

## ハイテク犯罪の現状と課題

警察庁生活安全局セキュリティシステム対策室

宮城直樹

ネットワーク利用犯罪、不正アクセス、電子計算機・電磁的記録対象犯罪といった「ハイテク犯罪」の現状について解説をするとともに、いくつかの事件例に即して現行のシステムの問題点を指摘する。また、MS BLAST の蔓延の際における関係者の対応について概説し、今後の対応についての方向性を探る。

High-tech Crime - Current Status & Countermeasures  
Security System Planning Office National Police Agency

Naoki Miyagi

I'm going to explain about current status of "High-tech crime" -Internet Crime , Violation of the Unauthorized Computer Access Law and Crime against Computer/Data ,and point out the problems of present system in case of some incidents. Moreover, outline the correspondence of the persons concerned in the case of spread of MS BLAST , and explore the directivity about future correspondence.

### 1-1 警察におけるハイテク犯罪の分類

いわゆるコンピュータに係る犯罪をどのように呼称するか、その内容をどのように分類するかは、論者の立場により様々であるが、その捜査、取締りを行う警察においては、これらの犯罪を「ハイテク犯罪」と呼称し、これをさらに「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」及び「ネットワーク利用犯罪」に分類している。

### 1-2 「不正アクセス禁止法違反」

「不正アクセス禁止法違反」とは、不正アクセス行為の禁止等に関する法律第8条第1号に掲げる罪（不正アクセス）及び第9条に掲げる罪（不正アクセスの助長）をいう。

法の禁止する行為の大体のイメージがつかめる程度に「不正アクセス」とはどのような行為であるかについて述べると、「電気通信回線に接続された電子計算機であってID・パスワードによりその電気通信回線を通じた利用ができる者を管理しているもの（電子計算機）に対し、電気通信回線を通じて、そのID・パスワードを窃用し、又はセキュリティホールを利用してアクセスする行為」となる。

ここで「電気通信回線」とはインターネットの外、LAN等も含むものであり、例えば社内LANにおいて他人のID・パスワードを窃用してサーバにアクセスする行為も不正アクセスに該当する。一方、不正アクセスは電気通信回線を通じて行われるものに限られていることから、いわゆるスタンドアローンの電子計算機に不正にアクセスする行為は、不正アクセスに該当しない。

### 1-3 「コンピュータ・電磁的記録対象犯罪」

「コンピュータ・電磁的記録対象犯罪」とは、刑法においてコンピュータ・電磁的記録に関し定められた罪をいう。

具体的には、「電磁的記録不正作出（刑法第161条の2）」、「電子計算機損壊等業務妨害（刑法第234条の2）」、「電子計算機使用詐欺（刑法第246条の2）」及び「電磁的記録毀棄（刑法258条及び259条）」をいう。

「電磁的記録不正作出」は電磁的記録に対する文書偽造に相当する行為であり、「電子計算機損壊等業務妨害」は電子計算機上で行う業務妨害に相当する行為である。

「電子計算機使用詐欺」とは、電子計算機そのものに対し虚偽の情報又は指令を与え、あるいは電子計算機に虚偽のプログラムを実行させるなどの方法で財産上不法の利益を得る行為等をいう。電子メールやウェブページを用いて人を欺き金銭等を詐取する行為、（他の方法で人を欺いた上、）インターネットバンキングを用いて財産上の利益を受け取るなどの行為は、「電子計算機使用詐欺」ではなく、「詐欺」に該当する。

「電磁的記録毀棄」とは、電磁的記録に対する文書毀棄に相当する行為をいう。

### 1-4 ネットワーク利用犯罪

「ネットワーク利用犯罪」とは、犯罪の構成要件に該当する行為についてネットワークを利用した犯罪又は構成要件に該当する行為ではないものの犯罪の感光に必要不可欠な手段としてネットワークを利用した犯罪をいう。

いわゆる出会い系サイトを利用した買春、電子掲示板を利用した脅迫、名誉毀損、ウェブサイトにおけるわいせつな画像の陳列、ストレージサービスを利用した著作権の侵害等の行為がこれに当たる。

## 2 ハイテク犯罪の検挙状況

最近におけるハイテク犯罪の検挙状況は次の表のとおりである。

	H12	H13	H14		H15	増減
			上半期	上半期		
不正アクセス禁止法違反	31	35	51	27	33	8
コンピュータ・電磁的記録対象犯罪	44	63	30	18	31	13
電子計算機使用詐欺	33	48	18	12	19	7
電磁的記録不正作出・毀棄	9	11	8	5	9	4
電子計算機損壊等業務妨害	2	4	4	1	3	2
ネットワーク利用犯罪	484	712	958	443	468	25
児童買春・児童ポルノ法違反(買春)	8	117	268	114	105	-9
"          (ポルノ)	113	128	140	64	55	-9
詐欺	53	103	112	59	44	-15
わいせつ物頒布等	154	103	109	55	39	-16
青少年保護条例違反	2	10	70	25	49	24
脅迫	17	40	33	18	21	3
著作権法違反	29	28	31	16	20	4
名誉毀損	30	42	27	13	26	13
その他	78	141	168	79	109	30
合          計	559	810	1,039	488	532	44

(注) 不正アクセス禁止法は平成12年2月13日の施行であり、平成12年中の同法違反の数字は、施行日以降のものである。

ハイテク犯罪の検挙のうち大きな割合を占め、かつ、その数が急増しているのは、ネットワーク利用犯罪である。中でも増加が著しいのは、児童買春と青少年保護条例違反(青少年とのみだらな行為等)であるが、これらのほとんどは出会い系サイトにおいて発生しているものである。また、詐欺も増勢にあるが、これらの多くはインターネットオークションや電子商取引を舞台として取行されている。

不正アクセス禁止法違反も増加しており、その態様も、インターネットの接続環境の変化やインターネット上で提供されるサービスの拡大に伴い、法施行当初に目立っていた他人のID・パスワードを窃用してインターネットに接続するといったものから、ウェブサイトの改竄、メール等の盗み見、ネットオークションの不正入札、さらにはオンラインゲームの不正操作と多様さを増してきている。

一方、コンピュータ・電磁的記録対象犯罪はおおむね増勢にあり、その中では電子計算機利用詐欺が多くを占めている。

### 3 ハイテク犯罪等相談受理状況

最近における警察のハイテク犯罪等相談受理状況は次のとおりである。

分類例	H12	H13	H14	H14(上)	H15上	前年同月比
詐欺、悪質商法等による被害に関するもの(インターネットオークション被害に関するものを除く)	1,396	1,963	3,193	1,331	8,776	+ 7,445
インターネットオークション被害に関するもの	1,301	2,099	3,978	1,495	2,309	+ 814
名誉毀損・誹謗中傷・脅迫による被害に関するもの	1,884	2,267	2,566	1,229	1,349	+ 120
不正アクセス・コンピュータウイルスに関するもの	505	1,335	1,246	693	506	-187
迷惑メール・スパムメールによる被害に関するもの	1,352	2,647	2,130	1,180	1,246	+ 66
違法有害なホームページ・掲示板等の通報、取締り要望に関するもの	2,896	3,282	2,261	1,176	2,605	+ 1,429
その他	1,801	3,684	3,955	1,988	2,306	318
計	11,135	17,277	19,329	9,092	19,097	10,005

ハイテク犯罪の検挙状況が主として警察の捜査活動の状況を表しているのに対し、相談等の受理状況は国民がいわゆるサイバー空間の在り様についてどのような不満や不安を感じているかの一つの指標となるものである。

平成15年上半年期に詐欺・悪質商法に関する相談が急増しているのは、不特定多数の者に対してインターネット上の有料コンテンツ使用料名下に金銭を請求する電子メールを送付する事案が多発したことによるものであり、この影響を除いてみると、インターネットオークション被害に関する相談の増加が著しく、次いでインターネットオークション被害を除く詐欺・悪質商法に関する相談、名誉毀損・誹謗中傷・脅迫による被害の増加が目立っている。

#### 4-1 個別事例から引き出される問題

2及び3で述べた検挙状況及び相談受理状況等を踏まえ、国民生活の安全の確保等の観点から留意されるべき事項のうちいくつかについて概説する。

#### 4-2 いわゆるファイル交換ソフトをめぐる問題

いわゆるファイル交換ソフトは、インターネット上の情報伝達、情報共有等における新たな可能性を秘めた興味深い存在と考えられるが、我が国では現在のところ、これを巡っては、わいせつ物関連事犯のほか、著作権等侵害事犯が目立っている状況にある。

警察においては、こうしたソフトを用いた事犯等について検挙を行っているが、常時接続環境の整備、回線の高速化に伴って、匿名性の高いいわゆる Freenet 型のファイル交換ソフト(サーバの機能を果たす特定のコンピュータを必要としないファイル交換ソフト)の利用が急速に拡大しつつあり、これによるわいせつ物関連事犯、著作権等侵害事犯の多発が懸念されるところである。また、こうしたファイル交換ソフトの利用、とりわけ動画等のサイズの大きいファイルの交換のための利用が、インターネットのトラフィックに与える影響も無視できない段階にきている

とされており、インターネット全体の安定性の確保の観点からも関係者の適切な対処が望まれる。  
さらに言えば、著作権等侵害事犯については、いわゆるストレージサービスを利用して敢行される場合も出てきており、これについても関係事業者等の適切な対処が望まれる。

#### 4-5 コンピュータ（端末）等の共用をめぐる問題

警察においては、いわゆるインターネットカフェにおいてコンピュータにキーロガーをインストールし、これによってインターネットバンキング等を行う者のID・パスワードを探知し、不正アクセスさらには詐欺等を敢行した事案を検挙している。

インターネットカフェを始めとして、一のコンピュータを不特定多数の者が共用する例は多い。キーロガーのインストールのようにID・パスワード等を盗み見ようとする意図が明白な場合はもとより、ブラウザの閲覧履歴保存機能、入力のオートコンプリート機能、パスワードの保存機能等に係る設定に当たり十分な配慮をしていなかったためにID・パスワードが第三者に漏れてしまう例もみられるところである。

利用者にあつては、こうした共用のコンピュータをインターネットバンキングその他の重要な事項の入力を伴うような態様で利用する際にはできるだけ慎重を期することが望まれる。

また、コンピュータを不特定多数の者に利用させる事業者等にあつては、不適切なソフトのインストールを防止するための措置をとるとともに、今述べたブラウザの閲覧履歴保存機能等の適切な設定、利用終了毎のリカバリの実施等の取組が望まれる。

#### 5 MS BLASTの蔓延の際の関係機関の対応

本年8月のMS BLASTの蔓延の際の関係機関・団体の対応状況は次のとおりである。

- 7. 16 OSベンダがMS03-26を公表
- 7. 17 @police(警察)がMS03-26に関する情報提供
- 7. 22 CERT/CCがMS03-26に関する情報提供
- 7. 23 セキュリティベンダがMS03-26に関する情報提供
- 8. 5 @policeがTCP135番ポートへのアクセス急増の警告
- 8. 12(午前2時にTCP135番ポートへのアクセスが激増)
  - 07:00 ワクチンベンダがMS03-26を利用したワームの蔓延の警告
  - 08:00 @policeがMS03-26を利用したワームの蔓延の警告
  - 10:30 OSベンダ等3社がMS03-26を利用したワームの蔓延の警告
  - 12:46 IPA/ISECがMS03-26を利用したワームの蔓延の警告
  - 18:00 @policeがワームの感染方法、動作を解析し、警告
- 8. 13
  - 午後 各紙がMS Blastについて報道

Windows の脆弱性が発表された7月16日から半月後の135番ポートへのアクセスの急増からわが国のコンピュータへの感染が始まった8月12日までの期間、そして8月12日午前2時から企業等の始業までの時間、この時間に国民に広く注意喚起ができなかったことが、わが国においてMS BLASTの蔓延を許してしまった一因と考えられる。

どのようなタイミングで、どのようなメディアを用いて、どのような事項を国民に伝えることが被害を最小化するのかについて、我々は検討を進めている。

そこでは、マスメディアを始めとした他のメディアの利用、ユーザーからの相談の窓口の在り方等多角的な論議が行われる必要がある。