高度知識情報化社会における個人情報保護に関する考察
－個人情報の収集・侵害類型と侵害防止技術を中心に－

成　　者政
葛西　和廣

A Study on Personal Information Protection in Advanced Information Society
-Focusing on the Collection, Invasion Type and Invasion Prevention Technology of Personal Information-

SUNG Kijung and KASAI Kazuhiro

要　旨

近年，社会の知識情報化の進展に伴い，コンピュータやネットワークを利用し，大量の個人情報が処理されるようになった．このような個人情報の取り扱いは，今後，ますます拡大していくと予想されるが，個人情報は，その性質上いったん誤った扱いをされてしまうと，当該個人などに取り返しのつかない被害を及ぼす恐れがあるものである．

そこで本稿では，個人情報保護の必要性と個人情報の保護に関する法律の概要などをふまえ，主に個人情報の収集・侵害類型と侵害防止技術などについて考察を行った．

キーワード

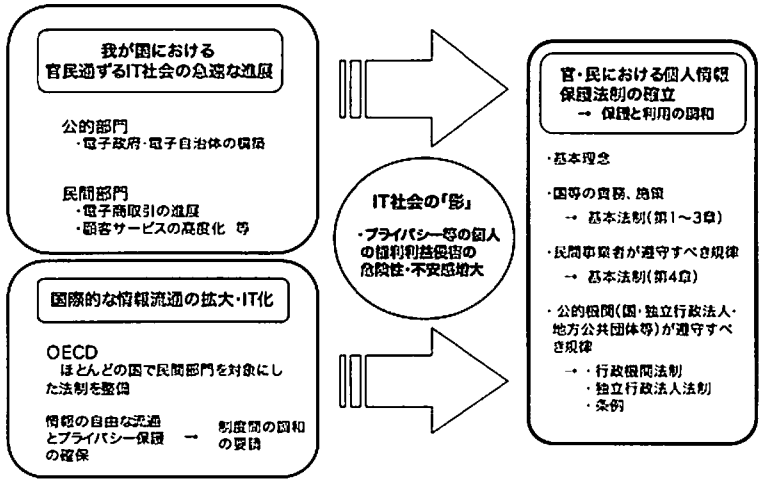
個人情報保護　　個人情報の収集・侵害類型　　個人情報の侵害防止技術

目　次

Ⅰ．はじめに－個人情報保護の必要性と背景－

近年，社会の知識情報化の進展に伴い，コンピュータやネットワークを利用し，大量の個人情報が処理されるようになった．このような個人情報の取り扱いは，今後，益々拡大していくと予想されるが，個人情報は，その性質上いったん誤った扱いをされてしまうと，当該個人などに取り返しのつかない被害を及ぼす恐れがあるものである[注1]．また，高度情報化社会の出現により，現代人は，自らの個人情報を外部に提供・漏洩させずには正常な社会・経済活動を営みにくくなり，個人情報の利用価値の増大は公共部門はもちろんのこと，民間領域での個人情報の収集・利用・保有を増加させる要因になっている（図表1）．

＜図表1＞　個人情報保護法制整備の背景



資料：内閣府国民生活局「個人情報保護法の解説」ウェブサイト資料による．

そして，情報技術（IT）の発展により個人情報および生活が，漏出され悪用されるケースの発生と，自由な通信秘密が保証されないなど，基本的な人権侵害の原因をも提供している．また，組織業務においても統合的な業務環境により非権限者が個人情報の照会を行ったり，重要情報のデータベース化によりある意味では情報管理が難しくなり，またネットワーク技術の発達により外部からのハッキングや内部者による情報流出が容易になっているのが現状である．

企業が消費者に適切で，差別化された商品やサービスを提供するために，個人情報の必要性が増加するほど，消費者の情報プライバシーは，益々侵害の可能性が増加するようになる．企業の立場では，消費者のプライバシーニーズを解決するために個人情報を健全に利用することで，企業の競争力を高め，消費者の個人情報を保護するための法的，制度的，技術的な措置を設けることはいうまでもないことであろう．

そこで本稿では以上のことをふまえ，主に個人情報の収集・侵害類型と侵害防止技術について考察を行った．

[注1]「個人情報の保護に関する基本方針」2004年4月2日閣議決定，1～2頁．

Ⅱ．個人情報保護の概念的整理と日本における個人情報保護

1．個人情報の概念

一般的に個人情報とは，個人の精神，身体，財産，社会的地位，身分などに関する事実・判断評価を示す個人に関する情報および当該情報に含まれている氏名，生年月日などの事項により個人を識別できる情報のことである．個人情報（Personal Information）について旧通商産業省（現，経済産業省）の定義[註2]を見ると，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，または個人別に付された番号[註3]，記号その他の符号，画像もしくは音声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）[註4]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[註5]を除く．すなわち，個人に関する情報であって，直接その情報により，またはその情報とその他の情報を組み合わせて，当該個人を識別することができる情報のことである．

そして，1978年から専門家グループによる作業を行い，OECD（経済協力開発機構）理事会の勧告案[註6]として1980年9月23日に採択された「プライバシー保護と国家間流通に関するガイドライン（Guideline on the Protection of Privacy and Transborder Flows of Personal Data)」[註7]は個人情報（正確には個人データ <personal data>）に関して，識別される，または識別されうる個人（情報主体）に関するすべての情報（any information relating to an identified or identifiable individual（data subject）と定義づけている[註8]．

2003年5月に成立し，2005年4月1日から全面的に施行された日本の個人情報の保護に関する法律によると，「個人情報とは，生存する個人の情報であって，特定の個人を識別できる情報（氏名，生年月日など）を指す．これには，他の情報と容易に照合することができることによって特定の個人を識別することができる情報（学生名簿などと照合する

[註2] 「民間部門における電子計算機処理に係る個人情報ガイドライン・解説書」『個人情報保護ハンドブック』通商産業省，1998年6月，6～7頁．

[註3] 個人別に付された番号とは，電話番号，銀行口座番号，保険証番号などを指す．

[註4] で定義されている個人情報の定義である．

[註5] 法人その他の団体の役員に関する情報とは，株主総会などで配布される事業報告書など，株主や顧客に配布される書類などに記載されている役員の経歴，持ち株数など，公表されているような情報を指す．

[註6] この勧告には，5部からなるガイドラインが附属している．すなわち，第1部は総則，第2部は国内適用における基本原則，第3部は国際適用における基本原則，第4部は国内実施，第5部は国際協力である．

[註7] このOECD勧告の基礎となったのは「市民的および政治的権利に関する国際規約」である．この国際規約は，1966年12月16日第21回国際連合総会で採択・1976年発効され，いわゆる国際人権B規約（自由権規約）として，基本的人権一般の保障に関する国際的な規約である．その第17条には次のようなプライバシーの権利が保障されている．①何人も，そのプライバシー，家族，住居もしくは通信に対して恣意的にもしくは不法に干渉され，または名誉および信用を不法に攻撃されない．②何人も，そのような干渉もしくは攻撃に対して法律による保護を受ける権利を有する（小林麻理穂『ITの進展と個人情報保護－オーストラリアにみる新たな法の運用とビジネスの展開－』敬文堂，2003年9月，9頁）．

[註8] OECD (2001)，Guideline on the Protection of Privacy and Transborder Flows of Personal Data, OECD, p.13

ことで個人を特定できるような学籍番号など）も含まれる」[註9]としている．ここで注目すべきことは「生存（生存性）」と「識別（識別性）」という言葉である．生存とは，生きている個人を指すので死亡した個人の情報は，この法律が規定する個人情報ではない．その理由としては，死者に関する個人情報は遺族の個人情報となる範囲で保護することができるので，あえて独立して保護する必要はないと考えたからである．

一方，識別の意味することは氏名，生年月日，住所，電話番号だけではなく，顔写真，画像，もしくは音声により当該個人を識別できるものであれば個人情報となる．また，それ自体では当該個人を特定できない断片的な情報であっても，その他の情報と照合することにより容易に当該個人を特定できる情報は個人情報となる．ひいては性別，年齢，趣味などの情報も個別的に使用される場合は識別できないが，このような情報が照合され，個人情報になる可能性もある（図表2）．

＜図表2＞　個人情報の範囲

ケース	該当の有無	説明
本人の氏名	○	多くの場合，特定の個人を識別できる
電話番号	○	他の情報と照合することで特定の個人を識別することができる
防犯カメラに映っている本人の映像	○	文字情報に限らず，特定の個人を識別できるものなら音声や画像も個人情報になる
雇用管理情報	○	企業が社員を評価した事項を含む
死者に関する情報	×	個人情報といえるためには，生存性が必要である
企業の財務情報	×	個人の情報ではない
単なる文字や数字が並んだだけのメールアドレス	△	ABC012@×××.co.jp のようなメールアドレスの場合，容易に個人を識別できない．ただし，コンプライアンス徹底という視点からは，個人情報として保護した方が無難である

資料：岡伸浩『図解個人情報保護法早わかり』中経出版，2005年2月，25頁．

EU欧州連合の「データ保護指令（Directive for the protection of personal data and privacy）」[註10]での個人情報とは，識別される，または識別可能な自然人（情報主体：企業やそれに準ずる団体と対比しての個人）に関連したすべての情報と定義づけ，この場合の識別可能な自然人とは識別番号（IDナンバー）の照合や個人の身体的，生理的，精神的，経済的，文化的，社会的特徴によって，直接的，または間接的に特定することができる者を意味する．

以上により，個人情報に関する定義は少しずつ異なるが，意識の表現，すなわち思想と

[註9]『個人情報の保護に関する法律』第1章第2条第1項（平成十五年五月三十日法律第五十七号）．

[註10] EUの個人情報保護法案は，「データ保護指令」としてOECDのガイドラインに基づき，1990年に欧州委員会（EC）が提案し1995年10月に発行され，加盟国が取るべき措置を詳細に定めたものである．この指令の目的は加盟国間の情報の自由な流れを確立し，維持すること，またEU諸国から加盟国以外の国への情報の流れを管理し，監視することにある．1997年12月には，「通信部門における個人データ処理及びプライバシー保護に関する欧州議会及び理事会の指令」を発行，そして1998年10月には「データ保護指令」を施行し，その第25条において，個人データに関する十分なレベルの保護が行われていない第3国への個人データの移動を禁じている（KOJINJOHO.comのウェブサイト資料による）．

信条が含まれ，他人と識別できる情報，言い換えれば，個人識別情報が主な内容になる情報であるといえる．

そして，一般的に，個人情報は＜図表3＞のように分類することができる．

＜図表3＞　個人情報の類型と具体的な例

分　　類	細　　分　　類	例　　示
1)戸籍的事項に関する情報	氏名，住所，性別，生年月日，本籍，続柄，婚姻，離婚，離縁，養子縁組，認知，禁治産，準禁治産，死亡などに関する情報	戸籍簿，除籍簿，戸籍見出簿，除籍見出簿，戸籍受付帳，人口動態調査票，住民異動届
2)経歴に関する情報	(1)学籍などに関する情報:学校名，入学・卒業年度，学業成績，退学・休学・停学の処分など	農業委員の経歴書,民生委員台帳，民生・児童委員候補者内申書，表彰候補者推薦調書，外国派遣者の経歴書
	(2)職業・職歴などに関する情報:所属会社名，職種，地位，在職期間，就職・退職年月日，昇任昇格・降任降格・配置転換，解雇・停職などの処分，職務の実績・評価，職歴，資格など	
	(3)賞罰に関する情報:叙位・叙勲・褒賞・表彰，犯罪・違反・補導歴など	
	(4)知識，技術，能力などに関する情報:各種試験の成績，資格・免許の種類，取得年月日，免許の停止，取消などの処分	
	(5)その他経歴，社会的活動に関する情報	
3)心身に関する情報	(1)心身障害などに関する情報:精神障害・身体障害の有無・程度，訓練記録など	精神保険法21条に基づく市長同意書
	(2)傷病，健康状態などに関する情報:傷病名，傷病歴，傷病の原因，治療の内容・方法・期間，検診結果，看護記録など	行旅病院取扱調書，療養見舞金申請書，生活保護医療券および診療報酬明細書
	(3)検査，診療などに関する情報:検査名，検査結果など	生活保護検診命令書，レントゲン間接撮影者名簿
	(4)その他心身に関する情報	
4)財産状況に関する情報	(1)資産などに関する情報:所有不動産・動産の種類・価格，債権・債務の内容，預貯金の種類・金額，相続・贈与などの有無・評価額	土地評価調書,換地計算書,生活保護台帳
	(2)収入などに関する情報:所得の種類・金額，課税・納税の金額，税などの滞納状況，給付金・補助金・貸付金などの受給・償還状況など	生活保護収入等申告書，母子寡婦福祉資金申請書，国民健康保険料滞納経過簿，国民健康保険料賦課台帳
	(3)その他財産状況に関する情報	
5)思想，信条などに関する情報	思想，信条，主義主張，信仰，宗教，支持政党，性格，意識，趣味，嗜好などに関する情報	
6)その他国民生活に関する情報	(1)家庭状況に関する情報:家族，扶養関係，同居・別居の別，父子・母子家庭である事実，里親・里子である事実，生活の状況など	生活保護扶養義務調書，母子世帯名簿，児童扶養手当名簿，児童手当現況届
	(2)住居状況に関する状況:住居の間取り・構造，持家・借家の別，居住人数，居住期間，敷地などの権利など	補償物件調査票，補償算定調書，補償物件写真集，換地割込図
	(3)公的扶助などに関する情報:要保護・準要保護世帯・生活保護受給者である事実，厚生施設・社会福祉施設などへの入所状況など	生活保護ケース記録票，生活保護面接記録票
	(4)社会的活動状況に関する情報	
	(5)その他個人生活に関する情報:苦情・要望，相談などの内容，私人間の紛争の内容，交友関係など	加入団体名，市民相談処理カード，母子家庭相談者処理カード，人権，同和問題相談事例報告書

資料：鴇野幸雄・内野伸之「石川県における情報公開制度の運用とその問題点－金沢市情報公開および個人情報保護制度を中心に－」『金沢大学大学教育開放センター紀要』Vol.15，金沢大学，1995年8月，64～66頁．

2．個人情報保護基本法制に関する経緯

パーソナルコンピュータ（PC）とインターネットの普及・発達などに代表される高度情報化社会の影響により，情報技術（IT）を利用し大量の個人情報が処理・利用されるよ

うになっている．ここでは日本における個人情報保護基本法制に関する主な経緯[註11]について簡略に述べると＜図表4＞のとおりである．

＜図表4＞　日本における個人情報保護基本法制に関する主な経緯

●1980年
・9月：プライバシー保護と個人データの国際流通についてのガイドラインに関するOECD理事会勧告

●1988年
・12月16日：「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」公布

●1999年
・2月28日：総理答弁（参議院本会議：住民基本台帳法一部改正法案質疑）
・7月23日：高度情報通信社会推進本部「個人情報保護検討部会」初会合
・11月19日：個人情報保護検討部会「我が国における個人情報保護システムの在り方について（中間報告）」
・12月3日：高度情報通信社会推進本部決定「我が国における個人情報保護システムの確立について」

●2000年
・2月4日：高度情報通信社会推進本部「個人情報保護法制化専門委員会」初会合
・6月2日：個人情報保護法制化専門委員会「個人情報保護基本法制に関する大綱案（中間整理）」
・10月11日：個人情報保護法制化専門委員会「個人情報保護基本法制に関する大綱」
・10月13日：情報通信技術（ICT）戦略本部決定「個人情報保護に関する基本法制の整備について」

●2001年
・3月27日：「個人情報の保護に関する法律案」提出（第151回国会）

●2002年
・3月15日：「行政機関の保有する個人情報の保護に関する法律案等4法案」提出（第154回国会）
・12月6日：「与党三党修正要綱」公表
・12月13日：「個人情報の保護に関する法律案」等審議未了廃案（第155回国会）

●2003年
・3月7日：「個人情報の保護に関する法律案」等再提出（第156回国会）
・5月23日：「個人情報の保護に関する法律案」可決・成立
・5月30日：「個人情報の保護に関する法律」公布

●2005年
・4月1日：「個人情報の保護に関する法律」施行

資料：首相官邸ウェブサイト資料による．

3．日本における個人情報の保護に関する法律の概要

この法律[註12]は6章59条と附則7条とからなり，第1章に目的，定義および基本理念を規定し，第2章に国および地方公共団体の責務など，第3章に個人情報保護に関する施策などについて規定している．そして，第4章に個人情報取扱者の義務など，第5章に雑則，第6章に罰則として構成されている．

[註11] これは首相官邸のウェブサイト資料による．

[註12] 個人情報の保護に関する法律の概要については，小林麻里絹「ITの進展と個人情報保護」敬文堂，2003年9月；岡　伸浩『図解個人情報保護法早わかり』中経出版，2005年2月；田淵義朗他『45分でわかる個人情報保護』日経BP社，2005年4月；三上明照「個人情報の保護に関する法律の概要」『Jurist』NO.1253，2003年10月，24～32頁；植山克郎「個人情報の保護に関する法律の概要」『NBL』通巻第764号，2003年7月，15～21頁；菱山大「個人情報の保護に関する法律について」『銀行法務21』2003年8月，4～10頁；吉羽真一郎・池村聡「個人情報保護法を理解しよう」『COMPUTRE & NETWORK LAN』No.252，2004年10月，68～82頁；赤堀勝彦「個人情報保護法についての一考察－企業の個人情報漏洩のリスクマネジメントについて－」『長崎県立大学論集』第39巻第4号，長崎県立大学，2006年3月，97～142頁；齋藤聡「個人情報保護法について」『産能大学紀要』第25巻第2号，産能大学，2005年2月，85～113頁などを参照されたい．

3-1. 目的と基本理念

この法律は高度情報通信社会の進展に伴い，個人情報の利用が顕著に拡大している中で，個人情報の適正な取り扱いをつうじて，個人情報の有用性に配慮しながら，個人の権利利益を保護することを目的としている（第1条）．また，個人情報は個人の人格と密接な関連を有するものであり，人格尊重の理念のもとで慎重に，適正に取り扱われるべきであることを，その基本理念として宣言している（第3条）．

3-2. 国および地方公共団体の責務および施策

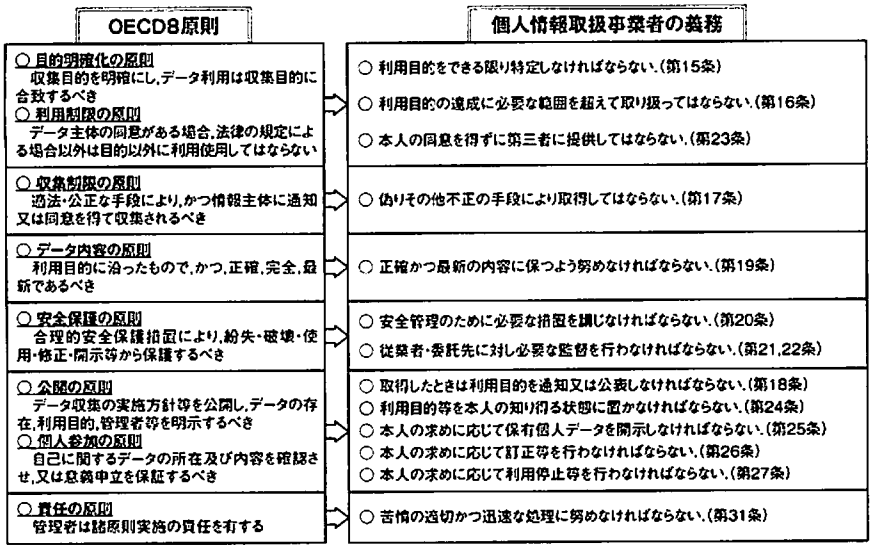
国と地方公共団体はこの法律の趣旨に従い，個人情報の適正な取り扱いを確保するために必要な施策を総合的に策定し，これを実施すべきである（第4，5条）．また，国は地方公共団体などを支援（第8条）し，苦情処理のための措置（第9条）および個人情報の適正な取り扱いを確保するための措置（第10条）を取らなければならない．

一方，地方公共団体は保有する個人情報を保護（第11条）し，地域内の事業者などを支援（第12条）し，事業者と個人の間に発生した苦情処理を斡旋（第13条）すべきである．

3-3. 個人情報取扱事業者の義務

この法律は，個人情報取扱事業者[注13]について具体的な義務を課しているが，この義務規定は個人情報保護の国際標準ともいえるOECDプライバシーガイドラインの8原則に沿ったものになっている（図表5）．

＜図表5＞　OECD8原則と個人情報取扱者の義務規定の対応



資料：首相官邸ウェブサイト資料による．

1）利用目的の特定および制限など

個人情報取扱事業者（以下，事業者と略する）は利用目的を可能な限り特定すべきで，

[注13] 個人情報取扱事業者とは，個人情報を，コンピュータなどを用いて検索することができるよう体系的に構成した個人情報データベースなどを事業活動に利用している事業者のことである．

利用目的を変更する場合は変更前の利用目的と相当な関連性を有すると合理的に認められる範囲を超えてはならない（第15条）．また，事業者は事前に本人の同意を得ずに特定された利用目的の達成に必要な範囲[注14]を超えて個人情報を取り扱ってはならない．この場合，法令などによる例外が認められている（第16条）．

個人情報の取得時にも事業者は虚偽，その他不正な手段により取得してはならない（第17条）．そして個人情報を取得した場合は事前にその利用目的を公表した場合を除いては迅速にその利用目的を本人に通知，または公表すべきである（第18条）．

2）データ内容の正確性の確保

事業者は，利用目的の達成に必要な範囲内で，個人データを正確，かつ最新の内容に保つように努めるべきである（第19条）．

3）安全管理措置および第3者への提供制限

事業者は，個人データが漏洩，滅失，毀損の防止，その他個人データの安全管理に必要で適切な安全管理措置[注15]を講ずるべきである（第20条）．そして，事前に本人の同意を得ずに，個人データを第3者に提供してはならない，ただし，法令などによる例外がある（第23条）．

4）公表・開示・訂正および利用停止

事業者は，個人データの利用目的などを本人に知り得る状態におくことを求められ（第24条），本人から当該本人が識別された個人データの開示を要求された際には直ちに開示することが，義務づけられている（第25条）．また，事業者は，保有個人データの内容が事実ではない理由で訂正，追加，削除要求を受けた場合，直ちに必要な調査を行い，その結果により訂正などをしなければならない（第26条）．そして，事業者は，利用目的の制限に違反して個人情報を取り扱っている場合や，違法な個人情報の取り扱いをしている場合は，本人からの要求に応じて利用停止，または消去を行うこと（第27条）が求められている．

Ⅲ．個人情報の収集方法および侵害類型

1．個人情報の収集方法－技術的手段を用いた情報の収集－

1-1．クッキー（Cookie）

クッキーとは，ウェブサイトの提供者が，ウェブブラウザをつうじて訪問者のコンピュータに一時的にデータを書き込んで保存させるしくみのことである．Cookieにはユーザーに関する情報や最後にサイトを訪れた日時，そのサイトの訪問回数などを記録しておくこ

[注14] ここでいう「特定された利用目的の達成に必要な範囲」とは，個人情報の取り扱いの手段，方法はもちろんのこと，取り扱う情報の内容，量などからみて，目的の達成に必要な限度を超えないことが要求されている（菱山大「個人情報の保護に関する法律について」『銀行法務21』2003年8月，7頁）．

[注15] ここでいう「適切な安全管理措置」とは，安全管理者の設置，監査体制の整備といった組織的保護措置や外部に接続するネットワークにおけるファイアーウォールの構築や情報の暗号化といった技術的措置が挙げられる（菱山大，前掲書，8頁）．

とができる．Cookie はユーザーの識別に使われ，認証システムや，WWW によるサービスをユーザーごとにカスタマイズするパーソナライズシステムの要素技術として利用されている[註16]．

一般的に，ユーザーが公開しない限り，クッキーそれだけではユーザーの身元をさらけ出したり，クッキーを用いてユーザーが訪問したサイトを確認することもできない．

しかし，ユーザーの身元確認のためにクッキーが用いられる方式[註17]としては，次の二つが挙げられる．まず第一に，クッキーはログイン情報（たとえば，氏名，住所，パスワードなど）を呼び出すのに使用される．第二に，クッキーの情報とマーケティングデータベースにあるユーザーの氏名，住所，以前の消費情報などを比較することでユーザーの身元を確認することができる．

1-2. ウェブバグ（Web bug）

ウェブバグはオンラインユーザーが知らない間にユーザーに関する情報を流出，またはユーザーのシステムを破壊することもできる技術のことである．これはウェブサイトに植えておいたきわめて小さいグラピックイメージファイルで，通常，当該ウェブページの壁紙（wallpaper）と同じ色を持つことで肉眼では見えないようになっている[註18]．

ウェブバグは，次のような情報を自分のホームサーバーに送ることができる．

①ウェブバグが設置されているページを訪問したコンピュータの IP アドレス
②ウェブバグが設置されているページの URL
③ウェブバグイメージの URL
④ウェブバグの設置されているページが閲覧された時間（日時）
⑤ウェブバグを持って行ったウェブブラウザの種類
⑥ウェブバグのホームサーバーが以前にユーザーのコンピュータに設置したクッキーの固有番号など

1-3. スパイウエア（Spyware）

スパイウエア[註19]とはコンピュータを使うユーザーの行動や個人情報などを収集したり，マイクロプロセッサの空き時間を利用して計算を行ったりするアプリケーションソフトのことである．得られたデータはマーケティング会社など，スパイウェアの作成元に送られる仕組みになっている．

スパイウェアは他のアプリケーションソフトとセットで配布され，インストールの際には，そのソフトと一括して利用条件の承諾などが求められる．また，スパイウェアはユーザーに気づかれないよう，ウィンドウなどに出ずにバックグラウンドで動作するため，ユーザーは，スパイウェアがインストールされていることさえ気づきにくい特徴を持っている．

スパイウェアが行なう活動の内容は，実はインストール時に表示される利用条件の中に

[註16] IT 用語辞典 e-Word のウェブサイト資料による．
[註17] Jang, B.J.（2003），p.36.
[註18] ウェブバグは，大きさが 1 × 1pixel 程度なので，「1-by-1 GIF」と呼ばれ，また肉眼では見えないので「clear GIF」とも呼ばれる．
[註19] IT 用語辞典 e-Word：higaitaisaku.com：フリー百科事典「ウィキペディア（Wikipedia）」などのウェブサイト資料による．

書かれているため，インストール時にその利用条件を承諾してしまっている以上，スパイウェアの活動は直ちに違法といえるものではない．しかし，利用条件をまともに読む人はほとんどいないため，ほとんどのユーザーはスパイウェアに気づかず，スパイウェアごとにソフトウェアをインストールしてしまう．このため，スパイウェアは事実上，無断で個人情報を収集しているとして，プライバシー擁護団体などの消費者団体を中心に反スパイウェア活動が起こっている．また，スパイウェアは一般ユーザーの間でもおおむね不評で，特にパソコンの扱いに慣れ，パソコンの動作を熟知しているユーザーほどスパイウェアを嫌悪する傾向がある．

なお，広告を表示する代わりに無料でソフトを利用できるアドウェア（adware）[注20]というものもあるが，意味の上ではアドウェアとスパイウェアの間に直接関係はない．しかし，アドウェアではユーザーに表示する広告を選別するなどの目的で情報収集を行っていることが非常に多く，かなりの割合のアドウェアがスパイウェアの機能を持っているのが現状である．

1-4．バックドア（Backdoor）

バックドア（Backdoor）[注21]とは，システムの開発者などにより密かに仕掛けられた不正な侵入経路のことである．バックドアによっては，システム管理者が関知できないものもある．また，システムに不正に侵入した者が，再侵入を容易にするために設けた接続方法も「バックドア」と呼ばれている．侵入者は，自らバックドアを設定することもあるが，システム管理者によって発覚しないようにするため，バックドアを仕掛ける専用ツール（ルートキット）を使うケースもある．

一部のコンピューターウイルスでは，感染したマシンにバックドアを設置するタイプがあり，無料で公開されているソフトウエアにバックドアが仕組まれていることもある．バックドアは，ホスト型侵入検知システムを導入することで検知することができる．

2．個人情報侵害の類型

個人情報の活用される各段階で，個人プライバシーが侵害される類型として，大きく収集，二次的活用，誤謬（エラー），そして不当なアクセスなどに分類することができる（図表6）．まず第一に，収集（collection）が挙げられる．企業が，正常な方法により個人情報を収集・利用することは個人情報の侵害にはならない．たとえば，消費者がサービスを受けるために保険契約を行う場合，情報主体としての消費者は氏名，住所，性別，所得，健康状態などの個人情報を提供するようになる．この場合，企業は提供された個人情報を効果的に管理することで差別化された製品やサービスを提供し，競争力を強化することができる．このようなデータベースマーケティング（Database Marketing）[注22]の成否はデー

[注20] これは，ソフトウェアの操作画面に直接広告を呼び出して表示するものや，ウェブブラウザに寄生して一定の間隔で広告ウィンドウを表示させるものなどがある（IT用語辞典e-Wordのウェブサイト資料による）．

[注21] セコムトラストシステムズの「よくわかる情報セキュリティ用語辞典」のウェブサイト資料による．

[注22] データベースマーケティングとは，顧客や見込み客に関するデータを収集し，コンピュータ化（デジタル化）されたリレーショナル・データベースによって管理することで，顧客によりよいサービスを提供し，長期的な関係構築を実現するマーケティングの一つの手法のことである．

＜図表6＞　個人情報の侵害類型

発生段階	侵害類型	具体的な侵害行為
収集段階	不法収集	・情報主体の同意のない個人情報収集 ・個人の私生活や権利を侵害しうる情報収集
処理段階	エラー	・間違えた情報の記録 ・変更された情報を修正しない
保管段階	不当なアクセス	・資料の不法流出（内部人の流出，業務上習得した個人情報の漏洩，外部からの物理的浸透による流出，管理不徹底による流出） ・データの不法閲覧 ・ハッキング，またはウイルス感染などによるデータの閲覧・挿入・変造・破壊 ・ハッキングなどによる資料の盗難
利用段階	二次的活用	・収集目的以外の用度に情報を活用する行為 ・情報主体の同意を得ず，第3者に情報を提供，または販売する行為 ・同意が撤回される，または収集目的が達成されたデータの不法保有

資料：Kim, S.O.（2001），*A Research on Privacy and Personal Information in Korea*, KIC.,p.86.

タベースに収集・貯蔵された情報の正確性によるもので，正確な情報収集は企業活動において不可欠である．企業は効果的なデータベースマーケティングのために個人情報を自らの必要により多様なルートをつうじて収集している．

企業における個人情報の収集段階で，情報プライバシーを保護するために必要のない個人情報の収集は原則的に制限し，合法的で正当な手続きによりデータ主体の認知や同意を得てから収集すべきである．

しかし，他企業の顧客情報などのような外部顧客情報は，消費者の同意，または許可が最初収集主体に与えられたものなので消費者の情報プライバシーを大きく侵害する余地もある．特に，激烈な競争の中で消費者の個人情報が競争優位を獲得するのにきわめて重要な要素として作用するので，企業の不法的な個人情報の収集が行われるおそれもある．

第二に，二次的活用（secondary use）である．特定の目的のために収集された個人情報が本人の同意，または許可なしで他の目的に再利用される場合，個人情報プライバシーは侵害される．最近，個人情報が企業経営に重要な資源として認識されることに従い，これを商業的目的として利用しようとする傾向が増加され，情報仲介業ともいえる専門企業が登場することで個人情報の二次使用はより深刻な問題として浮き彫りにされている．なお，顧客データおよび情報を共有する目的による企業間の戦略的提携が増え，法的訴訟まで提起されるなど社会的問題になっている．

第三に，誤謬（error）である．個人情報は静的情報と動的情報に分けることができるが，この中で動的個人情報は時間の経過に従い，その内容が急激に変化するが，これをデータベースに適切に反映できない場合，誤謬が発生され，個人に対する虚像をもたらし情報プ

[註23] ハッキングの技法として buffer overflow, snoofing attack, sniffing attack, spoofing attack (IP spoofing, ARP spoofing, e-mail spoofing, DNS spoofing), smurfing attack, spam mail, herf gun, scan attack, backorrifice, backdoor, wire tapping, data diddling, super zapping, scavenging などを挙げることができる（成春欽・鈴木尚通・田中正敏・葛西和廣「高度情報化社会におけるサイバー犯罪に関する論考－その概念と手法を中心に－」『松本大学研究紀要』第6号，松本大学，2008年1月，註42）．

ライバシーの侵害になる.

第四に，不当なアクセス（improper access）である．ハッキング行為[注23]のように不当にデータベースにアクセスする場合は，情報プライバシーの侵害が発生するのみならず，組織内の関係者が他の目的で個人情報を操作，流出する場合もある．特に，データベースに不当にアクセスされ個人情報が変更，または破壊されたことすら分からない場合，個人情報プライバシーの侵害はより深刻な問題となる．

Ⅳ．個人情報侵害防止技術

1．ウェブ基盤の個人情報保護技術ークライアントの匿名性提供技術[注24]ー

クライアント（client）はクライアント・サーバー関係で，あることを要求するプログラム，またはユーザーのことである．すなわち，コンピュータネットワークにおいて，サーバーコンピュータの提供する機能やデータを利用するコンピュータのことである．家庭でインターネットを利用する際のパソコンなどがこれに該当する．また，サーバーソフトウェアの提供する機能やデータを利用するソフトウェアのことで，ウェブブラウザなどがこれに該当する[注25]．

たとえば，インターネットの検索の際，ウェブブラウザをつうじてウェブページに関する要求をウェブサーバーすることができる．この場合，ブラウザは要求されたHTMLファイルを持ってきたり，戻す関係においてクライアントの役割を遂行する．このようなクライアントの匿名性を提供する技術の主な目標はユーザーと関連する情報を隠すことで，Anonymizer，Onion Routing，Crowdsなどの技術が開発されている．

1-1．アノニマイザ（Anonymizer）

アノニマイザは，Anonymizer Inc.[注26]がウェブサイトをつうじて提供する，IPアドレスのようなユーザーのインターネット利用情報を隠すツールとして，有料と無料サービスがある．

アノニマイザのメリットとしては次のような二つを挙げることができる．まず第一に，Privacy Testサービスの提供である．Privacy Testとは，ユーザーに本人の個人情報がどのように収集されているかを一目で見せることで，個人情報の流出に対する注意を促すサービスである．すなわち，ユーザーがPrivacy Testを一回クリックすることで，ユーザーのIPアドレス，ブラウザの種類，OSのみならず，ユーザーのインターネット環境，たとえば国家名と都市名などの情報も容易に他人により収集されることが可能である．

第二に，Privacy surfing機能の提供である．アノニマイザはPrivacy surfing機能を利用し，クッキーを利用したオンライン追跡から個人ユーザーのインターネット使用情報を

[注24] Im, J.I.（2004），*A Study on Technological Development and Policy for Privacy Protection*, NCA, pp.95-104.

[注25] Yahoo JapanのIT用語辞典のウェブサイト資料による．

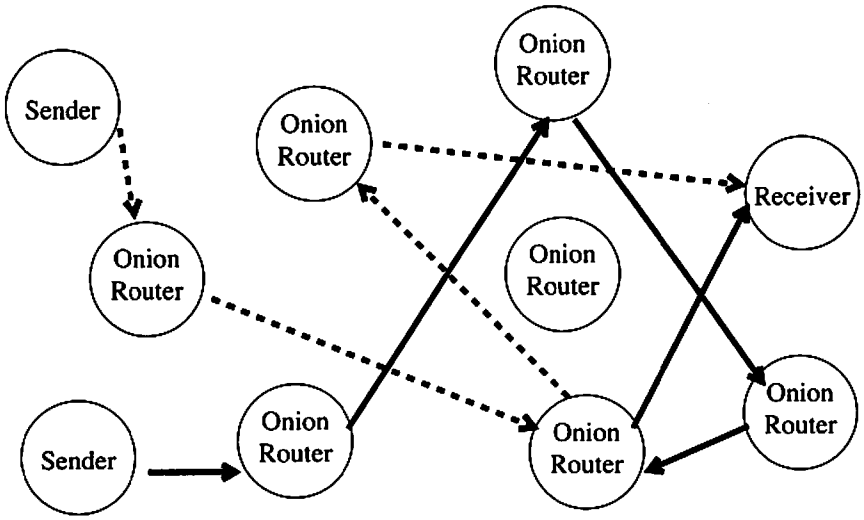
[注26] Lance Cottrelにより設立されたAnonymizer Inc.は個人消費者，法人，団体，そして政府代行機関などのインターネットプライバシーとセキュリティを提供する企業である．この企業はウェブプライバシー市場の先頭として，全世界の数百万のインターネットユーザーに安全なウェブ使用環境の提供を目標としている（http://www.anonymizer.con/）．

保護し，危険要素から防衛する機能を提供している．このサービスはユーザーをアノニマイザのサーバーにログインさせ，追跡されない新しいIPアドレスを割り当てることでウェブ上で匿名性を維持してくれるものである．これは，悪意的な目的を持つハッカーやスパムメールを発送するために情報を収集している人にユーザーの個人情報が漏洩されることを防ぐ役割を担っている．

1-2. オニオンルーティング（Onion Routing）

オニオンルーティング[注27]は公開されたネットワーク上での安全な通信を提供するシステム構造である．これはパケットの匿名性[注28]を維持することを目的として開発されたシステムである．このシステムは送信者（brower），Proxyサーバー，Onion Router，そして受信者（end application）で構成されている（図表7）．

＜図表7＞　Onion Routingの仕組み



資料：古原和邦他「プライバシー保護」11頁．

1）Mix-network基盤

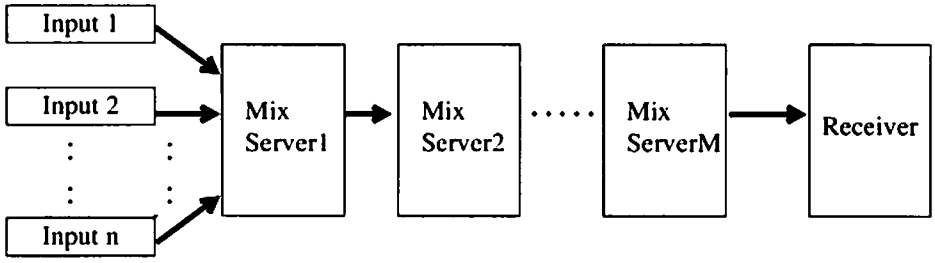
オニオンルーティングは送受信者間の非連結性（unlinkability）をつうじて，匿名性を提供するMix-network[注29]を基盤としている（図表8）．Mixサーバーは反復されるメッセージを除去したり，入力されるメッセージを貯蔵し同時に出力したり，またはこれを再び任意に整列し次のMixサーバーに伝送する機能を提供する．このような場合，Mixサーバーに入力されたメッセージと出力されたメッセージ間の関係を探すことができなくなり，通信中のメッセージの匿名性を提供することができるようになる．

[注27] http://www.onion-router.net/

[注28] オニオンルーティング・ネットワークをつうじてなされた要求は，世界中からランダムに選ばれた2～20台のコンピュータを経由するので，発信元のコンピュータを追跡することが難しくなる．さらに，通信内容と経路も暗号化されるため内容を見ることは困難である（国境なき記者団「ブロガーとサイバー反体制派のためのハンドブック」による）．

[注29] Abe, M.（1998），pp.437-447.

<図表8> Mix Network の仕組み



資料：古原和邦他「プライバシー保護」9 頁.

2) オニオンルーティングの特徴

オニオンルーティングの特徴としては，まず第一に，トラフィック分析（traffic analysis）および盗聴防止である．オニオンルーティングは現存する匿名性を提供する通信システムを調査・設計・具現，そして分析することを目的として実行されたプロジェクトの結果物である．このようなオニオンルーティングはインターネット基盤の連結指向システムとして，悪意的な攻撃者によるトラフィック分析および盗聴防止を目標とする．

第二に，非連結性の保障である．オニオンルーティングを用いたユーザーは誰と通信したか他人に知ることができないので，正当なユーザーではない攻撃者は，ネットワーク上で単に通信が行われた事実のみを知るしかない．

第三に，暗号化による通信トラフィック保護である．攻撃者が，トラフィックがオニオンルーティングネットワークを出るポイントを盗聴しようとする場合にもユーザーの通信内容は暗号化されているので盗聴することは難しい．

1-3. クラウズ（Crowds）

クラウズシステム[註30]は，ウェブを使用したネットワークユーザーの匿名性保護のために AT&T Labs[註31]で開発されたシステムである．

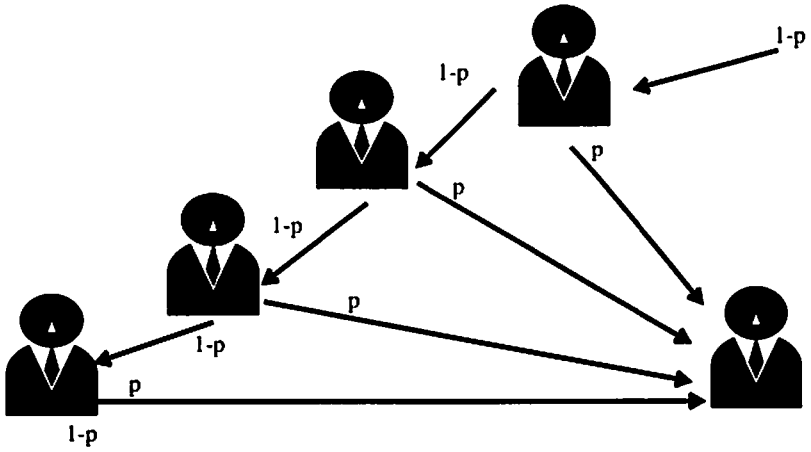
数多くの大衆の中でユーザーの存在を隠す（blending into a crowd）という意味で命名されたクラウズは，ユーザーを一つの大きくて多様なグループとして作動するようになる．そして，クラウズはメンバーを代表し，メンバーが通信を行う際に必要なサーバー接続やデータの伝達のようなものを要請する．したがって，ウェブサーバーの立場から見るとメンバーの中のどのユーザーがサービスを要請したか分からなくなる仕組みである．そして，最後にサービスを要請したユーザーが最初にサービスを要請したユーザーであるか否かについても分からない．また，クラウズは暗号を使用するので送信者の匿名性を提供することができる．

クラウズの仕組み[註32]としては，送信者はクラウズメンバーとして加入し，メンバーリストを入手する．そして，データ送信の際に，送信先を記述したデータをクラウズの他のメンバーに送る．データを受け取ったメンバーは，確率 p でデータを送信先に送り，確

[註30] Reiter, M.K. & A.D.Rubin（1999）, pp.32-38.
[註31] http://www.corp.att.com/attlabs/
[註32] 古原和邦他「プライバシー保護」8 頁.

率 1-p で他のメンバーに送る．このような仕組み（図表 9）により，送信先アドレスは，他のメンバーには秘密にできないが，送信者を隠すことはできる．

＜図表 9＞ Crowds の仕組み



資料：古原和邦他「プライバシー保護」7 頁．

2．ネットワーク基盤の個人情報保護技術[注33]

2-1．プロキシ（Proxy）技術

プロキシ[注34]とは代理行為という意味であり，ネットワーク技術ではプロトコルにおいて代理応答などの概念として用いられている．また，セキュリティ分野では主にセキュリティ上の理由で直接通信できない 2 ポイントにおいて通信する場合，その間で中継器として代理通信を遂行する機能をプロキシという．そして，このような中継機能をするものをプロキシサーバーという．

一般的にプロキシの具現はサーバーで最も多く行われるので，プロキシサーバーを中心にプロキシ技術について簡略に述べることにする．

1）プロキシサーバー（Proxy server）

プロキシサーバーは幅広い認証機能を持っているので，一般的に使用されている普通のサーバーよりは安全である．プロキシの認証機能はユーザーにホストコンピュータへのアクセスを許可しないので，ネットワーク通信内容を観察し，攻撃しようとする人に攻撃を難しくする要因になりうる．

2）プロキシサーバーの特徴

プロキシサーバーの大きな特徴[注35]としては，次のようなものが挙げられる．まず第一に，プロキシ機能である．プロキシサーバーはイントラネットとインターネットの間にあるホ

[注33] Im, J.I. (2004), ibid, NCA, pp.112-123.

[注34] Wayner, Peter, *Builing Security and Protecting Privacy in e-Government*（電子政府・電子自治体におけるセキュリティの構築とプライバシー保護）.

[注35] 財団法人千葉県産業振興センターのおもしろインターネット活用講座のウェブサイト資料による．

スト（ゲートウェイ）に搭載され，アプリケーションレベルゲートウェイ型のファイアウォールとしてイントラネットとインターネット間のホストの通信を中継・代理するためによく使用される．

このプロキシサーバーにだけグローバルIPアドレスを付け，イントラネット内のホストには直接インターネットにアクセスできないIPアドレス（プライベートIPアドレス）を付けておいて，インターネットと接続する場合は必ずプロキシサーバーを経由するようにすれば，インターネット上のサーバから見ると実際にアクセスしたホストは，プロキシサーバーとなるので，イントラネット内のホストが隠蔽できる．また，アプリケーションレベルゲートウェイなので，細かなアクセス制限も設定することができ，セキュリティの確保にもつながる．

このプロキシサーバーはインターネットと接続するためではなく，イントラネット内の部門間に設置することでセキュリティの確保やキャッシュ機能を利用し，ネットワーク負荷の抑制，レスポンスの向上に用いられることもある．

第二に，キャッシュ機能が挙げられる．プロキシサーバーのキャッシュ機能とは一度アクセスしたデータをローカルなキャッシュディスクに貯蔵し，同じデータにアクセスするホストからの要求に対してそのローカルディスク上のデータを返すような機能のことをいう．

この機能によって，重複したデータアクセスがなくなるため，周辺ネットワークの負荷が軽減されるようになる．キャッシュ上のデータをホストが要求した場合，プロキシサーバーがそのデータを返すために，レスポンスが向上するなどのメリットもある．また，このキャッシュ上のデータはプロキシサーバーの設定によって，ある期間で削除することが可能である．

2-2. ファイアウォール（Firewall，防火壁）

ファイアウォール[註36]とは，初期のインターネットが研究目的に開発され，開放的なアクセスの可能になるようにシステムとして構築され，セキュリティ側面で脆弱な特徴[註37]を持っているので，内部のネットワークとインターネットのような外部のネットワークの間に進入障壁を構築し，内部から外部に出ることができるが，外部から内部へ自由に入ることができないように構築したハードウェアおよびソフトウェアを包括するコンピュータセキュリティなどシステムのことである．すなわち，ファイアウォールシステムの基本目標はネットワークユーザーに可能な限りの透明性を保障し，リスクを減らそうとする積極

[註36] Firewallとは，2ポイントのネットワークの間のトラフィックを制御するために構成されたシステムのネットワークのことである．Firewallの機能をサポートするために要求される情報保護サービスは次のようである．①ユーザー認証，②アプローチ制御，③トラフィックの暗号化，④トラフィックログ，そして⑤監査追跡機能が挙げられる．

[註37] インターネットは次のようなセキュリティに脆弱な基盤で開発された．第一に，初期のインターネットが研究目的に開発されて開放接近（Open Access）性を追い求めたシステムであること．第二に，多様なユーザーがアクセスし既存の脆弱なセキュリティをもっと深化させたこと．第三に，インターネットはセキュリティに脆弱なTCP/IP Service基盤を持っていること．第四に，Spying，Spoofingの容易な構造を持っていること．そして第五に，初期のインターネットはセキュリティ政策の欠如（lack of policy）と複雑な構成を持っていたことなどによりセキュリティに脆弱であるといわれている．

的なセキュリティ対策を提供することである．

ファイアウォールシステムのメリットとしては，第一に，ネットワークに対するセキュリティを強化し，基本的に安全ではないサービスをフィルタリングすることでホストサーバーの危険を減少させることである．第二に，ホストシステムに対するアクセスを制御できる点である．第三に，設置したいホストサーバーだけに設置でき，経済的であるといえる．

ファイアウォールの技術[註38]には，大きく次の二つに分けることができる．

1) パケットフィルタリング（Packet filtering）

パケットフィルタリングでは，インターネットと組織内部ネットワークを接続するルータなどによって，通過することのできるIPパケット[註39]を限定する機能である．これを用いればFTP[註40]やTELNET[註41]などについて組織内部からインターネットへのアクセスは許可しても，インターネットから組織内へのアクセスは禁止するなどの設定が可能となる．また，インターネットにアクセスすることのできる組織内部端末を限定することも可能となる．

パケット検索の基準は用いるソフトウェアにより異なるが，一般的にソースIPアドレス，到着IPアドレス，ソースポートナンバー，到着ポートナンバー，そしてパケットの形態によって異なるルールを指定することが可能である．

2) アプリケーションレベルでのゲートウェイ

ゲートウェイを介して組織内部ユーザーがFTP・TELNETなどを行う方法には，大きく分けて次の二つの方法が挙げられる．まず第一に，ゲートウェイにいったんログインしてインターネットにアクセスする方法である．これは，ひとまずゲートウェイにログインしてから再度インターネット上のホストにログインすることで，ゲートウェイ上に組織内部ユーザーのアカウントを作成する必要があり，ユーザーのパスワードを盗まれて侵入される危険性も高くなる．

第二に，ゲートウェイ上に中継プログラムを動かす方法である．これは組織内外のコンピュータ間の通信を行う中継プログラム[註42]をゲートウェイ上で動かすものである．中継プログラムを用いることで，ゲートウェイ上に組織内部のユーザーアカウントを作成する必要がなく，組織内部ユーザーからは直接インターネットに接続しているように見える．

[註38] 財団法人千葉県産業振興センターのおもしろインターネット活用講座のウェブサイト資料による．

[註39] これはコンピュータ通信において，送信先のアドレスなどの制御情報を付加されたデータの小さなまとまりのことである（IT用語辞典e-Wordのウェブサイト資料による）．

[註40] これはインターネットやイントラネットなどのTCP/IPネットワークでファイルを転送するときに使われるプロトコルのことである（IT用語辞典e-Wordのウェブサイト資料による）．

[註41] これはインターネットやイントラネットなどのTCP/IPネットワークにおいて，ネットワークにつながれたコンピュータを遠隔操作するための標準方式のこと，また，そのために使用されるプロトコルのことである（IT用語辞典e-Wordのウェブサイト資料による）．

[註42] 中継プログラムの代表的な例としては，socks，WWWサーバーのプロキシ機能などがある．たとえば，socksはゲートウェイで走らせるサーバープログラムとsocks対応のクライアントアプリケーションから形成され，アプリケーションごとに発信元と送信先のIPアドレスをパラメータとしてアクセス制御を行うことが可能である（財団法人千葉県産業振興センターのおもしろインターネット活用講座のウェブサイト資料による）．

2-3. IDS(Intrusion Detection System：侵入探知システム，不正アクセス監視システム)[註43]

IDS[註44]とは，簡単にいうと不正トラフィックを監視するセキュリティ検知システムのことである．すなわち，IDSとはセキュリティ・エリアやDMZ（Demilitarized Zone：非武装地帯）公開エリアを常時監視し，DoS攻撃[註45],[註46]やポートスキャン・SYNパケット（接続要求）を連続して送信してくるような不正アクセスや攻撃を受けると，TCPセッションを切断したり，ファイアウォールのフィルタリングを変更するなど，自動的に防御するネットワーク侵入検知システムの総称のことである．

IDSの主な機能としては，パケットの中身をIDSに登録してあるシグネチャとマッチングして不正なアクセスを検知することである．そして，不正アクセスと検知した際には，管理者に連絡し，不正なアクセスを遮断することが可能である．

IDSの種類[註47]としては，まず大きく，ホスト監視型IDSとネットワーク監視型IDSの2種類に分類することができる．ホスト監視型はホスト上のOSのログなど特定ファイルのリソースを監視し，変更や改ざんがあった場合に不正行為を検出する機能を持っている．そして，ネットワーク監視型は，ネットワークの1カ所において，ネットワーク上の流れるパケットを監視し，不正なアクセスやアタックを検出する．

最近では「ステルスモード」という機能を搭載したものが多くなっており，これを用いることで，侵入者からIDSを守ることができる．IDS技術は，DoS攻撃に有効であるといえる．また，現在は，ファイアウォール（fire wall）と併用するのが一般的な傾向である．

第二に，シグネチャ方式（不正検知）とアノーマリ方式（異常検知）である[註48]．シグネチャ方式では，過去に発生した不正アクセスのパターンを事前にIDSに登録し，登

[註43] アール カーター 他(シスコシステムズ訳)「Ciscoセキュア IDS実装ガイド－侵入検知システムの実装・保守・運用を学ぶ」ソフトバンククリエイティブ，2003年8月；日吉龍「不正侵入検知[IDS]入門－Snort & Tripwireの基礎と実践」技術評論社，2004年3月などに詳しい．ここでは月刊情報セキュリティのウェブサイト資料による．

[註44] IDSはシステムを保護し，攻撃に対する対応および復旧，統計的分析・報告，消去収集および逆追跡，そして情報流出防止を目的とするシステムである．

[註45] インターネットでのサービス拒否（サービス不能，サービス妨害）攻撃とは，行為者がコンピュータシステムの正常的なサービスを妨害する目的で洪水（flooding）のように大量のデータパケットを送信し，対象ネットワークやシステムの性能を急激に低下させ，攻撃対象システムの提供するサービスを使用できないようにする攻撃のことで，ハッキング手法の中で最も一般的な方法である（成者政・鈴木尚通・田中正敏・葛西和廣「高度情報化社会におけるサイバー犯罪に関する論考－その概念と手法を中心に－」「松本大学研究紀要」第6号，松本大学，2008年1月，73頁）．

[註46] 2009年7月7日，午後6時頃，韓国の青瓦台（大統領官邸），国会議事堂，国防部，朝鮮日報など12の韓国主要機関のウェブサイトにアクセスが急激に増え始まった．韓国全国のコンピュータが1台あたり1秒に数百から数千回にわたり該当サイトにアクセスを行い，このような非正常的なアクセスを行うコンピュータが数千から数万台になると，各サイトは度はずれたトラフィック（traffic）を処理できず，ダウンされてしまった．また，同じ時刻に，米ホワイトハウスや国務部など米国の主なサイトも同じような攻撃を受けて，ダウンされてしまった．このように，悪性コードに感染された数万台のコンピュータが攻撃対象として目を付けたサイトに集中的にアクセスし，該当サイトをダウンさせることをDDoS攻撃という（韓国朝鮮日報のウェブサイト）．

[註47] KumarはIDSを侵入探知技法により，大きく非正常行為探知（anomaly detection）方法と誤用探知（misuse dection）方法に分類している．そして，モニタリング対象により，HIDS（ホスト基盤IDS：host baesd intrusion detection），NIDS（ネットワーク基盤IDS：networking based intrusion detection），そしてこの二つが結合されたHybrid IDSに分類することもできる（Im, J.I. (2004)，*ibid*, NCA, pp.118-122）．

[註48] これはMECHA-SECURITY.COMのウェブサイト資料による．

録したシグネチャ（signature）と同じ通信が発生した際に検知を行うが，少しでも異なる動作であると見つけられないデメリットがある．このような場合には，新しいシグネチャをIDSに追加する必要が生じる．

アノーマリ方式（不規則的な動作の探知）では，事前にIDSに正常な状態の通信の状況を記憶させておき，ネットワークを流れるデータが急に増えたり，通常とは異なるデータが流れた場合に，警告を出すことが可能である．すなわち，まずRFC（Request For Comment）[注49]やTCP/IPの規格のポリシーデータベース（RFCやTCP/IPの規格に準拠した正常なパケットのやりとり）を持ち，これに準拠しないパケットを不正として検出する．しかしそれではアラートが増えすぎるので，Knowledge Base Logging（センサで取得した攻撃情報）とトポロジデータベース（ネットワーク機器や経路情報）による統計的な相関関係によって精査し，アラートを少なくする仕組みである[注50]．この方式は，未知な攻撃にも対処可能であるので，ゼロデイアタック（Zero-day attacks）[注51]も防げることができる．

V．おわりに

本稿では，高度知識情報化社会における個人情報保護に関する考察，主に，個人情報保護の必要性と個人情報の保護に関する法律の概要などをふまえ，個人情報の収集・侵害類型と侵害防止技術などについて検討を行ってきた．個人情報保護については，組織的側面，人的側面，物理的側面，そして技術的側面に分けて，その対策を講じることが可能であるが，本稿では主に技術的な側面からみた対策を述べてきた．

近年，コンピュータネットワークでの個人情報の漏洩などが頻繁に起き，個人と組織は深刻な被害を被っている．このための簡単な対策としては，違法行為が，目的のファイル共有（交換）ソフト[注52]は使用しないことと，コンピュータウイルス[注53]対策を確実に行うことである．これだけの対策によりかなりの被害を事前に防ぐことが可能になる．

また，企業組織においても個人情報保護対策として余計にコストがかかるということで，消極的な対応に留まるケースもあると思われるが，個人情報保護対策を競争戦略，差別化戦略の一つとして位置付け，積極的な姿勢で取り組むべきであろう．このことにより企業活動の成果も一層向上するのであろう．

[注49] これは，インターネットに関する技術の標準を定める団体であるIETFが正式に発行する文書のことである（IT用語辞典e-Wordのウェブサイト資料による）．

[注50] 奥田利枝子「次世代IDSを利用したネットワークの危機管理」株式会社ディアイティ，2002年5月．

[注51] これは，ソフトウェアにセキュリティ上の脆弱性（セキュリティホール）が発見されたときに，開発者側が脆弱性に対する対策（パッチなど）を提供する前に，当該脆弱性を突いた攻撃をしかけるというものである（日立システム情報セキュリティブログによる）．

[注52] 代表的なファイル共有ソフトとしては，Napster，Gnutella，Cabos，share，BitTorrent，souleeek，WinMX，そしてWinnyなどが挙げられる．

[注53] 現在，日本で最も普及しているファイル共有ソフトの一つである，Winnyによる流出の多くは，Antinny（一般的にワームに分類されるトロイの木馬型不正プログラム）などのウイルスに感染することで発生しているといわれている．

【参考・引用文献】

[1] 小林麻里稲『IT の進展と個人情報保護』敬文堂，2003 年 9 月．
[2] 岡　伸浩『図解個人情報保護法早わかり』中経出版，2005 年 2 月．
[3] 田淵義朗他『45 分でわかる個人情報保護』日経 BP 社，2005 年 4 月．
[4]『平成 16 年度行政機関個人情報保護法施行状況調査結果報告書』総務省行政管理局，2005 年 6 月．
[5] 岡村久道『個人情報保護法入門』商事法務，2003 年 6 月．
[6]『個人情報ハンドブック－民間部門における電子計算機処理に関わる個人情報保護ガイドライン（解説書）－』，通商産業省機械情報産業局，1998 年 6 月．
[7] 平松毅『個人情報保護条例の理論と運用』『法と政治』第 50 巻第 2 号，関西学院大学，1999 年 6 月，239 ～ 342 頁．
[8] 岡田定『個人情報の安全性をめぐる諸問題』『経営情報研究』Vol.5,No.2，拓南大学，107 ～ 121 頁．
[9] 堀　正『情報社会におけるプライバシーと個人情報保護』『群馬大学社会情報学部研究論集』第 3 巻，群馬大学社会情報学部，1997 年，1 ～ 23 頁．
[10]『平成 17 年度個人情報の保護に関する法律施行状況の概要』内閣府，2006 年 6 月．
[11]『諸外国などにおける個人情報保護制度の運用実態に関する検討委員会・報告書』2007 年 1 月．
[12] 北原宗律『情報社会における企業倫理－個人情報の収集・利用とその保護に関して－』『信学技報』電信情報通信学会，2003 年，25 ～ 30 頁．
[13] 佐々木良一『セキュリティと個人情報保護の関係に関する考察』『信学技報』電信情報通信学会，2003 年，1 ～ 6 頁．
[14] 井戸田博樹『インターネット時代の個人情報保護』『研究紀要』第 1 巻第 1 号（創刊号），大阪成蹊大学現代経営情報学部，2003 年，95 ～ 107 頁．
[15]NTT データ技術開発本部システム科学研究所編『サイバーセキュリティの法と政策』NTT 出版，2004 年 3 月．
[16] 安保克也・下畑法近『ネットワーク時代のテロリズム』三修社，2003 年 2 月．
[17] 藤原宏高『サイバースペースと法規制』日本経済新聞社，1997 年 10 月．
[18] 羽室英太郎『サイバー犯罪・サイバーテロの攻撃手法と対策』立花書房，2007 年 4 月．
[19] 安保克也・下畑法近『ネットワーク時代のテロリズム－しのび寄る脅威との闘い・サイバーセキュリティー』三修社，2003 年 2 月．
[20] 江畑謙介『情報テロ－サイバースペースという戦場－』日経 BP 社，1998 年 5 月．
[21]H&C クラブ『ハッキング防衛マニュアル－ハッキング・手口知る人達の「本当の」ディフェンスガイド－』データハウス，1999 年 7 月．
[22]Abe, M.（1998）, "Universally verifiable mix-net with verfication work independent of the number of MIX servers", in Proceding of EUROCRYPT'98, Lecture Notes in Computer Science, Vol.1403, Springer-Verlag, pp.437-447.
[23]Jang, B.J.（2003）, *Research on Developments in Korea's Personal Information Protection System*, Yonsei Univ., p.36.
[24]OECD（2006）, REPORT ON THE CROSS-BORDER ENFORCEMENT OF PRIVACY LAWS, pp.1-41.
[25]OECD（2001）, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, pp.1-62.
[26]Huizenga, J.（2003）, Handbook of Privacy-Enhancing Technologies.
[27]Reiter, M.K. & A.D.Rubin（1999）, "Crowds:Anonymity for web transactions", ACM Transactions on Information and System Security, Vol.42, No.2, pp.32-38.