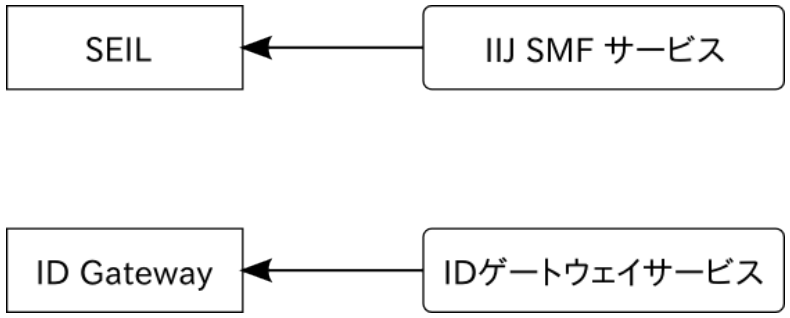
ゲートウェイソフトウェアの現状と今後

プロダクト本部 戦略的開発部
保岡 昌彦
yasuoka@iij.ad.jp

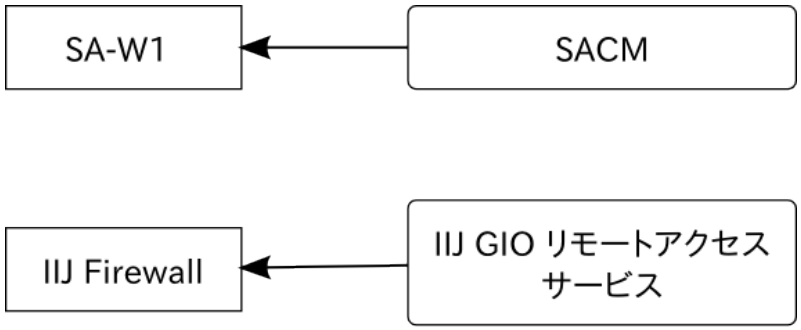
旧世代 (1998～)

- SEIL
  - IIJ SMF
  - NetBSD ベース
- ID Gateway
  - IDゲートウェイサービス
  - NetBSD ベース



新世代 (2012～)

- SA-W1
  - SACM
  - NetBSD 6 ベース
- IIJ Firewall
  - IIJ GIO リモートアクセス
  - OpenBSD ベース

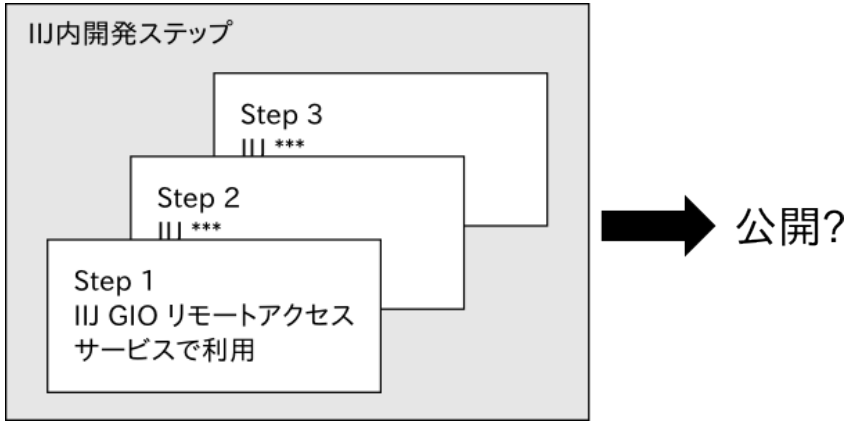


「統合ゲートウェイ」=「IIJ Firewall」

- IIJ内通称「統合ゲートウェイ」
  - その名のとおり、IIJ のサービスで用いられるゲートウェイを統合するものを目指している
  - 2013年春から、「IIJ GIO リモートアクセスサービス」で利用されている
- 「IIJ Firewall」
  - 開発段階
  - 今後の予定ははっきりとは決まっていないが、「IIJ Firewall」と呼んで開発を進めている

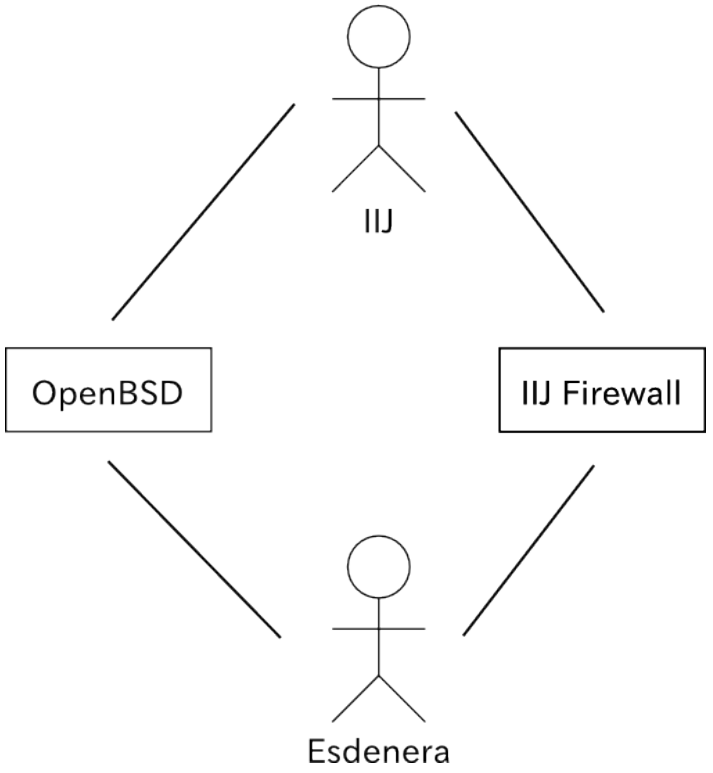
開発の現状と今後のプラン

- 当面、IIJ のサービスの裏側を支えるソフトウェアとして開発
- 現在
  - IIJ Firewall 1.0 をリリースし、Step 1 を消化
  - IIJ Firewall 2.0、Step 2 にむけ開発中
- その後は、一般公開など含め検討中



開発の体制

- Esdenera Networks GmbH (http://esdenera.com/) と IIJ が協力して開発



なぜ自社開発?

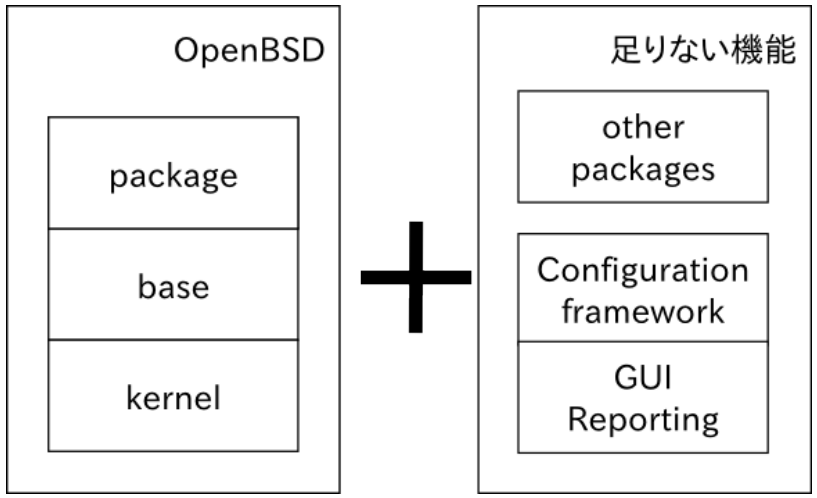
- ファイアウォールのコモディティ化
  - 一般的なファイアウォール製品の機能のおおよそは、オープンソースベースのソフトウェアで実現可能
- セキュリティ
  - ネットワークにとって基礎的で超重要な部分
  - 海外の「ブラックボックス」製品を使う?
  - オープンソース製品ならば「クリスタルボックス」

OpenBSD ベースで自社開発(1/4)

- ネットワークの機能がそろっている
  - Firewall
    - L2-L3 Firewall, Application Level Gateway, QoS
  - VPN
    - IPsec/IKEv1, IKEv2, L2TP/IPsec, PPTP, SSTP
  - L2/L3 Tunneling
    - IPIP, GRE, etherip, VXLAN, NVGRE
  - Virtualization
    - VMware (vmt, vmxnet2, vmxnet3, pvscsi)、KVM(virtio)
  - rdomain(vrf), carp, snmp, ospf, bgp, mpls

OpenBSD ベースで自社開発(2/4)

- 足りない機能を足す
  - OpenBSD に還元できるものは、なるべく還元
  - package の枠組みで足す
  - 設定やレポート系、CLI, web api, GUI を足す



OpenBSD ベースで自社開発(3/4)

- OpenBSD コミュニティ
  - OpenBSD をネットワークゲートウェイとして運用する人が多数
    - メーリングリストを通じてノウハウを共有
  - ネットワーク関連のデベロッパ多数
    - pf, OpenBGPD, relayd, iked,…
    - ハッカソンを通じて、技術情報を議論、交換

OpenBSD ベースで自社開発(4/4)

- なぜ、OpenBSD?
  - 文化
    - セキュリティ、安定性を重視
    - 実践を重んじる
  - リリースエンジニアリング
    - 6 か月ごとのリリース
    - 単純で明確な ABI 変更ポリシー
      - とくに Package subsystem にとって重要

Configuration Framework の実装 (1/3)

- 素の OpenBSD や Linux では、個々の機能をそれぞれ設定していく
  - vi /etc/pf.conf
- ネットワーク機器は統合された設定インタフェースを通じて設定していく
  - filter add INTERNET action pass src 0.0.0.0/0 …

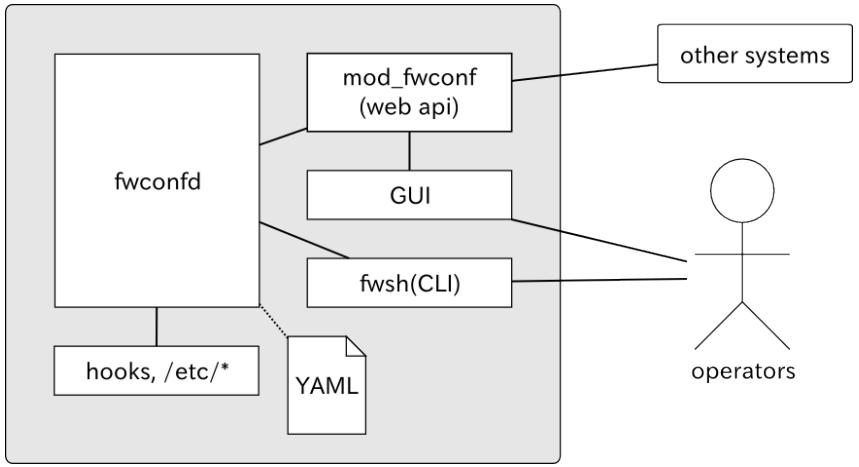
→ IIJ Firewall にも、統合された「設定インタフェース」が求められる

Configuration Framework の実装 (2/3)

- 設定インタフェース化は、いっぽうで柔軟性を失うことにつながる
  - 個々の機能としては実装済だけど、設定インタフェースがないので設定できない
  - 使いたい機能はどんどん設定化したいのに
- 機能をアドオンしても設定はアドオンできない?

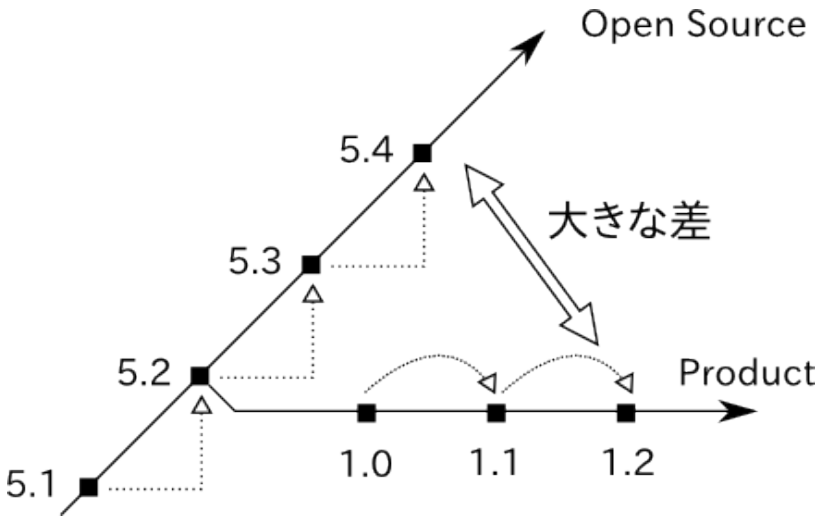
Configuration Framework の実装 (3/3)

- CLI、RESTful web api
  - GUI も開発中
- 設定スキーマは YAML 文書
  - ランタイムに拡張可能
    - package からもスキーマを足せる
    - 設定更新時のフックをアドオン



オープンソースベース製品にありがちな失敗: 陳腐化

- ベース OS との乖離
  - Open Source 側の変更を取り込めない
  - Open Source 側に変更をフィードバックできない
  - IIJ しか興味のない機能 (一般化不足)



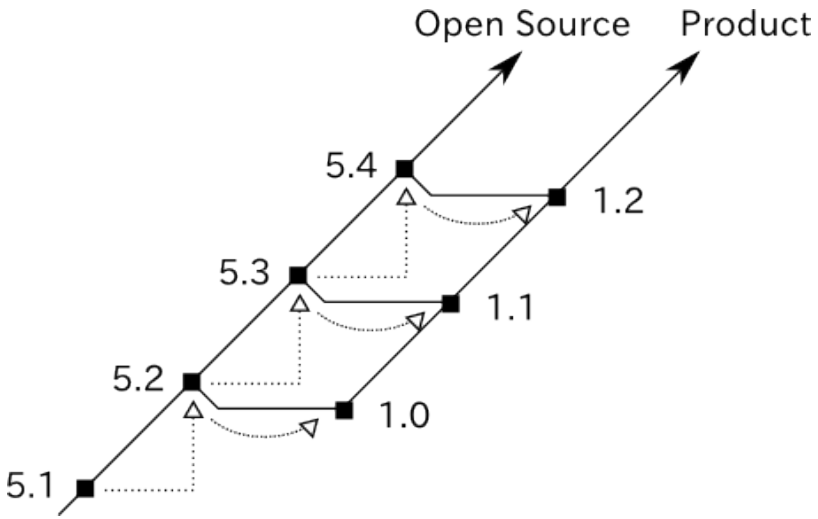
→ 陳腐化

→ 維持コストの増加

IIJ Firewall での取り組み: 陳腐化防止 (1/2)

- バージョンを同期
- ABI も一致

→ IIJ Firewall 1.2 (amd64) 上で、OpenBSD/amd64 5.4 バイナリが動く、ということ



- ABI 変更が必要な Product 固有の拡張はどうする?

IIJ Firewall での取り組み: 陳腐化防止 (2/2)

- 日々最新 (-current) 版とマージ
  - Gitを活用
  - OpenBSD VCS から自動で取り込む
  - 不必要な差を作らない
- リリースは最新から
  - 陳腐化こそ最大の敵
- 開発コミュニティへの積極的な参加
  - どんどんシェアする
- OSS と企業文化のミスマッチ

保守、検証用ツールと環境の整備

- 重大な問題が発生した場合に、どのように対応検証していくか

→道具は常に整備しておく

- ソースコードから再現可能なビルド
  - cvs, git, make
- ソースコードレベルでのデバッグ
  - gdb, cc –g, panic, core, ddb

→その他の取り組み

- panic からの shutdown, vmss2core

まとめ

- IIJ は、次世代ゲートウェイソフトウェアとして「IIJ Firewall」を開発している
- IIJ Firewall は OpenBSD に設定フレームワークなどの機能を足したもの
- 開発方針は、保守性、持続性に重点をおいている

最後に

- iij.news でも取り上げる予定
- ご意見などは、yasuoka at iij.ad.jp までお気軽に