１Ａ０７
社会セキュリティを目指す研究開発のための技術ロードマッピングの試み

○中島一郎（東北大学）

１．はじめに

情報化あるいはグローバル化の進展にともない、社会・産業活動の秩序や安定性を脅かす新しい問題が意識されるようになった。それらの予防・緊急時対応・復旧・復興については、マネジメント、インフラ・設備整備、技術、行政、国際連携、標準などの立場から多くの取組みが行われている[1]。また、これらの諸活動はセキュリティ産業と言うべき新産業の誕生と成長にもつながるものと考えられている。この新産業に日本がどのような取組みが可能か、技術と研究開発の立場から将来像を探る試みが技術ロードマッピングの手法を応用しながら開始された。その概要を報告する。

２．セキュリティ概念の変遷

セキュリティの概念は時代とともに変遷してきている。1990 年頃までは国際関係の文脈で国家安全保障を論じる場合に用いられることが多かったが、ネットワーク時代の到来とともに情報セキュリティに注目が集まった。OECD は「情報システムとネットワークのセキュリティに関するガイドライン」を 92 年に発表している[2]。

複雑な技術を用いた装置やシステムでは一部の故障や誤操作が重大な事態を招く。この問題を解くべく、リスク評価や安全工学の研究が進められてきているが、それらの安全性やリスク管理とは異なり、情報セキュリティは、コンピュータ・ウィルスやネットワーク犯罪にみられるように人間の何らかの意志に基づく攻撃への対応を扱うものであり、人間や人工物に起因するものであっても何らかの失敗によるものや事故は安全に関するものとして区分すべきだという考え方がある[3]。

2001 年 9 月の米国での同時多発テロ以降、情報システムやネットワークのみでなく、広く産業・社会システムについてのセキュリティが論じられるようになる。米国ではそのための省(DHS[1])の新設をはじめ、公的機関や民間機関での多数の活動が進められるようになる。カトリーナ・ハリケーン、東南アジアでの津波・地震、パンデミックにつながる可能性があるとされる鳥インフルエンザ流行を経て、人間の意志に基づく攻撃に必ずしも限定しない社会セキュリティの考え方が登場する。米国の提唱で始まったセキュリティに関する国際標準審議の場では、”The provision of protection against threats to people, physical assets, infrastructure, information and information technology assets including electronic networks and facilities, and to the movement of people and goods and related facilities.”[4]とされた。自然災害や伝染病、産業施設や社会インフラの火災や事故による支障なども含め、地域社会あるいは国、企業が全組織をあげて取り組む必要があるものを対象としていると言える。

セキュリティ概念はこのようにわずか四半世紀ほどの間に大きな変遷を続けてきており、現時点で国際的に共通のものとして受け入れられた定義があるわけではない。今後も変化していく可能性があるとも言えるが、産業・社会活動の安定性や秩序維持のためには既存の概念では不足している機能があるとするものであり、その機能を実現するには対応する新しい財・サービスが必要となる。

2004 年に発表された OECD 報告書では、セキュリティに対する新しいニーズは大規模で高成長の新産業を興すと指摘している。セキュリティ産業は多様な財・サービスを提供するもので統計的な取り扱いは困難としつつも、世界市場規模は 1,000-1,200 億ドル、成長率は経済成長全体をしのぐ 7-8%、市場の大部分は米国だが、独では 40 億ドル、仏と英ではそれぞれ 30 億ドルの市場と評価している[5]。

３．セキュリティ分野への技術ロードマッピングの応用

技術ロードマッピングの発展の系譜を図 1 に表す。当初は企業内の新製品や新技術の企画手法として考案され、国際半導体ロードマップ(ITRS)や

[1] Department of Homeland Security

英国の自動車展望のように、産業界全体の展望や政策立案の準備としても活用されている。

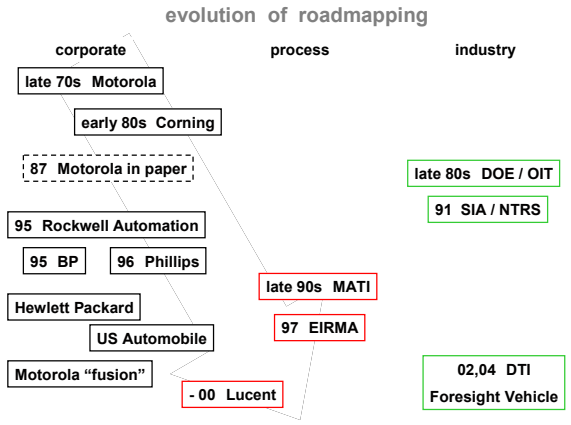

図１　技術ロードマッピングの発展

企業内での新製品開発における技術ロードマッピングでは、図２に模式的に描かれているように、市場、製品、構成技術、研究開発などの多層にわたる相互関係を時間軸上で分析し、これに他社との競争関係や将来にわたる不確実性・リスクなどの分析を加えるものとされている。異なる各層・各分野に属する専門家を集めて実施することが必要になり、企業内といえどもそれぞれの組織論理の違いや専門知識に基づく衝突もありうる。これを見越した上でひとつの見取り図と意思決定オプションを作成していく過程が企業内プランニングには重要であり、技術ロードマッピングの効果である。

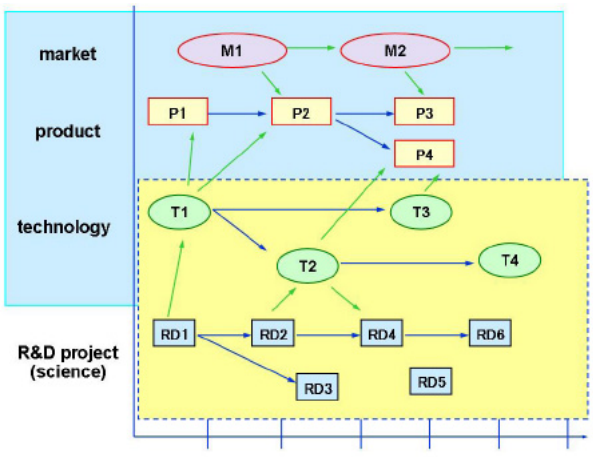

図２　多層的な技術ロードマッピング[6]

技術ロードマッピングを実施する分野が明確であり、層・専門が異なっても分野についての共通認識を持てる場合はこれでよいとして、セキュリティ分野のような新興領域で、これからの成長がどのような方向に向かうかについても明確な見通しがない場合はどのような方策があるだろうか。

成長初期で分野のイメージがまだ明確になっておらず、関係する層や専門領域もどこまで取り込むべきか判断しにくいセキュリティ分野の技術開発の展望を明らかにする作業の第１段階として、まず図３に示したマップの作成から取りかかることとした。

作業は(独)新エネルギー・産業技術総合開発機構(NEDO)の委託事業「セキュリティ技術調査研究」(2007 年度)の一環として、東北大学(中島研究室)と(独)産業技術総合研究所が共同で実施した。

作業の前提は次のようなものである。(1) セキュリティ産業が一応の規模に確立するであろう時期にその中核となっている財・サービスの市場、技術、企業群、それらを取り巻く国際関係や規制等の環境については予断を持って取り組むことを避ける。(2) しかしながら、現時点で入手しうる知識は今後の成長においては極めて初期の未熟なものかも知れないが、可能な限り広い範囲にわたり収集する。(3) こうして収集した技術や知識の単なる索引集になることを避けるため、収集した技術や知識を何らかの統一的なルールで整理する。(4) 収集した技術や知識が、技術ロードマッピング手法でみられるように市場など別の「層」と相互的な関係分析が可能なものかどうか検証を可能な限り試みる。(5) 作業過程での収集される情報は原則的に公開可能なものに限る。

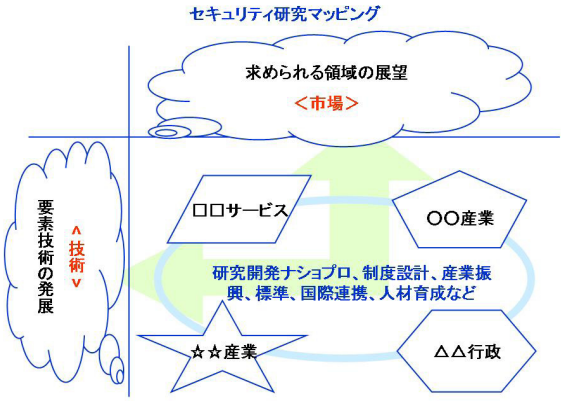

図３　技術ロードマッピングのセキュリティ分野への応用[7]

４．情報の公開範囲と参加メンバーの選定

企業内の技術ロードマッピングとは異なり、企業やその他の組織を超えた場での作業では、その場に出される情報の保秘、参加メンバー選択、成果の公開範囲が常に問題となる。可能な限りの情

報を収集できることは作業が成果をあげる上で重要だが、参加メンバーにとっては相互にどの程度の情報を提供しあうかについての駆け引きが生じる。また、最終成果のどの範囲が公開され、どの範囲が参加メンバー限定のものとなるかは、参加メンバーの動機付けにも大きな影響を与える。

表 1　セキュリティ科学技術政策の進展

2003 年	日米安全・安心な社会の構築に関する科学技術に関するワークショップ開催合意
2004 年	安全・安心な社会の構築に資する科学技術政策に関する懇談会報告（文科省） 第 1 回日米ワークショップ 科学技術基本計画・中目標(国土と社会の安全確保、暮らしの安全確保)
2005 年	第 2 回日米ワークショップ
2006 年	第 3 回日米ワークショップ
2007 年	科学技術連携施策群(テロ対策研究開発)

経済産業省と NEDO が 2004 年度から作成を開始し、2005 年度から発表してきている技術戦略マップの策定過程でもこの問題に何らかの対応をする必要があった。電子情報 6 分野(半導体、ストレージ・不揮発性メモリ、コンピュータ、ネットワーク、ソフトウェア)の 2004 年度の作業では情報は公開されることを前提に作業が進められた。参加メンバーのうち、企業メンバーは NEDO からの大型の研究開発支援先となっていた。いわば関係者による戦略マップ作成ということになる。戦略マップの見通す時間フレームワークの範囲内でこれらの関係者に出入りがないという前提を置けば、こうしたメンバーによる作業は効率的である。メンバーには参加への動機付けがされており、その範囲で機微な情報の提供、意見交換が可能になるからである。

表 2 ANSI/HSSP 対象分野[8]

Radiological/nuclear detectors
Chemical/explosives sensors
Anthrax detectors
Modeling, simulation and analysis
Decontamination standards
Training for emergency responders
Cyber security standards
Interoperable communications
Biometrics for entry/exit program
Certification of equipment/personnel

セキュリティ分野ではこの方法はとれない。将来の産業を構成する財・サービスについての確実な情報が現時点ではなく、それを提供する企業等の組織が誰なのかまだ明らかではないからである。この段階では可能な限り広い範囲の参加メンバーを獲得すべく、提供される情報については公開可能な範囲にとどめることとした。参加メンバーは情報提供についての負担は軽くなるが、逆に得られる情報の価値も少なくなる。参加メンバーの動機としては、自らの活動の他者への広報、参加時に交わされる他者の意見や見解の獲得ということになる。後者への考慮から、メンバーの発表や討議のセッションは非公開とし、参加メンバーだけが共有できるものとした。

参加メンバーの選定については、まず対象領域の選定を行った。表 1 にある政府報告や政策から技術分野をキーワードとして収集した。米国では DHS の指示で ANSI[2]（米国規格協会)が HSSP[3]（セキュリティに関する標準化推進計画）を進めており、そこで取り上げられている技術分野を参考とした。表 2 は HSSP が 2003 年に開始された当初に DHS が優先度の高い分野として示したものである。この時期は対テロ攻撃に重点を置いた計画であることがうかがえるリストである。

表 3 作業対象技術分野

密輸阻止
爆発物対策
核・放射性物質対策
災害時情報収集・共有
事業継続管理と自然災害
災害救助シミュレーション
地震災害予測・シミュレーション
産業・社会インフラの経年変化
ヒューマンエラー
位置・行動計測とインタフェース
食の安全検査
水の安全検査
文書情報セキュリティ
子供の事故予防と日常生活センシング
福祉機器の安全性
ロボットによる災害対応支援
災害時対応 IT 基盤
画像センシング
視覚による認証・認識
情報セキュリティ技術の安全性評価
組込み機器ソフトウェア検証

こうした準備の後、表 3 にあるような具体的な対象技術を選定した。2007 年度の NEDO 調査研究は電子情報分野に絞り込んだものであるため、それを重点にし、その他の分野についても参考として追加した。技術や研究の動向についての情報提供は大部分を産業技術総合研究所の各分野の研究者約 20 名に依頼することとし、評価メンバー

[2] American National Standards Institute
[3] Homeland Security Standards Panel

として、政府、企業から数名のメンバーの参加を求めた。

５．セキュリティ技術調査の結果

各技術分野については参加メンバーが事前準備をした上で 1 日(8 時間)かけて全員参加の発表・討議を実施、これに基づいて第 1 次報告をとりまとめた。NEDO の報告書がこれに相当する。

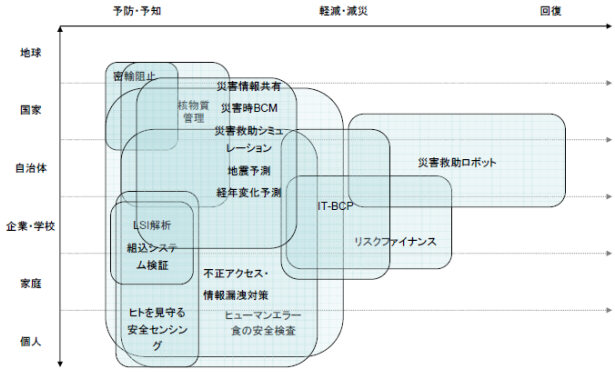

図 4　対象と過程に対する技術のマップ[9]

さらに図 2 の考え方に基づき、多様な技術に対する市場側からの評価・反応を試すため、第 1 次報告作成には参加していない企業メンバーを新たに募り、1 日(5 時間)かけて発表・討議を行った。

以下、報告の「まとめ」[9]の章の概略を紹介する。

図 4 では災害対応の時間的流れと対応主体の 2 つの軸で技術をマッピングしている。今回の調査研究は電子情報分野に主体を置いたものであることから、予防・予知など事前の段階に技術が集まっている。米国の HSSP の当初計画でもこの分野に重点が置かれており、セキュリティ産業技術の今後の分析の重点分野と考えられる。

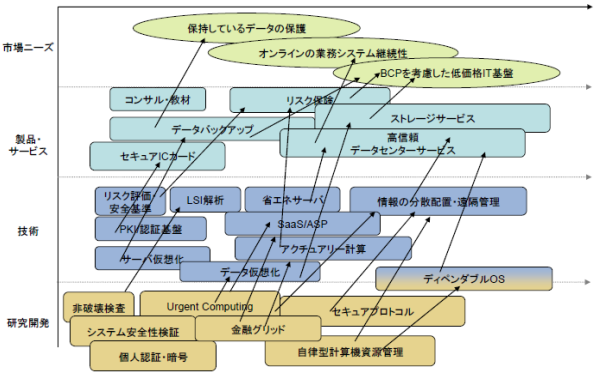

図 5 大規模 IT-BCP の技術マップ例[9]

さらに、情報処理・通信技術に関しては図 2 の多層的な技術ロードマッピングを意識し、市場から研究開発に至る 4 層で時間軸に沿った関係図を図 5 に描いている。

一例をあげれば、CMOS のゲート反転時にわずかに放出されるフォトンを検出する非破壊検査の研究開発の進展によって、LSI の動作状態での解析技術を確立することができる。電子マネー媒体となっている IC カードのセキュリティを確保する上でこの技術が鍵を握る。セキュア IC カードは各種のデータ保護、電子マネー、プライバシー保護などの市場の要求に応える手段として今後も成長が期待される。市場、製品、技術、研究開発の間の関係は一方通行ではなく、相互的である。

６．今後の調査研究

今回は電子情報分野に重点を置き、現時点での研究開発項目を列挙するものであった。今後の調査研究の方向については、セキュリティという広範で多様な技術の組み合わせが必要と予想される分野を扱うためには技術領域をさらに拡大し、技術間連携についても分析を進める必要がある。

一方、図 4 で示されるように技術群が凝集している分野についてはこれらをまとめて効果的に研究開発する仕組みを考えることが重要である。これについては関係する企業群・行政を含めたメンバーの参加を募り、図 5 のような多層的ロードマッピングに向けた活動を行い、並行して大型の共同研究プログラムの設計を進めることを検討していきたい。

参考文献

[1] 中島一郎, 社会のセキュリティに関する国際標準化の動向, 研究・技術計画学会年次大会要旨集, 2008

[2] OECD, Guidelines for the Security of Information Systems and Networks, 1992 & 2002

[3] Bruce Schneier, Beyond Fear, Thinking sensibly about Security in an Uncertain Wolrd, 2003

[4] ISO/AGS, Final Report of Advisory Group on Security, 2005

[5] OECD, The Security Economy, 2004

[6] R.Kostoff, R.Schaller, Science and Technology Roadmapping, 2001

[7] 中島一郎, セキュリティ技術研究開発のキックオフ, 平成 19 年度セキュリティ技術調査研究会報告書(NEDO) pp.1-8, 2008

[8] ANSI, HSSP N 1, 2003

[9] 一村信吾, 松井俊浩, まとめと提言, 平成 19 年度セキュリティ技術調査研究会報告書(NEDO) pp.183-187, 2008