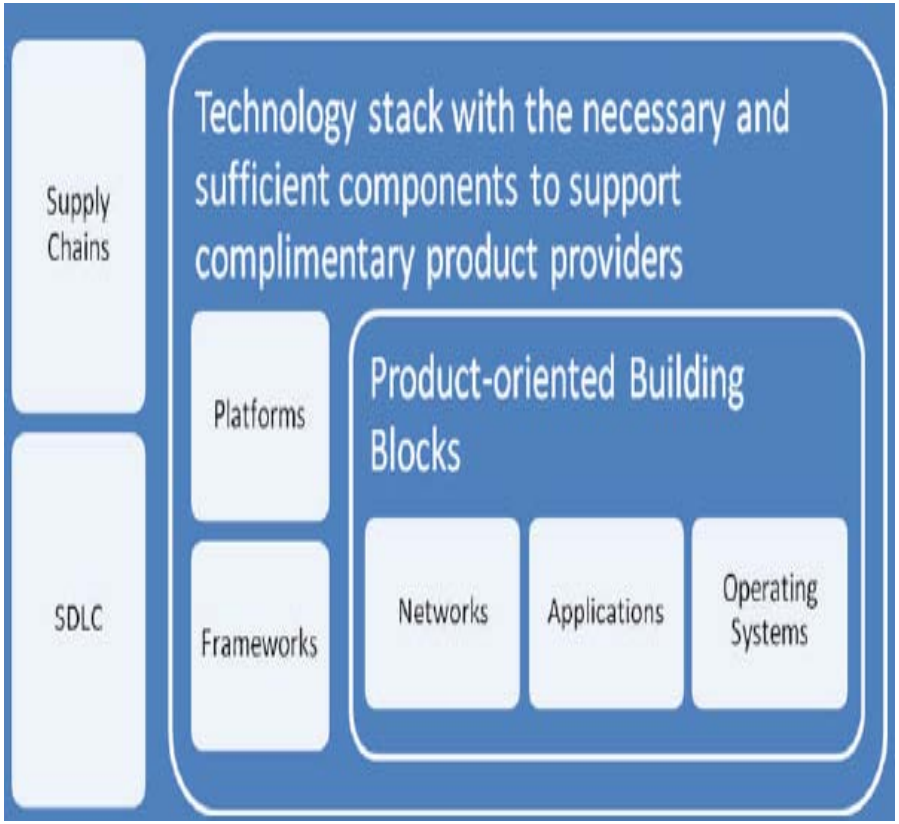
- *Potential ICT SCRM ISO Standard*
- *Development 2010-2013*
- *Adoption 2013-2016*

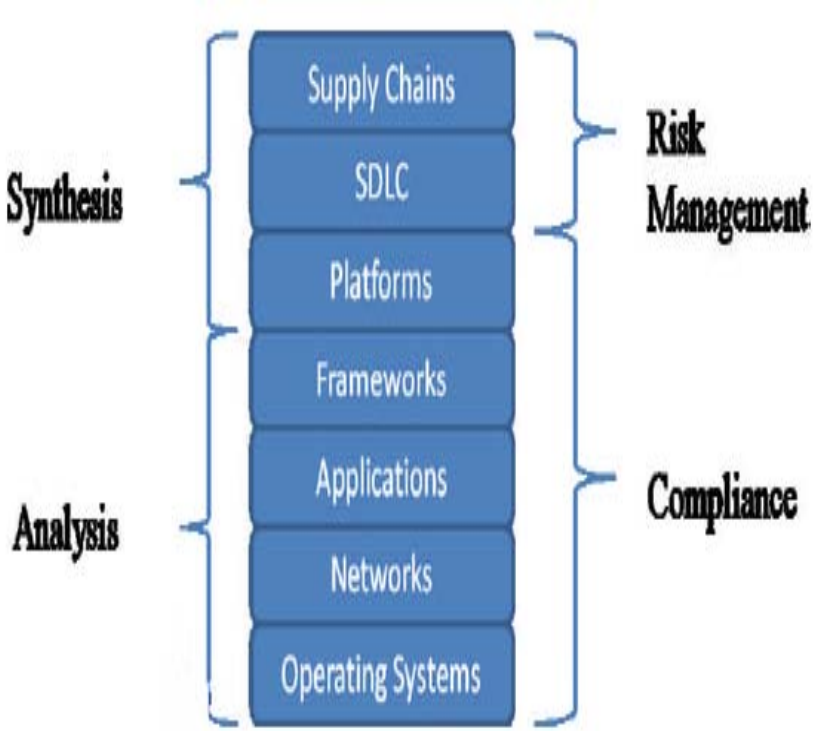
3.サプライチェーンが重要インフラの情報セキュリティにもたらす影響の考察（米国3）

IT技術発展の最新のビジネスモデルとしてのサプライチェーンリスク管理

Building A Cyber Supply Chain Assurance Reference Modelより

純民間からの視点





3.サプライチェーンが重要インフラの情報セキュリティにもたらす影響の考察（欧州）

欧州の研究開発計画（PROCENT）におけるサプライチェーン課題の展開

①紹介
②課題
③サプライチェーン統合のリスクの理解
④サプライチェーン統合のリスク管理
⑤評価のフレームワーク
⑥グッドプラクティスと現在の研究プロジェクトの例
⑦現在のリスクと新しい研究機会
⑧結論

⑦現在のリスクと新しい研究機会

1. 改良された革新的なトラストモデル
2. 評価と統合チェックテクニックの改良
3. 各種の産業分野と政府の購入で用いられているグッドプラクティスの研究
4. 偽装と乗っ取りを検出・防護する改良された技術ソリューション
5. 情報保証への新しいアプローチ
6. 在庫とコンフィグレーションの制御と維持への新しいアプローチ
7. グローバル規模での政策的必要性評価のアプローチ法の研究

3.サプライチェーンが重要インフラの情報セキュリティにもたらす影響の考察（わが国）

「サイバーセキュリティと経済」研究会における
山口英委員（奈良先端科学技術大学院大学）の議論

・サプライチェインの情報化と保護が、近年の諸外国におけるサイバーセキュリティ政策では大きな柱になっている（中略）。サプライチェインの情報セキュリティ対策についても議論すべきではないか。

・元々地域性の低い産業である情報セキュリティ産業を対象に、数年で解決できないような構造的課題を抱えているわが国において、内需拡大などを政策課題として考えることは、適切ではない。（中略）、わが国の情報セキュリティ産業が現状のような国際競争力を持たない状況をどのように改善し、そのビジネスを世界に広げていくのかを考えた方が、より建設的かつ的確な議論と政策提示ができるのではないか。「内需ゼロ」を前提とした、情報セキュリティ産業政策再設計による産業の国際化の推進を議論することを強く提案したい。

４．わが国重要インフラ関係者が取り組むべき対策に関する提言

①サプライチェーンの情報セキュリティ課題の認識

②サプライチェーン課題の先進国・地域の情報収集

③「事故前提社会」の下でのサプライチェーンの情報セキュリティ管理

④インシデント事例共有が必要

⑤産学官による集中的な課題検討の実施

⑥政府の雇用や具体的プロジェクトを通じた情報セキュリティ人材の維持と育成

⑦近い将来のガイドラインの作成を目指すこと