

Incident Losses Investigation Report 2nd edition

IDIR Incident Damage Investigation Report 2nd edition

JNSA

Incident Damage Investigation WG

Ver1.00

Table of Contents

Table of Contents.....	2
Executive Summary	3
I Introduction	4
II Incident Overview.....	5
1. What is an incident?.....	5
2. Incident response flow	6
(1) Initial response and investigation	7
(2) External response (outward-looking response)	7
(3) Recovery and prevention of recurrence (inward-looking response)	7
3. Damages incurred in the event of an incident	8
~The round-table discussion “Incident Response Vendors”~	9
III Incident response and its costs.....	13
1. Cost loss (Accident response loss).....	13
(1) Initial response and investigation	13
Security Column① “What I Think About Incident Debriefing”	17
(2) External response (outward-looking response)	19
(3) Recovery and prevention of recurrence (inward-looking response)	30
Security Column② “At The Scene of Recurrence Prevention Measure”	45
Security Column③ “What I Think as CSIRT staff”	47
2. Compensation loss	49
Security Column④ “Importance of Risk Communication”	55
~The round tabel discussion “Lawyers”~	57
3. Profit Loss.....	61
Security Column⑤ “A story about a SME that went bankrupt due to ransomware damage.”	62
Security Column⑥ “Cyber Insurance”	64
4. Financial Loss	67
5. Administrative loss.....	76
6. Intangible loss.....	78
~ The round table discussion “The Media”~	81
IV Model case (fiction).....	84
1. Support scams.....	84
2. Minor malware infection (Emotet)	85
3. Leakage of Credit Card Information, etc. from EC Site	86
4. Ransomware infection.....	88
V Final Thoughts	90
VI Glossary	93
VII References.....	96
Revision History.....	100