東京2020オリンピック・パラリンピック競技大会における NTTの貢献

～ 通信サービス with サイバーセキュリティの観点から ～

NTTは通信サービスを提供する東京2020ゴールドパートナー

https://www.ntt.co.jp/news2015/1501/150126a.html

NTT

ENGLISH

NTTグループ内検索

文字表示 小 中 大

NTTグループについて

NTT（持株会社）について

▶ニュースリリース ▶各社へのご案内 ▶商品・サービス ▶社会環境活動・災害対策 ▶会社案内 ▶株主・投資家情報 ▶研究開発 ▶採用のご案内

NTT HOME > NTT持株会社ニュースリリース > 2015年 > 東京2020オリンピック・パラリンピック競技大会 ゴールドパートナー（第1号）に決定

NTT持株会社
ニュースリリース

▸最新ニュースリリース

▸バックナンバー

▸English is Here

NTT持株会社
ニュースリリース内検索

1997 年 04 月～

2021 年 10 月

NTT持株会社ニュースリリース

2015年1月26日

東京2020オリンピック・パラリンピック競技大会 ゴールドパートナー（第1号）に決定

日本電信電話株式会社（本社：東京都千代田区、代表取締役社長：鵜浦博夫、以下NTT）は、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（以下東京2020）との間で、2020年に開催される東京2020オリンピック・パラリンピック競技大会を含む6年間に及ぶオリンピック日本代表・パラリンピック日本代表に関するパートナー契約を締結し、国内最高位のスポンサーシッププログラムであるゴールドパートナーの第1号に決定いたしました。

契約の対象となるサービス・グループ会社は、以下の通りです。

主なサービス

- 通信サービス

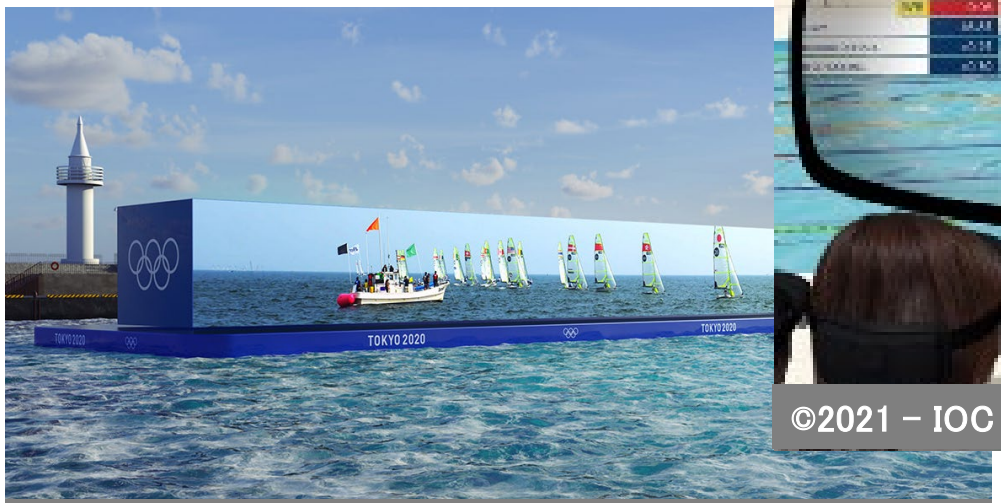
NTTが提供したもの・・・
東京2020大会の安定運営を支えた通信サービス

- 放送用ネットワーク
  光ケーブル 1,900km、専用線 10,000km
- 大会用データネットワーク
  会場LAN：光ケーブル1,200km、メタルケーブル3,900km
- CATVセットトップボックス6,800台
- Wi-Fi 11,000アクセスポイント
- 携帯電話19,600台、固定電話2,800台
- 総勢約1万人のNTT関係者（協力会社含む）が大会を支えた

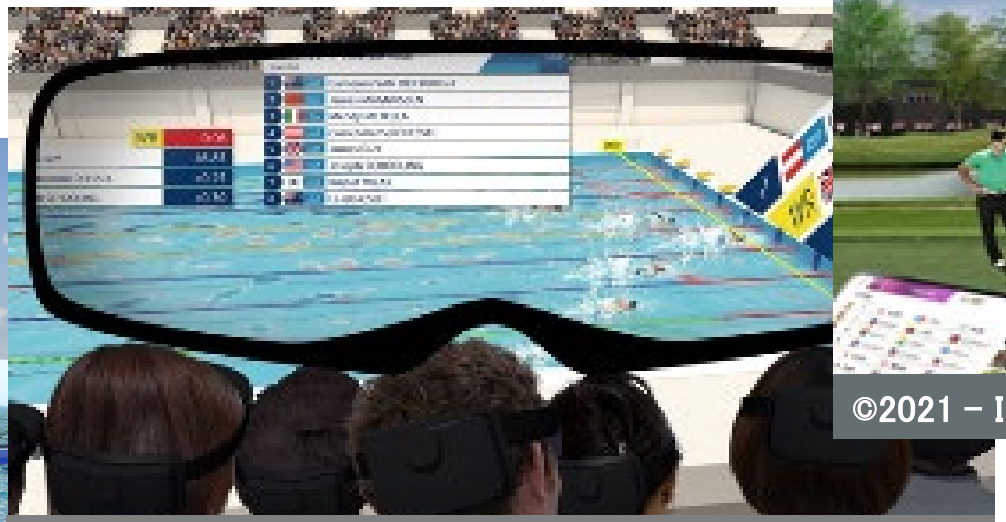
  ①大会期間中、会場で従事したNTT社員：約650人
  ②テクノロジーオペレーションセンタで従事したNTT社員：約350人
  ③セキュリティーオペレーションセンタで従事したNTT社員：約90人

Figures provided by TOCOG

NTTが提供したもの …
史上最高にイノベーティブな東京2020オリンピック
様々な新しい観戦体験へNTTの研究所技術や5Gで協力



5G x “Kirari!” ultra-realistic communication technology (Competitive Sailing)



5G X AR (Swimming)

Personalized Multi-angle Viewing (Golf)

サイバー攻撃から守る

- サイバー攻撃の傾向 1) ランサムウェア攻撃
  - 人手による攻撃
  - 二重の脅迫 （データ復旧、搾取データの勝手公開、それぞれへの身代金要求）
  - サプライチェーン攻撃や、サービス停止攻撃との、ミックス戦略
- サイバー攻撃の傾向 2) サプライチェーン攻撃
  - ICTサービス事業者への攻撃によるより広範な影響
  - 特定国からの攻撃?
- サイバー攻撃の傾向　3) 重要インフラストラクチャへの攻撃
  - IT（情報技術）のみならず、OT（運用技術）への攻撃
  - 暗号資産による身代金要求 （マネーロンダリングの容易さ）

成功の秘訣は「4つのT」

NTTは通信サービスにおけるネットワークセキュリティや
様々なサイバーセキュリティ対応を実施

T1: Threat Intelligence & Monitoring
（脅威情報とモニタリング）

T2: Total Security Solutions
（総合的セキュリティソリューション）

T3: Talent, Mind & Formation
（人材、心持、フォーメーション）

T4: Team 2020 – 複雑なステイクホルダーマネジメント

過去1年での、さらなる予想しなかったチャレンジ

- 開催の1年遅れ
  - サイバー脅威環境の変化
  - 再作業
  - 定まらない実施形態
- コロナ禍の影響
  - 多くが無観客開催となり、通信サービスがこれまでの大会で一番重要となった大会
  - 医療体制の護持
  - 偽サイト/フィッシングサイト

サイバーセキュリティの成功とは?

アスリートの成功：　卓越したパフォーマンス

メディアの成功：　注目を浴びる記事と写真

放送事業者の成功：スムーズな伝送

私たちのサイバーセキュリティの成功：
To Keep Calm and Carry On
（平静を保ち、普段通りに）

成功の結果　ーいくつかの事実とともにー

- **東京2020オリンピック・パラリンピック競技大会の進行に影響を与えるようなサイバー攻撃に至った事態は、皆無であった。**

  - *大会中、遮断したサイバーセキュリティ攻撃（未確認通信含む）は、約4億5,000万回*
  - *大会中、脆弱性を狙ったと思われる未確認通信は観察されたが、遮断を持って対処*

Figures provided by TOCOG

“A real success story from a cybersecurity perspective”

- “The Best Kind of Defense”
  （最高の種類の防護）
- “Having the Right People in Place”
  （いるべき人がいるべき場所に）
- “Going on the Offensive”
  （攻めて守る）
- “Intelligence-Driven Defense”
  （インテリジェンス主導型防護）


SECURITY MAGAZINE NEWS COLUMNS MANAGEMENT PHYSICAL CYBER SECTORS EXCLU

The Tokyo Olympics are a cybersecurity success story

August 17, 2021

Dr. Brian Gant

KEYWORDS cyber security /

In the months and weeks leading up to the Tokyo Olympics, intelligence agencies and cybersecurity experts warned of the risks of cyberattacks and the need to exercise preventative measures to prevent the kinds of incidents we have seen in the previous Olympics at Rio de Janeiro, Sochi, Pyeongchang

“The Tokyo Olympics are a cybersecurity success story”, written by Dr. Brian Gant
https://www.securitymagazine.com/articles/95880-the-tokyo-olympics-are-a-cybersecurity-success-story

成功の秘訣は「4つのT」
T1: Threat Intelligence & Monitoring
（脅威情報とモニタリング）

●平昌2018オリンピック・パラリンピック冬季競技大会からの学び
- マルウェア：　LAN/Wi-Fi/ブロードバンドサービスに影響
- 運営情報の窃取：　ID、パスワード、個人情報
- APT攻撃

・・・　クラウド・ネイティブの時代、そしてゼロ・トラストの環境下において、「危機管理」の必要性が、東京2020大会に向けて高まる　・・・

内外からの脅威情報およびモニタリング
―「日々の健康チェック」―

- 内側から
  - NDR (Network Detection & Response)
  - EDR (Endpoint Detection & Response)
  - UEBA (User & Entity Behavior Analytics)
- 外側から
  - NTT-CERT (集中的な公開情報モニタリング)
  - その他のパートナ等

- サイバーに加え、物理的なモニタリングの実施
  - 通信ケーブル、回線ルート、論理構成
  - 通信機器、およびそのソフトウェア
  - パスワード変更状況

成功の秘訣は「4つのT」

T2: Total Security Solutions

（総合的セキュリティソリューション）

ICT環境の複雑さに対応し、ホワイトリスト（可能な通信プロトコルのみを列挙）形式による、「サイバー衛生（Cyber Hygiene)環境」を維持

- ID (個人認証：多要素認証の活用含む)
- 通信トラヒック経時変化への対処、開会前短期での入念な会場設備確認
- 複数事業者製品の活用による防護 (多層防御の実現)
- 自社用意端末、関係者持ち込み端末の双方への対処
- R&D成果の活用 （改ざんを検知する真贋判定技術　等）

NTTグループの総合的セキュリティソリューション

- Wide Angle MSS – マネージド・セキュリティ・サービス
  - NTTのグローバルな脅威情報プラットフォームによって共有されたデータ、そしてハニーポット（わざとサイバー攻撃されやすいように仕掛けたコンピュータ等）の大規模ネットワーク
  - 散在するアクティビティの断片を組み合わせ、複合パターンに対処した分析エンジン
- 東京2020大会向けセキュリティ・オペレーション・センタ (SOC)ソリューション
  - 自動化、ルール策定、権限移譲
  - 東京2020組織委員会ならびにNTTの既存セキュリティオペレーションセンタとの緊密な連携
  - 高いスキルを持つ専門家による総合的分析（東京2020大会へのチューニング）

成功の秘訣は「4つのT」
T3: Talent, Mind & Formation
（人材、心持、フォーメーション）

- 予防保全意識を持ったチーム・メンバーの育成・定着
- 不通状態を回避するための状況監視の徹底
- 常にリアルタイムで情報を共有し、ネットワークのあらゆる側面への悪影響を防護
- 手順の標準化
- サッカーでいう「ボランチ」：関連する複数カテゴリーの潜在的問題を調査/分析する人材の重要性

トレーニング

- SOCオペレータ研修プログラム（100名以上が受講)
  - NTTコミュニケーションズの研修子会社において、2週間の短期集中トレーニングを実施 (センタ運営、脆弱性／マルウェア分析等）ー期間中は受講者間のチームワークも醸成
  - 受講後は、プロのセキュリティ技術者とチームを組み、オペレータの能力をサポート・向上。またNTTのセキュリティ子会社による実践訓練を実施

- “レッドチーム”（疑似攻撃による脆弱性発見チーム）は、ICTサービス事業者、他の重要インフラストラクチャ関係者、そして公的機関等と関係を持ちながら、「攻めのセキュリティ」を実現
  - 何が起こるか、どう対処するかを繰り返し検証
  - 優先度の低い項目排除などを通じた、正確なデータ学習により、セキュリティ機器の性能を維持

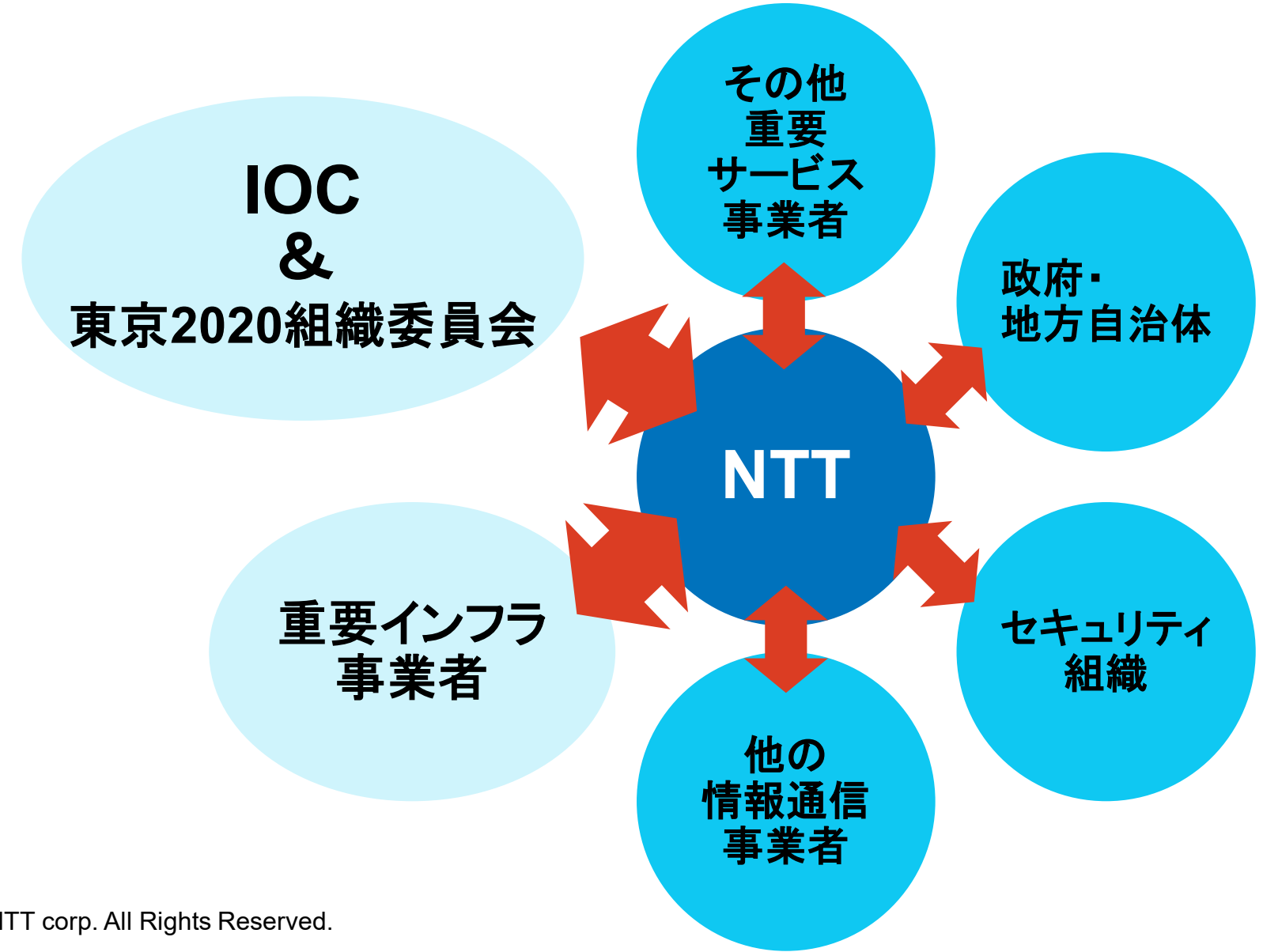
2022年以降に向けて

200人以上の熟練したメンバー（SOCオペレーター、レッドチームメンバを含む）が、グループ会社（NTT東日本/西日本/コミュニケーションズ/ドコモ）での新たなサイバーセキュリティミッションを開始

- NTTグループ内基幹システムのセキュリティ水準の維持・向上
- 顧客サービスのセキュリティ水準の維持・向上
- 顧客内部セキュリティ水準の維持・向上

成功の秘訣は「4つのT」

T4: Team 2020 – 複雑なステイクホルダーマネジメント



ICTサービス事業者ならびに重要インフラ関連機関とのコラボレーション

- ICTサービス事業者
  - ICT-ISAC Japan -ICT主要事業者のセキュリティ情報連絡-
  - 日本インターネットプロバイダー協会 / グローバルTier1（世界のトップレベルのインターネットプロバイダー各社）
  - 関係放送事業者
  - 関係ITサービス事業者、セキュリティサービス事業者
- 重要インフラ関連機関
  - 内閣サイバーセキュリティセンター
    - サイバーセキュリティ演習（リモートワーク環境下含む）、リスクアセスメント、サイバーセキュリティ協議会
  - 総務省
  - 日本シーサート協議会会員各社

公的機関とのコラボレーション

- 警察庁、警視庁、防衛省
- JPCERTコーディネーションセンター、FIRST (Forum of Incident Response and Security Teams)、CTA (Cyber Threat Alliance)
- 地方自治体（東京都ほか）

そして….

IOC/東京2020組織委員会
すべての種類の協力（リスクシナリオ分析、サイバー・ウォー・ゲーム　含む）