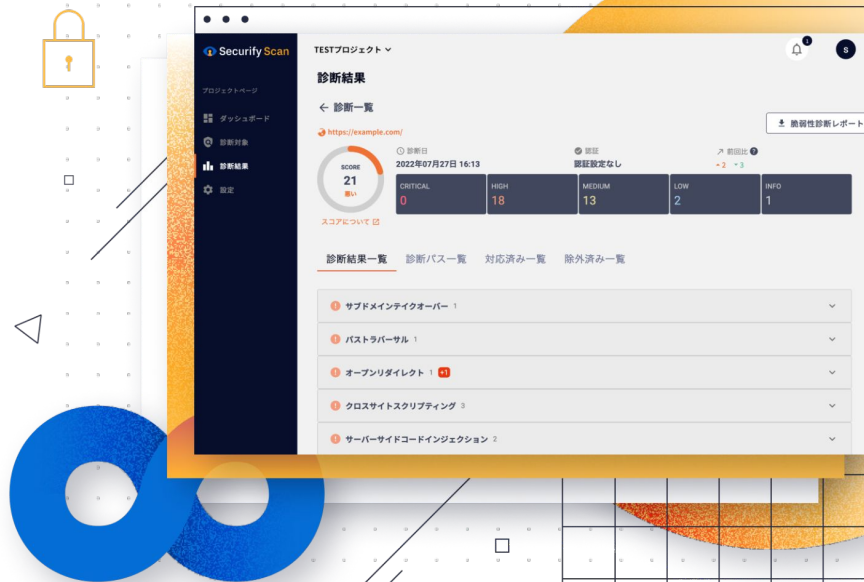


2024年、 義務化が進む セキュリティ対策とは

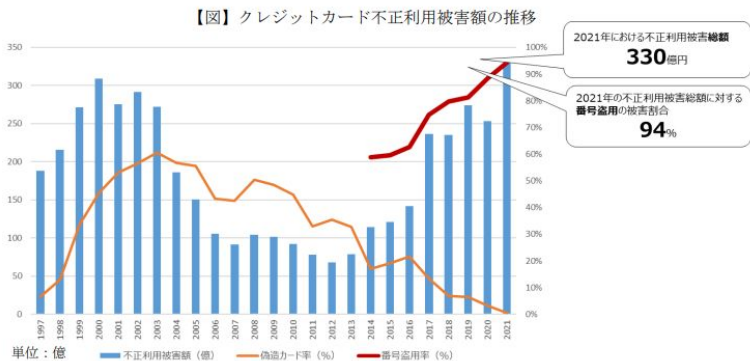


1. 全ECサイトに対しての脆弱性対策が義務化
2. Webセキュリティ対策の現状と対策の重要性
3. Webセキュリティ脆弱性対策の手法
4. 脆弱性診断ツールSecurify Scanとは

01

全ECサイトに対しての脆弱性対策が義務化

経済産業省から全ECサイトに対して脆弱性対策の義務化の指針が示されている



(出典) クレジットカード不正利用被害額の発生状況 (2022年3月 日本クレジット協会) より事務局作成

経済産業省は2023年1月20日に公開した「クレジットカード決済システムのセキュリティ対策強化検討会」(第6回)」の中で、**2024年3月末までに、全てのECサイトが脆弱性対策と本人認証を導入**することを、検討会の報告書案に盛り込んでいる。

具体的には、「クレジットカード番号等の適切管理義務の水準を引き上げるべく、**サイト自体の脆弱性対策を必須化(システム上の設定不備改善、脆弱性診断、ウイルス対策等)**」「不正利用防止措置として、利用者本人しか知り得ない・持ち得ない情報(ワンタイムパスワード・生体認証)による利用者の適切な確認(本人認証)の仕組みを順次導入(～2024年度末)」——の2点を盛り込んでいる。

今回は、全ECサイトの脆弱性対策の必須化とその対策方法についてお話しします。

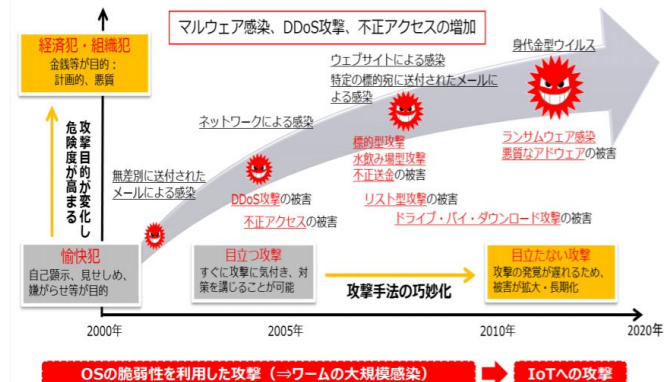
02

Webセキュリティ対策の現状と 対策の重要性

サイバー攻撃は、技術の進化が進み、年々手口が巧妙化。近年のDX推進等により、被害数も増加しています。近年では、内部データ(企業の機密情報や個人情報など)を盗むことだけでなく、情報の暴露やサービスの改ざん・停止を脅迫し身代金の要求を行うなどの被害が増加しています。

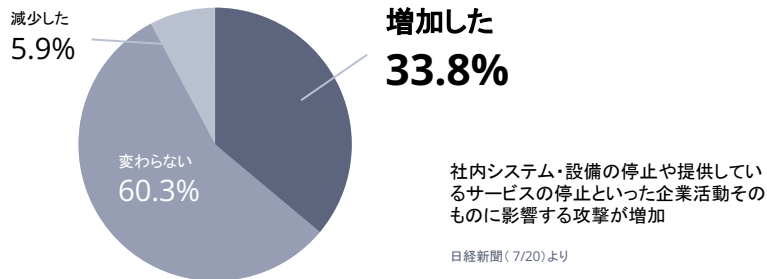
さらに、コロナ禍によりリモートワーク・DXの推進を行う企業が増加しました。しかし、企業の中にはセキュリティ対策を十分に行わずにリモートワーク・DXの推進が行われており、こうした企業を狙ったサイバー攻撃が増加しています。

実際に日経新聞の調査でも2020年4月以降に
サイバー攻撃が増加したと回答する企業は
33.8%にも上ります。



出展: 総務省サイバーセキュリティタスクフォース事務局サイバー攻撃の最近の動向等について

2020年4月以降に受けたサイバー攻撃



脆弱性(ぜいじゃくせい)とは、コンピュータのOSやソフトウェアにおいて、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情報セキュリティ上の欠陥のことを言います。脆弱性はセキュリティホールとも呼ばれます。

The screenshot shows the homepage of the National Cyber Security Center (NCSC) website. At the top, there is a navigation bar with the text "総務省 安心してインターネットを使うために 国民のための情報セキュリティサイト" and a search box. Below the navigation bar, there are several menu items: "はじめに", "基礎知識", "一般利用者の対策", "企業・組織の対策", and "用語辞典". The main content area is titled "脆弱性 (ぜいじゃくせい) とは？". It includes a sub-section "基礎知識" with a list of topics: "インターネットを使ったサービス", "どんな危険があるの?", "ウイルスとは?", "ウイルスの感染経路と主な活動", "ウイルスの感染経路", "ウイルスの主な活動", "不正アクセスとは?", "ホームページやファイルの改ざん", "他のシステムへの攻撃の踏み台に", "詐欺等の犯罪", "事故・障害", and "脆弱性(ぜいじゃくせい)とは?". The main text explains that in May 2022, the website was updated and provides a link to the new site: https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/index.html. It defines vulnerability as a weakness in the OS or software that can be exploited to cause security issues. It also mentions that vulnerabilities are often discovered by researchers and that users should be cautious of updates and patches.

総務省
国民のためのサイバーセキュリティサイトより参照

脆弱性対策って本当に必要？

脆弱性対策を行っていない企業も多いですが...
脆弱性対策は本当に必要なのか、
脆弱性はどれほど見つまっているのかを見ていきます。

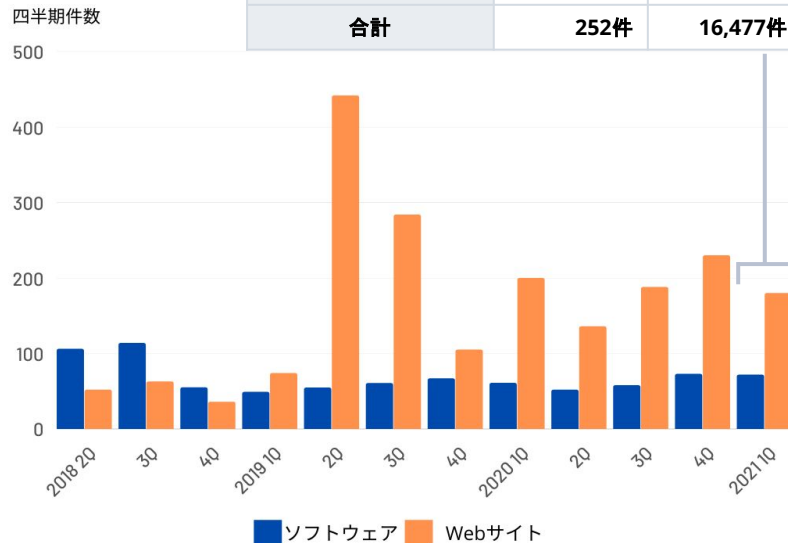
実際にIPAに届け出があった脆弱性は
2021年1月～3月だけで252件
(ソフトウェア 72件、Webサイト 180件)

同じ時期の届け出件数を、就業日あたりに換算すると...

4.05 /1就業日

しかし、これは届けられている脆弱性だけで...
まだ発見されていない脆弱性が数多く潜んでいます。

分類	本四半期件数	累計
ソフトウェア製品	72件	4,772件
ウェブサイト	180件	11,705件
合計	252件	16,477件



ソフトウェア等の脆弱性関連情報に関する届出状況(2021年第1四半期(1月～3月))

新型コロナウイルスワクチン大規模接種センター「誰でも、何度でも予約ができてしまう」予約システムに重大欠陥



【ワクチン大規模接種の予約システムでSQLインジェクション(脆弱性)が確認されたと】報道されています。架空の登録番号や生年月日で予約を行うことや、複数回の予約が行えてしまうといった事象がすでに確認されています。

防衛省の担当者は「善意に頼ったシンプルな予約システム。いたずらで予約されては必要な人の予約が取れない」と報道されています。

この事例では脆弱性が原因で大きく2つの問題が発生しています

- ①サービス利用者が開発者の意図しない挙動・体験をしてしまう
- ②個人情報などが流出する可能性が存在する



複数の脆弱性に関する事例を見てきました。

まとめると...脆弱性が見つかり、悪用されてしまうことで以下4つの被害・影響が発生します。

1 個人情報の悪用

流出した個人情報がさらにSNSやクラウドサービスの不正アクセスなどで新たなサイバー攻撃に繋がってしまいます。

2 個人情報漏洩に伴う損害賠償

ユーザに対しての慰謝料として、1情報につき約5,000～の賠償が発生します。
2次被害や流出した個人情報のセンシティブさによって金額も増加します。

3 サービスの停止 / 機会の損失

システム/サイトの一時停止/閉鎖や改修などといったシステム的な対応コストから、利用者やメディアへの問合せ対応まで幅広いコストを要します。

4 信用失墜

情報漏洩がない場合でも「情報流出の可能性」「改ざんされていた」等が報道されることで、社会的な信用低下に繋がります。

セキュリティは外部に委託しているから大丈夫.....??

セキュリティ人材は希少性が高く、そのノウハウや技術は属人化しやすい傾向にあります。そのため、セキュリティについては、外部に委託し、自社内でセキュリティを管轄しない方針を取られている企業も少なくありません。そんな企業の担当者様にとっては、今回のような発表があっても「ウチには関係無い内容」と捉えていませんか？

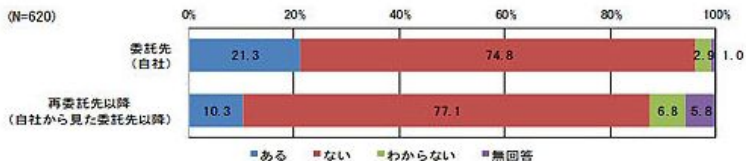
その認識は今回を機会に見直して頂ければと存じます。

なぜなら、前ページで説明した脆弱性の存在によって起こりうる被害・影響を被るのは、当然、システムを運用、所有されている企業様だからです。

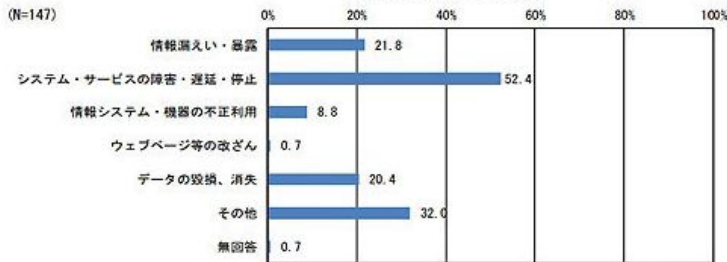
そのため、自社プロダクトのセキュリティリスクは自社内で可視化し、担保する意識が重要です。では、どのように社内で可視化を進めるのか、それが脆弱性診断ツールです。

外部委託が安全とは言えない！

受託業務(自社や再委託先以降(自社から見た委託先以降))における過去3年間のインシデントの経験



インシデント内容



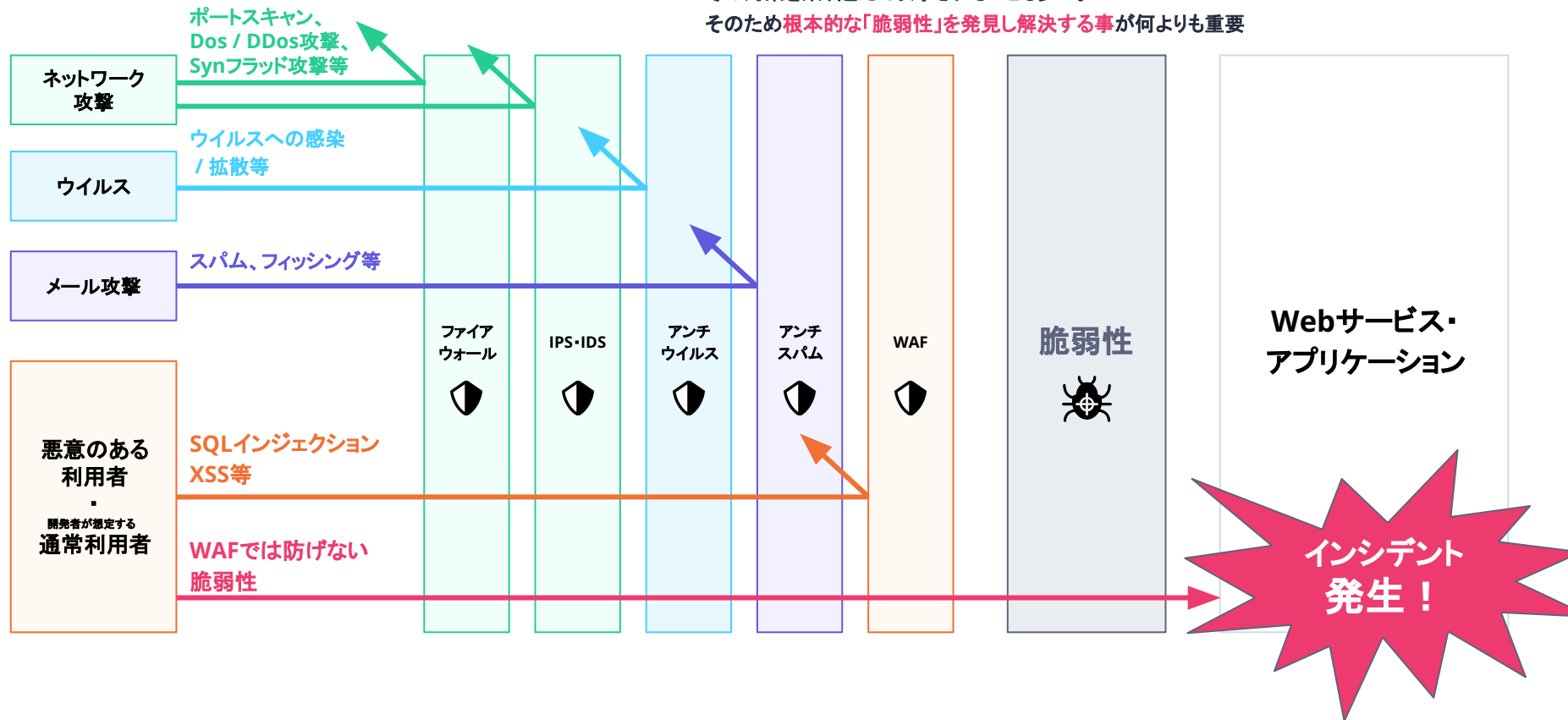
ITサプライチェーンの業務委託におけるセキュリティインシデント及びマネジメントに関する調査 情報処理推進機構(IPA)2018年3月26日

03

Webセキュリティ脆弱性対策の手法

Web 脆弱性対策におけるアプローチの一覧

脆弱性があっても、各セキュリティ製品でカバー出来る範囲もあるが、
その対策を乗り越えて攻撃されることも多い。
そのため**根本的な「脆弱性」を発見し解決する事**が何よりも重要



開発者・プロダクトオーナーとして自社のWebサービス・アプリケーションをリリースする前には、

①自社のサービス内に意図しない挙動や
情報流出の原因となる脆弱性がないか脆弱性診断で確認

②Webアプリケーション診断実施後、年々攻撃手法が高度化する中で
攻撃者視点で攻撃対象となってしまう部分がないか、
ペネトレーションテストで確認

この2つの確認が求められます。

そして、開発が進めば脆弱性が起きている可能性は高まり、時間が進めば攻撃手法は進化していきます。

今、対策を行っていないのであれば、まず脆弱性診断を行ってください。

	脆弱性診断 (手動診断)	脆弱性診断 (ツール)	ペネトレーション テスト
特徴 (メリット)	<ul style="list-style-type: none">● 知見を持ったセキュリティエンジニア(=ホワイトハッカー)がソースコードなどを参考にし、網羅的に診断● コードなどの設計をもとに 網羅的に修正が必要な脆弱性を報告する	<ul style="list-style-type: none">● 定常的・複数回の脆弱性診断を 低コストで実施することが可能● 自社で脆弱性診断を実施することが可能	<ul style="list-style-type: none">● 実際のハッカーによる攻撃を想定し、セキュリティエンジニアが脅威シナリオを検討し、疑似的なサイバー攻撃を実施● 攻撃者目線で現実的なシナリオに沿ってどこまで侵害されるかがわかる
デメリット	<ul style="list-style-type: none">● 特定の期間のみの脆弱性の把握になり、常時ではない● 診断準備・実施までの 期間がかかる● 値段が高額	<ul style="list-style-type: none">● セキュリティに関する知見が必要になる製品が多い。● 手動診断と比較して、網羅性と検出精度が劣る	<ul style="list-style-type: none">● 特定のシナリオや脅威に限定して診断を実施

自社提供のWebサービス・アプリケーションの脆弱性対策を行う場合、**脆弱性診断**を実施する必要がある。

よく言われる「ペネトレーションテスト」は脆弱性診断とは異なる！

1. 運用が「キツイ」と網羅的な診断が不可能

- 企業が抱える Webサイト/サービスは一つだけではなく多岐に渡る
- その中で脆弱性診断に対する工数が多くかかる状態の場合、網羅的に脆弱性対策を実施していくことが非常に難しい

2. 脆弱性診断の頻度を上げることが出来ない

- 昨今では日々、新たな脆弱性が数多く発見される状況になっている
- その中で脆弱性診断1回あたりの工数が大きくかかる場合、脆弱性診断を年～数年に1回の頻度でしか行えず、脆弱性を放置してしまうリスクがある

3. 多額のコストが発生してしまう

- 経済的・時間的・コミュニケーションコストなど大規模の費用が発生してしまう

04

Securify Scan による 「ラクな」脆弱性対策

本格的な脆弱性診断をいつでも手軽に



Securify(セキュリファイ)は自社の
プロダクトに対して、**手軽に、何度でも**
脆弱性診断の実施を可能にし、
セキュリティレベルを可視化・DevSecOps
への取り組みをサポートします。



セキュリティの専門知識は不要 使いやすいシンプルなインターフェイス

わかりやすいシンプルなインターフェイスで、セキュリティエンジニアでなくても、直感的に診断を実施・管理することが可能です。

TESTプロジェクト

診断結果

診断名	URL	スコア	増減	診断日時
example.com	https://example.com/	21	-2 -3	2022年07月27日 16:13
example.com	https://example.com/	21	+4 +2	2022年07月26日 11:54
example.com	https://example.com/	21	-33 -0	2022年07月22日 12:58
example.com	https://example.com/	100	-0 -0	2022年07月21日 15:01
example.com	https://example.com/	100	-0 -0	2022年07月21日 14:26
example.com	https://example.com/	100	-0 -33	2022年07月21日 13:51
example.com	https://example.com/	21	-6 +1	2022年07月13日 11:34
example.com	https://example.com/	21	-1 +1	2022年07月05日 11:40

現在のステータスを 一目で確認できるダッシュボード

最新の診断結果や、診断の状況、発見された脆弱性の推移など、現在のステータスを直感的に把握できます。



診断結果のスコア表示で 現在の状況を見える化

診断結果をスコアで表示します。プロダクトのセキュリティレベルを可視化することができ、改善へのモチベーションにもつながります。



検出された脆弱性の背景から 修正方法まで解説

脆弱性と判断した根拠となるリクエスト/レスポンスの表示、脆弱性の概要解説、該当箇所の修正方法の提案、トリアージに必要な情報を提供します。



診断結果をレポートとして PDFファイルで出力可能！

診断レポートの外部共有も簡単に実施することが可能です。

Security Scan 脆弱性診断レポート 作成日: 2022年08月28日

概要
診断日時: 2022年08月08日 14:13 診断対象: https://[redacted]

総合評価
High
改善が必要な検出項目

Critical	緊急に改善が必要な検出項目
High	改善が必要な検出項目
Medium	将来的に改善が必要な検出項目
Low	将来的な改善を推奨する検出項目
Info	リスクではないがご認識いただきたい情報

発見された脆弱性

以下に脆弱性の危険度ごとのサマリ件数と危険度ごとに発見された脆弱性の内容を記載いたします。
個別の脆弱性の説明については次項でご説明いたします。

Critical	0	High	1	Medium	10	Low	1	Info	2
----------	---	------	---	--------	----	-----	---	------	---

危険度	検出名	件数
High	サブドメインテイクオーバー	1
Medium	Mixed Content	1
Medium	クリックジャッキング	6
Medium	サーバサイドのリクエストフォージェリ (CVE-2021-29490)	1

Medium 機密情報の漏えい (git-config) 1

Medium 脆弱なJavaScriptライブラリの使用 (jquery 1.12.4) 1

Low プライベートIPアドレスの露出 1

Info 機密情報の漏えい (jupyter-notebook) 1

Info 開放されているポート 1

サブドメインテイクオーバー

対象エンドポイント
• https://[redacted]

概要
サブドメインテイクオーバーは、攻撃者によりサブドメインを乗っ取られてしまう恐れのある脆弱性です。
例として、作成したGitHub Pagesを `blog.example.com` というサブドメインに指定している場合を考えます。
GitHub Pagesでの運用をやめたとき、`blog.example.com` に割り当てていた、`<username>.github.io` というCHANGEレコードをそのままにしておくことがあります。
そのような場合に、攻撃者は `<username>` にあたるユーザー名をGitHubで取得し、同じようにしてGitHub Pagesをサブドメインで配置することが可能になります。

修正方法
[redacted] のCHANGEレコード、AAAAレコードを削除してください。

Mixed Content

対象エンドポイント
• https://[redacted]

概要
HTTPSで通信しているコンテンツの中にHTTPのコンテンツが含まれている場合、中間者攻撃に利用される恐れがあります。
これは混合コンテンツと呼ばれ、ブラウザによっては自動的に読み込みがブロックされてしまいます。
そのため、ブラウザによっては正しく動作していない可能性があります。

修正方法
スキームをhttpを指定しているURLは、httpsを使うように変更してください。

クリックジャッキング

Thank you.

