

広域インシデント情報共有 および分析技術の開発

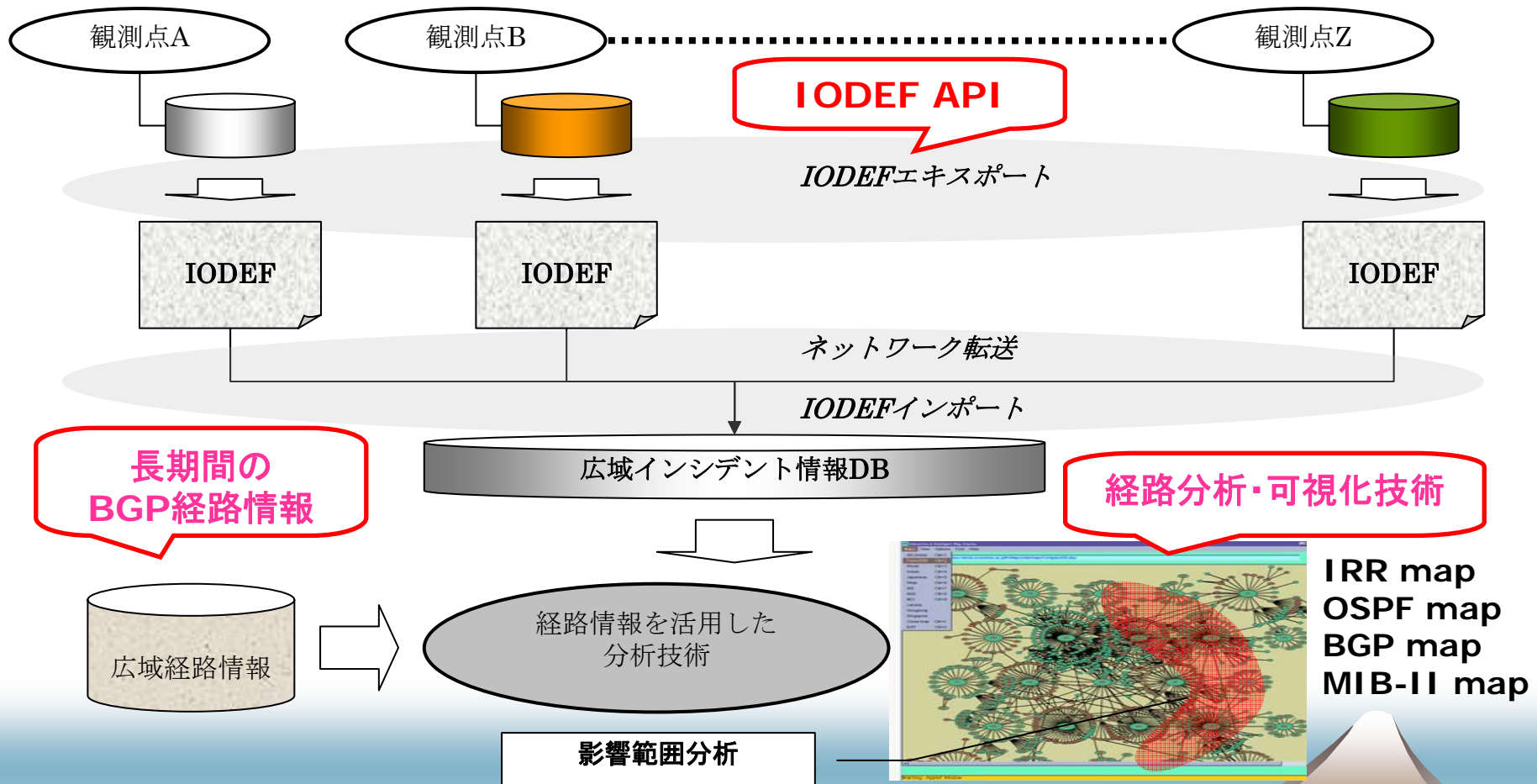
Glenn Mansfield Keeni

January 2006



広域インシデントの分析技術

IPA-IODEF project(2005)



Target Applications

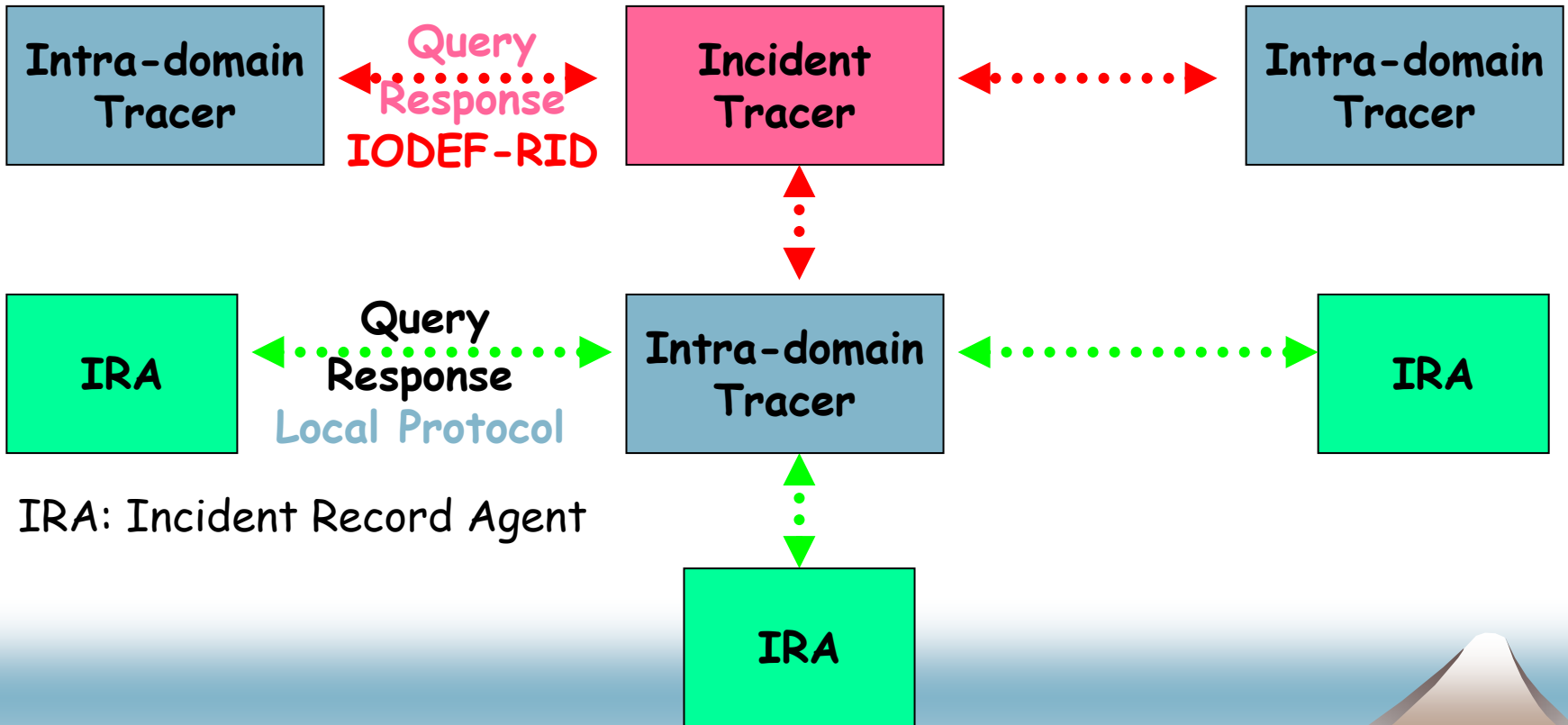
◆ 情報交換プラットフォーム提供

◆ 定点観測

- illegal packets/transactions
- Understand (Illegal) traffic dynamics
(*What ? Where? When?*)
- Understand attack mechanisms/patterns
 - (*How? Intent?*)

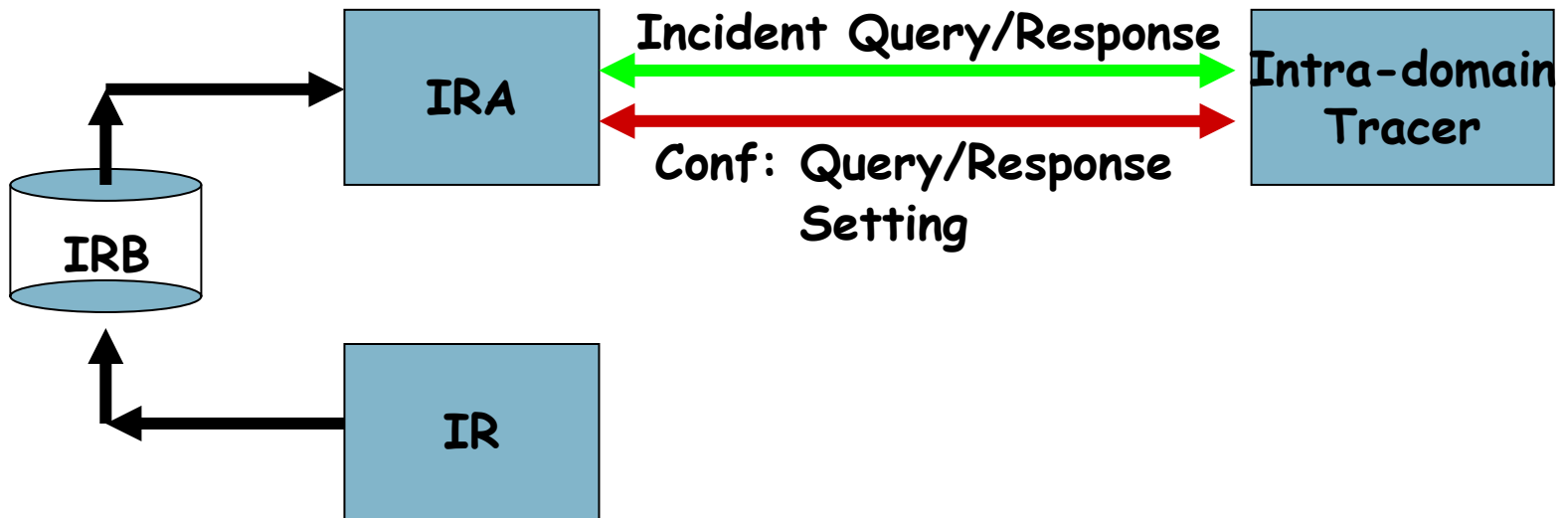
◆ 広域追跡

The two-tier Architecture



IRA: Incident Record Agent

The Intra-domain Architecture



IODEF-API

- ◆ **IODEFメッセージ作成 (IODEF message generation/manipulation)**
 - `com.cysols.iodef.element`パッケージの要素を構築し、IODEF in XMLを生成するためのAPIセット
- ◆ **IODEFメッセージ通知 (IODEF message sender)**
 - `com.cysols.iodef.transport`パッケージにてIODEF XMLファイル送信(含むE-mail)のための抽象クラスを提供する。この抽象クラスを利用して個別の送信方法を用いた実装クラスを作成可能とする。
- ◆ **IODEFメッセージ受信 (IODEF message receiver)**
 - `com.cysols.iodef.transport`パッケージにてIODEF XMLファイル受信および受信後の保存のための抽象クラスを提供する。この抽象クラスを利用して個別の受信方法を用いた実装クラスを作成可能とする。
- ◆ **IODEFインポート(Validation, export to XML file/XML DB)**
 - `com.cysols.iodef`パッケージにてXMLファイルのWriterインターフェース, およびIODEFメッセージのWriterインターフェースが提供される。また各Writerの実装クラスとしてIODEF XMLファイルのWriterクラス, XML DB(Apache Xindexに対応)のWriterクラスが提供される。
- ◆ **IODEFエクスポート(import from XML file/XML DB)**
 - `com.cysols.iodef`パッケージにてXMLファイルのReaderインターフェース, およびIODEFメッセージのReaderクラスが提供される。また各Readerの実装クラスとしてIODEF XMLファイルのReaderクラス, XML DB(Apache Xindexに対応)のReaderクラスが提供される。
- ◆ **RIDクエリメッセージ作成 (IODEF-RID query)**
 - `com.cysols.iodef.rid`パッケージにてRIDクエリの作成, 実行, 結果処理のためのインターフェースが提供される。
- ◆ **RIDレスポンスメッセージ作成 (IODEF-RID response)**
 - `com.cysols.iodef.rid.element`以下にあるRIDエレメントによってクエリと同様に応答メッセージを構築する。

Summary and future

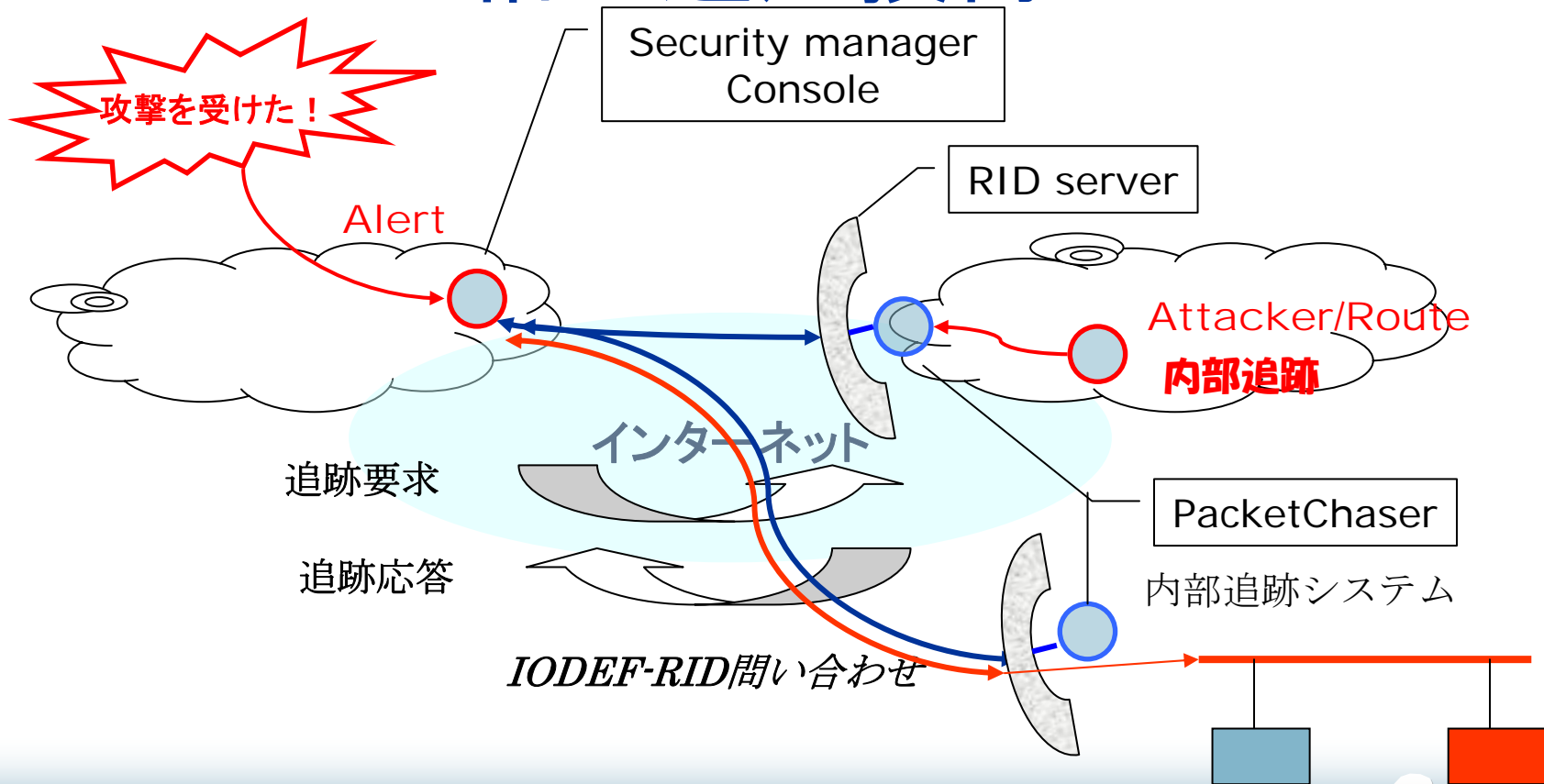
◆ 本開発

- 汎用的基盤となるIODEF-API → Done
- 広域インシデント情報の収集 → Done
- 複数組織にまたがる広域協調追跡 → Done

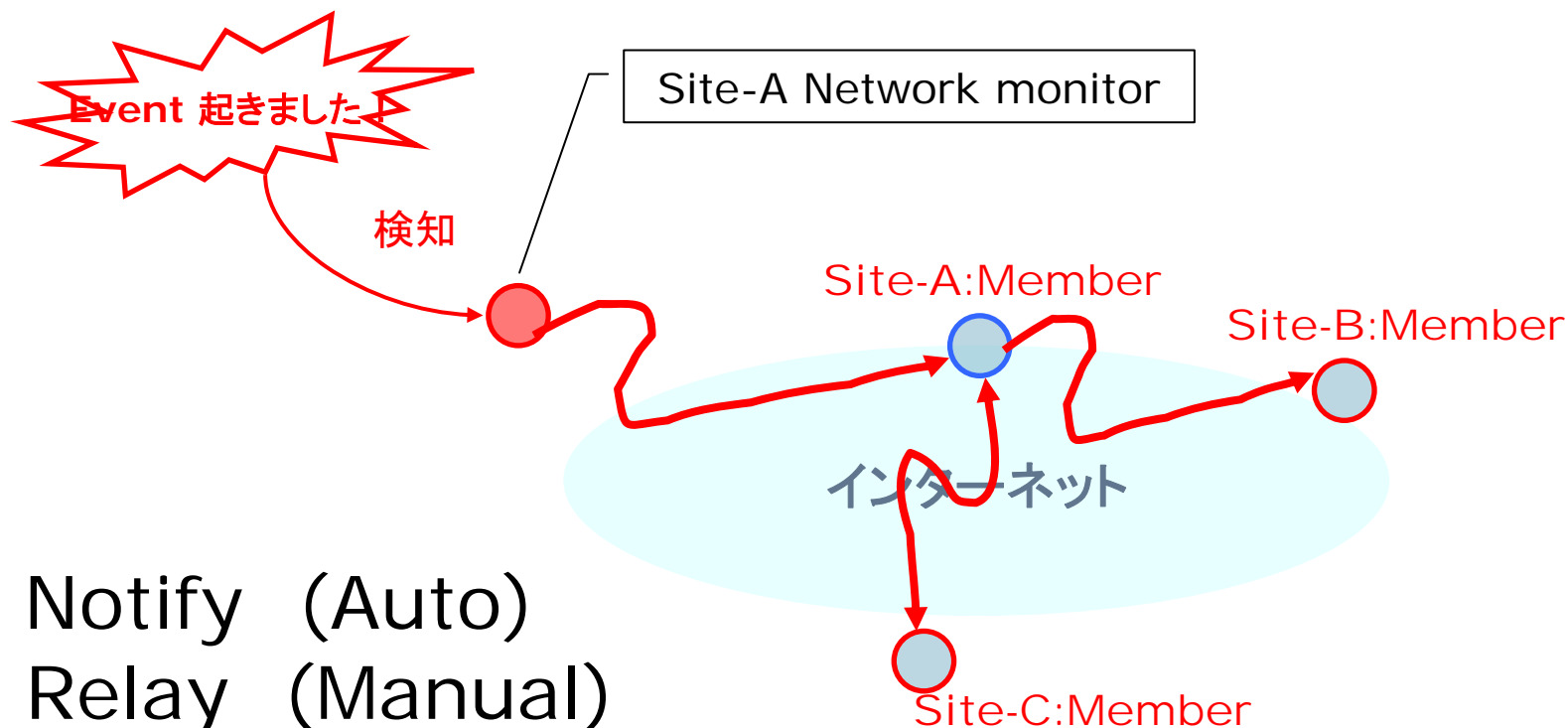
◆ 今後

- 普及：標準化の推進と定点観測等への適用
- 応用：既存運用管理アプリケーションとの連動

Demo-1:不正アクセス追跡システムの相互運用技術



Demo-2: 複数観測点における情報交換



Notify (Auto)
Relay (Manual)
Query (Manual)

From here:

- ◆ Use it
- ◆ Refine it
- ◆ Feedback to IETF-IODEF-WG

IETF-65, March 2006