FIRST

Improving Security Together

Incident Response: Collaboration and Sharing

Tule külasta meid
Kom og besøg os
Kom och besök oss
Tule käymään
Obiščite nas
Prídte nás Navštíviť!
Veniti sa ne vizitati
Kom ons bezoeken
Ejja arana
Jöjjön el látogatóba!
Atvaziuokite Mūsų aplankyti!
Nāciet ciemos!
Visite-nos!
Venez nous voir
Venga a visitarnos
Kommen Sie vorbei !
Odwiedz nas!
Come and visit us
มาเยี่ยมชมเรา

FIRST TC @ KYOTO
Kyoto 2012 FIRST Technical Colloquium
13-15 November 2012

welcome to Kyoto.

It is our pleasure to welcome you to the 2012 FIRST Technical Colloquium here in Kyoto. We are sure that the combination of the location, the programs, the presenters and the attendees will make an exciting three days for us all.

The tagline for the FIRST TC in Kyoto, "Incident Response: Collaboration and Sharing", asks us how we can further activate incident response through collaboration and sharing among the FIRST teams. We are also building an agenda which will lead to "Incident Response: Sharing to Win", the tagline for the 25th Annual FIRST Conference to be held next year in Bangkok.

FIRST TC in Kyoto includes three sessions; FIRST Seminar, FIRST Hands-On Classes and Summit Days (Future of Global Vulnerability Reporting Summit). We believe that the FIRST TC in Kyoto will trigger the new global era of the FIRST.

As you know, Kyoto proudly reigned as the capital of Japan for 1200 years and is considered as the heart of Japanese tradition. Now as a modern city, this history and heritage vividly lives with the 1.5 million people: Seventeen UNESCO World Cultural Heritage Sites are situated in a cityscape full of more than 2000 temples and shrines. Also during the "Koyo (red leaves/colored leaves)" season in Kyoto, the leaves of deciduous trees and shrubs take on red hue all at once and combined with the city's history and heritage, the scenes are fantastic. We hope you will enjoy Kyoto as much as you will enjoy the workshop.

We would like to thank all of the people who have worked to bring FIRST TC in Kyoto together, Nora Duhig, the Steering Committee and all of those who have put in an enormous amount of time and effort.

FIRST Japan Teams are looking forward to seeing everyone in beautiful autumn Kyoto!

Suguru Yamaguchi and Masato Terada

와서 우리를 방문
前来参观我们
Приезжайте к нам

وتأتي زيارة لنا

FIRST TC @ KYOTO
Kyoto 2012 FIRST Technical Colloquium
13-15 November 2012

organization committee.

General Chairs
Suguru Yamaguchi (FIRST SC)
Masato Terada (HIRT)

Advisory Committee
Koki Yoshida (NISC)
Takehiko Nakayama (CFC)

Finance Committee
Akiko Numata (HIRT)

Program Committee
Yoshiki Sugiura (NTT-CERT)
Mamoru Saito (IIJ-SECT)
Masayuki Okuhara (FJC-CERT)
Manabu Nakano (IPA-CERT)
Koichiro Komiyama (JPCERT/CC)
Takayuki Uchiyama (JPCERT/CC)
Hiroyuki Yoshiba (KKCSIRT)
Takeshi Matsuoka (MIXIRT)
Tatsuya Kitao (MUFG-CERT)
Itaru Kamiya (NTT-CERT)
Ikuya Hayashi (NTT-CERT)
Hikohiro Lin (Panasonic PSIRT)
Akifumi Yamai (YIRD)

Liaison Committee
Hiroki Iwai (JSOC)
Kunio Miyamoto (NTTDATA-CERT)
Hiroko Okashita (IPA-CERT)

Local Arrangement Committee
Kazuya Hiradate (NCSIRT)
Kensuke Masaki (NCSIRT)
Taku Murakami (NCSIRT)
Yuta Miura (KDDI-SOC)
Yoshitaka Inoue (NTT-CERT)
Naoya Kitawaki(KKCSIRT)

Publicity Committee
Tomonori Shiomi (MBSD-SIRT)
Natsuko Inui (CDI-CIRT)
Masako Someya (CDI-CIRT)
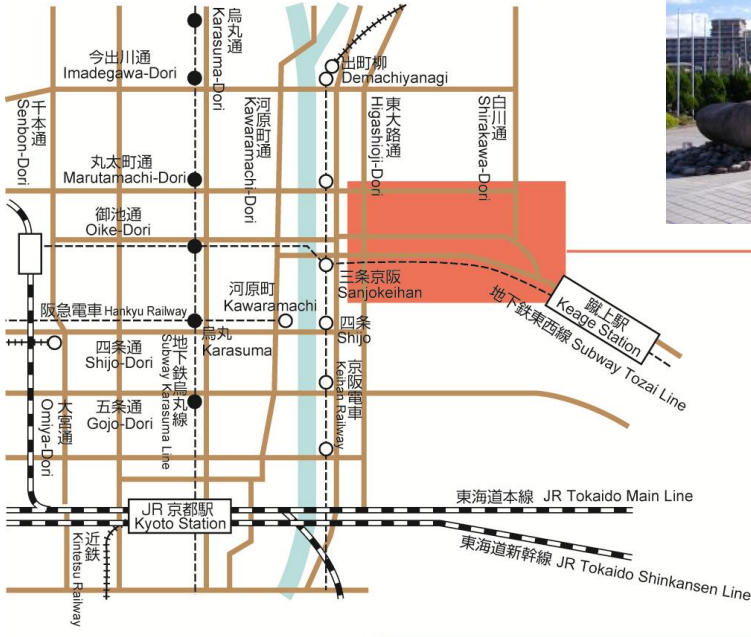Yusuke Gunji (Rakuten-CERT)
Naoko Ohnishi (HIRT)

Auditing Committee
Katsuyuki Matsumoto (SBCSIRT)

FIRST TC @ KYOTO
Kyoto 2012 FIRST Technical Colloquium
13-15 November 2012

Kyoto International Community House

FIRST TC @ KYOTO
Kyoto 2012 FIRST Technical Colloquium
13-15 November 2012

schedule at-a-glance.

		Room 1 & 2	Room 4	Room Kenshu
Nov 13	13:00-13:10	FIRST TC Opening		
	13:10-17:30	FIRST Seminar		Summit Days
Nov 14	09:30-09:40	Opening Remarks		
	09:40-12:30	FIRST Seminar		Summit Days
	14:00-17:30	FIRST Seminar		Summit Days
	18:00-21:00	Social Event		
Nov 15	09:30-09:40	Opening Remarks		
	09:40-12:30	Summit Days	Hands-On Class1	Hands-On Class2
	14:00-17:00	Summit Days	Hands-On Class3	Hands-On Class4 (13:00-17:00)
	17:00-17:10	Closing Remarks		

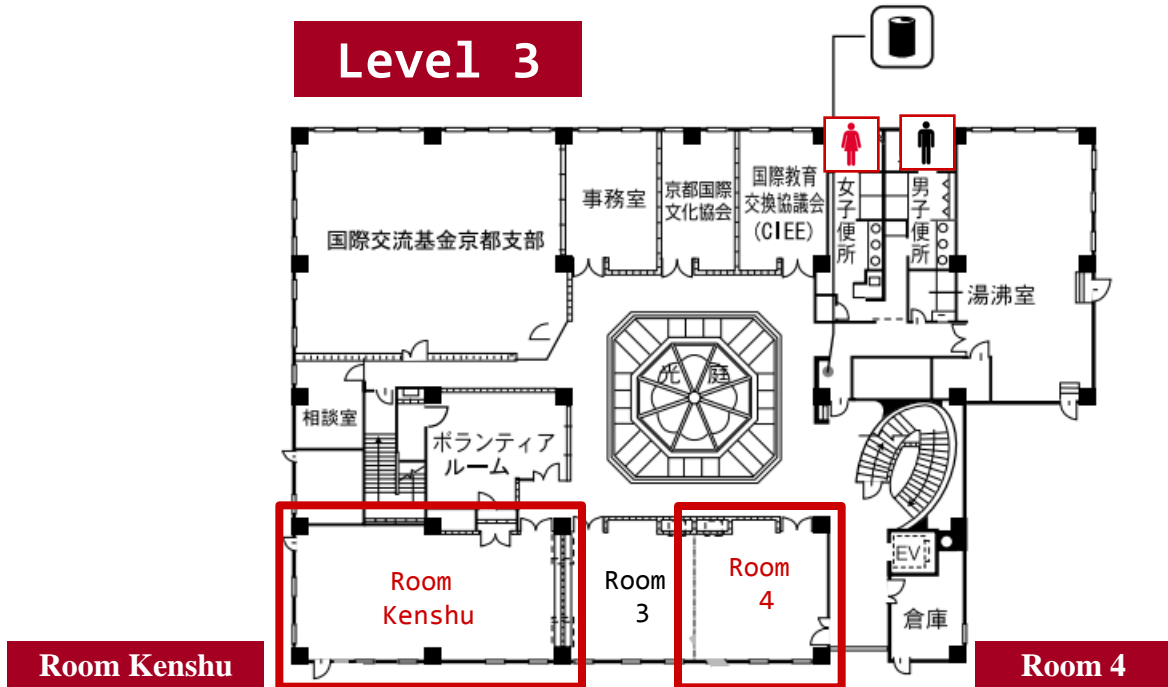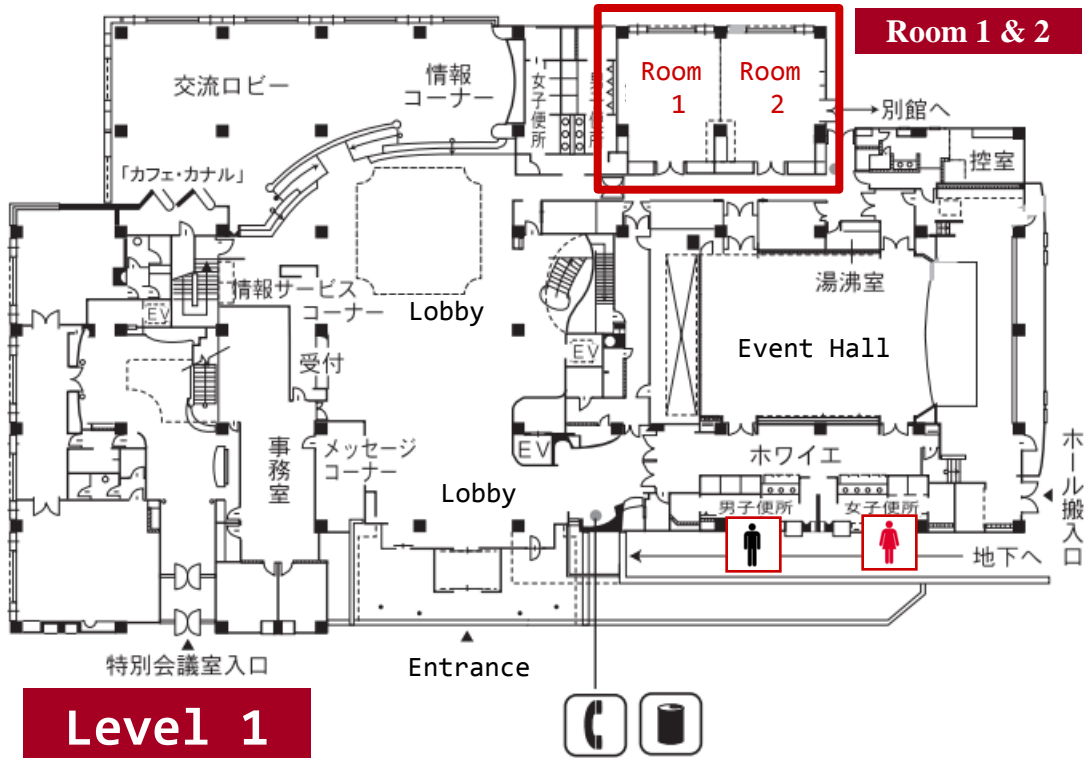# Incident Response: Collaboration and Sharing

floor plans.

Kyoto International Community House

Room 1 & 2

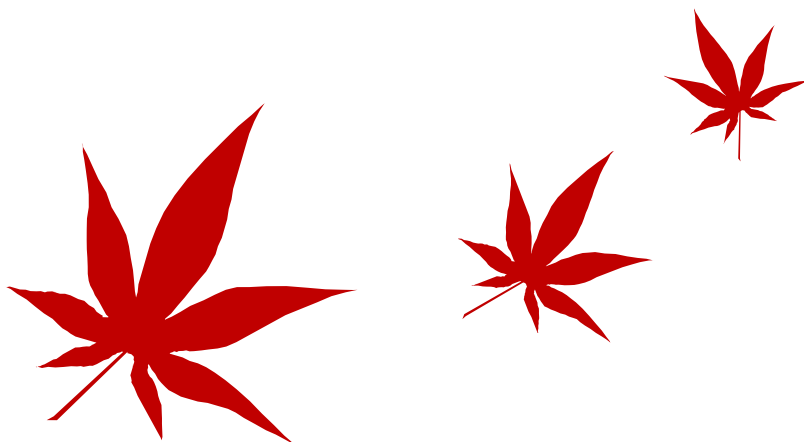Level 1

Level 3

Room Kenshu

Room 4

Summit Days

Future of Global Vulnerability Reporting Summit focuses on Current challenges & issues (coverage, scale, numbering and etc.) and proposed solutions of vulnerability tracking, especially "Global Vulnerability Identification Scheme".

Currently one of the most well known vulnerability identification schemes is Common Vulnerabilities and Exposures (CVE). CVE is used by many organizations throughout the world for cross-referencing vulnerabilities across various databases. However, the current process governing CVE has its limitations and has not been able to keep up with the ever increasing number of vulnerabilities being discovered and made public each year. At first, we would like to discuss the limitations of the current process, and how organizations currently use CVE to link their databases across the globe to for cross-referencing vulnerabilities. Second, we would like to discuss the next steps for challenge of "Global Vulnerability Identification Scheme" on the final day.

FIRST TC @ KYOTO
Kyoto 2012 FIRST Technical Colloquium
13-15 November 2012

TUESDAY, 13 November 2012

	FIRST Seminar //Room 1&2	Summit Days //Room Kenshu
13:00-13:10	**FIRST TC Opening** //Room 1&2 *Suguru Yamaguchi (FIRST), JP*	
13:10-13:15	Short Break	
13:15-14:00	**Security Activities in Thailand** *Soranun Jiwasurat (ThaiCERT), TH*	**The Current State of Vulnerability Reporting** *Harold Booth (NIST), US* *and Masashi Ohmori (IPA), JP*
14:00-14:45	**Smartphone Security: Pitfalls to Avoid** *Ken van Wyk (KRvW Associates, LLC), US*	**The Value of Global Vulnerability Reporting** *Dave Waltermire (NIST), US* *and Masato Terada (IPA), JP*
14:45-15:15	Coffee & Networking Break	
15:15-16:00	**Smartphone Security and Finding "Third-Party" Risks** *Tsukasa Oi (Fourteenforty Research Institute, Inc.) , JP*	**Global Vulnerability Identification and Usage: A Vendor's Perspective** *Kent Landfield (McAfee), US*
16:00-16:45	**Chasing the Fox: A closer look at an APT malware** *Andreas Schuster (Deutsche Telekom AG), DE*	**CVE Perspectives on Global Vulnerability Reporting** *Steve Christey (MITRE), US*
16:45-17:30	**Tracing Botnet in Taiwan** //Room 1&2 *Kai-chi Chang (III, ICST), TW*	

WEDNESDAY, 14 November 2012

	FIRST Seminar //Room 1&2	Summit Days //Room Kenshu
09:30-09:40	**Opening Remarks** //Room 1&2 *Suguru Yamaguchi (FIRST), JP*	
09:40-09:50	**Report from FIRST Educational Committee** //Room 1&2 *Shin Adachi (Education Committee Co-Chair), US*	
09:50-10:00	**About 25th Annual FIRST Conference (Bangkok, Thailand, 16-21 June 2013)**	
10:00-10:45	**Role of Cyber Security in Civil Protection** *Maurice Cashman (McAfee), DE*	**Vulnerability Handling in Japan and linking through CVE** *Takayuki Uchiyama (JPCERT/CC), JP*
10:45-11:00	Coffee & Networking Break	
11:00-11:45	**Public-Private partnership for counter Cyber-Intelligence and Malware analysis case study** *Takehiko Nakayama (CFC), JP and Yuji Kubo (CFC), JP*	**ThaiCERT Activities and how vulnerability information is being used** *Soranun Jiwasurat (ThaiCERT), TH*
11:45-12:30	**How we Collaborate and Share** *Wim Biemolt (SURFnet, SURFcert), NL*	**Activities for vulnerability by KrCERT/CC** *HongSoon Jung (KrCERT/CC, KISA), KR*
12:30-14:00	Lunch Break	
14:00-14:45	**Hot Topics in Internet Measurement : Power-law Properties in Indonesia Internet Traffic. Why do we care about it ?** *Bisyron Wahyudi (Id-SIRTII), ID*	**Structure and numbering of JVN, and Security content automation framework** *Masato Terada (IPA), JP*
14:45-15:30	**Responding to Security Incident: MyCERT approach and case study** *Megat Muazzam Abdul Mutalib (MyCERT), MY*	**Public-Private Partnership and Control System Security** *Hideaki Kobayashi (IPA, CSSC), JP*
15:30-16:00	Coffee & Networking Break	
16:00-16:45	**Tracing Attacks on Advanced Persistent Threats in Networked Systems** *Hiroshi Koide (Kyushu Institute of Technology, IPA), JP*	**Introduce SCADA vulnerability and a little suggestion for vulnerability numbering format** *Kai-chi Chang (III, ICST), TW*
16:45-17:30	**Effective Discovery of Malicious Websites** *Mitsuaki Akiyama (NTT-CERT), JP*	Clean up Room
17:30-18:00	Short Break	
18:00-21:00	**Social Event**	

FIRST TC @ KYOTO
Kyoto 2012 FIRST Technical Colloquium
13-15 November 2012

THURSDAY, 15 November 2012

FIRST Hands-On Classes

Time	Description
09:30-09:40	**Opening Remarks** //Room 1&2 *Masato Terada (HIRT), JP*
09:40-10:00	Short Break
10:00-12:30	**Class1** //Room 4 **Introduction to YARA** *Andreas Schuster (Deutsche Telekom AG), DE* — **Class2** //Room Kenshu **Smartphone App Security: Breaking and Building Secure Apps** *Ken van Wyk (KRvW Associates, LLC), US*
12:30-14:00	Lunch Break
14:00-17:00	**Class3** //Room 4 **Introduction to YARA** *Andreas Schuster (Deutsche Telekom AG), DE* — **Class4** //Room Kenshu **(13:00-17:00)** **Forensic Investigation & Malware Analysis against Targeted Attack using Free Tools** *Takahiro Haruyama (IIJ-SECT), JP* *and Hiroshi Suzuki (IIJ-SECT), JP*
17:00-17:10	**Closing Remarks** //Room 1&2 *Masato Terada (HIRT), JP*

Summit Days //Room 1&2

Time	Description
09:30-09:40	**Opening Remarks** //Room 1&2
09:40-10:00	Short Break
10:00-11:00	**Discussion of common themes and use cases from previous day** *Coordinator: Harold Booth (NIST), US*
11:00-11:15	Coffee & Networking Break
11:15-12:30	**Discussion of ideas for solutions to use cases** *Coordinator: Dave Waltermire (NIST), US*
12:30-14:00	Lunch Break
14:00-15:15	**Additional Discussion of Ideas** *Coordinator: Kent Landfield (McAfee), US*
15:15-15:45	Coffee & Networking Break
15:45-17:00	**Proposal of FIRST SIG planning "Vulnerability Reporting and Data eXchange"** *Coordinator: Takayuki Uchiyama (JPCERT/CC), JP and Steve Christey (MITRE), US*
17:00-17:10	**Closing Remarks**

FIRST TC @ KYOTO
Kyoto 2012 FIRST Technical Colloquium
13-15 November 2012

see you at the next conference.

Incident Response:
Sharing to Win

25TH **BANGKOK** JUNE **2013**
ANNUAL **FIRST** CONFERENCE

INCIDENT RESPONSE: SHARING TO WIN
BANGKOK, THAILAND | 16-21 JUNE 2013

FIRST.
Improving Security Together

FIRST TC @ KYOTO
Kyoto 2012 FIRST Technical Colloquium
13-15 November 2012

thank you FIRST TC @ Kyoto sponsors.

Diamond

HITACHI

Gold

SoftBank

Summit Days

IPA   **JPCERT CC®**

Supporting Organizations

National Information Security Center
Ministry of Internal Affairs and Communications
Ministry of Economy, Trade and Industry
National Police Agency

Sponsoring Organizations

Nippon CSIRT Association

FIRST TC @ KYOTO
Kyoto 2012 FIRST Technical Colloquium
13-15 November 2012