【学会紹介】

2021年度 第8回 日韓サイバー法学会

――グローバルパンデミック時代における刑事法的課題――

専修大学法学部准教授　森 住 信 人

はじめに

2021年9月25日（土），第8回日韓サイバー法学会が開催されました。日韓サイバー法学会は，当初，日髙義博先生と白允喆先生（大邱サイバー大学・施安政策研究院院長）が中心となって設立し，2013年に第1回学会が開催されて以降，年に1回，日本と韓国とで交互に開催されてきました。コロナ禍のために2020年には開催できなかったのですが，2021年はZoomを利用してのオンライン開催となりました。この第8回日韓サイバー法学会では，今村法律研究室も共催という形で係わりましたので，室報にて簡単にご紹介させていただければと考えた次第です。

申し訳ないことに学会の録画・録音がなされませんでしたので，本紹介は小生の曖昧なメモと記憶によります。各ご報告については配付された資料から概要を示すことができていると思われますが，正確なご報告は論者によって紀要などにご掲載されるのをお待ちいただきたく存じます。また，本室報で紹介する，崔鎬雄弁護士と黄興益先生のご報告は，韓国語で執筆されたものを楊萬植先生が翻訳し，ところによって小生が訂正しておりますので，必ずしもご報告を正確に紹介できているとは限らない点についてはご容赦いただければありがたく存じます。

開催前

第8回日韓サイバー法学会は，9月25日（土）13:30からの開催の予定でしたが，Zoomの接続確認のため，13:00には接続可能となりました。日韓共に参加者が順次接続し，互いに声を掛け合い，和気藹々とした，そして混沌とした雰囲気になっていました。複数の接続先から挨拶がなされたため，ハウリングが生じるなどもあり

ましたが，すぐに落ち着きました。日本側参加者には韓国語に通じた者がおりませんでしたので，すべての通訳を楊萬植先生にご担当いただきました。通常の会話から報告，質疑応答の翻訳までお一人でご負担なさいましたので，相当の負担だったかと思います。楊先生のご尽力なしには本学会は成り立ちません。紙上ではありますが，あらためて御礼申し上げさせていただければと存じます。

学　会

定刻になったところで，それまで三々五々に行われていた会話が止み，白先生と日髙先生によって参加者の紹介が行われました。その後，日髙先生による祝辞が寄せられ，粛々と学会が進行いたしました。

日髙義博先生祝辞

コロナ感染が収束しない中での日韓サイバー法学会の開催となりましたが，白先生，朴先生，楊先生のご尽力により，オンラインでの学会開催が可能となったことは，本当に嬉しいことです。長期にわたるコロナ禍は，大学の運営だけでなく，すべての社会活動にブレーキをかけてきています。非日常の連続であり，心身ともに疲弊感があります。しかし，いかなる状況にあっても，学問の道を歩みはじめた以

日髙義博先生の祝辞

上，中断は許されません。学術研究は継続しなければ，大きな成果は生まれません。その意味で，コロナ禍にあっても日韓サイバー法学会の開催方法を検討し，オンラインでの開催準備をしていただいた韓国側の会員の皆様に心からお礼を申し上げ，感謝の意を表します。

今年は早くもキンモクセイの花が咲き，朝夕に清閑な香りが漂っています。季節はもう秋に入ったのかと思い，時の流れの早さに驚いています。非日常の連続が解消されることを祈りながら，今回の学会において実り多い成果が得られることを期待しています。

【第１部】

日髙義博先生が座長となり，岡田好史先生によって第１報告「インターネット上の名誉毀損，侮辱に対する日本での法改正の動向」がなされました。当初，こちらにて岡田先生のご報告の概要を掲載する予定でしたが，本室報に岡田先生のご報告が掲載されるとのことですので，そちらをお読みいただければと存じます。

岡田先生のご報告には朴寅東弁護士（金＆張法律事務所）からコメントを寄せられ，これを契機として活発な議論が行われました。

岡田好史先生の報告

【第２部】

休憩を挟んでから行われた第２部では，白允喆先生が座長を務め，崔鎬雄弁護士（法務法人 DUKSU）による第２報告「ボイスフィッシング詐欺に関する研究」と，黄興益先生（檀國大学）による第３報告「國家産業保安に関して」がなされました。

第２報告の概要は以下のようです。

【第２報告】

「ボイスフィッシング詐欺に関する研究 ――貧しい人々だけが残されている現実について」

崔鎬雄弁護士（法務法人 DUKSU）

【概　要】

１．はじめに

ボイスフィッシング詐欺は，その被害が大きく，その方法も技術の発展に応じて多様化してい る。被害者のほとんどが生活困難から，藁をも掴みたい気持ちで瞬間的に欺かれてしまい，その犯罪に加担する単純加担者たちも自己の生計のために高額の所得を得たい誘惑で犯行に加担することになる。以下においては，ボイスフィッシング詐欺の犯罪手法，発生件数の広範さ，その罰則規定，検挙状況を調べ，単純な加担者に対する処罰が犯罪防止という目的だけであまりにも過度に行われている現実に対する検討をし，今後の対応方向について意見を提示したい。

電気通信手段による金融詐欺（いわゆる「ボイスフィッシング」）組織は，中国や国内の捜査機関の追跡が困難な地域でインターネット電話などを利用し，韓国の不特定多数の被害者を対象として捜査機関や金融監督院の詐称，貸出し口実，家族の拉致，個人情報の流出などの内容で被害者を欺き，これに騙された被害者たちにとって自分たちが管理する口座に金銭を振替または入金するようにし，または被害者から金銭の交付を受け，これを騙取する手法で犯罪を行う組織である。ボイスフィッシング組織の役割分担は，犯行全体を総括し，内部の各組織間における有機的な連絡を担当する「総責任者」，総責任者の指示を受けて内部の組織員を管理し彼らに欺

瞞手法と現金の回収方法などを教育・指示する「管理役」，不特定の多数の被害者に電話をかけ政府機関などを詐称して嘘をつき被害者を欺く「誘引役・コールセンター」，口座に入金された被害金を引き出して伝達したり，被害者と直接会ってお金を受け取る「現金引き出し役・現金回収役」，犯行に使用する大砲通帳や組織員などを募集する「募集役」など，それぞれ分担された役割を果たしている。しかし，捜査機関の検挙に備えた点組織で運営されており，テレグレムのようなセキュリティの高いメッセンジャーを介して連絡を取り交わし，組織員であっても相互の身分を知ることができないようになっている。

2．具体的な事例

従来通り電話などの電気通信を利用し知人を詐称して金銭を詐取する犯罪類型も継続的に起きているが，ここではボイスフィッシングによる犯罪類型の中でも機関を詐称する「機関詐称型」と貸し出しを口実にする「ローン詐欺型」とに分けて検討する。

⑴　機関詐称型

捜査機関，金融監督機関などであると脅かしてから，名義の盗用，大砲通帳などの事件と関係したと脅迫した上で，電話で現金を要求したり，誰かに会って現金を渡すように欺く方式であったり，被害者から被害者の通帳から出金が可能な情報を取得し金銭を詐取する方式である。被害者は捜査機関の要請であると信頼し，自分の主要な金融情報を提供することになるが，犯罪団体は捜査機関であると欺く過程で虚偽の通知書などを送って捜査機関であると信じるように誘導する。

⑵　貸し出し詐欺型

電話を使用して不特定の多数人を相手とし，ランダムに電話をかけて自分を「金融機関の職員」と紹介し，貸出を受けようとする被害者に低金利の貸出ができるかのように誘惑し，申請書を送って接続するよう誘導する手段である。被害者が申請書を作成すると，再び被害者に電話をかけ，既存の貸付金があって，他の場所で融資を受けると金融取引法違反となり，12ヶ月以内に融資を受けると契約違反となるから，既存の貸付金をすべて完納するようにする。そして，職員が直接行くようにしたのでその職員と直接に会って既存の貸付金の返済するよう指示する。このよう

な言葉に騙された被害者は，金融機関の職員を詐称する組織員（回収役）に既存の貸付金を現金で直接支給し，回収役は受け取った金銭を組織の指定された口座（大砲通帳）に入金する。しかし，実際，組織は被害者に融資をする意思や能力が全くなく，被害者から金銭を詐取する。被害者自らが金融機関から融資されると信じるように，作成された虚偽の文書を被害者に提供することも頻繁にある。

3．犯罪発生の現況

警察庁が公開した統計によると，2016年から2020年までボイスフィッシング関連犯罪の発生件数と被害額は，以下のようである。

区分	機関詐称型	被害額（億）	検挙件数	貸し出し詐欺型	被害額（億）	検挙件数
2016	3384	541	3860	13656	927	7526
2017	5685	967	3776	18574	1503	15842
2018	6221	1430	4673	27911	2610	25279
2019	7219	2506	5487	30448	3892	33791
2020	5006	1492	2924	16008	3036	20286

（出典：警察廳 ボイスフィッシングの現況）

上記の統計によると，2019年の一年だけで約3.7万件のボイスフィッシング関連犯罪が発生し，その被害額は7,000億ウォンに達している。上記のように，多くの被害が続出しており，被害額自体が天文学的な状況であって，捜査機関や政府機関においてもその深刻さを認識し，その対策に苦心している。

4．犯罪に対する適用法規

基本的に，ボイスフィッシング犯罪の処罰は，刑法上の「詐欺罪」（第347条）が適用され，ケースに応じて「コンピュータなどの詐欺利用罪」（第347条の２）または「恐喝罪」（第350条）が適用されている。また，詐欺額の規模によって詐欺罪の加重処罰の規定である「特定経済犯罪加重処罰等に関する法律」をもって処罰する（利得額が50億ウォン以上になると無期または５年以上の懲役，利得額が５億ウォン以上50億ウォン未満であると３年以上の有機懲役）。上記のように，ボイスフィッシング犯罪は組織化され，体系的に行われ，被害の程度が広範に及ぶため，刑事法上の重大な犯罪を目的とする組織やグループを組織したり，これに加入またはメンバーとして活動し

た者の全員にその目的とした罪で定められた刑で処罰できる「犯罪組織罪」（第114条）を適用する場合もある。

2020年ボイスフィッシング役割別検挙現況

組織上部（總責）	下部組織員	通信業者・換錢策	計座名義の貸與
2.1%	35.1%	8.2%	54.5%

（出典：韓國放送公社の警察廳　情報公開請求）

5．単純な加担者に対する過剰処罰の問題

⑴　前述のように，ボイスフィッシング組織は，総責任者から単なる金銭回収を担当する「回収役」まで，組織の形で体系化されている。ところで，実際，捜査機関が犯罪組織のメンバーを検挙してみるとその大部分は表で示すように，ほとんど単純な回収業務を担当し，または単純に通帳をレンタルした下部加担者である。

単純な加担者であるこれらのボイスフィッシング組織の犯罪方式や積極的な加担ではなく，単純なアルバイトと考えたり，別段の問題意識を持たずに加担するのがほとんどである。ほとんどの単純な加担者は，生活が困難な状況に置かれていたり，社会経験の不足な学生である。彼らは他のアルバイトや雇用よりも高額の収入を得ることができるという誘惑にさらされている。しかし，彼らも詐欺罪の共同正犯または詐欺罪の幇助となる。これは，未必的故意があり，ボイスフィッシングに対してある程度の暫定的な認識があって処罰される場合である。通常，単純な回収役の場合にも，立件されると拘束令状が発行され，加担と被害額に応じ懲役２年以上の実刑が宣告されている。実際，被害者が10人であり，その被害額が２億ウォン程度に達した事案でアルバイトとして加担した回収役の者に対し，裁判所は懲役２年６月を宣告した例がある。被告人は，単純な加担で500万ウォン程度の手数料の利得を得ただけであった。

⑵　捜査機関や司法機関では，ボイスフィッシング犯罪の被害額が7,000億ウォンに達し，その被害者もあまりに多く発生していることから，末端下部の加担者に対する強い処罰で犯罪を減らそうとする視点を持っている。しかし，総責任者などの実質的に詐取した金銭を取得する本体を検挙できない責任を単純な加担者だけに過度な処罰を科すことで犯罪を予防するということは，刑法上，その責任に相当した処罰を受けるべきであるという「責任主義」に反するとの問題点がある。犯罪組

織の国際化や点組織化により犯罪組織の本体の検挙が困難であるとしても，犯罪手法や利得取得に積極的に共謀や加担をしていなかった単純な加担者に対する現在の司法機関の処罰の程度は過度な点があると思われる。

6．結語――ボイスフィッシング犯罪に対する対応について

金融機関などの政府機関において新しいタイプのボイスフィッシングを認知した場合には，速やかな広報を通じて被害が拡散されないように対処すべきである。近年，コロナが長引くことにより小商工人の生計が困難な状況となっており，これを利用した新しい形態のボイスフィッシング手法が引き続き起きている現状（さらに災害支援金の支払いを内容とするボイスフィッシング手法も現れている）からすれば，政府機関はより細かいモニタリングを通じて継続的に犯罪の手法を認知させ，被害が拡大しないようにしなければならない。さらに，これまで検討したように，高額収入を得ることができるという誘惑に陥る可能性のある生計が困難な者や社会経験の少ない学生を対象にして，ボイスフィッシング犯罪の手法や加担した際には厳しい処罰を受けることになるとの教育や広報が必要である。これらの教育と広報を通じた予防措置が，単純な加担者にすべての責任を転嫁するような厳しい処罰よりも優先されるべきと考える。結局，ボイスフィッシングの犯罪集団を完全に検挙することは，犯罪組織の形態上，最終的には国際的捜査に協力する役割が重要であり，捜査機関と政府との外交的努力が要求される領域である。このような方法を通じて犯罪組織の本体を検挙し，実際に金銭を取得した者が隠匿した財産を追跡・没収して被害者の被害を回復できるよう努力すべきである。ボイスフィッシング犯罪の理解として，生計が困難な者との間での加害・被害関係のみの問題に拘泥するべきではないであろう。

第２報告については李相卓警察官（大田警察廳）からコメントが寄せられ，これを契機として活発な議論が行われました。

第２報告に続いて行われた第３報告の概要は以下のようです。

【第 3 報告】

「国家産業セキュリティについて――営業秘密保護法を中心として」

黃興益先生（法學博士，檀國大學校）

【概　要】

1．はじめに

現在，世界中で誰も事前に予見することはもちろん，経験することもできなかったスピードの技術革新によって，いわゆる第 4 次産業革命の時代を迎えている。既存の食生活，労働方式，生産や消費行動，さらには人々の間に生じる日常の生活様式の全般を変えるほどの革命的変化の波に直面している。代表的な例として，人工知能やロボット，ビッグデータ，クラウディング，3D プリンティング，ナノバイオテクノロジーなど，ほぼすべての知識・情報の分野に渡って目覚しい変化と発展が第 4 次産業革命をリードしている。したがって，国家間の熾烈な技術戦争に突入しており，特に，企業や労働現場においては産業の原動力である営業秘密や国家産業機密に対する関心がこれまで以上に高まっており，国家間の利害対立はさらに先鋭化していくと予測されている。それでは，4 次産業革命時代の産業機密を論じる前に，「営業秘密とは何か」について理解する必要がある。営業秘密を一言で表すと特許化されていないが，将来，無限の経済的価値を持つ企業の情報をあわせて営業秘密（trade secret）であるということができる。例えば，公然に知られておらず，独立した経済的価値を持つものであって，かなりの努力によって秘密が維持されているアイデアや生産・販売方法，その他の営業活動に有用な技術上又は経営上の情報ということができる。これは，民間企業を中心とする私的領域の性格が強い。これに比べて，公的領域の性格が強い「産業セキュリティ」は，最先端の技術だけでなく，産業活動に有用な技術上，経営上の情報を産業スパイなどの様々な危害要素から漏洩または侵害されないよう保護，管理するための対策や活動でありながら企業活動のために保護する価値のある人員・文書・施設・技術などの諸産業機密の侵害を防止し，関係のない者に漏洩されないように保護する活動を意味する。一言で表すと外国ハッカー，いわゆる産業スパイに自国の産業機密が流出されないように努力することを意味する。以下においては，アメリカなどの外国の営業秘密保護に関する

動向を検討し，わが国の技術を流出する時の処罰条項や産業機密の流出事例及び流出の兆候，対応措置などを論じてみよう。

2．アメリカ・ドイツ・日本の営業秘密保護の動向

(1)　諸外国における営業秘密の定義

①アメリカ（統一営業秘密保護法，UTSA）　経済的価値を得ることができる者に一般的に知られておらず，正当な手段によっては容易に得ることができないため，営業秘密を保有している者のみが現実的または潜在的に独自に経済的価値を持つことができること。つまり，適切かつ合理的な努力が加えられた製法，公式パターン，データの編集，プログラム，ツール，考案などを含むすべての情報

②ドイツ（不正競争防止法）　営業秘密とは概ね事業活動に関することであって，限られた者のみに知られており，一般には知られていないものであり，また，秘密維持の意思が明らかであるだけでなく，その情報を秘密に維持することにより，正当な利益を得ることができる情報

③日本（不正競争防止法）　秘密として管理されている生産方法，販売方法その他の事業活動に有用な技術上又は営業上の情報として公然に知られていない情報

(2)　アメリカの営業秘密保護の動向

①統一営業秘密保護法（UTSA：Uniform Trade Secrets Act）　アメリカでは1979年に公布された統一営業秘密保護法（UTSC）第１条第４項にて，「営業秘密とは公式（formula），様式（pattern），編集物（compilation），プログラム（program），図案（device），方法（method），技術（technique），または工程（process）を含む以下の条件を満足する情報を意味する。」と規定している。営業秘密に関する効率的な刑事法的保護のため，1996年に連邦経済スパイ法（EEA：The Economic Espionage Act）を制定した。

統一営業秘密保護法（UTSA）は，保護条件として，第一に，その情報の開示または使用によって経済的価値を得ることができる他人に一般的に知られておらず，予想することができたり，または公正な手段を使用しては容易に確保することができない実質的または潜在的に独立した経済的価値のあるもの，第二に，その情報の機密性を維持する義務があると判断できる合理的な努力の対象となるものであるとしている。

また，1996年のEEAにも営業秘密の定義が規定されているが，これによると，営業秘密は，「企業の財務，ビジネス，科学，技術や工学情報のすべての形態と様式としてその所有者が情報の秘密を維持する合理的な措置を取ったり，その情報が他人に対して秘密にすることが，実際上または潜在的な独立の経済価値を持つ場合」であるとしている。

②連邦経済スパイ法（EEA）　米国の連邦経済スパイ法においては刑事処罰となる行為の種類を大きく二つに分けている。外国を利することを目的として，営業秘密を侵害した場合（経済スパイ：Economic espionage）と，個人を利することを目的として，営業秘密を侵害する場合（営業秘密窃取罪：Theft of trade secrets）に分けて処罰している。

③営業秘密の民事的保護　一般的に，営業秘密の不正な流用に関する民事訴訟は，アメリカの他の民事訴訟と同様に行われ，幅広い証拠開示，申請手続，事実審理が含まれ，訴訟手続規則は，州と州裁判所，連邦裁判所によっても異なるが，一般的に関連する証拠開示の手続（文書及び調査依頼，実際の承認要請，質問書，供述録取）によって訴訟当事者は相手方の当事者から情報や文書を収集することができる。また，訴訟当事者は却下・棄却申請や概要審判などの訴訟を終了する申請をすることができ，事実審理前の準備も十分に行うことができる。原告は，証拠の優越基準に基づいて営業秘密の不正な流用を証明する責任を負う。つまり，不正な流用が発生したことを50％以上を証明する証拠を提出する必要がある。

（3）　ドイツの営業秘密保護の動向

①不正競争防止法（UWG：Gesetz gegen den unlauteren Wettbewerb）　ドイツでは，競争者，消費者やその他の取引参加者を不正な競争から保護することを目的とした不正競争防止法（UWG）がある。そして同法第４条２項の模倣行為と第17条の営業秘密保護規定のように禁止された行為の種類は，知的財産権を侵害する種類と重複的な範囲に該当するとされている。UWGでは，営業秘密（Unternehemensgeheimnis：営業秘密またはWirtschaftgeheimnis：経済秘密）は，「ビジネスの秘密（Geschäftsgeheimnis）」と「工業上の秘密（Betriebsgeheimnis）」という２つの概念に分かれている（17条１項，２項１号・２号）。商業上の秘密は，経済的・観念的な観点から秘密となる情報をいい，工業上の秘密はビジネスにおいての工業的・技術的な観点から秘

密となる情報であるとしている。

②刑事的および民事的保護　ドイツでは，営業秘密に対する刑事的保護の根拠は，不正競争防止法（UWG）の他に刑法（StGB第202条［データ検出などの禁止］，第203条［私的秘密の侵害］，第204条［他人の秘密の利用など］）等においても営業秘密の保護のための法体制を構築している。ドイツの裁判所によると，営業秘密は，(i)公的に知られていないこと，(ii)企業の営業活動と関連していること，(iii)該当企業の意思に基づいて秘密として保護していること，(iv)正当な経済的利益であることが，その保護要件である。

営業秘密に対する民事的保護として，禁止・除去命令，損害賠償，情報の提供，廃棄がある。禁止請求権（Unterlassungsanspruch），除去請求権（Beseitigungsansprunch）は，ドイツ民法（Bürgerliches Gesetzbuch：BGB）第1004条，UWG（不正競争防止法）第３条を根拠としているが，民法第1004条は「所有権が占有の侵奪または物件の誘致その他の方法で侵害されている場合に，所有者は，侵害者に対して侵害の排除を請求することができる。」と規定している。

ドイツでは従業員が秘密を漏洩した場合にも，それが雇用契約中でなければ，営業秘密として保護していないことを前提とする。雇用契約が終了した後は，営業秘密を保護すべき契約上の義務があるとはせず，「誠実に（auf redliche Weise）」取得した営業秘密は訴訟の対象にならない。「誠実な」という言葉の範囲を判断した判例もある。

(4)　日本の営業秘密保護の動向

①不正競争防止法　2004年に改正された不正競争防止法第２条４項によると，営業秘密とは「秘密に管理されている生産方法，販売方法その他の事業活動に有用な技術上または営業上の情報として公然に知られていないことであるもの」であると定義している。すなわち，「営業秘密」とは，(i)秘密に管理されていること（秘密管理性），(ii)事業活動に有用な情報であること（有用性），(iii)公然と知られていないこと（非公知性）という３つの要件を満たす技術上あるいは営業上の情報とし（第２条６項），この３つの要件すべてを満たしている場合，営業秘密として保護される条件となる。

②営業秘密の保護に関する動向　日本の営業秘密の保護は，1993年不正競争防止法の制定の際に明文化され，数回の改正，「技術流出防止指針」の制定や「営業秘密

管理指針」の改正などにより，その強化が進められてきた。しかし，最近，退職者などによる営業秘密（特に技術情報）の流出が頻繁になり，大きな問題となっており，今後もその深刻さは増大すると予想されている。2003年，不正競争防止法により初めて営業秘密を侵害する行為に対し刑事的に処罰する規定が設けられた。経済の発展と社会環境の変化により，営業秘密の侵害行為について刑法によって窃盗罪，業務上横領罪，背任罪などで処罰することは限界に直面し，大きな問題であるとの指摘もある。その後，2005年の不正競争防止法では，法人処罰，退職者の処罰，国外犯の処罰，法定刑の加重など処罰範囲が拡大され，2009年には「不正競争の目的」に限定されていた主観的構成要件を「不正な利益を得る目的またはその保有者に損害を加える目的」に改正し，その処罰範囲を拡大した。日本の現在の不正競争防止法においては７つの犯罪の種類を定めており，これらの犯罪は主観的構成要件として「不正な利益を得る目的と保有者に損害を加える目的」を必要とする目的犯であり，親告罪として構成されている。

(5)　韓国の営業秘密保護の動向

①営業秘密に関する裁判所の判断　最高裁判所は，営業秘密について，「営業秘密」とは，公然に知られていないこと（非公知性），独立した経済的価値をもつこと（経済性），相当な努力によって秘密として維持されること（秘密管理性），生産方法，販売方法その他の営業活動に有用な技術上または経営上の情報を指していると判断しており，営業秘密に該当するかどうかの判断に関しては，「ユーザーが主張する営業秘密自体の内容だけでなく，労働者の勤務期間，担当業務，職責，営業秘密へのアクセスの可能性，転職の会社で担当した業務の内容と性格，ユーザーと労働者が転職した会社との関係など，いくつかの事情を総合的に考慮しなければならない」と判断した。

②産業技術の流出における罰則条項

海外技術流出等の産業スパイ関連法令と処罰条項

法令	不正競争防止及び営業秘密保護に関する法律	産業技術の流出防止と保護に関する法律	刑法
罪	営業秘密侵害罪	産業技術流出罪	スパイ罪
処罰	10年以下の懲役または１億ウォン以下の罰金	10年以下の懲役または10億ウォン以下の罰金	死刑，無期懲役または７年以上の懲役

③営業秘密の保護の必要性　第４次産業革命時代における営業秘密の保護の必要性は産業の高度化と情報化，知能化に伴ってさらに増大しており，経済活動の過程において技術の高度化と市場競争の強化および顧客の多様化の傾向などにより営業秘密の重要性が質的な面ではもちろん，量的な面においても増大している。営業秘密は単純に企業，個々の産業レベルでのみ意味を持つものではなく，産業の技術力と競争力を支える経済発展の基盤を形成するために非常に重要である。

3．産業技術の流出事例

⑴　先端技術の流出実態

産業機密保護センターによると，国家の核心技術の流出事件が毎年継続的に増加する傾向にある。したがって，政府は，国家安全保障と国民経済に重大な影響を与えるおそれのある産業技術として半導体・造船・鉄鋼・情報通信など12の分野における関連技術を国家核心技術として指定している。これと関連し，産業府と警察庁などの関係機関によると，2011年から2016年までの６年間，国内の技術が海外に流出した事例は数百件にも達しているとしている。分野別にみると先端技術が集約されている電気電子分野（33％）での技術流出が集中されており，その次に機械，情報通信，化学，バイオテクノロジー，その他の分野において頻繁に流出されていた。また，被害を受けている企業別では，中小企業／ベンチャー企業での流出は63％に達し，大企業は17％，大学／研究所等で14％，その他で６％であると調査され，中小／ベンチャー企業における技術流出が深刻であることが確認されている。これらにおける技術の流出は主に転職した職員が移転またはスカウトされる際に生じていることが確認されている。

⑵　産業機密の探知手法

産業機密の探知手法をその主体別にみると，合法を仮装する方法と非合法的な方法で大別することができる。合法を仮装する方法の中で代表的なのは，スカウトの方法であって全体の産業スパイの70％を超えている。その次は技術協力を通じる買収（45％），合弁事業（45％），コピー（37％），FAX・コンピュータ・ネットワーク，視察・見学，産業研修，共同研究などの順であった。非合法的な方法としては，盗聴やハッキング，買収，偽装就職などがある。最も頻繁に使用されるタイプは，個

人の金銭的欲求を利用し，競争企業の職員を買収し，必要な営業秘密を入手する方法である。不正な侵入と第三者買収，情報ブローカーの利用などの様々な形で技術流出が行われているが，このようなものとしては営業秘密の侵害行為とハッキングが代表的な方法であるとすることができる。

⑶　産業機密（営業秘密）の流出を認知する契機

いずれの企業においても，産業機密が流出されるまで一連の兆候があるが，①他の会社で類似した製品を生産する場合，②共同研究，合弁投資などの意向書を締結した後に本契約を遅延する場合，③製品に対するA/Sなどを理由に技術資料を要求する場合，④注文量や売上高が急に減少した場合，⑤値下げの要求をしたり，取引先を交替しようとする場合，⑥核心的な人材が突然辞職する場合などである。

⑷　産業技術（営業秘密）の保護のための措置

まず，会社の内部統制および関連分野のセキュリティを強化し，第二に，大学内の産業保安と関連した学科の新設を通じ専門家を養成し，資格證取得制度を拡大し専門性を増大し，第三に，発明者に対するインセンティブの提供を積極的に推進して所信をもって働くことができる雰囲気づくりが重要である。

4．おわりに

技術革新が加速され，世界経済はグローバル的な展開様相を見せており，国家間・企業間の国際分業も高度化されている。特に，先端技術産業はその特性上技術競争が激しくなっており，各国は大規模な国策課題の選定やその他の立法を通じて技術保護主義を強化している。先進国は技術移転を避けるとともに，技術の寿命を短くし，次世代技術に急速に移行しなければならない状況に直面し，また，ある場合には技術の産業標準化のために開発を完了した技術を他の企業に移転する場合もある。また交渉力を高めるためにも，私たちが持っている既存の優位要素については，創造的な結合，またはパッケージ化を模索する必要もある。

第３報告については鄭成範先生（大邱サイバー大学）よりコメントを寄せられ，これを契機として活発な議論が行われました。

おわりに

日韓サイバー法学会としては初めての国際的なオンライン開催ということもあり，通信上の問題なども懸念されていたのですが，若干のトラブルはあったものの，終始ネットワークの接続状況は良好でした。本学会のテーマの一つでもありますが，ネットワーク技術の進歩を体感いたしました。

この度の日韓サイバー法学会では技術の進歩に伴う新たな形態の犯罪や，その取締りについてのご報告とそれぞれについての有意義な議論がなされました。世界的なコロナ禍のために対面による学会の開催が困難になる一方で，オンライン方式による学会開催も多数行われるようになってきたものと思われます。コロナ禍は私たちの生活・行動を変えることを余儀なくしている部分もありますが，オンライン方式という新たな形態での交流が浸透することで得られる利益も多々あるかと思われます。コロナ禍にあっても，学術交流を止めることなく継続して行えることを大変に嬉しく思います。

オンラインによる日韓サイバー法学会会場（日本側）