2022 年 3 月 3 日

経済安全保障とサイバーセキュリティ

森・濱田松本法律事務所
弁護士　蔦 大輔（執筆主担当）
TEL. 03 6266 8769
daisuke.tsuta@mhm-global.com
弁護士　宮岡 邦生
TEL. 03 6266 8738
kunio.miyaoka@mhm-global.com
弁護士　梅津 英明
TEL. 03 6212 8347
hideaki.umetsu@mhm-global.com

Ⅰ. はじめに

2 月 25 日に経済安全保障推進法案[1]が閣議決定されるなど、「経済安全保障」に注目が集まっています。そうした経済安全保障の重要な一分野として、サイバーセキュリティが挙げられます。

「経済安全保障」という概念には、必ずしも統一した定義はありませんが、一般には、軍事的脅威からの防衛という狭義の「安全保障」概念を超えて、経済・技術分野における自国産業の自立性や優位性の確保のための施策や国家戦略を広く含む概念と捉えられています[2]。経済安全保障を実現するための施策に関しては、自国産業の強靭化、育成といった「攻め」に関するものと、重要技術の流出防止といった「守り」に関するもの等様々なものがありますが、このうち、「守り」に関する施策として、重要なインフラの機能保証を含むサイバーセキュリティに関する取組みや、特に機微な情報についてのデータセキュリティに関する取組みを挙げることができます[3]。

わが国では、2022 年 2 月 1 日に、内閣官房「経済安全保障推進会議」において、「経済安全保障法制に関する提言」がとりまとめられ、これを受けて、上述のとおり同月 25 日に、経済安全保障推進法案が閣議決定されました。同法案は、①サプライチェーンの強靭化、②基幹インフラの安全性・信頼性の確保、③官民技術協力、④特許出願の非公開化の 4 つを中心的な施策としており、このうち②の基幹インフラ防護を中心に、サイバーセキュリティに関する取組みの強化も盛り込まれています。

以上の状況を踏まえ、本レターでは、サイバーセキュリティと深く関係する基幹イン

[1] 経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律案
[2] 経済安全保障の概念及び関係する諸施策については、INTERNATIONAL TRADE LAW / CRISIS MANAGEMENT BULLETIN 2021 年 11 月号「経済安全保障リスクと危機管理」もご参照ください。
[3] データセキュリティという観点では、2021 年に、データの管理（いわゆるガバメントアクセスの観点）が問題となったケースも報道されましたが、紙幅の都合上割愛します。https://www.nikkei.com/article/DGXZQOUC173RW0X11C21A0000000/

フラの安全性・信頼性の確保に焦点を当てつつ、サイバーセキュリティと経済安全保障の関係について概説します。

Ⅱ. 経済安全保障とサイバーセキュリティ

1. 安全保障とサイバーセキュリティ

サイバーセキュリティは、そもそも安全保障の問題でもあります。2022 年 2 月に開始されたロシアによるウクライナへの侵攻においても、物理的な攻撃に加え、サイバー攻撃が行われている旨が報じられており、国家によるサイバー攻撃からの防衛という側面からも、サイバーセキュリティの重要性が高まっています[4]。

日本におけるサイバーセキュリティへの取組みの基本理念等を定めたサイバーセキュリティ基本法は、その法目的（1 条）に「安全保障への寄与」を含めており、政府が定めるサイバーセキュリティ戦略においても、安全保障への寄与のための戦略として、わが国の防御力・抑止力・状況把握力の強化等が重要とされています。

また、国家の関与が疑われるサイバー攻撃集団による機密情報の窃取に対する近時の問題意識の高まりを受けて、2021 年 9 月に決定された新たなサイバーセキュリティ戦略は、国家の関与が疑われるサイバー活動を行う国家として、中国・北朝鮮・ロシアを名指ししています[5]。こうしたサイバー攻撃のターゲットは政府機関に限らず、民間事業者も多く被害に遭っています。

2. 新サイバーセキュリティ戦略と経済安全保障

上述した 2021 年 9 月の新サイバーセキュリティ戦略では、経済安全保障の視点も踏まえた施策も盛り込まれています。サイバー攻撃の多くが、個人情報や知的財産をターゲットとしていることを踏まえ、重要なインフラにおいて実装される IT システム・サービスや、業務提携・委託契約の態様について、サプライチェーン・リスクを含む様々なリスク・シナリオを勘案し、その安全性・信頼性を確保するための制度的検討を含む対策を推進することとされました。

ここにいう「サプライチェーン・リスク」という用語は多義的であり、サイバーセキュリティの関係では、大まかに、(1) 製品製造の過程で悪意ある機能が組み込まれるおそれと、(2) 製品、情報等の一連の商流（供給網）の中で、相対的に脆弱な組織が狙われて情報漏えい等するおそれという 2 つの意味で用いられます。(2) の関係では、直近でも、自動車部品メーカーに対するサイバー攻撃が行われ、サプライチェーンに大きな影響が出たことが報道されています。

現在、わが国の政府機関においては、サプライチェーン・リスクは、主に (1) の観

[4] 日本経済新聞 2022 年 2 月 28 日「ロシアのウクライナ侵攻、サイバー戦も激化」等
[5] サイバーセキュリティ戦略（2021 年 9 月 28 日閣議決定）8 頁参照

点から、「情報通信機器等の開発や製造過程において、情報の窃取・破壊や、情報システムの停止等の悪意のある機能が組み込まれる懸念」と定義されています（「IT 調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ」（以下「IT 調達申合せ」といいます）参照）。

IT 調達申合せは、サイバーセキュリティ基本法 26 条 1 項 2 号に基づき対策の基準として定められた統一基準群[6]の一つである「政府機関等の対策基準策定のためのガイドライン（令和 3 年度版）」において、「サプライチェーン・リスクに係る懸念が払拭できない企業の機器等を調達しないことが求められる」、とされていることを踏まえたもので、国家安全保障や機密性の高い情報を扱うシステム調達に際して適用されます。この申合せは、特定の国や特定の企業を直接名指ししして排除を求めるものではありませんが、特定の企業の製品を念頭に置いたものである旨の報道もなされています[7]。これらの調達の際には、原則として、内閣官房内閣サイバーセキュリティセンター（NISC）及びデジタル庁に対して助言を求めなければならないとされています[8]。

IT 調達申合せの対象は、当初は国の行政機関のみでしたが、改正により独立行政法人等にも拡大され、また、この申合せや上記統一基準群を引用する形で、サプライチェーン・リスクへの対応を含めたサイバーセキュリティ対策が求められる例が増えつつあります[9]。

Ⅲ. 経済安全保障推進法案におけるサイバーセキュリティ

1. 経済安全保障法制に関する有識者会議の提言

2022 年 2 月 1 日に、内閣官房「経済安全保障法制に関する有識者会議」において、「経済安全保障法制に関する提言」（以下「提言」といいます）が公表されました。同月 25 日に閣議決定された経済安全保障推進法案は、この提言を受けて、サプライチェーンの強靭化、基幹インフラの安全性・信頼性の確保、官民技術協力、特許出願の非公開化という 4 つについて法整備を行ったものです。前述のとおり、サイバーセキュリティの関係では、基幹インフラに関する施策が重要です。

具体的には、提言では、海外において、基幹インフラ事業を対象とするサイバー攻撃が多発している状況を踏まえ、外部にある主体が基幹インフラ事業者の設備供給や維持管理の受託者に影響を及ぼすことができる場合、その地位等を利用して妨害行為が行われるおそれが高まっているが、既存の業法が、外部からの妨害行為を未然に防止するための規定を備えていないことが現状の課題として挙げられています。

---

[6] https://www.nisc.go.jp/active/general/kijunr3.html
[7] https://www.nikkei.com/article/DGXMZO38728050Q8A211C1MM0000/
[8] IT 調達申合せの決定から 2021 年 3 月までに間に、NISC から各府省庁に対して 1,952 件の助言が行われ、そのうち、サプライチェーン・リスクの懸念が払拭できない機器等が含まれているとの助言が行われた割合は、約 4%（83 件）であったとされています。https://www.nisc.go.jp/conference/cs/dai25/pdf/25shiryou06.pdf
[9] 例えば、「政府機関等における無人航空機の調達等に関する方針について」（2021 年 9 月 14 日）等。

そして、上記 IT 調達申合せに言及した上で、基幹インフラサービスの安定的な提供確保のため、重要設備の導入や当該設備の維持管理等に係る重要な委託について、サプライチェーン・リスクも含めて政府が正しく実態とリスクを把握し、外部からの妨害行為（この妨害行為の一例として、サイバー攻撃が想定されていると考えられます）のリスクが大きい場合には、必要な措置を講じて妨害行為を未然に防止する仕組みを構築する必要があるとされました。

2. 経済安全保障推進法案における基幹インフラ防護制度

サイバーセキュリティ対策を考える上では、データセキュリティという文脈から、データの漏えい等への対策も重要ですが、情報システムの安全性・信頼性という観点から、事業継続リスクへの対策も重要です[10]。特に、社会インフラに関しては、後者の対策が重要であり、サイバーセキュリティ戦略本部「重要インフラの情報セキュリティ対策に係る第 4 次行動計画」[11]においても、任務保証（機能保証）[12]の考え方が重要とされています。このように、社会インフラの事業継続とサイバーセキュリティには密接な関係があります。

今般内閣官房から提出された経済安全保障推進法案は、全 7 章、99 条から構成されていますが、そのうち第三章「特定社会基盤役務の安定的な提供の確保」（49 条～59 条）が基幹インフラ防護に関する制度となっています。

大まかな法律上のスキームは、

① 政府が特定社会基盤役務基本指針を定める
② 主務大臣が、制度の対象となる特定社会基盤事業者を指定する
③ 特定社会基盤事業者における重要設備の導入・維持管理等の委託に関して、重要設備が外部からの役務の安定的な提供を妨害する行為の手段として使用されるおそれが大きいかどうかを審査する
④ 審査の結果に応じて、妨害行為を防止するために必要な措置を発令する

という仕組みになっています。

以下①～④について敷衍します。

①政府は、特定社会基盤役務基本方針を定めることとされています（49 条）。この

[10] 法律上の「サイバーセキュリティ」の定義には、情報システムや情報通信ネットワークの安全性及び信頼性の確保のために必要な措置を適切に維持管理することが含まれています（サイバーセキュリティ基本法 2 条）。
[11] この第 4 次行動計画の改訂版である「重要インフラのサイバーセキュリティに係る行動計画」の案が 2022 年 2 月 28 日までパブリックコメントの対象となっていました。今後正式な計画の策定が見込まれます。
[12] あらゆる組織が、自らが遂行すべき業務やサービスを「任務」と捉え、かかる「任務」を着実に遂行するために必要となる能力及び資産を確保することをいいます。特に重要なインフラにおいては、システム障害やサイバー攻撃をリスクと捉えつつ、そのサービスの安全かつ持続的な提供を行うことが重要です。

「特定社会基盤役務」は、要するに基幹インフラのサービスです。

次に、②にいう特定社会基盤事業者[13]とは、以下の 14 の対象分野[14]の事業を行う者のうち、重要設備の機能が停止・低下した場合に、サービスの安定的な提供に支障が生じ、国家・国民の安全を損なうおそれが大きいものとして主務省令で定める基準に該当する者と定義されています。各々の事業を所管する主務大臣（86 条 2 項）によって、具体的な事業者が指定され、その旨が公示されます（50 条 1 項、2 項）。

【対象分野】

電気	ガス	石油	水道	鉄道
貨物自動車運送	外航貨物	航空	空港	電気通信
放送	郵便	金融	クレジットカード	

また、主務大臣は、特定社会基盤事業者を指定するために必要な限度で、上記対象分野の事業を行う者に対して、必要な報告や資料の提出を求めることができます（58 条 1 項）。

③の審査に関して、主務大臣は、各特定社会基盤事業者から事前に届出がなされた導入等計画書に基づき妨害行為の手段として使用されるおそれが大きいかどうかを審査し、そのおそれが大きい場合には、④事業者に対する勧告及び勧告に応諾しない事業者に対する命令を行うことができます（52 条）[15]。

3. 基幹インフラの防護に関するサイバーセキュリティ上の留意点

経済安全保障推進法案による大まかなスキームは上記に示したとおりですが、どのような事業者がどのような基準で指定され、そして、どのような審査手続が行われるのかは、法律のみからは明らかではなく、国会における審議や下位法令の制定を待つ必要があります。

ただ、提言の中で、基幹インフラの防護については、サイバーセキュリティの文脈でいうサプライチェーン・リスクを含めたリスクの把握が必要とされている点に留意すべきと考えます。ここにいうサプライチェーン・リスクは、例えば、重要設備に用いている製品に悪意ある機能が組み込まれているために、その機能を用いたサイバー攻撃がなされ、基幹インフラの事業継続に影響を及ぼすおそれが生じてしまうリスク

[13] 類似の定義として、サイバーセキュリティ基本法 3 条 1 項は、いわゆる重要インフラ事業者を「重要社会基盤事業者」として定義しています。サイバーセキュリティ戦略本部は、情報通信、金融、航空、空港、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流、化学、クレジット、石油の 14 分野を重要インフラ分野と指定し、そのうちの一定の条件を満たす事業者を重要社会基盤事業者（重要インフラ事業者）と位置づけています。

[14] 14 の対象分野があるという点では、基幹インフラ分野と重要インフラ分野は同じであり、重複している分野も多いですが、例えば、重要インフラ分野とされている政府・行政サービスや医療が基幹インフラ分野とされていないなど、異なる部分も複数見受けられます。

[15] 提言の中で外国為替及び外国貿易法（外為法）27 条に基づく対内直接投資に言及していることや、条文構造に鑑みると、本法の下での審査は、外為法に基づく対内直接投資に関する審査スキームも参考にしたものになると考えられます。

や、特定社会基盤事業者自身は適切なサイバーセキュリティ対策を取っているが、重要設備の管理・運営を行う委託先を通じて特定社会基盤事業者が被害を受けるリスクが含まれていると考えられます。

特に前者のリスクに関しては、IT 調達申合せが関係してくる可能性があります。

IT 調達申合せは、各府省庁及び独立行政法人等が NISC 及びデジタル庁に助言を求める制度ですが、特定社会基盤事業者に関する審査に関しても、主務大臣は、勧告や命令を行う際には、あらかじめ内閣総理大臣その他関係行政機関の長に協議しなければならず（56 条 2 項）、また、主務大臣は、必要があると認めるときは、内閣総理大臣、関係行政機関の長その他の関係者に対して必要な協力を求めることができる（59 条）とされています。ここには当然 NISC やデジタル庁といったサイバーセキュリティ関係の機関も含まれます。

以上のとおり、提言におけるサプライチェーン・リスク及び IT 調達申合せへの言及と、経済安全保障推進法案における条文構造を見るに、基幹インフラに関する審査においては、IT 調達申合せに類似したスキームが導入される、又は、政府機関統一基準群や IT 調達申合せを引用した基準が設けられる可能性があると考えられます。

具体的にどのような制度になるかについては今後の動向を注視する必要があります。ただ、少なくとも、上記 14 の対象分野に該当する事業を行う事業者については、特定社会基盤事業者指定のために必要な範囲で、主務大臣から必要な報告や資料の提出が求められるなどの影響が及ぶ可能性がありますので、注意が必要です。

Ⅳ. 日本企業のサイバーセキュリティに対する脅威と対策の重要性

以上述べてきたように、今般の経済安全保障法案は、主として、政府組織を背景に持つサイバー攻撃から基幹インフラを防護するという観点から導入される予定の施策です。これによって直接的に影響を受ける事業者は、個別に指定される特定社会基盤事業者及びその委託先、また、指定を受けるかどうかという観点から調査対象となり得る 14 の対象分野に該当する事業を行う事業者といえます。

もっとも、これに該当しない事業者がサイバーセキュリティ対策を取らなくてよいということは全くありません。近時、いわゆる侵入型ランサムウェア攻撃をはじめとする、金銭窃取目的の犯罪者によるサイバー攻撃が増加しています。また、機密情報の窃取を狙うサイバー攻撃のケースにおいても、ターゲットに対する直接の攻撃ではなく、セキュリティが比較的手薄な取引先や海外拠点への攻撃を通じてターゲットが保有する機密情報の窃取を狙うケースも見られます（これも、サプライチェーンの弱点を突いた攻撃という点で、広い意味でサプライチェーン・リスクといえます）。当事務所においても、ランサムウェア被害に関する相談や、海外拠点に対する不正アクセスが発生した旨のご相談がさらに増加しており、例えば、2022 年 2 月に入ってから多数の被害が再度観測され始めているマルウェア「Emotet」（エモテット）についても、業種や規模に関係なくご相談が寄せられています。

さらに、今般のロシアによるウクライナ侵攻の影響も受けて、ロシアを拠点とするサイバー攻撃グループによるサイバー攻撃の激化にも留意が必要です。それが直接的な理由かどうかは明確ではありませんが、2022 年 3 月 1 日には、経済産業省、金融庁、総務省、厚生労働省、国土交通省（この 5 つは重要インフラ所管省庁です）、警察庁、NISC が共同で「サイバーセキュリティ対策の強化について（注意喚起）」を発出し、「昨今の情勢を踏まえるとサイバー攻撃事案のリスクが高まっていると考えられます」としており、一層の警戒が必要な状況にあるといえます[16]。

サイバーセキュリティに対する脅威が増す中で、企業としては、セキュリティインシデント（データの漏えい等や事業継続を脅かすシステム障害等）を予防するために、自社のみならず、グループ会社全体としての対策を講じる必要があります。

しかし、いかに適切な予防策をとったとしても、セキュリティインシデントの発生をゼロにすることは不可能であり、当事務所でも、サイバーセキュリティに関する助言を日常的にさせていただく中で、日々それを痛感しています。

サイバーセキュリティ対策を行う上では、インシデントの予防はもちろん、インシデントが発生することを前提に、その被害を最小限に抑えるための対策（例えば、インシデント対応のプランやサイバー攻撃等をトリガーとした BCP の策定、プランに沿った演習等）をあらかじめ講じておくことも重要です。

執筆主担当　弁護士　蔦 大輔（TSUTA Daisuke）

総務省行政管理局及び NISC において任期付職員として法改正等を担当し、当事務所でもサイバーセキュリティ、個人情報保護・プライバシー、IT・ICT を主な取扱い分野とする。近著として、『法律実務のためのデジタル・フォレンジックとサイバーセキュリティ』（商事法務 2021 年、共著）、『情報漏えい・サイバーセキュリティインシデント発生時の実務対応』（商事法務 NBL、2021 年）等。

[16] https://www.nisc.go.jp/press/pdf/20220301NISC_press.pdf

セミナー情報

- セミナー　『ロシア制裁強化の可能性と日本企業の備え』
  視聴期間　2022 年 2 月 8 日（火）～2022 年 3 月 7 日（月）
  講師　梅津 英明、大川 信太郎
  主催　森・濱田松本法律事務所

- セミナー　『アクティビスト株主対応における外為法の実務～立案担当者が教える日本企業からみた外為法のポイント～』
  開催日時　2022 年 2 月 28 日（月）　13:30～16:30
  講師　大川 信太郎
  主催　株式会社金融財務研究会

- セミナー　『第 4809 回金融ファクシミリ新聞社セミナー「企業における不正・不祥事の発生防止と発覚時の迅速・適格な対応ーサステナブルな経営を実現するためにコンプライアンス態勢の確立をー」』
  開催日時　2022 年 3 月 8 日（火）　13:30～15:30
  講師　木山 二郎
  主催　株式会社 FN コミュニケーションズ

- セミナー　『RCEP 完全対応！EPA を通じた輸出入コスト削減とビジネス拡大の基本と実践』
  開催日時　2022 年 4 月 8 日（金）　10:00～12:00
  講師　宮岡 邦生
  主催　株式会社金融財務研究会

- セミナー　『第 4844 回金融ファクシミリ新聞社セミナー「今、日本企業に求められる「ビジネスと人権」の実務対応のポイント」』
  開催日時　2022 年 4 月 14 日（木）　13:30～16:30
  講師　御代田 有恒
  主催　株式会社 FN コミュニケーションズ

文献情報

- 本　『ドローン・ビジネスと法規制（第 2 版）』
  出版社　株式会社清文社
  編集代表　戸嶋 浩二、林 浩美、岡田 淳、佐藤 典仁、島田 里奈、木村 純、輪千 浩平、福澤 寛人

- 本　『リーガル・トランスフォーメーション　ビジネス・ルール・チェンジ 2022』
  出版社　日本経済新聞出版社
  著者　棚橋 元、石本 茂彦、高谷 知佐子、飯田 耕一郎、武川 丈士、山崎 良太、梅津 英明、渡辺 邦広、末廣 裕亮、東 陽介、石橋 誠之、羽深 宏樹

- 論文　「経済安全保障と人権問題の交錯と対応の難しさ」
  掲載サイト　NBL No.1211
  著者等　石本 茂彦

- 本　『詳解 外為法 貿易管理編――外国法令も踏まえた理論と実務』
  出版社　株式会社商事法務
  著者　大川 信太郎

NEWS

- Chambers Global 2022 にて高い評価を得ました

  Chambers Global 2022 にて当事務所は日本における複数の分野で上位グループにランキングされ、International Trade 分野では、石本 茂彦、梅津 英明が高い評価を得ました。
  さらにタイ（Chandler MHM Limited）、ミャンマー（Myanmar Legal MHM Limited）及び中国においても以下の分野で上位グループにランキングされ、各オフィスに所属する弁護士がその分野で高い評価を得ております。
  詳細は Chambers のウェブサイトに掲載されております。

- 小川 智史 弁護士のコメントが、2022 年 2 月 8 日付 MLex の『Japan's METI presents AI guidelines amid global moves to regulate biased algorithms』と題した記事に掲載されました

- 蔦 大輔 弁護士のコメントが、読売新聞 34 面『[サイバーテロ　病院の危機] ＜2＞「予算ない」「知らなかった」…脆弱性　見過ごし被害』と題した記事に掲載されました

（当事務所に関するお問い合せ）
森・濱田松本法律事務所　広報担当
mhm_info@mhm-global.com
03-6212-8330
www.mhmjapan.com