

A study for CSIRTs strengthening: From a View point of Interactive Storytelling in an organization

18th June, 2012

NTT-CERT

Meiji Univ.

Meiji Univ.

Meiji Univ.

Okinawa Univ. Toshio TAKAGI

Ikuya HAYASHI

Daisuke SUGIHARA

Miyoko SUZUMURA

Aki NAKANISHI

1. Introduction

2. Approaches

2-1. Various Storytelling in the CSIRT

2-2. Interactive Storytelling in the CSIRT

3. Conclusions

1. Introduction



Basic skills for CSIRT members

in the section “CSIRT STAFFING” from

www.cert.org/csirts/csirt-staffing.html

The set of basic skills we believe CSIRT staff members need to have are described below, separated into two broad groups: *personal skills* and *technical skills*.

personal skills

- Communication
- Presentation Skills
- Ability to Follow Policies and Procedures
- **Team Skills**
- Integrity
- Knowing One's Limits
- **Coping with Stress**
- Problem Solving
- Time Management

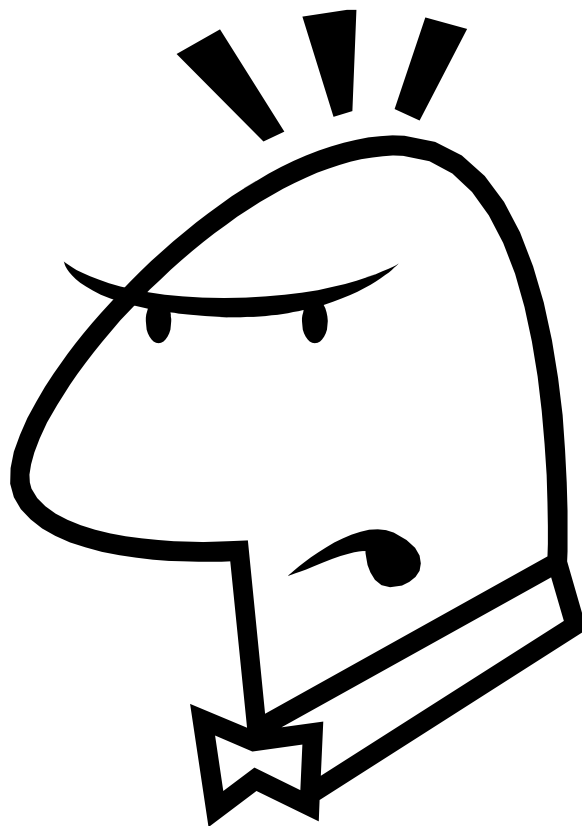
Technical skills

- Technical skills
- Incident Handling Skills

CSIRT staff need to be aware of their responsibilities, contribute to the goals of the team, and **work together** to **share** information, workload, and **experiences**.

they need the ability to **remain calm in tense situations**

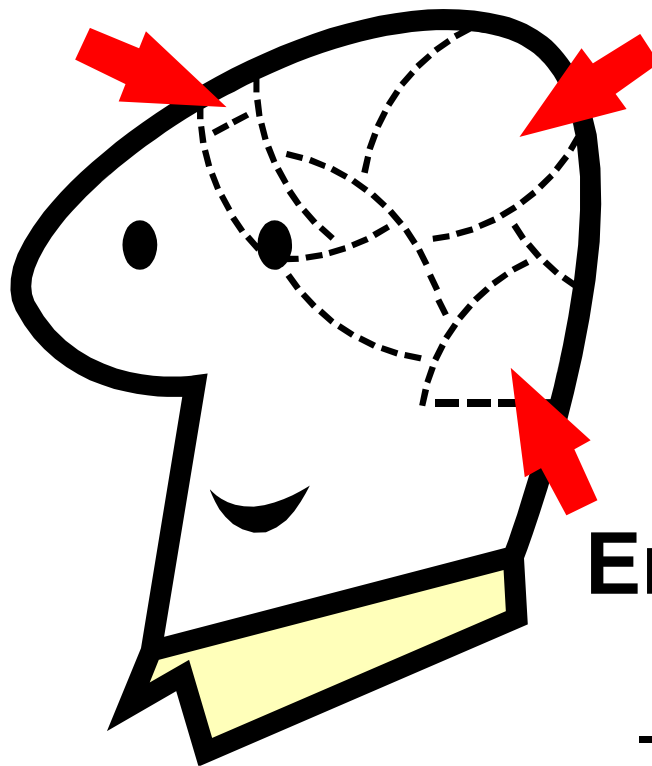
How do you try to get his corporation?



He might be your boss or colleagues.

Logical explanations (= traditional method)

- with Tables
- with Figures



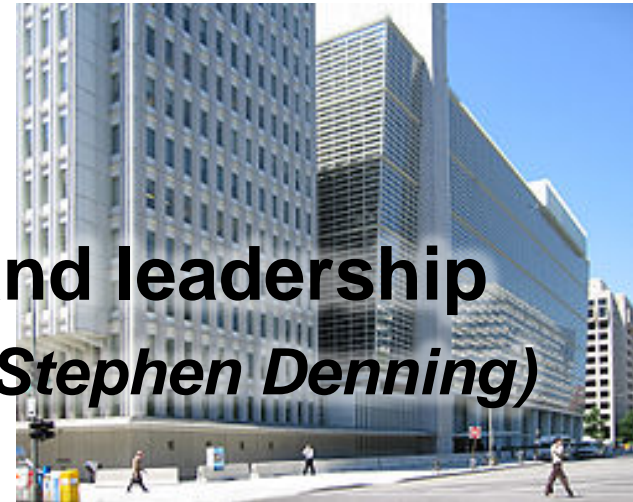
Emotional appeals

- with Stories
- with Facial expressions
- using gestures and intonation

Case1: the World Bank

the organizational change and leadership

Storytelling in Organizations (2004, Stephen Denning)



Case2: the change of a factory

the cost reduction through masses of grabs

Switch (2010, Chip Heath, Dan Heath)

**They can't make any action positively
without their own deep conviction.**



Confirmation bias:

the unconscious tendency to interpret new information in such a way that he/she reconfirms what he/she have already believed.



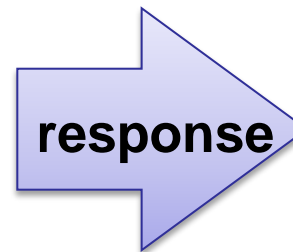
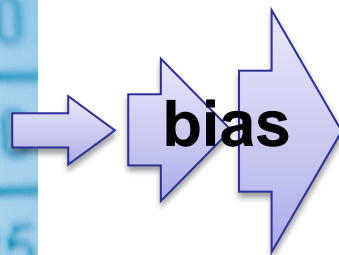
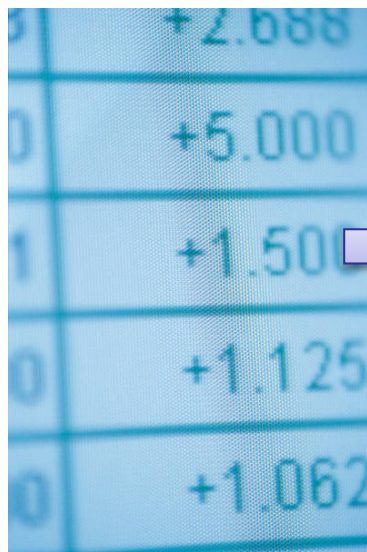
This bias works as a barrier, when they start to do something new.

The example

If she has a positive opinion which global warming is related to carbon dioxide emissions...

<Human's cognition-action flow>

A positive report



Reasonable actions



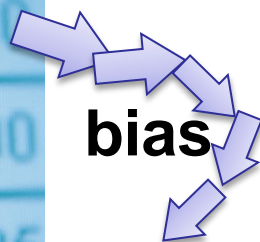
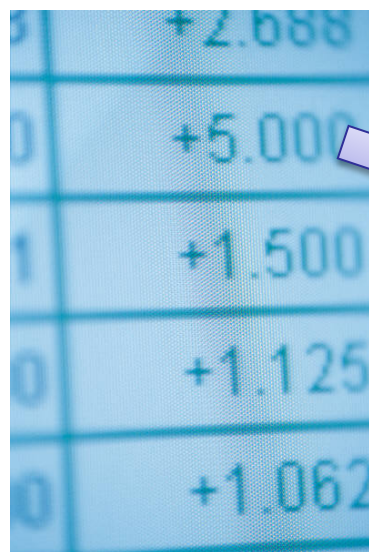
She applies it as the **support** of her idea.
This her **reality has been reinforced**
through the bias.

In the opposite case

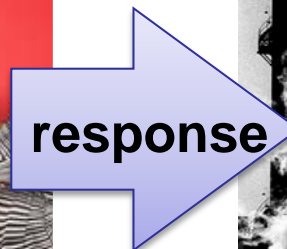
If she has a negative opinion...

<Human's cognition-action flow>

A positive report



bias



response



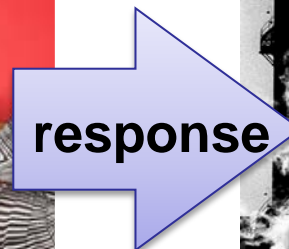
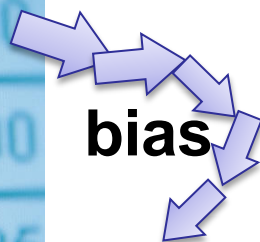
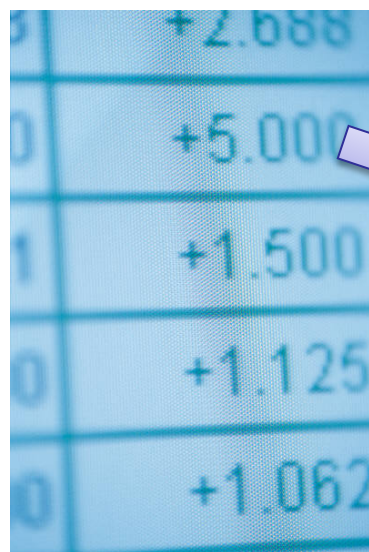
She thinks the report has something **wrong**.
Her **reality has been controlled**
through the bias.

In the opposite case

If she has a negative opinion...

<Human's cognition-action flow>

A positive report



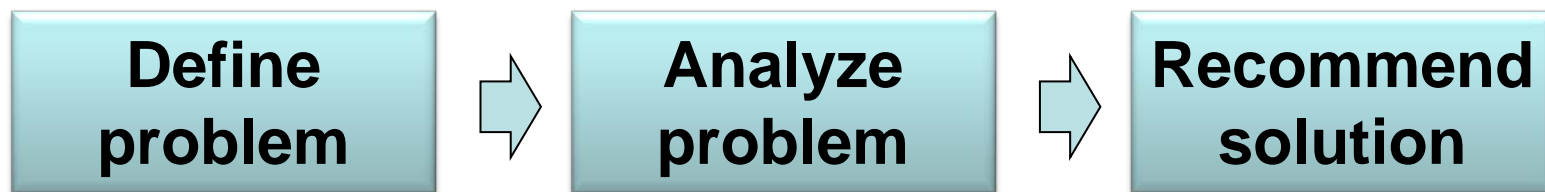
She thinks the report has something **wrong**.
Her **reality has been controlled**
through the bias.

Around 2000, various researchers have studied organizational storytelling from the perspective of leadership development.

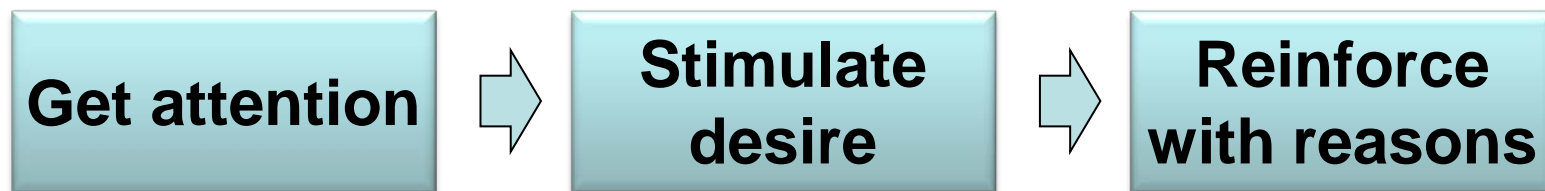
Storytelling is well known to be able to:

- reach his/her heart directly beyond the barrier.**
- change his/her reality by the narrative fashion.**
- eventually build up his/her own motivation and mind.**

The traditional method:

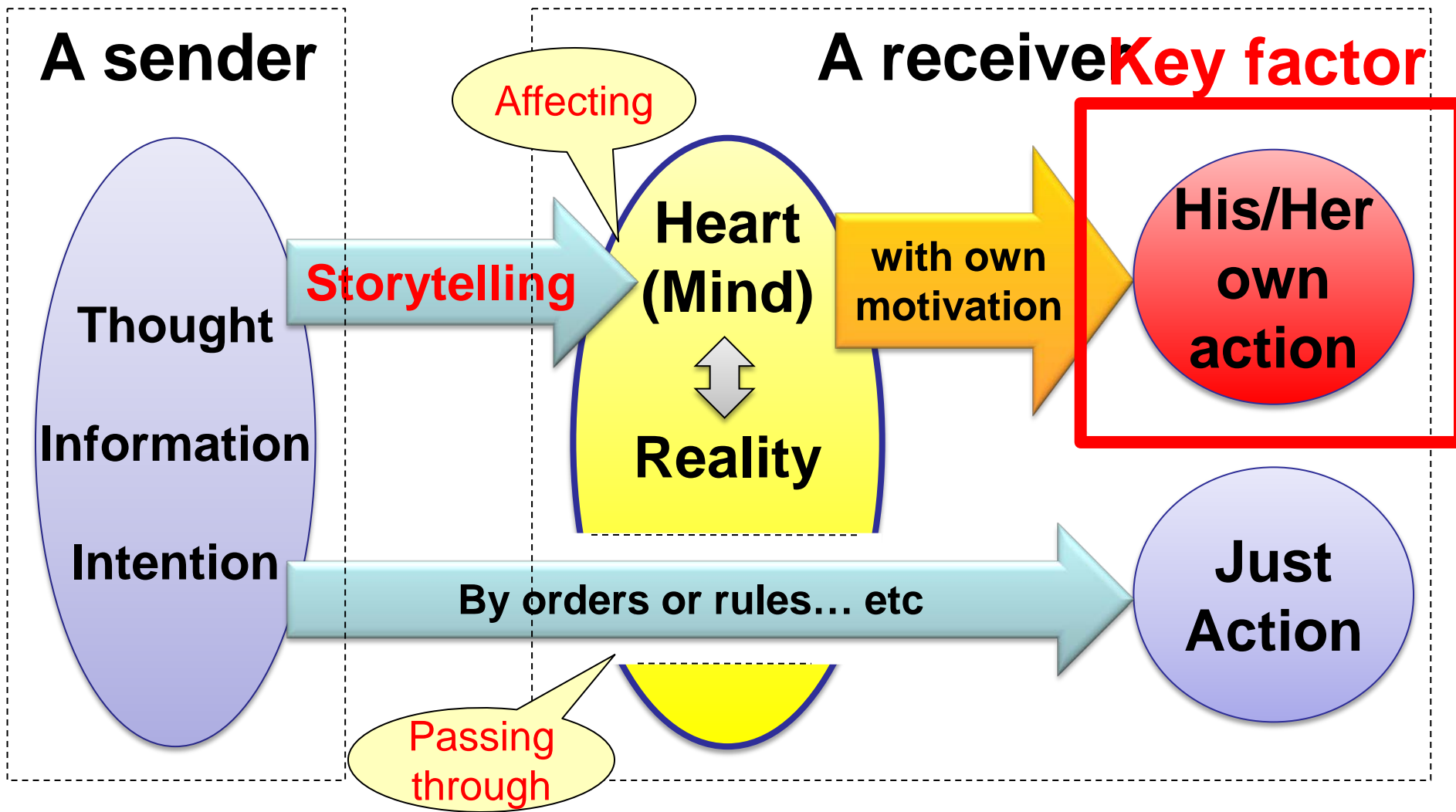


Storytelling:



from *The secret language of Leadership* (Denning, 2011)

The secret of storytelling



Look around you...

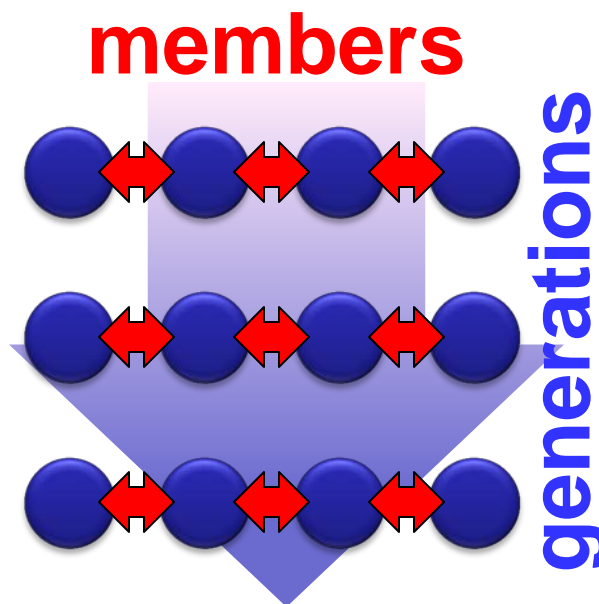
- **Procedure manuals**
- **Rule books**
- **List of contacts**
- **Daily/Monthly reports**
- **Incident reports**

Are they enough?



It is significant to treat something uncovered and unrecognized by the traditional methods.

- **sharing out other members**
- **transferring to successors**



Objectives (For examples)

- *personnel reassignments*
- *No understanding among others, such as your boss and colleagues.*
- *The team culture*
- *The team significance*

A new coming boss might break up a established CSIRT!!
(a real-world example in Japan)

It is significant to treat something uncovered and unrecognized by the traditional methods.

- **sharing out other members**
- **transferring to successors**



Objectives (For example)

- *personnel reassignments*
- *No understanding among others, such as your boss and colleagues.*
- *The team culture*
- *The team significance*

A new coming boss might break up a established CSIRT!!
(a real-world example in Japan)

**Through described actual CSIRT
operation scenes by storytelling,**

**To clarify something not to be described
and analyzed through ordinary
methods.**

And to make it available.

This report will show...

1. Effectiveness of making mutual understanding among members.

- Particularly for newbies. (Education)
- For over different positions. (Communication)
- Understanding to cope with stress.

2. Hints for being a excellent CSIRT.

- Transferring useful sets of **experiences and criteria.**
- Building the team culture and mind.



2. Approaches

2-1. Various Stories in the CSIRT

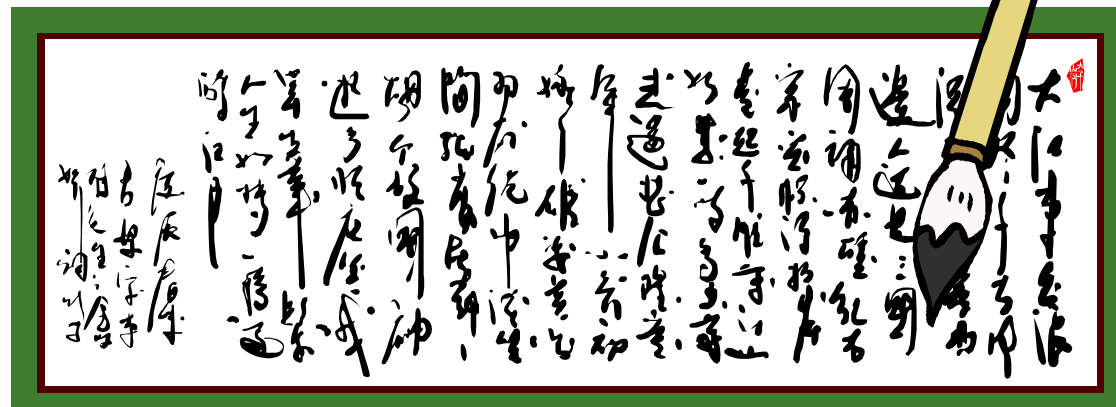


STEP1: Our approach

To make a foothold to analyze something elusive in the operation of CSIRT,

We conducted:

- To interview some members in a CSIRT about a same incident.
- To write some stories by using the storytelling method.



Interview Period:

from November 2009 through February 2010

Interviewees and related persons:

The
Internal
Control
Office

Mr.A :
Another Section
Chief manager
(Predecessor
Of CSIRT Chief Manager)

In this examination



CSIRT
Chief manager

He has just arrived at his post and has no experience of vulnerability management.



CSIRT
Operation Leader

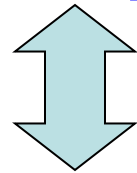
He is engaged in this job for 13 years, so he has rich experiences.

CSIRT
Operator
(New Comer)

3 stories in a case

They were completely different from fact-based documents such as incident reports. Each story includes a continuous process and cues from the **waver realities** on each person.

A set of points



A flux



To examine the stories, we had:

- **read them to other members.**
- **performed the short skit.**

then interviewed

A large, light blue downward-pointing arrow with a black outline, centered on the slide.

Members got

- **understanding each background**
- **understanding each mind**
- **shared criteria**

even over their positions and roles.

A written storytelling brings

- **Vicarious experiences**

to cope with stress against the first case.

to get a set of best practice referable to experiences and criteria.

→ "cosmology episode" (2005, Weick)

- **Sympathy**

to bring a good communication among not only current members but also newbies.

Storytelling is sure to lead to a new type of educational tools and communication tools.

Basic skills for CSIRT members

in the section “CSIRT STAFFING” from

www.cert.org/csirts/csirt-staffing.html

The set of basic skills we believe CSIRT staff members need to have are described below, separated into two broad groups: *personal skills* and *technical skills*.

personal skills

- Communication
- Presentation Skills
- Ability to Follow Policies and Procedures
- **Team Skills**
- Integrity
- Knowing One's Limits
- **Coping with Stress**
- Problem Solving

Technical skills

- Technical skills
- Incident Handling

Sympathy

CSIRT staff need to **be aware of their responsibilities**, contribute to the goals of the team, and **work together to share** information, workload, and **experiences**.

Vicarious experience

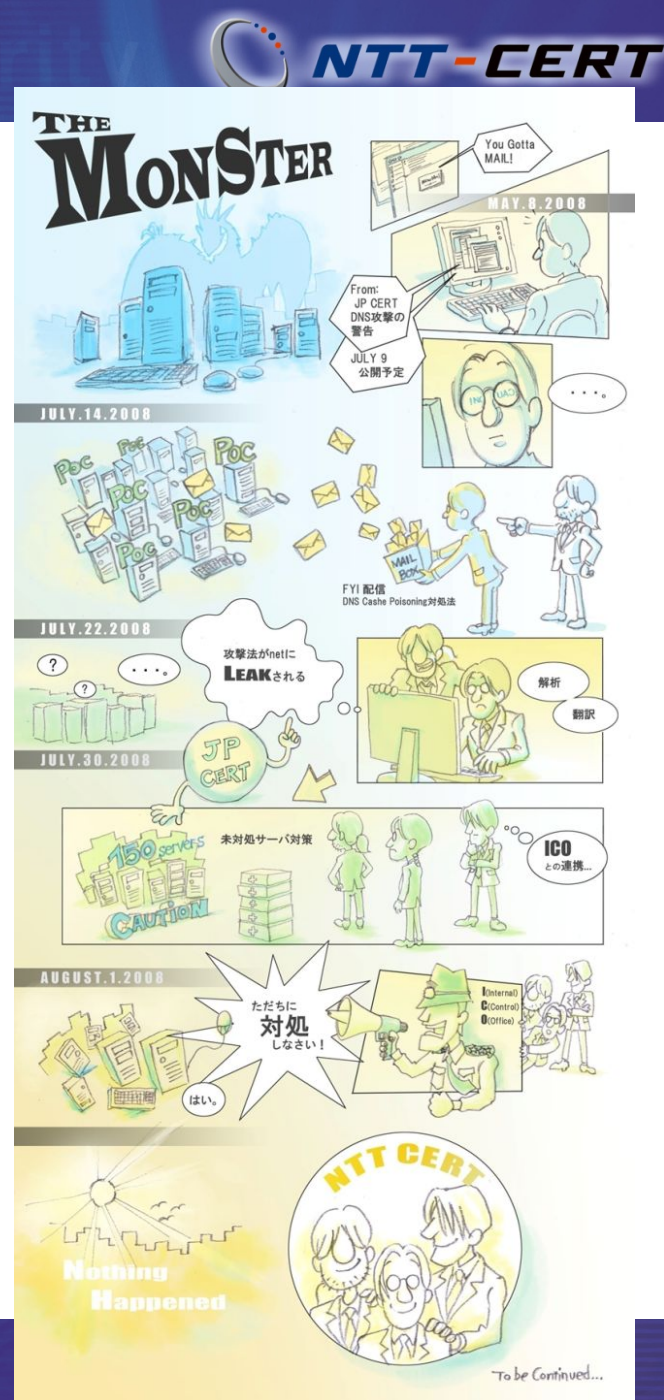
they need the ability to **remain calm in tense situations**

Storytelling in practice

Written stories, however, sometimes require long time to read.

What is the right format?

We also have an idea to use a manga.



2. Approaches

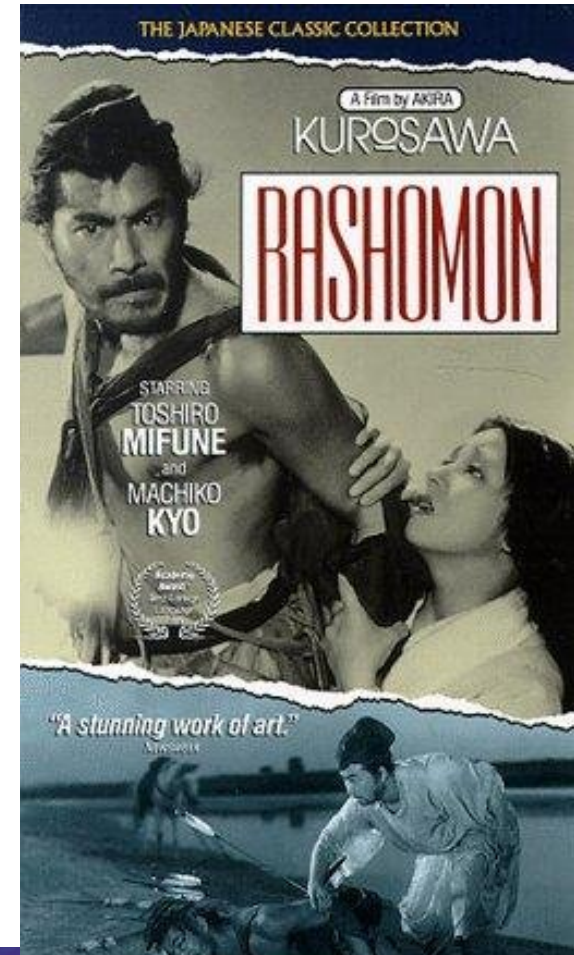
2-2. Interactive Storytelling in the CSIRT



Various different stories pertaining to the same event co-exist and overlap, **“Polyphony.”**

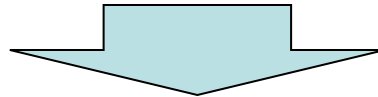
(Bakhtin, 1984)

This is like the movie *Rashomon*, directed by A.Kurosawa.

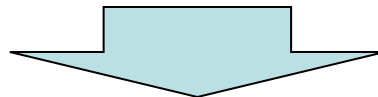


from Internet Movie Database
Home Vision Cinema
(<http://www.imdb.com/>)

Such as Rashomon describes, each person has its own story (reality) individually even through the same event.



Where is the collective mind within the organization? (Kiyomiya, 2008)

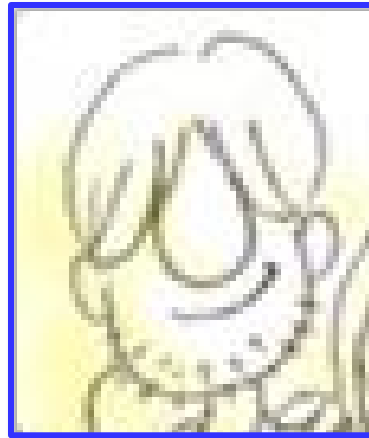


Where is the culture, mind and experiences in the **team (over generations)?**

**We compared the stories to reveal:
how collective minds were generated, and
where collective minds live in the team.**



The background



Difference	operation leader	chief manager
Career (in this team)	For 13 years Rich experiences of vulnerability management	just arrived
Interest (Intention)	Realistic judgment and management with a problem	the total optimization of constituencies from the high viewpoint given by the position

The attack method on DNS servers was discovered by a certain specialist.



This method would be shared with only due limited members (CSIRT), then released into public in about one month. The CSIRT must measure by that time.



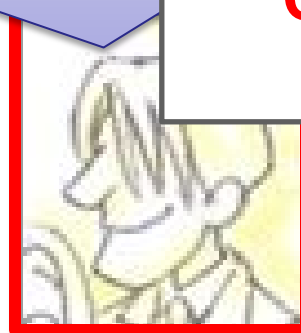
However, The attack method was leaked on a personal blog !! And they had to do something soon.

The background

It became unnecessary to hide this incident, thanks to this leak.

Now, the biggest worry is whether we will be blamed for hiding significant information.

Chief manager's story



Operation leader's story



It was troubled..... Because if media report this, the upper levels of the group will also know about it. And so, the person in charge of each company will be attacked with question, and they will be burdened even further.

The background

One day, the CISRT got information about a lot of vulnerable servers belonging to constituencies. So they wanted to inform the servers' administrators **efficiently**.



However, they didn't have the power and authorities enough to manage the constituencies.



Then, the idea of collaboration with the “**Internal control office**” was born.

The keyword "Internal Control Office" caused conflict with the members

	operation leader	chief manager
About to take collaboration	Negative	Positive
Because...	<ul style="list-style-type: none">• The image of the Internal Control Office is often described as “Police”.⇒ It may be a problem in future, if we were misunderstood as one of them.	<ul style="list-style-type: none">• Improvement in the presence of CSIRT• The interest of the Internal Control Office is also taken into consideration.

Interactive Storytelling

operation leader



Negative

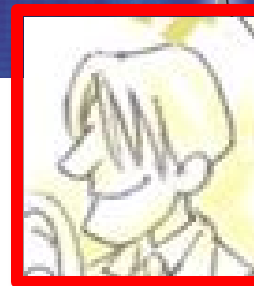
2) If we were misunderstood as relatives of the Internal Control Office. Everybody stops cooperating in CSIRT.

4) But I know all group companies don't take measures under name of us alone. So we want to be more effective.

6) Mmm..It seems almost no problem. (it would become a good experience of collaboration with others.)

Positive

A little conflict between members remained till the last. But, driven away for the purpose of gaining the legitimacy of the act of a team



chief manager

Positive

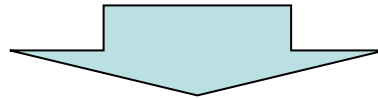
1) It is a chance duly to convey this issue and to increase the presence of CSIRT.

3) The I.C.O. understand their position well . So they can do well and sensitively. Don't worry.

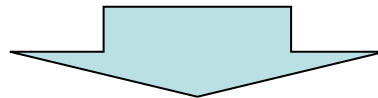
5) Ok. We'll appeal that it is support on the surface to the I.C.O . Actually, We'll involve and ask I.C.O. to direct to take measures.

The converged story = collective mind?

Polyphonic stories were converged into one CSIRT story through interactive storytelling.



After that, the converged story have got a legitimacy in the team(organization), and eventually shall be one of the guidelines(cues of decision) while the members keep talking about it.



Such converged stories might be possible to construct organizational culture and mind.

3. Conclusions



We have showed:

Various stories occurred among CSIRT members, and the **stories influenced each members through sharing events.**

- **Vicarious experiences**
- **Sympathies**

Various stories were converged into one CSIRT story.

- **The converged story **leaded to the team's action.****
- **And a part of them, which includes collective minds and cues of decision, **might be handed down to successors.****

Basic skills for CSIRT members

in the section “CSIRT STAFFING” from

www.cert.org/csirts/csirt-staffing.html

beyond generations

The
to ha
pers

personal skills

- Communicati
- Presentation
- Ability to Fo... es and Procedures
- **Team Skills**
- Integrity
- Knowing...s Limits
- **Coping with Stress**
- Problem Solving

Technical skills

- Technical skill
- Incident Han

Sympathy

CSIRT staff need to **be aware of their responsibilities**, contribute to the goals of the team, and **work together to share information, workload, and experiences.**

Vicarious experience

they need the ability to **remain calm in tense situations**

In this research, we are sure that understanding a “storytelling” can correctly help us to build up and keep on a good team even under high-pressured situations, where CSIRTs are.

If you could find out any secrets through your field with the idea of the storytelling, please let us know!!!

Share secrets, share happiness to all together!!! 😊

Thank you!!!

The conference:

2nd JAMS/JAIMS International Conference on Business & Information 2011
**JAMS(Japan Association for Management System)/JAIMS(Japan-America
Institute of Management Science) International Conference on Business &
Information 2011**

31st August ~2nd September 2011 at JAIMS, Honolulu, Hawaii, USA

The Title:

**Storytelling and Organizational Reality : A Case of the Computer Security
Incident Response Team**

Miyoko Suzumura, Meiji University

Kenichi Terajima, Meiji University

Aki Nakanishi, Meiji University

Toshio Takagi, Okinawa University

**Ikuya Hayashi, Meiji University; NTT Information Sharing Platform
Laboratories**

The conference:

The 11th IAMB Conference in San Francisco, California

**The 11th IAMB(International Academy of Management and Business)
Conference,2011 in San Francisco, California, Nov.7th~9th**

The title:

**Interactive Storytelling in Practice : A Case of the Computer Security
Incident Response Team**

Miyoko Suzumura, Meiji University

Daisuke Sugihara, Meiji University

Aki Nakanishi, Meiji University

Toshio Takagi, Okinawa University

Masayasu Takahashi, Meiji University

**Ikuya Hayashi, Meiji University; NTT Information Sharing Platform
Laboratories**

The conference:

International Conference on Information Systems(ICIS) 2011

JPAIS/JASMIN International Meeting 2011 4th December 2011

The title:

**A Social Life of Security: A story of the computer Security Incident
Response Team**

Miyoko Suzumura, Meiji University

Daisuke Sugihara, Meiji University

Aki Nakanishi, Meiji University

Toshio Takagi, Okinawa University

**Ikuya Hayashi, Meiji University; NTT Information Sharing Platform
Laboratories**