Featured Articles

Managed Security Services to Address Increasingly Sophisticated Cyber-attacks

Yoshitaka Narishima
Shinichi Kasai
Takayuki Sato
Masaki Mori
Akihiko Fujita

OVERVIEW: Companies and organizations have been facing increasingly severe security risks in recent years as cyber-attacks have grown more complicated and sophisticated. Also, as cloud services have spread, the connection of information appliances and control system devices to the Internet has added to the complexity of the information systems that must be protected. Managed security services are a group of integrated services that provide everything from consulting to operations and the application of security measures. These services include technical assistance in the handling of incidents by applying Hitachi's knowledge, and security event monitoring services that apply know-how in both construction and operations, thereby enabling the provision of solutions that are tailored to the information systems that are being protected and contributing to the safety and security of the social infrastructure.

INTRODUCTION

INFORMATION technology (IT) is increasingly being utilized to achieve an advanced social infrastructure that provides greater user convenience. As the role of IT systems grows in this type of social infrastructure, the importance of ensuring safety and security is becoming more and more important.

Companies and organizations have been facing stark security risks in recent years as cyber-attacks have grown more complex and sophisticated. This includes more advanced targeted e-mail attacks and larger distributed denial of service (DDoS) attacks, among others. Cyber-attacks target specific organizations or individuals and relentlessly attempt to steal confidential or personal information and to cripple IT system services, which even lead to exact money.

The information systems that must be protected used to be set up within the organizations, but due to the spread of cloud services, they can now be located outside the organizations and on the Internet. With internal corporate information systems sometimes linked to cloud services as well, the boundaries between security regions are becoming less clear, and the administration of security increasingly complicated. Also, in addition to personal computers (PCs) and other such IT devices, information appliances, control system devices, and other devices are now being connected to the Internet. This makes much larger number of system environments vulnerable to the cyber-attacks, making the scale of the threats even greater.

Against the background of these threats, taking security measures based on defense in depth in order to protect information systems from cyber-attacks, the necessity is also growing for the immediate detection of incidents when an attack occurs, so that events can be handled rapidly to hold damage to a minimum. To this end, monitoring systems must be strengthened, with advanced log management systems that constantly monitor the complex IT systems, as well as an organization comprised of engineering staff with the technical skills required to take necessary measures quickly. Also, the necessity for outsourcing security operations and security measures has been spreading as the operational burdens placed on information system departments has been increasing along with the required security expertise.

This article discusses managed security services, which are a set of comprehensive security measures designed to protect social infrastructures and information systems from more complicated and sophisticated cyber-attacks.

MANAGED SECURITY SERVICES

Offerings from Hitachi include managed security services that oppose cyber-attacks and other threats. These security solutions, everything from consulting to the application of security measures and operational services, provide total support for companies in the social infrastructure field and a variety of other industries and business categories, as well as for public agencies and local governments.

These services manage security during the operational phases of IT systems with expanded needs in outsourcing security measures and operations, and not only do they "protect IT," they offer an integrated set of security services designed for the "protection via IT." Managed security services comprise three categories: "managed security governance," "managed channel security," and "managed platform security," which can propose and provide the right solution for the information system being protected, as well as the responsible office and department in the organization (see Fig. 1).

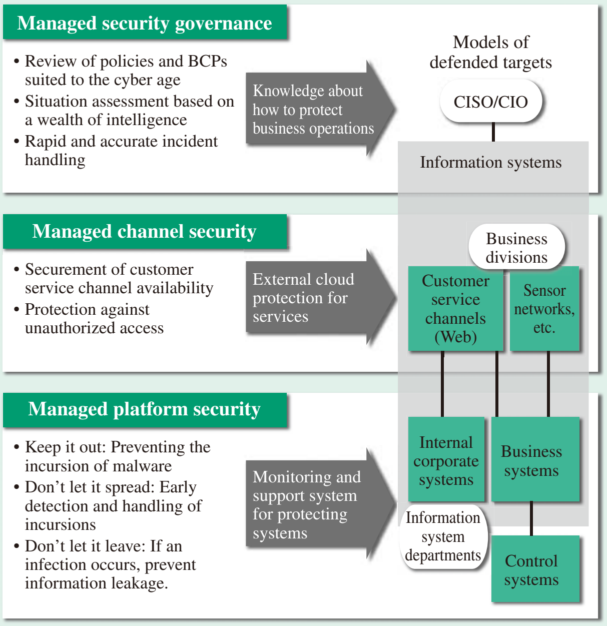
The features of each of these three service categories are described below.

Achieving Dynamic Security Management

In order to strengthen measures against vulnerabilities in managed security services, in addition to improvements based on the "PDCA cycle," with planning that involves constructing cybersecurity incident readiness/response teams (CSIRT) within organizations and reviewing business continuity plans (BCPs) (plan), measures and operations (do), inspections and audits (check), and improvements and corrections (act), the "OODA loop" concept is also adopted in order to achieve decision making that is both rapid and rational, through a series of steps that includes monitoring (observe), situational analysis (orient), decision making (decide), and action (act). This method is used to strengthen dynamic security management in the operational stage, to establish information security policies based on the assumption that incidents will occur, and to implement stronger and more rapid security measures (see Fig. 2).

Applying the Incident-handling Know-how of a Team of Professionals

The Hitachi Incident Response Team (HIRT), which acts as a CSIRT with responsibility for cyber-attack


Managed security governance
• Review of policies and BCPs suited to the cyber age
• Situation assessment based on a wealth of intelligence
• Rapid and accurate incident handling
Knowledge about how to protect business operations
Models of defended targets
CISO/CIO
Information systems
Managed channel security
• Securement of customer service channel availability
• Protection against unauthorized access
External cloud protection for services
Business divisions
Customer service channels (Web)
Sensor networks, etc.
Managed platform security
• Keep it out: Preventing the incursion of malware
• Don't let it spread: Early detection and handling of incursions
• Don't let it leave: If an infection occurs, prevent information leakage.
Monitoring and support system for protecting systems
Internal corporate systems
Business systems
Information system departments
Control systems

Category	Service menu	Feature overview
Managed security governance	Security consulting service	• Security policy formulation support • Security risk analysis support • Business continuity management formulation support
	Security diagnosis service	• IT infrastructure vulnerability diagnosis • Malware inspection
	Intelligence service	• System vulnerability information provision • Harmful rumor surveys regarding specific sites • Incident response support
	CSIRT technical support service	• CSIRT operation support within organizations • Targeted attack mail training
Managed channel security	Website protection service	• Web application firewalls • Website DDoS measures
	Website check service	• Web system vulnerability diagnosis • Tampering detection
Managed platform security	E-mail security service	• Anti-virus, anti-spam • Content filtering
	Web security service	• URL filtering during Web browsing • Anti-virus
	Security event monitoring service	• Integrated log management • Log correlation analysis
	Virtual server protection service	• Virtual UTM operation support

BCP: business continuity plan CISO: Chief Information Security Officer CIO: Chief Information Officer IT: information technology
CSIRT: cybersecurity incident readiness/response team DDoS: distributed denial of service URL: uniform resource locator UTM: unified threat management

Fig. 1—List of Menu Options for Managed Security Services.
The systems defended by each category of managed security services are shown above. The table lists the service menu options available in each category.

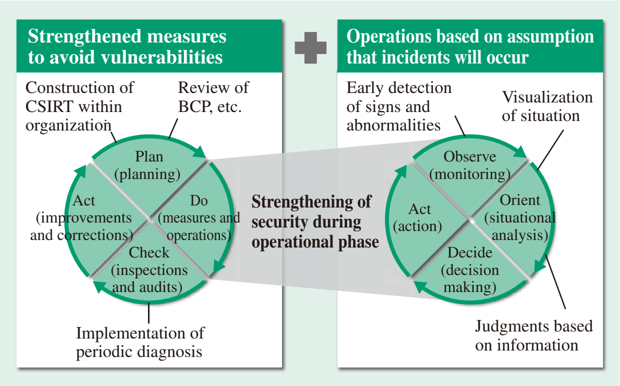

Strengthened measures to avoid vulnerabilities
Operations based on assumption that incidents will occur
Construction of CSIRT within organization
Review of BCP, etc.
Plan (planning)
Do (measures and operations)
Check (inspections and audits)
Act (improvements and corrections)
Implementation of periodic diagnosis
Strengthening of security during operational phase
Early detection of signs and abnormalities
Visualization of situation
Observe (monitoring)
Orient (situational analysis)
Decide (decision making)
Act (action)
Judgments based on information

Fig. 2—Relationship between PDCA Cycle and OODA Loop.
In addition to the continual improvements of the PDCA (plan, do, check, act) cycle, operations based on the OODA (observe, orient, decide, act) loop are adopted in order to strengthen security in the operational (do) phase.

measures, is a team of professionals within Hitachi with extensive know-how in handling incidents. HIRT cooperates with global partners to analyze and monitor intelligence on behalf of the customer's internal CSIRT, while offering various services including a "CSIRT technical support service" that provides related information and necessary responses, as well as an extremely advanced security operation and management system that is active 24 hours a day and 365 days a year.

Flexible Support for Cloud Environments

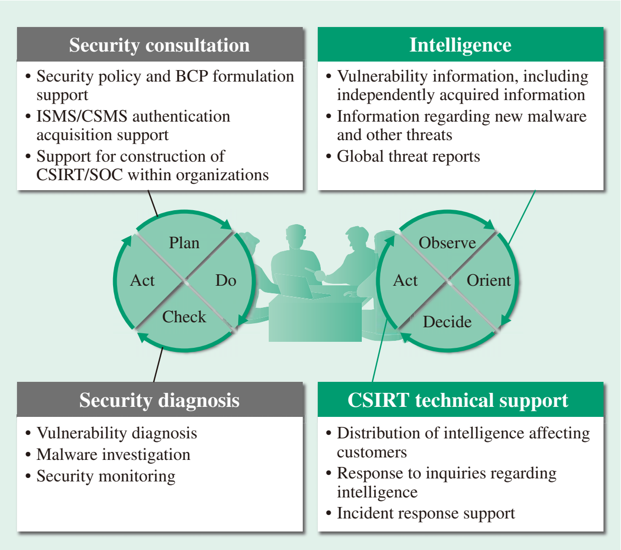
Complex security measures and operations are provided for multiple system environments including on-premises environments, cloud environments, distributed cloud environments, and others. Also, by providing services such as "virtual server protection services" and "security event monitoring services" that enable detailed individual security measures that have been difficult under cloud environments in the past, flexible support for cloud environments is achieved.

CATEGORIES AND SERVICE MENUS

Service menu options that warrant attention are described below for each of the three categories of managed security services.

Managed Security Governance

Managed security governance, which protects business operations, is comprised of professional consultation services and other services based on the knowledge accumulated as part of Hitachi's internal information system management, in addition to knowledge accumulated as part of activities supporting customer businesses (see Fig. 3).


Security consultation
• Security policy and BCP formulation support
• ISMS/CSMS authentication acquisition support
• Support for construction of CSIRT/SOC within organizations
Intelligence
• Vulnerability information, including independently acquired information
• Information regarding new malware and other threats
• Global threat reports
Plan
Act
Do
Check
Observe
Act
Orient
Decide
Security diagnosis
• Vulnerability diagnosis
• Malware investigation
• Security monitoring
CSIRT technical support
• Distribution of intelligence affecting customers
• Response to inquiries regarding intelligence
• Incident response support

ISMS: information security management system
CSMS: cybersecurity management system
SOC: security operation center

Fig. 3—Managed Security Governance Menu Configuration.
This diagram shows the service menus provided for managed security governance, and the relationship between the menus and the PDCA cycle and OODA loop.

The process of continual improvement activities through the PDCA cycle in information security management is an effective way to ensure information security in social infrastructures and IT systems. Security consulting services support the formulation of an organization's security policies and the analysis of security risks based on the ISO/IEC 27001 international standard for information security management. Organized and systematic security management is promoted by providing and working to establish these types of security management efforts for customers.

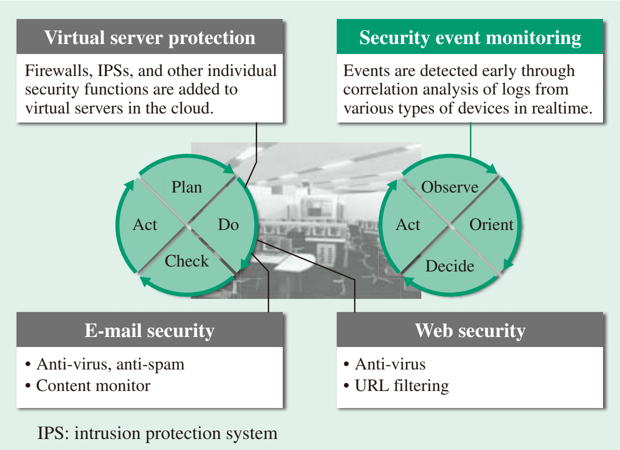
Mechanisms and systems that can rapidly handle incidents are necessary to deal with increasingly sophisticated cyber-attacks. By quickly acquiring valuable information such as newly discovered cyber-attack techniques and vulnerabilities, cyberterrorism information, and so on, it is possible to hold an advantage when it comes to implementing cyber-attack measures as well. Intelligence services exist that gather this type of threat information using a global intelligence network, in order to provide the information in a rapid and comprehensive manner. In addition to technical information, the intention behind each attack is also provided along with surrounding conditions, so that the scale of the threat can be determined with greater specificity. Information such as zero day vulnerabilities newly discovered in known vulnerability information as well as vulnerability information used to predict future threats is also provided and added to the information content that corresponds to the organization's system.

Finally, based on the gathered threat information and the log management system described below, the way incidents are actually handled is key, and the CSIRT inside the organization is responsible for fulfilling this role. The necessity of this type of system has increased in recent years, and a variety of different organizations including financial institutions have been constructing systems. A CSIRT technical support service provides operational support including incident handling and cyber-attack analysis for newly launched organizations. In the future, as cyber-attacks evolve even further, it is expected that still higher levels of security expertise will be required, and the need for these types of support services will increase.

Managed Channel Security

Managed channel security is a service that protects the customer's services by defending public websites from threats in an external cloud.

This service has become indispensable for business, and due to the fact that the public websites that are used in actual business involving the provision of corporate information and various business deals are always exposed to the Internet, they are ideal targets for attackers. There have been many cases recently of vulnerabilities in websites being exploited to tamper with the sites. Although in the past these types of attacks mainly involved displaying a flag or some other image, recently websites have been tampered with in ways that are not visible, with viruses injected in many cases. Users accessing such a site are unknowingly infected with the virus, and personal information and other information is stolen as a result. Not only is the organization with a website that has been tampered with a victim, it can also conceivably be seen as the party perpetrating the harm to its Web users, and so the strengthening of security is an urgent issue. Website protection services continuously defend public websites with DDoS attack measure services to protect websites from attacks coming from large-scale, globally distributed platforms, as well as Web Application Firewall (WAF) services.



Virtual server protection

Firewalls, IPSs, and other individual security functions are added to virtual servers in the cloud.

Security event monitoring

Events are detected early through correlation analysis of logs from various types of devices in realtime.

E-mail security

- Anti-virus, anti-spam
- Content monitor

Web security

- Anti-virus
- URL filtering

IPS: intrusion protection system

Fig. 4—Managed Platform Security Menu Configuration.
This diagram shows the service menus provided for managed platform security, and the relationship between the menus and the PDCA cycle and OODA loop.

Managed Platform Security

Managed platform security is a service that defends the customer's information and control systems from threats (see Fig. 4).

Based on the "defense in depth" concept, multiple layers of defenses include "internal measures" designed to prevent incursions by malware, "proliferation measures" designed to quickly detect any incursions and prevent them from proliferating, and "outbound measures" designed with goals that include preventing information from leaking in the case of an infection. Although outbound measures that do not allow information leaks are also important, internal measures must act as the first line of defense by reducing the incursion of targeted attack e-mail and other such threats inside the organization. The e-mail security service is a Software as a Service (SaaS) type service that provides multiple functions, including highly accurate anti-spam functions, as well as anti-virus functions that combine multiple commercial virus scanners with a proprietary artificial intelligence engine. Each advanced detection function enables the reduction of unwanted e-mail within the organization, thereby improving organizational work efficiency. It is also possible to take advantage of the SaaS features to reduce the time required to adopt security measures, cut costs, and decrease the burden of management.

The use of cloud solutions such as Hitachi Cloud Computing Solutions is growing. Benefits to the adoption of cloud solutions include a reduction in both cost and development time. On the other hand, concerns in the area of security are acting as an obstacle to usage. With a managed security service, in addition to the security provided by each cloud platform, functions such as firewalls and intrusion protection systems (IPSs) are also provided as virtual server protection services, with detailed settings and log analysis that are the same as for an on-premises environment.

In these types of systems as well, where on-premises environments are mixed with cloud environments utilizing virtualization technology, it is necessary to monitor each type of device on a regular basis in order to quickly detect security abnormalities, and to tie this in to the handling of incidents. Security event monitoring services provide comprehensive monitoring of systems in hybrid environments that include cloud services, detecting incidents at an early stage while offering advanced and rapid incident handling support by a team of professionals, in collaboration with Hitachi's Security Operation Center (SOC).

CASE STUDIES AND EFFECTS OF ADOPTION

Managed security services are provided as a set of services offering comprehensive security measures. Examples of adopted service menu options are described below.

E-mail security services are used by financial institutions as well as many other types of companies. A large number of customers have reported that the internal workload placed on their companies was decreased after the services were adopted, due to the high rate of detection. The support system, which is active 24 hours a day and 365 days a year, has been given high marks for providing customer service for incidents whenever they occur. Also, since the time required to adopt the services is short, there are even cases where the services are adopted as a measure while a targeted e-mail attack is already occurring.

Security event monitoring services used to be adopted with the goal of acquiring and storing logs in compliance with internal regulations and other such standards, but recently they have been adopted with increasing frequency in order to proactively detect cyber-attacks. It is possible to detect suspected incidents essentially in realtime by applying optimal detection rules based on past results using large amounts of collected logs. Also, by additionally using support services provided by expert engineers, not only is it possible to greatly reduce the time required to handle incidents after detection, the progression of damage can also be held in check. As a result, the effects of damage are either eliminated or minimized (see Fig. 5).

CONCLUSIONS

This article discussed managed security services, which are a set of comprehensive security measures designed to protect social infrastructures and information systems from increasingly complicated and sophisticated cyber-attacks.

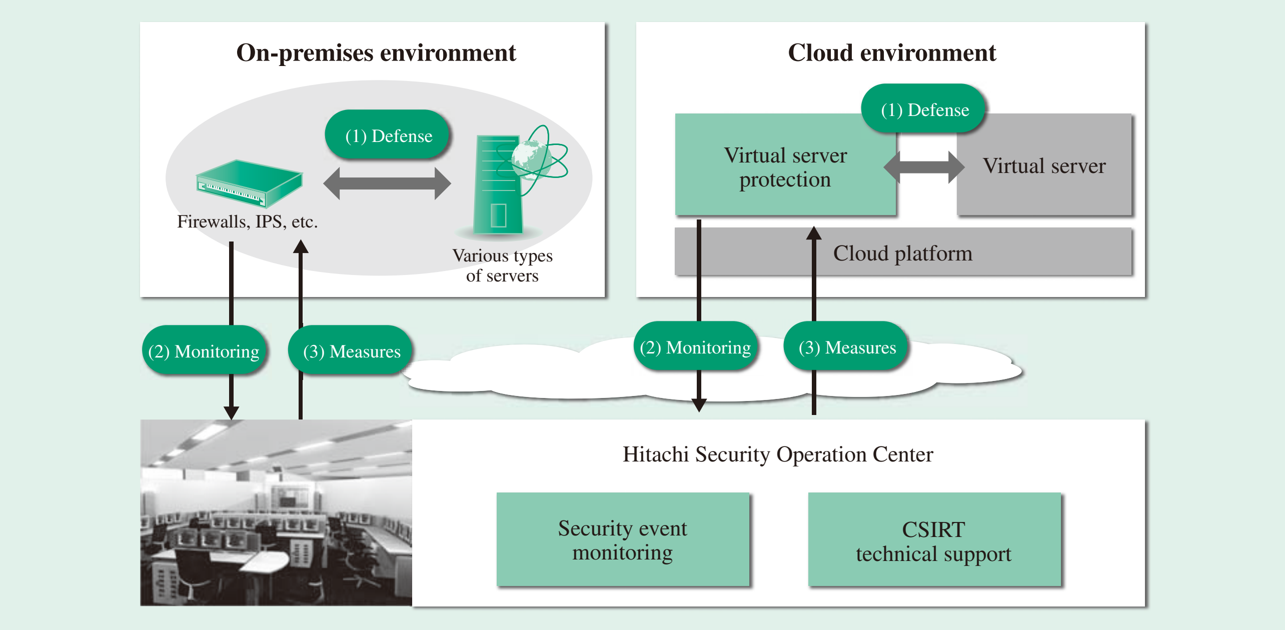


Fig. 5—Security Event Monitoring Service Overview.
These services can be provided for both on-premises and cloud environments. This diagram shows the relationship between defense, monitoring, and measure security operations available as outsourcing services.

Hitachi is itself dealing with a wide range of security issues as a group of companies, from diversifying system environments to cyber-attacks that are growing more advanced. As part of this process, group members with specialized skills use their knowledge to select countermeasures, and the security measures that represent the best practices are implemented. Efforts to expand menu options for managed security services will continue through the utilization of know-how that has actually been applied and the latest technologies. These efforts are aimed at achieving social innovation, and are based on infrastructure technology that has been cultivated over many long years, advanced IT, and security measures. This is why in addition to corporate systems, Hitachi is strengthening security measures that can be applied to social infrastructure systems including control systems as well.

Hitachi will continue to work towards solutions on all sorts of issues in partnership with its customers, thereby contributing to the achievement of a safe and secure society.

REFERENCE

(1) "Information Security Advisory Board: Recommendations to the Ministry of Internal Affairs and Communications Regarding the Promotion of Information Security Policies" (Apr. 2013), http://www.soumu.go.jp/main_content/000217000.pdf in Japanese.

ABOUT THE AUTHORS

Yoshitaka Narishima

Systems Department1, Security Solution Operations, Services Creation Division, Information & Telecommunication Systems Company, Hitachi, Ltd. He is currently engaged in proposal and implementation of security services.

Shinichi Kasai

Systems Department1, Security Solution Operations, Services Creation Division, Information & Telecommunication Systems Company, Hitachi, Ltd. He is currently engaged in proposal and implementation of security services.

Takayuki Sato

Systems Department1, Security Solution Operations, Services Creation Division, Information & Telecommunication Systems Company, Hitachi, Ltd. He is currently engaged in development and proposal, and implementation of security services.

Masaki Mori

Secureplaza Business Promotion Department, Security Solution Operations, Services Creation Division, Information & Telecommunication Systems Company, Hitachi, Ltd. He is currently engaged in sales of security solutions, including security services.

Akihiko Fujita

Network Services Division, Cloud ICT Service Business Group, Hitachi Systems, Ltd. He is currently engaged in development and proposal, and implementation of security services.