セキュリティ担当者のための
脆弱性対応ガイド

～企業情報システムの脆弱性対策～

情報セキュリティ早期警戒パートナーシップガイドライン
別冊

2017年 3 月

独立行政法人情報処理推進機構
一般社団法人 JPCERT コーディネーションセンター
一般社団法人 電子情報技術産業協会
一般社団法人 コンピュータソフトウェア協会
一般社団法人 情報サービス産業協会
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

目　　次

1. 情報システムを安全に使い続けるために 1
1.1. 情報システムと脆弱性 1
1.2. 本資料の目的 3

2. 欠かせない脆弱性への対処 4
2.1. 情報セキュリティ対策と脆弱性対策 4
2.2. 脆弱性に起因するトラブルとその影響 5
2.3. セキュリティ担当者に期待される役割 9

3. 脆弱性対策のポイント 11
3.1. 設計・開発・導入段階における対策実施 11
3.2. 運用段階における対策実施 14
3.3. 脆弱性の存在が判明した際の対処手順 17
3.4. 委託について 19

4. 参考資料 20
4.1. 情報セキュリティ早期警戒パートナーシップ 20
4.2. 参考 URL 21

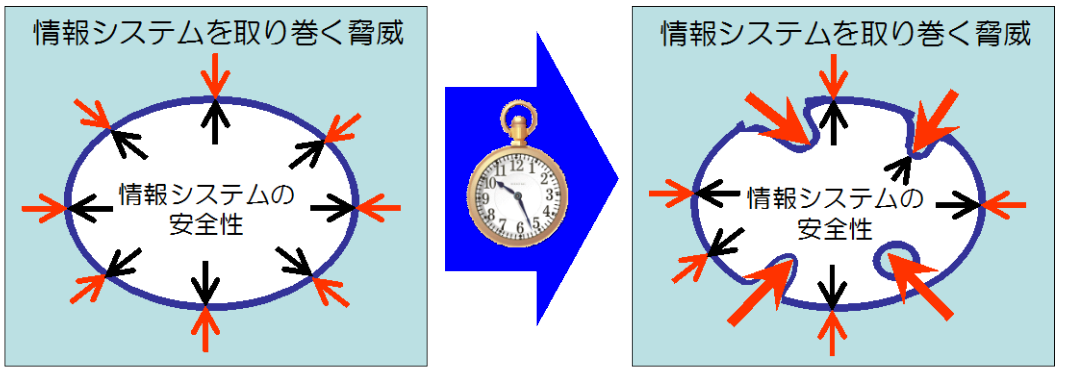
1. 情報システムを安全に使い続けるために

1.1. 情報システムと脆弱性

■時間が経つと情報システムの安全性は低下する

私たちがビジネスや生活の中で利用している情報システムのソフトウエアは消耗することがないため、時間が経ってもその機能は劣化しません。

しかし、時間が経ち、情報システムに対する新しい攻撃手法が開発されたり、情報セキュリティ上の「弱点」が発見されると、情報システムの安全性は低下します。つまり、開発時から何年間も更新されていない情報システムは、変化する脅威に対応できず、危険な状態に陥る可能性があるのです。



情報システムの脅威と安全性の変化

■脆弱性とはなにか

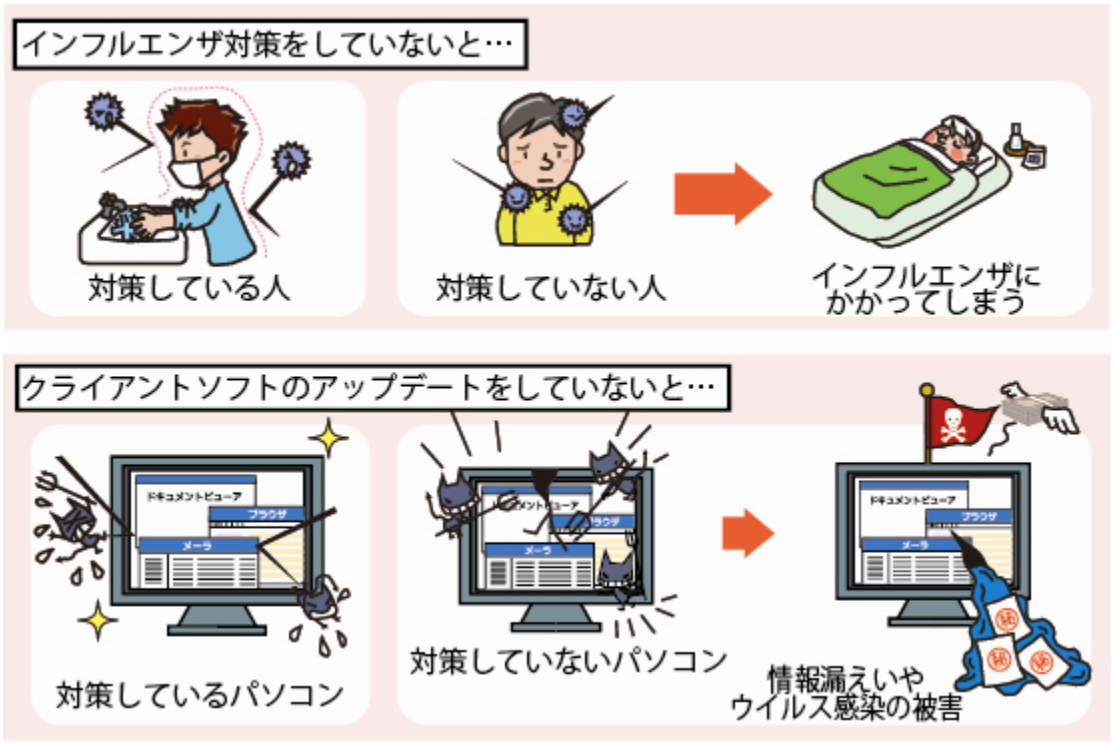
攻撃者は、一般に、情報セキュリティ上の「弱点」を突いて、情報システムに侵入したり、コンピュータウイルスを感染させます。このような「弱点」は、「脆弱性（ぜいじゃくせい）」[1]と呼ばれています。

[1] ソフトウエア等において、コンピュータ不正アクセス、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安全性上の問題箇所。ウェブアプリケーションにあっては、ウェブサイト運営者がアクセス制御機能により保護すべき情報等に誰もが

組織のネットワークシステムを建物にたとえると、脆弱性は外から建物に入る抜け穴のようなものです。いくら入口を厳重に固めても、外壁にほころびがあれば攻撃者はそこから侵入してきます。一般に利用されているソフトウエア製品に脆弱性があることがわかると、同じ製品を利用しているネットワークシステムはみな同様のほころびを抱えている状況に陥ります。

ソフトウエア製品の脆弱性は日々発見されていて、すでに数万種類もの脆弱性が公表されています[2]。これらの脆弱性は、ウイルス対策ソフトを使っても取り除くことができません。コンピュータウイルスを駆除しても、脆弱性対策を行わなければ新たなウイルスにより再び感染してしまう可能性があるのです。

ソフトウエア製品の脆弱性の場合、製品開発者が提供する修正プログラム（パッチ）を適用して解決します。また、ウェブサイトのように自ら開発したプログラムの脆弱性の場合、自身で問題箇所を改修する必要があります。



脆弱性対策のイメージ[3]

アクセスできるような、安全性が欠如している状態を含む。

[2] 米 NIST(National Institute of Standards and Technology)が運営する National Vulnerability Database (https://nvd.nist.gov/)より

[3] IPA「2010 年版 10 大脅威 あぶり出される組織の弱点！」（https://www.ipa.go.jp/security/vuln/10threats2010.html）より引用

1.2. 本資料の目的

本資料は、組織内の情報セキュリティを担当する方、特に情報システム分野に必ずしも詳しくない方を想定した内容になっています。

情報セキュリティの担当には、経営層の方（CIO[4]、CISO[5]など）の場合と、現場の管理者・作業者の場合が考えられます。本資料では、それらをまとめて「セキュリティ担当者」と呼びます。

本資料の目的は、セキュリティ担当者が、情報システムの脆弱性に対処する基本的な考え方を紹介することです。

[4] Chief Information Officer：最高情報責任者

[5] Chief Information Security Officer：最高情報セキュリティ責任者

2. 欠かせない脆弱性への対処

2.1. 情報セキュリティ対策と脆弱性対策

情報セキュリティ対策には、技術面、管理面、法令対応など様々な観点があり、組織内の状況に応じてそれらを適切なバランスで実施する必要があります。たとえば、ISO/IEC 27001 附属書 A では、情報セキュリティ管理策を以下のように分類整理しています。

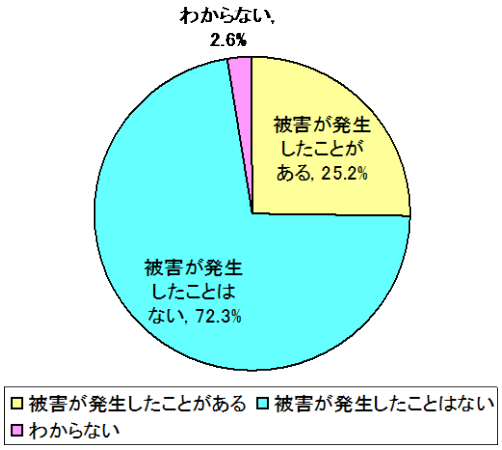
1. セキュリティ基本方針
2. 情報セキュリティのための組織
3. 資産の管理
4. 人的資源のセキュリティ
5. 物理的及び環境的セキュリティ
6. 通信及び運用管理
7. アクセス制御
8. 情報システムの取得, 開発及び保守
9. 情報セキュリティインシデントの管理
10. 事業継続管理
11. 順守

脆弱性対策は情報セキュリティ対策の一つで、攻撃を受ける弱点を減らす対策です。他の対策に注力していたとしても、脆弱性対策が不十分だと、次節に示すようなトラブルを招きかねません。セキュリティ担当者は、情報セキュリティ対策の一環として、情報システムの設計・開発、運用等の各フェーズで必要な脆弱性対策を実施することが求められます。また、脆弱性に起因するトラブルが発生した場合には、一連の対処業務の一つとして脆弱性対策を施し、問題が再発することを防がなければなりません。

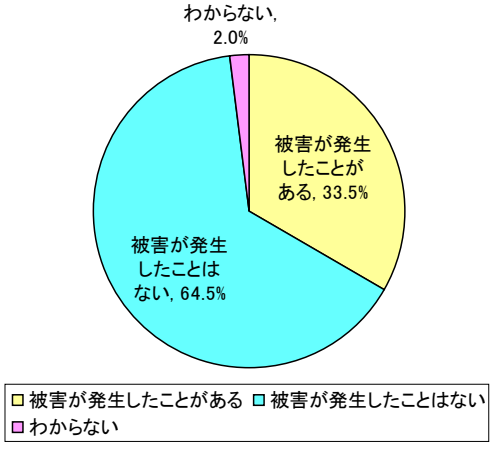
2.2. 脆弱性に起因するトラブルとその影響

組織内の情報システムに脆弱性があると、どのような問題が生じるのでしょうか。情報システムに脆弱性があっても、それを悪用する攻撃がなければトラブルは起こりません。しかし、脆弱性が狙われて攻撃が成功すると、組織にとって深刻なトラブルに発展することがあります。

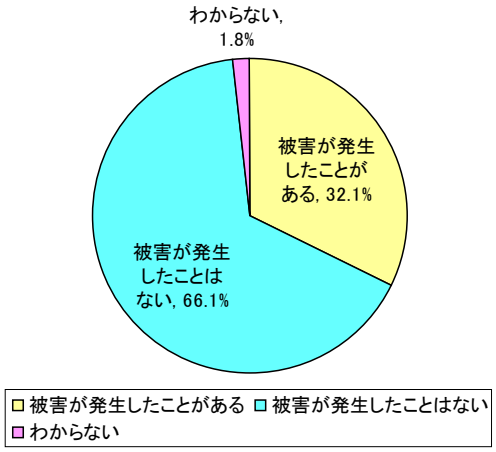
独立行政法人情報処理推進機構（IPA）が 2010 年に実施した実態調査[6]によると、脆弱性に起因するウイルスやワーム、不正アクセス等の被害経験については、ウェブサイト、組織内向けシステム、クライアント PC のいずれに関する被害についても３割前後の組織が「被害あり」としています。



ウェブサイト



組織内向けシステム



クライアント PC

脆弱性に起因するウイルスやワーム、不正アクセス等の被害経験

[6] IPA「企業等における脆弱性対策に関する実態調査報告書」(2010 年 7 月実施、310 機関回答)

別の調査では 2009 年に被害に遭った企業では平均 200 万ドルの損失が発生したことが報告[7]されています。

生じる被害は、情報漏えいに伴う補償や事業中断、復旧対策等の直接的なコストだけではありません。それまで築き上げてきたブランドや社会的信用が失墜し、大切な顧客を失う影響は深刻なものです。

以下では、近年の脆弱性に起因するトラブル事例をいくつか紹介します。

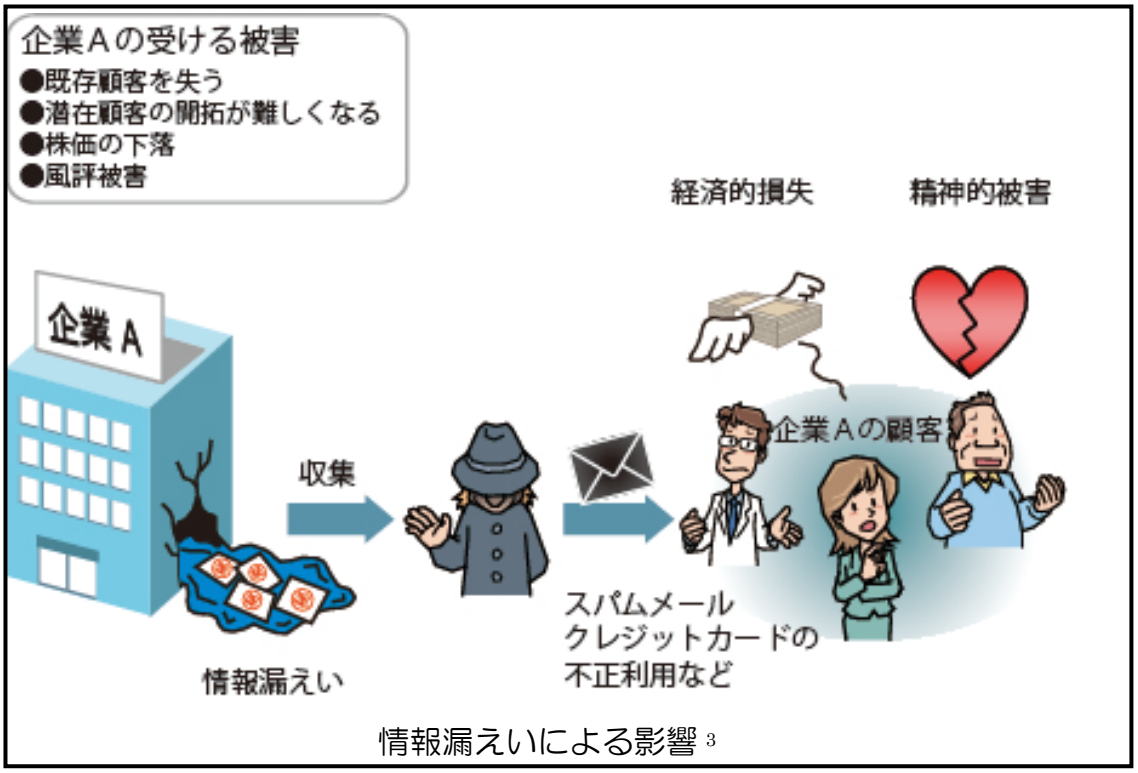
[7] Symantec; “2010 State of Enterprise Security Report”, 2010/03
http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=sesreport2010

■事例１　ウェブサイトへの不正アクセスによる事業中断

リスクとシステム一時停止の判断の重要性

インターネット上で商品を販売する事業者のウェブサイトが、不正アクセスを受け、トップページが改ざんされました。また過去の注文者情報（氏名、住所等）も流出した可能性があるにも関わらず、攻撃内容がログに残らないようにされていたため詳細な原因究明ができませんでした。その結果、原因究明や今後の対応検討のため、**ウェブサイトを３ヶ月停止することとなり、新商品の販売収益が予測よりもかなり低く**なりました。また、**顧客への説明・謝罪や原因究明等の対策コストを含めるとビジネス上の損失金額は数千万円**になると考えられます。

この不正アクセスは Apache Struts2 の脆弱性を突いたものでした。最新のパッチは２日前に公開されていましたが、パッチ適用には１ヶ月ほどウェブサイトを停止する必要があり、パッチを適用するためにウェブサイトを停止している期間の新商品の販売機会損失額と、ウェブサイトを停止せずに攻撃を受けた場合に被りうるリスクを検討している間に攻撃されました。結果としてはパッチ適用にかかる期間以上ウェブサイトを停止することになり、パッチ適用時よりも大きな機会損失となりました。このように脆弱性を悪用された結果、事業そのものの中断による機会損失が発生し、更には対策コストを合せると多額の損失金額に発展することがあります。



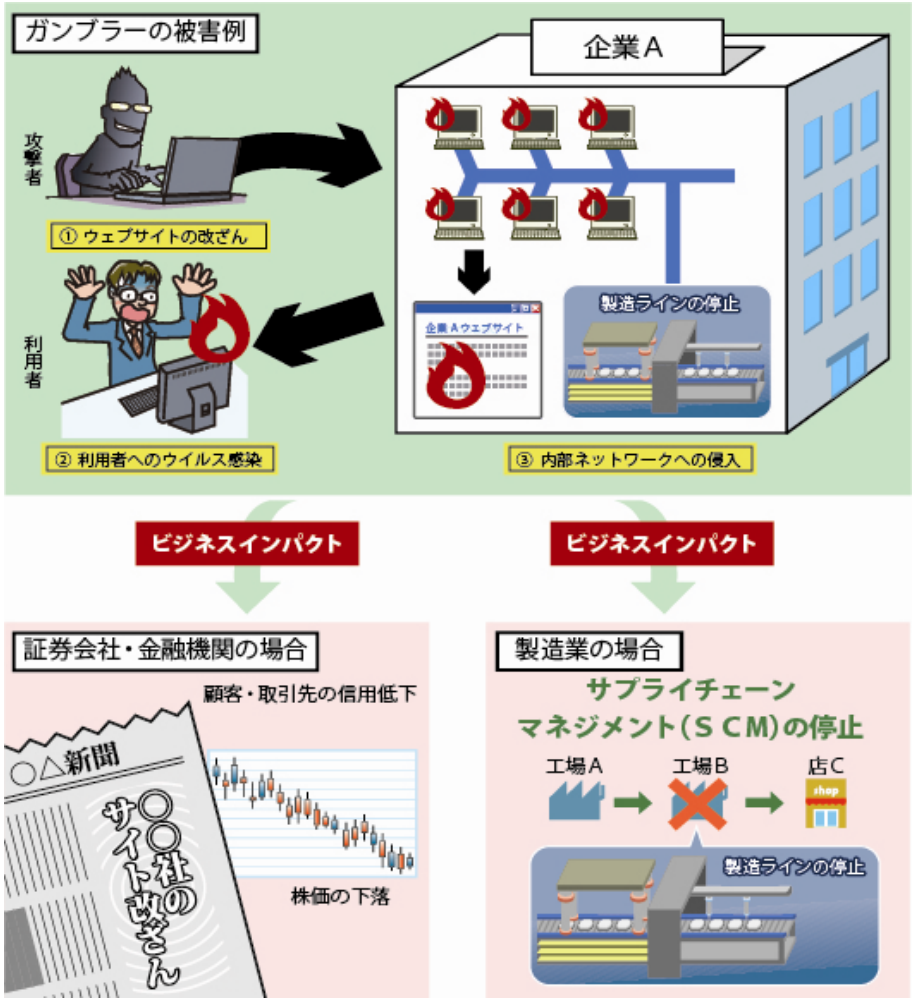
情報漏えいによる影響 [3]

■事例２　ウイルス感染が元で起きるウェブサイトの改ざん

クライアント PC における脆弱性対策の重要性

2009 年から 2010 年にかけては Gumblar（ガンブラー）と呼ばれる手口が猛威を振るいました。この手口では、ウェブサイト更新用の PC が、脆弱性を悪用するウイルスに感染することで、企業ウェブサイトの大きな被害につながります。FTP のログインアカウント情報が盗み出されて、閲覧者を不正なサイトへと誘導するように企業ウェブサイトが改ざんされたため被害は拡大しました。有名企業のサイトが次々と改ざんされた結果、企業自身が提供する本物のサイトでも信用できない状況にまで陥りました。

このように、組織が提供するウェブサイトが改ざんされると、組織の信用失墜や顧客離れにつながりかねません。1 台の PC に修正されていない脆弱性があったために、事業が脅かされることもあるのです。



Gumblar がもたらすビジネスインパクト [3]

■事例３　脆弱性によるクレジットカード情報漏えいの判例

セキュリティの要件や契約の重要性

不正アクセスを未然に防止することも重要ですが、万が一発生してしまった場合、その責任の所在をあらかじめ明確にし、自社の被害を最小限にすることも重要です。契約書にセキュリティ対策に関して記載していなかったため、セキュリティレベルの低いウェブサイトを構築した事業者へ損害賠償請求をおこなっても、請求できる額が減じられることがあります。

Ｃ社の通信販売用サイトがSQL インジェクションによる不正アクセスを受け、過去に利用した顧客のクレジットカード情報を含む個人情報が流出しました。Ｃ社は通信販売用サイトを構築したＤ社に対して、**個人情報漏えい対応や原因究明のための調査費用および売り上げの減少に対して約１億円の損害賠償請求**を行いました。

一審では、SQL インジェクション対策を講じていなかったこと、クレジットカード情報を暗号化せずデータベースへ保存していたことがＤ社の債務不履行かどうかが主要な争点となりました。技術水準として妥当なレベル[8]のSQL インジェクション対策を講じていなかったこと等はＤ社の重過失であり、損害額は約3200 万円とされました。情報の暗号化については契約書に明示されていなかったこと、また**Ｃ社の担当者がＤ社からの改修提案を受けたものの、対策せず放置したことからＣ社の過失（３割の過失相殺相当）**となりました。**Ｄ社は損害賠償としてＣ社の過失を相殺した約2300万円の支払いを命じられています。**（東京地判平成 26 年１月 23 日判時 2221 号 71 頁）

2.3. セキュリティ担当者に期待される役割

組織は、情報システムに起こりうるトラブルや影響を踏まえ、必要な脆弱性対策を実施する必要があります。もちろん、組織の情報システムにおいては、多くの場合、脆弱性対策が最優先課題ではないため、利用可能なリソースは限定的にならざるをえません。

したがって、組織のセキュリティ担当者（情報セキュリティ責任者、セキュリティ管理者）は、自組織に必要な脆弱性対策を無理のない形で適用するために、以下の役割を果たすことが期待されます。

■組織の情報セキュリティ責任者として

情報セキュリティ責任者は、組織としての観点から、脆弱性対策をどこまで

[8] 2008 年に IPA が公開した「大企業・中堅企業の情報システムのセキュリティ対策～脅威」

徹底すべきか適切に判断し、取り組みの方針を明確に示すことが求められます。その線引きは容易ではありませんが、従業員の負担を含む対策コストと想定される被害を勘案し、実現可能な方針を示す必要があります。たとえば、組織外になるべく迷惑をかけないように、組織の外とつながっているシステムや外部からの預かり情報、業務上重要なシステムの安全性を優先して脆弱性対策を行う方向が考えられます。

また、情報セキュリティ責任者は、組織としての取り組みの方針に基づき、必要な予算、人員、作業時間等のリソースを確保する役割を担います。

さらに、情報セキュリティ責任者は、必要に応じて、セキュリティ管理者と情報システムのオーナー部門の間の調整を求められることもあります。

■現場のセキュリティ管理者として

現場のセキュリティ管理者は、組織としての取り組み方針を踏まえ、現実的な対策を検討し、それを推進することが期待されます。

具体的には、まず、現状の把握を行う役割があります。ソフトウエアの新たな脆弱性が見つかると、攻撃者はそれを狙った攻撃ツールやコンピュータウイルスを作成します。したがって、現場のセキュリティ管理者は、自組織の情報システムがどのようなソフトウエアで構成されているか、それらの脆弱性が発見されていないか、明らかになった脆弱性について対策すべきか、そうした現状の把握を継続的に行いつつ、必要に応じて対策を実施すること、また対策を実施するよう情報システムのオーナー部門に働きかけることが求められます。

また、このような現状把握の結果から対策の方針を定め、情報セキュリティ責任者に的確に説明することが期待されます。さらに、従業員に対しては、脆弱性対策の必要性を理解できるよう、研修等にも工夫を行うべきでしょう。

3. 脆弱性対策のポイント

脆弱性対策は、情報システムのライフサイクルの様々な場面に適用することが望まれます。たとえば、システム構築時には、発注者としての要求事項の中に、既知の脆弱性の解消とテストを組み込むべきです。また、運用時に脆弱性の存在が発覚することもあります。脆弱性がもたらすリスクを的確に判断し、場合によってはシステムを停止しても対策を適用しなければなりません。

しかし、システムオーナーであるユーザ部門によっては、脆弱性の問題を充分に理解せず、組織として適切な対処がとられない可能性があります。セキュリティ担当者は、そのような状況において必要な脆弱性対策を実施するよう、適切に指導・対応する立場にあります。

以下に、システムの設計・開発段階、運用段階の各フェーズにおける脆弱性対策の考え方を紹介します。また、脆弱性の存在が判明した際の対処手順や、システム開発・構築、運用等における委託先との関係についても説明します。

3.1. 設計・開発・導入段階における対策実施

すでに運用を開始しているシステムにおいてセキュリティ上の問題が発覚した場合、システムの作り直しは困難なため、場あたり的な対策で済ませたり、リスクを容認せざるをえないこともあります。そうした事態を避けるため、設計・開発段階で脆弱性をできる限り解消しておく必要があります。

また、システム開発の予算や開発期間を抑制するため、既存のソフトウエア部品やサンプルプログラムを流用することがあります。そうした既存のプログラムに脆弱性が内在していた場合、最悪トラブルが生じて初めてその問題が発覚するということになりかねません。したがって、安全性が担保されていないサンプルプログラムの安易な流用は避け、参考元の確認やプログラム作成後のレビューなどのルールを設けるべきでしょう。

■ウェブサイトの場合

IPA が実施した実態調査 6 によると、インターネットに公開し、主に組織外とのやり取りに用いるウェブサイトについて、計画・設計から構築までの間に脆弱性の検査や修正などの対策を実施している組織は 5 割に満たない状況です。これは、公開ウェブサイトの構築において、デザインやコストが重視され、脆弱性対策に留意すべきことが認知されていないためと思われます。しかし、ウェブサイトは外部から攻撃を受けるリスクが高いことを踏まえれば、より手厚

い脆弱性対策を施すことが望まれます。

頻出する「作り込まれやすい」脆弱性は、設計・開発段階で未然に解消することが望まれます。特に、脆弱性届出[9]の上位を占めるクロスサイト・スクリプティング[10]や SQL インジェクション[11]の脆弱性は、プログラミングの際作り込んでしまうケースが大半であり、開発段階での確認・修正が不可欠です。したがって、セキュリティ担当者は、組織が用意する公開用のウェブサイトについて、

- 開発委託の要件に脆弱性対策を加えること
- 公開前に脆弱性を検査すること

を組織内のルールにするよう働きかけましょう。費用はかかりますが、脆弱性に起因するトラブルを避けるための必要経費と考えるべきです。

また、キャンペーンや調査等の目的で一時的に設置するウェブサイトの場合、管理体制やチェックが曖昧になりがちです。個人情報を取り扱う可能性が高いこと、一旦トラブルになれば組織の責任は免れないことから、安全性を担保する方策を講じておくことが重要です。

詳しくは「ウェブサイト運営者のための脆弱性対応ガイド」や「ウェブサイト構築事業者のための脆弱性対応ガイド」を参照してください。

■組織内システムの場合

グループウェアサーバ、ファイルサーバ、ディレクトリサーバ、バックアップサーバ等、イントラネット上に配置される組織内向けシステムの場合、外部ネットワークに直接つながっていないため、脆弱性に起因するトラブルが発生する可能性は低いと思われがちです。しかし、2.2 に示したとおり、約 3 割の組織が組織内向けシステムの脆弱性対策の遅れやミスが原因で被害を経験しています。これを考慮すれば、組織内システムの脆弱性を放置することはリスク管理上妥当とは言えません。そのシステムで扱う情報資産の重要性、サービスの継続性・信頼性に対する要求レベル、サービスの公開範囲などを踏まえ、重要なシステムについては脆弱性対策を適用すべきでしょう。たとえば、次のようなシステムについては、対策が必要と考えられます。

- 個人情報を扱うシステム

---

[9] https://www.ipa.go.jp/security/vuln/report/index.html

[10] Web サイトの掲示板などのプログラムを介して、悪意のあるコードがユーザのブラウザに送られてしまう脆弱性。

[11] 悪意あるリクエストにより、データベースの不正利用をまねく可能性がある脆弱性。データベースと連携したウェブアプリケーションの多くは、利用者からの入力情報を基にデータベースへの命令文を組み立てるが、命令文の組み立て方法に問題がある場合、攻撃によってデータベースの不正利用をまねく可能性がある。

・取引先や顧客等からの預かり情報を扱うシステム
（受発注、技術情報、顧客の内部情報等）
・業務上の重要情報を扱うシステム
（経営、人事、製品設計、研究開発、生産管理、知財等）

具体的には、既製のソフトウエアを用いる場合には既知の脆弱性について設計・開発段階で解消することが望まれます。納入前にソフトウエアの構成やパッチの適用状況について把握し、必要に応じて最新パッチの適用が必要です。また、システムを構成するソフトウエアとその脆弱性及び修正状況に関する情報は運用においても重要なので、適切に管理し継続的に把握するようにしてください。独自のソフトウエアを用いて構築されるシステムの場合には、ウェブサイトの脆弱性と同様に、プログラミング段階で作り込んでしまいやすい脆弱性を設計・開発段階で未然に解消することが大切です。

■クライアント PC の場合

IPA が実施した実態調査 6 によると、従業員のクライアント PC を導入する際に、ソフトウエアの脆弱性の検査や修正などの対策を「特にしていない」と回答した組織は 23.5%にもなります。「インターネットにはファイアウォールを介してつながっているので安全である」との判断があるかもしれませんが、近年、そのような従来の防御策を迂回して直接的に PC ユーザを狙う攻撃（偽サイトへの誘導、標的型攻撃 [12]、USB 経由のウイルス感染等）が急増している点を考慮すれば、そうした過信が危険なことは明らかです。

クライアント PC のセキュリティ確保のためには、脆弱性の修正（パッチの適用）がとても重要です。未対策の脆弱性はトラブルの根本的な原因となり、重大な問題を引き起こしうるものです。セキュリティ担当者、委託先、エンドユーザの誰が脆弱性対策を施すかは組織の規模や体制、予算等によって異なりますが、クライアント PC は導入時にできる限り必要なパッチの適用を済ませておくことをお薦めします。

また、OS、アプリケーション、プラグイン等のソフトウエアは長期にわたり使い続けることになりますが、古い製品には多数の脆弱性修正を施す必要があるだけでなく、サポートの期限が切れた場合には脆弱性が発見されてもパッチが提供されない事態にもなり得ます。導入時にソフトウエアをいつまで使い続けるかを計画し、サポートが途絶える前に円滑に新たなソフトウエアに移行することもトラブルを未然に防ぐ脆弱性対策のひとつです。

---

[12] 特定の組織や個人を対象とする攻撃。情報窃取を目的として特定の組織に送られる不審メールなどがある。

3.2. 運用段階における対策実施

ソフトウエア製品の脆弱性は突然公表されることがあります。新たな脆弱性が発見されれば、日を置かずにそれを狙う攻撃ツールやコンピュータウイルスが作られ流布されます。新たな脆弱性が自組織の情報システムの中にある場合には、その脆弱性を速やかに改修する必要があります。

したがって、情報システムの運用段階においては、脆弱性対策に継続して取り組むことが求められます。

■組織のソフトウエア構成や変更の状況を管理すること

公表された脆弱性が自組織に影響するかどうかを判断するためには、自組織における情報システムのソフトウエア構成（ソフトウエアの種類、バージョン等）や変更履歴（パッチの適用等）を日頃から把握しておくことが大切です。これによって、新たに明らかになった脆弱性の情報を得て迅速な対応を始めることができます。

ソフトウエア構成や変更の状況を管理するためには、たとえば、情報システム導入に際し、導入部門が必要なデータを登録するルールやしくみを整備する必要があります。また、管理を支援するツールも活用可能です。たとえば、IPAでは利用しているソフトウエア製品のバージョン確認を支援する「MyJVN バージョンチェッカ」を無料提供しています。

ただし、組織の規模が大きくなると、管理を徹底することが難しくなる場合もあります。また、組織内のシステムの中には、組織変更や異動、移転等により、構成を把握している担当者がいなくなって管理が曖昧になった機器があるかもしれません。そうしたシステムの脆弱性が放置され、トラブルの原因となることがあります。2003 年に猛威をふるったコンピュータワーム「Blaster」は、放置されたシステムの脆弱性対策が遅れたため、被害が拡大しました。

このような問題の解決策として、統合管理ツールを活用して、機器に搭載されているソフトウエアの種類とバージョン、パッチの適用状況等を集中管理する方法があります。

なお、運用時に不要になったサービスは停止するなど、セキュリティを考慮した設定変更も重要です。

また、情報システムのライフサイクルを意識することは重要です。古い OS やアプリケーションは新しい攻撃への耐性に乏しいものです。リスクが徐々に高まることを考慮して導入当初から計画を立てておき、適正な時期がきたら次バージョンへの切り替えを進めることが望まれます。アプリケーションの動作

環境を維持する必要がある場合には、仮想マシン上に動作環境を移行することも選択肢の一つです。

■脆弱性情報を収集すること

脆弱性情報を収集し、自組織のシステムに影響しうる脆弱性については対応を検討します。脆弱性情報は一部の例外を除き、製品開発者から予告なく突然公表されますから、常に情報収集を心がける必要があります。情報源としては、製品開発者がホームページ等に示す製品利用者向け情報、セキュリティ製品・サービスのベンダや情報セキュリティ関連機関がホームページやメール等で提供する脆弱性関連情報のアドバイザリ[13]などが挙げられます。

こうした情報収集はユーザ部門では難しいため、セキュリティ担当者が実施し、必要に応じて組織内に提供することが望まれます。スタッフが足りず、網羅的な常時収集が難しい場合であっても、特に業務に影響が大きいソフトウエアに対象を絞り込んで、何名かで分担し定期的な確認に取り組むべきです。ソフトウエア構成に基づいて収集する範囲を絞り込み、効率的な情報収集を行うことも有効です。たとえば、IPA では「MyJVN 脆弱性対策情報収集ツール[14]」を無料提供しています。これは、いくつかの情報を登録するだけで、自分に関係する脆弱性対策情報を自動的に収集・表示するツールです。なお、運用管理を外部に委託している場合には、脆弱性情報の収集を委託業務に含めるよう調整することも可能でしょう。

また、自組織が公開するウェブサイト等について脆弱性があるという連絡を組織外から受けることがあります。その場合は放置せずに、連絡を受けた内容と実態を確認して、対処について適切な判断を示すべきです。業務継続の必要性や改修の難度から、対策実施を先延ばしにする判断もありますが、それによってウェブサイト等にアクセスしたウェブサイト利用者が影響を受けるリスクも高まることを熟慮し、適切に対処することが望まれます。

■脆弱性検査を行うこと

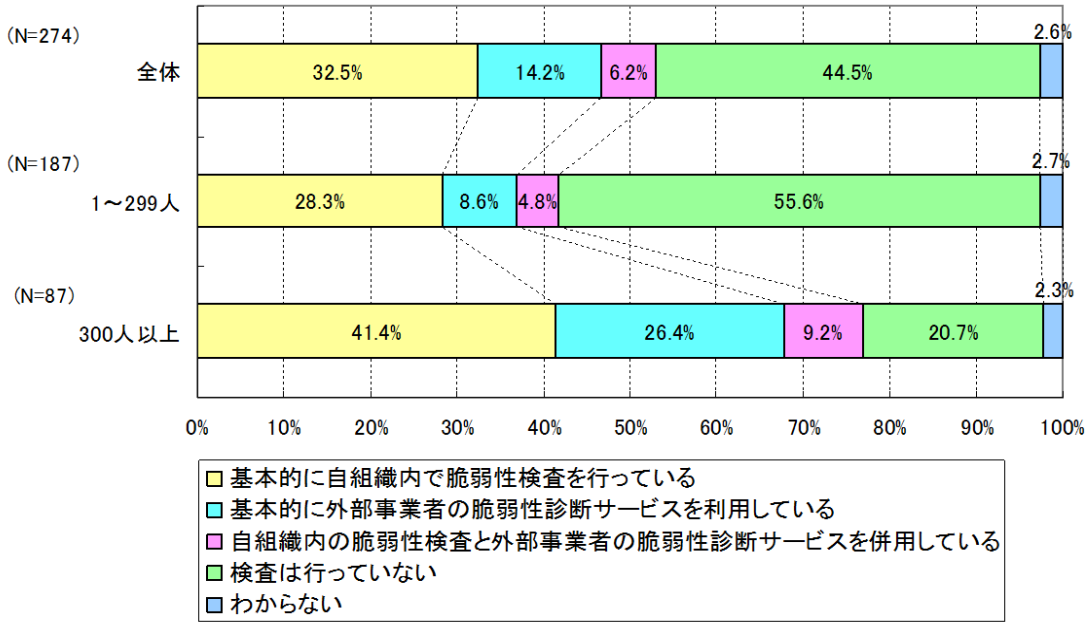
公開用ウェブサイトは、組織内のスタッフもしくは外部の事業者に委託して、脆弱性検査を行うようルール化することをお薦めします。予算等の制約で定期的な実施が難しい場合には、構築・改変時に実施する形でも有効です。

IPA が実施した実態調査 6 でも、全体で５割超、大企業等では約８割が運用中のウェブサイトの脆弱性検査を実施しており、２ 割の組織が検査を通じて脆

[13] 脆弱性対策情報ポータルサイト JVN（ https://jvn.jp/ ）、脆弱性対策情報データベース JVN iPedia（ http://jvndb.jvn.jp/ ）など

[14] 脆弱性対策情報共有フレームワーク MyJVN（ http://jvndb.jvn.jp/apis/myjvn/ ）

弱性に気づいた経験を有することが報告されています。



ウェブサイト脆弱性検査・診断サービスの利用状況

■修正プログラム（パッチ）を適用すること

脆弱性が自組織の情報システムのソフトウエアに存在していると判明した場合、対策を適用すべきか否かを判断する必要があります。専門的な知識が必要なため、セキュリティ担当者が判断を行ないます。その際、セキュリティ製品・サービスのベンダが示す脅威レベルの評価やソフトウエア製品開発者の提供する脅威及び修正適用に伴う影響の情報等が参考になります。また、外部の事業者に運用を委託している場合は、相談することも有効です。

また、最終的にはシステムのオーナー部門の合意が不可欠となります。対処を円滑に進めるために、組織内の合意形成を含む対処手順を定め、文書化しておくことが重要です。

たとえ外部と接続していないネットワークシステムの場合でも、内部にウイルスを持ち込まれる可能性も踏まえて、対策の要否を検討すべきです。

パッチの適用にあたっては、可能な限り事前にテストを行い、運用に支障がないことを確認した上で改修に着手することが望まれます。また、クライアント PC など、台数が多く手作業でのパッチ適用に手間がかかる場合は、統合管理ツールを活用すれば作業の自動化が可能です。

最近増えている、未公表の脆弱性を悪用する「ゼロデイ攻撃」については、

パッチが提供されるまでの間は一時的な対策として IPS（侵入防御システム）で攻撃を抑止し、提供され次第パッチを適用するという対処が可能です。

3.3. 脆弱性の存在が判明した際の対処手順

脆弱性の存在が明らかになった場合、セキュリティ担当者は以下の作業を行ないます。場合によっては、外部の委託先と連携した取り組みも可能です。

①セキュリティ上の問題の有無に関する調査

入手した脆弱性情報について、組織内の情報システム上の脆弱性の有無や問題が発生する条件等を調査します。

②影響と対策の方向性の検討

問題箇所が及ぼす影響を明確にして、修正方法や回避方法を検討します。

③対策作業計画の策定

対策作業を進める手順や期間等について計画を策定します。費用、人員等を勘案しつつ、代替機でのテスト、対策実施に伴うサービスの停止と再開等を計画します。代替機を用意できない場合、ソフトウエアの仮想環境の利用などで、比較的低予算でテストを行うことが可能です。

④対策の実施

作業計画に基づき対策を実施します。

なお、ウェブサイトの脆弱性については、脆弱性検査で発見される場合だけでなく、外部から連絡を受けて知らされる場合や、実際に問題が発生する場合も想定されます。

■第三者から指摘された場合

第三者から脆弱性の存在を指摘された際には、通知者を含む関係者間で良いコミュニケーションを維持することが対応を成功させる鍵となります。

脆弱性の通知は、IPA から連絡を受ける場合と、発見者から直接連絡を受ける場合の 2 つがあります。いずれの場合についても、連絡を受ける部署（問い合わせ窓口等）には、通知を受け取った旨の返信を速やかに行うよう説明してください。

・IPA から連絡を受ける場合の対応

ウェブサイトに関する脆弱性関連情報が発見者から IPA に届出られた際

には、IPA からウェブサイト運営者に通知を行います。IPA からの通知は主に電子メール（vuln-contact@ipa.go.jp）を利用して行われます。

・発見者から直接連絡を受ける場合の対応

発見者が IPA を介さずに脆弱性情報を直接ウェブサイト運営者に通知してくることもあります。この場合は、発見者との誠実な対話に努めるようしてください。

■トラブルが発生している場合

ウェブサイトにおけるセキュリティ上のトラブルに対しては、発見後の迅速な対応が必要です。特に、外部に悪影響を及ぼす状態にある（不正アクセスの踏み台にされている、フィッシング詐欺等に悪用されている、ウイルスを撒き散らしている等）場合には、まずウェブサイトを停止し被害の拡大を防ぎます。また、個人情報の漏洩やウェブサイト利用者へのウイルスの配布等が発生した場合には、速やかな被害事実の確認と公表、主務官庁等への報告も望まれます。

応急措置的な対策としては、WAF（ウェブ・アプリケーション・ファイアウォール）を用いて攻撃を凌ぐことも可能です。より恒久的な対策としては、ウイルス等の駆除や監視強化等の処置だけでなく、ウェブサイトの脆弱性が原因で侵害された可能性を考慮し、丁寧な調査を行って「入口にされた穴を見つけて塞ぐ」ことや「不正に開けられた裏口を探して閉じる」ことが重要です。手当てが不十分なままサービスを継続／再開すればトラブルを再発する可能性もあります。調査や脆弱性修正には十分な作業時間を取る必要があります。場合によっては作業のためにサービスを一時的に停止するといった決断も必要です。

セキュリティ担当者は、組織のリスク管理担当者や当該システムのオーナー部門、外部の専門事業者等と調整し、被害事実の公表やサービス再開のタイミングを考慮しながら、対策実施を主導する必要があります。

3.4. 委託について

脆弱性対策を含む情報システムの設計・開発、運用のセキュリティ管理に関する人的資源が充分でない場合、適切なスキルを有する事業者に委託することも有効です。ただし、曖昧な取り決めや不十分な合意形成が原因となって、問題化する可能性もあります。

■契約時に合意すべき事項

契約時には、以下のような脆弱性対策の取扱いについて、委託先と合意を取り付けることが望まれます。セキュリティ担当者は契約主体である情報システムのオーナー部門を支援し、合意形成を推進します。

- **納入後に公表された新規の脆弱性対策**

  ソフトウエア製品の脆弱性のうち、納入後に公表されたものについては、対策は有償と捉え、システム開発とは別の保守契約で対応することが適切と考えられます。

- **既知の重要な脆弱性対策**

  ソフトウエア製品の既知の重要な脆弱性やウェブサイトの著名な脆弱性の対策に関する著しい認識不足、ウェブサイトに対する設定ミスなど、委託先の責に帰する場合は無償とすべきです。

- **脆弱性検査の実施の有無**

  稼動中のウェブサイトに対し（もし可能であるならば納入前に）脆弱性検査を行い、脆弱性が見つかった場合にはその対策を施すことを契約に含めるべきです。引渡し段階ではウェブサイトが稼動していない場合も多いため、検査を計画的に実施するための配慮も必要です。

- **緊急事態時の費用負担**

  緊急事態の際は迅速な対策を要求されるため、組織と委託先との間で作業範囲、費用負担について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ます。契約の段階で明確にしておくべきですが、それが難しい場合にも、極力、覚書として残しておくことが望ましいと考えられます。

詳しくは経済産業省「アウトソーシングに関する情報セキュリティ対策ガイダンス」[15]を参照してください。

4. 参考資料

4.1. 情報セキュリティ早期警戒パートナーシップ

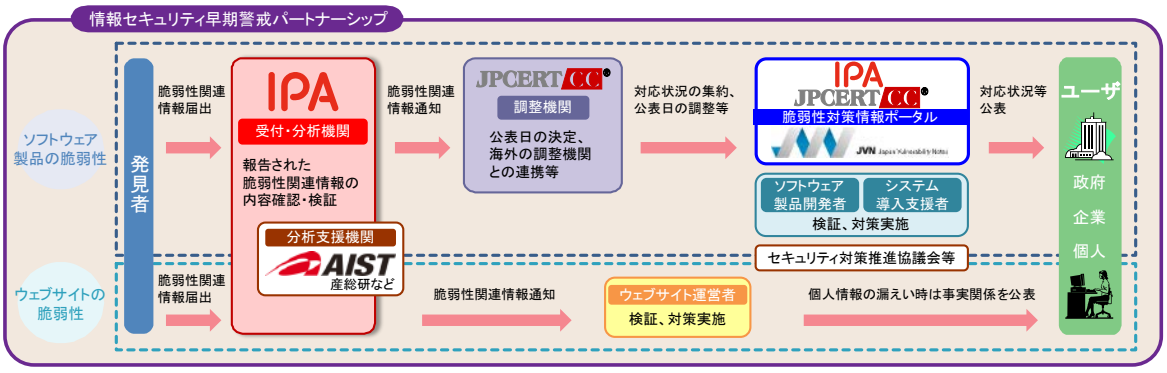
独立行政法人情報処理推進機構（IPA）では、経済産業省告示を踏まえ、2004年７月からソフトウエア製品及およびウェブアプリケーションの脆弱性に関する届出を受け付けています[16]。

（参考）

「ソフトウエア製品等の脆弱性関連情報に関する取扱規程[17]」（平成29年経済産業省告示第19号）」

「受付機関及び調整機関を定める告示（平成29年経済産業省告示第２０号）」

IPA では、ウェブサイトの脆弱性に関する届出を受け付けた場合、当該ウェブサイトの運営者にその旨を連絡し、脆弱性対策の実施を促します。



情報セキュリティ早期警戒パートナーシップのしくみ

15 http://www.meti.go.jp/policy/netsecurity/docs/secgov/2009_OutsourcingJohoSecurityTaisakuGuidance.pdf

16 https://www.ipa.go.jp/security/vuln/index.html

17 http://www.meti.go.jp/policy/netsecurity/index.html

4.2. 参考 URL

- 「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」（独立行政法人情報処理推進機構，一般社団法人 JPCERT コーディネーションセンター 他）
  https://www.ipa.go.jp/security/ciadr/partnership_guide.html
- 「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」（一般社団法人 情報サービス産業協会、一般社団法人 電子情報技術産業協会）
  https://www.ipa.go.jp/files/000002992.pdf
- パンフレット「情報システムを安全にお使いいただくために」（独立行政法人情報処理推進機構，一般社団法人 JPCERT コーディネーションセンター 他）
  https://www.ipa.go.jp/files/000011590.pdf
- 「ウェブサイト構築事業者のための脆弱性対応ガイド」（独立行政法人情報処理推進機構，一般社団法人 JPCERT コーディネーションセンター 他）
  https://www.ipa.go.jp/security/ciadr/vuln_sier_guide.pdf
- 「ウェブサイト運営者のための脆弱性対応ガイド」（独立行政法人情報処理推進機構，一般社団法人 JPCERT コーディネーションセンター 他）
  https://www.ipa.go.jp/security/ciadr/vuln_website_guide.pdf
- 「安全なウェブサイトの作り方」
  https://www.ipa.go.jp/security/vuln/websecurity.html
- 「知っていますか？脆弱性(ぜいじゃくせい)」
  https://www.ipa.go.jp/security/vuln/vuln_contents/
- 脆弱性対策情報ポータルサイト「JVN」 https://jvn.jp/
- 脆弱性対策情報データベース「JVN iPedia」 http://jvndb.jvn.jp/
- 脆弱性対策情報収集ツール「My JVN 脆弱性収集ツール」
  http://jvndb.jvn.jp/apis/myjvn/mjcheck.html
- ソフトウェア製品のバージョン確認「My JVN バージョンチェッカ」
  http://jvndb.jvn.jp/apis/myjvn/vccheck.html
  http://jvndb.jvn.jp/apis/myjvn/vccheckdotnet.html (for .NET)
- ウェブサイトの攻撃兆候検出ツール「iLogScanner」
  https://www.ipa.go.jp/security/vuln/iLogScanner/index.html
- 「アウトソーシングに関する情報セキュリティ対策ガイダンス」（経済産業省）
  http://www.meti.go.jp/policy/netsecurity/docs/secgov/2009_OutsourcingJohoSecurityTaisakuGuidance.pdf

・本資料の位置づけ

近年、日本国内においてソフトウエアやウェブアプリケーションの脆弱性が発見されることが増えており、これらの脆弱性を悪用した不正アクセス行為やコンピュータウイルスの増加により、企業活動が停止したり情報資産が滅失したり個人情報が漏洩したりといった、重大な被害が生じています。

そこで、脆弱性関連情報が発見された場合に、それらをどのように取り扱うべきかを示した経済産業省告示が制定されました。この告示をふまえ、関係者に推奨する行為をとりまとめた「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」が公表されています。

（参考）

「ソフトウエア製品等の脆弱性関連情報に関する取扱規程」（平成 29 年経済産業省告示第 19 号）」

「受付機関及び調整機関を定める告示（平成 29 年経済産業省告示第 20 号）」

本資料は、このガイドラインを補足するために、主に企業情報システムのセキュリティ対策における活用を想定して、脆弱性がもたらすトラブル、脆弱性対策が不可欠であること、セキュリティ担当者による脆弱性対応のポイントなどを解説しています。

関係者の方々は、脆弱性対応に向けた体制の検討や、実際の対応に際し、本資料を参考にご対応くださいますようお願い申し上げます。

なお、本資料の配布に制限はありません。

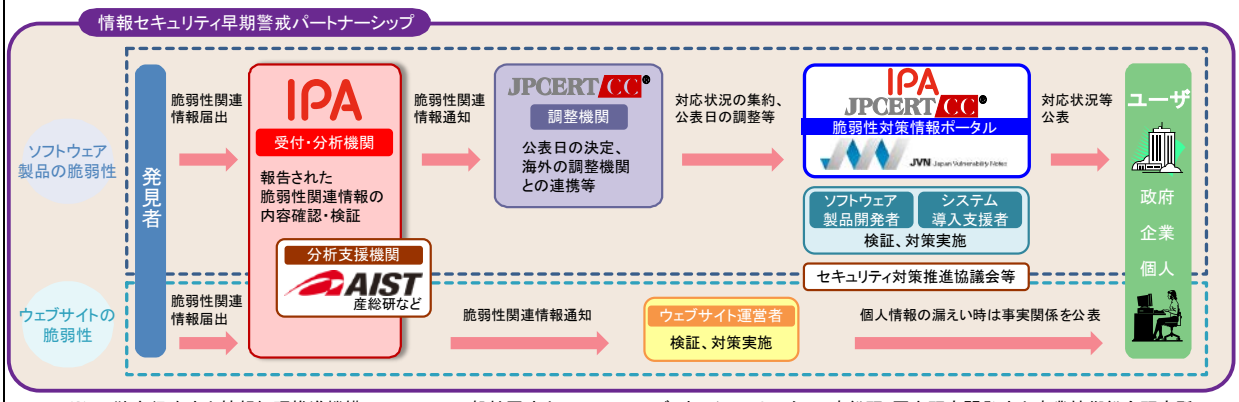
・本資料の読者層

本資料は主に以下の方の利用を想定しています。

・企業等の情報システム部門もしくは情報セキュリティ部門等の責任者の方

・企業等の情報セキュリティ管理者の方

・「情報セキュリティ早期警戒パートナーシップ」



※IPA:独立行政法人情報処理推進機構, JPCERT/CC:一般社団法人　JPCERTコーディネーションセンター、産総研:国立研究開発法人産業技術総合研究所

・本資料に関するお問合わせ先

独立行政法人情報処理推進機構（略称:IPA）　技術本部　セキュリティセンター

〒113-6591　東京都文京区本駒込二丁目 28 番 8 号　文京グリーンコートセンターオフィス 16 階

https://www.ipa.go.jp/security/　TEL: 03-5978-7527　FAX: 03-5978-7552

セキュリティ担当者のための脆弱性対応ガイド

ー 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ー

２０１１年　２月２８日　初版発行

２０１１年　３月２８日　第２版発行

２０１５年　３月２６日　第３版発行

２０１７年　３月３０日　第３版第２刷発行

［著作・制作］　情報システム等の脆弱性情報の取扱いに関する研究会

［事務局・発行］　独立行政法人情報処理推進機構