平成 22 年度
内閣官房情報セキュリティセンター委託調査

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

財団法人未来工学研究所

平成 23 年 3 月

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

1. 情報システムのサプライチェーンのセキュリティ問題の概要
1.1　情報システムのサプライチェーンの定義
1.2　サプライチェーンのセキュリティ課題が登場した背景
1.3 情報システムのサプライチェーンの概念図
2. サプライチェーンの情報セキュリテ問題の最近の動向と将来予測
2.1　米国における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
2.1.1 米国の商務省・NIST による情報サプライチェーン管理政策の近年の動向
2.1.2 米国の国土安全保障省による情報サプライチェーン管理政策の近年の動向
2.1.3 国防総省による情報サプライチェーン管理政策の近年の動向
2.1.4 大統領のサイバーセキュリティ・イニシアティブにおけるサプライチェーン課題
2.1.5 NISTIR 7622 文書
2 .1.6　日本企業に関わる米軍サプライチェーンの情報セキュリティ課題の一事例
2.2　欧州における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
2.2　欧州における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
2.2.1 ENISA の研究開発課題におけるサプライチェーンの情報セキュリティの提起
2.2.2　ENISA Quarterly Review におけるサプライチェーン課題の提起
2.2.3　EU の研究開発計画（PRCENT）における「サプライチェーン統合」の登場
2.3　わが国における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
2.3.1 わが国における近年のサプライチェーン問題の認識の推移
2.3.2 「第２次情報セキュリティ基本計画」におけるサプライチェーン課題の認識
2.3.3　「サイバーセキュリティと経済」研究会におけるサイバーセキュリティ課題の認識
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
3.1　米国における考察
3.1.1　サイバーセキュリティ・イニシアティブにおけるサプライチェーン関連技術開発
3.1.2 国防総省の視点から見たサプライチェーンリスク管理の標準化
3.1.3　IT 技術の歴史的発展から見たサイバー・サプライチェーンへの一考察
3.2　欧州における考察
3.2.1 欧州サイバー研究開発計画におけるサプライチェーン統合についての記述
3.3　わが国における考察
3.3.1　「サイバーセキュリティと経済」研究会における山口委員の議論
4. 今後の取り組みに向けた提言
5. 文献一覧

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　サプライチェーンの定義

2010年6月に公表されたNISTIR 7622ドラフト、”Piloting Supply Chain Risk Management Practices for Federal Information Systems” は、サプライチェーンに以下のような簡潔な定義を与えている。

本報告書において、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、移動して、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。

http://csrc.nist.gov/publications/drafts/nistir-7622/draft-nistir-7622.pdf

1.2　サプライチェーンの情報セキュリティが課題として登場した背景

サイバー・サプライチェーン・セキュリティという概念は、1980 年代末に米国で導入された Trusted Product Evaluation（高信頼製品評価）制度に始まる。当時の米国の関心は、防衛関連装備の調達において、そのコンポーネントや部品に民生品の採用が進んだ（いわゆる COTS 化[1]）ことによって、民生品の信頼性が問われるようになったことにあった。また、この頃に日本や欧州各国などの技術水準の上昇によって、米国産品だけによる装備品のコンポーネントや部品の調達が困難になったという事情（調達のグローバル化）もその背景にあった。

NCSC-TG-002, Trusted Product Evaluation, A Guide for Vendors, March 1988
http://www.fas.org/irp/nsa/rainbow/tg002.htm

その後、1990年代後半以降のIT技術の劇的な発展過程で、サーバ、PC、ルータ、ICチップなどのIT関連ハードウェアの価格が下落し、安価な民生用品が防衛装備などの政府調達システムに大量に採用されることとなり、ソフト面また、WindowsやLinuxなどのオープンOSや汎用ソフトウェアが、大型メインフレーム時代以来のいわゆるレガシーシステム中に大量に導入されることとなった（IT調達のオープン化）。

さらに2001年の9.11事件において重要インフラがテロ攻撃の手段や対象になり、その防護が国家的重要課題として浮上し、その後も相次いだ政府システムや重要インフラへのサイバー攻撃が、サプライチェーンのセキュリティ課題の重要性を一層広く認識させることなった。

以上に述べたように、COTS化、グローバル化、オープン化という三つの背景と、重要インフラへの攻撃の頻発が相まって、この課題の重要化に至ったといえる。

本報告書では、サプライチェーンのセキュリティという幅広い概念のうち、情報システムに関わるサプライチェーンのセキュリティについて主として論及する。また、この課題が近年米国において急速に関心を集め、対策も次々と公表されてきたので、本報告

---

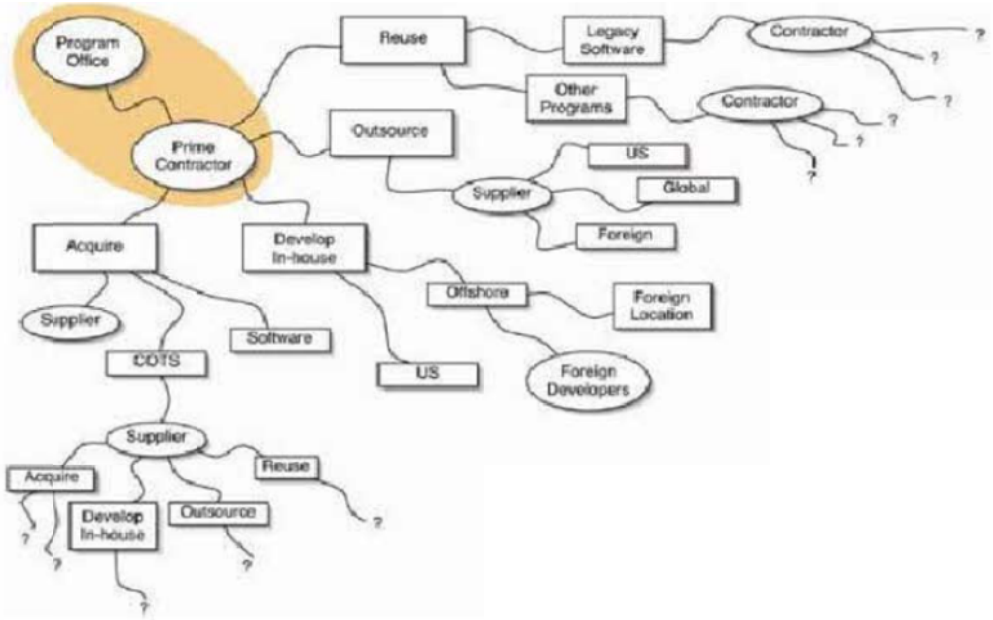
[1] COTS＝Commercially off the Shelf, 民間が開発したソフトウェアを政府部門が購入してそのまま使用すること

書では主に米国の動向を中心として叙述し、欧州とわが国の動向についても簡単に触れることとする。

1.3 サプライチェーンの概念図

米国で情報システムサプライチェーンのセキュリティについて論及されるとき、しばしば用いられる概念図が次ページに示した図表1-1である。発注者・運用者とシステム構築を依頼されたプライム・コントラクタ（システム・インテグレータ）から見たとき、情報システムが今日どのように製作され運用されているかを、この図はよく示していると考えられる。図表1-1はやや読み取りにくいので、次ページにおいて図表1-2として翻訳して再掲した。

図表1-1　アメリカにおけるサプライチェーンの概念図



図表 1-2　サプライチェーンの概念図（翻訳）

<table>
<tr><td rowspan="15">プログラム・オフィス（発注・運用者の中心部局）</td><td rowspan="15">プライム・コントラクタ（システム・インテグレータ）</td><td rowspan="2">再使用（リユース）</td><td>レガシーソフトウェア</td><td colspan="2">コントラクター（サプライヤ）</td><td>不明のサプライヤ群</td></tr>
<tr><td>その他のプログラム</td><td colspan="2">コントラクター（サプライヤ）</td><td>不明のサプライヤ群</td></tr>
<tr><td rowspan="3">外注(アウトソーシング)</td><td rowspan="3">サプライヤ</td><td colspan="3">米国内（のサプライヤ）</td></tr>
<tr><td colspan="3">グローバル（に展開しているサプライヤ）</td></tr>
<tr><td colspan="3">外国（のサプライヤ）</td></tr>
<tr><td rowspan="3">内製(インハウス開発)</td><td rowspan="2">海外</td><td colspan="3">外国に立地する開発者</td></tr>
<tr><td colspan="3">外国の開発者</td></tr>
<tr><td>米国内</td><td colspan="3">米国内の開発者</td></tr>
<tr><td rowspan="6">調達(購入)</td><td>ソフトウェア</td><td colspan="3"></td></tr>
<tr><td>サプライヤ</td><td colspan="3"></td></tr>
<tr><td rowspan="4">COTS</td><td rowspan="4">サプライヤ</td><td>再使用</td><td>不明のサプライヤ群</td></tr>
<tr><td>外注</td><td>不明のサプライヤ群</td></tr>
<tr><td>内製</td><td>不明のサプライヤ群</td></tr>
<tr><td>調達</td><td>不明のサプライヤ群</td></tr>
</table>

ENGINEERING FOR SYSTEM ASSURANCE Version 1.0 National Defense Industrial Association
http://www.ndia.org/Divisions/Divisions/SystemsEngineering/Documents/Committees/Systems%20Assurance%20Committee/2008/SA-Guidebook-v1-Oct2008-REV.pdf

上の二つの図が示しているように、情報システムのサプライチェーンが、システムの下部要素に行けば行くほど、その開発が、調達者である政府機関やそのプライム・コントラクタであるシステム・インテグレータの目を離れ、開発者の実体が定かではない国内外のサプライヤの手にゆだねられるという現実が存在している。政府情報システムの調達や開発におけるこのような現状の下で、システムの情報セキュリティをいかに担保するかが、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課題の本質であると考えられる。

２．サプライチェーンの情報セキュリティ問題の最近の動向と将来予測

2.1　米国における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

2.1.1 米国の商務省・NIST による情報サプライチェーン管理政策の動向

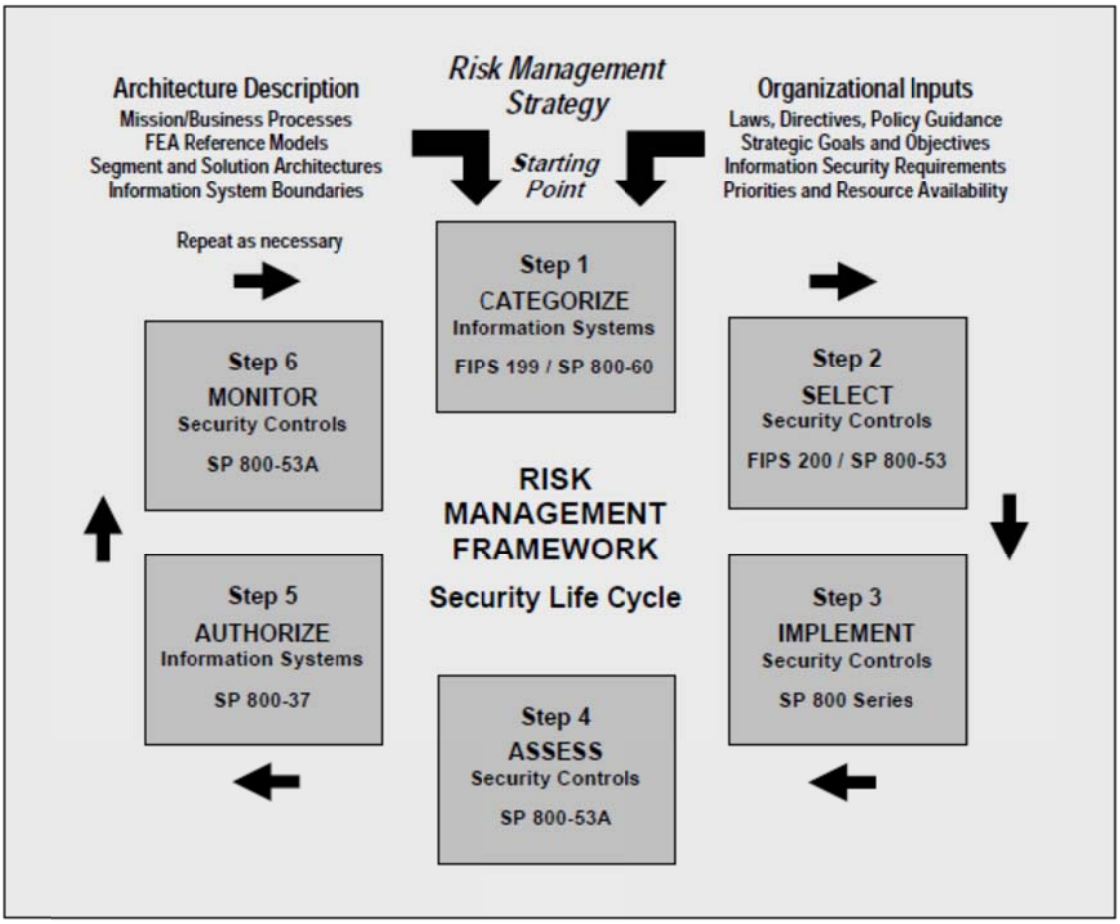
1.2 で述べたサプライチェーンにおける COTS の拡大、グローバル化、オープン化という三つの傾向を背景に、1996 年に施行された「情報技術マネジメント改革法」の第 5131 条で、連邦政府の調達する IT 機器に関わる「標準とガイドライン」の設定が求められている。
http://govinfo.library.unt.edu/npr/library/misc/s1124.html

また、9.11 テロ後の 2002 年には、「2002 年連邦情報セキュリティマネジメント法＝法律 107 347」が制定された。
http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

この二つの連邦法の下で商務省・NISTの手で策定されたのが、2004年2月公布の「連邦情報処理規格＝FIPS199」、及び2006年3月公布の「FIPS200」であった。FIPS199は「連邦政府の情報および情報システムに対する最低限のセキュリティ分類規格」を定めたものであり、FIPS200は「連邦政府の情報および情報システムに対する最低限のセキュリティ要求事項」を定めたものである。この二つの規格については、米国政府の調達に応じる外国企業が順守しなければならない情報セキュリティ基準として、わが国の情報処理機構（IPA）の手によって訳出されている。
http://www.ipa.go.jp/security/publications/nist/documents/FIPS-200-J.pdf
http://www.ipa.go.jp/security/publications/nist/documents/FIPS-199-J.pdf

さらに、2009 年 8 月には NIST から「連邦情報システムと組織に推奨されるセキュリティコントロール」と題する特別出版 800-53 第 3 版が刊行された。239 ページに及ぶ大部の NIST800-53 文書は、FIPS199 と FIPS200 と並んで、連邦政府の情報システムの調達に際するセキュリティ順守の基準を定めるものとなっている。NIST800-53 は下の図表 2-1 を掲げて、FIPS199 と FIPS200 と連動した情報リスクマネジメント戦略のフレームワークのサイクルを描いている。

図表 2-1　NIST800-53 が示すリスクマネジメント・フレームワーク



連邦情報システムと組織に推奨されるセキュリティコントロール、NIST 特別出版 800-53 第 3 版、2009 年 8 月
http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf

上の図の示すリスクマネジメント・フレームワークのサイクルは、以下の 6 つのステップから成っている。
ステップ 1 、FIPS 199 / SP 800-60 に基づいた情報システムの分類
ステップ 2、FIPS 200 / SP 800-53 に基づいたセキュリティコントロールの選択
ステップ 3、SP 800 Series に基づいたセキュリティコントロールの実施
ステップ 4、SP 800 53A に基づいたセキュリティコントロールへのアクセス
ステップ 5、SP 800 37 に基づいたセキュリティ情報システムの認可
ステップ 6、SP 800 53A に基づいたセキュリティコントロールの監視

なお、この項や以下の各項では政府調達の情報システムのサプライチェーンを対象とした記述が多いが、これらの政府調達に関わる規格やグッドプラクティスなどは、民間部門、

特に重要インフラの所有者・管理者にもほぼそのまま準用できることを、ここで確認しておきたい。

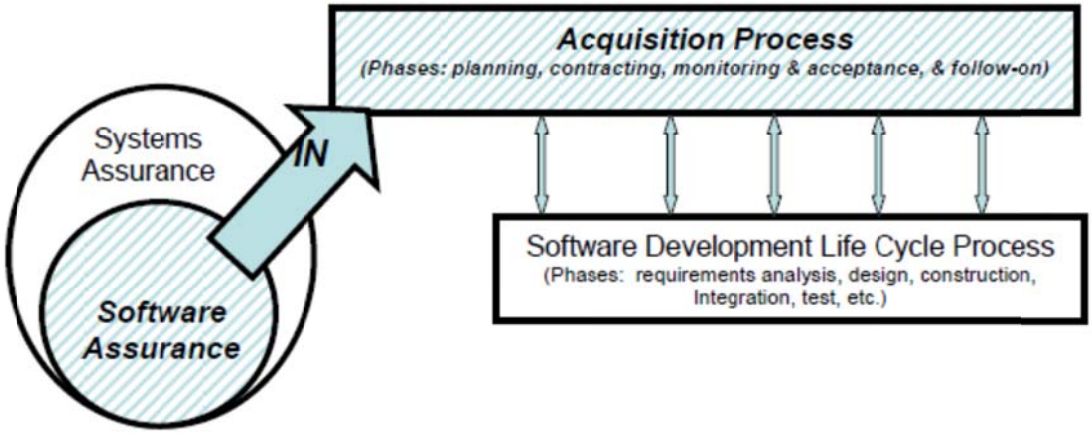
2.1.2 米国の国土安全保障省による情報サプライチェーン管理政策の近年の動向

米国では、重要インフラ・キー資源セクター（CIKRS）として 18 の分野が定められており、それぞれに担当官庁が決められている。農業（農務省と健康保健省）、防衛産業基盤（国防総省）、エネルギー（エネルギー省）、保健衛生（健康保健省）、国家的記念物（内務省）、銀行と財務（財務省）、水（環境庁）であり、残りの 11 分野（化学、商業施設、重要製造業、ダム、緊急時サービス、原子炉・核物質・核廃棄物、情報技術、通信、郵便と海運、運輸システム、政府機能）はすべて国土安全保障省が担当官庁となっている。

このうち、情報技術と通信が DHS のサイバーセキュリティ・通信局の担当であるが、その下に置かれたサイバーセキュリティ部がスポンサーしているのが、ソフトウェアアシュアランス(SwA)であり、その下に調達ワーキンググループが置かれている。このグループが 2008 年 10 月にソフトウェアの調達と外注のための参照ガイドとして提出したのが、”Soft-ware Assurance in Acquisition” である。

この参照ガイドは、ソフトウェア保証とソフトウェア調達プロセスの関係を図表 2-2 のように図示している。ソフトウェアの調達者側には、計画、契約、監視と検収、フォローオンの各フェイズがあり、サプライヤ内部で進行するソフトウェア開発のライフサイクルプロセスには、要求分析、設計、建設、統合、試験等のプロセスがある。調達者側が調達プロセスをガイドラインに沿って進め、サプライヤ内部の進行との協働性を高めることを下図は主張しているわけである。

図表 2-2　ソフトウェア保証とソフトウェア調達プロセス



Software Assurance in Acquisition: Mitigating Risks to the Enterprise
https://buildsecurityin.us-cert.gov/swa/downloads/SwA_in_Acquisition_102208.pdf

さらにこの参照ガイドは、調達者が調達するソフトウェアを適正評価（デューデリジェンス）する際の、調査表の作成を下の図表 2-3 のように例示している。ソフトウェアの歴史とライセンスから始まりセキュリティ履歴まで、評価対象となる部門ごとに優先順位を定め、各ソフトウェアの評価をスコアリングし、各ソフトウェアにウェイト付けを行って、総合評価を算出するという方式である。

下図の各評価項目において、「ソフトウェアセキュリティの自覚と訓練」、「ビルトインソフトウェアの防衛」「（ソフトウェア）保証の宣言とそのエビデンス」、「適時性と脆弱性緩和」「セキュリティの実績」など、情報セキュリティに係る領域が評価の対象になっていることが注目される。

図表 2.3　調達ソフトウェアのスコアリングのサンプル

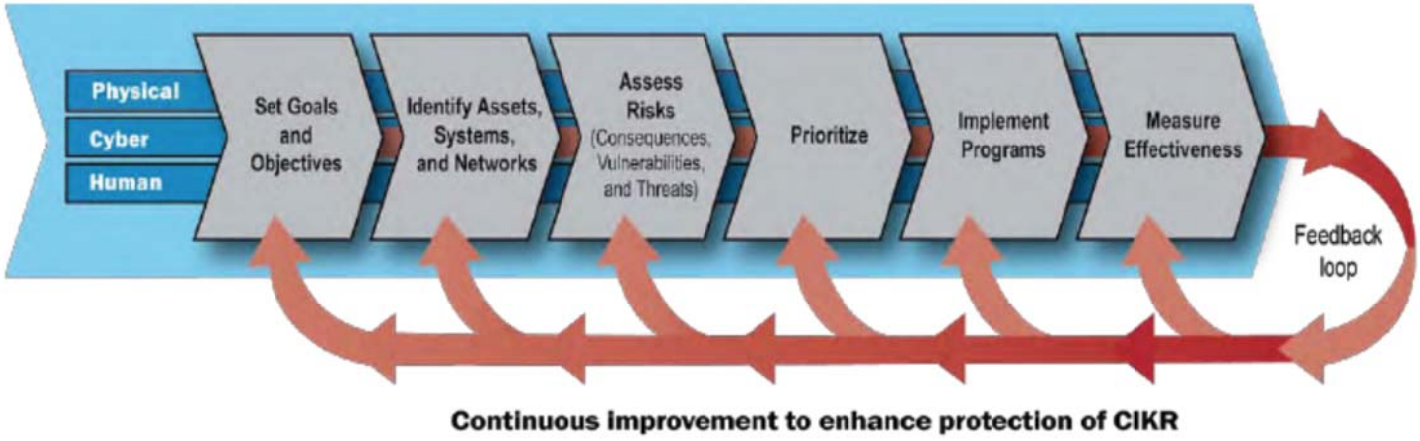
Categories	Priority	Product Score			Weighted Average			
		Product 1 Score (0–4)	Product 2 Score (0–4)	Product 3 Score (0–4)	Product 1	Product 2	Product 3	Average
					1.6	2.1	2.5	10.6
Software History & Licensing	5	2	2	3	8.4	11.4	13.0	10.9
Development Process Management	3	1	3	4	9.0	9.0	9.0	9.0
Software 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

また、上の図表 2-3 と同じ手法を用いたデユーデリジェンス用のスコアリング調査票が、COTS ソフトウェア、オープンソース・ソフトウェエア、カスタム・ソフトウェア、GOTS[2] ソフトウェアという 4 つの調達ソフトウェアの種類別に提供されている。

[2] Government off the shelf, 政府の他部門が開発したソフトウェアをそのまま利用すること。

その後、2009 年に国土安全保障省は、重要インフラのセキュリティに係る包括的文書として、”National Infrastructure Protection Plan Partnering to enhance protection and resiliency” を提出している。この文書の大きな特徴として、重要インフラのセキュリティを担う要素として、物理的セキュリティ、人間的セキュリティと並んで、サイバーセキュリティを三本柱として強調していることが注目される。

図表 2-4 国土安全保障省が示す重要インフラの強化改善サイクル



“National Infrastructure Protection Plan - Partnering to enhance protection and resiliency”
http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

上の報告書は、サプライチェーンの情報セキュリティについて特出して項を立ててはいないが、例えば、「重要インフラの最前線の防衛を樹立する継続的努力は、現在の脆弱性の減少と侵入の検出、情報活動とサプライチェーンセキュリティの強化による全分野的な脅威の防衛、研究開発と教育を強化することによる未来の環境を概観することなどによってなされる」（同報告書 119P、下線は引用者による）といったように、サプライチェーンのセキュリティ活動の必要が述べられている。

2.1.3 国防総省による情報サプライチェーン管理政策の近年の動向

1.2で触れたように、米国におけるサプライチェーンのセキュリティに関する関心は元々国防政策の一環として生まれたものである。こうした関心を防衛装備生産に生かすために、米国防衛産業協会（NDIA）は2008年10月に、“ENGINEERING FOR SYSTEM ASSURANCE Version 1.0”を公刊して、防衛関連産業における情報システムセキュリティのガイダンスとした。

この報告書では、サプライチェーンのセキュリティ課題は大きく取り上げられている。サプライヤ・アシュアランスの項では、サプライチェーンの情報セキュリティ課題が述べ

られており、特に以下の5項目について詳しくガイダンスが定められている。
①システム要素の重要性
②サプライヤのリスク評価
③オフザシェルフ（OTS）COTS 及び GOTS
④カスタムシステム
⑤信頼できる IC 半導体
http://www.acq.osd.mil/se/docs/SA-Guidebook-v1-Oct2008.pdf

例えば、①システム要素の重要性評価については下の図表 2-5 による分類が求められている。

図表 2-5　システム要素の重要度評価基準

重要度	定義	許容度	例
最高	システム内のシステム又は要素の不具合が、直接ミッション/ビジネスの能力を低下させ、ミッション/ビジネスの失敗をもたらす。	秒単位から分単位	オンラインの防衛関連トランザクションへの DoS 攻撃
高い	システム内のシステム又は要素の不具合が、システムのミッション/ビジネスの能力を深刻に低下させる可能性がある	分単位から時間単位	IT の不具合による駐屯地での停電
中間	システム又は要素の不具合が、システムのミッション/ビジネスの部分的または特定可能な能力を低下させる可能性がある	時間単位から日単位	IT システムの不具合による都市交通信号の機能喪失
低い	システム又は要素の不具合が、不都合をもたらす可能性がある	日単位	

上の表によって決定された重要性レベルに応じて、必要なソフトウェアアシュアランスを与える必要があり、ソフトウェアの重要性のレベルについては、”DoD Instruction 8500-2”が各々の定義を与えているとしている。

2.1.4 大統領のサイバーセキュリティ・イニシアティブにおけるサプライチェーン課題

2009 年 10 月、オバマ大統領はサイバーセキュリティに対する包括的な政策を発表した

（Comprehensive National Cybersecurity Initiative＝CNCI）。このなかで大統領府は米国のサイバーセキュリティに関わる 12 の課題を指摘し、国家政策の焦点を明らかにしている。「サプライチェーンのリスク管理」は、第 11 番目の課題として登場している。下の図表 2.6 に CNCI の指摘する 12 の課題を掲げる。

図表 2-6　CNCI の掲げるサイバーセキュリティ 12 の課題

#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

The Comprehensive National Cybersecurity Initiative、white house, Oct. 2009
http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative

#11 のサプライチェーンのリスク管理については、「サプライチェーンをよりよく管理し、リスクを緩和する強固なツールセットを提供し、連邦政府の技能、政策、プロセスを強化する」ことが目標として掲げてられている。

2.1.5 NISTIR 7622 文書（DRAFT）

2010 年 6 月、NIST は「連邦情報システムのためのチェーンリスク管理の実施を先導する」と題する NIST IR(Interagency Report)7622 の DRAFT（草案）を公表した。NISTIR 7266 は草案とはいえ、現時点においてサプライチェーンのセキュリティに関する最新文献であり、サプライチェーンリスク管理に関する極めて詳細な文書となっているので、本項でその概略をやや詳細に紹介する。

この報告書は 3 章構成になっており、1 章で報告書の性格を紹介し、2 章がサプライチェーンリスク管理の手段、3 章がサプライチェーンリスク管理の対策となっている。以下、

各章ごとに図表の形で大略を抄訳する。

図表 2-7　NISTIR 7266 の目的、対象、背景、ライフサイクル基準、前提条件

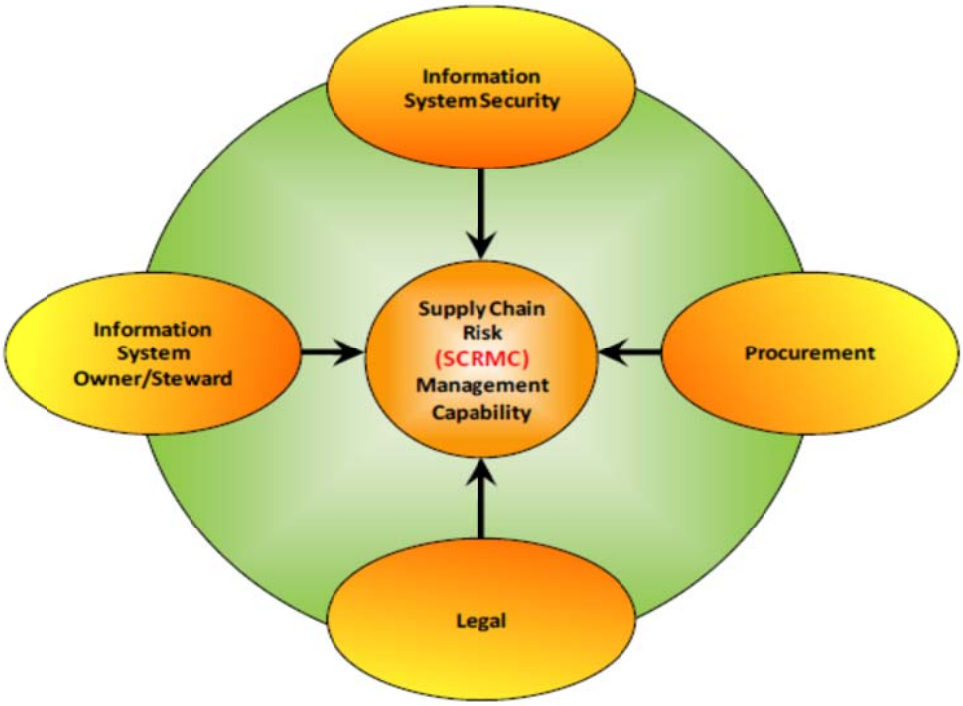
1.1 目的	本書の目的は、連邦政府規定によりインパクトレベルが高いと区分された情報システムへのサプライチェーンの脅威を低減するための対策リストを提供すること。
1.2 対象	サプライチェーンには、製品のライフサイクルである設計、開発、調達、システム統合、システム運用及び廃棄が含まれる。人、プロセス、サービス、製品やその構成要素は、すべてサプライチェーンに影響しうる。本書は、そのようなライフサイクルを通じたサプライチェーンリスクへの対処を対象とする。
1.3 背景	これまで本報告書で記述してきたので省略する
1.4 ライフサイクル基準	ライフサイクル基準については NISTSP 800-64 Rev2 Security Considerations in the System Development Life Cycle を参照する。 http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf
1.5 成功するサプライチェーンリスク管理の前提条件	サプライチェーンリスクマネジメントを効果的に実施するには、システム設計や運用の基本的な取組が前提となる。例えば、セキュリティ要件をライフサイクルの初期から組み込むこと、途中経過を適切に記録すること、危機管理計画にサプライチェーンを位置付けること、委託先を適切に管理すること等が前提となる。

2-8 NISTIR 726 の示すサプライチェーンリスク管理の手段

2.1 サプライチェーンリスク管理能力	サプライチェーンリスクマネジメントを機能させるには、情報システムセキュリティ、情報システム管理、調達、法務の各部門によるチームアプローチが必要である。
2,2 役割と責任	サプライチェーンに関わる役職や部門には次のようなものがある：経営者、CIO、契約管理者、契約担当者（技術担当）、法務アドバイザ、リスク担当役員、事業責任者・担当者、情報システム管理者、CISO、情報システムセキュリティ管理者、IT 投資役員会。
2.3 サプライチェーンリスク管理能力の実施	サプライチェーンリスクマネジメント機能の実施に当たっては、第 1 に、サプライチェーンリスクを特定し、コスト、性能、スケジュール等のリスクとのトレードオフを行ってサプライチェーンリスクマネジメントに関する要求を定める（第 3 章は、サプライヤやインテグレータに対する一般的な又は技術的な要求のソースとして使用できる）。第 2 に、可能性

	のあるサプライヤを特定し、市場分析を行う。第 3 に、調達、計画、実施、契約について法務部門や調達部門と調整を行う。それ以降も継続的にリスクマネジメントのモニタリングを行うことが必要である。連邦政府規定によりインパクトレベルが高いと区分された情報システムは、上記すべてを実施しなくてはならない。

図表 2-8 NISTIR 7266 の図示するサプライチェーンリスク管理能力



図表 2-9　NISTIR 7266 の示すサプライチェーンリスクマネジメント対策

3.1	インテグレータとサプライヤの活動を調達者から見て最大限可視化する
3.2	使用している構成要素の機密性を守る
3.3	サプライチェーンの保証を要求に組み込む
3.4	信頼性の高い構成要素を選定する
3.5	多様性を取り入れる
3.6	重要なプロセスと構成要素を特定し、防護する
3.7	防護性の高い設計にする
3.8	サプライチェーン環境を防護する
3.9	構成要素へのアクセスや公開を制限するシステム構成にする
3.10	外部サービスの利用やメンテナンスを正規に扱う
3.11	システム開発のライフサイクルを通じて試験を実施する
3.12	システム構成を管理する

3.13	人をサプライチェーンの一部と考える
3.14	サプライチェーンに関する意識啓発、人の教育・訓練を行う
3.15	サプライチェーンの配送メカニズムを強化する
3.16	運用システムを防護し、モニタし、監査する
3.17	要求の変更について交渉する
3.18	サプライチェーンの脆弱性を管理する
3.19	ソフトウェア更新時やパッチ適用時のサプライチェーンリスクを低減する
3.20	サプライチェーンインシデントに対応する
3.21	廃棄時のサプライチェーンリスクを低減する

2 .1.6　日本企業に関わる米軍サプライチェーンの情報セキュリティ課題の一事例

この項では、調達システムオープン化およびそのサプライチェー問題の一例として、米国空軍研究所のスーパーコンピュータシステムに関わる事例を紹介する。

米国ニューヨーク州ローマ市に立地する空軍研究所は、そのスーパーコンピュータシステムの演算クラスタの一部として、約1700台のソニー製PS3（各160GB）を購入し、Linux上で動く500テラFLOPSのスーパーコンピュータクラスタとした。このスーパーコンピュータの用途は、合成開口レーダー（SAR）の画像情報処理である。PS3の購入価格は総額66万3000ドルであり、この価格はインテル社製のXeonを用いたクラスタ構成よりも一桁安価なコストであるという。

しかし、米空軍が購入契約を結んだ数カ月後、SonyはPS3のOS（gameOS）のアップグレードを行うとともに、今後PS3はLinuxをサポートしないと発表した。空軍研究所のシステムはPS3ネットワークから切り離されているので、自動的にファームウェアを書きかえられる心配はないが、コンポーネントが故障して返送修理をメーカーに依頼した際にファームウェアが書きかえられ、Linuxが動かなくなることが心配されている。下に米空軍スーパーコンピュータシステムの写真と、この問題について論じた２つのメディア記事を情報源として挙げた。

図表 2-10　米空軍スーパーコンピュータシステムの一部に採用された PS3

The initial test cluster (source: US Air Force)]
Air Force may suffer collateral damage from PS3 firmware update,　ars technical, July 2010
http://arstechnica.com/gaming/news/2010/05/how-removing-ps3-linux-hurts-the-air-force.ars
http://www.4gamer.net/games/017/G001762/20101118052/

2.2　欧州における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

2.2.1 ENISA の研究開発課題におけるサプライチェーンの情報セキュリティの提起

ENISA は 2004 年 3 月に設立されたギリシャに本部を置く欧州連合（EU）の機関であり、ネットワークセキュリティ及び情報セキュリティに関する予防・対応能力を促進することを任務としている。EU 加盟国および欧州諸機関へ助言や勧告を行うとともに民間企業や産業関係者との連携を促進している。

その ENISA がサプライチェーンの情報セキュリティに関わる課題を認識し始めたのは、ENISA の文献による限り、2009 年頃からだったように思われる。ENISA は 2009 年の 3 月頃から、次世代のネットワーク関連の技術開発課題を探求する PROCENT（Priorities for Research on Current & Emerging Network Technologies）と称するプロジェクトを推進してきた。ENISA の文献を追う限り、PROCENT のエキスパートグループ（EG）において、サプライチェーンのリスク管理問題が浮上していったようである。
http://www.enisa.europa.eu/act/res/technologies/procent/eg1?searchterm=procent
http://www.enisa.europa.eu/act/res/technologies/procent?searchterm=procent

2.2.2　ENISA Quarterly Review におけるサプライチェーン課題の提起

ENISA は４半期毎のレビュー（ENISA Quarterly Review）を刊行しているが、その 2010 年第１号（2010 年３月発行）において初めてサプライチェーンについての議論が行われている。以下、「サプライチェーンの統合」と題する、スラボミール・ゴルニアクの論文が特筆している「サプライチェーン統合にともなう課題」と「サプライチェーンリスクのキーファクター」を紹介する。同論文は課題として７点、キーファクターとして４点を指摘している。

ENISA Quarterly Review, vol. 6, no. 1
http://www.enisa.europa.eu/publications/eqr/issues/eqr-q1-2005-vol.-6-no.-1

・サプライチェーン統合にともなう幾つかの課題

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 偽造や偽装によるシステムへの侵入を検出し、または打破できる、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。

・サプライチェーンリスクのキーファクター

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

2.2.3　EUの研究開発計画（PRCENT）における「サプライチェーン統合」の登場

2010年の4月、EUは先に触れた研究開発の優先分野を特定したPROCENTと称する情報セキュリティ関連研究開発プロジェクトを公表した。この報告書では、今後３～５年の優先開

発課題として５つの分野が挙げられ、サプライチェーンの統合はその第５番目に登場している。これら５つの分野とは、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、である。なお、⑤サプライチェーン統合に関する課題の詳細については、本報告書の3.2で述べることとする。

“Priorities for Research on Current and Emerging Network Trends”
http://www.enisa.europa.eu/act/it/library/deliverables/procent

2.3　わが国における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

2.3.1 わが国における近年のサプライチェーン問題の認識の推移

経済産業省が「設計と製造の無駄を見える化」を掲げて取り組んできた「サプライチェーン省資源化連携促進事業」のように、わが国ではサプライチェーンは長く物流やモノづくりに関わる問題としてとらえられることが多かった。オープン化・グローバル化が進むサプライチェーンを情報セキュリティ問題と結び付けて考えることは、最近に至るまでほとんど行われてこなかった

2.3.2 「第２次情報セキュリティ基本計画」におけるサプライチェーン課題の認識

わが国の情報セキュリティに関する基本プランは「情報セキュリティ基本計画」であるが、2006 年の「第１次基本計画」においてはサプライチェーンのセキュリティへの言及はまったくなかった。その後 2009 年２月に樹立公表された「第２次基本計画」において、幾つかの箇所でサプライチェーンの情報セキュリティについての論及がなされるに至った。

サプライチェーンの課題は、対策実施４領域の「企業」の項、横断的な情報セキュリティ基盤の「国際連携・協調」の推進の項で、「企業の領域においては、グローバル化に伴う企業活動の細分化、専門化が更に進展し、海外へのアウトソーシング、直接投資が拡大している。製品・サービスは、少なからぬ部分が IT を活用したグローバルなサプライチェーンを経て製造、提供されている。経済活動は国家の領域を超えて行われており、世界における情報セキュリティ対策の推進という観点から、グローバル企業の果たす役割は拡大している」と言及されている。この時点においては、サプライチェーンは、主としてグローバルな企業活動の問題として認識されていたように思われる。

http://www.nisc.go.jp/active/kihon/pdf/bpc01_ts.pdf
http://www.nisc.go.jp/active/kihon/pdf/bpc02_ts.pdf

2.3.3　「サイバーセキュリティと経済」研究会におけるサイバーセキュリティ課題の認識

2010 年 12 月に第１回が開催された経産省の「サイバーセキュリティと経済」研究会では、検討課題として 5 つの項目が掲げられている。①標的型攻撃への対処、②制御システムの安全性確保、③企業等の機密漏えい対策、④サイバーセキュリティ産業の強化、⑤そ

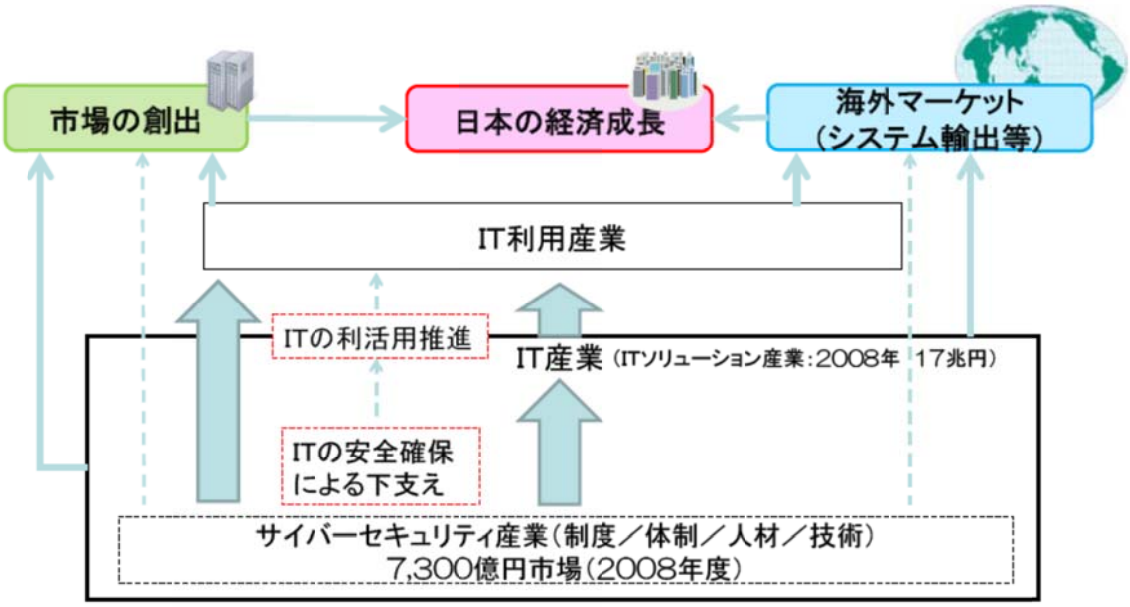
の他の論点。以上５つの論点では、サプライチェーンのセキュリティ問題は特に取り上げられていない。

なお、同研究会の委員の一人からサプライチェーンに関わる問題を提起しているので、3.3.1 の項で特記して報告する。

http://www.meti.go.jp/committee/kenkyukai/shoujo/cyber_security/001_04_00.pdf

同研究会の第１回会合で、経済産業省商務情報政策局が配布した資料に掲載された下の図表 2-11 は、「サイバーセキュリティ産業と経済の関係に関わる課題と題された概念図」である。ここではサイバーセキュリティ産業の強化を、サイバーセキュリティ産業、IT 産業、IT 利用産業の育成を通じて、市場の創出、経済成長、システム輸出等を通じての海外市場へ進出という形で、わが国の経済成長に結び付けるという方向性が示されている。

図表 2-11　経産省配布資料によるサイバーセキュリティ産業と経済に関わる課題



http://www.meti.go.jp/committee/kenkyukai/shoujo/cyber_security/001_05_00.pdf

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

3.1　米国における考察

3.1.1　サイバーセキュリティ・イニシアティブにおけるサプライチェーン関連技術開発

本報告書 2.1.4 で書いたように、米国ではホワイトハウスの主導下で、Comprehensive National Cybersecurity Initiative＝CNCI が推進されており、その第 11 項が「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」であった。この研究開発項目について、CNCI の記者発表では、次のように語られている。

「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」。

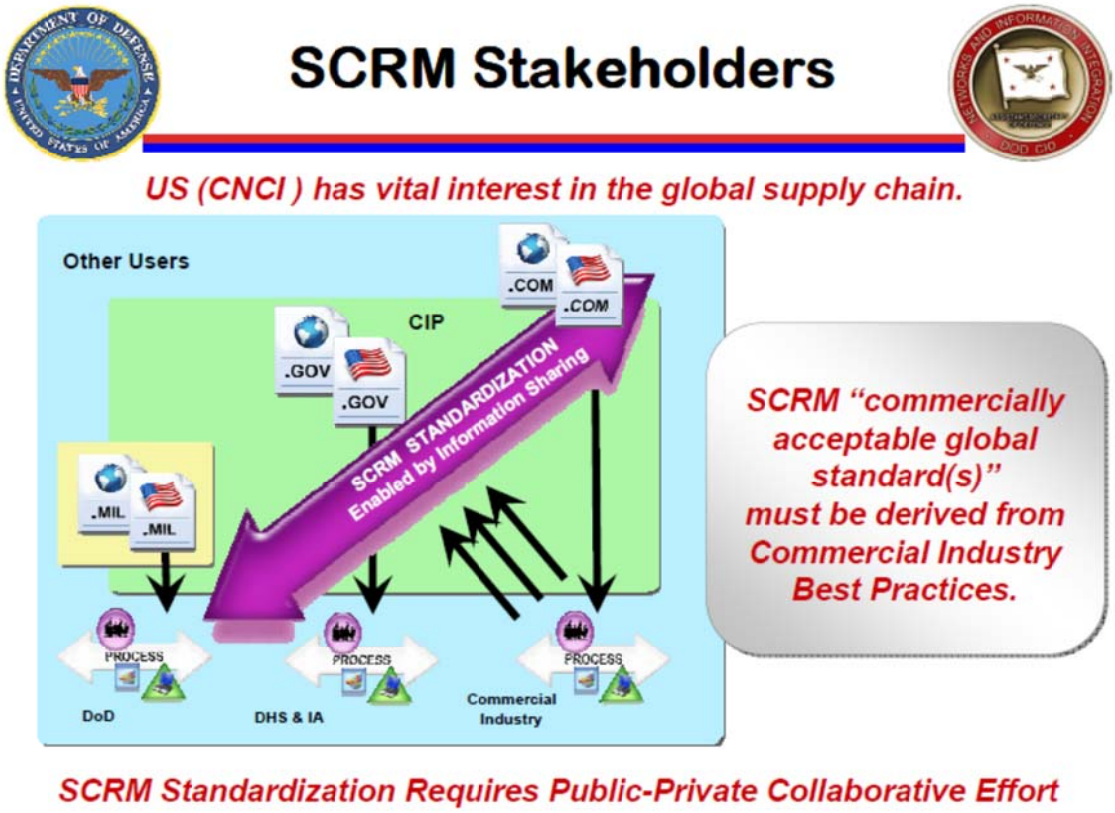
なお、CNCI の 12 項目の研究開発は、HSPD-23（国土安全保障大統領令-23）及び NSPD-54（国家安全保障大統領令-54）という形の大統領令として実施されているが、研究開発の詳細は極秘扱いとなっている。

3.1.2 国防総省の視点から見たサプライチェーンリスク管理の標準化

2010 年 9 月、米国防総省の ICT サプライチェーンリスク管理担当者であるドン・デイビッドソンは、ソフトウェア保証（SwA）フォーラムにおいて、3.1.1 で紹介した CNCI を受けて、SCRM（サプライチェーンリスク管理）とその標準化について、下の図表 3-1 に示したプレゼンテーションを行っている。

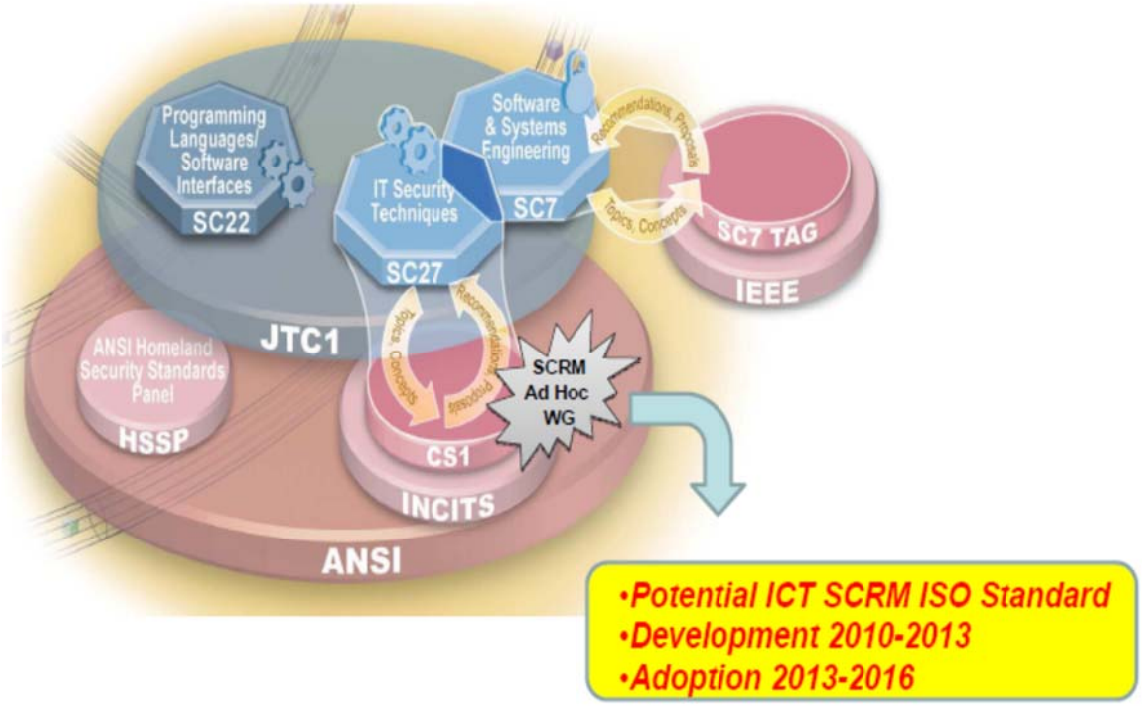
図の右側に書かれているように、サプライチェーンのリスク管理は、「民間産業のベストプラクティスから導き出された民間が受容できるグローバル標準でなければならない」とディビッドソンは強調している。

図表 3-1　国防総省の見るサプライチェーンリスク管理と標準化



さらに、デイビッドソンは、サプライチェーンリスク管理について、下の図のような標準化の方向性を示すとともに、大まかな開発期間（2010－2013 年）と採用の時期（2013-2016 年）を示している。

図表 3-2　国防総省の示すサプライチェーンリスク管理の標準化



https://buildsecurityin.us-cert.gov/swa/presentations_2010_10/02_Tuesday/11a_Don_Davidson_nist_28sep.pdf

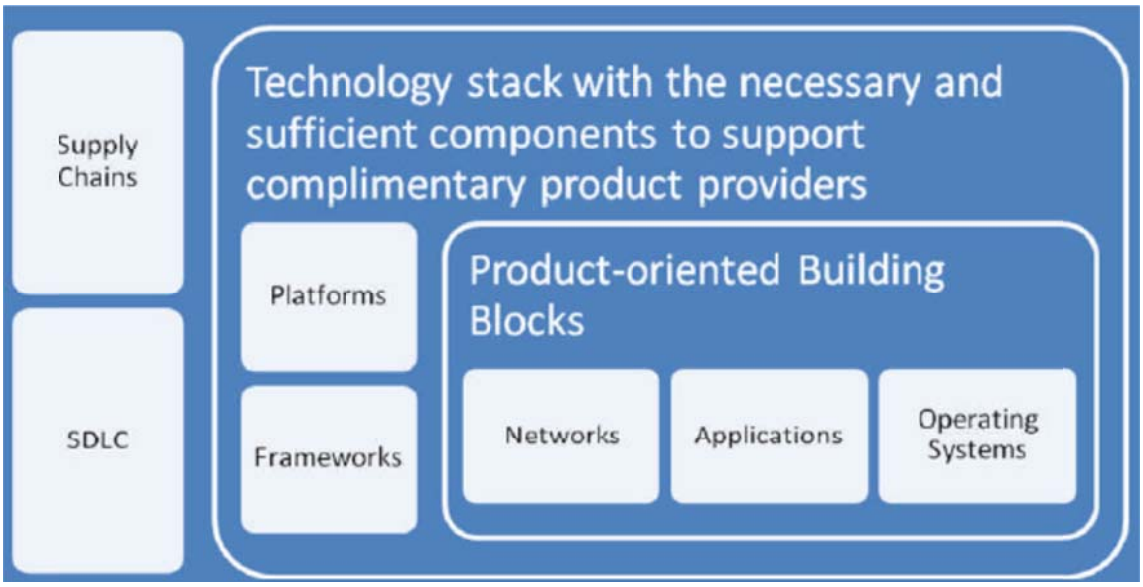
'

3.1.3　IT 技術の歴史的発展から見たサイバー・サプライチェーンへの一考察

米国メリーランド大学ビジネス大学院のロバート・H・スミス教授は、2009 年 6 月に発表した「Building A Cyber Supply Chain Assurance Reference Model」と題する論文で、サプライチェーンのサイバーセキュリティを IT 技術発展の最新のビジネスモデルとして論じている。純民間から提出された一つの視点として本項で紹介する。

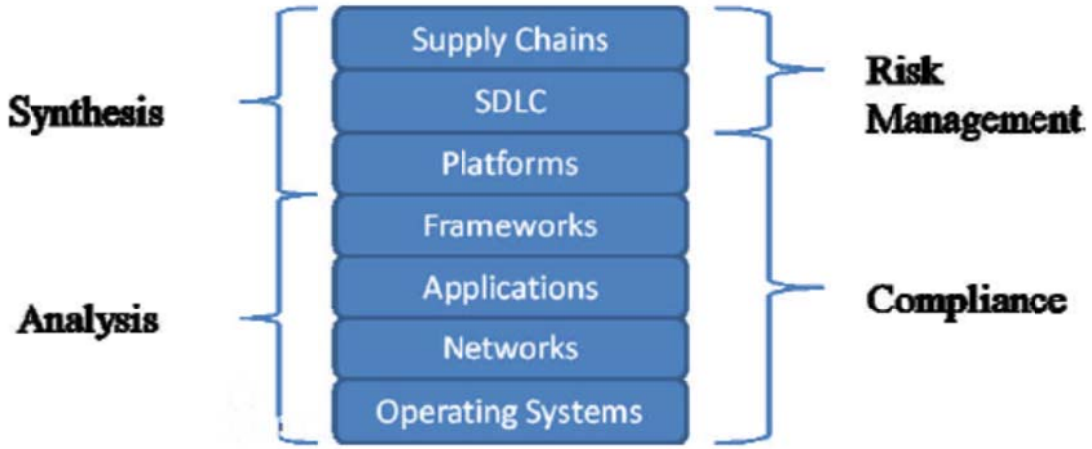
同教授は、OS、アプリケーション、ネットワーク、フレームワーク、プラットフォームと、ビジネスモデルが順次高度化するなかで、次世代のビジネスモデルとして、SDLC（System Development Life Cycle＝システム開発のライフサイクル）としてサプライチェーンを位置付けている。

図表 3-3　エンド・トゥ・エンド・ビジネスモデルのパラダイムシフト



また、同教授は、上の図を縦方向に積み重ねた下の図表 3-4 を示し、IT 市場がコンプライアンスとアナリシスから、統合力（シンセシス）とリスク管理へというヒエラルキーを形成する方向に向かうだろうと予測している。

図表 3-4　コンプライアンスとアナリシスから統合とリスク管理へのサイバー市場のフォーカスシフト



Building A Cyber Supply Chain Assurance Reference Model
http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2009-04/ispab_sboyson-hrossman_april2009.pdf

3.2　欧州における考察

3.2.1 欧州サイバー研究開発計画におけるサプライチェーン統合についての記述

本報告の2.2.3で触れたように、EUは2010年4月に公表した情報セキュリティに関わる研究開発計画（PROCENT）において、「サプライチェーンの統合」を第5番目の研究開発課題として提起している。原報告書では、サプライチェーンの統合に関する部分だけでも10ページに及んでいるので、ここではその部分の構成のみを紹介することとする。

「サプライチェーンの統合」

①問題の紹介

②取組まれる課題

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

上の各項のうち、⑦現在のリスクと新しい研究機会において取り上げられている7個の項目をここに紹介する。

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

“Priorities for Research on Current and Emerging Network Trends”

http://www.enisa.europa.eu/act/it/library/deliverables/procent

3.3　わが国における考察

3.3.1　「サイバーセキュリティと経済」研究会における山口委員の議論

サイバーセサプライチェーンの情報セキュリティ問題について、わが国の認識や対策は先進的であるとは言い難いが、制御システム（スマートグリッドを含む）のセキュリティなどとならんで、今後重要な情報セキュリティ課題として世界的なトピックとなっていくことは疑いをえないと思われる。

わが国ではこの課題についての議論はほとんど行われていないが、ここでは 2.3.3 で述べた「サイバーセキュリティと経済」における山口委員の意見を紹介する。同研究会の第 1 回会合には、３名の委員から意見が提出されているが、なかでも奈良先端科学技術大学院大学の山口英教授の「本研究会が議論すべき領域について」で、サプライチェーンについて特出して論じているので下に引用する。

「第四に、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が、このような柱を設定しないのは、通商政策、あるいは、産業政策を持つ経産省の研究会としては、適切であろうか。サプライチェー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」（下線は原文のママ）。

また、同教授は「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。そこで、そもそも内需は存在しないという前提、すなわち、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」（下線は原文のママ）とも発言されている。

重要インフラ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課題の重要性を指摘するとともに、わが国情報セキュリティ産業の国際化を考える必要性を訴えた数少ない議論の一つとしてここに引用した。

４．今後の取り組みに向けた提言

①サプライチェーンの情報セキュリティ課題の認識

重要インフラに係るサプライチェーンの情報セキュリティ問題が今後の国家的セキュリティ課題であるとの認識を、政府（NISC、重要インフラ所管官庁）や重要インフラ事業者などが共有し、この課題が情報セキュリティ政策会議における重要アジェンダとして取り上げられることが望ましい。

②サプライチェーン課題の先進国・地域の情報収集

サイバー・サプライチェーン問題への対応と対策について、わが国より先行している米国、EU、あるいは欧州各国のインシデント事例、インシデント対策、グッドプラクティス、標準化、研究開発などの現状について、広く情報収集に当たること。

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

セキュリティインシデントの発生＝不祥事＝当事者の責任問題という考え方が、日本では長く定着している。「国民を守る情報セキュリティ戦略」（2010 年 5 月、情報セキュリティ政策）が指摘する、「事故前提社会」という認識を共有することが、決定的に重要な段階に入っている。サプライチェーンのリスク管理についても同様な視点が必要である。

④インシデント事例共有が必要

どのレベルまでどういう形で公開するかは別として、サプライチェーンの情報セキュリティに係るわが国のインシデント事例を、NISC、所管官庁、事業者の間で透明性の高い形で共有するシステムが今後ますます必要になると思われる。RISI のような形のデータベース機関の設立や、低レベル情報の一般公開、ハイレベル情報の機密化などの手法も考えられる。また、IPA や JPCERT/CC のような既設組織の強化なども対策の一つかもしれない。

⑤産学官による集中的な課題検討の実施

わが国が総力を挙げて取り組むべき情報セキュリティ課題の特定が行われるなかで、その重点課題の一つにサプライチェーンの情報セキュリティが挙げられるべきである。サプライチェーンの情報セキュリティについて、官・学・産が集中して課題検討を実施する場を設けることが望ましい。

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

情報セキュリティに関わる人材の不足が深刻である。サプライチェーンに限らず情報セキュリティ人材の育成に政府の協力は欠かせない。政府自身による人材雇用や、継続的な情報セキュリティ関連のプロジェクトなどを通じて、人材の維持と育成を図ることが必要である。

⑦近い将来のガイドラインの作成を目指すこと

上記の各施策の実施を通じて、サプライチェーンの情報セキュリティについての、ガイドライン等のあり方を検討することが必要となると考えられる。

５．文献一覧

・Draft NISTIR 7622 Piloting Supply Chain Risk Management Practices for Federal Information Systems, June 2010
http://csrc.nist.gov/publications/drafts/nistir-7622/draft-nistir-7622.pdf

・NCSC-TG-002, Trusted Product Evaluation, A Guide for Vendors, March 1988
http://www.fas.org/irp/nsa/rainbow/tg002.htm

・ENGINEERING FOR SYSTEM ASSURANCE Version 1.0 National Defense Industrial Association
http://www.ndia.org/Divisions/Divisions/SystemsEngineering/Documents/Committees/Systems%20Assurance%20Committee/2008/SA-Guidebook-v1-Oct2008-REV.pdf

・1996年情報技術マネジメント改革法
http://govinfo.library.unt.edu/npr/library/misc/s1124.html

・2002 年連邦情報セキュリティマネジメント法
http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

・連邦情報処理規格＝FIPS199
http://www.ipa.go.jp/security/publications/nist/documents/FIPS-200-J.pdf

・連邦情報処理規格＝FIPS200
http://www.ipa.go.jp/security/publications/nist/documents/FIPS-199-J.pdf

・連邦情報システムと組織に推奨されるセキュリティコントロール、NIST 特別出版 800-53 第 3 版、2009 年 8 月
http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf

・National Infrastructure Protection Plan Partnering to enhance protection and resiliency
http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

・ENGINEERING FOR SYSTEM ASSURANCE Version 1.0, National Defense Industrial Association
http://www.acq.osd.mil/se/docs/SA-Guidebook-v1-Oct2008.pdf

・The Comprehensive National Cybersecurity Initiative、white house, Oct. 2009
http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative

・Air Force may suffer collateral damage from PS3 firmware update, ars technical, July 2010
http://arstechnica.com/gaming/news/2010/05/how-removing-ps3-linux-hurts-the-air-force.ars
http://www.4gamer.net/games/017/G001762/20101118052/
http://www.enisa.europa.eu/act/res/technologies/procent/eg1?searchterm=procent
http://www.enisa.europa.eu/act/res/technologies/procent?searchterm=procent

・ENISA Quarterly Review, vol. 6, no. 1
http://www.enisa.europa.eu/publications/eqr/issues/eqr-q1-2005-vol.-6-no.-1

・Priorities for Research on Current and Emerging Network Trends
http://www.enisa.europa.eu/act/it/library/deliverables/procent

・第１次情報セキュリティ基本計画
http://www.nisc.go.jp/active/kihon/pdf/bpc01_ts.pdf

・第２次情報セキュリティ基本計画
http://www.nisc.go.jp/active/kihon/pdf/bpc02_ts.pdf

・経産省「サイバーセキュリティと経済研究会」第１回配布資料４
http://www.meti.go.jp/committee/kenkyukai/shoujo/cyber_security/001_04_00.pdf
・同上、配布資料５
http://www.meti.go.jp/committee/kenkyukai/shoujo/cyber_security/001_05_00.pdf

・同上、参考資料１
http://www.meti.go.jp/committee/kenkyukai/shoujo/cyber_security/001_s01_00.pdf

・CyberSecurity, US CNCI-SCRM, Public-Private STANDARDIZATION, Don Davidson, Sept. 2010
https://buildsecurityin.us-cert.gov/swa/presentations_2010_10/02_Tuesday/11a_Don_Davidson_nist_28sep.pdf

・Building A Cyber Supply Chain Assurance Reference Model
http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2009-04/ispab_sboyson-hrossman_april2009.pdf

・Priorities for Research on Current and Emerging Network Trends
http://www.enisa.europa.eu/act/it/library/deliverables/procent