なぜ情報セキュリティが DX 推進にあたり不可欠なのか

東海大学情報通信学部／国立情報学研究所 客員教授
三角育生

はじめに

クラウド利用が普及し、新型コロナ対策などからテレワークが急速に普及している今日、デジタル・トランスフォーメーション（DX）の推進に関連して、情報セキュリティが、柔軟なビジネス・イノベーションを推進するときの障害となるとの発言をしばしば聞く。これは例えば、パソコンの持ち出し禁止、インターネットからの分離など、従来からしばしば実施されてきた、機密性の確保のためにパブリックなインターネット環境から境界で防護することを中心とする「対策」の影響があるのではないかと思われる。

しかしながら、その様な「対策」は、今日、必ずしも情報セキュリティの向上と業務の高度化・効率化に対して同時に貢献するものではない[1]。情報セキュリティの取り組みが、DX を推進する組織において適切に理解され、実施されることが望まれる。それに資するため、本稿では、著者の行政における経験を踏まえて、情報セキュリティが DX 推進にあたり不可欠なものであるとの考えを述べたい。

安全保障貿易審査において実施した DX の取組

安全保障貿易管理とは

著者は 2009 年、経済産業省にて、外国為替及び外国貿易法（外為法）25 条 1 項及び 48 条 1 項に基づく輸出許可（いわゆる安全保障貿易審査）等の審査責任者である課長に着任した。特定の地域を仕向地とする特定の種類の貨物を輸出しようとする者、特定の技術の提供を目的とする取引を行おうとする者は、経済産業大臣の許可を受けなければならない。特

[1] 例えば、地方自治体の情報セキュリティ対策について、平成 27 年度には機微な情報を扱うシステムのインターネットからの分離を強力に推進したが、令和 2 年度に、一部、見直しがかけられている（例えば、https://www.soumu.go.jp/main_content/000402431.pdf、https://www.soumu.go.jp/main_content/000727474.pdf 及び https://www.soumu.go.jp/main_content/000688754.pdf 参照。(2021 年 4 月閲覧)）。

定の種類の貨物・技術とは、例えば、武器や、原子力関連物資、化学兵器・生物兵器の原料などとなる物質や細菌等、ミサイル関連物資といった大量破壊関連の仕様の貨物等、先端材料、数値制御工作機械、エレクトロニクス、通信機器・暗号等の武器に用いることのできるハイスペックな貨物等である（リスト規制）。仕向地は、多くの場合に全地域が対象とされる。ただし、米国・EU 諸国等向けの場合には包括的な許可制度を含めて、簡素な申請の手続きとなっている。一方で、北朝鮮、イラン等の国向けの場合には許可申請手続きは事前の確認事項も含めて詳細なものとなっている。さらに、いわゆるキャッチオール規制といって、リスト規制品以外のものを取り扱う場合であっても、輸出しようとする貨物などが、大量破壊兵器等の開発、製造、使用又は貯蔵もしくは通常兵器の開発、製造又は使用に用いられるおそれがあることを輸出者が知った場合、又は経済産業大臣から、許可申請をすべき旨の通知を受けた場合には、輸出などに当たって経済産業大臣の許可が必要となる制度もある。

複雑な申請・審査手続きの改善に向けた電子化推進

この様に安全保障に係る輸出･技術提供許可申請手続きは複雑な制度となっており､2009 年当時、許可申請などのために提出する書類の様式は多様で、添付資料もケースによっては多量なものとなっていた。輸出される貨物の通関などの行政手続きは電子化が進められており、そのシステムと連携した輸出許可の電子申請の仕組みもあった。しかし、当時は、紙の書類による申請がほとんどであり、審査作業は、ペーパーワークであった。

特に業務量の多い作業は、申請情報をシステムに入力するなどの台帳管理業務などであった。2009 年は、リーマンショックの影響などもあり、申請件数はその前年よりも落ち込んでいた。しかし 2010 年になると、経済産業省本省で受け付けた申請件数は対前年度３割増と、ゆうに１万件を超え、過去５年間の申請件数と比して最大となった[3]。この様な状況の下、審査の質、すなわち安全保障の観点からの管理を損なうことなく、迅速な審査といった申請者のニーズに対応することが求められていた。

一般に行政組織の職員を容易に増員することは難しい。そこで、対策として、業務の電子化推進が考えられた。ただし、単にＩＴシステムを導入するのみでは、効果的・効率的な運用の実現を期待することは難しい。

何が求められ、何を審査するのかを根本から考え直す

業務の高度化・効率化にあたっては、審査業務の趣旨に戻って考えなおす必要がある。例えば、国際的な輸出管理の枠組みで求められる事項は、大量破壊兵器関連の物資などについ

ては最終需要者、最終用途の確認を厳格に実施する必要がある。そこで、審査にあたっては、輸入者等及び最終需要者の存在や身元の確からしさ、最終需要者等が兵器等開発又は製造を行っていないかどうか、最終需要者等の関係者に軍、兵器製造業者等問題となる者がいるかどうか、説明されている最終用途の妥当性などをチェックするわけである。

一方、審査担当者は、法令の条項などで担当が分かれていた。すなわち、貨物[2]の品目別[3]、技術・プログラム[4]かどうかで担当が分かれていたわけである。そうすると、一つの申請に、複数の品目やプログラムが含まれていると、それぞれの担当者が申請内容を審査することになる。しかしながら、上述のように、最終需要者などの審査は、貨物の品目の別などには原則影響されない。また、ある貨物を動作させるための定型的なプログラムは、最終用途の審査にあたって併せてチェックするのが妥当なものもある。従って、法令の根拠条文・項番別で担当を分けて審査する場合に、チェックするべき点が重複することなどもあり得るわけである。

また、申請等の様式や添付書類は、90 年代初頭に輸出管理が最終用途などの観点からの審査が重点化されて以来、各種の国際的な輸出管理の枠組みのルールなどを踏まえ、また、その時々の審査をめぐる情勢なども踏まえて見直しなどがされてきたためと考えられるが、結果として多様なものとなっていた。

加えて、過去の同一の最終需要者との取引と、申請された取引との比較なども行っており、この点は申請者に申告させるとともに、台帳上で検索などをする作業が発生する。この業務量は、台帳入力作業とともに、時間を要する大きなものであった。

抜本的な見直し目標の設定

上記の様な状況のなか、審査業務の改革にあたり、審査を高度化しつつ、審査時間や添付書類の漸減的な改善をしていくのでは、当時の、申請件数の大幅な増加には対応しきれないと考えられた。そのため、抜本的な見直し目標を設定した。そして、まずは、業務フローなどの見直し、すなわち業務フローの中で標準化できるものは標準化し、質問事項や申請書類等に記載されるデータについて明確化等を図ることなどから着手した[3]。

これにより、複数の審査担当者が、実質的に重複した作業を行っていたところは重複を解消し、ある種類の貨物等の申請が増えて業務量が一時的に増大したときに、その種類の貨物

---

[2] 外為法 48 条 1 項の許可を要するもの。

[3] 政令によって品目が区別され、項目の番号が付されている。

[4] 外為法 25 条 1 項の許可を要するもの。

等の担当グループを他の種類の貨物等の担当グループが支援に入ることができるようになった。この点は、以下に示す審査のためのシステム化を進めることで、より、審査担当者間での情報伝達などがやりやすくなるため、こうした運用をしやすくなるわけである。

また、申請関連の手続きについては、法令に加えて通達で詳細な手順等が定められていたが、これらについても見直しを図った。例えば、貨物や技術の種類などによって申請書類などの様式が異なっているものがあったが、これらを整理して、様式を整えた。申請に際して添付すべき資料の見直しも図り、様式に記載する事項をデータのエビデンス等として必要なものを整理した。こうした作業により、関連する通達 21 本を最終的に 3 本に整理・統合[5]した。

審査のシステム化で申請・審査・許可まで一気通貫に

この様な業務の見直し・整理を行ったうえで、審査のためのシステム化を行った。審査システムの構築にあたってはアジャイル的に審査担当者からのフィードバックを入れて行い、ユーザにとって使いやすく業務効率を高めるものとしていった。そして、電子申請システムと接続することにより、審査作業における大きな作業負担を発生させていた台帳管理業務量を軽減した。また、効率よく過去のデータを検索することなどもやりやすくなった。そして、審査の品質を高めるべく担当者は調査等により重点を置きやすくなり、同時に、作業効率も高まることで申請者の審査の迅速化というニーズにも応えられるようになった。

当時、著者は、この様に硬直的であった業務の見直し・整理を大幅に進めるべく、ICT を利活用し、サービスの高品質化とサービス利用者のニーズに応えることを Business Process Re-engineering [4]の実践として取り組んでいた。現在でいえば、DX の一形態である。

---

[5] 「輸出許可・役務取引許可・特定記録媒体等輸出等許可申請に係る提出書類及び注意事項等について」、https://www.meti.go.jp/policy/anpo/law_document/tutatu/tutatu24fy/tenpshorui_tutatu120401.pdf （2021 年 4 月閲覧)
「大量破壊兵器等及び通常兵器に係る補完的輸出規制に関する輸出手続等について」、https://www.meti.go.jp/policy/anpo/law_document/tutatu/tutatu24fy/hokanteki_yushutukisei.pdf （2021 年 4 月閲覧)
「『包括許可取扱要領』の一部を改正する通達」、https://www.meti.go.jp/policy/anpo/law_document/tutatu/tutatu24fy/houkatu_toriatukaiyouryou120401.pdf （2021 年 4 月閲覧)

情報セキュリティ対策の重要性

機密性確保の徹底と使いやすさの両立

輸出許可申請・審査・許可が一気通貫したシステムが構築されると、構築段階でも情報セキュリティ対策について検討して進めたものの、具体的な運用にあたり、審査業務の責任者としては、その情報セキュリティ対策が重大な関心事項となった。

すなわち、輸出許可申請の審査にあたって取り扱う要機密情報としては、申請者の営業に係る秘密情報や申請者自身などについての個人情報などがある。また、輸出管理の国際レジームのルールでは、他国で不許可となったものと本質的に同じ輸出許可申請案件については、当該他国との間での協議で同意が得られなければ輸出許可ができないことになっている[6]が、こうした外交などに係る情報も含みうる。これらの情報がオーソライズされていない者がアクセスできることは業務遂行上重大な支障となる。そのため従来から物理的な機密性確保のための対策や、情報セキュリティ対策のルールの徹底は図ってきていた。そして、DX を進めるにあたり、業務責任者として、システムについても一層の注意を図る必要を認識した。まずは、システムで扱うこれら要機密情報の確実な保護ができているか、という点が重大な課題となる。当時の政府における機密性に関する情報セキュリティ対策は、アクセス制御、組織外の通信回線との間の防護、必要に応じて独立回線とすること、暗号化、境界での監視等が基準[7]となっており、これらを適切に実装し運用されていることであった。業務の責任者として、審査のシステム化に着手する段階で、改めてこの点の確認をシステム担当部局に求めた。

ただし、機密性確保を進めた結果、システムの利用者たる申請者や審査官にとって使いにくいものとなっては、本末転倒である。システム化することによる業務効率の向上のメリットを損なうことのないような業務手順に無理のない対策が求められる。この点は、日本年金

---

[6] The Australia Group "Guidelines for Transfers of Sensitive Chemical or Biological Items" https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/guidelines.html（2021 年 4 月閲覧）

[7] 当時は、情報セキュリティ政策会議、「政府機関の情報セキュリティ対策のための統一技術基準」（2011.4.21)、https://www.nisc.go.jp/active/general/pdf/K305-101.pdf (2021 年 4 月閲覧)。基本的な考え方は境界での防護を中心としたものと解される。
なお、その後４回改定され、現在は、クラウドの安全性評価の活用やゼロトラストアーキテクチャの検討など境界での防護を主体とする当時からはモダナイズされた統一基準の改定の方向性の議論がなされている。https://www.nisc.go.jp/conference/cs/dai26/pdf/26shiryou05.pdf （2021 年 4 月閲覧)

機構への不正アクセスによる情報流出事案の報告書[1][8]においても、「組織の業務、取り扱う情報、保有するシステムに応じて、多様な対策の中からどう守りを構築するのか、目的に照らし、業務が円滑に実施できるような対策とは何か、組織として能動的に検討した上で最適な手法を設定し、実施することが肝要」とされている。日本年金機構の事件が生じる前であったが当時、審査業務責任者としては、当然、業務効率の向上のメリットを損なわないように留意した。

可用性の確保：業務部門と情報システム部門の連携

加えて、責任者として重大な関心があったものは、システムの障害や列度の高い地震などの影響によってシステムや情報の可用性が損なわれることに起因する事業継続への影響である。もしも可用性が損なわれれば、輸出許可を受けた輸出者が通関時に電子的に許可を示すことができず通関できなくなり、輸出者が大きな損害を被る可能性がある。この点について当時の政府の統一基準[4]では、省庁の業務継続計画と情報セキュリティに係る省庁の対策基準との整合性をとることなどが規定されていた。このため、業務責任者として、本件情報システム担当と、現実の事業継続の実施方法と、システムの可用性確保又は緊急時の代替策について、具体的に綿密な議論を行った。

業務部門と情報システム部門との間では、事業継続と情報システムに関する事業継続計画との整合性を十分に確保できていないケースが散見される。これは両部門間での連携が十分でないことに起因する。そこで、何について議論すべきかなどが論点となるが、まずは、重要な業務についての目標復旧時間の設定、非常時の優先順位付けなどについて調整する必要がある[2][9]。情報システム部門のみが情報システムに係る事業継続計画を考えることとなると、仮に可用性の確保を徹底するとなると過剰なコストが発生する可能性があり、一方で、予算の範囲内での可用性の確保となると、「想定外」の事態が生じるリスクが高まる。業務部門と情報システム部門が連携することにより、現実的なリスクマネジメントを行うことができる。

なお審査にあたっては、保存されているデータの完全性、申請者からのデータが正しく使われたことの保証、説明責任といった観点からの情報セキュリティ対策も重要である。

---

[8] 報告書 P19 参照。

[9] 著者は、輸出許可申請・審査・許可のシステム化を推進したときの経験から、内閣官房情報セキュリティセンターに勤務していたときに、この点を強調した文書を作成した。

おわりに

本稿では、著者の 2009 年から 2012 年にかけての行政における経験を踏まえて、DX を進めたときに情報セキュリティ対策が不可欠であると確信したことについて述べた。当時に比べると、現在は DX の概念が浸透し、また、クラウドサービスの普及、ゼロトラスト[10]などをはじめ採り得る手法、対策の選択肢が多様になり、業務を円滑に高度化することと情報セキュリティ対策の実施を同時達成できる環境がより充実してきている。DX の推進計画立案段階、情報システムの見直しの企画段階から、情報セキュリティ対策を、DX の具体的な実現方策の一部として検討を始めることにより、より効率的で効果的なものとすることができるようになったと考える。そこで、DX の推進にあたっては、その企画段階から情報セキュリティを取り込んだ形で進めるプラクティスが広く普及することを期待する。

参考文献

[1] サイバーセキュリティ戦略本部、「日本年金機構における個人情報流出事案に関する原因究明調査結果」、(2015.8.20)、
https://www.nisc.go.jp/active/kihon/pdf/incident_report.pdf (2021 年 4 月閲覧)
[2] 内閣官房情報セキュリティセンター、「IT-BCP 策定モデル」、2017 年 6 月、
https://www.nisc.go.jp/active/general/pdf/IT-BCP.pdf　(2021 年 4 月閲覧)
[3] 三角育生、「安全保障輸出審査の制度運用の状況と動向について」、CISTEC Journal、No.133 p.1-4 (2011.5)
[4] 例えば、Michel Hammer, James Champy、「Reengineering The Corporation」、Harper Business、(1993)

著者略歴

三角 育生（みすみ・いくお）
1987 年～2020 年 7 月、経済産業省。2012 年～2020 年 7 月、内閣官房内閣サイバーセキュリティセンター内閣参事官、内閣審議官。2017 年～現在、国立情報学研究所客員教授。2020 年 9 月～現在、東海大学情報通信学部客員教授。博士（工学）。

[10] 例えば、https://csrc.nist.gov/publications/detail/sp/800-207/final　(2021 年 4 月閲覧) 参照。