## 2.2.2 セキュリティホールの利用

セキュリティホール・脆弱性に関する情報

**ゼロデイ攻撃** - 脆弱性の対応までの日数がない攻撃

脆弱性を公開している組織

IPA: 情報処理推進機構

JPCERT/CC (Japan Computer Emergency Response Team Coordination Center)

JVN (Japan Vulnerability Notes)

→ 脆弱性情報データベース

**実習)** JVN を使ってみよう！

**関連)** IPA は情報処理関連の資格(IT パスポート含)にもあたっています

## 2.2.3 バッファオーバーフロー

アプリケーションのバグ(想定しない利用)を用いた攻撃

**バッファ** - データを一時的に保管しておくためのメモリ

データ(変数)や処理の流れ(戻りアドレス)が記憶されている

**関連)** C 言語プログラミングでの「配列の添字オーバーとプログラムの異常動作」

アプリの作成者などが修正プログラム(パッチ)を作成し適用する

プログラムの実行権限を調整する

## 2.2.4 サービス停止攻撃(DoS / DDoS 攻撃)

サービス(Web サーバ, メールサーバ など)を使用できなくする攻撃

DoS(Deny of Service), Distributed DoS

サービスを行っているホストの IP アドレスに対して

・過負荷をかける ← ホスト側での対策は困難

SynFlood 攻撃

メール爆弾

ホームページの大量アクセス

・異常処理を起こさせる

セキュリティホールなどの使用

分散(Distributed)攻撃

多数の踏み台ホスト → 攻撃用 bot の埋め込み(通常時はなにもしない)

→ ターゲットを一斉攻撃(通信開始)