インシデント対応について

2003年10月23日

日本ヒューレット・パッカード株式会社
セキュリティ・コンサルティング部
佐藤　慶浩

トピックス

① 国際動向：

ISO における Incident Management 関連文書

ISO / IEC IS 17799 での規格強化

ISO / IEC TR 18044 による新文書の作成

② コンピュータベンダーの脆弱性情報公開方針の紹介

HP 社の脆弱性情報公開方針

コンピュータベンダーの責務

お客様へのお願い

国際動向

国際的な動向

インシデント･マネージメントの関心は高い

ISO / IEC JTC1 の動向：

① ISO / IEC 17799 では、Incident Management のための章を新設する予定で検討をしている。

② ISO / IEC TR 18044 “Information Security Incident Management” を新規に作成している。

今週、パリで審議中。

ISO/IEC TR 18044 ISIM

インシデント・マネージメントの課題

Information Security Incident Management

Information Security Event

↓ ↓ ↓

Information Security Incident

既知のインシデント:手順に従う、分業による即時性

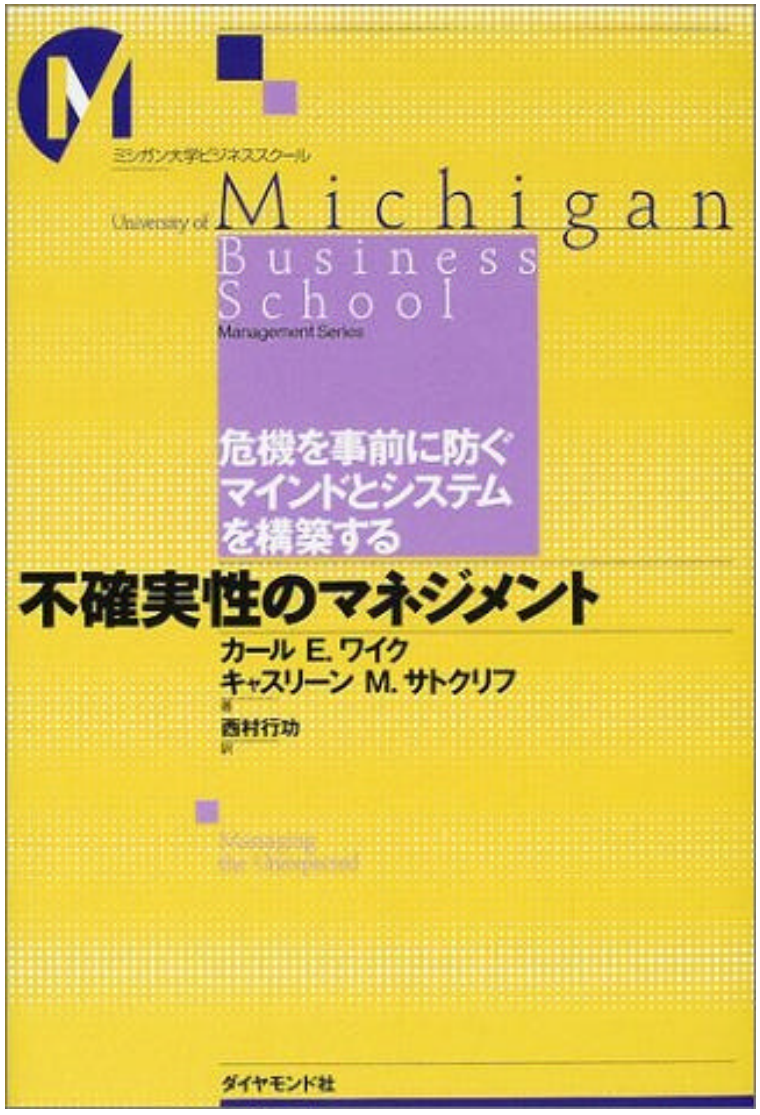
未知のインシデント:手順に束縛されない、分業の否定

推薦図書

Managing Unexpected

不確実性のマネジメント

出版 :ダイヤモンド社



ベンダーの脆弱性情報公開方針

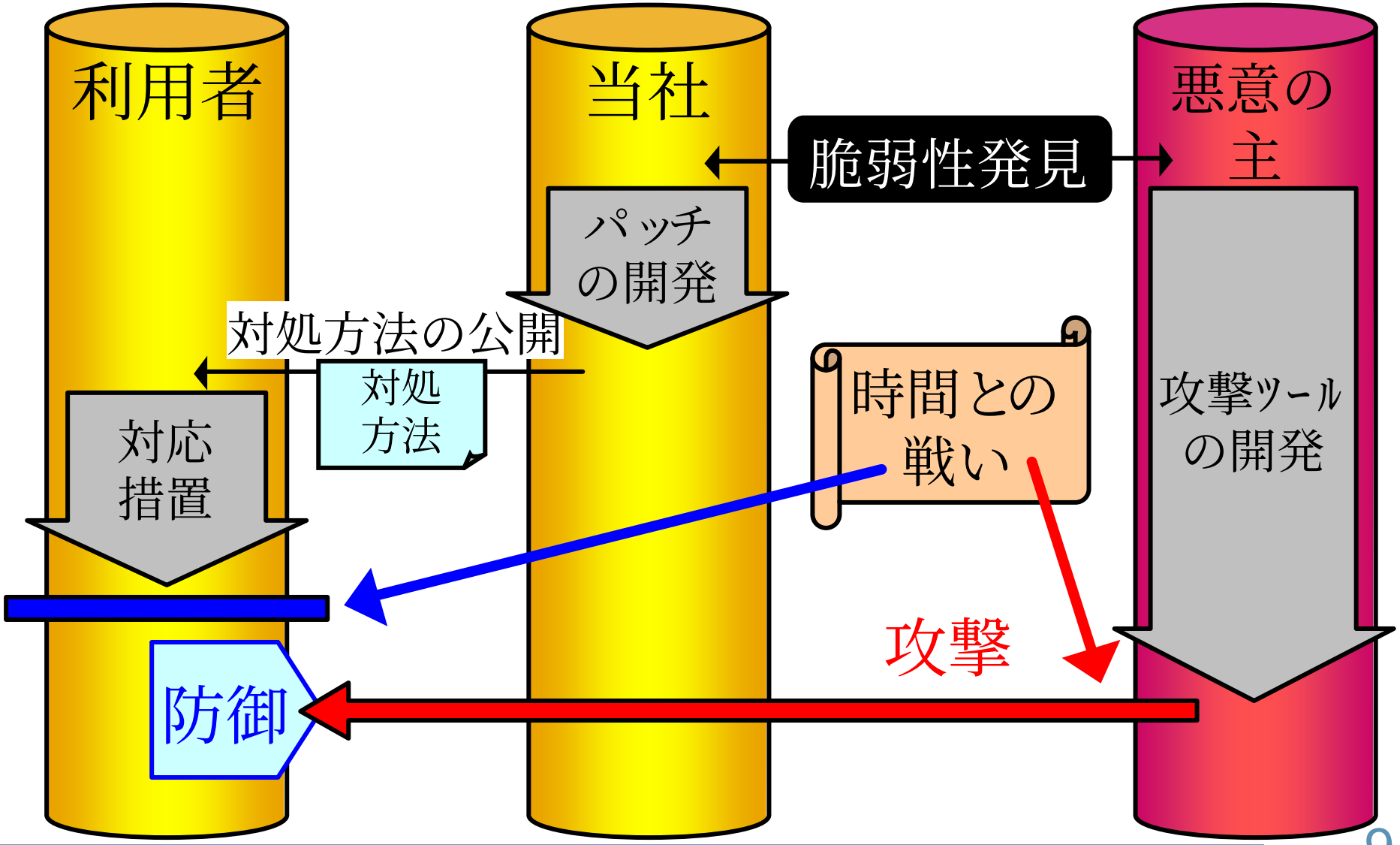
脆弱性情報公開方針

one time one message policy

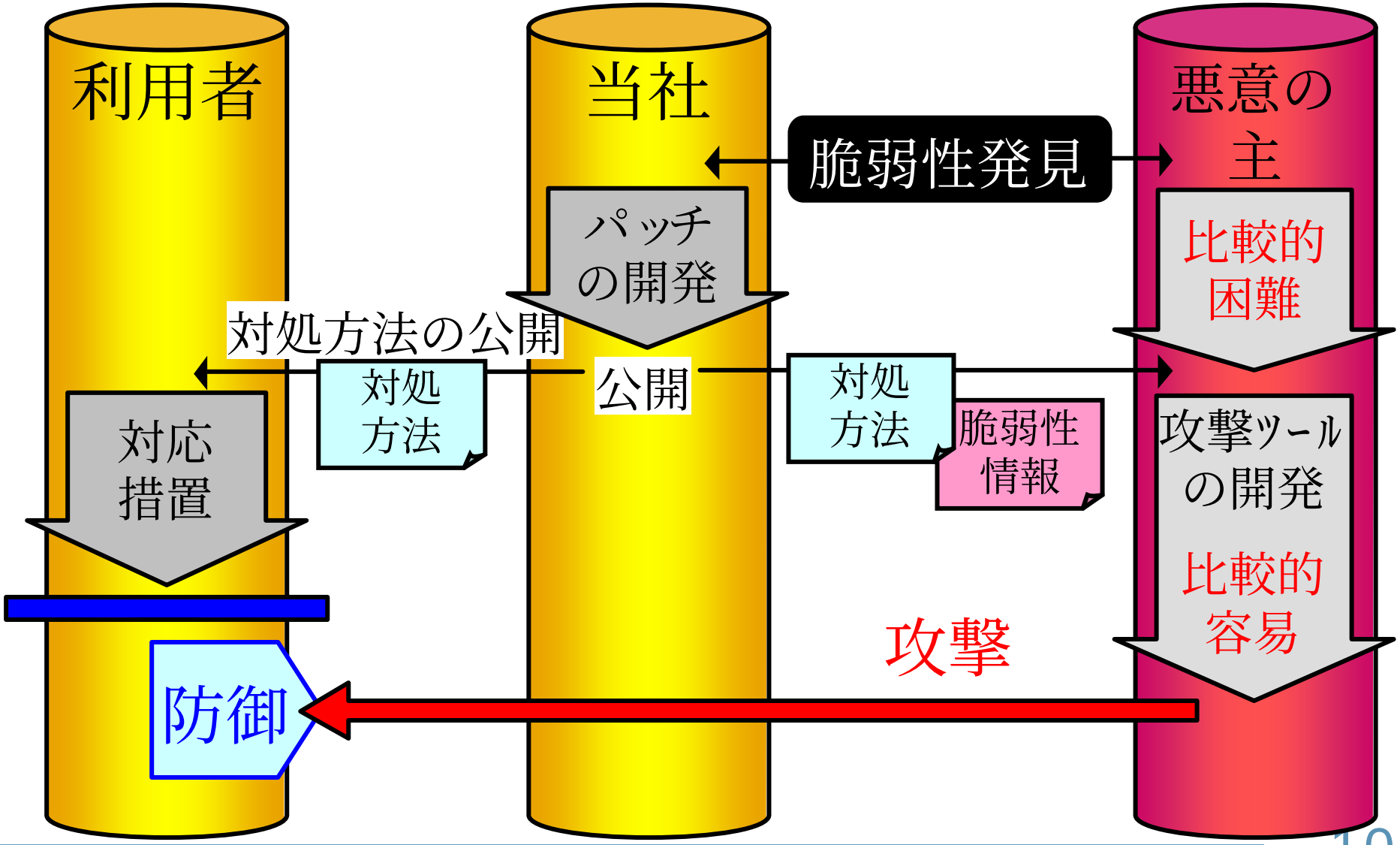
一時に唯一の情報を公開する方針

脆弱性情報については、いかなる優先提供もしない

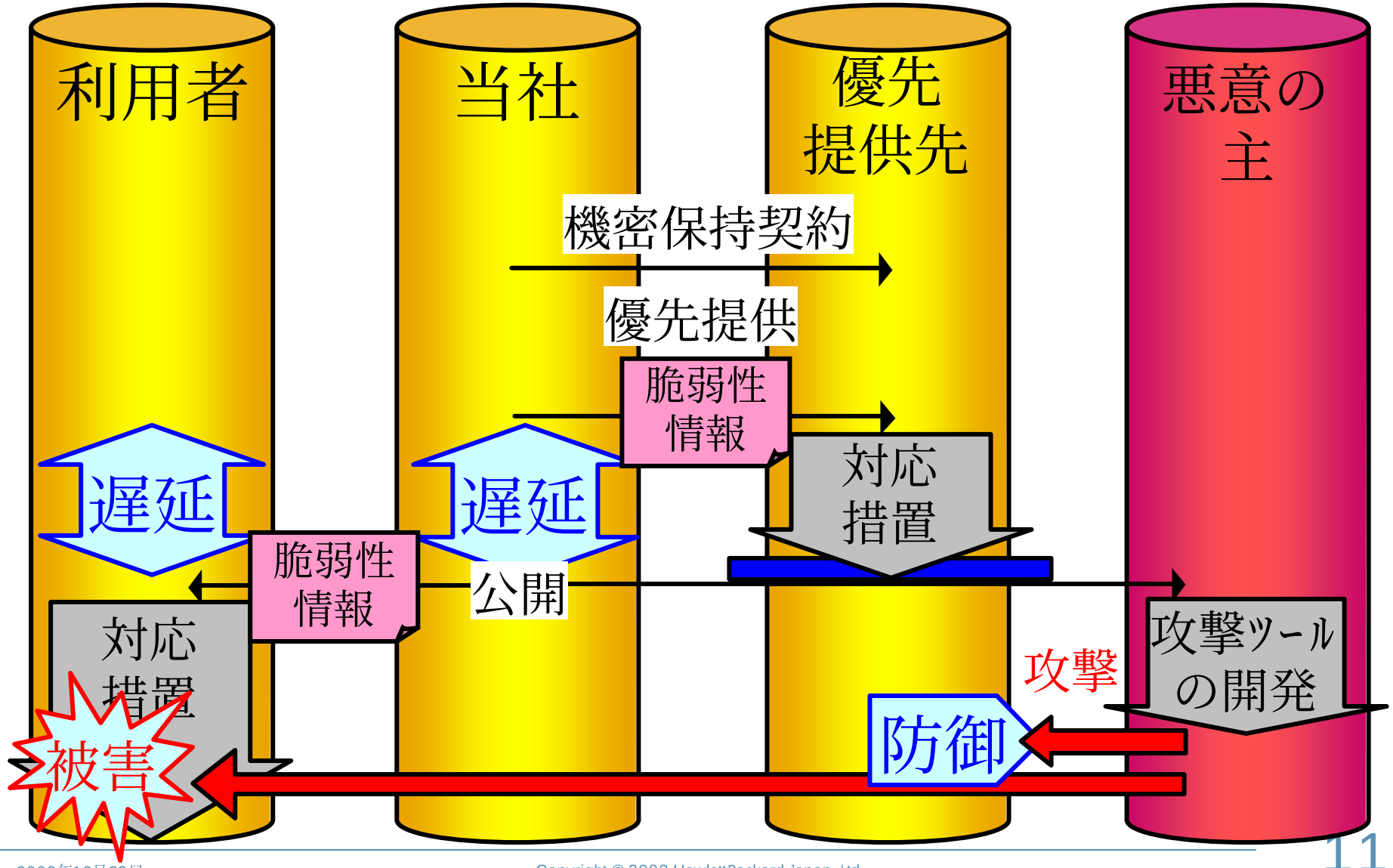
脆弱性情報　と　対策　と　攻撃ツール



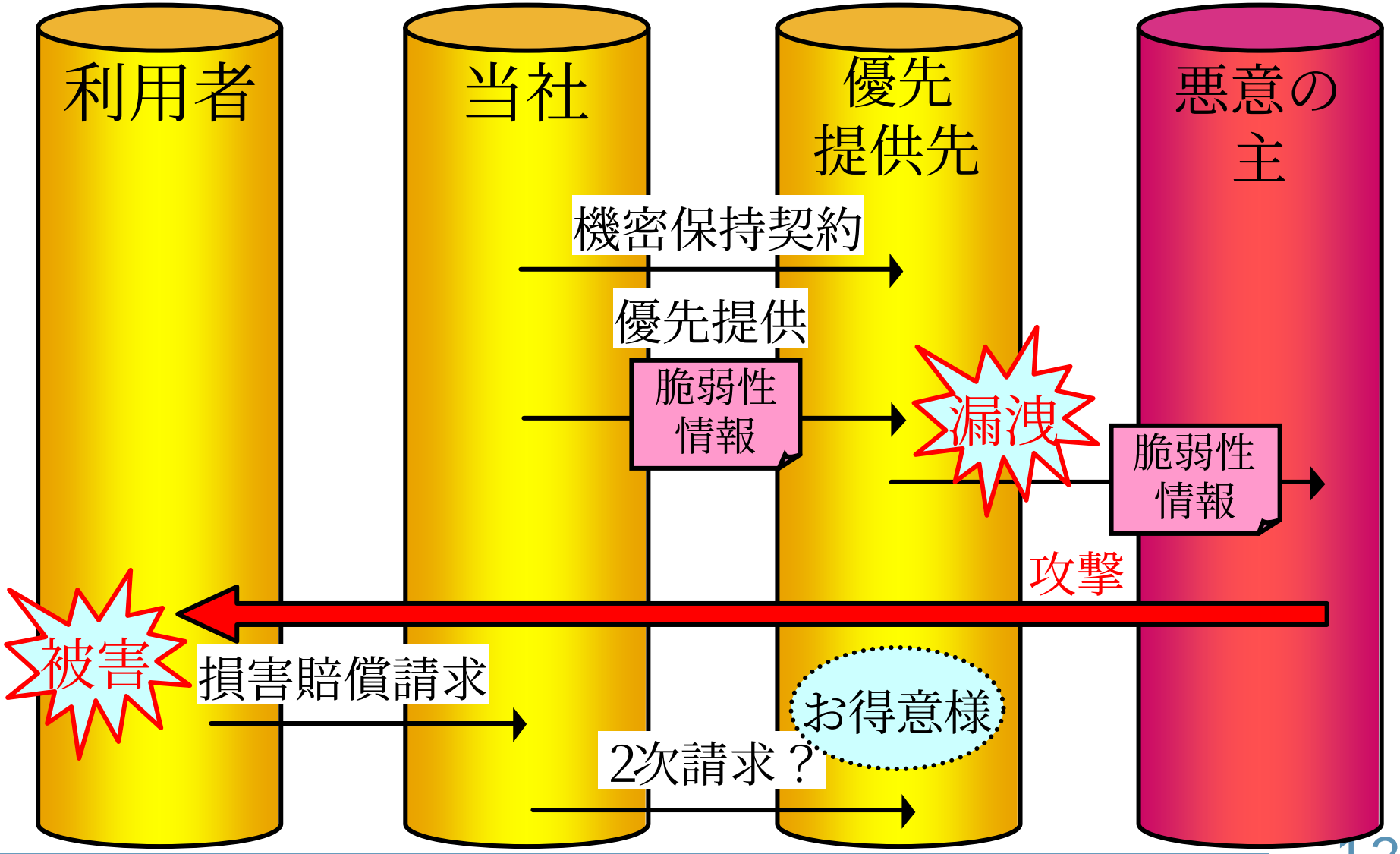
脆弱性情報　と　対策　と　攻撃ツール



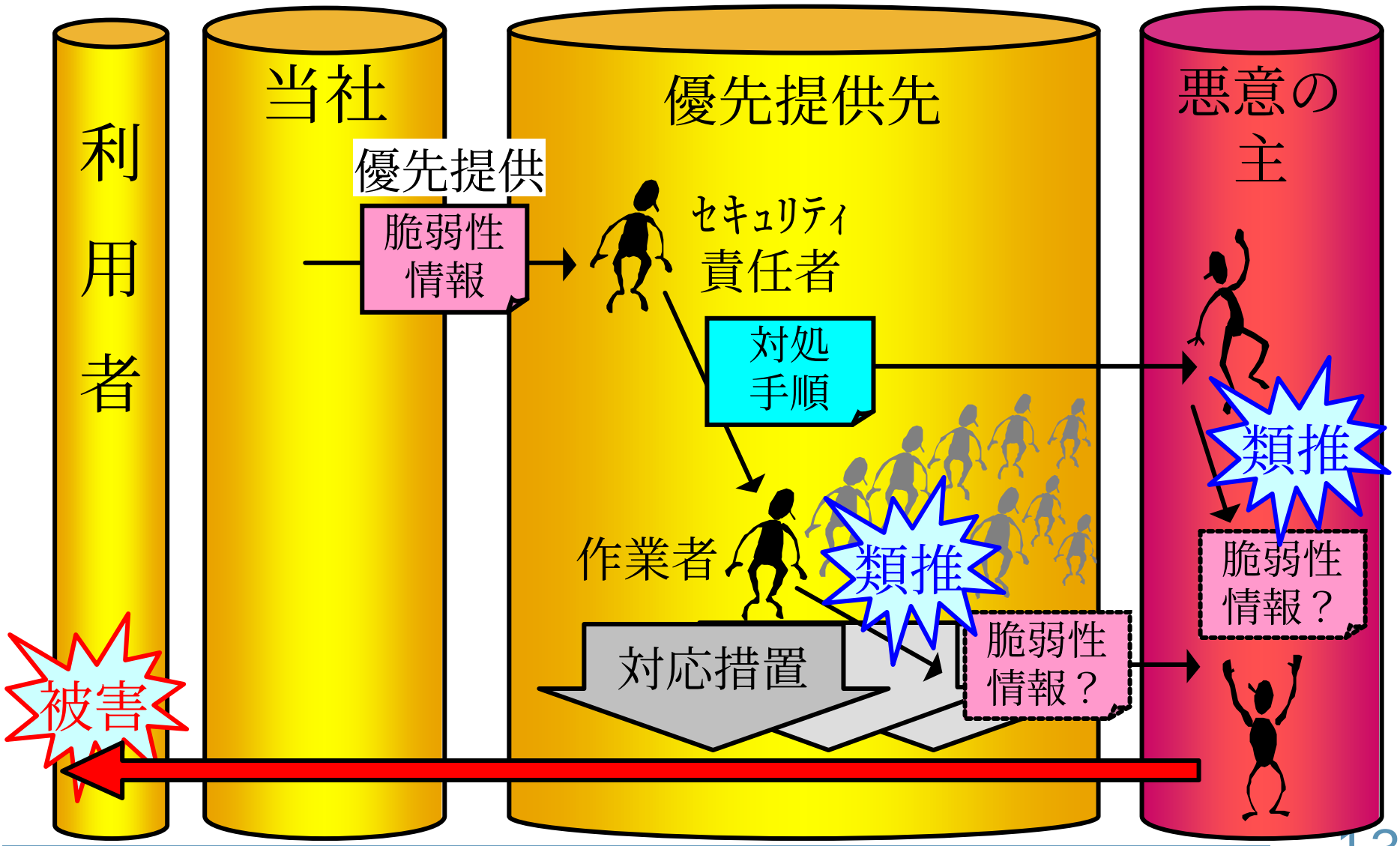
脆弱性情報の優先提供を要望する背景



脆弱性情報の優先提供の 問題点



脆弱性情報の優先提供の 問題点



コンピュータベンダーの責務

脆弱性を生まないような開発品質の向上

脆弱性の情報管理の徹底

対処方法の迅速な確立と提供

one time one message の保証

パッチ提供方針の明確化と確立

セキュリティ・パッチには、それ以外のパッチを混ぜない
セキュリティ対策向上のためでも機能追加を行なわない

お客様へのお願い

対処方法の取得

セキュリティ情報メーリングリストへの登録

http://www.hp.com/jp/security

対処方法への適時の対応

SIRT：Security Incident Response Team

セキュリティ・インシデント対応体制の確立

本日の資料

http://yosihiro.com/business/