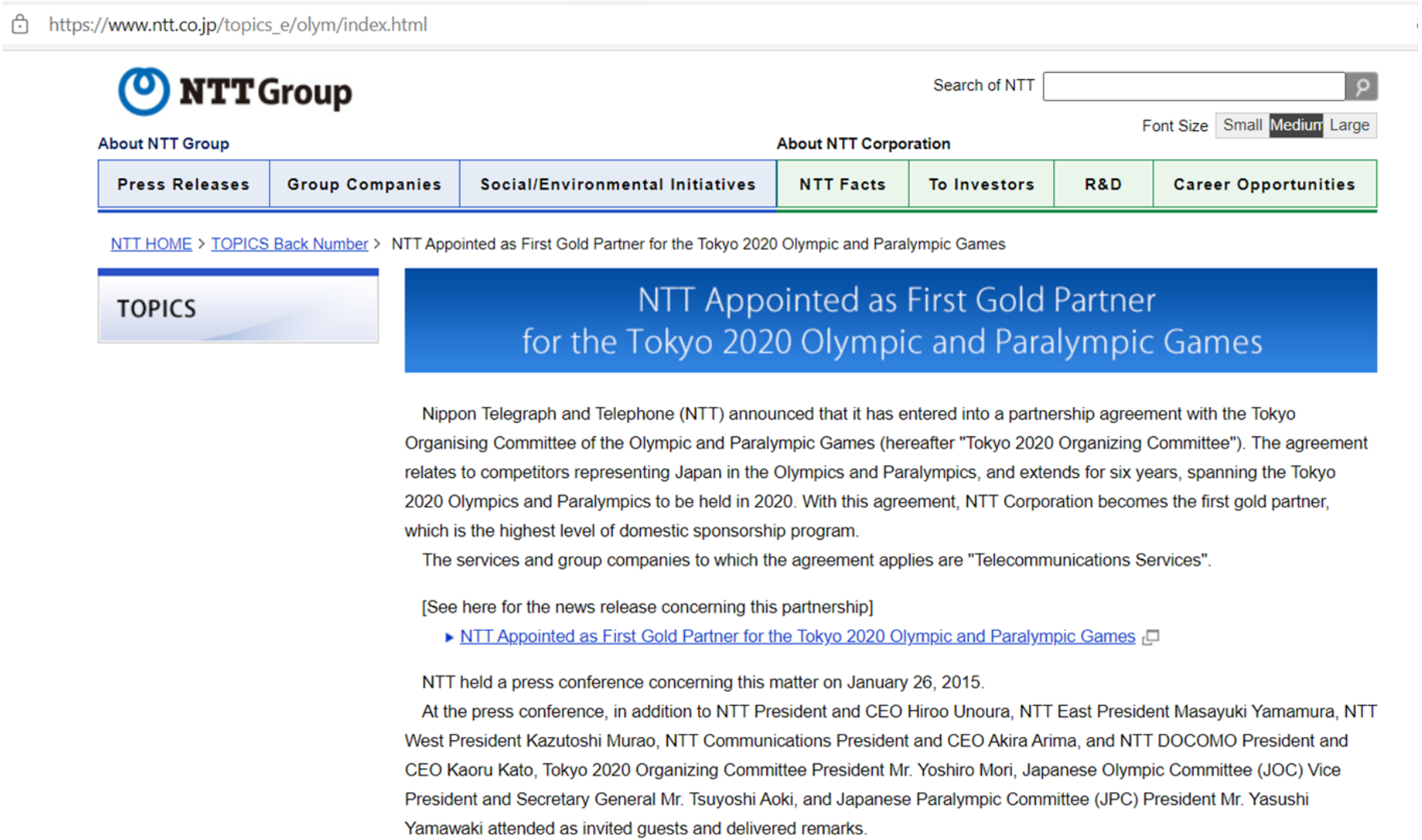
NTT's Contribution to the Olympic and Paralympic Games Tokyo 2020

- From the perspectives of Telecommunication Services with Cybersecurity -

Shinichi Yokohama
SVP of Security & Trust Office, CISO
NTT Corporation

TOKYO 2020
TOKYO 2020 PARALYMPIC GAMES
Tokyo 2020 Gold Partner
(Telecommunications Services)

NTT is a Tokyo 2020 Gold Partner (Telecommunications Services)



https://www.ntt.co.jp/topics_e/olym/index.html

NTT Group

Search of NTT

Font Size Small Medium Large

About NTT Group | About NTT Corporation

Press Releases | Group Companies | Social/Environmental Initiatives | NTT Facts | To Investors | R&D | Career Opportunities

NTT HOME > TOPICS Back Number > NTT Appointed as First Gold Partner for the Tokyo 2020 Olympic and Paralympic Games

TOPICS

NTT Appointed as First Gold Partner for the Tokyo 2020 Olympic and Paralympic Games

Nippon Telegraph and Telephone (NTT) announced that it has entered into a partnership agreement with the Tokyo Organising Committee of the Olympic and Paralympic Games (hereafter "Tokyo 2020 Organizing Committee"). The agreement relates to competitors representing Japan in the Olympics and Paralympics, and extends for six years, spanning the Tokyo 2020 Olympics and Paralympics to be held in 2020. With this agreement, NTT Corporation becomes the first gold partner, which is the highest level of domestic sponsorship program.

The services and group companies to which the agreement applies are "Telecommunications Services".

[See here for the news release concerning this partnership]

▸ NTT Appointed as First Gold Partner for the Tokyo 2020 Olympic and Paralympic Games

NTT held a press conference concerning this matter on January 26, 2015.

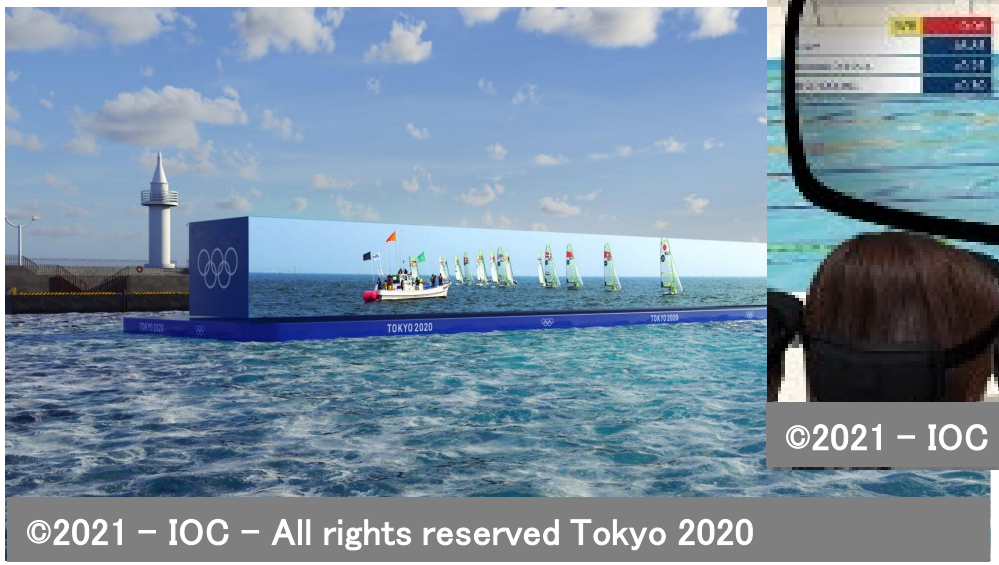
At the press conference, in addition to NTT President and CEO Hiroo Unoura, NTT East President Masayuki Yamamura, NTT West President Kazutoshi Murao, NTT Communications President and CEO Akira Arima, and NTT DOCOMO President and CEO Kaoru Kato, Tokyo 2020 Organizing Committee President Mr. Yoshiro Mori, Japanese Olympic Committee (JOC) Vice President and Secretary General Mr. Tsuyoshi Aoki, and Japanese Paralympic Committee (JPC) President Mr. Yasushi Yamawaki attended as invited guests and delivered remarks.

NTT Provided … Telecommunication services supporting the stable operation of the Games

- Broadcasting Circuit for the Games
  - Fiber Optic Cable 1,900km & Leased Line Circuits 10,000km
- Data Networks for the Games
  - Fiber Optic Cable 1,200km & Metal Cable 3,900km
- 6,800 CATV Set Top Boxes
- 11,000 Wi-Fi Access Points
- 19,600 Cell Phones & 2,800 Fixed-Line Telephones
- 10,000 personnel from NTT (including partner companies) supported the Games:
  - Including 650 at the venue during the Games, 350 at the Technology Operations Center, and 90 at the Security Operations Center

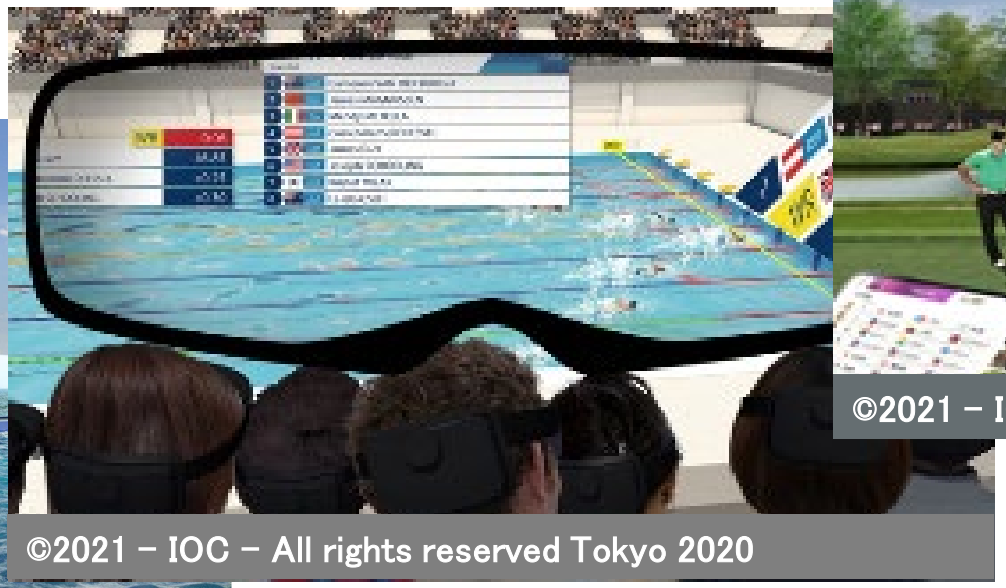
Figures provided by TOCOG

NTT Provided … the most innovative Olympic Games Tokyo 2020, with a variety of new spectator experiences through NTT R&D and 5G



©2021 – IOC – All rights reserved Tokyo 2020

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



©2021 – IOC – All rights reserved Tokyo 2020

5G X AR (Swimming)

©2021 – IOC – All rights reserved Tokyo 2020

Personalized Multi-angle Viewing (Golf)

Protection from Cyber Attacks

- Trend 1) Ransomware Attacks
  - Human-Operated Ransomware Attacks
  - Double Extortion
  - Mixed strategy with Supply Chain Attacks & Service Disruption Attacks
- Trend 2) Supply Chain Attack– SolarWinds and Exchange
  - Attacks on ICT Service Providers
  - Nation-State Attacks?
- Trend 3) Service Disruption in CII – Colonial and JBS
  - Attacks on both IT & OT resulting in service disruption
  - Paid using Cryptocurrency – easy for money laundering

Our Key Success Factors are “4T”

NTT has implemented network security for telecommunication services and various cyber security measures.

T1: Threat Intelligence & Monitoring

T2: Total Security Solutions

T3: Talent, Mind & Formation

T4: Team 2020 – Complex Stakeholders Management

Additional Unexpected Challenges in the past year

- Delayed by one year
- Change in cyber threat environment
- Some engineering re-work
- Implementation styles not easily fixed

- Covid-19
- Many games without spectators made the telecommunication services the most important part of the Games ever
- Protecting the medical system
- Fake & Phishing websites

What is our success?

Athletes' success : Supreme performance

Media's success : Eye-catching photos and reports

Broadcast's success : Smooth transmission

Our Cybersecurity's Success :
To Keep Calm and Carry On

The Results of our Success: Some Facts

- **There were NO situations resulting in cyber attacks that affected the operation of the Olympic and Paralympic Games Tokyo 2020.**

  - *The total number of security events that were blocked during the Games, including unauthorized communications to the official website, was 450 million.*
  - *During the Games, unauthorized communications targeting vulnerabilities in terminals were observed, but we responded by blocking the communications.*

Figures provided by TOCOG

“A real success story from a cybersecurity perspective”

- “The Best Kind of Defense”
- “Having the Right People in Place”
- “Going on the Offensive”
- “Intelligence-Driven Defense”

SECURITY MAGAZINE NEWS COLUMNS MANAGEMENT PHYSICAL CYBER SECTORS EXCLL

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

Our Key Success Factors are “4T”
T1: Threat Intelligence & Monitoring

- What we learned from PyeongChang 2018 Olympic and Paralympic Winter Games…
  - Malware
    - Affected LAN/Wi-Fi/Broadcasting services
  - Theft of operational information
    - ID, Password, Personal Information
  - APT Attacks

・・・ Heightened need for “Crisis Management” for the cloud-native era and a zero-trust environment ahead of the 2020 Games・・・

Threat Intelligence & Monitoring from Inside / Outside - “Daily Health Check” -

- Inside
  - NDR (Network Detection & Response)
  - EDR (Endpoint Detection & Response)
  - UEBA (User & Entity Behavior Analytics)
- Outside
  - NTT-CERT (intensive public monitoring)
  - Other Partners & Providers

- Cyber & Physical Convergence Monitoring
  - Cable, NW Route & Logical Topology
  - Hardware with Software
  - Password change status

Our Key Success Factors are “4T”

T2: Total Security Solutions

- Adapting to the complexity of the ICT environment to maintain a “Cyber Hygiene” environment using a whitelist method (listing only possible communication protocols).
  - ID (with Multi-Factor Authentication)
  - Traffic Volatility over time
  - Careful confirmation of venue facilities in a short period of time before the opening
  - Multi-vendor protection (for Defense in Depth)
  - Our Managed devices / BYOD …
  - Application of R&D results (e.g., “Authenticity and Integrity Monitoring Technology“ to detect tampering)

Total Security Solutions from NTT Group

- Wide Angle MSS – NTT's managed security service
  - Large network of honeypots and the data shared using the NTT Global Threat Intelligence Platform
  - Analysis engine to combine scattered activity fragments, and suppress or support the composite pattern

- Diligent SOC (Security Operation Center) Solutions
  - Automation, Rule Making & Local Empowerment
  - Close Collaboration among TOCOG-TOC/SOC, NTT-TOC & NTT-SOC/CERT
  - Comprehensive analysis by high-skilled professionals of the various kind of data flows, with special tuning for Tokyo 2020

Our Key Success Factors are “4T”

T3: Talent, Mind & Formation

- Fostering & Establishing “Preventive-Maintenance” Minded Teams & Members
- Thorough situation monitoring to avoid downtime
- Constant real-time information sharing to protect every aspect of networks from further negative impacts
- Standardization of procedures
- ‘Volante’ personnel who can investigate/analyze potential problems in multiple related categories.

Training

- Training program for SOC operators（more than 100 participants）
  - Using the training subsidiary of NTT Communications to provide a 2-week intensive training course (CSIRT, vulnerabilities and Malware analysis), with network building among participants
  - Team up with professional security engineers, who can support and enhance operators' capabilities. NTT's security subsidiary also conducted practical training.

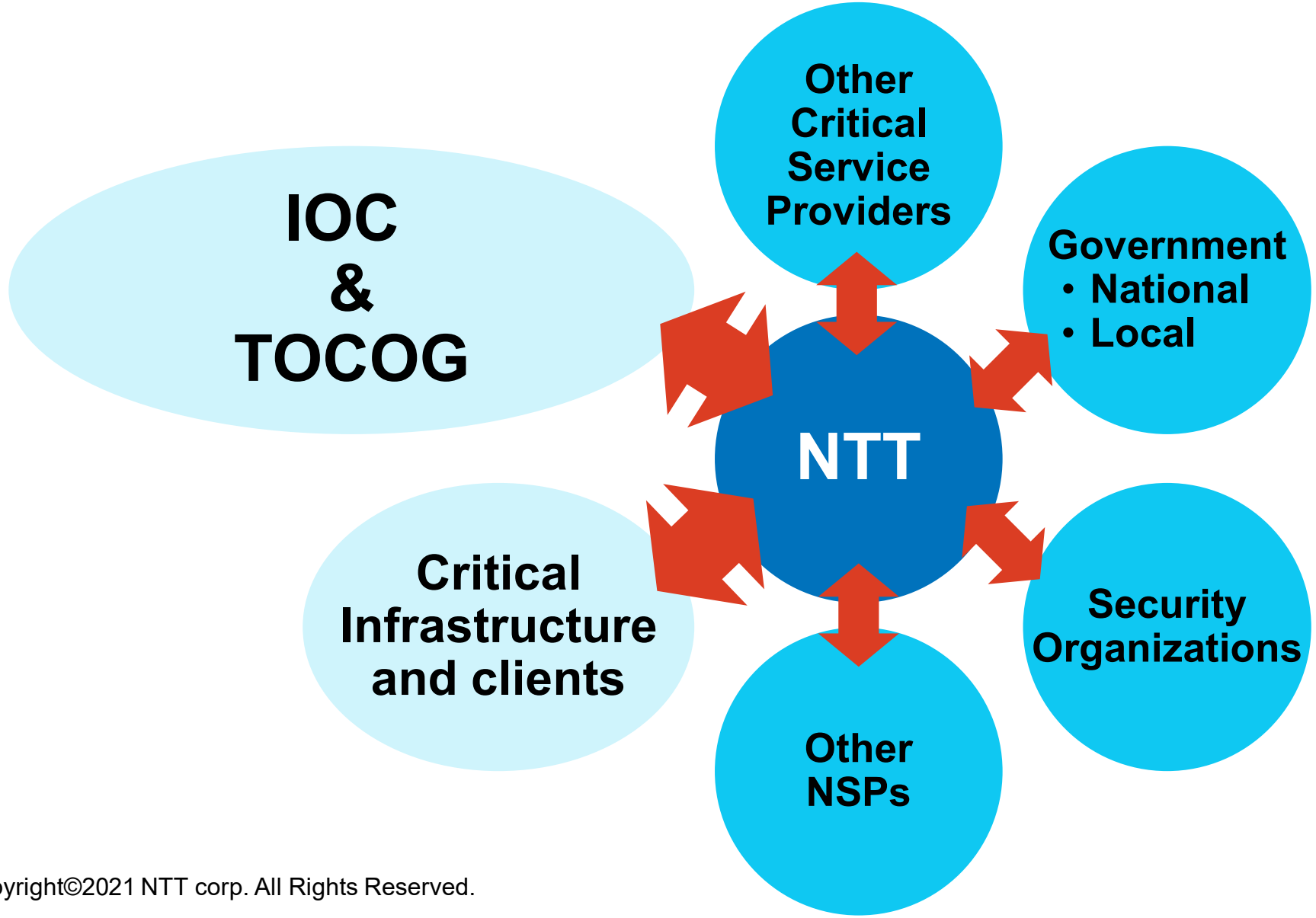
- "Red Team" has close relationships with ICT service providers, other CII, and public bodies in order to achieve "Offensive Security"
  - Repeatedly examine what may happen and how to deal with it.
  - Maintain performance of security devices through accurate data learning (by eliminating low priority items)

Towards 2022 and beyond

- More than 200 skilled members (incl. SOC operators & Red Team members) start new cyber security missions at Group companies. (East/West/Communications/DOCOMO)
  - Maintain and improve the security level of NTT Group's internal core systems
  - Maintain and improve the security level of customer service
  - Maintain and improve the internal security levels of the customers

Our Key Success Factors are “4T”

T4: Team 2020 - Complex Stakeholder Management



Collaboration with ICT Service Providers & CII

- ICT Service Providers
  - ICT-ISAC Japan — As ALL Japan ICT service providers —
  - JAIPA / Global Tier1 IP Network Providers
  - Broadcasting Service Providers
  - IT & Security Service Providers

- Critical Information Infrastructure
  - NISC
    - Exercises (incl. under remote work) & Risk Assessments
    - Cyber Security Council
  - MIC
  - Nippon CSIRT Association members

Collaboration with Public Bodies

- NPA, MPD, MOD
- JPCERT/CC, FIRST (Forum of Incident Response and Security Teams), & CTA (Cyber Threat Alliance)
- Local Governments

And....

- **IOC/TOCOG**
  - **All kind of cooperation incl. Risk Scenario Analysis, Cyber Wargames**

Thank you.
ありがとうございます。