サイバーテロへの備え

Preparedness for Cyber-terrorism

杉野　隆，Takashi Sugino
日本大学商学部，Department of Commerce, Nihon University

要旨

IoT がサイバー空間に急速に参入している。今後は，重要インフラや Smart TV，Smart meter などが本格的に IoT を利用すると予想されるが，野良 IoT の増加によってサイバーテロが発生し，社会基盤システムや社会生活に甚大な影響をもたらす可能性が大である。しかし，政府のサイバーセキュリティ戦略はサイバーテロへの備えという視点を欠いている。本稿では，サイバー攻撃の特徴，抑止理論の観点から見るサイバーテロの特徴を確認し，現状の課題，方向性について論じた。

1　はじめに

2018 年 7 月に公表された『サイバーセキュリティ戦略 2018』では，当然ながらサイバー攻撃について詳述しているが，サイバーテロについては全く触れていない。一方，警察庁では，「サイバーフォースセンター」[1]を中心に，民間事業者及び関係機関と連携し，事業者などから提供された情報を集約して総合的な分析を行い，事業者などに対し分析結果に基づく注意喚起などを行っている。ここにはサイバーテロ対策も含まれる。重要インフラ施設を運用する重要インフラ事業者を管轄する省庁は，金融庁，総務省，厚生労働省，経済産業省，国土交通省に分散しているが，事故が発生すると警察庁の事案となる。

本稿では，まず，サイバーテロとサイバー攻撃の相対的な違いを確認し，電力事業における Internet of Things（IoT）機器の代表例としてスマートメータの利用状況と重要性を紹介したのち，今後の IoT 機器の拡大とともにサイバーテロ対策はより重要な課題となり，政府の関与が求められることを提言する。

2　研究への動機

本研究の動機となった二つの動機を紹介する。

①Bruce Schneier の新著発刊

米国の暗号・情報セキュリティの研究者である Bruce Schneier が，本年 9 月に “Click Here to Kill Everybody”という著書[2]を出版した。Schneier は，あらゆるモノがインターネットに接続される状態を Internet + Things + us（略して Internet+）と呼んでいる。かつて Internet は仮想世界を構成するに過ぎなかったが，現在では，我々人間が Internet+に包摂され，すべてのモノがインターネットに接続され，IoT を経由して物理世界をセンスし，物理世界を動かす。このことにより，PC をクリックすれば誰をも殺すことができるようになったと，Schneier は警告を発している。

②「サイバーセキュリティ戦略 2018」の公表

1998 年 5 月に米国で大統領令 PDD 63 が発行され，サイバー攻撃から重要インフラ[3]を保護するために必要な措置を講じるという政策が始まった。その後日本では，2000 年 1～2 月に多くの中央官庁で Web ページが改ざんされるという事件が相次ぎ，政府は大きな衝撃を受けた。この事件によって，サイバー攻撃や大規模な個人情報漏えい事故への備えの必要性を認識した。日本の情報セキュリティ元年である。その直後の 2 月に内閣官房に情報セキュリティ対策推進室[4]が設置され，その年の 12 月に初めてのサイバーテロ対策計画として「重要インフラのサイバーテロ対策に係る

---

[1] 2001 年 4 月に警察庁情報通信局に設置された「サイバーテロ対策技術室」の別称

[2] Schneier, Bruce *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World*, W. W. Norton & Company, 2018.

[3] 日本では米国と定義がやや異なるが，日本では，「他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び社会経済活動の基盤であり，その機能が停止，低下又は利用不可能な状態に陥った場合に，我が国の国民生活または社会経済活動に多大な影響を及ぼす恐れが生じるもの」と定義されている。現在，情報通信，金融，航空，鉄道，電力，ガス，行政・サービス，医療，水道，物流，化学，クレジット，石油の 13 分野が指定されている。critical infrastructure

[4] 2005 年 4 月に改組され，情報セキュリティセンター，内閣サイバーセキュリティセンター（いずれも，NISC と略称）としてサイバーセキュリティ対策の中核を担っている。

特別行動計画」（以下，「特別行動計画」）を発表した。以降 4 年前後の間隔を置いて同種の行動計画が公表されている。「特別行動計画」では「サイバー攻撃」が 16 回，「サイバーテロ」が 17 回出現しているが，内訳は，「いわゆるサイバーテロ」が 8 回，「サイバーテロ対策」が 9 回である。「いわゆるサイバーテロ」とは「巷間言われる」といった限定付き表現であり，公式の用語とは認められないという印象を受ける。2005 年行動計画では，「サイバーテロ等」が 2 回，「サイバーテロ対策」が 2 回と大幅に減少し，2009 年以降も「サイバーテロ等」としてそれぞれ 1 回使われるだけである。

2014 年 11 月に施行されたサイバーセキュリティ基本法の規定に基づき，内閣にサイバーセキュリティ戦略本部が設置されたが，それに先立ち 2013 年 6 月に，サイバーセキュリティに関する基本的な計画を「サイバーセキュリティ戦略 2013」として公表した。ここでサイバーテロは 2 回出現したが，それ以降は忘れられている。過去のサイバーセキュリティ戦略及び重要インフラに特化した行動計画における「サイバーテロ」と「IoT」の出現回数を調べてみたところ，表に示すように，前者は初期を除き，非常に少ないが，一方後者は近年急増していることが分かる。

表　サイバーセキュリティ戦略での出現頻度

	情報セキュリティ基本計画，国民を守る情報セキュリティ戦略，サイバーセキュリティ戦略 [1)]						重要インフラの情報セキュリティ対策に係る行動計画 [2)]				
発表年	2006	2009	2010	2013	2015	2018	2000	2005	2009	2014	2018
頁数 [3)]	26	70	16	43	40	43	8	29	48	58	59
IoT	0	0	0	0	48	37	0	0	0	0	4
重要インフラ	36	58	30	49	40	37	多数	多数	多数	多数	多数
サイバーテロ	0	4	0	2[4)]	0	0	17	4[5)]	1	1	1

注1 戦略レベルの文書は，「情報セキュリティ基本計画」（2006，2009 年），「国民を守る情報セキュリティ戦略」（2010 年），「サイバーセキュリティ戦略」（2013 年以降）と名称を変更しつつ継続
注2 2000 年は「特別行動計画」，2005 年以降は第 1～4 次「行動計画」として公表
注3 頁数には表紙から目次までを，また 2018 年度にのみ別紙添付された担当府省庁一覧（3 頁）を除外
注4 「サイバーインテリジェンス対策のための不正通信防止協議会」に関する脚注にのみ出現
注5 本文ではなく脚注において，「サイバーインテリジェンス情報共有ネットワーク」の関連として出現

これらの文書はすべて NISC の管轄であるが，警察庁の文書では，警察白書も含め，「サイバーテロ」が頻出する。サイバーテロの管轄省庁には，警察庁，消防庁，海上保安庁及び防衛省があるが中心となるのは警察庁である。警察庁はサイバー犯罪の事案対処官庁と位置付けられている。

一方，警察庁は，先進国首脳会議（サミット）でのハイテク犯罪に関するそれまでの議論の積み重ねを受けて，「情報セキュリティ政策大系」（2000 年 2 月）[5]の中でサイバーテロを定義し，ハッカー，不正アクセス，サイバーテロなどのサイバー（当時はハイテク）犯罪対策を強力に進めると言明している。サイバー犯罪を新たな刑事犯として積極的に取り組む姿勢を示している。しかし，内閣官房の資料では，サイバーテロの定義も見当たらなかった。「いわゆるサイバーテロ」という表現は，組織間の縄張りへの配慮ということなのであろうか。

3　サイバー攻撃とサイバーテロの違い

サイバー攻撃全般の特徴と，サイバーテロ特有の性格とに分けて議論する。

3.1　定義

例えば日本大百科全書（ニッポニカ）では，サイバー攻撃を，「インターネットを通じ，企業などのシステムを攻撃する行為。標的とする団体や個人の持つサーバや個別のパソコンに不正ログインし，そのシステム内のデータを改ざん，破壊，盗むなどするのが一般的である。」と定義し，さらに付言して，「攻撃対象を社会基本インフラや政府機関としたものは，特にサイバーテロともよばれる。」としている。

この社会基本インフラに政府・自治体サービスを含めた概念が，重要インフラである。従来から，テロリズムを「政治的な目的を達成するために暴力及び暴力による脅迫を用いることをいい，

[5] ハッカー対策が中心であるが，霞が関における一連の Web 改ざん事件への言及はない。「サイバーテロ」は 59 回出現している。

大衆の間に恐怖心を植え付けることを最大の目的とする。」と定義していることと合わせて，サイバー空間におけるテロリズムをサイバーテロリズム cyber-terrorism，略してサイバーテロと定義することはごく自然であろう[6]。

3.2　サイバー攻撃の特徴

まず，サイバーテロを含むサイバー攻撃共通の特徴を述べる。サイバー空間においては，攻撃側が防御側に対して圧倒的な優位にある。防御側は，ソフトウェアあるいはネットワークにおける脆弱性を完全に排除することが困難であり，攻撃側はネットワークの最も脆弱なポイント（これもソフトウェアが自動的に探索してくれる。）を突いて攻撃すればよい。一方，防御側が，攻撃されている（された）ことを迅速に認知することは（Web サイト改ざん，情報漏えい，DoS/DDoS 攻撃など結果が分かり易い攻撃を除けば）困難であり，攻撃側の正体とその原因の特定には時間を要し，原因不明のまま終わることもある。特徴としては次の 3 点を挙げられる。

①攻撃に要するコストが少ない　サイバー攻撃の最大の特徴は，攻撃の実行に要するコストが，暗殺，破壊活動あるいは軍事攻撃などの物理的攻撃と比べて大幅に小さいことである。

②攻撃側及び攻撃手法の多様性と匿名性　攻撃は世界のどこからでも，どこに対しても実行できる。しかも，個人でも組織でも，手法は基本的には同一であり，攻撃側の正体は見分けにくい。

③攻撃の目標が目に見えないことが多い　攻撃の目的は，防御側の設備の物理的な破壊であるよりも，情報システムの機能又は信頼性，並びに社会的評判に対する破壊であることが多い。

④コンピュータウイルスは 1970 年に APRANET に発生した Creeper をもって嚆矢とするといわれるが，2000 年頃までは，作者が自らの技術力を誇示するための表現手段であったが，現在は，標的型攻撃やランサムウェアといった金銭詐取，防御側のシステム機能妨害といった大きな実害をもたらす攻撃が主流になっている。

3.2　サイバーテロとは

サイバー攻撃とサイバーテロは情報通信技術としては同一であり，特徴も重なるが，社会に与える影響は大きく異なる。サイバー攻撃は，個人又は組織に対してネットワークを麻痺させ，特定のサーバやデータベースを改ざん・破壊するわけだが，被害の範囲は限定されている[7]。しかし，サイバーテロリスト[8]が，情報通信技術を悪用して，組織や社会を機能不全に陥らせ，広範かつ甚大な損害や恐怖心を与えようとすれば，重要インフラを攻撃するほうが効率的である。これをサイバーテロとして分けて扱う。重大インフラ以外でも，例えば社会的影響力の大きい大企業を狙えば，効果は大きい[9]。また，サイバー攻撃はサイバー空間内に留まるのに対して，サイバーテロはその影響が物理空間にも及ぶ。例えば，空港や発電所の機能停止は社会活動に支障を来す，政府・自治体の運営に支障を来すといった事態を引き起こし，社会を不安に陥れる虞が大である。

3.3　サイバーテロと抑止理論

抑止とは，攻撃側による攻撃行動を防御側が何らかの手段によって防止することである。抑止理論は 1960 年代の核戦争時代に検証された理論だが，現在では安全保障分野のみならず，サイバーテロの予防にも適用されている。抑止には，懲罰的抑止（攻撃側に対し，耐え難い損害を与える対抗措置を防御側が取ると思わせる）と拒否的抑止（攻撃側に対し，攻撃行動による利得を与えないだけの能力を防御側が持っていると思わせる）がある。ただ，懲罰的抑止と拒否的抑止の境界は絶対的なものではなく，ここでは懲罰的抑止に絞って議論する。懲罰的抑止には次の三つの成立要件がある。

①　帰属問題　サイバー空間の向こうに存在するはずの攻撃側の物理的存在場所を特定できないことである。これには，IP アドレスの偽装，サーバの乗っ取り（踏み台攻撃）など技術的問題

---

[6] Pollitt, Mark M. CYBERTERRORISM - Fact or Fancy?, 1998, https://www.sciencedirect.com/science/article/pii/S1361372300870098

[7] もちろん，強力な感染力を持ち，ウイルス感染 PC から他の PC に感染させる能力を有するウイルスも多いが，被害はサイバー空間内に限定される。

[8] サイバーテロリストは，①国家機関や軍関係者，②ハッカー集団（Anonymous が代表的），③職業ハッカーなどに分類される。

[9] 2014 年 11 月に米ソニーピクチャーズエンタテインメント（SPE）が不正アクセスを受け，社内関係者間での電子メール、従業員の個人情報、未公開の映画本編のコピーといった様々な情報の流出を引き起こした。SPE は金正恩暗殺を描いたソニーのコメディ映画『The Interview』の上映を中止した（テロに屈したとの批判もあった）。翌 12 月に FBI は SPE の事件に北朝鮮のハッカー集団 Lazarus が関与したと断定した。

と，攻撃側の実体が多様であり，単独行為（個人，非国家グループ）なのか国家などの組織が背景にありその指示・支援による行動なのかが特定できない（匿名性）と防御側は威嚇した報復を履行することができないという二つの問題がある[10]。中国，ロシア，北朝鮮などの国家が各国へのサイバーテロ活動を支援している可能性が濃厚でも，決定的な証拠をつかめないままのケースが非常に多い。

② 伝達の問題　防御側が攻撃側の何を思いとどまらせようとしているのかが、相手には正確に把握できないという問題である。仮に防御側の警告を無視して攻撃に踏み切った場合にはどのような報復を招くことになるのかを，攻撃側に明確な形で伝達し，かつ理解させなければならない。

③ 信頼性の問題　防御側が威嚇する報復を履行する意思と能力を有することを攻撃側が信じているかという問題である。抑止が成立するか否かは，攻撃側の意思決定によって決まるので，攻撃側が防御側による報復の履行を信じるに至らなければ，抑止は成立し得ない。

④ 合理性の問題　攻撃側が③の比較衡量を合理的な計算に基づいて行うかという問題である。合理的計算がなければ，他の要件が満たされていようとも，抑止は成立しない。政治目的，宗教的又はイデオロギ的な変更を追求して，あるいは単純に技術的な好奇心から強固なセキュリティシステムを突破することを目的として攻撃側に対しては，基本的に抑止は機能しにくい。

特に合理性の問題が，例えば中東をはじめ世界各地でのテロ活動と同様に，サイバーテロの予防を困難にしている。

4 IoT

4.1 IoT の定義

Internet of Things という言葉を最初（1999 年）に使ったのは，無線タグの標準化団体 Auto-ID の創設者の一人である Kevin Ashton であり，彼は，「センサをあらゆる場所に配置することで，物理的なモノの世界とインターネットを結びつけること」と定義した。現在では，その構造が拡大し，ISO/IEC 20942 の Committee Draft では「物理世界及び仮想世界から得た情報を処理し，物理世界及び仮想世界に作用するインテリジェントサービスによって実体，人，システム及び情報資源が相互接続されたインフラストラクチャ（下線筆者）」と定義している。すなわち，IoT は，物理世界及び仮想世界のあらゆる人間活動を支える基盤であり，Schneier の Internet+と，ほぼ同様の概念である。

4.2 最近のサイバーテロの事例

ここ 10 年ほどの間に話題になったサイバーテロの事例をいくつか示す。

2010 年 6 月　イランの核関連施設の制御システムが USB メモリを介して Stuxnet に感染
2012 年 7 月　ロンドン，ソチ（2014），リオ（2016），平昌（2018）各オリンピック大会で大量の攻撃があったが，いずれも実質被害には至らず
2013 年 3 月　韓国の金融機関・放送局がトロイの木馬型マルウェアに感染しサービス不能に
2014 年 12 月 韓国原発の運営企業である韓国水力原子力から内部資料が流出
2015 年 5 月　日本年金機構。標的型メール攻撃によって 125 万人分の個人情報が漏えい
2015 年 12 月 ウクライナの変電所に DDoS 攻撃。翌年 12 月にマルウェア攻撃によって停電
2017 年 8 月　中東の発電所の制御システムがマルウェア感染により工場停止

英王立国際問題研究所（RIIA）が 2015 年 10 月に発表した調査[11]によると，世界各国における民間原子力発電所の情報セキュリティ対策は不十分であり，制御システムへの攻撃の結果，停電や原子炉そのものの損傷を招く恐れもあるという。

4.3 IoT とサイバーテロ

平成 29 年度版情報通信白書（図表 3-3-1-1）によると，世界の現在の IoT デバイス数では，コンシューマ用（監視カメラ，Smart TV，冷蔵庫などの家電製品）が最多だが，今後産業用途，医療用の接続台数が急速に伸びていくと予測されている。

---

[10] エストニアは，2007 年の首都タリン市への DDoS 攻撃によるサイバーテロ事件（Web War the First，WWI と呼ばれる。）にロシアが関与した主張したが，ロシアは関与と容疑者の捜索を拒絶した。結局，この事件では，同国在住のロシア系学生 1 人の逮捕に留まり，ロシアに対する国家責任追及には至らなかった。

[11] 原発は「サイバー攻撃」に曝されている：英シンクタンク報告，2015.10.19, https://wired.jp/2015/10/19/nuclear-power-plant-insecure/

各施設は，運用効率を高めるためにネットワーク化の度合いを深め，IoT 機器の導入が急増している。IoT が情報セキュリティ面で特に問題視される理由は, IoT 機器の脆弱性が高いからである。IoT 機器は，PC に比べてセキュリティパッチの管理・適用が難しい。また，情報システムにおける FireWall や IDS/IPS, マルウェア対策ソフトのようなリスク緩和策も少ない。IoT 機器は, actuator（作動装置）を持っており，物理空間の破壊に至る可能性もある。その上，システム管理下に置かれていないいわゆるシャドーIoT も多く，野良 IoT と呼ばれており。攻撃側にとっては，新たな標的が増え，活動範囲が拡大すると見えている。IoT は言い換えると Internet of Threats に他ならないわけである。これらの IoT 機器が重要インフラ内に多数存在し，世界中で攻撃の踏み台として利用され，サイバーテロを助長することが懸念されている。また，IoT 機器は設備に組み込まれているので，設備の更新まで 10 年以上も使い続けることが多く，パッチ適用ができない。このような事情から，重要インフラ分野がサイバーテロに晒されると，深刻な経済的損害と物理的な影響（工程停止，品質の劣化，人身事故など）を被る可能性がある。

4.4　サイバーセキュリティ戦略におけるサイバーテロ

NISC はサイバーセキュリティ政策の中心と位置づけられるが，サイバーセキュリティ戦略は，政府のサイバーセキュリティ政策に関する中長期計画を示すものであり，おおよそ 3 年スパンで改定されている。重要インフラの保護は当然に国の重要な施策として取り組むべき課題であろう。しかし，重要インフラのほとんどは民間企業が運営している事実に基づき，政府は，安全かつ持続的なサービスを確保するために必要な施策は重要インフラ事業者が自主的に取り組むべきことであり，重要インフラ保護に責任を有する政府は重要インフラ事業者との共通の施策として行動計画を策定するという基本姿勢を取り続けている。

特別行動計画は,「いわゆるサイバーテロなど，情報通信ネットワークや情報システムを利用した，国民生活や社会経済活動に重大な影響を及ぼす可能性があるいかなる攻撃からも重要インフラを防護することを目的として」策定されたのだが，以降，サイバーテロに関する政府の姿勢は後退したように見受けられる。

4.5 重要インフラの危惧

これまで，日本の重要インフラは信頼性の高いシステムであると信じられてきたが，2018 年 9 月の平成 30 年北海道胆振東部地震では，主力の苫東厚真火力発電所の全 3 基が緊急停止し，電力の需給バランスを保てず，わずか 18 分後に水力を含む全ての電源が停止して北海道全域が Black out してしまった。本州から 60 万キロワットの電力融通を受けられる北海道・本州間連系設備の融通枠では停止した苫東厚真火力発電所の供給量を埋められず，対応初期段階において連系設備を役立てられなかった。自助システム（家ごとに小型自家発電装置を設置）あるいは共助システム（地域／自治体単位の対策）の重要性が再認識されることになった。

電力分野におけるサイバーセキュリティ対策は，国民の安全に責任を持つ政府と，インフラの安定的な運用に責任を持つ事業者という官民が連携する形で検討されている。政府側は経済産業省電力安全課，事業者側は，金融や通信などの他の重要インフラ分野の取組を倣って，業界大のサイバーセキュリティ対策強化を目的に，2017 年 3 月に電力 ISAC（情報共有分析センター）が設立された。電力システムと各電力利用者の接点となるのはスマートメータ（SM）であり，これも IoT 機器である。従来各家庭に設置されていたアナログ型電力量計に替わって電力量をディジタル計測し，電力の流れを最適化するための制御機能を SM に持たせている。各戸の電力使用量の定期的な計測検診作業を不要としたり，各戸における太陽光発電量と原子力発電との負荷調整のための検出端としたりなど利点は大きい。一方で，IoT 機器を電力ネットワークへの入口として悪用されると，サイバーテロを引き起こすという懸念は残る[12]。有名な事故として，上述のウクライナで発生したサイバーテロがある。

2001 年 1 月に施行された高度情報通信ネットワーク社会形成基本法では, 民間主導による IT 化が指向された。一方，サイバーセキュリティ基本法では，国家主導による政策を指向している。しかし，欧米では，陸海空の 3 軍に宇宙とサイバー空間を合わせた 5 軍のうちの一つとしてサイバーセキュリティが捉えられているのに対して，日本では，軍事力非保持という憲法の規定もあり，非軍事の問題として民間が主体となって対応している。また，日本は，重要インフラシステ

[12] 経済産業省　電力 SWG の開催と電力分野におけるサイバーセキュリティ対策について，2018 年 6 月 http://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_denryoku/pdf/001_04_00.pdf

ムの信頼性が高く，停電もめったに起きない。しかしその分，普段の備えが不十分となり，いったん止まってしまうと利用者がパニックになりやすい傾向がある。

スマートグリッドを実現するために，各需要家に設置される SM は IoT 機器の典型であるが，2024 年までに 8,214 万台が設置される計画である [12)]。SM は無線 LAN 又は配電線で電力ネットワークに接続される。情報セキュリティの脆弱などこか 1 箇所の SM からマルウェアが侵入し，電力ネットワーク全体を脅威に晒す可能性もある。

4.6 サイバーテロ対策

以上の議論をもとに，今後のサイバーテロ対策を進める上で考慮すべきことをまとめる。

①組織における対策

サイバーテロの影響は，重要インフラ事業者，政府機関・地方自治体，一般企業，国民それぞれに及ぶ。各組織が情報セキュリティに関してこれまで整備してきた情報セキュリティマネジメントシステム（ISMS）における情報セキュリティ対策を IoT 機器にも適用することから始める必要があろう。すなわち，シャドーIoT を洗い出して情報資産として認知し，ISMS の管理下に置くことである。例えば，一般の情報システムであれば，初期パスワードの変更，マルウェア対策ソフトの導入，セキュリティ USB メモリの使用，暗号化などが社内規定化されている。ただし，通常の IT 機器に比して IoT 機器には，プラントの制御システムのような個別開発された高価なシステムばかりでなく，監視カメラ，家電製品といった設置個数が膨大であり，単価が安く，使用期間が長く，ソフトウェアの更新もほとんどされないといった機器が管理下に入ることになり，従来の ISMS の管理策ではコスト的に間尺に合わなくなる可能性がある。組織のトップの経営判断が必要になろう。

② 政府の政策

Schneier は，新著の中で，航空機が政府の規制によって今では最も安全な乗り物に転換された事例を挙げている。そして，認定されたソフトウェア技術者にソフトウェア製品が十分なレベルの脅威に耐えられることに責任を持たせることを提唱している。建築家からビルがちゃんと建つという言質を取るように。

政府なり専門家に責任を持たせるというこの議論は，福島第一原発事故の危険性に関連して，安倍総理が原発「の安全性については、原子力規制委員会の専門家に判断を委ね」[13]る，と発言したことの危さを想起させる。本来，原発の安全性保証は政府が責任を持つべきであり，規制委員会に任せて終わりというものではない。また，自動車の排気ガス規制に関しては，マスキー上院議員が大気浄化の強化を義務付ける法案を提出した（マスキー法案は成立したが，後に骨抜きされた。）ことが契機となって，日本の自動車メーカが自主的取り組み，結果として規制をクリアした。サイバー空間のサイバーテロは，物理空間における環境汚染と同様の外部不経済であるが，コストが安いので市場価格に基づいて内部経済化することも困難と思われる。したがって，政府の規制を必要するのではないか。ICT 産業は，環境汚染をもたらさないクリーンな産業と呼ばれて，市場機会及び競争圧力を確保しつつ，飛躍的な成長を遂げてきた。IoT 機器の普及とともに，今後は，政府としても，サイバーテロといった外部不経済を克服することが，企業倫理の点からも組織継続の論理を後押しすることになるのではないか。

5 まとめ

IoT の普及に伴い，サイバーテロの危険が増加している。本稿では，サイバーテロは IoT 機器を悪用して人の生命にも損害を与える重大性を指摘し，IoT 機器を使用する企業における ISMS 活動の補強が必要なこと，政府は企業の自主的取り組みに委ねるのではなく，政策目標としてサイバーセキュリティ強化のための技術開発，責任体制の強化の必要性を論じた。

[引用文献はそれぞれ脚注に示した。]

[13] 安倍内閣総理大臣記者会見，https://www.kantei.go.jp/jp/96_abe/statement/2013/0626kaiken.html