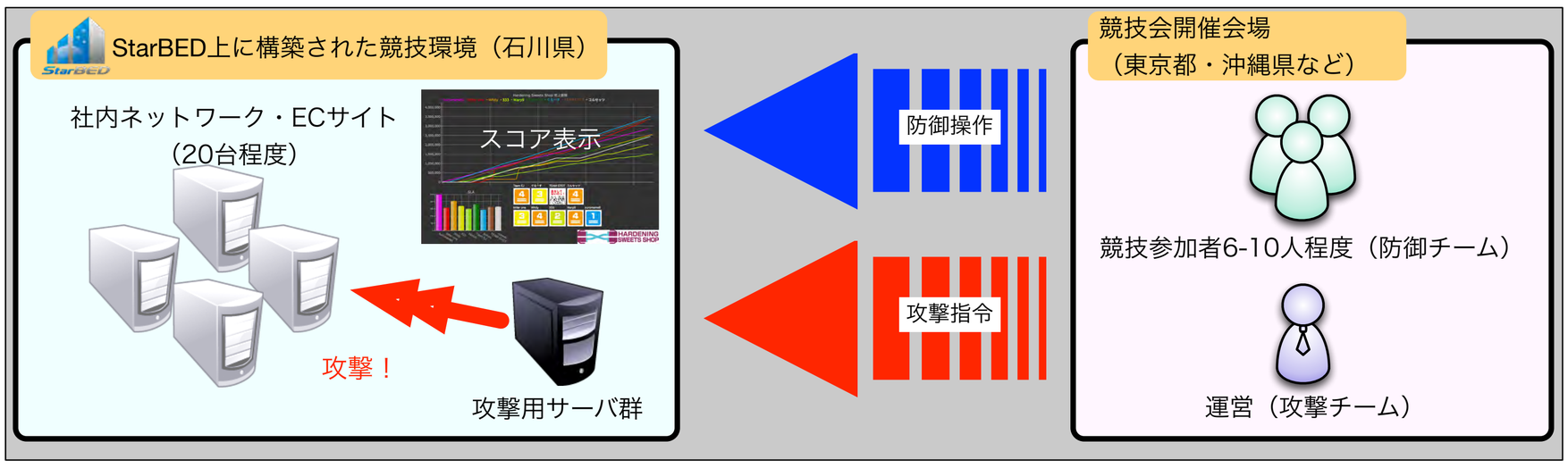
Contributions to Cyber Defence Trainings

高度化・頻繁化するサイバー攻撃に対する人材不足が叫ばれて久しい中、
さまざまな方面でセキュリティ人材の育成に貢献しています。

Hardening Project - 「衛る」技術を最大化するためのセキュリティコンペティション

攻撃する技術ではなく、実世界で必要となる「衛る」ための技術を検証するため一般からの参加者を募って実施されている競技会です。2012年4月の第1回目開催から過去6回すべての競技会においてNICTは特別協賛という形でかかわり、テストベッド研究開発推進センターおよびサイバー攻撃対策総合研究センターの物理的リソースとこれまでの知見、環境構築のための技術を提供し続けています。11月7日～8日にHardening 10 ValueChainを沖縄にて開催します。



Hardening 競技会は HardeningDayとSofteningDayから構成され、HardeningDayで実際の競技を、SofteningDayでは運営から競技中の攻撃内容の種明かしを、そしてそれぞれの参加者からはどのように攻撃の痕跡や脆弱性を確認し実際にどのように対応したかを共有することですべての参加者の経験値と意欲を向上させセキュリティ技術者としての次のステップへ踏み出す後押しをしています。

enPiT-Security(SecCap)- セキュリティ実践力のあるIT人材の育成

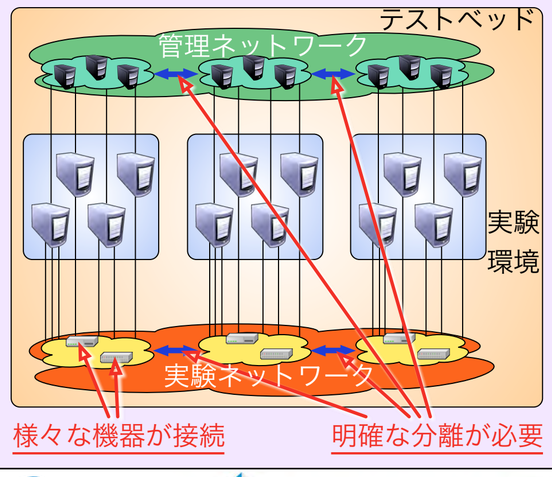
セキュリティを正しく理解し、実社会で活用できる技術を持つセキュリティ人材を育成するため、5つの連携大学（情報セキュリティ大学院大学、奈良先端科学技術大学院大学、北陸先端科学技術大学院大学、東北大学、慶應義塾大学）が実施しているこのプロジェクトに協賛し、手を動かして実践的なインシデントレスポンスを体験するための環境構築に技術や知見を提供しています。

サイバー人材育成環境構築を支える技術

StarBEDの研究開発・運営によって培ってきた技術に加えて、その上で行ったセキュリティ実験環境やサイバー人材育成イベントそのものへの参加により得られた知見を元に、環境構築のための用件の整理やそれに基づいた実践的なツールの開発を行っています。

セキュリティ実験のための テストベッド・サイバー人材育成環境

StarBEDおよびサイバー攻撃検証研究室で保有しているテストベッド環境は実験トラフィックと管理トラフィックの相互影響を排除するために実験側と管理側のネットワークをそれぞれ別に用意しています。StarBEDでは、管理の容易さから基本的に管理ネットワークは並列実行されるすべての実験で共通で利用して来ましたが、セキュリティ実験においてはインシデント漏洩を防ぐためそれぞれの実験環境を強固に分離する必要があります。また、セキュリティ実験で利用される機器は一般的なPCノードやスイッチだけではなく、攻撃模倣や観測、検知のための様々なアプライアンスを含むため、それぞれの設定の差異を吸収できる制御ソフトウェアが必要です。



必要とされる機能群

一般的なネットワーク実験環境を構築するための基本的な機能に加えて、実験全体で何がおこっているのかを常に確認する機能、万が一のことが起こった際に環境をすぐに物理的に切り離す機能などが必要になるため要求される機能群はより多く、また精度が高くなります。