IPA Better Life with IT

見落としていませんか？
セキュリティ対策
～ウェブサイトに必要な対策とは～

2018年 5月9日・11日
独立行政法人情報処理推進機構（IPA）
技術本部 セキュリティセンター
脆弱性分析エンジニア　熊谷 悠平

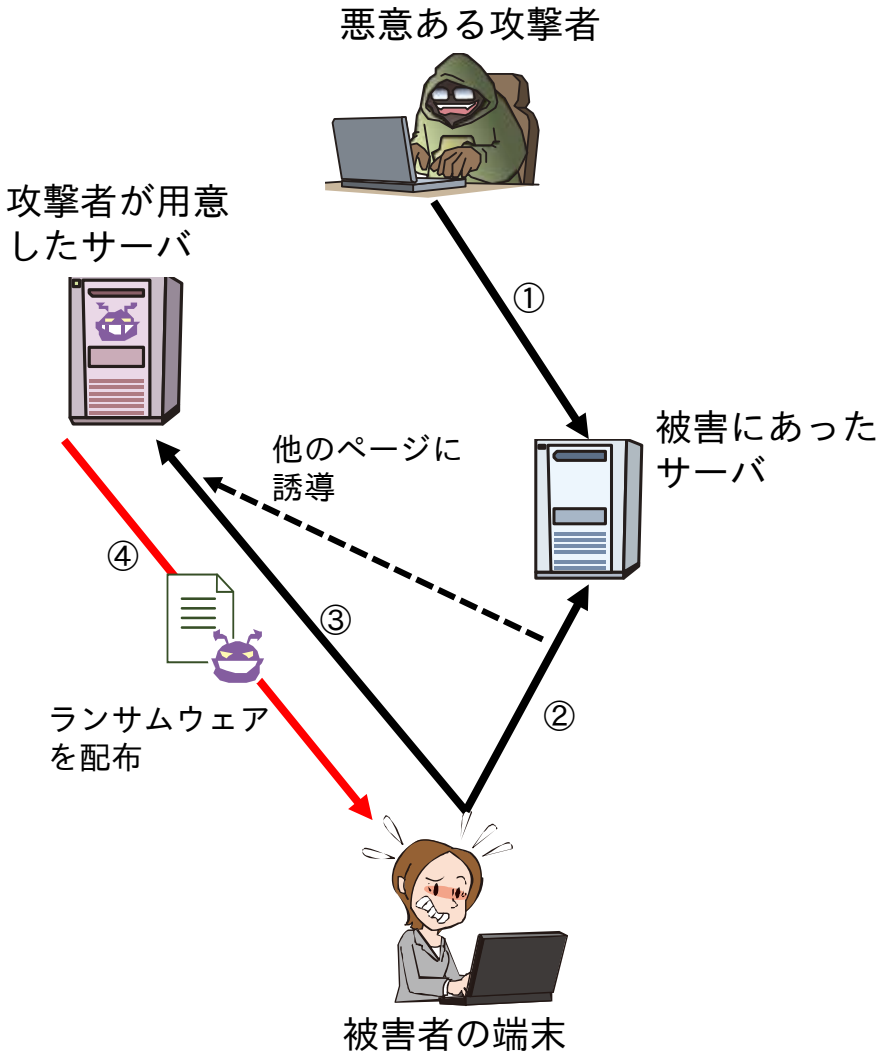
2017～2018年のウェブサイトにまつわる報道事例

時期	報道
2017/6	香川県立保健医療大のサイトに不正アクセス - 一部が改ざん(Security Next)
2017/8	HIS、最大1万人超の個人情報流出　バスツアー予約サイトから(ITmedia News)
2017/9	東京ガスに大量の不正アクセス、情報流出の恐れも(ZDNet Japan)
2017/9	東京ガスに再びリスト型攻撃、個人情報流出とポイント不正使用の疑い(日経BP)
2017/10	160人の個人情報流出か　島根大図書館システム不備(産経WEST)
2018/1	サイト改ざんが判明、外部へ誘導される状態に - 知多半島ケーブルネットワーク(Security Next)
2018/2	福岡放送 HPにサイバー攻撃　153人のメアド盗み見る(毎日新聞)
2018/3	健診1万2千人分の情報流出か　兵庫・尼崎市の委託サイト(産経WEST)
2018/4	前橋市教委 不正アクセス　2万人超の個人情報流出(毎日新聞)

どんなウェブサイトが狙われるかわからない！

2017年の大きな事件 ～改ざんによる利用者の誘導～

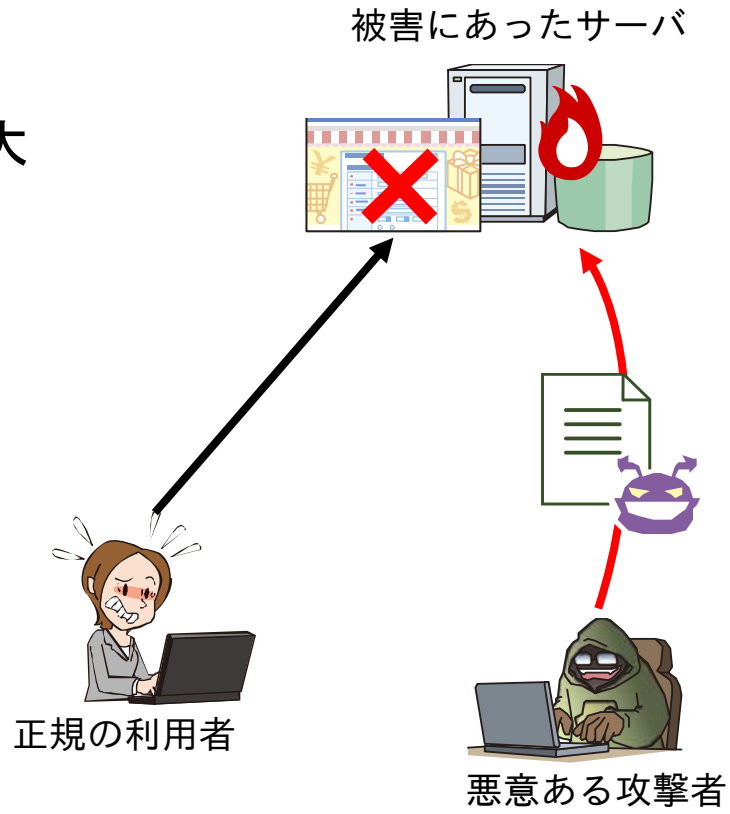
- ウェブサイトの設定を改ざん
  - 利用者を不正サイトへ誘導
  - ランサムウェアの配布サイト
    - **感染者の端末が使用できなくなる**
  - 修正・対策で1ヶ月サイト停止
- メンテナンス経路に問題
  - ファイアウォールの設定不備
  - SSH通信にセキュリティ上の脆弱性



2018年の大きな事件(1)
～マイニングツールの不正実行～

- 予約ページに接続しずらい事象
  - 運営者がサーバ上で不審な処理を確認
  - 不正なファイルがアップロードされている ことを確認
  - 不正な処理により、サーバへの負荷が増大

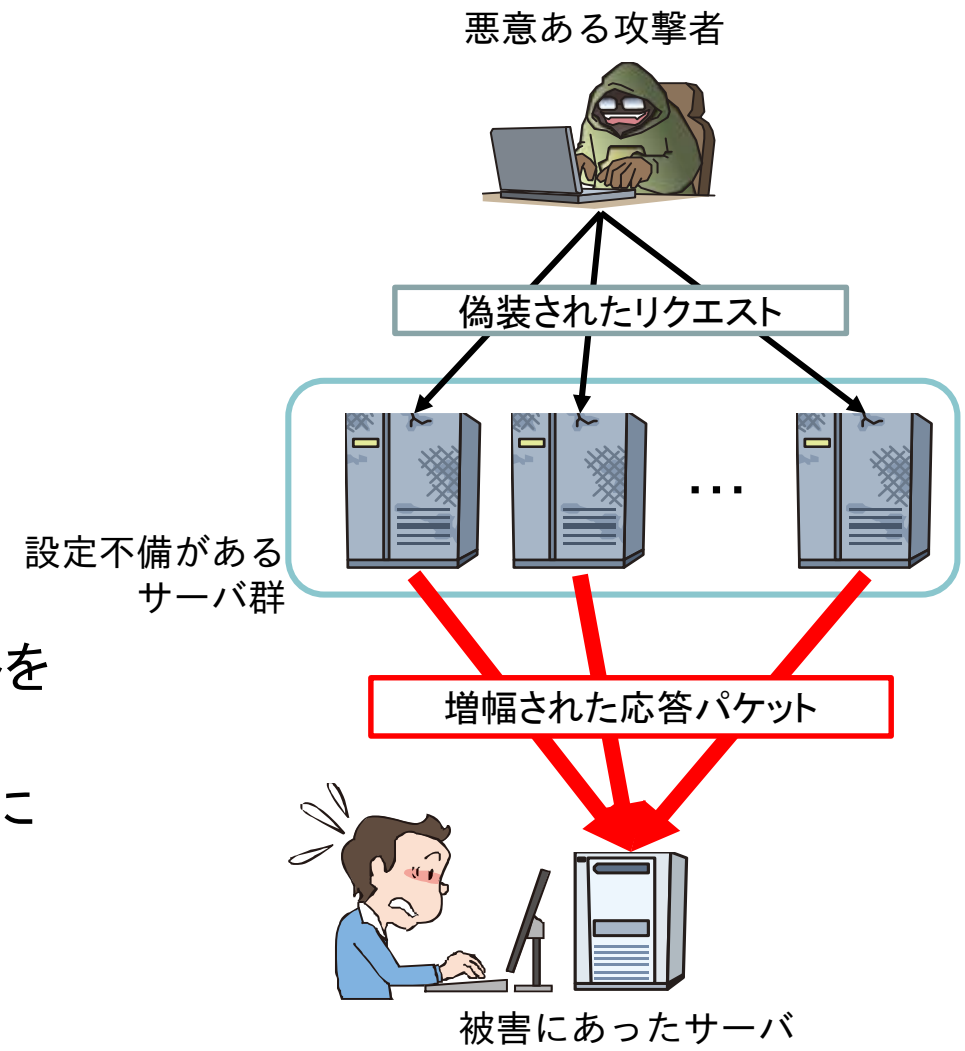
- インターネットからの不正アクセス が原因
  - 推測可能なパスワードの使用
  - IPアドレスによる制限がなかった
  - 再発防止策の実施、運用体制の 見直し等でサービスが2ヶ月停止



2018年の大きな事件(2)
～サーバ設定不備を攻撃に悪用～

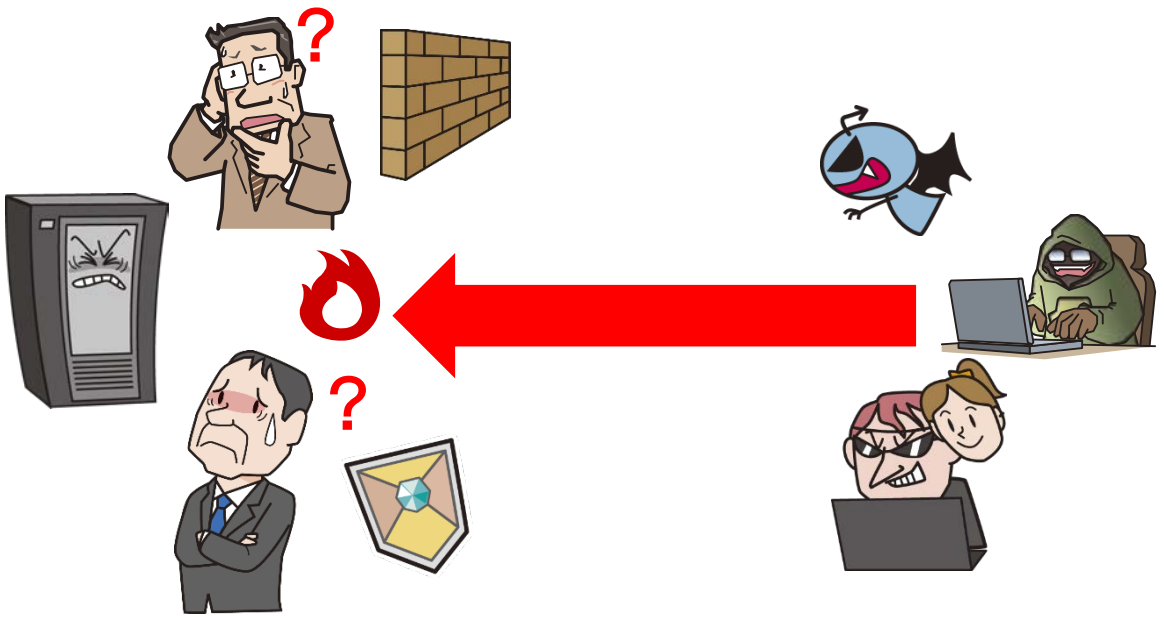
- 2月28日に有名サービスを標的としたDDoS攻撃が発生
  - サービスが断続的に利用不能に
  - 瞬間的に1.3TBの通信が発生

- 複数のサーバを踏み台にしたDDoS攻撃
  - 「memchached」の設定不備
  - 設定不備で外部からのリクエストを受け付けるサーバが存在
  - サーバ管理者が気づかないうちに攻撃に加担させられた
  - レンタルサーバ業者から警告を受けた例も



ウェブサイトへの攻撃に対して

- 何に注意すればいいの？
- どのような対策が必要になるの？



ウェブサイトの運営にかかわる各段階で
検討すべき項目は変わります。

ウェブサイト運営の流れと対策抜粋

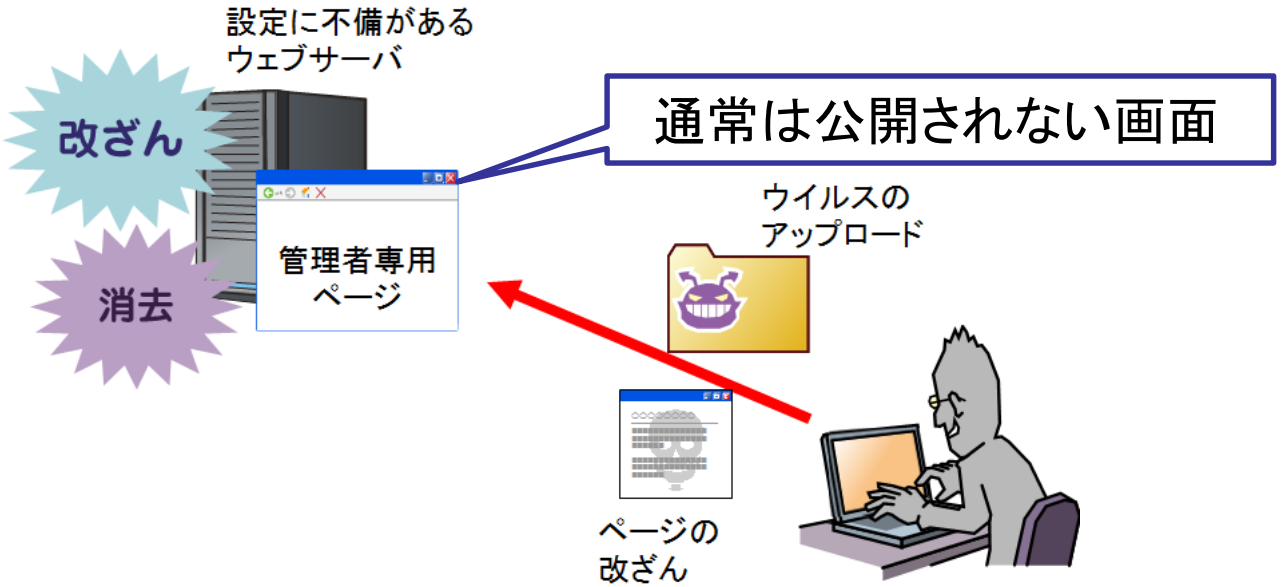
1.企画	・個人情報の保護等、セキュリティ要件の定義 ・運用体制の検討
2.設計	・セキュリティ上の脅威の分析 ・脆弱性を作りこまない設計
3.実装/構築	・使用するソフトウェアの脆弱性調査 ・セキュアプログラミング
4.テスト	・脆弱性診断 ・ペネトレーションテスト
5.運用/利用	・ログ等からの攻撃兆候の監視 ・定期的なアップデートの実施
6.廃棄	・データや記録媒体の安全な破棄の実施

脆弱性の原因ケース1

誤った設定で運用していた

- **管理者用**のページがインターネットに公開されていた
- **適切なアクセス制限**が行われていなかった
- **不必要なファイル**を削除していなかった
- 簡単なパスワードを使用していた

個人情報が記載されたファイルが公開されていた場合も

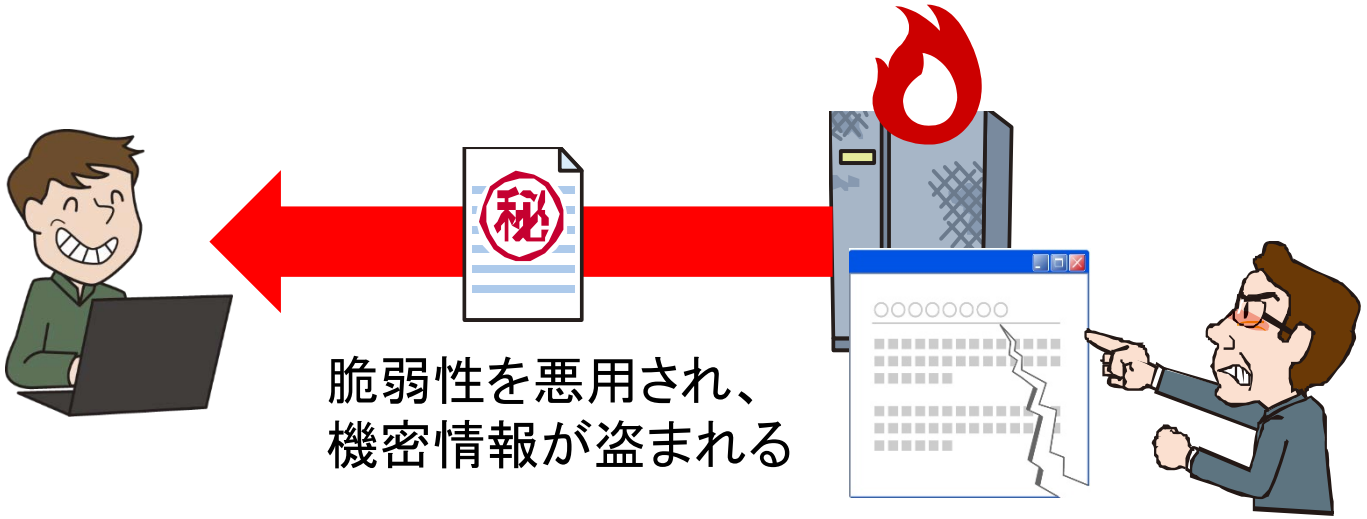


脆弱性の原因ケース2

ウェブアプリケーションに脆弱性がある

- 独自開発のウェブアプリケーションに脆弱性が存在
- **脆弱性対策**を考慮しない開発
  例：脆弱性の検査を行っていない、等

開発元に修正を依頼する必要があり、
修正に時間がかかることがある。



脆弱性を悪用され、
機密情報が盗まれる

脆弱性の原因ケース3

脆弱性が存在する製品を利用

- **脆弱性が存在する製品**を利用していることが原因

- 脆弱性が報告されても、利用者が放置することがある
- 有名な製品の脆弱性が報告されると、攻撃が急増することも

✓ 脆弱性があるソフトウェアの例

- アンケートプログラム
- 日記プログラム
- ウェブフレームワーク
- コンテンツ管理システム　等

✓ 存在していた脆弱性

- クロスサイトスクリプティング
- ディレクトリトラバーサル
- SQLインジェクション　等

安全なウェブサイトの作り方の概要

IPA 安全なウェブ

ウェブサイトの運営に関わる全ての人に向けた内容

- ✓ “**11種類の脆弱性**”の説明とその対策を説明
- ✓ 運用面からのウェブサイト全体の安全性を向上させるための方策を説明
- ✓ 7版から“パスワードの運用方法”の内容を拡充
- ✓ ウェブセキュリティの対策状況を把握ができるチェックリストつき

11種類の脆弱性

1	SQLインジェクション
2	OSコマンド・インジェクション
3	パス名パラメータの未チェック／ディレクトリ・トラバーサル
4	セッション管理の不備
5	クロスサイト・スクリプティング
6	CSRF（クロスサイト・リクエスト・フォージェリ）
7	HTTPヘッダ・インジェクション
8	メールヘッダ・インジェクション
9	クリックジャッキング
10	バッファオーバーフロー
11	アクセス制御や認可制御の欠落

高い危険性
・データベースやウェブサーバを不正操作
・内部データの 漏えい・改ざん・破壊

数多く見つかる脆弱性
・偽の情報が表示されたりする
・まれに、より深刻な脅威に繋がる

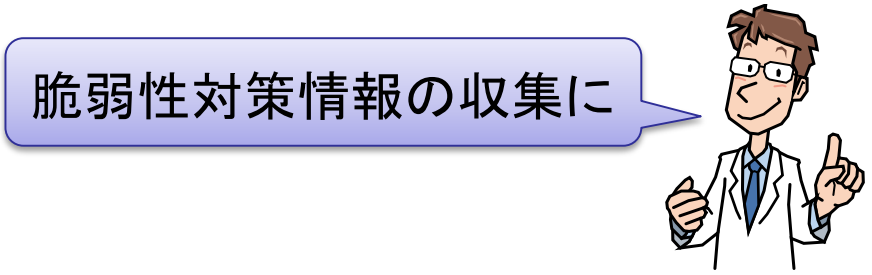
設定の改ざんに繋がる脆弱性
・利用者に意図しない操作をさせる
・登録情報の改変、設定の変更

脆弱性情報収集のために
脆弱性対策情報データベース JVN iPedia

- 脆弱性対策情報を蓄積するデータベース
  MyJVNの情報源。日本語版対策情報の登録件数は
  81,523件(2018年3月末)

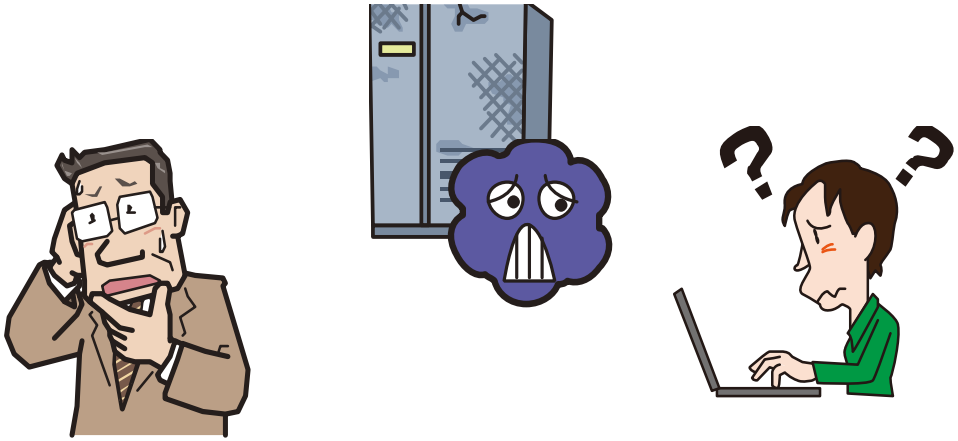
ipedia

公開される製品例
- Apache
- Tomcat
- MySQL
- SQL Server ・・・etc



対策が必要なのはわかったけど

- どんな対策が必要？
- どれぐらい予算がかかる？



ウェブサイトの種類によって、
運営者が実施できる対策が異なります。

ウェブサイトの運営形態の種類

運営形態	特徴	分類
モール	・ASP型のECサイトが複数集まっている形態	モール
ASP/ クラウド(SaaS)	・ウェブサイトに必要な機能をレンタルする形態	
レンタルサーバ/ クラウド(PaaS)	・保存領域とインフラの仮想環境をレンタルする形態 ・ソフトウェアの導入やサーバの運用は自社で実施	レンタル
クラウド(IaaS)	・ハードウェアをレンタルする形態 ・ソフトウェアの導入やサーバの運用は自社で実施	
データセンタ	・機器の設置場所をレンタルする形態 ・ソフトウェアの導入やサーバの運用は自社で実施	自社構築
オンプレミス	・自社の施設内で運用する形態 ・ネットワークやサーバを自社で用意する	

ウェブサイト毎にできる対策

対策	モール	レンタル	自社構築
ソフトウェアの更新	×	△	○
ウィルス対策製品の導入	×	△	○
パスワード・認証の強化	○	○	○
設定の見直し	×	○	○
脅威・手口を知る	○	○	○

お金をかけるだけがセキュリティ対策ではない！

追加で確認・検討すべき対策

分類	補足内容
モール	・どのような基準に沿ったセキュリティ対策を行っているか ・第三者の脆弱性検査や攻撃監視等を実施しているか
レンタル	・WAFや改ざん検知等のサービスの利用検討 ・アップデートやバックアップの定期取得等のメンテナンス計画 ・セキュリティ専門事業者による調査
自社構築	・物理的なセキュリティ対策の検討 ・運用体制やメンテナンス計画体制の構築 ・セキュリティ専門事業者による調査

WAF　・・・Web Application Firewall の略称。ウェブアプリケーションの脆弱性を悪用した攻撃からウェブアプリケーションを保護するセキュリティ対策の一つ。

まとめ

ウェブサイトを運営する組織にとって、サイバー攻撃は無視できない問題。
ウェブサイト運営者はセキュリティ対策を理解・実施する必要があります。

■まず、やってもらいたいこと
自社のウェブサイトについて
1. リスク分析を実施する(例：外部からの攻撃による情報漏洩)
2. 実施可能な対策を調査(例：サービス提供者のサービス等)
3. 優先して対処すべき問題を検討(例：金銭被害、社会的信用の失墜)

・人員や予算は有限
・どのような対策ができるか、ウェブサイト毎に異なる

「予算や人員がないから、やらない」ではなく、
何か起きて取返しが付かなくなる前に、
できる対策から実施することが必要。


IPA
Better Life
with IT