Vol.2009-EIP-45 No.6
2009/9/12

情報セキュリティと契約責任

山本 将之
株式会社 ラック(LAC)
〒105-7111 東京都港区東新橋 1-5-2
汐留シティセンター11F

概要：情報セキュリティの重要性が社会的に認識され、対策が進んでいる一方で、情報セキュリティが阻害され、情報漏えいなどの事件・事故の発生も相次いでいる。
人的対策の一環として組織と従業員等との間で情報セキュリティに関する契約を締結する場合が多くある。しかし、それらの契約の性質、責任については、過去の情報セキュリティ事件・事故に関連した裁判等でも明らかにはなっていない。
そこで本稿では、裁判例や調査報告書などから情報セキュリティに関する契約がどのように扱われていたかを確認し、その契約の性質、責任の内容について検討する。

The Legal Liability of Information Security

Masayuki YAMAMOTO
Little eArth Corporation Co., Ltd.(LAC)
Higashishinbashi 1-5-2, Minato, Tokyo, Japan

Abstract：Today, importance of information security is getting to be known as a social matter, on the other hand, the number of information security incidents such as information leakage has increased.
In order to deal with human issues, employers and employees often make contracts related to information security.
However, the responsibilities in those contracts are not made clear from most cases such as judgmental cases.
This report will discuss the aspects of how the information security contracts were handled, and will examine the nature and responsibilities in those contracts by referring to past judgmental cases and investigation reports.

1. はじめに

近年、情報セキュリティの重要性が社会的に認知され、大手企業の多くではすでに基本的な対策が施されている状況にある。しかし、情報セキュリティを確保する上で最も重要な要素である、組織の役員や従業員（以下、「従業員等」という）が必ずしも情報セキュリティに関する規程に則って行動していないことも事実である。

このような状況を改善するため、従業員等に組織内の情報セキュリティに関する規程を遵守することを誓わせ、誓約書や機密保持契約書などを提出させる場合が多く見受けられる。

しかし、2009 年 4 月に発覚した証券会社社員による顧客の個人情報漏えい事件[1]などでは、誓約書を提出していたにもかかわらず、個人情報を持ち出し、名簿業

[1] 情報システム部の部長代理が 1,486,651 名分の顧客リストを不正にコピーした上、49,159 名分を名簿業者に 32 万 8 千円で売却した事件

者に売却していた事実がある[2]。

そこで本稿では、組織と従業員等との間で締結される誓約、機密保持契約の情報セキュリティに関する契約とその責任について、検討する。

2005 年の個人情報保護法施行に伴い、個人情報をはじめとして情報を適切に取扱うことが強く求められるようになった。また、プライバシーマークや ISMS の普及により、それらの認証取得が多くの企業で進んだ。

法令や規格には、従業員の監督や委託先の監督の一環として契約の締結をその要素として求めている。これらに準拠する形で、多くの組織では従業員等や委託先との間で情報セキュリティに関する契約を締結している場合が多い[3]。

しかし、先に述べた証券会社社員による顧客の個人情報漏えい事件をはじめ、誓約や契約を締結しているにもかかわらず情報が漏えいするなどの情報セキュリティ事件事故が多発している。

2. 情報セキュリティとは

情報セキュリティを確保するために、契約を締結するとしているが、そもそも情報セキュリティとは何であるかを確認する必要がある。

一般に情報セキュリティとは、機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）を確保することとされている[4]。以下、ISO27001 の定義を参考に機密性、完全性、可用性について各要素がどのような内容であるかを確認しておく。

(ア) 機密性(Confidentiality)

機密性とは、「認可されていない個人、エンティティ又はプロセスに対して、情報を使用不可又は非公開にする」こととされ、情報資産にアクセスできる人が正当に許可された人に限られていることをいう。

(イ) 完全性(Integrity)

完全性とは、「資産の正確さ及び完全さを保護する」こととされ、情報資産が完全な状態で保管、処理され、内容が正確であることをいう。

(ウ) 可用性(Availability)

可用性とは、「認可されたエンティティが要求したときに、アクセス及び使用が可能である」こととされ、情報資産へのアクセスを許可された者が、必要な時に、利用できる状態にあることをいう。

3. 契約の種類

情報セキュリティに関する契約は、情報セキュリティの各要素に対応した内容となる。そのため、以下に各要素の実効性を担保するために結ばれる契約を裁判

[2] 三菱 UFJ 証券 「業務改善報告書(抜粋)」

[3] このほか、経済産業省「経済産業分野に関する個人情報保護ガイドライン」においても、契約による保護を求めている。

[4] ISO/IEC27001 では、情報セキュリティの定義として、上記 3 要素のほかに、真正性、責任追跡製、否認防止及び信頼性などを含めても良いとされている。

例や調査報告書等から洗い出し、一般的にどのような内容が盛り込まれているかを確認する。

(ア)機密性

機密性に関する契約としては、機密(秘密)保持契約と総称される契約が挙げられる。一般に機密保持契約の内容としては、業務上知りえた秘密を外部に公開しないことを定めたものである。

前述の証券会社社員による個人情報漏えい事件では、人事部が社員から「誓約書」及び「情報セキュリティ管理に係わる確認書」の提出をうけており、守秘義務、守秘情報の業務外利用の禁止に同意している。

(イ)完全性

完全性に関する契約としては、システム構築の際のシステム開発委託契約が挙げられる。この契約は、注文者と開発者との間で結ぶ契約で、システムやソフトウェアを開発することを債務の本旨とし、さらにバグが含まれないよう開発することなどを定めたものである。

システム開発委託契約が完全性に関する契約としてとりあげた理由は、情報システムにバグが存在した場合、当該システムにより情報資産に誤った処理がなされ、正確さ完全さを担保できなくなるためである[5]。

(ウ)可用性

可用性に関する契約としては、Service Level Agreement(SLA)が挙げられる。

SLAでは、システムや通信の稼動が契約で定められた範囲を維持することをサービス提供者と注文者との間で取り決めたものである。

具体的には、遅延時間、障害発生通知などが含まれることが多い[6]が、当事者双方の合意により、盛り込むことの出来るサービスの内容は様々である。

これらの契約は、情報セキュリティの各要素によりその内容や項目が異なってくる。また、契約自由の原則により、機密性、完全性、可用性のすべての要素に関わる項目をひとつの契約に含めることが可能となる。

そのため、情報セキュリティに関する契約は民法が定める 13 種類の典型契約とは内容がことなることが多く、その性質や責任の範囲が不明確なものが多い。

そこで、次に契約の性質や責任の範囲について、特に機密性に関する契約を中心に検討していく。

4. 契約の性質

情報セキュリティの各要素に関する契約について、その性質や責任はまだ明確になっていない。そこで、それぞれの要素に基づいた契約について、判例を手がかりにその性質を検討する。

[5] 岡村久道「情報セキュリティと法律」(商事法務,2007,初版)p.234 には、システム開発委託契約は可用性を担保する契約の一種として扱われている。

[6] 経済産業省「SaaS 向け SLA ガイドライン」p.22

(ア)判例からみた機密保持契約

機密性保持契約に関する判例として、大きく分けて4つの事例に関する契約が存在する。1つ目は、契約の主体が組織とその従業員等である場合であり、この場合、就業規則、労働契約等の1項目として機密保持契約が含まれている場合である。

2つ目の事例は、契約の主体が組織と当該組織を退職した従業員等である場合である。

3つ目の事例は、契約の主体が組織の従業員等以外の者との契約である。多くの場合、コンサルティング業務やソフトウェア等の開発委託業務に関連し、締結される契約のなかに機密保持契約が含まれている。

4つ目の事例は、契約の主体が組織の従業員等以外の者との契約であるが、既に契約が終了している場合である。

本稿では、組織と従業員等の契約に関する代表的な判例をもとに、その契約をどのように捉えているか、確認する。

東京地判 平成15年9月27日
（メリルリンチ・インベストメント・マネージャーズ事件）

資産運用を主たる業務とする株式会社Yの従業員であったXが、自己に対するいじめ・差別的な処遇があるとして、その担当弁護士に企業の機密情報をYの承諾なしに開示・交付したことにつき、秘密保持義務違反等を理由として懲戒解雇処分に処された。

XがYに対して労働契約上の地位の確認を求めた事例において、裁判所は、「Xは、労働契約上の秘密保持義務を負っており、企業機密をYの許可無しに業務以外の目的で使用、第三者に開示・交付することは、特段の事 情のない限り許されないとしつつ、弁護士に守秘義務があること、開示・交付の目的が自己救済を目的としており不当とはいえない」として秘密保持義務違反を否定した。

大阪高判 平成6年12月26日
（高発泡ポリエチレン生産技術事件[7]）

Xは、Xの親会社が有する特許を実施するために設立された子会社であり、当該特許の専用実施権者である。X は中国企業と当該特許の輸出に関する交渉をしていたが、合意に至らなかった。しかし、交渉の責任者であるYがXを退社し、別会社を設立、X 在籍中に交渉していた中国企業と技術等の売却・実施許諾契約を成立させた。

XがYに対して特許情報がXの営業秘密にあたるとして、損害賠償を請求した。

これに対して裁判所は、「本件技術に関する資料は，すべて施錠された特別の書類箱に入れられ，その鍵は被控訴人が管理し，必要時以外には出さないようにされていた」ことから、不正競争防止法上の営業秘密にあたり、「輸出の相手方に本件技術につき守秘義務を課すことも行なって」いたことから、在職中に知りえた営業秘密の保持義務を引き続き負うとされた。

[7] 本件については、退職後の従業員等についても、信義則から一定の範囲で情報を保護しなければならないとされるが、その範囲は明確ではないとされる。

組織と従業員等の間で結ばれた情報セキュリティに関する契約は、典型契約のうちの雇用契約をモデルとした労働契約に一部分が追加されたものであるということができる。

5. 契約責任

前章では、判例を手がかりとして、機密保持契約の性質を確認したが、これらの契約は、典型契約の雇用契約を中心に機密保持契約をその一部とした契約であるということができる。そこで、次にこれらの契約により、契約の当事者が負う責任の内容について検討する。

雇用契約とは、「労働者が労働に従事することを約し、使用者が報酬を与えることによって成立する契約」である。

一般に、労働に関する契約には、4つのパターンがあり、その一つが人の労務そのものを目的とするもので、「労働者を指図して、一定の目的に向けて効果を発揮させる権能は使用者に属する」[8]とする契約である。

雇用契約の大部分は、労働基本法による修正が大きく加えられている。

労働契約は、当然のことながら労務の提供と賃金の支払いを基本とした契約であるが、使用者と労働者との信頼関係が根幹にあるといえる。

そのため、「相互の利益に配慮し、誠実に行動すべき付随的義務を負う」[9]とされ、明示的な合意がなくとも労働者の義務を認めるものであるとする考えもある。

では、その付随義務による従業員等の義務とは何かが問題となる。

付随義務が認められえる根拠としては、多数の労働者がともに就労することから生じる共同生活の必要性、使用者の財産を管理・保全することが必要とされる。

そのため、労働の履行に直接関係があるものが主たる付随義務の対象となると考えられる。さらには、使用者の財産を守ることも付随義務の一種といえる[10]。この使用者の財産を守ることが、従業員に対して機密保持契約を締結する上での根拠となっている。

従業員等が労働契約にある機密保持契約を履行しなかった場合に負う責任として、使用者による人事権の行使(懲戒[11]や解雇[12]等)、債務不履行又は不法行為による損害賠償責任[13]を負うこととなる。

債務不履行責任による損害賠償責任が認められるのであれば、債務不履行責任の一種として認められる債務の履行も当

---

[8] 我妻 栄「民法2 債権法」(勁草書房,2009,第3版)p.341
[9] 松本恒雄・升田純「情報をめぐる法律・判例と実務」(民事法研究会,平成15,初版)p.126
[10] 日本労働学会編「講座 21世紀の労働法 第4巻 労働契約」(有斐閣,2000, 初版)p.15においても同様の内容がある。
[11] 従業員等の懲戒処分に関する判例として、古川鉱業事件(東京高判 昭55年2月18日)が挙げられる。
[12] 従業員等の解雇に関する判例として、三朝電機事件(東京地判 昭43年7月16日)が挙げられる。
[13] 従業員等に関する判例として、美濃窯業事件(名古屋地判 昭61年9月29日)がある。また、役員に関する判例としては、ダイオーズサービシーズ事件(東京地判 平14年8月30日)がある。

然に選択肢として有りうるとしている[14]。

しかし、従業員等が機密保持契約を履行しなかったことにより、情報が漏えいし、組織外に拡散している状態となる。

Winny による情報漏えい事件などにおいて指摘されているとおり、漏えいした情報の流通を止め、回収することは困難であると考えられている。

そのため、機密保持契約に関しては、使用者が債務不履行責任による解除権、履行請求を行うことに意味はないといえる。

6. 情報セキュリティの確保を担保する機密保持契約

機密保持契約に関する契約について判例からその契約モデルを確認した。契約モデルとしては、労働契約の一部として機密保持契約が取り扱われている。

このとき、必ずしも書面により機密保持契約に関する取り決めが必要とされているわけではなく、労働契約の付随義務として従業員等の機密保持義務が認められる場合がある。

このような機密保持契約の特性を考慮し、情報セキュリティを確保・維持するために実効性をもつ内容とするため、以下の 3 点に注意を払う必要がある。

(ア)契約の形式

労働契約の付随義務として、機密保持義務を負うこととなるが、その内容を使用者と従業員等の間で確実に書面化することにより、機密保持契約の義務範囲を明確化することができる。

また、従業員等に対する情報セキュリティ教育などの際に、機密保持に関する書面に記載し、情報セキュリティについての意識を常に持ち続けてもらうといった手法も考えられる。

(イ)契約の期間

在職中の従業員等は、労働契約の性質もあり、継続的に機密保持義務を従業員が負うこととなるのに対して、退職した従業員等は、機密保持契約を結んでいない状況となる。

この点に関し、本稿では触れていないが退職後も一定の間、付随義務を負うこととなる。

(ウ)責任の内容

前章で確認したとおり、機密保持契約を従業員等が履行しなかったことにより負う責任の内容としては、使用者による人事権の行使と債務不履行責任又は不法行為責任による損害賠償請求である。

つまり、組織が機密として取り扱う情報が一度、漏えいした後はそれらの情報の利用を停止させたり、回収したりすることは困難である。そのため組織は、日ごろから情報セキュリティを確保・維持するための対策を実施することが重要となってくる。

7. 課題

情報セキュリティに関する契約、特に

[14] 菅野和夫「労働法」(弘文堂,平成 20 年,第 8 版)p.73 では、「根拠が明確であれば、履行請求も可能であると考えられる」としている。

機密保持契約の性質、責任の内容が明確になっていない。

そのため、すべての情報セキュリティに関する契約について、情報セキュリティを確保するために実効性のある解釈を行う必要があるが、セキュリティと利便性のトレード･オフが問題となるように、どのような解釈を行い、情報セキュリティに実効性をもたせるかが大きな課題として残る。

謝辞

本稿は、情報セキュリティとそれに関する契約責任を明確にすることを目的とした研究である。本研究を進めるにあたり、助言を頂いた関係者各位に感謝する。

なお、本稿における意見の部分はすべて筆者の個人的な見解・意見であって、所属する組織とは関係ありません。