欧州におけるサイバーセキュリティ政策と研究開発の現状および最新動向調査

報告書

NICT パリ事務所

2010 年 10 月 31 日

目次

序文

昨今、インターネットや携帯電話を利用するアプリケーションとサービスの多様化、そして通信網の高速化が進みつつある一方で、サイバー空間の安全性および違法行為取締に関わる問題に関心が集まっている。本調査では、欧州におけるサイバーセキュリティ政策および研究開発状況を調べ、その最新動向を明らかにする。

サイバーセキュリティ政策に関しては、以下のテーマを調査対象とする。

- I CT インフラの保護対策（報告書第一部）
- 個人情報の保護対策（第二部）
- 違法・有害情報の規制政策（第三部）
- 違法ダウンロードの規制政策（第四部）

本報告書の第一部、第二部、第三部、第四部で、上記 4 つのテーマに対する欧州連合（EU）および欧州主要国（英独仏）の政策動向を調べる。とりわけ、所管機関、対策プログラムおよび法整備の動向を明らかにし、同分野で問題となっている事件および出来事についても簡単に紹介する。

本報告書第五部では、欧州におけるサイバーセキュリティ関連の市場動向と研究開発動向を示す。EU 発表の報告書を元に同部門の市場動向を概観するとともに、EU の第七次枠組計画および欧州主要国における研究開発動向を調べ、研究プロジェクト等を例示する。

また、公開された各種文献等を精査する他に、欧州の違法ダウンロード規制政策の現状を知るために、フランスの市民団体「クアドラチュール・デュ・ネット」に取材し、ヒアリング調査を実施した。その議事録も本報告書に掲載する。

なお本報告書では、必要な情報を入手した政府機関等のウェブサイトの URL を参考のため注に載せているが、これらのサイトに掲載された記事はサイト運営者の都合で随時移動および修正、削除される可能

性がある。よって、報告書の作成終了後、本報告書に掲載された URL から情報源となった記事にアクセスできないことがありうることを、ここで前もってお詫び申し上げたい。

最後に、本調査にあたっては、パリ大学院生の小野浩太郎氏に多くの支援をいただいたことを紹介する。

第一部　　欧州における ICT インフラ保護対策

第一部では、欧州における ICT インフラ保護対策の現状と最新動向を見て行く。EU と欧州主要国（英仏独）の同対策プログラムおよび法整備状況、所掌機関の概要と活動を重点に記す。欧州では、2007 年のエストニアにおける大規模なサイバー攻撃および中国を起源とするサイバー攻撃を主な理由に、ICT インフラ保護対策に対する意識が近年来高まっている。

第一章　欧州連合

EU では、2004 年にサイバーセキュリティ対策の専門機関である「欧州ネットワーク・情報安全庁（European Network and Information Security Agency : ENISA）」が設立され、それ以来 ICT インフラ保護[1]に関する政策および法整備が大きく進められている。政策プログラムとしては、2009 年の「重要情報インフラ防護」プログラムおよび 2009 年電子通信規制改革パッケージが注目される。後者の改革においては、2002 年に成立した「電子通信ネットワークとサービスのための共通規制枠組に係る指令」（枠組指令と以下略）が改正されており、通信網のセキュリティの向上が改正ポイントの一つであった。これら二つは平行して策定され、EU の現行の ICT インフラ保護政策の要となっている。さらに、2010 年 5 月に発表された EU の ICT 政策パッケージ「デジタル・アジェンダ」でも ICT インフラ保護に関する政策が打ち出されている。

[1] 本報告書において、ICT インフラという語には、ICT システム、サービス、ネットワーク、インフラの意味を含む。

以下に、ENISA の概要を示し、ついで、重要情報インフラ防護プログラム、電子通信規制改革パッケージ、デジタル・アジェンダにおける同分野の関連政策を見ていく。

欧州ネットワーク・情報安全庁の概要

ENISA は、EU の ICT インフラ保護に関する特殊専門機関であり、同分野の専門的な知識を提供する機関として、EU の政策決定に関して重要な役割を担っている[2]。

成立の背景と存在理由

ENISA は 2004 年に成立した「欧州ネットワーク・情報安全庁の設立に係る規則」を法的根拠に、EU の共同体庁（Community Agency）[3]として設立された[4]。ENISA は他の組織から独立して、ICT インフラ保護政策に関して発言を行うことが義務づけられている。

同機関は当初 2004 年 3 月から 5 年間の予定で設立された。電子通信規制改革パッケージ原案は 2007 年に策定されているが、そこでは、ENISA を新たに設立が提起された欧州統一規制機関「欧州電子通信市場庁」に融合させることが提案された。だが、結局法案の共同決定手続きの過程で、その必要性が認められず、新機関に融合させる案は棄却され、ENISA を独立した機関として存続させることが決定した。

活動内容

a) 情報収集およびリスク分析

---

[2] http://ec.europa.eu/information_society/policy/nis/enisa/index_en.htm
http://www.enisa.europa.eu/

[3] 共同体庁は、欧州公法に基づいて運営される組織であり、法人格を有する。「共同体機関（Community Institution）」（欧州委員会や欧州議会等）とは異なり、共同体庁として設立される機関は、一定の分野の専門機関である。
http://europa.eu/agencies/community_agencies/

[4] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML

情報を収集し、リスクの分析を行う

リスク査定活動、リスク管理およびそれについての研究を行う

b) EU 機関および加盟国の支援

欧州議会、欧州委員会およびその他の EU 機関、また加盟国所管当局に随時助言を与える

ICT セキュリティ部門関連の法整備の際に欧州委員会を支援する。

欧州委員会と加盟国の提携を促進する

欧州委員会、加盟国と産業界の対話を支援する

c) ICT セキュリティに関する市民の意識を高める

正しい利用法を伝えることにより、通信網と情報保護に関する市民の意識を高める

d) 研究開発および標準化活動を支援する

通信網と情報保護に係る技術の標準化活動を監視する

同分野の研究開発支援計画に関して、欧州委員会を支援する

研究機関や民間企業の共同研究・活動を強化する

e) 国際提携活動

EU と第三国の間での国際提携活動を促進する

重要情報インフラ防護

EU の ICT インフラ保護政策に関しては、欧州委員会が「重要情報インフラ防護についての通達書」を 2009 年 3 月に発表している[5]。これは、後に記す枠組指令の改正による法整備と平行して策定されており、それらは一組の政策となっている。

EU は 2006 年に ICT インフラセキュリティ戦略「安全情報社会のための戦略—対話、パートナーシップ、強化—」[6]を打ち出していた

[5] http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm

[6] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52006DC0251:EN:NOT

が、ステークホルダーによって実際には同戦略で示された政策が十分に実施されていなかった。重要情報インフラ防護プログラムは、ENISA の役割等を増大させるとともに、ICT インフラ防護に係る政策をさらに発展させることを目的とする。

また同プログラムの策定は、鉄道、電気、水道等の重要インフラ一般の防護に係る EU の対策強化の流れにも属する。2005 年末に欧州委員会は司法・内務閣僚理事会の要請を受けて、「欧州重要インフラ防護プログラム」の策定を開始し、2006 年末に同プログラムを発表していた。ここでは、エネルギー（電気、石油、ガス）と交通（道路、鉄道、航空、船舶）部門のインフラ保護政策が策定され、ICT 部門は将来的に優先して保護が必要となる分野とされた。そして、2009 年に、エネルギーと交通部門とは独立して、重要情報インフラ防護プログラムが発表されたのであった。

動機

ICT インフラは他の重要インフラの支えとなるプラットフォームであり、欧州の経済と社会の根幹である。よって、ICT インフラの寸断および破壊は EU 経済に多大な損出をもたらす可能性がある。2007 年には、実際にエストニアを狙った大規模なサイバーテロが起こっている[7]。

行動計画

2009 年の重要情報インフラ防護に係る通達書では、主に 2010 年末を期限として、以下の行動計画が示されている。

1）準備と予防

- EU 域内で加盟国が提携して活動できるように、ENISA の支援の下、2010 末までに各国のコンピューター緊急対応チーム（Computer Emergency Response Team : CERT[8]）の最低限の能力

[7] エストニアにおけるサイバー攻撃については後に記す。
[8] CERT は、公営の場合もあれば、非営利団体として活動していることもある。こ

とサービスのレベルを決定する。そして、2011 年末までに全加盟国内で、CERT が的確に機能できるようにする。

- 通信網セキュリティに関する官民パートナーシップ体制を 2010 年半ばまでに整え、通信網保護に関して官民セクターの提携を強化する
- 欧州委員会主導で、加盟国間で関連情報を共有するためのフォーラムを設立する。このフォーラムでは、ENISA 等の機関の活動成果を吸収する。

2）探知と対応

- 欧州規模のセキュリティシステム「欧州情報共有・警報システム」[9]を開発し、展開する。このシステムは EU 加盟国の全市民および中小企業向けに作られ、ICT セキュリティ関連の情報を共有することを可能にするものである。特に的確な実践に関する情報（フィッシングメール等の特定方法等）を共有すること、セキュリティに問題がある場合警告を出すこと、現在の通信網の状況等を把握することを目的とする。2010 末には、同システム作成のロードマップを策定することが目指される。

だが、同システムが具体的にどのようなものになるのかは発表されていない。2006 年に欧州委員会は、同システムを設立することができるかどうか、ENISA に調査を要請していた。2008 年 2 月に発表された ENISA の研究報告によると[10]、最良の手段は、EU 域内で中央集権的なシステムを作り、同分野の EU の役割を強化することではなく、加盟国内の既存の情報共有・警報システムをより生かすため、EU は情報センターとして機能すること、つまり加盟国間で情報交換し議論

こでは、公営の CERT のレベルを設定することが問題となる。

9 http://www.enisa.europa.eu/media/faq-on-enisa/faq-on-enisa-and-eisas

10 http://www.enisa.europa.eu/media/press-releases/2008-prs/european-information-sharing-and-alert-system-eisas

する場を提供すること、そして関連の情報を収集し分析することであるとされた。

ICT セキュリティシステムの研究開発に関しては、以上の他、欧州委員会は、EU 財政支援プログラム「テロおよび他のリスクのための予防、準備、対応マネージメント」[11]を通して、情報インフラに係る研究プロジェクトを支援している。これらのプロジェクトは、先に述べた「欧州情報共有・警報システム」および「第七次枠組計画」で助成されている ICT インフラ保護の研究開発プロジェクトを補完するものである。

3）リスク軽減と復旧

- 不測の事態に対応できるように、欧州委員会は、各加盟国が国レベルでの予行演習を規則的に実施することを促す。加盟国内の公営の CERT が予行演習計画の策定、および実施を主導する。ENISA は、同分野における最適な実践について専門知識を与える。2010 年末までに、各国は最低一度国家規模の予行演習を実施することが目標となる。
- 欧州規模で、サイバーテロおよび事故等を想定した国際予行演習を行う。2010 年末までに予行演習の方法を定め、実際に実施する。以上に関して、欧州委員会は財政支援を行う。
- EU 内で公営の CERT の提携活動を強化するため、既存の提携活動システム「EGC（European Government CERTs）」[12]にてこ入れし、同システムを拡張する。EGC は EU 諸国の CERT の非公式な団体であるが、2010 年末までに EGC 参加国の数を二倍に増やすことが目指される（現在は 9 カ国）。また ENISA は、欧州規模での CERT の提携活動を推進し支援する。

---

[11] テロおよび他の安全リスクに係る予防、準備、対応マネージメントは、先に述べた「欧州重要インフラ防護プログラム」を実施するための財政支援プログラムでもある。

[12] http://www.egc-group.org/

4）国際提携活動

問題が生じたインターネット網の修復と安定性を強化するため、次の活動を実施する。

- 欧州委員会主導で、官民両方のセクターとともに、欧州規模で議論し、インターネット網の修復と安定性に関する欧州で統一した優先事項を決定する。
- 欧州委員会の主導で、欧州レベルで、インターネット網の修復と安定性に係る規則およびガイドラインを策定する。2010年末までに、規則とガイドラインの第一草稿を起草する。
- 欧州委員会は加盟国と共同して、上記の欧州基準およびガイドラインを第三国に対して普及させる。
- 欧州委員会は 2010 年末までに、インターネット網の復旧とリスク軽減に関する世界規模の予行演習に欧州のステークホルダーが参加できるように支援するための枠組およびロードマップを提案する。

5）ICT 部門の欧州重要インフラのための基準

- 欧州委員会は、加盟国および全ステークホルダーと提携して、ICT 部門の重要インフラの問題点を特定するための基準を定める。

枠組指令およびプライバシー指令の改正

2002 年に成立された枠組指令には通信網の安全性に係る独立した規程条項は存在せず、第八条に加盟国規制機関の任務として、個人情報とプライバシーの保護と通信網の安全性を高めることが明記されているだけであった。だが近年来同分野の重要性が認知され、2009年の枠組指令の改正では一条項（第十三条 ab「セキュリティと完全性」）が付け加えられた。

それによると、通信網のセキュリティを強化するため、特に事業者

の義務と加盟国所管当局の権限が強化されるとともに、欧州委員会にEU共通の技術的措置を決定する権限が与えられた。

- 加盟国所管当局は、事業者にネットワークの安全性を検査するのに必要な情報を提供するように要請する権限を持つ。
- 加盟国所管当局は、事業者にネットワークの検査を実施する義務を課す権限を持つ。検査は独立した組織もしくは所管当局が行い、検査にかかる費用は事業者が支払わなければならない。
- 事業者はネットワークのセキュリティが侵害され、それが大きな影響を及ぼす場合、加盟国所管当局にその旨を通達する義務を持つ。
- 必要な場合、事業者から通知を受けた所管当局は、他国の所管当局およびENISAに情報提供し、欧州委員会と同庁にその件についての報告書を提出しなければならない。
- 事業者から通知を受けた所管当局は、セキュリティの侵害に関して、同当局が侵害情報の開示が公共の利益に適うと判断する場合、情報を公開することができる。
- 所管当局は、事業者が義務を遵守しない場合、罰則を科す権限を持つ。
- 共通のセキュリティ要件を設定する必要がある場合、欧州委員会は、ENISAの意見を最大限考慮しつつ、上記のためにEU域内で調和した技術的実施措置を決定することができる。なお、この措置は欧州および国際技術標準に基づくべきである。

デジタル・アジェンダ

2010年5月発表のデジタル・アジェンダでも、通信網の保護政策および施策が記されており、ICTインフラ保護の重要性の認識が高まっていることがわかる。

欧州委員会の活動

- 2010 年中に、EU の新しい通信網および情報セキュリティ方針を策定する。この方針には ENISA の活動をより強化し、またサイバー攻撃に対して、より迅速な CERT や EU 機関の対応を可能にする法整備が含まれる予定である。
- 2010 年までに、情報システムに対するサイバー攻撃対策に係る具体的な施策（法整備を含む）を発表する
- 2013 年までに、EU および全世界レベルでのサイバー空間上の規則を制定する。

以上を見ればわかる通り、EU では 2010 年内に ICT インフラ保護に関する新しい法案が提案される可能性がある。

その他の活動

- 2012 年までに欧州サイバー犯罪プラットフォームを設立する[13]。このプラットフォームは、ユーロポールの活動である「インターネット犯罪報告オンラインシステム」、「分析作業ファイル」[14]、「インターネット・科学捜査専門フォーラム」[15]を統一し、より一貫性のあるサイバー攻撃対策を可能にする。
- 2011 年までに、ユーロポールに欧州サイバー犯罪センター設立の可能性を検討する。
- リスク管理を向上させるために、関連ステークホルダーと提携して活動する。またサイバー犯罪に対する世界規模で提携した行動を行う。
- 2010 年から EU 規模のサイバーセキュリティ予備訓練の実施を支援する

---

[13] http://www.europol.europa.eu/index.asp?page=news&news=pr100622.htm
http://www.publications.parliament.uk/pa/ld200910/ldselect/ldeucom/68/68we05 htm

[14] 特にインターネット上の決済に係る犯罪対策に取り組んでいる。

[15] 専門的な情報を統括するとともに、サイバー犯罪に係る法執行の教育を行っている。

加盟国の活動

- 2012 年までに、国内の CERT 同士のつながりを改善し、ネットワークを構築する
- 欧州委員会と提携して、大規模なサイバー攻撃に対する予行演習を実施する。

エストニアへのサイバー攻撃

先に見た 2009 年 3 月に発表された「重要情報インフラ防護についての通達書」では、EU 域内の最近の大掛かりなサイバー攻撃の例として、2007 年のエストニアへの攻撃が挙げられている。

報道によれば[16]、2007 年 4 月、5 月にエストニア政府および銀行の通信網等が大規模なサイバー攻撃を受けた。エストニアで計画されていた旧ソ連軍兵士記念像撤去計画を受けて、サイバー攻撃が行われたと見られ、同攻撃へのロシア政府の関与が疑われた。エストニアはロシア政府を非難する声明を出したが、同政府は容疑を否認していた。結局、2008 年に犯人が逮捕され、エストニア在住の大学生（当時 20 歳）が容疑を認めている。犯人はロシア系エストニア人で、エストニア政府の記念像撤去計画に反発し、サイバー攻撃を仕掛けたのであった。攻撃のピーク時には、銀行カードおよび携帯電話の使用が停止されたようだ。この出来事は欧州に大きな影響を与え、欧州の ICT インフラ保護政策強化を加速させる原因となった。

第二章　英国

ついで、英国における ICT インフラ保護政策を概観する。まず、所

[16] http://news.bbc.co.uk/2/hi/technology/7208511.stm
http://www.itespresso.fr/guerre-informatique-la-russie-accusee-de-louer-des-botnets-pour-attaquer-lestonie-18594.html

掌機関の概要を記し、ついで対策プログラムを示す。

ICT インフラ保護対策所掌機関

英国では、ICT インフラの保護に関しては、幾つかの機関が分担して対策を講じている。以下にそれらの機関の概要を簡単に記す。

通信電子セキュリティ庁（Communications-Electronics Security Group：CESG）

CESG[17]は、英国政府の諜報機関である政府通信本部に属している。この機関は、主に中央省庁、軍、地方公共団体、裁判所等の公共機関を対象に、ICT セキュリティ分野について情報および助言、教育を与えている。

国家インフラ保護庁（Centre for the Protection of National Infrastructure：CPNI）

CPNI[18]は省庁間組織であり、テレコム部門を含む重要社会基盤（電気、水道等）の事業者およびそれらの部門の監督省庁に対して、テロやその他の脅威に関する情報、助言等を提供している。

ビジネス・イノベーション・技能省（Department of Business Innovation and Skill：BIS）

BIS 省[19]は、英国政府のテレコム部門の政策を所掌する組織であり、情報セキュリティ政策室が ICT インフラ政策を担当している。BIS 省の活動は、主に民間企業を対象としている。

サイバーセキュリティ庁およびサイバーセキュリティ運営センター

サイバーセキュリティ庁とサイバーセキュリティ運営センターは、2009 年に発表された「英国サイバーセキュリティ戦略」で設立され

[17] http://www.cesg.gov.uk/about_us/index.shtml
[18] http://www.cpni.gov.uk/default.aspx
[19] http://www.berr.gov.uk/whatwedo/sectors/infosec/index.html

た機関である。詳しい概要については、同戦略について述べる時に記す。

ICT インフラ保護政策

英国における ICT インフラの保護対策に関しては、「国家情報保証戦略」および「サイバーセキュリティ戦略」という 2 つの政策が策定されている。また、2009 年 6 月に発表された英国 ICT 政策パッケージ「デジタル・ブリテン」においても、ICT インフラ保護対策を含む ICT セキュリティ関連の政策に一章が割かれている。

以下に、これらの ICT インフラ保護に係る政策パッケージについて記す。

国家情報保証戦略

2007 年 6 月、内閣事務局に設置された情報保証支援中央局（CSIA）[20]は、2003 年に発表されていた「国家情報保証戦略（National Strategy for Information Assurance : NIAS）」を改定している。

この改定は、主に 1）ICT 部門の発展が著しいことと、2）2005 年にトニー･ブレア前首相の下で ICT を利用する公共サービス改革プロジェクトが策定されたことに由来する。公共サービス改革では、ICT を利用して多くの機関が情報を共有できるようにすることを目標の一つとしており、以上のため情報保証（information assurance : IA）が重要な位置を占める。よって、同戦略は公共サービス改革を達成するための手段の一つでもある。

克服されるべき脅威としては、サイバー空間における犯罪（不正認証、窃盗、情報漏洩等）の他、ICT の発展に伴う通信システムの脆弱

---

20 http://webarchive.nationalarchives.gov.uk/20090707073435/cabinetoffice.gov.uk/csia.aspx CSIA は、内閣事務局に 2009 年に新設されたサイバーセキュリティ庁の前身機関である。

性等が挙げられている。

目標

- 政府が適正に ICT を利用して、公共サービスを提供できるようにする
- 情報および通信システムを保護することによって、英国の国家安全を高める
- 政府、民間企業、市民が ICT から最大の利益を引き出すことによって、英国の経済・社会福祉を強化する

アプローチ

1. 公共機関の情報リスク管理を明瞭で、効果的なものにする：情報リスク管理の説明責任を、公共機関（省庁を含める）の最高意志決定組織（理事会など）が所管するようにする。複数の機関で情報を共有する場合、情報リスク管理の責任を一カ所に持たせた方が良いので、リスク管理を行う単一のポイントを特定する。各省は、傘下に持つ非省庁型公共機関に対して一貫したリスク管理方法を実施させる。
2. 政府省庁および関連機関において、適正な共通情報保証技術標準（IA Standard）を使用する：
3. 情報保証に係る能力を発展させる：具体的には、適正な製品とサービスを生産すること、政府が情報保証に係る技術革新および研究を調整し支援すること（複数ある研究を提携させる等）、各機関の情報リスク担当スタッフの能力を向上させること（情報セキュリティに特化した研究院等で教育を与える）、情報保証に係る意識を高めることが挙げられている

2007 年の同戦略発表当時、ICT セキュリティ産業界から、同内容の戦略はすでに 10 年ほど前から議論されてきたものであり、政府の対応が遅く、さらに同戦略の規模が小さすぎるという批判も出ていた[21]。

---

21 http://www.computerweekly.com/Articles/2007/08/24/226310/National-Information-Assur

デジタル・ブリテン

2009 年 6 月に発表された「デジタル・ブリテン最終報告書」の第七章は、サイバーセキュリティ政策をテーマとしている。国内レベルの政策に関しては、大きく分けて、ICT インフラのセキュリティの向上、個人のデジタル情報の保護、有害情報対策が問題とされている。

以下に、デジタル・ブリテンで示された ICT インフラのセキュリティに係る政府の具体的な行動指針を記す。

- サイバー攻撃に対する通信網の管理能力および回復力を知るために、政府主導で大規模なテストを実施する
- 「電子通信復元・対策グループ（Electronic Communications Resilience and Response Group：EC-RRG）」（民間企業、政府、情報通信庁から構成されるフォーラム）に、英国内の通信網保護対策活動の評価報告書を作成させる
- 通信網保護に関する EU の政策に積極的に歩調を合わせる。

英国サイバーセキュリティ戦略

2009 年 6 月英国政府は、「次世代のためのセキュリティ」という国家安全政策を発表し、そこではサイバー空間が重要な保護の対象として特定された。そして同政策と同時に、政府は「英国サイバーセキュリティ戦略　−サイバー空間における安全・防護・復元力」を発表している[22]。

この戦略は、インターネットショッピングが急速に普及し多額の決済がなされ、また情報通信技術が他の部門のインフラとなりその重要性が増すとともに、ICT インフラが機能しなくなった場合のリスクが潜在的に増大していることを受けて策定された。

---

ance-Strategy-is-too-little-too-late-says.htm

[22] http://www.cabinetoffice.gov.uk/reports/national_security.aspx
ここで、サイバー空間とは、あらゆる形態の通信網およびそれを利用する活動を指す。また、サイバーセキュリティとは、1）サイバー空間における英国国家の利益の保護と、2）情報通信技術を利用し、より広い意味での英国安全政策を追求することを指し、二重の意味を持つ。

この戦略の目的は、サイバーセキュリティを所掌する機関を 2 つ設立して、政府省庁がそれぞれ講じているサイバーセキュリティ対策を統合する包括的な政策枠組を提供することである。これは、先に記した国家情報保証戦略を補完するものである。

目標としては、1）サイバー空間の安全性を高めること、2）サイバー空間を利用して英国の国家安全を向上させること、3）サイバーセキュリティに関する知識やスキルを向上させ、かつ意思決定システムを改善することが挙げられている。

施策

- 省庁間共同プログラムの実施
  - 通信網を保護する技術のイノベーションを支援するために追加助成を実施する
  - 危機管理に係る技術を向上させる
- 公共セクター、産業、市民団体、市民、国際パートナーと提携を深める。
- サイバーセキュリティ関連の機関を 2 つ新設する。
  - サイバーセキュリティ庁 ： 同庁は内閣事務局に設置される。英国政府のサイバーセキュリティ戦略を主導し、省庁間を通して一貫性のあるサイバーセキュリティ戦略を打ち出すため、省庁間共同プログラムを実施する。2007 年の国家情報保証戦略は同プログラムの一部として組み込まれ、施策が重複する場合がある。
  - サイバーセキュリティ運営センター ： 同センターはサイバー空間を監視し、英国の通信網およびユーザーに対する攻撃を分析する。民間企業および市民に ICT 関連のリスクについて助言および情報を提供する。同センターは、英国政府の暗号および情報保証を所掌する政府通信本部（GCHA）の一機関である電子通信安全庁（CESG）[23]によって主導される。

[23] CESG は国立情報保証技術機関とも呼ばれている。

サイバーセキュリティ庁が主導する省庁間共同プログラムの行動方針として、次の事柄が挙げられている。

・安全・防護・復元システム：全てのセクターを対象に、サイバー攻撃を防ぐシステムを開発する。特に、情報保証に係る技術標準（ISO27000 シリーズ）の策定に努める。

・政策・基本原理・法制・規制対策：既存のサイバーセキュリティ関連の政策間に見られる歪みを特定する。

・意識改革：市民および関連団体と提携して、サイバーセキュリティに関する意識を高める[24]。

・スキルと教育：サイバーセキュリティ対策のスキルを向上させ、関連の教育を与える

・技術能力・研究開発：サイバーセキュリティ運営センターが提供する情報を基に、サイバー空間の保護に関する長期的な研究を行う。また政府および産業によって主導されている通信網の保護に係る研究開発を、追加助成する。サイバーセキュリティ庁は、英「技術戦略委員会」のセキュリティ・イノベーションプラットフォームと緊密に提携して活動する。

・サイバー空間の活用：犯罪やテロと戦うために、サイバー空間を最大限に有効活用する。

・国際参加：英国内のサイバーセキュリティ政策を他国向けに調整する。

・管理・役割・責任：英国のサイバーセキュリティ関連の管理能力を検査し、必要な場合、改革を実施する

以上のように、同戦略では、サイバー空間を保護するだけでなく、それを利用して、他の部門のセキュリティを向上させることが目標と

[24] www.getsafeonline.org
英国では、「ゲット・セイフ・オンライン（Get Safe Online）」という官民共同のキャンペーンが実施されている。このキャンペーンについては、次部で詳述する。

されている。

サイバーセキュリティ運営センターに関しては、すでに批判も出ている。同センターはサイバーセキュリティ関連の情報を分析するだけで、サイバー攻撃に対して積極的に対抗する能力を持たず不十分であるという意見がある[25]。

なお、サイバーセキュリティ庁の主催で、同分野の有能な人材を発掘するために、「サイバーセキュリティチャレンジ」というコンクールを実施する予定である[26]。これは、官民合同でスポンサーとなり、2010 年秋頃より参加者を募集する予定である。参加者は様々なスキルが試される。

以上のように、英国では、ICT インフラ保護対策に関して包括的な政策が策定されている。英国の ICT セキュリティ市場がフランス、ドイツに比べて大きいことも勘案すれば[27]、他国に比べ、英国は同部門の重要性に関して意識が高いと言える。

第三章　フランス

ついで、フランスにおける ICT インフラ保護対策について見ていく。

---

[25] http://www.v3.co.uk/v3/news/2256292/tories-set-expand-cyber

[26] http://cybersecuritychallenge.org.uk/site/Home
BBC の報道記事も参考のこと。
http://news.bbc.co.uk/2/hi/technology/8645041.stm

[27] 欧州の ICT セキュリティ部門の市場動向については、本報告書第五部で記す。

ICT インフラ保護対策所掌機関

経済・産業・雇用省

フランスでは、経済・産業・雇用省が電気通信部門の政策を所掌しており、民間部門向けの ICT インフラ保護対策を担当している[28]。

国家情報通信システム安全庁

「国家情報通信システム安全庁（Agence Nationale de la Sécurité des Systèmes d'Information : ANSSI）」は、主に政府機関の情報システムの安全性を確保することを目的とし、首相直轄の国防総事務局に付属する機関として 2009 年 7 月に設立された[29]。前身の機関は 2001 年に設立された「情報システム安全中央総局」であり、新機関においては、人員が増加され、役割が強化された。

成立の経緯

フランスでは、2007 年ごろより ICT インフラ保護について議論が盛んになされている。それは先に見たエストニアへの攻撃と中国に由来するサイバー攻撃の問題が至近の理由である。報道によれば、フランス国防総事務局長は中国に由来するサイバー攻撃がフランスおよびアメリカ、ドイツを対象に行われていることを認めている[30]。だが、これらの攻撃に中国政府が関与しているかどうかは判明していない。また 2007 年にフランス上院でも、国内の ICT インフラ保護対策について審議された際に、中国を起源とするサイバー攻撃について言及さ

---

28 http://www.telecom.gouv.fr/rubriques-menu/entreprises-economie-numerique/securite/29 html

29 http://www.ssi.gouv.fr/site_rubrique7 html

30 http://www.lexpress.fr/actualite/politique/cyber-attaques-la-france-touchee-a-son-tour_466485.html
http://www.lefigaro fr/international/20070908.WWW000000057_la_france_victime_de_cyber_attaques_chinoises.html

れている。その議事録には、特に外務省の情報システムが狙われたことが述べられている[31]。

以上のような背景を通して、2008 年 6 月にサルコジ大統領が発表した国防白書に、ICT インフラ保護専門の機関を創設することが盛り込まれた。

活動内容

国家情報通信システム安全庁の主な活動としては、以下のものが挙げられる。

- 政府の情報通信システム保護のために必要な規則を提案し、またその適用を検査する
- 政府の通信ネットワークに対するサイバーテロに対応する（監視、探知、警告、反撃を行う）
- 省庁間の最重要ネットワークの保護に必要な製品を開発する
- 大統領と政府の命令および連絡手段を担当している政府連絡センターの監督をする
- 安全性が確かめられた製品に対して、品質保証ラベルを交付する
- サイバーテロに対応できる人材の育成を行う

将来的には、サイバーテロを探知する機関を新たに設立する予定である。

なお 2010 年 2 月には、同庁とドイツの連邦情報セキュリティ庁の提携活動を定めた協定を結んでいる[32]。

---

[31] http://www.senat.fr/rap/r07-449/r07-4490.html
es_chinoises.html

[32] https://www.bsi.bund.de/cln_183/ContentBSI/EN/Press/pressreleases/BSI-ANSSI_050210.html

ICT インフラ保護政策

2008 年 10 月に策定された仏 ICT 政策パッケージ「デジタル・フランス 2012」では、ICT セキュリティも課題の一つとして挙げられているが、包括的な ICT インフラ保護対策は策定されていない。

第四章　ドイツ

最後に、ドイツにおける ICT インフラ保護対策を見ていく。

ICT インフラ保護対策機関

ドイツでは、連邦内務省傘下の連邦情報セキュリティ庁（Bundesamt für Sicherheit in der Informationstechnik : BSI）を中心に ICT インフラ保護対策が進められている[33]。以下に同庁の概要を簡単に示す。

連邦情報セキュリティ庁

設立の経緯

1980 年代ごろから連邦政府および議会で、ICT 部門のセキュリティを向上させる必要性が議論され始め、内務省の主導で中央暗号庁が 1986 年に設立された。その後、1989 年に同庁は中央情報通信技術セキュリティ庁に改組された。これが現在の連邦情報セキュリティ庁の前身機関となり、同庁は 1991 年に設立された。

組織および活動内容

連邦情報セキュリティ庁は、事務方の Z 局および下記の 3 部局から構成される。

---

33 https://www.bsi.bund.de/cln_183/sid_9DB49A64DFC58729F43E0EB6CB68CF5C/EN/Home/home_node html

第一部局は電子政府向けの安全なメール機能の開発等に取り組むとともに、ファイアウォール、通信網のセキュリティのために必要な技術要件等を開発している。また通信網の安全性を分析し、検証することを役割として持ち、この課には、連邦コンピューター緊急対応チームが設置され、公共機関のセキュリティ問題に対応している。

第二部局は、主にサイバー空間における暗号技術を発展させ、安全な情報システムを作ることを目的としている。

第三部局は、ICT の最新技術の安全性を検証・評価すること、ドイツ市場の IT 製品の安全性を強化し、安全な製品に対し安全認証を行うことを任務として持つ。

連邦情報技術セキュリティ強化法

なお 2009 年 8 月に連邦情報技術セキュリティ強化法が成立し、連邦情報セキュリティ庁の役割が強化された[34]。同庁の年次報告書によれば、セキュリティの脆弱性および新タイプのサイバー攻撃に関する情報収集と分析、攻撃の探知、一般市民および商業向けにセキュリティリスクに対する警告の実施、公共機関の IT システムの技術標準を策定すること等が任務として加わった[35]。

ICT インフラ保護政策

ドイツでは連邦内務省が 2005 年に「国家情報インフラ保護計画」を策定している[36]。この計画は公共機関、ビジネス、市民を対象にした包括的なサイバーセキュリティ戦略であり、予防（危機管理の強化および安全な製品の使用の促進）、準備（サイバー攻撃に関する情報

34 https://www.bsi.bund.de/cae/servlet/contentblob/881344/publicationFile/55623/BSI_Act_BSIG.pdf

35 https://www.bsi.bund.de/cln_174/ContentBSI/EN/Publications/Annualreport/bsiannualreport.html

36 http://www.cnipa.gov.it/site/_files/2006_01_17NPSI_Rom_Eng.pdf

収集および警告の実施)、持続性（長期的な視野の下関連の技術の発展、国家レベルでの対応、信頼できるサービスおよび製品の製造）という三つの活動方針を提案している。同計画の実施においては、連邦情報セキュリティ庁が大きな役割を担う。

2009 年 6 月には、社会インフラ一般を対象とする「国家重要インフラ防護戦略」[37]が策定されているが、同戦略のうちに国家情報インフラ保護計画は組み込まれた。

以上、EU および欧州主要国における ICT インフラ保護対策を概観してきた。同対策の重要性は国によって多少の差はあるものの、近年来益々認知される傾向にあり、EU 、英国、フランス、ドイツともに、ICT インフラ保護独立機関を設立している。そこでは、サイバーテロ対策の他、セキュリティを高めるための研究もなされている。ICT セキュリティを重視する傾向には、中国を起源とするサイバー攻撃が理由の一つとして挙げられることが多い。

37 http://www.bmi.bund.de/cae/servlet/contentblob/598732/publicationFile/34423/kritis_englisch.pdf

第二部　欧州における個人情報保護対策

第二部では、欧州における個人情報保護対策を見ていく。EU および欧州主要国の法整備、政策プランを記すとともに、現在欧州で問題となっている出来事、事件等についても示す。

第一章　欧州連合

EU では、電子通信部門の個人情報の保護に関して、すでに 1995 年に「個人情報の処理に関する個人の保護および同情報の自由な移動に係る指令」を策定しており、かなり早い時期から法整備が始まっている。同指令は 2002 年の「電子通信セクターにおける個人情報処理およびプライバシー保護に係る指令」（以下、プライバシー指令と略）によって強化されたが、2009 年の電子通信規制改革パッケージで同プライバシー指令は改正され、さらに個人情報保護が進められた。

以下に、EU の電子通信部門個人情報保護対策の最新動向を明らかにするために、2002 年プライバシー指令および 2009 年の同指令の改正法について記す。ついで、世界各地で問題を引き起こしている米グーグル社のサービス「ストリート・ビュー」の欧州における動向を示し、より具体的に個人情報保護に関する欧州の問題、事情を明らかにしたい。

2002 年プライバシー指令

EU の個人情報の保護対策に関しては、2002 年成立のプライバシー指令で法枠組が策定されている。この指令は、個人情報およびプライバシー権の保護に関する加盟国の規制政策を、EU 域内で調和し一貫性のあるものとすることを目的としている。EU はすでに 1995 年に個

人情報の保護に係る指令を出しており、テレコム部門の個人情報の保護に関する規制法を確立していた。2002 年のプライバシー指令においては、電子通信部門の技術の進歩に対応するために、規制法を近代化することが目指された。

この指令は、欧州連合基本権憲章で定められたプライバシー権等の基本権を遵守することを目的とし（特に欧州連合基本権憲章の第七条と第八条[38]）、電子通信ネットワークを利用する通信とトラフィックデータの機密性を加盟国が保証する義務を定めている（特に同指令第五条）。すなわち、加盟国はユーザーの同意なく、通信が傍受され（盗聴等）、保存されることを禁止しなければならない。同時に、国家の安全や犯罪の予防等に必要だと判断された場合は、この指令の効力は各国の判断で制限されうると明記されている（同指令第十五条）。

なお放送に関しては、この指令の対象に含まれていないが、ビデオ・オン・デマンドサービスに関しては、サービス利用者が特定されうるので、この指令の対象に含まれる。

この指令の主なポイントは次の通りである。

セキュリティの確保

- サービスのセキュリティを高めるために、サービスプロバイダーは対策を講じなければならない。
- 利用サービスのセキュリティが低い場合、その旨をサービスプロバイダーはユーザーに伝えなければならない。

通信の機密性の保証

加盟国は電子通信ネットワーク上での通信の機密性および関連するトラフィックデータを国内法によって、保障しなければならない（盗聴等の禁止等）。

[38] 欧州基本権憲章の第七条と第八条では、それぞれプライバシーの保護と個人情報の保護が定められている。

トラフィックデータ[39]の削除

サービスプロバイダーによって処理され、記憶されたトラフィックデータは、そのサービスのために保存しておく必要がなくなった場合、削除されるか、個人情報として特定できない状態にしなければならない。

ユーザーの位置情報の保護

GPS 等によってユーザー端末の位置情報を利用するサービスを提供する場合、サービスプロバイダーはユーザーから位置情報を利用していいかどうか事前承認を得なければならない。

電話帳等への登録の事前承認

消費者は、電話帳等の個人情報が記載される名簿に登録される前に、その目的を伝達されなければならないし、また登録を拒否できる機会が与えられなければならない。

迷惑メール対策

スパム等迷惑メール対策のために、企業等がダイレクトマーケティングを目的とする電子メールおよび FAX を消費者に送信する際に、事前に消費者の同意を得なければならない。

スパイウェアの使用禁止およびクッキー等の認証機能サービス利用の事前承認

- ユーザー端末に保存された情報は、ユーザーの私生活に属するので欧州人権条約の下で保護されなければならない。ユーザーの同意なく、スパイウェア等によって、端末内の情報を獲得したりすることは禁止される。
- クッキー等の認証機能サービスを提供するためには、ユーザーにその目的を明白に知らせ、事前にユーザーの同意を得る必要

[39] ここで、トラフィックデータとは電子通信ネットワークを利用した通信や決済のために処理されるあらゆるデータを意味する。通信時間、時間帯、通信料、メールアドレス等が含まれる。

がある。ユーザーはクッキーの使用を拒否できる機会が与えられなければならない。

ID 認証通知を拒否する権利の保護

発信者の電話番号等を受信者に通知するサービスを提供する場合、サービスプロバイダーはユーザーにそのようなサービスが存在することを知らせ、通知を拒否できる機会を与えて、通知を拒否する権利を保護しなければならない。逆に、受信者が発信者の電話番号の通知を拒否することも可能でなければならない。また、サービスプロバイダーは、発信者が認証通知を拒否している場合、受信者がその受信を拒否することを可能であるようにしなければならない。なお、いたずら電話の防止や緊急サービスを提供する場合には、サービスプロバイダーはこの義務を免除されうる。

以上のように、同指令では電子通信サービスに係るプライバシーおよび個人情報保護に関して基本的な法令が策定されている。

2009 年プライバシー指令の改正

さて、2002 年プライバシー指令は、2009 年末に枠組指令や他の個別指令とともに改正されている。改正法では、おサイフケータイ等 RFID 技術を使用するサービスにも、それが電子通信網と接続される場合、同指令の規程が同様に適用されることが明記された。なおデジタル・アジェンダでは、改正法の国内法化を支援するため、2011 年まで同指令についてのガイダンスを行うとされている。以下に、同指令の改正ポイントを見て行く。

個人情報の侵害の通知義務

個人情報保護に関して、改正法ではサービスプロバイダーの責任が高められる。顧客の個人情報の侵害があった場合、サービスプロバイダーは各国の所管当局と顧客にその旨を通知しなくては

ならない（サービスプロバイダーが、所管当局に個人情報漏洩に対し十分な処置を行ったことを証明すれば、顧客に通知する義務は免除される）。このような措置は、サービスプロバイダーが通信網とサービスの保護により力を入れることを促すと考えられている。

クッキーの利用規程とスパム対策

- サービスプロバイダーは消費者がクッキーの使用についての情報をより明確に提供され、またその使用を拒否する権利をより簡単に実行できるようにしなければならない。
- 改正法では、スパムメール対策は、SMS 等、他の類似する通信アプリケーションにも適用されるべきであることが明記された。
- サービスプロバイダーは合法的なスパム対策により、ビジネスと顧客を保護すべきであると明記された。

欧州委員会による調和的技術方策の採択

欧州委員会は、ICT インフラセキュリティと同様に、個人情報の保護に関する技術的な方策を EU 域内で統一したものとするために、調和的な措置を採択する権利を与えられた。この採択には、委員会決定で手続きが取られる。

欧州とグーグルストリートビュー

ついで、欧州における個人情報およびプライバシー侵害問題として、米グーグル社のサービス「ストリートビュー」関連のものを記す。

このアプリケーションは、同社のオンライン地図サービス「グーグルマップ」上から、ユーザーが世界各地の写真にアクセスすることを可能にするものであり、2007 年よりアメリカの諸都市を皮切りに世

界中でサービスが開始されている[40]。このサービスは各地の写真風景を閲覧することを可能にするものであるから、実際に写真撮影を行う必要があり、グーグルカーと呼ばれる専用の自動車および「トライク」と呼ばれる自転車[41]が世界各地を回り、日々写真を撮影し、収集している[42]。

図版 1　最新のグーグルカー

出典　グーグル

図版 2　トライク

[40] 参考：グーグルストリートビュー日本語版
http://www.google.co.jp/help/maps/streetview/
[41] 自動車が入れない小道等は、トライクと呼ばれる専用の三輪車で対応している。
[42] 参考：グーグルの日本語サイトにおけるグーグルストリートビューの舞台裏説明
http://www.google.co.jp/help/maps/streetview/behind-the-scenes html

出典　グーグル

ところで、撮影された写真には風景だけでなく、人物等が入る可能性もあるので、プライバシーを侵害する恐れがあるとして、このサービスはアメリカ本土および日本を含む世界各地で非難を浴びている。

欧州では、2008 年にフランスで開催された自転車競技大会「ツール・ド・フランス」で初めて、ストリートビューを目的とした写真撮影が開始された[43]。専用のカメラを取り付けた自動車が撮影を行いつつ同大会のコースを走破したのであった。

だが、以上のように華々しく同サービスが欧州に上陸したとはいえ、欧州各国の情報保護所掌機関および市民は、手放しで同サービスの普及を喜んでいるわけではない。例えば欧州諸国では、個人のプライバシーを保護するために、ストリートビューで表示される人々の写真の顔部分にモザイクを入れることが要請されており、実際に至近距離で撮影された人々の写真には、顔にモザイク加工が施されている。また、個人のプライバシーを侵害する写真（例えば個人宅庭園等において裸でいる状態の写真）がストリートビューでインターネット上にアップロードされたとして、写真の削除を求める訴えが欧州各国で度々なされている。自動車の天井部に設置したカメラが塀等を越えて、個人宅

[43] http://www.cnil.fr/la-cnil/actu-cnil/article/article//street-view-la-cnil-en-fait-le-tour/ http://www.cnil fr/la-cnil/actu-cnil/article/article//la-cnil-dans-la-roue-du-velo-de-street-view/

敷地内を撮影する場合もあるのだ。

2010 年 2 月には、EU の作業グループである「情報保護に係る第 29 条作業部会」[44]（以下 G29 と略す）がグーグルを非難する声明を発表している。G29 はグーグルのストリートビューが EU のプライバシー指令に違反する可能性があるとしつつ、特に以下の事柄をグーグルに要求している。

- グーグルは撮影した写真に間違いがあった場合等に備えて写真を一年間保存しているが、保存期間を 6 ヶ月に縮めること
- グーグルカーが通ることを前もって市民に伝えること
- 個人のプライバシーを侵害する写真を撮影しないこと

これを受けて、グーグルは EU でストリートビューサービスの実施を禁止することをほのめかせている。

ところで、以上のようにプライバシー侵害に関して多くの非難を浴びているグーグルは、欧州でさらに批判の対象となる問題も引き起こした。

2010 年 5 月グーグルは、主に欧州諸国で、グーグルカーが風景の写真だけではなく、保護されていない WIFI 網を通して通信した個人の情報も誤って収集してしまったことを発表した[45]。この個人情報の中には、銀行口座等のオンライン ID やパスワードも含まれうるとし

---

[44] G29 は 1995 年に成立した情報保護に係る指令によって、同指令を各国において十全に適用するために設立された。この作業部会には、欧州各国の情報保護規制を所掌する機関の責任者が参加している。現在、G29 の最高責任者は、仏 CNIL の最高責任者であるアレックス・チュルクが務めている（2008 年 2 月から）。
http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_fr htm

[45]
http://www.cnil fr/dossiers/internet-telecoms/actualites/article/550/streetview-la-cnil-vient-dengager-un-controle-de-google/
http://www.cnil fr/dossiers/internet-telecoms/actualites/article/550/street-view-la-cnil-met-en-demeure-google-de-lui-communiquer-les-donnees-wi-fi-enregistrees/
http://www.01net.com/editorial/517809/les-donnees-recoltees-par-les-google-cars-seront-transmises-a-la-cnil/
http://www.01net.com/editorial/516864/la-cnil-ouvre-une-enquete-sur-google-street-view/
グーグル責任者のインタビュー記事も参考のこと。
http://www.ft.com/cms/s/2/db664044-6f43-11df-9f43-00144feabdc0.html

ている。

この事件に関して、ドイツおよびフランス当局が直ちに調査に乗り出している。2010 年 6 月、フランス当局のクニル（CNIL）[46]はグーグルにグーグルカーが不当に収集した個人情報の開示をいち早く求め、収集された個人情報を精査した。その結果、E メールサービスへの個人認証パスワードおよびメール本文内容を断片的にグーグルが収集していたことを突き止めている。

グーグルはこの件について、誤ってプロトタイプの技術を使用したことが原因であるとし、率直に非を認めている。同社は第三者組織に調査を依頼するとともに、内部調査も行っている。また被害のあった国でグーグルカーによる写真撮影も一時的に停止させたが、各国当局の判断により、2010 年 7 月中旬よりアイルランド、ノルウェイ、スゥエーデン、南アフリカでは再び撮影を開始するとしている[47]。フランスでは、同年秋頃にクニルがストリートビュー向けの撮影について許可を出すか決定するとしている[48]。

第二章　英国

ついで、英国における電子通信部門の個人情報保護政策を見ていきたい。まず所掌機関の概要を示し、業界団体による自主規制や官民キャンペーンの状況について示す。最後に、近年来問題となっている行動ターゲッティング広告の英国における動向を記す。

---

[46] クニルについては後に詳述する。

[47] http://google-latlong.blogspot.com/2010/07/street-view-driving-update.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+blogspot/SbSV+%28Google+LatLong%29

[48] http://www.01net.com/editorial/519159/les-google-cars-repartent-sur-les-routes-mais-pas-en-france/

個人情報保護所掌機関 ICO

英国においては、非省庁型行政機関[49]で法務省から資金を供給されている「ICO（Information Commissioner’s Office）」が、個人情報管理政策を所掌する独立規制機関として活動している[50]。ICO は「情報保護法（Data Protection Act）」、「プライバシーおよび電子通信規則（the Privacy and Electronic Communications Regulations）」という個人情報保護に係る法律に基づいて、係争を解決し、一定の義務を履行しない事業者などを取り締まっている。「プライバシーおよび電子通信規則」は、EU の 2002 年プライバシー指令を国内法化するために成立されたものである。また情報保護に関する適正な実践と助言および情報を伝えることも活動の一つである[51]。

- 情報保護法（1998 年成立）は個人情報の保護に係る権利と義務の法枠組みを定めており、個人情報を収集し利用する組織の活動を規制している。
- プライバシーおよび電子通信規則（2003 年成立）は、電話、ファックス、スパムメールによる未承諾広告を規制する法律である。この法律によれば、広告発信者が広告を送るためには受取手の同意を得なければならない。

現在、ICO は オンライン上の個人情報に係る新しい綱領を準備しているところである。

---

[49] 非省庁型機関は、中央省庁から一定の業務をいわば委託された組織で、通常のヒエラルキーには属さず、独立して活動している。だが、資金は中央省庁から供給され、最終的な責任は大臣が受け負う。

[50] http://www.ico.gov.uk/

[51] 以上の他、ICO は、「情報自由法（the Freedom of Information Act）」、「環境情報規則（the Environmental Information Regulations）」という法律に基づき、公共機関の情報開示に係る業務を担っている。

産業団体 IAB による自主規制

英国では、ICO による法規制の他、インターネット広告業界団体「IAB（Internet Advertising Bureau）」[52]が、ダイレクトマーケティング広告に係る個人情報の取り扱いについて自主規制を実施している。規制活動には、IAB もメンバーである英国の広告業界団体の「CAP（Commitee of Advertising Practice）」[53]が定める「広告綱領（CAP codes）」[54]が準拠となる。この綱領は、テレビおよびラジオ放送における広告以外の広告を対象とし、インターネットを含め、新聞、映画、広告板の規制の準拠となる。同綱領のダイレクト広告に係る規則条項において、ダイレクトマーケティングを目的として利用されるデータベースの取り扱いが規制されている。また、IAB は行動ターゲッティング広告について情報を提供するインターネットサイトを立ち上げている[55]。

官民共同キャンペーン

また英国では、「ゲット・セイフ・オンライン」という官民共同のキャンペーンが実施されている。 このキャンペーンには、内閣事務局、ビジネス・イノベーション・技能省、内務省、国家インフラ防護庁、重大組織犯罪庁（内務省の一機関）、マイクロソフト、英 HSBC 銀行が出資している。このキャンペーンにおいては、インターネット上のサイト[56]で、消費者にコンピューターウィルスやオンライン上での決済に係る詐欺への注意に加えて、個人情報の保護に関する助言および情報等を提供し、適正な実践を促している。

---

52 http://www.iabuk net/en/1/regulationselfregulation.html
53 http://bcap.org.uk/
54 http://bcap.org.uk/The-Codes/CAP-Code/CAP-Code-Item.aspx?q=CAP%20Code_Direct%20Marketing%20Rules_43%20%20Database%20practice
55 http://www.youronlinechoices.com/
56 www.getsafeonline.org

デジタル・ブリテン

さて、2009 年 6 月に発表された「デジタル・ブリテン最終報告書」において、個人情報およびプライバシーの保護は、将来的に重要性を増していく問題として捉えられている。

だが、ここでは、単に個人情報の保護を強化することだけではなく、個人情報データベースを適正に使用することによって、新たなビジネスモデルやサービスを作成する可能性に言及されているのが特徴である。行動ターゲッティング広告[57]等、新しい広告配信方法は多くの収益をもたらす可能性があるとしている。

行動ターゲッティング広告の問題

日本でも YAHOO!JAPAN が実施している行動ターゲッティング広告に関して[58]、英国では EU から批判を受けている[59]。

英国の大手固定通信事業者でインターネットサービスプロバイダーである BT（ブリティッシュテレコム）は、2006 年と 2007 年に米フォーム社（Phorm）の行動ターゲッティング広告のソフトウェアを使って、BT ユーザーの同意なく、ユーザーの行動傾向を分析し広告配信に利用した。2008 年 4 月に BT はこの事実を認め、2008 年 10 月から 12 月には招待制で同ソフトのテストを行っている。2008 年 4 月から、欧州委員会は英国市民および欧州議会の英国議員から質問を受けており、同年 7 月には英国当局に行動ターゲッティング広告に関する法整備状況について質問状を提出している。その結果、欧州委員会は英国における通信の傍受および盗聴に係る法律が十分にユーザーの

---

[57] 行動ターゲッティング広告とは、対象となる顧客のインターネット上の行動履歴を元に、顧客の興味関心を推測し、より効果的な広告配信を行うための手法である。

[58] http://pr.yahoo.co.jp/release/2007/0213a.html

[59] http://www.lemondeinformatique.fr/actualites/lire-le-fai-bt-a-espionne-18-000-clients-grace-a-phorm-25763 html
http://www.theregister.co.uk/2009/07/06/bt_phorm/

プライバシーを保護するものではなく、2002 年のプライバシー指令が不十分な仕方で国内法化されていることを指摘している[60]。2009 年 4 月に欧州委員会は EU 指令が十全に適用されていないとして、英国に通達を出し、違反手続きを開始した。その結果、結局、2009 年 7 月に BT は通信網にフォーム社の技術システムを展開しないことを発表した[61]。

だが、行動ターゲッティング広告は単に非難の対象となっているわけではない。英国の公正取引庁（Office of Fair Trading ： OFT）は 2009 年 8 月からグーグル、マイクロソフト、フォームの行動ターゲッティング広告に関して調査を実施し、2010 年 5 月には報告書を発表している[62]。それによれば、行動ターゲッティング広告は今後多くの収益をもたらすと予想されるが、プライバシーを侵害する可能性もある。以上の対策のため、OFT はインターネット広告業界団体である IAB を通して、事業者が自主規制を進めていくことが望ましいという見解を示しており、新たに法整備を実施することについては現在のところ考えていないようだ。

以上のように、英国では行動ターゲッティング広告の是非に関して、それがもたらしうる収益とプライバシー侵害の間で問題が生じている。

第二章　フランス

ついで、フランスにおける電子通信部門の個人情報保護政策を見て

---

[60] http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/570
欧州委員会の違反手続きについては以下のサイトを参考のこと。
http://ec.europa.eu/information_society/policy/ecomm/implementation_enforcement/infringement/index_en.htm

[61] http://www.guardian.co.uk/business/2009/jul/06/btgroup-privacy-and-the-net

[62] http://www.oft.gov.uk/news-and-updates/press/2010/53-10
http://www.guardian.co.uk/media/2010/may/25/oft-self-regulation-behavioural-advertising

いく。まず、同分野の所掌機関である CNIL（クニル）の概要を示し、フランスで現在審議が進んでいる新ロプシ法案の動向を記す。なおフランスでは EU のプライバシー指令は、主に「デジタル経済における信頼のための法」によって 2004 年に国内法化されている。

個人情報所掌機関 CNIL

フランスにおけるオンライン上の個人情報の保護対策に関しては、1978 年に成立した「情報通信・ファイル・自由に係る法律」（以下「情報通信と自由法」と略す）[63]に基づき、同年設立された「情報通信技術と自由国家委員会（La Commission Nationale de l'Informatique et des Libertés : CNIL）」（以下クニルと呼ぶ）[64]が所掌している。クニルは政府省庁から独立した行政機関であり、サイバー空間における個人のプライバシーおよび自由を保護することを目的として活動している。

以下が主な活動である[65]。

- 個人情報およびプライバシーに関する市民の苦情を受け付けること
- 政府に同分野の法案を提案すること
- 大臣、行政機関、公共機関および民間企業に対して、情報通信と自由法に違反した行為をしていないか監査を実施すること
- 違反行為を罰すること（罰金等）[66]。

また、情報通信と自由法によれば、政府は個人情報の自動処理に係る法案を下院に提出する前に、クニルに意見を求める義務があり、政

63 http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068624&dateTexte=vig
この法は現在まで度々改正され、2004 年に大きく改正されている。

64 http://www.cnil.fr/

65 個人情報の保護に係る活動の他、行政機関の情報開示業務を所掌している。

66 行為が政府による国家安全を目的とするものである場合は例外とされている。

府による行き過ぎた規制を検証する役割を持つが、クニルの意見が法的拘束力を持つ訳ではない。

CNIL と新ロプシ法案

さて、個人情報に関連する政府法案を事前に検証する役割をクニルは有するので、政府に法案の修正を求める場合もありうる。その最近の例として、「国内治安向上に関する指針および計画法案（Loi d'Orientation et de Programmation pour la Performance de la Sécurité intérieure : LOPPSI）」（以下、新ロプシ法案と略）[67]を巡る問題を挙げる。

新ロプシ法案は、2002 年成立の「国内治安に関する指針および計画法（Loi d'Orientation et de Programmation pour la Sécurité intérieure : LOPSI）」[68]（以下、ロプシ法と略）を改正することを目的とし、立案された。ロプシ法によって、警察関連機関の再編成およびその権限が強化されるとともに、サイバー犯罪対策について法整備が進められたが、新ロプシ法案はそれをさらに強化することを目的としている。この法案は、2009 年 1 月にニコラ・サルコジ大統領政権下のミシェル・

---

67 http://www.interieur.gouv fr/misill/sections/a_la_une/toute_l_actualite/archives-actualites/archives-securite/loppsi/view

68 参考 : 2002 年ロプシ法 http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000780288&dateTexte=
ニコラ・サルコジ現大統領は、ジャック・シラク前大統領政権下で内務相として 2002 年にロプシ法を成立させている。また、ロプシ法を成立させた後、この法律を補完するものとして、「国内治安のための法（Loi Pour la Sécurité Intérieure）」を成立させている。後者の法律は、通称サルコジ法と呼ばれており、警察関連組織の改善と権限を強化させたものである。以上のように、フランスではサルコジ大統領の下、国内治安悪化対策と対テロ政策の名目で、内務省を初めとする行政機関および警察等法執行機関の権限強化が進められている。新ロプシ法案および本報告書第四部で詳述するアドピ法は、元内務省のサルコジ大統領が主導する国内治安対策強化を背景に策定されている。
参考 : サルコジ法 http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000412199&dateTexte=

アリオ・マリー内務相[69]によって初めて提案され、サイバーセキュリティ関連の条項[70]を含む具体的な措置案は 2009 年 3 月に提案されて、同年 5 月には閣議に提出されている。同法案は 2009 年度から 2013 年度を対象期間としている。

さて、新ロプシ法案には、個人情報の保護政策に関係する条項もあり、それが議論を巻き起こしている。以下にそれらの概要について簡単に見て行こう。

オンライン上のユーザーID 偽装取締

現在の刑法では、インターネット上のユーザーID 偽装に関しては、それが不正払い出し等で金銭被害が発生した場合のみ取締を行っていたが、新ロプシ法案では刑法の関連条項を改正し、金銭被害が発生しない場合でも処罰の対象とすることを提案している。

犯罪捜査向け個人情報ファイル

2003 年成立の「国内治安のための法」では、犯罪捜査を向上させるために、警察等が捜査過程で容疑者および犠牲者の個人情報を収集し、情報ファイル[71]を作成し、使用することを認めているが、その対象は一定の重い処罰を受けた犯罪[72]に限られている。新ロプシ法案はその対象を拡大し、より罪の軽い犯罪に関しても同ファイルを作成することを提案している[73]。また憲法違反等がないか検証するために、犯罪者の情報ファイルを監査する目的で、司法官を設置することも提

---

[69] 同内務相は、次部で記すアドピ法の成立にも関わっており、国内治安に関連する法案を次々と策定し、精力的に活動しており、次期首相候補としても名前が挙げられている。

[70] 新ロプシ法案には児童ポルノ取締対策法案も含まれる。これに関しては、次節で詳述する。

[71] パリ近郊を管轄とするフランス警察が持つ情報ファイルは STIC と呼ばれており、フランスの地方で警察業務を行う国家憲兵（Gendarmerie）のファイルは JUDEX と呼ばれている。現在この二つのファイルを統合中であり、2011 年に ARIANE と呼ばれる新しい情報ファイルが完成する予定である。

[72] 生命および人身に対する犯罪に関しては 5 年以上の自由刑、財産に対する犯罪に関しては 7 年以上の自由刑を受けた犯罪者が対象となる。

[73] 生命および人身に対する犯罪および財産に対する犯罪問わず、5 年以上の自由刑を受けた者をファイル作成の対象とする。

案されている。

スパイウェアの使用

新ロプシ法案は、犯罪捜査向上のため、捜査官に「遠距離から」組織犯罪の容疑者が所有するコンピューター上および USB 等の周辺機器に記録された情報を獲得することを許可する。「遠距離から」というのは、他者のコンピューター等に特殊なソフトを使用して潜入し、情報を獲得するということを意味する。このような措置はテロ等重大犯罪にのみ適用され、実際に実行するには検事の請求後、予審判事による許可が必要となるとされている。

さて、個人情報の保護政策について、以上のような概要を持つ新ロプシ法案であるが、クニルは 2009 年 1 月に同法案の草稿を付託され、2009 年 4 月にこの法案について意見を提出し、7 月に公表している[74]。同法案に対するクニルの意見について、以下に二つの点について記す。

スパイウェアの使用に関する意見

クニルによれば、スパイウェアの使用を許す措置案は、法文が曖昧であり、本来の用途以外に措置が実施される可能性がある。例えば、この措置案では、立法機関によって保護されている人々（弁護士、政治家等）によって使用されている情報システムの情報も収集することを認めてしまう。またこの措置案は、公共の情報システムへスパイウェアを設置することも許しており、インターネットカフェや WiFi ホットスポットでフィルタリングを実施することを許可するものであり、広範囲での個人情報収集を可能にするが、このような措置は例外

---

[74] http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/207/
http://www.cnil fr/la-cnil/actu-cnil/article/article/12/securite-interieure-la-cnil-publie-son-avis-sur-la-loppsi/
http://www.cnil fr/la-cnil/actu-cnil/article/article//securite-interieure-la-cnil-publie-son-avis-sur-la-loppsi/
http://www.edri.org/edri-gram/number7.15/cnil-opinion-opssi
クニルは準備段階の政府の法案に対して意見を提出することを任務としており、通常公開されることはなかったが、新ロプシ法に関しては公表されている。

的な捜査手段に留まるべきであると強調している。結局のところ、クニルは、この措置案が本来の目的を超えて適用される可能性があり再検討するべきであるとしている。またさらに、クニルはこの措置のために具体的などのようなソフトウェアが使用されるか提示されていないとし、危惧を表明している。

犯罪捜査向け情報ファイルに関する意見

情報ファイルの作成対象者の拡大については、クニルは最大限の留保を表明している。クニルの意見では、このような情報ファイルの作成は重大な犯罪の場合にのみ限られるべきである。

元々、犯罪捜査向けの情報ファイルの作成と管理について、クニルは批判的であった。2007 年 6 月から 2008 年 11 月にかけて、クニルはフランス警察の個人情報ファイル「STIC」の精査を行った[75]。STIC は 1990 年代に作成され始めたが、正式に認められたものではなく、2001 年になって合法的に存在が承認された。現在内務省がこのファイルを管理している。このファイルは当初犯罪捜査向けに作成されていたものだが、2003 年のサルコジ法によって、一定の職業（警察官、大使、司法官、ガードマン等）の募集の際に、閲覧することが許可されていた。クニルの検証では、STIC には不正確な情報が多分に含まれていたり、新しい情報が付け足されていなかったりすることが発見され、STIC の管理システムの改善を内務省に促している。STIC の情報は、直接失業等に関与しうるため、その正確さには最大限の注意が必要であるからである。

さて、新ロプシ法案は 2010 年 2 月に下院に提出され[76]、第一読会が開かれた。そして、法案は同月に採択されて、上院に提出された。上院による採決は 2010 年 6 月の予定であったが、結局同年秋に延期さ

75 http://www.cnil fr/la-cnil/actu-cnil/article/article//controle-du-stic-les-propositions-de-la-cnil-pour-une-utilisation-du-fichier-plus-respectueuse-du/

76 http://www.liberation fr/societe/0101618430-loppsi-2-une-loi-fourre-tout

れている。

さて、同法案の採決延期には、クニルが関与していると考えられる。何故なら、クニルによれば、2010 年 2 月に下院を通過した法案と 2009 年 4 月にクニルが意見を提出した法案にははっきりとした違いが見られ、2010 年 5 月上院議員の求めに応じて再度意見を提出し、6 月にそれを公表しているからである[77]。

クニルの発表では、下院を通過した案では、クニルの意見に基づいて幾つかの点で修正がなされたものの、修正されないままの点もあり、さらに新たに措置案が付け加えられていた。全ての法案が 2009 年 4 月にクニルが意見を出す段階で、クニルに渡されていなかったのだ。

修正された点に関しては、立法機関によって保護されている人々が、スパイウェアによる捜査の対象となりうるという問題は、法文を修正することによって改善された。修正されなかった点に関しては、スパイウェアのインターネットカフェや WiFi ホットスポットでの使用、個人情報ファイル作成の対象基準を拡大すること等は、新法案で修正されずに、下院に提出された。

2010 年 6 月に発表されたクニルの意見によると、とりわけ監視・防犯ビデオカメラの設置に関する措置案[78]が 2010 年 2 月に下院に提出

---

77 http://www.cnil fr/la-cnil/actu-cnil/article/article/12/les-observations-de-la-cnil-sur-les-nouvelles-dispositions-de-la-loppsi/

78 新ロプシ法案では、監視・防犯ビデオカメラの設置数を増加させるために、個人の監視カメラ設置に係る規制を緩和することが提案されている。具体的には、個人の防犯カメラによって撮影が許可される公道の部分を拡大する。現在フランスでは監視カメラを設置するための基準が厳しく制限されている。また法案では、費用節約のため、公共機関の監視カメラが撮影した映像を民間事業者が管理できる体制を整えることが提案されている。だが、撮影された映像の濫用を防ぐため、事業を委託された民間事業者の社員に元の映像フィルムが渡されることを禁止している[78]。また、ビデオテープの保存最短期間を地方行政の最高責任者である地方長官が決定できるようにするとしている。

以上のように、監視カメラの設置を増加させるための法案が提案される一方で、プライバシーを保護するための法案も提案されている。例えば、監視・防犯ビデオカメラの規制および監査を目的に 2007 年内務省傘下に設立された「ビデオ監視委員会」の権限と役割を強化し、また許可なくビデオ監視システムが設置されている建物を閉鎖できる権限を地方長官に与えるとしている。

された法案に新たに付け足された。つまり、クニルが 2009 年 1 月に付託された法案にはこの措置案は存在しなかった。

以上のように、新ロプシ法案はクニルの意見を全て取り入れたわけではなく、今後実際にこの法案が採択されるか注目を集めている。

第四章　ドイツ

連邦制を採用するドイツでは、日本やフランス等、中央集権的な行政システムを有する国家とは違い、個人情報保護政策について地方分権が進んでいる。本報告書では、連邦レベルで進められる政策に関してのみ簡単に触れるに留まる。

個人情報所掌機関 BfDI

ドイツにおける個人の情報保護所掌機関は、連邦内務省傘下の「データ保護および情報の自由のための連邦委員会（BfDi）」である[79]。同連邦委員会は 1978 年に設立され、その権限および役割は「連邦データ保護法」によって定められている。同法はドイツの個人情報保護に関する枠組みとなる法律で、1977 年に成立し、2009 年に改正されている。同委員会の任務は、連邦データ保護法が連邦公共機関および州公共機関、民間事業者等に実際に遵守されているかを監視する役割を持つ。なお 2005 年に成立した「ドイツ情報の自由法」[80]により、同委員会はデータ保護だけでなく、連邦公共機関が保有する情報の開示に

以上の防犯・監視ビデオカメラに係る措置案について、クニルは新たに批判をしている。特に、民間事業者に公共機関が撮影したビデオの管理を委託することを批判しており、民間事業者に委託した際にビデオの管理体制が十分でなくなる恐れがあること、第三国の事業者へ委託される可能性があることを指摘している。

79 http://www.bfdi.bund.de/cln_134/FR/Home/homepage_node.html

80 http://www.bfdi.bund.de/cae/servlet/contentblob/412040/publicationFile/24681/TextIFG_EN.pdf

ついても管轄としているが、個人情報保護の制度に比べ、情報公開制度に関しては整備が遅れているという指摘もある。

以上の連邦委員会の他、ドイツには各州の個人情報保護の監督官によって構成される作業グループ「デュッセルドルフ協会」がある。

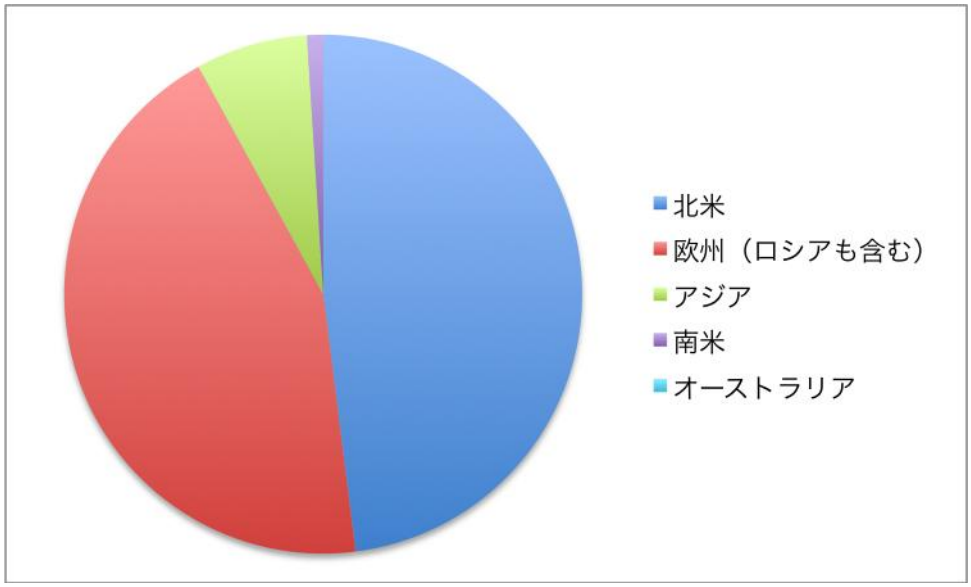
以上、欧州における個人情報保護政策を概観してきた。特に、英国では行動ターゲッティング広告の規制の是非、またフランスでは国内治安維持に係る措置と個人情報保護のバランスが問題となっており、それぞれ今後の進展が興味深い。

第三部　欧州における違法・有害情報の規制政策

次に、欧州におけるサイバー空間の違法・有害情報の規制政策を見ていきたい。ここで違法・有害情報とは、主に児童ポルノ画像や人種主義を増長させるような情報を指す。欧州では児童ポルノの単純所持が処罰の対象となっており、一般的に日本よりも児童ポルノの規制は非常に進んでいる考えられることが多い。

まず、世界の児童ポルノ産出状況を確認したい。以下の図は、英国のインターネット上の児童ポルノを監視している組織「IWF」[81]が作成した 2009 年の世界地域別児童ポルノの産出国データ（IWF への報告数）を表したものである[82]。

図版 3 世界の児童ポルノ産出状況



[81] IWF については次節で詳しく記す。
[82] http://www.iwf.org.uk/resources/trends#Internationalremoval

北米	48%
欧州（ロシアも含む）	44%
アジア	7%
南米	1%
オーストラリア	0%

出典　IWF

北米が 48%で最も高く、ロシアを含めた欧州は 44%、アジアは 7%、南米は 1%、オーストラリアは 1%にも満たないことが分かる。以上のデータは、日本が児童ポルノの制作、供給、消費の主要な拠点となっているという批判を覆すものになる[83]。だが、日本では漫画やアニメーション等の登場人物は児童ポルノの対象となっていないので、上記のような数値が出ている可能性がある。

第一章　欧州連合

EU では、1996 年に視聴覚放送および情報通信サービスにおける未成年者および人間の尊厳の保護についてのグリーンペーパー[84]が出され、初めて本格的に EU で規制政策の審議が開始された[85]。この審議は 1998 年に理事会勧告[86]に結実し、加盟国が有害・違法コンテンツの

---

[83] http://tokyo.usembassy.gov/j/p/tpj-20090105-72 html

[84] http://europa.eu/legislation_summaries/audiovisual_and_media/l24030_en.htm
正式名称は以下の通りである。
Green Paper on the protection of minors and human dignity in audiovisual and information services

[85] EU の違法・有害コンテンツの規制法および対策プログラムの主なものは、以下のサイトで取得することができる。
http://ec.europa.eu/information_society/activities/sip/policy/legislation/index_en htm

[86] http://europa.eu/legislation_summaries/audiovisual_and_media/l24030b_en htm
正式名称は以下の通りである。
Council Recommendation 98/560/EC of 24 September 1998 on the development of the competitiveness of the European audiovisual and information services industry by

規制政策枠組みを策定することが促された。また 2000 年には「インターネット上の児童ポルノ対策に係る理事会決定」という法令が成立され、法的手段も制定された。以上の他、1989 年に採択され、1997 年に改正された「国境のないテレビ指令」でも放送部門の有害コンテンツの規制法が制定されている。そして、現在 EU ではさらに違法・有害コンテンツの規制強化が進み、法整備が進められつつある。

以下に、主な同分野の主な EU 法令および勧告を記す[87]。

児童の性的搾取および児童ポルノに係る理事会枠組決定

2000 年、児童買春旅行の流行を受け、欧州議会は同旅行が児童の性的搾取と児童ポルノと緊密につながる犯罪行為であることを繰り返し主張し、欧州委員会にこれらの行為に関する最低限の規則を定める枠組規制法案を閣僚理事会へ提出することを要請した。そして、2003 年 12 月、「児童の性的搾取および児童ポルノに対する取り組みに係る理事会枠組決定」[88]（以下理事会枠組決定と略す）という法令が成立された。

理事会枠組決定では、児童の性的搾取および児童ポルノを取り締まる包括的な措置を講じるため、最低限の法的枠組、すなわち児童ポルノの定義、刑罰等の枠組みが定められた。これに基づき、加盟国は国内法の下、違反者に十分な罰則を課さなければならない。

---

promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity

[87] また EU とは別組織である「欧州評議会（Council of Europe）」でも児童ポルノの取締および被害にあった児童支援、専門家の育成等のガイドラインを定める「性的搾取および性的虐待に対する児童保護に係る欧州評議会協約」が 2007 年 10 月に策定されている。
http://conventions.coe.int/Treaty/EN/Summaries/Html/201.htm
http://conventions.coe.int/Treaty/EN/Treaties/Html/201.htm

[88]
http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_trafficking_in_human_beings/l33138_en.htm
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004F0068:EN:HTML

以下に、幾つかの主な条項を挙げる。

第一条　定義

同法における「児童」および「児童ポルノ」等の語が、以下のように定義されている。

・児童は 18 歳未満を指す。

・児童ポルノは以下のように定義される。

「「児童ポルノ」は、以下の事項を視覚的に描くもしくは表す性的な表現物を指す。

(1) 性的に露骨な行動に参加し、もしくは従事している実在する児童。児童の性器もしくは恥骨部のわいせつな表示を含む。

(2) (1)で言及された行動に参加し、もしくは従事している児童のように見える実在する人物。

(3) (1)で言及された行動に参加し、もしくは従事している実際には実在しない児童の写実的な画像」

第三条　児童ポルノに係る対策措置

加盟国は、児童ポルノの製造、流布、提供、獲得および所有を目的とする行動を罰することを保証しなければならない

第四条　教唆、援助、幇助、企図

加盟国は、児童の性的搾取および児童ポルノを教唆、支援、幇助する活動を罰すことを保証しなければならない。

以上のように、同枠組決定は EU における児童ポルノ規制法の最低限の共通枠組みを制定する法令である。第一条では、実在しない児童、つまりコンピューターグラフィックス等で描かれた写実的な（realistic）児童の画像も取り締まりの対象となっていること、また第三条では、児童ポルノの獲得および所有が禁止され、第四条では児童ポルノを幇助することも取締の対象とされていることが注目される。

理事会枠組決定の改正案

さて、2009 年 3 月、上記の理事会枠組決定の改正案が EU に提案された[89]。改正の理由は、現行の法令では 1) 情報通信技術を使用した新しい形態の児童搾取に対処できないこと、2) 各国が国境を越えて児童搾取の取締を行えないこと、3) 被害にあった児童への支援が十分でないこと、4) 児童搾取を予防する適切な措置が定められていないことが改正理由として挙げられており、これらの問題を解決する法案が提案されている。

改正法案においては、警察当局にインターネットユーザーによる児童ポルノサイトへのアクセスを遮断する権限を与える条項が付け加えられている。これはブロッキングあるいはフィルタリングとも呼ばれている措置である。これは、他国の児童ポルノサイトを警察当局が取り締まるのには限界があるため、海外に設置されている児童ポルノサイトへのアクセスを遮断して、児童ポルノの蔓延を防ぐことが狙いである。現在、欧州ではブロッキング措置の導入がすでに実施されている国、もしくは審議されている国があり、同法案が施行されるならば、EU 域内全域で同措置が導入されることになる。だが、同措置が当局により当初の目的を超えて適用される可能性があることを懸念して、導入に反対する意見もある[90]。同措置については、欧州主要国の動向を示す際に再び記す。

視聴覚メディアサービス指令

2007 年 12 月に成立した「視聴覚メディアサービス指令」において、放送部門の有害・違法コンテンツの規制がさらに強化された。

同指令は、EU 加盟国の視聴覚放送に係る規制法を EU 域内で調和

---

89 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0135:FIN:EN:PDF

90 http://en.eco.de/association/202_6106 htm

させることを目的としている。EU では、1980 年代から視聴覚放送の規制政策が始まり、1989 年に「国境のないテレビ指令」が制定されており、この指令は 1997 年と 2007 年に改正された[91]。そして、2007 年の改正の際に、この指令は視聴覚メディアサービス指令という呼称が与えられた。

2007 年の改正では、ICT 技術の進歩とビジネスモデルの変化に対応することが目的とされ、一度に不特定多数の受け手へと発信するテレビ放送の他に、受け手が受信を選択するオン・デマンド放送も規制の対象となったことが大きな変化である[92]。なお商業目的ではなく、共通の関心に基づいて、私的な利用のため視聴覚コンテンツを共有し、交換することに関してはこの指令は適用範囲としない。

なお同指令は、2009 年 12 月までに加盟国が国内法化することを義務づけていた。

同指令の主な規制テーマは以下の通りである。

- 文化的多様性の保存
- 未成年者および視聴者の保護
- メディアの多元主義
- 人種主義および宗教的憎悪に対する取り組み
- 各加盟国内メディア規制機関の独立性の保障

視聴覚メディアサービス指令における違法・有害情報規制に関しては、まず序文で、先に見た 2003 年の理事会枠組決定に従って、児童ポルノの流布を禁止することが確認される[93]。ついで、本文第三章第

---

[91] http://ec.europa.eu/avpolicy/reg/history/index_en.htm

[92] 視聴覚サービスという言葉には、音声のみのサービスとラジオサービスは含まれない。またテレビ放送という言葉には、アナログおよび地上波放送、生放送、ネット配信、NVOD（Near Video On demand）が入る。そして、VOD（Video On Demand）はオン・デマンド視聴覚サービスに入る。なお動画等がウェブサイト上でそれを見せるのが目的ではなく、副次的な要素となっている場合は規制の対象とならない。

[93] 「メディアサービスプロバイダーは加盟国の管轄の下で、児童の性的搾取および児童ポルノへの取り組みに係る理事会枠組決定（2003 年 12 月 22 日成立）の諸条項に従って、いかなる場合においても、児童ポルノ流布の禁止の法的対象とされなけ

六条[94]および第九条[95]で、違法・有害コンテンツを規制することを加盟国に命じている。同指令第八章第二七条はテレビ放送における未成年者の保護に係る規制となっている[96]。なお、序文では、表現の自由と有害情報の規制のバランスについても触れられている[97]。

インターネット安全プログラム

以上、違法・有害情報規制に係る EU の法整備状況および勧告を見てきたが、これらの規制法の制定と並行して、1999 年から EU は「インターネット安全プログラム（Safer Internet Program）」というインターネットの適正な使用に関する戦略を打ち出しており、その中に違

ればならない」（第 61 段落）

[94] 「適当な手段を使用して、加盟国は、メディアサービスプロバイダーによって加盟国の管轄の下で提供される視聴覚メディアサービスが、人種、性別、宗教や国籍に基づく憎悪を煽動するいかなるものも含まないようにすることを保障しなければならない」

[95]第九条は、視聴覚メディアサービスにおける商業目的の宣伝の規制条項である。そこでは、宣伝が人間の尊厳を傷つけ、また性別、人種および種族的出身、国籍、宗教、信仰、障害、年齢、性的指向に基づく差別を含み、もしくは増長してはいけないと定められている。また、煙草の宣伝は視聴覚放送において禁止され、アルコール飲料の宣伝は未成年者向けに行われてはならないし、過度の飲酒を勧めるものであってはならないとしている。

[96]

1「加盟国は、放送事業者によって加盟国の管轄の下で提供されるテレビ放送に、未成年者の身体的、精神的、道徳的成長を重大に損なう可能性のある放送プログラム、特にポルノグラフィーもしくは不当な暴力を含む放送プログラムが含まれないように保障しなければならない」

2「上記の第一段落に関して講じられる措置は、未成年者の身体的、精神的、道徳的成長を損なうように思われる他の放送プログラムにも同様に拡大して適用されなければならない。だが、放送時間の選択もしくは技術的な措置によって、放送圏内の未成年者が通常そのような放送を視聴しないことが保証されている場合は拡大適用されない」

[97] 「未成年者の身体的、精神的、道徳的成長および人間の尊厳を保護するために採用される措置は、欧州連合基本権憲章で定められたような表現の自由に係る基本権と注意深く釣り合いが保たれなくてはならない。特にオン・デマンド視聴覚メディアサービスに関しては、個人認証番号（PIN コード）、フィルタリングおよびラベリングシステムのような措置は、未成年者の身体的、精神的、道徳的成長および人間の尊厳を保護するのに十分なレベルに達していなければならない」（第 60 段落）

法・有害情報の取締政策も含まれている[98]。現在同プログラムは第三期目（2009 年～2013 年）に入った。（第一期目は 1999 年～2004、第二期目は 2005 年～2008 年）

同プログラムの主な目的は以下のものである。

- 安全なインターネットおよび他の通信技術の利用を、特に児童および若年者のために促進する
- 上記の点に関し、特に児童、保護者、世話人、教師、教育者に対して教育を与える
- インターネット上の違法コンテンツおよび有害活動に対して対策を講ずる

同プログラムでは、特に上記のテーマに係る EU レベルおよび加盟国内の活動を財政的に支援している。このため毎年作業プログラムを発表し、同分野の様々なプロジェクトを公募しており、第三期目は 5 年間で 5500 万ユーロが拠出される見込みである。

また、同プログラムは「Ins@fe」[99]という多くの関連組織から構成されるコンソーシアムを財政支援している。このコンソーシアムは毎年一度、インターネット安全デーを開催して、サイバー空間における未成年者の保護に係る問題について市民の意識を高めるための活動を行っている。

2010 年度から、各国に設置されたインターネット安全センターの主導の下、各国で児童および若年者によるフォーラムを開催する予定である。これは携帯電話等に使い慣れた児童および若年者から生の意見を聞くことが目的である。

以下に最新の 2010 年度作業プログラムの概要を見て行く。

---

98 http://ec.europa.eu/information_society/activities/sip/policy/index_en.htm
99 http://www.saferinternet.org/web/guest/about-us

2010 年度作業プログラム

目的

- インターネットの適正な使用について市民の意識を高める
- インターネット上の違法コンテンツおよび有害な活動に対策を講ずる
- 安全なインターネット環境を促進する
- 知識基盤を設立する

申請可能資格

EU 加盟国で設立された法人および EFTA 加盟国のノルウェイ、アイスランド、リヒテンシュタインで設立された法人

公募プロジェクト

以下に同プログラムで公募されているプロジェクトを挙げる[100]。

・インターネット安全センターの活動支援と欧州規模での提携活動

インターネット安全プログラムは、各加盟国に設置されたインターネット安全センター（Safer Internet Centre）[101]を公募によって財政支援している。

各インターネット安全センターは、サイバー空間における未成年者の保護について市民の意識を高めることを主な任務としており、その他、市民が違法コンテンツについて通報できるホットライン、もしくは児童およびその保護者が、不当な目的のため児童に近づく行為、有害コンテンツ、ネットいじめ等について助言を得ることができるヘルプラインを有している。この公募では、上記の活動、そしてそれらの

[100] より詳しい公募の条件に関しては、元の資料を参考のこと。
http://ec.europa.eu/information_society/activities/sip/policy/programme/current_prog/index_en.htm

[101] http://ec.europa.eu/information_society/activities/sip/projects/centres/index_en.htm#awareness_insafe

欧州規模での提携活動をサポートするプロジェクトに財政支援を行う。

加盟国内のインターネット安全センターの例を挙げると、フランスではトララレール（児童向けインターネット・マルチメディアコンテンツプロバイダー）、インターネット児童保護協会、高等教育・研究省、インターネットプロバイダー・サービス事業者協会が提携して、インターネット安全センターを運営している。

・欧州規模での法執行機関の提携活動

このプロジェクトでは、児童ポルノが国際規模で流布されていることを考慮し、各国の警察など法執行機関のネットワークを築き、欧州規模での提携を支援する活動に財政支援を行う。このネットワークは法執行機関の間で情報交換を行う拠点となるが、実際の捜査には関与しない。また、以上の提携活動に係るプロジェクトの他、P2P ネットワークにおける情報を分析するツールを法執行機関向けに開発するプロジェクトも同プロジェクトで公募されている。

・ネット依存の流行についての研究

このプロジェクトでは、欧州において未成年者のネット依存の状況を調査する活動に対して財政支援する。調査では、どのようにネット依存する未成年者が増えているか、またどのようにすればその増加を防ぐことができるか明らかにすることが問題となる。

・児童の新しいメディアの利用に関する社会調査

この公募プロジェクトでは、社会学者およびサイバー空間における児童保護の専門家を提携させ、児童がインターネット上の新しいメディアをどのように利用しているかを調査し、児童保護に関して配慮が必要なエリアを特定する活動を財政支援する。

ホットラインおよび自主規制の支援

EU は、各国の違法コンテンツのホットライン事業者、通信またはコンテンツ事業者による違法・コンテンツと青少年保護に関する EU レベルでの自主規制取り組みを支援している[102]。

ホットライン支援

INHOPE（Internet Hotline Provider in Europe Association）は、1999 年に EU の支援の下設立されたホットライン事業者の組織である[103]。同組織は参加事業者の支援を行っている。現在、33 カ国から 38 事業者が参加している。

自主規制支援

2007 年には、欧州の移動体通信およびコンテンツ事業者が「青少年および児童による安全な携帯電話の使用に関する欧州枠組協定」[104]を締結している。これは、EU 域内で未成年者による携帯電話の安全な使用を促進するために、共通の原則および措置を取り決めるもので、協定に署名した事業者が各国で実施している。2010 年 9 月までに、29 の欧州の主要な事業者が協定に参加している[105]。

また 2009 年 2 月には、ソーシャルネットワーキングサービスの事業者が中心となり、「EU のためのソーシャルネットワーキング原則」[106]という協定を結んでいる。ここでは、EU 域内で同サービスを実施する際の原則が取り決められている。

---

102 http://ec.europa.eu/information_society/activities/sip/self_reg/index_en.htm

103 https://www.inhope.org/en/about/about.html

104 http://ec.europa.eu/information_society/activities/sip/docs/mobile_2005/europeanframework.pdf

105 協定に参加している事業者のリストは以下のサイトから取得できる。http://www.gsmeurope.org/safer_mobile/signatories.shtml

106 http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

第二章　英国

ついで、英国における違法・有害コンテンツ規制の現状と最新動向を記す。

IWF の自主規制

インターネット上の違法・有害情報の規制政策に関して、英国ではケンブリッジに本拠地を持つインターネット監視財団（Internet Watch Foundation : IWF）による自主規制活動が大きな影響力を持つ[107]。IWF は 1996 年にインターネット業界によって設立された産業団体であり、同団体への登録組織の他、EU の「インターネット安全プログラム」から資金提供を受けており、世界的に有名なウェブ監視団体である。現在、IWF への登録団体は現在、インターネットサービスプロバイダー（ISP）、テレコムオペレーター、コンテンツ制作事業者等、100 団体に昇る。IWF は違法コンテンツに関するインターネットのホットラインとして設立され、自主規制を行う産業団体であるが、法執行機関[108]、英国政府[109]、関連の国際組織に違法コンテンツの情報を提供する等して、緊密に提携して活動している。

IWF は、1）世界中でホスティングされている児童ポルノの画像、2）英国内でホスティングされている犯罪性のある猥褻なアダルト画像、3）英国内でホスティングされている人種差別に関わるコンテンツ、4）英国内でホスティングされている写真やビデオ以外の児童ポルノを減少させることを目的としている。英国においては、児童ポル

---

[107] http://www.iwf.org.uk/
http://www.iwf.org.uk/public/page.103.htm

[108] 特に、児童搾取オンライン保護局、重大組織犯罪庁、中央警察小児性愛者対策班、スコットランド・ハイテク犯罪班等である。

[109] 特に、内務省、ビジネス・イノベーション・スキル省、法務省、教育省、文化・メディア・スポーツ省およびこの問題に関心を持つ国会議員等と提携している。

ノの基準は、量刑協議会（Sentencing Council）[110]が定めており、IWF の活動もこの基準に従う[111]。

以上の目的のため、IWF は市民による報告システム（ホットライン）およびネットワークの監視システムにより違法コンテンツを監視し、同コンテンツを減少させるため、a）「通知と削除」システムを実行し、b) ブロッキングのため児童ポルノの URL リストの作成を実施している。

a）の通知と削除システムとは、IWF が ISP に違法コンテンツを通知し、ついで削除させる手続きのことを言う。IWF から通知を受け取った IWF 参加組織は、そのコンテンツを迅速に削除するか、あるいは IWF の通知が適正なものではないという通知を返す義務を持つ。もし IWF の通知を受け取った組織がその通知を無視したり、それに同意しない場合、IWF の内部組織が調査を実施する。この調査によって、IWF による元の通知の妥当性が証明された場合、IWF は法執行機関に問題の解決を委託するか、IWF が IWF 登録資格を停止するかもしくは取り下げる等して制裁措置を取る。

b）IWF は違法コンテンツサイトのブラックリストを作成し、ISP へ渡す、これにより、ISP はユーザーによるそれらのサイトへのアクセスを切断できる。このようなブロッキングと言われる手段は、とりわけ海外でホスティングされている児童ポルノコンテンツへのアクセスを遮断するのに有効であり、違法コンテンツの削除以前の一時的な手段として捉えられている。IWF の役割はリストを作成し、それを IWF に登録する ISP に配布するのみであり、実際にアクセスの切断を実施するのは ISP である。なおブロッキングは、強制ではなく、ISP が任意で実施している。

ところで、以上の IWF のブラックリストによるブロッキング検閲

---

[110] 量刑協議会は、量刑に関するガイドラインおよびその実行を監視している法務省外部組織である。

[111] 詳しい基準については以下のサイトを参考のこと。
http://www.iwf.org.uk/police/page.105 htm

制度は問題も巻き起こしている。2008 年 12 月 5 日に IWF はウィキペディアに掲載された「スコーピオンズ」というロックバンドの 1976 年のアルバム（『Virgin Killer』）に関する記事をブラックリストに入れ、その結果、IWF に参加する ISP がユーザーによるその記事へのアクセスをブロックし、英国のユーザーはその記事へアクセスできなくなった。IWF がその記事をブラックリストに入れた理由は、記事に掲載されたロックバンドのアルバムのジャケット写真が、児童ポルノに属すると判断したからである。だが、このような措置に対して、ウィキペディアを運営するウィキペディア財団は同年 12 月 7 日に、同記事は違法コンテンツ規制の対象とはならないと声明を出し、最終的に翌日 12 月 8 日に IWF は同記事をブラックリストから削除することを決定し、ブロックは解除された[112]。

上記の IWF によるウィキペディアの記事のブロックは、大きな反響を呼んだ。IWF への批判としては、確かに 1976 年のリリース当時から『Virgin Killer』というアルバムのジャケット写真は、その是非が議論を巻き起こしてきたが、アルバムの販売禁止措置等は講じられておらず、アルバムは市場に 30 年以上前から普通に流通していた。よって、急にウィキペディアの記事のみアクセスが切断されるのはおかしいという意見がある。またより一般的な観点から、児童ポルノには反対するが、その検閲基準が広すぎ、検閲が行き過ぎる可能性が潜在的に存在し、結果として表現の自由を奪い、監視社会を到来させるものであるという意見を呼んだ。また今回の事件は、中国等の国のように、英国にも非常に厳しい検閲制度が存在することを知らしめるものであったとする意見もある。

---

[112] この事件について、より詳しい情報は以下の資料を参考のこと。
http://en.wikipedia.org/wiki/Wikipedia:Administrators%27_noticeboard/Major_UK_ISPs_reduced_to_using_2_IP_addresses
http://en.wikipedia.org/wiki/Internet_Watch_Foundation_and_Wikipedia
http://www.zdnet.co.uk/news/networking/2009/02/20/iwf-chief-why-wikipedia-block-went-wrong-39616171/
http://aaisp.net.uk/news-censorship.html

CEOP の活動

英国政府の児童の性的搾取および児童ポルノの流布取締を所掌する主な機関は、独立法執行機関である重大組織犯罪庁（Serious Organized Crime Agency : SOCA）に属する児童搾取オンライン保護局（Child Exploitation Online Protection Centre : CEOP）である[113]。CEOP では、同分野の取締を専門とする警察官および関連団体また民間企業の専門家が協力して児童の性的搾取および児童ポルノ根絶を目指して活動している。

CEOP の最近の注目すべき活動としては、2010 年 2 月に児童を性的搾取から保護する措置として、英国内のソーシャルネットワーキングサービス（SNS）に、未成年のユーザーが警察等の機関に直接助けを求めることができるワンクリックボタンを設置することを要請したことが挙げられる[114]。このボタンは「CLICKCEOP」とも呼ばれ、2006 年からすでに多くのサービス、例えば英国内の MSN メッセンジャー等に設置されていた。このボタンによって、CEOP だけでなく、IWF や児童保護団体等から直接助言等を得ることができる。2010 年 7 月には世界最大の SNS であるフェイスブックが、英国内において、同ボタンを設置することを決定している[115]。なおこのボタンは専用のアプリケーションをフェイスブックサイト内でダウンロードすることによって、フェイスブックの本人のページに設置することができる。

第三章　フランス

ついで、フランスにおける違法・有害情報の規制政策の最新動向を見て行こう。

---

113 www.ceop.gov.uk
114 http://www.ceop.gov.uk/mediacentre/pressreleases/2010/ceop_09032010.asp
115 http://www.ceop.police.uk/mediacentre/pressreleases/2010/ceop_12072010fb.asp

ISP 産業団体および警察当局のホットライン

「インターネットサービスプロバイダー協会（Association des Fournisseurs d'Accès et de services internet : AFA）」[116]は、フランスのインターネットサービスプロバイダー（以下 ISP と略）の産業団体として 1997 年に設立された。AFA はインターネット空間における未成年者保護を目的として、1998 年に違法コンテンツのホットラインをインターネット上に設置している[117]。このホットラインは、AFA の参加メンバーおよび EU の「インターネット安全プログラム」から資金提供を受けている。2009 年 9 月には携帯端末向けのホットラインを設置している。なお、AFA は「職業倫理綱領」において、未成年者保護のために ICRA というフィルタリング技術を保護者が使用することを推薦している[118]。

フランスでは、上記の AFA のホットラインの他に、警察機関に属する「情報通信技術に係る犯罪対策中央局（Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication : OCLTIC）」[119]が、同様にインターネット上にホットラインを、2008 年 11 月に設置し、管理運営している[120]。OCLTIC は、サイバー空間における犯罪を専門とする機関で、2000 年 5 月に設立された。

---

116 http://www.afa-france.com/

117 http://www.pointdecontact net/protectiondelenfance html

118 http://delegation.internet.gouv fr/mineurs/pratique.htm
http://www.afa-france.com/deontologie html#mineurs
http://www.fosi.org/icra/

119 http://www.interieur.gouv fr/sections/a_l_interieur/la_police_nationale/organisation/dcpj/cyber-criminalite/

120 https://www.internet-signalement.gouv fr/PortailWeb/planets/Accueil!input.action
http://www.zdnet.fr/actualites/le-gouvernement-ouvre-un-portail-anti-contenus-illicites-39384821 htm
http://www.clubic.com/actualite-284208-pharos-site-signaler-contenus-illicites html

新ロプシ法と児童ポルノ規制

本報告書第二部で記したように、フランスではサイバー犯罪を含む国内治安対策強化のために、2010 年夏、新ロプシ法案が上院で審議されているところであるが、この法案にはインターネット上の児童ポルノ規制対策法案も含まれている。

新ロプシ法案では、他国の児童ポルノサイトへのブロッキングを実施することが提案されている。現在フランスでは、他の多くの国のように、国内にホスティングされている違法児童ポルノサイトに関しては、警察当局が削除を行っているが、多くの児童ポルノサイトは他国にホスティングされている。よって、英国の IWF が行っているようなブロッキングの実施が必要不可欠であるという意見が増えており、新ロプシ法案はそのような意見を踏まえたものである。

新ロプシ法案では、警察当局（OCLTIC）が各 ISP に児童ポルノサイトのブラックリストを送付し、ISP はそのリストに記載されたコンテンツへのアクセスを切断する義務が課せられる。切断のために使用される技術的な手段に関しては、ISP の判断に委ねられるとされている。フランス当局のブロッキング措置は、英国の IWF を見習ったものである。だが、IWF は産業団体であり、ブロッキング措置は自主規制の枠に収まるものであるが、フランスでは内務省および警察当局が規制の主体となっている点が大きく異なる。

新ロプシ法案のブロッキング措置については、フランス国内で批判が多くなされている。インターネット上の自由と権利の擁護を目的とする市民団体クアドラチュール・デュ・ネット[121]は、新ロプシ法案を強く批判しているが、主なその理由は、児童ポルノや有害サイトの基準が曖昧であり、多くの関係ないサイトがブロッキングされる可能性があり、また将来的には海外に設置された映画のストリーミングサイト等へブロッキング対象が拡大される恐れがあるとしている。

[121] 同団体へ我々はヒアリングを実施した。ヒアリング議事録を次部に掲載する。

第四章　ドイツ

英国およびフランスと同様、ドイツにおいても、オンライン上の児童ポルノをインターネットサービスプロバイダー（ISP）と提携して取り締まる手段の法整備が 2009 年頃より進められている。「通信ネットワークにおける児童ポルノグラフィーへのアクセス制限に係る法案」によれば、1 万人以上の契約者を持つ ISP は、ドイツ連邦警察が作成したリストに記載されたサイトへのアクセスを遮断しなくてはならない。だがこの法案に、インターネット産業団体の ECO[122]等が反対している。その理由としては、警察機関の権力が強化されすぎること、合法的なサイトへのアクセスも遮断される恐れがあることが挙げられている。

この法案はすでに 2009 年 6 月と 7 月に下院と上院を通過しているが、ドイツ大統領がこの法案を憲法違反の恐れがあるとし、署名しておらず、まだ施行されていない[123]。ドイツ大統領は法案が憲法違反に抵触する恐れがある場合、法制化プロセスを停止できる権限を有し、政府により詳しい説明を求めることができる。報道によれば、ドイツ政府は大統領のこの判断を受けて、少なくとも 1 年間は同法を施行することはないとしている。

以上のように、ISP と提携した児童ポルノサイトへのアクセス遮断に関しては、ドイツでも議論が巻き起こっている。同措置に反対する人々は ISP を介してアクセスを遮断するのではなく、違法サイトを発見し削除する従来の方法が結局のところ最善の策であると考えているようだ。

---

122 http://en.eco.de/association/about.htm
123 http://en.eco.de/association/202_6940 htm
http://en.eco.de/association/202_6831 htm
http://en.eco.de/association/202_6706 htm
http://en.eco.de/association/202_7300 htm

以上、欧州主要国における違法・有害コンテンツ規制の現状と最新動向を見てきた。欧州では段々と同コンテンツの規制が強化され、所掌警察機関等が整備されて、児童ポルノ等のコンテンツへのアクセスを遮断するブロッキング措置の法整備も、EU レベルでも国レベルでも進められている。だが、そのような傾向に反対する人々も多く、これは、主にブロッキング措置が当初の目的を超えて行き過ぎたものになる可能性があることが主な理由である。

第四部　欧州における違法ダウンロードの規制政策

ついで、欧州における違法ダウンロードの規制政策について見て行きたい。世界各国で、音楽、映画、ビデオゲームソフト等をインターネット上にアップロードしたり、海賊版を作成することは著作権侵害行為として法的処罰の対象となっており、近年来逮捕者が後を絶たない。現在、それを追うようにして、違法ダウンロードを取り締まるための法整備が各国で進められている。だが、その方法によっては、ユーザーのインターネット・アクセス権を損なう可能性があるという批判が多くある。以下に、欧州における違法ダウンロード規制政策実施動向を著作権政策とともに見ていく。

第一章　欧州連合

EU では、現在各国毎に異なる著作権法令に EU 域内で統一性を持たせることが、EU 域内市場の形成に大きく貢献すると考えられ、著作権関連の政策は、テレコム部門を所掌する情報社会とメディア総局ではなく、域内市場・サービス総局が所掌している。以下に、EU の違法ダウンロード規制に係る法整備状況および最新政策を記す[124]。

著作権指令

まず、違法ダウンロード規制とも関係の深い著作権指令について簡

[124] http://ec.europa.eu/internal_market/copyright/copyright-infso/copyright-infso_en htm http://europa.eu/rapid/pressReleasesAction.do?reference=IP/01/528&format=HTML&aged=1&language=EN&guiLanguage=en

単に触れておこう。EU では 2001 年に「情報社会における著作権およびそれに関連する権利の諸側面の調和化に係る指令」（以下、著作権指令と略す）が成立されている。この指令は、1996 年に世界知的所有権機関（World Intellectual Property Organisation : WIPO）で締結され、2000 年に発効された「著作権に関する世界知的所有権機関条約（World Intellectual Property Organization Copyright treaty）」と「実演およびレコードに関する世界知的所有権機関条約（World Intellectual Property Organization Performances and Phonograms Treaty）」を、EU 域内で法令化することを狙いとしていた。同条約では、著作権制度を新しい技術、特に情報通信技術の進歩に合わせて改正して行く必要性が認識され、様々な点が見直された。旧来のビデオテープやカセットテープによる複製とは異なり、ICT 技術の発達によって、様々なコンテンツがその質を落とすことなく、無限に複製されることが可能になり、新しい著作権法の制定が望まれていたのであった[125]。2001 年に発表された EU の社会・経済戦略であるリスボン戦略において、知識経済への移行が目標とされたが、著作権指令はそれに必要な法的手段の一つとして位置づけられていた。

[125] 同指令の主要なポイントは、著作権保護の例外および制限について係る条項（第五条）と、著作権保護のための技術的手段に係る条項（第六条）である。
第五条では、著作権保護の例外と制限規定が定められており、加盟国はそこに列挙された例外とは別の例外を設けてはならないとされた。特に情報通信技術と関係があるのは、第五条 1 で定められた「一時的複製権」、第五条 2 (b)における「私的複製権」、第五条 2(c)および 3(c)「非営利目的の複製権」である。
第五条の 1 では、ルーターやサーバー、あるいはコンピュータ端末のキャッシュメモリー等に、ISP 等の第三者が技術的な要請から一時的に情報の複製を行うことが保護の例外として定められた。
第五条の 2(b)では、商業目的ではなく、私的な目的での複製が保護の対象外として認められた。
第五条の 2(c)では、図書館、教育施設、博物館等の非営利組織による著作物の複製について、その一部が複製権の適用外とされた。
第六条はデジタルコンテンツの技術的保護手段（Technological Protection Measurs）を回避しようとする行為（第六条 1）、またそのような回避手段の流布行為（第六条 2）から権利者を保護する事を狙ったものある。

より良い規制指令

ついで、2009 年に成立した EU の電子通信規制改革パッケージにおける違法ダウンロード規制に係る法令を見ていく。同パッケージは、「BEREC 設立に係る規則」、「市民の権利指令」および「より良い規制指令」からなる。最後のより良い規制指令では、2002 年に成立した枠組指令、アクセス指令、認可指令を改正しており、改正された枠組指令第一条に違法ダウンロード規制に係る文が書き加えられた[126]。

それによれば、電子通信ネットワークへの接続する権利は、EU の定める基本権の一部とされ、それを制限する措置は司法の検証等のプロセスを経た後でなければ実施されえないとされた。

この法文の意味を理解するには、これが盛り込まれることになった過程を知る必要がある。そもそもこの条項は、2007 年 11 月に欧州委員会が電子通信パッケージ改正案を欧州議会および閣僚理事会に提出した際には存在しなかった。だが、1）フランスの映画産業団体が欧州議会でロビー活動を行い、後に詳述するような段階的処罰措置を含む規制法を同パッケージ原案を修正することによって、EU 法として成立させようとした。2）それに気づいた市民団体クアドラチュー

[126] 第一条
3）電子通信ネットワークを通じたサービスおよびアプリケーションへの最終利用者の接続および利用に関して加盟国が講ずる措置は、EU 基本権憲章および共同体法の一般原則によって保障されているように、自然人の基本権および自由を尊重するものとする。
電子通信ネットワークを通じたサービスおよびアプリケーションへの最終利用者の接続および利用に関してこれらの基本権や人権を制限するいかなる措置も、これらの措置が民主社会において適当で、相応で、必要なものである場合に限り課すことができる。また、これらの適用は、効果的な司法の検証やしかるべきプロセスを含め、EU 基本権憲章および共同体法の一般原則に従って適切な手続きに関する安全措置のもとに行われるものとする。従って、これらの措置は、推定無罪の原則およびプライバシー権に対するしかるべき尊重のもとのみで講じられる。個人または関係者がヒアリングする権利を含め、事前、公正、公平な手続きは、EU 基本権憲章に従って、緊急の場合における適当な条件および手続き調整の必要性を条件として、保証されるものとする。効果的かつ時宜に応じた司法の検証に関する権利が保証されるものとする

ル・デュ・ネット[127]が対抗してロビー活動を行い、同措置に反対する欧州議会議員[128]が原案の修正案[129]を提出し、最終的に上記の法文が付け加えられたのであった。当時、フランスではアドピ法と呼ばれる違法ダウンロード規制法が審議されており、その成立に大きな影響を与えたと考えられている。また仏報道記事によると、フランスのサルコジ大統領は、2008 年 11 月に欧州委員会委員長ジョゼ・マニュエル・バローゾに 138 修正案を撤回することを要求する通達を送っている。だが、欧州委員会が一国の利益を優遇することはできないとして却下した[130]。

アドピ法はスリーストライク措置とも言われる段階的処罰措置を含み、映画や音楽の違法ダウンロード等、著作権違法行為を行った者に対し、行政機関が勧告メールを出し、それでも停止命令に従わない場合、行政機関の判断のみで強制的にインターネットへの接続を切断することを認める法律である。問題は、この法律では司法機関の判断を仰がずに行政機関の判断のみでインターネット接続を切断することができるという点にある。もしインターネットに接続する権利を市民の基本権の一部と考えられるならば、そのような重要な権利を制限する権限を行政機関に与えることは、行政機関の権限を不当に高めることになるのではないか。よって、インターネットに接続する権利を制限する措置を実施する場合には、司法機関の判断を事前に仰ぐべきであり、こうすることにより、行政機関と司法機関の権限の均衡が保

---

127 この点に関してより詳しくは、仏市民団体クアドラチュール・デュ・ネットとのヒアリング議事録も参考のこと。

128報道によれば、フランス人のギ・ボノおよびダニエル・コーンベット欧州議会議員が欧州議会に修正案を持ち込んだとされている。

129 この修正文は 138 修正案と呼ばれている。

130

http://www numerama.com/magazine/10783-president-de-l-ue-sarkozy-exige-le-retrait-de-l-amendement-138 html
http://www numerama.com/magazine/10791-URGENT-Riposte-Graduee-Barroso-dit-non-a-Nicolas-Sarkozy.html
なお、サルコジ大統領夫人カルラ・ブリューニ氏は歌手であり、アドピ法支持者であって、大統領を後押したとも言われている。

たれうる。以上のような考えが、アドピ法への主要な批判の一つである。上記の条文により、行政機関が司法機関の判断をまたずに、ユーザーのインターネットへのアクセスを切断することは不可能になった。

だが、先に引用した条項は玉虫色のものであるという意見もある。何故なら、条文には司法機関の「検証」が必要であるとされているが、どの程度司法機関が関わるのか言及されていない上に、緊急の場合には例外的な措置が取られる可能性があるからである。実際にどのようにこの指令が解釈され実施されるのかは、各加盟国内でどのように同指令が国内法化されるのかを見て行かなければならないだろう。

知識経済における著作権通達

以上が違法ダウンロード規制に係る EU 指令であるが、その他、EU では著作権制度改革に関する政策も発表している。以下に、知識経済における著作権通達およびデジタル・アジェンダの関連政策を見て行こう。

2008 年に欧州委員会は著作権に関する公の意見聴取を行い、2009 年 10 月に「知識経済における著作権」という通達を発表している。通達では意見聴取の結果がまとめられており、特に 1）図書館と資料館によるコンテンツのデジタル化、2）権利者不明の作品の取り扱い、3）教育と研究向けのコンテンツ使用と流布、4）障害者によるコンテンツアクセスの簡便化、5）ユーザー創造コンテンツにおける著作権保護が問題とされている。以上のように、同通達では違法ダウンロードの規制ではなく、非営利組織による著作権使用制度の改革等が主なテーマとなっている。

例として、1）のトピックだけ見ていく。

1）図書館と資料館によるコンテンツのデジタル化の問題

図書館や資料館等の非営利組織と著作権を所有する出版社や著作権保持者との間で、大きく意見が分かれていることが明らかになった。

前者によれば、コンテンツをデジタル化する際に、従来の著作権システムが障害となる場合があり、図書館や資料館は著作権保護の例外となるべきである。後者によれば、現状維持でライセンス制度もしくは契約制度を保持するべきだとしている。通達で、欧州委員会はあらゆる可能性を精査し、図書館や資料館に例外規定を設ける必要があるかどうか判断するとしている。

デジタル・アジェンダ

2010 年 5 月に発表されたデジタル・アジェンダには、テレコム部門の様々な ICT 政策目標および施策が記されている。その中でも、第一に挙げられている政策は単一市場形成に係るものである。つまり、テレコム部門の EU 単一市場がまだ十分に形成されていないとし、国境を越えてコンテンツおよびサービスを利用できるように、その障害となっている規制を撤廃する政策案が同 ICT 戦略の先頭に置かれている。

さて、テレコム部門の単一市場形成に係る政策の中でも、一番に挙げられている施策が著作権制度に関わるものである。これは、著作権のライセンス付与に係るシステムが国毎に異なり、オンライン・コンテンツの欧州単一市場を形成する障害となっていることに由来する。例えば、欧州全域を対象とする音楽のオンラインショップを作るには、各国の著作権管理団体と交渉する必要があり、このような手続きの必要性は EU 単一市場形成を妨げる一要素である。よって、EU 域内で著作権管理システムをより統一したものとする必要性がある。このように、EU では著作権管理システムを簡便化し、EU 単一市場を形成することを促進する政策が策定されている。以下に、デジタル・アジェンダで示された著作権に係る目標と施策を記す。

欧州委員会の活動目標と施策
目標

著作権の使用許可、管理、国境を越えたライセンス付与を簡便化する
<u>施策</u>
● 2010 年内に集団著作権管理に関する枠組指令を提案し、オンライン上の著作権管理の統括、透明性、汎欧州規模のライセンス付与を向上させる
● 2010 年内に権利者不明の作品に関する指令を提案し、欧州の文化作品のデジタル化および頒布を簡便化する

第二章　英国

違法ダウンロードの規制政策の最新動向としては、2010 年 6 月に施行されたデジタル経済法が注目されており、以下にその概略および問題点等を記す。

2010 年デジタル経済法

成立背景および概要

2009 年 6 月、英国の ICT 政策「デジタルブリテン最終報告」が発表された後、ビジネス・イノベーション・技能省（以下 BIS と略）[131] は P2P を利用する違法ダウンロード取締について意見聴取を実施し、ついで 11 月に段階的処罰措置を含めた厳格な取締法案を「デジタル経済法案」として、その他の施策とともに公表している。最終的に、この法案は 2010 年 6 月に「2010 年デジタル経済法」として制定された。

この法令では、次章で詳述するフランスのアドピ法と同様に段階的処罰措置を採用することが定められている。この措置は、まず違法ダ

[131]英国では、著作権および著作隣接権を所掌する機関は、ビジネス・イノベーション・技能省（BIS）傘下にある知的財産庁（通称特許庁）である。

ウンロードによる著作権違反者を IP アドレスから特定し、違反を警告する通知を送り、その後違法ダウンロードを止めない者のインターネットアクセスを ISP を通して強制的に切断するものである。

デジタル経済法では、段階的処罰措置の枠組を呈示するだけに留め、警告の通知やアクセス切断の具体的な措置については情報通信庁（OFCOM）の定める規制法によって法令化されることになっている。2010 年 5 月に同庁は、措置案について意見聴取を実施しており[132]、2010 年秋には法令化される見込みである。早ければ、2011 年頭には措置案は施行され、違反者は ISP からの警告の通知を受け取ることになる。

情報通信庁の措置案によると、著作権保持者（実際には著作権管理団体）は違法ダウンロードを行っていると考えられる者の IP アドレスを収集し、それを各 ISP に伝える。そして、ISP はその IP アドレスから契約者を特定し、警告の通知を送る。次の段階に入ると、著作権管理団体は ISP から無記名の著作権違反者リストを受け取り、司法当局にそのリスト内の違反者の特定を許可する命令を要請することができる。違反行為が続けられた場合、最初の警告から一年後、BIS 省の大臣が首相および上下院の同意に基づいて、ISP に違反者のインターネットアクセスを制限する（切断も含める）技術的な措置を下すことを命令することができる。英国では、テレコム部門の独立規制機関である情報通信庁が ISP の義務を監督する。よって、フランスのように、英国では違法ダウンロード取締を所掌する行政機関を設立するわけではない。

デジタル経済法への批判

以下に簡単に 2010 年デジタル経済法が定める違法ダウンロード取締法への主な批判をまとめる。

---

[132] http://stakeholders.ofcom.org.uk/consultations/copyright-infringement/summary

IP アドレスによる違反者特定方法への批判

IP アドレスによって違反者を特定するので、契約者宅に来た友人が違法ダウンロードを行った場合、罰せられるのはその IP アドレスを持つ契約者であり、誤って取締を実施してしまう可能性がある。

情報通信庁への措置案への批判

全ての ISP に違法ダウンロード取締に係る義務が課せられるのではなく、40 万人以上の契約者を持つ ISP のみが措置案の対象となっている。よって、BT 等の大手 ISP は不満を漏らしている。

法案成立手続きへの批判

デジタル経済法案は 2009 年 11 月に公表されたが、審議途中の 2010 年 5 月に英国で総選挙が実施されることが決定した。それで、反対意見が多かったにもかかわらず、選挙前に法案を可決するために同法案の推進派が審議を早め、十分な審議がなされずに成立させたという批判がある。

以上のように、デジタル経済法は、国内での審議が不十分なまま成立した経緯があり、結局実際に措置を講じてみないとどのような問題が起こるか分からないとも言われている。

第三章　フランス

ついで、フランスにおける違法ダウンロード規制政策を概観したい。フランスではアドピ法という段階的処罰措置を含む違法ダウンロード規制法が成立され、注目を集めている。

創造とインターネット法（アドピ法）

フランスでは、2008 年 6 月に文化・通信相クリスチーヌ・アルバ

ネル（当時）[133]が、「インターネット上の創作物の普及と保護促進法案」を閣議に提出した。この法律は、違法ダウンロード（P2P によるファイル共有）を厳しく取り締まるものとして非常に注目され、フランス国内および EU においてもその是非について大きな議論を呼び、最終的に 2009 年 6 月に施行されている。

以下に、同法の概要および成立背景、今後の展望を記す。なお、同法は「創造とインターネット法」、もしくは同法が設立することを定めた「インターネット上の創作物の普及と権利保護高等規制機関（Haute Autorité pour la Diffusion des Œuvres et la Protection des droits sur Internet : HADOPI[134]）」の名前から取り、「アドピ法」と略称されている。本報告書では、アドピ法という呼称を使用する。

法案の提出背景

フランスでは、2001 年成立の EU 著作権指令の国内法化が遅れ、2006 年 6 月に「情報社会における著作権と著作隣接権に係る法（loi relative au Droit d'Auteur et aux Droits Voisins dans la Société de l'Information : DADVSI）」が下院と上院で採択され、国内法化が終了した。フランスでは、同指令の国内法化の際、違法ダウンロード取締に係る措置も一緒に法令化する予定であったが、憲法院[135]によってそれらの措置に係る条項が削除され、同法は施行された。これを受け、当時文化・通信相であったクリスチーヌ・アルバネルが、憲法院の意見と合致するような措置を策定するために、フランスの大型電化製品およびレコード販売店グループ「FNAC（フナック）」の取締デニス・

---

[133] フランスでは、文化・通信省の芸術文化創造総局が芸術作品および文学作品の著作権および著作隣接権に関する政策を所掌している。同省の諮問機関として、2001 年に「文学および芸術所有権高等評議会」がある。大学教授等の著作権の専門家、関係省、著作権管理団体、消費者保護団体、映画や本等の産業団体の代表者から構成されている。
http://www.culture.gouv.fr/culture/min/index-min.htm
http://www.culture.gouv.fr/culture/min/index-min.htm

[134] HADOPI はフランス語でアドピと発音する。

[135] フランスの憲法院は法令等が憲法に違反していないか審議し、修正する機能を持つ公共機関であり、大きな権限を持つ。

オリビエンヌに調査を命じた。オリビンヌは 2007 年 11 月に報告書を提出し、その中で、違法ダウンロード取締を所掌する機関の設立と段階的処罰措置の実施の必要性を訴えた。同月彼の提案に対し、政府および映画、音楽、テレビ関連の企業および ISP が合意し協定を結んだ。この協定がアドピ法の原案となった。

アドピ法案の策定には、フランスのレコード店および音楽、映画、テレビ等の産業団体の政治への圧力があったことを否定することはできない。同法案支持者によれば、数年来、CD や DVD の売上げが落ちており、その理由はインターネットの違法ダウンロードが原因である[136]。産業団体の圧力のもと、サルコジ大統領が同法の策定を主導したのであった。

段階的処罰措置

さて、アドピ法の要は、ファイル共有による違法ダウンロードを所掌する「アドピ」と呼ばれる行政機関の設立とそれが実施するスリーストライク措置とも言われる段階的処罰制度に法的基盤を与えることである。段階的処罰措置とは、違法ダウンロードを行う者に対して、行政機関であるアドピが法令違反を警告する通知を二回出し、それでも違法ダウンロードを止めなかった場合、違反者のインターネットへのアクセスを ISP に命じて切断するというものである。違反者は 3 ヶ月から 1 年間インターネットにアクセス不可能になる。

ユーザーは警告を受けるとブラックリストに載り、インターネットへのアクセスが遮断された後、他の ISP と契約してもインターネットは遮断されたままである。またインターネットへのアクセス遮断中も ISP に通常通り通信料金を払い続けなければならない。

違反者を同定するシステムとしては、まず著作権者を代表する著作

[136] だが、このようなデータの信用性を疑わせるデータも存在し、実際のところ、売り上げ減少と P2P ファイル共有ソフトの利用増加の相関関係が完全に証明されているわけではないようだ。また、規制法によって、ファイル共有ソフトの使用による違法ダウンロードを禁じたとしても、その後ユーザーが CD や DVD を購入するようになることを証明するデータは存在しない。この点については、クアドラチュール・デュ・ネットとのヒアリング議事録を参考のこと。

権管理団体が違反者の IP アドレスを収集し[137]、それをアドピに伝える。アドピ機関はそれらの IP アドレスの情報を ISP に伝え、ISP はその IP アドレスに関する個人情報をアドピ機関に伝え、違反者を同定する。

アドピ法原案では、違法ダウンロード行為者のインターネットアクセス切断を命じるのは新設されるアドピであるとされていたが、行政機関が司法機関の判断を仰がずに独自の判断でそれを命ずることに問題はないのかという点が後に議論の対象となった。またアドピ法実施には、民間の団体が違反行為者の IP アドレスを ISP から収集する必要があるが、このような行為の是非が個人情報の保護の観点からも議論されることになった。

アドピ法成立過程

さて、アドピ法は紆余曲折を経て成立に至っている。その過程を以下に概観する。

CNIL の意見

2008 年 6 月にアドピ法案は文化・通信相によって閣議に提出されているが、その前に、同法案は行政機関による IP アドレスの収集に関わるので、情報通信分野の個人情報保護を所掌するクニル（CNIL）において審議され、批判的な意見を受けている。同機関は、違法ダウンロード規制に関して、著作権の保護措置と個人情報保護のバランス、言い換えると著作権保護措置が行き過ぎたものにならないことを検証する自らの任務として考えている。

政府はクニルの意見を公開しないことを要請していたが、仏「ラ・トリビューヌ」紙が 2008 年 11 月にクニルの意見を掲載している[138]。そこで、クニルは新行政機関にインターネットユーザーの IP アドレ

[137]実際には同団体が収集作業を民間企業に委託する

[138] http://www.latribune.fr/entreprises/communication/telecom--internet/20081103trib000305843/loi-antipiratage-le-gouvernement-critique-par-la-cnil-.html

スにアクセスする権利を認めることは個人情報保護に抵触すると述べている。また、違法ダウンロードの普及と CD および DVD の売上げの落ち込みのあいだに、確固とした因果関係を認めることはできないという意見も提出している。

ARCEP の意見

またフランスの電気通信部門の規制機関である電子通信・郵便規制機関（ARCEP）もアドピ法案に対して反対意見を提出している。それによると、フランスではインターネットユーザーは、インターネット、固定 IP 電話、IP テレビサービスからなるトリプルプレイサービスの契約者がほとんどであり、違法ダウンロード者のインターネット接続を切断すると、固定電話サービスも使用不可能になる恐れがある。緊急時の場合も考慮して、固定電話サービスの続行を保証する必要性を ARCEP は政府に提案している[139]。また、アドピ法の実施にあたって、ISP はユーザーのインターネット接続情報を保存する必要性があり、そのための費用がかかり、ISP の負担が増加することを指摘している。

さて、以上の意見を受けて、アドピ法案は 2008 年 6 月閣議に提出され、成立まで紆余曲折を経ることになる。

2009 年 3 月下院に法案が提出され、4 月に採決を行うことが決定した。多くの与党議員（国民連合党）は法案が採択されることを見越しており、採決の際議会に居合わせなかった。それを見た野党議員（社会党）が、採決まで姿を隠し、採決を行う時間ちょうどに大勢で駆けつけた。結局反対票が多く集まり、アドピ法案は棄却されることになる。

2009 年 4 月末、与党は再度採択を目指し、法案を下院に提出した。すでに多くの議論がなされたとして、翌月 5 月には下院で採決を行っ

[139] この点については後に修正され、トリプルプレイサービスに契約している人が、アドピ法によってインターネットへの接続を遮断されても、固定電話等は切断されず、通常通り使用できるようになった。

た。今回は採択され、ついで上院でも採択される。

2009 年 6 月、下院と上院での採決の後、同法は憲法院で審議されることになり、最終的に幾つかの条項が削除された。それにより、行政機関であるアドピの権限が制限されることになった[140]。憲法院によれば、インターネットに接続する権利は憲法で保証されている「自由に表現し伝達する権利」に属し、それを制限することは司法当局にのみ可能でなければならない。よって、アドピの権限は違法ダウンロード者を見つけ、それに警告することに留まり、インターネットアクセスを切断する権限はアドピの権限のうちに入るべきではない。さもなければ、憲法に違反することになる。

このようにして、アドピ法は 2009 年 6 月憲法院によって、段階的処罰措置の部分が憲法違反に当たるとして却下されて、施行されることになった。

新アドピ法

ところで、同年 6 月末、憲法院の修正のすぐ後、アドピ法を補完するためにミシェル・アリオ・マリー法務相（現内務相）が「インターネット上の文学作品および芸術作品の所有権に係る刑法的保護法（La loi relative à la protection pénale de la propriété littéraire et artistique sur internet）」を閣議に提出している。これは、憲法院によって修正された段階的処罰措置の箇所を再修正して、法案としたものである。当初アドピ法は文化通信相が提案したものであるが、今回は違法ダウンロードの取締措置にのみ関わる法案だったので、法務相が提案し、「刑法的保護」という言葉が使用されている。なお同法は、その性質上、「アドピ 2（HADOPI2）」とも呼ばれている。

同法案は再び多くの反論を招くことが予想されたので、政府は審議を早め、2009 年 9 月に採決を行い、下院と上院で採択された。同法案では、憲法院の修正に従い、違法ダウンロード者のインターネット

140 http://www.vie-publique fr/actualite/panorama/texte-discussion/projet-loi-favorisant-diffusion-protection-creation-internet html

アクセスを切断する最終的な権限は司法当局が有するとされた。だが、司法当局の役割を最低限なものにしており、実際に司法当局と行政当局のパワーバランスが十分に取れているのか問題視する人々もいる。

2009 年 9 月末再び同法案は憲法院に付託された。2009 年 10 月に、同院は法案の大部分を妥当とし、同法は施行されることが決定された。

以上のような紆余曲折を経て、2009 年 12 月末には新機関アドピが正式に発足した[141]。

アドピ法の最新動向

さて、2010 年 10 月初旬から ISP は違法ダウンロードを行っている者に対して実際に警告メールを送り始めている。だが、仏大手 ISP のフリーは警告メールを配信することを拒否し、アドピ法の実施に反発した。だが、直ちに政府は警告メールを送信しない事業者に罰則を与える行政命令を策定し、フリーも警告メールを配信し始めた。アドピ法が今後どのような社会的影響を与えるのか注目が集まっている。

DEEZER（ディ−ザー）

以上に見てきたように、現在フランスでは音楽や映画の違法ダウンロードを取り締まる法整備を行い、取締実施段階に入った。他方で、フランスでは合法的に音楽を無料で配信するインターネットサイト「DEEZER（ディーザー）」が人気を博している[142]。以下に、ディーザーの概要を簡単に示す。

2007 年 8 月、ディーザーは合法的な無料かつ無制限のインターネット音楽配信サイトとしてフランスで設立された。著作権違反に抵触しないために、ディーザーは仏著作権管理団体（SACEM および SESAM）と協定を結び、ディーザーが得る広告収入を同団体に分配

141 http://legifrance.gouv fr/affichTexte.do;jsessionid=D46B4A842F8F25C2AD05814838C41B48.tpdjo02v_3?cidTexte=JORFTEXT000021573619&dateTexte=20100104

142 http://www.deezer.com

することにより、著作権保持者が印税収入を得ることができるようにした。

ディーザーはウェブサイト上で、オン・デマンドサービスを提供し、ユーザーは音楽のネットラジオおよびサイト内で検索した楽曲をストリーミングで聞くことができる。現在、世界中の多くのレコード会社と協定を結び、700 万曲がストリーミング可能となっている。ユーザーは無料でサイトに登録でき、それにより新たなサービスを受けることができる（ユーザーによるプレイリストの作成等）。ディーザーの収入はほとんど広告収入によるものであり、サイトに登録して音楽を聴くと数十分毎に数十秒間の音声の広告が入る。なおパソコンの I チューン等に楽曲をダウンロードすることもできるが、その場合は有料となる。2009 年 11 月には有料サービス（4.9 ユーロ/月より）も開始し、より多くのサービスを契約者は受けることができる（ハイクオリティサウンドや音声の広告が途中で入らない等）。今後、どれほど有料サービス利用者が増加するか注目が集まっている。またアップル社の I フォーン等のスマートフォンに専用のアプリケーションをダウンロードすることによって、スマートフォンでディーザーのサービスを利用することも可能である。2009 年には 1200 万人（この内 700 万人がフランスから）が同サイトに登録しているが、登録せずに音楽を聴いている人々もいるはずであり、合計でかなりの人数の人々がこのサービスを使用していると考えられる。現在ディーザーのサービスは、フランスを含め、数カ国で使用可能である。

以上のように、著作権管理団体と音楽配信サービス事業者が広告収入を共有することによって、合法的に音楽配信を実施する事業は今までの音楽産業を改変するものであり、画期的なものであると考えられている。このようなサービスは欧州では今後さらに展開されていくことが予想される。

仏違法ダウンロード規制法に係るヒアリング調査

ヒアリング議事録

以上見てきたとおり、2009 年 10 月、フランスで違法ダウンロードを取り締まるアドピ法が成立した。この法律は、ファイル共有による違法ダウンロードを段階的処罰制度によって取り締まる措置を含んでおり、主にそれが理由で成立するまでに紆余曲折を経、多くの批判を受けた。また成立後も実際にどのような社会的影響を同法が与えるのか予測できない部分があり、今後の動向に注目が集まっている。本ヒアリングでは、アドピ法を批判している市民団体「クアドラチュール・デュ・ネット」[143]から、同法の問題点およびデジタル時代の著作権制度のあり方について意見を聴取した。

日程　2010 年 10 月 25 日

場所　NICT パリ事務所

先方（○）

市民団体 クアドラチュール・デュ・ネット　（La Quadrature du net）
ジェレミー・ジメールマン（Jérémie Zimmermann）[144]
フェリックス・トレゲ（Félix Tréguer）

当方（△）

NICT パリ事務所長　　藤田　清太郎
NICT パリ事務所　　加賀　円

---

[143] 参考リンク

http://www.laquadrature net/

[144] ジメールマン氏は同団体の設立者の一人で、広報を担当している。

ONOSO 研究員　　小野　浩太郎

先方組織概要

インターネット上の市民の権利と自由の擁護を目的とする団体

- 活動理念：旧来の司法原理をデジタル環境に適用することでは、問題を解決できない。
- 主な活動：デジタル時代における表現の自由、著作権、テレコムセクター規制、プライバシー保護に関する言論・啓蒙活動および EU でのロビー活動
- 資金：個人の寄付金の他、電子フロンティア財団、オープン・社会研究院、プライバシー・インターナショナル等による財政支援

ヒアリング概要

クアドラチュール・デュ・ネットの組織と活動について

（△）あなた方の組織の概要と主な活動について教えてほしい。

（○）クアドラチュール・デュ・ネットは市民団体であり、デジタル環境において、個人の自由を行政機関による規制から保護することを目的としている。我々は同分野の規制法案等を理解するための情報や手段を市民に提供し、各人が議論に参加できるようにしたいと考えている。

同団体の設立者は 4 名で、それに 3 名加えた 7 名で現在主な業務を行っている。他に 20 数名がボランティアで我々の活動に参加しているが、短期のボランティアや電話およびメールでの情報提供者等を含めると無数の支援者がいると言える。

主な活動は、市民およびマスメディアに向けての言論および啓蒙活動、関連規制法案の分析である。以上の他、EU でロビー活動も行っており、欧州議会議員等を訪ね、我々の主張を説明している。だが、ロビー活動は我々の活動の 10%を占めるに過ぎず、また多くのロビイストがそうであるように、情報等を隠して活動することもないので、

同団体はロビー活動専門の団体ではない。

団体参加者は、主に IT エンジニアの経歴を持ち、フリーソフトウェアの制作等を行っているものが多い。我々は語源的な意味でハッカーの集まりであると言える。ハッカーという言葉は現在通信システムやサービスを破壊する者のことを指し、悪い意味で使用されることが多いが、元々はコンピューター技術に強い情熱を持ち、システムやネットワークを作る人々のことを指す言葉であったのだ。

同団体の予算は年間 12 万ユーロで、そのうちの 5 万ユーロがオープン・社会研究院等により財政支援されており、残りの 7 万ユーロは個人の寄付金である。よって、予算は基本的に同団体の活動を支持する人々からの寄付に由来する。

（△）あなた方は 2008 年に同団体を設立しているが、それはどのような機会であったのだろうか。

（○）我々は同団体を 2008 年 3 月に設立したが、それは 2007 年に実施された大統領選挙でニコラ・サルコジ氏が当選したことに由来する。同大統領が選挙期間中に発表した政策案には、すでにアドピ法のような個人の自由を侵害する恐れがある法案が含まれており、それを強く懸念して同団体を設立するに至ったのだ。

（△）あなた方は主にフランスの規制法等に対して活動を行っているのか。

（○）現在はフランスよりも、EU 関連の活動をすることが多い。また欧州の他の国にある約 15 の我々と同じような団体とも提携して活動している。

アドピ法に反対する主な動機について

（△）あなた方がアドピ法に反対する主な動機は何か。

（○）アドピ法に反対する主な動機を簡単に言うのは難しい。何故なら、反対する理由が数多くあるからである。

だが、あえて簡単に言うならば、1）この法律には個人の基本的自由を無視し、むしろそれを侵害するような措置が含まれており、また

2）この法律はいかなる適時性を持たない、つまりいかなる経済的および社会的利益をもたらさないからである。ファイル共有ソフトの使用が社会および経済的損失を与えていることを証明する信頼できるデータは存在しない。

アドピ法と表現の自由との関係について

（△）アドピ法は最終的に違法ダウンロードを行う者のインターネットへのアクセスを切断する措置を含むが、このような措置は表現の自由を制限することにならないだろうか。現在、インターネット上で情報を得ることは日常生活の一部である。

（〇）その通りである。インターネットへのアクセス切断は罰則として重すぎる。この問題については、特にフランスの憲法院が 2009 年にアドピ法原案について審議した際に、表現の自由にインターネットに接続する権利も含まれると判断した。つまり憲法院によれば、三権分立を徹底させることが必要であり、行政当局ではなく、司法当局の判断によってのみインターネットへのアクセスは切断されうるのである。憲法院のこの判断は、我々がアドピ法に対する活動の中で得た最も大きいものである。

憲法院のこの判断により、結果として、アドピ法案は段階的処罰措置に係る条項が削除されて成立した。その後、フランス政府は憲法院の判断に沿うように原案を修正し、つまりインターネット切断を決定する権限を司法当局に与えることを明記して、修正案を成立させた。この修正案は「アドピ 2」と呼ばれている。この改正により、最終的な罰則はインターネットへのアクセス制限、あるいは 1500 ユーロの罰金、もしくはアクセス制限と 1500 ユーロの罰金の両方となり、罰金刑も罰則の一つになった。

（△）あなた方は政府による法案の修正に満足しているだろうか。

（〇）いいえ、修正案は決して満足の行くものではない。何故なら、確かにインターネットへのアクセス切断を決定するのは行政機関ではなく、司法当局になったが、その司法手続きは極めて単純化された

ものになる予定であり、公正な手続きが実施されない可能性が高い。あたかも司法当局の役割は行政機関が持ってくる書類に判子を押すだけのものであるかのようだ。よって、我々は欧州人権裁判所に申し立てを行うつもりであり、我々は申し出が受け入れられると確信している。

結局のところ、アドピ法制定の目的は、司法判断を回避することにあったと言ってよい。現在まで音楽や映画等の産業団体は違法アップロードおよびダウンロードに対して訴訟を起こしてきたが、裁判には非常に費用がかかるし、訴訟結果はまちまちである。だが、アドピ法により裁判手続きを回避しようとしたのだ。

アドピ法と個人情報の保護について

（△）アドピ法が施行されるには、著作権を管理する音楽や映画の産業団体が違法ダウンロードを行う者の IP アドレスを収集する必要がある。この点について、個人情報の保護の観点から問題はないだろうか。

（〇）まず IP アドレスが個人情報として認められるかどうかという問題があるが、我々は IP アドレスを初期設定の状態のままでは個人情報としてみなしうると考えている。

ついで、フランスにおいては、音楽や映画の産業団体が IP アドレスを収集することは例外的に合法的な活動として認められている。これは同団体の政府に対するロビー活動が成功した結果である。

問題は、インターネットを監視し、違法ダウンロードを行う者の IP アドレスを実際に見つける業務を、産業団体が「TMG（Trident Media Guard）」という民間の営利組織に委託していることである。公共スペースを監視し、不正行為を見つけ、その証拠を提示する業務は普通警察機関の仕事であるから、TMG のような組織は、誤解を恐れずに言えば、民間の警察組織である。これは非常に問題である。何故なら、市民がこのような組織を管理する手段はないし、もし TMG の活動に誤りがあったとしてもそれを見つけ出す手段はない。このように、民

間組織に普通行政機関等が行う業務[145]を委託する傾向は、最近フランスにおいて顕著に見られ、我々はそれを問題視している。

アドピ法と IP アドレスについて

（△）アドピ法によれば、違法ダウンロードを行う者を特定する際の証拠はIPアドレスであると聞いたが、その点に問題はないだろうか。

（○）我々は、IP アドレスは違法ダウンロード行為の証拠としていかなる価値も持たないと考えている。

まず IP アドレスは物的証拠ではないので、訴えられた者が異議申し立てを行うことが困難である。異議申し立てを行うことが困難な法律は、すでに適切なものではないと我々は考える。

ついで、IP アドレスに基づいて違法ダウンロードを行う者を特定するので、隣人や家に来た友人が違法ダウンロードを行った場合も契約者が罰せられることになる。

そして、技術的観点から言って、他人になりすまして、他の IP アドレスを使用することは可能である。また、IP アドレスの数は限られているので、携帯電話では、一つの IP アドレスを人々が共有して使うことを可能にする技術が使用されている。この点から考えても、IP アドレスによる容疑者の特定は難しいと言える。

よって、もしアドピ法によって要請された司法手続きが単純化されたものではなく、通常のものであるならば、IP アドレスは確固とした証拠として認められることはないだろう。

アドピ法の規制対象について

（△）アドピ法では、ユー・チューブ等ストリーミング形式の動画配信サービスの視聴も規制の対象になるのか。

（○）アドピ法は、ストリーミング形式による動画配信サービスの視

[145] この民間委託の問題には、監視カメラのフィルムの管理などが例として挙げられる。

聴は取締の対象としていない。だが、ストリーミングも複製の一種であることに間違いない。実際ユー・チューブやディーザー等のストリーミングサイトから、ビデオや音楽を個人のパソコンにダウンロードすることは極めて簡単である。よって、現在のようにインターネット上における文化作品の複製取締の法整備が進むならば、ストリーミングサイトへのブロッキング[146]が法制化されるだろう。例えば、香港に拠点を持つ有名なストリーミングサイト「メガビデオ」を、フランスの警察は差し押さえることは不可能である。だが、この場合、メガビデオへのフランス人ユーザーのアクセスを遮断すればよいのだ。現在、音楽および映画産業は以上のようなブロッキング措置を政府に法制化するように働きかけており、現在ポストアドピの段階に入っている。

ところで、現在の傾向として、ピア・ツー・ピアによるファイル共有ではなく、インターネット上で映画等を直接ダウンロードしたり、ストリーミングサイトを利用する人々が増加している。だが、我々はこのような傾向は、危険なものと考えている。

ピア・ツー・ピアのファイル共有システムにおいて、我々は健全な仕方で通信ネットワークを使用する。つまり、このシステムによれば、各人はダウンロードすることができるとともに、アップロードすることもでき、各人がネットワークに参加するので、ネットワークのトラフィックのバランスが良い。他方で、ダイレクトダウンロードサイトやストリーミングサイトは、中央のシステムに視聴者が一方向的にアクセスする従来のシステムを使用している。

後者のシステムの悪い点は、エンドユーザーによるアップロードを否定し、エンドユーザーが積極的な働きを行わない点である。ネットワークへのアップロードとは、ネットワークへの個人の積極的な参加を意味するが、メガビデオやグーグルのシステムは、ピア・ツー・ピアによって中心がなくなったネットワークに新たに中央を設定する

---

[146] ブロッキングとは、違法サイト等へユーザーがアクセスできないように、アクセスを遮断する措置である。

ので、より民主的でないと言える。またアップロードは、新しいサービスの実験およびイノベーションの条件であることも忘れてはならないだろう。

また経済的な観点から言って、例えば、メガビデオのプレミアムサービスには毎月数ユーロかかるが、欧州市民がメガビデオのサービスに契約したら、ユーロが欧州圏外に流出し、欧州の ICT インフラの設備投資やサービス開発に資金が供給されなくなる。これは欧州経済にとって良くない。

アドピ法成立過程について

（△）あなた方は、アドピ法の成立を妨げるために、EU の電子通信規制パッケージ改革案（以下テレコムパッケージ案と略）の審議の際に欧州議会でロビー活動を行っていたと聞いたが、具体的にはどのようなことを行ったのか。

（〇）欧州委員会が初めに提出したテレコムパッケージ原案は評価できるものであった。だが、2008 年 5 月、我々は欧州議会におけるテレコムパッケージ案の第一読会の際に、そこに奇妙な修正が幾つか加えられているとの報告を受けた。それらの修正された法文を合わせて勘案してみると、アドピ法のような段階的処罰措置を含んだ法律がテレコムパッケージ案で提案されていることがわかった。実はフランスの映画産業団体が欧州議会でロビー活動を行っており、テレコムパッケージをフランス国内におけるファイル共有取締のために利用しようとしていたのだ。よって、我々はこれに対抗し、ロビー活動を行い、段階的処罰措置に使用されうる法文の 8 割を撤回することに成功した。我々は、インターネットのアクセス切断には司法当局の決定が必要であるという内容の法文を枠組指令の改正案に盛り込むことに成功し、これは当時フランスで審議が進んでいたアドピ法案に強い打撃を与えた。だが、改正されたユニバーサル指令の第 20 条および第 21 条には、司法当局の判断を仰がずにインターネットのアクセスを制限することを可能にするような法文があり、それを撤回することに我々

は成功しなかった。現在、以上のように、司法を回避してインターネットのアクセスを制限する措置は、「模倣品・海賊版拡散防止条約（Anti-Counterfeiting Trade Agreement : ACTA）」で審議されており、法制化される危険がある。

全体的な観点から見て、実際に成立したテレコムパッケージはあまりいいものとは言えないが、もっとひどいものになった可能性もあるのだ。

アドピ法の予算について

（△）フランス政府はアドピ法の実施に対して、どのくらい予算を用意しているのか。

（○）1200 万ユーロが税金から投入されることになるだろう。また最近インターネットサービスプロバイダー（ISP）が政府と交渉し、作業費用が補償されることに決まった。これにより ISP の負担は減ったが、さらに多くの税金が使われることになる。

アドピ法に対する市民の反応と実際の効果について

（△）アドピ法は実施段階に入ったが、この法律に対する市民の反応はどのようなものだろうか。

（○）アドピ法の施行によりすでに警告通知をメールで受け取った人々がいる。彼らの話を聞くと、その通知を受けても技術的に細工を施してファイル共有を今後も続けるという人もいれば、一切止めてしまった人々もいる。大事なことは、ファイル共有を止めた人が CD や DVD を購入するようになるかというと、それを証明するものは何もないということである。

結局のところ、フランス政府には最終的にインターネットアクセスを切断するという罰則を本当に実行する意図はない可能性もある。もし実行すれば、逆に我々が先に説明した理由から、欧州人権裁判所によりこの法律自体が無効にされる可能性がある。むしろ、アドピ法とは一種のかかしのようなものであり、政府は市民を脅してファイル共

有を止めさせることを狙っている可能性が高い。

アドピ法に対するインターネットプロバイダーの反応について

（△）アドピ法に対する ISP の反応はどのようなものか。

（○）フランスには約 2000 の ISP[147]がいるが、どれも命令を受け、アドピ法の段階的処罰措置に参加することになる。大手 ISP のフリーは当初、顧客に警告通知メールを送るのを拒否していたが、フランス政府は、フリーのように警告メールの配信を拒否する ISP に罰則を与える行政命令をすぐに策定した。これにより、フリーも通知メールを送り始めた。

（△）フランス政府は、フリーのように警告メールを送信することを拒否する ISP が出てくることを予想していなかったのか。

（○）そのような予想はしていなかったであろう。だがフリーは単に自分の存在感を示すためだけに、警告メールを送ることを拒否した可能性がある。いずれにせよ、このような事態はいかにアドピ法が不完全なものかを示す要素の一つである。

デジタル時代の著作権のあり方について

（△）もしアドピ法のような規制法に問題があるとするならば、デジタル環境においてどのように著作権を保護すればよいのだろうか。

（○）この問題はアドピ法の是非を超えて、法哲学的な射程を持つと言えるだろう。

著作権について考える上で、最も大事なことは作者（アーティスト、作家等）と製造業者（産業界[148]）と市民（作品の受取り手）のバランスである。現在、このバランスは完全に崩れている。何故なら、著作

---

147 ここで、ISP とは、自分でインフラを持たないサービスプロバイダーおよび大中小規模の全ての事業者を含む。2000 という数字は仏電気通信・郵便部門の規制機関である「アルセップ（ARCEP）」に登録している事業者数である。

148 製造業者とはここで、具体的にはレコード会社や CD 等を売る販売店を指す。

権法は製造業者の利益を追求するばかりで、文化作品にアクセスする市民の権利を完全に無視しているからである。

少し前の時代までは、製造業者の利益を保護することは非常に重要であった。何故なら、文化作品を複製するには非常に費用がかかり、多大な投資が必要であったからである。だが、現在作品の複製にはほとんど費用がかからない。そもそもインターネットのシステムは巨大な複製システムであるとも言える。インターネット上のサーバ、各パソコン、携帯端末等で複製は随時行われ、それには費用はかからない。つまり、以前は文化作品の複製は一定の事業者にしか不可能であったのだが、現在は技術の進歩により、複製には費用がかからず、インターネットユーザー全員にとって可能であり、すなわち、みなが簡単に文化作品にアクセスできる。これは技術の進歩に基づく人類の進歩と言えるだろう。

また、現在 MP3 の端末で音楽を聞く 15 歳くらいの子供（未成年）は、著作権に関して全くどうでもいいと思っており、現状はこのようなものなのだ。

よって、デジタル時代の著作権保護政策には、まず技術の進展およびその使用方法の現状を理解し、それを考慮に入れなくてはならないだろう。法律上、すでに文化作品の複製は、私的使用、パロディ、教育現場での使用という条件で例外的に認められている。よって、非営利目的でのファイル共有は正当なものであり、それは許可されるべきだと法典に明記されるべきである。

（△）著作権制度において製造業者の利益が追求されているとは、音楽や映画等の産業界が作者と市民の間で、正当な取り分以上の利益を得ているということだろうか。

（〇）そうだ。1980 年代は彼らのいい分は正しかった。何故なら、音楽の CD を作成し、販売するには、録音費や宣伝費等が非常にかかったのだ。だが、現在は大幅により少ない費用で済む。言い換えれば、技術の発達によって製造業者の役割は大きく縮小したのである。

デジタル時代の新しい経済モデルについて

（△）技術の進歩により産業界の役割が縮小したならば、新しい経済モデルやビジネスモデルが必要になるのではないか。

（〇）そうだ。新しい複製技術が登場した時、作者に正当な報酬を与えるシステムを新たに作る必要がある。複製技術の歴史を見てみよう。レコード、ラジオ、カセットテープが登場したとき、音楽が失われると心配した人がいたが、そうはならなかった。ラジオ放送やカセットテープには課金され、それにより作者への報酬が間接的に保護されたのであった。アドピ法の賛同者はこのような考えを持つことができず、旧来の思考システムにとらわれたままである。

より具体的に言って、デジタル時代の新しい著作権保護の経済モデルとしては、まず作者が産業界に渡す最初の複製物の利益を絶対的に保護し、可能な限り、作者の報酬や産業界の利益が作品の売り上げ数に依存しないようにすべきである。

このためには、ICT 製品やインターネットや携帯電話の通信料金に課金し、その収入が産業界および作者へ行くようにする。このような経済モデルの促進を、我々の団体の設立者の一人であるフィリップ・エグランは著書で説いている[149]。

また、技術の進歩によって、ジャケットとして紙が一枚入った普通の音楽 CD を販売することは現在価値をもたなくなっている。だが、CD にアーティストのサインやポスター等をつけて、付加価値を持たせて販売することには常に大きな価値があるだろう。ただの CD は販売用ではなく、プロモーション等に使用するべきである。ディーザー等のストリーミングサイトのプレミアムサービスも付加価値を持ち、ユーザーはサービス料金を支払う価値がある。また音楽を販売しているアップル社の I チューンは、人々が音楽を探す手間を省き、様々な端末で利用できるので、これはこれで付加価値があると言えるだろう。I チューンは単に複製された音楽を販売しているわけではないのであ

[149] 参考
http://paigrain.debatpublic net/?page_id=171

る。要するに、今までのようにCDの売り上げだけに、収益源を見てはいけない。

異なる観点から言えば、インターネットの発展により、現在アーティストは産業界から独立して宣伝や楽曲の販売が可能な状態にあるが、レコード会社との契約によってそれが不可能である。新しい経済モデルは、現在のようにレコード会社がアーティストと視聴者である市民との間に入る必要性を縮小するであろう。

我々はこのような新しい経済モデルを実現しないかぎり、著作権法を巡る争いはなくならず、アドピ法のような法律を登場させるだけであると考えている。実際すでにレコード会社を通さず、インターネット上でプロモーション活動を行い、作品を作り続けているアーティストもおり、経済モデルは現在変わりつつあるのである。

（△）産業界は、その役割が縮小されているものの、その権益を維持したがっているということだろうか。

（○）そうだ。だが、それは理解不可能なことではないだろう。著作権政策を立案する際に、政府は音楽や映画の産業界の利益ばかり考えるのではなく、技術の発展に合わせて、個人の自由の保護も含めた社会全体の利益を考えなければならない。その際には、ICTに関わる多くの事業者に課金する等の新たな措置を考える必要がある。

違法ダウンロードとCDやDVDの売り上げ減少の関係について

（△）違法ダウンロードによって、レコード販売店等の売り上げが減少したと言われている。この関係についてはどのようにお考えか。

（○）実は、ファイル共有ソフトの使用とCDやDVDの売り上げ減少に相関関係はないという信頼できる研究が数多くある。これらの研究は米国会計検査院、カナダ政府、オランダ政府や多くの大学研究機関によって発表されたものであり、我々のウェブサイト[150]から入手できる。逆に、音楽産業界等のアドピ法推進者が提示するデータは信頼

[150] http://www.laquadrature.net/wiki/Documents

できるものとは言えない。アドピ法推進者にデータを提供する研究者の方法論はひどいものであるし、しばしばそれらの研究機関は音楽や映画の産業界によって資金を提供されている。なおアドピ法案成立のためにフランス政府にデータを提供したのは、テラ・コンシュルタン[151]であるが、この企業が分析するデータの 80%は産業界から提供されたものであり、中立的なものではないと言える。

欧州の著作権制度の現状について

（△）欧州委員会は違法ダウンロード取締についてどのような立場を取っているのか。アドピ法に賛成しているのか。

（○）欧州委員会は一度だけ、インターネットのアクセス制限は司法当局の判断を仰がなくてはならないと述べたことがある。だが、欧州委員会は、フランス国内のアドピ法の問題に直接介入することはできない。言い換えると、アドピ法が要請する司法手続きが非常に単純化されたものであるとか、民間企業が警察機関のような業務を行っているとか、我々が先に触れた問題は欧州委員会の管轄に入らない。これらの問題はむしろ欧州人権裁判所が取り扱う問題である。

だが、欧州委員会の著作権政策の傾向は、非常に懸念すべきものである。近年来、アドピ法のような措置やブロッキング措置を含む政策を立案する傾向があり、現在は先ほど述べた ACTA に同様の措置を盛り込むことが審議されている。また現在の欧州委員会で著作権政策を所掌する単一市場総局の欧州委員会委員は、フランス出身であり、サルコジ大統領に近いミシェル・バルニエ氏であることを忘れてはいけない。

（△）他の欧州諸国で段階的処罰措置を含む規制法を施行している国はあるか。ドイツは実施に反対していると聞いたが。

（○）フランスと英国以外では、まだアドピ法のような法律は成立していない。ドイツ、スウェーデン、イタリアは同法の制定を拒絶して

[151] http://www.teraconsultants.fr/fr/Accueil.html

いる。懸念されるべきは、一つの国で法律が施行されると他国が同法を国内で提案する際に、提案の根拠となるモデル例として取り上げる可能性があることである。

今後の活動予定について

（△）あなた方の今後の活動について教えてほしい。

（〇）まず、ブロッキング措置法案を撤回させることが今後の活動の一つとしてあげられる。現在フランスでは、インターネットサイトのブロッキング措置を含む法令が準備されている。すでにオンラインゲームに関しては、ブロッキング措置が実行されており、現在児童ポルノサイトへのブロッキング措置を講じる「ロプシ法案」が近く成立しそうだ。我々の考えでは、児童ポルノサイトへのブロッキング措置は将来的には、その対象を文化作品の複製に広げ、アドピ法と合わせて講じられるだろう[152]。このような取締政策はフランスだけでなく、欧州全体で実施される傾向にある。フランスでロビー活動をしている人々は、EU でロビー活動している人々と全く同一の団体である。よって、フランスにおいても、EU レベルでも同じような政策が取り上げられるのである。

以上の他、特に現在 ACTA の問題に力を入れている。これは薬や高級ブランド品等を含めた模造品および海賊版製品を取り締まるための多国間協定である。EU 、アメリカ、日本等 13 カ国が協議に参加しており、我々は特に上記三者が主導していると聞いている。ここでは、アドピ法のように、司法当局の判断を仰がすに、産業界と ISP を提携させてファイル共有ソフトを取り締まる措置についても協議されている。我々がすでに述べたようにアドピ法のような法律は表現の自由を侵害する恐れがあるのだから、公に民主的にその是非が議論されな

[152] これは、アドピ法のような段階的処罰措置により、国内のインターネットユーザーのファイル共有を取り締まり、ブロッキング措置によって、海外に設置されたサイトへのユーザーのアクセスを遮断するという二重の規制を意味する。

ければならないが、ACTA は三年前に協議が開始されているものの、全くその協議プロセスが公にされず、秘密裏に各国の所管省庁によって交渉されている。我々が入手した情報によれば、現在すでに協議はほとんど終了段階にあり、一度協定に署名されたら、参加国で国内法化プロセスが始まるだろう。欧州ではまず、欧州議会で協定の承認手続きがあり、その後、各国で国内法化が始まるだろう。また、この協定には、中国、ブラジル、ロシア、インド等の模造品を多く産出している国が参加しておらず、実際の効果は疑わしいということを付け加えておこう。

第四章　ドイツ

ドイツ[153]では 2005 年一年間に推定 4 億ファイル（そのうち 2000 万ファイルが映画）が違法にダウンロードされたと言われており、欧州で最も違法ダウンロードが行われている国の一つである。このような状況を受け、ドイツの音楽産業団体などが違法ダウンロードの厳罰化を要求し、2008 年にドイツでは著作権法が改正された。これにより、違法な複製物の使用が疑われる供給源からの著作物およびファイルのダウンロードが違法とされた。

だが、段階的処罰措置を含む法律が整備される英国、フランスとは異なり、ドイツでは同法の整備について、ドイツの音楽産業団体は導入を要求しているものの、現在までのところドイツ連邦政府は同法の導入を考えていないようだ。2010 年 6 月に連邦法務相ザビーネ・ロイトホイザー＝シュナレンベルガーは科学・人文学アカデミーで著作権について講演した際には、明瞭にフランスのアドピ法を批判している。その理由としては、同法による最終的なインターネットアクセス

[153] ドイツでは、「ドイツ特許商標庁(Deutsches Patent und Markenamt : DPMA)」が著作権行政を所掌している。
http://www.dpma.de/english/index.html

切断措置を、ユーザーからインターネットに自由にアクセスする権利を奪う過度な措置であること、また違法ダウンロードを行っていないものが罰せられる可能性があることを挙げている[154]。なお講演では、最終的なインターネットアクセス切断には批判的であるものの、違法ダウンロードを行うものへ警告通知を送る措置の有効性について明確な規則を設ける必要性については述べられている。

ドイツでは、「ディジライツ・ソリューション」等の民間企業が、P2P ネットワークのインターネット上のフォーラム（Gnutella, eMule, Kademia, BitTorrent 等）を監視するソフトウェアを使用して、著作権侵害となるダウンロード行為を記録しており、それらの情報は裁判に利用されている[155]。報道によれば、先に述べたディジライツ・ソリューションは月に 5000 人の違法ダウンロードを行うユーザーを特定した。

以上、欧州における違法ダウンロード規制政策の動向を見てきた。英国およびフランスで、多くの反発を呼びながら段階的処罰措置を含む規制法が整備されたことが注目される。市民団体クアドラチュール・デュ・ネットとのヒアリング議事録を見れば、仏アドピ法への批判点はかなり明確にわかるだろう。だが、同市民団体が提案する新しい経済モデルの有効性については未知数であるとも言える。今後、単に違法ダウンロードを規制する法制度の整備だけでなく、新しい経済モデルを構想することが必要とされるだろう。

---

[154] http://www.bmj.bund.de/enid/631091a041eddcfd5ad918d56fb85d81,014fa3706d635f6964092d0937303330093a0979656172092d0932303130093a096d6f6e7468092d093036093a095f7472636964092d0937303330/Speeches/Sabine_Leutheusser-Schnarrenberger_1n8.html
http://www.ecrans.fr/L-Allemagne-n-aura-pas-son-Hadopi,10167 html

[155] http://drs-software.com/home.php
http://www.zdnet.fr/actualites/telechargement-illegal-le-bon-filon-en-allemagne-pour-les-societes-de-lutte-contre-le-piratage-39709109 htm

第五部　欧州におけるサイバーセキュリティ部門の市場動向および研究開発支援の現状

最後に、欧州におけるサイバーセキュリティ部門の市場動向および研究開発の現状および研究事例を見ていく。まず、EU が発表した報告書に基づいて、EU 加盟国の同部門の市場動向を概観し、その後、EU の第七次枠組計画における研究開発支援動向、ついで欧州主要国（英独仏）における研究開発組織および研究プロジェクトを示す。

第一章　EU 加盟国の ICT セキュリティ部門の市場動向

EU は 2009 年 4 月に「欧州ネットワーク・情報セキュリティ市場報告書 —シナリオ、傾向、挑戦—」[156]を発表している。以上に基づいて、EU の市場動向を記す。

世界の中の EU

2005 年から 2007 年まで、世界規模で ICT セキュリティ市場は拡大を続けている。2007 年の時点で、EU 加盟国 27 カ国を合わせた ICT セキュリティ部門の市場[157]は日本および APEC（アジア太平洋地域諸国）[158]を超えて、アメリカにつぎ世界第二位を占める（図版 4 参考）。

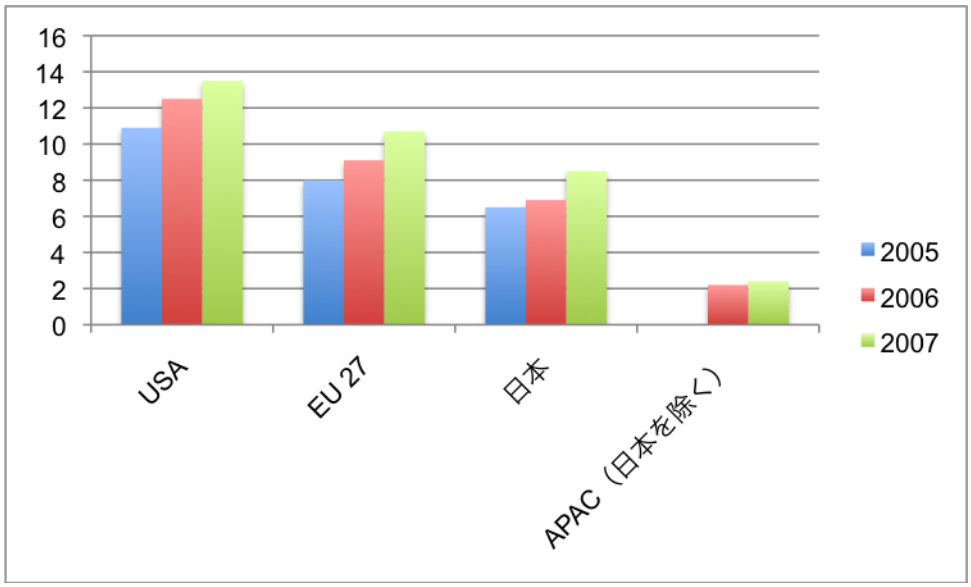
---

156 http://ec.europa.eu/information_society/policy/nis/strategy/activities/data_ict_market/index_en htm

157 ここで、ICT セキュリティ部門の市場は、企業および消費者による ICT セキュリティ関連のソフトウェア、サービス、ハードウェアの支出額によって規定される。

158 ここでは、日本を除く、オーストラリア、韓国、シンガポール、ニュージーラ

図版 4　2005−2007 年における世界の ICT セキュリティ市場動向（縦軸は 10 億ユーロが単位）



	2005	2006	2007
USA	10.9	12.5	13.5
EU 27	8	9.1	10.7
日本	6.5	6.9	8.5
APAC（日本を除く）		2.2	2.4

（数字は 10 億ユーロ単位）

出典　EU

以上から、各 EU 加盟国の市場は大きなものではないものの、27 カ国を合わせれば、ICT セキュリティの巨大な一つの市場を形成しうることがわかる。ICT セキュリティ部門だけでなく、一般的に言って、EU の経済政策は上記のような潜在性を秘めた単一市場を現実のものとすることを目指していると言えるだろう。また逆に言えば、アメリ

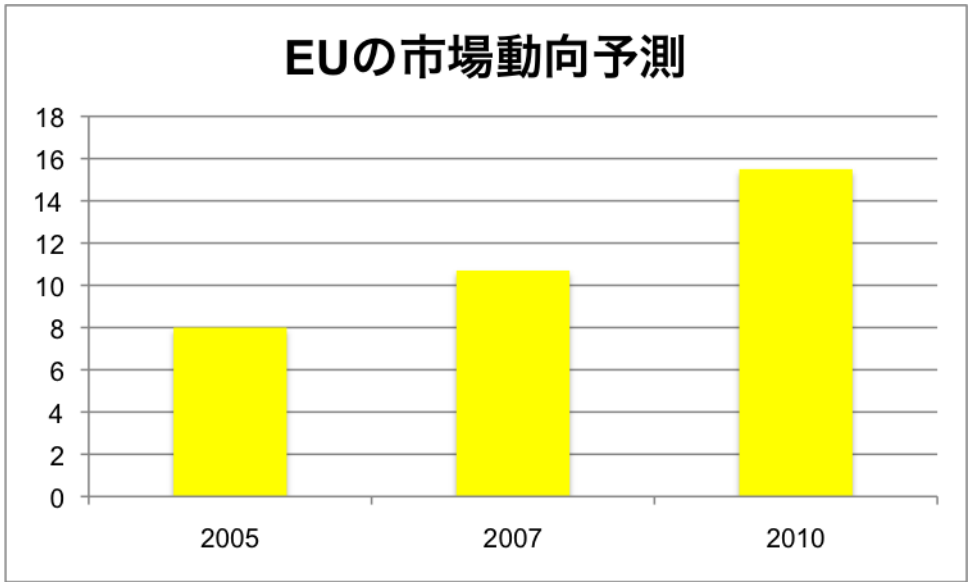
ンド、香港、インド、中国が調査対象である。

カと日本の ICT セキュリティ市場が他国と比べて、突出して大きいことわかる。

EU 市場の動向

ICT セキュリティ部門の EU 市場は、2010 年には 150 億 5000 万ユーロにまで拡大する見通しである（図版 5 参考）。2008 年から 2009 年にかけて、世界的な経済危機の影響で市場の拡大傾向は縮小したが、2010 年には勢いを取り戻すことが予測されている。2007 年から 2010 年にかけて 13.1%の成長が見込まれている。また、欧州の ICT 企業はその予算の 10%を ICT セキュリティにかけている。

図版 5　EU の ICT セキュリティ部門の市場動向予測



（単位は 10 億ユーロ）

出典　EU

4 つのグループ

また同報告書では、欧州 27 カ国を ICT セキュリティ部門への支出額に応じて、下記のように四つのグループに分け、市場動向を簡単に解説している（図版 6 参考）。

図版 6

第一グループ	第二グループ	第三グループ	第四グループ
デンマーク	オーストリア	キプロス	ブルガリア
フィンランド	ベルギー	チェコ共和国	エストニア
オランダ	ルクセンブルグ	ハンガリー	ラトヴィア
スェーデン	フランス	ギリシア	リトアニア
英国	ドイツ	イタリア	マルタ
	アイルランド	ポルトガル	ポーランド
		スロベニア	ルーマニア
		スペイン	スロバキア

出典　EU

第一グループ

このグループは北欧諸国とオランダと英国からなり、2007 年の ICT セキュリティ市場の全収入は 40 億ユーロを超え、EU 全市場の 38%に値する。また 2007 年から 2010 年にかけて、12.8%の成長が見込まれている。これは EU 全体の成長率を下回り、これらの国の市場が十分に成熟していることに由来する。

第二グループ

このグループには欧州の主要な大陸国とアイルランドが含まれる。これらの国は ICT 部門全体の観点から見れば、第一グループとほぼ同程度発展しており、欧州 ICT セキュリティ市場の全収入の 44%（47 億ユーロ）を占める。2007 年から 2010 年にかけての ICT セキュリティ市場の成長率は 13.1%で EU 全体の市場と同率である。

第三グループ

第三グループは南欧諸国と東欧数国から構成される。このグループの 2007 年の全収入は 17 億ユーロで、EU 全体の 16%を占める。2007 年から 2010 年にかけての市場成長率は 13.5%で、EU 全体の平均を上

回り、第一グループおよび第二グループを少しずつ追い上げている。

第四グループ

最後のグループはEU新加盟国からなる。ICTセキュリティ市場の収入はEU全体の市場の2%を占めるにすぎない。同グループでは、ICT全体の発展が他のグループに比べ遅れているが、市場の成長率は高い。2007年から2010年にかけてのICTセキュリティ市場の成長率は17.2%であることが見込まれている。

以上のように、欧州におけるICTセキュリティ部門の市場は拡大傾向にあり、EU全加盟国を合わせた市場規模は非常に大きい。そして、欧州のICT先進国ほど同部門の市場規模は大きく、EU新加盟国の市場規模は小さいが成長率は高い。

第二章　欧州連合の研究開発支援および研究プロジェクト事例

ついで、EUの研究開発支援助成プログラムである「第七次枠組計画」（以下FP7と略す）における同部門の公募動向および公募で採用された研究プロジェクトを記す[159]。

第一節 第七次枠組計画作業プログラムにおけるサイバーセキュリティ分野の位置づけおよび予算規模

本節では、FP7におけるサイバーセキュリティ分野の研究開発助成動向を記す。

[159]第七次枠組計画は2007年から2013年を期限とするEUの研究開発助成スキームの一つであり、公募を通して支援を行っている。以下のサイトを参考のこと。
http://cordis.europa.eu/fp7/ict/

ICT 部門研究開発助成作業プログラムにおけるセキュリティ分野の位置づけ

FP7 の ICT 部門全体の予算は 2007 年から 2013 年までの間、91 億ユーロが見込まれており、他の部門に比べて最大額が割り当てられている。これは EU の ICT 部門への関心の高さを示していえるだろう。

ICT 部門の研究開発助成は、欧州委員会の情報社会・メディア総局の管轄に入る。二年ごとに作業プログラムが策定され、そこには公募の方向性、テーマ別優先順位、助成額等が記されている。現在まで、2007 年～2008 年度作業プログラム（以下 WP07-08 と略す）、2009 年～2010 年度作業プログラム（WP09-10）、2011 年～2012 年度作業プログラム（WP11-12）が発表され、実際に公募が行われている[160]。

各作業プログラムで、ICT セキュリティ関連の公募は*「課題 1：普及し、信頼されたネットワークとサービス・インフラストラクチュアー」*に組み込まれている。なお WP07-08 においては ICT 部門とセキュリティ部門の合同公募[161]も実施されていた。

以下に、WP07-08、WP09-10、WP11-12 の「課題 1」のテーマおよび助成額の表を示す。

WP07-08

課題 1	予算額
1. 未来のネットワーク	2 億ユーロ
2. サービスとソフトウェア．アーキテクチャ、インフラストラクチュア、設計	1 億 2000 万ユーロ

[160] ftp://ftp.cordis.europa.eu/pub/fp7/ict/docs/ict-wp-2007-08_en.pdf
ftp://ftp.cordis.europa.eu/pub/fp7/ict/docs/ict-wp-2009-10_en.pdf
ftp://ftp.cordis.europa.eu/pub/fp7/ict/docs/ict-wp-2011-12_en.pdf
本報告書では 2010 年 10 月に発表されている WP11-12 について記すが、暫時内容が変更する可能性もある。

[161] ICT 部門とセキュリティ部門の合同公募において、ICT テーマには 2000 万ユーロが助成された。

3. ネットワーク化された企業のための情報通信技術	9000 万ユーロ
4. 安全で、依存できる信頼されたインフラストラクチュア	9000 万ユーロ
5. ネットワーク型メディア	8500 万ユーロ
6. 新パラダイムと実験施設	4000 万ユーロ
7. 重要インフラ防護	2000 万ユーロ（共同公募）

WP09-10

課題 1	予算額
1. 未来のネットワーク	1 億 8000 万ユーロ
2. インターネットサービス、ソフトウェア、仮想化	1 億 1000 万ユーロ
3. モノのインターネットと企業環境	5500 万ユーロ
4. 信頼できる ICT	9000 万ユーロ
5. ネットワーク化されたメディアと 3D インターネット	8000 万ユーロ
6. 未来のインターネット実験施設および実験研究	5000 万ユーロ

WP11-12

課題 1	予算額
1. 未来のネットワーク	1 億 6000 万ユーロ
2. クラウド・コンピューティング、インターネット・サービス、最新ソフトウェア工学	7000 万ユーロ
3. インターネット接続オブジェクト	3000 万ユーロ
4. 信頼できる ICT	8000 万ユーロ
5. ネットワーク・メディアと検索シ	7000 万ユーロ

ステム	
6. 未来のインターネット研究と実験	4500 万ユーロ

以上を見ればわかる通り、「課題 1」においては、未来のネットワークおよびサービス・ソフトウェアに関する研究開発に最も資金が供給され、続いて ICT セキュリティおよびメディア分野が位置づく。

参考のため、各作業プログラムにおける ICT セキュリティ部門への助成額を抜き出して示す。

- WP07-08 :「安全で、依存できる信頼されたインフラストラクチュア」: 9000 万ユーロ
- WP09-10 :「信頼できる ICT」: 9000 万ユーロ
- WP11-12 :「信頼できる ICT」: 8000 万ユーロ

WP11-12 において、予算額が少し減らされているが、おおよその規模は変化していない。

WP11-12 における「信頼できる ICT」の概要

以下に、ICT セキュリティ分野の最新研究開発助成動向を示すために、WP11-12 の公募テーマ「信頼できる ICT」の概要を記す。

なお、ここで「信頼できる ICT（Trustworthy ICT）」とは、次のような意味を持つ。

1）サイバー攻撃および操作ミスに対して安全で、信頼性が高く、回復が早い

2）サービスの質が保証されている

3）ユーザー情報を保護する

4）プライバシーを強化するとともに、ユーザーによる危機管理をサポートする実用的で信頼されたツールを提供する

以上のように、信頼できる ICT は複数の意味を持ち、サイバーセキュリティの多様な側面をカバーするテーマである。

目標

同テーマの最終目標は、人間および社会の価値と文化を尊重しつつ、信頼できる情報社会を建設することである。このテーマで採用される研究プロジェクトは、司法、社会、経済に係る研究と提携し、社会的に受け入れられ、経済的に問題のない実用的なセキュリティシステムを開発するものでなければならない。

予算規模

8000 万ユーロ

公募開始および締め切り時期

2011 年 7 月 26 日～2012 年 1 月 17 日（公募 8[162]）

主要優先事項

以上の目標を達成するために、次のトピックが公募の優先事項として挙げられている。

a)多様なネットワークによって結ばれたサービス・コンピューティング環境

1. スケラビリティおよびインターオペラビリティを実現するネットワーク・アーキテクチャおよびプロトコル
2. 複数のアクセス網と接続する多様なインターネット
3. 仮想化技術
4. 定量的セキュリティ
5. 宣言型言語・バイオメトリー・認証および暗号技術

b) 信頼・E アイデンティティ・プライバシー管理インフラストラクチュア

1. 信頼性を管理・査定するためのアーキテクチャ、プロトコ

[162] FP7 における公募時期はテーマによって異なる。WP07-08 では公募 1、2、3、WP09-10 では公募 4、5、6 が実施された。WP11-12 では公募 7、8、9 が行われる。公募 7 は 2010 年 9 月 28 日～2011 年 1 月 18 日、公募 8 は 2011 年 7 月 26 日～2012 年 1 月 17 日、公募 9 は 2012 年 1 月 18 日～2012 年 4 月 17 日にかけて実施される予定である。

ル、モデル、サービスおよびデバイス

2. 複数の ID とプライバシー保証の検証ツールを実現するプライバシー・インフラストラクチュア向けプロトコル

3. インターオペラブルな ID 要請の管理および多重認証デバイスの技術と標準化

c) データポリシー・ガバナンス・社会経済エコシステム

1. データガバナンスおよびその実施手段のための管理・ガバナンス枠組み

2. 複数のステークホルダー間で実施される多極化されたガバナンスとセキュリティに対する取り組み

d) ネットワーク作り・提携活動

セキュリティ関連の研究開発の成果を普及させる活動を支援する。特に、ICT 部門と法学および社会経済科学との提携、技術標準および最適な実践の普及、国ごとの研究開発の提携を支援する。

以上のように、優先事項に関しては、通信環境セキュリティを向上させるための個々の技術研究開発、セキュリティ管理および査定のためのアーキテクチャおよびツールの研究開発、データ管理および複数のステークホルダー間におけるセキュリティ共同管理に係る研究開発、法学、社会経済科学との提携を推進する活動および共通の技術標準や実践を普及する活動が支援される予定である。

第二節　第七次枠組計画における研究開発プロジェクト事例

ついで、FP7 において実際に採用された研究プロジェクトを見ていきたい[163]。すでに WP07-08 および WP09-10 の公募は締め切られ、実

[163] http://cordis.europa.eu/fp7/projects_en.html

際に研究開発は進められており、すでに終了したプロジェクトもある。

まず、以下に WP07-08 および WP09-10 の「課題 1」において採用された研究プロジェクト数を示す。

WP07-08「課題 1」における採用プロジェクト数

課題 1 のテーマ	採用プロジェクト数
1. 未来のネットワーク	46
2. サービスとソフトウェア．アーキテクチャ、インフラストラクチュア、設計	27
3. ネットワーク化された企業のための情報通信技術	10
4. 安全で、依存できる信頼されたインフラストラクチュア	24
5. ネットワーク型メディア	20
6. 新パラダイムと実験施設	14
7. 重要インフラ防護	9

WP09-010「課題 1」における採用プロジェクト数

課題 1 のテーマ	採用プロジェクト数
1. 未来のネットワーク	42
2. インターネットサービス、ソフトウェア、仮想化	22
3. モノのインターネットと企業環境	1
4. 信頼できる ICT	22
5. ネットワーク化されたメディアと 3D インターネット	9
6. 未来のインターネット実験施設および実験研究	14

ついで、次ページより、WP07-08 および WP09-10 において採用された研究プロジェクトの一覧表を示す。

WP07-08 の「安全で、依存できる信頼されたインフラストラクチュア」で採用された研究プロジェクト一覧

	プロジェクト名と略称	期間	全予算/FP7 拠出分	参加者名およびその国名
1	Detecting known security vulnerabilities from within design and development tools (SHIELDS)	2008/1/1-20 10/6/30	443 万ユーロ /325 万ユーロ	MONTIMAGE EURL（仏）、TXT E-SOLUTIONS SPA（伊）、FUNDACION EUROPEAN SOFTWARE INSTITUTE（西）、GROUPE DES ECOLES DES TELECOMMUNICATIONS（仏）、FRAUNHOFER-GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V（独）、STIFTELSEN SINTEF（ノルウェイ）、SEARCH-LAB SECURITY EVALUATION ANALYSIS AND RESEARCH LABORATORY, LTD（ハンガリー）
2	Think tank for converging technical and non-technical consumer needs in ICT trust, security and dependability (THINKTRUST)	2008/1/1-20 10/6/30	57 万 9999 ユーロ/58 万ユーロ	TELSCOM CONSULTING GMBH（スイス）、GROUPE DES ECOLES DES TELECOMMUNICATIONS（仏）、Technische Universitaet Darmstadt（独）

3	Privacy-aware Secure Monitoring (PRISM)	2008/3/1-2010/5/30	316 万ユーロ/230 万ユーロ	NETTARE S.R.L.（伊）、INSTITUTE OF COMMUNICATION AND COMPUTER SYSTEMS（ギリシア）、FTW FORSCHUNGSZENTRUM TELEKOMMUNIKATION WIEN BETRIEBS-GMBH（オーストリア）、CONSORZIO NAZIONALE INTERUNIVERSITARIO PER LE TELECOMUNICAZIONI（伊）、HITACHI EUROPE SAS（仏）、SALZBURG RESEARCH FORSCHUNGSGESELLSCHAFT M.B.H.（オーストリア）、FRAUNHOFER-GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V（独）
4	Genetic message oriented secure middleware (GEMOM)	2008/1/1-2010/6/30	461 万ユーロ/330 万ユーロ	DATEL CONSULTING INTERNATIONAL LTD（愛）、Q-SPHERE LIMITED UNITED（英）、DIGINUS LTD UNITED（英）、VALTION TEKNILLINEN TUTKIMUSKESKUS（フィンランド）、QUEEN MARY AND WESTFIELD

				COLLEGE, UNIVERSITY OF LONDON UNITED（英）、HEWLETT PACKARD ITALIANA SRL（伊）、JRC CAPITAL MANAGEMENT CONSULTANCY & RESEARCH GMBH（独）、NORSK REGNESENTRAL（ノルウェイ）、TXT E-SOLUTIONS SPA（伊）
5	International co-operation in trustworthy, secure and dependable ICT infrastructures (INCO-TRUST)	2008/1/1-2010/6/30	83 万ユーロ/83 万ユーロ	ATOS ORIGIN SOCIEDAD ANONIMA ESPANOLA（西）、GROUPE DES ECOLES DES TELECOMMUNICATIONS（仏）、Technische Universitaet Darmstadt（独）
6	Secure widespread identities for federated Telecommunications (SWIFT)	2008/1/1-2010/6/30	530 万ユーロ/348 万ユーロ	DESARROLLO DE APLICACIONES PARA LAS COMUNICACIONES CONTROL Y TECNOLOGIAS DE LA INFORMACION, S.L.（西）、ALCATEL-LUCENT BELL NV（ベルギー）、INSTITUTO DE TELECOMUNICACOES（ポルトガル）、NEC EUROPE LTD UNITED（英）、UNIVERSIDAD DE MURCIA（西）、PORTUGAL TELECOM INOVACAO SA（ポルトガル）、

				DEUTSCHE TELEKOM AG（独）、UNIVERSITAET STUTTGART（独）
7	Context-aware data-centric information sharing (CONSEQUENCE)	2008/1/1-2010/12/30	458 万ユーロ/290 万ユーロ	AE SYSTEMS (OPERATIONS) LTD（英）、CREATE-NET (CENTER FOR RESEARCH AND TELECOMMUNICATION EXPERIMENTATION FOR NETWORKED COMMUNITIES)（伊）、HEWLETT PACKARD ITALIANA SRL（伊）、THE SCIENCE AND TECHNOLOGY FACILITIES COUNCIL UNITED（英）、IMPERIAL COLLEGE OF SCIENCE, TECHNOLOGY AND MEDICINE（英）、CONSIGLIO NAZIONALE DELLE RICERCHE（伊）
8	Trusted Embedded Computing (TECOM)	2008/1/1-2010/12/30	900 万ユーロ/614 万ユーロ	AMTEC SPA（伊）、MIXED MODE GMBH（独）、SIRRIX AKTIENGESELLSCHAFT（独）、SYSGO AG（独）、EADS DEFENCE AND SECURITY SYSTEMS（仏）、SOCIETE AONIX SA（仏）、TRUSTED LOGIC（仏）、INFINEON TECHNOLOGIES AG（独）、TECHNISCHE

				UNIVERSITAET DRESDEN（独）
9	Infrastructure for heterogeneous, resilient, secure, complex, tightly inter-operating networks (INTERSECTION)	2008/1/1-2009/12/31	459 万ユーロ/290 万ユーロ	ITTI SP.ZO.O.（ポーランド）、CORONIS SYSTEMS SA（仏）、EIDGENÖSSISCHE TECHNISCHE HOCHSCHULE ZÜRICH（スイス）、TELEFONICA INVESTIGACION Y DESARROLLO SA（西）、POLSKA TELEFONIA CYFROWA SP. Z O.O.（ポーランド）、TELESPAZIO SPA（伊）、CONSORZIO INTERUNIVERSITARIO NAZIONALE PER L'INFORMATICA（伊）、FRAUNHOFER-GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V（独）、THALES RESEARCH & TECHNOLOGY (UK) LIMITED UNITED（英）、LANCASTER UNIVERSITY UNITED（英）
10	Worldwide observatory of malicious behaviors and attack threats (WOMBAT)	2008/1/1-2010/12/30	442 万ユーロ/289 万ユーロ	SYMANTEC LIMITED（愛）、TECHNISCHE UNIVERSITAET WIEN（オーストリア）、HISPASEC SISTEMAS S.L.（西）、INSTITUTE FOR INFOCOMM RESEARCH（シンガポール）、

				NAUKOWA I AKADEMICKA SIEC KOMPUTEROWA（ポーランド）、EURECOM（仏）、FOUNDATION FOR RESEARCH AND TECHNOLOGY HELLAS（ギリシア）、VERENIGING VOOR CHRISTELIJK HOGER ONDERWIJS WETENSCHAPPELIJK ONDERZOEK EN PATIENTENZORG（オランダ）、POLITECNICO DI MILANO（伊）
11	Managing emerging threats in ICT Infrastructures (FORWARD)	2008/1/1-2009/12/31	88 万 9950 ユーロ/88 万 9950 ユーロ	INSTITUTE FOR PARALLEL PROCESSING - BULGARIAN ACADEMY OF SCIENCES（ブルガリア）、CHALMERS TEKNISKA HOEGSKOLA AB（瑞）、FOUNDATION FOR RESEARCH AND TECHNOLOGY HELLAS（ギリシア）、VERENIGING VOOR CHRISTELIJK HOGER ONDERWIJS WETENSCHAPPELIJK ONDERZOEK EN PATIENTENZORG（オランダ）、INSTITUT EURECOM（仏）

12	Ad-hoc PAN and wireless sensor secure network (AWISSENET)	2008/1/1-2010/2/28	310 万ユーロ/196 万ユーロ	HALES COMMUNICATIONS S.A.（仏）、NORTHERN VENTURE LIMITED（キプロス）、TECHNOLOGICAL EDUCATIONAL INSTITUTE OF CHALKIDA（ギリシア）、TELECOMMUNICATION SYSTEMS INSTITUTE（ギリシア）、ALCATEL-LUCENT DEUTSCHLAND AG（独）、HELSINGIN YLIOPISTO（フィンランド）、UNIVERSIDAD POLITECNICA DE MADRID（西）
13	Trusted revocable biometric identities (TURBINE)	2008/2/1-2011/1/31	969 万ユーロ/635 万ユーロ	SAGEM ORGA GMBH（独）、GENIKON AEROPORIKON EFARMOGON AE IDIOTIKI EPICHEIRISI PAROCHIS YPIRESION ASFALEIAS（ギリシア）、CRYPTOLOG INTERNATIONAL（仏）、ARTTIC（仏）、UNIVERSITEIT TWENTE（蘭）、PHILIPS ELECTRONICS NEDERLAND B.V.（蘭）、KATHOLIEKE UNIVERSITEIT LEUVEN（ベルギー）、PRECISE BIOMETRICS AB（瑞）、HOGSKOLEN I GJOVIK（ノルウェイ）

14	Automated validation of trust and security of service-oriented architectures (AVANTSSAR)	2008/1/1-20 10/12/30	607 万ユーロ /380 万ユーロ	UNIVERSITE DE NANCY 2（仏）、UNIVERSITA DEGLI STUDI DI GENOVA（伊）、IBM RESEARCH GMBH（スイス）、INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE（仏）、INSTITUTUL E-AUSTRIA TIMISOARA（ルーマニア）、OPENTRUST（仏）、Centre National de la Recherche Scientifique (CNRS)（仏）、UNIVERSITE PAUL SABATIER TOULOUSE III（仏）、SAP AG（独）、SIEMENS AG（独）、EIDGENOESSISCHE TECHNISCHE HOCHSCHULE ZUERICH（スイス）

15	Privacy and identity management in Europe for life (PRIMELIFE)	2008/3/1-2011/2/28	1507 万ユーロ/1020 万ユーロ	BROWN UNIVERSITY（米）、UNABHAENGIGES LANDESZENTRUM FUER DATENSCHUTZ（独）、JOHANN WOLFGANG GOETHE UNIVERSITAET FRANKFURT AM MAIN（独）、CURE - CENTER FOR USABILITY RESEARCH AND ENGINEERING（オーストリア）、STICHTING KATHOLIEKE UNIVERSITEIT BRABANT UNIVERSITEIT VAN TILBURG（蘭）、KARLSTADS UNIVERSITET（瑞）、SAP AG（独）、TECHNISCHE UNIVERSITAET DRESDEN（独）、EUROPAEISCHES MICROSOFT INNOVATIONS CENTER GMBH（独）、GEIE ERCIM（仏）、KATHOLIEKE UNIVERSITEIT LEUVEN（ベルギー）、UNIVERSITA DEGLI STUDI DI MILANO（伊）、GIESECKE & DEVRIENT GMBH（独）、UNIVERSITA DEGLI STUDI DI BERGAMO（伊）
16	Privacy and identity management for community	2008/2/1-2011/1/31	595 万ユーロ/400 万ユーロ	LEIBNIZ-INSTITUT FUER MEERESWISSENSCHAFTEN（独）、IT-OBJECTS

	services (PICOS)			GMBH（独）、MASARYKOVA UNIVERZITA（チェコ）、CURE - CENTER FOR USABILITY RESEARCH AND ENGINEERING（オーストリア）、ATOS ORIGIN SOCIEDAD ANONIMA ESPANOLA（西）、T-MOBILE INTERNATIONAL AG & CO. KG.（独）、UNIVERSIDAD DE MALAGA（西）、HEWLETT PACKARD CENTRE DE COMPETENCES FRANCE（仏）、KATHOLIEKE UNIVERSITEIT LEUVEN（ベルギー）、HEWLETT-PACKARD LIMITED UNITED（英）
17	Managing assurance, security and trust for services (MASTER)	2008/2/1-2011/1/31	1503 万ユーロ/930 万ユーロ	ANECT A.S.（チェコ）、DELOITTE CONSEIL SAS（フランス）、COMPANIA ESPANOLA DE SEGUROS DE CREDITO A LA EXPORTACION SA（西）、STIFTELSEN SINTEF（ノルウェイ）、FONDAZIONE CENTRO SAN RAFFAELE DEL MONTE TABOR（伊）、IBM RESEARCH GMBH（スイス）、SAP AG（独）、DUBLIN CITY UNIVERSITY（愛）、ENGINEERING - INGEGNERIA

				INFORMATICA SPA（伊）、BRITISH TELECOMMUNICATIONS PLC.（英）、EIDGENOESSISCHE TECHNISCHE HOCHSCHULE ZUERICH（スイス）、UNIVERSITAET STUTTGART（独）、UNIVERSITA DEGLI STUDI DI TRENTO（伊）
18	European network of excellence in cryptology - Phase II (ECRYPT II)	2008/8/1-2012/7/31	372 万ユーロ/300 万ユーロ	ECOLE NORMALE SUPERIEURE（仏）、UNIVERSITA DEGLI STUDI DI SALERNO（伊）、ECOLE POLYTECHNIQUE FEDERALE DE LAUSANNE（スイス）、TECHNISCHE UNIVERSITAET GRAZ（オーストリア）、ROYAL HOLLOWAY AND BEDFORD NEW COLLEGE（英）、UNIVERSITY OF BRISTOL（英）、IBM RESEARCH GMBH（スイス）、FRANCE TELECOM SA（仏）、RUHR-UNIVERSITAET BOCHUM（独）、CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE（仏）、TECHNISCHE UNIVERSITEIT EINDHOVEN（蘭）

19	Secure supply chain management (SECURESCM)	2008/2/1-2011/1/31	346 万ユーロ/210 万ユーロ	EBS EUROPEAN BUSINESS SCHOOL GEMEINNUETZIGE GMBH（独）、FUNDACION ZARAGOZA LOGISTICS CENTER（西）、DHITECH DISTRETTO TECNOLOGICO HIGH-TECH SCARL（伊）、INTERNATIONAL UNIVERSITY IN GERMANY BRUCHSAL GEMEINNUETZIGE GESELLSCHAFT MIT BESCHRAENKTER HAFTUNG（独）、UNIVERSITA DEGLI STUDI DI MILANO（伊）、TECHNISCHE UNIVERSITEIT EINDHOVEN（蘭）
20	Unobtrusive authentication using activity related and soft biometrics (ACTIBIO)	2008/3/1-2011/2/28	436 万ユーロ/320 万ユーロ	CENTRO STUDI SU SCIENZA,SOCIETA E CITTADINANZA SRL（伊）、GROUP 4 SECURICOR EMPORIAS KAI PAROCHIS PROIGMENON YPIRESION KAI PROIONTON PLIROFORIKIS KAI TILEMATIKIS AE（ギリシア）、BAUDIREKTION URI（スイス）、TELETEL TECHNOLOGIA TILEPIKOINONIONKAI PLIROFORIKIS ANONYMI

				EMPORIKIVIOMICHANIKI ETAIREIA（ギリシア）、ALCATEL-LUCENT DEUTSCHLAND AG（独）、KING'S COLLEGE LONDON（英）、INSTITUT EURECOM （仏）、STARLAB BARCELONA SL（西）、UNIVERSITA DI PISA（伊）、UNIVERSITAT POLITECNICA DE CATALUNYA（西）
21	Mobile Biometry (MOBIO)	2008/1/1-2010/12/30	399 万ユーロ/290 万ユーロ	IDEARK SA（スイス）、EYEP MEDIA SA（スイス）、THE UNIVERSITY OF SURREY（英）、OULUN YLIOPISTO（フィンランド）、VYSOKE UCENI TECHNICKE V BRNE（チェコ）、UNIVERSITE D'AVIGNON ET DES PAYS DE VAUCLUSE（仏）、THE UNIVERSITY OF MANCHESTER（英）
22	Assessing, measuring, and benchmarking resilience (AMBER)	2008/1/1-2009/12/31	105 万ユーロ/105 万ユーロ	RESILTECH SOCIETA A RESPONSABILITA LIMITATA ITALY CHALMERS TEKNISKA HOEGSKOLA AKTIEBOLAG（瑞）、BUDAPESTI MUSZAKI ES GAZDASAGTUDOMANYI EGYETEM（ハンガリー）、THE UNIVERSITY OF NEWCASTLE UPON

				TYNE（英）、CITY UNIVERSITY（英）、UNIVERSITA DEGLI STUDI DI FIRENZE（伊）
23	Computer Aided Cryptography Engineering (CACE)	2008/1/1-20 10/12/30	473 万ユーロ /350 万ユーロ	ALEXANDRA INSTITUTTET A/S（デンマーク）、BERNER FACHHOCHSCHULE（スイス）、SIRRIX AKTIENGESELLSCHAFT（独）、UNIVERSITY OF HAIFA（イスラエル）、TEKNILLINEN KORKEAKOULU（フィンランド）、AARHUS UNIVERSITET（デンマーク）、UNIVERSITY OF BRISTOL（英）、NOKIA OYJ（フィンランド）、RUHR-UNIVERSITAET BOCHUM（独）、TECHNISCHE UNIVERSITEIT EINDHOVEN（蘭）、UNIVERSIDADE DO MINHO（ポルトガル）

24	Trusted architecture for securely shared services (TAS3)	2008/1/1-2011/12/31	1318 万ユーロ/940 万ユーロ	MEDISOFT B.V.（蘭）、ORACLE NEDERLAND BV（蘭）、STICHTING KENTEQ, KENNISCENTRUM BEROEPSONDERWIJS BEDRIJFSLEVEN VOOR TECHNIEK（蘭）、RISARIS LIMITED（愛）、INTALIO LIMITED（英）、EUROPEAN INSTITUTE FOR E-LEARNING（仏）、CUSTODIX NV（ベルギー）、SYNERGETICS N.V.（ベルギー）、THE UNIVERSITY OF NOTTINGHAM（英）、CONSIGLIO NAZIONALE DELLE RICERCHE（伊）、UNIVERSITY OF KENT AT CANTERBURY（英）、SAP AG（独）、UNIVERSIDAD DE ZARAGOZA（西）、UNIVERSITAET KARLSRUHE (TH)（独）、UNIVERSITAET KOBLENZ-LANDAU（独）、TECHNISCHE UNIVERSITEIT EINDHOVEN（蘭）、VRIJE UNIVERSITEIT BRUSSEL（ベルギー）

WP09-10 の「信頼された ICT」で採用された研究プロジェクト一覧

	プロジェクト名と略称	期間	全予算/FP7 拠出分	参加者名およびその国名
1	Network of Excellence on Engineering Secure Future Internet Software Services and Systems (NESSOS)	2010/10/1-2014/3/31	525 万ユーロ/380 万ユーロ	FUNDACION IMDEA SOFTWARE（西）、UNIVERSIDAD DE MALAGA（スペイン）、EIDGENÖSSISCHE TECHNISCHE HOCHSCHULE ZÜRICH（スイス）、SIEMENS AG（独）、UNIVERSITA DEGLI STUDI DI TRENTO（伊）、UNIVERSITAET DUISBURG-ESSEN（独）、LUDWIG-MAXIMILIANS-UNIVERSITAET MUENCHEN（独）、INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE（仏）、KATHOLIEKE UNIVERSITEIT LEUVEN（ベルギー）、ATOS ORIGIN SOCIEDAD ANONIMA ESPANOLA（西）、STIFTELSEN SINTEF（ノルウェイ）
2	Legal Technical Framework for Privacy	2010/09/1-2013/2/28	368 万ユーロ/275 万ユーロ	EUROP ASSISTANCE ITALIA SPA（伊）、FACHHOCHSCHULE SALZBURG GMBH（オーストリ

	Preserving Data Management (ENDORSE)			ア）、SEECOMMS (RESEARCH) CLG LBG（英）、UNIVERSIDAD DE ZARAGOZA（西）、DL LEGAL LLP（英）、SOLUTA.NET SRL（伊）、STICHTING KATHOLIEKE UNIVERSITEIT BRABANT UNIVERSITEIT VAN TILBURG（蘭）、CREATE-NET (CENTER FOR RESEARCH AND TELECOMMUNICATION EXPERIMENTATION FOR NETWORKED COMMUNITIES)（伊）
3	Trusted Biometrics under Spoofing Attacks (TABULA RASA)	2010/11/1-2014/4/30	569 万ユーロ/410 万ユーロ	INSTITUTE OF AUTOMATION CHINESE ACADEMY OF SCIENCES（中）、KEYLEMON SA（スイス）、BIOMETRY.COM AG（スイス）、UNIVERSIDAD AUTONOMA DE MADRID（西）、STARLAB BARCELONA SL（西）、MORPHO（仏）、EURECOM（仏）、UNIVERSITA DEGLI STUDI DI CAGLIARI（伊）、CENTRE FOR SCIENCE, SOCIETY AND CITIZENSHIP（伊）、OULUN YLIOPISTO（フィンランド）、UNIVERSITY OF SOUTHAMPTON（英）
4	Validating Changes and	2010/7/1-20	417 万ユーロ	UNIVERSITA' DEGLI STUDI DI MILANO-BICOCCA

	Upgrades in Networked Software (PINCETTE)	13/6/30	/280 万ユーロ	（伊）、VALTION TEKNILLINEN TUTKIMUSKESKUS（フィンランド）、ABB SCHWEIZ AG（スイス）、UNIVERSITA DELLA SVIZZERA ITALIANA（スイス）、THE CHANCELLOR, MASTERS AND SCHOLARS OF THE UNIVERSITY OF OXFORD（英）、ISRAEL AEROSPACE INDUSTRIES LTD.（イスラエル）
5	Secure Provision and Consumption in the Internet of Services (SPACIOS)	2010/10/1-2013/9/30	534 万ユーロ/335 万ユーロ	KARLSRUHER INSTITUT FUER TECHNOLOGIE（独）、INSTITUT POLYTECHNIQUE DE GRENOBLE（仏）、UNIVERSITA DEGLI STUDI DI GENOVA（伊）、SIEMENS AG（独）、SAP AG（独）、EIDGENÖSSISCHE TECHNISCHE HOCHSCHULE ZÜRICH（スイス）
6	ACcelerate Trust in digital life Organisation and Relations (ACTOR)	2010/6/1-2012/5/31	87 万 1539 ユーロ/80 万ユーロ	GEMALTO SA（仏）、NOKIA OYJ（フィンランド）、MICROSOFT RESEARCH AND DEVELOPMENT FRANCE（仏）、PHILIPS ELECTRONICS NEDERLAND B.V.（蘭）
7	Trustworthy Wireless Industrial Sensor neTworks (TWISNET)	2010/10/1-2013/9/30	337 万ユーロ/219 万ユーロ	ELECTRICITE DE FRANCE S.A.（仏）、UNIVERSITATEA POLITEHNICA DIN BUCURESTI（ルーマニア）、HOCHSCHULE FUER TECHNIK UND

				WIRTSCHAFT DRESDEN（独）、CISCO SYSTEMS INTERNATIONAL B. V.（蘭）、COMMISSARIAT A L ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES（仏）、SAP AG（独）
8	Global Identity Networking of Individuals - Support Action (GINI-SA)	2010/6/1-2012/5/31	84 万 4617 ユーロ/72 万 4995 ユーロ	NORTHID OY（フィンランド）、JOHANN WOLFGANG GOETHE UNIVERSITAET FRANKFURT AM MAIN（独）、FRAUNHOFER-GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V（独）、GOVERNMENT TO YOU（ギリシア）、TECHNISCHE UNIVERSITAET GRAZ（オーストリア）、KATHOLIEKE UNIVERSITEIT LEUVEN（ベルギー）
9	Usable TRUST in the Internet of Things (UTRUSTIT)	2010/9/1-2013/8/31	313 万ユーロ/240 万ユーロ	NORSK REGNESENTRAL STIFTELSE（ノルウェイ）、SWEDEN CONNECTIVITY AB（瑞）、SEARCH-LAB BIZTONSAGI ERTEKELO ELEMZO ES KUTATO LABORATORIUM KORLATOLT FELELOSSEGU TARSASAG（ハンガリー）、TECHNISCHE UNIVERSITAET CHEMNITZ（独）、KATHOLIEKE

				UNIVERSITEIT LEUVEN（ベルギー）
10	Design of Secure and energy-efficient embedded systems for Future internet applications (SECFUTUR)	2010/50/-2013/4/30	420 万ユーロ/270 万ユーロ	QUEENSLAND UNIVERSITY OF TECHNOLOGY - QLD QUT（オーストリア）、LINKOPINGS UNIVERSITET（瑞）、UNIVERSIDAD DE MALAGA（西）、ASCOM (SCHWEIZ) AG（スイス）、INFINEON TECHNOLOGIES AG （独）、SEARCH-LAB BIZTONSAGI ERTEKELO ELEMZO ES KUTATO LABORATORIUM KORLATOLT FELELOSSEGU TARSASAG（ハンガリー）、INSTITUTION OF THE RUSSIAN ACADEMY OF SCIENCES ST PETERSBURG INSTITUTE FOR INFORMATICS AND AUTOMATION OF RAS（露）、TELEFONICA INVESTIGACION Y DESARROLLO SA（西）、MIXED MODE GMBH（独）
11	TAMper Resistant Sensor node (TAMPRES)	2010/10/1-2013/9/30	432 万ユーロ/296 万ユーロ	NXP SEMICONDUCTORS GERMANY GMBH（独）、FRANCE TELECOM SA（仏）、COALESENSES GMBH（独）、TECHNISCHE UNIVERSITAET GRAZ（オーストリア）、UNIVERSITE CATHOLIQUE DE LOUVAIN（ベ

				ルギー）、EIDGENÖSSISCHE TECHNISCHE HOCHSCHULE ZÜRICH（スイス）、NXP SEMICONDUCTORS BELGIUM NV（ベルギー）
12	Building International Cooperation for Trustworthy ICT: Security, Privacy and Trust in Global Networks & Services (BIC)	2011/1/1-2013/12/31	83 万 7940 ユーロ/75 万ユーロ	TECHNISCHE UNIVERSITAET DARMSTADT（独）、INSTITUT TELECOM（仏）、ATOS ORIGIN SOCIEDAD ANONIMA ESPANOLA（西）
13	Secure and Trustworthy Composite Services (ANIKETOS)	2010/8/1-2014/1/31	1405 万ユーロ/960 万ユーロ	IVERPOOL JOHN MOORES UNIVERSITY（英）、ITALTEL S.P.A.（伊）、ELSAG DATAMAT S.P.A.（伊）、CONSIGLIO NAZIONALE DELLE RICERCHE（伊）、WIND TELECOMUNICAZIONI S.P.A.（伊）、DEEP BLUE SRL（伊）、WATERFORD INSTITUTE OF TECHNOLOGY（愛）、SEARCH-LAB BIZTONSAGI ERTEKELO ELEMZO ES KUTATO LABORATORIUM KORLATOLT FELELOSSEGU TARSASAG（ハンガリー）、DIMOS ATHINAION EPICHEIRISI MICHANOGRAFISIS（ギリシア）、THALES SERVICES

				SAS（仏）、UNIVERSITA DEGLI STUDI DI TRENTO（伊）、FUNDACION EUROPEAN SOFTWARE INSTITUTE（西）、PARIS-LODRON-UNIVERSITÄT SALZBURG（オーストリア）、ATOS ORIGIN SOCIEDAD ANONIMA ESPANOLA（スペイン）、SAP AG（独）、ATHENS TECHNOLOGY CENTER SA（ギリシア）
14	Policy and Security Configuration Management (POSECCO)	2010/10/1-2013/9/30	1132 万ユーロ/700 万ユーロ	POLITECNICO DI TORINO（伊）、UNIVERSITAET INNSBRUCK（オーストリア）、BERNER FACHHOCHSCHULE（スイス）、UNIVERSITA' DEGLI STUDI DI BERGAMO（伊）、CROSSGATE AG（独）、THALES SERVICES SAS（仏）、DELOITTE CONSEIL SAS（仏）、TECHNISCHE UNIVERSITEIT EINDHOVEN（蘭）、ATOS ORIGIN SOCIEDAD ANONIMA ESPANOLA（西）、IBM RESEARCH GMBH（西）

15	MAnagement of Security information and events in Service InFrastructures (MASSIF)	2010/10/1-2013/9/30	850 万ユーロ/595 万ユーロ	CONSORZIO INTERUNIVERSITARIO NAZIONALE PER L'INFORMATICA（伊）、FRANCE TELECOM SA（仏）、T-SYSTEMS SOUTH AFRICA (PTY) LTD（南アフリカ）、INSTITUTION OF THE RUSSIAN ACADEMY OF SCIENCES ST PETERSBURG INSTITUTE FOR INFORMATICS AND AUTOMATION OF RAS（露）、FUNDACAO DA FACULDADE DE CIENCIAS DA UNIVERSIDADE DE LISBOA（ポルトガル）、OPEN SOURCE SECURITY INFORMATION MANAGEMENT, S.L.（西）、FRAUNHOFER-GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V（独）、INSTITUT TELECOM（仏）、6CURE SAS（仏）、UNIVERSIDAD POLITECNICA DE MADRID（西）、EPSILON S.R.L.（伊）

16	Server-driven Outbound Web-application Sandboxing (WEBSAND)	2010/10/1-2013/9/30	494 万ユーロ/320 万ユーロ	SIEMENS AG（独）、UNIVERSITÄT PASSAU（独）、KATHOLIEKE UNIVERSITEIT LEUVEN（ベルギー）、CHALMERS TEKNISKA HOEGSKOLA AB（瑞）
17	Advanced Security Service cERTificate for SOA (ASSERT4SOA)	2010/10/1-2013/9/30	514 万ユーロ/340 万ユーロ	UNIVERSITA DEGLI STUDI DI MILANO（伊）、FRAUNHOFER-GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V（独）、UNIVERSIDAD DE MALAGA（西）、ENGINEERING - INGEGNERIA INFORMATICA SPA（伊）、FONDAZIONE UGO BORDONI（伊）、THE CITY UNIVERSITY（英）
18	Policy-Assessed system-level Security of Sensitive Information processing in Virtualised Environments (PASSIVE)	2010/6/1-2012/5/31	358 万ユーロ/235 万ユーロ	ANECT A.S. CZECH REPUBLICUNIVERSIDAD DE MALAGA SPAINATOS ORIGIN SOCIEDAD ANONIMA ESPANOLA SPAINENGINEERING - INGEGNERIA INFORMATICA SPA（伊）、TECHNISCHE UNIVERSITAET DRESDEN（独）、THALES RESEARCH & TECHNOLOGY (UK) LIMITED（独）、WATERFORD INSTITUTE OF

				TECHNOLOGY（愛）
19	A European Network of Excellence in Managing Threats and Vulnerabilities in the Future Internet: Europe for the World (SYSSEC)	2010/9/1-2014/8/31	295 万ユーロ /250 万ユーロ	VERENIGING VOOR CHRISTELIJK HOGER ONDERWIJS WETENSCHAPPELIJK ONDERZOEK EN PATIENTENZORG（蘭）、TUBITAK NATIONAL RESEARCH INSTITUTE OF ELECTRONICS AND CRYPTOLOGY（トルコ）、INSTITUTE FOR PARALLEL PROCESSING OF THE BULGARIAN ACADEMY OF SCIENCES（ブルガリア）、EURECOM（仏）、CHALMERS TEKNISKA HOEGSKOLA AB（瑞）、POLITECNICO DI MILANO（伊）、TECHNISCHE UNIVERSITAET WIEN（オーストリア）
20	Secure, Embedded Platform with advanced Process Isolation and Anonymity Capabilities (SEPIA)	2010/6/1-2013/5/31	326 万ユーロ /200 万ユーロ	INFINEON TECHNOLOGIES AG（独）、INFINEON TECHNOLOGIES AUSTRIA AG（オーストリア）、BRIGHTSIGHT BV（蘭）、ARM LIMITED（英）、GIESECKE & DEVRIENT GMBH（独）

21	Visual Analytic Representation of Large Datasets for Enhancing Network Security (VIS-SENSE)	2010/10/1-2013/9/30	332 万ユーロ/235 万ユーロ	EURECOM（仏）、SYMANTEC LIMITED（愛）、INSTITUT TELECOM（仏）、CENTRE FOR RESEARCH AND TECHNOLOGY HELLAS（ギリシア）、UNIVERSITAT KONSTANZ（独）
22	European Framework for Future Internet Compliance, Trust, Security and Privacy through effective clustering (EFFECTS+)	2010/09/1-2013/2/28	67 万 4192 ユーロ/62 万 4995 ユーロ	UNIVERSITA DEGLI STUDI DI TRENTO（伊）、HEWLETT-PACKARD LIMITED（英）、ATOS ORIGIN SOCIEDAD ANONIMA ESPANOLA（西）、SAP AG（独）

第三章　欧州主要国の ICT セキュリティ部門の研究開発組織および研究プロジェクト事例

本章では、欧州主要国（英仏独）における ICT セキュリティ部門の研究開発機関および研究プロジェクト事例について記す。特に公的研究開発組織の活動と、官民を問わず、公的研究開発支援機関から助成を受けているプロジェクトを示す。

第一節　英国

英国では工学・物理科学研究評議会（Engineering and Physical Sciences Research Council : EPSRC）[164]が ICT 部門を含む研究・開発支援を所掌する公共機関として活動している。公共セクターにおける ICT 部門の研究開発は一般に大学組織で行われており、EPSRC は大学の研究所等に助成している。また「情報セキュリティプロフェッショナル研究院」[165]と呼ばれる半官半民の機関では、ICT セキュリティの専門教育が実施されている。

次ページから、同機関が支援している ICT セキュリティ関連の研究プロジェクトリストを掲載する。より詳しい内容については、リストに記載したプロジェクトのウェブサイトを参考のこと。

---

[164] http://www.epsrc.ac.uk/about/Pages/default.aspx

[165] https://www.instisp.org/SSLPage.aspx?pid=183

EPSRC が助成する ICT セキュリティ関連の研究プロジェクト事例

プロジェクトタイトル	期間	研究機関	研究パートナー組織	予算規模	インターネットサイト
Next-Generation Data Security Architectures	2008/10/25-2013/10/24	Queen's University of Belfast	Ateml, France Telecom R and D, University of Texas	120 万ポンド	http://gow.epsrc.ac.uk/ViewGrant.aspx?GrantRef=EP/G007586/1
Analysing Security and Pryvacy Propoerties	2010/4/1-2015/3/31	University of Birmingham	3Form, Electoral Reform Services, Forensic Pathways, Google UK, Hewlett Packard Ltd, Microsoft Corporation (USA), Ministry of Justice, Open Rights Group OPT2Vote Ltd, Royal Holloway, Univ of London	99 万ポンド	http://gow.epsrc.ac.uk/ViewGrant.aspx?GrantRef=EP/H005501/1

Verification of security protocols: a multi-agent systems approach	2007/10/1-2010/9/30	Imperial College London	Polish Academy of Sciences	38 万ポンド	http://gow.epsrc.ac.uk/ViewGrant.aspx?GrantRef=EP/E035655/1
FRESNEL: FedeRatEd Secure sensor NEtwork Laboratory	2010/1/10-2013/1/9	University of Oxford	British Telecommunications Plc, Microsoft Research Ltd, Sensors and Instrumentation, KTN,Symbian Software Ltd, TRW Conekt	44 万ポンド	http://gow.epsrc.ac.uk/ViewGrant.aspx?GrantRef=EP/G070687/1
Quantum Computation: Foundations, Security, Cryptography and Group Theory	2008/2/1-2011/1/31	University of Glasgow		3 万 9000 ポンド	http://gow.epsrc.ac.uk/ViewGrant.aspx?GrantRef=EP/F020813/1
Quantum Computation: Foundations,	2008/5/1-2011/4/30	University of York		28 万ポンド	http://gow.epsrc.ac.uk/ViewGrant.aspx?GrantRef=EP/F005881/1

Security, Cryptography and Group Theory					
Quantum Computation: Foundations, Security, Cryptography and Group Theory	2008/6/18-2011/6/17	Newcastle University		27 万ポンド	http://gow.epsrc.ac.uk/ViewGrant.aspx?GrantRef=EP/F014945/1
Aspects of Security	2009/5/8-2011/5/7	Imperial College London		3 万 5000 ユーロ	http://gow.epsrc.ac.uk/ViewGrant.aspx?GrantRef=EP/H000321/1
Foundations of Secure Web Programming	2010/8/10-2015/7/31	Imperial College London		59 万ポンド	http://gow.epsrc.ac.uk/ViewGrant.aspx?GrantRef=EP/I004246/1

第二節　フランス

フランスでは、ICT 研究・開発は民間セクター以外では、グランゼコールと呼ばれるフランス独自の高等教育機関、大学、国立研究所で実施されている。

ICT セキュリティの研究機関

国立の研究機関である「フランス国立情報学自動制御研究所（INRIA）」においては、セキュリティ関連の研究・開発は、3 つの研究チームが取り組んでいる。

INRIA のセキュリティ関連の研究開発チーム

- 周囲ネットワーク向けサービス指向の安全アーキテクチャ (AMAZONE)[166]
- 拡散し安全な情報通信 (IDES)[167]
- アクティブ・オブジェクト、セマンティック、インターネット、セキュリティ(OASIS)[168]

グランゼコール

グランゼコールでは、まず「テレコム・ブルターニュ」[169]に「ネットワーク・セキュリティ・マルチメディア」という学部が設置されており、「ネットワークとサービスのセキュリティと確定（SERVAL）」というテーマの研究開発が行われている。

また、フランスで最も有名な ICT 高等教育・研究開発研究機関である「テレコム・パリテック」においては、2010 年 1 月、情報学とネットワーク学部に「ネットワークと情報セキュリティ」という研究グ

166 http://www.inria fr/recherche/equipes/amazones.fr.html
167 http://www.inria fr/recherche/equipes/indes fr html
168 http://www-sop.inria.fr/oasis/index.php
169 http://departements.telecom-bretagne.eu/rsm/
http://departements.telecom-bretagne.eu/rsm/recherche/serval/

ループが新設されており、ICT セキュリティへの関心が高まっていることが伺える[170]。このグループは ICT セキュリティ関連の多くのテーマに取り組み、包括的な研究を実施することが予定されている。

テレコム・パリテックの系列研究機関である「ユーレコム」には、「ネットワークとセキュリティ学部」が設置されており、「NS チーム」と呼ばれる研究グループが数多くの ICT セキュリティ関連の研究を行っている[171]。

ANR の公募プログラムと研究プロジェクト事例

フランスでは、フランス国立研究機構（ANR）が官民問わず ICT 部門を含めた研究開発の助成を行っている[172]。

2006 年と 2007 年には、ICT セキュリティ部門に特化した公募（2006 年度「セキュリティと情報通信」[173]・2007 年度「情報通信のセキュリティと確実性」[174]）を実施している。

また、2010 年の ICT 部門の最新公募では、「組み込みシステムと

---

170 http://www.infres.enst.fr/wp/sr/

171 http://www.eurecom.fr/research/overview.fr.htm
http://www.eurecom.fr/ce/researchce/nsteam.fr htm
以下がユーレコムの NS チームの研究テーマである。

- Malware Collection, Detection and Analysis
- Web Security
- Secure Software Design
- Security and Privacy in Social Networks
- Safebook: Peer-to-Peer OSN for Privacy and Trust
- System Security Aspects of On-line Social Networks
- Security in Autonomous Computing
- Security Protocols for Wireless Devices
- Access control, Identity Management and Privacy

172 ANR は英 ESPRC と違って、工学部門の研究開発に特化した研究助成組織ではなく、社会科学、人文科学の研究助成も行っており、より総合的な研究支援機関である。

173 http://www.agence-nationale-recherche fr/programmes-de-recherche/appel-detail/programme-securite-et-informatique-2006/

174 http://www.agence-nationale-recherche fr/programmes-de-recherche/appel-detail/programme-securite-et-surete-informatique-2007/

大規模インフラストラクチュア」[175]、「未来のネットワークと VERSO サービス」[176]、「コンテンツとインタラクション」[177]の三つのプログラムでセキュリティ関連の研究プロジェクトが募集されている。

次ページに、2007 年度の ANR 公募プログラム「情報通信のセキュリティと確実性」で採用された研究プロジェクトのリストを掲載する。

175 http://www.agence-nationale-recherche fr/programmes-de-recherche/appel-detail/systemes-embarques-et-grandes-infrastructures-2010/

176 http://www.agence-nationale-recherche fr/programmes-de-recherche/appel-detail/reseaux-du-futur-et-services-verso-2010/

177 http://www.agence-nationale-recherche fr/programmes-de-recherche/appel-detail/programme-contenus-et-interactions-2010/

2007 年度 ANR 公募プログラム「情報通信のセキュリティと確実性」において採用された研究プロジェクト

研究プロジェクトタイトル	プロジェクト略称	研究組織（責任者が所属する組織）	研究パートナー	ウェブサイト
Attack Standardization for FIngerPrint system certification	ASFIP	CEA-Leti	Leti, Ecole des Mines de St Etienne, Sagem Sécurité,	https://tokyo.emse.fr/trac/asfip
Formal analysis of electronic voting protocols	AVOTE	LORIA	France Telecom, LSV, Verimag	http://www.lsv.ens-cachan.fr/Projects/anr-avote/
Constraints and Abstractions for program VERificatioN	CAVERN	INRIA	ILOG, CEA Llist, CNRS, 13S	http://cavern.inria.fr/
Face Analysis and Recognition using 3D	FAR3D	Telecom lille1	USTL, Eurécom, Ecole Centrale de Lyon, THALES	http://www-rech.telecom-lille1.eu/far3d/
Convergence of Flow and Usage Controls in Organizations	FLUOR	Université de la Polynésie Française	Telecom Bretagne, Inria, LIUPPA, SWID	http://fluor.no-ip.fr/

Enhancing the Evaluation of Error consequences using Formal Methods	FME3	Université Joseph Fourrier	TIMA Laboratory, LIP6	http://tima.imag.fr/vds/FME3/
Liability Issues in Software Engineering	LISE	INRIA		http://ralyx.inria.fr/2009/Raweb/licit/uid32.html
Password Authentication and Methods for Privacy and Anonymity	PAMPA	EADS	Ecole Noramal Supérieure, Cryptolog International	https://crypto.di.ens.fr/pampa:main
RFID Authentication and Privacy	RFIDAP	CEA-Leti	EURECOM, France Télécom R+D, INRIA	http://www.rfid-ap.fr/Public/pages_web/main_focus12894.html
Security of Cryptographic Algorithms with Probabilities	SCALP	VERIMAG	INRIA, ENS Lyon, CNAM	http://scalp.gforge.inria.fr/
Symmetric Encryption with QUantum key	SEQURE	Thales	Télécom ParisTech, Institut d'Optique graduate school	http://www.demo-sequre.com/partners.html

Renewal				
Securing Flow of INformation for Computing pervasive Systems	SFINCS	LIFL	LIF, NORSYS, TRUSTED LOGIC, VERIMAG	http://sfincs.gforge.inria.fr/
Approximate Verification of Probabilistic Systems	VERAP	LRI		http://www.lri.fr/~mdr/verap/

第三節　ドイツ

最後に、ドイツにおけるICTセキュリティ部門の研究・開発プロジェクト事例を挙げる。本報告書では、基礎研究を行うことで知られているマックス・プランク学術振興協会参加のマックス・プランクソフトウェアシステム研究所の活動および研究プロジェクト、そして応用研究で知られているフラウン・フォーファー協会傘下のフラウン・フォーファー安全情報技術研究所の活動と研究プロジェクトを記す。

マックス・プランクソフトウェアシステム研究所[178]

ICTセキュリティに関しては、同研究所の「情報セキュリティと暗号学グループ」で研究開発が進められている。以下に、研究関心と現在進行している研究プロジェクトを三つ記す。

研究関心

- 形式的な手法と暗号学のリンク
- ウェブサービスのセキュリティ
- アド・ホックネットワークにおけるセキュリティと信頼性
- 企業プライバシー
- 情報フロー
- ステガノグラフィー（データ隠蔽）
- セキュリティプロトコル分析のためのプログラミング論理

研究プロジェクト事例

プロジェクト名 「X-pire！ どのようにインターネットに忘れることを

[178] http://www mpi-sws.org/index_flash.php?n=groups
http://www.infsec.cs.uni-saarland.de/
同研究所は、ソフトウェアシステムに関するハイリスク・ハイインパクトのある研究開発を行っている。

教えるか」[179]

内容　ウェブ上にアップロードしたテキストや写真に期限を設けて、消去する技術の研究

プロジェクト名　「どのようにプリンターはプライバシーを侵害するか」[180]

内容　プリンターから漏れ出る音を通して、印刷されたテキスト等を復元する技術の研究

プロジェクト名　「反映の漏洩　どのようにして隅からコンピューターのモニターを読むか」[181]

内容　パソコンのモニターから漏れた画面の反映を読み取る技術の研究

フラウン・フォーハー安全情報技術研究所[182]

同研究所では、ICT セキュリティのあらゆるテーマの研究開発が進められている。人員は 195 名（2010 年 7 月）であり、予算は 980 万ユーロ（2009 年）で、予算規模は年々拡大している。以下に、同研究所の研究グループとそれぞれのグループの研究プロジェクトを記す。各研究プロジェクトの詳しい内容については、プロジェクト名の下に記載したウェブサイトを参考のこと。

研究グループ名

- 組み込まれたセキュリティと信頼された OS
- 情報保証

---

[179] http://www.infsec.cs.uni-saarland.de/projects/forgetful-internet/

[180] http://www.infsec.cs.uni-saarland.de/projects/printer-acoustic/

[181] http://www.infsec.cs.uni-saarland.de/projects/reflections/

[182] http://www fraunhofer.de/en/institutes-research-establishments/
http://www.sit fraunhofer.de/en/index.jsp

- ネットワーク・セキュリティと早期警告システム
- セキュリティ・モデリングと確定
- 安全なモバイルシステム
- 周囲の安全
- アプリケーションとプロセスセキュリティ
- 安全サービスとクオリティ試験
- トランザクションとドキュメントセキュリティ

研究プロジェクトリスト

研究グループ名	組み込まれたセキュリティと信頼された OS
プロジェクト名	ASMONIA (Attack analysis and Security concepts for MObile Network infrastructures, supported by collaborative Information exchAnge)
ウェブサイト	http://www.asmonia.de/index.php?page=0
プロジェクト名	RESIST - Methoden und Werkzeuge zur Absicherung eingebetteter und mobiler Systeme gegen Angriffe der nächsten Generation
ウェブサイト	http://www.resist-projekt.de/index.php/home_de.html
プロジェクト名	Elliptic Curve Cryptograpy in Remote Keyless Entry
ウェブサイト	http://www.sit.fraunhofer.de/en/forschungsbereiche/projekte/ECC_RKE.jsp
プロジェクト名	Error Detection in Microprocessor Architectures
ウェブサイト	http://www.sit.fraunhofer.de/en/forschungsbereiche/projekte/Error_Det.jsp
プロジェクト名	Physical Unclonable Functions (PUFs)
ウェブサイト	http://www.sit.fraunhofer.de/en/forschungsbereiche/projekte/PUF.jsp

研究グループ名	情報保証
プロジェクト名	Digital Watermarking Container
ウェブサイト	http://www.sit.fraunhofer.de/en/forschungsbereiche/projekte/Wasserzeichen-Container.jsp
プロジェクト名	Project references: MP3-onlineshops

ウェブサイト	http://www.sit.fraunhofer.de/en/forschungsbereiche/projekte/Referenzprojekt_MP3_Onlineshop.jsp
プロジェクト名	Plugmark
ウェブサイト	http://www.sit.fraunhofer.de/en/forschungsbereiche/projekte/Plugmark.jsp

研究グループ名	ネットワーク・セキュリティと早期警告システム
プロジェクト名	Security in Embedded IP-based Systems
ウェブサイト	http://www.sit.fraunhofer.de/en/forschungsbereiche/projekte/SEIS.jsp
プロジェクト名	Early Warning Systems - Lab
ウェブサイト	http://www.sit.fraunhofer.de/en/forschungsbereiche/projekte/EWSLab.jsp

研究グループ名	ネットワーク・セキュリティと早期警告システム
プロジェクト名	Security in Embedded IP-based Systems
ウェブサイト	http://www.sit.fraunhofer.de/en/forschungsbereiche/projekte/SEIS.jsp
プロジェクト名	Early Warning Systems - Lab
ウェブサイト	http://www.sit.fraunhofer.de/en/forschungsbereiche/projekte/EWSLab.jsp

研究グループ名	セキュリティ・モデリングと確定
プロジェクト名	Security for automotive on-board networks
ウェブサイト	http://www.sit.fraunhofer.de/en/forschungsbereiche/projekte/EVITA.jsp
プロジェクト名	SERENITY - System Engineering for Security and Dependability
ウェブサイト	http://www.sit.fraunhofer.de/en/forschungsbereiche/pr

	ojekte/Serenity.jsp
プロジェクト名	SHVT - Methods and Tools for the Analysis and Design of secure Systems
ウェブサイト	http://www.sit.fraunhofer.de/en/forschungsbereiche/projekte/SHVT.jsp
プロジェクト名	Trusted Computing - Security Analysis
ウェブサイト	http://www.sit.fraunhofer.de/en/forschungsbereiche/projekte/SecAnal_TPM.jsp

研究グループ名	安全なモバイルシステム
プロジェクト名	HYDRA – Networked Embedded System Middleware for Heterogeneous Physical Devices in a Distributed Architecture
ウェブサイト	http://www.sit.fraunhofer.de/en/forschungsbereiche/projekte/hydra.jsp
プロジェクト名	Security for automotive on-board networks
ウェブサイト	http://www.sit.fraunhofer.de/en/forschungsbereiche/projekte/EVITA.jsp
プロジェクト名	NanoDataCenters
ウェブサイト	http://www.sit.fraunhofer.de/en/forschungsbereiche/projekte/NanoDataCenters.jsp
プロジェクト名	Security in Embedded IP-based Systems
ウェブサイト	http://www.sit.fraunhofer.de/en/forschungsbereiche/projekte/SEIS.jsp
プロジェクト名	Trusted Computing
ウェブサイト	http://www.sit.fraunhofer.de/en/forschungsbereiche/projekte/Trusted_Computing.jsp
プロジェクト名	Digital Signing of VoIP Communication
ウェブサイト	http://www.sit.fraunhofer.de/en/forschungsbereiche/pr

	ojekte/VoIP_Signaturen.jsp

研究グループ名	アンビエント・セキュリティ
プロジェクト名	Center for Advanced Security Research Darmstadt
ウェブサイト	http://www.sit.fraunhofer.de/en/forschungsbereiche/projekte/CASED.jsp
プロジェクト名	ContainIT
ウェブサイト	http://www.sit.fraunhofer.de/en/forschungsbereiche/projekte/ContainIT.jsp

研究グループ名	アプリケーションとプロセスセキュリティ
プロジェクト名	ADiWa – Allianz Digitaler Warenfluss
ウェブサイト	http://www.sit.fraunhofer.de/en/forschungsbereiche/projekte/adiwa.jsp
プロジェクト名	Center for Advanced Security Research Darmstadt
ウェブサイト	http://www.sit.fraunhofer.de/en/forschungsbereiche/projekte/CASED.jsp
プロジェクト名	KompEC - Centre for Competence in Electronic Business Transactions
ウェブサイト	http://www.sit.fraunhofer.de/en/forschungsbereiche/projekte/KompEC.jsp
プロジェクト名	Facilityboss
ウェブサイト	http://www.sit.fraunhofer.de/en/forschungsbereiche/projekte/FacilityBoss.jsp

研究グループ名	トランザクションとドキュメントセキュリティ
プロジェクト名	ADiWa – Allianz Digitaler Warenfluss
ウェブサイト	http://www.sit.fraunhofer.de/en/forschungsbereiche/projekte/adiwa.jsp

まとめ

以上、欧州におけるサイバーセキュリティ政策と同分野の研究開発動向を概観してきた。ここでは、その内容を要約し繰り返すことはしないが、一点のみ注意を喚起しておきたい。

我々はフランスの違法ダウンロード規制法について調査するために、市民団体クアドラチュール・デュ・ネットにヒアリングを行った。そこで明らかになったことの一つに、同団体のロビー活動が欧州議会議員を動かし、仏アドピ法案に反対する法文を EU 指令に盛り込むことができたという事実がある。そして、同団体がロビー活動を行う前に、逆にフランスの映画産業団体が欧州議会で違法ダウンロード規制法を EU 指令に盛り込むため、ロビー活動を実施していたことも明らかになった。以上のように、EU では産業団体や市民団体が自分の主張や利益を実現するために激しくロビー活動を行っているのだ。言い換えれば、欧州委員会、欧州議会、閣僚理事会による EU 法の共同決定手続きの水面下で行われているロビー活動は、EU 法の成立に強く関与しうるのであり、EU 機関周辺で活動する企業、産業団体、市民団体等は非公式なアクターなのだ。また、このようなロビー活動はテレコム部門に限定されることではないことが容易に想像できるだろう。EU 法の動向を知るためには、ロビー活動を行う団体の動きにも注意する必要がある。