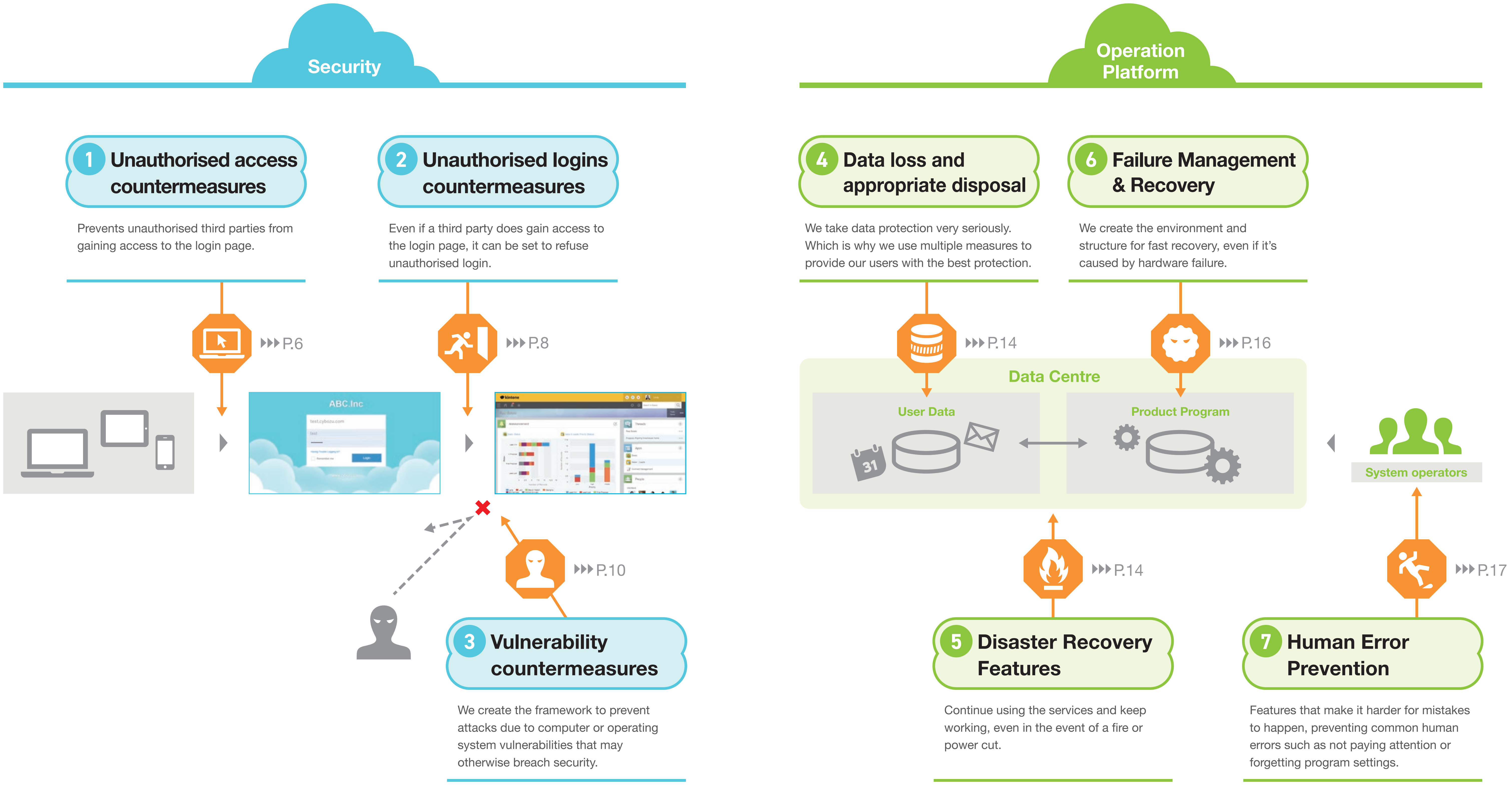
cybozu.com

Data Security & Operation Platform

Creating a service
that's always safe

7 important solutions for using cloud services safely



Security

1 Unauthorised access countermeasures

Prevents unauthorised third parties from gaining access to the login page.

▸▸▸P.6

2 Unauthorised logins countermeasures

Even if a third party does gain access to the login page, it can be set to refuse unauthorised login.

▸▸▸P.8

3 Vulnerability countermeasures

▸▸▸P.10

We create the framework to prevent attacks due to computer or operating system vulnerabilities that may otherwise breach security.

Operation Platform

4 Data loss and appropriate disposal

We take data protection very seriously. Which is why we use multiple measures to provide our users with the best protection.

▸▸▸P.14

6 Failure Management & Recovery

We create the environment and structure for fast recovery, even if it's caused by hardware failure.

▸▸▸P.16

5 Disaster Recovery Features

▸▸▸P.14

Continue using the services and keep working, even in the event of a fire or power cut.

7 Human Error Prevention

▸▸▸P.17

Features that make it harder for mistakes to happen, preventing common human errors such as not paying attention or forgetting program settings.

Security

A variety of security features so you can use our services safely.

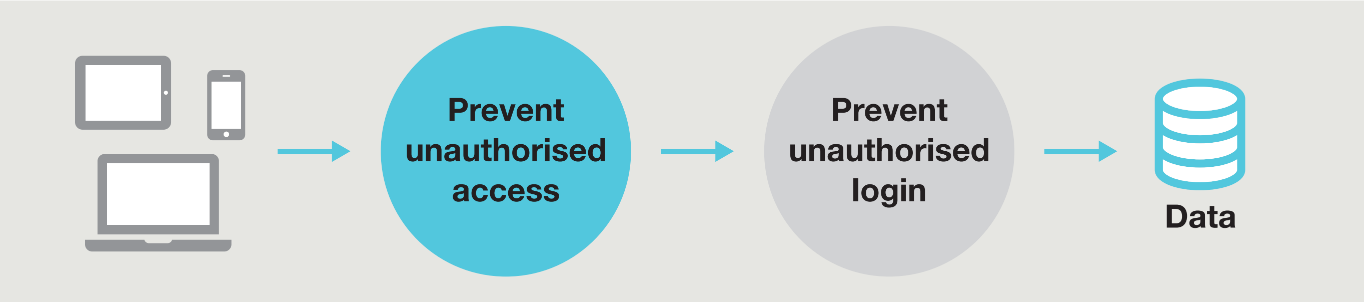
- ✓ We offer a variety of security related functions that can be set up to meet your policy requirements.
- ✓ Our expert team for security incidents (Cy-SIRT), are ready to deal with Cybozu product issues as well as vulnerabilities in whatever OS or third party software you're using.

User Login Security

Improved security using Multi-Factor Authentication

Product Security

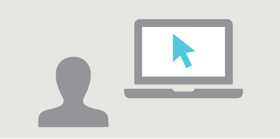
Improved security using Multi-Factor Authen- tication



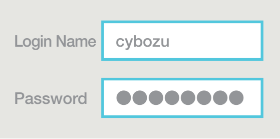
Basic Authentication

FREE

Add extra access restrictions to the standard login page. By adding Basic Authentication, only persons who know Basic Authentication login and password can proceed and gain access to the cybozu.com login page.



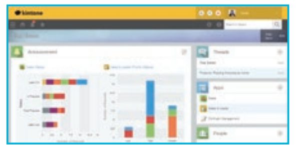
1. Access each service via its URL on cybozu.com



Login Name: cybozu
Password: ●●●●●●●●

2. Enter Basic Authentication Login Name and Password

3. Enter the Login Name and Password for cybozu.com



4. You have now gained access via 2-Factor Authentication and may use the services

IP Address Restrictions

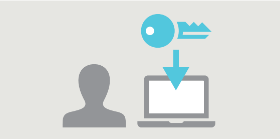
FREE

Stop access from IP addresses that are not listed.

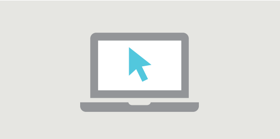
Client Certificate Authentication

Paid Option

Optional service to verify the connection source using Client Certificates. Use the client certificate authentication option to allow devices to access our services from a non-listed IP address if Client Certificate is installed. Only pay for the number of persons using mobile access: JPY 250 / month / user.

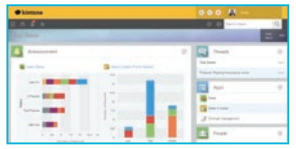


1. Import Client Certificate to a device used for mobile environment



2. Enter URL for client certificate authentication

3. Verify Client Certificate



4. Get to work at cybozu.com

Custom Subdomains

FREE

Access different login URLs for every business by issuing individual subdomains.

Any security setting change is applied immediately

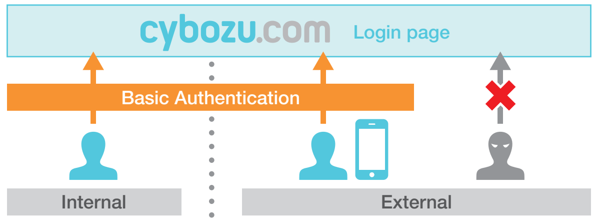
Make desired changes, such as Basic Authentication, IP Address Restrictions, issuing Certificates or changing the name of subdomains from the settings page and they're instantly applied.

4 examples of Security Settings

Improve security easily

IP Address Restrictions	Basic Authentication
Deny all	On

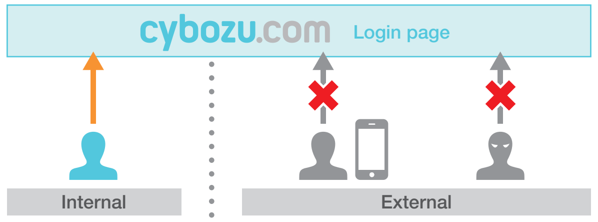
In addition to the login name and password of the user themselves, the Basic Authentication User Name and Password must also be entered each time.



Not allowing access from outside of the company

IP Address Restrictions	Basic Authentication
Allow specific IP addresses	Off

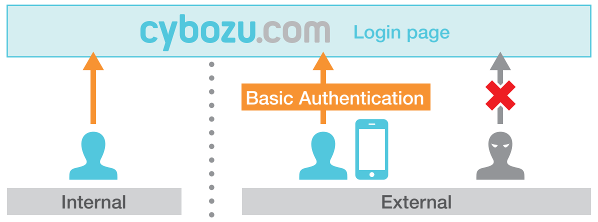
Access can be limited to an internal company network only, using IP Address Restrictions to only allow internal global IP addresses.



Enjoy the same level of smooth access whether inside or outside the company

IP Address Restrictions	Basic Authentication
Allow specific IP addresses	On

To gain access from outside the company, a Basic Authentication User Name and Password must be input, in addition to the verification on the login page.

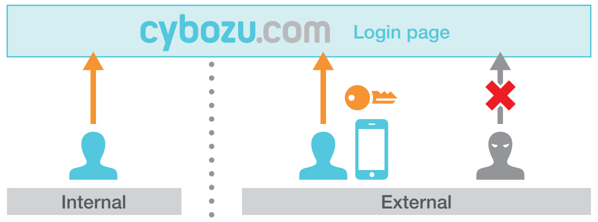


Use mobile devices and work outside the company, even more securely

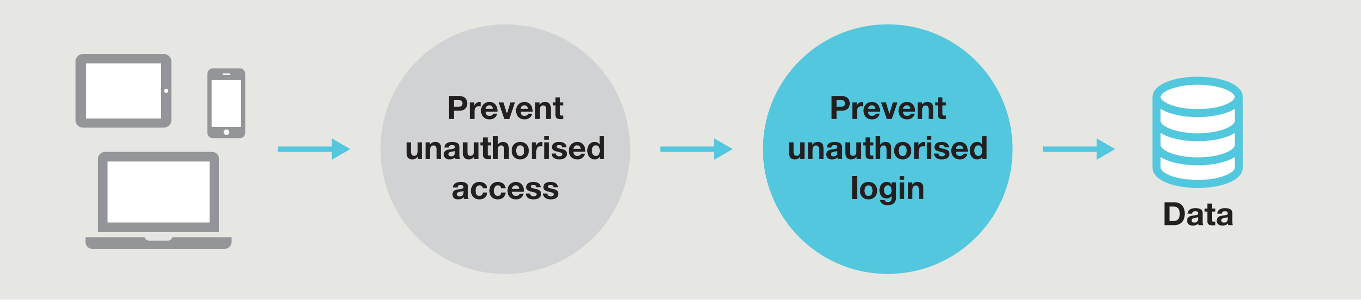
Paid Option

IP Address Restrictions	Client Certificate Authentication
Allow specific IP addresses	Permitted per user

You will need to retain a Client Certificate for client certificate authentication issued for each user to gain access from outside the company.



Improved security using Multi-Factor Authen- tication

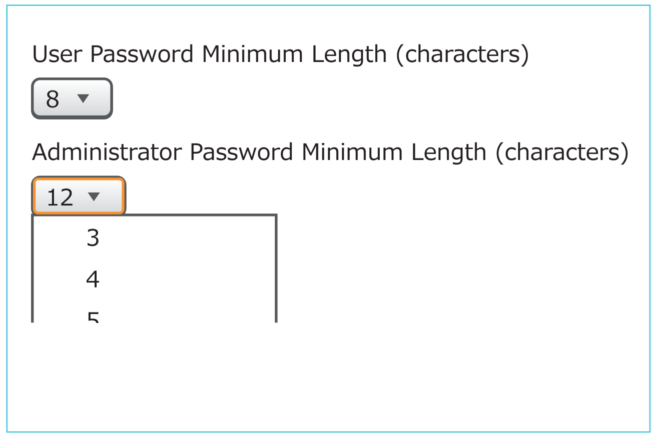


Configure various password policies

Apply a variety of password policies to suit your company.

Number of characters in password

Can be set between 3 and 15 characters for each user or administrator.



User Password Minimum Length (characters)

8 ▾

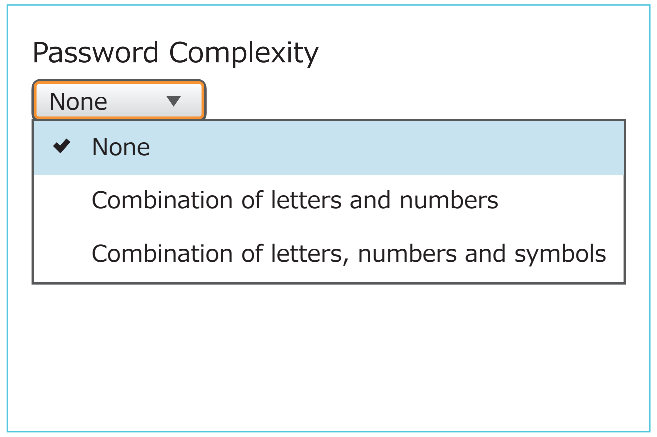
Administrator Password Minimum Length (characters)

12 ▾

3
4
5

Password complexity requirements

Specify the combination of letters and numbers.



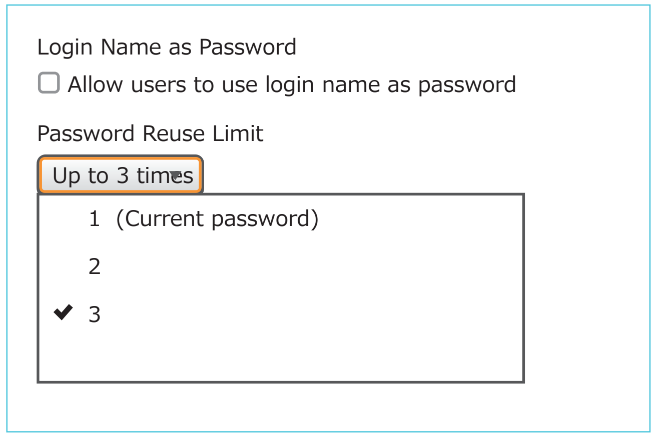
Password Complexity

None ▾

✓ None
Combination of letters and numbers
Combination of letters, numbers and symbols

Reuse password

Reject passwords that are the same as the login name, restrict the number of times a password can be reused (1-15 times).



Login Name as Password

□ Allow users to use login name as password

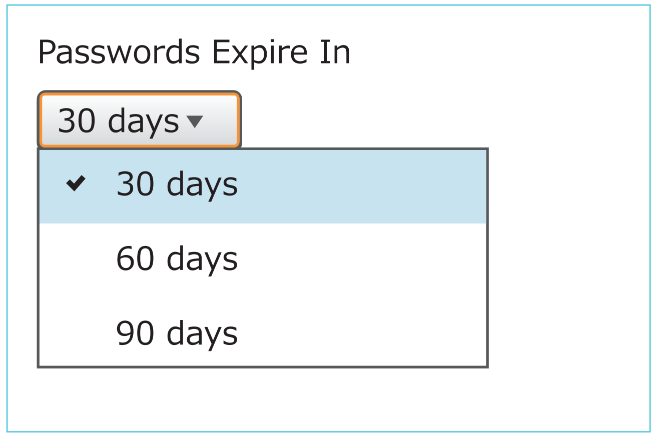
Password Reuse Limit

Up to 3 times ▾

1 (Current password)
2
✓ 3

Password expiration

The lifetime of a password can be set to 30, 60, 90 or 180 days, 1 year or no limit.



Passwords Expire In

30 days ▾

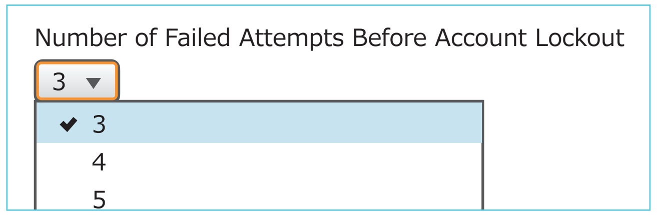
✓ 30 days
60 days
90 days

Account lockout function

Account can be locked if password is repeatedly entered incorrectly.

Set number of failed attempts before account lockout

Number of failed login attempts can be set between 3 and 10 times, or Never lockout.



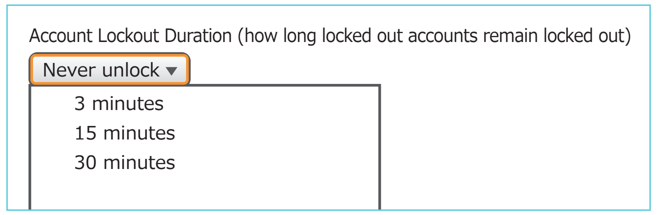
Number of Failed Attempts Before Account Lockout

3 ▾

✓ 3
4
5

Define Account Lockout Duration

You can select how long before unlocking an account, between 3, 15, 30 and 60 minutes, or Never unlock. If Never unlock is selected, the account can only be unlocked by the administrator.



Account Lockout Duration (how long locked out accounts remain locked out)

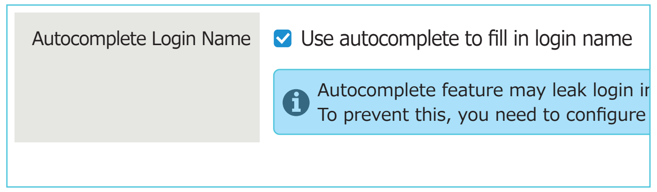
Never unlock ▾

3 minutes
15 minutes
30 minutes

Automatic login limiting function

Enable or disable autocomplete of login name

Specify whether to enable autocomplete for the login name. We recommend disabling this function unless IP address restrictions are in place.

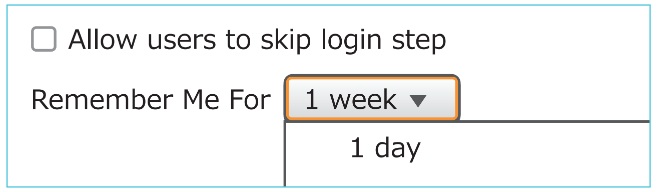


Autocomplete Login Name ☑ Use autocomplete to fill in login name

Autocomplete feature may leak login ir
To prevent this, you need to configure

Automatic Login Settings

You can specify whether to permit or refuse a period of login validity. If you select permit, the validity period can be set to 1 day, 1 week or 1 month.



□ Allow users to skip login step

Remember Me For 1 week ▾

1 day

Audit logs

Browse or download the audit log of operations such as logins or file downloads, etc. You can also configure for each log level to send a notification to specified e-mail addresses when an audit log entry is generated.

Date and Time	Accessed	User	Service	Module	Action	Result
2015-03-05 14:49:05	XX.XXX.XXX.XXX	sato	Garoon	Basic system	login	SUCCESS
2015-03-05 14:37:45	XX.XXX.XXX.XXX	sato	Garoon	Basic system	login	SUCCESS
2015-03-05 14:37:41	XX.XXX.XXX.XXX	sato	Garoon	Messages		FAILED
2015-03-05 14:37:41	XX.XXX.XXX.XXX	sato	Garoon	Basic system	login	SUCCESS
2015-03-05 14:32:09	XX.XXX.XXX.XXX	sato	Garoon	To-Do List	modify	SUCCESS
2015-03-05 14:41:22	XX.XXX.XXX.XXX	sato	Garoon	Bulletin Board	create	SUCCESS

*We do not offer a service to provide logs other than those with the Audit Log function.

Functions to prevent data leaks due to malicious websites

Clickjack Protection

This is a function to protect against Clickjacking, where the user is tricked into clicking on an image that leads to a service from a malicious website.

Login Page Image Settings feature

Images on the login page can be uniquely set to prevent login data/information leaks from Phishing sites.

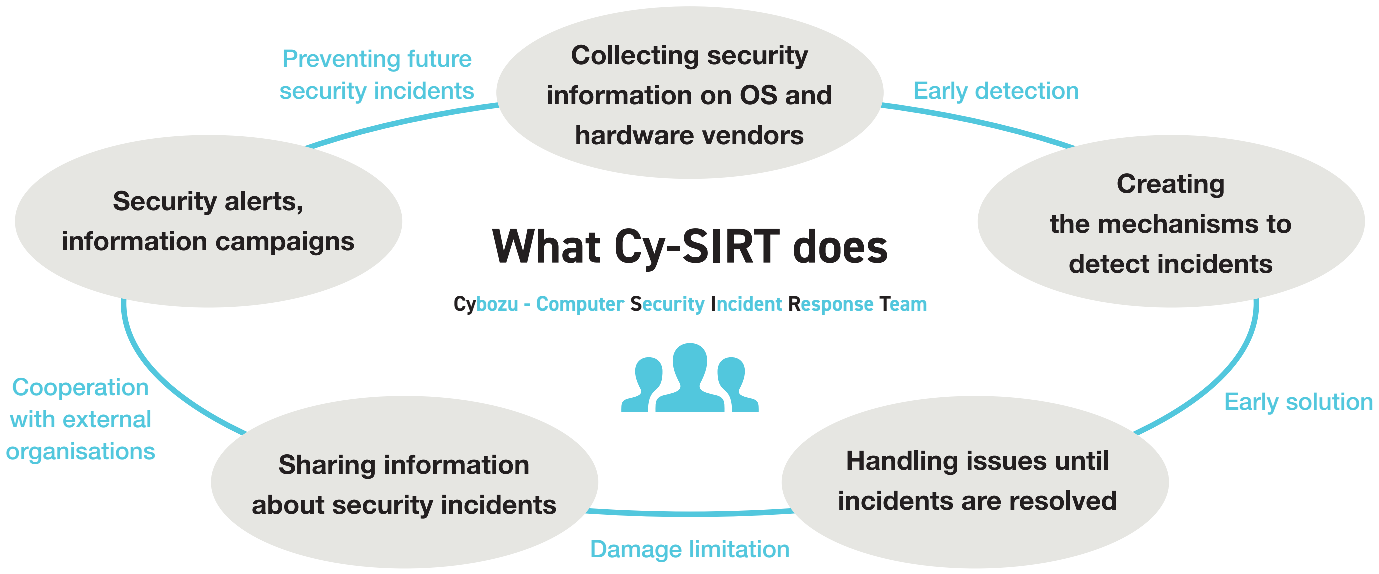
What we do to improve product security

In recent years, unauthorised access that exploits what are known as vulnerabilities in operating systems and software security has increasingly become a problem.

At Cybozu, we have been taking various measures to prevent damage caused by vulnerabilities in our products, third party software or the operating systems (OS) they run on.

Our team dedicated to dealing with security incidents: 'Cy-SIRT'

Cy-SIRT is our in-house expert security team created to prepare against and handle any security incidents. We work with external organisations and specialists to create policies to protect against threats and respond rapidly and in real-time to identify, contain and eradicate threats as they arise.



What Cy-SIRT does

Cybozu - Computer Security Incident Response Team

Collecting security information on OS and hardware vendors

Early detection

Creating the mechanisms to detect incidents

Early solution

Handling issues until incidents are resolved

Damage limitation

Sharing information about security incidents

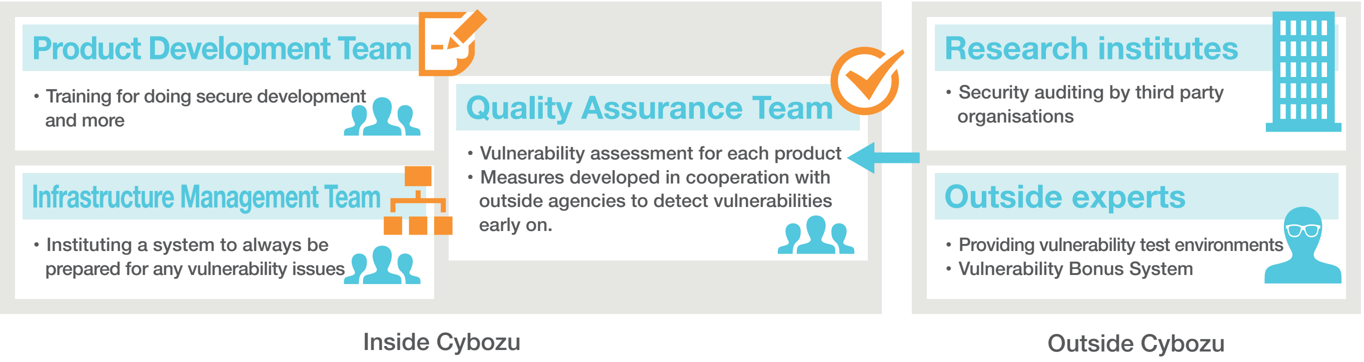
Cooperation with external organisations

Security alerts, information campaigns

Preventing future security incidents

Our work on Cybozu product vulnerabilities

Cybozu products undergo vulnerability testing, carried out by our Quality Assurance Team before being handed over to the user. The basis for handling all vulnerability issues is the in-house tests carried out by those who know all about how the products work. By enlisting the help of experts to detect vulnerabilities and external research organisations to carry out audits, we are constantly seeking to improve reliability.



Product Development Team
- Training for doing secure development and more

Infrastructure Management Team
- Instituting a system to always be prepared for any vulnerability issues

Quality Assurance Team
- Vulnerability assessment for each product
- Measures developed in cooperation with outside agencies to detect vulnerabilities early on.

Research institutes
- Security auditing by third party organisations

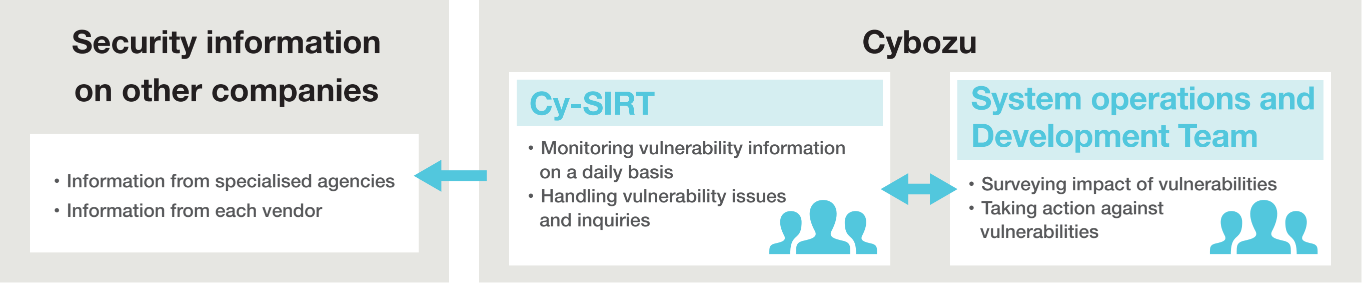
Outside experts
- Providing vulnerability test environments
- Vulnerability Bonus System

Inside Cybozu

Outside Cybozu

Working on the vulnerabilities of computer operating systems and third party software

We are constantly gathering information on the vulnerabilities of operating systems and third party software and taking action where necessary. These days, 'zero-day vulnerability' is an increasing problem, where software vulnerabilities are found by malicious parties who then mount attacks taking advantage of these vulnerabilities before the product developers have had a chance to produce updates to remedy the problem. Here at cybozu.com, if the developer cannot provide update programs fast enough, we may fix the problems ourselves.



Security information on other companies
- Information from specialised agencies
- Information from each vendor

Cybozu

Cy-SIRT
- Monitoring vulnerability information on a daily basis
- Handling vulnerability issues and inquiries

System operations and Development Team
- Surveying impact of vulnerabilities
- Taking action against vulnerabilities

Internal Security Management Policies at Cybozu

Certified Information Security Management System (ISMS)

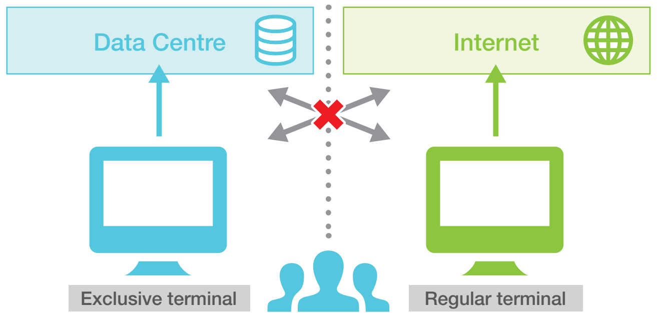
Cybozu Inc is certified according to ISO 27001 for our Information Security Management System (ISMS) in the following areas.

Scope of accredited certification: Design, construction and maintenance of operational infrastructure of a cloud service developed in-house.
Date of certification: 10 November 2011
Certification number: IS 577142
Accredited certification body: BSI Group Japan

IS 577142 / ISO 27001

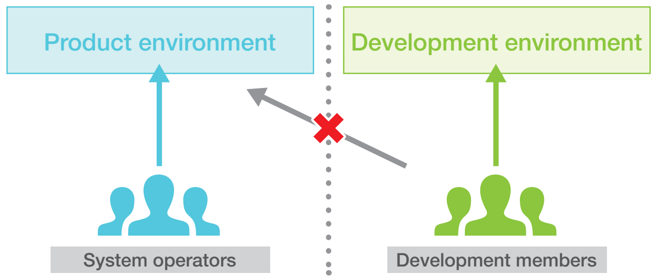
Purpose-specific devices for connecting to the data centre

System operators can only connect to the data centre using highly access-restricted devices. These specific devices are not connected to the internet so there is no risk of attacks or viruses via that route.



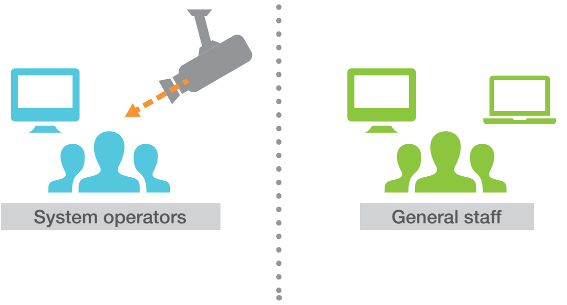
Separation of product environment and testing environment

The environment for testing products in development and the product environment for users are separated. Product environments are naturally not accessible by staff or even developers.



Separated working space for system operators

System operators work in a different area to general staff. The work space for system operators is equipped with security cameras to monitor who goes in and out.



Operation Platform

A system that's always ready to use

✓ Machines break down, people make mistakes, software has bugs

At Cybozu, we believe that the most important thing about a cloud service is the management system for the data we hold. Even in the worst-case scenario, we have all kinds of measures in place to ensure the safety of our hardware and operations so that your data is protected, and you can feel secure.

Backup System to protect user data

Data Loss Prevention and appropriate disposal

Disaster Recovery Plan

Our user data is stored safely on four storage servers, three located in East Japan and one in West Japan.

We call this backup system **'Square'**.

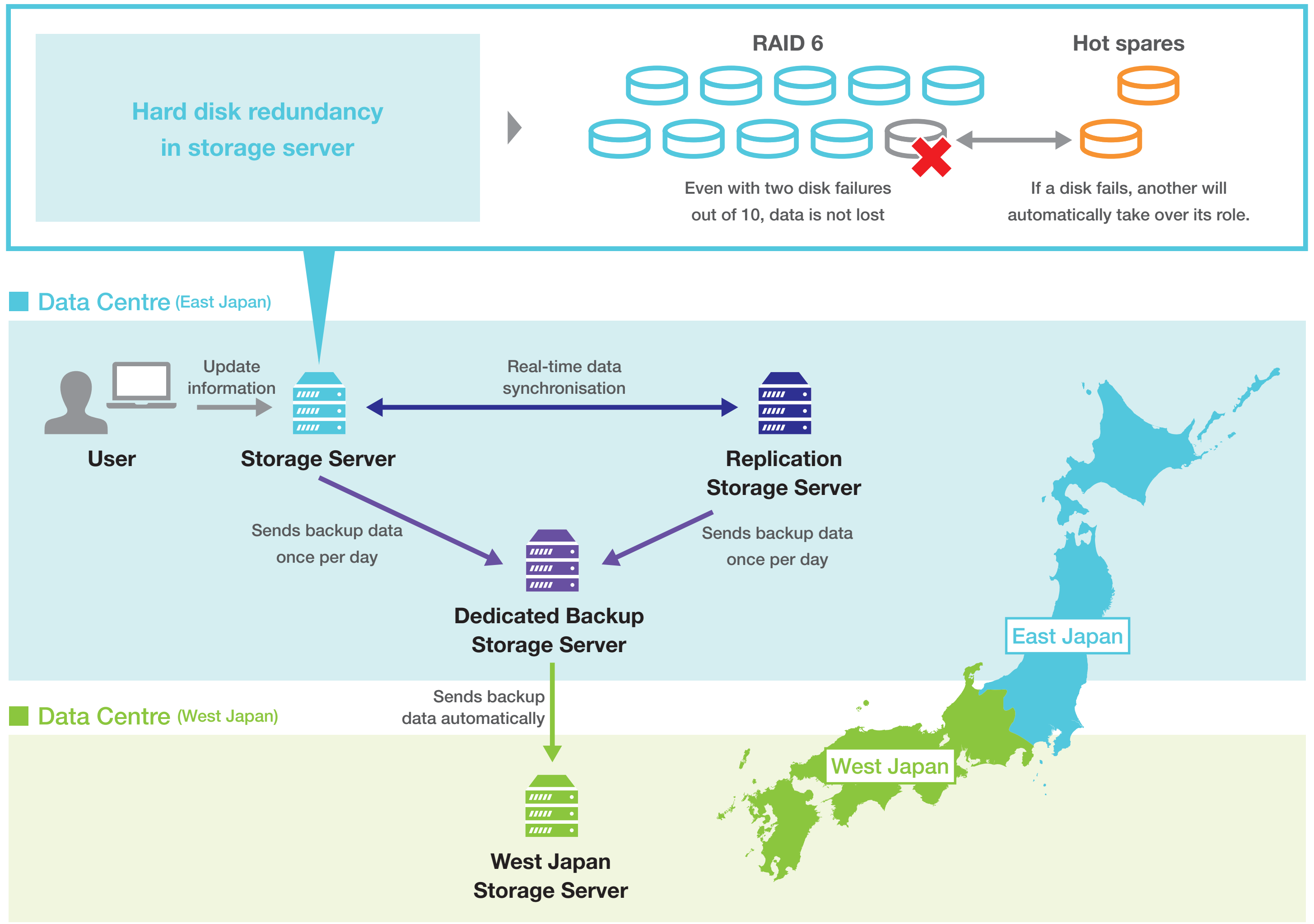
*The backup stored by Square is intended to provide for unforeseen server damage or disaster, it is not for repairing lost data caused by incorrect usage. However, there are instances when we may be able to provide restored backup data for a fee. For further information, please contact Support.

Hard Disk Redundancy (RAID 6)

The storage server to manage user data is made up of 12 hard disks per server. 10 of the 12 hard disks use a redundancy mechanism known as RAID 6, which allows two of the 10 disks to crash at the same time without any data being lost. The two additional hard disks are prepared as 'hot spares' which are permanently on standby with a management system in place to allow them to automatically switch over if a hard disk breaks down.

Backup storage servers save the most recent 14-days of differential backup data.

The East Japan Data Centre houses not only the storage servers that users normally use as well as the replication storage servers for redundancy , but also the backup storage servers. Data is received from each server once per day, storing the most recent 14-days of backup data. Thanks to having a dedicated backup storage server, even if other storage servers all broke down, the environment from the previous day would still be retrievable. We carry out restoring tests on a daily basis so we're always ready for the real thing on any given day.



Hard disk redundancy in storage server
RAID 6
Hot spares
Even with two disk failures out of 10, data is not lost
If a disk fails, another will automatically take over its role.
Data Centre (East Japan)
User
Update information
Storage Server
Real-time data synchronisation
Replication Storage Server
Sends backup data once per day
Sends backup data once per day
Dedicated Backup Storage Server
East Japan
Data Centre (West Japan)
Sends backup data automatically
West Japan
West Japan Storage Server

Mirroring (RAID 1)

When a user updates their information, the data on the storage server will be overwritten, and it will simultaneously be replicated to another storage server in real-time. We have safety measures in place to ensure that even if three or more of the hard disks in a storage server break down simultaneously or a power supply goes down, stopping the server itself, no data will be lost and our services will not stop working.

Remote Backup in West Japan Data Centre

In case a large scale disaster occurred in East Japan where our Data Centre is located, the backup data from the dedicated backup storage server is automatically sent to the Data Centre located in West Japan. Having the data stored in Data Centres that are located far away from each other serves as an effective BCP (business continuity measure) in the event of a disaster.

*The Data Centre in West Japan does not serve as hot standby for all services, only as a backup for user environments.

Reliable data centres to minimise disaster risks

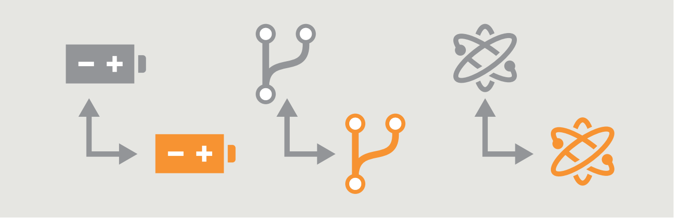
Data Centres Meet FISC Standards for Reliability

The data centres that house and manage the servers for cybozu.com comply with the exacting requirements of The Center for Financial Industry Information Systems (FISC) Facility Safety Standards. The data centres meet Tier 4 specifications, the highest level, for most of the categories in the Data Center Facility Standard regulated by the Japan Data Center Association.

*FISC (The Center for Financial Industry Information Systems)

Power Supply Line and Network Redundancy

Power supply, line and network redundancy are provided to help minimise any effects in the event of a disaster.



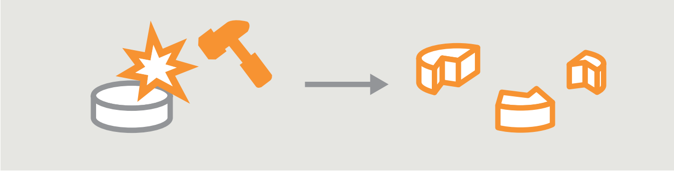
High Rating for Secure Network Encryption (SSL/TLS)

To maintain a high rating with Qualys SSL Labs, we change the encryption methods for our data centre line connections daily.

*Qualys SSL Labs is an evaluation system run by Qualys in the US.

Hard Disk Physical Destruction

After service, retired hard disks are physically destroyed to prevent any possible information leakage from such disks.



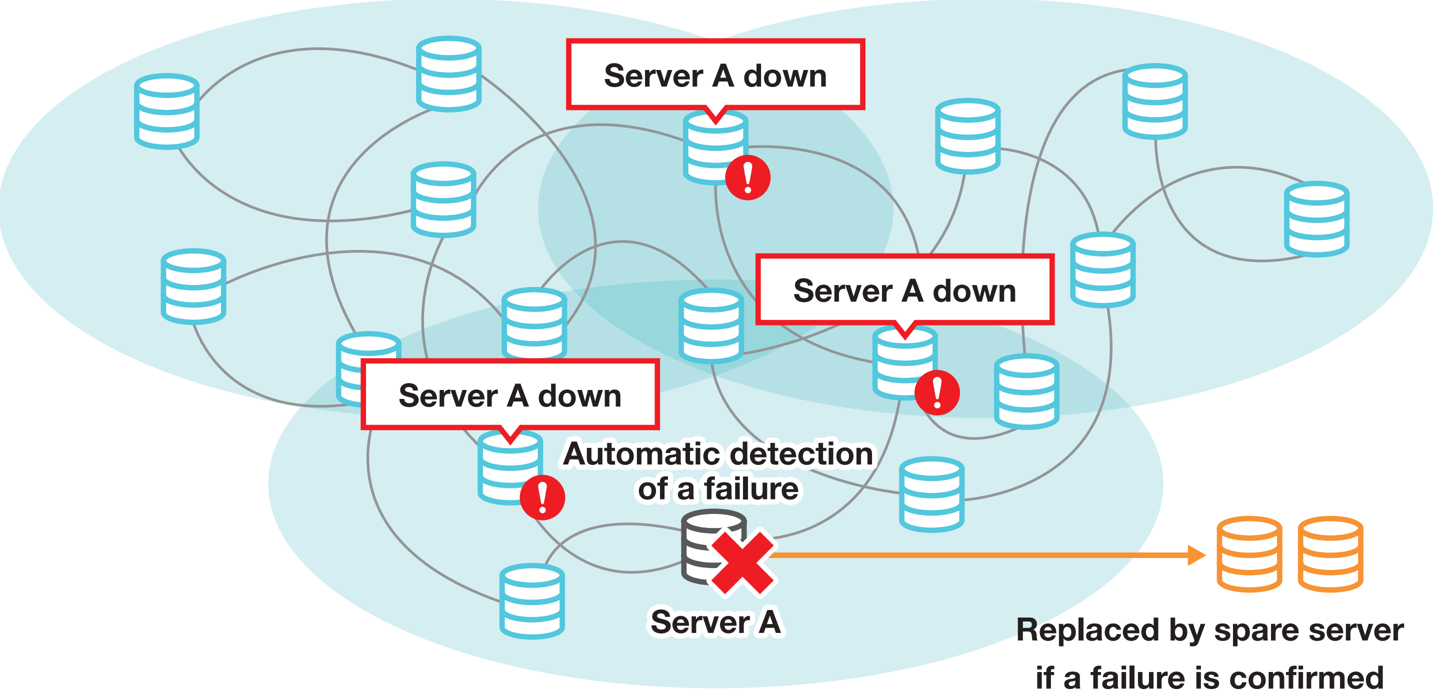
Automatically detect and prevent potential failures

Failure Management & Recovery

Autonomous failure management system

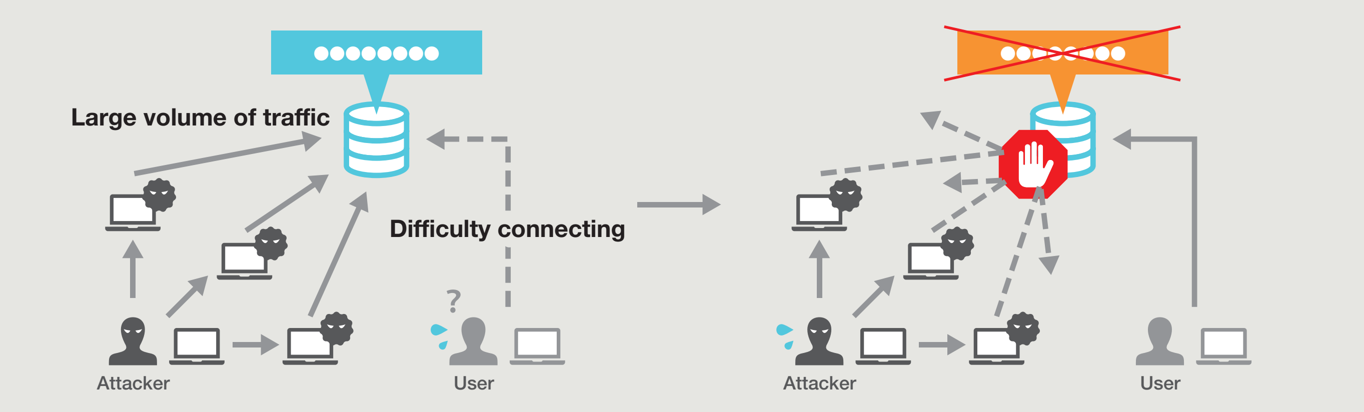
We have create an ‘autonomous decentralised agent system’ to prepare for potential damage to the virtual servers running programs or web servers for the various services. We call this system 'Tsukuyomi', after a prophet in Japanese mythology who can predict future events. Servers monitor each other to detect failures quickly. In the unlikely even that something is detected, they have to agree on whether or not it is a failure. If they conclude that it is a failure, the automatic recovery process instantly replaces the faulty server with the spare server, usually within 5 minutes.

If multiple servers briefly go down due to network damage, then a special recovery plan is initiated.


Server A down
Server A down
Server A down
Automatic detection of a failure
Server A
Replaced by spare server if a failure is confirmed

DoS, DDoS attack protection and mitigation

Denial of Service (DoS) attacks are common attacks wherein a huge volume of traffic (TCP, UDP and ICPM packets) is sent to a specific sub-domain (URL) within a very short time. In such instances, the requisite sub-domain will be automatically shut down to protect the other environments in the system. Network monitoring systems and intrusion detection/prevention systems are also in place.

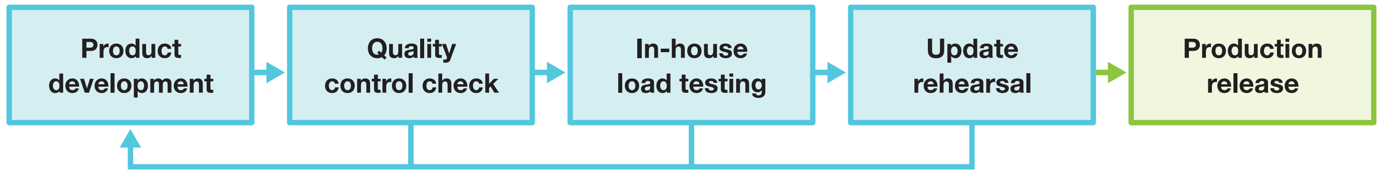


Human Error Prevention Management System

Human Error Prevention

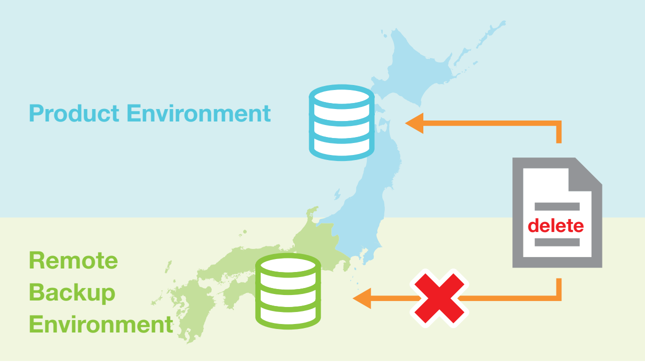
Service Updates

Systems are tested multiple times before updating to ensure that only the most stringently verified items are allowed into user environments.



Separation of product environment and remote backup environment

The product environment and remote backup environment are separated to prohibit simultaneous operation. This means that even if a program concerned with data deletion should unexpectedly take action, the remote backup data will never be simultaneously deleted.



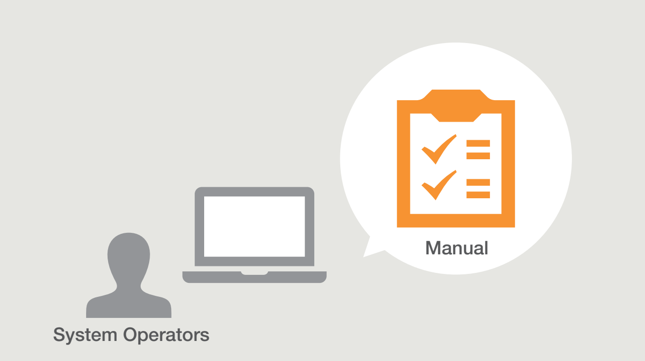
Reducing manual operation through automation

At cybozu.com, automation is promoted wherever possible to minimise the risks caused by manual errors. For example, we have automated the creation of user sub-domain environments and adding and cancelling services.

User
Eliminate manual operations

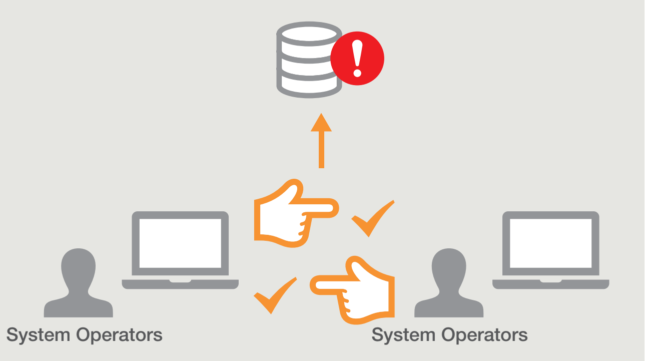
Compliance with procedures and automatic logging

Manual operations are only permitted while following prescriptive manuals. The system automatically logs all operations and allows checks on whether the rules are being followed.



Working alone is prohibited even in emergencies

For example, we allow manual operations without following a manual if a failure occurs during an emergency. However, even in an emergency, working alone is prohibited as two or more authorised system operators must always work together.



Product Environment

Service Level Objective (SLO)

To provide the most reliable infrastructure to our users, we set our targets at 99.99%* uptime rate.

*Except during planned maintenance.

Third party certification

Our Information Security Management system has achieved ISO 27001 and ISO 27017 certification from third party organisations.

ISO27001
Scope of accredited certification : Design, construction and maintenance of operational infrastructure of a cloud service developed in-house.
Date of certification : 10 November 2011 Accredited Certification number:IS 577142
Accredited certification body : BSI Group Japan

ISO27017
Scope of accredited certification : Information Security Management System (ISMS) Cloud Security Management System pertaining to system operation and maintenance of cybozu.com, Garoon and kintone as a cloud service provider
Date of certification : 10 November 2019 Accredited Certification number:CLOUD 715091
Accredited certification body : BSI Group Japan

CLOUD 715091 / ISO 27017
IS 577142 / ISO 27001

Security

Data Encryption

All data transmission and saved data is encrypted.

Vulnerability & Penetration Testing

Vulnerability tests are carried out regularly by third party organisations.

Reliability and Availability

Operating Hours

Our platform operates 24 hours a day, 365 days a year (excluding regular maintenance). Regular maintenance occurs on the second Sunday of the month between 01:00 a.m. - 07:00 a.m. (JST). During maintenance, services may be temporarily unavailable.

Planned Shutdowns

Notification of any planned shutdowns will be given one week in advance on the top page after logging in.

Redundancy

We operate a fully redundant system which includes servers, networks, storage and data.

Handling failures

Our system is continuously monitored, and in the event that a failure does occur, it is handled in accordance with the operating manual. As a rule, the target time for reporting a failure is within one hour of a failure being detected.

Updates

Platform and product updates are propagated across the platform at the same time for all users.

Data Management

Data Centre locations

cybozu.com is run from the East Japan Data Centre with backup data stored at the West Japan Data Centre.

Backup

Backups of user data are created every day nonstop.

Data Deletion

Entered data, user information and audit logs are deleted 30 days after the termination of the service contract with cybozu.com. All backup data is completely deleted approximately two weeks after the initial data deletion. However, if only part of the services within a user account sub-domain are cancelled, only the data for the parts that are cancelled will be deleted.

For Administrators

We restrict the administrators who have access to data, in line with the management system outlined in our company information security policy.

User Data Management

The data stored while using our services is to be managed solely by the user and Cybozu does not retain any right to it, unless where expressly permitted.

Support

Support Hours

Mon-Fri 9:00 a.m. - 12:00 a.m. / 1:00 p.m. - 5:30 p.m.
(Japan time: except holidays)
*Outside these times, the System Failure Help Desk is available in beta version.

Support Contact

Telephone, E-mail
*Differs according to contract type. For more details, please see the Service manual.

About cybozu.com

Find the latest information about our operation platform and security on the following websites.

cybozu.com Website Top Page

▶ https://www.cybozu.com/jp/

cybozu.com Operational Status

▶ https://status.cybozu.com/status/

cybozu.com News

▶ https://cs.cybozu.co.jp/cybozucom/

*Some information about cybozu.com services is also sent to the E-mail addresses of cybozu.com and system administrators.

cybozu.com Availability Results

▶ https://www.cybozu.com/jp/service/slo/availability.html

cybozu.com Terms of Service

▶ https://www.cybozu.com/jp/terms/

Security Checksheet

▶ https://www.cybozu.com/jp/support/data/cybozucom_securitysheet.pdf

cybozu.com
Executive Officer

Shinnosuke Saito
Manager of Cloud Service Department,
Information Technology Division
Cybozu, Inc.

cybozu.com

Cybozu, Inc.

For information about our products and services, please see our home page: https://www.cybozu.com/

*The information contained in this document is subject to change without notice.

May 2020