平成１１年度

ドイツにおけるコンピュータへの不正アクセス（クラッキング）と対策の実態調査

２０００年3月

情報処理振興事業協会
セキュリティセンター

目　次

はじめに

コンピュータによる犯罪行為は、以下の第１章からもわかるように、９８年、９９年と休むことなく増加した。しかし、これら一連の犯罪行為の分析は、２つの要因から、いまだに難しい状況となっている。ひとつは、刑法に触れる犯罪行為が急速に伸びているのに対して、それを把握する方法と分類方法の確立が遅れをとっているという点だ。ドイツ連邦刑事警察庁の犯罪統計では、９８年になって初めて、犯罪種類として「通信サービスへの不正アクセス」が加えられた。これに相当する犯罪行為が９８年以前から存在していたことはいうまでもない。もうひとつの要因は、データを攻撃された会社が、イメージダウンを恐れて、攻撃を受けたことを公にしない場合が多く見られるという点である。そのため専門家の多くは、コンピュータ犯罪によってドイツで発生した損害の種類と規模に関する統計はまだ氷山の一角に過ぎないと見ている。また、企業がイメージダウンを恐れるのは、多くの場合、ドイツ企業の多くがコンピュータ不正アクセスの危険に対して何ら対策を講じてこなかったことに対する羞恥心の現われでもある。

連邦情報技術安全庁[1]の依頼で作成された情報セキュリティに関するスタディが２０００年１月に発表されているが、ここでは３３社に対するアンケート調査しか行っていないため、本レポートではスタディから多くを紹介するのを控えた。しかし同スタディも、ドイツ企業の情報セキュリティに対する投資が全く不十分であるという結論に達している。ドイツ最大のハッカー組織である「カオス・コンピュータ・クラブ」の会員は、この状態を

「情報セキュリティは歯医者に行くのと似ている。歯医者に行くのを延ばせるだけ延ばして、結局滅法高いものについている」

と表現した。

[1] ＢＳＩは連邦内務省管轄下の連邦機関で、連邦の情報セキュリティを確保するため安全防止対策に取り組むほか、セキュリティ関連商品の評価と認証を行っている。また、セキュリティ関連商品のメーカーや販売者、ユーザーに対して情報技術のセキュリティに関する情報を提供したり、助言を行っている。

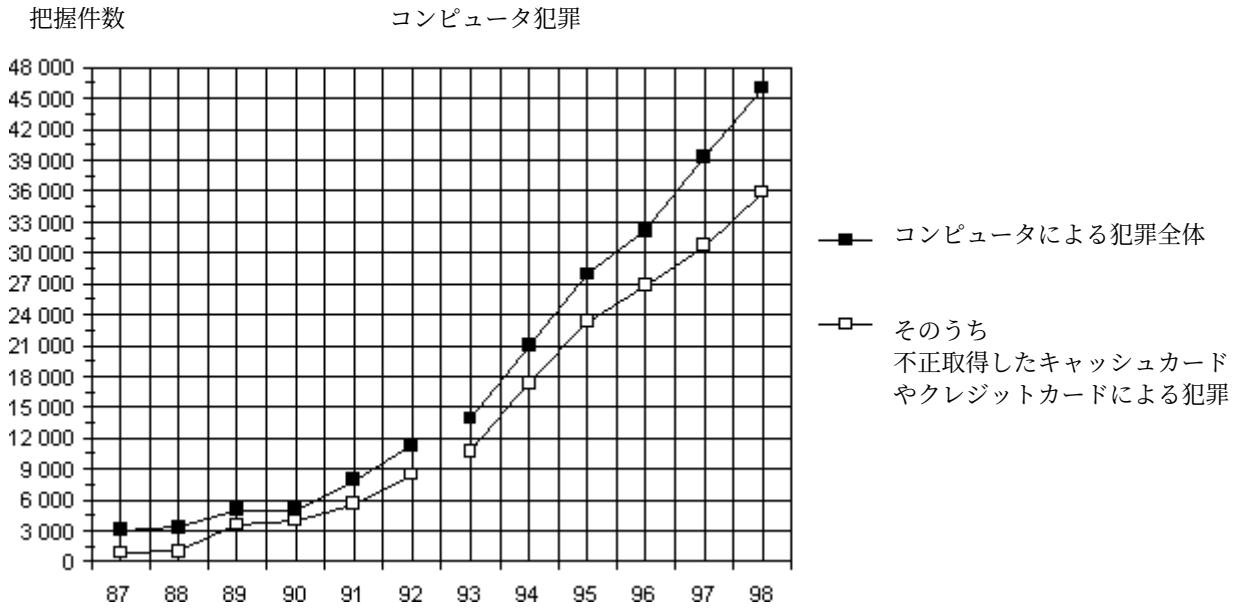
第１章　不正アクセスの状況

１．１　警察の犯罪統計の動向

ドイツのコンピュータ犯罪に関する統計資料は連邦刑事警察庁の犯罪統計でしか把握されていない。ただ、この犯罪統計は、犯罪を刑法典に準じた犯罪の種類別にしか集計しておらず、大まかに分類されているにすぎない。この分類に「通信サービスへの不正アクセス」の項が追加されたのは、９８年になってからである。したがって、同犯罪統計ではコンピュータに絡む犯罪の動向を表面的にしか見ることができない。

現在入手できる最新の連邦刑事警察庁の犯罪統計は９８年の統計である。前述したように、この年から「通信サービスへの不正アクセス」の項が追加されているため、それ以前の統計と単純に比較することはできない。ただ、通信サービスへの不正アクセス件数を除いても、９８年のコンピュータ犯罪件数は、前年比で約 12.5% 増加している。

８７年から９８年に把握されたコンピュータ犯罪件数の推移を追うと、以下の図１－１のようになる。



1987 年から 1990 年まで：旧西独
1991 年から 1992 年まで：ベルリンを含む旧西独
1993 年以降：ドイツ全域

図１－１　コンピュータ犯罪の推移（出所：連邦刑事警察庁犯罪統計）

図１－１で、上の線はコンピュータが絡む犯罪全体の件数で、下の線がそのうちのキャッシュカードやクレジットカードに絡む犯罪である。この図を見る限り、年を追う毎に２つの線の間隔が大きくなっているが、それはコンピュータに直接関連する犯罪が増加していることを意味する。

次に、コンピュータ犯罪統計を犯罪の種類毎にまとめたのが表１－１である。

表１－１　ドイツのコンピュータ犯罪の種類別件数（単位：件数）

犯罪の種類	把握件数		前年比		犯罪解決率（%）	
	1998 年	1997 年	絶対数	%	1998 年	1997 年
不正取得したキャッシュカードやクレジットカードによる犯罪	35909	30727	5182	16.9	39.4	42.4
コンピュータ詐欺[2]（刑法典２６３条ａ）	6465	6506	-41	-0.6	60.7	57.5
通信サービスへの不正アクセス	2109	1998 年から導入			31.5	
証拠データの偽造[3]（刑法典２６９条）、法的往来におけるデータ処理の欺罔[4]（刑法典２７０条）	349	380	-31	-8.2	89.7	93.7
データの改竄[5]（刑法典３０３条ａ）、コンピュータに対する破壊妨害行為[6]（刑法典３０３条ｂ）	326	187	139	74.3	40.2	52.9
データの盗み[7]（刑法典２０２条ａ）	267	213	54	25.4	80.1	60.1
ソフトウエアの不正コピー（コンピュータゲーム等の個人使用）	362	546	-184	-33.7	96.4	99.3
営利を目的としたソフトウエアの不正コピー	289	772	-483	-62.6	98.3	98.8
合計	46022	(39331)	X	X	43.4	(47.5)

（出所：連邦刑事警察庁犯罪統計）

なお、犯罪の特徴として、容疑者の 77.9%が男性で、69.8%が 21 歳以上、58%が人口 50 万人以上の大都市の住人であることが目立っている[8]。

---

[2] 第三者に財産上の不正な利益をもたらす目的で、不正プログラム若しくは不正又は不完全データの利用、不正利用等によって他者の財産に被害を与える行為のこと。

[3] 法的往来において証拠データを欺罔する目的でこれを保存又は変造して、当該データの認知に際して不真正又は変造された証書が提出されるようにするか、このようにして保存又は変造されたデータを利用すること。

[4] 法的往来におけるデータ処理の虚偽の影響は法的往来における欺罔と同意と見なされる。

[5] 不正にデータを削除し、又は使用不能にし、若しくは変造すること。

[6] 企業や公共機関に対して不正にデータを削除し、又は使用不能にし、若しくは変造すること。データ処理施設、あるいはデータ記録媒体を破壊、損傷、使用不能、除去、変造すること。

[7] 自己用ではないデータや、不正アクセスに対して特別な安全措置を施されたデータを自己又は他者用に不正に取得すること。

[8] なお、ドイツで人口 50 万人以上の大都市に住む住民は全人口の 31%である。

しかし、連邦情報技術安全庁の広報担当者は、警察の犯罪統計の証言力を全体として高く評価すべきではないとする。それは、統計に表れない潜在的な数字がかなり高いものと推測されると同時に、コンピュータに関連する不正行為が犯罪として監視されるようになってまだ間もないからである。

これらコンピュータに関連する犯罪行為によって生じた損害について、連邦刑事警察庁は公式なデータを公表しておらず、TÜV（技術監視協会）情報技術社[9]の社長はコンピュータ犯罪、データの不正取得、インターネット上のサボタージュによる損害は毎年約２００億マルクにまで達していると推測している。

ただ、連邦刑事警察庁の担当者が非公式に語っているところによれば、情報技術分野全体の損害はこれよりかなり大きいという。連邦刑事警察庁が把握できる法的に届け出ることのできる損害だけでも約７５００万マルクに達しているとし、それから推測して実際の損害は少なくとも３０００億マルクに上るであろうとする。ただこれは、被害届を出すことのできる損害によって発生する被害推定額で、自然災害や従業員の過失による損害は含まれていない。

２０００年はじめに Yahoo や Amazon 等のアメリカのインターネットサービス会社が「サービス拒否」攻撃された事件が発生しているが、事件に対して連邦刑事警察庁の幹部職員は、現時点でこの種の攻撃に対処する方策がないとコメントしている。しかし、シリー連邦内相は同事件直後に、ハッカー攻撃に対抗するため、連邦内務省、連邦経済技術省、連邦情報技術安全庁、連邦刑事警察庁が協力する、いわゆる「タスクフォース」を設置した。

１．２　ウイルスによる攻撃

９９年に出されたウイルスに対する警告は、Ｙ２Ｋ問題に絡んだウイルスに関するものが少なくなかった。ただ、この種のウイルスは近いうちに再び登場することがないため、ここでは詳述しない。

少なくとも規模の上で新しい現象は「Hoaxes」と呼ばれるウイルスで、ここでは警告自体が問題となる。警告が次々とメールされる毎にシステムの破壊を誘発するのである。さらに、連邦情報技術安全庁は９９年に、JavaScript と他のいわゆる「アクティブ内容」（ActiveX や Java 等）の使用を繰り返し警告した。ハッカーがこれによって、例えば、個人又は商業目的のインターネットユーザーのパスワードを含むユーザー確認データや、ローカルに保存されているデータを探り出すことができるからである。

９８年と９９年に届け出られたウイルスの被害状況をウイルスの種類別に分類したものを図１－２と図１－３に示しておく。一年間だけで、マクロによる被害が急増していることがわかる。

---

[9] TÜV Informationstechnik GmbH

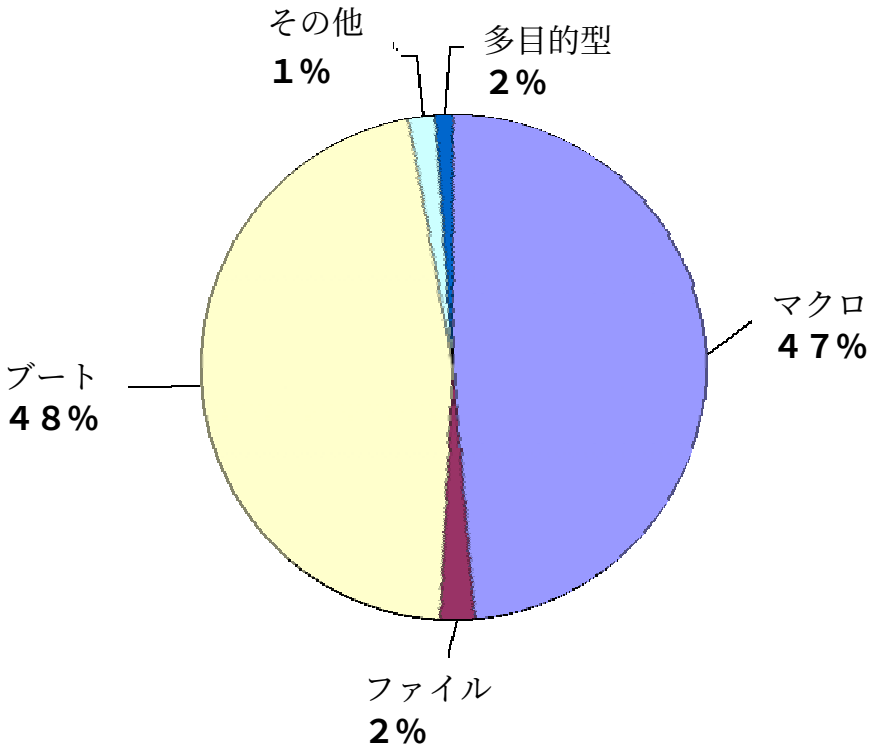


図１－２　コンピュータウイルスの種類（１９９８年）

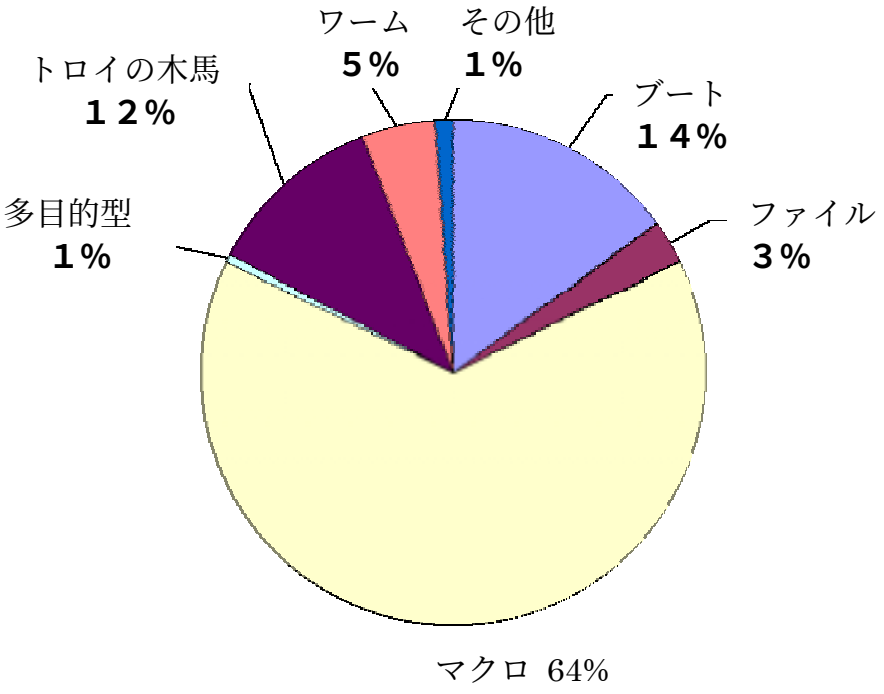


図１－３　コンピュータウイルスの種類（１９９９年）

第２章　情報技術セキュリティ産業

２．１　GMD 情報技術研究センターとフラウンホーファー協会の合併

大規模研究機関組織であるヘルムホルツ・センター[10]に属する GMD 情報技術研究センターとフラウンホーファー協会（FhG）[11]の合併が計画されており、この合併が情報技術の研究開発に大きな影響を与えるものと予想されている。両機関はこれまでに、電子透かし技術の開発で有名になったほか、GMD はメールトラスト[12]の標準化にも参加している。合併計画の背景として、財政難に苦しむ連邦政府が財政削減策のひとつとして研究開発に対する公的補助を効果的に分配しようとしていることが考えられ、GMD の場合、将来性のある情報技術の研究開発を行っていることから、委託研究等で独自に資金を確保していける可能性が高いと見て、政府側が公的補助を削減しても大きな問題が発生しないと見込んでいるものと予想される。フラウンホーファー協会内の情報技術関連研究所は、将来 GMD と共同で研究所連合を設立する予定で、情報技術分野の研究開発で共同戦略を展開していくことになる。すでに両機関の関連研究所所長からなる部会が設置されており、専門内容上の統合とフラウンホーファー協会内のその他の研究所とのネットワーク化に関する戦略構想の作成に着手した。

ただ、基礎研究を研究開発の重点のひとつとする GMD を実用化研究中心のフラウンホーファー協会と合併させては基礎研究が疎かになるとして、合併に反対する意見も聞かれる。

２．２　DFN-Cert 推奨の情報技術セキュリティ製品

現在 DFN-Cert が推奨している情報技術セキュリティ製品を以下に挙げておく。

その他の情報技術セキュリティ製品は、第４章の４．２項以降の製品のリストに掲載してある。

---

[10] １６の研究機関で構成され、ドイツ研究界の中心的存在となっている（連邦教育研究省管轄）。研究の中心は高度な技術設備や人材、多額の予算を必要とする研究で、研究は長期に渡り、国内外の他の研究所や研究者との共同研究も要求される。各研究機関の基本予算は連邦が９０%、研究機関の立地州が１０%の割合で補助している。

[11] フラウンホーファー協会は４９年に設立された技術の実用化を推進する応用研究開発機関で、国内に約５０の研究所、２１の研究所支部を備えているほか、国外にプレゼンテーションを目的とした４つのリソース・センターと４箇所に駐在員事務所を構えている。連邦と州の公的補助の対象となっており、連邦と州が９：１の割合で補助している。技術の実用化を推進するという特徴から、委託研究業務の占める割合も高い。なお、委託研究の約４分の３は経済・産業界からのものである。

[12] 第３章の３．３．３項参照。

ただ、商品の価格を挙げることは、公表されていなかったり、いろいろな仕様があるなどして簡単なことではなかった。そのため、わかる範囲で記入してある。記入されている場合は、工場引渡、ネット価格である。

ａ）ファイアウォール

* Articon 社：
  Firewall-1 (SunSPARC/SunOS4.1.3+Soliaris2.X, INTEL X86/Solaris 2.4/5, HP9000 700/800 HP-UX 9.0x/10.0 , Windoos NT, Windows 95 用）、Eagle 等
* Axis Information Systems 社：Raptor Eagle, The Wall
* BDG 社：Guardian (Windoos NT 用), Firewall-1, CyberGuard
* Biodata 社：BIGfire
* Bredex 社：
  UNIX, Windows NT, VMS 用インターネット・セキュリティ、ファイアウォール
* The Bristol Group 社：
  Checkpoint FireWall-1 (UNIX 用）, Checkpoint Fire Wall-1 SecuRemote (Windows 95, SUN OS, Solaris, HP-UX, Windows NT 用）
* Bull 社[13]：Netwall
* Centaur 社：インターネット・セキュリティ、ファイアウォール
* COMCAD 社：
  Firewall-1 (SUN, HP, Intel, Solaris, OpenLool GUI, Windows NT 用）
* Commercial Link Systems (CLS) 社：
  Concorde (Intel 用、Version 3.5＝ベーシック・ソフト、918 マルク）
* Competence Center Informatik (CCI) 社：ファイアウォール・システム
* Connect 社：ファイアウォール・システム
* Cybernet 社[14]：TIS Gauntlet, Sun Firewall-1
*ドイツ・テレコム社[15]：T-Intra-500-Protect
* Digital (DEC) 社：Altavista Firewall (UNIX, Windows NT 用）
* Axel Dunkel 社：
  TIS Gauntlet, Firewall-1, Borderware Firewall (Windows NT 用)
* easynet DV 社：FireWall/Plus
* Entrada Kommunikations 社：
  AltaVista (UNIX, Windows NT 用）, BIGfire, Borderware ,Norman Firewall
* GAI NetConsult 社：セキュリティ・コンセプト、ファイアウォール鑑定
* GeNUA 社：GeNUGate (主に Windows NT 用）

---

[13] 株式会社。その他は基本的に有限会社。ドイツでは日本と異なり、多くの企業が有限会社形態となっている。

[14] 脚注１３参照。

[15] 脚注１３参照。

* @GLOBE 社：Altavista Firewall, Secure Computing (Windows NT 用)
* IABG 社：TIS Gauntlet
* IBM 社：IBM Firewall
* ICON Systems 社：
  UNIX (Sun, HP, IBM), Microsoft (Windows, Windows NT 用)
  FireWall-1 （2000－70000 マルク）, Trend Micro Interscan VirusWall
* ID-Pro 社：
  GNU/Linux をベースとしたコネクション・ボックスとファイアウォールのシステム（2300－8100 マルク）
* INS 社：FLUX EF, FLUX AG, FLUX PR
* Integralis 社： Checkpoint FireWall-1
* in (統合情報システム）社：FireWall-1
* interface business 社：
  Firewall-1, AltaVista Firewall, Borderware Firewall (UNIX, Windows NT 用)
* INTERNET 社：BorderWare, Raptor Eagle, SmartGATE
* Internet2000 社：Altavista, BorderWare (UNIX, Windows, MAC 用)
* Internet SmartWare 社：販売は INTERNET 社経由
  SmartWall, BorderWare, Firewall (Windows NT 用)
* Intr@ware 社：Altavista, BorderWare (Windows NT 用)
* Iqproducts 社：FireWall-1, Trend Micro Interscan VirusWall
* iXnet 社：FireWall-1, Trend Micro Interscan VirusWall (UNIX 用)
* KrypNET Security 社：Firewall-1
* KryptoKom 社：KryptoWall
* Landis 社：Secure Computing, Raptor
* MANDATA System Consult 社：
  Secure Computing (Borderware) - (Windows NT, UNIX, HP3000 用)
* Microtec Electronic 社：
  Watchguard Firewall (Windows 95, Windows NT, Linux 用、5000－25000 マルク）
* Norman Data Defense Systems 社：Norman Firewall (Windows NT 用)
* PEM Intercomputing 社：Checkpoint Firewall-1（627－9600 マルク）
* POP Point of Presence 社：ファイアウォール・コンサルティング、構想、実現
* Prodata 社：Borderware, Firewall (Windows NT 用）, Sidewinder
* Quantum Software 社：
  ファイアウォール・サービス(SAP R/3, UNIX, Windows NT 用等)
* Sauer & Partner 社：FireWall/Plus
* SBK Software + Systeme 社：FireWall-1
* Siemens Nixdorf 社：Eagle
* Software Symbiose 社：Borderware, SmartFilter

* spring infotainment 社：BIGFire, TIS Gauntlet
* T&A SYSTEME 社：Ukiah NetRoad Firewall(UNIX, Windows NT 用)
* Telemation Netzwerk 社[16]：Cisco PIX Firewall
* topnet 社[17]：セキュリティ・コンサルティング、BorderWare Firewall Server
* Topologix 社：
  BorderWare Firewall Server(Windows, Windows NT, Digital UNIX, HP-UX, SCO UNIX, Solaris 用)
* WWL Connect Online Services 社：
  ファイアウォール、インタネット・セキュリティ
* Xlink 社：FireWall-1 (Checkpoint), NetWall (Bull 社)

b）暗号技術

1）ネットワーク層下流：

コンピュータとイーサネット間にブラックボックスとして使用される暗号ボックスが販売されている。暗号ボックスで伝送されるデータユニットを暗号化させ、受信側コンピュータにも同メーカのボックスを設置して、ボックスでデータユニットのコードを解くようにさせる。ドイツでは、以下の商品が入手できる。

* Kryptokom 社：KryptoguardLAN

たくさんのメーカが同じシステムを ATM でも使用しようとしている。ただ、イーサネットに較べて ATM は、155M ビット／s ないし 622M ビット／s と早くなるため、暗号化ハードウェアに高性能が要求される。現在販売又は開発されているソフトウェアは

* Cisco 社：ATM Encryption
* Cylink Corp. 社：Infoguard 100
* GTE Government Systems 社：FASTLANE ATM Encryptor (KG-75)
* MCNC 社：Enigma2 (DARPA プロジェクト)
* Secant 社：CellCase

と、ドイツ・メーカのものはない。ただ、ISDN 用のものとしてドイツ・メーカの

* Biodata 社：Babylon

がある。

---

[16] 脚注１３参照。
[17] 脚注１３参照。

2）ＩＰセキュリティ：

IPSEC 拡張は IPv6 に標準規定されており、すべての IPv6 インプリメンテーションにおいて IPSEC 拡張がなければならない。著名メーカのすべてが現在 IPv6 インプリメンテーションに取り組んでいるが、商品を入手することができるかどうかはまだ判断できない。ベータ・テスト・バージョンの中に米国の輸出制限からドイツで入手できないものがたくさんあるからである。

この分野の主な商品又は進行中のプロジェクトを挙げると以下のとおりとなる。

* FreeS/WAN プロジェクト (Linux) (oder FreeS/WAN プロジェクト)
* ipnsec (Linux)
* LIPsec-0.5 (Linux)
* JI Angelos IPSEC-Version
    - ipsec-0.5 (Linux)
    - BSDipsec (BSD/OS, NetBSD)
    - ISAKMP-Oakley (pluto-6.alpha) (Linux, BSD/OS, NetBSD, OpenBSD)
* OpenBSD はすでに IPSEC をソースツリーに入れている。
* Niels Provos Photuris Implementation (Solaris, Linux, OpenBSD, AIX)
* X-Kernel はアリゾナ大の IPSEC Implementation (Linux)をベースとした。
* NIST Cerberus (Linux)
* NRL IPSEC と IPv6 Implementation (BSD 4.4-Lite)
* Cisco 社： ISAKMP-Oakley Implementation (BSD 4.4)
* US DoD ISAKMP-Oakley Implementation
* FreeBSD IPSEC/Mobile-IP Implementation (mirror) (FreeBSD)
* Itojun 社：IPSEC Implementation (FreeBSD, BSDI)

商用 IPSEC インプリメンテーションとして

* SSH IPSEC Express は基本ソフトやルータ、ファイアウォールに IPSEC インプリメンテーション用のユニットを入れたツール・キットである。
* SSH ISAKMP/Oakley は SSH IPSEC Express と組み合わせることのできるキー管理機能インプリメンテーションである。

を挙げることができる。

3）SKIP：

SKIP は、二者択一キー管理プロトコルを利用する特殊 IPSEC インプリメンテーションである。SKIP は SUN によって開発されているが、現在 Solaris2.6 とともに市場

に出回っている。SKIP が ITEF 標準（IPSEC ISAKMP-Oakley）と食い違っていても、SUN ワークステーションが普及していることから、SKIP が将来インターネットにおいて重要になることは間違いない。
　SKIP インプリメンテーションとして、

* Sun SKIP 1.1 (Solaris, Windows-95 用)
　　・ FreeBSD 2.2.5 Patches (Sun SKIP Source Release 1.0 用)
　　・ FreeBSD Port (Sun SKIP Source Release 1.0 が必要)
* ETH 社（スイス・チューリヒ）：ENskip (mirror) (Solaris, Linux 用)
* Elvis 社： Windows (3.11, 95, NT)用 SKIP

がある。

4）Virtual Private Networks (VPN)：

IPSEC の意図は、将来 IP ホストのほとんどが IPSEC もサポートし、それによってインターネット上のホスト通信の安全を可能にするというものである。しかし、IPSEC の主要適用領域は現在 VPN 構成となっている。
主なソフトウェアとして以下を挙げることができる。

* Biodata 社：BabylonSec, BabylonNet
* hifn 社：MUM 1.0
* IRE 社：SafeNet VPN Encryptor
* Secure Computing 社：NETCourier
* TimeStep 社：Secure Virtual Private Networking

5）TLS --- Transport Layer Security：

TLS 仕様は主として SSL(Secure Socket Layer)をベースとしている。SSL は Netscape によって開発されたもので、現在たくさんのブラウザによってサポートされている。
現在、以下のソフトウェアが入手可能である。

* Netscapes SSL Informationen
* SSLeay
* SSR

6）Secure-DNS：

暗号署名に関しては、DNS 情報の信憑性と完全性が確認されなければならない。RFC-2065 で定義された標準のサンプル・インプリメンテーションが Paul Vixie 社の

Bind-4.9.5 をベースに Trusted Informations Systems 社(TIS)によって開発された。それが以下のソフトウェアである。これは今後 Bind-8.X バージョンに統合される予定である。

* TIS DNSSEC Beta 1.4.0

７）SSH：

SSH は、安全とはいえない rlogin プロトコルと rsh プロトコルに代わる安全なプロトコルとなった。SSH の場合も rlogin、rsh と同じユーザ・インターフェースとなるが、SSH は、RSA 署名によって情報の信憑性を証明してその後のデータ通信を暗号化する。SSH は商用ソフトウェアとしてもシェアウェアとしても入手できる。

* 商用 SSH Implementation (UNIX, Windows, Macintosh 用)
* シェアウェア SSH Version (mirror) (UNIX 用)

８）Kerberos：

Kerberos は、MIT においてネットワーク用信憑性証明システムとして開発された。わずかなバリエーションを含んでいるものもある。現在たくさんの商品に見られる。

* Kerberos V5 (RFC-1510)

９）電子メール・セキュリティ：

電子メールの安全では、PGP が最も普及している。S/MIME のように現在開発されているものもあるが、これらはまだ開発の初期段階にある。PEM は 1993 年以降 RFC として入手できたが、現在はもう多くの分野で使用されていない。

* PGP : PGP-2.6.3i (mirror) (UNIX, Windows, Mac 用)
  PGP-5.0i (mirror) (UNIX, Windows 用)
* RSA : S/MIME
* PEM (RFC-1421), (RFC-1422), (RFC-1423), (RFC-1424)

１０）ツールキット：

ツールキットには、これまで挙げた方式を構成するのに役立つユニットが含まれている。ここでは、それが API であったり、暗号方式であったり、PKI ユニットであったりする。

* e-Lock 社：e-Lock Toolkits
* Entrust 社：EntrustIPSec Negotiator Toolkit

２．３　HBCI／ホームバンキング・コンピュータインターフェイス

HBCI はホームバンキング標準である。ドイツの大手金融機関は２年前に同標準の導入に合意しており、HBCI がドイツの標準として導入されるものと見られている。最初の機能インプリメンテーションは、HBCI2.1 バージョンをベースとして、９９年末からドイツの大手銀行で実施されている。同標準の中心は、RSA 暗号方式によるセキュリティの高さ、電子署名、プロバイダーとソフトウエアからの独立性である。同標準で注目すべき特徴はデータの暗号化と認証方式である。

HBCI の暗号方式は非対称的で、公開鍵と非公開鍵で構成される鍵ペア２つが必要となる。銀行とクライアントはそれぞれ公開鍵と非公開鍵を所有する。すべてのトランザクションは受信者の公開鍵によって暗号化される。例えばクライアントが銀行に送金依頼する場合、クライアントは銀行の公開鍵を使って暗号化し、クライアントからのメッセージは銀行の非公開鍵によって銀行だけが読み出すことができる。さらに、送金依頼はクライアントの非公開鍵で電子署名される。その際、メッセージ全体に関する固定長のハッシュ値が作成され、ハッシュ値はクライアントの非公開鍵によって送信される。電子署名はどれもメッセージの内容とペアになっており、送信路で書き換えられなかったことを証明する。銀行は送金依頼を受信すると、データが本物であるかをクライアントの公開鍵で検査し、送信者が本人であることを確認する。

２．４　情報セキュリティ専門見本市：infosecurity.de

ドイツ初の情報セキュリティ専門見本市 infosecurity.de が、９９年１０月２６日から２８日までフランクフルト／マインで開催された。約９０社が出展した見本市には約４０００人の専門家が訪れ、見本市は成功裡に終わった。見本市の発起人は REC（Reed Exhibition Companies）社で、同社では、ドイツはイギリスに並ぶ情報セキュリティ製品の重要な市場であるとしている。見本市で紹介された製品は、インターネット・セキュリティ、ファイアウォール、バーチャル・プライベート・ネットワーク、PKI、ネットワーク・セキュリティ、暗号技術、コンピュータ・データ処理故障センター、電子商取引、スマートカード、データ伝送、ウイルスからの保護、ネットワーク・システム管理、接続管理、ソフトウエア審査等である。

なお、infosecurity.de ではメーカー主催のセミナーや基調講演等も実施された。

第３章　情報セキュリティと法律の動向

３．１　ドイツの暗号技術政策

連邦政府は９９年６月２日、暗号技術を電子商取引に利用する場合の規準を「ドイツの暗号技術基本政策」としてまとめ、閣議決定した。これは、安全な暗号技術を導入することによって、情報技術のグローバル利用においてドイツのユーザーをより保護することを目的としている。閣議で決定された内容は、ドイツでは将来も暗号方式や暗号製品が制限なく開発、製造、販売、使用されることを明確にしており、それによって、これまでセキュリティ問題にあまり真剣に取り組んでこなかったユーザーの意識化を図ろうとしている。連邦経済技術省と連邦内務省が共同で開始したイニシアチブ「インターネットのセキュリティ」も、政府のこの路線に沿うものである。

連邦政府はまた、ドイツの暗号技術メーカーの能力と国際競争力の強化を目指している。暗号技術市場では今後需要が伸びることが予想されるため、一層の市場努力が要求される。連邦政府は他の EU 加盟国と共同で、欧州経済共同体デュアルユース指令の第一回改正によって暗号技術に係る量産製品の域内輸出規制を廃止しており、それに伴う EU 域内市場開放によって暗号技術を巡る国際競争が一層激化するものと予想される。また、連邦政府は、連邦輸出庁と輸出規制手続きの簡素化も検討している。

連邦政府は、暗号技術の利用が増加するにつれて、技術を不法な目的で乱用するケースが増加するのを否定できないと見ており、そのため、連邦関係省庁で今後の動向を観察して、2 年後に報告書を作成することになった。

連邦政府がまとめた「ドイツの暗号技術基本政策」は以下のとおり。

１．連邦政府は、ドイツにおける暗号製品の使用を制限することを考えていない。連邦政府は、安全な暗号技術の使用が国民のデータ保護、電子商取引の発展、企業の秘密保持に重要な前提であると考えている。したがって、連邦政府は、ドイツにおける安全な暗号技術の普及を積極的に支援する。ここでは特に、国民、経済界、行政機関の中に情報技術の安全性に対する意識を高めることも含まれる。

２．連邦政府は、ユーザーが暗号技術の安全性に信頼を抱くことができるように努力する。したがって、連邦政府は、安全な暗号技術に対する信頼を築くための措置として、特に、暗号製品の安全機能の検査方法を改善し、検査に合格した製品の利用を推奨する。

３．連邦政府は、国家と経済、社会の安全のため、安全で高性能の暗号製品を開発、製造するドイツ製造メーカーの能力を放棄できないと考える。連邦政府はそのため、業界の国際市場競争力を強化するための措置を講じる。

４．安全な暗号方式の普及によって、通信を監視する犯罪捜査当局やセキュリティ関連当局の法的権限が空洞化されてはならない。したがって、この問題に関係する連邦省庁は、今後も動向を注意深く見守り、2 年後にこの問題に関する報告書を作成する。さらに連邦政府は、犯罪捜査当局やセキュリティ関連当局の技術能力を改善するよう努力する。

５．連邦政府は、暗号技術政策の分野で国際協力することに重点を置く。連邦政府は市場で開発されているオープン標準とインターオペラビリティのあるシステムを支持し、多国間、二国間レベルの協力の強化に努力する。

３．２　電子署名

情報通信サービス法（俗にマルチメディア法）[18]が施行されて２年以上が経過したが、連邦政府は、同法の国会通過時の決定に従い、同法の実施に関する経験を集めた報告書を作成した。コンピュータ不正アクセスや電子署名等に関して連邦政府は報告書[19]で次のように結論づけた。

・　これまでの経験によれば、電子署名法[20]と電子署名令[21]を根本的に改正しなければらないという要因はない。しかし、職業法的登記を証明書に記載する、認

---

[18] ９７年８月１日施行。市場経済原則に基づく新しい電子サービスの法的基盤を確立した。青少年保護、消費者保護、知的財産権保護に関する重要な法的基盤も整備された。同法の目的は、「情報通信サービス分野においてダイナミックに発展するサービスを形造るための基本を提示して、自由競争と正当なユーザーの利益、公共秩序の間に平衡をもたらす」ことである。法律の中心は、

・新しい情報通信サービス分野において市場の自由な発展を妨げる障害を除去して、サービスを提供、利用するための統一された経済条件を保証する
・データ保護、データの安全、著作権、青少年保護、消費者保護上必要な規則を導入して、それを管轄する

ことにある。しかし、同法の原則は規制緩和であり、内容は経済上の発展に必要な法的基本条件を記述するのに必要なだけの規制に制限されている。特に、サービス提供者の責任やデータ保護、電子署名に関する規制はこれまでにはなかった新しいもので、新規制によって情報通信分野における新しい法的規制と新技術の発展、新しいサービスの受け入れを推進するとともに、この分野で規制を国際的に標準化するための土台となるものである。

[19] 情報通信サービス法の実施に関連する新情報通信サービスの経験と動向に関する連邦政府報告書、９９年６月１８日付け、連邦議会印刷物 14/1191 番。

[20] ９７年８月１日施行。箇条法である情報通信サービス法の第３条に当る。以下の電子署名令とともに、デジタル式データ・ネットワークにおいて法的拘束力を有する契約の締結を可能としている。ユーザーは電子署名するためにカード(クレジットカード大)とカード読取機を使用する。

[21] ９７年１１月１日施行。

証機関を法的に定義する場合等で関連規定を明確にする必要があるほか、法律に準拠する電子署名の国際的認知を容易にするためにセキュリティの国際検査基準の適用に関する記述を電子署名令に補足する必要があるなど、個々に適切な措置が必要である。

・　現在の状況から判断すれば、電子署名に関する EU ガイドラインは電子署名法に根本的な適合措置を要求していない。ただ、EU ガイドラインによると、規制範囲を「簡単な」電子署名と責任規定にまで拡大することが必要となる。また、これまでの認証機関の許可手続きの他に「資格証明書」を交付する未許可認証機関を効果的に管理していかなければならない。

連邦政府は現在、私法上の書式規定を最新の商取引に適応させるための法案を作成している。特にここでは、電子署名をできるかぎり民法典§126[22]の法的書式と同等に扱うことが予定されている。そのため、民法典に新しい「電子書式」に関する記述が補足され、「電子書式」が書式のオプションとして根本的に利用されることになる。電子書式は電子署名法の要求を基本にしている。公法上の規制に関しても検討しているところである。また、社会保険制度における会計規則の改訂も実施された。ドイツでは電子署名法の制定がそれに応じた民法や公法の法律改正を推進することが期待されており、電子署名の実施に向け、法的基盤が徐々に整備されている。

３．３　電子署名の実態

政府の通信郵便業務統制局[23]は、欧州規模での公募後の９８年３月、ドイツテレコムに電子署名法に基づき認証機関を認定するための認定機関（トラストセンター）の構築を依頼した[24]。電子署名法によると、通信郵便業務統制局は認証機関の経営許可の授与、証明書の発行、関連規則遵守の監督を担当する。トラストセンターは９８年９月、通信郵便業務統制局に引渡され、同局の電子署名鍵も作成された。９９

---

[22] 一つ又は複数の意思表示からなる法律行為に関する規定の一つ。

[23] ９８年１月１日付けの通信、郵便業務の自由化に伴い、連邦郵政省が閉鎖され、これらの業務を監督、統制する機関として通信郵便業務統制局が設置された。

[24] 認証機関の認定機関を設置する前から認定機関（俗に「電子公証人」）として名乗りを挙げている組織もある。トリーア市のトラストセンターがそのひとつで、フランホーファー・テレマティック研究所と共同で設立された。同センターでは電子署名を公証するばかりでなく、送信図書が発信人と受取人以外に盗み見される可能性がないかについても監視する。センターからは公開コードと個人コードが記憶されたチップカードを受け取ることになる。チップカードがデータへのアクセスを細かく制御する可能性を提供するため、行政機関や企業でこの種の技術が盛んに利用されることも予想される。例えば、ドレストナー銀行では電子バンキングの普及で電子署名が重要な役割を果たすと見て、フランホーファー・テレマティック研究所とともに内部認証するための組織造りを開始した。

年１月 25日から通常事務が開始され、電子署名法が要求するように２４時間体制を取っている。

しかし、電子署名を巡るインフラストラクチャーを確立した後になって、電子署名普及への期待が大きすぎたことが判明した。ドイツテレコムの製品センターTelesec では、営業開始初年に電子署名パッケージ製品で約 3 万人の顧客を見込んでいたが、期待は大きく裏切られたほか、通信郵便業務統制局でも９９年１０月末時点でオンライン認証機関登記目録の利用者は３００人にも達していない状況である。

連邦政府は、電子署名をはじめ電子商取引の普及等新しい情報通信技術の利用を加速させるために公的機関が先駆者になるべきだと考えており、２０００年夏までに包括的な情報技術戦略案を提示する予定である[25]。なお、電子署名に関してはすでに以下の２つの例が見られる。

３．３．１　ニーダーザクセン州行政機関

ドイツ北西部に位置するニーダーザクセン州では、２０００年はじめに、連邦州では初めて電子署名が公共の行政機関に導入された。プロジェクトが完全に実現されるのは２００１年になる見込みだが、７００箇所で約１万２０００人が電子署名を利用することになるという。２０００年１月にはすでに、州大蔵省を中心として最初の７０００人に必要なソフトウエアとハードウエアが配備された。

同州の電子署名の中心となるのは「署名カード」と呼ばれるチップカードで、将来は署名カードによって支払い指示書が電子署名される。これによって、これまで実行されてきた会計用紙の手書き署名は廃止される。さらに将来は、受信者に至るまでのデータ保護の役割を果たす封筒の機能も、暗号技術によってチップカードで実現される。そのため、署名カードには公開鍵と非公開鍵からなる署名鍵ペア以外にもうひとつの鍵ペア（いわゆる「暗号鍵ペア」）が含まれている。それによって、データのやりとりがクライアント／サーバー型に暗号化される。同時に、担当者がカードを所持し、操作知識を持っていることが機能を利用する前の段階で自分を認証することにもなるため、署名カードの利用によって安全性が高められる。つまり、正しいチップカードとパスワードが使用されない限り、正当なユーザーとして予算データや入力マスクにアクセスできないシステムとなっている。

以上の機能を実現するため、以下のものが使用される。

・署名カード
・チップカード読取機（utimaco 社製）
・ソフトウエア構成
　－電子署名：BaaN 社製 PPM（Public Performance Management）

[25] 現在まで計画されている内容を付録１）に挙げておいた。

－暗号化：Secude 社[26]の STP（Secure Transport Provider）
－チップカードの使用解除、パスワードの変更機能：（PSE-Management）
－読取機のオペレーション：（ドライバー・ソフトウエア）

３．３．２ Sphinx

連邦内務省は、連邦省庁内／間の端末間セキュリティ・パイロット試験 SPHINX を実施しており、それによって連邦の行政機関における電子署名の導入と電子メッセージ・図書の暗号化が準備されている。試験に参加するのは、連邦の行政機関、州の行政機関、地方自治体の行政機関、経済界、団体等の職員である。

安全インフラストラクチャーに対する要求とパイロットプロジェクト SPHINX の目的は、以下のようにまとめることができる。

・製品メーカーに関係ないインターオペラビリティ。製造メーカーの異なる製品間においても、電子署名、暗号化されたメッセージを交換できる
・利用者からの受け入れ易さ、製品価格と性能のつりあいが取れ、操作しやすい（一般に普及している電子メール・ソフトウエアを利用できる）
・安全インフラストラクチャーの将来性の保証
・各コンポーネントと組織上の措置のセキュリティ水準が統一的に定義され、それが個々に検査できる
・機能性の実験と再開発
・人員や資金、組織面でのコストの評価

現在は電子署名と暗号技術を幅広く導入するための条件が設定されている段階で、まずベルリン・ボン情報ネット（IVBB）[27]で実施される。これに並行して、第三試験期では、別の機能性、特に証明書フォーマット X.509V3 とメール交換フォーマット S/MIME のインターオペラビリティがテストされる。 SPHINX の概要を表３－１に、パイロット試験への参加機関を表３－２にまとめておいた。 表の中で網掛けで表示した機関は第 2 期から新しく参加した機関であるが、今後新たにパイロット・プロジェクトに加わることも可能である。

---

[26] 同社は１９９６年１２月にドイツの大規模研究機関（ヘルムホルツ・センター）のひとつであるＧＭＤ情報工学研究センターから誕生した。SECUDE は Unix、MS-DOS、Windows95/NT 上で作動する携帯型安全ツールキットで、非対称／対称暗号を含んでいる。１９９１年から開発され、RSA や DES 等の暗号アルゴリスムと GSS-API や X509、PEM 等の標準プロトコルを実現する。個人コードの悪用から保護するため、チップカードも使用される。

[27] 政府、議会のベルリン移転によって行政機能が制限されないようにするため、情報通信ネット、ベルリン・ボン情報ネット（ＩＶＢＢ）が設置された。ＩＶＢＢは技術的に広帯域応用を要求しており、複数の場所からの図書の共同処理やマルチメディア、ビデオ会議を可能とし、イントラネット、Ｘ．５００等新しい情報処理技術を広範に適用している。なお、ＩＶＢＢはすでに９９年１月１日にスタートした。

表３－１　SPHINX 概要

活動内容	備考
第１期（１９９８年）： ユーザーが利用しやすいメール・アプリケーションの統合 インターオペラビリティ コスト見積（人員、資金、組織）	
第２期（１９９８／１９９９年）： ディレクトリ・サービスの確立 ディレクトリ・サービスの統合 ・クライアントと認証局（CA） ・証明書と証明書廃止リスト（CRL）の封鎖リスト 認証局（CA）製品とクライアント製品間の互換性 インターオペラビリティ機能領域の拡大 PKI[28]内プロセス組織を規制するための組織マニュアルの作成	
第３期（１９９９年半ば －２０００年半ば）： 第２期で未完了のもの メールトラスト・バージョン２の実施[29]。特に ・メール交換フォーマット：S/MIME ・鍵分離を含む証明書フォーマット：X.509V3 (Version 97) 認証局（CA）への要求 いくつかの認証局（CA）オペレータとの共同 PKI	 S/MIME：他の製造メーカーの製品との互換性、安全な暗号化の可能性、実績に対するテスト
第４期（準備期間：１９９９年後半、実施期間：２０００年より） 安全なオンライン接続、SSL の統合 チップカードのフォーマットとチップカード読取機のフォーマット 電子署名法に準拠 電子署名令に準拠 評価の可能性 時間スタンプ・サービス 資料保管	討論ベースとして計画 場合によっては Ipsec に従事 共通基準[30]、電子署名法の要求との比較

（出所：SPHINX 第２期最終報告書、GMD 情報工学研究センター）

[28] Public Key Infrastructure

[29] 第３章の３．３．３項参照。

[30] 第４章の４．１項参照。

表３－２　SPHINX 参加機関一覧（１９９９年３月１５日現在）

AA	連邦外務省
Bayr.Lda.f.Stat	バイエルン州統計データ処理局
BK	連邦首相府
BKA	連邦刑事警察庁
BMBau	連邦国土計画・土木建設・都市計画省[31]
BMBF	連邦教育学術研究技術省[32]
BMF	連邦大蔵省
BMI	連邦内務省
BMV	連邦交通省[33]
BMVg	連邦国防省（業務分野：連邦防衛行政庁）
BSI	連邦情報技術安全庁
Bundesdruckerei	連邦印刷局
BVA	連邦行政庁
DATEV	DATEV
DBT	ドイツ連邦議会
DIZ	マインツ・データ情報センター（ラインラント・プファルツ州）
DLR	ドイツ航空宇宙センター
DVZ M-V	メクレンブルク・フォアポムメルン州データ処理センター
GHP	Gora. Hecken & Partner Management- und Technologieberatung GmbH
HiServ GmbH	HiServ GmbH
HZD	ヘッセン情報処理センター
In.Min.d.Schl-Hol.	シュレスヴィヒ・ホルシュタイン州内務省
IZN-Hannover	ニーダーザクセン情報センター
KBA	連邦交通庁
Ld Rhein.-Pfalz	ラインラント・プファルツ州内務スポーツ省、 ラインラント・プファルツ州経済農業交通ブドウ栽培省
Lda.f.DV.Potsdam	ポツダム情報処理統計庁（ブランデンブルク州）
RegTP	連邦通信郵便業務統制庁
Sächs. Staatskanzlei	ザクセン州首相府
Sächs.Min.d.In	ザクセン州内務省
Sen.Kom.Pers.Bremen	ブレーメン市（州）政府人事委員会[34]
Stadtwerke München	ミュンヘン都市電力
TEKO	TEKO Ingenieurbüro GmbH
Telekom	ドイツテレコム IVBB 中央製品管理

（出所：SPHINX 第２期最終報告書、GMD 情報工学研究センター）

[31] 新政権誕生に伴い、連邦交通省と統合された。

[32] 新政権誕生に伴い、技術部門が連邦経済省に移管され、連邦教育研究省と改名された。

[33] 新政権誕生に伴い、連邦建設省と統合された。

[34] ブレーメンは都市であるが、州扱いされる特別州。

なお、プロジェクトは第 3 期はじめから連邦情報技術安全庁（BSI）によって管理されている。同パイロット試験の調整事務は、連邦内務省内に設置された連邦政府連邦行政機関情報技術調整相談部（KBSt）によって行われている。

＜利用製品＞

１）エンドユーザー製品

第 2 期に利用されたエンドユーザー製品を表３－３に示しておく。製造メーカー8社から計１０製品がパイロット試験での使用を認められた。第 2 期においては製造メーカーのうち 5 社に対して新バージョンの使用が許可されており、当該製品には表３－３中で（新）と付けておいた。なお、３つの製品がディレクトリ・サービスへのアクセスをサポートする。

表３－３　エンドユーザー製品

製品名	製造メーカー	バージョン
AuthentEmail	SECUDE	2.0.7 (新)
PEMPro Plug-In	Siemens Bereich ICT	2.0.5 (新)
PEMPro Editor	Siemens Bereich ICT	2.0.1 (新)
MULTISEC Mail	CoCoNet	2.1.3 (新)
EADI Crypt MSExchange	G & D	2.00.02 (新)
SmartGuard MTT – File Utility	KryptoKom	2.0 (新)
SmartGuard MTT	KryptoKom	2.20 (新)
CEMENT	Concord-Eracom	1.14
Safeguard Sign & Crypt	Utimaco	2.0f Beta
PEMCENTER	Algorithmic Research	データなし

（出所：SPHINX 第２期最終報告書、GMD 情報工学研究センター）

２）認証機関用製品

表３－４に示すのは、パイロット試験で使用された認証機関用製品である。製造メーカー2 社が第 2 期に新バージョンを導入しており、表３－４中に（新）と付けておいた。なお、1 社については既存製品に補助ソフトウエアが納入された。

表３－４　認証機関用製品

製品名	製造メーカー	バージョン	補助ソフトウエア
OpenPathCA	SSE	2.0.5 (新)	
SECUDE CA Management	SECUDE	2.0.7 (新)	
MULTISEC Trustcenter 500	CoCoNet、G&D	1.0	G&D から

（出所：SPHINX 第２期最終報告書、GMD 情報工学研究センター）

３）ディレクトリ・サービス用製品

X.500 ディレクトリ・サービスのオペレーションには、ジーメンス社の DirX[35]が利用された。なお、SPHINX に利用された暗号技術は、メールトラスト仕様バージョン２[36]をベースとしている。

３．３．３　メールトラスト

メールトラストは、オープンな情報環境において加入者へランダムアクセスする電子メールとファイル転送に暗号技術を応用するためのシステム・コンセプトで、ハードウエア・メーカーやインターネットサービス会社、情報セキュリティ会社の組織団体であるドイツ・テレトラスト（TeleTrust Deutschland e.V.）[37]によって開発された。

メールトラストの構成においては、以下を前提として利用者に信頼性のある技術を提供しようとしている。

・汎用セキュリティ技術の利用、ユーザーの登録認証と鍵の配布（例えば、RSA アルゴリズム、楕円曲線アルゴリズム等）に非対称的暗号方式（公開鍵暗号方式）、容量が大きいデータ暗号化に対称的暗号方式（例えば、DES（Data Encryption Standard）アルゴリズム、IDEA（International Data Encryption Algorithm）アルゴリズム等）
・セキュリティ技術の有効性の公開管理能力
・技術のセキュリティは加入者の非公開鍵の秘密厳守にだけ基づくものであって、秘密アルゴリズムをベースとしたものであってはならない
・信頼できる第三者機関（認証局やトラストセンター）の利用は、望まれない管理や必要のない（中央）管理につながるものであってはならない
・セキュリティ技術は情報に対するユーザーの自主決定を可能とし、これを奨励すべきである
・公開セキュリティ情報は、一般にアクセスできるディレクトリに含める
・セキュリティ機能は、ユーザーの利用環境を変更したり、制限することなく利用できるものとすべきである

これらの規準と電子署名法による法的制限を満たすため、インターネットの技術標準とメールトラストに参加する情報セキュリティ製品の開発者の技術コンセプトを、ドイツの主な適用分野（医療・健康保険行政機関、連邦省庁、州省庁、一般電

---

[35] X.500 (93)と Internet LDAP をベースとするディレクトリ・サーバー（Windows NT、UNIX 用）。

[36] 次項、３．３．３項参照。

[37] １９８９年に情報通信業界を中心に設立された。協会は、電子署名の受け入れ推進、電子情報交換の安全を強化する研究開発とその成果の商品化の推進、セキュリティ分野における技術標準化の推進等を行っている。協会にはＩＢM社、ジーメンス社、ドイツテレコム社の大手企業のほか、たくさんの中小企業も参加しており、会員数は約９０社に上る。

子法的取引）の組織上の条件と結び付けるのがメールトラスト仕様で、メールトラスト仕様は、セキュリティ・サービスの国際的なインターオペラビリティとそれに応じたドイツ国内でのセキュリティ・インフラストラクチャーを実現する。また、メールトラスト仕様は同時に、セキュリティ製品に対するテレトラスト協会による品質保証となる。

テレトラスト協会の会員企業によって提案されたシステムは、利用者に本人確認／登録認証する暗号方式、つまり電子署名と暗号化を提供するもので、セキュリティに対する要求が広範な環境において異なる製造メーカーの製品を使用して利用できるオープン情報システムが利用可能となる。インターオペラビリティはデータ交換フォーマットの統一と利用される安全インフラストラクチャーの共同化によって保障される。

現在有効なメールトラスト仕様バージョン２の詳細は以下のとおりである。

１）構成要素と PKI[38]構造：

・メールトラスト認証局の RA 構成要素は個々に実現可能なものとする
・電子メールをベースにしたプロトコルばかりでなく、ディレクトリ・アクセスによる証明書と証明書廃止リスト（CRL）の照会
・復号鍵のバックアップ
・クロス認証の可能性

２）証明書フォーマット：

・X.509v3 証明書フォーマット
・証明書拡張選択
・署名鍵と暗号鍵の分離、複数の鍵ペアの利用

３）認証要件：

・証明書を申請、呼び出すための新しいプロトコル（PKIX の部分量）
・プロトコルは、信頼できる認証の照会を可能にする対称的プロトコル（PKIX による）分だけ補足される

４）証明書撤回：

・X.509v2 証明書廃止リスト・フォーマット
・LDAPv3 のディレクトリ・サービスにアクセスすることによる証明書廃止リストの呼び出し
・MTT クライアントによる証明書廃止のための対称的プロトコルとデータフォーマット

[38] Public Key Infrastructure

・認証局で証明書廃止リストを確認するためのプロトコルと証明書廃止リスト・フォーマット。電子メールでも可能

5）鍵のバックアップ：
・暗号化された図書を元の平文に戻すための暗号鍵をバックアップするためのプロセス、接続プロトコール、フォーマットの仕様

6）PSE インターフェイス：
・暗号トークン又はソフトウエア PSE への PKCS#11 の部分量として規定された　インターフェイスが DIN（ドイツ工業）規格と一致しているか検査される

7）アルゴリズム：
・アルゴリズムが（初期）PKI[39]メッセージを確保するための MAC（メディア・アクセス制御）方式分だけ補足される
・アルゴリズム・リストの最新化。メールトラスト・バージョン２では、例えばハッシュ機能 RIPEMD-160 と電子署名方式 DSS が考慮されている。MD5 は、バージョン１．１と互換性のあるメッセージと署名検査を作成する場合だけにサポートされる

8）交換フォーマット：
・交換フォーマットが最新の図書フォーマット分だけ拡張される
・新しい条件付き交換フォーマットを S/MIME ベース上に導入する。ただし、これは後で PEM ベース上の交換フォーマットと交換される

[39] Public Key Infrastructure

第４章　情報技術セキュリティの認証

４．１　CC (Common Criteria) - ISO/IEC15408

情報セキュリティの審査と評価を国際的に統一するための共通基準、CC (CommonCriteria）が９９年に国際標準化機構と国際電気標準会議の規格 ISO/IEC 15408 として公開された。全ての情報技術関連製品と情報技術関連システムの安全性は、これを基準にして検査することができる。各国の国内基準と欧州の ITSEC を基に作られた CC は、国際的に統一されたセキュリティ評価の基盤として様々な可能性を提供する。

CC はすでにドイツでも広範に利用されており、最初の CC 証明書がすでに公開されている。また、CC プロジェクトに参加する機関では CC が認証の基盤として一段と活用されるようになっており、スマートカードばかりでなく、オペレーション・システム等従来の分野でも CC の適用件数が増加している。さらに、再認証の形で行われる ITSEC から CC 証明書への移管が、両基準に広範囲な互換性があることから、特別大きな出費なしに可能であることも判明した。

なお、ドイツは９８年１０月に英国、フランス、カナダ、米国とともに CC 証明書の相互承認協定に調印した。

４．２　BSI 証明書のある情報技術製品

表４－１　大型コンピュータシステム

製造メーカー／販売者	製品	製品タイプ	結果 ID 認証日
IBM Corporation	PR/SM for IBM S/390 CMOS Computer System Family 6972-G5	オペレーティングシステム	E4 BSI-DSZ-ITSEC-0142-1999 1999 年 3 月 11 日
Siemens-Nixdorf Informationssysteme AG	BS2000-SC Version 10.0	Siemens-Nixdorf-Systemfamilie 7500(/370-, /370-XA 利用メインフレーム・アーキテクチャ)用オペレーティングシステム。Basisversion BS2000Version10.0 用セキュリティパッケージ SECOS Version1.0 を含む。	Q3, F2[40] BSI-ITEC-0004-1992 1992 年 10 月 9 日

[40] ITSEC 評価 E3, F-C2 に相当。

表４－２　中型システム

製造メーカー・販売者	製品	製品タイプ	結果 ID 認証日
Bull S.A.、IBM Infotmationssysteme Deutschland GmbH	B1/EST-X Version 2.0.1 with AIX, Version 4.3.1	オペレーティングシステム	EAL4 BSI-DSZ-CC-0143-1999 1999年3月11日
IBM Informationssysteme Deutschland GmbH	AIX V 4.2	UNIXオペレーティングシステム	E3/高 BSI-ITSEC-0126-1997 1997年4月24日
IBM Informationssysteme Deutschland GmbH	AIX V 4.3	UNIXオペレーティングシステム	E3/高 BSI-ITSEC-0138-1998 1999年5月6日
Siemens-Nixdorf Informationssysteme AG	SINIX V5.42/ AUDIT V1.0	UNIXオペレーティングシステム	E2/中, F-C2 BSI-ITSEC-0083-1995 1995年10月13日
Siemens-Nixdorf Informationssysteme AG	Reliant UNIX 5.43 with AUDIT V2.0	UNIXオペレーティングシステム	E3/高 BSI-ITSEC-0127-1997 1997年4月24日
Tandem Computers GmbH	GUARDIAN 90 Version C20 with Safeguard Version C22L	Tandem NonStopコンピュータ用オペレーティングシステム	Q3, F2及びF7[41]E3/高 F-C2及びF-AV BSI-ITS-0017-1993 1993年10月12日
Siemens-Nixdorf Informationssystme AG	SINIX-S V5.22	MX300-Familyコンピュータ用UNIXオペレーティングシステム	Q2, F1~F2[42] BSI-ITS-0003-1991 1991年7月26日

[41] ITSEC評価E3, F-C2とF-AVに相当。

[42] ITSEC評価E1, F-C1からF-C2に相当。

表４－３　PC セキュリティ：セキュリティ・サーフェイス

製造メーカー・販売者	製品	製品タイプ	結果 ID 認証日
Utimaco Safeware AG	Safeguard Easy OS/2	OS/2 用 PC セキュリティ製品	E2/中 BSI-ITSEC-0058-1997 1997 年 9 月 23 日
Deutsche Telekom AG	SIKOM-TIBIS Version 002.05	PC セキュリティ製品	E3/高 BSI-ITSEC-0069-1996 1996 年 4 月 29 日
Utimaco Safeware AG	Safeguard Easy for DOS, v.2.0, ドイツ語／英語	PC セキュリティ製品	E2/中 BSI-ITSEC-0012-1992 1995 年 6 月 27 日
Computer Elektronik Infosys GmbH	WISO-Crypt Version 1.2	PC セキュリティ製品	E1/中 BSI-ITSEC-0057-1993 1994 年 12 月 21 日
Utimaco Safeware AG	Safeguard Professional 4.1A、追加オプション付き	PC セキュリティ製品	E2/中, F-C2 BSI-ITSEC-0013-1992 1994 年 3 月 17 日
Utimaco Safeware AG	Safeguard Professional 4.1A 英語版、追加オプション付き	PC セキュリティ製品	E2/中, F-C2 BSI-ITSEC-0072-1994 1994 年 10 月 28 日
PSB Gesellschaft für Programmierung und Systemberatung GmbH	Firmloc 2.11	PC セキュリティ製品	E2/中 BSI-ITSEC-0052-1993 1994 年 10 月 28 日
Utimaco Safeware AG	Safeguard Professional 3.1Z	PC セキュリティ製品	Q1, F1 から F2[43] BSI-ITS-0002-1991 1991 年 3 月 1 日

[43] ITSEC 評価 E1, F-C1 から F-C2 に相当。

表４－４　PC セキュリティ：完全性保護

製造メーカー・販売者	製品	製品タイプ	結果 ID 認証日
Arktos GmbH (元 Peter Hoffmann SERVICE GmbH)	PC-Safe B.I.V. Version 9.1	完全性保護用 PC 製品、正式に認められていないプログラムやデータの変更の確認と記録	E1/中 BSI-ITSEC-0015-1992 1994 年 4 月 6 日
Arktos GmbH (元 Peter Hoffmann SERVICE GmbH)	PC-Safe privat, Version 9.1	完全性保護用 PC 製品、正式に認められていないプログラムやデータの変更の確認と記録	E1/中 BSI-ITSEC-0101-1995 1995 年 9 月 29 日

表４－５　データ伝送

製造メーカー・販売者	製品	製品タイプ	結果 ID 認証日
BROKAT Infosystems AG	X-PRESSO Security Package 1.1	クライエント／サーバー利用を保護するためのセキュリティ製品	E3/高 BSI-ITSEC-0116-1997 1997 年 6 月 17 日
BROKAT Infosystems AG	X-PRESSO Security Package 1.3	クライエント／サーバー利用を保護するためのセキュリティ製品	E3/高 BSI-DSZ-ITSEC-0128-1998 1998 年 10 月 29 日
Deutsche Telekom AG	DOKRYPT 4.0	特に SFile 4.0 用機能図書館	E1/中 BSI-ITSEC-0118-1998 1998 年 3 月 31 日
Deutsche Telekom AG	SFile 4.0	データ伝送時の完全性と信頼を確保するためのセキュリティ製品	E1/中 BSI-ITSEC-0117-1997 1997 年 7 月 11 日
KryptoKom-Gesellschaft für kryptographische Informationssicherheit und Kommunikations-technologie mbH	KryptoGuard X.25 V.1.0	X.25 用伝送の安全	E2/高 BSI-ITSEC-0023-1992 1995 年 3 月 9 日

表４－６　スマートカード：オペレーティングシステム、カード読取器

製造メーカー・販売者	製品	製品タイプ	結果 ID 認証日
Siemens AG	安全モジュール SM-K	電話ないし類似の端末器からキャッシュレス・サービスを利用するためのセキュリティ・モジュール	E3/高 BSI-DSZ-ITSEC-0096-1998 1998 年 12 月 9 日
Setec Oy	Setcad 202 Software, Version 1.42	スマートカード読取器用オペレーティングソフトウエア	E4 BSI-ITSEC-0097-1996 1996 年 2 月 29 日
Setec Oy	Setcad 202 Software, Version 1.43	スマートカード読取器用オペレーティングソフトウエア	E4 BSI-ITSEC-0124-1998 1998 年 2 月 12 日
Setec Oy	Setcos 3.1 Version 3.1.1.	スマートカード・オペレーティングシステム	E4/高 BSI-ITSEC-0098-1996 1996 年 2 月 29 日
Setec Oy	Setcos 3.1 Version 3.1.1.1	スマートカード・オペレーティングシステム	E4/高 BSI-ITSEC-0125-1997 1997 年 5 月 6 日
Siemens-Nixdorf Informationssysteme AG	SICRYPT® Computer Card 2.0 (SCC-OS)のオペレーティングソフトウエア	SICRYPT Computer Card のオペレーティングシステム	Q4, F2[44]に近似 BSI-ITS-0010-1992 1993 年 7 月 15 日

表４－７　その他

製造メーカー・販売者	製品	製品タイプ	結果 ID 認証日
Tixi.Com GmbH	Tixi-Mail Box Pro with E-Mail Firewall Firmware Version 300.2.34	データ伝送時の PC 保護用製品	E1 BSI-ITSEC-0137-1998 1998 年 8 月 13 日
MOBA Dresden GmbH	MAWIS, Rev. 1.0	ゴミ箱 ID システム	E2/中 BSI-ITSEC-0060-1996 1996 年 6 月 10 日
BMW AG	EWS II, Version 01	コード化された電子持ち逃げ停止機能	E2/低 BSI-ITSEC-0086-1994 1996 年 4 月 1 日

[44] ITSEC 評価 E4（製品特有の機能）に相当。

表４－８　チップカード読取器[45]

製造メーカー・販売者	製品	製品タイプ	結果 ID 認証日
Cherry GmbH	カード読取器 G80-1501 HAD, Index/04 -Index/08	チップカード読取器が組み込まれた PC キーボード	E2/低 BSI-ITSEC-0026-1993 1994 年 1 月 31 日
Cherry GmbH	カード読取器 G80-1501 HAD, Index/09	チップカード読取器が組み込まれた PC キーボード	E2/低 BSI-ITSEC-0074-1994 1994 年 10 月 6 日
Cherry GmbH	カード読取器 G80-1501 HAD, Index/10	チップカード読取器が組み込まれた PC キーボード	E2/低 BSI-DSZ-ITSEC-0149-1999 1999 年 3 月 5 日
Celectronic GmbH	CARD STAR/medic Version 2.3	チップカード読取器	E2/低 BSI-ITSEC-0064-1994 1994 年 12 月 22 日
Celectronic GmbH	CARD STAR/medic Version 2.4 製品番号 4210	チップカード読取器	E2/低 BSI-ITSEC-0094-1995 1995 年 4 月 27 日
Celectronic GmbH	CARD STAR/medic Version 2.4 製品番号 4211	チップカード読取器	E2/低 BSI-ITSEC-0087-1994 1995 年 4 月 27 日
Celectronic GmbH	CARD STAR/medic Version 2.5	チップカード読取器	E2/低 BSI-ITSEC-0113-1996 1996 年 6 月 10 日
Celectronic GmbH	CARD STAR/medic Version 2.6 商品番号 4210 及び 4211	チップカード読取器	E2/低 BSI-DSZ-ITSEC-0147-1999 1999 年 2 月 10 日
Celectronic GmbH	CARD STAR/medic Version 3.0	携帯用チップカード読取器	E2/低 BSI-ITSEC-0092-1996 1996 年 3 月 1 日
Celectronic GmbH	CARD STAR/medic Version 4.0	チップカード読取器	E2/低 BSI-ITSEC-0120-1997 1997 年 2 月 24 日
Celectronic GmbH	CARD STAR/medic Version 4.5	チップカード読取器	E2/低 BSI-DSZ-ITSEC-0145-1998 1998 年 12 月 16 日

Siemens-Nixdorf Informationssysteme AG	SNI B1 PC-Card, Revision 2.27	チップカード読取器	E2/低 BSI-ITSEC-0133-1998 1998 年 3 月 27 日
SCM Microsystems GmbH	PSR 2, Revision 2.27	チップカード読取器	E2/低 BSI-ITSEC-0134-1998 1998 年 3 月 27 日

[45] ドイツの健康保険カード用チップカード読取器。連邦保険組合医師協会（KBV）の要求に基づく。

Siemens-Nixdorf Informationssysteme AG	B1 チップカード読取器の Firmware , B1 KLC, Version 4.0, Revision 1.11	チップカード読取器	E2/低 BSI-ITSEC-0119-1998 1998 年 2 月 27 日
Weser Informatik GmbH	携帯データ把握保証カード Version 1.1	携帯用チップカード読取器	E2/低 BSI-ITSEC-0089-1997 1997 年 10 月 10 日
ORGA Kartensysteme GmbH	HML 825, Version 3.2	携帯用チップカード読取器	E2/低 BSI-ITSEC-0078-1996 1996 年 3 月 1 日
ORGA Kartensysteme GmbH	HML 825, Version 3.3	携帯用チップカード読取器	E2/低 BSI-ITSEC-0121-1997 1997 年 8 月 7 日
etp-electronics trading and production	MediCard handy, Version2.8	携帯用チップカード読取器	E2/低 BSI-ITSEC-0112-1996 1996 年 9 月 27 日
Celectronic GmbH	CARD STAR/visit, Version 2.3	チップカード読取器	E2/低 BSI-ITSEC-0063-1994 1994 年 12 月 22 日
Celectronic GmbH	CARD STAR/visit, Version 2.4	チップカード読取器	E2/低 BSI-ITSEC-0093-1995 1995 年 4 月 27 日
Celectronic GmbH	CARD STAR/visit, Version 2.5	チップカード読取器	E2/低 BSI-ITSEC-0114-1996 1996 年 6 月 10 日
GEMPLUS Card International GmbH	GCR550, Version 2.1	チップカード読取器	E2/低 BSI-ITSEC-0028-1993 1993 年 12 月 20 日
GEMPLUS Card International GmbH	GCR550, Version 2.21	チップカード読取器	E2/低 BSI-ITSEC-0081-1994 1995 年 1 月 18 日
GEMPLUS Card International GmbH	GCR550, Version 2.22	チップカード読取器	E2/低 BSI-ITSEC-0090-1995 1995 年 5 月 26 日

Silver Büromaschinen Vertrieb	Walther Cardtype （PC インターフェイス付きバージョン) Software Version: E004/ 006	チップカード読取器と PC インターフェイス付き電子タイプライター	E2/低 BSI-ITSEC-0076-1994 1995 年 1 月 27 日
ORGA Kartensysteme GmbH	HML 500	チップカード読取器	E2/低 BSI-ITSEC-0036-1993 1993 年 12 月 20 日
ORGA Kartensysteme GmbH	HML 500,Version 2.6	チップカード読取器	E2/低 BSI-ITSEC-0080-1994 1995 年 1 月 18 日

IBM Informationssysteme Deutschland GmbH	IBM 5937-B04	チップカード読取器	E2/低 BSI-ITSEC-0038-1993 1994 年 4 月 22 日
IBM Informationssysteme Deutschland GmbH	IBM 5937-B04 シリーズ番号 00231 以降	チップカード読取器	E2/低 BSI-ITSEC-0066-1994 1995 年 1 月 18 日
IBM Informationssysteme Deutschland GmbH	IBM 5937-B05	チップカード読取器	E2/低 BSI-ITSEC-0039-1993 1994 年 4 月 22 日
IBM Entwicklung GmbH	IBM 5937-B05 シリーズ番号 51066 以降	チップカード読取器	E2/低 BSI-ITSEC-0067-1994 1995 年 1 月 18 日
Preh-Werke GmbH & Co KG	PC-Chip-KVK, Version 6.50	チップカード読取器が組み込まれた PC キイボード	E2/低 BSI-ITSEC-0070-1994 1994 年 12 月 22 日
Siemens AG	KV-CKT (J31032-K0108-L002-A1)	チップカード読取器	E2/低 BSI-ITSEC-0025-1993 1994 年 11 月 24 日
Siemens AG	KV-CKT (J31032-K0108-L012-A1)	チップカード読取器	E2/低 BSI-ITSEC-0055-1993 1994 年 11 月 24 日
TRT Philips Communication Systems	PE 115- 保険カード読取器	チップカード読取器	E2/低 BSI-ITSEC-0044-1993 1994 年 10 月 28 日

Optima Bürotechnik GmbH	MEDItype (PC インターフェイスなしバージョン)	チップカード読取器付き電子タイプライター	E2/低 BSI-ITSEC-0046-1993 1994 年 4 月 22 日
Optima Bürotechnik GmbH	MEDItype (PC インターフェイス付きバージョン) カード読取器ソフトウエアバージョン: E004/ 006	チップカード読取器と PC インターフェイス付き電子タイプライター	E2/低 BSI-ITSEC-0062-1994 1994 年 10 月 6 日
Krone AG	KVT1 V2.03	チップカード読取器	E2/低 BSI-ITSEC-0034-1993 1993 年 12 月 20 日
Krone AG	KVT1 V2.03A	チップカード読取器	E2/低 BSI-ITSEC-0073-1994 1994 年 10 月 6 日

４．３　BSI が認めた民間の認証機関の証明書

表４－９に、民間の認証機関の ITSEC 証明書又は CC 証明書[46]を取得し、その証明書が BSI によって正当と認められた製品を挙げる。ただ、暗号化と復号化に適した暗号アルゴリズムはまだ BSI によって認められていない。

なお、証明書は debis Systemhaus Information Security Services GmbH の認証局（debisZERT）が発行した。

[46] ４．１項参照。

表４－９　民間の認証機関の ITSEC 証明書又は CC 証明書を取得し、その証明書が BSI によって正当と認められた製品

製造メーカー・販売者	製品	製品タイプ／システムタイプ	結果 ID 認証日
Hermes Kreditversicherungs-AG	Hermes Online System, Version 2.0	インターネット接続	E1 debisZERT-DSZ-ITSEC-04015-1999 1999 年 9 月 15 日
Utimaco Safeware AG	SafeGuard Sign&Crypt SDK Version 2.0	機能図書館	E2 debisZERT-DSZ-ITSEC-04008-1999/1 1999 年 7 月 19 日
Utimaco Safeware AG	SafeGuard Sign&Crypt SDK Version 2.0	機能図書館	E2 debisZERT-DSZ-ITSEC-04008-1999 1999 年 5 月 21 日
MeTechnology Europe GmbH	MeSecure 1.03	クライアント／サーバー利用を保護するためのセキュリティ製品	E3 debisZERT-DSZ-ITSEC-04003-1999 1999 年 3 月 18 日
Utimaco Safeware AG	SafeGuard Sign&Crypt SDK Version 2.0	利用者用電子署名製品	E2 debisZERT-DSZ-ITSEC-04007-1999 1999 年 3 月 15 日
Setec Oy	Setsos 2.2	スマートカード・オペレーティングシステム	E3 debisZERT-DSZ-ITSEC-04011-1999 1999 年 2 月 22 日
Siemens AG	ドイツテレコム社の N.I.K.E.システムの中央セキュリティ・モジュール(SM-Z)	その他	E3/高 debisZERT-DSZ-ITSEC-04012-1998 1998 年 12 月 1 日
Setec Oy	Setsos 2.1	スマートカード・オペレーティングシステム	E3 debisZERT-DSZ-ITSEC-04010-1998 1998 年 10 月 22 日
ENVICOMP Entsorgungssysteme GmbH & Co.KG	EMS; Version 1.0	その他	E1/中 debisZERT-DSZ-ITSEC-04001-1998 1998 年 7 月 1 日
Utimaco Safeware AG	CardMan®, CardMan®Compact, CardMan®KeyboardCardMan®Mobile, CardMan®Software Development Kit, Version 2.2	チップカード読取器（オペレーティングソフトウエアと開発ソフトウエアを含む）	E2 debisZERT: BSI-ITSEC-0406-1998 1998 年 3 月 18 日

４．４　TÜV 情報技術社が発行した証明書

表４－１０　TÜV 情報技術社認証局[47]が発行した証明書

製造メーカー・販売者	製品	製品タイプ	結果 ID 認証日
Effeff Fritz Fuss GmbH & Co. KaA	Effeff B1, Version 1.0	チップカード読取器	E1, 低 TUVIT-DSZ-ITSEC-9106-1999 1999 年 5 月 28 日
Siemens AG (1999 年 4 月 1 日以降 Infineon Technologies AG)	SLE 66CX160S	チップカード・セキュリティ・コントローラ	E4, 高 TUVIT-DSZ-ITSEC-9102-1999 1999 年 3 月 22 日
SCM Microsystems GmbH	SwapSmart RS232 B1, Revision 2.34	チップカード読取器	E2, 低 TUVIT-DSZ-ITSEC-9101-1999 1999 年 3 月 15 日

４．５　BSI が認定した検査・認証機関

情報技術見本市 CEBIT 2000 の開催に当たり、BSI は BSI が認定した検査機関と認証機関のリストを公開した。

検査機関

Competence Center Informatik GmbH
Prüfstelle IT-Sicherheit
Lohberg 10
49716 Meppen

debis Systemhaus
Information Security Services GmbH
Prüfstelle IT-Sicherheit
Rabinstraße 8
53111 Bonn

[47] TÜV Informationstechnik GmbH。 TÜV は技術関係の監査を行う技術監査協会のこと。

Industrieanlagen-Betriebsgesellschaft mbH
Abteilung ITE
Einsteinstraße 20
85521 Ottobrunn

Tele Consulting GmbH
Prüflabor für IT-Sicherheit
Siedlerstraße 22-24
71126 Gäufelden

TÜV Informationstechnik GmbH
Prüfstelle für IT-Sicherheit
Am Technologiepark 1
45307 Essen

TÜV Nord e.V.
Software & Elektronik Labor
Große Bahnstraße 31
22525 Hamburg

TÜV Produkt Service GmbH
IQSE – Prüfstelle für IT-System
Ridlerstraße 31
80339 München

Vossloh System-Technik GmbH
Prüfstelle für IT-Sicherheit
Edisonstraße 3
24145 Kiel

認証機関
Bundesamt für Sicherheit in der Informationstechnik
Referat II 2
Godesberger Allee 183
53175 Bonn

debis Systemhaus
Information Security Services GmbH
Rabinstraße 8
53111 Bonn

TÜV Informationstechnik GmbH
Am Technologiepark 1
Gebäude A 6
45307 Essen

TÜV Produkt Service GmbH (IQSE)
Zertifizierungsstelle
Ridlerstraße 31
80339 München

参考文献）

不正アクセス状況：
- Computerkriminalität, BKA
- Informationen zu Programmen mit Schadensfunktionen, BSI
- Kryptographische Absicherung von Kommunikation, DFN-Cert

電子署名：
- Bei der Digitalen Signatur ist Niedersachsen ganz weit vorn, Niedersachen
- Richtlinie 1999/93/EG des europäischen parlaments und des Rates vom 13.12.1999
- Digitale Signatur: Rechtliche Rahmenbedingungen, DFN-Cert
- Digitale Signatur, TeleTrust
- CeBIT99”Digitale Signatur, Sicherheit für Electronic Commerce”, TeleTrust

ホームバンキング：
- HBCI: Die sichere Bank
- HBCI-Sicherheitsspezifikation

メールトラスト：
- MailTrust (AG8), TeleTrust

ISO/IEC15408：
- Gemeinsame Evaluationsmethodologie

SPHINX：
- Piloterprobung SPHINX - Bericht und Ausblick, BSI
- SPHINX, Abschlußbericht Phase2

BSI スタディ、認証：
- Deutsche IT-Sicherheitszertifikate
- Zusammenfassung des Endberichtes zum Projekt Kosten und Nutzen der IT-Sicherheit

政府、国会資料：

- Weg zu einer europaweiten Spitzenposition in der Informationsgesellschaft, BMWi/bmbf
- Eckpunkte der deutschen Kriptopolitik, BMWi
- Informationssicherheit - ein Ekpunkt einer zukunftsorientierten Sicherheitspolitik, BSI
- Bericht der Bundesregierung über die Erfahrungen und Entwicklungen bei den neuen Informations- und Kommunikationsdiensten in Zusammenhang mit der Umsetzung des Informations- und Kommunikationsdienste-Gesetzes, Deutscher Bundestag
- Zur Nutzung und Anwendung der neuen Medien in Deutschland - Chancen in der Informationsgesellschaften, Deutscher Bundestag
- Die neue Bundesregierung und der Datenschutz, Deutscher Bundestag

関連機関一覧：

- Entscheidungssammlung Online-Recht
- Ins Internet? - Aber sicher!, Webkatalog der Initiative “Sicherheit im Internet”

付録１）行政機関の情報化整備

連邦政府は、公的機関が電子商取引の普及等新しい情報通信技術の利用（例えば、法的拘束力のあるデジタル署名）を加速させる原動力になる必要があると考えており、２０００年夏までに包括的な情報技術戦略案を提示する予定である。
これまで立案された計画は以下のとおりである。

・　公共事業等公共の発注業務をインターネットで行う準備をするため、建設関連の行政機関でパイロット・プロジェクトが開始されており、２０００年上半期にその結果が提出される。公共の発注業務に対する入札をインターネットで行わせることによって、これまでマルチメディアを利用してこなかった企業が将来積極的にインターネットに対応するようになることを、連邦政府は期待している。

・　所得税申告は、２０００年１月から市販の納税申告プログラムを利用して電子提出することができるようになる。また、２０００年中には売上税（付加価値税）の申告や給与所得税の申告も同様に電子化される模様である。納税申告の電子化は、将来、その他の租税でも可能になる模様で、将来は納税証明書や必要な書類（給与所得税カードや貸借対照表等）の電子送付、電子署名の導入も実現されることになる模様である。なお、同事業はドイツ語の電子納税申告（Elektronische Steuer　ERklärung）の頭文字をとって「ELSTER」と命名されている。

・　「Media@Komm」事業の枠内でコンペが行われ、市町村等地方自治体に「バーチャル役所」や「バーチャル中央広場」の実現に向けたコンセプトを作成するよう要請した。コンペで選出される３つのコンセプトの実現と同事業の継続に、連邦経済技術省は今後数年間で最高６０００万マルクを公的補助する。

・　連邦経済技術省は、地方自治体の行政機関において安全なテレワーク（DATEL）を確立、試験するためのコンペに約２５０万マルクを提供する。審査に当たっては、コンセプトによって創設されるテレワーク雇用数とセキュリティ対策がキーポイントになる。

・　「情報技術２０００」構想の枠内で、２００２年までに各地の労働局[48]を含めた連邦労働施設[49]職員全員にネットワーク化されたパソコンを用意することを目指す。

---

[48] 連邦労働施設の官署として職業紹介、職業相談、職業教育、失業保険等に関する事務を行う。

それによって、各職員が職務遂行に必要な専門プログラム、オフィス・パッケージ、その他のプログラム、共同データバンクにネット上でアクセスできるようにする。さらに、連邦労働施設の電子情報データ・サービスを拡大させる。現在、同施設の電子情報データ・サービスはインターネット上で１日２０万件の利用が記録されている。

・　ドイツでは連邦や州、市町村等政治のたくさんのレベルで選挙が行われている。「インターネット選挙」事業が９９年春に開始された背景に、社会的変動性の増大、有権者の高齢化等がある。連邦政府の判断では、インターネットの普及によって技術健康保険組合役員選挙[50]等でパイロット・プロジェクトを開始できる状況にある。しかし、連邦政府の見解によると、憲法が要求する「秘密の選挙[51]」については、情報通信サービス法[52]によって必要な法的基本条件が整備されているものの、実際にはインターネットによる秘密の選挙は中期的にしか実現できない、とする。連邦経済省は「インターネット選挙」事業に１３０万マルク以上を公的補助していく予定で、その成果は催し物や図書の形で報告、保存され、将来幅広く有効に利用される予定である。

---

[49] 中央官庁ではなく、連邦労働大臣の管轄下に置かれた公法上の独立法人であるため、俗に使用されている連邦労働庁という訳語は使用しなかった。失業保険の支給のほか、職業相談、職業訓練、職業紹介を任務とする。

[50] ドイツの公的健康保険金庫（公法上の法人）のひとつ。技術者、技師等を対象とする。

[51] ここでは、個人が誰に投票したか、秘密が守られることをいう（基本法第３８条第１項）。

[52] 脚注１８参照。