Annex 2: Examples of Events That Could Give Rise to Consequences (Threats)

Events that could give rise to consequences (threats)			Example
Threats arising from an attack	External illegalities	Targeted attack	Carrying out an attack using ports, protocols, and services that one does not have access rights to.
			Carrying out an attack using the movement of authorized traffic/data beyond the network boundaries.
			Carrying out an attack that targets and infringes on the personal devices owned by employees in important positions.
			Carrying out a supply chain attack by targeting hardware, software, and/or firmware related to core businesses.
		Malware	Causing a malware infection through an e-mail attachment.
			Causing a malware infection through a website.
			Spreading ransomware using an exploit kit.
		Information theft	Obtaining sensitive information through the malicious use of vulnerabilities that leads to information leakage, such as SQL injection.
			Obtaining sensitive information through the malicious use of software vulnerabilities, such as OS command injection.
			Obtaining sensitive information via network sniffing of external networks.
		Denial of service attacks	Carrying out a simple denial of service (DoS) attack.
			Carrying out a dispersed DoS attack.
			Carrying out a targeted DoS attack.
		Tampering with websites	Tampering with a website through the malicious use of web application vulnerabilities that were incorporated into the application during development.
			Tampering with a website through the malicious use of software vulnerabilities.
			Tampering with a website by breaking into services used for administration.
		Unauthorized login to web services	Carrying out an attack by using combinations of ID and passwords leaked from other websites.
			Carrying out a brute force attack through login attempts or guessing of passwords.
		Attacks targeted at vulnerabilities	Carrying out an attack on unprepared and unprotected users through the malicious use of disclosed vulnerability information.
			Carrying out a non-targeted zero-day attack aimed at vulnerabilities for which corrective measures, such as patches, have not been provided.
			Causing a malware infection through the malicious use of the vulnerabilities of IoT equipment.
		Illegal use of financial information	Stealing information on financial transactions through Internet banking scamming tools.
			Carrying out a phishing scam.
		Interception/Interference of communications	Carrying out a communication interception attack.
			Carrying out a radio interference attack.
			Intercepting wireless network traffic by using interception devices set up externally.
		Tampering with data	Contaminating or tampering with extremely important data.
			Creating, deleting, or changing data on publicly accessible information systems.
			Inserting plausible but fraudulent data into the information systems of the organization.
		Social engineering	Peeping at materials or notes on the desks of other people when they are absent, and collecting confidential information, etc.
			Rummaging through garbage bins and collecting materials or notes that have been carelessly disposed of, to obtain the target information.
			Waiting for an opportunity to steal or search information systems/components.
		System destruction	Illegally installing malware that destroys systems.
	Internal illegalities	Illegal use	Illegally manipulating data.
			Illegally browsing confidential information.
			Illegally acquiring sensitive information.
		Illegal taking out (of information)	Illegally taking out confidential information.
			Intentionally transmit data to external parties.
		Compromise	An internal attacker pretending to be an authorized user, operating web applications and compromising a session.
			An internal attacker breaking into network and carrying out an attack that forcibly changes the settings.
Threats not arising from attacks	Natural phenomenon	Natural disasters	Occurrence of an earthquake.
			Occurrence of a typhoon.
			Occurrence of abnormal temperatures/humidity.
			Occurrence of lightning.
			Occurrence of flooding.
		Shortage of energy	Occurrence of a power outage.
			Occurrence of water shortage.
	Failure	Equipment failure	Occurrence of a fire.
			Occurrence of water leakage.
			Occurrence of plant or animal damage.
			Deterioration of facilities.
			Mulfunction of incidental facilities of buildings (such as air-conditioning equipment, entry/exit management devices, surveillance cameras, etc.)
		Hardware failure	Occurance of failure in memory, disks, CPU, or power devices.
			Occurrence of device error.
			Deterioration of equipment and cables.
		Software failure	Occurrence of abnormalities through potential bugs or overload of OS and applications.
			Decline in processing performance through the depletion of resources (overloading of memory and disks, etc.)
		Network failure	Decline in communications performance through competing communications.
			Failure in lines (dedicated/public), communications operators (connecting stations, ISP, NOC, IDC, etc.), communications equipment, or premises wiring.
	Threats arising from people	Operational errors	Privileged users exposing extremely important information/sensitive information by mistake.
			Privileged users mistakenly granting exceptional rights to other users.
			Sending out e-mails by mistake/Opening unnecessary e-mails/Deleting important data.
		Loss	Misplacing removable media/Loss of media through poor management.
		Inappropriate disposal	Recovering media that has been disposed of.
		Bringing in of unauthorized equipment	Connecting unauthorized equipment, media, and programs to internal networks.
		Unintentional disclosure of information	Leakage of important data through problematic settings on the web server.
		Neglect of duties	Forgetting to perform default operations.
		Lack of awareness of regulations/policies	Exercising authority on an overseas server in which data is stored on or processed through, because of a lack of awareness of regulations/legal requirements of the region in which the server reside.