INFORMATION★EXPRESS　No.1081

C-LINE

✧　発　行：中国情報通信懇談会
✧　TEL:082-222-3324　FAX:082-502-8152
✧　E-mail:jimukyoku@cic-infonet.jp
✧　http://www.cic-infonet.jp/

《中国情報通信懇談会／会員情報》

実践的サイバー防御演習「CYDER」

１０／３１（木）福山市内（初開催）

１１／８（金）山口市内

令和元年10月31日(木)福山市内、11月8日(金)山口市内において、実践的サイバー防御演習「CYDER」を開催しますので、ご案内いたします。

開催日程や、登録方法など演習の詳細につきましては、下記参考URLをご参照ください。

演習の受講にあたりましては、国や自治体を除き、実費をご負担いただく必要がございますが、本演習は、NICT が有するサイバーセキュリティに関する技術的知見と大規模計算環境を最大限に活用して実施している実践的な演習となっており、サイバー攻撃対策を学ぶよい機会になるものと存じます。

ぜひ、受講につきまして、ご検討ください。

実践的サイバー防御演習「CYDER」とは

昨今、行政機関や重要インフラ事業者等を狙ったサイバー攻撃はますます巧妙化する傾向にあり、機密情報漏えい等の被害は甚大なものとなっています。組織を標的としたサイバー攻撃への対策については、攻撃手法の解析が困難であることや攻撃を受けた後の対応が確立されていないこと、情報システム担当者等の対応能力の不足が指摘されているなど、十分とは言えない状況です。

このような状況を踏まえ、総務省では平成 25 年度から、サイバー攻撃への対応能力の向上を図ることを目的として、サイバー攻撃によるインシデント発生時の一連の対処方法を体験するための実践的サイバー防御演習「CYDER」をスタートさせました。

平成 28 年度からは、演習の質の向上や継続的・安定的な運用を実現するため、実施主体をNICTに変更し、平成 30 年度からは、重要インフラ事業者向けのコースを新設して、金融、交通インフラ、医療、教育研究機関等向けにそれぞれ最適化したシナリオを用いて演習を行うなど、さらなる内容の充実を図っています。

参考URL

NICT ホームページ【実践的サイバー防御演習「CYDER」】

https://cyder.nict.go.jp/

サイバーセキュリティ対策の重要性について

サイバー攻撃とは…？

・ 標的の**コンピュータやネットワークに不正侵入**し**データの破壊・改ざん**等を行なったり、**システムを機能不全**に陥らせること。

・ サイバー攻撃を受けた場合の実例

①住民とのメールによるやりとりや、LGWANを通じた他自治体とのやりとりが不能になります。

→ **平成27年6月、標的型攻撃により上田市役所庁内LANをインターネット及びLGWANから切断する事態となった。**

②自治体の職員用PCが不正アクセスやウイルス感染により不正に遠隔操作されます。

→ **令和元年5月、山口県立大学の職員メールアカウントが乗っ取られ大量の迷惑メールが送信された。**

③不正にファイルが暗号化され、データアクセス不能になります。

→ **平成29年5月、川崎市上下水道局のインターネット接続端末が身代金要求ウイルス(ランサムウェア)に感染。**

サイバーセキュリティ対策は三層分離のみでは不十分！

・ハード面(三層分離、ワクチンソフトの導入等)のセキュリティ対策が万全であっても、**人為的なミスによってインシデントが発生する場合があります**。また、インシデント発生時に備えた**体制の整備が不十分であると被害が拡大**します。

→ **ソフト面の対策（セキュリティ人材の育成、インシデント即応体制の整備）も重要。**

住基ネット

LGWAN

インターネット

CYDERの受講によりソフト面の対策も可能となる

・CYDERではインシデントの発見、初動対応及び報告等の**インシデントハンドリングを一通り体験**することが可能です。

・CYDERは**初心者の方でも受講可能**です。(特にAコースは初心者向けのコースとなっております。)