To digital contents Protection

Introduction to dCS(digital Contents Safeguard)

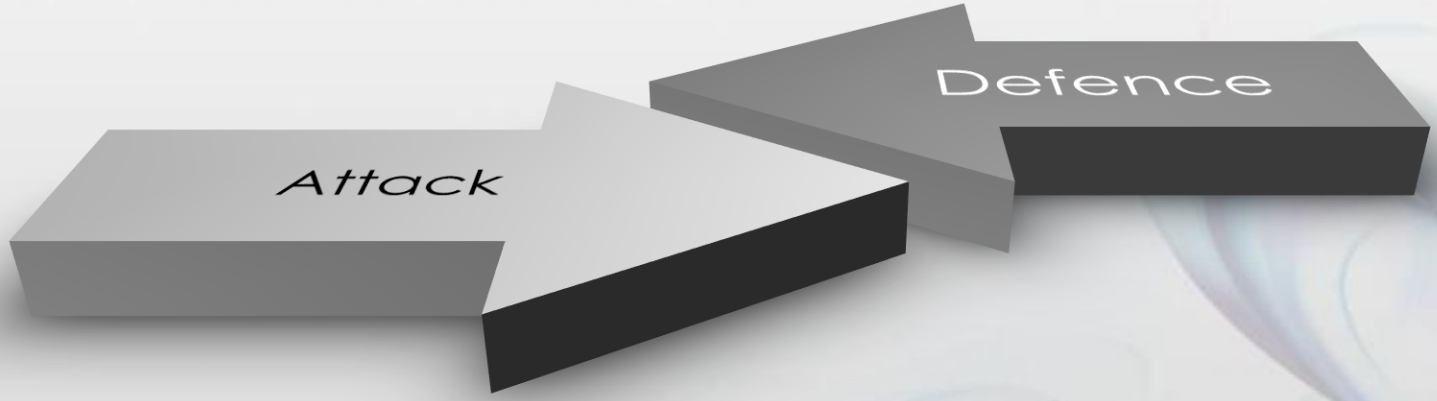
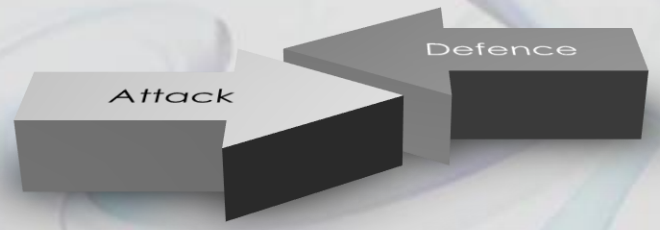
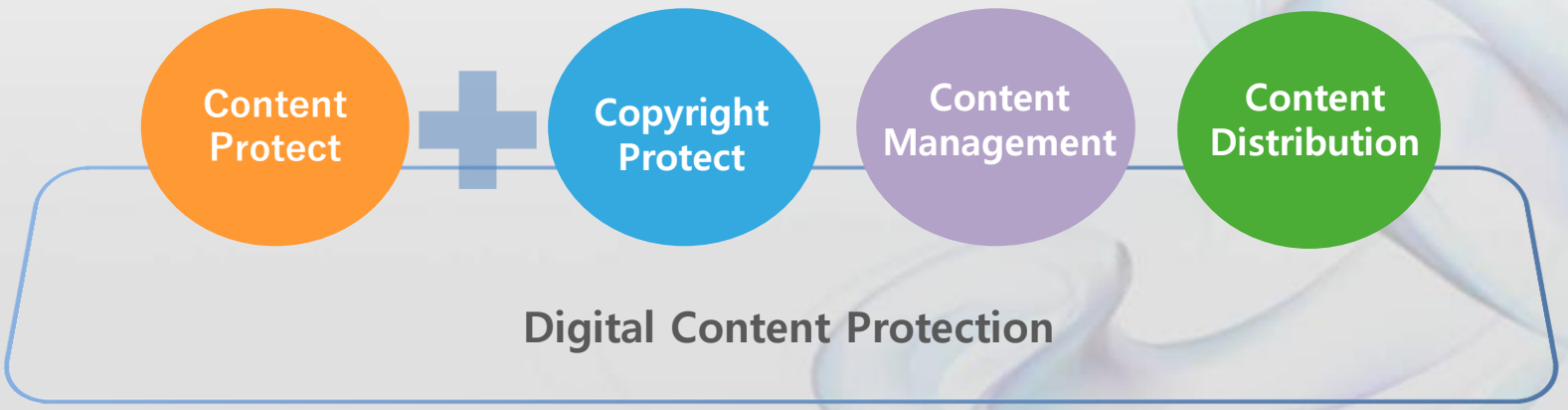


Table of Contents



Digital Content Protection

- ✓ Technology to protect against piracy or distribution by intervening in the stage of digital content creation to consumption
- ✓ Traditional digital content protection provided only the technology to protect the content.
- ✓ Recently, digital content protection requires various protection / management / distribution that is applied in the whole distribution process. And it encourages consumers to properly consume content, as well as copyright protection systems.



Transition of content consumption

- ✓ Accelerate the distribution of various mass multimedia information through the development of the Internet
- ✓ As the existing physical works are not only transformed into the form of digital content, but also produced in the digital form from the beginning, the paradigm change of content distribution

Need for Digital Content Protection

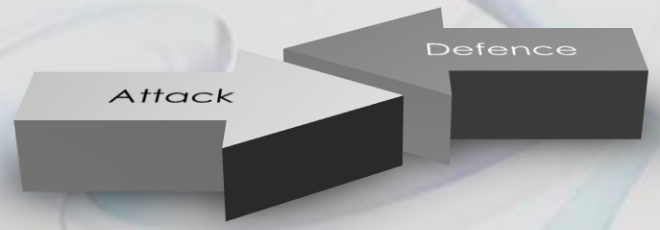
- ✓ Infinite reproduction of digital content, original and copy have the same characteristics
- ✓ As digital content emerges as high value-added merchandise, rights protection for authors is required

Content Distribution Types and Pros and Cons

Category	Contents	Application Case	Pros and Cons
Physical storage	Store content on CD/DVD or USB for sale and lease	Learning content, movie	Leverage existing publishing distribution No burden to build system Low level of content protection
Service method	Provides streaming and download service by constructing content DB centrally	Movie, Broadcast Content, Learning content	Easy distribution of content Establish and maintain high level content protection system Cost burden
System construction method	Provide content DB and system to local or overseas operators	Learning content, IPTV	Minimize service environment considerations No burden on system construction and maintenance Low level of content protection

✓ As contents distribution has recently shifted to a service or system construction method, damages to content leakage are increasing, and as social awareness is raised, operators must apply protection technologies such as DRM to protect contents.

Table of Contents



Digital content protection technology

✓ Type of protection technology

Category	Contents	Technology Type
Proactive Management	Encryption of the content itself	DRM, CAS
Post Management	Identification technology for unauthorized copy protection	Watermarking, Fingerprinting
Proactive Post Management	Content Identification and Metadata Management	DOI, INDdCS

✓ DRM vs Watermarking

구분	DRM	Watermarking
Special feature	Content encryption	Invisible information insertion
Strength	Easy to apply billing	Easy to distinguish original authors in case of dispute
Weakness	No perfect protection	Limitations of Post Processing

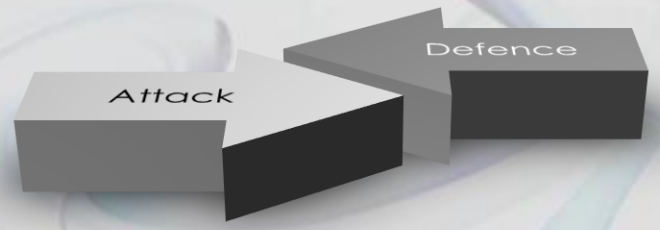
DRM

✓ technology that securely manages and protects digital contents throughout the entire distribution process from creation and use to digital contents and controls usage according to the authorized information

✓ Key features

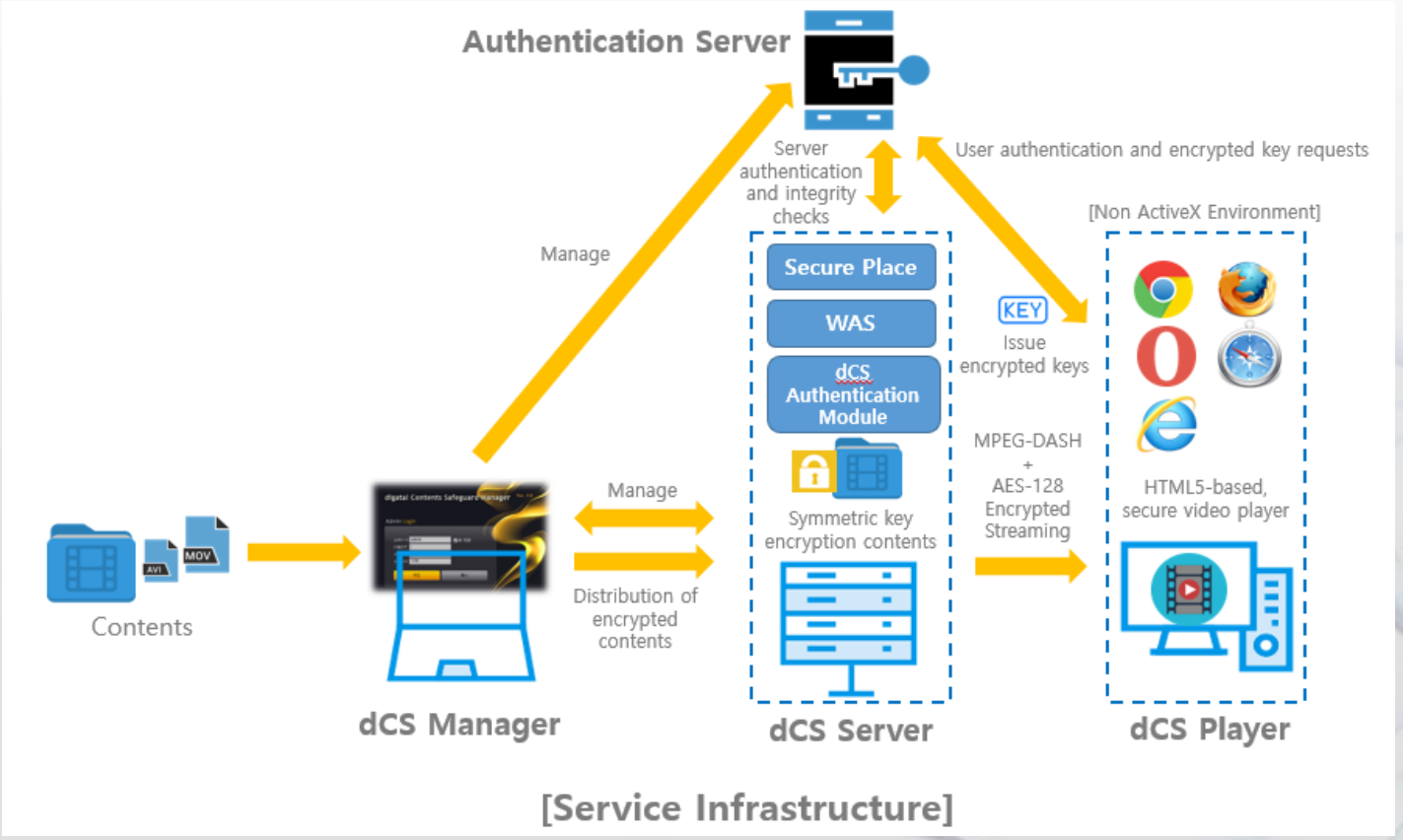
- **Cryptography : Provide confidentiality support and integrity**
- Copyright protection : Providing information such as content licenses, rights of use, and unique identification numbers
- Authentication : Device Verification and User Authentication
- **Key data management:** Securely create, transmit, and store sensitive information such as licenses, encryption keys, metadata, and user information

Table of Contents



What is dCS (digital Contents Safeguard)?

✓ dCS is an end-to-end security solution that prevents the distribution of copyrighted digital contents such as video, music, and documentation.

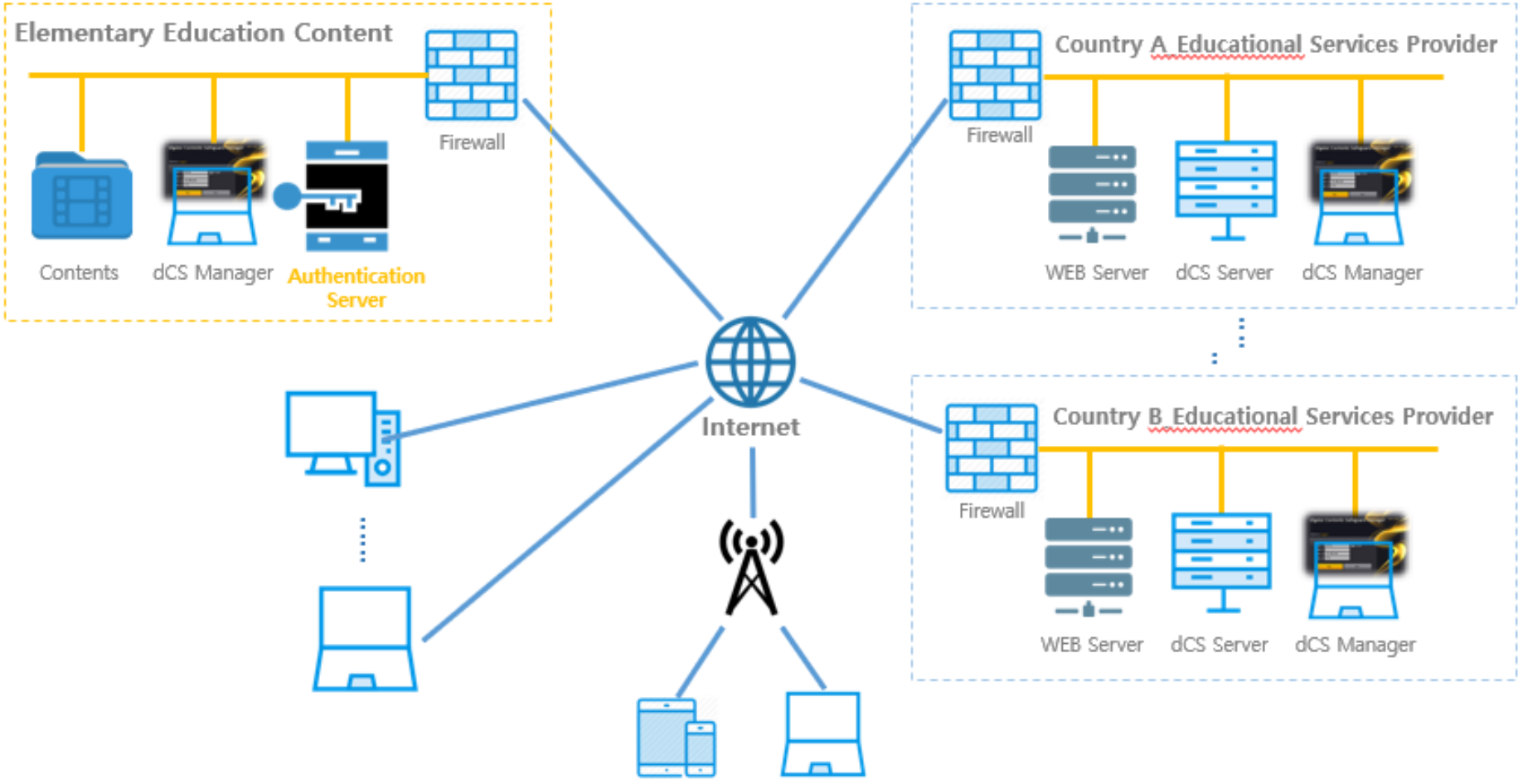


dCS application and expected effect

- ✓ Prevention of illegal use by contents leakage and contents DB replication by administrator
- ✓ Content Integrity Support - Tamper and Leak Check
- ✓ Ensure service confidentiality - Metadata for operation is managed through Secure Place
- ✓ Web service operation monitoring - Confirmation of abnormal status of web server through mutual authentication
- ✓ Guaranteed service speed - By applying the optimal encryption / decryption modules and techniques, it guarantees almost the same performance as the original content(Clear Contents) service speed.
- ✓ Operational Optimization Support - Provides content encryption module on file and folder level, Prevention of management duplication through interworking with existing management system, Alert function in case of abnormality

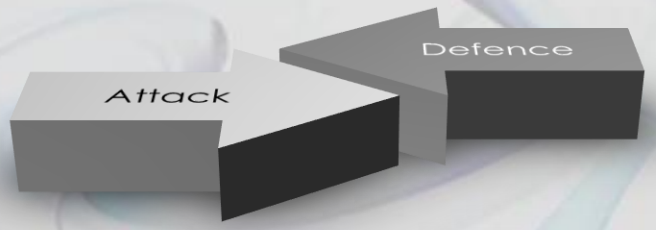
※ No need to add additional manpower even if the number of applied sites increases after introducing the solution

dCS Diagram



[Example Service Model: Educational Content]

Table of Contents



Key Features

✓ Encryption and Cryptographic Key Management Techniques

- Optimizing encryption performance by applying Open SSL module and AES-128 algorithm
- Double management of encryption key by storing encryption key in authentication server and local web server
- Generation of encryption key using random function
- Confidentiality by storing encryption key value in Secure Place

✓ Configuration module

- Secure Place & Trusted Execution Module
- Server mutual authentication module
- Digital content encryption & decryption module
- Digital content transfer Module

Configuration Module

✓ Secure Place & Trusted Execution

- Secure Place for LCMS and WEB Server
  - LCMS : Save content encryption key
  - WEB Server : Save Server Secret for Authentication
- Trusted Execution
  - Handling all functions related to encryption and decryption

Configuration Module

✓ Server mutual authentication module

- Check the contents integrity by sending and authenticating certificate from web server periodically and check contents leakage and random change
- Aperiodic WEB server authentication request and authentication verification from authentication server
- Provide notification function when authentication fails-API usage
- Sending secret update of WEB server encrypted with common key
- Apply Open-SSL

Configuration Module

✓ Digital Content Encryption & Decryption

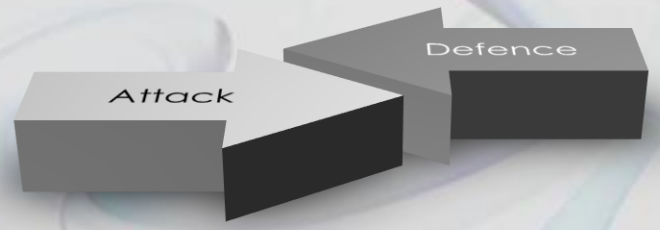
- Digital Content Encryption
  - Encrypt and store content at the time of Server Deploy
  - Store content encryption keys in LCMS Server Secure Repository
  - Using Cyclic AES-128
- Digital Content Decryption
  - Use a combination of the key stored in the LCMS Server and the key received from the authentication server.

Configuration Module

✓ Digital Content transfer Module

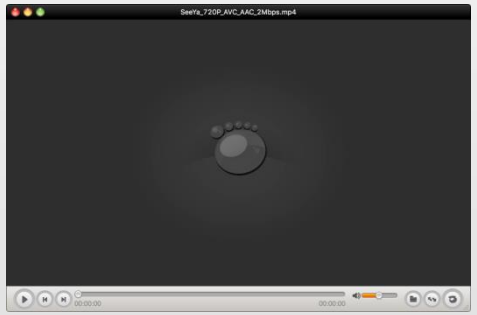
- When the Player (PC) makes a request, the WEB server requests the Trusted Execution Module in real time and receives the decrypted content.
  - To prevent the exposure of clear content
  - After receiving the request, it is directly decrypted on the memory and delivered to the WEB server.

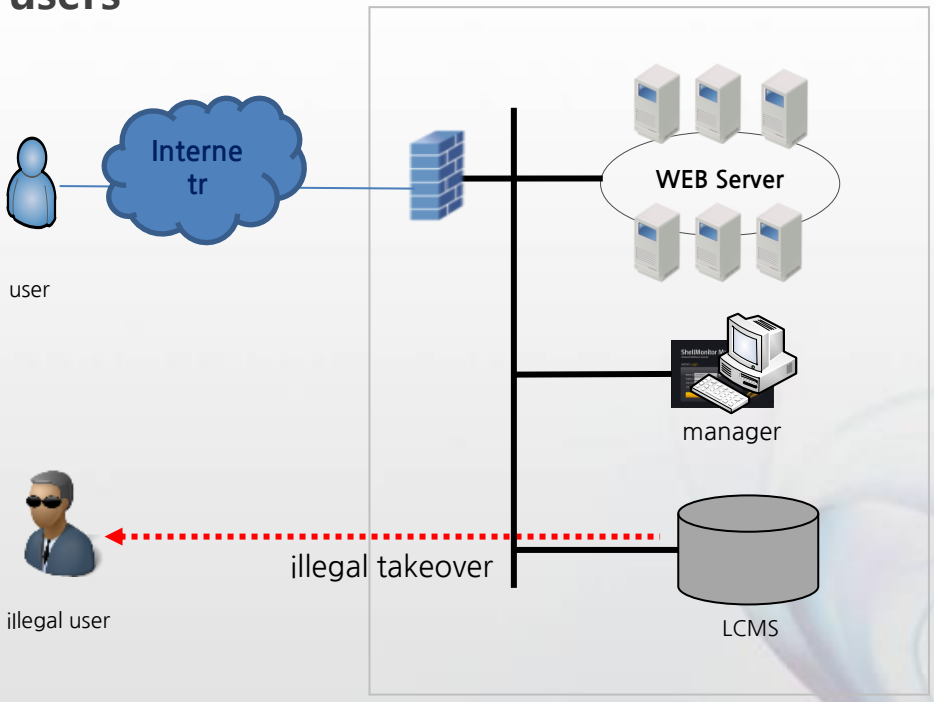
Table of Contents



Application Example

✓ **Normal users, illegal users**





✓ **When the normal user plays, time information is displayed in the progress bar at the bottom and the screen is played.**

✓ **When playing illegally leaked content, it does not play, and time information does not appear in the progress bar at the bottom**

Interworking plan

✓ CMS content encryption

- Provide content encryption and authentication key management module

✓ Interlocking with existing service management program

- Integration through API
- Interlock History
- Authentication failure, communication failure, server information (server name, domain name, server IP information)

✓ Content Decryption Support

- Providing decryption API for playing encrypted content
- Open/Play/Seek/Close function

Additional Web Services Protection Measures - WSS interworking application

✓ Content Services Server Protection

- Integration with WSS(Web Server Safeguard) Solutions
- Web source inspection: web shell, malicious URL detection and quarantine
- Web APT attack detection: Detection of random change of source code, data, and configuration file
- Web APT Attack Defense: Support for internal or external vulnerability attack and automatic defense

✓ User PC Protection

- Malicious URLs are URLs or IP addresses that distribute viruses, ransomware, etc. to PCs using web servers as a source of malicious code. If a malicious URL is inserted in the content service server, there is a risk that the service user PC is exposed to hacking.
- WSS protects user's PC using hacking attack by detecting and removing malicious URL in real time through black list & white list method.

Business Partnership

Expanding Trust Market New Service

Contents Service Platform
PC/Tablet/Smart Phone

+

dCS
WSS
Web/WAS Server
umv

Contents Service Platform

Thank You!

Address: 316-6 Yangjae-dong, Seocho-gu, Seoul, Korea
Website: http://www.umvglobal.com
e-mail: sales@umvglobal.com