平成 29 年度セキュリティ技術向上研修および平成 29 年度国立大学法人等情報化要員研修(「実践！サイバーセキュリティ演習ーインシデントレスポンス」) を受講して

玉　井　啓　介*
tamai@kit.ac.jp

はじめに

2017 年 10/26（木)、27（金)、平成 29 年度セキュリティ技術向上研修､10/30（月)､31（火)、平成 29 年度国立大学法人等情報化要員研修を続けて受講させていただきました。

前者は「研修用に構築した様々な脆弱性が存在する疑似的な情報システム環境に対して、脆弱性に対する対策を実施し、疑似的に発生させる様々なサイバー攻撃から情報システムを防御するための堅牢化（Hardening）に関する実践的な研修を実施する」と、主にサーバーサイドに係るインシデントレスポンスの研修だったことに対し、後者は「サイバー攻撃（標的型攻撃）に係るインシデントレスポンスの内容をひととおり体験し、そのプロセスの基本を習得することを目的」とされた研修で、主にクライアントサイドに係るインシデントレスポンスの研修で、続けて受講でタイトなスケジュールではありましたが、まとまった期間、セキュリティインシデントレスポンスのことだけに集中できた、大変有意義なひとときでした。

セキュリティ技術向上研修ついて

10/26（木)、27（金)、セキュリティ技術向上研修では、5 人 1 組のチームを組み、インシデントレスポンスに競技形式で取り組みます。適切なアクセス制限がなされているか、不要サービスはないか、不要ユーザはいないか、ユーザには安易なパスワードが付けられていないか､CMS を利用しているサーバがあれば､(脆弱性を含んだ) 不要なプラグインは使用していないか､といったまずは｢定石｣の点検から､チーム内で役割分担を行い、実施しました。競技の最後に実施業者の伊藤忠テクノソリューションズの方より講評をいただけるのですが、私たちのチームは全チームの中で最も迅速に対応できていたとの評価をいただけました。

ただ、その一方で脆弱性に気づけず、インシデントを発生させてしまった事例もありました(ウェブサイトの改ざんを許してしまいました)。不要ユーザのチェックおよび、強固なパスワードが付与されているかの確認が不十分だった点が落ち度でした。

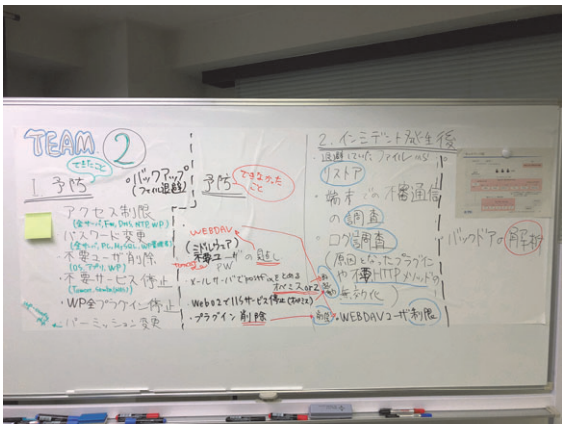

図 1　レスポンスのレビュー

そうしたレビューも含め、競技後に各チームのインシデントレスポンスの振り返りおよび内容の発表（図 1)、さらには各チームとの意見交換も行われました。さまざまな立場と得意分野で普段 IT サービスに係る業務に携わっている参加者の皆さまとの意見交換からは、実に多くの気づきを得ることができました。

参加者同士によるインシデントレスポンスのレビューの後は、攻撃者側の目線より、今回の研

＊高度技術支援センター　技術専門職員

修環境での攻撃の「手のうち」を公開していただきました。攻撃者側の考え方およびそのデモを実際に目にすることができるのは大変貴重で、インシデントレスポンスの手法を学ぶこと以上に、今回の研修の収穫だったと思っています。（図２）

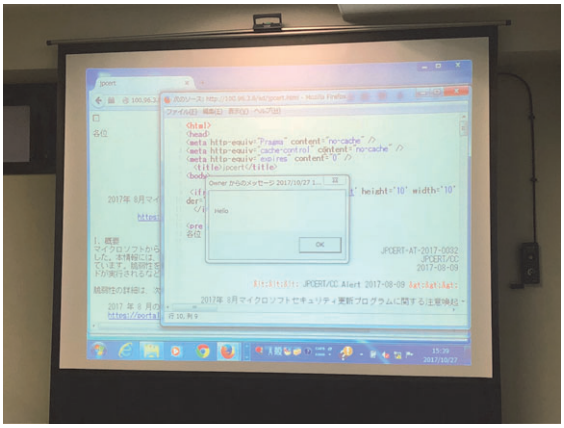

図２　サイバー攻撃のデモ

国立大学法人等情報化要員研修を受講して

10/30（月）、31（火）、国立大学法人等情報化要員研修では、架空の組織内のシステム管理者として、標的型メールを受信した社員から、その開封の是非の問い合わせが入り、それに対するインシデントレスポンスという、大変に起こりうる状況を想定しての実習を主に行いました。こちらもセキュリティ技術向上研修と同様、チームでの取り組みとなりました。

中でもとりわけ目を引き、私自身その習得の必要を感じたのは、以下の調査ツールでした。

- GeoIP
  インシデント調査の段階で特定したIPアドレスがどこの国に属しているかを調べる。
  https://www.maxmind.com/ja/geoip2-services-and-databases
- HashMyFiles
  ファイルの同一性を確認するためのハッシュ値を求める。
  http://www.nirsoft.net/utils/hash_my_files.html
- FTK Imager
  保存された（感染が疑われた）イメージをディスクマウントし、参照・調査する。
  http://accessdata.com/product-download/ftk-imager-version-3.4.3
- Strings
  プログラム内に埋め込まれている判読可能な文字列を抽出する。
  https://technet.microsoft.com/ja-jp/sysinternals/strings.aspx
- TCPView
  ネットワーク上のコンピュータとの接続状況や待ち受け状況などがリアルタイムに表示される。
  https://technet.microsoft.com/ja-jp/sysinternals/tcpview.aspx
- Wireshark
  ネットワーク上を実際に流れるパケットをキャプチャすることができ、通信内容を詳細に確認することができる。
  https://www.wireshark.org/
- Process Monitor
  実行中のプログラムの状態を確認できる。
  https://technet.microsoft.com/ja-jp/sysinternals/processmonitor.aspx
- RegRipper
  Windowsレジストリ内のデータを解析できる。ローカルのユーザ、グループに関する情報を確認できる。
  https://github.com/keydet89/RegRipper2.8

上記の調査ツールを駆使し、「記録保全」「被害拡大防止」の観点から、さまざまな証拠を集めたり、当事者および関連者（場合によっては社員全員を含む）に適切な注意喚起を出したり、契約ベンダに適切に調査依頼を出したり、といった、ツールへの知識、関係者との適切なやりとり、組織内のポリシーの見直し、は同時に非常に有意義な内容でした。

それぞれの研修、いずれもチームを組んで取り組めたこともあり、桝田センター長の「属人性を減らすためには、チームで対応できるように、様々な担当業務を複数人であたれるようにする(注)」という指摘を常に意識することとなりました。個々の知識と個々の技術習得と、こうしたチーム意識もともに意識して今後の自己研さんに勤しみたいと思います。

(注) 桝田秀夫「チームであたるということ」(情報科学センター広報誌 No.35, pp1-2, 2017年)