【表紙】

【提出書類】	内部統制報告書
【根拠条文】	金融商品取引法第24条の４の４第１項
【提出先】	関東財務局長
【提出日】	2024年７月25日
【会社名】	日東製網株式会社
【英訳名】	NITTO SEIMO CO.,LTD.
【代表者の役職氏名】	取締役社長　小　林　宏　明
【最高財務責任者の役職氏名】	該当事項はありません。
【本店の所在の場所】	東京都港区新橋二丁目20番15-701号
【縦覧に供する場所】	株式会社東京証券取引所 （東京都中央区日本橋兜町２番１号） 株式会社名古屋証券取引所 （名古屋市中区栄町三丁目８番20号）

1 【財務報告に係る内部統制の基本的枠組みに関する事項】

当社取締役社長小林宏明は、当社並びに連結子会社及び持分法適用会社（以下「当社グループ」）の財務報告に係る内部統制の整備及び運用に責任を有しており、「財務報告に係る内部統制の評価及び監査の基準並びに財務報告に係る内部統制の評価及び監査に関する実施基準の設定について（意見書）」（企業会計審議会 平成19年２月15日）に準拠して財務報告に係る内部統制を整備及び運用しております。

なお、財務報告に係る内部統制は、内部統制の各基本的要素が有機的に結びつき、一体となって機能することで、その目的を合理的な範囲で達成しようとするものであります。このため、財務報告に係る内部統制により財務報告の虚偽の記載を完全には防止又は発見することができない可能性があります。

2 【評価の範囲、基準日及び評価手続に関する事項】

当社グループの財務報告に係る内部統制の評価は、当連結会計年度の末日である2024年４月30日を基準日として行われており、評価に当たっては、一般に公正妥当と認められる財務報告に係る内部統制の評価の基準に準拠して実施いたしました。

本評価においては、連結ベースでの財務報告全体に重要な影響を及ぼす内部統制（全社的な内部統制）の評価を行った上で、その結果を踏まえて、評価対象とする業務プロセスを選定しております。当該業務プロセスの評価においては、選定された業務プロセスを分析した上で、財務報告の信頼性に重要な影響を及ぼす統制上の要点を識別し、関連文書の閲覧、当該内部統制に関係する適切な担当者への質問、業務の視察、内部統制の実施記録の検証等の手続を実施することにより、当該統制上の要点について整備及び運用状況を評価することによって、内部統制の有効性に関する評価を行いました。

財務報告に係る内部統制の評価の範囲については、当社並びに連結子会社11社及び持分法適用会社１社について、財務報告の信頼性に及ぼす影響の重要性の観点から必要な範囲を決定いたしました。財務報告の信頼性に及ぼす影響の重要性は、金額的及び質的影響の重要性を考慮して決定しており、当社及び連結子会社２社を対象として行った全社的な内部統制の評価結果を踏まえ、業務プロセスに係る内部統制の評価範囲を合理的に決定いたしました。なお、連結子会社である多久製網㈱、タイ・ニットウセイモウ・グローバル Co.,Ltd.、日東ネット㈱、日本ターニング㈱、㈱温泉津定置、ＣＮＫ㈱、㈲吉田漁業部、㈱庄司政吉商店及びヤマグチ㈱と、持分法適用会社であるレデス・ニットー・ペルーS.A.C.については金額的及び質的重要性の観点から僅少であると判断し、全社的な内部統制の評価範囲に含めていません。

業務プロセスに係る内部統制の評価範囲については、各事業拠点の前連結会計年度の売上高（連結会社間取引消去後）の金額が高い拠点から合算していき、前連結会計年度の連結売上高の概ね３分の２程度の割合に達している１事業拠点を対象としております。

対象とした重要な事業拠点においては、企業の事業目的に大きく関わる勘定科目として、売上高、売掛金及び棚卸資産に至る業務プロセスを評価の対象としました。さらに、選定した重要な事業拠点にかかわらず、それ以外の事業拠点をも含めた範囲について、重要な虚偽記載の発生可能性が高く、見積りや予測を伴う重要な勘定科目に係る業務プロセスやリスクが大きい取引を行っている事業又は業務に係る業務プロセスを財務報告への影響を勘案して重要性の大きい業務プロセスとして評価対象に追加しております。

3 【評価結果に関する事項】

上記の評価の結果、当社取締役社長小林宏明は2024年４月30日現在における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。

4 【付記事項】

該当事項はありません。

5 【特記事項】

（当社グループの情報ネットワークがサイバー攻撃を受けシステム障害が発生した問題について）

（１）サイバー攻撃によるシステム障害の発生

2024年１月16日(火)午前８時頃、外部から不正アクセスを受けサーバーに保存している各種ファイルが暗号化されていること等を確認いたしました。直ちにシステム会社とともに調査を行い、社内ネットワーク及びインターネット回線を切断し、システムを停止させ全てのパソコンを使用不可としました。翌１月17日(水)には、「全社対策本部」を設置し情報管理系統を一本化するとともに警察へも現状報告し、捜査に協力することや情報提供等の協力依頼を行いました。

その後、システム会社・専門家等の協力を得ながら、全PCのパスワードのリセット及びウィルスチェックを実施しインターネット接続を再開。保存データの正常な復旧状況を確認しながら、各種重要システムを順次再開して参りました。その結果、２月13日(火)には、ほぼ全ての業務が正常化するに至りました。

（２）本件インシデントの発生原因と影響について

本件インシデントの発生原因につきましては、攻撃者が弊社のVPN機器の脆弱性から認証突破してネットワーク内に侵入し、ランサムウェアを実行したものと思われます。

また、本件発生により、約１ヶ月間各種業務データ、業務用ソフトウェアにアクセスできなかったことから、2024年4月期第3四半期報告書の提出期限を、2024年３月18日(月)から2024年４月10日(水)と延長せざるを得ませんでした。

情報の流出につきましては、現時点におきましても、大規模なデータ移動は認められておらず、不審な通信先も認識されていないことから、情報漏えいはないものと考えておりますが、引き続き調査を進めております。

（３）今後の再発防止策、内部管理体制について

今後の再発防止策として、下記項目を速やかに実施いたします（一部は実施済）。

① 全てのサーバー機器へEDR製品の導入
② 既存アカウントの整理と全アカウントのパスワードリセット
③ 各ネットワーク機器のファームウェアの最新化と、最新化の運用ルール化及びセキュリティ関連製品のライフサイクル管理強化
④ VPN機器の認証強化（多重認証の導入）
⑤ 特に基幹システムデータについて、クラウド上でのオフライン化
⑥ サイバー保険への加入検討
⑦ システム障害/サイバー被害発生時の内部・外部対応役割・管理体制の見直し(BCP：緊急時対応マニュアルの刷新、社内関連規程の見直し等)
⑧ 全グループ従業員対象とした情報システム管理リテラシー向上教育の実施

今後とも、当局及びシステム関連専門家の方々と連絡を密にし、担当役員を先頭に再発防止に向けた社内体制の構築・定着化を図っていく所存であります。