The Great Escape - Part 1: “Secure Disk Card”

Secure Disk Card is developed for the purpose of "Disk Hacking Prevention" to block attempts to leak data through the network.

After PC boot-up, the connected internal disk is blocked. It is used by connecting through a smartphone app only when accessing the disk.

Product features

1. The disk connection status after boot-up -> switched to blocked.

- ✓ The internal disk (HDD, SSD) is not exposed (not displayed in the explorer window).
- ✓ Connection switching is allowed only during use.
- ✓ Minimization of network exposure of the internal disk (exposure only when the disk is in use).
- ✓ It is not used for the internal disk where the operating system is installed.

2. Simple installation and usage

- ✓ No need to install software such as device drivers on the PC.
- ✓ No devices are exposed to the device manager of the control panel.
- ✓ After installing the card in the PCIe slot, only the disk and motherboard are connected with a SATA cable.
- ✓ Use the internal disk for user data as if it were a USB memory.

3. Restriction of access through third-party smartphone apps

- ✓ Restriction of access by third parties through registration of user phone number.
- ✓ Stronger restriction of access by third parties due to password registration.

4. Switching to blocked status by timer setting.

- ✓ Effect of cable disconnection after disk backup.

5. Control of maintaining the disk connection status or switching to the blocked status.

- ✓ When out of range of Bluetooth signal.
- ✓ When the smartphone app is closed.

6. Long-term preservation of SSD data.

- ✓ Maintaining constant power connection and interface signal blocking status.

7. Various selectable PCIe brackets.

- ✓ Half-length PCIe bracket / LP (Low Profile) Bracket.
- ✓ Selection of a bracket that allows or suppresses DIP switch for forced emergency connection.

8. Prevention of data leakage at the endpoint of network separation PCs.

- ✓ Simply connecting a WiFi dongle in the form of a USB memory may penetrate the internal network

security.

- ✓ Used for preventing data leakage and disk hacking at the endpoint.
- ✓ Product not subject to security compliance inspection (confirmed by the National Cyber Security Center).

9. Support operating systems - Windows 11, Windows 10.

- ✓ Support for Windows 11 operating system requires a PC equipped with the hardware specifications required for Windows 11 installation.
  - ✓ In case of CPU, it only supports PC environments with Intel 12th generation or equivalent CPUs however.

Nomenclature of each part

①Bluetooth antenna

②PCIe Bracket

③Disk connection status indicator LED

☞ Blue LED lit when disk is connected

④DIP switch

☞ Forced disk connection in ON position (emergency use only)

⑤Disk identification switch

☞ Used for identifying the connected disks through the smartphone app in case of multiple secure disk cards installed.

☞ When the disk identification switch is pressed, the smartphone app displays thicker outlines around the device tab and disk button.

⑥Bluetooth module

⑦PCIe edge-finger part

⑧SATA connector #1 (connected to the SATA connector of the motherboard)

⑨SATA connector #2 (connected to the SATA connector of the HDD or SSD)

⑩Program port for the Bluetooth module

☞ Used for product manufacturing and A/S

Accessories

30cm SATA3 cables - 2 pieces

PCIe Bracket mounting bolt - 1 piece

Options

Equipped with a DIP switch as an emergency connection method to prepare for situations where data on the disk device connected to the emergency security disk card needs to be accessed.

- ✓ When it is necessary for an administrator to access the disks of a user who is absent.
- ✓ In cases where it is necessary to avoid any disruptions in PC operations despite the loss of a personnel's smartphone.

If the storage device connected to the security disk card is forcibly switched to a connected status by the DIP switch.

- ✓ Display the forced connection status for the disk on the device tab of the smartphone app.
- ✓ Forced connection by DIP switch → Automatic report to administrator (next version of smartphone app)

If strict security is required internally.

- ✓ Separately purchasable PCIe brackets are available that are designed to prevent manipulation of the DIP switch.

- Base Product -

STD Bracket + DIP Switch Active

STD Bracket + DIP Switch Suppressed

LP Bracket + DIP Switch Active

LP Bracket + DIP Switch Suppressed

A disk hacking prevention system that can be used as easily as using water, linked with a smartphone; Great Escape!

Bluetooth connection status display

Security status logo

Each disk button is associated with the product image and is arranged from top to bottom in the order of the most recently activated device tab to the first activated device tab.

Product images are arranged in accordance with the order of the device tabs, with the product image of the first activated device tab displayed at the back and the product image of the later activated device tab displayed at the front.

Why can't I have peace of mind with just one computer?

It's been a battle of spears and shields since the first virus!

Who will be the final winner? The victory can only be for the shield, Great Escape.

Intrusion and Damage → Detection → Vaccine Creation → Deployment → Treatment → Variants

Type of intrusion

Destructive attack

- ✓ Disk data (user data)
- ✓ System files (files for the operating system)

System resource exhaustion

- ✓ CPU overload
- ✓ Main memory depletion
- ✓ Disk capacity and I/O overload

Network resource exhaustion

- ✓ Network bandwidth exhaustion

Approach type

Software approach

- ✓ Operations based on white-list
- ✓ Password, Symmetric key encryption, Public key encryption

Recovery/remediation methods after a security breach

Maintaining disk connection status

Security of the Filter Driver concept residing on the operating system kernel

- ✓ Many cases are irreparable
- ✓ Many are not even aware that a data breach has occurred,

The time delay effect exists, but sustainable security is not guaranteed.

One disk device for user data can be safely protected.

Disk hacking prevention system: Great Escape!

Block internal disk?

Yes! This is a patented technology applied to Great Escape.

Existing computer's disk drive

Can you really have proper security

when the disk is constantly connected?

Maintain disk connection status after booting

Disk devices connected through a secure disk card

The world's first in the global industry! Preventing built-in disk connection after booting

Disk connections/blocks are then controlled through a smartphone app.

Maintaining disk block status after booting and switching to block only when the disk is connected during use.

Does water usually leak from the faucet?

Like how water is kept locked by the faucet when not in use, if the conditions for secure usage are simply made like using water, 99% of security issues can be resolved.

Use case 1

The type of work may be different, but the type of work performed is similar.

Daily work: 8 hours.

During working hours, the access time to pure disk devices is less than 5 minutes.

- ✓ The time required for reading, writing and erasing operations
- ✓ during document work such as Word, Excel, PowerPoint, PDF, etc.
- ✓ The time it takes to extract compressed files or to compress files
- ✓ The time it takes to copy a file or a folder
- ✓ Therefore, 7 hours and 55 minutes (99%) after computer boot-up is spent in disk waiting status.

Maintain the standby status of the internal disk device that accounts for 99% in a blocked status

- ✓ Make the operating system hide the disk device recognized in the Explorer window
- ✓ It does not expose the existence of disk devices connected through the security disk card to hackers who intrude through the network.

Disk standby status → 'Perfect Stealth' disk!

Can even the most excellent hacker hack a non-existent disk?

Use case 2

When I returned to my seat after finishing lunch, the LED on my PC was blinking rapidly.

I am the owner of the PC, but there are disk access operations occurring that I am not aware of.

It is said that unlike ransomware and other similar attacks, data breaches often do not leave clear evidence of the damage, making it difficult to even detect whether or not a data breach has occurred. However, I hope that this does not necessarily mean that data is being leaked in your case.

That being said, you can at least trust the security of the disk device connected to the secure disk card.

This is because it maintains a blocked status when it is not in use.

Disk backup cannot be overemphasized no matter how much emphasis is given to it!

Did you happen to disconnect the disk connection cable after backing up your disk?

Completing a backup also involves disconnecting the disk connection cable from the motherboard!

However, the tedious task of disconnecting the cable after disk backup that needs to be done not just once or twice, but every day or every other day,

What if there is no solution to resolve this issue?

Now leave it to the disk hack protection system - Part 1 secure disk card.

Secure disk card protects your data by electrically and safely blocking the interface signal of the cable through a timer setting of backup time + α in our smartphone app

Disk backup followed by cable disconnection made easy with our solution!

Choosing and using disks correctly according to their purposes

The saying "Don't put all your eggs in one basket" applies to computer security as well.

Even though the latest HDDs are available with up to 22TB of storage capacity, would you still expose a large capacity disk of several tens of terabytes to the network in a constantly vulnerable status?

Operating System installation disk

- ✓ Installation size: 21GB
- ✓ In terms of cost-effectiveness, it is better to use a low-capacity, high-performance SSD instead of a high-capacity, high-performance one.

Disk for user data

- ✓ Using a secure disk card together with a disk of several tens of terabytes in capacity.
- ✓ The disk is in an unused standby → blocked status to prevent exposure to the network.

Is your SSD, which you are keeping in separate storage, doing well today?

The fact that the unit memory element of SSDs and USB memory is the same NAND Flash memory

Have you ever experienced a sudden loss of all data on your USB memory?

Have you ever been unable to access your USB memory?

Are you storing your SSD separately, inside the desktop PC which has many heat-generating components?

Please do not store your SSD, which contains important data, in a drawer for an extended period of time like an HDD after removing it from the PC.

Storing an SSD with its power disconnected due to high temperatures inside a PC may lead to data loss within a year.

As multi-bitization of NAND Flash memory advances (SLC → MLC → TLC → QLC → ...) and

as semiconductor process technology becomes more miniaturized, memory devices become more susceptible to temperature.

Way to keep the data on USB memory or SSD safe!

Instead of storing separately when not in use, keep the device connected to maintain the power connection.

At the same time, the interface signal is maintained in a blocked status.

The secure disk card provides the solution for this.

Disk hacking prevention app

01. The app's launch icon and initial screen

Launch icon on the smartphone home screen

- ✓ Realize perfect security in disk standby status

The initial screen

- ✓ Display of devices supported by the app
- ✓ Display when the device is not detected

02. The main screen of the smartphone app

Bluetooth connection status, security status logo, settings

Device tab, disk button, lock button

Product image associated with the disk button

Bluetooth connection: Bluetooth blocking:

Security status logo

Perfect Security: Weak Security: Non-Security:

: Go to the settings screen for auxiliary menu

The same order as the arrangement of the disk buttons

Disk button up→down

Product image back→front

ⓐ Disk connection/blocking button

ⓑ Volume label display

ⓒ Connection/Blocking display

ⓓ Timer display

03. The app's settings screen - access registration (1)

It is used to allow or block access by others to activated devices.

Reset password and phone number.

Register your email address. This allows for resetting of the password and phone number in the event of a password loss by entering the email address that was previously registered.

For your information, the registered email address, phone number and password are stored in the non-volatile memory embedded in the hardware product.

The product cannot be used without registering a phone number or password.

In case of password loss, the device can be reset to the factory state by entering '#factory@reset.adm' in the e-mail address field, along with setting certain conditions in other menu items. However, this does not apply if an administrator password starting with '$' has been registered.

Register phone number

This is used to allow device usage for users who have registered the same phone number.

If you do not want to allow device usage, you can register a password.

Register password

ü This is used to prevent unauthorized access to the device by others.

ü Since the registered password can be reset through the user's pre-registered email address, it is recommended to register a strong password without worrying about losing it.

Change phone number

This is used to change the phone number.

Change password

This is used to change the password.

If the same password is entered consecutively three times, it will be reset to the factory mode.

04. App setting screen - recognition setting

This is used for maintaining or blocking the connection status of the internal disk connected to the secure disk card when the smartphone app is closed or when it goes out of Bluetooth connection range.

This is used to set the connection time for disk recognition during boot for the secure disk card or SSD Slide-Stacker product.

- ✓ Maintain disk connection status for up to 120 seconds during boot.
- ✓ If the position of the settings button is located in the red area, the continuous connection status is maintained.
- ✓ Adjust depending on PC performance, such as the type of storage device on which the operating system is installed.

As a common feature, it controls the connection status of the disk when the app is closed or when the user's smartphone is out of Bluetooth range.

05. App settings screen - volume label (disk label)

It is for specifying the same label as the volume label (or disk label) recognized by the operating system for the connected storage device (secure disk) through the hardware of the data leakage prevention system (secure disk card).

- ✓ Disk labels can only be entered in uppercase or lowercase English letters.
- ✓ Numbers and special characters are used for special purposes such as factory reset.

06. App setting screen - color setting

Different colors can be assigned to the disk connection/blocking button and lock button for each device to make it easier to distinguish connected storage devices.

It is used to easily distinguish which disk is mapped to which disk button by setting the background color of the disk connection/blocking button when multiple secure disk cards are installed on a PC.

- ✓ Specify the background color of the disk connection/blocking button and the background color of the lock button.
- ✓ In case of a security USB dongle, the background color of the disk connection/blocking button is transmitted as an LED color.
- ✓ The color of the disk button remains the same even if it is blocked, while the color of the lock button is locked.

07. App setting screen - timer setting

It is used to set a timer for a selected device to block the storage device connected to the device after a certain amount of time has elapsed.

As soon as the disk button is switched to the connected status, the timer starts and when the timer is over, the disk button is switched to the blocked status.

- ✓ Did you forget to switch the secure disk card with your public certification stored on it to blocked status after using internet banking? If a timer is pre-set, it will automatically switch to a blocked status after the timer ends.
- ✓ It is used to block interface signals after disk backup to safely protect the backed-up disk. (cable disconnect effect)

Maximum timer setting time: 18 hours

08. App setting screen - others setting

It is used to specify the displayed language on the screen and to choose the remaining time of the device tab in case of Bluetooth authentication failure.

Displays the current version of the app being used.

Select the language displayed on the main and settings screens.

Select the Bluetooth connection blocking time in case of authentication failure.

User's valuable data

It can be safely protected from invisible access through the network.

The Great Escape - Part 1: “Secure Disk Card”