桑名レポート：サイバーセキュリティの現場から（11）

サイバー衛生（Cyber Hygiene）

NTT アドバンステクノロジ株式会社
常務取締役　セキュリティ事業本部
本部長　**桑名 栄二**
博士（工学）、CISSP

本稿では、一般の衛生管理と同じように社内の IT 環境や個人のインターネット利用環境を健全な状態に保つことを推奨するサイバー衛生について紹介する。

サイバー衛生とは

米紙「ニューヨーク・タイムズ」によると、米国ボルチモア市では今年５月７日から数週間以上に渡り、市の PC 約 1 万台が“RobbinHood”という比較的新しいランサムウェアに感染し、同市のサービスが麻痺しているようである[1,2,3]。ランサムウェアについては、2017 年 3 月に公開された脆弱性を狙った WannaCry が 2017 年 5 月に世界的に流行し、大きな被害を出したことは記憶に新しい[4]。これは、事件の 2 カ月前に公開されたパッチを当てていれば被害は極小化できた。しかし、現実には 2 ヶ月前に公開されたパッチを当てていないコンピュータが多く存在し、被害は増長した。

ボルチモア市の事案のように依然として大規模なインシデント事案は発生しているが、WannaCry の被害、ビジネスメール詐欺等がニュースでも取り上げられるようになり、フィッシングメールへの注意、システムを最新の状態に保つ、セキュリティパッチを適用する等の日常的なセキュリティ管理の重要性に対する認識は広まりつつあるように思う。

サイバー衛生（サイバーハイジーン、cyber hygiene）とは、一般の衛生管理と同じように社内の IT 環境や個人の PC やインターネット接続環境を健全な状態に保つことを組織や社員一人ひとりに推奨し（Cyber Hygiene Is Everyone's Job）、セキュリティ意識を醸成する取り組みを指す[5]。ちなにみ、サイバー衛生という言葉は、実は新しい言葉ではなく、今から 20 年ほど前に米国の合同経済委員会で MCI WorldCom（当時）の Vinton G. Cerf 博士が使った言葉が最初のようである[6]。

インフルエンザが発生する時期には、マスクをする、手洗いを徹底する、感染が疑われる場合は出社しないなど、我々は当たり前のことに取り組む。これと同じように、会社の情報セキュリティについても、セキュリティ部門等の責任組織に加え、社員一人ひとりが自分の IT 環境を健全に良くしていこうと行動すること、これがサイバー衛生の概念である。たとえば、情報セキュリティ部門はパスワードポリシーを設定するが、一般ユーザーは強力なパスワードを自ら設定し、それらを秘密に管理しなければならない。

組織にとってのサイバー衛生

組織がサイバー攻撃から身を守るために備えておく必要のある基本的な考え方や指針の例としては、下記の事例がある。

CIS Controls（旧SANS Top20 Critical Security Controls）[7,8]

①許可されたデバイスと無許可のデバイスのインベントリ管理

ネットワーク上のすべてのハードウェアデバイスを能動的に管理する。アクセス権限を許可されたデバイスだけに付与する。無許可のデバイスや管理されていないデバイスを検出し、これらのデバイスがアクセス権限を取得することを防止する。

②許可されたソフトウェアと無許可のソフトウェアのインベントリ管理

ネットワーク上のすべてのソフトウェアを能動的に管理する。許可されたソフトウェアだけをインストールし、実行可能とする。無許可のソフトウェアや管理されていないソフトウェアを検出し、不正なソフトウェアのインストールと実行を防止する。

③モバイルデバイス、ラップトップ、ワークステーションおよびサーバに関するハードウェアおよびソフトウェアのセキュアな設定

攻撃者が脆弱なサービスや設定を悪用できないようにするため、厳格な設定管理および変更管理プロセス

を使用して、PC、サーバ等のセキュリティ設定を確立・実装し、能動的に管理する。

④継続的な脆弱性診断及び修復

継続的にソフトウェア更新、パッチ、セキュリティ勧告、脅威情報などの新たな情報を取得・評価し、この情報に基づいて措置を講じることで、脆弱性を特定して修復し、攻撃チャンスを最小限に抑える。

⑤管理権限のコントロールされた使用

コンピュータ、ネットワーク、アプリケーションの管理権限の使用、割り当て、設定を追跡、管理する。いわゆる特権ユーザー管理である。

⑥監査ログの保守、監視および分析

イベント監査ログを収集、管理、分析する。

このCIS Controls以外にも、英国GCHQ（UK Government Communications Headquarters）、NISTのCybersecurity Framework、CIS等から重要かつ共通的な部分を抽出した米国カーネギーメロン大学の11項目[9]（①重要事業、サービス、製品、およびそれらを支える資産を特定し優先順位をつける、②①に対するリスクを特定し優先順位を付けて対応する、③インシデント対応計画を策定する、④情報セキュリティ教育と啓発活動を実施する、⑤ネットワークセキュリティとその監視を確立する、⑥最小限の権限に基づいてアクセス制御を管理・維持する、⑦技術の進化に対応し、標準化された安全な設定を維持する、⑧データを保護し、回復するための管理策を実施する、⑨マルウェアからの侵害を防ぎ、監視する、⑩サプライチェーンを管理する、⑪脅威と脆弱性の監視と修復を行う）や、VMwareが提示する基本原則[10]もサイバー衛生の基本項目として一読をお薦めする。

個人にとってのサイバー衛生

個人にとってのベストプラクティス例としては、Symantec社の全9項目[11]がある。①ウイルスやマルウェアの対策ソフトウェアをインストールする、②ネットワークファイアウォールを使用する、③ソフトウェアを定期的にアップデートする、④強力なパスワードを設定する、⑤多要素認証を使用する、⑥デバイスの暗号化を用いる、⑦定期的にバックアップする、⑧ハードドライブを清潔に保つ（データを消去する時はディスク消去ツールを用いる）、⑨ルーターをセキュアに保つ（ルーターのデフォルトの名前やパスワードをオフにして更新する、リモート管理をオフにする、WiFiルーターのWPA2またはWPA3暗号化を利用する）。

これら9項目はどれも当たり前のことであるが、現実には守られていないことも多い。例えば、工事専用PCや持出専用のPCを考えてみよう。これらのPCは毎日利用されないこともあり、ウイルス対策ソフトのパターンファイルが古いまま利用されてしまうこともある。WannaCryの2カ月前のパッチが適用されていなかった例のように、古い版のパターンファイルのまま公衆無線LANなどセキュリティレベルの低いネットワークに接続し、そこでマルウェアに感染、その後帰社し、マルウェアを社内ネットワークに感染拡大させた事案がある。

まとめ

CIS Control[8]の冒頭に「防御する側として私たちが利用できるものは非常に多く、（中略）、セキュリティ担当者にとってみれば、インフラ保護のために必要な情報には事欠かないのです。ところが、こうしたテクノロジーや情報、およびその管理は、文字通り「膨大な選択肢による混沌（Fog of More）」をもたらしています」の一節がある。

その混沌とした状況から脱却するために、ベストプラクティスや具体的な対策事項が提示されている。どれも基本中の基本であり、地道に実行していかねばならないが、私個人としては「継続的な情報セキュリティ教育と啓発活動」が最も重要と考えている。

[1]https://www.nytimes.com/2019/05/25/us/nsa-hacking-tool-baltimore.html
[2]https://www.nytimes.com/2019/05/22/us/baltimore-ransomware.html
[3]https://www.baltimorecity.gov/node/17288
[4]https://ja.wikipedia.org/wiki/WannaCry
[5]https://insights.sei.cmu.edu/insider-threat/2017/11/cyber-hygiene-11-essential-practices.html
[6]https://www.jec.senate.gov/archive/Documents/Hearings/cerf22300.htm
[7]https://www.cisecurity.org/cybersecurity-best-practices/
[8]https://www.cisecurity.org/wp-content/uploads/2017/03/CIS-CSC_v6.1_Japanese_Final_r1.pdf
[9]https://resources.sei.cmu.edu/asset_files/Presentation/2017_017_001_508771.pdf
[10]https://www.vmware.com/content/dam/digitalmarketing/vmware/ja/pdf/products/vmware-core-principles-cyber-hygiene-whitepaper.pdf
[11]https://us.norton.com/internetsecurity-how-to-good-cyber-hygiene.html