第21回 セキュリティ解説

株式会社日立製作所 システム開発研究所主管研究員 寺田真敏（てらだ まさと）

脆弱性対策情報を提供しているサイトの活用方法

1 はじめに

国内においても、脆弱性対策のための情報提供サイトが充実してきています。今回は、"ソフトウエア等において、コンピュータウイルス、コンピュータ不正アクセス等の攻撃により、その機能や性能を損なう原因となり得る安全性上の問題箇所"といわれている"脆弱性"の対策のための情報提供サイトの活用方法について考えてみたいと思います。英語では、脆弱性に関する情報提供サイトのことを総称して"Vulnerability Database"と呼ぶことがあります。日本語訳すると、脆弱性情報データベースになると思いますが、脆弱性対策のために情報収集や情報提供をしているという思いを伝えるべく、ここでは"脆弱性情報"ではなく"脆弱性対策情報"と呼ぶことにします。

2 活用方法ポイントその1：脆弱性の原因の視点から分類してみよう

活用方法ポイントその1は、脆弱性の原因の視点からの分類です。

ここでの脆弱性の原因の視点からの分類とは、バッファオーバフロー、クロスサイトスクリプティングなどの専門用語レベルでの分類のことではありません。脆弱性の原因には、プログラムが稼動するための設定に内在するセキュリティ問題(Application Misconfigurations)と、プログラム自身に内在するコード上のセキュリティ問題(Software Flaws)の2つがあります。前者はシステム運用者自身が自分の環境にあった適切な設定に改善することが必要となり、後者は製品開発者の提供するセキュリティ修正プログラム（パッチ）により修復を行ないます。この時点で、脆弱性対策のための情報提供サイトは大きく2つに分類されることになります。

(1) プログラムが稼動するための設定に内在するセキュリティ問題

- (独)情報処理推進機構(IPA)：読者層別 情報セキュリティ対策 実践情報
  システム管理者向けに、"適切な機材を正しく設定し、攻撃を検出・対応できるようにすること"のための資料が掲載されています。
- Common Configuration Enumeration (CCE)
  米国では、機械的に設定とソフトウエアの脆弱性検査を行なうためのSecurity Content Automation Program (SCAP)という活動を進めています。CCEは、プログラムが稼動するための設定に内在するセキュリティ問題を回避するための枠組みです。

(2) プログラム自身に内在するコード上のセキュリティ問題
次節で紹介します。

3 活用方法のポイントその2:情報提供形態の視点から分類してみよう

活用方法のポイントその2は、主に、プログラム自身に内在するコード上のセキュリティ問題を取り扱う情報提供サイトを情報提供形態の視点から分類することです。

図1に示す4つの分類は、脆弱性対策のための情報をどのような切り口から取り出すことができるのかという代表的な例です。国内では、次の情報提供サイトが該当すると思います。

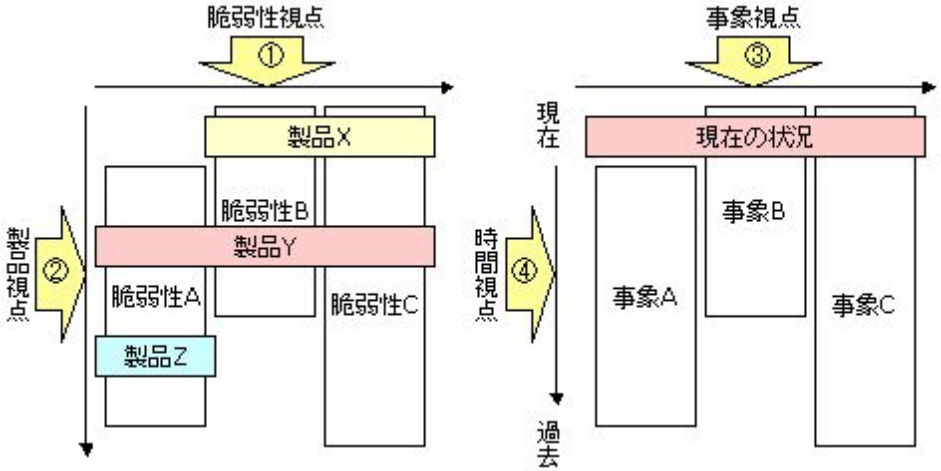

図1 情報提供形態の分類

(1) 脆弱性視点:脆弱性Cがどのような問題なのか、どのような製品に影響を及ぼすのか知りたい。

- JVN(JP Vendor Status Notes) [*1]
  JVNは、JPCERTコーディネーションセンターと(独)情報処理推進機構(以降、IPA)との共同運営による日本国内の製品開発者の脆弱性対策状況を公開するサイトです。JVNでは米CERT/CC(CERT Coordination Center)や英NISCC(National Infrastructure Security Co-ordination Centre)[*2]に報告された脆弱性の対策状況も掲載しています。また、2007年4月からJVN iPediaという脆弱性対策情報を網羅的に取り扱うサイトも整備されました。
- IPA:脆弱性関連情報の調査結果
  JVNに掲載された脆弱性対策情報の内、IPAに届出があったものについて、解説資料が掲載されています。

(2) 製品視点:製品Yに、どのような脆弱性が存在するのか知りたい。

- 各製品開発者の情報提供ページ
- @police:システム／ネットワーク管理者向け脆弱性情報

脆弱性対策情報を製品という視点から参照できるサイトです。また、同サイトで提供されている"研究開発成果"のページは、脆弱性や防御等に関する検証資料が掲載されおり、対策を推進する際の参考になります。

(3) 事象視点:ある脆弱性に関連する事象Cの経過状況、例えば、脆弱性を悪用する攻撃コード(Exploit Code)の発生を知りたい。

- JVN:TRnotes
  掲載数は少ないですが、脆弱性に関わる状況変化を提供しています。

(4) 時間視点:いま、注目すべき事象、例えば、緊急度の高い脆弱性やセキュリティ事故(インシデントと呼ばれています)を知りたい。

- @police:重要なお知らせ
- JPCERTコーディネーションセンター:注意喚起&緊急報告
- IPA:緊急対策情報

このように分類することにより、それぞれのサイトが持つ特徴がわかりますし、どのような視点で対策情報を取り出したいのか、どのような視点で対策情報を展開したいのかを考えることにもつながります。情報の入力(どの情報提供サイトを利用するのか)と出力(入力された情報の利用先)のバランスを考えることも、効果的な脆弱性対策を推進するためには必要だと思います。

海外での情報提供についてですが、脆弱性対策に関する代表的なサイトとしては、次のようなサイトがあります。

- US-CERT:Vulnerability Notes Database
- SecurityFocus:Vulnerabilities
- Secunia:Vulnerability and Virus Information

補足になりますが、これだけ情報提供サイトがあると、それぞれのサイトが提供する脆弱性対策情報のどれとどれが同じ情報なのかかがわからなくなってしまいます。この問題を解決するために、脆弱性に対して一意の識別子を付与することで、脆弱性対策情報同士の関連付けを行う仕組みとしてCommon Vulnerabilities and Exposures(CVE)があります。JVN iPediaは、CVEがカバーしていない国内の脆弱性対策情報同士の関連付けをサポートする役割も担っています。

4 活用方法のポイントその3:深刻度の視点から分類してみよう

活用方法のポイントその3は、深刻度の視点からの分類です。

現在、インターネットで公表されている深刻度には、プログラム自身に内在するコード上のセキュリティ問題の深刻度とインターネット全体の深刻度の2種類があります。前者は、個々のプログラム自身に内在するコード上のセキュリティ問題がどの程度悪用されやすいものなのかという視点で、後者はインターネットへの脅威の迫り具合を示す視点からレベル分けされています。

(1) プログラム自身に内在するコード上のセキュリティ問題の深刻度

- US-CERT:Vulnerability Notes - Metric

- NIST：NVD － CVSS Severity
- Secunia：Secunia Advisories － Criticality
- FrSIRT：Security Advisories and Vulnerabilities － Rated
- マイクロソフト：セキュリティ情報の深刻度評価システム

(2) インターネット全体の深刻度

- IBM Internet Security Systems：AlertCon
- Symantec：ThreatCon

今回は、脆弱性対策情報を提供しているサイトの活用方法が主題ですので、プログラム自身に内在するコード上のセキュリティ問題の深刻度について補足します。深刻度は、対策の優先度を考える際の客観的な指標となりますが、指標に対する過信は禁物です。事例を紹介しますと、図2は、NIST（米国国立標準技術研究所）のNVD（National Vulnerability Database）から脆弱性の攻撃形態として"Target Must Access Attacker's Resource"という項目に該当する件数を取り出したものです。"Target Must Access Attacker's Resource"は、日本語で受動的攻撃とも呼ばれている手法で、「ユーザに、電子メールやインスタントメッセンジャのメッセージ内のリンクをクリックさせることで、悪意あるWebサイトにアクセスさせる」という方法があります。"Target Must Access Attacker's Resource"に関する脆弱性は、一般ユーザの利用するクライアントPCが攻撃対象となり、多くの場合深刻度は低く見積もられていますが、ここ数年増加傾向にあります。

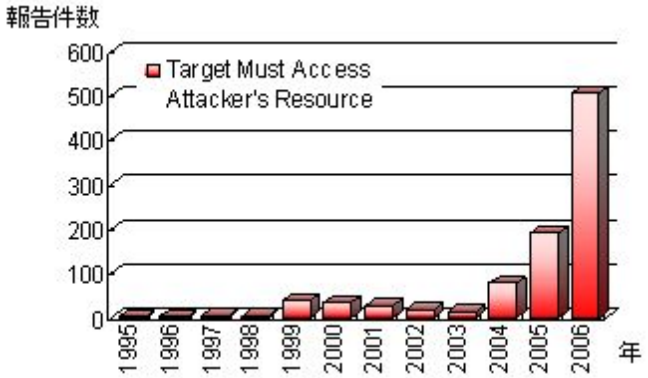

図2 Target Must Access Attacker's Resourceに関する脆弱性の報告件数(出典:NVD)

また、最近、脆弱性に対する汎用的な評価手法として、CVSS(Common Vulnerability Scoring System)という指標が米国を中心に普及しはじめています。CVSSで注目したいのは、脆弱性そのものの特性を評価する基本評価基準(Base Metrics)、脆弱性の現在の深刻度を評価する現状評価基準(Temporal Metrics)、製品利用者の利用環境も含め深刻度を評価する環境評価基準(Environmental Metrics)という視点を用意していることと、個々の基準で攻撃のされやすさ、攻撃コードや攻撃手法の状況などの評価項目を列挙していることです。ぜひ、数値やレベルに捕らわれることなく、どのような視点で深刻度を評価しようとしているのかを読み取りたいものです。CVSSについては、IPAから"ソフトウェア等におけるセキュリティ上の弱点の深刻度評価の試行について"という資料が提供されていますので参考にしてみてください。

5 おわりに

ネットワークワームのような大規模インシデントが影を潜め、特定の個人や組織に狙いを定めた標的型攻撃(Targeted Attack)など密かに侵害活動が進攻しているいまだからこそ、脆弱性対策のための情報提供や利用方法をいま一度見直したいと思っている今日この頃です。

[*1] JVNの名称は、2007年4月25日からJapan Vulnerability Notesに変更になりました。

[*2] 英NISCCは、2007年2月1日に、NSAC(National Security Advice Centre)の一部と統合し、CNPI(Centre for the Protection of National Infrastructure)という組織になりました。

profile

寺田　真敏(てらだ　まさと)

株式会社日立製作所　システム開発研究所主管研究員
兼　Hitachi Incident Response Teamチーフコーディネーションデザイナ
(独)情報処理推進機構セキュリティセンター非常勤研究員
JPCERTコーディネーションセンター専門委員

HIRTメンバとして日立のCSIRT(Computer Security and Incident Response Team)活動に取り組むと共に、システム開発研究所主管研究員として ネットワークセキュリティの研究に従事。2005年からはインターネットのCSIRTの団体であるFIRST(Forum of Incident Response and Security Team)加盟に伴い、対FIRSTのHIRT窓口を担当。2002年～2006年慶應義塾大学大学院社会人学生として、JVN(JPCERT/CC Vendor Status Notes)プロジェクトに参画し、近年、通信事業者のための情報共有分析センター(Telecom-ISAC Japan)などの情報セキュリティ対策推進活動に参画。その他、中央大学研究開発機構客員研究員、情報処理学会コンピュータセキュリティ研究会主査などを務める。