

2013年9月25日

(報道発表資料)

NTTコミュニケーションズ株式会社
株式会社日立製作所
日本電気株式会社

サイバー攻撃解析・防御モデル実践演習の実証実験を 総務省より受託

～本日、サイバー攻撃に対する第1回目の実践的防御演習を実施～

NTTコミュニケーションズ株式会社（以下 NTT Com）、株式会社日立製作所（以下 日立）および日本電気株式会社（以下 NEC）は、総務省の「サイバー攻撃解析・防御モデル実践演習」の実証実験（以下 本実証実験）を受託いたしました。

本実証実験は、新たなサイバー攻撃に対応可能な環境を実現するため、攻撃の解析および防御モデルの検討を行い、官民参加型のサイバー攻撃に対する実践的な防御演習をするもので、第1回目の実践的防御演習を本日実施します。

本実証実験は、増加するサイバー攻撃に対応するため、官民の LAN 管理者および LAN 運用者のインシデントレスポンス（被害の早期発見・検知ならびに対処）能力の向上を目的としており、日常の運用を考慮しながら、事業継続を脅かす攻撃に対応できる「総合力の高い情報システム管理者」の育成を目指すものです。この一環として、総務省主催の「CYDER－実践的防御演習－」（注）を、本日を第1回目として、2013年度中に合計6回実施予定です。

本実証実験は、官公庁や企業の ICT インフラを担う LAN 管理者や LAN 運用者が2～4名構成のチームで参加し、参加チームごとに大規模 LAN を模擬した環境で標的型攻撃インシデントを体験します。インシデントの発生から対応、回復までのインシデントハンドリングについての一連の流れを体験することで、サイバー攻撃への対処方法を学ぶことができます。

なお、「サイバー攻撃解析・防御モデル実践演習の実証実験」とは、巧妙化・複合化する標的型攻撃等の新たなサイバー攻撃に対応するため以下の実証実験を行

うものです。(実証実験の全体総括は NTT Com)

(A) サイバー攻撃の解析 (担当: 日立)

標的型攻撃等の新たなサイバー攻撃情報の迅速・効率的な収集、正確な解析

(B) 防御モデルの検討 (担当: NTT Com)

サイバー攻撃被害の把握、ならびに対応 (インシデントレスポンス) を効果的・効率的に行うための知見集積ならびにモデル (手法) の確立

(C) 実践的防御演習の実施 (担当: NEC)

演習実施事例の調査研究、上記(A)及び(B)の成果を活用した演習プログラムの策定・実施・評価・検証

「実践的防御演習」の演習プログラム、開催予定については、別紙をご参照ください。

以上

(注) CYDER (サイダー): Cyber Defense Exercise with Recurrence
継続的に実施する実践的なサイバー防御演習

<演習に関するお客様からのお問い合わせ先>

NEC ナショナルセキュリティ・ソリューション事業部
社会セキュリティグループ

電話: (03) 3456-5915

E-Mail: cyber_nec@nss.jp.nec.com

<別紙>

● 演習プログラム

CYDER のプログラムは、各回 2 日間実施します。演習 1 日目の午前に講義、午後
に実機を用いた実習を行います。演習 2 日目の午後にグループワークを行います。

演習 1 日目	演習 2 日目
<p style="text-align: center;">午前</p> <p>■ 講義</p> <ul style="list-style-type: none">・ 最近の標的型攻撃事例の紹介・ 標的型攻撃への対策・ インシデントハンドリングの心得・ 実習環境・ツールの解説	<p style="text-align: center;">午後</p> <p>■ グループワーク</p> <ul style="list-style-type: none">・ 各チーム報告書の発表・ 質疑応答／講師講評 <p>■ クロージング</p> <ul style="list-style-type: none">・ スキルチェックテスト／アンケート
<p style="text-align: center;">午後</p> <p>■ 実習</p> <ul style="list-style-type: none">・ 演習環境の把握・ 監視・分析業務・ インシデントハンドリング・ 報告書作成	

