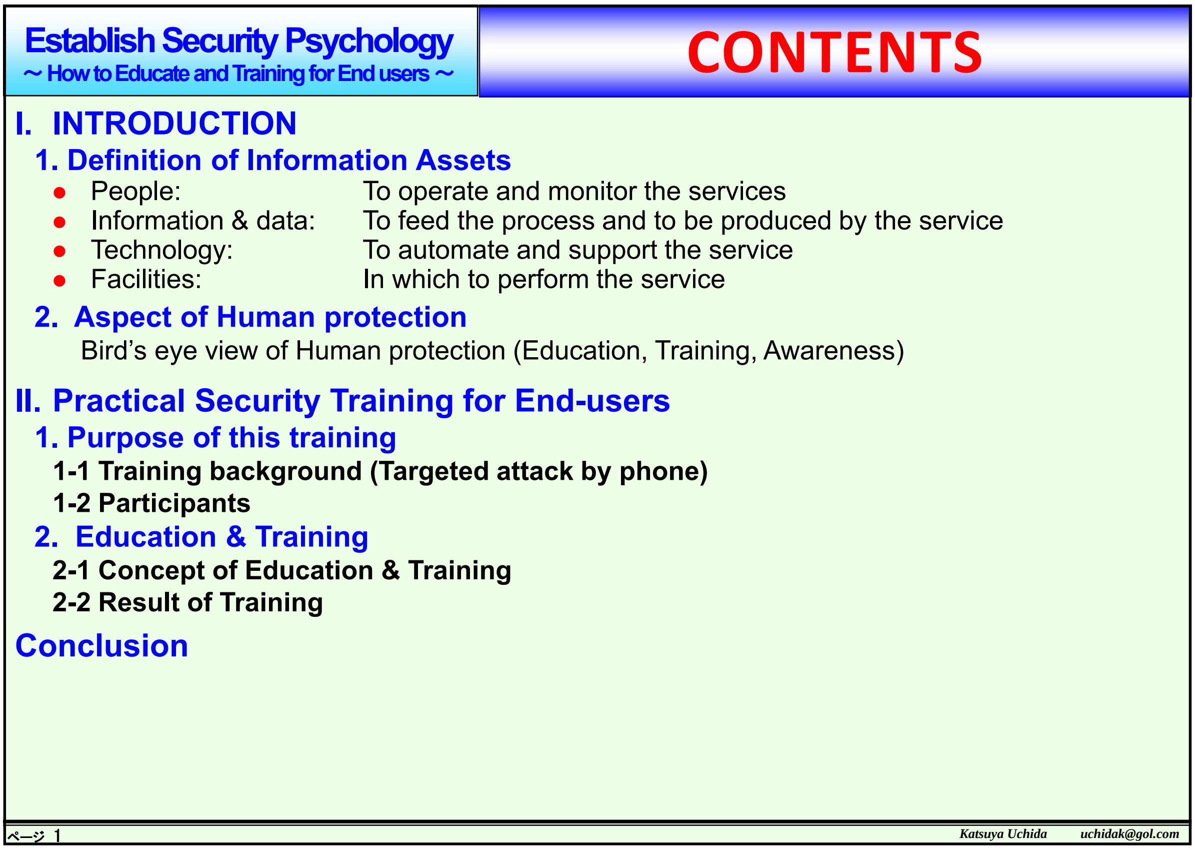
Establish Security Psychology

～ How to Educate and Training for End users ～

July 12, 2017
HCI International 2017

This file is stored in the following web page.
http://www.uchidak.com/Eng/

Katsuya UCHIDA, Ph.D.
（ uchidak@gol.com ）



Establish Security Psychology
～ How to Educate and Training for End users ～

CONTENTS

I. INTRODUCTION

1. Definition of Information Assets

● People:	To operate and monitor the services
● Information & data:	To feed the process and to be produced by the service
● Technology:	To automate and support the service
● Facilities:	In which to perform the service

2. Aspect of Human protection

Bird's eye view of Human protection (Education, Training, Awareness)

II. Practical Security Training for End-users

1. Purpose of this training

1-1 Training background (Targeted attack by phone)

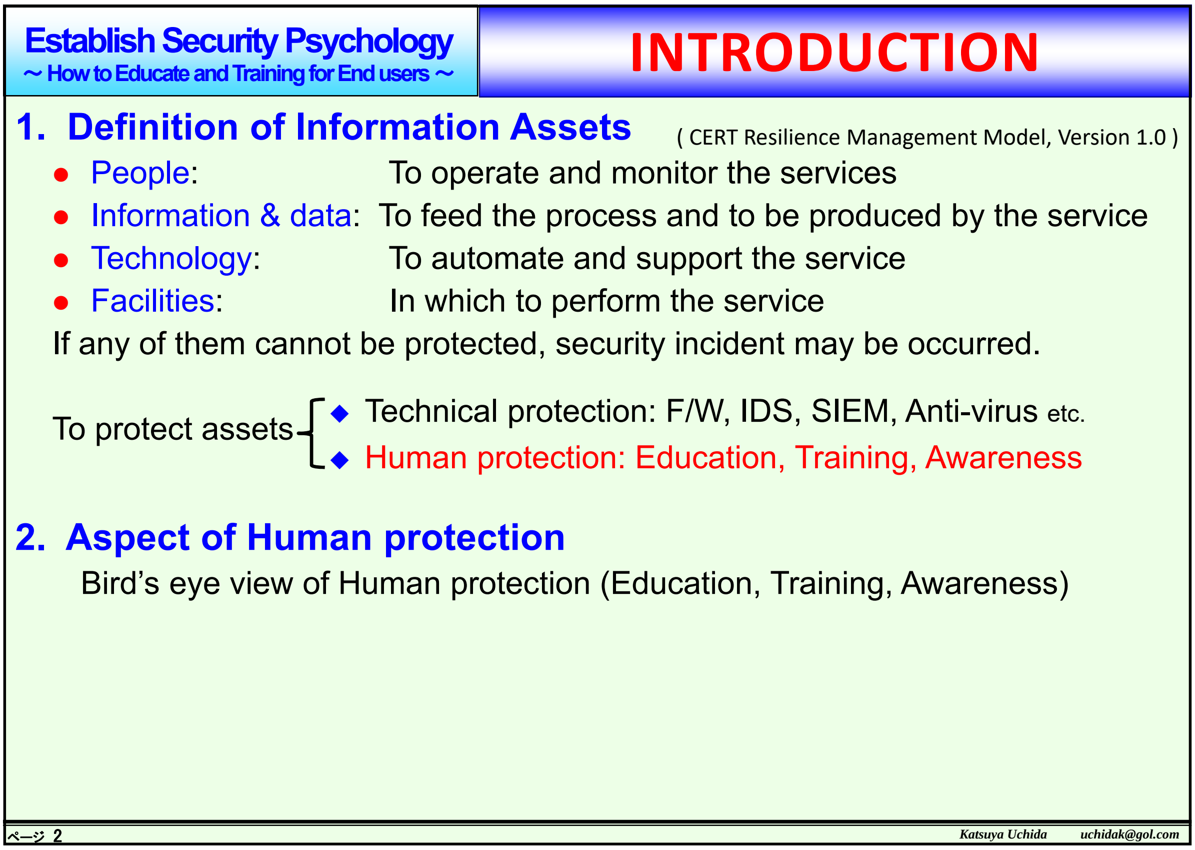
1-2 Participants

2. Education & Training

2-1 Concept of Education & Training

2-2 Result of Training

Conclusion



Establish Security Psychology
~ How to Educate and Training for End users ~

INTRODUCTION

1. Definition of Information Assets

(CERT Resilience Management Model, Version 1.0)

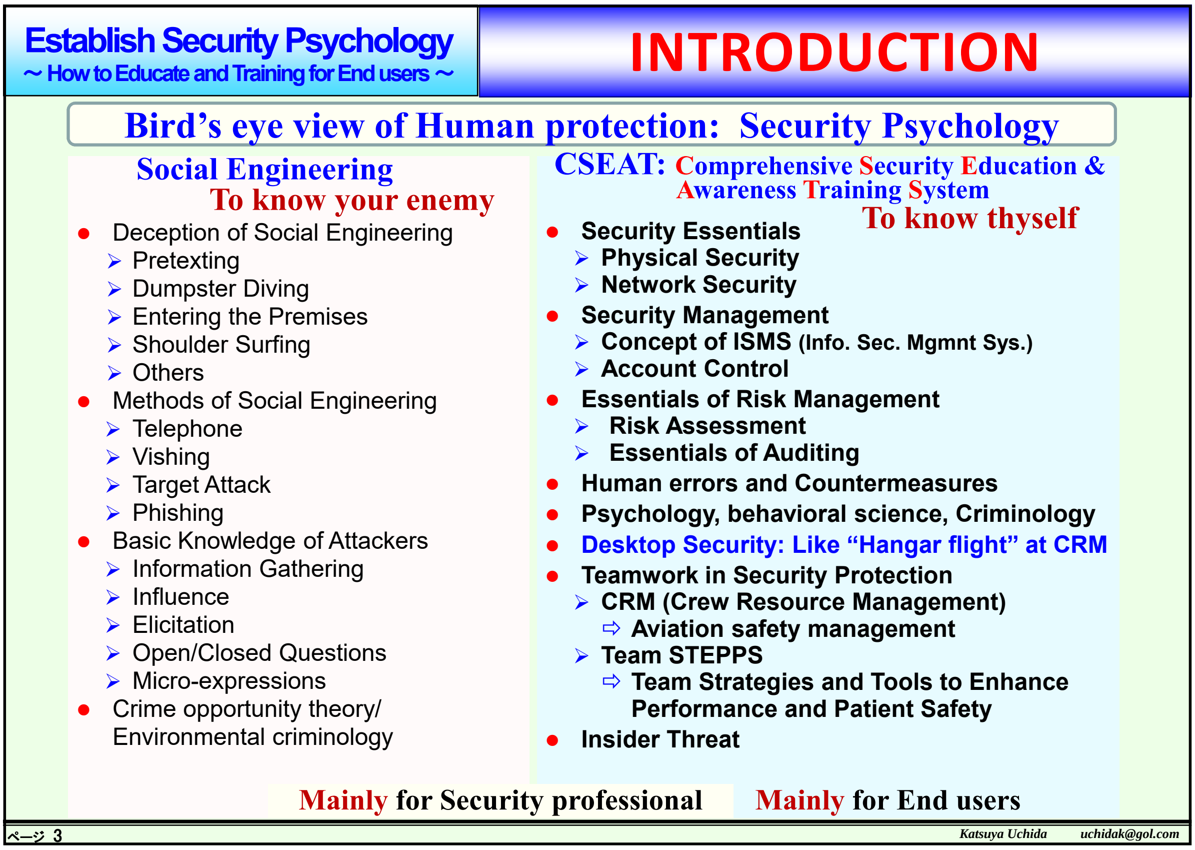
- People: To operate and monitor the services
- Information & data: To feed the process and to be produced by the service
- Technology: To automate and support the service
- Facilities: In which to perform the service

If any of them cannot be protected, security incident may be occurred.

To protect assets
- ◆ Technical protection: F/W, IDS, SIEM, Anti-virus etc.
- ◆ Human protection: Education, Training, Awareness

2. Aspect of Human protection

Bird's eye view of Human protection (Education, Training, Awareness)



Establish Security Psychology
~ How to Educate and Training for End users ~

INTRODUCTION

Bird's eye view of Human protection: Security Psychology

Social Engineering

To know your enemy

- Deception of Social Engineering
  - ➢ Pretexting
  - ➢ Dumpster Diving
  - ➢ Entering the Premises
  - ➢ Shoulder Surfing
  - ➢ Others
- Methods of Social Engineering
  - ➢ Telephone
  - ➢ Vishing
  - ➢ Target Attack
  - ➢ Phishing
- Basic Knowledge of Attackers
  - ➢ Information Gathering
  - ➢ Influence
  - ➢ Elicitation
  - ➢ Open/Closed Questions
  - ➢ Micro-expressions
- Crime opportunity theory/ Environmental criminology

Mainly for Security professional

CSEAT: Comprehensive Security Education & Awareness Training System

To know thyself

- **Security Essentials**
  - ➢ **Physical Security**
  - ➢ **Network Security**
- **Security Management**
  - ➢ **Concept of ISMS (Info. Sec. Mgmnt Sys.)**
  - ➢ **Account Control**
- **Essentials of Risk Management**
  - ➢ **Risk Assessment**
  - ➢ **Essentials of Auditing**
- **Human errors and Countermeasures**
- **Psychology, behavioral science, Criminology**
- **Desktop Security: Like "Hangar flight" at CRM**
- **Teamwork in Security Protection**
  - ➢ **CRM (Crew Resource Management)**
    - ⇨ **Aviation safety management**
  - ➢ **Team STEPPS**
    - ⇨ **Team Strategies and Tools to Enhance Performance and Patient Safety**
- **Insider Threat**

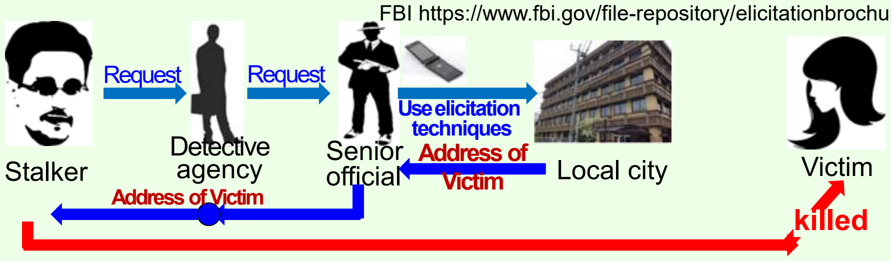
Mainly for End users

1. Purpose of this training

1-1 Training background (Targeted attack by phone)

- Private information about a woman who was stalked and killed by her former boyfriend a year ago is thought to have been leaked by the local government in Japan.
- Senior official of the firm is suspected of obtaining her address from the local government within hours of receiving the request and giving it to the detective agency.
- It seems that the senior official used the elicitation technique which is technique used to discreetly gather information

FBI https://www.fbi.gov/file-repository/elicitationbrochure.pdf/view



1-2 Participants of 3-hour training

- 37 staff of other local government
  ★ Citizen service group ★ Systems dept. etc.

2. Education & Training

2-1 Concept of Education & Training

- Due to the local government request, education and training will be determined 3 hours.
- Shortage of time;
  - ➢ Group work and discussions in subgroups will be replaced by watching a video.
  - ➢ Show typical figures below, teach participants not to make a simple mistake.
    - ◆ Fig. 1: No parking ・・・・・・ Show similar figures & learn the right selection method
    - ◆ Fig. 2: Illusion of Fraser・・・Experience is important
    - ◆ Fig. 3: Muller-Lyer illusion・・Need to confirmation

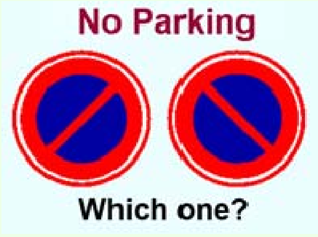


Fig. 1: No Parking Sign

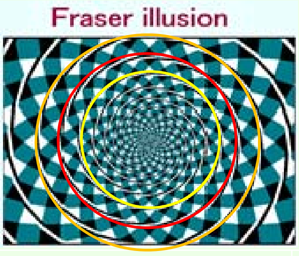


Figure 2: Illusion of Fraser

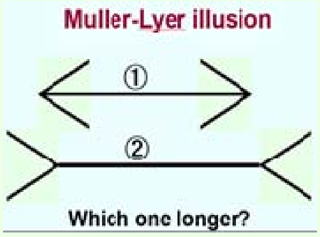


Figure 3: Mueller-Leier illusion

2. Education & Training

2-1 Concept of Education & Training

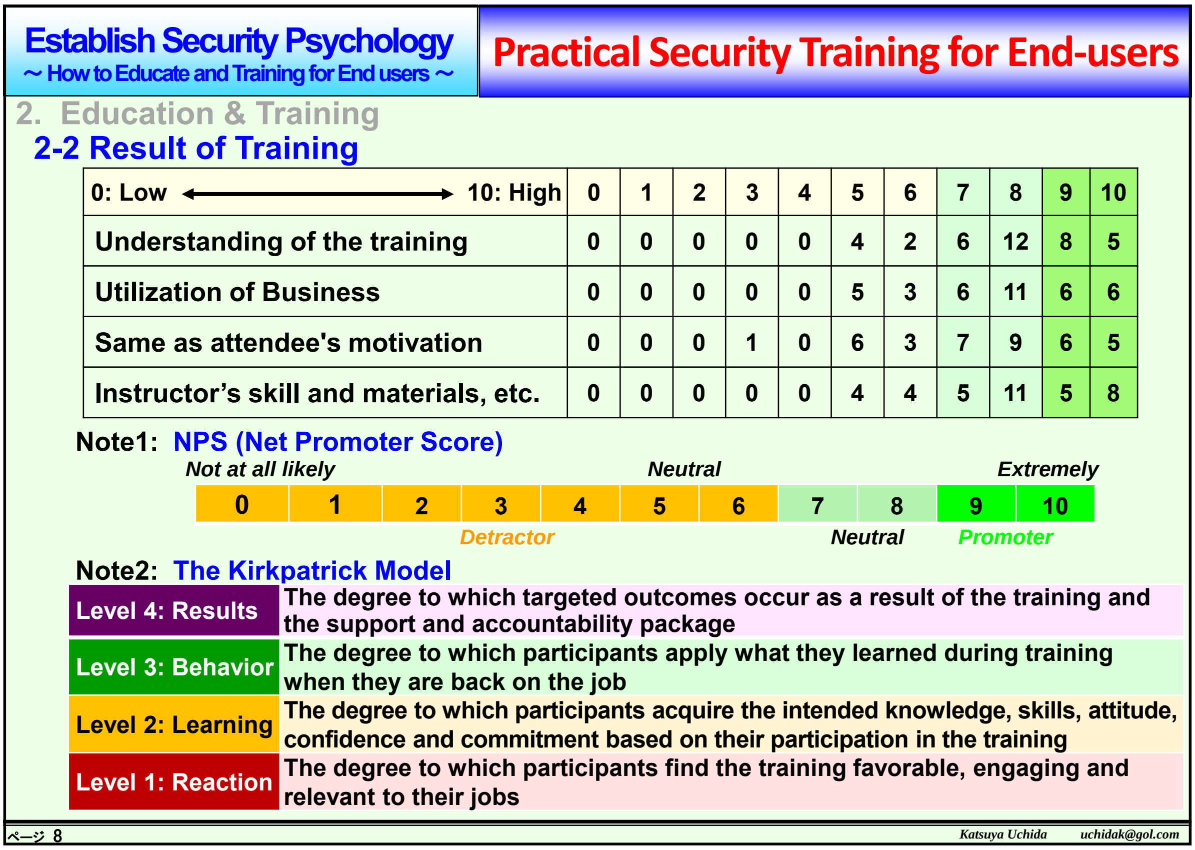
- Related topics of the Incident
  - Details of information leaks from the local government are not disclosed. Since the training is for local government staff, the contents of the incident were described briefly.
  - The information security issues of the local government, especially the security management was explained
- Elicitation Techniques (One of the most important social engineering)
  - This Elicitation techniques seemed to be used at this incident and were explained in detail. FBI: https://www.fbi.gov/file-repository/elicitation-brochure.pdf
- Teamwork training
  - Overview of human error & Countermeasures in other fields:
    - Aviation: CRM (Crew Resource Management)
    - Medical: Team STEPPS (Team Strategies and Tools to Enhance Performance and Patient Safety)
  - Human Error: an organization problem, not an individual problem.
  - Inattentional Blindness: a psychological lack of attention that is not associated with any vision defects or deficits.
    Use the invisible gorilla's video to make participants understand the meaning of inattentiveness blindness.

2. Education & Training

2-2 Result of Training

- Training Satisfaction
  - Very useful………………………… 57% (21 people)
  - Somewhat helpful………………… 43% (16 people)
  - Not very useful /Not useful at all: 0%
- Some comments for training
  - How to deal with the importance of organizational strength and organization?
  - It was an opportunity to think about the problem of the current information informing method
  - I reaffirmed the importance of business analysis
  - It was a good opportunity to reaffirm the stalker incident
  - It was a good opportunity to think human error from many points
  - I got the mental attitude to protect personal information
  - The way of thinking, the checking method etc were helpful
  - The point of view of thinking about creating a structure according to workers was helpful
- Would you recommend this training to others?

1 : Low	2	3	4	5	6 : High	No Answer
1 (3%) 35 (95%)	1 (3%) 34 (92%)	3 (8%) 33 (89%)	7 (19%) 30 (81%)	16 (43%) 23 (62%)	7 (19%) 7 (19%)	2 (5%) (cumulative)



Practical Security Training for End-users

2. Education & Training

2-2 Result of Training

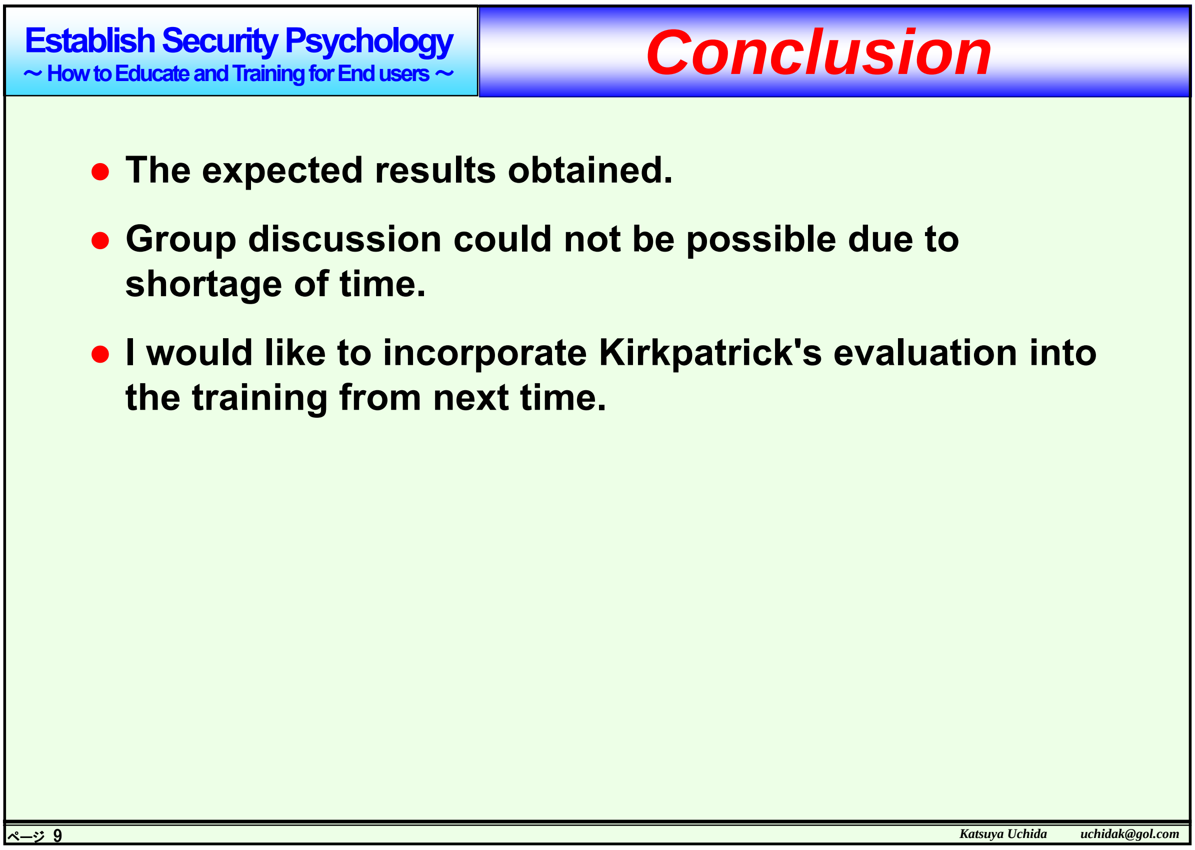
0: Low ⟷ 10: High	0	1	2	3	4	5	6	7	8	9	10
Understanding of the training	0	0	0	0	0	4	2	6	12	8	5
Utilization of Business	0	0	0	0	0	5	3	6	11	6	6
Same as attendee's motivation	0	0	0	1	0	6	3	7	9	6	5
Instructor’s skill and materials, etc.	0	0	0	0	0	4	4	5	11	5	8

Note1: NPS (Net Promoter Score)

Not at all likely					*Neutral*					*Extremely*
0	1	2	3	4	5	6	7	8	9	10
			Detractor					*Neutral*	*Promoter*	

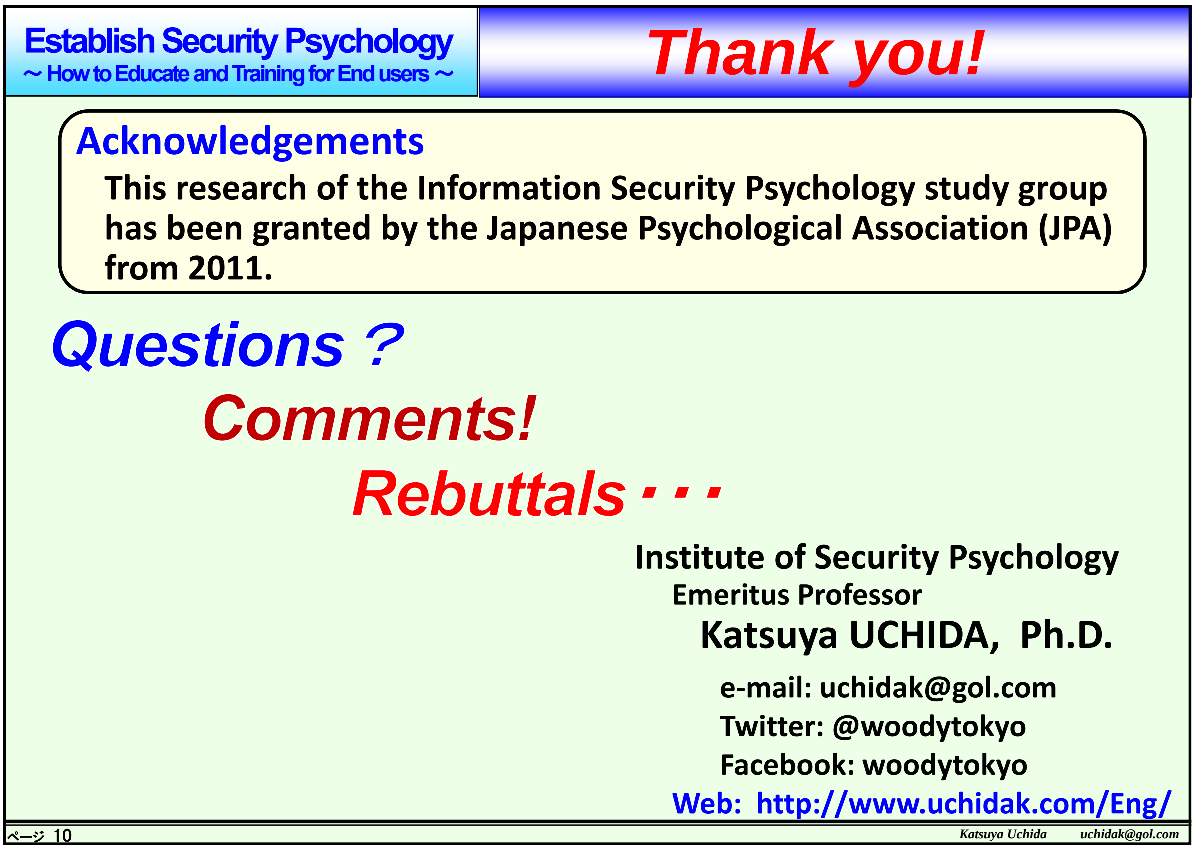
Note2: The Kirkpatrick Model

Level 4: Results	The degree to which targeted outcomes occur as a result of the training and the support and accountability package
Level 3: Behavior	The degree to which participants apply what they learned during training when they are back on the job
Level 2: Learning	The degree to which participants acquire the intended knowledge, skills, attitude, confidence and commitment based on their participation in the training
Level 1: Reaction	The degree to which participants find the training favorable, engaging and relevant to their jobs



Conclusion

- The expected results obtained.
- Group discussion could not be possible due to shortage of time.
- I would like to incorporate Kirkpatrick's evaluation into the training from next time.



Thank you!

Acknowledgements

This research of the Information Security Psychology study group has been granted by the Japanese Psychological Association (JPA) from 2011.

Questions ?

Comments!

Rebuttals・・・

Institute of Security Psychology
Emeritus Professor
Katsuya UCHIDA, Ph.D.

e-mail: uchidak@gol.com
Twitter: @woodytokyo
Facebook: woodytokyo
Web: http://www.uchidak.com/Eng/