Product Security

Various products implement software and provide the ability to connect to networks for convenient usage. This makes it necessary to ensure the security of our products to prevent leaks or alteration of information and to prevent damages that may result from a malicious third-party attempting to cause the product to malfunction.

At Panasonic, we have a specialized department for Corporate-wide product security which develops guidelines to promote security-conscious design, and we ensure the security of our products by streamlining our internal structure and rules, regularly reviewing these so that customers can safely use our products.

Collection and Distribution of Information and Education of Employees

Issues in product security and how to address them change on a daily basis. At Panasonic, we collect the most up to date information on product security by joining various security focused organizations, e.g. FIRST, a forum to share information on security incidents, and attending various global conferences. This information is shared with any relevant divisions and incorporated into training materials for product security to improve the knowledge and awareness of product security throughout the entire organization.

*FIRST: Forum of Incident Response and Security Teams

Promoting Product Security from Development

During the development phase of a product, we consider what assets and functions that need to be protected, as well as any potential attacks against them. Products are developed while minimizing these risks. In addition, security experts perform tests on the product prior to shipment, to ensure that Panasonic products do not contain any “security vulnerabilities” from both a hardware and software standpoint.

Post-shipment Response

When information on a product security issue (vulnerability information, etc.) is obtained, the information will be verified in cooperation with the relevant division. If it is confirmed that a product has a security issue, we provide an update or a countermeasure to ensure the security of the product. Additionally, verification mechanisms will be reviewed to prevent reoccurrence.