「グーグルに対するサイバー攻撃と中国との関係を巡る動向」

市川類＠JETRO/IPA NY

１．はじめに

Google は、2010 年 1 月 12 日、サイバー攻撃を受けたことを踏まえ、中国でのビジネスから撤退する可能性を示唆する発表を行った。本発表は、米国に限らず世界中において大きな話題となった。

米国の民間企業が、サイバー攻撃を受けたこと自体は、今に始まったものではない。しかしながら、今回の Google の件においては、Google という米国の IT の最先端を走る企業が攻撃を受けたということに加え、それに対する Google の対応が、これまでの民間企業の対応とは以下の 2 点で大きく異なっていたため、大きなインパクトを与えてきているものと考えられる。

① 今回 Google は、攻撃を受けた事実を公表するとともに、その攻撃源を中国であると特定したこと。これにより、今回の件も含めて、各紙が中国によるサイバー攻撃を巡る実態について、競い合って報道を行ってきており、サイバーセキュリティに係る関心が高まってきている。

② また、今回 Google は、サイバー攻撃と関連付けて、中国での検閲と中国でのビジネスとの関係に踏み込んだこと。これにより、インターネットの自由に係る議論が再度活発化し、米中間の外交・経済関係上の大きな論点の一つとなりつつある。

現時点においては、今後、本件によって引き起こされた各種の動きがどのように収束するのか不明である。しかしながら、このような問題意識の下、本報告書においては、今回の Google に対するサイバー攻撃と中国との関係を巡るこれまでの各種の動きについて、報告する。

２．今回のグーグルへの攻撃と中国との関係を巡る位置づけ

（１）今回の Google の発表内容とその背景

① Google の発表の内容

2010 年 1 月 12 日（15:00）、Google は、同社の公式ブログにて、「中国に対する新しいアプローチ」という文書を発表した。その主要な内容は、

・ Google は、中国を起源とするサイバー攻撃を受けた。これは言論の自由に係る問題である。
・ Google は、もはや中国の検閲を続ける意思がない。場合によっては、中国オフィスを閉鎖する。

との内容であり、具体的には、以下の通り[1]。

Google の発表文「中国に対する新しいアプローチ」要旨[2]

・ 12 月半ばに、Google は、中国を起源とする高度に洗練されたサイバー攻撃を受け、当社の知的資産が盗まれた。これは通常のセキュリティ案件とは異なる。
①この攻撃は、Google だけでなく 20 以上の大手企業を対象。（インターネット、金融、技術、メディア、化学セクター。現在これらの企業に連絡し、連邦政府とも連携して作業中。）
②攻撃者の主要目的は、中国の人権活動家の Gmail アカウントへアクセスすることであると示唆する証拠をつかんだこと。
③今回の攻撃とは別に、中国にかかる人権活動主導者の Gmail アカウント（米国、中国、欧州ベース）が、常に第三者によってアクセスされていることが判明したこと。
これは、ただ単にセキュリティと人権に関連する事項という問題ではなく、言論の自由に係るより大きな世界的な議論に係る問題である。

・ 我々は、2006 年 1 月に、Google.cn を立ち上げたが、その際、「新たな法律やその他の規制など、中国における状況を注意深くモニターし、もし、上記の目的が達成できないと判断した場合には、中国に対するアプローチを躊躇なく見直す」という方針を明確化していた。今回明らかになった彼らの攻撃と監視と、これまでのウェブでの言論の自由に係る制限に対する企てと併せて考えると、我々は、中国におけるビジネス運営の実現可能性を見直さざるを得ないとの結論になった。我々は、Google.cn における検索結果の検閲をもはや続ける意思はない、と決定した。今後数週間にわたって、我々は、法の枠内で（もしあるとすれば）フィルターなしでの検索エンジンの運営が可能であるとの前提にたって、中国政府と協議をするつもりである。我々は、この結果によっては、Google.cn と、場合によっては当社の中国オフィスを閉鎖することもありうると理解している。

② 今回の発表の背景と構図

[1]掲示したのは、SVP で Chief Legal Officer の David Drummond 氏。上記表明に関し、David Drummond 氏は、NYT 紙によるインタビューに、以下の通り、コメントしている。
・「Google の中国における収入は、あまり重要ではない（immaterial）。」しかしながら、Google は、急成長するインターネット市場での機会を実質上失うことは理解している。
・「もし、中国が主要市場になるのであれば、リスクはある。しかしながら、我々は、我々にとって耐えられない市場に対して、財政的な面での判断で居続けるという決定は行わない。」
・「もし、会社（Google）が、中国政府と合意することができなければ、中国での検索エンジンを閉鎖するかもしれないが、600 人以上の中国での従業員のいくつかは、保持し続けたい。」
http://www.nytimes.com/2010/01/13/technology/companies/13hacker.html
（なお、同氏は、CNBC によるインタビュー（動画）にも応えている。）
http://video.nytimes.com/video/2010/01/12/business/1247466517265/google-may-close-operations-in-china.html

[2] 出典：http://googleblog.blogspot.com/2010/01/new-approach-to-china.html より筆者作成。

上記の Google の発表は、世界中で大きな話題となっているが、米国国内での関心はとりわけ高い。例えば、1 月 12 日の Google の発表以降、1 月末までに、例えば、NYT 紙だけで 40 以上の関連する記事が掲載されている。

今回の Google の発表が大きな話題となっている背景としては、

・ そもそも Google は、中国への参入にあたって検閲が大きな障害となっており、不満を持っていたこと。
・ 一方、米中間全体を巡っては、「A.サイバーセキュリティ」と「B.インターネットの自由」を巡る課題が、従来から火種として存在していたこと。

が挙げられる。

このような中、Google へのサイバー攻撃をきっかけに、Google の中国に対する不満が爆発し、その結果、従来から火種として存在していた、米中間のサイバーセキュリティ、インターネットの自由を巡る議論に火がついたという構図であると理解できる。

＜Google の中国参入を巡る経緯[3]（Google の不満）＞

もともと、Google は、早期（2000 年頃）から中国語版は出し、中国でのビジネスにも先行していたが、米国内のデータセンターから提供するビジネス（Google.com）では、中国政府によるブロックによりビジネスが阻害された。このため、（やむなく）中国国内にデータセンターを置き、中国国内の法規制（検閲）を受ける Google.cn を 2006 年 1 月に立ち上げた。

しかしながら、Google が中国でのビジネス展開に手間取っているうちに、中国国内企業である Baidu に先行を許す結果となっている。中国の検索市場は、対前年比 28%増（2009 年 Q3）と大きく増大する傾向にあるが、その中で、現在の検索のシェアは、Baidu が 63.9%、Google が 31.3%の二強体制となっている[4]。

＜サイバーセキュリティとインターネットの自由を巡る米中関係[5]＞

一方、近年、米国では、サイバーセキュリティが大きな課題となっている。その際、連邦政府として名指しはしていないものの、中国からのサイバー攻撃（スパイ）が背景にあると言われており、特に最近では、2009 年 11 月の米中経済・安全保障レビュー委員会の報告書[6]では、中国のサイバースパイ、サイバウォーの能力増強に対する脅威を指摘している。このような中、DOD はサイバー司令部を 2009 年 10 月に設置するなど、対応を強化しつつある[7]。

---

[3] Google の中国市場参入を巡る経緯については、NY だより 2008 年 1 月号参照。
http://www.ipa.go.jp/about/NYreport/200801.pdf
[4] http://online.wsj.com/article/SB126333757451026659.html?mod=article-outset-box
[5] インターネット／セキュリティを係る米国・中国間の摩擦については、NY だより 2009 年 3 月号参照。
http://www.ipa.go.jp/about/NYreport/200903.pdf
[6] http://www.uscc.gov/pressreleases/2009/09_11_10pr.pdf
[7] NY だより 2010 年 3 月号参照。

また、米国では、従来より、人権問題、ビジネス等の観点から、中国の検閲政策については、不満が大きく、インターネット自由確保に係る法律が何度も議会に提出されており、また、Yahoo!が中国当局に中国人ジャーナリストにかかるログイン記録を提供した件については、大きな批判を浴びた。なお、最近では、2009 年 6 月、中国国内の PC に、フィルタリングソフト（Green Dam）を義務付けるとした規制案に対して、広範囲な検閲につながるものであるとして、米国は強く反対し、大きな話題となった（結局、中国側が撤回）[8]。

（２）今回の Google の発表に係る特徴とその影響

米国内では、これまでも民間企業等に対するサイバー攻撃の事例は多く報道されている。しかしながら、今回の Google の発表に関しては、サイバーセキュリティ、及び、インターネットの自由の両面に関して、従来の民間企業の場合とは異なった対応を取った点が特徴と言える。

このため、単なる一企業に対するサイバー攻撃の事例とみなされるのではなく、米中間の関係も含めて、大きな影響を与えている。

Ａ．サイバーセキュリティの観点

今回 Google は、サイバー攻撃の被害を受けたことを自ら発表し、その発信源が中国であると特定したことが特徴であると言える。

---

[8] 2009 年 6 月 9 日は、中国政府は同年 7 月 1 日以降に製造・販売される全てのコンピューターに、フィルタリング・ソフトウェアである「グリーンダム」を搭載させることを義務付けると発表した。
http://english.gov.cn/2009-06/09/content_1336077.htm
このグリーンダムは、子どもや青少年に悪影響を及ぼすとされるわいせつな画像や言葉を掲載する有害サイトをフィルターにかけ、閲覧できないようにするためソフトウェアであり、中国工信部が、2008 年 7 月、中国国内 2 社に対し制作を委託したものである。（なお、本ソフトウェアに関しては、青少年向けフィルタリングソフトを販売する米国の Solid Oak 社が、2009 年 6 月 18 日に著作権違反であると主張しており、その後 22 億ドルの損害賠償を求め訴えている。後述。）
http://www.nytimes.com/2009/06/09/world/asia/09china.html
http://www.afpbb.com/article/environment-science-it/science-technology/2612484/4276911
http://jp.wsj.com/Business-Companies/Technology/node_19944
しかしながら、本ソフトフェアの導入義務付けについては、米国を始め海外企業等からは、フィルタリング対象が広がり、広範な検閲となりかねないとの懸念・指摘がなされ、それを踏まえ、米国 USTR と商務省は 6 月 24 日に、本件の撤回を中国側に要請している。
http://japan.cnet.com/news/biz/story/0,2000056020,20395598,00.htm
また、本件については、国内ネットユーザーからも反対が非常に強かったこともあり、中国側は、7 月 1 日の当日、準備期間が短かったことなどとの理由により、無期限延長を発表するとともに、8 月 13 日には、搭載義務付けは見送ることとし、ただし、学校やインターネットカフェなど公共の場所のコンピューターに関しては、導入を継続して行うとした。
http://jp.reuters.com/article/topNews/idJPJAPAN-38800420090701
http://english.gov.cn/2009-08/13/content_1391011.htm

このため、これまでのところ米国のサイバーセキュリティ政策には、具体的にはあまり直結していないものの、米国内におけるサイバーセキュリティに係る認識が高まるとともに、（その後 Google は正式には何も発表していないのにも関らず）、各紙は、その発信源に係る調査や中国におけるハッカーを巡る状況等を競って報じてきている。

今回の Google の対応の特徴（サイバーセキュリティ面）

今回の特徴	従来の対応
・サイバー攻撃の事実を公開したこと。 今回の Google は、自らサイバー攻撃の事実を公開することに踏み切った。	これまで、連邦政府機関等がサイバー攻撃の被害を受けたとの報道は多くあったものの、民間企業における被害に関しては、攻撃があったとしても、民間企業側としては、その事実を自ら積極的には公開しないという通常の対応であった。
・攻撃源を中国であると特定したこと 今回 Google は、発信源が中国であると明示したこと[9]。	一般的にサイバー攻撃の源の特定は困難であり、このため、これまでサイバー攻撃の被害を受けた連邦政府機関等においては、全て発信源が中国らしいということは、匿名で述べていたものの、オフィシャルには断言を避けてきた。

しかしながら、そもそも発信源については、これまで連邦政府でさえ特定できなかったのと同様、司法権の及ばない（協力関係のない）中国においては、特定は困難であると考えられる。すなわち、仮に発信されたコンピューターを特定したとしても、それが本当の発信源なのか経由地なのかは、現地調査をしない限り、判断が困難であることに加え、仮には発信源となるコンピューターを特定したとしても、誰が誰の指示に基づいてそのコンピューターを操作したのかは、現地の司法当局の協力がなければ捜査は困難である。また、サイバー攻撃を仕掛けるようなハッカーは、当然ながらそれを熟知した上で攻撃を仕掛けているはずである。

このため、本件についても、各紙報道によると攻撃ルート等が絞り込まれつつあるものの、政府間では、米国側は中国側に対して調査・公開するよう要求するのに対し、中国側は事実無根だと主張する平行線の状況のままで推移している[10]。

[9] 今回の件において、Google は、サイバー攻撃が中国に係る人権活動家を対象にしていることから、その攻撃源は中国政府（あるいはその関係者）であると推定している。

[10] したがって、仮に本当に中国政府が関与していたとした場合、中国側が真面目に米国の主張を受け入れて調査（捜査）・公表することは想定しづらく、このまま平行線で推移するか、あるいは、スケープゴートを差し出すかという対応になるように思える。

また、上述の通り、根本的には、両国での司法間での協力が不可欠であると考えられるが、今回の Google の件も含めて両国とも互いに対する諜報活動を行っている模様であること、また、両国におけるサイバーセキュリティを巡る状況（NY だより 2010 年 3 月号参照）を踏まえると、少なくとも当面は困難であるように見受けられる。

また、その影響もあってか、米国政府内でも現時点で表立って関与しているのは主として国務省であり、サイバーセキュリティ関連当局（DOD、諜報当局、DHS 等）は、少なくとも表立っては関与していない。

Ｂ．インターネットの自由の観点

今回 Google は、サイバー攻撃を理由に中国の検閲問題を取り上げ、自らの中国事業から撤退可能性を示唆したことは大きな特徴であり、これは同社独自のガバナンス構造によるものである。

今回、この Google という一企業の意思決定が、米国、中国の両大国の政策に大きなインパクトを与え得たことは特筆に値する。特に、今後、仮に中国の検閲政策を多少なりとも変えることができたとしたら、Google のガバナンスは、同社のビジネスにとっても有効なものとして位置づけられることになろう。

今回の Google の対応の特徴（インターネットの自由の観点）

今回の特徴	従来の対応
・サイバー攻撃と検閲問題を絡ませたこと 今回 Google は、サイバー攻撃の対象が、中国の人権問題の活動家であり、その諜報（Gmail のハッキング）を目的としたものと想定されることから、中国政府が行う検閲の一環であるとの認識し、その検閲問題を改めて問題として提起したこと。	本来、中国からサイバー攻撃を受けたことと、中国の検閲問題（さらには中国事業の問題）とは別問題である。すなわち、もしサイバー攻撃自体を問題とするのであれば、中国に対して、サイバー攻撃をしないように求めることが筋論である。
・検閲問題を故に撤退可能性を示唆したこと 今回 Google は、企業としての将来市場・利益の確保よりも、同社独自の社是（Don't Be Evil）を重視したこと。 これは、同社の大きな意思決定において、同社是を作成した共同創業者が強く関与しているという Google の独自のガバナンスが影響している。	これまで、米国のインターネット企業は、中国の検閲問題を大きな問題としてきたものの、基本的には、（中国を含む）各国でビジネスを行うためには、悪法であっても各国の法に従わざるを得ないというのが基本的なスタンス。

また、今回の発表を期に、米国でのインターネットの自由に係る議論が再燃し、その結果、米中間におけるインターネットの自由を巡る対立が大きくなっており、今後の行方が注目される[11]。しかしながら、現時点では、米国国内で、他のインターネット企業が Google に追随している訳でなく、また、中国国内でも、検閲を廃止すべきとの世論が高まっている訳でも必ずしもないのが現況である。

以上を踏まえ、以下第 3 章、第 4 章においては、これらの 2 点の観点から、今回の Google の件を巡る動向について報告する。ただし、今後の Google と中国政府との交渉結果等により、今後の帰趨が大きく異なることに留意する必要がある。

[11] ただし、そもそも、インターネットの自由に関して、米中間は大きく対立しているように見えるものの、事実関係をみると、中国の行っている検閲活動と、米国を含む各国の行っている諜報活動及び有害情報規制は、本質的には程度問題の違い（規制対象とする情報の範囲、規制手法（事前、事後）の違い）であるとの見方もすることはできること（NY だより 2009 年 3 月号 P9 参照）に留意する必要がある。

３．Google へのサイバー攻撃とそれを巡る各種の動き

Google がサイバー攻撃を受けたという発表がなされて以来、本件に係る関心の高さを踏まえて、各紙が、本件に係る攻撃のルート・発信源、あるいは、中国におけるハッカーの状況について、競って報道を行ってきており、これらに係る実態が明らかになりつつある。

（１）サイバー攻撃のルートと攻撃対象の特定

前述の通り、特に司法権の及ばない海外（中国）において、サイバー攻撃の源を特定することは、一般的には困難である。このため、今回の Google の件についても、各種報道によると、その攻撃源は絞られつつあるものの、中国側は常に根拠がないものとして反論しており、平行線を辿っている。

①　Google による攻撃のルートの特定

今回の Google の発表直後において、Google は、自力で、本サイバー攻撃は、台湾経由で、34 社に対して攻撃がなされたことを確定したと報道されている。

＜攻撃ルートの特定＞

今回のサイバー攻撃に関して、Google は、まずは、攻撃を受けたとされる米国内の Gmail 保有者に対して、自主的に調査への協力を依頼していたことが報道されている[12]。

NYT 紙（2010 年 1 月 13 日付）[13]による報道（概要）

- 2010 年 1 月上旬、Stanford 大学の学生（20 歳）で、チベット活動家（チベット難民の娘）である Tenzin Seldon 氏は、大学職員から、同氏の Gmail アカウントがハッキングされたので、Google にコンタクトするように言われた。
- 同氏は、Google の David Drummond 氏（CLO）にコンタクトしたところ、「中国の誰かにハックされたので、ラップトップを見たい」と言われたので、同氏は、すぐにパスワードを変更し、Google に調査してもらった。
- ラップトップは、今週返却されたが、「ウィルス、マルウェアは探知されなかったが、アカウントには極秘に侵入されていた」とのコメントがあった。

[12] なお、それ以外にも、Gmail アカウントに関しては、2010 年 1 月 18 日付け NYT によると、北京内の少なくとも二人の外国人ジャーナリストの Gmail アカウントがハックされ、不明のアドレスに転送されるようになっていた、としている。
http://www.nytimes.com/2010/01/19/technology/companies/19google.html

[13] 出典：http://www.nytimes.com/2010/01/14/technology/14google.html
なお、Google は、同氏のケースは認めたが、他の活動家に対しても同様にハッキングの犠牲になったことを通知したかについては、コメントしていない。

次に、Google は、その攻撃が台湾経由で行われたことを突き止め、現地まで行って、コンサル等とともに、当該攻撃のもととなったコンピューターの調査を行い、他の企業も攻撃となったこと、発信源は中国らしいことを突き止めている。

しかしながら、Google 側は、中国政府機関によって運営され、あるいは少なくとも承認されたとの強い示唆を得たものの、完全に証明することはできなかったとしている。

NYT 紙（2010 年 1 月 14 日付け）[14]による報道（概要）

- 2009 年 12 月、Google の技術者は、同社のオフィスにて、中国の侵入者が Gmail アカウントに侵入したと思われる件について、反攻の検討を開始。
- Google の技術者は、攻撃の元と目された台湾へのコンピューターへのアクセスをどうにか確保し、そのコンピューターを調べた結果、攻撃の痕を発見した。その際、攻撃対象は、Google だけではなく他の 33 社が攻撃対象となっていることが判明。
- Google は、問題の広さを認識し、米国の諜報・法執行機関[15]に警告を発するとともに、それらの機関と連携して、攻撃の黒幕が、台湾でなく中国であることとの強力な証拠を収集することとした。

なお、今回の Google などへの攻撃は、Microsoft の IE（Internet Explorer）の脆弱性（セキュリティホール）[16]を狙ったものであり、この IE の脆弱性を利用してコンピューターにトロイの木馬をインストールすることで、当該コンピューターを遠隔操作することができたとされており[17]、これらの対策としては、Google の発表直後に、Google は暗号対策の強化[18]を、また、Microsoft は IE の緊急パッチの配布を行っている[19]。

---

[14] 出典：http://www.nytimes.com/2010/01/15/world/asia/15diplo.html
調査に加わった政府系コンサルの証言。

[15]おそらく、NSA、FBI を指すものと想定される。

[16] このセキュリティホールは IE6、7、8 の 3 バージョンに共通であるが、被害はバージョン 6 のみに見られており、Microsoft によると、IE7 および 8 のセキュリティ対策により、バージョン 7 と 8 では被害が防げたとしている。

[17] 2010 年 3 月 2 日付 NetworkWorld 誌。
http://www.networkworld.com/news/2010/030210-google-attack-based-on-unpatched.html
なお、Google の発表（2010 年 1 月 12 日）では、Gmail へのアカウントへのアクセスは phishing またはコンピューター上の Malware によって行われたとされている。
http://googleblog.blogspot.com/2010/01/new-approach-to-china.html

[18] Google は、上記発表の直後の 2010 年 1 月 12 日、Gmail の係るデフォルト設定において原則暗号が係るように見直し・強化を行った。
http://gmailblog.blogspot.com/2010/01/default-https-access-for-gmail.html
http://news.cnet.com/8301-30685_3-10433965-264.html

[19] Microsoft は、2010 年 1 月 21 日に本件に対応し、同社の IE のセキュリティの緊急見直しを行っている。なお、Microsoft の広報担当者は、今回の Google 等への一連の攻撃に IE の脆弱性が利用されたことを認めている。http://www.microsoft.com/technet/security/bulletin/ms10-002.mspx
http://www.eweek.com/c/a/Security/Microsoft-Patches-IE-Security-Vulnerability-Involved-in-Google-Attack-236870/

＜中国側の反応＞

Google の発表を踏まえ、米国側（クリントン長官）は、発表直後及びその後の演説において、中国側に対し、本件に係る調査と公表を求めている（後述）。

これに対し、中国側は自らの関与を否定している。具体的には、2010 年 1 月 25 日、中国政府運営のニュースメディアの報道において、中国政府のスポークスマンのインタビューとして、「中国がハッカーによる侵入を行ったあるいは容認されたとの如何なる指摘は全く根拠がなく、中国を中傷するものである」と反論している（2010 年 1 月 25 日付け NYT 紙[20]）。

② NSA 等との連携と中国の二つの学校の特定

＜NSA 等との連携＞

さらに、Google は、台湾から遡って、中国での攻撃源の特定等を行うために、NSA（National Security Agency）と正式に連携したことが報じられている。

具体的には、2010 年 2 月 4 日付け NYT 紙等[21]によると、事情を良く知る者の話しとして、Google は、DOD の NSA と、同社のサイバーセキュリティを破ったコンピューター攻撃者についてより知るため[22]の技術的支援[23]の協定を締結したと報道されている。ただし、本件に関しては、Google からの正式なコメントはなく、NSA もコメントできないとしている。

なお、本協定については、国土安全保障省（DHS）との協定ではない点が注目を浴びている。もちろん本分野で最も知見を有するのは NSA であるのは事実であるが、一方、本来、民間企業におけるサイバーインフラの保護に対しては権限を有するのは DHS であり、Google が NSA と協定を締結したことは、同社は、明らかに同社の検索エンジンや電子メールその他の Web サービスが、重要インフラとして DHS により規制されるのを避けているものと報道されている[24]。

一方で、NSA は、世界のインターネットの盗聴を行っている機関であることから、以前よりプライバシー対策に関して批判を受けている Google が NSA と協定を結ぶことに関しては、市民団体からは批判の声も出されている。例えば、

---

http://arstechnica.com/microsoft/news/2010/01/microsoft-warns-of-ie-security-flaw-used-in-google-attacks.ars

[20] http://www.nytimes.com/2010/01/26/world/asia/26google.html

[21] もともとは 2 月 3 日付け WP 紙。
http://www.nytimes.com/2010/02/05/science/05google.html
http://www.washingtonpost.com/wp-dyn/content/article/2010/02/03/AR2010020304057.html

[22] なお、本件の内容は、今回の攻撃者を特定するためというよりはむしろ Google のネットワークの防衛をより強固にすること（情報アシュアランス）に重点をおいているとのコメントもある。

[23] いわゆる CRADAs（Cooperative R&D agreement）と呼ばれる、官民連携の枠組みを活用。

[24] 実際に、Google は、これまでの DHS の重要インフラの官民連携の枠組み（情報技術分野、通信分野ともに）には全く参加していない。

Electric Privacy Information Center は、本連携に関し、世界中の Google の何百万ものサービス利用者のプライバシーに影響を与えかねないと懸念を示している。

なお、Google は、今回のサイバー攻撃に関して FBI とも連携を行っていると報じられているが、FBI も正式にはコメントを控えている。

＜中国の二学校の特定＞

そのような中、2010 年 2 月 18 日付け NYT 紙[25]は、調査に関連した関係者の話として、（台湾から遡って）攻撃源として、中国の二つの学校に遡ることができたと報道している。

なお、本追跡（逆探知）に関しては、NSA を含むセキュリティ専門家が調査に加わったとしており、また、同様の攻撃を受けた米国の国防関連のコントラクターによって得られた証拠をもとに、同職業学校においてウクライナの先生によって教えられている特定のコンピューターへの疑いにつながったとしている。

NYT 紙（2010 年 2 月 18 日付け）[26]によって報道された 2 つの学校

上海交通大学（Shanghai Jiaotong University）	中国のコンピューター科学にかかるトップレベルの大学。
藍翔高級技工学校（Lanxiang Vocational School）	山東省（東部）にある巨大な職業訓練校。軍の支援を受けるとともに、軍のためのコンピューター科学者を養成しており、また、Baidu とも強い関連があるとしている。更に、中国の Great Firewall（検閲システム）を作るのを手助けしたともされる[27]。

ただし、本件についてどのように解釈するか（本当に同 2 校及びその関係者が攻撃源なのか）は、やはり、専門家、政権内で意見が分かれているとされる[28]。。特に、専門家によると、中国側は、攻撃源を知られることがないように、高度に分散化した手法でオンラインでのスパイを実施していると指摘しており、また、中国政府が、同国の政策を支持するボランティアの「愛国者的ハッカー」を利用する場合が多いとも指摘している。

＜中国側の反応＞

上記 2 つの学校に係る報道に関しても、中国側は、学校、政府ともに関与を否定している。

---

[25] http://www.nytimes.com/2010/02/19/technology/19china.html?partner=rss&emc=rss
記述は、同紙によるもの。なお、学校は、報道発表後、一部その報道内容を否定している。

[26] http://www.nytimes.com/2010/02/19/technology/19china.html?partner=rss&emc=rss

[27] http://www.washingtonpost.com/wp-dyn/content/article/2010/02/19/AR2010021902643.html

[28] 例えば、以下の通り。

・当該学校が、中国政府の運用のカモフラージュとして使われたのではないか、
・（別の第三国が）諜報機関を騙すため（False Flag）として利用されたのではないか、
・米国技術系企業から知的財産を盗もうとする更に大きな産業スパイの一環として行われたのではないか

上記発表後の二日後の 2 月 20 日の新華社の報道[29]でによると、両学校とも、申し立て・主張を否定している。具体的には、同報道によると、上海交通大学の関係者は、根拠がないと主張し、また、藍翔高級技工学校の関係者は、調査の結果、校内が攻撃源と使われた証拠は見つからなかったと述べたとされる。また、藍翔高級技工学校については、そもそもウクライナなどの外国人スタッフはいないし、軍と密接な関係にはないと反論している。なお、今後の調査に関しては、もう攻撃に利用されたサーバーは既に閉鎖されているのではとの指摘もある。

また、中国政府も、2010 年 2 月 23 日付け報道で[30]、中国の外交部 Ma Zhaoxu 氏は、上記ニュース報告を否定し、「中国の法律はハッキングを禁じており、また、政府はそれを止めるであろう」「中国の学校から来たというというのは根拠がないし、中国政府が関与しているとの主張は無責任であるし、かつ、秘めた別の動機から言っているのだろう。」としている。

③ プログラムのコードからの推定

一方、上記の攻撃ルートの特定とは別に、今回の報道を受け、多くのセキュリティ専門家が、Google 等への攻撃に利用されたプログラム等の分析を行っており、その結果、そのコードの内容から分析して、中国あるいは中国政府と関連したプログラムであること、また、最近はプログラマーを特定したとの報道がなされている。ただし、複数のハッカーがやりとりしながら作成しているとの報道もある。

プログラム・コード等からの推計[31]

出典	概要
2010 年 1 月 13 日付け NYT[32]	・Google が攻撃を受けたという記述から判断すると、トロント大学の研究者が、2009 年 3 月に発表した「Ghostnet」と呼ばれる巨大な監視システムの内容と似ている。 ・この Ghostnet は、電子メールを狙った中国をベースとする自動のスパイシステムであり、何百もの政府機関の何千ものコンピューターを攻撃対象として自動的に文書を読み込み、中国の記憶装置（ストレージ）に送付するもの。
2010 年 1 月 20	・米国のセキュリティ企業 SecureWorks の Joe Stewart 氏（マルウェアの専門

[29] 2 月 21 日付け AP、2 月 20 日付け WSJ 等
http://www.boston.com/business/technology/articles/2010/02/21/schools_in_china_say_they_werent_behind_hacking/
http://online.wsj.com/article/SB10001424052748703787304575074703728470246.html
http://www.nytimes.com/2010/02/22/technology/22cyber.html
http://japan.cnet.com/news/sec/story/0,2000056024,20408966,00.htm
http://www.itmedia.co.jp/news/articles/1002/22/news027.html

[30] http://www.boston.com/business/technology/articles/2010/02/23/china_rejects_report_schools_linked_to_hacking/ AP
http://www.itmedia.co.jp/news/articles/1002/24/news059.html

[31] 出典：各種資料より筆者作成。ただし、それぞれの真偽は不明。

[32] http://www.nytimes.com/2010/01/14/technology/14google.html

日付け NYT[33]	家）によると、（上記とは別に）、今回の攻撃は、コンピューターのバックドアを開く種類のトロイの木馬型によるもの。 ・その主要なプログラムは、中国語のウェブサイトのみに記載されている中国の技術ペーパーによる特殊なアルゴリスムに基づくものであることを特定したとしている。
2010 年 2 月 19 日付け、WP[34]	・業界に詳しい人の話しとして、Google 等への攻撃に利用されたコードは、多くの中国のハッカー（専門家、コンサルタント、臨時コントラクターを含む）によって書かれたものであるとしている。 ・調査に関わった者の話にとして、開発者（学生を含む）は、IE6 の脆弱性を利用しており、現在 6 名まで絞られていると報道している。ただし、コードの開発者が攻撃を行った訳ではかならずしもなく、コードはハッカーのフォーラムの中でやりとりされている、としている。 ・なお、いずれの 6 名とも、上記の 2 学校の出身者ではないとのこと。
2010 年 2 月 21 日付け FT 等[35]	・専門家の話として、Google への攻撃のコードは、中国の 30 代のフリーランスのセキュリティコンサルタントが作成したと特定した。 ・ただし、この人物が攻撃を仕掛けたのではなく、中国政府の関係者がそのコードを入手したのではないかと報道している。

なお、FT の報道に関し、2010 年 2 月 23 日、国務省の Crowley 次官補は、会見で、「我々の持つ情報は、中国内の複数の個人の関与を強く疑わせるものと考えている」と発言している[36]。その上で、今後引き続き中国との協議を続けていくとしている。

④　中国からの攻撃対象企業の範囲

なお、Google と同様（同時）に攻撃を受けた企業としては、34 社がリストアップされているとともに、最近は、類似する事例はさらに多いとの調査も出てきている。いずれにせよ、Google に対する Gmail のハッキングといった盗聴目的以外にも、（場合によっては企業に対する産業スパイも含めた）更に幅広い目的でサイバー攻撃が行われているように見受けられる。

＜攻撃対象企業の範囲（当初）＞

上述の通り、実際の攻撃の対象については、Google の同調査に関連した人からの情報として、（Google を含めて）34 社に上るとしており、具体的には、以下の企業がリストアップされている。しかしながら、同時点で、攻撃を受けたことを認めた企業は、Adobe、Rackspace などと非常に限られる。

---

[33] http://www.nytimes.com/2010/01/20/technology/20cyber.html
[34] http://www.washingtonpost.com/wp-dyn/content/article/2010/02/19/AR2010021902643.html
[35] http://www.ft.com/cms/s/a6f5621c-1f21-11df-9584-00144feab49a,Authorised=false.html
http://arstechnica.com/tech-policy/news/2010/02/chinese-programmer-fingered-in-google-hack.ars
http://www.itmedia.co.jp/news/articles/1002/23/news022.html
[36] http://www.state.gov/r/pa/prs/dpb/2010/02/137167.htm
http://www.asahi.com/international/update/0224/TKY201002240120.html

Google 以外にサイバー攻撃を受けたと報道された米国企業（各種報道）[37][38]

報道された企業	企業側の発表
Adobe Systems	Adobe Systems は、2010 年 1 月 12 日、サイバー攻撃に合った旨を発表[39]。同発表では、この攻撃の起源が中国であるとは明言していないものの、「同様の攻撃を受けた企業に接触している」としている。
Rackspace[40]	Rackspace の関係者は、同社のサーバーが攻撃を受けたこと、関係者と協力の上、調査を支援していることを発言。（なおセキュリティ専門家によると、Google 等から盗まれたデータは、一旦同社のサイト（サーバー）に送られたあと、海外に転送された、としている）（2010 年 1 月 13 日付 WSJ）
Juniper Networks	現在攻撃を受けたか否かについて調査中であることは明らかにしているものの、詳細は発表していない。（2010 年 1 月 15 日 NYT 等）
Symantec	同上

[37] 出典：各種報道より作成
http://www.nytimes.com/2010/01/14/world/asia/14beijing.html
http://www.nytimes.com/2010/01/15/world/asia/15diplo.html
http://online.wsj.com/article/SB126333757451026659.html
http://www.washingtonpost.com/wp-dyn/content/article/2010/01/12/AR2010011203024.html
http://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html
http://www.bloomberg.com/apps/news?pid=newsarchive&sid=aE5FWLzQMZGY
http://www.computerworld.com/s/article/9144221/Google_attack_part_of_widespread_spying_effort
http://www.computerworld.com/s/article/9145019/Juniper_Symantec_investigating_after_Google_attack、http://www.guardian.co.uk/technology/2010/jan/14/google-yahoo-china-cyber-attack

[38] なお、今回の Google への攻撃と同じものかは不明であるものの（少なくともサーバー設置場所は異なる）、Google の発表のほぼ同時期（Google の被害の約 1 ヶ月後）に、Green Dam（フィルタリング）ソフトウェアに関し著作権違反であるとして中国政府等に訴えている Solid Oak Software 社の訴訟を担当している法律事務所が、中国からのサイバー攻撃を報告している。

Gipson Hoffman & Pancione 法律事務所は、2010 年 1 月 13 日、同社が Solid Oak Software 社の弁護士として中国への訴訟を起こした翌週の 1 月 11 日朝～12 日にかけて、同事務所の弁護士らが、同僚からのメールに成りすまされたトロイの木馬を添付したメールを受け取ったと発表した。同日付け CNet の記事によると、トロイの木馬の置かれているサーバーは中国であり、また、トラフィックの起源も中国だったとしており、また、FBI に報告をしたとしている。
http://finance.yahoo.com/news/Gipson-Hoffman-Pancione-Comes-bw-1192518024.html?x=0
http://news.cnet.com/8301-27080_3-10434551-245.html

なお、Solid Oak Software 社自体も、2009 年 6 月にも、同僚名を語ったメールに成りすましたトロイの木馬型のサイバー攻撃を受けており、FBI に報告をしている。
http://www.informationweek.com/news/security/attacks/showArticle.jhtml?articleID=218101882

なお、本件に係る攻撃の分析結果が、Malware lab から、2010 年 1 月 15 日に発表されている。同分析結果では、Solid Ork 社の従業員名での Gmail アカウントを利用し、トロイの木馬型の悪意あるファイルを添付しているとしている。
http://malwarelab.org/2010/01/malware-attacks-on-solid-oak-after-dispute-with-greendam/
また、同社の Facebook ページ（同社のソフトの Cybersitter 名）には、2010 年 1 月 18 日、中国からと見られる攻撃を（再度）受けたとのポスティングがされている。
http://www.facebook.com/pages/CYBERsitter/89420205851

[39] http://blogs.adobe.com/conversations/2010/01/adobe_investigates_corporate_n.html

[40] 米国の大手のホスティング企業。

Northrop Grumman	Northrop Grumman は、今回の攻撃の有無については解答せず、「単純なものから複雑なものに至るまで、様々な攻撃の対象になる可能性がある」と一般論を回答（2010 年 1 月 15 日付 ComputerWorld 紙）
Yahoo!	Yahoo は、「Google と同じ立場に立つ」「この種の情報は公開しないが、セキュリティ問題は真剣に捉え、適切に対処する」とし、今回の攻撃に関しては特にコメントをしていない。（2010 年 1 月 14 日付け Gardian 等）
Microsoft	Microsoft は、2010 年 1 月 14 日の公式ブログ記事[41]の中で、「サイバー攻撃を非難する」とはしているものの、自社はこのような攻撃は受けていないとしている。
Dow Chemical	（コメントなし）

また、Intel も、2010 年 2 月 22 日、同社が提出した年次レポートの中で、Google への攻撃と同時期に攻撃を受けたことを公表している[42]。

＜対象企業の広がり＞

なお、最近においては、各セキュリティ関連企業からは、Google 等に対する攻撃と類似する攻撃は、更に幅広いものであったとの報告がなされている。具体的には、以下の通り。

- セキュリティ企業である iSEC パートナーの研究者は、2010 年 2 月 26 日、Google によって明らかにされた最近のサイバー攻撃は、思ったより広範囲であり、非常に類似した攻撃を受けた企業数は 100 以上に上るとしている[43]
- McAfee は、2010 年 3 月 3 日、Bloomberg のインタビューに対して、中国を起源とし、企業の知的財産をハッキングした事例として、少なくとも 6 件の事例を発見したとしており[44]、いずれも、ソースコード、製品フォーミュラなど当該企業にとって最も重要な（Crown Jewels）知的財産を狙っていたとしている。

（２）中国におけるハッカーを巡る状況と中国政府の対応

一方、中国のハッカーは、個人が緩やかなコミュニティでつながるとともに、その一部として中国政府も絡んでいるという構図であると報道されており、このような状況であることを踏まえると、そもそも攻撃者の特定が攻撃を指示した組織の特定につながらず、また、その取り締まりも困難な状況にあるものと想定される。

[41] http://blogs.technet.com/microsoft_blog/archive/2010/01/14/the-recent-cyber-attacks.aspx
[42] http://www.businessweek.com/news/2010-02-23/intel-was-target-of-sophisticated-computer-attack-in-january.html
http://bits.blogs.nytimes.com/2010/02/23/intel-says-it-was-attacked-at-the-same-time-as-google/
http://www.informationweek.com/news/hardware/desktop/showArticle.jhtml?articleID=223100441
[43] http://online.wsj.com/article/SB10001424052748704625004575090111817090670.html
[44] http://www.businessweek.com/news/2010-03-03/mcafee-says-hackers-sought-crown-jewels-at-six-companies.html

① 中国におけるハッカーを巡る状況

＜中国におけるハッカーコミュニティ（分業化と緩やかなコミュニティ）＞

今回の Google による発表をきっかけに、中国におけるハッカーの状況が多く報道されている。これらを踏まえると、以下のような構図が浮かび上がる[45]。

- 中国におけるハッカーは、不正利益を目的に、それぞれの個人が、分業でやりとりを行いながらコードの作成等を行うことによって、小銭を稼ぐといった、緩やかなコミュニティでつながっており、一つの組織で抱え込まれているものではない。
- このような中、中国政府も、これらのコミュニティと暗に関係を有し、一時的にハッカーを雇ったり、あるいは、これらのコミュニティをハッキング実施に活用したりしている。

中国のハッカーコミュニティに係る最近の記事

「Hacking for Fun and Profit in China's Underworld」（2010 年 2 月 1 日 NYT[46]記事）

- 中国には、多くのハッカーのコミュニティがあり、クレジットカード番号の窃盗や、企業スパイの実施、他国に対するオンラインでの戦闘を実施しているとしている。また、そのような個人に加えて、いわゆる愛国者的なハッカーもおり、また、人民解放軍の中にも諜報目的のハッカーがいる。
- 実際に中国（及び東欧、ロシア）では、ハッキングは国家的なスポーツのようなものになっている。ハッカーの会議、ハッカーを訓練するための教育機関、コンピューターに侵入する方法やトロイの木馬を作る方法等を記載した雑誌（例えば 6 ドルで購入できる）などがある。
- 特に金銭面でのインセンティブが動機付けとなっている。あるハッカーは、米国連邦政府にハッキングを行い、その後それを踏まえて有力大学で講師を行い、また、中国のセキュリティ関連省庁で働いたという。ただ、最近は、企業秘密を盗み、あるいは、他のハッカーに教えることによって多額の利益を得ることができる。また、ウィルスやトロイの木馬を売ったり、オンラインゲームのアカウントに侵入したりすることによっても儲けることができる。

「Peoples Republic of Hacking」（2010 年 2 月 18 日付けの WSJ の記事[47]）

- Panda Burns Incense ウォームの事例は、中国のサイバー犯罪のネットワークを知る手ががりとなる。同ウォームは、Li Jun 氏によって作成され、2006～2007 年にかけて猛威を振るったもの（Li 氏は、その後 3 年間服役）。この Panda のケースは、中国での始めての組織的なサイバー犯罪のケース。
- ハッカーのフォーラムは、サイバーセキュリティを強化しようとする中国政府にとって、リクルーティングをする最も適した（fertile）場所（もちろん、中国政府は否定するが）。
- Li 氏は幼馴染の Lei 氏とともにチームを組んでインターネットユーザーからお金の窃盗を行っ

[45] なお、中国におけるサイバー戦闘能力に関し、Google の発表直後の 2010 年 1 月 13 日、「中国は 2003 年以来、3 万人の軍関係のサイバースパイと、15 万人の民間のコンピューター専門家（米国の軍、技術上の機密の収集等を目的）がいる」等を内容する FBI の機密報告書が判明したとのブログが発表されている。
http://www.thedailybeast.com/blogs-and-stories/2010-01-13/chinas-secret-cyber-terrorism/

[46] http://www.nytimes.com/2010/02/02/business/global/02hacker.html

[47] http://online.wsj.com/article/SB10001424052748704140104575057490343183782.html

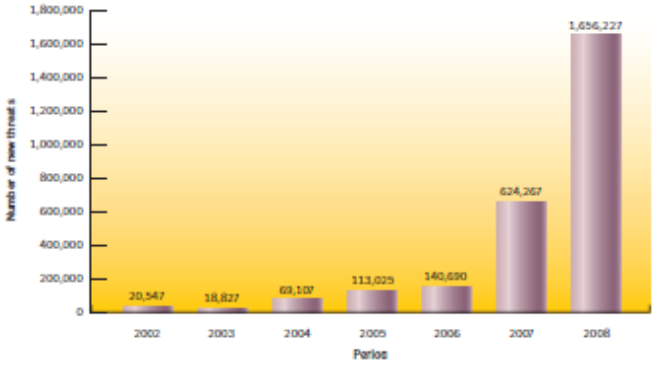
た。彼らは、オンラインでのハッカーの連合（”Small Swords Society”）から技巧を学んだ。一般的に中国のハッカーコミュニティは、米国やロシアとは異なり、広く広がって（Disperse）おり、かつ分断されている。
- 一般的には、中国のハッカーコミュニティは、大きな点数を稼ぐべく働くというよりは、自分の作品を売ることによって小額のお金を稼ぐ。（悪意あるプログラムのプログラマーは、どこかから買ってきたコードをつなぎあわせて作成する。組み立て工場のラインのようなもの）したがって、ピラミッドのような多層構造となっており、特定のギャングの支配にあるようなものではない。
- オンラインでの非公式のチャットルームみたいなところが犯罪養成所みたいなところになっている（その際、法に引っかからないように、「訓練」や「tutoring」などの言葉を使う）。そこで、コード（例えば 7$）やデータ（例えば 70$）とかでやりとりされる。参加者は匿名。中国語のみでの参加。
- 仮に誰かが逮捕されたり、フォーラムが閉鎖されたりしても、個人やネットワークは生きる。

＜分業化の進展と悪意あるコード数の増大＞

なお、もちろん、中国のハッカーコミュニティが世界の大半を占めているというわけではないが、このような中国のハッカーコミュニティにおける分業化という傾向は、世界全体において、悪意あるコード数が急増しているという傾向と符号する。

Symantec が 2009 年 4 月に発表した調査[48]によると、近年、新たに発見される悪意あるコード（脅威）に係る数は、近年、急速に増大しているとしている。同調査報告によると、これは、地下経済における組織化が進み、カスタム化された悪意あるコードや phishing に係るキットが広く流通し、それらのコードやキットに基づいて、実際に配布されるコード等が多様に作成されているためであるとしている。（同調査報告では、ロシアの事例を取り上げている。）

世界における新たな悪意あるコードの数の推移[49]



[48] http://www.symantec.com/connect/sites/default/files/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf
[49] 出典：http://www.symantec.com/connect/sites/default/files/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf

② ハッカーコミュニティに対する中国政府の動き

一方、中国政府は、中国はむしろハッカーの被害を多く受けている国であり、ハッカーの取り締まりを行っているとしているが、上記のようなハッカーコミュニティの構造の中で、どの程度真剣に取り締まりを行っているのかが論点になる。

＜中国におけるハッカー被害＞

中国政府は、上述の通り、Google に対する攻撃に関しては、自らは関与していない（関与したという証拠はない）とする一方で、中国は、むしろハッカーによる被害を受けている国であることを主張している[50]。

例えば、新華社通信のインタビューに対し中国の National Computer Network Emergency Response Technical Team は、中国が最もハッカーによって標的にされている国であり（2009 年には 26.2 万のインターネットアドレスがハッカーのターゲットとなった）、その 1/6 は米国からのものであるとしている（2010 年 1 月 25 日付け NYT[51]）。ただし、この米国からのハッキングのうち、もともと中国を攻撃源として米国を経由してきたものが、どの程度含まれるのか不明である[52]。

＜中国におけるサイバー犯罪の取締り＞

また、中国政府は、Google のサイバー攻撃に関連して、中国は、常にハッキングに対して取締りを行っていると発言している。

これに関し、中国は、2010 年 2 月 7 日と 8 日の中国の政府系報道において、同国最大のハッカー養成の商業的オペレーションとなっている Black Hawk Safety Net（2005 年に開始、1.2 万人の有料会員と 17 万人の無料会員）を手入れ・取締

---

[50] なお、Google の発表の直前の 2010 年 1 月 12 日、中国での Google のライバルである Baidu にサイトが、ハッキングを受け Iranian Cyber Army と名乗るサイトにリダイレクトされ、数時間閉鎖に追い込まれている。http://news.bbc.co.uk/2/hi/8453718.stm

この Iran Cyber Army と称するサイトにリダイレクトされるハッキングは、2009 年 12 月に Twitter に対しても行われている。http://zone-h.org/news/id/4733

本件に関しては、イラン側政府側は当然関連を否定している。一方、その直後、中国側の（愛国者的な）ハッカーコミュニティが、イラン政府に対して報復をすることを検討していると報じられている。
http://www.chinadaily.com.cn/china/2010-01/13/content_9310376.htm

なお、本件に関し、Baidu は、その後、ドメイン名の登録事業を行う Register.com を訴えている。
http://domainnamewire.com/2010/01/19/baidu-sues-register-com-over-hacking-incident/
http://domainnamewire.com/2010/02/24/how-baidu-got-hacked-by-the-iranian-cyber-army/

[51] http://www.nytimes.com/2010/01/26/world/asia/26google.html

なお、同 Team は、他の企業は、攻撃を受けた場合、同チームにコンタクトしてきているのに対し、Google からはコンタクトがないとしている。

[52] 一般的に、政治的な観点から米国政府が中国政府に対してハッキングし、盗聴を行うことは理解できるものの、経済犯罪の観点から、米国が中国企業にハッキングするメリットはあまり多くは想定されないし、また、言語の壁から言っても、米国人が中国企業を狙うには、障壁が高いように思える。

り（閉鎖）を行い、3 名を逮捕するとともに、数 10 万ドルの資金と機器を押収したとしている（2010 年 2 月 8 日付け NYT[53]）。

しかしながら、これに関して、西側専門家は、この逮捕によって中国側が Google 等に対するサイバー攻撃を止めようとするコミットメントを示すことにはならないと見ている。すなわち、実際に攻撃に利用されたと思われる有名なサーバーは全く閉鎖されておらず、また 3 名の逮捕はほとんど関係がない上に、そもそも、本件の取締りは、2009 年 11 月に行われたものであるのに、新華社通信は、最近行われたようなイメージで報道している、と分析している。

４．インターネットの自由と Google の中国でのビジネスを巡る動き

今回の Google の発表は、サイバー攻撃の観点以上に、インターネットの自由（検閲問題）のあり方について再度関心が集まっている。特にクリントン国務長官の新たな演説を踏まえ、米国内でのインターネットの自由に係る関心が高まり、その結果、米中間の対立が深まってきている。このような中、今後の米中間の動向に加え、Google と中国側との交渉がどのように妥結するのか注目される。

（１）今回の Google の意思決定に係る背景と評価（Google 内のガバナンス）

今回、Google が、中国からの撤退も辞さないとしたことについては、ビジネスの拡大を志向する営利企業としては、通常はなされない判断であるとして大きな話題になった。このような判断の背景には、Google の大きな方針に係る意思決定において、共同創業者の二人の意向が強く働いているという特殊なガバナンス体制があり、その中でのリスク／ベネフィット判断であるともみなすことができる。

＜今回の意思決定に係る Google 内部での議論＞

今回の意思決定に関しては、共同創業者である Larry Page 氏と Sergey Brin 氏の意向が強く働いていると報じられている（2010 年 1 月 14 日付け WSJ[54]等）。このうち、特に Brin 氏は、同社の社是・スローガンである「Don’t Be Evil」の保護者でもあるとともに、自身が幼少の頃のロシアでの経験（政府の検閲）を有しており、そのため、従来から、Google の中国でのビジネスが、同社の社是にとって相反する状況にあることに懸念をもっていたとされる[55]。

---

[53] http://www.nytimes.com/2010/02/08/world/asia/09hacker.html
[54] http://online.wsj.com/article/SB10001424052748704675104575001281662251848.html
[55] なお、もともと、2006 年に、中国に参入する際も Brin 氏からの反対が強かったとされる。また、これまでにも何度も再考する機会があったとされる（例えば、2008 年には、中国当局は、Google.cn だけでなく、Google.com を検閲するよう要求したとのこと。）

そのような背景のもと、今回、Google の従業員によってサイバー攻撃に係る証拠が集められ、攻撃が中国あるいは中国当局との関係が結びついてきた中で、CEO の Eric Schmidt 氏を含む 3 人で今後の対処方針の議論がなされた。その中で、Schmidt 氏は、従来どおり「中国の体制をオープンにするためには、やはり Google が中国でインターネットに係るビジネスをすることが、道徳上求められる」と主張したのに対し、Brin 氏は、「会社（Google）はもう十分に努力したし、もはや検索結果を検閲することは正当化されない」と激しく主張したとされる。

結局、3 人は、少なくとも攻撃があったことを公に公開することに合意し[56]、その後、Public Policy・広報担当の VP がいくつかの案を作ったが、最終的には、「人権」の言葉を含む最も強いものが選ばれた[57]。他の幹部は、発表前日（11 日）に知らされた。

＜今回の意思決定に係る評価＞

言うまでもなく、今回の Google が中国からの撤退する可能性があるという発表は、世界中から驚きをもって見られた。例えば、2010 年 1 月 12 日付け NYT[58]は、「Google は魅力的な市場を捨てる」との見出しで報道をしている。

しかしながら、その後、もちろん将来的に魅力的である市場を捨てることになるかもしれないが、少なくとも現行の財務的にはほとんど影響がないとの見方がなされている。例えば、2010 年 1 月 14 日付け NYT[59]では、アナリストによると Google は、既にそのことを計算済みなのではないかとしている。すなわち、Google の全世界の売上げは 220 億ドルであるのに対し、中国での収入は 3 億ドル（推定）程度にしか過ぎず、また、Google の広報担当者によると、中国からの収入の多くは、中国企業が米国の Google サイトに掲載している広告によるものであると示唆している。

なお、Google の今回の発表によって、市民による Google に対する好感度が大きくあがったとされている[60]。米国国内では、これまでプライバシー問題等で常に Google を批判してきた EEF（Electric Frontier Foundation）を始め、その他の多くの人権団体[61]、あるいは、共和・民主両党も、Google の意思決定を高く評価している。また、中国国内でも、若者達が Google China の本社に献花をしている。

---

http://www.nytimes.com/2010/01/14/technology/14google.html

[56] なお、その後 Google のスポークスマンによると、攻撃を公表した一つの要因は、活動家に対してアカウントが攻撃を受けていることを警告するため、としている。

[57] その後、中国での従業員のことを考慮して「米国の幹部によって決められた」とのコメントが挿入された。

[58] http://www.nytimes.com/2010/01/13/technology/companies/13hacker.html

[59] http://www.nytimes.com/2010/01/15/world/asia/15google.html
http://www.nytimes.com/2010/01/15/world/asia/15iht-china.html

[60] なお、もちろん Google は、当然広報・PR や財務的観点から意思決定をしたものでは全くないとしている。

[61] 例えば、以下の通り。

・Human Rights Watch（2010 年 1 月 12 日）
http://www.hrw.org/en/news/2010/01/12/china-google-challenges-censorship

一方、Google は、もちろん現時点で撤退を決めた訳ではなく、Google から見れば、中国政府から何らかの譲歩を引き出した上で、中国に残ることができれば、一番望ましい結果であり（1 月 19 日付け NYT[62]）、それに向けて現在中国政府との交渉を進めるとしている。したがって、営利企業の観点からは、撤退することとなった場合には、若干のリスクはあるが、一方で、中国の検閲を廃止（あるいは軽減）することに成功した場合は、競争環境上、それ以上のベネフィットがあると判断したともみなすことができる。

（２）米中の政府間における対立の再燃

一方、今回の Google の発表に伴い、米国側において、インターネットの自由に係る議論が再燃し、それに対して中国側が批判・反論する形で、米中間における対立が激化する結果となっている。ただし、米国内において他のインターネット企業が Google に追随している訳ではない。

①　Google の発表を受けた米国連邦政府の動きと中国政府の対応

今回の発表に関して、Google と米国連邦政府（国務省）は、事前に十分な連絡を取って準備を進めており、連携して対応を進めていたことが伺える。

＜Google の発表に対する米国連邦政府の動き＞
米国国務省のクリントン長官は、Google が発表を行った同日の 1 月 12 日付けで、「Google の中国での事業にかかるステートメント」を発表しており、中国側への懸念を表明している。
なお、本件に先立つ前週において、クリントン長官は、Google、Microsoft、Twitter、Cisco Systems などのハイテク企業の幹部と会談（夕食会）を行っており、その際 Google の CEO の Eric Schmidt 氏から、本件に関し長官に説明があったと報じられている[63]。

・Human Rights First（2010 年 1 月 13 日）
http://www.humanrightsfirst.org/media/hr/2010/alert/563/index.htm
・アムネスティーインターナショナル USA（AIUSA）（2010 年 1 月 29 日）
http://www.amnestyusa.org/document.php?id=ENGUSA20100129002&lang=e
ただし、その後、NSA と協定を締結したとの報道に対しては、マイナスの評価がなされている。

[62] http://www.nytimes.com/2010/01/20/technology/companies/20revenue.html

[63] http://jp.reuters.com/article/mostViewedNews/idJPJAPAN-13315420100113
http://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html
また、国務省の Crowley 次官補も、1 月 13 日、定例の記者会見において、Google とは、発表前から連絡を受けていたこと、今後とも米中間で議論していく旨の発言を行っている。

「Google の中国での事業に係るステートメント」（2010 年 1 月 12 日）[64]

- 我々は、Google からこれらの申し立ての説明を受け、非常に懸念と問題を感じている。我々は、中国政府に説明を求める。サイバースペースにおいて信頼を持って運営する能力は、現代社会・経済において、非常に重要である。
- 我々は、来週、21 世紀におけるインターネットの自由の中心的課題に関して述べる予定であり、また本件について、事実関係が明らかになり次第、更なるコメントを行う予定である[65]。

また、ホワイトハウスの Robert Gibbs 報道官は、2010 年 1 月 14 日の会見で、オバマ大統領も、Google が検閲を受け入れないとしたことを強く支持していると発言している[66]。

＜中国政府の反応＞

これに対して、中国側（中国外交部のスポークスウーマン）は、上記発表の二日後[67]の 2010 年 1 月 14 日、Google のサイバー攻撃・検閲に係る不満には全く触れずに、単に「中国は、外国のインターネット企業を歓迎するが、法に従ってオンラインサービスを提供する必要がある」、「中国のインターネットはオープンである」と述べている（2010 年 1 月 14 日付け NYT 紙[68]）。

一方、中国国務院の情報 Director（Wang Chen 氏）は、「インターネット企業は、国家の安定の脅威となりかねない、ニュース・情報の精査の強化が求められる」とし、「国民の意見を『ガイド』する必要性を強調がある」、同院の Web サイトに掲載している。

---

[64] http://www.state.gov/secretary/rm/2010/01/135105.htm

[65] なお、同日 1 月 12 日、国務省・ロス上級顧問も、ロイターのインタビューに対し、国務省（クリントン長官）は、来週 21 日に、中国を含む外国で検閲されていないインターネットへのアクセスを可能にすることを目的とする技術政策「インターネット・フリーダム」を発表すると答えている。（「コーカサス、中国、イラン、キューバなどでは、人々は検閲されていないインターネットに自由にアクセスできない。われわれのインターネット政策は、国民の情報へのアクセスを組織的に抑圧している国が存在することへの対応でもある。」）

[66] http://www.whitehouse.gov/the-press-office/briefing-white-house-press-secretary-robert-gibbs-11410

[67] なお、Google の発表直後（本発表以前）において、各紙が、中国関係者にインタビューを行っているが、各関係者とも、初耳であり、戸惑っている様子が伺える。
・ロイター報道によると、新華社は、唯一、中国政府高官は、Google の中国事業からの撤退の可能性を示したことについて、多くの情報を収集していると述べた、と報道している。「Google が中国から撤退するかどうかまだ判断しかねる。誰にも分からない」と述べた。
http://jp.reuters.com/article/topNews/idJPJAPAN-13323420100113
・NYT 紙によると、中国の在 NY 総領事館の Wenqi Gao 氏は、NYT の電話インタビューに対して、Google.cn に関して何も問題があるように見えない、と発言。「中国は、外国企業の法的権利と利益の保護にコミットしていることをここで再確認したい。」
http://www.nytimes.com/2010/01/14/world/asia/14beijing.html
・また、WP によると、中国在 SF 総領事館もコメントせず。
http://www.washingtonpost.com/wp-dyn/content/article/2010/01/12/AR2010011202948.html

[68] http://www.nytimes.com/2010/01/15/world/asia/15beijing.html

なお、米国国務省（キャンベル国務次官補）は、2010 年 1 月 19 日時点で、これまでの米中間で、本件に関し複数回協議をしていると明らかにしている[69]。

② クリントン国務長官の演説と中国政府の反応

その後、クリントン国務長官は「インターネットの自由について」に係る演説を行った。本演説の中で、Google の件を取り合げ、中国を非難したことから、インターネットの自由を巡る米中間の対立が再燃することになった。

＜クリントン国務長官の演説＞

2010 年 1 月 21 日、クリントン国務長官は「インターネットの自由について」と題する演説を実施した[70]。今回の演説は、米国の外交においてインターネットの自由に係る米国高官のビジョンとしては始めてのものと位置づけられる。

具体的には、世界の人々にとって、インターネットに接続する自由を得ることが重要となってきており、米国の外交政策としてもそれを推進するという内容であるが、その中で、検閲をベルリンの壁に例えた上で、中国やサウジアラビア、エジプト、チュニジア、ベトナム、ウズベキスタンなど検閲の事例として明示するとともに、Google の件に関しては、中国に対して、調査を行うとともに、その結果を公開すべきと要求した。

クリントン国務長官の演説「インターネットの自由について」要旨[71]

・情報ネットワークは、地球の新たな神経システムとなりつつある。ただし、技術は、善にも悪にも使える。
・昨年、情報の自由な流れに対する脅威となる動きがあった。中国、チュニジア、ウズベキスタン、ベトナム、エジプトなど。このような中、米国は、全ての人が一つのインターネットにつながることを支持する。
・フランクリンルーズベルトは、1941 年に 4 つの自由（表現の自由、崇拝の自由、欠如からの解放、恐怖からの解放）を謳った。21 世紀のインターネットの時代においては、政府の検閲はベルリンの壁のようなもの。また、そのネットワークが信頼できることが繁栄の前提。国務省は、世界的なサイバーセキュリティを強化する。このような中、この 4 つの自由に「接続の自由」を付け加えたい。この接続の自由は、社会を変革するとともに、個人にとっても非常に重要。
・国務省でも、21 世紀の国政・外交として、これに係る能力を強化する。産学との連携を強化。（外交に資する技術のイノベーションへの競争資金の提供、Civil Society 2.0 の実施等）
・近年米国企業もインターネットと情報の自由を考えている。特に Google の事例。我々は、中国当局に対して、本件に関るサイバー侵入に関し、調査を行い公表することを求める。
・情報へのアクセスに関しては、米国と中国は異なった見方を有するが、我々は、前向き、協力

[69] http://www.nikkei.co.jp/news/kaigai/20100120ATGM2001T20012010.html
[70] http://www.nytimes.com/2010/01/22/world/asia/22diplo.html
http://www.state.gov/secretary/rm/2010/01/135519.htm
なお、米国政府は、クリントンの演説に中国のブロガーをワシントン DC に招へいするとともに、翌日 22 日には在北京の中国大使館でも本件に係るブリーフィングに中国のブロガーを招待している。
[71] http://www.state.gov/secretary/rm/2010/01/135519.htm

的、包括的な関係の中で、違いを明確にするつもりである。これは、情報の自由の問題ではなく、我々はどのような世界にしたいのか、住みたいのかという問題である。国務省は、Global Internet Task Force を再活性化する。

なお、本演説に関しては、米国の人権団体等は支持する旨を発表している[72]

＜クリントン長官の演説に対する中国政府の反応とその後＞

このクリントン長官の演説に対して、中国側は強く反発し、米中間の対立が再燃することになる。実際に、1 月 22 日付け NYT 紙によると、上記演説前までは、中国政府は、本件を単に、Google が中国でのビジネスに失敗して撤退しようとしているという問題にしようとしていたが[73]、演説後には、中国の態度が変化しつつあるとしている。具体的な発言等は、以下の通り（1 月 22 日付け NYT 紙[74]、1 月 25 日付け NYT 紙[75]）

- 演説の翌日の 1 月 22 日、中国外交部の広報官は、同部のウェブサイトにおいて、「米国連邦政府は、事実関係を尊重するとともに、いわゆるインターネットの自由の問題を、根拠のない批判に使うことを辞めるべきだ」、「米中間に悪影響を及ぼす」とした上で、「中国のインターネットはオープンである」との文章を掲載。
- 中国の Global Times（共産党系の愛国者な新聞）の英語版では、社説において、「米国の要求は、途上国が情報の流れで先進国に競合できない中、情報・インターネットで覇権を握ろうとする『情報帝国主義』であり、民主主義の名の元で、自国の価値観を他国に押し付ける偽善的な取り組みである」と主張。
- 週の明けた 1 月 25 日、新華社通信によると、国務院は「政府が有害と考えるサイトを検閲することは全く正しく、事実に即することなく不必要に中国を非難したり、中国の法律を無視したり、中国の内政に関与しようとする者には断固として反対する」と述べた。
- 上記 Global Times は、「Google の件は、米国政府によって仕組まれた戦略であり、インターネットの自由は、米国の覇権支配に向けた第一歩にしか過ぎない」とのアナリストのコメントを掲載。

---

[72] 例えば、・Human Rights Watch（1 月 21 日）：演説を支持するとともに、いくつかの提言を発表。
- 米国の外交筋は今回の演説のような内容を定期的に公表するべきである。
- 米国の政府機関は体制を確立させるべき。（商務省や米国通商代表部（USTR）等）。
- 政府批判の検閲のために利用しないことを確立するよう、輸出規制を再検討すべき。

http://www.hrw.org/en/news/2010/01/21/us-clinton-press-internet-freedom

・Human Rights First（1 月 21 日）：演説を支持する趣旨のプレスリリースを発表。「Human Rights First は、クリントン国務長官の演説を受け、Global Network Initiative と協力しあい、外交上の優先事項としてインターネットの自由化を求めてくという、政府による努力を支援していく」

[73] 例えば、新華社通信によると、外交部次官は、Google の問題は過大解釈すべきでなく、米中間の二国間関係と結び付けられるべきでない、と発言したとしている。

[74] http://www.nytimes.com/2010/01/23/world/asia/23diplo.html

[75] http://www.nytimes.com/2010/01/26/world/asia/26google.html

・ 別の記事では、「米国議会は、9/11 以降諜報の権限を強化していることから、クリントン長官の中国への批判はダブルスタンダードである」としている。

なお、本件に関し、国務省の Crowley 次官補は、2010 年 1 月 22 日、在 DC の中国大使と議論を行ったとしている[76]。また、ホワイトハウスの報道官代理は、1 月 22 日、我々は中国からの返事を待っている段階であると述べている[77]。また、その後、1 月 28 日に、クリントン国務長官が、中国の楊外相と会談を行った際に、本件について議論を行う今後協議を継続することで合意したと報じられている[78]。

一方、2010 年 3 月 11 日、国務省は、2009 年版の人権報告書を発表しているが、その中で、中国に関しては、インターネットの自由の問題を明記している[79]。

③ 米国国内における動向（議会の動きとその他の民間企業の動き等）

このような中、米国国内では、連邦議会でのインターネットの自由に係る公聴会の開催や法案の提出など、インターネットの自由を巡る民間企業への規制等を巡る動きが再度活発化しつつある[80]が、一方、民間の IT 企業においては、Google に追随しようとする動きは見れらず、むしろ、政府が非関税障壁として取り組むべき課題であるとする意見も再燃しつつある。

＜連邦議会における動き＞

インターネットの自由に関し、連邦議会においては、上院（司法委員会）が、2010 年 3 月 2 日、「世界的なインターネットの自由と法の支配」に関する公聴会を[81]、また、下院（外交委員会）でも、3 月 10 日に、「グーグルの苦境：民主主義、安全保障、貿易の促進に向けた米国のサイバースペース政策の改革」に係る公聴会を開催している[82]。

---

[76] http://www.state.gov/r/pa/prs/dpb/2010/01/135694.htm
http://www.nytimes.com/2010/01/23/world/asia/23china.html

[77] http://www.whitehouse.gov/the-press-office/gaggle-deputy-press-secretary-bill-burton-aboard-air-force-one-en-route-cleveland-o

[78] http://sankei.jp.msn.com/world/america/100129/amr1001290953001-n1.htm

[79] http://www.state.gov/g/drl/rls/hrrpt/2009/eap/135989.htm

[80] http://www.nytimes.com/2010/03/02/technology/02internet.html
http://online.wsj.com/article/SB10001424052748704548604575097603307733826.html

[81] http://judiciary.senate.gov/hearings/hearing.cfm?id=4437
主催は、Richard J. Durbin 上院議員（民主党、イリノイ州選出）ら。
Durbin 上院議員は、Google がインターネット検閲への協力をやめるとしたことは評価した上で、Yahoo や Microsoft（Bing）なども、そのような努力を続けるべきであるとコメントしている。
http://latimesblogs.latimes.com/technology/2010/03/google-internet-censorship-china.html

[82] http://www.internationalrelations.house.gov/hearing_notice.asp?id=1160
主催は、Howard L. Berman 下院議員（民主党、カリフォルニア州選出）。もともと 2 月 10 日に開催予定であったが、悪天候により延期され、3 月の開催となった。

また、Chris Smith 下院議員（共和党、NJ 州）[83]、および David Wu 下院議員（民主党、OR 州）の 2 下院議員は、2010 年 3 月 9 日、インターネット上での国際的な言論の自由の促進に向けた党員集会である、Global Internet Freedom Caucus を発足する[84]とともに、Wu 下院議員は、同日、「インターネット自由基金の設立等に関する法案（H.R. 4784）」を議会に提出している[85]。

＜他の民間 IT 企業の動向＞

両公聴会には、Google からは Nicole Wong 副社長兼次席法務顧問が出席している[86]が、他の IT・インターネット系企業はほとんど参加していない。特に、上院の公聴会に関しては、その開催に当たって、Amazon、Apple、eBay、Verizon などの米国 IT 企業 30 社に対し、中国でのビジネス慣行と人権問題に係る情報提供を求める書簡を送ったほか[87]、Facebook、Twitter、Apple、HP、McAfee を証人として招待したものの、これらの企業は同公聴会での証言を拒否したとしている[88]。

また、Microsoft、Yahoo、Google などの 24 企業・団体は、2008 年に、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ティブである Global Network Initiative[89]を発足しているものの、2010 年 3 月 1 日付 NYT[90]

同公聴会では、米国へのサイバー攻撃と知財権の盗難の防止の重要性が確認された他、米中経済安全保障検討委員会（US-China Economic and Security Review Commission）の Larry M. Wortzel 氏により、中国によるサイバー攻撃の主な理由として、①政治的理由、②産業スパイ活動のため、③将来の攻撃に役立つ情報の収集ため、の 3 点が紹介された
http://csis.org/blog/house-google-hearing-and-observations-multinational-corporations-and-legal-framework

[83] なお、同氏は、これまで、Global Online Freedom Act 等を何度も提出してきているが、これまで廃案になってきている（NY だより 2009 年 3 月号参照）。

[84] http://techdailydose.nationaljournal.com/2010/03/net-freedom-caucus-launched.php
この超党派の党員集会は、インターネットの自由の促進に向け、インターネットの自由が侵害されている国々で事業を行う米国企業がオンライン上の自由を強化するための最低限の指標を策定するためのアイデアについて、議会、行政機関、産業界が議論できる場を提供することを目的としている。
http://www.house.gov/apps/list/press/or01_wu/pr100309InternetFreedom.html

[85] http://www.govtrack.us/congress/bill.xpd?bill=h111-4784
同法案では、大学や民間企業、その他研究機関などに対し、インターネット上での言論統制や検閲に対抗するための技術を開発するためのグラントやアワードなどを提供するインターネットの自由基金（Internet Freedom Foundation）の NSF 内への設立が提案されている。
http://techdailydose.nationaljournal.com/2010/03/net-freedom-caucus-launched.php
なお、これ以外にも、2010 年 1 月 26 日、インターネット検索企業による検閲を規制する権限を FCC に与える法案が提出されている。http://news.cnet.com/8301-13578_3-10466272-38.html
http://thomas.loc.gov/cgi-bin/bdquery/z?d111:hr.04504:

[86] 同氏は、Google は中国・イランなどにおけるインターネット検閲の中止に取り組んでいると述べたものの、時期については明言しなかったとのことである。
http://latimesblogs.latimes.com/technology/2010/03/google-internet-censorship-china.html

[87] http://www.nytimes.com/2010/03/02/technology/02internet.html

[88] http://government.zdnet.com/?p=7497

[89] http://www.globalnetworkinitiative.org/index.php NY だより 2009 年 3 月号を参照。

によると、同イニシアティブで定められた原則がどの程度実行に移されているかは依然として不明瞭としている。なお、Global Network Initiative は、クリントン長官の演説に関し、同組織が提供するガイドライン等と一致するものであり、同ガイドラインは国際的に受け入れ可能な標準であると述べている[91]、国際的に標準となるような取り組みの必要性を示唆している。

＜検閲を貿易障壁として取り扱うことを求める動き＞

なお、上記公聴会において、Google の Wong 氏が、再度[92]インターネット上の検閲を、貿易障壁（非関税障壁）とみなして、米国・外国政府間でルールを作成するよう要請したこと[93]を踏まえて、再度 WTO の活用の議論が出ている。

具体的には、その翌日の 3 月 3 日、Google と関連のある Computer & Communications Industry Association（CCIA）[94]および First Amendment Coalition は USTR に対し、中国側によるウェブアクセスと内容の制限は米国のインターネット企業とインターネット産業に対する差別にあたり、このような差別行為は、WTO の規則に違反するとの考えを表明したと報道されている。

そのような中、2010 年 3 月 9 日、USTR の Ron Kirk 代表は、中国による検閲を WTO に法的に訴えることができるか検討中と発言している[95]。ただし、同代表は、併せて、米中合同商業貿易委員会（JCCT）などの二国間協議の方がより迅速な結果をもたらす可能性があるとの見方を示している。

（３）中国国内での動向と Google と中国の交渉

一方、Google の撤退する可能性があることに関し、中国国内においては高学歴層を中心に懸念があり、また、中国政府にとっても望ましくないと考えていると想定されるものの、Green Dam のときのように、国内世論において検閲に反対する盛り上がりがある訳でない。

このような中、Google と中国側との交渉の結論が今後どうなるか注目される。

①　Google の撤退可能性に係る中国国内の動向

---

[90] http://www.nytimes.com/2010/03/02/technology/02internet.html
[91] http://www.globalnetworkinitiative.org/newsandevents/Clinton_Internet_Freedom.php
[92] 本件は、2007 年にも、Google によって提起がなされている。NY だより 2009 年 3 月号参照。
[93] http://www.informationweek.com/news/security/vulnerabilities/showArticle.jhtml?articleID=223101378
[94] CCIA は、2010 年 1 月 22 日には、インターネットの自由に係る政策ペーパーを作成しており、その中でも、検閲を貿易障害とみなすこと、を挙げている。
http://www.ccianet.org/CCIA/files/ccLibraryFiles/Filename/000000000315/InternetFreedomwh.pdf
[95] http://headlines.yahoo.co.jp/hl?a=20100310-00000680-reu-bus_all
http://www.nytimes.com/reuters/2010/03/09/technology/tech-us-usa-china-google-wto.html

今回の件に関して、中国国内においては、検閲の問題が原因ではなく、Google の中国でのビジネス上の問題であると報道されていることもあって、特に Google を利用する高学歴層を中心に、Google の撤退可能性を残念がる意見はあるものの、比較的冷静に受け止められている模様である。

＜中国国内での報道振りと世論の動向＞

今回の Google の中国撤退可能性の表明は、世界中を駆け巡ったが、2010 年 1 月 13 日付け NYT 紙[96]によると、中国国内では、当初、そもそもニュースが強く検閲されている。実際に、当初、中国のニュースポータルでは、Google の表明が載せられたが、その後、「free speech（言論の自由）」や「survellance（監視）」といった言葉は、削除されたとしている[97]。

その後、本件に係る情報は着実に広がっているものの、2010 年 1 月 20 日付け NYT[98]によると、中国国内では、中国側は政治化にしないよう、今回の Google の撤退可能性の発表は、同社が中国でのビジネスに成功していないというビジネス上のトラブルが原因と報道されており、したがって、市民・ネチズンは比較的冷静に見ているとされる。

このような中、一部 Google の主張を強く支持する層は一部裏には存在するものの、国内世論全体として、中国側は、検閲を廃止しなければいけないというような状況には全くないものと考えられる。

もちろん、一方で特に高学歴層を中心に、その理由はともかく、Google が中国から撤退することを残念に思い、あるいは懸念する層は着実に存在する[99]。

Google の発表直後、Google China の本部前には、献花が多数届け出られたことを始め、中国国内においても Google への支援が広がっていると報道されている（2010 年 1 月 14 日付け NYT[100]）。中でも、Google のユーザーは、Baidu よりも高学歴、富裕層であり、Baidu よりも（検閲が少ないためもあって）検索結果に対する評価は高く、これらの層には Google の検索エンジンは、重宝されているとされる。このため、若い教育レベルの高い中国人は、Google が撤退することに懸念を示しているとされる（2010 年 1 月 16 日付け NYT[101]）。

---

[96] http://www.nytimes.com/2010/01/14/world/asia/14beijing.html

[97] 一方、中国の Twitter のようなサイト Sina.com では、Google の発表直後、本件に係る話題がトレンドのトップになったとしている。
http://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011301168.html

[98] http://www.nytimes.com/2010/01/21/world/asia/21china.html

[99] なお、一方で、中国市民における対応として、検閲を抜けるためのツール（Fanqiang、AnchorFree、GIF）を活用する動きや、Google や Youtube の模倣サイトが作られる動き（Goojje、Youtubecn.com など。これに対し、Google は、当該模倣サイトに対し、停止を要求）、などもある。
http://www.nytimes.com/2010/01/16/technology/internet/16evade.html
http://www.itmedia.co.jp/news/articles/1002/10/news033.html

[100] http://www.nytimes.com/2010/01/15/world/asia/15china.html

[101] http://www.nytimes.com/2010/01/17/world/asia/17china.html

また、2010 年 2 月の報道によると、中国の科学者の 90%以上が Google の検索を利用し、48%が、もし Google が撤退するとなると研究に顕著な支障が生じるとして、懸念を表明している[102]。

＜中国から見た Google の撤退可能性の位置づけ＞

一方で、中国政府においても、できれば Google が撤退しないことを望んでいるものと考えられる。

実際、中国側は、Google の発表に対し、「中国は、外国のインターネット企業を歓迎する」としているが、実際に、Google が撤退するとなると中国の対外的イメージの観点からも望ましいものではない。また、産業構造的な観点からみても、仮に Google が撤退すると、Baidu に得になるかもしれないが、その場合 Baidu の独占となってしまい、Baidu においては Google との競争がなくなるため、技術革新を行うモチベーション（及び技術の習得先も）を失ってしまい、結局中国全体にとっても望ましくないとの見方がされている（2010 年 1 月 13 日付け NYT[103]）。

② Google と中国の交渉の状況

このように、中国側から見れば、検閲を廃止するつもりは全くなく、むしろインターネット管理は引き続き強化する方向にある[104]ものの、Google にはできれば残って欲しいという状況において、Google と中国側の交渉が行われており、今後その結論が注目される。

Google の CEO の Eric Schmidt 氏は、発表の約 1 週間後の 2010 年 1 月 21 日の決算発表時において、中国政府との対話を既に開始しており、中国でのビジネス継続を望む姿勢を明確にしつつも、あくまでも検閲撤廃を求める立場であると説明している[105]。

その際、もともと交渉は数週間とされていたが、その後 2 ヶ月強たった現時点でも、交渉の状況はほとんど明らかにされていない[106]。

---

[102] http://arstechnica.com/science/news/2010/02/chinese-scientists-worry-about-google-pullout.ars

[103] http://www.nytimes.com/2010/01/14/technology/companies/14baidu.html

[104] 2010 年 2 月 23 日付け報道（AP）によると、中国（商務部産業情報部）は、全ての Web サイト事業者（ドメイン取得者）に対して、ISP に直接会って写真を提供することを義務付けるよう、インターネット管理の強化を試行的に実施する方針と報じている。同規制は、ポルノ撲滅の一環の名目で行われるが、その他の全ての国内のオンラインコンテンツについても、政府は記録することが可能になるとされる。
http://www.afpbb.com/article/environment-science-it/science-technology/2701193/5393806
http://news.cnet.com/8301-27080_3-10458420-245.html
http://www.boston.com/business/technology/articles/2010/02/23/china_launches_strict_new_internet_controls/

[105] http://www.nikkei.co.jp/news/kaigai/20100122ATGM2201I22012010.html

[106] なお、本件の影響に伴い、2010 年 1 月 19 日、Google と ChinaUnicom は、Android のスマートフォン（2 機種：Samsung, Motorola）の発表の延期を表明したが、1 月 27 日、中国は Android に制限はないと説明しており、それを踏まえて、ChinaUnicom は 3 月 3 日販売の意向を表明している。

なお、これまでの断片的な情報は以下の通り。

- 2001 年 2 月 12 日、共同創業者の Brin 氏は、交渉の期限を示さず、「いつの日か、中国側が態度を変え、Google が検閲を受けない検索エンジンが提供できる日が来る可能性があると思う」とだけコメントをした[107]。
- 2010 年 2 月 23 日付けの WSJ[108]は、中国の旧正月で止まっていた中国側との協議が再開されたと報じている。ただし、協議は難航している模様であり、協議の内容は一切コメントできないとしている。
- 2010 年 3 月 2 日、Google は議会の公聴会において、Deadline は全く設定していないと発言[109]。
- 2010 年 3 月始め、新華社通信等から、中国の商務部（産業情報技術部）を中心に、中国政府側と Google が交渉しているとの噂が流れている[110]。

このような中、2010 年 3 月 10 日、Google の CEO の Eric Schmidt 氏は、Google と中国政府の協議はまもなく決定に至るであろうとの見解を示したと報じられている[111]。ただし、その後、3 月中に結論が出す必要があるが、交渉は行き詰った[112]、中国の広告代理店が Google に賠償を請求する[113]などの情報が流れており、Google にとっては厳しい状況に追い詰められているようにも見える。

---

http://www.nytimes.com/2010/01/20/technology/companies/20phone.html
http://www.nytimes.com/aponline/2010/01/27/business/AP-AS-China-Google.html
http://japan.cnet.com/mobile/story/0,3800078151,20409780,00.htm

[107] http://japan.cnet.com/news/media/story/0,2000056023,20408542,00.htm

[108] http://japan.cnet.com/news/biz/story/0,2000056020,20409135,00.htm

[109] http://www.businessweek.com/news/2010-03-02/google-doesn-t-have-timetable-to-end-censorship-executive-says.html
http://www.boston.com/business/technology/articles/2010/03/02/google_still_considering_how_to_proceed_in_china/

[110] 具体的には、同部部長は、中国政府が Google と交渉していると発言したこと、また、その後、同部副部長は、Google が受けたハッキング行為に係る報告書がまだ提出されていないこと、等が報道されている
http://www.computerworld.jp/topics/vs/176329.html
一方で、同副部長は、Google とは直接コンタクトはとっていないとの発言をしているとの報道もある。
http://www.boston.com/business/technology/articles/2010/03/06/china_no_direct_contact_with_google_on_dispute

[111] http://online.wsj.com/article/SB10001424052748703701004575113550674654886.html
http://japan.cnet.com/news/biz/story/0,2000056020,20410189,00.htm

[112] FT は、「交渉は前週行き詰まり、Google は 99.9%、Google.cn を閉鎖することになる」としている。
http://www.nytimes.com/reuters/2010/03/17/business/international-google-china.html

[113] 2010 年 3 月 17 日付け報道によると、Google の検索ページの広告スペースを販売している中国の広告代理店の連合体は、Google に対して、今後の中国ビジネスの見通しを明らかにするよう要求するとともに、中国事業を閉鎖した場合は、賠償を請求すると警告するレターを提出したと報じられている。（本件は、Google に対して撤退しないよう政治的財政的圧力をかけるものとみなされている。）
http://www.nytimes.com/reuters/2010/03/17/business/international-google-china.html
ただし、その翌日の 3 月 18 日には、その連合体に参加するほとんどの代理店がそのレターを承認していいないとも報道されている。
http://www.nytimes.com/2010/03/18/technology/18chigoogle.html

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の一切について、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。