本資料について

- 本資料は下記書籍を基にして作成されたものです。文章の内容の正確さは保障できないため、正確な知識を求める方は原文を参照してください。

- 書籍名：ハッカーの挑戦
- 著者：Mike Schiffman
- 監訳者：白濱 直哉
- 発行日：2002年11月29日
- 出版社：株式会社 翔泳社

ハッカーの挑戦

名城大学理工学部
渡邊研究室
川島隆太

はじめに

- インターネットの普及により、コンピュータセキュリティのインシデントが増加
- ツールを使用するだけで簡単に攻撃が行えてしまう
- ハッカーによって被害者になることも、加害者にされてしまうのも日常化

攻撃の難易度

- 低：攻撃用のスクリプトの実行や既知の攻撃手法を使うのみ
- 並：既知の攻撃手法を利用するが、手を加えて攻撃を深めている
- 難：攻撃用のスクリプトを自作でき、独創的な攻撃を行う
- 極悪：未公開の攻撃手法に加え、自分の痕跡を隠したり、再侵入するための裏口を作成しておく

対策、復旧の難易度

- 低：修正パッチを1つあてたり、ソフトウェアのアップデートといったことで、簡単に解決できる
- 並：ファイアウォールのポリシー変更や、マシン自体の再インストールが必要となる
- 難：多くのマシンへの複雑なパッチ適用やアップデートに加え、主要インフラの再構築が必要となる

セキュリティホール、脆弱性 (1)

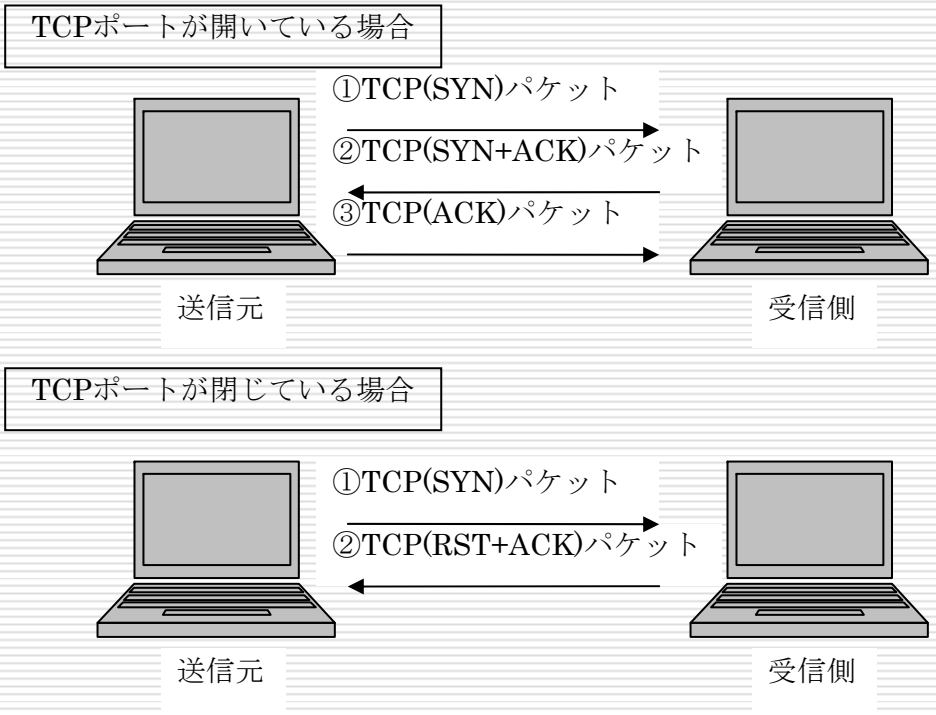
- ソフトウェアの設計ミスや不具合によって生じた、システムのセキュリティ上の弱点
- ネットワークにつながるあらゆるハードウェアやソフトウェアに存在
- 不正にコンピュータを操作されてしまう可能性
- ハッカーによる攻撃の起点

セキュリティホール、脆弱性 (2)

- 常にソフトウェアを最新の状態にしておくことが重要
  - こまめなアップデートの確認
  - 迅速な修正プログラムの適用
- ファイアウォールのフィルタリングルールの設定

ポートスキャン（1）

- サービスを提供しているマシン（サーバー）のポートに対してパケットの送受信を行い、ポートの開閉を調べる行為

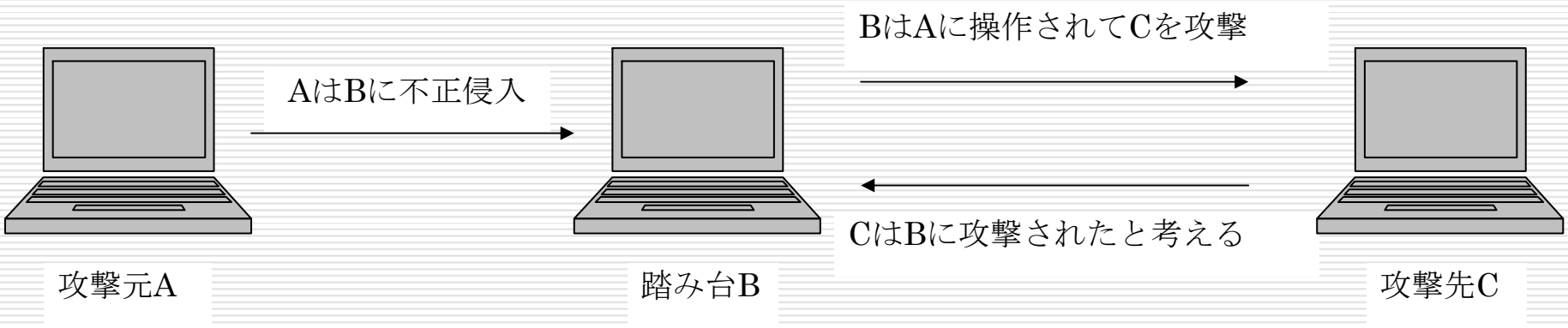


ポートスキャン (2)

- 標的から攻撃に必要な情報を収集するためのポートスキャンから、攻撃が始まる
  - 侵入口となりうるポートの有無を調査
  - パケット・フィルタリングの性能や設定を調査
- システム管理者はポートスキャンに敏感である必要がある

踏み台

- 不正アクセス等、攻撃の中継に利用されるコンピュータ
- 攻撃者を特定されにくくするために使われる一般的な手法
- 複数の踏み台が用いられることが多い

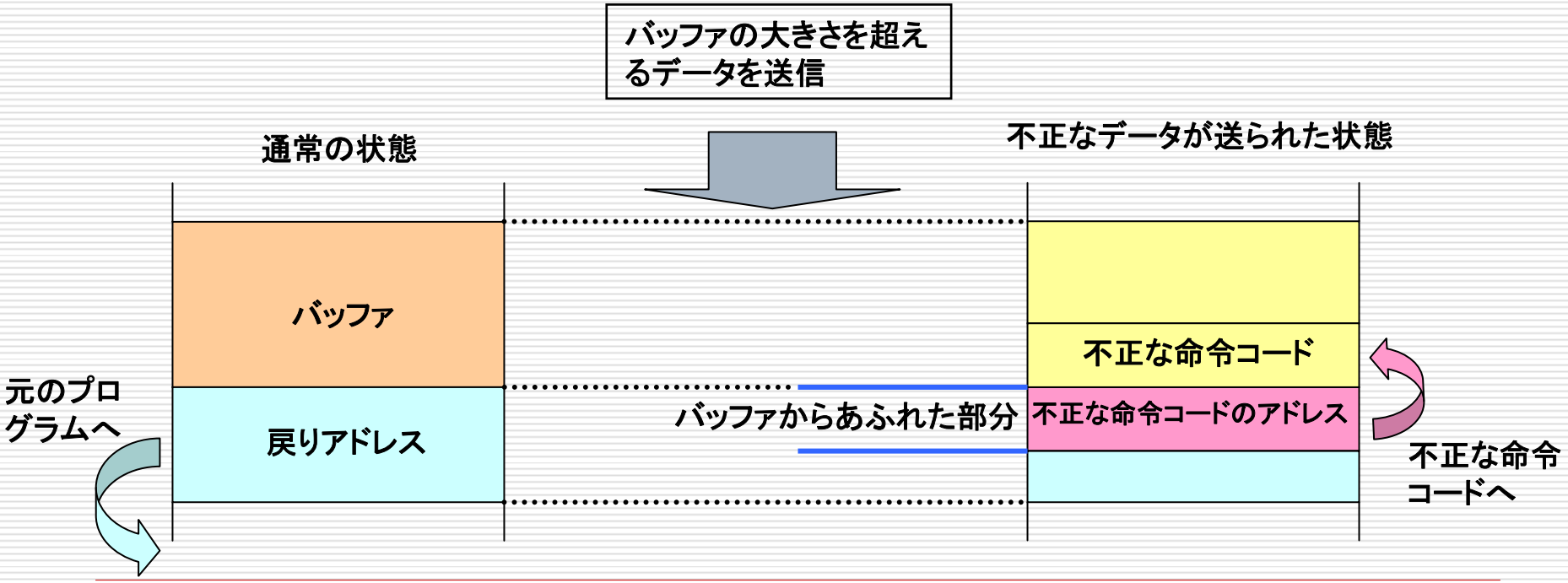


バッファ・オーバーフロー（1）

- セキュリティ・ホールを攻撃する代表的な手法
- サーバーとしての動作を停止させるサービス妨害（DoS）攻撃が可能
- いまだに決め手となる対策は存在していない

バッファ・オーバーフロー（2）

- バッファ・オーバーフローを利用した不正アクセス



DoS攻撃

- サーバなどのネットワークを構成する機器に対して大量のデータを送りつけるなどして、意図的に負荷をかけ、サービスを正常に提供できなくする攻撃
- 踏み台を利用して複数のコンピュータから一斉に攻撃をする分散型のDoS攻撃も存在
- 数の暴力を基本とした攻撃だが、それだけに防御が困難で効果的

ブルートフォース攻撃

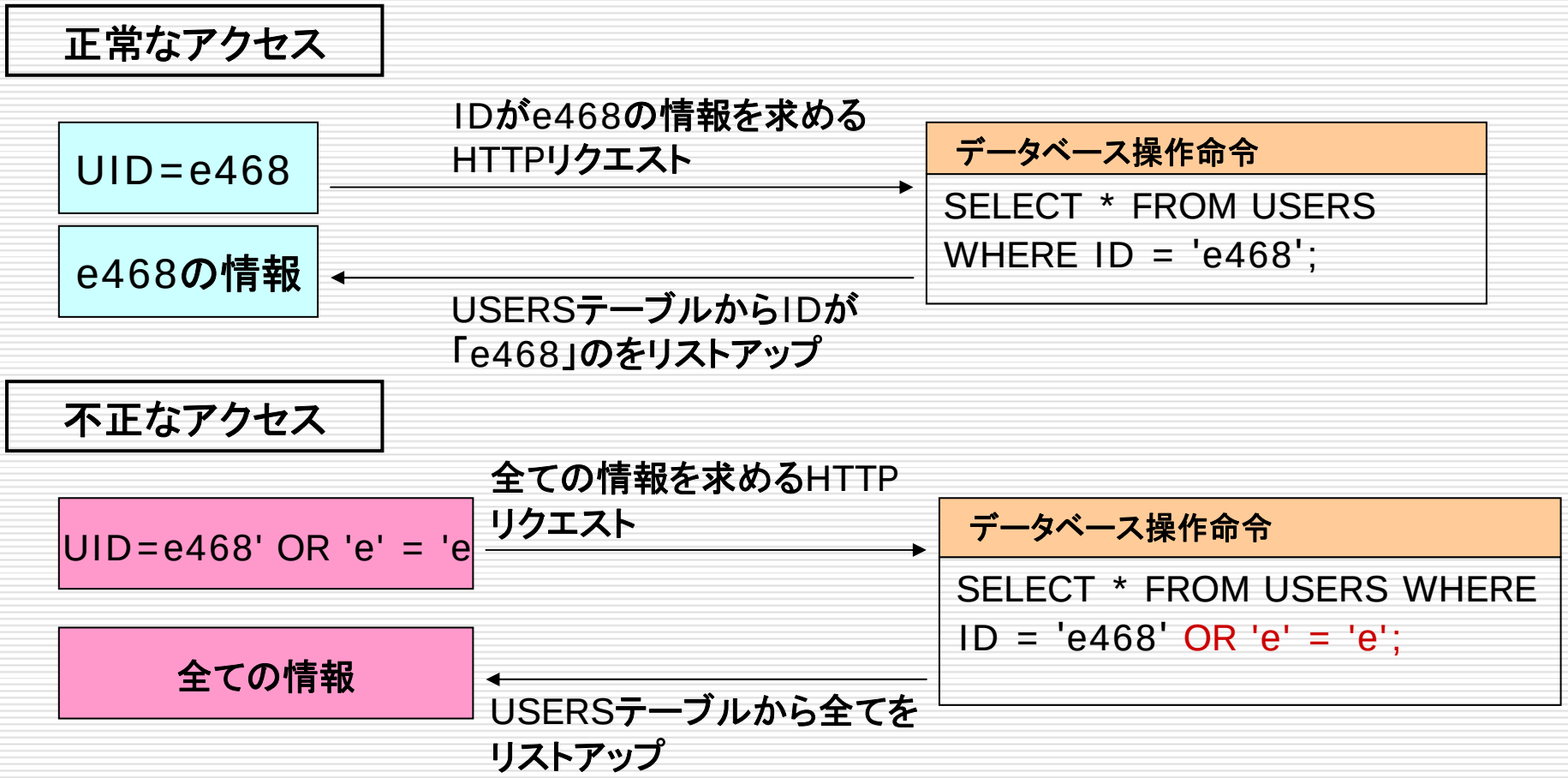
- 可能な文字の組み合わせを全て試していく暗号解読方法
- 効率の悪い攻撃だといえるが、時間をかければ確実に暗号解読できる
- パスワードとしてよく使われる文字列を用意しておく辞書攻撃もブルートフォース攻撃の一種
- パスワードに使う文字数、文字種を増やすことで解読を防げる可能性が増える

SQLインジェクション（1）

- Webサイトで、データベースへの問い合わせや操作を行なうプログラムにパラメータとしてSQL文の断片を与えることにより、データベースを改ざんしたり不正に情報を入手する攻撃

- 入力されたパラメータをチェックするだけで有効な対策となる

SQLインジェクション（2）



無線LANの危険性 (1)

- 無線の通信圏が広いと、攻撃者のウォードライブでアクセスポイントを見つけられてしまう
- 内部ネットワークに簡単に侵入できる可能性がある
- 無線LANでやりとりしているデータを盗まれる可能性がある
- インターネット接続の窓口として使用される可能性がある

無線LANの危険性 (2)

- 電波の強度を必要最低限に下げる
- 接続を許可するMACアドレスを制限
- WEP暗号による通信の暗号化
- アクセスポイントと他のネットワークの間にファイアウォールの導入

内部からの攻撃

- 内部の人間による攻撃を防ぐのは非常に難しい
- 権限をこまめに制限することで、ある程度防ぐことができる
- ワンタイムパスワードを利用した二因子認証
- 日常的なログの監査が重要

ルートキット

- コンピュータに不正に侵入した後に利用するソフトウェアをまとめたパッケージ
  - 侵入の痕跡を示すログイン記録を削除するツール
  - 再び侵入できるように裏口を設けるツール
  - ユーザーのキー入力を記録するツール
  - 自分の存在を隠す機能

- ルートキットを検出できるプログラムが存在する

不正侵入された場合の対応措置

- コンピュータを最初から構築しなおすことは、侵入前の状態に戻す信頼できる方法
- 攻撃により受けた被害、細工を全て見つけ出し修正するのには大きな労力がかかる
- どれだけ厳重に確認したとしても見つけられなかった攻撃が存在する可能性がある

まとめ

- 対策をするためには、どのような攻撃が行われているのか知っておく必要がある
- 新しい攻撃方法は常に生み出されているため、常に注意を怠らないことが重要