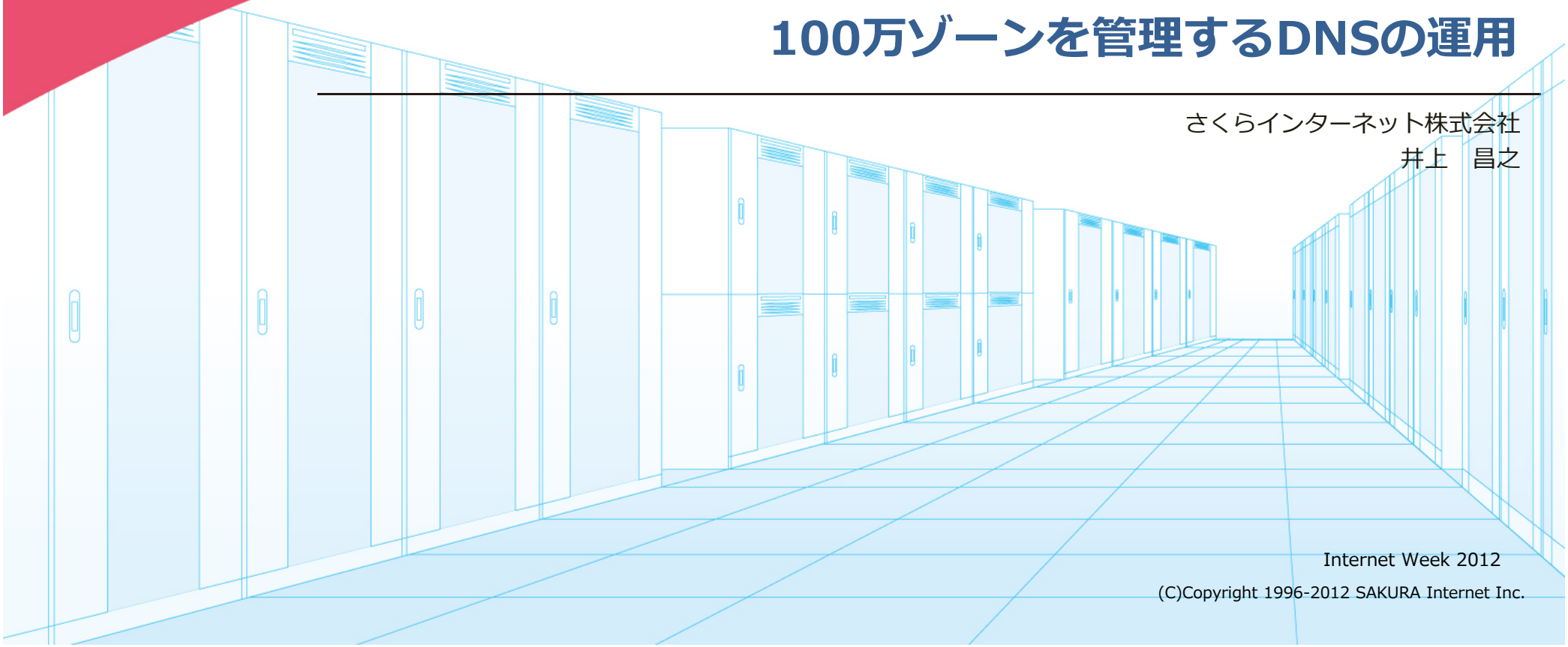
SAKURA Internet

www.sakura.ad.jp

100万ゾーンを管理するDNSの運用

さくらインターネット株式会社
井上　昌之



Internet Week 2012

目次

Nominum ANSの紹介

SAKURA Internet

- 権威サーバのために作られたサーバ
  - サーバ当たり**10億リソース記録可能**
  - レイテンシーはミリ秒で、50,000 QPS以上をベンチマークで記録
    - 100,000 QPS以上まで拡張可能と既に証明済み
  - １秒あたり5,000 DDNS 以上アップデート可能
- **常時オン**のサービス
  - 稼働中の構成/ゾーンデータアップデート(リスタート不要)
  - マルチマスター構成 (デュアルアクティブマスターでDNSアップデートをミラーリング)
- 業界をリードするDNSセキュリティ機能
  - **自動DNSSECライフサイクル管理**
  - GSS-TSIGの付いたマイクロソフトADインテグレーション
- ネットワークの可視化とイベントの認識性
  - DNSクエリーの詳細分析データ
  - スレッショルドベースの警告機能(SNMP, Syslog)
- 使い方は簡単
  - C, Java, Perl, Python, SOAP/XML管理APIs
  - ゾーン構成テンプレート
  - **ゾーンバージョン管理**、ロールバックおよびdiffs

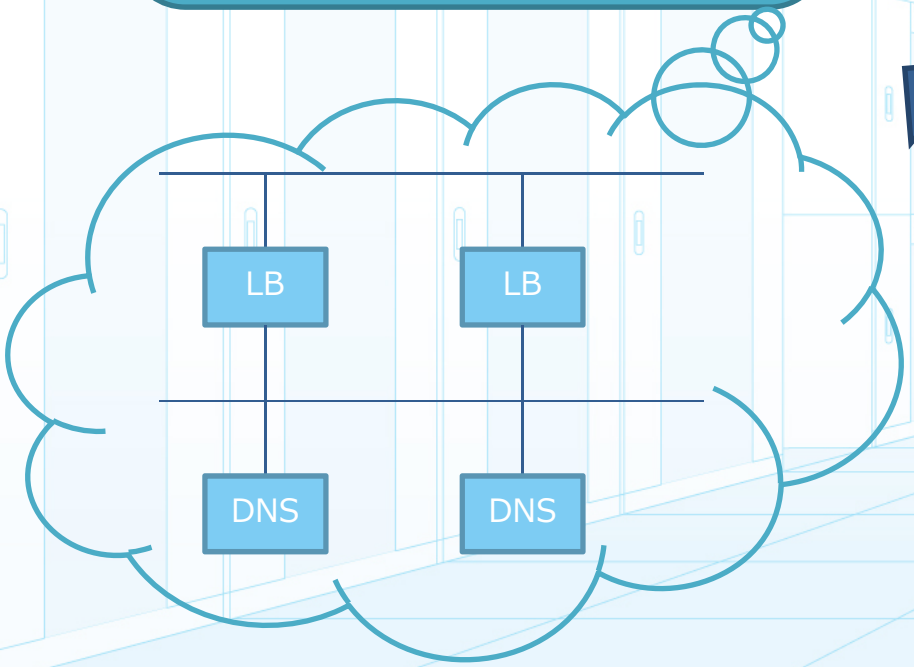
～ANSの概要より～

SAKURA Internet

- 当社DNSコンテンツサーバ環境の構成

スレーブ（ns1.dns.ne.jp）
・東京に設置(AS9370)
・外からのクエリに応答

スレーブ（ns2.dns.ne.jp）
・大阪に設置(AS9371)
・外からのクエリに応答



ゾーン転送

マスター
・ゾーン情報の管理

BINDで起きた問題

SAKURA Internet

- メモリの消費量が多い
  - 全てのゾーン情報をメモリ上に読み込む
  - ゾーン数は増え続け、限界が見え始める
    - 2007年頃、約40万ゾーンで1.8GByte...
- 動作が不安定
  - プロセスのダウンが頻発
  - 起動に120分～180分

BINDで起きた問題

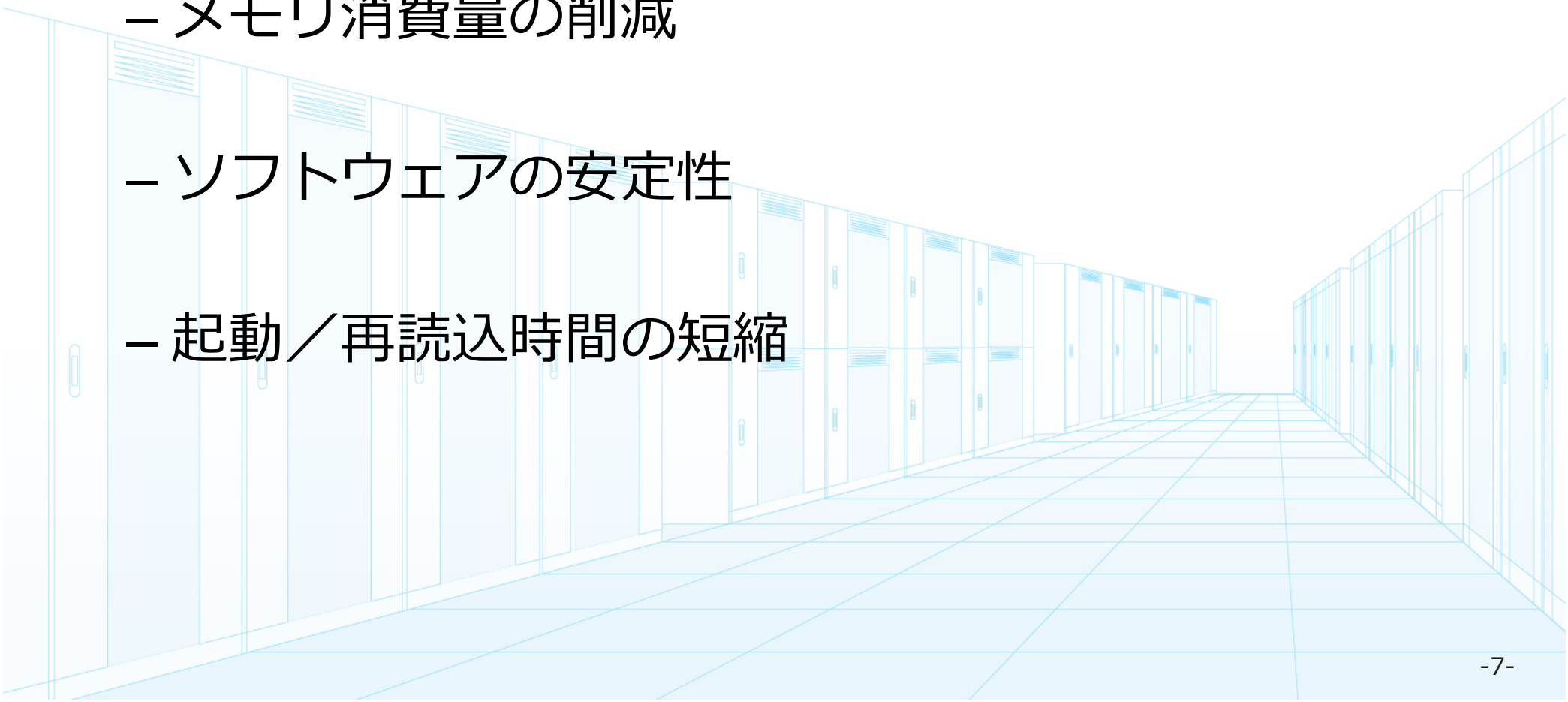
SAKURA Internet

- ゾーンの再読込時に応答がない
  - ゾーン数の増加と共に再読込(reconfig)の時間が増加
  - DNSのヘルスチェックでも失敗が目立つように

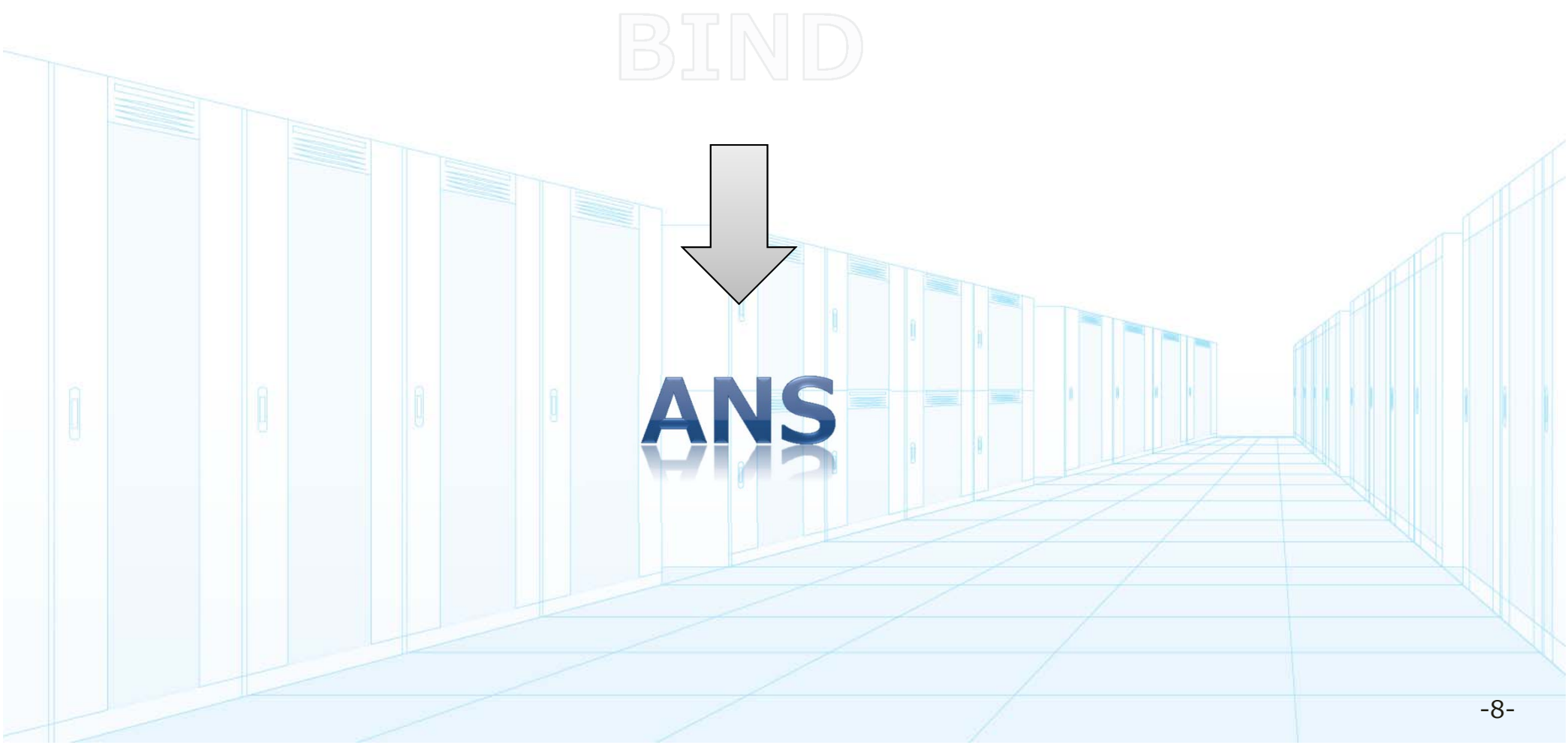
BINDで起きた問題

SAKURA Internet

- 課題
  - メモリ消費量の削減
  - ソフトウェアの安定性
  - 起動／再読込時間の短縮



Nominum ANSへ移行後



Nominum ANSへ移行後

SAKURA Internet

- メモリ使用量の削減
  - 約40万ゾーンで1.8Gから600M
  - 約100万ゾーン（現在の値）でも1.3G程度
- ソフトウェアの安定性
  - 約5年間ダウンなし
- 起動／再読込時間の短縮
  - 起動時間が最大180分から1分以内
  - ゾーン追加は一瞬

今後の課題

SAKURA Internet

- DBによるゾーン管理（BIND-DLZ等）
  - ウェブサービスとの親和性
  - リアルタイム更新
  - トラフィック性能が問題
- Nominum ANS以外の選択肢が欲しい
  - 全ての課題を解決できるものがない
  - ANS が使えなくなった場合は・・・

まとめ

- Nominum ANS導入の効果
  - 大量のゾーン管理
  - DNSサービスの安定提供
  - ゾーン情報の即時反映
- Nominum ANSの利用ケース
  - 大規模なDNSサービスの運用
    - 大量のゾーン管理
    - 応答性能が求められる環境