CyberBastion概要説明

CyberBastionとは

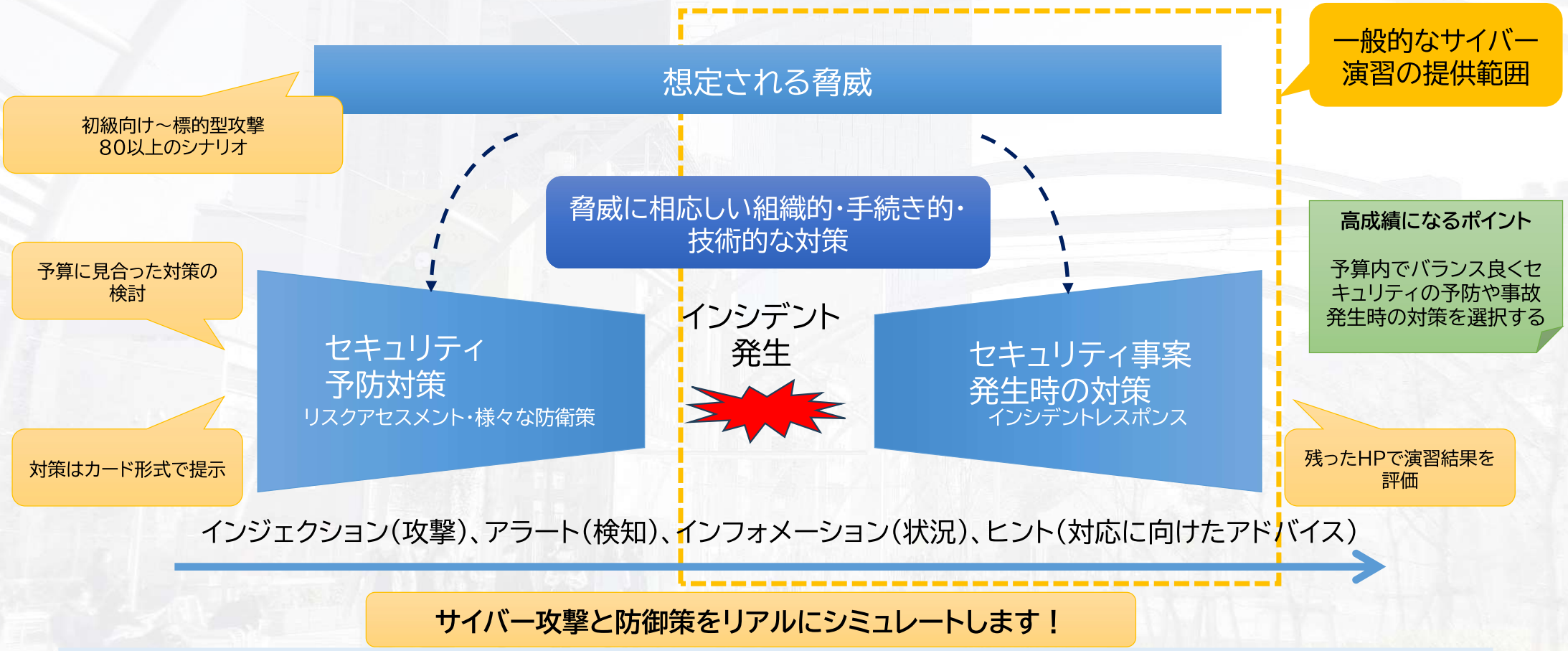
オンライン型サイバー演習プラットフォーム

1. セキュリティ担当部門の方をはじめ、セキュリティをこれから学ぶ一般社員や学生に対する初期研修にも活用できるサイバー演習
2. チームを作りゲーム感覚で楽しく演習することで組織全体の協力体制を強化できる
3. 脅威のシナリオが豊富で、最新の脅威にも対応できる
4. 与えられた予算内でバランス良く脅威に適合した対策の検討が出来るようになる

< InfoSec SEE 2024の様子>

CyberBastionを用いた演習の概要

脅威に対する事前・事後のセキュリティ対策検討の体験をとおし、実践的なセキュリティ対応能力を養います



サイバー攻撃と防御策をリアルにシミュレートします！

CyberBastionによる演習の流れ

■ オンラインのカード型演習
- 発生するイベントに対し、カードを選び被害を抑止

■ 全員の参加を確認したのち、概要が提示
- 開始すると、自動でシナリオが展開
- 各チームに予算とヘルスポイント(HP)が初期に付与
- 予算内でセキュリティ対策を選択し実施

2022年7月1日 午前4時、何者かによって防衛産業A社の従業員用正面玄関にマルウェアに感染したフラッシュドライブがばらまかれました。

彼らの目的は、企業のICTリソースを乗っ取ることで業務を妨害し、ITシステムで処理されているデータを奪うことでした。攻撃者らは、出勤前の従業員が 「サプライズ」 が仕掛けられたフラッシュドライブを見つけ、興味本位で会社のコンピュータに接続し、社内リソースにアクセス可能とすることを計画していた。

数人の従業員が路上に落ちているフラッシュドライブを見つけましたが、ほとんどは、社内で規定されている手順に従って、見つけたフラッシュドライブを検証するためにIT部門に引き渡しました。

しかし、内部監査部門のリンダさんだけは、拾ったフラッシュドライブの内容を確認するために、会社のコンピューターに接続しました。

モニターに表示されたファイルの中には、Bonuses_June_2022.xlsxという名前のエクセルファイルがあり、好奇心に駆られたリンダさんは、サイバー犯罪者からの「贈り物」が入ったファイルを開いてしまったのです。

■ イベントが発生するとチームのHPが減少
- 残っている予算と、途中追加される予算を使って、対策を進める

■ 演習終了
- 残ったHPで順位が決定

対策カードの内容

カード番号/カード名 ： (1)～(168)の168種類のカードがある

リスク管理

さまざまな種類の攻撃(例:マルウェア、フィッシング、DDoS)のリスクに直面する可能性のあるIT資産(ハードウェア、ソフトウェア、データ)を特定し、そのようなイベントの可能性と影響を推定します。
セキュリティの選択と実装の基礎。

カード説明 ： 対策内容の説明

カードの色 ： 対策のカテゴリを表す

- 【組織的対策】
- 【物理的対策】
- 【NW全体対策】
- 【NW境界対策】
- 【内部NW対策】
- 【ホスト対策】
- 【アプリケーション対策】
- 【データ対策】
- 【データソース】

カード価格 ： カード選択時点の予算内でカードを選択可能

各カテゴリの対策カード例

NTT AT

3 セキュリティ意識向上トレーニング 36 000 JPY	【セキュリティ意識向上トレーニング】 従業員のITセキュリティ意識向上のための活動。これには、脅威に関する知識、脅威を防止する方法、インシデント発生時および緊急時の対処方法が含まれ…
4 USBポートと外部記憶媒体の無効化 40 000 JPY	【USBポートと外部記憶媒体の無効化】 適切なGPOポリシーまたは専用のサイバーセキュリティアプリケーション(例:DLP)を設定することにより、情報漏えい対策セキュリティを実装します。…
34 アンチウイルスソフトウェア 88 000 JPY	【アンチウイルスソフトウェア】 コンピュータウイルスの検出、駆除を目的とするコンピュータプログラム。現在では、フィッシング、Web攻撃、DDoS攻撃など、他の多くの脅威からも保護す…
36 IT資産管理 128 000 JPY	【IT資産管理】 組織内で利用可能なICTリソースの情報を取得できるデータベースです。これは、使用されている機器のタイプ(ワークステーション、エッジデバイス、サーバ…
32 セキュアリモートアクセス 45 000 JPY	【セキュアリモートアクセス】 リモートアクセスを管理および実装するためのソフトウェアを使用することで、遠隔地にあるデバイスと安全に通信ができます。遠隔地での作業を扱う場合…
35 Anti-DDoSシステム 115 000 JPY	【Anti-DDoSシステム】 分散型サービス拒否 (DDoS) 攻撃は、サーバー、サービス、またはインフラストラクチャを使用不能にすることを目的としています。さまざまな手法を組…

11 ネットワークの分離 172 000 JPY	【ネットワークの分離】 組織内ネットワークを特定のユーザーグループ (会計、管理、生産など) 専用の小さなサブネット (セグメンテーション) に分割し、これらのセグメントとの間…
31 ネットワークトラフィックの暗号化 94 000 JPY	【ネットワークトラフィックの暗号化】 セキュリティで保護された通信とデータ交換を確保するために、ネットワークトラフィックの暗号化が使用されます。これにより、通信の盗聴や傍受、データ…
39 Webアプリケーションファイアウォール /WAF 138 000 JPY	【Webアプリケーションファイアウォール/WAF】 Webアプリケーションの保護に特化したツール。事前に定義されたルールを用いて、アプリケーションの送受信トラフィックを制御できます。ネガティブモデ…
52 アプリケーションのサンドボックス 45 000 JPY	【アプリケーションのサンドボックス】 目的は管理され制限されたコード実行環境を提供することです。これは、アプリケーションのソースが信頼できない場合に役立ちます。
67 証明書の登録 5000 JPY	【証明書の登録】 現在のデジタル証明書と期限切れのデジタル証明書 (例:証明書の透明性) に関する検索または記録された情報。
68 クラウドサービスの無効化 5000 JPY	【クラウドサービスの無効化】 クラウドサービスを無効化または停止するための情報 (例:AWS CloudTrail StopLogging) 。

【参考】シナリオ例

■APTグループによる攻撃、国家による攻撃、その他の危険なサイバー脅威など、現実世界のサイバー攻撃をシミュレートした80以上のシナリオを保有。四半期ごとに新しいシナリオか開発されるため、参加者は常に最新の課題や脅威を体験可能

シナリオ例

ランサムウェア	水飲み場から始まるランサムウェアキャンペーン。攻撃者は、侵害された国家金融規制当局のウェブサイトを使用して、被害者のコンピュータを感染させる
フィッシング	欧州各国の大使館を装ったフィッシングメールキャンペーン
トロイの木馬	リモートアクセス型トロイの木馬(RAT)を用いた金銭的動機に基づくキャンペーン

その他の標的型攻撃(APT)等の応用シナリオ

SolarWinds	国家を標榜するグループがSolarWindsのソフトウェア構築システムにアクセスし、バックドアを埋め込むことで、政府機関や民間企業など様々な組織のデータを閲覧し、盗みだした。
Trickbot	ハッカー集団がマルウェア[Trickbot]を使い、様々なシステムにアクセス、金融情報を含む機密データを盗み出した。
コロニアルパイプライン	ハッカー集団がコロニアル・パイプラインにランサムウェア攻撃を仕掛け、パイプラインの停止を招き、米国の複数の州で燃料不足が発生した。
Triton ICS	サウジアラビアの石油化学プラントの産業用制御システムを標的に、国家支援グループがTRITONマルウェアを使用し、安全システムを制御し、大惨事を引き起こす可能性があった。
ハーメチックワイパー	ハッカー集団がHermetic Wiperを使った破壊的な攻撃を仕掛けてきた マルウェアで、多数の組織のシステムからデータが消去された。
Lapsus$	国家に支援されたグループが、欧州の複数の組織を対象に、スピアフィッシングキャンペーンとカスタムバックドアを行い、機密データの窃取を狙った
UNC3524	中国の国家支援団体に関連するハッカー集団が、高度なサプライチェーン攻撃を用いて、政府機関やハイテク企業を含む様々な組織のシステムにアクセスした。
Uberへの攻撃	ハッカー集団がUberを標的にし、5,700万人以上の顧客とドライバーの個 人データを盗み出した。
APT41 Air India	国家に支援されたグループがエア・インディアを標的に高度なサイバー 攻撃を行い、乗客情報や旅行などの機密データにアクセスし、 履歴を閲覧できた。

CyberBastionの導入実績

■欧州の政府系、重要インフラ、企業などで幅広く活用

政府系： ポーランド大統領府

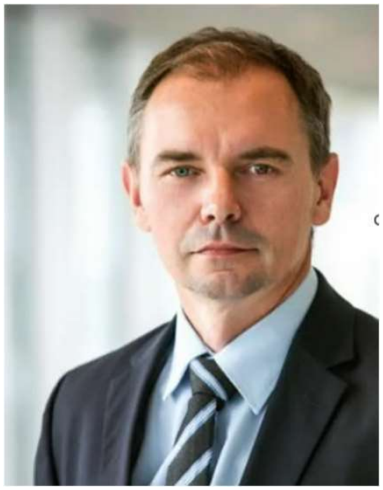
重要インフラ： ポーランド最大のN-GasPipeline

金融関係： 世界最大級の銀行、保険会社 等

教育： ポーランドの複数の大学での単位取得授業

その他： ITおよびセキュリティ関連の展示会やイベント

（参考）CyberBastionの開発背景等



- **FIRST会議等で著名なポーランドのMIROSLAW MAJ氏により提唱**
  - CERT-Polka（ポーランドのNational CSIRT）創設メンバー
  - ポーランド国防大臣顧問
  - ENISAの専門家でCERT等多数の出版物を共著
  - セキュリティ関連ツール開発
  - サイバー演習および若手育成を推進
- **リアルなカードゲームからオンラインプラットフォーム化へ**
  - 当初は、物理的なカードを用いてオンサイトで実施
  - オンライン化により、規模的・地理的にスケール可能に
- **欧州・米国への普及とマルチリンガル化**
  - 東欧から西欧、米国へと普及拡大。2024年はマルチリンガル化し、現在は日本語対応可能
- **シナリオ作成機能（シナリオエディタ）と教育用モジュール （2025年に向けて準備中）**

NTT-ATが提供する研修内容と想定ユースケース

NTT-ATが提供する研修内容(案)

トレーニングプラン例

Phase 1: 座学講義

- サイバー脅威の概要と対策
- セキュリティインシデントの流れとフェーズ
- 使用ツール(CyberBastion)の概要説明

Phase 2: CyberBastionを用いたサイバー演習

- 訓練用演習x2
- 本番演習x2
- 振り返り: トレーニングの成果と改善点のレビュー

想定されるユースケース

対象組織	特徴	課題	メリット
中小企業	セキュリティ専門部署を持たない、あるいはIT部門が小規模	リソースが限られている中、従業員のセキュリティ意識を高める必要がある	コストパフォーマンスが高く、簡単に導入できるトレーニングソリューション
大企業	セキュリティチームや専門部署を持ち、規模の大きい研修が必要	部署間連携を強化し、組織全体で統一されたセキュリティ意識を醸成する必要がある	カスタマイズ可能なシミュレーション訓練と進捗管理ツール
金融機関	金融庁のガイドラインを遵守しつつ、顧客情報保護の徹底が求められる	高度なセキュリティスキルを持つ専門職員と、基礎知識が必要な一般職員の両方に対応	実践的かつリアルな攻撃シナリオを提供するトレーニング

想定されるユースケース

対象組織	特徴	課題	メリット
医療機関	患者情報や機密データを扱い、セキュリティ対策が求められる	サイバー攻撃によるデータ流出のリスクを防ぎ、スタッフの教育を強化	短時間で効率的に学べるトレーニング
教育機関	学生や教職員向けに基本的なセキュリティ知識を普及させたい	費用面の制約がある中での効果的な学習手法の導入	安価かつゲーム感覚で学べるプラットフォーム
自治体	住民データや行政情報を保護するためのセキュリティ強化が必要	職員全体に対するセキュリティ意識向上のためのコスト効率が良いソリューション	簡単に導入可能で、実践的な研修内容

CyberBastionを用いた演習の流れ

Cyber Bastionによる演習の流れ

■ **オンラインのカード型演習**
- 発生するイベントに対し、カードを選び被害を抑止
- メンバはブラウザでCyber Bastionにアクセス。その際、指定されたIDでチームとして認識
- ブラウザでは、カードの選択画面とイベント発生を通知する画面がある

■ **全員の参加を確認したのち、概要が提示**
- 開始すると、自動でシナリオが展開
- 各チームに予算とヘルスポイントが初期に付与
- 予算内でセキュリティ対策を選択し実施
- 最初のうちは何も起きない→その間に予防的なセキュリティ対策を選択
- セキュリティ対策が150以上あるので、手分けして把握する必要あり

■ **イベントが発生するとチームのヘルスポイント(HP)が減少**
- 残っている予算でインシデント対応を実施
- 定期的に追加予算が配算されるので、その予算を使って、対策を実施

■ **演習終了**
- 残ったHPで順位が決定

演習の進め方

■ **チーム対抗戦**
- 1トークンで1チームの参加が可能。1チームのメンバ数は制限がないが、4～5名程度が理想
- ヘルスポイント(HP)が各チームに付与されており、イベントによりHPが減少。セキュリティ対策を行うことで、HPの減少を抑止。残ったHPが多い順で演習の順位が決定

■ **セキュリティ対策を予算内で選択し、演習内で発生するイベント(インシデント)に対処**
- 最初に攻撃の概要が提示されるので、イベントが発生するまでの時間で予防策を選択するのがよい
- イベント発生後、残った予算で事後対応を選択し、被害を抑止

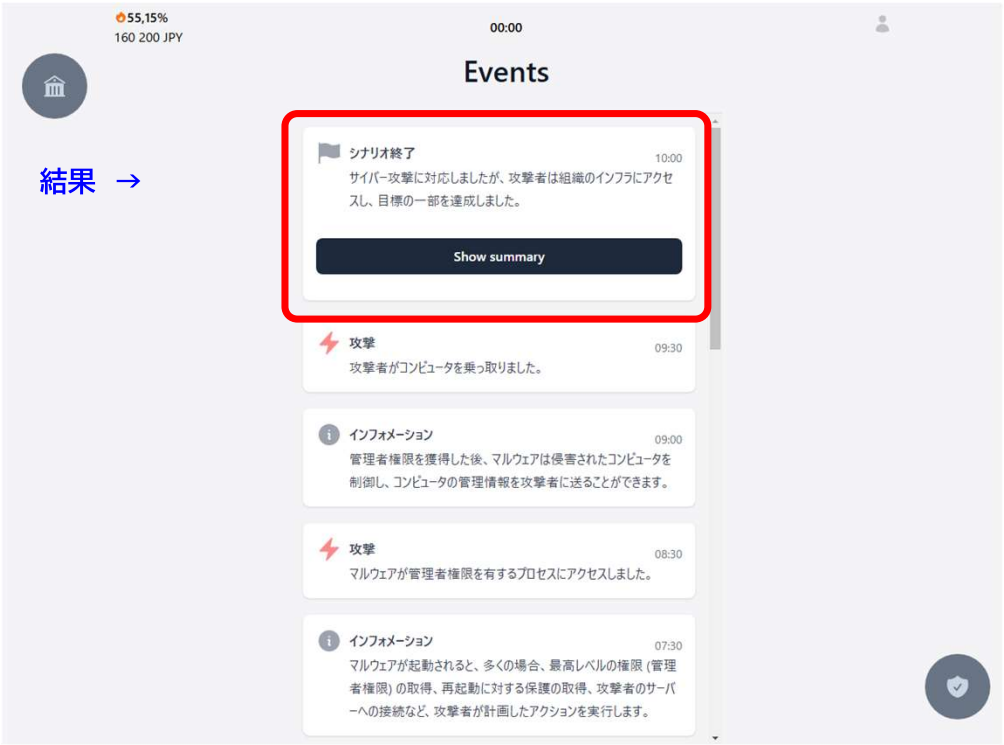
■ **セキュリティ対策が多いので、Gメンバで選択すべきセキュリティ対策の分野を割り当て、想定されるイベントに備えるのがよい**
- G内メンバで各々の得意分野があれば、その分野の対策を検討し互いに議論
- セキュリティ統括部隊、CSIRT等の役割に応じて議論
- または、一般社員同士が互いの経験や知識を基に議論

■ **オンラインチャット(Teams等)を用いて、意見交換を行いながらチームが活動することを想定**
- CBはブラウザがあれば、世界のどこからでもアクセス可能。CB画面とチャット画面を同時に表示し、議論しながら進めることを想定

演習実施中

司会者画面

終了後の画面



NTTアドバンステクノロジ株式会社は、IOWN構想を支える技術力と、国内外先端技術・ノウハウを強みとして、

不断のチャレンジを続け、「環境エネルギーとデジタル化」に貢献してまいります。