2-3 Total Cyber Security With Defense, Detection, and Measures for Protecting End Points

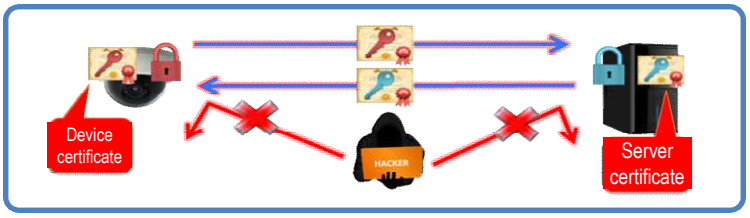
Techno logies for IoT

Secure cryptographic/authentication function achieved by generating cryptographic/authentication key from seeds with less risk of being guessed within IoT devices

(1) **Defense** Technology: Cryptography/Authentication

IoT device with vulnerable security are attack targets

- Man-in-the-middle attack
- Brute-force attack



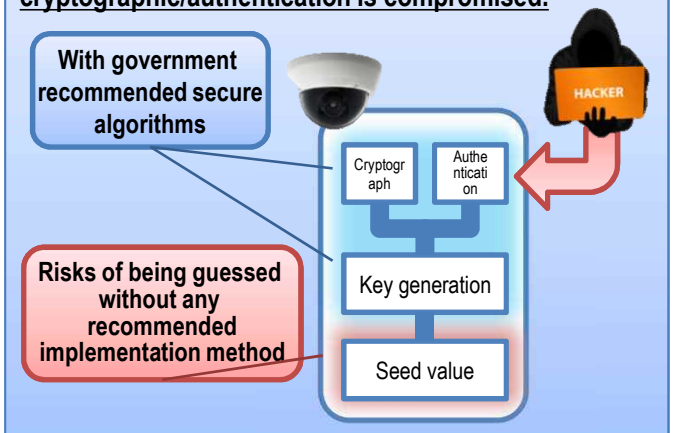
PKI authentication is required between endpoints.

(2) Seed Generation: Generation of Secure Keys From Seeds With Less Predicted Risks

Conventional issues Before	Effects by introduction After
Seeds with less fluctuation and secrets of designers have risks that the keys are guessed.	A hard-to-guess seed is generated with the function of an IoT device.
For a key generated outside the device, it is difficult to identify the leakage source if leakage occurs.	A seed and key are generated inside a device to reduce risks of leakage.

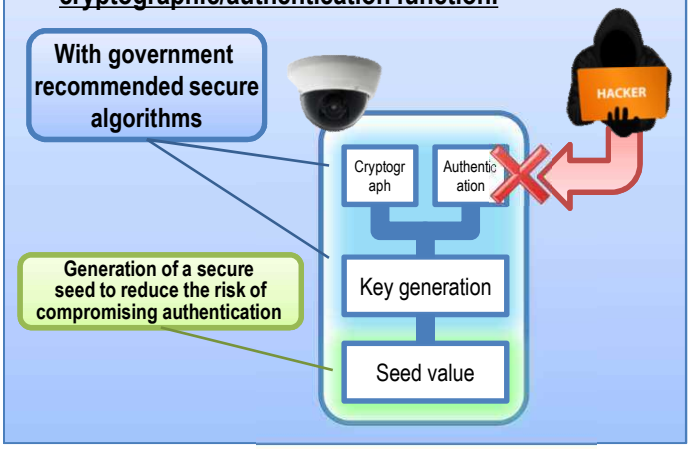
Before

There are risks that cryptographic/authentication key is guessed from the seed value and cryptographic/authentication is compromised.



After

A key is generated from a hard-to-guess seed generated inside the IoT device to achieve secure cryptographic/authentication function.



	Noise sources		Advantages	Disadvantages
	Methods	Overview		
Conventional methods	Device specific ID and others	Use of MAC address or device identifier	・Fast generation speed ・No additional cost	・Risk of being guessed from designer's secret
	/dev/random	Use of interruption (blocking type)	・Hard to guess ・No additional cost	・Slow generation speed with less interruption
	/dev/urandom	Use of interruption (non-blocking type)	・Fast generation speed ・No additional cost	・Risk of being guessed
	Physical random number generator	Use of dedicated hardware	・Fast generation speed ・Hard to guess	・Additional cost for dedicated hardware
Method from R&D results	Fluctuation of HW/SW	Use of fluctuation of oscillator, execution pipeline, branch prediction unit, scheduler, cache, etc.	・Fast generation speed ・Hard to guess ・No additional cost	・Evaluation of safety required

Panasonic

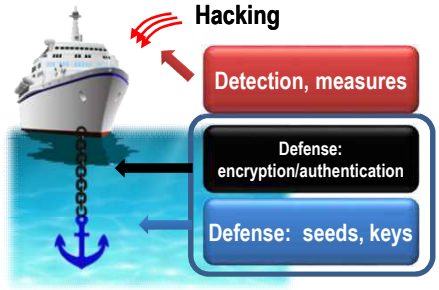
2-3 Total Cyber Security With Defense, Detection, and Measures for Protecting End Points

Techno logies for IoT

Early detection of cyberattacks by monitoring the logs of IoT devices along with network communications in order to prevent the spread of damage

(1) Required Security

For IoT having long life cycle without human intervention, *detection* and *measures* along with *defense* are important.

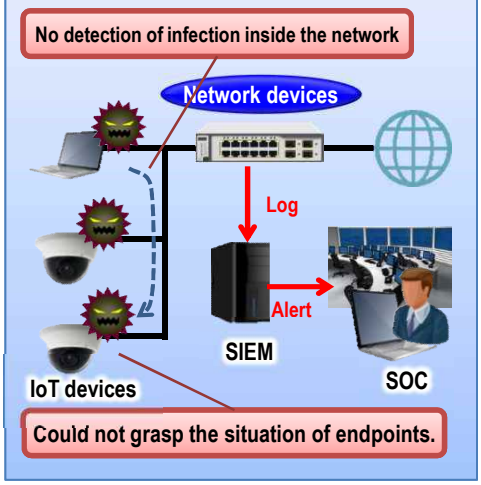


	IT security	IoT security
Measures	Windows Update Isolation of viruses and others	Measures against cyberattacks
Detection	Anti-virus software and others	
Defense	Standard cryptographic communication PKI authentication	Standard cryptographic communication PKI authentication

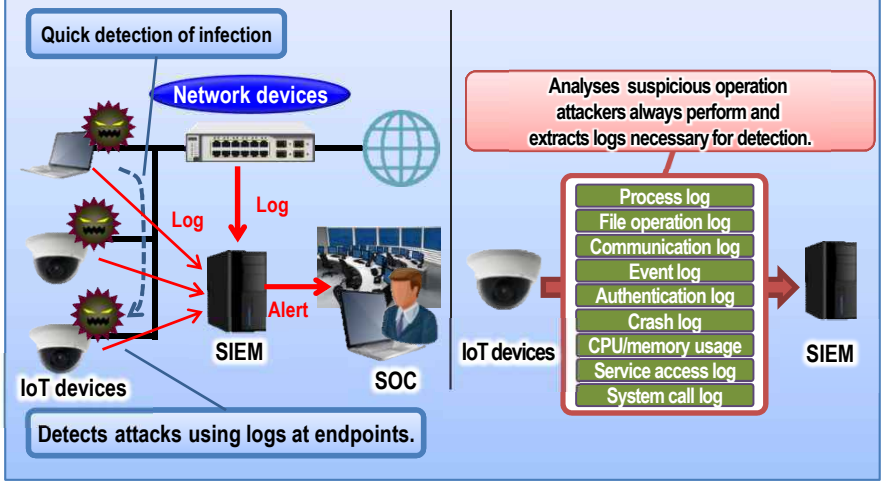
(2) Measures Against Cyberattacks: Quick Detection Using the Logs of IoT Devices and Measures

Conventional issues Before	Effects by introduction After
Could not detect infection within the network.	Quick detection of infection within the network using logs of IoT devices.
Took long time to analyze data without logs of the IoT devices.	Optimization of the incident response process using logs of IoT devices.
Difficult to make use of data due to the diversity of formats even if logs were output from IoT devices.	Outputting of logs in the same format as IT for using the existing SOC.

Before: Use of logs of network devices



After: Use of logs also of IoT devices



Reduction of incident response times for SOC by using logs collected from IoT devices