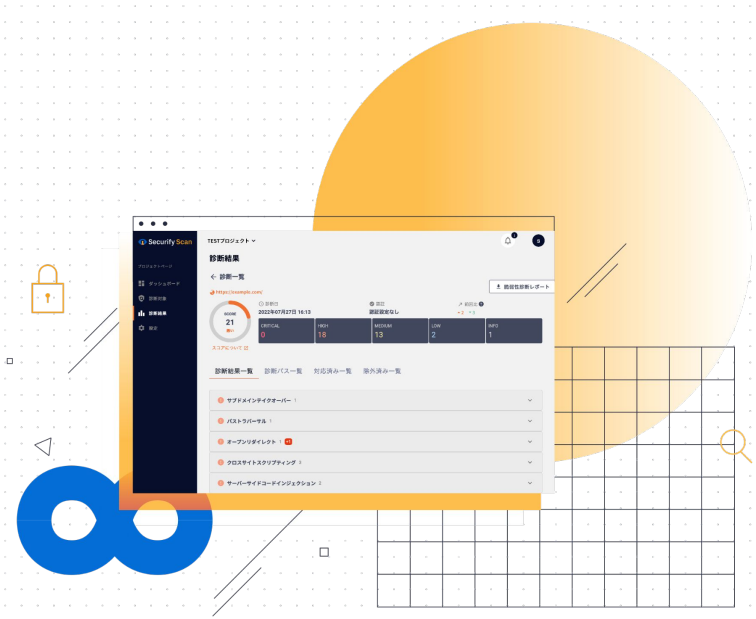
Securify Scan

リリース前に済ませておきたい！

開発者のためのセキュリティメソッド



3-SHAKE

目次

開発スピードはますます早くDevOpsの浸透

Securify Scan

近年、競争が高まりビジネスにおいてサービスの開発・リリースのスピードが必要不可欠となり、開発手法でもウォーターフォール型からアジャイル開発、DevOpsへとより効率的・スピードを重視した形へシフトしています。結果、週に複数回もデプロイを行うことが開発エンジニアに求められています。実際にある調査では、**調査対象の75%の企業が12回以下/週の頻度でデプロイを実行**している、**上位の組織では32回/週、営業日で考えると6回以上実施している企業も存在**するというデータがあります。

出展：https://circleci.com/landing-pages/assets/2017-VelocityReport-Updated-070219_JA.pdf

この開発・リリースにスピードが求められた結果、元来の開発フローにおいて、開発完了時に置かれていた**「セキュリティ対策が開発フローに追いつかず、担保できなくなっているというToil」が発生**しています。

▶ **しかし、サイバー攻撃の危機はますます増加しています。**
まずは、近年のサイバー攻撃・セキュリティの状況について見ていきたいと思います。

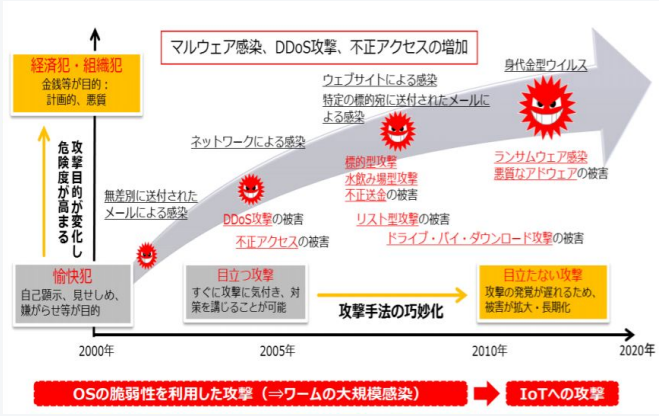
近年のサイバー攻撃・セキュリティの状況

Securify Scan

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。

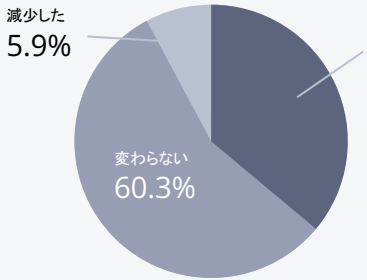
さらに、コロナ禍によりリモートワーク・DXの推進を行う企業が増加しました。しかし、企業の中にはセキュリティ対策を十分に行わずにリモートワーク・DXの推進が行われており、こうした企業を狙ったサイバー攻撃が増加しています。

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



社内システム・設備の停止や提供しているサービスの停止といった企業活動そのものに影響する攻撃が増加

日経新聞（7/20）より

近年のサイバー攻撃・セキュリティの状況 – セキュリティ10大脅威 –

では近年、具体的に「どのような脅威に注意すべきか？」セキュリティ研究者・実務担当者が集計しているデータを見る2つの傾向が見えてきます。

① 個人の脅威では

Webサービスなどの利用時にサービス内の
脆弱性が原因となる可能性が高い項目がランクインしている。

② 組織（企業）では

ランサムウェアや**標的型攻撃やパスワード関連**の項目が上位にランクインしている

実際にこの2つの観点で、脆弱性が原因になりうる項目を**赤く**。標準型攻撃やパスワード関連の項目を**青く**表示しています。

「情報セキュリティ 10大脅威 2021」

NEW：初めてランクインした脅威

昨年順位	個人	順位	組織	昨年順位
1位	スマホ決済の不正利用	1位	ランサムウェアによる被害	5位
2位	フィッシングによる個人情報等の詐欺	2位	標的型攻撃による機密情報の窃取	1位
7位	ネット上の誹謗・中傷・デマ	3位	テレワーク等のニューノーマルな働き方を狙った攻撃	NEW
5位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	4位	サプライチェーンの弱点を悪用した攻撃	4位
3位	クレジットカード情報の不正利用	5位	ビジネスメール詐欺による金銭被害	3位
4位	インターネットバンキングの不正利用	6位	内部不正による情報漏えい	2位
10位	インターネット上のサービスからの個人情報の窃取	7位	予期せぬIT基盤の障害に伴う業務停止	6位
9位	偽警告によるインターネット詐欺	8位	インターネット上のサービスへの不正ログイン	16位
6位	不正アプリによるスマートフォン利用者への被害	9位	不注意による情報漏えい等の被害	7位
8位	インターネット上のサービへの不正ログイン	10位	脆弱性対策情報の公開に伴う悪用増加	14位

出展：IPA「情報セキュリティ10大脅威 2021」

Securify Scan

では近年、具体的に「どのような脅威に注意すべきか？」セキュリティ研究者・実

「情報セキュリティ 10大脅威 2021」

NEW：初めてランクインした脅威

昨年順位	個人	順位	組織	昨年順位
				5位
				1位
				NEW
				4位
				3位
				2位
				6位
				16位
				7位
				14位

出展：IPA「情報セキュリティ10大脅威 2021」

企業に求められる対策

企業として、自社がサイバー攻撃の被害にあい、
情報流出が起きないように対策をする必要がある。

▶ 多くのサービスが存在・対策がとられている！（社内対策）

toC向けのWebサービス・アプリケーションを提供・開発する場合
利用ユーザーが自社サービスの脆弱性が原因で脅威遭遇しない対策が必要

Appendix 攻撃に対してのよくある対策手法

Securify Scan

製品 / サービス	対象	対策できる攻撃例
ファイヤーウォール	あらかじめ許可した通信のみを通過させる	不審なIPアドレスからのアクセス ポートスキャン
IPS・IDS	ネットワークレベルの不正な動作	Synフラッド攻撃 不正なIPヘッダ
アンチウイルス	サーバー、個人のパソコン	ウイルス・マルウェア感染時の 駆除・拡散の防止
アンチスパム	メール	迷惑メール ウイルスに感染する恐れがある添付ファイル
WAF	Webアプリケーション / Webサイト スマホアプリケーション	SQL・OSインジェクション クロスサイトスクリプティング
脆弱性診断	**Webアプリケーション / Webサイト スマホアプリケーション**	**SQL・OSインジェクション クロスサイトスクリプティング 固有の脆弱性（の検出）**

Securify Scan

ここでおさらい！よくある攻撃の詳細について！

1 脆弱性を狙った攻撃

OSやソフトウェア、Webサイトの脆弱性を狙ったサイバー攻撃も存在します。
修正プログラムが公開される前の脆弱性をつく攻撃のほかに、インジェクション、クロススクリプティングなどが代表的な攻撃です。インジェクションには、

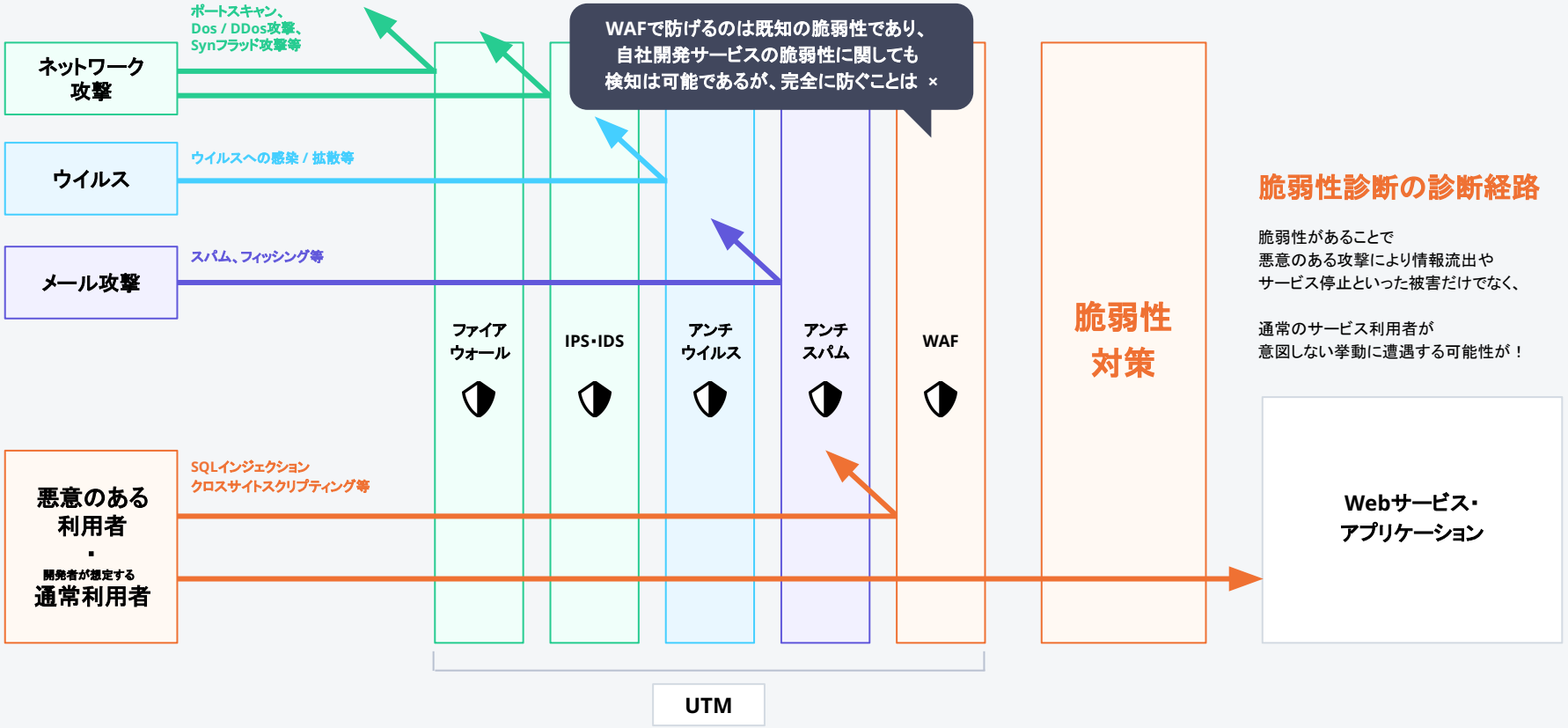
- SQLインジェクション（Webサーバーの脆弱性をつき不正なSQLを送信する）、
- OSインジェクション（脆弱性のあるアプリケーションに不正なOSコマンドを送信する）の2つがあります。

クロスサイトスクリプティングは悪意のあるスクリプトのついたURLを拡散し、そのリンクをクリックしたユーザーを不正なサイトへとばしたり、マルウェアを感染させるなどの被害を与えます。

2 標的型攻撃やパスワード関連の攻撃

特定の組織や個人を標的とし、悪意のあるプログラムを含んだファイルやURLを主にメールで送りつけ、情報を盗もうとするサイバー攻撃を「標的型攻撃」といいます。
パスワード関連の攻撃とは、総当たり攻撃（パスワードの組み合わせを総当たりで試す）などが知られています。

Appendix 攻撃に対してのよくある対策手法

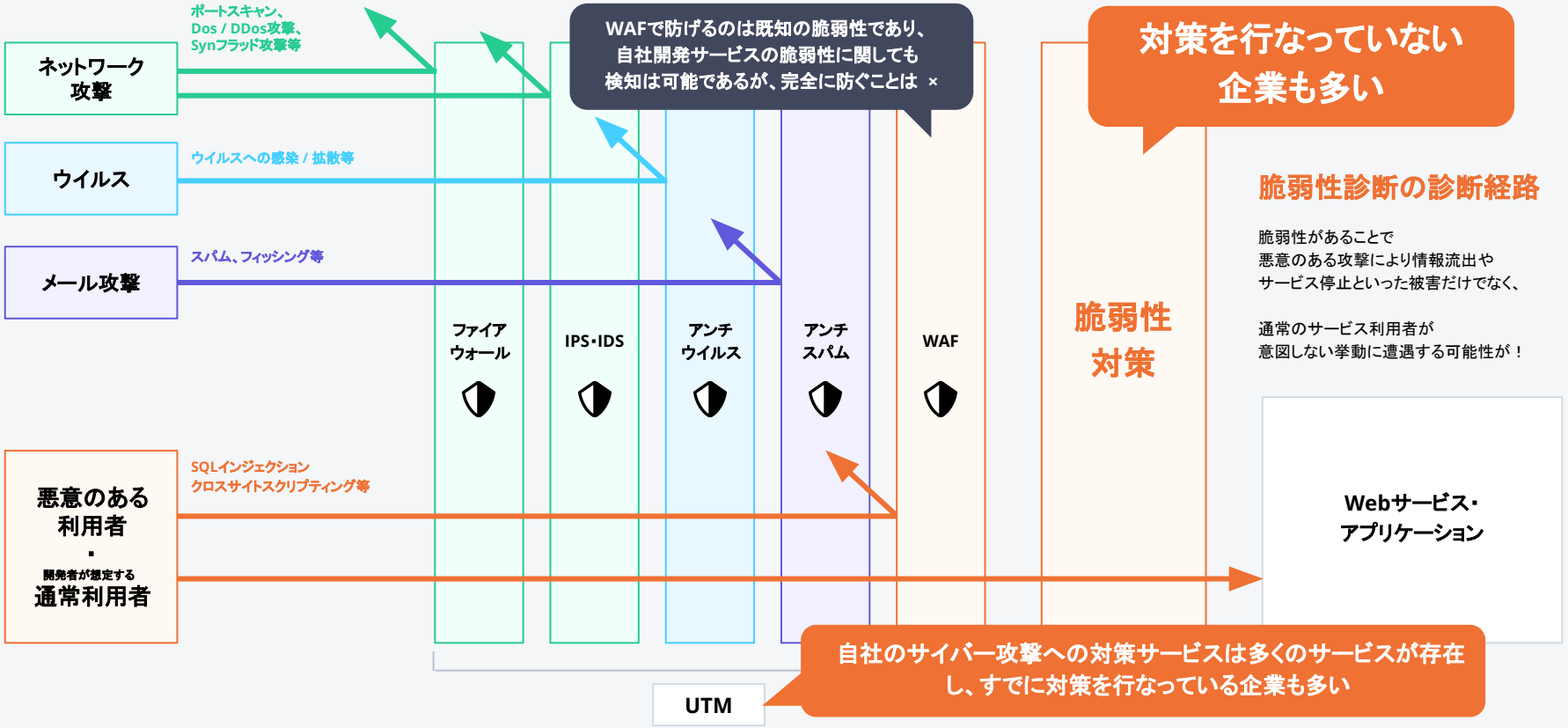


脆弱性診断の診断経路

脆弱性があることで
悪意のある攻撃により情報流出や
サービス停止といった被害だけでなく、

通常のサービス利用者が
意図しない挙動に遭遇する可能性が！

Appendix 攻撃に対してのよくある対策手法



『「脆弱性への対策が行われていない」というのは、脆弱性対策の必要性が高くないからではないのか？』
そう思われる方もいらっしゃるかと思います。

▶ ではここから、
「脆弱性対策が本当に必要なのか？」
「脆弱性があることでの影響」
を見ていきたいと思います。

脆弱性対策って本当に必要？

Securify Scan

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か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

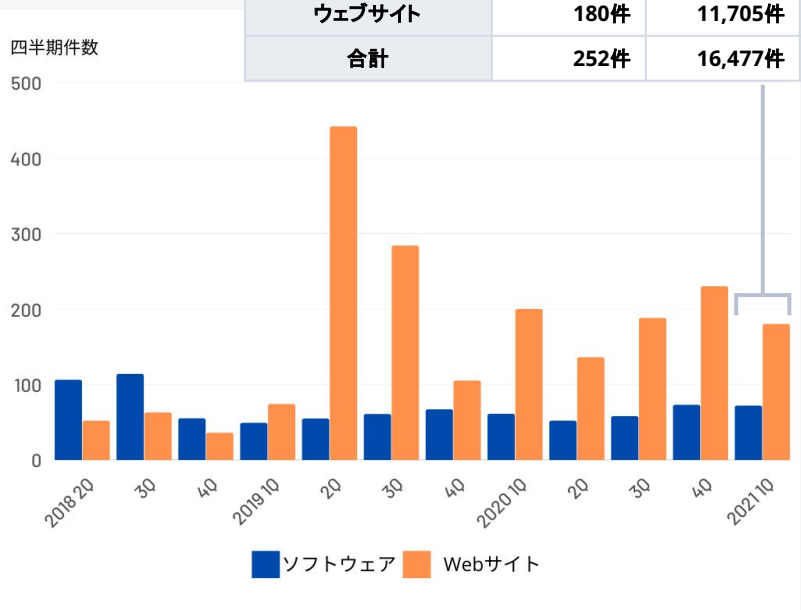
（ソフトウェア 72件、Webサイト 180件）

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）」

脆弱性対策って本当に必要？ – 脆弱性が原因とみられる被害事例 –

Securify Scan

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いった事象がすでに確認されています。

合法的にどのような脆弱性があるのか外部から確認することはできませんが、今までに確認されている事象だけでなく、他の予約者の個人情報を抜くことが可能な脆弱性が存在する可能性もあり得ます。

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。

毎日新聞　https://mainichi.jp/articles/20210517/k00/00m/040/165000c
AERA dot　https://dot.asahi.com/dot/2021051700045.html?page=1

脆弱性対策って本当に必要？ – 脆弱性が原因とみられる被害事例 –

Securify Scan

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

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

▶ サービスが正常に稼働していない

②個人情報などが流出する可能性が存在する

脆弱性対策って本当に必要？ – 脆弱性が原因とみられる被害事例 –

Securify Scan

公表日	企業名	インシデント概要
2019/5	Y社	大手家電量販店が営む通販サイトへの不正アクセス。セキュリティコード含む**クレジットカードの情報が7,832件流出した可能性**あり。決済アプリケーションの改ざんによってクレジットカードの登録・変更画面で入力した情報が、そのまま攻撃者のサーバーに送信されるようになっていたと見られる。
2019/7	S社	公式アプリに組み込まれた決済サービスの「外部ID（Google、Facebook等）連携」機能の脆弱性を攻撃され、第三者によってアカウントが不正利用される。被害人数は574人、被害金額は3,240万688円。**7月の開始からわずか8ヶ月でサービスは廃止**された。
2019/9	N社	大手旅客鉄道会社の運行スケジュール確認サイトにアクセスすると、**ご利用者にアンケートへの回答を求める不審なサイトが表示**ウェブサイトが改ざんされていた。当該サイトでは個人情報の保有はなく、情報流出はないとするも、不審なサイトからアンケートへ回答した場合、クレジットカード情報を求められ、入力した場合には流出する可能性があった。
2019/12	Z社	調理器具メーカーにて、グループ会社が運営するショッピングサイトが何者かにシステムの脆弱性を突くサイバー攻撃を受け顧客情報最大752件が流出した可能性があり。さらに**流出した個人のメールアドレス宛にフィッシングサイトへ誘導するメールが送られ、そこからクレジットカードの情報が流出。**
2019/12	P社	プレスリリースプラットフォームを運営する同社のサイトに、同一のIPアドレスから1時間あたり約100万件近い大量の不正アクセスが有りDBサーバーが高負荷状態となり**接続障害が発生し、サービスが停止。**復旧までの期間に配信を予定していたプレスリリース最大203本に影響。
2020/2	K社	ホームセンターを運営する同社のWebサイトが第三者からの不正アクセスを受け**利用者の意図とは無関係の外部サイトへ誘導**されるように改ざんされていたことを発表。同被害による個人情報の漏えいの被害はない。
2020/4	S社	音楽系事業を展開する同社の公式サイト内の複数の**コンテンツについて、外部からの改ざん行為**が確認された。6日間公式サイトを停止。 サーバーからの情報流出はない。
2020/7	J社	学習塾を経営する同社に対し、脆弱性をついたWebサーバーへの不正アクセスがあり**ホームページ内の全データが消失**した可能性がある他、サービスの資料請求画面から、体験入学に申し込んだ利用者の個人利用が流出した。把握できている流出件数は14,263件。

脆弱性対策って本当に必要？ －脆弱性が原因とみられる被害事例－

Securify Scan

「7pay（セブンペイ）」に脆弱性、情報漏洩の恐れ、外部ID遮断、開始から3か月でサービス廃止

株式会社セブン&アイ・ホールディングスの子会社が運営するバーコード決済サービス「7pay（セブンペイ）」が2019年7月ににリリースされました。しかし、リリース直後に不正アクセスが発生、さらにアプリ内に脆弱性（セキュリティー上の欠陥）あり、第三者がフェイスブックやLINE（ライン）などの外部IDで不正にログインし、個人情報を盗み取られる恐れがることがわかりました。

不正アクセスによる被害は808人／38,615,473円（7月31日時点）
上記の脆弱性（「2段階認証」がなされていない）など、
セキュリティー上の不備が次々と指摘され最終的に、
サービス開始から3か月でサービスの廃止となりました。

セブン銀行の決算発表によると
「7pay」の廃止に伴う損失約30億円※1

※日経新聞　https://www.nikkei.com/article/DGXMZO47224320R10C19A7000000/
※「7pay（セブンペイ）」サービス廃止のお知らせとこれまでの経緯、今後の対応に関する説明について
https://www.7andi.com/company/news/release/201908011500.html
※1「セブン銀行、3Qは7payの損失を吸収し連結で増益　チャージ取引増を主因にATM利用数増加」https://shikiho.jp/news/8/370138

脆弱性があることで起こりうる被害・影響

Securify Scan

複数の脆弱性に関しての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。

【2021年】近年の脆弱性を突くサイバー攻撃の状況

JNSAセキュリティ被害調査によると
2018年（1年間）のセキュリティインシデント事例の総数・一件当たりの平均は以下のようになっています。
※こちらは脆弱性だけではなく、人為的な紛失などが原因による情報漏洩も含んだ数字となっています。

漏えい人数	561万3,797人
インシデント件数	443件
想定損害賠償総額	2,684億5,743万円
一件あたりの漏えい人数	**1万3,334人**
一件あたり平均想定損害賠償額	**6億3,767万円**
一人あたり平均想定損害賠償額	**2万9,768円**

特定非営利活動法人　日本ネットワークセキュリティ協会　2018年 情報セキュリティインシデントに関する調査報告書【速報版】

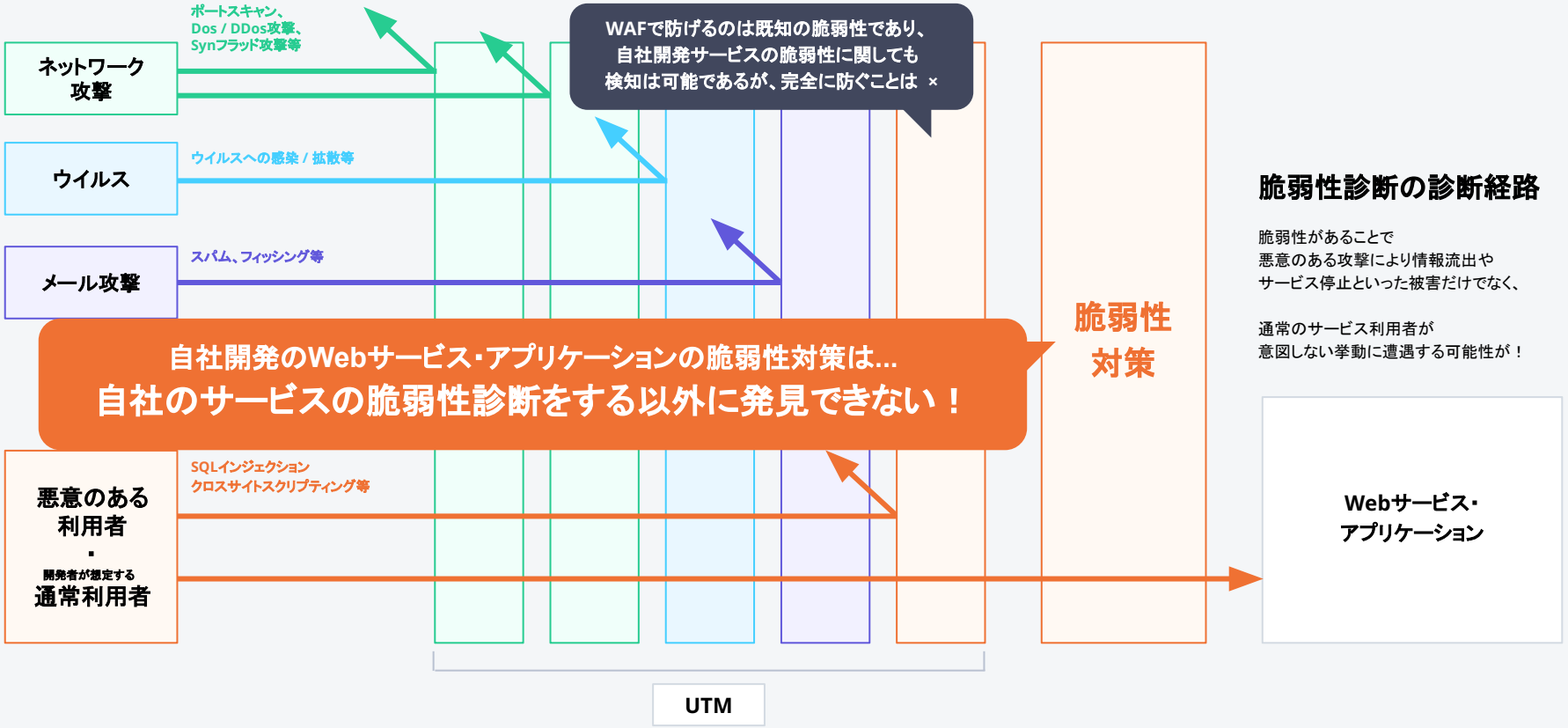
脆弱性が原因で被害が出ることはここまでお伝えしてきました。

しかし、脆弱性が全くないことを証明することは難しく、開発を行えば
開発したWebサービス・アプリケーションの中に脆弱性が存在する可能性があり続けます。

▶**では、**
「脆弱性に対してどのような対策が存在するのか？」
「どのような脆弱性対策が必要なのか？」
について考えていきます。

攻撃に対してのよくある対策手法(再掲)

Securify Scan



脆弱性診断の診断経路

脆弱性があることで
悪意のある攻撃により情報流出や
サービス停止といった被害だけでなく、

通常のサービス利用者が
意図しない挙動に遭遇する可能性が！

脆弱性への対策方法とは？

Securify Scan

	バグバウンティ （バグ報奨金制度）	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）	● 複数のバグハンター（ホワイトハッカー）が **多角的にサービス内を診断し、脆弱性を検証する** ● 一定期間、診断が継続する。 ● 想定していない脆弱性の発見が期待できる	● 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**	● 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	● 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	● 報告された脆弱性への対応優先度や適正な報奨金、バグハンターとの対応など **自社内でセキュリティへの知見や対応人材が必要** ● 国内サービスが限られ、**海外サービスが主流** ● **値段が高額**	● 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**	● 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低い**	● **特定のシナリオや脅威に限定して診断**を実施
脆弱性への対応	◎	○	○	—

脆弱性への対策方法とは？

Securify Scan

	バグバウンティ （バグ報奨金制度）	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）	• 複数のバグハンター（ホワイトハッカー）が**多角的にサービス内を診断し、脆弱性を検証する** • 一定期間、診断が継続する。 • 想定していない脆弱性の発見が期待できる	• 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**	• 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	• 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	• 報告された脆弱性への対応優先度や適正な報奨金、バグハンターとの対応など**自社内でセキュリティへの知見や対応人材が必要** • 国内サービスが限られ、**海外サービスが主流** • **値段が高額**	• 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**	• 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低い**	• **特定のシナリオや脅威に限定して診断**を実施
脆弱性への対応	◎	○		

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！

開発者・プロダクトオーナーに求められるセキュリティ対策とは？

Securify Scan

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。

開発者・プロダクトオーナーに求められるセキュリティ対策とは？

Securify Scan

しかし、ビジネスの中で開発スピードが求められる中、
リリースのタイミングに毎回、脆弱性診断を実施するのはコスト（金額・工数）的に
難しいのではないでしょうか？

言われたことは対応しているが…言われたから対応しているだけ…
自分事感が低い

正直、**開発が優先でセキュリティは後回し**になってしまっている。

社内に**ノウハウや知見がない**
対応が難しい

診断会社に依頼しているが
コストが高い

開発者・プロダクトオーナーに求められるセキュリティ対策とは？

Securify Scan

開発スピードへの追従とコストを考慮すると
各種ツールを自社で導入することが望ましいですが、
運用まで考慮すると、すべてを入れることは現実的ではありません

まずは「脆弱性診断ツール」を導入することがオススメです！

実際に外部公開した場合に攻撃される可能性のある脆弱性 を検出するため、
開発プロセスに脆弱性診断ツールを組み込み、
アプリケーションの リリース前 に 定期的 に実施することで、
セキュリティレベルを一定に保つことが可能です

開発者・プロダクトオーナーに求められるセキュリティ対策とは？

Securify Scan

	バグバウンティ （バグ報奨金制度）	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）	• 複数のバグハンター（ホワイトハッカー）が**多角的にサービス内を診断し、脆弱性を検証する** • 一定期間、診断が継続する。	• 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	• 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	• 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
	• 国内サービスが限られ、**海外サービスが主流** • **値段が高額**	• **値段が高額**	• 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低い**	• **特定のシナリオや脅威に限定して診断**を実施
脆弱性への対応	◎	○	○	—

ツールでの脆弱性診断を開発に組み込み、
開発の進捗に合わせて、社内で診断し、
脆弱性の対応状況を可視化し、
脆弱性の対応を定期的に実施することが求められる。

まとめ

Securify Scan

ビジネスの中に開発スピードが求められています。
一方で着実にサイバー攻撃の危機は身近なものになっており、発生した際の被害は甚大です。

開発者・プロダクトオーナーとして、Webサービス・アプリケーションをリリースする前には、
「脆弱性診断」が求められています。

しかし、「脆弱性診断」もこの新しい環境に合わせ形を変え実施していかなくてはなりません。

今、求められる脆弱性診断のあるべき姿とは
「開発プロセスの中に脆弱性診断を組み込み、
リリース前にセキュリティ対策を実現すること」です。

そのためには、自社で手軽に・低コストで導入できる、
簡易に診断を実施できるツールでの脆弱性診断を定期的に開発の進捗に合わせ実施し、
脆弱性の対応状況を可視化・対応することが求められます。
スリーシェイクが提供している「SecurifyScan」によって実現することが可能です。

Securify Scan（セキュリファイ スキャン）とは

Webアプリケーションの
継続的セキュリティを簡単に実現

Securify Scan

Securify Scan（セキュリファイスキャン）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。

▸ まずは2週間の無料トライアルでお試しいただけます！

Thank you.