IPA Better Life with IT

IPA
脆弱性対策
コンテンツ
リファレンス

2025年3月

独立行政法人**情報処理推進機構**
セキュリティセンター

Contents.

1. 脆弱性　(Vulnerability：バルネラビリティ)とは

「脆弱性」とは「ソフトウェア等におけるセキュリティ上の弱点」のことで「セキュリティホール」とも呼ばれます。本資料「IPA脆弱性対策コンテンツリファレンス」では「ウェブアプリケーション(ウェブサイト)」および「ソフトウェア製品」に関する脆弱性を対象とします。

近年、脆弱性がコンピュータウイルスや不正アクセス等の攻撃に悪用されるケースが増加しています。また、脆弱性に関する情報の公開後に、その脆弱性を狙う攻撃方法が作られ、広まるまでの期間が短くなる傾向があり、対策前にコンピュータウイルスに感染する危険性、公開サーバが攻撃され大きな被害を受ける危険性、および脆弱性を放置したことにより第三者が被害を受ける危険性も増大しています。

脆弱性については、対策がとられないまま放置されたり、対策がとられない状況で悪用可能な情報が先に公開されたりする場合の問題が指摘され、このような問題に対処するために、関係者間の適切な脆弱性に関する情報の共有と連携が強く求められています。

IPAでは、こうした脆弱性による危険の低減および被害の拡大防止に取組んでいます。

2. IPAにおける脆弱性対策に関する取組みについて

IPAでは、IT社会の脆弱性の低減を目的として、脆弱性対策時に役立つ資料の公表やツールの提供、脆弱性関連情報の集約・公開など様々な取組みを行なっています。

これらの取組みは大きく以下の4種に分けることができます。いずれもシステム等の開発者向けから経営層・一般利用者向けのものまで利用対象が幅広く、様々な職場の方や業務にて活用いただける内容になっています。
それぞれのコンテンツの詳細を次章から詳しくご紹介します。

■脆弱性の低減を目的としたIPA　4種類のコンテンツ

コンテンツ	説明
普及啓発資料･普及啓発ツール	脆弱性や脆弱性対策等の理解を促すための書籍資料や学習ツール、体験ツールです。技術的な資料から理論的な資料まで、幅広い分野の資料があり、技術に詳しくない方でも気軽に活用することができます。
情報セキュリティ 早期警戒パートナーシップ	一般の方や研究者の方が発見された、ウェブサイトおよびソフトウェア製品に関するセキュリティ上の問題の届出を受付け、ウェブサイト運営者やソフトウェア製品開発者へ連絡し、脆弱性への対応を促します。
検査･検証ツール	脆弱性があるかどうかを検査･検証する為のツールです。
JVN(Japan Vulnerability Notes)	ソフトウェアなどの脆弱性関連情報や対策情報を提供している脆弱性対策情報ポータルサイトです。また、JVNの情報を有効に活用するためのツールも提供しています。

３．開発工程別 － 情報システムの脆弱性に対するIPAの取組み －

本章では、前章で説明した4種のコンテンツについて開発工程をもとに分類し、各工程で活用可能な資料を紹介します。各工程で実施可能な対策を実施し、脆弱性修正の手戻りがないよう開発することが望ましいです。より早い工程での対策はコストパフォーマンスの面で効果があります。

それぞれの開発工程に応じて、各種コンテンツをご活用ください。

開発工程	セキュリティ対策	コンテンツ	POINT
企画/要件定義	・調査・動向把握 ・開発方針/体制整備	**・普及啓発資料・普及啓発ツール** -情報セキュリティ10大脅威 -安全なウェブサイトの作り方 -ウェブサイト構築事業者のための脆弱性対応ガイド　など	事前にセキュリティの動向を把握し、開発方針を決めておく
設計/実装	・セキュアプログラミング ・脆弱性を作りこまない設計・実装	**・普及啓発資料、普及啓発ツール** -安全なウェブサイトの作り方 -安全なSQLの呼び出し方 -脆弱性体験学習ツールAppGoat　など	脆弱性修正による開発の手戻りがないようにセキュリティを考慮したプログラミングやそのルール設定を行なう
テスト	・セキュリティテスト(ファジング・ペネトレーション等)	**・検査・検証ツール** -ファジング活用の手引き -ウェブ健康診断　など	脆弱性が作られないよう、また未知の脆弱性に対応できるようセキュリティ対策について確認できるテストを実施する
運用/利用/破棄	・システムの最新状況把握 ・新たに発覚した脆弱性への対応	**・普及啓発資料・普及啓発ツール** -Web Application Firewall 読本 -ウェブサイトの攻撃兆候検出ツール「iLogScanner」 **・JVN（Japan Vulnerability Notes）** -JVN iPedia　など **・情報セキュリティ早期警戒パートナーシップ**	運用しているシステムについて、常に最新の状況を把握する

経営者･経営層

企業規模は無関係！気づかないうちに脅威にさらされているかも

個人法人を問わず、またその規模にも関係なくネットワークを介した攻撃の脅威にさらされており、セキュリティ対策が必要です。セキュリティ対策について動向を把握し、脅威のない状態を維持する事ができるか、また、被害にあった時に適切な対応ができるかどうかが重要です。

近年のセキュリティに関する被害事例や動向把握には「情報セキュリティ10大脅威」「情報セキュリティ白書」が有効です。簡単に情報セキュリティを理解したい場合には「 5分でできる！情報セキュリティポイント学習」が有効です。

⇒11,20ページ参照

ソフトウェア製品開発者･ウェブサイト構築者

ウェブアプリの代表的な脆弱性は新しいものではない！開発から対策を

クロスサイト・スクリプティングやSQLインジェクション等の代表的な脆弱性の仕組みは昔から変わりません。開発段階からこれらの対策を組み込むことで、修正等の手戻りの可能性も低減でき、脆弱性対策を考慮した開発を行なうことは非常に重要です。

対策方法を具体的に示した「安全なウェブサイトの作り方」は開発時の教科書的な構成で非常に実用的です。体験的に学習したい方には「脆弱性体験学習ツールAppGoat」が有効です。

⇒11,20ページ参照

運用保守担当・管理者

委託先丸投げはNG！
契約段階からセキュリティへの配慮が必要

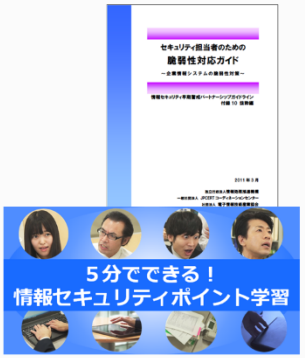
自分が行うべきセキュリティ対策はどのようなものがあるか知る事で、脆弱性が発覚した時に素早く対応することができます。委託時の契約段階からセキュリティ対策を意識する事が大切です。また、システム等の安全性は時間とともに低下します。常に安全な状態を維持する対策も重要です。

「脆弱性対応ガイド」は運用時のセキュリティ対策や担当者に期待される事項等をまとめた実用的な資料です。運用時の脆弱性対策情報収集には「icat」「MyJVN」が有効です。

⇒10,14ページ参照

セキュリティ室・セキュリティ担当者

システムだけでない！
今は「人」についてのセキュリティ対策も必要



昨今は「人」が原因となる情報セキュリティ事故も多く発生しています。これを防ぐためには、組織においてどのような教育・社内ルールが有効かを把握し、組織に適した対応を行なうことが大切です。

「脆弱性対応ガイド」により担当者が行なうべき対策を把握できます。社員のセキュリティ教育にあたっては「5分でできる！情報セキュリティポイント学習」が有効です。

⇒14,20ページ参照

ソフトウェア・ウェブサイト利用者

自分の身は自分で！
個人でもできるセキュリティ対策があります

インターネットが浸透した現代において、自分の身は自分で守らなければなりません。技術的な知識がなくても、例えば「使用しているソフトウェアを常に最新版にしておく」といった事も、有効なセキュリティ対策です。

「My JVNバージョンチェッカ」でPCにインストールされているソフウェア製品が最新かどうかを簡単にチェックできます。「icat」でIPAが公開した注意喚起情報をリアルタイムに確認できます。

⇒10ページ参照

情報システムの脆弱性に対するIPAの取組み　関連URL

- 情報セキュリティ関連サイト
  https://www.ipa.go.jp/security/guide/keihatsu.html
- 日常における情報セキュリティ対策
  https://www.ipa.go.jp/security/anshin/measures/everyday.html
- 安全なウェブサイトの運用管理に向けての20ヶ条
  ～セキュリティ対策のチェックポイント～
  https://www.ipa.go.jp/security/vuln/websecurity/sitecheck.html
- IPA Channel
  https://www.youtube.com/user/ipajp/videos

IPA脆弱性対策のためのコンテンツ

IPAでは、脆弱性対策のために様々な形で情報の提供を行なっています。
IPAの脆弱性対策に関する取組みは枠組みとしての対応、サービス提供としての対応、資料やツール提供としての対応等、様々なものがあります。

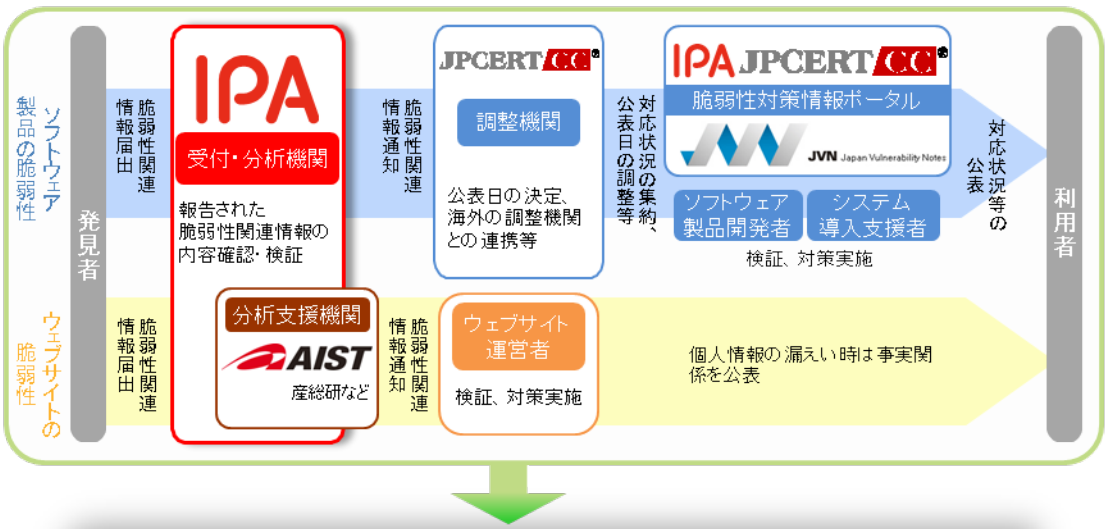
5. 脆弱性関連情報流通の基本枠組み「情報セキュリティ早期警戒パートナーシップ」

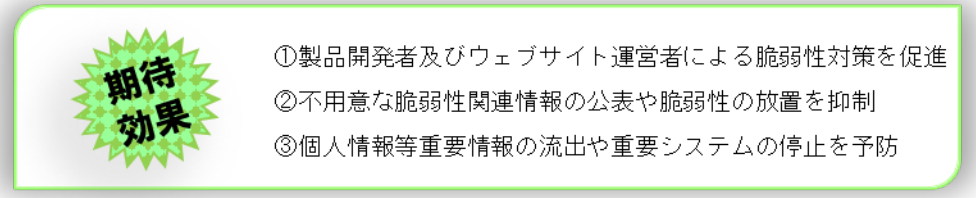
IPAでは、情報セキュリティ対策の一環として、経済産業省告示に従い、一般の方や研究者の方が発見された、ウェブサイトおよびソフトウェア製品に関するセキュリティ上の問題を受付け、ウェブサイト運営者およびソフトウェア製品開発者の方に連絡を行ない、問題についての対応を促します（脆弱性関連情報届出制度）。また、脆弱性関連情報が発見された場合に、発見者やウェブサイト運営者、ソフトウェア製品開発者等の関係者に対して推奨する行為をとりまとめた「ガイドライン」を公表しています。

「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」
URL： https://www.ipa.go.jp/security/guide/vuln/partnership_guide.html

「脆弱性ハンドブック」（2013年3月15日発行）
「情報システム等の脆弱性情報の取扱いに関する研究会」の主導のもと、脆弱性対策の実態把握とともに脆弱性対応を促す方策の推進に取組んでおり、この取組みの成果を集約した資料が「脆弱性ハンドブック」です。
情報システムにおける脆弱性の理解および脆弱性対策方法について全般的に解説しており、脆弱性対策を行うべき方々に活用いただける資料です。

情報セキュリティ早期警戒パートナーシップ



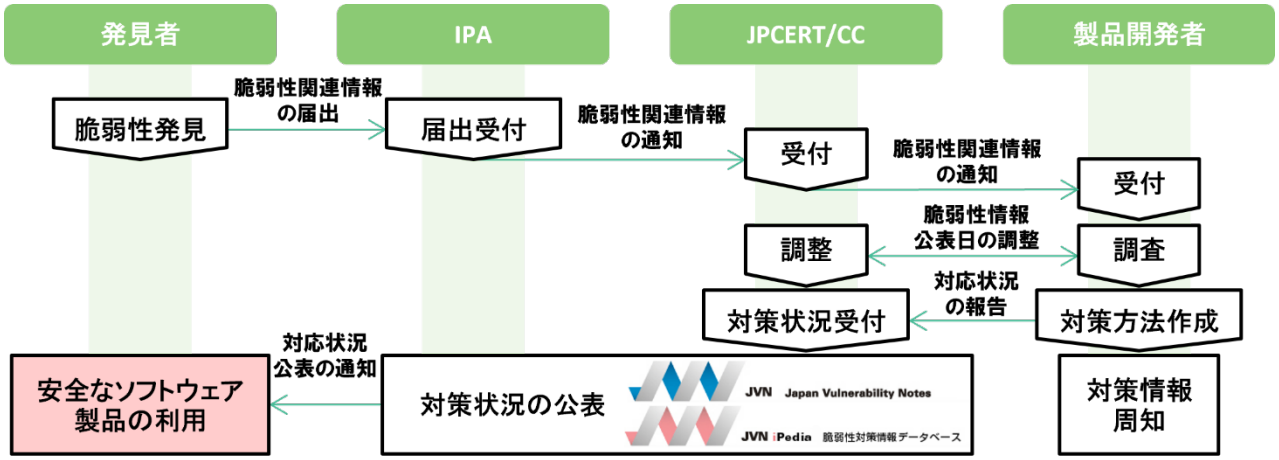


※IPA:独立行政法人情報処理推進機構, JPCERT/CC:一般社団法人 JPCERTコーディネーションセンター
AIST(産総研): 国立研究開発法人産業技術総合研究所

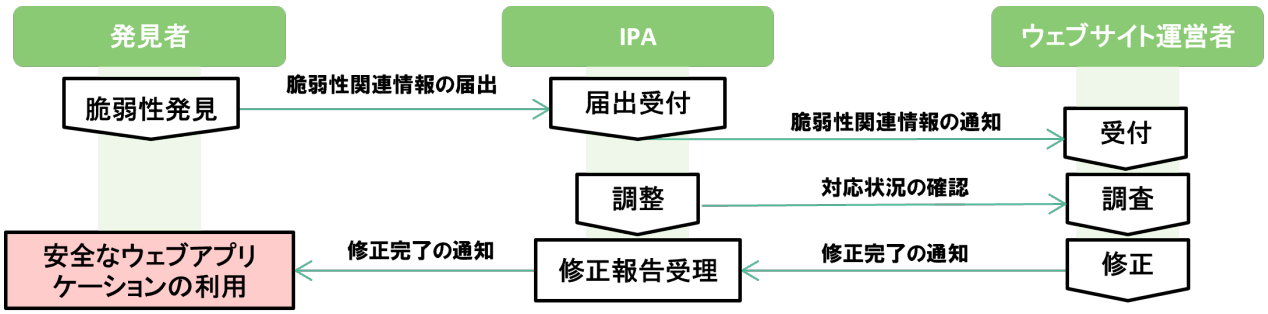
情報セキュリティ早期警戒パートナーシップ運用におけるメリット

発見者	ソフトウェア製品開発者	ウェブサイト運営者	ウェブサイト・ソフトウェア製品利用者
•届出に関する調整はIPAのみと行う為、個人情報を運営者・開発者へ通知不要 •脆弱性の発見者としてJVNにおいて記名が可能	•自身が開発した製品の未知の脆弱性情報を入手可能 •脆弱性対策情報を広く利用者へ周知可能 •脆弱性対策への取組みを利用者へアピール可能	•脆弱性情報と併せて対策に必要な情報(資料・アドバイスなど)を入手可能 •脆弱性悪用防止のため、本制度にて脆弱性情報の拡散を低減・抑止	•ソフトウェア製品の脆弱性対策情報を入手可能 •脆弱性対策された安全な製品・ウェブサイトが利用可能

ソフトウェア製品に関する取扱い



ウェブアプリケーションに関する取扱い



※ 取扱いの詳細は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をご参照ください。

情報セキュリティ早期警戒パートナーシップ　関連URL

・脆弱性関連情報の届出受付
https://www.ipa.go.jp/security/todokede/vuln/uketsuke.html

・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/guide/vuln/partnership_guide.html

6. IPA脆弱性対策のためのコンテンツ – サービスにて提供 –

JP ：日本語コンテンツ
EN ：英語コンテンツ

JVN（Japan Vulnerability Notes） JP EN

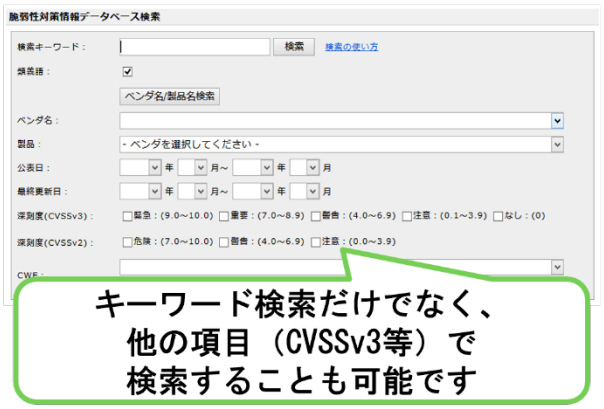
- JVNは日本で使用されているソフトウェア製品などの脆弱性関連情報とその対策情報を提供し、情報セキュリティ対策に資する事を目的とする脆弱性対策情報ポータルサイトで、脆弱性関連情報（脆弱性とその存在を調べる方法、さらに脆弱性悪用につながる情報）とそれに対する対策、製品開発者の対応状況を公開しています。
- JVNでは様々な脆弱性関連情報を収集し、原則として製品開発者との調整を通じて対策方法を準備した上で、それらを該当製品の利用者にとって分かりやすくまとめた形で掲載しています。製品開発者の対応状況には脆弱性に該当する製品の有無、対策情報（パッチ等）や回避策（ワークアラウンド）も含まれます。

- https://jvn.jp/

JVN Japan Vulnerability Notes

JVN iPedia JP EN

- JVN iPediaは、ソフトウェア製品の脆弱性対策情報を収集・公開することにより、製品開発者や一般利用者が脆弱性関連情報を容易に利用可能とすることを目的としたサービスで、JVNに掲載される情報のほか、国内外問わず公開された脆弱性対策情報を広く公開対象とし、データベースとして蓄積しています。2024年12月末時点で223,000件以上の情報があり、データは日々増え続けています。
- JVN iPediaでは、「特定の製品に存在する脆弱性を確認したい」「JVN・他組織で公開される情報をもとに脆弱性対策を調べたい」など、入手したい情報が特定されている場合に、検索機能(キーワード等)によって必要な情報を効果的に探すことが可能です。また、蓄積状況を容易に確認できるようにRSS形式(*)による脆弱性対策情報を提供しており、定期的な脆弱性情報の取得が可能です。
- (*)RSS(RDF Site Summary)



- https://jvndb.jvn.jp/

JVN iPedia 脆弱性対策情報データベース

X（旧 Twitter） IPA公式アカウント JP

JVN iPedia ：国内で広く利用されているソフトウェアの脆弱性を収集・蓄積した「脆弱性対策情報データベース JVN iPedia」 に新規登録している脆弱性対策情報のタイトルや URLの情報を発信します。

My JVN ：利用者のPCにインストールされているソフトウェアのバージョンが最新であるかを、簡易な操作でチェックする 「MyJVN バージョンチェッカ」 の対象ソフトウェアに関する更新情報を発信します。

ICATalerts ：IPAから発信している「緊急対策情報」 のうち、セキュリティ問題のタイトル(概要)と発信元のURLの情報を発信します。

運用方針： https://www.ipa.go.jp/socialmedia/x.html

6. IPA脆弱性対策のためのコンテンツ – サービスにて提供（続き）–

MyJVN

JP

•MyJVNは、PCやサーバの脆弱性対策を促進するために、対策情報を効率的に収集したり、簡単な操作で最新情報に基づいたチェックを行うことができる仕組み（フレームワーク）の総称です。

•MyJVN は、国際協力の強化に向け、米国政府の支援を受けた非営利団体MITRE Corporationが中心となって仕様策定を進めているソフトウェアの製品を記述するための共通基準「CPE（共通プラットフォーム一覧：Common Platform Enumeration）」を試行しています。また、既にCVE、CVSS、CWEを適用しています。

https://jvndb.jvn.jp/apis/myjvn/

▼MyJVN API

MyJVN API(*)は、JVN iPediaの情報を、ウェブを通じて利用するためのソフトウェアインタフェースです。 誰でも、MyJVNが提供するAPIを利用して様々な脆弱性対策情報を取得し、脆弱性対策情報を利用したサイトやアプリケーションを開発することが可能となります。
(*)API(Application Program Interface)

▼MyJVNバージョンチェッカ

MyJVNバージョンチェッカでは、マウスクリックだけの簡単な操作でPCにインストールされている複数のソフトウェア製品が最新のバージョンであるかを確認することができます。
◇.NET Framework 版 https://jvndb.jvn.jp/apis/myjvn/vccheckdotnet.html

サイバーセキュリティ注意喚起サービス「icat for JSON」

JP

•IPAが“重要なセキュリティ情報”としてウェブサイトやメール配信により周知している、脆弱性の対策情報を、リアルタイムでウェブサイト上に表示し確認するためのサービスです。企業や団体のウェブサイトでの利用による、一般の利用者への迅速なセキュリティ対策情報の発信と対策の促進を目的としています。

https://www.ipa.go.jp/security/vuln/icat.html

7. IPA脆弱性対策のためのコンテンツ

7章では、IPAで公開している脆弱性対策のための「資料」「ツール」について、それぞれの概要、利用対象、活用方法を詳しく紹介します。

7. 1 IPA脆弱性対策のためのコンテンツ – 資料として提供 –

名称	概要	利用対象	活用方法
情報セキュリティ10大脅威 JP 	前年に発生したセキュリティ事故や攻撃の状況等を基に、情報セキュリティ分野の研究者や実務担当者で構成された「10大脅威選考会」の投票により、情報システムを取巻く脅威を順位付けした資料で、各脅威について解説しています。	経営者 管理部門 利用者 運用・保守	前年に発生した被害事例や社会的に影響が大きかった事象に関するコンテンツとなっており、近年のセキュリティ動向の把握に有効な資料です。企業の研修やセキュリティ教育等で活用されています。
情報セキュリティ白書 JP EN 	国内外の注目すべき情報セキュリティ事件・事故や、新しいサービス・情報機器の利用拡大による新たな脅威など、広く情報セキュリティに関する出来事や状況をまとめた情報セキュリティに関する報告書です。ITの専門家や技術者だけでなく、一般の利用者にも情報セキュリティの現状を周知することを目的としています。	経営者 管理部門 利用者	広く情報セキュリティに関する出来事や状況など、幅広いテーマを取扱っています。企業の研修やセキュリティ教育等で活用されています。
安全なウェブサイトの作り方 JP 	ウェブサイト開発者や運営者がセキュリティを考慮したウェブサイトを作成するための資料です。IPAが届出を受付けた脆弱性関連情報を基に、届出件数の多かった脆弱性や攻撃による影響度が大きい脆弱性を取り上げています。	開発者 運用・保守 運営者	情報セキュリティ早期警戒パートナーシップでの取組みから見えた脆弱性や対策の実態を踏まえ、脆弱性の概要だけでなく、対策の注意点や失敗例等も記述した、非常に実用的な資料です。
安全なSQLの呼び出し方 JP EN 	SQLインジェクション攻撃への具体的な対策書として、ウェブアプリケーションの安全な実装方法を解説した資料です。ウェブサイトを狙ったSQLインジェクション 攻撃が継続し深刻な被害が発生している実態を踏まえ、SQLインジェクション対策が安全なものであるための要件を掘り下げて検討し、どの製品をどのように使えば安全なSQL呼び出しを実現できるのか、その考え方を整理しながら、いくつかの具体的ケースについて調査結果を示しています。	開発者 運用・保守 運営者	「安全なSQLの呼び出し方」は「安全なウェブサイトの作り方」の別冊という位置づけです。SQLインジェクションの対策についてより詳細に理解したい場合に活用できます。

7．1　IPA脆弱性対策のためのコンテンツ – 資料として提供(続き) –

名称	概要	利用対象	活用方法
別冊 「ウェブ健康診断仕様」  JP	ウェブサイトで基本的な脆弱性対策ができているか確認する方法を解説しています。危険度の高い脆弱性など13の診断項目について、検出パターンと、それに対応した脆弱性有無の判定基準が記載されています。手順に沿ってウェブサイトを健康診断することで「要治療・精密検査」「差し支えない」「異常は検出されなかった」のいずれかの診断結果が得られます。	開発者 運用・保守 運営者	現在運用しているウェブサイトを診断することで対策が行われているかの現状を知り、それに基づいて対策を検討できます。また、ウェブサイト構築における受入れ検査や検収の時点で活用すれば、その後に行うべき精密検査の見通しを立てることができます。 ※ ただし検査パターンを絞り込んだ診断ですので、脆弱性が検出されなかった場合でも、安全宣言には繋がりません。
Web Application Firewall 読本  JP EN	ウェブサイト運営者がWeb Application Firewall(ウェブ・アプリケーション・ファイアウォール、WAF)の導入を検討する際に、WAFに関する理解を手助けするための手引書です。WAFの概要、機能の詳細、導入におけるポイント、海外組織・機関におけるWAFに関する取組み等をまとめています。	運用・保守 運営者	WAFについて理解したい場合に有効です。また、付録としてオープンソースソフトウェアのWAFおよび商用製品のWAFを紹介しており、WAFの導入を考えている場合にも有効な資料です。
Web Application Firewall(WAF)の導入に向けた検討項目  JP	WAFの導入を検討されているウェブサイト運営者を対象とし、WAFにどのような製品種類が存在し、どのような特徴が存在するか解説しています。 ウェブサイトを運営する組織が、どのような基準から製品種類を選択すべきかについて解説しています。	経営者 運用・保守 運営者	WAFを導入・運用する際にどのような作業や検討が必要かについて解説しており、WAFをこれから導入する運営者が製品を検討する場合や、既に運用中の組織において運用体制を見直す場合等にご活用いただけます。

7. 1　IPA脆弱性対策のためのコンテンツ – 資料として提供(続き) –

名称	概要	利用対象	活用方法
上水道分野用のSCADA(監視制御システム)セキュリティ・グッドプラクティス  JP	上水道分野用SCADAのセキュリティ水準向上のため、オランダ政府とTNO Defence, Security and Safety社が実施した調査の報告書を翻訳したものです。本書には、自組織のセキュリティの現状を把握することができる39の対策項目(グッド・プラクティス)がチェックリストとして収められています。このチェックリストは上水道分野のセキュリティ対策の成功事例に基づき作成されていますが、水道・ガス・電力等の上水道分野以外の重要インフラ分野にも活用できます。	運用・保守 経営者	本書に記述されている39の対策項目(グッド・プラクティス)はセキュリティポリシーの作成等に関する企業経営者向け(11件)と、重要インフラシステムの管理に関する技術者向け(28件)の2種類に分類されており、自組織内でそれぞれの職位、職種に合った対策項目(グッド・プラクティス)を活用し、セキュリティ対策の実践に役立てることができます。
脆弱性ハンドブック  JP	IPAでは「情報システム等の脆弱性情報の取扱いに関する研究会」の主導のもと、脆弱性対策の実態把握とともに、企業を中心とした利用者、ソフトウェア製品開発者、ウェブサイト運営者における脆弱性対応を促す方策の推進に取組んでいます。脆弱性ハンドブックは、この取組の成果を集約し幅広い読者にむけて提供する為に作成したものです。	運営者 開発者 運営・保守 管理部門 経営者 利用者	情報システムにおける脆弱性の理解および脆弱性対策についてどの様に取組むべきかという方法について全般的に解説しており、脆弱性対策を行うべき方々に活用いただける資料です。
ソフトウエア製品開発者による 脆弱性対策情報の公表マニュアル  JP	ソフトウェア製品に脆弱性が発見され、修正した脆弱性情報をウェブサイト上で公表する際に考慮すべき内容を開発者向けの情報としてまとめています。	開発者 管理部門	脆弱性情報が公開され、ソフトウェア製品の利用者が対応する際に必要としている情報が、項目ごとに説明されています。 記載例と併せて参照することで、ソフトウェア製品の利用者に、脆弱性情報を適切に伝えることの理解を深めるために活用いただける資料です。

7. 1　IPA脆弱性対策のためのコンテンツ – 資料として提供(続き) –

名称	概要	利用対象	活用方法
ウェブサイト運営者のための脆弱性対応ガイド  JP	ウェブサイトの脆弱性がもたらす具体的なトラブルや運営者に問われる責任、ウェブサイトに求められる継続的な対策、脆弱性が見つかった場合の対応手順などを概説し、実際に脆弱性に関する通知を受けた場合の望ましい対応手順を脆弱性対応マニュアルとしてまとめています。	運営者 経営者 管理部門	ウェブサイトの運営において起こり得る問題の解説から問題発生時の対応手順などの理解に活用可能な資料です。ウェブサイト運営者やウェブサイトを持つ企業の経営層の方向けの資料です。
ウェブサイト構築事業者のための脆弱性対応ガイド  JP	情報サービス企業の技術者やウェブデザイナー、企業内でウェブサイト構築・運用を担当する技術者向けにシステムの納入前や納入後に考慮すべきことをまとめています。 また、ウェブサイト構築における問題に対応するため、ウェブサイトの責任者向けに脆弱性対策の重要性を簡潔に記したパンフレット「情報システムを安全にお使いいただくために」を作成しました。	開発者 経営者	ウェブサイト構築事業者がウェブサイト構築を請け負う場合に、どのような点に留意すべきか理解したい場合に活用可能な資料です。技術者だけでなく、ウェブ構築事業に携わる様々な部門の方に活用いただける資料です。
セキュリティ担当者のための脆弱性対応ガイド  JP	組織内で脆弱性対策の知識を必要とするセキュリティ担当者を対象とし、脆弱性に起因するトラブルや影響の事例、事業者に委託する際の考え方などを含めた、全般的な脆弱性対策を解説しています。	運用・保守 管理部門	セキュリティ担当者に期待される事項や、組織で行なうべきセキュリティ対策などがまとめられており、セキュリティ担当者の教科書的な資料です。
地方公共団体のための脆弱性対応ガイド  JP	「情報システム等の脆弱性情報の取扱いに関する研究会」の活動成果として、地方公共団体の脆弱性対策の実態を把握するとともに、その取り組みを促すための資料です。	開発者 管理部門 運用・保守	地方公共団体の職員が本ガイドを読むことで、脆弱性対策への考え方や、脆弱性が発見される以前に検討しておくべきことを知ることができます。

7. 1　IPA脆弱性対策のためのコンテンツ – 資料として提供(続き) –

名称	概要	利用対象	活用方法
ファジング活用の手引き  JP	ソフトウェア製品の脆弱性を検出する技術の一つ「ファジング」の概要、実践方法および製品開発組織におけるファジングの活用方法などをまとめた資料です。IPA における「脆弱性検出の普及活動」で培ったノウハウを基に、「ファジング活用によりどんな効果が得られるか」「どのようにファジングを実践すればよいか」などファジング実践のために必要な知識をまとめています。	開発者	ファジングとは何かという概要から、ファジングの一般的な活用方法、ファジングツールの紹介などをまとめており、ファジングを理解したい場合に有効な資料です。
別冊「ファジング実践資料」 ・ファジング実践編 ・UPnP編 ・テストデータ編 ・AFL編  JP	「ファジングを試したい」時にオープンソースソフトウェアなどを活用し、すぐにファジングを実践できるよう「ファジングツールの使い方」などをまとめた資料です。 「ファジング実践編」「UPnP編」「テストデータ編」「AFL編」の4種類の資料があります。	開発者	ファジングを実践する際に、以下の内容について具体的に理解したい場合に有効です。 ・「ファジングツールの使い方（オープンソースソフトウェアなど）や、ファジング結果の再現方法」 ・「UPnP機能へのファジング実践方法と、UPnP機能の仕組み」 ・「テストデータ作成の考え方や、テストデータの活用方法」
脆弱性対処に向けた製品開発者向けガイド  JP	製品開発者がセキュリティ対策として実施すべき項目をまとめたガイドです。 実施内容を最大3段階にレベル分けしているため、組織の状況に合わせて対応することができます。 また、一般消費者に自組織の取組み状況をアピールするために実施すべきことも記載されています。 主に中小規模の一般消費者向け製品の開発者を対象としています。	開発者 運用・保守 管理部門 経営者	ガイドの最後に実施状況を確認するためのチェックリストを付けています。組織の製品開発プロジェクトマネージャーが現状と課題を把握し、上長に報告するなどに活用できます。
制御システム利用者のための脆弱性対応ガイド  JP	制御システム分野のソフトウエア製品の脆弱性情報を、制御システムの利用者が受取った場合を想定し、脆弱性対策を含むセキュリティについてどのように対応すべきかを解説しています。	利用者 管理部門 経営者 運用・保守 開発者	制御システムを利用している企業の経営層が事業継続計画を策定する際に考慮すべき点、また調達・運用担当の管理者が具体的な対策として制御システムの安全な運用に求められる事項や運用時に注意すべき点についてまとめています。

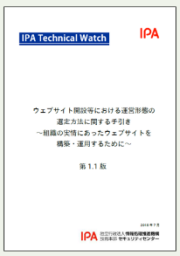
7. 1　IPA脆弱性対策のためのコンテンツ – 資料として提供(続き) –

名称	概要	利用対象	活用方法
制御システムのセキュリティリスク分析ガイド  JP	サイバー攻撃に対するリスクを低減し、セキュリティレベルを向上するリスクアスメントについて、制御システムを題材に具体的な手順を解説した実践的な手引きです。ガイドで紹介している分析手法と手順を用いたリスクアセスメントの実施例である「別冊：制御システムに対するリスク分析の実施例」や、実施時にそのまま活用できる分析フォーマット等の素材も提供しています。なお、本ガイドで示す分析手法と手順は、一般の情報システムにも適用できます。	開発者 運用・保守 管理部門	リスクアセスメントの全体像、具体的な実施手順、結果の活用方法を学ぶことができ、自組織におけるリスクアセスメントの実践や、外注時のリファレンス等に役立てることができます。
制御システム関連のサイバーインシデント事例  JP	制御システムで発生したサイバーインシデント事例について、公的機関の公開情報等をもとに、サイバー攻撃事例の概要と攻撃の流れを紹介する資料のシリーズです。 【#1】2015年 ウクライナ 大規模停電 【#2】2016年 ウクライナ マルウェアによる停電 【#3】2017年 安全計装システムを標的とするマルウェア 【#4】Stuxnet：制御システムを標的とする初めてのマルウェア 【#5】2019年 ランサムウェアによる操業停止 【#6】2018年 半導体製造企業のランサムウェアによる操業停止 【#7】2020年 医療関連企業のランサムウェアによる業務停止 【#8】2021年 水道局への不正侵入と飲料水汚染未遂 【#9】2021年 米国最大手のパイプラインのランサムウェア被害 【#10】2022年 衛星通信網へのサイバー攻撃 【#11】2022年 電力網への攻撃	開発者 運用・保守 管理部門	「制御システムのセキュリティリスク分析ガイド」で紹介している事業被害ベースのリスク分析を実施する際、過去に発生した攻撃事例に相当する攻撃ツリーを作成し、自社の制御システムに対する類似の脅威のリスク分析の実施やセキュリティ対策の策定に活用することができます。

7. 1　IPA脆弱性対策のためのコンテンツ – 資料として提供(続き) –

名称	概要	利用対象	活用方法
[ドイツBSI] 産業用制御システム(ICS)のセキュリティ 10大脅威と対策 2022  JP	ドイツ連邦政府 情報セキュリティ庁(BSI)が作成した「Industrial Control System Security - Top 10 Threats and Countermeasures 2022」の日本語訳です。 制御システムにとって危険度の高い10種類の脅威について、問題と原因、潜在的な脅威のシナリオ、対策を解説しています。また、制御システムを保有する事業者のセキュリティレベルを自己評価できるチェックリストが付属しています。	開発者 運用・保守 管理部門 経営者	制御システムに対して発生し得る脅威とその発生要因、具体的な手口、対策を体系的に理解することができます。 また、セルフチェックリストを用いて、自組織の現状把握ができ、対策の方針検討に着手することができます。
脆弱性体験学習ツール「AppGoat」を用いた集合教育実施の手引き  JP	脆弱性体験学習ツール「AppGoat」は、個人での自己学習だけではなく、大学での講義や組織の社内教育向けセミナー等といった複数人への集合教育にも活用できます。 本資料はAppGoatを使った集合教育を効果的に進めていくための段取りや事前に検討しておくべきポイント等を解説しています。	運営者 開発者 運用・保守	脆弱性体験学習ツール「AppGoat」を使った集合教育の実施を検討する際に、本資料を一読いただくことで、効率よく集合教育の準備を進めることができます。
AppGoatを利用した集合教育補助資料  JP	脆弱性体験学習ツール「AppGoat」は、個人での自己学習だけではなく、大学での講義や組織の社内教育向けセミナー等といった複数人への集合教育にも活用できます。 AppGoatのみを使って集合教育を行うこともできますが、AppGoatの説明を本資料と組み合わせて説明することで、より理解度を高めることが期待できます。(2020年3月末時点で7資料公開中)	運営者 開発者 運用・保守	脆弱性体験学習ツール「AppGoat」を使った集合教育を行う際に本資料を合わせて配布または投影することで、学習者の脆弱性の理解度を高めることを期待できます。
ソフトウェア脆弱性関連情報管理シート  JP	Microsoft Excel上で組織で利用しているソフトウェアの一覧をまとめ、さらに収集した脆弱性関連情報を管理するためのサンプル資料です。どのようにして脆弱性対策情報を収集したらよいかわからない方向けに、Microsoft Excelを使った場合の脆弱性関連情報の収集イメージを理解することができます。	運用・保守	Microsoft Excelに自組織で利用しているソフトウェアを入力して脆弱性関連情報の管理に活用できます。 また、組織の運用に併せて自由にカスタマイズして使うこともできます。

7. 1　IPA脆弱性対策のためのコンテンツ – 資料として提供(続き) –

名称	概要	利用対象	活用方法
脆弱性対策の効果的な進め方(実践編)  JP	広く普及しているソフトウェアに関する脆弱性情報の公開数は年々増加傾向にあります。システムの管理者やソフトウェアの開発者は、公表された脆弱性への対策として、利用しているソフトウェアのバージョンアップや、開発ソフトウェアへの対策プログラムの組み込みなどの適切な脆弱性対策が求められます。本書では、より効果的な対策を行う上での重要なポイントについて解説しています。	開発者 運用・保守	脆弱性対策を効果的に進めるため、脆弱性に関する情報をどのように収集するのが良いか、また収集した情報はどのように分析して対策に活用するのが良いか等についての概要を確認できます。
ウェブサイト開設等における運営形態の選定方法に関する手引き  JP	ウェブサイトを運営するにあたり、運営者はどのようにウェブサーバを運営するか、様々な運営形態から選択する必要があります。代表的な運営形態の特徴と、組織が安全にウェブサイトを運営可能な運営形態を選択するための観点について解説しています。	経営者 管理部門 開発者 運用・保守 運営者	これから新たにウェブサイトを開設する組織が運営形態の選択を検討する場合だけでなく、既にウェブサイトを運営している場合の運営状態の見直しや、ウェブサイトを更改する際にも活用していただけます。
安全なウェブサイト運営にむけて～企業ウェブサイトのための脆弱性対応ガイド～  JP	中小企業のウェブサイト運営者が、ウェブサイト(ホームページ)をサイバー攻撃から守り、安全に運用するために大切な「脆弱性対策のポイント」を解説しています。 また、脆弱性がもとで起きた被害事例や、脆弱性対策のための参考資料・チェックリストも紹介しています。	経営者 管理部門 開発者 運用・保守 運営者	「脆弱性対策のポイント」とあわせて、参考資料やチェックリストを参照することで、運用中ウェブサイトの脆弱性対策の状況確認や、実施した方がよい脆弱性対策の洗い出し等に活用できます。
ウェブサイト運営のファーストステップ～ウェブサイト運営者がまず知っておくべき脅威と責任～  JP	「ウェブサイト運営のファーストステップ」は、ウェブサイトを運営する上で、まず知っておく必要がある脅威や運営者の責任といった基礎知識を、登場するキャラクターの会話を通じて分かりやすく解説しています。	運営者	ウェブサイトを運営する上で避けては通れない脅威や責任について学んでいただき、安全なウェブサイト運営を検討するためのきっかけとして、ご活用いただくことを目的としています。

7. 1　IPA脆弱性対策のためのコンテンツ – 資料として提供(続き) –

名称	概要	利用対象	活用方法
ネット接続製品の安全な選定／利用ガイド  JP	インターネットに接続する製品の選定時、利用時のセキュリティに関する確認ポイント7つを、イラストで分かりやすく記載したガイドです。 また、確認ポイントや確認場所、実施しなかった場合の影響などを詳しく解説した「詳細版」へのリンクも掲載しています。合わせて参照することで、より理解度を高めることができます。	利用者	ポイント7つを確認することで、家電量販店やEC サイトなどで製品を購入する際に、安全な製品を選んだり、購入した製品を安全に利用したりするきっかけとして、活用できます。
IoT開発におけるセキュリティ設計の手引き  JP	IoT開発において、セキュリティ設計を担当する開発者が実施すべき脅威分析・対策検討・脆弱性への対応について解説している資料です。設計段階からセキュリティを考慮した開発(セキュリティ・バイ・デザイン)を支援することにより、セキュアなIoT製品・サービスの普及の促進を目的としています。	開発者	IoT製品の提供において必要となるセキュリティ上の検討事項や対策について、包括的に理解することができます。また、本書で紹介している国内外のIoTセキュリティガイドや、付録の「IoTにおける暗号技術のチェックリスト」を参考に、自社の対策状況や実装が適切か、チェックすることができます。
IoT製品・サービス脆弱性対応ガイド  JP	安全安心なIoT製品・サービスを提供するために、企業の経営者・管理者が実施すべきIoT脆弱性対策のポイントを理解するための資料です。脆弱性対策の取組状況や課題、脆弱性による問題発生時の被害や知見など IoT製品・サービス開発者における脆弱性対策の促進を目的としています。	経営者 開発者 運用・保守	IoT製品・サービスの提供における、セキュリティ対応に対する企業の責任の考え方や、脆弱性対策が必要な理由等を解説し、企業としてセキュリティ対応に取り組んでいただく必要性を理解していただく場合に活用できます。
ECサイト構築・運用セキュリティガイドライン  JP	ECサイトを構築、運営されている中小企業の皆様に、ECサイトのセキュリティ対策を実施することがいかに重要であるかを認識いただき、ECサイトのセキュリティ確保のために経営者が実行すべき項目や、セキュリティ対策を担当される実務担当者が具体的に実践すべきセキュリティ対策の内容を、パッケージやスクラッチ開発による自社構築サイトを中心に記載しています。	経営者 運営者 運用・保守	「第1部　経営者編」は、ECサイトを新規に構築しようとしている、あるいは既に運営している経営者が、自社のECサイトにおけるセキュリティ対策の必要性を認識していただく資料です。 「第2部　実践編」は、ECサイトにおけるセキュリティ対策を実践する責任者および担当者が、ECサイトの構築時および運用時に、必要なセキュリティ対策を検討する上で、優先する対策や自社のECサイトの状況に見合った実践すべき対策の範囲や実現方法を適切に決めていただくための資料です。

7. 2 IPA脆弱性対策のためのコンテンツ – ツールとして提供 –

名称	概要	利用対象	活用方法
ウェブサイトの攻撃兆候検出ツール「iLogScanner」 JP 	自組織が管理しているウェブサイトにおいて、悪意ある利用者より攻撃されている可能性がないかを確認するツールです。SQLインジェクションなどのウェブサイトの脆弱性を狙った攻撃やSSHやFTPなどのメンテナンス用に利用しているアプリケーションを狙った攻撃の兆候をチェックすることができます。	開発者 運用・保守	利用者は、ウェブサイトのログやSSH、FTPのログを収集し、そのログを「iLogScanner」に取り込むことで、出力されるレポートからウェブサイトに関わる攻撃の兆候を確認することができます。 定期的に確認を行うことで、ウェブサイトへの攻撃状況を把握することができ、脆弱性対策を早期に行うなどの適切な対応を行う指針として活用することができます。
脆弱性体験学習ツール AppGoat JP 	脆弱性の検証手法から原理、影響、対策までを演習しながら学習できる体験型学習ツールです。 学習テーマ毎に用意された演習問題を通して、埋め込まれた脆弱性の発見、プログラミング上の問題点の把握、対策手法などについて対話的に学習できます。	開発者	学生から技術者まで様々なレベルの利用者が脆弱性の発見／検証の方法から対策までを実習形式で体系的に学習できます。
知っていますか？脆弱性 JP 	ウェブサイトの脆弱性（ソフトウェア等におけるセキュリティ上の弱点）について理解を深めていただくための、ウェブサイトの脆弱性を分かりやすく解説するコンテンツです。	運営者 開発者	脆弱性についての理解を広め、対策の普及・向上を図るため、代表的な10 種類の脆弱性を、わかりやすく、アニメーションで解説しています。
5分でできる！情報セキュリティポイント学習 JP 	各企業の現状に即した情報セキュリティ対策を学習できるツールとして、主に中小企業の方を対象にした情報セキュリティ学習ツールです。 職場の日常の1コマを取り入れた親しみやすい学習テーマで、セキュリティに関する様々な事例を疑似体験しながら正しい対処法を学ぶことができます。学習時間は1テーマあたり5分程度です。	管理部門 運営者 運用・保守 利用者	学習テーマは、「メールについて」「バックアップについて」「ウイルス対策について」「個人所有端末について」等があり、事例を疑似体験しながら学習できます。 学習後にはその内容に関する確認テストを用意しており、学習結果の理解度をチェックできます。 学習テーマは、「5分でできる！情報セキュリティ自社診断」25診断項目に対応コースや職種などで分類されたコースとして提供しています。

7. 3 IPA脆弱性対策のためのコンテンツ － その他 －

IPA テクニカルウォッチ

JP EN

- IPAテクニカルウォッチはIPAが公開している技術レポートです。毎回テーマを設定し、そのテーマに関連する状況や課題などを分析・解説しています。
- レポートはセキュリティに関する技術的な分析、調査・レポート、また対策の紹介など、技術部門にとどまらず様々な職種に役立つ情報を公開しています。

https://www.ipa.go.jp/security/reports/technicalwatch/index.html

IPA Technical Watch

映像で知る情報セキュリティ ～映像コンテンツ一覧～

JP

- IPAでは情報セキュリティに関する脅威や対策などを学んでいただくための映像コンテンツを、YouTube内の「IPA Channel」を通じて公開しています。
- 技術的な解説や、新入社員・小学生／中高生を対象とした教材、一般のユーザ向けの啓発動画など、様々な職種を対象とした動画を公開しています。社内研修などで活用いただくことも可能です。
  https://www.ipa.go.jp/security/videos/list.html

その他

情報セキュリティ･ポータルサイト「ここからセキュリティ！」

ー情報セキュリティを「始める」「学ぶ・教える」「強化」するポータルサイトー

https://www.ipa.go.jp/security/kokokara/

- 経済産業省を始め、総務省、警察庁などの関係省庁と、国内のセキュリティや通信に関連した団体、民間企業のコンテンツを集約したコンテンツを公開しています。
- 脅威の名称とその現象を一つにまとめ、利用者がセキュリティ初心者であっても、自身の情報を守るために有効なセキュリティ情報に簡単にたどり着けるよう分類しています。

情報セキュリティに関する届出について

IPAセキュリティセンターでは、経済産業省の告示に基づき、コンピュータウイルス・不正アクセス・脆弱性関連情報に関する発見・被害の届出や、標的型攻撃に関する相談・情報提供などを受け付けています。

ウェブフォームやメールで届出ができます。詳しくは下記のサイトを御覧ください。
URL: https://www.ipa.go.jp/security/todokede/index.html

コンピュータウイルス・不正アクセス情報

コンピュータウイルスを発見またはコンピュータウイルスに感染した場合や、ネットワーク（インターネット、LAN、WAN、パソコン通信など）に接続されたコンピュータへの不正アクセスによる被害を受けた場合に届け出てください。

ソフトウェア製品脆弱性関連情報

OSやブラウザ等のクライアント上のソフトウェア、ウェブサーバ等のサーバ上のソフトウェア、プリンタやICカード等のソフトウェアを組み込んだハードウエア等に対する脆弱性を発見した場合に届け出てください。

標的型サイバー攻撃の特別相談窓口

標的型メールを受け取った際の相談窓口です。また、標的型メール攻撃についての情報提供を受付けています。また、限られた対象にのみ行われる標的型メール攻撃については、その手口や実態を把握するために、情報提供をお願いしています。

ウェブアプリケーション脆弱性関連情報

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そのサイト固有のサービスを構成するシステムに対する脆弱性を発見した場合に届け出てください。

IPA Better Life with IT

独立行政法人**情報処理推進機構**
セキュリティセンター