Ver 1.8

AMIYA
サイバーセキュリティトレーニング

Powered by CYBERGYM

(C) AMIYA Corporation

サイバー攻撃被害の85%は”人”の脆弱性が原因

”人“の脆弱性が原因で発生するサイバー攻撃被害

- メール誤送信による情報漏洩
- フィッシングサイトやフィッシングメールからマルウェアに感染
- VPN機器の脆弱性を放置、ランサムウェアの侵入経路に
- 事業部門が契約したクラウドサービスから情報漏洩（認証強度が弱い）
- 設定ミスでサーバをインターネットへ公開、DDoS Bot化
- インターネット分離できていると勘違い、
  実はインターネットに繋がっていたシステムから不正侵入

被害を拡大する誤った行為

- 経営層がサイバー攻撃被害の実情や事業への影響を把握しておらず、組織的なセキュリティ対応の実施を指示していない
- 一般社員が不審な兆候に気づいていたが、セキュリティ部門へ報告せず放置、その後ランサムウェアに感染
- エンジニアによる誤ったインシデント初動対応によりログが消失、原因/被害範囲が特定できず、被害が長期化

“人”の脆弱性に対処する手段なしには、
どれだけシステム的なセキュリティ対策を実施しても効果的ではない

(C) AMIYA Corporation

役割に応じて必要とされるセキュリティ意識/スキル

経営層

- 最新セキュリティ動向
- 利害関係者マネジメント
- 情報セキュリティ基礎
- 標的型攻撃メール
- 規程/マニュアル整備
- デューデリジェンス
- コンプライアンス

一般社員

- 最新セキュリティ動向
- 情報セキュリティ基礎
- 標的型攻撃メール
- 規程/マニュアル理解

セキュリティエンジニア

- CSIRTトレーニング
- ペネトレーション
- OTセキュリティ
- セキュア開発
- デジタルフォレンジック
- インシデントレスポンス
- アクティブディフェンス

経営層から一般社員まで、全従業員のセキュリティ意識/スキル向上が組織を守る

(C) AMIYA Corporation

各種ガイドラインでも必須の項目

セキュリティ意識向上プログラムを確立し維持する

「セキュリティ意識向上プログラムの目的は、組織の資産やデータを安全に扱う方法を、組織の従業員に教育することです。入社時及び最低でも年１回のトレーニングを実施します。」

CIS Controls v8

役割に応じたセキュリティ意識とスキルのトレーニングを実施する

「IT専門家を対象としたセキュアなシステム管理コースやウェブアプリケーション開発者を対象としたOWASP TOP10の脆弱性を認識および防御するためのトレーニングなど。」

CIS Controls v8

金融	金融機関等コンピュータシステムの安全対策基準・解説書
官公庁	政府機関の情報セキュリティ対策のための統一基準
水道	水道分野における情報セキュリティ確保に係るガイドライン
交通	国土交通省所管重要インフラにおける情報セキュリティ確保に係るガイドライン
重要インフラ	重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針
地方自治体	地方公共団体における情報セキュリティポリシーに関するガイドライン
中小企業	中小企業の情報セキュリティ対策ガイドライン
教育	教育情報セキュリティポリシーに関するガイドライン

(C) AMIYA Corporation

AMIYA サイバーセキュリティトレーニング

”実践型”トレーニングで動けるあらゆる層の人材を育成

経営層から一般社員、エンジニアまでの全ての層に、実践型のトレーニングを提供

最新の攻撃を体感する	ハッカーは新しい攻撃手法を日々開発しています。それに追従するためには、実際に新たな攻撃手法を体感し、その攻撃のリスクや対処方法を理解することが効果的です。
定着率が向上する	実践型のトレーニングは、座学に比べて長期的な記憶に残りやすく、実践的なスキルを身につけるのにも効果的です。セキュリティエンジニアは、実際に攻撃をシュミレーションすることで攻撃手法を理解し、具体的に防御策を検討できるようになります。
危機管理能力が向上する	インシデントが発生した場合、従業員は速やかに行動する必要があります。実践型のトレーニングを受けることで、従業員はインシデントに対する適切な対処方法を学び、パニックに陥ることなく正確かつ迅速に対処することができます。
従業員へ安心感を与える	実際にサイバー攻撃シナリオに直面し、それに対処できるようにすることで、自信が身につきます。従業員が攻撃に対処できるという自信があると、ストレスや不安を軽減し、従業員の安心感を高めることができます。

(C) AMIYA Corporation

イスラエル発の最新セキュリティトレーニング

イスラエルのCYBERGYM社と提携し、最新セキュリティトレーニングを提供。
CYBERGYM社は、イスラエル電力公社とCyber Control社の共同事業として2013年に設立。

イスラエル電力公社を狙った攻撃

- 年間 **2億** 回以上の攻撃
- 最高月間攻撃数 **7,000万** 件以上
- 月 **1,000** 回以上の攻撃が電力公社ネットワークに侵入

※2020年実績

▶ それでも、国内唯一の重要インフラを守り続けられている理由は？

経営層、一般社員(12,000人)、エンジニアへの
最先端のサイバーセキュリティトレーニング

CYBERGYM が実施

WorldWideにセキュリティトレーニングを展開

(C) AMIYA Corporation

“超”実践型トレーニング

“リアルタイム” のサイバー攻撃を体感

最新のトレーニング施設で、
レッドチームによるリアルタイムのサイバー攻撃を体験。
実際にサイバー攻撃を受けることで、
サイバー攻撃や防御方法への理解が深まります。

イスラエル発

“最新”セキュリティトレーニング

サイバーセキュリティ先進国であるイスラエル。
重要インフラで培ったセキュリティナレッジをトレーニング化。

(C) AMIYA Corporation

役割分担でトレーニングを効率化

役割分担でトレーニング効率を最大化。
受講者は、レッドチームからのサイバー攻撃からトレーニング環境を守る。

WHITE TEAM

トレーニング管理
（講師）

アクティビティを管理し、
トレーニングの効果を最大化

BLUE TEAM

防御
（受講者）

レッドチームからの攻撃から
トレーニング環境を守る

RED TEAM

攻撃
（ホワイトハッカー）

ブルーチームへの
サイバー攻撃を実施

(C) AMIYA Corporation

経営層/一般社員向けトレーニング

経営層向け

経営層向け机上トレーニング

対象：経営層、マネジメント層、経営企画	開催対象：個社ごと
サイバー攻撃を受けた際に的確かつ迅速な対応を行うための経営判断能力の習得、シミュレーションを行います。 日頃、トレーニングなどの経験の少ない経営層がアクティブラーニングを体験できます。	開催場所：お客様先 or オンライン 受講価格：600,000円～（税抜）/1社

Cyber Strategy for Executives

対象：経営層、マネジメント層、経営企画	開催対象：個社ごと
慶應義塾大学法学部田村教授が講師を務める経営層向けトレーニング。 善管注意義務など経営層が知っておくべき法律について理解し、実際にアクティブラーニングを行います。	開催場所：お客様先 or オンライン 受講価格：1,600,000円～（税抜）/1社

一般社員向け

CSIRT向けインシデントレスポンス机上トレーニング

対象：CSIRTメンバー/ステークホルダー	開催対象：個社ごと
最新のサイバーセキュリティ動向及びインシデントハンドリングの机上訓練を通じ、 サイバーセキュリティインシデントに対応するために必要な組織、機能、手順、人材を理解します。	開催場所：お客様先（2時間） 受講価格：600,000円～（税抜）/1社

一般社員向けトレーニング（標的型攻撃メール訓練＋セキュリティ講習）

対象：一般社員、新入社員	開催対象：個社ごと
標的型攻撃メール訓練を体験後に、サイバーセキュリティ講習を実施。 攻撃を体験した後の講習のため、従業員の習熟度が向上します。	開催場所：お客様先 or オンライン 受講価格：480,000円～（税抜）/1社

一般社員向けeラーニング

対象：一般社員、新入社員	
一般社員に向けたサイバーセキュリティに特化した本格的eラーニングコンテンツ。 アニメの動画でわかりやすく、飽きのこない充実コンテンツ3つをセットでご提供	開催場所：オンライン 受講価格：10,000円（税抜）/3コース・1アカウント

(C) AMIYA Corporation

セキュリティエンジニア養成トレーニング

初級

インシデント初動対応トレーニング　サイバー攻撃の初動対応

対象：IT担当者、情報セキュリティ担当者	開催対象：オープン
インシデント発生時、まず実施すべき基本的な初動対応（端末隔離や証拠保全など）の知識やスキルを習得します。	開催場所：アリーナ（1日） 受講価格：100,000円（税抜）/1人

Cyber-Threats and Defense Essentials　サイバー攻撃の検知/対応/復旧

対象：IT担当者、情報セキュリティ担当者、SOCアナリスト、情報処理安全確保支援士	開催対象：オープン
ハッカーの攻撃手法であるAPT攻撃に沿って、生のレッドチームからの攻撃を体験。 ツール等を使い調査や分析方法について学び、サイバー攻撃の検知能力を向上します。	開催場所：オンデマンド＆アリーナ（1日） 受講価格：250,000円（税抜）/1人

中級

Forensics Training　サイバー攻撃の特定（フォレンジック）

対象：IT担当者、情報セキュリティ担当者、情報処理安全確保支援士	開催対象：オープン
実践的なトレーニングを通じて、組織内におけるデジタルフォレンジックの全工程を自ら組み立て、中心的立場で実行できる能力を習得します。	開催場所：アリーナ（2日） 受講価格：400,000円（税抜）/1人

Penetration Tester Training　サイバー攻撃（脆弱性診断/ペネトレーションテスト）

対象：IT担当者、情報セキュリティ担当者、SOCアナリスト、脆弱性診断士	開催対象：オープン
実践的なトレーニングを通じて、脆弱性診断やペネトレーションテストを行う際に必要不可欠となる知識やテクニックを習得します。	開催場所：オンデマンド＆アリーナ（2日） 受講価格：500,000円（税抜）/1人

開発

Secure Coding for Developers　セキュア開発

対象：開発担当者	開催対象：オープン
セキュアな製品を完成させるまでの一連の概念と開発手法の習得を目的とし、要件定義・設計・コーディングの段階で製品の安全性を確保するスキルの習得を目標とします。	開催場所：アリーナ（2日） 受講価格：300,000円（税抜）/1人

(C) AMIYA Corporation

経営層向け机上トレーニング

経営層向け

AMIYA

サイバーセキュリティ問題は、セキュリティ・情報管理部門だけの技術的な問題ではなく経営課題として捉える必要があります。
サイバー攻撃を受けた際に的確かつ迅速な対応を行うための経営判断能力の習得、シミュレーションを行います。

対象

- 経営層
- マネジメント層
- 経営企画

受講者の声

製造業

サイバー攻撃が事業継続上のリスクとなっている昨今、
セキュリティリスク対応を経営陣としてどう陣頭指揮を取って
いくべきなのかを理解できました。

プログラム

1. サイバーセキュリティ最新動向
2. サイバーセキュリティの概念とインシデント事例
3. 経営層の判断と責任
4. 組織におけるサイバーセキュリティ対策
5. サンプル事例での机上演習
6. 演習のレビューとディスカッション

Goal

実際にサイバー攻撃を受けたことを想定し、的確な判断スキルの習得と具体的な事前準備を促進します。また、経営層として必要なサイバーセキュリティの心得・対策を学びます。

場所	要相談（オンサイト/オフサイト）
期間	2時間～2日間まで応相談
費用	60万円(税抜) ～/1社

(C) AMIYA Corporation

Cyber Strategy for Executives

経営層向け

AMIYA

サイバーセキュリティ問題は、セキュリティ・情報管理部門だけの技術的な問題ではなく経営課題として捉える必要があります。
善管注意義務など経営層が知っておくべき法律について理解し、実際にアクティブラーニングを行います。

慶應義塾大学法学部 田村教授と共同開発

田村 次郎 教授

慶應義塾大学法学部 教授
交渉学協会 理事長
日本説得交渉学会 会長
ホワイト&ケース法律事務所特別顧問（弁護士）

対象

- 経営層
- マネジメント層
- 経営企画

受講者の声

製造業

サイバー攻撃が事業継続上のリスクとなっている昨今、
セキュリティリスク対応を経営陣としてどう陣頭指揮を取って
いくべきなのかを理解できました。

プログラム

1. サイバーセキュリティ最新動向
2. 利害関係者マネジメント
3. デューデリジェンス（適正手続き）
4. コンプライアンス
5. アクティブラーニング（模擬ケース）

Goal

実際にサイバー攻撃を受けたことを想定し、的確な判断スキルの習得と具体的な事前準備を促進します。また、善管注意義務の履行に必要な心得・対策を学びます

場所	要相談（オンサイト/オフサイト）
期間	2時間〜2日間まで応相談
費用	160万円(税抜) 〜/1社

(C) AMIYA Corporation

CSIRT向けインシデントレスポンス机上訓練

一般社員向け

AMIYA

万一の緊急対応を焦らず、スムーズに実施するためには、平時の訓練が必要不可欠です。
平時の取り組みから緊急時の取り組みまでを総合的に訓練することで、CSIRTチームの練度を向上します。

プログラム

1. 検知/連絡受付
2. トリアージ（検査・分析）
3. 対応方針の検討
4. 復旧措置と再発防止
5. 情報公開の検討
6. まとめ及び質問

対象

- CSIRTチームの練度を向上したい組織
- 社内のステークホルダーを巻き込んでセキュリティ推進をしたい組織

Goal

平時・有事におけるCSIRTチームの活動を机上で体験することで、CSIRTチームの練度を向上し、万一の事態でも適切な対応ができるチームを目指します。

受講者の声

医療関係

CSIRT組織を立ち上げたばかりで、インシデント対応マニュアルの不備が見つかり、ブラッシュアップに役立ちました。

場所	要相談
期間	約 2時間
費用	60万円(税抜) ～/1社

(C) AMIYA Corporation

標的型攻撃メール訓練＆セキュリティ講習

一般社員向け

AMIYA

受講者は、事前に訓練用の安全な標的型攻撃メール（フィッシングメール）を送付し、サイバー攻撃を経験します。
その後、それに対する正しい対処方法を含めた情報セキュリティに関する研修を実施します。

受講者の声

製造業

毎年実施していた研修と比較し、事前に標的型攻撃メールを受けることで、社員の理解度が向上したと感じました。

Goal

社会人として、最低限必要な情報セキュリティに関する基礎知識を習得します。

プログラム

1. セキュリティ対策の基本
2. 情報セキュリティ事故の傾向
3. セキュリティ事故の防止
4. ソーシャルエンジニアリング対策
5. 情報セキュリティ事故事例①
6. マルウェア対策の基本
7. 標的型攻撃メールの見抜き方
8. 情報セキュリティ事故事例②
9. テレワークにおけるセキュリティ
10. オンラインミーティングにおけるセキュリティ
11. セキュリティ事故が生じた際の報告

場所	お客様先 or オンライン
期間	約 1時間
費用	48万円(税抜) ～/1社

(C) AMIYA Corporation

eラーニング（一般社員向け）

一般社員が理解しやすいアニメテイストの情報セキュリティ動画を提供します。
さらに、受講後はシステム上でテストに回答してもらうことで、理解度をチェックできます。

プログラム

1. 情報セキュリティ＜サイバー編＞
2. 情報セキュリティ＜入門編＞
3. 情報セキュリティ＜手口解説編＞

Goal

情報セキュリティに関する初歩的な知識を習得し、情報セキュリティ意識を向上します。

場所	eラーニング形式
期間	3ヶ月
費用	1万円(税抜) /3コース・1アカウント

受講者の声

製造業

年に1回、従業員全員に受講してもらってます。
アニメテイストなので、ITリテラシーが高くなくても抵抗感ないことが良いポイントだと感じています。

(C) AMIYA Corporation

AMIYA

エンジニア向け

インシデント初動対応トレーニング

インシデント発生時の基本的な初動対応を実践的に習得するトレーニングです。
インシデントに適切に対応することで、被害範囲の最小化・証拠保全による原因の早期究明に繋がります。

対象

- 社内セキュリティ担当部門として、有事に備えた実践的な訓練を積みたい方
- 新しくセキュリティ部門に配属される方

受講者の声

製造業

証拠保全のための具体的なコマンドや発生事象を時系列でしっかりと記録しておくなど、インシデント対応に必要な手法を体系的に理解できた。

小売業

事前にトレーニングを受けておくことの必要性を感じた。さらに、社内のインシデント対応マニュアルを整備し、インシデントに備えたい。

プログラム

1. サイバーセキュリティの基礎
2. インシデント対応の基本
3. マルウェアフォレンジック
4. インシデント対応演習
5. クロージングセッション

Goal

外部パートナーと協力してインシデントを収束できることを目標とし、基本的なインシデント初動対応スキルを習得します。

場所	日本橋アリーナ
期間	演習 1 日間
費用	10万円(税抜) /1人

(C) AMIYA Corporation

Cyber-Threats and Defense Essentials

エンジニア向け

AMIYA

サイバーセキュリティの基礎の復習と、実際にAPT攻撃を受けて検知する業務を実体験する実践的なトレーニングです。
イスラエルのセキュリティエンジニア率いるレッドチームと連携し、仮想化技術によって安全に分離された環境下で
リアルタイムに実際のAPT攻撃を体験できます。

対象

- 社内セキュリティ担当部門として、有事に備えた実践的な訓練を積みたい方
- システム部門とセキュリティ部門の調整役を担っている方
- 新しくセキュリティ部門に配属される方

受講者の声

製造業

セキュリティ対策について考えが甘かった。特に脆弱性があるとどうなるのかが理解できた。

金融業

サイバー攻撃に関する調査は実践する機会はあまりないですが、トレーニングを通じて日々の訓練の必要性を痛感しました。

Goal

実際のサイバー攻撃を受け、複数の検出・監視ツールを駆使してサイバー攻撃を検出し、その分析を行うためのスキルを習得します。

プログラム

1. オープニングセッション
2. サイバーセキュリティの概念
3. アクティブディフェンスの概念
4. WireShark概論&演習
5. Sysinternals概要&演習
6. マルウェアフォレンジック演習
7. SIEM概論
8. アリーナインフラについて
9. APT攻撃演習
10. 演習レビュー
11. クロージングセッション

場所	日本橋アリーナ
期間	座学はオンデマンド＆演習１日間
費用	25万円(税抜) /1人

(C) AMIYA Corporation

エンジニア向け

AMIYA

Forensics Training

デジタルフォレンジックに必要不可欠となる知識やテクニックを習得します。
仮想化技術によって安全に分離された環境で、実際のデジタルフォレンジック演習を行います。

対象

- 有事に備えた実践的なデジタルフォレンジックスキルを習得したい方
- CSIRT/SOCチームに配属される方
- 新しくセキュリティ部門に配属される方

受講者の声

製造業

実践形式でデジタルフォレンジックを経験できた

製造業

実際のインシデント時に早急にクロージングできるよう、定期的に訓練をしておきたいと感じた

Goal

実践的なトレーニングを通じて、組織内におけるデジタルフォレンジックの全工程を自ら組み立て、中心的立場で実行することができる能力の習得します。

プログラム

1. オープニングセッション
2. ファーストレスポンダー
3. マルウェア概要
4. Sysinternals概要
5. 演習フォレンジック
6. ネットワークフォレンジック概要&演習
7. 機密ファイルを盗むハンズオン
8. クロージングセッション

場所	赤坂アリーナ
期間	2日間
費用	40万円(税抜) /1人

(C) AMIYA Corporation

Penetration Tester Training

エンジニア向け

AMIYA

脆弱性診断やペネトレーションテストを行う際に必要不可欠となる知識やテクニックを習得します。
イスラエルのセキュリティエンジニア率いるレッドチームと連携し、仮想化技術によって安全に分離された環境で、
実際のペネトレーションテスト演習を行います。

対象

- 社内セキュリティ担当部門として、ペネトレーションテスト/脆弱性診断の実践的なスキルを習得したい方
- 社内システム開発担当としてセキュリティの品質管理に携わる方
- プログラミングの実務経験があり、セキュリティの知見を身に付けたい方

受講者の声

IT業界/システムエンジニア

脆弱性診断を体系的に学ぶことができたため、社内システムに対して、脆弱性診断を定期的に実施したい。

IT業界/システムエンジニア

開発案件に脆弱性診断を加えることで、売上向上につなげたい。

Goal

的確な脆弱性やマルウェアに関する網羅的な知識をベースとしてペネトレーションテストを実施するための様々なツールや手法について習得することを目標とします。

プログラム

1. オープニングセッション
2. 侵入テストの概要
3. ネットワーク情報収集と演習
4. Web情報収集と演習
5. Kali Linux 演習
6. Metasploit 演習
7. ワイヤレスネットワークへの攻撃演習
8. モバイルプラットフォームへの攻撃演習
9. Webアプリケーションの脆弱性と攻撃演習
10. クロージングセッション

場所	日本橋アリーナ
期間	座学はオンデマンド＆演習2日間
費用	50万円(税抜)/1人

(C) AMIYA Corporation

AMIYA

エンジニア向け

Secure Coding for Developers

要件定義・設計・コーディングの段階で、セキュリティ上の脆弱性を含まない開発のための開発エンジニア向けトレーニング。
イスラエルのホワイトハッカーが実際に攻撃を仕掛け、脆弱性が明らかになった箇所を受講者が改修し、
再度攻撃がなされるというサイクルを、ハッカー及び講師からのフィードバックとともに繰り返します。

対象

- セキュア開発の基本知識を習得したい方
- ツールを使用したセキュアコーディングスキルを習得したい方
- 脆弱性に対する修正スキルを習得したい方

受講者の声

IT業界/システムエンジニア

脆弱性があった時に実際何が起こるか？ということが体験できた。

IT業界/システムエンジニア

開発プロジェクトにセキュア開発を組み込むことで、競争優位性を作れるなと感じた。

Goal

セキュアな製品を完成させるまでの一連の概念と開発手法の習得を目的とし、要件定義・設計・コーディングの段階で製品の安全性を確保するスキルの習得を目標とします。

プログラム

1. オープニングセッション
2. セキュアコーディング概説
3. セキュアコーディング手法（入力バリデーション、認証と認可、暗号の使用、フレームワーク）
4. コーディング規約とコードレビュー
5. コードレビュー演習
6. 静的コード解析
7. Web脆弱性演習
8. クロージングセッション

場所	日本橋アリーナ
期間	2日間
費用	30万円(税抜) /1人

(C) AMIYA Corporation

AMIYA

エンジニア向け

CYBERGYM's Zero to 'Hero'

サイバーセキュリティのコアメンバーとなり得るCSIRT/SOCのチームメンバーを育成します。
イスラエルのセキュリティエンジニア率いるレッドチームと連携し、仮想化技術によって安全に分離された環境で、実際の演習を行います。

対象

- 有事に備えた実践的なセキュリティスキルを習得したい方
- CSIRT/SOCチームに配属される方
- 新しくセキュリティ部門に配属される方

受講者の声

IT業界/システムエンジニア

サイバーセキュリティについて体系的に学ぶことができた。

IT業界/セキュリティエンジニア

自習でもスキルアップができる。

プログラム

1. サイバーセキュリティ基礎とテクノロジー
2. インシデントレスポンストレーニング
3. SIEM侵入検知トレーニング
4. デジタルフォレンジックトレーニング
5. SOCチーム 手順&ポリシーワークショップ
6. クロージングセッション

Goal

検知や調査が困難なAPT攻撃への対応能力を向上させ、FWやIPS、SIEM、EDR等のセキュリティオペレーションをよりスムーズに実現できるようになることを目指します。

場所	赤坂アリーナ
期間	約 60日間
費用	250万円(税抜) /1人

(C) AMIYA Corporation

ICS Defense Essentials

エンジニア向け

AMIYA

OT(Operational Technology)におけるサイバーセキュリティに必要な概念を習得します。
本トレーニングでは、イスラエルのセキュリティエンジニア率いるレッドチームと連携し、
仮想化技術によって分離された安全な環境下で、工場プラントとPLCを用いた実際の攻撃をリアルタイムに体験します。

対象

- OT/ICS担当部門として、有事に備えた実践的な訓練を積みたい方
- OT/ICSシステム部門とセキュリティ部門の調整役を担っている方
- 新しくOT/ICS又はセキュリティ部門に配属される方

受講者の声

製造業

ITとICSの連携が必要であると痛感。

製造業

APT攻撃の仕組みとそのフェーズごとにやるべきことを理解した。

Goal

制御装置への実際のサイバー攻撃を体験し、複数の検出・監視ツールを駆使してサイバーインシデントを検出し、その初期分析を行うためのスキルを習得します

プログラム

1. オープニングセッション
2. サイバーセキュリティの概念
3. アクティブディフェンスの概念
4. ハッカーの視点（SCADA）
5. Modbusプロトコル
6. WireShark概要&演習
7. ケーススタディ
8. アリーナインフラについて
9. ハンズオン演習
10. 演習振り返り
11. クロージングセッション

場所	赤坂アリーナ
期間	2日間
費用	30万円(税抜) /1人

(C) AMIYA Corporation

AMIYA
サイバーセキュリティトレーニング

Powered by CYBERGYM

(C) AMIYA Corporation