実践セキュリティ特論 上原先生 第二回課題

28G23027
川原尚己

問 1：ファイアウォールやルータでネットワークを分離する境界線防衛モデルは最近限界が指摘されている．どのような理由で限界と言われるようになったのか，代替案としてどのような防衛モデルが考え出されたのか説明せよ．

Windows Update などの脆弱性対策やマルウェア対策のパターンファイル更新などで例外的にネット接続が必要となることが多いが，それが原因で攻撃を許すことになりやすいため．

Zero Trust Network が代替案として考えられており，これはネットワークによる防御をあきらめ，危機感通信のたびに毎回認証してアクセス制御を行おうとする手法である．

問 2：IPA 高度標的型対策ガイドが勧めるシステム構成と運用方法について簡潔に説明せよ．

システムの内部侵入に対する対策は突破されるものとして考え，侵入された後に，内部で侵入の拡大を防ぐことを目標とする．

問 3：クロスサイトリクエストフォージェリ対策として Web サービス設計時にどのようなことが考えられるか説明せよ．

Referer が正しいリンク元化を確認し，正しい場合のみ処理を実行したり，処理を実行する直前のページで再度パスワードの入力を求め，実行ページでは，再度入力されたパスワードが正しい場合にのみ処理を実行する．

参考文献：

https://www.ipa.go.jp/security/vuln/websecurity/csrf.html