東京2020大会に向けた サイバーセキュリティの準備

平成27年12月16日

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
テクノロジーサービス局長　　舘　剛司

自己紹介

舘　剛司（たち　たけし）

東京オリンピック・パラリンピック競技大会組織委員会

テクノロジーサービス局　局長

略歴：

1989年、大阪大学大学院・修士課程修了。同年、日本電信電話株式会社（NTT）入社。

映像伝送システム・次世代IPネットワークの開発、サイバーセキュリティ分野の研究開発戦略の策定などに従事。米国カリフォルニア大学バークレー校　経営工学・修士課程修了。

2013年より、米国のR&D子会社（NTT Innovation Institute, Inc.）設立とサイバーセキュリティ分野のR&Dプロジェクトに従事。

2014年より組織委員会へ出向し、東京2020大会の運営や準備活動に必要なネットワーク・情報システムなど技術全般に関する計画策定、開発、運用、サポートなどを統括。

本日のアジェンダ

1. 東京2020大会に際して、どのようなリスクを想定すべきか？
2. “大会を守る”とは？
3. 組織委員会のアプローチ
4. IoT時代のサイバーセキュリティ人材
5. 2020年に向けた取り組み

1. 東京2020大会に際して、どのようなリスクを想定すべきか？

大会用システム・ネットワークの概要（London 2012の場合）

スタッフ

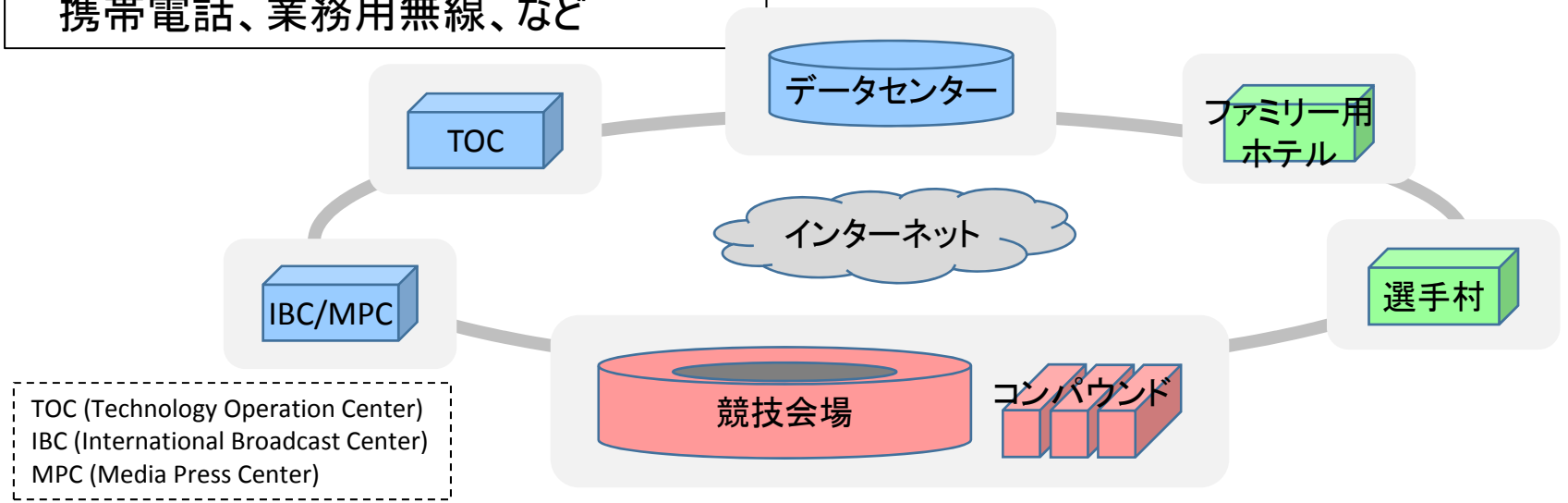
- 組織委員会スタッフ　8,000名／その他大会運営に関わったスタッフ　70,000名

ネットワーク

- 国内100以上のロケにまたがる大会用ネットワーク
- 提供された通信サービス：Eメール、インターネット、ビデオ/Web会議、IP電話、携帯電話、業務用無線、など

情報システム

- 発行された認証カード　25,000名分
- オリンピック26競技302種目、パラリンピック20競技503種目の競技結果をリアルタイムに放送局・メディアに提供
- 競技スケジュール、天候、輸送などに関わる情報を、14,700人のアスリートに提供



TOC (Technology Operation Center)
IBC (International Broadcast Center)
MPC (Media Press Center)

London 2012におけるサイバーセキュリティ

“大会公式サイトには、2週間の開催期間で2億2,100万のサイバー攻撃”

“7月26日（開会式前日）に、東欧のハッカー集団が大会のITインフラに対して数10分間に渡って脆弱性を探すためのスキャンをかけてきた。”

“7月26日（開会式当日）に電力システムを狙った攻撃の情報を受け、多くの技術者を要所ごとに配置するマニュアル操作に切り替えた。”

“同日午後5時には、（大会公式サイトへの）DDoS攻撃がピークに達し、北米および欧州の90のIPアドレスから1千万リクエストのDDoS攻撃が40分間にわたって続いた。”

“8月3日（大会終了間近）には、一秒あたり30万パケットのDDoS攻撃が同じIPアドレスから送られてきた。このアドレスはプレス向けに用意され共同利用されていたもの。”

【出典】“London 2012 prepares for cyber-attacks” (The Guardian, Apr 4, 2012)
http://www.theguardian.com/sport/2012/apr/04/london-2012-prepares-cyber-attacks
“The 'cyber-attack' threat to London's Olympic ceremony” (BBC, Jul 8,2013)
http://www.bbc.co.uk/news/uk-23195283
“How the London Olympics dealt with six major cyber attacks” (Compiuting, Mar 6, 2013)
http://www.computing.co.uk/ctg/news/2252841/how-the-london-olympics-dealt-with-six-major-cyber-attacks

過去大会でも想定されていたリスク（例）

分類	項目	備考
金銭目的のサイバー犯罪	偽チケット販売サイト	国内だけでなく海外でも想定される
	フィッシング、偽サイト、偽アクセスポイントなどによる個人情報の搾取	
	ランサムウェアによる脅迫	
ハクティビストの攻撃	大会サイトへの攻撃（DoS攻撃、改ざん）	大会に関するメディア報道、国の記念日、ネガティブ・キャンペーン、関連イベント開催などがきっかけ
	スポンサーや開催都市など関連サイトへの攻撃	周辺サイトがとばっちりを受けやすい
	競技対戦国の関連サイトへの攻撃	近年のスポーツイベントにつきもの
サイバーテロ	大会システムへの侵入によるシステム破壊、データ破壊	狙われるかどうかは、大会開催時の国内外の情勢に依存
	大会システムの乗っ取り	
	重要インフラへのサイバー攻撃	
サイバー戦争	要人を狙ったサイバースパイ	海外要人も多数来訪するため

2020大会におけるソーシャルネットワークの活用予測

【出典】 “ascent, a vision for sport and technology,” (Atos SE (Societas Europaea))
http://atos.net/content/dam/global/olympic-games/atos-ascent-vision-sport-and-technology-2013.pdf

全世界でのTV視聴者数	40億人, 全人口の57%（London 2012） ⇩ **50億人, 全人口の66%（Tokyo 2020）**
ソーシャルネットワーク（Facebook, Youtube, Twitter）の全ユーザ数	13億人（London 2012） ⇩ **43億人（Tokyo 2020）**
ソーシャルネットワークで大会コンテンツをシェアする人数	10億人（London 2012） ⇩ **データトラヒック増加率 3,000%（Tokyo 2020）**
男子100m決勝でのピークツイート数	80,000メッセージ／秒（London 2012） ⇩ **660,000メッセージ／秒（Tokyo 2020）**

2020年に向けたテクノロジーの動向

【出典】 “ascent, a vision for sport and technology,” (Atos SE (Societas Europaea))
http://atos.net/content/dam/global/olympic-games/atos-ascent-vision-sport-and-technology-2013.pdf

Atos Scientific Communityが注目する5つの動向：

1. リアルタイムでのデータ利用
   - パターンが形成されている最中でも、それを特定し反応する技術
2. ソーシャルネットワークの標準化
   - ビッグプレイヤーによる独占的エコシステムから、より多様なネットワークがオープンに連携する環境への移行
3. カスタマイズされた視聴体験
   - 個人の嗜好にあわせたショー、イベント、カメラ視野、コメントスタイルなどを提供するパーソナルTVチャンネル
4. 新しいセキュリティ情報源
   - ソーシャル分析、音声認識・顔認識、ロボット警官、ロボットカメラ、クラウドソーシング…
5. テクノスポーツ
   - 競技ビデオゲーム、仮想スポーツリーグ、ロボット競技…

スポーツ分野におけるIoTとは？

＊アドバンスト・スタッツ＝選手のプレー内容に関する統計情報
（ベーシック・スタッツ）をもとに、より高度な分析を行った統計情報

測定・収集（インプット）


カメラ映像分析


無線データ伝送

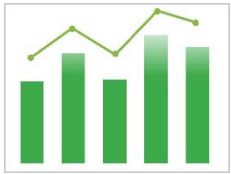


ウェアラブルデバイス

可視化・分析（アウトプット）


4K・8K映像


VRゴーグル


アドバンスド・スタッツ*

スポーツ版
ビッグデータ

競技者

日々の上達が見える
どうすればいいのかが分かる

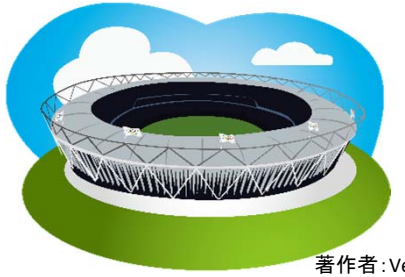

著作者：Vector Open Stock


著作者：Micah Lawrence


著作者：freedesignfile.com

観戦者

今までになかった臨場感
今までわからなかった面白さ


著作者：Vector Open Stock

東京2020大会で想定される環境の変化

社会全体のますますのIT化

- モバイル端末の進化・普及により、ロンドン大会より桁違いに大きい通信トラヒック
- スポーツイベントの世界でも、ネットワークにつながるもの（IoT）が急激に増加

大会システム・放送システムの進化

- インターネットやクラウドへの依存度の増加
- 放送システムにおけるIP技術の採用拡大

国際情勢の変化

- サイバーテロやサイバー戦争に巻き込まれるリスク

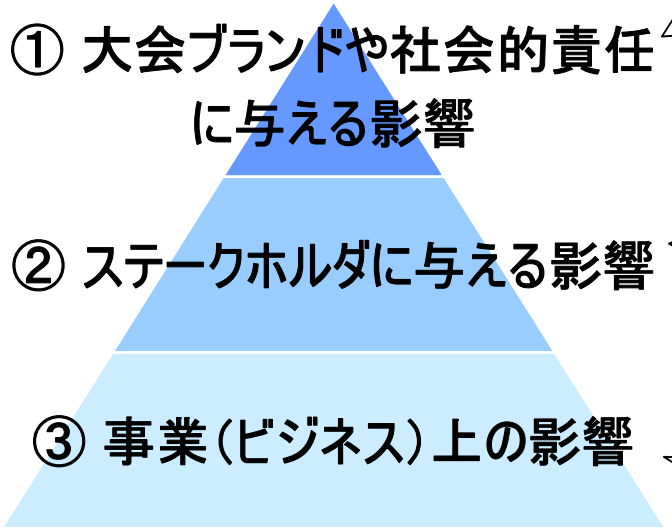
関係機関どうしの連携の重要性

- リスクの広域化・複雑化に伴い、一組織・機関に閉じてできる対策の限界

2. “大会を守る”とは？

オリンピックを守るとは？

『オリンピックにおける最大のリスクとは、結局はレピュテーションリスクに尽きるだろう。』
（Mr. Oliver Hoare, ロンドン大会における英国内務省所属の大会全体のセキュリティ責任者）



- オリンピック憲章でうたう根本原則に反しない。
- オリンピック・ムーブメントを具現化する。
- パラリンピックについても同様に重視する。

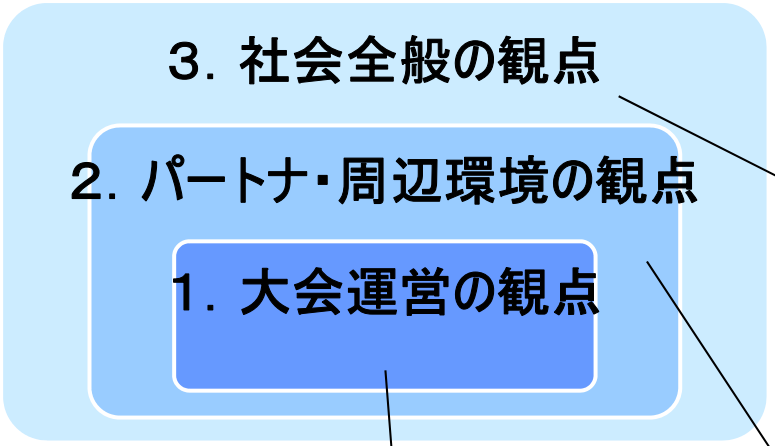
- ステークホルダ（放送局、競技団体など）に迷惑をかけない。
- 円滑に大会を運営する。

- 赤字を出さない／法律を守る／けが人・病人を出さない／サステナビリティに則う／レガシーを残す

（注）本ページの記載内容は、サイバーセキュリティ対策検討用の仮評価結果であり、実際の評価と異なる可能性があります。

守るべき対象は？

想定リスクの全体像



「狙われやすい」「対策が漏れやすい」のは、むしろ大会システムの周辺環境や日本社会のインフラ、関連企業のサイトなどである。

3．間接的に大会への影響が懸念されるもの

- *対象リスク事例＝自然災害／パンデミック／社会基盤に対するテロ・サイバーテロ／SNS上での日本・東京に対する評価・評判／RUGBY 2019へのテロ*

1．組織委員会の管轄範囲内で、大会運営に直接影響するもの

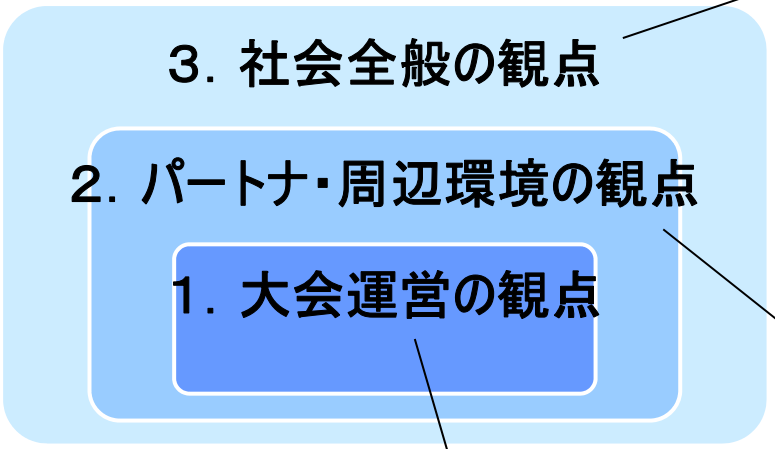
- *対象リスク事例＝観客の動線管理／選手村での食事提供／大会システムへのハッキング／内部情報漏えい／予算不足に伴う運用レベルの低下*

2．パートナや周辺環境の問題で、大会への影響が大きいもの

- *対象リスク事例＝災害に伴う避難誘導／サプライチェーン内在リスク／偽チケット販売サイト／重要インフラの障害・停止／会場周辺でのパニック／参加国のボイコット／ドーピング*

サイバーセキュリティ・ガバナンスの課題

想定リスクの全体像



3．社会が抱える課題

- *産業界として、いかにサイバーセキュリティの成熟度を上げられるか？*
- *産業界や教育機関が、いかに将来のセキュリティ人材を安定供給できるか？2020年以降に人材が活躍できる場を提供できるか？*

2．パートナや関連ステークホルダの抱える課題

- *緊急時に組織をまたがって、いかに迅速に情報共有できるか？必要な判断ができるか？*
- *必要なセキュリティ人材をいかにそろえるか？訓練するか？*

1．組織委員会の抱える課題

- *異なる出身母体を持つ人材から構成される時限組織において、どのようにセキュリティ・ガバナンスを効かせるか？*
- *サイト・セキュリティとサイバー・セキュリティとをいかに統合的にガバナンスできるか？*

大会成功に向けて社会が抱える課題

- ✓ 日本の通信環境（インターネット、公衆WiFiなど）の課題　⇒対策徹底の難しさ
- ✓ モバイルトラヒックの急増に伴う課題　⇒トレンドを読む難しさ
- ✓ ネットワークにつながるモノ（IoT）が急激に増加していることに伴うルール・体制の課題　⇒社会インフラ全体の複雑性が増している
- ✓ サイバーセキュリティ人材不足に関する課題　⇒どこまで育成すればいいのか？
- ✓ 関係機関における情報収集・情報共有に関する課題　⇒言うほど簡単ではない。。。
- ✓ 関係各国との連携体制に関する課題　⇒オリンピックだからこそ協力を仰ぐべき

- ✓ グローバルに見ると、日本として**サイバーセキュリティの“経験値”が足りないのでは**ないか？

他の開催都市が有している経験値

- ✓ 基本的には、物理的なテロ・犯罪・政治的活動がサイバー区間に移行しているだけ。
  - ➢ ロンドン：政治的プロテスト集団、アラブ・イスラム武装勢力
  - ➢ ソチ：イスラム武装勢力、国内分離独立勢力
  - ➢ リオデジャネイロ：麻薬組織、マフィア
  - ➢ 平昌：隣国との関係
- ✓ 実戦経験のない組織は、本番にはきわめて弱い。より実戦的な演習を取り入れるべき。
  - ➢ 大規模スポーツイベントの運営において、幹部クラスが大きな意思決定を迅速に行うことができるための演習が必要。
  - ➢ 演習で恥をかくことを恐れるべきではない。経験値が上がらないことをこそ恐れるべき。

3. 組織委員会のアプローチ

組織委員会がとるべきアプローチ

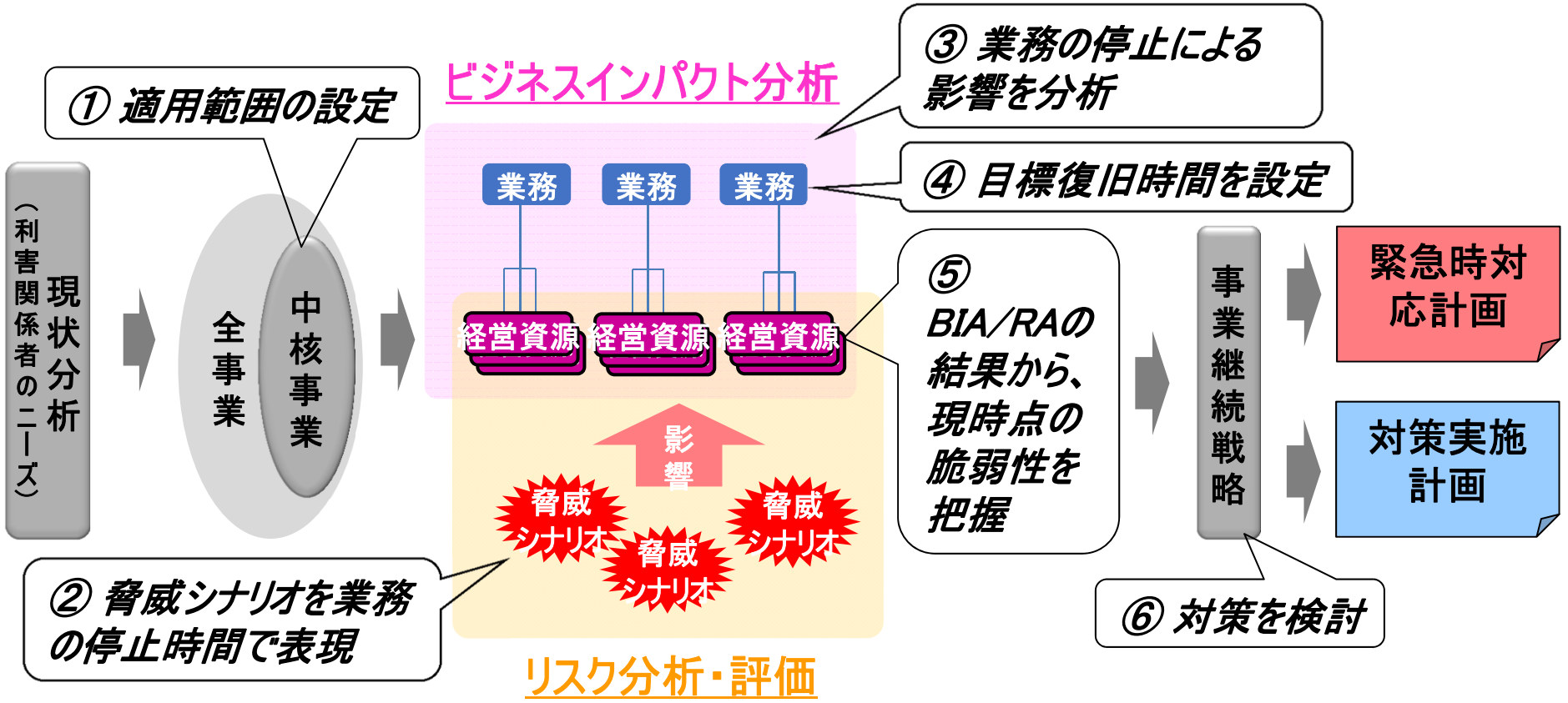
アプローチ①　リスク・アーキテクチャ（全体像）の把握

- ✓ 特定のシステムや情報を守るだけでは不十分。組織委員会の事業（ビジネス）である大会のオペレーション（事業継続性）やレピュテーションを守るという目標設定が必要。
- ✓ 複雑化したITシステムも含め、いろいろな要素が複雑に関連してくる大会運営のリスクを洗い出そうとすると、**経験則だけに頼っていても限界がある。基本に立ち返った検討が必要。**

アプローチ②　関係機関との連携

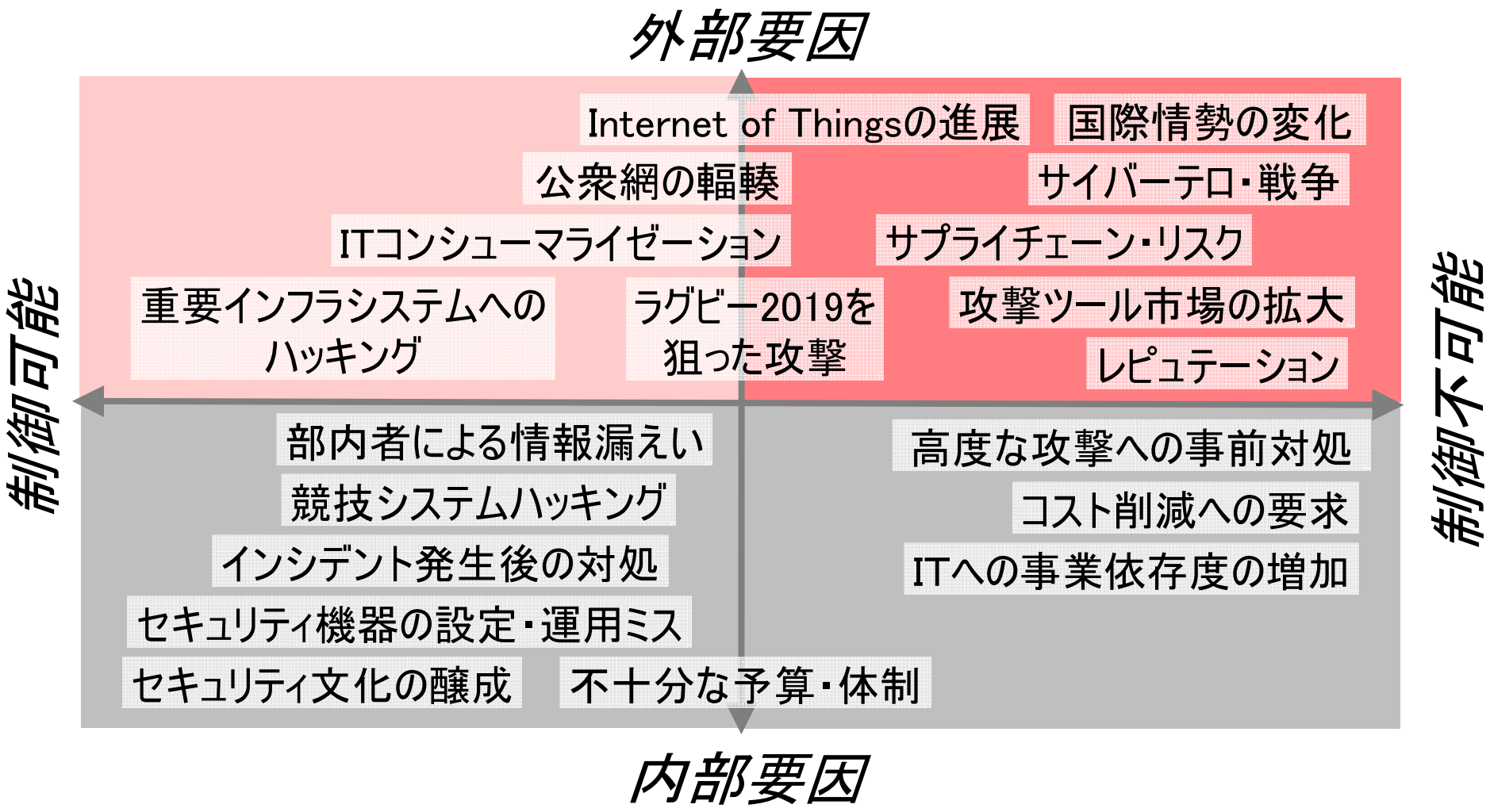
- ✓ リスク全体像を把握し、管理するためには、関係業界、行政機関、国際機関、近隣諸国などとの連携が必要。

アプローチ①　リスク・アーキテクチャの把握
＜事業継続性の検討フロー＞



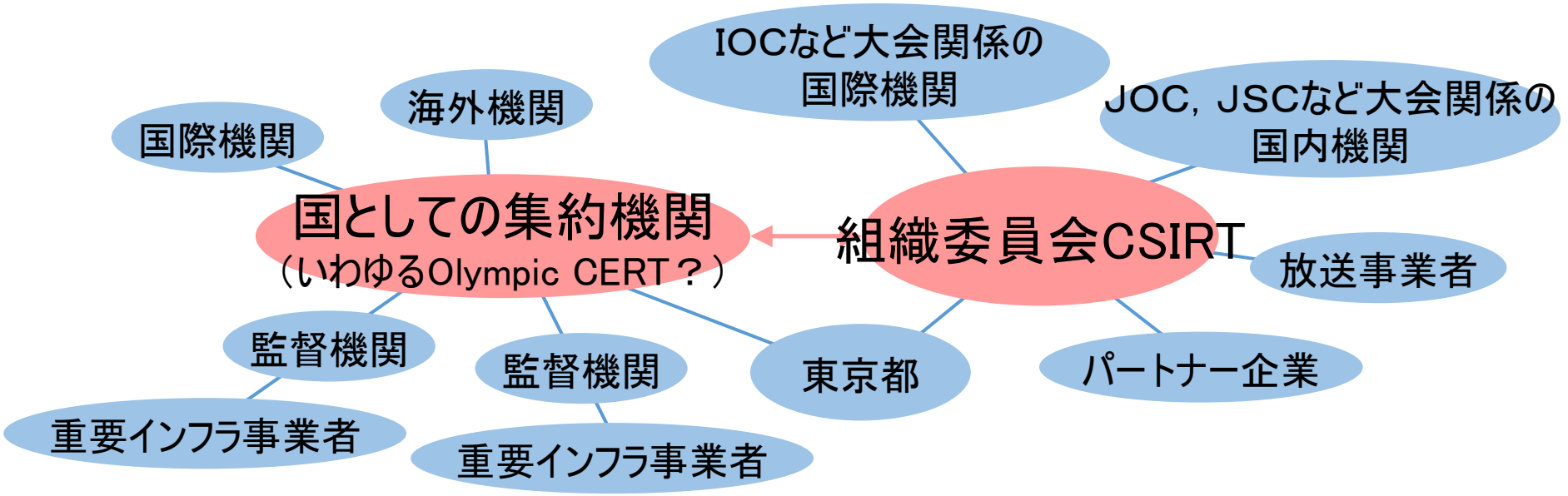
✓ 攻撃者側も体系的・合理的な考え方にそって、システムや組織に内在する脆弱性・弱みをついてくる。守る側も、結局は同じ手法でしか対策を検討できない。

システム・ネットワークに関するリスクの分類例



（注）本ページの記載内容は初期検討用の仮評価結果であり、実際の評価と異なる可能性があります。

アプローチ②　関係機関との連携



- ✓ “連携”は図に書いて指示するだけでは進まない。
- ✓ **相手の“顔”や“力量”が見えていること、個人間の“信頼関係”があること、**がいざという時に連携が機能する必要条件。

災害・危機対応における日米の考え方の違い

日本

- ✓国・公共機関・地方公共団体・事業者・住民それぞれの役割を明確に。
- ✓平時の業務の延長上に災害・危機対応を位置付け。
- ✓**平時の指揮統制の対応能力を超える災害・危機に対しては十分に機能しない可能性も。**

米国

- ✓災害規模に応じて**国やさまざまな組織が柔軟に連携する仕組み**。
- ✓巨大災害の発生時に、大統領による災害宣言によって連邦政府の機関（アメリカ合衆国連邦緊急事態管理庁）が災害・危機対応業務を直接指揮・統制。
- ✓郡・市においても、対応能力を超えるような災害・危機 発生時には、州が代わって直接物資やサービスを提供。
- ✓企業（NPOを含む）・ボランティアを地域の一部として位置付け。

【出展】“災害・危機対応における日米比較と国際規格ISO22320” 東田光裕、小阪尚子、前田裕二、NTT技術ジャーナル2013.3.
http://www.ntt.co.jp/journal/1303/files/jn201303048.pdf￥

4. IoT時代のサイバーセキュリティ人材

攻撃専門チームの必要性

- ✓ 関連するシステム全体の複雑性が増すにしたがい、すべてのリスクを洗い出す作業がますます難しくなってきている。
  - ➢ 「穴を見つけてふさぐ」という終わりのない作業だけを繰り返しても、モチベーションが下がる、どこかで妥協したくなる。
- ✓ むしろ「新しい穴を見つける」「誰も気づかなかった抜け道を見つける」という**“クリエーティビティ”が重要**。
  - ➢ 特にIoTのような新しいインフラを対象とする際には、「守る」だけでなく、「攻める」ためのアイディア出しこそが近道。最初からすべての穴を見つける必要などない。
  - ➢ 取り組むべき課題は、**「組織をまたがって検討に必要な情報にアクセスできるような仕組み・権限をいかに持たせるか？」、「攻撃専門チームの知見（組織にとって最重要機密情報）をいかにセキュアに管理するか？」**

サイバーセキュリティのクリエータとは？

✓ 現在のサイバーセキュリティの世界を作り上げた先達も、クリエータだった。

Brain（コンピュータウイルス）

BrainまたはBrain virusとは、パキスタン人の兄弟が作成した、極めて初期のコンピューターウイルスである。文献によっては最初のコンピューターウイルスと紹介されている。

このウイルスはフロッピーディスク内のブートセクタに寄生し、フロッピーディスクからシステムをコピーすることによって感染する。（中略）作者はパキスタンでコンピューターの販売・メンテナンス、ソフトウェアの販売を行なっていた会社を経営する兄弟であった。

彼らは違法コピー対策として、違法コピーにより感染し、その感染ソフトを起動した場合にとあるメッセージを表示するようにしたプログラムを仕込んだ。そのメッセージには著作権者でもあるウイルス製作者の名前と、会社名、連絡先が表示され、ウイルスに注意し、ワクチン接種が必要な場合は会社へ連絡するように書かれていた（すなわちウイルスと自ら名乗った）。（後略）

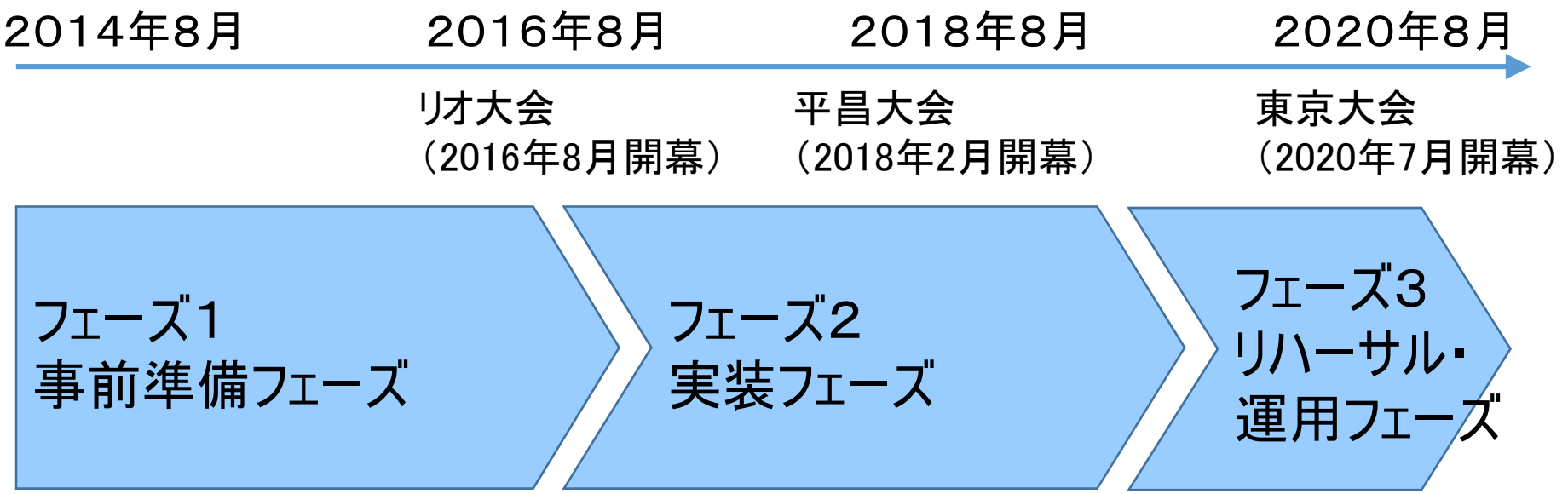
【出典】ウィキペディア　https://ja.wikipedia.org/wiki/Brain_(コンピュータウイルス)

レガシーとしてのサイバー人材

- ✓ これまでの日本の社会では、サイバーセキュリティはほとんどの場合、コストでしかなかった。
  - ➢ いかにコストを減らして“本業”に集中できるか、にしか興味がない人達がまだまだ大多数。
  - ➢ この認識で育成される人材とは、結局は“守ることができる人材”でしかない。“いたちごっこ”の構造はなにも変わらない。
- ✓ これからは、「だれも考え付かなかったITの活用方法」「攻撃者の目線になりきった完璧な防御方法」を実現して、**世界のハッカーと勝負できる“クリエータ”**が求められているのではないか。
  - ➢ このような人材が社会や組織のIT化を支えるポストにつき、競争力の源泉として活躍するような絵姿こそが、2020年のレガシーではないか。

5.　2020年に向けた取り組み

2020年に向けたロードマップ



- 関係機関とのコンセンサス形成（連携、役割分担など）
- リスク評価手法についての合意

- リスク評価の本格化
- システム設計・運用設計への反映
- 関係機関での対策実装

- 実運用への移行
- テストイベント、リハーサルを通した実演習

（注）上記のあくまで計画レベルであり、実行を保証するものではありません。

各界との連携が必要と考える課題（1．Olympic CSIRT）

- ✓ Olympic CSIRTに、インシデント発生時に民間企業（ISPなど）から迅速にインシデント情報が集まりやすいよう、**環境作り（業界ISACなど民間を巻き込んだ体制、情報提供のインセンティブ）が必要**ではないか？
- ✓ 大会期間中の特別措置として、通信遮断、通信傍受、サイトテイクダウンなどの非常措置が迅速に取れるよう、**環境・ルール(法的側面、個人情報の取り扱い・共有ルールなど)の整備**が必要ではないか？

各界との連携が必要と考える課題
（2．社会インフラのリスク洗出し・評価）

- ✓ 大会運営に際して想定される社会インフラのサイバー・リスクの洗出し・評価を、**各事業者や業界・監督官庁に閉じずに、業界横断的に議論する場**が必要ではないか？
- ✓ たとえば**放送業界、物流業界、交通業界など**のシステムや業務オペレーションが、最近ではインターネットやクラウドに依存している部分も多いが、各事業者や業界に閉じてリスク評価や対策検討するだけでは、全体を見たリスク分析にはならないのではないか？

各界との連携が必要と考える課題（３．防衛能力強化）

- ✓ 攻撃者や攻撃対象の情報を収集し、防御方法・体制をブラッシュアップするためにも、攻撃者視点の分析や攻撃シナリオ作成などを行う専門チームが必要ではないか？
- ✓ 大会を一部の関係者だけの閉じたイベントに終わらせないために、模擬大会システムを使ったハッカソン開催など、**サイバーセキュリティ分野でのエンゲージメント活動（世の中の参加意識を高める活動）**が有効ではないか？

最後に

- ✓ 国を挙げての一大イベントだからこそ、大会の直接の関係者（組織委員会、スポンサー企業など）だけががんばってもうまくいかない、限られた人々だけでやっても意味がない、というのはサイバーセキュリティにも当てはまります。
- ✓ 業界全体・社会全体（さらには近隣諸国も交えて）で、『大会・街・国を守っていく／サイバー総合力として一段のレベルアップを目指していく』という目的意識を醸成することが、『一番の対策／一番大事なレガシー』と考えます。