JT solutions

Solutions & Technology

2. Integrated Security Solutions

4 Key Solutions in “Access Wall” – FES / IES / EES / EKS

1. FES (File Encryption System)

① Providing encrypted virtual directories (folders) to protect internal company info or research findings (files) and maximizing the security of confidential data through access control such as limiting the number of access and reading when sharing files.

② Using installed FES Application (Agent) that authenticates users and operates/monitors virtual directories (folders), users can protect files without going through complicated procedures.

2. IES (Image Encryption System)

① Encrypting images and videos transmitted from CCTV to enhance security for real-time video data.

② IES is a lightweight solution that can be easily ported to any device such as LTE Router, car black box and so on.

③ Video encrypted through IES cannot be decrypted even if data is leaked, so illegal theft, duplication, and distribution of video are fundamentally prevented.

2. Integrated Security Solutions

4 Key Solutions in “Access Wall” – FES / IES / EES / EKS

3. EES (Email Encryption System)

① When sending e-mail for internal/external, all information contained in the e-mail is encrypted and transmitted to enhance e-mail security.

② In addition to linking with internal mail servers, 100% linking with commercial emails such as Gmail is possible.

③ Since the email contents are encrypted on the mail server, all email contents such as subject, body, and attachments are prevented from being leaked even when the server is hacked.

④ Enabling users to control read & write rights through device and user authentication method provided by the integrated authentication solution.

⑤ Not only does it provide access control to the information by limiting the number of times or setting the viewing period for encrypted information that has already been transmitted, but also supports the function to cancel the viewing authority after transmission.

2. Integrated Security Solutions

4 Key Solutions in “Access Wall” – FES / IES / EES / EKS

4. EKS (Encrypted Keyboard System)

① The encrypted data generated by keyboard of EKS cannot be decrypted without the decrypting key which is already granted to target users.

② Performing initial authentication of H/W keyboard by using internal security card and then mutual authentication of encryption/decryption key through communication with authentication server

③ Encryption can be applied from the initial input device called keyboards.

④ Without interlocking with the communication interval security solution, complete data protection is possible.

⑤ Encryption is maintained even after data is shared and also the rights of decryption granted to each device can be cancelled of by "Central Command".

⑥ Jintech’s KMS (Key Management System) - centralized key management system

2. Integrated Security Solutions

Technical Strengths of “Access Wall”

1. **Dynamic encryption method**

- Encrypted content constantly changes to make it impossible to detect key patterns

2. **Access control through real-time change of authentication key**

- The personal/device authentication key for receiving authorization before requesting data from the server constantly changes during communication with the server, responding to the duplication and loss of the device or software.

3. **Reinforced data leakage prevention based on real-time changes in encryption keys**

- By changing the encryption key in units of sentences in the keyboard and in units of communication in the device, even if the operation of extracting the encryption key from one sentence or communication data is successful, the next sentence or data must also be extracted.

4. **Encryption algorithm change**

- Encryption Algorithm of OTP (One Time Password) Concept: After randomly arranging various algorithms according to user account, the data encryption algorithm is automatically changed over time.