IPA Better Life with IT

ウェブサイトに必要なセキュリティ対策とは

2019年 5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
木村 泰介

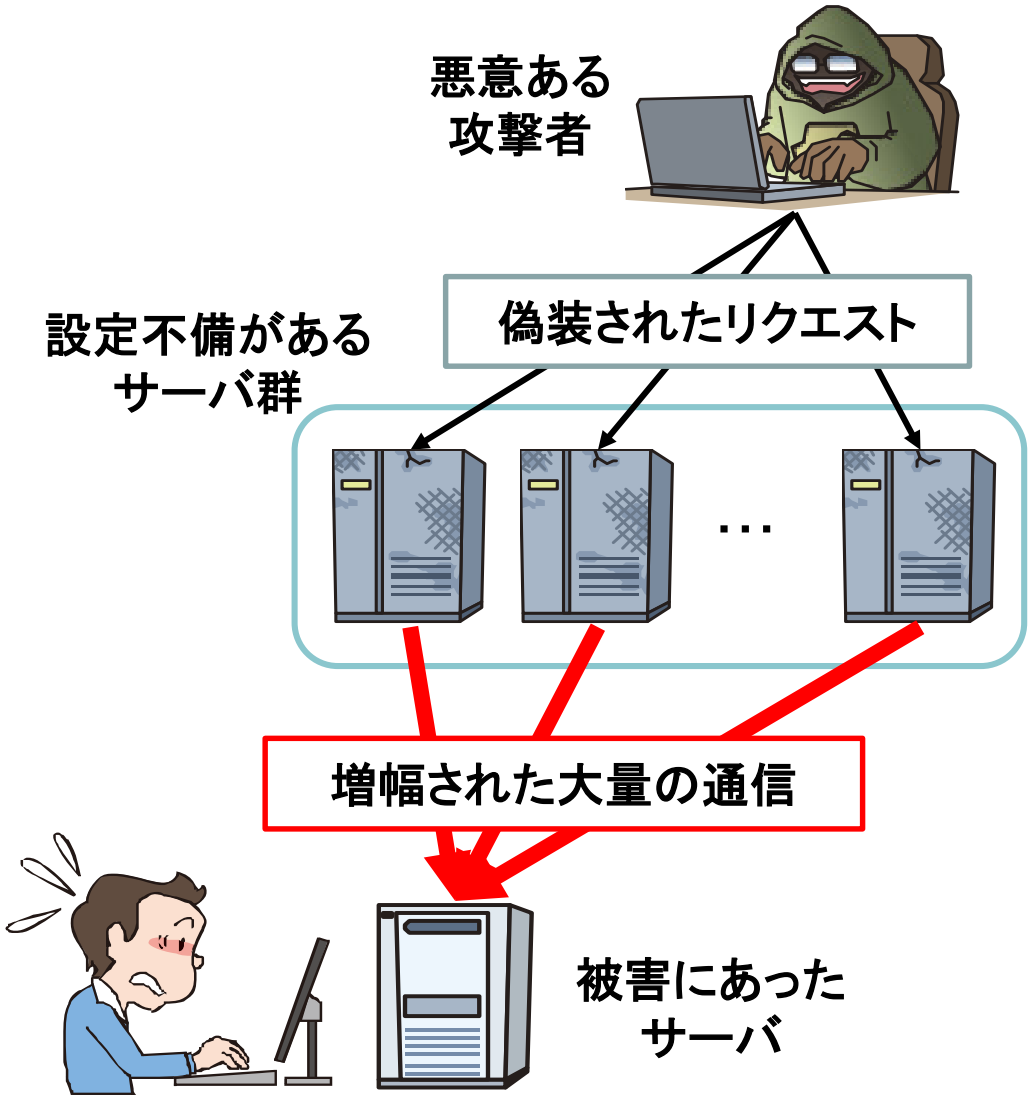
2018～2019年のウェブサイトに まつわる報道事例

時期	報道
2018/3	「memcached」利用した1.7Tbps規模のDDoS攻撃(Security Next)
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)
2018/6	1週間に2400件超のサイト改ざん － 詐欺サイト誘導の踏み台に(Security Next)
2018/7	「
2018/8	「
2018/9	Z
2018/10	F
2018/11	「おさいふPonta」にパスワードリスト攻撃、1時間に約30万件(Security Next)
2019/1	ホスティングサービスに不正アクセス、約5000サイトが改ざん(Security Next)
2019/2	法令遵守支援の会員向けサイトに不正アクセス － 日本貸金業協会(Security Next)
2019/3	予約システム「Coubic」に不正アクセス － 管理用PWを奪われる(Security Next)

ウェブサイトの個人情報や
金銭だけが標的ではない！

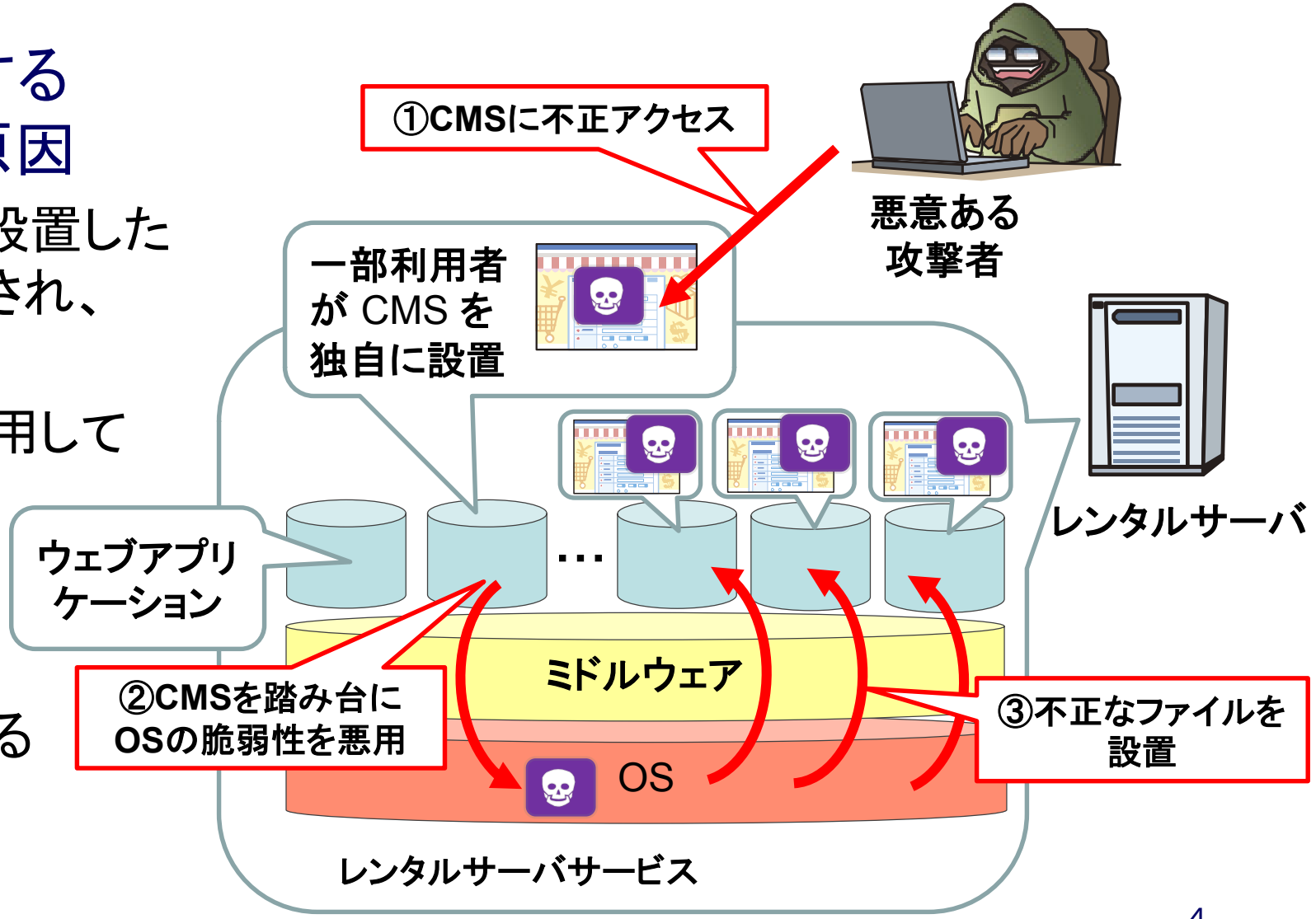
「memcached」利用した1.7Tbps規模のDDoS攻撃

- 複数のサーバを踏み台に利用して攻撃
  - 「memchached」の設定不備が原因
  - 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
- 有名サービスを標的とした DDoS 攻撃
  - サービスが断続的に利用不能に
  - 瞬間的に1.7TBの通信が発生



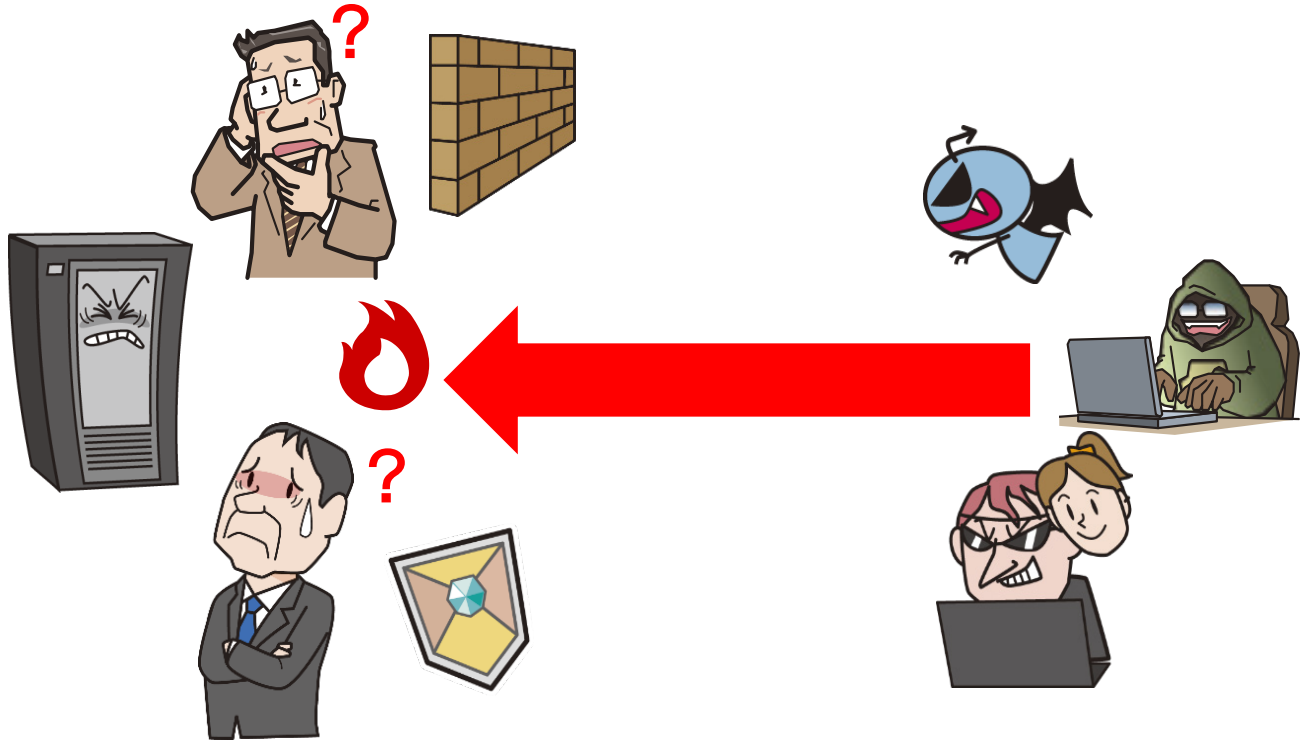
ホスティングサービスに不正アクセス、約5000サイトが改ざん

- レンタルサーバで稼働するサーバOSの脆弱性が原因
  - 特定の利用者が独自に設置したCMSのアカウントを侵害され、踏み台に利用される
  - サーバOSの脆弱性を悪用して不正なファイルを設置
- 約5000サイトが被害
  - 画像ファイルが設置される



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？



ウェブサイトの構築にかかわる各段階と、
ウェブサイトの種類によって、
検討すべき項目や対策は変わります

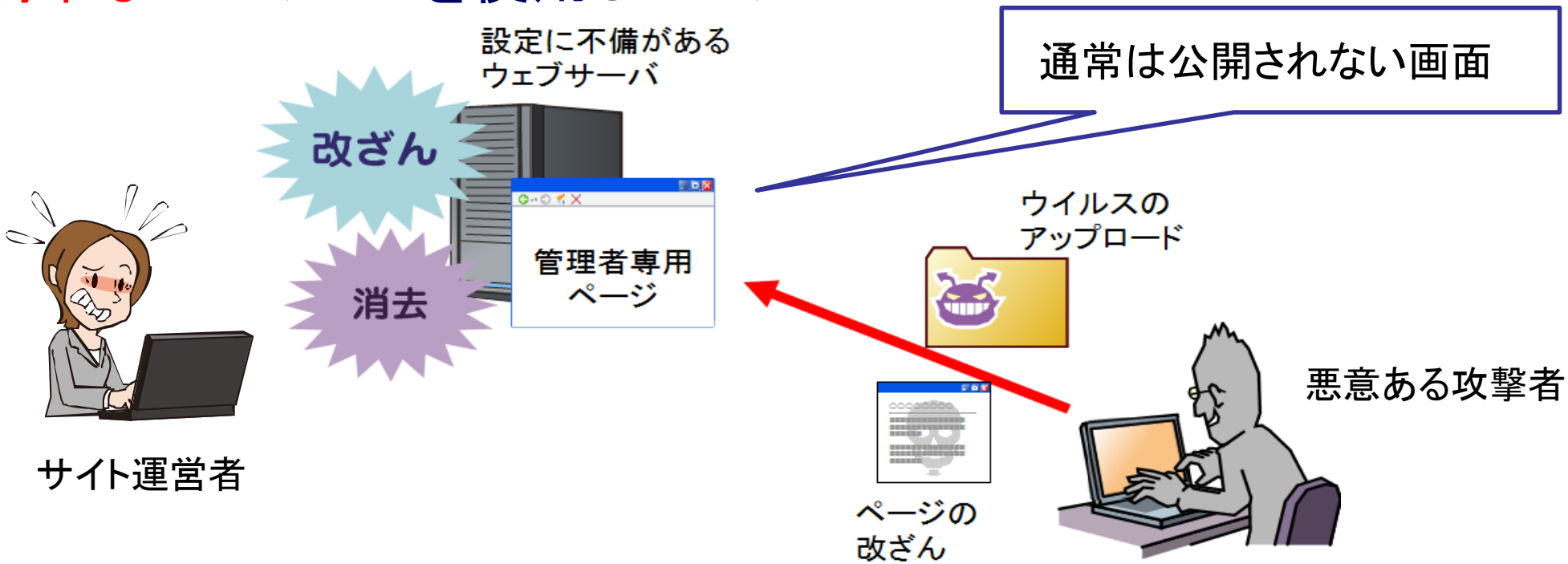
ウェブサイトの構築から運営における各段階と対策抜粋

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

誤った設定でウェブサイトを構築し、運営していた

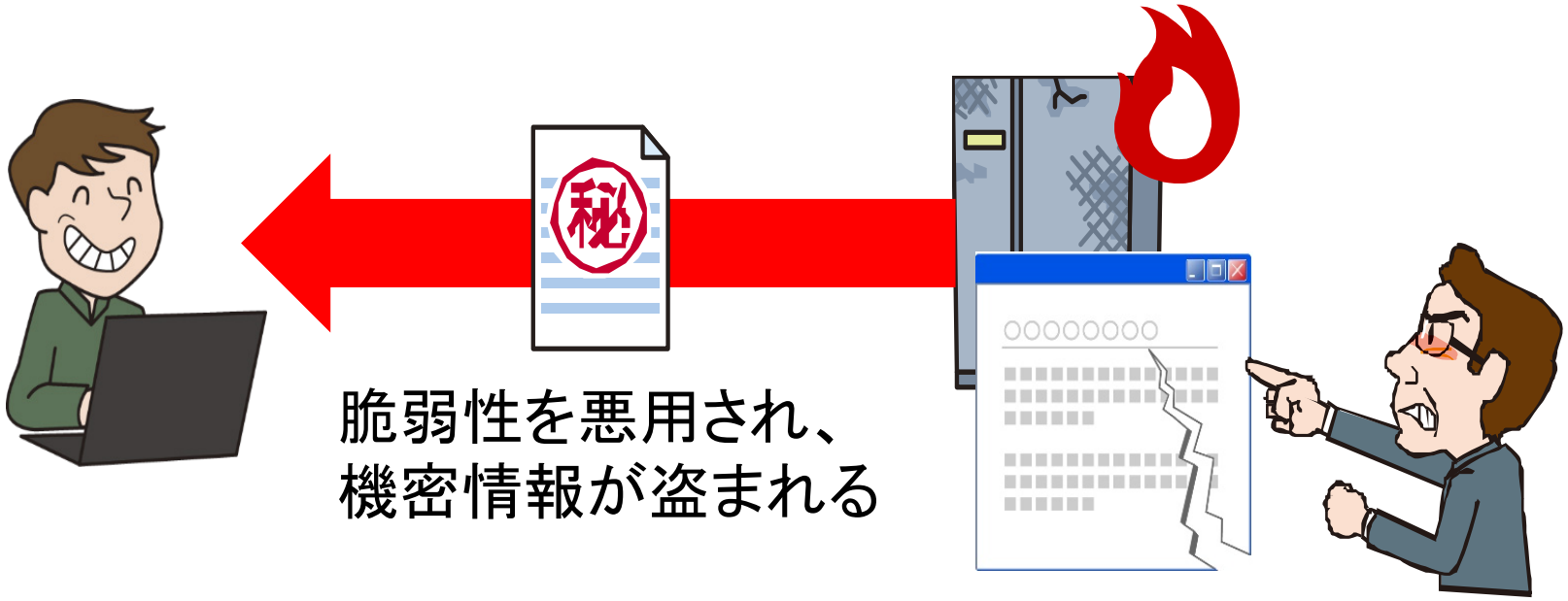
- 管理者用のページがインターネットに公開されていた
- 適切なアクセス制限が行われていなかった
- 不必要なファイルを削除していなかった
- 簡単なパスワードを使用していた



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



脆弱性を悪用され、
機密情報が盗まれる

安全なウェブサイトの作り方の概要

ウェブサイトの開発者や構築に関わる人に向けた内容

- ✓ “**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

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、攻撃が急増する場合もある

✓ 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

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 JVN iPedia
日本語版対策情報の登録件数は 97,444 件(2019年3月末)

登録されている製品例
- Apache
- Tomcat
- MySQL
- SQL Server ・・・etc

ipedia

脆弱性対策情報の収集に

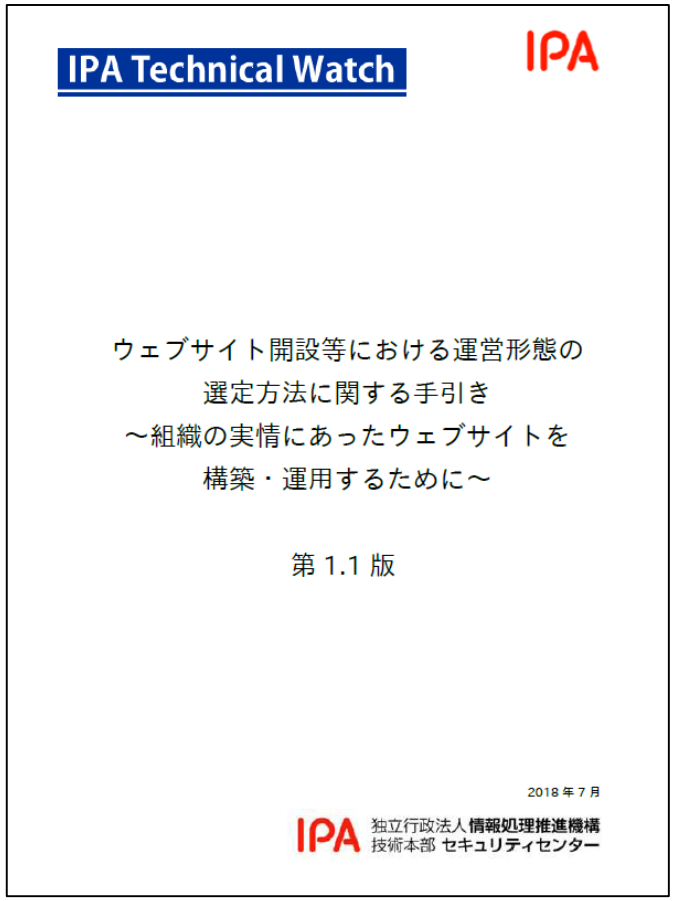
ウェブサイトの運営形態の種類

運営形態	特徴
モール	・ASP型のECサイトが複数集まっている形態
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
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
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

ウェブサイトの運営形態ごとにやらなければならない対策

対策	モール / ASP / クラウド(SaaS)	レンタルサーバ / クラウド(PaaS・IaaS)	データセンタ / オンプレミス
ソフトウェアの更新	サービス事業者	利用者 / サービス事業者	利用者
ウイルス対策製品の導入	サービス事業者	利用者 / サービス事業者	利用者
パスワード・認証の強化	利用者	利用者	利用者
設定の見直し	サービス事業者	利用者	利用者
脅威・手口を知る	利用者	利用者	利用者

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



IPA　ウェブサイト開設

- 運営組織の状況に即したウェブサイト運営形態の選び方を解説
- 運営形態毎の特徴や選定基準を記載
- 運営形態調達が必要な機材や管理責任の範囲を記載
- 運営形態毎に検討が必要なセキュリティ対策について紹介
- 実際の脅威への対策、障害対応の準備の必要性について記載

ウェブサイト開設時だけでなく、
運営中の対策漏れの確認にも

https://www.ipa.go.jp/security/technicalwatch/20180530.html

まとめ

◆ これからウェブサイトを開設する予定の方
1. 誤った設定でウェブサイトを構築しない
2. 脆弱性のあるウェブアプリケーションを作りこまない
3. 脆弱性がある製品を利用しない

◆ 既に自社でウェブサイトを運営している方
1. 自社の運営形態を把握（例：レンタルサービスを利用している）
2. やらなければならない対策を調査（例：パスワード・認証の強化）
3. 優先して対処する問題を検討（例：情報漏えい対策）