8　アナログ犯罪への対応

(1) 増加するアナログ犯罪

インターネットを利用した様々な取引は利便性も高く、今後ますます普及していくことは確実であると思われる。サービス提供者側も、利用者側も、インターネットの特性を理解し、正しいセキュリティ上の対策を行うことで、安心で安全な取引が行えるということが広く認知されるようになってきている。

しかしながら、サービス提供者側、利用者側のセキュリティレベルが上がったことで、システム上のセキュリティ対策では防ぐことのできない「アナログ犯罪」と言われる事例も発生している。

最近発生した「アナログ犯罪」の事例では、インターネットバンキングに申込を行うことで還付金がもらえるという詐欺がある。犯行の手口は、市役所、年金保険センター、保険会社などの名前を騙り、「保険金（年金）が還付されるので、必要書類を送付する」という電話がある。後日、実在する金融機関のインターネットバンキング開設申込書が送付される。被害者が申込を行い、契約手続きが完了する頃を見計らって、再度、犯人から「還付の手続きのため、ID やパスワードの情報が必要なので教えて欲しい」といった電話があるという。犯人は、聞き出した正しい ID とパスワードでインターネットバンキングにアクセスし、口座から預金を不正に引き出してしまうという事例である。被害者の多くは、情報リテラシーが低い高齢者である。

(2) 利用者への教育、啓蒙

上記のような「アナログ犯罪」では、ID やパスワードを技術的手段によって不正入手するのではなく、本人から直接に聞き出してしまうために、システム的な対応が取りづらい事例といえる。

銀行では、このような事例に対処するためには、利用者への教育、啓蒙が必須ということで、銀行サイト上で犯罪事例を公開し、その対策をわかりやすく説明することや、パンフレットの配布など行っている。

全国銀行協会でも「銀行とりひき相談所」を開設し、不審な電話や訪問があった場合の相談窓口を開設している。

インターネット犯罪に付随して発生するこのようなアナログ犯罪にも、今後十分に注意を払う必要がある。