弊社のセキュリティに関する取り組みと実例

浜田 浩史
伊藤忠テクノソリューションズ株式会社

概要：CTC グループでは、ISO27001 およびプライバシーマークに準拠し、情報セキュリティ・個人情報保護マネジメントシステムを構築して運用している。ここでは、企業がセキュリティをどのように考えているか、CTC 社員が日々どのようにセキュリティを意識しているかについて説明をする。

キーワード：情報セキュリティ、ISMS、教育

1. CTC の情報管理体制

CTC グループには、8000 名を超える社員が所属している。弊社では、ISO27001、そして、P マークに準拠し、ISMS のシステムを構築し、情報セキュリティに取り組んでいる。

組織体制としては、CTC グループ全体の ISMS を統括する責任者としてチーフコンプライアンスオフィサー（CCO）を「情報セキュリティ担当役員」としている。その下に、組織ごとに責任者を決め、情報セキュリティを守っていくという体制を作っている。各組織の情報管理リーダは、毎年新しいメンバーが任命されている（図 1）。

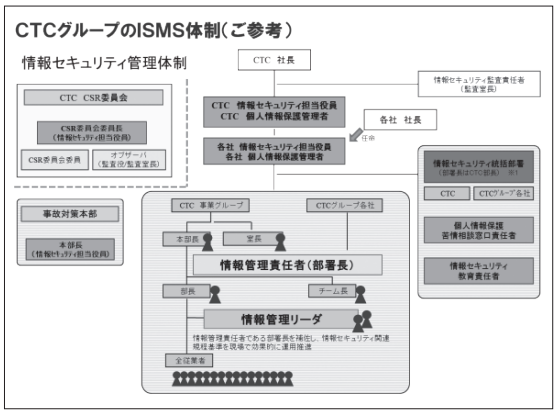

図 1　CTC グループの ISMS 体制

情報セキュリティの統括部署であるセキュリティ・工事管理部では、苦情の窓口や情報管理リーダや従業員への教育を担当している。

情報管理リーダは毎年変わるため、集合研修で教育を行っている。また、グループの全役員・社員に対して e ラーニングによる教育を年に 1 回実施している。さらに、CTC グループの行動基準や情報セキュリティ基本方針等、ルールや関連する規定等の文書は社員が閲覧できるポータルサイトに掲載している。

また、我々と共に仕事をしているパートナー会社にもセキュリティを守ってもらわないと、情報が漏えいした場合に問題になるので、必ず契約前に、委託先の会社や従業員が本当にセキュリティを守っているかをチェックシートに基いて確認し、情報セキュリティについての覚書等、セキュリティに特化した契約を別途締結してから、業務委託の契約を結ぶことになっている。

2. CTC 社員のセキュアな一日

弊社の社員がどのくらいセキュリティを意識して、日々の業務に当たっているかを、一日の行動から見ていく。

まず、朝出社すると、IC カードの社員証をかざしてオフィスの扉を開ける。次に、指紋または掌の静脈をかざす生体認証で第 2 扉を開けて、執務室に入る。なお、業務に利用するパソコンのログインパスワードは、3 か月おきに変更を求められる。始業前の 8：55 には、館内放送で、セキュリティ向上についての声掛けが流れるようになっている。この館内放送は、セキュリティについての啓蒙活動を毎日行うことで、従業員にセキュリティ

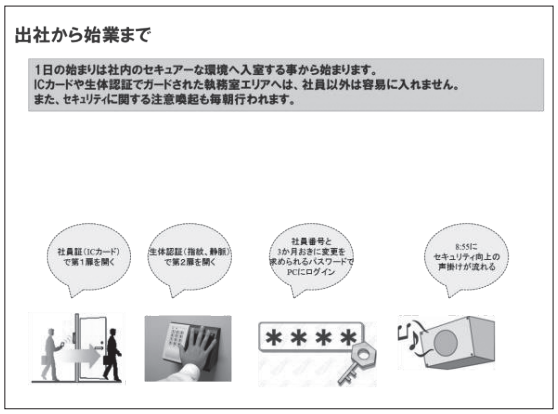

図 2　出社から始業まで

の意識を少しでも持たせる目的がある（図2）。

電子メールに関しては、システムで守られている部分と、人で守られている部分に分かれている。システムで守られている部分としては、外からウイルス付きのメールが送られてきた場合に、全てウイルスチェックソフトによって無効化されてユーザに届く。また、社内から添付ファイル付きのメールを外部に送る際には、宛先と添付ファイルに間違いがないかどうか確認を促す画面が表示され、確認後送信ボタンを押しても、すぐには送信されない。送信されるまで10秒間の合間があり、その間に間違いに気づけばメール送信をキャンセルすることもできる。また、添付ファイルにパスワードをかけないと、送信されない。

添付ファイルのパスワードについては、以前は添付ファイルとは別のメールで相手に知らせるようにというルールだったが、その別のメールも宛先を間違えていると意味がないため、今では、パスワードは事前に取り決めておくこととしている。これは、システムではなく利用者が運用で注意している部分である。

また、人的に注意してガードしている点としては、宛先が合っているか、添付するファイルが間違っていないかということを、指さし確認をすることとしている。さらに、重要な内容や宛先の場合は、二人以上でダブルチェックを行っている。

書類については、鍵のかかったキャビネットに保管されている。また、機密性や完全性、可用性に応じて管理レベルを設定し、管理台帳に記入している。そして、廃棄についてのルールも設定し、不要な書類は書類専用の廃棄BOXに入れて廃棄している。

社外への書類の持ち出しにもルールがあり、機密情報が含まれた書類を持ち出す場合は部長の承認が必要だ。社内の他オフィスに行く場合は、シンクライアントを利用してシステムで共有されたファイルを使ってプレゼンテーションを行うことにより、極力書類を持ち出さないようにしている。

そして、パソコンについては、用途に応じて3種類に分けられている。都度必要な情報のみ格納し利用後に削除する社外への持出し専用のPC、社外への持出しは一切できない持出禁止のPC、記憶装置を持たず、インターネットで社内環境に接続して利用するPCがある。このように使い分けることで、極力情報が外に漏れないようにしている。

勤務時間が終わり、退社時には、書類等は施錠できるキャビネット等にしまうことになっている。退社時に重要書類を社外に持ち出すことは禁止されている。

しかし、気をつけていても、セキュリティ事故が起こってしまうこともある。最も重要なことは、起きてしまった時に、必ず関係各所に連絡することだ。連絡が遅れると、後からの方が大きな問題になってしまうことも多い。

3. 最後に

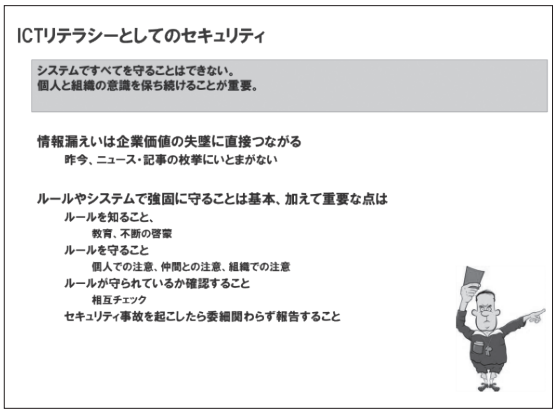

図3　ICTリテラシーとしてのセキュリティ

情報漏えいは、企業価値の失墜に直接つながるもので、企業にとって大きなリスクである。会社としてシステムやルールを整備することは基本であるが、加えて重要なのは、ルールを知ること、ルールを守ること、ルールが守られているかを確認することである。この3つがそろって初めてセキュリティが守られていると言えるだろう。

しかし、どんなにシステムやルールがしっかりしていても、セキュリティ事故がゼロになることは難しい。一人一人が日々心を新たにしてセキュアな一日を過ごしていくことが重要である。