

# I ODEF demonstration

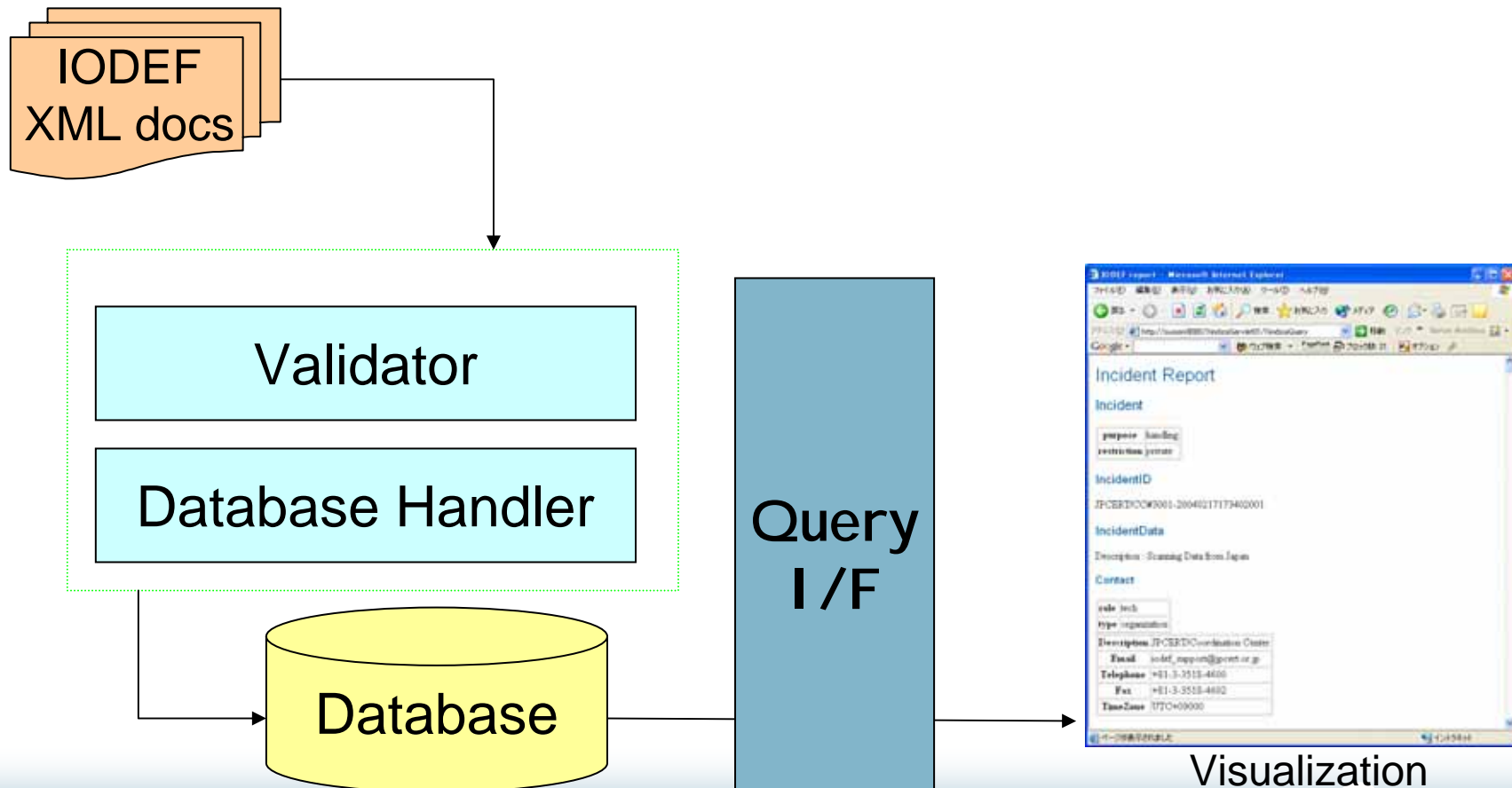
Glenn M. Keeni/Abe Katsuhisa

*INCH-WG, IETF-59*

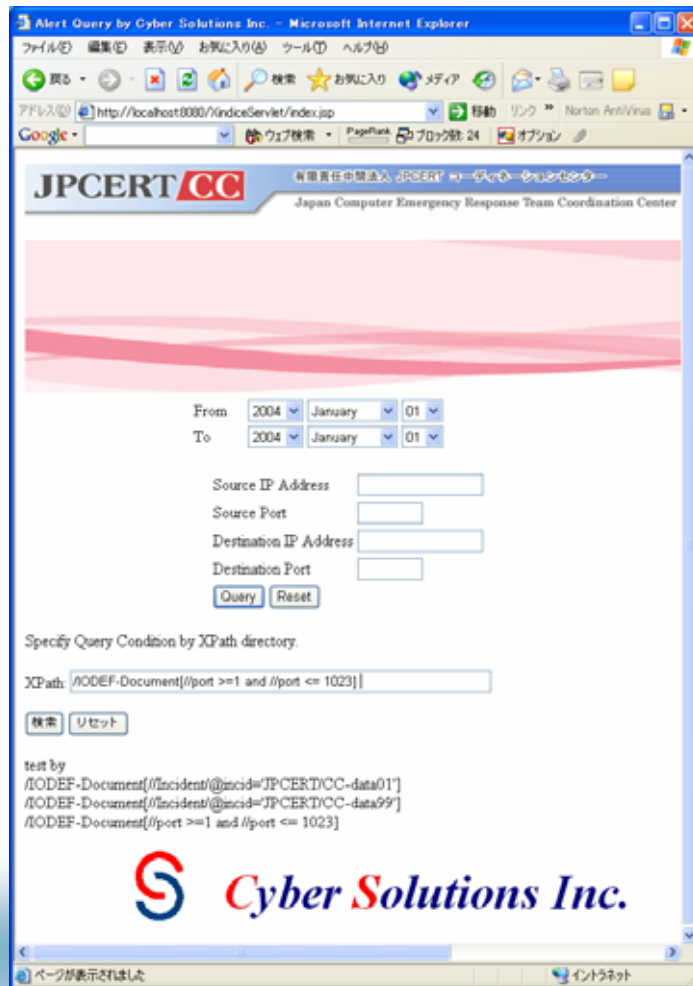
*March, 2004*



# The IODEF based system



# Screen Shots



Alert Query by Cyber Solutions Inc. - Microsoft Internet Explorer

http://localhost:8000/IndiceServlet/index.jsp

JPCERT CC  
Japan Computer Emergency Response Team Coordination Center

From: 2004 January 01  
To: 2004 January 01

Source IP Address  
Source Port  
Destination IP Address  
Destination Port

Query Reset

Specify Query Condition by XPath directory.

XPath: /NODEF-Document[//port >=1 and //port <= 1023]

検索 リセット

test by  
/NODEF-Document[//Incident/@incid='JPCERT/CC-data01']  
/NODEF-Document[//Incident/@incid='JPCERT/CC-data99']  
/NODEF-Document[//port >=1 and //port <= 1023]

Cyber Solutions Inc.



IODEF report - Microsoft Internet Explorer

http://localhost:8000/IndiceServlet/IndiceQuery

## Incident Report

Incident Id : JPCERT/CC#3001-2004021717340201

IncidentData (Scanning Data from Japan)

Contact	Role : tech Type : organization
Description	JPCERT/Coordination Center
E-mail	iodef_support@jpcert.or.jp
Telephone	+81-3-3518-4600
Fax	+81-3-3518-4602
TimeZone	UTC+0900
Time	Report Time :20040217 Start Time :20040217 End Time :20040217

Expectation : Please Check and Block scanning if possible

Assessment

Severity	medium
Completion	
Type	4

SYSTEM - Category : source

Address	69.150.57.255 (pv4-addr)
Node	Name : Location :
Port	4368
Service	Protocol : TCP OS :

DetectTime :  
2004-01-30T14:00:06-09:00

Cyber Solutions Inc.