

【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31日
【会社名】	株式会社イズミ
【英訳名】	IZUMI CO., LTD.
【代表者の役職氏名】	代表取締役社長 山西 泰明
【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】	広島県広島市東区二葉の里三丁目3番1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)

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】

当社代表取締役社長山西泰明は、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」という。）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、企業会計審議会の公表した「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）」に示されている内部統制の基本的枠組み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、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】

財務報告に係る内部統制の評価は、当事業年度の末日である2024年2月29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おります。

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、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っております。

財務報告に係る内部統制の評価の範囲は、当社グループについて、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6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しております。なお、連結子会社9社及び持分法適用会社3社については、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おりません。

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、前連結会計年度の概ね2/3に達している1事業拠点を「重要な事業拠点」といたしました。選定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対象としております。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】

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。

したがって、当事業年度末日時点において、当社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

2024年2月15日早朝に当社グループの情報ネットワークが、第三者からランサムウェア型サイバー攻撃を受けて、一部のサーバーが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。システム障害発生後、被害拡大を防止するため、当社は、速やかに当社グループの社内ネットワークが繋がっている全サーバーの停止と社内外のネットワークの遮断を実施しました。

当社は、サイバー攻撃の被害を受けた直後から、事態の緊急性と経営全般に係る内容であることから、BCP計画にもとづき、直ちに対策本部を設置して、営業活動への影響低減や、決算業務の遂行のため、社内ネットワークや各システムの早期復旧を全力で対応して参りました。

ただし、経理関連データへのアクセス障害、代替的な業務プロセスの構築、システム復旧等の対応が必要となり決算手続に遅延が生じ結果として、法定期限までに有価証券報告書が提出できない状況となりました。なお、財務会計システムへの侵入はなかった結果、財務会計データの被害はありませんでした。

サイバー攻撃を受け、システム障害が発生した原因について、外部専門家の協力のもと調査を実施した結果、情報セキュリティに関する重要性は認識して対応は行っていたものの、サイバー攻撃に係るシステム上の対応が十分

ではなかったことが判明しました。

当社内でその指摘の真因である内部統制の課題を検討した結果、当社グループ全体のサイバーセキュリティとIT戦略を一元管理し、迅速な意思決定と施策を行うための体制・組織が不十分（サイバーセキュリティに関する戦略が不十分）であり、刻々と高度化するサイバー攻撃に対応するため、情報セキュリティのリスクを網羅的に把握し評価するための組織体制が十分ではなかった（リスクの評価と対応が不十分）との認識に至りました。

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、適切な分析及び対応方針の策定が行われず、第三者によるシステムへ不正アクセスを許して被害をうけるとともに、回復までに一定の時間を要し、法定期限までに有価証券報告書が提出できない状況が生じたという事態を踏まえて、サイバー攻撃による被害を受けた2024年2月15日において、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、2024年2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2月15日に発覚したため、是正まで約2週間の期間しかなく、是正策の実施と評価を完了することができなかった為です。

4 【付記事項】

「3 評価結果に関する事項」に記載した全社的な統制上の開示すべき重要な不備を改善するために、復旧作業と並行して、復旧作業での課題や、外部専門家の協力のもとで実施した原因究明を踏まえて、再発防止策の検討と実施につきましては、全社を挙げて迅速に取り組んで参りました。

そして、サイバーセキュリティの技術的な課題への対応と全社的な統制の不備の是正のために人、ハード、体制の観点で必要な措置を、実施しております。

サイバーセキュリティの体制・組織面におきましては、当社グループ全体のセキュリティとIT戦略を一元管理するとともに、迅速な意思決定と施策を行うため、セキュリティ関連の意思決定を中心に担当し、全社的なセキュリティ強化を推進するCISO(情報セキュリティ責任者)を設置しました。

また、刻々と高度化するサイバー攻撃に対応するため、情報セキュリティのリスクを網羅的に把握し評価するため、セキュリティ情報の収集と分析、企画を担う情報セキュリティ担当を設置しております。

これらの体制の下で、識別されたシステム上の技術的な課題について、異なる防御層を重ねて、セキュリティを強化する多層防御と監視体制の構築等の対応を行っており、更に、今後、継続してサイバー攻撃を受けた時に、より即応できるBCP計画の策定、被害回復を迅速にするための更なる技術的対応等を実施して参ります。

以上のとおり、当事業年度末日後内部統制報告書提出日までに、評価結果に関する事項に記載された開示すべき重要な不備を是正するための施策は既に整備され、運用を開始しておりますが、引き続き、施策の着実な運用とサイバーセキュリティ対応の高度化に取り組んで参ります。

5 【特記事項】

該当事項はありません。