OSS利用時のセキュリティ基本のキ

Kazuo Moriwaka
Red Hat K.K. Solution Architect
2016-11-22

このスライドの目的

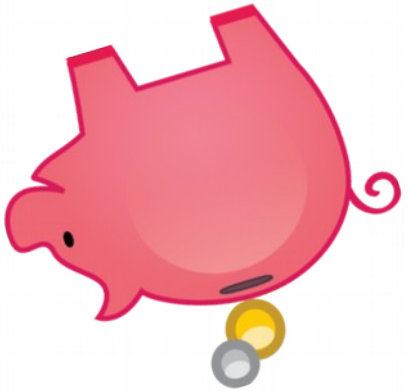
- 対象: OSSを利用するまたは既に利用しているが、セキュリティについてそれほど詳しくない方
- 目的:
  - 基本的なセキュリティ対策である
    「メンテナンスされているソフトウェアを使う」
    「ソフトウェアの更新情報を把握する」
    「既知の問題の修正を反映する」
    「適切な設定を徹底する」
    の必要性を伝え、注意するべきポイントを示す

agenda

- 「セキュリティ上の問題」って何？
- ソフトウェアはメンテナンスが重要
- OSSのセキュリティの基本
  - ソフトウェア選定
  - 更新情報を把握
  - ソフトウェア更新をシステムへ反映
  - 適切な設定を徹底

「セキュリティ上の問題」って何?

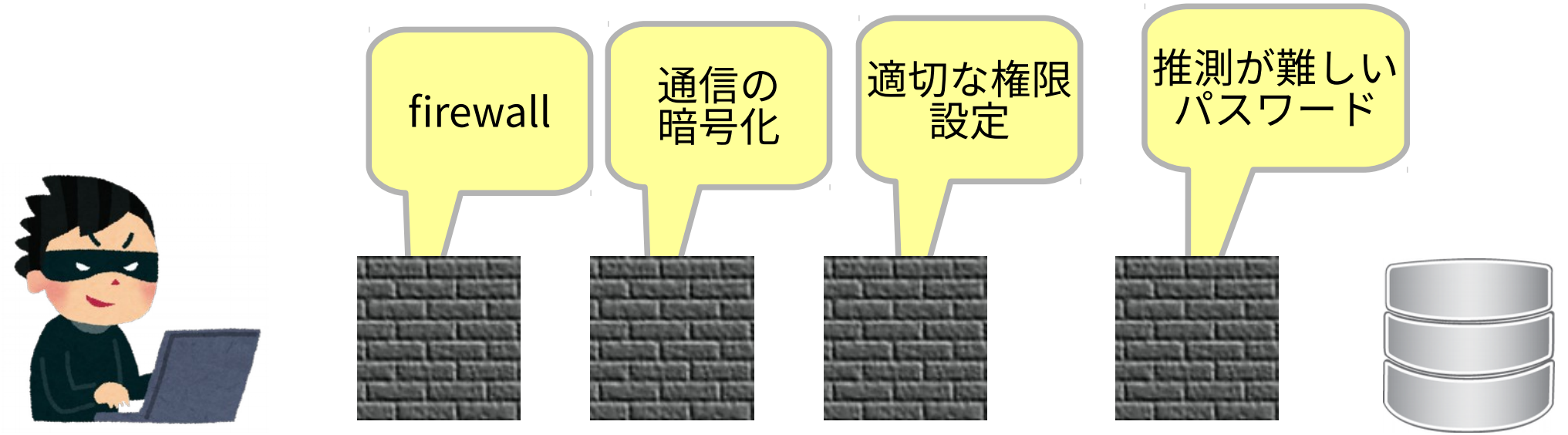
- 「本来できてはいけないことができてしまう」問題全般
  - 見えるべきでない情報が見える
  - 管理権限がないシステムを停止させられる
  - 他ユーザに影響を与える
  - データを破壊できる
  - などなど



- 「ソフトウェアのセキュリティ上の問題」では、ソフトウェアの問題により本来できてはいけないことができてしまう
  - ソフトウェア以外にもハードウェアや運用の問題もセキュリティ上の問題になります
- 被害を受けるだけでなく加害者になってしまう危険性

セキュリティは多層防御

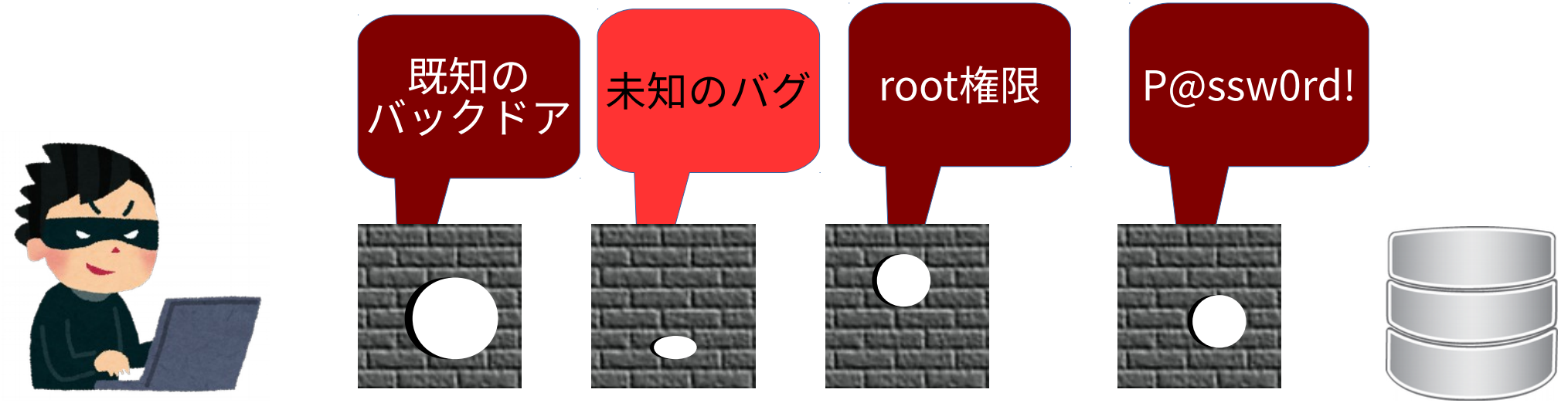
- 既知のもの、未知のもの含め一切問題がないシステムは存在しない
- 様々な緩和策を組みあわせて攻撃を難しくする



既知の問題への対策の重要性

- セキュリティの問題は対策に穴を開けてしまう
- 攻撃者が目標までたどりつくルートを完成させないことが重要

  →未知の問題は存在していて攻撃者は入手できる
  →既知の問題への対策は攻撃の難易度を上げる



ソフトウェアはメンテナンスが命

- ソフトウェアはメンテナンスが非常に大事です
  - 問題の発現・発見
  - 発見した問題を追跡調査
  - 修正
- メンテナンスされないとどうなる?
  - 問題の発現・発見はされ続ける
  - 勝手に直ったりはしません

    → 既知の問題が継続的に増えていきます
    → それを利用した攻撃用プログラムも用意されます
  - どんどん腐っていく「ゾンビ」のようなもの

OSS利用時のセキュリティ

「セキュリティが大事」というときに何を気にする必要があるか?

- ソフトウェア選定
  →メンテナンスされているソフトウェアを選ぶ
- 更新情報を把握
  →ソフトウェア提供元の更新情報を把握する
- ソフトウェア更新をシステムへ反映
  →迅速に各システムを更新する
- 適切な設定を徹底
  →設定上の問題もセキュリティ上の問題になる

ソフトウェア選定

- メンテナンスされないソフトウェアは利用しない
  - 利用期間がサポート期間に含まれることを確認する
  - 場合によっては運用中のバージョン変更を計画に折り込む
- メンテナンスされるものを調達する
  - メンテナンスを提供している企業(Red Hatなど)と契約
    - 「問いあわせ対応」ではなく「修正の開発・提供」ができる企業を選ぶ
  - コミュニティに頼る場合はその状況をチェックする
    - 「最新版」であっても数年放置されているような、コミュニティが機能していないケースもある
    - 場合によってはコミュニティを維持するため自社エンジニアを投入する

更新情報を把握

- ソフトウェア提供元からの更新情報を把握する
- 企業や各コミュニティでの更新情報を確認
- 自分のシステムに影響する更新を把握
  - システムで利用しているソフトウェアとバージョン
  - 各ソフトウェアの修正情報

ソフトウェア更新をシステムへ反映

- 元のソフトウェアが更新されていても自分のシステムに古い版が入っていては意味がない
  - 定期的なソフトウェア更新作業を折り込んだ運用設計が必須
  - 重要なシステムについてはスムーズな更新のためにテスト用環境などを用意する
- 特にセキュリティ問題については迅速な反映が求められます
  - 既知のセキュリティ問題を利用した攻撃ツールが流通する
  - 未知のセキュリティ問題が攻撃者により発見され、攻撃に使われたツールから問題が発見されることも多い

適切な設定を徹底

- 設定上の問題もセキュリティ上の問題になります
  - 適切な設定を徹底することが重要
- 設定ポリシーの策定
  - 誰から何を守るかの目的設定、実現可能性、ポリシーを徹底するための手段
- 設定作業を自動化することで人的ミスを防ぐ
  - 設定を集中管理、変更履歴管理
  - 手順書の解釈違いや抜け漏れなどの人的ミスを予防
- 設定がポリシーに沿っているかを定期的にチェックする
  - 組織のポリシーと設定が整合していることを自動的に確認
  - 抜け漏れの検出、何らかの事故による設定変更の検出

道具を使う

セキュリティを維持してシステム運用するのは大変なので
様々な道具が使われます

- Issue Tracker
  - 多数の問題を並列に処理するため事実上必須
- インベントリ管理
  - 利用ソフトウェアとバージョンの管理
- 脆弱性情報の入手
  - JPCERT/CC: https://www.jpcert.or.jp/
  - USCERT: https://www.kb.cert.org/vuls/
- 設定の徹底
  - Ansible, Puppetなどによる設定の自動化
  - OpenSCAPによる設定チェック

まとめ

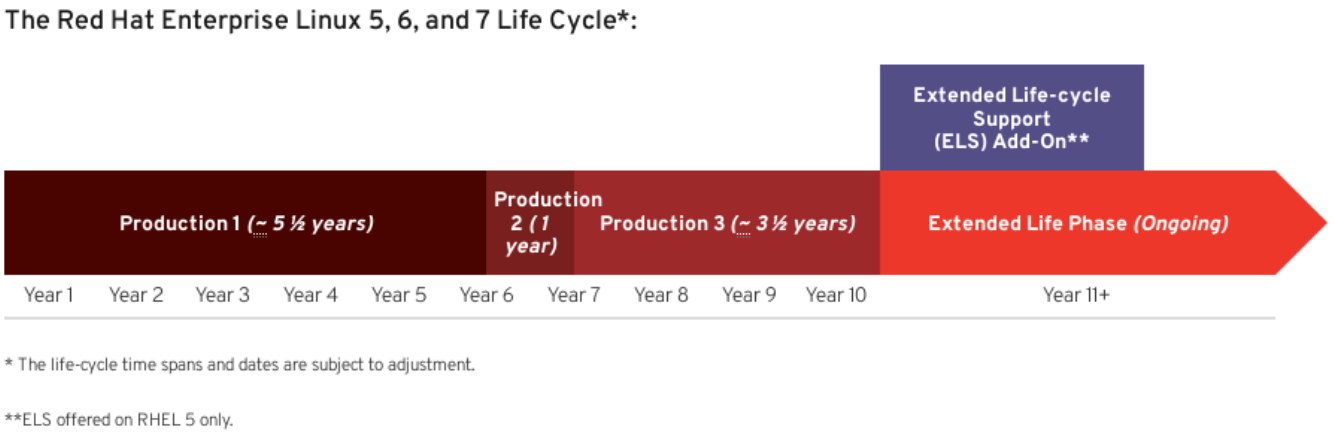
OSSを利用する時の基本的な注意点

- ソフトウェア選定
  →メンテナンスされているソフトウェアを選ぶ
- 更新情報を把握
  →ソフトウェアの更新情報を把握する
- ソフトウェア更新をシステムへ反映
  →迅速に各システムを更新する
- 適切な設定を徹底
  →設定上の問題もセキュリティ上の問題になる

おまけ: Red Hat Enterprise Linuxでのセキュリティ基本のキ

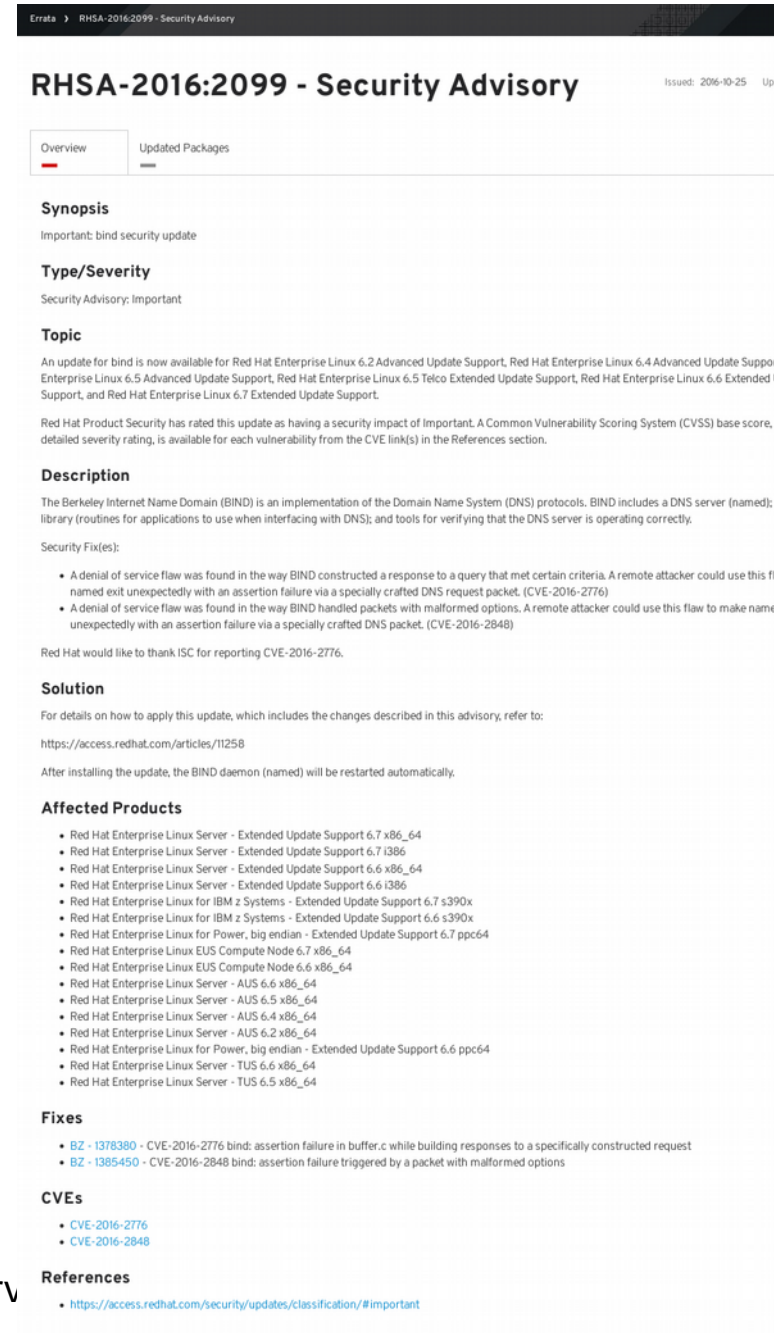
ソフトウェア選定

- 10年間のライフサイクルと更新ポリシーを公開
  - コミュニティでのメンテナンスが終了しても基本的にはサポート期間中はメンテナンスを維持
    - OpenJDKについて例外あり
  - 各ソフトウェアにメンテナンス担当エンジニアやグループを割り当て
  - セキュリティ対策については別途専門のチームも対応



更新情報を把握

- Webでの更新情報公開
- 更新情報の入手
  - 登録したシステムに影響があるものだけをメール通知
  - 製品・脆弱性から検索
  - メーリングリスト、RSSなどでも配信
- システムに適用可能な更新を一覧
  - yum updateinfo
- Red Hat Satelliteで複数台の確認
- 重要な問題についてはRed Hat Insightsのレポートにも表示



Errata › RHSA-2016:2099 - Security Advisory

RHSA-2016:2099 - Security Advisory

Issued: 2016-10-25 Up

Overview | Updated Packages

Synopsis

Important: bind security update

Type/Severity

Security Advisory: Important

Topic

An update for bind is now available for Red Hat Enterprise Linux 6.2 Advanced Update Support, Red Hat Enterprise Linux 6.4 Advanced Update Suppo
Enterprise Linux 6.5 Advanced Update Support, Red Hat Enterprise Linux 6.5 Telco Extended Update Support, Red Hat Enterprise Linux 6.6 Extended
Support, and Red Hat Enterprise Linux 6.7 Extended Update Support.

Red Hat Product Security has rated this update as having a security impact of Important. A Common Vulnerability Scoring System (CVSS) base score,
detailed severity rating, is available for each vulnerability from the CVE link(s) in the References section.

Description

The Berkeley Internet Name Domain (BIND) is an implementation of the Domain Name System (DNS) protocols. BIND includes a DNS server (named);
library (routines for applications to use when interfacing with DNS); and tools for verifying that the DNS server is operating correctly.

Security Fix(es):

- A denial of service flaw was found in the way BIND constructed a response to a query that met certain criteria. A remote attacker could use this fl
named exit unexpectedly with an assertion failure via a specially crafted DNS request packet. (CVE-2016-2776)
- A denial of service flaw was found in the way BIND handled packets with malformed options. A remote attacker could use this flaw to make name
unexpectedly with an assertion failure via a specially crafted DNS packet. (CVE-2016-2848)

Red Hat would like to thank ISC for reporting CVE-2016-2776.

Solution

For details on how to apply this update, which includes the changes described in this advisory, refer to:

https://access.redhat.com/articles/11258

After installing the update, the BIND daemon (named) will be restarted automatically.

Affected Products

- Red Hat Enterprise Linux Server - Extended Update Support 6.7 x86_64
- Red Hat Enterprise Linux Server - Extended Update Support 6.7 i386
- Red Hat Enterprise Linux Server - Extended Update Support 6.6 x86_64
- Red Hat Enterprise Linux Server - Extended Update Support 6.6 i386
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 6.7 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 6.6 s390x
- Red Hat Enterprise Linux for Power, big endian - Extended Update Support 6.7 ppc64
- Red Hat Enterprise Linux EUS Compute Node 6.7 x86_64
- Red Hat Enterprise Linux EUS Compute Node 6.6 x86_64
- Red Hat Enterprise Linux Server - AUS 6.6 x86_64
- Red Hat Enterprise Linux Server - AUS 6.5 x86_64
- Red Hat Enterprise Linux Server - AUS 6.4 x86_64
- Red Hat Enterprise Linux Server - AUS 6.2 x86_64
- Red Hat Enterprise Linux for Power, big endian - Extended Update Support 6.6 ppc64
- Red Hat Enterprise Linux Server - TUS 6.6 x86_64
- Red Hat Enterprise Linux Server - TUS 6.5 x86_64

Fixes

- BZ - 1378380 - CVE-2016-2776 bind: assertion failure in buffer.c while building responses to a specifically constructed request
- BZ - 1385450 - CVE-2016-2848 bind: assertion failure triggered by a packet with malformed options

CVEs

- CVE-2016-2776
- CVE-2016-2848

References

- https://access.redhat.com/security/updates/classification/#important

ソフトウェア更新をシステムへ反映

- yum updateによるアップデート
  - コマンド一回でシステムの全パッケージを更新する
    - 部分的な更新も可能
  - 依存関係管理により組み合わせが破綻することによる障害を予防
- Red Hat Satelliteによるアップデート
  - 多数のRHELを一括して更新
  - テスト環境で実施した更新と同じ更新内容だけを本番環境へ反映するコンテンツ管理機能
  - 電源offなどで通信不可であっても次回接続後に更新を実行して更新漏れを防ぐ

適切な設定を徹底

- 設定の自動化：
  - Red Hat Satellite同梱のPuppetによる設定管理
  - Ansibleでの自動化
- 設定のチェック:
  - SCAP WorkbenchによるSCAPポリシー作成
  - OpenSCAPによる設定のチェック
  - Red Hat Insightsで一般的な設定上の問題を警告