２． ドイツにおけるインターネットカフェ関連法令

２．１　ドイツにおけるインターネットカフェの現状

ドイツの人口は 8,269 万人[1]、インターネットユーザー数が 3,750 万人[2]、インターネット普及率は 45.4%となっている。また、パソコンの普及状況は 54.5%[3]である。

ドイツのインターネットカフェ軒数については、包括的な統計データではないが、World of Internet-Cafes（旅行者のための情報提供サイト）に登録されているインターネットカフェは 642 軒である。同サイトに登録していないインターネットカフェがかなり存在すると考えられるほか、ドイツではコールショップ[4]と呼ばれる店舗にもほぼインターネットスペースが併設されている。

以下は、ベルリンのインターネットカフェ 2 店舗における、利用事例である。

【事例１】easyInternetcafe

ベルリンの中心市街地にある大型チェーン店であり、ビルの 1 階～2 階部に開店している（図表２－１）。1 階には Dunkin’ Donuts も入っており、飲食しながらインターネット端末を使うことができる。

図表２－１．easyInternetcafe の入口看板

＊本報告書にて参照しているインターネット情報（URL）は、すべて 2007 年 10 月 29 日現在のものである。

[1] 2005 年の推計値。（財）日本 ITU 協会『ワールド ICT ビジュアルデータブック 2007』2007 年 7 月。

[2] 2005 年の推計値。（財）日本 ITU 協会『ワールド ICT ビジュアルデータブック 2007』2007 年 7 月。

[3] 2005 年の推計値。「パソコンの普及状況」とは、その国の人口 100 人あたりのパソコン台数のこと。（財）日本 ITU 協会『ワールド ICT ビジュアルデータブック 2007』2007 年 7 月。

[4] 利用者が国際電話を安価にかけることができる店舗。

図表２－２は Dunkin’ Donuts と隣接した 1 階部であり、2 階部はインターネット端末の並んだ机が、教室形式で同じ向きに何列も並べられている。各端末の画面の見通しはよく、通路から各画面を用意に見渡すことができる。日本のような座席ごとの仕切りや、個室・半個室のブース等は設置されていない。

図表２－２．easyInternetcafe の店舗内（1 階）

利用者はまず入口近くの券売機でチケットを購入する（図表２－３を参照のこと）。利用料金は 1 時間 1 ユーロ、24 時間 5 ユーロ、7 日間 15 ユーロ、30 日間 30 ユーロである。チケットに ID 番号が記載されており、インターネット端末でのログイン時に入力し、パスワードは自分で設定する。購入したチケットの有効時間内であれば、ID 番号とパスワードを入力することで何度でも利用することができる。利用者の本人確認（身分証明書の提示等）や年齢確認は一切行っておらず、入口に店員すら立っていない。また、利用者は自由に座席を選ぶことや移動することができ、どの端末を利用したかの記録は（少なくとも紙の帳簿上では）取られていない。端末は、壊れていて利用できないものが多い。

図表２－３．easyInternetcafe **の利用券売機**

インターネット端末にはサーバタイプのフィルタリングソフトが導入されているため、利用者の年齢に関わりなく、アダルトサイト等の有害サイトの閲覧は一律にブロックされる。ただし、日本のアダルトサイトについては、半分程度のサイトはブロックされることなく閲覧可能であったが、これはフィルタリングソフトのデータベースの精度の問題と思われる。

【事例２】IT-Café

ベルリンの中心市街地にある小規模店舗であり、パソコン教室に併設された喫茶店の一角がインターネット利用に供されている。端末数は 4 台であり、カウンターの正面に設置されているため、端末の画面はカウンター内の店員から常時見えるようになっている。

利用料金は 15 分で 50 ユーロセントであるが、ドリンクを 1 つ注文すると 1 時間無料で利用できる。利用にあたっては、身分証明書の提示などの本人確認は一切行われない。

インターネット端末にはサーバタイプのフィルタリングソフトが導入されており、やはり利用者の年齢に関わりなく、アダルトサイト等の有害サイトの閲覧はブロックされる。日本のアダルトサイトについては事例 1 と全く同じサイトがブロックされた。

２．２　インターネットカフェ関連法制の実態

現在のところドイツ国内でインターネットカフェ[5]の利用について犯罪防止のため本人確認を義務付ける法規は存在しない。インターネットカフェに限られないが情報通信システムの利用に際して本人確認を義務付ける法改正について議論がなされており、現段階ではデータ保護の観点からの抵抗が強く、これらがいつ実現するかについては見通しは立っていない。

ただし、情報通信手段を用いた犯罪における利用防止の観点ではなく、青少年保護に関連して本人確認を義務付ける規則は若干存在する。

本節では、以下の①～②の 2 つの観点から、ドイツの連邦法及び州法に関する整理を行う。

①インターネットカフェの利用に際して本人確認を義務付ける法規（２．２．１節）

これは主に青少年保護の観点から、インターネットカフェのコンピュータにインストールされているコンピュータゲームの利用に関連して、あるいはオンラインゲームの利用が可能な場合に、青少年の利用を防止するため年齢の確認が義務付けられている。インターネットカフェにおける本人確認手段として現在実施されている唯一の法的規制であるため、関連する法規及びその背景について解説する。

②インターネットを利用した犯罪の防止、ならびに犯罪捜査を目的とした情報通信手段の監視に関する法規（２．２．２節）

ドイツでの議論では、本人確認がインターネットを利用した犯罪の防止に効力を持つと考えられていない、または効力を発揮するための前提条件に欠けているとの判断が大勢を占めており、義務付けにはいたっていない。この項目ではドイツの捜査機関が本人確認に代わる手段としてどのような方法を採っているかについて参考のため確認する。

２．２．１　インターネットカフェの利用に際して本人確認を義務付ける法規

（1）インターネットカフェの利用に関わる身分証明

ドイツでは、通信手段の中でも特にプリペイド型の携帯電話やインターネットカフェ、コールショップなどの利用監視は犯罪捜査機関にとって盲点となっていることから、様々な規制の導入が検討されてきた。憲法擁護庁ならびに連邦刑事局の方面からはインターネットカフェに対し、本人確認の義務付けを行うべきだとの声もあるが、過去の議論では固定電話などと違って利用者の記録が残らないことや、インターネットカフェ、コールショップの経営者にアラブ、トルコ系を含む外国人が多い[6]という背景などもあって本人確認が実際に機能するかどうかには疑問があるとされている。

---

[5] ドイツにおいてもインターネットカフェの定義は他の国における一般的な定義と異なることはなく、「一般利用者に対して料金を課してコンピュータからのインターネットアクセスを提供する営利施設」とされている。“ Associations for protection of young persons, ” Bundesarbeitsgemeinschaft Kinder- und Jugendschutz ホームページ（http://www.bag-jugendschutz.de ）。

[6] インターネットカフェ等がそのような外国人の集会所になっている場合が往々にしてある。

そのため、ドイツのテロ対策の中では予防措置として危険団体などに対するオンライン捜査の実施、また捜査手段としては各種個人特定データや通信データの保存と捜査機関への提供義務付けなどの方向での検討が中心となっている。

インターネットカフェ関連では、バーデン・ヴュルテンベルク州のシュマルツル憲法擁護官がインターネットカフェでの本人確認の義務付けに関する提案を行っている。

（2）インターネットカフェにおける本人確認

現在ドイツでインターネットカフェにおける本人確認を義務付ける法的規制は、青少年保護の観点からのものに限られる。この青少年保護にかかわる年齢確認は、正式にはインターネットカフェを対象としたものではなく、インターネットカフェにおけるゲームの利用に関連して、遊戯施設とみなされたインターネットカフェへの青少年の立ち入りを制限するものである。

インターネットカフェとして営業を行っていても実際にはオンラインゲームを含むコンピュータゲームのための利用が一定の限度を超える場合には、そのような施設は法的にはインターネットカフェではなくゲームセンターと同様の扱いを受けることになるため青少年がこれに立ち入ることはできない[8]。ただし、技術的手段[9]（年齢認証ソフトの利用）及び

---

[8] インターネットカフェの法的地位に関する判例：
ベルリン市の高等行政裁判所（Berliner Oberverwaltungsgericht OVG）は 2002 年 12 月 7 日の決定ならびに 2004 年 5 月 12 日の判決によりインターネットカフェの営業には、設置されているコンピュータが専ら、またはその大多数がゲームの目的に使用できる場合、営業規則 33i 条（遊戯場、賭博場の営業許可）にもとづき遊戯場営業許可を取得する必要があるとの判断を行った。この判断においては設置されているコンピュータが実際にゲームのために使用されているかどうかにはよらない。これは州刑事局の検査の対象となったインターネットカフェの多くでインターネット接続がまったくないか、インターネットが暴力的な内容のオンライン対戦ゲームの目的で使用されていたことによるものである。

この 2002 年 12 月の決定により約一か月の間に当時ベルリンにあった 160 軒のインターネットカフェのうち 20 軒が閉店した。この決定によれば、インターネットカフェに設置されているコンピュータが主に（オンラインゲームを含む）ゲーム用に利用できる、またはゲーム専用に使用されている場合、そのインターネットカフェは（未成年者の利用が制限される）遊戯施設扱いとなるとされている。また、設置されているコンピュータに対する課税はインターネット利用のためのコンピュータに対する 1 ヶ月 12.78 ユーロ・台ではなく、遊戯設備に対する遊興税 153.39 ユーロが課せられる。この決定については犯罪防止や未成年者の保護よりも、財政難に際しての税収確保の厳格化と見る向きが多い。

いずれにせよこの決定により、多くのインターネットカフェが遊興施設とみなされることになり（明確な基準はなく、管轄税務署の裁量により判断）インターネットカフェの多くは未成年者の利用に関しても制限の対象となった。

ベルリン州刑事局（Landeskriminalamt LKA）は 2002 年に市内のインターネットカフェに対し 250 回の抜き打ち検査を実施したが、このうち半数以上の検査で青少年保護法（Jugendschutzgesetz）に対する違反が確認され重大な違反に関しては閉店が命じられた。違反の主なものは年少者に対して年齢制限のあるゲームの利用を認めていたり、ハードディスク上に児童ポルノなどが保存されていたなどである。刑事局の観点から見ると上記の

監督措置（年齢確認や利用目的の監督）によって青少年保護法に関する規定が遵守されていると認められる場合には遊戯施設として課税・営業監督の対象となっているインターネットカフェであっても青少年が立ち入ることは可能である。

同様に児童会館（Jugendzentren）などの非営利目的的施設に設けられているインターネット設備についても教育的な監督・指導がある場合にはゲームが利用できる施設であってもゲームセンターとみなされることはない。この場合にも青少年保護法に定められた年齢確認・制限規定は適用される。

また、飲食店としての営業許可を取得したインターネットカフェにあっては、青少年保護法にもとづく一般的な措置（16 歳未満のものに対する 5 時から 23 時以外の時間の立ち入り禁止、アルコール飲料の提供禁止）を講じることが必要である。

（3）ドイツの身分証明に関する法規（参考）

ドイツではドイツ基本法第 116 条 1 項の規定により満 16 歳に達した国民に身分証明書の所有が義務付けられている。

（4）インターネットカフェの利用に関わる判例（本人確認とは直接関連しないもの）

インターネットカフェでは通常、全ての利用者に対し任意の目的でインターネットの利用を提供している。この点に関しては、インターネットカフェ利用者の使用方法について営業者の監督責任はどこまで生じるかという問題が議論されている。より具体的には利用者がインターネットカフェを利用して犯罪行為を行った場合、営業者が幇助罪に問われるのを防ぐためには犯罪行為を阻止する必要があるかという点に関心が持たれている。一般的には、犯罪行為に対してその手段を提供したものに対しては幇助罪が適用される。

インターネットカフェの場合についてはミュンヘン検察庁 I 部（StA München I）が、インターネットカフェ営業者はその営業施設が犯罪行為に利用された場合にも責任を負わないとする判断を示している（467 Js 319998/96）。これはインターネット利用サービスの提供が、特定の犯罪者に対するものではなく不特定多数に対するものであって、かつそれらの利用者全てが犯罪行為に加担する状況は考えにくいためである（仮にそのような関与が合った場合には当然ながら幇助罪の対象となる）。

２．２．２　インターネットを利用した犯罪の防止、ならびに犯罪捜査を目的とした情報通信手段の監視に関する法規

（1）犯罪防止を目的とするインターネット利用者に対する身分証明に関する議論

2001 年 9 月の米国における大規模テロを受けて、より広範なテロ対策が必要であるとの

判決は、課税が目的ではなく、青少年保護の徹底のための手段であるということになる。ベルリン刑事局では課税によってインターネットカフェ自体が減少することに期待しているという。これらの判断を受けてバイエルン州でも本来のインターネットカフェとゲームセンターとして営業されているインターネットカフェの区別を厳格化する方向に動いている。

[9] インターネットカフェ向けに市販されているソフトウェアとしては WebBlock Proxy などの年齢認証機能付のフィルタリングソフトウェアがある。ゲームについては特に技術的な規則は存在せず、青少年保護関連法規の規定による監督義務が発生する。

認識が高まり、ドイツでも数次にわたりテロ対策法の制定・改正が繰り返されている。これら一連の法改正においてもインターネット関連の監視手段の強化は重要な位置を占めている[10]。

2006 年からショイブレ連邦内務相は、インターネット利用者監視の強化を要求している。具体的な提案はカタログとしてまとめられているが、この分野ではすでに複数の州が共同で運営するインターネットパトロールや共同テロ防止センターGTAZ （Gemeinsame Terrorismusabwehrzentrum）が存在する。前者は違法サイトなどの監視（1998 年活動開始)、後者は連邦の保安・諜報・防諜機関が 2004 年から共同で運営するもので、インターネット上での潜在的危険組織の活動監視や電子メール通信の監視（検閲）を行っている。

連邦政府のこういった姿勢に反して経済界を中心に、国内の大学などが運営する電子メール暗号化システムや暗号化ソフトを多用している。連邦政府はこれらのソフトの使用も制限したいとしているが、経済界は産業スパイ対策などのために、このような動きを歓迎していない。

A. テロ対策補完法

2006 年 12 月 10 日、連邦政府はテロ対策の一環として整備されてきた「テロ対策法」の改正を「テロ対策補完法」（Terrorismusbekämpfungsergänzungsgesetz TBEG）として連邦議会を通過させた。この法改正の焦点はいわゆる「テロ対策データベース」（Anti-Terror-Datei）の整備ならびに諜報・防諜機関（以下ではまとめて情報機関とする）の権限拡大にあった[11]。

今回改正にあたって連邦政府は、「2002 年 1 月 9 日に施行されたテロ対策法で有効性を確認することができた監視原則を維持しつつ拡大する。」と発表している。

B. インターネットユーザーの身元確認の強化に関連する動き

2001 年 10 月には連邦政府は電話通信網に対する通信傍受について規定する電話通信監

---

[10] 捜査機関による電話の通信傍受はすでに 1998 年から法制化・実施されている。

[11] テロ対策法改正の基本方針：

（1）航空会社、銀行、郵便、電話通信事業及びオンラインサービス企業などに対して、テロ対策の目的で情報機関に付与されている情報取得の権限は今後も国内で治安妨害を意図する勢力の解明に活用される。この監視対象にはイスラム原理主義者組織のほかに極右組織なども含まれる。

（2）携帯電話の認識を目的とする IMSI キャッチャーも同様の目的のために活用される。

（3）ドイツの情報機関に対してはシェンゲン情報システム （SIS）に登録されている国内外の重大な危険に関与する人物の登録データへのアクセスが認められる。

（4）情報機関は今後その任務遂行のため、連邦道路交通局（Kraftfahrtbundesamt）の中央車両登録簿に記録されている車両・所有者データへの自動アクセスが確保される。この権限は軍防諜機関（MAD）及び連邦情報庁（BND）にも拡大される。BND による他の目的でのこの新権限の行使は認められない。

（5）資金洗浄の疑いに対する税関の捜査権限はテロ資金源の捜査にも拡大される。

（6）既存のテロ対策法及び今回の法改正で新たに付与された権限は法律施行後 5 年間に限定されるものとする。

（7）期限付きの権限行使については、期限終了前に連邦政府によってその有効性に関する学術的評価が実施され連邦政府から連邦議会に対して報告される。

視規則（Telekommunikations-Überwachungsverordnung TKÜV ）を制定したがこれに続いてテレマティック研究所（Instituts für Telematik 、トリーア大学）の所長、マイネル教授は匿名ユーザーによる有害情報の拡散を防ぐためインターネット利用の際にデジタル署名（認証カードを利用）による確認を義務付けることを提案した。

すでに2001年の大規模テロ発生以前からドイツではトリーア大学のマイネル教授らの提案に基づいてインターネットの利用に際して一種のデジタル ID カード の利用を義務付けることが検討されていた。ドイツの関係機関ではこれを監視手段に残された穴を埋める方法と見ているが実際の導入には様々な問題があり、現在までのところ実現にはいたっていない。

ドイツの研究者が提案しているのは個人のコンピュータにスキャナーを取り付け、IC カード（「インターネット・パスポート」）に保存されている本人確認データを読み取らせる方法である。同様にフーバー・バイエルン州政府書記官長はこのような認証チップを 2001 年当時計画されていた新 ID カードに埋め込むことを提案した。

このような動きに対し、データ保護専門家は一般利用者にとってのリスクや悪影響だけでなく、捜査機関自身にとっても諸刃の剣となる可能性があることを警告している。デジタル署名（デジタル認証システム）によるインターネット利用が義務付けられた場合、データの暗号化が全ての利用者にとって可能となることが前提となる。電子商取引においては本人確認を安全に行うことができることは歓迎すべきである。しかし通信内容の秘匿化が可能であっても、サイバー空間のいたるところに個人の行動に関するデータが残るようになるという点にほぼ全てのデータ保護関係者や市民団体が懸念を示している。このような不安に対して IT 関係者は公共機関による個人に対する無制限の行動監視を困難とするため、動的 ID を生成することができるインターネット・パスポートの導入を提案している。しかし、このようなシステムの複雑化は証明書発行コストの爆発的な増加が予想されるため財務省印刷局及びその下部組織であり身分証明書製作に当たる D-Trust 社はそのような提案を歓迎していない。インターネット・パスポートの導入には利点も存在するものの、一方で利用者がプライバシー保護のために通信データを暗号化するようになるとテロ対策は現在よりも困難となることは必至である。

このため、当時（2001 年末）シリー内相が提案したテロ対策カタログ（いわゆる「オットー・カタログ」）でもインターネットに関する本人確認義務の導入は盛り込まれていない 。シリー内相はデジタル署名よりも、バイオメトリック・データなどによる物理的身分証明書の信頼性向上を目指したものと見られている。

（2）いわゆる「ショイブレ・カタログ」（テロ対策データベース）

ドイツでは上記のように ID カード形式の身分証明書による本人確認の有効性に疑問がもたれ、かつ電子認証制度についての様々な技術的・社会的ハードルが高いことから、インターネットを利用した犯罪への対策としては本人確認よりもオンライン捜査やオンラインデータの監視・分析に力が入れられてきた。

2001 年頃から導入が進んでいる情報通信分野における監視強化策の中核を構成するのは歴代内務大臣の主導で提案されてきた「データ整備」が挙げられる。これは、2006 年 12 月 1 日に連邦議会で承認された新テロ対策法 の一部である「共通データ法」（Gemeinsame-Dateien-Gesetz）に基づいて 2007 年 3 月 1 日から利用されているデータベースを指している。

データベースは連邦刑事局（BKA）の専門家 72 人によって準備されたものでイスラム系

テロ組織の構成や行動パターンを調査し、テロを未然に防止することを目的としている。

この共通データベースには 3 月末までの時点で 38 の公的機関が参加している。データベースの構築に参加すると同時にデータの利用を認められている機関は現在のところ連邦刑事局、軍事防諜機関（Militärischer Abschirmdienst MAD）、憲法擁護庁（Verfassungsschutz）、連邦情報庁（Bundesnachrichtendienst BND）、税関刑事局（Zollkriminalamt）、各州の憲法擁護局（Landesämter für Verfassungsschutz）及び同じく各州の州刑事局（Landeskriminalämter）である。

連邦議会での野党の質問に対して、連邦政府が行った回答によるとこのテロ対策統合データベースを構成する個々のデータベースは 334 件、また継続収集される個別のデータは 511 種類に上る（ただし各州警察、連邦警察及び税関に関するもののみ。諜報・防諜機関に関連するデータベースの件数及び内容は機密保持面の理由から公表されていない。 ）。整備されるデータの内容としてはテロ対策に必要なデータに限定されず、国内治安対策に利用されるデータも多く含まれている。BKA に設置されているテロ対策データベースは複数のアクセスレベルに分類される。機密（Verschlußsache VS）扱いのデータへのアクセスは Sina システム（Sichere Inter-Netzwerk Architektur）で保護された VPN 接続でアクセスするようになっている。基本データ群にはテロ容疑者または潜在的テロ組織構成員や企業、団体などの銀行口座、電話番号、メールアドレス、免許証データ及び関係者リストなどが含まれる。これらの基本データ・アクセス及び個々のデータベースの組合せ検索とは別に諜報・防諜機関の機密データへのアクセスも可能である。この特殊情報の検索では検索者は検索結果を直接知ることはできないが、該当機関には、検索者の連絡先が通知され、機関側から該当者に連絡を行うシステムとなっており、諜報機関と警察のデータ分離が確保されている。このシステムには例外が設けられており、優先順位の高い事件や緊急の場合には、アクセス権を持つ全ての捜査関係者が全ての機密レベルのデータに直接アクセスできるようになっている。このようなアクセスを行った場合にはアクセスの妥当性について事後評価が実施される。

2007 年 2 月 13 日から 14 日にかけてベルリンで開催された欧州警察会議（European Police Congress）での報告によるとこのようなデータベースの構築には SAP、Oracle、SPS や IBM などが参加しているという。ツィールケ BKA 長官によるとドイツ＝オーストリア間で締結されているプリューム条約に基づく DNA データの共有･比較によってすでに 1500 件の「成果」があがっている。オーストリアからのデータ提供に続き、スペインからのデータ提供が本年中に実施されるという。

（3）オンライン捜査に関する法規

BKA 及び各州の刑事局がこのほか手を焼いているのは最近増加しているインターネット犯罪である。BKA が把握しているフィッシング・サイトは 2006 年 5 月には 12,000 件であったが 11 月の時点ではすでに 32,000 件に増加している。また、ボットネットワークの数も爆発的に増大しており、BSI（連邦情報技術安全局）が確認した有害プログラムは 20,000 種におよぶ。

シュレーダー政権（前政権）のシリー前内相（SPD）は 2005 年夏、インターネットによる犯罪捜査の手段として捜査機関にオンライン捜査（インターネットを利用した一般のコンピュータ内の捜索、公的ハッキング）を行うことを業務規定の形式で認めた。シリー前内相は、この業務規定はインターネットフォーラムなどの外部からの監視が目的だったとしている。この許可には法的根拠が欠けていることから連邦裁（Bundesgerichtshof BGH）

は今年 2 月、このような捜査は認められないとする判断を行った。連邦内務省によると連邦裁の判断までに実施されたオンライン捜査の件数は 1 ダースに満たないとされる。実際にこの方法による捜査を実施したのは憲法擁護庁であるとされている。憲法擁護庁自身は捜査を行ったことを認めているが、シリー内相の指示によりどのような捜査手段を導入する意図があり、またオンライン捜査をどの時点で開始したかなどについての連邦議会での質問には回答を避けている。

ショイブレ現内相（CDU）は BKA が示した計画に対する野党及び連立与党 SPD の反発を受けて 2007 年 4 月 26 日、このような秘密捜査を一時停止することを命じたが、政府の方針は早期にオンライン捜査の法的根拠を確立することにある。内相の見解ではインターネットはテロ組織などにとって安全な連絡手段を提供しており、このような捜査手段がテロ対策として必要かつ重要であるとの立場は変えていない。 政府は現在、ノルトライン・ヴェストファーレン州法 で認められているオンライン捜査についての連邦憲法裁判所（Bundesverfassungsgericht）の判断を見て、法制化に着手すると見られている。

法的な問題は別として、BKA ではインターネットから隠密裏に個人のコンピュータにまでアクセスするオンライン捜査なしには、テロとの戦いを成功に導くことはできないと見ている 。既述したデータベースの分析に基づいて現在ドイツの捜査機関や防諜機関が実施しているイスラム系テロリスト捜査の件数は 219 件でこれらの約半数は BKA が担当している。イスラム系テロリスト対策には言語・文化面での障害が存在するがこれらを解決するため、イスラム学者の募集に対しては 4 件の募集に 240 名が応募し 2 件のアラビア語翻訳者募集に対しては 80 名からの応募があった。

実際の捜査を行うのは BKA 内に設置されているインターネット・モニタリング･分析センター IMAS（Internet-Monitoring- und Analyse-Stelle）である。同センターは危険サイトに分類されたサイトのコンテンツ約 5,000 件を日夜監視している。最近の成功例としてはムハンマド風刺画事件に関連してドイツの歌手ネーナの殺害を計画していたトルコ系移民の若者 8 名の逮捕がある。ドイツではイスラム系移民人口が増大しており、BKA では若者層における最近の宗教観の過激化を警戒している。

（4）公共機関による通信傍受を認める法規（参考）

○電話通信に対する他の監視手段に関する現行の法規定

インターネットカフェでの本人確認ではないが､電話通信法第 110 条から第 113 条 では、電話会社は通信サービスの提供開始時点で政府機関による通信傍受を可能とする設備を、事業者負担で整備し、情報機関（連邦情報庁 BND・軍防諜機関 MAD）及び保安機関（憲法擁護庁・警察）の求めに応じて契約者の電話番号、氏名、自然人の場合には生年月日、契約開始の年月日、住所などを提供することを義務付けている。

現在、ドイツの刑事捜査機関は日常的に国内のプロバイダーや電話通信事業者に対し、刑事犯罪と関連する可能性のある通信記録の提供を要請している。ほとんどの場合、問合せの対象は（主に動的）IP アドレスまたは電話番号の確認である。通信内容の確認は IP アドレスや電話番号、ユーザー名や個人特定データの問合せと同様に日常的に利用されているが件数は少ない。

①IP アドレスは、捜査機関が行う、著作権侵害行為やインターネット上の名誉毀損行為などの捜査において、特定の時間帯にある IP アドレスを使用していた人物の特定のために問

合せがなされる。ただし、IP アドレス利用者の特定による捜査は現在、電話通信事業者によるデータ保持に関する法的な最低保持期間や接続データの保管基準が存在しないため有効に機能していない。ドイツのデータ保護関連法規はこれらのデータの保持を料金清算の目的に限定して保持することを求めている。
②しかし、現実にはドイツテレコムでは IP 接続データを最高 80 日間保持しているのに対し他のプロバイダーにおける保持期間はコスト上の理由からこれを大幅に下回るのが通例となっている。また、技術的な知識を持つ犯罪者は JAVA 匿名プロキシ（JAP）や国外のプロキシを利用している例が多いことも障害となっている。
③同様の問題はコールショップやインターネットカフェにも当てはまり、現在の法基準ではインターネットを利用した行為者の特定・犯罪捜査には限界が存在している[13]。

[13] 2006 年末の情報による。

２．３　インターネットカフェ関連法令条文

（１）「青少年保護法」（連邦法）

○関連する条項の抜粋訳

「青少年保護法」
2002 年 7 月 23 日公示
（最終改正：2004 年 7 月 23 日）

第１章：一般規定
第 1 条：定義

第 2 条：確認・証明義務
(1) 本法の規定にもとづき監督権者による同伴が行われる場合、第 1 条 1 項の 4 に定められている者（注：満 18 歳以上の監督権者）は求めがあった場合、証明を行わなければならない。主催者または営業者は疑義が生じた場合、監督権の有無を確認しなければならない。
(2) 本法の規定にもとづいて年齢制限の対象となる者は求めに応じ、適切な方法でその年齢を証明しなければならない。主催者または営業者は疑義が生じた場合、年齢を確認しなければならない。

第 3 条：規則の表示
(1) 主催者または営業者は第 4 条から第 13 条 までの規定にもとづきその営業施設及び催しに際し適用される規則を、また一般向けの映画上映の際には映画の年齢制限、もしくは第 14 条 7 項 による提供者表示を明確に視認及び判読可能な方法で表示しなければならない。
(2) 主催者または営業者は映画ソフトまたはゲームソフトの年齢制限に関する表示として第 14 条 2 項に規定されている表示のみを用いることができる。
一般向けの映画イベントに映画を提供する者には提供の際に年齢制限または第 14 条 7 項の提供者表示について通知することが義務付けられる。第 14 条 6 項の手続きに従って州高等裁判所または自主規制機関が表示を行った映画、映画ソフト及びゲームソフトについては予告または宣伝に際して青少年に有害な内容について通知してはならず、青少年に有害な方法によって予告または広告を行ってはならない。

第 2 章：公共の場における青少年保護
第 4 条：飲食店
第 5 条：ダンス施設

第 6 条：遊戯場、賭博場
(1) 一般利用者向けの遊戯場またはそれに類する、遊戯を主目的とする施設に児童[14]または青少年[15]を立ち入らせてはならない。
(2) 一般利用者向けの賭博ゲームへの児童及び青少年の参加は祭事、狩猟祭、年末市、特別

[14] 14 歳未満の者（第 1 条第 1 項における定義）。
[15] 18 歳未満 14 歳以上の者（第 1 条第 1 項における定義）。

市その他のこれらに類する催事であってかつ賞の金額が僅少である場合にのみ許可されるものとする。

第 7 条：青少年に有害な催し及び営利施設
第 8 条：青少年に有害な場所
第 9 条：アルコール飲料
第 10 条：公共の場における喫煙、タバコ製品

第 3 章：メディア領域における青少年保護
第 3 章 1 節：記録媒体
第 11 条：映画上映
第 12 条：映画またはゲームが保存された記録媒体
第 13 条：画面を有するゲーム機
第 14 条：映画、映画ソフト、ゲームソフトの表示
第 15 条：青少年に有害な記録媒体

第 3 章 2 節：テレメディア
第 16 条：テレメディアに関する特別規定
第 18 条にもとづく青少年有害メディア・リストに登録されているテレメディアについての規定は州法により定められるものとする。

第 4 章：連邦青少年有害メディア審査センター
第 17 条：名称及び管轄
第 18 条：青少年有害メディア・リスト
第 19 条：人員構成
第 20 条：審査申請権を持つ団体
第 21 条：手続き
第 22 条：定期発行記録媒体またはテレメディアの登録
第 23 条：略式手続き
第 24 条：青少年有害メディア・リストの更新
第 25 条：訴訟

第 5 章：規則制定権の付与
第 26 条：規則制定権の付与

第 6 章：違反に対する措置
第 27 条：罰則

第 28 条：罰金規定
（以下は、確認表示義務に対する違反に関する規定のみを抄訳）
(1) 主催者または営業者として故意または過失により
1. 第 3 条 1 項に反して営業施設もしくは会場に、定められた表示を行わない、または正しくない表示ないし規定によらない表示を行った者

2. 第 3 条 2 項に反する表示を行った者
3. 第 3 条 2 項の 2 に反して警告を行わない、または正しくない警告を行なったか適時に警告を行わなかった者
4. 第 3 条 2 項の 3 に反して指摘を与え、映画ソフトまたはゲームソフトについて予告または映画、映画ソフトやゲームソフトの宣伝を行った者
7. 第6条1項に反して児童または青少年に一般利用者向けの遊戯施設もしくは該当条項に挙げられている施設への立ち入りを許可した者
8. 第 6 条 2 項に反して児童または青少年に賭博ゲームの利用を許可した者

(5) 秩序違反に対しては最高 50,000 ユーロまでの罰金を科することができる。

第 7 章：付則
第 29 条：移行規則

第 30 条：施行、失効
(1) この法律は放送、テレメディアにおける人権及び青少年の保護に関する州際協定が施行された日をもって発効する。
（略：喫煙に関する規定）

（2）「営業規則」（連邦法）[16]

○関連する条項の抜粋訳

「営業規則」
1999 年 2 月 22 日公示
（最終改正：2007 年 9 月 7 日）

第 I 部：一般規則

第 II 部：恒常的営利事業
I. 一般要件
II. 特別な監督または許可の要件
B. 特別な許可を必要とする営業者
（他の事業形態に関してはインターネットカフェに適用された判例がないため除外する）
第 33i 条：遊戯場及びこれに類する事業
(1) 営業目的をもって、専らまたは主に遊戯機器の設置、もしくは第 33c 条 1 項の 1（賞金付きゲーム設備の営業に関する監督機関の許可）または第 33d 条 1 項の 1（第 33c 条に規定されている以外の賞金付きゲーム設備に対する監督機関の許可）または営業目的でもって非賭博用の娯楽機器を設置する遊戯場またはこれに類する施設を運営することを意図す

16 「営業規則」は、基本的には営業許可を要する事業の、開業許可の手続きや要件を定めるものである。連邦法であるが、実際の監督には州の機関が当たる。

る者は管轄官庁の許可を取得しなければならない。
一般市民、利用客または事業所所在地または隣接地の住民を危険、重大な損失または重大な負担から保護するために必要と認められる場合、営業許可には期限または付帯条件を設定することができる。営業許可が行われた後であっても同様の目的で付帯条件を設定、変更または追加することは認められる。
(2) 以下の場合には営業は許可されない：

1. 第 33c 条 2 項（第 33c 条 1 項の設備に対する営業不許可の事由）または第 33d 条 3 項（同 33d 条に関する規定）に挙げられている不許可の理由が存在する場合
2. 事業運営に予定されている空間が設備または位置の観点から（事業）警察の要求に適合しない場合
3. 事業の運営が青少年に対し悪影響を与える場合、過剰な娯楽提供、連邦汚染防止法に規定されている環境への悪影響、またはその他の容認しがたい負担を一般市民、付近住民または公共の利益に供される施設に与える懸念が存在する場合

第 X 部：刑罰及び罰金規則
第 IX 部：営業中央登録簿