〔金沢星稜大学経済学会 公開講演会〕2004 年 11 月 4 日

サイバー犯罪と情報セキュリティ

Cyber Crime and Information Security

慶應義塾大学大学院法務研究科・法学部教授／弁護士　安冨　潔

安冨　ご紹介いただきました，慶應義塾大学の安冨でございます。今日は，金沢星稜大学からお招きをいただきまして，これからお話をさせていただく機会を得たことを，非常に感謝しております。

今，ご紹介いただきましたけれども，私は，大学で刑事訴訟法という講座を担当しております。経済学を勉強しておられる皆さんと，少し，方向が違うかと思いますが，今日は，最近のサイバー世界，コンピュータの世界での，さまざまな不正な行為，あるいは，違法行為というようなことが，しばしば伝えられておりますけれども，そのようなサイバー犯罪について，お話をさせていただきたいと思っております。

先ほどご紹介いただきました稲原先生と，わたしは大学で同窓でございまして，以来，お付き合いをさせていただいていたようなことから，「本学へ来て，話をしてくれ」ということで，「それでは喜んで」というようなことで，はせ参じ駆けつけてきたような次第でございます。

先ほどもご紹介がありましたけれども，私は大学では刑事訴訟法を教えておりますが，別に大きなテーマとして，情報犯罪あるいは情報セキュリティーという問題に関心を持っております。

今から十数年前でありますけれども，法律の分野でまだあまりコンピュータ犯罪などということに関心がない時代に，コンピュータ犯罪と刑事手続きについての論文をまとめて発表したことから，このような問題に関心を持つようになって，そのまま研究を続けているという次第です。

まず，サイバーの世界，あるいはインターネットの世界というのは，グローバルな，世界的，地球的な規模でのネットワークであるということが特徴として挙げられます。そして，だれでも参加できる開かれたオープンなネットワークであるということも，その特徴の一つであります。オープンネットワークというのは，それぞれ，発信者・受信者，双方向からアクセスできるというものです。そして，そこには不特定多数の人が参加することができます。皆さんもインターネットをお使いになっておられると思いますけれども，メールにしろ，インターネットの発受信にしろ，双方向で利用できます。そして，常時性といいましょうか，時間的にもいつでもアクセスできる。さらに，地理的無限定性，グローバルということで，地球の裏側で起こっているような出来事が伝えられます。たとえば，いまアメリカ大統領の選挙が話題となっていますが，昔であれば，新聞など紙媒体でしか伝わってこなかったわけですが，いまや，ブッシュ大統領が再選されたというような情報がネットで同時的に伝わってきます。このようなところに，インターネットの特性があるということであります。

ただ，ここまでは，非常にいいことばかりのように見えるのですが，一つ困ったことがあるのは，発信者がだれであるかということがよく分からない，つまり，匿名性という特徴を持っていることです。インターネットでは，だれがどのような情報を出しているのかということが分かりません。このことは，実は，犯罪や不正行為を引き起こしやすいという問題をかかえています。

インターネットは，オープンネットワークでありますけれども，一方では，情報の共有化という利便性のある環境を作ることができます。今までだと，図書館に行って本を開かなければ手に入らなかった情報がインターネットを開くとすぐに手に入る。そのような利便性をもたらしてくれます。しかし，他方で，情報は，さまざまな形でいろいろなところに分散して存在いたします。情報の分散化は，あるところに弱点がありますと，そこがねらわれて，ほかのところも連鎖的におかしくなってしまうという問題もあるわけです。

インターネットを利用するということは，それぞれ利用者の責任です。インターネットで流される情報というのは，だれが出しているのか，その内容は正しいのかというと，これは分かりません。情報を入手して，それをどう利用して使っていくか。これは，インターネットを使うそれぞれの人，個人個人の責任ということになります。

皆さんも，自分のホームページをお持ちかもしれません。その情報を発信する者としての責任があります。また，情報を受信をする，インターネットを利用する人も，自己防衛をしておく必要があります。

このように，インターネットには，利便性があると同時に，弱点もリスクもあるというわけであります。

その弱点の，最も典型的なものが，いわゆるサイバー犯罪と呼ばれるものであります。1980 年代以降，さまざまな形で，インターネットを利用して，不正な行為が行われるようになったわけですが，時代的に四つぐらいの段階があります。

一番古くは，いわゆるコンピュータ犯罪ととらえた時代があります。1970 年代後半から 80 年代前半ごろになりまして，スタンドアローンのコンピュータ，あるいは，その媒体としてのフロッピーディスク等に記録されている情報をターゲットにして行われた犯罪であります。コンピュータ犯罪については，日本でも，1987 年に刑法で，データを改変する，コンピュータを壊すとかして業務を妨害する，コンピュータを手段として詐欺をする，データを損壊するなどというようなことを犯罪とするとして法律の改正が行われました。

その後は，コンピュータがネットワークで結ばれるということになってまいりまして，ネットワークを利用した不正な行為を犯罪ととらえるようになってまいります。このような時代には，ネットワーク犯罪ととらえられます。

このようなコンピュータやネットワークを悪用した犯罪が頻繁に起こってくるようになりまして，しかもそれが，地球的な規模で起こるといったことから，1997 年に，アメリカのデンバーでサミットが開かれ，このデンバーサミットにおいて，コミュニケが発表されて，「コンピュータ技術及び電気通信技術を悪用した犯罪」をハイテク犯罪と定義するとされました。

以来，「ハイテク犯罪」という言葉が，一般に使われるよう

になってきたわけであります。しかし，今日では，さらに進んでサイバー犯罪という捉え方が一般的となりつつあります。サイバー犯罪という言葉は，ヨーロッパ評議会（Council of Europe）で策定されたサイバー犯罪条約において，情報セキュリティーを守るという観点から，これを「サイバー犯罪」と名づけたところに出て参ります。

このように時代的に，コンピュータ犯罪からネットワーク犯罪，そして，ハイテク犯罪からサイバー犯罪へ，このように移り変わってきているということがいえます。

このサイバー犯罪というのは，どのような特徴があるかというと，一つは，情報セキュリティを保護するということであります。それから二つ目には，コンピュータや通信技術を利用しているということです。その意味では，ハイテク犯罪に情報のセキュリティーを加えているというところに，サイバー犯罪の特徴があるわけであります。

さて，わが国の現状をみてみますと，1998年以降，急増しているのはネットワークを利用した犯罪です。それに対して，コンピュータ犯罪は，むしろ少なくなっております。ネットワークを利用して詐欺をするとか，あるいは，ネットワークを利用してわいせつな像画等を頒布するとか，そのような犯罪が，非常に急激に増えているわけであります。

2000年になりますと，不正アクセス禁止法という法律ができて，まだ多くはありませんが，不正アクセス禁止法違反の行為，つまり不正アクセスも見られます。このような状況が昨今の状況であります。

具体的に申し上げますと，不正アクセス禁止法違反が，2001年に67件，2002年には105件，2003年には145と徐々に増えています。これに対して，コンピュータ犯罪は，2001年に63件，2002年に30件，2003年に5件とあまり多くはありません。その中でも，電子計算機詐欺事件というのが，2001年から2003年にかけてそれぞれ48件，18件，34件ということで，多少多いという程度であります。むしろ，ネットワークを利用した犯罪というのが，非常に急増していますが，特にネットワーク詐欺事件というのが，2001年に485件であったものが2002年に514件，2003年には521件というように増えております。どのような手口があるかは，また後でお話をしたいと思います。

それから，出会い系サイトを利用したような児童買春やネットワークを利用した児童ポルノ事件もあります。そのほか，電子メール等々を使った脅迫事件とか，あるいは名誉棄損事件とかというようなものも見られます。このような状況でございます。

今年の上半期の状況について警察庁の統計が出ておりますので，ご覧いただけるかと思います。それほど，今までの傾向に変化があるわけではありませんけれども，上半期，1月から7月までの間に，1,063件ということで，昨年よりも約12％増加しています。しかも，ネットワーク利用犯罪が，そのうちの92％を占めています。

次に，サイバー犯罪についての相談です。警察庁等に「何かおかしい。ウイルスを仕掛けられたのではないか」，あるいは「変な画像が流れている。取り締まってほしい」。このようなことを相談する件数がこれであります。これも，1999年から見ますと，2003年にはものすごく増えてきているということが分かります。今年の上半期の相談受理状況を見ますと，昨年よりも1万3,969件増えています。その中で特に，いわゆるネットワークを利用した詐欺事件，あるいは悪質商法などについての相談が増えています。これは，いわゆるインターネットオークションなどを利用したときに，オークションに申し込んで，お金も払ったのだけれども，物が届かないというような苦情などの相談などが多いわけです。それから，わいせつなメールが届いたとか，あるいはネットワーク上でひぼう中傷するようなことが書かれているというようなこととか，迷惑メールがどんどん流れてきて困っているというようなことで，相談件数が急増している状況であります。

昨年のサイバー犯罪の検挙件数は1,849件ですけれども，これは，その前年に比べると，15％増加しています。その中の89％がネットワークを利用しているものであります。先ほど申し上げたような，出会い系サイトを利用したような児童買春事件とか，あるいは，青少年保護条例違反とか，あるいは，インターネットオークションを利用する詐欺，あるいは，わいせつ物の頒布など，このようなものが多く占めているわけであります。

不正アクセス禁止法違反の行為，例えば，ＩＤパスワードなどがかけてあるようなパソコンに忍び込むような場合をいうわけですが，そのようなものも増えてきています。

さて，もう少し細かくお話をしたいと思います。コンピュータ犯罪，いわゆるコンピュータ，もしくは電磁的記録を対象とする犯罪は，1987年5月21日に刑法が改正されてできたものでありますけれども，刑法では「電磁的記録」を定義しています。「電磁的記録」と漢字を使わなくても，データとかプログラムとかというように言ったほうが分かりやすいのではないかと思われるかもしれませんけれども，日本の法律は，片仮名文字で表記するのは伝統的ではありません。そこで，このデータとかプログラムなどというようなものをまとめて，「電磁的記録」と定義をするわけであります。法律の条文によりますと，「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ている」，これを電磁的記録というとされています。要するに，データ，プログラム，そのようなものであるということであります。そして，これが電子計算機，コンピュータによって供される。このようなものを「電磁的記録」というわけであります。

そこで，刑法では，具体的にどのような犯罪があるのかといいますと，電磁的公正証書原本不実記録罪（157条），不実記録電磁的公正証書原本供用罪（158条），電磁的記録不正作出・不正電磁的記録録供用罪（161条の2），支払用カード電磁的記録不正作出罪（163条の2），電子計算機損壊等業務妨害罪（234条の2），電子計算機使用詐欺罪（246条の2），公用電磁的記録毀棄罪（258条），私用電磁的記録毀棄罪（259条）があります。電磁的公正証書原本不実記録罪・不実記録電磁的公正証書原本供用罪とか，電磁的記録不正作出・不正電磁的記録録供用罪というのは，要するに，公正証書や文書の偽造と偽造したものの使用です。それから，支払用カード電磁的記録不正作出罪とあるのが，いわゆるクレジットカードを利用したの詐欺などに使われる偽造のクレジットカードを作ることを処罰するものです。それから，電子計算機損壊等業務妨害というのは，コンピュータなどを壊すというものでありますし，電子計算機使用詐欺罪はコンピュータを使ってお金をだまし取るというような行為，電磁的記録毀棄罪は，電磁的記録媒体，つまりフロッピーディスクなどを壊すというようなものです。このようなものが，刑法でコンピュータ犯罪とされております。

それから，ネットワーク犯罪ということを申し上げましたけれども，これは，犯罪の手段にネットワークを利用していると

いうものであります。典型的なものが，オークション詐欺でして，他人の名義をかたって，偽の電子メールで注文をして，品物を受け取りながら代金を支払わない。つまり，他人に成り済まして物をだまし取るというものです。それと，虚偽の品物をホームページなどに出品して，落札者から入金をさせておいて逃げてしまう。お金をだまし取ってしまうというものがあります。犯罪の数では後者のほうが多いようです。例えば，「パソコン売ります」というようなことを，ホームページに出すわけですね。あるいは，メールで送りつけるわけです。そして，このパソコンですが，非常に安い。それで，どこどこにお金を振り込んでください，というようなことを出すわけですね。そして，購入者はお金を振り込んで，もう送られて来るかなと思って楽しみにしていたら，ちっとも送ってこない。これはおかしいなと思って，もう一度ホームページを見にいくと，そのホームページはリンクデッドになっていて，見事に消え去って，どこに行ってしまったか分からない。この段階になって初めて「あっ，だまされた」と思っても，もう後の祭りというわけです。そのような被害経験に遭われた方はいらっしゃらないことを望みますけれども，しかし，そのようなケースがしばしばあるのです。これもネットワークのオークションを使った詐欺事件の典型的なパターンなのですけれども，まず，犯人が銀行へ行きまして架空の口座を開設いたします。そして，ネットオークションに品物を出品します。これをみた被害者は，「いいものがあるから，買ってみたい」ということで申し込みをします。申し込みをいたしまして，「じゃあ，ＯＫだよ」という返事が，犯人から来ます。そこで，被害者は指定された口座へお金を振り込みます。被害者は「いつ来るかな，いつ来るかな」と思って楽しみにして待っていると，全然品物が送られてこない。「おかしいな」と思ってしらべてもホームページは閉鎖されていて，犯人は，その架空口座から現金を引き落として，どこかへ逃げてしまうというものです。これらはいずれも刑法上の詐欺罪が成立します。

そのほか，インターネットを利用した典型的なものとして，マルチ商法などもありますし，いわゆる「ねずみ講」というものもあります。ねずみ講というのは，一番上の人が仲間の人に，「幾ら幾らで，講をやりましょう」ともちかけ，一人の親が，二人の子を誘ってくる。そうすると，その二人の子が，またさらに何人かの子を誘ってくる。どんどんどんどん参加する人が増えてくる。増えるたびに，お金が上へ上へと上がっていくわけです。上へ上へと上がっていくというのは，一番上の人はみんなからもらえるわけですけれども，下の人は払うばかりになるわけでして，下になる会員の人は，さらに子をたくさん見つけてこないと，出資したお金が戻ってこないということになります。結局，一番末端の人は，出資はすれどお金は戻ってこないという被害を受けるのです。このようなのが，典型的なねずみ講であります。インターネットを利用してねずみ講を運用するのは犯罪ですけれども，いまだなお，被害が続いています。このインターネットを利用したねずみ講は，無限連鎖講の防止に関する法律違反となります。

そのほか，マルチ商法，すなわち特定商取引に関する法律違反，例えばエステとか，あるいは英会話の教材とか，そのような販売がインターネットを通じて行われる場合があります。この場合には，連鎖販売取引や広告規制があります。

それから，信用棄損や業務妨害は，うその情報を流して，ある企業の経済的な信用を低下させるような行為をいうという場合であります。これも刑法上の信用毀損罪という犯罪となります。

そのほか，根拠のない株価情報を流して，株価操作をするような場合とか，あるいは，高利回り元本保証をうたっての実質的な損傷補てんと認められるようなことをするようなことがあります。「絶対損はさせません」。絶対損はさせませんというような，もうけ話が世の中にあるはずがないのでありますけれども，口車に乗せられて，お金を株など，あるいは，一定の商品に投下するようなことがあったりするわけであります。これも証券取引法違反の犯罪であります。

また，インターネットを利用してのひぼう中傷というものもあります。元々は，被害に遭った人と，それから，犯人との間で，何かトラブルがあり，犯人は，そのことについて，何でもいいのですけれども，被害者に対する悪口をネット上に書き込む。そうしますと，それを関係ない一般の人が見て，被害者に対してメールを送ったり，場合によっては，ストーカー的な行為が行われるということになります。もとはといえば，そのような意味では，ネットにひぼう中傷を書き込んだ人間と，被害者との間でのトラブルから起こるわけでありますけれども，間接的な嫌がらせをして，自己満足を図るというようなことがあったりもいたします。

警視庁のホームページに載っていたものでありますけれども，例えば，「自分は恋人募集中です」，「メールください。名前は何とかです」，「東京に住むＯＬです。引っ越したばかりで，寂しく，金に困っています。氏名○○，住所どこどこ，携帯番号何番」というようなことを書き込まれますと，それを見て，犯人が，その携帯電話に電話をするようなことが起こったり，あるいは，「私は 21 歳の大学生です。彼氏と別れてもはや 1 年。そろそろ別の男性と付き合いたいです。連絡待っています」というようなことで，住所とか電話番号を載せる。このようなことが載ることによって，ストーカーの被害に遭ったり，あるいは，迷惑な電話がかかったりする。このようなことで，本当はこの人が別に載せているわけでなくて，何か嫌がらせで，困らせてやろうということで，このようなメールやら，ホームページに掲載されたりするということがあるわけであります。

このようなひぼう中傷による行為は，多くの人に社会的な評価を低下させるような事実を示すということでありまして，それは，本当かどうかは関係ないわけであります。他人の名誉を棄損するというようなことになれば，これは，名誉棄損罪ということになります。

それから，そのほかにも，著作権者の承諾なく著作物を複製したり，あるいは，ホームページに載せたりして，公衆送信するということで，著作権を侵害するような行為，これも著作権法違反の犯罪であります。

そのほか，サイバースクワッテングというのですが，ドメイン名をまず先行取得して，後で登録しようと思った人が登録を申請すると，そのドメイン名はすでに登録されているということで登録ができない。そこで，先行登録しておいた者が，「じゃあ，譲ってやるから，幾ら幾らよこせ」というような一種の恐喝のようなことをしたり，あるいは，不正競争防止法に違反するような行為をしたりするということもあります。これも刑法の恐喝罪や商標法違反，不正競争防止法違反となります。

いずれにせよ，わが国のこれまでの法律ですと，いわゆる情報そのもの，情報自体を保護するという発想ではありません。日本の法律の考え方というのは，情報それ自体を守るというのではなく，その情報が記録されている媒体，フロッピーディスク等あるいはコンピュータを対象として保護するとするわけです。ですから，いわゆる情報窃盗というのは，わが国では犯罪

ではありません。

すなわち，パソコンを持っていったら，それは窃盗罪です。しかし，そのパソコンの中に入っているデータを，例えば，自分でフロッピーディスクを持っていって中にあるデータをフロッピーディスクに写して，そのフロッピーディスクを持ち去るとします。この場合，自分のフロッピーディスクでありますから，情報だけを持ち出しているわけで，これは犯罪とはなりません。パソコンごと持っていったら，犯罪ですが，自分で持って行った電磁的記録媒体に情報を写して持ち去っても犯罪にはならないのです。今，それはおかしいではないかというようなことで，経済産業省で，法律を改正するべきだというような指摘がされていますが，まだ具体的な立法への動きはありません。

わが国では，刑事罰で情報を保護するということについて，コンセンサスが得られていません。現行の刑法は，明治時代にできた法律です。そのころに，情報を守ろうなどという発想は，現実的ではなかったわけですね。

その意味では，いわゆる処罰の間げきといいますか，罰せられないでしまっているという部分があります。そこは時代にあわせて埋めなければいけないと思います。そこで，不正アクセス禁止法とか，あるいは，このサイバー犯罪条約というようなものができあがって，今，新たな法律を作ろうというような動きが見られるわけであります。

さて，不正アクセス禁止法ですが，これは平成12年に新しくできた法律であります。ネットワークを利用した不正な行為を，どのように取り締まるかというときに，従前の刑法では，コンピュータだけをターゲットにしていたことから，不正なアクセスは取り締まることができなかったので，これを取り締まろうということでできた法律であります。

この法律は，高度情報通信社会の健全な発展を守る，ハイテク犯罪を防止することで電気通信秩序を維持するということを目的としています。法律の内容は，不正アクセス行為を禁止し，処罰する，アクセス管理者による防御装置等を設けるというものです。この法律の特徴は，アクセス制御機能，つまり，ＩＤパスワード，指紋だとか，いろいろなやり方がありますけれども，アクセス制御機能が設けられている電気通信回線に接続されたコンピュータを不正に利用されないように守ろうというようなことを念頭においた法律であります。

不正アクセス禁止法で対象とされるコンピュータは，電気通信回線に接続されているものに限られます。つまり，ネットワークにつながっていないといけないということであります。それからもう一つ，アクセス制御機能，これはあまりなじみのない言葉かもしれませんけれども，ＩＤとかパスワードとか，そのようなものでアクセス制御がかかっていなければならないということです。

皆さんがお使いのコンピュータ，いろいろパソコンなどお持ちだと思いますけれども，それが，立ち上げたときにＩＤ・パスワードなどを入れないと，開けないというようになっていて，しかもそれが，ネットワークにつながっているれば，不正アクセス禁止法の対象となるコンピュータということになります。しかし，立ち上げるときにＩＤ・パスワードなどで制御がかかっていないと，不正アクセス禁止法の対象になりません。また，スタンドアローンで使われているようなコンピュータは，不正アクセス禁止法の対象にならないのであります。

そのような不正アクセス禁止法の対象となるコンピュータについて，他人のＩＤ・パスワードを盗んで使うとか，いわゆるセキュリティーホールを攻撃して侵入するとか，そのような行為を処罰するというのが，不正アクセス禁止法です。もっとも，1年以下の懲役，50万円以下の罰金ということで，刑罰はそんなに重くはありません。

それだけではなく，他人の使うＩＤパスワードを入手してきて，売りつけたり，あるいは提供したりして，不正アクセスを助長するような行為も処罰をするということになっています。

不正アクセス行為には，具体的に申し上げますと，他人のＩＤパスワードを無断で使って，他人に成り済まして，インターネット・サービス・プロバイダーにアクセスして課金を免れるというような行為があります。それから，他人の携帯電話に着信した通話を，自己の携帯電話に転送するように設定した例とか，あるいは，他人の開設したホームページを管理するプロバイダーのサーバーに不正にアクセスして，ホームページの改ざんを繰り返したり，このようなことが，例として挙げられます。ほかにも，他人のＩＤパスワードを入力して，プロバイダーに接続して，そのＩＤパスワードを公開して，インターネットを利用して，契約内容を変更するような情報を入手するとかいう例もあります。

もちろんＩＤ・パスワードでアクセス制御をした管理者が，アクセスしてもかまいませんが，管理者の了解を得てやるというアクセスも犯罪の対象にはなりません。

被害を受けた人からの届け出でありますけれども，プロバイダーからの被害の届け出というのが，大体半分ぐらいありますね。それ以外では一般企業が多いですが，大学はほとんどないですね。しかし，これは，別に被害が少なかったということではないと思います。むしろ，セキュリティーのレベルが高くないからではないかと思っています。プロバイダーとか一般の企業は，セキュリティーが破られるということは，社会的信用を下げることになります。しかし，大学は，風土としてセキュリティ意識が高くないことと，セキュリティへの投資にあまり関心がないという状況があるように感じます。むしろ，大学が踏み台になっているというケースはたくさんあります。しかし，なかなかそれが気がつかないという状況ではないでしょうか。本学においても，情報センターがとある思いますけれども，ひょっとしたら，踏み台になっているかもしれません。セキュリティーレベルが高くなければ，それが破られたことに気がつかないという，そのようなことになるわけであります。その意味では，セキュリティーというのは，投資すればするほど，そのレベルは高くなりますけれども，そこら辺のバランスの問題というのもあるところが，難しいところであります。

このように，サイバー犯罪に対処する法律も徐々に整備されてきつつあるのでありますけれども，先ほど申し上げたように，まだまだ法の間げきが見られます。この国会で，「犯罪の国際化及び組織化並びに情報処理の高度化に対処するための刑法等の一部を改正する法律案」が提案されています。この法律が通ることが期待されているわけでございますけれども，なかなか思うように進行していないのであります。

今のが，いわゆるサイバー犯罪の状況ですが，そのほかにもインターネットを利用した不正な行為というものがあります。

犯罪ではなくても，さまざまな不正行為が起っているのですが，その原因を考えるにあたって，デジタル情報というものの持つ特徴から考えてみる必要があります。

デジタル情報というのは，これは全く同じ品質のものがコピーできます。皆さんもご存じのとおり，フロッピーディスクならフロッピーディスクを入れて，ガチャッとやれば，全く同じものができあがるわけです。例えば，紙に書いたり，皆さんが

一生懸命メモを取ったりされますけれども，ここから写しても，内容は同じかもしれませんが，しかし，筆跡・字体，このようなものは，全く違うのが通常ですよね。ところが，デジタル情報というのは，デジタル的に処理されますので，同じものができるという，そのような特徴があります。

それから，短い時間にたくさんの複製を作ることができます。それから，情報を加工したりすることが非常に簡単です。のりとはさみで切って張ってというようなことなく，ガチャッと入れて，ちょこちょこっとキーボードを押せば，直ちに，情報が加工されて出てきます。

それから，異なる種類の情報，例えば音とか映像とか，そのようなものが1枚のものに収録されます。例えば，ＤＶＤでも，ＣＤ－ＲＯＭでも何でも構いませんけれども，そこに入っているものは文字情報であったり，画像情報であったり，音情報であったり，そのようなものが一つの電磁記録媒体に記録されます。

ところが，紙に書いた文字は，紙に書き写すことで写しができます。写真は，ネガフィルムから印画紙に現像されるというような形でしか記録されません。音は音で，録音テープというものでしか録音できなかった。そのような意味で，文字だとか，画像だとか，音声，このようなものはそれぞれ，それぞれによって，媒体ごとに違った形式で記録・保存されますけれども，デジタル情報については，それがすべて一つの媒体にデジタル信号で記録できるというところに，特徴があります。

さて，いろいろな有害な情報というものがインターネットを流れているということは，先ほど申し上げたとおりであります。

この中で，企業の経済活動との関係で問題になることについて，お話をしたいと思います。聞かれたことがあるかどうか分かりませんけれども，ネット告発という問題があります。インターネット上で，ある特定の企業，あるいは，特定の個人に対して，「おかしなことをやっている」というようにして，告発をする。そのようなものをいいます。

典型的な例に，皆さん，あるいはご存じかもしれません。東芝事件というのがあります。東芝事件というのは，東芝のビデオデッキを買った人，Ａさんとしましょう。このＡさんが，2台のビデオデッキを購入いたしました。ところが，どうもちょっと具合が悪いというので，そのビデオデッキについて，相談センターにクレームを申し出たのです。ところが，対応した社員が不親切だということで，その対応のやり取りを，あるプロバイダーの掲示板に投稿したわけであります。ところがそれに対して，東芝が対応したのですけれども，その対応の仕方がまた，あまりうまくなくて，ますますＡさんを怒らせてしまいました。そこで，東芝側は掲示板への書き込みを禁止する措置を取るように求めたわけであります。Ａさんは腹に据えかねて，「じゃあ」というので，自分でホームページを立ち上げて，そこに，東芝とのやり取りの経過を載せたのです。たしかに東芝の対応のまずさを感じる内容のものです。そこで，東芝は「謝罪する」ということを条件に，ホームページの掲載を辞めるように求めて仮処分を申し立てました。その結果，東芝がＡさんに対して謝罪して収まったのですが，ホームページに載っている情報というのは，いろいろ複製されまして，今でもまだ，捜していけば出てきます。

そのようなネット告発というのは，例えば，商品だとか，サービス，接客態度というようなものについてクレームをするというものであります。あるいは，企業の体質，営業方針に対する不満を述べる。あるいは企業に対するひぼう中傷，あるいは，現在の裁判や交渉の経過などを発表するものもあります。最近では，内部告発もあります。内部者告発は，内部者通報制度という法制度の中でやっていくべきであって，ネット等を使ってやっていいということでは，決してありません。

このようなネット告発。これは，先ほどお話ししましたように，インターネットの特徴が顕著に現れるわけでありまして，瞬時にして，全世界規模で情報が伝わってしまいます。つまり，迅速に広い範囲でその影響をもたらすことになります。

それから，何よりもまず，匿名での告発であるということは，他人になりすましてやっているということがあるかもしれません。そのような匿名での告発というものは，だれがやっているのか分からない。それから，顔が見えないものですから，電話で話せないことなど，相手と直接に話せないことを書いてしまう。その事柄の真偽の判断ができないという難しさがあります。「2ちゃんねる」などを見ていただいても，いろいろなことが書いてあります。本当かなと思えるようなことが，まことしやかに流れているというのは危険なことであります。

このようなネット告発がされますと，企業にとってみますと，大きなリスクを背負うことになります。何よりも一番重要なことは，初期対応の重要性でありまして，最初の対応を失敗しますと，先ほどの東芝事件のように，後々まで尾を引いて，クレーム等々に対する対応を録音されて，それがネット上に流れてしまって，取り返しのつかない損害が発生するということにもなりかねません。そのようなネット告発があった際の，危機管理というものを慎重にしておく必要があります。

それから，告発があった場合，その内容も慎重に検討する必要があるわけでありまして，あちらの部署ではこのように言っている，こちらの部署ではこのように言っている。言っていることがまちまちですと，ますます告発者をいらだたせることにもなるわけであります。もし，それが法的な責任ということになるのであれば，これは，法律専門家に相談する必要があります。もちろん，場合によっては，紛争解決の手段としては，やはり，裁判というものを積極的に活用するということが，考えられていいと思います。

ネット告発については，憲法の中では，「表現の自由」というものが保障されているわけですが，何を言ったっていいということではないわけでして，他人の権利を侵害するよなことになっては本来の告発の意義も失われてしまいます。表現に対しては，表現で対抗することになります。つまり，東芝事件でもそうでしたが，真しな態度で，表現には表現で対応するということが必要であろうと思います。

それから，法的措置が必要だということになれば，これは，交渉経過あるいは証拠を集めて，法律の専門家に相談をするということが必要だろうと思います。さっき申し上げたように，だれがやっているのかがよく分からないというのが，非常に難しい問題であります。ホームページ・Ｅメールなどの告発者を特定するという方法です。メールサーバーの場合には，送受信記録が残っておりますし，メッセージヘッダを見れば，どこから経由してきているかということは，すぐ分かります。それから，掲示板などに書き込みさせるなどというような場合には，よくありますけれども，その掲示板にアドレスを表示させるような設定ができますので，そのようにするというようなことが必要であります。

例えば，メッセージヘッダ，このようなものも見ていただければ，どのようにメッセージが流れているかということを見ることができます。

もちろん，実際にだれが告発しているかということまでは判

明しませんが，それが分からなくても，その内容が不正な行為であるということになれば，被疑者不詳で，告発者を訴えるということを警察に相談するということはできます。県警でも，石川県の場合であれば，石川県の警察本部の中にサイバー犯罪対策室という所がありますから，そこに連絡をするということもできますし，また，被疑者不詳での，刑事告訴や刑事告発をすることもできます。

その際に重要なことは，まず，証拠を集めるということであります。これはこの場合だけではなく被害を受けたときには同じでありますけれども，証拠を集めて，そして専門家に相談をするということが，大事であります。その際，電磁的記録媒体に，ホームページ，あるいはメールをコピーして保存しておくということが重要です。

そのほか，不正な行為として，皆さん，悩まされている方がいらっしゃるかもしれませんが，いわゆるコンピュータウイルスの問題があります。コンピュータウイルスは，第三者のプログラム，あるいは，データベースに対して，意図的に何らかの被害を及ぼすように作られたプログラムというもので，感染機能・潜伏機能・発病機能，この三つのどれかを有するものと，当時の通商産業省，今の経済産業省の「コンピュータウイルス対策基準」に示されています。コンピュータウイルスには，いろいろな種類があるのですけれども，ブート型とか，あるいは，ファイル感染型とか，マクロウイルスとかいうようなものがあります。マクロウイルスはトロイの木馬などでも有名であります。

例えば，W 32/Hybris のようなものがウイルスの一つの例であります。このハイブリスというウイルスにかかると，画面が渦巻き状態になってしまいます。それから，PE_MARBURG というのですけれども，赤い丸にバッテンがついたものがずらっと画面に出てきます。これもファイル感染型のウイルスの一つであります。

そのほか，最近では，Nimuda というようなものとか，それから，Badtrans というようなものとか。さらに最近では，WORM_MYDOOM.M というような，トロイの木馬型のウイルスなのですけれども，このような添付ファイルがついたりしているものもあります。このようなエグゼファイル（.exe）の拡張子を上手にごまかして，テキストファイルのように見せかけているようなものとか，最近，かなり巧妙なものが見られるようになっております。ウイルス対策ソフトもだいぶ出てまいりましたので，その意味では，少し状況が変わってきたかもしれませんが，コンピュータウイルスに適切に対応していただかなくてはいけない状況にあります。

ウイルスにかかりますと，問題になるのは，業務に重大な支障を生ずるということであります。皆さんも，ウイルスにかかったことのある方であれば，ご経験のとおり，ウイルスを駆除して，元通りに立ち直らせるというための間，仕事ができなくなってしまいます。それから，コンピュータウイルスにかかったということになりますと，セキュリティーが不十分だという企業への不信感を招くことにもなります。

いずれにせよ，コンピュータウイルスについては，今のところ，法的な対応が，十分ではありません。ウイルスを製造したり，保管したり，感染させただけでは，犯罪とはなりません。先ほどご紹介しましたサイバー犯罪条約では，ウイルスの製造，販売，使用のための調達，輸入，配布またはその他の方法によって利用可能とすることを規制しています。

これを受けて，今度の国会に法律案として審議されていますので，いずれは法律となると思われますが，今の時点では，ウイルスに感染させたというだけでは，犯罪とはならないのであります。

ネットワーク社会は，非常に危険にさらされていると言っていいのであります。サイバー犯罪，あるいは，それ以外のネットワークを利用した不正な行為，特に外部からの不正なアクセスによる侵入，あるいは，ウイルス感染による被害の増大，内部情報の漏えい，情報資産の私的利用などネットワーク，あるいは情報資産に対する脅威となっているわけであります。

そのような脅威に対して，どのようなリスクがあるのか，これを分析し，対策を立てることが必要になります。どのような情報資産があるのか。それに対してどこが弱いのか，そこにどのような脅威があるのか，そして，どのようなリスクなのかということを考えて，その対策を立てていくということになります。

これがまさにセキュリティー対策ということになるわけであります。セキュリティーという場合，一般には，機密性（Confidentiality）・完全性（Integrity）・可用性（Availability）がセキュリティーの3要素だといわれています。情報は，その人だけが使えるものでなければならない（機密性）し，情報は，いつも最新のものとして使えるものでなければならない（完全性）し，それをいつでも使えるものでなければならない（可用性）というわけです。このような意味で，機密性・完全性・可用性ということがセキュリティの要素とされるわけです。

このような機密性・完全性・可用性を要素とするセキュリティーというものについての保護の取り組みというのが重要であります。このセキュリティーの3要素を軸として，どのような制度を作るか。そして，セキュリティーを守るためにどのような技術を開発するか。このセキュリティーに対して，どのような運営をするか。このセキュリティーを守るために，どのような支援組織を作るか。このような全体をスキルとして考えて，セキュリティーというものへの取り組みが語られなければなりません。その際，最も基本的なセキュリティーに対する考え方があり，それを具体的に動かす基本方針・対策基準・実施手順といういわばピラミッド型の枠の中でセキュリティーの対応，対策というものが必要になってくるわけであります。

セキュリティー・ポリシーは，計画，策定，導入，運用というサイクル，循環機能を持っているものであることが重要です。

今日，電子社会を迎えようとして，わが国の法制度とのかかわりということを，最後にまとめてお話をしてみたいと思います。

ご存じのとおり，わが国は電子立国として，いわゆる e-Japan 計画というものを立てております。そこには，e-Japan 実現計画として，幾つかの法的な整備を図るべきだということがうたわれております。一つは，電子商取引のルール，これを整備すること。二つ目には，個人情報保護法を整備すること。三つ目には，インターネットを利用した，株主総会等々を実現すること。4番目には，コンピュータ利用犯罪への刑事罰の導入。このような柱であります。

今，サイバースペースとの関係では，最も基本となる高度情報通信ネットワーク社会形成基本法という法律があります。電子商取引との関係での電子署名及び認証業務に関する法律など幾つかの法律があります。

しかし，このような法律はすべてＩＴ社会を完全なものとするために作られているともいえません。今の社会は，情報技術の発達は非常に速いですから，それに添うような形の法律を作っていくということが，必要になってくるのだろうと思います。

それには，政府それから事業者，そして消費者。ここでＢ to

BというのはBusiness to Businessだというので２Ｂとかと書いてあります。Business to Consumerというような，事業者と消費者の関係，それぞれに深いかかわりを持っている内容であります。

そこで，重要なことは，ＩＴ社会というのは，匿名社会でありますから，成り済ましがないかどうか，いいかえれば本人かどうかということ，そして，改ざんがないかということ，真正性，そして，後からそれをごまかすこと，事後否認がないかどうかであります。つまり，本人性と真正性，事後否認です。

メッセージについては，暗号技術や電子署名・電子認証によってこれらの本人性と真正性，事後否認の防止が図られます。

また，プロバイダーにとっても，情報流通に関する責任があると思います。違法・有害情報をコントロールする一方で表現の自由・通信の秘密という人々の暮らしの上でのコミュニケーションの基本を守るということが必要です。このような中で，情報仲介者，プロバイダーにとって，違法・有害な情報を削除するとか，あるいは，迅速な被害者救済ということを通して，また，被害の拡大を防止するというようなことが求められています。そして「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律」という法律で，プロバイダーに情報流通により自己の権利を侵害された被害者から発信者情報の開示請求を定めるとともに，プロバイダーの側にも免責を認めるようになっています。

このような法律が整備されつつある中で，ネットワーク社会には，大きな脅威が訪れていると言っていいと思います。このような今日の電子社会において，新たな法整備の必要性が，今，問われているように思います。

そこで，ＩＴ社会が健全に発展するために，どのような観点から，法的な整備がされるべきなのかということであります。

一つは，まず，先ほど申し上げたように，わが国には伝統的に情報を記録する「媒体」を対象として保護する，つまり，コンピュータそれ自体，あるいは，電磁記録媒体としてのＤＶＤ，ＣＤやフロッピーディスクなど，そのような「物」を守ることとされ，端的に情報そのものを保護するという考え方が浸透してません。この点は，情報漏えい，あるいは，個人情報保護という観点から，少し法整備がなされてきたという状況にあります。しかし，より一層「情報」自体を保護するという考え方が展開されるべきだろうと思います。一言でいえば，情報窃盗を処罰するということであります。

二つ目は，先ほどから申し上げているような，情報セキュリティー，機密性や完全性や可用性を確保できるものでなければ，ＩＴ社会というものは，健全に発展していかないだろうということです。すなわち，情報セキュリティーを，一層確保するという手段が，いっそう構築されるべきであります。

そして，最後に，ネットワーク社会というのは，一つの国一つの国ごとの，それぞれの国で構築されるものでは決してありません。ネットワークというのは，地球規模で，全世界を一つのネットでくくるというところに，その特徴があるわけでありますから，さまざまなルールが，国際的な観点から作られていかなければならないということであります。

このように「情報」を保護し，そして，情報セキュリティーを確保し，国際的な協調を図る，というシステムを構築していくことが求められているのだと思います。これが電子社会の特性を考慮した，法的な視点であろうかと考えます。

大体予定したところで，お約束の時間でございますので，以上でお話を終えさせていただきます。どうもご清聴ありがとうございました。

Ｑ　青少年対策なのですけれども，アメリカでは青少年対策として，インターネット，あるいはテレビなどで，専用のＩＣチップなどを組み込んだり，さまざまな対策で，有害環境浄化に対して，保護者の意識がかなり高いのです。一方，日本では，そのような問題にして，親の意思が低いといいますか，野放し状態になっていますけれども，これに対して，今後，日本でこうした青少年対策に対する有害環境浄化を含めて，先生は，どのようなお考え……。

安冨　非常に重要な視点のご指摘だと思います。ご案内のとおり，アメリカでは法律も含めて，それからまた，技術的にもこれに対して対応している状況にあります。

わたしもそのような意味では，アメリカと同様に，青少年の有害情報への対策ということをしていかなくてはいけないと思っています。

それについては，警察などでは青少年保護の観点から検討していますし，大手のプロバイダーやＯＳを提供しているような会社などで，非常に問題意識を持っています。そして，専門家を交えて，どのようにやっていこうか，実はこれからその問題は，スタートして，始めようとしているところであります。

技術的には可能だと思いますし，後は法的な問題だろうというように思っています。もちろん難しいのは，表現の自由であるとか，あるいは，コミュニケーションの自由とか，そのような憲法上保障されている自由権を守りつつ，一方では，しかし，それが野放しであっていいということでは決してありませんから，そのような意味での，青少年への有害情報の遮断とか，そのようなことを法的な視点として考えていくべきだろうと思います。ただ，残念ながら，その問題について，わが国で必ずしも，研究者を含めて，まだ意識は高くなくて，どちらかというと，まだまだこれからの課題という現状にあると思われます。しかし，やっていかなければならない問題であると思っています。

本当に難しい問題なのだろうと思うのですけれども，どちらかというと，日本の場合，今まで，そのようなネット上の問題だけではなくて，本とか雑誌とかにおいて，青少年有害情報の図書などに規制をかけるというのは，出版の自由だとか，表現の自由だとかの問題から，規制できない方向で動いてきていて，法律というよりは，自治体の条例などで規制がなされている状況だといえます。でも，ネットの問題というのは，そのような自治体の条例とかでは，実効性を伴わないわけですから，少なくとも，法律で規制をかけていく必要があると思っています。

Ｑ　インターネットで流されている情報につきまして，著作権法の保護案，著作法上の保護というのは，これは，適用されるのですか？

安冨　もちろん，一定の情報について著作権の保護を受けます。例えば，ホームページで，だれかほかの人のホームページをそのまま載せてしまうとか，そのようなことをやったら，著作権法違反になります。ホームページにも著作権はあります。

今，お話に出たので，ホームページのことにちょっと触れます。例えば，ホームページなどを作った場合に，リンクを張りますね。リンクを張るときに，フレーム・リンクといって，あるリンクのところをクリックしますと，そのままそのホームペ

ージに入れ替わるようになり，出てくるのがフレーム・リンクといいますけれども，これは，その著作権違反になります。といいますのは，どこかリンクを張っていますよという形で，ぽこっと小さい水のような画面が出てくるとか，元のところから違うところにリンクを張って，その違うところが共有されていますよ，という形でリンクを張るならいいのです。ところが，クリックするとそのまま替わってしまうというのは，その元のホームページの著作権を侵害することになりますから，リンクの張り方の書き方として，フレーム・リンクなどを張るときは気をつないといけません。

Q　分からないのですけれども，スパムメールというのは何でしょうか？

安冨　スパムメールというのは，やたらとメールが送られてくるものをいいます。スパムというのは，アメリカの缶詰で，いろいろなミートをギューッと混ぜて，固めたものをいうのです。それと同じように，いろいろなメールが送られてくることを，スパムメールというのです。迷惑な話です。

スパムメールが送られてくるのは，個人情報がどこかから漏れているのですね。どこかにアドレスが分かってしまっているのです。アドレスをロボットで集めて，そして集めた個人情報を企業が買って，そこでどんどんメールを流すのですね。

Q　新聞とかの報道でも，情報の重要性というのは，いろいろいわれていますけれども，実際に企業の人が，仕事の利便性とかを考えてかってにアクセスポイントを設置するとか，そのようなことが実際に起こる。なかなか管理者のいうことを聞いてもらえないという問題があるのですけれども，そのようなマネジメントのことについて，先生は，どのようにお考えなのでしょうか。

安冨　最初に申し上げましたように，情報管理というのは，基本的に自分で情報を管理することだと思うのですね。だから情報の自己管理ができないからといって，何でもかんでも法律で縛るというものでもないと思います。ですから，会社の情報もその企業の人間である以上は，企業の資産として守るといいますか，そのような倫理観が，最後はやはり，問題になってくるのだろうと思います。

何よりも，匿名性のあるネット社会では，相手の顔が見えませんので，どうしても大胆な不正が起こりやすいといえます。やはり最後のところは，倫理と教育といいますか，そこのところが，最終的には非常に重要になってくるのだろうと思います。しかし，必要最小限といいましょうか，ある程度のところは，やはり，法律で縛っておかないと無法地帯になってしまう。

現実の社会でだめなことが，バーチャルな世界，ネットワークの社会でＯＫだということでは決してないので，現実の社会で違法だとされることは，ネットの社会でも違法なのだという，そこのところの最低線を法で縛る必要があるのだろうなと思います。

Q　実は，半年ほど前に，ある大学の先生が開発したソフトがありまして，それが何か，世界で撮った映画会社の映画ソフトをダウンロードしてくるという，そのようなソフトらしいのです。何か事件になって，警察が検挙したとか，私は，先生のお話を聞く範囲内だけですと，これは著作権関連なのだろうと思うのですけれども，概要はどのようなことだったのでしょうか。お話し願えれば……。

安冨　Winny（ウィニー）というソフトのことをお話しになっているのだと思います。それは，ファイルとファイルを自由に交換できるというソフトです。そのファイルを交換するソフトそのものは，必ずしも違法なことではないのです。ただ，例えば音楽なら音楽，映像なら映像，これをそのファイル交換ソフトを使って，自由に交換できることになるわけですね。そうすると，ここに著作権侵害が起こることになります。そのような意味で，このファイル交換ソフトそのものは違法でなくても，それを使って無断でファイルを交換するのは著作権を侵害することになるので，ファイルを作成した人がそうした著作権侵害を知ってファイルを作ったとすれば，著作権侵害行為を助けるということになってしまうということで，Winnyの作者を警察は検挙したのですね。

Winnyの作者に対する裁判の問題が出てきていますけれども，ソフトそのものに対して規制しようとかということでは全くないのであって，そのソフトを使うことによって，著作権が侵害されてしまうのを助けるようなことになったので，その点で著作権侵害の幇助となるかが争われています。結果的に，有罪になるか，無罪になるかはまだ分かりません。