RISTEX 社会技術研究開発センター
Research Institute of Science and Technology for Society

平成 21 年度　文部科学省　安全・安心科学技術プロジェクト
「テロ対策のための科学技術の最新動向および研究成果の実装化に関する調査研究」

RISTEX CT Newsletter

第 9 号　　発行日 2010 年 2 月 12 日

# ホテルセキュリティの現状と対策：高まるホテルテロの脅威

長谷川　美沙　　RISTEX 研究助手

## １．はじめに

2001 年の米同時多発テロにはじまり、2009 年 12 月 25 日の米デトロイト便テロ未遂事件の発生により、航空セキュリティをめぐる論議は白熱している。しかしテロリストによる日々のテロ行為に目を向けると、航空機よりもむしろホテルを標的としたテロ攻撃が圧倒的に多い。ところが、空港や航空セクターに対するセキュリティ対策と比較するとホテルのセキュリティ対策は相対的に脆弱との指摘が数多く、実際に機能すらしなかった事例さえ見受けられる。2010 年には横浜で APEC 首脳会議を控える日本にとっても、この点、注意が喚起されるべきであろう。以下ではホテルを標的としたテロの現状を示したうえで、ホテルセキュリティの問題点、今後の課題について考察する。

## ２．ホテルへのテロ攻撃の現状

### ①ホテルへのテロ攻撃件数（CBS ニュース調べ）

2010 年 1 月 4 日に放送された CBS ニュースによると、米同時多発テロが発生した 2001 年 9 月 11 日を境界とした前後 8 年間における海外の米系ホテルを狙ったテロ攻撃件数は、9.11 以前は 30 件だったのに対して 9.11 以降は 62 件と 2 倍以上に膨れ上がっている[1]。ここで取り上げられているテロ件数は米系ホテルに限ってのことだが、決して米系ホテルだけでなく、他国のホテルも当然テロの攻撃対象となっており、ホテルを対象としたテロ攻撃が発生する可能性はより一層高まっていると言えよう。

### ②なぜホテルなのか？

---

[1] “CBS Evening News: Hotel Security 2010”, *CBS News*, 2010/01/04, http://www.petergreenberg.com/2010/01/04/cbs-evening-news-hotel-security-2010/ (2010/02/01 閲覧)

理由はいくつか考えられるが、前述したCBSニュースでは大きく次の3点を挙げている[2]。

- 複数の出入り口がある
- 車でのアクセスが容易
- 検査されることなく放置された鞄類がいくつもある

つまり、テロリストがテロ攻撃を「実行」そして「成功」しやすい環境であると考えられる。ホテルのロビーはいつも宿泊客やイベント参加者、業者など、様々な来訪者で混雑しており、車はホテルをひっきりなしに出入りし、誰の目にも留まっていない鞄類が無造作に置かれた状況を良く目にする。CBS ニュースによると、ニューヨークで一番大きなホテルであるヒルトン・ホテルには 2058 部屋があり、毎日 3000 人以上の人々がホテルを利用しているとのことである[3]。つまり、ホテルではテロ攻撃を比較的容易に遂行しうる状況が日常的に備わっており、それゆえにこれまで数々の攻撃が実行されてきたといえよう。

その他、先に挙げた理由以外にも、ホテルは一定の場所に定常的に立地しているため、テロリストから見れば比較的攻撃しやすいことや、ランドマーク的ホテルへの攻撃は社会に対する反響が大きい点なども指摘される。

③ホスピタリティとセキュリティのバランス

そもそもホテルがテロリストに狙われる根本的な問題として、ホテル業界がホスピタリティ産業であるということがあげられる。ホテルに宿泊する「ゲスト」は第一義的にはあくまでも「ゲスト」であって「テロリスト」や「犯罪者」として見るべきではない、との考えがホテル経営の基本である。ホテルの責任者も安全確保の重要性を認識はしているものの、実際問題として、ホテル内に通じる全てのドアをロックしたり、全ての鞄や車を検査することはゲストへのホスピタリティを低下させるとして懸念されるのが一般的である。ましてや、テロ攻撃が起こるか起こらないか分からない状況であれば、それらの対策を実施することはより一層非効率的と判断されがちであろう[4]。

## ３．ホテルへのテロ攻撃が増加した背景：テログループの組織形態の変化

9.11 同時多発テロ以降、アルカイダは国際テロ組織の象徴として今もなお君臨しているが、その実態は、以前のような中央集権的な組織形態からより小規模かつ多数の組織やセル等に分化し、それぞれが活動を行うという、いわばフランチャイズ的な性格を強めた組織形態に変化してきていると指摘される[5]。現にアラビア半島のアルカイダやアルカイダとの連

---

2 同上
3 同上
4 同上
5 “Study: Terror attacks on hotels surge since 9/11”, *msnbc*, 2009/09/08
http://www.msnbc.msn.com/id/32730101/ns/world_news-terrorism/ (2010/02/02 閲覧)

携を表明したばかりのソマリアのイスラム過激派組織アルシャバブ[6]といった地方組織の台頭も見受けられる。パキスタン・タリバン（ローカルタリバン）も近年、アフガニスタンで生まれた武装勢力タリバンの活動に触発され、テロ攻撃を各地で頻繁に行っている。他にも過激な思想をもつ、名前もないローカルな過激派グループが多数存在する。このような小組織は限られた軍事訓練しか受けることができず、資金的制約も厳しいことが考えられる。彼らにとっては、政府関連機関や軍事施設といった「ハード」ターゲットよりも、アクセスが容易でセキュリティが比較的低いホテルや公共施設等の「ソフト」ターゲットをテロ攻撃の対象として選定する傾向があると指摘される[7]。

## ４．対応策案

ホテルの安全を確保するためにクリアしなければならない諸問題は依然として残るものの、ホテル側もわざと「目につく」警備員を配置したり、入り口に金属探知機を設置するなどの対策を実施してきた。しかし、2009 年インドネシア・ジャカルタ市内で発生したホテル爆破テロ事件などで見受けられたように、開発途上国などではこのような対策だけでは不十分な事例が目立つようになっている。以下に、近く実装化が期待されている最新技術が CBS ニュースで報道されていたので紹介する。加えて、ハード面だけでなくソフト面での改善についてもふれる。

### ①対策Ⅰ：ハード面[8]

Berry Plastics Corporation 社が開発したプラスチックの網の目でできた壁紙は、建物に強い衝撃が加わったとしても、その衝撃を吸収することで建物の構造そのものは維持することができるとされる。テロの標的になりやすい世界中の軍事施設や大使館ではすでに導入されており、１年以内には商業利用も可能となる予定だ。その他、爆発現場では飛散したガラスの破片により多くの死傷者が発生することから、ガラスの飛散防止フィルムや、疑わしい人物の追跡・特定のため細部にいたるまで鮮明に拡大表示可能なモニタリング・カメラ、車が突入してきた場合に、0.5 秒で衝立が立ち上がり、車がホテルに衝突するのを防御するバリケードなどが取り上げられている。

しかし、これらの製品を導入するにはいずれもコスト負担が大きいため、CBS ニュースが放送された 2010 年 1 月 4 日時点では、米国内のホテルから製品に関する問い合わせは一件もなかったようで、積極的に取り組む姿勢は見られなかったという。

---

6 “Somali Islamists al-Shabab 'join al-Qaeda fight'”, *BBC News*, 2010/02/01 http://news.bbc.co.uk/2/hi/africa/8491329.stm (2010/02/02 閲覧)

7 “Study: Terror attacks on hotels surge since 9/11”, *msnbc*, 2009/09/08, 前掲

8 “CBS Evening News: Hotel Security 2010”, *CBS News*, 2010/01/04, 前掲

②対策Ⅱ：ソフト面

過去の主なテロ攻撃の事例を検証すると、テログループの作戦として、内通者をターゲット施設内に送り込むという手法が見受けられるようになっている。2009 年 7 月にジャカルタで発生した JW マリオットとリッツ・カールトンの同時爆破テロの場合は、容疑者の一人が両ホテルを担当する花屋として潜入し、自爆犯 2 名を手引きしたとされている。また、未確認情報ではあるが、2008 年 11 月にムンバイで発生したタージマハルホテルなどを襲った同時多発テロでは、犯行グループの一人がシェフとしてタージマハルホテルで 10 ヶ月間働いていたとの情報もあった[9]。少なくともいくつかの事例では、テロリスト達は内部の人間しか知り得ないセキュリティプロセスやアクセス方法といったインサイダー情報を事前に入手することで、高い攻撃成功率が想定されうるようなターゲットの選定からテロ遂行までの綿密な計画を立てていたと考えられる。このような内部協力者を排除するためのひとつの案として、ゲストや従業員をある程度スクリーニングすべきとの指摘もある[10]。特に従業員においては、どのようなバックグラウンドをもつ人物なのか十分に目を向ける必要があり、将来的には雇用基準や既存従業員の経歴や犯罪歴などのチェック方法のガイドラインなどについて検討していく必要があるとの議論も出ている。

## ４．従業員の意識改革の重要性[11]

ホテルの保安管理はとかく保安担当チームのみが責任を負っていると考えられがちである。しかし、彼らが十分にホテルを防護・保護できるかどうかは、従業員一人一人から寄せられる情報に大きく左右されると指摘する報告がある。フロントスタッフはもちろん、ルームメイド、清掃係、駐車係、庭師にいたるまで、従事する職務を問わず、個々人が見たり、感じたりしたことで、「ちょっとした違和感」を感じた事柄等を迅速にそして正確に保安担当者に伝達・報告することが重要であるとの指摘だ。テロリストは現金による資金援助を受けるケースが多いことから、例えば、クレジット・カードではなく現金でチェックインする人物がいたり、チェックインの際にクレジット・カードが何らかの理由で使用不能になっている人物がいたりした場合には、少なくとも何らかの注意を払うようにしておくべきであろう。

また、ホテル内で保安管轄区域ごとに保安責任者とその任務・役割を明確にしておくべきとの指摘もある。ホテルが管理すべき保安区域には、正門から玄関までの区域、駐車場、

---

9 “Officials quit over India attacks“ *BBC News*, 2008/11/29, http://news.bbc.co.uk/2/hi/south_asia/7756068.stm (2010/02/01 閲覧)

10 “Hotel Security After Jakarta: Rethinking Faulty Assumptions”, World Check, Aug 2009, http://www.world-check.com/media/d/content_experttalk_reference/ExpertTalk_Aug09.pdf (2010/02/01 閲覧)

11 David Rubens, “Hotel Security Management: Strategies and Tactics for Modern World”, February 2010, p.4.（2010 年 2 月 12 日閲覧）

従業員以外立ち入り禁止区域、従業員の通用口やゴミ捨て場等のサービスエリアなども含まれる。仮にそのうちのひとつでもホテル側の目の行き届いていない区域があれば、それはテロリストや犯罪者にとって格好の脆弱ポイントを露呈させることになり、テロ攻撃のターゲットに選定される可能性が高まりうると考えるべきであろう。

これらのことを踏まえると、ホテルのセキュリティ向上のためには、保安担当責任者だけでなく、従業員全員が危機管理意識を常に持ち、セキュリティ管理責任を共有するという、経営面での意識改革が必要であると言えよう。

## ５．最後に

ホテルへのテロ攻撃の可能性を完璧に排除しうる万能策は必ずしも存在しない。しかし、テロを「実行させにくい」環境づくりは可能であり、また推進されるべきである。そのためにはホテル保安に関して様々な側面から対策を講じ、それぞれが相互補完的にセキュリティを強化してゆくよう、重層的に保安対策を実践していくしかない。もちろん高度先端技術を用いたセキュリティ機器の導入はひとつの対策ではあるが、どんなに最新鋭の機器を使用しても、もしテロ側の内通者がいれば、セキュリティ面での脆弱性が外部に露呈されてしまう可能性は十分に考えられる。そもそもセキュリティ機器を導入しても、スタッフなどの訓練が不十分であれば意味をなさない。事実、ジャカルタの JW マリオット爆破テロ事件の犯人は爆発物を荷物の中に隠していたが、通常ならばセキュリティスクリーンに荷物を通過させるべきところを、荷物が大きすぎてスクリーンを通過できないことを口実に検査を免れ、内部協力者の助けも得て、最終的には裏口の従業員通用口から爆発物を持ち込んだとの報告がある[12]。本来ならば、入り口の検査員が荷物を開けさせて中身を全部チェックするべきであったが、「ゲスト」に「煩わしい思い」をさせたくなかったという配慮が、かえって致命的な結果を招いてしまった。なぜ、ホテルの入口で宿泊客や来訪客にできるだけ失礼にならないような言葉づかいで荷物を適切に検査することがなぜできなかったのか。ゲストに対する中途半端な配慮は、ゲストに対する「安全安心の提供」というホテル側のサービスをかえって著しく損ないかねない点を認識するべきであろう。このようなことを繰り返さないためにも、従業員一人一人の危機管理意識の改革とそのための継続的な訓練が、今後のホテルセキュリティ面での重要な要素になると思われる。

繰り返しになるが、ホテルのセキュリティ管理は複数の要素を組み合わせ、多角的かつ重層的な対策を講じることで強化を図ることができる。すなわち、セキュリティ機器といった物理的セキュリティ、従業員とゲストのスクリーニング、最後に、従業員の固定観念を払拭した危機管理意識の改革と訓練。いずれの要素も欠かすことなく、バランス良く組み合わせてゆくことが、今後のホテルのさらなるセキュリティ向上に不可欠な第一歩ではないかと感じる。

---

12 “Hotel Security After Jakarta: Rethinking Faulty Assumptions”, World Check, Aug 2009, 前掲

# 国内外における主要な会議・展示会

（注：弊センター主催以外の会議に関するお問い合わせ・お申し込みは、直接先方にお願いいたします。）

会議名：**2010 AFCEA Tokyo TechNet**
会期：2010年2月16日～18日
会場：ニュー山王ホテル
主催：AFCEA（The Armed Forces Communications and Electronics Association）
概要：“Everything... Globally Connected”をテーマに、展示会、C4I・サイバーセキュリティ等に関するパネル・ディスカッションなど様々なイベントが催される。
ウェブサイト：http://tokyo.afceachapter.org/

会議名：**AAAS 2010 Annual Meeting**
会期：2010年2月18-22日
会場：San Diego Convention Center（米カリフォルニア州サンディエゴ）
主催：米国科学振興協会（AAAS）
概要：AAASの年次総会。「Bridging Science and Society」をテーマに、気候変動、公衆衛生、エネルギー、海洋資源など様々なシンポジウム・セミナーが開催される。
ウェブサイト：http://www.aaas.org/meetings/

会議名：**Border Security 2010**
会期：2010年3月3-4日
会場：Crowne Plaza Rome St. Peter’s Hotel（イタリア・ローマ）
主催：SMi
概要：陸・海・空のセキュリティ管理に関する国際会議。空港セキュリティをはじめ国境管理技術につき、発表・展示が行われる。
ウェブサイト：http://www.smi-online.co.uk/events/overview.asp?is=1&ref=3192

会議名：**医療安全教育セミナー2010 春季**
会期：2010年3月7日　10：00-16：30
会場：東京大学医学部医学教育研究棟13階セミナー室（東京都文京区本郷7-3-1）
主催：国際予防医学リスクマネージメント連盟
概要：言語的／非言語的リスクコミュニケーションの実習。
ウェブサイト：http://www.jsrmpm.org/RC2010/

会議名：**1st Annual Biological Safety Conference**
会期：2010年3月8-12日
会場：Kemri Training Centre Nairobi（ケニア・ナイロビ）
主催：African Biological Safety Association
概要：アフリカの風土病、新興・再興感染症に対するバイオセイフティおよびバイオセキュリティにつき発表・展示が行われる。
ウェブサイト：
http://www.afbsa.org/index.php?option=com_content&view=article&id=51:confere

会議名：**2010 USPACOM Science and Technology Conference**
会期：2010年3月15-18日
会場：ヒルトン・ハワイアン・ビレッジ（米ハワイ）
主催：NDIA (National Defense Industrial Association)
概要：“Integrating Technologies to Fill Capability Gaps”をテーマに、PACOM(米太平洋軍)の直面する課題、解決のための技術などにつき発表・展示が行われる。
ウェブサイト：http://www.ndia.org/meetings/0540/Pages/default.aspx

会議名：**2010 Annual Biometrics and Forensic Summit**
会期：2010年3月30日-4月1日
会場：Manchester Grand Hyatt（米カリフォルニア州サンディエゴ）
主催：米陸軍インテリジェンス・センター
概要：戦場におけるバイオメトリクス・フォレンジック技術に関する会議および展示会。
ウェブサイト：https://www.ncsi.com/biometrics10/index.shtml

会議名：**11th Annual Science & Engineering Technology Conference / DoD Tech Exposition**
会期：2010年4月13-15日
会場：Embassy Suite Hotel（米サウスカロライナ州チャールストン）
主催：National Defense Industrial Association(NDIA)
概要：NDIA主催の第11回年次総会。産官学間で国防技術情報の共有化を図る。陸軍、海軍、空軍、連合軍のセッションが設けられ、分野ごとに発表・議論が行われる。
ウェブサイト：http://www.ndia.org/meetings/0720/Pages/default.aspx

会議名：**3rd Sample Prep '10 - Sample Preparation for Virus, Toxin & Pathogen Detection**　会期：2010年5月6-7日
会場：TBA（米ワシントンDC）
主催：Knowledge Foundation

概要：ウィルス、毒物、病原体の最新鋭検出技術につき発表・展示が行われる。
ウェブサイト：
http://www.knowledgefoundation.com/viewevents.php?event_id=215&act=evt&utm_campaign=Sample%20Prep%202010%20-%20Final%20Call%20for%20Speakers&utm_content=n2noro@jst.go.jp&utm_medium=Email&utm_source=VerticalResponse&utm_term=Sample%20Prep%202010

会議名：**The 10th International Symposium on Protection against Chemical and Biological Warfare Agents**
会期：2010 年 6 月 8-11 日
会場：Kistamässan（スウェーデン・ストックホルム郊外）
主催：スウェーデン外務省、防衛研究局、ほか
概要：生物化学兵器テロ対策の現状と課題、対策に資する研究開発などに関する大規模な国際シンポジウム。CB 兵器対策技術展示会併設。
ウェブサイト：http://www.cbwsymp.foi.se/

会議名：**Biodetection Technologies 2010**
会期：2010 年 6 月 17-18 日
会場：TBA（米ワシントン DC）
主催：Knowledge Foundation
概要：バイオディフェンス分野における最新の探知技術、R&D などに関して議論予定。
ウェブサイト：http://www.knowledgefoundation.com/viewevents.php?event_id=216&act=evt

RISTEX CT Newsletter　第 9 号
発行人：（独）科学技術振興機構　社会技術研究開発センター
　　古川勝久　野呂尚子　友次晋介　長谷川美沙
発行日：2010 年 2 月 12 日

〒102-0084　東京都千代田区二番町 3　麹町スクエア 5 階
Tel: 03-5214-0134　　Fax: 03-5214-0140
e-mail: ct-seminar@ristex.jst.go.jp
HP: http://www.ristex.jp/index.html

バックナンバー：http://www.ristex.jp/aboutus/enterprize/trust/terrorism/newsletter.html



平成 21 年度文部科学省　安全・安心科学技術プロジェクト
「テロ対策のための科学技術の最新動向および研究成果の実装化に関する調査研究」
RISTEX CT Newsletter Issue No. 9　2010 年 2 月 12 日