マンガで
わかる！

株式会社川口設計プロデュース

サイバー攻撃対応トレーニング
Micro Hardening

「知っている」から「対応できる」にするために

川口設計

株式会社 川口設計

〒101-0051　東京都千代田区神田神保町 2 丁目 2 番 202
E-mail：info@sec-k.co.jp
HP：https://www.sec-k.co.jp/

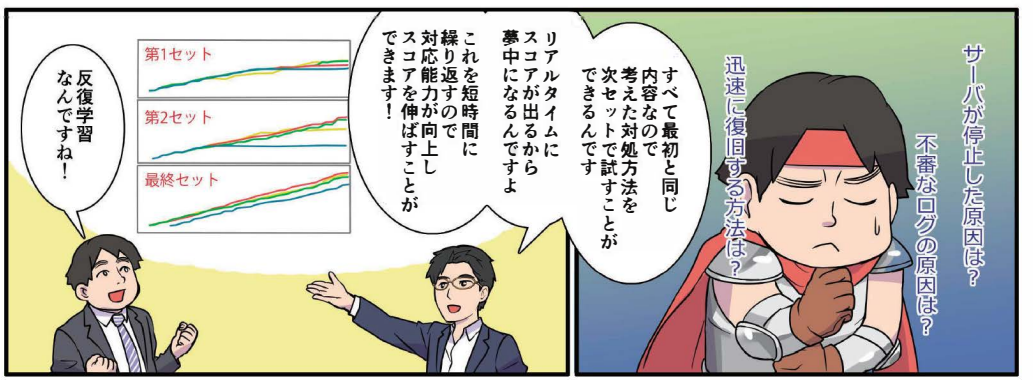
競合会社β社が
不正アクセスを受け
サーバーダウンだけでなく
対応が遅れたため
情報漏洩を引き起こした
同じような
攻撃を受けた場合
うちはちゃんと
対応できるのか？
えぇっと…
α社
CISO　上野 茂樹
いろいろ
セキュリティ対策は
やってるんですが
同じことが起きても
見つけられるか
どうかは
わかりません
α社
情報システム部
部長　中西 大介
わからないとは
どういうことだ！
自社のシステム
だろう！
外部のベンタさんに
お願いしている
部分が多くて
自社で対応している
人間が少ないんですよ！
セキュリティ
インシデントに
対応した経験も
少ないですし…
バンッ
お前が担当して
いたじゃないか
チームの育成は
どうなったんだ
IT全体でやらなければ
ならない事が多くて
まだ教育できて
いないんですよ…
つまり
社内で対応できる人材も
事前に問題に気づく人材も
今ほとんどいない
ということなんだな？
た、大変申し訳
ありません…
なぁ～
形だけのCSIRTじゃあ
β社の事例は
ひとごとじゃないぞ…
あの…
実はその対策に
取り入れて
いただきたいものが
ありまして…
取り入れたい
もの？
『MicroHardening』
というトレーニング
です
マイクロハードニング
数日前――
株式会社川口設計
代表取締役
川口 洋
『MicroHardening』で
CSIRTを担うメンバーに
トレーニングするのは
どうでしょう
トレーニング？
自社内で
対応できる人材を
育てておくべきかと
思いまして
何かあったときに
取引先のベンダさんに
対応してもらう必要も
ありますが
社内の調整も含めて
対応できなければ
会社を守ることが
できません
CISOや経営会議に
報告するのは
中西さんですよね？
うぅっ…
ですが
うちの社員も
研修を受けに行ったり
書籍を読んだりして
色んな事案を
知っているはずなので
できなくないかと…
『知っている』と
『対応できる』では
大分違いますよ！
部長になった
中西さん一人で
ずっと対応する
わけにもいきませんよね
チームを育てないと
た、確かに…
その人のたちのために
「教育」と「レベル維持」かつ
セキュリティインシデントに
対応する
「スピード感」や「緊迫感」も
経験してもらえるので
オススメな
トレーニング手段ですよ
若手もベテランも
一緒にできるん
ですか？
もちろん！

擬似サイバー攻撃対応を複数回繰り返すものでして
よりカジュアルにゲーム感覚で能力を磨くことができるんですよ
スコアも出ますしね
サイバー攻撃
VS
エンジニア

くりかえし45分
大事なことは1回45分の短い演習を『繰り返しやる』ことです

演習の内容ですが体験できれば「対応できる」に成長できるものを盛り込んでいます
・意外に気付いていない問題
・ちょっとしたミスから発生した問題
・知っていれば防げていた問題

演習はセットごとにリセットされ
演習開始時には同じ環境で実施します


サーバが停止した原因は？
不審なログの原因は？
迅速に復旧する方法は？
すべて最初と同じ内容なので考えた対処方法を次セットで試すことができるんです
リアルタイムにスコアが出るから夢中になるんですよ
これを短時間に繰り返すので対応能力が向上しスコアを伸ばすことができます！
第1セット
第2セット
最終セット
反復学習なんですね！

またこれは4人1組のチームでチャレンジしていただきます
4人？個人じゃないんですか？
個人の能力を組み合わせて組織を守るところに目を向けてもらうためですよ
コミュニケーション
一人で完結する仕事はあまりありませんよね
「チームで協力して対応する」という経験が重要なんです
個人の力を伸ばすトレーニングは他にもありますし

また
チームでの役割分担
対応記録の取得
情報共有など
技術外の対応も合わせてトレーニングさせる目的です
自分が普段運用しているシステムなので分かっているつもりでもいざというときに動けない…
なんてことはよくあります
ギスギス

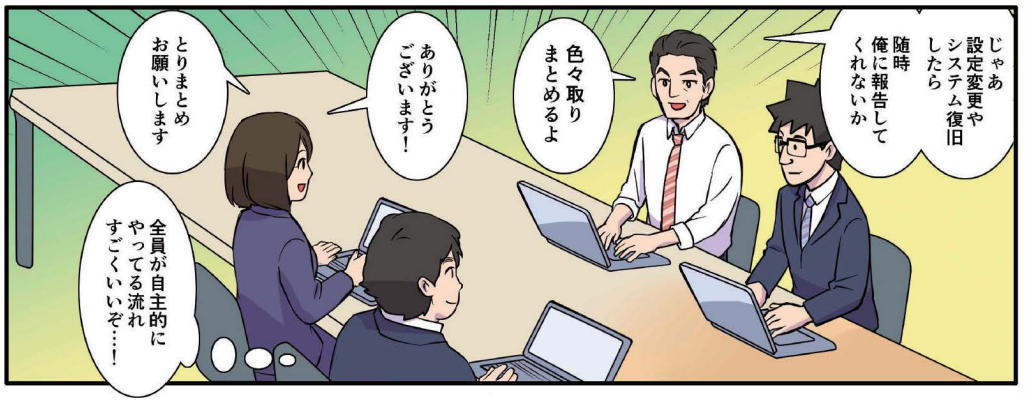
このトレーニングは※サイバーコロッセオにも採用されています
実践的な教育でチーム全体の刺激になりますし
中西さんの悩みを払拭できるかと思います！
※NICTナショナルサイバートレーニングセンター主催
東京2020オリンピック・パラリンピック競技大会の
適切な運営に向けた実践的な演習事業

ベテランエンジニアの知見やデキるエンジニアの手法を見て学ぶチャンスにもなりますよ
確かに！なかなか見る機会ないですもんね

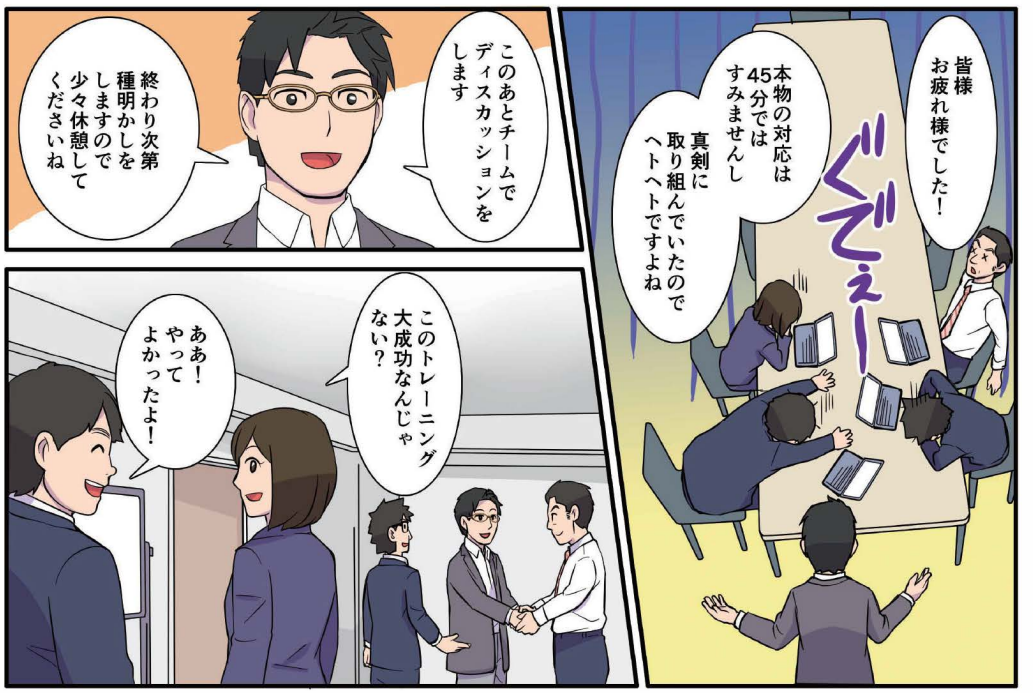
ぜひ弊社でも取り入れたいです！
ちょっと持ち帰らせてください！
連絡おまちしています！

しばらくして――
――では
これから皆様には
『MicroHardening』に
チャレンジして
いただきます
今からクラウド上に
構築したWebサイトに
様々なサイバー攻撃が
やってきますので
自分が普段
運用している
システムのつもりで
守っていただきます！
1セット45分
4人1組の
チームという
制約以外は
自由に対応して
いただいて構いません
まずは1回
トライしてみましょう
先輩の足を
引っ張らないかな…
α社
CSIRT担当
津村 健人
α社
CSIRT担当
佳山 一郎
α社
CSIRT担当
伊藤 綾
座学で
セキュリティ教育を
受けたことはあるけど
できるかしら……
うちのシステムと
違うが大丈夫
だろうか…
このメンバーで
どうやって
やるかな
前のスクリーンに
スコアを表示するので
順調に伸びて
いくように
頑張ってください
それでは……
スタートです！
皆さん
グラフが横ばいに
なっていますよ
ぐんっ
つー…
システムが
止まってますよー
本番だったら
お客様から
クレームですね
ホントだ！
何が起きて
るんだ…？
何が原因
かしら？
ここの
サービスが
止まってるぞ
じゃあ
このコマンドで
起動して…
おおっ
スコアがまた
上昇しはじめ
ましたね
おや
ホームページが
改ざんされて
そうですね
そんなことで
大丈夫ですかー？
誰か
ホームページ
確認してるか!?
見ていますけど
何かおかしい
ですかね…？
ちゃんと
チェック
してるかー？
ここ
やられてるぞ！
直さなきゃ
じゃあ私
修正して
おきます
先輩たち
みんなすげー……！
僕も
何かしなきゃ！
あれ
誰かパスワード
変えた？
あっ
すみません！
脆弱なもの
でしたので
取り急ぎ変更して
おこうかと…
ログインエラー

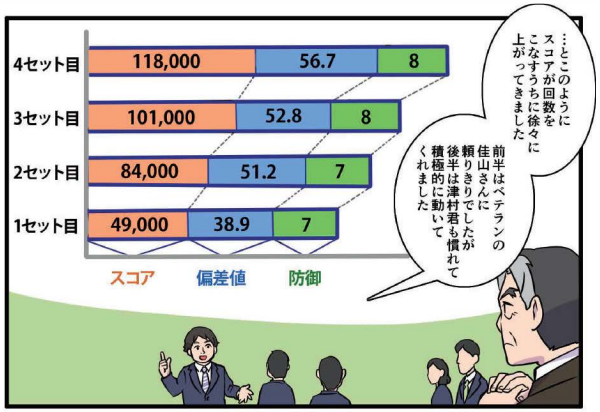
そっかありがとな！
いやいや…
対応はありがたいけど
変更したら随時共有してね
すっすみません！

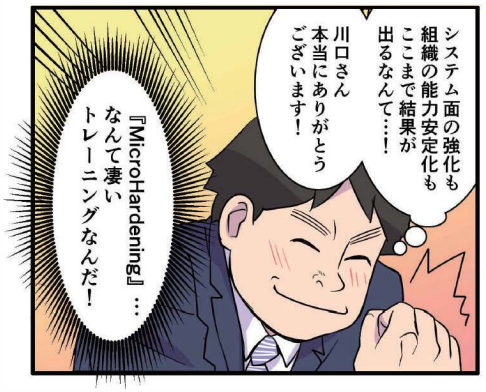

じゃあ設定変更やシステム復旧したら随時俺に報告してくれないか
色々取りまとめるよ
ありがとうございます！
とりまとめお願いします
全員が自主的にやってる流れすごくいいぞ…！

～4セット目が終了～


皆様お疲れ様でした！
ぐでぇー
本物の対応は45分ではすみませんし真剣に取り組んでいたのでヘトヘトですよね
このあとチームでディスカッションをします
終わり次第種明かしをしますので少々休憩してくださいね
このトレーニング大成功なんじゃない？
ああ！やってよかったよ！

・実践的だったため
知識だけだったものが
実際にできるようになった
・自分のスキルアップにつながった
ぜひもう一度受けたい！
・先輩がどのように対応しているか
わかってよかった
先輩のようになりたい
セキュリティの知識だけではなくチームワークという意味でもいい経験になっております


4セット目 118,000 56.7 8
3セット目 101,000 52.8 8
2セット目 84,000 51.2 7
1セット目 49,000 38.9 7
スコア 偏差値 防御
…とこのようにスコアが回数をこなすうちに徐々に上がってきました
前半はベテランの佳山さんに頼りきりでしたが後半は津村君も慣れて積極的に動いてくれました


システム面の強化も組織の能力安定化もここまで結果が出るなんて…！
川口さん本当にありがとうございます！
『MicroHardening』…なんて凄いトレーニングなんだ！

中西用意頼んだぞ
はい！

素晴らしい結果だな！
よし次年度の新卒研修にも『MicroHardening』を導入しよう

セキュリティ問題で悩む人を一人でも減らしたい
そんな想いで今後も活動していきます。

多くのベテランエンジニアはセキュリティを含むさまざまなトラブルを経験することで育ってきました。
しかし現在のビジネス環境ではトラブルから学ぶという余裕もない状況も多くあります。
MicroHardeningでサイバー攻撃の対応経験を積んでもらえば「知っている」が「できる」に変わります

株式会社川口設計

会社方針

株式会社川口設計は「自助」「共助」「公助」の視点から日本のサイバーセキュリティ向上に取り組みます。

■ 自助

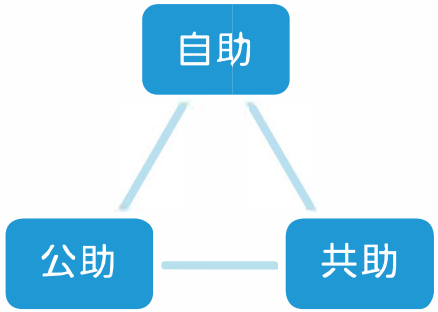
「セキュリティに関する
ちょっとした知識と体験」で
効果が出る対策を提供したい

■ 共助

コミュニティに育ててもらった
恩をコミュニティに返したい

■ 公助

日本のサイバーセキュリティを
守りたい



サービス内容

人材育成・トレーニング

サイバーセキュリティに関する
トレーニングを提供します。

- サイバー攻撃対応トレーニング「Micro Hardening」
- サイバーレンジ提供

顧問・アドバイザー

サイバーセキュリティに対する疑問・不安を
解決するためのお手伝いをします。

- 民間企業
- 公共機関 など

コンサルティング

セキュリティシステムやサービスの
設計・構築・運用の支援を行います。

- SOC 支援　・CSIRT 支援
- セキュリティ製品評価支援

啓発活動・リテラシー向上

セキュリティに関する理解度および
認知度向上のためのプレゼンテーション
講義を行います。

- 経営層向け　・CSIRT 向け
- 一般ユーザ向け

■ トレーニング提供について 現状のサイバー攻撃対応の課題

現状のサイバー攻撃対応の課題は下記が考えらます。

知識の問題

- セキュリティに関する基本的な知識が不足している
- セキュリティに関するトレーニングが退屈で敬遠される

実践の問題

- 知識はあるが、経験が不足しており、緊急時に対応できない
- 手順書や規定が整備されているが、対応のスピード感や温度感がわからない
- システム運用を軽視した対応で障害が引き起こされる

組織の問題

- システムの資産管理ができていないため、対策に漏れがでている
- 対応能力の向上は個人の取組に依存しており、組織として対応できない

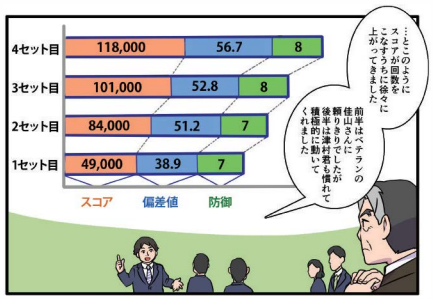
この課題を解消するために、エンジニアが手を動かして、繰り返しサイバー攻撃対応を経験するトレーニング **「Micro Hardening」** を提供しています。

Micro Hardeningとは

45分を1セットとしたサイバー攻撃対応を4人1チームで複数回繰り返し、サイバー攻撃対応能力の向上を目指します。毎回同じ攻撃が行われるため「現状調査」「防御」「復旧」「痕跡調査」を繰り返し知識を経験として定着することができます。

■ サイバー攻撃を「知っている」から「対応できる」に

サイバー攻撃に関する知識に体験を加えることで、企業のシステムを支えるエンジニアのセキュリティ対応能力を強化します。



活用シーン

- インフラエンジニアの攻撃被害疑似体験
- CSIRTチームやSOC担当者の対応訓練
- システム開発、運用エンジニアの対応訓練
- 新入社員研修におけるセキュリティスキル向上

■ 複数セット繰り返すことの効果

第１セット

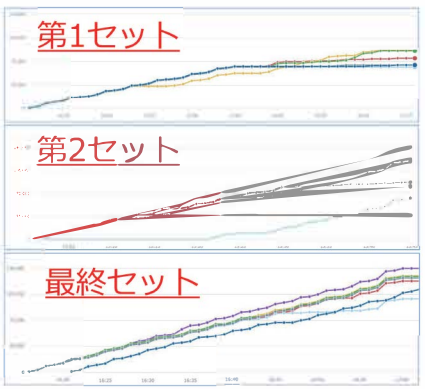
様子見。スコアは上がらず。環境に慣れていないため、多くのグループのスコアが中盤から停滞します。ここで発生した攻撃を次のセットの対応にどのように生かすかが重要です。

第２セット

徐々にスコアが上がりますが、セキュリティ対策で障害になるグループも。本トレーニングでは、システムの安定稼働を前提としたセキュリティ対策の実施を行うことが求められます。

最終セット

全体的にスコアが上がります。ほとんどのグループが攻撃の防御、システムの復旧を行うことができるようになることに加え　、45分の演習を複数回繰り返すことで対応能力が向上したことを実感できます。



▲ スコア例

マンガ内の Micro Hardening は
小さなシステムでの演習を
やってもらいました。もっとリアルで
ハードなものを体験したい場合
「Hardening Project 」のイベントにも
参加してみてください。お待ちしています！

Hardening Project
ホームページ