経済産業省委託事業

シンガポールにおける
営業秘密管理マニュアル

2022 年 3 月
独立行政法人　日本貿易振興機構
シンガポール事務所
(知的財産部)

報告書の利用についての注意・免責事項

本報告書は、日本貿易振興機構（ジェトロ）が現地調査会社に委託し作成したものであり、調査後の法律改正などによって情報が変わる場合があります。掲載した情報・コメントは調査委託先の判断によるものであり、情報の正確性や一般的な解釈がこのとおりであることを保証するものではありません。また、本報告書はあくまでも参考情報の提供を目的としており、法的助言を構成するものではなく、法的助言として依拠すべきものではありません。本報告書にてご提供する情報等に基づいて行為をされる場合には、必ず個別の事案に沿った具体的な法的助言を別途お求め下さい。

ジェトロおよび調査委託先は、本報告書の記載内容に関して生じた直接的、間接的、派生的、特別の、付随的、あるいは懲罰的な損害および利益の喪失について、それが契約、不法行為、無過失責任、あるいはその他の原因に基づき生じたかにかかわらず、一切の責任を負いません。これは、たとえジェトロまたは調査委託先が係る損害等の可能性を知らされていても同様とします。

JETRO - 営業秘密マニュアル

目次

I. はじめに

市場において、自社製品・サービスが競争力を発揮するためには、それらを支える自社独自の技術情報や営業情報といった営業秘密を適切に保護することは極めて重要であり、製造、販売等の拠点を海外にも有する場合には、各国における関連法規や権利行使のプラクティス、商習慣等の相違を考慮した上で、拠点ごとに営業秘密を適切に管理する必要がある。

とりわけ、シンガポールでは営業秘密が法令において定義されていないことから、ある情報が営業秘密であるかを判断するにあたって裁判例を考慮する必要がある。例えば、シンガポールでは、「営業秘密」に該当するために必要な要件は存在しないが、裁判所は、ある情報が「営業秘密」であるか否かを判断するに当たって、情報の性質、情報にアクセスすることを許可された者、及び当該情報を保護するために実施されている保護措置などを含む、多くの要因を考慮に入れることとしている。

そこで、本稿は、こうした実情を踏まえ、日系企業のシンガポールにおける営業秘密管理体制の整備・構築、又はその見直しに資するべく、シンガポールにおける営業秘密の管理方法について、現地専門家の経験を踏まえて、基本マニュアルとしてまとめたものである。

本稿は、「法制度編」と「漏えい対策実践編」から構成され、いずれのパートについても、日本との異同や日本との比較において、シンガポールで特に留意すべき点を中心に説明している。もっとも、シンガポールにおいて、営業秘密の不正取得からの保護、競合者による営業秘密の利用に対処するという点で、日本における営業秘密管理の考え方と共通する部分も多く、経済産業省の「秘密情報の保護ハンドブック～企業価値向上に向けて～」（以下、本稿では「ハンドブック」という。）の内容が参考になると考えられるため、本稿とあわせて活用することで、ぜひ、シンガポールにおける営業秘密の管理の整備にお役立て頂きたい。

II. 第 1 部:法制度

(1) シンガポールにおける営業秘密の定義と範囲（シンガポールと日本の違い）

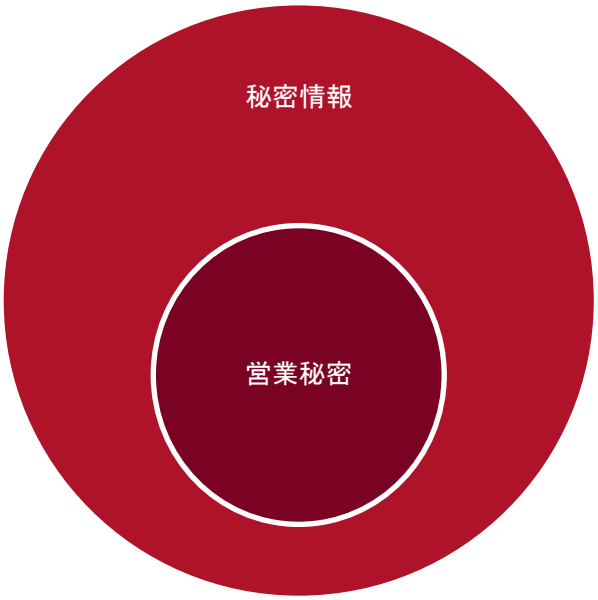
1.1 「営業秘密」の定義

シンガポールにおける営業秘密の保護について、同国はＷＴＯ（世界貿易機関）の加盟国であり、ＴＲＩＰＳ協定（知的所有権の貿易関連側面に関する協定）において「開示されていない情報の保護」（同協定第 39 条）が加盟国の義務として定められていることから、日本と同様、企業・事業者等が保有する営業秘密について、法的な保護を受けることが可能である。

しかし、アメリカやイギリスなど判例法（コモンロー）が主たる法源となるシンガポールでは、日本の不正競争防止法のような営業秘密の保護を規定する明確な法律は存在せず、「営業秘密」という用語の法律上の定義も存在しない。「営業秘密」という用語は一般的に、高度に秘密であるか又は機微性の高い情報、例えば秘密の化学式や秘密の製造プロセスを指すものとされている[1]。

シンガポールの裁判所では、営業秘密は、秘密情報の一形態であって、その中で最高度の秘密性を有するもの、としている。下の図は、秘密情報と営業秘密の関係を示したもので、営業秘密は秘密情報の一部に含まれるものとなっている。

[1] Ng-Loy Wee Loon, *Law of Intellectual Property in Singapore* （「Ng-Loy 論文」）, [38.0.1].



「秘密情報」についても、法令上の定義はない。「秘密情報」は、一般に「必要な程度の秘密性を有する情報」をいうとされている[2]。その意味するところは、当該情報がパブリックドメインの中で自由に利用可能な状態ではなく[3]、かつ、公有の財産又は公知の知識となっていないこと、である[4]。裁判所は、ある情報が秘密であるかの判断にあたって、過去の裁判所の判決を参照することができる。シンガポール及びその他のコモンローの国、例えば英国、カナダ、香港、そしてオーストラリアなどの裁判所の判決が公開されている。

営業秘密に関する裁判所の判決の内容又は記録の公開にあたっては、特段の制限はない。

従業員との関係では、特に退職した従業員について、「営業秘密」と、

---

2 Ng-Loy 論文 [39.1.1].

3 Stratech Systems Ltd v Guthrie Properties (S) Pte Ltd [2001] SGHC 77 (「Stratech 事件」) at [37]。また、https://www.ipos.gov.sg/about-ip/other-ips/confidential-information-trade-secrets で閲覧可能（2020 年 12 月 20 日時点）である、シンガポール知的財産局 (「IPOS」)の「*Confidential Information & Trade Secrets*」(「IPOS - CI & TS」)も参照のこと。

4 Stratech 事件で高等裁判所の引用した、*Saltman Engineering Co Ltd v Campbell Engineering Co. Ltd* [1948] 65 RPC 203 at 215

営業秘密のレベルに達しない単なる「秘密情報」との区別が重要となることがある。

- 営業秘密については、雇用後に従業員であった者が当該営業秘密を開示又は使用しないことは、黙示的な義務となっている。黙示的な義務は、明示的な書面による義務がなかったとしても適用される。
- 対照的に、このような黙示的な義務は、単なる秘密情報については存在しない。退職者は通常、退職後の当該秘密情報の使用及び開示に関して、雇用契約における明示的な条件にのみ拘束される。

営業秘密又はこれと同等のものに具体的に何が該当するのかという網羅的なリストは存在しない。製造過程における秘密などは営業秘密の典型例であるが、この他、無数の多様な情報が営業秘密となりうる。もっとも、一部の情報については、それが秘密といえる期間は短いかもしれない。例えば、特許による保護を求めて企業自身が情報を公衆に開示することによって、当該情報が秘密性を失う場合などがある[5]。

最終的に、ある情報が営業秘密であるか否かを決定する際には、裁判所は、情報の性質、それにアクセスすることを許可された者の指定、流通の程度、及び自由に開示することができる他の情報から容易に分離することができるか否かを含め、様々な要素について検討を行う。これは、事案ごとの判断となる。秘密情報（4 ページを参照のこと）と同様に、ある情報が営業秘密であるかどうかの判断にあたっては、裁判所は過去の裁判例を参照することができる。

1.2 営業秘密の保護の範囲

シンガポールでは、秘密情報について出願・登録などの手続きはなく、また、秘密情報又は営業秘密が保護される期間についての法定の期間又は制限も存在しない。

一般的に、営業秘密は、コモンロー上の秘密侵害の原則（「**BOC: breach of confidence**」）、及び（該当する場合には）知的財産（「**IP : Intellectual Property**」）法及び契約法により保護される。秘密情報（営業秘密を含む。）を知り得た者は、一般に秘密を保持する義務を負

5 *Tang Siew Choy v Certact Pte Ltd* [1993] 1 SLR(R) 835 at [16].

い、第三者に開示することはできない。もし秘密情報を開示した場合、その者は、当該秘密情報の所有者に対して、BOC に基づく不法行為について責任を負うこととなる。

典型的には、秘密情報は、多くの手段を通じて保護される。例えば秘密保持契約（「**NDA: non-disclosure agreement**」）では、契約上、当事者の情報を秘密に保持すること、当該情報へのアクセスを制限すること、組織内で適切な手順を講じること、当該秘密情報と営業秘密の流布に関する明確な記録を保持することを要求する[6]。「当該秘密情報と営業秘密の流布に関する明確な記録を保持すること」とは、例えば、組織は、機密情報の開示先、開示日、開示された機密情報、及びそのような開示に付随し、関連する保護措置について記録しておくことなどである。

1.3 シンガポールと日本の違い

日本とシンガポールにおける「営業秘密」の定義の比較を、下の図に示す。

シンガポール	日本
•法令において定義されていない。 •秘密情報の一形態である。 •一般的には、高度に秘密又は機微性の高い情報を示す。 •ある情報が営業秘密であるかを判断するにあたって、裁判所は多数の要素を考慮する。例えば、情報の性質、これにアクセスすることが許されている人物の指定の有無、情報の配布が許されている範囲、当該情報が他の自由に開示できる情報から容易に区別できるようになっているか、等である。	•不正競争防止法（不競法）において、「技術上又は営業上の情報」であって以下を満たすものとして明示的に定義されている。 ・ 保有者の事業活動に有用な価値ある情報であること ・ 秘密として保有または管理されていること ・ 公然と知られていないこと ・ただし、不競法は、上記の各要素についてのさらなる定義は定めていない。

日本の不正競争防止法（不競法）では、当該情報が秘密情報として管理されていることを立証するためには、営業秘密保有企業が当該情報を秘密であると単に主観的に認識しているだけでは不十分であり、営

6 IPOS - CI & TS

業秘密保有企業の秘密管理意思（特定の情報を秘密として管理しようとする意思）が、具体的状況に応じた経済合理的な秘密管理措置[7]によって、従業員に明確に示され、結果として、従業員が当該秘密の保有者の秘密管理意思を容易に認識できる（換言すれば、認識可能性が確保される）必要がある。しかし、シンガポールとは異なり、一般的な「秘密情報」と比較して「営業秘密」が高度に秘密である、又は機微情報であることは要求されていない。

シンガポールのルールと日本の不競法とのもう一つの大きな違いは、不競法ではどのような行為が不競法違反（すなわち、営業秘密の侵害）を構成するかを規定していることである。その行為は、次のとおりである（括弧内は該当条文）。

- 窃盗、詐欺、強迫その他不正の手段により営業秘密を取得し、又は当該不正取得により取得した営業秘密を使用し、もしくは開示する行為（不競法第 2 条第 1 項第 4 号）
- その営業秘密について不正取得が行われたことを知って、又は重大な過失により知らないで営業秘密を取得し、使用し、もしくは開示する行為（不競法第 2 条第 1 項第 5 号）
- 当該営業秘密について不正取得があったことを知った後、又は、重大な過失により知らなかった場合に、取得した営業秘密を使用又は開示する行為（不競法第 2 条第 1 項第 6 号）
- 不正の利益を得る、又は保有者に危害を加える目的で保有者から示された営業秘密を使用し、又は開示する行為（不競法第 2

7 秘密管理性要件は、従来、①情報にアクセスできる者が制限されていること（アクセス制限）、②情報にアクセスした者に当該情報が営業秘密であることが認識できるようにされていること（認識可能性）の 2 つが判断の要素になると説明されてきた。しかしながら、両者は秘密管理性の有無を判断する重要なファクターであるが、それぞれ別個独立した要件ではなく、「アクセス制限」は、「認識可能性」を担保する一つの手段であると考えられる。したがって、情報にアクセスした者が秘密であると認識できる（「認識可能性」を満たす）場合に、十分なアクセス制限がないことを根拠に秘密管理性が否定されることはない。もっとも、従業員等がある情報について秘密情報であると現実に認識していれば、営業秘密保有企業による秘密管理措置が全く必要ではないということではない。法の条文上「秘密として管理されている」と規定されていることを踏まえれば（法第２条第６項）、何らの秘密管理措置がなされていない場合には秘密管理性要件は満たさないと考えられる。

条第 1 項第 7 号）

- 上記の不正取得行為により営業秘密が開示されていることを知って、又は重大な過失により知らないで、営業秘密を取得し、使用し、又は開示する行為（不競法第 2 条第 1 項第 8 号）
- 不正取得行為により当該営業秘密が開示されたことを知った後、もしくは重大な過失により知らなかった場合に、当該営業秘密を使用し、又は開示する行為（不競法第 2 条第 1 項第 9 号）
- 技術上の営業秘密の前述の使用行為（不正使用行為）によって生じた物を譲渡、引き渡し、展示、輸入、輸入、又は電気通信回線を通じて提供する行為（不競法第 2 条第 1 項第 10 号）

さらに、シンガポールでは、単なる秘密情報と区別して別途営業秘密を定義し、営業秘密にのみ退職者が在職中の営業秘密を開示又は使用しないという黙示の義務が課される。一方で、日本の不競法はこのような構造を採用していない。

他方、日本における営業秘密の保護に関する法律の規定は、以下の点でシンガポールのルールと同一である。

- 営業秘密の出願・登録手続きは存在せず、営業秘密を保護することができる期間を規定した法定の期間又は制限も存在しない。
- また、特許法等の知的財産法、契約法、不法行為法の違反（該当する場合）の原則により、不競法上の営業秘密に該当しない情報を保護することも可能である。
- 日本でも、秘密保持契約（「NDA」という。）を通じて、契約上、当事者に保持している情報を秘密にすること、当該情報へのアクセスを制限すること、適切な手段を講じ、当該秘密情報・営業秘密の流出に関する明確な記録を保持することなどを要求することにより秘密情報を保護することが一般的である。

1.4 まとめ

- シンガポールにおいて、営業秘密は秘密情報の一形態である。
- シンガポールにおいて、「営業秘密」あるいは「秘密情報」についての法律上の定義はないが、判例法であるコモンローによ

り、「営業秘密」は秘密情報のうち高い程度の秘密性を有するものとされている。他方で「秘密情報」は一般に、パブリックドメインの中で自由に利用可能な状態ではない、必要な程度の秘密性を有する情報を指すものとされている。

- この点で、「営業秘密」について不競法による明示的な定義を置いている日本とは異なる。
- 営業秘密は一般的に、コモンロー上の法理である「BOC」、及び要件を満たす場合には知的財産法及び契約法において保護されている。

(2) 営業秘密の管理方法

2.1 <u>企業機密をどう管理・共有するか　－　保護のための実務</u>

1. 上記のとおり、シンガポールでは「営業秘密」は定義されておらず、情報の一部が「営業秘密」に該当するために必要な決まった要素は存在しない。しかしながら、裁判所は、ある情報が「営業秘密」であるか否かを判断するに当たって、情報の性質、情報にアクセスすることを許可された者、及び当該情報を保護するために実施されている保護措置などを含む、多くの要因を考慮に入れる。したがって、営業秘密を保有するすべての組織は、中小企業から国際的な企業に至るまで、その営業秘密を保護するための実効的な措置を講じるべきである。

企業の内部及び外部で（例えば、シンガポール法人と、現地パートナー企業及び委託先との間の関係において）営業秘密を管理するための4つの重要なステップは、次のとおりである:

- 企業等が保有する情報の中から営業秘密を特定すること。
- 企業の営業秘密のカタログ又はリストを作成し、どのような営業秘密を企業が保有し、当該営業秘密の秘密管理措置としてどのような保護手段が講じられているかを継続して確認・フォローできるよう、随時更新すること。
- 営業秘密保護のための契約や、物理的及び技術的措置を組織全

体で講じること。

- 不正があった場合の行動計画を策定すること。

これらの施策は、社内で、またグループ会社における子会社間で横断的に適用されるべきである。もちろん、各社の正確な対応策や対応計画は、事業や業務の性質、営業秘密の性質、従業員の営業秘密へのアクセスの必要性、グループ会社間取引の性質などを考慮に入れて策定されるべきである。

4 つのステップの詳細と、営業秘密の漏洩防止のための具体的な対策については、第 2 部(1)「シンガポールにおける秘密情報の管理の方策」を参照されたい。III

2.2 <u>シンガポール国外への営業秘密の移転</u>

日本の不競法では、不正に取得した営業秘密（情報自体）の開示について不競法に違反すると定めているところ（不競法第 2 条第 1 項第 4 号～第 9 号)、開示先について国内向け・国内向けの区別はないことから、いずれも営業秘密の開示（移転）として不競法に違反することとなる。また、不正に入手した営業秘密の使用行為により生じた物を譲渡し、引き渡し、譲渡若しくは引渡しのために展示し、輸出し、輸入し、又は電磁的に提供する行為も不競法に違反すると定めている（不競法第 2 条第 1 項第 10 号)。

シンガポールでは、営業秘密をシンガポールから他国へ開示・移転することを規制する法律は存在しない。しかし、営業秘密の侵害により生じた物の譲渡、引き渡し、譲渡若しくは引渡しのための展示、輸出、輸入、又は電磁的提供行為については、下記の第 I 部(3)(3.1)で解説する BOC に基づく請求原因のための 3 要素を満たす場合には、侵害行為となりうる。

一般的に、企業としては、開示・移転される営業秘密を特定し、そのような営業秘密の開示・移転を保護するための措置を講じ、そのような措置が現場で適切に実施されることを確保すべきである。

さらに、当該営業秘密が 2012 年シンガポール個人データ保護法(「**PDPA** (Singapore Personal Data Protection Act 2012)」)に基づく

「個人データ」を構成する範囲において、組織[8]は、当該営業秘密がPDPA第26条に基づく「**移転制限義務**」を遵守することを確認しなければならない。これにより、シンガポール国外の国又は地域への個人データの移転は、移転された個人データに付与される保護の基準がPDPAに基づき提供される保護と同等であることを確実にする、という法の要件に従う場合を除き、禁止されている[9]。

この点は、例えば、当該営業秘密にPDPAの下で「個人データ」とみなされる顧客リスト及び情報が含まれる場合などに関係する可能性がある。

移転制限義務の内容に関して、2014年個人データ保護規則（Personal Data Protection Regulations 2014。「本**規則**」）は、組織が個人データをシンガポール国外の国又は地域に移転する前に、次のことをしなければならないと規定している。

- 移転された個人データに関してPDPAの他のすべての条項に確実に準拠するために適切な措置を講じること
- 移転された個人データの受領者が、移転された個人データに少なくともPDPAの保護と同等の保護基準を提供するという法的強制力のある義務に拘束されることを確保するために、適切な措置を講じること

法的強制力のある義務は、2つの方法で受領者に対して課すことが可能である[10]。

---

8 PDPAに基づき、「組織」とは、(a)シンガポールの法律に基づき設立されたか承認されたか否かを問わず、または(b)シンガポールに居住するか、または事務所もしくは事業所を有するか否かを問わず、業務であるか非業務であるかを問わず、あらゆる個人、会社、団体または個人の団体を含む。第2条参照。

9 PDPA第2条は、「個人データ」を、「個人に関するデータであって、当該データから、又は当該データと組織が実際にアクセス又はアクセスする可能性のあるその他の情報から当該個人を識別することができるもので、真実であるか否かを問わない」と定義している。

10 シンガポール個人情報保護委員会(「PDPC」)、特定のトピックスに関する個人情報保護法に関する諮問指針（*Advisory Guidelines on the Personal Data Protection Act for Selected Topics*）(2020年6月2日改訂)(「主要概念に関する指針」)(https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Advisory-Guidelines-on-Key-Concepts-in-the-PDPA-(2-June-2020).pdf?la=en)、19.3項及び19.4項参照)。

- 第 1 に、以下のいずれかの形態で受領者に課す場合。

  (i) 法律（規則を含むがこれに限定されない。）

  (ii) 個人データを移転することができる国及び地域を限定した契約

  (iii) 拘束力のある会社規則[11]であって、当該拘束力のある会社規則が適用される移転個人データの受領者、当該個人データが移転される国及び地域、並びに拘束力のある会社規則により課されるそれぞれの権利及び義務を定めているもの

  (iv) その他の、法的拘束力のある証書[12]

- 第 2 に、個人データが転送される国又は地域の法律に基づき付与又は承認された「特定認証（specified certification）」を受領する主体が保有している場合。なお、「特定認証」とは、アジア太平洋経済協力　越境プライバシー規則(「APEC CBPR」)システム又はアジア太平洋経済協力　プライバシー処理者認定(「APEC PRP」)システムに基づく認証を意味する。これは、シンガポールと日本の両国が APEC CBPR システムに参加していることに関連している。PDPA が受領する主体に課す移転制限義務は、以下の場合に満たされる。

  (i) 受領者が組織として個人データを受領し、有効な APEC CBPR システムの認証を保有している場合

  (ii) 受領者が、個人データをデータ仲介者[13]として受領し、

---

11 このような拘束力のある会社規則は、受領者が移転する側の組織に関連する組織であり、まだ移転に関連する他の法的強制力のある義務（規則に定められているもの）をまだ受けていない場合に、採択することができる。さらに、規則では、次の場合、受領者が「移転する側の組織に関連している」と規定している。すなわち、 (a) 受領者が、直接・間接を問わず、移転する側の組織を支配している場合 (b) 受領者が、直接・間接を問わず、移転する側の組織によって支配されている場合 (c) 受領者と移転組織が、直接・間接を問わず、共通の者の支配下にある場合、である。

12 主要概念に関する指針、第 19 章

13 PDPA の下では、「データ仲介業者」とは、他の組織に代わって個人データを処理する組織を意味するが、他の組織の従業員は含まない。第 2 章参照。また、「処理」とは、個人データに関連して業務又は一連の業務を遂行することを意味し、記録、

有効な APEC CBPR 又は PRP システムの認証のいずれか、又はその両方を保有している場合

さらに、事業者が提供するクラウドサービスを使用して個人データがシンガポール国外に転送される場合、当該サービスを利用する企業は、当該事業者が、(a)同等のデータ保護体制を有する場所にのみデータを転送すること、又は(b)移転されたデータについて同程度の保護基準を保証する法的強制力のある義務を負うこと、を保証しなければならない。これは、クラウドサービス提供事業者との適切な条件による契約を通じて行うことが可能である[14]。

たとえば、ある組織 ABC が、グループの集中的な顧客管理システムを通じて、顧客の個人データを海外の親会社に移転しているとする。移転される個人データに適用される保護の規定を含む移転の条件は、組織 ABC とその本社の双方に適用される拘束力のある会社規則に定められている。組織 ABC は、これらの拘束力のある会社規則を検討し、それらが規則に基づいて定められた条件を満たしており、PDPA に基づく基準と同等の保護を提供するものであると評価した。この場合、組織 ABC の海外への個人データの譲渡は、譲渡制限義務を遵守したものとされる[15]。

営業秘密の漏洩防止のための具体的な対策については、第 2 部を参照のこと。III

2.3 登録要件

シンガポールには営業秘密保護の登録要件は存在しない。

2.4 まとめ

- 企業は、保有する営業秘密を特定しリスト化するためのシステムを導入し、営業秘密を保護するための契約上、物理的、技術

保管、整理、改変、検索、組合せ、送信及び消去又は破棄を含む。第 2 章参照。

14 個人データ保護委員会の「特定のトピックスに関する個人情報保護法に関する諮問指針（*Advisory Guidelines on the Personal Data Protection Act for Selected Topics*）」(2019 年 10 月 9 日改訂)。https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Selected-Topics/Advisory-Guidelines-on-PDPA-for-Selected-Topics-9-Oct-2019.pdf?la=en で閲覧可能（2020 年 12 月 20 日時点）である。

15 *主要概念に関するガイドライン*、19.6 項。

的、組織的な保護措置を導入し、不適切な取り扱いがあった場合のアクションプランを策定するべきである。

- 営業秘密をシンガポール国外に開示・移転すること自体を規制する法律は存在しない。しかし、企業は、当該開示・移転が関連の法律を遵守したものであることの確認をする必要がある。
- シンガポールでは、営業秘密を保護するにあたって営業秘密を登録することは必要とされていないし、またそのための制度も存在しない。

(3) 営業秘密の侵害

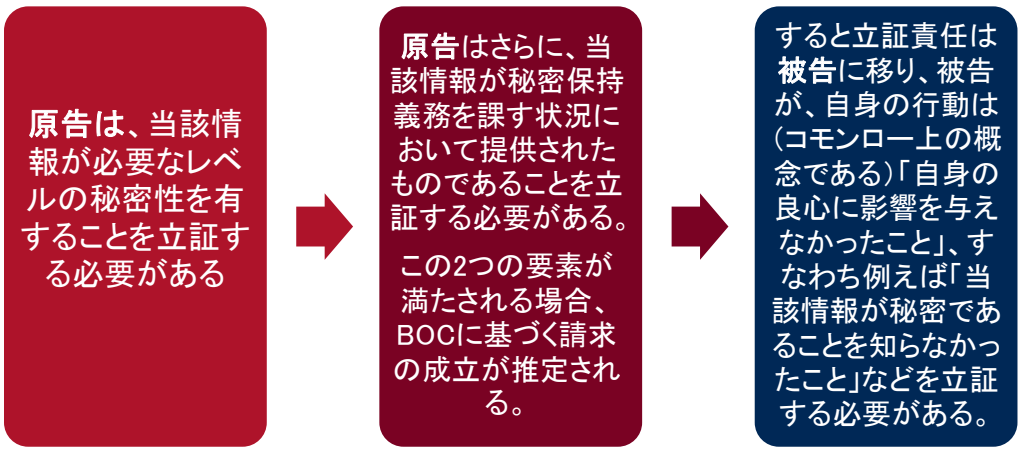
上記のように、営業秘密は、一般的にBOCに関するコモンローの原則、知的財産法、そして契約法などによって保護されている。以下、各概念について説明する。

3.1 秘密保持義務違反（BOC）

秘密情報（営業秘密を含む。）にアクセスできる者は、一般に秘密を保持する義務を負い、第三者に開示することはできない。当該情報を開示する者は、当該秘密情報の所有者に対し、BOC に基づく不法行為について責任を負う。

BOCに基づく訴訟は、以下のステップで行われる[16]。

[16] *I-Admin (Singapore) Pte Ltd v Hong Ying Ting and others* [2020] 1 SLR 1130（「*I-Admin 事件*」の [61]。



(A)　当該情報は、秘密でなければならない

必要な程度の秘密性を有する情報とは、公衆が自由に入手できない情報をいう[17]。現段階では、営業秘密に関する企業内の方針及び保護措置が取られていることをもって、営業秘密が公衆の利用に供されていないことを証明することを助けることができる[18]。

(B)　情報は、秘密保持義務を課す状況において提供されなければならない

BOC に基づく請求の第 2 の要素は、営業秘密の所有者・占有者と受領者との間に明示的に（例えば、雇用契約又は秘密保持契約の中の秘密保持条項を通じて）又は黙示的に、当該営業秘密に関して秘密を保持する義務を課す契約が存在する場合に満たされる[19]。

そのような明示的又は黙示的な契約上の義務がない場合でも（すなわち、法的義務がない場合であっても）、当事者は、依然として、営業秘密を守る衡平法上の義務を負う場合がある。つまり、当事者間で秘密保持義務を定めた契約がない場合でも、秘密情報を受け取った当事者に、そのような情報を秘密にすることを義務付ける衡平法上の義務を

17　*Stratech* 事件の[33]

18　*Clearlab SG Pte Ltd v Ting Chong Chai* [2015] 1 SLR 163 （「*Clearlab* 事件」）の[135]を参照。

19　*Clearlab* 事件の[65]を参照。

課すことができる。営業秘密が開示された状況が、合理的な人物がその状況を考慮すれば、当該情報が当事者にとって秘密であることを認識できるような状況であることについて、当事者が証明することができる場合に衡平法上の義務が生じ、従って受領当事者に衡平法上の守秘義務が課されることになる。

この段階において、営業秘密、企業内の慣行、従業員に与えられた営業秘密へのアクセス権の程度、及び営業秘密の管理及び保護の方法に関する企業の規定類及び保護措置の存在は、当該秘密が秘密保持義務が課された状況下で開示されたことを証明するのに有用である。

(C)　被告による、（コモンロー上の概念である）「良心が影響されなかったこと」の証明

上記 2 つの要素が満たされた時点で、BOC に基づいた請求の成立が推定されるため、被告が、これに対する反証をしなければならない。例えば、以下のような事情の存在の証明である。

- 営業秘密が、必要な程度の秘密性を有していなかったこと、又は秘密保持義務を課す状況において付与されなかったこと。例えば、当該営業秘密について、当該企業の従業員が自由に営業秘密にアクセスし、そして公知となったことや、当該営業秘密が既に公知となっていたことを証明できる場合がある。
- コモンロー上の概念である「良心が影響を受けなかった」こと。これは例えば以下のようなものである。

    (iii)　情報の秘密性を知らなかった場合（意図的に知らないようにした場合の判断や、被告側の過失が本要件の判断に影響するのかといった点については、議論の余地がある。）

    (iv)　偶然その情報に触れた場合

    (v)　当該情報が、公衆の利用に供された物、又は取得者が合法的に所有していた物から、独立の創作又は独立の研究・リバースエンジニアリングを通じて取得された場合

    (vi)　公衆の利益に関するものであって、公にされるべき情報である場合（例えば、情報が何らかの不正に関する情報

である場合)。この抗弁は、警察等の、情報を受領する適切な利害関係を有する者に対する開示のみが対象である。

3.2 その他の、実務上可能な請求原因

(A) 著作権法

著作物（例えば、取扱説明書、コンピュータソフトウェア、データベースなど）から構成される営業秘密は、秘密情報に関する法の規定に加え、著作権法によって保護される[20]。

例えば、コンピュータソフトウェア開発者は、基盤となるソフトウェアアーキテクチャ、アルゴリズム、ソースコードの著作権者として、それらの機密性を保ちつつ、自らのソフトウェアを商業化することができる。

したがって、著作物である営業秘密の所有者は、当該著作物を侵害した者に対し、著作権侵害に基づく救済を求めることができる。これらには民事上の救済措置及び刑事上の制裁措置も含まれる（下記第 1 部(4)4.2 を参照)。II3.24.2

(B) 契約違反

営業秘密の所有者と侵害者との間に当該営業秘密を保護する契約がある場合は、侵害者は契約違反という点に対しても責任を負う可能性がある。これは、両当事者間の契約条件及び両当事者の関係によることになる。

(C) 時効について

BOC、著作権侵害、契約違反に基づく訴えの時効期間は、請求原因の発生した日から 6 年間となっている。

3.3 まとめ

- 営業秘密は、まず BOC の法理によって保護される。
- 営業秘密の不正な使用が著作権の侵害にも該当する場合、損害

[20] なお、一般原則として、秘密情報に関して特許による保護を求めることはできない。特許を取得した場合は他者が当該発明を使用する行為を排除する 20 年間の独占的な権利が付与されるが、代わりに、特許の出願の過程で発明を公開しなければならない。従って、当該情報はパブリックドメインとなり、秘密とは言えなくなるからである。

を受けた当事者は侵害者に対して、著作権侵害に基づく訴えを起こすことができる。

- 営業秘密の所有者と侵害者との間に当該営業秘密を保護することを内容とした契約が存在する場合は、侵害者は契約違反の責任も負うことになる。

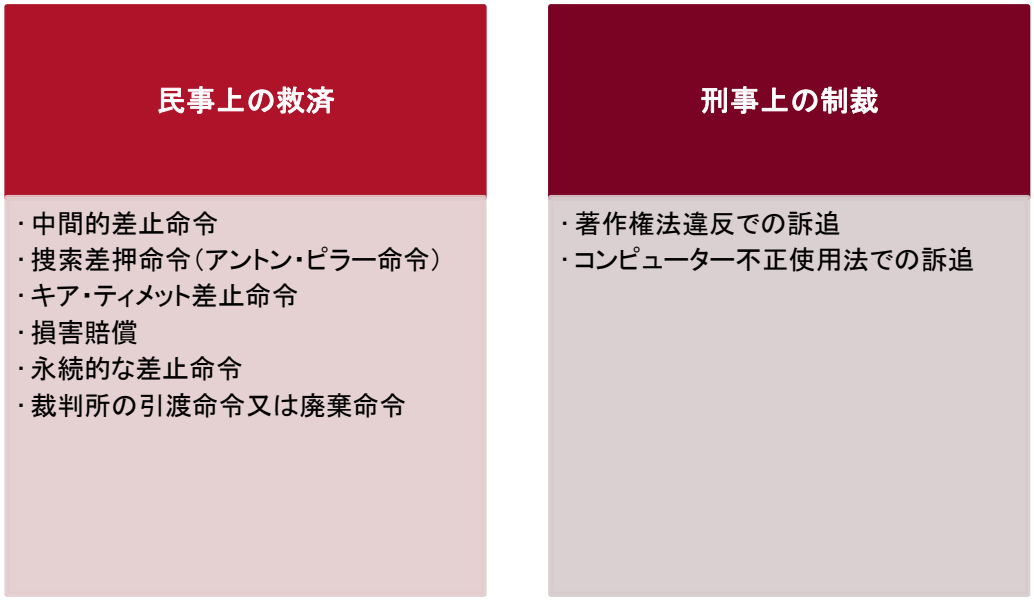
(4) 救済手段

シンガポールにおいては、下記のような、日本の不競法において認められている秘密性の立証のための立証手段又は証拠収集手段が用意されているわけではない。

- 技術上の秘密を取得した者の当該技術上の秘密を使用する行為等の推定（不競法第 5 条の 2）
- 損害の額の推定等（不競法第 5 条）
- 秘密保持命令（不競法第 10 条）
- 当事者尋問等の公開停止（不競法第 13 条）

日本の法制度では、裁判所が当事者及び代理人に対して、審理中に提出された情報を第三者に対して公開することを禁じる秘密保持命令（不競法第 10 条）を出すことができる。この秘密保持命令違反に対しては、刑事罰も用意されている（不競法第 21 条第 2 項第 6 号）。

一方、シンガポールの裁判所でも、当事者が裁判所に対し、BOC の訴えにおける秘密情報を保護するための措置の申し出を行うことが可能である。例えば、第三者への開示を防ぐために、書面を名前で特定された「秘密のグループ」に対してのみ書面を公開することや、裁判ファイルに第三者がアクセスすることを禁止する封入命令、審理手続が非公開の法廷でのみ行われることを申し入れることが可能である。下の表は、シンガポールにおいて、営業秘密の侵害に対して認められている民事上及び刑事上の救済手段の概要を示したものである。



4.1 民事上の救済手段

(A) 暫定的な救済

(i) 仮処分命令

BOC の状況では、被害を受けた秘密情報又は営業秘密の所有者・占有者は、裁判や仲裁の結果又はその他の事項の最終決定が出るまで、侵害者がその秘密情報・営業秘密を使用、悪用、開示、複製又はその他の方法で取り扱うことを防止するために、暫定的又は仮の差止命令を取得することを試みることができる。すなわち、シンガポールの裁判所は、当事者が秘密情報・営業秘密を第三者に開示することを、事件の審理の時まで禁止する命令を出すことが可能となっている。シンガポール裁判所規則（Singapore Rules of Court）の Order 29 が、裁判所に、仮処分命令の権限を与えている。

暫定的差止命令を認めるべきか否かを検討するに当たり、裁判所は、次のことについて確証を得なければならない。

- 審理されるべき、深刻な問題があること（すなわち、その主張が法律上取り上げる価値がないもの、又は訴権の乱用的なものではないこと）。
- 差止命令が発せられない場合、損害賠償という手段では、請求人に加えられる可能性のある損害に対する適切な救済とはなら

ないこと。

- 比較衡量の結果、差止命令を認めることが好ましいと認められること。

(ii)　アントン・ピラー（Anton Piller）命令

申立人はまた、侵害者に対する訴訟において証拠を形成する書類その他の物件の調査、検査、除去又は写しを作成するために、侵害者の施設に立ち入るための捜索及び差押命令を裁判所に申請することができる。シンガポール裁判所規則（Singapore Rules of Court）の Order 29 は、裁判所に対して、事件の対象物であるいかなる財物についても、その留置、管理又は保全の命令の実施の目的で、事件の当事者の占有する不動産に立ち入ることをいかなる者に対しても許可することのできる権限を与えている。

被告が当該書類又は物品を隠匿、破棄又は処分することを防止するために、当該申請は、（侵害者に通知することなく）一方当事者のみの手続きで行われる。そのため、裁判所は、申立人による完全かつ率直な開示を要求し、そうでない場合には認められた命令は、取り消されることがある。申請者はまた、損害賠償・補償（当該命令の実行によって生じた損失を被告に補償するためのもの）に関する誓約を行わなければならない。

捜索差押命令を確保するためには、申請者は、次のことを裁判官に納得させなければならない。

- 事実に基づき、違反についての極めて強い（すなわち、侵害者に対する請求・申立てが正当化される可能性が高い）事例であること。
- 命令が出されない場合、請求する者に対する損害（実際のもの又は潜在的なもの）が非常に大きいこと。
- 侵害者が証拠を破棄する可能性があること。
- 捜索差押の効果が、その正当な目的に見合ったものであること。

この救済手段は、秘密情報が保管されていると疑われる施設に入り、文書、記録、コンピューターデバイス（個人用も含む）、その他秘密情報が保管されていると思われるあらゆる媒体を押収し、当該保管媒体

を調査・検査し、及び/又は侵害者が所持するすべての秘密情報のコピーを除去することができるという、その侵襲的性質から裁判所に認められることは稀である。

(iii)　キア・ティメット（Quia Timet）差止命令

侵害が発生していないが、そのおそれがある又は差し迫っている場合は、営業秘密の所有者は、その発生前に営業秘密の開示を防止するために、キア・ティメット（Quia Timet）差止命令を求める権利を有する[21]。

これは、被申立人による違反又は法律上の不正であって、そのおそれ又は差し迫った状況があり、かつ、それが回復することができない損害を請求人に与えるものである場合に、その実行を抑制するための差し止め命令である。

裁判所が当該差止命令を発する前に、請求人は、被申立人が請求人に回復不能の損害をもたらすような行為上の不正を犯す現実の危険があることを証明しなければならない。「回復不能の損害」とは、直ちに中間的差止命令を得ても回復することができず、かつ、請求人が損害賠償の判決を得ても十分に補償することができない損害をいう[22]。

(B)　恒久的救済

契約違反及び秘密侵害の訴えの根拠は、制定法には存在しない。例えば契約違反・秘密侵害の訴えがシンガポール高等裁判所に提起されたとする。裁判所は、最高裁判所法において付与されている権限を行使できるとされており、最高裁判所法の第一別紙には、裁判所の権限には、「法及び衡平法上の全ての救助及び救済を与えることが含まれ、これには、差止命令又は特定履行に加え、又はこれに代わるものとしての、損害賠償を認めることが含まれる」と規定されている。これが裁判による救済の根拠となっている。

契約違反・秘密保持違反の訴訟に基づいて利用可能な民事救済は、以

21　*CDL Hotels International Ltd v Pontiac Marina Pte Ltd* [1998] 1 SLR(R) 975 において、シンガポール控訴裁判所は、キア・ティメット（quia timet）の申し立てを、「認識されている不正を避けるために提起される措置」と説明している。

22　*Royal Insurance Co Ltd v Midland Insurance Co.* (1908) 26 RPC 95 at [97]。これは、*Millennium Pharmaceuticals, Inc. v Drug Houses of Australia Pte Ltd* [2018] SGHC 149 at [88]で支持された。

下の通りである

- 損害賠償（補償としての賠償と秘密侵害に対する衡平法上の損害賠償を含む。）又は不当利得（I-Admin[56]を参照。）。なお、シンガポール法においては、契約違反には懲罰的損害賠償の判決を与えることはできないとの一般原則がある。シンガポール控訴裁判所はこの点に関する可能性を完全に否定してはいないものの、その可能性は「確かに、きわめてまれであろう」としている（Turf Club Auto Emporium Pte Ltd v Yeo Boong Hua [2018] 2 SLR 655 at [198]を参照のこと）。よって、秘密保持義務違反の損害賠償は、損害賠償（補償としての賠償と衡平法上の損害賠償を含む）及び不当利得に限定されている。

- 恒久的差止命令（例えば、侵害者が営業秘密を使用、悪用、開示、複製、又は他の方法で取り扱うことを制限するもの）（I-Admin[56]を参照。）

- 営業秘密の引渡し又は廃棄を命ずる裁判所の命令（I-Admin[56]を参照。）
- 著作権侵害訴訟において、裁判所は、著作権者に対し、将来の侵害を制限する差止命令、損害賠償もしくは不当利得又は法定損害賠償、及び侵害物品の引渡し・処分命令を言い渡すことができる。

4.2 <u>刑事上の制裁手段</u>

BOC に基づく訴えの対象となる行為は、シンガポールの他の法律に基づく違法行為に該当し、別途、刑事責任を生じさせることもある。なお、シンガポールにおいて、この刑事訴追には時効が存在しない。

(A)　著作権法

- 著作権法（2021 年改正）第 444 条は、著作権が成立している著作物について、販売又は賃貸、商業的取引、商業的取引目的での輸入、又は商業的取引目的での保有を行うことは、当該物が著作物を侵害する複製物であることを知っていた（又は、知っているべき合理的理由があった）場合には、犯罪となると定めている。

- 著作権法（2021 年改正）第 445 条は、商業的な利益を得る目的で権利の侵害を故意に行った者は罰する旨を定めている。

第 444 条に違反の行為を行った場合、個人であれば、100,000 シンガポールドル又は侵害の対象となった著作物ごとに 10,000 シンガポールドルの、いずれか高い方の金額を上限とした罰金、5 年以下の懲役、又はその両方が科される。法人の場合は、200,000 シンガポールドル又は侵害の対象となった著作物ごとに 20,000 シンガポールドルの、いずれか高い方の金額を上限とした罰金が科される。

第 444 条違反の行為を行った場合、個人であれば、100,000 シンガポールドルを上限とした罰金、5 年以下の懲役、又はその両方が科される。法人の場合は、200,000 シンガポールドルを上限とした罰金が科される。

(B)　コンピュータ不正使用法

BOC の事案がコンピュータ内のデータ又はプログラムの不正なアクセス・改ざん（例えば、営業秘密を含む文書の電子的コピーの不正なダウンロード）を含む場合、これはシンガポールコンピュータ不正使用法(Cap. 50A)(「**CMA**」)に基づく違反も構成することがある。

CMA の違反は、その性質上、刑法犯である。被害者は、刑事告訴により、CMA 違反を警察に報告し、刑事訴追を求めることができる。CMC は、犯罪者、コンピュータ、プログラム又はデータが犯罪時にシンガポールに所在していた場合にのみ適用される。

CMA 第 3 条では、コンピュータに保存されているデータ又は又はプログラムへの不正アクセスを行う目的で、コンピュータ上で意図的に何らかの機能を実行させることが禁止されている。違法行為の成立のためには、当該資料が秘密の性質を有している必要はない。この不正アクセスには、従業員等が業務範囲外の目的のためにコンピュータファイルにアクセスする状況も含まれる。

第 3 条違反の罪で有罪となった者は、最初の違法行為については 5,000 シンガポールドル以下の罰金もしくは 2 年以下の懲役、2 回目及びその後の違法行為については 10,000 シンガポールドル以下の罰金、3 年以下の懲役、又はその両方が科せられる。不正アクセスの結果、損害が発生した場合には、非常に厳しい罰則が課される[23]。

---

[23] CMA 第 3 項(1)及び(2)。第 3 条の違反の結果として損害が生じた場合、違反者には 50,000 ドル以下の罰金もしくは 7 年以下の懲役が科され、又はこれらが併科さ

CMA 第 5 条では、コンピュータの内容の不正な変更を引き起こすと知っている行為を行うことが禁止されている。第 3 条に基づいて有罪となった者には、最初の違法行為については 10,000 シンガポールドル以下の罰金、3 年以下の懲役、又はその両方、2 回目及びその後の違法行為については 20,000 シンガポールドル以下の罰金、5 年以下の懲役、又はその両方が科せられる。不正アクセスの結果、損害が発生した場合には、非常に厳しい罰則が課される[24]。

さらに、CMA 第 13 条で、裁判所は、CMA に基づく犯罪で有罪判決を受けた者に対し、当該犯罪によりコンピュータ、プログラム又はデータに生じたいかなる損害についても、いかなる人物に対しても金銭的補償を行うよう命じることができる。当該補償金の支払命令は、当該命令に基づいて支払われた金額を超えて民事訴訟において損害賠償を請求する権利を妨げるものではない。原告は、そのような損害が発生した場合直ちに暫定的差止命令を得ても回復することができず、かつ、請求人が損害賠償の判決を得ても十分は補償を得られないことを証明する必要がある。

4.3 裁判外の紛争処理

当事者は、訴訟又は仲裁による訴訟手続の開始とは別に、調停等の裁判外の紛争解決手続による紛争の解決を検討することができる。

調停は、任意のプロセスである。調停の手続きでは、すべての関係当事者の同意に基づき、紛争当事者が紛争を友好的に内部で解決するのを助ける中立的な第三者の調停人が関与する。調停の内容は厳密に秘密性が保たれ、対立的な状況を避ける方法で行われる。調停は、多くの場合、当事者間の紛争を解決するのに時間と費用効率の良い解決方法であると考えられている[25]。

当事者は、内部的に又は第三者機関が管理する調停の手続きで調停を

れる。

24 CMA 第 5 条(1)及び(2)。第 3 条の違反の結果として損害が生じた場合、違反者には 50,000 ドル以下の罰金もしくは 7 年以下の懲役が科され、又はこれらが併科される。

25 2017 年 11 月 1 日、シンガポールにおいて調停法（the Mediation Act）が運用開始された。この法律では、調停手続きにおける多くの法的な観点について明確化及び成文化がなされた。この法律は、シンガポールにおいて一部または全部の手続きがなされる調停、及び、当事者がシンガポール方を適用することに同意した調停に適用される。

行うことについて合意することができる。シンガポールでは、シンガポール調停センター（「SMC」(Singapore Mediation Centre)）とシンガポール国際調停センター（「SIMC」(Singapore International Mediation Centre)）が主要な機関となっている。

特に、2020 年 9 月 12 日、SIMC と日本国際調停センター（「JIMC」）は、新型コロナウイルスのパンデミックの状況において、シンガポール・日本帯の企業を含むクロスボーダーのビジネス事業者に対し、商業上の紛争を解決するための経済的で、迅速かつ効果的なルートを提供するための共同プロトコル（「本プロトコル」）を運営するための覚書に署名した[26]。本プロトコルは、あらゆる種類の国境を越えた紛争が、迅速、経済的かつ効果的な調停手続を通じて解決されることを可能にすることを目的としている。本プロトコルは 2021 年 9 月 11 日まで有効であった。

本プロトコルの主な特徴は次のとおりである[27]。

- 調停は、JIMC 又は SIMC の何れかに、20,000 円又は 250 シンガポールドルのいずれか低い額を手数料として納付することにより、提出することができる。JIMC と SIMC は、調停を共同で管理する。
- 各事案は、経験豊富な 2 名の調停員（各機関が 1 名ずつ指名）によって解決される。
- 両当事者は、日本市場に適合した固定料金と割引料金という利益を享受できる。例えば、130 万シンガポールドル未満の紛争では、各当事者が支払うのは 6,500 シンガポールドルである[28]。
- 調停は、現在の渡航に関する制限を回避するために、オンラインで実施することができる。

---

26 http://simc.com.sg/v2/wp-content/uploads/2020/09/JIMC-SIMC-Joint-Protocol_FINAL-for-web.pdf でアクセスできる（2020 年 12 月 20 日時点）。

27 SIMC の、「JIMC - SIMC Joint COVID-19 Protocol」。https://simc.com.sg/jimc-simc-joint-covid-19-protocol/#:~:text=This%20is%20the%20first%20known,jurisdictional%20barriers%20to%20promote%20settlement でアクセスできる（2020 年 12 月 20 日時点）。

28 http://simc.com.sg/v2/wp-content/uploads/2020/09/JIMC-SIMC-Joint-Protocol_FINAL-for-web.pdf で入手可能な料金表を参照のこと。

- 和解の合意書は、シンガポールをはじめとした、調停に関するシンガポール条約の批准国において、当該条約に基づいて執行することができる。

4.4 まとめ

- 営業秘密の不正使用をされた場合、民事及び刑事上の責任追及手段が用意されている。
- 民事責任に関しては、中間的差止命令や捜索差押命令といった仮の救済手段と、営業秘密の使用又は開示に対する恒久的な差止などの恒久的な救済手段、損害賠償、秘密情報の引き渡し又は廃棄といった救済手段が用意されている。
- 侵害者は、事案に応じて、著作権法・コンピュータ不正使用法などの刑事責任も負う場合がある。

(5) 統計情報

2015 年から 2019 年までの刑事事件及び民事事件の訴訟件数や、シンガポールにおける法的事件に関する勝訴数、敗訴数といった、公的に利用可能な統計的な情報は、存在しない。かかる統計情報は一般的に裁判所からは公開されていない。

近年の、BOC の法理に関する最も影響力の大きな判決は、「I-Admin」事件である。その概要は、下記の第 1 部(6)に記載の通りである。

(6) 秘密の保護に関する法律の発展動向

6.1 BOC に関する伝統的なテストから離れ、「I-Admin」事件の判断要素へ

伝統的に、秘密保持義務違反の請求は、次の 3 つの要素が示されることに基づいていた。すなわち、(a)当該情報がその性質上秘密であること、(b)秘密といえる状況において提供されたこと、及び(c)その情報が許可なく、原告に損害を与える形で使用されたこと、である[29]。

しかし、デジタル化された社会を背景として、保護された情報（営業秘密を含む）の不正な複製、悪用、及び搾取を防止することは、今や

[29] *I-Admin* 事件の[43]。

著しく困難になっていることが認識されており、これに基づきシンガポール控訴裁判所は、最近、BOC クレームの判断基準を、上記の「I-Admin」事件で示された判断要素に変更した[30]。

I-Admin 事件において、原告である I-Admin (Singapore) Pte Ltd. (「I-Admin (SG)」)は、給与管理データ処理サービス及び人事情報システムの事業を行っていた。同社は I-Admin (Shanghai) Ltd.をはじめとする多くの 100%子会社を運営していた。この事件の第一被告及び第二被告は、I-Admin (SG)及び I-Admin (Shanghai) Ltd.の元従業員であった。彼らは、I-Admin からの退職後、シンガポールに Nice Payroll Pte Ltd.という会社を設立し、同様に給与アウトソーシングサービスや人事管理機能を提供していた。Nice Payroll Pte Ltd.はこの訴訟の第三被告となっている。原告は、被告らの活動についてフォレンジック調査を行い、Nice Payrol の施設において捜索及び差押えを行うための裁判所からの命令を得た。これらの調査を通じて、原告は、被告の機器・サーバーから原告の資料を多数回収し、被告が電子メールでこれらの資料の一部を配布していることを発見した。これらの資料には、I-Admin (SG)のソースコード、給与システム及び人事サービスをサポートするデータベース、事業開発及び顧客関連資料、並びにその運営に関連する資料が含まれていた。原告はそこで、被告らに対し、秘密保持義務違反等を主張する訴訟を開始した。

伝統的な判断基準からの主な違いは、原告に損害を与える形で被告が秘密情報を不正に使用したことを立証しなければならないという原告への要件を撤廃することである。原告が、I-Admin 要素の最初の 2 つを証明した場合、(コモンロー上の概念である)「自己の良心への影響がなかったこと」を示すという立証の責任は被告に移ることになる。

このような立証責任の転換は、違反の可能性は数年後になって初めて発見される場合もあり、このため原告となる可能性のある者が、立証の観点から委縮してしまうという、秘密情報の所有者が直面する実際的な困難に対処しようとするものである。対照的に、I-Admin 事件における BOC の新たなテストは、被告人は請求の対象となる不正行為についての責任という点で、はるかに適切な位置にあるとの認識に立って

30 *I-Admin* 事件の[3]。

いる[31]。

この BOC に基づく請求の法的枠組みの改正は、秘密情報を悪用した従業員に対峙する企業に対して、より大きな保護を与えることになる、歓迎すべき変更といえる。これは、企業が秘密情報の不正使用を立証する際の立証上の困難を解決するのに役立つといえる。今や、秘密情報にアクセスしたという行為それだけでも、請求を行うために十分なものとなっている。このことは、不正を行った社員が自分の痕跡を隠そうとするための措置を講じた場合に、特に役立つといえる。

6.2 衡平法上の損害賠償の利用可能性

さらに、I-Admin 事件の裁判所は、衡平法上の損害賠償が BOC の訴訟において利用可能な救済であることを明確にした。「衡平法上の損害賠償」とは、裁判所が損害賠償の額を査定するにあたって特定の根拠に限定されないという損害賠償である[32]。これにより、裁判所は、損害賠償額の算定においてより柔軟性を持つことができるようになる。裁判所は、特定の要素又は枠組みに限定されることなく、損害賠償額の算定に最も適切であると考える方法を決定する裁量を持つ。

例えば、I-Admin 事件では、2 名の元従業員が原告の秘密情報（ソフトウェアやビジネス資料など）を悪用し、これを使って競合する事業を立ち上げ、それによって、当該資料や情報を開発する時間と手間を節約したという事情があった。原告に与えられる衡平法上の損害賠償の額の決定にあたって、裁判所は、下記の検討がこれに関連すると述べた[33]。

- 被告が、もし原告の資料に接することなく当該ソフトウェア又は資料を作成しようとした場合に被告が出費したであろう追加費用
- 競業する事業を立ち上げ、それがより早く収益を上げられるようにできた時間の短縮

BOC に基づく案件において、衡平法上の損害賠償が利用可能になるというのは、それぞれの事件の状況において、最も適切かつ公正な救済

31 *I-Admin* 事件の[62]。
32 *I-Admin* 事件の[73]。
33 *I-Admin* 事件の[79]。

が原告に与えられることを確保できるという柔軟性を裁判所が持つようになるという意味において、大きな進展である。

6.3 まとめ

- I-Admin 事件についての控訴裁判所は、伝統的な BOC のテストを修正し、被告が秘密情報の不正な使用を行ったことを原告が立証しなければならない、という原告の義務を無くした。
- I-Admin 事件で示された 2 つの要素を原告が立証した場合、立証責任は被告に移り、自己の良心に影響がなかったことの立証を行わなければならなくなる。これは被告による使用の証拠を得ることが一般に原告にとっては難しいという立証の困難性に対応したものである。
- I-Admin 事件では、BOC に基づく請求において衡平法上の損害賠償が利用可能であることを明らかにした。これにより裁判所は、損害額の算定について、事案に応じて適切な決定を行う広い裁量を持つことになる。

III. 第 2 部：漏洩防止のための実務的な対策

(1) シンガポールにおける秘密情報管理の手順

営業秘密を管理するための 4 つの重要なステップは、次のとおりである

- 自社において保有・管理する営業秘密の特定（保護すべき情報の選択及びその重要性の分類）
- 営業秘密のカタログ又はリストの作成・維持（現行の管理システムの確認）
- 保護のための契約上、物理的、技術的な、組織上の措置の実施（情報管理のための具体的なシステム）
- 不正が起きた場合の対応計画の立案

以下、シンガポールに特有の問題に対応するために行うべき、営業秘密管理の実例・システムについて解説する。

(A) 営業秘密の特定

営業秘密には、アイデア、プロセス、製品作成、レシピ、方法論、計画、データ、ソフトウェアなど、膨大な情報が含まれる。営業秘密を特定することで、企業は営業秘密を完全に保護することで得られる価値を認識することができる。そのため、企業は、保護する価値のあるすべての営業秘密を特定するべきである。リスト又はインベントリが作成されれば、企業はその中から保護に値すると考えるものを選び、関連費用決定することができる。

まず、営業秘密を特定し、これに見合うレベルの保護を特定するために、以下の点を検討すべきである。

- これらの「秘密」は、関連する法の下で、営業秘密に該当するのか？
- この情報は、どの程度（企業の内外において）知られているのか？

(i) 秘密情報と従業員の経験・技能との境界を明確にすることは可能か？

(ii) 競業他社が情報を独自に情報を獲得するために利用しなければならないリソースはどの程度か？

(iii) 情報を完成させるのに要した努力（時間、人的資源、金銭的なリソース）はどのようなものであったか？

- 営業秘密としての管理は、正しいアプローチか（特許、著作権、意匠等などに比して）？
- 企業がアクセスできるものであって、かつ保護・維持する義務を負っている第三者の営業秘密は存在しているか？

(B) 営業秘密のカタログを作成し、維持する

次に、企業が保有する営業秘密の種類及びアクセス可能な第三者の営業秘密に関連する情報を記載したカタログを作成すべきである。これは以下の点を含める必要がある。

- 企業が保有する営業秘密の種類
- 企業がアクセス可能な、第三者の営業秘密
- 秘密情報が使用・保管される国と地域
- 営業秘密が自己の所有であるのか、またはライセンスされているか
- どの当事者がどの営業秘密にアクセスしているか
- 各営業秘密を保護するために実施されている措置
- 有効期限（又は失効する可能性のある期限）
- 営業秘密の分類（重要性により低、中、高レベルの区別）
- 各営業秘密について、定期的な見直し日の設定

このリストは、関連する営業秘密の所有権及び権益を確立し、証明するのに役立つもので、企業が保護を必要とする営業秘密につきさらに認識を持つのに役立つものとなる。

(C) 保護のための契約上、物理的、技術的な組織上の措置（情報管理のための具体的なシステム）を実施する。

次に、企業は、組織内での営業秘密の不必要な複製・共有を最小限に

抑えるために、リスク管理マニュアルと手続きを実施するべきである。これらの措置は、営業秘密の不正アクセス、使用、開示、喪失及び改ざんを防止し、従業員のための明確なマニュアル及びガイダンスを提供し、そして第三者の営業秘密に関して課された義務の違反を回避するのに役立つ。

このようなマニュアルやポリシーは、組織内、そしてパートナー企業のネットワーク内での協力と透明性を促進する必要性とのバランスをとる必要があると考えられる。

以下、組織的な保護措置として導入することが推奨される措置を記載する。

- 適切に設計され、実施されたポリシー及びマニュアル、並びに並びに秘密保持義務に関する、従業員に対する定期的な指導・教養等のトレーニング。
- 適切なソフトウェア等を使用した、企業内実務の頻繁なモニタリングにより、プロトコルとポリシーが遵守されていることの確認。
- 当該従業員がその情報を知る必要が本当にあるか、という観点からの秘密情報へのアクセス制限と、かかるアクセス制限の記録の保持。
- 物理的な障壁、鍵の掛かる仕組み、ペーパーシュレッダーの実施。
- パスワード、ファイアウォール、自動侵入検知システム、及び組織の特定の活動に合わせた認証手段を含む技術的な安全対策の実施。
- 労働契約内の規定など、営業秘密の保護を支援するために必要な雇用関係上の規定の実施。
- 退社時の面談で機密保持義務を理解し遵守していることの確認、及び、退社時に機密情報を保持していない旨の誓約書への署名をすること。
- 情報を秘密として保持することに関する、従業員への実践的な指導。たとえば、公共交通機関、エレベーター、トレードショ

ー、カンファレンスなどで企業の業務について話し合いをしないよう従業員に助言したり、公共の場所で仕事に関連する機器を使用する際には注意を払うよう助言したりすることが考えられる。

- 従業員が機密情報にアクセスする際に、営業秘密を第三者と共有することに関連して、秘密保持契約や機密保持契約など必要な契約条項を入れこみ、契約の締結に当たってフォローアップすること。
- 契約を定期的に見直し、常に従業員の役職に合ったものとし、適切な保護を提供することを確保すること。
- 企業の秘密情報に関連した、顕著な又は注目すべき開発行為について、並行して書面での記録を維持し、口頭で従業員に開示された情報についても記録を維持すること。
- 適切な場合、競業避止契約を使用すること。秘密保持契約は、主要な研究開発活動の従業員が不適切な使用又は開示を行うことを防止するには不十分である場合がある。それに対して競業避止契約は、営業秘密を使用又は開示する機会を最小限にするために、従業員のその後の活動に一定の線を引くことにより、より広範な保護を提供することができる。
- 秘密であることを示す通知の使用。文書資料に「機密」と表示すること（透かしや冒頭などに）等を検討する。これは、秘密情報を含む技術図面や文書を取り扱う際に特に重要である。
- 異なるレベルの機微性を有する情報に対し、異なる水準の保護措置を取ることを検討すること。
- 営業秘密とノウハウと個人情報保護に関するグループ全体のポリシーを展開すること。
- 現在の手順が適切であるかどうかを判断するために、セキュリティの手続きを頻繁に見直し、内部監査又は外部監査を実施すること。。
- 訴訟又は仲裁におけるディスクロージャー、ディスカバリー、又は文書作成の義務について、かかる紛争が生じた場合には、

適宜これを確認すること。

- 営業秘密に関する契約には、紛争解決に関する適切かつ効果的な条項を設けること。企業としては、秘密情報や営業秘密に関連した契約から生じる全ての紛争について仲裁で解決するという条項を設け、手続きを秘密にするのが望ましいであろう[34]。

また、新型コロナの蔓延により、リモートワーキングが必要となっているが、企業はその IT システムがそのような変更をサポートできるかを確認し、増大するサイバーセキュリティと個人情報についてのリスクに対応することが必要となっている。企業として、これらのリスクに対応するために導入するべき点について、以下、記載する。なお、附属書 E の、リモートワークにおけるチェックリストも参照のこと。

- **制限されたシステムへのアクセス**：つい最近までは、オンプレ環境でのみアクセス可能なシステムのみを有していた企業がほとんどであった。リモートワーキング環境への変化に伴い、多くの企業がリモートアクセスのためにシステムを解放したが、システムのインテグリティを保つためには、当該システムが適切に設定され、リモートアクセスのための追加の認証手続き（例えば、二要素認証）を導入することが必要である。

- **リモートワーキングのための IT リソース**：リモートワーキング実現のために従業員用の追加のデバイスを導入した場合、これらが最新のセキュリティソフトを備え、さらに必要なセキュリティパッチが適用されていることを確実にする必要がある。もし従業員に、リモートワークのために従業員の私的なデバイスを使用することを許可するのであれば、その使用についての明確なルールを作成し、特に、企業が保有する情報のダウンロード及び拡散について規定することが必要となる。

- **リモートでの接続**：リモートでの接続数の増大により、不正な目的での接

---

[34] シンガポール国際仲裁センターのモデル条項・サンプルにおける仲裁合意には、以下の記載がある。「本契約に起因または関連する紛争は、その存在、有効性または終了に関する疑義を含め、その時点で有効なシンガポール国際仲裁センター(「SIAC」)の仲裁規則(「SIAC 規則」)に基づきシンガポール国際仲裁センターが管理する仲裁に付され、仲裁により最終的に解決されるものとする。当該規則は、本条において言及することにより組み込まれるものとみなされる。仲裁地は、[●シンガポール]とする。仲裁裁判所は、[●]人の仲裁人で構成されるものとする。仲裁の言語は、[●]とする」。なお、[●]が付された部分の文言は、両当事者の合意に応じて、適宜括弧内に記入するものとする。この点の詳細については、https://www.siac.org.sg/model-clauses/siac-model-clause を参照のこと。

続が目立たなくなる危険性がある。もし従業員が安全ではない、又は汚染された接続手段をリモートワークに使用した場合（例えば、カフェでのインターネット接続など）はなおさらである。企業としては、このようなリスクへの体側、例えば安全な接続経路でのみアクセスを認めるなどの適切な対応を取ることが必要となる。

このような安全管理措置の信頼性維持のため、企業としては営業秘密管理のシステム又は監視のために、特定の部署又は責任者を置くべきである。

(D)　不正な流用などに対応するプランの立案

最後に、企業は、営業秘密の不正な流用に対処するための計画を策定すべきである。これは、避けられないセキュリティ侵害行為に備え、企業が修復不能な被害を被ることを防止し、営業秘密が急速に流布することを防止するために迅速に行動することを可能にするためである。対応の遅れは、前述の暫定的な差止命令及びその他の暫定的救済を得られるかという企業の能力に影響を与える可能性がある。

対応プランは、以下のような内容を備えるべきである。

- 違反の種類に応じた適切な措置を講じるために、違反をランク化し、又は分類する方法を定める。
- 違反が発生した場合、誰に通知すべきかを特定する（社内のアドバイザー（例えば経営層、社内弁護士、広報、HR、IT 部門など）及び社外のアドバイザー（外部弁護士、フォレンジック調査の専門家など）を含む)。
- 営業秘密（又はその中の一定の種類の営業秘密）へのアクセスを停止又は制限するための措置を設定する。
- 誰が、どのように違反の詳細を調査し、文書化するか、特定する。
- 違反に対する救済手段を求める措置を設定する。
- どの部署が、どの措置を講じる責任を負うかを特定する（理想的には、IT 担当者、取締役、弁護士、記録の管理責任者、及び必要に応じて広報スタッフが関与する分野横断的なアプローチをとる)。

- 個人情報保護法の下での要件に関する特別な考慮事項を含める。これらの制度は営業秘密や他の知的財産制度とは異なるためである。
- 不正流用に対する行動計画に基づく責任者に簡単にアクセスできるようにする。
- 不正流用に対する行動計画の効果的な実施を確実にするためのトレーニングプログラムを含め、演習訓練を実施する。
- 関連するすべての法律及び業務上の考慮要素に基づき、定期的に更新する。

(2) 秘密情報に関する契約書作成上の留意事項

秘密情報の保護に関する契約・契約条項を作成する際に留意すべきいくつかのポイントを以下に記載する。

2.1 <u>秘密保持条項</u>

秘密保持原則に基づいて保護される商業情報は、多くの形態をとりうる。ほとんどの種類の情報が、商業情報及び個人情報を含む秘密情報の対象となり得る。従って、コモンローの下では、秘密情報の網羅的なリストは存在しない。ある情報が秘密情報であるか、営業秘密であるかは、当該情報の性質及びその他の要素、例えば企業にとっての商業的な価値などによる。

秘密情報の例をいくつか挙げると、以下のとおりである。

- 最終製品においては分析することができない製法
- 最終製品からは明らかとならないレシピ
- プロセス（例えば、発酵技術など）
- ビジネス方法（公共の場で使用されるようになるまで）
- 財務情報
- 統計情報
- 顧客及びサプライヤーのリスト、連絡先情報及びデータ
- 設計、スケッチ及び図面

- 製品・工程の改善
- 特許出願中の新規発明
- 事業計画
- コンピュータプログラム
- 発見、科学的な理論又は数学的な方法

秘密保持契約には、常に以下のような重要な条項が含まれているべきである。これは、秘密保持契約、雇用契約、ライセンス契約、ディストリビューション契約、フランチャイズ契約、及び秘密又は機微な情報が交換される当事者間のその他の商業契約を含む、あらゆる種類の契約に適用される。

- **「秘密情報」の適切な定義**

  秘密情報として保護されるようにするためには、当該情報は必要な秘密性を有していなければならない。企業は、その事業の性質及び他者との取引を考慮して、企業が保護しようとする対象の秘密情報を考えなければならない。「秘密情報」の定義は、受領当事者に対する情報の意図的又は不注意による開示並びに秘密情報に由来する成果物をカバーするのに十分に広くなければならない。当然、受領当事者は、この定義を可能な限り狭く維持することを望むと考えられる。また、資料が真に秘密でなくなった場合（すなわち、必要な程度の秘密性を失った場合）、これに反する契約の文言があっても、その事実を変更することはできない。秘密情報の定義において、情報が保護されなくなる特定の状況を記述する明示的な言葉を含めることにより、これを確認することが通常である。（附属書 C の 1 条(f)及び 3 条を参照のこと。）

- **情報を秘密に保持するという中心的な義務と、許可された目的にのみ使用する義務**

  秘密保持の中心的な義務に加えて、開示当事者は、受領当事者が情報を使用できる目的を明確に規定すべきである。

- **開示当事者（A）が受領当事者（B）に対して、他の当事者への情報開示を許可する状況及びその相手方**

通常、当事者（B）による従業員及びアドバイザーへの営業秘密の開示は許される。当事者（A）は、秘密情報を受領する当事者（B）のすべての従業員及びアドバイザーに対し、別途、秘密保持契約に署名するよう要求することができる。この方法は、一般的には、煩雑であると見られることもある。一方で当事者（B）がその従業員又はアドバイザーによる秘密保持違反に対して責任を負う方法としては合理的であるといえる。適用される法律や規制の下で必要とされる当事者（B）による開示は、常に許可されるべきである。

- **ディール、プロジェクト、取引が実現しない場合、又は終了に至った場合、情報と記録はどうなるか**

  開示当事者は、プロジェクト又は取引が進行しない場合の、又は場合によっては要求に応じての、秘密情報の返却又は破棄について規定すべきである。ただし、受領当事者は、秘密情報を含む一定の記録を維持することを法律上要求されることがある（取締役会議事録など）。

- **契約の存続期間**

  秘密情報は、その秘密性を保持する限り、秘密情報として保護することができ、理論的には無期限に保護することができる。しかし実際には、例えば以下のような、多くの制約がある。

  (i) 情報は、時代遅れになり、商業的価値を失うことによって、真の秘密性を失うことがある。動きの激しい業界では、このことは、秘密が比較的短期間しか価値を持たないことを意味するかもしれない。

  (ii) 秘密保持契約又は非開示契約は、通常、期限が限定されている。

  (iii) 元従業員の場合、守秘義務は、元従業員の契約における制限条項と同様の期間は当然に継続すると見なされるであろうが、その義務を退職後にも強制することには困難があるかもしれない。

  技術情報は、ほとんど無期限に商業的価値を維持することができるが、ビジネス上の情報は、短期間しか価値を維持できない

場合がある。従って、両当事者は、保護される情報の種類に関連して、契約の期間について現実的な期間を設定すべきである。

2.2 競業避止条項及び勧誘禁止条項

秘密情報、特に営業秘密の保護は、取引制限に関する条項を正当化することができる理由として認められている。営業秘密の保護には、主に 2 つの方法がある。

- 契約上の秘密保持契約（独立した契約としての秘密保持契約又は非開示契約（NDA）であるか、又は商業的な契約の中に含まれる秘密保持条項又は非開示条項であるかは問われない）
- 制限条項

秘密保持契約（又は NDA）、又は契約条項には、非勧誘条項、開示当事者の従業員又は顧客を勧誘することを一方の当事者に制限する条項、又は競業避止条項（一方の当事者が企業を退職した後に競合他社に関与する、又は利害関係を持つ、勤務する、又は他の方法で取引することを制限する。）などの制限条項が含まれる場合がある。ただし、そのような制限条項が有効となるためには、以下の原則が適用される。

シンガポールでは、当該条項を強制しようとする当事者が以下のことを証明できない限り、制限条項は強制不能であるというのが原則的な立場である。

- 当該条項は、強制しようとする当事者の正当な利益を保護するものであること。使用者が制限条項を通じて保護しようとする正当な利益は、一般に、(i)営業秘密又は営業秘密に類似する秘密情報[35]、(ii)顧客、顧客又はサプライヤーのような取引関係を保護するという利益[36]、及び(iii)安定した熟練の労働力を維持す

35 雇用契約にすでに営業秘密または秘密情報を保護する明示的な秘密保持条項が含まれている場合、たとえ従業員であった者が雇用の過程で営業秘密または機密情報にアクセスしていたとしても、このことは制限条項を正当化するものではない。*Lee Gwee Noi*, [66] を参照のこと。

36 十分な正当事由として取引関係に依拠するためには、会社は、従業員がその顧客について、事業を指揮する場所において現実に影響を及ぼし、または将来影響を及ぼす可能性のある、個人的知識および影響力を有していたことを証明しなければならない。

るという利益[37]、の 3 つである

- 制限は、当事者の利益のために合理的であり、かつ、公共の利益のために合理的であること[38]。

したがって、企業は、雇用契約において、企業における特定の従業員の役割及び影響力、秘密情報及び営業秘密へのアクセスに照らして絞り込まれ、かつ企業の正当な利益を保護するために必要な範囲でのみ従業員を制限するような方法で、制限条項を作成するよう、注意すべきである。

2.3 分離条項

シンガポールの裁判所では、分離の原則は、限られた状況において、また制限条項を有効にするために制限条項の一部を削除しても当該条項に文法上の問題が生じない場合にのみ適用される。シンガポールの裁判所は、両当事者の合意した条項を書き直すようなことはしない。しかし制限条項の中の、違反部分の分離に関するこの条項は、抑止効果のために、依然として契約に残してもよいだろう。

2.4 準拠法及び裁判管轄条項

秘密保持契約に準拠法及び管轄条項が含まれる場合、その秘密保持契約にどの準拠法及び管轄が適用されるかについて、シンガポール法は規定していない。両当事者は、準拠法及び裁判管轄について合意することができる。

準拠法及び裁判合意管轄条項がない場合、当事者は、抵触法の原則に従って、当該契約に適用される準拠法及び合意裁判管轄権を主張しなければならない。

第 I 部(2)に記載の「秘密情報に関する契約書作成上の留意事項」は、シンガポール法が該当の契約に適用されることを前提としていることに留意されたい。

(3) 漏えい事案への対応

詳細については、上記第 1 部の(4)（「救済手段」）及び第 2 部の

---

37 *Man Financial (S) Pte Ltd v Wong Bark Chuan David* [2008] 1 SLR(R) 663, [94].

38 *Lek Gwee Noi v Humming Flowers & Gifts Pte Ltd* [2014] 3 SLR 27 ("*Lek Gwee Noi*"), [34].

(1)(1)(D) （「不正な流用などに対応するプランの立案」）を参照のこと。

セキュリティリスク又は事案を特定し、適時に対応するためには、下記の点を含んだ対応計画を策定しておく必要がある。各項目について、企業が対応できているか、チェックする必要がある。

項目	**チェックリスト**
システム上の動きが常にモニタリングされており、疑わしいリスク、危険又は事案の発生があった場合、各所に通知されるプロセスができている。	
事案の発生が通知された場合、それが真に危険性のある事象であるかを調査し判断する内部のプロセスが導入されている	
調査の内容及び結果が書面化されるプロセスが導入されている	
不正な使用又は漏えい（不正アクセス又は不正なダウンロード）についての証拠を、企業の記録から保存するプロセスが導入されている	
必要な場合、外部専門家（外部の弁護士、コンピュータのフォレンジック調査のチーム）への相談を行うことができる	
内部への必要な連絡（ディスカバリー制度に対応したリティゲーションホールドの通知、経営層への報告など）がなされるようになっている	
当局（個人情報保護又はサイバーセキュリティ関連の当局）への開示が必要であるかを判断するプロセスがある	

各事案により、適切な救済手段（例えば、刑事及び民事手続き、裁判によらない紛争解決手続きなど）を判断できる（詳細については、上記第 I 部(4)を参照。）	

II3.2III(1)0

(4) 参考資料:関連文書等のフォーマット例

以下の文書のためのいくつかのサンプル条項を本書の附属書として添付する。

- 附属書 A：企業のポリシーにおける秘密保持条項の例
- 附属書 B：雇用契約における競業避止条項の例
- 附属書 C：取引先との間の秘密保持契約書における秘密保持条項の例
- 附属書 D：企業内施設への訪問者に対する秘密保持義務の通知の例
- 附属書 E：リモートワークのためのサイバーセキュリティとデータ保護チェックリスト

これらのサンプル条項は、シンガポール法が該当の契約に適用されることを前提として作成されていることに注意されたい。これらの条項は、例示的な目的のみを目的としており、関連する文脈、従業員、秘密情報の種類及びシナリオに合わせて変更することなく無差別に使用されてはならない。

附属書 A

企業のポリシーにおける秘密保持条項の例

注:これは、企業のポリシーにおける秘密保持条項の例です。必要に応じて変更した上でご使用ください。

1. As part of our workforce, you have a duty to keep our Company's assets confidential, protect them from unauthorised use or loss, and to use them only for legitimate business purposes. Disclosure of our confidential information can cause our Company substantial damage.

2. Some examples of confidential information include:

   (a) Non-public research, technical data, trade secrets, and other non-public intellectual property;

   (b) Non-public products, business or marketing plans;

   (c) Proprietary software code, formulas, drawings, designs, recipes;

   (d) Non-public financial and forecasted information relating to shipment, revenue, margin, product and costs;

   (e) Information relating to customer sales, customer contacts and customer behaviour and other confidential customer information;

   (f) Information relating to supplier metrics, contacts, data and other confidential supplier information; and

   (g) Employee information such as salaries and organisational charts.

3. Every employee should take appropriate measures to protect the Company's confidential information in the following ways:

   (a) Store all confidential information in a way that is not seen or accessible by persons who do not need access to that information;

   (b) When you are away from your desk, lock documents that contain confidential information in a cabinet or drawer. If reviewing soft copies of documents that contain confidential information, lock your electronic devices;

   (c) Carefully review and comply with our company policies regarding

confidential information;

(d) Consider your audience whenever communicating anything within the Company or to external parties. In particular, double check messages, attachments and recipients prior to sending them to prevent unintentional dissemination of confidential information; and

(e) Hold all confidential and/or proprietary information in strictest confidence at all times during your employment and thereafter.

(f) [●If applicable] Before sharing any confidential information with an outside party, in writing or orally, ensure an appropriate Non-Disclosure Agreement ("NDA"), approved by the Company, is in place.

4. Third Party Confidential Information. Treat the confidential information of third parties in accordance with the law, contractual agreements with such third parties, and the highest business standards. If you obtain third party confidential information pursuant to an NDA, be sure to comply with the terms of that NDA.

5. Customer Confidential Information. Information that belongs to our customers which is not intended for public distribution is generally considered customer confidential information. This information may or may not have been disclosed under an NDA. In addition, our customers' contracts may specifically preclude us from mentioning that they are our customers. You must follow the confidentiality requirements specified by our customers.

6. Competitor Confidential Information. Be very careful when you are having conversations with people who work for competitors, to avoid receiving any confidential information from them. Obtain any information regarding our competitors legally and ethically.

7. Unauthorised use or disclosure of another party's confidential information or trade secrets may result in civil and criminal consequences. Please approach the [●Human Resources Team] if you have any questions regarding the above.

＜参考和訳＞

1. 当社の従業員の一員として、貴殿は、当社の資産を秘密に保持し、それらを不正使用又は喪失から保護し、それらを正当な事業目的のためにのみ使用する義務を負います。当社の秘密情報を開示することは、当社に重大な損害を与える可能性があります。

2. 秘密情報の例としては、以下のものがあります。

   (a) 非公開の研究、技術データ、営業秘密、その他の非公開の知的財産

   (b) 非公開の製品、業務又はマーケティング計画

   (c) 独自のソフトウェアコード、製法、図面、デザイン、レシピ

   (d) 出荷、収益、マージン、製品及びコストに関する非公開の財務情報及び予測情報

   (e) 顧客への販売、顧客との連絡先、顧客の行動、その他の顧客の秘密情報に関連した情報

   (f) サプライヤーの指標、連絡先、データ及びその他のサプライヤーの秘密情報に関連下情報

   (g) 給与や組織図などの従業員情報

3. すべての従業員は、当社の秘密情報を保護するための、以下のような適切な措置を講じなければなりません。

   (a) すべての秘密情報を、当該情報にアクセスする必要のない者が閲覧又はアクセスできない方法で保管すること。

   (b) デスクから離れる場合は、秘密情報を含む文書をキャビネット又は引き出しに施錠すること。秘密情報を含む文書のソフトコピーをレビューする場合は、電子デバイスをロックすること。

   (c) 秘密情報に関する当社のポリシーを慎重に検討し、遵守すること。

   (d) 企業内部、又は外部と何らかのコミュニケーションをする場合は常に、聞く相手を考えること。特に、メッセージや添付文書、及び受領者を送信前にダブルチェックし、意図しない秘密情報の流布を防止すること。

(e) 全ての秘密情報・専有情報を、在職中及びその後も常に、厳格に秘密として保持すること。

(f) [●該当する場合]秘密情報を外部当事者と文書又は口頭で共有する前に、当社が承認した適切な秘密保持契約書(「**NDA**」)が締結されていることを確認すること。

4. **第三者の秘密情報。**第三者の秘密情報については、法令、第三者との契約のほか、最高レベルの業界標準に従い取り扱うこと。貴殿が秘密保持契約に基づいて第三者の秘密情報を取得する場合、当該秘密保持契約の条件を必ず順守すること。

5. **顧客の秘密情報。**当社の顧客に属する情報であって、公表を目的としないものは、一般に顧客の秘密情報とみなされます。当該情報は、秘密保持契約に基づいて開示される場合も、基づかない場合もあります。さらに、当社の顧客の契約は、当社が顧客であることを言及することを特に禁止している場合があります。貴殿は、当社の顧客が指定する秘密保持の要件に従わなければなりません。

6. **競業他社の秘密情報。**競合他社のために働いている人と会話をするときは、秘密情報を受け取らないように十分注意してください。競合他社に関する情報は、適法に、また倫理に沿って入手してください。

7. 相手方当事者の秘密情報又は営業秘密を不正に使用又は開示すると、民事上及び刑事上の結果を招くことがあります。上記についてご不明な点がある場合は、[●人事チーム]まで問い合わせてください。

附属書 B

雇用契約における競業避止条項の例

注:これは、雇用契約における競業避止条項の例です。必要に応じて変更した上でご使用ください。

1. The Singapore High Court case of Tan Kok Yong Steve v Itochu Singapore Pte Ltd [2018] SGHC 85 provides a useful example of an enforceable non-compete clause. There, the Court upheld a non-compete clause that extended to Vietnam and Philippines for a period of 2 years. This was the first decision in over a decade that the Singapore Courts enforced a 2-year non-compete clause. Please note that the Court found that the activity scope, geographical scope and the temporal scope of the restraint of trade clause was reasonable between parties and not against the public interest, given the ex-employee in question's role and activities at the ex-employer and the restraints in question.

2. The non-competition clause in that case stated:

> "The Employee hereby agrees and undertakes that during the Employment and for a period of 2 years (Two Years) after termination of the Employment, the Employee will not, without the Employer's prior written consent, directly or indirectly, whether for the Employee's own account or for the account of any other party, be employed or engaged in any capacity or otherwise be interested in or involved with any company or business which competes with the Employer and/or any Affiliate in respect of Restricted Goods or Restricted Services within the Restricted Area.
>
> …
>
> "Restricted Area"
>
> means the area (geographical or otherwise) constituting the market of the Employer and that of any Affiliate for the Restricted Goods and Restricted Services;
>
> "Restricted Goods"
>
> means any product competitive with any product sold or supplied by the Employer and/or any Affiliate with which the Employee

was concerned during the period of 12 months immediately preceding the date of termination of the Employment;

"Restricted Services"

means any services competitive with any of the services sold or supplied by the Employer and/or any Affiliate with which the Employee was concerned during the period of 12 months immediately preceding the date of termination of the Employment."

＜参考和訳＞

1. シンガポール高等裁判所の事件 ***Tan Kok Yong Steve v Itochu Singapore Pte Ltd*** [2018] SGHC 85 は、強制可能な競業避止条項の有用な例を提供している。この事件で裁判所は、ベトナムとフィリピンにまたがり、2 年間という期間の競業避止条項につき、これを有効とした。これは、シンガポールの裁判所が、最近 10 年以上の期間で初めて、2 年間の競業避止条項を強制力があるとした判決である。裁判所は、当該元従業員の役割、前雇用者での活動、及び該当の制限を考慮すると、取引制限条項における活動の範囲、地理的範囲及び時間的範囲は、当事者間において合理的であり、公益に反するものではないと判断した。

2. その事案における競業避止条項は、以下のように規定していた。

「従業員は、ここに、本雇用期間中及び本雇用の終了後 2 年間、雇用主の事前の書面による同意なしに、直接にも間接にも、従業員自身の計算によるか他者の計算によるかを問わず、制限地域内において、制限商品又は制限サービスに関して雇用主又は関連会社と競合する企業又は事業に雇用され、いかなる立場としても契約し、又はその他利害関係を有したり、関与しないことに同意し、約束する。

...

「制限区域」

とは、雇用者及び関連会社の制限商品及び制限サービスの市場を構成するエリア(地理的又はその他)を意味する。

「制限商品」

とは、雇用の終了日の直前 12 ヶ月間に従業員が関係していた雇用主及び/又は関係会社が販売又は供給した製品と競合する製品を意味する。

「制限サービス」

とは、雇用の終了日の直前 12 ヶ月間に従業員が関係していた雇用主及び/又は関連会社が販売又は供給したサービスと競合するサービスを意味する。

附属書 C

ビジネスパートナーとの秘密保持契約における秘密保持条項の例

*注:これは、秘密情報を開示する当事者(「**開示当事者**」)とそれを受領する当事者(「**受領者**」)との間で締結される NDA の秘密保持条項のサンプルです。必要に応じて変更した上でご使用ください。*

1. "Confidential Information" means all confidential information relating to the [state the purpose for which the agreement is entered into, e.g. the evaluation or establishment of a collaboration in respect of a particular project] (the "Purpose") which the Disclosing Party directly or indirectly discloses to the Recipient [before, on or after the date of this agreement]. This includes:

   (a) The fact that discussions and negotiations are taking place concerning the Purpose and the status of those discussions and negotiations;

   (b) The existence and terms of this agreement;

   (c) All confidential or proprietary information relating to:

      (i) The business, affairs, customers, clients, suppliers, plans, intentions, or market opportunities of the Disclosing Party; and

      (ii) The operations, processes, product information, know-how, technical information, designs, trade secrets or software of the Disclosing Party;

   (d) Any information, findings, data or analysis derived from Confidential Information; [and]

   (e) Any other information that is identified as being of a confidential or proprietary nature;

   (f) But excludes any information that:

      (i) Is, or becomes, generally available to the public other than as a direct or indirect result of the information being disclosed by the Recipient in breach of this agreement [(except that any compilation of otherwise public

information in a form not publicly known shall still be treated as Confidential Information)];

(ii) Was available to the Recipient on a non-confidential basis prior to disclosure by the Disclosing Party;

(iii) Was, is, or becomes available to the Recipient on a non-confidential basis from a person who, to the Recipient's knowledge, is not under any confidentiality obligation in respect of that information;

(iv) Was lawfully in the possession of the Recipient before the information was disclosed by the Disclosing Party;

(v) Is developed by or for the Recipient independently of the information disclosed by the Disclosing Party;

(vi) The parties agree in writing that the information is not confidential.

2. Confidentiality Obligations. The Recipient will keep secret and retain in strictest confidence, and will not, without the prior written consent of the Disclosing Party, furnish, make available, or disclose the Confidential Information to any third party. Unless otherwise provided in this agreement, the Recipient shall not make use of the Confidential Information for its own commercial uses or for the benefit of any third party, and shall use the Confidential Information only for the purposes for which this agreement is entered into.

3. Confidentiality Period. This agreement and the Recipient's duty to hold Confidential Information in confidence shall survive until [●date].

4. Standard of Care. The Recipient shall protect the Confidential Information received hereunder from disclosure to any unauthorised person, firm, corporation or other third party by using the same degree of care that it uses to prevent the unauthorised disclosure of its own confidential information of a like nature, but in no event less than a reasonable degree of care.

5. Return or Destruction of Confidential Information. If so requested by the Disclosing Party at any time by notice in writing to the Recipient, the Recipient shall:

(g) Destroy [or return to the Disclosing Party] all documents and materials [(and any copies)] containing, reflecting, incorporating or based on the Disclosing Party's Confidential Information;

(h) Erase all the Disclosing Party's Confidential Information from its computer and communications systems and devices used by it, or which is stored in electronic form; [and]

(i) [To the extent technically and legally practicable,] erase all the Disclosing Party's Confidential Information which is stored in electronic form on systems and data storage services provided by third parties; and

(j) Certify in writing to the Disclosing Party that it has complied with the requirements of this Clause.

Nothing in this Clause hall require the Recipient to return or destroy any documents and materials containing or based on the Disclosing Party's Confidential Information that the Recipient is required to retain by applicable law, or to satisfy the requirements of a regulatory authority or body of competent jurisdiction or the rules of any listing authority or stock exchange, to which it is subject. The provisions of this agreement shall continue to apply to any documents and materials retained by the Recipient pursuant to this Clause.

6. Equitable Remedies. The Recipient acknowledges and agrees that in the event of any actual or threatened breach by the Recipient of this agreement, the Disclosing Party will be entitled to seek immediate injunctive and other equitable relief, without bond and without the necessity of showing actual monetary damages. Nothing herein will be construed as prohibiting the Disclosing Party from pursuing any other remedies available to it, including the recovery of any damages that it is able to prove.

＜参考和訳＞

1. 「**秘密情報**」とは、[本契約締結の目的、例えば、特定のプロジェクトに関する共同研究の評価又は設立、などを記載]（「**本目的**」）に関連するすべての秘密情報を意味し、開示当事者は、[本契約締結日の前、又は締結日以後]に直接又は間接にこれを受領者に開示する。これには、以下を含む。

- 本目的について協議及び交渉が行われている事実、及びその協議及び交渉の状況
- この契約の存在、及びその条項
- 以下に関連するすべての秘密又は専有情報

  (i) 開示当事者の事業、業務、顧客、クライアント、サプライヤー、計画、意図又は市場機会

  (ii) 開示当事者の業務、プロセス、製品情報、ノウハウ、技術情報、デザイン、営業秘密又はソフトウェア
- 秘密情報に由来する情報、知見、データ又は分析
- その他、機密性又は専有性を有すると特定される情報
- ただし、以下の情報は含まない。

  (i) 本契約に違反して受領者により情報開示されたことの直接又は間接の結果としてではなくして、一般に公知であり、又は公知となった情報。[（公知ではない形式のその他の公開情報の編集物は、依然として秘密情報として取り扱われる。）]

  (ii) 開示当事者による開示前に受領者が秘密とならない方法で入手可能であったもの。

  (iii) 受領者が知る限り、当該情報に関して秘密保持義務を負わない者から秘密とならない方法で受領者が入手した、又は入手可能となった情報。

  (iv) 開示当事者が情報を開示する前に、合法的に受領者が保有していたもの。

  (v) 開示当事者により開示された情報とは独立して、受領者により、又は受領者のために開発されたもの。

  (vi) 両当事者が、当該情報が秘密ではないと書面で同意したもの。

2. **秘密保持義務。**受領者は、秘密性を保持し、厳重に秘密として保管するものとし、開示者の事前の書面による同意なしに、秘密情報を第三

者に提供、提供又は開示しないものとする。本契約に別段の定めがない限り、受領者は、秘密情報を自己の商業的使用又は第三者の利益のために使用しないものとし、秘密情報を本契約が締結された目的にのみ使用するものとする。

3. **秘密保持期間。**本契約及び受領者による秘密情報を秘密に保持する義務は、[●日付]まで存続するものとする。

4. **保護措置の基準。**受領者は、本契約に基づき受領した秘密情報を、同様の性質の自己の秘密情報の無断開示を防止するために使用するのと同程度の注意をもって、ただしいかなる場合にも合理的な程度を下回らない注意をもって、権限のない人物、事務所、法人又はその他の第三者への開示から保護する。

5. **秘密情報の返却又は破棄。**開示当事者が受領者に書面で通知要求する場合はいつでも、受領者は、下記事項を行うものとする:

   - 開示当事者の秘密情報を含み、反映し、組み込まれ、又はそれに基づいているすべての文書及び資料[（及びコピー）]を破棄する[又は開示者に返却する]。
   - 開示当事者のすべての秘密情報を、開示当事者が使用するコンピュータ及び通信システム及び機器、又は電子形式で保管される機器から消去すること。
   - [技術的及び法的に実行可能な範囲において、]第三者が提供するシステム及びデータ保管サービスに電子形式で保存されているすべての開示当事者の秘密情報を消去すること。
   - 本項の要件を遵守したことを書面で開示当事者に証明すること。

   本項のいかなる規定も、受領者が適用法により、又は管轄権を有する規制当局もしくは組織の要件、又は対象となる上場機関もしくは証券取引所の規則の要件を満たすために保持することを要求される、開示当事者の秘密情報を含む又はそれに基づく文書及び資料の返却又は破棄を受領者に要求するものではない。本契約の規定は、本項に基づき受領者が保管する文書及び資料に引き続き適用されるものとする。

6. **衡平法上の救済。**受領者は、本契約の受領者による実際の違反又は違反のおそれがある場合、開示当事者が、保証金なしにまた実際の金銭

的損害賠償を示す必要なしに、即時の差止命令及びその他の衡平法上の救済を求める権利を有することを確認し、これに同意する。本契約のいかなる規定も、開示当事者が、開示当事者が証明することのできる損害賠償の支払いを含め、開示当事者が利用可能なその他の救済手段を求めることを禁じるものと解釈されないものとする。

附属書 D

企業内施設への訪問者に対する秘密保持義務の通知の例

注:これは、「訪問者受付」における秘密保持義務の通知であって、公共の場所/公共の待合場所/公共の会議室の入口に目立つように表示されるものの例です。必要に応じて変更した上でご使用ください。

[●Company name] (the "**Company**")

All visitors to the Company's premises understand that they may be given access to confidential information belonging to the Company through their relationship with the Company or as a result of their access to the Company's premises.

All visitors understand and acknowledge that the Company's confidential information and trade secrets consist of information and materials that are proprietary, valuable and not available in the public domain.

All visitors agree to hold in strictest confidence and confidential information and/or trade secrets that they may obtain access to or receive in the course of or by virtue of their access to the Company's premises. The removal of any document (including soft copies), equipment, or other materials from the Company's premises without the Company's authorisation, and/or unauthorised access to the Company's proprietary information and materials, may result in civil and criminal penalties.

＜参考和訳＞

[●会社名](「当社」)

当社の施設へのすべての訪問者は、当社との関係に基づき、又は当社の施設へのアクセスの結果として、当社に帰属する秘密情報へのアクセスを許可されることがあることを理解するものとします。

すべての訪問者は、当社の秘密情報及び営業秘密が、専有性があり、価値があり、公知では入手できない情報及び資料で構成されていることを理解し、認識するものとします。

すべての訪問者は、当社の施設へのアクセスの過程で、又はそのせいでアクセスし、又は取得することがある秘密情報及び/又は営業秘密を、最も厳格に

秘密として保持することに同意するものとします。当社の許可なしに、文書（ソフトコピーを含む)、機器又はその他の資料を当社の施設から持ち出すこと、及び/又は企業の専有情報及び資料への権限のないアクセスは、民事的な罰則及び刑事的な罰則を科されることがあります。

附属書 E

リモートワークのためのサイバーセキュリティとデータ保護チェックリスト

注:上記の第２部(1)(1)(C)の実務ガイドラインに加えて、新型コロナウイルスのパンデミックによるリモートワークの普及に伴い、企業が検討すべきリモートワークのためのサイバーセキュリティ及びデータ保護チェックリストを以下に示します III(1)(1)(C)[39]。

Cybersecurity and Data Protection Checklist for Teleworking

Item	Completed?
Do we have two-factor authentication in place for remote access?	
Are restricted systems capable of being accessed remotely and appropriately configured?	
Are restricted systems subject to additional layer of authentication or security for remote access?	
Are all remote workers utilizing organization-owned devices for remote access?	
Are those devices fully updated with security software and patches?	
Are remote workers utilising personally-owned devices for remote access?	
Are those devices subject to appropriate security controls?	
Have we prepared our network and workforce for how to address the increased risk in cyber attacks in the remote working context?	
Have we issued appropriate privacy notices and/or obtained suitable consents for our planned monitoring activities?	
Do we need to address privacy terms with any vendors or other third parties that may access the data from our devices?	
Do we need to address any cross-border transfer restrictions that may apply to our workforce's remote access to systems?	

[39] 詳しくは https://www.bakermckenzie.com/en/insight/publications/2020/03/covid19-cybersecurity-privacy-risks-teleworking をご覧ください。

Do we need to carry out a data protection impact assessment on the proposed data collection and processing activities?	

＜参考和訳＞

リモートワークのための、サイバーセキュリティ及びデータ保護チェックリスト

項目	**完了の有無**
リモートアクセスのための二要素認証が導入されているか？	
リモートアクセスが可能となっている制限つきシステムに、適切な設定がなされているか？	
制限つきシステムには、リモートアクセスのための追加的な認証又はセキュリティが導入されているか？	
リモートアクセスをする従業員は、リモートアクセスのために会社所有のデバイスを利用しているか？	
それらのデバイスは、セキュリティソフト及びパッチが完全にアップデートされているか？	
リモートアクセスをする従業員は、リモートアクセスのために個人所有のデバイスを利用しているか？	
それらのデバイスに対して、適切にセキュリティの管理がなされているか？	
リモートワーキングに伴うサイバーアタックのリスクの増大にどのようにネットワーク及び従業員が対応するか、準備できているか？	
従業員のモニタリングについて、適切なプライバシー通知を出し、十分な同意を得ているか？	
会社のデバイスからデータにアクセスする可能性のあるベンダー及びその他の第三者との間でプライバシーに関する条件について対処する必要はあるか？	
従業員のシステムへのリモートアクセスに当たって適用のある、データの域外移転の制限に対応する必要があるか？	
予定されているデータの収集及び処理の手続きに当たって、データ保護のための影響評価を行う必要はあるか？	

経済産業省委託事業

シンガポールにおける営業秘密管理マニュアル作成

2022 年 3 月
禁無断転載

[調査受託]
Baker & McKenzie. Wong & Leow
独立行政法人　日本貿易振興機構
シンガポール事務所
(知的財産部)

本冊子は、2021年度に日本貿易振興機構シンガポール事務所知的財産部が調査委託を行ったBaker & McKenzie. Wong & Leowが作成した調査報告等に基づくものであり、その後の法改正等によって記載内容の情報は変わる場合があります。また、記載された内容には正確を期しているものの、完全に正確なものであると保証するものではございません。