

## 「インターネットとセキュリティに係る米国・中国間の通商・外交動向」

市川類@JETRO/IPA NY

### 1. はじめに

世界の情報技術（IT）分野において、米国が重要な国であることはもちろんであるが、それに加え、近年、中国も大きな位置付けを有するようになってきている。その際、米国と中国は、もともと異なった社会・経済体制を背景にする国であることから、両国間のITに係る通商・外交関係には大きな課題が存在する。

両国間においては、従来から、輸出入・投資だけではなく、知的財産権が重要な問題になっているが、特に、インターネットを始めとする近年情報技術（IT）の進展、普及に伴い、二国間で新たな問題が生じつつある。具体的には、通商と安全保障の両面に関する以下の2点があげられる。

- ・ インターネットを通じて、情報がグローバルにやりとりがなされるようになる中、「インターネット規制・検閲」を巡る両国間の考え方、基準が大きく異なるため、大きな対立が存在する。
- ・ また、インターネットの進展により、諜報活動等がインターネットを通じて行われるようになる中、国際的な視点での「サイバー・セキュリティ」が米国内では大きな課題となりつつある。

また、これらの課題のベースには、インターネット上の情報を制御する各種情報技術（IT）があり、今後これらの技術に係る国際間の取引にも影響する可能性も否定できない。

このような問題意識のもと、本報告においては、米国から見た中国との関係における、情報技術（IT）に係るこれらの問題の動向について報告する<sup>1</sup>。

### 2. 米国と中国におけるITに係る二国間関係と新たな課題

#### （1）ITに係る米国と中国の位置付けと通商問題

##### ①ITに係る米国と中国の位置付け（概要）

##### <世界における米国と中国の位置付け>

世界において、米国と中国は大きな位置を占めるに到ってきている。経済規模（GDP）としては、現在、米国が、世界で一番大きな国であること言うまでもな

<sup>1</sup> なお、両案件とも、必ずしも明確な政策方向が見えている訳ではない。

いが、中国は、近年の急成長に伴い、日本に次いで第3位の国にまで成長している。

また、IT関係でも、米国は世界最大の市場であるとともに、高い競争力を有する企業が多く存在すると言われるが、中国も、IT支出としては、今や日本に次いで世界第3位の国に成長しているとともに、インターネット・ユーザー数としても、米国を抜いて、世界第1位の国となっている。また、中国は、今後とも、他国と比較して、引き続き大きな成長が見込まれている。

米国と中国に係る GDP、IT市場規模、インターネット・ユーザー数

	米国	中国	中国の最近の伸び	(参考)日本
GDP <sup>2</sup>	25.4% (1位)	6.1% (4位)	・近年2桁の伸びで成長。 ・2007年の順位は、その後、統計の修正により3位に <sup>3</sup> 。	8.1% (2位)
IT支出 <sup>4</sup>	(1位)	(3位)	・2年前の5位から上昇。 ・08～09年の成長率は8%増 <sup>5</sup>	(2位)
インターネット・ユーザー数 <sup>6</sup>	16% (2位)	18% (1位)	・1年間で62%増(07年6月～08年6月) <sup>7</sup>	6% (3位)

#### <米国企業の中国市場への参入>

このように、中国市場が急速に拡大する中、世界的にIT分野で競争力を有する米国大手IT各社(特に、ソフトウェア、インターネット・サービス等)は、中国市場に、積極的に参入を進めてきている。

- ・ソフトウェアで世界最大手であるMicrosoft社は、中国市場に取り組むため、2006年末に多額の研究開発資金の投資を発表したことに加え<sup>8</sup>、最近では「グレートチャイナ経営戦略委員会」を設置し、海賊版対策、新たな研究開発投資等に取り組んでいる<sup>9</sup>。

<sup>2</sup> World Bank データ(2007年)より。

<http://siteresources.worldbank.org/DATASTATISTICS/Resources/GDP.pdf>

<sup>3</sup> <http://www.afpbb.com/article/economy/2558105/3682063>

<sup>4</sup> ITの世界的業界団体であるWITSA(World Information Technology and Services Alliance)が、2008年5月に発表した報告「Digital Planet 2008」のデータ。

[http://www.japancorp.net/Article.Asp?Art\\_ID=18281](http://www.japancorp.net/Article.Asp?Art_ID=18281)

<sup>5</sup> IDCの2008年12月の発表。中国のIT市場の成長率(2009年～2010年)としては、8%増を予想しており、これはアジア太平洋地域全体(日本を除く)の平均予測成長率である1.8%をはるかにしのぐ。

<http://www.idc.com/getdoc.jsp?containerId=prSG21576608>

<sup>6</sup> コムスコアのデータ。(2008年6月) <http://japan.internet.com/busnews/20090126/10.html>

<sup>7</sup> China Internet Network Information Center: CINICのデータ。2008年6月現在の中国のネットユーザー総数は、前年同時期と比較して9,100万人増(2億5,300万人)。

<http://www.cnnic.net.cn/download/2008/CNNIC22threport-en.pdf>

<sup>8</sup> <http://japan.cnet.com/column/china/story/0.2000055907.20344912.00.htm>

<sup>9</sup> <http://it.nikkei.co.jp/internet/news/index.aspx?n=MMITbp000021112008>

- ・ インターネット・サービス（検索）の最大手である Google は、2006年1月、Google.cn を設置し、中国市場に本格的に参入している<sup>10</sup>。また、Google 中国は、2008年4月、今後5年以内に中国の検索分野のリーディングカンパニーとなることを表明するとともに、各種会社への投資計画の意向も示している<sup>11</sup>。
- ・ ルーター等のネットワーク機器大手の Cisco は、従来より新興国への投資を積極的に進めており<sup>12</sup>、中国市場に対しても、2007年11月に、160億ドル投資する計画を立案するとともに、2008年4月には、「シスコ中国部戦略委員会」を設立し、中国市場での成長率目標を25%に設定している<sup>13</sup>。

なお、PCなどのハードウェア製品については、世界的には、米国系企業は競争力を有するが、中国系企業も競争力を有しているとともに<sup>14</sup>、これらのハードウェアに係る製造拠点として、中国は重要な役割を担いつつある。実際に、2007年の米国におけるコンピューター輸入額の総額<sup>15</sup>は303億ドルであったが、そのうち中国からの輸入額は、全体の76.7%を占める232億ドルであった<sup>16</sup>。

## ②ITを巡る通商・対外問題

このように、中国市場が拡大する中、米中間では各種の通商問題が存在する。一般的に、通商問題は、歴史的には、モノの輸出入に関わる各種問題が中心であり、その後、対外直接投資を含むサービス分野にまで拡大してきている。また、その際、経済的な観点に加え、国家安全保障の観点からの製品・技術の輸出入に係る制限も存在する。

このような中、情報通信（IT）産業は、モノである「ハードウェア」や、サービスである「ITサービス」に加え、知的財産そのものとも言える「ソフトウェア」、また、国境間を容易に超える「インターネット・サービス」が組み合わさった複合的な産業であるといえる。このため、IT産業としては、他の産業と比較して、「知的財産権」に係る通商問題が、ソフトウェア産業を中心に、従来から大きな問題になっていることに加え、特に、近年のインターネットの進展に伴い、ITに係る特有の問題として、以下の2点が生じてきている。

<sup>10</sup> なお、中国における検索サービス市場（2008年）では、Baidu（百度）が62.2%と大半を占めるが、Googleも27.8%と健闘しており、次いでYahoo! Chinaが5.8%となっている。

<http://blogmag.ascii.jp/china/2009/02/002386.html>

<sup>11</sup> <http://japan.internet.com/busnews/20080415/26.html>

<sup>12</sup> [http://www.cisco.com/web/JP/news/pr/newsroom\\_us/2008/11/hd\\_110508b.html](http://www.cisco.com/web/JP/news/pr/newsroom_us/2008/11/hd_110508b.html)

<sup>13</sup> <http://www.chinapress.jp/release/10589/>

<sup>14</sup> なお、中国市場におけるPCのシェア（2007年第一四半期）は、レノボ（中国）36.1%、方正（中国）13.4%、同方（中国）10.3%となるが、次いで、HP7.7%、Dell7.2%となっている。

<http://pc.nikkeibp.co.jp/article/NEWS/20070607/274011/?set=relate>

<sup>15</sup> 主要取引国6ヶ国：カナダ、中国、日本、メキシコ、ドイツ、英国

<sup>16</sup> [http://import-export.suite101.com/article.cfm/us\\_imported\\_and\\_exported\\_computer\\_sales](http://import-export.suite101.com/article.cfm/us_imported_and_exported_computer_sales)

- ・ ①インターネット・サービスを中心に、インターネットを通じて情報が国境を超えてやりとりされる中、各国間の規制・検閲の基準等が異なることにより、新たな摩擦が生じてきていること。
- ・ ②インターネットを通じたハッキング等を通じて、安全保障の観点からのサイバー・セキュリティを巡る国家間の紛争が生じてきていること。

以下、(2)において、知的財産権を巡る米中関係の動向をレビューした上で、(3)において、上記①、②に係る問題の整理を行う。

## (2) ITに関わる知的財産を巡る米中関係の動向

### ①知的財産権問題に係る国際的枠組みと米国の制度

知的財産権を巡る通商問題については、ソフトウェアなどのIT産業に関わらず、音楽・映像・ゲーム、あるいは、ハードウェア製品を巡る模倣品、あるいは知的財産制度の調和まで、以前から議論されてきており、既に国際的な枠組みが存在する。

知的財産に係る国際的な通商の枠組みとしては、TRIPS協定(Agreement on Trade-Related Aspects of Intellectual Property Rights)がある。同協定は、1994年に、貿易上必要とされる最低限の知的財産権の保護や、権利行使手続きの整備を加盟各国に義務付けることを目的とし、WTOが制定したマラケシュ協定の一部として制定されたものである<sup>17</sup>。なお、TRIP協定とは別に、2007年10月には、米国、EU、スイス、日本が、今後、知財権保護に関する新しい国際的枠組みである「模倣品・海賊版拡散防止条約(Anti-Counterfeiting Trade Agreement: ACTA、仮称)」を構築することを発表している<sup>18,19</sup>。

<sup>17</sup> 具体的には、①貿易システムの基本原則や、他の国際的知的財産関連合意の適用方法、②知的財産権の適切な保護方法、③知的財産権の執行方法、④WTO加盟国間の、知財を巡る論争の解決方法、⑤新システム導入の移行期における特別措置、の5点を定めている

[http://www.wto.org/english/thewto\\_e/whatis\\_e/tif\\_e/agrm7\\_e.htm](http://www.wto.org/english/thewto_e/whatis_e/tif_e/agrm7_e.htm)

<http://www.tuat.ac.jp/~crc/b/img/trips.doc>

<sup>18</sup> <http://www.eff.org/issues/acta>

[http://www.meti.go.jp/press/20071023001/001\\_press.pdf](http://www.meti.go.jp/press/20071023001/001_press.pdf)

<sup>19</sup> なお、知的財産権関係に係る国際組織としては、世界知的所有権機関(WIPO)がある。WIPOは、国際機関と参加国間の協力を通じた知財保護の促進に向け、調和の取れた国際的な知財保護システムを構築することを目的として1967年に設立された国連の特別機関で、全世界から150カ国以上が加盟している。WIPOは、特許協力条約(PCT)の国際事務局として、各種条約の申請処理に当たっており、同分野における過去の成果としては、1996年、WIPO著作権条約、およびWIPO実演・レコード条約が採択されたことなどが挙げられる。<http://www.wipo.int/portal/index.html.en>

このような中、米国においては、知的財産権に係る通商政策に関し、スペシャル 301 条 (Special 301) と呼ばれる独自の制度 (一方的措置) を有している。

これは、米国の 1974 年通商法 (The 1974 Trade Act) における、諸外国による知的財産権の侵害に対する制裁に関連した条項 (Section 182) であり、同条項は 1988 年の包括通商競争力法 (Omnibus Foreign Trade and Competitiveness Act) によって策定され、1994 年に施行開始されたものである。同条項では、以下のような枠組みを有している。

- ・ USTR は、適切な知的財産法を制定していない、適切で効果的な知的財産の保護を行っていない国等を特定し、これらの国に関する年次報告書を作成。同報告書では、知財権への取り組みが不足している国を、問題の大きな順に「優先国」 (priority foreign country)、「優先監視国」 (priority watch list)、「監視国」 (watch list) の 3 段階に指定。
- ・ 同報告書で優先国に選出された国に対しては、調査と交渉が行われ、当該国を優先国として指定するかどうか判断される。なお、優先国として指定された場合、米国との貿易相手国としての立場を剥奪するという措置が講じられる可能性がある<sup>20</sup>。

## ②中国の知的財産権問題 (海賊版問題) の動向

言うまでもなく、中国国内には CD、DVD、ブランド品などのコピー製品が蔓延しており、これらの事態は国際的にも問題視されている。

実際、米国通商代表部 (Office of the United States Trade Representative : USTR) が 2008 年 4 月 25 日に発表した、2008 年のスペシャル 301 報告書<sup>21</sup>においても、中国は、2006 年、2007 年に引き続き、優先監視国に指定している<sup>22</sup>。また、知財権侵害作品の取締りに関し、米国 USTR は、以前から中国と 2 国間協議を行っていたが、これらの協議では、知財権保護にかかる米国の懸念は解決されなかったため、2007 年 4 月、米国は、WTO に対し、「中国による知財権保護の取り組みは不十分であり、TRIPS 協定における同国の合意に反している」とする訴えを起こしている。2009 年 1 月 26 日、WTO の紛争解決パネルは同件に関する調査報告書を発表し、この中で、中国の知財保護体制は TRIPS 協定における合意と矛盾しているとの判断を下し、中国は著作権法と関税基準を改正するよう提言している<sup>23</sup>。

<sup>20</sup> [http://www.ustr.gov/Trade\\_Sectors/Intellectual\\_Property/Section\\_Index.html](http://www.ustr.gov/Trade_Sectors/Intellectual_Property/Section_Index.html)

<sup>21</sup> [http://www.ustr.gov/Document\\_Library/Press\\_Releases/2008/April/USTR\\_Issues\\_2008\\_Special\\_301\\_Report.html](http://www.ustr.gov/Document_Library/Press_Releases/2008/April/USTR_Issues_2008_Special_301_Report.html)

<sup>22</sup> [http://www.ustr.gov/Document\\_Library/Reports\\_Publications/2008/2008\\_Special\\_301\\_Report/Section\\_Index.html](http://www.ustr.gov/Document_Library/Reports_Publications/2008/2008_Special_301_Report/Section_Index.html)

なお、他に優先監視国に指定されている国は、ロシア、アルゼンチン、チリ、インド、イスラエル、パキスタン、タイ、ベネズエラの 8 カ国。

<sup>23</sup> [http://www.wto.org/english/tratop\\_e/dispu\\_e/362r\\_e.pdf](http://www.wto.org/english/tratop_e/dispu_e/362r_e.pdf)



また、2009年2月17日に、国際知的所有権協会（International Intellectual Property Alliance : IIPA）が USTR の官報での要請に応じて発行した提言書である<sup>24</sup>「Special 301 Review」でも、中国は世界で最も海賊版製品が多い国とされ、これまでに引き続き「優先的警戒リスト」の対象国となっている<sup>25</sup>。同報告書は、中国での海賊版に起因する損失は、2008年には35億400万ドルに上ったと推定している<sup>26</sup>。

中国における海賊版による被害の推移<sup>27</sup>

INDUSTRY	2008		2007		2006		2005		2004	
	Loss	Level	Loss	Level	Loss	Level	Loss	Level	Loss	Level
Motion Pictures <sup>2</sup>	NA	NA	NA	NA	NA	NA	244.0	93%	280.0	95%
Records & Music <sup>3</sup>	564.0	90%	451.2	90%	206.0	85%	204.0	85%	202.9	85%
Business Software <sup>4</sup>	2940.0	79%	2999.0	82%	2172.0	82%	1554.0	86%	1488.0	90%
Entertainment Software <sup>5</sup>	NA	NA	NA	95%	NA	NA	589.9	92%	510.0	90%
Books	NA	NA	52.0	NA	52.0	NA	52.0	NA	50.0	NA
TOTALS	3504.0		3502.2		2430.0		2643.9		2530.9	

※単位：100万ドル

このうち、ビジネスソフトウェアに関しては、2004年以降海賊版による市場損失率は年々低下しており、2008年の損失率は79%であった。しかし、損失額では、2008年の推定損失額は2004年（14億8,800万ドル）の約2倍の29億4,000万ドルと著しく増加しているとしている。なお、同報告書では、インターネット人口の増加と共に、インターネットやモバイル機器を利用したデジタルコンテンツの著作権侵害が悪化している点も指摘されており、オンライン上に掲載される音楽やビデオの著作権侵害率は99%であると推測されている。

③中国市場におけるマイクロソフトの取り組み

このような中、ビジネスソフトウェア市場の最大手である Microsoft は、この急速に拡大しつつある中国市場において、海賊版で悩んでいる企業の一つである。実際に、Business Software Alliance の調査によると、2007年の中国におけるソフトウェアの82%は非正規に購入されたものとされる<sup>28</sup>。また、2008年10月22日

[http://www.ustr.gov/assets/Document\\_Library/Press\\_Releases/2009/January/asset\\_upload\\_file105\\_15317.pdf](http://www.ustr.gov/assets/Document_Library/Press_Releases/2009/January/asset_upload_file105_15317.pdf)

なお、米国側のもう一つの主張である「中国国内における著作権侵害への刑事罰の緩さは国際法に違反する」については、退けられている。実際、中国の裁判所は2008年12月31日、Microsoftのソフトウェアを偽造したとして2007年に逮捕、起訴された計11人に対し、同国内における同様の事件の判決としては過去最長となる懲役1年半～6年半の実刑判決を下している。（後述）

[http://news.cnet.com/8301-10805\\_3-10130564-75.html](http://news.cnet.com/8301-10805_3-10130564-75.html)

<http://www.reuters.com/article/technologyNews/idUSTRE50Q1NX20090127>

<sup>24</sup> <http://www.iipa.com/rbc/2009/2009SPEC301COVERLETTER.pdf>

<sup>25</sup> <http://www.iipa.com/rbc/2009/2009SPEC301PRC.pdf>

<sup>26</sup> ただし、同報告書で推定の対象となっているのは、音楽およびビジネスソフトウェアのみ。

<sup>27</sup> <http://www.iipa.com/rbc/2009/2009SPEC301PRC.pdf>

<sup>28</sup> [http://www.mercurynews.com/ci\\_11345544?source=rss](http://www.mercurynews.com/ci_11345544?source=rss)

付 Guardian 紙の報道によると、中国に出回る Microsoft の製品の 90%は海賊版であり、同社の利益を著しく侵害しているとのことである<sup>29</sup>。

このような中、同社は、2006年、一般的な海賊版対策として、海賊版対策プログラム「Genuine Software Initiative<sup>30</sup>」を立ち上げ、①消費者や再販業者に対する、海賊版の利用に伴うリスクなどに関する教育の徹底、②偽造対策技術や、そのような技術を盛り込んだ製品への投資の拡大、③偽造製品対策にあたっての、政府や警察機関への協力提供、の3つの活動を開始した。

しかしながら、中国では、同プログラムの開始以降も、同社製品の海賊版の製造・流通が続いてきたため、同社は、こうした対応等<sup>31</sup>と平行して、特に、中国当局・司法当局の全面的な協力を得て海賊版対策を進める一方で、中国当局に対して、中国に対する多額の技術面での投資を約束している。

- ・ 2006年3月、中国情報産業部、国家版權局、中国商務省は、「国内で生産されるコンピューターに対し、販売前に正規のソフトウェアをインストールする」よう要求する回覧を共同で発表するとともに<sup>32</sup>、また、同年4月10日には、州・地方政府に対し、正規版のソフトウェアがプレインストールされているコンピューターの購入を義務付ける発表を行った<sup>33</sup>。これに伴い、Microsoft は、中国市場の 65%を占める Lenovo 等の大手コンピューターメーカーら<sup>34</sup>との間で、同社の OS ソフトウェアをプレインストールするという点で合意している<sup>35</sup>。これにより、同社は、約 16 億ドルに相当する正当な OS ソフトウェア売上を計上できるとされている<sup>36</sup>。なお、この直後の同年4月18日、Microsoft は、訪米中の胡錦濤国家主席との間で中国政府に対する経済・IT 開発支援に関する覚書を交わしており、同覚書には、同社がその後5年間にわたり、年間7億ドルに相当するハードウェアを中国国内の

<sup>29</sup> <http://www.guardian.co.uk/world/2008/oct/22/microsoft-china>

<sup>30</sup> <http://www.microsoft.com/genuine/default.aspx?displaylang=en>

<sup>31</sup> それ以外にも、同社は、ここ数年の間で、中国に特化した海賊版対策を講じている。その1つとして、2005年にコピーソフトのユーザーに対し、コピー製品の入手経路を明らかにすることを条件として正規ソフトを半額で提供するというキャンペーンを行った。また、2007年と2008年にも、中国の平均年収と比較してソフトウェア価格が高額であることに着目し、2年連続で無条件での大幅値下げを行っている。

[http://news.cnet.com/2100-1016\\_3-5598882.html](http://news.cnet.com/2100-1016_3-5598882.html)

<http://arstechnica.com/microsoft/news/2007/08/shocker-microsoft-combats-chinese-piracy-via-major-price-cuts.ars>

[http://www.chinadaily.com.cn/china/2007-08/07/content\\_5448926.htm](http://www.chinadaily.com.cn/china/2007-08/07/content_5448926.htm)

<sup>32</sup> [http://english.gov.cn/chinatoday/2006-04/27/content\\_267503.htm](http://english.gov.cn/chinatoday/2006-04/27/content_267503.htm)

<sup>33</sup> [http://english.gov.cn/2006-04/10/content\\_250418.htm](http://english.gov.cn/2006-04/10/content_250418.htm)

<sup>34</sup> Founder、TCL、Tsinghua Tongfang、Redmond など。

<sup>35</sup> [http://english.gov.cn/chinatoday/2006-04/27/content\\_267503.htm](http://english.gov.cn/chinatoday/2006-04/27/content_267503.htm)

<sup>36</sup> 実際、Microsoft China の副社長である Pamela S. Passman 氏は 2006年4月16日、Xinhua 紙とのインタビューに対し、「中国はこれまで知財権保護の取り組みに関して大きく前進しており、MS は中国と長期的な協力関係を築いていきたい」とする声明を発表している。

[http://english.gov.cn/chinatoday/2006-04/16/content\\_255428.htm](http://english.gov.cn/chinatoday/2006-04/16/content_255428.htm)

企業からの購入するほか、中国のソフトウェア会社、およびソフトウェア開発関連の研究開発やトレーニングなどに対し、それぞれ1億ドルを投資するという内容が含まれている<sup>37</sup>。

- ・ Microsoftは、中国公安省やFBIに対して海賊版製品に関する情報提供を行うなど、両国の捜査当局と違法製品の取締りに向けた協力体制も構築している。この結果、2007年7月、中国公安省とFBIは中国広東省で同社製品の大量の違法コピーを行っていた偽造シンジケートの摘発に成功している<sup>38</sup>。同団体は20億ドル相当の違法な同社製品の製造・流通に携わっていたとされる<sup>39</sup>。なお、同件の容疑者11人に対しては、広東省深川の人民法院（People's Court）が2008年12月31日、懲役1年半～6年半と、中国国内で起こった同様の事件では最高となる実刑判決を下している<sup>40</sup>。なお、Microsoftは、これに先立つ、2008年11月には、中国における研究開発費として今後3年間に総額10億ドル以上投資すると発表している<sup>41</sup>。

なお、Microsoftは、2008年秋、新しい海賊版対策ツール<sup>42</sup>として、コピー製品が検索された場合、ユーザーのデスクトップを1時間おきにブラックアウトさせる措置を導入しているが、この措置を巡っては中国国内では大きな波紋が巻き起こった<sup>43</sup>。

<sup>37</sup> なお、両者は2002年6月にも、中国のソフトウェア市場の発展を目的とし、教育、トレーニング、研究協力、ハードウェア製造のアウトソースなどの面において、その後3年間で7億5000万ドルの投資を行うとする覚書に調印している。<http://www.microsoft.com/presspass/press/2002/jun02/06-27chinapr.mspx>

<sup>38</sup> <http://www.microsoft.com/presspass/press/2007/jul07/07-24CounterfeitingSyndicatePR.mspx>  
[http://www.usatoday.com/tech/products/software/2007-07-24-fbi-china-pirate-software\\_N.htm?csp=34](http://www.usatoday.com/tech/products/software/2007-07-24-fbi-china-pirate-software_N.htm?csp=34)  
<http://www.nytimes.com/2007/07/25/business/worldbusiness/25soft.html>

<sup>39</sup> <http://www.microsoft.com/presspass/press/2007/jul07/07-24CounterfeitingSyndicatePR.mspx>

<sup>40</sup> <http://www.nytimes.com/2009/01/01/business/worldbusiness/01soft.html>

<sup>41</sup> <http://www.microsoft.com/presspass/press/2008/dec08/12-31ChinaSentencingPR.mspx>

<sup>42</sup> <http://japan.cnet.com/news/biz/story/0,2000056020,20385979,00.htm>

<sup>43</sup> 同ツールは、コンピューター内のファイルやシステムがコピーされたものであるかを探知するもので、コピー製品検索の過程でコンピューターに関する特定の情報を記録し、コピー製品がインストールされている事が判明した場合、ユーザーへの通知を行うというもの。

[http://www.usatoday.com/tech/news/2008-10-26-microsoft\\_N.htm](http://www.usatoday.com/tech/news/2008-10-26-microsoft_N.htm)

<sup>43</sup> この対策を巡っては、「MSには、ユーザーの許可なくハードウェアをコントロールする権限はない」、「法的権限もユーザーの同意もなくコンピューターを検索することは、ハッカー行為と等しい」、「MSは、海賊版の利用者だけでなく、正規品利用者に対してもハッカー行為を行っている」、などユーザーからのMS批判が巻き起こった他、中国ソフトウェア協会（China Software Industry Association: CSIA）も、MSに対して法的措置を講じることを検討しているという。また、中国人弁護士はこの件に関し、正規ソフトの利用者に対してもハッキングを行ったとし、10億ドルの損害賠償を起すとしている。

[http://www.usatoday.com/tech/news/2008-10-26-microsoft\\_N.htm](http://www.usatoday.com/tech/news/2008-10-26-microsoft_N.htm)

<http://www.guardian.co.uk/world/2008/oct/22/microsoft-china>

[http://www.chinadaily.com.cn/bizchina/2008-11/14/content\\_7205213.htm](http://www.chinadaily.com.cn/bizchina/2008-11/14/content_7205213.htm)



(3) インターネットの進展に伴う新たな通商・外交問題

上記の知的財産権を巡る問題に加え、近年、インターネットが普及・進展し、情報が国境を越えてグローバルに駆け巡る中、ITに関して、新たな通商・外交問題が生じてきている。

① インターネット規制・検閲を巡る国際的調和に係る問題

世界各国とも、それぞれの社会・経済的経緯を背景に、多かれ少なかれ、インターネット上で流通される情報・コンテンツに対する何らかの規制が行われている。ただし、それらの範囲や規制の方法は、米国と中国では全く異なると言える。

具体的には、米国においては、一般的には、通信の自由や表現の自由が確立されており、インターネットで流通される情報・コンテンツは、自由であるべきとされている。従ってそのような情報・コンテンツに対する制限は限定的であり、かつ民間の自主規制に大きく依存している<sup>44</sup>。これに対し、中国においては、国家の名誉や体制の維持に影響を与えるようなコンテンツも規制対象になり、また、それらは、政府によってチェック（検閲）され、アクセスが制限されるとともに、それらの違反は犯罪捜査の対象となる<sup>45</sup>。

米国・中国におけるインターネット規制（検閲等）の比較<sup>46</sup>

	米国	中国
規制対象（アクセス制限対象）	<ul style="list-style-type: none"> <li>・ 性的情報、暴力を促進する情報</li> <li>・ 知財権を侵害する情報等</li> </ul>	<ul style="list-style-type: none"> <li>・ 国家安全を危機に晒す情報等、国家の名誉を汚す情報等</li> <li>・ 国家統一を揺るがす情報等、社会の安定を揺るがす情報等</li> <li>・ 性的情報、暴力を広める情報</li> <li>・ その他法律で禁止する情報</li> </ul>
規制主体（アクセス制限主体）	<ul style="list-style-type: none"> <li>・ 主として企業による自主規制（ただし、児童ポルノを除く）</li> </ul>	<ul style="list-style-type: none"> <li>・ 政府による直接規制</li> <li>・ 企業によるフィルタリング規制等（政府の指示に基づく）</li> </ul>
犯罪者捜査等のための検閲、当局への情報提供	<ul style="list-style-type: none"> <li>・ 愛国者法に基づく盗聴</li> <li>・ 犯罪捜査のための企業への情報提供依頼</li> </ul>	<ul style="list-style-type: none"> <li>・ 犯罪捜査のための盗聴・モニタリング（上記規制違反の発見を含む）</li> <li>・ 犯罪捜査のための企業への情報提供依頼（上記規制違反者を含む）</li> </ul>

<sup>44</sup> ニューヨークだより 2009年1月号参照。

<sup>45</sup> なお、これらの犯罪捜査を含む規制対象は、原則としては、各国とも、サーバーの立地主義であり、国内にサーバーを立地した企業に対する規制、情報提供要求という形式をとる。一方、インターネットを通じて、情報・コンテンツがグローバルに流通される中、世界的には、(米国のような)最低基準の国の規制の情報が世界中に流通されることになる。このため、(中国のような)規制基準の高い国においては、そもそもネットワーク段階での、国内への情報の流通そのものの制限をかけることが特徴であると言える。

<sup>46</sup> 筆者作成。

このように、米中間でインターネットに係る規制・検閲に係る基準等が大きく異なる中、米国においては、中国に対して、以下のような問題意識がある。

- ・ 人権的発想・民主化の推進の観点から、中国国民が自由に情報を入手できないことに対する問題意識（特に、米国発の情報を中国国民が入手できていないことに対する不満）。
- ・ ビジネスの観点からは、これらの規制の違いが、米国企業にとって非関税障壁となっているという問題意識。すなわち、海外からの中国へのインターネット・サービス提供した場合、当局によって恣意的に止められることにより、ビジネスに支障が生じ、また、中国国内に参入した場合は、中国の国内法制に対応するが故に、上記中国の検閲等の協力を受けているとの米国内で批判を受け、ビジネスを行いつらい状況にある。

一方、このような規制に関し、電気通信サービスなどに係る WTO のサービス貿易の一環として国際的な枠組みはあるが、このようなコンテンツ規制に係る基準、手法の調和に係る国際的な交渉枠組みは存在しない。

## ②国際的なサイバー・セキュリティへの対応に係る問題

国家間の国家安全保障に関しては、従来より、国内重要施設等に対する破壊活動に対する防衛に加え、国防上だけでなく、外交上、あるいは場合によっては企業秘密に係る各種の諜報活動が互いに行われている。

近年のインターネットの進展と IT システムの重要性の増大に伴い、これらの活動がインターネットを通じて行われるようになってきており、このため、米国においては、サイバー・セキュリティの強化が喫緊の課題となっている。

その際、米国においては、中国からのハッキング等が問題になっている模様である。この背景としては、以下の二つの見方ができる。

- ・ ①もともと、政府 IT システム等の状況等に関し、米中両国に非対称性が存在すること。すなわち、米国政府においては、システムの IT 化が進展しているため、中国から見ると、ハッキングによって情報を入手することによって、国防、外交上優位に立つことが可能であるとともに、この方法は、米国が圧倒的に優位を有する軍備等において直接的に対抗することと比較して、圧倒的に低コストであること。
- ・ ②また、中国当局は、上述のとおり、国内外の情報を検閲すべく、インターネットを通じて情報を入手する技術的能力を高めているが、その延長で、米国政府の機密情報の入手を試みていることという可能性があること。

一方、サイバー・セキュリティに係る国際的な枠組みについては、現時点で存在しないとの指摘もある。また、技術の輸出という観点からは、既に、安全保障

の観点からの武器輸出禁止のレジームなどにおいて、一部情報セキュリティ技術が含まれ<sup>47</sup>、また、暗号に係る輸出規制に係る枠組みなどは存在する。しかしながら、サイバー・セキュリティ対策においては、トータルな管理が求められるため、今後、更なる動きが起きる可能性も否定できない。

### ③中国における強制認証（CCC）問題

上記には直接関係はしないものの、関連する事項として、中国における強制認証（China Compulsory Certification：CCC 制度）<sup>48</sup>制度を巡る動きがあげられる。

2008年1月、中国国家品質監督検査検疫総局（General Administration of Quality Supervision, Inspection and Quarantine）および中国質量認証中心（China Quality Certification Centre）は、2009年5月以降、以下の8カテゴリー13製品に該当する情報セキュリティ製品も強制認証の対象に含めることを発表した<sup>49</sup>。

これらの技術は、上述のインターネット検閲やサイバー・セキュリティにも強く関連する技術であり、本通達が施行されると、米国の民間企業等の情報セキュリティ技術が、強制認証の手続き・プロセスを通じて、中国当局等に流出する可能性・懸念が考えられる。

新たに CCC の対象にするとされた情報セキュリティ製品<sup>50</sup>

製品カテゴリー	製品名	CCC 実施規定
境界セキュリティ	ファイアウォール製品	CNCA-11C-074
	ネットワーク安全隔離カード（network secure separation card）、およびラインセレクター製品	CNCA-11C-075
	安全隔離カード、および情報交換製品	CNCA-11C-076
コミュニケーション・セキュリティ	セキュアルーター（secure router）製品	CNCA-11C-077
認証、およびアクセスコントロール	スマートカード COS 製品	CNCA-11C-078
データセキュリティ	データバックアップ、リカバリー製品	CNCA-11C-079
基本プラットフォーム	安全動作システム	CNCA-11C-080
	安全データベースシステム	CNCA-11C-081
コンテンツセキュリティ	スパム対策製品	CNCA-11C-082
評価、監査、モニタリング	IDS	CNCA-11C-083
	ネットワーク脆弱性スキャナー製品	CNCA-11C-084
	セキュリティ監査製品	CNCA-11C-085
アプリケーション・セキュリティ	ウェブサイトリカバリー製品	CNCA-11C-086

<sup>47</sup> <http://www.access.gpo.gov/bis/ear/pdf/ccl5-pt2.pdf>

<sup>48</sup> なお、中国のこの独自の強制認証（China Compulsory Certification：CCC）制度は、2003年8月から、導入されている。これは、外国企業が中国に輸出したり販売したりする製品の一部に対して同国政府の強制認証を義務付けるものであり、現在、人間の健康・環境・動物・もしくは国家の安全に関連する製品で、19グループの132製品カテゴリーが対象とされている。（コンピューターやサーバーなども含む。）

<sup>49</sup> <http://www.ccc-us.com/ccc.htm>

<sup>50</sup> <http://www.ccc-us.com/ccc.htm>

本件に関しては、「米中商業・貿易に関する共同委員会（U.S.-China Joint Commission on Commerce and Trade : JCCT）」にて取り扱われ、2008年9月、中国側はITセキュリティ製品に対するCCCの最終的な規制内容の発表を、米中間での相互同意が締結されるまで延期することに合意している<sup>51</sup>。また、2008年10月、WTO/TBT会合において、米国側は質問とコメントを提出している<sup>52</sup>。

しかしながら、本件については、産業界の動き<sup>53</sup>も含めて、米国内ではほとんど報道されておらず、また、国防総省、国土安全保障省などがどのように評価・判断しているのかについても不明である<sup>54</sup>。

以上を踏まえつつ、以下の章においては、上記①、②に係る米中間の関係・動向について記載する。ただし、これらのいずれも、必ずしも、新たな政策の方向が見えてきている訳ではないことに留意する必要がある。

### 3. 中国当局によるインターネット検閲・規制に係る米国の動向

#### (1) 中国におけるインターネット検閲・規制を巡る動向

##### ①中国における言論の自由と検閲・規制

中国においても、憲法によって、原則、言論、集会、出版の自由などが保障されてはいる。しかしながら、国家の利益がこれらの権利に先んじるとされるため、このような自由は実質的には制限されている<sup>55</sup>。また、メディアに関しても、新華通信社（Xinhua News Agency）などのメディアを国家が統制してきている<sup>56</sup>。

<sup>51</sup> [http://www.ustr.gov/assets/Document\\_Library/Reports\\_Publications/2008/asset\\_upload\\_file192\\_15258.pdf](http://www.ustr.gov/assets/Document_Library/Reports_Publications/2008/asset_upload_file192_15258.pdf)

[http://www.ustr.gov/assets/Document\\_Library/Press\\_Releases/2008/September/asset\\_upload\\_file882\\_15113.pdf](http://www.ustr.gov/assets/Document_Library/Press_Releases/2008/September/asset_upload_file882_15113.pdf)

<sup>52</sup> <http://www.wtcenter.org.tw/SmartKMS/fileviewer?id=97817>

<sup>53</sup> ソフトウェア情報産業協会（Software & Information Industry Association: SIIA）は、この件に関して中国政府に何らかの働きかけを行っている模様だが、同団体のスタンスや具体的な行動内容などの公式な情報は同協会メンバーのみへの公開となっており、具体的な情報は公開されていない。

<http://www.sii.net/govt/issue.asp?issue=CHIN#54>

<sup>54</sup> なお、本通達の実施に関し、2009年3月16日、中国側は延期する意向である旨、日本で報道されている（米国側では全く報道はない）。

<http://www.nikkei.co.jp/news/main/20090317AT2M1602816032009.html>

<sup>55</sup> <http://www.freedomhouse.org/template.cfm?page=251&year=2008>

<sup>56</sup> 具体的には、共産党の情報宣伝部（Central Propaganda Department）はメディア機関に対し、政治的にセンシティブ、且つ国家安全保障と共産党の支配への脅威となりうるトピックについて、その報道を制限する指示を出すなど、規制を行っている。報道規制の対象は、抗議活動、自然災害、チベット・台湾問題などから、共産党批判、プロパガンダに反するような視点の報道なども含まれる。

<http://www.cfr.org/publication/11515/#2>

インターネットについても、2000年10月に制定された「インターネット情報サービスの管理」に係る規則<sup>57</sup>において、インターネット情報サービス企業に対し、以下の9種類の情報内容に係る作成、再作成、発表、掲載を禁じている。また、もしウェブサイト上に禁止情報が掲載されていた場合、速やかに削除した上で関連情報を収集し、関連機関に通達するようにも定めている<sup>58</sup>。

インターネット上での掲載などが禁止されている情報・コンテンツ内容<sup>59</sup>

- 憲法で定められた基本原則に反する情報
- 国家の安全を危険にさらす情報、国家機密を暴露する情報、政府を転覆させる情報、国家の統一を揺るがすような情報
- 国家の名誉と利益を侵害する情報
- 民族憎悪や民族間差別を扇動する情報、その他、国家の統一性を揺るがす情報
- 宗教に関する国家の政策を批判、または、邪悪なカルトの教えを布教したり、封建的、迷信的な信仰を助長するような情報
- 噂を広め、社会の秩序を乱し、社会の安定を揺るがすような情報
- ポルノやその他猥褻なコンテンツなどを広めたり、賭け事、暴力、殺人、テロ行為を促進する、または犯罪を推進するような情報
- 他者を侮辱、中傷したり、他者の権利や利益を侵害するような情報
- その他、法律によって禁止されている情報

上記の規制に基づき、当局が「不適切」と判断した中国内外のウェブサイトについては、当局はキーワードを利用してニュースのフィルタリングを行うほか<sup>60</sup>、国内のインターネット全体について、必要なアクセスの遮断ができるように構成している<sup>61</sup>。（巨大なイントラネットであるとされる。）

<http://www.freedomhouse.org/template.cfm?page=251&year=2008>

<sup>57</sup> [http://www.novexcn.com/internet\\_law\\_2000.html](http://www.novexcn.com/internet_law_2000.html) (Article 15)

<http://www.networkworld.com/news/2008/051208-china-internet.html>

<http://www.greatfirewallofchina.org/faq/>

なお、それ以前に1990年代半ば頃から、特定の情報へのアクセス妨害などにより、ネット上に流される情報の規制が行われていたのではないかとされている。

<http://www.efa.org.au/Issues/Censor/cens3.html#china>

また、ハーバード大学法科大学院の研究者が2002年5～11月にかけて実施した調査によると、中国国内における、インターネットのフィルタリングは2002年9月以降急激に高度化したとのことであり、2000年のインターネット規制制定の2年後と、早い段階から検閲を行っている。

<http://cyber.law.harvard.edu/filtering/china/>

<sup>58</sup> なお、2002年にはISPに対して、政治的な内容を含む電子メールのスクリーニングを義務付け、ユーザーによる反体制的な内容のウェブサイトへの書き込みへの責任を問う内容の新法が施行されている。

<http://www.usatoday.com/tech/news/2002/01/18/china-internet.htm>

また、2005年には、2000年の「インターネット情報サービスの管理」に係る規制が改正され、コンテンツの監視の対象が、携帯電話のテキスト・メッセージ、電子メールといった通信内容や、ブログ、チャットルームにまで拡大されている。

<http://www.globalenvision.org/library/7/967>

<sup>59</sup> [http://www.novexcn.com/internet\\_law\\_2000.html](http://www.novexcn.com/internet_law_2000.html)

<sup>60</sup> [http://www.rsf.org/IMG/pdf/Internet\\_enemies\\_2009\\_2\\_.pdf](http://www.rsf.org/IMG/pdf/Internet_enemies_2009_2_.pdf)

<sup>61</sup> <http://cyber.law.harvard.edu/filtering/china/appendix-tech.html>

<http://arstechnica.com/old/content/2007/10/chinas-great-firewall-turns-its-attention-to-rss-feeds.ars>



## ②中国のインターネット規制・検閲を巡る最近の動き

### <最近のインターネット規制・検閲の事例>

中国のこのようなインターネット規制は、最近も、引き続き実施されており、特に規制緩和する方向にはない<sup>62</sup>。国境なき記者団が、2009年3月に発表した『Internet Enemies』<sup>63</sup>でも、ネット検閲やアクセス規制を行っている12カ国<sup>64</sup>のうちの1つとして、中国が取り上げられている。

同報告書によると、北京オリンピックの影響で、Wikipedia や YouTube などの英語版サイトはアクセス可能になったものの、これらの中国語版については依然としてアクセス規制の対象となっていると指摘されている。また、それ以外も、米国の国営ラジオ放送局 Voice of America、英国 BBC ニュースの中国語版サイトなどのほか、チベット問題、天安門事件、人権、民主主義、法輪功など、中国政府にとってセンシティブな情報を含むサイトが規制されているとされる<sup>65</sup>。

具体的に、最近の中国国内のウェブサイトに対する中国政府による検閲事例としては、例えば、以下のような事例が報道されている。

- ・ 有名な事例としては、2008年3月に中国のチベット自治区で起こった暴動を巡るアクセス遮断。当局はこの事件に関する情報を掲載したウェブサイトだけでなく、YouTube のような動画共有サイトや Google、Yahoo などの検索エンジンなどへのアクセスまで一時遮断した<sup>66</sup>。
- ・ また、同年5月、四川省にて大地震が発生した際も、インターネット上で政府の対応不備に関する議論が持ち上がると、当局は即座に検閲を強化<sup>67</sup>。
- ・ 最近では、2008年12月半ば、BBC、および米国の国営ラジオ放送局である Voice of America の中国語版サイトなどのページへのアクセスが数日間に渡

<sup>62</sup> 民主主義と自由の促進を目的とした超党派の NGO である Freedom House の 2008 年の発表によると、2007 年、中国当局は国内のジャーナリストやサイバー反体制派に対する厳しい取締りを実行し、この結果、同年末の時点で、少なくとも 29 人のジャーナリストと 51 人のサイバー反体制派が投獄されたとのことであった。Freedom House はこの人数について、世界でも最も多いとしている。

<http://www.freedomhouse.org/template.cfm?page=251&year=2008>

<sup>63</sup> [http://www.rsf.org/article.php3?id\\_article=30543](http://www.rsf.org/article.php3?id_article=30543)

<sup>64</sup> その他は、ミャンマー、キューバ、エジプト、イラン、北朝鮮、サウジアラビア、シリア、チュニジア、トルクメニスタン、ウズベキスタン、ベトナム。

<sup>65</sup> [http://www.nytimes.com/2008/12/23/world/asia/23china.html?\\_r=1&partner=rss&emc=rss](http://www.nytimes.com/2008/12/23/world/asia/23china.html?_r=1&partner=rss&emc=rss)

<sup>66</sup> [http://technology.timesonline.co.uk/tol/news/tech\\_and\\_web/article3568040.ece](http://technology.timesonline.co.uk/tol/news/tech_and_web/article3568040.ece)  
[http://www.nytimes.com/2008/03/17/business/media/17youtube.html?\\_r=1&ex=1363492800&en=09e3c9795934db40&ei=5088&partner=rssnyt&emc=rss&oref=slogin](http://www.nytimes.com/2008/03/17/business/media/17youtube.html?_r=1&ex=1363492800&en=09e3c9795934db40&ei=5088&partner=rssnyt&emc=rss&oref=slogin)  
[http://www.nytimes.com/2008/01/04/business/worldbusiness/04fobriefs-RESTRICTIONS\\_BRF.html?ex=1357102800&en=b4ea95f914fb62c9&ei=5088&partner=rssnyt&emc=rss](http://www.nytimes.com/2008/01/04/business/worldbusiness/04fobriefs-RESTRICTIONS_BRF.html?ex=1357102800&en=b4ea95f914fb62c9&ei=5088&partner=rssnyt&emc=rss)

<sup>67</sup> <http://blog.wired.com/27bstroke6/2008/05/deadly-earthqua.html>

って遮断された。これは、「"2つの中国"や、中国と台湾をそれぞれ独立した政権と見なすような書き方をしている情報」としていたためとされる<sup>68</sup>。

- ・ また、2009年1月20日に行われたオバマ新大統領の就任演説に際しては、生放送中、オバマ大統領が共産主義や、反対意見を抑圧しようとする検閲などに言及すると、突如放送画面が切り替わったほか、演説後の中国当局による翻訳版でも、上記に関する部分が削除された<sup>69</sup>。

なお、北京オリンピックを控えていた2008年夏においては、国際的世論に合わせる形で海外サイトの検閲を弱め、それまでは規制対象としていたBBC中国語サイトやNew York Timesなどの海外のニュースサイトを一部開放するなどの対応を行ったとされるが<sup>70</sup>、オリンピック終了後には再び検閲を強化しており<sup>71</sup>、同国政府の検閲に対する姿勢は基本的には変化していない。

#### <検閲・規制対象サービスの拡大>

また、これらの検閲、規制は、ウェブページや検索ページだけではなく、最近普及しつつある新たなインターネット・サービスにも広がっている模様である。

例えば、2008年7月、Twitterでの掲載内容が中国当局によって監視され、かつ、場合によっては同サービスの利用が制限されているとの報道がなされている<sup>72</sup>。また、同月、ソーシャル・ネットワーク・サービスであるFacebookが中国で利用できなくなったとの噂も報道されている（ただし、同報道を行ったCNETの中国

<sup>68</sup> New York Timesの12月16日付け記事によると、中国外務省Liu Jianchaoスポークスマンは記者会見の中で、「いくつかのサイトは、中国の法律に反する情報を掲載している」、「中国政府はこのようなウェブサイトへのアクセスを遮断する権利を有している」、「該当するウェブサイトには、自主制限を求める」との趣旨の発言を行っており、Jianchao氏は「中国の法律に反する情報」として、「"2つの中国"や、中国と台湾をそれぞれ独立した政権と見なすような書き方をしている情報」としている。

<http://news.bbc.co.uk/2/hi/asia-pacific/7785248.stm>

<http://www.nytimes.com/2008/12/17/world/asia/17china.html>

また、その3日後の2008年12月19日から21日にかけて、New York Times紙のウェブサイト全面に対し、中国国内からのアクセスが再び遮断されていると見られる状態が続いている、との報道がなされた。この件に関しては、中国側はコメントを発表していない。

<http://www.nytimes.com/2008/12/23/world/asia/23china.html?partner=rss&emc=rss>

<sup>69</sup> <http://www.msnbc.msn.com/id/28768271/>

なお、国内の各紙も同様に、共産主義や検閲に言及した内容は省略した上で記事を作成しており、各紙のインターネットサイトに掲載されている記事についてもこれらの情報は省略されている。

<sup>70</sup> <http://www.dailytech.com/China+Quietly+Unblocks+EnglishLanguage+Websites/article11413.htm>

ただし、五輪開催期間中も、人権擁護団体であるAmnesty Internationalは引き続きアクセス遮断の対象となっていたとの報道があり、その他のウェブサイトの中にもアクセス禁止の対象に含まれていたものがあると考えられる。

[http://www.amnesty.org.au/china/comments/media\\_freedom\\_in\\_china/](http://www.amnesty.org.au/china/comments/media_freedom_in_china/)

<sup>71</sup> <http://www.dailytech.com/PostOlympics+China+Turns+Its+Back+on+Internet+Censorship+Promises/article13716.htm>

<sup>72</sup> [http://www.businessweek.com/globalbiz/blog/eyeonasia/archives/2008/07/the\\_long\\_arm\\_of.html?campaign\\_id=rss\\_tech](http://www.businessweek.com/globalbiz/blog/eyeonasia/archives/2008/07/the_long_arm_of.html?campaign_id=rss_tech)

支社は、完全にブロックはされていないとしている)<sup>73</sup>。2008年8月には、音楽ストアのiTunesにおいて、チベット関連のアルバムへのアクセスができなくなったと報道されている<sup>74</sup>。更に、2008年10月には、IP電話等を運営するSkypeのサービスにおいて、中国における通信（チャット）内容が、中国当局に検閲（問題あるキーワードが含まれているかチェック）されているとのトロント大学が発表し、Skype側がその事実を認めたと報道されている<sup>75</sup>。

#### <ポルノ等有害情報に対する規制>

なお、上記政治的内容に係る規制とは別に、中国当局は、2009年1月には、インターネット上に流通するポルノなどについて、取締りキャンペーンを打ち立てた。具体的には、当局は下品なコンテンツやアダルトコンテンツを提供しているMSやGoogleの他、中国国内で最も人気のある検索エンジンを提供するBaiduなど19のウェブサイトを特定し、これらの企業に対してポルノの取締りを強化しよう通達した<sup>76</sup>。なお、実際にその後1250のサイトが閉鎖されたとされている<sup>77</sup>。

これについては、米国内では好意的な意見も少なくなく、賛否両論がなされている。

### （2）中国に進出する米国インターネット・サービス企業等を巡る動き

#### <米国インターネット・サービス企業による中国法人の設立>

中国においてインターネットが急速に普及する中、米国のインターネット・サービス企業にとって、中国市場の確保は重要な戦略の1つである。その際、上述の中国のインターネットに係る検閲・規制が障壁となっており、中国国外からサービスを提供するのではなく、中国国内に法人を設置してサービスを提供せざるを得ない場合があるとされる。

一般的に、インターネット・サービス企業が、中国市場に参入するにあたっては、①海外（米国）にサーバーを設置し、海外から中国向けのサービス（中国語）を提供する、②中国国内に子会社を設置し、サーバーも設置することにより、

<sup>73</sup> [http://news.cnet.com/8301-13577\\_3-9982616-36.html](http://news.cnet.com/8301-13577_3-9982616-36.html)

<sup>74</sup> <http://online.wsj.com/article/SB121939794188363329.html>

<sup>75</sup> <http://www.itmedia.co.jp/news/articles/0810/03/news027.html>

<http://www.redherring.com/Home/25138>

<sup>76</sup> [http://www.mercurynews.com/ci\\_11413565?source=rss](http://www.mercurynews.com/ci_11413565?source=rss)

<http://japan.cnet.com/marketing/story/0,3800080523,20386103,00.htm>

<http://www.nytimes.com/2009/01/06/world/asia/06pornography.html>

なお、豪州でも、同じような規制もあるとの報道もなされている。

[http://www.informationweek.com/news/internet/policy/showArticle.jhtml;jsessionid=4MAQDZ5ODIH1UQSNL0SKH0CJUNN2JVN?articleID=212700627&cid=RSSfeed\\_IWK\\_News&requestid=5893](http://www.informationweek.com/news/internet/policy/showArticle.jhtml;jsessionid=4MAQDZ5ODIH1UQSNL0SKH0CJUNN2JVN?articleID=212700627&cid=RSSfeed_IWK_News&requestid=5893)

64

<sup>77</sup> <http://www.foxnews.com/story/0,2933,482224,00.html>

中国向けのサービスを提供する、の二つの方法があり、その判断にあたっては、文化的な問題やローカライゼーションの問題などを考慮する必要がある。

しかしながら、結果的には、米国のインターネット・サービス企業の大手はどこも、中国国内に子会社を設立することによってビジネスを展開している。その要因の一つに、中国国外では、当局によって恣意的にアクセスが制限されることがあげられる。実際に、Googleは、当初、米国からサービスを提供していたが、アクセスがブロックされたり、あるいは、検閲技術のためアクセススピードが遅なったりするなどの問題が発生し、その間に中国国内企業のBaiduに先行を許したとされる<sup>78</sup>。

#### <中国政府当局との検閲に係る協力と批判>

一方、中国国内でビジネスを行うにあたっては、中国の法人として、中国の法律、当局の方針に従う必要がある。このため、各企業は、上述の同規則に違反する内容を掲載したユーザーに関する情報を当局へ提出することも含め、中国政府によるインターネット規制・検閲に従っている。

- ・ Googleは、2006年1月末、中国版の検索ウェブサイト Google.cn を正式に発足した<sup>79</sup>際、中国政府との間で検索結果の検閲（自動フィルタリングなどを使用、特定の言葉の検索結果が出ないような仕組み）に協力することで合意していることが報道された<sup>80</sup>。なお、同社は、中国国内ではインターネット検索（画像検索含む）しか提供していないが、これは、同社が他国で提供しているサービスのうち、電子メールやブログサービスなどについては、中国で展開すると中国当局への個人に対する検閲にまで協力せざるを得なくなるためである。
- ・ Microsoft<sup>81</sup>の広報担当者は、2006年1月、ZD Netに対し、中国政府の要求に応じて、政府批判を行った中国人ユーザーのブログ記事へのアクセス制限を行っていることを認めた<sup>82</sup>。同社は、以前から、中国政府の要求に応じる形で、中国政府に対する批判を行っていたブログをサーバーから削除していたほか、「民主主義」、「人権」、「台湾独立」などの政治的に敏感とされる用語が記述されているブログへのアクセスをブロックするよう設定してい

<sup>78</sup> 詳細は NY だより 2008 年 1 月号を参照。

<sup>79</sup> <http://www.nytimes.com/2006/04/23/magazine/23google.html?pagewanted=8&ei=5090&en=972002761056363f&ex=1303444800>

<sup>80</sup> <http://www.wired.com/science/discoveries/news/2006/01/70081>

これに関し、Google の Rachel Whetstone 氏は、2007 年 4 月、「Google が検閲に協力しつつも、言論の自由の促進に努力することは不思議ではない」と発言している。

<http://news.zdnet.co.uk/internet/0,1000000097,39288868,00.htm>

<sup>81</sup> 同社は、2005 年 6 月から「MSN Spaces」サービスを開始。

<sup>82</sup> [http://news.cnet.com/Microsoft-censors-Chinese-blogger/2100-1028\\_3-6017540.html](http://news.cnet.com/Microsoft-censors-Chinese-blogger/2100-1028_3-6017540.html)

るとされていたとされる<sup>83</sup>が、これをきっかけに、2006年1月末、ブログサービスの運営に関し、政府から特定の内容に関する記述のあるブログへのアクセス制限要請を受けた場合の対応方針を発表している<sup>84</sup>。これは、あくまで「現地の法律に従う」というもの。

しかしながら、そもそも中国における言論の自由やプライバシーの侵害に対して批判が強い中、米国IT企業が中国政府によるインターネット検閲へ協力していることについては、これらの行為に加担しているものとして、米国内から多くの批判が寄せられている<sup>85</sup>。また、特に、天安門事件15周年の報道に関連して機密漏洩罪で中国人ジャーナリストが10年の懲役刑に処せられた事件等に関しては、Yahoo!が同氏のメールのログイン記録を中国政府に提供したためであるとして、2007年4月に、Yahoo!は訴えられており、更に大きな批判を浴びた<sup>86</sup>。

### (3) 米国議会・連邦政府の反応と最近の動き

#### ①米国議会における動き

<中国のインターネット規制・検閲に対する法案（2002年～2005年）>

<sup>83</sup>[http://uscpublicdiplomacy.com/index.php/newsroom/specialreports\\_detail/200628\\_us\\_technology\\_companies\\_in\\_china\\_corporate\\_diplomacy/](http://uscpublicdiplomacy.com/index.php/newsroom/specialreports_detail/200628_us_technology_companies_in_china_corporate_diplomacy/)

<sup>84</sup>具体的には、以下の3つの場合においては、政府の要請に従う形でブログ記事へのアクセスに対する措置を講じる。

- ・そのブログ内容が、当該国の政府が規定する法律に反するとの通達をMSが受け取った際、または、MSの利用規定に違反する内容が掲載された際、MSはブログへのアクセスを遮断する。
- ・当該国政府による命令が下された際、その国の法律に従うため、当該国内のみにおいて該当するブログコンテンツへのアクセスを遮断する。
- ・該当刻の政府がブログコンテンツへのアクセス遮断をMSに命じた際、MSはコンテンツオーナーに対し、その理由を通達する。

<http://www.microsoft.com/presspass/press/2006/jan06/01-31 BloggingPR.msp>

<sup>85</sup>例えば、国境なき記者団(Reporters Without Borders)、その他米国主要メディアは、米国インターネット企業が中国におけるジャーナリスト糾弾に手を貸しているとして批判している。

なお、Google社に対しては、一部株主が、2007年5月株主総会で、「Googleは自ら検閲活動を行うべきではない」とする決議案を提出している。(ただし、この決議案は否決されている)

[http://news.cnet.com/2100-1038\\_3-6182997.html](http://news.cnet.com/2100-1038_3-6182997.html)

<sup>86</sup> NYだより2007年10月号参照。

なお、この事件を教訓に、Yahoo!は、捜査当局へのデータ提出に非常に気を遣っているとの事例が報道されている。2009年3月、ベルギーの地方裁判所は、Yahoo!がユーザー情報をベルギーの捜査当局の要求に応じず提出しなかったことについて、Yahoo!を有罪とした。しかしながら、これに対して、Yahoo!は、ベルギーに拠点を持たない企業であり、米国・ベルギー間の国際協定に基づき要請があれば提出したのに、それがなかったから提出しなかっただけだとして、上訴している。

<http://jp.techcrunch.com/archives/20090302yahoo-fined-by-belgian-court-for-refusing-to-give-up-e-mail-account-info/>



米国議会では、以前より、言論の自由の観点から、中国のような政府による国家的な検閲を問題視する見方がある。具体的には、2002年以降、ほぼ毎年、本件に係る担当部門の設置、毎年の議会の報告等を内容とする「グローバルインターネット自由法（Global Internet Freedom Act：GIFA）」が議会に提出されている<sup>87</sup>。しかしながら、これらの法案はいずれも成立に至っていない。

Global Internet Freedom Act（2002年～2005年）

提出日	ネット上の自由に係る内容
Global Internet Freedom Act ・ 下院 H.R. 5524 (02年10月2日 <sup>88</sup> ) ・ 上院 S. 3093 (02年10月10日 <sup>89</sup> ) ・ 下院 H.R. 48 (03年1月7日 <sup>90</sup> ) ・ 上院 S. 1183 (03年6月4日 <sup>91</sup> ) ・ 下院 H.R. 2216 (05年5月10日 <sup>92</sup> )	<ul style="list-style-type: none"> <li>・ 米国国際報道局（International Broadcasting Bureau the Office）<sup>93</sup>内に、国家的インターネット妨害に対す包括的な国際的戦略の構築にあたる、世界インターネット自由局（Office of Global Internet Freedom）を設置する。</li> <li>・ 同局に対し、インターネット使用への国家的妨害状況をまとめた年次報告書を議会に提出すると共に、米国がこの問題に対処するよう要求する。</li> <li>・ 米国議会は、以下3点を追求すべきであるとの姿勢を表明する。                         <ol style="list-style-type: none"> <li>(1) インターネット上の情報へのアクセスを制限、検閲、禁止、妨害する政府を批判するべきである、</li> <li>(2) 上記の行動を批判する決議を、国際連合に提出する、</li> <li>(3) 国家的インターネット検閲や、インターネット使用者の迫害を打倒するような技術を配備する。</li> </ol> </li> </ul>

<中国に進出する米国企業等を規制する法案（2006年～2008年）>

一方、2006年初において、上述のとおり、米国のIT企業が中国における検閲・規制に協力していると報道が多くなされる中、2006年2月15日、連邦下院人権小委員会は、Yahoo!、Microsoft、Google、Ciscoの代表を呼んで、中国のインターネット規制に関する公聴会を開催した。同公聴会では、潜在的市場として期待

<sup>87</sup> 同法案をこれまで積極的に提出してきている、Christopher Cox 下院議員は、「過去にいくつかの政府がパンフレットの配布の禁止やラジオ・TV放送の妨害を行ったように、現在、多くの政府がインターネットへのアクセスを遮断することで、人々が情報を自由に送受信することを妨げようとしている。同法案はこのような不正行為の終焉に役立つものであり、米国が言論・報道・連携の自由を支援するためには、全体主義的な政権によるインターネットの制御を打ち負かすための法律が必要である」といった趣旨の声明を発表している。

<http://www.techlawjournal.com/topstories/2002/20021010b.asp>

<sup>88</sup> [http://thomas.loc.gov/cgi-bin/bdquery/z?d107:h.r.05524:](http://thomas.loc.gov/cgi-bin/bdquery/z?d107:h.r.05524;)

<sup>89</sup> [http://www.thomas.gov/cgi-bin/bdquery/z?d107:s.03093:](http://www.thomas.gov/cgi-bin/bdquery/z?d107:s.03093;)

<sup>90</sup> [http://www.thomas.gov/cgi-bin/bdquery/z?d108:h.r.00048:](http://www.thomas.gov/cgi-bin/bdquery/z?d108:h.r.00048;)

<sup>91</sup> <http://www.govtrack.us/congress/bill.xpd?bill=s108-1183>

<sup>92</sup> <http://www.govtrack.us/congress/bill.xpd?bill=h109-2216>

<sup>93</sup> 国際報道局と、米国国防総省内にある放送理事会（Broadcasting Board of Governors）の傘下であり、敵対国、占領国、同盟国などに向け「Voice of America」をはじめとした親米的な放送を提供している。なお、02年10月10日提出法案のみ、商務省の電気通信情報局（NTIA）内に設立、となっている。

の高い中国においてビジネスを行っていくために、同国の法律等に遵守するあまり、米国の象徴といえる表現の自由と、それを実現するために必要とされる個人のプライバシー保護を放棄することの是非が問われた。同公聴会における企業代表の発言は、各社はビジネスを行う国・地域における法律に遵守しているだけであると現状説明に留まっている<sup>94</sup>。

その公聴会の翌日、Christopher Smith 下院議員は、Global Online Freedom Act (H.R. 4780)<sup>95</sup>を議会に提出している。同法案の特徴としては、これまでの同種の法案とは異なり、インターネット規制国の指定、米国企業における規制、輸出の規制等の一方的措置が含まれていることがあげられる。ただし、同法案も、最終的には廃案となっている<sup>96</sup>。

なお、最近の同種の法案としては、2007年1月に下院外交委員会に提出されたGlobal Online Freedom Act (H.R. 275)がある。具体的には、以下のような項目を掲げているが、同法案についても、結局、投票にかけられることなく、時間切れで廃案となっている。

#### Global Online Freedom Act (H.R.275) の要旨<sup>97</sup>

<ul style="list-style-type: none"> <li>1961年海外援助法 (Foreign Assistance Act of 1961) を改正し、諸外国における電子情報の自由度に関する年次評価を行う。</li> </ul>
<ul style="list-style-type: none"> <li>国務省に、電子情報の自由を促進し、外国政府によるインターネットの妨害に対する国際的戦略の構築に当たる、世界インターネット自由局 (Office of Global Internet Freedom : OGIF) を設置する。</li> </ul>
<ul style="list-style-type: none"> <li>ネット規制を行う国家で事業を行う米国企業に対し、個人を特定できるような情報を含む電気通信の本拠地設置を禁止する。</li> </ul>
<ul style="list-style-type: none"> <li>ネット規制を行う国家で、ネットを介して個人情報入手・収集する米国企業に対し、DOJの許可なく、個人情報を該当国政府に引き渡すことを禁止する</li> </ul>

<sup>94</sup> [http://www.informationweek.com/news/showArticle.jhtml?articleID=178600547;](http://www.informationweek.com/news/showArticle.jhtml?articleID=178600547)  
[http://select.nytimes.com/2006/02/19/opinion/19kristof.html?\\_r=1&n=Top/News/Business/Companies/Yahoo!%20Inc.&oref=slogin](http://select.nytimes.com/2006/02/19/opinion/19kristof.html?_r=1&n=Top/News/Business/Companies/Yahoo!%20Inc.&oref=slogin)

<sup>95</sup> Global Online Freedom Act(H.R. 4780)06年2月16日  
[http://thomas.loc.gov/cgi-bin/bdquery/z?d109:h.r.04780:](http://thomas.loc.gov/cgi-bin/bdquery/z?d109:h.r.04780)

同法案は、Christopher Smith 下院議員、他 14 名による共同提出。主な内容は、以下の通り。

- ・ 1961年海外援助法 (Foreign Assistance Act of 1961) を改正し、海外経済安全補助に関する条項において、各国の電子情報の自由度の評価を求めるよう改正する。
- ・ 国務省内に、電子情報の自由の強化に向けた特定の活動を行う、世界インターネット自由局を設置。
- ・ 大統領は、インターネット規制国を指定する。
- ・ 米国企業を対象として、海外におけるオンラインにおける自由の保護に関する最低基準を提供する。
- ・ インターネット規制国に対する輸出規制を行う。

<sup>96</sup> [http://uscpublicdiplomacy.com/index.php/newsroom/specialreports\\_detail/200628\\_us\\_technology\\_companies\\_in\\_china\\_corporate\\_diplomacy/](http://uscpublicdiplomacy.com/index.php/newsroom/specialreports_detail/200628_us_technology_companies_in_china_corporate_diplomacy/)

<sup>97</sup> [http://www.thomas.gov/cgi-bin/bdquery/z?d110:H.R.275:](http://www.thomas.gov/cgi-bin/bdquery/z?d110:H.R.275)

同法案は、Christopher Smith 下院議員、他 8 名による共同提出。

<ul style="list-style-type: none"> <li>• ネット規制を行う国家でサーチエンジンを作成・提供・ホストする米国企業に対し、フィルターや検索結果に影響を与えるような用語やパラメーターの提出を義務付ける</li> </ul>
<ul style="list-style-type: none"> <li>• ネットコンテンツをホスティングする米国企業に対し、ネット規制国に関する特定の規制情報をOGIFに提出するよう義務付ける</li> </ul>
<ul style="list-style-type: none"> <li>• ネット規制国において、ネットコンテンツをホスティングする米国企業に対し、米国がサポートするウェブサイトやコンテンツを妨害することを禁止する</li> </ul>
<ul style="list-style-type: none"> <li>• 同法で設定された規則に違反したものに対する罰則を設定する</li> </ul>
<ul style="list-style-type: none"> <li>• 顕著なインターネット規制を行っている国に対する、輸出規制品や輸出ライセンス要件の開発に関するフィージビリティ調査を実施する</li> </ul>

## ②連邦政府における動き

### <国務省、司法省の動き>

上記の議会における動きに対して、連邦政府（ブッシュ政権当時）は、インターネット上での言論の自由は保護されるべきであるとはしつつも、定義が不明確であり、かつ、一方的措置を含むような法制化には反対の意向を示している。

具体的には、2008年5月、国務省及び司法省は、下院外交委員会の議長に対し、同法案に反対の姿勢を示す書簡を提出している<sup>98</sup>。両省とも、同法は、米国の外交政策に多くの影響を与えるとの懸念を示し、具体的には、以下のような問題点を指摘している<sup>99</sup>。

- 「インターネット規制を行う国家」の定義が曖昧であり、例えば、ナチを否定する欧州諸国も対象になる可能性がある。
- 本法律を策定すると、外国が報復を行い、米国に情報提供の協力をしなくなる可能性がある。その結果、これらの国々においては、テロリストらが自由に情報交換を行う「サイバースタートランド」が構築される可能性もある。
- 米国企業は、「二流」国家とみなされた国から報復を受ける可能性がある。また、米国企業が、米国法と「ネット規制を行う国家」の相反する法律の両方を遵守しなければならないという不可能な状況に陥ってしまう。

一方、本問題が大きく取り上げられた2006年2月、ライス国務長官（当時）は、国務省内に「Global Internet Freedom Task Force (GIFT<sup>100</sup>)」を設立した。GIFTは、表現の自由と自由な情報の流れを最大化し、抑圧的な政権による検閲や討論

<sup>98</sup> <http://www.usdoj.gov/ola/views-letters/110-2/05-19-08-hr275-online-freedom-act.pdf>

<sup>99</sup> [http://news.cnet.com/8301-13578\\_3-9956124-38.html](http://news.cnet.com/8301-13578_3-9956124-38.html)

[http://news.cnet.com/8301-13578\\_3-9952815-38.html](http://news.cnet.com/8301-13578_3-9952815-38.html)

<http://japan.cnet.com/news/media/story/0,2000056023,20374430,00.htm>

[http://news.cnet.com/8301-13578\\_3-9952815-38.html?part=rss&subj=news&tag=2547-1\\_3-0-20](http://news.cnet.com/8301-13578_3-9952815-38.html?part=rss&subj=news&tag=2547-1_3-0-20)

<sup>100</sup> <http://www.america.gov/st/freepress->

<english/2008/July/20080715094516xjsnommis0.3989832.html>

の抑圧を最小化し、インターネット上の情報を促進することを目的とする<sup>101</sup>。  
GIFTは、2006年12月、以下の3点を優先事項とする世界的なインターネット自由戦略を策定しており、今後、その執行にあたって、他省庁や国家安全保障会議や国家経済会議などと連携するとしている。

- 世界各国におけるインターネットの自由に係るモニタリング（モニタリングの強化、大使館による報告の強化）
- インターネットの自由に対する挑戦への対応（問題を見つけたときの外国政府への懸念表明、会合・対話、他国との連携、多国間機関との連携等）
- インターネットへのアクセスの拡大によるインターネットの自由の促進（途上国へのインターネットアクセス支援（USAID等）、フィルタリングされていない情報の提供の促進、検閲に対応する先端技術へのグラント等）

なお、最近では、2008年度の国務省の予算内に、中国やイランなどのネット検閲を行う国が設定したファイアウォールなどに対抗するためのアンチ検閲ツール・サービスの開発資金1500万ドルが盛り込まれている<sup>102</sup>。

#### <産業界等の要請と USTR の動き>

また、産業界等においては、本件については、国際貿易上の非関税障壁として、国際間で対応してほしいとの意見が強い。

Googleは、「同社にとっての最大の国際貿易上の障害は検閲である」として、本件に関して何度かUSTRを訪問しているとしている（2007年6月時点）。これに関して、USTRのスポークスマンは、「ネット検閲は人権問題同様、本来ならば国務省管轄の問題となるが、この問題がもし国際貿易規定に違反しているとなれば、USTRが介入する可能性もある」と述べている<sup>103</sup>。その後も、2007年8月に開催されたコンファレンスの中で、グーグルのCEOであるEric Schmidt氏は、「表現の自由を守るために、各国政府はインターネット検閲を非関税障壁と捉えるべきだ」と呼びかけており<sup>104</sup>、また、2007年11月、言論の自由を擁護する団体であるCalifornia First Amendment CoalitionがUSTRに対し、中国のネット検閲は米国のインターネット企業のビジネスを妨げているとする訴えを、中国と

<sup>101</sup> <http://www.america.gov/st/texttrans-english/2006/December/20061220173640xjsnommis0.7082331.html>

<sup>102</sup> 同資金は、国務省が設定する計1億6400万ドルの「民主主義基金(Democracy Fund)」の一部。Defense News, "U.S. Launches Internet Anti-Censorship Effort," January 7, 2008. Obtained via Nexis.

<sup>103</sup> <http://www.foxnews.com/story/0,2933,286609,00.html>

<sup>104</sup> <http://japan.cnet.com/news/media/story/0,2000056023,20355385,00.htm>

WTOに提出するよう求める嘆願書を提出している<sup>105</sup>。しかしながら、その後同件を巡っての大きな動きは起こっていない模様である<sup>106</sup>。

### ③産業界等における最近の動き

#### <インターネット・サービス業界の動き>

米国インターネット・サービス企業においては、中国政府の検閲への協力に関する批判があることを受け、最近では自主規制に向けた取り組みを開始している。

2008年8月、Yahoo!、Google、マイクロソフトなどは、中国をはじめとするインターネット上での言論の自由が制限されている国における行動規範を作成することを発表し<sup>107</sup>、同年10月、法律関係の学術機関、人権擁護団体の他、YahooやGoogleなどのインターネット企業を含む24企業・団体が集結し、ネットユーザーの人権、言論の自由とプライバシーの保護を目指したイニシアチブである、「Global Network Initiative: GNI」が発足した<sup>108</sup>。GNIでは既に、

- 原則（言論の自由やプライバシーなどに関し、参加すべき企業が取り組むべき原則を規定）
- 実施ガイドライン（上記原則を実施するために、取り組むべき事項を規定）
- ガバナンス・説明責任・学習に関するフレームワーク（今後取り組むべき手順をフェーズ1～フェーズ3に分けて規定）

を策定している。

なお、Reporters without Frontiersは、2009年3月に発表した報告書において、GNIの取り組みを評価しつつも、どれだけ体制に変化を与えられるかについて、懐疑的な見解を示している<sup>109</sup>。

#### <Ciscoの動き>

一方、2006年議会の公聴会に呼ばれたIT大手企業4社のうち、Cisco Systemsについては、従来から、中国市場向けも含めてオンライン検閲を可能にするソフ

<sup>105</sup> <http://pcworld.about.com/od/industrynews/Group-wants-WTO-suit-filed-aga.htm>  
<http://www.computerworld.jp/news/trd/90829.html>

<sup>106</sup> なお、EUでは、ネット検閲を貿易障害の1つとして扱うよう求める採決が下されている。

また、中国政府は、WTOのもとで、2008年11月、Reuters、Dow Jones、Bloombergなどの金融情報配信企業に対し、今後、中国国内の報道機関と同等に事業が展開できるようにすることに合意したとされ、中国政府は今後、中国経済に関する報道の検閲が行いにくくなるだろうと予想されている。

[http://www.huffingtonpost.com/michael-a-santoro-and-wendy-goldberg/chinese-internet-censorsh\\_b\\_156212.html](http://www.huffingtonpost.com/michael-a-santoro-and-wendy-goldberg/chinese-internet-censorsh_b_156212.html)[0]

<sup>107</sup> <http://www.itmedia.co.jp/news/articles/0808/06/news066.html>  
[http://online.wsj.com/article/SB121790071076312259.html?mod=rss\\_whats\\_news\\_technology](http://online.wsj.com/article/SB121790071076312259.html?mod=rss_whats_news_technology)

<sup>108</sup> [http://www.globalnetworkinitiative.org/newsandevents/Diverse\\_Coalition\\_Launches\\_New\\_Effort\\_To\\_Respond\\_to\\_Government\\_Censorship\\_and\\_Threats\\_to\\_Privacy.php](http://www.globalnetworkinitiative.org/newsandevents/Diverse_Coalition_Launches_New_Effort_To_Respond_to_Government_Censorship_and_Threats_to_Privacy.php)

<sup>109</sup> [http://www.businessweek.com/technology/content/mar2009/tc20090312\\_381922.htm?campaign\\_id=rss\\_tech](http://www.businessweek.com/technology/content/mar2009/tc20090312_381922.htm?campaign_id=rss_tech)



トウェアを世界各国の市場で販売していると言われていた<sup>110</sup>が、特に、2008年5月、「中国国内で行われるネット検閲は同社に取ってのビジネスチャンスである」との内容を含んだ内部資料が流出したとの報道が流れ<sup>111</sup>、同社への批判は高まった<sup>112</sup>。しかしながら、同社は、上述のGNIには参加していない<sup>113</sup>。

#### 4. 中国からのハッキングと米国におけるサイバー・セキュリティを巡る動き

##### (1) 米国のサイバー・セキュリティと中国の関与

###### ①米国のサイバー・セキュリティ事案の動向

米国では、近年、サイバー・セキュリティが重要な課題になっている。この際、日本では、政府による情報セキュリティ対策としては、一般的には、企業等における個人情報を含む企業秘密の流出を中心としたセキュリティ対策の推進を念頭に置くことが多いが、米国では、連邦政府によるサイバー・セキュリティ対策とは、連邦政府における機密情報に対するハッキングや重要施設に対する攻撃に対する対応が中心に議論されている。

この連邦政府に対するサイバー・セキュリティ事案の数は、近年、急激に増加してきている。実際に、FISMA (Federal Information Security Management Act) に基づいて行われた OMB の報告によると、2007年における事案件数は、約1.3万件と、前年度の0.5万件の2倍以上に増加しており、その中でも、特に不正アクセスの件数は、不適切な使用と並んで急激に増加している<sup>114</sup>。

<sup>110</sup> [http://uscpublicdiplomacy.com/index.php/newsroom/specialreports\\_detail/200628\\_us\\_technology\\_companies\\_in\\_china\\_corporate\\_diplomacy/](http://uscpublicdiplomacy.com/index.php/newsroom/specialreports_detail/200628_us_technology_companies_in_china_corporate_diplomacy/)

<sup>111</sup> [http://www.washingtonpost.com/wp-dyn/content/article/2008/05/19/AR2008051902661.html?nav=rss\\_technology](http://www.washingtonpost.com/wp-dyn/content/article/2008/05/19/AR2008051902661.html?nav=rss_technology)

<sup>112</sup> <http://blog.wired.com/27bstroke6/2008/05/leaked-cisco-do.html>  
<http://blogs.law.harvard.edu/palfrey/2008/05/22/leaked-cisco-document-chinese-censorship-among-opportunities/>

<sup>113</sup> なお、同社は、2009年1月、今後も中国市場のあり方に沿ったビジョン・戦略を通じて中国市場でのビジネスを行っていくとし、同市場の重要性について明言している。

[http://en.ce.cn/Business/Enterprise/200901/14/t20090114\\_17957373.shtml](http://en.ce.cn/Business/Enterprise/200901/14/t20090114_17957373.shtml)

<sup>114</sup> ただし、「不正アクセス」のうちの85%は、機器の盗難、紛失に伴うものとされる。

連邦政府におけるサイバー・セキュリティ事案件数（US-CERT への報告件数）<sup>115</sup>

事件の種類	2005年度	2006年度	2007年度
不正アクセス（Unauthorized Access）	304	706	2321
サービス妨害（Denial of Services）	31	37	36
悪質なコード（Malicious Code）	1806	1465	1607
不適切な使用（Improper Usage）	370	638	3305
アクセスの試み（Scams/Probes/Attempted Access）	976	1388	1661
調査中（Under Investigation）	82	912	4056
総計	3569	5146	12986

ただし、同報告書を含め、連邦政府等のサイバー・セキュリティの観点からまとめたオフィシャルな報告書においては、これらの事案に係る中国の関与の可能性やその位置付けなどについてはまったく記載されていない。

②中国によるサイバー攻撃、ハッキングに係る報道

一方、報道記事においては、この連邦政府におけるサイバー・セキュリティの急増の背景には、中国あるいは中国政府によるハッキング等の行為があるのではないかと推測が多くなされている。例えば、2008年3月14日付け USA Today は、上記のセキュリティ事案の急増に関連し、中国による米国連邦政府の IT システムへの侵入に政府の焦点があたっているとの連邦政府関係者の話を紹介している<sup>116</sup>。また、最近では、2009年2月には、下院国土安全委員会の Bennie Thompson 議長が Bloomberg とのインタビューの中で、米国にとって主要なハッキングの脅威は中国であるとコメントするなど<sup>117</sup>、引き続き中国によるハッキングが続いていることを匂わせる発言を行っている<sup>118</sup>。

実際に、過去数年間、米国内では、中国によると見られる米国政府機関に対するハッキング等の事案が多く報道されている。これらを見ると、単なるオンライン上のハッキングだけではなく、米国政府の中国訪問時における物理的な情報入手や、連邦政府への機器納入を通じたハッキングなど事例も報道されている<sup>119</sup>。

<sup>115</sup>出典: OMB 報告書 (“Fiscal Year 2008 Report to Congress on Implementation of The Federal Information Security Management Act of 2002”) より。

[http://www.whitehouse.gov/omb/infocreg/reports/2007\\_fisma\\_report.pdf](http://www.whitehouse.gov/omb/infocreg/reports/2007_fisma_report.pdf)

なお、同報告書の 2008 年版には同じ表は掲載されていない。

[http://www.whitehouse.gov/omb/assets/reports/fy2008\\_fisma.pdf](http://www.whitehouse.gov/omb/assets/reports/fy2008_fisma.pdf)

<sup>116</sup>[http://www.usatoday.com/news/washington/2008-03-13-cybersecurity\\_N.htm](http://www.usatoday.com/news/washington/2008-03-13-cybersecurity_N.htm)

<sup>117</sup>[http://www.bloomberg.com/apps/news?pid=20601087&sid=aP7TPI\\_IQwFQ&refer=worldwide](http://www.bloomberg.com/apps/news?pid=20601087&sid=aP7TPI_IQwFQ&refer=worldwide)

<sup>118</sup>ただ、中国大使館は今回の Thompson 氏の発言に対し、米国政府へのサイバー攻撃に対する同国政府の関与を否定している。

<sup>119</sup>なお、連邦政府以外にも、ダルフール問題に関する啓蒙活動を行う NGO である Save Darfur Coalition が中国国内からのハッキング被害に遭った件について、2008年3月に、FBI が捜査を開始して

中国によると見られる米政府への主なサイバー攻撃の事例（2007年以降）

報道出典 ／時期	対象	報道・発表の概要	中国の反応
FOX News 報道(DOD 匿名者) 07年9月 <sup>120</sup>	DOD 07年 6月	<ul style="list-style-type: none"> <li>国防長官府の政策事務部門のコンピューターがハッキングされた。対象は、機密扱いされていない e-mail が含まれた部分で、運営上の安全には重要ではない分野。</li> <li>ハッキングが中国軍部によるものであると結論付けることはできなかったが、技術的に中国政府から来たものであると判断するに充分なほど技術的に高度なものであった。</li> <li>国防総省広報によると、同事件により、約3週間に渡ってコンピューターがオフラインになったという。</li> </ul>	中国外務省広報の Jiang Yu 氏は、定例会見で、報道の内容を否定。
下院国土 安全保障 小委員会 07年9月 <sup>121</sup>	DHS 06年 6月	<ul style="list-style-type: none"> <li>下院国土安全保障小委員会は、国土安全保障省（DHS）に対し、中国からのハッキング事例と思われる案件について詳細な調査を指示。</li> <li>同小委員会の調査によると、DHS の数十台のコンピューターがハッカーにより攻撃され、機密情報が中国語ウェブサイトへ移動していたこと、また、DHS のコントラクターである Unisys 社が、完全なシステムを導入していなかったことに加え、その情報を適切に DHS に提供していなかったこと等が指摘されている。</li> <li>同委員会はそのウェブサイトが中国政府のウェブサイトであったかどうかについてのコメントは控えている。</li> </ul>	ワシントンポスト紙によると、中国政府が米国へのハッキング疑惑を一切否定
DOE 研究 所発表 07年12月 <sup>122</sup>	DOE 研究 所 07年 10月	<ul style="list-style-type: none"> <li>DOE オークリッジ国立研究所は、全国で多くの研究所等で被害を受けていると思われる洗練された攻撃にあった。</li> <li>ハッカーは、同研究所からの公式を装ったメールを、同研究所職員に送信し、職員がメールに添付されたファイル、または添付の URL を開くと、ハッカーがそのコンピューター上の情報にアクセス可能になるというもの。機密情報は盗まれていないが、同研究所の訪問者の個人情報盗まれた。</li> <li>なお、Information Week による SANS Institute のディレクターへのインタビューによると、同手法は政府機関向けに多用されており、その情報は中国に流れている例があったとしている。</li> </ul>	コメントなし（在米中国大使館）。なお、同研究所も、犯人の特定は不可能とコメント
AP 通信報 道(匿名者) 08年3月 <sup>123</sup>	DOC 07年 12月	<ul style="list-style-type: none"> <li>商務長官の Carlos Gutierrez 氏が中国訪問中、米国の代表団が席をはずした間に、中国側が商務省のノートパソコンをコピーした可能性があり、それに基づき、政府のネットワークにハッキングしているという。実際に、US-CERT に侵入の報告が最低3回はなされているとのこと。</li> <li>商務省広報の Richard Mills 氏は、上記の点については調査が行われているため、予測的な答えを行うべきでないとし、コメントを控</li> </ul>	AP 通信は、中国大使館と中国総領事館にコメントを求めたものの、コメントな

いたとの報道もある。[http://www.washingtonpost.com/wp-dyn/content/article/2008/03/20/AR2008032003193.html?nav=rss\\_technology](http://www.washingtonpost.com/wp-dyn/content/article/2008/03/20/AR2008032003193.html?nav=rss_technology)  
<sup>120</sup> <http://www.foxnews.com/story/0,2933,295640,00.html>  
<sup>121</sup> <http://homeland.house.gov/press/index.asp?ID=268&SubSection=1&Issue=4&DocumentType=0&PublishDate=2007&issue=4>  
<http://www.cnn.com/2007/US/09/24/homelandsecurity.computers/index.html>  
<http://www.washingtonpost.com/wp-dyn/content/article/2007/09/23/AR2007092301471.html>  
<sup>122</sup> <http://www.informationweek.com/news/internet/showArticle.jhtml?articleID=204702720>  
<sup>123</sup> <http://www.cnn.com/2008/US/05/29/china.hackers/index.html>  
<http://wiredvision.jp/news/200806/2008060320.html>  
[http://news.cnet.com/8301-10784\\_3-9955375-7.html](http://news.cnet.com/8301-10784_3-9955375-7.html)

		<ul style="list-style-type: none"> <li>えた。</li> <li>なお、CNNによると、FBI や国土安全保障省（DHS）は、この件について調査を行っていないとしている。</li> </ul>	し。
FBI 08年5月 124	連邦 政府 各機 関	<ul style="list-style-type: none"> <li>FBI は、連邦政府に売られた中国製のネットワーク機器（シスコブランド）調査した結果、3500 台が偽造のものであったと発表した。これは、FBI の取り組み資料がネットに投稿されたことを踏まえて公表したもの。</li> <li>本調査は、中国政府あるいは犯罪組織が、偽造した機器を使って、政府の DB に不正アクセスしようとしている懸念に基づき実施されたとされる。ただし、ロイターの取材に対し、匿名の政府関係者は、脆弱にはなっていないと述べたとされる。</li> </ul>	（特になし）
Frank Wolf 下院議員 08年6月 125	Frank Wolf 下院議員 06年 4月	<ul style="list-style-type: none"> <li>中国の人権問題に関し、長年にわたり批判を行ってきた Frank Wolf 議員は、2006 年 4 月に、事務所のコンピューターがされ、FBI と相談したところ、中国から操作を行っていることが判明したと発表。コンピューターには、中国の反体制活動派に関する情報があったという。</li> <li>なお、本報道に関し、Chris Smith 議員も AP 通信に対し、同様の経験を発表。</li> </ul>	中国外務省 広報の Qin Gang 氏は、 否定。

しかしながら、いずれの事案についても、中国側はもちろん、米国連邦政府側も、オフィシャルには、中国側の関与あるいは事案の存在そのものを否定しており、真偽は不明であることに留意することが必要である。

### ③議会報告書における中国サイバー攻撃能力増強に係る懸念

一方、米中間に係る安全保障あるいは経済に係る最近の米国連邦政府の報告書においては、近年、中国におけるサイバー攻撃の能力増強について懸念する記述がなされてきている。

2008年3月に国防総省が米国議会に提出した、「中国の軍事力に関する年次報告書 2008」<sup>124</sup>では、近年、米国連邦政府を含む世界中のコンピューター・ネットワークが、中国を起源とする侵入に晒されているとし、具体的に2007年には、国防総省や他の連邦政府機関、防衛関連のシンクタンク、コントラクターが中国を起源とする侵入の被害を受けたほか、ドイツ、英国でも侵入の被害を受けているとしている。なお、これらの侵入実行者と、中国人民軍、あるいは、同国政府と

<sup>124</sup> <http://www.fbi.gov/pressrel/pressrel08/finch050908.htm>  
<http://japan.cnet.com/news/sec/story/0,2000056024,20373023,00.htm>  
[http://news.cnet.com/8301-10784\\_3-9941060-7.html](http://news.cnet.com/8301-10784_3-9941060-7.html)  
<http://www.technobahn.com/cgi-bin/news/read2?f=200804230005>

<sup>125</sup> <http://www.cbsnews.com/stories/2008/06/12/world/main4175658.shtml>  
[http://www.nytimes.com/idg/IDG\\_852573C40069388048257466000851ED.html](http://www.nytimes.com/idg/IDG_852573C40069388048257466000851ED.html)  
<http://wolf.house.gov/index.cfm?sectionid=34&parentid=6&sectiontree=6,34&itemid=1174>

<sup>126</sup> [http://www.defenselink.mil/pubs/pdfs/China\\_Military\\_Report\\_08.pdf](http://www.defenselink.mil/pubs/pdfs/China_Military_Report_08.pdf)  
[http://www.informationweek.com/news/security/attacks/showArticle.jhtml?articleID=212101227&cid=RSSfeed\\_IWK\\_News](http://www.informationweek.com/news/security/attacks/showArticle.jhtml?articleID=212101227&cid=RSSfeed_IWK_News)

のつながりははっきりしていないものの、人民軍が何らかに関与しているのではないかと推測を示している。

また、米議会が設置した「米中経済・安全保障関係検討委員会（U.S.-China Economic and Security Review Commission）」は、2008年10月、米中の二国間貿易・経済関係に関する年次報告書『U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION』を発表している<sup>127</sup>。

この中の「米国の国防に影響を及ぼすと見られる中国の活動」項目の中で、米国にとっては中国によるサイバー攻撃が大きな脅威となっていることを示す記述がある。具体的には、以下の内容を記載している<sup>128</sup>。

- まず一般論として、コンピューターとインターネットの利用の拡大が進む中、サイバースペースは米国の政府、経済において、重大な弱点となっていること。
- 中国は、このような米国のサイバースペースへの依存の状況を利用している可能性があること。その際、①サイバー作戦にかかるコストは、従来の諜報・軍事コストと比較して低いこと、②サイバー作戦のアクセス源の特定は、非常に困難であること、③サイバー攻撃は、敵を混乱させる事が可能であること、④サイバー攻撃について取るべきに関する法的枠組みが設立されていないこと、の4点が、サイバー作戦・攻撃に関する現状としてあげられる<sup>129</sup>。
- 中国は、サイバー戦争の能力の増強を積極的に志向しており、これは中国にとって、非対称的なアドバンテージとなっていること。この結果、米国の従来型の軍事力の優位性が失われる可能性があること。

なお、中国のサイバー戦闘能力の強化については、各種報道もなされている。例えば、2006年8月のGovernment Computer Newsの報道によると、中国は、米国DODの非機密情報のネットワーク（NIPRNet）から10～20テラバイトの情

<sup>127</sup> [http://www.uscc.gov/annual\\_report/2008/annual\\_report\\_full\\_08.pdf](http://www.uscc.gov/annual_report/2008/annual_report_full_08.pdf)

同報告書では400ページ以上に及び、①米中間の経済・貿易関係、②中国による、米国の国防に影響を及ぼすと見られる活動、③中国による、エネルギー・環境関連政策と活動、④中国による、外国での活動と対外関係、⑤中国における、メディアおよび情報統制、に関する包括的な報告がある。

[http://news.cnet.com/8301-1009\\_3-10107323-83.html](http://news.cnet.com/8301-1009_3-10107323-83.html)

[http://www.informationweek.com/news/security/attacks/showArticle.jhtml?articleID=212101227&cid=RSSfeed\\_IWK\\_News](http://www.informationweek.com/news/security/attacks/showArticle.jhtml?articleID=212101227&cid=RSSfeed_IWK_News)

<sup>128</sup> なお、個別具体論としては、以下のような記載もある。

・2002年に、中国によって、国防総省の情報システム機関であるUnited States Army Information Systems Engineering Commandやサンディア国立研究所などが攻撃された。

・また、米戦略軍Joint Task Force for Global Network OperationsのColonel Gary McAlum参謀総長による、「中国は戦争ツールの1つとしてのサイバー作戦の重要性を認識し、サイバー作戦に焦点を当てた資源やトレーニングの強化を行っている」との証言を引用するとともに、中国は現在、サイバー諜報プログラムを保有しており、同分野における能力は先端的であると結論付けている

<sup>129</sup> [http://www.uscc.gov/annual\\_report/2008/annual\\_report\\_full\\_08.pdf](http://www.uscc.gov/annual_report/2008/annual_report_full_08.pdf), P167.



報をダウンロードしたとされている<sup>130</sup>。また、SC マガジンの2008年1月の記事<sup>131</sup>によると、Mike McConnell 国家情報長官はニューヨーカー誌とのインタビューの中で、近年、中国政府や軍部のハッカーが、米国及びその同盟国政府のコンピューター／ネットワークにハッキングしていると指摘したほか、中国は米政府担当のハッカー40,000人を抱えていると述べたとのしている。

## (2) 連邦政府におけるサイバー・セキュリティ強化の動き

### ＜前ブッシュ政権でのサイバー・セキュリティ強化の動き＞

こうしたハッキング等のサイバー攻撃の増大に対応するため、連邦政府においては、昨年からの機密（非公開）の対策として、サイバー・セキュリティ対策を強化しつつある。

2008年1月、ブッシュ大統領（当時）は、Comprehensive Cyber Security Initiativeに係る大統領令に署名をした<sup>132</sup>。本大統領令に係る詳細は、機密情報として公表されていないが、連邦政府に対するサイバー攻撃を保護するため、国防総省のNSA（National Security Agency）等の諜報機関におけるモニタリングを強化する内容やTrusted Internet Computingなど12分野の取り組みを含む<sup>133</sup>と報道されている。また、2008年3月、2009年度予算要求でサイバー・セキュリティに対して前年比10%増の計73億ドルを要求しており<sup>134</sup>、また、同月には、シリコンバレーの企業家のRod Beckstrom氏を、DHSにおけるサイバー・セキュリティのトップ（国家サイバー・セキュリティセンター局長）に任命している<sup>135</sup>。

<sup>130</sup> <http://gcn.com/articles/2006/08/17/red-storm-rising.aspx>

<http://www.guardian.co.uk/technology/2008/nov/20/china-us-military-hacking>

<sup>131</sup> <http://www.scmagazineuk.com/US-cyber-war-with-China-Russia-says-New-Yorker-magazine/article/105428/>

<sup>132</sup> <http://www.washingtonpost.com/wp-dyn/content/article/2008/01/25/AR2008012503261.html>  
<http://opencrs.com/document/R40427/>

なお、サイバーセキュリティ予算の増大を踏まえ、最近、国防系のITベンダーが積極的に取り組みを進めていると報道されている。

<http://online.wsj.com/article/SB123733224282463205.html>

<sup>133</sup> [http://www.nextgov.com/nextgov/ng\\_20080801\\_9053.php](http://www.nextgov.com/nextgov/ng_20080801_9053.php)

具体的に、12分野としては、Trusted Internet Computing, Intrusion detection, Intrusion prevention, R&D, Situational awareness, Cyber counter intelligence, Classified network security, Cyber education and training, Implementation of information security technologies, Deterrence strategies, Global supply chain security, Public/private collaborationが報道されている。

<sup>134</sup> [http://www.usatoday.com/news/washington/2008-03-13-cybersecurity\\_N.htm](http://www.usatoday.com/news/washington/2008-03-13-cybersecurity_N.htm)

<sup>135</sup> <http://www.washingtonpost.com/wp-dyn/content/article/2008/03/19/AR2008031903354.html>

このような動きに関し、連邦政府は中国との関係について全く触れていないが、多くの記事は、これらの背景として、中国からの連邦政府に対するハッキングの深刻化があると報道している。

#### <オバマ政権におけるサイバー・セキュリティ対策の動向>

オバマ大統領は、選挙戦出馬時から、サイバー・セキュリティの強化及び大統領に直接報告する国家サイバー・アドバイザー（National Cyber Advisor）を設置することを公約に掲げており、また、就任後、2009年2月9日には、これまでのサイバー・セキュリティ政策の評価・見直しに着手している<sup>136</sup>。なお、米国連邦政府内のサイバー・セキュリティ対策に関しては、国防・諜報機関係の取り組みとその他の民生機関での取り組みに壁がある模様である<sup>137</sup>。

ただし、いずれにせよ、同政権でも、現時点では、中国に名指しにした政策や通商・外交政策としての対応は見当たらない。

このレポートに対するご質問、ご意見、ご要望がありましたら、tagui\_ichikawa@jetro.go.jp までお願いします。

なお、本レポートは、注記した参考資料等を利用して作成しているものであり、本レポートの内容に関しては、その有用性、正確性、知的財産権の不侵害等的一切について、執筆者及び執筆者が所属する組織が如何なる保証をするものでもありません。また、本レポートの読者が、本レポート内の情報の利用によって損害を被った場合も、執筆者及び執筆者が所属する組織が如何なる責任を負うものでもありません。

<sup>136</sup> NY だより 2009年2月号参照。

<sup>137</sup> 上述の Beckstrom 氏は、2009年3月5日、連邦政府のサイバーセキュリティ政策は NSA に牛耳られており、もっと民生系の省庁がリードすべきとの批判をして、同職を辞任している。

<http://online.wsj.com/article/SB123638468860758145.html>

<http://www.computerworld.jp/topics/gov/138129.html>

なお、翌週、3月12日、この後任に近いポストとして、Microsoft 社の Chief Trustworthy Infrastructure Strategist で、DOD の Cyber Crime Center 等での勤務経験を有する Philip Reitingner 氏が任命されている。

[http://news.cnet.com/8301-13578\\_3-10195176-38.html](http://news.cnet.com/8301-13578_3-10195176-38.html)