Success stories of Japan's cybersecurity
日本のサイバーセキュリティの先進的取り組み

ISIC Japan webinar: July 26, 2022

Mihoko Matsubara 松原実穂子

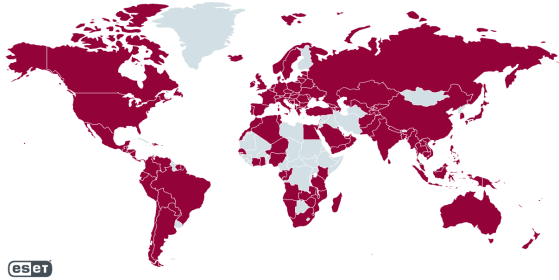
Chief Cybersecurity Strategist, NTT Corporation

日本電信電話株式会社　チーフ・サイバーセキュリティ・ストラテジスト

TrickBot takedown TrickBotのテイクダウンへの寄与

- TrickBot
  - Banking data & account credential theft
  - Election interference attempts → Prevented interference to the 2020 U.S. Presidential election
  - Threats to hospitals
  - Infected over one million devices since 2016
- In October 2020, global companies collaborated and cut off key TrickBot infrastructure
  - **NTT**, Microsoft, Lumen, Symantec, etc.

- TrickBotとは
  - オンラインバンキングのアカウント情報窃取
  - 選挙介入に悪用の恐れ → 2020年の米大統領選挙への介入を防止
  - 病院のネットワークに感染
  - 2016年以降、100万台以上に感染
- 2020年10月、グローバル企業が協力し、TrickBotの主要インフラを遮断
  - **NTT**、マイクロソフト、ルーメン、シマンテック等



https://www.eset.com/int/about/newsroom/press-releases/research/eset-takes-part-in-global-operation-to-disrupt-trickbot-a-botnet-that-has-infected-over-a-million-c/

Tokyo 2020 success story 東京2020の成功

- Unprecedented challenges
  - COVID-19 pandemic
- Advantages
  - 2019 G20 Osaka Summit
  - 2019 Rugby World Cup
- Tokyo 2020
  - No disruption by **450 million cyberattacks, twice as many as ones on London 2012,** to the operations during the games
  - Dr. Brian Gant's Security Magazine article**: "Success story," "Best kind of defense"**

- 未曾有の困難の数々
  - 新型コロナウイルス
- 利点
  - 2019年G20大阪サミット
  - 2019年ラグビーワールドカップ
- 東京2020
  - **ロンドン五輪の受けた攻撃の2倍の4.5億回**ものサイバー攻撃、大会運営に支障をきたすような被害を防止
  - 米メリービル大学のブライアン・ガント助教の「セキュリティ・マガジン」寄稿記事：**「成功事例」「最善の防御」**

Dr. Brian Gant, "The Tokyo Olympics are a cybersecurity success story," Security Magazine, August 17, 2021, https://www.securitymagazine.com/articles/95880-the-tokyo-olympics-are-a-cybersecurity-success-story

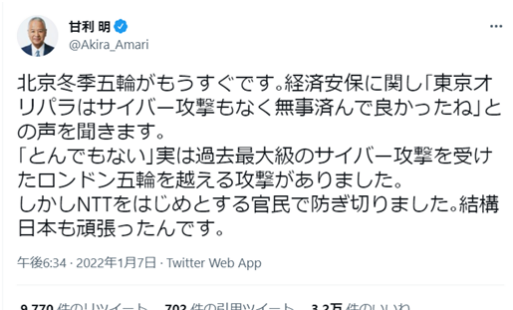
Lessons learned from Tokyo 2020

- **Four T's** to minimize potential damages
  - **T**hreat intelligence & Monitoring
  - **T**otal security solutions
  - **T**alent, Mind & Formation
  - **T**eam 2020
- Japan can protect global events
  - Early detection & response
  - Defense-in-depth

NTT's press release dated October 21, 2021
English: https://group.ntt/en/newsrelease/2021/10/21/211021a.html
日本語版：https://group.ntt/jp/newsrelease/2021/10/21/211021a.html

東京2020の教訓とは

- 被害を最小化するための**4つのT**
  - 脅威情報とモニタリング
  - 総合的セキュリティソリューション
  - 人材、心持、フォーメーション
  - ステイクホルダーマネジメント
- 日本は国際的なイベントを守ることができる
  - 早期検知・対応
  - 多層防御



https://twitter.com/akira_amari/status/1479385880544813059

Japanese Cross-Sector Forum 1/2
産業横断サイバーセキュリティ人材育成検討会

■ Launched in 2015

- 44 critical infrastructure companies across sectors

■ Goals

- Define what cybersecurity professionals and their required missions and skillsets are, based on the NIST Cybersecurity Framework
- Create an ecosystem to educate, hire, train, and retain cybersecurity professionals in collaboration with academia and government

■ 2015年に設立

- 日本の主要重要インフラ企業44社加盟

■ 目標

- NIST（米国立標準技術研究所）サイバーセキュリティ・フレームワークに基づき、サイバーセキュリティ人材とは何か、それぞれの種類の人材に求められる任務とスキルを定義
- 官民学で連携し、人材の教育、雇用、研修、維持のエコシステムを作る

Cross-Sector Forum website: https://cyber-risk.or.jp/
産業横断サイバーセキュリティ人材検討会（現在、「産業横断サイバーセキュリティ検討会」）

Japanese Cross-Sector Forum 2/2
産業横断サイバーセキュリティ人材育成検討会

NTT

■ Activities

- Involved in policy-making processes
- Sponsoring university courses
- NIST cybersecurity conferences

■ 活動

- 政策作りへの寄与
- 大学の寄付講座
- NIST主催のサイバーセキュリティ会議

https://www.nist.gov/node/1332326/japanese-cross-sector-forum/

Cynthia Brumfield, "Why NIST is so popular in Japan," CyberScoop, November 8, 2018, https://www.cyberscoop.com/nist-japan-workforce/

NPA's attribution of a cyber espionage attempt
サイバースパイの試みの実行犯について警察庁が発表

- In April 2021, NPA Commissioner-General Mitsuhiro Matsumoto's press conference = **Japan's first standalone public attribution**
  - Tick highly likely conducted cyberattacks on 200 Japanese organizations
  - Unit 61419 under the PLA Strategic Support Force in Qingdao, Shandong Province, was highly likely involved in the cyber espionage attempt
  - Japan's attribution efforts reportedly attracted a lot of attention from the **foreign intelligence community**

- 2021年4月、警察庁の松本長官の定例記者会見での発表 = **初めての日本単独の攻撃元特定・公表**
  - サイバー攻撃集団「Tick」が 約200の日本の組織への一連のサイバー攻撃を実行した可能性が高い
  - 中国人民解放軍戦略支援部隊ネットワークシステム部第61419部隊が関与している可能性が高い
  - **海外の情報機関、治安機関からの照会**が相次いだとの報道

https://www.asahi.com/articles/ASP4Q5WXZP4QUTIL012.html

2021 Locked Shields cyber exercise
2021年のロックド・シールズ演習

- NATO Cooperative Cyber Defence Centre of Excellence's annual exercise since 2010
- More than 2,000 people from 30 countries in April 2021
  - **Japan + USA**
    - MOD/SDF, NISC, IPA, JPCERT/CC, critical infrastructure companies
    - **Indo-Pacific Command**
- Scenario
  - Critical infrastructure
    - Water supplies, finance, mobile network
  - Disinformation champaigns
  - Legal and policy teams

- 2010年以降毎年開催されている NATOサイバー防衛協力センター主催の 年次サイバー演習
- 2021年4月開催の演習には30カ国から 2000人以上参加
  - **日本・米国チーム**
    - 防衛省・自衛隊、内閣サイバーセキュリティセンター、独立行政法人　情報処理推進機構、JPCERT/CC、**重要インフラ企業**
    - **米インド太平洋軍**

- シナリオ
  - 重要インフラ
    - 水道、金融、モバイルネットワーク

https://news.sky.com/story/nato-prepares-for-worlds-largest-cyber-war-game-with-focus-on-grey-zone-12274488

  - 偽情報
  - 法律、政策の専門家チーム

2022 Locked Shields cyber exercise
2022年のロックド・シールズ演習

- More than 2,000 people from 33 countries in April 2022
  - **Japan + UK**
    - MOD/SDF, NISC, Ministry of Internal Affairs and Communications, National Police Agency, IPA, JPCERT/CC, critical infrastructure companies
    - **UK Ministry of Defence, Armed Forces**
- Scenario
  - More than 8,000 live-fire attacks
  - Critical infrastructure
    - Reserve management and financial messaging systems of a central bank
  - Forensic, legal, media and information operations

- 2022年4月開催の演習には33カ国から2000人以上参加
  - **日本・英国チーム**
    - 防衛省・自衛隊、内閣サイバーセキュリティセンター、総務省、警察庁、独立行政法人　情報処理推進機構、JPCERT/CC、重要インフラ企業
    - **英国防省、英軍**
- シナリオ
  - 8000回以上の攻撃
  - 重要インフラ
    - 中央銀行の外貨準備や金融メッセージ・システム
  - フォレンジック、法律、メディア、情報戦

https://twitter.com/ModJapan_jp/status/1517113397745426439

What is next?　今後の課題

■ Efforts to continue or increase

- Contribution to global cybersecurity
- Enhance capabilities to protect critical infrastructure via international public-private partnerships
- Public attribution

■ Future steps to take

- Increase publication or presentations about Japan’s efforts and contribution in English
- Contribution to Paris 2024, Los Angeles 2028, Brisbane 2032

■ 今後も継続・増やすべき努力

- グローバルのサイバーセキュリティへの貢献
- 国際的な官民連携による重要インフラ防御の能力向上
- 攻撃元の特定と公表

■ 今後行うべき努力

- 日本の取り組みや貢献について英語で公表、プレゼンの拡大
- 2024年のパリ五輪、2028年のロサンゼルス五輪、2032年のブリスベン五輪への貢献