

Appendix 1 Reporting Items and Format for Information Security Incidents

(1) Reporting items

Reporting items	Registration Rule 9.2 (Urgent)	Registration Rule 9.3 (Confirmed)
Name of cloud service provider	<input type="radio"/>	<input type="radio"/> (Form 7)
Name of registered cloud service	<input type="radio"/>	<input type="radio"/> (Form 7)
Cloud service (region) targeted by incident	<input type="radio"/>	<input type="radio"/>
Point of time for reporting (number of reports)	<input type="radio"/>	
Date and time of recognizing the occurrence of an incident	<input type="radio"/>	
Matter that occurred	<input type="radio"/>	
Scope of impact	<input type="radio"/>	
Cause of incident (overview)	<input type="radio"/>	
Incident occurrence, recognition, response status (progress of recovery work, etc.), date and time of recovery (scheduled)	<input type="radio"/>	
Date and time of incident occurrence		<input type="radio"/>
Date and time of recovery		<input type="radio"/>
Overview of incident		<input type="radio"/>
Overview of service causing the incident		<input type="radio"/>
Incident occurrence status		<input type="radio"/>
Incident response status		<input type="radio"/>
Cause of incident (details)		<input type="radio"/>
Impact on government agencies and details on impact (if unable to answer, state reason why)		<input type="radio"/>
Measures to prevent recurrence		<input type="radio"/>

(2) Reporting format

Registration Rules 9.2 (Urgent)

As long as the reporting items are satisfied, any reporting format may be used. Reports in English are also acceptable; however, when necessary, the ISMAP Operations Support Organization may request additional submission of a Japanese translation for reference.

Registration Rules 9.3 (Confirmed)

Report submission shall be based on “Form 7 Information Security Incident Report.” All reports must be in Japanese.