

Matters pointed out by the external committee

1. Analysis of causes for the unauthorized access to project information sharing tool and Fujitsu's delayed response after detection of the incident

The external committee indicated the following causes for the unauthorized access:

- (1) An insufficient information protection system
- (2) Fujitsu's inability to strengthen and manage security due to personnel and budget restrictions on ProjectWEB
- (3) An insufficient system to detect unauthorized access immediately
- (4) Most of the management tasks of each tenant were left to the discretion of the individual tenant manager

In addition, the external committee has pointed out the following reasons for the delay in Fujitsu's response after the discovery of the incident:

- (1) Fujitsu's response was based on the assumption that it was an incident related to an individual project
- (2) It took Fujitsu time to grasp the structure of ProjectWEB as operations were depending on specific individuals and log management was inadequate
- (3) There was little common understanding about the nature of the system of ProjectWEB and it was difficult to anticipate the importance of information that could be damaged and the business impact
- (4) The framework for responding to security incidents did not function effectively
- (5) There was a culture or lack of preparation that hindered a prompt response to security incidents
- (6) Fujitsu's approach towards customers was not appropriate

The external committee further analyzed the causes that led to this situation and pointed out the following:

- (1) ProjectWEB was used for a wider range of environments and purposes than initially expected, and was not handled in accordance with the previously defined property and usage conditions of the system
- (2) Fujitsu's organizational structure tended to be vertically segmented, and, as a

consequence, internal systems were not managed in a company-wide unified or centralized manner

- (3) Information management and security were not given priority due to the convenience of business and a focus on cost reduction
- (4) Fujitsu did not proactively take initiative in responding to the incident

2. Recommendations by the external committee to prevent recurrence

In light of the above summarized findings and the review and implementation status of recurrence prevention measures at Fujitsu, the report of the external committee includes the following recommendations on measures to prevent recurrence:

- (1) Enhancement of security of in-house IT systems
- (2) Establishment of an organization that immediately detects and responds to unauthorized access and vulnerabilities
- (3) Establishment of a centralized management of in-house IT systems and clarification of the positioning of each system
- (4) Company-wide thorough education to create and raise awareness towards security measures
- (5) Enhancement of communication with relevant authorities
- (6) Fostering of a corporate culture in which information management and security are not subordinated to business convenience and cost reduction
- (7) Improvement of internal and external communication at the time incidents occur
- (8) Other matters to be further examined at Fujitsu (improvement of corporate culture, etc.)