# Service Platform Based on the Next-Generation IMS

MISU Toshiyuki, NAKAI Shoichiro, TSUKAMOTO Katsumi,
KURIHARA Hiroshi, KAYAHARA Masayuki, OKABE Toshiya

## Abstract

This paper discusses the next-generation IMS platform, security technology and service delivery platform (SDP). These are required components for the service platforms of the next generation network (NGN), which will form the basis for building NGN services such as the fixed mobile convergence (FMC) and communications broadcasting convergence services.

**Keywords**

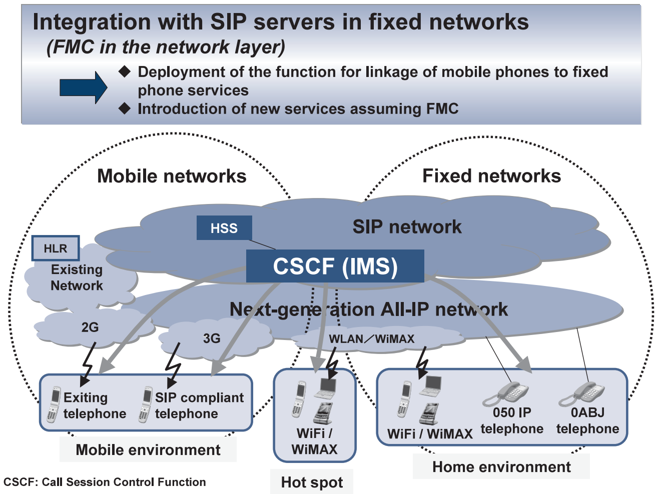
3GPP, IMS, MMD, ALL-IP, NGN, FMC, next-generation SIP server, security technology, SDP (Service Delivery Platform)

## 1. Introduction

The trend of migration to the NGN, and the all-IP restructuring of existing networks into new, IP-based networks has recently been actively making progress among carriers. The background of this trend is the intensification of competition between carriers and a long-term drop in the communications fees. Both fixed and mobile communications carriers are accelerating their endeavors to apply IP networks in order to reduce the network operations costs and to enable the introduction of new services aimed at setting them apart from other communication carriers. Above all, the FMC is expected to be a major source of income for carriers because it offers the possibility of new value-added services based on the linkage of fixed and mobile telephones (**Fig. 1**).

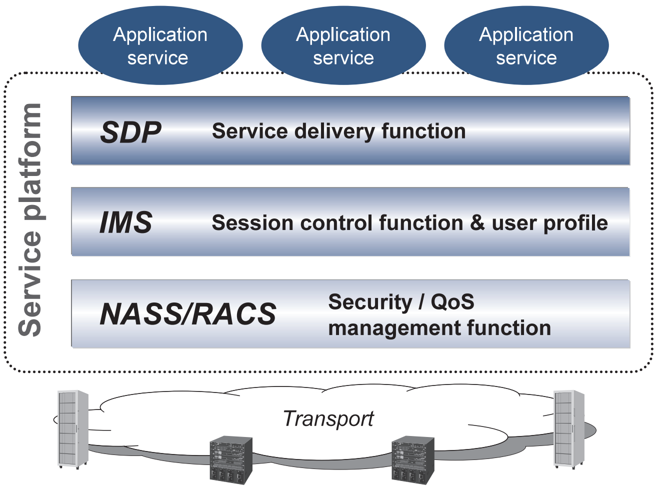
The network services of NGN are implemented via a platform called the IMS (IP Multimedia Subsystem), which is defined by 3GPP/3GPP2 (3rd Generation Partnership Projects). Introduction of the IMS makes it possible to provide IP-based multimedia services for cellular phone and WLAN (Wireless LAN) terminals, independently from the access networks. As the NGN provides services on an architecture common to both the fixed and mobile networks, the role of the software for use in its control system is more and more important.

In this paper, we discuss the characteristics of the service platform that will be implemented based on the IMS. As shown in the image of the NGN assembly in **Fig. 2**, the NGN is com-


Integration with SIP servers in fixed networks
(FMC in the network layer)
◆ Deployment of the function for linkage of mobile phones to fixed phone services
◆ Introduction of new services assuming FMC
Mobile networks
Fixed networks
HSS
SIP network
HLR
Existing Network
CSCF (IMS)
Next-generation All-IP network
2G
3G
WLAN／WiMAX
Exiting telephone
SIP compliant telephone
Mobile environment
WiFi / WiMAX
Hot spot
WiFi / WiMAX
050 IP telephone
0ABJ telephone
Home environment

CSCF: Call Session Control Function
HSS: Home Subscriber Server

Fig. 1 FMC by IMS.


Application service
Application service
Application service
Service platform
SDP
Service delivery function
IMS
Session control function & user profile
NASS/RACS
Security / QoS management function
Transport

**SDP**: Service Delivery Platform
**IMS**: IP Multimedia Subsystem
**NASS**: Network Attachment Subsystem
**RACS**: Resource and Admission Control Subsystem

Fig. 2 Image of the NGN assembly.

posed of security/QoS management functions and service delivery functions centered on the IMS platform. All of these form the service platform for the NGN and are positioned as the core functions of the NGN services.

Later in this paper, we will describe the next-generation SIP server products for the NGN in Section 4, its security technology in Section 5, and its SDP in Section 6.

## 2. NEC's Efforts in Developing VoIP and IMS

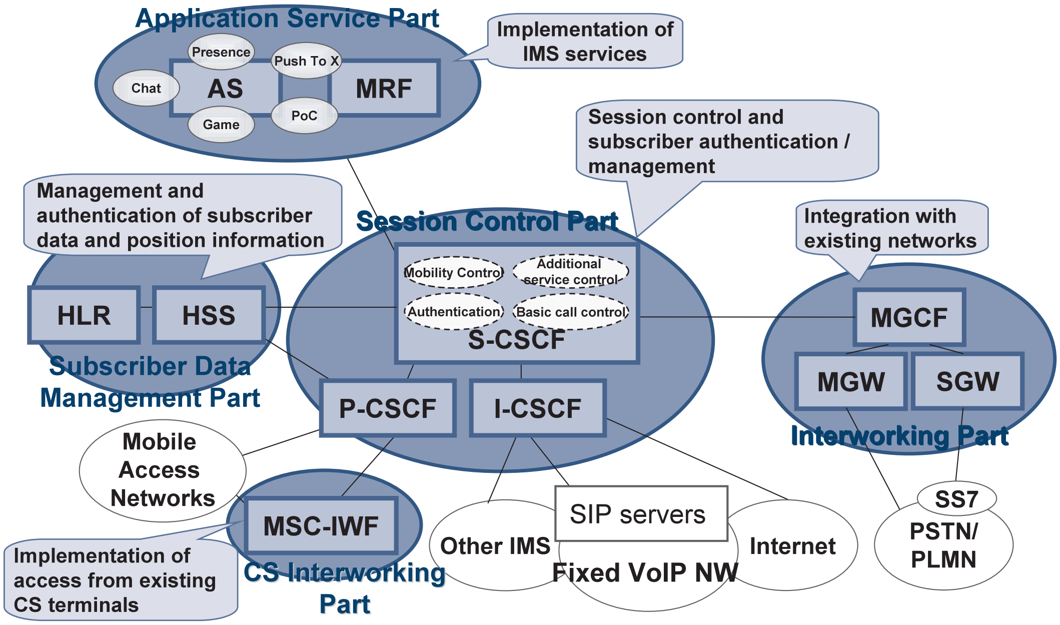
The IMS uses the SIP (Session Initiation Protocol) as the control protocol. In order to incorporate the most advanced IP technology, NEC has developed VoIP products from a very early stage by always considering compliance with the latest SIP-related RFC. In addition, we have led the Japanese market in the introduction of SIP-based products and our products, including SIP servers have gained the No. 1 share in the soft switch market for Japanese carriers (survey by Fuji Chimera Research Institute, Inc.).

In the case of the IMS products, too, we started commercialization very early on and improved the reliability, availability and scalability of the products by inheriting the achievements with SIP servers for fixed networks. Pursuing compliance with standard specifications such as 3GPP/3GPP2, we verified interconnections through trials with multiple carriers and eventually succeeded in commercializing them as the IMS platform infrastructures (**Fig. 3**).

In Section 3, we will introduce the PoC (Push to talk over Cellular) service platform as an example using the IMS platform.

## 3. Construction of PoC Service Platform in Cellular Phone Network

The PoC service provides cellular phones with 1-to-1 or 1-to-N voice exchange communications while assigning speech precedence just as in transceiver or professional radio communications. The first commercial service was begun in 2002 by Nextel (now Sprint Nextel) in the USA. As this has led to commercial ascendancy over competitors, Nextel has attracted attention with its impressive success as a result of the high


Application Service Part
Implementation of IMS services
Presence
Push To X
Chat
AS
MRF
Game
PoC
Session control and subscriber authentication / management
Management and authentication of subscriber data and position information
Session Control Part
Integration with existing networks
Mobility Control
Additional service control
Authentication
Basic call control
S-CSCF
HLR
HSS
MGCF
Subscriber Data Management Part
MGW
SGW
P-CSCF
I-CSCF
Interworking Part
Mobile Access Networks
SS7
MSC-IWF
SIP servers
PSTN/ PLMN
Other IMS
Internet
Implementation of access from existing CS terminals
CS Interworking Part
Fixed VoIP NW

**P-CSCF**: Proxy Call Session Control Function
**I-CSCF**: Interrogating Call Session Control Function
**S-CSCF**: Serving Call Session Control Function
**HSS**: Home Subscriber Server
**HLR**: Home Location Register
**MSC-IWF**: MSC-Interworking Function

**AS**: Application Server
**MRF**: Multimedia Resource Function
**MGCF**: Media Gateway Control Function
**MGW**: Media Gateway
**SGW**: Signaling Gateway

Fig. 3 IMS product lineup of NEC.

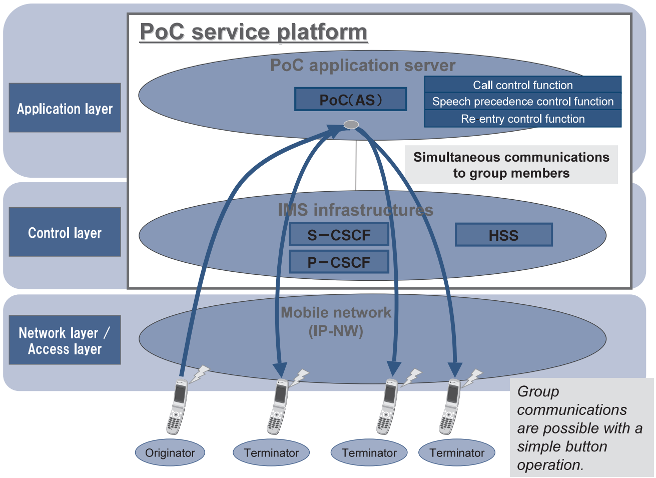

PoC service platform
PoC application server
Application layer
PoC(AS)
Call control function
Speech precedence control function
Re entry control function
Simultaneous communications to group members
Control layer
IMS infrastructures
S−CSCF
P−CSCF
HSS
Network layer / Access layer
Mobile network (IP-NW)
Originator
Terminator
Terminator
Terminator
Group communications are possible with a simple button operation.

Fig. 4 Function blocks of PoC services.

ARPU (Average Revenue Per User) and low cancellation rate. In Japan, a PoC service has been begun since Nov. 2005 as a new communication service that differs from legacy voice service and mail service.

The PoC service platform is composed of the IMS platform that handle the SIP call session control (S-CSCF/P-CSCF) and subscriber information management (HSS) functions, and the application server (PoC (AS)) that provides the “call origination/termination control”, “speech precedence control” and “re-entry control” functions (**Fig. 4**). To ensure flexible expansion of services, the functions that are dependent on the services are concentrated in the application server (PoC (AS)).

### 3.1 Call Origination/Termination Control

The main roles of the PoC (AS) in the call origination/termination control function are as follows.

**(1) Service Authentication**

This function is used for confirmation and authentication at the start of  a PoC service connection request from mobile equipment, such as a validity check of the connected mobile equipment and an upper limit check of the connecting members.

**(2) “Floor” Information Management**

The “floor” is a feature that is opened for managing the PoC service call when it is initiated. It is used for the centralized management of the information on the floor (identifier, opening time, number of members, etc.) and the information of the members entered in the floor (called, joined, separated, etc.). It manages the status of each member and notifies the user of the current status of the other parties of the communication.

**(3) Duplication and Transmission of Message in 1-to-N Communications**

This function duplicates the message from the call-originating mobile equipment and distributes the duplicated messages to all of the call-terminating mobile devices to enable the 1-to-N communication that is one of the innovative features of the PoC service.

### 3.2 Speech Precedence Control

Since the PoC service consists of half duplex communication, it is necessary to control the Speech precedence. The Speech precedence control is performed using the RTCP (RTP Control Protocol) upon receipt of a Speech precedence acquisition request from mobile equipment. It is the management of the user holding the Speech precedence that enables inhibition of other users’ Speech precedence acquisition. The voice data from the mobile equipment holding the Speech precedence is duplicated and distributed to other users using the RTP (Real-time Transport Protocol) in order to enable 1-to-N communications.

### 3.3 Re-Entry Control

The re-entry function allows a user who has exited the floor to re-enter it, if it is continued. This function is required because communications in the mobile environment are sometimes disconnected against the will of the users. When a user requests re-entry to the floor, this function first judges if the floor is continued and connects the user’s mobile equipment to the floor if it is still continued. In addition to the continued existence of the floor, other conditions can also be added for permitting re-entry by adding them according to the service specifications of each carrier.

## 4. Platform Products Supporting NGN

NEC believes that the software platform products for the NGN should meet the following requirements; the first of them is that they provide the services available with the existing circuit switched networks and also in the IP networks with the same high safety and reliability standards, and achieve optimum carrier grade; the second is that the hardware and interfaces that they support are open and comply with the industry standards; the last is that they converge the mobile and fixed networks, and are able to provide FMC compatibility.

We are developing and commercializing the next-generation SIP servers to meet the above requirements (**Fig. 5**).

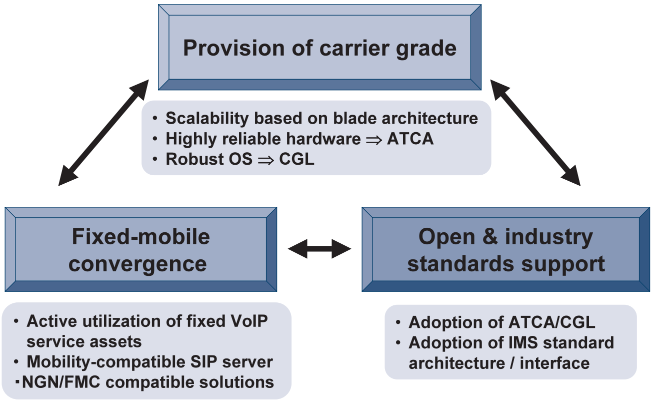

Provision of carrier grade
• Scalability based on blade architecture
• Highly reliable hardware ⇒ ATCA
• Robust OS ⇒ CGL
Fixed-mobile convergence
Open & industry standards support
• Active utilization of fixed VoIP service assets
• Mobility-compatible SIP server
•NGN/FMC compatible solutions
• Adoption of ATCA/CGL
• Adoption of IMS standard architecture / interface

Fig. 5 Concept of next-generation SIP server products.

These products have the following features.

**(1) Inheritance of Already-Approved SIP Software**

The software assets of NEC's SIP servers that have already achieved significant results are inherited to implement next-generation SIP servers with high functionality, high quality and high performance.

**(2) Compatibility with Standardization**

FMC compatibility enables the enhancement of the services based on a close convergence of fixed and mobile networks, by providing compliance with the NGN standard of ITU-T/TISPAN as well as with the IMS/MMD (Multi-Media Domain) standards of 3GPP/3GPP2.

**(3) CG/HA Extension Middleware**

The high-reliability middleware that has achieved powerful results with NEC's past SIP servers is advanced further to implement the CG (Carrier Grade)/HA (High Availability) with high reliability.

**(4) ATCA Platform**

In order to offer high-performance hardware and continual delivery of stable functions, NEC's ATCA (Advanced Telecom Computing Architecture) hardware that has achieved great results is used by providing compliance with the PICMG (PCI Industrial Computer Manufacturers Group) and NEBS (Network Equipment Building System) in addition to existing universal server functions. A blade arrangement is adopted to enable front-panel maintenance design and high scalability. In addition, an independent monitoring module is provided to facilitate replacements in case of failure and enable highly accurate fault monitoring.

**(5) Kernel Manufactured by Monta Vista (MV)**

MV has a highly approved history in the field of embedded Linux. The high-accuracy, high-performance CGL (Carrier Grade Linux) kernel is incorporated and a support system in direct connection with MV is established.

In the future, we will continue to contribute to the creation of new communication modes for the user and the expansion of businesses for communication carriers by providing optimum NGN environments centered around the next-generation SIP servers as well as providing service solutions that are available on the NGN.

## 5. Security Technology in NGN

In the process of the evolution of carrier networks supporting the NGN, it is expected that the subjects and contents of communications will be diversified and the capabilities of networks and terminals will be improved further. The introduction of open technology in the networks will also accelerate and its role will also be changed to that of a service platform incorporating various applications. These changes will increase user convenience and advance the services, but might also involve a risk of more sophisticated security attacks and the consequent serious damage that might be caused by them.

In this context, the roles that the carrier networks should assume for the sake of security can be grouped into the following four areas; 1) strength against malicious users (intentional threats), 2) resistance to errors and accidents, 3) impartiality in service delivery, 4) efficient construction/operation of security systems. While some issues can be solved by improving the method of operations, applying education or preparing legislation, technological countermeasures are essential for improving resistance to malicious users.

Some of the technological countermeasures studied by NEC for improving the attack resistance of the NGN are as follows.

**(1) Behavior-Monitoring IPS**

The behavior-monitoring IPS (Intrusion Prevention System) detects and prevents illegal actions by monitoring the behavior of the programs running on the server. For example, while the maintenance personnel update files after completing the authentication procedure, programs abusing the vulnerability of the OS such as buffer overflow do not execute the authentication procedure. The conduct-monitoring IPS notices this difference in behavior and detects and prevents illegal actions including unknown attacks before they occur.

**(2) Flow Behavior Analysis Technology**

This is an application for applying concept of behavior-monitoring IPS to the network traffic. Illegal traffic has previously been detected by comparing the header information and the payload bit patterns of each packet with the signature, but the flow behavior analysis technology estimates the application based on the information obtained without seeing the contents of each packet, such as the packet size and arrival time interval. It estimates the application using the statistical information and the transition of packet characteristics identified after observation over a certain period. This technology makes it possible to detect applications while maintaining the secrecy of user traffic that is so important in any carrier network, as well as being able to detect P2P (Peer to peer) traffic, disguise of priority traffic such as VoIP and also to detect quality degradation.

**(3) High-Speed Security Engine**

The NGN should accommodate a huge number of terminals as the service platforms, and these terminals should accommodate a wide range of functions including home appliances and sensors. Therefore, the intrusion detection system is required to feature a high performance standard in order to allow the NGN servers to exhibit their full capabilities. The security operation speed is increased by enclosing the functions in the system as hardware while maintaining an open interface flexibility. The specific functions provided in this way are the virus/worm detection function (string search), protocol abnormality detection function (keyword extraction, URI normalization and code conversion) and traffic measuring function (session management and TCP). The fast security engine achieves compatibility between high speed and flexibility by means of an optimum division of functions into hardware and software.

**(4) Mutual Protection**

The border control using a firewall or SBC (Session Border Controller) is effective against illegal access from another carrier network or the Internet, and the end point control using the behavior-monitoring IPS or high-speed security engine is effective against attacks based on internal intrusion by crossing the network border. However, for the NGN to meet security requirements similar to those of traditional telephone networks, it is not enough to execute the control operations referred to above individually. Here, it is effective to introduce the idea of mutual protection. When an attack is blocked at an end point such as a server, this function notifies all of the border protection system components at critical points in the network of the detected information to automatically shut off any subsequent illegal traffic. This function makes it possible to expand the protection range, prevent enlargement of damage, take immediate action after attack detection and localize the damage.

In order to apply quick countermeasures economically, even when the network increases in scale and complexity in the future, it will not be enough to improve the individual countermeasure technologies but it will also be necessary to apply countermeasures more comprehensively by enabling linkages and compatibility.

## 6. Construction of a Service Delivery Platform (SDP) for NGN

For communications carriers and service providers, how to create, develop and introduce outstanding and innovative services efficiently and quickly to the NGN has become an important topic. It is the SDP that is the response to these needs for the development and delivery of such new services. It is attracting attention as a foundation for achieving various functions from the development of services to their introduction, maintenance/administration, and accounting and user management.

Under these circumstances, NEC assumes SDP that pays attention to SIP adopted as a core technology of the NGN to be the SIP-SDP, and is currently commercializing practical SIP application servers using it.

### 6.1 Positioning of SIP-SDP in NGN

**Fig. 6** shows the positioning of the SIP-SDP in the NGN.

The SIP-SDP is a platform belonging to the Application layer and includes the following SIP application servers (ASs).

(1) Call Control AS
(2) Presence AS
(3) Media Control AS

All of these ASs support the SIP, communicate with the

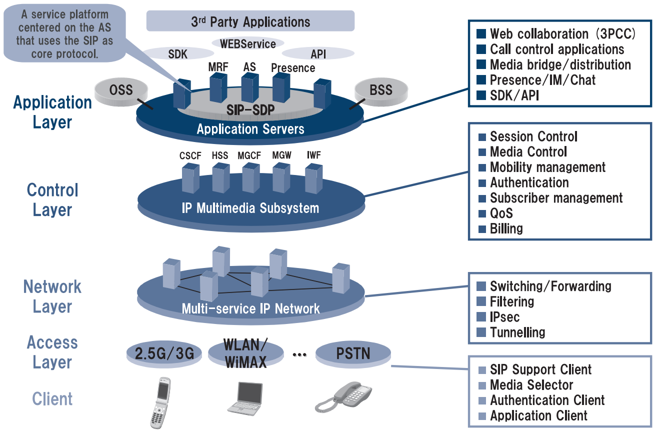


Fig. 6 The SIP-SDP in the NGN.

nodes in the Control layer by means of the SIP and use open APIs to implement convergence with external systems by simple programming or communications interfaces. The APIs are of a basic design that do not permit system awareness of the Control layer configuration or lower-level protocols, thus allowing a larger number of service developers to develop services easily and speedily.

The SIP-SDP realizes the linkage between the IP applications such as job systems or web services on the Internet and the SIP-based communication infrastructure, enabling expansion of the service domain as well as rapid development and delivery of new services.

### 6.2 Features of SIP-SDP

The SIP-SDP has the following features.

**(1) Quick Service Development/Introduction**

Easy-to-use programming APIs and communication APIs such as Java, .NET, XML, HTTP or SOAP are used as the open APIs to increase the development speed of new services to much higher speeds than before.

**(2) Simple Programming**

Complicated SIP call control procedures are hidden so the SIP interface verification and communication testing, which have been necessary every time a service is developed, are no longer required.

**(3) Flexible System Configuration**

Application servers that provide and control services individually are provided at the higher level of the commonly-used SIP application servers (Call Control, Presence, Media Control etc.) This facilitates the addition of services and enables configuration of the system according to the types and scales of services.

### 6.3 SIPHIA as a Call Control AS

The Call Control AS part of the SIP-SDP is implemented using the SIP/Web Collaborator product “SIPHIA.”

SIPHIA was announced and begun to be marketed in October 2004 as a software product providing linkages between standard web application servers and multimedia communication systems that were in compliance with the SIP standard. It offers simple programming APIs that can be handled by many applications programmers without difficulty and allows J2EE/.NET applications to control SIP services such as “1-to-1 communication” and “voice distribution.”

The call control that is performed based on program logic, human operation or event generation in this way is referred to as 3PCC (3rd party Call Control), and SIPHIA is positioned as an SIP application server that provides the 3PCC function (**Fig. 7**).

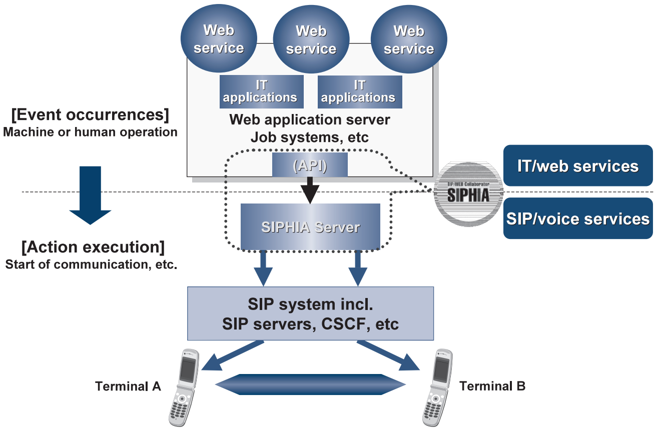


Fig. 7 3PCC functions available with SIPHIA.

The API provided by SIPHIA enables switching and synthesis of a call in progress in addition to basic connection controls. This for instance, enables playback of arbitrary voice guidance for a call in progress and switching of the call for transfer or teleconference calls.

### 6.4 Services Implemented by SIP-SDP

We consider that SIP-SDP plays an important role in the delivery of the NGN services. The PoC services described above are evolving from voice communications to mass-media communications (from “Push to Talk” to “Push to X”) and, from a broader viewpoint, it is also urgently required to construct FMC services that utilize presence and position information and the communications broadcasting convergence services (mobile TV, etc.). The modes of communications are expanding from human-to-human to human-to-object or object-to-object, and from simple communications services to various services that are close to actual lifestyles of people. We will enhance SIP-SDP further by considering the necessity of applying IT technology and ensuring that the secure implementation of such services is taken into full consideration.

## 7. Conclusion

In the above, we discussed the next-generation IMS (IP Multimedia Subsystem) platform, security technology and the SDP (Service Delivery Platform) that are required components for building the service platforms of the NGN. In the future, we will construct various NGN services on these service platforms and position them among our core business operations.

## Authors' Profiles

**MISU Toshiyuki**
Chief Manager,
1st Network Software Division,
Network Software Operations Unit,
NEC Corporation

**NAKAI Shoichiro**
Chief Manager,
1st Network Software Division,
Network Software Operations Unit,
NEC Corporation

**TSUKAMOTO Katsumi**
Senior Manager,
OMCS Operations Unit,
NEC Corporation

**KURIHARA Hiroshi**
Manager,
1st Network Software Division,
Network Software Operations Unit,
NEC Corporation

**KAYAHARA Masayuki**
Assistant Manager,
1st Network Software Division,
Network Software Operations Unit,
NEC Corporation

**OKABE Toshiya**
Assistant Manager,
System Platforms Research Laboratories,
NEC Corporation

●The details about this paper can be seen at the following.
**SIP server CX6820-SS: http://www.sw.nec.co.jp/netsoft/cx6820-ss/**
**SIPHIA: http://www.sw.nec.co.jp/netsoft/SIPHIA/**