地方公共団体のための脆弱性（ぜいじゃくせい）対応ガイド

～　情報システムを安全に使い続けるために　～

2017年3月　第2版

独立行政法人**情報処理推進機構**

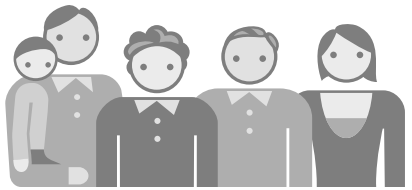
『脆弱性』（ぜいじゃくせい）について、ご存知ですか？

- 本資料は、地方公共団体の皆様が、情報システム(住民向けITサービス、公開系)を安全に使い続けるために避けて通れない「脆弱性対策」についてご紹介する目的で作成しました。

- 脆弱性は、情報セキュリティ上の「弱点」「ほころび」です。情報システムに脆弱性があると攻撃が容易になり、情報流出やシステムの改ざん、停止などの事態が起こることもあります。（参考.1.参照）

- 本資料は、次の内容で構成されています。
  - 情報システムを安全に使い続けるために理解すべきことについて
  - 調査結果に基づく組織的な対応について
  - 脆弱性が見つかったときの対応について

- 本資料は、次の方にお読みいただくことを想定しています。
  - 地方公共団体の幹部の皆様
  - 情報システムを保有する各担当課の皆様
  - IT担当課の皆様



目次

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

1.2. 脆弱性に起因する影響の例

1.1. 情報システムと脆弱性

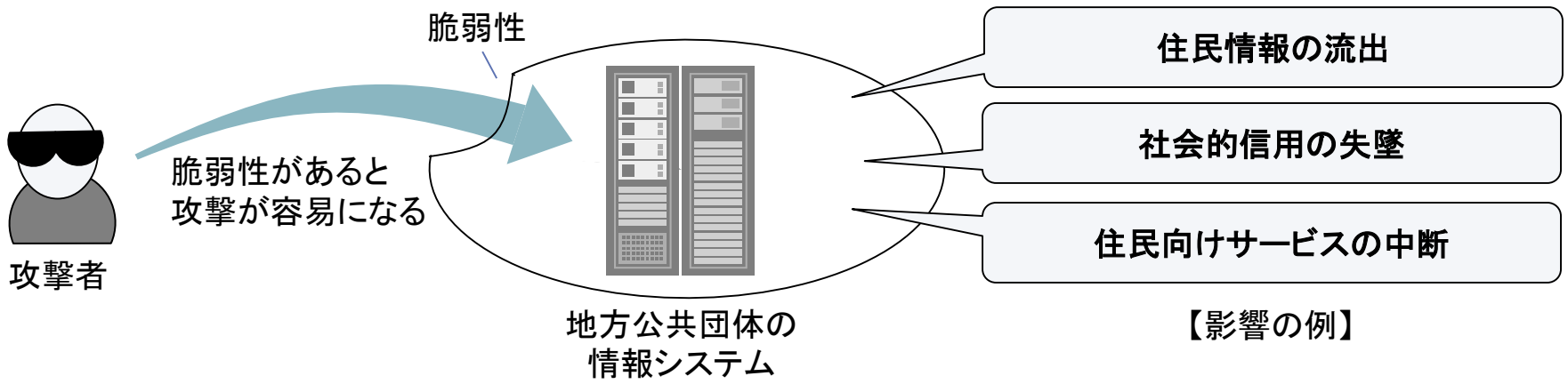
- 今や、住民向けサービスの基盤として、情報システムの利用は欠かすことができません。

- ただし、情報システムは、「動いているから大丈夫」なように見えても、時間が経つとその安全性は低下します。

- 情報システムを安全に保ち、安全な住民向けサービスを維持するためには、脆弱性（参考.1.参照）への対策が重要になります。
  - 脆弱性とは、情報セキュリティ上の「弱点」「ほころび」です。
  - 脆弱性は、情報システムの開発から時間がたてばたつほど発見されやすくなります。
  - 脆弱性対策を誤ると、市民の信頼を失う結果になってしまいます。

1.2. 脆弱性に起因する影響の例

- 脆弱性対策を怠ると、攻撃が容易になり、地方公共団体や住民に様々な影響を及ぼす可能性があります。
  - 事例1：大手メーカの子会社が運営していたウェブサイトが侵入され、氏名やパスワード情報など約1億件の個人情報が外部に流出しました。サーバの脆弱性を悪用したと見られ、対応に係る費用は1年で約140億円と試算されています。
  - 事例2：複数の自治体のサーバ上にフィッシング詐欺サイトが設置されていました。ウェブサイトを構築するコンテンツ管理システムの脆弱性を悪用されました。このような場合、悪用されたサイトの運営者は厳しく非難され、社会的信用を失うこともあります。
  - 事例3：自治体の公共施設予約システムが脆弱性を攻撃され不正アクセスを受けた結果、システムを停止しました。このように、脆弱性が狙われると、住民向けサービスを中断する事態になりかねません。



2.調査結果※に基づく組織的な対応

2.1. 幹部の方へ

2.2. 情報システムを保有する各担当課の方へ

2.3. IT担当課の方へ

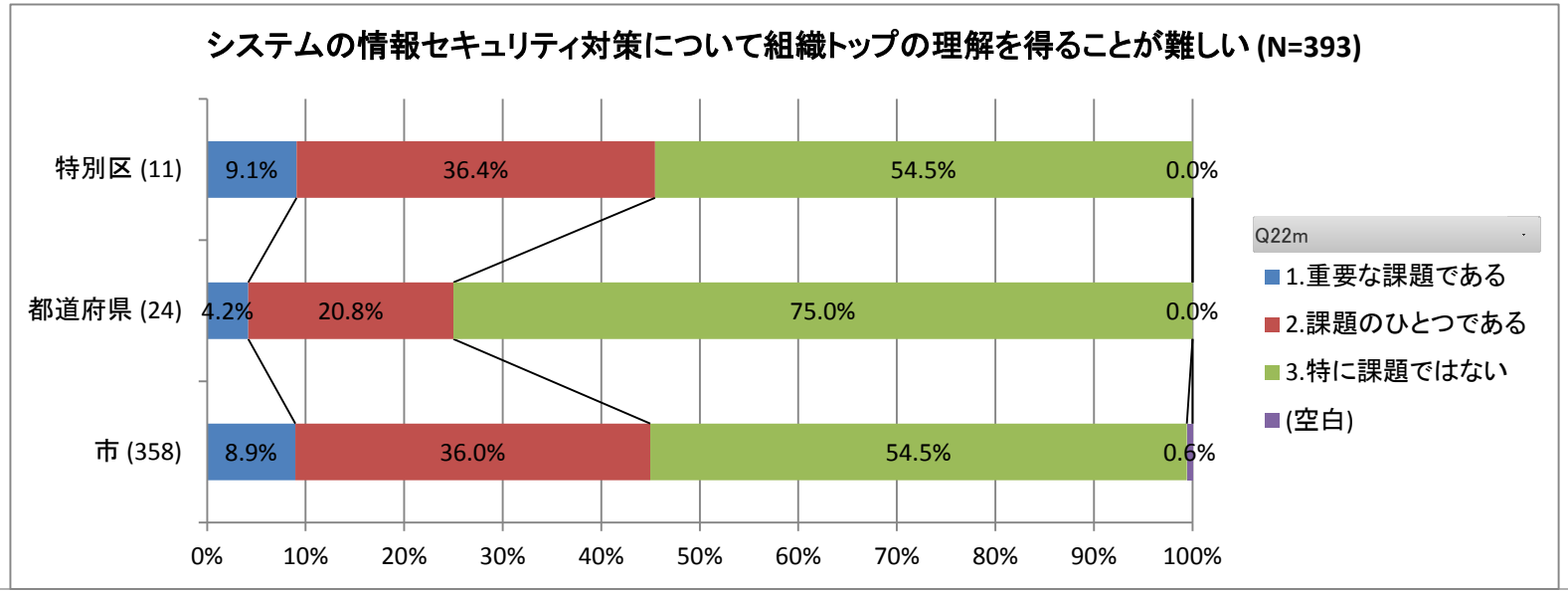
※地方公共団体における脆弱性対策の実態に関する調査
［調査主体］情報処理推進機構(IPA)
［調査協力］地方自治情報センター（LASDEC）
［調査概要］地方公共団体を対象とするアンケート調査を実施し、脆弱性対策の実態や公表のあり方に関する考え方や問題点を調査した。また、地方公共団体関係者から脆弱性対策及びパートナーシップに関する理解を促すための方策についてヒアリング調査を行った。
［調査時期］平成23年9月～12月
［調査対象］
アンケート：地方公共団体（情報セキュリティ部署）47都道府県、23特別区、786市 、有効回収数399件 (47.6%)
ヒアリング：地方公共団体（情報セキュリティ部署） 2県、1特別区、5市

2.1. 幹部の方へ

- 情報システムの安全性は、時とともに低下します。
  - 安全性を維持するためには、脆弱性の検査や、脆弱性への対応が必要になります。
  - 脆弱性への対応を怠って問題が発生すると、住民からの信頼を失うリスクがあります。

- 脆弱性は突然見つかることがあり、突発的な対応が要求される場合があります。
  予算や人的資源等の柔軟な組み換えが必要となることをご理解ください。

（ご参考）市や特別区の4割程度は、『システムの情報セキュリティ対策について組織トップの理解を得ることが難しい』ことを課題としてとらえています。（括弧内の数字は件数）

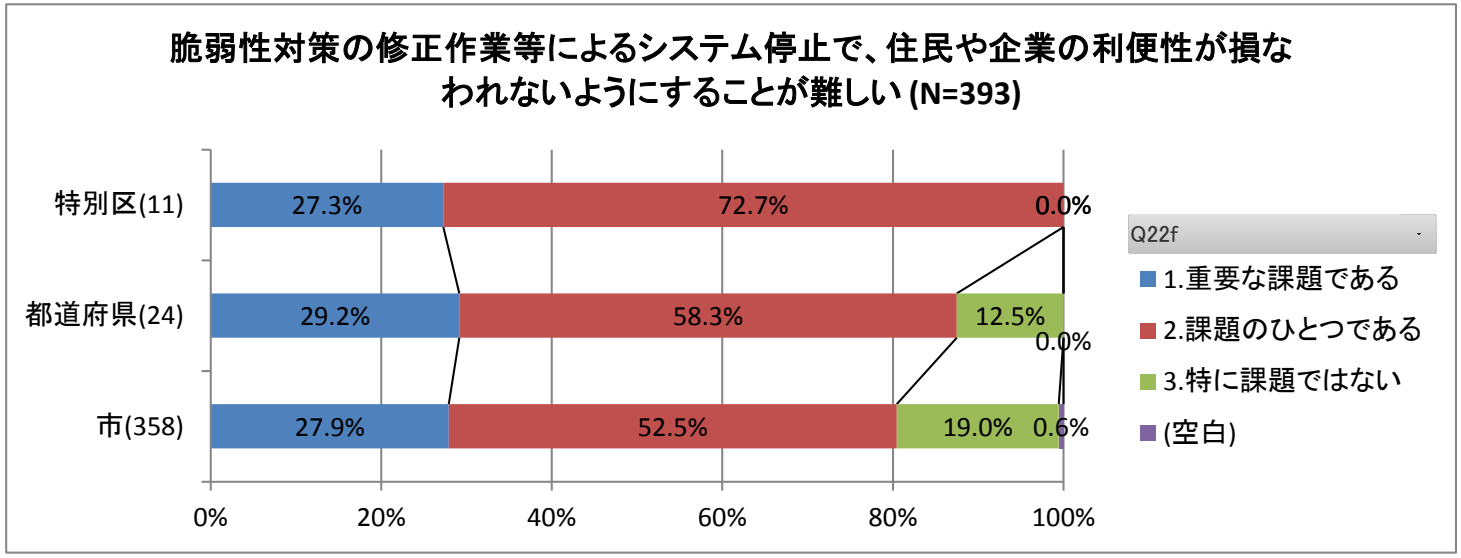


IPA「地方公共団体における脆弱性対策の実態に関する調査 アンケート」結果より

2.2. 情報システムを保有する各担当課の方へ（原課の方へ）

- 脆弱性対策を怠って、保有する情報システムに問題が発生した際の対処は、各担当課が担うことになります。
  - 情報システムの安全性は時間が経つと低下するので、脆弱性検査等の継続的な対策が必要です。
  - 脆弱性対策のためシステムを停止することがありますが、住民向けサービスには、代替システムを用いてでも維持すべきケースがあります。
- 委託業者との契約時の調整をはじめとして、IT担当課の情報提供・支援を受けると脆弱性対策における問題を回避しやすくなります。

（ご参考）特別区、都道府県、市のいずれも、『脆弱性対策の修正作業等によるシステム停止で、住民や企業の利便性が損なわれないようにすることが難しい』ことを課題ととらえる割合が大半を占めています。



IPA「地方公共団体における脆弱性対策の実態に関する調査 アンケート」結果より

2.3. IT担当課の方へ（情報政策課の方へ）

- 脆弱性対策は、開発・運用事業者に一任することで解決するわけではありません。
  - 開発・運用を委託する業者との間の、曖昧な取り決めや不十分な合意形成が原因となって、問題となる場合もあります。
  - 脆弱性対策について契約時に合意すべき事項として、次の例が挙げられます*。

開発の契約で合意することが望ましい事項の例

- 開発時の段階で見つけた既知の重要な脆弱性の対策は契約の範囲に含まれるように調整する。
- 納入前のウェブサイトに対し脆弱性検査を行い、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方向で調整する。
- 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、設定ミスなど開発事業者の責に帰する場合は無償とする方向で調整する。

保守・運用の契約で合意することが望ましい事項の例

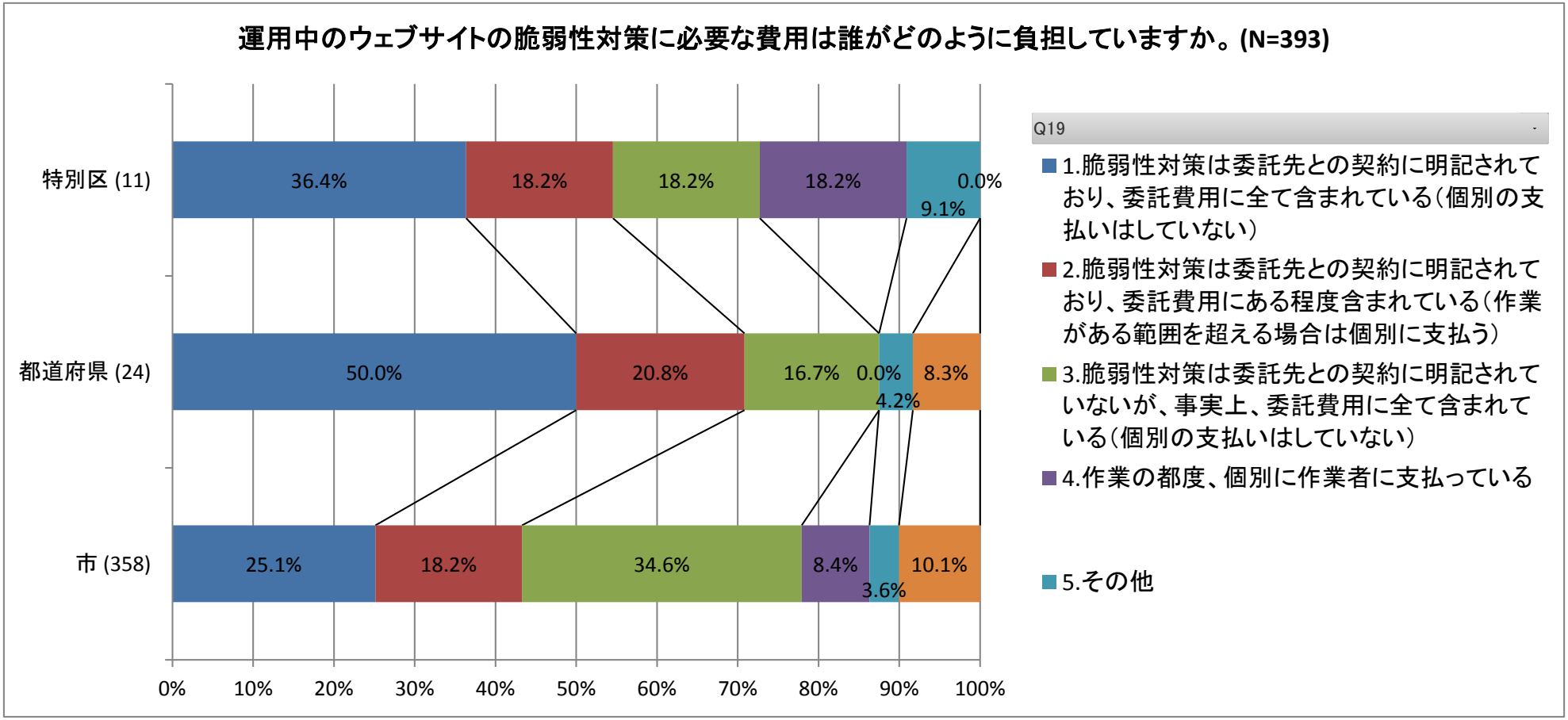
- 保守フェーズの新規脆弱性への対策は保守契約で対応する。
  （例）「乙は、対象アプリケーションの潜在的な障害を、顕在化する前に発見した場合、当該障害の是正を行うための修正を実施する。」
- 当該情報システムに関する深刻な脆弱性の情報が公開されたら連絡してもらう方向で調整する。
- 緊急事態時に発生する調査費用・対策費用の負担については、契約の段階で明確にしておく。

- 必要に応じて庁内の調達ガイドラインを策定し、各担当課に提供することが望まれます。

(*) IPA「情報システム等の脆弱性情報の取扱いに関する研究会」関連資料、
経済産業省「「情報システムの信頼性向上のための取引慣行・契約に関する研究会」情報システム・モデル取引・契約書（第一版）、
社団法人情報サービス産業協会「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」等を基に構成

2.3. IT担当課の方へ(情報政策課の方へ)

- （ご参考）運用中のウェブサイトの脆弱性対策に必要な費用負担について、『契約に明記されていないが、事実上、委託費用にすべて含まれている』との回答が、特別区で18.2%、都道府県で16.7%、市では34.6%を占めています。
- 責任の所在が不明瞭だと、修正が必要な際や、事故が起きた際に対応が難しくなります。

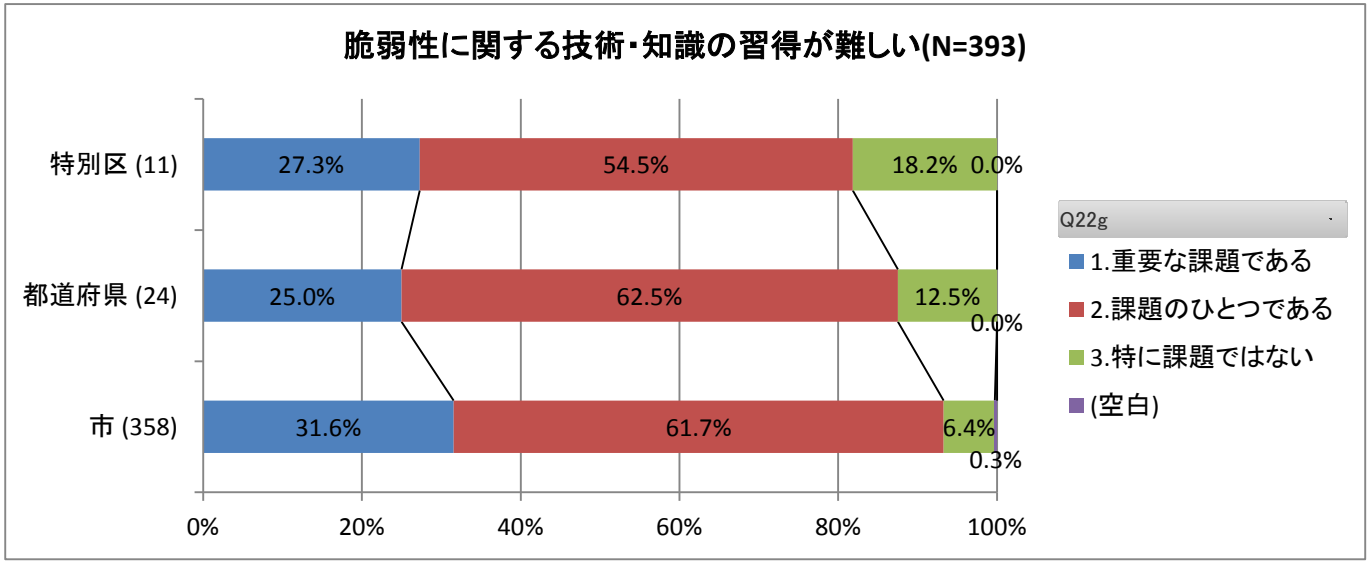


 IPA「地方公共団体における脆弱性対策の実態に関する調査 アンケート」結果より

2.3. IT担当課の方へ(情報政策課の方へ)

- 脆弱性対策を進める上で、担当者の人事ローテーションは地方公共団体の共通の悩みです。
  - ITやシステムを理解できる人材の育成に時間がかかる
  - システムの管理レベルが属人化してしまう
  - 委託業者に依存してしまう
- 基準や手順をガイドラインにまとめるなどして、経験・知見を共有している地方公共団体では、人事ローテーションがあっても脆弱性対策はうまく機能しています。
- また、脆弱性対策を円滑に実施するためには、情報システムを保有する各担当課とIT担当課との間の連携・情報共有が重要となります。

(ご参考)『脆弱性に関する技術知識の習得が難しい』ことを課題ととらえる割合は、特別区で8割超、都道府県や市では9割前後を占めています。



IPA「地方公共団体における脆弱性対策の実態に関する調査 アンケート」結果より

3.脆弱性が見つかったら

3.1.発見時の対応
3.2.脆弱性情報の取り扱いの問題点
3.3.脆弱性情報の取り扱いの事例

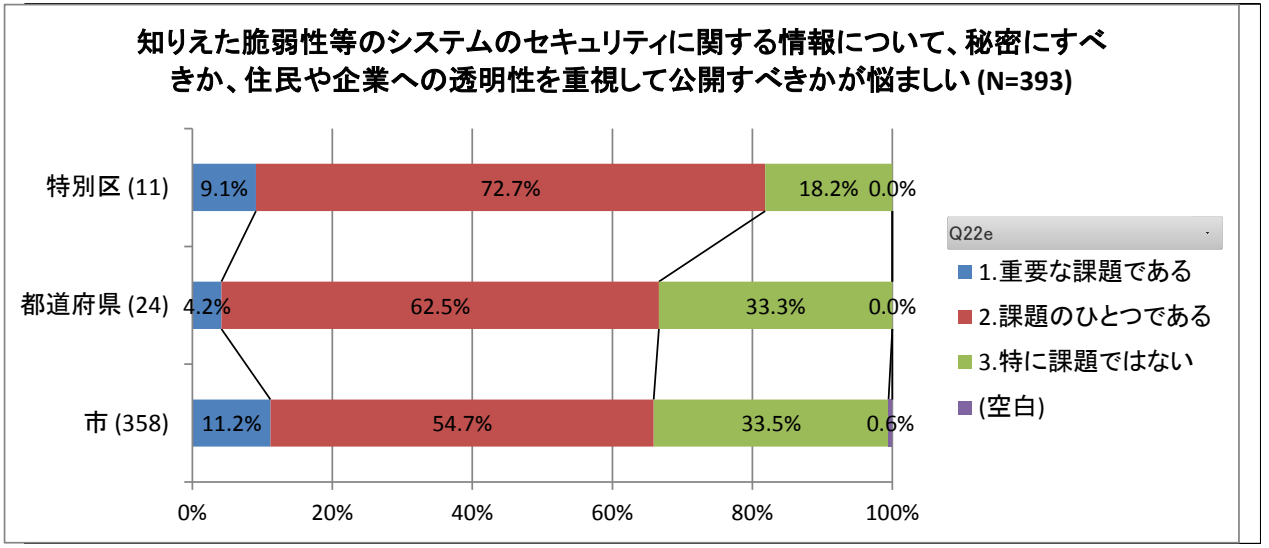
3.1.発見時の対応

脆弱性の存在が判明した際の対処手順は下記の通りです。

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
   - 影響やリスクを明確にして、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。
   - リスク、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、ソフトウェアの仮想環境を利用することで、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。

3.2.脆弱性情報の取り扱いの問題点

- 地方公共団体は、住民向けサービスのシステムについて未公表の脆弱性関連情報を得ると、以下の判断に悩まされます。
- 情報の公開/非公開
  - 透明性を優先して、脆弱性を修正する前にその情報を公表すると、広く影響が出ます。
    - システムが攻撃され、住民の情報が流出するなどの被害が生じる可能性があります。
    - 他の地方公共団体や民間企業等の類似システムが攻撃対象となる可能性があります。
- サービスの継続/停止
  - 住民向けサービスの継続は、地方公共団体にとって非常に重要な業務です。
  - 一方、脆弱性を抱えたまま住民にサービスを提供し続け、その間にシステムが攻撃されると、住民の情報などが流出する可能性もあります。



IPA「地方公共団体における脆弱性対策の実態に関する調査 アンケート」結果より

3.3.脆弱性情報の取り扱いの事例

- この問題点の取扱いについてどのような方針をとるべきか、事前に検討しておくことが望まれます。実際の事例についてご紹介します。
- 取扱いの判断例：
  - 攻撃を受けるリスクなど脆弱性の影響について、IPA、LASDECなどから情報提供を受け、サービスの継続性を判断する。深刻な場合は、サービスを止めることも視野に入れる。
  - 脆弱性情報は、情報公開条例の例外条項に該当すると判断し、対策が適用されるまでは非公開の扱いとする。
- 公表の例：
  - 脆弱性のあるシステムは、可能であればサービスを停止することの告知を事前に行った上で停止し、改修する。その際、必要に応じて代替サイトを立ち上げサービスを継続する。
- 脆弱性情報の取り扱いに対する組織的な対応例：
  - 運営するウェブサービスに脆弱性が発見された場合の対応手順を文書化して、組織内で共有する。
  - 委託先との契約も、脆弱性対策を念頭に置いたものとする。

参考資料

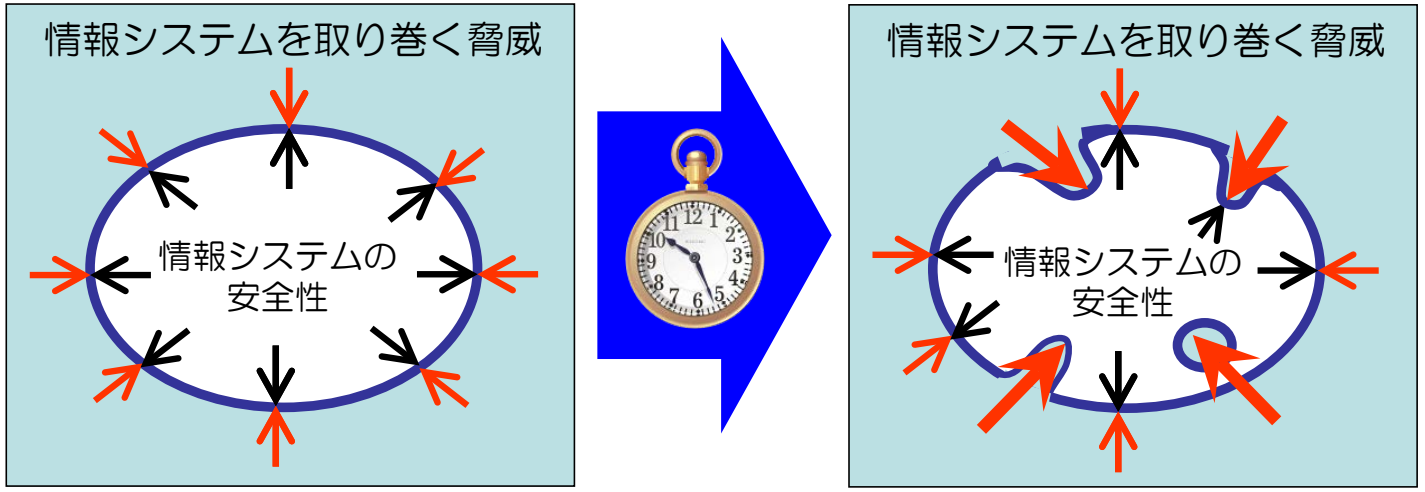
参考.1 脆弱性とはなにか

参考.2 情報セキュリティ早期警戒パートナーシップ

参考.3 参考URL

参考.1. 脆弱性とはなにか?

- 時間が経つと情報システムの安全性は低下してしまいます。
- 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ります。
- 理由としては、一般に次のことが言えるからです。
  - 新しい攻撃手法の開発
  - 情報セキュリティ上の「弱点」(脆弱性)の発見



開発当初は、脅威に対して適切な対処がなされ、安全性が高い

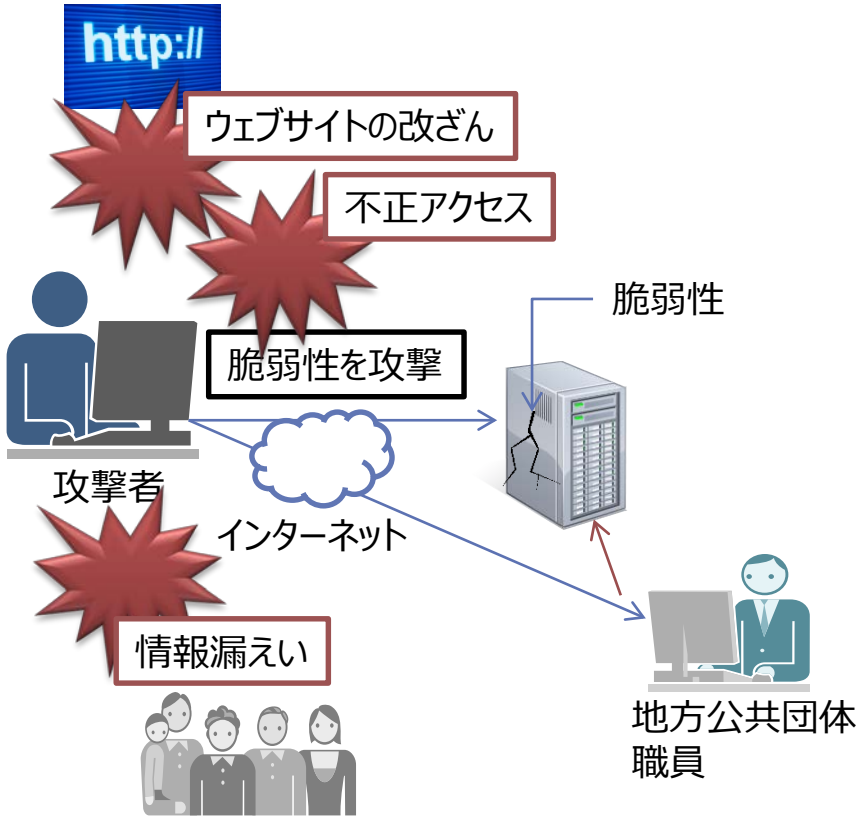
時間が経つと脅威が変化するため、そのままでは安全性を維持できない

参考.1. 脆弱性とはなにか?

脆弱性 ＝ 情報セキュリティ上の「弱点」「ほころび」

- 脆弱性が悪用されると、『個人情報の漏えい』、『ウェブサイトの改ざん』、『不正アクセス』をされてしまいます。
- ソフトウェア製品の脆弱性は日々発見されています。既に数万種類が公表されています。

詳細は以下の文献をご参照ください。
IPA「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/



脆弱性の問題は、ウイルス対策ソフトウェアでは解決しません。

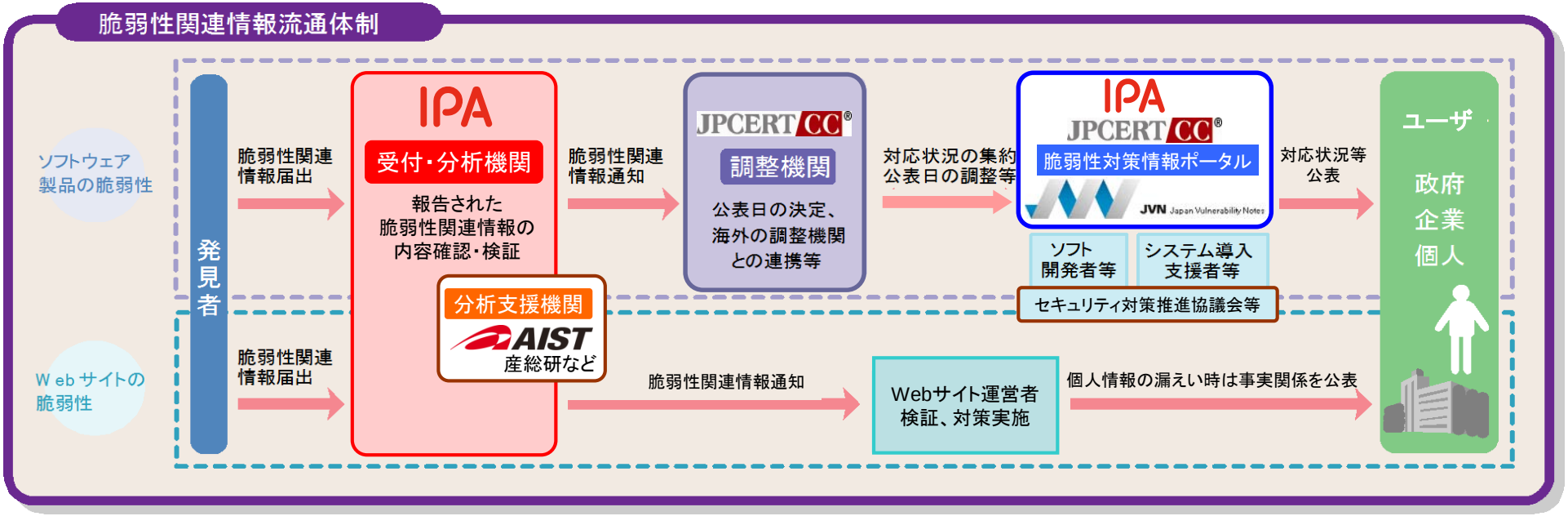
- ウイルスを駆除しても脆弱性を修正しなければ、再感染の可能性があります。
- ソフトウェア製品の場合、製品ベンダの修正プログラム（パッチ）を適用する必要があります。
- ウェブサイトの場合、問題箇所を改修する必要があります。

情報セキュリティ対策と脆弱性対策の関係は？

- 脆弱性対策は情報セキュリティ対策の一つです。
- 脆弱性対策が不十分だとトラブルを招くこともあります。

参考.2. 情報セキュリティ早期警戒パートナーシップ

- 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。
  - 「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）
- 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。
- ウェブサイト運営者が地方公共団体であった場合には、総務省を介して都道府県に、さらに都道府県から市町村に連絡する仕組みになっています。



※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

参考.3. 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
- 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/000059697.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/files/000058491.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/files/000058492.pdf
- 「安全なウェブサイトの作り方」
  - https://www.ipa.go.jp/files/000017316.pdf
- 「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/
- 「IPA セキュア・プログラミング講座」
  - https://www.ipa.go.jp/security/awareness/vendor/programming/index.html
- 脆弱性対策情報ポータルサイト
  - http://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「MyJVN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「MyJVNバージョンチェッカ」
  - http://jvndb.jvn.jp/apis/myjvn/vccheck.html
- 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
- サイバーセキュリティ注意喚起サービス「icat for JSON」
  - https://www.ipa.go.jp/security/vuln/icat.html