# Annex 4: Examples of Risk Sources

| Classification | | Examples | Example of applicable "event that could give rise to consequences (threat)" |
|---|---|---|---|
| Hard | System | Leaving system bugs as they are<br>Equipment not yet being replaced<br>Inadequate maintenance<br>Non-adoption of redundancy | Hardware failure, software failure, network failure |
| | | Inadequate data backup<br>Emergency power facilities not yet being installed | Hardware failure, software failure, network failure, inadequate power, natural disasters |
| | | Inadequate seismic resistance/water resistance measures<br>Backup sites not yet being installed<br>Facilities not yet being replaced | Natural disasters, facility breakdown |
| | Security | Inadequate Denial of service (DoS) countermeasures (devices/settings) | DoS attack |
| | | Systems to detect illegalities not yet being introduced, or the system's inadequateness | Targeted attack, malware, DoS attack, illegal login to web services |
| | | Security cameras not yet being installed | Social engineering |
| | | Unprotected communication routes | Wiretapping/Interference of communications |
| Soft | Vulnerability countermeasures | Corrective programs not yet being applied<br>Leaving known vulnerabilities as they are<br>Continuous use of software after its support is terminated | Information theft, tampering with websites, attacks that target vulnerabilities |
| | Connection environment | Environment that enables connection from USB, external media | Malware, illegal use, illegal taking out (of information) |
| | | Environment that allows access to anyone<br>Environment with connection to external networks<br>Environment with connection to the Internet<br>Links with peripheral systems<br>Environment that enables erroneous operation and intentional operation<br>Environment that enables the receipt of illegal information from external parties | Targeted attack, malware, information theft, DoS attack, tampering with websites, illegal login to web services, tampering with data, system destruction, illegal use, illegal taking out (of information), compromise |
| | | Data stored on or processed through an overseas server | Lack of awareness of regulations/policies |
| | Rules | Granting access rights to people who do not need them<br>Leaving unneeded accounts as they are<br>Inadequate ID management for operators who are allowed to carry out work<br>Ignoring password changes | Targeted attack, information theft, tampering with websites, illegal login to web services, illegal use, illegal taking out (of information), compromise |
| | | Lack of thoroughness in encrypting network communications | Wiretapping/Interference of communications |
| | | Rules related to the authorization of disposal not yet being established, or their lack of thoroughness | Inappropriate disposal |
| | | Inadequate entry/exit management | Illegal use, illegal taking out (of information), social engineering |
| | | Inappropriate storage of equipment and information<br>Lack of thoroughness in personal identification of external vendors<br>Not locking up | Social engineering |
| Skills/Human resources | Common across the organization | Long working hours | Operational errors, neglect of duties |
| | | Inadequate internal security education<br>Absence of security awareness | Illegal use, illegal taking out (of information), operational errors, loss, bringing in of unauthorized equipment, neglect of duties |
| | | Easy and simple password settings<br>Reusing passwords | Illegal login to web services, illegal use of financial information |
| | | Leaving confidential/important documents lying around<br>PC login when absent not yet being set | Social engineering |
| | | Installation of illegal applications<br>Not conducting virus scans during update/maintenance work | Malware, information theft, tampering with websites, attacks that target vulnerabilities |
| | Security department | Omission of verification during maintenance | Malware, system destruction |
| | | Inadequate skills of information security personnel<br>Coding that does not fulfill security requirements | Attacks that target vulnerabilities, tampering with websites, operational errors, unintentional disclosure of information |
| | | Shortage of information security personnel<br>Inadequate security training | Targeted attack, malware, DoS attack, attacks that target vulnerabilities |