

ウェブサイト運営における脅威と責任

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

堀江 亘

ウェブサイトにおける様々な脅威

情報漏洩

ウェブサイト改ざん

踏み台

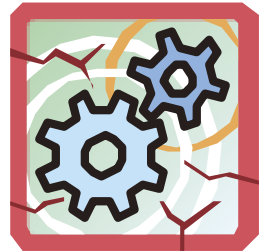
システム・サービスの障害

セキュリティ上の脅威



セキュリティ上の脅威の主な発生要因

- ◆ ウェブサイトの脆弱性を悪用した不正アクセス
 - 脆弱性とは
プログラムの不具合や設計上のミスが原因となって発生した
セキュリティ上の欠陥のこと
- ◆ ウェブサイトの不適切な運用
 - アクセス制限の不備など



不正アクセスなどの被害にあわないためには、
適切な対策が不可欠

そうは言っても・・・

不正アクセスとか言われても、イマイチ実感がわかない
自分たちには、関係のない話じゃないの？

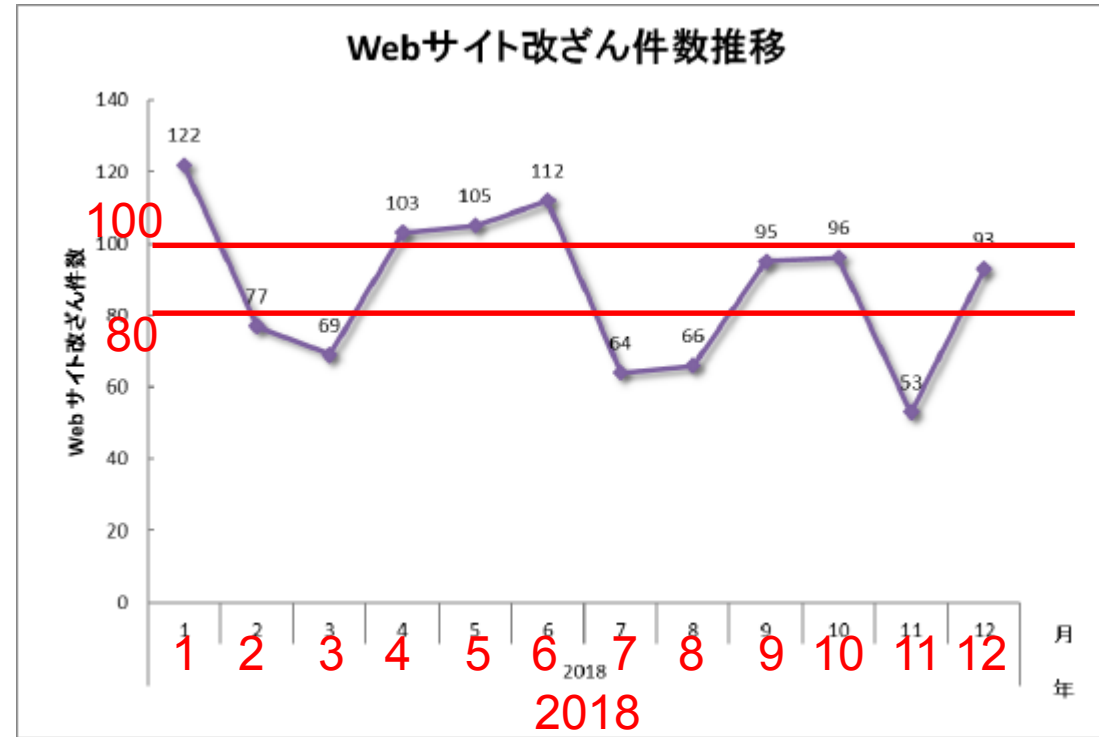
セキュリティに対するよくあるギモン

- ① **大きなウェブサイトじゃない**から攻撃なんて受けないのでは？
- ② **これまで問題は発生していないし、特に対策なんてしなくても、今後も大丈夫**なのでは？
- ③ ウェブサイトの運用は信頼のおける**委託先に全部**任せているから、何かあっても**委託先の責任**なのでは？



攻撃を受けるのは大企業だけなのか①

- ◆ 大企業は、十分な対策が行われている場合が多く、**攻撃が困難**
 - 対策にまで手がまわっていない脆弱なウェブサイトが標的に
- ◆ 攻撃ツールなどの流通によって脆弱なウェブサイトの**調査・攻撃が容易に**



(出典) JPCERT/CC インシデント報告対応レポート
[2018年10月1日～2018年12月31日]

企業規模や、機密情報の取扱いの有無
に関わらず、攻撃の対象となる

攻撃を受けるのは大企業だけなのか②

～事例 A～

- ◆ 従業員数**10人**の企業が運営する通販サイトでクレジットカード情報が流出
 - 決済代行会社からの指摘により、発覚
 - 原因は外部からの**不正アクセス**
 - **侵入経路**や流出したカード情報の正確な件数などは**特定できず**
 - 利用者およそ**2,000人**のクレジットカード情報が流出したおそれ
 - およそ**3ヵ月間**に渡り、通販サイトの公開を停止

これまで問題なかったから大丈夫？

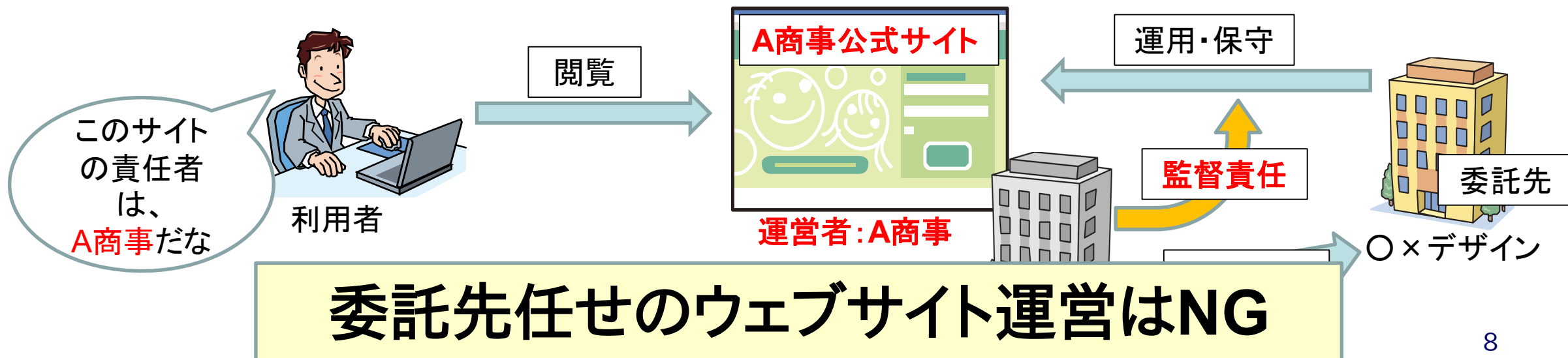
- ◆ 既に攻撃を受けている可能性
 - 攻撃発覚のほとんどは、外部からの指摘によるもの
 - 攻撃者は、極力攻撃の痕跡を消そうとする傾向にある
- ◆ ウェブサイトの脆弱性は放っておくだけでも増える
 - ウェブサイトでよく使用されるソフトウェアは、新たな脆弱性がしばしば発見される
 - 脆弱なバージョンを使用し続けることは、攻撃を受けるリスクにつながる

これまで大丈夫だったからと言って
今後も安全とは限らない

ウェブサイトは委託先任せでOK? ①

保守契約を結び、委託先が運用保守を行っていたとしても…

- ◆ **ウェブサイトの責任者は、ウェブサイト運営者**
- ◆ ウェブサイト運営者は、委託先に対する**監督責任**がある
- ◆ 監督責任を怠った場合、直接的な過失が委託先にあったとしても、**ウェブサイト運営者の責任が問われる**



ウェブサイトは委託先任せでOK? ②

～事例 B～

- ◆ 運用を委託していた通販サイトでおおよそ7,000件のクレジットカード情報が流出
 - － 委託先の問題
 - 原因はシステムの脆弱性を悪用した外部からの不正アクセス
 - システムのソフトウェアが脆弱なバージョンのまま放置されていた
 - 脆弱性診断などは実施しておらず、セキュリティ情報を更新する体制もなかった
 - － 委託元(ウェブサイト運営者)の問題
 - 委託先との信頼関係が強固であることから、最善なウェブサイト運営が行われているものと過信し、委託先管理を怠った

ウェブサイトは委託先任せでOK？③

～事例 C～

- ◆ 委託先のアクセス制限不備により、およそ**5万人分**の個人情報

漏えいの原因は、委託先にあったが、
委託元が委託先を指揮・監督する立場にあった
ことによる責任が認められた

- 裁判所は、委託元の損害賠償責任を認め、一人当たり**最大3万5000円**の支払い命令

◆ ウェブサイト運営者の責任

ウェブサイトの責任者は、ウェブサイト運営者である
ウェブサイト運営者には、**ウェブサイトを安全に運営する責任**がある
(委託先任せのウェブサイト運営はNG)

◆ ウェブサイトにおけるセキュリティ上の脅威

- 情報漏えいなどの**セキュリティ上の脅威**は、主に**脆弱性**が原因である
- **どのようなウェブサイト**も、脆弱であれば**攻撃を受けるリスク**がある
- これまで問題がなかったからといって、**今後も安全とは限らない**

**ウェブサイトの脅威は他人事ではなく当事者
しっかりした対策を!**

ウェブサイト運営のファーストステップ

- ウェブサイトを運営する上で発生する**脅威**や**責任**といった事柄を**対話形式**で解説した入門書

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～



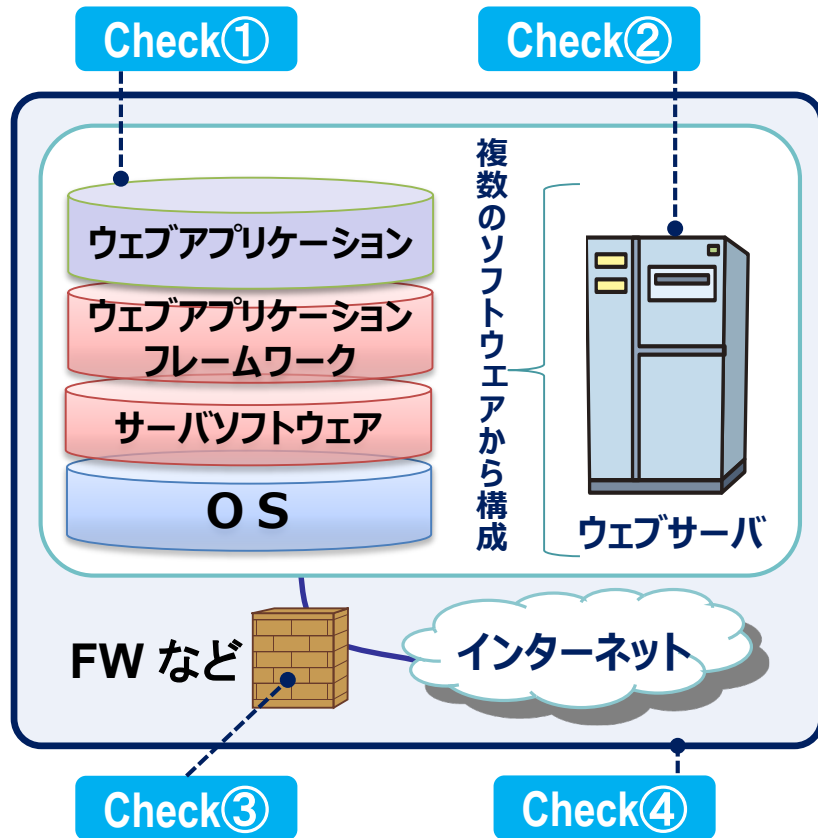
2019年3月

IPA 独立行政法人個人情報保護委員会
www.ipa.go.jp

最後に: ウェブサイトの対策

安全なウェブサイトの運用管理に向けての20ヶ条

- ◆ ウェブサイトは**複数の要素**によって構成される
- ◆ ウェブサイトの対策は**構成要素毎に対策することが重要**



Check① ウェブアプリケーションのセキュリティ対策

⇒ ウェブアプリケーションの脆弱性対策など8項目

Check② ウェブサーバーのセキュリティ対策

⇒ ソフトウェアのバージョンアップなど6項目

Check③ ネットワークのセキュリティ対策

⇒ ネットワーク機器の適切な運用など4項目

Check④ その他のセキュリティ対策

⇒ その他の対策に関する2項目

