SS 研システム技術分科会 2020 年度会合レポート
DX 時代の、真のデジタル化に向けて　～法律面を含む諸問題の検討～

大阪大学大学院 情報科学研究科
鎌田将吾

サイエンティフィック・システム研究会（SS 研）のシステム技術分科会 2020 年度会合が 2021 年 1 月 20 日にオンラインで開催された。本会合では、3 件の講演とパネルディスカッションが行われ、DX を推進していく上での法律面に関する諸問題について議論がなされた。

教育のデジタル化の法的課題

情報セキュリティ大学院大学 湯淺墾道 氏

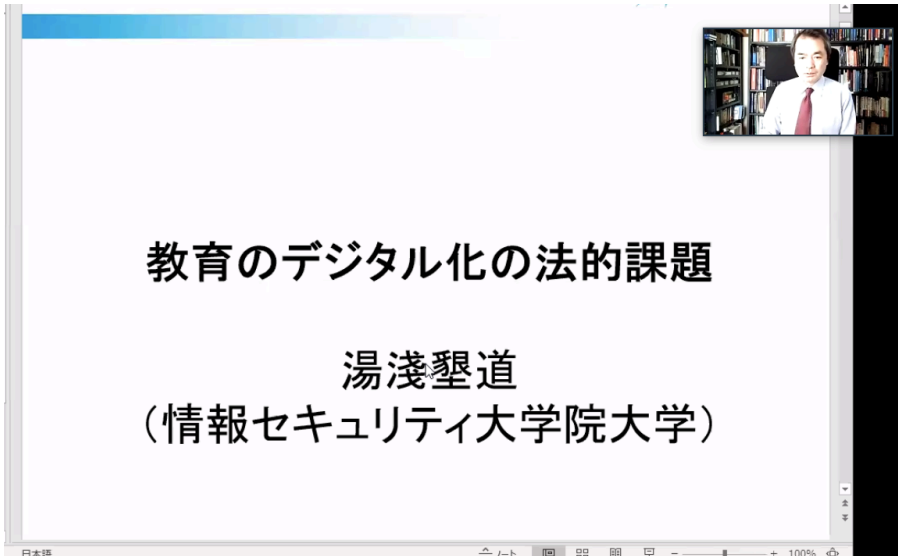
教育のデジタル化を進める上での問題を法律の観点から考えていった。
まず、日本での通信教育の現状が紹介された。 通信制課程の高校や、大学では通信による教育を行うことができるとされている。さらに、大学では 2001 年に大学設置基準が改正され、教室以外での授業が可能になり、オンライン教育が可能になった。

オンライン教育をしていく上で著作権の問題が生じる。著作権法上、学校教育で使うのであれば、先生や生徒は著作権者に断りなく著作物の使用が可能である。しかし、オンライン等の遠隔授業の場合、上述した著作物の断りなき使用に制限がかかる。直接、対面で受講している生徒がいて、それと同時に遠隔で受講している生徒がいる場合は著作物を断りなく遠隔で配信しても問題はない。しかし、遠隔だけの受講者の場合や、対面で実施した授業を後からオンデマンドで配信するような場合には、著作権者の許諾が必要となる。つまり、従来の著作権法が許される遠隔配信は限定的である。こうした背景から、2018 年に改正著作権法が公布された。補償金を SARTRAS という機関に支払えば、著作権者の許諾を得なくても、著作物の遠隔のみでの配信やオンデマンドでの配信ができるようになる。この制度は、2020 年度は特例として補償金額を無料とし、2021 年度から開始予定である。

これにより、オンライン教育における著作権法上の制約が弱くなることが期待されるが、個人情報やプライバシーをどのように保護するかという問題を考えなければならない。GIGA スクールが進んでいく上で、ほとんどの学校が外部リソースを使用することになると考えられる。学校法人が外部リソースに対するユーザ契約者となり、生徒に外部リソースを使わせる場合、生徒の個人情報については誰が責任を負うことになるのかという問題が生じる。これは、生徒の個人情報を業務委託する場合、あるいは外部リソースに対して第三者提供する場合で責任の所在が異なってくる。これらの点が十分に詰めることができないまま、外部リソースの導入が進められているのが現状である。他にも、データの保存期間、感想文や絵のような生徒の製作物に対するプライバシーや、転校にも対応するためのデータポータビリティの問題を考えなければならない。

セキュリティに関するオンライン教育の法的問題が紹介された。セキュリティ人材育成などの授業では、ハンズオンを取り入れた実践形式が多い。その際の授業をオンライン化する場合に問題が生じる。例えば、不正攻撃やマルウェアを実機で扱う授業をオンラインで行なった場合に、不正アクセス禁止法やマルウェアに関する罪に抵触する恐れがある。現状、オンライン教育でこれらを扱っても罪になるのかは不明であり、安心してオンライン授業・教育ができないという問題がある。教育目的であれば問題ないということを明文化すべきである。

また、外部からの攻撃によって、個人情報を漏洩した場合の罪について考えなければならない。情報漏洩が起きた際に、個人情報を扱った事業者がどの程度の義務を果たしていれば、免責となるのか明確な基準がないのが現状である。今後議論していかなければならない。



プロバイダの責任

明治大学 丸橋透 氏

プロバイダが負う責任について、法律の条項や裁判事例を基に考えていった。

導入として、トランプ大統領の SNS 永久追放についての紹介がされた。各 SNS はトランプ大統領のアカウントを停止・削除をしたが、表現の自由についての懸念が残る。SNS 事業者はアップロードされたコンテンツを取捨選択編集すること（content moderation）についての透明性（Transparency）、説明責任（accountability）をきちんと果たすべきである、と The SANTA CLARA PRINCIPLES は提言している。日本では、違法・有害情報対策とプラットフォーム規制についての議論が進んでいる。昨年秋には、総務省が「インターネット上の誹謗中傷への対応に関する政策パッケージ」を公表し、プラットフォームサービスに関する研究会、発信者情報に関する研究会を実施していく方針を出した。対策としては、法規制をとらずに、自主的支援の取り組みの支援と、透明性と説明責任の向上を行なっていく方針であり、The SANTA CLARA PRINCIPLES の提言が想定されている。

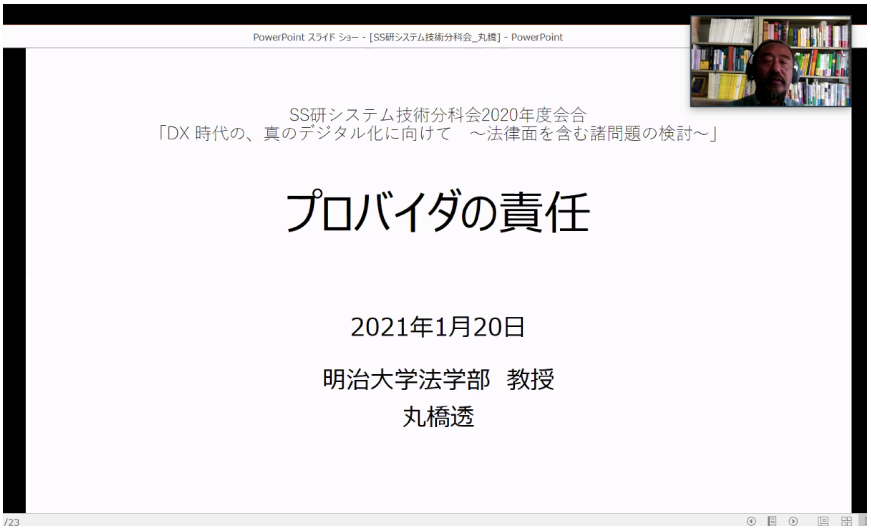
また、誹謗中傷・海賊版対策は自動化により事前抑止すべきか、あるいはそもそも自動化による適正な事前抑止はできるのかを考えていった。総務省が公表した「インターネット上の誹謗中傷への対応の在り方に関する緊急提言」では、今後 AI 技術による誹謗中傷などの情報の削除への期待が記載されている。しかしながら、文脈を理解し適切に削除等が行える AI が本当にできるかがそもそもの問題である。自動的に削除された場合の表現の自由についても議論すべき点である。

SNS 等で誹謗中傷が起きた場合や海賊版がアップロードされた場合のプロバイダの責任について考えていった。SNS 事業者などの HSP（Hosting Service Provider）は、誹謗中傷や海賊版の発信を可能にしたとして責任を負う可能性がある。これは、問題があるコンテンツを削除するなどの実行すべき義務を行わなかった場合に該当する。

HSP の責任についての裁判が二例紹介された。いずれも、教育機関が HSP の立場として関わったものである。一例目は、都立大学事件である。ここでは、ホスティングサービスを提供している大学側（HSP 側）が責任を負うことは適当でないとされた。HSP 側は誹謗中傷に該当する文章が名誉毀損にあたるかどうかについての判断が困難であるため、上記の判決が下された。この判決内容に加えて、例外的事例についても言及され、加害行為の態様が甚だしく悪質なことが明白な場合は責任を負う可能性があるとされた。二例目は、磁気活水器独立当事者参加事件である。誹謗中傷の書き込みをした者が、自身に損害賠償責任債務がないことが認められ、ホスティングサービスをしている大学側（HSP 側）も参加した裁判である。ここでは、書き込み自体には名誉毀損に当たるが、違法性阻却事由があるとされた。

HSP の著作権侵害についても紹介された。HSP が著作権を侵害する者にあたるかどうかというのが問題になり、意見が別れる。

HSP は、コンテンツを削除する際に、不法行為による発信者に対しての責任を負う可能性があると同時に、コンテンツを削除しなかった際には、被害者に対してこれまで紹介してきたような責任を負うことになる。後者が問題になるのは、違法性を認知した時のみであるため、違法情報の削除に消極的になる方がリスクは低いとされる。この問題を解消し、違法情報の蔓延を抑止する必要性から、各国で 2000 年前後にプロバイダ責任に関する立法が行われた。日本でも、プロバイダ責任制限法が成立し、コンテンツを削除しても発信者に対する責任が免責されるようになった。



ブロックチェーンの活用可能性とその法的意義
―今後のための問題点の提示―

西南学院大学　原謙一　氏

ブロックチェーンの活用性可能性を紹介し、活用していく上での法的意義を示した。さらに、それらを踏まえて検討も行った。

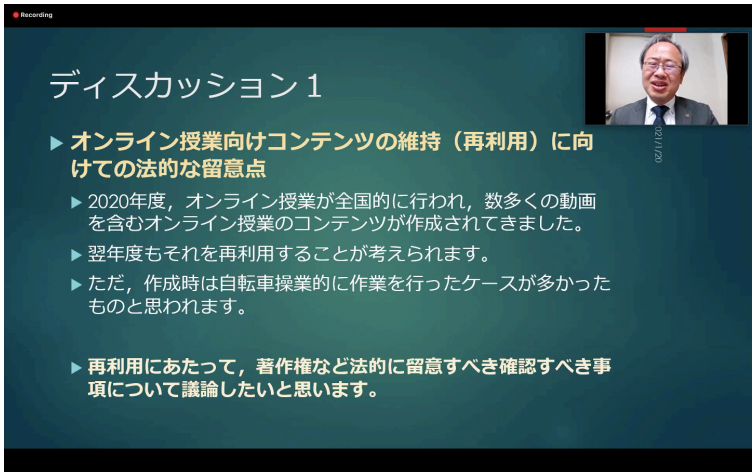
はじめにブロックチェーンの技術紹介がなされた。ブロックチェーンとは、トークンをネットワーク上で取引するための技術である。PC などのウォレットは、トークンの電子データを暗号化し、暗号化されたデータを取引している。この際の取引情報は Peer to Peer を用いて、ネットワークに参加している全員に共有される。取引情報が共有されるのは、正しい取引ができているかどうかを共有された者たちが確認するためである。正しいと確認された取引情報は、いくつかまとめられて1つのブロックにされ、ネットワーク上に記録される。このとき、ブロックにはそれまでの取引情報と最新の取引情報が記録され、各ブロックは連鎖的に繋がった状態になる。ブロックが連鎖的に繋がっている、すなわち、取引情報が全て記録・共有されているため、ある取引情報を改ざんしようとしたら、全てを改ざんしなければならない。つまり、ブロックチェーンは改ざんが事実上不可能な技術であり、これが大きな特徴である。

取引されるトークンに込められた意味として、金銭的価値や支払い目的があげられる。トークンに金銭的価値を見込んで、暗号資産（仮想通貨）が登場した。しかし、暗号資産を用いてお金を支払うという行為は現実的ではなく、金融資産という性質が強くなった。現在では、金銭的価値や支払い目的とは別の使用方法が考えられる。

上述の別の使用方法として、たとえば、①情報の記録の例として不動産登記をブロックチェーンで代替する可能性が紹介された。しかし、すでに日本では不動産登記を電子的に申請・取得が可能であり、これをブロックチェーンで置き換えるメリットは低いことが指摘された。次に、②情報の証明の例として、学生の学習状況や成績を学校間で設けたブロックチェーンで共有して証明することのほか、パートナーシップ（以下、PS）の証明が紹介された。日本では同性婚の法制度は存在しないが、地方自治体レベルで PS 証明書が発行され、各種の手続で証明書として活用されている。ただ、この証明書の発行業務を行っていない自治体居住者は証明書の取得ができないため、特定企業が PS の関係を当事者に確認の上、（前記のとおり改ざんできないものとして存在する）ブロックチェーン上に記録することで、証明書の代替機能を実現しようとする試みが動き出している。これは法的に同性婚を認めるものではなく、そこに法的意義は乏しいとしても、行政サービスを補う現実的意義を有する。さらに、③情報の追跡として、トークン上にのせた情報のやり取りを利用した投票や物の移転情報の確認という例が紹介され、そのほか、④トークン上に不動産の扉を開錠するアクセス権を付与し、借り手と貸し手でやり取りすることによって民泊建物の扉を開閉する電子キーの交付・返却を実現した例も紹介された。③は選挙に④は様々な物の利用権取引に応用可能であり、法的にも現実的にも意義を有する可能性がある。

以上のように、決済以外の領域で拡大するブロックチェーンの活用も、①は検討の意義が薄く、③・④のように法的・現実的意義が存在する領域でまさに法的観点からの検討が必要となるとの評価が述べられた。ただ、実社会においては、法的意義まで存在しなくても、②のように累積する情報がデジタルに収集・記録されていない領

域においてはブロックチェーンを活用する意義があり、今後、この分野で活用がさらに拡大する可能性があると指摘された。ただし、記録された情報が改ざん不可能であることからブロックチェーン上の記録に信頼が寄せられているので、記録した時点で誤った情報であれば虚偽の情報が記録され続ける危険もある。したがって、②の分野の中でも、記録の時点で真偽を正確に確認可能な情報についてのみ、ブロックチェーンを活用すべきであると述べられた。

パネルディスカッション

後援者 3 名にモデレーターとして長崎大学の上繁義史氏を加えパネルディスカッションが行われた。主に「オンライン授業向けのコンテンツの維持に向けての法的な留意点」、「プライバシーバイデザイン時代のプロバイダの責任とは」、「新たな技術（ブロックチェーン等）の導入による課題解決の可能性」、「教育機関が取り組むべきデジタルトランスフォーメーションとは」について議論が行われた。様々な ICT の活用が進んだり、新たな技術が登場すると同時に、現状の法律では適用しづらい問題や、別の新たな問題が次々と出現してくる。そういった問題に対して、どのように対応してデジタル化を進めていく必要があるか意見が交換された。