東京2020大会に向けた サイバーセキュリティのチャレンジ

～経営リスクマネジメントの実践的ケーススタディ～

平成31年2月18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員会

テクノロジーサービス局　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。

本日の視点

- ✓ 『オリンピックに向けた準備・運営（テクノロジー面）というプロジェクトの全権を任された際に、責任者・経営者として、サイバーセキュリティをどのように捉え、どのように対策に取り組むのか？』
- ✓ この実践的ケーススタディをもとに、組織・企業として抱えるサイバーセキュリティの本質的・共通的な課題に迫ってみます。

アジェンダ

- ✓ ケーススタディの前提条件（東京2020大会とは？）
- ✓ ポイント１：課題の定義（なにを守るのか？）
- ✓ ポイント２：CISOの役割（なにをすべきなのか？）
- ✓ ポイント３：組織全体の課題（だれの責任なのか？）
- ✓ ポイント４：守りと攻め（攻撃者の目線）
- ✓ 最後に（リーダーの資質）

ケーススタディの前提条件
（東京2020大会とは？）

リオ2016大会開会式の日本選手団入場行進

大会規模の比較

競技数	20
種目数	163
参加選手	5,152
会場数	34
内:都内	22
チケット枚数	202万枚

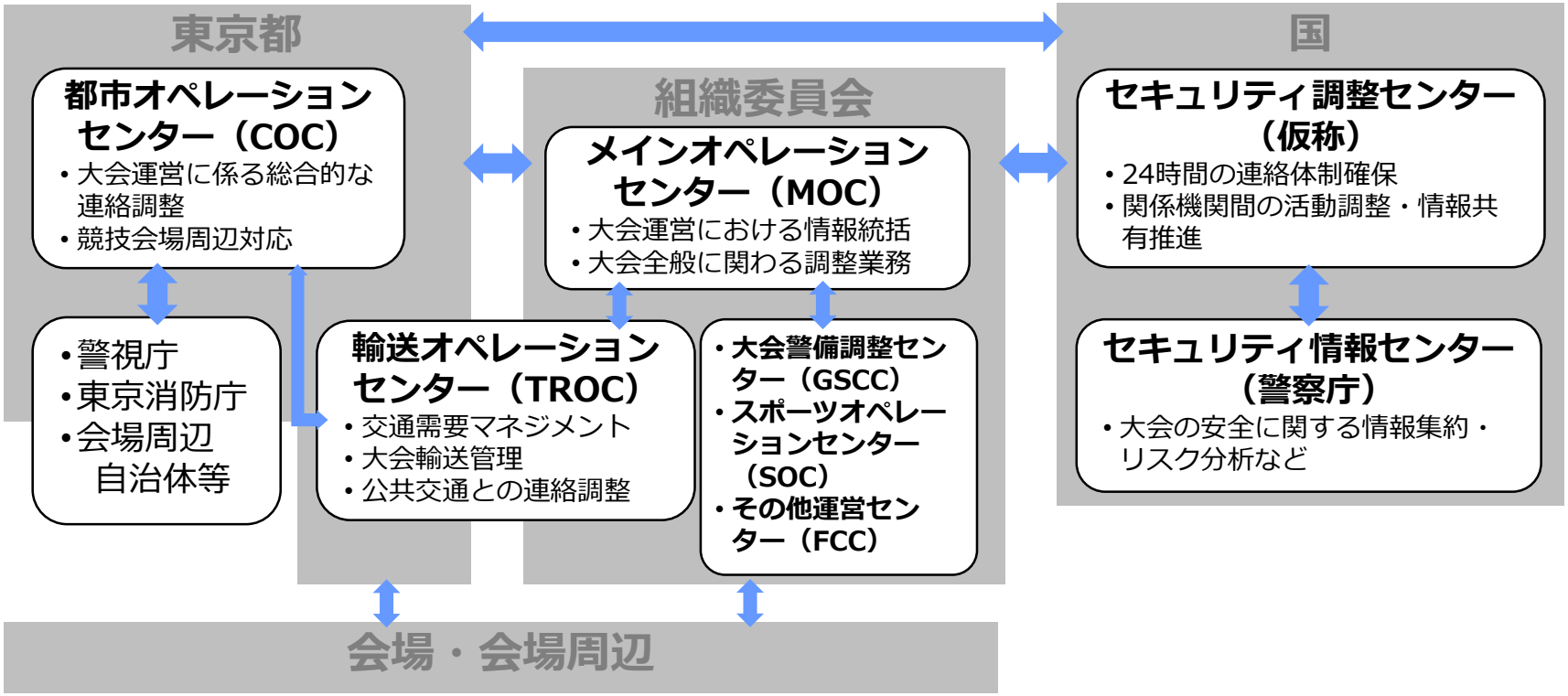
競技数	33
種目数	339
参加選手	11,090
会場数	42
内:都内	25
チケット枚数	1,010万枚

大会運営業務とその規模感（例）

- ✓ イベントオペレーション（モノの調達・流通）
  - 競技用具、計測機器・PC・通信機、競技用什器類、医療用品など／大会関係者に提供する食事：**1,400万食**（オリンピックのみ）、ピーク時は**30分で1万食提供**
- ✓ イベントオペレーション（ヒトの移動・輸送）
  - **観客：780万人**（オリンピック）、**230万人**（パラリンピック）／アクレディテーションカード発行枚数：**20万枚**／関係者・観客の輸送に必要な**バス：2,000台**／開催都市を訪れる**期間中の観光客2,000万人**
- ✓ スポーツオペレーション（競技運営）
  - 選手･役員数：**18,200人**／33競技（オリンピック）、**8,000人**／22競技（パラリンピック）
- ✓ ファシリティオペレーション（会場設置・運営）
  - **選手村16,000人収容**／**国際放送センター75,000㎡**／必要な**倉庫面積80,000以上**
- ✓ ビジネスオペレーション（販売・顧客管理）
  - チケット販売総数**1,010万枚**、公式モバイルアプリダウンロード数**最大2,000万**

オペレーションセンターを中心とした体制

- ✓ **大量の物流、関係者や観客の輸送・誘導、猛暑への対策、台風やゲリラ豪雨への対応、急なスケジュール変更、**など、さまざまな課題やインシデントに対処するための集中管理体制が必要。



ロンドン2012大会の
サイバーセキュリティインシデント

- ✓ 大会公式サイトに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実行。
- ✓ 7月27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替え**。
- ✓ 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分間にわたって継続。
- ✓ 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アドレスから送付。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。

リオ2016大会のトラブル概観

- ✓ テレビでは放映されない数々のトラブルが発生。
  - 「（ゴルフ）競技中に過負荷による競技情報システムダウン」「大会初日の過負荷によるモバイルアプリダウン」**「インターネット回線トラブル」「停電・電源トラブル（五輪閉会式時間中の会場一帯の停電も含む）」**「多発するサイバー犯罪（なりすましWi-Fi、ATMスキミング）」など。
- ✓ 競技会場のIT環境はかなり貧弱。
  - 「観客向けWi-Fiはかなり限定的」「特にパラリンピックでは大型ディスプレイもかなり撤去」「競技がどう進行しているのか、見ていてもよくわからない」
- ✓ 競技運営だけはほぼ完ぺき。それ以外**（特に輸送・警備・サイネージ）はかなり関係者に不評**。
  - ギリギリまで予算削減・人員削減を行い、大会関係者や観客の満足度・サービスレベルを犠牲に。

平昌2018大会・開会式で発生したインシデントに関するおもな経緯・報道(1/2)

- ✓ 2018/1/6：米マカフィー社が、平昌冬季五輪の関連機関を標的にしたサイバー攻撃が確認されたと明らかに。
  - ➢ 2017年12月下旬の対テロ訓練期間中に、関係機関からを装った標的型メール攻撃を観測。
- ✓ 2018/2/9：開会式の45分前から、**プレス関係者向けの通信環境や映像配信、大会Webサイトなどに影響**。
  - ➢ **これまでオリンピックを標的としてきたサイバー攻撃と比べ、明らかに影響範囲が広い。**
- ✓ 2018/2/10：平昌大会組織員会が、大会開会式で発生したサイバー攻撃について正式発表。
  - ➢ 『開会式運営や競技運営に直接影響を与えるものではなく、システムは数時間で回復した。詳しい原因は解析中。』

平昌2018大会・開会式で発生したインシデントに関するおもな経緯・報道(2/2)

- ✓ 2018/2/12：米シスコシステムズ社の情報分析チーム（Cisco Talos）が、攻撃に用いたとみられるマルウェアの検体サンプルを確認したと報告。
  - ➢ マルウェアからはシステム破壊の機能のみが確認されている。
  - ➢ マルウェアには**44個の平昌五輪関連の資格情報（ユーザー名、パスワード等）とみられる文字列がハードコーディング**されている。
- ✓ 2018/2/14：Cyber Scoop社の報道によると、『Atos社内の複数のシステムが、2017年12月からすでに侵入されていた可能性が高い。』
  - ➢ Virus Totalにポストされたファイルをもとに、Cyber Scoop社が分析。
- ✓ 2018/2/25：米紙ワシントンポストが、『ロシア軍スパイが平昌組織委員会のコンピュータ数百台をハッキングし、北朝鮮の仕業と見せかけようとした』との米国情報当局者の話を報告。
  - ➢ コンピュータ用のルータ（通信機器）をハッキングし、ネットワークを麻痺させるマルウエアを埋め込んだとの分析。

ポイント１：課題の定義
（なにを守るのか？）

リオ2016大会のカヌー競技会場

インシデントに関する考察(1)

✓ **攻撃目的の変化・攻撃手法の進化**

- これまでの大会では、インターネットに晒されるWebサイトへの攻撃が主流だった。これに伴って、大会ボイコットキャンペーンも盛んだった。
- 今回は大会前の表立った活動はあまり見られなかったが、（おそらくは標的型攻撃を経て）明らかに**内部に侵入されてピンポイントでの攻撃**を許している。
- 自らの主張を世の中に訴える（ハクティビスト）というよりは、**目的を持った攻撃**に近い印象。

攻撃目的の変化・攻撃手法の進化

✓ “ハクティビストの攻撃”のレベルから、“サイバーテロ”と呼べる攻撃レベルへと、進化している。

分類	項目	
金銭目的のサイバー犯罪	偽チケット販売サイト	各大会で必ず顕在化するリスク
	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）	
	スポンサーや開催都市など関連サイトへの攻撃	
	競技対戦国の関連サイトへの攻撃	
サイバーテロ	大会システムへの侵入・乗っ取りによるシステム破壊、データ破壊	よりビジネスインパクトが大きいリスク
	重要インフラへのサイバー攻撃	
サイバー戦争	多数来日する海外要人を狙ったサイバースパイ	
	リアルテロの手段としてのサイバー （認証カード改ざん、セキュリティカメラへのハッキングなど）	

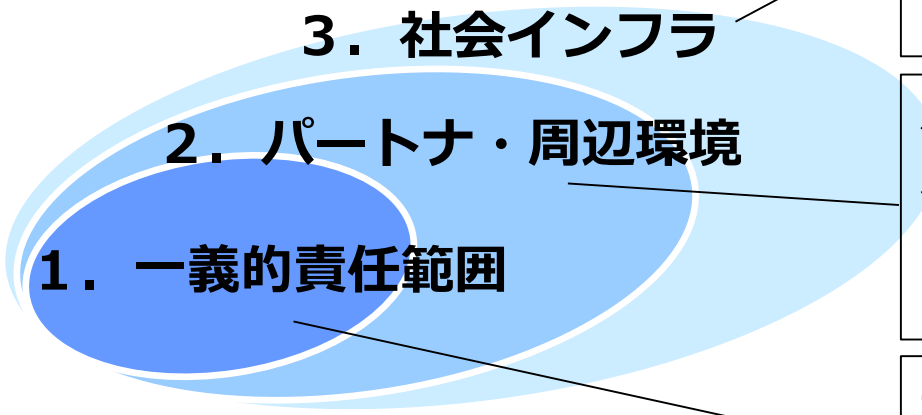
ポイント１：課題の定義

- ✓ **これまでにない危機感の高まりを受けて、まずは取り組むべき課題をどう定義するか。**
- ✓ **ITの世界では時間軸が早い、これまでの事業での常識が通用するとは限らない。**
- ✓ **「今まで事故が起きていないから大丈夫」「この対策で、これまで大丈夫だったから」という判断は根拠がない。**

なにを守るべきなのか？

- ✓ 自社で運用する業務システム・ネットワークだけを守っても、事業を守ることにはならない。
- ✓ 事業委託先や社会的レピュテーションも含めて、総合的に守る観点が必要。

想定リスクの全体像



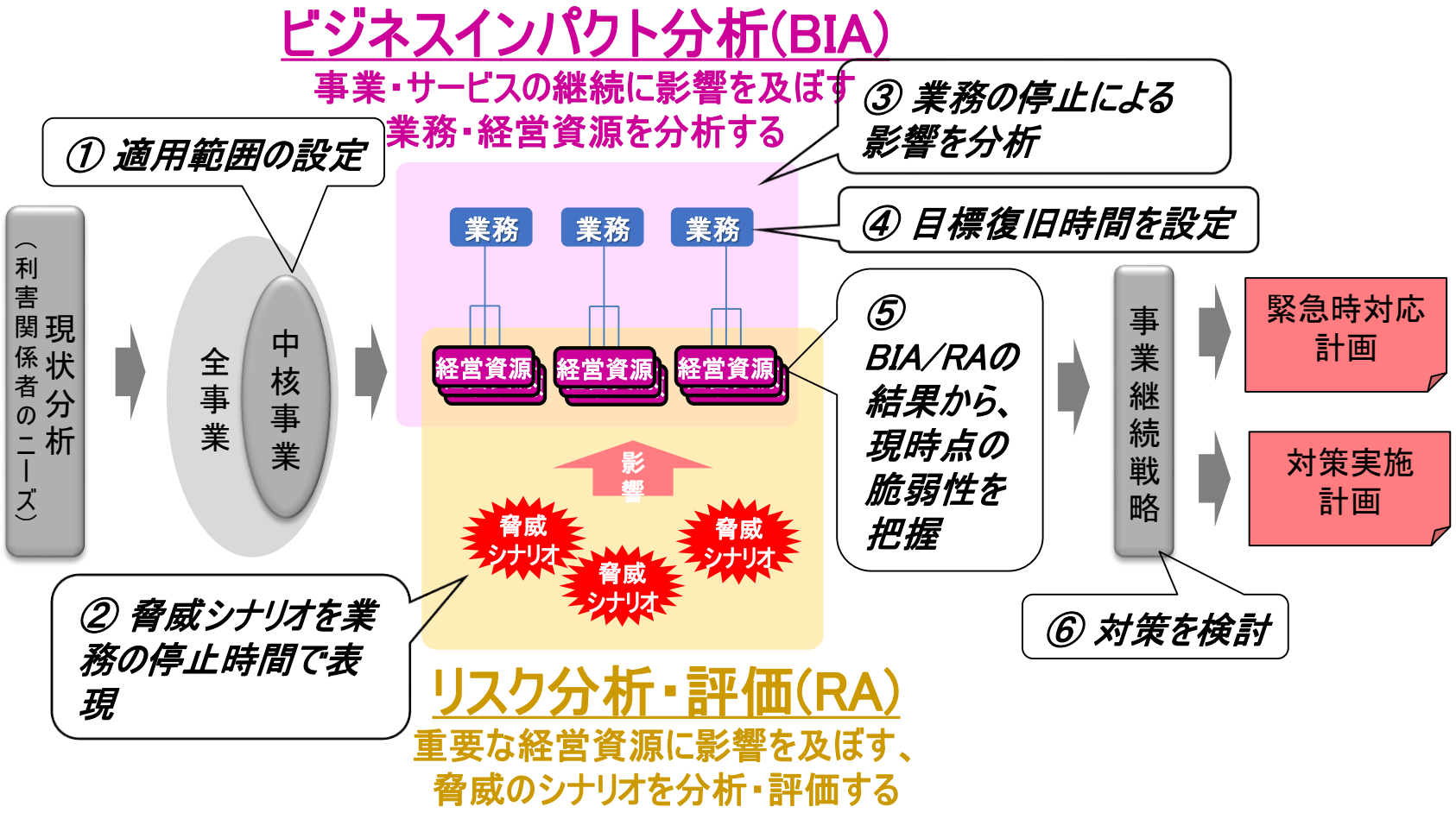
間接的に事業に影響するリスク
（重要インフラで発生するサイバーテロ／SNS上でのネガティブキャンペーンなど）

パートナや周辺環境に内在するリスク
（サプライチェーン・リスク／請負会社側での情報漏えいなど）

事業主体側で管理すべきリスク
（基幹システムへのハッキング／内部情報漏えいなど）

リスク評価と対策立案

- ✓ ISO22320（社会セキュリティ緊急事態管理）にもとづく分析フロー。



ポイント２：CISOの役割
（なにをすべきなのか？）

平昌2018大会の国際放送センター

インシデントに関する考察(2)

✓ 上流工程での検討・対策の重要性

- 大会直前のタイミングで、国が関与して大会のサイバーセキュリティ対策を強化しても、事故は防げなかった。
- インシデント対応やフォレンジック対策など事後対策に関心が集まり勝ちだが、まずはネットワークや情報システムの**基本設計段階から、セキュリティ要件や運用体制のガバナンスについての考慮・徹底・定期的棚卸し**が重要。
- 高度な対策の前に、まず優先すべき対策：①サーバ堅牢化・管理者アカウント管理強化／②アウトソーシング事業者へのガバナンス強化／③エンドユーザ対策
- より高度なエンドポイントセキュリティ対策の導入にあたっては、作業の手戻り防止と全体費用の最適化のために、**実施時期・順序について十分な考慮が必要**。
- 組織として未成熟な段階でのソリューション導入は無駄な投資になりかねない。

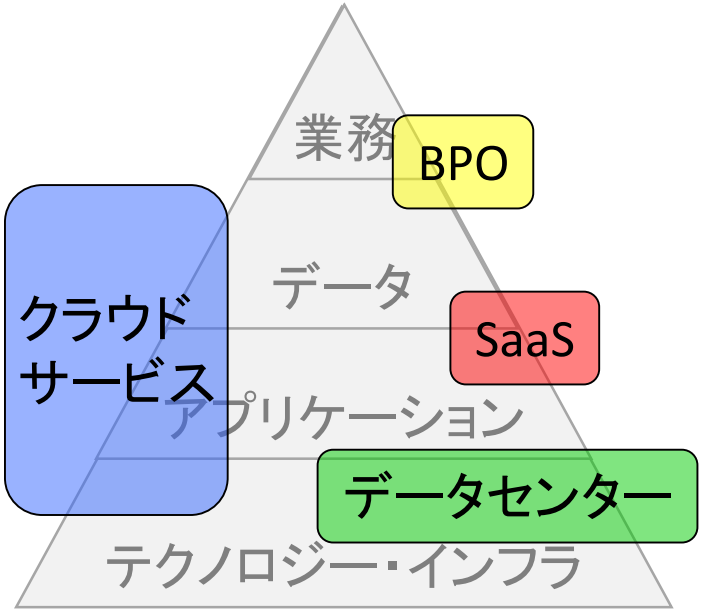
ITガバナンスの課題

✓ 組織委員会における前提条件

- なるべくIT資産を持ちたくない。
- 多岐にわたる業務、関係組織との連携、失敗は許されない。
- 限られたリソースの中、スポンサー企業や関連組織の協力を最大限に仰ぎたい。
- つまり、クラウド、SaaS、BPOを最大限に活用したい。

✓ 課題

- ヘテロジニアスな環境において、**統一的なITセキュリティ・ポリシー、情報セキュリティ管理、迅速なインシデント対応**などをいかに実現するか？
- アウトソーシング先のＩＴ基盤、運用も含めた**ガバナンス強化**が必要。



ポイント２：CISOの役割

- ✓ **「すでにできあがったシステム、組織、業務フローにおいて情報セキュリティを確保する」だけでは不十分。**
- ✓ **「これから変化するシステム・組織において、情報セキュリティの確保のために、もっとも最適なプロセス・アプローチ・リソース計画を策定・実践する。」業務システム全体のアーキテクチャ設計がポイント。**
- ✓ **さらに、ITセキュリティ投資の優先度の見極めがポイント。（なにを捨てて、なにを救うか）**

ポイント３：組織全体の課題（だれの責任なのか？）

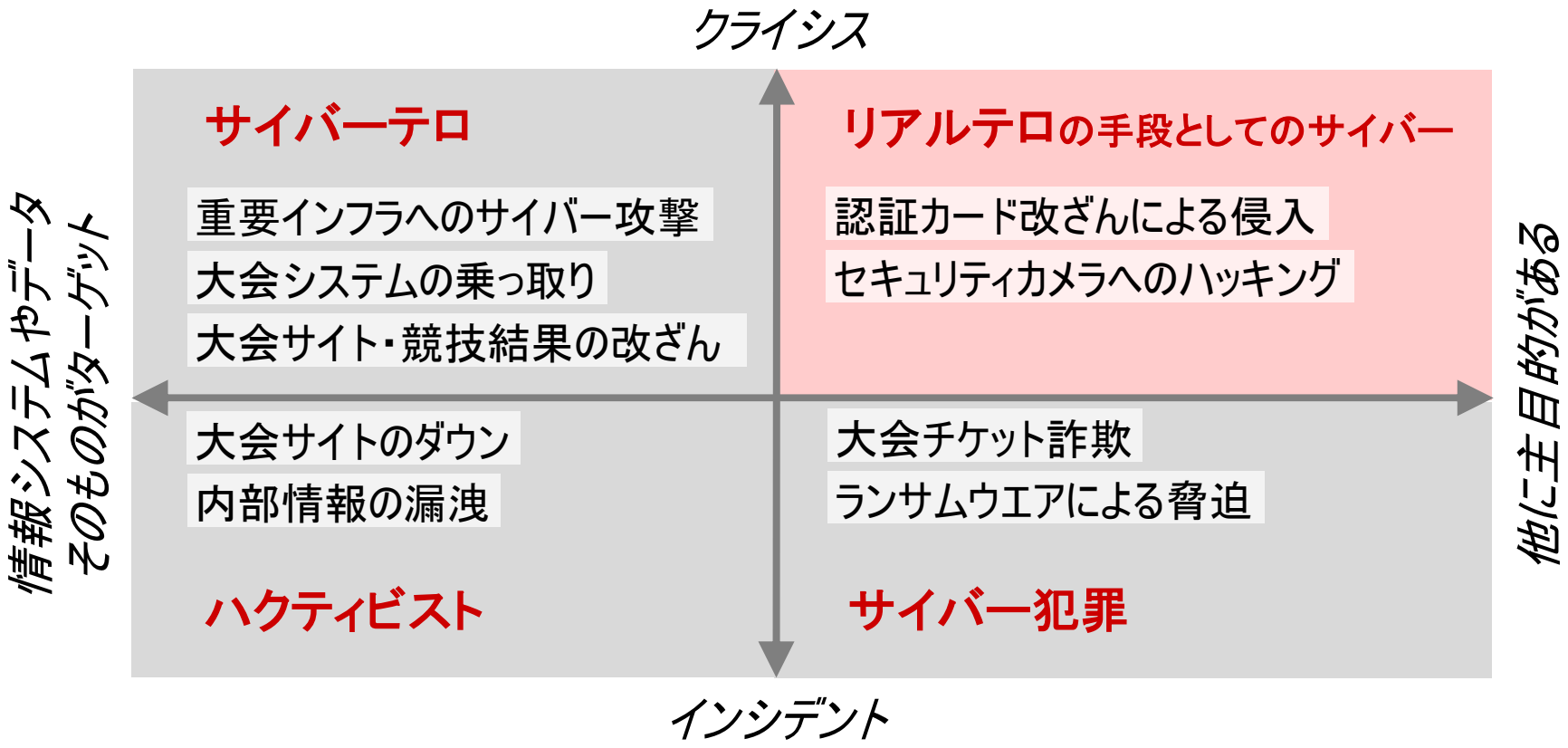
平昌2018大会のテクノロジーオペレーションセンター

実は現実空間で起きていることが、サイバー空間でも起きているだけ

- ✓ **ロンドン**：プロテスト集団による政治的主張、アラブ・イスラム武装勢力によるテロ
- ✓ **ソチ**：イスラム武装勢力、国内分離独立勢力などによるテロ
- ✓ **リオデジャネイロ**：麻薬組織、マフィアなどによる犯罪
- ✓ **平昌**：隣国との関係、ドーピング疑惑に関わる国家的関与
- ✓ **東京（予想）**：
  - ➢ 海外での模造品流通（偽サイト、偽チケットなど）
  - ➢ インバウンドのハクティビスト（過激な自然保護団体など）
  - ➢ インバウンドのテロリスト・犯罪者
  - ➢ ホームグローン・テロ

手段としてのサイバー

✓テロ・業務妨害の手段として、サイバー攻撃のコストパフォーマンスが非常に高いため、これまで想定する必要がなかったリスク要因となってきた。



ポイント３：組織全体の課題(1/2)

- ✓**もはや情報システム部門の所掌範囲を超えた課題であり、業務部門をまたがった関与が必要。**
  - **警備部門：リアルテロの手段としてのサイバーセキュリティ対策**
  - **総務部門：情報漏えい事故に際しての対外的説明責任／真に有効な情報セキュリティのガバナンスルール**
  - **調達部門：業務委託先の情報セキュリティ管理義務条項**
  - **法務部門：サイバー攻撃による事業損失に対する適切な免責条項**
  - **広報部門：ネット上の公開情報の適切な管理（デマ、詐欺情報などの監視）／レピュテーションモニタリング**
- ✓**社内で必要なのは、サイバーセキュリティ分野の専門家の育成ではなく、各業務における専門家にITやサイバーに関する知見、それに付随するリスクに関する知識、を身に着けさせること。そのためのモチベーションを持たせること。**

ポイント３：組織全体の課題(2/2)

- ✓ **組織として重要なのは、事業リスク全体の観点から、サイバーセキュリティ対策の優先順位や投資バランスを正しく判断できること。**
  - ➢ **『情報セキュリティ』vs.『事業継続性』／『レピュテーション対策』vs.『業務効率性』／『社員教育コスト』vs.『システム更改コスト』**
  - ➢ **得てして、見積もりが難しい項目（サイバーセキュリティリスク＆対策）は低く評価される傾向がある。**

ポイント４：守りと攻め
（攻撃者の目線）

リオ2016大会の近代五種競技

インシデントに関する考察(3)

- ✓ 実はサイバーセキュリティのインシデント以外にも、放送コメンテーター用システムなど主要システムでトラブルが多発。
- ✓ これらの課題、ITガバナンスの欠如、などは、サイバーセキュリティ面にも影響。
- ✓ 一方で、大会におけるITの活用は大会ごとにますます増加傾向。

アクション１（運営のスマート化）

準備 → 実行 → 後始末

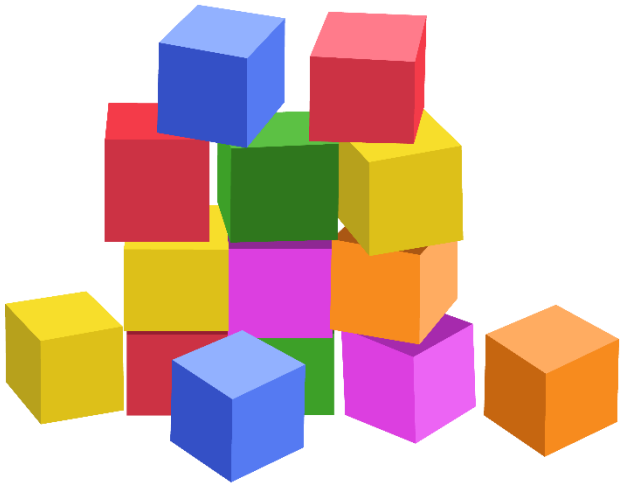
- ✓ 大量の物流・輸送をスマートにこなす
  - **水素エネルギーや再生可能エネルギーの活用**により、カーボン排出量を最小化する大会運営を実現する。
  - **大量の交通データ分析**に基づくきめ細かい渋滞予測、急な競技スケジュール変更などにも**迅速に対応できる**関係者車両の最適配置、などITを最大限活用して実現する。
- ✓ 現場ボランティアを支えるモバイル
  - **モバイルデバイスを活用し状況を見える化**することで、現場の最適判断と快適な業務環境を実現する。
- ✓ 観客の快適をサポートするＡＩ
  - **ロボット・多言語翻訳**によるフレンドリーな会場案内や競技解説、**チャットボット**による迅速な問い合わせ応答（コールセンターなどのオペレーションコストの削減）、トイレや売店の待ち時間予測など、**課題解決のためのAI活用**を実現する。
- ✓ 会場の警備をサポートするテクノロジー
  - **生体認証**を活用した迅速・安全な関係者の入退場管理、セキュリティカメラと画像処理技術による**混雑度モニタリング**、などにより警備員業務を効率化する。
- ✓ 大量の物品調達の後始末は？
  - 大会後の物品二次利用やオークション販売を支える、**リユース支援プラットフォーム**を活用する。

ポイント４：守りと攻め

- ✓守りのサイバーセキュリティ対策：穴を防ぐだけの仕事であれば、モチベーションが長続きしない、言い訳を考える状況に追い込まれる。
- ✓攻めのサイバーセキュリティ対策：情報システムを活用するからこそのサイバーセキュリティ。サイバーセキュリティを、もっとクリエーティブな仕事にするべき。
- ✓まずは経営層に、もっと情報システムについて攻めの正しい姿勢が欲しい。＝サイバーセキュリティにも意識の高い経営者
- ✓情報システムのトラブルの９０％以上は、サイバーセキュリティ以外。まずは情報システムとその設計・運用に関する理解を。

攻撃者目線の重要性

- ✓ 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困難に。
  - ➢ 「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探す」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、「組織をまたがって必要な情報にアクセスできる仕組み・権限をいかに持たせるか？」、「攻撃専門チームの知見をいかに安全に管理・継承するか？」



Free Download Web

最後に（リーダーの資質）

リオ2016大会の7人制ラグビー

現場のリーダーに求められる資質

- ✓ オリンピック・パラリンピックの準備・運営とは、すべてにおいてグローバルクラスのプロジェクト。
  - ➢ 関与する人材・組織／プロジェクト管理の方法論／指揮命令系統／狙ってくる団体（自然保護団体、ハッカーコミュニティなど）
- ✓ 現場のリーダーには、単にITセキュリティの専門家であるだけでなく、リーダーとしての資質や実戦経験が求められる。
  - ① **技術的スキル・経験**＝情報セキュリティ対策とサイバー犯罪対策（攻撃予兆分析、フォレンジック対策など）の両スキルを備える。
  - ② **リーダーシップ**＝大会時に発生するインシデントに対して迅速・的確な判断・決断ができる。
  - ③ **コミュニケーションカ・人脈**＝ハッカーコミュニティや海外主要機関のキーメンバーと顔が見える信頼関係を持つ。（英語力・コミュニケーション力も重要）

インシデントに関する考察(4)

✓ **本当の意味での連携のむずかしさ**

- 英語でのコミュニケーション、業務の進め方の閉鎖性、などにも起因して、組織をまたがった連携・コミュニケーションに課題がなかったか？
- 大会運営においてサイバーインシデントが発生した際には、『競技運営の継続』『重要な情報システムの復旧』こそが最優先であり、情報システム部門責任者の迅速・適切な判断と、それを支えるガバナンス体制が重要なはずだが。。。
- 組織をまたがったシステム監査、ログ情報の統合的な収集分析、事前合同演習の実施、などに課題がなかったか？
- 意識していても、**ついつい縦割り組織の弊害、互いの領域に踏み込まない妥協、などがまかり通っていないか？**

ご清聴ありがとうございました。

2016 Getty Images