L-002

# 安寧で持続可能なサイバーコミュニティシステムの試作と評価
# Feasibility Study of Reliable and Sustainable Cyber Community System for Kyoto City

横山 淳† 今井 賢治‡ 前田 悠希† 内藤 昭三‡
Atsushi Yokoyama Kenji Imai Yuki Maeda Shozo Naito

## 1. まえがき

近年, 観光立国の実現に向けた取り組みを背景に[1], 地域ブランドの発信や地域活性化を図った地域社会の ICT 利活用が強く進められている. 一方, 2015 年度の日本年金機構個人情報漏洩[2]や, 2016 年度の佐賀県学校教育ネットワークに対する未成年の不正アクセスの問題[3]に見られるように, ICT 利活用は高いセキュリティレベルに準拠したシステムにより進められなければならない. 従って, 地域ブランド構築, 地域活性を促進しつつ, かつセキュアな情報基盤を担える ICT システムの構築は喫緊の課題といえる.

本稿では, 前述の様な ICT システムの構築に向けた, 一般の都市計画で施行される"防犯対策", "景観政策"をインターネット空間に展開するシステムについて紹介する. 本システムは, 本研究の共著者であるサイバー京都研究所が管理している「.kyoto」ドメインにて試験運用されており, その結果に沿って報告する. 前述の"防犯対策", "景観政策"を担うシステムは, それぞれ「京都セキュリティ」, 「京都クオリティ」と呼称される. 図 1 に京都セキュリティ, 京都クオリティ, および.kyoto ドメインを含むシステムの全体構成図を示す.

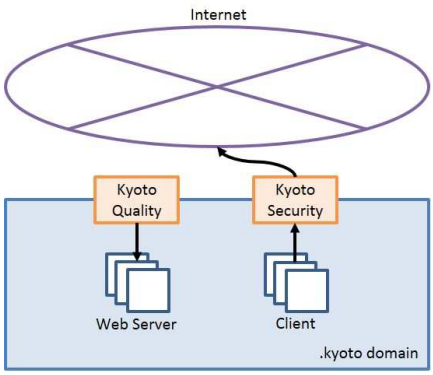



図 1　本システムの全体構成図

## 2. 京都セキュリティの実現

京都セキュリティは, .kyoto ドメインを利用しているユーザに, 安全なインターネット環境を提供し, ICT 利活用を促進するシステムである. 安全なインターネット環境を提供する方法としては, DNS RPZ (Response Policy Zones)を採用する[4]. DNS RPZ とは, ユーザが悪意のあるウェブサイトへアクセスを試みた際に, DNS サーバ側で安全なウェブサイトへ誘導するセキュリティ手法のことである.

### 2.1 システム概要

図 2 に, 京都セキュリティの処理の流れを示す. 本システムは, 悪意のあるウェブサイトの情報を管理する管理 DNS サーバ, 悪意のあるウェブサイトをブロッキングし, 安全なウェブサイトへ誘導する DNS RPZ サーバ, 正常なリクエストを処理する権威 DNS サーバの 3 つの DNS サーバから構成される.

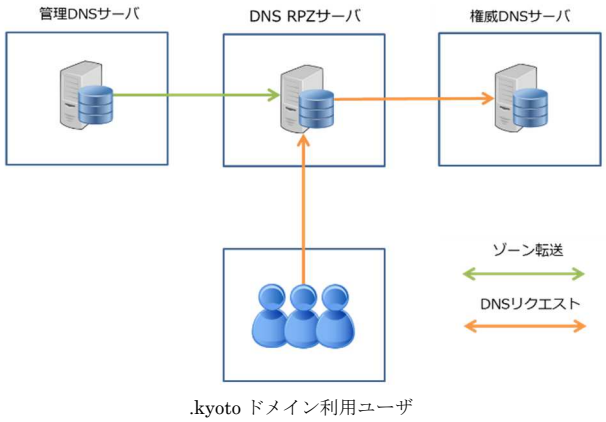



図 2　京都セキュリティの処理の流れ

.kyoto ドメイン利用ユーザは, ウェブサイトへのアクセス時に DNS RPZ サーバにより名前解決を行う. DNS RPZ サーバは, 常時, 管理 DNS サーバの情報を参照しており, ユーザからのリクエストが悪意のあるウェブサイトであるならば, 安全な誘導先のウェブサイトをレスポンスする. 正常なリクエストであるならば, 権威 DNS サーバに処理をデリゲーションし, その結果をユーザにレスポンスする.

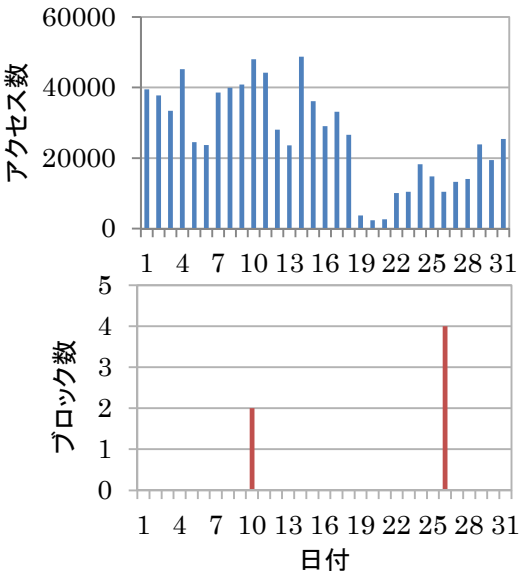
### 2.2 実験

本システムを府内の協力法人・個人, 合わせて 10 団体に導入し, 2017 年 2 月中旬より実証実験を開始した. 悪意のあるウェブサイトの情報として, 約 800 万件分の情報を収集した環境下で実験を行った.

表 1 に全ユーザの日別の総アクセス数, およびブロック数を示す. 合計約 868,000 アクセス中, 6 回のブロックの発生が確認された.

ブロックされたウェブサイトは, アクセスした端末に侵入, 破壊等を行うクラッキングサイト, または詐欺行為を目的とするフィッシングサイトのどちらかであった. ユーザのアクセス経路は不明であるが, いずれもインターネットの掲示板, ブログ, スパムメールに, 低価格でのブランド品, ドラッグ品の提供を謳う文言と URL を貼付する方法でユーザの誘導を図っていた. ユーザを悪意のあるウェブサイトに導く手法が多様化する中で, 出口戦略としてウェブセキュリティや DNS RPZ を採用する重要性を示す結果といえる.

表 1 総アクセス数とブロック数(3 月分)




## 3. 京都クオリティの実現

京都クオリティは, 都市計画の”景観政策”に擬え, .kyoto ドメイン内のウェブサイトの品質を審査するシステムである. .kyoto ドメイン内部のウェブサイトを定期的に巡回し, 「京都らしさ」,および「デザイン品質」の 2 点に関して品質を評価する.

### 3.1 システム概要

「京都らしさ」, および「デザイン品質」は, ディープラーニング[5]による学習結果を用いて評価される. それぞれ, 「京都らしい」・「京都らしくない」画像, 「品質の良い」, 「品質の悪い」画像を分類問題として学習させ, ドメイン内のウェブサイトや画像を評価する.

図 3 は, 京都クオリティのシステム構成である. 本システムは 3 つのサブシステムから成り立っており, それぞれデータ収集を担当する Data Collection System, 収集したデータを学習する Learning System, 評価を実施する Verification である.

Data Collection System は, キーワード検索により画像収集を行う. 「京都らしい」, 「京都らしくない」, 「品質の良い」, 「品質の悪い」の全 4 種の画像を収集する. 「京都らしい」キーワードは全部で 299 ワード用意し, 204335 画像収集した. その後, 目視によりノイズ除去し, 49088 画像に絞り込んだ. 表 3 に抜粋したキーワードを示す. 「京都らしくない」キーワードは「大聖堂」, 「トロピカル」, 「高層ビル」など全 127 ワードであり, 91197 画像を収集した. 「品質の良い」, 「品質の悪い」画像はそれぞれ, 4007 枚, 52849 枚収集した. キーワードは, 共著者である京都サイバー研究所が定めている. 「品質の悪い」画像は, internet archive[6]を活用し, 古いウェブサイトを巡回することで収集している.

Learning System は, 取集した 4 種の画像をディープラーニングにより学習する. かつ, サーバとして機能し, 画像をクエリーとして受信すると, 評価結果を返答する. ディープラーニングの構成は図 4 の通りである. 本ディープラーニングは, 64×64 pixel にサイズを変更した画像を入力とする. 特徴次元 50 の 3×3 の Convolution 層を次段に配置し, その後 2×2 の Pooling 層を配置する. Convolution とはエッジ等の特徴を抽出する処理のことであり, 特徴次元は抽出する特徴数を示している. Pooling とは, 微小な空間変化に対する不感性を得る為に局所的な特徴を収縮させる処理のことである. 同様の層を 3 層繰り返し, その後, 特徴次元 300 の Fully connected 層を配置する. Fully connected とは空間情報を集成し, 全特徴を結合する処理のことである. 次段に, 汎化性能を向上の為に反応をランダムに不感にする Drop out 層を配置し, 最後に, 分類の為に Softmax 層を加えた構成となっている.

Verification は, .kyoto ドメイン内のウェブサイトのスクリーンショット, または入力された画像を Learning System に問い合わせる機能を持つ.

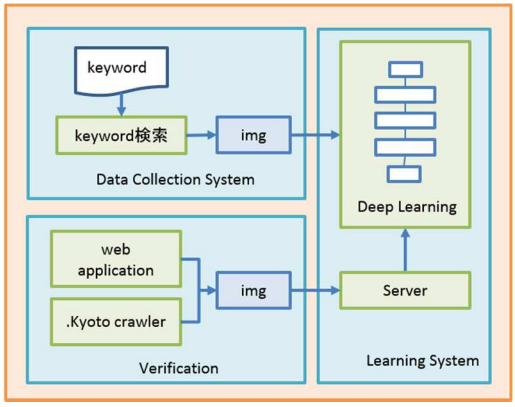



図 3 京都クオリティの処理の流れ

### 3.2 実験

評価用画像として, 「京都らしい」, 「京都らしくない」, 「品質の良い」, 「品質の悪い」の 4 種, それぞれ 146 件, 21 件, 54 件, 100 件を上述と同様の方法で,収集し, 本システムの精度を確認した. 京都らしさは, 「京都らしい」と 0.85 以上で判定された画像のみ「京都らしい」と判定, 「品質の良い」と 0.85 以上で判定された画像のみ「品質の良い」と判定するルールを設定した.

結果は表 4 の通りである. また, 誤判定となった画像の例を図 5 に示す.

表 3 「京都らしい」キーワード抜粋

| | | | |
|---|---|---|---|
| 嵯峨ぎく | 嵐電 | 京町屋 | 京懐石 |
| 清水坂 | 紫式部 | 茶道 | 清水焼 |
| 狂言 | 枯山水 | 舞妓さん | 賀茂なす |

表 4 京都クオリティ評価結

| | 京都らしさ | デザイン品質 |
|---|---|---|
| 検知率 | 81.5% | 62.9% |
| 誤検知率 | 7.4% | 8.0% |

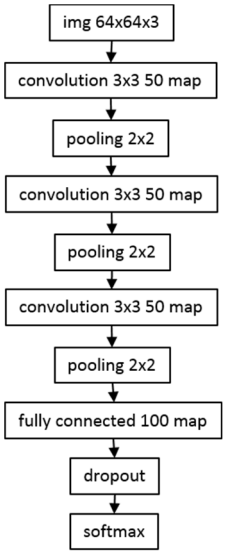



図 4　ディープラーニング構成図

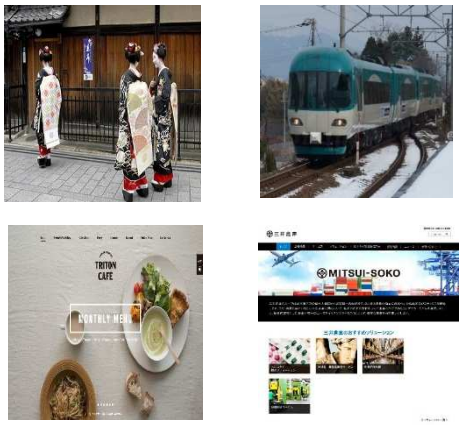



図 5　誤判定画像
(上段) 京都らしさ誤判定画像. 「京都らしい」画像にも関わらず, 「京都らしくない」と判定された画像. (下段) デザイン品質誤判定画像. 「品質が良い」画像にも関わらず, 「品質が悪い」と判定された画像

## 4. おわりに

セキュリティを担保しつつ, かつ地域ブランドの発信・活性化を図る ICT システム構築の一環として, 本稿では「京都セキュリティ」, および「京都クオリティ」について紹介した. 前者の「京都セキュリティ」については, 試験運用の段階であり, 悪意のあるサイトへのアクセスを遮断するなど効果も確認されている. 今後は, 精度の向上を図るだけではなく, DNS ブロッキングの問題の一つとして指摘されている「通信の秘密」への抵触性[7]についても議論を深め, 実運用への移行を視野に研究を進めていく予定である.

また, 後者の「京都クオリティ」であるが, いわゆる「～らしさ」や「～感」といった人間の持つ感覚を取り扱う問題であり, 一般的な分類問題と比較して, 定義が明確でない故に特有の難しさがある. 問題を俯瞰した場合, 「京都らしさ」とは何かという逆問題を解いている立場に近い. また, 本研究では, 「枯山水」, 「賀茂なす」, 「舞妓さん」などのキーワードを, それぞれ別のタグに分類するのではなく, 1 つの「京都らしさ」というタグに集約している. 一般的にはタグを集約することは精度の低下に繋がる為, 避けられる方法ではあるが, Grad-CAM[8]などのディープラーニングの判断を可視化する手法を使うことで, 与えられた画像の何が京都らしいのか, 何が京都らしくなかったのか, 判断基準を把握することができる. 故に, 「京都らしさ」という 1 つの基準に集約させることで総合的な「京都らしさ」を判別することが可能になり, 隠された「京都らしさ」などを人工知能の認識能力により発見することもできよう. 現在, 精度面含め道半ばであるが, 歴史的・文化的深みのある「京都らしさ」というものの発見が, ディープラーニング, そして本研究により成されることを期待している.

### 謝辞

本研究実施するに当たりアドバイス頂いた株式会社データ変換研究所 代表取締役 畑中豊司氏, 京都情報大学院大学 准教授 立石聡明先生, 同大学 湯下秀樹先生に感謝致します. また, 本研究は, 公益財団法人京都産業２１ 平成２８年度地域産業育成産学連携推進事業の助成を受けて行われました. ここに感謝の意を表明します.

### 参考文献

[1] 国土交通省観光庁, “観光立国の実現に向けた取り組み”, https://www.mlit.go.jp/common/000131293.pdf, (閲覧日: 2017 年 5 月 2 日)
[2] 内閣サイバーセキュリティセンター サイバーセキュリティ戦略本部, “日本年金機構における個人情報流出事案に関する原因究明調査結果”, https://www.nisc.go.jp/active/kihon/pdf/incident_report.pdf (閲覧日: 2017 年 5 月 2 日)
[3] 佐賀県学校教育ネットワークセキュリティ対策検討委員会, “提言書”, http://www.pref.saga.lg.jp/kyouiku/kiji00351508/3_51508_25075_up_7t66188r.pdf (閲覧日: 2017 年 5 月 2 日)
[4] RPZ Community, “DNS RPZ Portal”, https://dnsrpz.info/ (閲覧日: 2017 年 5 月 2 日)
[5] Alex Krizhevsky, Ilya Sutskever, Geoff Hinton, “Imagenet classification with deep convolutional neural networks”, In Advances in Neural Information Processing Systems, 25, (2012).
[6] The Internet Archive, “Internet Archive: Wayback Machine”, https://archive.org/ (閲覧日: 2017 年 5 月 2 日)
[7] 児童ポルノ流通防止協議会, “ブロッキングに関する報告書”, 一般財団法人インターネット協会 https://www.iajapan.org/press/pdf/siryou5-20100325.pdf (閲覧日: 2017 年 5 月 2 日)
[8] Ramprasaath R. Selvaraju, et al., “Grad-CAM: Visual Explanations from Deep Networks via Gradient-based Localization”, arXiv preprint arXiv:1610.02391 (2016)

† アイマトリックス株式会社
‡ 京都情報大学院大学 サイバー京都研究所