Monthly Research 2016.9

脅威分析の役割と手法の紹介

F F R I , Inc.
http://www.ffri.jp

E-Mail: research-feedback[at]ffri.jp
Twitter: @FFRI_Research

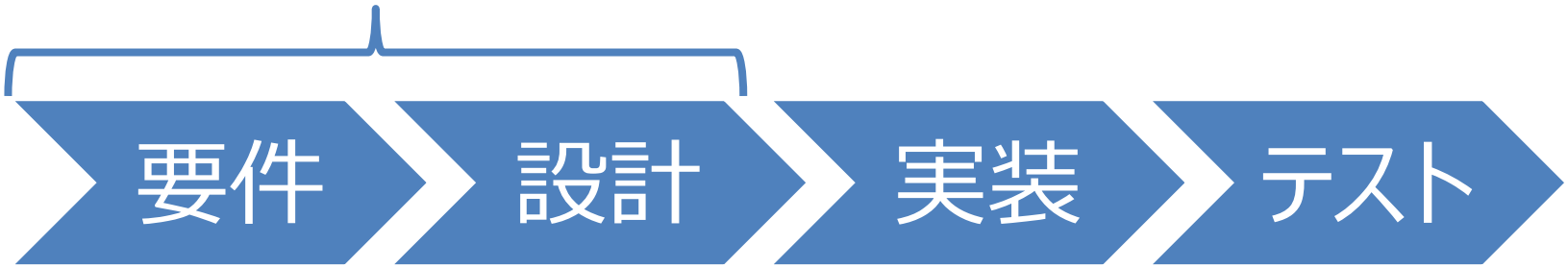
目次

- 脅威分析について
- 脅威分析の流れ
- 分析手法
  - DFD(Data Flow Diagram)
  - STRIDE
  - Attack Library
  - Attack Tree
- まとめ
- 参考情報

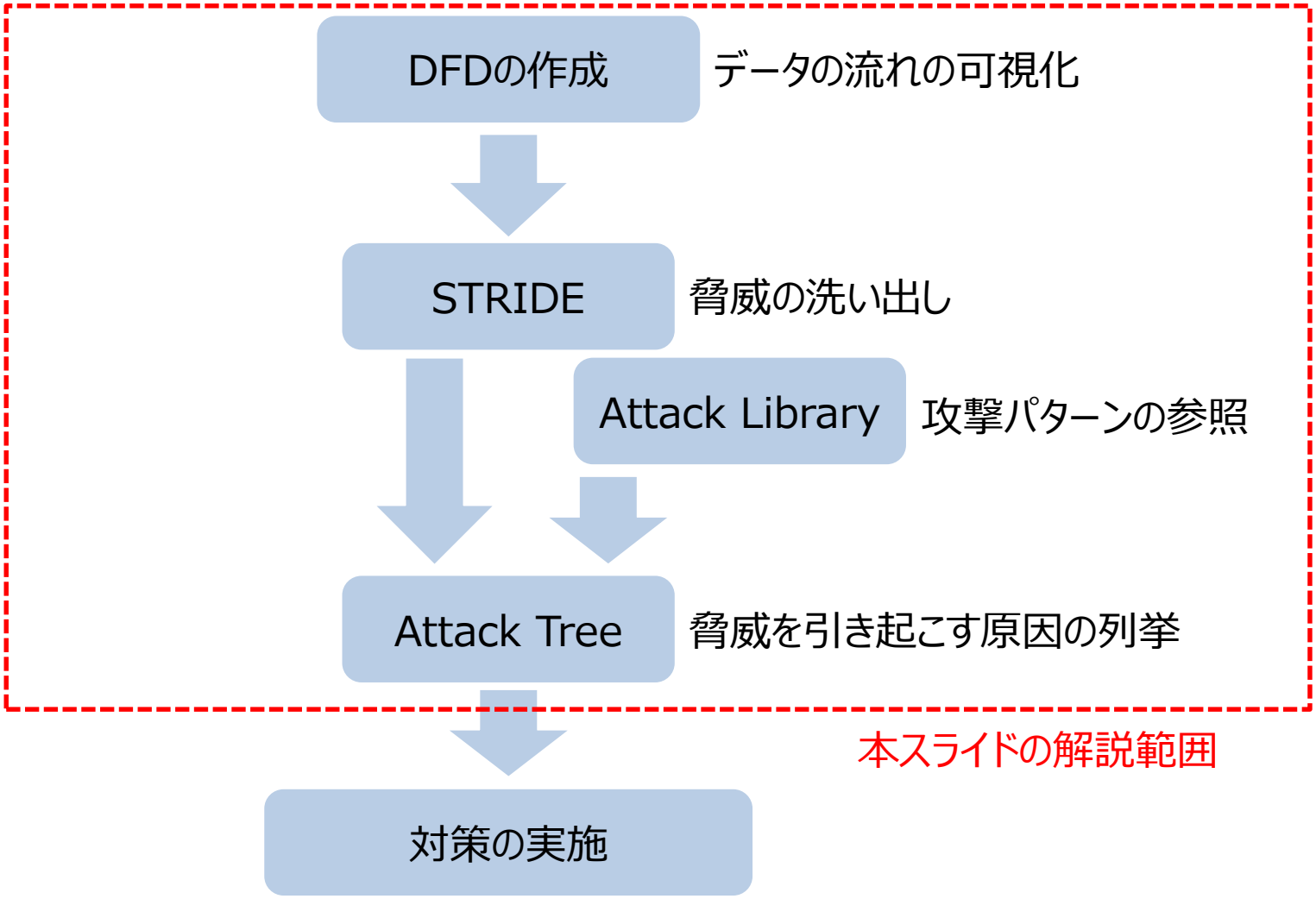
脅威分析について

- システムなどに対してのセキュリティ上のリスクを把握・対処するために行う作業
- 脅威について
  - 資産に損害を与える原因
    - 環境的脅威と人的脅威に大別される
- 脅威分析は以下の要件の策定と設計のフェーズで行う
  - 設計後に実施し、問題が発見された場合は要件/設計を見直す

脅威分析を行うフェーズ

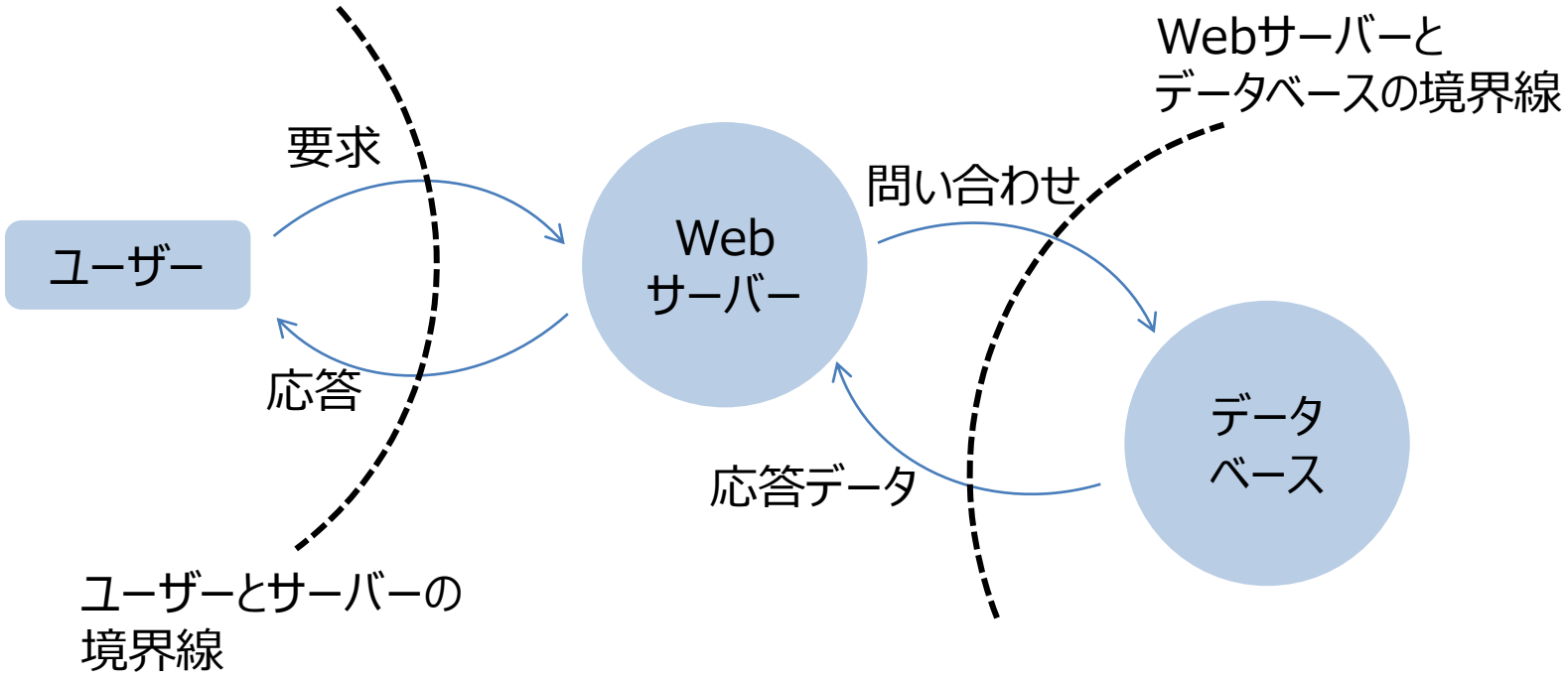


脅威分析の流れ(例)


DFDの作成
データの流れの可視化
STRIDE
脅威の洗い出し
Attack Library
攻撃パターンの参照
Attack Tree
脅威を引き起こす原因の列挙
本スライドの解説範囲
対策の実施

DFD(Data Flow Diagram)について

- DFDとは情報システムのデータの流れを図示したもの
  - システムへの入力や出力の関係が把握しやすくなる



STRIDE

- STRIDEとは?
  - システムに生じうる脅威を発見するための手法で広く用いられている
  - 脅威を6パターンの特性より導出する
- STRIDEとはそれぞれ情報セキュリティに関する要素の頭文字である

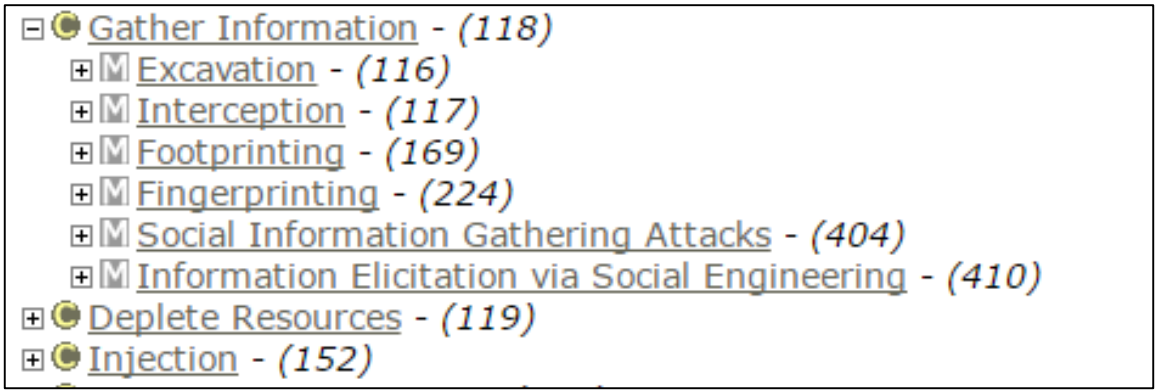
要素名	概要	脅威例
Spoofing	なりすまし	第三者が正規のユーザーを装う
Tampering	改ざん	データを偽造する
Repudiation	否認	ログの消去により証拠隠滅を図る
Information Disclosure	情報漏えい	クレジットカード番号の流出
Denial of Service	サービス妨害	サーバーに多大な負荷をかける
Elevation of Privilege	権限昇格	管理者権限が取得される

STRIDEの例

- p5のDFDの例を利用して解説
- Spoofing: なりすまし
  - 悪意のある第三者が正規のユーザーになりすましてシステムにログインされる
- Tampering: 改ざん
  - データベースに記録されている情報を書き換える
- Repudiation: 否認
  - Webサーバーのアクセスログを消去して侵入の痕跡を消される
- Information disclosure: 情報漏えい
  - データベースから他の顧客情報が流出する
- Denial of Service: サービス妨害
  - Webサーバーにアクセスが集中し要求の処理ができなくなる
- Escalation of privilege: 権限昇格
  - Webサーバー内で不正なプログラムを実行される

Attack Library

- システムの脅威の列挙を効率的に行えるようにするためのもの
- STRIDEは抽象的であるため、それを補う形で脅威の具体例などを記録していく事によって有益な情報源となる
  - 脅威についての傾向などはMITREが公開しているCAPECなどが参考になる



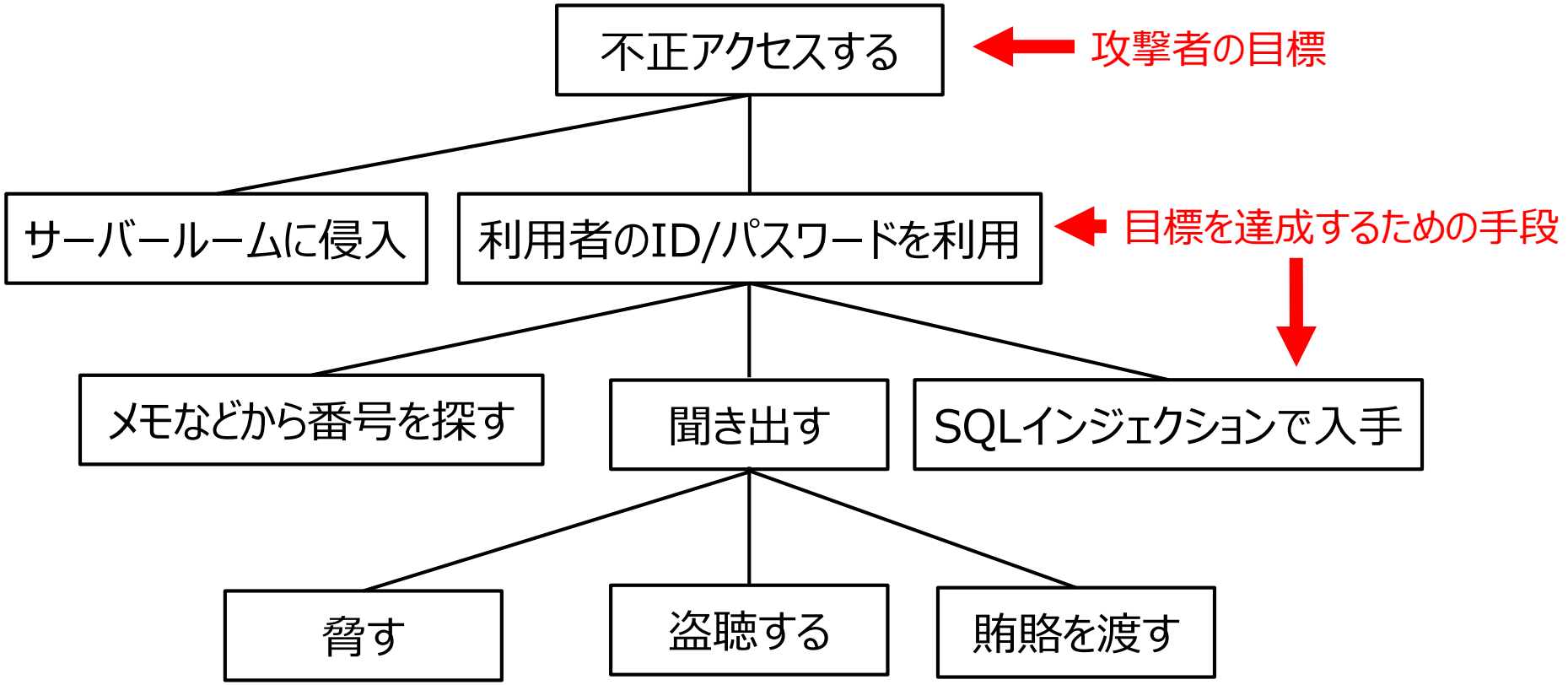
https://capec.mitre.org/

- 脅威情報について分類することによって作業の効率化が期待できる
- 一般的な情報を蓄積するため、一度作成すると別のプロジェクトでも再利用が可能
- 後述するAttack Treeの作成の際の参考になる

Attack Tree

- Attack Treeについて
  - 発見された脅威を引き起こす原因を列挙する方法である
    - Attack Treeは木構造で表現される
- Attack Treeのメリット
  - 調査対象の脅威についての攻撃手段を可視化できる
  - 攻撃されやすい箇所の特定が容易になる
- Attack Treeのデメリット
  - Attack Treeの作成には時間がかかる
- Attack Treeの作り方
  1. 攻撃者の目標を洗い出し、ツリーの一番上(ルート)に記載する
  2. 洗いだした目標についての攻撃手段を洗い出し、ノードに記載する

Attack Treeの例



まとめ

- 脅威分析を始める際にはDFDを基に分析を行う
- STRIDEは脅威を洗い出す際に、脅威の特性がパターン化されているので脅威の導出が行い易い
- Attack Libraryに過去に洗い出された情報を蓄積していく事によって作業の効率化が期待できる
  - CAPECは攻撃情報が網羅されているので作成の参考になる
- Attack Treeを用いる事によって脅威とそれを引き起こす原因の関係が把握しやすくなり、対策を考える際の有益な情報となる
- 一連のプロセスを経由することによって様々な視点からの情報が得られ、想定外の脅威の発見につながるなどの効果が見込める

参考情報

- Threat Modeling
  - http://as.wiley.com/WileyCDA/WileyTitle/productCd-1118809998.html
- Strategies for Threat Modeling脅威モデリングの戦略
  - https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnxzaWdzdGF3ZWJ8Z3g6NmE4NDhjYWNhOGYxMDBlOQ
- STRIDE
  - https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnxzaWdzdGF3ZWJ8Z3g6MmY4ZTgxNmY5ODFhZWY5MA
- Attack Trees
  - https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnxzaWdzdGF3ZWJ8Z3g6M2UzZDhjYWE5ZmU2NzJjYQ
- Attack Libraries
  - https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnxzaWdzdGF3ZWJ8Z3g6YmVkN2EwODFjMDcxMjg3
- CAPEC
  - https://capec.mitre.org/
- 脅威モデル分析
  - https://msdn.microsoft.com/ja-jp/library/aa561499.aspx