基礎研レポート

LINE ヤフーの個人情報流出事案

不正アクセスに対する体制整備はどうだったか

保険研究部 専務取締役 研究理事　松澤　登
(03)3512-1866　matuzawa@nli-research.co.jp

1――はじめに

LINE ヤフー株式会社（以下、LY 社）は、ポータルサイト Yahoo!の運営やコミュニケーションアプリである LINE を運営する会社であることは比較的知られていると思われる。ただ、現在の LY 社の形になるまで、TOB や株式交換などが行われており、また、LY 社には多数の子会社・関連会社があるなど企業形態としては複雑である。その LY 社がサイバー攻撃を受け、2023 年 9 月 14 日～10 月 27 日にかけて個人情報が漏えいしたことが同年 10 月 27 日に判明した。

この事案を受け、2024 年 3 月 5 日付で総務省は LINE ヤフー株式会社（以下、LY 社）に対して、通信の秘密の保護及びサイバーセキュリティの確保の徹底を求める行政指導を行った[1]。これは LY 社がサイバー攻撃を受け、各種情報をハッキングされたことに対して、管理態勢が不十分として、改善を指導するとともに、改善の状況の報告を求めたものである。これに対して、LY 社は 4 月 1 日に総務省に対して報告[2]を行ったところ、同月 16 日、総務省は LY 社の対応が不十分として再度指導を行った[3]。

また、あわせて個人情報保護委員会も 2024 年 3 月 28 日に個人情報の保護に関する法律に基づく勧告を行った[4]。

本稿ではこの間の状況や動きなどを解説するものである。本事案では事実関係が複雑なこともあり、かいつまんで解説を行いたい。

ちなみに総務省等は今回の事案に直接関係していないことながら、個人情報保護が不十分となる背景となる部分（＝資本関係）について強い指導を行っているところが特筆される。

---

1 総務省 https://www.soumu.go.jp/main_content/000932387.pdf　参照。
2 LINE ヤフー株式会社　https://www.lycorp.co.jp/ja/news/2024/20240401_appendix_ja.pdf　参照。
3 総務省 https://www.soumu.go.jp/main_content/000942792.pdf　参照。
4 個人情報保護委員会 https://www.ppc.go.jp/files/pdf/240328_houdou.pdf　参照。

| Copyright ©2024 NLI Research Institute All rights reserved

2――発生した事案

1｜LY 社の業務委託関係

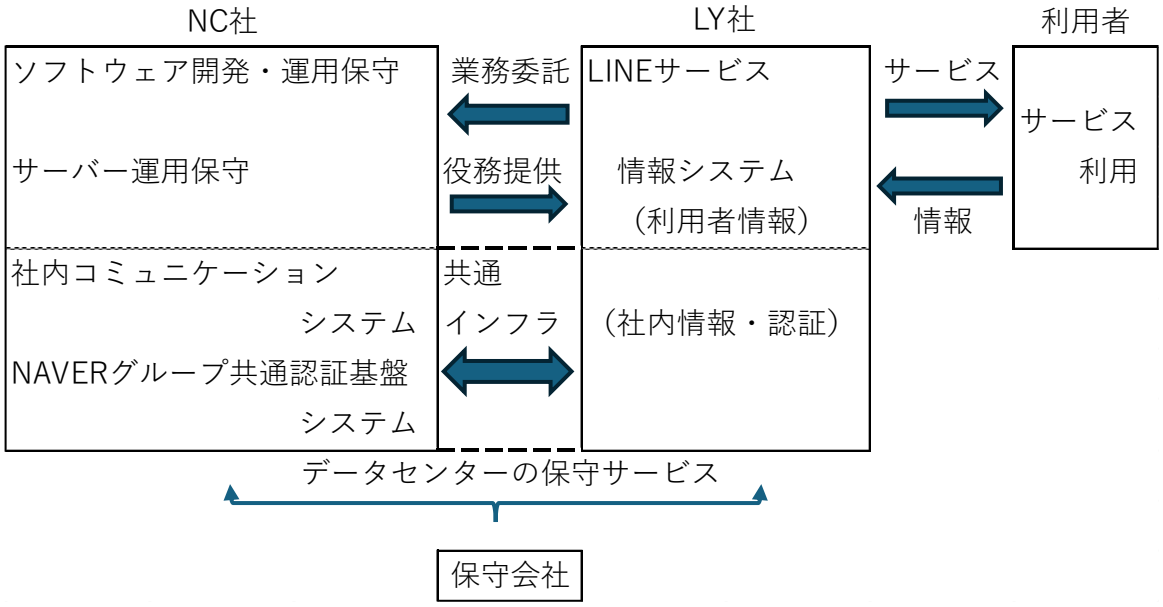
今回の事案を理解するには LY 社の業務委託関係を整理する必要がある。まず、LY 社のうち LINE 事業は韓国 NAVER 社の日本法人である NHN Japan 社が 2011 年 6 月にサービスを提供開始したものであり、NAVER 社と業務上の関係が近い。

LY 社は NAVER 社のグループ会社（以下、NAVER 社も含め、あわせて N 社側という）である NAVER Cloud（以下、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[5]。同契約に基づいて、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ている。これとは別に、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[6]。 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は行っていない。

また、韓国企業である保守会社（以下、保守会社）は LY 社と NC 社の双方からセキュリティに係るメインテナンス業務委託契約を受託し、双方のデータセンターのウイルス対策管理サーバにアクセスすることができた[7]。

これを図示すると概ね図表 1 の通りである。

【図表 1】LY 社と NC 社と保守の委託・受託関係



2｜攻撃者による NC 社･LY 社への侵入

(1)2023 年 8 月 10 日、同月 24 日、保守会社の PC がマルウェア攻撃を受け、攻撃者は保守会社の PC を遠隔操作することができる状態となった。

---

[5] 前掲注 3　p3 参照。
[6] 前掲注 4　p 3 参照
[7] 前掲注 3　p 3 参照。

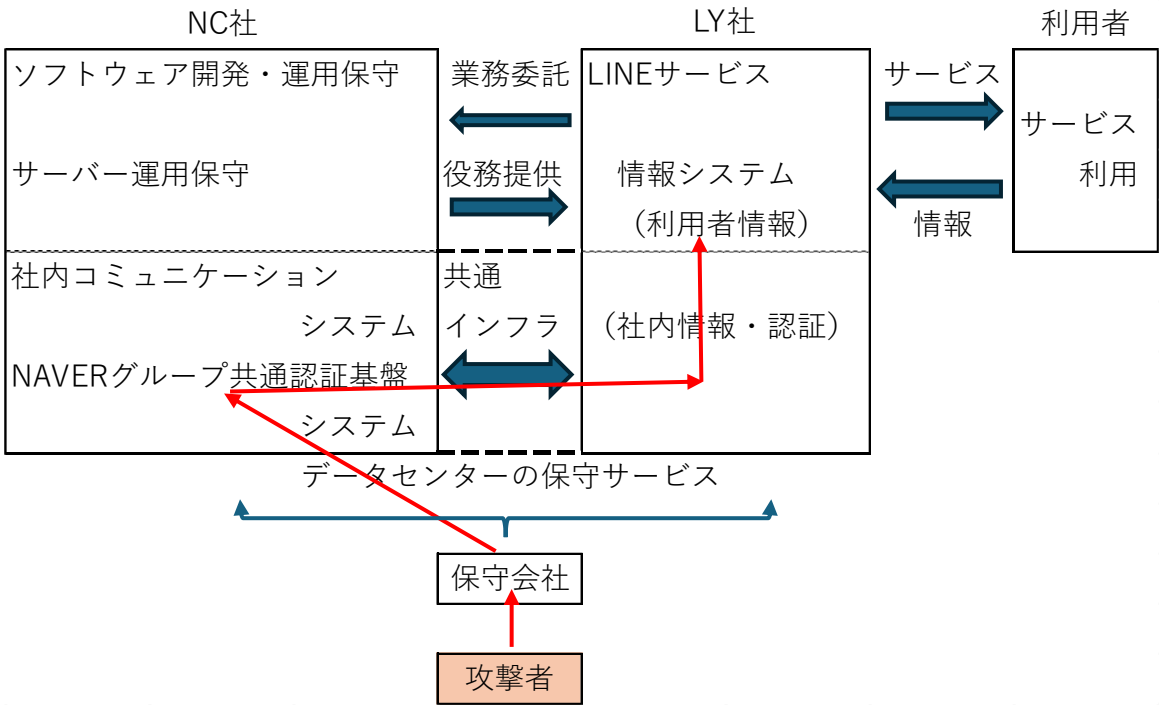
Copyright ©2024 NLI Research Institute All rights reserved

(2)同年 9 月 14 日、保守会社が NC 社データセンターの定期点検作業のため NC 社の管理者 PC にリモート接続したところ、攻撃者は遠隔操作手法を用いて、NC 社管理者 PC および 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。

(3)攻撃者は、2023 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た。そして、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・パスワードを不正に入手した。

(4) 攻撃者は、2023 年 9 月 14 日、前記(2)のとおり取得した LY 社の従業員の ID・パスワードを利用して、LY 社の従業員が利用する認証基盤システムへ不正アクセスしたうえで、さらに 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（図表 2)。

【図表 2】攻撃者の侵入経路（赤の矢印）



3｜攻撃者による LY 社データの窃取

2023 年 9 月 14 日以降、10 月 27 日まで、攻撃者は、上述のとおり入手した LY 社の従業者の ID・パスワードを用いて、各種システムへ不正アクセスし、LINE 利用者の個人データ、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。

3――総務省からの指導事項(3 月 5 日付)

1｜事案発生の要因

総務省によれば不正アクセスを許した事案発生の原因として以下の 4 点が挙げられている。

(1) システムやネットワーク構成等に係る N 社側への強い依存（図表 3 の A）

LY 社はその設立経緯から NC 社のプラットフォームを利用してきている。LY 社と NC 社のシステムは同期もしていた。LY 社は NC 社に委託業務を行わせるために、旧 LINE 社環境に広範なアクセスを許容してきた。また従業員アカウントの認証基盤についても共通化されており、旧 LINE 従業員のパスワードが NC 社の従業員管理システムにて管理・保全されてきた。

(2) 不十分な技術的安全管理措置（図表 3 の B）

上記(1)の通り、NC 社から LY 社のネットワークに対して特定のポートに係る通信を除いて広くアクセスが許容されており、厳格なアクセス制御がなされていなかった。また重要な社内システムへのログインにあたって多要素認証等が求められていなかったこと、不正を検知するための適切な仕組みも導入されていなかったこと等、様々な技術的不備が存在した。

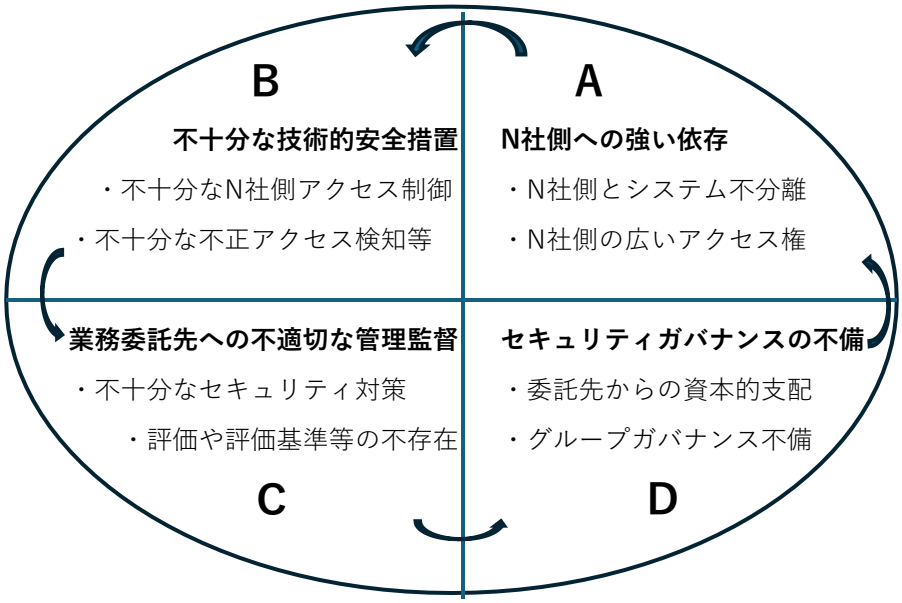
(3) 業務委託先の不適切な管理監督（図表 3 の C）

攻撃は業務委託先である保守会社および NC 社経由でなされたところ、このような事態を防ぐための安全管理措置・サイバーセキュリティ対策を保守会社および NC 社は行っていなかった。また契約上も定期的な評価や一定基準遵守の規定がなく、適切な管理監督がなされていなかった。

(4) セキュリティガバナンスの不備（図表 3 の D）

旧 LINE 社の社内ネットワークやシステム権限が N 社側の大きな技術的支援を受けて、複雑に形成され、現在でも保守運用を N 社側に頼らざるを得ないという関係が存在している。また、資本関係からは LY 社の親会社の株式の半数を N 社側が保有しているなど、LY 社は N 社側から資本的支配を受ける関係にある。以上を図示すると図表 3 の通りである。

【図表 3】LY 社における問題点（総務省指摘事項による）



これを見ると、総務省は LY 社の N 社側への強い依存が事案の背景あると考えていることがわかる。すなわち、LY 社の LINE にかかわるシステムが N 社側のものをベースとして作られており、システム

管理全般をN社側に頼らざるを得なかった。そのため、LY社自身が自社のためのセキュリティ対策をとることができず（あるいは行わず）、N社側だよりになっていたことがある。しかも、N社側はLY社に対して資本関係で優位に立ち、LY社がN社側に対してシステム監査・管理指導するという関係になかったことなども合わせ、本件事案につながったと考えているものと言える。

2｜総務省からの注意事項

LY 社の前身企業であり、本事案により不正アクセスを受けた各種サーバやシステム等を有する旧LINE社に対しては、総務省から2021年4月26日付けで社内システムに関する安全管理措置の一環としてアクセス管理の徹底等も含めて行政指導を行っていた(事案は下記枠内に記載)にもかかわらず、なおもアクセス管理の不備を一因とする本事案を招いたとの注意事項を総務省は指摘している。

上記指導は、2021年3月17日にLINE社が公表した事案で、LINEの再委託先企業であるLINE China（Shanghai LINE Digital Technology Limited. Dalian Branch）の従業員による、社内システムの1つであるモニタリング支援システムに対するアクセスのうち、特に通信の秘密又は個人情報に該当する可能性のある情報を含みうる LINE メッセンジャーに係るもの及び捜査機関対応業務従事者用システムに対するアクセスに関して行われたものである。この事案においては、LINE Chinaのエンジニア4名がLINE利用者の個人情報に計35回のアクセスを行っていた事実関係が認められた、

ただし、本事案においては、LINE社からの報告に基づく限りにおいては、通信の秘密の侵害又は個人情報の漏えい等があった旨は確認できなかった。

3｜指摘事項

本事案を受けて(1)安全管理措置・委託先管理の抜本的見直し、(2)グループ全体のセキュリティガバナンスの本質的見直し、(3)利用者対応の徹底、が総務省から指摘された。

以下では項を改めて、①総務省指摘事項、②LY社対応方針[8]、③総務省再指摘事項の順に記載する。なお、項目が多いため、ポイントとなる事項のみに絞って解説し、(3)については省略する。

4――総務省からの指導事項･LY社対応方針･総務省再指摘事項

1｜安全管理措置･委託先管理の抜本的見直し

①総務省指摘事項

ここでの総務省の指摘事項はN社側からのシステム分離を進めることやアクセス制限を適正化（上記図表3のAおよびB）すること、LY社自身の安全管理措置の適正化（同じくC）についての改善指導である。内容は以下の通りである。

ア）NC社を含むN社側からLY社システムへのアクセスは必要最小限のものとし、その他のアクセスを認めない措置を講じること

イ）共通化している認証基盤や情報の同期を認めるシステム構成を再評価し、特にNC社の認証基盤等

[8] 対応方針については概要のみしか公表されていない。

Copyright ©2024 NLI Research Institute All rights reserved

と LY 社の認証基盤等を技術面・運用面で完全に分離すること
ウ）SOC（セキュリティオペレーションセンター）の Tire1（ログを調査して疑わしい動きを探知する機能（または職員））は現在 NC 社にあるが、これを LY 社自身で運用すること
エ）ID とパスワードだけの認証方式ではなく、多要素認証の導入をすること
オ）リスクに応じた委託先管理手法を検討し、基準策定、実施を行うこと
カ）LY 社から NC 社に対して再発防止策が策定されるよう適切な管理監督を行うこと

②LY 社対応方針
ア）不必要な通信の遮断を 2024 年 3 月実施完了（ただし、下記イ）参照）
イ）N 社側および NC 社との認証基盤分離とシステム分離については、従業員向けシステムについては 2025 年 3 月末、国内子会社は 2026 年 3 月末、海外子会社 2026 年 12 月末完了予定。
ウ）SOC の Tire1 については 2024 年 10 月に LY 社へ移行予定
エ）重要システムに対して二要素認証の適用を 2024 年 3 月完了
オ）委託先管理手法の検討及び導入は完了。ただし、管理の実施はこれからであり、また自社における侵害の有無や範囲を把握するのは 2024 年 9 月予定
カ）NC 社への監督検討を定めた覚書の締結、本件関係委託先企業との契約解除を 2024 年 3 月完了

③総務省再指摘事項
評価できる点としてはエ)二要素認証の導入などである一方､委託先管理計画は策定されたものの、その実施についてはこれからである点などについて課題としている。特にイ）N 社側とのシステムが完全に分離されるのが 2 年先という点を問題点として指摘している。また明確性を欠く安全管理措置や委託先管理の計画については具体的な計画の早期提出を求めている。

2｜グループ全体のセキュリティガバナンスの本質的見直し
①総務省指摘事項
ここでの総務省の指摘事項はグループガバナンスの適正化についてであり、上記図表 3 の D に関するものである。内容は以下の通りである。
LY 社内におけるセキュリティガバナンス体制の抜本的な見直しや是正策の検討を行うことに加え、親会社等も含めたグループ内において、委託先への適切な管理・監督を機能させるための LY 社の経営体制の見直しや、適正な意思決定プロセスの構築等に向けた、適切な検討がなされるよう、親会社等に対しても必要な働き掛けを行うこと。

②LY 社対応方針
資本的な関係の見直しについて関係各社への見直しの要請を行い LY 社経営体制の見直しについて、同社指名報酬委員会での議論を開始した。また、N 社側への業務委託の縮小・終了の方針を決定した。

③総務省再指摘事項

Copyright ©2024 NLI Research Institute All rights reserved

総務省はN社側への委託関係の縮小・終了に焦点を当てている。まず、「N社側への委託」についての基本的な考え方と委託範囲について報告すること、縮小・終了の具体的な計画を策定し報告することを要請している。そのうえで、「委託先から資本的な支配を相当程度受ける関係の見直し等を含め」経営体制の見直しを行うことを要求している。

ここで総務省は資本関係について特に問題視をしていることは特筆に値する。今回の事案は資本関係と直接の関係がないが、LY社が委託先に十分な管理を行えなかった背景として、資本関係が重大な影響を及ぼしていると総務省は認識していることがわかる。

5――個人情報保護委員会による勧告

1｜個人情報保護委員会が指摘する情報保護法上の問題

個人情報保護委員会（以下、個情委）は技術的安全管理措置の不備、組織的安全措置の不備を指摘している[9]が、特に以下の点を問題視している。問題意識は総務省と大きくは異ならない。

・LY 社は、個人データの取扱いに関し、自らの判断で個人情報保護法および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 LINE 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。

・上述（p5）の2021年度の事案に対しては、個人情報保護委員会からの指導もなされたものの、、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。しかし、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。 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。

・LY社においては、旧LINE社に対する2021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。

[9] 前掲注4参照。

2｜委員会による勧告

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を勧告した。勧告内容として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ことを求めている。この勧告は 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のものである。

6――検討

1｜検討の視点

これまで総務省・個情委と LY 社とのやり取りを見てきたが、どこがどの程度の問題なのかがにわかにはわからない。そこで個人情報保護委員会が公表している個人情報保護ガイドライン（通則編）の 10（別添）講ずべき安全管理措置の内容を物差しとし、ガイドラインにそって事案を見ていきたい。ガイドラインの項目は以下の通りである。

10－1．基本方針の策定
10－2．個人データの取扱いに係る規律の整備
10－3．組織的安全管理措置 (1)組織体制の整備 (2)個人データの取扱いに係る規律に従った運用 (3)個人データの取扱状況を確認するための手段の整備 (4)漏洩等事案に対する体制の整備 (5)取り扱い状況の把握及び安全管理措置の見直し
10－4．人的安全措置
10－5．物理的安全管理措置 (1)個人データを取り扱う区域の管理 (2)機器及び電子媒体の盗難等の防止 (3)電子媒体を持ち運ぶ際の漏洩等の防止 (4)個人データの削除及び機器、電子媒体の廃棄
10－6．技術的安全管理措置 (1)アクセス制御 (2)アクセス者の識別と認証 (3)外部からの不正アクセス等の防止 (4)情報システムの使用に伴う漏洩の防止
10－7．外部環境の把握

Copyright ©2024 NLI Research Institute All rights reserved

2｜LY 社の問題点

ガイドラインに照らした LY 社の個別の問題点は以下の通りである。

(1)ガイドライン 10－3(1)（組織体制の整備）によれば、「個人データの取扱いに関する責任者と責任の明確化」や「個人データを複数の部署で取り扱う場合の各部署の役割分担及び責任の明確化」が求められている。

この点、LY 社はシステムのセキュリティ管理を業務委託先である NC 社とセキュリティメンテナンス業務を委託した保守会社に委託していると総務省が指摘している[10]。そして個情委によれば LY 社にデータ責任所管があったとされるが、個情委からはア）技術的安全措置が講じられていなかったこと、イ）安全管理措置の評価、見直し、改善に問題が認められること、漏洩等の事案に適切に対応できなかったことから「組織体制が必ずしも十分に機能していたとはいいがたい」[11]と認定されている。

これは LY 社が通信業者でありながら、通信の秘密を守るための責任を果たす体制を自社内に構築できていなかったということになる。

(2) ガイドライン 10―3 (1)（組織体制の整備）の別の解説では「個人データの漏洩等事案の発生又は兆候を把握した場合の責任者への報告連絡体制」を整備すべきとし、さらにガイドライン 10－3 (4)では「漏洩事案等に対応する体制の整備」が求められるとしている。

この点、本事案では漏洩が始まって発覚まで 1 カ月以上要した(9 月 14 日～10 月 27 日)うえ、事実関係の調査及び原因の究明については、LY 社は、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[12]と個情委に指摘されている。また、SOC の Tier1（上述、ログを調査して疑わしい動きを探知する機能（または職員））が LY 社でなく NC 社にあったことも加え、漏洩事案等に対する体制の整備がなされていなかったと言えよう。

(3)ガイドライン 10－5(1)は個人情報データベース等を取り扱うサーバやメインコンピュータ等の重要な情報システムを管理する区域（以下、管理区域という）及び（中略）について適切な管理を行わなければならないとある。

総務省によれば「N 社側の日本向けサービス提供用のネットワーク機器が貴社（LY 社）のデータセンター内に設置されており、同機器について NC 社から貴社のネットワークを介してアクセスがなされ、その保守管理が実施されていた」[13]との指摘がなされている。物理的には区分されていたとしても、技術的にアクセス可能となっていることは問題であろう。

(4) ガイドライン 10―6（技術的安全管理措置）(1)の解説の一つ目と二つ目では「個人情報データベースを取り扱うことのできる情報システムを限定する」および「情報システムによってアクセスでき

10 前掲注 1　p 1 参照。
11 前掲注 4　p 10 参照。
12 前掲注 4　p 10 参照。
13 前掲注 1　p 2 の注記参照。

Copyright ©2024 NLI Research Institute All rights reserved

ることのできる個人情報データベースを限定する」と記載されている。

この点に関しては、まずN社側及びLY社が共同で共通認証基盤システムを利用していたということが個情委および総務省から指摘されている[14]。このことは攻撃者にLY社の重要システムに不正アクセスを許してしまった原因になっている

共通の認識基盤に加えて、LY社はLINEのシステムの運用管理をNC社に委託していた。この委託に際し、総務省の指摘では必要最小限のアクセス権限だけではなく、より幅広いアクセス権限を認めていた[15]とのことである。これはアクセスできる個人情報データベースを制限するというガイドラインに抵触すると考えられる。

(5)ガイドライン10－6(1)の解説の三つ目は「ユーザーIDに付与するアクセス権により、個人情報データベース等を取り扱う情報システムを使用できる従業者を限定する」とあり、さらにガイドライン6(2)ではアクセス権の識別と認証として「ユーザーID、パスワード、磁気・ICカード等」と例を挙げている。

この点に関しては、LINEのアカウント情報やメッセージを管理するサーバについては、ID、パスワードのほか、登録されたスマートフォンがアクセスのために必要であったが、これと別のユーザー情報を含むデータ分析システムにはIDとパスワードだけアクセスすることができていたとのことである。LY社はデータ分析システムには機微情報が含まれていないとの判断[16]だったが、実際に不正アクセスによって個人データが流出しており、総務省は多要素による認証をデータ分析システムについても求め、既にLY社も対応したとしている。

3｜小括

以上の通り、個別事象として、ガイドライン10－3，10－5，10－6に抵触しており、従ってガイドライン10－1（基本方針の策定)、10－2（個人データの取扱いに係る規律の整備）が形骸化していたものとみるのが妥当だろう。ガイドラインのあらゆる点で十分な水準に達していなかったことが想定される。

7――おわりに

LINEは日本においてインフラ化している。個人間のコミュニケーションのみならず、飲食店の割引クーポンの配布、果ては行政手続のお知らせなどにも利用されている。通信事業者であるということだけではなく、あらゆる個人情報が集まるプラットフォームということができる。

そのようなLY社が親会社や兄弟会社にシステム運用を委託し、物理的にも、権限としてもシステムへのアクセスを過大に認めていたということである。LY社がこのような状況を認識しつつ、かつこれらの問題点について改善をN社側に言えなかったということであれば、企業体質という構造的な問題

14 前掲注１　p２および前掲注４　p３参照。
15 前掲注１　p２参照
16 前掲注４　p９参照。

Copyright ©2024 NLI Research Institute All rights reserved

となる。

総務省が親会社等との物理的関係だけでなく、資本関係についても分離を強く求めているのはこの点に問題意識があるのだろう。またこのように資本関係についてまで指導しているのは、これが上述ｐ５に記載した事案を含め二度目だということもあろう。直接的な原因とまでは言えない資本関係まで変更を要求するのは行き過ぎとの考えもあろうが、総務省の考えも理解できるところである。

引き続き日本のインフラであり続けるためには、LY 社の毅然たる対応が求められるところである。

 Copyright ©2024 NLI Research Institute All rights reserved