# 第110回月例研究会報告

１．日時：2005 年１月25 日（火）18：30 ～ 20：30
２．場所：中央大学駿河台記念館520 号会議室
３．演題：「サイバー犯罪の現状と情報セキュリティに関する警察の取組み」
４．講師：警察庁　生活安全局　情報技術犯罪対策課　係長　間仁田　裕美　氏

（報告者：No.1449　平　真寿美）

１．講演要旨

サイバー犯罪の現状と情報セキュリティに関する警察の取組みについて、次の５テーマで事例を交え、課題・問題点・方向性等を講演された。

①サイバー犯罪等の現状、②情報セキュリティに関する政府の取組み、③法制面の整備、④情報セキュリティに関する警察の取組み、⑤国際的な連携。

(1) サイバー犯罪等の現状

サイバー犯罪は、従来「ハイテク犯罪」と称されてきたが、国際的動向にあわせ警察庁では、「情報技術を利用する犯罪」として、不正アクセス禁止法違反、コンピュータ・電磁的記録対象犯罪、ネットワーク利用犯罪、の３種類に分類して対策を進めている。

平成15 年度末現在インタネットの利用者は7730 万人、人口普及率は60.6％となり、それに伴いサーバー犯罪も増加している。犯罪検挙事例や相談件数増、検挙数の右上リの増加、ネットワーク利用犯罪の占める割合の多さ（1849 件のうち約89%）等で示すことができる。さらに、コンピュータウイルス、DOS 攻撃、インターネット・カフェの悪用、フィッシング、これらによる個人情報漏洩も多く発生しており（事例を紹介）、それら事案への注意点・対策、相談窓口を述べる。行政・民間部門の情報セキュリティ対策の現状を見ると、業種によるバラツキはあるものの、情報セキュリティポリシーに規定しているとおりにセキュリティ教育や監査を実施している事業体は、半数以下であるのが実情である。

(2) 情報セキュリティに関する政府の取組み

平成12 年11 月成立の「高度情報通信ネットワーク社会形成基本法（IT 基本法）」に基づくIT 基本戦略（e－japan 戦略・戦略）の中のセキュリティ関係施策で説明する。
今後の施策の柱は、「高度情報通信ネットワークの安全性及び信頼性の確保、個人情報の保護」の基本方針の下、政府部内の情報セキュリティ対策、重要インフラのサイバーテロ対策、制度・基盤の整備、人材育成、である。政府部内の情報セキュリティ関連体制（内閣総理大臣を本部長とする「高度情報通信ネットワーク社会推進戦略本部」に属する情報セキュリティ対策推進会議・情報セキュリティ対策推進・情報セキュリティ専門調査会や内閣官房のIT 担当室・情報セキュリティ対策推進室など）において、行動計画・アクションプランで具体化している。

(3) 法制面の整備

法制面は、セキュリティ対策関連法として、「不正アクセス行為の禁止等に関する法律（不正アクセス禁止法）」、及び「出会い系サイト規制法」で整備状況を示す。
不正アクセス禁止法は、不正アクセス行為の定義、行為の具体例、都道府県公安委員会の関り（アクセス管理者への助言・指導、事例分析、手口・原因解明）を内容とする法律である。過去４年間の不正アクセス行為の発生状況（認知件数と検挙件数）からは、検挙事件数の増加が右上リ（平成12 年から、31，35，51，58 事件と増加）であることがわかる。

出会い系サイト関係では、不正誘引事件の例を３件（女子中学生に対する援助交際の誘引、中学生に対する猥褻行為の誘引、13 歳以下への不正誘引）示す。検挙数は同様に右上がりで、特に平成14 年は前年888 件が1733 件と大幅に増加した。約半数が児童買春・児童ポルノ法違反である。

(4) 情報セキュリティに関する警察の取組み

警察の取組を次３点から紹介する。
①体制：警察庁は、情報技術犯罪対策課及び、情報技術解析課・技術センタが主体となって、都道府県警察のサイバー犯罪プロジェクトと連絡・調整・指導、技術支援などにより、犯罪取締り・広報啓発・産業界等との連携・サイバーパトロール・犯罪相談対応など、を行っている。

②サイバー犯罪の特長：捜査上の問題点でもあり、匿名性・無痕跡性・被害者の不特定多数性・地理的／時間的無限定性があり、国境・時間をこえ、いつでも痕跡を残さず不特定多数に被害が及び、対策は、喫緊の課題である。
③対策推進の面：「警察庁情報セキュリティ政策体系―2004」に基づき、体制整備と取り締まりの強化、産業界との連携強化、広報啓発の推進、外国関係機関との連携強化、サイバーテロ対策、を実施している。サイバーテロ対策について紹介すると、その目的は、発生の未然防止、被害拡大の防止、事件の検挙であり、そのためにサイバーフォースを創設し、重要インフラを支える官民の各事業体と連携して対応している。
　ネットワークは、社会・経済活動の根幹であり、全世界に構築されたインフラであるから、官民が連携して安全性・信頼性を確保する必要があり、そのめに、各種協議会等で産業界との連携体制も強化している。

(5) 国際的な連携
　国際連携としては、
・過去のG ８（サミット）で合意された政府間のハイテク犯罪に関する行動計画・原則・対策の実施。
・産業界との連携についても、G ８において、官民合同の会合、ワークショップで各国において産業界と政府の対話と連携を深める必要性を合意した。
・欧州評議会における「サイバー犯罪に関する条約」（実体法、手続法、国際協力の３部分から成る）が2004 年７月に発効し、日本は条約締結に向け、国内法の整備（ 刑法、刑事訴訟法、電波法、児童ポルノ禁止法、有線電気通信法、不正アクセス禁止法などの改正である）を進めている。
などにより、国際にも整合した対応を実施中である。

２．質疑応答
　以下、活発な質疑応答があり、終わりに講師に満場の拍手で御礼した。
１）スパムメールの取り締まり対策、対象などは？
⇒　迷惑メールの１つとして対応している。警察庁は迷惑メールの改正研究会に参加している。
取り締まり強化策として、経済産業省の、特定商取引法の規定（メールに広告表示）実施上守られていないことを受け、運用を強化する、経産省に（問題）受付部署を設け、悪質な者を警察に届けるなどを、検討中である。

２）サイバーテロは「不正アクセス禁止法違反」、「コンピュータ・電磁的記録対象犯罪」、「ネットワーク利用犯罪」の３類の中で、どういうものとして対策を考えているか？
⇒　定義はない。重要インフラ、社会的に影響が大きい犯罪として、その抑止、早急な対策を推進中。

３）サイバー犯罪捜査において、企業の協力（ログ、機器の提供等）は任意か強制か？
⇒　事件が起こった（被害がある）ので捜査する、となって令状があれば（取得、差押などは）強制であるが、兆候が見える場合等に、協力依頼を行うことがあり、これは任意。

４）サイバーパトロールは、情報収集が活動の中心と理解したが、パトロール中に警告を発するなどもあるのか？
⇒　違法情報や社会的に有害な情報など（が発信されていたら、）の場合であるが、違法を発見すれば取締まる、社会的有害な情報は、管理者に話をする（が、これは、法律に基づく警告とはいえない）。

５）「脆弱性の公表」で立件された例があるが、これへの考え方を伺いたい。
⇒　公表したことが悪質ではなく、不正アクセスの手口を実践したことが違法である。脆弱性に関しては、IPA，経済産業省が受付を行う制度がある。

６）情報窃盗について、情報は財物ではないので、窃盗罪にならない、となっているが、法的な対応はどのくらい進んでいるのか。所管など現状について、コメントをいただきたい。
⇒　当初窃盗罪の対象である財物として、刑法での対象化が検討されたが、刑法改正時に、範囲の設定などの困難があったので、見送られた。
他の法律、例えば不正競争防止法の改正（企業秘密の防衛強化）で企業の情報窃盗に対応しているが、

企業外については、未だ検討段階である。
所管官庁であるが、刑法は法務省、不正競争防止法は経済産業省、その罰則に基づく取締りは警察庁、行政処分ならそれぞれの主管官庁となる。

７）個人情報保護法では、個人情報保護の強化が求められているが、合理的な安全対策について検討されているのか？
⇒　業界からの相談は多い。各省庁のガイドラインに基づいた保護を行っていただきたい。なお、各省庁は横断的なコミュニケーションも行っている。

８）「警察庁情報セキュリティ政策体系―2004」は、中身もわかりやすいものとなっているが、警察庁自身のセキュリティ対策の中で、セキュリティ監査への取組みを紹介いただきたい。
⇒　各省に横断的な対策は、内閣官房でセキュリティ基準を策定する。
それ以外は、独自基準を作り一定間隔で監査を実施することになる。
警察のシステムは、一定以上のセキュリティレベルを保持する必要があるため、独自基準を策定し、監査に取り組んでいる。

３．所感
振込め詐欺、架空請求、カード盗難による２次被害など、身近に日々報道されるサーバー犯罪について、取締側から見た状況・対策を、政策面を中心に多面的・広範囲に説明いただき、システム監査を行う上で、参考とすべきことが多く意義深いものであった。
犯罪の事例や各種統計資料の数値等で、その増加傾向を実感するとともに、瞬時に世界中と繋がるインフラの下では、性善説を前提とした安全神話の維持が困難になってきた現状が実感できる。
システム監査人としての立場からは、「インターネット・カフェ等を利用する場合の注意点」や、「サイバー犯罪の特長＝捜査上の問題点」に挙げられている事項に対し、『システムそのものに、なんらかのガードがかかっているか』の視点で監査することが必要なのではないか、と考えさせられた。

以上