# LINE 事件と中国におけるガバメントアクセス規定

GBL 研究所理事・CIPP/E 浅井敏雄 [1]

【目　次】

（各箇所をクリックすると該当箇所にジャンプします）



## ■LINE 問題の経緯

本年 3 月 19 日、LINE 利用者の個人情報を中国の会社が閲覧できた問題（以下「本件」という）で、個人情報保護委員会（以下「委員会」という）は、LINE 株式会社（以下「LINE 社」という）に対し、個人情報保護法（以下「法」という）第 40 条第 1 項に基づく報告徴収を行うとともに、同月 31 日より立入検査を開始しました。

**4 月 23 日、委員会は、本件の立入検査は継続中であるものの一定の確認が終了したとして、「個人情報の保護に関する法律に基づく行政上の対応について」（LINE 株式会社・令和 3 年 4 月 23 日）を公表**しました。

## ■4 月 23 日委員会公表内容

（注）一部省略・編集。[ ]内は筆者追記（以下同じ）

### 1. 今回の指導・公表の趣旨

本件の立入検査は継続中であるものの、一定の確認が終了した。**LINE 社が委託等した個人データは秘匿性が高く、数量も多いことから、不適切な取扱いが生じた場合の影響も大きい[ので]、LINE 社には、それに応じた高い安全管理措置が必要であり（＊1）**、この観点から改善を要する事項が認められ、法第 41 条に基づく**指導を行った**[のでこれを公表する]。[報道によれば、その上で、1 か月以内に改善状況を報告するよう求めたとのこと [2]]

### 2. 今回の指導の内容

(1)**個人データの取扱いを委託する場合** [3]**には、**法第 22 条に基づき委託先に対する必要かつ適切な監督を行う義務があるところ、**法第 20 条に基づき自らが講ずべき安全管理措置と同等の措置が講じられるよう、例えば次のような手法により必要かつ適切な監督を行うこと。（＊2）**

**〇委託先**（再委託先を含む。以下同じ）のシステム開発者**に個人データへのアクセス権限を付与する場合には、その[アクセス権限付与の]必要性及び[アクセス]権限付与の範囲を組織的に検討した上、必要な技術的安全管理措置を講ずること。**

---

[1] **【本稿の筆者】** 一般社団法人 GBL 研究所理事／IAPP CIPP/E (Certified Information Privacy Professional/Europe)／UniLaw 企業法務研究所代表 浅井敏雄(Facebook)

[2] **【改善状況報告要求】**（参考）NHK「個人情報保護委 LINE に行政指導 業務委託先への監督体制不十分」2021 年 4 月 24 日

[3] **【LINE 社による委託の具体的内容】** LINE 社が委員会発表と同日（4 月 23 日）に公表した「当社に対する個人情報保護委員会からの指導および当社の改善策について」（以下「LINE 社公表文」という）には以下のように記載されている。「当社は、当社サービスにおけるコンテンツのモニタリング業務を行うための社内ツールである LINE Monitoring Platform（以下、LMP）を含む各種システムの開発・保守業務を、中国子会社である Shanghai LINE Digital Technology Limited. Dalian Branch（以下、LINE China）に再委託しておりました。また、当該業務委託においては、業務の過程で個人データを取り扱い得ることから、当該業務に必要な範囲におけるアクセス権限を付与したうえで、個人データの取扱いも委託しておりました。」

〇委託先のシステム開発者に個人データへのアクセス権限を付与する場合には、**不正閲覧等を防止するため、アクセスしたデータの適切な検証を可能とするログの保存・分析など組織的安全管理措置を検討した上、必要な措置を講ずること。**

**〇委託先における個人データの取扱状況を把握するため、定期的に監査を行う**など、委託契約の実施状況を調査した上で、委託内容等の見直しの検討を含め、適切に評価する措置を講ずること。

(2)LINE サービスの提供に関してメッセージ等の個人情報を取得する場合には、取得する個人情報の範囲を分かりやすく通知するとともに、通知内容が適切に表示されているか確認する体制を整備すること。[4]

### 2. 本年 4 月 23 日現在の立入検査による確認の状況

(1) 法第 22 条の委託先の監督については、上記 1.(1)のとおり一部改善を要する事項があり、改善を求めた。

**(2) 法第 24 条の外国にある第三者への提供の制限**

**〇「基準適合体制」については、**一部改善を要する事項はあるものの、**基準適合体制を整備するための措置が概ね講じられていた。(＊3)**

**〇「本人の同意」については、**プライバシーポリシーにおいて、利用者の個人情報の**利用目的**(サービスの提供・改善、コンテンツの開発・ 改善、不正利用防止等)**及び業務委託先の外国の第三者へ提供することが明記されており、利用者にとって外国にある第三者に提供する場面を特定できなかったとは言い難い。(＊4)**

(以 上)

## ■4 月 23 日委員会公表内容の分析

### 1. 法 24 条(外国にある第三者への提供の制限)違反の有無

筆者もそうでしたが、本件については、最初に本件がニュースとなった際、一体何が問題になっているのかなかなか理解できなかった企業担当者が多かったのではないでしょうか。

何故なら、外国にある第三者に個人データを提供する場合であっても、本件のようにその提供が個人データの取扱いの委託に伴い行われる場合、提供元(本件では LINE)と提供先の外国にある第三者(本件では中国の子会社)との間で法上の事業者の義務と同様の義務を委託先に課す委託契約(基本的には委託した取扱い以外の利用・提供を禁止し法 20 条の安全管理措置を義務付ければよい)を締結しておけば、その提供自体は本人の同意なく適法に行うことができるからです(法 24 条「第三者」括弧書き、23 条 5 項一号、規則第 11 条の 2、「個人情報の保護に関する法律についてのガイドライン(外国にある第三者への提供編)」(以下「外国ガイドライン」という)2(3), 4-1)。[5]

この点、上記(＊3)では、「基準適合体制」を整備するための措置が概ね講じられていた、とされています。**この「基準適合体制」とは**法 24 条の条文中の「外国にある…第三者」の後の括弧内の「個人データの取扱いについてこの節の規定により個人情報取扱事業者が講ずべきこととされている措置に相当する措置を継続的に講ずるために必要なものとして個人情報保護委員会規則で定める基準」であり、**具体的には上記委託契約等**と思われます。そして、これについては「基準適合体制を整備するための措置が概ね講じられていた」とされているので、**この点に関しては法 24 条違反はなかった**ことになります。

そうすると、本人同意は不要となる筈ですが、それにもかかわらず、上記(＊4)では「本人の同意」について触れており、その意味が良く分かりません。可能性としては、LINE 社は「基準適合体制」を整備するための措置により本来本人の同意は不要であるにもかかわらず、LINE 社はそれを選択せず(またはそれに重ねて)、LINE 利用者によるプライバシーポリシーへの同意をもって法 24 条を遵守しようとしていたのかもしれません。そして、それについては、「外国ガイドライン」(2.1)にある「個々の事例ごとに判断されるべきではあるが、…法第 24 条において求められる本人の同意を取得する場合、本人の権利利益保護の観点から、外国にある第三者に個人データを提供することを明確にしなければならない」とされているところ、この点に関しても、『「本人の同意」については、…利用者の個人情報の利用目的…及び業務委託先の外国の第三者へ提供することが明記されており、利用者にとって外国にある第三者に提供する場面を特定できなかったとは言い難い』とされているので、**本人の同意に関しても法 24 条違反はなかった**ことになります。

従って、**いずれにしても、LINE 社に法 24 条違反はなかった**ことになります。

---

[4] **【通知内容の不適切な表示】**「LINE 社公表文」では以下のように記載されている。『当社は、当社サービスのユーザーの皆さまに対して[身に覚えのないアカウントからの出会い系スパム、商品やサービスの広告の迷惑メッセージ等の]「通報」機能を提供しております。「通報」画面においては、「通報」に際して当社に送信されるトーク等の情報の範囲を記載した文言が表示されますが、過去に LINE アプリを修正した際に生じたバグにより、本来当社が意図していた通報時の説明文言とは一部異なる文言が表示されていたことを確認し…[したが、既に訂正した]』

[5] **【委託契約に基づく個人情報の外国にある第三者への提供】**(参考) 弁護士ドットコムニュース「LINE「個人情報」問題で考える「無料サービス」の対価と安全性 データの安全確保への課題は？」2021 年 4 月 18 日,Yahoo Japan. 委託契約は、この中の影島弁護士の「しかしながら、適切な契約やグループ内規程などがあれば、同意なく海外にデータを移転できますので(前記 3)、この方法を用いて移転していたのであれば問題ありません」との発言の中の「適切な契約」に当たる。

## 2. 法 22 条(委託先の監督)・20 条(安全管理措置)

上記(＊1)では、委託先において法第 20 条の安全管理措置と同等の措置が講じられるよう改善措置を行うことが指導されています。

しかし、**法 22 条の委託先の監督・法 20 条の安全管理措置については、具体的な個人情報の漏えい(またはその可能性)が発覚して初めてが委員会の立入調査が行われるのが通常**だと思われます。これに対し、本件では、筆者の知る限りそのような事象は報道されていません。**それにもかかわらず、本件で立入検査がなされたのは何故か？**その答えは、上記(＊1)および一部報道で指摘されていた中国の「国家情報法」(いわば国家スパイ活動基本法)にあると思われます。

すなわち、LINE は、今や国内で約 8600 万人もの国民が利用し、自治体の情報発信や各種手続きなどにも活用される社会インフラとなり、LINE 社が委託等した個人データは秘匿性が高く、数量も多い。特に**委託先が中国の企業である場合、国家情報法等により、中国政府からの日本国民の個人情報へのアクセス(閲覧・入手等)(ガバメントアクセス)の可能性もあり、**不適切な取扱いが生じた場合の影響も大きい[6]ので、LINE 社には、それに応じた高い安全管理措置が必要である。そして、この中国政府による個人情報を含むデータへの「ガバメントアクセス」の可能性について(おそらくは政府・政界筋から)**日本の安全保障上の懸念が示された**のではないかと思われます。[7]

なお、この「ガバメントアクセス」については、委員会の「個人情報保護法 いわゆる 3 年ごと見直し 制度改正大綱」(令和元年(2019 年)12 月 13 日)で、次のように記載されていました(p 29,30)。

「海外への業務委託の一般化…が進む中、…外国政府による無制限なガバメント・アクセスによって、我が国で取得され越境移転された個人データが不適切に利用されるおそれがあ[り、]こうした国家管理的規制は、個人の権利利益の保護の観点から看過しがたいリスクをもたらすおそれがある。…」

この大綱発表後、2020 年には三菱電機の事件[8]、FBI 長官による中国のスパイ活動に関する警告[9]等があり、一方、LINE は非常に多くの国民が利用し社会インフラともなり、このコロナ禍で更なる活用拡大の可能性もありました。[10]

**以上の諸事情を総合的に考えると、本件の本質は中国政府による個人情報を含むデータへの「ガバメントアクセス」への懸念である**と思われます。

**そこで、以下においては、この観点から、中国の「国家情報法」および「サイバーセキュリティー法」における「ガバメントアクセス」関連規定について解説**します。

## ■国家情報法およびサイバーセキュリティー法制定の背景

習近平氏が総書記(共産党中央委員会総書記・同中央軍事委員会主席)に就任した **2012 年以降、中国では、以下のように相次いで国家安全保障に関する施策・法律の制定**がなされました(脚注[11]資料「岡村」p 64,65)

2013 年:国家安全(保障)政策を主導する国家安全委員会の創設決定

**2014 年:習近平国家主席が以下内容の「総合的国家安全観」という国家安全政策の新基本原則を打ち出す。**

**【「総合的国家安全観」】 国家の安全(保障)という概念を**、政治・国土・軍事・**経済・文化・社会・科学技術・情報**・生態系・**資源**・核**という極めて幅広い分野に適用しそれらの**包括的かつ効果的な安全の**実現を目指す国家政策の理念**。

**以降、この「総合的国家安全観」に基づく国家安全保障を強化するための法的基盤整備として以下の法令が制定**されました。

2014 年:反スパイ法(外国政府等によるスパイ行為を防止)

2015 年:国家安全法(「総合的国家安全観」の全般的な内容をそのまま反映)

2015 年:反テロリズム法(法目的:テロ行為の防止。少数民族による分離独立活動等も対象となり得ると思われる[12])

2016 年:国外 NGO 国内活動管理法(国外 NGO の中国国内での活動規制)

**2016 年:サイバーセキュリティ法(サイバー空間の国家安全保障と民間に対する個人情報保護の義務付け)**

---

[6] **【LINE の利用者数・社会インフラ化】** 「LINE データ管理問題、社会インフラの情報流出リスクに懸念の声」 2021 年 03 月 22 日, ITmediaNEWS

[7] **【LINE 問題 安保上の懸念】** 瀬川奈都子「LINE の情報管理、安保上の懸念も 国際分業に潜むリスク」2021 年 3 月 18 日 日本経済新聞

[8] **【三菱電機の事件】** 吉野 次郎「三菱電機も被害、国際サイバー諜報戦は敵だらけ 英国の元スパイが明かす"真実"」 2020.1.21, 日経ビジネス. 須藤龍也「中国の影、たどり着いた雑居ビル 三菱電機サイバー攻撃」2021 年 3 月 28 日, 朝日新聞デジタル

[9] **【FBI 長官による中国のスパイ活動に関する警告】** 「FBI 長官、中国のスパイ活動に異例の警告」 2020 年 7 月 8 日

[10] **【LINE の利用者数・社会インフラ化】** 「LINE データ管理問題、社会インフラの情報流出リスクに懸念の声」 2021 年 03 月 22 日, ITmediaNEWS

[11] **【中国国家情報法に関し主に参考とした資料】** (1)(原文条文)「中华人民共和国国家情报法」. (2) 岡村志嘉子 「中国の国家情報法」 2017/12/08 国立国会図書館デジタルコレクション － 解説の他、条文の全訳を含む(「岡村」). (3) (同法英訳)National Intelligence Law of the P.R.C. (2017) (China Law Translate)

[12] **【中国反テロ法の対象】** (参考) 「中国で反テロ法が成立 少数派締め付けに懸念」 2015 年 12 月 28 日, BBC ニュース

**2017 年:国家情報法(国家による情報活動(諜報活動)を強化・保障)**
2017 年:核安全法(核の安全確保)
以上から分かるように、**国家情報法もサイバーセキュリティー法も、上記の「総合的国家安全観」に基づく国家安全保障を実現するための法的基盤の一部**ということができます。

## ■中国国家情報法におけるガバメント・アクセス関連規定

### 1. 本法の性格・国家情報活動の範囲・実行機関・方法等

本法は、国家情報活動(脚注の英訳では"national intelligence work")(国家による諜報活動)の在り方や実施体制について明確な法的根拠を示したものです。
本法上、この**「国家情報活動」の範囲に**関する明確な規定はありませんが、第 1 条に国家情報活動の目的が「総合的国家安全観」の堅持等であることが規定されていることから、経済・科学技術等に関する情報活動、すなわち、**産業スパイ活動等も含まれる**可能性があると思われます。
本法の第 10 条では、「国家情報活動機構は、業務上の必要に基づき、法に従い**必要な方法、手段**及び経路を利用し、**国内外において**情報活動を行う」**とされているので、全ての手段(例:通信傍受(15)[13]、インターネットを通じた諜報活動)による諜報活動と外国での諜報活動が含まれます**。
この**国家情報活動を担う機関は**、第 5 条から、具体的には、**国家安全省、公安省情報部門および中国人民解放軍の情報部門(同条で「国家情報活動機構」と総称)**であると解されています(岡村 p 71 脚注)。
本法第 11 条には、特に、国家情報活動機構が、**外国の機関・組織・個人**による中国の国家安全・利益に危害を及ぼす行為**に関する**またはこれを防止・処罰するための**情報活動**をしなければならない旨規定されています。
本法第 12 条には、**国家情報活動はこれを関係個人・組織(民間企業・民間人も含まれると思われる)に委託できる**旨規定されています。
なお、**国家情報法は、ファーウェイをめぐる対立等でも**、中国企業と中国政府の協力関係を裏付ける法律として**米国等で問題視**されてきたとされています。[14]

### 2. 中国企業・中国国民の協力義務

本法 14 条では、国家情報活動機構は、国家情報活動に関し、関係する機関・組織・国民に対し、必要な支持・援助・協力を求めることができるとされ、**第 7 条で「如何なる組織・国民も、法に基づき、国家情報活動に対する支持・援助・協力を行い、知り得た国家情報活動についての秘密を守らなければならない」と規定**されています。
**すなわち、中国の民間企業・民間人も情報活動への協力等を求められた場合、これに応じる義務およびその場合における秘密保持義務を負います。本法に関し海外から最も警戒されているのはこの点です。**
前記の通り、国家情報活動には外国での活動も含まれ、また、「如何なる…国民も」ですから、**外国(例:日本)にいる中国国民も、国家情報活動(中国政府による諜報活動)に対する協力義務を負う**ことになります。

### 3. 諜報活動に協力した個人・組織の保護・奨励・国家補償等

本法第 7 条第 2 項に国家情報活動に協力等した個人・組織の保護、同 9 条に同活動に貢献した個人・組織の表彰・報奨、25 条にこれらの個人・組織が協力により蒙った損失の国家補償が規定されています。

## ■中国サイバーセキュリティー法におけるガバメント・アクセス関連規定

### 1. 中国サイバーセキュリティー法におけるガバメント・アクセス関連規定

---

[13] **【通信傍受】** 本法 15 条で国家情報活動機構は「技術的偵察措置」を講ずることができるとされ、この措置は具体的には通信傍受であると解されている(岡村 p 73 脚注)
[14] **【国家情報法とファーウェイ制裁事件】** 福田直之、冨名腰隆『外国でスパイ「中国企業に求めたことない」全人代報道官』2019 年 3 月 5 日, 朝日新聞デジタル. なお、この記事によれば、全人代報道官は、国家情報法に関連し、「中国企業に現地の法律に違反する活動を求めたことも求めることもない」と述べたとされている。

中国サイバーセキュリティー法[15]（以下「CS 法」という）の第 1 の目的はネットワーク空間における国家の主権[支配・統治権]・国家安全保障および社会の公共の利益[社会秩序の維持]です(1 条前段)。その他の法目的として「公民、法人その他の組織の適法な権益」の保護も挙げられており(1 条中段)、同法には個人情報保護に関する規定（40 条以下）もありますが、それらは、あくまでネットワーク運営者の義務であり、政府機関は規制されていません。この点は EU の GDPR のような個人情報に関する国家からの人権保護が重要な側面を有する法制とは本質的に異なります。

CS 法では、国家安全の観点から、国内外からのネットワーク攻撃等に対し、国家の防御責務（5 条）、ネットワーク運営者のセキュリティー確保義務（21 条）等が定められています。

更に、**ネットワーク運営者（日本企業の中国子会社を含めほぼ全ての民間企業が含まれる）は、公安機関または国のセキュリティー機関が行う国家安全保障活動または犯罪捜査に対し、技術支援および協力をしなければなりません**(28 条)。**この技術支援には、公安機関等が行う国民・企業による遵守監視活動への技術支援、および、ネットワーク運営者が収集した個人ユーザ等の個人情報の提供も含まれる**と思われます。

### 2. 公安機関インターネットセキュリティー監督検査規定におけるガバメント・アクセス関連規定

「公安機関インターネットセキュリティー監督検査規定」は **CS 法と中国人民警察法の下位法令であり、ネットワーク運営者のセキュリティー確保義務の遵守状況に関し公安機関（人民警察）が行う監督・検査について定める**ものです（1 条）。（以下の記述の根拠および本規定全体の解説については脚注資料 [16]参照）

そして、**本規定によれば、公安機関は国家安全保障、インターネットセキュリティー、違法情報の公開・送信防止等の観点から企業に対し現地検査（立入検査）および遠隔検査（システム侵入テスト等）を行うことができるとされており、実際、日本企業の中国企業に対しても行われている**ようです [17]。

**現地検査では、コンピュータ室等への立入り調査、担当者等からの聴取、検査対象企業の情報・データ（企業秘密、知的財産を含む）の閲覧・コピー、情報セキュリティーのチェック等が行われます。**

**遠隔検査には検査対象企業のシステムへの「侵入テスト」（内容的にはハッキングと同じ）が含まれます。**人民警察は**その際専門業者の支援を受けることができます。遠隔検査では、検査対象企業が気づかない内に、自社システムに侵入され、その情報セキュリティーに関する情報、自社保有情報・データが公安機関にチェックおよび入手され他の政府機関等に提供される可能性があると思われます。**

**監督検査は、**国家安全保障、インターネットセキュリティー、違法情報の公開・送信防止、テロリズム防止等の観点から行われること、また、遠隔検査が日本企業の中国子会社から国境を越えその日本企業にまで及ぶことも少なくとも物理的・技術的には可能と思われることから、**非常に広範に、かつ、（可能性としては）日本国内の企業にまで及び得る**ものと思われます。

## ■終わりに

報道 [18]によれば、今回、LINE 社は、今後中国で日本国内利用者の情報を扱うサービス開発やデータ運用をせず、中国で個人情報を扱わない方針のようです。しかし、どの企業でもこのような対応ができるわけでもありません。また、日中間の輸出と輸入を合わせた貿易額で既に中国は米国を上回っており、2020 年には輸出でも中国が米国を超えたとされています。[19] 従って、日本企業は、今後も、上記のような中国におけるガバメント・アクセスの問題を完全に回避することはできず、どうにかしてそのリスクを最小限化する方策を考えるしかありません。

---

**【注】**

[15] **【中国サイバーセキュリティー法に関する参考資料】** 浅井敏雄「中国サイバーセキュリティー法（インターネット安全法）：データ・ローカライゼーションと個人データ保護」2017 年 10 月

[16] **【「公安機関インターネットセキュリティー監督検査規定」に関する全般的解説】** 浅井敏雄『中国の国家安全保障と「中国サイバーキュリティー法」の執行規定～「公安機関インターネットセキュリティー監督検査規定」の概要～』企業法務ナビ, 2020/09/24

[17] **【日本企業の中国拠点に対する監督検査の実施状況】** 新村僚「中国サイバーセキュリティー法対応-説明準備できていますか？」2020 年 9 月 13 日, Internet Initiative Japan Inc.（「新村」）

[18] **【LINE による個人情報国内移管方針】**「LINE、中国で個人データ扱わず　個人情報問題で方針」2021 年 3 月 23 日, 日本経済新聞

[19] **【日中間の貿易額】**（参考）加谷珪一『急激ペースで「中国従属化」が進む日本経済の大問題』2021 年 4 月 19 日, JBPress, Yahoo ニュース