



Kuroco: Infrastructure Performance (Overview)

Table of Contents

- 1. Data Center**
- 2. Backup and Restore · Server Logs**
- 3. Product Security Measures**
- 4. Security Features**
- 5. Network Configuration**
- 6. Ensuring Operation of Admin Panel in the Browser**
- 7. Maintenance · Operating System**
- 8. Standard Support**
- 9. Response Flow When an Issue is Found**
- 10. Use of External Cloud Services**
- 11. Security Checklist**

1.Data Center

Kuroco is a secure cloud service platform operating on the Google Cloud Platform (GCP) - providing convenient processing power, database storage, and other features to support the scaling and growth of your business.

3 Reasons Kuroco Chooses to Use GCP

[1] Best-in-Class for Cost Performance

GCP does not require an upfront cost for preparing the infrastructure used, and only charges for the amount used by the number of users. This enables Kuroco to provide an efficient, pay-as-you-go pricing model for our users.

[2] Highest Level of iDC Security and Reliability

GCP provides a high level of security and durability, incl. numerous accreditations and audits (ex. ISO/IEC 27001, HIPAA, FedRAMP, SOC1/2/3 HIPAA, CSA STAR), which is passed on to Kuroco's users.

[3] Flexible Support for Capacity Prediction

Operating at constant maximum capacity creates additional costs and overhead. GCP makes it easy to scale capacity up or down according to your needs. It is also possible to reduce capacity during low-usage times.

Data Center • Network

Kuroco seriously considers the stability and performance of the server environment as much as possible, and uses GCP servers located in the regions our clients operate in. Google's expertise ensures constant stability, quick response times for sudden increases in traffic, and robust security. Kuroco's cloud servers are monitored 24 hours per day, 365 days per year.

We also physically maintain the security of our servers.



Google Cloud Platform

Kuroco's servers provide best-in-class operating and cost performance, with unrivaled security.

2. Backup and Restore | Server Logs

Backup and Restore

Kuroco executes a full data backup once per day between 2:00 am and 6:00 am, and stores it for 5 days (i.e. 5 generations of backup data are stored).

In the unlikely event that a failure occurs, it is possible to restore the latest backup state prior to the failure for a fee:

- Optional Paid Service

- Restore Backup Data customer

\$650 per time: entire data backup is extracted from Kuroco and restored to the

✳ Tax is included.

Server Logs

You can check the saved logs in Kuroco's admin panel. The entire service is stored in BigQuery for at least 12 months.

Log Clock Information

The log time is based on the clock used in GCP.

3. Product Security Measures (1)

Based on best practices laid out by Japan's Information Processing Promotion Agency (IPA), Kuroco develops software and operates infrastructure with appropriate security in order to eliminate vulnerabilities. This includes security issues resulting from improperly applied software patches.

To overcome security loopholes, it is necessary to always check the latest trends and take countermeasures in advance. If a vulnerability is announced by the IPA (or other authorities) it is necessary to apply any patches promptly. We are taking appropriate measures against vulnerabilities.

- Kuroco complies with IPA security policies (see: <http://www.ipa.go.jp/security/vuln/websecurity.html>)

- Typical website vulnerabilities supported by Kuroco

Web application security measures

- SQL injection
- OS command | injection
- Unchecked pathname parameter / directory traversal
- Insufficient session management
- Cross-site scripting
- CSRF (cross-site request forgery)
- HTTP header injection
- Email header injection
- Click-jacking
- Buffer overflow
- Lack of access and authorization control

- Measures that Kuroco refers to during operation

Efforts to improve the safety of websites

- Web server related
- DNS related
- Network eavesdropping countermeasures
- Phishing fraud countermeasures
- Password related (encryption)
- WAF protection of web applications
- Important measures for mobile websites

※ WAF is a standard feature offered for the admin panel and endpoints

3. Product Security Measures (2)

■ Introduction of automated vulnerability diagnosis

Kuroco has introduced an external vulnerability diagnosis tool that automatically checks the customer's site on a daily basis. It protects the website's applications (API, programs, middleware, OS), and defends against the threat of web server hacking. It also automatically scans and diagnoses external network vulnerabilities on a daily basis.

We are constantly applying countermeasure patches across the entire Kuroco platform to ensure security.

✂ Kuroco Front / Kuroco Files are statically hosted, so automatic vulnerability diagnosis is not performed.

[Deployment Tool] VAddy (Japanese) <https://vaddy.net/ja/>

[Prerequisites]

1. Used as an automation tool
2. The Kuroco admin panel is out of scope
3. When diagnosing the Kuroco admin panel or individual company sites, each company is responsible for their own diagnosis

[If a company needs evidence of vulnerability]

1. Vaddy Enterprise (59,800 yen/month) can be activated from the admin panel.
2. Diagnoses in the admin panel may result in the false positives due to the characteristics of the application.

Automated diagnoses are not recommended

4. Security Features

■ Kuroco's password management functionality (standard specification)

Detailed settings (admin panel) ensure durability and compliance with internal regulations (financial institutions, etc.)

- Encrypted password storage (hashing)
- Specify the number of characters in passwords (at least 8 characters)
- Specify the validity period/date of passwords
- Alphanumeric characters can be mixed with symbols
- Forcibly require password reset after a period of time
- Forced locking of password if incorrectly entered 5 times consecutively
- Disabling of passwords used in the past (the number of tracked previous passwords can be specified)
- Forced password change at first login functionality
- Automatic login functionality

■ https connection is always enabled, with provision of standard TLS certificate

In addition, API connections and KurocoFront have their own domains. A fixed and free TLS certificate is provided by default.

※ You cannot import a TLS certificate.

■ Restrict connections by IP address

Kuroco is able to restrict connections by IP address.

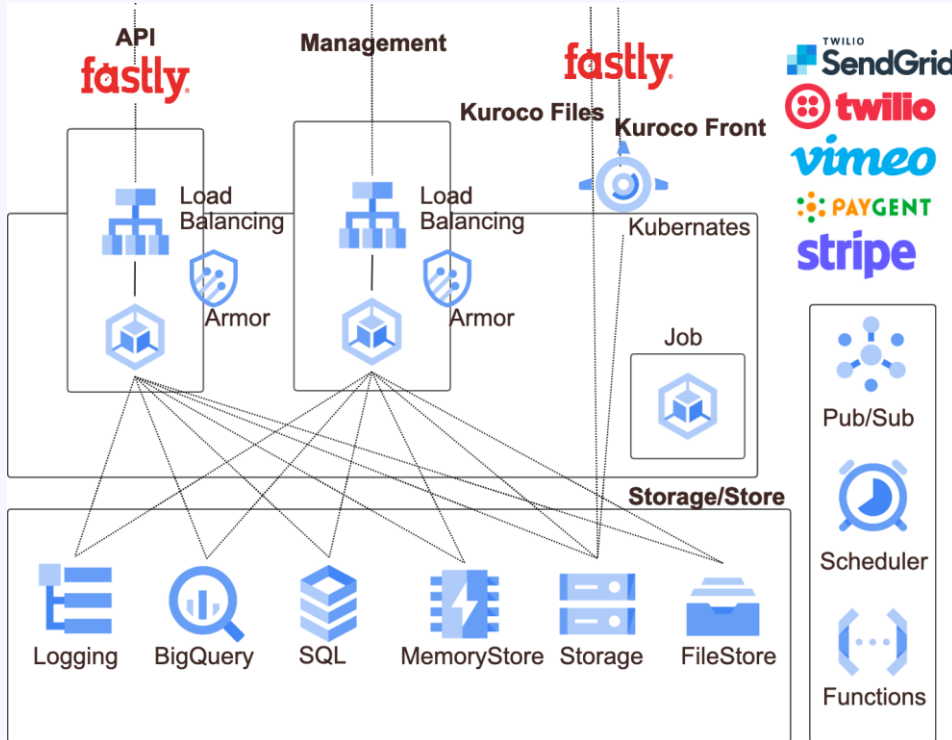
■ DoS (DDoS) attack countermeasures

In the event of unauthorized access such as a DoS attack, access will be automatically blocked by GCP (WAF) or Fastly (CDN). At present, this service is still available.

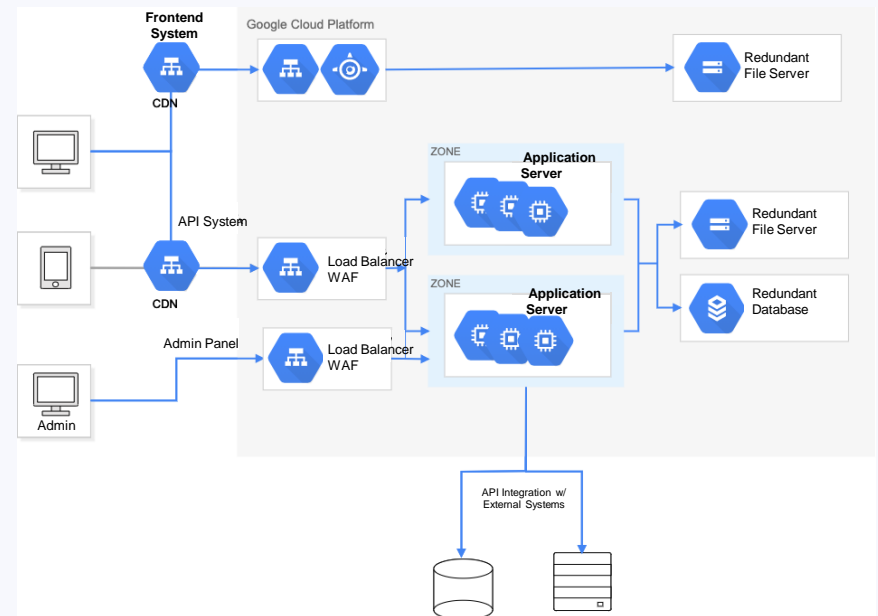
Depending on the customer, important services may be outsourced to an external server. Please contact us in advance before conducting security checks or pseudo-attacks etc. through a third-party organization.

5. Network Configuration

Kuroco has cloud-native configurations on GCP



Below is a simplified version of the diagram to the left:



Diverta Co., Ltd. improves maintainability and expandability by building a headless CMS by cloud-native development using Kubernetes:
 Reference: <https://cloud.google.com/blog/ja/topics/customers/diverta-kubernetes-cms>

6. Ensuring Operation of Admin Panel in the Browser

The following browsers are recommended for using Kuroco's admin panel:

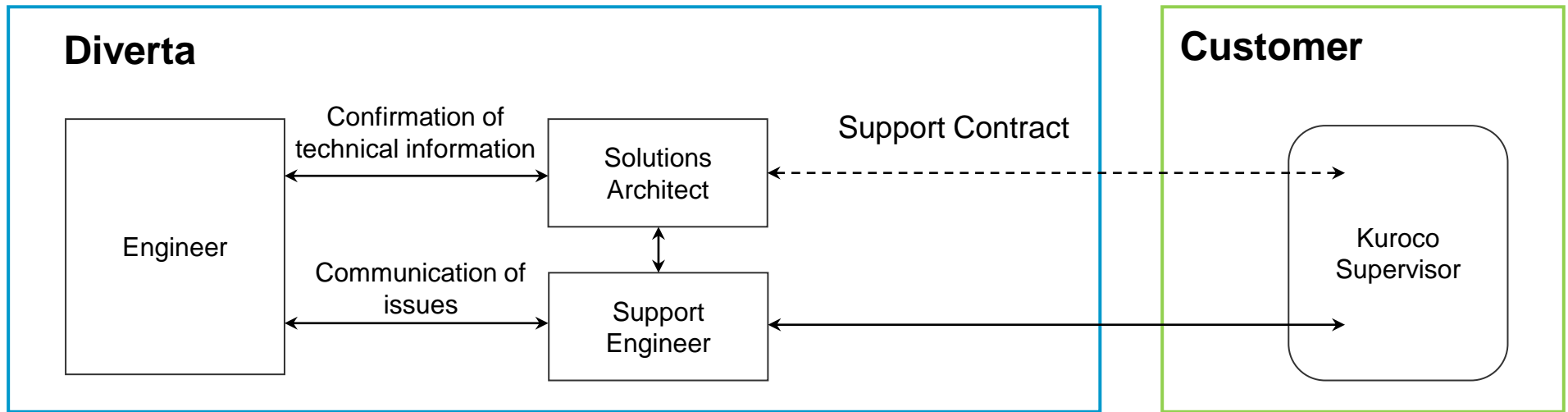
- ◆ Kuroco API / KurocoFront / KurocoFiles have no browser restrictions.

- ◆ Use of admin panel on a desktop computer:
 - Microsoft Edge (Windows 10) - latest version
 - Mozilla Firefox - latest version
 - Safari - latest version
 - Google Chrome - latest version

- ※ We recommend using the latest version of each browser

- ◆ Use of the admin panel on a smartphone or tablet
 - You can use the desktop version of the admin panel on smartphones and tablets, but depending on the size of the screen, the layout may not fit correctly and/or some functions may not work.

■ Diagram of Kuroco’s Operating System



■ Each Role

Person	Work performed	Policy for responding to failures and emergencies
Engineer	<ul style="list-style-type: none"> Managing Kuroco’s infrastructure, responding to failures, and receiving monitoring notifications. Functional design and development of Kuroco. 	<ul style="list-style-type: none"> Notifications are received by 3 engineers. Cause of failure is checked, and if 3+ hours required, person in charge or customer is contacted to report the progress as needed. For emergency responses, we will do our best to reply by Slack or Zendesk (email), including weeknights and holidays.
Solution Architect	<ul style="list-style-type: none"> Verification of customizations and settings made by the development team. (If maintenance contract exists) Notify the customer in charge. 	<ul style="list-style-type: none"> For customers who have a support contract, our solution architects will respond individually, based on the contract details
Support Engineer	<ul style="list-style-type: none"> Notification and communication to customers. Posting on support sites. Email contact. 	<ul style="list-style-type: none"> Standard support: business hours on weekdays (11:00-18:30) Inquiries can be made via Slack or Zendesk (email). In the event of a serious failure, we may notify the entire team, and send simultaneous notification by email or on the support site.

8. Standard Support

Kuroco's continuous usage fee includes infrastructure usage fees and application maintenance fees. Normally, when operating on an in-house system, it is necessary to request that the person in charge of the system or an external partner perform the work and countermeasures listed below.

The work items listed are estimates that are often overlooked and should be taken into consideration when selecting a system for installation.

■ Maintenance Work

1. Kuroco Maintenance

- Application error handling
- Fixing application bugs
- Version updates

(* Does not include operation verification tests for individual customer sites upgrading Kuroco)

2. Infrastructure Maintenance

- Infrastructure (GCP) troubleshooting
- OS, middleware security updates

■ Infrastructure Operation Work

1. Real-Time Monitoring

- (1) Life-and-death monitoring | Operational status of hardware and networks
- (2) Performance monitoring | Response time
- (3) Resource monitoring | Memory, CPU, disk status
- (4) Abnormality monitoring | Application operating status

2. Audit Log Analysis

Security officer receives audit logs, checks once a month

※ Kuroco's admin screen, front-end components other than APIs, custom programs, etc. are not covered by standard support.

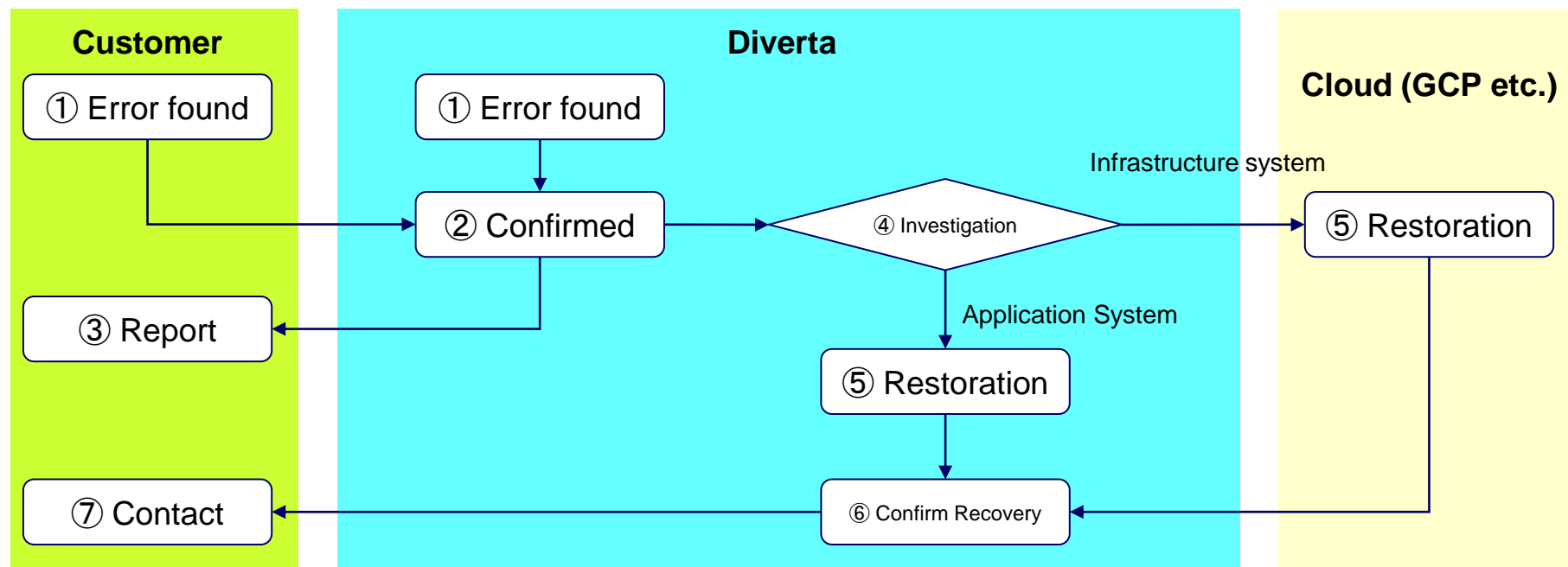
■ Kuroco SLA Guarantee

Kuroco is a cloud service with a Service Level Agreement (SLA).

This is also a quality assurance system that guarantees a high uptime for servers and refunds the usage fee at a certain rate in the event that this high rate cannot be maintained due to any server failure. We have an SLA guarantee of 99.9% per month. (31 days x 24 hours x 99.9% uptime is guaranteed).

9. Response Flow When an Issue is Found

In the event of a system failure, we will follow the flow below for response and restoration work.



- ① Failure detection: Reporting failure status when a failure is detected.
- ② Confirmation of failure: After reporting the discovery of a failure, confirm the phenomenon as soon as possible.
- ③ Situation report: Report the phenomenon as soon as possible after confirming the discovery of the failure.
- ④ Investigation of the cause: In parallel with the emergency contact, conduct an investigation to identify the cause of the system failure. After identifying the cause, **the estimated time until restoration is usually more than 3 hours:**
- ⑤ Restoration work: Restoration work will begin as soon as the cause of the system failure is identified. Select the corresponding department according to the cause of the system failure.
 - Network failure/hardware failure → Cloud Service (Diverta infrastructure engineer work)
 - Software failure → Customer or Diverta engineer work
- ⑥ Restoration confirmation: As soon as the work is completed, we will confirm the restoration of the system.
- ⑦ Contact for restoration: After confirming that the system has been restored, we will contact you for restoration.

10. Use of External Cloud Services

Kuroco has functions for integrating with external cloud services. Here are the main cloud services and their capabilities in Kuroco.

Cloud Service	Operating Company	Usage	Function
GCP	Google LLC	Required	Infrastructure
Twilio SendGrid	Twilio Inc.	Required	Email
Amazon S3	Amazon.com, Inc.	Required	Backup
GitHub	GitHub, Inc.	When Integrated	Hosting
Twilio	Twilio Inc.	When Integrated	SMS
Firebase	Google LLC	When Integrated	Storage
Vimeo	Vimeo.com, Inc.	When Integrated	Video Uploads
Slack	Slack Technologies, LLC	When Integrated	Slack API
Google Analytics	Google LLC	When Integrated	Access Analysis
VAddy	Bit Forest Inc.	When Integrated	Security Diagnosis
Paygent	Paygent Inc.	When Integrated	Payment Service

11. Security Checklist

The following security check sheets are available for Kuroco services upon request. Please visit <https://kuroco.app/ja/docs/> or contact our support team.

- "Security Implementation Checklist", supervised by the Information-technology Promotion Agency (IPA)
- Ministry of Economy, Trade and Industry (METI) published the "SLA Guidelines Appendix for SaaS (Kuroco version)"

No part of this document may be copied, duplicated, transcribed, or reproduced in any way without permission from Diverta Inc.

Reproduction, use of know-how, disclosure of trade secrets, etc. are prohibited.

- Inquiries



Diverta Co., Ltd. Kuroco Division

Central Plaza (6F), 1-1 Kaguragashi, Shinjuku-ku, Tokyo, Japan

〒162-0823

[Email] business@diverta.co.jp

