

## SINA・導入事例



# German Federal Office,

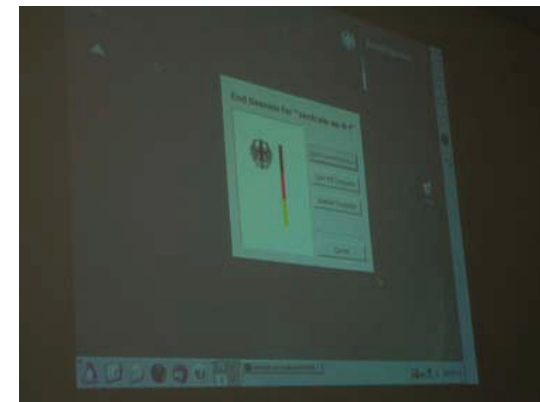




ドイツ外務省のデータセンター



外務省CIOを交えて懇談会



外務省専用端末の立ち上がり画面／SINA



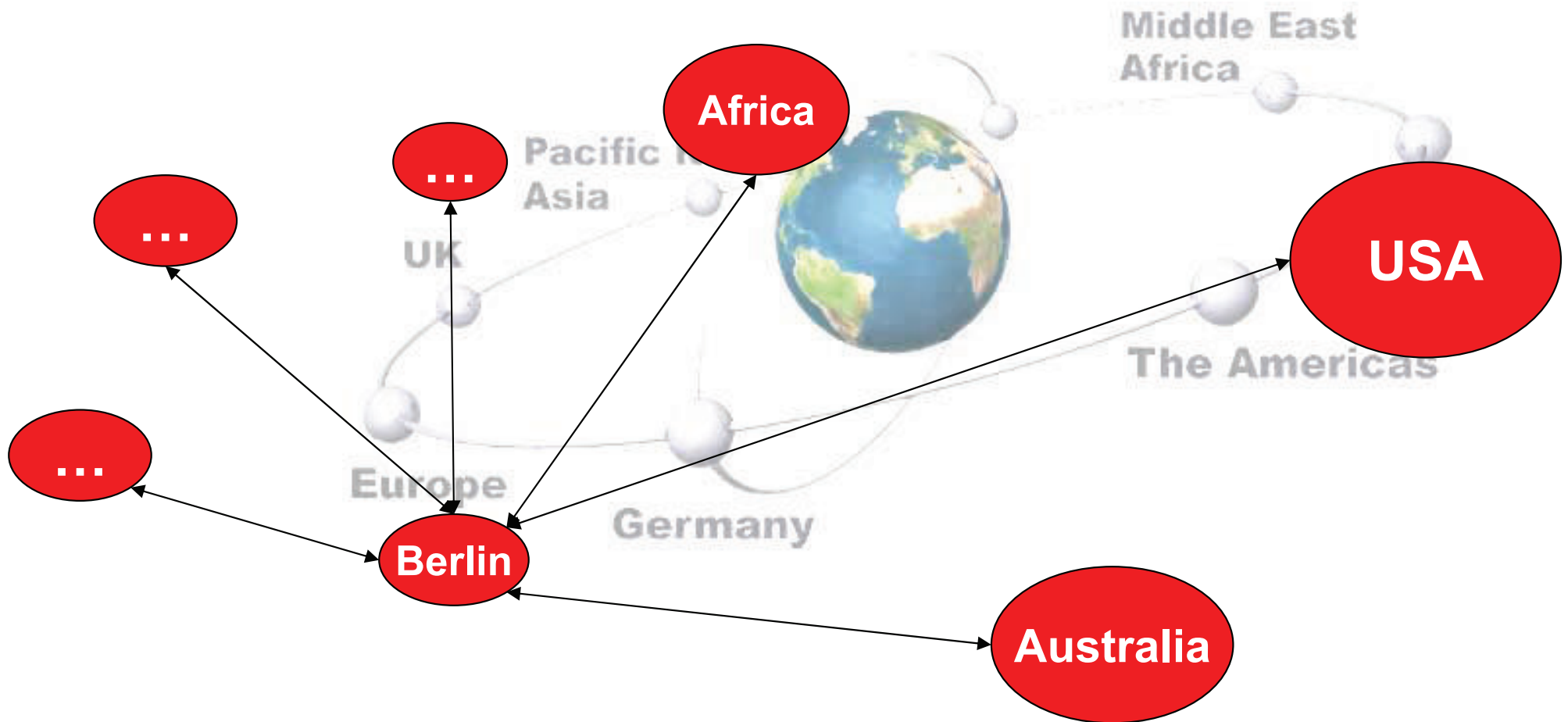
# **Securing Germany in the World With Open Source and SINA**

**Rolf Theodor Schuster**  
**CIO**  
**German Federal Foreign Office, Berlin**



## 【世界規模でのネットワーク基盤を構築】

- 世界220ヶ所以上のドイツ大使館、領事館で利用
- ベルリンに本部、ボンに複数組織を設置





## 2001年時点では:

本部と各国大使館において最低限のネットワークしか存在しなかった

プロトコル X.25、ISDN、アナログ・ライン、インマルサットを利用

統合されたネットワークになっていない

基本的に費用の掛かる構造: 使用量や距離の問題

莫大な通信費用が掛かっていた

クローズド・ソース・セキュリティ・コンポーネントだった





## 掲げた目標:

全世界で使える、安全なネットワークシステムの構築

10,000人を越えるスタッフの利用が可能なシステム

難しいネットワーク構築を含む世界220ヶ所での利用可能なシステム

2003年末までの構築が必須

## 予算の制限:

**費用対効果を重視!**



## 目標となる機能:

全てのスタッフにより良い機能を提供

全ての大使館でメール利用可能

全てのスタッフがメールの利用可能

インターネットを利用した安全性の高い情報をスタッフに提供

安全性と要求の有効性を重視

## さらなる目標:

システムの拡張性

複雑さを最小限に抑える

効率的なオペレーション、ネットワークの監視、管理の実現

安全なリモートアクセスと管理





## ソリューション:

オープンスタンダード、オープンソースシステムの利用

OpenLDAP、PostgreSQL、Apache、Cyrus、Exim、Samba、SSH などの利用

管理ツール: Webmin (webベースのUnixのシステム管理ツール) の利用

LinuxベースのVPN技術である、SINA™を採用

## SINAによる安全性の確保:

SINAは全ての要求を満たしていた

評価の結果、オープンソースを基本とした高い安全性のあるプラットフォームであることが実証された

システム構築、インストール、メンテナンスが容易

モバイルユーザーも安全性の高いネットワーク利用が可能

更なる安全性強化対応でも費用対効果が高い

異なるコンポーネント → 複雑なセキュリティの構築が可能

## なぜSINAを選択したのか？

国内外での高い安全性が証明されている

オープンソースを基本としているので、政府によるシステム監査が可能

ライセンスモデル → コンポーネント毎の価格設定となっており、  
接続クライアント数毎の価格設定ではない

「低」から「高」までセキュリティ環境設定が可能  
→ ニーズに合わせたレベル設定が可能

## 結果:

Secunet社の協力から2年が経過し

- SINAの技術を使い、220ヶ所全てがオンラインで稼働中
- 膨大な通信費用の削減に成功 (通信コスト10億円の削減と20%の人員削減)
- スタッフがオフィス環境の中で機能性の拡張に成功

Secunet社は全てのプロジェクトの重要な局面において優秀なパートナーである  
(ITセキュリティ、オープンソースプラットフォームへの移行、コンセプト、人員 などなど)



# SINA Virtual Workstation

