法律と情報技術の協働（コラボレーション）の研究

北　原　宗　律

（受付　2013 年 5 月 31 日）

1. は　じ　め　に

情報社会法は，21世紀の高度情報通信ネットワーク社会を形成し，運営することに大きな役割を担っている。また，情報社会法は，情報（コンテンツ），情報処理機器ならびに情報流通経路を規律する社会規範である。情報社会においては，人は，その人生の大部分を，情報生活として過ごすことになろう。「Web 24/7」という表現がそのことを表している。つまり，人は，1 日の24時間，1 週間の 7 日間，ウェブ，すなわち，インターネットに接続しているということである。情報生活とは，仕事のためであれ，遊びのためであれ，情報もしくは情報機器と接している時間のことである。人は，オンラインで，行政サービス，金融サービス，教育サービス，あるいは消費サービスを，インターネットやクラウドから享受することが可能である。

他方，そのような生活を送っている最中に，不運にも，いわゆる「情報事故」に出くわすことがあるかもしれない。情報事故とは，インターネット・ユーザが，その権利や利益を侵害される事故のことである。つまり，データ保護権の侵害，個人情報の濫用，プライバシーの侵害，フィシング詐欺，データ悪用，誹謗中傷，個人情報の不当開示，サービス拒絶，権限の超越，著作権侵害，幼児ポルノ写真開示，等々の情報犯罪やコンピュータ悪用事案である。

情報社会は，これらの犯罪行為や違法行為を防止するために，「情報社会法」という法律体系を用意している［1］。しかしながら，その中のいくつかの法規範は，遵守されないことが多い。つまり，それらの法律に関しては，規範コミュニケーションが成立していないのである。あるいは，その実効性が著しく底化している。このことは，すなわち，情報としての法律がその実効力を失いかけているということを意味する。

情報犯罪は，その多くは，情報技術を利用して実行される。コンピュータ・ウイルスもコンピュータ・プログラムの一つであると言われている。コンピュータ誤用とはコンピュータを道具として，そして，インターネット・アクセスを介して実行される多くの犯罪的攻撃の集合的用語である［2］。

本小論において，筆者は，法律と情報技術の協働（コラボレーション）を提案したいと考

えている。情報社会の中には，すでにその「協働」を導入している法律がある。つまり，情報技術を法律の中に導入することによって，当該法律の実効性を回復することを目論んでいるのである。究極的には，法的正義の実現である。かかる高度な目的の実現のために，法律との協働のために利用される情報技術には，その安全性ならびに構造に関して，一定の水準が要請される。

本小論の目的を達成するために，まず，法律分野における情報技術の利用の状況を概観する（2)。つぎに，技術による法の実現の意義を解明するために，自動車技術による道路交通法の遵守の様子を検討する（3)。そのつぎに，法律と情報技術の協働について，いくかの事案について検討する（4)。最後に，情報技術の安全性と構造の水準について，あるべき基準について検討する（5)。

2. 法における情報技術の利用

2.1 情報技術の利用

技術は，一般的に，中立的である。このことは情報技術にもあてはまる。ある有名なハッカーがその高度な情報技術能力を買われて情報サービス企業に採用されたことがある。ハッカーは情報技術を用いてその会社のネットワークを攻撃していた。元ハッカーは，今度は，自分の会社となった企業のネットワークを守る立場に変わってしまった。しかし，そこで利用される情報技術はハッカー当時のそれと何のちがいがあるだろうか。ネットワークを保護する場合も，ハッカー当時と同じ情報技術を使用することだろう。元ハッカーは新しいハッカーと対峙することになるのである。そこでは，情報技術を以て情報技術を制するというような状況にあるということは推察できる。

2.2 法における情報技術利用の促進

21世紀に入って，日本政府は，教育，福祉等の住民サービスの向上や行政の効率化および情報格差の是正を視野に入れた地方の包括的なデジタル化を推進してきた［3]。また，内閣は，行政手続に関連する情報技術の利用に関する法律を提案した。さらに，2002年に，政府は，住民基本台帳ネットワークシステムを構築したことにより，行政機関に個人情報を提供することが可能となった。

かかる情報環境にあって，消費者はオンラインショッピングに参加するためにコンピュータを利用する。消費者は売買契約を締結するためにコンピュータを使用していると言い換えることができる。また，納税者は，住民基本台帳ネットワークシステム用の IC カードの中の電子証明書を用いて納税のために電子納税システムを利用する。今や，IC カードは，紙の

健康保険証や運転免許証に代わって，個人認証の役割を担っている。

このような現状は，人は，自らの法的権利を行使するために情報技術を利用していると言ってよい。人はただ，ブラウザ上のメッセージに従ってコンピュータを操作したり，アイコンをクリックしたりするだけである。その上，その際，人は，外観上は，関連法律を遵守しているように見える。つまり，その情報技術が人の法律行為の適法性を保証しているのである。

2.3 法執行機関における情報技術の利用

コンピュータ・パワーの増進に伴い，データ転送，及び魅力的で使い勝手のよい画面仕様における進歩が法律の執行機関において予想外のさまざまな可能性を開いた。とりわけ，データの収集，データの分析においてである。また，機関内ならびに機関外の関係者とのデータの共有についてである。情報技術は，究極的には，地方の法執行機関に対して，広範囲に及びより複雑化する任務の遂行に多大な支援力を発揮するツールになっている［4］。警察業務において情報技術が最も注目される 2 つの分野は犯罪マッピングと情報統合である［5］。

今日，法執行機関は，以前にくらべてその何倍も情報技術に頼っている。いわば，情報技術が現代の世界と同時に，警察においても多大な効果をもたらしている。その二つが結びつくこと（marrying）によって，より効果的で安全な職場環境や共同社会が生まれる。情報技術が利用される場所にかかわらず，警察機関の日常の任務における諸活動が任務手順書として特徴付けられる。情報技術の応用は，ひとつの手順を容易に自動化する（いや，そうなるなずである。）。情報技術が用いられるところでは，任務を最高のレベルで遂行することができるのである［6］。

2.4 コンピュータ応用による情報技術監査

監査人（Auditors）とは，監査専門人（Audit professionals）と呼ばれ，その任務は，独立して，企業の内部管理統制を点検し評価し，その結果を経営者に報告することである。

デジタル社会において，企業は情報システムをその中枢に導入していることから，その経営基盤は情報技術によって支えられている。そのため，内部統制の点検・評価の対象が情報システムと利用される情報技術になっている。その結果，監査人は，「情報技術監査人」または「コンピュータ監査専門人」に代わられた。　情報技術監査人は結論を導き出すために，企業の書類や記録から証拠を収集する。この監査のための証拠には，紙の記録，これらの記録や取引が速やかに適切に記録され，適切な権威ある署名や表記がなされたという証拠が含まれる。

3. 技術利用による法の実現

3.1 大型貨物自動車による交通事故

数年前，高速道路上で，大型貨物自動車による重大事故が続けて発生した。大型自動車が制限速度をはるかに超える速度で前方車両に衝突する事故が多かった。しかも，前方車両の乗員が死亡するという重大な事故であった。警察は，それらの事故の原因は，大型車の極度の制限速度違反にあるとした。

3.2 情報としての道路交通法

道路交通法は，車両が高速度道路上で最高速度を超えて走行することを禁止している。そして，同施行令は，大型貨物自動車の高速道路上での最高速度を時速100キロメートルと規定している。前述の大事故はこの最高速度をはるかに超える速度で走行したためであると考えられている。このことは，法定速度が遵守されなかったことを意味する。すなわち，情報としての法律が大型貨物自動車の運転者には何の強制力も発揮できなかったと言わざるを得ない。

3.3 技術の応用

そこで，法律が改正され，道路運送車両法の保安基準の改正が実施された。その改正により，大型貨物自動車への「速度抑制装置」（いわゆる「リミッタ」）の装着が義務化されたのである。その装置を装着した自動車は，いくらアクセルを踏み込んでも，時速90キロメールになると，燃料供給がとまる仕掛けになっている。この装置のおかげで，大型貨物自動車は最高速度を守り，道路交通法を遵守しながら走行している。これは，あくまでも，外観上そう見えるだけで，運転手の意図とは関係ない。速度抑制装置という一つの技術がその運転者をして，法定速度を遵守させたということになる。

3.4 技術の水準

道路運送車両法の保安基準は，前述の速度抑制装置の構造基準を決めている。その構造基準とは，大型貨物自動車が時速90キロメートルを超えないように燃料のエンジンへの供給を調節することができるとある。そうすると，大型車は時速90キロメートル以下で走行せざるを得ないのである。また，すべての大型車は回転速度計（いわゆる「タコメータ」）も装着されている。

この装置の構造は，当該保安基準を十分に実現できるものでなければならない。すなわち，その構造のなかに法律の内容が埋め込まれていると考えることもできる。これが本装置の製

造者にとっての構造基準であり，その装置の利用者にとっての安全基準である。

3.5 技術の画一性

技術は，一般的には，中立的で，厳格で，しかも画一的である。本事案の大型自動車の場合，その速度抑制装置が運転手から緊急避難の権利を奪うことになるのではないかという危惧がある。つまり，例えば，時速120，130キロメートルでその場を通り過ぎた方が重大な事故を避けることができたのに，それができなかったせいで，より重大な事故に巻き込まれたということにはなりはしないかということである。

4. 法律と情報技術の協働

4.1 E メール技術と法律

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。また，「電子計算機の映像画を介して」とは，「コンピュータ等の情報端末器のモニタ上に表示されたブラウザ上のメッセージやアイコンを介して」というように理解されよう。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。しかし，同法は，E メール技術に直接触れることはない。

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。しかし，これらのプロトコルの意味を理解する必要はない。プロトコルによってメッセージの交換ができるのである。

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であるEメールをより安全にするために多くの暗号システムが導入されている。一般的な暗号化技術として，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。PEMは，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 暗号化技術と法律

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，暗号化技術は認証隠し，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として利用されることもある［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，暗号化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］。しかしながら，同基準は，電子署名法で利用可能な暗号化技術の構造基準および安全基準として理解しなければならない。

暗号化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，暗号化技術は，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　情報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機能を有する。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］。

4.4 インターネット技術と法律

インターネットは，それ自身の技術によって，そのユーザをして，適法な行為へと導くことができる社会的空間のひとつである。たとえば，ファイアウオール・ルータは，私的なネットワークの安全性を確保するためにアクセス・コントロール・リスト（ACLs）などの手法を用いている。

ACLs は，ユーザのアクセス・リスト，マトリックス（ユーザと権限の対照表），および権限表から構成されており，ユーザの権限や特権を管理することができる。ACL は，ファイル・ストレージ・システム，ソフトウエアやネットワーク機器へのアクセスを制御する。一般的には，ACLs は，特定のユーザ，コンピュータ，時刻，期間，特別なファイルのために，そのアクセスを制限することが可能である。このような特殊性が管理者に強力な制御権限を与えている［14］。

インターネット・プロトコル・セキュリティ（IPSec）は，ソース公開型のプロトコルであり，LAN，WAN およびインターネットのような IP（インターネット・プロトコル）に基づいたネットワーク上の通信の安全を確保している。そのプロトコルは，IP パケットにおけるデータの統合性，ユーザの秘匿性，権限性を守るように設計されている［15］。

PAP（Password Authentication Protocol）は，PPP（Point to Point Protocol）コンピュータ同士に認証を与え，リモートコンピュータを識別するだけで，無権限アクセスを防止することはできない。そのため，ルータ，あるいはアクセス・サーバがユーザのアクセス権を決定する。ファイル及び交換メッセージを保護するのは PGP（Pretty Good Privacy）である。PGP は，ファイルとメッセージの暗号化と復号化に，利用される暗号技術である。PGP は，公開鍵方式と共通鍵方式という複数の暗号アルゴリズムを組み合わせたものである。それは，E メールとファイル・ストレージ・アプリケーションの暗号化ならびに認証のためのデファクト標準となっている［16］。

EU 指令（95/46/EC）は，データ管理者に対して，個人データの保護のために適切な技術

的・組織的措置を実施することを求めている。つまり，特に，データ処理がネットワークを介するデータ移転を含む場合に，事故または違法な改ざん，無権限の開示やアクセスから，ならびに，その他のすべての違法なデータ処理から，個人データを保護するために，管理者は，一定の技術的措置を実施しなければならないということである。その際に，前述のインターネット技術の適用もその視野に入っているものと思われる。

4.5 プライバシー強化技術と法律

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。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。

4.6 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。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［18］。

4.7 電子メールフィルタリング技術と法律

電子メールのための SaaS（Software-as-a-Service）は，基本的には，ある組織にやってくる電子メールのストリームからそのメールに隠れている，スパムメール，詐欺的メールおよびマルウエア等の除去機能を持っている。その結果，その組織が悪意のメールに汚染されないような仕組みを施しているのである［19］。これは，トランスポート層のネットワーク通信上におかれている通信のセキュリティを確保するためのプロトコルである「SSL」（Secure Socket Layer）または「TLS」（Transport Layer Security）を利用することによって実現されている［20］。

4.8 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［21］。

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［22］。

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［23］。

4.9 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［24］，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［25］。

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［26］。

「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［27］。

4.10 プライバシー・バイ・デザインと法律

自己の情報に関して，その収集・利用・開示を決定できる権利は，自由な社会が形成される本質的な基盤である。技術的進歩が，このような権利とその権利を効果的に行使する個人の能力に対して新規の問題提起を始めた。規制および方針というものは，もはや，プライバシーを守るには十分ではない。情報技術がますます複雑化し，しかも，技術間の連携が強化されるという情況では，プライバシーをシステム設計及びシステムプロセスに直接的に埋め込む方法以外に解決策は存在しないとまで言われている［28］。

「プライバシー・バイ・デザイン」（PbD: Privacy by Design）という概念は，情報通信技

術（ICT）の成長と系統的効果を向けられ，情報の全生涯（情報の取得から消去まで）に係る，情報技術とシステムの設計・稼働・管理の中にプライバシーを埋め込むことである［29］。

4.11 クラウドコンピューティング技術と法律

個人情報を含む情報処理システムは，その構造において，プライバシー・バイ・デザイン（privacy by design: PbD）ということが要求されている。クラウドはその PbD 技術を提供する。それは，プライバシー影響評価におけるチェックリストに反映されるべきである。

個人データのための特別なセグメントを有するシステムのアプリケーション構造にユーザがどのようにアプローチするかを考慮することが重要である。とりわけ，クレジットカードのデータを貯蔵している e コマース・システムや健康データを貯蔵する健康ケアシステムである。プライバシーへの鍵は，クラウドにおいては，センシティブ・データと非センシティブ・データを厳格に区別することである［30］。ただし，非センシティブ・データでも，センシティブな要素は暗号化されているのである。

4.12 アクセス制御技術と法律

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。

クラウドにおいて，ネットワークアクセスコントロールは，クラウド内にあるインスタンスの論理的なグルーピングへの出入口における，ホストベースのアクセスコントロールを実施するクラウドファイアウォールポリシーとして現れる。アクセスコントロールは SPI（SaaS，PaaS，IaaS）クラウド提供モデルにおいて，そして，標準的な応用モデルにおいて，非常に重要なセキュリティ管理機能である［31］。

4.13　構造技術と法律

セキュリティ管理者は，当該システムの外部（周辺）からセキュリティ措置をスタートさせなければならない。そして，中心部へと移動する。サーバやホストコンピュータを無防備のままに放っておいてはいけない。主要周辺レイヤが装備されているならば，セキュリティ管理者は，少なくとも，ひとつのセキュリティ・アンブレラ・レイヤを持つことになり，セキュリティに関して何の装備もないよりは安全である［32］。

このようなレイヤ方法は，階層型セキュリティ方針，すなわち，多重防御（defence-in-depth）を発展させることである。レイヤが重要なのは，保護の水準を追加できるからである。ひとつの階層（レイヤ）が破られても，管理者は，その下に多重の階層を持っており，保有する価値ある資産を継続的に保護することができる。たとえば，ある攻撃者がファイアウォールを破ろうとしているならば，その次には，IDS（Intrusion Detection System：侵入検知システム）が立ちはだかり，さらには，ネットワーク全体に及ぶ危険から保護するためのホスト・セキュリティが用意されている［33］。このような方法によって，他のどのシステムが危険に曝されているのかについて気を配る必要はなく，当面のファイアウォール問題に集中して取り組むことができる。

5.　情報技術の安全基準と構造基準

5.1　情報技術の安全基準

ある情報技術を利用する際に通常の利用方法に従って利用すれば，当該技術に起因する事故は発生しないという程度の安全性の基準がある。

生体認証システムは，文字数字式のパスワードや個人識別番号のような従来型の方法に対して，国のセキュリティからクレジットカード処理にいたるまでいくつかの分野においてセキュリティを保証する絶対に誤ることない方法と考えられてきた［34］。

生体認証協会は，アプリケーションレベルとデバイスレベルのインタフェースに関して広く受け入れられるような基準を開発した。それはOS及びベンダー依存型ではない。生体認証システムに含まれる情報の機微性のために，国の内外からの侵入者によって攻撃されるだろうと思われている［35］。

電子署名の安全性の基準は，「整数の素因数分解」，「離散対数の計算」，または「離散対数の計算」の有する「困難性」に基づくものとされている。この電子署名に利用される情報技術は暗号化技術であるので，この安全性の基準は，暗号化技術の安全性の基準に当て嵌まるものである。

5.2 情報技術の構造基準

生体認証システムに関して，保管方式および通信方式のいずれにおいても，貯蔵された情報に係わる保証性と安全性のメカニズムが必要とされる。重要なことは，生体認証システムが安全に利用され得るように，当該システムの構造と運営の基盤となる設計原理を把握することにある。

生体認証システムによって確保された安全性の水準を最大限にするために，多様式型システムが識別と証明目的のための単一の生体認証よりは効果的なものとして考えられている。多様式型生体認証システムは，多重センサーから得られた同一の個人の複数のシグネイチャ（サイン）を活用する。単一センサから得られた情報では十分な特徴が欠けているので，多重センサーから獲得した情報（シグネイチャ）を活用することによって，識別・証明システムの高精度化を図ることでその欠点を補足している［36］。

前節で電子署名，すなわち，暗号化技術の安全基準に触れたが，このような安全性の水準を維持するためには，暗号化技術の構造もその水準にあるものでなければならない。したがって，暗号化技術の安全性の基準は，同時に，その技術の構造基準になっていると言える。

5.3 基準の必要性

法律の中に取り込まれたこれらの情報技術の利用者は当該法律の名宛人である。その名宛人は法律を遵守する義務がある。その利用者は契約を締結したり行政手続を遂行する時に，これらの情報技術を利用することになろう。法律の名宛人のほとんどは，通常，情報技術について十分な知識を有しているとは考えられない。このことは，法律と情報技術の協働を導入する際に，第一に考慮されなければならないことである。

それゆえ，それらの情報技術には，安全性および構造について，一定の基準が設定されていなければならない。情報技術の安全性の水準が保証されなければならない。そして，その安全性の水準を実現できる構造が要求される。この協働が成功するには，それらの基準を模索するための情報技術影響評価が欠かせない。個人情報・個人データを扱うシステムに対しては，少なくとも，プライバシー影響評価が実施されなければならない［37］。

情報技術は，また，法律執行機関，すなわち，警察行政においても利用されている。しかし，その利用目的は，前述の協働の目的とはまったく異なるであろう。だが，当局は，効果的で，情報豊富な警察業務にとっては不可欠な手段であるといわれる［38］。

そのうえ，技術もまた大きなセキュリティ・リスクをもたらすということも認識されている。適切なセキュリティコントロールもなく，基幹業務用の情報技術システムを操作する法律執行機関は，社会に，警察自身に，そして政府に，最大の危険性をもたらすことになる。このようなシステムの中のデータはとりわけ機微なものであり，基幹業務に必須のものであ

る。センシティブ事案の報告，秘密捜査データ，機関の諜報，容疑者情報，個人情報，および人事情報などは，悪意の攻撃，信頼できない内通者，システムの偶発的誤用あるいは自然災害等々による危険に曝されているデータの例である［39］。

6. 結　　論

今日，時代はいわゆる「ユビキタス時代」である。その情報環境においては，人は 1 週間のうちの 7 日間，1 日のうちの24時間インターネットに接続した情報端末を利用することができる。電子政府は，行政手続において情報技術の利用を勧めている。人は，コンピュータを操作しながら法律行為を実行することができる。しかも，同時に関連法律を遵守する結果になっている。

前章で述べたように，法律と情報技術の融合は，適法性や法律遵守の情況を向上させている。法律の目的を実現するために，法律の中での情報技術の応用を推進する条項を持つべきであると考える。

法律の中には，情報技術の応用を明確に宣言するものもある。あるいは，それほど明示的ではないにしろ，情報技術の応用を示唆しているものもある。結果的には，情報技術以外の方法では法律を実現できないわけである。

電子消費者契約法の中には，消費者が電子的方法，情報処理システムおよび通信ネットワークシステムを利用すべきであるということを記述する数カ条が存在する。法律の目的を実現するために，法律は，当該法律の条項の中に，情報技術の利用を促すような明文規定を配置すべきである。同法は，消費者に対して，情報技術の利用を求めている。しかしながら，電子署名法は，その中には，情報技術の利用を明示的な方法で規定しているわけではない。同法のいくつかの条項は，暗号技術を用いることなくして，同法の目的は達成できないことを示唆している。

プライバシー影響評価制度におけるプライバシー・バイ・デザインの手法は，技術的措置を用いてプライバシー・リスクを最小化することを目指している。この手法は，プライバシーの課題が現実的問題となる前にそれらの課題を評価しそれに取り組むことである。移動型通信機器企業は必要なプライバシー措置が設計において取り込まれている，あるいは埋め込まれていることを保証する責任を持つべきである。

コンピュータシステムの重要な要素が情報社会において多くの社会システムの中に取り入れられている。なぜなら，コンピュータシステム自体が政治的・社会的性格を具有しているからである。

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，それらの利用者に対して，ある倫理的な配慮を要請する。つまり，そのような技術はその利用者に倫理的行動をとるように仕向けるのである。それゆえ，このような技術は倫理的技術という性格を有するものと考えられる。

このような技術は，法律そのものに代わって，当該法律の内容を実現するために利用されると言うことができよう。なぜなら，かかる技術は社会的で倫理的であるからである。ここに，法律と情報技術の協働の意義が見出されるのである。すなわち，その協働は社会的正義ならびに法的正義の実現を目指している。それゆえに，このような手法は，法律と情報技術の協働というよりはむしろ融合という方がふさわしいであろう。つまり，前述の目的の達成のため，情報技術が法律の中に埋め込まれた状態で，つまり，両者が統合化された状態であるからである。

この協働にはさまざまな問題があるのは確かである。まず，技術が技術を規制することの正当性である。第二には，この協働はある情報技術がインストールされたコンピュータシステムを利用せざるをえないということが起こる。第三に，この協働が技術の進歩に対応しなければならない。最後には，技術の標準化という問題が残される。

コンピュータシステム技術は日々進歩を続け，留まることはない。したがって，どんな要求であろうと，コンピュータ技術はその要求に応える時が必ずややってくるもと信じている［40］。

法律は，社会と技術の双方の発展の姿を自らに反映させなければならない。技術決定主義者も社会調整主義者も完全に正しいとはいえない。情報社会は，デジタル技術によって能力を与えられた人々と調整的役割りの人々の関係の中に根ざしているといえる［41］。

参照・引用文献

［1］ 参照，北原宗律『情報社会の法律』創成社　2012年。
［2］ Andrew Murray, *Information Technology Law: The Law and Society*, Oxford Univ. Press 2010, p. 327.
［3］ 参照，『情報通信白書』（2003年英語版），62頁以下。
［4］ Cf., National Law Enforcement and Corrections Technology Center, *A Guide for Applying Information Technology in Law Enforcement*, U.S. Department of Justice 2001, p. 1.
［5］ M. E. Whitman/H. J. Mattord, *Management of Information Security,* 2nd ed., THOMSON 2008, p. 384.
［6］ Kent Reichert, Use of Information Technology by Law Enforcement, 2001, pp. 1–4.（http://www.sas.upenn.edu/jerrylee/programs/fjc/paper_dec01.pdf）.
［7］ M. E. Whitman/H. J. Mattord, Management of Information Security, 2nd ed., THOMSON 2008, p. 384.
［8］ National Law Enforcement and Corrections Technology Center, ibi., pp. 1–2.
［9］ Y. Akdeniz/C. Walker/D. Wall（eds.）, The Internet, Law and Society, Longman 2000, p. 320.
［10］ Cf., M. Andress, *Surviving Security: How to Integrate People, Process, and Technology,* SAMS 2002, pp. 88ff.
［11］ Y. Akdeniz/C. Walker/D. Wall（eds.）, Ibid.
［12］ Tim Mather/Subra Kumaraswamy/Shahed Latif, *Cloud Security and Privacy*, O'REILLY 2009, p. 220.

［13］ 参照，北原前掲書，153頁。
［14］ Tim Mather/Subra Kumaraswamy/Shahed Latif, *Cloud Security and Privacy*, O'REILLY 2009, p. 220.
［15］ M. E. Whitman/H. J. Mattord, *Reading and Cases in the Management of Information Security*, Course Technology 2006, p. 63.
［16］ M. E. Whitman/H. J. Mattord, *Management of Information Security,* 2nd ed., THOMSON 2008, p. 373.
［17］ Ibid.
［18］ M. E. Whitman/H. J. Mattord, *Principles of Information Security,* 3rd ed., Course Technology 2009, pp. 245－246.
［19］ Tim Mather/Subra Kumaraswamy/Shahed Latif, *Cloud Security and Privacy*, O'REILLY 2009, p.220.
［20］ Ibid.
［21］ Tim Mather/Subra Kumaraswamy/Shahed Latif, ibid., p. 221.
［22］ M. E. Whitman/H. J. Mattord, ibid.
［23］ Ibid.
［24］「Do Not Track」規制の変遷については，参照，城田真琴『ビッグデータの衝撃』東洋経済　2012年，193頁以下。
［25］ 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.
［26］ Cf., ibid., The Do Not Track Field Guide.
［27］ US FTC, ibid., pp. 4－5.
［28］ The Commissioner's Message, in: Privacy by Design: Strong Privacy Protection – Now, and Well into the Future, A Report on the State of PbD of the 33rd International Conference of Data Protection and Privacy Commissioners, 2011.
［29］ Ibid., p. 3.
［30］ M. Andress, *Surviving Security: How to Integrate People, Process, and Technology,* SAMS 2002, pp. 26－27.
［31］ 参照，ティム・マザー／サブラ・クマラスワミ／シャヘド・ラティフ『クラウドセキュリティ＆プライバシー』オライリー・ジャパン2010年，123頁以下。
［32］ M. Andress, ibid., p. 25.
［33］ M. E. Whitman/H. J. Mattord, *Management of Information Security,* 2nd ed., THOMSON 2008, p. 64.
［34］ Ibid.
［35］ M. E. Whitman/H. J. Mattord, *Principles of Information Security,* 3rd ed., Course Technology 209, pp. 340ff.
［36］ Cf., Office of the Privacy Commissioner（Australian government）, *Privacy Impact Assessment Guide,* 2006.
［37］ COPS（U.S. Department of Justice）, *Law Enforcement Tech Guide for Information Technology Security: How to Assess Risk and Establish Effective Policies*, 2006, p. 3.
［38］ Ibid.
［39］ Ibid.
［40］ P. G. Neumann, *Computer Related Risks,* Acm Press 1995, p. 4.
［41］ Andrew Murray, ibid., p. 574.