特集：営業秘密保護法制の再構成

【講演録】

富士通の情報管理について

西　田　雅　俊

国内企業は情報管理について結構オーソドックスであり、先般経済産業省が指針を出した内容について忠実に行おうとしており、どこまで守れるのかというところはあるのですが、国内企業、経済産業省とは結構いろいろ情報交換もしながら進めているところもありますので、どういうことをやっているか、少しお話しさせて頂きたいと思います。

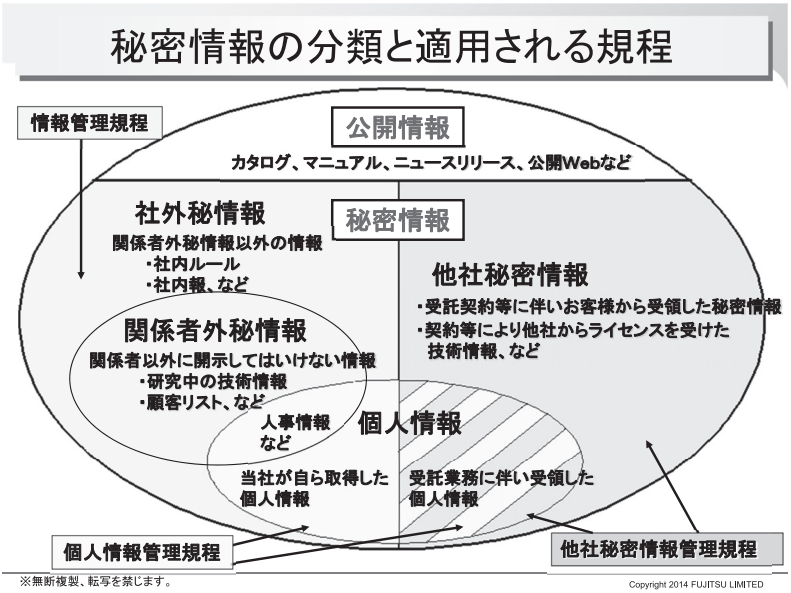
当社の業務はともかくとして、従業員が今約16万人強、グループ会社を入れると約500社、こういう中で秘密管理をどうしていくのかというところが問題となるかと思います。そのときに会社としての全体的な理念というものを示さないといけないということで、「FUJITSU Way」というものが存在します。「FUJITSU Way」には企業理念から企業指針、行動指針を示しておりますが、その中の行動規範の中で「機密を保持します」ということを従業員、グループの存在意義、大切にするべき価値観、社員一人一人が日々の活動において行動すべき原理原則の行動として書かせて頂いております。特に「機密を保持します」、それから知財についても「知的財産を守り、尊重します」ということを行動規範の中で明示しております。

ただこれだけ言っても漠然としていますので、では具体的にはどうなっているのかというところですが、当社の規範であります「FUJITSU Way」の中の「機密を保持します」というところを取り上げて、富士通グループ全体の情報セキュリティの基本方針というものを設定しております。この方針に基づいて、情報管理とICTセキュリティ――これは情報システムにおけるいろいろなセキュリティ管理です――このような規程というものを作って、社員に徹底をしているのが現状です。

では秘密情報の分類と適用される規程ですが、今日の紹介している資料

（図１）もそうですし、カタログ、マニュアル、ニュースリリース、公開文献、これは公開情報として当然世の中に出ていることで秘密情報ではありません。それ以外の情報は基本的に全て秘密情報として管理しましょうと考えております。秘密情報と言っても、１つ１つそれぞれ用途もしくは定義が違っております。この資料の中の下の円の左半分、これがどちらかというと富士通そのものが持っている情報を管理する内容になっております。大きくは「情報管理規程」というものに基づきまして、「社外秘」と「関係者外秘」に分けておりますが、「社外秘」というのは社内のルールであったり、社内報のような社員のみに知ってもらうような内容であったりということで、比較的、社員であれば知っているような情報については「社外秘情報」として取り扱われます。一方、先ほどコカ・コーラ様でもお話しされていましたが、限定してこの人しか触れてはいけない、特定の人しか見てはいけない、たとえば研究中の技術情報であるとか、顧客リストであるとか、こういうものについては「関係者外秘情報」という形で文書やデータに記載して、厳密な管理のもと、これを使用するということになります。

図１



一方、必ずしも秘密情報というのは当社だけの情報ではありません。たとえば第三者の技術ノウハウを受けとる場合や、お客様からの受託契約に基づいて頂いたお客様の秘密情報につきましては、これは秘密情報の中ではまた「他社秘密情報」と捉え、「他社秘密情報の管理規程」というのを設けまして、しっかりと管理致します。当社の情報が漏れた場合は当社が単純にダメージを受けるだけなのですが、第三者の秘密情報が漏れた場合、当然当社のダメージだけではなくて、社会的信用を失ってしまうという大きな問題が起こりますので、規程を分けた形で対応しております。

それとよく最近問題になっております個人情報、これについては「個人情報管理規程」ということで、しっかりと個人情報を守るポリシーを作り、このような規程を設けております。

細かく言うと時間が足らないので細かくは申し上げませんが、「情報管理規程」ということでは社内を流通する情報の扱いを規定するということで、基本ルールは「公開情報を除き社外に開示しない」。「『秘密』表示をする」とか、「関係者以外アクセスできないようにする」ようにしております。当然秘密情報を第三者に公開するときにはNDA、いわゆる秘密保持契約を締結した上でしっかりと「秘密」表示をして公開しております。

それからアクセス管理とか情報の廃棄については、指針に沿って必ずパスワードを設定したり、廃棄するときはシュレッダーや焼却処理というものをしっかりと行うというルール決めをしております。

次に最近よく問題になる、個人情報の問題です。これは「プライバシーマーク」というマークの制度に準拠した個人情報の管理をしております。当然、利用目的を特定して、その目的の範囲で利用するということと、当然関係者以外には開示しないということで、やはり一番大きなところは利用目的の明確化、その目的の範囲の中で、必要な範囲で取得する。余計な情報は絶対にもらわない。もらったばかりに管理や責任が非常に大きくなります。情報の入手については適法かつ適切な方法で取得する。個人情報については紛失、漏洩すると大問題になりますので、安全管理対策を施していきます。

それからID、パスワード、暗号化、鍵付きロッカー、場合によってはその部屋に入れない等、セキュリティをしっかりと施しております。

それから資料の一番下に記載しておりますが、管理責任者を必ずおいて、

各部門で運用細則を作成する。私共はさきほどお話ししましたように、世界で16万人強の従業員がいます。中央集権的に情報管理を行うように言っても、なかなか細部までこれを回すというのは本来難しいところがありますので、各部門、たとえば事業部門、営業部門で「こういう情報を扱う場合は『運用細則』を決めて作成した上でしっかりと管理をする、そして適切に年１回の監査を行っていく」ということを遵守しております。

また「他社秘密情報管理規程」ということで、これは契約で定められた目的にのみ使用することを遵守しております。当然、関係者以外には開示しないということで、特に私共、多方面のお客様とお付き合いをさせて頂いておりますので、そこでの秘密情報につきましては当然管理責任者もしっかりと配置致します。それから情報管理の有資格者に対しては、教育というものを――後ほど少しお話ししますけども――行った上でアクセス権限を与えます。

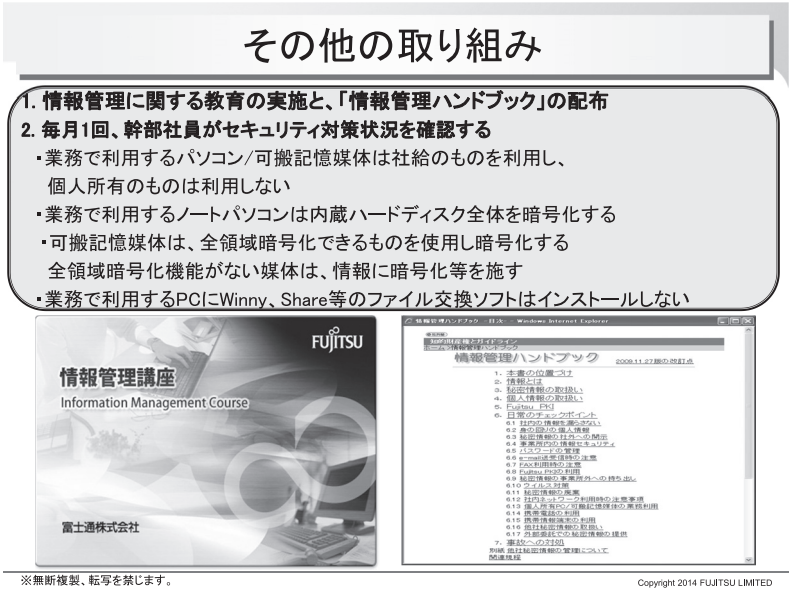
資料によっては台帳管理というものを行っていきます。当然セキュリティとしてID、パスワードや鍵付きロッカー、それからネットワーク、ノートPCも暗号化等でアクセス制限をしたり、どうしても紙で渡さないといけない場合は手渡しだとか書留だとか、セキュリティが守られる手段を使用します。

他社秘密情報は秘密保持の期間が過ぎると必ず返却とか廃却をしないといけなくなりますから、台帳等でしっかりと管理していきます。

電機業界、特に当社の業界は結構独特なところがあります。当社が注文頂いた仕事を委託先に出すという場合もありますので、委託先には当然同等の義務を課した契約を締結した上で秘密情報を提供する、かつ最終的には審査も行うということを実行しております。

とはいっても従業員に対してもしっかり教育をやらないといけないということで、情報管理に対する教育、資料（図２）の左に記載しておりますが、これはeラーニングの教材なのですが、このような講座を開講して従業員に教育を実施しております。また情報管理ハンドブックというものをしっかりと紙で配ったり、最近はWeb上に公開して社員がいつでも見ることが可能にしております。月に１回、特に管理職がしっかりと、自分の部署のセキュリティ対策情報の確認を行う。基本的に業務で利用するパソコンやUSBメモリーなどの外部記憶媒体については社給のものを使うこ

図 2



とを義務づけております。個人所有のものは使用禁止という原則を貫いております。業務で利用するノートパソコンは内蔵のハードディスク全体を暗号化する。紛失しても中身を見ることができないようにしております。当然USB等も暗号化できるものを使用していく。業務で使用するPCについては、ファイル交換ソフト、これについてもインストールを絶対にしない。万が一インストールされていても、毎朝チェックツールが起動し、入っている場合にはアラームが出るという仕組みになっております。

ここまで企業としては最大限努力しております。それでも悪意を持って管理者が情報漏洩してしまえば防ぎようがないのが現状であると思います。なので、なかなかここまでやっても、実際問題どこまで情報管理を行うことができるかというのは、企業としては非常に頭の痛いところだと思っております。

最近よく話題になるのが従業員退職時の問題、当然秘密情報が転職先へ漏洩する恐れがあるということで、当たり前のことを行っているのですが、先ほどから髙部先生、田村先生からお話があったように、どこまで退職時

に契約の条件で情報漏洩を止められるのかというのは、職業選択の自由とも絡んで、なかなか難しい問題、ここは逆に言えば、他の企業の方々もどのように行っておられるのか、お話を聞きたいところです。当社としては誓約書の取得ぐらいがぎりぎりのところ、あとはたとえば退職という話になったら会社の情報を頻繁にダウンロードしていないかログを取って確認をしたり、可変版記憶媒体の使用を制限したり持ち出せないように制限をかけるのですが、基本的に退職する場合、技術者はほとんどが競合他社に転職するのが現状だと思います。他のまったく違う会社に転職するというのは、たとえばこういう知財の仕事や総務や経理の仕事であれば可能かもしれませんが、技術者は、たとえばデバイスをやっている技術者は絶対デバイスの技術を期待されて行くわけですから、その技術やノウハウをどこまで情報流出を抑えられるかというのは非常に頭の痛い問題だと思っています。

あと海外、特に中国というところでのビジネスでの問題です。中国のビジネスで日本企業単独ではなかなかやりにくいところがあって、合弁とかアライアンスというものをやっていく中で、日本の技術を非常に期待されております。当然技術情報の提供を行ったり、技術移転を行う。ところがやはり中国という国はご存じのように人材の流動化、それから流動化に伴う情報の流出というのが非常に問題になります。NDAを当然結んでいても、NDAはある意味保険みたいなもので、結局は持ち出されれば何の意味もなしません。よって情報管理として当然NDAは結ぶとしても、重要技術というものをブラックボックス化するとか、日本から持ち出さない、それから先ほどお話ししました現地での教育・情報管理の体制というものを徹底していかないと、なかなか解決できない問題だと考えております。

昨今特許と秘密情報という相反するところがあるのですが、特許で守るもの、ノウハウとして情報管理として守るものというものを明確化しなければならないと考えております。たとえば製造方法、先ほど方法のことが田村先生からも優先順位のお話の中に出ておりましたが、やはり製造方法も技術者としては、どうしても特許を出したいがために、特許を出してそれが公開されてしまい結局その製造方法を真似られてしまうというケースも出て来ておりますので、会社としても何を特許にして何を秘密にするのかという問題について今迫られているところがあります。

最後に、当社の問題だけでないと思いますが、最近、一社ではなかなかビジネスが回らない時代、特にオープンイノベーションと言われている時代、異業種の企業と組む、もしくはいろいろな場でいろいろな人が議論をし合う、その中でどこまで自分たちの秘密情報というのを出していいのか、それか出してはいけないのか難しい場面に出くわします。情報を出さないと何も生まれないし仲間が増えない。情報を出し過ぎると自分たちのノウハウが漏れてしまう。このバランスをどう取っていくのかというのが非常に頭の痛い問題でもあり、逆に言えば、そこをしっかり解決し、日本企業がまた復活していくようなことをやっていかないと、このオープンイノベーションの時代、企業の成長がなかなか難しいのではないかと思っております。

内容的には皆様の参考にならなかったかもしれません。国内企業ではどこでも実施されている内容だったかもしれませんが、今日は国内企業を代表してご説明をさせて頂きました。