2001 年 8 月 2 日
弁護士 牧野二郎

ネットワークセキュリティと紛争処理

0. はじめに

今予想される危険性ということで、かなり犯罪が多くなってきているとのお話聞いて今年は 30 倍とかいう状況の様で、来年の警察白書等を見るのが怖いな、と思っております。

私が今一番怖いというか、考えております点は、不正アクセスが怖いとか怖くないとかいう議論ではなくて、どうもその先にあるものがだいぶ見えてきたかな、と言うことです。 後ほどお話が出てくるかと思いますけど、DoS 攻撃などでも、DoS 攻撃をしてサーバをダウンさせることが目的では無かったんだろうと私は今考えております。 ダウンさせることによって、その業務が停止して、それが株価に直結していく。ダウンしたという情報で株価が急速に低迷する。 そしてその後、急速に回復したという情報でまた株価が急速に上がっていく。 これを組織的に狙うことによって、株価操作が技術的にできる様になってくる。 これを相当組織的にやっている、あるいは、やってくるということを念頭に置くべきだろうと思います。

それからホームページ書き換え問題について言えば、各決算期が近くなった時に決算内容を書き換える、あるいは、株価を表示するホームページに侵入することによって株価を書き換える、という様なことに当然入ってくるでしょう。 彼らのスキルはやはりものすごい勢いで進んでいると考えておくべきでしょう。 そうしますと、これから狙われるのは、一企業のーホームページをいたずら書きというレベルでは無くて、それを踏み台にしながら世界経済あるいは様々な経済活動、あるいは金融活動に対する犯罪行為というのが進んでいくだろう、と思っています。

そういうことに対して、ある意味では企業の皆さんの徹底的な対応、あるいは大学のネットワークの先生方が大変努力されている様でありますけれども、どうも大学生の諸君は大変スキルがありますし、元気もありますし、大変困った様な状況も多々見受けられるわけであります。 私は良く著作権の相談をされまして、大学には著作権という概念が通用しないという話をしょっちゅうしまして、著作権概念はあるのですが守ってくれる人がいないという意味です。 やはり大学の中で著作権を大事にするということがほとんど常識になっていない、常識と非常識が逆転している。 そういう学生達が多い。 そこでそういったスキルのある人間が増産されてくると、やもすれば大変危険な状態が起きかねない。 そういうことに対して我々はどう対応したら良いのかということをやはり知恵を寄せていかないといけないだろうと考えております。

恐らく犯罪の国際化ということで、先程も話のあった海外の犯罪者あるいは場合によっては日本の犯罪者のスキルが上がってくると、日本でやると日本の警察に捕まるから他の国家に入ろうということでいたずらをする、カジノに入り込んでまた悪さをするということが出てくるのではないかと思われるわけです。 そういう意味では実体が見えない、身体がここに居て行為があちらに出るというそのタイムラグというか、ラグを利用して、様々な行為が行われるだろうと思います。私が今一番興味を持って進めているのが、電子署名、電子認証ということです。 恐らく経済活動の今後のインフラになるだろうと思われるそういう認証システムというものを大変強く興味を持っており、電子商取引のインフラを安全な形で普及させなければいけない、ということを考えてやっております。 Public Key Infrastructure をどう確保するかということに大変興味を持っているわけですけれども、このシステムは恐らく攻撃対象となっていくんだろう、と思っています。 こういった事が恐らく全世界対応という事で出てくるでしょうし、一方ではその大きな仕組みとして国際犯罪的なものにもなるん

だろうと思います。 そういう意味でサイバー犯罪というのかネットワーク犯罪の欧州協議会で検討されておられる犯罪防止条約、犯罪の対策の条約というのがあります。 警察庁とはちょっと立場が違うかもしれませんが、私は大変批判的にこれを見ております。 犯罪構成要件があまりにも緩いということで、サイバー犯罪という犯罪概念が本当に的確なのかどうかということをもっと慎重にしないといけないのではないかと考えております。 それから実際にはログのリアルタイム盗聴というのか傍受というのか、コンテンツの盗聴傍受というのが規定されているわけで、元々、私は盗聴というのが好きではないですから、通信傍受法の時も反対をさせて頂いたという様な経緯もございまして、かなり欧州協議会の方では広範な盗聴傍受ということを認めるということで法律化しようということで考えられている様です。 今後わが国でも批准するかどうか、どういう態度をとるかという点については、わが国の盗聴法、通信傍受法との関連も充分注意しながら対応しなければいけない問題だろうなと思っています。決して頭ごなしにおかしいとか良いとか言うわけではなくて、犯罪が国際化しているので、国際的対応が必要だと私も思うわけです。 しかし、それはあくまでも各国のコンセンサスでキチッと支えを置いていかないといけないのではないかと思っています。 その観点からしますと、どうもネットワーク管理者の皆さんにとっては、両方に敵が居る様な、体内にやんちゃなヤツを抱えて、その脇では警察がキッと睨んでいて、どうも自分のところが生きた心地がしないというのが正直なところではないかという気が致します。 そういう意味では、今日、私はメインとしてはネットワークセキュリティの観点でありますけれども、管理者の皆さんがどういう管理責任を問わされるのか、どうしておけば管理責任を問わずに済むか、ということでありますけれども、その辺りのところを若干考察させて頂きたいということで考えて参りました。

1. 刑事責任の原則と民事責任

一番目に、刑事責任の原則と民事責任の原則ということで、極々当たり前のことでありますけれども、刑事責任の場合、あくまでも基本になるのが、故意責任である。 従って犯罪実証、あるいは犯罪の対象被害者等々、あるいはシステムを認識し、これに対して侵害行為を行っていくということが基本になってくる。 過失犯罪の処罰というのは刑事法においては基本的には例外現象と考えておられて、故意犯の規定というのは山ほどありますけれども、過失犯の規定というのは構成要件で明確に規定されているものだけが過失犯になるという形になっております。 従って原則は故意犯、例外は過失犯ということになる。 更に、刑事責任の根拠としては、法益侵害といった客観要件、故意というような主観的な要件がどうしても必要になって参ります。 その意味では、従来から客観的な違法と主観的な違法、という事が議論されて参りました。 従って、管理者の皆さんには、この故意責任というのはあり得ないわけです。 よほど、ある指導者が自らサーバを管理して「攻撃せよ」と言ってサーバを管理している場合は故意責任が出てくるのですけれども、それ以外の場合ですと、通常、故意責任というのは出てこない。 では、過失責任ということがあり得るのか、注意義務違反ということがあれば、刑事法の成立の可能性が皆無というわけでは無いだろうと理論的には言えると思います。ただ、構成要件があるのでしょうか、ということで言いますと、現段階ではハッキリとした形、例えば過失傷害罪ですとか過失致死罪という様な犯罪形態の様にハッキリとは、規定されていないと理解しているのであります。 従って、不正アクセスについても、実は過失で不正アクセスする可能性というのは、どうもあるようです。 具体的な実例としては、知らない間に何かが動いてアクセスしてしまうという様なことも中にはあるのかもしれませんが、非常にリアルな意味では故意犯と限定していって良いであろうと考えております。 そういう意味では、刑事犯の故意責任の原則というのがあります。 これに対して、民事責任というのは、あまり詳しく書いてありませんけれども、民事責任は故意責任も過失責任も両方あります。 むしろ故意と重大な過失というのは、ほとんど領海線上にあると言えます。重大な過失と、通常の過失というのは、本当に区別出来るのか、と言うと、正直申し上げて私にはハッキリ区別できません。 そうしますと、民事の世界ですと、権利侵害というのが客観要件になって、主観要件としては、故意から重大な過失、通常の過失、軽過失というところまで全てをカバ

一する様な主観的な落ち度あるいは主観的な違法性というところで理解されるということになって参ります。 従って、私たちが通常の民事訴訟起こす場合には、故意または過失により、といういい加減な書き方をして訴状をおこさせて頂いております。 要するに私には判らない、あなたがどういう気持ちで攻撃をされたか良く判らない、しかし、いずれにせよ、お前はここに来ていたずらしたのだから、故意もしくは過失によって人に損害を与えた。 で、民事の場合、損害があるかどうか、と、行為と損害の間の因果関係があるか、というのが最大のポイントであります。 従って、あまり主観要件に拘泥されるということは無い、ということです。

ちょっと視点が違いますが、最近、ホームページとか掲示板で企業に対する猛烈な書き込みが成されるし、大学の先生あるいは研究者の皆さんに対しても猛烈な罵詈雑言を掲示板で書く、という様なことが起きております。 それに対してどう対応したら良いのだろうか、私に相談してきた人には、名誉棄損だとか業務妨害になる時には是非警察庁にご相談に行ってみてください、と振ってるものですから、大変迷惑をされているかもしれませんけれども、大変難しい問題がございます。 それで、民事訴訟でやれるのか、という様なことを良く言われるのですが、今申し上げた様に、故意とかいうのは余り問題なく、むしろ損害が発生しているのかという問題と、それから、因果関係があるのかというのが、これは大変難しい議論です。立証はものすごい困難だと私は理解しております。 ですから、実はものすごい数の企業妨害に対するご相談を受けているのですが、現時点まで私自身は一つも提訴に至っていません。 立証できるという自身のある事案というのがまだ私の手元に無いものですから、それについては、明確な損害と因果関係というのが、民事事件の場合は、大変重要になってくる。 逆に言いますと、先生方または管理者の皆さんが民事訴訟の被告になるといった場合には、故意/過失の問題は管理者としては出て参りますが、被害が本当に出たのかという問題、そして被害が自分のところから発しているのか、あるいは踏み台になって元々因果関係の中間地点でしかないのか、という辺りが、大変重要な問題になってくると一般的には思うわけです。

2. セキュリティ侵害の類型と法的責任

さて、2 番目として、セキュリティ侵害の類型と法的責任ということでありますけれども、一応いくつかの類型を分けて、違法性の中身が違ってくるだろうということで、検討しておくべきと思いました。

まず皆さんのコントロールされてますサーバが停止する、機能停止ということがあるとします。 先程申し上げた DoS 攻撃等でサーバがダウンするということがあろうかと思います。 この場合は、どちらかと言うと、全くの被害者になるわけで、確かに他の人のデータを預かっている、あるいは、通信の媒介行為を行っている、そのサービスが停止するということはあろうかと思います。 サービス停止については、恐らく契約の中で、短時間サーバがダウンしてサービスの提供が出来なかった場合の損害賠償あるいは利用課金の返済、あるいは免責、という規定があろうかと思います。 従って、そこは余り大きな問題にはならないでしょう。 86 年頃に、世田谷区で地下ケーブルが燃えてしまった事案において、NTT に対して損害賠償請求の裁判が起こされましたけども、いわゆる通信料以外では損害賠償の責任は無いということで結論が落ちております。 で、もう一つ、どこまでこれは法律論になるのか、是非専門の皆さんと我々法律家が研究しないといけない事だと思うのですが、インターネットというのは、いわゆる専用回線の（電話回線と違って）Best Effort というのでしょうか、繋がるかどうか分からない、極力頑張りましょう、メールが届かないということもままある、という前提を置きます。 メールが届かないから損害賠償という話は聞いたことが無いわけです。 そうしますと、いわゆる今の NTT の事件で、電話回線が止まった、これはもう死活問題だというのは何となくわかるわけで、それでも責任が無いという判例が出ているわけです。 そうすると、インターネット回線がダウンしたからと言って損害賠償請求されるのか、ということで言いますと、どうも Best Effort というのが、もう一つフィルターになって責任関係が弱くなってくるのかな、と私は理解し

ております。 ただ、現在の様に大変強いインフラというのか、だんだん重要なインフラ（基幹インフラ）になって来ましたので、そうなってきますと、また考え方を少しずつ修正しなければいけない事態も生まれてくる、と思っております。 ただ、そういう意味では、通信が仮に途絶えたとし、あるいは落ちたとしても、そう大きな責任は出てこないというのと、Best Effort の世界という 2 重の安全面が働いていると考えております。 ただ、民事責任を負うかどうか、という点でありますけれども、1 つご注意頂きたいのは、民事責任は無くても、民事訴訟で引きずり回されるという事は山ほどありますので、これはなかなか避けられない。 不当訴訟だといって反訴起こしても結構ですけれども、あまり生産性が無いということになります。 そうしますと、初期対応の問題として、こうした攻撃への危険性というのは予測できるのだろうか、予測出来たとすると予防策はあり得るのだろうか、それに対する対策というのは実施されていたのかどうか、この辺りが恐らく事前対策としての被害者もしくは関係者に対する説明という意味で役に立ってくるだろう、と私は理解しております。現時点では、私はこの秋くらいからものすごい勢いでこの DoS 攻撃が再発するだろうと実は思っています。常時接続そしてブロードバンドが、低料金で接続し利用が可能です。 先日あるソフトウェアをはめ込んで外からの攻撃を見てみましたら、1 日に 4〜5 回攻撃が入ってくるのが見えるわけです。 インターネットに直付けして Port Scan かけられて、攻撃用ソフトを産み落とされていれば、常時接続でありますし、ケーブルを使って、ボンボン放り込んでいったら、とんでもないことになる、というのは目に見えるものです。 そうしますと、私はこれは「怖い、怖い、怖い。」という話ではなくて、皆さんの責任がその度にグレードが上がっているとも理解出来るわけです。 要するに、低料金で通常の市民が大変高機能のコンピュータを常時接続で接続し、メールに対するセキュリティもほとんどしていないという条件がかみ合ってくる場合、いつ DoS 攻撃がかけられてもおかしくは無いと判断するのが、だんだん常識になってくるのでは無いかと思います。 ですから、その意味では、注意義務がものすごく高くなりつつありますよ、ということだと思います。 DoS 攻撃の危険性を予測して頂きたい。 予防策はあるのか、予防出来ないこと、あるいは、予防することに猛烈な費用がかかる場合はそんなことしなくて良いのです。 要するに、期待可能性という議論がございます。 簡単にできるかどうか、ということでありますが、どうも私の聞いた範囲では、ある一定の機能のルーターをかませることでも対応できる、と聞いておりますし、ソフトウェアの Firewall の様な形でも対応ができる、とも聞いております。 これに関しては、技術者ではありませんので、専門の先生方のご判断だと思います。 ある程度廉価に対応ができるということになって参りますと、これは注意義務の範囲に徐々に入ってくるということになるだろう、と思います。 具体的に実際に対応は施されていたのかどうか、例えば、ある一定の監視が出来る様になっていたのかどうか、あるいは負荷がかかったら、1 度回線を切ってしまうという様な一時的に回線を切って防御する様な仕組みを考えていたかどうか、あるいはそういう措置が取られていたかどうか、ということが問題にはなるでしょう。 そうしますと、事故が起きた時にすぐに損害が拡大し、あるいは、波及していくことを防止するべくメールを打って、「実はこういう事態が発生しました」「当方ではあらかじめこういうことを予想して、こういう対策をうって参りました」「こういうことで最低限の形でくい止めました」もしくは「残念ながらこういうことになりました」という説明が出来る。 そうなってきますと、充分な対応をしていたということになると、それを持って弁護士のところに行って、「損害を受けたのですがどうでしょうか」と言った時に、分からないながらも弁護士は、「だってこんなこと一生懸命やっていたらこれ以上訴訟起こしたって絶対勝てない」「過失の範囲がこれじゃ特定出来ない」「過失のレベルまで行ってない」「これじゃ無理だよ」と、要するにズル抜けだったら法的責任追求してもいいかもしれないけれども、それ以外ダメだよ、と相談された弁護士の方で「これは訴訟起こせないな」「立証大変だな」と答えるでしょう。 立証になったとしても先生方の方が猛烈な資料持っておられるし、技術的なスキルもありますので、よほどあちらが鑑定人、技術士か何かを使って被害の中身を徹底的に洗って対決してこない限り、まあまあ比較的優位かと思われます。 その意味ではあまり心配いらないと思われます。 専門家として最低限のキチッとした注意義務を果たして頂ければ、いいだろうと思います。 ただ今後は注意していないと、お医者さんの訴訟でもそうですが、お医者さんの方がスキル持ってるから大丈夫だと思っていますと、

必ず被害者側にも医師を加えた弁護団というのが出来上がりますし、被害者側でカルテを開示して、やはりミスはミスとして見つかるという角度がものすごく高くなってきております。 インターネットはだんだん、だんだん、オープンになってきておりますので、落ち度は比較的見えるだろう、と考えられます。 充分注意は必要だ、ということかと思います。

スパムメールの発信基地にされたり、あるいは踏み台にされる、という様なことも出てくると思います。 踏み台にされるということの法的評価ですけれども、セキュリティ対策を取る必要というのは当然あるわけです。 しかし、それが法律上の義務になるのか、すなわち、それを懈怠した時に懈怠責任というのでしょうか、その義務を尽くさないことが刑事罰になるということになるのか。 現段階のセキュリティ対策をとる義務・必要性というのは、先程少しお話がありましたけれども努力義務、あるいは、民事的な要素が出てくるか、という辺りになると理解しております。 実際に基礎的なセキュリティ対策が一般化した場合にはどうなのか、ということです。 例えば、Firewall もかつての様な値段ではなくて、私の知りうる範囲ですが、Personal Firewall 六千何百円とか、八千何百円とかで売っている、という場合に、専門のサーバが何も Firewall を入れてない、セキュリティ対策してない、ということになりますと、これはちょっと問題外だと思います。そういう意味では、クラッキングの事故発生報告とそれに対する対応策、あるいはパッチ等の指導、あるいは配付が成されている場合、どう対応するのか、ということになります。 先程警察庁の方からご説明ありましたし、私もどういう対策が取られるべきだとされているのかと思い見てみました。 確かにホームページが出ております。 インターネットをちょっと検索するだけで、ホームページのクラッキング事件に関してはこういう対応してください、とリンクまで張ってパッチが配られているわけです。 今までそんなことなかったと思うのですが、警察庁のホームページでキッチリと教えてくれているわけです。 そうしますと、そこまで対策が示されていながら管理者がそのホームページを見てないということは、かなり大きな落ち度になるでしょう。 要するに、パッチが配られていることを知らなかった、とは言わせないという国家の対策があるのでしょうか。(笑) 知らないとは言わせないぞ、薬がちゃんとここに置いてあるのに、なぜ取りに来ないか、という職業人としての責任を徐々に高めていくというのが、我々の義務だと思います。その意味では、やはり昔の様にどう対応したら良いのか、ということを考える段階はもう終わっています。 そうすると、あとは確かにパッチを当てる時に変に当てるとサーバがダウンしてしまうので、そう簡単に当てられないよ、とか、色々費用の問題やダブルで走らせなければならない問題、あるいは、もっと大事な情報が無くなってしまうからそう簡単には出来ない、という様なそういう事情はあろうかと思います。 そういったことは、細かくメモして頂いて、業務報告をして頂いて、常に全体でセキュリティのことを考えて頂くということは、どうしても必要になってくるでしょう。 そういうことを小まめにやって頂けてれば、そういう意味での民事責任も含めて大きな法律問題にはならない、と考えて頂いて良いと思っております。

ここでは一つの視点としまして、不正アクセス禁止法というところで、管理者の責任という規定がございました。 それをここにプリント、第 5 条ですけれども、写させて頂きましたので、少し見て頂ければ助かります。

この 5 条では、一番最後のところに、「速やかにその機能の高度化その他当該特定電子計算機を不正アクセス行為から防御するため必要な措置を講ずるよう努めるものとする。」ということで、管理者としては常にこうした努力を払わなければいけない、ということになってくるわけです。 この辺は実は私は行為者の不正アクセス行為をやって逮捕された人の弁護などをやる場合に、大変よく思うわけであります。 実際には、非常にズル抜けのところが多いのです。 つい先日もある有名な化粧品会社でしょうか、ホームページに個人情報のファイルをポンッとオンラインに置いておいて（それがクラックされたんでしょうか、と彼らは言っておりますが）、表に出てしまって漏洩事件起こしたというのがつい先日ありました。私の立場では、クラックされたのかもしれませんけど、管理者の落ち度の方が大きすぎる、あれは本当に民事訴訟で責任を問われても致し方ない世界だろう、と思うわけです。 そういう意味で、必要な措置を講ずるというレベルは

毎年高くなってきている。 ところが、それをキチッと守っておられないズル抜けの管理が大変多い、その意味では、先生方もズル抜けになっていないかどうかを良く注意をして頂きたい、ということであります。
時々感じるのが、大学もそうですが、サーバ管理者が不用意にサーバを又貸ししたり無断でレンタルしてるケースがあります。 わいせつサイト等で色々問題が起きて、とんでもないということで潰しにかかってみると、どうも正規の所に寄生してわけです。 正規の管理者はそれを認識してないらしく、サーバが大きいものですから、その中のある部分に変なサイトが出来上がってるというのがあるわけです。 私達は内情証明郵便で上に上に辿っていった管理者の大元のところに刃を突きつけるわけでありますけれども、それをやって初めて気がついた、という管理者の方が結構いらっしゃいます。そういう意味では、サーバ全体のお掃除の様なことを常にやって頂かないと、どういう構成で何が入っているのかというのを徹底的にチェックしていくことも管理業務の一つとなります。 担当者任せにしておくと、とんでもない痛い思いをする、ということもございます。 その辺では、やはり管理責任というのは出てくるだろうと思われます。 これは民事責任という主旨でありますけれども、強く感じるところであります。

それから、乗っ取られて攻撃基地にされる、という様なことがよくあるかと思われます。 これはいわゆる踏み台論というものであります。 これまで踏み台論というのはあまり大きく議論がされてきていない、少なくとも法律論的には踏み台にされたことで、直ちに何か共犯の様なことになるかというと、必ずしもそこまでの戦意的な議論は無かったわけです。ただ、一つヒントになるというのか、注意はした方がいいなと思うのは、自動車損害賠償保障法第 3 条という規定がございます。 これはあくまでも”車”という特殊な移動体、これが事故起こすというのはしょっちゅう有ることなものですから、その所有者(運行供用者)の責任というのを書いた規定であります。 現在はサーバ管理者に対してこういう法律はありませんから、そういう意味ではサーバ管理運用責任法などというのは無いわけですから、今日の段階では胸をなで下ろしていて頂ければ良いのであります。

私が今ちょっと怖いなと思うのは、大学あるいは研究所のパソコンが(これは素人が危険と感じているだけかもしれませんが)、非常に高性能であって、あるいは、非常に機能のあるソフトウェアが大量に入っていて、そして、通常のパソコンでは出来ない様々な行為が出来る。 それが例えば遠隔操作の様な形で大学の持っているスーパーコンピュータの機能を発揮して何か非常にすごいことが出来る、という様なちょっと例外的なケースを想定しますと、私はある意味でものすごい性能のあるコンピュータを制御する責任というのは、ひょっとすると車の所有者と同様の責任が出てこないとも限らないな、と思うことがあります。 それは恐らく出火責任等々の火元責任者(お部屋のところに時々書いてありますね、この部屋の防火責任者はこの人ですよ、と。)と自動車の運行供用者とのちょうど間くらいから、その辺のある一定の法的な責任を根拠付ける仕組みになってくるのではないかという気が致しております。 その意味で、鍵をかけないまま車を置いておくというのと同様に、誰でも入れる様に甘い管理の元で大型コンピュータを電源入れたまま放置してあると、いかにもどうぞお使いくださいと置いてある、ということで、運行供用者責任の様なものが出てきてもおかしくは無いな、という気が致しております。 そういう意味での先生方の充分な注意というのは必要になってくるのではないでしょうか。そうしますと、運行供用者に責任を認めるという法論理を使ってきますと、例えば企業や大学が足掛かりにされて、ものすごい攻撃を受けたとします。 もしその大学が Secure にしておれば通常起きない、といった様な場合(そういう特殊性の場合だと思いますが)、ひょっとすると今後損害賠償請求の訴訟が起きる可能性があるのではないか、という気がしております。

次に、ウイルスを配付してしまった、という場合のお話です。 この事件は結構多発しております。 ウィルススキャンソフトウェアがかなり一般化しておりますが、自分のところでウィルスをメールにつけてまいてしまったけどどうしたら良いだ

ろうか、という相談結構入ってまいります。 その時に私が一番最初に聞くのは、「ところで御社はウィルススキャンをキチッと履行されていますか」ということです。 で、「していません。」という方に関しては全ての訴訟が起きてくると覚悟して、とにかく責任者を配置して「ごめんなさい」の繰り返しで、ともかく被害が無いかどうか、これ以上広がらない様にという徹底した指導をやって下さいということをお話しています。 で、「ウィルススキャンをかけています」ということになると、最新のウィルスパターンまであたっているのかどうか、ということを確認したうえで、それでも出た場合には、メールでいいからともかく「ウィルススキャンに引っかからないメールが走っているから気をつけてくれ」「私のところではウィルススキャンをキチッと実施しています」「これに引っかからない例外的なウィルスが走っていますので充分ご注意ください」という（そんなの 30～40 分で対応出来るはずでありますけれども）、その様な内容のメールを出しなさい、と申します。 まさに後者のケースは不可抗力の問題になります。 ところが前者の場合、ウィルススキャンソフトが存在し、それが今ではただ同然の金額でばらまかれているわけであります。 新品のパソコン買うと全部入っておりますよね。 そういう状態になってくると、もはやウィルススキャンをしていないということはむしろ大きな過失を認定する基礎になってくるのではなかろうか、と思います。 少々厳しい言い方をしておるかもしれませんが、そう考えます。 日本ではまだウィルスの問題で（ウィルスをばらまかれたということで）、大きな訴訟は起きていない様です。 公式なところでは報告されていませんので、今のところ見たことがありませんけれども、アメリカで去年の暮れにウィルスに感染したという被害者の方から、ウィルスを送ってきた企業に対して損害賠償の請求訴訟が起こされたという報道がを見ました。 それがどの様に進行しているのか色々調べているのですが、まだ出てこないので、まだ結論は出ていないのだと思います。 今後は恐らくウィルスをばらまいてしまった場合、それが社会的に大きな意味を持つ団体もしくは企業、もちろん大学もそうでありますけれども、それが大変多くの被害をばらまいてしまったという場合には被害者からの損害賠償請求があった時に具体的な過失というのを認定するうえで、ウィルススキャンをやっていないというのは過失の根拠にされてしまうだろう、と私は理解しております。 従いまして、メール送受信時には必ずウィルススキャンをかけて頂くということが、やはり必須になってくるんではなかろうかと思います。 ごく最近でしょうか、よく見えない、とんでもないものが出ましたと、ウィルス対策の開発会社が無料で特殊なソフトを配るということも行なわれています。 そうしますと、そういうものが出ているにも関わらずセキュリティ管理者が何もしていない、放置しているというのは、やはり問題がある、問題の根拠になってくるだろう、と思います。従いまして、先生方のところあるいは、管理者の皆さんのところで、ある一定の対策をしている、ということであれば（それでも起きることはありますので、ウィルス事件というのは。）、先程申し上げた不可抗力です、と言うことが判る様な文面でのメールを出し、直ちに対応策をとって頂きたい、ということをしなければいけないということになると思います。

以上の様なシステム管理というテクニカルな場合とは違いまして、違法書き込みが成された場合とか、違法書き込みが公開される様な場合というのがままあります。 これが先程お話しました掲示板等々の問題もありますし、大学のホームページ、企業のホームページ、企業の掲示板というものも結構出て参りました。 そういう意味ではこのケースだけはどちらかと言うと少し慎重に対応しなければいけないケースだろうと思っています。 場合によっては刑事事件になる危険性すらある、ということであります。 具体的には名誉棄損であるとか業務妨害、あるいは脅迫といった様なことが考えられるわけであります。 それから民事事件としても損害賠償の対象となる可能性があります。
そこで、いくつかの事例を挙げておりますので、お話をしたいと思います。 客観的に見ますと、どう言っても、その書き込みをやった第一次責任者といいますか、一番最初に書き込みしてそれを公開した人間が刑事責任もしくは民事責任を負うというのは、それは当たり前です。 これはもう当然のことですから、前提に置いておきましょう。 問題は、管理者がそれに対しどう対応したら良いのか、ということであります。 その時にいくつかの判例が出ているわけでありますけれども、管理者としてまず書き込む前にチェックすべきなのかどうか、ある意味では検閲というか審査というか、そういうも

のをすべきなのかどうかという問題が一つ。 それから、何もしなかった、あるいは、書き込みが告発されたとか、あるいは通知された時に何か対応すべき義務があるのかどうか、という事後的な対策という点が一つ。 恐らくはこういう 2 つの方向性というのは見ていかなければいけないだろう、と思っています。 アメリカのミレニアム・コピーライト・アクト（新世紀著作権法）というのが 98 年に出来ましたけれども、その中でプロバイダ（情報の提供場所を準備している管理者）に対して、著作権法の観点からの責任免除規定（責任裏付け規定）がありました。 要するに、当たり前のことですけど、著作権法に違反するコンテンツが挙がっていた場合、その挙がっていたことをプロバイダに通告をするには、権利者でないとダメだという規定になっています。 要するに私の書いたものが私に無断で Web に挙がっていて、私が被害者であり、私は正当な権利者であるということでプロバイダに文句を言う。 プロバイダはその権利関係を明確にしたうえで、それを使って金を儲けていて、事前に認識し、違法性が判った場合には消さなければいけない、という規定があります。そうすると、そういう要件が無ければ免責されるということになるわけです。これは、著作権の問題について限定されたものでありますので、今後通常の名誉棄損であるとか業務妨害とかいった様なことにどう影響してくるのか、というのはまだ未解決の問題であります。

ここで、ごく簡単にこれまでの判例の流れというのを見てみますと、1 番最初に 91 年、これは BBS の問題でありますけれどもコンピュサーブ事件というものがありました。 ここに書いてある通り、コンピュサーブが何も管理してない、ということであると、それは「見てないからね」ということで免責になりました。

次にプロディジー事件というのは 95 年に起きたわけですけど、プロディジー社が自ら掲載内容編集して管理する、安全ですよ、ということを言ってしまったわけです。 そうしますと、「大丈夫ですよ、私が管理していますよ」と言ったばかりに、コントロールしているはずだ、コントロールする義務がある、ということになり、編集責任というのが出てくるということで、編集者としての責任というのが認められたというケースでありました。

ちょっと飛ばして頂いて、ニフティ事件というのが有名な事件でございます。 電子会議室の中での発言内容について名誉棄損に該当するのではないか、そうしたことについてどうするのか、という議論でありました。 一般論として監視義務とか削除義務というのは無いということを一般的な議論として言いました。 ものすごい数の書き込み、あるいは、掲示あるいはホームページ、これらを全部監視しなければならないと言ったら大変なことになるわけで、こんなことしなくて良い、と言いました。 しかし、Nifty のシスオペがそうした違法事実を知りつつ、手をこまねいたこと自体に対して、条理上の作為義務が生じるのではないか、という議論が行われました。 これは大変面白い議論です。 どういう事かと言うと、一般的に何もしなくて良い、そして何らかの権利者からアクセスがあった場合、それに対して、コンテンツを消さなければいけないと言っているわけではなく、何らかの対応しているか、という言い方でした。 その時に何らかの対応の中身が、掲示はしているけれども被害を申告した人と書き込んだ人を合わせるとか、話し合いの仲介の労をとっていたという事実があった場合には、これは出来るべきことをやっているから問題ないということで、5 つ位訴えの中で、訴訟の対象物になったのですが、4 つ位がそういう話しで全部終わりました。 1 つだけ残ったのが、いくらクレーム言っても完全に無視して何も対応しなかった。 で、シスオペはそれが表現の自由だと信じて今でも戦っておられる訳ですけれども、裁判所的に言いますと、被害者が「被害だ、被害だ」と言ってるわけですから、それは何らかの形で場を設定するなり、話し合いをするなり、両者のメールをやり取りをされるなり、何か対応が出来たんじゃなかろうか、というのが裁判所の考え方だったわけです。 そういう意味では、常識的な対応をしたかどうか、消えてる/消えてないというメルクマールでは無く、対応していたかしていなかったか、というところで、責任落としています。 これが一つの論点です。

もう一つは、非常に面白いのですが、被害を訴えている人というのは、必ずしも Nifty の会員かどうかは判らない。 書き込みしたのは Nifty の会員だろうけれども、シスオペが本当にそれを消すべき理由があるのかどうか、会員外の人の権利を守るべき法的地位にあるのかどうか、ということですが、民事責任というのは基本的に契約責任があります。 と

ころが、会員外の人とは契約ありませんから何の責任法律関係無いわけです。 そうすると不法行為しか無いわけです。シスオペが黙っているということは不法行為を助長しているのか。 不法行為を助長しているということになると、一つ目の問題の監視義務が出てきてしまいますので、それは無いと言うことです。 ここである種の理論矛盾に漂着したわけです。 そこで裁判所はウルトラ C を使ったわけです。 どういうことをやったかと言うと、電車があっちから走ってくる、私と鉄道会社は何の契約関係も無い。 しかし、電車がもうちょっと進むと線路の上に石ころが置いてある。 この石ころに躓いたら電車転倒してしまう。 そうすると、これは当然どかすべきで、自分で石を置いたら“往来危険汽車転覆罪”で大変な犯罪になるわけです。 ところが、自分で置いた訳じゃない。 人が置いた石をどかすかどうかと言うことですが、たまたまそこでチラッと見て、「石が置いてあるなー。石はどかした方がいいんじゃないかなー。」と、電車があっちからどうも来ているぞ、これは大変なことだからどかそうかな、と思う。 しかし自分が轢かれたら怖いな、とか色々逡巡するわけです。その時の私の地位が条理上だと裁判所は説明するわけです。 要するに法律的にハッキリ書いているわけでも契約のものでも無い、しかし、あなたには他の人の権利を守る常識的な・社会倫理規範的な、そういう地位がありますよ。 これと似た様なものが、恐らく皆さんにあるのだということだと思います。 そうしますと、条理上ということで言うと、クレームが飛んできたら、そのクレームに対して的確に反応して頂きたい。 但し、クレームがあったから直ちに消す、ということになると、クレームを言うことによって、全部消えてしまうという安易な流れが出てきます。 そうすると、表現行為に対するチリング・イフェクトという萎縮効果が出てきてしまうので、これは裁判所としては嫌なのです。 ですから、常にこう何かをしなさい、しなかったら違法ですよ、という言い方はしない。 文句があったら、その人を聞いて、書いた人と会わせてあげるとか、ある種の情報交流をしてあげるという様なことはしてあげるべきなのだろう、ということであります。 その辺りをちょっとご注意頂きたい、ということであります。

これを前提に考えてみますと、都立大学事件というのは 99 年 9 月にあったわけでありますけれども、大学内ネットワークのホームページに名誉棄損を内容とする書き込みがあった場合、被害者に対してこれを保護すべき法的義務が存在するかについて、一般的なそういう法的地位というのは無い、ということになったわけです。 ここからが問題なのですが、その内容を知って、明白に名誉棄損に当たる、被害が甚大である、加害者の行為が悪質である、という場合に限って、言ってみれば、犯罪行為が目の前で行われている時に、窮迫不正の侵害がまさに目の前で行われているのにお前ほっておいていいのか、こういう感じで、極めて例外的なケースに、大学の責任が肯定される、と言うものであり、本件の事件では、大学の責任は否定された、ということがありました。 従って、大学当局としては、表現の自由はどこまでか、というギリギリの悩みは持つだろう、と思います。 そういう意味では、ここに書いた様な被害、それから悪質さ、ということを自主的に判断して頂く、ということになるのではないでしょうか。

最後になりますが、ゼラン事件というが上から 3 つ目の判例に出て参りました。 問題発言があった場合、損害賠償を避けるために、表現を削除する方向となる可能性がある。 この方向では表現の萎縮効果をもたらすことになるため、Distributor（運搬者あるいは場所の提供者）としての、責任というのもどうだろうか、させるべきではないのではないか、という流れが出てきていると指摘しています。 そうしますと、今までどちらかと言うと我が国でも条理上の責任ということで何らかの管理責任を認めるという方向を取っておりましたけれども、表現のチリング・イフェクトということを考えると、あまりそれを乱発しますと表現行為が萎縮してしまう危険もある、ということでこれは少し押さえ気味にコントロールをしていこうという流れが出てきている様だ、ということであります。 しかし、そうは言っても無責任で良いということではありません。 ある程度の責任が出てくるというのはある、と思います。

3. 紛争処理の可能性と現実性 専門家 ADR の制度を確立すること

最後に「紛争処理の可能性と現実性」ということでありますけれども、私は今日、大変多くの専門家がいらっしゃるので、

是非ともこれを最後にまとめとしてお話ししたいわけですが、専門家の運営する ADR(Alternative Dispute Resolution : もう一つの紛争解決手段)、もう一つのとは、司法作用いわゆる裁判という以外の調停、斡旋、あるいは何らかの評決をする様な仕組み、これを是非作りたいということであります。 それを邪魔しているものとして弁護士法第 72 条といのがございまして、弁護士以外は弁護士活動しちゃいけないという訳です。 そうしますと、侵害者がいる、被害者がいる、その間である一定のルールを決めて行こうという裁定をする行為は、権利の対立を調整するための法律的な行為だと豪語している人たちが一部いるわけです。 そういう人たちが自分のテリトリーをやくざが如くに守ろうとするわけです。 それが弁護士法 72 条という規定で、これに反する者は信託銀行であろうと、司法書士の先生であろうと、税理士であろうと、はじき飛ばすというテリトリーを作っているのです。 私はこの規定は撤廃すべきだと思っていますし、弁護士会の中にもこれはいらないと考えている人も出てきています。 この規定が邪魔になって専門家が専門的知識を利用して評議員になる、判定員になる、ということが現段階で出来ない状況となっています。 ですから、是非この条文を改正して、ある種私達の様な権利関係にずっと経験を積んできた人間と、技術的な側面あるいは科学的な側面を充分理解している先生方と、あるいは専門家の皆さんと、同じボードについてその侵害行為が違法行為なのか適法行為なのか、この被害はどうしたら守れるのか、ということを徹底して議論して、ルール作りをするという、司法とはまた別の(司法は証人尋問して権利関係明確にして国家としての判決をする、という大変重要な機能があります。)、もっとスピーディな世界で技術的なことも踏まえて今の様な議論をする場面が必要なのでしょう。 そういうものを ADR として作っていく必要がある。こういったことを我々が意図的に進めていかないと駄目だ、ということであります。 大変面白いのは法務省も裁判所も ADR 構想については賛成なのです。 なぜならば、司法当局がこういうネットワーク犯罪を見事に切り裁けるかというと、裁けない、というのは彼らが一番良く判っているのです。 ですから、もっと的確に前に進まなければいけない。 アメリカで言う前提的仮処分というのでしょうか、仮処分かけたら 3 日で結論が出る、こういう時代でないと対応できないわけです。 日本の様に仮処分かけて 2 ヶ月後に審尋が入り、審尋の結果が大体 6 ヶ月後です。 6 ヶ月間もあればソフトウェアの生命終わってしまいます。 6 ヶ月間で仮処分すらも出ないということになると、これはもう機能不全ということになります。 そうしますと、前提的仮処分が出る様な、あるいは一定のルールが決まる様な、そういう仕組みを作らなければいけない。 これがこれからの紛争処理の眼目になるのではないかと思われます。 政府もその方向を取りたいと考えておられるわけであります。 これに頑に抵抗しているのが我々弁護士ということでございますので、まあ袋叩きにして頂きたい。(笑) それで何とか ADR を作っていかなくてはいけない、ということだと思います。 大変過激な発言を致しました。とりあえず私のお話しはここまでにさせて頂きます。(拍手)