無断転載を禁じます

SI 事業者における脆弱性関連情報取扱に関する体制と手順整備のためのガイダンス

第 1.0 版

2005 年 8 月

社団法人　情報サービス産業協会

Japan Information Technology Services Industry Association

社団法人　電子情報技術産業協会

Japan Electronics & Information Technology Industries Association

目次

1. はじめに

1.1. 背景

これまで、コンピュータ・ウィルスやコンピュータ不正アクセス等によって不特定多数の者に対して引き起こされる被害の拡大をできるだけ限定された範囲に局限化するための取組みとして、コンピュータ・ウィルス、不正アクセス届出制度やインターネット定点観測などの仕組みが運用されてきた。ところが近年、ソフトウェア製品やウェブアプリケーションの「脆弱性」の悪用による被害が急増し、その被害拡大のスピードは個々のユーザによる対処だけでは困難な状況となりつつある。これに対し、「脆弱性」そのものをできるだけ早期に取り除くことによって、被害の発生そのものを抑制するための取組みとして、経済産業省告示「ソフトウェア等脆弱性関連情報取扱基準」が2004年7月7日に公示され、翌日8日から施行された。この告示および、告示を受けて7月8日に発表された「情報セキュリティ早期警戒パートナーシップガイドライン」では、発見された脆弱性関連情報の国内における受付から公表までの体制と手順を定めている。この動きに対し、(社) 電子情報技術産業協会 (JEITA) および (社) 情報サービス産業協会 (JISA) では、情報システムを構成するソフトウェア製品の製品開発ベンダーが「情報セキュリティ早期警戒パートナーシップ」に賛同し、提供製品に係わる脆弱性への対応を率先かつ協調して進めるために、「製品開発ベンダーにおける脆弱性関連情報に関する体制と手順整備のためのガイドライン」をまとめ、2004年10月に公表した。

ここで、情報セキュリティ上の「脆弱性」とは、ソフトウェア製品およびウェブアプリケーションにおいて、コンピュータ・ウィルスや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うる安全性上の問題箇所である。通常の使用では問題とならないが、脆弱性を悪用することによりネットワーク攻撃等に利用される可能性があるという点において、通常の不具合やいわゆるバグとは区別される。

一方、実際に脆弱性を悪用した被害拡大を抑制するためには、脆弱性の早期発見と製品開発ベンダーによる対策の早期提供だけではなく、提供された対策を迅速に導入・実施するという対策公表後の対応や、ウェブアプリケーションで発見された脆弱性を迅速に修正するといった、脆弱性通知後の対応が非常に重要となる。これは、前述の経済産業省告示等で示された脆弱性関連情報取扱い体制の外側の役割ではあるが、特に、顧客からの委託を受け、情報システムの構築・運用・保守等を行っているSI事業者にとっては、脆弱性への迅速かつ適切な対応が社会からも顧客からも求められることになる。

1.2. 本書の位置付け

本書は、情報システムやウェブアプリケーションの構築・運用・保守等を行っているSI事業者が、脆弱性情報が公表された後、製品開発ベンダーや顧客と連携し、迅速かつ適切な対応をとるために必要な社内体制や対応手順を整備するための手引書として活用されることを目的としたものである。また、なかなか顧客に理解されにくいソフトウェア等の脆弱性と瑕疵の区別を理解していただくための啓発にも活用可能であると考える。修正対策が与えるシステムへの影響、情報サービス産業の元請－下請という業界構造、顧客との対策費用調整など、脆弱性対応にあたりSI事業者が考慮しなくてはならないポイントは非常に多岐にわたるため、事前に対応体制や手順を定めておくことは有効である。なお、本書では、各事項において「必要である」等の表現を用いているが、本書はあくまでSI事業者にとっての「参考書」という位置付けであり、先に公表したJEITA/JISAの製品開発ベンダー向けガイドラインが、製品開発ベンダーとして「整備すべき」必要最小限の要件を示している点と異なることに留意されたい。

以下の第2章では、前述の告示等で示された国内の脆弱性関連情報取扱体制の概要およびSI事業者の位置付けについて全体像を述べる。第3章では、SI事業者が脆弱性に対応するために共通的に必要な事項を示す。第4章では、情報システムで使用しているソフトウェア製品等に関する脆弱性が公表された際の対応手順を、続く第5章では、ウェブアプリケーションに関する脆弱性が通知された際の対応手順について述べる。最後に、付録として様式例、システム開発セキュリティ・センターのモデル事例などを紹介する。

特に、ウェブアプリケーションの脆弱性への対応には、設計・構築の段階で脆弱性をウェブアプリケーションに作り込む可能性を最小限に抑えることが重要であるが、本書の記述対象範囲には含めない。また、脆弱性を悪用したインシデントが実際に発生してしまった場合の対応については、これまでにもいくつかの参考書が出ているため、本書の対象外とする。

本ガイドラインの前提となっている文書一覧を次に掲げ参考とする。

(a) 経済産業省 : 告示第235号「ソフトウェア等脆弱性関連情報取扱基準」、2004年7月7日、http://www.meti.go.jp/policy/netsecurity/downloadfiles/vulhandlingG.pdf

(b) 経済産業省 : 告示第236号、2004年7月7日

(c) 独立行政法人 情報処理推進機構(IPA)、有限責任中間法人 JPCERT コーディネーションセンター(JPCERT/CC)、社団法人 電子情報技術産業協会(JEITA)、社団法人 日本パーソナルコンピュータソフトウエア協会(JPSA)、社団法人 情報サービス産業協会(JISA)、特定非営利活動法人 日本ネットワークセキュリティ協会(JNSA) :「情報セキュリティ早期警戒パートナーシップガイドライン」、2004年7月8日制定、2005年7月8日改訂、http://www.IPA.go.jp/security/ciadr/partnership_guide.pdf

(d) JPCERT/CC : 脆弱性関連情報取扱ガイドライン、2004年8月25日、http://www.JPCERT.or.jp/vh/guideline.pdf

(e) JEITA-JISA ：「製品開発ベンダーにおける脆弱性関連情報取扱いに関する体制手順整備のためのガイドライン」、2004 年 10 月 13 日、http://it.JEITA.or.jp/infOSySInfo/0407JEITA-guideline/

2. ソフトウェア等脆弱性関連情報取扱体制と SI 事業者の位置付け

2.1. 「情報セキュリティ早期警戒パートナーシップ」の概要

2.1.1. 「情報セキュリティ早期警戒パートナーシップ」の狙い

(a) 新規の脆弱性による社会的規模での被害防止

脆弱性関連情報は、脆弱性の性質、特徴を示す脆弱性情報だけではなく、その検証方法、それを利用した攻撃方法も含む情報である。いずれも、これらの情報が保護されないまま放置されたり、意図的に暴露されたりすると、悪用される危険性がある。このため「情報セキュリティ早期警戒パートナーシップ」は、新たな脆弱性が発見された場合、社会的規模での被害拡大を予防するため、次の事項を狙っている。

① 幅広い関係者による早期対策立案
② 脆弱性関連情報の非公表での流通と保護
③ これを踏まえた脆弱性情報の早期公表
④ 関係者による対策の実施

(b) 脆弱性を製品開発者の瑕疵とは区別し、脆弱性の社会的解決を指向

脆弱性をコンピュータ・ウィルス、コンピュータ不正アクセス等の悪意の存在によって初めて顕在化する、機能、性能を損なう問題個所と定義し、ソフトウェア製品の脆弱性と瑕疵（品質不良、バグ等）を区別している。これにより、脆弱性を瑕疵の問題として製品開発者だけに対策を求めるのではなく、社会的な枠組として各パートナーが共同して解決するべきだという社会的合意を形成しようとしている。

2.1.2. 「情報セキュリティ早期警戒パートナーシップ」の対象

① ソフトウェア製品：ソフトウェア自体又はそれを組込んだハードウェアであって、フリーウェアも含む汎用性を有する製品。
・OS、ブラウザ、メーラ等のクライアント上のソフトウェア
・DBMS、ウェブサーバ等のサーバ上のソフトウェア
・プリンタ、IC カード、PDA、コピー機等のソフトウェアを組込んだハードウェア

② ウェブアプリケーション：インターネット上のウェブサイトで稼動する固有のシステム。
[SI 事業者との関係] ウェブサイト運営者は脆弱性が発見されたウェブアプリケーションの運営主体である。SI 事業者がウェブサイト運営者の場合もあるが、本書ではウェブアプリケーションの開発者または保守・運用者の場合を対象とする。

2.1.3. 「情報セキュリティ早期警戒パートナーシップ」の用語定義

「情報セキュリティ早期警戒パートナーシップガイドライン」（2004 年 7 月 8 日）による用語定義を示す。特に、一般的な「脆弱性」と、機密管理が必要とされる攻撃方法などを含む「脆弱性関連情報」とを区別していることが重要である。

No	用語	定義
1	脆弱性	脆弱性とは、ソフトウエア製品やウェブアプリケーション等において、コンピュータ不正アクセスやコンピュータウイルス等の攻撃により、その機能や性能を損なう原因となり得るセキュリティ上の問題箇所です。 なお、ウェブアプリケーションにおいて、ウェブサイト運営者の不適切な運用によって、個人情報等が適切なアクセス制御の下に管理されておらずセキュリティが維持できなくなっている状態も含みます。
2	脆弱性関連情報	脆弱性関連情報とは、脆弱性に関する情報であり、次のいずれかに該当するものです。 1) 脆弱性情報 脆弱性の性質及び特徴を示す情報のことです。 2) 検証方法 脆弱性が存在することを調べるための方法です。例えば、特定の入力パターンにより脆弱性の有無を検証するツール等が該当します。 3) 攻撃方法 脆弱性を悪用するプログラムやコマンド、データおよびそれらの使い方です。例えば、エクスプロイトコードや、コンピュータウイルス等が該当します。
3	対策方法	対策方法は、脆弱性から生ずる問題を回避するまたは解決を図る方法のことであり、回避方法と修正方法から成ります。ただし、本ガイドラインで、「対策方法」との記述がある場合、「回避方法または修正方法」の意味となります。 1) 回避方法 脆弱性が原因となって生じる被害を回避するための方法（修正方法は含まない）であり、ワークアラウンドと呼ばれます。 2) 修正方法 脆弱性そのものを修正する方法であり、パッチ等と呼ばれます。
4	対応状況	調整機関から脆弱性関連情報の通知を受けた製品開発者が報告する製品開発者の脆弱性に関する対策方法、取り組みの状況などを含む対応状況のことです。
5	ソフトウエア製品	ソフトウエア自体又はソフトウエアを組み込んだハードウエア等の汎用性を有する製品のことです。ただし、いわゆるオープンソースソフトウエアのように技術情報を統括する企業が一社に定まらないもの、複数の者又は団体によりその改善が行われるものも含みます。
6	ウェブアプリケーション	インターネットのウェブサイトなどで、公衆に向けて提供するサービスを構成するシステムで、そのソフトウエアがサイトごとに個別に設計･構築され、一般には配布されていないもののことを指します。
7	発見者	発見者とは、脆弱性関連情報を発見または取得した人を含みます。例えば、ソフトウエアの脆弱性を発見した人や、インターネット上で脆弱性関連情報を入手した人などが当てはまります。ソフトウエアの脆弱性を発見した人のみを対象としているわけではありません。
8	製品開発者	製品開発者とは、ソフトウエアを開発した企業または個人です。企業の場合それが外国の会社である場合には、そのソフトウエア製品の国内での主たる販売権を有する会社（外国企業の日本法人や総代理店など）を指します。
9	脆弱性検証	脆弱性検証とは、製品開発者がJPCERT/CC から脆弱性関連情報を受け取った際に、該当するソフトウエア製品の有無、およびその新規性の有無を検証することです。
10	ウェブサイト運営者	ウェブサイト運営者とは、脆弱性関連情報が発見されたウェブアプリケーションを運営する主体です。当該ウェブアプリケーションが企業や組織によって運営されているのであれば、その企業や組織が該当します。個人によって運営されているのであれば、その個人が該当します。

2.1.4. 各パートナーの役割と脆弱性関連情報取扱手順

(a) ソフトウェア製品に係わる脆弱性

① 脆弱性を発見した場合、「発見者」はその脆弱性関連情報を「受付機関（IPA）」に届出を行い、公表されるまでの間、第三者に漏れないように適切に管理する。

② 「調整機関（JPCERT/CC）」は一般非公表を前提として、「製品開発者」に脆弱性関連情報を開示し、対策を求める。「製品開発者」は必要な対策を立案し、「調整機関（JPCERT/CC）」と一般への公表日を調整する。

③ 対策完了後、「IPA」、「JPCERT/CC」は脆弱性とその対策をセットにして一般に公表する。

(b) ウェブサイトの脆弱性

① ウェブサイトの脆弱性の場合も、「発見者」はその脆弱性関連情報を「受付機関（IPA）」に届出を行う。また、「ウェブサイト運営者」がその脆弱性を修正するまでの間は、第三者に漏れないように適切に管理する。

② 「受付機関（IPA）」から脆弱性を通知された「ウェブサイト運営者」は、必要な対策を実施し、「受付機関（IPA）」へ完了を報告するが、この脆弱性に関しては「ウェブサイト運営者」は積極的公表の義務は無い。

③ この脆弱性が原因による個人情報漏洩、またはその可能性がある場合は二次被害防止のために事実関係を公表する。また、個人情報保護法及び関連省庁ガイドラインに従う。

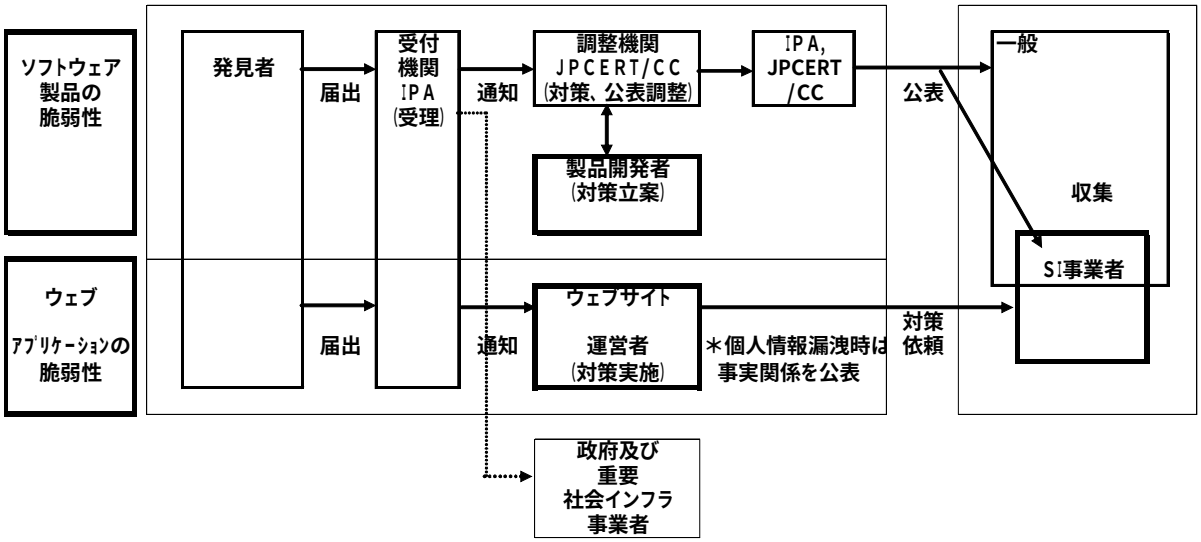


図 2-1 情報セキュリティ早期警戒パートナーシップの役割と脆弱性関連情報取扱手順

2.1.5. 公表前の脆弱性関連情報の保護

① 公表前に脆弱性関連情報を受け取ることができる事業者は、脆弱性関連情報を外部の第三者（担当部門以外の社内も含む）に漏らさないような管理ができる事業者であることが要求される。

② このため、製品開発者は脆弱性関連情報を機密管理するための業界自主ガイドライン（JEITA・JISA、JPSA）を制定し、社内体制を整備しつつある。

2.1.6. 政府及び重要社会インフラ事業者への開示

国民の日常生活に必要不可欠なサービスを提供するための基盤となる設備に重大な影響を与えるおそれがあると認められる場合、受付機関（IPA）は脆弱性関連情報を公表前に政府及び重要インフラ事業者（情報通信、金融、航空、鉄道、電力、ガス等）には開示し、先行的な対策実施を可能とすることが想定されている。（経産省告示235号　V 2受付機関基準（6）、パートナーシップガイドライン 3.（1）　10）優先的な情報提供）

2.2. 脆弱性関連情報取扱体制の SI 事業者の位置付け

「情報セキュリティ早期警戒パートナーシップ」枠組の中で、公表前に脆弱性関連情報の開示を受ける製品開発者、ウェブサイト運営者、政府及び重要インフラ事業者と異なり、SI 事業者は公表後にのみ脆弱性情報を知りうる一般関係者と同じ位置にある（図2－2）。

しかし、SI 事業者は、ウェブサイト運営者、政府及び重要インフラ事業者及び一般顧客で稼動するシステムを納入し、保守する立場にあるため、現在開発中のシステム及び顧客へ既に納入したシステムに対し、セキュリティ確保のための対策を実施するという重要な役割を担っている。

(a) **脆弱性情報の収集と評価：**（図 2-2 の番号①）

新規の脆弱性情報を収集、評価し、既知の脆弱性情報を含め、脆弱性情報を的確に把握する。

(b) **システムのセキュリティ確保**

① 新規開発システム： 顧客と合意した必要なレベルのセキュリティを、システム構築プロセスの中でシステムに作り込む。（図 2-2 の番号②）

② 納入済システム： 新規の脆弱性が公表された場合、必要な時期に適切なセキュリティ確保策を顧客に通知、提案を行い、顧客と連携して実施する。（図 2-2 の番号③）

(c) **顧客との連携：**（図 2-2 の番号③）

① 新規の脆弱性が公表された場合、顧客はシステムが扱っている情報資産価値に対する経営判断を行い、対策を決める。SI 事業者は顧客への脆弱性情報の説明責任を果し、顧客が正しい認識の下に対策内容と費用を決める支援を行う必要がある。

② 被害拡大防止のためにシステムの稼動停止を提案する局面も想定される。また、通常の場合でも、実環境上で対策の最終試験を行うため、システムの稼動停止が必要な場合がある。このため、システムの稼動停止に対する顧客との連携が必須である。

(d) **製品開発者との連携：**（図 2-2 の番号④）

公表された対策について問題がある場合、製品開発者に対し協力を求める。また、製品開発者は、SI 事業者に的確な支援を行うよう努める必要がある。

(e) **ウェブサイト運営者との連携：**（図 2-2 の番号⑤）

ウェブアプリケーションの場合、ソフトウェア製品と異なり、脆弱性関連情報はウェブサイト運営者に個別に通知され、ウェブサイト運営者から SI 事業者に知らされることになる。このため、脆弱性が修正されるまで、対策を実施する受託契約に基づき脆弱性関連情報を第三者に漏れないようにウェブサイト運営者と連携して管理する必要がある。

(f) **発見者としての役割：**（図 2-2 の番号⑥）

SI プロセスの中でソフトウェア等の脆弱性を発見した場合、「情報セキュリティ早期警戒パートナーシップ」での「発見者」としての役割を的確に果す。

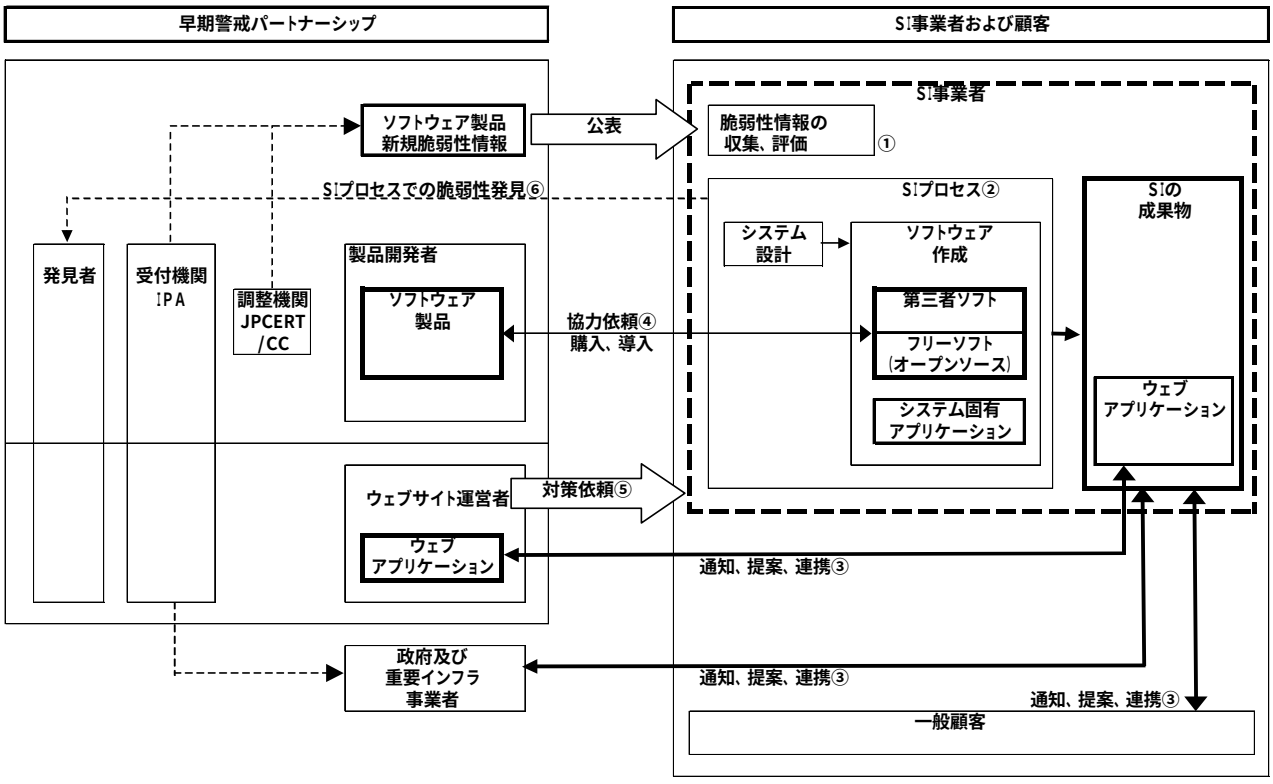


図 2-2 情報セキュリティ早期警戒パートナーシップでの SI 事業者の位置付け

3. ソフトウェア等脆弱性関連情報取扱体制への SI 事業者として共通的に必要な取組事項

3.1. 基本姿勢：顧客の側に立った脆弱性対策と SI 事業者の役割への自覚・実践

3.1.1. 顧客の側に立った脆弱性対策

「情報セキュリティ早期警戒パートナーシップ」では、脆弱性とソフトウェア製品開発者の瑕疵を区別している。これは SI 事業者にも当てはまり、SI 成果物としての納入システムに潜んだ新規の脆弱性については SI 事業者の瑕疵とは区別したい。しかし、SI 事業者は顧客とソフトウェア製品開発者の中間に位置するため、顧客との関係によっては脆弱性対策実施にあたってのコストを背負い込まざるを得ない場合がある。このため、この状況を改善しない限り、「情報セキュリティ早期警戒パートナーシップ」は最前線で機能しない場合があり、社会的規模の対策が進まないと想像される。

しかし、既知の脆弱性とその重大性に対する著しい認識不足、ウェブアプリケーションでの必要な設定漏れや設定ミス等で顧客システムで事件・事故が発生した場合は、SI 事業者の瑕疵（品質不良、バグ等）として真摯に対応する必要がある。

また、SI 事業者の顧客であるユーザ企業は、SI事業者は「ソフトウェアの脆弱性による損害についても、お客様に対しては責任を取らざるを得ない」という厳しい立場にあるため、SI 事業者に対し「脆弱性の発生は防ぎきれず、かつその脆弱性を狙う人達がいるので仕方がない」というようなスタンスを捨て、「提供するソフトウェアに脆弱性が発生しないための工夫等、提供されるソフトウェアの品質の向上」を求めている（社団法人日本情報システム・ユーザー協会）。

> 参考：ユーザー企業における情報セキュリティ対策に関する意見等について
>
> 平成16年10月14日社団法人日本情報システム・ユーザー協会（JUAS）
>
> ① 事業者は、理由の如何に問わず、システムの不具合によってお客様にご迷惑をおかけすることがないように、厳しい努力を求められている。ソフトウェアの脆弱性による損害についても、お客様に対しては責任を取らざるを得ないと受け止めている。
>
> ② ソフトウェアベンダーに対し、「脆弱性の発生は防ぎきれず、かつその脆弱性を狙う人達がいるので仕方がない」というようなスタンスを捨て、提供するソフトウェアに脆弱性が発生しないための工夫（脆弱性が存在しても、それを顕在化させない工夫を含む）等、提供されるソフトウェアの品質の向上を望む。

3.1.2. ＳＩ事業者の役割への自覚・実践

このため、SI 事業者はあくまで顧客の側に立ち、ソフトウェアに脆弱性が発生しないための工夫（セキュリティ技術）を強化していく役割と責任がある。また、顧客とソフトウェア製品開発者との脆弱性対策の費用負担についても、この前提があってこそ、顧客の理解が得られると考える。したがって、

SI 事業者として次の役割と責任を自覚し、実践することが必要である。

① セキュアなシステム構築ためのセキュリティ技術、プロジェクト管理力の強化：これで顧客への品質責任を果すことができ、対策立案等でソフトウェア製品開発者への影響力を強化できる。(3.2.1 項参照)

② 脆弱性に関するリスク管理・危機管理と事件・事故管理：ソフトウェア製品開発者は脆弱性関連情報を第三者には非公開で保護しながら、「調整機関 (JPCERT/CC)」と調整した時期までに対策を立案することに役割の主体がある。しかし、SI 事業者は、脆弱性情報の公表後に悪意ある攻撃者との時間的競争の中で、顧客と連携し顧客システムの正常稼動と被害拡大防止のための対策を行う必要がある。このため、SI 事業者は、顧客システム稼動維持と被害拡大防止のためのリスク管理・危機管理の一環として脆弱性対策を認識する必要がある。また、個人情報漏洩等の事件・事故が発生した場合の顧客との連絡調整手順・社内体制等も明確にしておく必要がある。(3.2.2 項参照)

③ 顧客、ソフトウェア製品開発者との適正な費用負担についての提案力の強化：SI 事業者が高いセキュリティ技術力に基づき、脆弱性と瑕疵 (品質不良、バグ) を的確に区別し、納得できる提案を各パートナーに提示することによって、適正な費用負担を実現できる。(3.3 項参照)

3.2. 脆弱性関連情報取扱体制作りのための組織的配慮事項

「情報セキュリティ早期警戒パートナーシップ」の定着に従い、SI 事業者の顧客である一般顧客、ウェブサイト運営者、政府及び重要インフラ事業者での脆弱性関連情報への認識が高まるため、SI 事業者として期待される役割を果すことが事業運営にとっても重要な事項となっていくと予想される。

ただし、SI 事業者はソフトウェア製品については原則として公表後の脆弱性情報を取り扱うため、SI 事業者の期待される役割は製品開発者とは異なると考える。製品開発者向けガイドライン (JEITA-JISA) では、第三者に非公表で脆弱性関連情報を取り扱うため、全社的体制作りとしてベンダーCSIRT (シーサート：Computer Security Incident Response Team) 等の情報収集と機密保持体制などに重点を置いているのに対し、SI 事業者は 3.1 項で記述した次の事項に注力した体制作りが基本と考える。

① セキュアなシステム構築のためのセキュリティ技術、プロジェクト管理力の強化

② 脆弱性に関するリスク管理・危機管理と事件・事故対策

本書では SI 事業者の多様性を考え、体制整備を行う上での配慮事項をまとめることにとどめ、そ

の実現方法はSI事業者それぞれでの検討とすることにした。

3.2.1. セキュアなシステム構築のためのセキュリティ技術、プロジェクト管理力の強化

本項については、既知の脆弱性に対するＳＥへの周知のレベルからIT製品のセキュリティ確保のための技術標準 ISO/IEC15408 までの幅広い領域であるため、本書では詳細には触れないが、脆弱性関連情報取扱いのための体制整備を行う上で関連する事項についてのみ記述する。なお、付録 3 に体制整備の例としてシステム開発セキュリティセンターのモデル事例を添付したので参考にしていただきたい。

(1) 開発標準とセキュリティ実装のレビュー体制の整備

① SI事業者がCMM、QMSなどで運用している開発標準に、セキュリティの作り込みを明確にする。

② 上記開発標準が実際のシステム構築で実現されているかをレビューする機能を整備する。この機能の実現方法としては、既存のプロジェクトレビュー体制に追加することで対応できる場合もあるし、必要によってはセキュリティ専門のレビュー部門を整備する方法も考えられる。

(2) 納入システムの構成管理

① 納入後のシステムに対する新規脆弱性問題の対策のためには、該当の脆弱性を持つソフトウェアが納入システムに使われているかを把握する必要がある。このためには、納入システムのソフトウェア構成管理を継続的に行う必要がある。

② しかし、SI 事業者は顧客ごとのＳＥ部門で組織化されている場合が多いため、全社範囲で納入システムのソフトウェア製品構成を一元的に把握しにくいことも考えられる。このため、構成管理を効率よく行うための社内連携体制の構築やツールの導入が課題となる。

③ また、保守契約がなされていないシステムに対してまで、保守契約がなされているシステムと同等のソフトウェア構成管理を長年維持することは困難であるため、この機能の整備は保守契約がなされたシステムに対し優先的に実施するべきである。

(3) 脆弱性関連情報の収集と評価及び情報共有

① ソフトウェア製品開発者では全社的な CSIRT の設置が提案され、第三者に非公開の脆弱性関連情報を含めて収集、評価し、データベース化を行うことが想定されている。しかし、SI事業者の場合は原則として公表後の対応となるため、脆弱性情報のデータベースは社内で整備しなくても、公表されたデータベース（JVN など）を如何にうまく活用するかがポイントである。SI 事業者としては、分かりやすく対策の副作用情報なども含む有用な公的データ

ベースの整備を提案したい。

② また、SI 事業者は顧客と協力し、脆弱性対策を進めなければならないため、顧客のシステム部門との情報共有が最重要であり、この関係により、脆弱性対策の必要性、費用分担などに対する顧客側の理解の土台とすることができる。

③ SI 事業者の場合、納入システムを熟知しているＳＥ部門が脆弱性情報を最終的に評価する必要がある。このため、ＳＥ自身が関係する脆弱性情報に敏感でなければならない。しかし、ＳＥ部門が脆弱性情報のデータベースを毎日見に行き、発生する脆弱性情報を把握することには困難が伴う。このため、次の工夫が必要である。

- ＳＥ部門での把握漏れを防止するための全社的なスタッフ組織の設置
- 既存スタッフ組織の利用（例えば社内情報システム部門との情報共有など）
- 脆弱性情報配信サービスの利用

3.2.2. 脆弱性に関するリスク管理・危機管理と事件・事故対策

(1) リスク管理・危機管理の整備

脆弱性問題による顧客システムでの事件・事故が発生した場合、顧客の経営層と連携し対応するためには、SI 事業者も経営層が問題解決を主導できるリスク管理・危機管理体制を整備しておく必要がある。

(2) 政府及び重要インフラ事業者を顧客とする SI 事業者への影響

① 政府及び重要インフラ事業者である顧客は SI 事業者よりも先行して非公表時に脆弱性関連情報の開示を受ける場合があると想像される。この場合、SI 事業者は顧客から公表前に対策を依頼されるケースも考えられる。この場合は顧客から機密保持に関する特別な指示があると考えられ、この指示に迅速に対応できるためには、ISMS 等の情報セキュリティマネジメントシステムを日頃から構築し、セキュリティ管理レベルを上げておく必要がある。

② ソフトウェア製品開発者は SI 事業者の購入規模に応じ、脆弱性問題を含む保守サービスの優先サービスを行っている場合がある。しかし、社会的規模での被害が発生すると予想される場合は、この枠組だけでは SI 事業者は有効な対策を実施することができない恐れがある。このため、政府及び重要インフラ事業者の要請により、ソフトウェア製品開発者は SI 事業者の購入規模にかかわらず、システムの社会的重要性による優先サービスを行う等の新しい枠組も必要である。

(3) ソフトウェア製品開発者との連携

① 業界としてソフトウェア製品開発者とSI事業者間で、パッチ適用に伴う副作用の情報を含めた情報共有の体制を整備するべきである。

② 個別企業においては、ソフトウェア製品開発者に脆弱性情報に関する SI 事業者向けの窓口を準備してもらい、SI事業者側としてもその窓口に社内各部門から個別にコンタクトをとるのではなく、一括してコンタクトを取る窓口を設置する等の工夫も必要である。

(4) 発見者としての役割

① SI事業者はシステム構築プロセスの中でソフトウェア製品を実装しているため、脆弱性を発見しやすい立場にある。このため、「情報セキュリティ早期警戒パートナーシップ」の枠組に従い、発見者として IPA への届出を行う。

② SI 事業者としても、脆弱性関連情報の漏洩のリスクがあるため、脆弱性関連情報を社内の限定された関係者にのみ開示する必要がある。製品開発者向けガイドライン（JEITA-JISA）では、「その対応が決まっていない段階で社内を含む第三者へ情報を流通させてはならない。社内の者であっても、限定した最小限の関係者にのみ情報を提供しなければならない（4.1.4 情報共有の枠組み）」としている。また、システム構築プロセスでの脆弱性の発見者は個人ではなく法人としての SI 事業者であるが、これを理由に社外に開示しなければ、社内では公表して良いと考えてはならない。できる限り、情報漏洩のリスクを減らす責務がある。

③ ソフトウェア製品開発者と排他的利用権を取得し、システムに実装する場合などの影響が自社内にとどまり、社会的に影響が無い場合は、IPA に届出を行わず、ソフトウェア製品開発者にのみ通知してもよいが、ソフトウェア製品開発者との間で「情報セキュリティ早期警戒パートナーシップ」に準じた脆弱性関連情報保護の枠組を整備する必要がある。

3.3. 脆弱性対策への費用負担の調整と SI 契約、保守契約のあり方

3.3.1. SI 事業者としての基本的考え方

情報サービス産業協会（JISA）は情報セキュリティに関する費用負担について、「脆弱性は原則的に瑕疵担保責任の対象外とすべきである」との基本的な考え方を示している。これは、「情報セキュリティ早期警戒パートナーシップ」での脆弱性と瑕疵を区別する考え方を前提として、SI 事業者としてさらに踏み込み、脆弱性を瑕疵担保責任から外し、対策費用は顧客負担とする方向を示したものである。

この基本的考え方は平成 14 年 2 月 13 日開催の JISA 理事会で承認され、JISA ポジションペーパ

として JISA ホームページで公表されている。また、これを具体化したものとしてモデル契約書が作成され、ポジションペーパも含め、平成 14 年 5 月に JISA から「新しいソフトウェア開発委託取引のあり方とモデル契約書の解説」（以下モデル契約書という）が発行されている。

SI 事業者は互いに競争関係にあるが、脆弱性対策の費用負担問題に関しては、足並みを揃えて、このモデル契約書に従い受注活動及び顧客との契約交渉を実施する必要がある。

3.3.2. モデル契約書を推進する前提として SI 事業者に要求される責務

モデル契約書では、脆弱性に対する保守契約、脆弱性に係わる瑕疵担保責任の免責、脆弱性に関する SI 事業者の責に帰する瑕疵の基準などを示しているが、これらを顧客に主張するためには、SI 事業者も自ら 3.1 項で示した基本姿勢を明確に示し、また、姿勢だけではなく実践し、事実として顧客に十分納得していただく必要がある。

3.3.3. モデル契約書の内容と考え方

(1) 脆弱性対策のための保守契約（モデル契約書第 32 条）

① インターネットなどに関係したウェブアプリケーションの場合、システムの納入後にも新たな脆弱性が日々発生するため、保守・運用を通じて継続的にセキュリティ対策が施されることが不可欠である。

② この対策の実施については、顧客が社会的責任を考慮し最終的に決定すべきものである。このため、顧客と SI 事業者が連携し、セキュリティ対策の保守契約として別途締結して対応するべきである。モデル契約書では、顧客と SI 事業者が発生した脆弱性に対し、影響と対策費用を協議し対策を決め、顧客の費用負担で対策を実施するものとしている。

③ SI 事業者は、新規システム受注においては最初からモデル契約書に従った契約をできる限り実現することを努力し、納入済システムでは既存の契約にセキュリティに関する覚書を追加することでモデル契約に近づけることが必要である。

> （セキュリティ）
> 第 32 条　乙が納入した本件プログラムにセキュリティ対策を実施する必要がある場合、甲及び乙は、その対策につき、**協議の上その対策を決める**ものとする。**この場合の費用は、甲の負担**とする。
>
> 補注：甲は委託者である顧客、乙は受託者である SI 事業者

(2) 脆弱性対策と瑕疵担保責任の区別の明確化（モデル契約書第 31 条）

① 有償契約により顧客にシステムを納入した SI 事業者は、契約で特に免責の定めがない限り、納入物の瑕疵等については瑕疵担責任を負う（民法 634 条）。また、請負契約での瑕疵担保責任は、SI 事業者に過失がなくても責任が問われる無過失責任主義であることが、法

律上の通説となっている。

② しかし、システムの納入後に新規の脆弱性が発生した場合の対策実施については、「情報セキュリティ早期警戒パートナーシップ」の枠組で社会的な解決を図る必要があるとされている。また、このケースで、脆弱性の影響が重大で、緊急に対策を実施する必要がある時に、SI 事業者の瑕疵担保責任の対象とすることは SI 事業者側に大きな負担を強いるため、請負契約での顧客、SI 事業者間での利益不均衡が著しくなる可能性がある。

③ このため、新規の脆弱性と瑕疵とは区別し、その脆弱性対策は瑕疵担保責任の対象外とするべきである。ただし、SI 事業者による既知の脆弱性に対する著しい認識不足、ウェブアプリケーションでの必要な設定漏れ、設定ミス等の場合はSI事業者の責とされても止むを得ない場合がある。

④ このため、モデル契約書では SI 事業者の責に帰するものではないと認められた場合には、顧客は協議・調査によって生じた費用をSI事業者に支払うものとしている。また、このための対策については顧客の費用負担で、別途保守契約を締結するものとしている（前項参照 モデル契約書第 32 条）。

（保証及び責任の範囲）
第31条 2. 第23条（補注：本件プログラムの検収）に基づく本件プログラムの検収後、瑕疵が発見された場合、甲及び乙はその原因について協議・調査するものとする。協議・調査の結果、当該瑕疵が**乙の責**に帰すべきものであると認められた場合、乙は無償で補修・追完を行うものし、**乙の責に帰すべきものではない**と認められた場合には、**甲は協議・調査によって乙に生じた費用を乙に支払う**ものとする。

(3) 脆弱性に関する SI 事業者の責に帰する瑕疵の基準（有償対応、無償対応の基準）

① 脆弱性に関する対策費用について、顧客に対し SI 事業者が無償で対応するか、有償で対応するかは、SI 事業者の経営問題だけではなく、情報セキュリティ早期警戒パートナーシップが有効に機能し、社会的な規模で脆弱性対策が実現できるかを決める重要問題である。

② 前項で SI 事業者の責に帰する脆弱性に関する瑕疵の例として、「SI 事業者による既知の脆弱性に対する著しい認識不足」、「ウェブアプリケーションでの必要な設定漏れ」を例示したが、SI 事業者の責に帰する「著しい認識不足」、「必要な設定漏れ、設定ミス」における「著しさ」、「必要さ」の程度までは、モデル契約書では基準を定めていない。このため、今後さらに具体的検討を積み重ねる必要がある。しかし、各パートナーが現実には利害を調整する必要があるため、その拠り所として契約時点を基準とした次の考え方を提案する。

③ 有償､無償の基準

時期	考え方
契約時 及び 開発中	・ 脆弱性対策は、できる限り顧客と合意して見積りに織り込む。 ・ 影響が小さいため対策不要と SI 事業者が判断した脆弱性に対し、顧客が必要と判断した場合は見積りに織り込む。 ・ 既知の脆弱性であっても対策が不明な脆弱性は無償対象とはしない
納入時 及び 保守 フェーズ	・ ソフトウェア製品の既知の重要な脆弱性の対策に関する著しい認識不足、ウェブアプリケーションに対する必要な設定漏れ、設定ミスなど SI 事業者の責に帰する場合は無償とする。(納入時点または保守開始時点のセキュリティレベルの確認と顧客との意識合わせが必要) ・ 納入後発生した新規の脆弱性については、必要に応じ対策費用を見積り、有償とする。 ・ 保守フェーズの新規脆弱性への対策は別途保守契約で対応する。 ・ アウトソーシングの場合も保守での考え方に準ずる。

(4) 第三者ソフト、フリーソフト利用による被害への損害賠償の免責(モデル契約書 19 条、20 条)

① 第三者ソフトは利用する顧客名義でのライセンス契約、フリーソフトは顧客での利用決定をモデル契約書は推奨している。このため、これを前提とすると、第三者ソフト、フリーソフトの不具合、脆弱性について、SI 事業者は責任を負う必要はない。

② 第三者ソフト、フリーソフトのいずれでも、SI 事業者は顧客に対し可能な範囲で、脆弱性関連情報の提供､その回避策と対策などのための開発を行うが､問題解決のために要する情報の取得と必要な開発等にかかる費用は受益者負担の原則に従い､モデル契約書では顧客において負担するものとしている。

(第三者ソフトの利用、フリーソフトの利用)
第 19 条 2. 第31条にかかわらず、**第三者ソフトに起因する不具合**又は権利侵害については、当該第三者ソフトの利用に関する契約に基づき処理するものとし、**乙は責任を負わない**ものとする。
第20条 2. 甲乙間で特段の定めのない限り、ソフトウェア作成業務への**フリーソフトの利用に起因して不具合**又は権利侵害の問題が発生した場合には、甲乙協議の上、解決するものとし、**これに要する費用は甲の負担**とする。

3.3.4. 脆弱性関連情報取扱における費用負担問題の発生局面と注意事項

SI 事業者はモデル契約書の内容の実現に業界を上げて努力する必要があるが､一朝一夕に実現できない。このため、実際のビジネスでは次に示すような努力と注意を払いつつ顧客、関係者との合意を取り付ける必要がある。

(1) 脆弱性内容と対策案の正確な説明

費用負担を論じる前に顧客に脆弱性内容と対策案について正確に説明する説明責任は SI 事業

者にある。特に顧客の情報システム部門には納得できるように説明し、対策方法などに対する協力を取り付ける努力を行う。

(2) 想定される被害の説明と対策案の費用比較の提示

発見された脆弱性によって引き起こされる事件・事故による被害の大きさを顧客の経営層に説明し、対策方法のセキュリティレベル別の対策案と費用比較の提示を行い、投資規模について的確な経営判断ができるよう支援する。

(3) 緊急事態時での顧客との費用負担の調整

被害拡大防止のため、緊急な対策を要求されるため、顧客との間で作業範囲、費用負担についての十分な協議のないまま、作業を進める状況が多々あると予想される。このような危機管理・リスク管理時の解決としては、事前にモデル契約書の内容で、契約しておくことがベストであるが、そうでない場合においても、モデル契約に基づく交渉を概略でも行い、覚書として残すことが必要である。

(4) 再委託先との連携と責任分担

個人情報保護法では個人情報の取扱いの全部又は一部を委託する場合に委託先に対する必要かつ適切な監督が義務付けられている（第 22 条）。個人情報を扱うウェブアプリケーションの脆弱性により個人情報漏洩事件・事故が起きれば、まず顧客が責任を問われ、損害賠償などを負担することとなるが、委託を受けているSI事業者も顧客からの信頼と社会的信用を失い、場合によっては顧客から損害賠償を要求される可能性もある。ところが、情報サービス産業業界の全体構造の特徴として、再委託先さらには再々委託先等との協働作業によるシステム構築、運用が多いという委託業務の連鎖が挙げられる。このため、特に元請SI事業者は複数の再委託先や再々委託先に対し、必要かつ適切な監督を行う重要な責務がある。

先に顧客との契約に際し、できるだけJISAのモデル契約書の考え方を反映させる必要があると述べたが、同様に SI 事業者間での元請、再委託先の関係にもこの考え方を当てはめることができる。再委託先もしくは元請との契約においては、脆弱性対応に関する責任分担についてできる限り明示し、合意しておく必要がある。

4. 脆弱性情報取扱手順の整備（ソフトウェア製品等の脆弱性対応）

ここでは、ソフトウェア製品等の脆弱性対応を示す。ソフトウェア製品等の脆弱性対応の特徴は次の通りである。

① 製品開発者には情報セキュリティ早期警戒パートナーシップを通して発見された自社製品に関する脆弱性関連情報の通知がある。しかし、SI 事業者は待っていても誰からも通知されず、日々公表される脆弱性情報から自分が係わっている顧客システムに関係のある脆弱性情報を的確に掴み取る必要がある。

② このため、脆弱性情報の収集（4.1 項）とさらに自社関連システムへ影響を与える脆弱性情報であるかの判別（4.2 項）が必要である。

③ これを踏まえ、対策の検討（4.3 項）、顧客への通知と調整（4.4 項）、対策の実施（4. 5 項）のステップを踏む必要がある。

4.1. 脆弱性情報の収集

SI 事業者としてソフトウェアの脆弱性情報を積極的に収集する必要があると考えられる。ただしソフトウェアは多岐に渡るため、組織的な体制を構築することが望ましい。収集した情報はプロジェクト責任者等に速やかに伝わるような体制を構築する必要がある。

(1) 情報収集の方法

SI 事業者として日々発生する可能性のある脆弱性情報を収集する必要がある。脆弱性情報収集先例を下記に記す。

① JVN（JP Vendor Status Notes） http://jvn.jp/

② 製品ベンダーの公表情報

③ JPCERT/CC http://www.jpcert.or.jp/

④ 独立行政法人 情報処理推進機構 http://www.ipa.go.jp/security/

⑤ 各セキュリティベンダーの公表情報

⑥ 有償で配信している脆弱性情報

(2) 社内体制の整備と共有化

開発･運用･保守業務を実施している組織に対して脆弱性情報の共有化をすることが望ましい。元請企業、顧客からの問い合わせ等の共有化も行い、社内全体で共通認識が取れるように体制を構築するべきである。

(3) 製品ベンダーとの体制整備

SI 事業者として取り扱っている製品の製品ベンダーとは、脆弱性情報に関する連絡体制を整

備することが望ましい。対応に伴う不具合の情報共有等を含め、問い合わせ窓口の設置など、最新の情報収集が行えるような体制を構築しておく必要がある。

4.2. 脆弱性情報の評価

自社関連システムに影響を与える脆弱性情報が公表された際に、その脆弱性に対応すべきかどうかを判断するための手順について説明する。脆弱性情報は顧客の環境に合わせて評価するため、影響範囲を評価することは難しいが、4.1 で記述したように、脆弱性情報を共有化することで、基本的な評価基準を設定することが望ましい。

(1) ベンダー、元請企業からの詳細情報収集

公表された脆弱性情報に関して、製品ベンダー等から以下のような情報を収集する。

① 製品のバージョン

② パッチ導入後の不具合等の情報

③ 検証方法の情報（再現ツール等）

(2) 契約の確認と自社関連システムへの影響範囲の調査

① 自社が係わる運用・保守を実施している顧客システムがどれくらい存在しているのか把握する。

② 該当するソフトウェアを利用したシステムを運用・保守している場合、契約に基づき対応すべきか否かを判断する。

③ 上記のためには、運用・保守のガイドライン（自社標準）等の中に、脆弱性情報の収集方法や、構成管理の方法、顧客への通知方法等を整理しておき、早期に対応ができる組織単位、プロジェクト単位の体制を構築しておく必要がある。

(3) 脆弱性情報の分析

製品ベンダーから公表される影響度合いや対策方法等での分類を以下のような形で整理することが望ましい。

① パッチを適用し修正

② ソフトウェアの設定値の変更により回避

③ 他のソフトウェアの設定により回避

④ 新たなソフトウェア、機器への入れ替え、追加導入により回避

(4) 作業費用見積りのための基本情報の整理

また上記のような分類に加え、作業費用を見積もるために以下のような基本情報を整理しておく必要がある。

・ 作業内容

・ 作業時間（システム停止、対策、確認、復旧までの時間見合い）

・ 正常稼動の確認方法

・ 検証方法（対策が正しく実施されたかどうかの確認方法）

(5) 評価項目の整理

対策後にアプリケーションが問題なく稼動していることを確認するために、最低限必要な確認作業の項目（ログイン、登録、更新、削除等）を整理しておく必要がある。

また、運用保守・業務においては、アプリケーション毎のテスト項目を整理し、顧客と認識をあわせておくべきである。

4.3. 対策の検討

顧客システムに影響を及ぼす可能性のある脆弱性情報を把握した時は、その脆弱性に対する概略の影響評価を行い、その時点で顧客システムに何らかの対策が必要と判断した時は顧客に初期通知を行う。

時間的に許されれば、対策方針と概略計画を立案してから、4.4 項の「顧客への通知と調整」で示す顧客との調整、合意作業に入る。この合意により顧客からの実施の委託を請けた場合、さらに対策の具体化を行い、再見積りを実施する。手順は次のとおりであるが、脆弱性の重要度および緊急度に応じ柔軟に対応する必要がある。

① 調査環境の決定と合意

自社に再現環境がある場合は自社である程度の調査および対策を進めることができるが、SI 事業者の多くは顧客の環境に特化してシステム構築を行っているため、顧客環境(実環境)上で調査を行う必要がある。

実環境での実施が困難である場合は、擬似環境（シミュレータ）による調査もしくは、他社事例などをベースにしたモデル検討（机上検討）とする。この場合に限らず、一般に多くの要素で構成されるシステムでは、単一のパッチの影響を事前に予測することが困難であり、対策の実施段階でも想定外の作業が多く発生することから、再見積りは適宜実施できることが好ましい。

② パッチ適用の影響調査と、限界の確認

当該脆弱性情報に基づき、発生する現象の再現と、それに伴うシステムの影響度を調査する。現象を再現するための基礎データやツールを構築する必要があるが、製品ベンダーや公的機関から適宜、無償提供を受ける場合を除くと、有償実施の対象となる。その現象を確認し、

対応するべきシステムの範囲、構成要素を特定するが、現象がどうしても再現されない場合は、関係機関との調整やセキュリティ専門家等のアドバイスを受けてパッチ適用を保留することも検討する。

次にパッチ適用後の影響を調査する。特に、適用前にリソース、性能条件の調査が必要である。

③ パッチ適用以外の選択肢の調査提案

修正拠点が散在する、改変が大規模に及ぶ、パッチの検証が不十分でシステム停止などのリスクが大きい、稼動を停止できないなど修正作業自体が困難である場合は、パッチ適用以外の選択肢を調査提案する。

- 保険の適用
- 情報自体のセキュリティ強化(暗号化など)
- 攻撃に対する監視の強化
- 代替システムの導入と業務フローの改変

④ 対策の実施計画見積りおよび費用見積り

パッチ適用など対策実施の計画を策定し、顧客に提示する。

- 作業内容、責任範囲
- 目的、全体日程、実施体制、責任窓口、契約関係
- 作業条件（環境準備やバックアップ作業など顧客側で準備すべきことを含む）
- 完了条件(検収要件)
- 費用見積り、再見積り条件
- 免責事項

4.4. 顧客への通知と調整

顧客への通知手順と留意すべき点を述べる。

脆弱性情報の評価を受けて、自社が関わった関連システムに影響を与える可能性の高い顧客と、今後の施策を進めるために必要な合意を形成する。このため自社が関わった関連システムについて保守契約しておき、技術分野および顧客別に構成管理しておくことが望ましい。

4.4.1. 契約の確認

顧客との調整にあたって、契約内容を確認する。

① 瑕疵期間内の場合の対応方法

② 脆弱性への対応についての記載の有無と記載内容(対応の範囲など)

③ 脆弱性への対応を行う場合の有償、無償の条件

④ 有償の場合の費用や対応範囲の上限

⑤ 無償の場合の対応範囲

⑥ その他、免責事項など

4.4.2. **顧客への初期通知**

顧客の関連システムに対象となる脆弱性が含まれる可能性があるかどうかは、設計情報などの開示が必要となる場合があり、顧客の関連システム全体にかかわっている場合を除き、判断できないケースが発生すると考えられる。したがって、顧客への脆弱性情報の通知は、原則として保守契約を結んでいる場合に行う。ただし、現在は保守契約が存在しないが自社が構築したシステムで、当該脆弱性の影響が極めて大きいと考えられる場合、重要な顧客である場合、など個別の事情に応じ、脆弱性情報を顧客に通知することは有益である。

いずれの場合も、具体的な実施策を決定するためには、顧客の実環境上で影響度などを調査しなければならず、顧客との協力関係が非常に重要となる。

初期通知内容としては次のようなものがある。

①当該脆弱性情報および、情報収集源の紹介（JVN、製品ベンダー、JPCERT/CC、IPA等 ）

②自社の対応方針と顧客へのお願い（実施条件　顧客の協力依頼　無償範囲の通知）

③対策（具体的実施策）の策定の提案（見積り提示時期の見込み、提示方法）

④完了基準の提示、合意

4.4.3. **有償、無償対応の基準と判定**

① 対策検討および対策実施自体は、潜在する瑕疵ではなく、高度化する情報システムの新しい利用法の発見、機能要求の高度化に伴う新たな脅威の出現、という使用環境に対する機能変更と同等と考えられ、有償の追加構築と判断する。

② 無償対応の範囲としては、当該脆弱性情報の追跡と、明示的に影響がある脆弱性情報の顧客への通知、および顧客からその情報に関して対策の見積りを依頼された際の通常の見積り活動である。ただし、顧客側から適切な環境、設計資料などの提供を受けた後、調査を要するような詳細見積りを別途実施する場合については有償対応の交渉を行う。

③ 保守契約において機能追加変更などを請け負っている場合は、その範囲での対応とそれを超える対応とを区別し顧客に十分説明しておく。

4.4.4. **顧客への見積り提示**

「4.3 対策の検討」で作成した見積りを顧客へ提示する。見積りとしては、全体の概算と、詳細見積りのための調査費用とを提示する。

4.4.5. **顧客との対応方針の合意形成**

① 顧客と対応方針、概要計画について合意する。初期の段階では対応方針（大日程　実施方針　窓口）のみの合意でもよい。概要計画には、実施策、日程計画、実施体制、責任範囲、無償対応範囲および完了条件を記載し、顧客と合意する。

② 既存の保守契約がある場合は、その範囲で実施できるかどうかを判断し、必要ならば業務実施のための再契約もしくは追加契約を締結する。

③ どのような確認方法で脆弱性が消滅したことを確認するかについても、完了条件（検収条件）としてあらかじめ顧客と合意しておく。

4.5. **対策の実施**

対策方針についての顧客との合意、もしくは、顧客からの対策策定の委託を請けて具体的対策を提案し実施する。

4.5.1. **試験環境における試験**

(a) 試験環境での確認項目

パッチを実環境に導入する前に、擬似環境もしくは専用試験環境において、パッチの妥当性を以下のような項目において確認する。これらの情報は、当該ソフトウェア製品ベンダーから提供されている場合もあるが、製品ベンダーによる確認が不十分のケースもあるので試験環境における確認は重要である。

① 当該脆弱性情報の現象の再現

② パッチインストールの完全性、インストール手順の確認

③ 当該脆弱性情報の現象是正の確認

④ パッチを含むモジュール、周辺モジュールの動作検証、2次障害の有無の確認

(b) **試験環境について**

① 自社もしくは顧客内に構築された試験環境

システム構築で検証のため構築された試験環境を自社もしくは顧客内に再現して実施するケースがほとんどであると考えられるが、OS 更新などで再現できない場合は擬似的に用意する。専用開発ツールなどを用いる場合もある。

② 公的機関もしくは関係者共同で構築された試験環境

相互接続性確認などは、自社あるいは顧客の環境だけでは確認できないケースが多いと考えられる。また、試験環境の再現にはコスト、期間を要する場合があり、それが脆弱性対策を遅らせる原因にもなりうることから、共有利用可能な試験環境を公的機関もしくは関係者共同体に構築することは今後検討すべき項目である。

4.5.2. 顧客環境における対策の実施

試験環境での確認完了後、顧客環境における対策を実施する。事前に顧客側でバックアップ等を実施していただき、対策前状態に戻せるかを確認して対策を実施する。バックアップ自体を顧客から請け負うこともある。対策前状態に戻す方法が無いか困難である場合は、顧客との契約等文書による合意の上、代替システムを用意の上実施など、他の方策を検討したうえで対策を選定し実施する。

4.5.3. 対策効果の確認

次に、対策実施によって当該脆弱性を消滅できたか否かを確認する。脆弱性の有無を確認するためのツール等が製品ベンダーから提供されている場合は、そのツールを用いて脆弱性が無くなったことを確認する。ツールが提供されていない場合は、パッチ等が確実に適用されているかどうかをソフトウェア製品のバージョン情報やインストール情報などをチェックすることにより確認する。攻撃手法が明らかになっている場合には実際に攻撃して脆弱性が無くなったことを確認することも可能であるが、必ず顧客との合意の上で細心の注意払った上で行う必要がある。

4.5.4. 対策実施上の問題点等の情報共有

パッチは限定された条件下で動作が検証されたものであって、多くの要素が組み合わされたシステム上に与える影響すべてが検証されているわけではない。したがって、パッチを含む対策実施にともなう問題点、関連情報は、顧客との間だけではなく、脆弱性関連情報の速やかかつ確実な対策を実施するうえで、できる限り多くの関係者で情報を共有できることが好ましい。当面は顧客固有の秘密情報が露呈されない工夫を施した上で、あるいは顧客の了解の下で、当該情報を製品ベンダーへフィードバックするか、関係会社との情報共有をはかるといったことを実施する。

今後、こういった対策実施上の問題点等の情報を共有するための公的なスキームの整備も重要である。

5. 脆弱性関連情報取扱手順の整備(ウェブシステムの脆弱性対応)

ここでは、ウェブシステムの脆弱性対応を示す。ウェブシステムの脆弱性対応の特徴は次の通りである。

① SI 事業者は、情報セキュリティ早期警戒パートナーシップや脆弱性の発見者により通知を受けたウェブサイト運営者から連絡を受けて対応を迫られる場合が通常であり、対象システムが最初から特定されている。

② 対象システムの URL、脆弱性の検証方法や攻撃手法など、脆弱性関連情報に該当する機密情報を取り扱う必要がある。

③ 同様の脆弱性を持つ可能性があるウェブシステムへの対策の横展開が必要である。

5.1. 脆弱性関連情報の通知

ウェブサイト運営者である顧客が当該ウェブシステムの脆弱性について誰から通知されたのかによって、SI 事業者の対応が若干異なるため、以下にそれぞれの場合について説明する。

5.1.1. 顧客が IPA を経由して脆弱性関連の通知を受けた場合

ウェブアプリケーションの脆弱性関連情報は IPA からウェブサイト運営者に通知される。SI 事業者は、ウェブサイト運営者である顧客から本通知に関する情報を受けることになる。

IPA から顧客への脆弱性関連情報の通知は、メールを利用して以下のとおり 2 段階で行われる。第 1 段階では、脆弱性の可能性があるウェブサイト URL に記載された連絡先へ、当該 URL の通知と、詳細情報の連絡先(対応の窓口)の返信を依頼される。第 2 段階では、顧客の対応窓口へ、脆弱性の種類や発生しうるリスクなどの詳細情報を通知される。この通知には、IPA の取扱番号(IPA ＃番号)が付されるので、IPA との連絡の際にはこの番号を用いる。いずれの場合も、顧客は、通知を受け取った旨の返信や脆弱性存在の有無の確認報告は、速やかに行うように努める。(返信や報告の期限の目安は、IPA のサイトを参照のこと。)

脆弱性の対応が完了した場合、顧客は修正完了報告(取扱番号、対象のウェブサイト URL、対応の内容)を IPA へ行うように努めることを求められる。IPA による修正確認を希望する場合には、同意書を提出し、確認日時を調整の上、問題点が修正されているか確認をしてもらうことができる。

詳細情報通知後の IPA とウェブサイト運営者の脆弱性関連情報取扱いプロセスの概略図を図 5-1 に示す。

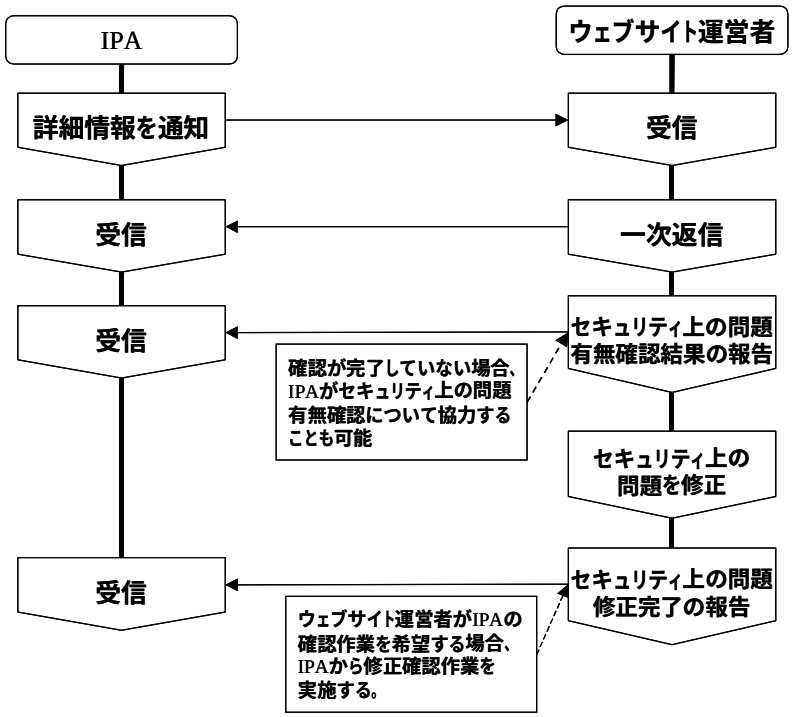


図5-1 IPAの脆弱性関連情報の取扱いプロセス

以上のような流れの中で、SI 事業者は以下のように振舞うことになる。

(1) 脆弱性関連情報の確認

顧客より通知された脆弱性関連情報の内容を確認する。IPA に脆弱性関連情報を通知した発見者の名前はウェブサイト運営者には通知されないが、調査などでウェブサイト運営者が希望し、発見者もこれに同意した場合には、交換されるすべての写しを IPA に提供することを条件に、直接の情報交換を選ぶことができる。したがって、必要に応じて脆弱性関連情報の詳細に関して、発見者と直接の情報交換を顧客に提言する。

(2) 調査対象ウェブシステムの特定と影響評価

顧客のウェブシステムを担当した開発部門に対して、脆弱性関連情報に関連する調査対象の特定と影響評価を指示する。

(3) 顧客への対応方針の報告

開発部門での当該ウェブシステム特定作業が完了する目処を勘案して、当面の対応方針を決め、顧客に報告する。

(4) 顧客への受領通知の発行と詳細情報の管理

顧客より情報提供を受けた場合、受け取りしだい受領通知を返すと共に、預かった情報は機密情報として適切に管理する。

5.1.2. 発見者から直接、脆弱性関連情報の通知を受けた場合

発見者が IPA を介さずに直接にウェブサイト運営者に脆弱性関連情報を通知してきた場合に、ウェブサイト運営者である顧客からSI事業者に相談された時には、発見者との誠実な対話に努めるように勧める。万一に発見者との対話に感情的な行き違いなどから円滑に進まなくなることが予想される場合には、中立的な仲介役として IPA の介在を求めることもできることを顧客に伝える。

(1) 脆弱性関連情報の確認

顧客より通知された脆弱性関連情報の内容を確認する。通知の中に明示されなかった場合、次の事項を関連情報として、顧客に発見者への確認を依頼する。

①脆弱性関連情報を既に IPA や他者に通知したかどうか。

②脆弱性関連情報を公表する意思とその時期。

③顧客が対策を含めた脆弱性対応状況を公表する際の謝辞における発見者名の記載方法についての希望。

(2) 調査対象ウェブシステムの特定と影響評価

顧客のウェブシステムを担当した開発部門に対して、脆弱性関連情報に関連する調査対象の特定と影響評価を指示する。

(3) 顧客への対応方針の報告

開発部門での当該ウェブシステム特定作業が完了する目処を勘案して、当面の対応方針を決め、顧客に報告する。発見者に対応方針を伝えるかどうかを顧客と相談する。

(4) 顧客への受領通知の発行と詳細情報の管理

顧客より情報提供を受けた場合、受け取りしだい受領通知を返すと共に、預かった情報は機密情報として適切に管理する。

5.2. 脆弱性関連情報の評価

脆弱性関連情報の調査では、それらの脆弱性関連情報に対して「再現試験」とそれに続く「脆弱性評価」を行う。万一、当該脆弱性に起因して個人情報漏洩の事件があった場合、ウェブサイト運営者は、その事実を一般に公表するなど適切な処置が必要となるため、この観点から脆弱性の影響を評価する。

(1) 脆弱性を通知されたウェブシステムを確認する

脆弱性を通知されたウェブシステムの構成要素（OS やミドルウェア、アプリケーションなど）とその版番号や OS、ミドルウェアの設定情報を確認する。当該ウェブシステムの構成要素や設定情報について既に存在がわかっている脆弱性の中に、通知された脆弱性と同じものがないかを調べる。

(2) 指摘された脆弱性につながる現象の再現を試みる

通知された脆弱性関連情報に基づき、指摘された脆弱性につながる現象の再現を試みる。 なお、テスト環境が構築できず、顧客の本番環境を使用する場合は、顧客の同意を得た上で再現テストを実施する。再現を確認できた場合は、顧客にその旨を報告し、顧客が抱えている危険性を緩和するための対策を提示する。その際、個人情報などの情報漏洩が確認できた場合は、顧客に対しインシデント対応措置を実施するよう助言する。再現を確認できなかった場合は、顧客にその旨を伝え、さらに詳細な説明や脆弱性が発生する環境、設定条件などの補足情報の提供を依頼する。

(3) 脆弱性の原因と発現の条件を特定する

再現できた脆弱性の原因を特定する。原因がウェブシステムを構成するミドルウェアなどの製品の脆弱性に起因することが判明した場合には、IPA にその旨を連絡し、以降は 4.3 の製品の脆弱性対応を参照する。これまでに公表されていない製品の脆弱性である場合は、特に情報の守秘に関する配慮が必要となることに留意する。

原因と発現の条件が特定できたら、当該ウェブシステムと同様な構成要素で構築されているウェブシステムでも、同様な脆弱性が存在しないか確認する。

5.3. 対策の検討

対応が必要であると判断した際に、対策を検討する手順と留意すべき点を述べる。

対応が必要であると判断した後、顧客との調整を経て対策を実施することになるが、その前に影響度合いなどを調査しておかなければならない。システム全体に対策が必要なのか、部分的な対策でよいのか、対策適用による影響度など、いくつかの観点から対策を検討する。ウェブシステムの脆弱性は、ソフトウェア製品の脆弱性のように作業対象が明確になっている場合と異なり、広範な対策が求められるケース、脆弱性を持つ対象のみに対策を施せばよいケース、脆弱性を持つ対象以外で対策を施すケースなどがある。

また、公開された脆弱性対応のパッチを自発的に適用する場合と異なり、発見者によって外部から通知されているという点も考慮する必要がある。

5.3.1. 脆弱性の影響範囲の調査

まず、脆弱性が及ぶ範囲を調査する。たとえば、ウェブサーバ、アプリケーションサーバ、データベースサーバのような三層構造のシステムにおいて、脆弱性を放置して攻撃された場合、すべてのサーバに影響があるのか、アプリケーションサーバ単体などにのみ影響があるのか、踏み台にされて被害がさらに拡大する可能性があるのかなど、被害を想定した影響範囲を確定する。

① ネットワーク・ノード(サーバ、ネットワーク機器など)単位における影響度

② システム全体における影響度

③ 他のシステム(外部を含む)に対する影響度

ここで調査した結果は、対策を施すか否か、どの範囲に対策を行うかなどの判断材料となる。

5.3.2. 対策適用の影響度の調査

ウェブシステムに対する被害の影響範囲が確定した後、考えられる対策方法とその対策による影響を調査する。たとえば、ウェブアプリケーションを修正しなければならないのか、設定のみを変更すればよいのか、システムを停止せずに対応できるのか、対応のためにシステムを停止しなければならない時間がどのくらいかなどについて調査する。

① 修正を行うことが必要か否か。必要な場合の修正費用。

② 設定漏れなどの場合、設定変更で対応可能か否か。設定変更の場合の費用。

③ 脆弱性のあるノードそのものではなく、他のネットワーク機器などの対応によって回避可能か否か。その場合の費用。

④ それぞれの対策を講じた場合、システム停止の有無、停止を伴う場合の停止時間。

⑤ 冗長構成などの場合に、システムを停止せずに対策を適用することの可否。たとえば、二重構成の場合、一方を停止して対策を適用することができるが、同時に動かすと異なるバージョンのソフトウェアが混在して、期待した通りに動かなくなるケースがある。このような場合には、一時的に二重構成のいずれのシステムも停止しなければならない。

5.3.3. 修正方法の検討

アプリケーションの修正が必要な場合、その修正方法を検討する。その際、修正にかかる期間、費用などを見積もる。修正を実際に行うかどうかは、顧客との調整によって変わる可能性もあるため、状況に応じて判断する。明らかに修正が必要な場合には、顧客との調整に先行して修正を開始することも検討する。

5.3.4. 対応計画(スケジュール)の策定

対応方法によってスケジュール(準備期間や作業時間など)が変わるような場合、顧客との調整後

に、あるいは、顧客と調整しながら、対応計画を考える場合がある。しかし、準備に必要な期間や、要員の確保に必要な期間、影響度や段階的な対応のマイルストーンなどを対応方法に応じて、あらかじめ見積もっておかなければならない。

5.3.5. 対応費用の見積り

対応費用については、顧客との調整において重要な要素となるため、顧客に提示できるように見積もっておく。

5.4. 顧客との調整

対策の検討の後、顧客への対応手順と留意すべき点を述べる。

5.4.1. 契約の確認

顧客との調整にあたって、契約内容を確認する。

① 瑕疵期間内の場合の対応方法

② 脆弱性への対応についての記載の有無と記載内容(対応の範囲など)

③ 脆弱性への対応を行う場合の有償、無償の条件

④ 有償の場合の費用や対応範囲の上限

⑤ 無償の場合の対応範囲

⑥ その他、免責事項など

5.4.2. 顧客との対応方法、費用、日程の調整

顧客との調整にあたって、脆弱性の内容の説明、想定される被害の説明、費用などの提示、日程の調整などを行わなければならない。対策を行うか否か、どの方法によって対策を行うかなどの最終判断はウェブサイト運営者としての顧客が行わなければならないため、顧客が判断するに十分な情報を提供しなければならない。また、事故の発生時に、SI 事業者が十分な対応を行っていたことを示すために、提供した情報を文書などで残しておくことが望ましい。

(1) 脆弱性の内容の説明

顧客は IPA からの通知の内容を十分に把握しているとは限らない。そのため、IPA からの通知の内容がどのようなものなのか、何が起きるのかなどの十分な説明を行う必要がある。十分な理解が得られない場合、脆弱性が放置されるなどの不適切な対応が行われる可能性がある。

(2) 想定される被害の説明

脆弱性を放置した場合に想定される被害について、十分な説明を行う。顧客の直接的な被害だけでなく、間接的に起こりうる問題についても提示する。すなわち、放置による情報漏洩などの可能性や、情報漏洩による社会的信用の失墜、踏み台になった場合には加害者として追求されることな

どについても理解していただく必要がある。十分な説明を怠って顧客が対策不要と判断した場合に情報漏洩などの事故が発生すると、SI 事業者に損害責任を求められることも考えられる。

(3) 考えられる対策と、費用、および SI 事業者としての推奨する対応方法の提示

顧客に最終判断を委ねる必要があるため、考えうる対策と費用および対策による影響度、SI 事業者としての推奨する対応方法を提示する。たとえば、停止できないシステムにおいて、費用が高くシステム停止を伴う対応と、費用が安くシステム停止が伴わないが本質的な解決ではない対応方法(回避方法)がある場合、それぞれを提示して説明した上で、段階的な対策を講じるなどの推奨案を提示する。ただし、「無償の対応で SI 事業者が負担しなければならない費用」などの比較によって推奨案を提示するのではなく、顧客の立場に立って、もっとも最適と思われる推奨案を提示し、誠意ある対応を行わなければならない。

(4) 有償の場合の費用と作業範囲の合意

有償の場合でも、契約書などで費用の額が明確になっている場合と、個別に調整しなければならない場合がある。個別調整の場合には、後の紛糾を防ぐために顧客との間で覚書などを取り交わしておく。脆弱性の場合には、早急な対応を迫られるため、顧客との間で費用や作業範囲を明確にしないまま、対応作業を実施する場合がある。早期警戒パートナーシップの流れにおいては、第三者の発見者が存在するため、自発的な脆弱性対応に比べて特に対応のスピードが要求される。このような場合、顧客との合意が明確になっていないと、作業後に顧客との間でトラブルになることも考えられる。細かい点については対応実施後でも構わないが、費用の概算と作業範囲については、大筋で顧客と合意し、覚書などの文書として残しておくべきである。

(5) 作業時の連絡体制の確認

通常の作業の開始、終了の連絡方法以外に、事故が発生した場合の連絡体制を確認しておく。万が一、確認作業などで不慮の事態が発生した場合の緊急連絡方法や、作業中止・続行の判断の責任者などを確認しておく。

5.4.3. 対応方針の決定

十分な情報を提供し、討議した上で、最終的な対応方針を顧客に決定していただく。顧客に最終判断を委ねるのは、対策のための費用と被害による損失を比べた場合に、顧客が経営判断などによって対策を行わなくてよいと判断するケースもあるからである。そのような場合、SI 事業者は、社会的責任や発見者が脆弱性関連情報をリークする可能性などについても説明し、可能な限り顧客を説得しなければならない。顧客の判断によって情報漏洩などの事故が発生した場合に、SI 事業者の怠慢を指摘されないように、自己を防衛することも必要である。したがって、顧客への説明は口

頭のみではなく、文書で説明内容を残し、説明した事実を確認できるようにしておくことが望ましい。

5.5. 対策の実施

当該ウェブシステムへの対策を実施する際の留意すべき点を述べる。

脆弱性の対応は一般の不具合の修正と同様に、十分な試験を行い、作業手順を明確にしておく。ウェブシステムの場合には 24 時間運営を行っている場合が多く、停止時間を最短にする手順が求められる。

5.5.1. 修正の作成

ウェブアプリケーションの修正が必要な場合には、修正版プログラムやパッチなどを作成する。設定変更の場合や回避策の場合にも予め必要な設定変更ファイルを作成したり、回避策実施のために必要なプラグラムなどを作成する。

5.5.2. 試験環境における試験と作業手順の確立

試験環境において事前に対応作業を行う。設定変更や回避策の適用、パッチの適用による影響の確認だけでなく、作業時間やシステムの停止時間を最短にする手順を確立する。

① 脆弱性の存在を確認する。この時、確認作業自体がデータの破壊などを引き起こす場合があるため、顧客環境でデータ破壊などを回避して確認する方法について検討する。

② 脆弱性消失の確認方法および動作確認方法を確立する。

③ 対策により対象となる脆弱性が消滅することを確認する。

④ 対策によりミドルウェアやアプリケーションなど、稼動している他のプログラムに影響が無いことを確認する。

⑤ 対策により、他のノードなどのシステム全体に影響が無いことを確認する。

⑥ 作業を中止し、原状復帰するための手順を確立する。

⑦ 全体の作業時間および停止時間を最短にする対策の適用手順を策定する。この時、いくつかの段階で確認ポイントを置き、作業中止の判断とステップバックの作業を行えるようにする。

⑧ ⑦で策定した対策の適用手順についての作業訓練を行う。

5.5.3. 顧客環境における対策の実施

顧客環境における対策の適用作業を行う前に、顧客との最終調整を行う。試験環境において策定した作業手順を説明し、サービス停止時間の再確認を行う。顧客に検収していただくための判断方法も確認し、作業スケジュール、連絡体制などを最終決定する。顧客との最終調整後、脆弱性の

対策作業を実施する。

5.5.4. 対策効果の確認

次に、対策実施によって当該脆弱性を消滅できたか否かを確認する。この脆弱性の確認作業に際しては、試験環境においての確認で検討したとおり、確認作業によって顧客データが破壊されることがないよう注意する。攻撃手法が明らかになっている場合には実際に攻撃して脆弱性が無くなったことを確認することも可能であるが、必ず顧客との合意の上で細心の注意払った上で行う必要がある。

5.6. その他

5.6.1. IPA と発見者への対応完了通知

対応が完了したことをウェブサイト運営者である顧客を通じて IPA へ通知する。回避策であるか、本質的な修正であるかを問わず、脆弱性が少なくとも見かけ上は消失した時点で IPA へ報告を行う。詳細情報の通知の際に添付された「修正完了報告書」を用いて報告する。IPA が詳細情報を通知してから、IPA へ修正完了報告書を提出するまでの期間が 9 ヶ月を超えた場合、IPA は当該脆弱性の取扱いを終了し、協力を仰げなくなる場合がある。この期限は、IPA と調整することが可能である。なお、報告期限が過ぎても連絡が無い場合には、IPA からメールまたは電話で問い合わせが行われる場合がある。

「修正完了報告書」には IPA が確認作業を行うか否かを指定する欄があり、IPA へ確認協力を依頼することが可能である。IPA の確認を希望する場合は、日時の調整を行い、顧客が同意書を提出しなければならない。

ウェブサイト運営者が「対応しない」と決断した場合には、その旨を顧客から IPA へ通知していただく。

IPA は顧客からの「修正完了報告書」および希望した場合の確認作業の終了を待って、発見者に通知する。

発見者が直接連絡してきた場合には、顧客から発見者に対応が完了したことを連絡していただく。この時、発見者による確認作業を行うか否かなど、顧客と発見者の間で調整が必要である。IPA へ調整を依頼している場合には、IPA へ連絡し、対応完了後の発見者との調整を依頼する。

5.6.2. 契約内容の見直し

対応の完了後、あるいは対応と並行して、契約書の見直しを行う。問題なく対応できた場合には契約の見直しを行う必要は無いが、契約書の中で脆弱性の対応について明記されていない場合や、一連の対応において契約書の解釈の問題などが発生した場合には、顧客との間で覚書などを

取り交わしながら、契約の更改を行うようにするのが望ましい。3.3 項で記述したように、JISA が発行した「モデル契約書」の「セキュリティ」の項などを参照するとよい。

5.6.3. 事故の通知

個人情報漏洩などの事故が発生した場合には主務官庁に連絡しなければならない。ウェブサイト運営者が行うことであるが、脆弱性の対応者の一員として SI 事業者も認識しておくべき事項の一つである。事故の通知は個人情報保護法や各省庁のガイドラインにしたがって実施する。

5.6.4. 他の顧客への展開

同様のシステムを他の顧客に使用しているか否かを確認する。同様のシステムがある場合には、他の顧客にも連絡、調整して対応を行う。これは、IPA から SI 事業者に直接要請されることがある。この場合、SI 事業者は IPA に対して対応状況を報告する必要があるが、個別の顧客名までを通知する必要はない。なお、付録 2 に、類似脆弱性の有無を確認する社内依頼文のサンプルを添付した。

6. まとめ

本書で述べたようなSI事業者における脆弱性情報に対する適切な対応とそのための体制と手順の整備は、社会からも顧客からも今後益々要求されることになると考えられ、本書がSI事業者にとって社内対応体制を整備する際の一助となれば幸いである。同時に、脆弱性への対応がいわゆる瑕疵とは区別されるべきであることに関する顧客の理解を得るための継続的な活動を続けることも重要であり、本書が今後の顧客とSI事業者との相互理解を促進するための参考となることを期待する。また、本書では範囲外としたが、ウェブアプリケーションの設計・構築の段階で脆弱性を作り込まない開発手法の研究や教育、脆弱性を悪用したインシデントが実際に発生してしまった場合の対応についての準備も重要である。なお、脆弱性情報やパッチの副作用情報などのSI事業者間の共有は今後の課題である。

付録 1：IPA からの脆弱性関連情報通知と IPA への脆弱性修正完了報告の様式

(1) IPA から顧客への脆弱性関連情報の通知フォーマット例 (第1段階)

件名:【IPA#********】ウェブページのセキュリティ上の問題

○○ 様

独立行政法人 情報処理推進機構(IPA)セキュリティセンターです。

IPA では、情報セキュリティ対策の一環で、経済産業省告示に従い、一般の方や研究者の方が発見され、IPA に報告されたウェブページのセキュリティ上の問題点を、ウェブページの管理者の方に連絡する業務をおこなっています。

このたび、下記ウェブページのセキュリティ上の問題について届出がありましたので、ご連絡します。

対象の URL:

http://example.co.jp/xxxxxxx/yyyyyyy.html

今後、問題の詳細・影響などの詳細情報をご連絡するために、連絡先、担当者様をお教えいただきたく、下記の IPA 連絡先メールアドレス宛へ返信をお願いします。

IPA 連絡先メールアドレス: vuln-contact@ipa.go.jp

詳細情報をご連絡した後、セキュリティ上の問題の有無の確認、修正をお願いいたします。

なお、ウェブサイトの運用・管理を外部の事業者に委託されている場合も、IPA からの連絡窓口は○○様とさせていただきます。お手数ですが、委託先へは○○様よりご連絡ください。

以上、よろしくお願いいたします。

(2) IPA から顧客への脆弱性関連情報の通知フォーマット例 (第2段階)

件名:【IPA#********】セキュリティ上の問題に関する詳細情報送付の件

このメールは、取扱番号 IPA******** に関する連絡です。

○○ 様

IPA セキュリティセンターです。

先に、貴ウェブページのセキュリティ上の問題に関し IPA に届出があったことをご連絡しました。本メールでは、このセキュリティ上の問題の詳細と、今後の取扱いについてご連絡します。

なお、詳細情報の送付を確認するため、本メールに返信をお願いいたします。その際、件名に取扱番号 IPA******** を加えてください。

1.詳細情報

発見者から次の報告が届いています。

==========

1) セキュリティ上の問題を確認したウェブサイトの URL

http://example.co.jp/xxxxxxx/yyyyyyy.html

2) セキュリティ上の問題の種類

クロスサイトスクリプティング

入力フォーム欄に下記の文字列を入れて送信することにより、確認

3) 問題の説明

画面に遷移後、スクリプトが実行されてダイアログが表示されました。

(スクリプト例)

上記から、任意のスクリプトが実行できる可能性が高いものと考えられます。

4) セキュリティ上の問題により発生しうる脅威

悪意のあるスクリプトの実行等

==========

IPA では検証や確認を行っていませんが、発見者からの情報によれば、セキュリティ上の問題が存在する可能性がありますので、問題の有無を調査してください。

問題の有無の調査にあたっては、以下のページを参考にしてください。

- IPA セキュリティセンター 「セキュア・プログラミング講座」

http://www.ipa.go.jp/security/awareness/vendor/programming/

2.今後の取扱いについて

1) 取扱番号の使用

今後のご連絡の際は下記取扱番号をメールの件名に加えてください。

取扱番号: IPA#**********

2) 一次返信

詳細情報の送付を確認するため、返信をお願いします。

3) セキュリティ上の問題の有無の調査

セキュリティ上の問題の有無を調査してください。その結果を、本メール受信後 20 営業日以内を目処にお知らせください。

4) セキュリティ上の問題の修正

セキュリティ上の問題が存在した場合は修正をお願いします。

修正は、3 ヶ月以内を目処に実施してください。

5) 修正完了報告書の送付

修正完了後、添付の「修正完了報告書.txt」に必要事項記入の上、送付してください。

6) 委託事業者との連絡

ウェブサイトの運用・管理を第三者に委託している場合も、IPA からの連絡窓口は、○○○○様とさせていただきます。お手数ですが、委託先へは、○○様からご連絡ください。

上記を含む今後の取扱いについては、添付の「今後のセキュリティ上の問題に関する取扱いのお願い.pdf」をご参照ください。

以上、よろしくお願いいたします。

(3) 顧客から IPA への脆弱性の修正完了報告書例

セキュリティ上の問題の修正完了報告書

1. セキュリティ上の問題の修正完了報告

セキュリティ上の問題の修正が完了したことを以下の通り報告します。

取扱番号：IPA#**********

対象ウェブページ URL：http://example.co.jp/xxxxxxx/yyyyyyy.html

対応内容：

2. IPA による確認作業

この報告の後、IPA によるセキュリティ上の問題の修正に対する確認作業を

□ 希望します （※ 希望される場合は、同意書を提出いただきます）

□ 希望しません

3. 今後、同じサイトにセキュリティ上の問題があるとの届出があった場合の連絡先

□ 以下のアドレスを使用する

メールアドレス：

ご担当者名:

□ ウェブサイトの受付窓口を通じて、その都度担当者を決定する

平成　年　月　日

組織名：

所　属：

氏　名：

＊　＊

【 アンケート 】

お手数ですが、以下のアンケートにご協力ください。

このアンケートは、IPA が公表する統計情報の集計のために利用します。

統計情報は、ウェブサイト、およびウェブサイト運営者が特定されない形で公表します。

※) 各回答欄において「その他」を選択した場合、および、問 2 (ウ) 、 問 3 に関しては、具体的な内容を記入してください。

◆ 問い

今回、修正していただいたセキュリティ上の問題に関して、下記の選択項目より該当するものを選び、回答欄に記入してください（複数選択可）。

その他を選択した場合、問 2 (ウ) および 問 3 に関しては、回答欄に具体的な内容を記入してください。

---

1 セキュリティ上の問題の原因

(ア) 原因が何に依存していたかに関して、以下の中から回答してください

a. ウェブアプリケーションの設計

b. ウェブサイト特有の設定・運用

c. その他

(イ) 原因の詳細に関して、以下の中から回答してください

a. 許可する意図のないアクセスを可能にしている

b. 入力チェックを適切にしていない（意図しない SQL コマンドなどの実行が可能になる）

c. 入力チェックを適切にしていない（オーバーフローが生じる）

d. クロスサイトスクリプティングが可能になる不備が存在する

e. エラー処理を適切にしていない

f. 暗号化に失敗している・解読可能な方法で暗号化している

g. その他

……

2 セキュリティ上の問題の影響

(ア) 実際に生じた被害に関して、以下の中から回答してください

a. アクセス制御を回避された

b. 情報漏洩（個人情報）が生じた

c. 情報漏洩（サーバの実装情報）が生じた

d. 情報漏洩（その他の機密情報）が生じた

e. Cookie の漏洩が生じた

f. なりすましをされた

g. データを改ざん、破壊された

h. サービス不能状態に陥った

i. 意図しないコマンドを実行された

j. 被害はなかった

k. その他

(イ) 実際には生じなかったが、生じる可能性のあった被害に関して、以下の中から回答してください

a. アクセス制御を回避される

b. 情報漏洩（個人情報）が生じる

c. 情報漏洩（サーバの実装情報）が生じる

d. 情報漏洩（その他の機密情報）が生じる

e. Cookie の漏洩が生じる

f. なりすましをされる

g. データを改ざん、破壊される

h. サービス不能状態に陥る

i. 意図しないコマンドを実行される

j. その他

(ウ) (イ)で「情報漏洩」を選択した場合、漏洩する可能性のあった情報の種類を回答してください

例) 氏名、クレジットカード情報、ユーザのパスワード

……

3 その他

今回の脆弱性関連情報の通知に関して、ご意見を回答してください

◆ 回答欄

1 (ア) [　　]

　(イ) [　　]

2 (ア) [　　]

　(イ) [　　]

　(ウ) [　　]

3　　[　　]

ご協力ありがとうございました。

付録 2 類似脆弱性の有無についての社内調査依頼例

【社外秘】

各プロジェクト セキュリティ責任者の皆様へ

制度に基づく通知であることを明記

経済産業省告示の情報セキュリティ早期警戒パートナーシップ制度に則り、先日、IPA から当社に対し、以下の通知がありました。

・ 当社が構築したシステムにおいて情報セキュリティ上の脆弱性が発見された旨の通知

・ 当社の類似システムにおける問題有無の調査依頼

これを受け、当社関係のシステムを対象に類似脆弱性の問題有無の調査を実施します。つきましては、貴プロジェクトにおいて、下記の調査・報告の実施をお願いいたします。なお、IPA に対する報告はシステム開発セキュリティ・センターにて行いますが、個別のお客様名については報告いたしません。

※重要※

調査が不十分であったり、お客様への情報提供を怠った結果として、同様の脆弱性が当社関係の他システムから発見された場合は、当社の信用失墜につながる事態となる可能性があります。

調査の重要性について説明

(1) 脆弱性の概要

○○事業部で開発された Java アプリケーションインストールモジュールを利用したプログラムを利用者が実行すると、Java 環境のセキュリティポリシーを強制的に書き換えます。この書き換え内容に問題があるため、ウェブページ上に仕掛けられた罠などにより、クライアント上のファイルが盗み見られたり、破壊されたり、クライアントが第三者への攻撃の踏み台にされる可能性があります。また、他の Java アプリケーションが動作しなくなる可能性があります。

※ IPA から当該脆弱性について注意喚起が公開されています。

IPA「Java セキュリティポリシーの独自設定に関する注意喚起」

http://www.ipa.go.jp/security/vuln/20050228javapolicy.html

脆弱性の結果、どのような脅威があるのかを明記

(2) 調査対象範囲

下記条件全てに該当するシステムについて調査願います。なお、調査は当社が開発したシステ

ムについてはお客様との保守契約の有無に関わらず実施してください。また、当社が開発したシステムではなくても現在保守契約を締結しているシステムについては調査願います。

1) クライアントプログラムの実行環境として J2RE を使用し、クライアント PC に J2RE をインストールさせるシステム。

2) ○○事業部が開発し Java アプリケーションインストールモジュールを利用している、もしくは、独自に J2RE のセキュリティポリシーファイル (java.policy) の書き換えを行っているシステム、または、他のセキュリティポリシーファイル(ユーザポリシーファイルなど)を読み込み、java.policy の書き換えと同等の機能を実現しているシステム。

調査対象をできるだけ具体的に明示

(3) 調査内容

J2RE セキュリティポリシーファイル (java.policy) または他のセキュリティポリシーファイルにおいて、grant エントリーを用いて不適切、不必要なポリシー設定を行っていないかを確認してください。

以下のような適用範囲を制限していない grant エントリーは、任意の Web サイトに設置された Java アプレットに対して有効になってしまい、クライアントPCのセキュリティレベルを低下させる事となります。この様な設定を行っていないか確認してください。また、そのプログラムに必要最小限のアクセス権を設定しているかを確認してください。

×悪い設定例

```
-------------------------------------------------------------
grant {
permission java.io.FilePermission 〜〜〜略〜〜〜
};
-------------------------------------------------------------
```

→ grant エントリーは、signedBy フィールドを利用した署名確認や、codeBase フィールドを利用したコードベース指定を行う必要があります。

○良い設定例

```
-------------------------------------------------------------
grant signedBy "example", codeBase "http://example.com/*" {
permission java.io.FilePermission 〜〜〜略〜〜〜
};
-------------------------------------------------------------
```

(4)該当した場合の対応

原則として、お客様と保守・運用契約を締結しているシステム、瑕疵期間中のシステム、当社自らが提供しているシステムについては、社内関連規程（情報セキュリティ脆弱性対応手順書）に従って、各プロジェクトにおいて個別に対応願います。お客様との保守契約等がないシステムの対応については、お客様へ本件についての情報提供を行い、改修要否の判断をお客様と相談してください。なお、対応に当たっては、JISA-JEITA が発行している「SI 事業者における脆弱性関連情報取扱に関する体制と手順整備のための課題とガイダンス」も参考にしてください。また、個別プロジェクトで判断が難しい場合は、システム開発セキュリティ・センターでも相談を受けます。

社内で手順が決まっていない場合は、本ガイダンスも参考にしてください

(5)報告事項

1)類似脆弱性が存在するシステムの有無

2)類似システムが存在した場合は、以下の情報も合わせて報告願います。

◆当該システムの属性情報

a)システム名（もしくはサービス名）

b)お客様名

c)開発形態

当社開発システム／他社開発システム

d)サービス開始年月日

e)現在の契約状況

瑕疵期間中／定期保守受託／運用受託／無し

f)担当者名および連絡先

お客様名も報告してもらいますので、機密情報として取り扱う必要があります

(6)報告様式および報告方法

◆報告様式：○○○○.xls

◆報告方法：上記様式に記入後、所定のパスワードを付与し、下記アドレスへ送付してください。

csirt@ssdc.xx.co.jp

(7)報告期限

200X.X.X（金） 10：00 厳守

(8) 参考

o 経済産業省 情報セキュリティ早期警戒パートナーシップ

http://www.meti.go.jp/policy/it_policy/press/0005399/

o JISA-JEITA 「SI 事業者における脆弱性関連情報取扱に関する体制と手順整備のための課題とガイダンス」

http://www.jisa.or.jp/xxxxx/xxxxxx/xxxxxx.html

o Java セキュリティポリシーの独自設定に関する注意喚起

http://www.ipa.go.jp/security/vuln/20050228javapolicy.html

o ウェブポケットがユーザにセキュリティレベルを下げる設定を指示していた問題

http://www.securityfocus.com/archive/79/257540

※過去に公開された類似事例

【本件問合せ先】

システム開発セキュリティ・センター

CSIRT チーム

TEL: 03-XXXX-XXXX

E-mail: csirt@ssdc.xx.co.jp

以上

付録 3：SI 事業者におけるセキュリティ対応体制のモデル事例

ここでは、「システム開発セキュリティ・センター」のモデル事例を紹介する。セキュアなシステム構築のためのセキュリティ技術、プロジェクト管理力の強化を目的とした組織を構築する際の参考にしていただきたい。

1. 目的と役割

システム開発セキュリティ・センターは、受託システム開発、ソフトウェア製品開発、ソリューション製品開発、社内システム開発の各プロジェクトが、セキュリティの確保された開発環境でセキュアなシステムを開発できるように、システム開発プロセスを規定し、各プロジェクトのセキュリティ対策が強化され、顧客の情報セキュリティを確保することを目的とする。

システム開発セキュリティ・センターの役割は以下の通り。

・セキュリティ関連情報の収集・発信

・システム開発セキュリティリテラシ向上教育

・システム開発プロセス関連文書の整備

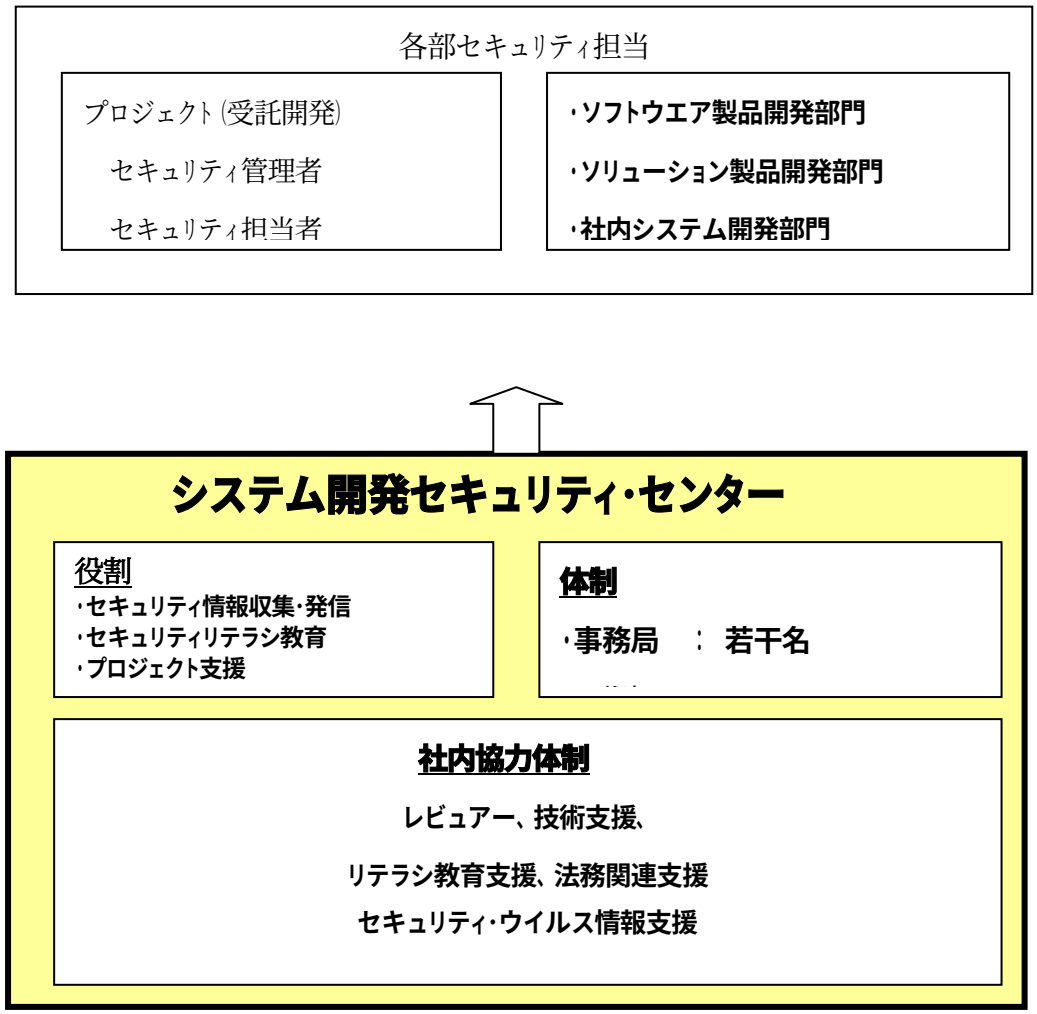
・システム開発におけるセキュリティ関連技術支援

2. 活動

システム開発セキュリティ・センターは、従来からの活動をさらに発展・強化し、システム開発のセキュリティ対策プロセスを見直し、開発プロジェクトのセキュリティ対策 向上を図り、セキュアなシステム開発を推進する。

主な作業項目	活動
セキュリティ情報の収集・発信	①公的機関からのセキュリティ情報（脆弱性、パッチ等）収集・プロジェクトへの発信
	②社内ホームページをセキュリティ情報発信の基盤として運用
	③緊急時に組織単位に警告メール送信
	④セキュリティ技術主管部を中心にした QA 回答チームを組織化。QA の内容は FAQ としてホームページに掲載
システム開発セキュリティリテラシ向上	⑤プロジェクト担当・セキュリティ担当に対する教育
	⑥リテラシ向上のための教材をホームページ上より公開
	⑦開発環境セキュリティポリシーをホームページ上に公開
	⑧セキュアシステム開発ガイドをホームページ上に公開 ・システム基礎編　・アプリケーション編　・個人情報保護編
プロジェクト支援	⑨システム開発プロセス改訂、セキュアシステム開発ガイド等整備
	⑩セキュリティ・プロセス・レビュー参加
	⑪脆弱性サイト調査

3. システム開発セキュリティ・センター体制図



4. セキュアシステム開発プロセスの概要

(1) 基本方針

①開発する顧客システム(ネットワーク、サーバ、アプリケーション)に対する外部からの悪意ある攻撃および個人情報保護に対するセキュリティ対策とプロジェクトの開発環境セキュリティを対象範囲とする。

②基本的にはプロジェクト内でのセキュリティ・レビューとして実施するが、付表1に示すセキュリティ要求度を定義し、セキュリティ要求度「高」については、第三者レビューをルール化する。

③提案レビューで、セキュリティ要求度を設定し、品質保証レビューでセキュリティ要求度に応

じたセキュリティプロセス実施と開発環境のセキュリティ対応の状況につき確認する。

(2) セキュリティレビュー実施時期

① 提案段階

セキュリティ要求度の設定、リスク／提案内容の評価

② 要件定義・論理設計終了時

セキュリティ要件・機能および開発環境セキュリティの必要十分チェック（客先承認）

③ 物理設計終了時

セキュリティ設計の妥当性確認、システム実装注意点の確認および開発環境セキュリティの必要十分チェック

④ 統合・システムテスト時

セキュリティシステムの実装確認およびテスト環境セキュリティの確認

⑤ リリース時

セキュリティシステムの品質判定（客先受入れ検収）

(3) セキュアシステム開発プロセス実施体制

①全社主管 ： システム開発セキュリティ・センター

・セキュリティ情報の収集と発信

・セキュリティ要求度「高」のプロジェクトの第三者レビュー実施

②各部 ： 部内セキュリティ担当

・部内へのセキュリティ情報の周知徹底

・部内プロジェクトのセキュリティプロセスの指導と支援

・セキュリティ要求度「中」のプロジェクトの第三者レビュー実施

③各プロジェクト ： プロジェクト内セキュリティ担当

・プロジェクトメンバへのセキュリティ情報の周知徹底

・自プロジェクト（セキュリティ要求度「低」）のセキュリティレビュー実施

付表1. セキュリティ要求度

レベル	適用基準	該当ケース例	補足条件	役割
高	提供するシステムのセキュリティ不備が社会的問題かつ会社の信用につながる恐れのある案件。	①不特定多数の利用者が利用するインターネット業務 （官公庁・金融・運輸・通信・流通等の一般大衆向けシステム） ②国家的機密を要する業務 （政府省庁から機密保護を要求されたシステム） ③テロ等の対象となる業務 （原子力・ダム・公的研究所・放送／新聞等の基幹システム） ④人命に関わる業務 （医療・交通・工場等の制御系のシステム） ⑤重要なプライバシー情報を取り扱う業務 （クレジット番号、銀行口座番号等）	■左記ケースは案件の規模に関係なく、セキュリティ脆弱を攻撃された時の社会的影響度で判定する。 ■会社がセキュリティ全体責任を負っていない場合で、問題発生時に社名が公表される可能性がある時、高レベルとする。逆にその可能性が無ければ中レベルとする。	■レベルの申請：実行PM予定者 ■レベルの照査：組織長 ■主レビューア：システム開発セキュリティ・センター
中	提供するシステムのセキュリティ不備が会社の責任問題になる案件	①顧客のユーザが利用するインターネット業務 （一般企業の BtoB、BtoC の新規システム） ②高レベルのケースで会社がシステム全体の責任を 負っていない案件	■セキュリティ脆弱を攻撃された場合の影響範囲が特定され、対応のためのシステム停止が許される場合。 ■①のケースで会社がセキュリティ全体責任を負っていれば中レベルとし、そうで無ければ低レベルとする。	■レベルの申請：実行PM予定者 ■レベルの照査：組織長 ■主レビューア：部内セキュリティ担当者
低	発注側でセキュリティ環境が確立しており、その環境下で基本的なセキュリティの考慮を行う案件	①ネットワーク、セキュリティ方針が発注側の責任で確立している環境に追加変更するインターネット業務 （一般企業の BtoB、BtoC の追加変更システム） ②中レベルのケースで会社がシステム全体の責任を 負っていない案件	■セキュリティに関する仕様を発注側より提供されるシステム。 ■①のケースで会社にセキュリティに関する追加サービスを要求された場合は、中レベルとする。	■レベルの申請：実行PM予定者 ■レベルの照査：組織長 ■主レビューア：プロジェクト内 セキュリティ 担当者

※上記はあくまでモデル事例としてのサンプルです。

セキュリティ委員会・脆弱性等取扱基準作成検討部会　委員名簿

部会長	西尾　秀一	(株)エヌ・ティ・ティ・データ
副部会長	山本　富夫	三菱電機インフォメーションシステムズ(株)
委員	野村　武史	オムロンソフトウェア(株)
〃	香取　浩二	(株)ＣＳＫ
〃	宮嶌　明	ＪＦＥシステムズ(株)
〃	鈴木　修	東芝情報システム(株)
〃	河本　高文	東芝ソリューション(株)
〃	青木　美佐	日本アイ・ビー・エム(株)
〃	吉並　弘之	日本電気(株)
〃	前野　茂人	日本電子計算(株)
〃	五十嵐　智	日本ユニシス(株)
〃	内藤　聰	日本ユニシス・ソリューション(株)
〃	中田　雅弘	(株)日立製作所
〃	大力　洋介	富士通(株)
〃	土屋　昭治	富士通(株)
〃	片柳　勲	富士通エフ・アイ・ピー(株)
〃	合原　英次郎	松下電器産業(株)
〃	西岡　秀司	三菱電機(株)
〃	林　美喜男	横河電機(株)
〃	清水　孝祥	横河電機(株)
〃	浅井　克彦	リコーソフトウエア(株)
〃	吉川　博晴	リコーソフトウエア(株)
オブザーバ	川口　修司	経済産業省
オブザーバ	佐藤　貴幸	経済産業省
オブザーバ	南　英生	経済産業省
オブザーバ	石飛　節	経済産業省
オブザーバ	大林　正英	有限責任中間法人ＪＰＣＥＲＴコーディネーションセンター
オブザーバ	平田　雅浩	有限責任中間法人ＪＰＣＥＲＴコーディネーションセンター

オブザーバ	鎌田 敬介	有限責任中間法人ＪＰＣＥＲＴコーディネーションセンター
オブザーバ	福澤 淳二	独立行政法人 情報処理推進機構
事務局	田原 幸朗	(社)情報サービス産業協会
事務局	佐藤 厚夫	(社)情報サービス産業協会