米国のサプライチェーンのセキュリティ対策（3）
―Second Draft NIST SP800-161―

客員主任研究員　横山　恭三

はじめに

米国・国立標準技術研究所（National Institute of Standards and Technology：NIST）は、2014 年 6 月 3 日にパブリックコメントを求める Second Draft NIST Special Publication 800-161 として「連邦政府のための情報システム及び組織のサプライチェーン・リスク・マネージメント・プラクティス（Supply Chain Risk Management Practices for Federal Information Systems and Organizations）」を公表した。因みに、パブリックコメントの提出期限は 2014 年 6 月 3 日から 2014 年 7 月 18 日の間であった

筆者は、拙稿「米国のサプライチェーンのセキュリティ対策（第五巻第二号平成 23 年 9 月）」において、「米国は、サプライチェーン・リスク・マネージメント（Supply Chain Risk Management：SCRM）（以下、「SCRM」という）のベストプラクティスの開発を促進している。NIST は、ソフトウェア、ハードウェア、ファームウェア、又は情報システム・サービスの取得の間の SCRM を実行するための方法論をすべての政府組織のために開発している。国土安全保障省は、非国家安全保障システムのための SCRM パイロットプログラムに取り組み、国防総省は国家安全保障システムのための SCRM パイロットプログラムに取り組んでいる」と述べ、米国のサプライチェーンのセキュリティ対策の概要を説明している。

NIST の SCRM プログラムは、2008 年に、「包括的国家サイバー・セキュリティー・イニシアティブ（Comprehensive National Cybersecurity Initiative：CNCI 」の 11 番目のイニシアティブに応えて、非国家安全保障の情報システムのための SCRM の開発を開始したときに始まった。6 年を経て、米国の SCRM は、パブリックコメントを求める段階に至った。

本稿は、第二次草案 SP800―161「連邦政府の情報システム及び組織のためのサプライチェーン・リスク・マネージメント・プラクティス」の骨子を紹介するものである。

なお、第 2 次草案では、サプライチェーン・リスクに代わり、情報通信技術サプライチェーン・リスク（以下、「ICT サプライチェーン・リスク」という）という用語が使用されている。同草案の中で ICT サプライチェーン・リスクは、次のように定義されている。「ICT サプライチェーン・リスクには、ICT サプライチェーンにおける劣悪な開発・製造行為のみならず、偽物の挿入、無認可製造、改ざん、窃取、悪意あるソフトウェアの挿入が含ま

れる。ICT サプライチェーンにおける脅威が既存の脆弱性を利用するとき、これらのリスクは現実のものになる。」

１．NIST

米国・国立標準技術研究所（NIST）の情報技術ラボラトリ（Information Technology Laboratory：ITL）は、国家の評価及び標準に関する基盤に係る分野において技術的リーダーシップを発揮提供することにより、米国の経済と公共福祉に貢献している。ITL は、テストの開発、テスト技法の開発、参照データの作成、概念実証の実施および技術的分析を通じて、情報技術の開発と生産的利用の発展に貢献している。ITL の責務には、連邦政府のコンピュータシステムにおいて、機密ではないものの機微な情報に対する費用対効果の高いセキュリティとプライバシーを実現するための、技術面、物理面、管理面および運用面での標準およびガイドラインを策定することが含まれている。

今回、NIST は、ICTSCRM（情報通信技術サプライチェーン・リスク・マネージメント）の軽減戦略や実装方法に関するガイドラインだけでなく、ツールと評価基準の研究・開発のために、民間及び公的セクターの利害関係者と協力し、第二次草案 SP800―161 を完成させた。

2. 包括的国家サイバーセキュリティ・イニシアティブ（CNCI）

2008 年 1 月に、米国政府が発表した大統領令第 54／第 23 号（National Security and Homeland Security Presidential Directive：NSPD54／HSPD23）「包括的国家サイバーセキュリティ・イニシアティブ（CNCI）」には、3 つの目標と 12 のイニシアティブが示されている。その 11 番目のイニチアティブが「グローバル・サプライチェーン・リスク・マネージメントのための複数方面からのアプローチを開発する」である。そして、CNCI では、何故、サプライチェーンのセキュリティ対策が重要なのかについて次のように述べている。

「情報通信技術（ICT）市場のグローバル化は、米国に害を与えようとする者に、無許可のアクセス、データの改ざん、又は通信を妨害するためにサプライチェーンに侵入する機会を増加させている。国内及びグローバル化されたサプライチェーンに起因するリスクは、製品、システム、及びサービスの全ライフサイクルを通して、戦略的かつ包括的な方法で管理されなければならない。このリスクを管理することは、リスク、脆弱性、及び調達に関する包括的な認識を必要とする。即ち、①設計から破棄までの製品のライフサイクル全体で、技術的及び運用上のリスクを軽減するためのツールと資源の開発と使用、②複雑なグローバル市場を反映した新しい調達政策及び手順の開発、③SCRM の標準規格並びにベストプラクティスを開発・適応するための企業との協力。」

今回の第二次草案も CNCI の指示に沿った形で作成されている。

3．Draft IR7622[1]

NIST は、2010 年 6 月、Draft IR7622「連邦情報システムのための試験的な SCRM プラクティス（Piloting Supply Chain Risk Management Practices for Federal Information Systems)」を公表した。

この草案は、3 章構成になっており、1 章で草案の性格を紹介し、2 章が SCRM の実践、3 章が SCRM プラクティスとなっている。3 章では、SCRM プラクティスとして、次の 21 個の活動が提示されている。

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可視化する。
②使用している構成要素の機密性を守る。
③サプライチェーンの保証を要求に組み込む。
④信頼性の高い構成要素を選定する。
⑤多様性を取り入れる。
⑥重要なプロセスと構成要素を防護する。
⑦防護性の高い設計にする。
⑧サプライチェーン環境を防護する。
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。
⑩外部サービスの利用やメンテナンスを正規の活動として扱う。
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。
⑫システム構成を管理する。
⑬人をサプライチェーンの一部と考える。
⑭サプライチェーンに関する意識啓発、教育・訓練を行う。
⑮サプライチェーンの配送メカニズムを強化する。
⑯運用システムを防護し、モニターし、監査する。
⑰要求の変更について交渉する。
⑱サプライチェーンの脆弱性を管理する。
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。
⑳サプライチェーン・インシデントに対応する。
㉑廃棄時のサプライチェーン・リスクを低減する。

4．Second Draft SP800―161

（1）背景[2]

既述したが、NIST の ICT SCRM プログラムは、2008 年に、包括的国家サイバー・セキュリティ・イニシアティブ（CNCI）の 11 番目のイニシアティブに応えて、非国家安全保障の情報システムのための ICTSCRM の開発を開始したときに始まった。CNCI

[1]http://csrc.nist.gov/publications/drafts/nistir-7622/draft-nistir-7622.pdf
[2] NIST ファクトシート http://csrc.nist.gov/scrm/documents/nist_ict-scrm_fact-sheet.pdf

の 11 番目のイニシアティブは「世界的なサプライチェーン・リスク管理のために多角的なアプローチを開発する」というものであった。

NIST は、国防省と共に「CNCI 11 ワーキング・グループ 2（ライフサイクルプロセスと標準化)」の共同責任者を務めた。ワーキング・グループ 2 は、産業界と協力して、サプライチェーン・ツール、資源、及びリスク・マネージメント・プラクティスを開発する責任を負った。

NIST は、連邦機関の ICTSCRM を手助けするために、複雑な世界的な市場を反映した基礎的・反復可能・実行可能なプラクティスを開発するために、学界、産業界及び政府を越えて多様な利害関係者と密接に協力した。NIST は、①政府へ納入する民間セクターのサプライヤの ICTSCRM の現状の調査、②ICTSCRM の戦略及びイニシアティブの特定及び分析、③ウェブ・ベースのリスク評価並びに④共同ツールの開発の 4 件に補助金を支出した。そして、2012 年 10 月に、IR7622「連邦情報システムのための概念的サプライチェーン・リスク・マネージメント・プラクティス」を公表した。それには ICT SCRM の方法論とプラクティスが含まれている。この文書は 2010 年 10 月に発表された Draft IR7622「連邦情報システムのための試験的な SCRM プラクティス（Piloting Supply Chain Risk Management Practices for Federal Information Systems)」を更新したものである

また、NIST は、2 日間のワークショップを開催し、ICTSCRM の基礎の構築に利害関係者を関与させた。そのワークショップでは、現状と必要とされるものの特定、商業的に合理的な ICTSCRM の標準とプラクティス、ツールとテクノロジーとテクニック、そして、研究のリソースが議論された。このワークショップは、ICTSCRM に関する NIST の現在の研究の基礎を設定し、第二次草案 SP800-161 の策定の方向性を明確に示した

（2）策定方針[3]

意図的であるか意図的でないにせよ、組織はますますサプライチェーン危殆化（supply chain compromise）のリスクにさらされている。

> ICT サプライチェーン危殆化（ICT supply chain compromise）とは、ICT サプライチェーンの中で、敵対者がシステム又はシステムが処理、保管若しくは送信する情報の機密性、完全性又は有用性を危うくすることである。ICT サプライチェーン危殆化は、製品又はサービスのシステム開発ライフサイクルのどこででも起こり得る。（第二次草案 SP800-161 から）

ICTSCRM は、その製品及びサービスの品質を確保しつつ、サプライチェーンの完全性、セキュリティ及びレジリエンス（回復力）を確保することを要求する。

NIST は、次の主要な事項を含む ICTSCRM の策定方針を開発した。

[3]NIST ファクトシート http://csrc.nist.gov/scrm/documents/nist_ict-scrm_fact-sheet.pdf

●既存の基礎的プラクティスを活用する。

ICTSCRM は、情報セキュリティとサプライチェーン・マネジメントの交わる部分に位置する。既存のサプライチェーンとサイバー・セキュリティ・プラクティスは、効果的な ICTSCRM プログラムを構築するため基礎を提供する。

●組織全体の関与を重視する。

効果的 ICTSCRM は、組織の各層（経営陣、事業プロセス、及び情報システム）が関与する組織全体の活動として、システム開発のライフサイクルを通して実行される。

●リスク・マネージメント・プロセスの一部として実行する。

ICTSCRM は、NIST SP 800-39「情報セキュリティ・リスクのマネージング（Managing Information Security Risk）」で述べられているように、リスク・マネージネント活動の一部として実行されるべきである。

活動には、対処すべきリスクを特定・評価し、適切な軽減措置を決定し、選択された軽減戦略を文書化した ICTSCRM 計画を作成し、そして、その計画の履行状況を監督する。ICT サプライチェーンは、それぞれの組織で異なるので、ICT SCRM 計画は、個々の組織の現状に適合されたものでなければならない。

○リスク：ICT サプライチェーンのリスクは、連邦政府機関が取得する ICT 製品とサービスの開発と輸送に係る多くのプロセスと意思決定の可視化・理解度・監督の不足に関連している。

○脅威と脆弱性

効果的な SCRM は、脅威と脆弱性に対する綜合的な視点を必要とする。脅威は、「敵対的」（例えば、不正工作する、偽造する）又は「敵対的でない」（例えば、低品質、自然災害）のいずれかである。脆弱性は、「内部」（例えば、組織的手順）又は「外部」（例えば、組織のサプライチェーンの一部）であるかもしれない。

●重要システムの特定

費用効果がよいサプライチェーンのリスク軽減には、最も脆弱であり、かつ危殆化された場合に組織に甚大な影響をもたらすシステム／コンポ―メントを特定することが必要である。

（3）Second Draft SP800―161 の構成・内容[4]

この第二次草案は 3 章構成になっており、第 1 章「導入」では、目的、背景などの同草案の性格の説明と 13 項目の基礎的 ICTSCRM プラクティスを提示している。第 2 章「ICT SCRM を組織全体のリスク・マネージメントへの統合（INTEGRATION OF ICT SCRM INTO ORGANIZATION-WIDE RISK MANAGEMENT）」では、リスク・マネージメント・プロセスにおける ICTSCRM 活動の内容が説明されている。第 3 章「ICT SCRM 対策（ICT

[4]http://csrc.nist.gov/publications/drafts/800-161/sp800_161_2nd_draft.pdf

SCRM CONTROLS)」では、セキュリティ対策（security controls）について、13 の大項目（見出し）とそれ関連する合計 78 項目の対策が説明されている。そして各対策には ICT SCRM へ適用する場合のガイダンスが記述されている。

> セキュリティ対策（security controls）とは、「管理、運用及び技術的なコントロール（すなわち、保護措置又は対策）は、情報システムにとっての、システムとその情報の機密性、完全性及び有用性を保護するための処方箋である」と定義される。

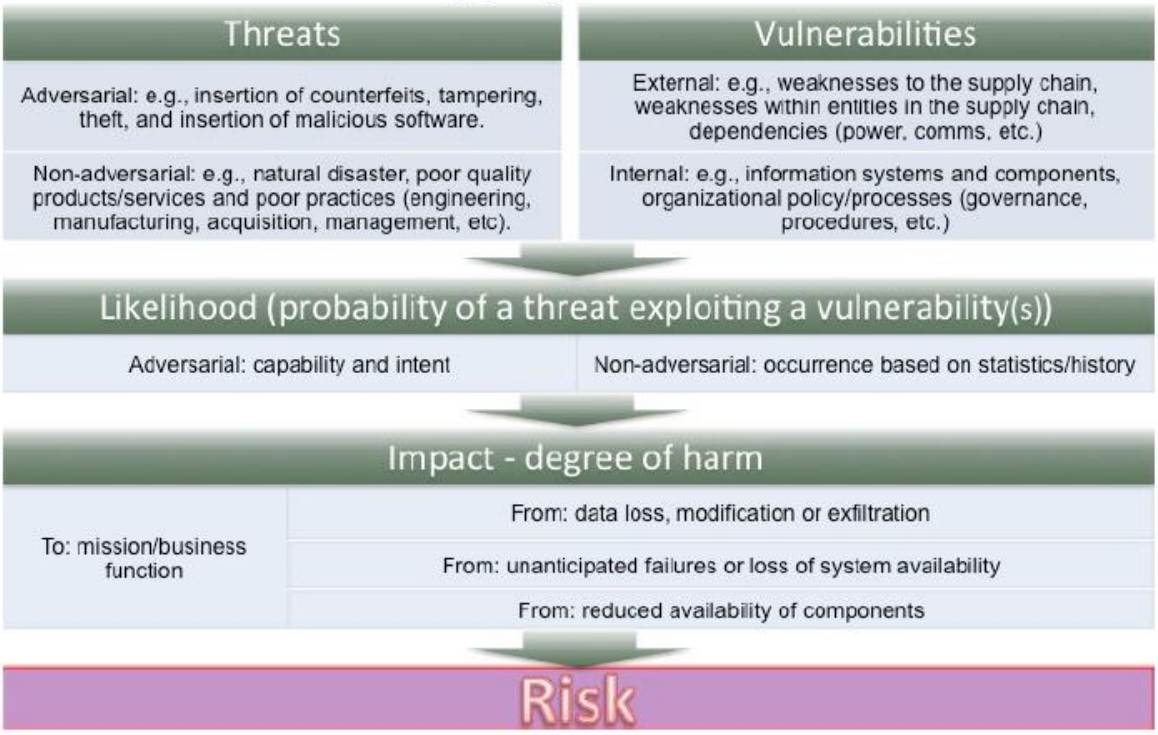
以下、各章ごとに主要な事項について述べる。

ア．第 1 章の主要な事項

（ア）ICT サプライチェーン・リスク

ICT サプライチェーン・リスクには、ICT サプライチェーンにおける劣悪な開発・製造行為のみならず、偽物の挿入、無認可製造、改ざん、窃取、悪意あるソフトウェアの挿入が含まれる。ICT サプライチェーンにおける脅威が、既存の脆弱性を利用するとき、これらのリスクは現実のものになる。図 1 は、脆弱性を利用する対象脅威の公算と被害の程度から生じる ICT サプライチェーン・リスクを描写している。

図 1　　ICT サプライチェーン・リスク[5]



イ．基礎的プラクティス

[5]NISTSP800－161 第 1 章ページ 7
http://csrc.nist.gov/publications/drafts/800-161/sp800_161_2nd_draft.pdf

以下は、先進的なICTSCRM方策を開発・実行する組織の能力を向上させるために実践することができる分野横断的な基礎的プラクティスの具体的な例である。

①リスク・マネージメント体系と（NIST SP 800-39に基づく）リスク・マネージメント・プロセスを実践する。それには組織全体の（NIST SP 800-30に基づく）リスク評価プロセスが含まれる。

②各部門からのICTSCRM要求事項（リクワイアメント）を統合し、これらの要求事項を組織の政策に組み入れる組織統治構造を確立する。

③FIPS 199「連邦政府の情報及び情報システムのカテゴリー化のための基準（Standards for Security Categorization of Federal Information and Information Systems）」のインパクト・レベルを決定するための一貫した、明確に記述された、反復可能なプロセスを確立する。

④定義されたFIPS 199のインパクト・レベルに従いリスク評価プロセスを使用する。それには、致命度解析、脅威解析、及び脆弱性解析が含まれる。

⑤品質保証と品質管理プロセスとプラクティスを含む品質及び信頼性プログラムを実践する。

⑥行動を起こす責任を有する者、行動と結果に責任を有する者、相談及び／又は情報を提供される者を含む意思決定に関与する広範な職員が関与することを確実にするためにICTSCRMの役割と責任を確立する。それらの職員とは、法務官、危機管理監（Risk Executive）、人事、財務、IT事業、プログラム・マネージャー／システム・エンジニア、情報セキュリティ、調達／補給、物流などである。

⑦ガイダンスと規制の適切な実践を確実にするために、十分な資源が情報セキュリティとICTSCRMに割り当てられることを確実にする。

⑧システム工学、ICTセキュリティ・プラクティス及び取得（acquisition）のための一貫した、明確に記述された、反復可能なプロセスを実践する。

⑨NIST SP 800-53 修正版4「連邦政府の情報システムと組織のためのセキュリティとプライバシー規制（Security and Privacy Controls for Federal Information Systems and Organizations）」の中の適切かつ適合した情報セキュリティ基準を実践する。

⑩セキュリティと品質要求事項の整合性を確実にするために内部部門の互いの抑制と均衡を確立する。

⑪資格のある相手先商標製造会社（OEM）又は許可を受けた卸売業者及び再販業者から直接購入するためのガイドラインを含むサプライヤ・マネージメント・プログラムを確立する。

⑫サプライチェーンの完全性と信頼性を確実にするために有害事象の間における ICT サプライチェーン・リスクの考慮事項を組み込んだテストされた反復可能な非常事態対応

計画を実践する。有害事象とは、ハリケーンのような自然災害又は労働ストライキのような経済的混乱などである。

⑬セキュリティ・インシデントを特定し、対応し、そして軽減するために、強力なインシデント・マネージメント・プログラムを実践する。このプログラムは、ICT サプライチェーンに由来するインシデントを含むセキュリティ・インシデントの原因を特定できなければならない。

イ．第 2 章の主要な事項

（ア）ICT サプライチェーン脅威のエージェント（agent）

ICT サプライチェーン脅威のエージェントは、例えば、攻撃者又は産業スパイなど情報セキュリティ脅威のエージェントと類似している。下表は、ICT サプライチェーン脅威のエージェントの例を挙げている。

エージェント	シナリオ	例
偽造者	ICT サプライチェーンに偽物を挿入する。	犯罪グループは、金銭目的で、偽物の ICT コンポーネントを入手し、売却しようとする。具体的には、組織犯罪グループは、灰色市場を通して再販業者に売却できる ICT コンポーネントを手に入れるために、処分された装置を探し求め、余剰品を購入し、そして、設計図を入手する。
インサイダー	知的財産の損失	不満を抱いたインサイダーは、金銭目的を含むさまざまな理由のために、競合他社または外国のインテリジェンス機関に知的財産を販売または譲渡する。知的財産には、ソフトウェア・コード、設計図又は文書が含まれる。
外国のインテリジェンス機関	悪意あるコードの挿入	外国のインテリジェンス機関は、ICT サプライチェーンに侵入し、望まれていない機能（新しい機能又は既存の機能の変更）を埋め込もうとする。その機能は、情報を窃取するため又はシステム若しくは任務活動を妨害するために、システムが稼働している時に使用される。
テロリスト	無許可アクセス（不正アクセス）	テロリストは ICT サプライチェーンに侵入し、望まれていない機能（新しい機能又は既

		存の機能の変更)を埋め込む又はシステム若しくは任務活動を妨害しようとする。
産業スパイ	産業スパイ行為	産業スパイは､情報の収集又はシステム若しくは任務活動を妨害するために ICT サプライチェーンに侵入しようとする。

ウ．第 3 章の主要な事項

（ア）ICTSCRM セキュリティ対策

13 の大項目（見出し）と見出しに関連する合計 78 項目の対策が説明されている。紙幅の都合上、大項目（見出し）のみについて述べる。

①アクセス制御（ACCESS CONTROL）：アカウント管理、最小特権など

②意識向上と訓練（AWARENESS AND TRAINING）：役割基盤のセキュリティ教育など

③監査と説明責任（AUDIT AND ACCOUNTABILITY）：否認防止など

④セキュリティ評価と認可（SECURITY ASSESSMENT AND AUTHORIZATION）：継続した監視など

⑤構成管理（CONFIGURATION MANAGEMENT）：構成変更管理など

⑥緊急事態対処計画（CONTINGENCY PLANNING）：代替保管サイトなど

⑦識別と認証（IDENTIFICATION AND AUTHENTICATION）：識別子管理など

⑧インシデント対応（INCIDENT RESPONSE）：インシデント処理など

⑨整備（MAINTENANCE）：管理保守など

⑩媒体保護（MEDIA PROTECTION）：媒体サニタイジングなど

⑪物理的保護と環境保護（PHYSICAL AND ENVIRONMENTAL PROTECTION）：物理的アクセス制御など

⑫計画（PLANNING）：システムセキュリティ計画など

⑬プログラム管理（PROGRAM MANAGEMENT）：脅威認識プログラムなど

５．米国の認識と対処方策

2012 年 10 月、米下院・情報常設特別委員会（House Permanent Select Committee on Intelligence : HPSCI）は、委員会メンバーが、直接中国に出向き電気通信機器会社であるファーウエイ（華為）と ZTE（中興通訊股分有限公司）の担当者にインタビューした結果等を纏めた報告書（「中国のファーウエイと ZTE によりもたらされる米国の国家安全保障問題に関する調査報告書（Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE」）を公表した。（本報告書については、BSK 第 25-8 号を参照されたい。）

その中で、サプライチェーン攻撃の脅威について次のように述べている。

○悪意のあるハードウェア又はソフトウェアを米国の顧客向けの中国製の電気通信の構成品とシステムに挿入することによって、北京は、危機又は戦争の時に、重要な国家安全保障上のシステムを停止又は機能低下させることができる。
○送電網または金融ネットワークなどの重要インフラに埋め込まれた悪意のあるウイルスは、中国の軍事力の中でも驚異的な兵器となるであろう。
○中国の悪意のあるハードウェア又はソフトウェアは、センシティブな米国の国家安全保障システムに侵入するための強力なスパイ活動の道具でもある。そして、センシティブな企業秘密、先進の研究開発データ及び米国に対して不当な外交的又は商業的優位を得ることに役立つと中国が考える交渉又は訴訟に関する情報が蔵置されている外部と接続されていない米国企業のネットワークへのアクセスを提供する。

諸外国では、サプライチェーン攻撃の脅威は現実のものと考え、さまざまな対応措置を講じている。表1は、米国をはじめ各国の対応措置を取りまとめたものである。

表1　サプライチェーン・リスクに対する諸外国の対応措置

2006年5月	米国務省、レノボから購入した1万6000台のPCについて、機密文書を扱わない業務だけで使用すると発表
2010年5月	インド政府は、一部の中国製通信設備・機器に対して、安全検査を厳格化するなど事実上の輸入禁止措置
2010年11月	ファーウエイは、英国に、第3者の評価チームなどが製品の独立した評価などを実施することが可能な「Cyber Security Evaluation Centre」を建設
2011年11月	米下院情報委員会は、ファーウエイ及びZTEなど中国企業をスパイ疑惑で調査
2012年3月	豪政府、高速通信網の敷設事業入札を巡り、ファーウエイの応札を拒否
2012年10月	米下院情報委員会は、政府に対し、ファーウエイおよびZTE両社の製品を政府の機器から排除するよう提言
2013年7月	英国の政府通信本部（GCHQ）や情報局保安部（MI5）が、レノボ社のパソコンに外部からのリモート操作でパソコン内のデータにアクセスできる工作（バックドア）が施されていたと公表。同時に2000年代半ばに米国、カナダ、豪州、ニュージーランドが同メーカーのパソコンを使用禁止とする通達が出されたとも明かした。（英紙インディペンデントの報道、GCHQはノーコメント[6]）

[6]東京新聞2013年7月31日夕刊

2014 年 5 月	中国政府は、米マイクロソフト社の基本ソフト「ウンドゥズ 8」を政府機関が利用するコンピュータから排除するとともに、IT 関連製品やサービスについて安全審査制度を導入

おわりに

我が国では、これまでサプライチェーンは物流やモノづくりにかかわる問題としてとらえられることが多かった。そのため、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つけて考えることは最近までほとんどなかった。

昨年 6 月に情報セキュリティ政策会議が作成・公表した「サイバーセキュリティ戦略」において、政策文書として初めて、「既知脆弱性への未対応、危殆化された技術の利用やマルウェアを埋め込まれる等のサプライチェーン・リスク」への対応強化が謳われた。

しかし、未だ、政府機関及び企業においてサプライチェーン・リスクの重大性が認識されているとは言えない。例えば、米国等は、中国産 PC を、機密情報を扱う部署から撤去している。しかし、我が国では、中国製電気製品に対する警戒心が欠如している。せめて、機密情報を扱う部署では、中国産 PC や中国産の部品が組み込まれた PC を使用しないくらいの対策が必要である。

情報システムのサプライチェーン・リスクへの対応は、企業だけで出来るものではない。国及び企業が一体となって進めなければならない。我が国も、国がイニシアティブをとり、サプライチェーン・リスクに係る包括的な調査研究を官民共同で実施し、早急に,我が国に適合したサプライチェーン・リスク・マネージメント・ベスト・プラクティスを策定しなければならない時期に来ている。（了）