サイバー演習による インシデントハンドリング能力の強化

矢野 由紀子　伊藤 篤史　舩越 健生　佐藤 和代

要 旨

サイバー攻撃による脅威が深刻化する状況のなかで、サイバー攻撃に対応できる人材の育成が喫緊の課題となっています。NECでは、このような人材が持つべきスキルは何か、また、実際にサイバー攻撃を受けた際にどのような対応をすればよいのかを検討し、有効な研修プログラムの開発に取り組んできました。本稿では、複数の事例とともに、NECが提供しているサイバーセキュリティ実践演習の開発における考え方を紹介します。

KeyWords　人材育成／サイバー演習／インシデント対応／インシデントハンドリング／サイバー攻撃／CSIRT

1. はじめに

サイバー攻撃の高度化により、情報資産や事業継続に対する脅威が高まっているなか、企業や団体におけるセキュリティ人材の不足は深刻な問題になっています。またスマートフォンやSNS、IoTなどの普及は、セキュリティに携わる人に求められる知識や能力を一段と複雑なものにしています。

セキュリティ人材不足の傾向は世界的に生じており、国内と同様に海外でも政府系ウェブサイトが改ざんされるなどの深刻なセキュリティインシデントが発生しています。このような問題に、適切に対処することができる人材の育成に対する需要はより高まっています[1)]。

本稿では、サイバー攻撃の脅威に対し適切に対処するための人材スキル定義、及びその人材を育成するための演習プログラム開発について説明するとともに、国内及びASEANにおいて実際に取り組んだ事業について紹介します。

2. どのようなセキュリティ人材の育成が必要か

本章では、サイバー攻撃の脅威に適切に対処するために必要な人材について考えます。

2.1 組織内CSIRTと人材育成

企業や組織では、サイバー攻撃に対処するためにファイアウォールやIPSなどのセキュリティアプライアンスの導入を積極的に進めています。

このようなセキュリティシステムの運用者を育成するための研修は、製品メーカーが提供するプログラムだけでなく、SIベンダーなどからも趣向を凝らしたプログラムが豊富に提供されており、テクニカルスキルの拡充に貢献しています。しかし、テクニカルスキルだけでは激化するサイバー攻撃に適切に対処することはできません。このような状況からCSIRT（Computer Security Incident Response Team）を立ち上げる組織が多くなっています。CSIRTは、セキュリティインシデントに一元的に対応するための組織です。情報セキュリティに関連する窓口が集約され、外部機関との連携も取りやすくなることが期待されます（**図1**）。

2.2 CSIRTに要求される人材像

サイバーセキュリティインシデントが発生した時、CSIRTには、発生している事象の解明や被害拡大の防止だけでなく、組織活動を継続させることが求められます。

組織の活動を維持するためには、状況を俯瞰的に把握

●インシデント発生時における窓口・情報の一元化
- 多部門がかかわるケースでの部門間調整(横・縦)
- 組織外からの通報窓口、他組織への働きかけ

●対応ノウハウの蓄積
- 攻撃手段の変化、高度化に伴う事前準備の必要性
- 経験値を増やすことで、より確実な対応が可能に

●外部との信頼の構築
- FIRST、APCERT などのフォーラムを利用した外部との連携

図1　CSIRTの利点

CRIST の要員には、テクニカルスキルのみでなく、外部組織や他のメンバーとの連携能力などの高いヒューマンスキルが要求される

タイプ	スキルの概要
ヒューマンスキル	・明確な指示や取り決めなどがなく、時間的制約がある状況下でも、必要なことを受け入れ、判断できること ・業務内容の異なる部署や、外部組織との対話を円滑にできること ・規則や取り決めなどに従うことができること ・強いストレスのある状況下で業務を遂行できること ・チームの評判を守る大局的な視点と行動ができること ・勉強を続ける姿勢があること ・問題解決能力 ・他のメンバーとの連携能力 ・時間管理能力
テクニカルスキル	・インターネットに関する知識 ・ネットワークプロトコル(IPv4、IPv6、ICMP、TCP、UDP) ・ネットワークインフラ(ルータ、スイッチ、DNS、メールサーバ) ・ネットワーク上のサービス及びその実装プロトコル(SMTP、HTTP、HTTPS、FTP、Telnet、SSH、IMAP、POP3) ・セキュリティの三原則(機密性・完全性・可用性)、多層防御など ・コンピュータ、ネットワークに対する脅威 ・攻撃手法(IP スプーフィング、DoS、ウイルス、ワームなど) ・暗号化技術(3DES、AES、IDEA、RSA、DSA、MD5、SHA) ・運用上の問題(バックアップ、セキュリティパッチ、アップデート) ・プログラミング及びコンピュータ管理能力

参考文献：コンピュータセキュリティインシデント対応チーム(CSIRT)のためのハンドブック CERT/CC 発行(翻訳：JPCERT/CC)

図2　CSIRT人材に求められるスキル

し、できるだけ短い時間で何を優先するかを的確に判断し対処していくことが必要です。

それを実行するためには、システムへの対処を行うテクニカルスキルだけでなく、状況を判断する能力と、組織内の関連部署との調整や外部組織との連携を行う能力などの高いヒューマンスキルも必要です（**図2**）。

CSIRTへの期待が非常に大きなものになってる一方で、実際にインシデントを経験する機会が少ない、ノウハウが属人化しがちで人に教えることが難しいなど、CSIRT要員の育成には、多くの障壁が存在しています。

このような状況を踏まえて、NECは、「インシデントハンドリング演習」の開発に取り組むことにしました。

3.「インシデントハンドリング演習」の概要

本章では、NECが立ち上げた「インシデントハンドリング演習」の概要を紹介します。

サイバー攻撃を受けた際に、CSIRTがどのように対処するべきなのかを、実際の場面と同じように時系列に体験し、解析などのテクニカルなところだけでなく、上司への報告や関連部門との連携、外部機関とのコミュニケーションなど、ヒューマンスキルの要素も加えた内容とすることを考えました。

「インシデントハンドリング演習」は、標的型攻撃に対する典型的な対処の流れを辿りつつ、実機を使った解析作業なども盛り込んだ実践的なもので、これまで、複数の人材育成事業の実施を通じて改良を重ね、その有効性を検証してきました。

3.1「インシデントハンドリング演習」の狙い

「インシデントハンドリング演習」は、以下の４点を主な狙いとしています。

- 最近の標的型攻撃を理解する
- 対応の手順について、シナリオを辿って体験する
- 対応に利用する手法・ツールを使ってみる
- 組織内外との連携について知る

また、演習で体験したことを、自組織の状況と照らし合わせることで、自組織の課題が明らかになり、改善につなげられるような知見を得られることも目標としています。

3.2「インシデントハンドリング演習」の対象者

「インシデントハンドリング演習」は、企業や団体の情報システム部門で情報セキュリティを担当する人を対象としています。これからCSRITを立ち上げようとしていたり、既に立ち上げていても有効に機能していない組織のメンバーを想定しています。また、新たにセキュリティ業務を担当したり、CSIRTのメンバーに加わったりする人にもとても有効です。

3.3「インシデントハンドリング演習」の構成と提供形態

「インシデントハンドリング演習」は、「講義」「実習」「グループワーク」の大きく３つのコンテンツで構成されています（**図3**）。

講義では、インシデントハンドリングに必要な基礎知識について学習します。合わせて、実習で使用するシステムの環境やツールの操作も体験します。

実習では、受講者は実機を操作しながら実際のサイバー

図3　インシデントハンドリング演習の構成

攻撃の事例に基づいたインシデント解析を体験しながら、インシデントハンドリングの一連の流れを学びます。受講者は3～4人でチームを組み、チームの中で指示、調査/解析、報告/連絡などの役割を分担してインシデントハンドリングに取り組みます。同じ組織から複数名で受講できる場合は、1つのチームに入って、実際の業務の役割に応じた分担で受講してもらうことも推奨しています。

グループワークでは、自組織におけるポリシーや運用面での対策を、講師や他の受講者とディスカッションします。演習を通じて学んだ知識や経験を、実際の業務に生かせるようにすることが狙いです。

1回の演習は、コンテンツのボリュームを考慮して2日間とし、講師と受講者や、受講者同士の円滑なコミュニケーションのため、一堂に会する集合型としました。実習に使用するPCやサーバなども、NECが提供します。

演習の進行は、1名の講師と複数名のチューターが行います。チューターは受講者の実習の理解と進捗をサポートし、通常は受講者10～15名程度に対して1名を配置しています。

3.4 実習で体験するシナリオ

実習では、仮想環境上に実際の組織のサーバやネットワークが模擬された環境に、侵入のログやRAT（Remote Access Tool、Remote Administration Tool：遠隔操作用のマルウェア）などのマルウェアを再現し、インシデントハンドリングの一連の流れ（シナリオ）を体験できるようにしています。シナリオは、実際に発生した標的型攻撃による情報流出事例などを参考にした、リアリティの高いものになっています。

以下にシナリオの一例を掲載します。

（1）通報者に対する通知
（2）検知に対する事実確認
（3）注意喚起
（4）調査結果レビュー
（5）表層解析
（6）現状の整理と報告
（7）被害範囲の調査
（8）ログ解析
（9）内部感染の原因調査
（10）情報漏えい報告

実効性の高いシナリオを作成するために、北陸先端科学技術大学院大学などの学術機関や、NECサイバーセキュリティ・ファクトリー[2)]のパートナー企業などと連携し、高度な知見や最新の事例を取り入れています。また、実習で使用するツール類は、自組織に戻ってから実際に導入しやすいように、フリーのものやOSの標準のものを中心に採用しています。

3.5 効果の計測方法

演習の受講を通じて、受講者のスキルが向上しているかどうか計測するために、受講前と受講後にスキルチェックテストを実施し、点数の比較による定量的な計測を行っています。

また、受講後のアンケートについては、演習終了時に行うアンケートだけでなく、少し時間が経ってからその後の状況を確認する“フォローアップアンケート”も試行的に行うようにしています。

4.「インシデントハンドリング演習」の実施と効果

本章では、NECがこれまで取り組んできた国内外における演習事業の概要について紹介します。

4.1 実践的サイバー防御演習（CYDER）

実践的サイバー防御演習（CYDER：Cyber Defense Exercise with Recurrence）は、2013年度から始まった総務省のプロジェクトです。官公庁や重要インフラ企業を対象としたもので、標的型攻撃によるインシデントハンドリングのシナリオを策定し、演習を実施してきました。サイバーセキュリティの脅威の変化に合わせて活動を拡大し、地方公共団体向けのシナリオなども拡充しています[3)]。

これまでにのべ2,000名以上の方が受講しています。受講後アンケートによると、「自組織内にCSIRTを立ち上げて関連団体に加盟した」「インシデント初動対応マニュアルを作成した」「演習で使用したツールを自組織で使え

るように整備した」などの成果が形となっているのはうれしいことです。

4.2 ASEAN各国を対象としたサイバー演習

総務省の「ASEAN諸国におけるサイバー防御能力の向上に向けた実践的演習のモデル事業」の一環として、2015年度からタイ、マレーシアなどのASEAN各国の政府サイバーセキュリティ関係機関を対象に、サイバー演習を実施しています。この演習は、前述のCYDERをベースとしていますが、開催する国特有の事情や国民性を考慮してシナリオの内容や演習の時間配分、進め方の調整を行いました。日本で実施しているCYDERに比べて実習に十分な時間を取りましたが、それでも実習時間はもっと長く取ってほしかったという意見が多く出ました。また、タイでは現地語のチューターを配置することにより、チーム実習やグループワークのディスカッションなどがとても活発になり、理解度も向上するという、顕著な効果が確認できました。

5. おわりに

サイバー攻撃の脅威は、大きくなるばかりですが、国民が安全にそして安心して暮らせる社会の実現のためには、それを支えるセキュリティ人材の役割がますます重要になると考えます。

NECは、これまで培った技術力とシステムインテグレーションのノウハウを生かして、サイバーセキュリティの人材育成と能力向上にこれからも貢献していきます。

参考文献

1) 総務省：総務省におけるサイバーセキュリティ政策の最新動向，2017.2
http://www.soumu.go.jp/main_content/000469744.pdf
2) 矢野 由紀子ほか：高度化するサイバー攻撃への取り組み「サイバーセキュリティ・ファクトリー」，NEC技報 Vol.67 No.1，pp.127-131，2014.11
http://jpn.nec.com/techrep/journal/g14/n01/pdf/140128.pdf
3) 総務省：サイバー攻撃（標的型攻撃）対策防御モデルの解説，2017.2
http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000125.html

執筆者プロフィール

矢野 由紀子
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
シニアエキスパート
電子情報通信学会会員

伊藤 篤史
ナショナルセキュリティ・ソリューション事業部
事業戦略企画グループ
マネージャー

舩越 健生
ナショナルセキュリティ・ソリューション事業部
事業戦略企画グループ
マネージャー

佐藤 和代
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
マネージャー

関連URL

実践！サイバーセキュリティ演習-インシデントレスポンス編-」
https://www.neclearning.jp/courseoutline/courseId/SN316/

NEC、マレーシアの政府系機関に「実践的サイバー防御演習」を提供
http://jpn.nec.com/press/201703/20170307_02.html

NEC、ASEAN6か国を対象としたサイバー攻撃防御演習を実施
http://jpn.nec.com/press/201702/20170217_03.html

実践的サイバー防御演習「CYDER」
https://cyder.nict.go.jp/

国立研究開発法人　情報通信研究機構「ナショナルサイバートレーニングセンター」
https://www.nict.go.jp/nct/

NEC、「サイバーセキュリティ・ファクトリー」が本格稼働
http://jpn.nec.com/press/201406/20140616_01.html

NEC 技報のご案内

NEC技報の論文をご覧いただきありがとうございます。
ご興味がありましたら、関連する他の論文もご一読ください。

NEC技報WEBサイトはこちら

NEC技報（日本語）　NEC Technical Journal（英語）

Vol.70 No.2　ビジネスの安全・安心を支えるサイバーセキュリティ特集
～Futureproof Security　安心の先へ。～

ビジネスの安全・安心を支えるサイバーセキュリティ特集によせて
増大するサイバー犯罪の根源的な解決へ～“産学官”のオールジャパンで立ち向かう第三者機関の姿とは？～
サイバーセキュリティを取り巻く社会動向とNECの取り組み

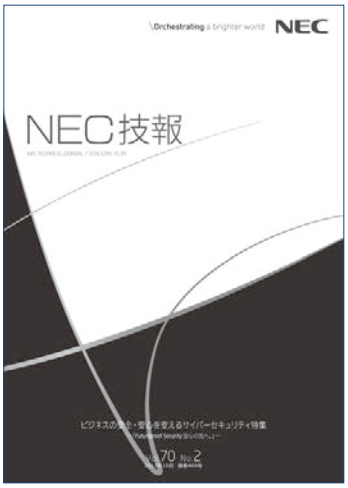
◇ 特集論文

社会の動向とNECの取り組み
重要インフラに対するサイバー攻撃の実態と分析
2017 サイバー攻撃最新動向 NEC Cyber Threat Intelligence活用モデル
サイバーセキュリティ対策の社内事例

サイバーセキュリティソリューション
複雑化 / 高度化するサイバー脅威に対抗するSOCとセキュリティ監視サービス
攻撃被害を極小化するためのインシデント対応支援ソリューション
サイバー演習によるインシデントハンドリング能力の強化
セキュリティ統合管理・対処ソリューション「NEC Cyber Security Platform」
クラウド型ファイル暗号化サービス －ActSecureクラウドセキュアファイルサービス－
セキュリティLCMサービス
EMMを活用したセキュアなモバイルワークソリューション
IoT 時代の経営を支援するサイバーセキュリティコンサルティング

サイバーセキュリティへのAI技術の活用
AI（人工知能）を活用した未知のサイバー攻撃対策
採るべき対策の「なぜ？」に答えるAIの可能性
オープンソースインテリジェンスを活用したサイバー脅威の検出と自動分析
犯罪捜査支援のためのサイバー・フィジカル統合分析技術

お客様に安全・安心を届けるための社内の取り組み
安全・安心な製品・サービスをご提供するための取り組み ～セキュア開発・運用～
サイバーセキュリティ人材のタレントマネジメント



Vol.70 No.2
（2017年10月）

特集TOP