

# スマート化する職場と労働者のプライバシー

竹地 潔  
(富山大学教授)

現在わが国では、「スマート革命」が進行中であり、「いつでも、どこでも、何でも、誰でも」ネットワークに簡単につながるができるユビキタスネットワーク環境が実現する一方、ネットワーク上に爆発的に増大する多種多様なデジタル情報を収集・蓄積し、その分析・利活用を行うことを通じて、異変の察知や近未来の予測等が可能・容易になりつつある。このような情報通信技術（ICT）の新たな革新の波は、労働の現場にも押し寄せている。企業は、電子タグやGPS、生体認証技術等々、新たなICTを導入し、それらを通じて取得した多種多様なデータを人事労務管理の効率化のためにも利活用し始めている。その反面、新たなICTは、労働者の位置情報を正確かつ継続的にリアルタイムで取得するとともに、その蓄積を通じて労働者の行動履歴を獲得し、それとその他の個人情報と紐付けることにより労働者の人物像を明らかにすることを可能にする。このことは、労働者のプライバシーや人格にとって重大な脅威である。本論は、電子タグやGPSに基づく労働者の監視および生体認証の利用に関して、労働者のプライバシーへのそれらの影響等を踏まえたうえで、それらをめぐる法的問題に対して、現行法がどのように対応するのか、対応しうるのかについて検討し論ずる。

## 目次

- I 問題の所在
- II RFIDやGPSに基づく労働者の監視
- III RFIDやGPSに基づく監視とその脅威にさらされる労働者
- IV RFIDやGPSに基づく労働者の監視への法的対応
- V 労働者のプライバシーへのさらなる脅威——生体認証

## I 問題の所在

現在わが国では、ユビキタスネットワーク環境の完成とビッグデータに代表されるスマート化の始動により、「スマート革命」が進行中である<sup>1)</sup>。つまり、「いつでも、どこでも、何でも、誰でも」ネットワークに簡単につながるができるネットワーク環境が実現する一方、ネットワーク上に

爆発的に増大する多種多様なデジタル情報を収集・蓄積し、その分析・利活用を行うことを通じて、異変の察知や近未来の予測等が可能・容易になりつつある。このようなビッグデータの分析・利活用が製品開発、販売促進、保守メンテナンス・サポート、コンプライアンス等、事業活動の効率的な実施に役立てられることが大いに期待されている。

もちろん、このような情報通信技術（ICT）の新たな革新の波は、労働の現場にも押し寄せている。企業は、電子タグやGPS、生体認証技術等々、新たなICTを導入し、それらを通じて取得した多種多様なデータを人事労務管理の効率化のためにも利活用し始めている。その反面、新たなICTは、労働者の位置情報を正確かつ継続的にリアルタイムで取得するとともに、その蓄積を通じて労働者の行動履歴を獲得し、それとその他の個人情報

報と紐付けることにより労働者の人物像を明らかにすることを可能にする。つまり、これらの技術を用いれば、使用者は労働者の一挙手一投足を監視するとともに、労働者を丸裸にすることもできる。このことは、まさに労働者のプライバシーや人格にとって重大な脅威である。

本論は、電子タグやGPSに基づく労働者の監視を中心に、労働者のプライバシーや人格へのその影響等を踏まえたうえで、それをめぐる法的問題に対して、現行法がどのように対応するのか、対応しうるのかについて検討し論ずる<sup>2)</sup>。また、生体認証についても論ずるが、その問題性と法的対応の方向性のみを示すにとどまる。

## II RFID や GPS に基づく労働者の監視

電子タグ (Radio Frequency Identification—以下、RFID という) とは、IC チップと小型アンテナで構成された一種の記憶媒体で、それに記憶された人やモノの個別情報を電波によって非接触で読み書きすることができる自動認識技術である。それは、ユビキタスネットワーク環境を支える重要な技術であり、さまざまな用途、たとえば、在庫管理、棚卸、生産管理、物流管理、トレーサビリティ、入退出管理などで利活用され、事業の効率化とコストの削減に役立っている<sup>3)</sup>。

人事労務管理の分野において最も普及している利用方法は、RFID 内蔵の社員証による入退室管理や PC ログイン認証である。それは勤怠管理にも用いられ、それから得られたデータに基づき給与計算処理が自動的に行われる。このように、RFID を用いれば、事業場内において、いつ、誰が、どこにいるか (または、何をしているか) が使用者にとって一目瞭然となり、その技術は人事労務管理の効率化とコストの削減に大いに役立つ。さらに、RFID は、(ビデオカメラと連携して) 個々の労働者の作業履歴を記録し、その分析を通じて業務プロセスの改善を行うことも可能にし、現場作業の「見える化」の実現に寄与する、と考えられている。

他方、GPS とは、Global Positioning System (全世界測位システム) の略称であり、人工衛星、コ

ンピュータ、受信機から成り、異なる人工衛星から送られた信号が地上の受信機にそれぞれ到達する時刻の差を計算することによって、地球上の受信機の現在位置 (緯度と経度) を測定するシステムである。それもユビキタスネットワーク環境を支える技術であり、周知のとおり、自動車の走行時に現在位置や目的地への経路案内を行う「カーナビ」を始め、地図検索やナビゲーションなどさまざまな用途で利活用されている<sup>4)</sup>。

従来から、GPS は社用車の運行管理のため用いられてきた。近年、スマートフォンの急速な普及に伴って、人員の適正配置や業務の効率化などを目的に、外回りの多い労働者に対し GPS 機能付き携帯電話・端末を貸与し、電気通信事業者を通じて労働者の位置情報を取得し、その他の情報と紐付けて労働者の行動把握を行う企業が増加している。従来ならば使用者の監視の目が届かなかった事業場外の労働者の行動についても、GPS を利用することにより、使用者は把握することが可能となった。

## III RFID や GPS に基づく監視とその脅威にさらされる労働者

前述の RFID や GPS の技術を利用して、使用者は、事業場内外の労働者の現在位置を知ることができるようになった。この両技術を用いた位置情報の取得はその他の方法・手段を用いた場合と比べて顕著な特徴がある。つまり、対象者 (物) の現在位置を「正確」かつ「継続的」に「リアルタイム」で特定・把握できるという特徴である。そうであるがゆえに、使用者は常に労働者の位置情報を取得して、彼らの行動をリアルタイムで把握することができるとともに、位置情報の蓄積を通じて彼らの行動履歴をも獲得できる。

このような RFID や GPS に基づく位置情報の取得・利用について、労働者の権利利益等に対するその影響の観点から、さまざまな懸念がある。

RFID や GPS を通じて取得される労働者の位置情報は個人を識別可能な「個人情報」であり、個人情報保護法上の保護対象である。その取得・利用に際して、使用者が個人情報保護法およびそ

れに基づく諸ガイドライン上の諸義務・諸措置を履行しないと、同法違反に問われうる。たとえば、本来の目的である制服管理のみならず、労働者本人に気づかれることなく彼らを監視するため、制服に縫い付けたRFIDを利用するとか、社員証の代わりに、RFIDの体内への埋め込みを労働者に強要するとか<sup>5)</sup>、または、労働者に貸与し携帯させているGPS機能付き携帯電話・端末等の位置情報を本人に無断で電気通信事業者から取得するといったことは、個人情報保護法違反にあたり、プライバシーの侵害にも問われうる。また、携帯電話・端末等の位置情報を、その利用者である労働者本人に無断で取得することは、憲法上の「通信の秘密」を侵すことにもなる<sup>6)</sup>。

RFIDやGPSに基づく監視は、それを通じて取得する情報に基づき、作業工程の効率化や作業速度の加速化を極限まで進めることを可能にする。その結果、労働者は、職務遂行をコントロールできる、残されたわずかな裁量(仕事のやり方に対する自律)さえも奪われ、自らを行為者としての人間というよりも、高度に管理化された生産組織の単なる一歯車と感ずるようになる<sup>7)</sup>。それゆえに、RFIDやGPSに基づく監視は従来の監視方法・手段よりも、労働者としての自律や人間の尊厳にとって潜在的に重大な脅威である。

労働者による業務用の携帯電話・端末等の携行は通常、勤務時間内にとどまらず勤務時間外にも及ぶことが多い。そのため、労働義務を負わない(労務指揮権の及ばない)私的領域における労働者の行動についても、使用者がそのGPS機能を用いて監視ないし追跡することができる。実際にそうすれば、四六時中、労働者は使用者の監視下に置かれることになる。このことはまさに、労働者のプライバシーへの重大な脅威である。

前述したように、RFIDやGPSを用いて取得した位置情報を蓄積すれば、労働者の行動履歴を把握することができる。そしてそれに基づき、交遊関係、性的志向、身体的・精神的健康状態、政治的・宗教的所属、金銭や家族に関する家庭内の問題といった「センシティブでかつ極めて私的な事柄」さえも明らかにしうる<sup>8)</sup>。さらに今後は、「ライフログ」の活用によるプロフィール分析、

つまり位置情報を含め「蓄積された個人の生活の履歴」に関する情報を大量に収集、記録、保存し、コンピュータを通じて行動科学的に分析することによって、意識的な行動のみならず無意識的な行動についても、個人特有の傾向やパターンが解明され、各個人の人物像が浮き彫りにされうる<sup>9)</sup>。そして、その分析結果が個別の労働者の人事労務管理等に利用されることになろう<sup>10)</sup>。

RFIDやGPSを用いた位置情報の取得・利用が、ただ対象者の足取りを視覚的に追跡するのにとどまるのであれば、従来の単純な監視の延長線上にあるものとして位置づけられる。しかし、前述の「ライフログ」の利用によるプロフィール分析は、個人の心の中、つまり、無意識的領域まで見透そうとするものであるため、監視を受けているとの意識に基づく自覚的行動によって、監視者を欺くことができる従来の単純な監視とは質的に大きな差異がある<sup>11)</sup>。したがって、使用者が、RFIDやGPSその他の監視方法・手段を通じて取得した労働者の「ライフログ」を利用して、彼らのプロフィール分析を行い、その分析結果を人事労務管理に利用することになれば、プライバシーの侵害という問題にとどまらず、労働者の「人格」ないし人格権にかかわる問題が生じることになろう<sup>12)</sup>。

なお、使用者から貸与されるGPS機能付き携帯電話・端末等は通常、業務連絡のためのツールでもある。勤務時間内のみならず勤務時間外にもそれを携行するよう求められると、労働者は、四六時中使用者の監視下に置かれることになる。同時に、管理監督者などから携帯電話・端末等を通じて随時業務について指示ないし指図されたり、場合によっては叱責されたりすることもある。使用者によるこのような四六時中の監視およびそれに基づくリアルタイムの指示や指図等は、労働者に対し著しい精神的圧迫を加え<sup>13)</sup>、労使間に精神的支配・服従関係を形成し、労働者個人の自由な意思に基づく行動を大幅に制限することになろう。このような労働者の「奴隷」的な拘束状態(ジオスレイバリー (geoslavery))<sup>14)</sup>から労働者を解き放つことも重大な課題である。

## IV RFID や GPS に基づく労働者の監視への法的対応

### 1 序

前述したように、RFID や GPS に基づく労働者の位置情報の取得・利用によって、労働者のさまざまな権利利益、つまり、プライバシー権、人格権、通信の秘密などが侵害されるのみならず、労働者の人格それ自体が重大な脅威にさらされるおそれがある。このような状況に対して、わが国の現行法は、個人情報保護法による事前の規制と、プライバシーの侵害等への事後の法的救済をもって、対応することになる。

### 2 個人情報保護法による法的規制

#### (1) 位置情報の取扱いと個人情報保護法

個人情報保護法（正式名称——「個人情報の保護に関する法律」）は、個人情報の有用性に配慮しつつ、個人の権利利益の保護を目的に、民間部門における個人情報の適正な取扱いに関する一般的なルールとして、「個人情報取扱事業者」に対し「個人情報」「個人データ」および「保有個人データ」の取扱いについて遵守すべき法律上の各種の義務を課している。

個人の位置情報の取得および利用が個人情報保護法の適用を受けるかどうかについては、まず、当該位置情報が個人情報保護法2条1項の定める「個人情報」に該当するかどうかが問題となる。「個人情報」とは、「生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができるもの、それにより個人を識別することができるものを含む。）」と定められている。個人の位置情報が「個人情報」に該当するかどうかは、同法の定める生存性と個人識別性の要件を満たすかどうかによって左右される。RFID や GPS を通じて使用者が取得する労働者の位置情報については、通常、二つの要件を満たし、「個人情報」に該当するといえよう。なお、当該位置情報が、容易に検索できるコンピュータを用いたデータ

ベース等で体系的に整理されていると、「個人データ」に含まれ、そのうち、個人情報取扱事業者が開示、訂正、利用停止等を行う権限のあるものは、「保有個人データ」に含まれる。

したがって、RFID や GPS を通じて労働者の位置情報を取得し利用しようとする使用者は、特定の個人情報を容易に検索できるコンピュータを用いたデータベース等を事業の用に供し、かつ当該データベース等に5000人分以上の個人情報を保有しているならば、「個人情報取扱事業者」として、労働者の位置情報の取得および利用に際して、その他の個人情報と同様に、個人情報保護法の定める次のような遵守すべき諸義務を負うことになる<sup>15)</sup>。まず、位置情報の取扱いに際して、利用目的の特定、利用目的による制限、適正な取得、利用目的の通知等を行う義務がある（15条～18条）。また、その位置情報が「個人データ」として存するときは、データ内容の正確性の確保、安全管理措置、従業者の監督、委託先の監督、第三者提供の制限をなす義務がある（19条～23条）。さらに、それが「保有データ」として存するときは、保有個人データに関する事項の公表等、開示、訂正等、利用停止等の義務がある（24条～27条）。

#### (2) 個人情報保護法と雇用管理分野のガイドライン

前述したように、個人情報保護法では、個人情報の適正な取扱いに関する一般的なルールとして民間事業者の遵守すべき法律上の義務が定められている。それとともに、同義務の履行のため、民間事業者が講ずべき具体的な措置等について、事業等の分野の特性を勘案した各種の指針が策定されている。RFID や GPS に基づく労働者の位置情報の取得・利用に関して、まず、問題となる指針は、「雇用管理分野における個人情報保護に関するガイドライン」（平成24年5月14日厚生労働省<sup>16)</sup>）である。それは、事業者が雇用管理に関する個人情報の適正な取扱いの確保に関して行う活動を支援するため、当該活動の実情や特性等を踏まえ、事業者が講ずべき措置について定めた指針である。それは、雇用管理に関する個人情報一般の取扱いに関するルールを定めるものであり、労働者の「位置情報」の取扱いに言及し、それ到的

を絞った特別なルールを定めてはいない。

しかし、雇用管理に関する個人情報の取扱いに関しては、前述のガイドラインに加えて、その他のガイドラインが定める、事業者の講ずべき措置にも留意する必要がある。RFIDやGPSに基づく労働者の位置情報の取得・利用については、「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」（平成26年12月12日厚生労働省・経済産業省）が問題となる。同ガイドラインでは、個人情報保護法20条の安全管理措置の一環として、ビデオおよびオンラインによる従業員のモニタリングを実施するに際しての、次のような留意点が示されている。つまり、①モニタリングの目的、すなわち取得する個人情報の利用目的をあらかじめ特定し、社内規程に定めるとともに、従業員に明示すること、②モニタリングの実施に関する責任者とその権限を定めること、③モニタリングを実施する場合には、あらかじめモニタリングの実施について定めた社内規程案を策定するものとし、事前に社内に徹底すること、④モニタリングの実施状況については、適正に行われているか監査または確認を行うこと、である。当該社内規程の策定にあたっては、あらかじめ労働組合等に通知し、必要に応じて協議を行うこと、また、その策定後、労働者等に周知することが望ましい、とされている。

使用者が顧客などの個人データの安全管理等のためRFIDやGPSを用いて労働者の位置情報を取得し利用することは、同ガイドラインの「従業員のモニタリング」と同一視することができよう。したがって、このようにして使用者が労働者の位置情報を取得し利用しようとする場合には、同ガイドラインの示す、労働者の個人情報の適正な取扱いに関する前述の諸事項に留意しなければならない。

なお、個人情報保護法制定・施行前に公表され、法的拘束力はないが、グローバル・スタンダードにより十二分にかなう「労働者の個人情報保護に関する行動指針」（平成12年12月20日）によれば、モニタリングを行う場合、原則として労働者に対し、実施理由、実施時間帯および収集される情報内容等を事前に通知するとともに、労働者の権利

利益を侵害しないよう配慮すること、とりわけ継続的なモニタリングは労働者の健康と安全の確保、または業務上の財産の保全に必要な場合に限定すること、が求められている。また、RFIDに基づく労働者の位置情報の取得等については、消費者保護のための指針ではあるが、「電子タグに関するプライバシー保護ガイドライン」（平成16年6月8日総務省・経済産業省）の示す諸ルールも考慮する必要がある。

### （3）電気通信分野のガイドライン

次に、GPS機能付き携帯電話・端末を用いた労働者の位置情報の取得・利用との関係において、問題となるのは、「電気通信事業者における個人情報保護に関するガイドライン」（平成25年9月9日総務省）である。

同ガイドラインは、電気通信サービスの利便性の向上を図るとともに、利用者の権利利益を保護することを目的に、「通信の秘密」および個人情報の適正な取扱いについて、電気通信事業者の遵守すべき基本的事項が定められている。その中で、「通信の秘密」の要請から、「位置情報」の取扱いに関する特別な規定が置かれている。つまり、同ガイドライン26条1項において、「電気通信事業者は、利用者の同意がある場合、裁判官の発付した令状に従う場合その他の違法性阻却事由がある場合を除いては、位置情報（移動体端末を所持する者の位置を示す情報であって、発信者情報でないものをいう。以下同じ。）を他人に提供しないものとする」と定め、原則として利用者本人の同意を得ずに他人に提供することが禁止されている。また、同条2項において、「電気通信事業者が、位置情報を加入者又はその指示する者に通知するサービスを提供し、又は第三者に提供させる場合には、利用者の権利が不当に侵害されることを防止するため必要な措置を講ずるものとする」と定め、利用者以外への提供に際しての権利侵害の防止措置を求めている。同ガイドラインの解説<sup>17)</sup>によると、その具体的内容として、①利用者の意思に基づいて位置情報の提供を行うこと<sup>18)</sup>、②位置情報の提供について利用者の認識・予見可能性を確保すること<sup>19)</sup>、③位置情報について適切な取扱いを行うこと<sup>20)</sup>、④第三者と提携の上サー

ビスを提供する場合は、提携に関する契約に係る約款等の記載により利用者のプライバシー保護に配慮することなど、が挙げられている。

実際に、電気通信事業者は、前述のガイドラインに従って、労働者の位置情報の提供サービスに関する約款で、加入者（契約者）である使用者に対し、利用者である労働者の「同意」を取得することを義務づけている。また、機能面においても、勤務時間外のプライバシー保護を配慮して、携帯電話の利用者側で位置情報取得の可否を制御できる「位置送信拒否設定」などを設けている<sup>21)</sup>。

したがって、電気通信事業者の位置情報提供サービスを利用して、業務用のGPS機能付き携帯電話等から発せられる労働者の位置情報を取得しようとするためには、使用者はまず、それを携行している労働者から、位置情報の提供について「同意」を得なければならない。とはいえ、対使用者との関係において取引力・交渉力で劣位にいる個々の労働者の実態を前提にすると、労働者から単に「同意」を得ればよいというものではなく、その「同意」のあり方が問われ、労働者の自由な意思に基づく同意の取得が求められる。

### 3 プライバシー権または人格権への侵害を理由とする法的救済

#### (1) 労働者の観察・監視によって生じうる使用者の法的責任

使用者は、人事労務管理、製品・サービスの品質管理および財産保全などのため、労働者の職務遂行状態を観察したり、監視したりする必要がある。通常、このような労働者の言動に対する観察および監視は、使用者による労務指揮権および施設管理権の行使の一環として行われ、適法なものである。しかし、観察や監視の目的、対象、方法や手段、または、程度によっては、労働者のプライバシー権または人格権への侵害が発生しうる。そのような場合には、使用者は、不法行為に基づく損害賠償責任を問われたり、また、労働契約上の付随義務としての、労働者のプライバシー権や人格権を尊重（保護）する義務に違反するとして、債務不履行に基づく損害賠償責任を問われる<sup>22)</sup>。さらに、場合によっては、人格権に基づ

く差止請求が認められる余地がある。

以下、RFIDやGPSに基づく労働者の位置情報の取得および利用の適法性をめぐる問題について、勤務時間中の場合と勤務時間外の場合に分けて検討する。

#### (2) 勤務時間中における労働者の位置情報の取得・利用

前述したように、個人情報保護法およびその各種のガイドラインにより、勤務時間中であれば、RFIDやGPSを用いて労働者の位置情報を取得し利用するためには、そのことに関する社内規程を策定するとともに、労働者本人に対し、取得・利用の目的、仕組み、取得される情報の種類等について従前に周知徹底することが求められている。さらに、業務用のGPS携帯電話等を通じた位置情報の取得や利用については、労働者から明確な同意を得なければならない。

このような個人情報保護法上の義務および関連ガイドラインの要請する措置に違反した場合、私法上の効力が生じるかどうかは問題となるが、同法からは、直ちにそのような法的効力が生じることはない。とはいえ、同法上の義務の違反等により労働者の権利利益が侵害され、労働者とその損害の賠償を請求するといった場合、少なくとも法の解釈・適用において、使用者が同法の定める諸義務を履行したかどうか、または（および）関連ガイドラインの要請する諸措置を講じたかどうか、その損害賠償請求の前提となる不法行為法上の注意義務違反等を判断するのにあたって考慮されるべき重要な要素であることはいうまでもない<sup>23)</sup>。

また、個人情報保護法上の諸義務および関連ガイドラインの要請する諸措置がそのまま、労働契約上の付随義務としてのプライバシー権・人格権尊重義務または個人情報保護義務の具体的な内容となるかどうかは問題となりうる。このことについても、同法および関連ガイドラインの法的性質を考慮すると、否定的にならざるをえない。もちろん、同法上の諸義務および関連ガイドラインの諸措置は、労働者の個人情報の取扱いの各場面ごとで問題となる使用者のプライバシー権・人格権尊重義務または個人情報保護義務の具体的な内容

を確定するに際して参考にされるよりどころの1つとはなりえよう<sup>24)</sup>。

RFID や GPS に基づく勤務時間中の労働者の位置情報の取得・利用に関する適法性は、労働者の職務遂行の観察や監視をめぐるこれまでの諸裁判例と同様に、その具体的目的、態様・程度、当該目的を達するのにより侵害的ではない他に採りうる方法の存否、および、その実施にあたっての事前の説明・協議の有無など諸般の事情を考慮して判断されることになろう<sup>25)</sup>。その判断に際しては、前述した個人情報保護法上の諸義務および関連ガイドラインの諸措置を履践したかどうか、履践したとしてもどの程度であったかが重要なポイントとなろう。

したがって、勤務時間中であっても、使用者が、労働者本人に無断で極秘裏に位置情報を取得する場合や、位置情報の取得自体を労働者本人に知らせたとしても、労働組合等への事前の説明や協議をなさず、または、その目的や方法などについて労働者本人に十分な説明を行わずに、位置情報を取得する場合などは、プライバシー権または人格権への侵害にあたり、違法とされよう。とりわけ、GPS 機能付き携帯電話・端末等を通じて、位置情報の取得を行おうとする場合は、少なくとも、労働者本人への十分な情報提供・説明を行ったうえで、書面等で明確な同意を得なければ、適法とされないであろう。

実際に、ナビシステムによる居場所確認 (GPS 等を通じた位置情報の取得・利用) の適法性が争われた東起業事件 (東京地裁平 24・5・31 労判 1056 号 19 頁) において、その導入の目的は、外回りの多い従業員の勤務状況を把握し、緊急連絡や事故等の対応のため居場所を確認することであり、原告以外複数の従業員にも使用されていることから、相応の合理性があると認めたとうえで、「原告が労務提供が義務付けられる勤務時間及びその前後の時間帯において、被告が本件ナビシステムを使用して原告の勤務状況を確認することが違法である」とはいえない、とした。この判断に際して裁判所は、ナビシステムへの携帯電話の接続に原告が当初抵抗していたが、上司からの強い指示を受けて、結局それに同意した、と認定していたこ

とも留意する必要がある。したがって、本判決は、勤務時間中およびその前後における労働者の位置情報の取得が適法とされるには、少なくとも、その目的の合理性と労働者の「同意」が必要であると考えている、といえよう。ただし、同裁判所による「同意」の捉え方については、賛否が生じるであろうが。

### (3) 勤務時間外における労働者の位置情報の取得・利用

勤務時間を終えて事業場外にいる労働者は、労働義務から解放され、本人の思うまま自由に私的な活動を行うことができる。他方、使用者は、このような私的領域にいる労働者に対し、労務指揮権等を根拠に、彼らの言動の観察ないし監視を行う権限はない。したがって、使用者が労働者に対し業務用の GPS 機能付き携帯電話等を勤務時間外にも携帯するよう求め、それを通じて勤務時間外における労働者の位置情報を取得することはプライバシー権または人格権の侵害に該当する可能性が高い。

それでは、労働者本人の同意があれば、勤務時間外における彼らの位置情報を取得し利用することは例外的に許されるのか。通常、使用者にとって、勤務時間外における労働者の位置情報の取得・利用について、業務上の必要性はほとんどないであろう。その必要性があるのは、ごく稀なケースである。このことを踏まえ、私的領域における労働者のプライバシー権の保護の観点から、勤務時間外における労働者の位置情報の取扱いが適法とされるのは、業務との関連で特別な必要性があり、なおかつ、その旨を含め位置情報の取得・利用について十分な情報提供・説明を行ったうえで、労働者本人から書面等で明確な同意を得た場合に限定されよう。そうでない限り、プライバシー権の侵害に該当し、違法と評価されよう。つまり、勤務時間外における位置情報の取扱いについて、特別な必要性がない場合や、勤務時間中ばかりではなく勤務時間外の時間帯をも含めて包括的に同意を取得する場合などである。

実際に、前述の東起業事件では、勤務時間外における労働者の位置情報の取得について、「早朝、深夜、休日、退職後のように、従業員に労務提供

義務がない時間帯、期間において本件ナビシステムを利用して原告の居場所確認をすることは、特段の必要性のない限り、許されないというべきである」とされた。

それに加えて、仮に労働者の同意があり、使用者がプライバシー権の侵害を問われえないような場合でさえ、労働者の位置情報の取得・利用の仕方によっては、労働者の人格権との関連で問題が生じうる。つまり、使用者が、業務用のGPS機能付き携帯電話・端末等を通じた四六時中の監視およびそれに基づくリアルタイムの指図・命令等により、著しい精神的な圧迫を加え、自主的な行動を大幅に制限するような、前述した「ジオスレイバリー」のような奴隷的拘束状態に労働者を縛り付けるようなときは、労働者は、人格権の侵害を理由に、使用者に対し損害賠償責任を追及したり、差止請求を行ったりすることができるであろう。

## V 労働者のプライバシーへのさらなる脅威——生体認証

さらにわが国の企業では、前述のRFID内蔵の社員証の代わりに（とともに）、ネットワークのアクセス制御をはじめ、労働者の入退出管理や勤怠管理のため、生体認証も利活用されるようになってきた。生体認証は、指紋、静脈、虹彩、顔などの生体的特徴を利用して特定の個人を認証する技術である。それは、個人自らの生体情報を用いるので、暗証番号・パスワード等の「知識」や、鍵・カード等の「所有物」といったその他の認証手段に伴う忘却、紛失ないし盗難といったリスクを回避できる確実な認証手段である。それゆえに、ユビキタスネットワーク環境において、ネットワークへの脅威に対し情報の安全性を保つため、情報の機密性・完全性を確保するとともに、情報を操作できる個人を正確かつ容易に特定できる認証手段として、生体認証が不可欠なインフラである<sup>26)</sup>。

生体認証は、他の認証手段よりも際立った利便性を有する反面、その利用する生体情報がセンシティブな個人情報であるため、プライバシーや個

人情報保護をめぐる諸問題を抱えている<sup>27)</sup>。たとえば、①本人の知らないうちに生体情報のいくつかは取得可能であり、本人の同意を得ずにそれが取得・利用されるおそれがあること、②本人認証のためのみと称して、生体情報が取得されたが、本来の目的とは異なる監視や行動追跡またはプロファイリングのためそれが転用されるおそれがあること、③生体情報が外部に漏洩してしまうと、（暗証番号やカードのように）それを無効化ないし交換することは不可能であるため、他人がその生体情報から人工生体情報を作成し本人になりすましてそれを利用しても、無権限者による不正行為であることを本人が証明することはきわめて困難であること、④取得された生体情報によっては、人種情報、健康状態、病歴などのセンシティブな個人情報が不可避免的に明らかになること、⑤生体情報の取得、とりわけ指紋の採取は、「犯罪者扱いするのか！」といった抵抗感ないし屈辱感を抱かせ、精神的苦痛を与えうること、である。

職場への生体認証の導入に伴って、労働者は以上のようなプライバシーや人間としての尊厳への脅威にさらされることになる。このことについては、現行法は、個人情報保護法による使用者への事前の規制を通じて、労働者の権利利益の保護を図ることになろう<sup>28)</sup>。もっとも、生体認証に対する個人情報保護法の適用については、同認証に伴う生体情報の取得・利用特有の問題への対処のため特別な考慮が必要となるが、現行法の下では、それに関する包括的な指針やガイドライン等は策定されてはいない。ただ、最近改訂されたばかりの「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」（平成26年12月12日厚生労働省・経済産業省）は、個人データの安全管理措置の一環として生体認証の利用を推奨するにもかかわらず、「生体認証を利用する場合には、当該識別と認証の方法を実施するために必要な情報（例えば、指紋、静脈）が、特定の個人を識別することができることから、個人情報に該当する可能性があることに留意する」とことと指摘するだけにとどまっている<sup>29)</sup>。

とはいえ、前述したように、労働者のモニタリングないし監視の道具として用いられうること



や、労働者のプライバシーや人格への脅威がきわめて大きいことを考慮すると、生体認証のため労働者の生体情報を取得し利用するためには、使用者は少なくとも、そのことに関する社内規程を策定するとともに、その取得・利用の目的、仕組み、取得する情報の種類等について十分な情報提供・説明を行ったうえで、生体情報の取得・利用について労働者から自由な意思に基づく同意を得ること、および、取得した生体情報のより厳格な安全管理措置を実施することを明確に義務づけられる必要がある。さらに、生体認証の導入・実施に際しては、使用者はあらかじめ労働組合等に通知し、必要に応じて協議を行うことも求められよう。

企業への情報セキュリティの社会的要請が強まる中、そのセキュリティ確保にとって優れた生体認証の有用性や利便性に目を奪われ、その脅威にさらされる労働者の権利利益がなおざりにされてはならない。

追記：いわゆる個人情報保護法改正案が、2015年5月21日に衆議院で可決されたが、年金情報流出問題等の影響により、初校校正時点になっても、参議院で審議中である。そのため、本論は同改正（案）を踏まえて検討し論じてはならず、現行法を前提とするものであることをお断りする。

- 1) 総務省「第二章「スマート革命」が促すICT産業・社会の変革」『情報通信白書平成24年版』（2012年）136頁以下参照。スマート革命の進捗状況については、それ以降の各年の同白書を参照。
- 2) GPS機能付き携帯電話・端末による労働者の位置情報の取得・利用をめぐる問題については、すでに拙稿「スマホとともに、ジオスレイバリーがやって来る！——GPSに基づく労働監視 vs 労働者のプライバシー・人格権」富大経済論集 58巻 2-3号 235頁（2013年）で検討した。本論は、GPSのみならずその他のICTを用いた位置情報や生体情報の取得・利用全般について考察を深め論ずるものである。
- 3) 岸上順一監修『ポイント図解式RFID教科書——ユビキタス社会に向けた無線ICタグのすべて』アスキー（2005年）、一般社団法人日本自動認識システム協会『よくわかるRFID（改訂2版）——電子タグのすべて』オーム社（2014年）参照。
- 4) 各種のサービスの特徴や内容、問題点等については、神崎洋治『スマートフォンGPS活用ブック』日経BP社（2012年）参照。
- 5) RFIDを用いた労働者の監視に関する諸外国の実例を紹介する「職場でICタグを使った監視」ワールド・オブ・ワーク 8号 24頁以下（2007年）を参照。
- 6) 「通信の秘密」の保障は、通信の内容ばかりではなく、発信元または受信元の氏名・住所および通信の日時や回数など、通信に関するすべての事項に及ぶ。もちろん、GPSを通じて

収集される位置情報も含まれる。

- 7) NATIONAL WORKRIGHTS INSTITUTE ウェブサイトからJeremy Gruber, RFID and Workplace Privacy 参照。
- 8) 被疑者の車両に取り付けたGPSを通じた捜査機関の監視・追跡に関する事例ではあるが、位置情報を記録すれば、個人の日常生活の詳細を明らかにできると、いち早く米国の裁判例が指摘している。State v. Jackson, 76 P.3d 217 (Wash. 2003)。
- 9) 安岡寛道編著『ビッグデータ時代のライフログ』東洋経済新報社 5頁以下（2012年）や、城田真琴『ビッグデータの衝撃』東洋経済新報社 182頁以下（2012年）参照。
- 10) アメリカにおけるその実例については、ベン・ウェイバー『職場の人間科学——ビッグデータで考える「理想の働き方」』早川書房（2014年）、ネイサン・イーグル、ケント・グリーン『みんなのビッグデータ——リアリティ・マイニングから見える世界』NTT出版（2015年）参照。日本の利用例として、矢野和男『データの見えざる手——ウェアラブルセンサが明かす人間・組織・社会の法則』草思社（2014年）参照。
- 11) 安岡・前掲注9）書 198-202頁（安岡執筆担当）参照。
- 12) たとえば、プロフィール分析により導き出された人物像が対象労働者の実像を正確に描写するものでなかった場合、その誤った人物像に基づき処遇されると、対象労働者は重大な権利侵害を受けることになる。なお、行動ターゲティング広告などを念頭に置いたライフログの利用に関する問題点として、①ユーザーが知らないうちに情報が収集されていること、②ライフログの実態がよく分かっていないこと、③プライバシー侵害の可能性、④誰の関心事であるかについての誤解可能性、⑤ユーザーの知る権利の制約、⑥平等性を損なうおそれ、⑦犯罪組織によって利用され、経済的・物理的被害を生じさせるおそれ、といった点が指摘されている。日本弁護士連合会『デジタル社会のプライバシー——共通番号制・ライフログ・電子マネー』航思社 69-77頁（2012年）参照。
- 13) <http://www.asakawa-clinic.jp/pc/free2.html> 参照。精神科医の浅川雅晴氏によると、携帯電話に上司から着信があることが精神的な負担となり、心身症を患う若手社員が増加中である。一言で表せば、この現象は「ケータイ恐怖症」である。症状はさまざまで、うつや動悸、頭痛、吐き気、多汗などである。悪化すると、「幻想振動症候群」に陥る。つまり、着信がないのにケータイが鳴っていると勘違いしたり、パイプレーターが振動していると錯覚するようになる。
- 14) ジオスレイバリーとは、次の論文の筆者の作り出した、「ジオ (geo-)」と「スレイバリー (slavery)」と組み合わせた造語である。Jerome E. Dobson & Peter F. Fisher, "Geoslavery," *IEEE Technology and Society Magazine*, (Spring 2003), at 47 (<https://www.msu.edu/~kg/874/geoslavery.pdf>)。
- 15) 5000人未満の個人情報しか保有しない企業は、個人情報保護法の義務規定は適用されない。とはいえ、後述される雇用管理分野のガイドラインによると、「個人情報取扱事業者」以外の企業についても、個人情報取扱事業者に準じて、個人情報の適正な取扱いの確保に努めることが求められている。
- 16) 拙稿「新たな段階を迎えた労働者の個人情報保護と企業の対応」季労 213号 71頁以下（2006年）と拙著『従業員の個人情報保護と人権——求められる企業の積極的対応』大阪企業人権協議会（2007年）参照。
- 17) 電気通信事業における個人情報保護に関するガイドライン（平成25年総務省）の解説参照。

- 18) 解説によると、利用者からの同意取得について「個々の位置情報の提供ごとのほか、サービス提供開始時などに事前に行うことも可能である。もっとも、同意取得は移動体端末の操作や書面による確認などの方法により明確に行うべきであるほか、全くの包括的な内容の同意を得ることは適当でなく、位置情報を提供する者の範囲を特定しておくなどすることが望ましい」とするとともに、「事前の同意は原則として撤回できなければならない」とする。
- 19) 解説では、利用者の認識・予見可能性の確保について、「画面表示や移動体端末の鳴動等の方法により、位置情報が提供されることを認識できることを可能とすることなどが考えられる」とする。
- 20) 解説によると、「GPSによる位置情報など、電気通信サービスの提供に必要な位置情報は、原則として利用者の意思に基づかずに取得してはならない」とする。
- 21) 「位置送信拒否設定」があるからといって、実際に労働者が位置情報取得の可否を制御できるかどうかは別問題である。このことについて詳しくは、拙稿・前掲注2) 論文88頁参照。
- 22) 拙稿「人事労務管理と労働者の人格的利益の保護」日本労働法学会編『労働者の人格と平等 講座21世紀の労働法第6巻』有斐閣(2000年)79頁以下参照。
- 23) 拙稿・前掲注16) 論文74頁参照。
- 24) 拙稿・前掲注16) 論文74頁参照。
- 25) たとえば、指導員の教育訓練のため教習車にテープレコーダーを設置した広沢自動車学校事件(徳島地決昭61.11.17 労判488号46頁)では、録音の実施にあたり十分な事情説明

や協議を通じて従業員の納得を得よう努めなかったことや、監視による心理的圧迫を考慮して、従業員の「自由な同意」を得ることなく一方的に録音することは違法である、とされた。労働者の職務遂行の観察または監視に関するその他の事例については、拙稿・前掲注22) 論文85頁参照。

- 26) 生体認証技術全般について、小松尚久ほか『バイオメトリクスのおはなし——あなたの身体情報が鍵になる』日本規格協会(2008年)参照。
- 27) 松前恵環「バイオメトリクス技術とプライバシー——その法的側面についての一考察」情報学研究：東京大学大学院情報学環紀要73号51頁、55頁以下(2008年)参照。
- 28) 個人情報保護法の生体情報への適用一般に関しては、新保史生「個人情報保護法に基づくバイオメトリクスの利用」情報メディア研究4巻1号55頁(2006年)を参照。
- 29) 金融・信用分野のガイドラインにおいては、機微(センシティブ)情報に該当する生体認証情報は、本人の同意がない限り、取得、利用、第三者提供してはならないとされている。「金融分野における個人情報保護に関するガイドライン」(平成25年3月19日金融庁)や「経済産業分野のうち信用分野における個人情報保護ガイドライン」(平成21年10月9日経済産業省)参照。

たけち・きよし 富山大学経済学部経営法学科教授。最近の主な著作に「職場と入れ墨——偏見と寛容の狭間」富大経済論集60巻2号355頁(2014年)。労働法専攻。