ISSN 2432-6089

法と情報雑誌

The Law and Information Magazine

第 11 巻第 4 号（通巻第 75 号・2026 年 4 月）

法と情報研究会　編

（第 2 分冊）

本 号 目 次

法情報学Ⅰ講義案（その3）

2026 年 4 月 11 日
元明治大学法学部教授
夏　井　高　人

諸言

私は，明治大学法学部専任教授として採用されて以来，明治大学法学部において 1997 年度から 2025 年度まで法情報学の科目を担当してきた。

2020 年以降は，明治大学法学部 3 年次・4 年次配当の講義科目『法情報学I』及び『法情報学II』を電子板書方式によるオンライン授業（メディア授業）として提供・実施してきた。そのような電子的な講義を提供するために，事前に講義案を準備した。
各授業年度において，前年度の講義案の内容を見直し，誤字・脱字等を補正し，誤解や錯覚等のあった箇所を改めた。また，当該年度において最新の講義内容を提供するために必要な改訂を重ねてきた。

ただし，これまで，『法情報学I』及び『法情報学II』の講義案を一般公開したことはなく，また，オープンデータとして講義案の内容に誰でもアクセスできることを許諾したこともない。

私は，2026 年 3 月末日をもって明治大学を定年退職した。

受講中には『法情報学I』の講義内容を十分に理解することができず不本意な結果に終わってしまった受講生が社会人として独学で法情報学の勉強に再挑戦するための助けとするため，また，後任の教員において私がどのような分量と質の講義を提供していたのかを知る機会を提供するため，そして，この講義案の読者全員に対して法情報学の分野における実験的な講義の記録を資料として提供するため，2025 年度に実施した『法情報学I』の第 1 回～第 14 回（最終回）の講義案を一部修正し，形式と体裁を整えた上で，法と情報雑誌の中で資料として分割公表することにした。

この「法情報学I講義案（その3）」は，2025 年度に実施した『法情報学I』の第 8 回～第 9 回の講義内容を収録している。第 8 回及び第 9 回は，オープンデータとしての法情報がプライバシー情報または個人情報を含む場合における法的問題を理解するための前提となる保護法益としてのプライバシーのとらえかたと関連法令の概要を集中的に説明することを目的とする講義内容となっている。

念のため付言しておくと，この講義案の中で参考サイトの場所として示した URL 等は，講義の準備のために確認した日に存在したものであり，その確認日は，講義案の中で明示してある。
実際に使用した講義案に近いものを記録化して公表するというこの「法情報学I講義案（その3）」の目的に照らし，授業の準備のために実際に確認した日以降のものに関しては，原則として，それらの参考サ

イトが現時点でも存在するかどうか，現時点における URL が同一のものであるかを確認していない。
ただし，現時点では完全に消滅してしまった参考サイトに関しては，その URL 等を講義案の原稿の中から削除した上で，本文を一部修正して対応する扱いとした。

他方，講義案の中で引用・参照している書籍（特に著作権保護期間経過後の書籍）の表題に関しては，出版社や版の相違によって異なっている場合がある。
学術論文であれば，当該書籍や文献資料等がどの版のものであるかを仔細に検討し，版の間の相違を明確に意識して識別することが重要になることがあり得るが，『法情報学I』及び『法情報学II』の講義は，特定の書籍の個別の解説や内容の検討結果等を提供することを目的としていない。
それゆえ，同一の内容の書籍であっても複数の異なる表題をもつ版が存在する場合，厳密さを重視するというよりは，受講生が探して読むために必要な識別子としての書誌情報という観点から選択した表題を示すことにした。

そして，講義の中で参照・引用した法令の条項等は，当該の回の講義を準備する際には条項の内容等を確認したけれども，その後の法令の改廃等を全く反映していない。
それゆえ，観念的には，現時点では日本国内において有効に施行されていない法令の条項が含まれていることがあり得る。

加えて，実際の講義においては，分量の関係から，参考資料やレジュメ等の名称の別文書として（受講生の予習のために）事前に提供し，実際のオンライン講義（メディア授業）では，事前提供した参考資料等の内容を重複して提供することなく，事前提供した参考資料等の該当箇所等を参照しながら講義を実施した。そのような事前提供資料の中には，私の個人ブログである「Cyberlaw ブログ」及び「怠け者の散歩道2」の個々の記事の中で示した私見や参考資料等も含まれる。
しかし，この「法情報学I講義案（その3）」では，当該回の講義案の内容と参考資料等の内容を統合した内容のものとして一体化して編集してある。
それゆえ，実際に実施された講義においては，受講生は，この「法情報学I講義案（その3）」に講義案として収録した分量の講義内容全部について，当該回の講義時間内に提供を受けたというわけではない。

なお，この「法情報学I講義案（その3）」のための原稿の校正に際し，唐亀侑久氏及び須藤美有氏の助力を得た。各氏の助力に心から感謝する。

＊＊＊

－目 次－

法情報学Ⅰ第8回講義案
プライバシー保護との関係（1）

(2025 年 6 月 9 日開講)

明治大学法学部教授
夏 井 高 人

1 総説

1．1 プライバシーの概念を正確に定義すべき必要性

「プライバシー（privacy）」という語は，一般用語としてもしばしば用いられます。しかし，世間話としての「プライバシー」の文脈においては，法的には無意味なことまたは無力なことが含まれることが珍しくありません。
そのような場合，その会話において使用されている「プライバシー」という語の概念定義及び適用範囲が明確に示されないのが普通です。そのような場合，各人各様に恣意的に理解された意味・内容をもつ「プライバシー」なるものが存在することになります。

しかしながら，適用可能な法令及び法制度によって保護されるべき利益（保護法益）として裁判所が判断可能な範囲内にあるものでなければ，法的に保護されるプライバシーではありません。

他方において，大学法学部において専門教育を受ける場合においても，「プライバシー」に関し，簡単な定義のような文言を暗記するだけでは全く役に立たないだけではなく，逆にかなり大きな弊害があります。

プライバシーと関連する法理論や判例法はかなり多数あり，相互に異なった内容または矛盾する内容となっていることがあるので，それらの中の主要なものを理解し，検討し，それらの関連法理論や判例法を（「プライバシー」の正しい意味内容と用法を理解するための手段として）使いこなせるようになるべきです。

1．2 古典的なプライバシー概念

「privacy」という英語は，直訳すると，「私事であること」というようなことを示す一般用語化しています。
法学の文脈における「privacy」との語の本格的な使用は，元は，アメリカ合衆国のウォーレン（Samuel Warren）とブランダイス（Louis Brandeis）が 1890 年に Harvard Law Review で公表した「The Right to privacy」を最初とすると一般に理解されています（伊藤正己『プライバシーの権利』（岩波書店，1963）参照）。

ウォーレンとブランダイスが主唱する「プライバシーの権利」は，原語としては，「right to privacy」なのであって，「privacy right」ではない点が重要です。
この微妙なレベルの相違に着眼することは，プライバシーという語が一般化し，その概念内容が拡散してしまった今日であるからこそ，逆に重要なことです。

法学の領域では，各人が自由に考え，素人の間での会話で話題にする「プライバシー」を検討対象にはしません。

> 法律家ではない一般人が「プライバシー」を話題にすることは完全に自由（思想信条の自由・言論の自由の範囲内）です。しかし，俗に「プライバシー」と呼ばれている対象または現象の全てが法的概念としての「プライバシー」と一致しているとは限りませんし，また，その全てが法的に保護されるわけでもありません。
> 法学部の学生は，一般用語としての「プライバシー」という語の俗用をひとまず忘れ，その法学上の概念の正しい理解に努めなければなりません。その点が単なる雑談やジャーナリズムと学術及び法律実務との大きな相違点です。

法学の世界においては，法律要件と法律効果が安定的に解釈可能な範囲内で，法的に保護される利益としての「プライバシー」を問題にします。

一般に，法概念としての「プライバシー」と関連する法理論や判例法は，かなり多数あります。
それらの法理論や判例法中で，法学上の概念としての「プライバシー」の意義を正確に理解するためには，(1)プロッサー（W. Prosser）の 4 類型の理論と(2)米国判例法上の「プライバシーの合理的な期待（Reasonable expectation of privacy）」の理論・判例法を知り，理解することが必須となっています。

1．3 プライバシーの概念に関するプロッサーの4類型

ウォーレンとブランダイスの見解が主流となった時代において，「プライバシー」は，簡単に言えば，「ひとりにしておかれること（"to be let alone"）」を意味するものとして理解されていました。
俗な表現で言い換えると，「構わないでくれ（Leave me alone, Don't mind）」とか「干渉しないでくれ（Don't interfere）」などに近いものです。

不法行為法（tort law）を専攻する法学者プロッサー（Prosser, William L.）は，1960 年，California Law Review vol.48, issue 3, pp.383-423 に「Privacy」と題する論文を公表しました。

> Prosser, William L., Privacy
> https://lawcat.berkeley.edu/record/1109651?v=pdf
> [2025 年 6 月 8 日確認]

プロッサーは，この論文の中で，「Without any attempt to exact definition」とことわりつつ，過去の関連判例の帰納法的な検討と考察を基礎として，不法行為訴訟における原告が 4 つの異なる類型の主張を同じ「privacy」の利益の侵害として主張しているという事実を明らかにしました。
プロッサーが明確化した 4 類型は，以下のとおりです。

1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.
2. Public disclosure of embarrassing private facts about the plaintiff.
3. Publicity which places the plaintiff in a false light in the public eye.
4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness.

プロッサーの 4 つの類型に関して，日本語で書かれた解説を含む代表的な書籍としては，堀部政男『プライバシーと高度情報化社会』(岩波新書，1988)，新保史生『プライバシーの権利の生成と展開』(成文堂，2001)があります。

日本国の憲法学においては，これまでのところ，プロッサーの 4 類型の中で第 1 の類型と第 2 の類型のものを「プライバシー」として理解する傾向が強いのに対し，第 3 の類型と第 4 の類型はあまり重視されてきませんでした。

しかしながら，インターネットを介して行われる常時監視が極めて強化されている今日であるからこそ，「right to privacy」の現在的な意味を再検討しなければならないという事態に直面していることを明確に認識する必要があります。
そして，そのための考察において，プロッサーの 4 類型の中でも特に第 3 の類型と第 4 の類型は依然として大きな意味をもち続けていると考えられます。
特に，第 3 の類型は，SNS 上の炎上の原因となる要素として重要であり，名誉棄損行為や侮辱行為を含め，人格侵害行為の中核部分を構成することがあります。
第 4 の類型は，著作権法違反行為の本質と密接に関連する部分を含みます。また，不正競争行為や業務妨害行為を構成し得る要素ももちます。これらの諸点は，SNS や生成 AI の利用と関係して生じている現代的な諸問題を理解する上でも重要になることがあります。

これらの諸要素は，4 つの孤立した類型要素の集合として存在し得るものです。しかし，それらの類型要素が常に分断的に存在していると理解するのではなく，複合的な侵害行為の類型としても存在し得るということを理解することが重要です。
あるプライバシー侵害行為が複合的な法益侵害となり得ることについて，プロッサーは，その論文の中で，「What has emerged from the decisions is no simple matter. It is not one tort, but a complex of four」と表現しています。

プロッサーの研究成果は，米国のプライバシー侵害と関係する訴訟において大きな役割を果たしてきましたし，現在でも大きな影響力をもっていると考えられます。

米国のリステイトメントに基づく不法行為法(torts law)の統一モデル法(uniform model codes)は，プ

ロッサーの 4 類型の理論を踏まえて構築されています。

それゆえ，米国の制定法(州法レベルの実定法)としての不法行為法の一部としてのプライバシー保護法の重要部分を理解するためには，プロッサーの理論を知ることが必須となります。

> 一般に，日本国の法体系全体の中における位置づけとしては，プライバシー保護と関連する法体系は，基本的には民法(不法行為法)の一部であり，憲法はその法哲学上の根拠の 1 つを与えているのに過ぎません。
> プライバシーの利益に対する侵害行為があっても，日本国憲法を法的根拠とすることだけでは，日本国の裁判所においていかなる種類の損害賠償請求訴訟も提起できず，いかなる種類の差止請求訴訟も提起できないので，完全に無力です。そのため，プライバシー侵害と関連する紛争の裁判所における解決を考える限り，憲法学を学ぶだけでは全く無力です。
>
> プライバシーの民事上の保護と関連する法解釈は，基本的に，全て民法(財産法)の法解釈学の一部です。実体法上の権利としてのプライバシーの保護を求めるための損害賠償請求訴訟に適用される基本法令は，民事訴訟法です。
>
> そのような民法上の法解釈が正しく行われることを必須の前提として，民法第 709 条に基づき，プライバシー侵害による損害の賠償を求める民事訴訟が提起され，民事訴訟法に定める訴訟手続に従って裁判所によって審理され，原告勝訴の判決が確定すると，その判決を基礎として，民事執行法に従った強制執行が実施されます。

プロッサーの理論は，そのような意味での民法の法解釈の中で，講学上の不法行為の類型概念として参照され，考察され，法解釈の助けとして利用されます。

プライバシー侵害訴訟は，このような一般的な民事上の権利のライフサイクルの中でその一部として理解されるべきです。

そして，事案類型の相違に即した過去の関連民事裁判例の帰納法を基礎とする調査・分析・検討とその結果の応用の積み重ねを継続することが非常に重要になります。

1．4 「プライバシーの合理的な期待」の概念

米国の判例法(case law)においては，「プライバシーの合理的な期待」の理論が現在でもなお維持されています。

一般に，米国の判例法及び法理論においては，プライバシーの客観的かつ適法かつ合理的な期待(objective, legitimate, reasonable expectation of privacy)が侵害されたときにプライバシー侵害があると理解されています。

米国のプライバシー保護関連の制定法（連邦法及び州法）や米国連邦政府の関連政策文書等の中にも同一の文言が多々見られます。

それゆえ，「プライバシーの合理的な期待」の理論の内容を知らないことには，プライバシー保護と関連する米国の制定法，判例法及び政策文書の内容を正しく読解することができません。
それだけではなく，「プライバシーの合理的な期待」の理論は，日本国におけるプライバシー侵害関連の損害賠償請求訴訟等においても裁判所の判断の根底を形成していると解されます。
その結果として，「プライバシーの合理的な期待」の理論を知らなければ，プライバシーとして法的な保護を受けることのできる客観的な期待が認められる事柄の範囲を知ることができません。

ところで，プライバシーの「期待（expectation）」は，裁判官等の判定者の視点から見て，「期待すること」が合理的か否かを評価した判断結果のようなものです。
換言すると，その「期待」が裁判所において認められるということは，個々具体的な個人（自然人）にとって現実に期待できたかどうかが審議されるということを意味するのではなく，「当該事案における社会環境及び状況の下において当のプライバシーが保護されていると期待できると判断（評価）できる」ということが証拠によって証明されているということを意味します。厳密には，事実（Sein）として保護されていると認定するというのではなく，当為（Sollen）として保護されるべきであると価値判断できるということを意味しています。
このような論理構造は，不法行為（民法第 709 条）に基づく損害賠償請求訴訟において「期待可能性」が重要な要素となる場合には，通有するものです。

裁判官がそのように判断し，その判断に従って裁判をする権限をもつことは，日本国憲法によって定められていることです。裁判官ではない一般国民にはそのような（国家法上の）権限がありません。そして，評価結果としての「期待」は，一般用語としての「期待」という語のもつニュアンスとは大きく異なるものであり，基本的に，当該本人の主観的な期待や欲望とは無関係のものだということを理解してください。

私人が各人各様に自己流に解釈した概念内容としての主観的なプライバシーの期待（subjective expectation of privacy）が存在し得ますし，そのことそれ自体としては，各人の思想・信条の自由及び学問の自由の範囲内です。
しかし，そのような私人の主観的な思考結果としての個別の期待が破られたとしても，必ずしも「プライバシーの客観的かつ適法かつ合理的な期待」の侵害があると判断されるわけではないという当たり前のことを理解することが重要です。

> 法学上の概念の中で，「期待」の評価が問題となる別の例として「期待可能性」の概念があります。
>
> 期待可能性とは，「本人が現実に何らかの行動をとろうとしたか否か」という意味をもつのではなく，裁判官等の評価者の視点から見て，当該本人に対し，当該環境条件の下において，「ある行動をとることができた可能性の有無」の判断を強制できるという意味をもっています。つまり，ここでもまた，一般用語としての「期待」とは相当に異なる意味をもっています。

一般に，大学や企業を含め，民間組織内においては，当該民間組織上の判断権限をもつ者（経営陣，組織内の部や課の長など）が存在します。その民間組織上の権限に基づく判断に誤りがあるときは，民事訴訟等により当該民間組織上の判断の是正や損害賠償を請求することが可能ですが，その請求が必ず認容または棄却されるわけではありません。そのような請求があった場合，やはり，最終的には裁判官の判断が強制されます。公務員の職場である官庁，公務所等の組織でも基本的には同じです。

一般に，大学法学部の学生は，一般用語としての用例に習熟していることは無論のこととした上で，法学上の概念を正しく認識・理解し，法解釈における用例を正確に習得しなければなりません。

ここに，「プライバシーの期待」の理解をめぐって，個人の主観的意識と客観的な法規範との間のギャップが存在し得ます。

例えば，ある人が，自分の識別番号，顔写真，氏名等を記載した従業者身分証明カードを首からぶら下げたまま公道を歩いているという状況において，その公道を往来する人々は，そのカードを目にすることができます。
この例のような場合において，仮にその顔写真や氏名等の符号が一般的にはプライバシーの一部を構成するとしても，その者自身がそのような状態を招来しており，自らの意思でそれらの画像や符号を世間の目に晒しているのである以上，それらの画像や符号を「知られたくない」という欲望が社会によって是認されることはなく，「見るな！」と大声で叫んでみても無意味であり，そのような主張が法によって守られることもありません。故意による場合ではなく過失による場合であっても，自招危難またはほぼ 100%の過失相殺として扱われることになるでしょう。

同様のことは，インターネット上でも起きます。
例えば，自分の意思で SNS サイトに登録し，自己に関する情報の一部を公表している場合，既に公表されている情報，あるいは，公開されている情報から容易に推知可能な情報に関しては，自らが公開したものとなるので，「そのような情報もプライバシーの一部として保護されるべきだ」という欲望が是認されることはありません。

他方において，「プライバシー」は，「営業秘密」の場合と同様，本人が秘密のものとして保護する措置を講じている場合でなければ，法的に保護されるべき理由がないと言わざるを得ません。

現実には，ここで述べているようなことに全く納得できない個人が存在することでしょう。場合によっては，そのような個人の態度をめぐり議論が沸騰することがあります。
例えば，SNS サイト上において，納得しない本人に対し，「自業自得だろ！」のような批判が殺到し，炎上してしまうようなタイプのトラブル事例がその典型例です。
そのような炎上が生じてしまう一般的な原因を分析してみると，結局，①当該本人が自分自身を客観視していなかったこと，または，②当該本人が自分自身を客観視する能力をもたないこと，または，③当該本人が自己の意見に客観性をもたせることができなかったこと，または，④当該本人が自己の意見に客観性があるか否かを検討しもしくは自己評価するというプロセスを経ていなかったこと，または，⑤これらに類する事由が存在したことなどにそもそもの原因があると言えるかもしれません。

そして，プライバシーの客観的な期待は，それが「客観的」と表現されているとは言っても，何か絶対値のようなものが存在するわけではなく，相対的かつ関係的なものです。
それは，環境要素（environmental elements）や状況要素（situational elements）を基礎とするものであり，それらの要素の変動によって，客観的な期待の内容及び程度も変化します。

> 日本国の裁判所の判決理由の中で「諸般の事情に鑑み」またはこれに類する表現が用いられる場合，ここで説明するような意味での環境要素や状況要素を総合評価したという趣旨を示す場合があります。

例えば，何も問題が生じていない平時であれば，国際空港における検問は極めて機械的で簡単なものかもしれません。

> 何も問題のない状況の下において，他に特別の必要性もないのに，検問の担当官が事細かに旅先の状況や交友関係等を質問することは，プライバシーの客観的かつ適法かつ合理的な期待を裏切る行為となり得ます。職場において，他に特別の必要性もないのに，上司がそのような詳細な質問をした場合，パワーハラスメントの一種として違法行為を構成することもあり得ます。

しかし，環境要素が大きく変化し，例えば，新型コロナ等の疫病が流行しているような特別の状況の下においては，プライバシーの客観的かつ適法かつ合理的な期待の基礎となる環境要素や状況要素が大きく変化し，体温検査だけではなくより精密な生化学検査等が強制的に実施され，あるいは，旅行先における接触者の有無等が細かく質問されることにもなります。
更に，戦時や国際的な紛争時においては，スパイ（工作員）及びテロリストの侵入の防止や国防上の機密の漏洩の防止の目的のために，飛行場等における検問における点検事項が更に強化されます。
最も極端な状況下においては，プライバシーの客観的かつ適法かつ合理的な期待をもつことが全くできないような事態となることもあります。

これらの場合と同様に，一般に，警察目的または情報セキュリティの目的のために，プライバシーの客観的かつ適法かつ合理的な期待が大きく縮減される場合があります。

電子的な環境における環境要素の変化としては，例えば，SNS が存在しなかった時代と SNS が一般的に利用されるようになった時代とでは，人々の考え方が変化しました。

当初においては，SNS における匿名性が守られると信じた利用者が多く，また，警察の能力では誹謗中傷行為等の加害者を特定して逮捕することは無理だと考える人々が少なくありませんでした。
しかし，SNS をめぐる状況は変化し続けています。

> 世界的なレベルでは，SNS のようなプラットフォーム上において誹謗中傷や偽情報の流布が行われた場合における当該プラットフォーム事業者の法的責任を明確化し，行政指導，制裁金や罰則の適用を強化する立法が次第に増えています。

その結果として，X（旧 Twitter）や Meta（旧 Facebook）のような SNS の運営者が「表現の自由」だけを口実にして何もせずに逃げ回るということができにくくなりつつあることは事実だと思われます。

これらの SNS を運営する事業者の多くは，やるべきことを何もしないで「手抜き」状態にしたままで，収益の増大または極大化だけを正当とするビジネスモデルを採用しているので，今後も「プライバシー保護」のために尽力するようになるとは考えにくいと言わざるを得ません。しかし，何もしないでいると行政指導を受けまたは処罰される時代へと変化しつつあることは事実だと思われます。

そのような環境要素や状況要素の変化は，無論，「プライバシーの合理的な期待」の対象，内容及び範囲に関しても微妙に影響を与え続けています。

より正確には，SNS 等のインターネット上のサービスの利用者の側における主観的願望という意味での「プライバシーの合理的な期待」が合理的なものであると判断される範囲を変化させ続けており，また，判断者である裁判官の側における知識・認識・理解も変化し続けているということは言えます。

伝統的な判例法解釈の手法だけでは対処できないような速度と微妙さをもった変化なので，今後，この分野における関連情報の収集及び分析のための手法やツールがどんどん開発される必要性があります。また，そのような帰納法を基礎とする分析や考察は，今後の裁判運営や立法活動のために大きく寄与することだろうと考えられます。

そして，これらのいずれの環境要素や状況要素が変化した後の時点においては，プライバシーの客観的かつ適法かつ合理的な期待を評価する前提としての，保護法益としてのプライバシーの保護の必要性と，プライバシーの客観的かつ適法かつ合理的な期待の縮減を求める別の保護法益との間の利益衡量を改めて検討することが必要となります。

そのような比較衡量を行う場合においても比例原則（proportionality）が適用されると解するのが普通ですし，日本国の裁判例においても明示または黙示に比例原則が考慮されています。
ただし，日本国の裁判例においては，「比例原則」または「比例性」の原則の別名として「相当性」が用いられることが少なくありません。

日本国の行政上の政策判断等の中でも比例原則が考慮されているか否かに関しては，個々の事案の特質に応じた慎重な検討を要します。

1.5 まとめ

法的概念としてのプライバシーとその適用範囲（scope）とは，結局のところ，プライバシー保護の合理的な期待が社会的に是認される範囲のことを意味することになります。

裁判所は，そのようにして社会的に是認される範囲内で，法的保護を与える必要性の有無を判定します。そのような判定は，事案類型と文脈及び TPO を勘案して行われるので，数学における線形的な定義のようなものが成立しているわけではありません。

民事訴訟実務においては，常に，数学上の多変量解析のような思考が求められ，そのようなタイプの思考を可能とするだけの十分な思考・判断の能力をもっていないと裁判官の職を遂行できません。

それゆえ，法的概念としての「プライバシー」に関しては，簡単な定義を暗記するだけでは全く足りず，様々な裁判事例とその類型の整理を通じて，よく整理された事案類型毎の適用範囲の相違と特徴を理解することが大事です。

他方において，通常の民法の法解釈学を離れ，法社会学的な見地にたってみても，プロッサーの理論は，情報ネットワークシステムを社会基盤とする情報社会（information society）またはデータ駆動型経済（data driven economy）におけるプライバシーというものの本質を理解する上でも非常に重要な手掛かりを提供するものです。

この講義では，プロッサーの 4 類型理論を説明した上で，私がプロッサーの 4 類型を仔細に検討した上で提案している一部修正理論について説明します。

2　プロッサーの理論

2.1　プロッサーの 4 類型

(A) プロッサーの第 1 類型

プロッサーの第 1 類型は，(1)「seclusion」への「intrusion」，もしくは，(2)「solitude」への「intrusion」，または，「private affairs」への「intrusion」のいずれかに該当する場合を指し，これらの態様の行為がプライバシーという保護法益を侵害する行為としてとらえられています。

「seclusion」は，「離れていること」を意味します。

> 他人との接触を避けて暮らすことは，それ自体としては，各人の自由の範囲内にあります。ただし，納税の義務や（徴兵制のある国では）兵役の義務等の国法上の義務があるので，現実には完全な「seclusion」を実現することは不可能なことです。
> そのように「seclusion」の状態にある者を何らかの態様により無理やり社会の中にひっぱりこもうとすることは，「seclusion」に対する干渉となるかもしれません。
> そのような場合，当該個人の「人間の尊厳」を損なうという形式で議論されることもあるかもしれませんが，「人間の尊厳」は，価値判断の結果であって事実そのものではないので，事実としての行為類型としては，

「seclusion」に対する「intrusion」を考えることになります。

「solitude」は，「孤独でいること」を意味します。

一般に，都会の中に住んでいても他人との交渉・接触を可能な限り避け，孤立して生きることは，各人の自由の範囲内にあります。
ただし，納税の義務等の国法上の義務や当該居住地域における条例や慣行上の義務その他の義務があるので，現実には完全な「solitude」を実現することは不可能なことです。

「private affairs」は，一般に，「私事」と訳されています。

「affairs」は，静的または動的な出来事（events）を意味する場合には「私事」で良いものの，ある「場所（location）」または「空間（space）」を意味する場合には「私事」ではなく「私的空間」とするのが妥当なので，本当はなかなか面倒な概念です。

その意味を正しく理解した上で「私事」と訳している例では，実際には狭い意味での「私事」と「私的空間」を併せた意味で「私事」という語を用いています。
そのため，そのように訳している例では，その訳文を正確に読解するためには，（「私事」の日本語の一般的な用例としてではなく）日本語の特殊な用例であるとの認識・理解が必須となります。このこともまた，この授業の中で重視している「読む」ということの一例です。

前者の「private affairs」（狭義の私事）の例としては，（婚姻・離婚・その他の交際等を含め）個人の私的な行動だけではなく，個人の嗜癖や性格傾向等を含むことがあります。

正当な理由なく，無権限で，私事（private affairs）に接触する行為は，「intrusion」に該当し得ます。それらの事柄を本人から強引に聞きだそうとする行為や，本人を騙して聞きだそうとする行為もまた，「intrusion」となります。

「私的空間」という意味での「private affairs」の例としては，例えば，個人の居宅や居室をあげることができます。

一般に，「private affairs」（私的空間）に対する「intrusion」として評価される行為は，民事上の損害賠償等の問題を生じさせ得るだけではなく，刑法上の住居侵入罪や不退去罪のような犯罪行為をも成立させ得ます。

一般に，特定の空間に対する侵害行為は，事案により，社会的法益（治安の阻害）や国家的法益（国防の阻害）を構成することもあります。
しかし，これらの社会法益及び国家法益の侵害行為は，私的利益としてのプライバシー侵害とは異なる保護法益の侵害行為として理解されます。

プロッサーの第 1 の類型における「intrusion」は，それだけでは概念内容（意味）を確定することが必ずしも容易ではないことがしばしばあります。

そのような場合，プロッサーの他の類型（第 2，第 3 及び第 4 の類型）の特徴と比較・検討し，意味内容として重複しないように合理的な理解を試みると，適正な法解釈・概念理解が可能となります。

> 以上のような検討を踏まえた上で，第 2 類型が私事の暴露（外部への公開）を内容とする類型であり，第 3 類型及び第 4 類型が外部に表示された外形的要素を必須の構成要素としていることから，第 1 の類型における「intrusion」を「侵入」もしくは「干渉」またはこれに類するものとして理解するのが妥当です。
>
> このように解する場合における「侵入」とは「無権限アクセス（unauthorized access）」と同値です。
> そして，「権限のある場合」とは，一般的な違法性阻却事由と同様，(1)本人の同意（consent または permission）がある場合，(2)裁判所（裁判官）の発する捜査令状や執行命令等に基づく場合，(3)現行犯逮捕の現場における捜索・身体検査のような正当な警察活動の範囲内にある場合，(4)緊急避難の場合，(5)正当防衛の場合，(6)公衆衛生上（疫病流行の防止等）の重要な公共の利益のために必要な場合などを考えることができます。
>
> これら「intrusion」との関係で成立し得る違法性阻却事由それぞれについて比例原則（proportionality）が適用されます。
> それゆえ，例えば，正当防衛や緊急避難の場合であっても，手段や程度の相当性の範囲内が比例する範囲内では適法行為とされます。
>
> そのような比例原則（proportionality）に適う範囲内にある場合に限るということを必須の前提とした上で，違法性阻却が認められるものとして適法行為と評価される場合，あるいは，正当行為として適法行為と評価される場合においては，仮に外形的・形式的には「seclusion」もしくは，「solitude」を損なう行為または「private affairs」に接触する行為であっても，その行為は，第 1 類型の「intrusion」ではなく，権限に基づくアクセスとなります。

EU の一般データ保護規則(EU) 2016/679（GDPR）の中にもプロッサーの第 1 類型の重要な要素である「private affairs」の概念と密接に関連する条項があります。

例えば，GDPR の第 9 条第 1 項は，特別類型のデータの処理を禁止しています。この特別類型のデータは，「機微のデータ（sensitive data）」または「機微の情報（sensitive information）」と呼ばれ，特別に厳格な法的保護の下に置かれています。

> この特別類型のデータの中には，人種上または民族上の出自（racial or ethnic origin），政治的意見（political opinions），信教または思想上の信条（religious or philosophical beliefs），労働組合への加入（trade union membership）を明らかにするデータ，遺伝子データ（genetic data）や生化学データ（biometric data）などのほか，個人の「性生活または性的指向（sex life or sexual orientation）」を明らかにするデータも含まれ

> ています。特段の正当事由や違法性阻却事由がないのに，これらのデータをデータ処理することは，違法行為となる可能性があります。

そして，EU の GDPR では，このような重要な個人データ（機微の個人データ）の類型に属するデータまたは情報は，プライバシーの一種としても理解されています。性別に関するデータや私生活上の性的行為に関するデータも同様です。

> 国際的な環境においては通常の日本人の感覚とはかなり異なるタイプの思考や感受性が無数に存在しているので，意図しない心理的衝突を避けるため，これらの機微のデータまたは機微の情報（特に性や性生活と関連する情報）を話題にすることを極力避けるようにすることが賢明です。
> なお，これらの機微のデータまたは機微の情報と関連する話題は，国によっては，ヘイトスピーチとして処罰されることがあるので，注意を要します。

日本国の個人情報保護法においても，「機微のデータ（sensitive data）」または「機微の情報（sensitive information）」は，「要配慮個人情報」として特に厳重に保護されています。

個人情報保護法第 2 条第 3 項は，「要配慮個人情報」に関し，「本人の人種，信条，社会的身分，病歴，犯罪の経歴，犯罪により害を被った事実その他本人に対する不当な差別，偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報をいう」と定義しています。

(B) プロッサーの第 2 類型

第 2 の類型は，「embarrassing private facts」の「public disclosure」です。
一般用語としては，「embarrassing」は，「恥ずかしい」等という意味があるので，そのままだと「embarrassing private facts」は，「恥ずかしい私的な事実」となりそうです。
しかし，第 2 類型でいう「embarrassing」とは，本人が「恥ずかしい」と感じているどうかという点に重点があるのではなく，本人が「秘匿しておきたい」と思っていることから，それが暴露されると本人が「恥ずかしい」と感じることを含め，「秘匿の期待が裏切られて心外だという気持ちになる」という程度の意味をもつ語として理解するのが妥当です。
その結果として，本人が秘匿したいと思っていない事実が公開されたとしても，形式的には第 2 類型のプライバシーの利益が侵害されたことにはなりません。

第 2 類型に関しては，米国や欧州だけではなく，日本国内においても，芸能人の不倫等を内容とする雑誌ゴシップ記事やテレビのバラエティ番組における暴露，SNS における暴露的攻撃言動等を含め，かなり多数の事例があります。

第 2 類型は，プライバシー侵害の典型例として理解されることが多く，ウォーレンとブランダイスによる米国連邦裁判所の裁判事例を類型化するという試みの中でも特に重視されていると言えます。ここでは，報道の自由との関係（調整）が特に問題となり得ます。

日本国の裁判事例としては，非常に有名な宴のあと事件昭和 39 年 9 月 28 日東京地裁判決・判例時報 385 号 12 頁の事例及び石に泳ぐ魚事件最高裁平成 14 年 9 月 24 日・裁判集民事 207 号 243 頁もそのような事例に入るかもしれません。
ただし，この裁判事例は，本質的には，第 2 類型と第 3 類型の両方に属する事案だと考えるのが妥当です。なお，ここでは，表現の自由との関係（調整）が問題となり得ます。

この問題は，一般に，私人の秘事の暴露を伴うモデル小説やモデルドラマ等では常に議論の対象となり得ます。
社会的なトラブルの発生を完全に避けたいと思うのであれば，実在の人物を素材として小説やシナリオ等を書くことを再検討すべきでしょう。理想的には，（モデルなしに）完全に創作の作品を書くことのできる能力をもつべきです。

現在のインターネット環境において，SNS 上における無軌道な言動の横行によって，プロッサーの第 2 類型に属するプライバシーの利益の侵害がかなり多数みられます。そのことから，プロッサーの第 2 類型は，サイバー法の観点からも大きな重要性をもつ類型だと言えます。

なお，SNS 上の炎上事例の中には，損害賠償請求等によっては回復できない深刻なダメージを生じさせるようなものがあり得ます。
そのような非常に悪質な事案に関しては，刑法に定める名誉棄損罪だけではなく，強要罪，脅迫罪または業務妨害罪等の関連犯罪の成否についても真剣に検討されるべきでしょう。

やじうまのようにして SNS 上の炎上に加担する言動を加えた人々は，刑法上では強要罪，脅迫罪，侮辱等の共同正犯に該当し，民事上では直接の加害者と共に共同不法行為者に該当し得ます。

(C) プロッサーの第 3 の類型と第 4 の類型

プロッサーの第 3 の類型と第 4 の類型は，一般に，プライバシーとは関係のない類型とする見解が比較的多いように思われます。

例えば，第 3 類型は，名誉棄損の問題の中に解消されるとする見解が多く，第 4 類型は，（一般的には商業的利益が存在する場合に限定される）パブリシティの権利の問題の中に解消されるという見解が多いというのが現状です。

しかし，そのように商業的利益が存在する場合に限定して狭く解する見解は妥当ではありません。

一般に，知的財産権の分野で限定されているパブリシティの権利と関連する法理論を民法解釈学の分野における類似の法的検討課題に対してそのまま無修正で応用または適用することは，愚鈍なことだと言えます。

特に，SNS 上の様々なトラブルをプライバシーの問題の一種としても考察してみようとする場合を

含め，様々な特殊問題を解析する上でかなり大きな重要性をもつ類型です。

> 例えば，LINE や X（旧 Twitter）等の SNS 上での「前科事実の公表」というような類型の事案（例：東京高裁令和 1 年(ネ)第 4733 号投稿記事削除請求控訴事件 2020 年 6 月 29 日判決）を考えてみます。
>
> そのような投稿行為が名誉棄損行為に該当せず，また，プロッサーの第 2 類型のプライバシーに該当しない場合を想定した上で，かつ，当の前科者が真に反省し，生まれ変わったようになっていた場合においては，LINE や X（旧 Twitter）等の SNS 上での「前科事実の公表」が，そのような改悛の事実を隠蔽または打ち消すのと同じ効果をもち，「現時点においても過去の犯罪行為実行時と全く同じ人格のままだ」との誤った印象を社会内に流布することになり得ます。
> その結果，当の前科者の社会復帰を深刻に妨げる効果をもつことは事実です。それと同時に，そのような誤った印象を与えることによって，当該の者の現時点における社会的評価に対して新たな深刻な違法行為を発生させていることにもなります。
>
> 加えて，前科者に対するいわれのない差別行為及びヘイトスピーチ（hate speech）を助長することにもなり得ます。
> そのことから，このような事案をプロッサーの第 3 類型のプライバシーの発展形のようなものとしてとらえることは可能です。
> 無論，原告の保護法益として，プライバシーの利益とは全く別に，「前科者が社会復帰する法的利益」のようなものを考えることも可能です。

ただし，プロッサーの第 3 の類型と第 4 の類型に関しては，民法（財産法）と知的財産法の内容を十分に習得した者でないと理解し難く，混乱するおそれがあるという点については，十分に留意しなければなりません。

2．2 プロッサーの 4 類型の再整理

プロッサーが活躍した時代から既に何十年も経っています。その間に，人々が現実に生きている社会環境も人々の感受性も大きく変化しました。

プロッサーの 4 つの類型の内容（侵害される保護法益の実質・態様）に即して，かつ，現代のサイバー空間の存在を踏まえて整理してみると，プロッサーの 4 類型中の第 1 の類型を更に 2 つに分け，侵入タイプの行為類型と知得タイプの行為類型とに分けて考える必要性があるということが分ります。

以下のようになります。

1-1：プライバシー領域への侵入
1-2：プライバシー情報の知得

2:プライバシー情報の第三者に対する開示(漏示・漏洩の一種)
3:プライバシー情報の濫用・誤用による名誉毀損等(窃用の一種)
4:プライバシー情報の不当な商業利用等(窃用の一種)

ここで 1-1(プライバシー領域への侵入)と 1-2(プライバシー情報の知得)とを分けて理解するのは，侵入者が他人の私的空間に侵入した場合，その私的空間内にある秘密情報等を現実に知得する段階にまで至らなくても，単なる侵入(intrusion)だけで十分に大きな法益侵害が成立すると考えられるからです。
そして，このようにして考えることにより，例えば，サイバー空間における不正アクセスのような違法行為に関し，単に無権限アクセスを違法に実行する行為だけで一定の法益侵害が発生しており，その法益侵害とは別に，当該無権限アクセス先のデータ空間にあるデータを取得(知得)する行為は別の法益侵害を構成するということが理解しやすくなります。

他人が(知的財産権のような)専有権(proprietary rights)をもつデータの無権限の知得行為は，その専有権の法的性質の相違に応じて多種多様です。
例えば，プライバシーの利益や個人データとしての法的利益の侵害が発生することもあるし，著作権や営業秘密のような知的財産権の侵害が発生することもあるし，更に，それらの法益侵害が混在することもあり得ます。

要するに，ある 1 個の侵害行為によって 1 個の法益侵害しか発生しないと硬直的に理解するのではなく，現実の社会関係に即して，どのような法益侵害があるのかを多面的かつ個別・具体的に検討・理解する必要性があります。

換言すると，1 つまたは複数の属性値(attribute)をもつ構造体(structure)として 1 つの侵害行為を記述することが可能です。

2.3 サイバー空間における類型の修正

私は，サイバー空間におけるプライバシー侵害に関して，一般理論としては，プロッサーの理論を上述のように整理した上で，更に修正すべきだと考えています。

すなわち，(1)侵入型，(2)知得型，(3)開示型及び(4)不当な二次利用型の 4 つの類型として更に整理し直して考察することが可能です。

(1) 侵入型

この類型は，自分自身及び正当な権限のある者しかアクセスできない空間の中に無権限で入る行為の類型です。

例えば，自分自身で構築・運営している Web サーバでは，自分だけが管理者兼利用者であり，自分が承認した者だけに対してアクセス権を与えているのが普通です。しかし，その Web サーバ内の私的空間の中に無権限者が不正アクセスを実行した場合，「私的空間であること」という保護利益が損なわれたことになります。
クラウド上の仮想サーバでも基本的には同じです。

(2) 知得型

この類型は，何らかの方法により，正当な理由なく，ネット経由で，自己以外の者の私的情報を入手する行為の類型です。

その入手のために実行される手段が不正アクセス行為である場合，侵入型の行為を手段として知得型の行為が実行されたことになります。これらは，刑法における牽連犯と同じような関係（目的と手段の関係）にたちます。

(3) 開示型

この類型は，正当な理由なく，私人に関する私的情報を第三者に対して開示する行為の類型です。

当該私人から提供された情報であっても，第三者に対する開示が認められていない場合，事前に本人の同意（consent）を受けた上でなければ，開示行為について正当な理由があるとは言えません。
正当な理由のない知得によって取得した情報を第三者に対して開示する行為は，知得型の行為を手段として開示型の行為が実行されたことになります。これらは，刑法における牽連犯と同じような関係（目的と手段の関係）にたちます。
同様に，知得の手段として侵入型の行為が実行され，知得された情報を第三者に対して開示した場合，順次，刑法における牽連犯と同じような関係（目的と手段の関係）にたちます。

(4) 不当な二次利用型

この類型は，本来私的なものとして専有されているはずの法的利益を，正当な理由なく，二次利用（reuse）する行為の類型です。

一般的には，肖像権や（著作者人格権と著作権を含め）著作権法上の権利の侵害だけが論じられていますが，今後は，それ以外の保護法益も検討されるべきです。

経済的利益を目的とする二次利用の場合，プロッサーの第 4 類型が該当しますが，経済的利益を目的としない場合も含め得るものとして理論全体の再構築が必要だと思われます。

3 修正された類型に関するより詳しい説明

プロッサーの理論を基礎とした上で，現代の状況を踏まえ，(1)侵入型，(2)知得型，(3)開示型及び(4)不当な二次利用型の 4 つの類型としてプロッサーの理論を再整理した新たな類型論に関し，更に詳しく説明します。

3.1 侵入型

侵入型の類型の行為は，古典的には，例えば，新聞記者や雑誌記者等が，映画俳優が宿泊しているホテルの部屋，野球選手・フットボール選手等のスポーツ選手の競技場シャワールーム等に勝手に入りこんで強引に取材したりする行為がその代表的なものだと理解されてきました。

> かつて，パパラッチ（paparazzi）と呼ばれる人々が有名人を追いかけまわし，スキャンダル写真等を撮影して雑誌社に提供した行為等もその一種として理解できるかもしれません。

これらの行為は，行為類型の別に従い，物理的に建物や居室に侵入する行為を伴い，あるいは，物理的に追跡を継続する行為を伴うものです。
後者の物理的な追跡継続行為は，現代では，プライバシー侵害という側面だけではなく，ストーカー犯罪や危険運転犯罪（あおり運転行為等）といったような犯罪行為をも構成し得ます。

このような物理的な侵入行為とは異なり，サイバー空間における侵入型の行為は，物理的にではなく，電子的に実行されます。

> ここでいう「電子的に」とは，例えば，スマートフォン，タブレット，Wifi 通信可能なノート PC，Wifi 通信可能なデジカメ，Wifi 通信可能なモニタカメラ，無線ルータ，その他 Bluetooth により接続可能な機器類等に関し，アクセス制御されておらず，または，アクセス制御に脆弱性がある場合，これらの機器に対し，正当な理由なく（無権限で）アクセスする行為として存在するということを意味しています。

一般に，これらの機器を購入した時点では，同型式の機器と共通の ID やパスワード等が設定されています。それらを初期設定のままにしておくと，その初期設定を知っているサイバー攻撃者にとっては，当該機器が何もアクセス制御していないのと同じということになります。

> スマートフォンの中には生体認証を導入しているものもあり，そのような機器類を購入した利用者が最初に生体認証のためのデータを登録するような仕組みになっているものもありますが，脆弱性が全くないわけではありません。

> 他方，仮に端末装置としてのスマートフォンのアクセス制御が正常に機能しているとしても，そのスマートフォンと公衆回線とをつなぐための無線ルータの ID やパスワードが初期設定のままだと，結局，全体として何もアクセス制御がないのと同じことになります。

更に，様々な場面で利用されている音声認識システムでは，マイクによって自動的に収録された音声データを AI システムによって解析し，その音声内容が命令文または質問文であると（AI システムが自動的に）解釈可能な場合には，デバイスに対する何らかのプロンプト入力であると仮定し，そのために必要な処理を自動的に選択し，実行します。
このような場合，これらのシステムは，利用者が何らかの命令または問いかけをしたかどうかを音データによって識別します。

それゆえ，これらのシステムは，利用者が何らかの命令または問いかけをしない間も，常時，それらの機器が設置された空間内の音声を探知し続けています。

IPv6 の環境下では，個々の機器類をピンポイントで識別・特定できます。GPS データと組み合わせれば，ピンポイントで所在地識別が可能となります。

カメラやセンサーによって利用者の表情に関するデータも取得するような機器類では，当該空間における音データだけはなく，画像データや音声データも常時取得されていることになります。自動車に装備されているドライブレコーダも基本的には同じです。

これらの機器類が定型約款に定める保護条項に反して利用された場合，あるいは，不正アクセスを受けた場合，侵入型の行為が実行されたことになります。

ここで説明したような事案類型のものとして現実に発生した事案としては，夫婦が乳児をベッドに寝かせたまま外出中にスマートフォンを用いてリモートで室内を監視できるシステムが不正アクセスを受け，第三者によって室内の様子が第三者によって覗き見られたという出来事が多発したという事例などがあります。

このような行為は，単なる好奇心によるものだけではなく，例えば，乳幼児の誘拐と人身売買の準備作業，あるいは，強盗，殺人または脅迫・強要のための準備作業として実行されていることもあり得ると考えられます。

スマートフォンや音声認識デバイス等それ自体には全く問題がなかったけれども，データを記録するクラウド側に問題があったと疑われた事案もあります。

例えば，米国では，女優 Jennifer Lawrence 等が iCloud 上に記録していた写真が誰かによって奪われ，ネット上で第三者に開示されたという事案があります。
この事案では，無権限で iCloud にアクセスした段階で「侵入」の類型が成立します。そして，写真を取得した段階では「知得」の類型となり，その写真をネット上で第三者に開示した段階で「開示」の類型となります。これら異なる類型は，順次手段結果の関係となっているので，刑法に定める牽連犯のような事案類型として理解することもできます。

なお，仮に各国の個人データ保護法令（日本国では個人情報保護法）に違反してデータ記録の

ためのクラウドサーバ（ストレージサーバ）を設置・運用している事業者が存在しているとすれば，その事業者は，「安全なものだ」と信用して「私生活」と関係する写真や文書等をそのサーバに記録している利用者の個人データ保護に関し，故意または過失による法令違反行為を実行していることになります。

> このような類型の事案において，当該運用者が，個々の利用者の（事前の）同意を得ることなく個々の利用者のデータ記録領域にアクセスし，その利用者の私生活と関係する写真や文書等にアクセスする行為は，侵入型の違法行為となり得ます。

後述の生成 AI では，利用者が入力したプロンプト内容の AI システムによる自動学習を介して，そのような法令違反行為が大量かつ自動的に実行されることがあり得ます。

3.2 知得型

知得型の行為の動機は，多種多様です。

上述の米国の有名女優を狙った事案では，単なる好奇心や趣味のレベルの動機によるものだったかもしれません。しかし，「第三者の好奇心や趣味のために私生活を知られることがない」という利益は，明らかに，法的保護に値します。
そのような利益が法的に保護される合理的な期待を肯定できる場合が圧倒的に多いと言えるでしょう。
有名人ではない普通の一般私人であっても，「私的情報を知られないこと」は，保護法益とされるべきです。

> 例えば，ある人から聞いたところによれば，その人は，生徒の怠惰な行動に怒りを覚えたときは，日記帳にそれを書き，閉じたまま一晩置いておくということを習慣化しておいたそうです。
> 一晩寝ると，大概の場合，怒りもおさまり，その生徒に対して冷静に対処できるようになるとのことでした。
>
> 一般に，怒りにまかせた感情的な行動をとっても，ほとんど全ての場合において，良い結果を得られません。
> 一晩寝かせるという方法は，それ自体としては，賢い方法かもしれません。
> しかし，仮にその日記帳の中身を誰かが勝手に読んだとします。そのような場合，誰かが勝手に読んだということだけで，かなり大きな問題が発生するリスクが生じていることは，明らかだと思われます。
> その日記の中には，当該生徒が怠惰であるということに対する怒りの感情が露骨に記述されているかもしれません。それゆえ，そのようなリスクの発生を避けるという意味での法的利益が肯定されます。
>
> ギリシア神話の中にある「王様の耳はロバの耳」というミダス王の物語を想起すべきです。
>
> プライバシー保護という文脈からは逸れますが，日記や日誌の内容の知得行為は，国防上または情報

セキュリティ上の深刻な脅威を構成することがあり得ますので，注意を要します。

NISC，サイバー攻撃対応の訓練情報が流出　富士通ツールへの不正アクセスで
ITMedia：2021 年 6 月 4 日
https://www.itmedia.co.jp/news/articles/2106/04/news154.html
[2025 年 6 月 9 日確認]

一般に，国防上の秘密は，個人の私生活上の秘密等とはかなり異なる性質をもつものですが，国家の安全のために極めて大きな重要性をもつものであることを否定する学説は存在しません。
これらの点に関しては，夏井高人「情報社会の素描(2・完)」法律論叢第 90 巻第 6 号 165～211 頁(2018 年)で詳しく論じています。

サイバー空間においては，日記として意識的に書き綴られたものではなくても，自動的に私人の生活履歴の記録として機能してしまうものがあります。

例えば，Web サイトへの訪問履歴がその一例です。訪問履歴の内容を解析することにより，当該利用者の趣味のレベルの傾向性だけではなく，当該利用者の性的嗜好，思想傾向，宗教団体や政治団体の加入，消費行動等の事実を推測可能になってしまいます。

例えば，「エロサイトや過激な画像サイトばかり訪問している」という事実を示す訪問履歴が正当な理由なく誰かに知得されると，そのことだけで困惑してしまう人が少なくないでしょう。

現在，インターネット上の電子商取引サイトやポイントカード等においては，消費行動履歴だけではなく，インターネット上の行動履歴等も結合して電子的なマーケティングが行われることが普通になってきました。
それらの自動処理が非公開のクラウドコンピューティングサービスによって実行されている場合であっても，クラウドサーバに対するハッキングやランサム攻撃によって，第三者がそのマーケティング関連情報を知得してしまうことがあります。そのようなサイバー攻撃は，例えば，サイバー戦等の軍事的行為の手段としてのサイバー攻撃またはテロ行為の一種である場合を含みます。

さて，マーケティングのための行動履歴データは，それ自体としては，仮に公開データであったとしても，収集された後にプロファイリング（profiling）と呼ばれる自動処理が実行されると，単なるバラバラのデータではなく，特定の個人との関係において，ある属性値を示し得るデータセット（datasets）となってしまうことがあります。

この種の問題は，私的情報ではない公開情報によって発生する場合，あるいは，私的情報と公開情報とが混在する状況で発生する場合が一般化してきています。

それゆえ，これらの問題に関しては，私的な事柄であることを重要な要素とするプライバシー保護法制及びプライバシー保護の理論だけでは適切に対処できません。

各国の個人データ保護法制は，プライバシー保護とは別の側面から私人の利益（特に，個人の尊厳）を守ろうとする新たな法的仕組みの 1 つです。
特に，EU の一般データ保護規則（GDPR）では，プライバシー保護及び個人データ保護の両方の側面から，プロファイリングやログ（履歴）に関し，厳重な保護条項を定めています。

3. 3 開示型

一般に，LINE や X（旧 Twitter）等の SNS 上で私人の秘密が暴露（開示）され，名誉棄損の結果が生ずるような事例は，むしろ日常的に発生する類型のものとなっているかもしれません。

プロッサーの理論における第 3 類型では，開示の結果としての名誉棄損により「誤った評価や印象を与えること」という点を重視しています。
しかし，名誉棄損の結果を生じさせなくても，（特に，侵入＋知得＋開示の順次牽連的な状況の下においては）開示だけでプライバシーという保護法益の侵害があり得ると理解できるので，プロッサーの第 2 類型においても，開示だけでプライバシーの問題となると理解されています。

一般に，名誉棄損行為は，プライバシー侵害行為を全く伴わない場合があります。公表されている事実だけを基礎とし，自分勝手な評価を付加した表現物を作成・流布することによって名誉棄損の結果を発生させることもできるからです。

このような事案は，古典的な私事の暴露による名誉棄損行為とは別の社会類型に属する行動だと言えます。

一般に，開示型においては，プライバシー情報が「開示されないこと」が保護法益であり，第三者に対する開示の結果として名誉棄損等の結果が生ずる場合には，「開示されないこと」とは別の保護法益の侵害があると理解すべきだと言えます。
開示の結果として名誉棄損が発生する場合の保護法益に関しては，根本的には「個人の尊厳」から派生する「名誉権」または「公正な社会的評価を受ける利益」として理解することが可能でしょう。

3. 4 不当な二次利用型

（プライバシー侵害としての側面）

公開情報を不当に二次利用（reuse）する行為に関して，著作権の文脈で議論が生ずることはあっても，プライバシー侵害の一種として理解すべきかどうかに関しては，従来はあまり議論されてきませんでした。

例えば，最近話題になった日本国内の犯罪事案として，アダルトビデオの画像にアダルト女優で

はない有名女優の画像を自動的に合成する「ディープフェイク（deep fake）」と呼ばれる技術を悪用して偽のアダルト映像作品を作成し，荒稼ぎしていた者らが逮捕されたという事案があります。

このような事案において素材（material）として使用された画像は，全て公開された映像作品の画像の一部です。

しかし，そのような二次的利用は，当の女優の同意や映画作品の著作権をもつ企業等の同意または許諾を得たものではありません。違法な二次利用行為となります。
違法な二次利用行為は，肖像権の侵害，パブリシティの権利の侵害，著作権または隣接権の侵害，名誉権の侵害等を発生させ得るものです。

このようなタイプの問題は，一般的には，プライバシー侵害の問題としてはとらえられていないだろうと思われます。関連分野の法学者の無関心・無理解によってそのような状況となってしまっている部分も少なくありません。

しかし，一般に，プライバシーの範囲内にある私的画像や私的動画等を組み合わせた二次利用物が無権限で作成された場合，明らかにプロッサーの第 3 類型または第 4 類型のプライバシー侵害が発生し得ます。

公開された映像作品を素材とするような場合において，プライバシーの侵害はないと理解することは，プライバシーの範囲内にある私的画像や私的動画等を組み合わせた二次利用物が無権限で作成された場合との対比において，明らかにバランスを欠く考え方だろうと思われます。

生成 AI を用いてわいせつ画像を自動生成する場合においても，当該生成された画像の中に実在の人物の画像要素が含まれている場合，あるいは，実在の人物の画像だと信じさせるためにチューニング等の処理が実行されている場合には，わいせつ画像に関する犯罪としての側面だけではなく，プロッサーの第 3 類型及び第 4 類型の意味におけるプライバシー侵害としての側面も検討されるべきです。

> 生成 AI でわいせつポスター　販売容疑で4人逮捕、全国初―警視庁
> 時事通信:2025 年 4 月 15 日
> https://www.jiji.com/jc/article?k=2025041500333
> [2025 年 6 月 9 日確認]

（プライバシー侵害以外の悪影響）

ディープフェイク（deep fake）は，プライバシーや個人データ保護という文脈で問題となるだけではなく，特に公的機関から提供されるオープンデータとの関係では，オープンデータの正確性と有用性を損なうものであり，その結果として，公的機関が提供するオープンデータへの信頼全体に

対して深刻な影響を与え得るものです。
そのようなタイプの問題はプライバシー侵害と直接に関係するものではありませんが，ここで付言しておきます。

一般に，公的機関が提供するオープンデータに関し，ディープフェイクの原因となる要素の混入が横行することになると，そのようなオープンデータを二次利用して新たに創作されたコンテンツ等も偽（fake）の構成要素を最初から含んでいることになります。

ディープフェイクの原因となる要素の混入は，担当職員等の内部者の非違行為，外部からのサイバー攻撃によって生ずることがあります。しかし，それだけではなく，例えば，当該公的機関が使用している生成 AI の基礎をなすモデルの中に最初からディープフェイクの原因となる要素が（LLM の学習結果として）混入していることによってそのような結果が生じていることもあり得ます。

そのような生成 AI の中に伏在している要因によってディープフェイクの原因となる要素が自動的に生成されてしまう場合，生成 AI の信頼性とセキュリティを確立するための仕組みが設けられており，かつ，担当職員等がそのような仕組みに精通していて使いこなしているという条件を満たしていない限り，当該公的機関が当該公的機関に内在する問題に気づくことがないという深刻な事態が発生することがあり得ます。

公的機関から提供されるオープンデータの中におけるディープフェイクの要素の混入が横行するようになると，政府のデータ経済戦略の一部として公的機関がオープンデータを提供することにより，スタートアップや中小企業等を支援しようとする経済政策全体を阻害しまたは頓挫させる大きな要因となり得ます。

このようなディープフェイクが国防上でも情報セキュリティ上でも深刻な悪影響を与え得ることは，言うまでもありません。

そのようなディープフェイクが横行した場合，無論，生成 AI を応用したデータ分析が成立しなくなり，また，当該生成 AI システムそれ自体も（自滅的に）破綻することになります。

（法的対応）

幾つかの国を除き，世界各国とも，生成 AI によって自動生成される偽情報，偽報道及び偽データの流通による民主主義及び選挙活動に対する深刻な悪影響を憂慮し，立法的な対応を検討しています。

> 日本国においては，人工知能（AI）と関連する法令として，人工知能関連技術の研究開発及び活用の推進に関する法律（令和 7 年法律第 53 号）が制定されましたが，この法律は，AI 技術の悪用及び濫用に対処するための法律ではありません。
> 日本国においては，特に新しい法令を制定しなくても，AI 技術の悪用及び濫用に関しては，プライバシ

一保護の側面では，既に説明したとおりです。刑法上では，名誉毀損罪，侮辱罪及び業務妨害罪の適用が検討されるべきです。
他方，公権力主体，私企業及び個人を含め，業務を妨害する行為のための手段として AI 技術が悪用または濫用される場合，事案の相違により，業務妨害罪(刑法第 233 条)，電子計算機損壊等業務妨害(刑法第 234 条の 2)，公用電磁的記録毀棄罪(刑法 258 条)，私用電磁的記録毀棄罪(刑法第 259 条)の成立を検討可能な場合が多いと考えられ，それらの刑法上の犯罪行為として捜査・処罰すべきだと考えられます。
更に，国家権力の破壊，社会秩序の破壊のための手段として AI 技術が悪用または濫用される場合，事案の相違により，刑法第 77 条～刑法第 96 条の 6 のいずれかの条項の適用が検討されるべきです。
詳論は避けます。

4 補説

4.1 サイバー攻撃との関係

例えば，通信回線を遮断している PC への(テンペスト攻撃，キーロガーやスキマーを用いた攻撃等の)サイバー攻撃により，PC 内におけるデータ処理を外部から傍受する行為は，刑事法上の無権限アクセスの一種として考察可能なだけではなく，プロッサーの第 1 類型における「seclusion」の「intrusion」の問題を含み得るものとして理解することも可能です。

VPN の保護能力の程度には限界があるとはいえ，VPN による防護を無権限で破り，通信内容を傍受する行為は，電気通信事業法に定める通信の秘密の侵害行為の一種として考察可能なだけではなく，「solitude」の「intrusion」の問題を含み得るものとして理解することも可能です。

量子コンピュータによる総当たり的な超高速解析処理の下ではほとんど無意味化されつつあるとはいえ，現在の標準的なレベルで暗号化された電子ファイルを無権限で解読(復号)する行為も同じように考えることができます。

アクセス制御のあるクラウド上のストレージ領域に対する無権限のアクセスは，不正アクセス禁止法に定める不正アクセス罪の該当性が問題となるだけではなく，「private affairs」の「intrusion」の問題を含み得るものとして理解することも可能です。
スパイウェアを用いた行動監視や通信傍受行為の中にも「private affairs」の「intrusion」の一種として理解するのが妥当な行動類型が含まれています。

4.2 AI との関係

いわゆる人工知能技術(AI)は，サイバー空間のプライバシー保護という文脈においても大きな問題を生じさせ続けています。

最近の具体的な出来事として，OpenAI の ChatGPT のような AI サービスに関し，日本国の個人情報保護委員会は，注意喚起を行いました。

> 生成 AI サービスの利用に関する注意喚起等について
> 個人情報保護委員会:2023 年 6 月 2 日
> https://www.ppc.go.jp/news/careful_information/230602_AI_utilize_alert/
> [2025 年 6 月 9 日確認]

この注意喚起は，かなり遅い対応であり，かつ，どうにも手ぬるい対応だと評価せざるを得ません。また，（口先だけの応答は別として，実質的にみた場合）無視され続けているようです。この注意喚起に従うと，AI モデル（LLM）の生成のための学習ができなくなってしまうからです。

4.３ 混合データセットの取扱い

今後，サイバー空間においては，生成 AI と関連する個人データ保護上の法的問題が今後ますますもって増加することになるだろうと予測されます。

また，生成 AI では個人データ（personal data）と非個人データ（non-personal data）が混在した混合データセット（mixed data set）を自動的に処理することが普通なので，そのような混在型のデータセットに適用される個人データ保護関連法令の条項及びその解釈・運用を正確に理解している必要性があります。

詳論は避けます。

５ まとめ

この講義では，法情報へのアクセスとの関係で理解が必要となる範囲内で，正確な意味でのプライバシーの概念を理解するための必須の前提となる法理論の幾つかを説明しました。

一般に，「プライバシー」の本質の理解との関係においては，特に，各人各様の異なる態様の私生活があり，それら多種多様な私生活に対応して個別・具体的で多種多様なプライバシーが存在しているということを理解することが大事です。

一般に，「全ての人に共通な私事」は存在しません。
無数に存在する異なるタイプの私的空間及びその内部における様々な出来事であることを示す総称として「私事」という語（符号・文字列）が使用されているだけです。カテゴリを示す抽象名称の一種だと言えるでしょう。

多種多様な私事が存在し得ることを理解するには，「自分が生活してきた世界」だけではなく，（過去の世界を含め）自分が知らない世界を可能な限り広く網羅的に知り，自分の価値観とは異なる価値観をもつ極めて大勢の人々が存在していることを知る必要があります。
自分の既存の経験や知識からの想像だけでは大きな限界があります。それゆえ，可能な限り多数の古典を読破し続けることが必須となります。

他方において，多種多様な私生活や価値観と関係する情報もプライバシー情報の一種として法的に保護されなければならないということを正しく認識するための方法論（手段）もまた多種多様であり得ます。

非常に優れた法学者によって構築された類型論は，種々雑多な現実の事案を整理して理解するための手段として，大きな助けとなります。

しかし，どれだけ優れた類型論であっても，時代の変化と共に陳腐化することがあり，また，後になって欠点が見つかることがあります。
それゆえ，非常に優れた方法論（手段）であっても，常に「見直し」と「改善」が必要になります。そして，ダメになってしまったときは，捨て去ることも必要となります。

第 8 回の講義の中では，プロッサーの 4 類型を解説し，その類型論を修正した新たな類型論を説明しました。

どんなに優れた方法論であっても，常に「見直し」と「改善」が必要です。

法情報学Ⅰ第9回講義案
プライバシー保護との関係（2）

(2025 年 6 月 16 日開講)

元明治大学法学部教授
夏 井 高 人

1 総説

一般に，プライバシーの法的保護と個人データの法的保護とでは，内容的に重なる部分が少なくありませんが，異なる部分もあります。

例えば，プロッサーの 4 類型に即して考えてみた場合，第 1 類型と第 2 類型のプライバシーでは保護の対象が「秘匿されていること」または「秘密になっていること」が重要です。
それゆえ，（本人の意思により，または，法律上の規定に基づき）最初からオープンになっている情報やデータに関しては，秘匿も秘密も存在しないので，（プロッサーの第 1 類型と第 2 類型との関係では）そもそも「プライバシーの合理的な期待」が成立しません。

しかし，そのように最初からオープンになっている情報やデータであっても，その情報やデータの中に個人情報（個人データ）が含まれている場合，個人情報（個人データ）として法的な保護を受けることがあります。

> 例えば，個人と関係する何らかの情報（データ）に関し，個人情報保護（個人データ保護）のための「正確性の原則」が適用される場合，当該情報（データ）がオープンのものであるか秘匿もしくは秘密のものであるかに拘わらず，その情報（データ）の内容は，「正確」でなければなりません。
> 具体例としては，例えば，住民基本台帳法（昭和 42 年法律第 81 号）に基づく住民基本台帳データは，同法所定の要件を満たす限り閲覧可能なので，オープンなデータであると言えます。しかし，市町村長は，個人データの法的保護の目的のために，住民基本台帳の基礎となっている住民票の記載内容が正確であることを確保すべき義務を負っており，住民基本台帳の一部の写しを提供する場合にはその写しの内容が正確であることを確保しなければなりません。

そのようにして，プライバシー情報とはいえない情報またはプライバシー情報と非プライバシー情報とが混在する情報であっても，その情報に対して正確性の原則が適用されることを通じて一定の法的保護が与えられている場合，その情報は，プライバシー情報（プライバシーデータ）ではない個人情報（個人データ）として存在し，法的に保護されていることになります。

特定の個人識別情報に対して正確性の原則が遵守されない場合（＝正確性の保証がない場合），当該個人識別情報は識別力が保証されない「単なる情報」になります。そのような場合においては，例えば，国の機関による個人番号及び関連データの入力作業にも影響を与え，当該個人が

正確に識別されなくなってしまうことや別人として扱われてしまうこと，その結果として，当該データが正確であることを基礎とする各種業務に大混乱が発生することがあり得ます。個人データの誤入力によってデータの正確性が失われたことによる被害発生の実例は，例えば，基礎年金の受給等と関連して，過去に多数存在します。

> 例えば，住民基本台帳データのように，入力されたデータが（所定の要件を満たすことを条件として）公開データであり，それゆえに秘密性がなく，従ってプライバシー侵害が直ちに生ずるわけではなくても，もし誤入力されれば，個人情報保護（個人データ保護）の基本原則の 1 つである「正確性の原則」に反する違法行為となり，関連する個人情報保護法令の違反行為に該当することになります。

2　個人データ保護法制の歴史

2.1　一般的な説明

プライバシーと関連する法的保護の法理は，主として，米国の不法行為法（tort law）の法解釈（判例法）の蓄積の中で形成されてきました（第 8 回の講義内容参照）。

これに対し，個人データの法的保護は，主として，関連国際条約や関連行政法規の制定を通じて形成されてきました。

個人データの保護が国際的な規模で最初に議論された場所は，OECD（経済協力開発機構）と欧州評議会（Council of Europe，以下「CoE」と略称する。）でした。
OECD と CoE は，相互に密接に連携しながら，個人データの保護に関する国際的な枠組みの構築のための努力を重ねました。
OECD と CoE における検討結果は，後に，EC（後の EU）の 1995 年の個人データ保護指令 95/46/EC の立法にも非常に大きな影響を与えています。

この間，産業立国をめざす日本国の政府は，(1)電子的なデータの流通に伴う国際的に通用する個人データ（個人情報）の法的保護の枠組みを導入しなければ，貿易立国を維持することが不可能であるとの認識にたち，(2)行政管理庁（当時）を責任主体とする研究チームを欧州各国に派遣し，既に個人データ保護のための法制を構築していた諸国の法制調査を遂行すると同時に，(3)OECD 及び CoE にも政府関係官庁の職員を派遣し，世界規模の個人データ保護法制の動きに関与しました。

> このような動きの中で中心的な役割を果たしたのは，一橋大学教授（当時）の堀部政男氏でした。
> 堀部政男氏は，その後，OECD において極めて重要な役割を果たし，また，日本国において個人情報保護委員会が設置されるとその初代委員長に就任しました。

日本国の個人情報保護法制は，以上のような国際的な動きの中で検討され，日本国の国内法とし

て運用されてきたものです。

日本国の個人情報保護法制は，行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律（昭和 63 年法律第 95 号・旧行政機関個人情報保護法）の立法から始まります。
その後，個人情報の保護に関する法律（平成 15 年法律第 57 号・個人情報保護法），行政機関の保有する個人情報の保護に関する法律（平成 15 年法律第 58 号・行政機関個人情報保護法）及び独立行政法人等の保有する個人情報の保護に関する法律（平成 15 年法律第 59 号・独立行政法人等個人情報保護法）の立法によって基本的な法制枠組みが確立されました。
これらの法令に関しては，法改正が重ねられてきました。
行政機関個人情報保護法及び独立行政法人等個人情報保護法は，デジタル社会の形成を図るための関係法律の整備に関する法律（令和 3 年法律第 37 号）によって廃止されました。

日本国における現行の個人情報保護法制は，個人情報保護法（平成 15 年法律第 57 号）に一本化されています。なお，個人情報保護法に関しては，更なる改正が予定されています。

この講義（第 9 回）では，日本国の個人情報保護法制の母法ともいうべき(1)CoE の条約と決議等，(2)OECD のガイドライン及び(3)EU（旧 EC）の個人データ保護法制の立法史を説明した上で，日本国の法制の概略を説明します。
米国の関連立法及び判例法並びに EU の判例法の説明は省略します。

2．2 欧州評議会（CoE）の関連条約と決議等

欧州評議会（CoE）における個人データ保護のための国際的な法的枠組み構築のための取組み及び CoE 条約締結に至る経過に関しては，「個人データの自動的な処理と関連する個人の保護に関する条約の説明書（Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data）」（以下，「CoE 条約説明書」という。）の中で詳細に説明されています。CoE と OECD 及び主要各国との関係及び共同作業に関しても，CoE 条約説明書の中で詳細に述べられています。

> Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)
> https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108
> [2025 年 6 月 16 日確認]

CoE 条約説明書の中で述べられているような経過を経て，1981 年 1 月 28 日，ストラスブールにおいて，「個人データの自動的な処理と関連する個人の保護に関する条約（ETS No.108）」（以下「CoE 条約」という。）の締結のための式典が行われました。

CoE 条約説明書のパラグラフ 4 の中では，「1968 年，欧州評議会の議員会議は，閣僚委員会に対

し，勧告第 509 号を発した。これは，欧州人権条約及び構成国の自国の法律が，個人のプライバシーの権利について，現代の科学及び技術に対応した十分な保護を提供するものであるか否かを問うものであった。この勧告に応じて，閣僚委員会の指示に基づき行われた調査結果は，『現在の構成国の立法は，自動的なデータバンクと関連する個人のプライバシーその他の権利及び利益について不十分な保護しか与えてない』ということを示していた。この検討結果に基づき，閣僚委員会は，1973 年及び 1974 年，データ保護に関する 2 つの決議を採択した」と説明されています。

ここでいう「データバンク」（ドイツ語系の用語）とは「データベース」（英語系の用語）のことを指します。

CoE 条約における個人データ保護の基本理念は，この 2 つの決議，すなわち，「民間部門における電子的なデータバンクに対応する個人のプライバシーの保護に関する決議第 22 号（Resolution (73)22 on the Protection of the Privacy of Individuals vis-a-vis Electronic Data Banks in the Private Sector）」（1973 年）と「公的部門における電子的なデータバンクに対応する個人のプライバシーの保護に関する決議第 29 号（Resolution (74)29 on the Protection of the Privacy of Individuals vis-a-vis Electronic Data Banks in the Private Sector）」（1974 年）の中で明示されています。

これら 2 つの決議は，世界の個人データ保護法制の歴史を研究する上で極めて重要なものです。

CoE の「民間部門における電子的なデータバンクに対応する個人のプライバシーの保護に関する決議第 22 号」（1973 年）の決議の別紙は，以下のとおり，基本原則を定めています。

1. 記録保存される情報は，正確なものであるべきであり，かつ，最新の状態に保たれるべきである。
   一般に，個人の親密な私生活に関する情報または不当な差別をもたらし得る情報は，記録されてはならならず，または，もし記録される場合には，他に伝達されてはならない。

   The information stored should be accurate and should be kept up to date.
   In general, information relating to the intimate private life of persons or information which might lead to unfair discrimination should not be recorded or, if recorded, should not be disseminated.

2. 情報は，それが記録保存される目的との関連において適切なものでありかつ適格なものであるべきである。

   The information should be appropriate and relevant with regard to the purpose for which it has been stored.

3. 情報は，詐欺的な手段または不正な手段によって取得されてはならない。

   The information should not be obtained by fraudulent or unfair means.

4. 当該期限を超えて一定の類型に属する情報が保存されまたは利用されることのない期限を個別に定める

ための規定が定められるべきである。

Rules should be laid down to specify the periods beyond which certain categories of information should no longer be kept or used.

5. 適切な承認がない場合，情報は，その情報が記録保存された目的とは異なる目的のために利用されてはならず，かつ，第三者に対して伝達されてはならない。

Without appropriate authorisation, information should not be used for purposes other than those for which it has been stored, nor communicated to third parties.

6. 一般原則として，関係する個人は，彼に関して記録保存されている情報，その情報が記録保存される目的及びその情報の個々の開示の詳細について知る権利をもつべきである。

As a general rule, the person concerned should have the right to know the information stored about him, the purpose for which it has been recorded, and particulars of each release of this information.

7. 不正確な情報を正確なものとするため，及び，利用が終了した情報または違法な方法で取得された情報を削除するために，全ての手立てが講じられるべきである。

Every care should be taken to correct inaccurate information and to erase obsolete information or information obtained in an unlawful way.

8. 情報の侵害または濫用に対して，注意が払われるべきである。
電子的なデータバンクは，そのような情報を取得する権限をもたない者に抗して，データバンクによって保有されているデータに対するアクセスを阻止する防護システム，及び，意図的なものであるか否かを問わず，情報の誤伝達を検出する防護システムを具備すべきである。

Precautions should be taken against any abuse or misuse of information.
Electronic data banks should be equipped with security systems which bar access to the data held by them to persons not entitled to obtain such information, and which provide for the detection of misdirections of information, whether intentional or not.

9. 記録保存された情報へのアクセスは，その情報を知る正当な理由をもつ者だけに限定されるべきである。
電子的なデータバンクの業務運用の従業者は，データの濫用を避けることを狙いとする行動の規定，及び，とりわけ，職業上の守秘義務に関する規定によって拘束されるべきである。

Access to the information stored should be confined to persons who have a valid reason to know it.
The operating staff of electronic data banks should be bound by rules of conduct aimed at preventing the misuse of data and, in particular, by rules of professional secrecy.

10. 統計データは，集約された形態においてのみ，かつ，その情報を特定の個人と結びつけることが不可能な方法によってのみ，開示されるべきである。

Statistical data should be released only in aggregate form and in such a way that it is impossible to link the information to a particular person.

このようにして成立した CoE 条約の第 1 条(目的)は，「この条約の目的は，各加盟国の領域内において全ての個人のために，彼の国籍及び居住地の別を問わず，彼に関連する個人データの自動的な処理と関連する彼の権利及び基本的な自由を保護すること，とりわけ，彼のプライバシーの権利を保護すること(以下「データ保護」という。)を目的とする」と定めています。

CoE 条約の第 2 条(定義)は，「個人データ」に関し，「識別される個人または識別可能な個人(以下「データ主体」という。)に関連する情報を意味し」と定義し，「自動的な処理」に関し，「その全部または一部が自動的な方法によって行われる場合には，次の業務処理を含む：すなわち，データの記録保存，それらのデータの論理的な業務処理と数学的な業務処理を行うこと，それらの修正，削除，検索または移動を行うことを意味し」と定義し，そして，「ファイルの管理者」に関し，「自然人または法人，行政機関，官庁その他の組織であって，自国の法律に従い，自動的なデータファイルの目的をどのようなものとするかを決定し，どの類型に属する個人データを記録保存すべきかを決定し，そして，どのような業務処理に対してそれらが適用されるのかを決定する権限を有する者のことを意味する」と定義しています。

CoE 条約の第 6 条(特別類型に属するデータ)は，「人種的な出自，政治的な意見または宗教上の信条その他の信条を明らかにする個人データ，並びに，健康と関係する個人データまたは性生活と関係する個人データは，自国の法律が適切な安全確保措置を定めていない限り，自動的に処理できない。有罪判決と関連する個人データについても同じである」と定めています。

CoE 条約の第 7 条(データの安全性)は，「自動的なデータファイルに記録保存された個人データを，偶発的な破壊または無権限による破壊，偶発的な喪失から保護し，かつ，無権限によるアクセス，改変または移転から保護するために，適切な防護措置が講じられなければならない」と定めています。

私は，EU 法の参考訳等において，個人データ保護の文脈における動詞の「store」及び名詞の「storage」を「記録保存」と訳し，個人データ保護の文脈における類似の概念である「record」を「記録」と訳し，「own」を「保有」と訳し，「hold」を「保存」等と訳し，「keep」を「保管」等と訳し，相互に区別できるようにしています。これらの語(英語)は別の状態を意味する語なので，それに対応する訳語(日本語)も異なるものでなければなりません。
動詞の「store」及び名詞の「storage」に関し，「蔵置」と訳す例がありますが，「蔵置」とは，墳墓の中に遺体や遺骨等を収納して埋葬する行為のことを意味する法律用語なので，適切な訳語ではありません。
動詞の「store」及び名詞の「storage」に関し，「蓄蔵」または「貯蔵」と訳す例もあります。これらは，「storage」が本来は倉庫を示す概念であり，「store」が物体である商品等を収納または保管する行為のことを示す概

念であることから，そのような場合には適しています。しかし，「蓄蔵」または「貯蔵」は，電子的な媒体に電子的なデータを記録して保存するような場合には，適切な訳語と言えるかどうか疑問が残ります。

更に，CoE 条約は，追加議定書（ETS No.181）によって，2001 年 11 月 8 日に実質的な一部改正が行われました。
この一部改正は，個人データ保護の実効性を確保するため，独立の監督機関を設置し，個人データを処理する者がその監督機関の監督に服することを追加して定めるものです。

日本国の行政組織である個人情報保護委員会は，CoE や EU において理解されているような意味での「独立の監督機関」ではあるとは言えません。

2．3 OECD のガイドラインとフレームワーク

CoE における条約案の起草作業と並行して，OECD においても個人データ保護のための基本的な枠組みを構築する作業が進められました。

CoE における作業と OECD における作業とを比較検討してみると，CoE においては，国際法上の法的拘束力をもつ法規範形式の 1 つである条約（Treaty or Convention）を構築し，可能な限り多数の加盟国を得て，統一的な法規範が支配する領域を拡大しようとする努力の現れであったと理解することができます。
これに対し，OECD が行った努力は，法的拘束力のある法規範を定めることによる弊害として，そのような法規範を受容できない国にプライバシー及び個人データ保護のための国家制度が構築されなくなってしまうという問題点があることを認識した上で，拘束力の緩い勧告的な文書としてガイドライン（Guidelines）を構築し，提案するというものでした。

CoE における作業と OECD における作業とは，基本的には同じ戦略を目的とするもので，内容的にもほぼ近似または類似するのですが，具体的な手段（戦術）が異なっているのだと認識・理解できます。
目的と手段の一般的な相互関係を理解する上でも非常に良い具体例だと考えられます。

さて，OECD の最初の版のガイドライン（OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data）は，1980 年に公表されました。

このガイドラインは，2013 年に全面改正され，『OECD Privacy Framework』となりました。
日本語による 2013 年のフレームワークの解説書としては，堀部政男・新保史生・野村至『OECD プライバシーガイドライン－30 年の進化と未来』（JIPDEC・2014 年）があります。

OECD の 1980 年のガイドラインの実質は，マネジメントシステムの導入による個人データ保護のための合理的な仕組みを構築する上での基本指針を示すものです。

この OECD のガイドラインを完全に遵守したとしても，(機械処理または自動処理されないプライバシー情報を含め)かなりの種類のプライバシー情報に対してガイドラインが適用されません。
そのため，基本的には，全体としてのプライバシーの利益の法的保護のための指針とはなっていません。
この点は，2013 年のフレームワークでも同じです。

2. 4 OECD の個人データ保護 8 原則とその影響

OECD の 1980 年ガイドラインは，個人データ保護上の 8 つの原則を提示しています。

(1) 収集制限の原則(Collection Limitation Principle)

個人データの収集に対する制限が存在すべきであり，かつ，そのようなデータは，適法かつ公正な手段により入手されるべきであり，それが適切であるときは，データ主体が了解している状態でまたはデータ主体の事前の同意を得た上で入手されるべきである。

There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

(2) データ品質の原則(Data Quality Principle)

個人データは，当該個人データが使用される目的にとって適格であるべきであり，かつ，当該目的のために必要な範囲内で，正確であり，完全でありかつ最新のものであるべきである。

Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

(3) 目的の特定の原則(Purpose Specification Principle)

個人データが収集される目的は，遅くともデータ収集の時点よりも前に特定されるべきであり，かつ，その後の利用は，当該目的を満たすためまたは当該目的と互換性のないような別の目的ではあるけれども個々の目的変更の際に特定されているような別の目的を満たすために限定されるべきである。

The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

(4) 利用の限定の原則(Use Limitation Principle)

以下の場合を除き，個人データは，第 9 項に従って特定された目的以外の目的のために開示され，利用でき

るようにされまたはそれ以外の利用をされてはならない:

a) データ主体の事前の同意がある場合;または

b) 法の権威による場合

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

a) with the consent of the data subject; or

b) by the authority of law.

(5) セキュリティ上の安全確保の原則(Security Safeguards Principle)

個人データは, データの紛失もしくは無権限アクセス, 破壊, 使用, 改変または開示のようなリスクに抗する合理的なセキュリティ上の安全確保によって防護されるべきである。

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

(6) 公開性の原則(Openness Principle)

個人データと関係する開発, 実務及び政策に関し, 一般的な公開性の基本方針が存在すべきである。個人データの存在及び性質, 個人データ利用の主たる目的並びにデータ管理者の識別名及び常居住地を確定する手段が容易に利用できるようになっているべきである。

There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

(7) 個人の参加の原則(Individual Participation Principle)

個人は, 以下の諸権利をもつべきである:

a) データ管理者またはそれ以外の者から, そのデータ管理者が当該個人と関連するデータを保有しているか否かの確認を得る権利;

b) 当該個人に対し, 当該個人と関連するデータを伝達させる権利:

  i 合理的な時間内に;

  ii 無料でまたは過剰ではない料金で;

  iii 合理的な態様で;かつ,

  iv 当該個人にとって容易に認識可能な方式で;

c) 副項(a)及び副項(b)の下において行われた求めが拒否される場合, その理由が与えられる権利, 及び, そのような拒否に対して異議を申立て得る権利;並びに

d) その個人と関連するデータに異議を申し立て得る権利, 及び, 異議が認められる場合, そのデータを消

去させ，訂正させ，完全なものとさせまたは修正させる権利。

An individuals should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
b) to have communicated to him, data relating to him:
   i within a reasonable time;
   ii at a charge, if any, that is not excessive;
   iii in a reasonable manner; and
   iv in a form that is readily intelligible to him;
c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
d) to challenge data relating to them and, if the challenge is successful to have the data erased, rectified, completed or amended.

(8) 説明責任の原則（Accountability Principle）

データ管理者は，上述の諸原則に実効性を与える措置を遵守していることに関し，説明責任を負うべきである。

A data controller should be accountable for complying with measures which give effect to the principles stated above.

この 1980 年のガイドラインの 8 原則は，しばしば「プライバシー保護 8 原則」と呼ばれますが，その実質的な内容は「個人データ保護」のための 8 原則です。

1980 年のガイドラインの 8 原則は， EU（旧 EC）の個人データ保護指令 95/46/EC に対して強い影響を与え，それらの法規に定める法規範の骨格部分とも一致しています。そのことから，個人データ保護指令 95/46/EC の法解釈においても OECD の 1980 年のガイドラインの 8 原則の理解が必須となっています。

また，1980 年のガイドラインの 8 原則は，日本国における個人情報保護と関連する法制の内容とその発展の歴史を理解する上でも重要なものです。

他方，2013 年のフレームワークは，個人データ保護指令 95/46/EC の全面改正法令である一般データ保護規則(EU) 2016/679（GDPR）に対して強い影響を与えました。

2013 年のフレームワークに含まれている基本原則は，1980 年のガイドラインの中で示されている 8 原則をそのまま踏襲するものです。
それゆえ，一般データ保護規則(EU) 2016/679（GDPR）に含まれている個人データ保護のための基本原則は，OECD の 8 原則を踏襲するものだと言えます。

なお，個人データ保護のための 8 原則以外の様々な手順等に関し，2013 年のフレームワークによって改訂・増補が行われています。そのようにして改訂された内容が，一般データ保護規則(EU) 2016/679（GDPR）にも大きく反映されています。

CoE 条約の場合と同様，OECD の 1980 年のガイドライン及び 2013 年のフレームワークに含まれている基本原則は，OECD の基本原則の影響を受けた EU の個人データ保護指令 95/46/EC 及び一般データ保護規則(EU) 2016/679（GDPR）の基本原則と共に，日本国の個人情報保護法制に対しても大きな影響を与えています。
OECD の基本原則と日本国の個人情報保護法（平成 15 年法律第 57 号）の関連条項との対応関係は，以下のとおりです。

(1) 収集制限の原則 → 個人情報保護法第 3 条の法解釈，第 18 条
(2) データ品質の原則 → 個人情報保護法第 22 条
(3) 目的の特定の原則 → 個人情報保護法第 17 条
(4) 利用の限定の原則 → 個人情報保護法第 18 条
(5) 安全確保の原則 → 個人情報保護法第 23 条
(6) 公開性の原則 → 個人情報保護法第 32 条
(7) 個人の参加の原則 → 個人情報保護法第 33 条，第 34 条，第 35 条
(8) 説明責任の原則 → 個人情報保護法第 36 条，第 37 条

2.5 自己情報コントロール権は存在するか？

OECD の 1980 年のガイドライン及び 2013 年のフレームワークは，いわゆる「自己情報コントロール権」の理論を承認する趣旨の文書ではありません。OECD の 8 原則の中にある「関与の権利」は，自己情報コントロール権の一種ではありません。
世界の判例法をみると，自己情報コントロール権の理論は，米国の連邦最高裁の判例法によって明確に否定されています。EU の構成国の中で，自己情報コントロール権を定める法令をもつ国はありません。
つまり，そのような権利は，世界中のどこにも存在しません。
仮に自己に関する情報を完全に管理できる権利が存在するとすれば，ある者（A）は，他の者（B）の脳内の記憶にアクセスして A に関する情報の有無及びその内容を管理できるはずです。

しかし，一般に，私人対私人の関係において，相手方の同意なしに相手方の思考内容にアクセスできる権利は存在しません。
公権力対私人の関係においても当該私人の同意なしに当該私人の思考内容に公権力機関がアクセスする権限は認められていないばかりか，逆に，日本国憲法をはじめ世界各国の憲法の人権保障条項は，国民の思想・信条の自由や国家による自白の強要の禁止を定めています。したがって，国家の権力者や公務員が，国民に対し，当該権力者や公務員が個々の国民によってどのように理解されているかを強制的に調べる権限は認められず，脳内の様子を自白するように強要する

ことも認められません。

他者に対して権利行使できる権利という意味での「自己情報コントロール権」が存在するとすれば，思想・信条の自由が存在しないのと同じことになりますし，プライバシーが存在しないことと同じ状態になります。その結果，個人の自由を基盤とする世界は破滅します。

要するに，個人の尊厳と自由を基本的な価値として尊重する国家においては，他者に対して権利行使できる権利という意味での「自己情報コントロール権」が存立する余地がありません。

> 機械処理または自動処理されている個人データの中で，当該個人データの本人が事業者に対して処理を委任した場合（例:クラウド上のストレージの利用者が自分の個人データを含むファイル等をそのストレージの中で保存するような場合），当該委任したデータの処理が適正に行われているかどうかの管理状況の説明を請求できることや，当該委任が終了した際に当該データの消去または返還を請求できることは，民法に定める委任契約及びそれに類する契約の性質上当然のことです。
> 委任契約に基づくこれらの請求は，憲法上の基本人権の一種としての「自己情報コントロール権」の行使として実行されるものではなく，民法上の権利の通常の行使の一形態に過ぎません。
> EU の一般データ保護規則(EU) 2016/679（GDPR）の中で定められた個人データの可搬性（portability）の権利もまた同じであり，もともと当該個人データの本人が保有しており，事業者（A）に対してその管理・運営を委任していたファイルやデータを別の事業者（B）に移転することを当初の事業者（A）に対して請求できる権利であり，これもまた民法上の権利の通常の行使の一形態に過ぎないと理解することが可能です。
>
> 一般に，憲法や行政法の分野に属する事柄しか知らないとこのような民法解釈上の当然の事理を認識できなくなるかもしれないので，そのような偏った思考しかできないようになってしまうことを避けるため，大学法学部の学生としては，民法（特に財産法）の中で定められている基本的な事柄についても可能な限り広範かつ適正に理解しているべきです。

3　日本国における個人情報保護法の立法史

3.1　最初の個人情報保護法令

日本国において最初に制定された個人情報保護法令は，行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律（昭和 63 年法律第 95 号・旧行政機関個人情報保護法）です。

旧行政機関個人情報保護法の第 1 条（目的）は，「この法律は，行政機関における個人情報の電子計算機による処理の進展にかんがみ，行政機関の保有する電子計算機処理に係る個人情報の取扱いに関する基本的事項を定めることにより，行政の適正かつ円滑な運営を図りつつ，個人の権利利益を保護することを目的とする」と定めています。

旧行政機関個人情報保護法の第 2 条第 2 号における「個人情報」の定義は，「生存する個人に関する情報であって，当該情報に含まれる氏名，生年月日その他の記述又は個人別に付された番号，記号その他の符号により当該個人を識別できるもの（当該情報のみでは識別できないが，他の情報と容易に照合することができ，それにより当該個人を識別できるものを含む。）をいう。ただし，法人その他の団体に関して記録された情報に含まれる当該法人その他の団体の役員に関する情報を除く」でした。

この定義を読むと，現行の個人情報保護法における定義とあまり変わりのないものであるということに気づくはずです。

旧行政機関個人情報保護法が制定された当時において，民間企業に対して適用される個人情報保護のための立法が同時に行われなかったのは，当時の産業界において，「個人情報を保護していたのでは，企業活動など全くできなくなってしまう」という（個人情報保護に対して強く否定的・拒否的な）考え方が企業経営者の中では支配的だったからです。

旧行政機関個人情報保護法の第 2 条第 3 号は，「電子計算機処理」を「電子計算機を使用して行われる情報の入力，蓄積，編集，加工，修正，更新，検索，消去，出力又はこれらに類する処理をいう。ただし，専ら文章を作成し，又は文書図画の内容を記録するための処理その他の政令で定める処理を除く」と定義しています。

また，同条第 4 号は，「個人情報ファイル」を「一定の事務の目的を達成するために体系的に構成された個人情報の集合物であって，電子計算機処理を行うため磁気テープ，磁気ディスクその他これらに準ずる方法により一定の事項を確実に記録しておくことができる物（以下「磁気テープ等」という。）に記録されたものをいう」と定義しています。

いずれの定義の表現に関しても古臭く感じられるかもしれません。
しかし，どのような時代状況を反映してこの法令が制定されたのかを理解する上では，非常に重要な用語例だと言えます。

他方，同条第 5 号は，「処理情報」を「個人情報ファイルに記録されている個人情報をいう」と定義しています。
この「処理」は，「processing」に対応するもので，概念内容を明確に示すことのできる表現を用いていました。

旧行政機関個人情報保護法は，立法技術という観点からは世界的に標準的な語彙を用いた適切な法令だったと評価できます。

また，旧行政機関個人情報保護法は，全体として，OECD の 1980 年ガイドランの基本原則を基礎として構築されている部分が少なくなく，その意味で，個人データの保護という観点からは，非常にわかりやすい法令だったと言えます。

3. 2 平成 15 年における立法整備

平成 15 年, 民間企業等の個人情報取扱事業者に適用される個人情報の保護に関する法律（平成 15 年法律第 57 号・個人情報保護法），行政機関に適用される行政機関の保有する個人情報の保護に関する法律（平成 15 年法律第 58 号・行政機関個人情報保護法）及び独立行政法人等に適用される独立行政法人等の保有する個人情報の保護に関する法律（平成 15 年法律第 59 号・独立行政法人等個人情報保護法）という 3 つの法令が制定されました。

行政機関個人情報保護法の制定により，旧行政機関個人情報保護法は廃止されました。

一般に，これらの平成 15 年（2003）に整備された日本国の個人情報保護法令は，CoE の個人データ保護条約に適合させるためではなく，旧 EC（現在の EU）の個人データ保護指令 95/46/EC の第 25 条の中で定められた「十分性」の要件を充足するために制定されたものだと言われています。

> 個人データ保護指令 95/46/EC の十分性の要件を満たしているときは，EU（旧 EC）の構成国ではない第三国であっても，「EU（旧 EC）の域内と同レベルの十分な個人データ保護が存在する」と欧州委員会が判定するときは，（個別の協定や認定を経ることなく包括的に）EU（旧 EC）の構成国と当該第三国との間で個人データのやりとりを実行できます。
> 個人データ保護指令 95/46/EC によって定められた十分性の要件を満たしていない場合，例えば，日本国内に拠点のある日本企業は，個別の政府間協定を締結しない限り，または，当該支店や代理店等が所在する EU の構成国の職務権限のある当局から個別の許可・承認を得ない限り，EU 域内に所在する支店や代理店との間で自社が管理する従業者データや顧客データのような個人データのやりとりができなくなります。これは極めて煩瑣なことであり，円滑な企業経営を困難にするものです。
> 日本国は，EU（旧 EC）からみて「第三国」に該当します。
>
> 日本国の企業にとって EU（旧 EU）の構成国は非常に重要な取引相手が存在する諸国ですので，個人データ保護指令 95/46/EC が制定されたことによって，日本国の企業の経営者の誰もが個人情報（個人データ）の保護ための EU（旧 EC）の法制と同等の日本国の法制をもつことに反対できなくなってしまったのだと理解することが可能です。

日本国において，一般的な個人情報保護法令が存在するということは，それ自体として，旧 EC（EU）におけるのと同様の十分な保護を与える国だということを示す証拠となり得ます。

その後，一般データ保護規則(EU) 2016/679（GDPR）が制定されました。この立法により，個人データ保護指令 95/46/EC は廃止されました。
個人データ保護指令 95/46/EC によって定められた十分性の要件は，同指令の後継法令としての GDPR の第 45 条に承継されています。

そして，2019 年，日本国は，個人データ保護指令 95/46/EC を承継する GDPR の第 45 条にも基づく「十分性の判定」を得ました。

それゆえ，GDPR が適用される環境の下においても，十分性の要件を満たすことによって，個別の協定や許可等を要することなく，EU の構成国と日本国との間で支障なく個人データをやりとりできます。

> 日本国における個人情報保護法の制定過程においては，個人データ保護指令 95/46/EC への対応だけが検討されたわけではありません。
> それよりもだいぶ前の時点から，多方面にわたり，民間企業等にも適用される法令の必要性が検討されていました。しかし，当時，民間企業に適用される個人情報保護法令の制定に反対する意見が非常に強く，立法が難航しました。
> それにもかかわらず日本国が個人情報保護法制をもつようになった実質的な要因としては，個人データ保護指令 95/46/EC が旧 EC（EU）域内の構成国内に事業所をもつ企業や旧 EC（EU）構成国内にある企業と取引している民間企業にとって死活問題となり得る要素（十分性の要件）を含んでいたためだと考えられます。

一般に，日本国において制定された個人情報保護の各法令及び地方公共団体（地方自治体）が制定している個人情報保護条例によって，全ての分野を網羅する個人情報保護法制が存在すると理解されています。
しかし，天皇，国会及び裁判所に適用される個人情報保護法令は存在しません。

3. 2. 1 個人情報保護法

個人情報保護法（平成 15 年法律第 57 号）は，基本的には，公権力主体ではない個人情報取扱事業者に対して適用される法律として制定されました。

個人情報保護法は，個人情報取扱事業者の義務を定め，個人情報取扱事業者に対する行政監督，義務違反行為に対する行政上の制裁と罰則を定める行政法規です。

個人情報保護法は，平成 15 年以降にも一部改正が行われています。

デジタル社会の形成を図るための関係法律の整備に関する法律（令和 3 年法律第 37 号）による一部改正後の個人情報保護法の第 1 条（目的）は，「この法律は、デジタル社会の進展に伴い個人情報の利用が著しく拡大していることに鑑み、個人情報の適正な取扱いに関し、基本理念及び政府による基本方針の作成その他の個人情報の保護に関する施策の基本となる事項を定め、国及び地方公共団体の責務等を明らかにし、個人情報を取り扱う事業者及び行政機関等についてこれらの特性に応じて遵守すべき義務等を定めるとともに、個人情報保護委員会を設置することにより、行政機関等の事務及び事業の適正かつ円滑な運営を図り、並

びに個人情報の適正かつ効果的な活用が新たな産業の創出並びに活力ある経済社会及び豊かな国民生活の実現に資するものであることその他の個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的とする」と定めています。

個人情報保護法は，個人情報取扱事業者の義務を定めています。この義務は，本質的には，行政監督のための判断基準としての義務です。
それゆえ，個人情報保護法に定める義務が個人情報取扱事業者の義務の全てであるということにはなりません。

> 個人情報（個人データ）と関連する保護法益に関し，誰かの（故意または過失による）加害行為によって，個人情報の本人に対して何らかの被害が生じた場合，個人情報保護法によってその救済が得られるわけではありません。
>
> 個人情報取扱事業者の義務違反行為が個人情報の本人に対して何らかの法益侵害（名誉毀損，侮辱，信用毀損，業務妨害，強要，脅迫，通信の秘密侵害等）を発生させる場合，(1)適用可能な刑罰法令による処罰が問題となり，また，(2)民法上の不法行為（民法第 709 条）または債務不履行（民法第 415 条以下）等を原因とする民事訴訟による損害賠償請求等が問題となり得ます。
> このことは，個人情報取扱事業者ではない者による刑法上及び民法上の一般的な義務の違反行為による同様の法益侵害においても同じです。
> ただし，個人情報（個人データ）と関連する保護法益を侵害する加害者が国及びその機関のような公権力主体である場合には，国家賠償法（昭和 22 律第 125 号）を根拠法令とする損害賠償請求等が行われ得ます。
>
> これらいずれの場合においても，個人情報保護法を根拠法令として損害賠償請求が行われ得るわけではありません。また，日本国の国家体制の下においては，日本国憲法を根拠法令とする私人（国民）の損害賠償請求という法制度は存在しません。
> つまり，個人情報と関係して現実に何らかの被害が発生した場合における法的対処は，その大部分において，個人情報保護法や日本国憲法の解釈・適用の問題になるのではなく，刑法等の刑罰法令及び民法等の諸々の民事法令の解釈・適用の問題となります。
>
> それゆえ，個人情報の法的保護に関しては，個人情報保護法だけではなく，刑法や民法等の基本的な法令に関する十分な理解が必須です。

個人情報取扱事業者は，刑法及び民法を含め，全ての法令を遵守すべき国法上の義務があります。
それゆえ，個人情報取扱事業者が負うべき法的義務を理解するためには，個人情報保護法に定める義務に限定することなく，適用可能な全ての法令に基づく法的義務を検討しなければなりません。

> 一般に，個人情報保護に限らず，（知的財産権の分野を含め）特定の法分野の専門家になろうとする

ときは，まず，日本国の法制度全体について十分な理解を得ていることが必須の前提となります。

一般に，法制度に限らず，どの分野においても，そもそも当該分野の「全体」を理解し，その全体像を掴んでいるのでなければ，当該個別の分野が「全体」の中での特定の「部分」を理解することを理解することは不可能です。大は小を兼ねますが，小が大を兼ねることはありません。

結局，時間がかかっても，全体の構造（structure）を理解することが大事です。

3. 2. 2 行政機関個人情報保護法

平成 15 年の法制整備の際，行政機関に適用される個人情報保護法として，行政機関の保有する個人情報の保護に関する法律（平成 15 年法律第 58 号・行政機関個人情報保護法）が制定されました。

行政機関個人情報保護法は，デジタル社会の形成を図るための関係法律の整備に関する法律によって廃止されました。
この行政機関個人情報保護法の廃止の後，従来は行政機関個人情報保護法の中で定められていた事項の主要部分は，個人情報保護法（平成 15 年法律第 57 号）の中に組込まれました。

3. 2. 3 独立行政法人等個人情報保護法

独立行政法人とは，独立行政法人通則法（平成 11 年法律第 103 号）の中で定められた独立行政法人のことを意味します。独立行政法人には，中期目標管理法人，国立研究開発法人，行政執行法人が含まれます（同法第 2 条参照）。

平成 15 年の法制整備の際，独立行政法人通則法に定める独立行政法人等に適用される個人情報保護法として，独立行政法人等の保有する個人情報の保護に関する法律（平成 15 年法律第 59 号・独立行政法人等個人情報保護法）が制定されました。

独立行政法人等個人情報保護法は，デジタル社会の形成を図るための関係法律の整備に関する法律によって廃止されました。
この独立行政法人等個人情報保護法の廃止の後，従来は独立行政法人等個人情報保護法の中で定められていた事項の主要部分は，個人情報保護法（平成 15 年法律第 57 号）の中に組込まれました。

法と情報雑誌に収録されている参考訳のリスト

（1 巻 1 号から 11 巻 4 号まで）

このリストは，参考訳が作成された法令等のカテゴリや年代等を把握しやすくすることを主たる狙いとしている。

参考訳を作成した文書名は，略記表記となっている。そのため，実際の参考訳の表題とは異なっていることがある。なお，法と情報雑誌の表示にある目次内の誤記等は補正してある。

参考訳作成者名は，敬称等抜きの略称で表記してある。本来の氏名・所属は次のとおり。

丸橋： 丸橋 透（明治大学法学部専任教授）
小西： 小西知世（明治大学法学部専任教授）
夏井： 夏井高人（元明治大学法学部専任教授）

文書の名称	作成者	号	巻・頁	年
（欧州議会及び理事会が採択した法令）	夏井			
規則(EU) 2025/38（サイバー結束法） [参考訳]	夏井	72 号	11 巻 1 号 1～107 頁	2026
規則(EU) 2024/1689（人工知能法） [前文の参考訳]	夏井	57 号	9 巻 3 号 1～130 頁	2024
規則(EU) 2024/1689（人工知能法） [第 1 条～第 63 条の参考訳]	夏井	58 号	9 巻 4 号 1～143 頁	2024
規則(EU) 2024/1689（人工知能法） [第 64 条～第 113 条の参考訳]	夏井	59 号	9 巻 5 号 1～88 頁	2024
規則(EU) 2024/1689（人工知能法） [別紙の参考訳]	夏井	59 号	9 巻 5 号 89～145 頁	2024
規則(EU) 2024/2847（サイバー回復力法） [参考訳]	夏井	63 号	10 巻 2 号 1～246 頁	2025
規則(EU) 2023/2854（データ法） [参考訳]	夏井	69 号	10 巻 8 号 1～203 頁	2025
規則(EU) 2023/1543 [参考訳]	丸橋	62 号	10 巻 1 号 1～165 頁	2025
規則(EU) 2022/2554 [参考訳]	夏井	66 号	10 巻 5 号 1～234 頁	2025
規則(EU) 2022/2065（デジタルサービス法）[参考訳]	夏井	52 号	8 巻 2 号 1～299 頁	2023
規則(EU) 2022/1925（デジタル市場法） [参考訳]	夏井	70 号	10 巻 9 号 1～187 頁	2025
規則(EU) 2022/868（データ統治法）[参考訳]	夏井	53 号	8 巻 3 号 1～130 頁	2023
規則(EU) 2022/850 [参考訳]	夏井	55 号	9 巻 1 号 1～57 頁	2024
規則(EU) 2021/1232 [参考訳]	夏井	46 号	6 巻 6 号 219～255 頁	2021
規則(EU) 2021/1149 [参考訳]	夏井	43 号	6 巻 3 号 1～103 頁	2021
規則(EU) 2021/1148 [参考訳]	夏井	43 号	6 巻 3 号 104～220 頁	2021
規則(EU) 2021/887 [参考訳]	夏井	42 号	6 巻 2 号 1～95 頁	2021
規則(EU) 2021/818 [参考訳]	夏井	44 号	6 巻 4 号 265～343 頁	2021
規則(EU) 2021/785 [参考訳]	夏井	44 号	6 巻 4 号 1～37 頁	2021
規則(EU) 2021/784 [参考訳]	夏井	46 号	6 巻 6 号 256～338 頁	2021

規則(EU) 2021/694 [参考訳・改訂版]	夏井	74 号	11 巻 3 号 1～122 頁	2026
規則(EU) 2021/694 [参考訳]	夏井	41 号	6 巻 1 号 1～104 頁	2021
規則(EU) 2021/693 [参考訳]	夏井	44 号	6 巻 4 号 440～486 頁	2021
規則(EU) 2020/1784 [参考訳]	夏井	45 号	6 巻 5 号 82～159 頁	2021
規則(EU) 2020/1783 [参考訳]	夏井	45 号	6 巻 5 号 1～81 頁	2021
規則(EU) 2019/1150 [参考訳]	夏井	71 号	10 巻 10 号 1～69 頁	2025
指令(EU) 2019/884 [参考訳]	丸橋	36 号	4 巻 6 号 149～161 頁	2019
規則(EU) 2019/881（サイバーセキュリティ法） [参考訳・改訂版]	夏井	38 号	4 巻 8 号 16～86 頁	2019
規則(EU) 2019/881（サイバーセキュリティ法） [参考訳]	夏井	37 号	4 巻 7 号 1～70 頁	2019
規則(EU) 2019/880 [参考訳]	夏井	47 号	7 巻 1 号 222～261 頁	2022
規則(EU) 2019/818 [参考訳]	丸橋	37 号	4 巻 7 号 156～221 頁	2019
規則(EU) 2019/817 [参考訳]	丸橋	37 号	4 巻 7 号 78～155 頁	2019
規則(EU) 2019/816 [参考訳]	丸橋	36 号	4 巻 6 号 176～208 頁	2019
規則(EU) 2018/1971 [参考訳]	夏井	33 号	4 巻 3 号 1～41 頁	2019
規則(EU) 2018/1862 [参考訳]	夏井	36 号	4 巻 6 号 1～70 頁	2019
規則(EU) 2018/1861 [参考訳]	夏井	34 号	4 巻 4 号 89～146 頁	2019
規則(EU) 2018/1860 [参考訳]	夏井	34 号	4 巻 4 号 69～88 頁	2019
規則(EU) 2018/1807 [参考訳]	夏井	31 号	4 巻 1 号 82～100 頁	2019
規則(EU) 2018/1805 [参考訳]	夏井	36 号	4 巻 6 号 71～122 頁	2019
規則(EU) 2018/1727 [参考訳]	夏井	35 号	4 巻 5 号 1～60 頁	2019
規則(EU) 2018/1726 [参考訳・改訂版]	夏井	75 号	11 巻 4 号 1～129 頁	2026
規則(EU) 2018/1726 [参考訳]	夏井	33 号	4 巻 3 号 138～188 頁	2019
規則(EU) 2018/1725 [参考訳]	夏井	31 号	4 巻 1 号 1～81 頁	2019
規則(EU) 2018/1724 [参考訳]	夏井	31 号	4 巻 1 号 101～151 頁	2019
規則(EU) 2018/1241 [参考訳]	夏井	34 号	4 巻 4 号 1～7 頁	2019
規則(EU) 2018/1240 [参考訳]	夏井	33 号	4 巻 3 号 42～137 頁	2019
規則(EU) 2018/302 [参考訳]	夏井	35 号	4 巻 5 号 119～142 頁	2019
規則(EU) 2017/2394 [参考訳]	夏井	24 号	3 巻 6 号 1～36 頁	2018
規則(EU) 2017/2226 [参考訳・改訂版]	丸橋	33 号	4 巻 3 号 233～329 頁	2019
規則(EU) 2017/2226 [参考訳]	丸橋	21 号	3 巻 3 号 201～300 頁	2018
規則(EU) 2017/1939 [参考訳]	夏井	19 号	3 巻 1 号 1～91 頁	2018
規則(EU) 2017/1563 [参考訳]	夏井	17 号	2 巻 11 号 42～50 頁	2017
規則(EU) 2017/1128 [参考訳]	夏井	24 号	3 巻 6 号 114～132 頁	2018
規則(EU) 2017/625 [参考訳]	夏井	48 号	7 巻 2 号 1～357 頁	2022
規則(EU) 2017/458[参考訳]	夏井	13 号	2 巻 7 号 83～96 頁	2017
規則(EU) 2016/1624 [参考訳]	夏井	12 号	2 巻 6 号 1～98 頁	2017
規則(EU) 2016/794（一部改正後） [参考訳]	夏井	34 号	4 巻 4 号 8～68 頁	2019

規則(EU) 2016/794 [参考訳]	夏井	9 号	2 巻 3 号 1～101 頁	2017
指令(EU) 2016/681 [参考訳]	夏井	9 号	2 巻 3 号 119～155 頁	2017
規則(EU) 2016/679（一般データ保護規則）[参考訳・再訂版]	夏井	23 号	3 巻 5 号 1～114 頁	2018
規則(EU) 2016/679（一般データ保護規則）[参考訳・改訂版]	夏井	11 号	2 巻 5 号 188～331 頁	2017
規則(EU) 2016/679（一般データ保護規則）[参考訳]	夏井	3 号	1 巻 3 号 1～186 頁	2016
規則(EU) 2016/589 [参考訳]	夏井	23 号	3 巻 5 号 133～167 頁	2018
規則(EU) 2016/399（シェンゲンボーダーコード）[参考訳]	夏井	13 号	2 巻 7 号 1～82 頁	2017
規則(EU) 2015/1525 [参考訳]	夏井	43 号	6 巻 3 号 409～443 頁	2021
規則(EU) No 910/2014 [参考訳]	夏井	16 号	2 巻 10 号 147～196 頁	2017
規則(EU) No 600/2014 [参考訳]	夏井	22 号	3 巻 4 号 1～79 頁	2018
規則(EU) No 1295/2013 [参考訳]	夏井	17 号	2 巻 11 号 121～155 頁	2017
規則(EU) No 608/2013 [参考訳]	夏井	44 号	6 巻 4 号 132～197 頁	2021
規則(EU) No 526/2013 [参考訳]	夏井	25 号	3 巻 7 号 263～292 頁	2018
規則(EU) No 524/2013 [参考訳]	夏井	24 号	3 巻 6 号 61～83 頁	2018
規則(EU) No 1151/2012 [参考訳]	夏井	48 号	7 巻 2 号 506～598 頁	2022
規則(EU) No 1024/2012 [参考訳]	夏井	15 号	2 巻 9 号 93～114 頁	2017
規則(EU) No 648/2012 [参考訳]	夏井	26 号	3 巻 8 号 1～96 頁	2018
規則(EU) No 182/2011 [参考訳]	夏井	23 号	3 巻 5 号 168～179 頁	2018
規則(EC) No 1211/2009 [参考訳]	夏井	28 号	3 巻 10 号 1～17 頁	2018
規則(EC) No 767/2008（VIS 規則） [参考訳]	夏井	11 号	2 巻 5 号 1～59 頁	2017
規則(EC) No 766/2008 [参考訳]	夏井	43 号	6 巻 3 号 312～351 頁	2021
規則(EC) No 2006/2004 [参考訳]	夏井	24 号	3 巻 6 号 37～56 頁	2018
規則(EC) No 444/2009 [参考訳]	夏井	13 号	2 巻 7 号 118～129 頁	2017
規則(EC) No 1049/2001 [参考訳]	夏井	9 号	2 巻 3 号 102～118 頁	2017
規則(EC) No 45/2001 [参考訳・改訂版]	夏井	11 号	2 巻 5 号 111～146 頁	2017
規則(EC) No 45/2001 [参考訳]	夏井	2 号	1 巻 2 号 34～73 頁	2016
規則(EC) 2887/2000 [参考訳]	夏井	28 号	3 巻 10 号 64～74 頁	2018
規則(EC) No 1073/1999 [参考訳]	夏井	9 号	2 巻 3 号 156～171 頁	2017
規則(EU, Euratom) 2023/2841 [参考訳]	夏井	73 号	11 巻 2 号 1～82 頁	2026
規則(EU, Euratom) 2020/2223 [参考訳]	夏井	42 号	6 巻 2 号 153～230 頁	2021
規則(EU, Euratom) 2016/2030 [参考訳]	夏井	42 号	6 巻 2 号 143～152 頁	2021
規則(EU, Euratom) No 883/2013 [参考訳・改訂版]	夏井	42 号	6 巻 2 号 231～311 頁	2021
規則(EU, Euratom) No 883/2013 [参考訳]	夏井	10 号	2 巻 4 号 1～35 頁	2017
指令(EU) 2024/2853 [参考訳]	夏井	64 号	10 巻 3 号 1～80 頁	2025
指令(EU) 2024/1203 [参考訳]	夏井	61 号	9 巻 7 号 1～81 頁	2024
指令(EU) 2023/1544 [参考訳]	丸橋	62 号	10 巻 1 号 166～200 頁	2025
指令(EU) 2023/977 [参考訳]	夏井	55 号	9 巻 1 号 63～132 頁	2024

指令(EU) 2022/2557 [参考訳]	夏井	54 号	8 巻 4 号 207～303 頁	2023
指令(EU) 2022/2555（NIS2 指令）[参考訳]	夏井	54 号	8 巻 4 号 1～206 頁	2023
指令(EU) 2019/1024 [参考訳]	夏井	39 号	5 巻 1 号 57～136 頁	2020
指令(EU) 2019/790 [参考訳]	夏井	47 号	7 巻 1 号 1～113 頁	2022
指令(EU) 2018/1972 [参考訳]	夏井	32 号	4 巻 2 号 1～212 頁	2019
指令(EU) 2017/1564 [参考訳]	夏井	17 号	2 巻 11 号 27～41 頁	2017
指令(EU) 2017/1371 [参考訳]	夏井	19 号	3 巻 1 号 92～109 頁	2018
指令(EU) 2017/541 [参考訳]	夏井	14 号	2 巻 8 号 1～29 頁	2017
指令(EU) 2016/1148 [参考訳・再訂版]	夏井	46 号	6 巻 6 号 467～548 頁	2021
指令(EU) 2016/1148 [参考訳・改訂版]	夏井	14 号	2 巻 8 号 120～163 頁	2017
指令(EU) 2016/1034 [参考訳]	夏井	21 号	3 巻 3 号 176～180 頁	2018
指令(EU) 2016/943 [参考訳]	夏井	15 号	2 巻 9 号 489～514 頁	2017
指令(EU) 2016/680 [参考訳・改訂版]	夏井	46 号	6 巻 6 号 339～466 頁	2021
指令(EU) 2016/680 [参考訳]	夏井	7 号	2 巻 1 号 41～140 頁	2017
指令(EU) 2015/2366 [参考訳]	夏井	20 号	3 巻 2 号 1～115 頁	2018
指令(EU) 2015/1535 [参考訳]	夏井	25 号	3 巻 7 号 1～20 頁	2018
指令(EU) 2015/849（改正後） [参考訳]	夏井	26 号	3 巻 8 号 276～328 頁	2018
指令(EU) 2015/849 [参考訳]	夏井	20 号	3 巻 2 号 140～198 頁頁	2018
指令 2014/65/EU [参考訳]	夏井	21 号	3 巻 3 号 1～175 頁	2018
指令 2014/60/EU [参考訳]	夏井	47 号	7 巻 1 号 381～409 頁	2022
指令 2014/42/EU [参考訳]	夏井	25 号	3 巻 7 号 246～262 頁	2018
指令 2014/41/EU [参考訳]	夏井	25 号	3 巻 7 号 199～245 頁	2018
指令 2014/26/EU [参考訳]	夏井	44 号	6 巻 4 号 344～439 頁	2021
指令 2013/40/EU[参考訳・改訂版]	夏井	14 号	2 巻 8 号 164～185 頁	2017
指令 2013/40/EU[参考訳]	夏井	1 号	1 巻 1 号 51～61 頁	2016
指令 2013/37/EU [参考訳]	夏井	15 号	2 巻 9 号 1～25 頁	2017
指令 2013/11/EU [参考訳]	夏井	24 号	3 巻 6 号 84～113 頁	2018
指令 2012/28/EU [参考訳]	夏井	17 号	2 巻 11 号 105～120 頁	2017
指令 2011/77/EU（改正後） [参考訳]	夏井	47 号	7 巻 1 号 193～209 頁	2022
指令 2011/77/EU [参考訳]	夏井	17 号	2 巻 11 号 88～99 頁	2017
指令 2011/24/EU [参考訳]	夏井	24 号	3 巻 6 号 133～169 頁	2018
指令 2010/40/EU [参考訳]	夏井	15 号	2 巻 9 号 26～47 頁	2017
指令 2010/13/EU [参考訳]	夏井	18 号	2 巻 12 号 24～72 頁	2017
指令 2009/147/EC [参考訳]	夏井	61 号	9 巻 7 号 82～105 頁	2024
指令 2009/140/EC [参考訳]	夏井	29 号	3 巻 11 号 46～98 頁	2018
指令 2009/136/EC [参考訳]	夏井	29 号	3 巻 11 号 1～45 頁	2018
指令 2009/110/EC [参考訳]	夏井	18 号	2 巻 12 号 1～23 頁	2017

指令 2009/24/EC [参考訳・改訂版]	夏井	47 号	7 巻 1 号 114〜134 頁	2022
指令 2009/24/EC [参考訳]	夏井	17 号	2 巻 11 号 51〜62 頁	2017
指令 2008/99/EC [参考訳]	夏井	35 号	4 巻 5 号 143〜160 頁	2019
指令 2007/2/EC [参考訳]	夏井	15 号	2 巻 9 号 1〜25 頁	2017
指令 2006/123/EC [参考訳]	夏井	30 号	3 巻 12 号 1〜56 頁	2018
指令 2006/116/EC（改正後）[参考訳]	夏井	47 号	7 巻 1 号 174〜192 頁	2022
指令 2006/116/EC [参考訳]	夏井	17 号	2 巻 11 号 77〜87 頁	2017
指令 2006/115/EC [参考訳]	夏井	17 号	2 巻 11 号 63〜76 頁	2017
指令 2006/24/EC [参考訳・改訂版]	夏井	69 号	10 巻 8 号 204〜231 頁	2025
指令 2006/24/EC [参考訳]	夏井	5 号	1 巻 5 号 47〜65 頁	2016
指令 2004/82/EC [参考訳]	夏井	11 号	2 巻 5 号 60〜70 頁	2017
指令 2004/48/EC [参考訳]	夏井	44 号	6 巻 4 号 38〜74 頁	2021
指令 2004/23/EC [参考訳]	夏井	24 号	3 巻 6 号 170〜191 頁	2018
指令 2003/98/EC [参考訳]	夏井	15 号	2 巻 9 号 48〜59 頁	2017
指令 2002/58/EC [参考訳・改訂版]	夏井	11 号	2 巻 5 号 158〜187 頁	2017
指令 2002/58/EC [参考訳]	夏井	2 号	1 巻 2 号 117〜162 頁	2016
指令 2002/22/EC（改正後）[参考訳]	夏井	27 号	3 巻 9 号 59〜87 頁	2018
指令 2002/22/EC [参考訳]	夏井	27 号	3 巻 9 号 88〜129 頁	2018
指令 2002/21/EC（改正後）[参考訳]	夏井	27 号	3 巻 9 号 31〜58 頁	2018
指令 2002/21/EC [参考訳]	夏井	25 号	3 巻 7 号 76〜108 頁	2018
指令 2002/20/EC（改正後）[参考訳]	夏井	27 号	3 巻 9 号 17〜30 頁	2018
指令 2002/20/EC [参考訳]	夏井	26 号	3 巻 8 号 352〜374 頁	2018
指令 2002/19/EC（改正後）[参考訳]	夏井	27 号	3 巻 9 号 1〜16 頁	2018
指令 2002/19/EC [参考訳]	夏井	26 号	3 巻 8 号 329〜351 頁	2018
指令 2001/29/EC [参考訳]	夏井	17 号	2 巻 11 号 1〜26 頁	2017
指令 2000/31/EC [参考訳]	夏井	19 号	3 巻 1 号 110〜141 頁	2018
指令 1999/34/EC [参考訳]	夏井	16 号	2 巻 10 号 292〜296 頁	2017
指令 98/48/EC [参考訳]	夏井	25 号	3 巻 7 号 51〜66 頁	2018
指令 98/34/EC [参考訳]	夏井	25 号	3 巻 7 号 21〜39 頁	2018
指令 98/10/EC [参考訳]	夏井	27 号	3 巻 9 号 130〜165 頁	2018
指令 97/66/EC [参考訳・改訂版]	夏井	25 号	3 巻 7 号 109〜123 頁	2018
指令 97/66/EC [参考訳]	夏井	5 号	1 巻 5 号 66〜83 頁	2016
指令 97/33/EC [参考訳]	夏井	25 号	3 巻 7 号 146〜175 頁	2018
指令 97/13/EC [参考訳]	夏井	25 号	3 巻 7 号 124〜145 頁	2018
指令 97/7/EC [参考訳]	夏井	29 号	3 巻 11 号 127〜142 頁	2018
指令 97/4/EC [参考訳]	夏井	49 号	7 巻 3 号 187〜201 頁	2022
指令 96/9/EC [参考訳・改訂版]	夏井	18 号	2 巻 12 号 73〜92 頁	2017

指令 95/62/EC [参考訳]	夏井	27 号	3 巻 9 号 166～197 頁	2018
指令 95/47/EC [参考訳]	夏井	28 号	3 巻 10 号 75～84 頁	2018
指令 95/46/EC [参考訳・再訂版]	夏井	50 号	7 巻 4 号 1～66 頁	2022
指令 95/46/EC [参考訳・改訂版]	夏井	11 号	2 巻 5 号 332～365 頁	2017
指令 95/46/EC [参考訳]	夏井	5 号	1 巻 5 号 1～46 頁	2016
決定(EU) 2022/2481 [参考訳]	夏井	55 号	9 巻 1 号 133～199 頁	2024
決定 No 568/2009/EC [参考訳]	夏井	45 号	6 巻 5 号 188～210 頁	2021
決定 No 70/2008/EC [参考訳]	夏井	44 号	6 巻 4 号 198～222 頁	2021
決定 2004/387/EC [参考訳]	夏井	44 号	6 巻 4 号 223～264 頁	2021
（理事会が採択した法令）				
理事会規則(EU) 2019/796 [参考訳]	夏井	56 号	9 巻 2 号 38～64 頁	2024
理事会規則(EC) No 116/2009 [参考訳]	夏井	47 号	7 巻 1 号 339～358 頁	2022
理事会規則(EC) No 510/2006 [参考訳]	夏井	48 号	7 巻 2 号 464～505 頁	2022
理事会規則(EC) No 509/2006 [参考訳]	夏井	49 号	7 巻 3 号 27～60 頁	2022
理事会規則(EC) No 2252/2004[参考訳]	夏井	13 号	2 巻 7 号 104～117 頁	2017
理事会規則(EC) No 1383/2003 [参考訳]	夏井	44 号	6 巻 4 号 75～108 頁	2021
理事会規則(EC) No 692/2003 [参考訳]	夏井	48 号	7 巻 2 号 411～435 頁	2022
理事会規則(EC) No 535/97 [参考訳]	夏井	48 号	7 巻 2 号 390～399 頁	2022
理事会規則(EC) No 3295/94 [参考訳]	夏井	44 号	6 巻 4 号 109～131 頁	2021
理事会規則(EEC) No 3911/92 [参考訳]	夏井	47 号	7 巻 1 号 322～338 頁	2022
理事会規則(EEC) No 2082/92 [参考訳]	夏井	49 号	7 巻 3 号 1～26 頁	2022
理事会規則(EEC) No 2081/92 [参考訳]	夏井	48 号	7 巻 2 号 358～389 頁	2022
理事会規則(Euratom, EC) No 2185/96 [参考訳]	夏井	42 号	6 巻 2 号 112～127 頁	2021
理事会規則(EC, Euratom) No 2988/95 [参考訳]	夏井	42 号	6 巻 2 号 128～142 頁	2021
理事会指令 93/98/EEC [参考訳]	夏井	47 号	7 巻 1 号 153～173 頁	2022
理事会指令 93/13/EEC [参考訳]	夏井	29 号	3 巻 11 号 143～152 頁	2018
理事会指令 93/7/EEC [参考訳]	夏井	47 号	7 巻 1 号 359～380 頁	2022
理事会指令 92/44/EEC [参考訳]	夏井	29 号	3 巻 11 号 99～114 頁	2018
理事会指令 92/28/EEC [参考訳]	夏井	29 号	3 巻 11 号 160～170 頁	2018
理事会指令 91/250/EEC [参考訳]	夏井	47 号	7 巻 1 号 135～152 頁	2022
理事会指令 90/387/EEC [参考訳]	夏井	25 号	3 巻 7 号 176～192 頁	2018
理事会指令 89/395/EEC [参考訳]	夏井	49 号	7 巻 3 号 112～133 頁	2022
理事会指令 86/197/EEC [参考訳]	夏井	49 号	7 巻 3 号 104～111 頁	2022
理事会指令 85/374/EEC [参考訳]	夏井	16 号	2 巻 10 号 278～291 頁	2017
理事会指令 84/450/EEC [参考訳]	夏井	29 号	3 巻 11 号 153～159 頁	2018
理事会指令 83/189/EEC [参考訳]	夏井	25 号	3 巻 7 号 40～50 頁	2018

理事会指令 79/112/EEC [参考訳]	夏井	49 号	7 巻 3 号 61〜103 頁	2022
理事会枠組み指令 2005/222/JHA [参考訳]	夏井	35 号	4 巻 5 号 161〜169 頁	2019
理事会決定(EU) 2023/436 [参考訳]	夏井	54 号	8 巻 4 号 304〜324 頁	2023
理事会決定 2019/797/CFSP [参考訳]	夏井	56 号	9 巻 2 号 1〜37 頁	2024
理事会決定 2014/496/CFSP [参考訳]	夏井	29 号	3 巻 11 号 171〜177 頁	2018
理事会決定 2009/968/JHA [参考訳]	夏井	8 号	2 巻 2 号 140〜154 頁	2017
理事会決定 2009/936/JHA [参考訳]	夏井	8 号	2 巻 2 号 119〜139 頁	2017
理事会決定 2009/935/JHA [参考訳]	夏井	8 号	2 巻 2 号 114〜118 頁	2017
理事会決定 2009/934/JHA [参考訳]	夏井	8 号	2 巻 2 号 99〜113 頁	2017
理事会決定 2009/917/JHA [参考訳・改訂版]	夏井	43 号	6 巻 3 号 508〜550 頁	2021
理事会決定 2009/917/JHA [参考訳]	夏井	8 号	2 巻 2 号 1〜30 頁	2017
理事会決定 2009/902/JHA [参考訳]	夏井	43 号	6 巻 3 号 221〜232 頁	2021
理事会決定 2009/426/JHA [参考訳]	夏井	10 号	2 巻 4 号 36〜80 頁	2017
理事会決定 2009/371/JHA [参考訳]	夏井	8 号	2 巻 2 号 31〜98 頁	2017
理事会決定 2008/633/JHA [参考訳]	夏井	14 号	2 巻 8 号 48〜66 頁	2017
理事会決定 2008/616/JHA [参考訳]	小西・夏井	15 号	2 巻 9 号 116〜200 頁	2017
理事会決定 2008/615/JHA [参考訳・改訂版]	夏井	70 号	10 巻 9 号 188〜237 頁	2025
理事会決定 2008/615/JHA [参考訳]	夏井	8 号	2 巻 2 号 155〜181 頁	2017
理事会決定 2007/845/JHA [参考訳]	夏井	34 号	4 巻 4 号 166〜173 頁	2019
理事会決定 2005/671/JHA [参考訳]	夏井	14 号	2 巻 8 号 30〜37 頁	2017
理事会決定 2004/512/EC [参考訳]	夏井	14 号	2 巻 8 号 67〜74 頁	2017
理事会決定 2002/187/JHA [参考訳・改訂版]	夏井	35 号	4 巻 5 号 61〜86 頁	2019
理事会決定 2002/187/JHA（改正後） [参考訳]	夏井	10 号	2 巻 4 号 81〜125 頁	2017
理事会決定 2002/187/JHA [参考訳]	夏井	10 号	2 巻 4 号 126〜152 頁	2017
理事会決定 2000/799/JHA [参考訳]	夏井	35 号	4 巻 5 号 115〜118 頁	2019
理事会決定 2000/642/JHA [参考訳]	夏井	37 号	4 巻 7 号 71〜77 頁	2019
理事会決定 2001/470/EC [参考訳]	夏井	45 号	6 巻 5 号 160〜187 頁	2021
理事会決定 1999/468/EC [参考訳]	夏井	24 号	3 巻 6 号 192〜198 頁	2018
理事会決定(EC) No 515/97 [参考訳]	夏井	43 号	6 巻 3 号 248〜311 頁	2021
理事会決定 87/373/EEC [参考訳]	夏井	25 号	3 巻 7 号 193〜198 頁	2018
理事会決定 87/95/EEC [参考訳]	夏井	29 号	3 巻 11 号 115〜126 頁	2018
理事会枠組み決定 2009/905/JHA [参考訳]	夏井	14 号	2 巻 8 号 41〜47 頁	2017
理事会枠組み決定 2009/315/JHA [参考訳]	丸橋	36 号	4 巻 6 号 162〜175 頁	2019
理事会枠組み決定 2008/977/JHA [参考訳]	夏井	7 号	2 巻 1 号 141〜169 頁	2017
理事会枠組み決定 2008/919/JHA [参考訳]	夏井	11 号	2 巻 5 号 86〜94 頁	2017
理事会枠組み決定 2008/841/JHA [参考訳]	夏井	43 号	6 巻 3 号 233〜247 頁	2021
理事会枠組み決定 2006/960/JHA [参考訳]	夏井	11 号	2 巻 5 号 95〜110 頁	2017

理事会枠組み決定 2005/212/JHA [参考訳]	夏井	34 号	4 巻 4 号 190～197 頁	2019
理事会枠組み決定 2003/577/JHA [参考訳]	夏井	34 号	4 巻 4 号 174～189 頁	2019
理事会枠組み決定 2003/568/JHA [参考訳]	夏井	35 号	4 巻 5 号 170～177 頁	2019
理事会枠組み決定 2002/584/JHA [参考訳]	夏井	35 号	4 巻 5 号 185～213 頁	2019
理事会枠組み決定 2002/475/JHA [参考訳]	夏井	11 号	2 巻 5 号 71～85 頁	2017
理事会枠組み決定 2002/465/JHA [参考訳]	夏井	35 号	4 巻 5 号 178～184 頁	2019
理事会決議(2020/C 342 I/01) [参考訳]	夏井	44 号	6 巻 4 号 513～537 頁	2021
理事会決議(96/C 224/02) [参考訳]	夏井	24 号	3 巻 6 号 57～60 頁	2018
(欧州委員会が採択した法令)				
委員会規則(EC) No 2796/2000 [参考訳]	夏井	48 号	7 巻 2 号 406～410 頁	2022
委員会規則(EC) No 1068/97 [参考訳]	夏井	48 号	7 巻 2 号 400～405 頁	2022
委員会指令 2002/77/EC [参考訳]	夏井	28 号	3 巻 10 号 23～35 頁	2018
委員会指令 1999/10/EC [参考訳]	夏井	49 号	7 巻 3 号 237～246 頁	2022
委員会指令 93/102/EC [参考訳]	夏井	49 号	7 巻 3 号 166～174 頁	2022
委員会指令 91/72/EEC [参考訳]	夏井	49 号	7 巻 3 号 166～174 頁	2022
委員会指令 90/388/EEC [参考訳]	夏井	28 号	3 巻 10 号 36～51 頁	2018
委員会決定(EU) 2023/2099 [参考訳]	夏井	55 号	9 巻 1 号 58～62 頁	2024
委員会決定(EU) 2019/236 [参考訳]	夏井	33 号	4 巻 3 号 189～197 頁	2019
委員会決定(EU) 2019/165 [参考訳]	夏井	33 号	4 巻 3 号 204～212 頁	2019
委員会決定(EU) 2019/154 [参考訳]	夏井	33 号	4 巻 3 号 198～203 頁	2019
委員会決定(EU) 2018/1996 [参考訳]	夏井	34 号	4 巻 4 号 157～165 頁	2019
委員会決定(EU) 2018/1962 [参考訳]	夏井	34 号	4 巻 4 号 147～156 頁	2019
委員会決定(EU) 2018/1961 [参考訳]	夏井	33 号	4 巻 3 号 223～232 頁	2019
委員会決定(EU) 2018/1927 [参考訳]	夏井	33 号	4 巻 3 号 213～222 頁	2019
委員会決定 2011/833/EU [参考訳・改訂版]	夏井	39 号	5 巻 1 号 37～56 頁	2020
委員会決定 2011/833/EU [参考訳]	夏井	12 号	2 巻 6 号 159～169 頁	2017
委員会決定 2011/130/EU [参考訳]	夏井	30 号	3 巻 12 号 171～180 頁	2018
委員会決定 2010/425/EU [参考訳]	夏井	30 号	3 巻 12 号 116～125 頁	2018
委員会決定 2009/767/EC [参考訳]	夏井	30 号	3 巻 12 号 63～115 頁	2018
委員会決定 2009/739/EC [参考訳]	夏井	30 号	3 巻 12 号 57～62 頁	2018
委員会決定 2008/602/EC [参考訳]	夏井	14 号	2 巻 8 号 80～90 頁	2017
委員会決定 2008/597/EC [参考訳]	夏井	11 号	2 巻 5 号 147～157 頁	2017
委員会決定 2008/49/EC [参考訳]	夏井	15 号	2 巻 9 号 84～92 頁	2017
委員会決定 2006/752/EC [参考訳]	夏井	14 号	2 巻 8 号 75～79 頁	2017
委員会決定 2002/627/EC [参考訳]	夏井	28 号	3 巻 10 号 18～22 頁	2018
委員会決定 2006/291/EC, Euratom [参考訳]	夏井	12 号	2 巻 6 号 170～176 頁	2017

委員会決定 1999/352/EC, ECSC, Euratom [参考訳]	夏井	42 号	6 巻 2 号 96～105 頁	2021
委員会委任規則(EU)2017/2055 [参考訳]	夏井	20 号	3 巻 2 号 116～139 頁	2018
委員会委任規則(EU)2017/570 [参考訳]	夏井	21 号	3 巻 3 号 198～200 頁	2018
委員会委任規則(EU)2017/569 [参考訳]	夏井	21 号	3 巻 3 号 195～197 頁	2018
委員会委任規則(EU)2017/568 [参考訳]	夏井	21 号	3 巻 3 号 188～194 頁	2018
委員会委任規則(EU)2017/567 [参考訳]	夏井	22 号	3 巻 4 号 97～128 頁	2018
委員会委任規則(EU)2017/566 [参考訳]	夏井	21 号	3 巻 3 号 181～187 頁	2018
委員会委任規則(EU)2016/2020 [参考訳]	夏井	22 号	3 巻 4 号 80～85 頁	2018
委員会委任規則(EU)2016/2021 [参考訳]	夏井	22 号	3 巻 4 号 86～92 頁	2018
委員会委任規則(EU)2016/2022 [参考訳]	夏井	22 号	3 巻 4 号 93～96 頁	2018
委員会委任規則(EU) No 149/2013 [参考訳]	夏井	26 号	3 巻 8 号 154～175 頁	2018
委員会実装規則(EU) 2021/1079 [参考訳]	夏井	47 号	7 巻 1 号 262～321 頁	2022
委員会実装規則(EU) 2018/151 [参考訳]	夏井	23 号	3 巻 5 号 192～198 頁	2018
委員会実装規則(EU) 2015/1502 [参考訳]	夏井	16 号	2 巻 10 号 261～277 頁	2017
委員会実装規則(EU) 2015/1501 [参考訳]	夏井	16 号	2 巻 10 号 252～260 頁	2017
委員会実装規則(EU) 2015/806 [参考訳]	夏井	16 号	2 巻 10 号 246～251 頁	2017
委員会実装規則(EU) No 1247/2012 [参考訳]	夏井	26 号	3 巻 8 号 119～132 頁	2018
委員会実装決定(EU) 2023/1353 [参考訳]	夏井	55 号	9 巻 1 号 230～245 頁	2024
委員会実装決定(EU) 2016/650 [参考訳]	夏井	16 号	2 巻 10 号 240～245 頁	2017
委員会実装決定(EU) 2015/1984 [参考訳]	夏井	16 号	2 巻 10 号 231～239 頁	2017
委員会実装決定(EU) 2015/1506 [参考訳・改訂版]	夏井	30 号	3 巻 12 号 187～194 頁	2018
委員会実装決定(EU) 2015/1506 [参考訳]	夏井	16 号	2 巻 10 号 223～230 頁	2017
委員会実装決定(EU) 2015/1505 [参考訳・改訂版]	夏井	30 号	3 巻 12 号 153～170 頁	2018
委員会実装決定(EU) 2015/1505 [参考訳]	夏井	16 号	2 巻 10 号 207～222 頁	2017
委員会実装決定(EU) 2015/296 [参考訳]	夏井	16 号	2 巻 10 号 197～206 頁	2017
委員会実装決定 2014/148/EU [参考訳]	夏井	30 号	3 巻 12 号 181～186 頁	2018
委員会実装決定 2013/662/EU [参考訳]	夏井	30 号	3 巻 12 号 126～152 頁	2018
委員会勧告(EU) 2017/1584 [参考訳]	夏井	25 号	3 巻 7 号 293～327 頁	2018
(欧州委員会等から発出された通知)				
JOIN(2018) 16 final [参考訳]	夏井	27 号	3 巻 9 号 281～295 頁	2018
JOIN(2018) 14 final [参考訳]	夏井	29 号	3 巻 11 号 178～198 頁	2018
JOIN(2017) 450 final [参考訳]	夏井	18 号	2 巻 12 号 113～147 頁	2017
JOIN(2017) 30 final [参考訳]	夏井	14 号	2 巻 8 号 91～119 頁	2017
JOIN(2016) 18 final [参考訳]	丸橋	31 号	4 巻 1 号 220～242 頁	2019
COM(2022) 496 final [参考訳]	夏井	51 号	8 巻 1 号 1～80 頁	2023
COM(2022) 495 final [参考訳]	夏井	51 号	8 巻 1 号 81～161 頁	2023

COM(2021) 206 final [参考訳]	夏井	45 号	6 巻 5 号 320～562 頁	2021
COM(2020) 825 final [参考訳]	夏井	46 号	6 巻 6 号 1～218 頁	2021
COM(2020) 767 final [参考訳]	夏井	45 号	6 巻 5 号 563～669 頁	2021
COM(2020) 712 final [参考訳]	夏井	45 号	6 巻 5 号 233～319 頁	2021
COM(2020) 66 final [参考訳]	夏井	40 号	5 巻 2 号 1～83 頁	2020
COM(2019) 250 final [参考訳]	夏井	65 号	10 巻 4 号 1～51 頁	2025
COM(2018) 470 final [参考訳]	夏井	28 号	3 巻 10 号 85～106 頁	2018
COM(2018) 226 final [参考訳]	夏井	25 号	3 巻 7 号 328～357 頁	2018
COM(2018) 225 final [参考訳]	丸橋	26 号	3 巻 8 号 201～275 頁	2018
COM(2018) 246 final [参考訳]	夏井	27 号	3 巻 9 号 269～280 頁	2018
COM(2018) 237 final [参考訳]	夏井	27 号	3 巻 9 号 198～232 頁	2018
COM(2018) 232 final [参考訳]	夏井	28 号	3 巻 10 号 107～127 頁	2018
COM(2018) 109 final [参考訳]	夏井	26 号	3 巻 8 号 181～200 頁	2018
COM(2018) 43 final [参考訳]	夏井	23 号	3 巻 5 号 115～132 頁	2018
COM(2017) 608 final [参考訳]	夏井	17 号	2 巻 11 号 156～176 頁	2017
COM(2017) 477 final [参考訳]	夏井	31 号	4 巻 1 号 152～219 頁	2019
COM(2017) 10 final [参考訳]	丸橋・夏井	10 号	2 巻 4 号 195～248 頁	2017
COM(2017) 8 final [参考訳]	夏井	10 号	2 巻 4 号 249～354 頁	2017
COM(2017) 7 final [参考訳]	夏井	18 号	2 巻 12 号 93～112 頁	2017
COM(2016) 790 final [参考訳]	夏井	15 号	2 巻 9 号 473～488 頁	2017
COM(2014) 442 final [参考訳]	夏井	22 号	3 巻 4 号 129～147 頁	2018
COM/2013/048 final [参考訳]	夏井	1 号	1 巻 1 号 1～50 頁	2016
SWD(2018) 146 final [参考訳]	夏井	28 号	3 巻 10 号 128～184 頁	2018
SWD(2018) 137 final [参考訳]	夏井	27 号	3 巻 9 号 233～268 頁	2018
SWD(2017) 473 final 及び SWD(2017) 474 final	丸橋	20 号	3 巻 2 号 199～332 頁	2018
(欧州議会, 理事会及び欧州委員会の文書)				
欧州連合基本権憲章 [参考訳]	夏井	2 号	1 巻 2 号 1～33 頁	2016
デジタルの権利及び基本原則に関する欧州宣言[参考訳]	夏井	55 号	9 巻 1 号 200～229 頁	2024
決定 No 1247/2002/EC [参考訳]	夏井	10 号	2 巻 4 号 355～360 頁	2017
(理事会の文書)				
法へのアクセス報告書(2015/C 97/03) [参考訳・改訂版]	夏井	39 号	5 巻 1 号 1～36 頁	2020
法へのアクセス報告書(2015/C 97/03) [参考訳]	夏井	12 号	2 巻 6 号 136～158 頁	2017
(欧州議会の文書)				
決議(2015/2103(INL)) [参考訳]	夏井	11 号	2 巻 5 号 438～492 頁	2017

決議 2008/2125 [参考訳]	夏井	44 号	6 巻 4 号 487～512 頁	2021
(欧州データ保護監督官(EDPS)の文書)				
EDPS データ保護法改正パッケージ意見書 [参考訳]	夏井	14 号	2 巻 8 号 257～371 頁	2017
EDPS 意見書(Opinion 5/2017) [参考訳]	夏井	12 号	2 巻 6 号 177～216 頁	2017
EDPS 意見書(Opinion 3/2015) [参考訳]	夏井	12 号	2 巻 6 号 217～238 頁	2017
(欧州経済社会委員会(EESC)の文書)				
意見書(2017/C 434/06)	夏井	19 号	3 巻 1 号 151～170 頁	2018
意見書(TEN/629)	夏井	12 号	2 巻 6 号 239～257 頁	2017
(Frontex が採択した決定)				
Frontex 長官決定 36/2008 [参考訳]	夏井	12 号	2 巻 6 号 129～135 頁	2017
Frontex 運営委員会決定 No34/2016 [参考訳]	夏井	12 号	2 巻 6 号 125～128 頁	2017
Frontex 運営委員会決定 No58/2015 [参考訳]	夏井	12 号	2 巻 6 号 99～113 頁	2017
Frontex 運営委員会決定 No34/2015 [参考訳]	夏井	12 号	2 巻 6 号 114～124 頁	2017
(Eurojust が採択した規則)				
個人データの処理及び保護に関する追加規則 [参考訳]	夏井	10 号	2 巻 4 号 181～194 頁	2017
個人データの処理及び保護に関する規則 [参考訳]	夏井	10 号	2 巻 4 号 153～180 頁	2017
(OLAF が採択した決定)				
DPO に関する長官決定	夏井	9 号	2 巻 3 号 172～183 頁	2017
(EU のその他の規則)				
標準手続規則 2011/C 206/06 [参考訳]	夏井	23 号	3 巻 5 号 186～191 頁	2018
上級委員会手続規則 2011/C 183/05 [参考訳]	夏井	23 号	3 巻 5 号 180～185 頁	2018
(司法裁判所の判決・意見)				
Privacy International 事件判決 Case C-623/17 [参考訳]	丸橋	47 号	7 巻 1 号 410～443 頁	2022
La Quadrature du Net and Others 事件判決 Case C-511/18 [参考訳]	丸橋	47 号	7 巻 1 号 444～523 頁	2022
司法裁判所大法廷意見 Case Opinion 1/15 [参考訳]	丸橋	14 号	2 巻 8 号 186～256 頁	2017
司法裁判所大法廷判決(2016 年 12 月 21 日)[参考訳]	丸橋	7 号	2 巻 1 号 1～40 頁	2017
Camera di Commercio et al.事件判決 Case C-398/15 [参考訳]	丸橋	16 号	2 巻 10 号 1～20 頁	2017
Balogh 事件判決 Case C-25/15 [参考訳]	丸橋	38 号	4 巻 8 号 1～15 頁	2019
Maximillian Schrems 事件判決 Case C-362/14 [参考訳]	丸橋	25 号	3 巻 7 号 358～397 頁	2018
独立弁論官 MENGOZZI 意見書[参考訳]	丸橋	11 号	2 巻 5 号 366～437 頁	2017

（司法裁判所の規則・決定）				
2016 年改正欧州司法裁判所規程 [参考訳]	夏井	15 号	2 巻 9 号 283～303 頁	2017
2016 年改正欧州司法裁判所手続規則 [参考訳]	夏井	15 号	2 巻 9 号 201～282 頁	2017
司法裁判所手続規則補足規則 [参考訳]	夏井	15 号	2 巻 9 号 304～314 頁	2017
2016 年改正一般裁判所手続規則 [参考訳]	夏井	15 号	2 巻 9 号 368～449 頁	2017
2013 年改正一般裁判所手続規則 [参考訳・改訂版]	夏井	16 号	2 巻 10 号 92～146 頁	2017
2013 年改正一般裁判所手続規則 [参考訳]	夏井	15 号	2 巻 9 号 315～367 頁	2017
決定(EU) 2016/2387 [参考訳]	夏井	15 号	2 巻 9 号 454～472 頁	2017
決定 2014/333/EU [参考訳]	夏井	16 号	2 巻 10 号 85～91 頁	2017
決定 2011/C 289/08 [参考訳]	夏井	19 号	3 巻 1 号 146～150 頁	2018
決定 2011/C 289/07 [参考訳]	夏井	19 号	3 巻 1 号 142～145 頁	2018
決定 2011/C 289/06 [参考訳]	夏井	15 号	2 巻 9 号 450～453 頁	2017
（EFTA 裁判所の規則・決定）				
2010 年改正 EFTA 裁判所手続規則 [参考訳]	夏井	16 号	2 巻 10 号 40～80 頁	2017
e-EFTACourt 決定(2017/C 73/09) [参考訳]	夏井	16 号	2 巻 10 号 81～84 頁	2017
（欧州評議会の文書）				
人工知能枠組み条約（CETS No. 225）[参考訳]	夏井	59 号	9 巻 5 号 146～181 頁	2024
人工知能枠組み条約（CETS No. 225）の説明書[参考訳]	夏井	60 号	9 巻 6 号 1～100 頁	2024
サイバー犯罪条約（ETS No.185）の説明書 [参考訳]	夏井	6 号	1 巻 6 号 1～132 頁	2016
個人データ保護条約（ETS No.108） [参考訳]	夏井	4 号	1 巻 4 号 1～20 頁	2016
個人データ保護条約追加議定書（ETS No.181） [参考訳]	夏井	4 号	1 巻 4 号 21～25 頁	2016
個人データ保護条約（ETS No.108）の説明書 [参考訳]	夏井	4 号	1 巻 4 号 26～61 頁	2016
決議第 29 号（1974 年）[参考訳]	夏井	4 号	1 巻 4 号 66～69 頁	2016
決議第 22 号（1973 年）[参考訳]	夏井	4 号	1 巻 4 号 62～65 頁	2016
勧告 No R (95) 13 [参考訳]	夏井	6 号	1 巻 6 号 135～139 頁	2016
勧告 No R (89) 9 [参考訳]	夏井	6 号	1 巻 6 号 133～134 頁	2016
勧告 No R (87) 15 [参考訳]	夏井	6 号	1 巻 6 号 140～149 頁	2016
勧告 No R (80) 13 [参考訳]	夏井	4 号	1 巻 4 号 70～71 頁	2016
（カナダの文書）				
プライバシー監査報告（2017 年 9 月 21 日）[参考訳]	丸橋	16 号	2 巻 10 号 21～39 頁	2017

法と情報研究会第 5 回公開研究報告会（開催結果要旨）

日 時:2026 年 3 月 8 日（日）午後 12:30 ～17:30

場 所:明治大学駿河台校舎リバティタワー8 階 1085 教室

プログラム（敬称等略）

12:00 開場
12:30 開催挨拶・趣旨説明 丸橋透（明治大学法学部専任教授）
12:45 新保史生（慶應義塾大学総合政策学部教授）「夏井高人訳にみる「規則(EU) 2024/1689（人工知能法）」の正確な読解」
13:40 休憩
13:45 金子敏哉（明治大学法学部専任教授）「著作権・商標権侵害に係る損害額の近時の算定動向」
14:40 休憩
14:45 小西知世（明治大学法学部専任教授）「AI 利用におけるヒューマンインザループと医師法 17 条」
15:40 休憩
15:50 夏井高人（明治大学法学部専任教授）「単一化と処理主義の時代」
17:20 終了挨拶 佐々木秀智（明治大学法学部専任教授）
17:30 懇親会

2026 Printed in Japan
ISSN 2432-6089
法と情報雑誌　第 11 巻第 4 号（通巻第 75 号）（第 2 分冊）
The Law and Information Magazine vol.11 no.4 (consecutive no.75 part 2)

2026 年 4 月 12 日発行
発行者　夏井高人
発行所　法と情報研究会（代表 夏井高人）
東京都千代田区神田駿河台 1－1
学校法人明治大学研究棟
（非売品）