交通セキュリティセミナー

大規模スポーツイベントにおける交通分野のセキュリティ対策

平成29年12月7日　海運クラブ 2階ホール

主催：一般財団法人運輸総合研究所
後援：国土交通省
協力：公益財団法人東京オリンピック・パラリンピック競技大会組織委員会

講演1
大規模スポーツイベントにおける セキュリティ

トマー・フルマン
（CEO, International Security & Defense Systems Ltd.）

ISDS社は1982年の創業以来，セキュリティコンサルティングをグローバルに展開してきた．現在では，世界の16か所にオフィスを展開している．

これまで，オリンピック・パラリンピックなどのメガイベント，空港，鉄道，発電・通信施設などの主要インフラの物理的なセキュリティやサイバーセキュリティ対策を実施してきた．

2016年のリオ大会では，イスラエルの民間会社としてオフィシャルサプライヤーとなり，地元警察や軍をはじめ，大会スタッフ，ボランティアなど約4万5千人に対して，教育，訓練を実施した．本日は，リオ大会での経験についてお話をしたい．

リオ大会では，約100人の国家元首，世界各国から10,000人以上の選手を迎えた．メディア関係者は20,000人以上が集まった．競技会場は32か所，競技種目などは1,000以上であった．セキュリティに関する対策は，スタジアムとその周辺，交通アクセス，国全体の大きく3つの階層に分け実施した．競技やイベントが開催されるスタジアムでは，数万人規模で観客が集まってくることから，安全な環境をスタジアムの内外で確保することが重要となる．交通アクセスについては，観客や選手などが定刻に安全にスタジアムに到着できることが重要となる．

シャロム・ドレフ
（Director Security Systems, International Security & Defense Systems Ltd.）

まず，リオ大会での教訓に基づく課題についてお話したい．

オリンピック・パラリンピックのようなメガイベントでは，競技会場，練習所，選手村などが，各地に点在しており，セキュリティ上の課題となることから，それぞれの施設を一体管理するとともに，クラスターとして独立運用できることが必要となる．

2番目は，競技会場のレイアウトや所在地が多種多様であるということである．数十万人が集まるような競技もあれば，500人しか集まらない競技もある．競技内容により，観客も異なる．さらに，競技会場の特性に合わせた計画とオペレーションも必要となる．

3番目は，要人警護について，それぞれ国ごとに異なるセキュリティに関する要件がある．例えば，アメリカは大変厳しいセキュリティ要件があり，国務省のセキュリティ部門などから何百という要件を出してくる．こうた要件を計画に取り込まなければならないし，その検証作業も必要となる．

4番目は，3週間という短期間に集中的に競技が開催され，過密プログラムとなっていることである．それぞれの競技をプログラムの時間内で終了する必要があるが，万が一の遅延に備え，セキュ


トマー・フルマン

大規模スポーツイベントにおける交通分野のセキュリティ対策
プログラム

主催者挨拶：黒野匡彦　一般財団法人運輸総合研究所会長
講　演　1：「大規模スポーツイベントにおけるセキュリティ」
　　トマー・フルマン　CEO, International Security & Defense Systems Ltd.
講　演　2-1：「大規模スポーツイベントにおける脅威
　　－セキュリティからサイバーディフェンスまで－」
　　シャロム・ドレフ　Director Security Systems,
　　International Security & Defense Systems Ltd.
講　演　2-2：「公共交通とサイバー攻撃の脅威
　　－リオデジャネイロオリンピック・パラリンピックなどの事例から－」
　　シャロム・ドレフ　Director Security Systems,
　　International Security & Defense Systems Ltd.
閉会挨拶：春成　誠　一般財団法人運輸総合研究所理事長

リティ計画にはリダンダンシーが不可欠となる.

5番目は, 軍隊, 警察, 民間警備会社, 自治体職員, ボランティアなど大変多くの人々がセキュリティに関わることである. それぞれの組織ごとに様々なアサインメントがある. 例えばセキュリティガードを事例に挙げると, 会場入口においてエックス線スクリーニングをする人, チケットを確認する人など様々な役割がある. それぞれの組織毎の文化, スキル, コンピテンスも当然異なるが, 各組織がハーモニーを奏でるように調整しなければならない. このためには, コマンドコントロールが必要となるが, 意識統制には時間を要するし, 非常に詳細な手順とトレーニングが必要となる.

最後の課題は, トレーニングである. 例えば警察官は, 一般的にセキュリティのスキルもコンピテンスもあって, 自らの使命を遂行できると思いがちであるが, なかには経験のない警官もいる. こうしたことから, これまでに起きたテロ事件などをもとに, それぞれの役割を明示したミッショントレーニングが必要となる. さらに, 組織間の連携が円滑になるように実践トレーニングを行う必要がある.

こうした課題に対応するために, 警備の計画は, コンセプト設計の段階から始めなければならない. このため, リオ大会の4年前から具体的な作業を始めた.

講演2-1

大規模スポーツイベントにおける脅威 ーセキュリティからサイバーディフェンスまでー

シャロム・ドレフ
(Director Security Systems, International Security & Defense Systems Ltd.)

ここからは, サイバーセキュリティの分野に特化したお話をしたい.

10年程前にサイバーセキュリティに関する先端的なアプリケーションソフトが空港や国境警備に導入された. これをきっかけとして, 当社でも実践的なソフトを用いたソリューションを提供していきたいと考えた.

最初に, 一般的なセキュリティのアプローチをサイバーセキュリティの分野に応用することに取り組んだ. 具体的な手順は, 脅威の評価, リスク分析を実施するとともに, 予想される攻撃のタイプに応じた対策を検討した.

近年, サイバー攻撃の脅威は, 情報技術の進展に伴い, 被害や損害も大変大きくなっている.

DOS攻撃(ウェブサービスに大量のリクエストや巨大なデータを送りつけるなどしてサービスを利用不能にする攻撃), C&Cサーバー(パソコンやサーバーなどが第三者に乗っ取られ, 不正アクセスや迷惑メールの大量配信などを行う中継地点として利用されること)などの攻撃手法がパワフルになってきている. さらに, 昨今のソーシャルエンジニアリング攻撃は, 非常に高度化されており, 攻撃に使うEメールの内容は, Twitterやブログなどのネット情報を活用して偽装され, 巧妙化されている.

これまでのサイバー攻撃の事例についていくつか紹介したい. アメリカ軍のデータベースにワームが入り込み多くの情報を盗んだ. この攻撃は, 情報が非常に巧みな形で外に流れるようになっており, 検知するためのセキュリティシステムさえも乗り越えてしまい, 従来の検知技術がまったく機能しなかった.

また, コンフィッカーというワームにより, Windowsのパソコンが何百万台も感染した. このワームはWindowsのOSシステムの欠陥を突いたもので, USBを差し込むとワームが侵入し, バックドアを作り情報が漏洩された.

最近の事例としてランサムウェアNotPetyaを紹介したい. 被害を受けたのは, 海運会社であり, コンテナの出荷情報や位置情報などに関するシステムが被害を受けたことにより, 数週間に渡り貨物の遅延など混乱が生じ, 大きな損失を計上した.

こうした攻撃に対して, ファイヤーウォールやサンドボックスによる対策を講じているが, 攻撃者は専門的な知識や潤沢な資金などにより, 新たなツールを開発して攻撃を仕掛けてくる.

こうしたことから, 保護対策は非常に重要となる. トレーニングによるユーザースキルアップや個人の意識を高めることが不可決ではあるが, うっかりミスで添付ファイルやリンクをクリックするリスクを完全になくすことはできない. このように, 今日のセキュリティは, 保護対策や検出対策では不十分であるので, ケースによっては, リアルタイム監視など効果的な対応を行う必要もある.

一般的に, セキュリティ対策に無限のリソースを投入することは, 現実的ではない. 日常業務で利用するコンピュータは, 高いパフォーマンスや処理スピードに対する要求が強いことから, 運用面を重視した効率的なセキュリティが求められている.

一方で, 交通機関や電力関連の重要インフラなどについては, 極めて高い防護レベルが求められる.

サイバー攻撃について, セキュリティシステムなど技術的な面を重視しがちであるが, 内部犯行が非常に深刻な脅威となる. サイバー攻撃についての大規模な調査をした結果, この5年間で成功した攻撃の7割位は内部犯行によるものである

シャロム・ドレフ

ことが分かった. 内部犯行の動機は, 個人的利益や会社への恨みなど様々である. 彼らは, システム管理や経理業務を担当しており, 実際の業務で使用するアクセス権限を使って犯行を行う. こうした内部犯行は, 技術的な脅威とは異なる脅威となる.

国家がサイバー攻撃に関与するケースもある. 動機は政治目的であり, 軍が直接関与する攻撃が近年増加している. こうした攻撃は, 国家の威信に傷をつけることや, 通信や電力網をダウンさせることで, 国家機能にダメージを与えることを目的としたものがほとんどである. エストニアでの通信障害の事例は, インターネットを遮断させて世界から隔絶させることを目的としたものであると言われている.

講演2-2

公共交通とサイバー攻撃の脅威
ーリオデジャネイロオリンピック・パラリンピックなどの事例からー

シャロム・ドレフ
(Director Security Systems, International Security & Defense Systems Ltd.)

ここからは, 運輸部門に対する物理的な攻撃についてお話したい.

オリ・パラでは, 選手団や観客が利用する航空, 鉄道, バスなどがテロの標的となる. また, 開催都市の交通手段の警備が厳重な場合, 攻撃者は警備の盲点を突き, 地方都市などの交通機関に対して攻撃を仕掛けてくる可能性があるので, 注意を払わなければならない.

交通機関は, 長年テロリストの標的となってきた. 交通機関は, 多数の利用者, 閉鎖的な空間による被害の拡大などテロリストにとっては魅力的なターゲットの1つとなる. テロリストはイラクやシリアなどでの実戦経験により, 自動小銃や手榴弾の扱い方に精通している. また, 入手しやすい材料から強力な爆弾が製造されており, その製造方法もインターネットで公開され誰でも入手できるようになっている.

それでは, 交通機関をターゲットとした過去のテロ事例について, お話していきたい. マドリード列車爆破テロ事件では, 何百人という人が犠牲となった. ロンドンでは鉄道を狙った爆破テロが起きている. また, 大量の爆発物が積載された車が列車やバスに突っ込んで巨大な爆発が起こり, 多くの犠牲がでている. さらには, 盗んだブルドーザーを運転して, バスに突っ込み6人が亡くなるという事件も起きた. 爆発物はテロリストが, 交通機関の利用者として直接車内に持ち込むこともあるが, 夜間帯のターミナルに駐車しているバスに爆発物を仕掛けるケースもある.

爆発物以外では, 運転手からバスのハンドルを乗っ取って, 橋や崖から転落させれば, 爆弾がなくても多くの人を殺傷することができる. さらに, 地下鉄やバス等の利用者の誘拐も考えられる. 誘拐が起こると警察の特殊部隊等が解放しようとしても非常に困難な状況になる.

メガイベントでは道路を閉鎖して歩行者天国とすることがある. 道路閉鎖に用いられるバリアは非常にシンプルなものとなっている. フランスの独立記念日に起きたニーストラックテロ事件では, 花火見物をしていた人々の列にトラックが突っ込み86人を殺害した. 警官はハンドガンを使用したが, トラックを止めることができなかった. 走行中のトラックを止めるには特別な対策が必要となる.

これまで事例等についていくつか紹介したが, ここから対策についてお話したい. オリ・パラのような大規模イベントでは, 宿泊施設, 競技場, 練習場, さらには, こうした施設を結ぶ交通機関に対しての脆弱性やリスク評価を実施して対策を立てることが必要となる.

その際, 競技会場などの周辺をどのぐらい車両が通行するのか, そうした車両を緊急時にストップすることができるのかということについても検討を行う.

では, 実際に2016年リオ大会ではどういった対策を行ったか時間の都合があるので, 概要についてお話したい. まずそれぞれのエリアのセグメンテーションを行い, それぞれのエリアを分断することが必要となる.

最初のエリアが, フリートラフィックという公共エリアとなる. このエリアには選手団, 役員, 観客, 地元の人などが入ることができる. こうしたエリアでもセキュリティの確保は, もちろん必要となる.

次に, オリ・パラの会場の外周部にセキュリティを確保するためのペリメータを設けて, その内外を結ぶゲートにチェックポイントを設置しセキュリティチェックを行う. さらに, 会場内においても様々な箇所で, 爆発物, 武器などの持ち込みについて一人一人スクリーニングを実施した. こうしたエリア分割による警備を実施することにより, 効率的セキュリティを行うことができると考えている.

それから警備のターゲットについても対応の仕方が異なる. 例えば, セキュリティが確保された練習場から競技会場までの選手の移動であれば, 競技会場に入ってくる段階で, すでに金属探知機等でスクリーニングされているので, 危険物や禁止品は持っていないということを確かめた上で競技会場に入れることができる.

(以上は, 講演を要約したものである.)

(とりまとめ:深作和久)