米国，欧州および中国における営業秘密漏えいに関する法制と対応

Morgan, Lewis & Bockius LLP　東京代表パートナー，外国法事務弁護士。ジョージタウン大学（J.D.）卒業。各種業界におけるM&A，商取引全般，知的財産権のライセンスおよび国際紛争解決を主に取り扱う。

荒木源徳
Araki Motonori

Morgan, Lewis & Bockius LLP　アソシエイト，弁護士，ニューヨーク州弁護士。コロンビア大学（LL.M.）卒業。M&A，紛争解決，商取引，ライセンス，コーポレート・ガバナンスおよびコンプライアンスを含む会社法全般を主に取り扱う。

佐藤菜緒
Sato Nao

近時，日本企業の営業秘密が中国の再委託先から不正に持ち出されたことや，欧米子会社で第三者から不正アクセスを受けたことに関する報道が増えている。企業活動のグローバル化の加速に伴い，日本企業の営業秘密の保護は日本国内のみでは十分ではなくなっており，進出先の各国における法制・実務をふまえた保護，さらには漏えいへの対応が求められている。本稿では，特に進出企業の多い米国，欧州（EU）および中国について，営業秘密の保護に関する法制度，漏えい防止対策，実際に漏えいがあった場合の措置について考える。[1]

Ⅰ　米　国

1　米国における営業秘密の保護法制

⑴　統一営業秘密法（Uniform Trade Secrets Act：以下「UTSA」という）

同法は，全米で統一的な営業秘密の保護を図るために1979年に制定されたモデル法であり，各州が営業秘密法を制定するにあたり，ひな形として用いられた。2021年９月現在，ニューヨーク州を除くすべての州において導入されている。ニューヨーク州では，引き続き，州のコモンローによって営業秘密が保護されている。

⑵　連邦経済スパイ法（Economic Espionage Act：以下「EEA」という）

同法は，1996年に制定された連邦法で，連邦検察官は，これに基づき，営業秘密の窃盗に起因する刑事責任を追及することができる。

⑶　連邦営業秘密保護法（Defend Trade Secrets Act：以下「DTSA」という）

同法は，2016年にEEAの改正法として制定された，連邦レベルの営業秘密保護法である。営業秘密の所有者は，DTSAに基づき，連邦裁判所に対して営業秘密に関する民事上の救済を求めることができる。DTSAについては，損害賠償を定めた条項（18 U.S.C. § 1836）に，米国外での行為への適用を可能とする定めを追加する法案（Protect American Trade Secrets Act of 2021）が，2021年７月１日に下院に提出されている。当該法案は，中国および中国共産党による米国に対する悪意ある影響等に対抗することを目的とする包括的な中国対抗法案（Countering Communist China Act）の一部をなすものである。当該法案が成立した場合，米国外での行為（外国人，外国法人，本社が国外の法人による行為を含む）についても同条が適用されることになる。

2　営業秘密が侵害される場面

⑴　外部者による侵害

外部者による営業秘密の侵害の場面として想定されるのは，競合他社，外国政府，外国軍隊，外国政府系企業等による侵害であるが，これらの者による侵害が，営業秘密の侵

＊ 本稿の準備にあたっては，Morgan, Lewis & Bockius LLP の各現地オフィスに所属の弁護士（米国についてSeth M. Gerber，欧州についてNick Bolterおよび中国についてTodd Liao）から示唆を得た。

[1] 営業秘密については，日本弁理士会の会誌である月刊「パテント」が詳しい。向山純子ほか「米国における営業秘密の現状について」月刊パテント Vol. 70 No. 9，7頁以下，荒木源徳ほか「日本企業の米国子会社における営業秘密の保護に関する実務的考察」月刊パテント Vol. 70 No. 9，13頁以下，浅井敏雄「EU営業秘密指令の概要」月刊パテント Vol. 74 No. 1，84頁以下等。

害全体に対して占める割合は低い。

⑵　内部者による侵害

営業秘密の侵害は，９割以上の場合において，従業員，元従業員等によって行われている。この，従業員，元従業員については，職位や職種に限らず，すべての（元）従業員による侵害のリスクがあると考えるべきである。最も典型的な例は，競合他社に転職した元従業員による営業秘密の使用であるが，外国人従業員が退職後に自国に戻り，営業秘密中の情報を用いて自国で特許を登録する例などもある。

⑶　「不可避的開示論（Inevitable Disclosure Doctrine）」による転職等の差止め

「不可避的開示論」とは，元従業員の転職先での新しい職務のために，当該従業員の前職での営業秘密の開示が避けられない場合があり得ることを認める理論である。特に経営判断に関わる役員等の場合，元の雇用主から具体的な営業秘密を持ち出していなかったとしても，新しい職務の遂行にあたり，元の雇用主からの営業秘密の開示を避けられない場面があり得ることは想像に難くない。このような場合，「不可避的開示論」に基づき，元の雇用主は，一定期間（たとえば２年間），元従業員が新たな雇用主の元でまったく働くことができない，または直接競合する職務に就けないこととする差止命令を求めることができる。ただし，カリフォルニア州では従業員の転職の事由が優先され，このような差止めは認められていない。

⑷　リモートワークと営業秘密

2020年初頭以降の新型コロナウイルスの感染拡大に伴い，各企業でリモートワークが導入された。リモートワーク環境下においては，従業員が営業秘密を含むメールや文書を個人的なメールアカウントに転送しプリントアウトする，プリントアウトした書類を自宅のデスク上に放置する等の事態が頻発しており，リモートワーク導入以前と比べて営業秘密の漏えいのリスクは格段に高まっているといわざるを得ない。なお，新型コロナウイルスの感染拡大の収束後においても，一定数の企業においてはリモートワークの継続が見込まれることから，リモートワーク環境下での営業秘密の保護の強化は，各企業において検討されるべき課題である。

３　営業秘密の漏えい防止対策

米国企業においては，営業秘密の漏えい防止対策として，一般に以下の措置がとられていることが多い。

① 雇用契約／秘密保持契約の締結。
② 営業秘密の保護に関する管理方針／就業規則における営業秘密や秘密保持に関する規定の制定。
③ アクセス制限（業務目的以外での社有パソコンの使用禁止，会社の業務情報をUSBその他の携帯機器に保存し，移転することの禁止等）。
④ 営業秘密の範囲指定（営業秘密であることを媒体上に明記する等。たとえば，重要な内部文書について，ヘッダーまたはフッターに秘密情報である旨，すなわち「Confidential – Proprietary Trade Secret Information」等の明記を義務化）。
⑤ DLP（Data Loss Prevention）ソフトウエアの導入。当該ソフトウエアを使用することで，営業秘密を分類し，当該企業が設定した管理方針の違反を特定することができる。違反行為が確認されると，警告，暗号化，その他の保護措置を講じて修復を行い，営業秘密が共有されることを防ぐ。また，従業員による活動を監視・制御することで営業秘密を保護し，その侵害に関する証拠保全にも役立つものである。
⑥ 退職前面談（エグジット・インタビュー）による秘密保持義務の書面化，退職する従業員のパソコンのハードドライブや関連する電子メール等のファイルを保存し，証拠保全。

前記の措置について重要な点は，「当該状況下において，秘密を守るための合理的な手段」がとられているかどうかである。たとえ

ば，小規模な企業であれば，秘密保持契約の締結のみで十分とされるかもしれないが，数十億ドル規模の企業になれば，秘密保持契約締結の他にも複数の対策が必要と解されることが多い。

4　営業秘密の漏えいが発生した場合の対応

営業秘密の漏えいが発生した場合，訴訟を含め，短期間で集中的に対応することが必要となる。

⑴　徹底的な調査

ただちに法律事務所等の専門家に連絡し，徹底的な調査を開始して，証拠を保全する。通常この手続には，１日から３日程度の時間を要する。

⑵　営業秘密の定義づけ

何が「営業秘密」であるかの定義づけは，当該営業秘密が侵害された場面においてはじめて行われるのが通常である。専門家と企業との間で緊密に連携し，侵害された営業秘密の範囲を短期間のうちに確定する必要がある。

⑶　「要求書（Demand Letter）」の送付

企業が調査を行い，被疑侵害者（たとえば，元従業員）が営業秘密を不正に持ち出し，使用し，開示したと（フォレンジック調査で取得した証拠などに基づいて）判断した場合，通常は，被疑侵害者に対して，①営業秘密が含まれる会社の資産（たとえば，書類，コンピュータやUSB等）の返却や②営業秘密の即時使用中止を要求する通知を送付する。被疑侵害者が協力的な場合，被疑侵害者が所有するデバイスや電子メールについて独立したフォレンジック専門家に調査を依頼し，営業秘密を削除できることもある。

⑷　訴　訟

要求書を送付した後，被疑侵害者が協力的でない場合，被疑侵害者に対して訴訟を開始することになる。訴訟では，営業秘密のさらなる不正利用を防止するために，緊急停止命令（Temporary Restraining Order），さらには予備的差止命令（Preliminary Injunction）を求め，迅速な証拠開示を遂行する。予備的差止命令が出されると，当事者間で和解に向けた協議が開始され，２週間から数カ月の間で和解することが多い。

⑸　上記以外の対応方法（ITCへの申立）

不正利用された営業秘密を利用して製造された製品が米国に輸入された場合，米国企業は，米国国際貿易委員会（the US International Trade Commission：以下「ITC」という）に営業秘密の不正利用に関する申立てをすることができる。ITCへの申立てによる場合，営業秘密の不正利用に対する損害賠償を認めることはできないが，当該製品の輸入を排除する権限を有する。また，ITCの調査は，地方裁判所における訴訟よりはるかに迅速に進行するのが通例である。

⑹　リストへの掲載

営業秘密の所有者は，不正使用者を「企業リスト」に載せるよう政府に要求することができる。掲載された不正使用者は，輸出された米国製品の入手を禁止される（米国商務省の輸出管理規則（EAR）15 C.F.R. Section 744.11参照）。また，米国財務省外国資産管理局（OFAC）の特別指定国民・凍結者リスト（Specially Designated Nationals and Blocked Persons List：SDNリスト）に不正使用者を登録させることもでき，その結果，米国人が当該不正使用者と取引を行うことが禁止される（大統領令（EO）13757参照）。

Ⅱ　欧州（EU）

1　欧州（EU）における営業秘密の保護法制

EUにおける営業秘密に関する法律は，営業秘密の不法な取得，使用，開示に対する保護に関する指令（Directive（EU）2016/943：以下

「指令」という）によって，ある程度の調和が図られている。一般に指令は，達成すべき結果について加盟国を拘束するが，結果達成の方法については加盟国に裁量がある。そのため，各加盟国は指令を実施するために独自の法律を制定することになり，EUを全体としてみた場合，各加盟国の立場は単一ではない[2]。

2　営業秘密が侵害される場面

(1)　外部者による侵害

外部者による営業秘密の侵害の場面としては，取引先による契約上の秘密保持義務違反や営業秘密の使用範囲の制限を超えた使用，窃盗（たとえば，サイバー攻撃）による場合，経済スパイによる場合等があげられる。

(2)　内部者による侵害

EUにおいても，従業員による雇用契約または就業規則上の秘密保持義務違反，営業秘密の使用範囲の制限を超えた使用，無断での営業秘密の複製等は，典型的な営業秘密の侵害の場面といえる。なお，上記いずれの侵害の場面についても，グローバル化，アウトソーシングの増加，サプライチェーンの長期化といった傾向がすべて，意図しないで営業秘密の開示に至るリスクを高める方向に働いていることに留意すべきである。

(3)　労働者の転職等の自由との関係

指令１条３項には，「この指令のいかなる条項も，労働者の移動性を制限するための根拠を提供するものと理解してはならない。とりわけ，その移動性の実施に関し，この指令は，以下のための根拠を提供しない」との規定があり，そのなかには「就業の通常過程において誠実に取得した経験および技能を労働者が使用することを制限すること」の定めが(b)号に明記されている。したがって，米国で認められている「不可避的開示論」に基づく転職等の差止め（前述Ⅰ２(3)参照）は，EUでは基本的に認められていないと解されている。

3　営業秘密の漏えい防止対策

指令その他の立法が具体的な防止対策を規定するものではないが，企業は，営業秘密の保護のために以下の措置をとることを検討すべきである。

① すべての営業秘密特定のための監査，およびその記録。当該記録は，営業秘密の存在およびこれに対する権利の立証（後に訴訟で必要となる）に役立つ。
② 営業秘密の保管に関する保護措置の実施。これには，営業秘密へのアクセス制限，文書の機密性の表示，ハードコピーの社外持出禁止，電子ファイルのパスワード・認証手段等による保護等が含まれる。
③ 営業秘密に関する従業員研修，従業員による企業の営業秘密保護方針の確認および署名。
④ 雇用契約における営業秘密の明確な保護（秘密保持義務条項，および雇用終了後の営業秘密の使用を制限する条項を含める）。
⑤ 企業の営業秘密を扱うすべての取引先との秘密保持契約の締結（または秘密保持義務条項を含む契約の締結）。
⑥ 交渉段階では，一定程度手続が進むまで営業秘密を非開示とすること。
⑦ セキュリティ手順の頻繁な見直し。
⑧ サイバー攻撃リスクの積極的な管理（例：データの暗号化，最新のソフトウェアの使用，アクセス可能な従業員の身元調査，使用済データの適切な廃棄等）。
⑨ サイバー攻撃のリスクに備えた保険加入（営業秘密の開示は防げないが，経済的な影響を軽減可能）。

4　営業秘密の漏えいが発生した場合の対応

いったん営業秘密が公に開示されると，開示前の状況には戻せず，権利者である企業に

[2] 指令を国内法化したものに加えて，各国の法令によっても営業秘密は保護されている。本稿では紙面の関係上，指令の解説に限定しているため，各国における保護法制を検討される際には，その点にご留意いただきたい。

壊滅的な影響を与える可能性がある。よって，権利者は被疑侵害者に対してただちに暫定的救済を求めることが不可欠である。

⑴　**指令10条に基づく暫定的救済**

指令10条は，営業秘密保有者の要請に基づき，司法当局が被疑侵害者に以下のすべての救済を命じることができることを加盟国が保証すべきであると規定している。

① 暫定的に営業秘密の使用／開示を停止または禁止すること。
② 侵害品（不法に取得された営業秘密から利益を得る商品）の製造，提供，市場への配置または使用を禁止すること。
③ 被疑侵害品の押収および引渡しにより，市場への参入／流通を防止すること。

上記の暫定的救済は，申請者が，(a)営業秘密保有者であることおよび(b)営業秘密が不法に取得され，不法に使用され，もしくは開示されていること（または当該取得，使用もしくは開示が差し迫っていること）を十分な確実性をもって裁判所に納得させられることを条件とする。

なお，裁判所は，営業秘密保有者に対し，最終的に違法行為が発見されなかった場合に支払われる被疑侵害者への補償のための担保を差し入れるよう要求することができる。

⑵　**暫定的救済に続く措置**

㋐　**法的手続**

暫定的救済の付与に続いて，営業秘密保有者は，関連当局での訴訟の本案の決定につながる法的手続を速やかに開始すべきである。指令は，関連当局による差止命令，是正的救済措置および損害賠償（被疑侵害者が不法な取得，使用または開示に従事していることを知っていた，または知っているべきであった場合）を規定している。状況に応じて，契約違反による救済措置も可能である（例：営業秘密の不正使用が秘密保持契約違反に起因する場合）。

㋑　**是正措置**

営業秘密侵害の根本原因の分析および背景調査を行い，再発防止のための是正措置を実施する。

㋒　**被害報告**

サイバー攻撃を受けた場合，企業は，規制当局やデータが流出した可能性のある第三者にセキュリティ侵害を報告しなければならない。潜在的な風評被害の軽減には，危機管理の経験を持つ広報担当者の支援が有用である。

Ⅲ　中　国[3]

1　中国における営業秘密の保護法制

中国には，統一された営業秘密法は存在しない。営業秘密の保護は，主に，「反不正当競争法」[4]および「司法解釈」によって図られている。「反不正当競争法」は，1993年に公布され，直近では2019年に改正された。

2　営業秘密が侵害される場面

⑴　**外部者による侵害**

外部者による営業秘密の侵害の場面としては，下請けまたは顧客といった，取引先からの漏えいの場合，ハッキングなどの行為によって盗用される場合等が想定される。また，近年，インターネット上の新たな侵害形態として，文書共有サイトに営業秘密情報が無断でアップロードされる等の被害が多発しているのも，中国における営業秘密侵害の特徴である。

⑵　**内部者による侵害**

中国においても，従業員，元従業員等によ

[3] 中国の営業秘密については，独立行政法人日本貿易振興機構上海事務所の「中国における営業秘密管理マニュアル」（2020年3月）が詳しい。

[4] 反不正当競争法の各条項について，http://www.lindapatent.com/jp/law_other/965.html を参照。

る営業秘密の侵害が最も多くの割合を占めている。これには，正規雇用の従業員に限らず，派遣従業員等による侵害も含まれる。典型的な事例としては，在職中の従業員による競合他社に対する営業秘密の漏えい，競合他社に転職した元従業員による営業秘密の使用に加えて，従業員がみずから設立した競合会社での営業秘密の流用等があげられる。

3　営業秘密の漏えい防止対策

中国における営業秘密の漏えい防止対策の検討にあたっては，反不正当競争法における「営業秘密」の定義および司法解釈[5]に定められる「秘密保護措置」を考慮することが重要である。

(1)　「営業秘密」の定義

反不正当競争法において，「営業秘密」は，「公衆に知られていない，商業的価値を有し，かつ，権利者が関連の秘密保護措置をとった，技術情報，経営情報等の商業情報」（同法９条）と定義されている。

(2)　「秘密保護措置」

上記の定義から，中国において，ある情報が「営業秘密」に該当し，法律上保護されるためには，「秘密保護措置」をとったことが必要となる。

この「秘密保護措置」については，司法解釈に規定されており，権利者が以下のうち少なくとも一の手段をとる限り，法律上「秘密保護措置」をとっていると認められる（もちろん，より多くの手段がとられていることが望ましい）。

① 守秘契約または守秘条項を含む契約を締結する。
② 営業秘密にアクセスし，またはそれを入手できる可能性のある従業員，元従業員，サプライヤー，顧客，訪問者等に守秘義務を課すために，定款，研修，規則や手順，書面による通知等の方法を使用する。
③ 分類された工場の建物，作業場，その他の生産現場への訪問者のアクセスを制限する。
④ 印付け，分類，隔離，暗号化，保管のための封印，その他のアクセス制限等の手段により，営業秘密を区別して管理する。
⑤ 営業秘密への不正アクセスの原因となるおそれのあるコンピュータ，電子機器，ネットワーク機器，記憶装置，ソフトウェア等の使用またはこれらによる保存もしくは複製を禁止し，または制限する。
⑥ 離職する従業員に対し，アクセスまたは取得した営業秘密を登録，返却，削除または破棄すること，およびその守秘義務が解雇後も存在することの確認を求める。

なお，上記の措置は，是正措置ではないため，被疑侵害行為が発生する前に予防的に実施されていなければならない。

司法解釈により，法律上「秘密保護措置」をとったと認められた場合，被疑侵害者側がこれを覆すのは困難である。

4　営業秘密の漏えいが発生した場合の対応

(1)　初動対応

営業秘密の漏えい（またはその兆候）が発生した場合，速やかに事実関係の調査を開始する。漏えいの兆候としては，従業員による業務上必要のないアクセス行為や特定の競合他社との頻繁な接触，競合他社に転職した元従業員の前職と同じ分野での研究開発の実施，また取引先からの突然の取引の打切り等があげられる。調査の目的は，迅速に証拠を収集し，保全することである。したがって，できる限り速やかに，現地の法律事務所その他の専門家に相談する等して，専門家による調査を実施すべきである。

[5] 最高人民法院の「不正競争民事案件の審理における法律適用の若干問題に関する司法解釈」（2007年２月１日施行）11条。

⑵　民事訴訟

営業秘密の権利者は，侵害者に対して，民事訴訟を提起し，侵害行為の差止めおよび損害賠償を求めることができる。

㋐　損害賠償の金額

損害賠償の金額は，反不正当競争法17条および司法解釈[6]に基づき，以下の①ないし③を基準に，その順序で算定される。

① 権利侵害行為によって被った実際の損害に基づき算定。
② 侵害者が権利侵害行為によって得た利益に基づき算定。
③ 参照可能なロイヤルティに基づき合理的に算定。

ただし，上記３つの損害賠償額の算定手段が利用できない状況下では，裁判所は個々のケースの詳細に応じて500万元以下の賠償額を決定することができる。

①または②の算定方法による場合において，侵害行為が悪意で実施され，かつ，情状が重大であるときは，いわゆる「懲罰的賠償制度」が適用される可能性もある。適用された場合，賠償額は，①または②の基準で算定される金額の１倍以上５倍以下の金額で確定される[7]。

㋑　証拠の公証認証手続

民事訴訟による損害賠償等を求める場合，権利者が，侵害された営業秘密が法律上の「営業秘密」に該当することや相手方に営業秘密の侵害行為があったことを証明する証拠を提出しなければならない。この際，中国においては，民事訴訟に提出される証拠は，原則として公証認証手続を経る必要があることに注意が必要である。

たとえば，他社が製造，販売している製品が自社の営業秘密を利用して製造されていることを主張する場合，当該他社製品を購入して証拠として提出することとなるが，公証認証手続なしにこれを購入し，証拠として提出したとしても，基本的に証拠能力は認められない。この場合，被疑侵害品の購入にあたり，公証人を同行させ，被疑侵害業者による販売行為や販売時に交付された発票などを現認させる手続を行う必要があり，これを「公証購入」という。

⑶　行政摘発

行政摘発は，日本にはない法的措置である。営業秘密の侵害に対しては，各地の市場監督管理局によって，侵害行為の停止命令，違法所得の没収，過料等の行政処分が科される。行政摘発後に侵害者に対して民事訴訟を提起し，損害賠償請求することも可能であることから，後の民事訴訟を見据えて，侵害行為の証拠収集手段の１つとして行政摘発が利用されたと考えられる事例も散見される。また，被害規模等に応じて，行政機関の判断で，刑事制裁の対象として刑事手続に移送される場合もある。

Ⅳ　おわりに

営業秘密の保護に関する各国の実務は，日本の実務に通じるものも少なくない反面，各国（米国の場合には各州）に特有の事項も含まれる。また，一度侵害されると元には戻らない営業秘密の特性上，いずれの国においても，迅速に専門的な対応をすることが求められる。本稿が，各国での実務の確認，ならびに日常的な営業秘密の管理体制および侵害発生時の対応の両側面からの検討のきっかけとなれば，幸いである。

---

[6] 最高人民法院の「営業秘密侵害民事事件の審理における法律適用の若干問題に関する司法解釈」（2020年９月12日施行）（以下「2020年司法解釈」という）20条。

[7] 合理的ロイヤルティについて，中国の他の知財法（たとえば，特許法，商標法，著作権法）では，合理的ロイヤルティに基づき懲罰的損害賠償の金額を定める旨の規定が明記されている。しかし，営業秘密に関する反不正当競争法や2020年司法解釈にはそのような規定はない。今後，法改正や司法解釈の進展が注目される。