

SWEST28

皆でセキュリティの第一歩を踏み出そう！
初めての脅威分析ハンズオン

脅威分析・ハンズオン・モチーフ説明

●全体構成

- ハンズオンの概要と目標
- 脅威分析とは？
- ハンズオン（脅威分析）の全体像
- ハンズオンのモチーフ
- ハンズオンで利用するワークシート
- ハンズオンの手順
- ユースケース分析
- ハンズオンを始めよう！

●ハンズオンの概要と目標

• 概要

- 現在、悪い人にセキュリティを破られ社会問題となるケースが頻発しています
その際に、悪い人は製品やシステムの脆弱性（穴）を突いて悪事を働きます



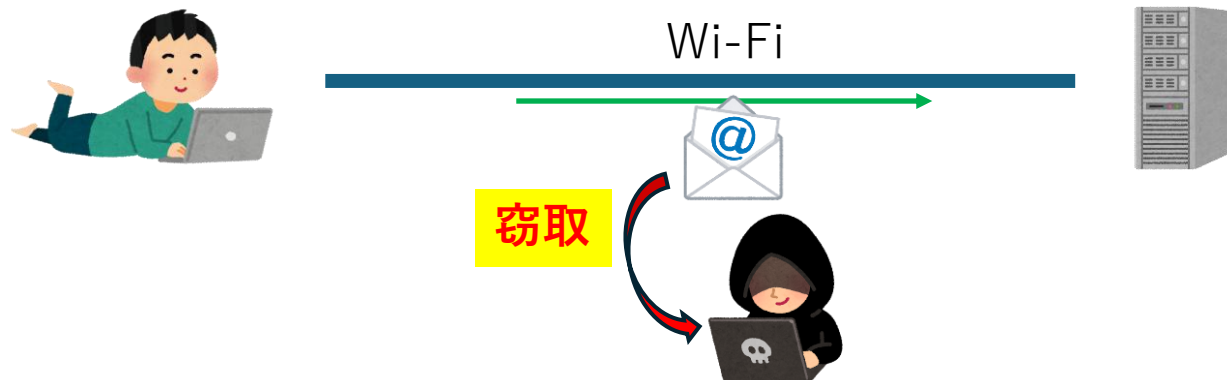
- そのため、本ハンズオンでは、セキュリティ強化（≡穴を塞ぐ）の第一歩として必要である「**脅威分析**」を体験してもらいます

• 目標

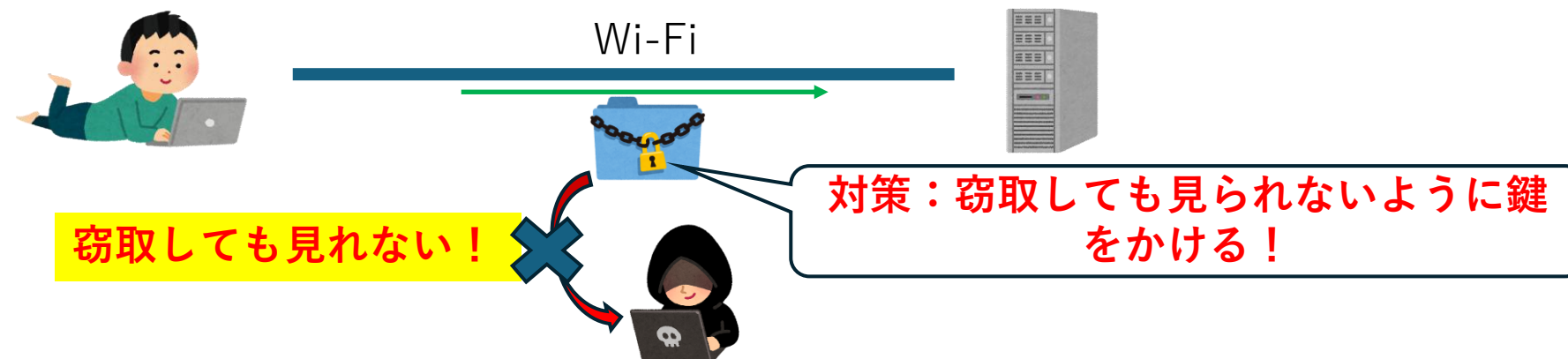
- 以下のような内容を持って帰ってもらうことを目標としています
 - セキュリティってこわいし、何やればいいかわからない・・・という状況から**ちょっとだけ前進する**
 - 「脅威分析とは？どういうことをやるもの？」を**なんとなく知ってもらう**
 - 今後、脅威分析を行うことになった際に「以前少しやったなあ」となるように**最初の一步を体験**してもらう
 - （意欲的な方には）脅威分析の知識を今後つけてもらうための**足掛かり**とする

●脅威分析とは？

- “脅威”とは、「**“守りたいもの”への攻撃**」を指します
 - 攻撃例：Wi-Fiで送信したメールが第三者に漏えいする

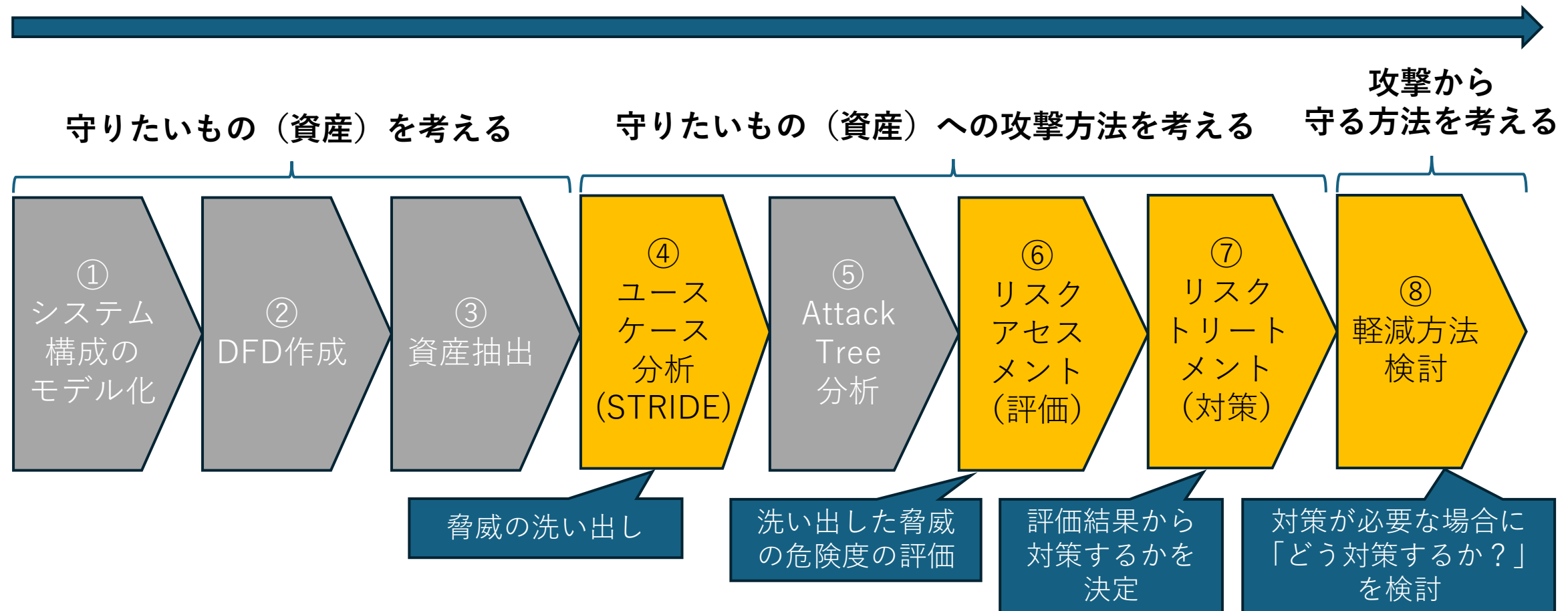


- “脅威分析”とは、「**守りたいものへの攻撃方法を洗い出して、攻撃から守り通すための対策を考える活動**」です



●ハンズオン（脅威分析）の全体像

- 脅威分析の全体像のうち、橙色の項目を今回のハンズオンで実施



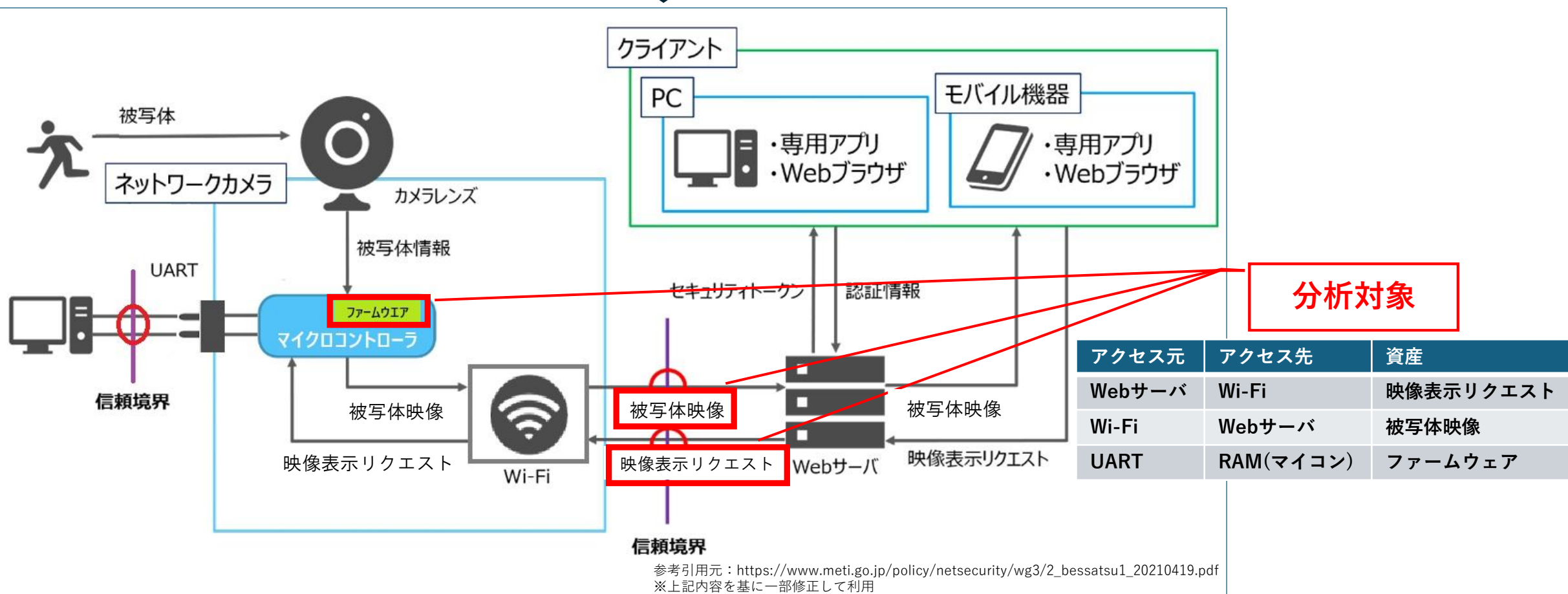
●ハンズオンのモチーフ



分析対象：
ネットワークカメラ
※ペットカメラ・見守りカメラを想定



モデル化・DFD図を作成



●ハンズオンで利用するワークシート

- 後スライドの手順にしたがって参考資料を見ながらハンズオンを実施し、班ごとに配布するワークシートを左側から順番に埋めてください
- 記載方法は自由ですが、皆さんが考えた内容をポストイットに記載してワークシートの各マスに貼り、班員で議論することを想定しています

この範囲がハンズオンの対象

アクセス元	アクセス先	資産	STRIDE (ガイドワード)	脅威	影響度	攻撃容易度	リスク	トリートメント	軽減方法
Webサーバ	Wi-Fi	映像表示リクエスト	S: なりすまし	①	⑬	⑭	⑮	⑯	⑰
			T: 改ざん	②					
			R: 否認	—	—	—	—	—	—
			I: 漏洩	③					
			D: サービス拒否	④					
			E: 権限昇格	—	—	—	—	—	—

マス毎に記載

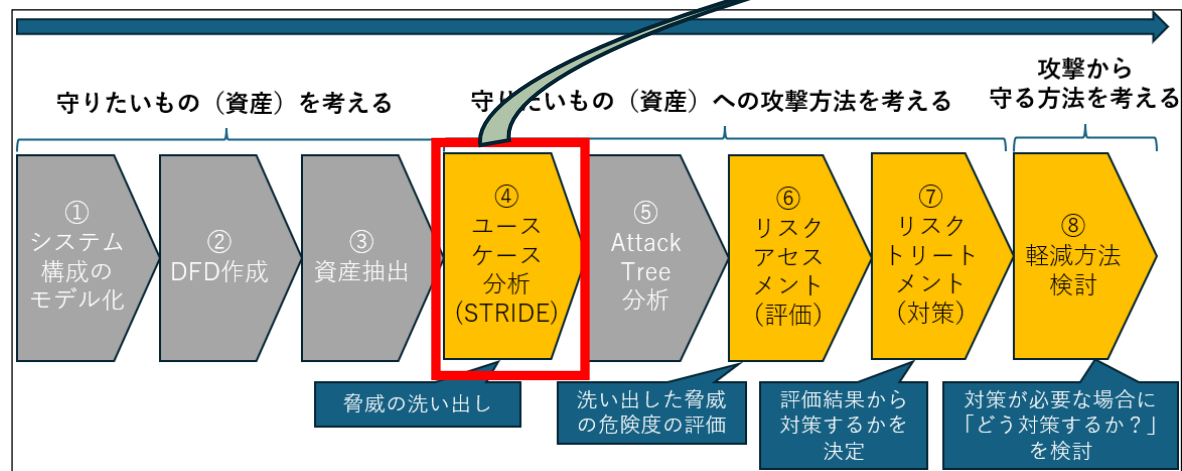
●ハンズオンの手順

※：時間に余裕がある場合に実施

No	内容	参考資料	時間
1	ユースケース分析 (STRIDE) ※次スライドで説明	STRIDEの脅威モデルと、脅威の例	30分
2	リスクアセスメント (1. で導出した脅威のリスク値算出)	影響と攻撃実現性、そしてリスクの評価	10分
3	リスクトリートメント (2. の結果から対策方針検討)	Treatmentの4つの選択肢	※
4	軽減方法検討 (3. で軽減を選択した脅威のみ)	リスクの軽減方法（各脅威に対する対策技術）	※
5	各グループから感想発表（準備込み）	—	10分
6	講評・まとめ	—	※

● ユースケース分析

- ユースケース分析には様々な方法がありますが、今回はSTRIDEを利用します
- STRIDEはガイドワードを利用した分析で、それぞれのワードに沿った脅威を考える分析手法です
- 参考資料を見ながら、各ガイドワードに対して脅威を考えてみてください



ハンズオン（脅威分析）の全体像

ユースケース分析の範囲

アクセス元	アクセス先	資産	STRIDE (ガイドワード)	脅威	影響度	攻撃容易度	リスク	トリートメント	軽減方法
Webサーバ	Wi-Fi	映像表示リスト	S: なりすまし	①	⑪	⑫	⑬	⑭	⑮
			T: 改ざん	②					
			R: 否認	—	—	—	—	—	—
			I: 漏洩	③					
			D: サービス拒否	④					
			E: 権限昇格	—	—	—	—	—	—

ガイドワード