法律と情報技術の融合による適法性と法遵守性の保証

北　原　宗　律

（受付　2014 年 5 月 29 日）

1. は　じ　め　に

情報社会法体系において，情報技術が法律の中に導入されている。情報技術が条文中に埋め込まれている法律が多数存在する。つまり，情報技術が法律の中で定義されているのである。法律を実行しようとすれば，その情報技術を利用することになる。例えば，電子消費者契約法は，消費者に対し，「電磁的方法」を利用することを要求する。インターネットショッピングにおいて，ユーザは，「電子情報システム」，「電子メール技術」および「情報コミュニケーション技術」（インターネット）を利用せざるを得ない。また，青少年インターネット環境整備法は，プロバイダに対して，販売する携帯電話に，情報フィルタリング・ブロッキング技術を設定することを義務づけている。

これらの法律は，当事者に情報技術を利用させることによって，その法律の目的を達成しようとしているのである。言い換えれば，この方法はユーザの法律行為の適法性を保証するものである。結果として，法律は自らの実効性を維持する。法律は，同時に，法律の内容を実現している。

このような消費者及び顧客は自分の法的権利を行使するために情報技術を利用したといえる。彼らは，その法的権利を行使し，かつ，契約の目的を適法に達成したのである。

ところで，情報サービスプロバイダ（ISP）は，組織や個人ユーザに IT インフラストラクチャを提供する。しかも，ISP は，システム稼働に関わる関連法律とのコンプライアンスを維持できるような構造（アーキテクチャ）が設備された情報システムを提供しなければならない。これは，ISP としての企業倫理の一端である。システム，アプリケーション，情報を保護するために，そして，様々な規制，プライバシー，データ保護に基づく要求事項を遵守するために，ISP は，構造基準ならびに安全性基準を IT インフラストラクチャに設定しておかなければならない。これらの要求事項に応えるために，さまざまの情報技術の応用が求められる。

前述の情報環境の下では，法律と情報技術が協働することが必要である。そして，その協働を通して，適法性と遵守性を維持しながら法律の目的を実現することができる。さらに，情報技術が法律の条文に埋め込まれるという方法が採用さるべきものと思われる。この方法

が，「法律と情報技術の融合」という手段である。この融合によって，情報技術に法的権威が附与されるのである。つまり，情報技術が法的な強行性を持つようになる。

2. 法律と情報技術の融合

2.1 融合の方法

初期の段階では，法律が情報技術と協働して，法律の意思を実現することを考えていた。あるいは，法律が自らの目的の達成を目指して，法律と情報技術との結合ということを考えていた。「協働」（collaboration）にしろ，「結合」（combination）にしろ，そこでは，二つの要素が「協力」して一つの目標を達成しようとする活動であって，その二つの要素は明確に区別され一体化することはない[1]。

情報社会法について言えば，情報技術を法律の文言の中で定義している法規範が存在する。言い換えるならば，情報技術が法律の条項の中に埋め込まれているのである。法律が情報技術の中に埋め込まれているのではない。その二つの要素が区別され得ないほどに溶け込んでいるのである。これこそ，筆者の言う「融合」である。この融合によって，他のところでは「情報技術」であるものが，関連法律の中で法律概念に変わってしまったのである。そうすると，法律は，法律名宛て人に対して，その種の情報技術を利用することを勧めることになる。いや，その法律を実行する場合には，当該情報技術を利用せざるを得ない。つまり，法律は，名宛人の情報技術利用を通して法律そのものの目的の実現を図ろうとしているのである。

電子消費者契約法において，電子消費者契約とは，「消費者と事業者との間で電磁的方法により電子計算機の映像面を介して締結される契約であって，事業者又はその委託を受けた者が当該映像面に表示する手続に従って消費者がその使用する電子計算機を用いて送信することによってその申込み又はその承諾の意思表示を行うものをいう」と規定される。また，同法において，電磁的方法とは，「電子情報処理組織を使用する方法その他の情報通信の技術を利用する方法をいう」とある。さらに，電子承諾通知とは，「契約の申込みに対する承諾の通知であって，電磁的方法のうち契約の申込みに対する承諾をしようとする者が使用する電子計算機等（電子計算機，ファクシミリ装置，テレックス又は電話機をいう。以下同じ。）と当該契約の申込みをした者が使用する電子計算機等とを接続する電気通信回線を通じて送信する方法により行うものをいう」と定められている[2]。

このように，消費者は，Web で商品を購入したい場合には，電子消費者契約を締結するために，インターネットに接続したコンピュータを操作するだけでよい。つまり，コンピュータ画面のブラウザ上のメッセージやアイコンをクリックするだけでよい。ちなみに，消費者は自分の法的権利を行使するために情報技術を利用したといえる。その上，それらの操作行

為は当該法律に則っている。つまり，その行為は適法なものであった。その結果，情報システムがそれらの操作行為の適法性を保証していたのである。

2.2 融合の概念

融合は，情報技術を法律の中に埋め込むという方法で行われる。つまり，情報技術が法律の条項の中で定義されなければならない。定義されることによって，情報技術が法的意味を賦与されるのである。すなわち，情報技術が，その他の法的概念と同じように法的権威を持つことになる。

情報技術が法律の文言の中に埋め込まれた情報環境の下では，人は，情報としての法律を実行する代わりに，コンピュータか情報システムを操作し，その情報技術を利用することになる。利用者はブラウザ上のメッセージを見ながらコンピュータを操作する。その操作プロセスはシステムのプログラムの中に記述されている。

電子消費者契約とは，電磁的方法による消費者と事業者間の契約である。この電磁的方法は，電子機器とアプリケーション，すなわち，コンピュータ，ブラウザ，ネットワーク，インターネット等を利用することである。このような情報技術の利用行為が法律行為として考えられる。すなわち，電子契約においては，電子メールの送信が法律行為としての申込と承諾に見做されるのである。それゆえ，法律行為に関わる情報技術には，その構造と安全性の法的基準が求められるのである[3]。

2.3 融合の目的

法律と情報技術の融合には三つの目的がある。一つ目は，消費者，顧客，利用者の操作プロセスの適法性の保証である。消費者は売買契約を Web 上で締結しようとする。購入者は実際はブラウザ上のメッセージに従ってキーを押したり，アイコンをクリックしているだけである。しかし，彼らは，確かに，電子消費者契約法に従ってその法的権利を行使しているのである。その操作プロセスは電子消費者契約の内容と合致しているのである。すなわち，システムのプログラムがその操作プロセスの適法性を保証する結果となっている。

第二の目的は，情報サービス事業者の事業に関する種々の規制における法遵守性を保証することである。融合的な情報技術基盤，もしくは，情報環境の下で，情報システムを提供・操作する際に課せられるさまざまな要求事項に関連した遵守性，いわゆる「コンプライアンス」を達成しなければならない。

そのコンプライアンス達成のために，情報システムの構造（アーキテクチャ）が極めて重要となる。情報サービス事業者は，そのシステムを計画し構築する段階で考慮しなければならない構造基準がある。事業に関連する規制がその構造基準を要求している。すなわち，法

律は，組織に対して，「セキュリティ標準」（security by default），「プライバシーバイデザイン」（privacy by design），「データ保護標準」（data protection by default），そして「認証・アクセス管理標準」（identity/access management by default）を要求しているのである。

第三の目的は，法律と情報技術の融合を通じて，Web 上で，諺のひとつである「毒を以て毒を制す」を実践することである。すなわち，「情報技術を以て情報技術を制す」を実践するということである。ハッカーは，ネットワーク技術者がネットワークを保護するために使うのと同じ情報技術を用いてネットワークを攻撃する。その反対のことをやろうということである。つまり，情報技術が Web 上の違法行為を防止することができるであろう。こちらの情報技術は融合を通して法的根拠を有しているからである。

3. 情報技術の構造基準と安全性基準

3.1 基準の必要性

融合的情報環境の下でも，法律名宛人の多くは情報技術について十分な知識を保持しているわけではない。その法律名宛人は，時には顧客として，時には消費者として，またある時には納税者として情報技術を利用するのである。これらの人々は，通常，情報技術ならびにアプリケーションソフトウエアの変化を認識するに十分な時間を持っていない。その上，ほとんどの情報技術はいわゆる「技術影響評価」を経ることはない。最も重要なことは，そのような情報技術を利用し，さまざまな情報端末機器を操作することがひとつの法律行為として見做されることである。したがって，そこで利用される情報技術について，法律が，その構造と安全性に関して一定の基準を確定し公表しなければならない。

3.2 安全性基準

融合的情報環境下では，中核的情報技術基盤の要求事項は，安全性，データ保護，プライバシー，法遵守性及び監査という観点から想定した構造，利用者，データならびに操作に及ぶものと考えられる。

組織の中核的情報技術基盤のネットワーク，ホストコンピュータ及びアプリケーションのレベルの安全性を考慮することから，さまざまな脅威が検証されることになろう。それから，セキュリティポリシーが策定され，組織内で共有される。

それらの要求事項は，利用者管理，認証管理，利用権限管理，アクセス管理，データ管理，リソース管理，モニタイング，監視に関係するものである。

情報技術に賦与される安全性の面から検討すべきことがある。人が情報技術を利用している際に，その権利や利益が奪われることはないという確証はない。そこで，情報技術の通常

の利用方法の下では決して情報事故は発生しないという程度の安全性標準を情報技術は具備されていなければならない。つまり，これが相対的安全性という考え方である。

3.3 構 造 基 準

システム，アプリケーションならびに情報を内外の脅威から護り，種々の規制やプライバシーとデータ保護要求事項を遵守するために，組織は，「産業標準フレームワーク」のようなものから派生した「情報技術総合とアプリケーションレベル規制」フレームワークを導入しなければならない[4]。認証・アクセス管理（IAM）プロセスとプラクティスはアクセス管理とオペレーションセキュリティの領域で，組織が目的を達成することに資するものである。IAM は，一つのシステム構造であると同時に，技術コンポーネント，プロセス及び標準プラクティスの集合体でもある[5]。

個人情報の収集・利用・提供を行う情報システムは，プライバシー保護，データ保護および情報安全性の観点から一定の水準を維持しなければならない。筆者がシステムの構造に言及する理由は，システム設計の段階で技術的方法によってそれらの問題を解決したいと考えるからである。それゆえ，プライバシー影響評価やデータ保護影響評価によるプライバシー・バイ・デザインという考え方はその情報システムに適切な構造水準を提供するはずである。結局のところ，情報システムは，前節で説明したような情報技術の多くを導入しなければならない。

4. 法律と情報技術の融合インスタンス

4.1 融合の概要

二つの条件が整えば，融合は達成されよう。その一つの条件とは，情報技術が法律の文言の中で定義されていることである。二つ目の条件とは，その法律が当該情報技術の構造基準と安全性基準を規定していることである。法律がそれらの基準を規定していない場合には，その技術が通常利用されているという事実を以て，それらの基準はすでに確定していることとする。

4.2 情報技術と法律

4.2.1 E メール技術と電子消費者契約法

E メール技術が電子消費者契約法に取り込まれている。同法の第 2 条において，「電子消費者契約」とは，「消費者と事業者との間で電磁的方法により電子計算機の映像面を介して締結される契約であって，事業者又はその委託を受けた者が当該映像面に表示する手続に従って

消費者がその使用する電子計算機を用いて送信することによってその申込み又はその承諾の意思表示を行うものをいう」（第1項）と規定されている。また，第3項においては，「電磁的方法」とは，「電子情報処理組織を使用する方法その他の情報通信の技術を利用する方法をいう」と定められている。さらに，第4項において，「電子承諾通知」とは，「契約の申込みに対する承諾の通知であって，電磁的方法のうち契約の申込みに対する承諾をしようとする者が使用する電子計算機等と当該契約の申込みをした者が使用する電子計算機等とを接続する電気通信回線を通じて送信する方法により行うものをいう」としている。

前述のように，電磁的方法とは，電子的情報処理システムやその他の情報技術を用いることであると理解される。すなわち，コンピュータを使用することで十分であろう。そして，申込みや承諾のための電磁的記録の送信には電子メール技術を利用するということである。つまり，「電子消費者契約」とは，いわゆる「インターネットショッピング」や「ネットショッピング」を意味している。

Eメール技術は，SMTP（Simple Mail Transfer Protocol）とPOP（Post Office Protocol）という2つのプロトコルを使用する。これらは，いずれも，TCP/IP（Transfer Control Protocol/Internet Protocol）プロトコルに含まれる[6]。

多くの暗号システムは，そのままでは極めて安全性に問題のあるコミュニケーション方法のひとつのEメールをより安全にするために導入されている。一般的な情報技術として，S/MIME（Secure Multipurpose Internet Mail Extentions），PEM（Pretty Enhanced Mail），およびPGP（Pretty Good Privacy）というものがある[7]。

S/MIMEは，公開鍵暗号システム上でデジタル署名による暗号化と認証を追加することによって，MIMEコード方式を構成する。PEMは，公開鍵暗号方式とともに機能する標準のひとつで，インターネット技術協議会により提案されたものである。通信中に傍受，改ざんができないように暗号化が施された電子メールである[8]。

4.2.2　認証技術と法律

1999年に，日本では，「不正アクセス禁止法」（正式名称は「不正アクセス行為の禁止等に関する法律」である。）が成立した。同法（第2条）における「不正アクセス行為」とは，「アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能に係る他人の識別符号を入力して当該特定電子計算機を作動させ，当該アクセス制御機能により制限されている特定利用をし得る状態にさせる行為」（4項1号），「アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能による特定利用の制限を免れることができる情報又は指令を入力して当該特定電子計算機を作動させ，その制限されている特定利用をし得る状態にさせる行為」（4項2号），および「電気通信回線を介して接続された他の特定電子計算機が有するアクセス制御機能によりその特定利用を制限されて

いる特定電子計算機に電気通信回線を通じてその制限を免れることができる情報又は指令を入力して当該特定電子計算機を作動させ，その制限されている特定利用をし得る状態にさせる行為」（4項3号）である。

4.2.3　暗号化技術と電子署名法

暗号化は，メッセージ内容の安全性を確保するために用いられるひとつの技術である。また，認証を隠したり，ステガノグラフィー（データ隠蔽技術），リメエイラー（メール転送），クローン・アカウント（account cloning）およびIPアドレス偽装攻撃（spoofing）というような情報隠しの技法がある[9]。暗号化は，情報の秘密性・完全性・真実性を与えることができる。デジタル署名は，暗号技術の利用によって可能となるもので，情報の送信者に認証を与えるものである。

電子署名法は，この暗号化技術を利用している。この法律の目的は，電子署名により電磁的記録の真正性の推定を保証することである。同法において，情報を表現するために作成される電磁的記録は，当該電磁的記録に記録される情報について本人による電子署名が行われるときは，真正に成立したものと推定するとされる。この電磁的記録の真正性および電子署名は公開鍵暗号システムによって証明される。

日本の電子署名法の主要条文は以下のように定められている。

第1条（目的）

この法律は，電子署名に関し，電磁的記録の真正な成立の推定，特定認証業務に関する認定の制度その他必要な事項を定めることにより，電子署名の円滑な利用 の確保による情報の電磁的方式による流通及び情報処理の促進を図り，もって国民生活の向上及び国民経済の健全な発展に寄与することを目的とする。

第2条（定義）

1　この法律において「電子署名」とは，電磁的記録（電子的方式，磁気的方式その他人の知覚によっては認識することができない方式で作られ る記録であって，電子計算機による情報処理の用に供されるものをいう。以下同じ。）に記録することができる情報について行われる措置であって，次の要件の いずれにも該当するものをいう。

一　当該情報が当該措置を行った者の作成に係るものであることを示すためのものであること。

二　当該情報について改変が行われていないかどうかを確認することができるものであること。

2　この法律において「認証業務」とは，自らが行う電子署名についてその業務を利用する者（以下「利用者」という。）その他の者の求めに応じ，当該利用者が電子署名を行ったものであることを確認するために用いられる事項が当該利用者に係るものであること

を証明する業務をいう。

3　この法律において「特定認証業務」とは，電子署名のうち，その方式に応じて本人だけが行うことができるものとして主務省令で定める基準に適合するものについて行われる認証業務をいう。

しかし，これらの条項の中で，暗号化技術を法律の中に導入すると宣言しているものはない。だが，同法施行規則第 2 条に以下のように規定されている。すなわち，

「法第二条第三項の主務省令で定める基準は，電子署名の安全性が次のいずれかの有する困難性に基づくものであることとする。

一　ほぼ同じ大きさの二つの素数の積である千二十四ビット以上の整数の素因数分解

二　大きさ千二十四ビット以上の有限体の乗法群における離散対数の計算

三　楕円曲線上の点がなす大きさ百六十ビット以上の群における離散対数の計算

四　前三号に掲げるものに相当する困難性を有するものとして主務大臣が認めるもの」

これは，電子署名の安全性の基準を述べているものと理解できる。同時に，各種ある暗号化技術の構造を記述しているものと理解されるはずである。アメリカ連邦政府の「電子署名に関する法律」においても，暗号技術は特定されていない。つまり，電子署名の形式については何の規定もない。今後開発される電子署名技術，すなわち，暗号技術を容易に法律に取り込むことができるように配慮されたために，その名称と形式を曖昧にされたということである[10]。

暗号技術の利用は産業スパイの世界を連想させるものである。しかしながら，一般には秘匿性と暗号化という正当な多くの目的がある。多くは商取引と関係があり，第三者の好奇心から金融情報を保護し，取引の当事者間での意思表示の否認を防止するためである。したがって，暗号技術は，グローバルな電子商取引の発展のために不可欠なものである[11]。

4.3　フィルタリング技術と法律

4.3.1　パケットフィルタリング技術と法律

パケット・フィルタリング・ファイアーウオールは，簡易なネットワーク装置である。その機能は，送信・受信されるパケットのヘッダ部を検証することによって，パケット（情報）をフィルタ（濾過）することである。すなわち，パケット・ヘッダ内の数値データに基づいて選択的に情報をフィルタリングすることができる。つまり，そのパケットを受け入れるべきか拒否すべきかを決定する。この装置は，IP アドレス，パケットのタイプ，ポート番号などの要素に基づいてパケットをフィルタリングする[12]。

青少年インターネット環境整備法は，情報サービス業者に対して，この情報フィルタリング技術をユーザに提供することを義務づけている。同法は，未成年者をインターネット上の

有害情報から保護するための諸措置の策定を目的とし，インターネットの利用環境に関する改善方針を定めている[13]。

4.3.2　Web コンテンツフィルタリング技術と法律

クラウドにおいては，SaaS 事業者は，悪意のメール（マルウエア）の脅威を探し回り，ユーザクライアントに対して安全な通信だけが配信されることを保証する。SaaS 事業者は，HTTP ヘッダ情報，ページコンテンツの認証機能をもつ URL フィルタリングを補足している。Web コンテンツのための SaaS は，外部へ送信される情報からセンシティブ情報（例えば，ID 番号，クレジットカード情報，知的財産など）を検知する（データ漏洩保護）。このようなセンシティブ情報は，ユーザが適切な認証を経ずに外部へ送信できるはずである。Web 上の流通情報は，データ漏洩を防止するためにも，コンテンツ分析，ファイル・タイプ，パターン照合という方法で精査される[13]。

コンテンツフィルタリングは組織のシステムをその誤用および不意のサービス拒絶状況から保護するのに効果的である。コンテンツ・フィルタはソフトウエア・プログラム単体のこともあり，コンピュータと一体化したシステムの場合もある。いずれにしても，それは，ネットワークに送信されるコンテンツの精査を管理者に可能にする機能を持つ。最も一般的なコンテンツ・フィルタの応用は，ポルノグラフィやゲームのようなビジネス以外の情報を用いて実行される Web サイトへのアクセスを制限することである。また，フィルタは，外部からの迷惑メール（スパムメール）の制限にも効果的である[14]。

コンテンツフィルタは，従業者がネットワーク資源を不適切に使用していないことを保証する。不運にも，このようなシステムは，広範囲の通信状態を表すデータや不許可の送信先，制限された e メールの送信元アドレスのリストの最新データを必要とする。最近のコンテンツフィルタリングシステムは，制限されたデータベースを自動的に更新する。その方法はアンチウイルスプログラムが更新されるのと同様の方法である。このようなアプリケーションは，許可・不許可のいずれのサイトでも探し当てる。例えば，「ヌード」や「セックス」というようなキーワードにもヒットする。もちろん，コンテンツ創造者は，このようなヘマな表現を隠すことでその制約をかいくぐっている。このことが，ネットワークやセキュリティ技術者に余分な課題をもたらしている[15]。

4.4　プライバシーとデータ保護技術と法律

4.4.1　プライバシー強化技術とプライバシー法

情報通信技術（ICT）は，ユーザ，消費者および市民のためのプライバシー保護という形でさまざまな解決方法を提供している。プライバシーを保護するための ICT の適用は，プライバシー強化技術（PETs: Privacy-Enhancing Technologies）という名称の下に広く認知され

てきた[16]。PETs は，データ・システムの処理機能を失わない程度にまで，個人データを厳選もしくは削減することによってプライバシーを保護する ICT 措置の根幹的システムとして定義される[17]。PETs はプライバシーを強化する技術的なものであり，プライバシー保護は情報セキュリティや秘匿性とは同義ではない。また，PETs は EU プライバシー指令において，その法的詳細化のために適用されなければならないとしている。その結果，データ処理に過度の要求をすることなくしてデータ保護の保証が可能であるとする。PETs を適用し個人データ処理を効率化することによって，当該組織は，個人データをめぐるサービスおよび処理に関して社会の高度な期待に応えることが可能となる。

4.4.2　データ監査技術と法律

データ監査技術を法律に埋め込むことによって，データ管理者は個人データの一生を把握することが可能である。データ管理者による保有する個人データのすべてを把握することは，データ保護法の実効性を向上させることに資するものである[18]。保有個人データに論理的 IC タグを貼付することで，個人データの流れを把握することが可能である。この論理的 IC タグは，電子メールのような IP パケットのヘッダーと同じ役割を担っている。すなわち，IC タグには個人データのデータ，つまりメタデータが記録されている。

パケットフィルタリングファイアウオールはすべてのパケットのヘッダを認識し，宛先アドレス，パケットのタイプ，その他の重要情報のようなヘッダ情報に基づいて，選択的にパケットをフィルタリングすることができる。ファイアウオールは，ネットワーク上のデータパケットを探し回り，ファイアウオールデータベースの規則を遵守しているかその規則に違反しているかを見つけ出すのである[19]。

4.4.3　足跡追跡技術と法律

アメリカ合衆国連邦貿易委員会（FTC）は，インターネット上でのユーザの追跡を禁止する措置（a do-not-track mechanism）の基準を作成した。追跡禁止措置とは，オンライン・ビジネスにおいて，オンライン追跡及び顧客データの保有に関する拒否権を認めることである。

オンライン追跡禁止法（The Do Not Track Me Online Act）において，当該情報の収集または利用を効果的かつ容易に禁止できることを顧客に認め，そして，その収集や利用の拒否を当該顧客が選択できることを該当企業に尊重させるためのオンライン拒否表示措置の基準を定めることを FTC が規定しなければならないとする（第 3 条）。

アメリカでは，一般的には，インターネットのプライバシー保護は民間企業の自主規制に任されている。FTC 報告書によれば，2011年の春には，Mozilla の Firefox および Microsoft の IE にはすでに DNT（Do Not Track）が導入されており，その直後には Android 版のブラウザにも導入されたということである。そして，Apple の Safari には2011年の夏に導入された。この結果，2012年までには，インターネットユーザの半分近くの人が，DNT をサポー

トした新しいブラウザを利用できるはずであるとしている[20]。

DNT ヘッダのサポート提供を委任する法律上の明示的な要求事項は存在しない。すなわち，ブラウザ上の DNT 機構を介して足跡を追跡されたくないという消費者の要求のサポート方法の時期を銘記するための法的な，法律遵守に向けられた考慮が存在する[21]。

「追跡禁止」の設定を要請する立法府の提案に加えて，さまざまな事業者が，オンライン追跡を消費者が制御できるツールを開発してきた。多くのベンダ事業者は，そのブラウザ上では，ウエブサイト間の移動を追跡しないように消費者がサイト運営者に指示することが可能であるとした。また，W3C（World Wide Web Consortium）は「追跡禁止」（Do Not Track）の世界標準を作成するべく作業グループを召集した[22]。

4.4.4　匿名化技術と法律

デジタル経済はこれまで経験したことのない規模の大きさで個人データの収集に向かおうとしている。ソーシャルネットワーク，種々のリテーラ，情報サービスプロバイダから一般企業の多くが個人情報を収集し，個人を識別できない方法でのみ他の企業に提供されていることを保証している[23]。日本の統計法においては，「統計調査」とは，「行政機関等が統計の作成を目的として個人又は法人その他の団体に対し事実の報告を求めることにより行う調査をいう」（第 2 条 5 項 1 号）と規定される。「調査票情報」とは，「統計調査によって集められた情報のうち，文書，図画又は電磁的記録に記録されているものをいう」（同項11号）とされる。また，「匿名データ」とは，「一般の利用に供することを目的として調査票情報を特定の個人又は法人その他の団体の識別（他の情報との照合による識別を含む。）ができないように加工したものをいう」（同項12号）とある。そして，この「匿名データ」は行政機関等によって作成されることが認められている（同法第35条）。さらに，この「匿名データ」を，学術研究の発展を目的として，一般の求めに応じて提供できると規定されている（同法第36条）。

しかしながら，統計情報を匿名化する方法について明確な説明はない。もし，匿名化を技術的方法で実施するのであれば，匿名化技術の構造基準及び安全性基準を公表しなければならない。匿名化はひとつの技術であって，パブリッククラウドではデータの安全性を強化するために導入されている。それゆえ，データ分析やデータ利用が認められているのである[24]。データ匿名化は，データが公表または利用される際に，中核的情報の識別を防止するためのデータ変換方法である。

4.4.5　非識別化・再識別化技術と法律

記録データが一端非識別化（de-identify）されると，元の個人への接続が絶たれるので，そのデータを安全に外部に提供することができる[25]。しかし，個人と個人を区別するいかなる情報も，再識別化匿名データ（re-identifying anonymous data）として利用することが

可能である。そのため，組織は，氏名，住所，電話番号のような明確な識別子付きの個人に固有のデータに関して，出力データが匿名データのように見えるので匿名性が維持されるという前提の下に利用・提供が可能である[26]。ドイツ連邦データ保護法によれば，匿名化とは，相当の時間・費用・労力をかけても再び識別されたまたは識別可能な個人の属性に辿り着くことができないような方法で行う個人データの変更方法であるという（Sec3(7)　BDSG)。

4.4.6　別称技術と法律

別称（alias）はいくつかの特別な状況を作り出すことができる。つまり，個人に交換関係にある異なった別称を装うことを認めるものである。ひとつの別称はウエブフォーラム投稿用に，また，もうひとつの別称は電子メール交換用に，という具合に，多くのオンラインユーザは，真性な正体を護るために，偽名としてそれらの別称を使用している[27]。別称（エイリアス）は，電話番号，氏名または住所に代わり得る二つとない識別子である。これは，人がその私的な情報を安全に維持することができるということを意味している。

この別称技術はドイツ連邦データ保護法に導入されている。同法によれば，「別称」とは，「データ主体の特定を不可能にまたはできる限り困難にするために，当該データ主体の氏名およびその他の識別要素を他の識別子に置き換えることである」（第 3 条6a 項）と定義されている。

5. お わ り に

本研究の主要目的は，法律と情報技術との間に新しい関係を見出そうとするものである。その関係は，協働，結合，および融合という様態として現れる。法律と情報技術はお互い相容れないものと考えられてきた。しかし，それは時間的問題にのみ通用するように思われる。つまり，法律は常に情報技術の後ろを歩んできたからである。

法律が技術の後を追うというよりもむしろ，電磁的方法においては情報技術が法律の内容を表現できているとは思われないのである。

この研究は，法律と情報技術間の関係の諸態様を追究することである。第 1 に，コンピュータシステムおよびネットワークの重要な特性が多くの社会システムに採り入れられている。第 2 に，情報・ネットワーキング技術は，倫理的・社会的様相を具有している。それゆえ，情報技術は法律規範と強い親近性を持っている。また，ネットワーキング技術は，人と人との繋がりを形成するのに役に立っている。第 3 に，情報技術は，人の行為の適法性を保証することができる。同時に，情報技術は，組織の事業遂行の法遵守性をも保証する。その結果，情報社会は法的正義に到達することができる。

個人が自らの法的権利を行使するために情報技術を利用することに正当性はあるのだろう

か。電子メールは，電子消費者契約における当事者の申込と承諾データを移転させる唯一の方法である。情報技術はその契約において法的推論を提供しているわけではない。

前述の融合において，より困難な問題は，立法者が法律の文言の中に情報技術を記述する方法である。電子署名法はその一つの適切なモデルになっていると考えられる。すなわち，法律が，まず，情報技術の利用を示唆することになろう。その条項の文面から，情報技術のひとつである暗号技術を移用しないと，その法律内容を実現できないことが理解されるはずである。つぎに，その情報技術の構造（architecture）と安全性（security）の基準が明示されていることである。つまり，同法施行規則が構造基準と安全性基準を掲げているのである。

コンピュータシステムの重要な特徴が情報社会の社会システムに取り入れられている。また，情報技術の重要な特徴も現実の政治的・社会的システムに取り入れられている。情報システムが社会システムの問題解決に寄与してきた。

情報セキュリティ技術は認証技術，データ保護技術及び情報フィルタリング技術を含んでいる。これらの技術はそのユーザに倫理的配慮を求めている。すなわち，これらの技術はそのユーザを倫理的行動に導く。それゆえ，これらの技術は倫理的技術と呼んでもよいだろう。

情報技術は多くの法律分野で利用されてきた。その事実は情報技術が法的観点から正当性を持っていることの証明だろう。TCP/IP はインターネットユーザの行動をコントロールするインターネット上の法律的役割を担っている。

これらの情報技術は法律に代わって法律の内容を実現するために利用されているということが認められよう。これこそ，法律と情報技術の融合である。融合は法的正義の実現を目指している。

確かに，この融合をめぐってさまざまの問題が浮かび上がる。まず，技術が技術をコントロールする状況が生まれる。つぎに，融合はそのユーザに対して一定の情報技術が投入された特定システムの利用を強いることになる。融合は技術の発展に速やかに対応しなければならない。最後に，情報技術の標準化の問題が残されている。

引用・参照文献

［1］ Cf., M.Kitahara, The Collaboration of Law and Information Technology, *Social Systems Solutions applied by Economic Sciences and Mathematical Solutions*, Kyushu Univ. Press 2011, pp. 1ff.
［2］ Cf., M. Kitahara, ibid., p. 15.
［3］ Cf., ibid., pp. 26ff.
［4］ Tim Mather/Subra Kumaraswamy/Shahed Latif, *Cloud Security and Privacy*, O'Reilly 2009, pp. 73ff.
［5］ Tim Mather/Subra Kumaraswamy/Shahed Latif, ibid., p. 99.
［6］ Cf., National Law Enforcement and Corrections Technology Center, *A Guide for ApplyingInformation Technology in Law Enforcement*, U.S. Department of Justice 2001, p. 1.
［7］ Cf., Japan National Police Agency, the White Paper on Police, 2012, p. 22.

［8］ Y. Akdeniz/C. Walker/D. Wall（eds.）, *The Internet, Law and Society*, Longman 2000, p. 320.
［9］ Ibid., p. 321.
［10］ M.E. Whitman/H.J. Mattord, *Management of Information Security,* 2nd ed., Thomson 2008, p. 353.
［11］ Tim Mather/Subra Kumaraswamy/Shahed Latif, *Cloud Security and Privacy*, O'Reilly 2009, p. 220.
［12］ Ibid.
［13］ M.E. Whitman/H.J. Mattord, *Reading and Cases in the Management of Information Security*, Course Technology 2006, p. 63.
［14］ M.E. Whitman/H.J. Mattord, *Management of Information Security,* 2nd ed., Thomson 2008, p. 373.
［15］ Ibid.
［16］ G.W. van Blarkom/J.J. Borking/J.G.E. Olk（eds.）, Handbook of Privacy and Privacy-Enhancing Technologies, PISA 2003, p. 33.
［17］ Ibid.
［18］ Cf., R. Morgan/R. Boardman, Data Protection Strategy: Implementing Data Protection Compliance, Sweet and Maxwell 2003, p. 33.
［19］ M.E. Whitman/H.J. Mattord, *Principles of Information Security,* 3rd ed., Course Technology 2009, pp. 245－246.
［20］ Cf., The Do Not Track Field Guide（https://developer.mozilla.org/en-US/docs/tag/DNT）. The US FTC, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, FTC Report March 2012, p. 4.
［21］ Cf., ibid., The Do Not Track Field Guide.
［22］ US FTC, ibid., pp. 4－5.
［23］ Cf., A. Narayanan/V. Shmatikov, Privacy and Security: Myths and Fallacies of "Personally Identifiable Information," *Communication of the ACM*, Vol. 53 No. 6, 2010, p. 25.
［24］ Jeff Sedayao, Enhancing Cloud Security Using Data Anonymization, IT@Intel White Paper, 2012, p. 2.
［25］ A. Narayanan/V. Shmatikov, ibid.
［26］ Cf., Latanya Sweeney, *k*-Anonymity: A Model for Protecting Privacy, International Journal on Uncertainty, Fuzziness and Knowledge-asked Systems, 10(5), 2002, pp. 557－570.
［27］ Cf., R. Hölzer/B. Malin/L. Sweeney, Email Alias Detection Using Social Network Analysis（http://dataprivacylab.org/dataprivacy/projects/emailalias/paper.pdf）.