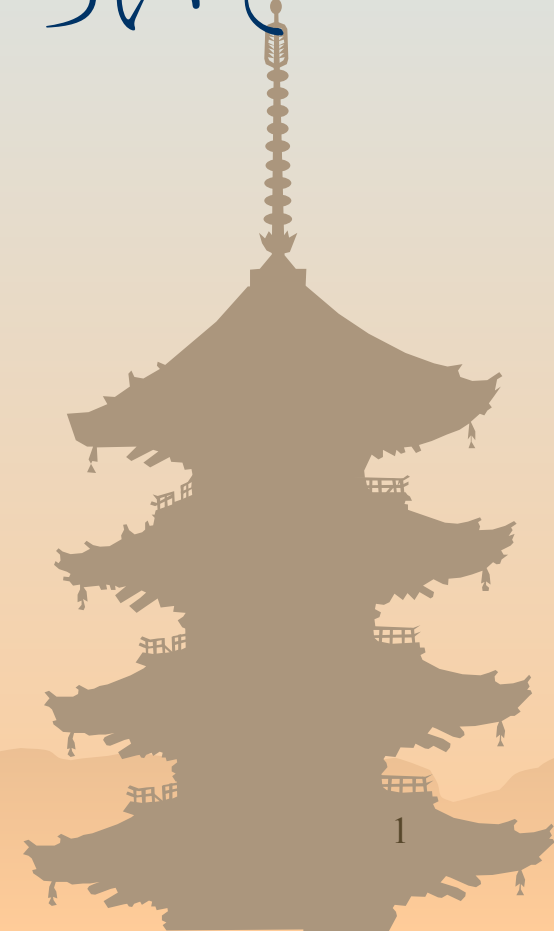


# 情報セキュリティ(9)

## アクティブディフェンスについて



# サイバー正当防衛 について考えみましょう

- 今回は、ちょっと技術から離れて(一服して)、ポリシーについて考えてみましょう。
- リアルな社会でも、さまざまな凶悪な犯罪が日々、報道されています。
  - 厚労省元幹部への傷害
  - 無差別な殺人 などなど
- このような危険に対しては、抵抗することが認められています(正当防衛)

# サイバー正当防衛 について考えみましょう

- それでは、サイバー上では、どこまで防衛措置としての、抵抗手段が許容されるでしょうか？
  - (D)DoSアタックを仕掛けてくるサーバには、カウンターアタックが許容されるでしょうか？
  - スパスメールサーバに対しては？
- 参考資料に、「アクティブディフェンス」という考え方が紹介されています。

# サイバー正当防衛 について考えみましょう

- これまでの情報セキュリティ対策は、基本的に「パッシブ (Passive)」な防衛です。
  - ファイアーウォールで守る
  - 暗号化して盗聴に対抗する
  - 認証 (パスワード、バイオメトリックスなど) 手段を講じる
  - 情報破壊に対してデータベースを二重化して対抗する など

# サイバー正当防衛 について考えみましょう

- パッシブな防衛は、コストもかかります。
- セキュリティ犯罪に対しては、そのもとから絶つ、という手段も考えられます。
- みなさんは、基本的に、アクティブディフェンスの考え方に賛成ですか、反対ですか？
- どのような条件がそろえば、アクティブディフェンスが許容されると考えますか？

# サイバー正当防衛 について考えみましょう

- 2008年ノーベル化学賞受賞者の下村脩さんのご子息、下村努さんは、情報セキュリティの専門家です。
  - クラッカー Kevin Mitnickの追跡者として(お父さん以上に?)有名です。
  - 資料のpptにあるデイビッド・ディットリッチは、当時、過剰防衛として訴えられました。
- どこからが過剰防衛でしょう？