

IDカード読取データを用いたキャンパス滞在証跡提示環境の試作 A Prototype Design for Attendance Confirmation System by Scanned ID Card Data

板東孝文, 松浦健二

Takafumi BANDO, Kenji MATSUURA

{bandou.takafumi, ma2}@tokushima-u.ac.jp

徳島大学 情報センター

Center for Administration of Information Technology, Tokushima University

概要

働き方改革の推進に伴い、労働時間の適正化という観点から、就業者の労働時間に関する客観的データ照合が求められている。すなわち、厚生労働省が策定したガイドラインに則り、客観性のある、申告制と証跡との照合に関するプロセスを検討する必要がある。そのような背景の下、キャンパス内の滞在を示す客観的データを収集、蓄積、配布するための環境の設計と試作を行った。本論文では、その設計について述べ、運用を想定した際の課題を論じる。

キーワード

職員証, セキュリティゲート, 働き方改革, Shibboleth

1 はじめに

昨今、労働時間の適正化に関心が寄せられており、使用者による労務管理における労働時間の管理方法や、その管理データの信頼性が課題となっている。国立大学法人等では、職員就業規則により定められている雇用形態などに応じて、就労者による労働時間の申告と、使用者による確認が行われていると考えられるが、必ずしも客観的な方法で行われているとは言えない。また、雇用形態の多様化により、労働時間に関しても、その根拠データが一元的に管理されるのには課題があると考えられる。

そのため、労働時間の実態の把握という点では透明性が低くなる可能性があることが課題の一つとして挙げられる。一方で、2019年4月から働き方改革関連の法案が施行され、国立大学法人においても、その推進が求められている。そのような背景から、客観的かつ信頼性の高い、一元的な労働時間管理方法の整備が課題として挙げられていた。そのためには、客観性の高い正確な証

跡データと、その運用環境が必要である。

また、近年では、情報技術の発展により、情報システムを利用した勤怠管理 [1] が提案されており、本学においても、既存の情報システムとの連携を考慮した環境を構築することにより、効率的な運用が期待できる。

そこで、情報センターでは平成30年度に、大学全体の労務管理を統括する総務部人事課と協議し、セキュリティゲートにおけるIDカードの読取データを応用したキャンパス滞在証跡提示環境の試作を行った。

本学における就労者は、雇用形態と、それに基づく勤務体系が多岐にわたり、勤務環境、勤務時間が多様である。そこで、キャンパス内のセキュリティゲートのIDカード読取データを利用することにより、ある程度網羅的に滞在の根拠データの収集が期待できる。また、個人に一意であるIDカードを利用するため、その所有者のキャンパス内の滞在状況が明確であり、客観性が高く、加えてそのデータは既設のセキュリティゲート管理システムにより一元的に管理されている。これらの観点から、本提案により労働時間管理における適切な証跡デー

タの提供の試験的な運用が可能となり、試験運用を行うことによる問題の発見などを経て、より適切な労務管理体制の構築が期待でき、働き方改革の推進につながる。

本論文では、働き方改革に関連するガイドラインの即した環境の構築という観点から設計された、本提案におけるシステム構成・仕様を述べるとともに、生成されるデータに関する検証、今後の課題について論じる。

2 試作の動機付け

2019年4月から施行されている働き方改革関連の法案に先駆け、労働時間の適正な把握のために使用者が講ずべき措置に関するガイドライン [2] が2017年1月に策定された。ガイドラインでは、労働基準法の規定の観点から、使用者が労働時間を適切に管理する責務を有していることと、労働時間の把握に係る自己申告制の運用上問題が生じている状況があることが述べられている。特にガイドラインの4節では、自己申告制により始業・終業時刻の確認及び記録を行う場合に使用者が講ずべき措置について、以下のように記載されている。

自己申告により把握した労働時間が実際の労働時間と合致しているか否かについて、必要に応じて実態調査を実施し、所要の労働時間の補正をすること。

特に、入退場記録やパソコンの使用時間の記録など、事業場内にいた時間の分かるデータを有している場合に、労働者からの自己申告により把握した労働時間と当該データで分かった事業場内にいた時間との間に著しい乖離が生じているときには、実態調査を実施し、所要の労働時間の補正をすること。

このガイドラインで示されるとおり、自己申告による労働時間と、客観的証跡データとの間に著しい乖離の有無が確認できる環境が必要となる。また、そのためには、特定の就業者に対して対応する使用者、またはその確認を行う職務従事者が設定されることが必要となる。つまり、労働時間を自己申告する就業者と、実態との差の確認及び承認を行う立場の管理者の2階層の体制を実現する必要があると考えた。

本提案では、ガイドラインに即した環境実現の可能性を検証することを主な目的とした試作を行う。

3 セキュリティゲート

本提案では、キャンパス滞在時間の客観的証跡データが網羅的に必要と仮定する。つまり、個人が特定の区域に滞在した事実を客観的データとして蓄積する仕組み

が必要である。関連研究では、画像処理に基づいた入退室識別 [3] が提案されているが、こちらは不特定の人の往来を数的に管理するシステムであるため、特定の個人の入退勤を管理する意図とは異なり、本提案における証跡データとしては不適である。また、在室管理システム [4] が提案されているが、こちらは限定された区域における、特定の少人数の滞在状況を管理するシステムであるため、全学的な広範囲のデータを必要とする場合には適さない。

本提案では、個人を特定することができ、なおかつ全学を網羅しているデータが必要と仮定する。また、本提案で効率的に運用するためには、データが情報システムで適切に管理されていることが望ましい。

近年、さまざまな大学で、ICチップ付きのIDカードの導入 [5] が進んでいる。本学においても、2016年度からICチップ付きのIDカードとして職員証が導入され、それ以前から導入されていた学生証 (IC) と合わせて、全構成員がIDカードを保有するようになった。IDカードは個人に一意な身分証であり、入退館セキュリティゲートの認証用等にも利用されている。

個人に一意なIDカードを利用したセキュリティゲートの認証は、その所有者が認証が行われた時刻・場所に滞在したことの証明となるという点に着目した。つまり、セキュリティゲートの読取データを利用できれば、特定の区域に進入するためのセキュリティゲートの認証という日常的な行為から、キャンパス滞在の客観的な証跡データが得られる可能性があると考えた。

本提案では、職員証IDカードの一意性と、全学的に管理されている入退館セキュリティゲート管理システムの網羅性に着目し、そのIDカード認証データを、適当なフォーマットに再構成し、客観的証跡として提示するシステム (以下、本システム) を設計する。

4 システム設計

4.1 方針

本節では、本システムを設計するにあたって前提とする運用について述べる。また、既存システムであるセキュリティゲートの運用と本システムの設計の関係性について述べる。

本システムは、労務管理における労働時間管理において、就業者の労働時間の自己申告制が採用されている場合を主な想定としている。本システムでは、そのような環境において、労働時間の実態調査を行う必要性が生じた際に、客観的データを、証跡の一例として提供可能とすることを目指す。つまり、本システムにおいて提供されるデータで労働時間管理そのものを行うわけではない。また、本システムで提供される証跡提示環境は、

今後の本学の労働時間管理の運用プロセスの検証を主な目的とした試作である。そのため、全学を対象とすることを目的としているが、必ずしも今後の本学の労働時間管理プロセスに組み込むことを最終的な目的とはしていない。

4.2 セキュリティーゲートの運用

本学のセキュリティーゲートは、各棟入口など必要な場所に設置されているが、管理区域の外部にしかIDカードリーダーが設定されていないことが多い。つまり入室の際にはIDカードの読取で開錠するが、退室の際には読取を必要としない箇所が存在する。そのような箇所では、退室の際にもIDカード読取を行う、意識付けを考慮した運用が必要である。また、セキュリティーゲートのユーザデータの更新は半月に一度行われるが、別途権限を持つ各部局の管理者によって都度行われており、分散管理による柔軟な運用を取り入れている。本提案では、このような運用状況に即したシステム設計を行う。

また、セキュリティーゲートの読取データを証跡データとして利用するためには、前提となるセキュリティーゲートの運用ポリシーを考慮する必要があるが、本学では、統一されたセキュリティーゲートの運用ポリシーは存在せず、基本的に導入部局に一任しているのが現状である。そのため、本システムの設計は特定のセキュリティーゲート運用ポリシーを前提としていない。本システムの試作で得られた成果を含め、統一したセキュリティーゲート運用ポリシーを検討することは、本学の将来的な課題と捉える。

4.3 概要

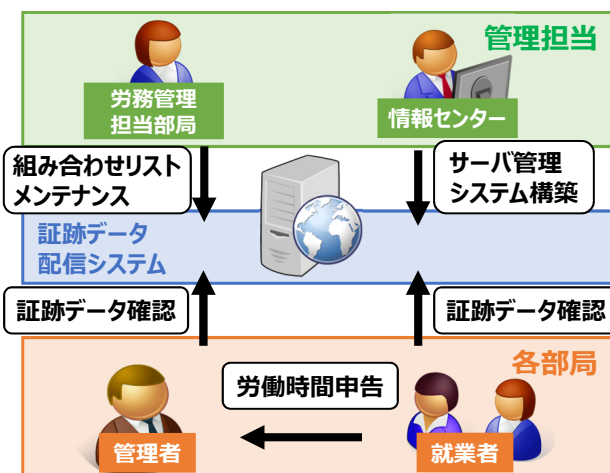


図- 1: 概要図

本提案の概要図を図-1に示す。本システムにおける証跡を提示するためのシステム構築と、システムを実装するサーバの管理を情報センターが担当し、運用上必要となる就業者と管理者の組み合わせリストのメンテナンスに関しては、労務管理の担当部局で月次の業務として行うことを前提とする。利用者側に関しては、各部局における管理者は、管理者自身が労働時間を管理する対象となる就業者の証跡データを参照できる。また、就業者は自身の証跡データを参照することができる。

4.4 システム構成

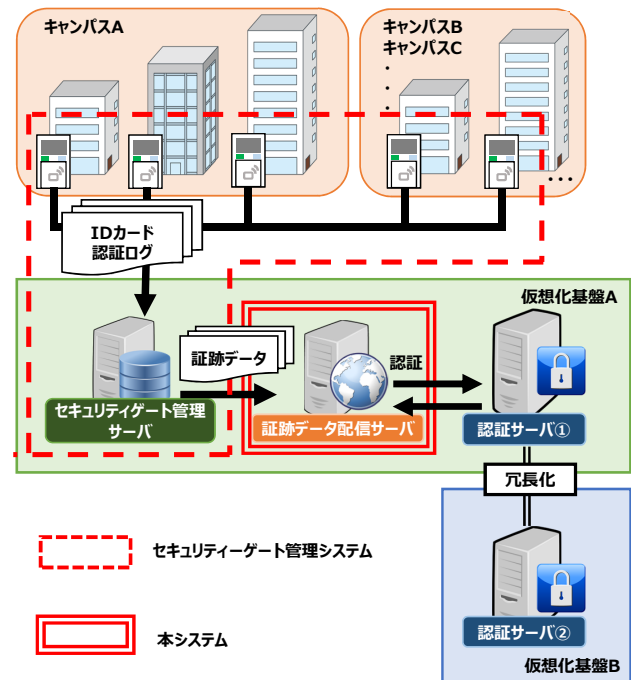


図- 2: システム構成図

本システムの構成図を図-2に示す。各棟の出入口や、建物内の管理区域の出入口にセキュリティーゲートが設けられていることを前提とし、セキュリティーゲート用IDカードリーダーの認証ログがセキュリティゲート管理サーバに集約され、認証されたアカウントに対し、氏名が補完され、読取データとしてCSV形式で保存されている。本システムでは、IDカードの読取データから最低限の情報のみを抽出し、セキュリティゲート管理サーバから定期的に取得する。ここで、後続の処理で再度氏名の補完処理を行う事を避けるため、合わせて氏名を抽出しておく。また、本システムは証跡データの提供のために学内限定公開のWebサーバとして構築されている。その提供にあたり、利用者に対してはWeb閲覧の際に認証を行っており、その方式として、Shibboleth[6]を採用した。本学ではShibbolethによる統合認証環境が構築済みであり、本システムの認証にShibbolethを利用す

る事で、SSO の認証・認可機構を組み込むことが簡易に実現できた。また、Shibboleth により提供される属性を利用することにより、閲覧の認可制御をスクリプトで自動的に機能するような展開も可能である。

4.5 システムフロー

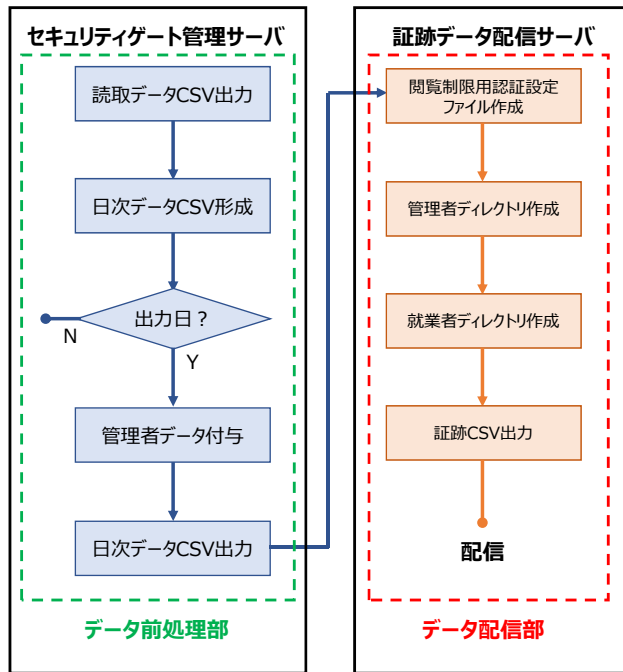


図- 3: システムフロー

本提案におけるシステムフローを図-3 に示す。本提案は、図-3 で示されるようにセキュリティゲート管理サーバ上で行うデータ前処理部と、証跡データ配信サーバで行うデータ配信部で構成される。

データ前処理部を担うセキュリティゲート管理サーバは、既存の独立したシステムであり、要求仕様変更や、システムのリプレースなどにより、今後運用状況が変化する可能性が考えられる。そのため、本提案ではデータの前処理とデータ配信部を別構成とし、データ前処理部に変更があった場合でも、データ配信部は入力された CSV に基づいて動作することができる設計とした。また、本学における就業者の多数は Excel の使用に支障はない。そこで、現行の労働時間申告の方法との親和性を考慮し、最終的な出力を CSV とする実装を行った。次節より、データの前処理とデータ配信部のそれぞれの処理の詳細について述べる。

4.5.1 データ前処理部

データの前処理部では、セキュリティゲート管理サーバに蓄積されている ID カードの読取データを使用する。

セキュリティゲート管理サーバにおける、ID カード読取データは、1 回の読取につき 1 レコードのデータとして出力される。さらにそのデータが棟ごと、日ごとに 1 つのファイルにまとめて出力される。図-4 に、ID カード読取データ CSV の一例を示す。

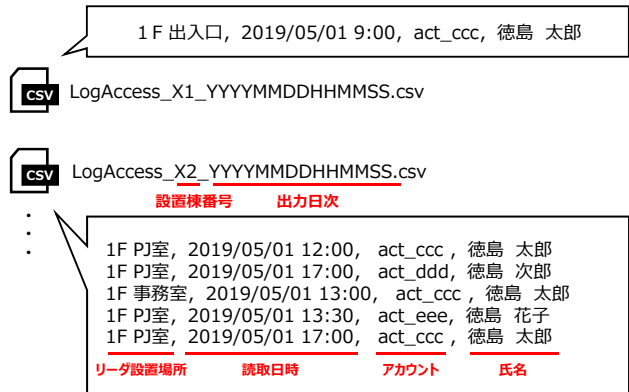



図- 4: 読取データ CSV

図-4 におけるアカウントとは、本学教職員における個人で一意であり、職員証から得られる。以降の処理において、個人の特定にはアカウントを用いる。

本提案では、前述した ID カード読取データを証跡データの元データとして使用する。これらのデータは、既存のシステムによって逐次出力されている。ID カード読取データは、1 回の読取につき 1 行出力されるため、1 日のうちに複数回読取を行った場合、複数行のデータが出力される。キャンパス内滞在時間の証跡として利用する為には、読取場所によらない、1 日の規定の範囲の中で最も早い時刻のデータと、最も遅い時刻のデータが必要となる。それらを効率的に取得するために、日ごとに全棟の読取データ 1 つの CSV ファイルにマージする。そしてその CSV ファイルから、就業者、日ごとに、最も早い時刻と、最も遅い時刻の読取日時をそれぞれ開始時刻、終了時刻として取得し、1 日分を 1 行のデータとして出力する。ここでの最初と最後の判定は、AM5:00:00 から翌日の AM4:59:59 の範囲で行う。そのため、この範囲での読取が 1 回しか行われなかった場合、終了時刻が欠損する。また、開始時刻、終了時刻が AM4:59:59 をまたぐ読取データがあった場合、同一日の読取データと解釈することはできない。つまり、AM4:59:59 以前にキャンパスへの滞在を開始した場合、本来の滞在日として認識する事ができない。こういった場合は、運用上の確認、及び承認のフローで別途個別に対応する必要がある。図-5 に、出力される日次データ CSV の一例を示す。

表- 1: 日次データ CSV・証跡 CSV 出力項目

項目名	形式	説明
manager	act.aaa	管理者のアカウント (ユニーク ID)
employee	act.bbb	就業者のアカウント (ユニーク ID)
name	漢字氏名	就業者の氏名
date	出勤日	AM5:00:00～翌日 AM4:59:59 間で滞在開始となる日付
week	漢字曜日	日付に対応する曜日
start	YYYY/MM/DD HH:MM:SS	出勤日範囲内で最初に職員証を読取器にかざした時刻
end	YYYY/MM/DD HH:MM:SS	出勤日範囲内で最後に職員証を読取器にかざした時刻
jikan	HH.99	start から end までの時間 (単位: 時)
chouka	HH.99	jikan が 8 時間を超えた場合, その超過した時間 (単位: 時)
department	所属コード	就業者の所属コード
section	セクションコード	就業者のセクションコード
sectionname	セクション名称	就業者のセクション名称
managername	管理者漢字氏名 (役職名)	管理者の氏名又は役職名

 daily-s.csv

```

XXXXXXXXX1, 徳島太郎, 2019/5/1, 2019/5/1 9:00, 2019/5/1 17:00 ...
XXXXXXXXX1, 徳島太郎, 2019/5/2, 2019/5/2 8:50, 2019/5/2 18:00 ...
XXXXXXXXX1, 徳島花子, 2019/5/1, 2019/5/1 13:30, 2019/5/1 21:00 ...
.

```

図- 5: 日次データ CSV

先に述べた処理で、ID カード読取データを日と就業者ごとに 1 行のデータとして形成した。次の処理として、2 節で述べたように、ガイドラインに即するためには、就業者に対して、対応する管理者の情報が必要であるため、形成したデータに管理者の情報を付与する。ここでは、管理者の情報を取得する為に、事前に作成した管理者管理用データベースを使用する。日次データに含まれるアカウントをキーに管理者管理用データベースから、必要属性を取得する。最終的に出力される項目の一覧を表-1 に示す。出力項目の氏名は、4.4 節で述べたように、ID カード読取データが生成される際に補完されたものをそのまま使用する。また、所属コード、セクションコード、セクション名称は、セキュリティゲート管理システムが構成員管理システムから連携された情報を利用している。これらは、既存のセキュリティゲート管理システムで実装されている仕組みを利用することにより、簡易な実装を実現した。加えて、管理者名称に関しては、セキュリティゲート管理システム固有の管理者情報を利用している。jikan, chouka は、start, end から自動計算して表示する。そのため、前節で述べたような、終了時刻が欠損している場合は、出力されない。そのような場合は、ユーザが自らデータを補完して、使用者に承認してもらう運用を想定している。jikan, chouka の項目は、ユーザがより容易に滞在時間の状況

を把握できることを目的とし、出力している。

4.5.2 データ前処理部の処理日

本システムでは毎月 1 日に前月最終日の処理を行い、16 日～月末日に前日の処理を行う。2 日～15 日に関しては、異動に伴う就業者の所属の変更や管理者の変更のための管理者管理用データベース更新用の作業日として設定されており、この期間は図-3 における、日次データ CSV の形成までの処理を行い、後続の管理者データ付与以降の処理は行わない。

4.5.3 データ配信部

データ前処理部で作成した CSV ファイルは、定時の処理として 1 日 1 回証跡データ配信サーバに送信される。この処理は、1 日の集計範囲を AM5:00:00 から翌日の AM4:59:59 としている関係で、AM5:00:00 以降に行わなくてはならない。CSV ファイルの送信には scp 等の暗号通信を用いる。セキュアな通信を行うため、予め用意した公開鍵と秘密鍵のペアによる認証を取り入れる。また、送信した CSV ファイルは、セキュリティゲート管理サーバ内でバックアップ用フォルダへと退避させる。

証跡データ配信サーバでは、送られてきた CSV ファイルを元に、データ配信部の処理として、配信用のディレクトリ構成と配信用 CSV の作成を行う。配信用のディレクトリ構成は、2 節で述べた理由から、管理者と就業者の 2 階層構造とした。まず、CSV から manager 列のデータを一意に抽出する。それらのデータに基づき、manager のアカウントをディレクトリの名称として上位ディレクトリを作成する。次に、CSV の employee 列の

データを抽出し、それぞれ対応する manager ディレクトリの下部に employee のアカウントを名称としてディレクトリを作成する。そのディレクトリ構成を、以下の図-6 に示す。

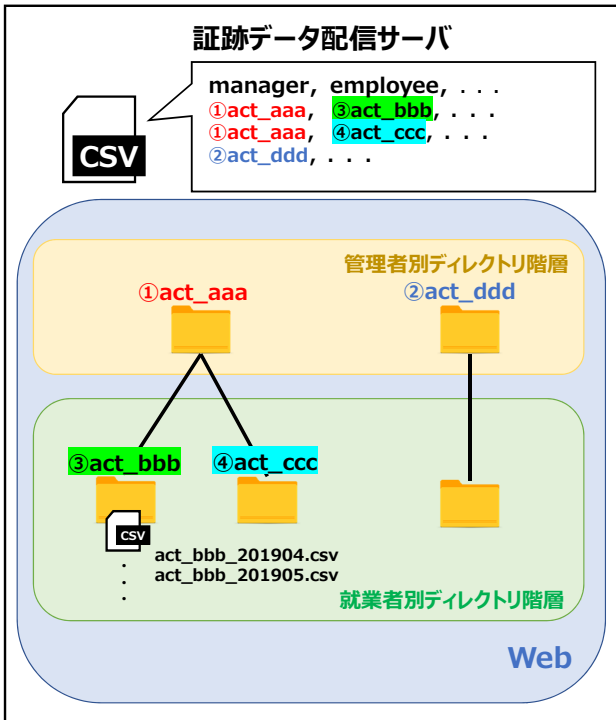


図- 6: ディレクトリ構成

作成した就業者のディレクトリに対し、その就業者に該当するデータ行をアカウントをキーに CSV ファイルから抽出し、提示用の CSV に保存する。この CSV は月ごとに 1 ファイルとしており、月初の処理の際にファイルを新規作成し、それ以外の日はファイル末尾に追記する。CSV を公開している Web ページの構成を以下の図-7 に示す。

Index of /idc/ [redacted] / [redacted]			
Name	Last modified	Size	Description
Parent Directory			
[redacted]_201902.csv	2019-03-01 06:36	2.8K	
[redacted]_201903.csv	2019-03-30 06:35	2.9K	
[redacted]_201904.csv	2019-04-27 06:35	2.8K	
[redacted]_201905.csv	2019-05-22 06:35	1.6K	

図- 7: CSV 公開ページ

また、作成した各ディレクトリには Shibboleth による認証と個人毎の認可を課すことにより、アクセス制限を行っている。管理者は自身のディレクトリの下層にある全ての就業者のディレクトリにアクセスできるが、就

業者は自身のディレクトリのみアクセスできる。これらの制限は、日次データ CSV を元に apache の認可設定ファイルを動的に生成することで実現している。この処理は、図 3 における閲覧制限用認証設定ファイル作成である。

4.6 異動時の想定

国立大学法人等では、定期的に就業者や管理者の異動が発生する。それが本システムに与える影響としては、就業者と管理者の対応関係の変化が挙げられる。前節で述べたように、本システムは管理者と就業者の 2 階層で構築されている。よって、管理者が異動するケースと、就業者が異動するケースが考えられる。どちらの場合も、本システムは特別な対応を要しない。異動が発生すると、管理者管理用データベースが更新され、それに基づきデータ配信部の処理を行う。表-2、図-8 に管理者が異動した場合のディレクトリ構成について示す。2019 年の 4 月に異動が発生し、act_bbb の管理者が、act_aaa から act_ccc に変更された。この場合、act_ccc のディレクトリの配下に新しく act_bbb のディレクトリが作成され、4 月以降のログはそちらに出力されていく。なお、異動前の act_aaa のディレクトリには 2019 年 3 月以前のデータがそのまま残る。

表- 2: 異動時の例

	管理者	就業者
異動前	act_aaa	act_bbb
異動後	act_ccc	act_bbb

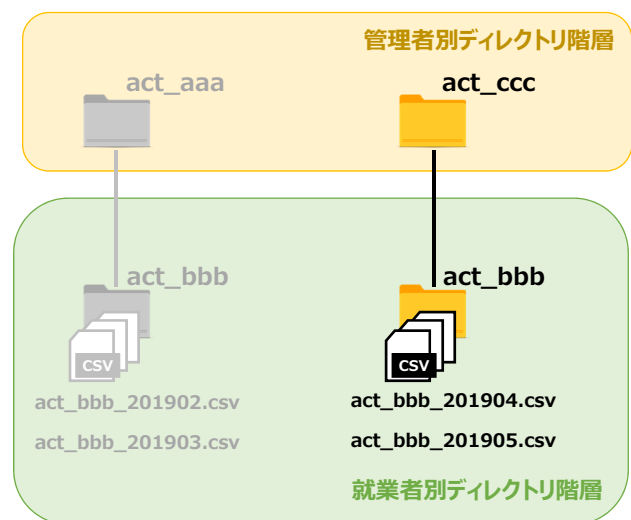


図- 8: 異動時のディレクトリ構成

4.7 検証

本節では、IDカードの読み取りデータを証跡データとして利用する上での正確性や、欠損の発生率などの検討のために行った検証について述べる。

4.7.1 検証条件

- 対象：徳島大学 情報センター 構成員 15名
(教員5名, 職員10名)
- 期間：2018年11月1日～2018年11月30日
- 場所：徳島大学 常三島キャンパス
情報センター棟 執務室 A, B

上記の条件で検証を行った。対象場所となる情報センター棟 執務室 A, B は常時施錠されており、それぞれ入口にIDカードリーダーが設置されている。検証では、それら2台のカードリーダーの読取データを使用した。各員はIDカードリーダーにIDカードを読み取らせ開錠し、入室する。退室時は、開錠にIDカードの読み取りを必要としない。

本検証では、対象の各員に、検証期間は出勤時と退勤時に必ずIDカードを読み取らせることを促した。これは、執務室に2人以上が同時に入室する場合、後続の人員がIDカードの読み取りを行わない可能性が高いこと、退室時にIDカードの読み取りを必要としないため、退勤時には意識的に行わなければ読み取りデータが蓄積できない可能性が高いことを考慮したためである。

4.7.2 検証結果

表-3: 検証結果

のべ出勤日数	データ件数	要確認データ件数
310	310 (100%)	20 (6.4%)

表-3に、検証結果を示す。のべ出勤日数とは、検証の対象となる各員の出勤日数の合計である。データ件数とは、表-1における start, end がどちらも欠損していないデータの件数である。また、要確認データ件数とは、データのうち、end が各員の退勤の基準とする時刻以前かつその時刻と一定の乖離があり、使用者による確認を必要とすると考えられるデータの件数である。

4.7.3 考察

前節の結果から、データ件数は、のべ出勤日数と一致した。ここから、少なくとも1回の読み取りを行った日は、必ず2回以上の読み取りを行っていることが分かる。よって、セキュリティゲートのIDカード読取データは、ある特定日にキャンパスに滞在したこと自体の証跡として利用できる可能性が高いと考えられる。次に、6.4%が要確認データとして検出された。これらは、本来滞在しているべき時刻の滞在が確認できないデータであり、キャンパス滞在時間の証跡として利用するためには使用者の確認が必要と考えられる。これらに関しては、以下のような原因が確認できた。

1. 退勤時の読み取り忘れ
2. 執務室以外での業務を行い、直帰した
3. 出勤したが、勤務時間内に出張に出発した
4. 早退

1に関しては、注意喚起で発生件数を減少させられる。しかし、実際の運用では、執務室の入退室に必ずしもIDカードの読み取りを必要としない場合が考えられる。例えば、特定の時間は開錠されており、それ以外の時間は施錠されているような運用をしているセキュリティゲートの場合、要確認データの発生件数は増加することが予想される。2～4に関しては、本システムを運用する上で何らかの対策を行うことは難しいと考えられる。2に関しては、セキュリティゲート管理システムの仕様上、主に滞在する執務室以外のカードリーダーで読み取ったデータを使用することができるため、滞在した棟、部屋のセキュリティゲートにIDカードを読み取らせる運用を行えば、ある程度対応可能と考えられる。

4.8 今後の課題

本提案は、本学における労務管理プロセスに直接的に組み込む事が目的ではないが、今後の展望によっては、本格的な稼働も想定できる。その場合、いくつかの課題がある。その課題について、以下に述べる。

(1) IDカード読取以外の証跡データへの対応

本提案は、セキュリティゲートのIDカードリーダーの読取データを利用することにより、証跡データを提示している。そのため、IDカードを利用しない棟への滞在に関しては検知できない。また、一部の棟に関しては、IDカードリーダーは設置されているが、部局独自の運用を行っており、セキュリティゲート管理サーバにデータが蓄積されない。これらのようなケースは、キャンパス内滞在の証跡を

本システムから確認することはできない。よって、何らかの方法で証跡データを、本システムに蓄積するデータのフォーマットに加工し、マージする必要がある。

(2) 就業者から管理者への訂正フローの整備

本提案は、就業者の自己申告による労働時間と証跡データの間に着しい乖離があった場合に、実態調査の支援を行う事を想定している。しかし、本提案においてフォローできるのは、管理者による就業者の証跡データの確認と、管理者から異議があった場合に、就業者が自身の証跡データを確認することまでである。労務管理の観点からは、そのような場合に、就業者から管理者への実態の報告とその承認が必要となる。本提案では、そのフローについて実装できておらず、運用でカバーする必要があるため、その部分は本システムで完結しない。

(3) 管理者管理用データベース更新の自動化

1節で述べたとおり、本提案における管理者と就業者の対応関係は、月次の処理として労務管理の担当部局が確認し、更新データがあった場合、情報センターが管理者管理用データベースを更新する。この作業の猶予期間として、4.5.1節で述べたように、毎月2日～15日はデータの生成を行わないため、この期間は証跡データの提示にラグが発生する。

(4) 人事給与システムとの連携

本学では、労働時間の最終的な管理を人事給与システムで行っており、労務管理全体から考えると、本システムは補助的な位置づけとなる。現状、本システムは、各利用者が運用レベルで利用できると考えるが、本システムと人事給与システムは連携していない。システムの系をサイロ型とせず統合連携を考慮すると、データ配信サーバの担う機能を、人事給与システムが担う方針とする方が、整理は容易と考える。ただし、有償機能であることが想定されるため、全体最適化とコストのトレードオフのバランス次第であると考えられる。

(5) 要確認データへの対応

4.7.2節で述べたように、証跡データの収集において、使用者による確認を要するとされるデータが発生している。このようなデータの発生件数を減少させるためには、本提案を組み込んだ勤怠管理の総合的な運用プロセスを定め、それに則った運用を推進する必要がある。また、本システムでフォローできない要確認データに関しては、別途、追加センサや機能を導入・統合といった対応も想定される。

5 おわりに

本論文では、働き方改革に関して、厚生労働省が策定したガイドラインに則った環境の構築について述べた。セキュリティゲートのIDカード読取データを利用することにより、特別な作業を必要とせず日常的な行為から、滞在の証跡データを取得することが実現できた。本学のキャンパス滞在時間管理に対して、運用でのフォローは必要であるが、欠損率が低い証跡データの生成を実現した。これにより、策定されたガイドラインにおける、自己申告と客観的証跡データの間で発生した乖離の状況の確認ができる環境という水準を満たした機能性を実現しており、管理プロセスの適正化に関して、一定の貢献が可能と考える。しかし、本格的に運用するためには、いくつかの課題がある。これらの課題は、システム的な課題でもあるが、そもそもの運用プロセスにも関わる課題でもあり、コストも含めた総合的な観点から検討していきたい。

謝辞

本システムの試作にあたり、徳島大学総務部人事課の皆様と徳島大学情報センタースタッフ江崎真一氏には多大なご助言、ご助力を頂きました。深く感謝申し上げます。

参考文献

- [1] 西田義人, 田中成典, 古田均, 馬石直登, 北川洋平, 打尾 賢一 動画像による個人識別技術を用いた勤怠管理に関する研究, 映像情報メディア学会誌: 映像情報メディア 63(11), pp.1611-1621, 2009.
- [2] 厚生労働省—労働時間の適正な把握のために使用者が講ずべき措置に関するガイドライン <https://www.mhlw.go.jp/file/06-Seisakujouhou-11200000-Roudoukijunkyouku/0000149439.pdf>, 2017.
- [3] 良永早耶佳, 大坪敦, 橋本大和, 廣重法道, 鶴田直之, プライバシーを考慮した安価でポータブルな入退室者カウント画像処理システムの開発, 第80回全国大会講演論文集, pp.523-524, 2018,
- [4] 田中優斗, 福島拓, 吉野孝, 入退室時に利用者がとるポーズを用いた在室管理システムの提案, GN Workshop 2014 論文集, pp.1-6, 2014.
- [5] 清水さや子, 戸田勝善, 吉田次郎, 横田賢史, 東京海洋大学における第3期ICカード学生証導入と運用評価, 学術情報処理研究, No.20, pp.90-96, 2016.
- [6] Shibboleth, <https://www.shibboleth.net/>