

情報セキュリティ基礎

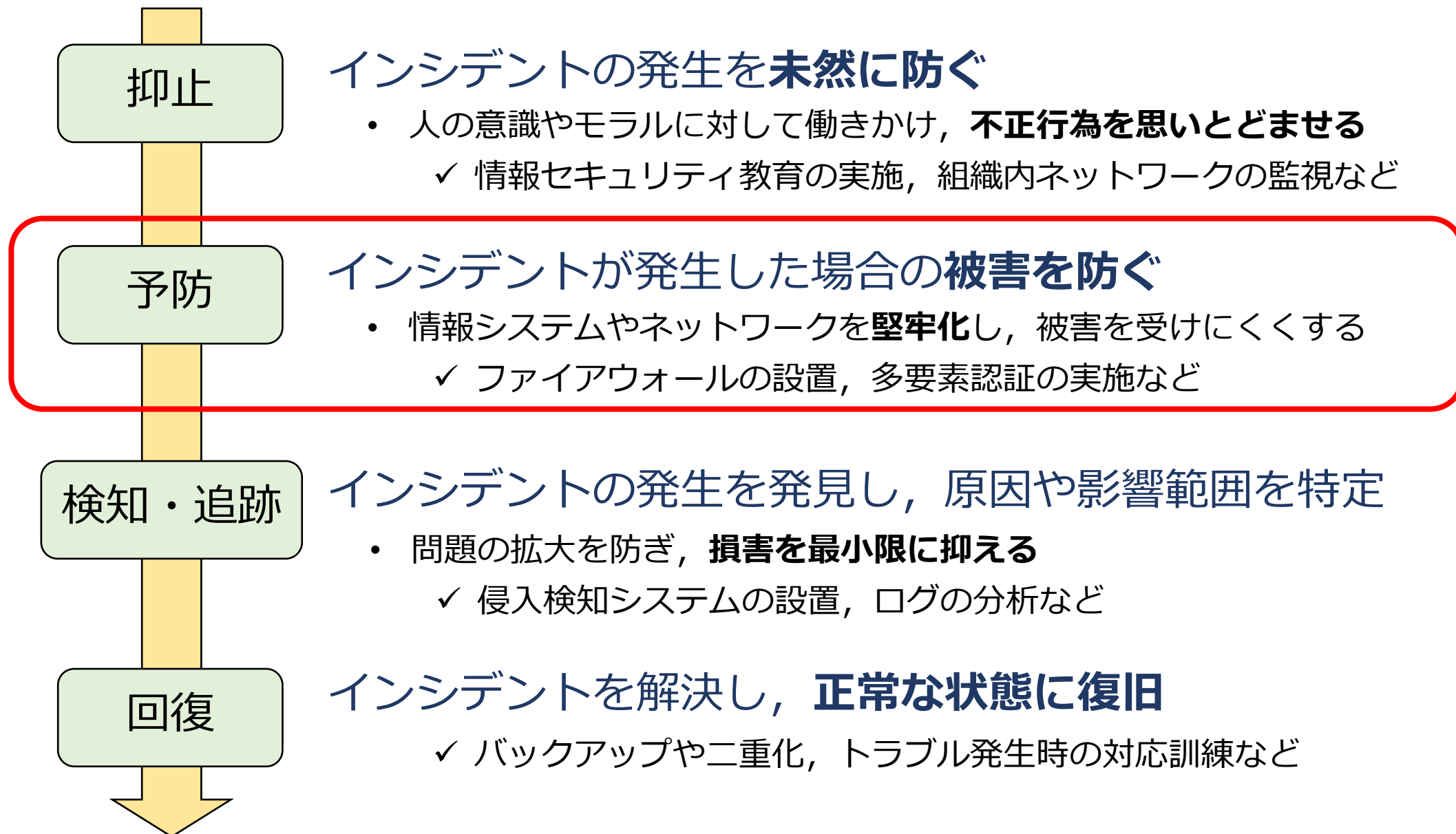
第7回 攻撃の検知と防御

藤本 章宏

今回の目標

- ファイアウォールやIDS/IPSの仕組みを知る
- それぞれのセキュリティ製品でできることとできないことを理解する

情報セキュリティ対策



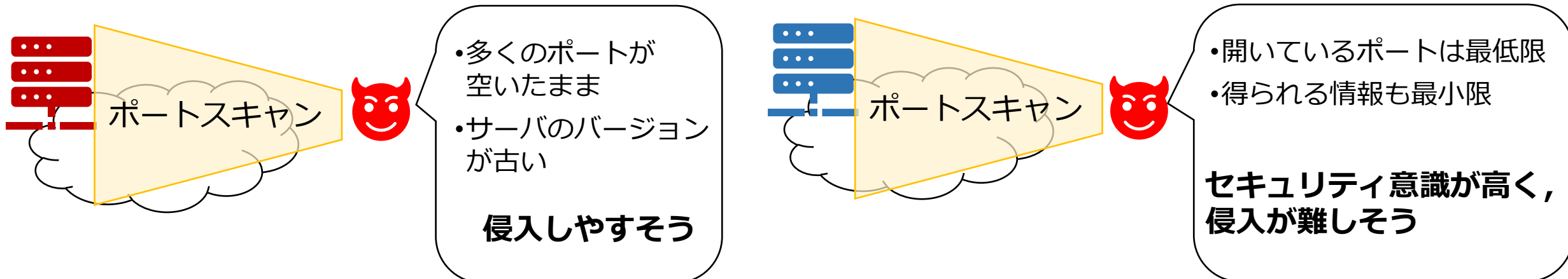
ホストの堅牢化（要塞化）

OS / ソフトウェアのバグや設定ミス等によって発生する
セキュリティホールを塞ぐこと

- ✓ OSやソフトウェアのバージョンを最新化
- ✓ セキュリティパッチの適用
- ✓ 不要なサービスや機能の停止

堅牢化の重要性

容易に侵入できないと思わせ、攻撃を思いとどまらせる



ホストの堅牢化における検討事項

原則として「最小限」を考える

- 最小限のサービスを運用
 - ✓ 最小構成でOSをインストール
 - ✓ 不要なサービスや機能を停止
 - ✓ 不要なエラーメッセージを返さない
- 権限を持ったユーザを最小限に
 - ✓ 不要なアカウントの削除
 - 利用するユーザアカウントについてもセキュリティ対策
 - ✓ 複雑なパスワードや、アカウントのロックアウト
 - ✓ ディレクトリやファイルには適切なアクセス権を設定

攻撃の予防・検知・防御

名称	特徴
ファイアウォール	主にIPアドレスやポート番号を使って設定されたルールに従ってパケットを通過/遮断
ネットワーク型IDS (Intrusion Detection System)	ネットワーク中を流れるパケットを監視し、通信の特徴を見て攻撃を検知
ホスト型IDS	インストールされたコンピュータを監視し、ログインの成功/失敗などの発生しているイベントから攻撃を検知
IPS (Intrusion Protection System)	ネットワーク型IDSと同等の機能に加え、実際に通信を遮断
ホスト型IPS	ホスト型IDSの機能に加え、攻撃を遮断
WAF (Web Application Firewall)	クロスサイトスクリプティング、SQLインジェクションなど、Webアプリケーションへの攻撃を検知・遮断
サンドボックス	セキュアな仮想環境で実際にファイルやリンク先へアクセスし、その結果を見て攻撃を検知

ファイアウォール

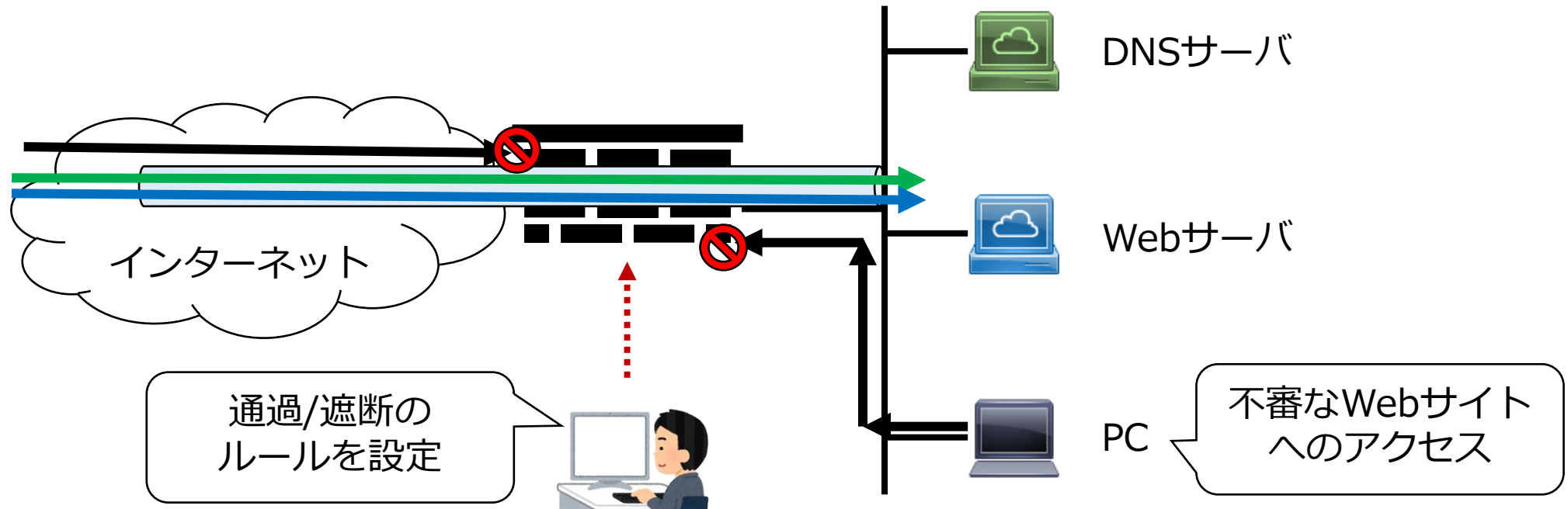
ネットワークセグメント間において、ルールに基づきパケットを破棄

- ✓送信元IPアドレス
- ✓宛先ポート番号

アクセス制御リスト
(ACL; Access Control List)と呼ばれる

注意点

通信速度を保つためには、十分な処理能力を持つFWが必要



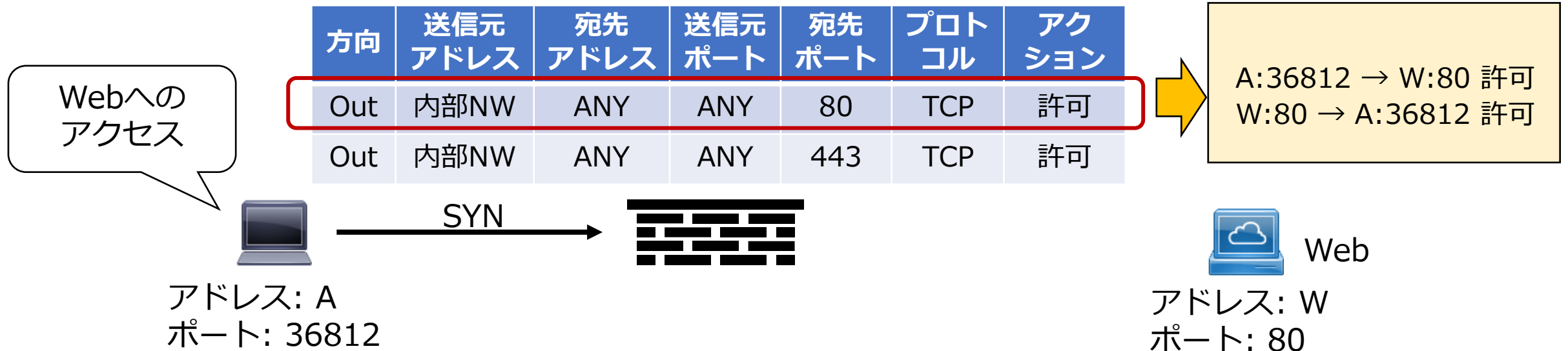
FWのフィルタリング方式

ステートフルインスペクション(≒動的パケットフィルタ)

- ✓ 通信開始時に、必要なルールを動的に設定
- ✓ 通信状態を監視し、不自然なパケットが見つかったと破棄

動作例

- ① 通信要求がFWに到着
- ② 許可されたセッションはセッション管理用テーブルに登録
通信用のルールを自動生成



FWで防御できない攻撃

基本的には、ACLに書かれたルールに従うアクセス制御

➡ ルールに則った通信は通してしまう

- 正規のアクセスに見える攻撃
 - ✓ （許可しているポートへの）ポートスキャン
 - ✓ パスワードクラック
 - ✓ Webアプリケーションへの攻撃（クロスサイトスクリプティング等）
- DDoS攻撃(多数の接続元からの攻撃)
 - ✓ 全ての攻撃元をルールに追加することは不可能
- マルウェアの侵入
 - メールへの添付, Webサイトからのダウンロード等は
（完全には）防げない

IDS (Intrusion Detection System)

発生している事象をリアルタイムに監視し，侵入や攻撃を検知

ネットワーク型侵入検知システム (NIDS)

ネットワークを流れるパケットをリアルタイムに監視

ホスト型侵入検知システム (HIDS)

ホスト内で発生するイベント（不正な操作，ファイルの改ざん等）
をリアルタイムに監視

WAF (Web Application Firewall)

Webアプリケーションに特化したIPSのような働き

✓ 典型的にはシグネチャのパターンマッチング

製品によって、様々な形で提供

- ✓ クラウド型
- ✓ アプライアンス型
- ✓ ソフトウェア型

ソフトウェア型

- ✓ Webサーバやリバースプロキシにインストール
- ✓ 比較的安価

クラウド型

- ✓ DNSの設定だけで済むので導入が容易
- ✓ DDoS対策とセットになっていることも
- ✓ カスタマイズはしづらい

インターネット

アプライアンス（専用機器）型

- ✓ 負荷分散や暗号化機能を備えた機種も
- ✓ 比較的高価。大規模なサイト向け

リバース
プロキシ

Web

