

## The Security Economy

Summary in Japanese

---

### セキュリティ経済

日本語要約

#### はじめに

OECD 事務局、事務総長諮問ユニット

#### バリー・スティーブンス

「セキュリティ」は近年、非常に大きな注目を集めている。世界はテロやコンピュータ・ウイルスから詐欺、組織犯罪に至る様々な潜在的危険にさらされており、多くの人々にとって益々危険な場所になっていると認識されている。その結果、セキュリティ問題への注目が高まるとともに、セキュリティ関連のモノやサービスへの需要が着実に伸び、政府セクターでも企業セクターでも広範かつ多様な経済活動を生み出している。これが、急成長を遂げているセキュリティ経済である。

「セキュリティ経済」という用語は、それが示す概念と同様に比較的新しく、生命や財産が意図的に脅かされるリスクの防止・軽減に関連した様々な活動を表現しようとしたものである。最広義で用いられる場合には、防衛・諜報防止、警察、民間警備、武装護衛、セキュリティ技術提供者に関連したあらゆる事柄が含まれる。より狭義には、個人や企業のセキュリティ向け民間支出のみを指す。本書では、セキュリティ経済はセキュリティ産業（政府や政府関連機関のセキュリティ関連活動とのインターフェースを含む）とほぼ同義語として用いられている。

セキュリティ産業は、生命、財産等の資産、情報を脅かす悪意ある行為対策として安全を売る多くの企業や個人から成っている。セキュリティ産業によって生み出される製品やサービスは、火災報知器・盗難警報器や錠・金庫から、電子アクセスコントロールやバイオメトリクス（生体認証）、電子商品監視（EAS）、セキュリティ・コンサルティング、更には、装甲車サービスや警備機器、防壁まで多岐にわたる。長い間、セキュリティ産業 少なくともその大部分 は警察組織や国家安全保障を担当する軍隊とは切り離されていた。しかし近年では、セキュリティ産業はこうした他の関係者と益々オーバーラップするようになってき

ているように思われる。セキュリティ会社は、かつてはその大半のモノやサービスを家庭や企業に販売していたが、現在では政府も重要な顧客となっている。しかも、政府は他の業界の民間企業に影響するセキュリティ規制の強化にも動いている。驚くべきことではないだろうが、一部では、セキュリティ産業は非常に多様化・断片化している上、顧客との真に統一的な接点も欠けているため、「セキュリティ産業」について論じるのは時期尚早との声も聞かれる。しかし、その一方で、まだ明確に定義できるセキュリティ産業というのは存在していないが、遠からずそうした産業が誕生する可能性は非常に高いとの見方もある。重要な「新興」産業をめぐってこうした見解の相違があるのは珍しいことではない。

比較的限定された定義でも、セキュリティ経済を定量化するのは容易ではない。すべてのセキュリティ措置について支出がなされているわけではないので、評価が難しいからである。しかも、多くの場合、セキュリティは益々モノやサービスに組み込まれるようになってきているので、その付加価値の測定も難しい。加えて、セキュリティ支出に関しては信頼性の高いデータを入手するのが難しく、推計値は極めて大雑把な概算値であるケースが多い。従って、大体的場合、民間のセキュリティ産業の規模やその長期的な発展度を評価する際には業界団体の資料や特別な調査レポート等に頼らざるを得ないのが現状である。公共セクターのセキュリティ支出については情報を入手できる国もあるにはあるが、民間のセキュリティ支出と同様、信憑性に欠ける面がある。

このように測定が難しいにもかかわらず、各種の指標等からすると、セキュリティ産業は経済のビッグ・プレーヤーとして急成長し、拡大している。入手可能な推計によれば、民間のセキュリティ産業の売上高は世界全体で 1,000~1,200 億ドルに達する。国別のシェアでトップに立っているのは米国であるが、他の OECD 諸国にも大規模なセキュリティ産業が形成されている。例えば、ドイツのセキュリティ産業の売上高は約 40 億ドル、フランスと英国は約 30 億ドルと推計される。2001 年 9 月 11 日以降にセキュリティ支出が急増したという業界データは殆どないが、長期的なデータによれば、売上高の年間伸び率は約 7~8%と、平均の年間経済成長率を優に上回っている。

## 需要を生み出している主な要因

何がこうした急拡大の原動力となっているのか。セキュリティ製品/サービスの世界的な需要は、ある程度は技術の進歩によって促進されている面もあるが、本書の第 1 章が示しているように、主な原動力となっているのは広範かつ多様な社会的、経済的、制度的要素である。

こうした要素の多くはあらゆるレベル 政府、企業、個人 で高まっている犯罪行為（詐欺、闇経済取引、窃盗、破壊行為、薬物関連犯罪、暴力犯罪等）の防止・探知や安全強化への需要に関係している。興味深いのは、犯罪統計によれば多くの国では（組織犯罪ではない）通常犯罪の発生率は 1990 年半ば以降低下しているということである。一方、組織犯罪は多くの国で増加している。このことは、犯罪動向の全体像が実際には大きなばらつきがあることを示唆している。また、人々が認識する犯罪レベルが不安感形成において非常に重要な要素となっており、従って技術は必ずしも問題を解決できるとは限らないということも示唆している。

一部の国では減少している犯罪もあるものの、犯罪による経済への負担全体は膨大なものとなっている模様である。犯罪による国家レベルのコストを定量化しようとした最近の試みによれば、米国では GDP の 20%、英国では GDP の 7% と推計されている。この推計値には、犯罪防止や刑務所向けの財政支出の形による実際的なコストばかりでなく、身体への傷害や精神的ストレス等の無形のコストも含まれる。

特に 9 月 11 日の米国同時多発テロ後には、テロ行為による大規模破壊の可能性や大量破壊兵器による脅威もセキュリティ需要の増大につながる重要な要素として浮上してきている。

セキュリティ上の懸念を更に大きく押し上げているのがグローバル化である。例えば、外国貿易の拡大はヒトや貨物の輸送増を刺激している。航空・鉄道・道路・海上輸送の伸びは、強盗や組織的な密輸を助長するセキュリティ侵害のリスクを増大させ、政府による国境監視策強化に拍車をかけている。移民の増加は国の不法移民阻止能力を低下させる一方、場合によっては地域社会の不安感も煽っている。生産活動の国際化によりコミュニケーションやサプライチェーンは益々グローバル化、専門化、断片化し、特に脆弱な面を生み出している。同時に、企業や政府は業務を更に効率化し、セキュリティ面をよりコスト効果的に管理する方法を模索している。制度の再編が需要の増加を後押ししているケースもある（米国の国土安全保障省の創設はその顕著な例である）。更に、新しいより高度な監視・認証技術もより手頃な価格で次々と市場に投入されている。

各種の予測や見通しは、こうした要素が今後も引き続きセキュリティ関連の活動を刺激していくことを示唆している。移動性の高まりは確実に政府にも実業界にもセキュリティと効率性の面で特に大きな課題を突きつけるだろう。世界の商品貿易の伸び率は、航空貨物等多くの輸送セクターの高い伸び率と結び付いて、中期的に経済成長率を上回り続ける見込みである。また、移民圧力も今後何十年か続いていくものと予想される。例えば、国連は平均の年間新移民者数について、米国は 100 万人以上、ドイツは 20 万人以上、カナダは 17 万人以上と予測している。一方、勢いが増している電子商取引もサイバー犯罪の温床となるだろう。最後に、高齢化社会の進展がリスクに対する一般の認識やセキュリティ製品/サービスの需要に今後どのような影響を及ぼすかという問題もある（特に OECD 諸国ではそうである）。

## 将来の識別・監視技術

セキュリティ活動全体の拡大を背景に、セキュリティ機能の遂行に利用される技術も急成長の恩恵を受けている。例えば、監視・識別製品の市場規模は現在、150 億ドルと推計されている。これらは企業のセキュリティシステムの柱となっている製品であり、これにはアクセスコントロール、境界管理、バイオメトリクス等が含まれる。コンピュータ・セキュリティ製品の市場規模は現在、40 億ドルと推計されており、これには本人のアクセスを証明する「フロントエンド型」のセキュリティを提供するトークン、カード、バイオメトリクス等が含まれる。向こう 7~10 年の成長予測も非常に堅調である。世界のセキュリティ産業は年率 7~8% というこれまでの成長率を維持する見込みであるが、バイオメトリクス、RFID（無線 IC タグ）技術、コンピュータ・セキュリティ等については特に高い伸びが見込まれる。

実際、RFID とバイオメトリクスは近年、注目を集めるようになった技術で、将来セキュリティ分野で重要な役割を果たすものと思われる。また、衛星を利用したナビゲーションやトラッキング、暗号、電気通信の進歩等も注目されている。更に、より確立された監視技術の中にも IT 技術との融合によって注目を浴びているものもある。その顕著な例は CCTV（閉回路テレビジョン）である。

## バイオメトリクス

1990 年代末以降、バイオメトリクスは建物、コンピュータ、ネットワークへのアクセスを確保する益々有望な解決策となってきた。指、顔、虹彩、網膜、声等のデジタルスキニングは市民 ID やネットワークへのアクセスから監視、電話による通信システムに至るまで様々な用途で既に利用されている。今後これらの用途は急速に拡大する見込みであり、本書の第 2 章でベルナル・ディディエが指摘しているように、生体測定上の偽造（指や虹彩等の作り物）探知技術の改善や遠隔識別による監視技術の開発等によるこれらの用途の性能向上に多くの努力が傾注されるだろう。しかし、人々の許容を阻む潜在的な障害 指紋採取への抵抗感やプライバシーへの懸念等 を克服しようとするれば、効果的な解決策を見出す必要がある。

## RFID システム

RFID 技術は近年、大きな注目を集めている。特に商取引では、商品位置や消費者行動に関する情報を伝達する送信センサーとインテリジェント・リーダーを内蔵した追跡装置や無線 IC タグ等の技術が利用されている。電子商品監視（EAS）、ポータブル・データキャプチャー、ネットワークシステム、測位システム等様々なシステムが利用されているが、RFID 技術は小売店等が一般的に利用するにはまだ高価過ぎるため、あまり普及していない。この 2~3 年のうちには様々な用途 衣料品、危険商品、消費者向けパッケージ商品、通貨、治療中の患者の追跡等 で広範なパイロットプログラムが行われる可能性が高い。第 3 章でスティーブ・ホッジスも、「店内で支払いを行う必要のない」小売店、家庭での在庫チェック、サプライチェーンにおける製品情報の提供に RFID が利用される可能性を指摘している。ただ、RFID システムの導入には多額の投資が必要されることやプライバシー保護という厄介な問題等、多くの障害を克服しなければならない。

## 衛星を利用した追跡と監視

ルネ・オースタリンクが第 4 章で述べているように、これらの技術の用途は近年、大幅に拡大している。現在、海上交通や自家用車のナビゲーション技術から、商品の出荷状況や陸上輸送の監視、車両管理、道路使用料を請求するための自動車の監視まで、多くの関連機能で利用されている。2000 年代後半には更に多くの衛星が打ち上げられ、ガリレオのような極めて高度な衛星システムが稼働を開始するので、現行の利用が拡大するとともに、新たな用途も生まれる可能性が高い。

## 「ハイブリット・テクノロジー」カード

高速視覚認証用のホログラムを埋め込んだ極めて高度な光メモリカードの利用が始まっている。多くの場合、カードにはマイクロイメージ・セキュリティ機

能や、例えば電子政府サービスへのアクセスを提供する多用途 IC チップが内蔵されている。第 5 章でアルフィオ・トリジとルイジ・メザノッテは、向こう 5 年以内に全市民に安全な電子 ID カードを提供しようとするイタリアの取り組みの中でこうした技術がどのように利用されているかを紹介している。

要するに、中・長期的に見てセキュリティ技術の成長を左右しそうな極めて重要な要素は、技術的な問題ではなく、これらの技術がどの程度一般に受け入れられるか、技術のメリットがどの程度明瞭に認識されるか、消費者がセキュリティへの懸念をどの程度優先させるかなのである。

## 長期的な経済への影響

近年の出来事が物語っているように、地方・国家・地域経済は多くの様々なセキュリティ上の脅威にさらされている。とりわけ、セキュリティ上の脅威は非常に高い代償を強いることになりかねない。悲劇的な人命の喪失を別にしても、9月11日の米国同時多発テロの経済的コストは総額で約1,200億ドルに上ると現在考えられている。これには物理的資産やインフラへの影響ばかりでなく、雇用、金融市場、事業の継続性等への影響も含まれる。同時多発テロ以降、主要な業界は事業に対する大規模な脅威への対策に乗り出している。例えば、海上輸送業界では、海上輸送システムが周到に計画されたテロ攻撃を受ければ被害は何百億ドルにも上ると考えている。しかしながら、凶行がそれほど大規模なものでなくても被害は多額に上る可能性がある。一例を挙げれば、米国の場合、1990年代末には社会保障給付詐欺だけでもコストは7億5,000万ドルと推計され、本人なりすまし詐欺による銀行等の金融機関の被害額は年間約20億ドルと考えられている。英国でも、全企業の5分の2強が最近、セキュリティ上の被害にあったと報告しており、産業界全体では被害額は数十億ポンド前後に上る模様である。

しかし、セキュリティの改善にもコストがかかる。このコストは一般に次の二つである。一つは、必要なセキュリティ上の仕組みを導入するための投資、もう一つは、セキュリティ上の仕組みが業界や経済全体の運営に及ぼす恐れのある悪影響である。

深刻な脅威によって甚大な損害を被る可能性に直面し、政府や企業は、巨額に上りかねない投資を検討せざるを得なくなっている。上述の海上輸送業界の場合、国際海事機関（IMO）で交渉が行われているセキュリティ対策によって船会社に課される初期負担は6億ドルを優に超える可能性があると考えられている。殆どの国の企業は自社の資産や情報システムを守るための投資を増やしている。例えば米国の場合、推計によれば、同時多発テロを受けて民間セクターの自国領土内のセキュリティコストは総額で年間約100億ドルに上っている（テロから間もない2003年には460～760億ドルと、この額をはるかに上回っていた可能性がある）。政府その他の公的機関もセキュリティ支出の総額を増やしており、中には極めて大幅に増やしているケースもある。米国の国土安全保障省の予算は2002/03年度から現在の300億ドルを優に超える水準へと倍増しており、航空セキュリティ向け予算が48億ドル、国境セキュリティ向け予算が106億ドルに上っている。こうした投資を賄うのが政府の税収であれ、民間支出であれ、その経済への影響は小さくない。

セキュリティが厳しくなれば、納期が長期化するとともに、グローバルなサプライチェーンや綿密に調整されたジャストインタイムの配送システムに支障を

きたす可能性がある。近年、セキュリティへの懸念が強まった結果、貿易会社では輸送、出荷、保険、関税に関するコストが増えている。こうした「摩擦的な」コストは往々にして貿易を割高なものとし、フローを減少させる。OECD のシミュレーションによれば、同時多発テロ後に導入された措置によって貿易コストは1%増加し、世界全体で年間約 750 億ドルの経済的厚生損失につながっている可能性がある。

本書の第 6 章でティルマン・ブリュックが指摘しているように、セキュリティとグローバル化、セキュリティと技術進歩等トレードオフの可能性は他にもある。また、セキュリティ面の不安によるその他の重大な間接的・二次的影響もあるが、その多くはあまりよく理解されておらず、定量化の難しいものである。

もちろん、これらの要素については視野に入れなければならない。短・中期的にはコストが高くつくかもしれないが、それによって深刻な損害や混乱を防げるのであれば、長期的には膨大な利益につながり得る。問題はセキュリティ対策と効率性の最適のバランスをいかに実現するかである。新技術はその実現を後押ししてくれるだろうし、様々な文献や資料も豊富なケーススタディや実例を提供してくれる。米国税関によって提案されている新たな電子積荷目録処理システムに関する調査によれば、このシステムを採用した場合の直接的なコスト節減額は米国の輸入業者だけでも 20 年間で 220 億ドルを超え、米国政府の節減額は同じ期間に 40 億ドルを大幅に超えると推計されている。

しかし、公共セクターと民間セクターのそれぞれの役割を再評価する余地もある。政府の介入を正当化する主な論拠はセキュリティの公共財としての性格である。投資する者は必ずしも自身のセキュリティ投資が他者にもプラスの外部性を及ぼすことについては考慮しない。その結果、実際のセキュリティ・レベルは往々にして最適のレベルを下回ることになる。このような望ましくない結果は、信頼できる執行ルールを伴う規制や調整によって軽減することができる。しかしそれでも、政府はどの程度関与すべきか、どのように介入すべきか、どのような政策を優先的に実施すべきかという問題は残る。

大規模災害にはマイナスの外部性が伴うことを考えると、補助金をめぐる周知の落とし穴を回避するという条件下で、政府が民間セクターにセキュリティ改善を支援するための補助金を提供する余地もあるかもしれない。また、政府規制が最も適切な手段と思われる場合には、規制の影響を受ける企業を規制作りに関与させることが不可欠である。実際、近年では航空会社や金融機関等には以前よりはるかに強いセキュリティ義務が課されるようになっている。この結果、民間企業はしばしば、民間セクターへのリスク転嫁が益々進み、企業は必ずしも目には見えないものの多額に上りかねないコストを課されるようになってきていると感じている。しかし、官民のリスク負担者がセキュリティコストを分担するのが明らかに適切であると思われる場合でも、どのような手段を用いるか（税金によるか規制によるか等）について難しい選択をしなければならない。セキュリティ経済に影響を及ぼす政府の政策を現在の状況や選好に合わせるよう更に配慮する必要があることは明らかである。

セキュリティ分野の官民協力、特に民間セクターの自主的な取り組みに対する政府の支援は大きな可能性を秘めているように思われる。例えば、荷送人、仲介業者、運送会社を取り決めをし、その取り決め政府が積極的なパートナー（関税や入国管理等）としても促進者（外部業務委託の保証や民間セクターの業

務が認可を受けていることの確証・認証等)としても関与するようにしてサプライチェーン全体の完全性を確保するようなイニシアティブである。

## 長期的な社会への影響

セキュリティ技術の普及と高度化に伴い、多くの動きが同時に起こっている。まず、監視が益々「きつく」なっている。また「民営化」も進んでいる。例えば米国の場合、推計によれば、民間のセキュリティ支出は1980~2000年の20年間に五倍以上増え、警察支出の二倍以上に上っている。更に、セキュリティ技術はより「自動化」するとともに、個人情報を含むデータベースと益々「統合化」し、「グローバル化」も進んでいる。

上述の各章は監視技術の利用増をデータ等で裏付け、今後この分野が大幅に伸びることを示唆している。監視技術の効果向上は、検索可能なデータベースとのリンクや、チェック・ソート・特定への高性能コンピューティング技術の利用によって、少なくともある程度はもたらされている。その好例は、コンピュータが顔の特徴、表情、行動パターンに基づいてソートし、カテゴリー化できるアルゴリズムによる(数学的にコード化された)顔認識装置とCCTVとのリンクである。このように、本書の第7章でデイビッド・ライオンが指摘しているように、21世紀に入ってから、こうした「ソーシャル・ソーティング(社会的仕分け)」と「識別」のプロセスは益々自動化されている。興味深いのは、ソーティング技術が発展しているのは警察や行政の分野ばかりでなく、マーケティング分野でも発展していることである。従って、人々は監視によって(しばしば本人の知らぬ間に)、罪を犯す可能性のある人物や見込み客として分類されている。この結果、リスクプロファイリングの利用が増え、「予測プロファイリング」への依存度が高まっている。

同時に、官と民、国と市民社会による監視は収斂しており、様々な情報源 公共サービス、警察、諜報機関、企業、消費者 によるデータベースが益々統合化されていくのは必至のように思われる。公的なデータネットワークと商業的なデータネットワークとの結合が進展していくにつれ、(多国籍企業等によるデータ収集によって空港や港で)グローバルな監視体制が構築される可能性は非常に高まっている。

従って、社会全体として今後、監視・識別技術の普及にどう対応していくかという重要な問題が浮上している。例えば、セキュリティと民主的な自由はこれまで往々にして相互に補完し得る概念ではなく、二者択一的なものとなってきた。プライバシーの問題は重要であるが、今後はアカウントビリティの問題も同じくらい重要なものとなる。監視システムをどのように管理するのか。誰がカテゴリーを作るのか。ソーシャル・ソーティングやリスクプロファイリングは普通の人々にどのような影響を及ぼすのか。地方の組織や機関が、確立された法的枠組みの下で自らを規制する多くの機会が存在する中で、政府は今後も引き続き重要な規制機関と見なされるのか。

将来を占う兆候は否定的なものばかりではない。実際、一部の組織は個人のデリケートな情報にこれまでよりはるかに配慮するようになっている。個人データの脆弱性の認識も高まっている。更に、最近では、外国への流出が認められている個人データに対する制約を大幅に強化する国際的取り決めもなされ始めている。多くの人々にとって識別・監視技術の進歩は止められないように思われる。

できることは、社会が総じて最も有益と見なす方向へとその発展と利用を導いていくことくらいだろう。従って、極めて重要となるのは、当該技術、それに対する社会の賛否両論の意見、そして規制機関の対応が如何に相互に作用し合うかである。

© OECD 2004

This summary is not an official OECD translation.

Reproduction of this summary is allowed provided the OECD copyright and the title of the original publication are mentioned.

多言語版要約は、英語とフランス語で発表された OECD 出版物の抄録を翻訳したものです。OECD Online Bookshop [www.oecd.org/bookshop/](http://www.oecd.org/bookshop/)から無料で入手できます。

お問い合わせは OECD 広報局権利・翻訳部にお願いいたします。

[rights@oecd.org](mailto:rights@oecd.org)

Fax: +33 (0)1 45 24 13 91

OECD Rights and Translation unit (PAC)  
2 rue André-Pascal  
75116 Paris  
France

ウェブサイト [www.oecd.org/rights/](http://www.oecd.org/rights/)

