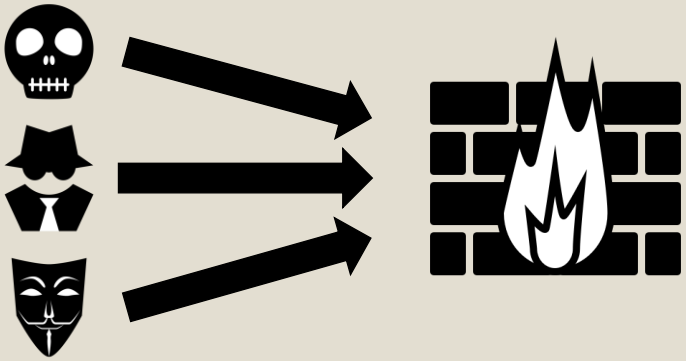
バッチ正規化を用いた ディープラーニングによる侵入検知手法

侵入検知システム（IDS：Intrusion Detection System）は、システムへの不正アクセスや管理者権限を奪う試みなどの**侵入行為(攻撃)を検知するシステム**である。

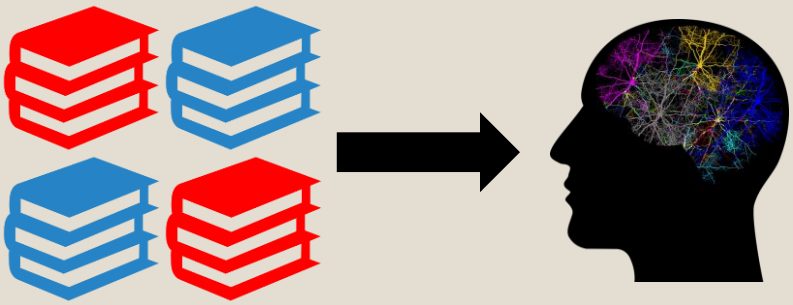
研究目的：理想のIDS

- **未知の攻撃**も検知できる
- **誤検知**が少ない
- **パターン定義**の自動化



提案手法：IDSへの応用

- 正常と攻撃の両パターンのデータを大量に用意し、ディープラーニングを用いて学習を行い、通信を判定する。



提案手法：既存IDSの改善

- 正常・攻撃の特徴や違いなどを明確に定義し、手動で登録しなければならない

→人間では発見できないような特徴や違いを定義でき、自動で学習してくれる

- 登録されていない攻撃は検知することができない

→新しい攻撃や亜種攻撃などにも対応できる