脆弱性定量化に向けての検討WG

脆弱性定量化に向けての検討WGリーダー
京セラコミュニケーションシステム株式会社　郷間　佳市郎

■ はじめに

最近では「脆弱性」という言葉が、ずいぶんと一般的に通用するようになってきていますが、一昔前は「きじゃくせい」などと読まれたりと、あまりあちこちで通用する言葉ではなかったと記憶しています。今でも、読み間違えないようにと「ぜい弱性」と記述したり、あえて「欠陥」や「弱点」といった他の言葉に置き換えてしまう場合もあるようですが、さすがに「きじゃくせい」と読む方も減り、一般的な用語として浸透してきているように感じます。しかし、言葉は浸透してきたものの、では、個々の脆弱性がどれだけ危険なのかといった本質的な意味については、これを説明しようとすると、かなりの困難が伴います。立場や環境によって捉え方や理解度がまちまちであり、説明に苦労したり、場合によっては相手に誤解を与えてしまう場合も少なくありません。自分ではわかったつもりでも、いざ、自分の上司や他の部署の人に伝えようとしたら一苦労したという経験のある方も多いと思います。個々の脆弱性の説明でさえ難しいわけですから、では、あるサーバに複数の脆弱性が存在する場合に全体としても危険度はどうでしょうといった判断や、異なる脆弱性を複数持ったサーバ同士を比べて、どのサーバから最初に対処をはじめるべきかといった優先順位を判断をしようとした場合には、さらに困ってしまうわけです。

■ 活動目的と内容

どのようにしたら、脆弱性についてわかりやすくなるか。それに対する答えのひとつが定量化（数値化）です。定量化によって、個々の比較はもちろん、定量化によって求められた数値を統計計算することによって、その性質や相関関係も明らかにできる可能性があります。もしかしたら、その結果をトリガーにしてセキュリティ対処を自動化するといったことも、あながち夢物語とは言えないのではないかと思っています。

このように、脆弱性の複雑さに関する問題を解決できないかという意識から、本ＷＧがスタートしました。定量化できないのか、できるのか、もし定量化できるとしたら、それは脆弱性の何なのかといったことから議論がはじまったわけです。また、ベンダーとしては、とにかくパッチを提供したら、関係するすべてのサーバに適用してもらいたいと思っていますが、実はシステムの現場では、できればパッチはあてたくないのだという実情も、参加者の議論の中からあらためて明らかになってきました。実際にシステムの現場に携わっている参加者も多いことから、セキュリティ製品のベンダーとしての立場の方だけでなく、システムの運用を維持するという立場からの発言が多いことも特徴です。

異なる立場から脆弱性とその脅威、そしてその運

用についてと、議論が幅広く広がり、収拾できなくなる場面もありますが、これまで、脆弱性というキーワードで、このように多様な立場の人が定期的に会合を開くということは、あまり行われてこなかったのではないかと思っており、WGとしての存在意義を強く感じています。

■ 今後の予定

最終的には、自分たちで納得のいく定量化のアプローチを見つけたいということが目標です。

米国では、ネットワーク製品ベンダーやアンチウイルスベンダーの一部が中心になって、脆弱性の定量化の取組みが行われています。先日、米国において開催されたRSAカンファレンスでも発表があり、日本でも報じられたことから、すでにご存知の方も多いかもしれません。もちろん本WGの中でも、米国での取組みに対する勉強を行いました。自分たちの目指しているものと比べてどうなのか、実際それが利用できるのか、できないのかといったことにも踏み込んで、WGの場で意見交換を行っています。

■ WGメンバー

リーダー：郷間　佳市郎
（京セラコミュニケーションシステム）

メンバー：鹿児島　健　（インフォセック）
小野　泰司　（インフォセック）
北島　健治　（エス·アンド·アイ）
中嶋　一樹　（住商エレクトロニクス）
金岡　晃　（セコム）
坂本　慶　（ディアイティ）
松井　康宏　（日本アイ·ビー·エム）
宮永　直樹　（日本電気）
世良田　照治（日本電気）
奥原　雅之　（富士通）
長谷川　喜也（富士通）
伊藤　良孝
（三井物産セキュアディレクション）
横山　哲也　（横河電機）
岩井　博樹　（ラック）