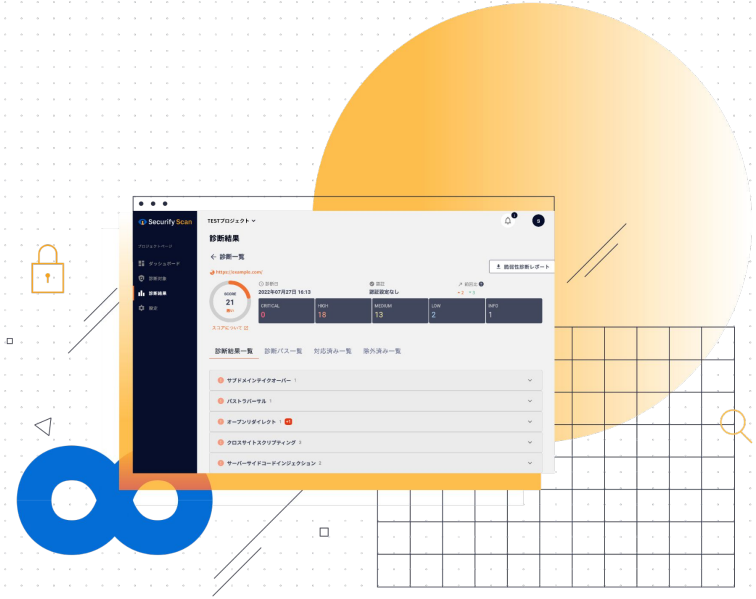
Securify Scan

エンジニアの

「セキュリティあるある」から紐解く

開発現場におけるセキュリティ対策の向き合い方



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。

▶ **では、まずWebアプリケーションの開発現場で**
よくある脆弱性対策を見ていきましょう。

開発現場でのセキュリティ対策

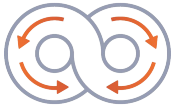
Securify Scan

リリース前に一度だけ、
脆弱性診断を実施、診断後に対応

企画

開発

リリース



保守・運用

日々の保守開発業務の中では、
外部へ依頼する脆弱性診断の
実施はできていない

開発における全体的な流れの中でのセキュリティ対策について、よくある状況が見えてきました。
このような状況では日々発見されている脆弱性やリリースされ変更が加えられるアプリケーションに対して、対策が追いついていかないと考えられます。

▶ **ではここから、**
開発者の視点から開発におけるセキュリティについて、
具体的に開発現場でどのようなことが起きているかを
「あるある」形式で見ていきましょう。

開発現場におけるセキュリティあるある①

Securify Scan

▶ 機能開発だけで精一杯でセキュリティに対応する時間がない！

開発者としては当然、「良いものを作って、お客様へ提供したい」と考えています。
機能開発の締め切りを意識するあまり、セキュリティ対策の重要性は認識しているものの、セキュリティを二の次としてしまうジレンマに苛まれています。

このように**セキュリティの必要性は十分認識しているが、機能開発をすることに精一杯でセキュリティを考慮する余裕がない**という開発現場が多いのではないでしょうか。

Securify Scan

▶ 脆弱性診断後の修正対応でスケジュールが逼迫！

社内規定等でシステムのリリース前に脆弱性診断を実施するように義務付けられている企業もあります。

脆弱性診断を実施したは良いが、その後の指摘対応で想定外の工数が取られてしまい、対応していてはリリーススケジュールに遅延してしまうという場面に陥ることがあります。

このような状況でやむを得ず、**クリティカルな脆弱性の対応のみを実施し、それ以外はリリース後に対応する**ということをされた方も多いのではないのでしょうか。

Securify Scan

▶ どうやって脆弱性対応をして良いのかわからない！

脆弱性の対応は多種多様であり、修正方法が難解なものも少なくありません。

セキュリティエンジニアではないアプリケーションエンジニアが対応する場合、検出された脆弱性の原理を理解し、どのように修正しなければならないかの調査からしなければなりません。

その際、現場に有識者がいないため、なにか疑問が出た際に聞ける先がいなかったり、仮に修正対応が完了しても、本当に問題ないのかを確認できないといった不安があるのではないでしょうか。

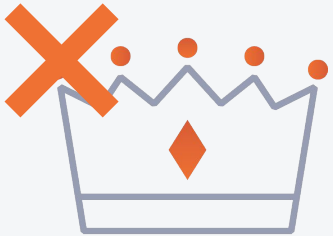
Securify Scan

▶ 脆弱性対応をやっても直接的に評価されない！

脆弱性の対応はアプリケーションの機能とは違い、わかりやすく目に見えるものではありません。

また、脆弱性の対応はその性質上、「できていて当たり前」であり、マイナスをゼロにする作業と見なされやすいです。

そのため、脆弱性の対応を開発工程の中できちんと実施できていても、**周囲の方のセキュリティに対する理解が十分でなければ、評価されなかったりすることも少なくありません。**



Securify Scan

▶ 外部の脆弱性診断は時間もお金もかかって大変！

脆弱性診断の必要性から外部のセキュリティベンダーに脆弱性診断を依頼するケースもよくあります。

この場合、診断対象に関するヒアリングから始まり、**診断完了まで1ヶ月単位の時間を要する**ことがよくあります。
また、昨今のセキュリティ意識の向上から、「脆弱性診断の順番待ち」が発生しており、さらに納期が伸びる可能性があります。

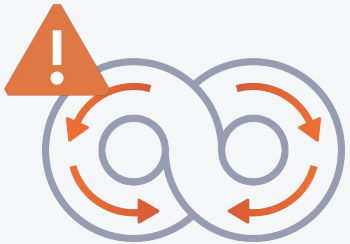
当然、これだけの時間がかかる作業であるため、**費用も高額**となることが想定されます。

▶ 日々のリリースごとの脆弱性診断は大変だけど、問題ないか不安！

システムの初回リリースや大幅なアップデート時に脆弱性診断を実施して、セキュリティ上、クリティカルな問題がないかを確認することは比較的行われています。

しかし、保守開発や自社サービス開発のように、日々、修正とリリースを繰り返すような現場では、都度、外部セキュリティベンダーでの脆弱性診断を実施することは現実的ではありません。

そのため、**小さな修正程度であれば、脆弱性が混入する可能性は低いと考え、リリースするが、開発者としては本当に問題ないか不安**となります。



▶フレームワークが担保してくれているはずなのに脆弱性が発覚！

昨今のフレームワークの進化によって、標準でセキュアな開発環境を提供し、SQLインジェクション等の脆弱性を混入させないようになっています。

しかし、業務ロジックに依存する部分や、例外的にフレームワークに頼らずに自前でコーディングする部分については、フレームワーク外でセキュリティを担保しなければなりません。
また、ミドルウェアやフレームワークを複数重ねた際にも重ねたことによる脆弱性が生まれる可能性があります。

そのため、**知らず知らずのうちに脆弱性を埋め込んでしまい、セキュリティのホールを作り出してしまう事象があります。**

▶ 脆弱性診断ツールを導入したが、使いこなせない！

IPAが推奨している脆弱性診断ツールである「OWASP ZAP※」やその他の脆弱性診断ツールが存在しており、自社で脆弱性診断を実施することが可能です。

しかし、**ツールの設定や使用方法が困難で習熟コストが高い**ため、使いこなせないことや**検出された脆弱性について解釈することが困難**であり、放置されるケースが散見されます。

また、具体的にどのように開発工程内に脆弱性診断を組み込んでいくかまで検討できていないことも見受けられます。

※ https://www.ipa.go.jp/about/press/20160928-2.html

開発現場でのセキュリティあるあるをここまでお伝えしてきました。
開発者であれば、一つないしは複数の「あるある」を経験されているのではないでしょうか。

▶ では、**どうやって開発現場とセキュリティの良い関係を築けていけるのか**について考えていきます。

開発現場とセキュリティとの良い関係を築くステップ

Securify Scan

開発現場とセキュリティとの良い関係を築くステップ

Securify Scan

ステップ1

セキュリティ対策の自分事化

日々、さまざまなメディアを通じてサイバー攻撃に関するニュースが流れていますが、どこか**他人事**のように感じているのではないでしょうか。

具体的に、どのような脅威があり、どのくらい**ビジネスインパクト**があるかを把握することで、自分たちのビジネスにもリスクが存在していることを実感できます。

このようなリスクを逆手にとって、
「セキュリティ対策をアピールすることによる競合との差別化戦略」
を施策として実施することがオススメです。

セキュリティ対策を顧客へアピールすることで、企業イメージの向上やビジネス機会の拡大、売上の向上等のビジネスへの貢献が期待でき、自分事として取り組めます。

脆弱性の届出件数

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

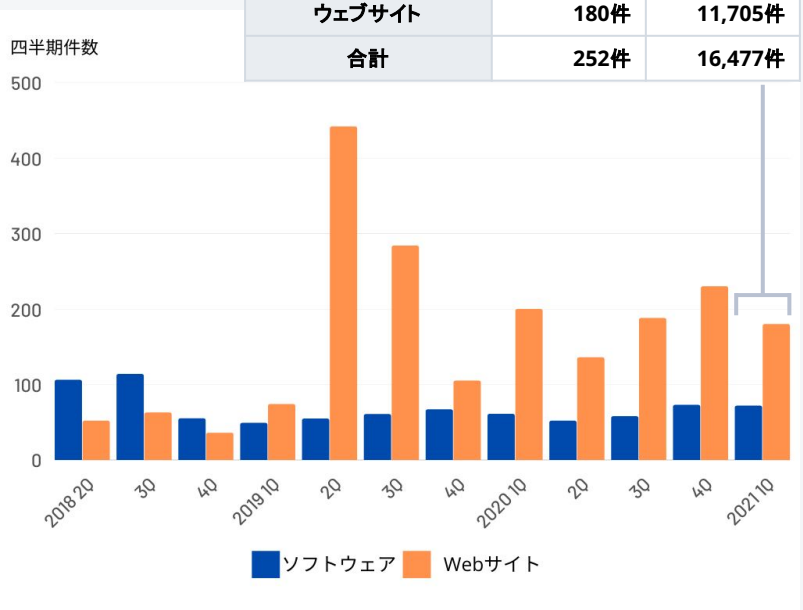
（ソフトウェア 72件、Webサイト 180件）

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。

開発現場とセキュリティとの良い関係を築くステップ

Securify Scan

ステップ2

セキュリティ対策の知識向上

セキュリティに関する分野は専門性が高く、難しいと感じる方も多くいらっしゃると思います。

まずは「**小さく分解して、できるところから始める**」ことをオススメします。

アプリケーションレイヤーのセキュリティと言っても、いくつもの種類があります。現状を鑑みて、どこからなら着手できそうかを仕分けをして、小さくできるところから始めていけば、着実に効果が出てきます。

また、「**チーム全員でセキュリティの本を輪読する**」など、チームメンバー全員が何らかの形でセキュリティにふれることで、知識をチーム全体でキャッチアップしつつ、当事者意識を持つ取り組みもオススメです。

開発現場とセキュリティとの良い関係を築くステップ

Securify Scan

ステップ3

開発プロセスにセキュリティ対策を組み込み

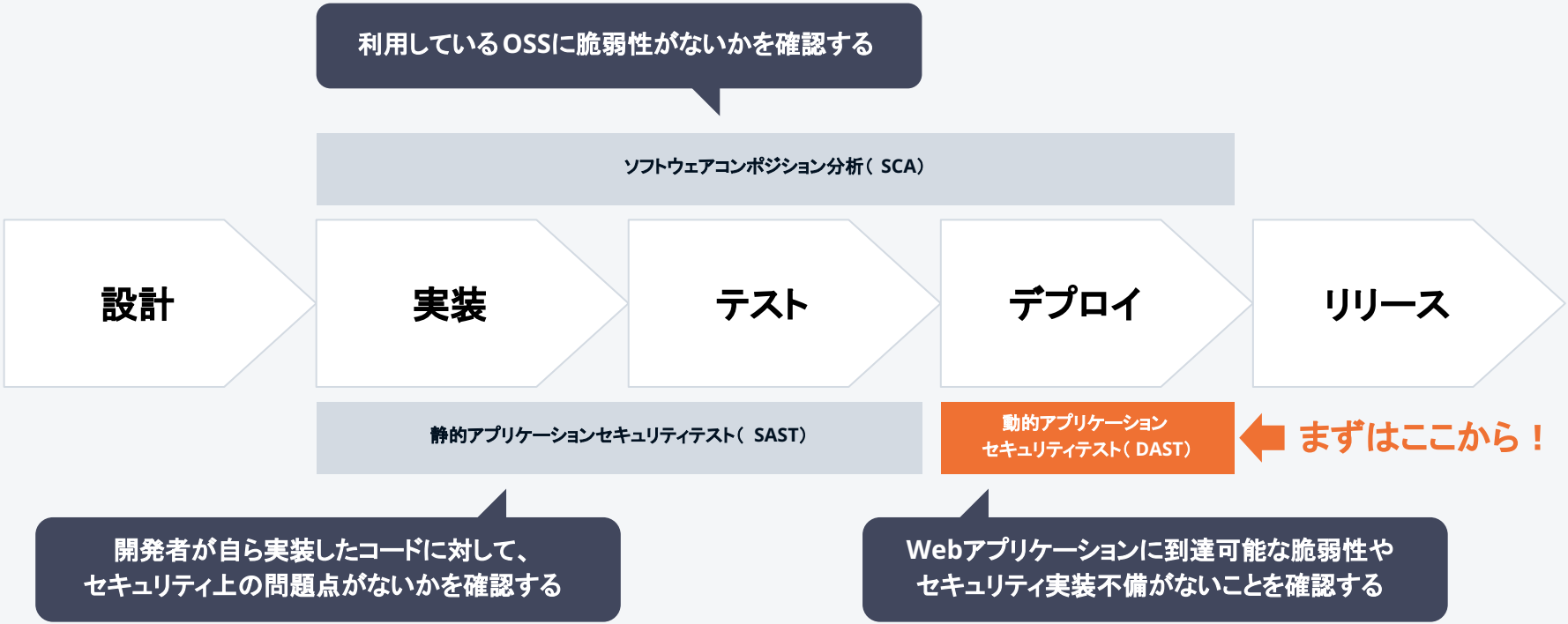
脆弱性診断をリリース直前にやっていた場合は、開発の**実装・テスト工程**でセキュリティチェックを自社内でかけることで**最低限のセキュリティ品質を担保**しながら、スピーディーに開発を進めることができます。

開発プロセスに組み込む際には脆弱性診断ツールを利用することが考えられますが、あくまで、ツールとして最低限のチェックであるという認識が重要です。

ツールの性質上、手動による脆弱性診断よりも精度は劣ることがあるため、リリース時の変更箇所やスケジュールを考慮し、手動の脆弱性診断もセットで実施することをオススメしております。

開発現場とセキュリティとの良い関係を築くステップ

Securify Scan



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.