資料６－２

別紙１

公表資料

LINE ヤフー株式会社における LINE に関する個人データの漏えい等事案に対する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【詳細資料】

第１　事案の概要等

１　LINE ヤフー株式会社（以下「LY 社」という。）[1]はコミュニケーションアプリである LINE（以下「LINE」という。）の開発・運営を行っており、LINE のユーザー（以下「LINE ユーザー」という。）[2]、取引先、従業者等に関する個人データを取り扱っている。

２　本件は、令和５年８月 10 日及び同月 24 日に、LY 社の業務委託先の韓国企業であるセキュリティ保守会社（以下「A 社」という。）の従業者により業務上使用されていた PC（以下「A 社 PC」という。）がマルウェアに感染したことが契機となり、同年９月 14 日から 10 月 27 日の間、LY 社の情報システム（以下「本件情報システム」という。）が不正アクセスを受け、LINE に関するユーザー、取引先、従業者等に関する個人データ（以下「本件個人データ」という。）が漏えい等した事案（以下「本件事案」という。）である。

３　本件事案により漏えい（漏えいのおそれを含む。以下同じ。）した個人データは約 52 万人分であり、その内訳は下表のとおり。

	漏えいのおそれを含む総件数	漏えいが確認された件数	漏えいのおそれがある件数
LINE ユーザーの個人データ	302,980 人分（うち、130,192 人分は日本のユーザー）	253,229 人分（うち、114,738 人分は日本のユーザー）	49,751 人分（うち、15,454 人分は日本のユーザー）
取引先の個人データ	86,211 人分	86,122 人分	89 人分
従業者の個人データ	130,315 人分	59,644 人分	70,671 人分

４　個人情報保護委員会（以下「当委員会」という。）は、LY 社より、個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「個人情報保護法」という。）第 26 条第１項に規定される漏えい等報告を受領した（令和５年 11 月７日付け速報、同月 14 日付け

[1] LY 社は、令和５年 10 月１日、旧ヤフー株式会社（以下「旧ヤフー社」という。）と旧 LINE 株式会社（以下「旧 L 社」という。）が合併し、組成された。合併以降、LINE は LY 社が運営している。

[2] 全世界で約 1.95 億人のユーザーを抱え、そのうち日本のユーザーは約 9,600 万人とされる。

中間報及び同年 12 月 27 日付け確報)。また、当委員会は、令和５年 12 月 12 日、個人情報保護法第 146 条第１項の規定による報告等の求めを行い、同月 26 日に LY 社からこれに対する報告書を受領した。その後、関係者へのヒアリング等の調査を実施し、事案の解明に努めてきた。

第２　事実関係

１　不正アクセスを受けた LY 社の情報システムについて

本件事案では、LINE サービスの運営に関わる LY 社の従業者が利用する複数の情報システムが不正アクセスを受け、前記第１の３のとおり、本件個人データが漏えいし、又は漏えいのおそれが発生した[3]。不正アクセスを受け、保管する個人データが漏えい等した情報システムは、LY 社のデータセンター（日本）に所在するものと NAVER Cloud 社（以下「NC 社」という。）[4]のデータセンター（韓国）に所在する[5]ものがあり、具体的には下表のとおりである。

なお、LY 社によると、LINE のアカウント情報、メッセージ、通話音声、動画配信等を管理するサーバへの不正アクセスは確認されていない。

システム名称	漏えいした個人データ	所在するデータセンター
データ分析システム[6]	ユーザー情報（302,469 人分）	LY 社
ソースコード管理システム	ユーザー情報（471 人分）	LY 社
社内文書管理システム	ユーザー情報	LY 社

[3] 本件事案発生時点、旧 L 社と旧ヤフー社の情報システムは分離して管理していたため、本件事案により不正アクセスを受けたのは旧 L 社の情報システムに限られ、Yahoo! JAPAN 等の旧ヤフー社提供のサービスに関する情報システムに影響はなかった。

[4] 韓国の企業である NAVER Cloud Corporation（韓国語表記네이버클라우드 주식회사)。同社は、韓国の大手 IT 企業であり検索エンジン「ネイバー」を運営する NAVER CORP.（韓国語表記네이버）の 100%子会社である。以下、NAVER CORP.及び NAVER Cloud Corporation をはじめとする子会社らをまとめて「NAVER グループ」という。

[5] LY 社によれば、LINE に関する個人データを NC 社のデータセンター（韓国）に保管するに際して、個人情報保護法第 28 条（外国にある第三者への提供の制限）の規律に関して、NC 社が個人情報の保護に関する法律施行規則（平成 28 年個人情報保護委員会規則第３号）第 16 条第２号で定める個人情報の取扱いに係る国際的な枠組みに基づく認定を受けていることを確認し、さらに、本人から外国にある第三者へ提供することの同意を取得している。

[6] LINE の各種サービス（メッセージへのリアクションやスタンプ購入等）についてユーザーの利用履歴を分析するためのシステム。

	（40 人分） 取引先情報（34 人分） 従業者情報（６人分）	
認証基盤システム	従業者情報 （29,313 人分）	LY 社
ウイルス対策管理サーバ	従業者情報(552 人分)	LY 社
社内コミュニケーション等に係るシステム	取引先情報(106 人分) 従業者情報 （78,410 人分）	NC 社
NAVER グループ共通認証基盤システム[7]	取引先情報 （86,071 人分） 従業者情報 （22,034 人分）	LY 社及び NC 社

２　本件情報システムに関する業務委託等－各社の関係性について

⑴　LY 社と NC 社の業務委託関係

LY 社は NC 社との間で、IT サービス利用等に関する業務委託契約を締結している。また、同契約に基づき、NC 社は、LINE に関するサーバ、ソフトウェア等の開発及び運用保守を実施し、LY 社は、NC 社のデータセンターに所在する社内コミュニケーション等に係るシステム及び LY 社と NC 社の両方のデータセンターに所在する共通認証基盤システムを従業者向けシステムとして利用している。

なお、LY 社は、NC 社に対して本件個人データの取扱いに係る委託[8]は行っていない。

⑵　ウイルス対策管理サーバの保守業務

LY 社は、A 社との間で、セキュリティに係るメンテナンス業務委託契約を締結しており、同契約に基づいて、A 社は、LY 社のデータセンターに所在するウイルス対策管理サーバへのアクセス権限を付与され、保守業務を行っていた。

また、NC 社も A 社との間で、セキュリティに係るメンテナンス業務委託契約を締結しており、同契約に基づき、A 社は NC 社のデータセンターに所在する NC 社のウイルス対策管理サーバの保守業務も行っていた。

なお、LY 社は、A 社に対して本件個人データの取扱いに係る委託は行っていない。

---

[7] NAVER グループの従業者と LY 社の従業者が共同で利用する認証基盤システム。以下「共通認証基盤システム」という。

[8] 個人情報保護法第 27 条第 5 項第 1 号。個人情報取扱事業者が利用目的の達成に必要な範囲内において個人データの取扱いの全部又は一部を委託することに伴って当該個人データが提供されることをいう。

３　不正アクセス及び漏えいに至った経緯

⑴　A 社への不正アクセス

A 社は、令和５年８月 10 日及び同月 24 日、不正アクセスを受け、同年９月７日頃に、A 社 PC がマルウェアに感染したことにより、不正アクセスの行為者（以下「攻撃者」という。）が、A 社 PC を遠隔操作できる状態となった（①）。その後、攻撃者は、マルウェア感染した A 社 PC を悪用し、後述のように、NC 社のデータセンターに所在するシステム及び LY 社のデータセンターに所在するシステムに対し、立て続けに不正アクセスを行った。

⑵　NC 社への不正アクセス

A 社の従業者は、令和５年９月 14 日に、前記第２の２⑵の業務委託契約に基づく定期点検作業のため、NC 社からアクセスを許可された NC 社の管理者 PC にリモート接続したところ、攻撃者は、前記⑴の遠隔操作の手法を用いて NC 社の管理者 PC 及び NC 社のウイルス対策管理サーバをマルウェアに感染させた（②）。

その後、攻撃者は、令和５年９月 18 日から同月 26 日にかけて、NC 社のウイルス対策管理サーバを踏み台として、NC 社の管理者権限を奪取し、その管理者権限により、NC 社の認証基盤システムに不正アクセスしてマルウェアに感染させ、そこに保存されていた、共通認証基盤システムにアクセスするための LY 社従業者の ID・パスワードのハッシュ値や、LY 社の認証基盤システムにアクセスするための LY 社従業者の ID・パスワードのハッシュ値を不正に入手した（③）。

⑶　LY 社への不正アクセス

攻撃者は、令和５年９月 14 日、前記⑵のとおりマルウェアを感染させた NC 社の管理者 PC から、NC 社のネットワークを介して、LY 社が A 社に発行した業務委託先用の ID・パスワードを用いて、LY 社のデータセンターに所在するウイルス対策管理サーバへ不正アクセスし、LY 社の従業者情報に関する個人データを不正に取得した（④）。

さらに、令和５年９月 27 日以降、攻撃者は、前記⑵のとおり入手した LY 社の従業者の ID・パスワードのハッシュ値を用いて、LY 社の従業者が利用する認証基盤システムへ不正アクセスし（⑤）、LY 社のデータ分析システム、ソースコード管理システム、社内文書管理システム及び社内コミュニケーション等に係るシステムへアクセスするための ID・パスワードを不正に入手した後、各種システムへ不正アクセスし、LINE ユーザーの個人データ、LY 社の取引先及び従業者の個人データを不正に取得した（⑥）。また、攻撃者は、前記⑵のとおり入手した ID・パスワードのハッシュ値を用いて、共通認証基盤システムへ不正アクセスし、LY 社の取引先情報及び従業者情報に関する個人データを不正に取得した（⑦）。

第３　問題の所在－本件事案の特性

本件事案は、セキュリティ保守の業務委託先の韓国企業である A 社への不正アクセスに端を発し、IT サービス利用等に関する業務委託先で情報資産を共有していた韓国の NC 社を踏み台としたサイバー攻撃であり、LY 社のサプライチェーン[9]が侵入経路となった不正アクセスである。

LY 社においては、個人データの所在場所を問わず、業務委託先との接続も含めたサプライチェーン全体について、その安全管理のために、個人情報保護法第 23 条及び個人情報の保護に関する法律についてのガイドライン（通則編）（以下「ガイドライン」という。）に従い、必要かつ適切な措置を講ずる必要があったところ、不正アクセス及び漏えいに至った事実関係に鑑みると、以下の点が不正アクセスの原因となっていると考えられる。

１　NC 社データセンターと LY 社データセンターとのネットワーク接続

NC 社を含む NAVER グループの従業者と LY 社のうち LINE の開発・運営に関わる従業者は、社内メールやファイル共有システム等の社内コミュニケーションを利用するための認証基盤システムを共同で利用している。共通認証基盤システムは、もともと、NAVER CORP.がグループ会社の従業者情報や組織情報を一元化することを目的として導入したものであり、後記第５の２⑴アのとおり NAVER CORP.の日本法人が LINE を開発したという経緯があることから、LY 社のうち旧 L 社の従業者は、共通認証基盤システムを利用していた。

NAVER グループ及び LY 社が共同で共通認証基盤システムを利用していたことに起因し、NAVER グループの情報システムが多数所在する NC 社データセンターと LY 社データセンターとの間はネットワーク接続が不可避であったこと及び NC 社と LY 社は、同じグループ会社として様々な業務を協業してきた経緯から、NC 社に対しては、LY 社のシステムへの広範囲なアクセスが許可されていた。

本件では、前記第２の３⑵及び⑶のとおり、共通認証基盤システムから LY 社の従業者の個人データが漏えいしており、さらに、同システムを足がかりとして、LY 社のデータセンターへ攻撃者の侵入がなされたところ、LY 社と NC 社との間で業務上必要な通信のみ接続を許可するよう適切に制御していれば、攻撃者による LY 社のデータセンターへの侵入を防止できた可能性がある。

２　重要度の高い情報システムへのアクセス管理

LY 社では、本件事案で不正アクセスの被害がなかった LINE のアカウント情報、メッ

[9] 業務システムや IT サービス等の商品の調達・製造からサービスが利用者に届くまでの一連の流れのこと。

セージ、通話音声、動画配信等を管理するサーバについては、重要度が高い個人データを管理する情報システムであると認識し、当委員会が行った令和３年の指導を踏まえた再発防止策として、かかるサーバへのアクセスには ID・パスワードに加え、事前登録されたスマートフォンの所持確認を行うことによる多要素認証を導入していた。

他方、本件で不正アクセスがなされたデータ分析システム等については、LINE のユーザー情報が保管されているにもかかわらず、ID・パスワードのみでの認証方式を採用していた。仮に、データ分析システム等へのアクセスについて、攻撃者が LY 社の従業者になりすましたログインを防止するような強度の高い認証方式を導入していれば、攻撃者が前記第２の３⑵及び⑶の不正アクセスで漏えいした従業者情報（LY 社従業者の ID・パスワードを含む。）を利用したとしても、さらなる侵入には至らなかった可能性がある。

第４　旧Ｌ社に対して当委員会が行った令和３年の指導について

１　事案の概要

令和３年３月、LY 社の前身である旧 L 社がシステム開発を再委託していた中国の子会社 Shanghai LINE Digital Technology Limited において、LINE ユーザーに関する個人情報に、エンジニア４名が計 35 回のアクセスを行っていた事実関係が認められた。この事案について、当委員会は、令和３年４月 23 日、旧 L 社に対し、個人情報保護法第 41 条[10]に基づき、委託先における個人データの取扱いに関して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適切な監督等を実施するよう指導を行った（以下「令和３年行政指導」という。）。

２　指導に対する旧Ｌ社の対応

旧 L 社は、令和３年行政指導に対して、委託先の監督及びアクセス管理の強化のため、以下の再発防止策を講ずることとした。

⑴　委託先の個人データへのアクセス権限を業務上必要な範囲に限定するよう、アクセス権限付与を見直す。

⑵　個人データの取扱いを委託する委託先企業に対して、年に１回の監査を実施することとする。

⑶　重要度の高い個人データにアクセス可能な権限のログインには多要素認証を導入する。

---

[10] 個人情報の保護に関する法律等の一部を改正する法律（令和２年法律第 44 号）による個人情報保護法の改正前の条文番号。

３　本件事案との関連性

⑴　委託先の監督について

旧Ｌ社及びLY社は、前記２⑴及び⑵に従い、個人データの取扱いがある委託先を監督していたが、本件において、LY社は、NC社及びA社に対し、本件個人データの取扱いを委託していなかったため、NC社及びA社は個人データの取扱いがある委託先として管理されておらず、定期的な実地監査等の委託先に対する監督は行っていなかった。

⑵　多要素認証の導入について

旧Ｌ社は、令和４年４月～７月、外部と接続するシステム（VPN機器等）とLINEメッセージ等の秘匿性の高い個人データにアクセス可能なシステム（LINEメッセージにおける迷惑行為等の利用者情報があった際に対応するモニタリングツール等）について、他システムより優先して多要素認証を導入した。しかし、前記第３の２のとおり、本件個人データのうちユーザーに関する個人データが管理されていたデータ分析システム等については、多要素認証導入の検討もされないまま、未導入のままとなった。

第５　個人情報保護法上の問題点

１　技術的安全管理措置の不備

ガイドラインにおいて、個人情報取扱事業者は、担当者及び取り扱う個人情報データベース等の範囲を限定するために、適切なアクセス制御を行わなければならないと規定されている（10-6⑴アクセス制御）。

本件の攻撃者によるNC社のデータセンターからLY社のデータセンターへの接続方法は、通常の業務として想定されている接続方法とは異なるものであったにもかかわらず、NC社とLY社のネットワーク間において導入・運用している侵入検知システムは、本件の攻撃者による不正アクセスを防止及び検知することができなかった。これは、LY社が、NC社に対し、前記第３の１のとおりLY社のネットワーク及び社内システムへの広範なアクセスを許容していたにもかかわらず、サーバ、ネットワーク及び社内システムを保護するための十分な措置を講じておらず、特定のポートに係る通信をブロックするのみで、それ以外の通信は広く許容されていたことが一因であったものと認められる。

LY社が、このような広範なネットワーク接続によるリスクを理解し、NC社のシステムや端末からLY社のネットワークやシステムに関して、真に必要な通信のみを許容し、その他のアクセスを認めない仕組み等の措置をとっていれば、不正アクセスを防止又は検知できた可能性がある。

以上から、LY 社においては、技術的安全管理措置（アクセス制御）に不備が認められる。

２　組織的安全管理措置の不備

LY 社においては、以下のとおり、組織的安全管理措置に不備が認められる。

⑴　個人データの取扱状況の把握及び安全管理措置の評価、見直し及び改善について

ガイドラインにおいて、個人情報取扱事業者は、個人データの取扱状況を把握し、安全管理措置の評価、見直し及び改善に取り組まなければならないと規定されている（10-3⑸ 取扱状況の把握及び安全管理措置の見直し）。

しかしながら、LY 社においては、個人データの取扱状況の把握及び安全管理措置の評価、見直し及び改善について、以下のような問題点が認められる。

ア　NC 社との関係に応じたリスク管理に関する問題点

LINE は、2011 年に NHN Japan 株式会社（現 NAVER CORP. の日本法人、以下「NHN Japan」という。）が開始したサービスである。NHN Japan は、2013 年にウェブサービス事業とゲーム事業を分割し、ウェブサービス事業は NHN Japan から商号変更した旧 L 社が引き続き運営した。旧 L 社は、当時親会社であった、NAVER CORP. や、NAVER CORP. の子会社等、NAVER グループから技術面及びインフラ面の支援を受けながら事業運営を行ってきた。そのような沿革から、LY 社は、今回不正アクセスを受けたシステムを含む複数の重要なシステムについても、サーバやソフトウェア等のインフラの構築及び運営業務を NC 社に任せ、NAVER グループと共同利用する共通認証基盤システムや NC 社が提供するシステムの利用を続けてきた。

個人情報取扱事業者は、個人情報保護法第 23 条及びガイドライン「10　（別添）講ずべき安全管理措置」に例示される具体的な措置に従い、取り扱う個人データの性質及び量やそのリスクに応じて、必要かつ適切な措置を自ら判断し、個人データを管理する情報システムやネットワーク構成を構築し、又は業務委託先等に構築させなければならない。

しかしながら、LY 社は、個人データの取扱いに関し、自らの判断でガイドラインに則した安全管理措置を講じなければならないところ、旧 L 社の沿革に起因する NC 社との共通認証基盤システムや NC 社との広範なネットワーク接続を許容するネットワーク構成の利用を継続してきた。また、LY 社は、NC 社に対して本件個人データの取扱いの委託は行っていないと整理していたため、実際に NC 社に対して自らの安全管理措置と同等の措置が講じられるよう監督を行うことはなく、結果として、NC 社に業務委託し構築させたシステムが侵入経路及び漏えい原因となり、本件個人データが漏えいした。

すなわち、LY 社は、その安全管理のために必要かつ適切な措置を講ずる責任の所在と手段の検討及び把握が曖昧なまま、ユーザーの個人データを含む大量の個

人データを取り扱っていたものである。

LY 社は、このようなリスクや課題を認識すべきであったにもかかわらず、共通認証基盤システムの共同利用や、NC 社に対する重要なシステムの構築及び運営の業務委託を継続してきたものであり、個人データの取扱状況の把握及び安全管理措置の評価、見直し及び改善に問題があると言わざるを得ない。

イ　令和３年行政指導後の対応に関する問題点

前記第４の２⑶のとおり、委託先における個人データの取扱いに関して適切な監督等を実施するよう求めた令和３年行政指導に対し、LY 社は、再発防止策の一つとして、重要度の高い個人データにアクセス可能な権限のログインには多要素認証を導入するとしたが、本件事案で不正アクセスを受けたデータ分析システム等において保管されているユーザーの情報の機微性が、他のシステムと比較して相対的に低いと判断し、多要素認証の導入を見送ってきた[11]。

しかしながら、本件個人データのうち、データ分析システムに保管されている個人データは、ユーザーの LINE 各種サービス（メッセージへのリアクションやスタンプ購入等）の利用履歴に関する個人データであるところ、これらのサービス利用履歴は、個人の行動範囲、経済状況、趣味・嗜好等のプライバシーに関するデータであり、本人の権利利益の保護の観点からは、機微性の低い情報と分類することはできない。

そもそも、LY 社においては、①NC 社との共通認証基盤システムの利用及び②NC 社との広範なネットワーク接続という点において、安全管理措置に関わる特殊性が存在していたものであるから、これらに起因するリスクを適切に評価し、ユーザーのサービス利用履歴等の個人データについても、多要素認証導入を積極的に判断するべきであった。

以上から、LY 社においては、令和３年行政指導後の安全管理措置の評価、見直し及び改善が十分ではなかったものと認められる。

なお、令和５年 10 月１日の旧Ｌ社と旧ヤフー社の経営統合に当たり、旧ヤフー社における管理規程では、多要素認証機能を設けることを定めていたことから、経営統合後は、旧ヤフー社の規程に準拠し、多要素認証を基本とすることとした。LY 社においては、経営統合前後にこれらの規程を見直すに当たって、本件個人データについても多要素認証の導入等の安全管理措置を見直し、改善する機会があったにも関わらず、速やかな実施に至らなかった点についても問題が認められる。

---

[11] LY 社によると、令和３年行政指導を踏まえ、多要素認証を導入するシステムを選定した基準及び導入しないと決定したシステムに対するリスク評価について、経営陣が関与した意思決定のプロセス及び証跡が残っておらず、不正アクセスを受けたデータ分析システム等に対して、多要素認証を導入する計画はなかったとされる。

⑵　漏えい等事案に対応する体制の整備について

ガイドラインにおいて、個人情報取扱事業者は、漏えい等事案の発生又は兆候を把握した場合に適切かつ迅速に対応するための体制を整備しなければならないと規定されている（10-3⑷ 漏えい等事案に対応する体制の整備）。

本件では、不正アクセスの原因や侵害範囲等の全容を明らかにするに当たっては、A社PC及びサーバを調査し、また、NC社に構築及び運営を業務委託するシステムのアクセスログを調査する必要があった。

しかしながら、LY 社は、自らの判断でガイドラインに則した安全管理措置を講じなければならず、漏えい等事案の発生時には事実関係の調査及び原因の究明が実施できるような体制を整備すべきであるところ、事実関係の調査及び原因の究明については、NC社やNAVERグループに頼らざるを得ない状況であり、LY社が本件事案の全容を把握するために約３か月半という時間を要した。

このように、LY 社は、自社の漏えい等事態に関する事実関係の調査及び原因の究明が速やかになされなかったものであり、漏えい等事案に対応する体制の整備の観点からも不備が認められる。

⑶　組織体制の整備等について

ガイドラインにおいて、個人情報取扱事業者は、個人データの取扱いに関する責任者の責任の明確化などを含めた安全管理措置を講ずるための組織体制を整備しなければならないと規定されている（10-3⑴ 組織体制の整備）。

しかしながら、LY社においては、旧L社に対する令和３年行政指導後も、他社との広範なネットワーク接続を継続しているにもかかわらず、前記のとおり、アクセス制御等の技術的安全管理措置が講じられていなかったこと、個人データの取扱状況の把握及び安全管理措置の評価、見直し及び改善に問題が認められること、漏えい等事案への対応を速やかに行うことができなかったことから、その組織体制が必ずしも十分に機能していたとは言い難い。

令和５年10月に経営統合が行われ、事業規模が拡大し、今後とも、大量かつ重要度の高い個人データの取扱いが想定されるところ、その取扱いに万全を期すために、個人データの取扱いに関する責任者（DPO等）が中心となって、安全管理措置が徹底される組織体制を整備し、その実効性のある運用の確保に注力すべきである。

第６　当委員会の対応

１　事案の重大性について

本件事案は、約9,600万人もの日本のユーザーを抱えるLINEにおいて、約52万人分の個人データが不正アクセスにより漏えいした事案である。

また、漏えいした個人データの中には、ユーザーのLINE各種サービス（メッセージ

へのリアクションやスタンプ購入等）の利用履歴に関する個人データが含まれており、これらのサービス利用履歴は、マーケティング等の経済活動において有用性が高い一方、個人の行動範囲、経済状況、趣味・嗜好等のプライバシーに関するデータであるため、不適正に取り扱われた場合、本人の権利利益に対する重大な侵害につながるリスクがある。

このような本件事案の重大性、影響を受けた個人データ等の性質及び量を考慮した上で、適切な権限行使を行う必要がある。

２　勧告（個人情報保護法第 148 条第１項）

⑴　前記第５の２⑴のとおり、LY 社は、個人データの取扱いに関し、自らの判断でガイドラインに則した安全管理措置を講じなければならないところ、NC 社との共通認証基盤システムやNC 社との広範なネットワーク接続を許容するネットワーク構成の利用を継続し、令和３年行政指導後も、本件個人データについて、その安全管理のために必要かつ適切な措置を講ずる責任の所在と手段の検討及び把握が曖昧なまま、ユーザー情報を含む大量の個人データを取り扱っていた。

LY 社は、このようなリスクや課題を認識すべきであったにもかかわらず、共通認証基盤システムの共同利用や、NC 社に対する重要なシステムの構築及び運営の業務委託を継続してきたものであり、個人データの取扱状況の把握及び安全管理措置の評価、見直し及び改善に問題があり、組織的安全管理措置の不備が認められる。

⑵　また、LY 社は、技術的安全管理措置（アクセス制御）の不備について、本件事案発生後、NC 社と LY 社間のネットワーク接続にファイアウォールを導入するとともに、ACL（アクセスコントロールリスト）の適用により、必要なアクセスのみを許可するという一定の措置を講ずることとしている。

しかしながら、本件において、侵入検知システムが不十分であり、適切なアクセス制御がなされていなかった点は、LY 社が NC 社との間で、従業者アカウントの認証情報を、共通認証基盤システムや情報の同期を認めるシステム構成によって共有しており、NC 社に対し、LY 社のネットワーク及び社内システムへの広範なアクセスを許容していたという組織的安全管理措置の不備に起因するものである。

⑶　LY 社は､NC 社とのシステム及びネットワークの分離を目指しているものの､現状、根本的な対策については時間を要するとしている。令和３年行政指導後に再び本件漏えい等事案が発生し、また、LY 社が多数のユーザーを含む個人データの取扱いを今後も継続していくことからすると、この状態を放置しておくことは、個人の権利利益を侵害するおそれが高い。

⑷　以上から、個人情報保護法第 148 条第１項の規定により、同法第 23 条の規定違反（組織的安全管理措置の不備）を是正するために必要な措置として、NC 社との共通認証基盤システムの利用、NC 社との広範なネットワーク接続を許容するネットワー

ク構成及び重要度の高い個人データを保管する情報システムに対するアクセス者の識別と認証の方式に関するリスクや課題を適切に把握するために、安全管理措置が徹底される組織体制を整備し、また、漏えい等事案に対応する体制の整備並びに安全管理措置の評価、見直し及び改善を行うよう勧告する。

３　報告等の求め（個人情報保護法第 146 条第１項）

LY 社に対し、個人情報保護法第 146 条第１項の規定により、再発防止策の実施状況を含む前記２の勧告に対する改善状況について、令和６年４月 26 日（金）までに初回の報告を求め、以降、同年６月 28 日（金）、同年９月 30 日（月）、同年 12 月 27 日（金）及び令和７年３月 31 日（月）までに報告等を求める。

以　上