資料５－１

# サイバーセキュリティ人材の育成の強化について

平成２７年１２月

総務省

# 実践的なセキュリティ人材の育成



■ 総務省では、新たな「サイバーセキュリティ戦略」を踏まえ、産学官連携で人材育成のための実践的な演習の取組を推進

官公庁・重要インフラ企業
政府、重要インフラ等
の機密情報を守る
人材を育成

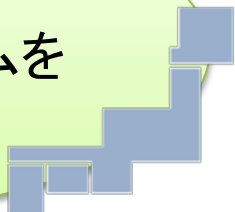

**総務省におけるサイバー演習事業**

- CYDER
- サイバーコロッセオ

オリピック・パラリンピック
2020年開催の東京大会を守る人材を育成

地方公共団体

地公体の情報システムを
守る人材を育成



# 研究開発用クラウド環境によるサイバー防御演習の実施



- NICTでは、標的型攻撃など新たな脅威に対抗する技術の検証環境を、容易かつ高精細に構築する技術の研究開発を行うため、石川県に大規模なクラウド環境を設置。
- 同環境を活用し、総務省の施策として、官公庁・大企業等のLAN管理者のサイバー攻撃への対応能力向上のために、実践的なサイバー防御演習（CYDER)を実施。

**NICT北陸StarBED研究センター**
（セキュリティ研究開発用クラウド環境）

活用

## 総務省施策　サイバー防御演習（ＣＹＤＥＲ）

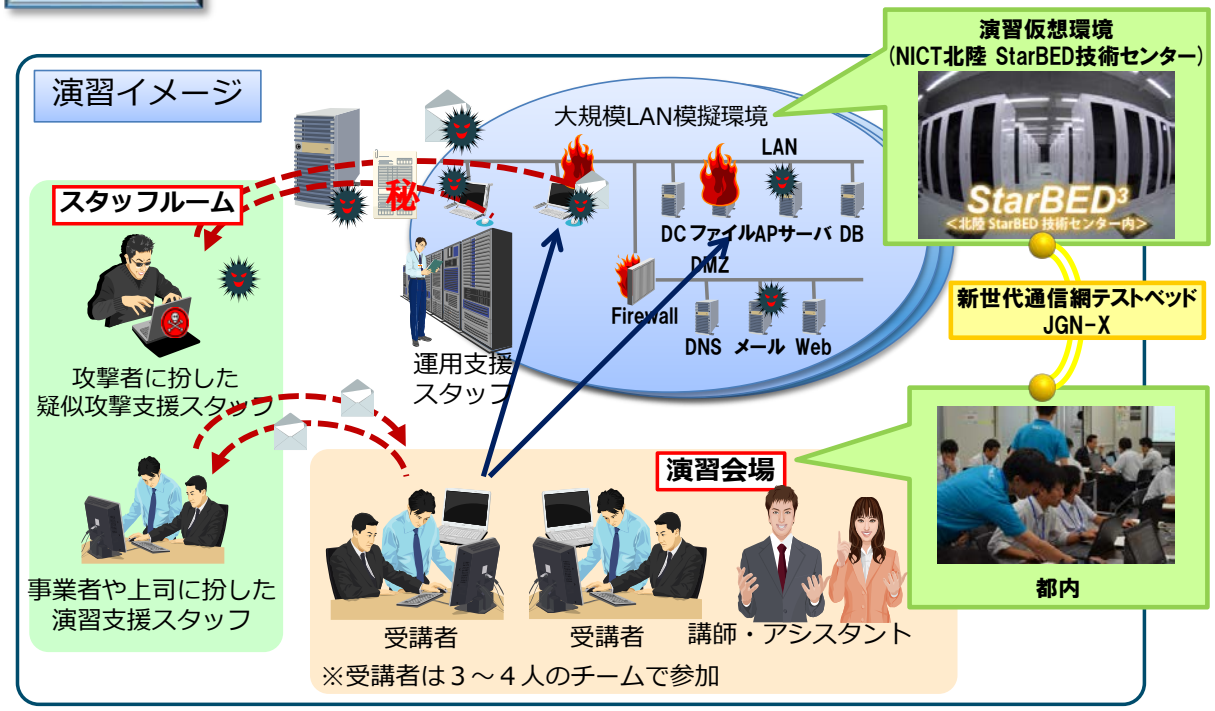
サイダー

○ 数千人規模のネットワークを忠実に再現し、事案発生から対処までの実践的な一連の流れを体験

# 実践的サイバー防御演習（CYDER：CYber Defense Exercise with Recurrence）

■ 官公庁・大企業等のLAN管理者のサイバー攻撃への対応能力向上のため、実践的なサイバー防御演習を実施。
■ 職員が数千人規模の組織内ネットワークを模擬した大規模環境によるサイバー演習は国内唯一。
■ 平成25年度から5カ年計画（現在3年目）。サイバー攻撃の最新動向を元に毎年実践的な防御モデルの改良を積み重ね。

## 概要図




## CYDERの特徴

✓ **大規模かつリアルな模擬演習環境**
数千人規模の組織内ネットワークを忠実に再現した**大規模かつリアルな模擬環境**で演習を実施

✓ **サイバー攻撃への一連の対応を体験**
ログの分析など個々の技術的対応にとどまらず、チームでの参加により、**インシデントハンドリングの一連の流れ※を体験**することで、組織としての実践的対処能力を強化
（※　感染端末の特定、被害拡大防止、原因究明、上司への報告　等）

## 平成27年度の取組結果

✓ **参加組織数**
**約70組織**、**約300名**のLAN管理者が演習に参加

✓ **官公庁・重要インフラ事業者に加え、重要な情報を持つ独法・特殊法人も参加**

✓ **新規シナリオの追加**
年金機構事案を想定した**標的型メール攻撃**に対応
（H26：水飲み場型攻撃）

## 来年度に向けた施策強化の検討

・ **年金機構の事案やマイナンバーの導入を踏まえ、演習の主たる対象に、独法及び地方公共団体等を追加し、年間の演習受講者を大幅に増大することを検討**
・ **大規模設備やネットワークセキュリティに関する幅広い知見を有する国立研究開発法人情報通信研究機構（NICT）が、それらを活用して継続的・安定的に実践的サイバー防御演習を実施できるよう措置を検討**

# 2020年東京オリンピック・パラリンピック競技大会に向けたサイバーセキュリティ対策の必要性



「初のデジタルオリンピック」と呼ばれた2012年ロンドン五輪での経験を踏まえ、2020年東京五輪関連システムについては更に万全なサイバーセキュリティ確保体制が必要。

## ロンドン五輪の経験

- ✓ メイン競技場を含む英国全土94すべての会場をネットワークで接続
- ✓ 大会記録の表示、チケット販売、開会式等イベント制御等、多様な重要システムを整備
- ✓ インターネットでの大会模様のライブ配信、ソーシャルメディアでの情報配信等、リアルタイムの情報発信　等


ロンドン五輪開催中の２週間で・・・

- ・２億1200万の不正アクセス
- ・開会式時に照明システムに対するDoS攻撃の予告　等

・大規模サイバー攻撃対処訓練を事前に5回以上実施
・ロンドン五輪開催時には約850名による体制でネットワークを監視

ロンドン五輪時よりも更に巧妙化するサイバー攻撃に備えるためには、サイバーセキュリティ人材の育成が急務

# 2020年東京オリンピック・パラリンピック開催に向けたサイバー演習による人材の育成

## 概要

2020年東京オリンピック・パラリンピック競技大会関連システムの模擬環境を構築し、大会の運営に係るシステムや放送など、複数のシステムに係る攻撃・防御双方の実践的な演習を行うことにより、オリンピック開催時に想定される高度な攻撃に対処可能な高度な能力を有するサイバーセキュリティ人材の育成を図る。

**2020東京オリンピック・パラリンピックを想定した大規模演習基盤による演習の実施（”サイバー・コロッセオ”）**

## 概要図


NICTのクラウド環境と、その演習で得られた知見を活用

## 具体的内容

- 公式ホームページやチケット販売、Wifi通信環境、放送システム等、多様なシステムの模擬システムの開発
- 上記の取組を通じて疑似オリンピックシステムを構築し、オリンピック開催時を想定したサイバー攻撃の攻撃・防御手法の検証及び訓練を行う。
- オリンピック組織委員会等と連携し、システムを構築。実際のオリンピックシステム担当者の訓練にも用いる。