Cross-ministerial Strategic Innovation Promotion Program (SIP)

Hitachi

3-2 Protection for Critical Infrastructure Companies by Rapidly Distributing Information on a Very Urgent Threat

Social implementation technologies

Rapid distribution of threat information in a standard format which enables machine-processing ; Development of an information sharing system to protect critical infrastructure companies as early as possible

Features

I. Rapid distribution in a standard format

The latest standard format (STIX*1/TAXII*2), which is the international standard specifications for determination by machine, is used for rapid distribution of information received by the system to companies.

II. Related information and severity of threats are shown

For the threat information accumulated by the system, simplified analysis is conducted using the relevancy analysis function and shows related information and severity in an easy-to-view manner.

III. Support for automation of security measures

The measures can be streamlined by outputting threat information by the *YARA*3 rule*, which is the setup format of security devices.

IV. Provisioning of an introduction guide

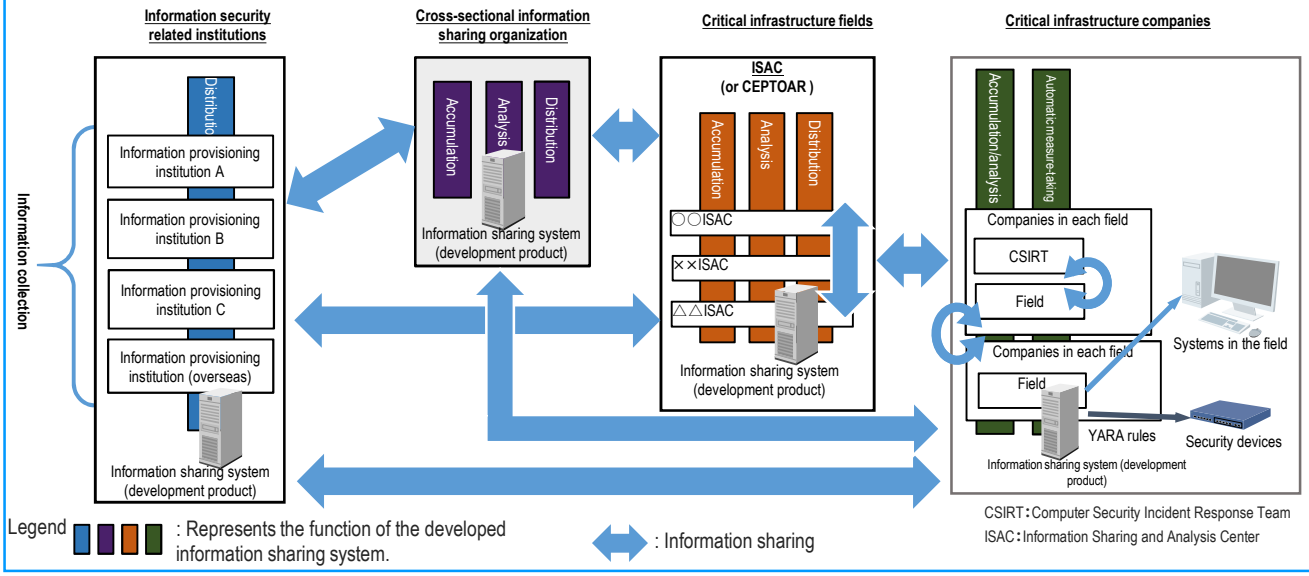
A design guide is provided as a support tool for building an information sharing mechanism based on the actual circumstances of each organization.

Background and Purpose

Issue (i) It takes long time because currently threat information received by email is manually judged and transferred.	(i) Rapid distribution in a standard format, which enables machine judgement, achieves rapid transfer. This enables critical infrastructure companies to take quick actions.
Issue (ii) Information on cyberattacks needs to be collected and made of use for precautions but there is so much information that needs to be manually chosen.	(ii) By knowing the related information and severity of threats, each organization can easily choose the information necessary for themselves.
Issue (iii) Setting measures into security devices is time consuming.	(iii) Automated support for security measures can save time and labor for setting measures into devices.
Issue (iv) There is no idea about how to start information sharing.	(iv) An information sharing mechanism is built according to the design guide, which is a support tool, based on each organization's actual circumstances.

Application Image

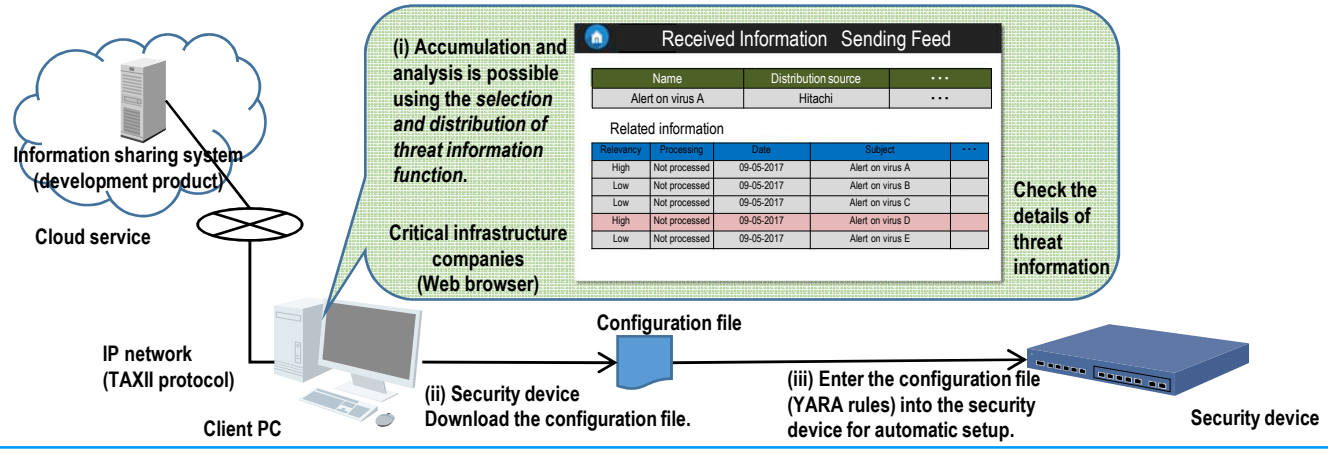
◆ A mechanism for lining an information sharing system is built to speed up the operation from the acquisition and distribution of threat information through to measure implementation.



(*1) The abbreviation of Trusted Automated eXchange of Indicator Information, which is the format specifications for presenting information on cyberattacks.
(*2) The abbreviation of Trusted Automated eXchange of Indicator Information, which is a protocol for sending and receiving information on cyber threats.
(*3) Software for malware analysis and detection used for system security measures, presenting the set of condition formats to be used.

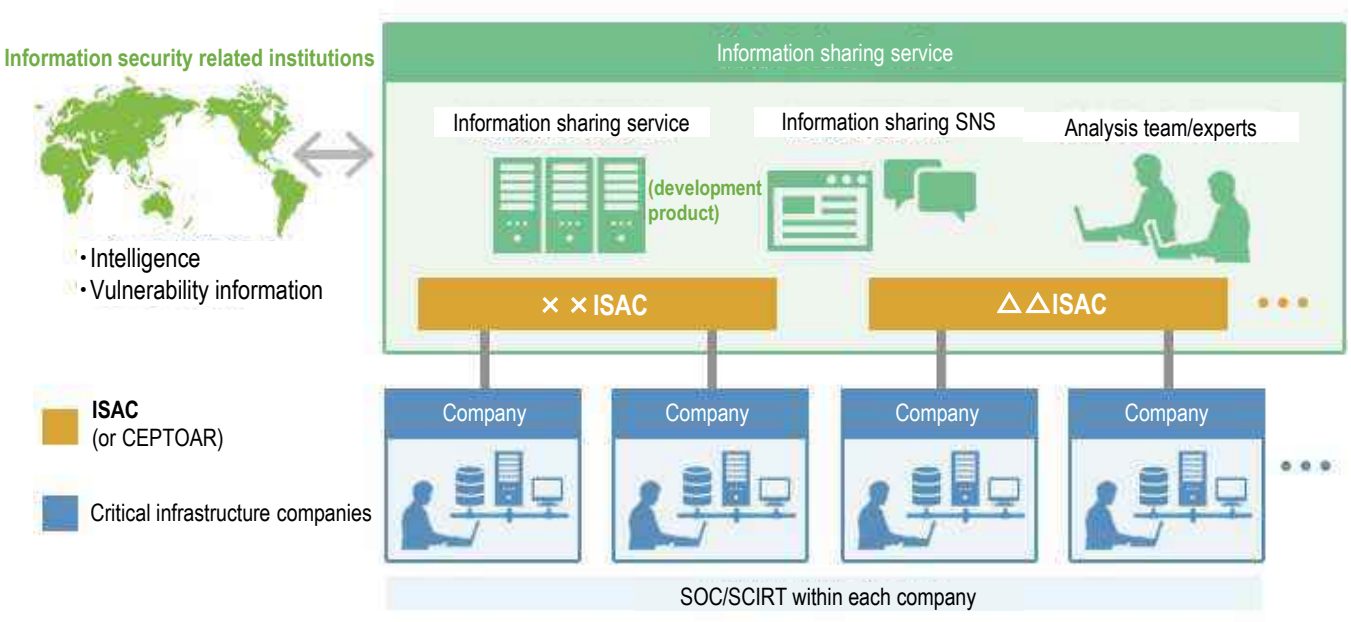
Product Image

◆Use of a cloud environment for multiple users can use the information sharing system from anywhere



Introduction image

◆ Information distributed from domestic and international information security related institutions is collected and accumulated using STIX and TAXII with the information sharing system positioned as the core for the operation, and the severity of the information is ranked. The related information is sorted for intuitive convenience and then provided as a service for grouping.



Schedule

◆An information sharing system was developed in 2017, and it was evaluated and verified by critical infrastructure companies or other institutions. A system incorporating the results of evaluation and verification in 2017 was put into practical application and social implementation in 2018.
◆Full-scale roll out will be carried out from April, 2020.

FY 2017	FY 2018	FY 2019	FY 2020
Evaluation and verification	Development continued	Practical application	Operation of the new function