Kuroco インフラパフォーマンス概要

株式会社ディバータ

目次

1．データセンターについて

KurocoはGoogle Cloud Platform (GCP) 上で提供しているクラウドサービスであり、安全なクラウドサービスプラットフォームで、ビジネスのスケールと成長をサポートする処理能力、データベースストレージ、およびその他の機能を提供しています。

KurocoがGCPを選ぶ３つの理由

[1] 圧倒的なコストパフォーマンス

GCPはインフラを用意する初期コストが不要であり、また使用した分だけ支払う利用形態が取れるので、ユーザー数に応じて徐々にインフラを強化しやすいのが特長です。結果としてKuroco利用料金に対して適切な料金設定でKurocoユーザーにご提供が可能となります。

[2] iDC最高レベルのセキュリティと耐久性

高いセキュリティレベルと耐久性を特徴とする技術プラットフォームであり、ISO/IEC 27001、HIPAA、FedRAMP、SOC1/2/3 HIPAA、CSA STARといった数々の認定および監査に合格している堅牢性をKurocoユーザーにも提供が可能となります。

[3] キャパシティ予測にも柔軟な対応が可能

最大値を考慮してキャパシティを設定すると高額になりがちですが、GCPなら必要に応じてリソースの増減やスケールアップ、またスケールダウンの実行などが可能となります。

データセンター・ネットワーク

Kurocoはサーバの安定やパフォーマンスにも最大に考慮し、日本企業向けにはGoogle Cloud Platform（東京リージョン）を利用しています。
アクセスの集中への対応や、セキュリティの堅牢性はGoogleのノウハウが活用されています。
この選択により安定したサーバ環境と急激なトラフィックの増加などに柔軟に対応することが可能です。

サーバは国内有数のデータセンターで365日24時間監視されており、物理的にも高度なセキュリティ対策を行っています。

Google Cloud Platform

Kurocoおよび、搭載されているサーバはセキュリティ面においても万全の体制と圧倒的なコストパフォーマンスを提供します

バックアップとリストア

Kurocoは、1日1回午前2時～6時の間にフルバックアップを実施し、5日間保管致します（5世代管理）。

万が一障害等が発生した場合でも、復旧後に障害前の最新のバックアップの状態に復元することが可能です。
バックアップデータを有償にてリストア（復元）することは可能です。

■有償オプションサービス
・バックアップデータ リストア　　88,000円/1回 ・・・Kuroco全体バックアップからのお客様情報の抽出とデータ復元作業
※ 税込みです。

サーバログ

Kuroco管理画面にて、保存ログを確認することが可能です。サービス全体で最低12カ月間 BigQuery に保存しています。

ログのクロックに関する情報

ログの時間はGCP上のクロックを使用しています。

3．製品セキュリティ対策（1）

Kurocoは「情報処理推進機構(IPA) 安全なウェブサイトの作り方」に基づき、脆弱性や攻撃による影響度が大きい脆弱性を排除すべく適切なセキュリティを考慮したソフトウェア開発およびインフラ運用を実施しています。

我々クラウド事業者が適切にパッチを適用しないことで、お客様のKuroco環境またシステム全体に影響を与えるセキュリティホールが残ってしまうなどはあってはならないことですので、常に最新の動向を確認し、事前に対策を行うことはもとより、IPA等より脆弱性が発表された場合には、速やかにプログラム適用を行うことで脆弱性対策を適切に行っております。

■Kurocoが準拠するセキュリティ開発ポリシー
情報処理推進機構(IPA)推奨 『 安全なウェブサイトの作り方 改訂第7版第4刷公開』（2021年3月31）
http://www.ipa.go.jp/security/vuln/websecurity.html

■Kurocoが対応済みの代表的なWebサイト脆弱性

ウェブアプリケーションのセキュリティ対策
・SQLインジェクション
・OSコマンド・インジェクション
・パス名パラメータの未チェック／ディレクトリ・トラバーサル
・セッション管理の不備
・クロスサイト・スクリプティング
・CSRF（クロスサイト・リクエスト・フォージェリ）
・HTTPヘッダ・インジェクション
・メールヘッダ・インジェクション
・クリックジャッキング
・バッファオーバーフロー
・アクセス制御や認可制御の欠落

■Kurocoが運用時に参照している対策

ウェブサイトの安全性向上のための取り組み
・ウェブサーバに関する対策
・DNSに関する対策
・ネットワーク盗聴への対策
・フィッシング詐欺を助長しないための対策
・パスワードに関する対策（暗号化）
・WAFによるウェブアプリケーションの保護
・携帯ウェブ向けのサイトにおける注意点

※管理画面、APIエンドポイントにおいては
WAFを標準装備しております。

■DBの暗号化

データベースはGoogle CloudのCloud SQLを利用しており、AES-256で暗号化されています。

■自動脆弱性診断の導入

Kurocoでは、外部の自動脆弱性診断ツールを導入しており、代表サイトに対して日次でチェックを実施しております。

Webサーバーに対するハッキングの脅威に対し、Webサイト内のアプリケーション（API、プログラム、ミドルウェア、OS）に加え、ネットワークの脆弱性を毎日自動的に外部からスキャンし、診断を行います。

そこで発見された対応事項については随時Kuroco全体へのパッチ適用を行っております。
※Kuroco Front/Kuroco Filesに関しては静的ホスティングになりますので、自動脆弱性診断は実施しておりません。

［導入ツール］　VAddy　https://vaddy.net/ja/

［前提条件］

1．自動診断型ツールを採用しています。
2．Kurocoの管理画面側は対象外です。
3．Kuroco管理画面、また各社個別のサイトを診断する場合には各社様独自で実施して頂いております。

［各社様でエビデンス等が必要な場合］

1. VaddyのEnterprise(月額59,800円)が管理画面から利用できますので、そちらからお申し込みください。
2. Kuroco管理画面の診断に関しては、アプリケーションの特性上、誤検知が多くなりますので、
   自動診断はお勧めしません。

■Kurocoのパスワード管理機能（標準仕様）

管理画面よりさまざまな細かい設定が可能です。金融機関などの社内規定にも準拠しており堅牢性を確保します。
・パスワードの暗号化保存（ハッシュ化）
・パスワードの文字数指定（8文字～）
・パスワードの有効期間日指定
・英数字記号混合でのパスワード強制化が可能
・指定期間が経過したパスワードを強制的に変更させる機能
・パスワード入力を5回連続で間違えた場合の強制ロック機能
・過去に利用したパスワードを利用できなくする機能（遡る回数指定可能）
・初回ログイン時にパスワード変更を強制する機能
・オートログイン機能

■https常時接続および標準TLS証明書の提供

通信は全てhttpsに限定されておりTLS証明書も標準提供されています。また、API通信及びKurocoFrontは、独自ドメインの設定と無料TLS証明書の標準提供が可能です。

■IPアドレスによる接続制限

KurocoはIPアドレスによる接続制限が可能です。

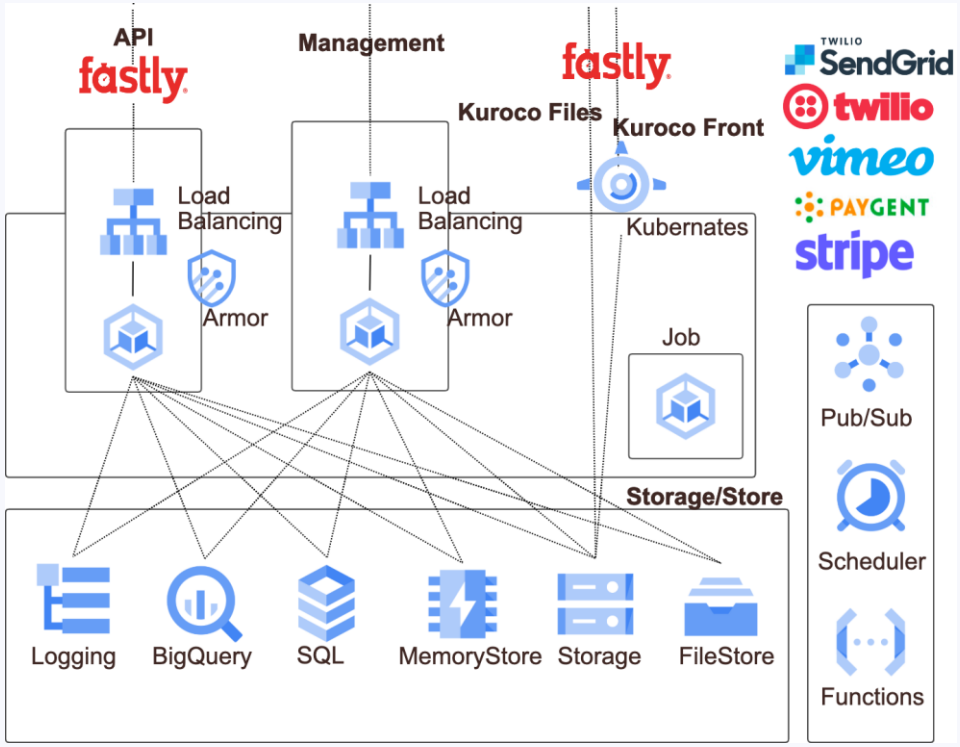
■ DoS（DDoS）攻撃対策について

現状のKurocoではDoS攻撃のような不正アクセスが発生した場合には、
GCP(WAF)またはFastly(CDN)で自動ブロックがされる対応となっております。
現状ではサービス停止に至る事態にまでは至っておりません。
お客様によっては自社の重要なサービス運営を外部サーバに委託することになりますので、第三者機関を通じたセキュリティチェックや疑似アタックを実施するなどのケースは事前にご連絡頂いた上で、実施が可能でございます。

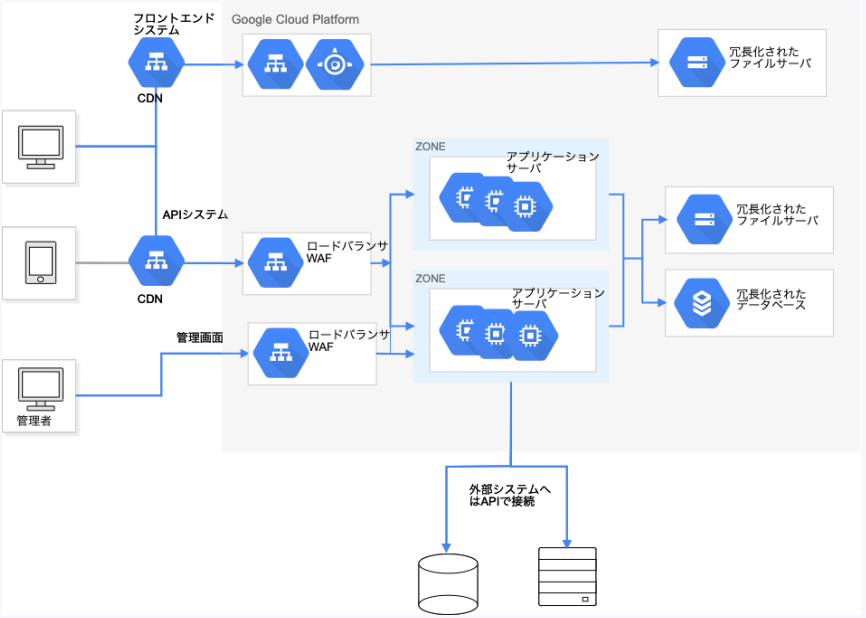
5．ネットワーク構成に関して

Kuroco は GCP 上でクラウドネイティブな構成になっております。また、3 つの AZ で冗長化構成をとっており、高い安定性を実現しております。

アプリケーションは Google Kubernetes Engine（GKE） 上で運用されており、アクセスの増減に応じて自動的にリソースをスケールアップ・スケールダウンできるオートスケーリング機能に対応しています。これにより、ピーク時のトラフィックにも柔軟かつ効率的に対応可能です。



以下は左記の図を簡易にしたもの



参考）株式会社ディバータ：Kubernetes を活用したクラウド ネイティブ開発によるヘッドレス CMS の構築で、メンテナンス性や拡張性を向上
https://cloud.google.com/blog/ja/topics/customers/diverta-kubernetes-cms

Kurocoの管理画面は下記のブラウザを推奨ブラウザとしております。

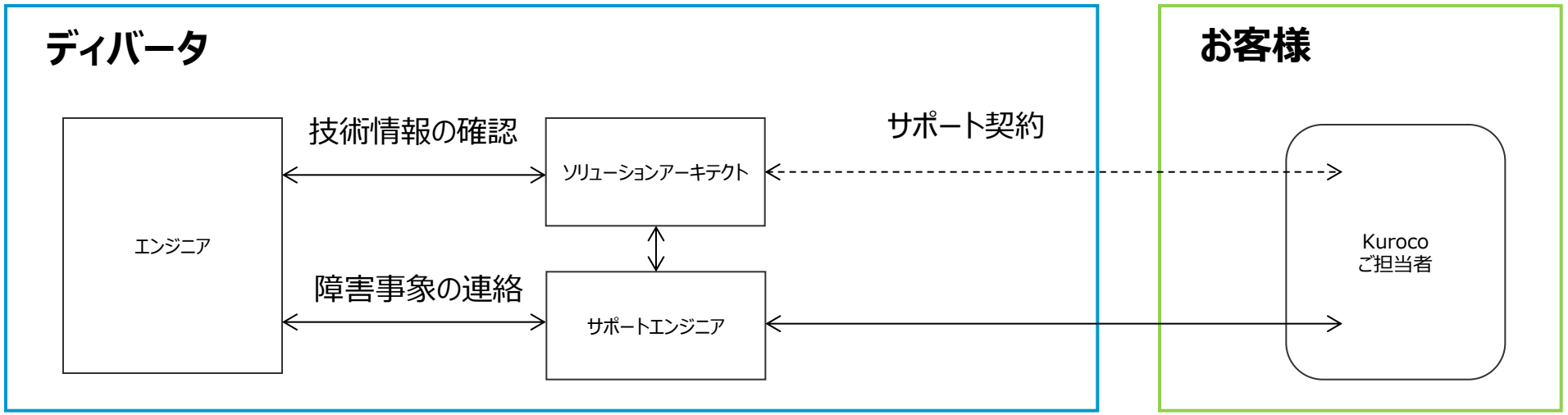
◆ Kuroco API/Kuroco Front/Kuroco Filesはブラウザ等の制限はありません。

◆管理画面のPCからの利用
・Microsoft Edge（Windows 11）最新版
・Mozilla Firefox　最新版
・Safari　最新版
・Google Chrome 最新版

※それぞれ最新版を推奨します。

◆管理画面のスマートフォン、タブレットからの利用
・スマートフォンやタブレットはPC向け管理画面がご利用いただけますが、画面のサイズによってはレイアウトが崩れたり、一部機能が動作しない場合があります。

■Kuroco運用体制図



■各自の役割

担当職務	作業内容	障害時・緊急時の対応方針
エンジニア	・Kurocoのインフラ管理および障害時の対応と、監視通知の受信 ・Kurocoの機能設計、開発	●監視通知は常時3名のエンジニアが受信しベストエフォートで対応 ●障害の原因調査を行い、復旧までに3時間を超えると判断した場合は担当またはお客様に連絡し、進捗を随時報告。 ●緊急時の対応についてはSlackかZendesk(メール)にてベストエフォートですが休日夜間の対応も行います。
ソリューション・アーキテクト	・開発チームが行ったカスタマイズや設定の確認作業。 ・（保守契約がある場合）担当のお客様への通知、連絡。	●サポート契約を締結中のお客様についてはソリューション・アーキテクトが契約内容に基づき個別対応
サポートエンジニア	お客様への通知、連絡。サポートサイトへの掲載。メール送信連絡。	●標準サポートは平日の営業時間11:00～18:30 ●問合せ方法はSlackかZendesk(メール)での対応 ●障害発生時は影響度合いにより全社への通知が必要と当社が判断した場合は、メールによる一斉通知、またはサポートサイトへの告知を実施。

Kurocoの継続利用料にはインフラ利用料とアプリケーション保守に関する費用も含んでおります。通常、自社システムで運営する場合には下記に挙げる作業や対策をシステム担当者や外部パートナーに作業依頼を行う必要があります。
ここに挙げている作業項目は見落とされがちな見積項目であり、システム導入選定の際には考慮すべき内容です。

■保守作業

１．Kuroco保守
・アプリケーションの障害対応
・アプリケーション不具合の改修
・バージョンアップ対応
（※Kurocoのバージョンアップ時の個々のお客様サイトの動作検証テストは含まれません。）
２．インフラの保守
・インフラ（GCP）の障害対応
・OS、ミドルウェアのセキュリティアップデート

■インフラ運用作業

１．リアルタイム監視について
（１）死活監視｜ハードウェアやネットワークの運転状況
（２）性能監視｜レスポンスタイム
（３）資源監視｜メモリ、ＣＰＵ、ディスクの状態
（４）異常監視｜アプリケーション稼働状況

２．監査ログ分析
セキュリティ責任者が監査ログを取得し、月1回確認

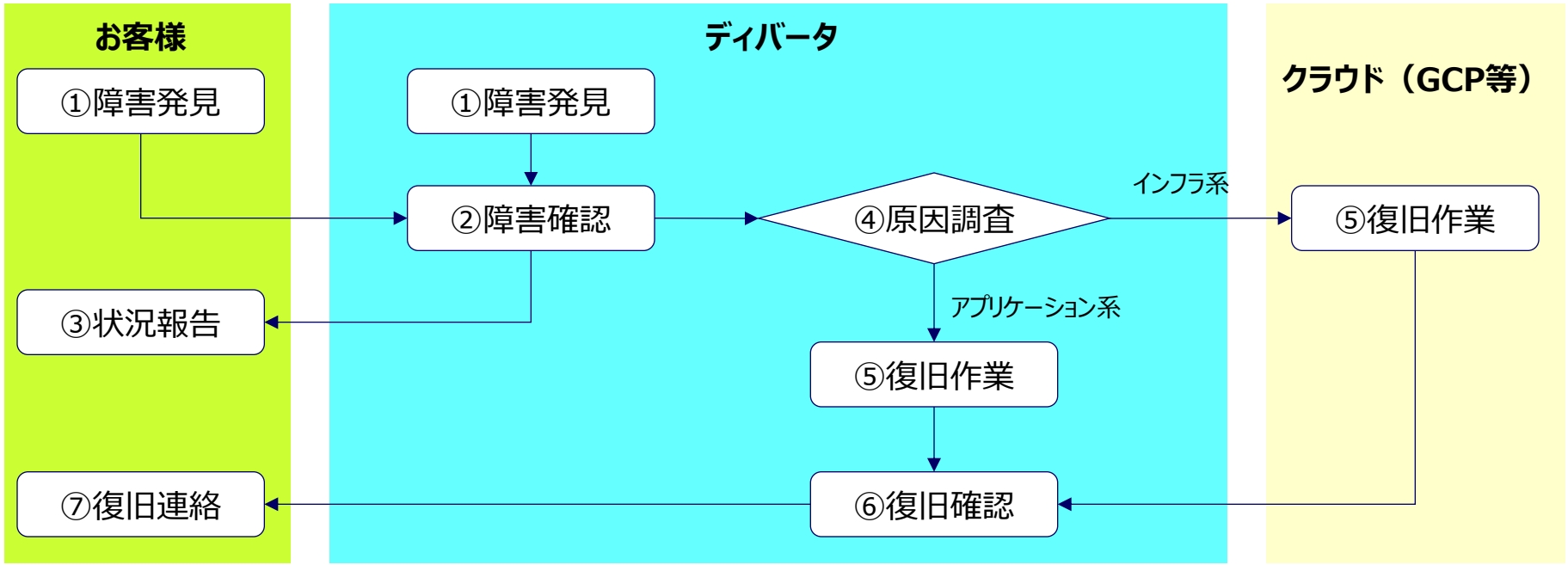
※Kurocoで提供している管理画面、API以外のフロントエンドやカスタムプログラムなどの動作保証は標準サポート対象外です。

■KurocoのSLA保証

Kurocoはサービス品質保証制度（SLA）を定めているクラウドサービスです。
サーバーの高稼働率を保証し、万一のサーバー障害などで高稼働率を維持できない場合、一定の割合で利用料金を返金する品質保証制度でもあります。１ヶ月あたり99.9%のSLA保証を設定しております。（31日×24時間×99.9%の稼働を保証）

9．障害発生時の対応フロー

システムに障害が発生した場合には、下記のフローにて対応・復旧作業を行います。



①障害発見：障害発見時には障害状況の報告。
②障害確認：障害発見の報告後、早急に現象の確認を実施。
③状況報告：障害発見の確認後、早急に現象の報告を実施。
④原因調査：緊急連絡と平行し、システム障害の発生している原因を特定するための調査を行う。また原因特定後、
復旧までに３時間を超えると予測できる場合には進捗を報告する。
⑤復旧作業：システム障害の原因の特定が完了し次第、復旧作業を開始する。システム障害原因によって、対応する部門を選定。
○ネットワーク障害/ ハードウェア障害→クラウドサービス（ディバータ インフラエンジニア作業）
○ソフトウェア障害→お客様もしくはディバータエンジニア作業
⑥復旧確認：復旧作業が完了し次第、システムの復旧確認を行う。
⑦復旧連絡：システムの復旧確認後、復旧連絡を行う。

10. 外部クラウドサービスの利用

Kurocoでは、外部のクラウドサービスとの連携機能を持っています。
主なクラウドサービスとKurocoでの機能を次に示します。

クラウドサービス	運営会社	利用区分	機能
GCP	Google LLC	必須	インフラ構築
Twilio SendGrid	Twilio Inc.	必須	メール送信
Amazon S3	Amazon.com, Inc.	必須	バックアップ機能
GitHub	GitHub, Inc.	連携時	ホスティング
Twilio	Twilio Inc.	連携時	SMS送信
Firebase	Google LLC	連携時	ストレージ利用
Vimeo	Vimeo.com, Inc.	連携時	動画アップロード
Slack	Slack Technologies, LLC	連携時	Slack APIの利用
Google Analytics	Google LLC	連携時	アクセス解析
VAddy	株式会社ビットフォレスト	連携時	脆弱性診断
Paygent	株式会社ペイジェント	連携時	支払サービス

11. セキュリティチェックシートの提供

Kurocoのサービスについて下記のセキュリティチェックシートの用意があり、提供が可能です。
提供を希望する場合は https://kuroco.app/ja/docs/ を参照の上ご連絡下さい。

- 独立行政法人情報処理推進機構（IPA）監修「セキュリティ実装チェックリスト」
- 経済産業省（METI）発刊「SaaS向けSLAガイドライン別表（Kuroco版）」
- セキュリティ評価プラットフォーム「Assured（アシュアード）」（別途 Assured のご契約が必要です）

お問い合わせ

株式会社ディバータ Kuroco事業部

〒162-0823　東京都新宿区神楽河岸1-1　セントラルプラザ6階
[Email]　business@diverta.co.jp