



NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

脆弱性定量化に向けての検討WG

郷間佳市郎

京セラ コミュニケーションシステム

2005年6月13日

(2004年11月からの活動報告)

活動目的・内容



- 脆弱性の定量化アプローチについて、
国外の情報を含め検討を行い、
WGとしての検討結果を出す
- 立場の違う人たちがメンバーとして参加
・メーカー、システムインテグレータ、ISP etc.
- 月1～2回のペースでミーティングを開催
- 2004年11月から活動を開始
今期はアプローチ方法の検討を行った

Copyright (c) 2005 NPO日本ネットワークセキュリティ協会

Page 2

WGメンバー (社名昇順)



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・ピー・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)
	横地 裕	(横河電機)
	横山 哲也	(横河電機)
	岩井 博樹	(ラック)

Copyright (c) 2005 NPO日本ネットワークセキュリティ協会

Page 3

まず、目的をひとつ設定



何のために、誰のためのものか？



意思決定者が、対応する／しないの決定、あるいは、
対応の緊急性を判断するための指標となる数値


【具体的なシチュエーション】

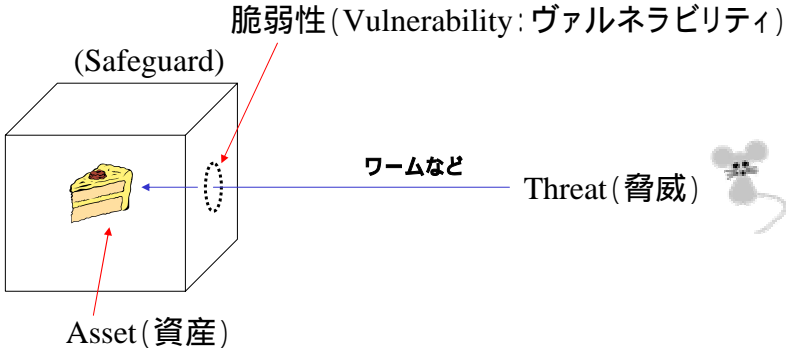
パッチがリリースされた時に、即座に適用するか、
次の定期保守まで待つかという判断に使える指標

Copyright (c) 2005 NPO日本ネットワークセキュリティ協会

Page 4

一般論の確認






例) ある穴しか通らない虫がいたとすれば、その虫に対して、その穴はヴァルネラブルであるということになる。そして、その穴はヴァルネラビリティと呼ばれることになる

Copyright (c) 2005 NPO日本ネットワークセキュリティ協会
Page 5

一般論の確認




一般論としては、以下の関係が有名である。

$$R = T \times A \times V$$


(R:リスク T:脅威 A:資産 V:脆弱性)

この式は、理論的には正しいが、現場で使うことが困難
(定量化が難しい)



今回、「これをわざと忘れてみる」ことにした

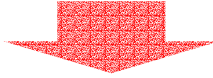
Copyright (c) 2005 NPO日本ネットワークセキュリティ協会
Page 6



一般論の確認

我々の知りたい(使いたい)脆弱性とは何か？


我々の目的のためには、純粋なV(脆弱性)ではなく、T(脅威)を含めた方がわかりやすい



これを、仮に「Z(Zeijakusei)」と呼ぶことにした

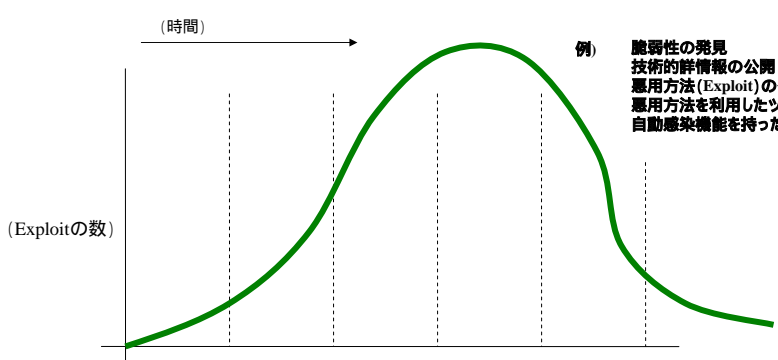
今回の目的を考えると、
求めるべきものは「Z」である

Copyright (c) 2005 NPO日本ネットワークセキュリティ協会
Page 7



一般論の確認

CERT/CCなどで紹介されている脆弱性の悪用という観点からの時系列変化

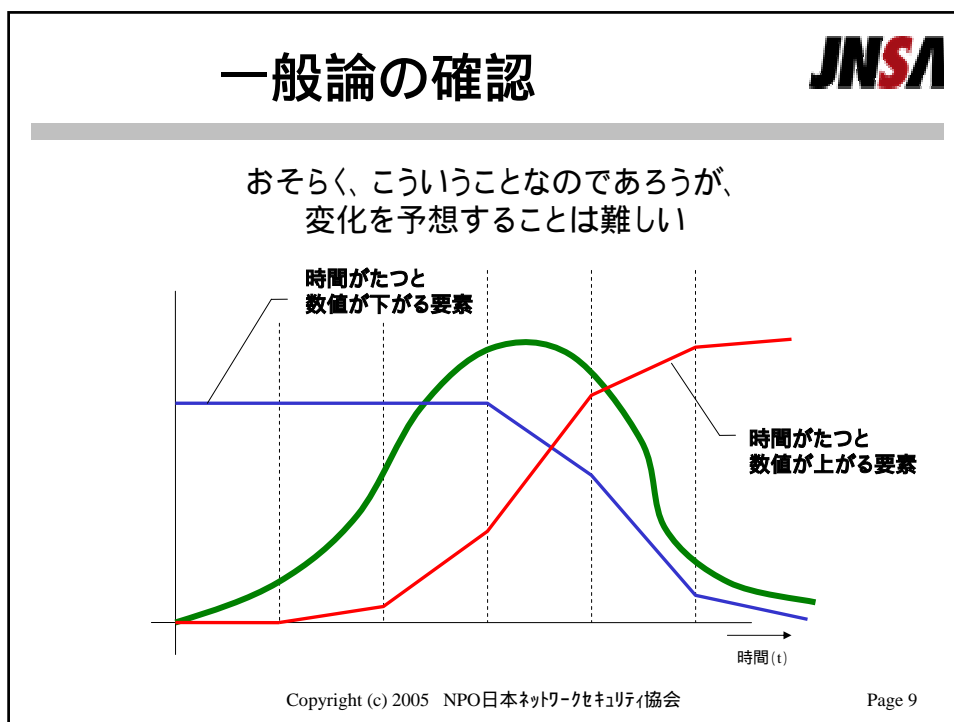


例)

- 脆弱性の発見
- 技術的詳細情報の公開
- 悪用方法(Exploit)の公開
- 悪用方法を利用したツールの公開
- 自動感染機能を持ったツールの公開

本当にこのような曲線を示すのか？

Copyright (c) 2005 NPO日本ネットワークセキュリティ協会
Page 8



一般論の確認

JNSA


時間に依存するパラメータの扱いは？

時間に依存するパラメータは、
測定可能 / 予測可能であれば「Z」の要素になる

↓

- 今回、求めようとしているものは、汎用的な意思決定に利用されるもの
対処までの猶予期間のようなものも含んでいる
- したがって、測定可能 / 予測可能でないものは「Z」の要素には入らない
- 統計的に信頼できるものは、予測可能なものとする

Copyright (c) 2005 NPO日本ネットワークセキュリティ協会 Page 10



既存の定量化方式


WGでの議論をふまえながら、
既存の定量化方式についてのサーベイも行った

米国nCircle社 IP360で実装されている方式

米国 NIAC が提唱した CVSS の方式

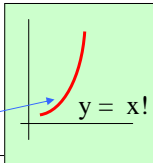
- ・NIAC=National Infrastructure Advisory Council
- ・CVSS=Common Vulnerability Scoring System

Copyright (c) 2005 NPO日本ネットワークセキュリティ協会
Page 11



nCircleのアプローチ

脆弱性自体の脅威
リモートから管理者権限が奪取されてしまう脆弱性は危険度が高いが、ローカルでアクセスしなければ攻撃が成功しないものは危険度は低い。これを表すように、 $y = x!$ という式で求められる曲線で表される式で、この数値を算出する仕組みになっている。



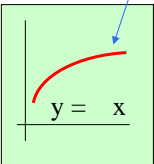
$$V_n = \sqrt{t_n} \cdot \frac{r_n!}{S_n^2}$$

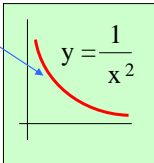
t_n : 脆弱性に関する情報が、主なニュースグループやセキュリティ関連のWebサイトに公開させてからの日数

r_n : 脆弱性自体の脅威(6段階“Risk Class”定義)

S_n : 攻撃を成功させるためのスキルセット(6段階“Type of Tool Available”で定義)

脆弱性の情報が公開されてからの日数
発見されたばかりの脆弱性の危険度は急激に上昇するが、どこまでも急激に高くなるというものではなく、ある一定の段階でその上昇は鈍化するということから、 $y = \sqrt{x}$ という式で求められる曲線で表される式で、この数値を算出する。





攻撃を成功させるためのスキルセット
攻撃のために専門的なスキルが必要か否かを、ツールの存在や攻撃手法の公開状況によって判断。攻撃のためにスキルが必要であるものほど危険度が下がるような $y = 1/x^2$ という式で求められ曲線で表される式で、この数値を算出している。

Copyright (c) 2005 NPO日本ネットワークセキュリティ協会
Page 12

CVSS のアプローチ JNSA

3種類にスコアが用意され、使う側でどれを使うかを選択することができる

10
×

Base Score
ベンダーによって設定され、一度設定されたら、その後に変更はされない

Base Scoreをもとに

Temporal Score
ベンダーによって設定され、時間とともに変化する

Temporal Scoreをもとに

Environmental Score
エンドユーザによって任意に設定され、最終的なスコアを意味する

条件によって係数が決まっているので、これを各スコアのマトリックスにしたがって計算
(値は一例です)

(例)

	Yes	No
・脆弱性が遠隔から攻撃できるか?	1.0	0.7
・脆弱性の攻撃に認証が必要か?	0.6	1.0

[修復方法のレベル]

・ベンダーから正式な解決策が提示された	0.87
・暫定的な解決策が提示されている	0.90
・解決策はあるが、正式なものではない	0.95
・解決策がないが、解決策を適用できない	1.00

[損害の可能性]

・損害の可能性はない	0.87
・少し影響がある	0.90
・重大な影響がある	0.95
・破壊的な影響がある	1.00

スコア(10点が危険度の最高点)

Copyright (c) 2005 NPO日本ネットワークセキュリティ協会 Page 13

今後の検討課題 JNSA

- 既存の定量化に、予測不可能な時系列変化要素が見出された
- 定量化に用いる「具体的な要素」の洗い出し(すでに検討を開始)
- いくつかのシチュエーションを用意する必要があるか?
「目的」によって、要素が変わる

Copyright (c) 2005 NPO日本ネットワークセキュリティ協会 Page 14

