2015 年 10 月 26 日

報道関係各位

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

総務省主催の「実践的サイバー防御演習（CYDER)」を実施

～「サイバー攻撃複合防御モデル・実践演習の実証実験」の一環～

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、総務省から受託した「サイバー攻撃複合防御モデル・実践演習の実証実験」の一環として、今年度第 1 回目の「実践的サイバー防御演習（CYDER)」(注)を本日から実施します。

（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

CYDER は、増加するサイバー攻撃に対応するため、官民の情報システム管理者のインシデントハンドリング（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」の養成を目指すものです。2015 年度は、今年度に発生した大規模な情報流出事案をカリキュラムに取り込み、本日を第 1 回目として、合計 6 回（200 名以上）を実施する予定です。

＜CYDER の特長＞

官公庁や重要インフラ事業者等の情報システム管理者が 3～4 名構成のチームで参加し、参加チームごとに大規模（職員が数千人規模）な模擬 LAN 環境で情報セキュリティ事故の発生から回復までの一連のインシデントハンドリング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。

演習は技術的な対処だけでなく、部門内への指示やエスカレーション、社外の関係機関との情報連携など被害拡大を防止するために重要な対処も体験できます。

CYDER 演習プログラム、「サイバー攻撃複合防御モデル・実践演習の実証実験」の概要は、以下の通りです。

＜CYDER 演習プログラム＞

演習１日目	演習２日目
午前 **■ 講義** ・最近の標的型攻撃事例等の紹介 ・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	**午前** **■グループワーク** ・講師による解説 ・質疑応答 ・実機による確認 **■クロージング** ・スキルチェックテスト／アンケート
午後 **■実習** ・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	

＜「サイバー攻撃複合防御モデル・実践演習の実証実験」の概要＞

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行うもの。

(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）

・標的型攻撃などのサイバー攻撃及びインシデントレスポンス事例の調査研究

・サイバー攻撃に対する検知、対策（予防対策・事後対策）及びインシデントレスポンスから構成される防御モデルの確立

(C) 実践的サイバー防御演習の実施（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

以上