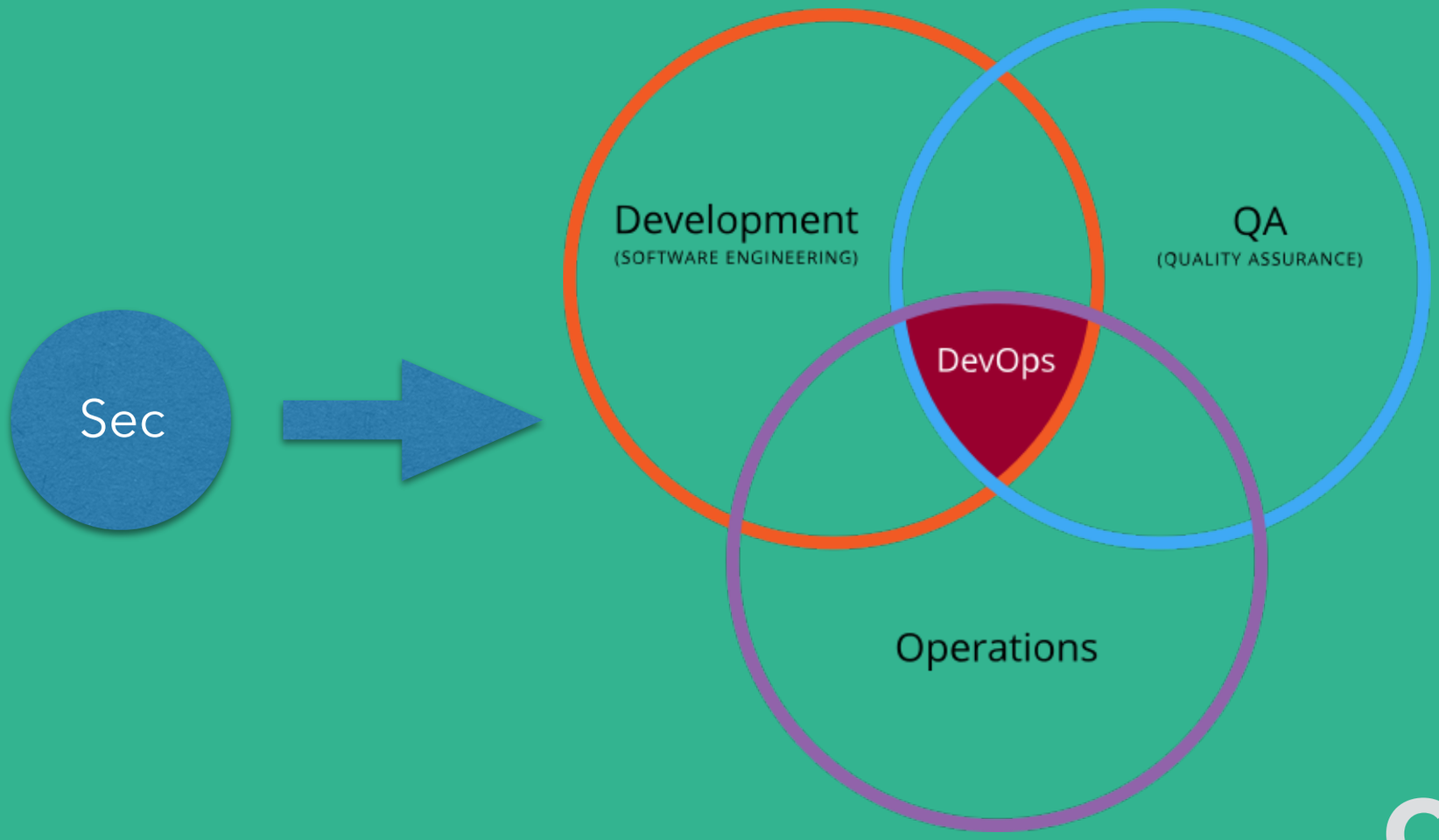
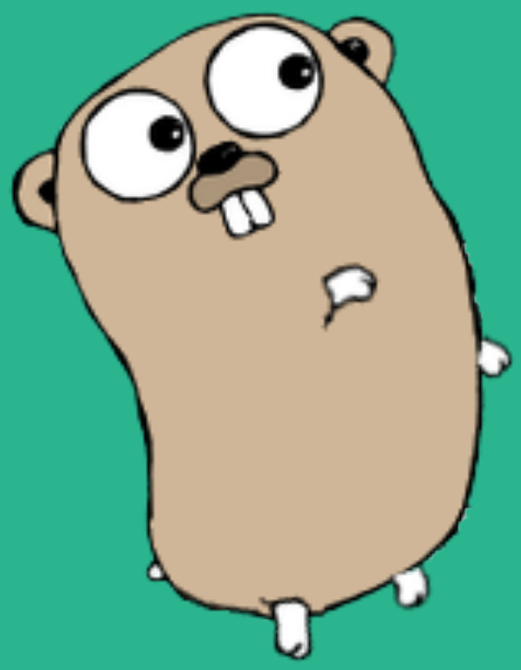
はじめようDevSecOps



CC By Rajiv.Pantderivative

CypherTec Inc.

yu fujioka



whoami

yu fujioka:

所属：CypherTec Inc.

- Software Engineer 兼 Security Engineer
- ソフトウェア開発やセキュリティ診断業務を担当
- Go と Docker とサーバーレスアーキテクチャが好き

この LT の内容は個人の見解であり、
所属する組織の見解と必ずしも一致するものではありません。

まずは

DevOps

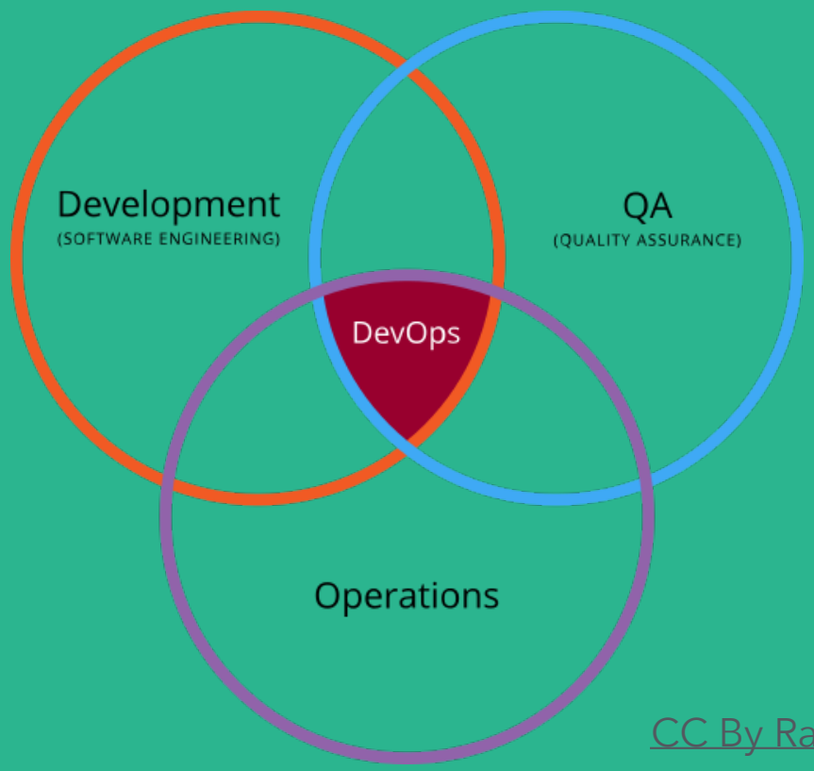
のことを知っていますか？

Development 開発

Operations 運用

開発、運用等の異なるセクションが連携・協力して進めるという概念。
この用語を捉える明確な定義はなく、アジャイルの流れの中で発生したムーブメント、カルチャーと捉えると分かりやすい。

※2007年頃からその雛形が生まれ始めるが、2009年の Flickr 社員のプレゼンで広く認知される。
頻繁に変更が発生するアジャイル開発の現場で起きた開発チームと運用チームの軋轢を
取り上げ、開発と運用をシームレスに統合させる必要性を述べた。



どうやって実現するの？

ざっくり言うと

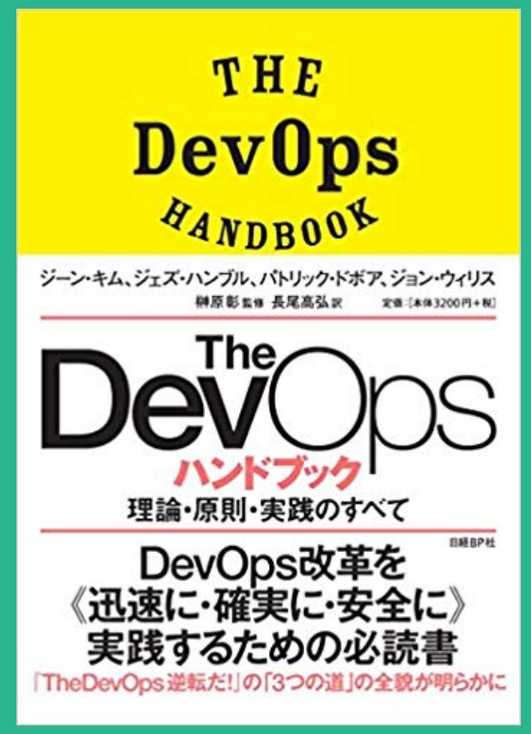
1. 組織改革
   デリバリーに関わるさまざまなチームの協調を育み、組織が
   一丸となって問題解決に当たり、新しい知識、知恵を生み出していく
2. 自動化
   技術やツールを用いて、デリバリーに関わるさまざまなプロセスを統合する
   ex) IaaC, Ansible, Chef, Jenkins, Selenium...

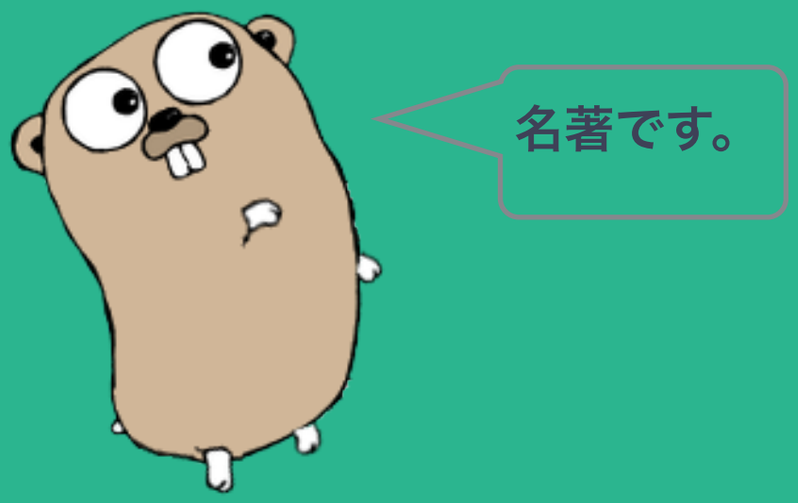
天文学が望遠鏡ではないのと同じように、
DevOpsはオートメーションではない（Christopher Little）

何を持って達成と言えるの？

ゴールはない。（多分）

THE DevOps ハンドブック(2017)では組織論や自動化以外にも、個人のマルチタスクの制御や生涯学習の必要性などにも言及している。
DevOps の手法を適用することによって
成果は上がるが、改善し続ける作業に終わりはない。





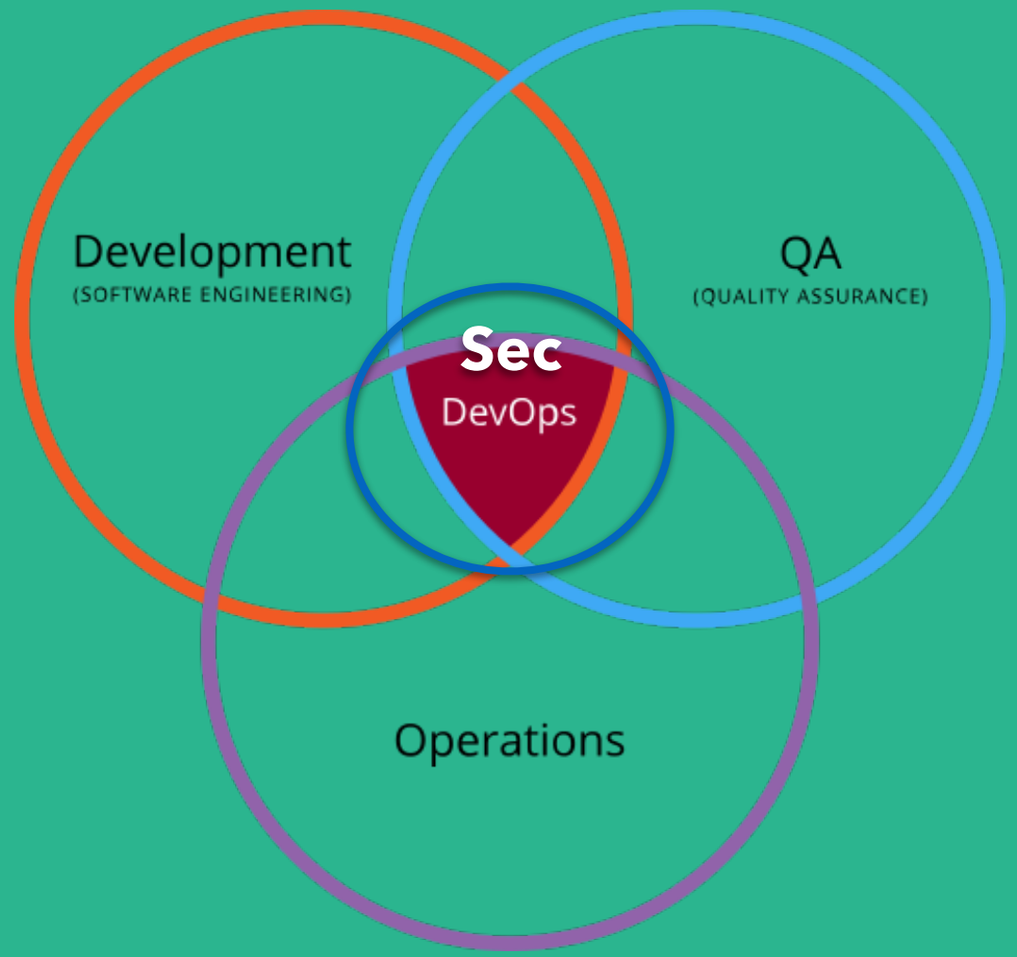
小さな組織の DevOps

当社のような小さな組織(社員10名程度)では、
開発担当者と運用担当者が同じというケースが多い。
　👉そのためセクショナリズムに起因する諍いは起こりづらい

しかしその分個々の担当者の負担は大きく、
自動化によってプロセスを統合する必要性は高い。

組織改革については各社で頑張ってください！

What is DevSecOps ?



Development 開発

Security セキュリティ

Operations 運用

2018年頃からDevOps におけるセキュリティの重要性を強調するため、DevSecOps という言葉が使われ始めた。

しかし、元々 DevOps はセキュリティも含めた広範な概念であり、実は目新しい話ではない。

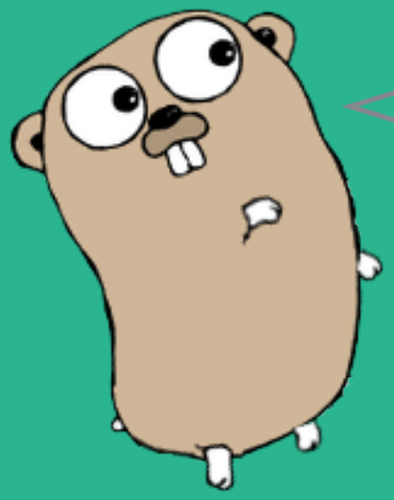
⇒ 2016頃から、RuggedDevOps や DevOpsSec という言葉は存在している。

コンテキストが異なるだけで、実質的に
DevOps === DevSecOps と理解している。

DevOps におけるセキュリティの重要性

従来のように開発の最後にセキュリティチェックを行うと、DevOps のサイクルはそこで止まらざるを得ない。

そして通常のテストと同様、開発の後半になればなるほど手戻りによる痛みは大きくなる。



情報セキュリティによる足止めはそのなかでも最悪なものの1つ

(JustinArbuckle)

⇒DevOps のサイクル全体にセキュリティを浸透させる必要がある

DevOps にセキュリティを浸透させるポイント

~THE DevOps HANDBOOK より~

・セキュリティチームを開発の初期段階から関わらせ、
開発サイクルの中でセキュリティの情報を浸透させる

社内にセキュリティチームがいれば良いけど・・・

・典型的なIT組織では開発、運用、セキュリティのエンジニアの比率は100:10:1
開発サイクル全体にセキュリティを浸透させるにはその一部を自動化し、
開発と運用の日常業務に情報セキュリティを組み込む必要がある。

自動化はツールでもできそう。できることから始めよう！

でもセキュリティのツールって
お高いんでしょう？

高機能な製品は安くはないですね・・・

Product	Price	Remarks
IriusRisk	ASK	価格はアプリ数毎。Community Edition がある
ThreatModeler	ASK	
Evident.io(ESP)	$199 per month and scale to support AWS environment	
Checkmarx	ASK?	
Contrast Security	ASK	Community Edition がある。日本の代理店もある
IMMUNIO	Free~$999	
Aqua Security	GCP Marketplace で $0.33/hour	
Dome9 Security	ASK	
WhiteSource	$4,000~	

上記は 9 Great DevSecOps Tools for Dev Teams to Integrate Throughout the DevOps Pipeline で紹介されていたツールを調べた価格表
先月の Software Design に載っていた WhiteSource も $4,000~ とお高め

Qiita に翻訳記事を投稿しています。

⇒開発チームのための DevOps パイプラインを統合する９つの優れた DevSecOps ツール

お金ないんだけど

OSS でなんとかできないかな・・・？

多分できる！

<table>
<tr><th>対象</th><th>内側から試験</th><th>外側から試験</th></tr>
<tr><td>アプリケーション</td><td>(UnitTest)</td><td rowspan="2">OWASP ZAP</td></tr>
<tr><td>アプリケーション
ライブラリ</td><td>Vuls + OWASP
Dependency Check</td></tr>
<tr><td>ミドルウェア</td><td rowspan="2">Vuls</td><td rowspan="2">Nmap, Nessus,
Metasploit,
OpenVAS</td></tr>
<tr><td>OS</td></tr>
<tr><td>NW機器</td><td colspan="2">Vuls + OVAL</td></tr>
<tr><td>可視化</td><td colspan="2">Vuls repo or faraday</td></tr>
</table>

上記は Future Architect 社らのメンバーの「ぼくの考えたさいきょうのDevSecOps」より抜粋
⇨素晴らしい資料。やりたいこと全部書いてあった。

OSS では他にも Nikto や OWASP Benchmark、さまざまなツールがあります。
OWASP の Free for Open Source Application Security Tools にもまとまっています。

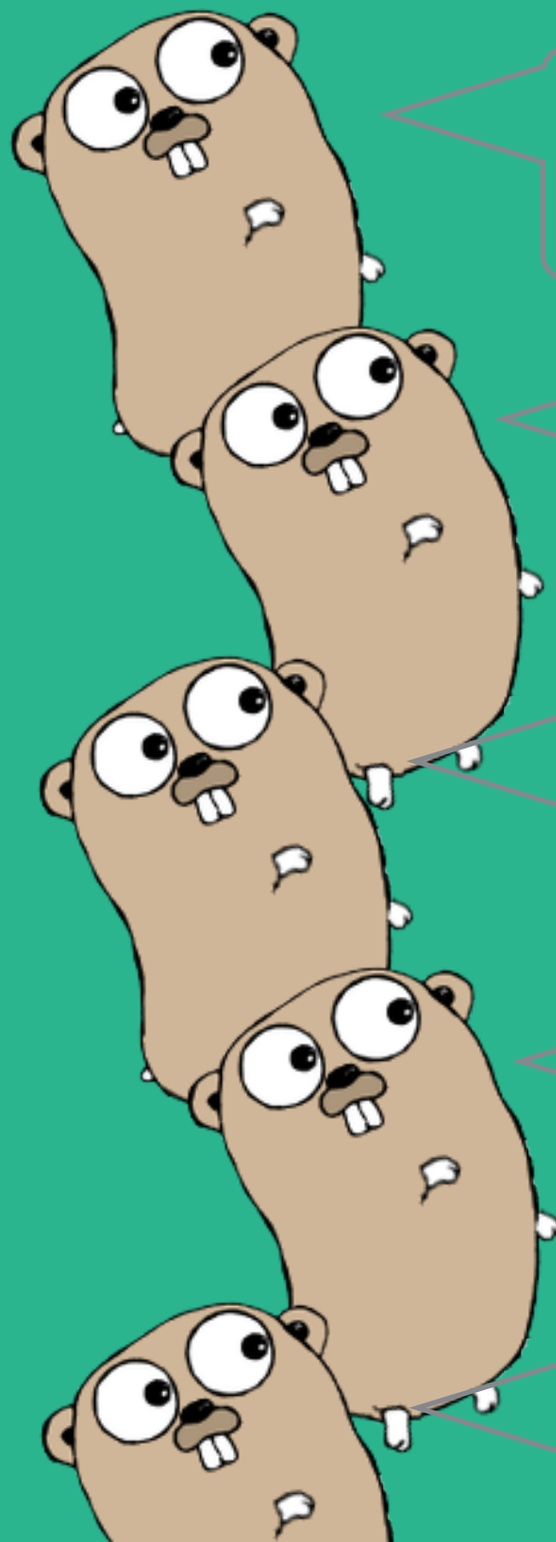
そもそも CI/CD のパイプラインすら構築してないから無理だよね・・・？

できることは沢山ある！

- 全部を一度にやろうとしたらエンジニアが死ぬ
  インフラ、コード、ライブラリ、アプリケーション、
  それぞれに適したセキュリティツールを一つずつ
  導入していき、少しずつでも改善していくことが大事。
- npm audit コマンドを定期的に実行することや、
  GitHub の Security Alert にちゃんと対応することも
  立派なセキュリティ対策と言える。

セキュアコーディングも大事だし、セキュアな言語の採用なども重要。
Go はエラーハンドリングやテスト駆動開発がし易い言語なのでおすすめ

正論という名の改善への障壁



そんなことより先に自動テスト書いてよ

レガシーコードのリファクタが先でしょ

それよりもまずコンテナ化しようよ

マイクロサービス化してからの方がやりやすいよ

夏季休暇ちゃんと取得した？

よく使われる反論

なんとか Pay みたいになっても
良いんですか？

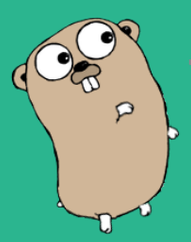
セキュリティの優先度は決して低くない

- 世界に衝撃を与えたパナマ文書の流出は WordPress の古いプラグインの脆弱性が利用された。
  ⇒自動チェックさえしていれば確実に防げた事故
- 「脆弱性対策情報の公開に伴う悪用増加」は、2018年情報セキュリティ10大脅威の第4位
- セキュリティ・インシデントが発生してしまった時の膨大な損失

7 Pay のニュースを見ると胃が痛くなるのは私だけでしょうか？

reference

- The DevOps ハンドブック 理論・原則・実践のすべて
- DevOpsとは何か？ そのツールと組織文化、アジャイルとの違い
- DevOps(Wikipedia)
- RedHat : DevSecOps とは
- 9 Great DevSecOps Tools for Dev Teams to Integrate Throughout the DevOps Pipeline
- 開発チームのための DevOps パイプラインを統合する９つの優れた DevSecOps ツール
- ぼくの考えたさいきょうのDevSecOps
- Nikto
- OWASP Benchmark
- Free for Open Source Application Security Tools
- IPA: 情報セキュリティ10大脅威 2018



The Go gopher was designed by Renée French.