『ビジネス』を護る サイバーセキュリティデイズ 2019

東京2020オリンピック・パラリンピックを控え、日本の企業等がサイバー攻撃の格好のターゲットになることが懸念されています。特に優良な情報や資産を持つ中小企業はランサムウェアなどの標的になりやすく、企業存続にかかる重大な打撃を受けかねません。

今回は、経営層が把握すべきサイバー攻撃のリスクと対策を分かり易く解説するとともに、セキュリティ担当者がゲーム感覚でサイバー攻撃に対処する能力の向上を目指す実践的訓練を併せて実施します。

こんなお悩みはありませんか

- どのようなリスクがあるか分からない
- **我社のセキュリティ対策に不安がある**
- セキュリティ担当者の確保が難しい

Practice Day

2019年 2月 6日(水)　午後 1:00-6:00
金沢商工会議所　金沢市尾山町9-13

定員 60名 参加無料

セキュリティ担当者を対象にゲーム感覚でサイバー攻撃に対処する能力の向上を図る実践的訓練(Micro Hardening)を実施。詳しくは裏面をご覧ください。

Seminar Day

2019年 2月 7日(木)　午後 1:30-5:00
金沢東急ホテル　金沢市香林坊２-１-１

定員 150名 参加無料

ファシリテータ　篠田 陽一 氏　　北陸先端科学技術大学院大学教授／内閣サイバーセキュリティセンター補佐官／国立研究開発法人情報通信研究機構　R&Dアドバイザー

講演1　サイバーセキュリティ政策の最新動向
　講師　木村 公彦 氏　　総務省 サイバーセキュリティ統括官室 参事官(総括担当)

講演2　東京2020に向けたサイバーセキュリティ対策　～過去大会の教訓を企業で活かす～
　講師　中西 克彦 氏　　NEC ネクサソリューションズ株式会社／公益財団法人東京オリンピック・パラリンピック競技大会組織委員会

講演3　インシデント例から学ぶセキュリティ対策の重要さ　～ 今すぐできるリスク評価 ～
　講師　森島 直人 氏　　EYアドバイザリー・アンド・コンサルティング株式会社 シニアマネージャー

講演4　事業継続を意識したサイバーセキュリティ対策の実践 ～Micro Hardeningの活動を通して得られたこと～
　講師　川口 洋 氏　　株式会社川口設計　代表取締役

申込方法

【Micro Hardening】次のwebページからお申し込みください。
https://microhardening.connpass.com/event/115017/
【セミナー】電子メールに参加希望者の「所属」、「氏名」を記載して次のアドレス宛にお申し込みください。 hokuriku-jigyo@soumu.go.jp

締切 1/30(水)

主催：総務省北陸総合通信局、北陸情報通信協議会、国立研究開発法人情報通信研究機構、北陸経済連合会(順不同)

協力：中部経済産業局電力・ガス事業北陸支局、富山県警察本部、石川県警察本部、福井県警察本部、富山県商工会議所連合会、石川県商工会議所連合会、福井県商工会議所連合会(調整中)

お問合せ：国立研究開発法人情報通信研究機構　北陸StarBED技術センター　(石川県能美市)　tel 0761-51-8118

（ファシリテーター）

篠田 陽一 氏　北陸先端科学技術大学院大学　教授
内閣サイバーセキュリティセンター　サイバーセキュリティ補佐官

- 情報環境、ネットワーク分散情報システム、ソフトウェア開発環境の研究に従事。
- 2007年より 内閣官房情報セキュリティセンター　情報セキュリティ補佐官
- 2015年より 内閣サイバーセキュリティセンター　サイバーセキュリティ補佐官

（講　師）

木村 公彦 氏　総務省 サイバーセキュリティ統括官室　参事官（総括担当）

- 1992年、郵政省（現総務省）入省。総合通信基盤局事業政策課統括補佐、情報通信研究機構ワシントン事務所長、総務省総合通信基盤局事業政策課調査官、警察庁長官官房国際課国際協力室長、総務省情報通信国際戦略局国際協力課長などを経て、2018年7月より現職。

中西 克彦 氏　NEC ネクサソリューションズ株式会社／公益財団法人東京オリンピック・パラリンピック競技大会組織委員会

- NECネクサソリューションズ入社後。WAFの開発、セキュリティ診断業務、社内外のインシデントレスポンスに携わる。省庁や重要インフラ向けサイバー演習のシナリオ作成および講師を担当。
- 2015年より(公財)東京オリンピック・パラリンピック競技大会組織委員会に出向、CSIRT構築、演習の検討、政府組織との 連携などを推進。
- ISOG-J 運営委員、ISLA™2017、CISSP

森島 直人 氏　EYアドバイザリー・アンド・コンサルティング株式会社 シニアマネージャー

- 奈良先端科学技術大学院大学で教鞭をとった後、公認会計士を取得
- 監査法人にて情報セキュリティマネジメントシステムやCSIRT、脆弱性管理態勢等の構築、情報セキュリティ対策に係る整備及び運用の外部評価等に従事。（工学博士）

川口 洋 氏　株式会社川口設計　代表取締役

- 2002年 大手セキュリティ会社に入社。社内のインフラシステムの維持運用業務ののち、セキュリティ監視センターに配属
- 2013-2016年 内閣サイバーセキュリティセンター(NISC)に出向。行政機関のセキュリティインシデントの対応、国民向け普及啓発活動などに従事
- 2018年 株式会社川口設計 設立

Micro Hardening とは

Micro Hardening は「衛る技術の価値を最大化することを目指す」プロジェクトであるHardening Projectから生まれたサブプロジェクトであり、「ゲーム感覚で」サイバー攻撃に対処する能力を磨くことを目指すものです。

参加者は4人一組となり、45分という限られた時間のなかで、提供されたECサイトに対する様々なサイバー攻撃に対処することが求められます。

ECサイトで買い物を行うクローラ（買い物ロボット）が購入した金額が得点となり、さらに防いだ攻撃に応じたボーナス得点が得られ、ECサイトを安定稼働させることが高得点につながります。

45分を1セットとし、3セット繰り返すことで、毎回少しずつ攻撃の状況を観測し、対処方法を試すことで、エンジニアとしての能力向上を図ります。

◆参加者に準備いただくこと（セミナー参加者は必要ありません）

・ノートパソコンと電源
・SSHターミナルクライアント（必須）　Windowsの方はTeratermセットが便利
・VNCクライアント
・LinuxサーバにSSHでログインしてコマンドが打てること
・自分のパソコンのhostsファイルを編集できること（管理者権限を持っていること）