ウェブサイト運営者向け「セキュリティ問い合わせ窓口設置」の手引き

ウェブサイトの運営には日ごろからセキュリティ対策を行うことが重要です

攻撃者は無差別にウェブサイトを狙っています。そのウェブサイトにセキュリティ上の問題（脆弱性）があると攻撃を受けてしまい、情報流出やシステムの改ざん、停止などの事態が発生し、事業に影響を及ぼしかねません。また、セキュリティ上の問題は時間の経過とともに新たなものが発見されていくため、日頃からセキュリティ上の問題への対処を検討し、タイムリーに対応していくことが重要です。

セキュリティ上の問題について外部から受ける窓口があることが重要です

窓口がない場合

運用中のウェブサイトにセキュリティ上の問題があることを外部からの指摘によって初めて気がつくケースが少なくありません。この場合、外部からのセキュリティ上の問題の指摘を受け付ける窓口がないと、そもそも指摘を受け付けられない、指摘を受けても社内で迅速に展開ができない等により、対応が後手後手になってしまい、サイバー攻撃の被害にあう可能性が高まります。

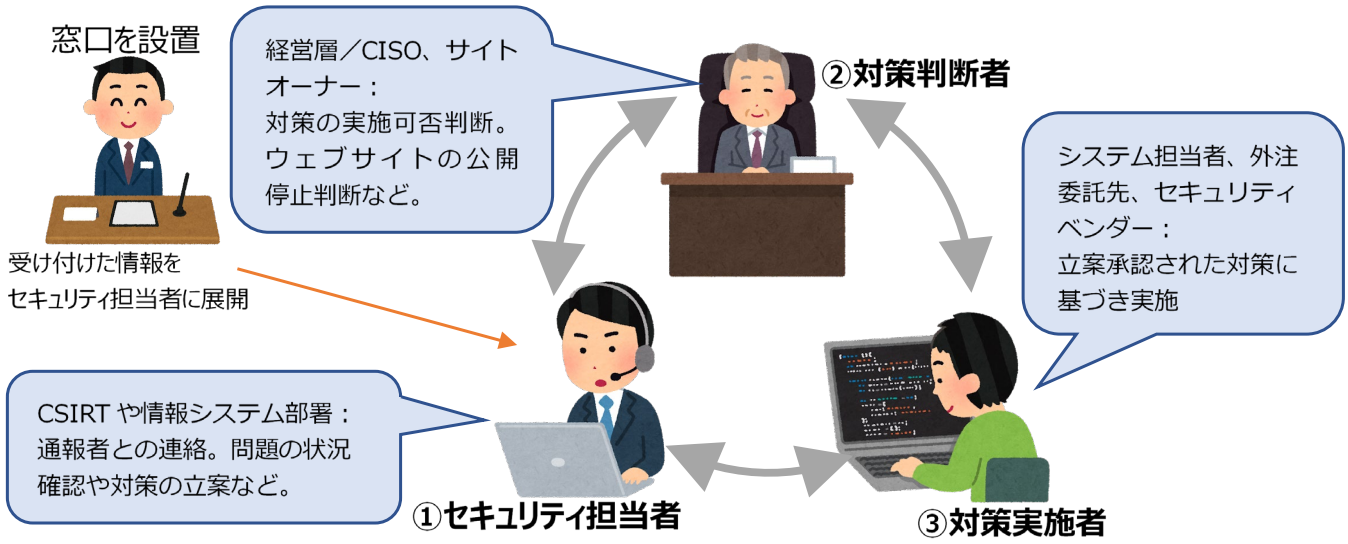
窓口がある場合

予め窓口を設置しておくことで、発見者がセキュリティ上の問題に気付いてから、問題が修正されるまで時間を短縮することが可能となり、攻撃被害を受ける可能性を大きく減らすことができます。これによって、事業の安定性や信頼性をより高め、攻撃被害による各種損失を未然に防ぐことが可能となります。ウェブサイトを安全に保ち、サービスを維持するためには、外部から情報を受け付ける仕組みの構築が重要になります。

- IPA からもウェブサイトに関する脆弱性についてウェブサイト運営者に連絡する場合があります。
  詳細は下記を参照ください。

  ・情報セキュリティ早期警戒パートナーシップの紹介 - 脆弱性取扱プロセスの要点解説 -
  https://www.ipa.go.jp/files/000059695.pdf
  ・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
  https://www.ipa.go.jp/security/ciadr/partnership_guide.html

セキュリティ上の問題の情報を適切に取扱うための体制・役割分担を決めておきます



① セキュリティ担当者

経営層（もしくは権限委嘱を受けた責任者、CISO 等）の責任において、セキュリティ上の問題についての情報を取り扱う最低1名のセキュリティ担当者を定めて下さい。セキュリティ担当者は情報システムや情報セキュリティの一定レベルの知識を持っていることが望ましいです。会社として CSIRT を設置している場合にはそのメンバー、設置していない場合には情報システム部署の担当者を指名することが一般的ですが、セキュリティ担当者が受け付けた情報の一次取扱者となり、問題の状況確認や対策の立案、通報者との連絡や対策実施者への引き継ぎ、対策判断者への説明等を行う役割を担います。

② 対策判断者

対策実施にあたっては経営層やウェブサイトのオーナー部署（通常は広報部署が多い）が、対策判断者としてその可否を判断する等の役割を担います。さらに攻撃を受けた場合を想定し、被害を予防するためのウェブサイトの公開停止等も対策判断者が判断を下します。これらを経営の責任において予め定めておくことが大事であり、相互の社内連絡先や連絡方法を整理しておきます。

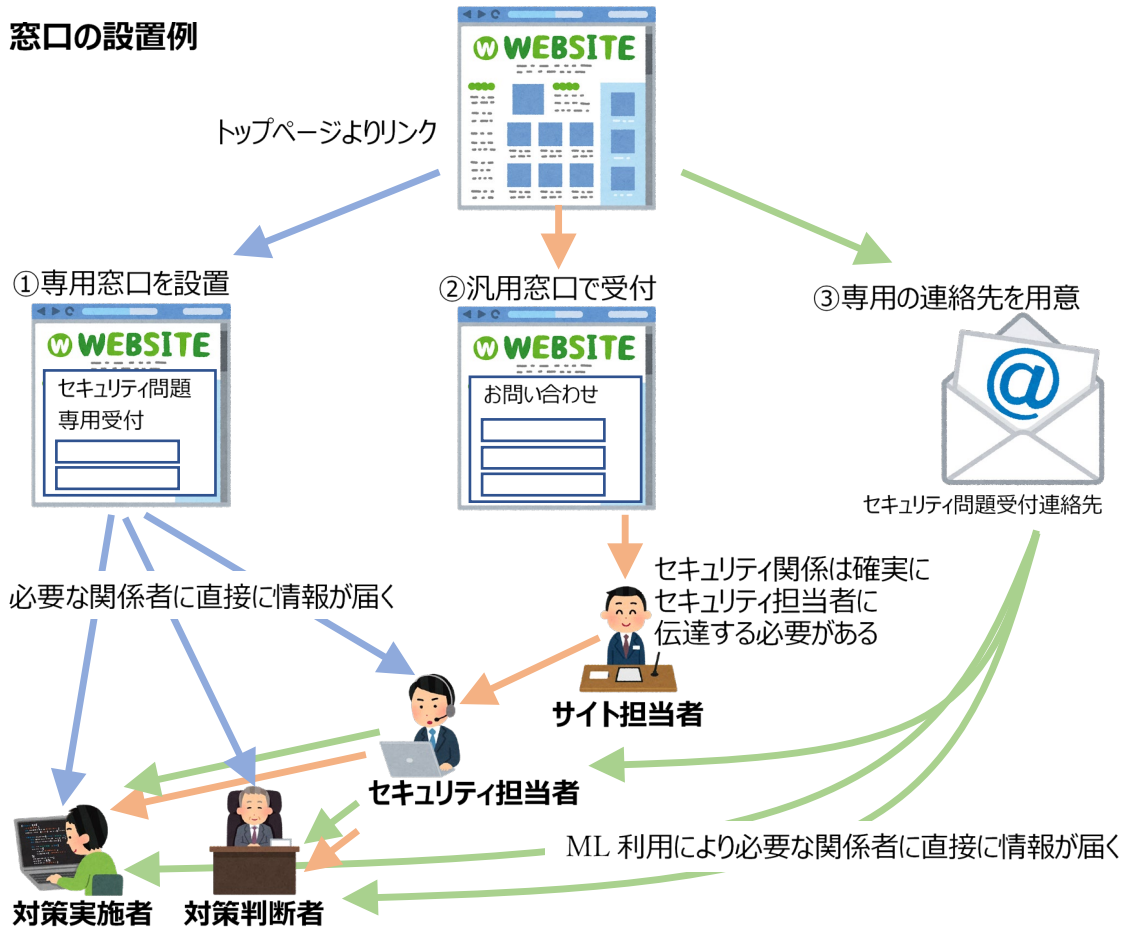
③ 対策実施者

対策判断者の決定のもと、セキュリティ担当者が立案した対策に基づき、実際に脆弱性のあるプログラムに修正を実施します。ウェブサイトの構築や運用を外部委託先に委託している場合などには、情報システム担当者やセキュリティ担当者とシステム構築・運用委託先との作業範囲や責任範囲を明確にしておきます。

- 体制・役割分担、エスカレーション手順などを関係者で予め決めておくことが重要です。
  脆弱性の指摘を受けてからの一連の対応の流れについては、下記ガイドなども参考にしてください。

  ・ウェブサイト運営者のための脆弱性対応ガイド
  https://www.ipa.go.jp/files/000058492.pdf

窓口の設置方法は複数考えられ、それぞれ情報の流れ方が異なります



①メリット：必要な関係者に直接かつ確実に情報が届くので対応開始が早く、漏れがない
デメリット：専用ページのための構築作業、運用のための工数が発生する

②メリット：汎用窓口ページを利用するのでサイト運用コストが安い
デメリット：サイト担当者からセキュリティ担当者に確実に情報伝達される仕組みが必要

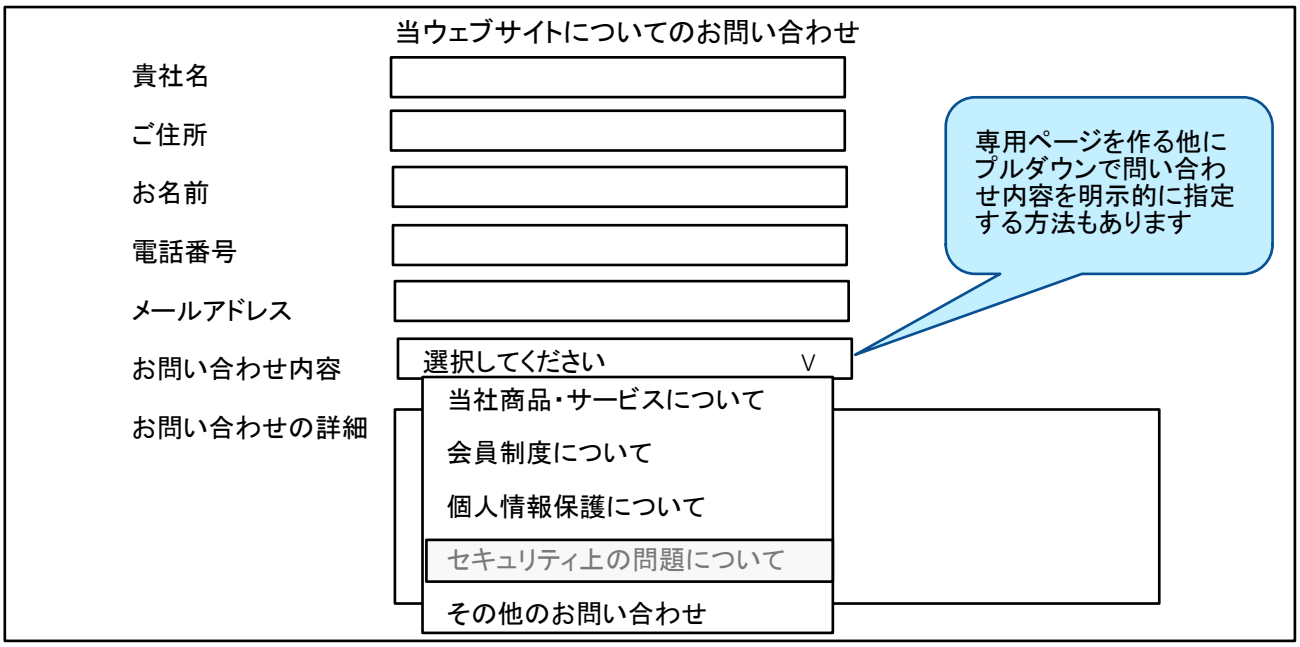
③メリット：必要な関係者に直接かつ確実に情報が届くので対応開始が早く、漏れがない
デメリット：特筆するべきデメリットはない（CSIRT 設置組織は専用メールアドレスを用意しているところが多い）

窓口の設置方法はいろいろと考えられますが、代表的な方法は、ウェブサイト上に専用の問い合わせフォームを置いて専用窓口を設置する方法（①専用窓口を設置）、汎用的な問い合わせフォームを使って汎用窓口で受付を行いサイト担当者が問い合わせ内容に応じて振り分ける方法（②汎用窓口で受付）、セキュリティ担当者や関係者に直接届く専用メールアドレスを設ける方法（③専用の連絡先を用意）などです。大きなポイントになるのは、外部の発見者からどのような方法で情報を受け取るか（例：ウェブフォーム、メールアドレス）、そして、外部から受け取った情報をどのように組織内部のセキュリティ担当者等の関係者に情報連携するか（例：関係者に直接届くようにする、サイト担当者を仲介して展開する）です。

それぞれにメリット、デメリットがありますので、コスト、人的リソース、システム環境など、それぞれの状況に合わせて検討してください。

窓口イメージ

■ウェブフォームの場合



■メールアドレスの場合

当サイトのセキュリティに関する問題についてご連絡ください。

それ以外のご用件については[お問い合わせページ]にお願いします。

通報窓口：セキュリティ担当

E-mail ： **@****.**

電話 ： 03－＊＊＊＊－＊＊＊＊

窓口設置に関する Q&A

Q1 どういったウェブサイトの場合に、窓口設置は必要でしょうか。

次のケースに該当する場合、セキュリティ対策を行うことが特に強く望まれます。脆弱性が潜んでいることが少なくありません。そのため、該当するウェブサイトの場合は、窓口を設置することを特に推奨します。

(1) 個人情報、顧客情報等の重要な情報を預かっている（情報流出防止のため脆弱性管理と窓口設置が強く望まれます）

(2) ウェブサイトに脆弱性となりやすい機能（例えば、ユーザ登録画面や入力欄フォーム等）がある

(3) ウェブサイトの構築後にメンテナンスをしていない。

Q2 窓口への問い合わせの頻度はどの程度でしょうか。

IPA が 2020 年度に実施した小規模ウェブサイト運営者を対象としたアンケート調査結果によれば、脆弱性に気付いたきっかけは、組織外（「社外の関係者や取引先等」、「ウェブサイトの利用者」など）からの連絡を受けたことをきっかけとした回答は合わせて 31.3%という結果が得られました。組織外からの連絡を受けることが多くなっている傾向がみられます。

Q3 セキュリティに詳しい要員がおらず体制が組めません。

体制や役割分担の検討にあたって、自組織内で一定のセキュリティを担保できない場合は、セキュリティベンダーやシステムの運用保守業者に外部委託することも検討が必要です。また、ウェブサイトの構成自体を見直し、セキュリティパッチを自動適用する機能のあるクラウドサービス上でウェブサイトを運営するなど、自組織での対応の必要が少なくなるようにすることも一案になります。

Q4 窓口設置のコストはどのくらいですか。

ホームページ上に窓口のページを作成したり、メールアドレスを作成したりするだけですので、新たな費用はほとんど掛かりません。社内のエスカレーション体制やルールを整える必要がありますが、問題発生後にあわてて対応を検討するよりも計画的に対応することで全体コストはむしろ安くなる可能性があります。

Q5 経営層に必要性を理解してもらうにはどうしたら良いでしょうか。

P2 に紹介している「ウェブサイト運営者のための脆弱性対応ガイド」に被害事例を掲載しています。その中で損害額や対応に要した期間等が紹介されていますので、具体的な数字で経営層にご理解いただくことが出来ると思います。

Q6 窓口を設置することで逆に怪しい通報をうけることはないでしょうか。

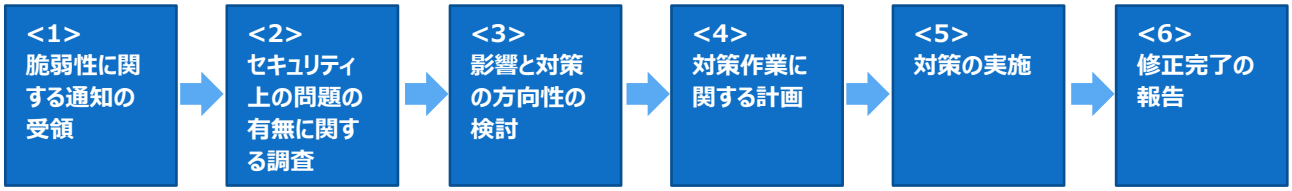
IPA から連絡があった場合には、本資料の最後に記載している IPA の連絡先に問合せをお願いします。IPA 以外からの問合せについては、問合せの記載内容や問合せ元の信ぴょう性を確認してください。疑念が払しょくできない場合は、委託先のシステムベンダーやセキュリティベンダーに相談することが考えられます。

Q7 窓口を設置すると、セキュリティ上の問題が多いサイトと見られそうです。

ウェブサイトに不正侵入されて会員の個人情報やクレジットカード情報などが流出したというニュースが頻繁に流れるようになり、利用者にとってウェブサイトが安全なのかという点は以前にも増して関心事となってきています。窓口を設置することは、外部から寄せられる情報にいち早く対応できる体制が整えられていることを示すもので、むしろアピールポイントとしていくことが重要です。最近では、セキュリティ上の問題にいち早く対応するための CSIRT と呼ばれる組織を設置する企業が増えており、顧客に対してセキュリティ課題への積極的な取組姿勢をアピールするツールにもなっています。

Q8 窓口に寄せられる情報に対して、どのようなアクションを起こしたら良いのでしょうか。

寄せられた情報をもとに、脆弱性の有無について調査し、必要であれば脆弱性修正プログラムの適用といった対策を行います。対処にあたっては全体方針や、対策の計画をウェブサイト運営者自身の判断に基づいて行うことが必要となります。詳細は、P2 でご紹介した「ウェブサイト運営者のための脆弱性対応ガイド」を参照ください。



独立行政法人 情報処理推進機構
Information-technology Promotion Agency, Japan

〒113-6591
東京都文京区本駒込２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
URL https://www.ipa.go.jp/security/
MAIL vuln-inq@ipa.go.jp