リオ2016大会の振り返りと東京2020大会へ向けたサイバーセキュリティの取組み

平成29年7月19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

アジェンダ

1．オリンピックに関わるテクノロジー
2．オリンピックの情報システム
3．オリンピックのサイバーセキュリティ
4．なにをどう守るのか？
5．大会後のレガシーを目指して

１．オリンピックに関わるテクノロジー

2016 Getty Images

リオ2016大会のテクノロジー概観(1/2)

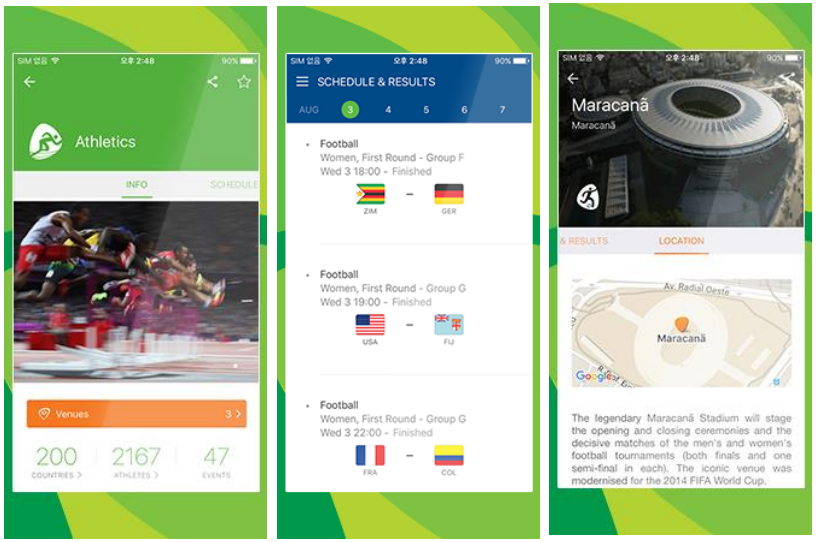
- ✓ ３６０度カメラ映像配信
  - OBS(Olympic Broadcast Service, IOCの下部組織)による試験導入。開会式や一部競技の映像を配信。
  - 海外の複数放送局ではVRゴーグルでの視聴にも対応。
- ✓ Olympic Channel
  - OBSが8月から始めた会員制の動画アーカイブサービス。
  - 大会期間中以外でも視聴できる環境を提供。（これまでは大会後1か月までしかネット上で視聴できなかった）

リオ2016大会の国際放送センター

(c) Tokyo 2020

リオ2016大会のテクノロジー概観(2/2)

- ✓ モバイルアプリ “Rio 2016 Mobile App”
  - ➢ Android/iPhone/Windows Phoneに対応。7か国語。
  - ➢ 大会前には聖火リレーのルートマップ・スケジュール、会場情報、関連動画など。大会期間中は競技スケジュール、競技結果、国別メダル数、選手情報、お気に入り競技の登録機能、関連写真など。
  - ➢ 大会毎にモバイルアプリが充実・進化。放送局が提供するアプリは動画も視聴。
- ✓ モバイルトラヒックの状況
  - ➢ 大会関係者（IOC関係者、スポンサーなど）によるモバイルデータ通信量は、ロンドン2012大会の4倍、2014FIFAワールドカップの10倍。



リオ2016大会のモバイルアプリケーション

https://www.rio2016.com/en/app

オリンピックのテクノロジーの変遷(1/2)

開催年　大会	大会運営の観点 （情報システム、運営体制など）	大会観戦の観点 （放送、デジタルメディアなど）
1948年　ロンドン大会		半径50マイルでのテレビ放送
1960年　ローマ大会		欧州18か国でオリンピック初めての生中継
1960年　スコーバレー冬季大会	**コンピュータ（パンチカード打ち込み）による競技結果データ処理**（選手や観客が競技中でも経過が分かるように）	
1964年　東京大会	**オンラインシステムによる競技結果の集計・配信**	初の衛星放送による中継
1968年　メキシコシティー大会	大規模な放送センター、プレスセンター	初のカラー放送、生のスローモーション映像
1988年　ソウル大会	計時機器精度が1/100秒から1/1000秒へ、 個別の情報システムを統合した**大会用統合情報システム**へ	

オリンピックのテクノロジーの変遷(2/2)

開催年　大会	大会運営の観点 （情報システム、運営体制など）	大会観戦の観点 （放送、デジタルメディアなど）
1996年　アトランタ大会		インターネット上で初のオリンピック公式サイト
2000年　シドニー大会		BSハイビジョンの試験放送、**スポーツプレゼンテーション**の導入
2008年　北京大会		全競技のハイビジョン放送
2010年　バンクーバー冬季大会		初のIP動画配信
2012年　ロンドン大会	**モバイルトラヒック対策**や**サイバーセキュリティ**が課題として顕在化	スマートフォン、SNSの普及（テレビ観戦だけでない視聴スタイルの普及）
2016年　リオデジャネイロ大会	**クラウドベースの情報システム**へ移行	360度カメラ映像の試験導入、会員向け映像アーカイブサービス開始（Olympic Channel）
2018年　平昌冬季大会	完全クラウドベースの情報システムへ移行	5G試験導入？VR試験導入？

スポーツ・プレゼンテーションとは

- ✓ シドニー2000大会から導入されたコンセプトで、スポーツ競技を劇場型のショーとして扱う考え方です。
- ✓ ファンやアスリートにとっての興奮や参加感を重視することで、ショーとしてのスポーツイベントの魅力を高めることを狙っています。
- ✓ 具体的にスポーツ・プレゼンテーションを構成する基本要素としては、**音楽、ビデオボード、映像・音声、照明、特殊効果、進行係、アナウンサー、スポンサー広告、競技の儀礼・作法、（開催地の）文化演出**など。

課題：東京2020大会では、最新テクノロジーを使ってスポーツ・プレゼンテーションを進化させられないか？

2016 Getty Images

スポーツテクノロジーの動向予測

【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

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
   - 競技進行中に競技データをリアルタイム処理して活用・表示
2. ソーシャルネットワークの標準化
   - 多様なSNSがオープンに連携する環境へ
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…

スポーツテクノロジーの背景にあるもの

＊アドバンスド・スタッツ＝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

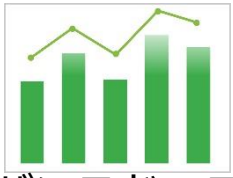
無線データ伝送

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

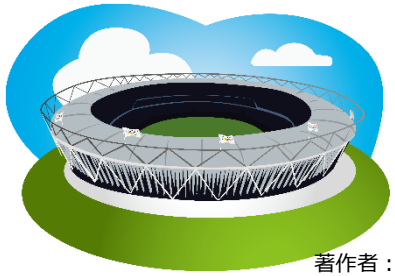
著作者：Vector Open Stock

著作者：Micah Lawrence

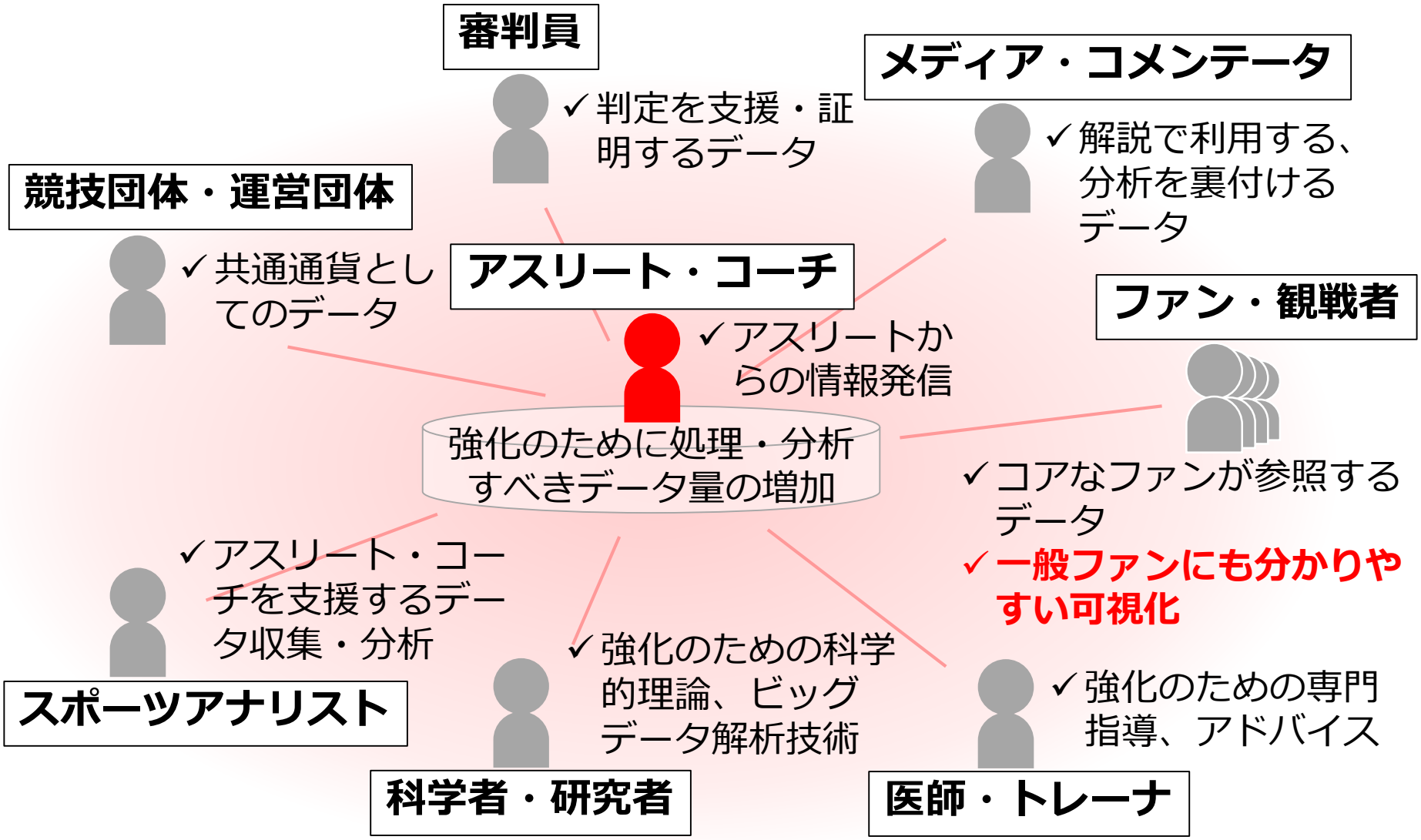
著作者：freedesignfile.com

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

スポーツ版ビッグデータをめぐるエコシステム



2020年に向けたスポーツプレゼンテーション

- ✓ アスリートやコーチが、勝つために何を考え、何を工夫するか？これを理解することが、すなわち観戦者・視聴者にとってのゲームの面白さです。
- ✓ スポーツの新しい見方・見せ方（エンターテイメント性）を追求すると、つねにアスリート自身の視点が根底にあります。
  - ➢ アスリートのパフォーマンスや戦略性を、いかに分かりやすく可視化できるかが、テクノロジーの役割。
  - ➢ さらに、可視化するために**クリエータのセンス**が問われている。

より強くなる・早くなる工夫　　**本人も気づいていなかった能力**

まだ誰もやっていない技　　**競技中になにを考えているか**

著作者：Vector Fantasy

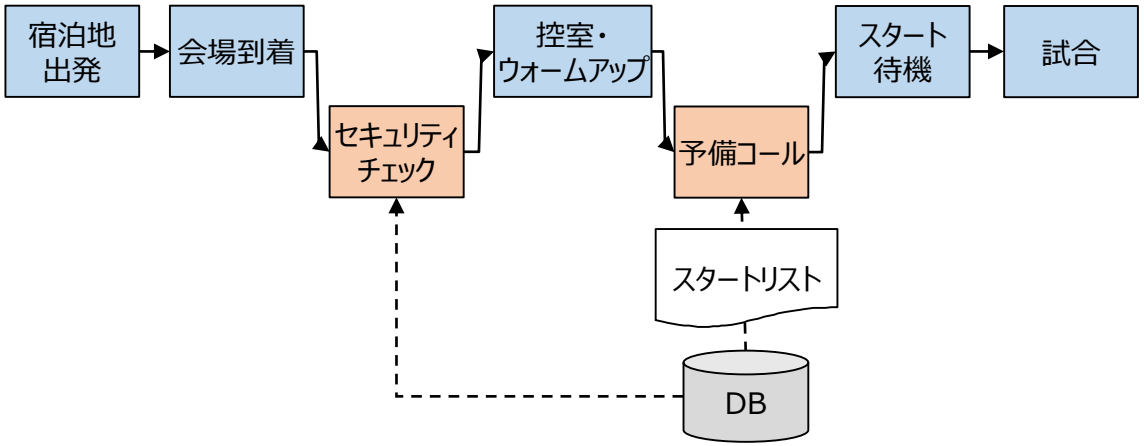
著作者：Vector Open Stock

著作者：Micah Lawrence

著作者：Micah Lawrence

著作者：freedesignfile.com

2．オリンピックの情報システム



大会運営業務とは？

✓ 組織委員会が携わる大会運営業務は、大きく４つの分野に分かれます。

1. イベントオペレーション

- モノ：調達、物流、食料･飲料供給、清掃など
- ヒト：出入国管理、スタッフの輸送・移動、宿泊管理、VIP警護、観客誘導、入場管理、サイネージなど

2. スポーツオペレーション

- 競技運営、メディカルサービス、ドーピングコントロール、選手の輸送・移動、放送・メディアオペレーションなど

3. ファシリティオペレーション

- 会場整備、会場運営、選手村管理、電力供給、通信インフラ提供、会場フェンスなど

4. ビジネスオペレーション

- チケット販売管理、ライセンス商品販売管理、ビジネス開発、収支管理など

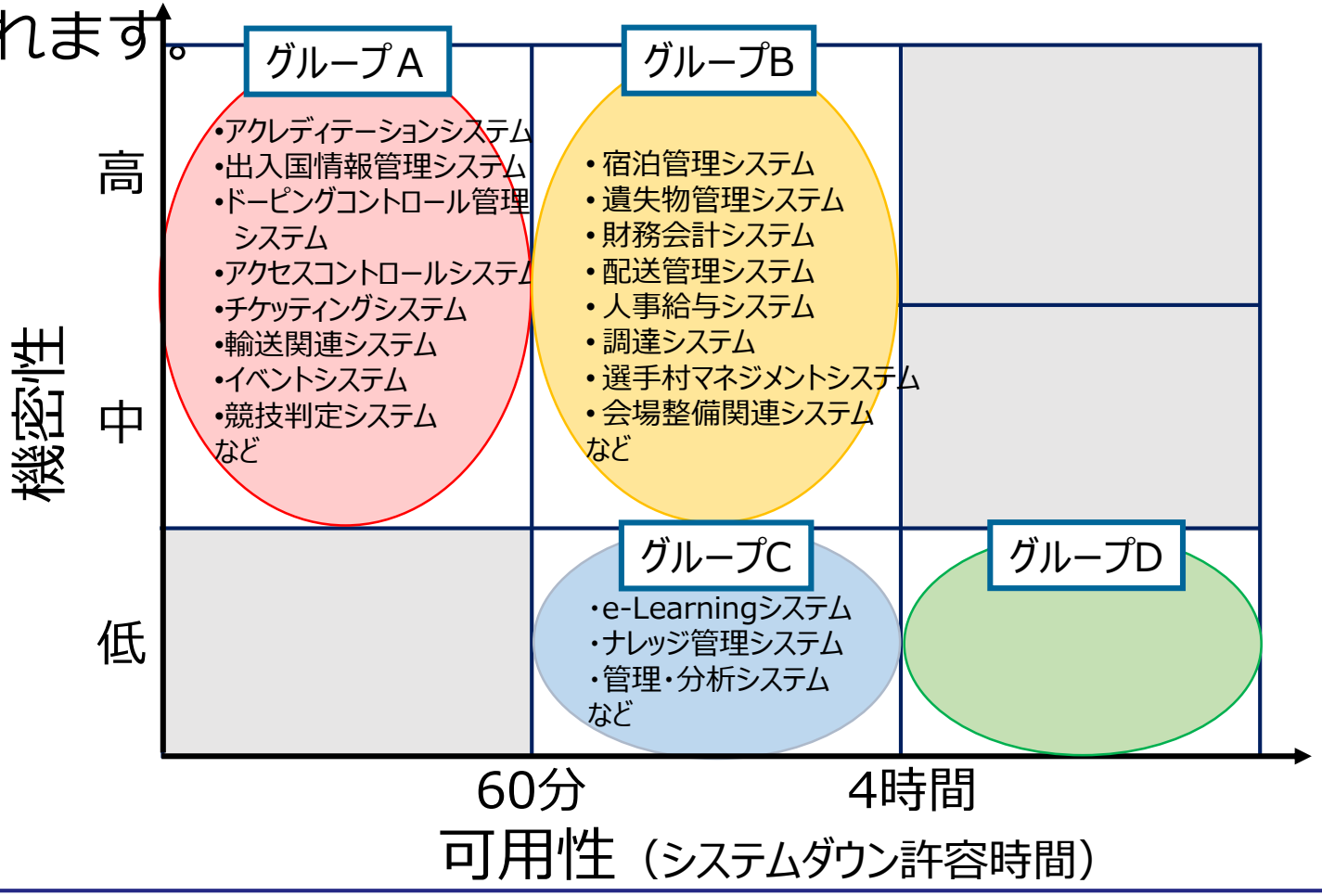
大会運営業務を支えるシステム

✓ 運営業務を支える数十もの情報システムを設計・構築していく必要があります。

カテゴリー	おもなシステムと関連するオペレーション
1．イベントオペレーション	• 輸送管理システム、宿泊管理システム、受発注管理システム、アクレディテーションシステムなど • セレモニー用システム、放送・プレス用機材など
2．スポーツオペレーション	• 競技計測機器、審判判定ツール、競技ボランティア管理システム、会場のA&V機器など • ドーピング検体管理システムなど
3．ファシリティオペレーション	• LAN・WAN・インターネット・ • 電力供給、予備電源 • ビル管理システム、CAD図面管理
4．ビジネスオペレーション	• ECサイト、チケット販売管理システム、CRMなど • 偽サイト監視、レピュテーションモニタリングなど

システムの非機能要件によるカテゴリー

- ✓ 「システムの可用性」「扱うデータの機密性」をもとに、設計ポリシーとして、いくつかのカテゴリーに分かれます。



エンタープライズアーキテクチャの遷移

- ✓ プロジェクトのフェーズごとに業務が複雑化し、全体設計が徐々に遷移します。

構成要素	事前プロジェクト (2014-2016) →	準備プロジェクト (2016-2019) →	テストイベント＆大会 (2019-2020)
業務	連絡、スケジュール共有 ドキュメント作成 電話・会議など	財務会計、人事管理、 調達管理、広報、物販、 プロジェクト管理など	関係者向けサービス、 競技計測、食事提供、 観客誘導、警備など
データ（情報）	周知事項 ワークショップ資料 企画書・計画書など	予算、人事情報、 会場図面、スケジュール、 プレスリリース資料など	個人情報（関係者、観客）、 輸送・宿泊、競技結果、 運営スケジュール、 ドーピング検査結果など
アプリケーション	Eメール、スケジューラ ファイル共有 TV会議など	バックオフィスシステム、 プロジェクト管理ツール、 CADシステム、 Webサイト・ECサイトなど	大会運営アプリケーション、 競技計測システム、 メディア向け情報配信、 関係者認証システムなど
テクノロジー（インフラ）	ファイルサーバ SaaS・クラウドサービス インターネット回線など	データセンター プライベートクラウド Webホスティングなど	WAN、TOC、SOC BC/DR対策 放送回線、CDNなど

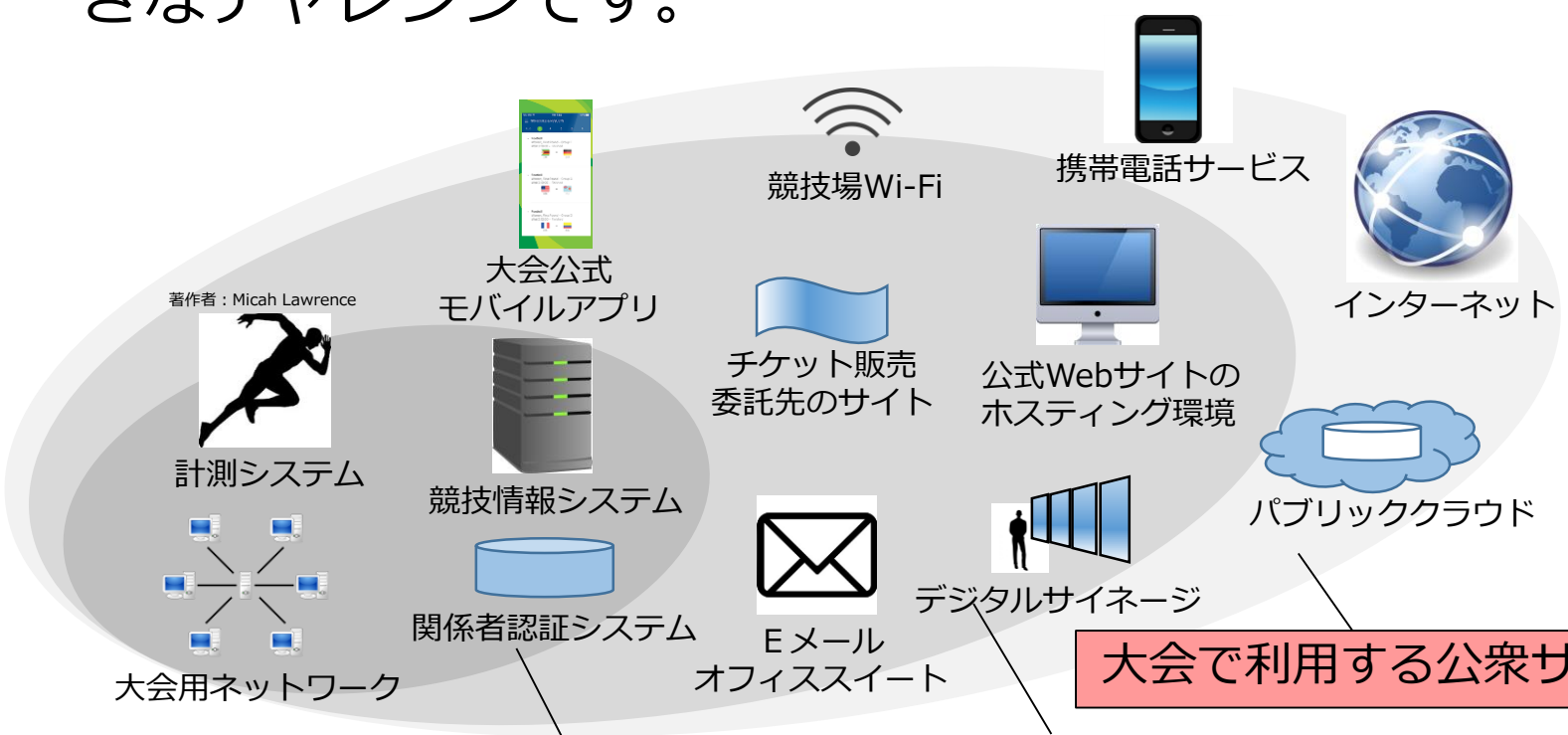
ITセキュリティ・アーキテクチャの遷移

- ✓ それに従い、必要とされるＩＴセキュリティ対策（非機能要件）も、徐々に高度化します。

	事前プロジェクト (2014-2016)	→ 準備プロジェクト (2016-2019)	→ テストイベント＆大会 (2019-2020)
主要なITセキュリティ対策	FW、VLAN、インターネットVPNなど	ファイル暗号化、端末認証、多要素認証、シングルサインオン、UTM、プロキシ、WAFなど	SIEM、ユーザ振舞い監視、スレットインテリジェンス収集、フォレンジック、BC/DR、CDNなど
対策の考え方	**境界防御 Peripheral Protection** 境界線で外敵の侵入を防ぎ、組織内部を守る。	**エンドポイント End Point Security** 境界線の内外を問わず、職員が扱う情報や端末（エンドポイント）そのものを守る。	**多層防衛 Defense in Depth** 「特効薬はない」という前提に立ち、多様な対策を何重にも施す。一旦侵入を許しても、被害の拡大を防げる。

最近の大会を支えるテクノロジー

✓大会運営を支えるシステム・ネットワークは、ますます多岐にわたり、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が大きなチャレンジです。



3．オリンピックのサイバーセキュリティ

ブラジル陸軍のサイバー部隊（CDCiber）

http://www.brasil.gov.br/defesa-e-seguranca/2015/09/forcas-armadas-vao-monitorar-redes-de-internet-na-rio-2016/ciber.jpg/view

ロンドン2012大会で観測されたサイバー攻撃

“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

リオ2016大会で観測されたサイバー攻撃

“大会開始前からネット上ではサイバー攻撃の呼びかけが見られた。”

- オリンピック期間中に4千万回のセキュリティ脅威を観測、2千3百万回の攻撃をブロック、大規模なDDoS攻撃は223回。（Cisco Systems）
- 開会式が始まる前から、大会Webサイトなどにピークで540Gbpsという最大規模のDDoS攻撃。(Arbor Networks)

“大会WebサイトはCDNで守られ被害（サイトダウン）はなし。一方で組織委員会内では、Bot感染による情報（暗号化ファイル）の漏えいが発生。周辺環境にも多くの被害が発生。”

- リオ大会に関わる公共事業を請け負った建設会社のWebサイトから個人情報漏えい。
- 期間中に要人（リオ州知事、市長、スポーツ大臣など）の個人情報漏えい。

“2014年のFIFAワールドカップ開催後あたりから、ラテンアメリカ圏においてブラジルのサイバー犯罪件数が突出[1)]。”

- 2014年に確認されたATMのスキミングデバイスの改良版が、今回も大会開催場所周辺で確認。
- POSレジがマルウエア感染し、観光客のクレジットカード情報が流出。
- 大会前からチケット販売偽サイト、大会関連フィッシングサイト、偽ホットスポットなどが多数乱立。

1) デジタル・フォレンジック研究会　第４２９号コラム「2016年リオ・オリンピックに関連したサイバー攻撃の発生状況と対処体制」
名和 利男 理事（株式会社サイバーディフェンス研究所、専務理事/上級分析官）　https://digitalforensic.jp/2016/09/12/column429/

大会で想定されるサイバーセキュリティのリスク

必ず顕在化するリスク

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も依存
	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

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
- ✓ **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

東京2020大会で想定される環境の変化

✓ 「サイバーセキュリティ」は、大会準備においても最も予測が難しい要素の一つになりつつあります。

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*

社会全体のますますのIT化

- *モバイル端末やSNSの進化・普及による、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*

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、ひとつの組織・機関に閉じてできる対策には限界が*

大会に特有な要件の考慮(1/3)

1. 同時多発攻撃・複合的攻撃

- ✓ 注目度が高い大会であるため、複数拠点・複数システムを対象とした同時多発サイバー攻撃を想定するべきです。
- ✓ 自然災害（台風、集中豪雨など）が発生しやすい時期でもあり、災害発生に意図的に合わせたサイバー攻撃も想定するべきです。（気象観測システム、河川監視システムへの攻撃など）

大会に特有な要件の考慮(2/3)

2. ITのさらなる活用環境

- ✓ スマホを介した各種情報提供（各種サービス連携の仕組み）や動画視聴、CRMを活用したチケット販売促進（売れ残りチケット再販、空席販売）、混雑状況の予測と観客の誘導（群衆管理システム）など、大会周辺ではこれまで以上のIT活用が検討・計画されています。
- ✓ 上記に伴い、各種サービス連携や顧客情報連携など、システム間連携が多様化することに伴うインシデントの広域化、複雑化も想定されるべきです。

大会に特有な要件の考慮(3/3)

3. グローバルなオペレーション

- ✓ 大会運営スタッフの多くは海外から来日する外国人（TOPスポンサー、国際競技団体、放送局、IOC･IPCなど）であり、さらに一部のコアシステムは海外のデータセンターにホスティングされます。
- ✓ これまで以上に、グローバルな環境での情報共有や迅速な対応が必要です。（英語によるインシデント情報共有、海外インテリジェンス機関との連携など）

４．なにをどう守るのか？

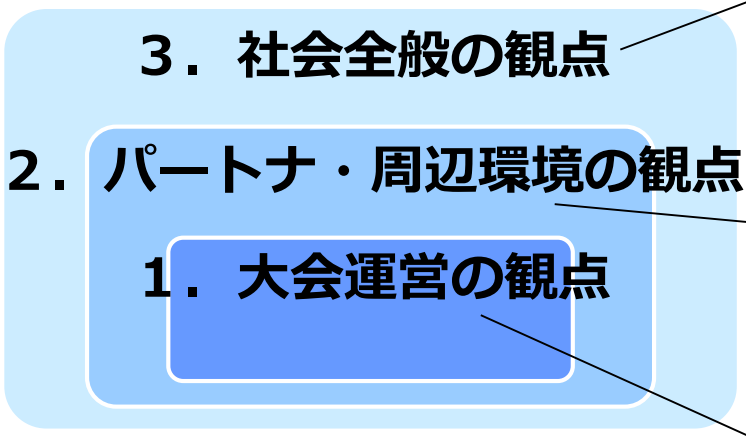
リオ組織委員会のテクノロジー・オペレーション・センター

(c) Tokyo 2020

オリンピックでは、なにを守るべきなのか？

- ✓ 大会用システム・ネットワークだけを守っても、大会運営を守ることにはなりません。
- ✓ 周辺の社会インフラやレピュテーションも含めて、総合的に守る観点が必要です。

想定リスクの全体像



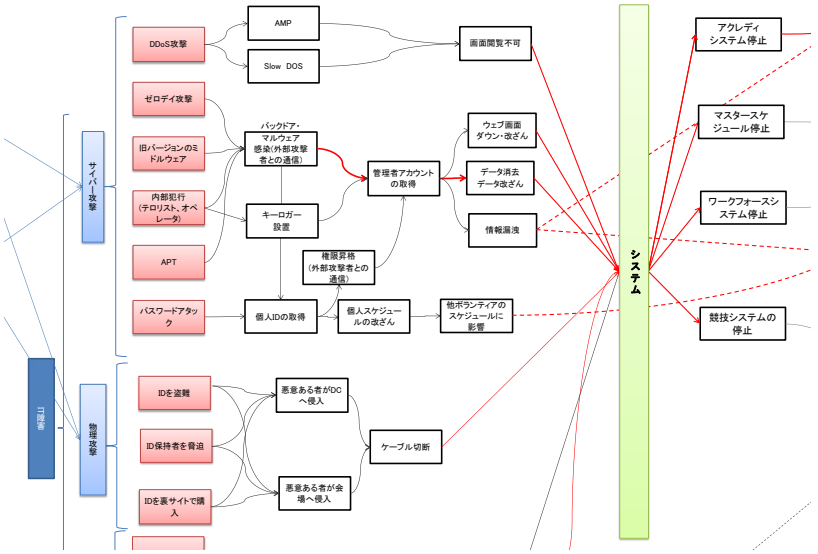
間接的に大会に影響するリスク
（自然災害／会場外で発生するテロ・サイバーテロ／SNS上での日本・東京に対する評価・評判など）

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／偽チケット販売サイト／重要インフラの障害など）

組織委員会側で管理すべきリスク
（大会システムへのハッキング／内部情報漏えいなど）

リスクの全体像（リスク・アーキテクチャ）

- ✓ リスク・アーキテクチャ＝東京2020大会の運営において想定されるさまざまな脅威シナリオをもとに、リスク要因を分析し、その全体像を捕らえようとするもの。
  - ➢ 英国ではもともと政府で行っていたリスク評価のフレームワークを改良して適用（OSSSRA(Olympic Safety and Security Strategic Risk Assessment)）。
  - ➢ 米国ではSuper Bowlなど大規模スポーツイベントの際に、2年前に25の委員会を立上げ、官民連携して統合的リスク管理を開始。（9.11以降の動き）
  - ➢ 組織委員会もスポンサー企業と連携して、ISO22320（社会セキュリティ緊急事態管理）にもとづく分析方法を導入中。

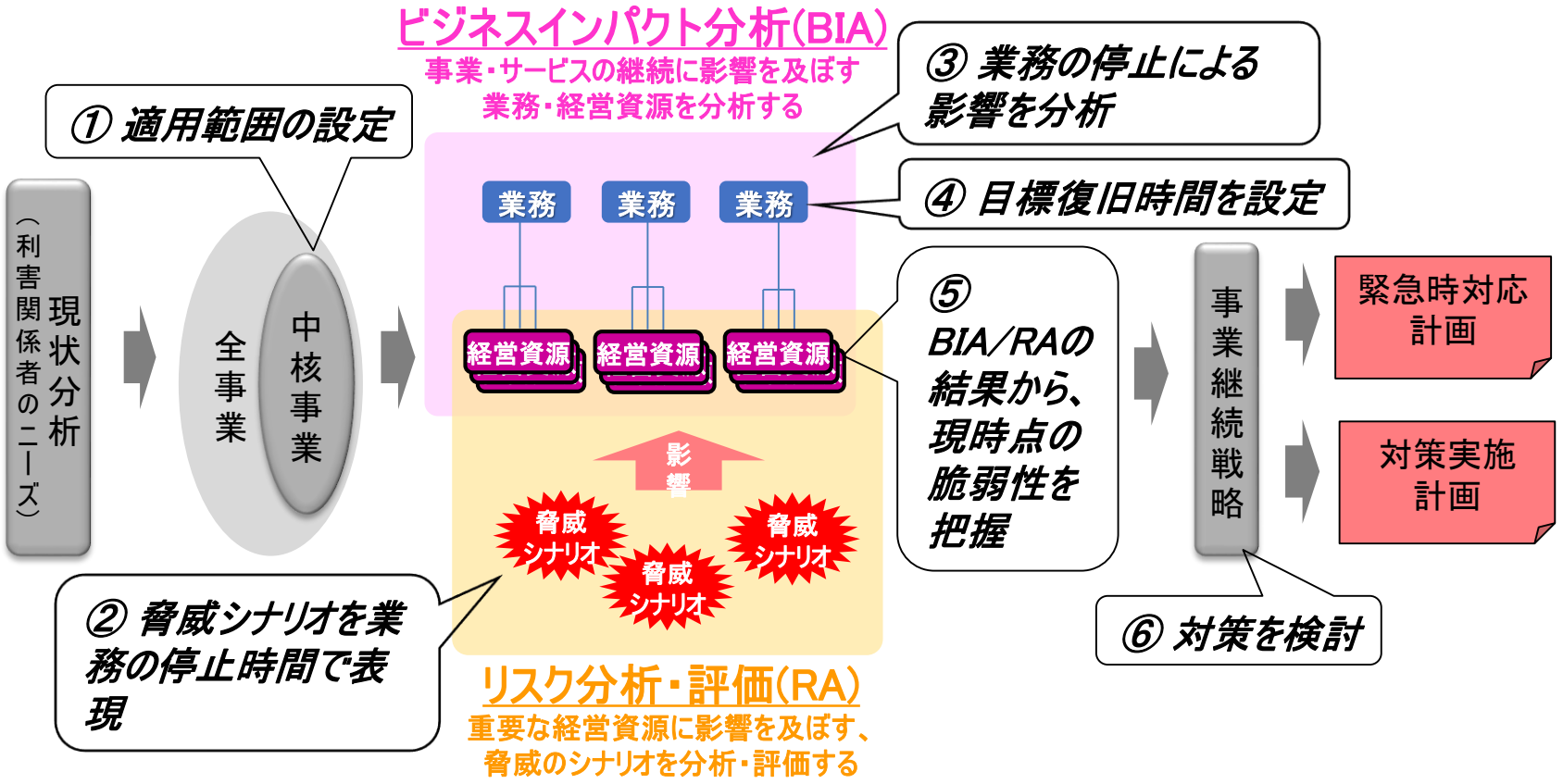


(c) Tokyo 2020

TOKYO 2020

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。



リスクマネジメント活動のフェーズ

- ✓ フェーズ１　内部活動（2014年～）
  - **体制整備：**FA(Functional Area)をまたがるリスク洗出しプロジェクト
  - **計画・実行：**リスクレジスタ／重要システム洗出し／定期的なシステム残存リスク評価／PDCA
  - **ガバナンス：**セキュリティポリシー・ガイドライン／委託契約への反映
- ✓ フェーズ２　関係機関との調整（2017年より本格化）
  - **体制整備：**パートナー・サプライヤー／アウトソーシング事業者／クラウドサービス事業者／重要インフラ事業者／競技場オーナー／開催都市・自治体
  - **情報共有：**大会運営計画／輸送計画／警備計画／システム運用計画／トラブル・インシデント情報／災害・防災情報
- ✓ フェーズ３　第三者チェック・監査・合同演習訓練（2018～2019年より本格化）
  - **監査：**ルール化・プロセス定義
  - **演習訓練：**シナリオ作成／合同演習

組織委員会におけるITセキュリティ対策の基本的考え方

✓ 組織委員会のリスクマネジメント方針

1.大会を予定通りに開催する。／2.大会を安全に運営し、完遂する。／3.大会のすべての関係者の満足を得る。アスリート・ファーストの視点を持ちつつ、観客・スポンサーなどの関係者の快適さを損なわない。／4.組織委員会の社会的信頼性を保持する。／5.大会を適切な財政計画で運営する。

✓ 上記方針を受けて、ITセキュリティ対策の検討にあたっては、以下の考え方に基づいています。

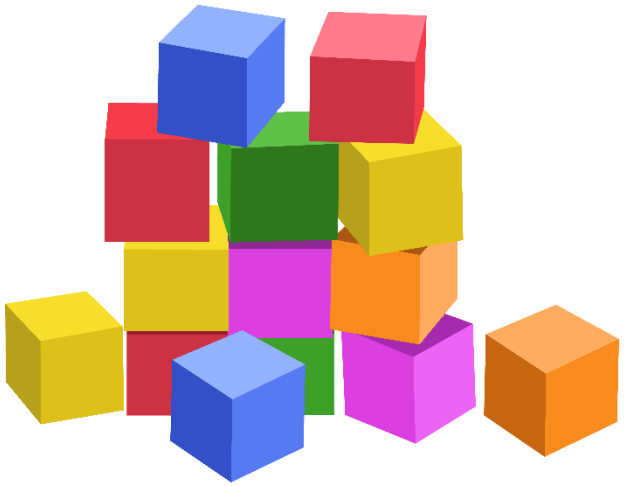
- **大会運営に影響を与えうるITセキュリティ上の脅威を排除**する対策とする。
- 職員の急激な増加にも耐えうる**柔軟性・拡張性**を備えた対策とする。
- リモートオフィス環境などもカバーする、**より包括的な対策**とする。
- 情報システムユーザ（関係者）の**業務にできる限り影響を与えない**対策とする。
- ITサービス停止や機密情報漏えい・改ざんなどによる**レピュテーション低下を回避**する対策とする。
- 安定運用・コスト効率化の観点から、対策を導入する**技術基盤をできるだけ統一**する。

５．大会後のレガシーを目指して

2016 Getty Images

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難しくなってきています。
  - ➢ 「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

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、クリエータでした。
- ✓ 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でしょうか。

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)

東京2020大会のレガシーに向けて

✓ 東京2020大会におけるサイバーセキュリティのレガシーはどうあるべきでしょうか。

【守りの観点】

- 社会インフラのＩｏＴ化が進むことで、システムの複雑性・サイバーリスクの不透明性がますます増える。
- なにか“きっかけ”がなければ、便利さを享受するだけで、総合的・横断的にセキュリティを見直すことはほとんどない。

【攻めの観点】

- 一方で、“ITの活用度”と“サイバーセキュリティの成熟度”との間には相関関係（あるべきバランス）がある。
- セキュリティを単なるコストとみるのではなく、ＩＴ活用に必要なプロセスとみるべき。

(c) Tokyo 2020

ご清聴ありがとうございました。

2016 Getty Images