Authentication
Access Control
Encryption
Certification

SSCom

SSCom Manual Overview

Hitachi Systems, Ltd.

Introduction

This manual is a brief explanation of SSCom. It also describes the manual that you need to refer to when using the SSCom.

■ Target Readers

It is assumed that you are the following readers:

- Readers who have a basic knowledge about operation of Microsoft Windows.
- Readers who have a basic knowledge about the Internet.
- Readers who have a basic knowledge about computer network.

■ Manual Structure

This manual is organized into the following chapters:

Chapter 1 Overview of SSCom

This chapter is an overview of SSCom.

Chapter 2 System Structure of SSCom

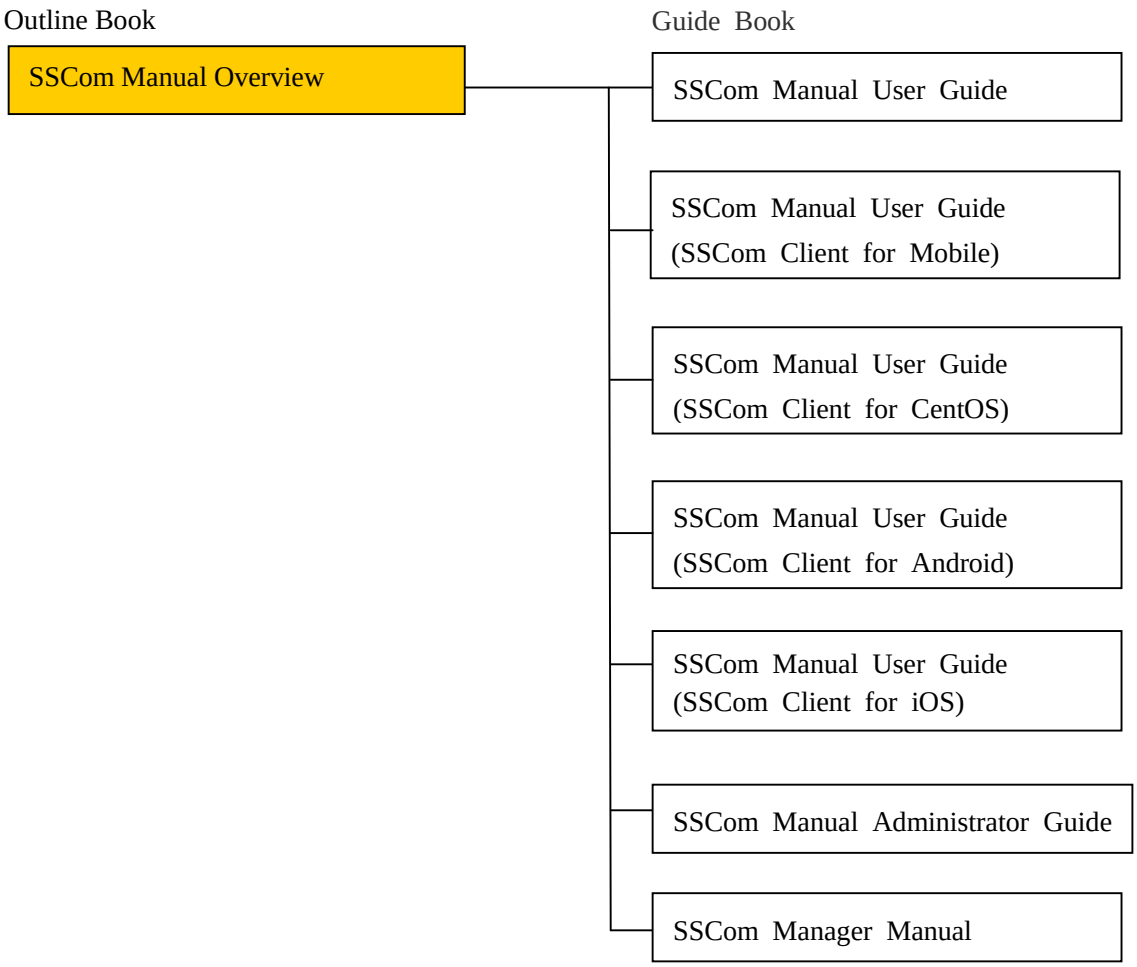
This chapter describes the system structure of SSCom.

Chapter 3 Access Control

This chapter describes Access Control of SSCom.

■ Organization of the Manual

Organization of SSCom Product Manual is shown as follows:



#	Document Name	Classification	Summary
1	SSCom Manual Overview (this manual)	Overview	Overview of SSCom.
2	SSCom Manual User Guide	Guide Book	Describes installation and operation methods of SSCom Client for PC.
3	SSCom Manual User Guide (SSCom Client for Mobile)	Guide Book	Describes installation and operation methods of SSCom Client for Mobile.
4	SSCom Manual User Guide (SSCom Client for CentOS)	Guide Book	Describes installation and operation methods of SSCom Client for CentOS.
5	SSCom Manual User Guide (SSCom Client for Android)	Guide Book	Describes installation and operation methods of SSCom Client for Android.
6	SSCom Manual User Guide (SSCom Client for iOS)	Guide Book	Describes installation and operation methods of SSCom Client for iOS.
7	SSCom Manual Administrator Guide	Guide Book	Describes how to build remote access system by using SSCom.
8	SSCom Manager Manual	Guide Book	Describes the operation method of SSCom Manager.

■ How to read

You can choose the relevant chapters to read by your purpose of using this manual. It is recommended that you refer to specific chapter by your purpose of use.

The Purpose of Reading	Relevant Chapter
Want to know the functions of SSCom.	Chapter 1
Want to know the Operating Environment of SSCom.	Chapter 1
Want to know the system structure of SSCom.	Chapter 2
Want to know the access control mechanism of SSCom.	Chapter 3

■ Description of Notations

Details of product name for notation used in this manual are shown in the following table:

Notation used in this Manual	Official Name
VPN Server	SSCom VPN Server
AP Server	SSCom AP Server
GAC Server	SSCom GAC Server
Windows 2003	Microsoft Windows Server 2003
Windows Vista	Microsoft Windows Vista
Windows 7	Microsoft Windows 7
Windows 8 / 8.1	Microsoft Windows 8 / 8.1
Windows 2008	Microsoft Windows Server 2008
Windows 2012	Microsoft Windows Server 2012
CentOS	CentOS 5.5(x86)

▪ Windows Vista, Windows 7, Windows 8 / 8.1, Windows 2008 are collectively referred to as Windows in this manual.

▪ Windows 2003, Windows 2008, Windows 2012 are collectively referred to as Windows Server in this manual.

▪ SSCom Client, SSCom Client for CentOS, SSCom Client for Android, SSCom Client for iOS, SSCom Client for Mobile are collectively referred to as SSCom Client in this manual.

■ Description of Abbreviations

Details of abbreviations used in this manual are shown in the following table:

Abbreviation	Official Name
CA	Certificate Authority
CRL	Certificate Revocation List
DN	Distinguished Name
DNS	Domain Name System
HTTP	HyperText Transfer Protocol
IP	Internet Protocol
LDAP	Lightweight Directory Access Protocol
SSL	Secure Socket Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
URL	Uniform Resource Locator
VPN	Virtual Private Network
RDP	Remote Desktop Protocol

■ Matters that need attention in export

The product is among the strategic materials and technology which meets all the stipulations of foreign exchange and foreign trade law.

Please make sure related formalities be followed based on observing relevant laws when exporting the product (including bringing it to foreign countries from Japan, or presenting it to non-domestic residents).

If you have any questions, please contact the purchasing agency of this product.

■ Trademark

All company names, brand names and product names recorded in this manual are registered trademark of each company.

■ Notes

▪ This manual does not record any machinery products or program products required when using the software. If there is a need, please refer to other supporting manuals.

▪ This manual subjects to change without prior notice.

Table of Contents

1

1. Overview of SSCom

SSCom is a kind of software that encrypts the communication between client and the server, so as to prevent important information from being stolen by malicious third party in network transmission.

This chapter is an overview of SSCom.

<Chapter Structure>

1.1 Function Overview

SSCom is a kind of software that encrypts the communication between client and the server, so as to protect important information from malicious third party in network transmission. At the same time, intensified security can be realized both internally and externally to the company through user authentication, access control, certificate and authentication device. For example, if you want to access important internal documents from outside the company, using SSCom can ensure you of safe access by eliminating security threats.

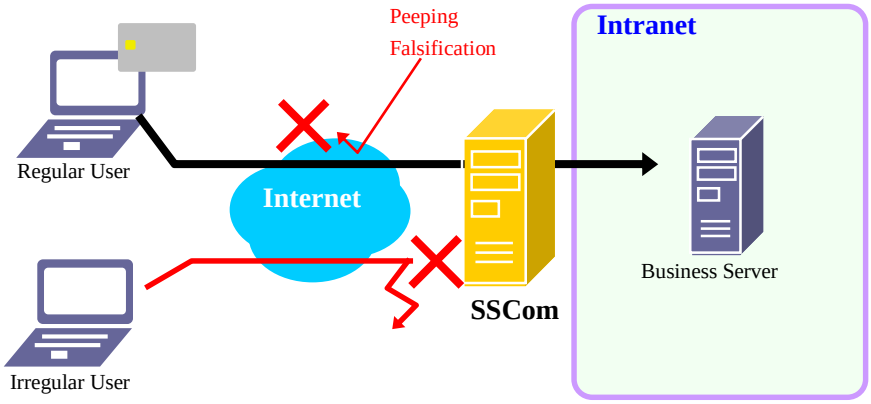


Fig1.1-1 Overview of SSCom

1.2 Features of SSCom

SSCom realizes intensified security both internally and externally to the company through the following features:

(1) Encrypted Communication

The communications between the client and server are encrypted by industry-standard SSL, so as to realize communication by VPN. Even communications channel with less-safety such as the Internet can realize safe transmission. AES (256 bit) can be used to achieve the strongest encryption, so it can also be applied to business dealing with important information such as financial and health care.

It can provide support from both company LAN connection and remote connections respectively. Meanwhile, by building Extranet, it helps to access business server from other places on business trips and prevents members-only information from being intercepted.

* Communications supported by SSCom are those TCP/IP communications which established from the client side.

(2) Access Control

Combined with authentication by certificate, it sets up access control to any servers that can be identified by IP address and port numbers. In the case of Web server, you can specify the control of a per-directory basis.

Users that can have access to information can be specified not only by specific person and group, but also the department and position the user belongs, or lay limits on content that can be accessed by different travel places. Different access limits can also be set according to connection source addresses.

(3) User Authentication by Certificate

It recognizes the users' identity by certificate issued to each of them. In this way, malicious third party can be prevented from acting as authorized users.

(4) Prevent Unauthorized Use of Authentication Information

The certificate is kept in IC card or other authentication device, so as to prevent the leak and unauthorized use of authentication information such as ID/Password and so on.

(5) Integrated Management

The necessary information for user information and access control of the SSCom user is integrated managed by the directory server. It helps to reduce the burden of operational management.

1.3 Product Composition of SSCom

SSCom consists of the following products:

- SSCom Client
- SSCom VPN Server
- SSCom AP Server
- SSCom GAC Server
- SSCom Manager
- SSCom CA/Lite
- Key Management Tools

Encrypted communication channel between SSCom Client running on client PC and SSCom VPN/AP Server is established, enabling communication between client and business server through the encrypted communication channel, so as to ensure smooth and safe data information transmission between them.

SSCom GAC Server can execute integrated management on information in user authentication and access control, and deal with authentication requests from SSCom VPN Server and SSCom AP Server.

Besides the products above mentioned, as the database for saving user authentication information and access control information, SSCom GAC Server needs the directory server. (The directory server is bundled together with SSCom Lite.)

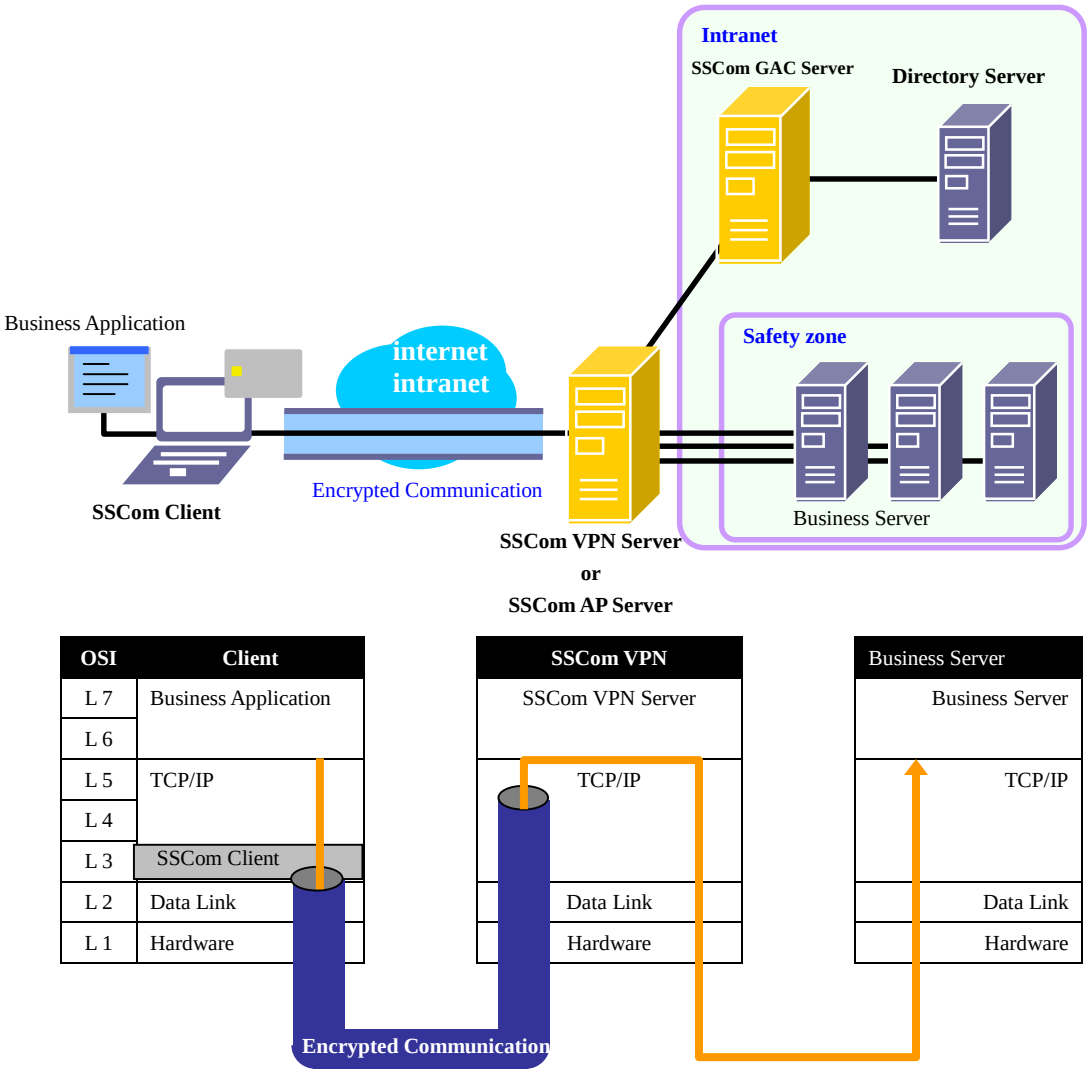


Fig.1.3-1 Product Composition of SSCom

1.3.1 SSCom Client

It is the software running on the client PC, establishes encrypted communication channel between the client and SSCom VPN/AP Server.

SSCom Client does the following process:

- SSCom Client establishes encrypted communication channel with SSCom VPN/AP Server.
- While establishing the encrypted communication channel with SSCom VPN/AP Server, SSCom Client sends certain user certificate saved in the authentication device of the client PC to SSCom VPN/AP Server to conduct personal authentication.
- Whether the SSCom Server is reliable depends on the server certificate it issues.
- Password needed in using authentication device can be modified.

1.3.2 SSCom VPN Server

It deals with encryption communication and network access control when external users trying to access the Intranet. Configured in the entrance of the Intranet, it controls access from the external network.

While the communication between SSCom Client and SSCom VPN Server is enabled, all the TCP/IP communications are sent to SSCom VPN Server, creating the same environment as company Intranet.

SSCom VPN Server does the following process:

- SSCom VPN Server establishes encrypted communication channel with SSCom Client.
- It performs personal authentication through user certificate sent from SSCom Client.
- It controls on per user access from external network to company Intranet.
  - (*)Proceed access control (IP address, port unit) on each business server.
  - (*)Access right control can be conducted through one SSCom VPN Server to several business servers.
  - (*)Access Control is performed according to attributes of each group (multiple users are integrated in a group to realize unified management) and each individual. (subordinate departments, position, etc.)
- DNS Naming Resolution of the SSCom Client is designated to the SSCom VPN Server, thus realize Naming Resolution on internal DNS Server.

■Attention ■

SSCom VPN Server doesn't function as firewall. Therefore, access to SSCom VPN Server must be reached through the Internet by firewall (or equivalent function).

1.3.3 SSCom AP Server

It is the software that runs on the front of Web server and takes on encryption communication and access control, and it controls access to Web contents by URL unit.

SSCom Client initiates communication to SSCom AP Server and accesses Web content according to relative access right.

SSCom AP Server does the following process:

- It performs personal authentication through user certificate sent from SSCom Client.
- It performs access control measured in URL to Web content to each user.
  (*)Access Control can be conducted through one SSCom AP Server to several business servers.
  (*)Access Control can be performed according to attributes of each group (multiple users are integrated in a group to realize unified management) and each individual (subordinate departments, position, etc).

1.3.4 SSCom GAC Server

SSCom GAC Server manages information on personal authentication and access control. Both SSCom VPN Server and SSCom AP Server rely on the SSCom GAC Server to realize integrated information management on personal authentication and access control.

SSCom GAC Server does the following process:

- It performs integrated information management on personal authentication and access control.
- Access Control can be committed not only on each user, but also on group (Group Access Control). Besides, flexible control can be conducted by the attributes of each users (subordinate departments, position, etc).
- Communication between SSCom GAC Server and SSCom VPN/AP Server can also be realized by encryption and server authentication.
- Multiple SSCom VPN/AP Server can be managed by one SSCom GAC Server.
- SSCom GAC Server conducts unified accumulation on log to all SSCom VPN/AP Server.

1.3.5 SSCom Manager

SSCom Manager is a Web system that performs overall management required personal authentication, access control Settings, and certificate issuance and management for using SSCom. The following can be realized by using the SSCom Manager:

- User Information Management
  Register and manage the users with granted access.

- Issuance and Invalidation of the Certificate
  The certificate of the SSCom user can be issued or invalidated.

- Group Information Management
  Register the groups with granted authority, and users belonging to the groups. Can be set access control by group.

- Server Information Management
  Register the business server with granted authority, as well as the SSCom Server.

1.3.6 SSCom CA/Lite

SSCom CA/Lite is a system that issues or invalidates certificate on the Web. It issues certificates according to standard specifications X.509. Please refer to "SSCom Manager Manual" for details.

1.3.7 Key Management Tool

It is a tool that manages server certificates of each SSCom product. This tool is standardly attached to each product of SSCom. Please refer to "SSCom Manual Administrator Guide" for details.

1.4 Operating Environment of SSCom

Operating environment of each SSCom product is described as follows:

1.4.1 Operating Environment of SSCom Client

The table below shows the Operating Environment of SSCom Client:

Table 1.4.1-1 Operating Environment of SSCom Client

OS Supported	Windows Vista Business for Japanese edition Windows Vista Enterprise for Japanese edition Windows 7 All Editions for Japanese edition Windows 8 / 8.1 All Editions for Japanese edition
CPU	1GHz or higher recommended
RAM	Minimum 256MB/512MB or higher recommended
Hard Disk	Free space 20MB or higher
Device Supported * 1	IC card Reader: PC/SC (Delay type/PC card type)
Authentication Device Supported	■ MULTOS(contact type IC card) * 2 ■ TOSMART(contact type IC card) ■ eToken PRO(USB token) ■ FeliCa (non-contact type IC card) ■ Crypto API Device Supported
Browser Supported * 3	Internet Explorer 7.0 / 8.0 / 9.0 / 10.0 / 11.0* 4
Application Supported	Applications meet the following conditions: i. Client-Server applications that use TCP/IP of Winsock. ii. Applications that launch communication from client side.
Protocol Supported	TCP/IP
Other conditions	・Not be used with other server products containing SSCom on the same computer at the same time. ・Spare USB interface needed to connect the authentication device . ・Authentication device to be used on operating system that supports it.

* 1: For details about authentication devices which finished test, please refer to the SSCom site.
-> http://www.hitachi-systems.com/solution/s002/sscom/
* 2: Date access application supported MULTOS is necessary.
* 3: It is necessary when using Web authentication function.
* 4: Compatible mode of IE7.0 should be configured.

1.4.2 Operating Environment of SSCom Client for CentOS

The table below shows the Operating Environment of SSCom Client for CentOS:

Table1.4.2-1 Operating Environment of SSCom Client for CentOS

OS Supported	CentOS 5.4 / 5.5
CPU	1GHz or higher recommended
RAM	Minimum 256MB/512MB or higher recommended
Hard Disk	Free space 20MB or higher
Protocol Supported	TCP/IP
Other Conditions	・Not be used with other server products containing SSCom on the same computer at the same time.

1.4.3 Operating Environment of SSCom Client for Android

The table below shows the Operating Environment of SSCom Client for Android:

Table1.4.3-1 Operating Environment of SSCom Client for Android

OS Supported	Android 2.1 / 2.2 / 2.3 / 3.0 / 4.0
Protocol Supported	RDP

1.4.4 Operating Environment of SSCom Client for iOS

The table below shows the Operating Environment of SSCom Client for iOS:

Table1.4.4-1 Operating Environment of SSCom Client for iOS

OS Supported	iOS 4.2 / 4.3 / 5.0 / 5.1 / 6.0
Protocol Supported	RDP

1.4.5 Operating Environment of SSCom Client for Mobile

The table below shows the Operating Environment of SSCom Client for Mobile:

Table1.4.5-1 Operating Environment of SSCom Client for Mobile

OS Supported	Windows Mobile 6.0 / 6.1 Professional Windows Mobile 6.0 Classic
Protocol Supported	TCP/IP

1.4.6 Operating Environment of SSCom VPN Server

The table below shows the Operating Environment of SSCom VPN Server:

Table1.4.6-1 Operating Environment of SSCom VPN Server

OS Supported	(1)SSCom Lite Windows Server 2003 R2 Standard Edition SP2 Windows Server 2008 Standard Edition SP2 Windows Server 2008 R2 Standard Edition SP1(x64) Windows Server 2012 Standard Edition(x64) (2)Other than SSCom Lite Oracle Solaris 9(sparc) Oracle Solaris 10(sparc) Windows Server 2003 R2 Standard Edition SP2 Windows Server 2008 Standard Edition SP2 Windows Server 2008 R2 Standard Edition SP1(x64) Windows Server 2012 Standard Edition(x64) CentOS 5.4 / 5.5(x86)
CPU	2GHz or higher recommended
RAM	Minimum 512MB/1GB or higher recommended
Hard Disk	Free space 1GB or higher (increase by log size)

* 1: Other than described as x64 about Windows, it's 32bit Windows.

■Attention■

Required memory space varies according to different operating system environments.

1.4.7 Operating Environment of SSCom AP Server

The table below shows the Operating Environment of SSCom AP Server:

Table1.4.7-1 Operating Environment of SSCom AP Server

OS Supported * 1	Oracle Solaris 9(sparc) Oracle Solaris 10(sparc) Windows Server 2003 R2 Standard Edition SP2 Windows Server 2008 Standard Edition SP2 Windows Server 2008 R2 Standard Edition SP1(x64) Windows Server 2012 Standard Edition(x64) CentOS 5.4 / 5.5(x86)
CPU	2GHz or higher recommended
RAM	Minimum 512MB/1GB or higher recommended
Hard Disk	Free space 1GB or higher (increase by log size)

* 1: Other than described as x64 about Windows, it's 32bit Windows.

■Attention■

Required memory space varies according to different operating system environments.

1.4.8 Operating Environment of SSCom GAC Server

The table below shows the Operating Environment of SSCom GAC Server:

Table1.4.8-1 Operating Environment of SSCom GAC Server

OS Supported * 1	(1)SSCom Lite Windows Server 2003 R2 Standard Edition SP2 Windows Server 2008 Standard Edition SP2 Windows Server 2008 R2 Standard Edition SP1(x64) Windows Server 2012 Standard Edition(x64) (2)Other than SSCom Lite Oracle Solaris 9(sparc) Oracle Solaris 10(sparc) Windows Server 2003 R2 Standard Edition SP2 Windows Server 2008 Standard Edition SP2 Windows Server 2008 R2 Standard Edition SP1(x64) Windows Server 2012 Standard Edition(x64) CentOS 5.4 / 5.5(x86)
CPU	2GHz or higher recommended
RAM	Minimum 512MB/1GB or higher recommended
Hard Disk	Free space 1GB or higher (increase by log size)
Directory Server	Sun Java(TM) System Directory Server 3.x / 4.x / 5.0, 5.1, 5.2 / 6.3 / 7.0 OpenLDAP

* 1: Other than described as x64 about Windows, it's 32bit Windows.

■Attention■

Required memory space varies according to different operating system environments.

1.4.9 Operating Environment of SSCom Manager

The table below shows the Operating Environment of SSCom Manager:

Table1.4.9-1 Operating Environment of SSCom Manager

OS Supported * 1	Windows Server 2003 R2 Standard Edition SP2 Windows Server 2008 Standard Edition SP2 Windows Server 2008 R2 Standard Edition SP1(x64) Windows Server 2012 Standard Edition(x64)
CPU	2GHz or higher recommended
RAM	Minimum 512MB/1GB or higher recommended
Hard Disk	Free space 1GB or higher (increase by log size)
Web Server	Windows 2003 : Internet Information Services 6.0 Windows 2008 : Internet Information Services 7.0/7.5 Windows 2012 : Internet Information Services 8.0 (Compatibility mode of IIS6.0 should be configured with Windows 2008 / Windows 2012. Please refer to the configuration steps in "SSCom Manual Administrator Guide ")
.NET Framework	.NET Framework 2.0 SP2 .NET Framework 3.0 SP1 .NET Framework 3.5 SP1 .NET Framework 4.5
Browser Supported	Internet Explorer 7.0 / 8.0 / 9.0 / 10.0 * 2

* 1: Other than described as x64 about Windows, it's 32bit Windows.

* 2: Compatible mode of IE7.0 should be configured.

1.4.10 Operating Environment of SSCom CA/Lite

The table below shows the Operating Environment of SSCom CA/Lite:

Table1.4.10-1 Operating Environment of SSCom CA/Lite

OS Supported * 1	Windows Server 2003 R2 Standard Edition SP2 Windows Server 2008 Standard Edition SP2 Windows Server 2008 R2 Standard Edition SP1(x64) Windows Server 2012 Standard Edition(x64)
CPU	2GHz or higher recommended
RAM	Minimum 512MB/1GB or higher recommended
Hard Disk	Free space 1GB or higher (increase by log size)
Web Server	Windows 2003 : Internet Information Services 6.0 Windows 2008 : Internet Information Services 7.0/7.5 Windows 2012 : Internet Information Services 8.0 (Compatibility mode of IIS6.0 should be configured with Windows 2008 / Windows 2012. Please refer to the configuration steps in "SSCom Manual Administrator Guide ")
.NET Framework	.NET Framework 2.0 SP2 .NET Framework 3.0 SP1 .NET Framework 3.5 SP1 .NET Framework 4.5
Browser Supported	Internet Explorer 7.0 / 8.0 / 9.0 / 10.0 * 2

* 1: Other than described as x64 about Windows, it's 32bit Windows.

* 2: Compatible mode of IE7.0 should be configured.

1.4.11 Operating Environment of Key Management Tool

It's operating environment is same as each SSCom Server. The tool is running on the same server with SSCom VPN/AP/GAC Server.

This page is blank.

2

2. System Structure of SSCom

This section describes basic systematic structure of SSCom.

<Chapter Structure>

2.1 VPN Communication (Remote Access)

2.2 Web Authentication Function

2.1 VPN Communication (Remote Access)

SSCom VPN Server is configured at the interface between company Intranet and external network, so as to limit access from the outside.

The following functions are realized:

- User authentication is practiced by certificates to restrict users who can access to it.
- Restricted access to server by each user and group can be realized through IP address and port number.
- Encrypt the communication channel between SSCom Client and SSCom VPN Server.
- Business applications can be accessed by internal IP address.
- DNS name resolution can be executed by the DNS server in the company.
- Access of multiple business servers can be managed through one single SSCom VPN Server.

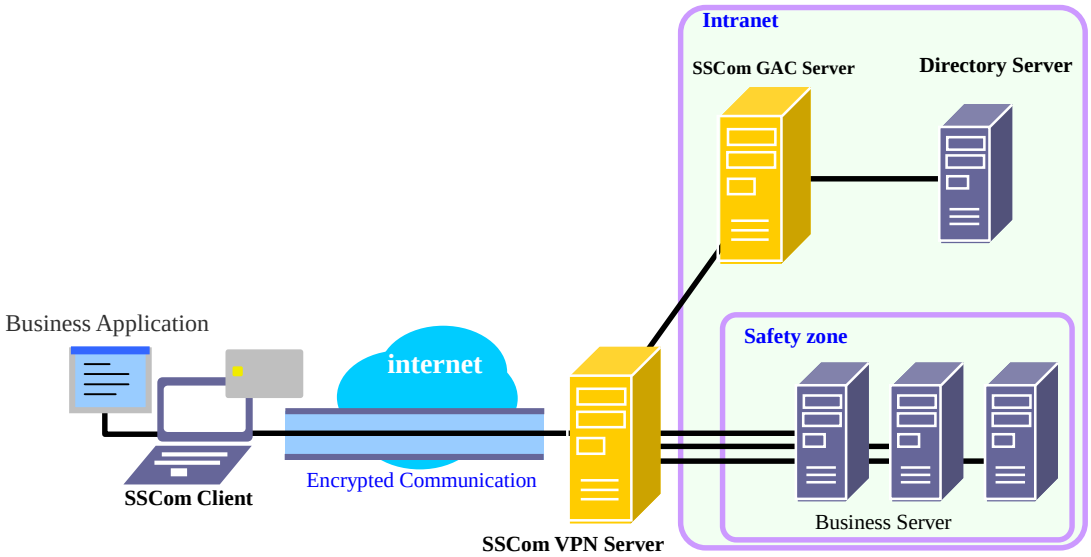


Fig 2.1-1 System Example of Remote Access by VPN communication

Access by the following steps:

1. When SSCom Client detects communication signals from business applications, it connects to SSCom VPN Server by certificates in the authentication device. If this authentication device has been set up a password, it is required to enter the password.
2. SSCom VPN Server sends a request to SSCom GAC Server to confirm the "user authentication" and "access right".
3. SSCom GAC Server checks the "user authentication" and "access right" by the information saved in the directory server and sends the result to SSCom VPN Server.
4. If both "user authentication" and "access right" are passed, SSCom VPN Server can establish connection with business Server. (If not allowed, communication would be cut off.)
5. Based on then communication channel between SSCom Client and SSCom VPN Server in step 1 and communication channel between SSCom VPN Server and business Server in step 4, a series of communication has been established between the PC Client and business server. Communication between the business applications and business server flows through this channel.

Please pay attention to the following points with the system configuration:

- VPN communication can be conducted only when the VPN communication function of SSCom Client is effective.
- Business applications have the same access right as internal IP address system.
- In VPN communication, the source address of packet that connects business server is the address of SSCom VPN Server. Please note this point when access control in business server is implemented by IP address.
- SSCom VPN Server does not have the function of firewall. Please make sure that the firewall function be set up between SSCom VPN Server and the Internet.

2.2 Web Authentication Function

As SSCom AP Server is set up between Web server and Intranet, Access to Web contents can be controlled by folder unit.

The following functions are realized:

- Access Control on each user or group to Web contents can be controlled on folder-unit basis.
- To limit the user access by authentication with user certificate.
  * Also support authentication by ID/PW.
- Communication channel between SSCom Client and SSCom AP Server is encrypted.

SSCom AP Server executes Web authentication function through the following 3 approaches:

- Single Approach
  It refers to the one-to-one correspondence between SSCom AP Server and Web server. Users access IP address of SSCom AP Server through Web browser.

- Reversed Proxy Approach
  It is a way of one SSCom AP Server managing multiple Web servers. The Web server that you want to access can be recognized by the path of the URL.

- Virtual Host approach
  It is a way to manage multiple Web servers with one SSCom AP Server. The Web server that you want to access can be recognized by the host name specified in the URL.

2.2.1 Single Approach

It refers to the one-to-one correspondence between SSCom AP Server and Web server. Users access IP address of SSCom AP Server through Web browser.

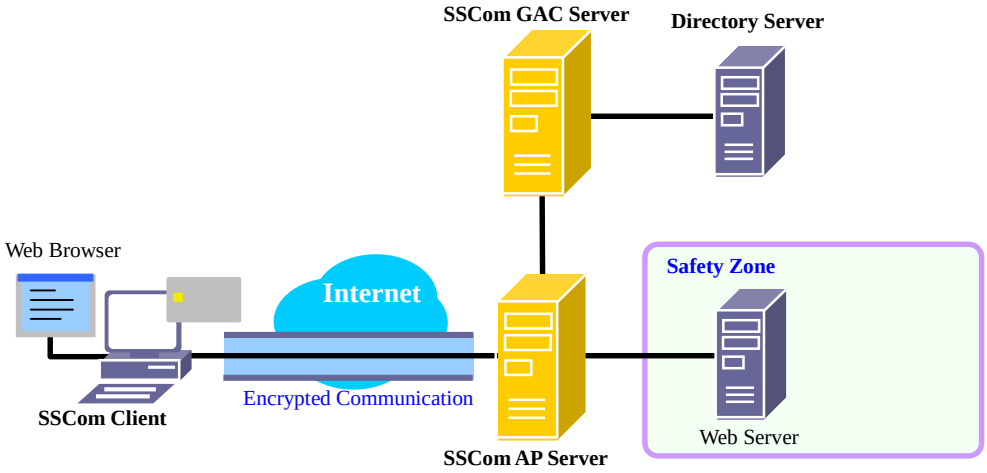


Fig.2.2.1-1 System configuration example to use Web Authentication Function (Single Approach)

Access by the following steps:

1. When SSCom Client detects communication signals from Web browser, it connects to SSCom AP Server by using certificates in the authentication device.
   * In the case of authentication by ID / PW, an authentication request of ID / PW will be performed when accessing the address of SSCom AP Server.
2. SSCom AP Server sends a request to SSCom GAC Server to confirm the "user authentication" and "access right".
3. SSCom GAC Server checks the "user authentication" and "access right" by the information saved in the directory server and sends the result to SSCom AP Server.
4. If both "user authentication" and "access right" are passed, SSCom AP Server establishes connection with the Web server. (If not allowed, communication would be cut off.)
5. Based on communication channel between SSCom Client and SSCom AP Server in step 1 and communication channel between SSCom AP Server and Web server in step 4, a series of communication channel have been established between the PC Client and Web server. Communication between the Web server and Web browser flows right through this channel.

Please pay attention to the following points when building the system:

- Web authentication can be conducted only when the Web authentication function of SSCom Client is effective.
- While the Web browser accessing to the Web server, IP address and port number of the SSCom AP Server will be specified.
- It is necessary to change the proxy setting of Web browser on the client side to use this function.

2.2.2 Reversed Proxy Approach

It is a way of one SSCom AP Server managing multiple Web servers. The Web server that you want to access can be recognized by the path of the URL.

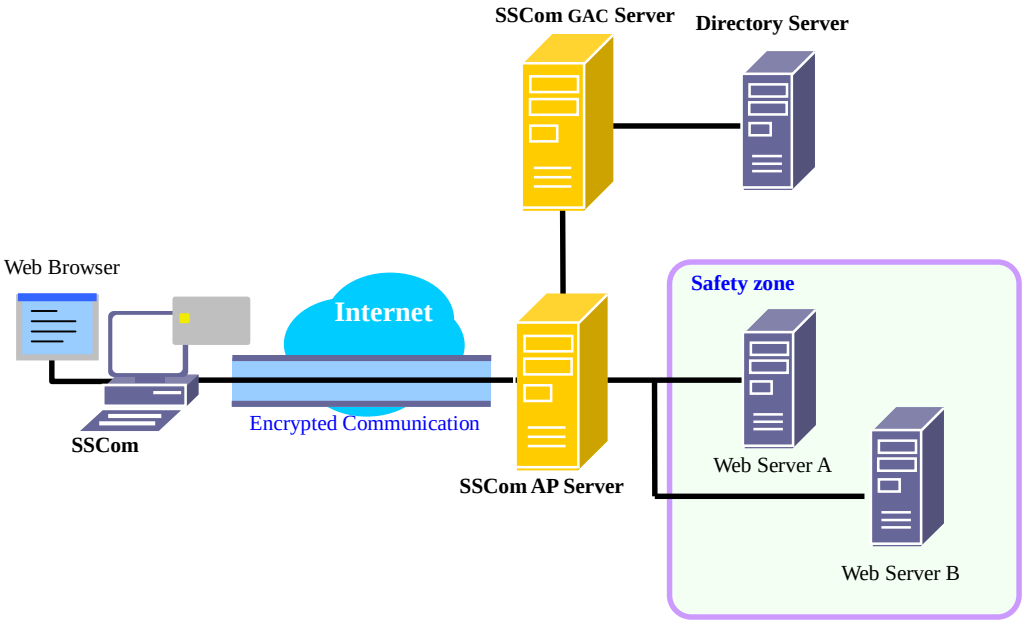


Fig.2.2.2-1 System configuration example to use Web Authentication Function (Reversed Proxy Approach)

The flow of authentication and access control is the same with the Single Approach.
When the Web browser connects Web server, specify the format of URL as follows:

https://"IP address of SSCom AP Server"/ "host name of Web server*"/*

The host name of Web server is used for SSCom AP Server to recognize Web servers. Please use the SSCom Manager to define the Web server's IP address, port number and host name.

2.2.3 Virtual Host Approach

It is a way to manage multiple Web servers with one SSCom AP Server. The Web server that you want to access can be recognized by the host name specified in the URL.

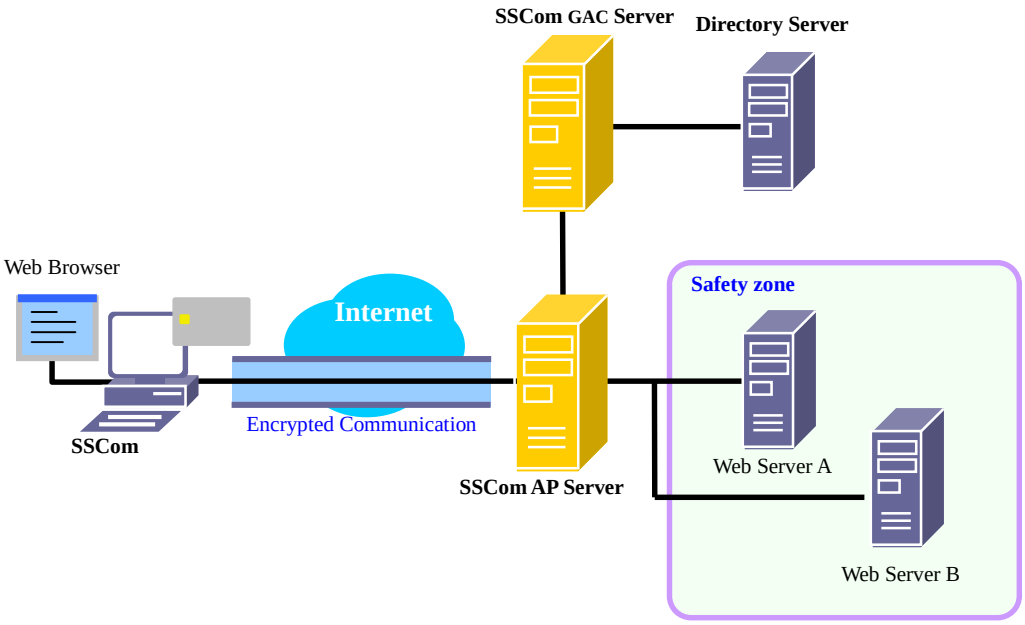


Fig.2.2.3-1 System configuration example to use Web Authentication Function (Virtual Host Approach)

The flow of authentication and access control is the same with the Single Approach.
When the Web browser connects Web server, specify the format of URL as follows:

https:// "host name of Web server"/

The host name of Web server is used for SSCom AP Server to recognize Web servers. Please use the SSCom Manager to define the Web server's IP address, port number and host name. In addition, to show IP address of SSCom AP Server, please edit "hosts" file on PC client.

This page is blank.

3

3. Access Control

This chapter describes Access Control of SSCom.

<Chapter Structure>

3.1 Overview of Access Control

3.2 Requisite Definitions on Access Control

3.3 Detailed Contents of Access Control

3.1 Overview of Access Control

SSCom can impose control on user's authority to access business server (defined by port number and IP address). Users and groups which have access right to each business server can be registered through access control. The access control has high flexibility and various conditions can be defined. SSCom Manager is used to define access rights.

Access Control realized by SSCom is described as follows:

- Access right can be granted on a per-user basis.
- Multiple users are defined in groups and access right can be granted by groups. The same user can be registered into more than one group.
- User information such as subordinate department or position can be set as conditions of access control. Flexible definition can be done by the combination of multiple conditions.
- Access right can be used in any combination of user unit, group unit and conditions.
- Access right of the same user can be adjusted by access locale: inside or outside the company.
- For Web directory, access right can be changed on URL-unit basis.

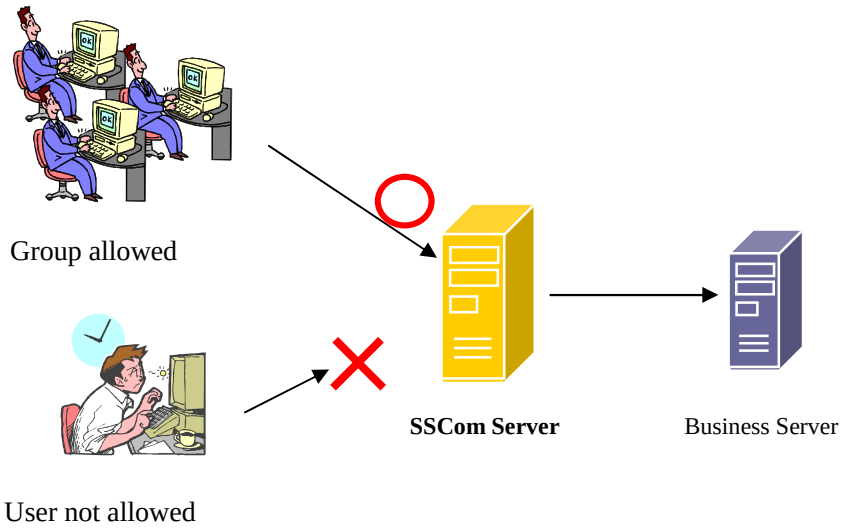


Fig.3.1-1 Overview of Access Control

3.2 Requisite Definitions on Access Control

3.2.1 User Definition

(1) Overview of User Definition

User information (name or subordinate department) is registered to directory server by using SSCom Manager. SSCom can do access control by the user information.

As user certificate in the authentication device records only personal ID (Common Name) information, if the user information changes, you just need to do related modification job in the directory server.

(2) Attributes of User Definition

Information such as user name and subordinate department can be set as attributes. Attributes can also be customized. For detailed contents of attributes which can be defined, please refer to "SSCom Manager Manual".

3.2.2 Group Definition

(1) Overview of Group Definition

Multiple users can be divided into groups and access right can be granted to group. Group information is registered into directory server by using SSCom Manager.

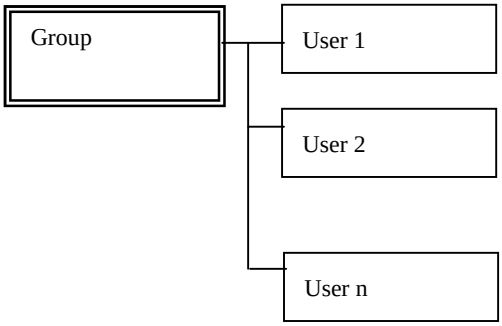
"Disclosure Target Group" can be used in Group Definition, which is a group for granting access right.

(2) Attributes of Group Definition

Unique group name can be set to groups.

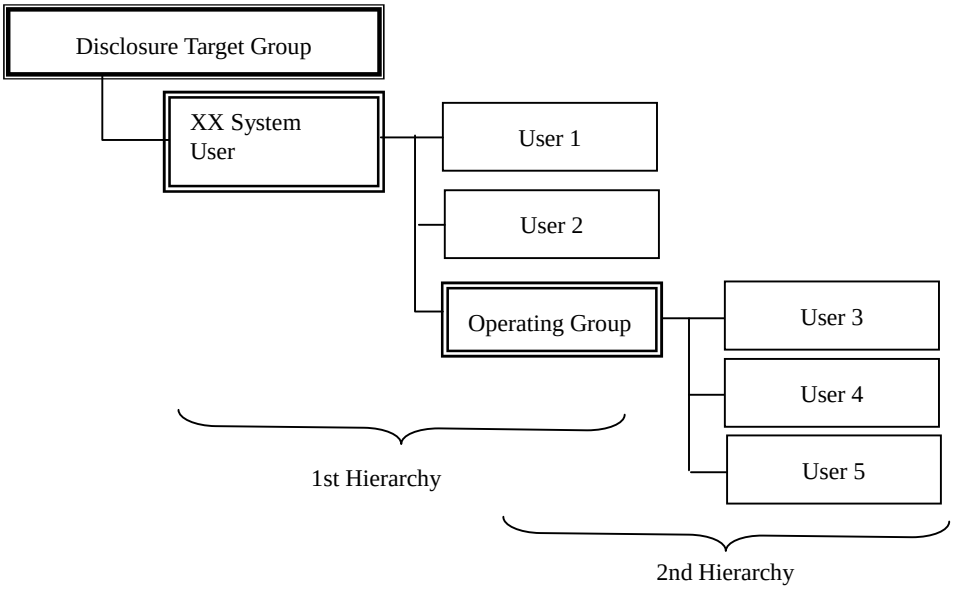
(3) Group Structure

Multiple users can be registered in one group.



In the "Disclosure Target Group", other groups can be registered to a group, and it can be managed hierarchically. You can register up to a maximum of 10 hierarchies.

Access right granted to the upper layer group will be inherited by the lower layer ones.



3.2.3 Server Definition

(1) Overview of Server Definition

SSCom Manager can be used to register business Server to which SSCom do access control and SSCom Server (SSCom VPN/AP Server).

SSCom takes access control on server-unit basis (combination of IP address and port number) and users who are allowed to access to the server are registered to the business server.

(2) Attributes of Server Definition

Besides server name, IP address, port number, any information on access control will be defined. Please refer to "SSCom Manager Manual" for details.

3.3 Detailed Contents of Access Control

3.3.1 Definition of Terms

When you define access control of SSCom, SSCom Servers are referred to as follows:

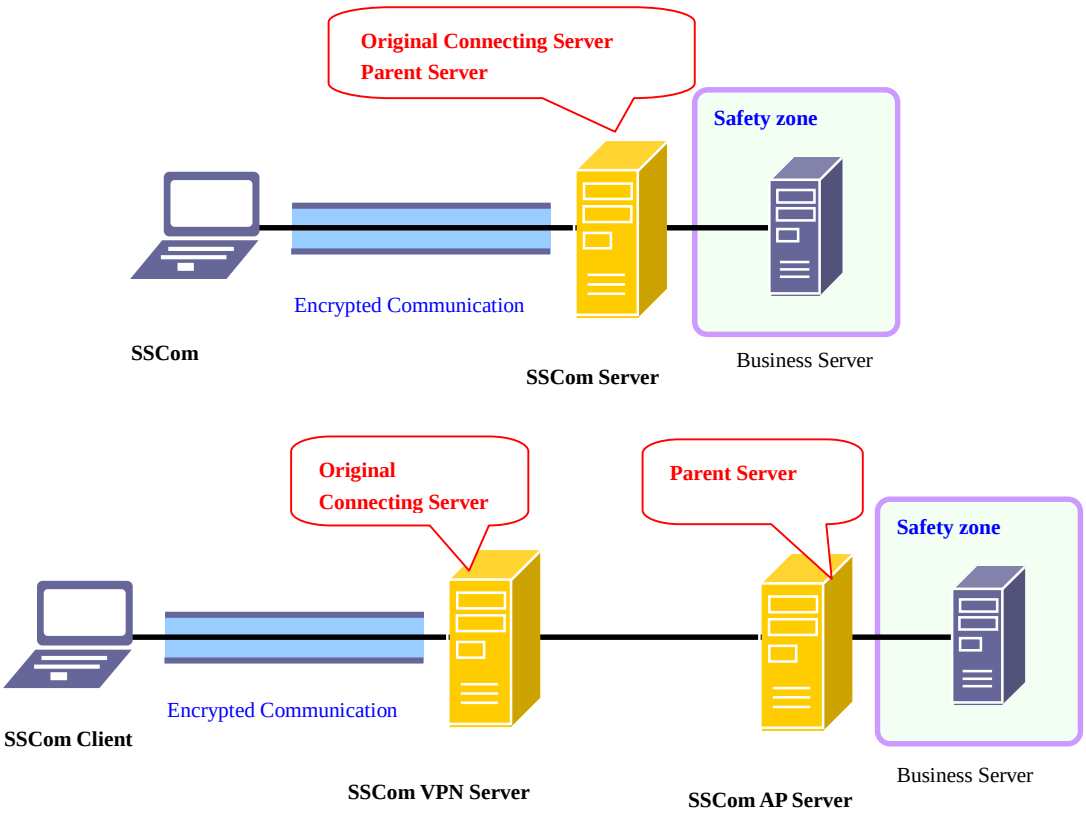
(1) Original Connecting Server

SSCom VPN Server and SSCom AP Server connected by SSCom Client are called "Original Connecting Server".

(2) Parent Server

SSCom VPN Server and SSCom AP Server, which work on the front of the network to protect business Server and deal with the connection requests from client PC, are called "Parent Server".

A "Parent Server" can manage multiple business servers, and one business server can only be managed by one "Parent Server".



3.3.2 Types of Access Right

Multiple conditions of access control can be combined into flexible measures. Types of access right are provided as follows:

- Basic judgment (effective in VPN communication)
- Access right of original connecting server (effective in VPN communication)
- Access right of users (effective in VPN communication and Web authentication)
- Access right of groups (effective in VPN communication and Web authentication)
- Access right granted by user attributes (effective in VPN communication and Web authentication)
- Access right of Web contents (effective in Web authentication)

(1) Basic judgment

There are two approaches available to choose from for judgment on access right in VPN communication. It is called "basic judgment", you can choose between "Access allowed" or "Access not allowed".

It is defined to each SSCom Server by the server definition tool.

Access allowed	Access allowed to all communication machines besides servers with restricted access.
Access not allowed	Access allowed only to permitted business servers, access to other communication machines are all prohibited.

(2) Access right of original connecting server

Different access right can be granted to the same user depending on the original connecting server it uses. This function enables access within the company, but remote access not allowed.

(3) Access right of users

Access right of each business server can be granted to specified users.

(4) Access right of groups

Access right of each business server can be granted to users that belong to specified group.

(5) Access right granted by user attributes

Each business server can grant access to users with the attribute value specified in user definition.

By defining string conditional expression (= or ≠) of specified attribute and specified value, it decides on whether to grant access according to whether the condition is established or not.

Example of prerequisite

Conditional expression for users whose subordinate information is "eigyou" "subordinate information" "=" "eigyou"
Conditional expression for users who subordinate to departments besides "eigyou" "subordinate information" "≠" "eigyou"

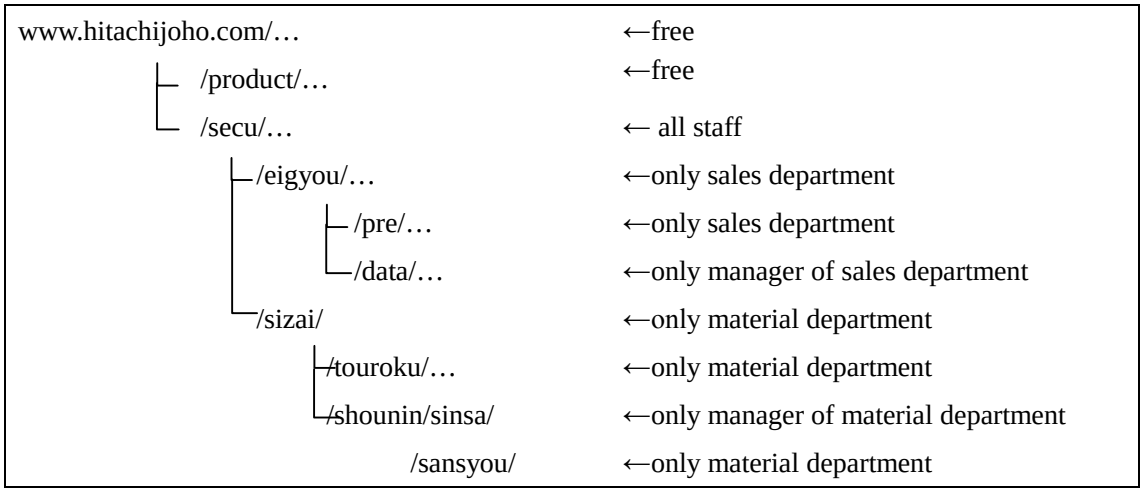
Such conditional expression can record 5 groups of comparison values at most ("AND" condition). Combined condition such as [grant access to the one whose subordinate information is "eigyou" and position is department director] can also be processed by the function.

"(subordinate information ="eigyou") AND (position = "department director")"

(6) Access right of Web contents

Access right of Web contents can be granted through Web authentication function of SSCom AP Server by folder unit.

For example, flexible access right can be granted as follows:



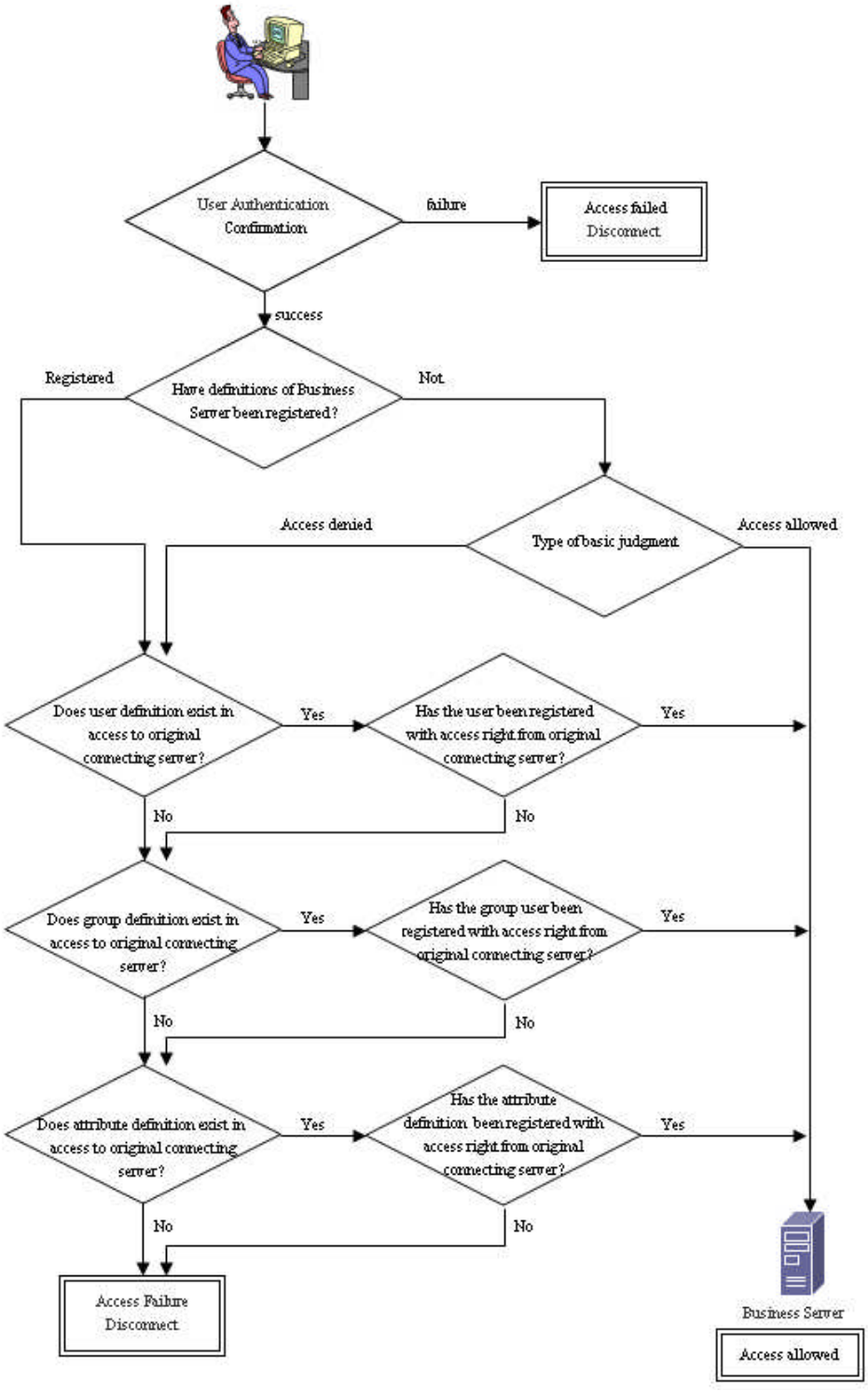
The following access right can be set:

- Access right by user unit
- Access right by group unit
- Access right by user attribute
- Access right by IP address or subnet address of original connecting server

Subordinate folder can inherit access right from upper folder.

3.3.3 Combination of Access Right

Access Control in VPN communication is executed on the combination of "basic judgment", "original connecting server", "user", "group" and "user attributes".



Please pay attention to the following points with access control definition:

- The access right registration number that each business server (port number unit) can define by "user", "group", and "user attribute" has nothing to do with difference in original connecting servers, and it can reach 50 at most. When a large number of registrations arise (more than 50 people), we recommend using group definition to group users, and granting access permission to such groups.
- In registrations on the same original connecting server, access right will be judged by OR conditions of "user", "group" and "user attribute". That is to say, as long as there is a matching definition, access right can be achieved.
- Logical judgment (AND condition) is done on conditions defined by "user attribute" (up to 5). In other words, all users matching the conditions can get access.
- Access Control definition can be done by the combination of user attribute, group, and user.

Appendix 1.Terms

CA - Certificate Authority

Also called Certificate Authority, it is a trusted third party organization that issues digital certificates online to guarantee the existence and reliability of an individual or corporation.

For example, if you do an electronic payment using credit card on the Internet, usually the credit card company will be the Certificate Authority.

CRL - Certificate Revocation List

The list which contains all certificates still exist in the effective period but have already been revoked.

DN - Distinguished Name

It is a mandatory attribute that specifies the items registered in directory server according to the directory tree structure.

For instance, for people it will be "cn=Barbara Jeansen, o=Ace Inc, c=us".

HTTP - HyperText Transfer Protocol

Agreement of data transfer on WWW, running on the standard Internet protocol TCP/IP

LDAP - Lightweight Directory Access Protocol

Protocol used with the services that respond the location information about variety of information resources distributed on the Internet. It lightens the processing of the protocol so that it could be used even on the Internet for LAN standard.

It is supported by such as Outlook Express of Microsoft or the address management tool of Messenger developed by Netscape Communications Inc. U.S.

MULTOS

OS used in e-commerce recommended by the British company---Mondex International. Based on OS built in IC card, software applications can be chosen to support its use with operations on the IC card.

Proxy

It monitors connections between LAN and external networks, and isolates unauthorized connections from external networks.

A proxy server is provided on the Firewall to block the Internet and Intranet, and used to control the communication between both networks. It is also called "proxy server".

It receives commands from the computer within the Intranet, and sends directions to the specified server on the Internet.

RSA

RSA here refers to the RSA computer security company in U.S. RSA Security Japan Inc. is a subsidiary of the U.S.

(Please pay special attention to that in some cases it points to RSA public-key cryptography.)

SSCom Client

It is the software running on the client PC, establishes encrypted communication channel between the client and SSCom VPN/AP Server. It initiates personal authentication by notifying SSCom Server of user certificate saved in client PC.

SSCom Server

The general name of SSCom products. (SSCom VPN Server, SSCom AP Server, SSCom GAC Server)

SSCom AP Server

It is the software that runs on the front of Web server and takes on encryption communication and access control, and it controls access to Web contents by URL unit.

SSCom GAC Server

SSCom GAC Server manages information on personal authentication and access control. Both SSCom VPN Server and SSCom AP Server rely on the SSCom GAC Server to realize integrated information management on personal authentication and access control.

SSCom VPN Server

It deals with encryption communication and network access control when external users trying to access the Intranet. Configured in the entrance of the Intranet, it controls access from the external network.

SSCom CA/Lite

The software responsible for certificate issuance and management.

SSL - Secure Socket Layer

The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of message transmission by Web server on the Internet. Both Netscape Navigator and Internet Explorer can support SSL.

Public key encryption is used on the uses' side to confirm whether the Web server is the legitimate object. Data exchange will be enabled if it is confirmed as the right one. The method of private key encryption which encrypts and decrypts faster will be used in practical data exchange.

Virtual IC Card

User certificates of SSCom Client are not saved in peripheral equipment, but be registered into virtual authentication device in the PC that installs SSCom Client.

X.509 - ISO/ITU X.509 v3.0

The Directory-Authentication Framework

Personal Certificate (Digital Certificate)

It refers to the certificate issued on the Internet to ensure the reliability and validity of existence of individual and legal entity. Issued by the third party, the certificate confirms the legal identify of the object. Public key encryption method is introduced here to verify whether the digital certificate is fake or being properly used.

Public-key Encryption

A cryptographic system that uses two keys -- a public key and a private or secret key.

RSA algorithm developed by RSA Security Inc. U.S. is representative. Private and public keys come in pairs. Private key can only be hold by person while the public key can be hold by anyone. The sender sends the data encrypted with the public key of the recipient. Because the data encrypted with the public key cannot be decrypted but only with the private key, only the recipient could know its contents. Unlike private key cryptography, key management is relatively easy. But, there is a disadvantage that encryption and decryption is slower than private key cryptography.

Private-key Encryption

It is an encryption method by which the sender and the receiver share the same key to encrypt messages, also can be called method of symmetric key. The secret key is kept private in data encryption. Typically represented by DES (Data Encryption Standard) developed by IBM in the United States and other cases.

Compared with the public key cryptosystem, it processes faster in encrypting and decrypting. But this system has the risk that the key be decrypted by others. The key must be passed on to others before nobody else knows it, and management takes much time as the number of keys increases with increasing number of users.

Authentication

A method of identification based on the internet security functions, which confirms the truth and reliability of an individual or of an entity. After confirmation of individual and corporate credit information, digital certificates are issued by a third authentication party.

Certificate Authority

->CA

Proxy Server

->Proxy

Single Approach

It is one of the Web authentication methods using SSCom AP Server. It refers to the one-to-one correspondence between SSCom AP Server and Web server.

Virtual Host Approach

It is one of the Web authentication methods using SSCom AP Server. Web server is recognized by the specified host name inputted on Web browser.

Reversed Proxy Approach

It is one of the Web authentication methods using SSCom AP Server. Web server is recognized by the path part the URL inputted on Web browser.

July. 2014, 10th Edition.