平成２８年度　第２回企業向け人権啓発講座
日　時：平成２８年６月２８日（火）１４：００～１６：００
場　所：京都私学会館
テーマ：インターネット社会と人権
　　～企業に求められる情報管理の徹底とリスク回避について
講　師：山崎　文明　氏（公立大学法人会津大学　特任教授）

【はじめに】
○講師
　ほとんどの方は，私を初めて御覧になったと思いますが，先週の火曜日に『クローズアップ現代プラス』に生出演しました。見たという方はいらっしゃいますか。
　ATM から一瞬にして１８億円がなくなったという事件の解説を『クローズアップ現代』でやりました。それのコメンテーターという形で生出演させてもらいました。
　私のプロフィールは最後のページに付けさせていただいております。コンピュータの情報セキュリティを４０年くらい専門にやっていまして，恐らく日本で一番古いセキュリティの専門家という風に思っていただいてもいいのかなと思います。

【講演】
○講師
　それでは本題に入ります。「インターネット社会と人権」という難しい話です。
　毎年，日本は豊かになっている。文明，文化も発達しているという中で，果たして人権侵害というものが，まだそんなに存在するのだろうか。悲しい現実ではありますけれども，どんなに社会が豊かになろうと，やはりあるのだということです。
　減少傾向にあるということであれば理解できますが，残念ながらインターネット関連の人権侵害というのは，確実に毎年増えています。これだけ発達した世の中において，人権侵害が増えているという悲しい現実がございます。
　皆さんお気付きだと思うのですけれども，いわゆるプライバシーの侵害，名誉毀損，誹謗，中傷の類い，こういったものが増えている。
　その背景としては，匿名性が高いということです。誰が書き込んで，誰が誹謗中傷しようが，その攻撃している張本人はどこの誰か分からないというところが，こういった人間のある意味で本性をさらすような現象につながっているということです。
　どんな人権侵害，プライバシー侵害が行われているかということで，一つ具体的な事例，現実を振り返ってみたいと思います。
　これは２０１１年にあったあるホテルでのソーシャルメディア書込み事件。御記憶にあるでしょうか。そのホテル中にある飲食店で働いていたアルバイトの大学生がウエイトレスとして働いていました。
　２２時頃にプロサッカー選手（J リーガー）がお客さまとして来るわけです。

非常にきれいなモデルさんを同伴していました。有名人を間近に見ると，我々もやはり舞い上がるところはあると思うのですけれど，大学生ですから，間近で二枚目のプロサッカー選手を見て，この喜びを誰かと共有したいと思い，ソーシャルメディアに「今夜は２人で泊まるらしい。」ということを，書き込んでしまいました。アルバイト時間中にもかかわらず，ツイッターというソーシャルメディア，これに書込みをしてしまうわけです。

皆さん，もうお分かりだと思います。こういう行為をするのは，ホテル業にとってはあるまじきことですよね。ホテルマンはプライバシーを尊んでくれるだろうという期待して，我々はホテルを気兼ねなく利用できているわけです。いつ，誰と，どこで御飯を食べているということを公にされると，色々な意味で差支えが出てくるわけです。

結果的に社会的な批判が高まり，ホテルの支配人はホームページ上に謝罪の意を掲示せざるを得なくなったということです。従業員やアルバイトの教育を一つ間違えると，こういった事件に巻き込まれるという象徴的な話で，他人事ではないということです。

企業としての信用失墜，イメージダウン，ひいてはお客さま離れというものが考えられます。

この事件，もう一つ非常に特徴的なことが起こりました。それはこの３番目に書かせていただいた「投稿者自身に跳ね返る制裁」という問題です。

この第一の被害者は，このカップルですよね。プロサッカー選手とモデルさん。自分たちのプライバシーが公にさらされてしまったということで，第一の被害者。

第二の被害者は間違いなくホテルですね。従業員のしでかしたことで，結果的には企業であるホテル側にばく大な損害がある。

そして，第三の被害者は，実はこの書込みをやったアルバイトの大学生。その学生自身が，実は事件の被害者になってしまったというのが非常に特徴的な事件です。

これはどういうことかと申しますと，２２時５０分にこのアルバイトの大学生は，書込みをするわけですが，夜中の２時４４分ですよ。「この店員ばか。」，さらに「これマジか。」，「守秘義務っていうもんがあるだろう，ふざけた店だな。」ということで，徐々にこのアルバイトの大学生に対する批判が巻き起こっていくわけです。

そしてこの最初に書込みをした大学生，一体どこの誰かということで，犯人探しが行われ，５時間後に完全なプロファイリングを終えるわけです。プロファイリングというのは，その個人に対する様々な情報，色々なサイトで公開されている情報を名寄せして持ってくるわけです。例えば，メールアドレス，携帯電話の番号，あるいはハンドル名ですとか，様々な名寄せに使えるキーがあるわけです。例えば，氏名，生年月日，顔写真，住所，自宅の外観。自宅の外観写真ですよ。それから学歴，趣味，就職希望先等々が全てプロファイリングされて，「こいつだ。」という形で公表されたわけです。

個人情報を取得するため，追跡部隊を編成することで，この犯人探しを手分けしてやるわけです。これは書込みをした人物のこと，追い詰めるような形で本人探しをされているわけです。

これを見ますと，生年月日や住所，どこの高校を出て，予備校がどこで，どの大学の何学部に在籍中か，学籍番号，それから書込みをした人物が働いていた飲食店名。就職希望先まで出ています。また，携帯電話の機種，それから自宅は窓２つの角部屋だということ。実は自宅の写真まで出てくるわけです。これがたった５時間。しかも真夜中に手分けしてやるわけです。

結果的に彼女は世間のさらし者になるわけです。これは皆さんに考えていただきたいのですが，完璧にインターネット上に漏出しているデータを削除するのは難しい世の中ですので，こういった情報は何度削除しても復活してくるわけです。

だとすると，まず彼女はホテル業界に就職できたでしょうか。可能性としては非常に低いですよね。どこにでもいる大学生だった気がするんですよ。

本人は恐らく大後悔していると思います。ものすごく反省していると思いますよ。自分の進路を自分で摘んでしまいましたから。

そういうことを考えると，皆さん，書込みをした大学生に何とか日常を取り戻してあげたいと，思われるんじゃないでしょうか。

ところがこういう形でインターネット上にずっと公開され続けるわけです。たった１回の若い頃の過ちが，繰り返し思い起こされるような形で公開されるわけです。

こういうことができるということは，非常に大きな攻撃手段になり得ます。今お見せしたプロファイリング，正しいかどうかなんて本人以外には分からないんですよ。赤の他人である可能性だって否定できないわけです。

だとすると，例えば，憎いと思う人を世間のさらし者にして，そのことで社会的な生命を断つということができるわけです。

そういう意味で，ものすごく恐ろしいことが簡単にできてしまうと。しかも見ず知らずの人たちが，真夜中に連携を取るというこの時代。こういった恐ろしい現実があるということです。

これが一つの例ではありますが，確実にインターネットを使った人権侵害というのは，こういう形で起こっています。

繰り返しになりますが，そもそもの被害者はカップルです。第２の被害者はホテルです。第３の被害者は，たった一言書込みをした人物です。

では，第４の被害者はというと，実はプロファイルを暴き立てた匿名の人たちなんです。もし，その相手が特定できて，書込みをした人物がプライバシーの侵害を訴えた場合，その人たちもまた犯罪者になり得るということです。結局，関係者全員がこれは不幸になるわけです。誰も幸せな人は出てこないわけです。そういう意味では，本当に悲しい事件だということが言えると思います。

さて，今日は京都という土地柄を考えまして，少し観光について考えてみましょう。今観光に関わる話題といえば，民泊というのが気になりませんか。今まで観光旅行をする際は，正規のホテルとして届出がされているような所に宿泊先を求めていました。例えば，マンションなどを保有していて，いつも何室か空いていると。ここに外国人などの観光客を泊めることができたら，喜ばれるんじゃないかいうことで，民泊という世界があるわけです。

一方で，タクシーも，日頃使っていない車を有効活用しよう，あるいは同じ目的地の人がいるんだったら乗せてあげようということで，Uber（ウーバー）など

というサービスが出てきています。
つまり，空いている部屋を必要とする人に取り次ぐ Airbnb（エアー・ビー・アンド・ビー）という業態ですね。それから，Uber（ウーバー）という見ず知らずの人にタクシー代わりに車を使ってもらうというシステム。京都の観光業に携わっていらっしゃる方には，一つの脅威として認識されているかもしれません。
でも，どうなんでしょう。知らない人の車に乗るんですよ。これは一昔前だったら白タクと言いましたよね。白タクは使ってはいけませんと。
そうでなくても，子供の頃は，親から「知らない人に付いて行ってはいけない。」と言われていました。それを知らない人の車に乗って，知らない人の家に泊まりに行くんですよ。こんなことが現実に起こっているわけです。
これは乗る方も恐ろしいですが，利用する方も怖いですよね。まともな人が乗ってくるのはいいんですが，強盗を乗せてしまったら大変なことになりますし，自宅を開放するといっても，ちゃんとお金を払ってくれるんだろうか，盗難目的で宿泊されると怖いということで，新聞などでは Airbnb（エアー・ビー・アンド・ビー）に関してはテロリストの隠れ家になるのではないかと指摘する人も出てきています。泊める側にもリスクがある，乗せる側にもリスクがあるというのがこの業態です。
ではなぜ，この業態がこの世に登場してきたのかということをお考えになったことはありますか。それはインターネットがあるからでしょう。インターネットで，そういった需要と供給を結び付けている一つのビジネスモデルがある。
それはそうですね。確かにその見方は合っていますし，こういう業態をシェアリング・エコノミーと呼ばれています。実は需要と供給を結び付けるというのは目新しい業態ではありませんが，この業態が，今この時点でこの世に登場してきた背景には，先ほどお見せしたように，個人がプロファイリングできるということがあります。実は，こうした人物を評価できるということが，このビジネスを成り立たせている。
つまり，この車のドライバーは安全運転をしますとか，あるいはこのお客さまは確実にお金を払ってくれて，部屋を汚さない。ごみを勝手に出したりしない。そういう利用者の評価。それから供給者側の評価があるわけです。このホテルはきちんと夕食の世話もしてくれるし，決まった時間に営業しているとか，そういう双方の評価というものがこのビジネスを可能にしているわけです。
そういう意味では，個人をプロファイリングすることができれば，その個人に対する様々なサービス提供ができるということが言われています。
今，アメリカでどういうビジネスモデルがあるかと言いますと，データブローカーという業態があります。データブローカーという言葉を聞かれたことはありますか。個人の情報を収集して，その個人の情報を必要とする人に売るという業態，これをデータブローカーといいます。
世界最大手のデータブローカーは，L 社という会社で，この会社は日本では特許情報の検索システムだとか，判例情報の検索システムで有名な会社です。まさかそういった個人情報を売っているとは，皆さん想像が付かないと思います。この最大の情報ブローカーは幾つかの部門に分かれていまして，その中には個人情報の売買を専門に行う部門もあります。

医療情報なども扱っていますが，医療情報はこのＬ社とは別に，Ａ社という世界最大の患者情報を売る会社が出てきています。今，海外の会社などが日本にもその患者情報を買いに来ているわけです。

今，一番高く売れる患者情報は何だと思いますか。これは認知症の患者情報です。

例えば，患者情報を買ってどうするのか。これは製薬会社に売るわけです。今，世界で一番需要が伸びているのが，認知症薬です。認知症薬の開発に成功すれば，製薬会社はばく大な利益を得ることができるということで，世界中から認知症患者情報を買っているのです。

そういう意味では，我々は何気なく病院に行くわけですけが，その情報自体が売買対象になっているという現実があるわけです。

例えば，火災保険を掛けて，家を何回も燃やす人がいる。その度に保険金を受け取るような人がいるわけです。保険会社からすると迷惑な存在ですよね。そういう人を相手にしていると，保険料率を上げなければいけないということで，正直な一般の消費者まで迷惑を被るわけですから，そういう人の保険を引き受けるのをやめましょうとなっていき，ここで人を区別し始めるわけです。

自動車保険もそうです。当たり屋という世界がありますよね。自分から車に当たりに行っては，ばく大な保険金請求をするという。そういう人たちを保険に入れるわけには行かないわけですから，そこで，常習者をデータベースにすれば，保険会社に需要があるわけです。それで，その人から申込みがあったら，排除するわけです。

一面だけ捉えていると，保険の健全化ということにつながるわけですが，例えば，間違えてそこに登録されたら，二度と保険に入れないという惨めな立場に置かれることになります。

そういう必要性があるから，情報を集める人がいて，その情報を有料で売るという業態が出てきているわけです。

個人情報というのは，火災保険の詐欺をする人，自動車保険の詐欺をする人，様々な情報をカテゴリー別に利用することができますが，究極は個人ですから，この個人がどういう人物かということを特定したくなるわけです。

そういう意味で，例えば，皆さんがお持ちになっている携帯電話の番号，クレジットカードの番号，電子マネーを使った場合の電子マネー番号，社会保険の番号，健康保険証の番号，最近で言うとマイナンバー，そんなものがあれば，例えば，携帯電話の番号とかメールアドレスを名寄せのキーにするわけですね。そして個人をプロファイリングすることができます。プロファイリングをして，そこから必要なデータを抽出するというのが，今の名簿業者のビジネスモデルになっているわけです。

日本の名簿業者はどんどん進化しています。一昔前，学校の卒業生名簿とか，そういうカテゴリー別に印刷物があって，それを閲覧してコピーを取って，１枚幾らというようなビジネスだったわけです。

今は紙で個人情報は扱っていません。全てデータベース化されています。使っている携帯電話番号で名寄せをして，例えば，３０代キャリアウーマンで高額サプリメントを買う人たちといった購買履歴を含めて企業の要望に合わせた情報

を抽出して売るという形になっています。
そのさきがけみたいなものが，この C 社で，ニューヨークの証券取引所に上場しています。つまり，社会的に認知されたビジネスのモデルだということです。こういった業態が，反社会的な行為であれば，株式を公開できないわけですけれども，証券取引所に上場された会社ということは，社会が認めているわけです。
そのデータベースのサイズが，２５０テラとかという途方もないサイズのデータベースを運用しています。
今，日本の名簿業者も，これに非常に近い業態になりつつあります。今，私は関西地区を中心に健康保険証の番号が１４万人ぐらい漏えいしている事件を調査していますが，これも病院が持っている診療歴と健康保険証が結び付いていまして，漏えい元とかは全く分からない。要するに，複数の情報源を一つのキー，健康保険証番号のようなもので名寄せしていますので，元々のデータが何だったか分からなくなっています。
日本も例外でなくなりつつあるのですけれども，この C 社の元社長が，自分たちのこういうビジネスが，なぜ社会に必要とされているのかということを説得するために言い放った一言が，「私はこの会社をサイバー空間上のナニー（nanny）にする。」と言ったんです。サイバー空間上のナニーにする。
ナニーというのは英語でおばちゃんという意味です。つまり，昔は，町の全てを知っている，村の全てを知っているおばちゃんがいたわけです。道行く子を見ては，「あの子はどこそこの長男で，今どこの小学校に行ってる。」とか，「今こちらに歩いてきたのは，あそこの三男の高校生で，こないだ向かいの女の子にふられた。」とか，ありとあらゆる情報をそのおばちゃんは知っているわけです。そんな時代がありましたよね。我々がいたローカルコミュニティという地域がしっかりしていた頃は，そういったつながりがあったわけです。赤の他人といえども，家族のように暮らしていた時代があった。
今，それが崩壊しているわけですね。ナニー（おばちゃん）がいなくなっちゃったわけです。それでこの会社は，社会から見たサイバー空間におけるナニー（おばちゃん）を目指すと言ったのです。
これはどういう意味かというと，思い出してください。Uber（ウーバー）とか Airbnb（エアー・ビー・アンド・ビー）の世界です。「この人は絶対信用できます。」，「この運転手は大丈夫だから，使っていいですよ。」，これは「今，うちのお母さん調子が悪いんだけど，誰か車に乗せてくれないか。」と言ったら，向かいのお兄ちゃんが「今，ちょっと車が空いてるから，連れてってあげる。」というような世界でしょう。それは見ず知らずではなくて，同じ町内のお兄ちゃんだということで，普段からコミュニケーションがあるからできてしまうわけです。
それをサイバー空間上で実現しているのが，Uber（ウーバー）とか Airbnb（エアー・ビー・アンド・ビー）であるということです。つまりそこには匿名性というものはなく，評価，格付けされているわけです。ドライバーの評価，利用者の評価，旅館，民泊，宿泊者としての評価，それが行われているから，こういったビジネスが成り立ちます。
全く見ず知らずの人が泊まるわけではない，全く見ず知らずの人を車に乗せるわけではない，つまり，こういう格付けをやる会社がそういう信用情報を持って

いるから，それぞれの会社が，それぞれのサービス提供者，利用者を格付けしているから成り立つわけです。

そして，それを総合的にやっている会社もあります。つまり，グローバルとか地球規模の経済とか言うけれども，一方で我々が今目にしている世界というのは村化しているわけです。小さな村化している。それがインターネットのパワーだということです。

つまり，社会が村化することが安心・安全をもたらすのだという考え方です。匿名性を排除して，相手を格付けるということです。それが，今，私たちが生きている時代だということです。

一方で，分野別にデータベースがあるというお話をしましたが，これも悲しい現実です。売れ筋のデータというのは時代とともに変わりますが，今，一番需要があるのが万引きをした人のデータです。

そのデータベースを売るわけです。誰が買うのか。スーパーなどの小売業です。

日本でも万引きというのは，年間５千億円近い被害が出ています。これを１日に換算すると十二，三億円の損失が出ているわけです。この中には内引きというのも入っていますけれども，一般のお客さんが商品をくすねる，これは万引き。従業員がくすねるものが内引きです。

実は，悲しいことに，日本でも内引き被害が増えている。つまり，従業員が商品窃盗をやるわけです。もう一つ，皆さん御存じだと思いますが，万引きというのはすごく再犯率が高いです。一度やると，病み付きになる。それからゲートウエイ犯罪といいまして，人が悪事に走る最初のちょっとした悪さ。そういう意味では小学生や中学生，そういった子どもたちには注意を向けていく必要があるのです。ゲートウエイ犯罪，それをきっかけに色々な法律を犯すことで凶悪になってしまう。

再犯率が非常に高いこと。これは全国小売業の調査報告書ですが，５６パーセントぐらいしか警察に届けないのですね。ケースバイケースで判断しますというのが約４割です。

先ほど御紹介したＣ社は，従業員５千人という数字が出ていたかと思うのですが，他にアルバイトが１万人いて，データベースを広げていく。

そうすると，例えば，スーパーマーケットのチェーン店があって，そこで従業員を雇おうとすると照会を掛けたくなりますよね。その人の万引き歴がないかどうか。それを可能にしているわけです。

この背景には，万引きは再犯率が高いので，例えば，過去に万引きをやったことがある人をスーパーのアルバイトで雇うと，今度は内引きをやりますからね。それを防ぐために照会を掛けている。

統計から見ると，ほとんどは警察への届出を辞退するわけです。大事（おおごと）にはしませんからといって辞退するのですが，仮に皆さんが万引きをしたとして，警察に届けられるかデータベースに登録されるか，どちらか選べと言われたらどうしますか。データベースに登録されるのを選びますよね。ということは，本人同意を取れるわけです。個人情報保護に詳しい方は，本人同意が基本だというのはよく御存じだと思いますが，これは本人同意が取れてしまいますからね。本人同意を取った形で，万引きデータベースに記録が残ってしまう。

そういう意味で，今，グローバルな世界が村化しているという話をしたのですが，一方で，村八分の世界が復活する可能性が出ています。

私が，今，一番恐れているのは，アルバイトのあっせんをインターネットでやる業態が出てきていますよね。テレビを見ても，コマーシャルを打つくらいもうかっているわけです。テレビＣＭが打てるくらいですからね。

アルバイトって，僕らの頃は大学の学生課に貼ってあるアルバイトの募集を見て，あるいはハローワークへ行ってみたいなことだったけれども，今はそんなことをする学生は１人もいません。インターネットでバイト募集広告を検索するから。

アルバイトのあっせん会社が人を格付けしたらどうなると思いますか。例えば，あっせん先のスーパーの店長に，「今回派遣したバイトはどうでしたか。」，「いや，よくやってくれるよ。非常に気の利く子だった。」といい評価だったらいいですよね。「あの子は一から十まで説明しないと動かないんだ。」とか書かれてしまうかもしれません。

中には，店長が気に掛けている女性アルバイトに男性アルバイトが色目を使った。これは店長としては腹立たしいわけです。自分よりイケメンのバイトだったりとか。そうすると，バイトあっせん会社から聞いてきたら，悪い評価を言いますよね。その評価を信じて，バイトあっせん会社がその個人の評価ということで記録したらどうなると思いますか。どのバイトを申し込んでも，なぜか理由も分からずにアルバイトに就けない。

これは公開されていないので，私は想像で言っていますが，アルバイトあっせん会社としては，企業がお客さまですよね。そうすると，良いアルバイトを紹介してほしいという企業の期待に応えようとします。そうすると応募してきたバイトの格付けをやらないはずがない。そうすると，自分には全く身に覚えのない世界で，チェック現象が起こるかもしれない。実はそういう問題があります。

アメリカのジャーナリストは，この C 社のビジネスというのはいかがなものかということで，C 社のデータベースに記録されている人たちは，C 社の顧客ではない。登録されている人たちにとって，この信用調査会社を変える方法がない。問題改善につながる経済的圧力を加えることもできない。つまり，C 社を意に沿った形で行動を是正するパワーを誰も持ち得ない。そういう意味で，C 社というのは選択の余地がない会社だということ。

どうですか，皆さん。アメリカって，我々日本に比べたときに，非常に先進的なイメージを持たれていたのが，少し違うなと思いませんか。アメリカにはプライバシー保護というのはないのですね。

ここから先は人権の話ではありますけれども，法律ではないわけです。要するに企業としてのモラルですね。企業としてどこまでやるかということで，どこかで線引きをしていただきたい。これは法律もないわけです。これをやってはいけないという法律はない。

我々一人一人が心掛けなくてはいけないのは，最初は区別なのです。でも，これが実をいうと差別なんです。この区別と差別の境目は，恐らく誰にも分からない。ひたすらその人の人格に依存するわけです。

そういう意味で，利便性だけを追求していくと，実は知らないうちに人を阻害

してしまう，人権侵害を起こしてしまうかもしれないというのが，大きな問題です。御説明しましたように，個人をプロファイリングするということが，直接的な人権侵害につながっていくのだということで，やはり，できるだけ情報漏えいを起こさないということが大事だということです。

人権侵害という側面もが，一方では企業としては経営に大きなダメージがあります。

ある教材販売会社が，顧客の情報を漏えいしましたということで，多額の損失を計上し，株価が下がりましたし，いまだに復活の気配がないということで，会長退任という事態に進んでいるのは御承知のとおりかと思います。

こういった情報漏えい事件は，度々国内で起こっているわけですが，この背景には個人情報の売買市場があるということです。C 社の例で具体的にお話ししましたが，日本も例外ではないということです。

当然そこで売り買いがされていて，データブローカーに近いビジネス形態が出ています。

そういう意味で，個人情報の漏えいというのは，まず背景としては，個人情報そのものが非常に商品化しているということと，一方で漏えいした場合の訴訟リスクというのが年々高くなっている。

個人情報の漏えいに関していえば，損害賠償請求訴訟，プライバシーの侵害を根拠とした損害賠償の訴訟が行われる。

例えば，過去に，顧客情報が漏えいしたエステサロン会社があります。エステサロンの情報ですから，身長とか体重などの自分の身体に関するコンプレックス情報，そういったものが記録されているわけです。

このとき，裁判所はどういう判断をしたかというと，「本件情報は保健医療そのものに該当するものではないが，住所，氏名等の基本的な識別情報のみの場合と比較して，一般人の感受性を基準にしても秘匿されるべき必要性が高いことは否定できない。」ということで，医療機関ほどの機微な情報ではないけれども，それに近い情報だということで慰謝料の支払いを認めるわけです。

皆さん気を付けていただきたいのは，必要以上の属性情報を収集すると漏えいしたときの損害賠償の請求額が限りなく跳ね上がるということです。

ある人材派遣の会社がありますが，ここも過去に漏えい事件を起こしています。このときは容姿の格付けをしていました。この女性は非常に美しいとか，そうでもないとか，そういうのをランク付けしたわけです。これが問題となり，この事案では結局和解するわけですが，和解金額が必要となりました。

そういう意味では，どうしても人材派遣の会社に，例えば受付の人材の派遣を依頼する際に，できるだけかわいい人をと言ってしまいますよね。派遣を行う企業としては，その記録が残っていたりすると，どうしても写真を眺めながら A とか B とかやりたくなってしまうわけです。そこで格付けするということが行われているのですが，そういった情報が一度漏えいすると，非常に高い確率で損害賠償金の支払を求められる情報になる。

もう一つ人権侵害という意味では，こうした漏えいした個人情報が犯罪に利用されたケースが増えているということで，闇金融とか振り込め詐欺，架空請求書詐欺などの詐欺，こういったものは大量の個人情報を集めて成立する犯罪だとい

うことですね。
例えば，架空請求書の送り付け詐欺の一例を御紹介しますと，この犯人グループは，１２万通送付しているわけです。１２万通ですよ。皆さん，架空請求書を受け取ったことはありますか。はがきが１枚来るのですが，見たこともないアダルトサイトから「あなたは閲覧をしている。閲覧料として６万円請求します。」というようなことが書いてある。２日以内に支払わなければ裁判所に訴えると。
裁判沙汰になるんだと思うと，やっぱり驚いてしまう人がいて，払込みをする人がいるんですね。とりあえずは裁判を避けたいから払い込んでおいて，後から何とかしようと。それが後からというのはないんですね。犯人の居所は知れませんので，後からというのはもうないということで，被害者が後を絶たない。
大量に出せば出すほど，ある一定のパーセンテージで振り込む人が出てきますので，大量に出すということがこの犯罪のポイントになるわけです。では一体どれくらいのはがきを投かんしているかというと，１千通，２千通じゃないということですね。この犯人は捕らえてみれば１２万通。１２万通のはがき，ちょっと想像してください。ダンボール箱，幾つくらい。
この１２万人分もの住所氏名をどうやって集めたのか。街頭アンケートをやりましたというのはありえないわけで，当然こういった大量の情報を持っている企業などから漏れているということです。
では，なぜ情報は漏れるのかということで，最後に年金機構の事案を御紹介します。この事件は丁度今から１年前，昨年６月に発覚したわけですが，覚えていらっしゃいますか。新聞等はこぞって，そのパスワード管理を問題にしましたね。職員の方々が操作しているファイルに対してパスワードを掛けなければいけなかった。これを指摘するわけです。
マスコミだけではなく，８月，事件発覚の２箇月後に年金機構が調査委員会報告書というのを出すのですが，こちらでもやはりパスワードの問題を大きく採り上げているわけです。
御説明しておきたいのですが，年金機構の方がメールの添付ファイルを開いて，パソコンが感染します。この感染したパソコンが C&C サーバーという遠隔操作を行うサーバーに接続され，自由にパソコンをリモートで操作できるようになりましたので，この年金情報が外部漏えいしていくわけです。このパソコンがウイルスに感染して遠隔操作状態にあるということは，キーボードのストロークとか，それからディスプレイに表示されている画面は遠隔から見えるわけです。
キーボードのストロークも，例えば，パスワードの表示は＊（アスタリスク）でマスキングしてありますといっても，キーボードをたたいているわけだから，あるプログラムを送り込めばどのキーをたたいたのかというのは転送されるわけです。
ですから，この事案に関しては，年金機構の方がパスワード管理をしっかりしていても防ぎ得なかったわけです。全くの的外れの指摘だということです。
それから，この遠隔操作に使われたサーバー，IP アドレスという番号が振られているコンピュータに接続に行くわけですが，この通信を見つけてネットワークの監視をしていてよかったということになっているわけですが，実際には，御紹介した IP アドレスというのは，セキュリティ専門家であれば何年も前から知っ

ていたIPアドレスなので，見つけられて当然の話なのです。
見つけられて当然のIPアドレスだから見つかったわけで，相手が本気だったら全くセキュリティソフトウエアが認識していないIPアドレスを使ってきますので，本気の攻撃だったらまず見つかっていなかったということです。
それから，内閣サイバーセキュリティセンターとう所でネットワーク監視をしているのですが，ここから各公的機関と伝言ゲームになっていて，情報が伝わるのに時間が掛かっているわけです。
今起こっている遠隔操作を使ったハッキングということは，コンピュータの前に人がスタンバイしているわけです。ばらまいたウイルスを誰かが開いて，その瞬間から遠隔操作を始めるためにスタンバイしている人がいるので，時間も掛かっていたら，時既に遅しです。大体１０分位内に線を抜くということをやらないと，結果的にはもうデータが漏えいした後だということです。
それから，この事件の発端は，添付ファイルを開いてしまったということになるわけですが，そもそもその担当者にどうやってそのメールが飛んで来たのか。どうやって犯人にはその担当者のメールアドレスが分かったのかというのが一番大きなポイントです。
ところが，公式な報告書の中にはメールアドレスの漏えいルートについてはほとんど触れていない。どこから漏れたのかということについては調査していないのですね。
皆さんの会社に変な通信要求が来たときに，攻撃されるのではないかと驚かれると思うのですが，相手の会社に問い合わせる場合がありますね。「お宅の会社から変な通信要求が来ている。」と。
だとすると，相手の会社のネットワーク管理者が誰かが分からないのにメールを出したり電話を掛けたりする必要がありますので，情報を登録しているわけです。それが公開されている。
私は山崎文明ですので，YAMASAKI FUMIAKIというのを例にすると，YAMASAKI-FUMIAKI@○○.JPなんですよ。この１人の人の名前とメールアドレスの組合せが分かれば，もうこっちのものです。職員録が手に入れば，あその職員録にメールアドレスがなくても，当てずっぽうでその人のメールアドレスが作れるでしょう。だから，こういうところから犯人はメールアドレスを想像して作ったかもしれません。
そういう意味では，こういったJPRSに届け出るときのメールアドレスを他の人と違った系列にするとか，あるいは警察庁などもよくやっていますけれどもYAMASAKI-FUMIAKIでもいいのですけれども，その後に００と付けたりとか，APと付けたりとか，１文字，２文字足すだけで，想像して作るということはできません。そういうメールアドレス体系にされれば，フィッシングメールといったものが飛び込んで来る可能性は極端に減ります。
それから，危険なのは「INFO@」何とかというお問合せメール，これはどの会社にも当たりますよね。あのメールアドレスってものすごくリスクが高いでしょう。だって，見ず知らずの人が，何の目的でメールを送ってくるか分からないわけですから，一番危険なメールアドレス。全部ドメインを分けておくということが大事です。同じドメインだったら全滅しますからね。

それから，民間のセミナーに申し込むとき，最近必ずメールアドレスを書かせます。あれは売り買いされている可能性があります。ですから，例えば，山崎先生がセキュリティのセミナーをやる。そういうセミナーに申し込んでいるのは，その会社のセキュリティ担当者だったりする可能性が極めて高いです。そういう人たちのメールアドレスをピンポイントで狙ってフィッシングが行われるという可能性がある。

実は，DMARC（ディーマーク）という仕組みがあります。フィッシングメールというのは，たいていの場合，@マークから後ろを偽装するわけです。皆さんの会社名などです。大きな会社だったら人事部から連絡があったり，人事部が，例えば，「定期健康診断のお知らせ」という形で届きます。メールアドレスを見ると，@マークから後ろが自社のドメインです。安心しますよね。これは社内メールだと思うじゃないですか。それで開いたりすることが多い。たいていの場合は送信者アドレス偽装というのをやっています。

送信者アドレス偽装というのは，簡単にできるということが，技術的に問題なのですが，一方で不審メールは本来の IP ドレスが取られているメールサーバーからは飛んで来ないのです。

だから，今回，ある企業がフィッシングメール被害で感染した事件では，あれはメールの表示上とは全く別の所から飛んで来ているので，IP アドレスとドメイン名を照合すれば，表示されている IP アドレスではないわけだから，１００パーセント見抜けますよね。これは人間の目では見られないのです。だから，もはや注意すればいい時代は過ぎ去っている。完全なコピーメールを使いますので注意しようがない。一昔前だったら，日本語がたどたどしいとか，そういうことで見破れましたが，今はそれはできない。全く本物のメールを使っている。

ただ，技術的には IP アドレスが違うというところで検出できる。その仕組みが SPF というものです。もう一つ，発信者が電子署名を付けておく。会社の署名を付けて送るという方法があります。この２つを併用すると，ほぼ完璧にフィッシングメールはなくせる。

その仕組みを DMARC（ディーマーク）と言います。この事件も取引先各社との DMARC（ディーマーク）対応をすれば事件は起こらなかったのです。ほとんどお金は掛からない。こういうことを知らないで，セキュリティ対策を強化しますと，ばく大な費用が掛かる。

もう一つ申し上げておきたいのは，最近やたらセキュリティの専門家が「攻撃が高度化している。」とか言いますよ。巧妙になっているとか。でも実際に行われていることは昔と全く変わっていない。

年金機構の場合も，ゼロデイ攻撃だったというのが非常に大きな問題なんです。ゼロデイ攻撃というのは，そのソフトウエアの開発元が欠陥を見つけます。この欠陥を使ってハッキングされるわけですが，それに対する修正プログラムというのを必ず開発します。欠陥が見つかってから修正プログラムをメーカーさんが出してくるまでの期間，この間はぜい弱な状態が続いているわけです。この間に攻撃されたら仕方ないということになるのですが，この間の攻撃をゼロデイアタックといいます。

では，日本年金機構の事案はゼロデイアタックだったのかということで，確認

をしておきましょう。今回，一太郎というワープロソフトに感染しているわけです。一太郎というのは，ジャストシステムという会社が開発しているワープロソフトですが，ジャストシステムは２０１４年１１月１３日にぜい弱性がありましたと公表しているわけです。事件発覚の半年前ですよ。事件が発覚したのは去年の６月。これは１４年の１１月。つまり，事件発覚の半年前に，ジャストシステムはぜい弱性が見つかったという発表をしている。

どんなぜい弱性であったか，システム管理者の権限でコンピュータを任意に操作できる可能性があります。正に今回の遠隔操作状態です。

この事実を公表したということは，この時点でジャストシステムは修正プログラムを完成していて，配布を始めてから攻撃しているわけです。

つまり日本年金機構のシステム管理者が自社で使っているジャストシステムの一太郎というソフトウエアに確実に修正プログラムを掛けていれば，あの事件は起こらなかった。だからパスワードの問題じゃないのです。

どうでしょうか，皆さん。セキュリティの話題。二言目にはプログラムを最新状態にしましょうと言われていますよね。つまり，修正プログラムをいつも最新の状態にするということが一番基本であると。

そういう意味では，今回の日本年金機構の事案も例外ではない。一太郎を最新にしておけば，あの事件は起こらなかったのです。

まとめると，個人情報の漏えいというのはものすごく，想像を絶するような人権侵害となる可能性があるのだということです。

基本は，立場を自分に置き換えて，自分がやられたら嫌だなと思うことは人にやらないということです。こんな情報収集をしたらもうかるんじゃないかと。自分がそこで格付けされたらどう思うかです。企業の経営方針とか，企業の品格ということを十分考えて検討していただきたいというのが，私の切なる思いです。区別と差別は紙一重だということですね。

それから，世間のセキュリティコンサルタント，セキュリティベンダーさんは，高度化している，巧妙化しているというけれども，我々利用者からすると，やれることは今までどおり、使わないプログラムは消してしまいましょうとか，使っているプログラムは最新状態にしましょうとか，そういう話です。

それからメールアドレス，問題ということであれば，早速メールアドレスの変更を考えていただきたいと思いますし，できれば日本中の企業が DMARC（ディーマーク）に対応してください。そうすると日本中からフィッシングメール，詐欺メールというのはほとんどなくなります。

それから，ホワイトリストという方法もありますということで，Windows7 以降をお使いの方は Apploker（アップロッカー）というのをマイクロソフトが無料で付けています。これは許可したプログラム以外は動かない仕組みです。

ウイルスと言いますが，パソコンの OS から見ると，ウイルスというのも一つのプログラムでしかありません。そういう意味では許可されていないわけですから，ウイルスであったにせよ，添付ファイルを開いても動かないわけです。こういう無料のソフトが付いてきているわけです。

それから，データを無価値化しましょうということで，冒頭お話ししたＡＴＭの不正操作による引出し事件。あれも南アフリカの銀行から情報が漏れて，その

情報を基に磁気カードを作るわけです。
皆さん考えてみてください。その情報がもし暗号化されていたら，犯人がそれを入手しても磁気カードは作れないわけです。ですから，漏れて困る情報は暗号化しなさいということを最後に申し上げておきたいと思います。
漏えいしないということがもちろん大事ですが，漏えいしても被害者を作らないということ，これも重要な対策だということを真剣に考えていただければと思います。

○司会
山崎先生，ありがとうございました。
続きまして，質疑応答のほうに入らせていただきます。御質問のある方は挙手をお願いいたします。

○質問者１
私は IT 系の仕事をしておりまして，特にセキュリティとかの部分で先生の御意見と，あとプラスアルファで皆さんに伝えてほしいなと思うことがあります。
ある情報漏えい事件に関して，私から言わせれば，最新のシステムを入れたから破られたというのが正解じゃないかと思っているのですが。何が言いたいかというと，様々なシステムを入れたり，最新のものにするという形で対応される所が多いのですけが，実際セキュリティ問題で情報漏えいなどが起こるとき，ヒューマンエラーは避けられない。そういう意味では，セキュリティを高めていても人間に対しての教育が必要なのではないかと思っているのですが，いかがでしょうか。
あと一つ，解説をお願いしたいのは，人権問題に関わるのかどうか分からないのですが，ハッカーと言っていますけれども，ハッカーとクラッカーとの区別を説明していただければと思います。

○講師
まず，最初の質問ですが，私は，実は文部科学省の「２０２０年代に向けた教育の情報化に関する懇談会」という政府委員をやっていまして，１日が私の発表の当番日で，ある学校の情報漏えい事件のお話をする予定です。学校って個人情報の漏えい事件などでは被害者的な目で皆さん御覧になるけれども，私から見ると，彼らが放置しているサーバーが悪用されたという現実があるわけです。
教育現場というのは，一部のサーバーモンキーという言い方をしますけれども，民間企業みたいなシステム管理部がないのですね。あの人は数学を教えているからコンピュータが分かるんじゃないかとか，訳の分からない理由でサーバー管理者に選ばれたりしているわけです。
選ばれた方は，いや，他の先生ができないので自分がやっているだけで，自分だって本業があるという思いでやっているわけです。一生懸命やっているんだとか，好きでやっているんでしょうみたいな話がされているのが教育現場です。挙句の果てに，お金がないからセキュリティなんて二の次だというのが現実なんです。

この情報漏えい事件は，御指摘どおり，最新のシステムでも何でもないんですよ。ただ，インターネットを使ってこんなことができますよということで，例えば，児童，生徒が自発的にテストを受けたり，自分で学習できるようなシステムと，いわゆる成績処理を中心とする校務システムというのがあります。

恐らく，まだ私は事実確認ができていないのですが，ドメインが分割されていないんです。公開メールアドレスのドメインは，リスクが高いから業務ドメインと分けるべきだとお話ししましたよね。学校の場合も，校務システムとドメインを分けるべきなんですが，これをやっていなかったのだと思います。これはセキュリティのイロハのイです。

このような事例，実は前からあることです。教職員が使うパソコンと生徒が使う教育用パソコンが LAN で結ばれていたといって，生徒が進路指導の内容を見に行くわけです。生徒がアクセスできるのは教育システムですよ。先生方がお使いになるのは校務システム。本来ネットワークは別々でなければいけないのに，教育システムから校務システムにアクセスできるんです。

別のある中学校で起こったのですが，校務用のサーバーにアクセスして，校長先生の名前をパスワード入力したら通ってしまった。これでいかにセキュリティがぜい弱かということで，わざわざその情報を印刷して学校に提出するわけです。

これも明らかに，学校だからということで一つのドメインで運用されている。外部から見える。これも外から見えるドメインの中にファイルサーバーを置いているから，こういうことになるわけです。

だから私に言わせると，教育システムとして最新かもしれないが，セキュリティのイロハのイもできていなかったのだと思うのです。

幾つか例をお見せしましたが，初めての例じゃないのです。以前から私が指摘していることがまた起こったという話です。

文部科学省での懇談会でも，私が提案しているのはこういう内容です。パッチを確実に当てるとか，固定パスワードはもう限界だと言われるので，例えば，パスワード生成ツールを使って強制的にそのパスワードを使わせる。

本当に防御側がやれることは決まっていて，目新しい話は余りないのです。そんな話です。

それから，ハッカーとクラッカーの話です。ハッカーというのはコンピュータに対する天才的な技術を持った人です。クラッカーというのは，それを悪用するとそれをクラッカーと言いますというのがあるのですが，私は年に６回，多いときは１３回くらいアメリカに行ってセキュリティのコンサルタントとか政府の関係者と話をします。ここ４０年くらい，その話の中で，クラッカーという単語は一度も聞かないですね。悪いことをする人も，英語でもハッカーと言っています。

意味的には使い分けているところもありますが，実際には使われていないです。

○司会

他にございませんでしょうか。

○質問者２

防止の方策として DMARC（ディーマーク）と，それともう一つ EMET（エメット）とおっしゃっていましたが，これは個人の私用の方法にも利用できるのでしょうか。

○講師
EMET（エメット）は、マイクロソフト社のサイトから，Applocker（アップロッカー）は，個人ライセンスです。

○質問者２
そうしたら，インストールして，個人の私物のパソコンもそうしておきなさいということでしょうか。

○講師
そうですね。EMET（エメット）の場合は，簡単に立ち上げることができます。それはほとんどデフォルトというか，初期設定のままで使えば十分です。それでほとんどのウイルスは動かない。
Applocker（アップロッカー）の場合は先ほど申しあげたように，ホワイトリスト方式があって，時々このプログラムは動かしていいかと聞いてくるわけです。それにこまめに判断をしてウイルスではないプログラムに許可を与えるというもの。少しチューニングをすると，しばらく落ち着くまでに時間が掛かる。
いずれも無料です。
今 Windows10 というのが出てきていますよね。あれでセキュリティがすごく強化されていて，Windows のアンチウイルスにお金を払わなくてよくなっているわけです。世界で一番ウイルスを集めている会社ってどこだと思いますか。マイクロソフトです。
その会社がアンチウイルスソフトを出しているのですから，これを使わない手はない。

○質問者２
Windows7 とかを使っている人は，今 Windows10 の無料アップデートをしたら，トラブルでうまく動かないという話があります。

○講師
そういう現象が起こっているみたいですね。ファイルが消えてしまったみたいなことを言っている人がいる。私は真相が分からないのですが。

○質問者２
どうもありがとうございました。

○司会
他にございますでしょうか。

○講師
　日本の情報セキュリティに関する情報は，ほとんどアンチウイルスベンダーを代表とするセキュリティ専門ベンダーの情報が９９パーセントくらいです。彼らは自分たちの製品を売るために競っているのですね。彼らの話だけ聞いていると，変な方向に行ってしまう。

○司会
　よろしいでしょうか。これにて，本日の講座は終了となります。
　山崎先生，ありがとうございました。それでは今一度，山崎先生に感謝の意をこめまして，拍手でお送りいただきますようお願いいたします。
　ありがとうございました。

（終了）