資料編Ⅰ

（諸外国における産業界等との連携の現状等に関する調査）

目次

Ⅰ　調査の概要

１．調査の背景と目的

情報通信ネットワークの普及・発展に伴い、電子商取引、行政情報の提供、住民基本台帳ネットワーク等重要な社会経済活動が情報通信ネットワークへの依存を高めており、サイバースペースにおける安全が確保されないと、社会経済活動の根幹を揺るがしかねない危険性をはらんでいる。匿名性、無痕跡性、地理的・時間的無制約性というネットワークの特性は、ハイテク犯罪の防止や捜査を困難なものとしており、産業界等が発展させてきた情報通信インフラであるネットワーク上の治安を良好に保つための法執行活動等においては、産業界等との連携が重要になっている。産業界等との連携の重要性は、平成 9 年のＧ８司法内務閣僚会合で合意され翌年のバーミンガム・サミットでその推進が合意された「ハイテク犯罪と闘うための原則と行動計画」でも指摘されており、これを受け、平成 13 年 5 月には、Ｇ８各国による政府と産業界等とのハイレベル合同会合が東京においても開催されたところである。我が国政府としても最重要課題の一つとして e-Japan 重点計画（平成 13 年 3 月 29 日 IT 戦略本部決定）に警察が産業界等との連携を強化することを盛り込み、これを受けて警察において産業界等との連携を深めるための施策を推進しているところである。

警察庁においては、情報セキュリティに関する産業界等と政府機関との連携の在り方、特に警察との連携の在り方について検討を行うため当会議を設置したところであり、諸外国における法執行機関と産業界等との連携の現状等について好事例を把握することで、今後の産業界等との連携に関わる施策の検討に活用するため、本調査を行った。

２．調査の方法

本調査では、法執行機関と産業界等との連携を先進的に行っている米英独仏 4 カ国について、産業界（電気通信事業者（ISP）、Web コンテンツ事業者、情報機器メーカー、オペレーティングシステム事業者等）や官公庁、市民団体等を対象として、各国 6、7 件の聞き取り調査を実施した。

なお、本調査結果は、あくまでも聞き取り調査に基づき作成したものであり、事実確認等を経ていない場合もあることに留意されたい。

調査対象カテゴリー

＜電気通信事業者＞

- ISP （含 ISP 団体加盟企業）
- ISP 団体

＜Web コンテンツ事業者＞

- Web コンテンツ企業
- コンテンツプロバイダー団体

＜情報機器メーカー＞

- 情報機器メーカー
- 情報機器メーカー団体

＜オペレーティングシステム事業者＞

- OS 事業者

＜官公庁＞

- 政府機関（連邦政府機関）
- 地方自治体

＜市民団体＞

- 市民団体
- 公益団体
- 消費者団体

＜その他＞

- 州警察

３．調査の内容

(1) 法執行機関との連携状況

①情報セキュリティに対しての認識

②セキュリティ対策のための体制

③情報セキュリティ確保のための対策及び対応

○サイバー攻撃発生時の産業界等における連絡・連携体制

・連絡・連携体制の構築の状況及び手段

・共有する情報の種類

・緊急時対応計画の策定状況

○違法・有害情報発見時の対応状況

④法執行機関との連携の状況

○サイバー攻撃の発生情報の警戒や緊急対処に必要な情報の入手方法

・情報セキュリティポータルサイトの実態

・法執行機関との情報の共有の実態

○ハイテク犯罪捜査を迅速かつ円滑に実施するための産業界等による法執行機関への協力の現状

・犯罪捜査に必要な情報（ログ、個人情報等）の提供

⑤産業界における連携の状況

⑥人材育成

○情報セキュリティ対策に携わる人材育成の推進状況

・法執行機関、産業界等が実施している人材育成のための方策

○国民の情報セキュリティを向上させるために法執行機関、産業界等で推進する対策の現状

・ハイテク犯罪に関する相談窓口

・教員、児童生徒等学校教育関係者、地方自治体職員等の情報セキュリティ意識を向上させるための方策

(2)産業界等の法執行機関に対する要望及び法執行機関の取り組みの評価

○産業界等と法執行機関との連携の取り組みの現状と評価

○産業界等と法執行機関とが協力して実施すべき施策

II　米国

１．情報セキュリティに対しての認識

情報セキュリティが自社の事業に直接関わる ISP（Internet Service Provider）やメーカー等の企業以外では、これまで情報セキュリティについてはあまり注意が払われてこなかったが、近年になってハッカーやコンピュータウイルス、DoS 攻撃等の被害が多く出たことなどから、情報セキュリティに対する認識が高まってきたところである。

２．情報セキュリティ対策のための体制

情報セキュリティが自社の事業に直接関わる企業では、情報セキュリティ対策のための専門部署が設けられている。例えば、世界的に事業を行っている ISP では、主要国にコンピュータウイルス等の発生・広がりに対応するサイバーアタックチームが置かれている。また、顧客向けの連絡・情報提供窓口を置いている企業もある。

こうした専門的な部署以外に、経営陣が参加するセキュリティグループを擁する企業もある。この企業では、COO（Chief Operating Officer 最高執行責任者）、CTO（Chief Technology Officer 最高技術責任者）等がネットワークセキュリティのリーダーとともに週１回のミーティングに参加し、セキュリティに関わる事項での意見交換、経営方針の検討などが行われている。

■情報セキュリティ対策のための体制について

○IDC（Internet Data Center）事業者としては、オペレーショナルセキュリティが一番の優先事項である。世界規模でのコンピュータウイルス感染が発生した場合には、ウイルスが米国に入る前に検知し、それを防ぐ必要がある。そのため、主要国にはサイバーアタック対応チームを用意している。（ISP 団体加盟企業）

○経営陣が参加するセキュリティグループを設けている。COO、CTO、ネットワークセキュリティのリーダー等が参加し、毎週、最新の脅威やセキュリティ対策について意見交換を行い、経営方針やポリシーをたてている。経営レベル以外に、海外を含めてセキュリティ対策を行う部署がある。（Web コンテンツ企業）

○社内ネットワーク及びサービス提供をしているネットワークなど全てを管理する情報セキュリティ部隊がおり、アクセスのモニタリングや最新技術の動向をチェックしている。また、顧客や当社のネットワークに対する攻撃やソフトウェアのバグなどを追跡している組織がある。（OS 事業者）

○情報セキュリティの担当者はいたが、彼らを取りまとめるスキルのある人物がいなかったので、情報セキュリティの責任者を外部から雇った。（地方自治体）

3．情報セキュリティ確保のための対策及び対応

3.1 事前対策（予防）

ここでは、コンピュータウイルスや不正アクセス、DoS 攻撃といったネットワークへの攻撃を事前に防いだり、攻撃を速やかに察知したりするために、実施されている対策についてまとめた。

3.1.1 情報セキュリティ対策

コンピュータウイルスや不正アクセス、DoS 攻撃といったネットワークへの攻撃に対する事前の対策（予防）として、FW（FireWall）、ウイルス検知、ネットワークのモニタリングといった通常の対策のほかに、セキュリティ関連サイト等による情報収集や企業間での情報交換などが行われている。また、自社のネットワークの脆弱性に関する情報を収集している例もある。

通常の業務としてログの保存も行われているが、何か問題があったときに備えるというよりも、ビジネス上での目的に使われている。

■情報セキュリティ対策について

○ISP はビジネス上の目的からログ保存を行っている。ログデータが捜査上の証拠となることはあるが、保存の目的は捜査のためではなく、ビジネス上のものである。そのため保存するデータは企業によって異なる。（ISP 団体加盟企業）

○大きな DoS 攻撃等、当社のシステムに対する攻撃を監視している。（Web コンテンツ企業）

○ユーザーや(良識ある)ハッカー達から当社のシステムやサービスの脆弱性に関する情報を集めている。過去に脆弱性などの問題点を定期的に報告したユーザーを雇ったこともある。また、ハッカーコミュニティにも顔を出して、当社のセキュリティに関わる情報がないかチェックしている。（Web コンテンツ企業）

○バグやソフトの脆弱性に気付いた際には、そのバグや脆弱性の重大性、その欠陥によって生じるであろう被害の程度等を考慮した上で、すぐに公表してユーザーや顧客に対応してもらう、もしくは、一般に知れ渡る前にバグを修正するためのパッチなどを開発した後に公表するといった対応を行う。（OS 事業者）

○IT 部署に担当者を一人置き、ハイテク犯罪の手法やソフトの脆弱性に関する情報を NIPC（国家インフラ保護センター）、CERT/CC*などのサイトから収集している。（地方自治体）

＜参考＞

*CERT/CC（Computer Emergency Response Team Coordination Center）
Morris Worm と呼ばれるコンピュータウイルス事件が起こった直後の 1988 年 12 月に、DARPA（Defense Advanced Research Projects Agency）によって CERT が設立された。その後 CERT/CC へと拡大し、カーネギーメロン大学におけるネットワークシステム強化プログラムの一部となっている。現在では、不正行為への対応を行うチームに対する設立援助、複数チームのコーディネート、トレーニング、セキュリティ脆弱性の原因追及及び改善策の提供などを行っている。

3.1.2 違法・有害情報対策

今回の調査では、コンピュータウイルスといった不正プログラムや児童ポルノなどの違法・有害情報について、日頃から Web サイトを監視しているところはなかった。いずれも、ユーザー等から通報などがあった時点で、あらかじめ決められた法執行機関等に連絡するといった対応が行われている。

■違法・有害情報対策について

○違法・有害情報のモニタリングは行っていない。（ISP 団体加盟企業）

○ユーザーの Web サイトのモニタリングは行っていない。ライブラリや検索エンジンでリンクを貼っている Web サイトにおける違法・有害情報をチェックするのは不可能である。ユーザーなど第三者からの連絡により、Web サイトをチェックし、違法・有害情報と見なせば、リンクから外す。（Web コンテンツ企業）

○ホスティングサービスにおいても、ユーザーのコンテンツ、インデックスを監視することはない。ユーザーの全コンテンツをモニタリングするのは、全ての電話や手紙の中身を監視するのと同じで不可能である。また、このような監視は法律では許されてもいない。義務もない。（Web コンテンツ企業）

○違法・有害情報のサイトをモニターしている部署はない。ソフトウェアの脆弱性に関する情報は積極的に収集している。バグトラック等の情報提供や情報交換をしている公開サイトを持っており、バグや脆弱性に気付いたユーザーや企業のセキュリティ担当者が情報を提供してくれている。このように非公式な形で情報が集まっている。（OS 事業者）

○対策は行っていない。（地方自治体）

○何が有害な情報であるかどうかの判断は主観に基づくものであり、最終的な解決は難しい。良い情報、悪い情報を国が一元的に判断することには反対である。言論の自由が確保されるべきである。フィルタリングソフトは、情報の有害性を安易に判断してしまうツールであり、利用を強制することには反対である。（市民団体）

3.1.3 情報・データ漏洩対策

個人情報を扱っている地方自治体では、情報保護が非常に重要な問題となっている。そのために個人情報は、安全でクローズドなネットワークに保存されており、ハッキング等の脅威から守られている。

■情報・データ漏洩対策について

○情報保護は非常に重要な問題である。個人情報は全て安全でクローズドなネットワークに保存されているので、ハッキングされることはない。（地方自治体）

○顧客が自社のサービスを利用する際に必要なパスワードは保存していない。パスワードリマインダーはそのために必要である。（Web コンテンツ企業）

3.1.4 ネットワーク詐欺等の不正行為対策

ユーザーID の付与段階での本人確認についての懸念が指摘された。

■ネットワーク詐欺等の不正行為対策について

○ユーザーID の付与段階での本人確認には問題がある。使い勝手とセキュリティとのバランスを取る必要がある。現状、コンピュータにあまり詳しくないユーザーでも簡単に使えるようにするために簡単な手続きとなっている。（ISP 団体加盟企業）

3.2 問題発生時の対応

3.2.1 自社に対する攻撃時の対応

ISP 等のサービス事業者が、コンピュータウイルスや不正アクセス、DoS 攻撃といったネットワークへの攻撃等を受けた場合、攻撃の内容、アクセス先等が調べられ、攻撃と判断されれば、警察に通報する時に備えて、攻撃に関する全ての情報、記録（ログ情報等）が集められ保存される。そして、FBI 等の法執行機関に通報して、自社で収集した情報が提供されている。この場合、情報収集にあたっての令状（subpoena）は不要とされる。

法執行機関への通報を行うかどうかは、被害にあった企業が判断することになる。ISP、OS 事業者では、自社が攻撃された場合に通報を行っている。一方、ソフトウェア等にバグや脆弱性などが発見されても、メーカーには法執行機関等への報告等の義務はない。

■自社に対する攻撃時の対応について

○コンピュータウイルス等に対応するため、主要国にサイバーアタック対応チームを用意している。サイバーアタックが発生した場合、証拠を保全しファイルをコピーするとともに、顧客への連絡を行う。また、内部でサイバー攻撃に関する調査をし、法執行機関へ通報する。その際、被害にあった企業名は明かさない。企業名を明かすかどうかは顧客の判断による。（ISP 団体加盟企業）

○ハイテク犯罪捜査に伴い、ユーザーID とユーザーの特定を行うかどうかは、誰が捜査を始めたかによって異なる。ISP 自身が被害者となった場合には、US Patriot Act（愛国者法）により、収集した情報を全て法執行機関に提供することができる。（ISP 団体加盟企業）

○大きな攻撃があった場合、ISP と協力して、できる限りトレースし、どこからの攻撃なのか等詳細を調べる。小さな攻撃は、通常のアクセスなのか見分けがつかないことが多い。（Web コンテンツ企業）

○当社が被害にあったとしてもよほど大きな損害を受けない限り、法執行機関へは通報しない。しかし、subpoena 等の法的手続きを経た上での法執行機関の要請であれば、情報を提供する。要請された情報は技術部門が収集し、それが法律的に開示できるかどうかを法務部で確認した後に提出する（Web コンテンツ企業）

○自社のオンラインサービス上での犯罪行為に対してならば、ISP やコンテンツ提供者がモニタリングをしても良いことになっている。インターネット詐欺や児童ポルノ、誘拐等の犯罪がネットワークを通じて行われているという情報が入れば、できるだけ早くその犯罪行為で利用されているウェブサイトやメールのやり取りのデータを見つけ、それを保存している。その後は、通報し、犯人を追跡するか、そのまま泳がせておくか、法執行機関の判断を待つ。当社のアカウントを使ってメールを送り、詐欺を行った事件があったが、そのケースではシークレットサービスに通報した。（Web コンテンツ企業）

○自社ネットワークに対する攻撃や普通ではありえないアクセスを見つけた時は、まずセキュリティ部隊が調査を行う。具体的には、どのような行為が行われているのか、どこからのアクセスなのか、ソフトウェアのバグではないか等の詳細を調べている。調査の結果、攻撃と判断すれば、警察に通報する時に備えて、この攻撃に関する全ての情報、記録（ログ情報等）を集めて保存する。さらに、FBI などの全国規模で捜査する法執行機関に通報し、情報提供する。（OS 事業者）

○アメリカの法律では、当社や当社が顧客に提供しているネットワークが被害を受け、警察の捜査が入れば、令状（subpoena）がなくても、犯罪の証拠に関する情報を収集することができる。そのため、当社が被害者となれば、積極的に情報提供をしている。（OS 事業者）

○顧客が攻撃を受けたり、ソフトウェアのバグ、脆弱性等を見つけたりした場合には、

対応窓口に連絡をしてもらっている。（OS 事業者）

○自社が被害にあった場合には、FBI などの全国規模で捜査する法執行機関に通報する。バグや脆弱性を発見した時、政府や法執行機関に連絡するが、それは主要顧客であるからであって、報告義務や協定があるわけではない。（OS 事業者）

○企業が脅威にさらされたり、使用ソフトの脆弱性に気付いたりした時は、NIPC（国家インフラ保護センター）に報告している。（OS 事業者）

○当社の製品やサービスを使用している顧客が被害を受けた場合は、攻撃内容や被害の詳細、ログなどの記録、脆弱性にもたらされる攻撃可能性等について警察に連絡するかどうかは被害者である顧客が決める。（OS 事業者）

○どのようなケースには、どの機関（法執行機関や NIPC 等の団体）に報告するかといったことを定めた社内規定がある。そこでは、被害を受けた場合、提供する情報は何か、社内の許可なく提供できる情報は何か、どのような手順を踏むべきか等を示している。（OS 事業者）

3.2.2 違法・有害情報確認時の対応

一般に ISP では、違法･有害情報の監視はしていない。ユーザー等の連絡があった時点で、警告や情報の削除など ISP の規定に応じた対応が行われている。また、児童ポルノについては、法的な報告義務がある。

■違法･有害情報確認時の対応について

○違法・有害情報のモニタリングは行っていないが、チャットルームなどで自殺をほのめかすといったことを発見した場合には、最寄りの警察に通報している。（ISP 団体加盟企業）

○児童ポルノに関しては法的な報告義務がある。ユーザーなど第三者から児童ポルノに関する情報を得ると、そのサイトの画像をダウンロードして、司法長官に報告している。（Web コンテンツ企業）

○ユーザーなど第三者からの連絡により、リンク先のサイトをチェックし、違法・有害情報と見なせば、リンクから外す。（Web コンテンツ企業）

○ISP が自社の Web 上にある不適切な情報に対して警告や削除を行うことについては反対しない。ISP とユーザーには民間の契約関係があり、ISP 利用に際してのルールがある。（市民団体）

4．法執行機関との連携の状況

4.1 捜査協力

4.1.1 捜査協力の内容

ISP 等は、ログ保存の法的義務はなく、通常はビジネス目的のためにログの保存を行っている。法執行機関は、特定の犯罪に関連して、必要な期間、必要な情報を保全することを要請できる。ISP ではこれに対応する義務が生じるが、この要請ではデータを削除しないことまでが範囲とされ、保全されたデータの内容を見るためには令状が必要とされる。また、顧客等から情報や記録を収集する必要がある場合にも、令状が必要とされる。捜査のために提供した情報は公開しないことが前提である。また、アメリカの法律により法執行機関は捜査協力に提供した資料を他社に公表してはいけないことになっている。

■捜査協力の内容について

○ISP にログ保存の法律上の義務はない。法執行機関は特定の犯罪に関連して保全命令を出し、必要な期間、必要な情報を保全することを要請できる。（ISP 団体加盟企業）

○1994 年に改正された電気通信コミュニケーション法で、法執行機関が捜査のために特定の犯罪に関連するデータの保全を求めることが法律上認められている。最小六ヶ月から必要な期間、データの保全を要求できる。この要請はレターで行えばよく、裁判所の令状等は不要である。要請が行われると ISP にはこれに対応する義務が発生する。口頭での要請でも法律上は可能と考えられているが、ISP 側で証拠を残すためにも書類を要求している。保全要請で行えるのはデータの削除をしないことまでである。保全された情報の中身を見るためには令状等が必要となる。（ISP 団体加盟企業）

○ISP のサーバを経由して攻撃が行われた場合等、攻撃者が自社の顧客でない場合には、内部調査の段階から捜査当局が関与することが可能である。取り扱う情報や場合によって、対応する法律や手続きが異なる。（ISP 団体加盟企業）

○ソフトウェア企業では法律により自社の製品を利用した攻撃や被害に関する情報を収集できない。どうしても顧客から情報や記録を収集する必要があれば、令状（subpoena）を出して、顧客からもらう必要がある。（OS 事業者）

○捜査において提供した情報は公開しないことが前提である。また、アメリカの法律により法執行機関は捜査協力に提供した資料を他社に公表してはいけないことになっている。しかし、自発的に提供した情報に関しては、公開されるかどうか定かではない。法律で明文化されていないので不明確である。（OS 事業者）

4.1.2 コンタクトポイント

ISP をはじめとして大手の情報関連企業では、いつでも法執行機関が連絡できるように、コンタクトポイントが設置されている。ただ、法執行機関から連絡が入るのは、テロや爆弾の予告や誘拐など一刻を争う非常事態に限られることが多い。また、捜査協力の依頼に対する部署を設置している企業もある。

■コンタクトポイントについて

○法執行機関はサイバーアタックチームに対して 24 時間アクセスすることができる。チームのコストは全て ISP が負担している。中小の ISP はコストの問題等でコンタクトポイントを用意することは困難である。（ISP 団体加盟企業）

○24 時間いつでも法執行機関が連絡できるように、コンタクトポイントを設置している。担当者のポケベルや携帯電話の番号を教える法執行機関を限定しており、一般には FBI のローカルオフィスのハイテク犯罪部隊である。法執行機関から連絡が入るのは、テロや爆弾の予告や誘拐など一刻を争う非常事態が多い。また、多くの場合、個人的付合いで法執行機関職員に連絡先を知らせている。（Web コンテンツ企業）

○法執行機関から要求された情報については、法務部を通す。直接技術部門の社員が法執行機関に渡すことはない。（Web コンテンツ企業）

○大手情報関連企業については、24 時間連絡することのできる窓口を設けていると思う。ただし、法執行機関との関係においては、企業が法執行機関に連絡する体制はできていても、何か起こった際に法執行機関が各企業に連絡することができるという体制にはない。（情報機器メーカー団体）

○法執行機関からの捜査協力の依頼に対応する部署を設置している。（OS 事業者）

4.1.3 コスト負担

捜査協力のためにそろえたデータに対する費用は、捜査機関に請求することができる。また、ISP 等が捜査協力のために新たなツールを開発した場合でも、法執行機関がその開発費を負担する。

このように捜査協力した場合の必要経費について法執行機関が負担するといっても、機会費用などについては補償されないため、企業側の負担は大きい。

■コスト負担について

○データ保全のコストはデータ保存に比べると大きなものではない。データ保存は全てのユーザーに関するログを蓄積しなければならない。データ保全は、特定のユーザーのログを特定期間蓄積するだけでよい。（ISP 団体加盟企業）

○保全した情報で召喚状により実際の捜査に使用されたものについては、必要経費の払い戻しが行われる。保全要請が乱発されるとコストの問題が発生するので、乱発しないという了解が法執行機関との間にある。ISP 団体から保全に関する税制優遇等の要請を国家安全局に対して行った。（ISP 団体加盟企業）

○1 年ほど前に法律が制定され、捜査協力のためにそろえたデータに対する費用を捜査機関に請求できるようになった。また、愛国者法により、ISP が捜査協力を行うにあたってツール類を開発した場合に法執行機関がその開発費を負担するようになった。法執行機関への請求は社内でコスト換算表を作り、その単価を元に行っている。全額負担してもらうことは少ない。（Web コンテンツ企業）

○Y2K 問題で法執行機関と共同作業を進めた経験から、法執行機関への協力コストがセキュリティ侵害での損失以上に嵩むことを懸念して、民間は協力に消極的である。そこで当団体が、法執行機関と民間企業との協力関係について話し合う枠組みとしての役割を果たすようになった。（情報機器メーカー団体）

○データ保存、保全や捜査のためにコンピュータが没収されるといったコストの他、捜査のために業務を中断する結果生まれる損失、被害にあった企業の信用低下、顧客情報の漏洩等、数字で表しにくい被害が大きい。保全を図ったデータが実際の捜査に使われ、その必要経費が支払われたとしても、ビジネスに対するダメージを埋め合わせることはできない。（情報機器メーカー団体）

○捜査協力にはとてもコストがかかる。特に OS 製品の情報やネットワークの記録などをそろえるのに時間を取られることが大きい。法執行機関との対応でもヒューマンリソースを奪われる。捜査協力した場合、データ提出などで発生した費用に対しては支払いを受けることができる。しかし、人材確保や機会費用は対象でない。（OS 事業者）

4.2 情報提供・情報交換及び技術協力

情報セキュリティについての日常的な情報交換が、業界や非公式の団体などを通じて行われている。こうした場では、人的関係を築くことが重視されている。人的コネクションがあれば、問題が生じた時、誰に連絡すればいいのか、その問題には誰が精通しているのかといったことが容易に判断でき、円滑な問題解決が可能となる。また、こうした団体を通じて法執行機関に被害に関する情報提供が行われている。

技術協力の面では、法執行機関から要請があれば技術情報の提供が行われている。また、政府機関から資金援助を受けて、セキュリティに関する研究開発を実施している企業もある。

■情報提供・情報交換及び技術協力について

○法執行機関から当社の法務部に依頼があれば、技術関連の情報を提供することがある。（Web コンテンツ企業）

○官民の連携には人と人との間のつながりが大切である。情報セキュリティについても、官民の間で自由に情報共有を行うことができる体制・場所の提供が必要である。（情報機器メーカー団体）

○問題発生時には、CERT に情報提供を行っている。CERT には情報技術関連の省庁や企業が集まっており、ネットワークやコンピュータに対する脅威や攻撃、新しいハッキングテクニックなどの情報を共有できる体制にある。CERT は大きな成果をあげている。（OS 事業者）

○当社では、政府からの資金援助を受けてセキュリティに関する研究を実施している。（OS 事業者）

○IT-ISAC*は被害等の情報を FBI に報告している。顧客企業が被害を受けた場合に、企業を特定できるデータを渡すことはない。（OS 事業者）

○連邦政府との情報共有はあまり行っていない。市警とは定期的に情報共有や技術交流を行っている。（地方自治体）

○AGORA**という非公式なグループがあり、FBI や地方警察、地方政府、企業のネットワーク担当者が集まって月に一回、情報交換を行っている。人的ネットワークを築くことが会合の最も重要な点である。人的コネクションがあれば、問題が生じた時に政府機関の誰に連絡すればいいのか、その問題には誰が精通しているのかなど、問題解決がスムーズにできる。（地方自治体）

＜参考＞

*IT-ISAC（Information Sharing and Analysis Center for Information Technology）
2001 年 1 月、マイクロソフトやオラクル、IBM などトップレベルの企業 19 社が、連邦機関である CIAC 及び CERT とチームを組んで情報シェアに取り組むとした発表を行った。民間の企業は競合する企業同士ということもあり、製品脆弱性やハッカー攻撃傾向などの情報はこれまで機密情報として取り扱われていた。しかしそのような情報を共有し、共同対策を打ち立てることにより消費者からの信頼を取り戻し、インターネットを介した事業収入を確保することを狙いとしている。
この情報共有プログラムは、IT-ISAC と呼ばれる非営利機関として機能する。これら企業機密に関わる情報の共有は企業同士の信頼関係の上に成り立っており、また同時に政府機関からは最新のスレット情報が提供される、という相互支援が同プログラムの前提となっている。IT-ISAC 発足当時のノーマン・ミネタ商務長官は「共同戦線を張ることにより、サイバーアタッカーに対して威嚇を行っていく」と語っている。

**AGORA
AGORA とは、古代ギリシャにおけるアテネ市民の公的な活動や商取引の中心だった広場のこと。AGORA は、IT 分野における地域ネットワークであり、急速に普及する情報通信技術における新しいセキュリティに取り組むために 1995 年 10 月に設立された非公式な組織である。当初 50 人で始まったミーティングは、600 人以上に拡大しており、米 20 州、カナダ 5 州から、154 の企業、120 の米政府機関（連邦、地方）に属するメンバーが集まる。AGORA の目的は、共通の問題やベストプラクティスについて情報共有するための信頼できる方法を確立することであり、情報通信インフラを守る知識のシェア、情報セキュリティに関する調査の実施、業務を進める上での能力を向上するシェアドサービス、法執行機関を含めて参加者へのサポート、教育機会のシェアなどを主要テーマとしている。

５．産業界における連携の状況

産業界では、情報セキュリティの脅威に対応し、被害状況、攻撃の手口、その時の企業の対応などについての情報交換・共有が行われている。また、情報関連企業の団体である IT-ISAC では、今後どのような攻撃の可能性があるか等、将来的なことについての情報交換が行われている。

■産業界における連携の状況について

○同業他社との協力関係が築かれている。DoS 攻撃を受けた時には、攻撃についての情報共有を行った。このような協力関係は非公式で、個人的付合いで行うことが多い。（Web コンテンツ企業）

○IT-ISAC では、IT 関連企業約 20 社が過去の被害（コンピュータセキュリティの侵害、ウイルス、DoS 攻撃等）とそれに対して行った各企業の対応に関する情報を収集するのに加え、今後どのような攻撃の可能性があるか等、将来的なことについての情報も共有するという活動を行っている。今後どのような攻撃の可能性があるか等、将来的なことについての情報も共有するという点でユニークである。IT-ISAC の重要性は、過去の分析よりも、これから起きることを防ぐという点である。共有されている情報の中身としては、過去の手口の理解／分析、市販されているソフトの有効性・互換性、FBI 等の情報源から寄せられる警告等である。（情報機器メーカー団体）

○被害等の情報は IT-ISAC に報告している。また、CERT に情報提供を行っている。（OS 事業者）

6．人材育成

6.1 公的機関を対象とした人材育成活動

公的機関の要請に応じて、情報セキュリティに関する技術やハイテク犯罪についての講演等を行うなど、公的機関の人材育成に民間企業が協力している状況がみられる。

■公的機関を対象とした人材育成活動について

○地方の法執行機関等を対象として、要請に応じて技術やハイテク犯罪に関する講演やセミナーを現地で開くこともある。（Web コンテンツ企業）

○依頼があれば、公的機関の職員に対して、製品やネットワークに関する講習会を実施している。無料であるが、当社に対する利益は大きいと考えている。法執行機関の職員が製品やネットワークの知識を身につけることは、ハイテク犯罪の捜査がスムーズになり、犯罪の抑止にもつながる。（OS 事業者）

○庁内の職員への教育は、採用直後のオリエンテーションぐらいで、スキルをつけるための講習会などは行っていない。（地方自治体）

6.2 顧客等を対象とした人材育成活動

業界団体や民間団体などが、情報セキュリティへの対応が難しい一般ユーザー、中小企業に対して、啓発、研修といった活動を行っている。

■顧客等を対象とした人材育成活動について

○司法省、国防省からの強い支持で、2 年前より Cyber Citizenship Program を実施している。子供のうちから、ネットワーク上の行動に対する責任・マナー・倫理を教えるプログラムである。司法省・国防省がこのプログラムに積極的であった背景には、ティーンエイジャーによる国防省サーバへのハッキング等、若い層によるハイテク犯罪が多かったことがある。（情報機器メーカー団体）

○Staysafeonline.net というプログラムがあり、特に中小企業・個人向けにどのようにサイバー攻撃の対象となることを防ぐか、もし被害にあったらどうすればいいのかという点について啓蒙している。（情報機器メーカー団体）

○一般ユーザーを対象として、Web サイトでプライバシー関連のコンテンツを提供することや、プライバシーに関連した書籍等を発行している。大学で講義も行っている。（市民団体）

7．国・官公庁の取り組みに対する評価

7.1 産業界との連携の在り方

ハイテク犯罪が多くなってきた当時、法執行機関にはそれに対応する人材がほとんどおらず、人材育成等で産業界の支援を必要としていた。一方、産業界においても業界だけでハイテク犯罪を抑えることに限界を感じており、政府の力が必要であった。こうした背景があって、産官協力への理解が進み、協力関係が築かれてきたと考えられている。

そして、実効性のある協力関係を築くためには、産業界、法執行機関が互いを理解し、信頼関係を築くことが必要であることが指摘された。

■連携の在り方について

①人間関係の構築

○法執行機関と民間企業との間での対話を継続的に行うことが必要である。産業界、法執行機関双方が互いを理解すべきであり、信頼関係を築かなければならない。（ISP 団体加盟企業）

○法執行機関は日ごろから企業と親密な人間関係を築くことが重要である。知らない法執行官から捜査協力を要請されても、提供した情報がどのように利用されるか分からないため、個人情報保護上、簡単に渡すことはできない。知り合いの執行官ならば安心なので、信頼してデータを渡すことができる。（Web コンテンツ企業）

○官民の連携には人と人との間のつながりが大切である。情報セキュリティについても、官民の間で自由に情報共有を行うことができる体制、場所が必要ではないか。産業界、政府相互の信頼を築いていくことが必要である。（情報機器メーカー団体）

②人材育成支援

○捜査を担当する人材の育成についてどのように支援できるか、対話が始まったばかりである。（情報機器メーカー団体）

7.2 国･官公庁の取り組みに対する評価及び要望

ハイテク犯罪に対応した法制度の整備が進められているが、その検討過程で ISP の意向が反映されたこともあり、それらの法制度については概ね良い評価が得られているようである。一方、警察機関内だけで意思決定されることに対する懸念が市民団体から指摘された。

また、人材については、連邦政府に比べ、地方及び海外の法執行機関で課題があるとの指摘があった。国・官公庁に対する要望としても、人材育成があげられ、産業界との信頼関係を築くためにも、人材育成に予算をつけ、国が情報セキュリティの問題について真剣に取り組んでいるということを示すことが必要であるという指摘があった。

また、連絡窓口とともに、情報セキュリティを扱う機関の一本化が求められている。各企業が同じ問題を全く異なる法執行機関に報告することになれば、問題の全体像を把握することが不可能となり、解決も遅れてしまうことが懸念されている。

■国･官公庁の取り組みに対する評価ついて

①法制度整備

○捜査に当たって、法執行機関が特定の犯罪に関連して保全命令を出し、必要な期間、ログ等の必要な情報を保全することを要請できる。捜査上の目的とプライバシーの保護のバランスを取る上で良い制度となっている。（ISP 団体加盟企業）

○愛国者法では、技術変化に対応して法律がアップデートされた。電話を対象とした法律では、インターネットをどう解釈すべきかに時間がかかっていたが、愛国者法制定後はスムーズな対応が可能になった。法律策定の初期の段階から ISP の意向が反映されている。（ISP 団体加盟企業）

○愛国者法の成立により、サイバーテロやハッキングは生物兵器使用と同等のものとみなされるようになった。従来、ハッキング等については被害規模が大きくなければ捜査が行えなかったが、愛国者法以後は捜査当局が積極的に捜査できるようになっている。（ISP 団体加盟企業）

②人材

○FBI の IT セクションの職員はとても訓練されており、その FBI からトレーニングを受けている司法省の IT セクションの職員も知識が豊富である。司法省や FBI の IT セクションの職員は、コンピュータ関連企業と密接な関係を築いており、最新の技術や動向について詳しいことが多い。一方、地方や海外の法執行機関の職員はコンピュータ技術などに精通していない。（Web コンテンツ企業）

■要望について

①人材育成

○法執行機関内部の人材育成が必要である。官民が信頼できる協力関係を築くためにも、官は十分な知識を持つための投資を行うべきである。（ISP 団体加盟企業）

○法執行機関の職員はセキュリティに関する知識と基本的なスキルを身につけて欲しい。（Web コンテンツ企業）

○ハイテク犯罪捜査のための経験・知識が不足している。DoS 攻撃等のネットワークを利用したハイテク犯罪だけではなく、コンピュータを媒体とした犯罪（児童ポルノ、ネットワーク詐欺等）を取り締まるのに必要な知識が足りない人が捜査を担当している。産業界との信頼関係を築くためにも、国が情報セキュリティの問題について真剣に取り組んでいるということを、予算をつけ、人材を育成しているという形で示すことが必要である。（情報機器メーカー団体）

○政府はスキルある人材を採用し、最新の装備をそろえるところから始めて欲しい。（OS 事業者）

②国際的対話

○G8 等の国際的な対話も重要である。（ISP 団体加盟企業）

③民間の事業活動への理解

○海外の法執行機関に対する要望としては、捜査協力をする際などの国際間法的手続きについて理解を深めて欲しい。国際的な捜査協力をする場合、国際条約に基づいた手続きを踏む必要があることを理解して欲しい。（Web コンテンツ企業）

④法制度の整備

○規制過多になる状況は避けるべきである。規制が合理的で、フレキシブルなものであれば、ISP も協力する。ログの保存期間等を定めるといったことは行わず、フレキシブルな対応を行うべきである。（ISP 団体加盟企業）

○警察権力が拡大していく方向にあり危惧している。テロに対する懸念が高まっていることは理解しているが、意思決定が秘密裏に行われるようになることを警戒している。選挙で国民に選ばれた議会ではなく、警察機関の中で意思決定が行われるようになることに対して反対の立場である。（市民団体）

○ISP が自社の Web 上にある不適切な情報に対して警告や削除を行うことについては反対しない。ISP とユーザーには民間の契約関係があり、ISP 利用に際してのルールがある。政府が一元的な判断を下すことに対して反対している。（市民団体）

○通信傍受に関するセーフガードが除去された。これまでの通信傍受では、通話先の電話番号と通話内容では保護のレベルが異なっていた。電話番号が低いレベルの保護であるのに対し、通話内容は高いレベルの保護が要求されていた。しかし、愛国者法ではインターネット上のやり取りについて、E-mail を含めて低いレベルのものと位置づけられている。E-mail は高いレベルの保護が求められる。（ユーザー団体）

⑤連絡窓口等の一本化

○法執行機関が企業に連絡をする場合の窓口は決められているので、一本化して欲しい。例え技術部門が持っているデータの提供を要求する場合でも、当社の連絡窓口を通して、所定の手続きを踏まなければ協力できない。（Web コンテンツ企業）

○産官連携･協力を取りまとめる窓口を一本化することは重要である。一本化しないと各企業が同じ問題を全く異なる法執行機関に報告することになる。これでは問題の全体像を把握することが不可能であり、解決も遅れてしまう。（OS 事業者）

⑥技術開発

○犯罪が起きる前の防犯が必要であり、情報セキュリティを確保するために、もっと政府は予算をかけ、安全なネットワークを築くべきである。国がそういった姿勢をみせることが、他の企業への啓蒙にもつながる。（情報機器メーカー団体）

○必要な研究開発であっても、営利を目的とする企業では投資することがなかなか難しい分野について、政府が積極的に研究・開発を行うという姿勢をみせる必要がある。（情報機器メーカー団体）

Ⅲ　英国

１．情報セキュリティに対しての認識

情報セキュリティが自社の事業に直接関わるISP等の企業以外では、情報セキュリティへの関心はあまり高くないのが現状である。法執行機関においては、官民連携の枠組みであるInternet Crime Forum*の発足等、最近になってさまざまな取り組みが始まりつつあるが、地域警察レベルでは、ハイテク犯罪に対する捜査の優先順位はあまり高くない。原因としては、例えばDoS攻撃が英国においては犯罪行為と認定されていない等、ネットワーク犯罪の概念自体がまだ確立されていないこと、警察にコンピュータ犯罪に関する知識とそれに対応することのできる人的リソースが絶対的に不足していること等があげられる。

インターネット上の犯罪という点では、英国で現在最も問題となり、かつ、積極的に対応が取られているのが、ネット上における児童ポルノである。

＜参考＞

* Internet Crime Forum （前Industry Government Police Forum）
1996年にAssociation of Chief Police Officersのイニシアティブより設立されたハイテク犯罪対策のための官民連携組織。IT業界、法執行機関、政府、消費者団体等12団体がメンバーとなっており、四半期に一回定期的な会合を行っている。この会合の他にもテーマ毎にサブグループが形成されており、児童ポルノ、スパムメール、データ保存、インターネット詐欺等の個別のテーマについての対応を検討している。長期的な人的ネットワークの形成に役立っており、インフォーマルにも頻繁にミーティングを持っている。

２．情報セキュリティ対策のための体制

情報セキュリティが自社の事業に直接関わる企業では、情報セキュリティに対する意識も高く、インターネットを利用した犯罪（ウイルス、ハッキング、DoS攻撃等）に対して、技術的な予防策をとったりネットワークを定期的にモニターしたりするほか、社内に対策チーム（小規模な企業は除く。）をつくるなど、何かあった場合に組織的に対応できる体制をとっている。一方、一般企業の情報セキュリティへの意識はまだ低い。

インターネットサービスを提供する企業の中には、新種のウイルス等の情報が入った際にユーザーに対して警告と対応策を通知するところもあるが、一般にこのような対策は本来ユーザー責任で行うべきであるという認識が強い。

■情報セキュリティ対策のための体制について
○ネットワークセキュリティマネージャーは、何かあった場合にすぐにシニアマネージャー（ボードメンバー）に連絡し、対応がとれる体制になっている。（Webコンテ

ンツ企業）
○政府機関から定期的にネットワークの脆弱性等の最新情報を受け取っている。（Web コンテンツ企業）

3．情報セキュリティ確保のための対策及び対応

3.1 事前対策（予防）

ここでは、コンピュータウイルスや不正アクセス、DoS 攻撃といったネットワークへの攻撃を事前に防いだり、攻撃を速やかに察知したりするために、実施されている対策についてまとめている。

3.1.1 情報セキュリティ対策

コンピュータウイルスや不正アクセス、DoS 攻撃といったネットワークへの攻撃に対する事前の対策（予防）として、FW（FireWall）、ウイルス検知といった対策が主である。ただし、一般企業の情報セキュリティに対する意識はまだ低く、多くの企業がファイアウォールを適切に設定していない、ウィルスソフトを定期的にアップデートしていないとの指摘があった。

ログの保存については、現在法的な義務付けはなく、ビジネスの目的によって各企業における保存期間はまちまちである。

■情報セキュリティ対策について
○ネットワーク犯罪予防策としては、ファイアウォールやウイルス検知といった通常の対策を取っているが、（企業で使用される）ファイアウォールの 90%が適切に設定されていないことは周知の事実であり、また多くのウイルス検知ソフトが定期的にアップデートされていない。（ISP 団体）
○ウイルスへの対策は、本来ユーザー責任であると考える ISP 企業は多く、現在 ISP 各社がこのような対策をとっているのは、ビジネスサービスの観点であり、法令等によって（ISP へ）義務化されるべき性質のものではないと考える。（ISP 団体）
○ISP がネットワーク上の情報をモニターすることは、特別の場合を除いて Electronic Commerce Directive、EU Directive 及び Regulations of Investigatory Powers Act (RIP) (Interception of Communication Act として改正)により禁止されている。（ISP 団体）
○自社のネットワークについては、継続的にアクセスを監視するなど、セキュリティに気をつけている。（Web コンテンツ企業）
○情報セキュリティは実際の被害が起きるまでその必要性をなかなか認めてもらいに

くいため、一般企業内のネットワーク担当者は苦労しているようだ。（Web コンテンツ企業）

○ユーザーに対し、①コンテンツ内容へ責任を持つ（有害･違法な情報を掲載しない）、②犯罪や他のユーザーの迷惑になるような利用をしない、③チェーンメール、スパムメール、ウイルス、ねずみ講等の行為をしないこと等を契約条件として義務付けている。（ISP）

○当社の機器は安全なサイトにアクセスを限定できるブラウザーを搭載しており、安全なサイトにしかアクセスできない設定になっている。（情報機器メーカー）

3.1.2 違法・有害情報対策

産業・法執行機関ともに定期的な違法・有害情報のモニタリング等はしていない。基本的には、ユーザー等から通報があった場合に対処している。

ただし、児童ポルノについては例外となっており、定期的に違法なサイトがないか監視しつつ､一般ユーザーからの情報を 24 時間体制で受け付けている団体が存在する。

■違法・有害情報対策について

○違法・有害情報のモニタリングは行っていない。ISP はインフラの提供を行うだけであって、インターネット上に流れる情報への責任は持たない。（ISP 団体）

○電話会社が顧客の通話内容を聴くことが許されていないように､ISP は送信される情報の中身をモニターすることは許されていない。（ISP）

○違法行為を行ったユーザーは、二度と当社のサービスが使えないような対処をとることもある。（ISP）

○ウェブサイトのレーティングを行い、フィルターの導入を薦めている。特定のサイトを削除する必要がないため、表現・言論の自由を侵害することなく、児童を有害な情報から守ることができている。(公益団体)

○24 時間アクセスできるホットラインを用意しネットワーク上の児童ポルノに関する情報を外部から収集するとともに、自らも定期的にチャットルームなどウェブサイトをパトロールしている。その結果、違法性の度合いに応じて 3 つのグループにカテゴリー分けし、その情報を ISP へ提供している。（公益団体）

3.1.3 情報・データ漏洩対策

金銭の取引をネット上で行う企業（銀行等）以外は、厳しいユーザー認証が必要との認識はない。

また、外部に出してもよいデータをハンドブックにより規定し、違反に対しては厳しい罰則を与えている場合もある。

■情報・データ漏洩対策について

○金銭の取引を自社の Web 上で行う企業は、ユーザーの詳細な情報収集やユーザー認証について高い関心をもって行っているが、それ以外の企業にとっては、あまりインセンティブのない行為である。（ISP 団体）

○通常ユーザーは電話会社を経由して ISP へ料金を支払う形式を取っているため、ユーザーと ISP の間に直接の金銭関係はない。このため多くの ISP はユーザー認証にそれほど関心をもっていない。（ISP 団体）

○内部データの外部への公表については社内ハンドブックにより規定されている。情報セキュリティを脅かすような行為を行った場合、解雇ということも有り得る。実際に金銭的な被害があった場合、法的手段に訴えることも有り得る。（情報機器メーカー）

3.1.4 ネットワーク詐欺等の不正行為対策

インターネット上の詐欺防止対策としては、貿易産業省が後援する業界団体や消費者団体が信頼のおけるウェブサイトを認定し、認定されたサイトは認定マークをウェブサイトに掲載している。ユーザーが安心してインターネット上で取引を行える環境を整えている。

3.2 問題発生時の対応

3.2.1 法執行機関への連絡

ハイテク犯罪の種類により、法執行機関への連絡先が異なっており、現在その対応を Internet Crime Forum が整理しようとしている。

インターネット上における DoS 攻撃等の行為については、必ずしも違法かどうか判断が明確にできないため、違法性の高い行為であっても、ISP の多くは社内における対応に留め、実際に法執行機関へ通報されるケースは必ずしも多くないようである。

一方、児童ポルノについては、ユーザーからの情報等により発見した ISP が IWF（Internet Watch Foundation）*に連絡し、同団体が違法性の有無を判断し、必要に

応じて法執行機関に通報するといった対応がとられている。また、IWF からも違法・有害情報のサイトに関わる情報が定期的に ISP へ提供され、ISP は当該サイトを削除する等の対応を行っている。多くの ISP 企業は、社内に違法・有害情報対策チームを結成しており、有害と認定された情報を削除する権限が、法律上（Obscene Publication Act）認められている。

ユーザーから通報があった場合、多くの企業は社内の違法行為対策チーム内で、当該通報内容を検討する。検討の結果、犯罪の可能性が高いと認定されれば担当の法執行機関へ通報する。警察の通報先は、警察内の Single Point of Contact(SPOC)である。捜査官は犯罪捜査を行う場合、SPOC を通さなければならないことになっており、捜査官に申請された案件が捜査を進める条件を満たしているか SPOC で判断する。この判断結果をもとに、捜査が開始され、産業界の協力が必要とわかった場合、産業界への協力依頼も、SPOC が行う。ISP 等にログデータ等の情報提供を依頼する場合には、法的な手続きが必要となっている。

■法執行機関への連絡について

○スパムメール、DoS 攻撃や一部のハッキング行為のように、当該行為が非社会的行為であっても、犯罪とは認識されないケースが多くある。各社の社内警察ともいえる犯罪対策チームが当該行為の内容により対応を決めている。犯罪行為であると認定したときだけ法執行機関へ連絡する。（ISP 団体）

○英国においては DoS 攻撃やスパムメールは犯罪として取り扱われていないため、通報したとしても、警察は対応できない。したがって、社内・業界内で対処する。（ISP 団体）

○ウイルスやハッキングといった違法行為を通報したとしても、警察側は取り合ってくれないことが過去のケースとして多い。このような問題に警察側はあまり興味をもっていないようだ。（ISP 団体）

○あるユーザーが特定のプロバイダーからスパムメールを送付していることが分かった場合、当該プロバイダーに連絡し、そのアカウントを削除するようにしている。（ISP 団体）

○SPOC は 50 警察機関当り一箇所の割合で設けられている。SPOC は必要な情報提供依頼をファクシミリで ISP に依頼することができる。SPOC によってそのフォーマットは異なっており、また一連のプロセスは非常に官僚的で効率が悪い。時間がかかりすぎるため、結果的に長期のログデータの保存が必要となっている。（ISP 団体）

○一般ユーザーから寄せられた児童ポルノに関する情報の違法性を判断し、必要に応じて ISP や法執行機関に連絡している。ただし、違法かどうかの判断は裁判所しかできないため、「違法性が高い」という判断を使っている。（公益団体）

○あらゆる情報ソースから寄せられたネットワーク上の児童ポルノに関する情報を整理し、まとめた形で英国法執行機関及び Interpol に通報している。（公益団体）

＜参考＞

*IWF（Internet Watch Foundation）
インターネット上における違法･有害情報、中でも特に児童ポルノの問題を解決するために 1996 年 9 月に設立された。財源は、EU と英国 IT 業界（1997 年 4 月より）からそれぞれ 50%ずつの資金を得ている。活動としては、24 時間違法･有害情報について通報できる 24 時間のホットラインを持つとともに、ウェブサイト上の定期的な監視を行っている。多くの ISP が同財団に加盟しており、相互に協力関係にある。コンテンツの違法性を判断し、違法だった場合には、ISP 等に削除を依頼するとともに法執行機関へ通報する。コンテンツのレーティングも行っている。インターポールや海外の法執行機関へ通報・連携することもある。

4．法執行機関との連携の状況

4.1 捜査協力

4.1.1 捜査協力の内容

法執行機関から要請があれば各社は必要な情報を提供している。

ログの保存については、現在法的な義務付けはなく、ビジネスの目的によって各企業保存期間はまちまちである。ただし、現在審議されている Anti-Terrorism Crime and Security Bill が発行され効力をもつようになれば 6 ヶ月間のデータ保存が義務付けられるようになる。現在、この法案は、産業界からコストの面で不可能であるとともに、犯罪捜査上意味のないものとして大きな反対を受けている。

また、現在捜査に必要な情報データの提供を、警察は、裁判所命令がない限り、ISP 等の関係企業へ「依頼」しているものであるが、Regulation on Investigatory Powers Act 2000（RIP Act:2000 年捜査権限規制法）が施行されれば裁判所命令がなくとも、「請求」することができるようになるなど、警察の捜査権が強化される方向にある。

■捜査協力の内容について

○法執行機関は、産業界へ情報提供を依頼するには、法律に則った手続きを踏まなければならない。法律によって、捜査協力依頼には、対応するよう義務付けられている。（ISP 団体、ISP）

○警察が捜査中に産業界からの情報が証拠として役に立つと分かった場合、当該警察内における Police Liaison Units と ISP の間で協力体制がつくられる。その中には少なくとも 1 人はハイテク犯罪に関して何らかの訓練を受けた捜査官が配置されるようになっている。（ISP 団体）

○法執行機関への情報の提供と顧客のプライバシー保護のバランスは難しい。特に警

察から、特定の顧客情報だけではなく、大勢の顧客情報開示の依頼があった場合に問題になる。(ISP 団体)

○法執行機関に対しては、特に捜査協力体制が構築されているわけではなく、何か要請が来たときに個別に対応しているだけである。(ISP)

4.1.2 コスト負担

捜査協力のためにそろえたデータに対する費用は、捜査機関に請求しているが、制度的に認められているわけではない。データ保存については、各企業の負担となっている。

■コスト負担について

○多くの企業は、法執行機関への協力にかかったデータ保全等の費用については自社で負担しているが、企業によっては請求するところもある(制度的に認められているわけではなく、実際に支払われているかどうかは不明)。現在誰がどの費用を負担すべきかというガイドラインはないが、捜査協力によって利益を得ることはしないというのが、業界の方針である。(ISP 団体)

○捜査にかかった費用の補填を制度的に認めてもらえるように現在法執行機関へ働きかけている。人権団体等で捜査に協力しているところも捜査協力費用の支払いを望んでいる。(ISP 団体)

○Anti-Terrorism Crime and Security Act により、長い期間のデータ保存に対する政府からの費用補填が行われることとなった。(ISP 団体)

○Regulation of Investigatory Power (RIP) Act が施行されれば、将来的には捜査へ協力した費用が支払われるようになるようだ。(Web コンテンツ企業)

○各企業は、法執行機関の要請により、「妥当な範囲」で協力することになっているが、「妥当な範囲」というのが明確でない。そこに費やすコスト(協力に必要な機材を確保する費用、スタッフの人件費等)を全て自社で負担することはできない。(ISP)

4.2 情報提供・情報交換及び技術協力

1996 年に警察側のイニシアティブにより、Internet Crime Forum が設立された。同フォーラムのメンバーは、警察やシークレットサービスのような法執行機関、その他関係各省庁及び産業界から構成され、3 ヵ月に一度ハイテク犯罪に関する情報･意見交換のためのミーティングをもっている。

その他にも政府関係者と産業界が情報交流を行う機会はフォーマル、インフォーマルベースで頻繁にある。業界団体の中には、英国内外の法執行機関への対応を担当す

る部署を設け、法執行機関との間で長期的な人間関係を築いている。

また、技術協力については、CERT チームが行っている。

■情報提供・情報交換及び技術協力について

○ISP・法執行機関双方に情報セキュリティについて活発に活動している人達が何人かおり、頻繁に日常からインフォーマルに情報交換をしているため、お互いをよく知っている。（ISP 団体）

○内務省、貿易産業省、その他ハイテク犯罪関連の政府機関と、情報セキュリティ・犯罪捜査について意見交換を行う非公式の機会を頻繁にもっている。（ISP 団体）

○企業秘密保持の観点から、技術・ノウハウに関する情報交換は行っていない。（Web コンテンツ企業）

○企業として各法執行機関と良い関係を築いており、制度上 Single コンタクトとなっていても何かあった場合に懇意にしているところ（例えばスコットランドヤード等）へ同時に情報を提供することがある。（Web コンテンツ企業）

○地方自治体間については、インターネットや情報セキュリティに関する情報交換・共有のできる NPO（Improvement and Development Agency（IDeA））が設立されている。また、地方自治体、警察、消防、住居及びその他行政機関の IT マネージャーの団体である SOCITM においても地方自治体の電子政府化やそれに伴う情報セキュリティに関する情報交換･提供が行われている。（政府機関）

○当社はバーチャルな CERT チームを持つ国際規模の情報セキュリティチーム FIRST（First Instance Response Security Teams）のメンバーであるため、ネットワークやソフトの脆弱性とその対応に関する情報を比較的早めに受け取ることができる。また、政府からも定期的に脆弱性に関する情報を受け取っている。（Web コンテンツ企業）

○児童保護に関するその他の慈善団体等とも協力し、情報収集を行っている。公共機関、慈善団体、地域警察等の各情報リソースを利用し、インターネット上の児童ポルノに関するサイトを撲滅する活動を行っている。（公益団体）

５．産業界における連携の状況

業界団体の中では、会員間で日常的に非公式の形で、人的ネットワークをベースに情報セキュリティに関する情報交換が行われている。

ISP 間でのユーザー情報の交換は法律（ Data Protection Act）上認められていない。

■産業界における連携の状況について

○ISP 間における情報交換はインフォーマルであり、ハイテク犯罪に関する連携は、フォーマルな形では行っていない。（ISP 団体）

○業界団体として、ISP 各社に法執行機関との関わり方についてアドバイスを行うことはある。（ISP 団体）

○当社が特定のユーザー（例え加害者であったとしても）の情報を他の ISP に渡すことは Data Protection Act により禁止されている。このような個人情報は、法執行機関にのみ渡すことができる。（ISP）

○児童ポルノについて監視を行っている IWF（Internet Watch Foundation）と緊密な関係であり、当社のセキュリティマネージャーは、IWF の理事会及び協議会メンバーである。（Web コンテンツ企業）

○国際組織にも加盟しており、国境をまたぐ捜査への協力も行っている。国際組織のメンバーとは年 4 回定期的に会合を持っており、情報交換・人脈の形成を行っている。（公益団体）

○ISP の業界団体や他の団体と共同でウェブサイトやニュースグループのレーティングを行っている。（公益団体）

6．人材育成

6.1 公的機関を対象とした人材育成活動

業界団体で、定期的に情報セキュリティに関する技術やハイテク犯罪についての講演・セミナー等を行う他、警察職員のための訓練プログラムを作成するなど、公的機関の人材育成に民間企業が積極的に協力している状況がみられる。

■公的機関を対象とした人材育成活動について

○セミナーを通じて、法執行機関の職員に対し、ハイテク犯罪及びその対応についてトレーニングを提供している。（ISP 団体）

○会員企業及び政府機関職員の啓蒙を目的とした、弁護士によるハイテク犯罪や情報セキュリティに関する法的課題についてのセミナーを主催している。法執行機関側からもプレゼンテーションを行ってもらい、双方の意見交換の場となるようにしている。（ISP 団体）

○（団体内の）訓練担当グループが SPOC 等警察官の情報セキュリティに関する訓練プログラム作成の責任を負っている。また、業界団体として、警察における情報セキュリティに関する訓練の質の向上を要請している。さらに下院にも働きかけた結果、警察官の訓練費用が国家予算として認められることとなった。（ISP 団体）

○SPOC の警察官は一週間の訓練に参加しなければならず、訓練修了時には、捜査協力の依頼等を行うことができるようになる認定証が授与される。（ISP 団体）

○内務省にできた High Tech Crime Unit は、各地域警察に少なくとも 2 人以上のネットワークやハイテク犯罪に詳しい捜査官を育成するために、教育訓練を行っている。（ISP 団体、Web コンテンツ企業）

○2001 年に Information Security (Inforsec) Training Paths and Competencies Scheme が政府より打ち出され、情報セキュリティに携わる政府関係機関職員に対して、その能力向上のための訓練が行われることとなった。これは内閣府が主管のスキームで、英国コンピュータ協会（British Computer Society）、セキュリティ管理組合（Guild of Security Controllers）及び英国教育機関の代表者の協力を得ている。（政府機関）

6.2 企業側の人材育成活動

基本的に社員の教育は、自社で行っているが、業界団体が主催するセミナー等には頻繁に参加している。

■企業側の人材育成活動について

○社員の訓練は基本的に各社自分で行っている。（ISP 団体、Web コンテンツ企業）

○ソフトウェアや児童ポルノそのものに関する訓練は団体内部で行っているが、法律に関する研修については、警視庁（スコットランドヤード）主催のものを受けている。（公益団体）
○Y2K 問題の時に政府による費用負担で、訓練を受けることができたが、情報セキュリティついては、知る限りでは特にそのような取り組みはない。（情報機器メーカー）

7．国・官公庁の取り組みに対する評価

7.1 産業界との連携の在り方

法執行機関及び産業双方はお互いの協力が必要との認識をもっている。

実効性のある協力関係を築くためには、産業界、法執行機関が互いを理解し、長期的な信頼関係を築くことが必要であることが指摘された。

■産業界との連携の在り方について
○理にかなった制度や法律をつくってもらうために、行政側に正しい知識を持ってもらうことの必要性と、新たにつくられる制度や法律が個人のプライバシーを侵害する危険性を防ぐために、法執行機関や行政への情報・知識面での協力は重要であると感じている。（Web コンテンツ企業）
○長期間にわたる信頼関係が必要である。（ISP 団体）

7.2 国･官公庁の取り組みの評価及び要望

情報セキュリティの産官連携の枠組みである Internet Crime Forum については、ハイテク犯罪に関する情報交換及び人的ネットワーク構築の場として、その効果が認められている。

一方で、捜査に関わる一連の手続きが非効率で時間がかかる、ハイテク犯罪に関する知識が欠如しているといった面で批判があった。さらに、ハイテク犯罪に対応した法制度の整備が進められているが、産業界からコストの面で不可能であるとともに、犯罪捜査上意味のないものとして大きな反対を受けている。

■国･官公庁の取り組みに対する評価について
①法制度整備（Anti-Terrorism Crime and Security Bill について）
○法執行機関は、どのデータをどうして保存したいのか、またどのように使うか分からないため、全てのデータの保存を義務付けようとしている。また、警察の捜査に時間がかかるため必要なデータを特定するのに非常に長い時間を有することから、長い期間の保存を望んでいる。しかし、データ保存には、保存するという行為以外

にそのデータの管理及びセキュリティの確保といった付随のコストと莫大なコストが必要となる。（ISP 団体企業）

○法執行機関が長期のデータ保存を望む意図も分かるが、コスト的にこれを行うのは不可能である。（ISP 団体、ISP）

○英国でデータ保存が義務付けられたとしても、グローバルに展開している ISP は、そのデータが他国に保存してある場合など問題となるのではないか。（ISP 団体）

②人材

○ハッキングやウイルスについては、地元の警察に通報することになっているが、一般的に英国の警察のネットワーク犯罪に対する対応はうまくいっていない。警察官の多くは、訓練を受けていないため、対応の仕方がよくわかっていないケースが多い。ハイテク犯罪が深刻なものと受け取られておらず、また政治的にも情報セキュリティ対策について大きな関心をもたれていないことがネックとなっている。（ISP 団体）

③捜査体制

○警察におけるあらゆる手続きが非常に不適切、官僚的、非効率であり遅い。警察側もそれを認めている。（ISP 団体）

○一度に多くの犯罪捜査を抱えており、一つの事件が解決するのに時間がかかり過ぎる。（ISP 団体）

○警察は、どのような情報が欲しいか特定せずに、持っている情報全てを提供しろというスタンスである。技術者の立場としては、全ての情報よりも、役に立つ情報のみを提供する方法にしたい。（ISP 団体）

○ハイテク犯罪に対する認識が、政府・法執行機関側で希薄である。英国の警察は、43 の地域警察に分かれており、全国ベースでこれを統括する組織が存在しない。このため、各警察組織は自分の管轄の地域のみに意識が集中する傾向があり、横断的に全体を見渡すことができていない。ハイテク犯罪はグローバルであるとの認識を持つべきである。この点では、内務省にできた High Tech Crime Unit により主導権が発揮されはじめたことは、評価できる。（Web コンテンツ企業）

○犯罪が複数国間で起こった際の国際間の協調体制が現状では非常に脆弱であることが懸念される。（ISP 団体）

○児童ポルノについては法執行機関の対応に満足している。（公益団体）

④産官連携

○Internet Crime Forum はうまくいっている取り組みの一つである。成功の秘訣は、同じ人が長期間参加しているため、知識レベルがあがるとともに人的つながりも強くなっている点である。これとは対照的に内務省の取り組みで、児童ポルノ犯罪を主に扱っている Internet Task Force という枠組みがあるが、これは逆に参加者が

頻繁に変わるためかうまくいっていないと聞いている。（ISP 団体）

○情報提供等の捜査協力を行っても、その情報がどのように使われたのかフィードバッグが法執行機関の方からない。産業界としては、自分たちの提供した情報がどのように使われたのか、知りたい。そのことによって、次の機会にどうすれば犯人逮捕にもっと貢献することができるか考えることができる。（ISP 団体）

⑤政府によるキャンペーンについて

○政府が 2001 年に行ったインターネットを安全に利用するための意識向上キャンペーンについては、インターネットを利用することに対する恐怖心を煽っただけである。（ISP 団体）

■要望について

○事件発生から捜査に取りかかり産業界に情報データの依頼をするまでのプロセスに時間がかかりすぎている。このため、警察側が長い期間のデータ保存を望んでいるわけであるが、ISP にそのような依頼をする前に警察内における手続きを効率化して欲しい。（ISP 団体）

○法執行機関の職員はセキュリティに関する知識と基本的なスキルを身につけて欲しい。（ISP 団体、Web コンテンツ企業）

○ハイテク犯罪の多くは、詐欺や児童ポルノ等、それ自体が新しい犯罪というわけではなく、インターネットを利用してこのように古くからある犯罪が行われるだけである。現在、警察は、ハイテク犯罪の技術的な面が理解できないばかりによほど大きな事件以外は取り組んでくれないため、全て ISP の方で対応している。普通に路上で起きる事件と同様にきちんと対応して欲しい。このためにも、これらの犯罪がインターネット上で行われる場合にはどのように取り組めばよいのかといったことに必要な知識・専門性を身に付けて欲しい。（ISP 団体）

Ⅳ　ドイツ

１．情報セキュリティに対しての認識

企業、連邦政府、法執行機関におけるハイテク犯罪への理解は進んでいる。しかし、地方自治体や一般消費者レベルはまだ十分ではない。ドイツの消費者は個人情報やクレジットカード情報等をインターネット上でやり取りすることに対して抵抗があるため、電子商取引やインターネットバンキングの利用は低調である。

ドイツ国内で最も関心が高く、また近年増加している問題は違法・有害情報である。警察への通報件数も最も多い。中でも児童ポルノ対策が大きな問題になっている。その他、暴力や人種差別等の表現を含むコンテンツへの対策の必要性が指摘されている。特に 2002 年 4 月のエルフルト銃撃事件（退学処分になった学生が教師を射殺した事件）以降、コンピュータゲームやビデオ、Web サイトの暴力表現への批判が高まっている。また、極右の Web サイトが急増していることが問題となっている。1996 年に 32 サイトであったのが 2000 年には 800 サイト、2001 年には 1300 サイトに達している。

その他、Dialler（ダイヤル Q2 と類似の 190 番に自動接続するプログラム）やスパムメールが問題になっている。特に Dialler については多くの機関から問題性が指摘された。

コンピュータウイルス、不正アクセス、DoS 攻撃等も問題となっているが、警察への通報件数は多くない。近年、企業は外部からの攻撃よりも内部犯罪を危惧するようになってきている。

OS 事業者は海賊版ソフトを問題視している。オンラインオークション等で悪質な偽造品の取引が行われている。一方で海賊版ソフトに対する一般消費者の認識は低い。

２．情報セキュリティ対策のための体制

ドイツは連邦制の行政機構を取っていることもありハイテク犯罪に対する統一的なガイドラインやマニュアルは提供されていない。BSI（Federal Agency for Security in Information Technology)を含む、連邦政府から提供されるマニュアル等は推奨情報であり、連邦政府、州政府、地方自治体への強制力は持たない。各機関は個々のポリシーに基づいてセキュリティ対策を行っている。

個々の行政機関には、IT Security Officer と IT Security Management Team を設置することやセキュリティポリシーを策定することが期待されているが、地方自治体の全てが実践している段階にはない。その他、ある程度以上の規模を持つ組織においては、Data Protection Officer の設置が期待されている。

海賊版ソフトを問題視しているOS事業者では、海賊版ソフト対策や消費者保護を行う専門組織を設置している。さらに違法ソフトウェアのオンライン販売を国際的に監視するチームを置いている。

■情報セキュリティ対策のための体制について

○行政機関に対しては、IT Security Officer と IT Security Management Team を設置することが期待されているが、地方自治体の全てが IT Security Officer を設置しているわけではない。その他、ある程度以上の規模を持つ組織においては、Data Protection Officer を設置することが期待されている。（連邦政府機関）

○行政機関向けに IT Security Handbook、IT Tool Guide を提供している。IT Security Handbook には、IT Security Officer の果たす役割が述べられている。IT Tool Guide には情報セキュリティに利用できるツールの紹介がなされている。これらのハンドブック、ガイドラインは推奨情報であり、行政機関には準拠する義務はない。個々の機関の判断により利用を行っている。（連邦政府機関）

○IT を利用する全ての行政機関は、コンティンジェンシープランなどを含むセキュリティポリシーを策定することが期待されている。しかし、現在のところ全ての地方自治体がセキュリティポリシーを策定しているわけではない。（連邦政府機関）

○セキュリティポリシーは現在策定中である。IT Security Officer の設置もまだ行っていない。ただし、e-Government への対応に向けて規制や対策の在り方についてワーキンググループで検討を行っている。将来的には、セキュリティポリシーと情報セキュリティ対策に向けた組織体制を整える予定である。（地方自治体）

○ドイツでは、2005 年までに、全ての連邦政府機関がオンラインサービスを提供することを目指した「Bund Online 2005」を進めている。e-Government の実現に向けて、BSI では e-Government Handbook を提供している。このハンドブックでは、e-Government における情報セキュリティの重要性を強調し、暗号や認証などに関する情報を提供している。（連邦政府機関）

○海賊版ソフト対策や消費者保護を行う専門組織を国毎に設置している。その他、ドイツ国内ではないが、違法ソフトウェアのオンライン販売を監視する国際的なチームを設置している。（OS 事業者）

3．情報セキュリティ確保のための対策及び対応

3.1 事前対策（予防）

3.1.1　情報セキュリティ対策

情報セキュリティ対策としては、ファイアウォールやアンチウイルスソフトといった通常の対策が多くの企業や行政機関で行われている。ただし、こうした製品は正しく設定し、定期的に更新しなければ有効ではないとの指摘もある。

ハイテク犯罪に関するモニタリングを行うことは法執行機関だけに許されている。ISP等がモニタリングを行うことはない。

BSIからDoS攻撃、コンピュータウイルス対策に関するガイドラインが提供されている。行政機関向けにBaseline Protection Manual for IT Securityが提供されている。このマニュアルの利用は強制されていないが、州政府や地方自治体に対して、最低限取り組むべきITセキュリティ対策を知らせる効果があった。

BSIではその他に、行政機関の情報セキュリティ対策を診断し、改善に向けた対策方法の指導を行っている。セキュリティ診断は一律に行っているのではなく、要望のあった行政機関に対して実施している。

■情報セキュリティ対策について

○多くの企業がファイアウォールやアンチウイルスソフト等の市販の製品を利用している。ただし、正しく設定し、定期的に更新する必要がある。（ISP団体）

○ファイアウォール、アンチウイルスソフト、IDSを利用している。職場からのインターネット接続はほとんどの職員について認めていない。業務上必要なサイトへの限定的な利用だけを認めている。コンピュータウイルスへの感染を防ぐために、機能を限定した電子メールシステムを利用している。（地方自治体）

○ハイテク犯罪に関するインターネット上のモニタリングは法執行機関だけが行うことができる。（州警察）

○DoS攻撃、コンピュータウイルス対策に関するガイドラインを提供している。その他、行政機関を対象にBaseline Protection Manual for IT Securityを提供している。このマニュアルの利用は強制されていないが、州政府や地方自治体に対して最低限取り組むべきITセキュリティ対策を知らせる効果があった。（連邦政府機関）

○行政機関に対してセキュリティ対策の改善アドバイスを行っている。チェックを依頼してきた行政機関に対して、セキュリティ上の問題点の特定と対策方法を指導している。チェックは行政機関の依頼に基づいており、一律に監視しているわけではない。（連邦政府機関）

3.1.2 違法・有害情報対策

ドイツ刑法（Strafgestzbuch-StGB）では違法・有害情報に関する規定があり、違法・有害情報を提供しているコンテンツプロバイダーは法的な責任を負う。アクセスプロバイダーの法的責任は、自社のサービス上における違法コンテンツの存在を認識し、かつ当該情報が法的にも現実的にも削除することが可能であり妥当な場合にのみ生じる。

ドイツ刑法での違法・有害情報に関する規定

- § 130 StGB ? Demagogy
- § 130 a StGB ? Instruction on illegal actions
- § 131 StGB ? Glorification of violence and the portraying of racism.
- § 86 StGB ? Distribution of propaganda material from illegal organisations
- § 87 StGB ? Activities that lead to sabotage
- § 184, 3 StGB ? Distribution of hard pornographic material, especially to children.

ドイツ国内では、違法・有害情報の通報を受け付けるホットラインが運用されている。ホットラインでは、通報された情報の違法性・有害性を調査し、削除要請等を行っている。

ISP や民間団体等によるネットワーク上の違法・有害情報の監視は行われていない。法律上、法執行機関以外が違法・有害情報の監視を行うことは認められておらず、基本的にはユーザーなどの通報や苦情を受けてから対応をしている。法執行機関による監視は、連邦警察局（BKA）と一つの州警察が行っている。他の州警察では監視を行っていない。

違法・有害情報対策としては、フィルタリングソフトの利用や教育等の重要性が指摘されている。ただし、フィルタリングソフトの利用は個々のユーザーが行うべきものであり、アクセスプロバイダーに利用を義務づけることは適切でないという指摘がある。

■違法・有害情報対策について

○提供する情報の責任はコンテンツプロバイダーが負う。アクセスプロバイダーの法的責任は、自社のサービス上における違法コンテンツの存在を認識し、かつ当該情報が法的にも現実的にも削除することが可能であり妥当な場合にのみ生じる。（コンテンツプロバイダー団体）

○運用しているホットラインでは、ユーザーから違法・有害情報の通報を受け付けている。ホットラインは通報を受けてから該当情報の調査を行う。自社のサービス上で違法・有害情報が流通することを防止・抑制するために、多くの ISP やコンテンツプロバイダーが、ホットラインのニュースグループ査定サービスの利用を行っている。（ISP 団体）

○違法・有害情報の通報を受け付けるホットラインを提供している。e-mail やチャット等の個人間におけるコミュニケーションについては対象としていない。こうした場合には、法執行機関への通報や弁護士へ相談するようアドバイスしている。（コンテンツプロバイダー団体）

○ISP や民間団体等によるネットワーク上の違法・有害情報の監視は法律上認められていない。法執行機関だけが法律上、監視を行うことが認められている。（コンテンツプロバイダー団体）

○法執行機関によるネットワーク監視は法的に認められている。州警察のネットワーク犯罪捜査チーム（Network Crime Investigation Unit）は州の法律に基づき違法コンテンツの監視を行っている。他の州警察は監視を行っていない。監視は、Web サイトの閲覧やチャットルームへペンネームを用いて参加することにより行っている。（州警察）

○違法・有害情報対策は、フィルタリングソフトの利用や教育によって進めるべきである。（ISP 団体）

○違法・有害情報対策としてはフィルタリングソフトの利用が有効である。ただし、フィルタリングソフトも最終的な解決とはならない。違法ではない情報へのアクセスを阻害することもある。団体では Web サイトを通じてフィルタリングソフトの情報提供を行っている。国際的で柔軟性のある規格として ICRA 基準を支持している。ユーザーが利用を望まない情報の登録を行うことができる。（コンテンツプロバイダー団体）

○デュッセルドルフでは、アクセスプロバイダーに対してフィルタリングソフトの利用命令が出された。しかし、アクセスプロバイダーが提供しているのは、インターネット接続サービスであり、コンテンツの監視機能は含まれない。アクセスプロバイダーへのフィルタリングソフトの義務づけは違法・有害情報に対する適切な手段ではないと考えている。フィルタリングソフトの利用は学校や大学、家庭の PC などだけで有効である。ドイツ刑法には、違法・有害情報に関する規定があり、こうしたサイトの提供者は法的責任を負う。こうした規制で十分である。（連邦政府機関）

3.1.3　情報・データ漏洩対策

市民がオンライン上で行政サービスの申請を行うことはデータ保護法で認められておらず、署名などが必要な手続きは窓口で行う必要がある。また、企業においては、データ保護に関するポリシーを策定・公開し、ユーザーの同意を得てから個人情報を得るなどの配慮がなされている。

■情報・データ漏洩対策について

○市民がオンライン上から行政サービスの申請を行うことはデータ保護法で認められていない。そのためネットワーク上でのユーザー認証は行われていない。署名などの個人情報が必要な手続きの場合には、窓口で対面により行う必要がある。（地方自治体）

○ある程度以上の規模の行政組織には Data Protection Officer を設置することが期待されている。（連邦政府機関）

○データ保護に関するポリシーを Web サイトに掲載している。ポリシーの中で責任を持って個人情報を保護することを表明している。（OS 事業者）

○Web サイトで提供している多くのサービスにはユーザー認証の必要がない。特別なサービスを利用する時にだけ、ユーザーから個人情報を得ている。個人情報をどのように保管し利用するのかについては説明を行い、ユーザーの同意を得た場合にのみサービス提供を行っている。（OS 事業者）

3.1.4　ネットワーク詐欺等の不正行為対策

ドイツでは、現在ダイヤル Q2 と類似したサービスである Dialler が大きな問題となっている。日本と同様、ダイヤルアップ接続の設定を Dialler サービス経由のものに勝手に変更するプログラムや、Dialler 上で提供されている詐欺的なサービスや商品購入に誘導するポップアップ広告等が問題となっている。Dialler の概要や問題点等に関する情報提供が警察や消費者団体、自治体などから行われている。

OS 事業者では海賊版ソフト対策に力を入れている。ネットワークオークションなどを通じて、海賊版ソフトが取引されているが、それらの多くは偽物であり完全なソフトウェアでないものも多い。海賊版ソフト対策として、OS 事業者は普及・啓発活動を行っている。また、消費者が購入した製品が正規のものであるかどうかを検査するチェックサービスを提供している。その他、海賊版対策の専門部署で実際に製品購入を行い、海賊版ソフトの取引状況の把握を行っている。

■ネットワーク詐欺等の不正行為対策について

○インターネットを利用している際にユーザーを Dialler サービスに誘導するポップアップ広告が表示され、Dialler を通じたサービスや商品の購入を促す。これらのサービスは詐欺であることが多い。警察では市民に対してこれらのサービスを利用しないようプレスリリースを発表した。(州警察)

○Dialler が大きな問題となっている。インターネット利用中にダイヤルアップ自動設定プログラムがユーザーの PC にインストールされ、Dialler サービスによる接続サービスを利用するよう設定が変えられる。その結果、多額の接続料金が請求されるというものである。ダイヤルアップ自動設定プログラムの概要や問題点についてまとめたリーフレットを作成し、消費者相談センター(Consumer Advice Center)で消費者に配布している。(消費者団体)

○市とは関係のない企業により、Dialler サービスにおいて市のサービスに関する情報提供が行われている。このサービスを利用すると 1 分あたり 1.86 ユーロの課金がなされる。市のサービスに関する情報は Web サイトや市役所に電話することにより簡単に得ることができるため、市民は Dialler サービスを利用する必要性はない。市では、Web サイトや Citizen Information Center を通じて、市の情報を入手するための適切な方法に関する情報を提供している。(地方自治体)

○海賊版ソフトへの対応が一番の問題である。ネットワークオークションを通じて、安価に取引されている。こうした場で取引される製品には偽物が多く、単なる部品やハンドブックでしかなく完全なソフトウェアでないものもある。オンライン詐欺といえる。(OS 事業者)

○海賊版ソフト対策としては、報道発表やメールニュース、Web サイトを通じた普及・啓発活動を行っている。その他、消費者が購入した製品が正規のものであるかどうかを検査するチェックサービスを提供している。年間 90,000 製品のチェックを行ったところ 99%が違法なものであった。その他、海賊版ソフトの専門部署では社員が製品を実際に購入して、取引状況の把握を行っている。(OS 事業者)

3.2 問題発生時の対応

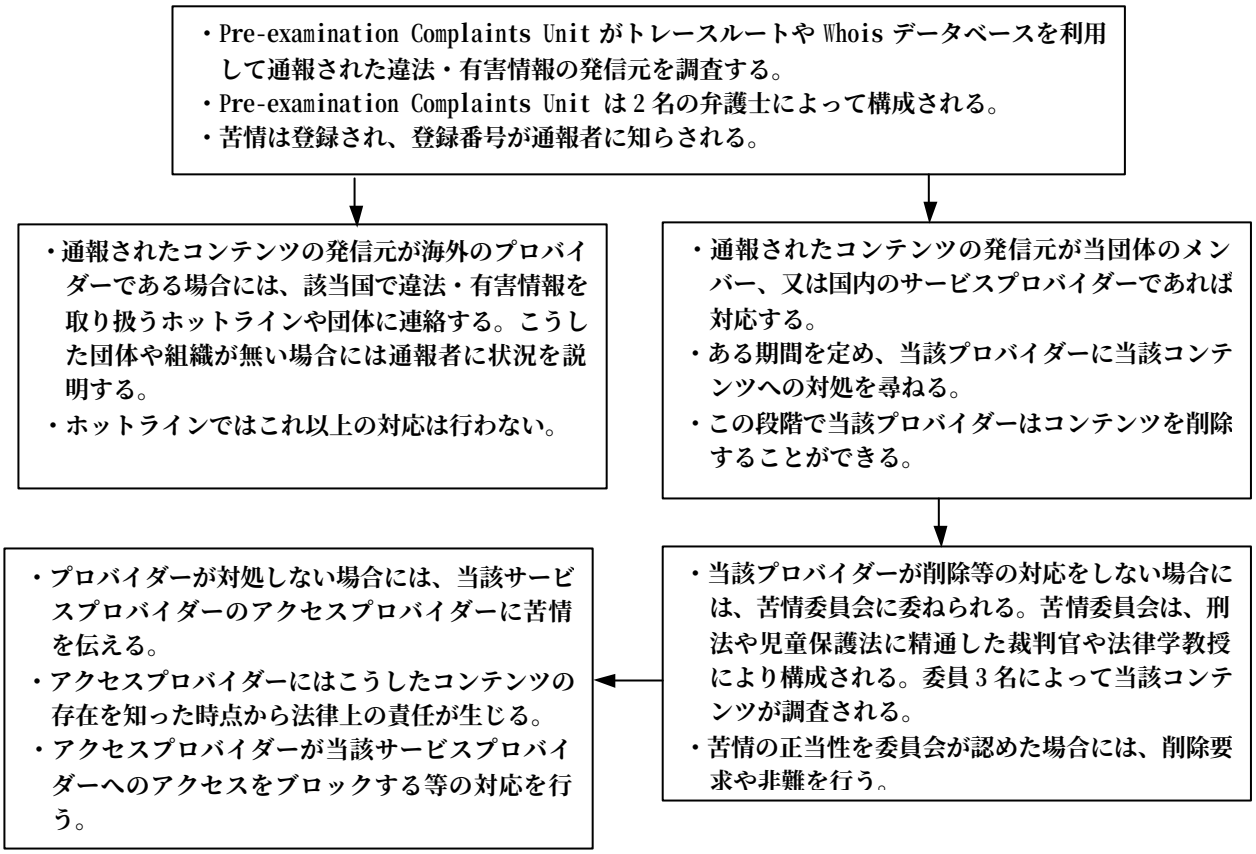
ハイテク犯罪の種類や影響範囲などにより、通報や捜査に関する手順は異なる。現状はケースバイケースで取り扱われており、標準的な手順は決まっていない。

3.2.1　違法・有害情報確認時の対応

ネットワーク上で違法・有害情報が見つけられた場合には、ISP 団体やコンテンツプロバイダー団体が開設しているホットライン又は警察へ通報が行われている。

ホットラインでは通報された情報を調査し、違法なものについては削除するようコンテンツプロバイダーに要請している。ここ数年、通報された違法・有害情報の多くが削除されるなど効果をあげている。もしもコンテンツプロバイダーが要請に従わない場合には、当該コンテンツプロバイダーが利用しているアクセスプロバイダーへ対応を要請する。また当該コンテンツプロバイダーが団体に所属している場合には、除名処分を行う。ホットラインから警察への通報は通常行われていないが、生命や健康への危険が迫っている場合には直ちに通報を行っている。

ホットラインにおける違法・有害情報への対応手順の例



違法・有害情報の警察への通報は市民から行われるケースが多い。企業からの通報はあまり行われていない。通報は電話や e-mail、FAX で寄せられている。警察は通報されたコンテンツを調査し、関連法規に照らし合わせ本当に違法情報であるかどうかを判断している。違法情報を掲載しているコンテンツプロバイダーの特定がなされると、当該 Web サイトへアクセスできないようにするといった対応が警察によって即座に行われる。

■違法・有害情報確認時の対応について

○Usenet Newsgroup における違法・有害情報の通報を受け付けるホットラインを開設している。通報は e-mail 等によって行える。通報を受け取った後、コンテンツの調査を行う。（ISP 団体）

○違法・有害情報のホットラインへの通報は Web 上から行える。証拠を添付することも可能である。通報者にはホットラインから通報を受理した旨とコンテンツ調査のスケジュールが知らされる。通報者には、その後の進捗や対処結果を回答している。（コンテンツプロバイダー団体）

○ホットラインに通報された違法・有害情報の多くは削除されている。（コンテンツプロバイダー団体）

○ホットラインから法執行機関への通報は通常行っていない。ただし、生命や健康への危険が迫っている場合には通常の手順を踏まずに警察へ通報する。警察へは、当該コンテンツに関する URL 等の情報とともに文書で送っている。ただし、警察からは捜査結果に関するフィードバックは行われていない。（コンテンツプロバイダー団体）

○違法・有害情報の警察への通報は市民から行われるケースが多い。企業からの通報はあまり行われていない。通報は電話や e-mail、FAX で寄せられている。（州警察）

○通報されたコンテンツの調査を行い、関連法規と照らし合わせ、本当に違法な情報であるかどうかを判断している。違法情報を掲載しているコンテンツプロバイダーの Web サイトの特定がなされた場合、警察は当該 Web サイトへのアクセスをブロックするといった対応を即座に行う。（州警察）

3.2.2　海賊版ソフト確認時の対応

OS 事業者では、消費者が購入したソフトウェアが正規なものであるかどうかを確認するチェックサービスを提供している。チェックの結果、購入したソフトウェアが海賊版であることがわかったユーザーは、OS 事業者に海賊版ソフトの購入元や提供者に関する情報を提供することにより、OS 事業者から正規の製品を得ることができる。

法執行機関から OS 事業者に海賊版ソフトの取引に関する情報が寄せられる場合もある。

OS 事業者は海賊版ソフトの供給者に対して、様々な対応を行っている。民法に基づいて警告を行うことや、法執行機関に通報することもある。捜査や刑事告訴など、さらなる対応を行うべきであると判断した場合に通報を行う。

■海賊版ソフト確認時の対応について

○購入した製品が正規のものであるかどうかのチェックの結果、海賊版であることがわかったユーザーは、OS 事業者に海賊版ソフトの購入元や提供者に関する情報を提供することにより、OS 事業者から正規の製品を得ることができる。（OS 事業者）

○法執行機関から OS 事業者に海賊版ソフトの取引に関する情報が寄せられる場合もある。例えば、オークションサイトで OS 事業者製の海賊版ソフトが取引されている疑いがあるという情報が寄せられている。（OS 事業者）

○海賊版ソフトの供給者に対しては、様々な対応を行っている。民法に基づいて警告を行うことや、法執行機関へ通報することもある。法執行機関への通報は捜査や刑事告訴などさらなる対応が必要と判断した場合に行う。（OS 事業者）

3.2.3　不正アクセス等発生時の対応

不正アクセス等のインシデント発生を法執行機関へ通報する義務は課されていない。通報はボランティアベースで行われている。

BSI が設置している CERT（Computer Emergency Response Team）が連邦政府機関のコンタクトポイントとなっており、連邦政府のネットワークに対する DoS 攻撃やコンピュータウイルス等に対応する。州政府や地方自治体においても、独自の CERT を設置する取り組みが進められている。

全ての行政機関はハイテク犯罪発生時にどこの誰に報告すべきかを定めたガイドラインを作ることが期待されており、BSI が提供している IT Security Handbook の中にも示されている。

■不正アクセス等発生時の対応について

○ISP 等に対して法執行機関と協力する義務は課されておらず、インシデントの報告も

義務ではない。協力はボランティアベースで行われている。（州警察）

○CERT が連邦機関の IT セキュリティに関するコンタクトポイントとなっている。連邦政府のネットワークに対する DoS 攻撃やコンピュータウイルスへの対応を行っている。州政府や地方自治体においても、独自の CERT を設置する取り組みが進められている。（連邦政府機関）

○全ての行政機関にはハイテク犯罪発生時にどのような対応をとるべきかを定めたガイドラインを策定することが期待されている。提供している IT Security Handbook の中でも、対応マニュアルの例が記載されている。例えば、不正アクセスやスパイ行為、不正なデータ操作などが行われた場合には、IT Security Officer に連絡すべきであるとされている。いくつかの自治体では Virus Protection Officer の設置も行われている。（連邦政府機関）

4．法執行機関との連携の状況

4.1 捜査協力

4.1.1　捜査協力の内容

ドイツでは、ISP にログ保存の義務づけはなされていない。ログの保存は事業上の観点から ISP が自発的に行っているものであり、保存状況も企業により異なる。大手 ISP が通常 80 日間ログを保存しているのに対し、より短期間しか保存していない企業や全く保存を行っていない企業も存在する。

法執行機関がハイテク犯罪を捜査する上で、ISP や企業にログ等の顧客情報の開示を求めるためには、裁判所命令を要する。ISP や企業はデータ保護法により顧客情報を保護する義務があるが、裁判所命令に基づく要請がなされた場合には、顧客情報を開示しても法的な責任は問われない。

現在、ISP にログ保存の義務化や保存期間の延長に関する議論が行われているところである。法執行機関は義務づけを求めているが、ISP 団体は負担が大きくなることから反対している。

■捜査協力の内容について

○ISP へのログ保存の義務づけはなされておらず、ログの保存は自発的に行われている。保存状況も企業によって異なり、大手 ISP が通常 80 日間保存しているのに対し、より短期間のみ保存している企業や全く保存を行っていない企業も存在する。（州警察）

○法執行機関が裁判所命令に基づき顧客情報の開示を求めた場合には、企業や団体は法執行機関に顧客情報を提供しなくてはならない。裁判所命令がなければ、法執行

機関が企業や団体の内部を捜査することや証拠を押収することはできない。(州警察)

○裁判所命令による開示要求がなされた場合、ユーザーID やアクセス時間、特定の時間に利用していたコンテンツ等のユーザー情報を開示しなくてはならない。(州警察)

○データ保護法に基づき顧客情報を保護している。ただし、裁判所命令に基づく法執行機関や検察官による捜査に対しては、顧客情報を提供することは問題なく行える。(OS 事業者)

○現在、ログの保存義務を ISP に課すかどうか、その場合の保存期間をどの程度にするかといった点が議論されている。保存期間としては 6 ヶ月という案もでているが、これより長くすべき、短くすべきとの意見で分かれている。(ISP 団体)

4.1.2 コスト負担

ログを保存するためのコストは ISP が負担している。ISP は、現在よりもさらに長期間のログ保存に対しては、コスト負担が大きいことから反対している。

■コスト負担について

○現在、ログ保存のコストは ISP が負担している。しかし、これ以上のコスト負担は難しい。今、議論されているような 6 ヶ月間のログ保存が義務づけられると、現在の市場環境では負担できない。(ISP 団体)

4.2 情報提供・情報交換及び技術協力

企業等と法執行機関との間での情報交換に関する制度的な枠組みはない。

しかし、企業や団体、行政機関等と法執行機関との間のコミュニケーションはインフォーマルな形で密接に行われている。特定のハイテク犯罪に関する情報交換だけではなく、今後の法規制の在り方など、様々なレベルでの情報交換がなされている。

また、ドイツを情報社会に適応した国とするために組織された Initiative D21 においては、インターネット関連企業、メディア関連企業、学校、大学、行政機関等が幅広く参画して活動を行っている。Initiative D21 のワーキンググループの一つとして Internet Security and Trust in the Network があり、インターネット上のセキュリティを確立し信頼形成を高めるための取り組みが進められている。

■情報提供・情報交換及び技術協力について

○ISP 団体と BSI、BKA 等の関連する機関との間では、インフォーマルな形での協力が

行われている。法執行機関に対してインターネット上のセキュリティに関するトレーニングの提供も行っている。（ISP 団体）

○ホットラインに通報されてきた違法コンテンツについて、必要に応じて法執行機関と情報交換を行っている。その他、BKA との間では定期的な情報交換や議論を行っている。また、児童保護法やドイツ刑法の改正議論にも参加している。(コンテンツプロバイダー団体)

○インターネットやメディア関連産業、学校、大学、行政機関等により構成される Initiative D21 は、ドイツを情報社会に対応した国とするための活動を行っており、様々な業種にわたる 300 の企業が参画している。Initiative D21 のワーキンググループの一つ Internet Security and Trust in the Network では、インターネット上の信頼を形作ることを目的としており、CERT の設置に向けて取り組みを進めている。こうした信頼形成のための取り組みを行うことにより、インターネットの利用が進むものと考えている。(連邦政府機関)

５．産業界における連携の状況

業界団体を中心に、参加企業同士でインフォーマルな情報交換が行われている。

ISP 団体では、メンバー間でのインフォーマルな情報交換が行われている。Working Group Security（WG Security）を設立し、セキュリティ問題に対する経験や情報の交換を行っている。また、CERT の設立も目指している。その他、ISP 団体では企業におけるセキュリティ意識の向上を目指し、企業の管理者向けに「The Best Current Proactive Law and Security」を提供している。

コンテンツプロバイダー団体では、運用しているホットラインの活動にもとづき児童保護に関連した助言をメンバー企業であるかどうかを問わずに行っている。また、関連する法規制やフィルタリングプログラムなどに関する情報を提供している。

OS 事業者は、業界団体を通じて、海賊版ソフト対策の情報交換を行っている。

地方自治体に対しては、BSI が Web や雑誌を通じて情報提供を行っている。さらに、地方自治体に対して支援を行うホットラインを設けており、電話や e-mail で相談を行うことができる。

■産業界における連携の状況について

○ISP 等インターネット関連企業により構成される団体では、メンバー間の密接な協力関係のもと、インフォーマルで大量の情報が交換されている。2001 年に WG Security を設立し、セキュリティ問題への対処経験や情報の交換を行っている。（ISP 団体）

○CERT Response Team）の設立を目指している。（ISP 団体）
○企業内での情報セキュリティ意識の向上が必要である。特に管理者の意識を高める必要がある。そこで「The Best Current Practice Law and Security」等のガイドラインを管理者に提供している。（ISP 団体）
○コンテンツプロバイダー団体ではメンバー企業であるかどうかを問わず、児童保護に関連した助言を行っている。関連する法規制やフィルタリングプログラム等に関する情報を提供している。（コンテンツプロバイダー団体）
○大手のコンテンツプロバイダーは当団体のメンバーである。また、多くのコンテンツプロバイダーはなんらかの業界団体に参加している。当団体は他の団体とのリンクとしての役割も果たしているため、ニュースレターの発行や会合の開催等を行うことにより、団体経由により関連情報を多くのコンテンツプロバイダーに提供することができる。（コンテンツプロバイダー団体）
○OS 事業者ではソフトウェアメーカー団体（BSA：Business Software Line)、ハイテク企業団体（Bitcom)、ソフトウェア業界団体（VSI：German Association of the Software Industry）を通じて、海賊版ソフト対策等に関する情報交換を行っている。（OS 事業者）
○Web 上で様々な情報提供を行っている。登録することにより、最新の情報を入手することができる。また、雑誌「Communication and IT Security」の発行を行っている。（連邦政府機関）
○コンピュータウイルス等の問題に直面した地方自治体に対する支援を行うホットラインを設けており、電話や e-mail でコンタクトすることが可能である。（連邦政府機関）

６．人材育成

6.1 公的機関を対象とした人材育成活動

公的機関を対象とした情報セキュリティに関するトレーニングを業界団体が行うなど、積極的な協力が行われている。

行政機関に対しては、BSI から様々なガイドラインが提供されている。その他、行政機関向けのトレーニングは連邦政府により提供されている。

法執行機関では、連邦政府や民間企業、外国政府が提供するトレーニングに参加するとともに、内部でも訓練が行われている。

■公的機関を対象とした人材育成活動について

○法執行機関を対象とした情報セキュリティに関するトレーニングを定期的ではないが単発で行っている。（ISP 団体）

○公的機関向けの IT セキュリティに関するトレーニングを提供していた。現在は、Fachhochshule Bund が行っている。公的機関の IT マネージャを対象としている。各団体の IT マネージャが参加し、セキュリティに関する知識を習得する。IT マネージャは習得した知識を実践するとともに、組織の他の人員に知識を伝えている。（連邦政府機関）

○OS 事業者では、警察向けのトレーニングを行っている。製品に関連した内容であり、偽造製品との見分け方などが含まれる。（OS 事業者）

○警察ではインターネット犯罪やインターネット関連産業に関連する多くのトレーニングを受けている。これらのトレーニングは BSI や BKA 等の連邦政府と産業界によって行われている。その他、外国機関が開催しているトレーニングへの参加も行っている。例えばスイス警察がスイス検察庁やインターネット産業と協力して開催されたトレーニングに参加している。他にも英国や仏国で開催されたトレーニングにも参加している。（州警察）

○連邦政府によるトレーニングは、連邦政府、州政府、BKA、州警察、インターネット産業、消費者団体などの様々なメンバー間での議論の場としての役割を果たしている。（州警察）

○警察内でのトレーニングも行われている。警察に入る前に、インターネット産業で働いており、インターネットやコンピュータの専門家である職員が講師となっている。トレーニングには、インターネット関連犯罪や対策に関する知識を必要とする職員に対して行われている。（州警察）

6.2 企業側の人材育成活動

企業内の情報セキュリティ対策を高めるためには、社員の意識向上、特に管理者における認識を高める必要があると考えられ、ハンドブックの提供などが行われている。

■企業側の人材育成活動について

○ISP 団体では、企業内での情報セキュリティ意識向上を目指している。特に管理者の意識を高める必要を感じており、「The Best Current Practice Law and Security」等のガイドラインを管理者に提供している。（ISP 団体）

6.3 一般ユーザーへの普及・啓発活動

BSI が積極的に一般ユーザーへの普及・啓発活動を行っている。様々なレポートを提供するとともに、コンピュータウイルス対策に関する CD-ROM の提供なども行っている。業界団体の取り組みも盛んである。地方自治体では、情報セキュリティへの理解の度合いによって取り組み方が異なっている。消費者団体はリソースの問題から積極的な対応は行えていない。法執行機関は一般ユーザーへの普及・啓発活動はあまり行っていない。

違法・有害情報対策に関しては、業界団体がガイドブックの提供やフィルタリングソフトの情報提供等を行っている。その他、現在問題となっている Dialler に対しては、消費者団体、地方自治体、法執行機関などが Web やパンフレット等を通じて情報提供を行っている。

■一般ユーザーへの普及・啓発活動について

○コンピュータウイルス関連の啓蒙活動は、主に連邦政府内務省の BSI が行っている。BSI では様々な報告書を発行するとともに、最近では消費者向けの CD-ROM を提供している。CD-ROM にはインターネットセキュリティやコンピュータウイルスへの対策方法に関する情報が含まれている。（消費者団体）

○一般ユーザー向けの情報提供や普及啓発活動の状況は、地方自治体の情報セキュリティに関する理解によって異なる。自治体によってハイテク犯罪に対する理解は異なり、全ての団体で学校や図書館等と連携した取り組みを行っているわけではない。いくつかの自治体では、Web サイト上で関連情報の提供などを行っている。（連邦政府機関）

○青少年に対する有害情報対策やインターネットセキュリティ対策は重要な問題であるが、人員が限られていることもあり、啓蒙活動などは実施していない。今後もリソースの問題からインターネットセキュリティに関する啓蒙活動などは行えない。（消費者団体）

○保護者に対して、安心して子供に Web 利用を行わせるためのガイド「Save Surf Guide」

を提供している。その他、児童保護に関連した様々な記事を定期的に出している。また、現在、他の児童保護の団体との協力のもと、一般ユーザー向けに配布するパンフレットの作成を進めている。（コンテンツプロバイダー団体）

○海賊版ソフト対策の普及啓発活動を行っている。広報活動を通じてソフトウェア・チェックサービスの利用が広がっている。（OS 事業者）

○Initiative D21 の中で学校等の教育分野に対して、特別な製品ライセンスの提供を行っている。（OS 事業者）

○現在、ドイツで最も問題となっているのはスパムメールと Dialler（ダイヤルアップ自動設定プログラム）である。Dialler はホームページ閲覧中に勝手に PC にインストールされ、ダイヤル Q2 と同種のサービスである 190 サービスに繋がるよう設定される。その結果、多額の接続料金が請求されるというものである。Dialler の概要と問題点を説明したリーフレットを用意しており、消費者相談センター（Consumer Advice Center）で入手することができる。（消費者団体）

○警察では一般的に市民向けの普及啓発は行っていない。特定の案件について報道発表を行うことはある。最近では例えば Dialler について行った。190 番サービスへ誘導する広告がポップアップしサービスや製品の購買を勧める。これらのサービスは詐欺であることが多く、消費者は金銭的な被害を受ける。市民に対してこれらのサービスを利用しないようプレスリリースを行った。（州警察）

7．国・官公庁の取り組みに対する評価

7.1 産業界との連携の在り方

産業界と法執行機関との連携は密接に行われている。法執行機関、行政機関の人材育成に産業界が積極的に貢献している。インフォーマルな形での情報交流が様々なイベントや会合において行われている。ハイテク犯罪に関連した法改正や ISP へのログ保存義務づけなどの議論は、産業界を含んだ形で進められている。

また、違法・有害情報対策で見られるように、ホットラインの開設など民間分野での自主的な取り組みが活発に行われており、法執行機関との連携も必要に応じて行われている。

7.2 国･官公庁の取り組みに対する評価及び要望

ハイテク犯罪に対する国や法執行機関の取り組みは評価されている。ハイテク犯罪関連の法規制は既に多くなされており、概ね必要な対応が行われていると考えられている。予算的な制約から適切な装備を持っていないという指摘もあるが、特に児童ポルノ等の

違法・有害情報対策は進んでいるという認識がなされている。

また、BSI や BKA といった連邦政府機関は情報セキュリティ対策に積極的な活動を行っている。数多くのガイドラインやトレーニング等を提供しており、情報セキュリティ対策の充実に寄与しており、高く評価されている。

一方で、政府は旧来のメディアでの対策をインターネットにも当てはめようとしているという批判もある。また、今後は国内を念頭においた対応ではなく、ヨーロッパ全体を見据えた対応をしていくことが必要であるとの指摘がある。

また、ドイツでは歴史的な背景からナチズムに関連した情報への規制は強いが、過度の規制は表現の自由等の観点から問題であるという指摘もある。

■国･官公庁の取り組みに対する評価について

①法制度整備

○ドイツ刑法には、違法・有害情報に関する規定があり、こうしたサイトの提供者は法的責任を負う。こうした規制で十分である。（連邦政府機関）

○ハイテク犯罪関連への法規制は既に多く行われているが、さらに規制を行う必要がある。例えば、プロバイダーにログの保存を義務づけることは、法執行機関に役立つ。（州警察）

○違法ソフトウェアに対する法規制に関して、供給者、ユーザーへの罰則を強めても良いのではないか。現行法では供給者、ユーザーは販売又は使用した製品の弁償を行う必要があるだけで、製品が違法なものであることに対する罰則が科されていない。（OS 事業者）

②捜査体制

○より多くの人員や必要な機器を購入するための予算等のリソースをインターネット関連犯罪に割くべきである。当州警察は相対的には恵まれているが、他の州警察ではリソースの不足から活動が制限されている。（州警察）

○政府機関は予算的な問題から、インターネット犯罪に対抗する適切な装備を持っていない。ただし、インターネット犯罪に対する認識は高く、児童ポルノや児童保護等の分野では多くの取り組みがなされている。（OS 事業者）

○インターネット犯罪の問題は犯人特定が難しい点である。州や国境を越えた広域捜査が難しい。どこで犯罪が行われたのか、どこに犯人が所在するのか、どこで被害が生じたのかが問題となる。（OS 事業者）

③官民連携

○ドイツでは様々なイニシアティブや団体がインターネットセキュリティに取り組んでいる。中心的なものは BSI と連邦経済省（BMWi）の initiative D21 によるものであり、これらの活動を支持している。（消費者団体）

■要望について

○将来は、法規制や団体での取り組みの焦点を国内レベルからヨーロッパ全体に移す必要がある。（コンテンツプロバイダー団体）

○政府との議論は問題が多い。政府はどのような対策や規制が本当に効果を持つのかどうか理解する必要がある。電波や放送業向けの対策をインターネットに適用しようとしている。インターネットは国際的なメディアであり、こうした対策では意味がない。（コンテンツプロバイダー団体）

○デュッセルドルフでは、プロバイダーに対してフィルタリングソフトの利用命令が出された。しかし、プロバイダーが提供しているのは、インターネット接続サービスであり、コンテンツの監視機能は含まれない。プロバイダーへのフィルタリングソフトの義務づけは違法・有害情報に対する適切な手段ではないと考えている。（連邦政府機関）

V　フランス

１．情報セキュリティに対しての認識

日常的にウイルスやDoS攻撃を受けているISPやWebコンテンツ企業等のIT産業の企業は情報セキュリティに注意を払っており、対策を講じていることが多い。特にインターネットへの常時接続サービスが普及した結果、DoS攻撃やスキャニングが増加しており、IT企業の多くはこれらをネットワークに対する脅威と認識し、セキュリティ意識を高めている。

しかし、フランスにおいてもIT産業以外の企業及び一般ユーザーのセキュリティ意識は低い。インターネットの問題を取り扱う消費者団体でも、主な関心はインターネットを利用した詐欺や児童ポルノ対策であり、ハッキングやウイルス対策への関心は薄い。また、フランスの地方自治体はIT技術を取り入れ始めたところであり、セキュリティを意識するほどのレベルに達していない。

■情報セキュリティに対しての認識について

○ウイルスや不正アクセスによる被害を受けたこともあり、セキュリティ機能を強化した新しいネットワークシステムを導入した。しかし、セキュリティ等の技術的なことは全て外部委託で民間企業に任せており、職員のセキュリティ意識は低いままである。（地方自治体）

○ハイテク犯罪としては、不正アクセス等のネットワークの脅威よりも違法・有害情報、特に児童ポルノの方に問題意識がある。（市民団体）

２．情報セキュリティ対策のための体制

米国等のケースと同じく、事業に情報技術を取り入れている企業にとって、情報セキュリティの確保は重要課題である。そのため、これらの企業ではセキュリティの技術やハイテク犯罪に精通している人材を新たに採用して、情報セキュリティのための専門部署を設置し、又は専門チームを組織していることが多い。中には、元ハッカーを雇う企業もある。警察の犯罪捜査官よりスキルのある人材が集まる企業もあり、このような企業では、ハイテク犯罪に遭遇してもまずは自力で犯人捜査を行い、証拠を収集した後に警察に通報することがある。また、セキュリティ専門部署はユーザーのセキュリティのために連絡・相談窓口となることが多い。

しかし、セキュリティ意識の低い企業や団体ではセキュリティ体制が整っておらず、情報技術専門の部署は存在しても、ネットワークの管理・運用を優先して、セキュリティ対策は後回しになっている。

■情報セキュリティ対策のための体制について

○法人向けのセキュリティサービスを提供する部署にセキュリティ専門の技術者を採用し、セキュリティ担当チームを設置した。セキュリティ情報のユーザーへの提供や何か起きた際の対応を行うことになっている。（情報機器メーカー）

○ハイテク犯罪対策の専門チームを組織している。専門チームは社内の法人向けの部署と連携して、定期的に顧客の受けるハイテク犯罪の情報を収集し、最新のハイテク犯罪の手口や動向を調査している。警察に通報する前に自力で犯罪捜査することもある。ただし、自主捜査に関する社内規定を定めており、当社で行うことは、①ハイテク犯罪の定義、②犯罪者の割り出し、③犯罪の重要度の評価、④対処方法の確立に限っている。（OS 事業者）

○元ハッカーを採用して、ハイテク犯罪対策専門のチームを組織しており、ハイテク犯罪のモニタリング及びハイテク犯罪に関する情報の収集を行っている。元ハッカーなのでスキルが豊富であり、犯罪対策には有益である。（Web コンテンツ企業）

○IT 担当の部署がシステム管理・運用及びセキュリティ対策を行っている。しかし、IT 担当部署はスムーズなネットワーク運用に注力しており、セキュリティ対策にはあまり関心がない。（地方自治体）

3．情報セキュリティ確保のための対策及び対応

3.1 事前対策（予防）

3.1.1 情報セキュリティ対策

ネットワークに対する脅威の予防策は、FW、ウイルス検知、データのバックアップ、モニタリング等の一般的な対策が中心である。また、非常時の対応方法を示したセキュリティポリシーや社内ガイドラインを設定し、リスク管理を行っている企業も多い。

情報技術産業の企業では、法執行機関からの提出要請に備えて、業務上発生するログを保存している。フランスは個人情報保護に厳しいこともあり、ログのビジネス利用は行われていない。

■情報セキュリティ対策について

○ファイアウォールの設定、データのバックアップ、ウイルスメールのフィルタリング、DoS 攻撃に備えたアクセス制御等を行っている。また、ネットワークセンタを二つ設置して、リスク分散を行っている。どのような攻撃を受けた時にバックアップを利用するのか等は社内ガイドラインで定めている。（ISP）

○社内システムではファイアウォールやログインシステムの導入、厳重なアクセス権設定等を行っており、世界で最も堅固なシステムの一つと思っている。（情報機器メーカー）

○当社製の PC にはハードディスクとは独立したチップを搭載しており、パスワードや電子認証に関するデータ等セキュリティが必要な全てのデータを安全に格納できるようになっている。しかし、ハードウェアだけでセキュリティを確保することは難しく、セキュリティの大部分はソフトウェアに依存している。（情報機器メーカー）

○ハイテク犯罪としてはウイルスメールやスキャニングが多い。データのバックアップはもちろんのこと、フィルタリング及びアクセス制御、不正アクセス検知システムを導入している。また、定期的にネットワークの安全性や保存データの真正性を点検している。これらの対策で不正アクセスなど企業に直接攻撃を加えてくる行為のほとんどは検知できる。ただ、今後 DoS 攻撃等の組織的な攻撃が増えてくると危険だと思う。（Web コンテンツ企業）

○不正アクセスや児童ポルノ、詐欺等に関しては既存の法律（刑法等）で定義されているが、社内ガイドラインでもハイテク犯罪及び有害行為を定義しており、各犯罪行為の危険度や重大性を評価している。この社内ガイドラインでは、ハイテク犯罪に遭遇した場合の対処方法も示している。（Web コンテンツ企業）

○ファイアウォール、アンチウイルスツールを導入している。また、不正アクセス対策としてモニタリングシステムを導入しているが、職員は新しい機能についていけず、上手く扱えないでいる。（地方自治体）

3.1.2 違法・有害情報対策

どの企業・組織も違法・有害情報対策に神経を使っているが、有効な予防策を見出せていないようである。実際にモニタリングを行っているところは、自社のホスティングサービスの監視をしている Web コンテンツ企業だけであった。ほとんどの場合、社内ガイドラインを用意して、違法・有害情報を発見したユーザーもしくは違法･有害情報により被害を受けたユーザーから連絡を受けてから、ガイドラインに沿った対応をするところが多い。

■違法･有害情報対策について

○子供が違法･有害情報に触れないように、フィルタリングの導入や保護者の目が届く範囲での子供のインターネット利用を奨励しているが、あまり効果がない。最近増加傾向にあるアダルト関連のスパムメールも違法･有害情報と言えるが、メールフィルタリング等である程度防止できている。（市民団体）

○他のハイテク犯罪と異なり、違法･有害情報はアプリケーションなどの技術を導入しても防げないことが多い。違法･有害情報の危険性、違法性をユーザーに認知させること、法執行機関が積極的に取り締まること等の取り組みが必要である。市民団体はユーザーの意識向上のために独自のキャンペーンを展開している。（市民団体）

○不正アクセス等の直接攻撃よりもホームページの書き換えや誹謗中傷等の企業のイメージを壊す行為の方が防御策に限界があり、恐れている。（Web コンテンツ企業）

○当社のホスティングサービスを利用した Web サイトのコンテンツに対する責任は当社にはなく、Web サイトの管理者にあるが、違法･有害情報のモニタリングは行っている。（Web コンテンツ企業）

○ISP が違法・有害情報を見つけた時のガイドラインを用意している。そのガイドラインでは、どのような違法・有害情報であれば、どの法執行機関に通報すればいいのかを示している。（ISP 団体）

○通常モニタリングは行っていないが、当社に関係する犯罪が発生した時、セキュリティ対策チームがその犯罪に関する情報を収集する。（OS 事業者）

3.1.3 情報・データ漏洩対策

フランスは Computing and Freedom Law により個人情報の漏洩を厳しく規制している。法律に加えて、雇用契約や従業員規則で情報漏洩の禁止を明記する企業もある。また、個人情報へのアクセス権を特定社員に限定するところもある。このように情報・データ漏洩対策としては内部犯行の防止策が中心である。

データ転送時の漏洩防止のためにユーザー認証に暗号や独自のエンコーディングを利用する企業がある一方、個人ユーザーは個人情報以外に守るべきデータを持っていないので、個人ユーザーに対するデータ漏洩対策はそれほど重要ではないと考える企業もある。

■情報･データ漏洩対策について

○特に情報漏洩防止のためのガイドラインを作成していない。しかし、個人のデリケートな情報に触れることのできる職員には The Computing and Freedom Law が適用されるのはもちろんのこと、これらの職員に対しては雇用契約において情報漏洩禁止に関する特別条項を加えている。（地方自治体）

○フランスでは Computing and Freedom Law により個人情報の保護は義務化されており、National Commission for Computing and Freedom(CNIL)が個人情報保護状況を監督及びモニターしている。しかし、CNIL だけでは対処しきれていないので、個人情報を利用する際の注意事項等の情報をユーザーに提供している。（市民団体）

○本人の承諾なしに個人情報を公開したり、調べたりすることはできないので、ユーザー認証の際に情報漏洩を防止するために、独自のエンコードシステムを導入した。また、データの転送には暗号をかけるなどで対処している。（Web コンテンツ企業）

○社員による内部犯行を防ぐために､システムに関する部屋などセキュリティの確保が必要な場所への入室を制限している。また、顧客データなどの重要データを扱える社員を限定している。（ISP）

○ほとんどの個人ユーザーは守るべき重要データを保有していないと思っている｡個人ユーザーよりも法人ユーザーの方がデータ漏洩対策を必要としている。データ漏洩対策においてもハードだけでは限界があるので、ソフトとシステムコンサルティングが必要である。（情報機器メーカー）

3.2 問題発生時の対応

ハイテク犯罪を確認しても、企業や団体は法執行機関に通報する義務はない。そのため、自社がハイテク犯罪の被害を受ければ、被害者として警察等に通報するが、自社と直接関係のないハイテク犯罪を発見しても、積極的に通報しないようである。

多くの場合、ハイテク犯罪はユーザーからの連絡で見つかる。そのため、ISP や Web コンテンツ企業ではセキュリティ及びハイテク犯罪関連の連絡窓口として専用のメールアドレスを設置している。

ISP 団体である AFA*が児童ポルノ等の違法・有害情報対策のポータルサイトを作成しており、情報を提供している。また、このポータルサイトはユーザーから法執行機関への通報窓口にもなっており、ユーザーがこのサイトを通じて犯罪内容を通報すると内容に応じて AFA が監督官庁に連絡し、連絡を受けた監督官庁が担当の警察に連絡する体制が整っている。他にも、法執行機関がハイテク犯罪対策の Web サイトを設置しており、ユーザーが直接通報することも可能である。

■問題発生時の対応について

○ISP 各社はユーザーからの違法・有害情報に関する通報を対処するために、専用のメールアドレスを用意している。（ISP）

○ISP 団体である AFA は通報用のポータルサイトを設置しており、ハイテク犯罪（主に児童ポルノ等の違法・有害情報）を確認したユーザーは 24 時間いつでも通報することができる。AFA はユーザーからの通報を受けると、児童ポルノであれば家族省というように通報内容に適当な法執行機関に連絡し、法執行機関は AFA からの通報を受けて、担当の警察に連絡する体制となっている。（ISP）

○内務省の「情報通信技術に関わる犯罪対策室（OCLCTIC）」が設置しているハイテク犯罪防止のポータルサイトでは、違法・有害情報に関する通報を受け付けているだけでなく、ハイテク犯罪に関する情報も提供されている。また、国防省管轄の警察（Gendarmerie）もユーザーからの通報メールの連絡窓口を用意している。ポータルサイトでユーザーにハイテク犯罪の情報提供も行っている。（ISP）

○セキュリティに関するユーザー向けのコンタクトポイントとしてメールアドレスを公開しており、ハイテク犯罪に関するユーザーからの連絡もここに集まる。このメールの設置は義務化されている。（Web コンテンツ企業）

＜参考＞

*AFA　(Association des Fournisseurs d'Acces et de Services Internet)
http://www.afa-france.com
（違法・有害情報対策のポータルサイト http://www.pointdecontact.net）
フランス ISP の業界団体である。ISP 以外にも Web コンテンツ企業等も加盟している。インターネット産業の代表者として政府との調整やインターネット上の違法・有害情報に反対する活動を行っている。具体的には、インターネット業界としての違法・有害情報に対する基本方針を定めること、違法・有害情報対策を政府機関と協力して行うこと、業界に課せられる規制について政府と話し合うことなどを主な活動としている。

3.2.1 違法・有害情報確認時の対応

ISP 等はコンテンツの監視を行っていないため、ユーザーの連絡により違法・有害情報を確認することが多い。自社サービス上に違法・有害情報が掲載されていれば、ユーザーとの契約に則り、管理者として削除又は外部アクセス禁止の措置を取る。しかし、自社のリソースを利用していない違法・有害コンテンツに関する連絡を受けても、ISP や Web コンテンツ企業がユーザーに代わって警察に通報することはない。

■違法・有害情報確認時の対応について
○当社のユーザーが違法・有害と認められる情報をホームページなどで提供していれば、管理者としてその情報を削除する。若しくは、外部からその HP にアクセスできないように設定する。違法・有害情報を提供した場合の措置はユーザーとの契約に明記してある。（ISP）
○違法･有害情報を発見したユーザーから通報を受けても、警察への通報はユーザーに行ってもらっている。（ISP、市民団体）

3.2.2 不正アクセス等の攻撃時の対応

ハイテク犯罪により自社が被害を受ければ、警察に通報することが多い。しかし、企業や団体の IT スキルによって警察への信頼度が異なる。ISP や Web コンテンツ企業などスキルの高い技術者を集めている企業には、警察の IT 分野におけるスキルに疑問を持つところもあり、このような企業は警察による捜査にあまり期待せず、独自の調査で犯人特定を試みている。一方、地方自治体のように、どんなに小さくとも全ての攻撃を警察に報告しているところもある。

■不正アクセス等の攻撃時の対応について

○当社が被害を受ければ警察に通報するが、当社のユーザーの被害であれば、ユーザーが通報する。（ISP、Web コンテンツ企業）

○警察は小規模の事件であれば捜査してくれないことが多い。そのため、当社に関連するハイテク犯罪を発見しても、なるべく自力でその犯罪の調査を進める。当社内で調査を進め、証拠が十分揃った段階で警察に通報する。通報先はハイテク犯罪専門の政府機関（BEFTI*）や地元の警察など様々である。（OS 事業者）

○ウイルスによる被害や不正アクセス等のハイテク犯罪であれば、当組織が ISP 業界を代表して法執行機関に通報している。通常、通報先は内務省である。（ISP 団体）

○攻撃を受ければ、どんな小さな攻撃でも全て地元警察に報告している。通報時には問題が生じた時点のトラフィックフローのデータや被害を受けたハードディスク等を任意に提出している。（地方自治体）

＜参考＞

*BEFTI　(Brigade d'Enquetes sur les Fraudes aux Technologies de l'Information)
フランスのパリ県警のハイテク犯罪捜査専門の部隊。パリ県及びパリ県近郊でハイテク犯罪に遭遇したユーザーや企業の通報先でもある。

4．法執行機関との連携の状況

4.1 捜査協力

4.1.1 捜査協力の内容

昨秋、ログ保存に関する規定を定めた Daily Security 法が成立した。法律が施行されれば、ISP 等にログ保存の法的義務が発生する。政府は細則を決める法規命令で、3 ヶ月以上のログ保存、ユーザーのサイト訪問履歴など詳細な情報の保存等の義務化を試みたが、産業界にとって負担となるこれらの細則は産業界の反対に合い、定められなかった。法規命令が決まらなかったので、法律の施行に至っていない。今秋に再度議論される予定だが、施行までの期間は ISP 等にログ保存の法的義務はない。

現行の法制度でも法的手続きを踏んだ上で法執行機関が ISP 等にログの提出を要請すれば、ISP 等に提出義務が生じる。この法執行機関の法的要請に備えて、ISP 等はログ保存を行っているのが現状である。アクセス記録、身元情報等を 3 ヶ月間保存するのが一般的のようである。

■捜査協力の内容について

○昨秋、ログ保存を義務化する法律（Daily Security 法）が成立したが、まだ法規命令が定まっていないため、施行されていない。そのため、現在のところ、ログ保存は法的な義務ではない。（ISP 団体）

○法執行機関が法的手続きの上で要請をすれば、ISP は捜査協力をしなければならない。提供するデータはアクセスログやユーザプロフィール程度であり、ログ以外の個人情報（メールの中身や訪れたサイト等）は渡さない。ログの使用は捜査協力の時にだけ使用し、マーケティングなどには利用しない。（ISP）

○現状ではログ保存期限を定めた法律はなく、保存期間は企業ごとで異なる。当社は通常、3 ヶ月ログを蓄積し、その後アーカイブにして保存する。アーカイブとして保存する期間は特に定めていない。Daily Security 法の法規命令で長期間のログ保存を法的に義務化する政府の動きがあったが、産業界からの反対もあり、未だ何も決まっていない。（ISP）

○全てのログを 1 年以上保存することには反対である。自由なインターネット社会の秩序を保つために必要な情報だけを保存すれば良い。長期間保存することはコストも負担もかかる。長期間の大量データの保存を法執行機関が要求するのであれば、ISP としてはコスト負担を法執行機関に求めるつもりである。保存するログの内容及び保存期間についても、今秋に再度議論される予定である。（ISP 団体）

○ハイテク犯罪の捜査における技術的側面について、法執行機関にアドバイスをすることがある。また、ノウハウを教授することもある。（OS 事業者）

4.1.2 コンタクトポイント

今回のインタビューでは、法施行機関からの連絡窓口を 24 時間用意している企業はなかった。ただし、ISP 業界では、インタビュー先の ISP 団体が ISP 各社と法執行機関との連絡窓口の役割を果たしており、法執行機関がログの提出などを要請する場合は、この ISP 団体を通して行うことが多いようである。

■コンタクトポイントについて

○ISP 団体が ISP 業界と政府機関とのコンタクトポイントの役割を果たしている。ISP 団体はハイテク犯罪を専門とする部署を設置しており、政府機関からの要請及びユーザーからの通報を受け付けている。ISP 業界全体で裁判所及び法執行機関からおよそ 500 件／月の正式な要請を受けている。そのほとんどは特定ユーザーの身元確認である。（ISP、ISP 団体）

○24 時間対応可能ではないが、当社の法務部が法執行機関からの連絡窓口となってい

る。（Web コンテンツ企業）

4.1.3 コスト負担

法的には捜査協力で生じた費用を協力要請元の法執行機関に請求することができるが、実際に利用したことのある企業は少ないようである。その理由は、請求方法が複雑な上、算出に係る単価が低く、最終的に請求する額も安くなることが挙げられている。

昨秋成立した Daily Security 法の法規命令に関する議論の中で、一定期間のログ保存を義務化するのであれば、ログ保存に係る費用を政府がもっと負担すべきではないか、との意見が出た。

■コスト負担について

○法律上は捜査協力の際に生じるコスト及びデータ保存に係るコストを請求することができるが、単価が低く結果的に請求額も微々たるものになるので、当社は請求せずに自己負担している。（ISP）

○法律上、捜査協力にかかる費用は要請してきた法執行機関に請求することができる。しかし、請求方法が複雑すぎることや請求できる単価が低すぎること等からほとんどのケースでは、ISP がコストを負担している。（ISP 団体）

○昨秋、法的にログ保存期間を定める議論がなされた時、同時にログ保存等の捜査協力にかかる費用を政府がもっと負担すべきではないか、という議論があった。しかし、ログ保存の期間設定と同様に未だ何も決まっていない。（ISP 団体）

4.2 情報提供・情報交換及び技術協力

地方自治体が参加する Security Circle や OS 事業者が定期的に開いている法執行機関の職員と会合以外、セキュリティやハイテク犯罪に関する情報交換として特に表立ったことは行われていないようである。

■情報提供・情報交換及び技術協力について

○ヨーロッパ全域のセキュリティを担当する部署が、定期的に各地の法執行機関と会合を開いており、ハイテク犯罪に関する意見交換や情報提供を行っている。（OS 事業者）

○インターネット関連企業が直面する問題や課題について当組織が政府機関に知らせている。また、ISP 団体は政府に働きかけてインターネット業界に係る規制緩和を提言することで、インターネット業界ができることとできないことを政府に教えている。（ISP 団体）

○様々な機関や企業が参加して設立された組織 Security Circle に参加し、参加者と情報交換を行っている。（地方自治体）

５．産業界における連携の状況

ハイテク犯罪防止は業界全体にメリットをもたらすことが多いので、ハイテク犯罪対策における業界内での協力は行いやすい。ISP 業界では、インタビュー先の ISP 団体がネットワークセキュリティに関するガイドラインを作成するなど、ISP 団体を通じて ISP 各社の意思疎通が上手く行われているようである。また、OS 事業者のように提携企業と共同してハイテク犯罪対策の技術開発を行うところもある。

■産業界における連携の状況について

○ISP 企業間で共通のガイドラインを作成した。どのような脅威に対して、どのような手順を取れば良いのか、どのようなケースにおいてどのような企業又は政府機関と協力すれば良いのか、法執行機関からの要請を受けた時の対応はどのようにすれば良いか等のガイドラインである。（ISP、ISP 団体）

○当社はハイテク犯罪防止のための技術開発を他社と共同で行っていないが、他のフランス ISP では行ったことがあるようだ。（ISP）

○ヨーロッパ全域の ISP 団体 EuroISPA に所属し、ハイテク犯罪に関する意見や情報交換を行っている。また、市民団体である Vivre Le Net とも定期的に情報交換を行っている。（ISP 団体）

○当社がハイテク犯罪の被害にあったときにパートナー企業のサポートが必要となるので、ハイテク犯罪についての情報共有をパートナー企業と頻繁に行っている。また、業界団体やサポート企業と連携して、セキュリティ対策技術の研究開発に力を入れている。（OS 事業者）

○他社や業界団体と協力してハイテク犯罪対策の技術開発や情報交換を行っている。（Web コンテンツ企業）

6．人材育成

6.1 公的機関を対象とした人材育成活動

法執行機関の職員の人材育成は急務であるが、今回インタビューを行った範囲では、公的機関の人材育成に協力しているケースは少なかった。人材育成の協力を確認できたのは、大手 OS 事業者だけであった。

■公的機関を対象とした人材育成活動について
○法執行機関に様々な技術講習やノウハウを提供している。特にコンピュータ詐欺に関する講習が多い。法執行機関の職員はもっと勉強したいようであり、講習を行う人材が不足している状況である。（OS 事業者）

6.2 企業側の人材育成活動

社員は社内で育成することが一般的であり、他社の外部研修を受けるケースは少ないようである。

■企業側の人材育成活動について
○外部の研修もあるが、基本的には社内で研修を行っている。ハイテク犯罪専門対策チームが中心となって、社員のセキュリティ意識向上のための講習会やハイテク犯罪に対抗するための技術的訓練を提供している。（Web コンテンツ企業）
○イントラネット経由でセキュリティ情報を職員に流す程度である。（地方自治体）

6.3 一般ユーザーへの普及・啓発活動

ユーザーのセキュリティ意識向上は今後の大きな課題と認識されている。特に児童ポルノ等の違法・有害情報に対する啓発活動が盛んである。インターネット上に限らず、児童ポルノ全般に反対するキャンペーンを政府が行うなど、政府及び業界団体が様々な取り組みを行っている。しかし、今のところ大きな効果をもたらしていない。

■一般ユーザーへの普及・啓発活動ついて
○昨年、児童ポルノ等有害コンテンツの防止運動を行い、子供に有害コンテンツを触れさせないためのガイドラインを広めようとした。しかし、この運動はインターネット業界や専門家の間の議論に留まってしまい、一般国民にまで広く浸透しなかった。（ISP 団体）
○インターネット上の違法･有害情報に反対するキャンペーンを行っているが、ユー

ザーの意識はなかなか向上しない。TV コマーシャルや地域コミュニティにおける講習会、インターネットカフェでの講習会、地方政府による講習会などが効果的な啓発活動と考えており、将来、実施したいと思っている。（市民団体）

7．国・官公庁の取り組みに対する評価

7.1 産業界との連携の在り方

インターネットの普及当時に比べ、産業界と法執行機関との関係は改善したが、Daily Security 法の法規命令における議論のように、法執行機関はインターネット産業の特性を理解していないと思われているところがある。また、企業同士の意見交換や情報共有に比べ、産官の意見交換等はあまり行われておらず、両者の関係はまだ発展途上にあるといえる。

■産業界との連携の在り方について

○インターネットが普及し始めた頃に比べると、産業界と法執行機関との関係は飛躍的に改善した。法執行機関もインターネットの自由な文化を理解し、捜査協力の要請は法的手続きが必要であることを理解するようになった。（ISP）

○それでも政府機関は最新のインターネット社会の情報に疎いことがあるので、常に新しい情報について勉強してほしい。一方で、産業界は、インターネット社会がどのように機能しており、どうすれば改善するのかなどを政府にもっと説明するべきだろう。（ISP）

7.2 国･官公庁の取り組みに対する評価及び要望

ハイテク犯罪専門の機関（OCLCTIC）の設立や産業界から不評であるが Daily Security 法の成立など、政府はハイテク犯罪対策に力を注いでいる。それでも、インタビュー先の各社が政策の一貫性のなさを指摘していた。体系的な政策なく、各省庁毎に異なる対策を打ち出しているため、産業界に混乱が生じている。

また、両者の相互理解が進んでいないため、インターネット産業が甘受可能な規制の範囲を政府が理解できず、産業界に期待しすぎる面があるという指摘を ISP 団体から得た。

捜査活動の遅さも大きな問題である。これもインタビュー先の各社が指摘していた。捜査官のスキル不足が原因と指摘する企業もあるように、捜査スピードの迅速化と共に、捜査官のスキルアップが要望されている。

■国・官公庁の取り組みに対する評価について

○政府機関はハイテク犯罪に対して体系的な政策を打ち出せないでいる。各省庁が異なる対策や指針を打ち出しており、産業界に混乱をもたらすことがある。（ISP）

○ハイテク犯罪に対する法執行機関の姿勢に一貫性がない。現行の法律ではハイテク犯罪に対応できておらず、罰則も軽い。政府は Daily Security 法を制定したものの、産業界からの反対もあり法規命令を定められず、施行できない。一方では、欧州評議会のサイバー犯罪条約に署名したものの批准できずにいる。このようなフランスの立法・行政の一貫性のなさが問題である。ハイテク犯罪に精通した弁護士が少ないのも問題である。（OS 事業者、市民団体）

■要望について

○フランスの法執行機関はユーザーのサイト訪問履歴やメールの中身まで保存することを ISP 業界に期待している。しかし、ISP 業界はこれらのユーザー情報はプライバシーとして反対している。フランスは伝統的に個人情報保護を厳しく行う国であり、法執行機関といえどもメールの中身など私的情報を強制的に集めることはできないことを理解して欲しい。（ISP 団体）

○警察の捜査はとても遅い。当社が当社のサービス内で違法・有害情報を見つけても、警察に捜査をしてもらう意図ですぐに削除しないことがある。しかし、通報しても警察はすぐに動いてくれない。警察はもっと素早く対応してほしい。（ISP、ISP 団体、市民団体、地方自治体）

○ここ数年、ハイテク犯罪対策機関を設置するなど、フランス政府はハイテク犯罪対策に力を入れてきたと思う。しかし、ハイテク犯罪捜査に関わる法執行官のスキルはまだまだ低く、最新のハイテク犯罪に対抗するためにはもっとスキルを磨くべきだろう。初動捜査が遅い原因の一つは警察官の能力不足にあると思う。（Web コンテンツ企業、市民団体）

○法執行機関は違法･有害情報に触れないための方策やファイアウォール設置の仕方等をユーザーに説明することで、ユーザーに事前対策の必要性を理解させる努力をして欲しい。（市民団体）

○ヨーロッパの各国と協力して､域内の者が公開している児童ポルノのサイトを早急に締め出すためにもハイテク犯罪における国際協力を積極的に行ってもらいたい。（市民団体）