HITACHI
Inspire the Next

Japanese-Style STIX and TAXII Information Sharing Platform

December 7, 2017
Masato Terada
Hitachi Incident Response Team
Hitachi Ltd.

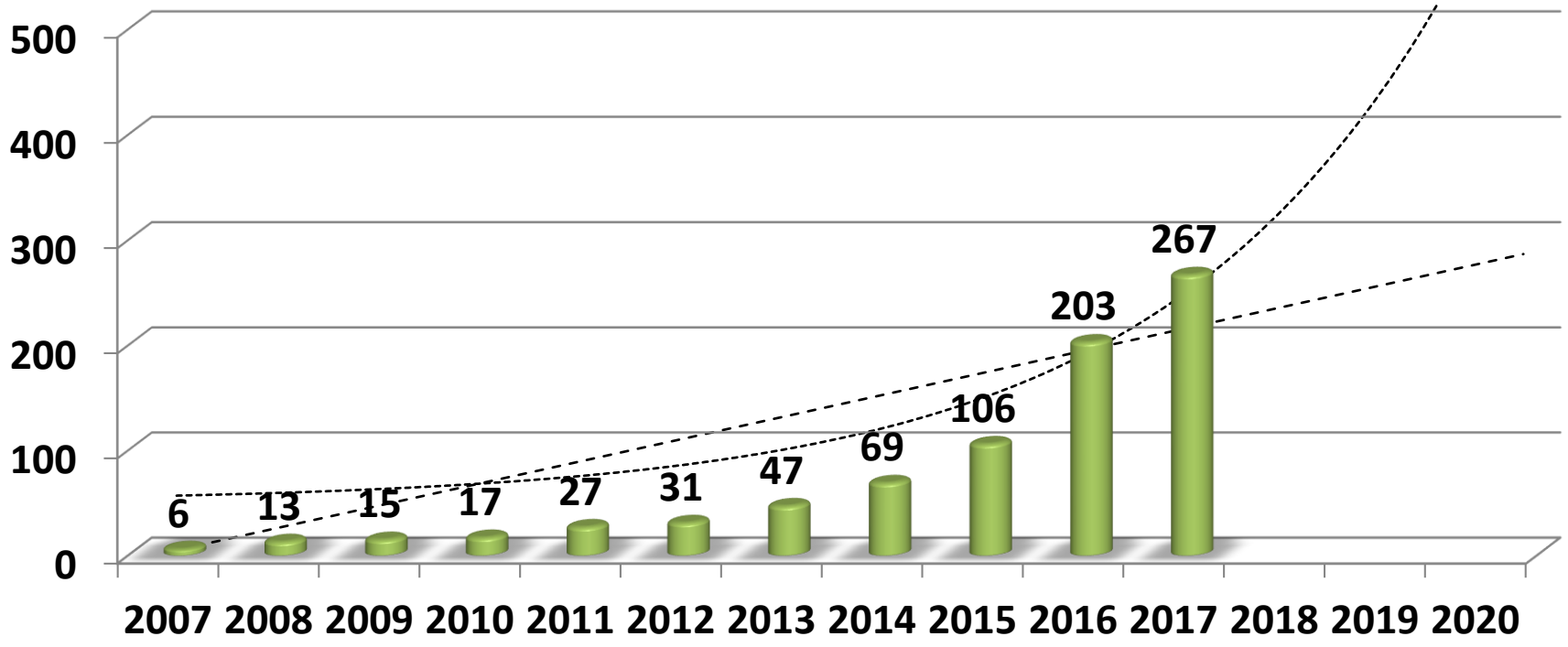
abstract.

In Japan, many organizations focus on CSIRT and CSIRT functions as cyber security countermeasure. Also many organizations promote to share the information for establishment of enterprise CSIRT, operate of CSIRT, threat intelligence and so on for cyber security countermeasure. However, in Japan, in order to disseminate information sharing of threat information by machine readable based security automation, we need to respond to requirements such as flow control of information traffic by the scale of CSIRT, group control of information traffic by the purpose, sector, severity and type, distribution control of threat and vulnerability information by same distribution channel and so on.
In this presentation, we will introduce construction situation of CSIRT and ISAC communities, information sharing trial using STIX/TAXII and the information sharing platform prototype for realizing the collaboration via systems and persons.

opening.

HITACHI
Inspire the Next

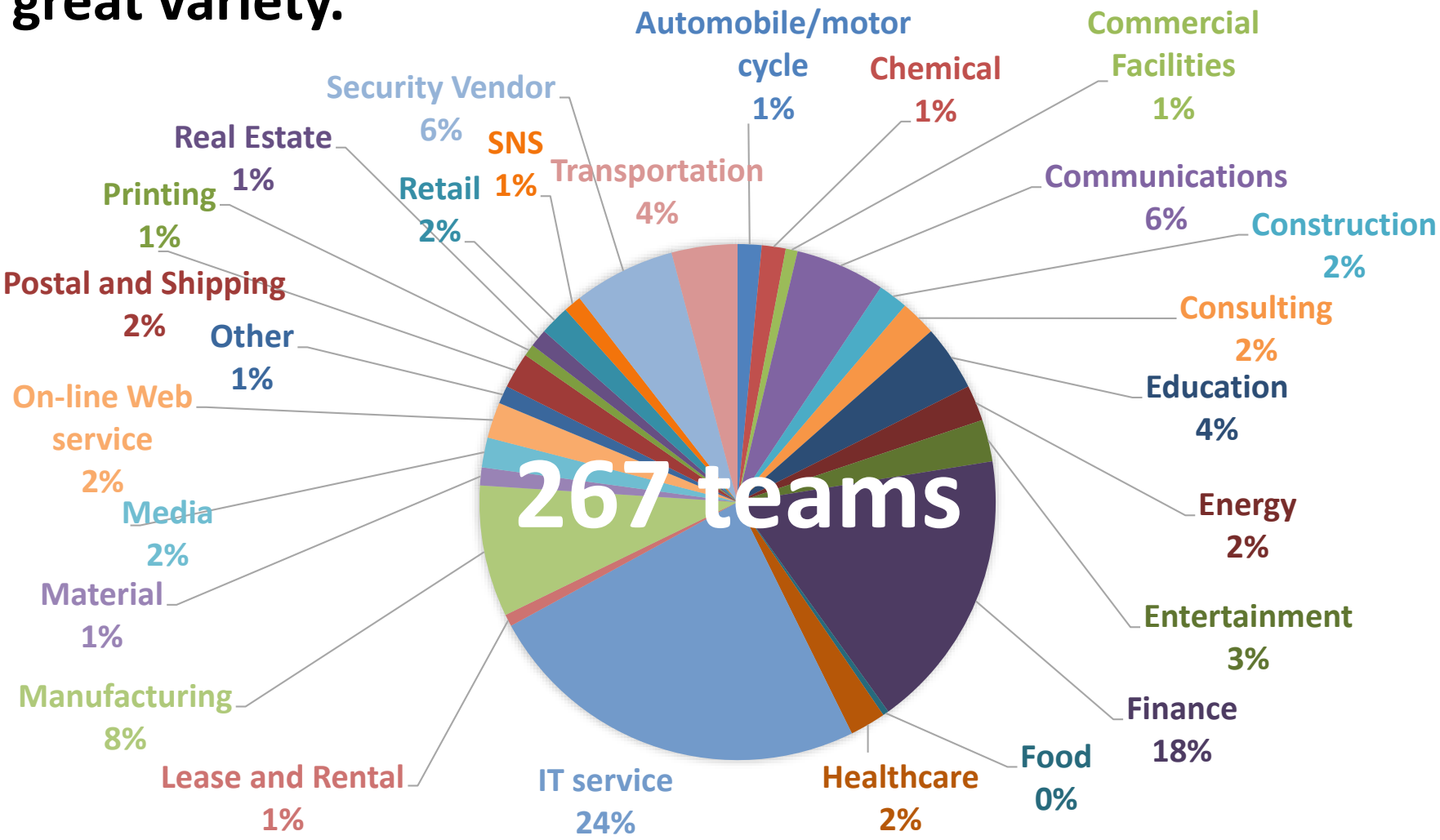
In Japan, many organizations focus on CSIRT as Cyber security countermeasure. Many organizations promote to establish enterprise CSIRT.
As of December 1st 2017, Nippon CSIRT Association which is CSIRT community, has 267 member teams.



opening.

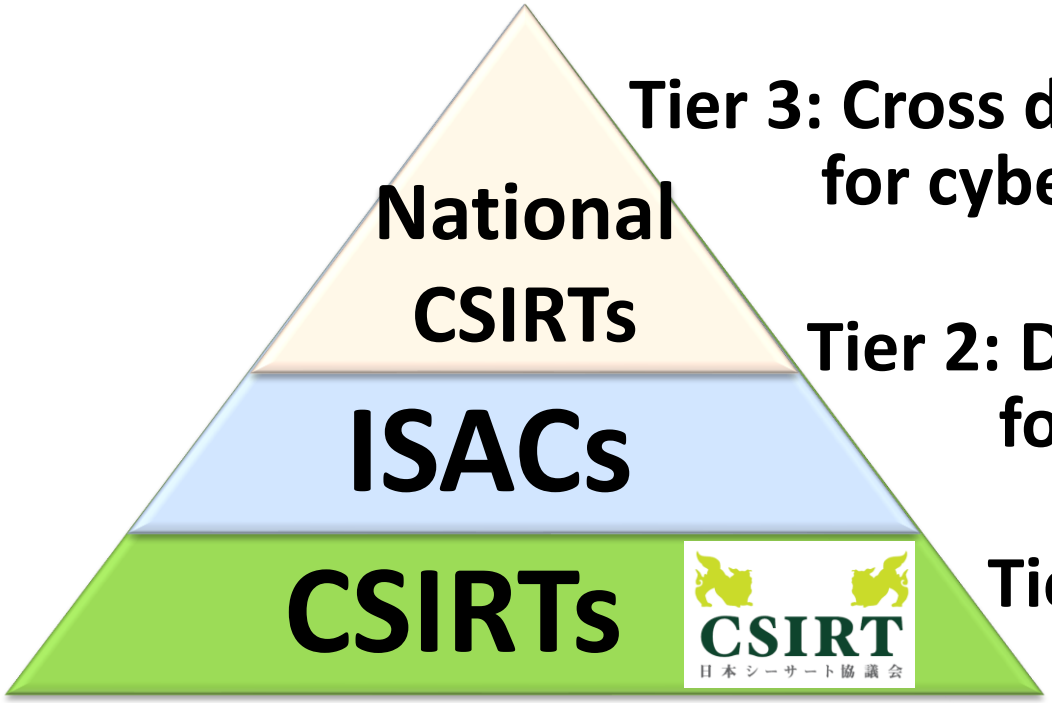
HITACHI
Inspire the Next

The characteristic of member teams classification is to great variety.



HITACHI
Inspire the Next

Also, some ISACs such as ICT-ISAC Japan, Financials ISAC Japan, JE-ISAC and Japan-Auto-ISAC started up. Nippon CSIRT Association introduced the following layered capability model for cyber security.



Tier 3: Cross domain capability for cyber security

Tier 2: Domain specific capability for cyber security

Tier 1: Basic capability for cyber security

information sharing.

HITACHI
Inspire the Next

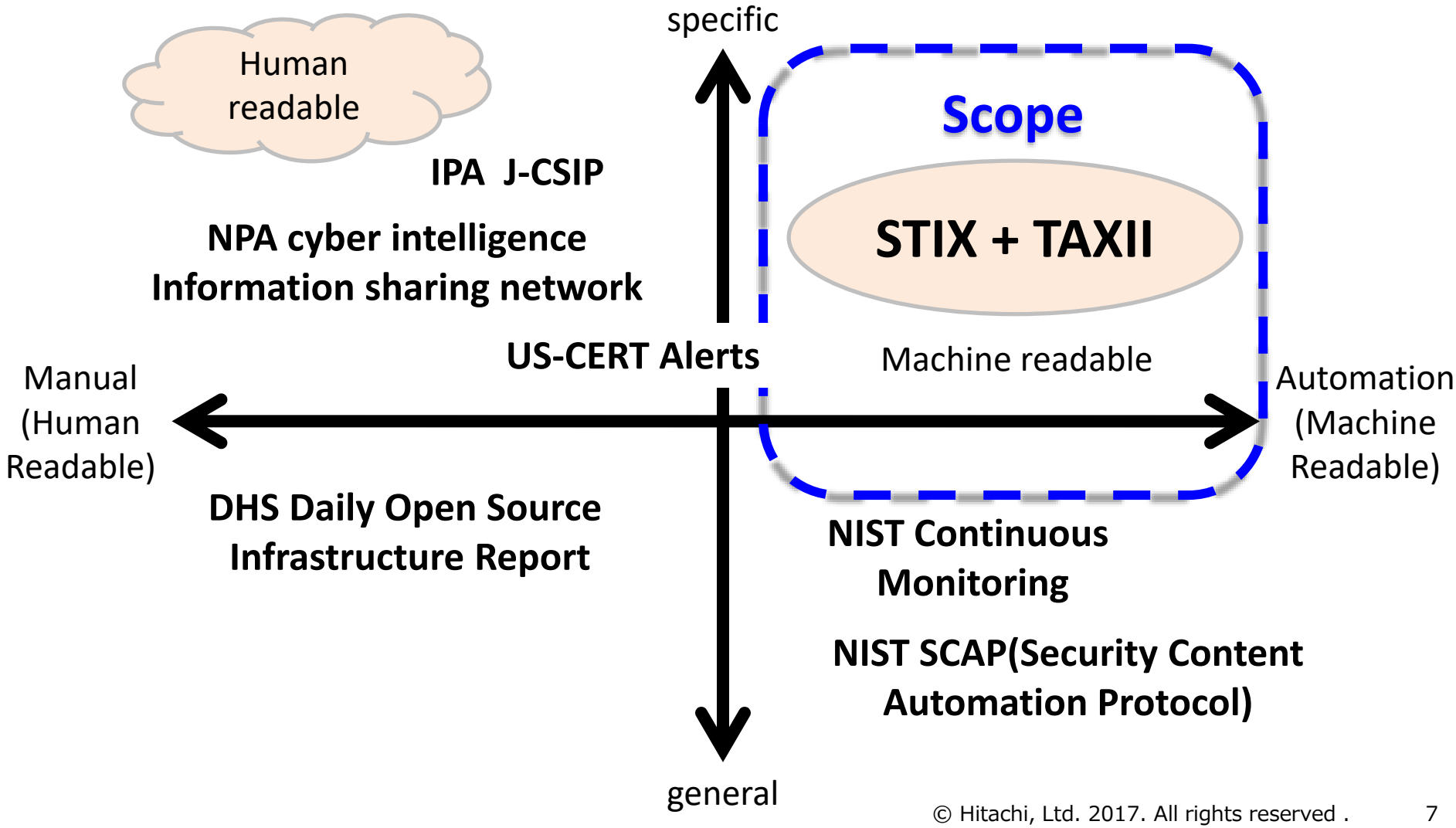
objective

Collaboration for the collective defense by measurement and indicators.

information sharing.

HITACHI
Inspire the Next

security automation



information sharing.

HITACHI
Inspire the Next

collaboration via persons vs systems

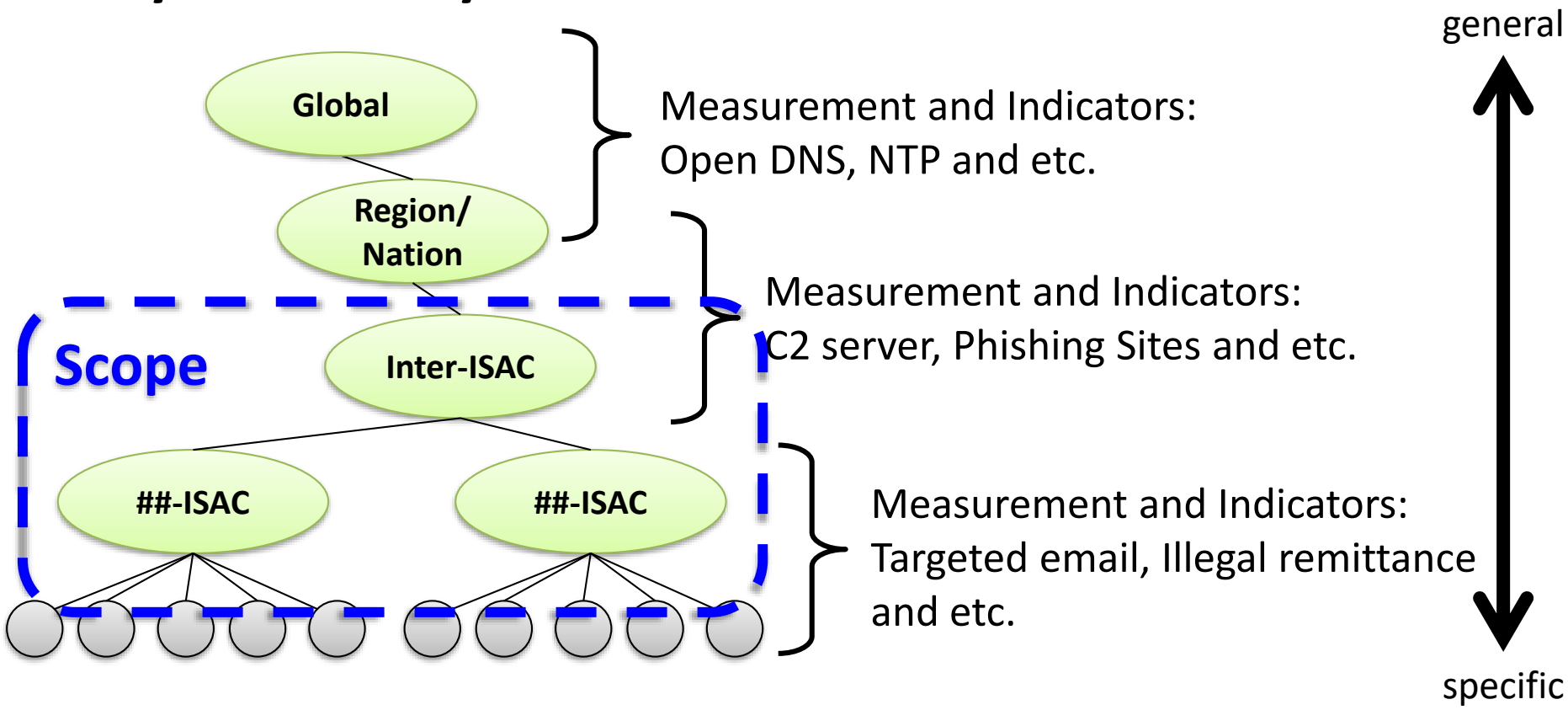
- **Collaboration via systems to match the speed of a threat actor's activities and to respond**

	For an earthquake	For defensive measures against cyber attacks
Collaboration via systems (computer-based information sharing, machine-readable)	Fast reports on earthquakes, delivered by email	Systematization that uses STIX and TAXII etc. STIX(Structured Threat Information eXpression) TAXII(Trusted Automated eXchange of Indicator Information)
Collaboration via persons (human-based information sharing, human-readable)	News conferences by the Meteorological Agency	Collaboration using email, SNS and etc.

HITACHI
Inspire the Next

layered measurement approach

- **Layered measurement approach to understand the cyber security situation**



collaboration possibilities.

HITACHI
Inspire the Next

layered measurement approach

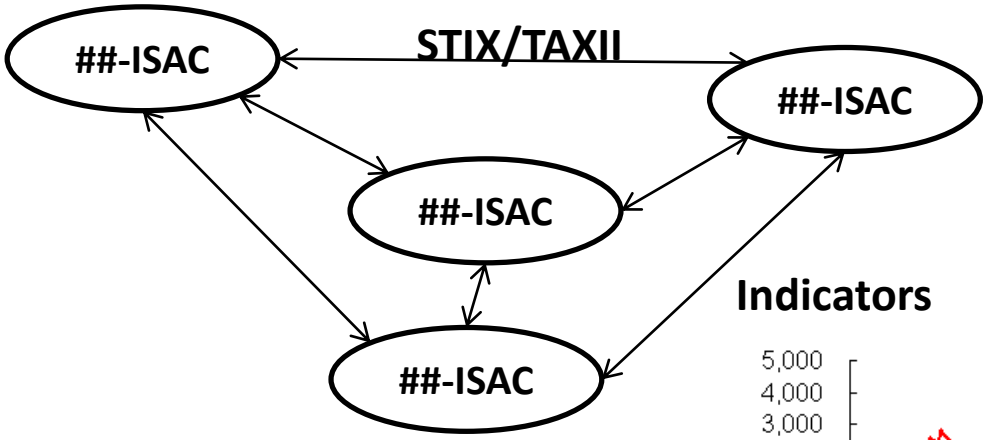
Layer	Measurement and migration
Global	**Global cyber health** Indicators: Open proxy, Open Resolver, Open NTP and etc. =>Improvement of Internet Infrastructure Security
Region/Nation Inter-ISAC	**National cyber health** Indicators: C2 server, Phishing Sites and etc. =>Eliminate general cyber threats in each of countries by each of countries.
ISAC	**cyber health of domain** Indicators: Targeted email, Illegal remittance(Finance domain) and etc =>Eliminate domain specific cyber threats

collaboration possibilities.

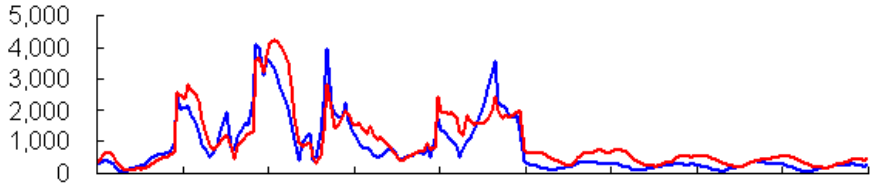
HITACHI
Inspire the Next

countermeasure based approach

- **Measurement and indicators for achieving cyber security measures**
  - Ex. Number of C2 server indicators (sites/day)
    Number of Phishing Site indicators (sites/day)



Indicators



collaboration possibilities.

HITACHI
Inspire the Next

activities plan of experimental system

Current activities

feed: C2

feed: VCITY

feed: BKMW_CONF, BKMW_ATTK, BKMW_MANU

Next step activities

STIX extension

distributed C2 monitoring system

current activities.

HITACHI
Inspire the Next

countermeasure based approach

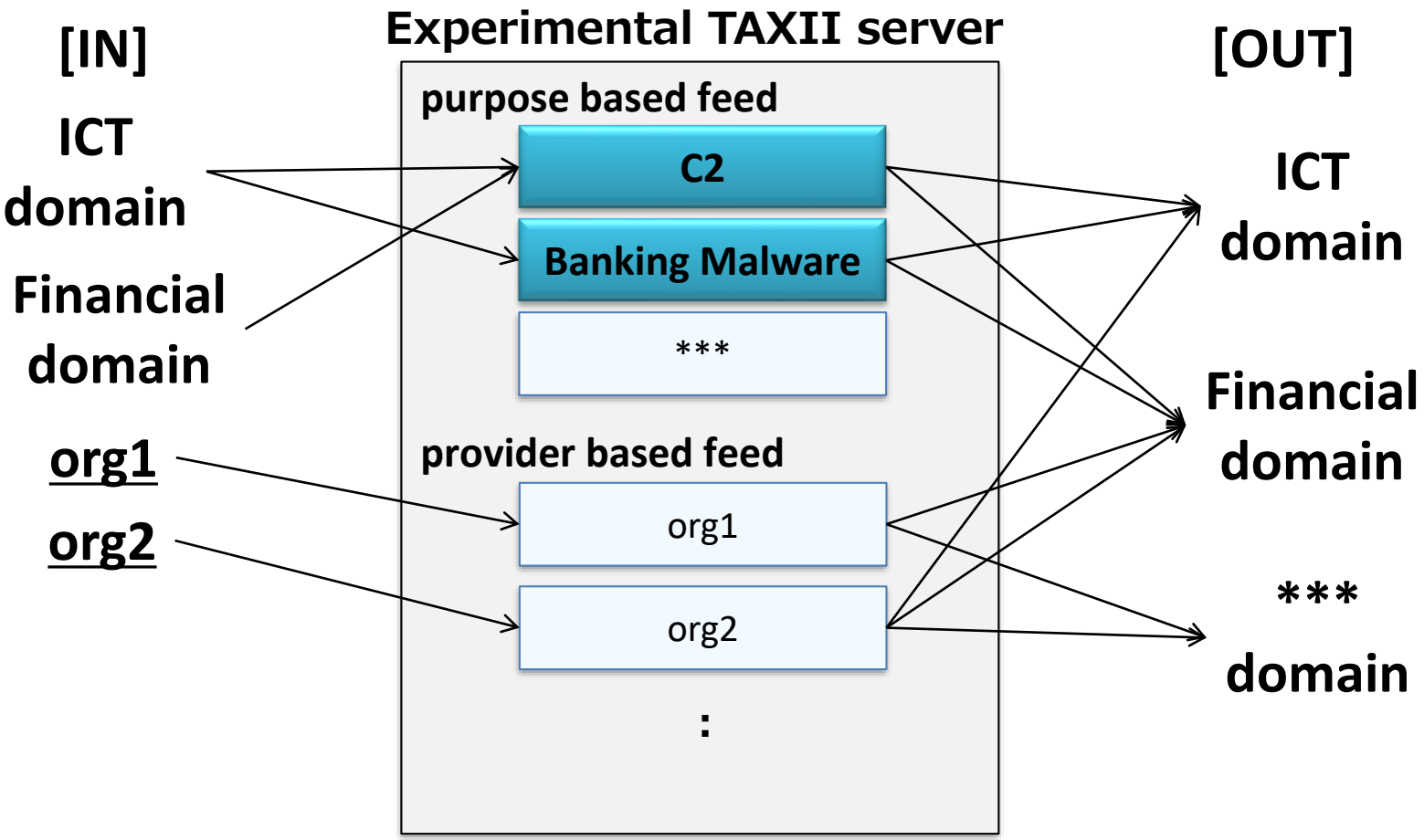
- **Process of measurement and indicators**
  We would like to respond to requirements such as flow control of information traffic by the scale of organization, group control of information traffic by the purpose, sector, severity and type, distribution control of threat.

Preparation of purpose and provider based information feeds in feasibility study.

HITACHI
Inspire the Next

countermeasure based approach

- **Process of measurement and indicators**



current activities.

HITACHI
Inspire the Next

feed list: active

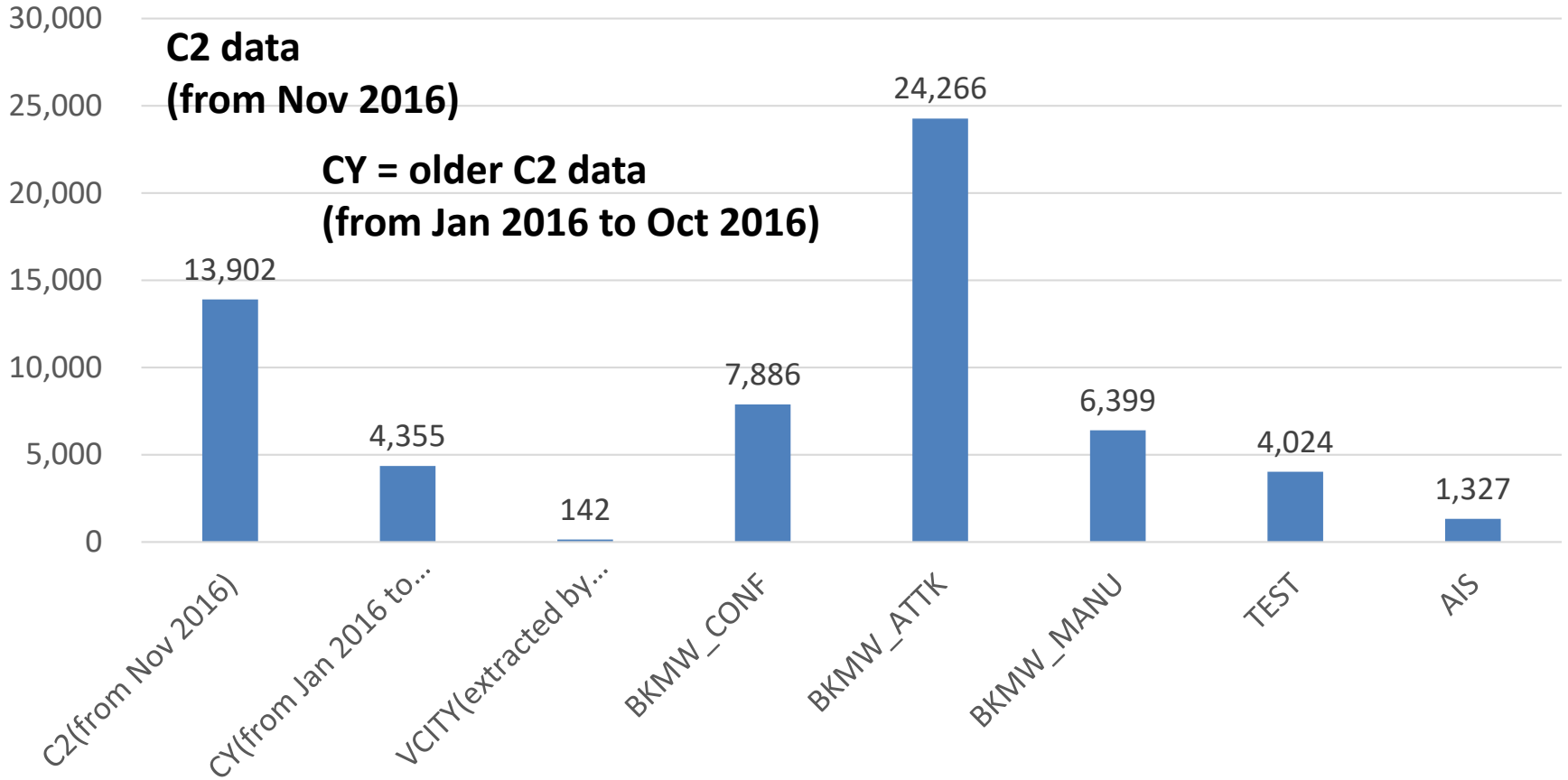
Type	Feed Name	Overview
purpose based feed	Default	get all the feeds
	C2 (from Nov 2016)	C2 information (IP addresses, domains or URLs) detected by the dynamic analysis device in joined organizations.
	CY	Older data of Feed C2 (from Jan 2016 to Oct 2016)
	VCITY	C2 information (IP addresses, domains and URLs) extracted by the destination analysis system.
	BKMW_CONF	Configuration download site of Banking Malware
	BKMW_ATTK	Invocation (targeted) Banking URL and Manipulation sites of Banking Malware
	BKMW_MANU	Manipulation site of Banking Malware
	TEST	For test
provider based feed	N/A	

current activities.

HITACHI
Inspire the Next

indicator counts of feeds

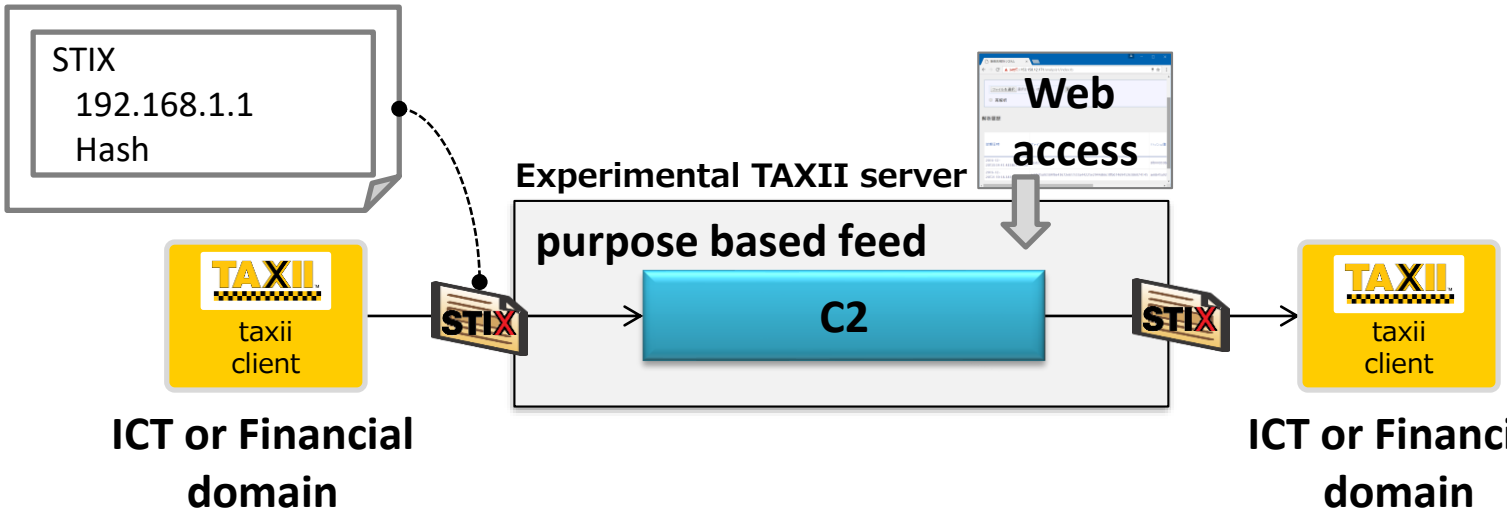
Nov 30, 2016 - Nov 4, 2017



HITACHI
Inspire the Next

feed: C2

- **C2 information detected by the dynamic analysis device in joined organizations.**
  - From two organizations (ICT and Financial domains)
  - Provide C2 (URL, domain or IP address) as an indicator, and malware hash as additional information
  - Using STIX 1.1.1

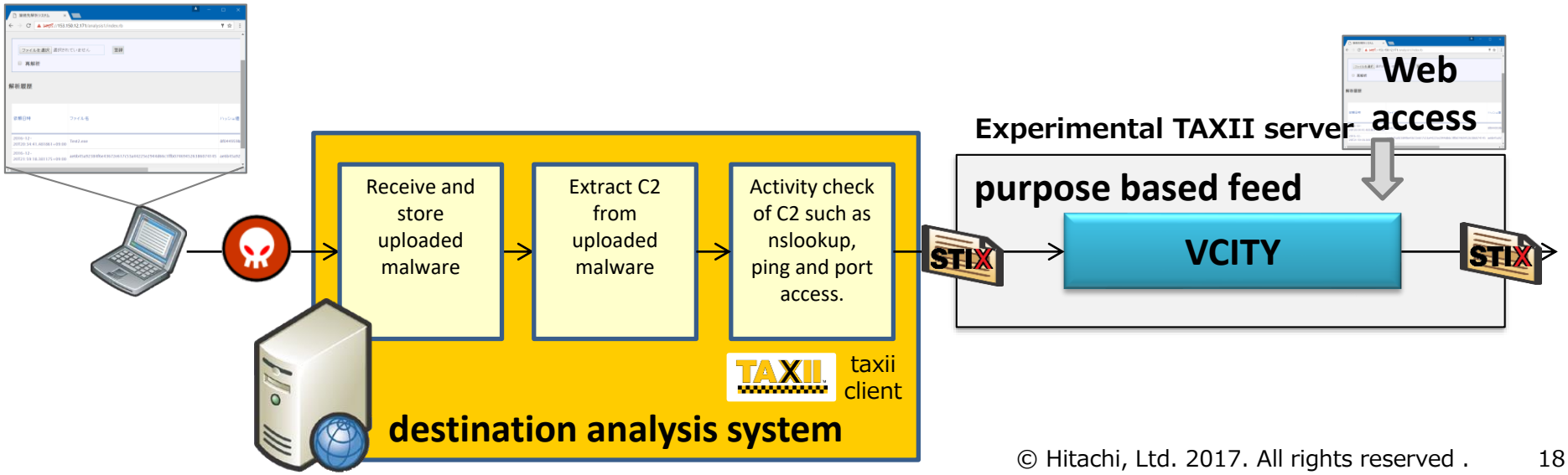


current activities.

HITACHI
Inspire the Next

feed: VCITY

- **C2 information extracted by the destination analysis system.**
  - From the destination analysis system
  - Provide C2 (URL, domain or IP address) as an indicator, and malware hash/activity check as additional information
  - Using STIX 1.1.1 and STIX extension

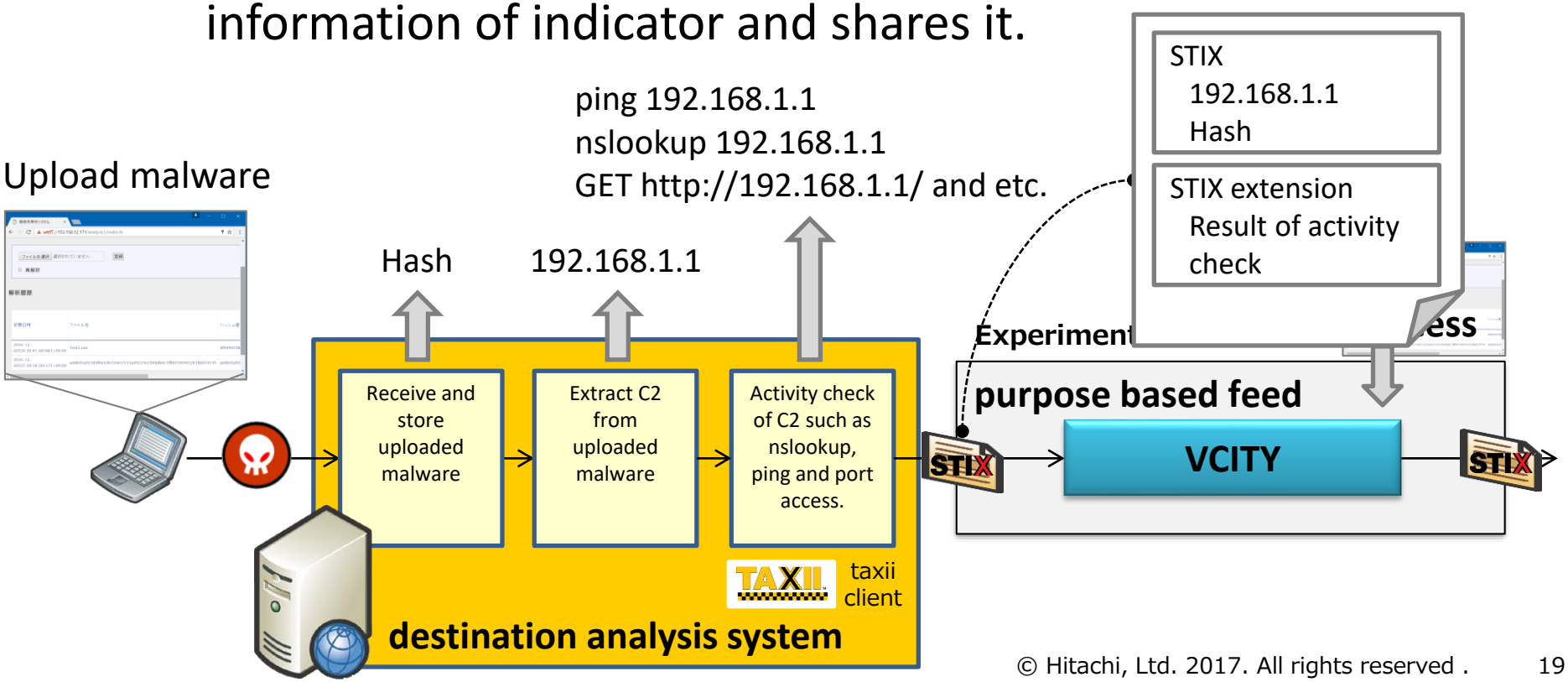


current activities.

HITACHI
Inspire the Next

feed: VCITY

- **C2 information extracted by the destination analysis system.**
  - Destination analysis system gathers activity check as related information of indicator and shares it.



current activities.

HITACHI
Inspire the Next

feed: BKMW_CONF, BKMW_ATTK, BKMW_MANU

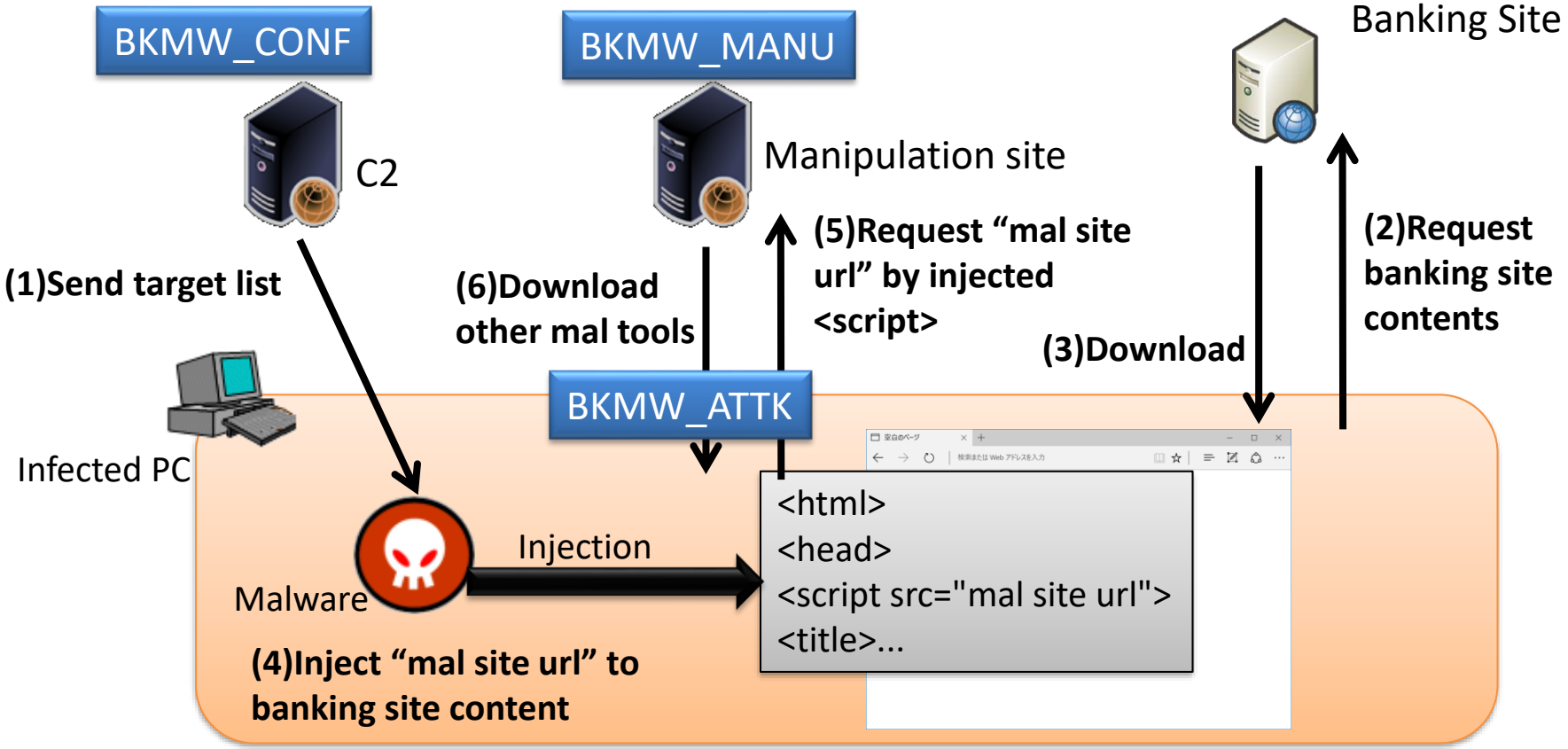
- **Banking Malware information for collaboration possibilities between ICT and Financial domain**
  - From the Banking Malware observable system
  - Provide Configuration download site/Manipulation site/Malware hash as an indicator, and malware hash/invocation (targeted) Banking URL as additional information
  - Using STIX 1.1.1 and STIX extension

current activities.

HITACHI
Inspire the Next

feed: BKMW_CONF, BKMW_ATTK, BKMW_MANU

- **Banking Malware information for collaboration possibilities between ICT and Financial domain**

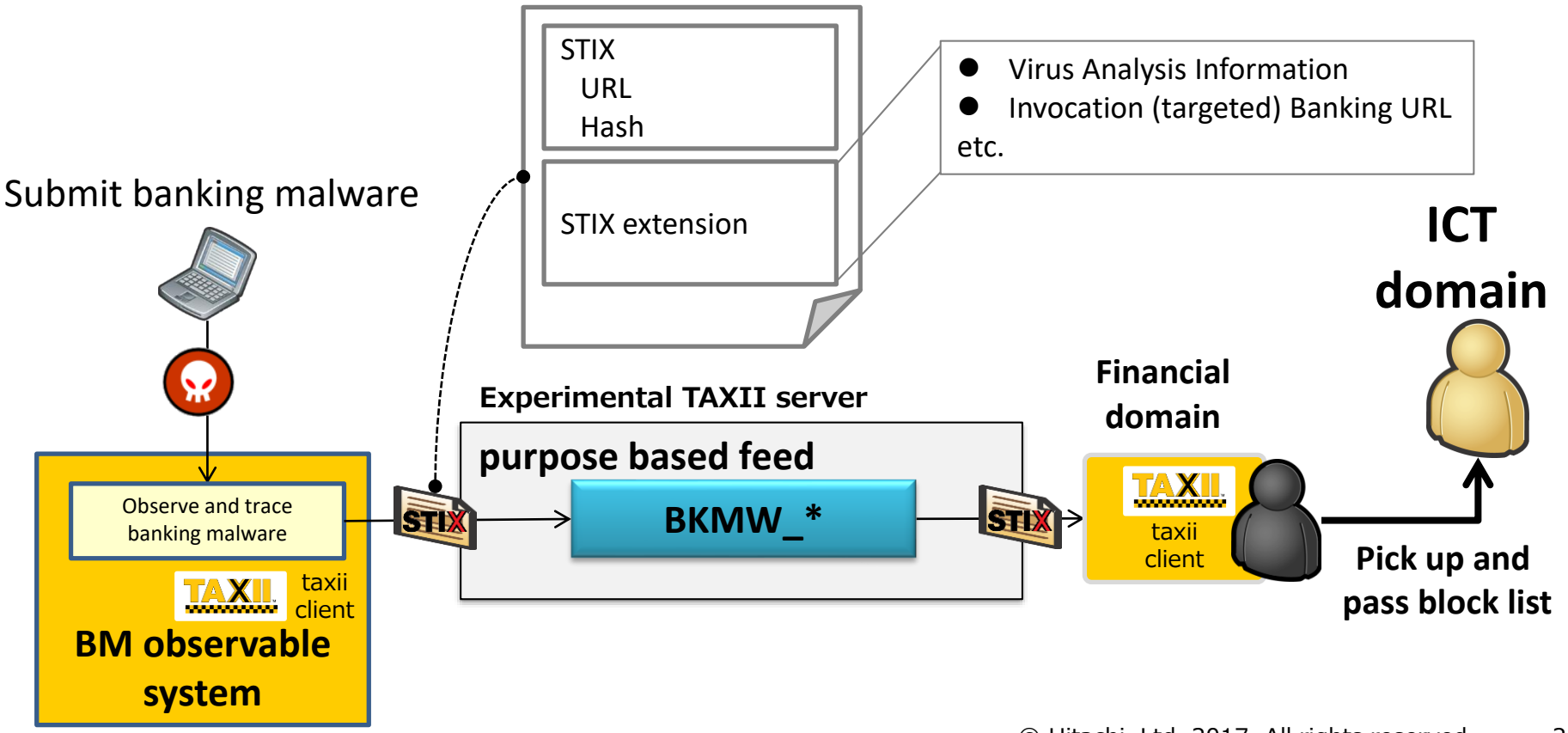


current activities.

HITACHI
Inspire the Next

feed: BKMW_CONF, BKMW_ATTK, BKMW_MANU

- **Banking Malware information for collaboration possibilities between ICT and Financial domain**



next step activities.

HITACHI
Inspire the Next

countermeasure based approach

- **Construction of provider based feed (from public sector such as AIS) environment**
- **Preparation of operation guide for STIX in Japan**
- **Development and review STIX extension in Japan**
  - Common template for inter-ISACs
  - Custom template for each ISAC
- **Feasibility study of distributed C2 monitoring system using STIX/TAXII**

next step activities.

HITACHI
Inspire the Next

STIX extension

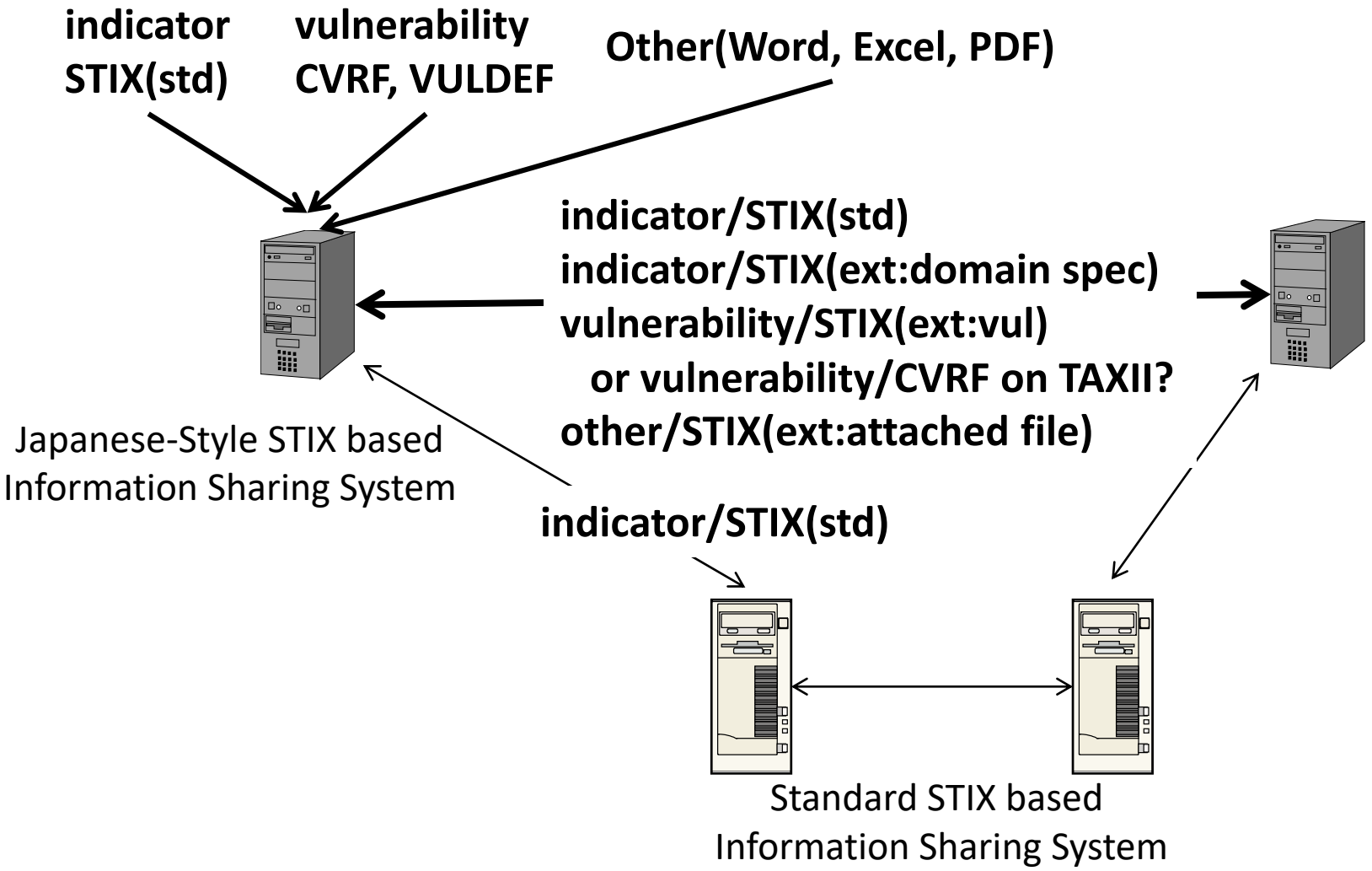
- **Development and review STIX extension in Japan**
  We would like to respond to requirements such as distribution control of threat and vulnerability information by same distribution channel and so on.

Feasibility study of STIX extension to respond to requirements, if it is really necessary.

next step activities.

HITACHI
Inspire the Next

STIX extension



HITACHI
Inspire the Next

STIX extension for STIX 2.x

- **Using custom object extensions**

```
{
 "type": "bundle",
 "id": "bundle--44af6c39-c09b-49c5-9de2-394224b04982",
 "objects": [{
  "type": "indicator",
  "id": "indicator--d81f86b9-975b-bc0b-775e-810c5ad45a4f",
  "created": "2014-06-29T13:49:37.079000Z",
  "labels": ["malicious-activity"],
  "name": "Malicious site hosting downloader",
  "pattern": "[url:value = http://www.example.com/example.exe']",
  "extensions": {
   "x-##-isac.jp": {
    "monitoring": {
     "input": " http://www.example.com/example.exe",
     "domain-name": ["www.test.co.jp", "example.co.jp"],
     "ipv4-addr": ["2.3.4.5", "12.13.14.15"],
     "network-traffic": { "dst_port": "80" },
     "ping-ext": { "lost": "0%" },
     "http-response-ext": { "status_code": 200, "reason_phrase": "OK" },
     "observe-time": "2017-09-04T10:31:37+00:00" },
    "process-time": { "system-name": "isac-monitor" },
    "id": "MM-20170904103137-08127-DSKOQ",
    "submit-time": "2017-09-06T04:53:03+09:00" } }
 }]
}
```

ISAC name

Template name

STIX 2.x Object

Custom Object Extension for ##-ISAC Japan

next step activities.

HITACHI
Inspire the Next

STIX extension for STIX 1.x

- **Tentative approach**

  STIX extension using "indicator:description"

```
<stix:STIX_Package>
 <stix:Indicators><stix:Indicator id="ICT-ISAC:indicator-01d88335-3c0a-43e5-9708-19d5fd70f916">
   <indicator:Title>__C2__ http://www.example.com/example.exe</indicator:Title>
   <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.1">C2</indicator:Type>
   <indicator:Description>
{ "x-##-isac.jp": {
     "monitoring": {
      "input": " http://www.example.com/example.exe",  "domain-name": ["www.test.co.jp", "example.co.jp"],
      "ipv4-addr": ["2.3.4.5", "12.13.14.15"],  "network-traffic": { "dst_port": "80" },
      "ping-ext": { "lost": "0%" },  "http-response-ext": { "status_code": 200, "reason_phrase": "OK" },
      "observe-time": "2017-09-04T10:31:37+00:00" },  "process-time": { "system-name": "isac-monitor" },
      "id": "MM-20170904103137-08127-DSKOQ", "submit-time": "2017-09-06T04:53:03+09:00" } }
   </indicator:Description>
   <indicator:Observable id="ICT-ISAC:observableURIObj-01d88335-3c0a-43e5-9708-19d5fd70f916">
    <cybox:Title>Domain Watchlist</cybox:Title>
    <cybox:Object id="ICT-ISAC:URIObj-01d88335-3c0a-43e5-9708-19d5fd70f916">
     <cybox:Properties xsi:type="URIObj:URIObjectType">
      <URIObj:Value>http://www.example.com/example.exe</URIObj:Value>
     </cybox:Properties>
    </cybox:Object>
   </indicator:Observable>
  </stix:Indicator></stix:Indicators>
</stix:STIX_Package>
```

ISAC name

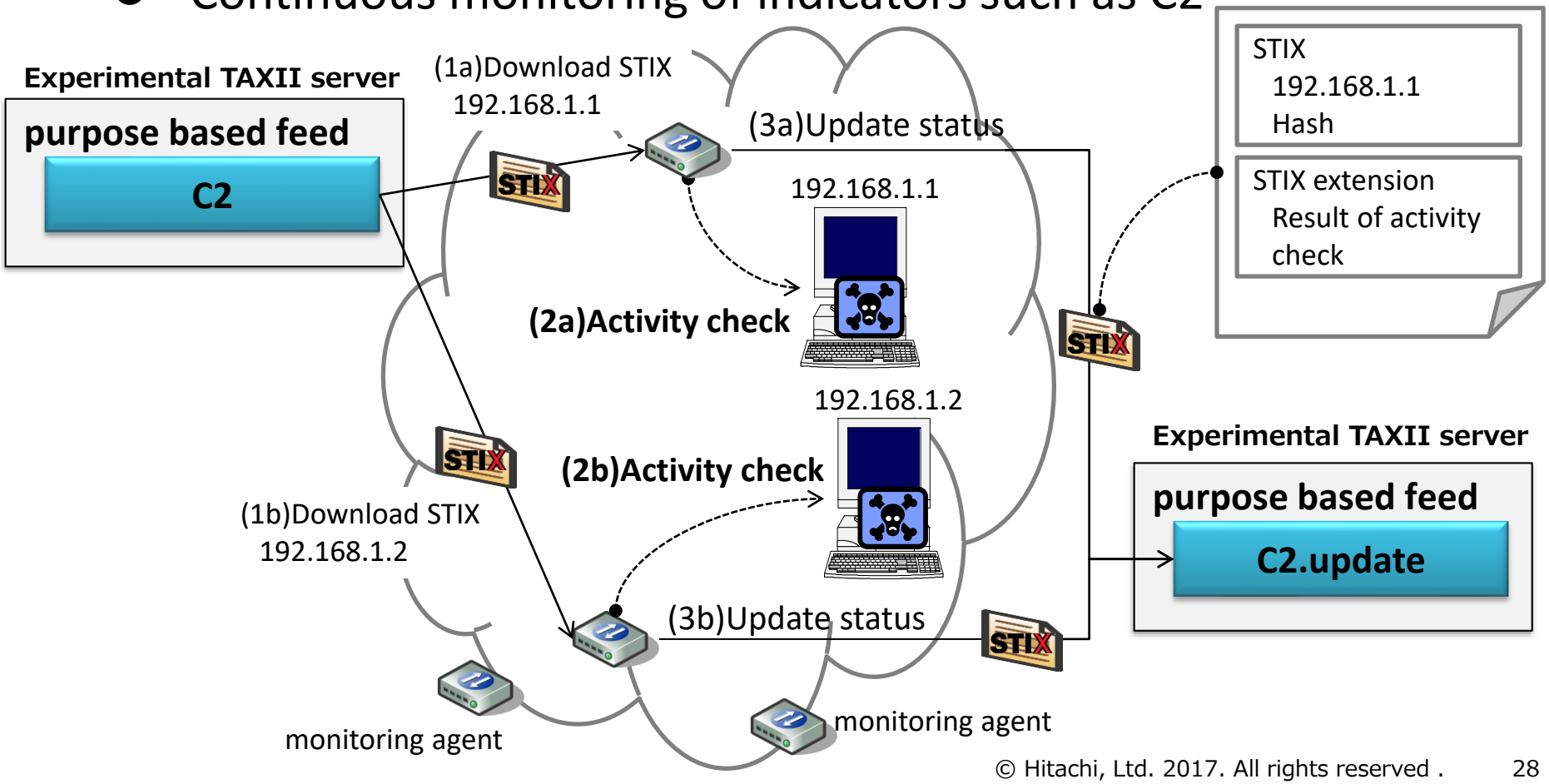
Template name

next step activities.

HITACHI
Inspire the Next

feasibility study of distributed C2 monitoring system

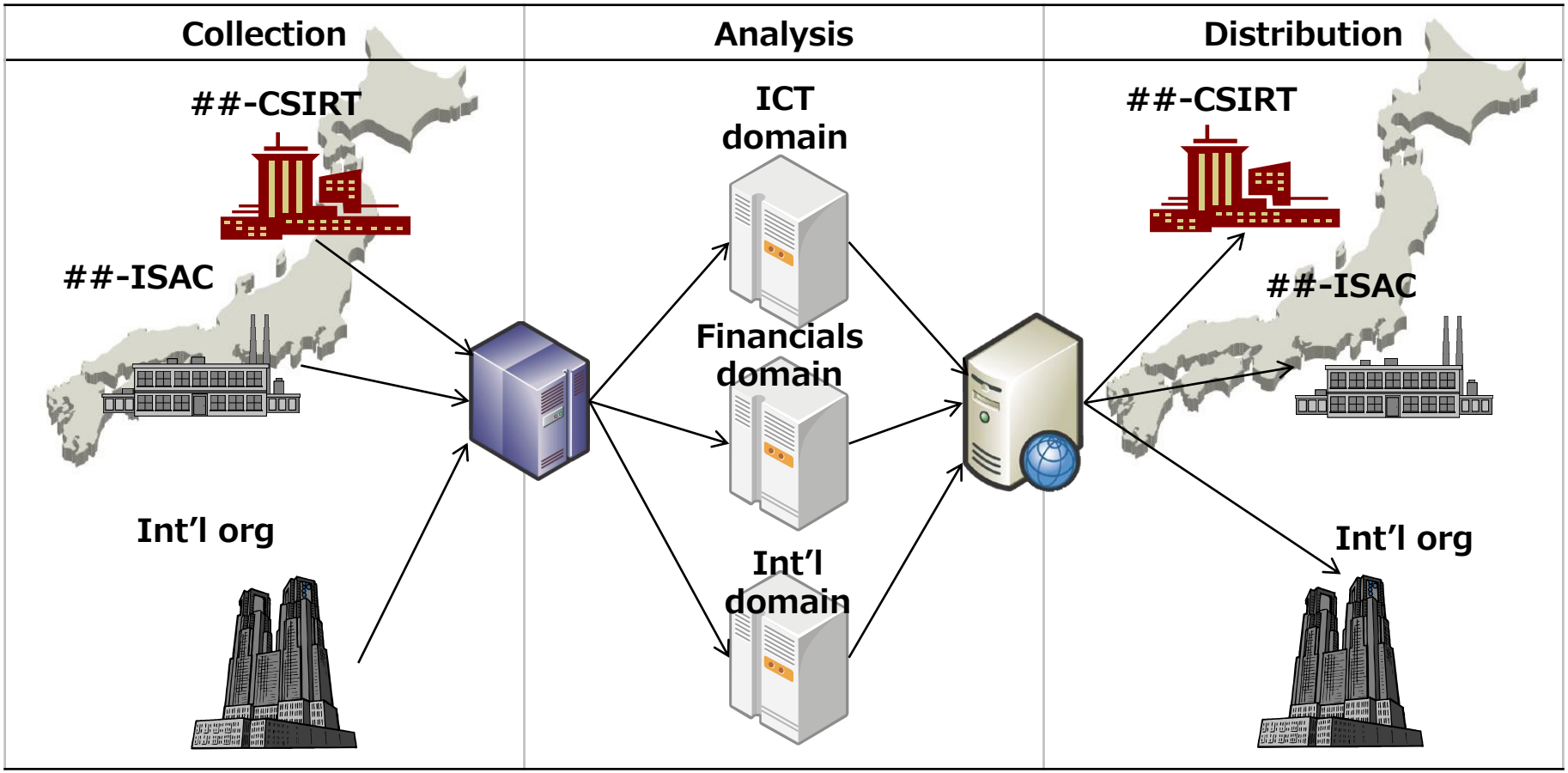
- **Security automation for the collective defense**
  - Continuous monitoring of indicators such as C2



HITACHI
Inspire the Next

security automation for the collective defense

- **Process of measurement and indicators**



closing.

HITACHI
Inspire the Next

security automation for the collective defense

Collaborate together
to make our Internet secure.

HITACHI
Inspire the Next

Japanese-Style STIX and TAXII Information Sharing Platform

Acknowledgement

This work was supported by the Information Sharing Infrastructure project of the Ministry of Internal Affairs and Communications, Japan.

総務省
MIC Ministry of Internal Affairs and Communications