3-3　2025 年日本国際博覧会向けサイバー防御講習「CIDLE」

3-3　“CIDLE” Cyber Incident Defense Learning for Expo 2025 Osaka, Kansai, Japan

阿部 則夫　花田 智洋
ABE Norio and HANADA Tomohiro

2025 年日本国際博覧会（略称「大阪・関西万博」、以下「万博」）では、複雑かつ多様な情報技術の利活用に伴うサイバーリスクへの備えが不可欠である。万博関係組織のサイバーセキュリティ対応力強化を目的に、2023 年度から 2024 年度末にかけてナショナルサイバートレーニングセンター（以下、当センター）は万博向けサイバー防御講習「CIDLE（シードル）」を実施した。本講習は、日本国際博覧会協会全体のセキュリティ意識向上と、関連組織の情報システム担当者等によるインシデント検知から報告・公表までの体系的習得を通じ、現場対応力向上に重点を置いた。CIDLE は CYDER やサイバーコロッセオで培った知見を活用し、オンラインと集合形式の双方を組み合わせた実践的プログラムとした。得られた知見とノウハウは、セキュリティ人材育成資産として今後の社会全体のセキュリティ対策向上に活かす。

To counter Expo 2025 cyber risks, CIDLE training was held (FY2023-FY2024). Using NICT's CYDER/Cyber Colosseo expertise, it boosted security awareness and incident response for over 600, enhancing overall cyber defense.

At the Expo 2025 Osaka, Kansai, Japan, preparing for cyber risks arising from the complex and diverse use of information technologies is essential. To strengthen the Expo-related organizations' cybersecurity capabilities, the National Cyber Training Center conducted the “CIDLE” cyber defense training program from FY2023 through the end of FY2024. The program aimed to raise security awareness across the Japan Association for the 2025 World Exposition and enhance on-site response capabilities through systematic learning by IT system personnel in related organizations, covering the full process from incident detection to reporting and public disclosure. Leveraging expertise from CYDER and Cyber Colosseo, CIDLE combined online and in-person formats into a practical program. The acquired knowledge and know-how will serve as a resource for cultivating cybersecurity talent and improving overall societal security measures.

1　まえがき

2025 年に開催される日本国際博覧会（略称「大阪･関西万博」、以下「万博」）は、世界各国から多様な人々と最先端技術が集まり、文化・社会・技術の交流が行われる大規模な国際イベントである。会場の運営や来場者向けサービスでは、ネットワーク、IoT 機器、スマートフォンアプリ、クラウドサービス、AI など、様々な情報技術の活用が計画されていた。こうした複雑なシステムが連携する環境では、利便性の向上と同時に、サイバーリスクへの十分な備えが不可欠である。

近年のサイバー脅威は高度化・多様化しており、標的型攻撃、DDoS、フィッシング、クラウドサービスを狙った攻撃などが代表例である。とりわけ、国内外から注目を集める万博のようなイベントでは、一度重大なセキュリティインシデントが発生すれば、来場者の安全やイベント運営の継続性のみならず、日本全体の信頼性にも影響を及ぼしかねない。

こうした状況を踏まえ、大阪府・大阪市等からの要請に基づき、万博に関わる組織のサイバー対応力の強化を目的として、2023 年度から 2024 年度末にかけてナショナルサイバートレーニングセンター（以下、当センター）は万博向けサイバー防御講習「CIDLE（Cyber Incident Defense Learning for Expo 2025, シードル）」を実施した。

この講習は、セキュリティインシデントの検知・受付から、インシデントレスポンス、報告・公表に至るまでの一連の流れを体系的に学ぶ内容とし、単なる知

識の習得にとどまらず、現場での対応力の向上に重点を置いている。特に、現場担当者が自らの役割を正しく理解し、実際のインシデントを想定した上で適切に対応できることを目指して構成した。

2　CIDLE 実施内容

2.1　概要

CIDLE では、万博関連組織のサイバーセキュリティを強化し、安全な開催に資することを目的に、表 1 に示す複数の専門的なトレーニングコースを展開した。これらのコースは、組織全体のセキュリティ水準向上と、現場で実際に対応する担当者の実務能力強化という二つの目的に基づき設計した。急速に変化する脅威環境に対応するため、実際のインシデント事例に基づくケーススタディや、最新の攻撃手法への対処法を取り入れ、実践的かつ体系的な内容とした。

CIDLE は、当センターがこれまでの活動を通じて蓄積してきた人材育成の知見と、現場から得られた多くの経験を基に設計した。中でも、地方自治体や国の機関・重要インフラ事業者を対象に実施してきた実践的サイバー防御演習「CYDER」[1] の集合演習とオンライン演習から得られた知見を土台とした。

加えて、東京 2020 オリンピック・パラリンピック競技大会に向けた実践的サイバー演習「サイバーコロッセオ」[2] で得られた知見も CIDLE に反映した。「サイバーコロッセオ」は、大規模なシステムを舞台に攻撃と防御の双方の視点から演習を行う極めて実践的な内容だった。そこで得られた、高度かつ現実味のあるシナリオ設計や運営の工夫を CIDLE にも反映した。

2.2　提供プログラム

2.2.1　オンライン演習

CIDLE では、当センターが提供する「プレ CYDER」及び「CYDER オンライン入門コース」を基に、「オンラインカレッジエレメンツ I･II」及び「オンラインカレッジ」としてオンライン演習を提供した。

オンラインカレッジエレメンツ I･II は、e ラーニング教材と解説動画を組み合わせた形式で提供した。オンラインカレッジエレメンツ I では、医療機関におけるランサムウェア事例を基に、インシデントハンドリングの初動対応の基本を学ぶ内容とした。オンラインカレッジエレメンツ II では、脆弱（ぜいじゃく）なパスワードによる情報漏えいを基に、委託管理の重要性を扱った。いずれも実際のセキュリティインシデントを題材に、初学者にも理解しやすい構成とし、組織全体のセキュリティリテラシー向上に寄与した。

一方、オンラインカレッジは、より実務的な内容に踏み込み、インシデント対応の一連の流れをオンラインで体験できる構成とした。さらに、オンライン上の仮想環境を用いたメモリ保全のハンズオン演習も実施し、技術的な対応力の習得を支援した。

2.2.2　集合演習

受講者がインシデントハンドリングに必要な知識とスキルを段階的かつ体系的に習得できるよう、4 種類の集合演習コース（集合カレッジ I、集合カレッジ II、集合演習 I、集合演習 II）を設計した。集合カレッジでは、セキュリティインシデントに関する座学を主体としたインシデントハンドリングに関する講義と実機演習を実施した。集合演習では、グループワークやロールプレイを中心に大規模イベント向けのインシデント対応演習を実施した。特に、万博を想定したセキュリティインシデントへの対応力を養うことを目的とし、過去の大規模イベントにおいて実際に発生したセキュリティインシデント事例を多数提示し、現実に起こり得るリスクへの備えを体系的に確認・強化できる構成とした。ディスカッションでは、チーム内連携強化を目的とした課題を議論し、実践的な対応力の育成を図った。

表 1　CIDLE 演習コース

■ 2023 年度

コース	形式	所要時間	実施時期	受講対象者
CIDLE オンラインカレッジエレメンツ I	オンライン	2 ～ 3 時間	令和 5 年12月～令和 6 年 1 月	博覧会協会職員（システム担当課等）
CIDLE オンラインカレッジ	オンライン	3.5 時間	令和 5 年 9 月～令和 6 年10月	博覧会協会職員（サイバーセキュリティ担当課等）
CIDLE 集合カレッジ I	集合	2 日	令和 6 年 2 月	博覧会協会職員（サイバーセキュリティ担当課等）
CIDLE 集合演習 I	集合	1 日	令和 6 年 2 月	博覧会協会職員（サイバーセキュリティ担当課等）

■ 2024 年度

コース	形式	日数	実施時期	
CIDLE オンラインカレッジエレメンツ II	オンライン	2 ～ 3 時間	令和 6 年11月～令和 7 年 1 月	博覧会協会職員（全職員）
CIDLE 集合カレッジ I	集合	2 日	令和 7 年 1 月	博覧会協会職員（サイバーセキュリティ担当課等）
CIDLE 集合演習 I	集合	1 日	令和 7 年 1 月	博覧会協会職員（サイバーセキュリティ担当課等）
CIDLE 集合カレッジ II	集合	2 日	令和 7 年 2 月	博覧会協会職員（サイバーセキュリティ担当課等）
CIDLE 集合演習 II	集合	1 日	令和 7 年 2 月	博覧会協会職員（サイバーセキュリティ担当課等）

演習は 4 人 1 組のグループ形式で実施し、参加者同士の活発な意見交換が行えるよう配慮した。

2.2.2.1　集合カレッジ

集合カレッジⅠでは、座学とハンズオン演習を組み合わせた 2 日間のプログラムで、インシデントハンドリングの全体像を体系的に学習した。具体的には、「インシデントハンドリングの概要」や、「検知・連絡受付」「トリアージ」「インシデントレスポンス」「復旧措置」「再発防止策の検討」「報告・公表」に至るまでの一連のプロセスを網羅し、さらに IT 基礎やネットワークに関する学習も構成に含めた。

集合カレッジⅡでは、カレッジⅠで習得した基礎知識を発展させ、より高度な技術的内容に取り組めるようにした。ハンズオン演習では受講者の応用力と分析力の強化を目的とし、攻撃者の視点に立った分析、マルウェア解析、ログ解析などを扱い、Kali Linux[3]、Sysinternals ツール群 [4]、Wireshark[5] などを用いた実践的な内容を実施した。

2.2.2.2　集合演習

集合カレッジに加えて、1 日完結型の演習として集合演習Ⅰ及び集合演習Ⅱを実施した。集合演習Ⅰでは、情報漏えいインシデントを題材に、集合カレッジⅠで習得したスキルを活用し、インシデントハンドリングの流れを実践的に体験する内容とした。続く集合演習Ⅱでは、実際のログを用いた調査・分析を通じて、より現実的かつ複雑なセキュリティインシデント対応に取り組み、実践力向上を目指した。

なお、集合カレッジⅡ及び集合演習Ⅱへの参加にあたっては、それぞれ前段階となる集合カレッジⅠ及び集合演習Ⅰの修了を受講要件とすることで、受講者が無理なく知識・技術を段階的に習得できるよう配慮した。

さらに、最新の脅威動向を踏まえ、SaaS 型クラウドサービス事例と対策を演習内容へ追加した。そのほか、テキストとは別に補足資料として、クラウドセキュリティに関する資料を、オンプレミス環境との相違点を踏まえつつ、SaaS クラウドサービスにおける適切なセキュリティ対策検討の参考資料として提供した。

2.3　演習環境

受講者が実践的スキルとチーム連携能力を効果的に高めることを目的に、現実に近い状況を再現した演習環境を整備した。演習では、タスク管理ツールや、サイバーセキュリティ競技で利用されている Web プラットフォーム「CTFd[6]」などのシステムを積極的に活用し、学習効果の向上と実務に直結する対応力強化を図った。

タスク管理ツールは、プロジェクト管理やタスクの可視化、チーム内情報共有を支援するオープンソースの管理ツールを用いた。本演習ではこれらを活用することで、実際の組織環境に即したインシデント対応のプロセスを体験的に学ぶ機会を提供した。実務に近いシステムを使用することで、受講者は所属組織でのツールの活用方法を見直し、再整理するきっかけを得ることができた。

また、CTFd を用いることで、問題解決型の演習環境を提供し、自動採点や進捗管理といった機能を通じて学習プロセスを効率化した。さらに、ゲーム性やランキング機能を活用し、受講者のモチベーションを高めながら学習効果の可視化と継続的な学習意欲維持に寄与した。

これらのツールを組み合わせることで、実践的かつ活発なチーム内連携が可能となり、受講者の総合的な能力向上に大きく貢献した。

2.4　講師・チューター

受講者に高度で実践的な学習機会を提供するため、質の高い講師陣をそろえ、教育効果を最大化するインストラクション設計を行った。

講師陣の体制は、講師統括責任者、講師、チューターで構成した。

講師統括責任者は、効果的なトレーニングの提供に必要なスキルを国際的に認定する資格 CompTIA CTT+（Certified Technical Trainer）[7] を保有し、学習効果の高い演習提供のため、講師・チューターへの指導を行う。

講師には、国家資格である情報処理安全確保支援士や国際的に認知された情報セキュリティ専門資格 CISSP（Certified Information Systems Security Professional）[8] など、高度な専門資格の要件を満たす人材を配置した。加えて、サイバーセキュリティまたはインシデントハンドリングに関する豊富な演習実績を必須とし、深い知識と経験で演習の専門性と信頼性を支えた。

チューターには、情報セキュリティ専門資格を保有し、サイバーセキュリティまたはインシデントハンドリングに関する演習実績がある人材を配置した。これにより、受講者からの専門的な質問にも的確に回答できる体制を整えた。

さらに、講師統括責任者と NICT 職員が中心となり、講義・演習の両面で複数回のリハーサルを行い、演習運用を指導した。準備、プレゼンテーション、コミュニケーション、ファシリテーション、評価といったインストラクションの主要要素を網羅的に確認し、受講者が最大限の学びを得られるよう改善を続けた。

3　実施結果

3.1　オンライン演習の成果

受講者からのアンケートでは、コンテンツ内容と実務との関連性について肯定的な意見が多く寄せられた。

- 「単なる知識研修と異なり、実例を挙げた研修で臨場感もありよかった。」
- 「基本的な用語についても分かりやすく説明されており、これまで曖昧だった内容がよく理解できた。」
- 「事前の準備に加え、自らや組織としての対策が大切であると感じた。」

特に、オンラインカレッジの仮想環境を活用したメモリ保全のハンズオン演習については、実践的な操作に対する高い評価を得た。

- 「フォレンジックの具体的な進め方など、一部ではあるが実践できたことで理解が深まった。」
- 「テキストだけでなく動画での説明や、実践演習における具体的なケースが参考になった。」

一方で、今後の演習企画に向けた貴重な要望も得られた。

難易度：「難易度が低かった」または「高かった」など、個々の受講者のレベルに応じた調整の必要性が示唆された。

学習効果維持：「分割受講の際に過日の学習内容が薄れるため、途中でクイズ形式の学習を設けてほしい」との声があり、継続的な学習効果を維持するための工夫が求められた。

3.2　集合演習の成果

図 1 は演習風景の一部である。集合カレッジ I･II 及び集合演習 I・II では、座学とハンズオン演習を組み合わせた体系的な内容により、インシデントハンドリングに関する知識と実践力の向上を図った。

受講者からのアンケート結果として、「知識・スキルが向上した」との回答が 90 % を超え、講習の有効性が確認された。自由記述では、「網羅的にインシデントハンドリングの全体像が説明され、理解が深まった。技術的な内容も多かったが、わかりやすいスライドと説明で、専門外の受講者でも理解できた。」「実際の組織を想定したシナリオに基づいた講義となっている点が役に立った。」「グループでコミュニケーションをとりながら実施し、異なる発想を得られたのがよかった（警備セキュリティ視点など）。」との意見が見られた。

「博覧会協会の実態に即した内容にしてほしい」という声のほか、講習の内容を復習できる e ラーニングを希望する意見もあった。

4　おわりに

CIDLE を通じて得られた実践的サイバー防御講習の知見と運営ノウハウは、今後のセキュリティ人材育成における資産として活用する。当センターが培った「CYDER」や「サイバーコロッセオ」の経験と CIDLE の成果を統合し、大規模イベント、地方自治体、国の機関・重要インフラなど、多様な組織のサイバーセキュリティ人材育成に貢献していく。これらの知見を活用し、インシデントハンドリングを中心としたサイバー

図 1　CIDLE 集合演習の風景

セキュリティ関連の新たなコンテンツ開発につなげ、社会全体のセキュリティ対策の向上に寄与していく。

【参考文献】

1 NICT サイバーセキュリティ研究所ナショナルサイバートレーニングセンター, CYDER
https://cyder.nict.go.jp
2 NICT サイバーセキュリティ研究所ナショナルサイバートレーニングセンター, 東京 2020 オリンピック・パラリンピック競技大会に向けた実践的サイバー演習「サイバーコロッセオ」
https://www.nict.go.jp/press/2017/12/07-1.html
3 OffSec, Kali Linux
https://www.kali.org/
4 Microsoft, Sysinternals
https://learn.microsoft.com/ja-jp/sysinternals/
5 Wireshark Foundation, Wireshark
https://www.wireshark.org/about
6 CTFd, CTFd,
https://ctfd.io/
7 CompTIA, CTT+
https://www.comptia.jp/certif/additional_professional/comptia_cttcbt_201/
8 ISC2, CISSP
https://japan.isc2.org/cissp_about.html

阿部 則夫（あべ のりお）
サイバーセキュリティ研究所
ナショナルサイバートレーニングセンター
サイバートレーニング研究室
主任研究技術員
サイバーセキュリティ、人材育成

花田 智洋（はなだ ともひろ）
サイバーセキュリティ研究所
ナショナルサイバートレーニングセンター
サイバートレーニング研究室
室長
サイバーセキュリティ、人材育成
【受賞歴】
2021 年　令和 3 年度科学技術分野の文部科学大臣表彰 科学技術賞 理解増進部門