1. 脆弱性にかかわる法的側面について

弁護士／宇都宮大学講師
高橋 郁夫　ikuo@comit.jp

脆弱性は，利用者もしくは攻撃者の特異な利用・攻撃の場合に生じる安全性の欠如状態をも指す点で，通常の瑕疵よりも広い概念となる．この概念の違いが，脆弱性を修正すべき義務の法的な位置づけを左右することになる．さらに脆弱性の発見行為について，不正アクセス禁止法の該当性，契約上の制限の問題があり，脆弱性の公開については，同様に契約上の制限の問題や「完全開示」論と「責任ある開示」論の衝突，表現の自由の中での位置づけの問題がある．特にこの最後の問題に関連して，ソフトウェア等脆弱性関連情報取扱基準は，注目すべきものとなる．

脆弱性の概念☆1

セキュリティ上の問題を引き起こす問題点を脆弱性というとき，その脆弱性は，法的にどのような問題を有するものとして議論されるのであろうか．その法的な問題点をできるだけ広くとりあげて議論することが本件での問題となる．

ここで，「脆弱性」を定義するとすれば，(1) 不具合であること──プログラム等が意図した（正しい）結果をもたらさない状態であること (2) セキュリティに関すること── 少なくても，その「不具合」が，電子計算機の運用に関する機密性，保全性，可用性に関連するものであること，(3) (1) の不具合が，外部からの攻撃を誘引するものであること (4) (2) および (3) に関連する (1) を引き起こす要因または事項であることの 4 つ観点が必要となるものと思われる．法的に利用されることのある「瑕疵」という用語との差異を示したのが，図 -1 になる．

この図で明らかな通り，一般に議論されている欠陥というものに比較して，脆弱性というのは，特殊な利用や攻撃によって，安全性が損なわれる点まで含むという意味できわめて広い概念である．その意味で，脆弱性があること自体を，瑕疵であると認識することはできないであろうと思われる．

ソフトウェアの提供行為と脆弱性

では，ソフトウェアの提供行為に際して，ソフトウェアに脆弱性が存在した場合，それは法的にどのようなものとして位置づけられるのか．一般にソフトウェアの提供行為は，ライセンス契約の概念で捉えられる．すなわち，ソフトウェアは著作権法上の保護を受けるが，著作権法のみで規律されるものではなく，ソフトウェアの使用に関し，ライセンス契約が締結され，ライセンサー（ベンダ）がライセンシー（ユーザ）に対し，ライセンス契約の範囲内でソフトウェアの使用を許諾するのが通常

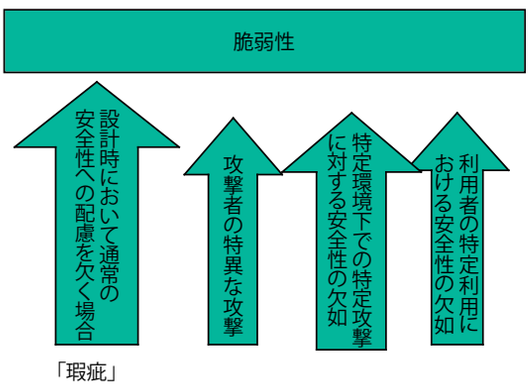

図 -1　脆弱性の概念

☆1　なお，本稿のテーマについては，脆弱性情報取扱の法律問題研究会「情報システム等の脆弱性情報の取扱いにおける法律面の調査」（http://www.ipa.go.jp/security/fy15/reports/vuln_law/documents/vuln_law_2004.pdf）が詳細に報告しており，本稿の分析の詳細を知るためには，かかる報告書を参照されたい．

である．ライセンス契約の具体的な内容（ライセンス条件）をどのようなものにするかは，私的自治の原則，契約自由の原則により，基本的には契約当事者間に委ねられることとなる．なお，ソフトウェアは無体物であるため，ソフトウェアのライセンス契約において，一般に製造物責任法の問題は生じない（製造物責任法 2 条 1 項）．

では，上記のような脆弱性について，そのプログラム等の提供者は，それを脆弱性のない状態にまで，修補すべき義務があるのか，あるとして，それは法的にどのように位置づけられるのか．

この点については，一般的な事象としては，脆弱性に関して，ライセンス契約でもって一定の定めをなすことが考えられ，その定めの有効性の問題となることになろう．しかしながら，本稿では，まず，脆弱性の法的な意義を明らかにするために，そのような契約上の定めがない場合を考えてみることにする．法的には，ソフトウェアの提供行為については，一定のなすべき債務ということが言え，脆弱性のあるソフトウェアの提供が，債務の本旨に従った債務の提供がなされるかどうかという点が問題になるものと考えられる（なお，解釈論としては，明らかではないが，履行として認容した後は，瑕疵担保責任（民法 570 条，566 条，商法 526 条 1 項等）の問題となると考えられる）．しかしながら，かかるソフトウェアの提供行為が，債務の本旨に従った債務の提供か否かという点については，設計時における通常備えられるべき安全性の程度を備えているかどうかで判断されると考えられよう．

ソフトウェアに関する何らかの不具合に関連して，ライセンス契約においては，欠点や脆弱性については責任を負わない旨の条項が定められている場合があり，そのような条項が，法的に効力を有するのか，という問題がある．消費者契約法の適用がなされるべきものかどうかという点とそもそも上記のように設計時点において通常備えられるべき安全性の程度を備えているかという点をもとに具体的な事例との関係で考慮されるべきものと考える．

脆弱性の発見行為と法的な問題点

◆不正アクセス禁止法との問題点

特定の Web サイトの脆弱性が報告されている場合に，その情報を利用し，または，応用して，他の Web サイトに同種の脆弱性が存在するかどうか確かめること，そして，その結果，不正アクセスをしてしまうことになるのではないかという論点がある．

我が国においては，「不正アクセス禁止法」により，無権限アクセスに対して，刑事的な規制がなされている．法により禁止されている「不正アクセス」は「他人の識別符号を入力して」または，「特定利用の制限を免れることができる情報（識別符号であるものを除く）又は指令を入力して」「アクセス制御機能により制限されている特定利用をし得る状態にさせる行為」（不正アクセス禁止法第 3 条）である．脆弱性に対する問題との関係で，意識しておくべきことは，故意犯であり，システムを対応し得る状態におく（アクセス）という認識が必要であるということである．その一方で，ファイルの改竄であるとか，情報の取得，漏洩などといった「犯意」などといったものは必要ではないこととなる．その行為において，脆弱性の情報の検証をするためというような意図があったとしても，犯罪の成否には，関係はない．また，この法律の制定の当時において，すでに，脆弱性の検証などが違法となるのではないかという議論があったにもかかわらず，そのような意図を考慮せずに犯罪が成立することを当然としているのであり，そのような立法の経緯からも脆弱性の検証の意図が犯罪の成否に影響を与えるものとは思えない．また，同様な趣旨からして，正当業務行為などの見地から，違法性が阻却されると考えることは，困難であろう．

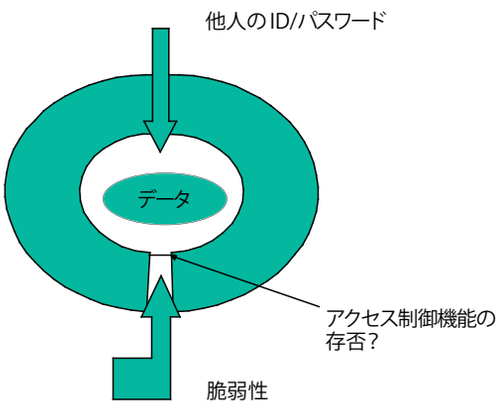

図 -2　脆弱性と不正アクセス禁止法

この法律の適用に関し，いわゆる脆弱性を利用するタイプの不正アクセス行為については，アクセス制御機能の回避をしたといえるかどうかが，犯罪の成否を決める鍵になる（図 -2）．同法 3 条 2 項 3 号が，主としてセキュリティホールを利用して攻撃する方法を主として想定した規定とされている．図 -2 で示したように脆弱性のある部分というのは，厳密には，OS によって提供されるべきアクセス制御機能が，存在しない．しかしながら，社会的には，「制限」が存在していると見て保護すべき場合，すなわち，「普通は，そこは使えない，そこを使うことは社会通念上認められていないといえるという場合」には，社会通念上，アクセス制御機能ありとすると

いうことである．ここでは，結局，技術的な観点よりも社会通念という観点が入って来ざるを得なくなることになる．したがって，かかる形態の不正アクセス行為の限界については，アクセス制御機能の回避といえるかどうかについては脆弱性の種類および攻撃手法との関係でさらに困難な問題がある．

これらの問題が具体的に議論されたのが，コンピュータソフトウェア著作権協会（ACCS）の CGI を操作し，保存されていた個人情報を入手したとして，不正アクセス禁止法違反に問われた大学の研究員の事件，いわゆる office 氏の事件である．この第 1 審の判決（東京地裁判決・平成 17 年 3 月 25 日）が報道されており，これらの論点との関係で簡単に触れると以下のようになる．まず，裁判所は，「特定電子計算機」をコンピュータのプロトコルごとに捉えるべきという弁護側の主張を排斥し，アクセス制御機能の有無を特定電子計算機ごとに判断するとした．そして，「本件においては，本件 CGI および本件ログファイルを閲覧するには，FTP を介して識別符号を入力するものとされていたのであるから，本件サーバはアクセス制御機能を有する特定電子計算機といえる」とした．その上で，制限がなされていることの意味については，「プログラムの瑕疵（かし）や設定上の不備があるため，識別符号を入力する以外の方法によってもこれを入力したときと同じ特定利用ができることをもって，ただちに識別符号の入力により特定利用の制限を解除する機能がアクセス制御機能に該当しなくなるわけではないと解すべき」として，脆弱性がある場合でも，アクセス制御機能ありとすべき場合があることを認めており，「本件の各特定利用ができたのは，プログラムの瑕疵または設定上の不備があったためにすぎないのであり，アクセス管理者が本件アクセス行為のようなかたちで特定利用することを誰にでも認めていたとはいえない．よって，本件においても，本件 CGI および本件ログファイルの各閲覧は，アクセス制御機能による特定利用の制限にかかっていたものということができる」とした．その結果「被告人は，本件 CGI および本件ログファイルの閲覧という各特定利用を制限している FTP プロトコルを利用したアクセス制御機能を有する本件サーバに，その制限を免れる指令を電気通信回線を通じて入力して本件サーバを作動させて前記各特定利用をしうる状態にしたといえ，被告人の行為は，不正アクセス行為に該当する」と判断しているのである．

◆脆弱性発見行為のその余の法的な問題

脆弱性発見行為のその余の法的な問題として，いわゆるライセンス契約上の問題と脆弱性の発見行為の問題が挙げられる．具体的には，リバース・エンジニアリングによって発見する行為はどうなのかという問題がある．一般に，ライセンス契約においては，ソフトウェアの著作権を保護するために，このリバース・エンジニアリングを禁止する条項が置かれることがある．しかしながら，当該条項の有効性に関しては，独占禁止法に抵触するのではないかという立場も多い．また，仮にリバース・エンジニアリング禁止条項が有効であると判断されるケースであったとしても，単に受付窓口に脆弱性情報を報告したに過ぎない場合は，契約違反・債務不履行の問題は生じ得るが，ライセンサーにどのような財産的損害が発生したと考えるべきかという問題があると思われる．

脆弱性情報の公開の法的問題点

◆脆弱性情報の公開と契約上の制限

秘密保持契約と脆弱性の公開

ソフトウェア商品について販売開始後に独立してセキュリティ調査会社に，その脆弱性の調査を依頼する際には，秘密保持契約を締結するということがある．その場合に，その脆弱性の情報を公開することはどうかという問題がある．このような場合，まさに，かかる脆弱性の公開が，そのソフトウェアやそれを提供している会社にとって致命傷となることもあるために秘密保持契約を締結するのであるから，かかる秘密保持の利益は十分に保護に値し，かかる条項に違反し，公開することは許されないと考えるべきである．もっとも，その脆弱性の程度が大きい場合，また，公的機関等に対して秘密保持を前提にして報告する場合は，また，別個の考慮が可能であろう．

ライセンス契約と脆弱性の発見

同種の問題として，ライセンスを受けているユーザが，ソフトウェアの脆弱性を発見し，ライセンサーの同意を得ないまま他社に通知するとき，その契約法との関係はどうなるかという問題がある．この点については，発見するために種々の利用をすることが，ライセンス契約違反ということは困難なように思われる．また，それによって得られた脆弱性情報の公開を禁止する趣旨というのを一般のライセンス契約に読み込むことは困難なように思われる．

◆脆弱性情報の公開と表現の自由等

表現の自由との関係

脆弱性情報を公開することが法的にどのように判断されるべきかという問題がある．

この点については，まず，脆弱性の情報も，その情報

「完全開示」対「責任ある開示」

• 攻撃者はこれらの記述をすでに知っており，彼らがなし得る方法をすべての人が知り得るのがベストである．	• 脆弱性の大多数は，自己の力量の顕示などの目的によって導かれて調査され，公開される．
• ベンダは，ひとたび公開されれば脆弱性を隠すことはできない．	• 脆弱性を公開する効果的な他の方法がある．
• 将来におけるよりよいシステムをつくるために脆弱性情報は公開することが必要である．	• よりよいシステムを作るためといっても脆弱性の詳細を教えたりテストしたりする必要はない．
• 脆弱性情報は発見者の財産である．	• 自分の財産だといっても，自分の宣伝，財産的利益，エゴのメッセージなどである．

表 -1　「完全開示」対「責任ある開示」

自体を発表することは，表現の自由として，憲法上，保護されるべき権利として尊重に値するということがいえるであろう．また，脆弱性情報についていえば，完全開示論と提供者等に修正の機会を与えるべきとする「責任ある開示」論との対立がある☆2（表 -1）ということができる．

この点については，前述の office 氏事件においては，裁判所は，情状関係の部分であるが，「本件アクセスが可能となるセキュリティホールを発見し，これを ACCS 等に知らせないまま，自己の能力，技能を誇示したいとの動機もあって，セキュリティに関するイベントで発表するために，本件各不正アクセス行為に及んだのであって，このような犯行の経緯や動機に酌量の余地はない．被告人は，関係機関にセキュリティ対策を広く知らせるために本件各アクセス行為をし，その手法を発表したなどと供述するが，ACCS 等に事前に報告せずに修正の機会を与えないまま公表し，攻撃の危険性を高めているのであって，供述するとおりの動機があったとしても，到底正当視できるものではない」と述べている．裁判所としては，事前の通知なしの公開について積極的な評価をしているといえないことは明らかであろう．

脆弱性情報の公開と社会的評価

脆弱性を発見され，通知されたソフトウェア会社が，たとえば，そのような評価がもとで，製品の売り上げが低下した（もしくは，営業上の地位が損なわれた）として発見・公開者に対して損害賠償を提起してきた場合，発見・公開者の立場はどのように取り扱われるかという問題がある．インターネットの Web ページで脆弱性につき公開するような場合は，公然と事実を摘示し，名誉を毀損したと一応は言え，名誉等の侵害ということで民事上不法行為が成立し，損害賠償義務が発生することになりそうである．しかしながら，事実の摘示行為が，①公共の利害に関する事実に係り，②目的がもっぱら公益を図ることになったと認める場合（刑法 230 条の 2 参照）などには，違法性が阻却されることになり，民事上の損害賠償責任を負わないということも考えられる．

脆弱性情報の流通のスキーム

◆ソフトウェア等脆弱性関連情報取扱基準

経済産業省は「ソフトウェア等脆弱性関連情報取扱基準」（平成 16 年経済産業省告示第 235 号）☆3 を公示した．そして脆弱性関連情報の届出の受付機関として独立行政法人情報処理推進機構（IPA），脆弱性関連情報に関して製品開発者への連絡および公表に係る調整機関として有限責任中間法人 JPCERT コーディネーションセンター（JPCERT/CC）を指定した．

この制度は，「情報システム等の脆弱性情報の取扱いに関する研究会報告書～ 脆弱性関連情報流通の枠組み構築に係る提言～」☆4 において①ソフトウェア製品の脆弱性と，②Web アプリケーション脆弱性に関連して，脆弱性関連情報の届出を受け付ける機能（受付機関），ソフトウェア製品の脆弱性の公表時期を調整する仕組み（調整機関），対策方法や届出件数等の統計データを集

☆2　この議論については，拙稿「ソフトウェアの脆弱性をめぐる法律問題」（経済産業省「セキュリティホールに関する法律の諸外国調査」所収）（http://www.meti.go.jp/policy/netsecurity/Foreign_Law_Report.pdf）を参照されたい．
☆3　http://www.meti.go.jp/policy/netsecurity/downloadfiles/vulhandlingG.pdf
☆4　http://www.ipa.go.jp/security/fy15/reports/vuln_handling/documents/vuln_handling_2004.pdf

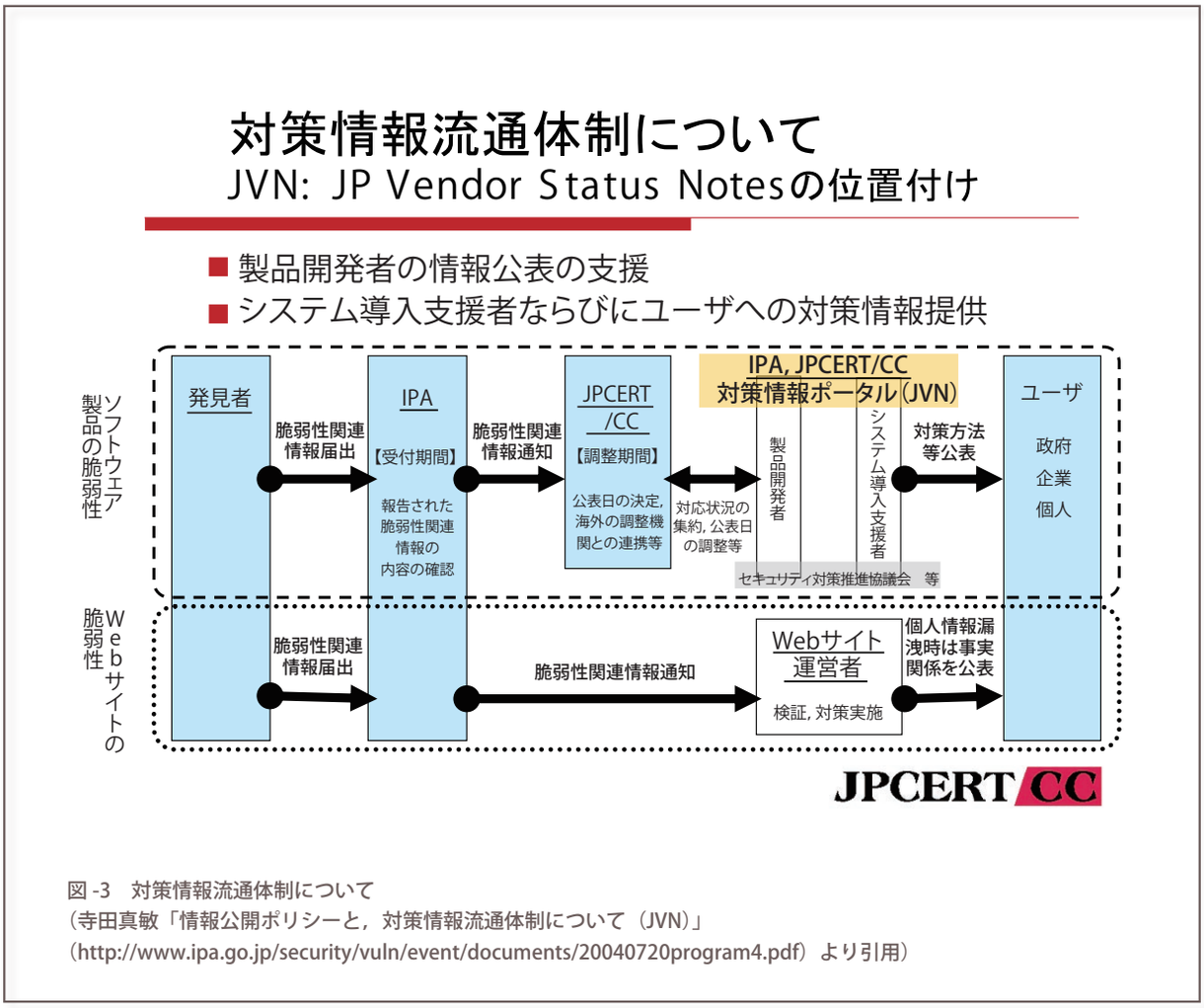

図 -3　対策情報流通体制について
（寺田真敏「情報公開ポリシーと，対策情報流通体制について（JVN）」
（http://www.ipa.go.jp/security/vuln/event/documents/20040720program4.pdf）より引用）

積・公表する機能が必要という認識のもとに，「脆弱性関連情報の流通制御」と「対策方法の適用の迅速化」を両立させるために，脆弱性関連情報の公表に係るルールを策定し，発見者，製品開発者，Web サイト運営者が本枠組みに協力することに意義があるという提案に対応したものである．この基準が念頭に置く体制は，以下の図のようなものである（図 -3）．なお，詳細な点については，研究会報告書や「脆弱性関連情報取り扱い説明会」資料[☆5] を参照いただきたい．

◆基準の法的意義と運用の成果

この体制は，その体制に準拠することを「関係者に推奨するもの」にすぎないことに留意すべきである．この体制に従ったことによって法的に直ちになんらかの効果が生じるものではない．また，脆弱性を発見するのに，不正アクセス禁止法違反などの行為をなしたときにこのような脆弱性情報の取扱体制に準拠したからといって，その違法性が阻却されるというようなこともない．

一般的な観点で考えれば，かかる取扱体制などを完全に無視して脆弱性を発表するような発表者の行為について，その態様・程度において，その Web サイトの運営者について，業務を運営する権利を妨害した，また，個人情報の漏洩がなされた場合には，その情報主体に対して，その情報について管理する法的利益を侵害したとして，民事的な責任を問われることは十分にあり得ることだということができる．

（平成 17 年 4 月 1 日受付）

☆5 http://www.ipa.go.jp/security/vuln/event/20040720.html