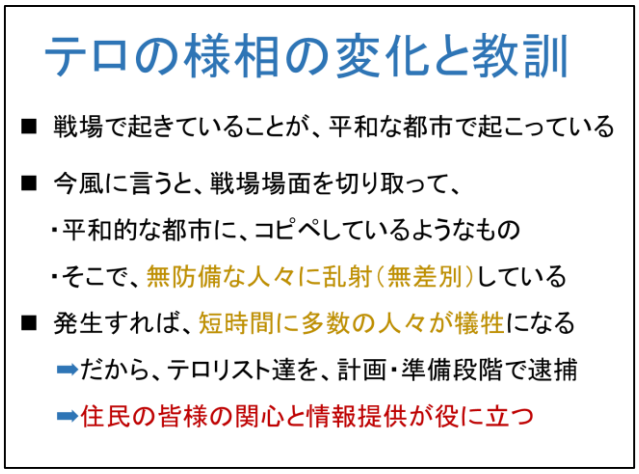
テーマ：2020 に向け、テロに対し如何に対応するか

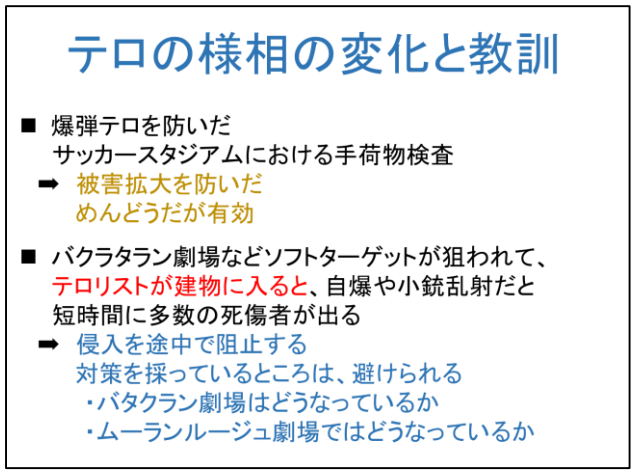
2020 年に、東京オリンピック・パラリンピックが開催されます。来日する外国人は 1 日 92 万人、オリンピック期間中では延べ 1564 万人にのぼると予想されています。つまり東京都の人口が倍近くに増えるわけです。この膨大な人数の入国者に、テロリストが紛れ込んでも発見できない可能性があります。そのために、皆さんにお示したテーマでパネルディスカッションをしていただこうというのが今回の目的です。

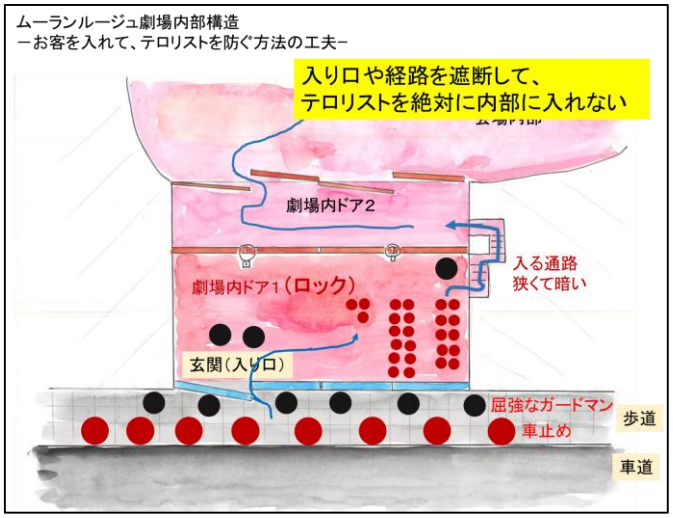
ところで近年開催されたオリンピック・パラリンピックでも、最大のリスクがテロでした。爆弾などを使用した物理的なテロへの対策に加え、ネット社会の弱点を狙うサイバーテロ対策が重要になってきました。

Q：「軍事・情報戦略研究所所長」の西村さんに、最近の国際テロの状況や特徴についてお話しいただきたいと思います。

パワーポイント例







地下鉄での警戒・監視

- 警察官による警戒・尋問
  怪しい者には、銃を向けて、上半身裸に
  警察官は3人一組（一人は自動小銃携行）
- 列車の中でもビデオカメラによる監視
  「ビデオ撮影中」の張り紙
- 乗車中に乗車券のチェック

Q：移民の少ない日本では、宗教的な対立や民族の軋轢などは見当たらないので安全だと思われがちですが、我が国におけるテロの可能性についてどのようにお考えですか。西村さんどうですか。

普段はイスラム過激派組織によるテロの可能性は低い。

オリンピックが近づくと、テロの対象となるＶＩＰや外国人が来日してくるので、それを狙ってテロリスト達が入国し、テロを実行する可能性が高まる。

次に問題になるのが、日朝関係にもよるが、米朝関係、日朝関係が悪化すると、北朝鮮工作員や特殊部隊によるオリンピックの妨害の可能性がある。北朝鮮特殊部隊や工作員のテロは、イスラム過激派組織よりも訓練を受けていて、軍人の中でも特にえりすぐりの兵士なので、対処が難しい。

警察だけでは、対応が難しいだろう。

Q：警視庁や東京消防庁では、テロ対策訓練に力を入れております。また、東京マラソンで警視庁が自働車テロを防ぐため、イスラエル製の新しい車両止めを用いたように、装備も強化しています。それでも防ぎきれないのがテロではないでしょうか。テロ対策には住民や事業者の皆さんの協力が欠かせないと思いますが、具体的な期待について、板橋さんと今浦さんにお話ししていただければと思います。まず、板橋さんからお願いします。

著名な施設が狙われる。

Q：次に、サイバーテロを取り上げたいと思います。オリンピックでのサイバーテロの脅威と、政府の取組について、板橋さんお話しいただけますか。

サイバー攻撃では、中国人民軍や北朝鮮の関与が問題になりますが、この脅威についてどう考えれば良いか、これは西村さんにお聞きします。

Ａ：北朝鮮のサイバー攻撃の可能性が高い

①北朝鮮の 2012 年までのサイバー攻撃ツールは、大量にメール送って、送り先のコンピューターの機能をストップさせる「DDoS」の基本的なものであった。

だが 2013 年には、攻撃目標に侵入してサーバーから情報を盗み破壊するクラッキングのレベルに達したものとみられている。

これまでは韓国の民間企業だけが攻撃対象となっていた。2014 年 12 月には、攻撃対象を米国企業に向け、コンピューターの機能をマヒさせることができることができた。近い将来には、韓国や日本の端末器を利用したサイバー攻撃により、これらの国が発信源となり、コンピューターから軍事情報等を盗んだり、サーバーを破壊したりしてくる可能性がある。

②2016 年 10 月頃、北朝鮮と関係するハッカー（ラザルスと呼ばれるハッカー集団）が、

2015 年 10 月のフィリピンの銀行、ベトナムの銀行、バングラディッシュの銀行（92 億円）、エクアドルの銀行にサイバー攻撃が行われ、送金指示で多額のお金が盗まれた。

③2017 年 5 月、世界約 150 か国、30 万台以上に身代金要求型ウイルス（ランサムウエア）による攻撃が行われた。ハッカーはウイルスに感染したパソコンの文書や写真を暗号化し、それを解除する費用として 300～600 ドル相当の仮想通過ビットコインを要求した。これらの攻撃で約 7 万ドル（約 791 億円）がハッカーに渡ったが、データの復旧には全く応じていない。

最近コインチェックのビットコインが盗まれたが、北朝鮮のハッカー集団の証拠が全くないので、私は別のハッカー集団だと考えている。

北朝鮮が「ほほ笑み外交」を展開する裏で、韓国の動向を不正な手法で探ろうとしていた実態が浮き彫りとなった形だ。

北朝鮮が支援するハッカー集団が２月上旬から３月中旬までに、８千回以上のサイバー攻撃を韓国の政府機関や大手企業に仕掛けていたことが分かった。感染被害は明らかになっていないが、知的財産や機密情報の窃取を目的とした攻撃であることが判明。北朝鮮が「ほほ笑み外交」を展開する裏で、韓国の動向を不正な手法で探ろうとしていた実態が浮き彫りとなった形だ。

元情報将校は、米情報セキュリティー会社「ファイア・アイ」が先月２０日に発表した、韓国や日本、中東諸国の企業や団体などにサイバー攻撃を仕掛けていた北朝鮮のハッカー集団「ＡＰＴ３７（別名Ｒｅａｐｅｒ）」などが関与している可能性を指摘。「韓国の機密情報を不正に得て有利な外交を進めようとしている恐れがある」（元情報将校）という。