

The Great East Japan Earthquake - What we did as CSIRTs-

June 14, 2011

Itaru Kamiya, NTT-CERT

Yoshinobu Matsuzaki, IIJ-SECT

Teruo Fujikawa, NCSIRT

Yusuke Gunji, Rakuten-CERT

Moderator: **Takayuki Uchiyama, JPCERT/CC**

23_{rd}

12 - 17 June 2011

Annual **FIRST** Conference

Hilton Vienna | Austria



Vienna

What happened?

- **Earthquake Occurred** 3/11/11 14:46:18 (JST)

Recorded a 9.0 on the Richter scale

Most powerful earthquake to hit Japan

- **Tsunami**

15 minutes after the initial earthquake, large tsunamis in the Pacific Ocean formed. Coastal regions in the Tohoku and Kanto areas were damaged by the massive tsunamis

- **Nuclear Power Plant stoppages and issues**

3/11: Nuclear power plants automatically stopped right after the earthquake

Core cooling system stopped and a Nuclear Emergency was declared

3/12: Hydrogen explosion at the reactor building

- Concerns about radiation contamination

- Electricity shortage due to plant stoppages

19 teams

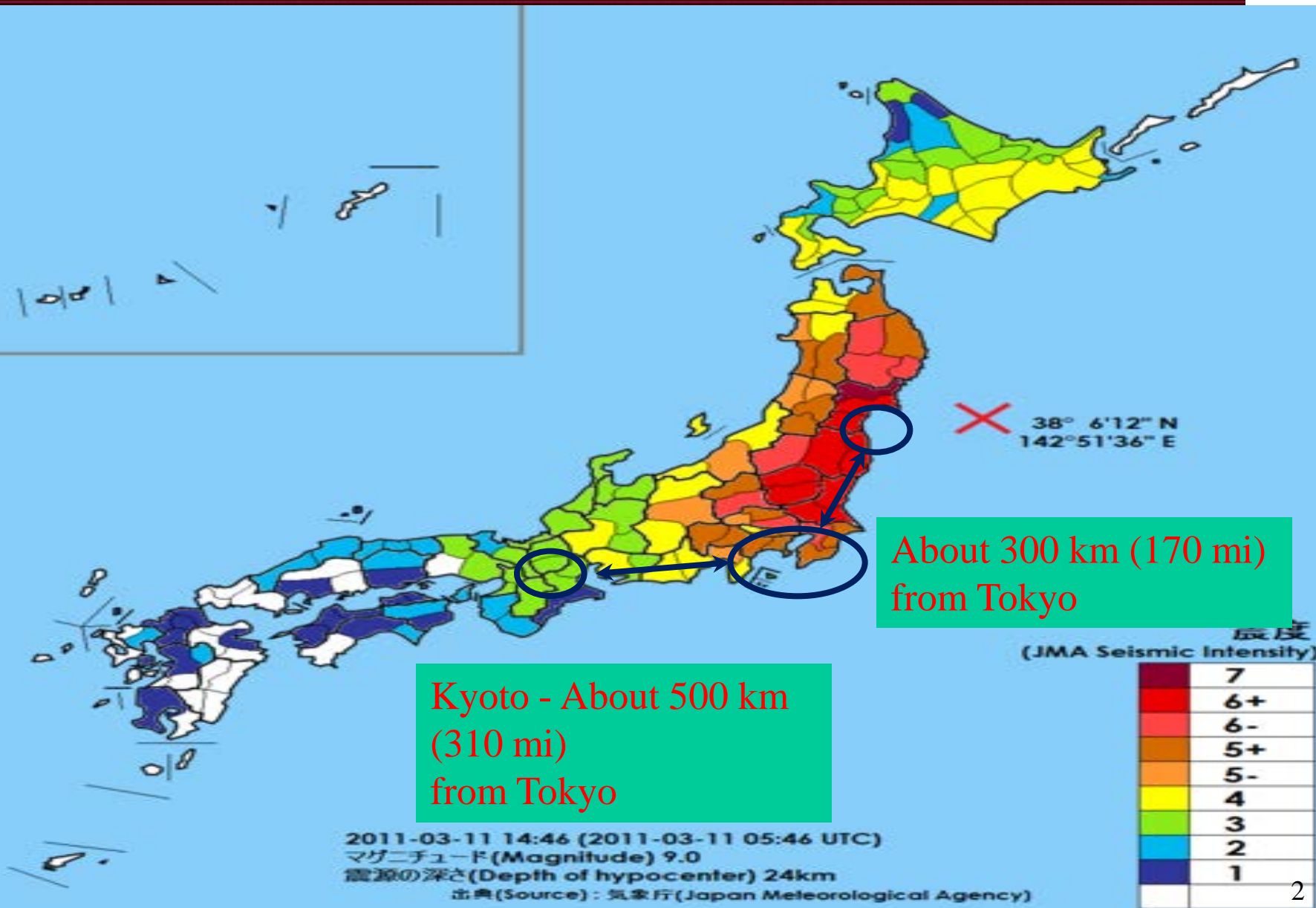
FIRST
JapanTeams

12 - 17 June 2011

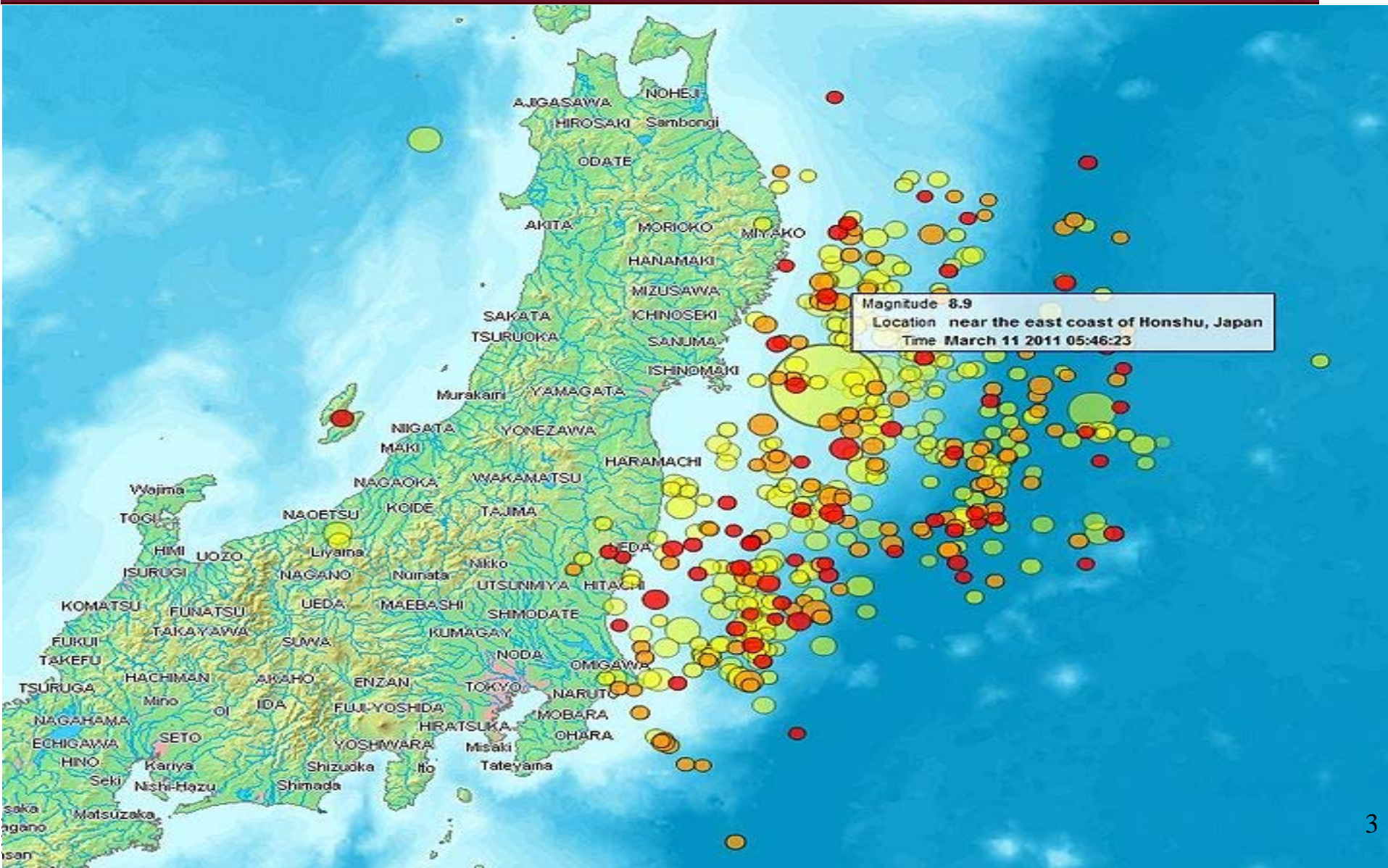


Vienna

The Main Earthquake



Location of the Aftershocks



Some Photos



Some Numbers on the Earthquake

- Data as of end of May
 - Death toll: over 18,000
 - Another 13,000+ still reported as missing
 - Over 130,000 still remaining in temporary shelter
 - Over 76,000 buildings damaged, over 6,000 completely destroyed
- Reference Numbers
 - The population of Tokyo is around 13 million (~ 10% of total population)
 - Kanto region has over 42 million people

Electricity Issues

- The maximum amount of electricity that could be provided was cut severely due to nuclear power plants going down
- Affected mass transportation
 - People were not able to get to work due to trains not running
- As a result, rolling blackouts were planned
 - The Tokyo region was split into groups for planned blackouts



Rolling Blackouts

計画停電の実施方法

- 停電する地域（イメージ） 【具体的な停電地域については別紙による】
供給の再開を迅速に行うため、グループを分散化



※停電時間は、多少前後する場合があります。

Discussion Agenda

- Where were you and what you did right after the earthquake?
- What kind of disaster recovery efforts did your company partake? Is there anything that was done as a CSIRT?
- Infrastructure Issues – Electric, Communications etc.
- Incidents directly related to the disaster and what was done as a CSIRT to solve such issues
- Final Thoughts – what should be done in the future?



Discussion Agenda

- Where were you and what you did right after the earthquake?
- What kind of disaster recovery efforts did your company partake? Is there anything that was done as a CSIRT?
- Infrastructure Issues – Electric, Communications etc.
- Incidents directly related to the disaster and what was done as a CSIRT to solve such issues
- Final Thoughts – what should be done in the future?



Where were you and what you did right after the earthquake? - NTT-CERT

- Itaru Kamiya

- Works for NTT
- Member of NTT-CERT
- Doing IR, vul handling, Sensor NW, etc

- At 3/11

- at my office in Tokyo
- walked home for 30km



Where were you and what you did right after the earthquake?

– IIJ-SECT (1/3)

- Was at an IPv6-related meeting in another company's office when the big earthquake hit
- According to reports collected, the damage in the north-eastern part of Japan was very severe, but not so in Tokyo area
 - All members of IIJ-SECT were safe in Tokyo
- Elevators had become out of service

Where were you and what you did right after the earthquake?

– IIJ-SECT (2/3)

- Returned to our office
- Railroads were suspended all day long pending safety checks, and a lot of cars caused heavy traffic jams
 - Some people stayed at office overnight, others walked back home

Where were you and what you did right after the earthquake?

– IIJ-SECT (3/3)

- One member of IIJ-SECT (ME!) was put into IIJ disaster recovery team
 - Information gathering & response
- Next day, almost all businesses in Tokyo appeared normal as usual Saturdays
 - Went to a hotel to make arrangements with their staff about **my wedding party** 😊

Where were you and what you did right after the earthquake?

- NCSIRT

● Profile

- Teruo Fujikawa
- NRI SecureTechnologies, Ltd.
- Managed Security Service Provider
- IT Security Analyst
- Rep. of NCSIRT



● We did

- 1st. EVACUATION!
- 2nd. Confirmation about our service continuance
Contact to our Customers

19 teams

FIRST
JapanTeams

12 - 17 June 2011



Vienna

Where were you and what you did right after the earthquake? - NCSIRT

- Unexpected matter

- Telephone call limitation



- Stop of public transportation

- Heavy traffic jam



10mile

19 teams

FIRST
JapanTeams

12 - 17 June 2011



Vienna

● Yusuke “Scott” Gunji

- Father of 4 kids
- Second rep of Rakuten-CERT (CISSP)
- Ex: Yahoo! Japan, mixi (The biggest SNS in Japan)

What happened on 3.11?

- Rakuten-CERT

- I was in Tokyo office (8th Floor).
- Start collecting information from web, but still working as usual for a couple hours.
- 2 hours later, company decided to allow us to go home. (not order)
 - We didn't have enough information about transportation. Web news didn't have a clue as well.
- After the quake, cel phone didn't work at all, very worried about my family, but could get contact them with company IP phone.

What happened 3.11? -2-

- Rakuten-CERT

- Left office around 5 pm.
- Bought a bike, and tried to get home with it. (30km away ;-)
- On the way, traffic jammed and people were walking home.
- Some of train came back around midnight.



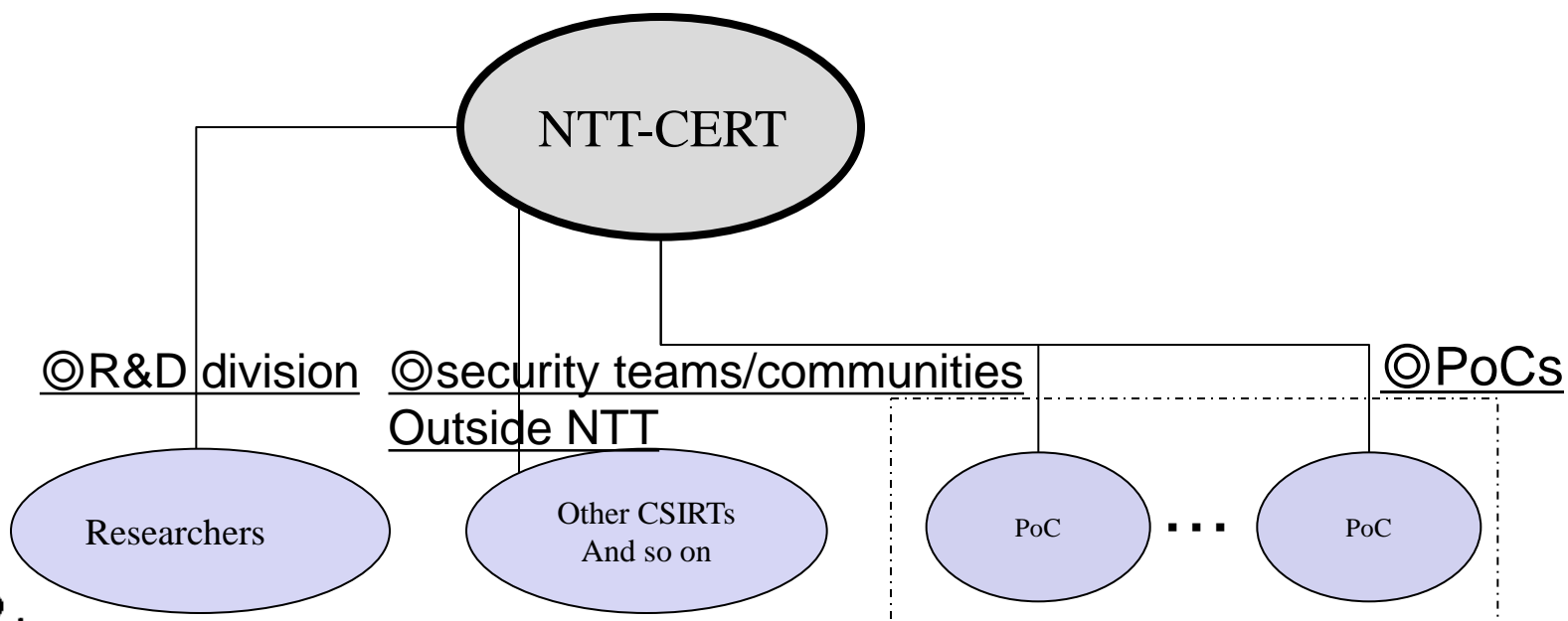
Discussion Agenda

- Where were you and what you did right after the earthquake?
- What kind of disaster recovery efforts did your company partake? Is there anything that was done as a CSIRT?
- Infrastructure Issues – Electric, Communications etc.
- Incidents directly related to the disaster and what was done as a CSIRT to solve such issues
- Final Thoughts – what should be done in the future?



What kind of disaster recovery efforts did your company partake? Is there anything that was done as a CSIRT?(1/3) – NTT-CERT

Regular formation



What kind of disaster recovery efforts did your company partake? Is there anything that was done as a CSIRT?(2/3) – NTT-CERT

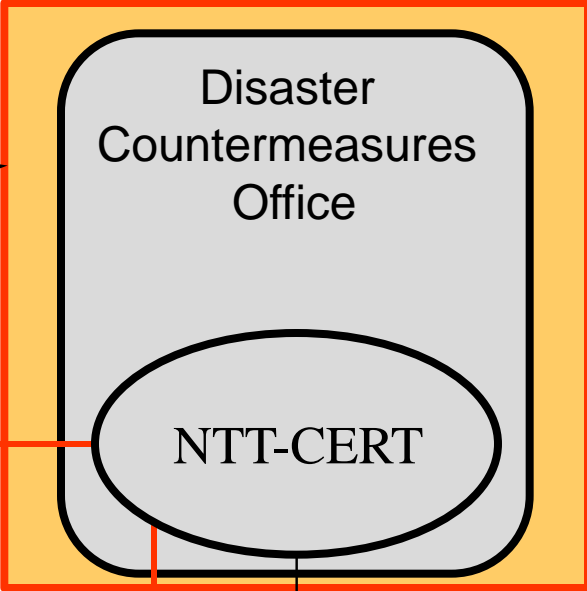
Formation under the emergency

huge disaster happens



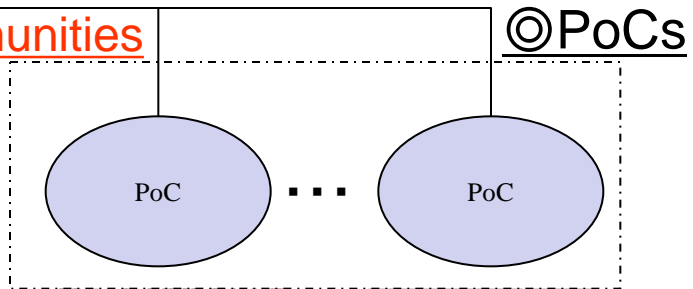
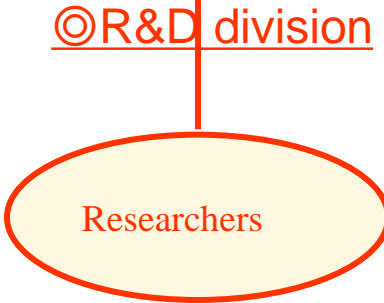
Emergency declaration and Order from MIC*

— More Cooperation than normal times



NTT have to establish the Disaster Countermeasures Office in accordance with disaster prevention operation plans based on the Basic Act on Disaster Control Measures.

MIC: The Ministry of Internal Affairs and Communications



What kind of disaster recovery efforts did your company partake? Is there anything that was done as a CSIRT?(3/3) – NTT-CERT

Disaster Countermeasures Office

- (1) Prevent cyber attacks against NTT telecommunications equipment that take advantage of the earthquake
 - Information gathering from security teams or communities outside NTT
 - Extensive Public monitoring
- (2) Early detection about rumors and hoaxes against NTT group companies
 - Extensive Public monitoring
more from peoples voices (BBS, Social Medias, tweet, etc)

Enhancement of support for NTT group companies

- (1) 24/7

Infrastructure Issues – Electric, Communications etc.

- NTT-CERT

- working against blackout risk
 - Recheck our working environment
 - Locations of servers (and rout to get there), auto-locks, Fire, manuals
 - Confirm priorities among our services and tasks
 - Announce changes in services to our constituency
 - Change our working location
 - more safer place
- Policy changes on Information Management
 - Transfer the authority to permit taking out information, to each shift leaders
 - Revise the members' contacts list
 - Give priority to members' connectivity
 - Private info added(private address, private phone number etc)

Incidents directly related to the disaster and what was done as a CSIRT to solve such issues(1/3) – NTT-CERT

Hoaxes and rumors

- Information obtained through our public monitoring made possible to warn and send an early alert to our customers against hoaxes and rumors related to our services.
- After the earthquake, we found some rumors fueling the fear.
- There can be cases, someone abusing rumors that can harm our customers. Sharing information about live rumors made group companies to announce early alerts against such rumors.



Incidents directly related to the disaster and what was done as a CSIRT to solve such issues(2/3) – NTT-CERT

Miss announcement corrections

- Found errors in the contents listed on the homepages through public monitoring, and achieved a rapid correction.
- At the earthquake damaged region, we've set many Emergency Phones, and listed at our web site. In the list some addresses were written wrong. And this data was also used as source data for the other data retrieval services
- This address information being incorrect created a potential situation where people who needed to use the emergency phones can't use them. This error was found quickly and the information corrected.

Incidents directly related to the disaster and what was done as a CSIRT to solve such issues(3/3) – NTT-CERT

Critical support for disaster

- Found the case that some people couldn't make safety confirmation phone call, lead early advising announcement to our customer.
- Mobile phone can configure to reject phone call from public telephone (many people configured like this to shutout prank call). We noticed through public monitoring that many people having hard time to confirm each others safety.
- Could announce about mobile phone receiving configuration, and this prevent a situation that people take a lot of time to confirm each others safety. This error was found quickly and the information corrected.

What kind of disaster recovery efforts did your company partake? Is there anything that was done as a CSIRT? – IJ-SECT (1/4)

● As an ISP company

- Free offering of PaaS and SaaS cloud service for organizations who publish information necessary to people in the struck areas
- Launched mirror web sites of local govts, etc.
- Offered mobile devices and PCs
- etc.

What kind of disaster recovery efforts did your company partake? Is there anything that was done as a CSIRT? – IIJ-SECT (2/4)

● As a CSIRT

- On the day of the disaster, we were put out of the loop, with low priority (if any!)
- From the following day, started our regular CSIRT business
- Took precautions against disaster related incidents

What kind of disaster recovery efforts did your company partake? Is there anything that was done as a CSIRT? – IJ-SECT (3/4)

● As a CSIRT

- Answered inquiries from Microsoft, etc.
 - Sincere thanks to Microsoft for having postponed the release of IE9 Japanese version, and to Cisco for having deferred the release of March IOS Security Advisory bundle

What kind of disaster recovery efforts did your company partake? Is there anything that was done as a CSIRT? – IIJ-SECT (4/4)

● As a CSIRT

- “Stop using PDF and Excel just for plain texts and numbers!” movement
 - Waste of bandwidth and CPU load
 - Not readable on cellphones of evacuees
 - E.g., “Power Usage Graph” by Tokyo Electric Power Company (TEPCO)
 - GIF file only -> CSV file added

- The damage in the struck areas was of course severe, and Tokyo area was also affected
 - Blackout & Rolling Blackout
 - Physical distribution networks affected
 - “buy-up”s
 - Gasoline thefts
 - Unbelievably many cases were reported also in Tokyo;
40 cases within 2 weeks!

- As an ISP company
 - IX traffic dropped
 - Customer's devices remained down for a long time while IIJ service was kept up and running
 - Customers were unreachable via phone/FAX
- As a CSIRT
 - Teleworking during the next week
 - Confusions of railroads due to rolling blackout

Incidents directly related to the disaster and what was done as a CSIRT to solve such issues – IIJ-SECT (1/2)

- Gathered information about incidents exploiting the disaster, and took precautions against them
 - SEO poisoning in English (“japan”, “tsunami”, “earthquake”, etc.), soon after the disaster
 - Targeted attack emails in Japanese followed in a few days
 - False rumors, misinformation, chain emails
 - Donation scams

Incidents directly related to the disaster and what was done as a CSIRT to solve such issues – IIJ-SECT (2/2)

- Observed no direct damage within our constituency

19 teams

FIRST
JapanTeams

12 - 17 June 2011



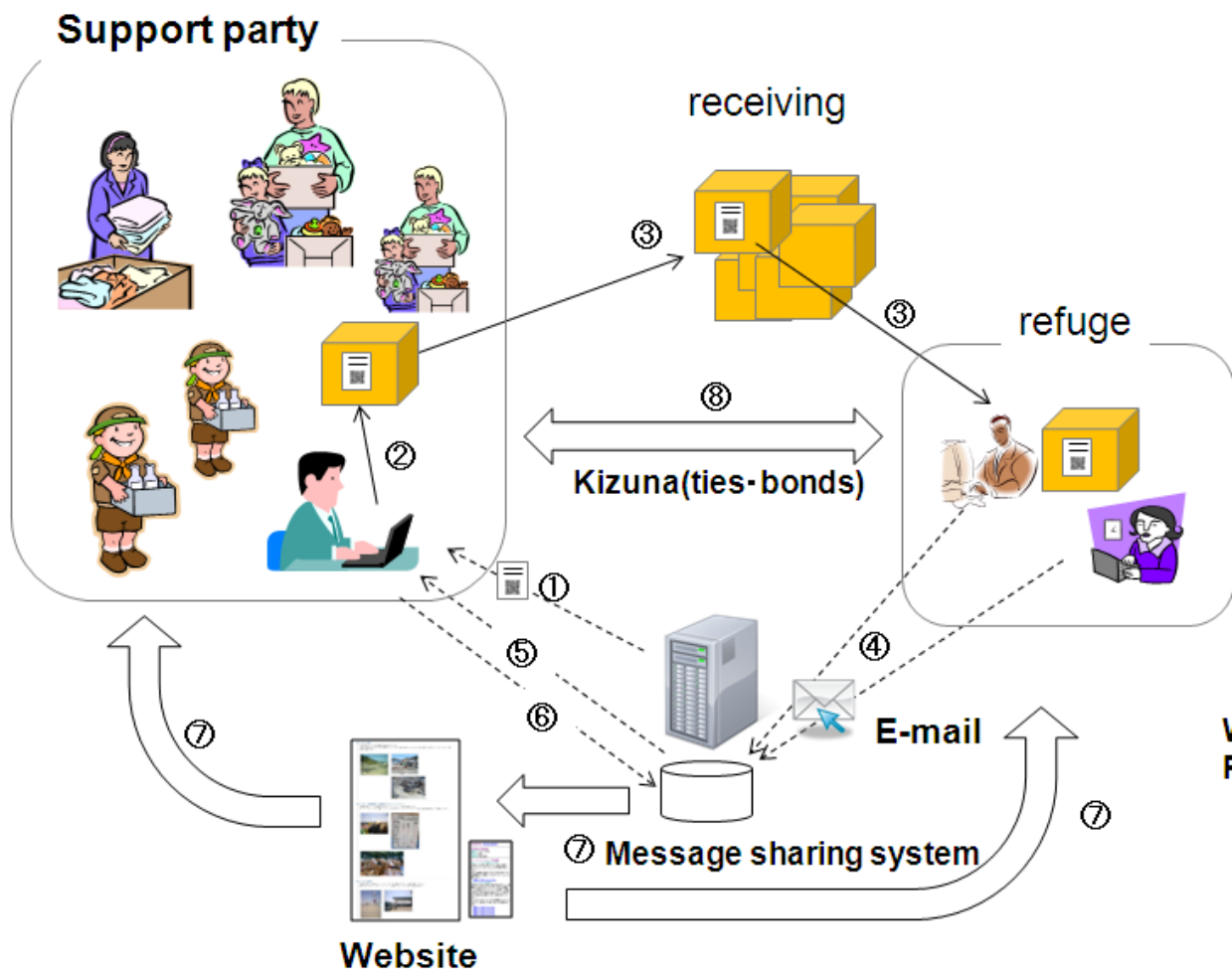
Vienna

What kind of disaster recovery efforts did your company partake? Is there anything that was done as a CSIRT? - NCSIRT

- DataCenter
 - Parent company NRI (Systems Integrator) has some data centers
 - Switch to Private power generation
- On next business day (Monday Morning)
 - Standby for customer's call
- As CSIRT
 - We did as usual (incident monitoring, information gathering)
- Started Feedback system from victims
 - Details in next page...

KIZUNA(ties・bonds)

Feedback system from victims - NCSIRT



Label attached on Box

We provide 「message board」.
Please send a e-mail.

Infrastructure Issues – Electric, Communications etc.

- NCSIRT

- Rolling blackout

- DataCenter Continuation

- switch training is really important
 - enough fuel

- Remote Access

- Confirmation of teleworking rule

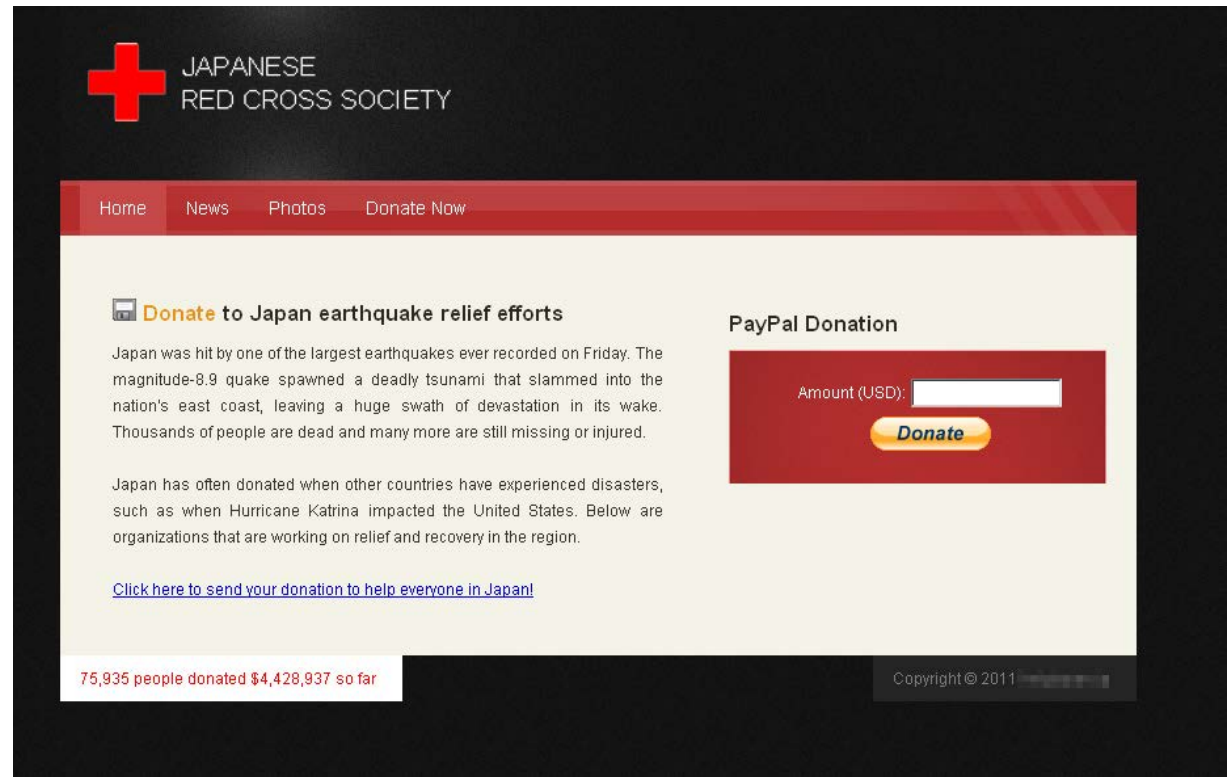
- Telephone call limitation

- Internet phone (Skype etc.) were good
 - Twitter, Facebook worked well



Incidents directly related to the disaster and what was done as a CSIRT to solve such issues - NCSIRT

- Phishing malicious website
- Chain e-mail false rumor of oil plant explosion



What happened after 3.11?

- Rakuten-CERT

- Company ordered employees to stand by at home for more than a week (3.11 – 3.21).
- Some members who needed to run the operation were allowed to work at office.
- As a CERT, actually there was nothing we could do.

Company contribution and efforts

- Rakuten-CERT

● Technical

- Shutdown out-of-operation servers due to power shortage.
- Maintain mailing system (not sending mail magazine to the disaster stricken area).

● CSR

- Donation system
- Empower sufferers with our EC/travel service
- Sharing information through our web service
- Saving power program (reduce 40% YoY)

Discussion Agenda

- Where were you and what you did right after the earthquake?
- What kind of disaster recovery efforts did your company partake? Is there anything that was done as a CSIRT?
- Infrastructure Issues – Electric, Communications etc.
- Incidents directly related to the disaster and what was done as a CSIRT to solve such issues
- Final Thoughts – what should be done in the future?



Final Thoughts – what should be done in the future?

- NTT-CERT

- There are many unexpected security exceptions we had to make
 - outside services which usually banned at our office can be very useful tools.
 - banning is not security
- concern with practices under exceptions for a while
 - status and situations keep changing
- Things we normally don't do, are impossible to do (or very hard to do)
 - Normal Practices to be matured is important, small change of everyday-work
 - worked a lot under emergency
- Situation changes as time goes by, and so does things we can do
 - this time of period was in the phase of repairing infrastructure, therefore not many things CSIRTS could do.
 - (but NTT-CERT was thanked to be in a disaster countermeasures team from other members)
- rotationally shifted work
 - Centralized logs, Work Management with whitebord... useful
- prepare for the worst
 - disaster hitting direct the greater Tokyo area

Final Thoughts – what should be done in the future?

– IIJ-SECT (1/2)

- Network infrastructure should prepare for a LOT of teleworkers
 - Tens of millions of them, perhaps?
 - All the traffic and load of remote desktops, VoIP, video conferences, file transfers, etc.

Final Thoughts – what should be done in the future?

– IIJ-SECT (2/2)

IIJ-SECT was mainly **Type-2** on the 1st day

- 3 types of CSIRT during a natural disaster
 1. All members taken to the recovery team
 - “Bring as many as possible to our recovery team, it’s the top priority!...”
 2. Put out of the loop
 - All the other people are just too busy to hear us...
 3. Continues CSIRT business
 - Great!!!

19 teams

FIRST
JapanTeams

12 - 17 June 2011



Vienna

Final Thoughts – what should be done in the future?

- NCSIRT

- Risk to exceed assumption
- Disaster Reduction
 - Preparation
 - Remote access system
 - Teleworking rule
 - Training
 - Training for switch to DR site, Private power generation
 - Training for remote access
- Similar in the world of the information security

19 teams

FIRST
JapanTeams

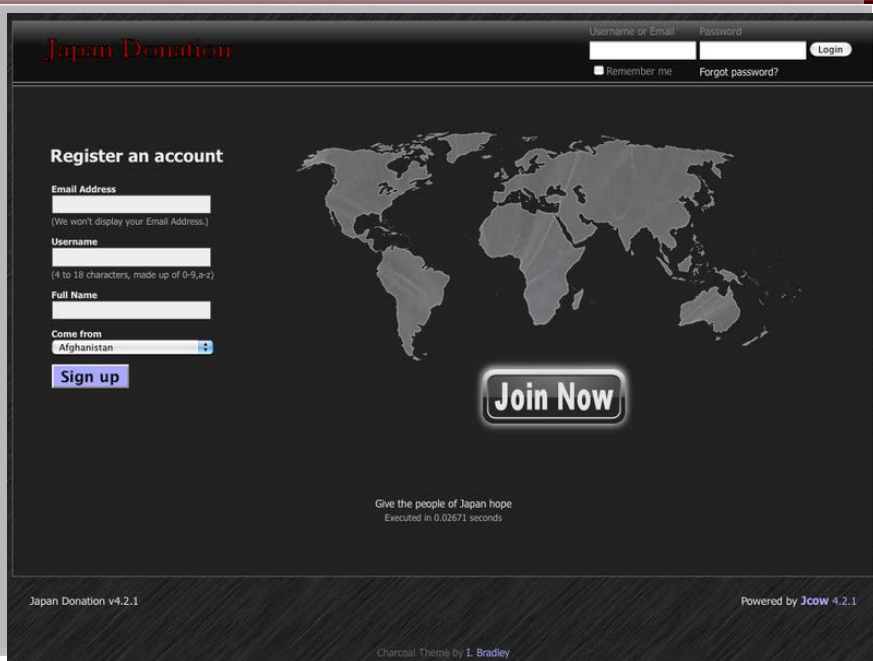
12 - 17 June 2011



Vienna

- Maintain the emergency escalation flow (contact list)
- Remote access environment
- iDC redundancy
- Social Networks (Facebook, Twitter, mixi, etc.) were very helpful for communications confirming safety of others
- Was hard to get through on mobile phones, so webmail such as Gmail were also useful

Must be prepared for anything!



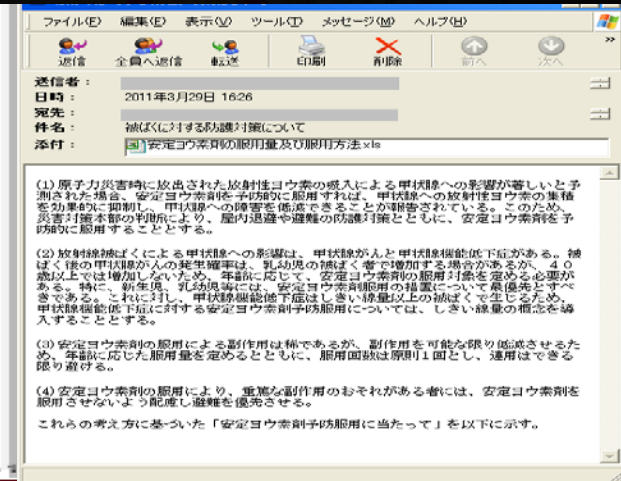
Donation scam site

Announcement of an attack against Tokyo Electric

This was taken down the next day...

Targeted email using fear against radiation

Need to be ready for anything!



Conclusions / Final Thoughts

- Preparation in case of emergency is critical
 - However, must understand that not everything can be prepared for
 - In case of disaster, expect the unexpected, and use previous experiences to get through the unexpected
 - A disaster of this magnitude may occur again, perhaps even bigger
- As CSIRTs, there was not that much that could be done at first
 - Business continuity became top priority
- Social networks were helpful for confirmation of safety
- CSIRT activities critical during emergency times
 - Attacks are always being prepared -> scams, targeted attacks, etc.
 - May have been in trouble if an attack occurred during the first week after the disaster

SPECIAL Panel Session: The day disaster struck the northeastern part of Japan

Special Thanks To:



FIRST Program Committee

And...

23rd

Annual **FIRST** Conference

Hilton Vienna | Austria

12 - 17 June 2011



SPECIAL Panel Session: The day disaster struck the northeastern part of Japan

Organizations

**that provided equipment
and other goods**

**to the areas most affected
by the disaster**

23rd


Annual FIRST Conference

Hilton Vienna | Austria

12 - 17 June 2011



SPECIAL Panel Session: The day disaster struck the northeastern part of Japan



Organizations
that delayed releasing
of scheduled updates
to accommodate system
administrators in Japan

23_{rd}

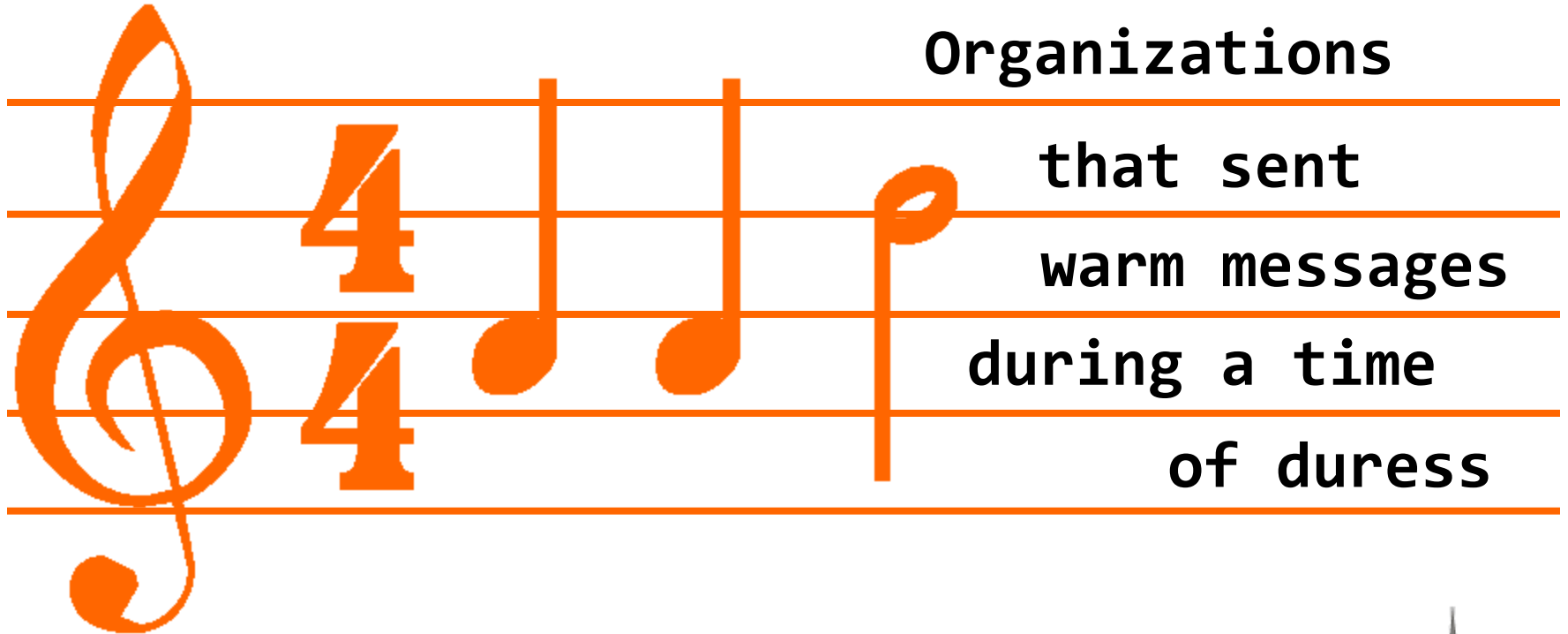
Annual **FIRST** Conference

Hilton Vienna | Austria

12 - 17 June 2011



SPECIAL Panel Session: The day disaster struck the northeastern part of Japan



Organizations

**that sent
warm messages
during a time
of duress**

23_{rd}

Annual FIRST Conference

Hilton Vienna | Austria

12 - 17 June 2011



References

- Images:

http://en.wikipedia.org/wiki/2011_T%C5%8Dhoku_earthquake_and_tsunami

<http://www.tepco.co.jp/index-j.html>

https://www-304.ibm.com/connections/blogs/tokyo-soc/entry/spam_jp_20110331?lang=en_us

<http://www.antiphishing.jp/news/alert/2011314.html>

- Figures

<http://topics.nytimes.com/top/news/international/countriesandterritories/japan/index.html>

<http://www.guardian.co.uk/world/japan-earthquake-and-tsunami>

