2022年6月29日

各　位

会　　社　　名　株式会社ニップン
代　表　者　名　代表取締役社長 前鶴 俊哉
（コード番号　2001　東証プライム）
問　合　せ　先　広報部長 福山 幸一郎
（Tel　(03)3511-5307）

内部統制報告書の訂正報告書の提出に関するお知らせ

当社は、金融商品取引法第２４条の４の５第１項に基づき、本日、内部統制報告書の訂正報告書を関東財務局に提出いたしましたので、下記のとおりお知らせいたします。

記

１．訂正の対象となる内部統制報告書
第１９７期　　（自 2020年4月1日　　至 2021年3月31日）

２．訂正の内容
上記の各内部統制報告書の記載事項のうち、3【評価結果に関する事項】を以下のとおり訂正いたします。訂正箇所には＿＿を付しております。

3【評価結果に関する事項】
（訂正前）
上記の評価の結果、2021年3月31日現在の当社グループの財務報告に係る内部統制は有効であると判断いたしました。

（訂正後）
下記に記載した財務報告に係る内部統制の不備は、財務報告に重要な影響を及ぼす可能性が高く、開示すべき重要な不備に該当すると判断いたしました。従って、当事業年度末日において、当社グループの財務報告に係る内部統制は有効でないと判断いたしました。

記

2021年7月7日に子会社のニップンビジネスシステム株式会社において管理運用する当社グループの情報ネットワークが、外部からのサイバー攻撃を受け、大部分のサーバーが同時多発的に全部又は一部を暗号化されたことにより、システム障

害が発生しました。

サイバー攻撃を受け、システム障害が発生した根本原因について、当社代表取締役の指揮の下に外部の専門家を含めて根本原因調査を実施した結果、サイバーセキュリティに係るシステムの技術的な脆弱性対応が十分にできていなかったという事実の指摘がなされるとともに、その事実の背景にある組織や内部統制の課題として、サイバーセキュリティに関するポリシー群が不十分であったこと、サイバーセキュリティ管理体制における明確な指示系統・責任体制の曖昧さ、ＩＴ・サイバーセキュリティに関する経営層のリーダーシップに基づく管理体制や経営資源（人材、投資等）の確保が不十分だったこと、の３件が指摘されました。

これは、ランサムウェアによるサイバー攻撃の被害が経済界で顕著になり、2020年12月18日の経済産業省によるサイバーセキュリティの取組の強化に関する注意喚起の発出を受けて各企業が予見されるリスクとしてサイバー攻撃を認識し、セキュリティ強化へ一斉に取り組み始めるなど、サイバーセキュリティリスクの高まりの中で、当社においてはサイバーセキュリティリスクを認識していたものの、その対応強化が遅れることとなりました。

結果として、サイバーセキュリティに関するリスクの評価が不十分であったことから、ＩＴ投資予算の不足、専門性を備えた人材の不足等により、要因別の詳細な分析及び対応方針の策定が行われず、システムへの侵入を許し、四半期報告書の法定提出期限までに財務諸表の公表ができない状況が生じたという重大な事実を踏まえると、サイバー攻撃による被害を受けた 2021 年７月７日以前において、サイバーセキュリティに関する全社的な内部統制（リスクの評価と対応）について、重要な不備があったと評価しました。

このため、予見されるリスクとしてサイバーセキュリティリスクへの対応を強化すべきであった 2021 年３月末時点の当社の財務報告に関する内部統制は有効ではなく、開示すべき重要な不備が存在すると評価いたしました。

当該重要な不備が、当事業年度の末日までに是正されなかった理由は、当該重要な不備が当事業年度末日後に発覚したためであります。

なお、財務報告データシステムは強固にセキュリティ対策等が過去から図られＩＴ全般統制は継続して有効と評価しており、財務データシステムそのものへの侵入は阻止できた結果、財務データの改ざんはなく財務報告に金額的あるいは質的に重要な虚偽記載につながる事実はありませんでした。

また、当社は、財務報告に係る内部統制の整備及び運用の重要性は充分に認識しており、根本原因の調査結果を真摯に受け止め、再発防止及び改善策を策定し、必要な措置を内部統制評価の基準日である 2022 年３月 31 日までに実施いたしました。従って、当社の 2022 年３月末時点における全社統制（リスク評価と対応）に

ついては、適正に整備・運用されており、重要な不備は改善されていると評価しております。当社が実施した改善策の概要は以下のとおりです。

・システムの脆弱性の改善（パッチ適用、バックアップ体制の整備、ファイアーウォール設置等）

・サイバーセキュリティに関するポリシーの基本体系の整備・運用

・サイバーセキュリティ対策における責任と権限が明確化され、運用面における業務内容の可視化・共有化が進み、属人化を防ぎ、ＩＴ戦略に関する他部門との調整や具体的対応をつつがなく行うことができる体制の整備・運用

・経営層のサイバーセキュリティに対する意識向上を図り、ＩＴに係る経営戦略（人材確保・投資を含む予算措置など）や適切なリスク評価が行われる体制の整備・運用

以上