攻める人，守る人

野村 隆昌
インターナショナル・ネットワークセキュリティ（株）

性善説をとっていた．つまり，相互接続と相互協力の精神は，この5年で完全に崩壊した．商売「そのもの」となったインターネット，私もそれで日々の糧を得ているわけだが，昔のような牧歌的な世界を望むことは完全に不可能となった．セキュリティ監査・教育を行う筆者が，その立場から，今日のネットワークセキュリティ現場をどう考えているかを述べる．

誰が攻撃しているのか

我々は仕事の上で，クラッカー☆1と交流を持つ．ネットワーク監査を行う上では攻撃の方法を知らなければならないし，彼らの考え方を踏襲しなければならない．

今日のインターネットは，新宿歌舞伎町と大差ない．猥褻と金，欲望と権利，犯罪，が渦巻いている．そんな状況であるから，セキュリティが声高に叫ばれるのである．攻撃をする者（クラッカー）らはいくつかのタイプに分類される．まず，素人同然のクラッカーである．彼らはイタズラ半分に攻撃を楽しむ．しかし，何をどう攻めたらどうなる，という知識と経験が浅い．たとえば，渋谷にたむろする目付きの悪い若者程度でたいしたことはできない．捕まえることは簡単だろうが，きりがない．しかし，こうした層は，単行本「Windowsの悪のマニュアル」や雑誌「ハッカージャパン」などによって日々量産されている．次に，最も恐れるべき，経験を積んだクラッカーについて．彼らは，ある程度確信犯的に攻撃を行う．踏み台を作るために地方国立大学を狙い，自分の名声のために有名企業を襲う．彼らは「引き際」や「足跡消し」まで知っている．捕まえることは難しい．最後は，職業的クラッカーである．依頼による攻撃を行う．このクラスは，物理的侵入までも辞さない．物理的にファイヤウォールの内側に入ることを目指す．また，あたりまえだが，彼らは国内／国外を問わず攻撃を行う．

問題は，管理者達が，攻撃しているクラッカーの姿をどこまで認識しているか，ということだ．レベルの違い，スタイルの違いを正しく理解していないと，やみくもに「攻撃されている」と騒ぐだけになってしまう．

誰が攻撃されているのか

どこのサーバでも常にある程度の攻撃は受けているだろう．しかし，破られたとなると話は別である．破られた，あるいは，破られていた，あるいは，破られていることに気づかないという場合，大抵は「最低限なすべきこと」を実施できていないに過ぎないことが多い．大企業であれば，本来の管理者以外が立てた実験サーバ，中小企業であれば，雑誌に書いてあった通りに立てたサーバ，あるいは，SIが立てたままのサーバ，である．新聞に載るのは，全攻撃成功分のうち，ほんの僅かである．報道されいているものの1000倍程度は攻撃が成功しているのではと推測される．

問題は，攻撃されていることをどこまで認識しているか，である．ご存知のように，ログは取り方によっては十分とれないし，一部のOSではろくなログもとれない．また，tcp_wrapperだけでは不十分なことは言うまでもない．それ以上やそれ以下の検知を行っている管理者がどれほどいるだろうか．

セキュリティって何だ？

ネットワークについて少し詳しい人であれば，こうした状況について「簡単なことなのに，なんでこんなに騒ぎになっているのか」と思うだろう．Y2Kにしても同様，誰でも気づく，いわば“アホ”みたいなことに，当時は気づいていなかった，というだけでこれだけの騒ぎである．セキュリティの本質はそういうところにある．たとえば，ルータのアクセス制御機能を使って正しく設定する，ということでかなりの被害は防げるが，それを実施できている企業は本当に少ない．また，余計なサービスは停止しよう，というと，

☆1 ネットワークの攻撃を行う者をすべてクラッカーと表記しているが，いわゆるハッカー／クラッカーの呼称問題議論に著者は興味がない．どちらでも同じと考えているが，あえてクラッカーと表記した．

「よく分からないから停止できない」といわれることがある．よく分からないって，ヨクワカラナイ物を動かしていて不安がない神経のほうがそれこそ私にはヨクワカラナイのだが．それはさておき，サービスの停止は簡単なことである．それすらできていない企業はたくさんある．また，すぐにファイヤウォールだの何だのと，誰かに頼る傾向にある．たとえば立派なDMZ（ファイヤウォールを利用した非武装地帯）を組む場合，本当にそれが必要なのだろうか．高価なファイヤウォールは必要なのだろうか．

セキュリティ問題は，所詮，人間の怠慢と注意不足にある．ということは絶対になくなることも，ある量以上に爆発的に増えることもない．しかし，一般的な人間程度に手を抜くと，安全は脅かされる．そこで最低限の努力をし続けなければならないと筆者は考える．

現在の問題点のまとめ

つまり，ネットワーク管理者の「現実の」侵入に対する理解が問題である．誰がどのように侵入するのか．それを淡々と理解しているべきだ．我々はまだまだその認識が足りないと思う．主な原因は，知識と経験の正しい報告・共有ができていないことではないだろうか．また，誤った知識や余分な知識，誤解が拍車をかけているように思う．

啓蒙活動と問題

我々セキュリティ関係者としては，なるべく真実を伝えなければならない．真実ということは，つまり，「～らしい」ではなく「～である」ということだ．そもそも，セキュリティ問題は「不安」を前提としているので，「～らしい」では不安は解決されない．また，迅速でなければならない．JPCERTのように，コードが公開された弱点を半年経ってから警告するようでは，まともな啓蒙活動とはいえない．

さて，そこで問題となるのが，攻撃コードを公開すべきか，である．私は積極的に公開すべきだと考える．攻撃コードの存在しない攻撃は，緊急に対処する必要がない．しかし，攻撃コードがあれば，すぐに対処をしなければならない．現実に誰でも攻撃できるとなれば，すぐに対策が打たれるだろう．しかし，それを知らなかった場合．こうしたコードは悪用され，知らなかった管理者は攻撃を受ける．弊害がないわけではない．

現時点では，私は，「攻撃コードは公開されるべき」だが「書籍でレベルの低いコードやツールをばらまくことは，クラッカーの底辺を広げ，管理者には本質的に役に立たないからやめるべき」と考えている．皆さんはどう考えるだろうか．

攻撃コード公開

たとえば，バッファオーバーフロー（バッファオーバーラン，スタックオーバーフロー）攻撃を例にとろう．非常に分かりやすい．

JPCERT-E-INF-99-0001-01「緊急報告－NFSマウントデーモンmountdを悪用したアタック」（初版1999/04/22）を引用[1]する．

「攻撃者にリモートから管理者（root）権限を不正に入手される可能性があります．その際に，不正なプログラムを送り込まれ，それを管理者権限で実行される可能性があります」と書かれている．可能性があります，可能性があります，と，二度繰り返されるよりも，技術的に詳細になりすぎるのでここではコードは省略するが，明らかにコードを読んだほうが分かりやすい．

また，コードを読めば，バッファオーバーフローという概念も非常に理解しやすい．

さて，対策については，再度JPCERTより引用すると，

(1) mountdのバージョンアップ
(2) NFSサービスの停止
(3) 全ユーザのパスワード変更と不要なアカウントの削除
(4) システムの再構築

と記述されている．

しかし，冷静に考えれば，他に，ルータ，ファイヤウォールレベルでの対策がある．rpc（remote procedure call）のポートとmountdのポートを閉じればよい．システムの再構築以前に指摘すべきではないかと思う．

話が逸れたが，ツール（攻撃コード）が存在するならば，積極的に公開すべき，という一例を紹介した．しかし，問題はそうもいっていられない．

流行

1つの攻撃方法が実行されると，なぜか流行る．発表と同時に複数のクラッカーが試そうとするのだろう．ともかく一定期間，同じ攻撃が続く．

これは間違いなく，攻撃コードの公開に起因している．こうした実状がある以上，公開は差し控えろという動きは否定しにくい．しかし，どこかで誰かが公開している以上，それを解析し，各自が危険性を確認することで，より安全が高まるのではないだろうか．それとも私は人間の善意に頼りすぎているのだろうか．

攻撃コードはどこにあるのか

ここまで書いた以上，攻撃コードが掲載されているページをいくつか紹介したかったが，たとえば，本書の目的に反するというような意見をいくつか頂戴した．ここでは紹介を避ける．この「判断」こそが，誤りの原因でもあると考えている．確かに不要かもしれないが，「本人が存在を確認するしかない」という私の意志には，反するものである．自己矛盾である．

嘘・大袈裟・まぎらわしい

セキュリティ関連製品の販売で頭が痛いのが，「誇大広告」や「妄想的宣伝」である．一言でいえば大袈裟．たとえば非常に高価なファイヤウォール製品には，美辞麗句が並ぶが，本当にそんなに素晴らしいものだろうか．あるいはまだ使う人は少数だがLinuxのipchains，あるいは世界に誇るべきdelegate．それらと比較して，どれほど安全なのだろうか．

マスコミにもかなりの責任がある．セキュリティ製品の本質は，「ある状況下で，それを安全な“状態”にできるか」という1点のみである．そうした切り口の記事というのはほとんど見たことがない．目にするのは「売れている」「インストールが簡単」といった，本質的ではないことばかりである．こうした，業者とマスコミのデタラメによって，安易に構築されてしまったファイヤウォールやルータ，サーバ環境が蔓延しているように感じられる．逆に地道にオープンソースソフトウェアで作られた環境のほうが安全と感じられることもある．

最後に，いうまでもなく，我々もその業界の一員であるから，大袈裟や嘘を言わないように努力している．果たしてこの文章は・・・ということは，皆さんで検討して判断してほしい．怪しいと思うことを確認する，それがセキュリティを高める唯一の方法なのだから．

参考文献
1) JPCERT: http://www.jpcert.or.jp/info/99-0001/, E-mail:info@jpcert.or.jp
(1999.10.7)

情報の公開と入手，そして判断することが大切だ

浅香　緑
情報処理振興事業協会（IPA）

“攻める人，守る人”という主題で，守る立場から何か書いてほしいという依頼を，エディタの塚本さんからいただきました．私が守る人の立場になるのは，侵入検出システム（IDS: Intrusion Detection System）を研究しているからなのでしょう．しかし野村さんのエッセイを読んで少々困ってしまいました．私は野村さんが攻撃する立場の方なのかと思っていたのですが，どうやら私と同じ守る立場の方のようです．おまけに私のように一歩引っ込んだところにいる研究者と違って，現場で日々セキュリティ監査・教育に取り組んでいる方です．野村さんの意見にうなずくところはあっても，反論するようなところはありません．今回は反対意見ではなく，同じ見解を若干異なる視点から述べたいと思います．

新しい侵入方法が見つかるほど儲かる製品？

ユーザがセキュリティ環境を構築するにあたって，製品の果たす役割も少なくありません．私が研究しているIDSも，この2年ほどの間に急速に製品が出てきました．ユーザの選択の幅が広がるということは歓迎すべきですが，若干気になるところがあります．それはIDSの多くが，シグネチャという侵入検出のためのルールをデータベースにして，それと合致するものを侵入とみなすという検出手法をとることにあります．この手法ですと未知の侵入は検出できないので，新たな侵入方法が発見されるごとにシグネチャのアップデートが必要になってきます．一方IDSの研究ではシグネチャベースでない，未知の手法も検出可能な方法もあるのですが，こちらは誤検出の問題などもあり，製品で取り入れているものはまだまだ少ない状況です．

シグネチャベースの検出手法はそれなりに有用なのですが，ベンダがこの手法だけを中心に製品を開発するのは問題だと思います（現状はそうなりつつあります）．それは常にシグネチャのアップデートに対応しなければならないからです．アップデート作業はユーザには負担ですし，もしそれが有償だったりすれば，新しい侵入事例が検出されればされるほどベンダは儲かることになります．意地悪な言い方をすれば，既知の侵入パターンにはパッチやその他の対応法も公表されているので，そちらで対応をとれば十分ということもあります．本当にそれだけのコストをかけて製品を導入する価値があるかは十分検討しなければなりません．ベンダとユーザは必ずしも利害が一致していないということを，忘れてはいけません．

製品には，多かれ少なかれこのような性質があるので，本当に何が必要かということは，ユーザ自らが考えなければなりません．セキュリティは厳重にすればするだけよいといったもので

はありません．それぞれのサイトには固有の事情もありますから，それを考慮してセキュリティポリシーを定め，ポリシーに基づいたセキュリティを構築するということが必要です．しかしいろいろ判断するためには，知識が必要となりますし，そのための情報の公開も問題になってきます．

攻撃コードは公開すべきか

最近はセキュリティ関連の書籍も増え，情報もいろいろ公開されてきましたが，その中で攻撃コードの公開については，まだまだタブー視されているように思われます．しかし一部で公表しない姿勢をとっても，インターネット上で探せば情報を簡単に入手できる状況でもあります．

野村さんのエッセイは，私だけでなくセキュリティ関係者ならばほとんど異議がないものと思われます．その中で攻撃コードの公開については，唯一議論の分かれるところかもしれません．しかしここでも私は野村さんと同意見で，攻撃コード，手法は無条件ではないとしても，公開されるべきだと思っています．その理由は自分自身の経験にあります．

私は1995年ごろから侵入検出システムの研究を始めたのですが，その当時実際どのような侵入の手口があるのか調べるために多大な労力を使いました．CERTなどに問い合わせても，当然教えてもらえるものでもなく，また現在のように簡単にインターネット上からツールや手法を簡単に得ることもできませんでした．あまりに情報が入手できないので，プロジェクトのメンバの誰かをアンダーグラウンドに潜伏させようかという話まで冗談で出たほどです．そのとき私は，研究をしようという人間までが，研究ターゲットの情報を簡単に得られないというのは，なんとこの分野は不便なのだろうと思いました．危険ということで，何でも非公開ということが有効なのだろうかと思いました．しかしどうやらそのような状況が問題だと思ったのは私だけではないようで，海外の研究者や学生からも攻撃手法の詳細を知りたいという声が徐々に広がり，現在米国のパーデュー大学を中心に，研究者が利用できる侵入手法などの弱点データベース（vulnerability database）の作成についての議論が行われています[1]．危なそうなものにはすべて蓋をするというのではなく，どのように情報を共有していくかなど，今後の議論には十分期待できるものがあります．

啓蒙活動も重要

繰り返しになりますが，セキュリティの基本は正確な情報を迅速に入手し，自ら判断し対応するということにあると思います．どこまでセキュリティを施すかは，サイトごとに異なりますし，やみくもにセキュリティを厳重にすればよいというものでもありません．常にユーザ自身が判断して決定していかなければなりません．判断のためには正確な情報が必要です．そのために手法等の知識も必要になってくるでしょうし，専門家による啓蒙活動といったことも重要でしょう．現在私の在籍するIPAにも，セキュリティセンターという部署があり，セミナーなどの啓蒙活動も行っています．“啓蒙”と口で言うだけなら簡単なのですが，具体的に何をするかは難しいところです．一朝一夕に効果があがる方法というのはないのかもしれませんが，有効な方法をいろいろ考えることは重要だと思います．

参考文献
1) http://www.cerias.purdue.edu/vdbw.html

(1999.10.12)

私は攻める側

匿名☆2

塚本氏および野村氏からの要請により攻める側の立場から述べさせていただきます．係る議論の有効性のあるやなしやは別として，野村氏の呼称されるところのクラッカーに関して，やはり，作為的あるいは無作為的な誤謬があるのは否めない事実ですし，一部に係る誤謬を煽り立てる書籍が出回っているのも事実です．私が今回意見を述べさせていただくゆえは，クラッカーの実像を多少なりとも知っていただくためです．

クラッカーに対する根本的誤謬

現在，マスコミに登場するクラッカーはそのほとんどが誇大に，かつ不正確に報道されています．一体，クラッカーと呼ばれている人達はどう定義されるべきなのか，それすら曖昧なまま，コンピュータ業界特有の，無意味な技術信仰と，デマゴーグ的な煽り立てによって，クラッカーという存在が，神格化，あるいは悪魔化されているのではないでしょうか．クラッカーといわれている人のほとんどは，ネットワーク上において，ある意味で無害であると，あえて申し上げておきます．以下，クラッカーに対する簡単な定義と危険度を4段階に分けて説明しましょう．

☆2 エディタ注釈
会誌の記事には社会的な責任がある．そのため，匿名記事は厳しく戒められねばなりません．しかし，今回の記事では，あえてそのタブーを犯しました．それは，守る側の主張だけでなく，どうしても攻める側の主張が必要であると判断したからで，それには匿名でなければ書いていただけなかったからです．匿名記事にするにあたっては，会誌編集長に事情を説明し許可を得ました．

クラッカーとは

通信ネットワークあるいは物理的有形力を用いて，特定あるいは不特定の第三者の所有する電子計算機にゆえなく接続し，電子計算機，周辺機器，またはデータを不当に破壊し，あるいは破壊しようとするもの．また，データを窃取し，あるいはしようとするもの．

クラッカーの危険度

クラッカーといえるのは前記の定義で述べた通りですが，実際，この定義に当てはまる人間はネットワーク，UNIXに関して，ネットワークプログラミングに関して，開発に不自由しない程度の知識を持っています．人にもよりますが，最高5年程度の開発経験があれば，どんなにコンピュータに向いていない方が，どんなに試行錯誤をしてもクラッキングに必要な係る知識は身に付けられるでしょう．できればアセンブラを知っているに越したことはありませんね．自分でプログラミングをしないにしても，アメリカや，東欧，北欧のサイトからダウンロードしてきたコードを解析できれば，それである程度目的は達せられます．

0．危険度のないもの

CGI，Pearl，あるいはネットワークプログラミングの知識がなく，単に本を聞きかじり，誇張するもの．この層が一番多いでしょう．

I．危険度が低いもの

掲示板荒し．ジャンクメーラー．CGI，Pearlなどやネットワークアーキテクチャについてはあまり知らないが，何をどうしろ，と指示されれば100サイトに付き1サイト程度は成功する．

II．やや危険度が高いもの

パスワードクラック，セキュリテイの穴の情報を得て，自ら適切なツールを探し，あるいはツールを作ることによって，アカウントを取得したり，成りすましなどができ，実際にサイトに潜入できるもの．大学生，大学院生などに多い．

III．危険度が高いもの

ファイヤウォールの設定ミスやWWWサーバ，sendmailなどの不備について実際に不備の多いサーバを自ら発見し，ツールを用いるか，あるいはツールを作ることによって侵入するもの．あるいは，ウイルス，トロイの木馬などの迷惑兵器を量産するもの．

前者の場合は背後に何らかの組織が介在している可能性も考えられる．特に強力なのはイスラエル，ハンガリーなど東欧，です．筆者もあるサーバにてイスラエルのクラッカーと鉢合わせをしたことがありますが，豊富なツールと手段で，おおらかにクラッキングを楽しんでおられました．

どのように進入するのか

踏み台を探すにはやはり大学が一番でしょう．電算室あるいはコンピュータの利用形態はいろいろ考えられますが，一番手っ取り早いのは，電算室に入る利用カードが学生証などではなく，バーコードなどで入室管理されているところでしょう．教育施設の管理者さんは，有名大学であればあるほど，相当程度入室証が偽造されている可能性があると考えていた方がよいでしょう．

この時点で本来刑法上の住居不法侵入，文書偽造など，諸罪が適用される可能性があります．

電算室でのパスワードは直に覗き込む，メモを奪う，あるいはメモ用紙に写っている筆跡からユーザ，IDなどを得ます．もしここで，メモ用紙を盗んだりすれば窃盗罪です．通常クラッカーはメモを残したり，メモに書いたりせず，すべて暗記します．

次に，大学や監視の甘いインターネットカフェ，総合大学などで，学生が不用意に立てているサイト（不用意にFTPを開けていればベストです）を使い，目標に対する事前調査を行います．キーワードは一言，しつこさです．成功するもしないもすべてしつこいこと，この一言に尽きるでしょう．

クラッカーはなぜ，クラッキングをするのでしょうか．別にネットワークには，詐欺を始め，さまざまな行為類型の犯罪者達がいるのです．モバイル化が進み，使い捨て，あるいは飛ばし電話を使って，まったく足をつけずにクラックすることは容易になったともいえるでしょう．しかし，クラッカーが係る苦労をして，アカウントを得て，サーバに侵入し，利益のあるサイトはどんなサイトか，それを考えてみるのが一番重要ではないでしょうか．個人情報のやりとりはネットには流すべきではない．筆者はそう考えます．

もっといろいろ，述べたいことはあったのですが，字数を大幅に超えていますのでこの辺で支離滅裂に，失礼いたします．

(1999.10.18)

目で見て感じられる「状態」を議論せよ！

野村 隆昌
インターナショナル・ネットワークセキュリティ（株）

浅香さん，匿名さん，貴重なコメントありがとうございました．また，匿名許可などにより，従来の，ステレオタイプ的なセキュリティ議論の定石を破る場になりました．塚本様をはじめ関係各位に深く感謝いたします．

IDS（侵入検知システム）

お二人の意見を拝見しまして，いく

つか気がついた点についてコメントしたいと思います．まずはIDSについて述べます．

ご指摘のように，IDSの問題点の本質は，シグネチャをどうするか，の1点に集約されます．浅香さんは，シグネチャの開発とアップデートの問題点を指摘されました．ベンダの限界（?）についての話題と認識しました．

ご存知かと思いますが，違う試みを紹介します．たとえば，NFR社のN-Code．NFR社のIDS，Network Flight Recorder（NFR）には，N-Codeという公開されたシグネチャ記述言語があります．これは，Linux開発モデルのバザール型（伽藍とバザール[1]のバザール）に近い形でシグネチャを生産できるのではないでしょうか．あるいは，この「方法」をもう少し進歩させ，メタシグネチャDBを開発する，「しかけ」を準備するという案です．

さらに，もう1点，現状，多くの人の目は，ネットワーク型IDSに向いていますが，そろそろ，エンタプライズ型IDSでしょう．いくつかの攻撃手法は，すでに，既存のIDSの能力を超えつつあります．ネットワーク型，サーバ型，クライアント型とし，相互に通知可能な仕組みです．そろそろ完成された製品が出るだろうと予想し期待しています．

（しつこく）攻撃コード公開

大前提ですが，日本語以外のリソースはたくさんあります．しかし，我々の言語圏オリジナルの情報は少ないので誰かが積極的に扱い，公開されている状況になることを私は望んでいます．

まず，日本の大学で，ネットワークセキュリティを専門に扱う「場所」がないということが，攻撃コード公開に歯止めをかけているように思います．米国では時々大学が絡みつつ（一部，濡れ衣スキャンダルになったりしていますが），攻撃コードの収集・公開を行っています．少々学術系がきちんとしたスタンスでもっと大幅にセキュリティを扱うようになれば，知識の集約と開放が加速されるのではと期待しています．セキュリティの根本の問題は，「不安」です．それを解消するためには，ある程度の開放が必要だと感じます．

啓蒙

浅香さんのおっしゃったことに一言付け加えさせてもらえれば，「どこまでセキュリティを施すかは，サイトごとに異なりますし，やみくもにセキュリティを厳重にすればよいというものでもありません．常にユーザ自身が判断して決定していかなければなりません．判断のためには正確な情報が必要です．」という一文ですが，これは「セキュリティは緩くても構わない」ということが言いたいのではなく，「セキュリティに対する正しい理解と知識と判断を」というところに重要なポイントがあります．

実在するクラッカー

匿名氏は，根本的誤謬，と表現されていますが，基本的には，「ある種」の人とカテゴライズせずには議論が進まなかったマスコミ・報道のあり方に対する抵抗を感じます．確かに直感的にこれまでのセキュリティ報道のあり方は間違った方向であることを感じます．時としてセキュリティは，「見えざる脅威」が「売り物」なのですが，これを，見えざる脅威のまま商売することは危険だ，と，再認識します．販売するにあたっては，「目に見える脅威」にすることが大切であると感じます．匿名氏は，いかにもクラッカーらしく，自分の実態を示しました．

「状態」を切り出せ

私がセキュリティの説明をするときによく使う言葉に，「状態」があります．「安全な状態」「正しくフィルタリングされた状態」「echoが返らない状態」「vulnerabilityがある状態」などです．セキュリティは，明日は違う「世界の状態」を知ったうえで，「今の状態」を認識することで，高めていくことが可能です．その中で考えるならば，「I'm here.」という匿名氏からのメッセージは，「クラッカーが実在する状態」を非明示に明示しています．

再度啓蒙
～目で見て感じられる「状態」を議論せよ！～

これまでの啓蒙は，「～の虞がある」形式でした．そこから想像できるのは，「ハッカーがいるかもしれない状態」であり，それも，「虞」の域を出ないものです．次世代の啓蒙は，「あなたが置かれた状態の判断の方法」に徹してはどうでしょうか．「コレはこの程度，こうなんだよ」と言わないと，効果的な啓蒙ではないように思います．理系であれば誰でも知っている「臨界の虞」は，あのような形で「臨界という状態」になりました．臨界になってからでは遅い，のです．

参考文献
1) Raymond, E.: The Cathedral and the Bazaar, Linux Congress (May 1997).

(1999.10.19)

～ 議論の続きは，次のURLをご覧ください．http://www.ipsj.or.jp/magazine/interessay.html ～