【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】	2022年６月29日
【会社名】	株式会社ニップン
【英訳名】	NIPPN CORPORATION
【代表者の役職氏名】	代表取締役社長　　前鶴　俊哉
【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】	東京都千代田区麹町四丁目８番地
【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】

代表取締役社長前鶴　俊哉は、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改訂について（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、2022年３月31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）を評価したうえで、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うえで、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、内部統制の有効性を評価しました。

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、当社と連結子会社との合計27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ました。なお、連結子会社19社及び持分法適用会社14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、前連結会計年度の連結売上高の概ね３分の２に達している５事業拠点を「重要な事業拠点」としました。選定した重要な事業拠点においては、当社グループ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、2022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。

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等)

（１）サイバー攻撃によるシステム障害の発生とその後の取り組み

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（以下、ニップンビジネスシステム）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ることにより、システム障害が発生しました。

当社は速やかに全サーバーの停止と社内外のネットワークの遮断を行った結果、グループネットワーク内で運用している当社及び国内グループ会社の財務会計システム、販売管理といった主要な基幹システムを含む全ての社内システム、データが保存されているファイルサーバー、バックアップサーバーへのアクセスができなくなりました。

当社経営陣は、障害発生当日である2021年７月７日にシステム関連部門を中心とした対策チームを組成し、危機管理基本規程に基づき危機管理委員会を設置しました。

その後、2021年７月19日に同委員会を改組して「大規模システム障害対策本部」を立ち上げて、本件インシデントの原因究明等について、外部のサイバーセキュリティ専門家に依頼して調査を実施し、侵入経路や影響範囲を特定するとともに、その助言に基づいて二次被害の抑止策の実施及び被害を受けた情報システムや業務関連データの復旧（情報システムの再導入を含む）に注力していくこととしました。

当社単体のその他の業務関連システムについては、データの整合性や復旧プロセスの合理化を図るため、データの上流である受発注、入出庫、在庫管理等を担う物流管理・販売管理システムの復旧を最優先し、下流へと順次対応を行っていくことを基本方針とし、復旧に向けて取り組んでまいりました。外部専門家を交えて対応に当たった結果、

物流管理システムについては、2021年７月７日のシステム停止後から受注出荷の記録・入出庫等の対応を手作業で行っている状態であったため、システム復旧までの暫定的な処置として、受発注機能のみを搭載する代替システムを導入し、2021年９月上旬から稼働しました。当社の業務関連システムについては、2022年の年始に主要な基幹システムの復旧を完了いたしました。

一方、決算の取り纏めについては、従来の財務会計システムの復旧の目途が立たない状況下で、当社は新規に財務会計システム（以下、新財務会計システム）を購入して、新たに財務報告に係る内部統制を構築し、決算を一からやり直すことが虚偽記載のない正確な決算を報告するための最速かつ最善な方法との判断に至りました。この判断に沿って、新財務会計システムは2021年７月21日から別環境（クラウド版）にてシステムの導入の手配を進め、2021年９月17日からフルバージョンでの利用が可能になりました。連結会計システムについては、2021年８月30日から利用を開始しています。ただし、新財務会計システムは利用開始となったものの、他の基幹システムとの連動ができず、手作業による対応が必要となる状況が継続していました。

当社は決算作業を速やかに進めるために外部人材活用や外部専門家の支援を受けたものの、企業内容等の開示に関する内閣府令に規定する四半期報告書の提出期限延長に関する承認申請を提出せざるを得ませんでした。当社は2021年８月16日に2022年３月期第１四半期報告書の提出期限を2021年11月15日とする延長に関する承認申請書を関東財務局へ提出し、ご承認をいただきました。

2022年３月期第１四半期の決算取り纏めに当たり、決算を行うために必要なデータ及び資料等が当社及びグループ会社の各従業員が使用しているパソコン（以下、ＰＣ）内のフォルダやニップンビジネスシステムが保管しているＤＶＤ等の記録媒体に存在しているか、可能な限りの探索調査を実施しました。印刷物として残されていたものを収集し、2021年６月以前の業務プロセスによる作成していた紙ベースの入出金帳票やＤＶＤのバックアップデータを基に、システム取り込み様式で用意したエクセルシートに仕訳伝票を入力して作業を取り進めることといたしました。その結果、当社は2021年11月15日に2022年３月期第１四半期報告書を提出しました。

2022年３月期第２四半期決算については、二次障害防止のため、当社情報ネットワークを完全に遮断のうえ、「原因調査」、「侵害調査」、「漏洩調査」並びにセキュリティ対策を順次、相応の時間を掛け実施しております。会計データに連動している業務管理や物流管理など停止した基幹システムの復旧が受発注機能のみを搭載した代替システムの仮復旧に留まったため、大半の基幹システム復旧が第３四半期末である年末にずれ込みました。その結果、利用可能になった新財務会計システムを他の基幹システムと連動させることができず、正常な状態であれば、各システムに入力された日々の取引データが自動的に集計され、振替伝票データへ変換され、財務会計システムへ自動取り込みされるという一連のプロセスを全て手作業で実施することとなり、決算処理の元となる帳票をエクセル等による手作業で作成せざるを得ない状況となりました。このように、手作業で作成された帳票類を基に本来自動作成されていた振替伝票を経理担当者が一から作成する必要があり、売上の集計や入金の消し込みなどに多大な時間を要することとなりました。会計監査人のレビューに関しても、第２四半期以降の基幹システムが停止している期間は、当社の業務プロセスを大きく変更せざるを得ない特殊な状況になったため、変更プロセスに対応する当社の新たに構築した内部統制を理解した上で必要な手続を経て実施することとなり、これまでよりも多くの時間を要することとなりました。このように、決算とレビューに多大な時間を要することとなったため、当社は2021年11月12日に2022年３月期第２四半期報告書の提出期限を2022年１月31日とする延長に関する承認申請書を関東財務局へ提出し、ご承認をいただき、2022年１月31日に2022年３月期第２四半期報告書を提出しました。

2022年３月期第３四半期決算については、単体決算でのエクセル等による手作業による集計作業に習熟度が向上したものの、2022年３月期第２四半期と同様に未だに基幹システムがもとの状況まで復旧できておらず、決算に時間を要することとなりました。当社は2022年２月14日に2022年３月期第３四半期報告書の提出期限を2022年３月18日とする延長に関する承認申請書を関東財務局へ提出し、ご承認いただき、当社は2022年３月18日に2022年３月期第3四半期報告書を提出しました。

2022年３月期においては、2022年１月以降、会計データに連動している業務管理や物流管理などの基幹システムと新財務会計システムとの自動連係が漸くシステム障害前と同様の会計処理ができる状態に復旧しました。当社は、2022年３月期有価証券報告書を法定期限内の2022年６月29日に提出しました。

（２）本件インシデントの原因と対策

①本件インシデントの原因

サイバーセキュリティに関するリスクが高まる中で、インターネットと当社ネットワークシステムの境界線を制御する機器（以下、ＶＰＮ）の脆弱性についての対応が遅れた結果、外部の攻撃者の侵入を許して本件インシデントが発生してしまったことに関して、その根本原因を明らかにし、社内の制度や内部統制の運用上の問題を調査・分析・整理するとともに、再発防止策の策定と、サイバーセキュリティの体制強化を行うため、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が３件指摘されました。

サイバーセキュリティに関しては、当社では従来、端末ＰＣへの不正侵入検知システムやウィルス対策ソフトの導入・適時の更新（対策ソフトのＡｇｅｎｔがサーバー・ＰＣ上で１日に数回、自動的に更新する仕組み）を実施し、常にＰＣ・サーバーが最新の状態で保たれる仕組みを保持しておりました。また、ファイアーウォール（以下、Ｆ

W）については外部のマネージドサービス会社（利用者に代わり、サーバーなどの管理業務を行う会社）に業務を委託し、専門的立場からの助言や設定見直しが必要な場合には提案を受ける仕組みが構築されていました。

バックアップ体制については、10年程度前までは各拠点で個々のサーバーを運用していたものを、一元管理に移行し、かつ、ディザスタリカバリー（災害復旧）の視点も取り入れた上でサーバーを地理的に離れた３拠点のデータセンターに分散させました。

本件インシデントが発生したのは、当社が構築したネットワークシステムに隠れていた脆弱性を突いて外部から侵入されたことに因るものと判明しています。ＶＰＮ及び社内認証やアクセス制御を管理するサーバー（以下、ＡＤサーバー）にパッチ処理はなされていたものの最新ではなく、パッチを更新すべきＶＰＮの脆弱性情報が2021年５月に公開された後、まだ当社の機器に最新の状態が適用される前に本件インシデントが発生し、システムのネットワーク内に二重のＦＷが無かったことで被害が拡大しました。

この当社ネットワークシステムに隠れていた脆弱性を生み出した背景にある内部統制に係る原因として指摘された３件の課題の内容は以下のとおりです。

1) **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**

これまで当社には、情報セキュリティ規程やニップンネット運用・利用規則といった規程類がありました。子会社のニップンビジネスシステムにも情報セキュリティ規程やニップンネット運用・利用規則をはじめ、システム運用管理規程やシステム開発・導入規定など各種規程類がありました。しかし、サイバーセキュリティリスクの重大性及びこれに対する対策の重要性を全社の基本方針として明確に示したものではありませんでした。当社、ニップンビジネスシステムそれぞれの情報セキュリティ規程においても、具体的な運用ルールや手続きを記した要領、ガイドライン、マニュアル等は定められていませんでした。今回のようなインシデントの際の行動指針やフローチャートも明確に規定されていませんでした。

2) **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**

情報システム管掌役員は選任されていたものの、サイバーセキュリティリスク管理体制を構築し遂行する役員レベルの総括責任者としての役割は曖昧でした。本来一元的管理されるべきセキュリティ対策の内容を決定し実施する権限が当社にある筈のところ、実務現場では、ニップンビジネスシステムへ指示責任が不明確なまま同社の担当者の個人の資質に頼った業務遂行がなされていました。

3) **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**

サイバーセキュリティ対策を包含するＩＴ全般の投資については投融資委員会等で計画されており、一定の投資もされ、実績の報告もされてきました。しかし、戦略や計画等が中期経営計画及びＢＣＰ等に詳細に盛り込まれてはおらず、サイバーセキュリティを担える人材もここ最近毎年新人を採用してきているものの、専門的な知識のある人材が充分に配置されたというには不十分な状態でした。その結果、サイバーセキュリティリスクの把握や検討が困難となり、必要な人的資源の確保、システム関連の物的資源確保の予算措置及び現場から経営陣に対しての現状の充分な報告がされなかったことで、経営陣のリーダーシップが不足していました。

②本件インシデントの改善策

このような指摘を受けて、当社の行った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に関しては、当社システムと外部環境は現状遮断を継続し、パッチ適用を実施後に遮断を解除する方針のもと、３月末までに情報セキュリティ管理規程に基づき脆弱性管理ルールに定められたパッチ適用判断基準に従い、３月末時点で復旧している最重要のサーバーの中からパッチ適用範囲を定め、ＡＤサーバーのセキュリティパッチを実施しました。また、サーバーにもＦＷを実装してＦＷの二重化をいたしました。その他にも、リモートネットワークアクセスの多様素認証、ネットワーク侵入検知・防止ソリューションの導入、導入ソフトの許認可やサポート状況の確認徹底等の対策を実施しています。バックアップについても、各システムの重要度に応じたバックアップ方針（方式、頻度、保管先）に従って、自動バックアップや復旧データの保護を実施しました。また、事実の背景にある内部統制に係る原因として指摘された３件の課題に対する改善の内容は以下のとおりです。

1) 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

当社は2022年３月28日開催の取締役会で、「情報セキュリティ基本方針」の制定を決議しました。同時に「情報セキュリティ管理規程」等の規程類を整備いたしました。具体的な運用ルールや手続きを記した要領、ガイドライン、マニュアル等を定め、インシデント発生時の行動指針やフローチャートを策定し、脆弱性管理ルールにもとづいたパッチ適用の運用をし、システムの重要度に応じたバックアップ方針（バックアップ方式、頻度、保管先）に基づき運用し、インシデント発生時の財務報告への影響を低減する復旧体制を構築しました。不正アクセスを軽減するために、必要な人に必要な範囲のみのアクセスを提供するネットワークの制御・不正アクセスの検知に関して規定しました。サイバーセキュリティンシデント発生時に実施すべき一連の対応を規定しました。これによって、サイバーセキュリティリスク管理体制の構築や運用手続の基本となる体制ができあがりました。

2) 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

2022年３月に上記情報セキュリティ管理規程において、サイバーセキュリティ管理体制の明確な指示系統・責任体制を定めるとともに、2022年２月25日開催の当社取締役会において情報システム推進部を新たに設置することを決議し、2022年３月28日の当社取締役会においてＩＴ管掌取締役選任の報告がありました。これによって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が構築されました。

3) 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

本件インシデント発生以後、直ちに対策本部を設置して当社代表取締役の指示のもと、本件インシデントで指摘された課題に対する改善に全社一丸となって取り組んでおります。ＩＴ関連の新体制が決議されたことにより、必要な人材確保や予算措置がより具体的かつ迅速に実行できる組織基盤が構築されました。2022年３月28日開催の当社取締役会に内部監査の一環として「情報セキュリティ監査」の整備が報告されました。内部監査の結果は当社取締役会に報告されます。前述した当社の改善活動に連動して、当社グループの情報ネットワークを管理運用するニップンビジネスシステムの2022年３月28日開催の取締役会においても、社内規程類の整備を決議し、これらの規程の内容に沿って運用されていることを確認いたしました。

これによって、経営層のサイバーセキュリティに対する意識向上が図られて、ＩＴに係る経営戦略（人材確保・投資を含む予算措置など）の体制が構築され、適切なリスク評価と対応が行われました。

当社は今回のインシデントに対する再発防止策に取り組むことで、適切な財務報告体制を確保するために全社的な内部統制（リスク評価と対応）を再整備することといたしました。目指すのは、2021年７月７日未明に当社に対して行われたサイバー攻撃と同様の手口による攻撃に対して、適切に防御し、かつ、復旧するための規程整備とセキュリティ上の改善を実施することです。

そのレベルは３月末までにセキュリティコントロールの指標であるＣＩＳ　Ｃｏｎｔｒｏｌｓの要求事項から効率性を重視し、情報セキュリティ管理規程に必要情報を集約しながら策定しました。詳細手順が必要なものは各ルールとして整備いたしました。具体的には、情報セキュリティ基本方針や情報セキュリティ管理規程等を整備し、同規程でサイバーセキュリティ管理体制の明確な指示系統と責任体制を定めました。また、これらの規程の内容に沿って、３月末のシステム環境で、システム及びデータベースの脆弱性強化対策（パッチ、バックアップ等）が定めたポリシーに沿って行われていることを確認いたしました。

この施策は当社が2021年７月７日未明に受けたサイバー攻撃と同様の手口によるリスクに対応しております。従って、2022年３月末日時点において、当社は本件インシデントと同様の手口に対するサイバーセキュリティのリスクに対応した適正な財務報告を行う体制を確保いたしました。

さらに、外部の専門家を含めた社内調査の結果、３月までに整備が必要とされた情報システム推進部の設置を2022年２月25日開催の当社取締役会で決議し、同４月からのＩＴ管掌役員選任を2022年３月28日開催の当社取締役会で報

告しました。併せて、当該部署の人材や予算の確保や責任体制への組織基盤の構築を行うとともに、情報セキュリティ監査体制を整備し、運用しました。

以上の結果から、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、適正に整備・運用されていると結論づけました。

（３）本件インシデントの内部統制上の整理（不備の特定と評価）

①全社的な内部統制について

当社はインシデント直後の早い時期からいわゆる封じ込めのためにシステムを止めるとともにネットワークを切り離して影響の拡大を防ぎ、原因究明のために必要な情報の保全を図りました。当時、システム復旧の目途が立たない状況下で、当社は新システムを導入して新しい内部統制を構築し、決算を一からやり直すことが虚偽記載のない正確な決算を報告するための最速かつ最善な方法との判断に至りましたが、その一方で業務プロセスの変更や決算開示日程の遅れなど会社経営に重大な影響を与える結果となりました。

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ております。このため、当社の2021年3月末時点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。従って、当社は本日2021年６月29日に提出した第197期内部統制報告書の訂正報告書を提出いたしました。

このような四半期報告の遅延という重要な事態をもたらす状態については、前述の記載のとおり、セキュリティパッチを実施し、ＦＷの二重化を行い、内部統制に係る原因として指摘された３件の課題に対する改善策を内部統制の基準日である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。

また、当社及びグループ内において、全社的な内部統制のサイバーセキュリティに係る類似の課題がないことを確認しています。

②ＩＴ全般統制（ＩＴＧＣ）について

本件インシデントの直接的な原因は、ＶＰＮの脆弱性をつかれて攻撃者に侵入され、ＡＤサーバーの脆弱性に乗じて暗号化されたことです。

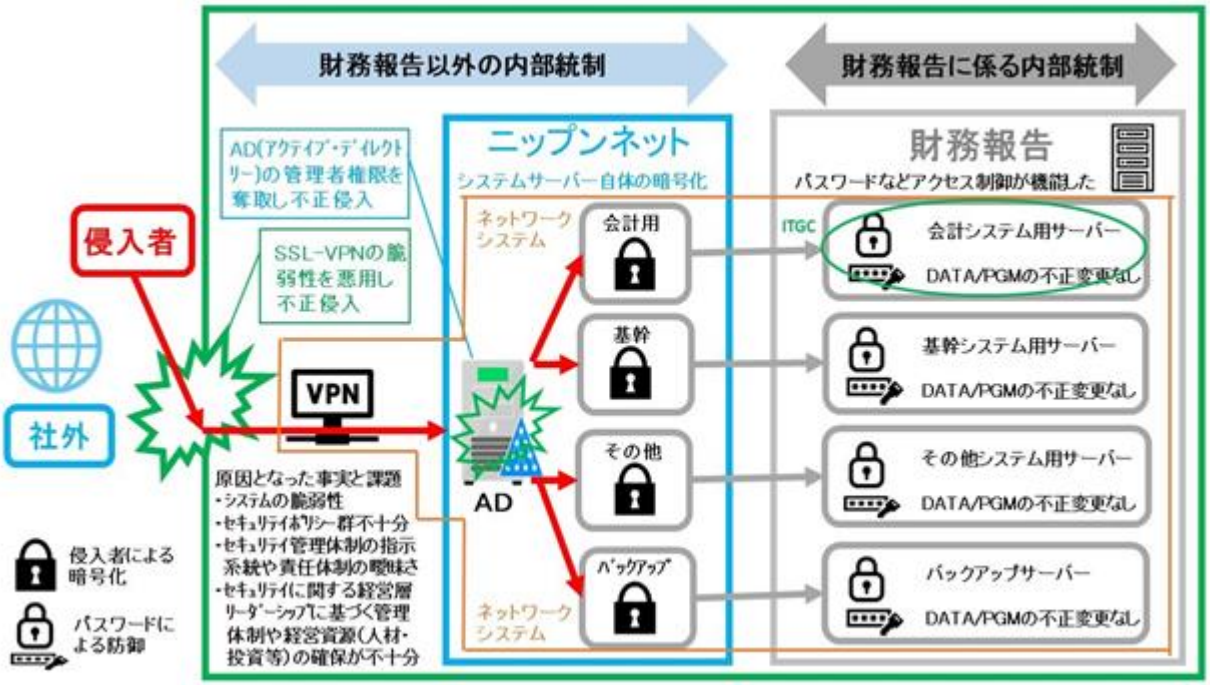
当社の場合、財務データの生成・保管に係る各システムについてＩＴシステムの開発、運用保守、アクセス管理等の手続をルールに定め、経営者評価の過程で各システムのＩＴ全般統制の有効性を評価しております。なお、ＶＰＮ及びＡＤサーバーは、会計システムサーバー等とは異なり、財務データの生成・保管に直結しないため、ＩＴ全般統制の対象とはしておりません。

本件インシデントにより、財務報告に係るシステムにつながる汎用サーバー自体は暗号化されてデータの取り出しができなくなったものの、ＩＴ全般統制の評価対象であるシステムのパスワード管理が有効に機能していたため、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、保管されていた財務報告に係るデータやプログラムの不正な改ざんは検出されず、財務報告に金額的あるいは質的な重要な虚偽記載につながる事実はありませんでした。

2022年３月期の内部統制監査制度の経営者評価で、各システムのＩＴ全般統制を評価した結果、不備は検出されませんでした。従って、2022年３月期のＩＴ全般統制について有効と評価いたしました。

（４）補足説明資料

①本件インシデントとネットワークシステムの範囲



②ＩＴＧＣの対象システム範囲