Africa Asia collaboration on CSIRT Creation

Koichiro (Sparky) Komiyama

JPCERT/CC

AP* Retreat Meeting, Busan, South Korea
(in conjunction with APNIC32) 2011/9/2

AFRICAN INTERNET, SECURITY

ICT Ranking

The Networked Readiness Index 2010–2011

Country/Economy	Rank	Score	Rank within income group*	
Sweden	**1**	**5.60**	**HI**	**1**
Singapore	2	5.59	HI	2
Finland	3	5.43	HI	3
Switzerland	4	5.33	HI	4
United States	5	5.33	HI	5
Taiwan, China	6	5.30	HI	6
Denmark	7	5.29	HI	7
Canada	8	5.21	HI	8
Norway	9	5.21	HI	9
Korea, Rep.	10	5.19	HI	10
Netherlands	11	5.19	HI	11
Hong Kong SAR	12	5.19	HI	12
Germany	13	5.14	HI	13
Luxembourg	14	5.14	HI	14
United Kingdom	15	5.12	HI	15
Iceland	16	5.07	HI	16
Australia	17	5.06	HI	17
New Zealand	18	5.03	HI	18
Japan	19	4.95	HI	19
France	20	4.92	HI	20
Austria	21	4.90	HI	21
Israel	22	4.81	HI	22

Country/Economy	Rank	Score		
Tajikistan	112	3.25		
Côte d'Ivoire	113	3.20	LM	26
Benin	114	3.20	LO	10
Bangladesh	115	3.19	LO	11
Kyrgyz Republic	116	3.18	LO	12
Algeria	117	3.17	UM	31
Tanzania	118	3.16	LO	13
Venezuela	119	3.16	UM	32
Mali	120	3.14	LO	14
Lesotho	121	3.14	LM	27
Burkina Faso	122	3.09	LO	15
Ethiopia	123	3.08	LO	16
Syria	124	3.06	LM	28
Cameroon	125	3.04	LM	29
Libya	126	3.03	UM	33
Paraguay	127	3.00	LM	30
Nicaragua	128	2.99	LM	31
Madagascar	129	2.98	LO	17
Mauritania	130	2.98	LO	18
Nepal	131	2.97	LO	19
Zimbabwe	132	2.93	LO	20
Angola	133	2.93	LM	32
Swaziland	134	2.91	LM	33
Bolivia	135	2.89	LM	34
Timor-Leste	136	2.72	LM	35
Burundi	137	2.67	LO	21
Chad	138	2.59	LO	22

Source: The Networked Readiness Index 2010–2011 by World Economic Forum

Security Issues

■ Fraud

— Spam and Phishing in Western Africa

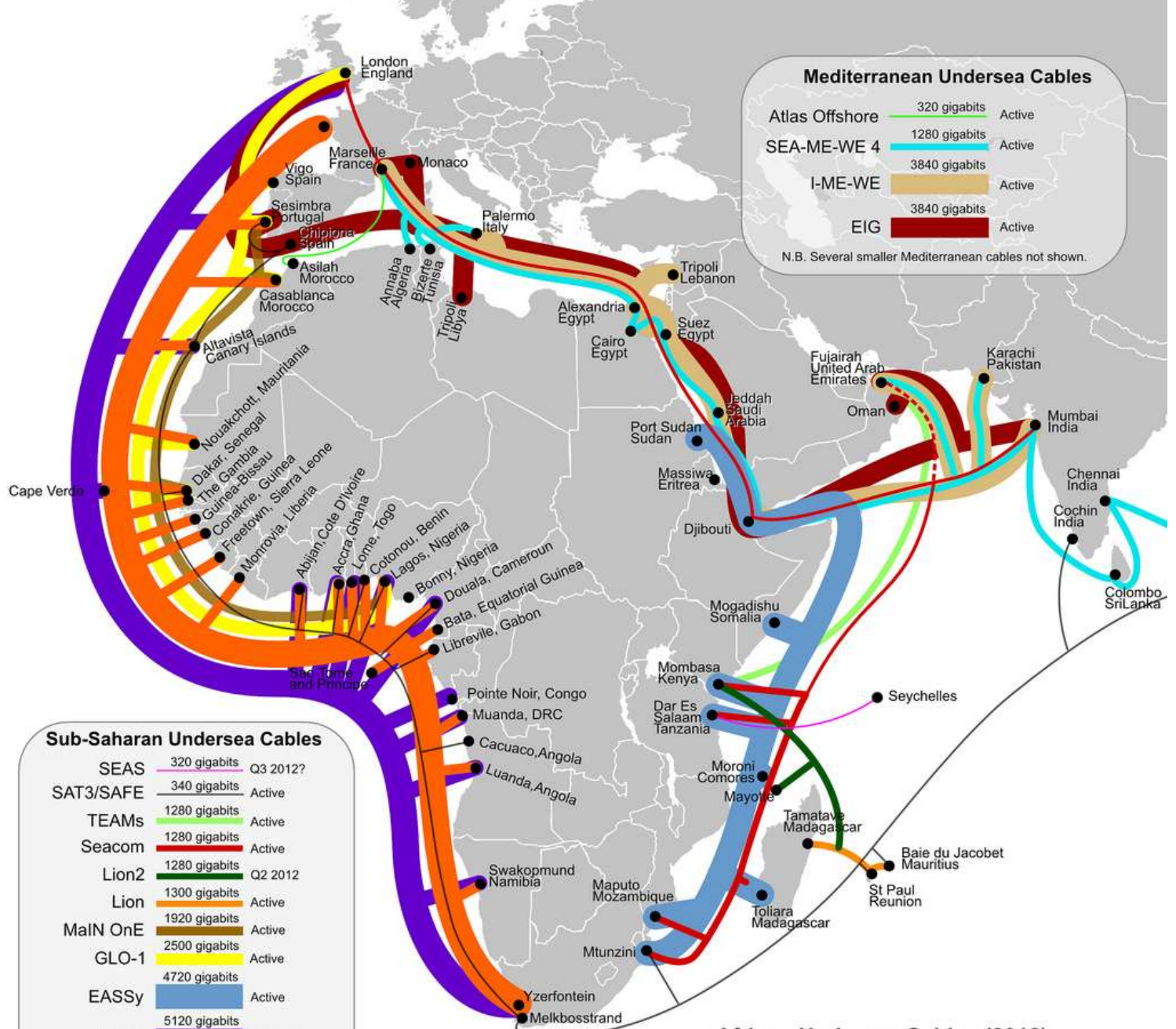— Advance-fee fraud(also called the Nigerian scam, Nigerian bank scam, Nigerian letter)

■ Bots

— The top five international cities with the highest zombie population:

1. Johannesburg, South Africa
2. Cape Town, South Africa
3. Lisbon, Portugal
4. New Delhi, India
5. Bangalore, India

— (Source: A Zombie Invasion
http://blogs.mcafee.com/consumer/family-safety/a-zombie-invasion)

Mediterranean Undersea Cables

Atlas Offshore	320 gigabits	Active
SEA-ME-WE 4	1280 gigabits	Active
I-ME-WE	3840 gigabits	Active
EIG	3840 gigabits	Active

N.B. Several smaller Mediterranean cables not shown.

Sub-Saharan Undersea Cables

SEAS	320 gigabits	Q3 2012?
SAT3/SAFE	340 gigabits	Active
TEAMs	1280 gigabits	Active
Seacom	1280 gigabits	Active
Lion2	1280 gigabits	Q2 2012
Lion	1300 gigabits	Active
MaIN OnE	1920 gigabits	Active
GLO-1	2500 gigabits	Active
EASSy	4720 gigabits	Active
WACS	5120 gigabits	Q2 2011
ACE	5120 gigabits	Q3 2012

African Undersea Cables (2012)
http://manypossibilities.net/african-undersea-cables
Version 28 - Mar 2011
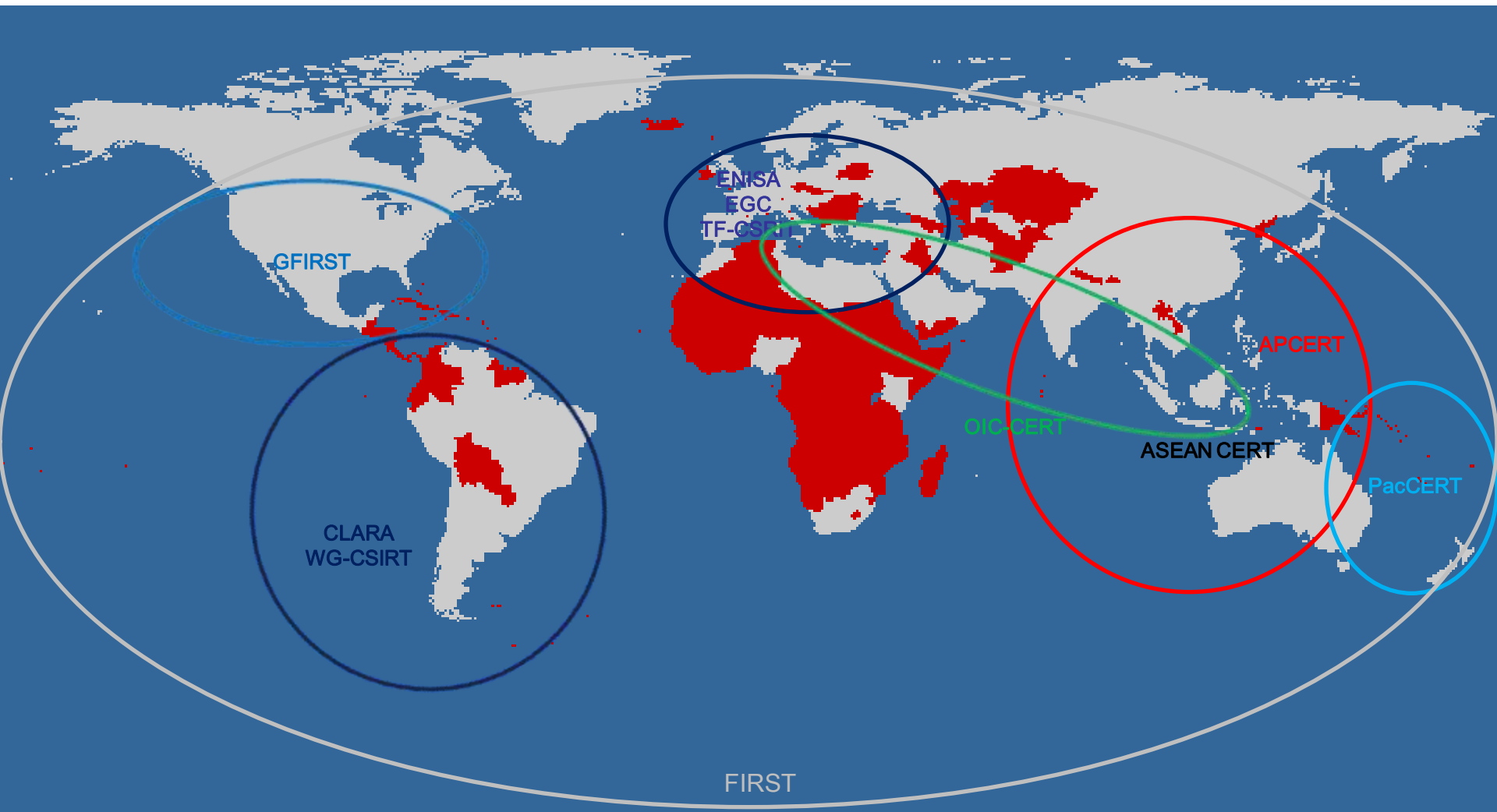
JPCERT/CC PROVIDE CSIRT TRAINING IN AFRICA

Let's develop100 CSIRT instructors in Africa!

Ideas behind

■ Teaching "teacher of teachers"

— Training course development by African community

— Localization for Africa

■ By Africans

— Creating their community (regional)CSIRT in African continent

■ 54 countries.

■ Back to back with local ICT events

— AFNOG meeting / AFRINIC meeting

Managers Course (3days) | Technical Course (5days) | Advanced Course (5days)

Kigali (May 2010)

Johannesburg (Nov 2010)

Dar es Salaam (May/June 2011)

Cameroon (Fall 2011)
Tentative

Training by JPCERT

Training by African instructors

Workshop with open participation

CERT Instructor Training Course for Managers
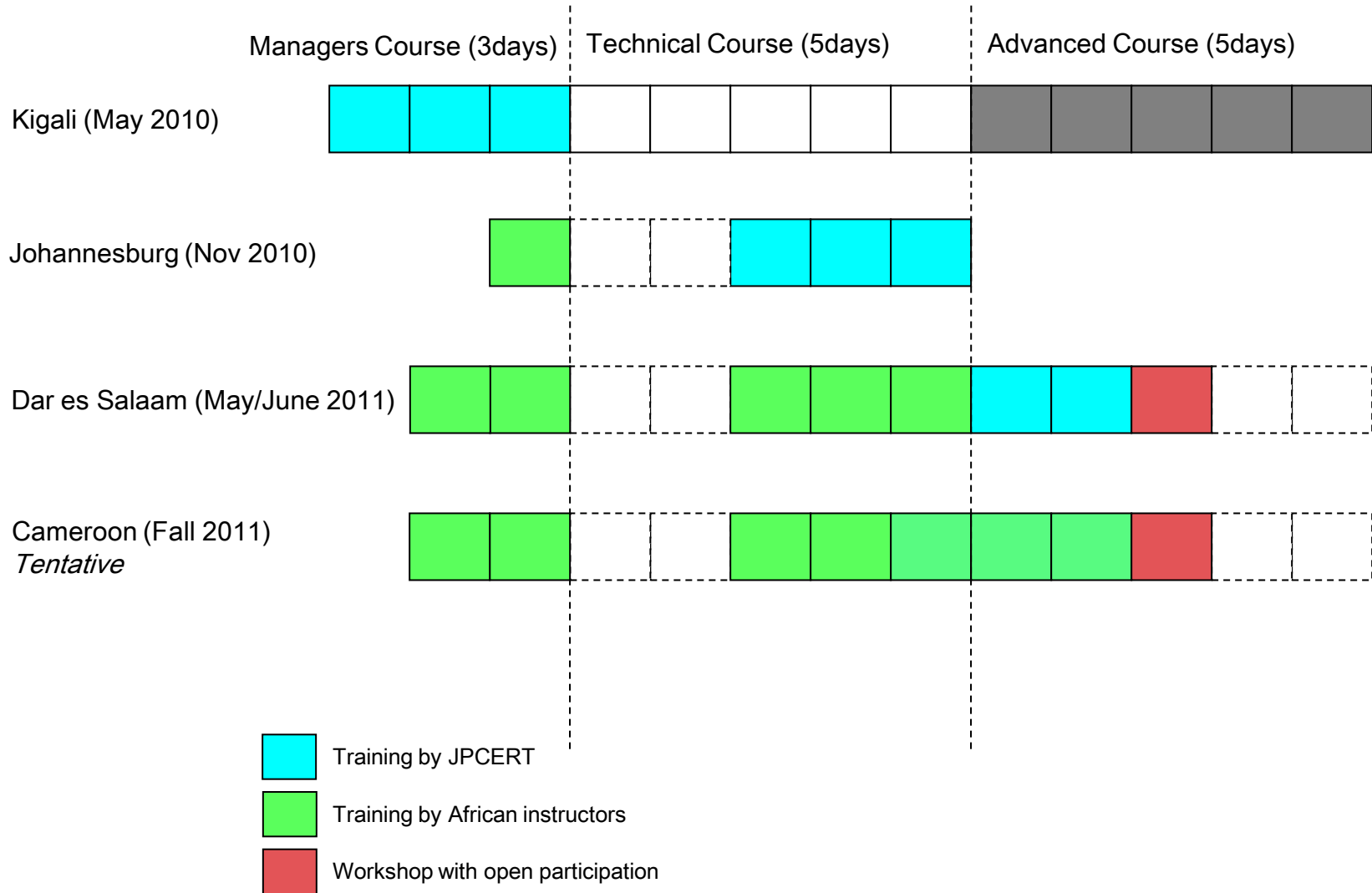
- Date: 31 May 2010
- Venue: Kigali, Rwanda
- Hosted by: AfNOG, AfriNIC, AfREN and AAF
- Participants: 30 (instructor candidates and additional participants)
- Training program:
  — Internet security trend
  — Overview of CSIRT and fundamentals of computer security incident handling
  — Creating a CSIRT
  — International CERT activities
- URL: http://africaasia.net/2010-6-CERT.html

JPCERT CC®

- Date: 20-22 November 2010
- Venue: Johannesburg, South Africa
- Hosted by: AfriNIC and AAF
- Participants: 30 Engineers from South Africa, Uganda, Kenya, DRC, Somalia, and so on.
- Training program:
  - CSIRT culture and philosophy
  - Network traffic analysis (hands-on)
  - Log analysis (hands-on)
  - Tools and operations
- URL: http://meeting.afrinic.net/afrinic-13/index.php/the-meeting/agenda

Agenda

- About CERT-MU
- Road-Map
- Plan v/s Actual
- Challenges and Roadblocks
- Some Important Tips
- Conclusion

QCC Information Security

CERT Instructor Training Course

- Date: 5/31-6/4 2011

- Venue: Dar es Salaam, Tanzania

- Hosted by: AfNOGand AAF

- Participants: 23 Engineers from 8 countries (Tanzania, Ghana, Kenya, DRC, Somalia, and so on.)

- Training program:
  - —5. 30 CERT Introduction (CERT Training Course for Manager and Policy Maker)
  - —5.31~6.2 CERT Training Course for Technical Staff
  - —6.3~6.4 CERT Training Course on Web Security

- URL: N/A

Lessons learned

- Internet experts in Africa are keen on developing CSIRT
- freedom of expression, privacy, trust, and security online
- Lack of practical experience -> "start small with minimum function"

Next Step

- AfricaCERT
  - Continent wide CSIRT. Now asking for comment on the project blueprint
- Kenya
  - Kenya Computer Incident Response Team (KE-CIRT) has been launched officially.
  - Couple of industry initiatives are going on as well
- Training
  - CSIRT Training (Afrinic 15 at Cameroon ,November 2011)
    - http://meeting.afrinic.net/afrinic-15/
  - Two-day Security seminar(Nigeria, November 2011)

Thank You

Web: https://www.jpcert.or.jp/
http://blog.jpcert.or.jp

Email: global-cc@jpcert.or.jp