令和６年度電力市場監視機能強化等事業

（電気事業法に基づく監査における業務調査事業）

実施結果報告書

令和 7 年 2 月 28 日

有限責任監査法人トーマツ

令和 7 年 2 月 28 日

経済産業省　御中

有限責任監査法人トーマツ
パートナー　木崎　利郎
パートナー　奥田　健一

有限責任監査法人トーマツ（以下、「当法人」という。）では、経済産業省（以下、「貴省」という。）のご依頼に基づき、2024 年 8 月 22 日から 2025 年 2 月 28 日までの間、電気事業法に基づく監査における業務調査事業を実施しました。その結果を報告書としてまとめましたので、ご報告申し上げます。

本報告書は、貴省と当法人との間で締結された、令和 6 年 8 月 22 日付け業務委託契約書に基づいて実施した電気事業法に基づく監査における業務調査事業について報告するものであり、保証業務として実施したものではありません。内容の採否や使用方法については、貴省自らの責任でご判断いただくよう、お願い申し上げます。

本報告書に記載されている情報は、調査時点のものであり、公開情報を除き、貴省または調査対象者から提出を受けた資料、また、その内容についての質問を基礎としております。当法人は当該資料等の妥当性・正確性について検証する義務及び更新する義務を負っておりません。

本調査は、貴省と当法人が協議及び合意した範囲、手続等を前提として実施されたものであり、本調査が異なる前提で実施された場合は、閲覧対象の内容が異なる可能性があります。

なお、本報告書は公表版であり、調査対象者の企業情報やセキュリティ等に配慮し、該当部分を伏せ字としております。

目次

Ⅰ　実施概要

1.　目的

本調査は、大手電力会社による情報漏洩・不正閲覧が明らかとなり、電気事業の中立性・信頼性に疑念を抱かせる事態となっているところ、電力の適正な取引確保の観点から、各事業者の法令遵守状況等に係る電力・ガス取引監視等委員会の監視機能の強化を図ることを目的とし、電気事業法に基づく監査において実施する情報管理についての監査に係る分析調査を実施した。

2.　受託業務の内容

電気事業法施行規則第 33 条の 15 第 1 項第 2 号において、託送供給及び電力量調整供給の業務を行う部門に非公開情報の管理の用に供するシステムとして、「必要に応じて区分された非公開情報ごとに、それぞれ当該区分された非公開情報を利用し、または提供するために入手することができる者として特定された者のみが当該情報を入手することができるものであること」、「当該システムを使用して非公開情報を入手した者を識別することができる事項、当該者が入手した非公開情報の内容及び当該非公開情報を入手した日時を記録し、これを保存するものであること」を満たすことが確保されたものを構築することになっている。

そのため、非公開情報の管理の用に供するシステムについて、特定された者のみが当該情報を入手することができることになっているか、システムログ[1]から確認した。具体的な実施内容は以下に示す。

2.1　調査の概要及び実施方法

本調査は、各一般送配電事業者（以下「各事業者」という。）のシステムのうち電力・ガス取引監視等委員会事務局総務課総合監査室（以下「総合監査室」という。）が指定した 4 システムについて、当法人にてリスクを評価することにより各事業者あたり 1 システムを選定し、その後、選定したシステムのシステムログ（アクセスログ[2]及び操作ログ[3]）を入手しログ分析を行った。各プロセスの実施方法は次のとおりである。

2.1.1 対象システムの選定

(1) リスク評価シートの作成

ログ分析の対象となるシステム選定のためのリスク評価にあたり、リスク評価項目及

---

[1] システムログは、システムの動作履歴の記録である。本調査では、アクセスログと操作ログを対象とした。アクセスログと操作ログの説明については、注記 2 及び 3 を参照。

[2] アクセスログは、システムへアクセス（ログインを試みた）した際の記録である。アクセス日時、ユーザ ID、アクセス元、アクセス先などの情報が含まれる。

[3] 操作ログは、ユーザがシステム内で行った操作の記録である。ユーザ ID、操作日時、実行されたコマンド、操作の種類などの情報が含まれる。

びリスクスコア算出方法の検討を行い、リスク評価シートを作成した。

システムの重要度（リスクが顕在化した際の影響度）、リスクの発生可能性の観点から評価し、リスクスコアを算出する様式とした。

- 重要度：システム規模や利用目的、システム構成といったシステムの属性からリスクが顕在化した際の影響度を重要度として評価
- 発生可能性：セキュリティ、不正利用等想定されるリスクの発生可能性をコントロールの整備状況から評価

具体的な評価項目については、2.2 評価観点に示す。

(2) リスク評価

リスク評価は、各事業者より「表 1 総合監査室が提示したリスク評価に関する資料リスト」に示す資料を入手し、以下の手法を用いて実施した。

＜手法＞

- 資料閲覧：
  各事業者より提供された資料を閲覧し、システム概要及びコントロールの整備状況を把握した。
- 質問：
  資料閲覧により、生じた確認事項を各事業者の担当者へ質問し回答を得た。

表 1 に記載の資料以外にリスク評価を行う上で必要な資料を追加で入手した。

表 1 総合監査室が提示したリスク評価に関する資料リスト

No.	資料名	内容
1	組織内のシステムとアプリケーションのリスト	各システムが処理しているデータの内容、及びシステム間でどのようにデータが共有されているかわかる資料
2	システム設計・構成が分かる資料	データフロー図、ネットワーク図などの資料
3	社内と社外のユーザ数（概算）が分かる資料	システムリスク評価に活用するため、外部に接続しているシステムの特定及びユーザ数（外部からのアクセス可能者）が把握できる資料
4	データ分類が分かる文書	各データの機密性のレベル、データ保護の必要性の有無がわかる資料
5	組織のデータを分類するための基準	
6	データマッピング文書	組織内のデータの流れと、データが保存されている場所を示す文書

No.	資料名	内容
7	リスク評価レポート	過去に社内で実施したシステムリスク評価に関するレポート（実施している場合）
8	脆弱性評価と侵害インシデントの報告資料	システムのセキュリティ脆弱性や過去のセキュリティ侵害の詳細が報告された資料（実施している場合）
9	現行のセキュリティポリシーやプロシージャ	組織のセキュリティ戦略とガイドラインを定義した文書（セキュリティポリシー） データの品質管理、データのセキュリティなど規程類が別途ある場合には、これも含む。
10		誰がどのシステムやデータにアクセスできるかを定義した文書（アクセス制御ポリシー）
11	インシデント対応計画	セキュリティインシデントが発生した場合の対応プロセスを定めた文書直近のインシデントの情報（件数と概要）を含む。
12	システムごとの年間アクセス件数データ	解析に係る工数やシステムの重要性判断のため、システムごとの年間アクセス件数及びアクセスの月次推移が分かる資料（直近 1 年間分）

(3) 対象システムの選定

各システム属性や各社の内部環境、及び外部環境を把握し、コントロールの整備状況を踏まえリスクを評価した。事業者ごとに、4 システムのうち、リスクスコアの合計値が最も高いシステムを対象システムとして選定した。

選定した対象システムを「表 2 各事業者のログ分析対象システム」に示す。

表 2 各事業者のログ分析対象システム

地域	事業者	対象システム
北海道	北海道電力ネットワーク株式会社	託送業務システム
東北	東北電力ネットワーク株式会社	営業オンライン
東京	東京電力パワーグリッド株式会社	PG サービス業務支援システム（PGSS）

地域	事業者	対象システム
中部	中部電力パワーグリッド株式会社	お客さまサービスシステム(CIS)
北陸	北陸電力送配電株式会社	営業システム
関西	関西電力送配電株式会社	託送 OSS（ホスト）
中国	中国電力ネットワーク株式会社	営業システム
四国	四国電力送配電株式会社	託送お客さま管理システム
九州	九州電力送配電株式会社	電力輸送部門 IT システム（TSMS）
沖縄	沖縄電力株式会社	営業システム

2.1.2 システムログの分析

(1) 未加工ログの受け取り

各事業者と協議し、対象となるログの確認及び受取方法を調整し、各事業者より未加工ログ（一切加工されていない状態のログ）を直接入手した。当該ログは、当法人にて本調査の関係者のみにアクセス制御されたフォルダ及び分析環境で厳重に管理し、分析に利用した。

(2) アクセスログの分析

選定した各事業者の 1 システムについて、事業者が提出した 1 ヶ月分のログ及び「非公開情報を入手可能な者の名簿」（以下「ホワイトリスト」という。）を照合することにより、非公開情報を入手することができない者が情報を入手していないかを分析した。

(ｱ) 各事業者との事前調整

前項で選定したシステムを対象とし、各事業者とログ依頼に関する事前調整のミーティングを行った。取得ログの内容、アクセス権管理、認証（アクセス方法）、権限設定、小売・委託先・販売店とのシステム共有の状況、共有 ID[4]の利用状況、事業者によるログモニタリングの実施状況等をヒアリングした上で、ログの提供を依頼した。

(ｲ) パイロットテスト

アクセスログ分析は、1 日分の少量データを用いた確認を行い、分析方法を確立することとした。(以下、「パイロットテスト」という。) パイロットテストでは、アクセスログ分析に利用可能なログを取得できていること、取得したログに権限のない者によるアクセスがないかを確認するための必要項目が含まれていることの確認を行い、ログデータの有効性を検討した。また、ログ分析方法を検討し、分析するためのスクリプト[5]を作成した。

[4] 共有 ID は、一つの ID を複数人で利用（共有）している ID を指す。

[5] スクリプトは、特定のログデータを抽出、集計、解析するために使用される、ログ分析を自動化するための一連のコマンドやプログラムコードを指す。

(ｳ) アクセスログ分析

各事業者より、総合監査室が指定した 2024 年 7 月の 1 か月分のログを入手し、パイロットテストで確立した分析方法に則り、アクセスログ分析を実施した。

アクセスログからシステムにログインを試みたユーザを抽出し、ホワイトリストと突合し、ユーザを①有権限者、②権限のない者に分類した。また、共有 ID によるアクセスは、各事業者への質問、管理簿の閲覧等により利用者の特定を行った。

ここで言う有権限者とは、事前に認定されたアクセス権限を持つものを指す。ホワイトリストに記載されたユーザがシステムにアクセスした場合を、有権限者によるアクセスと識別し、記載されていないユーザがアクセスした場合を、権限のない者によるアクセスと識別した。

(3) 操作ログの分析

アクセスログ分析において、権限のない者に分類したアクセスについて、当該アクセスに紐づく操作ログを入手し、操作ログから、アクセスした画面及び実行した操作内容を抽出した。アクセスした画面や操作内容から非公開情報へのアクセス有無の確認及び操作の分析を行った。

2.1.3 実施報告書の作成

本事業の成果について、分析結果を取りまとめ、各事業者と協議し、認識合わせを行った上で本報告書を作成し、総合監査室に提出した。

2.2 評価観点

2.2.1 対象システムの選定の観点

(1) リスク評価項目の設定

評価にあたって、システムの重要度（リスクが顕在化した場合の影響度）の判定（以下、「重要度判定」という。）とリスクの発生可能性を評価（以下「発生可能性評価」という）し、リスクスコアを算出することとした。評価における客観性を担保するため、以下(2)に記す基準と当法人の知見をもとに、システムの重要度とリスクの発生可能性の観点から評価項目を設定しリスク評価シートを作成した。リスク評価シートの主な評価項目を「表 3 リスク評価シートの主な評価項目」に示す。

表 3 リスク評価シートの主な評価項目

評価観点	リスク分類	主な評価項目
重要度評価	－	• システム利用目的 • データの機密性レベル • インターフェースボリューム • ユーザ数、年間アクセス数 • システム構成の複雑度 等

評価観点	リスク分類	主な評価項目（リスク）	主な評価項目（コントロール）
発生可能性評価	①データ品質・データ管理リスク	• データ信頼性リスク	• システム及びデータの機密性、可用性、信ぴょう性、回復性を確保するための管理策の整備有無等
	②不正にかかるリスク（アクセス権管理・技術運用管理）	• 情報への未承認アクセスリスク	• 利用者 ID やアクセス権の設定手順、削除に関するルールの整備有無等
	③サイバーにかかるリスク	• セキュリティが有効でない、不十分であるリスク • インシデント発生時の事業継続リスク • インシデントによる被害拡大リスク	• 防御対策の実装、脆弱性の識別の有無 • インシデント対応及び事業継続の対応計画と復旧計画の整備有無等

(2) 参考とした基準

評価項目の検討にあたり、以下の基準を参考とした。重要度判定では、一般送配電事業は重要インフラサービスに該当する点を考慮した。発生可能性評価では、リスクに対応するコントロールの整備状況を確認するため、システム監査の基準、データ管理の基準、システム観点における不正防止の考え方、サイバーセキュリティの一般的なフレームワークの観点を考慮し、基準を選択した。

表 4 参考とした基準

評価項目	参考にした基準
重要度判定	• 重要インフラにおける情報セキュリティ対策の優先順位付けに係る手引書（第 1 版）（内閣サイバーセキュリティセンター）
発生可能性評価	• データ品質管理ガイドブック（デジタル庁） • 組織における内部不正防止ガイドライン（情報処理推進機構） • システム管理基準（経済産業省） • システム監査基準（経済産業省） • 金融機関等のシステム監査基準（公益財団法人 金融情報システムセンター）

評価項目	参考にした基準
	• 重要インフラのサイバーセキュリティを改善させるためのフレームワーク（第 1.1 版）（米国国立標準技術研究所）

(3) リスクスコアの算出方法

リスク評価シートは重要度判定と発生可能性評価の二部構成とした。重要度判定で評価したリスク顕在化の影響度のスコアと発生可能性評価で評価したリスクの発生可能性のスコアをかけあわせ、リスクスコアを算出した。システムごとのリスクスコアの合計が 4 システムの中で最も高い 1 システムをログ分析対象として、事業者ごとに選定した。

(ｱ) 重要度判定

システムの重要度を全 7 項目にて High、Middle、Low で評価し、その合計をシステム重要度スコアとして算出した。（システムの重要度はリスク顕在化の影響度と位置づけた）

評価結果=High（当てはまる）	リスクスコア：3
評価結果＝Middle（一部当てはまる）	リスクスコア：2
評価結果＝Low（当てはまらない）	リスクスコア：1

(ｲ) 発生可能性評価

コントロールの整備状況を全 26 項目にて評価した。26 項目の評価結果を踏まえ、想定されるリスク全 9 項目の発生可能性を High、Middle、Low で評価し、その合計をリスクの発生可能性評価スコアとして算出した。

評価結果=High（当てはまる）	リスクスコア：3
評価結果＝Middle（一部当てはまる）	リスクスコア：2
評価結果＝Low（当てはまらない）	リスクスコア：1

(ｳ) 総合判定

重要度判定で算出したシステム重要度スコアと、発生可能性評価で算出した発生可能性評価スコアを合計し、トータルスコアを算出した。4 システムを比較し最もトータルスコアが高い 1 システムをログ分析対象として選定した。

2.2.2 アクセスログ分析の観点

(1) ログ分析の前提事項の確認観点

(ｱ) ホワイトリストの信頼性

各事業者から入手したアクセスログとホワイトリストを突合し、有権限者によるアクセスか否かを判断する前提として、ホワイトリストの信頼性を確認し、ログ分析の基礎データとできるかを確認した。ホワイトリストの信頼性を確認するにあたり、主

に以下の事項を確認した。各事業者において、ホワイトリストの作成方法が異なるため、共通する観点を記載する。

表 5 ホワイトリストの信頼性の確認観点

項目	確認観点
ホワイトリストの作成方法	• ホワイトリストは人事情報システムから出力されているか。 • ホワイトリストは対象システムから出力したユーザ一覧自体を利用していないか。（システムへアクセスを許可されたユーザと非公開情報へアクセスを許可されたユーザが異なる場合があるため）
ホワイトリストの作成するために利用したデータの理解	• ホワイトリストを作成するために利用したデータはどのように登録されているか。（人事情報を管理するシステム間との自動連携、申請書に基づき手作業でシステムへ登録している等）

(ｲ) 権限設定の正確性、網羅性

人事情報から連携された所属に基づいて、システムに権限が正確に漏れなく設定されていることを確認した。

(ｳ) ログの網羅性の確認

ログの網羅性を確認することにより、すべてのアクセスが正確に記録されていることの心証を得て、ログ分析の基礎データとして利用した。

ログの網羅性の確認は、各事業者より、ログの保管方法と取得方法に関する資料を受領し、以下の事項を確認した。

表 6 ログの網羅性の確認観点

項目	確認観点
ログの保管方法	• ログファイルが安全に保管されているか。 • 保管場所へアクセス権限のある者のみがアクセスできる状態であるか。 • ログが改ざんされないような保護措置が講じられているか。
ログの取得方法	• ログがどのように出力されているか。 • ログに条件（特定のイベントのみを指定して出力等）を付して出力している場合、条件の設定が妥当か。

(2) アクセスログ分析の観点

アクセスログの分析は、アクセスログとホワイトリストを突合し、アクセス者の一覧を作成し、さらに有権限者と権限のない者によるアクセスに分類した。

アクセスログ分析の具体的な観点は、「表 7 分析観点と内容」に示す。

表 7 分析観点と内容

分析観点	内容
権限のない者によるアクセスの有無	権限のない者によるアクセスの有無を確かめた。 • 他社小売事業者（自社小売部門）の権限のない者のアクセス • ネットワーク事業者（自社託送部門）の権限のない者のアクセス • 委託先等（工事店等）の権限のない者のアクセス
共有 ID によるアクセス者の特定	共有 ID を利用したアクセス者を特定し、ホワイトリストで許可された権限者によるアクセスであることを確かめた。
共有 ID の利用状況の確認	共有 ID について、下記を確かめた。 • どのような状況で共有 ID が利用されるのか • 共有 ID の利用が具体的にルール化（明文化）されているか
有権限者によるアクセス日付の妥当性の確認	有権限者のアクセスについて、アクセス日時が権限付与期間内となっているかを確かめた。 （期間内の異動や退職等により、期間中にアクセス権がはく奪された場合等を想定）
有権限者によるアクセス権限の妥当性の確認	有権限者のアクセスについて、許可された権限範囲外のアクセスがないかを確かめた。 （期間内に異動等が発生しているものの、付与された権限が正確かつ漏れなく修正されていない場合等を想定）
権限のない者によるアクセスの理由確認	権限のない者がアクセスしていた場合、どのような対象者がどの程度アクセスしていたかを確かめた。 （権限のない者のアクセスにより、エラーが発生する場合であっても同様に確認した）
（論理分割[6]の場合）非公開情報にかかる画面制御の確認	システムが論理的に分割されている場合、権限のない者（一般送配電事業者以外のユーザ）がシステムにログイン後、非公開情報にアクセスできないことを確かめた。

[6] 情報遮断のためにアクセス制御を用いる手法をいう。例えば、情報システムの利用者ごとに個別の ID を付与し、所属組織に応じて閲覧権限を設定することが含まれる。閲覧権限が設定されていない利用者が情報にアクセスしようとした場合、エラー処理や情報のマスキング（符号化や空欄として返す）を行うことで、システム上の情報遮断を実現する。

2.2.3 操作ログ分析の観点

権限のない者がアクセスしていることが判明した場合については、非公開情報へのアクセス有無を確認するため操作ログを確認し、どの画面にアクセスしているか、どのような動作をしているのか（画面を表示する、検索する、出力する等）を分析した。

3. 実施スケジュール

本調査の主な実施内容について、「表 8 実施内容及びスケジュール」に示す。

表 8 実施内容及びスケジュール

実施内容		実施先	場所・手段	実施日時
全体共通	キックオフ	総合監査室	オンライン会議	令和 6 年 8 月 9 日
	9 月度月次状況共有	総合監査室	オンライン会議	令和 6 年 9 月 30 日
	10 月度月次状況共有	総合監査室	貴省会議室・オンライン会議	令和 6 年 11 月 6 日
	11 月度月次状況共有	総合監査室	貴省会議室・オンライン会議	令和 6 年 12 月 2 日
	12 月度月次状況共有	総合監査室	オンライン会議	令和 7 年 1 月 16 日
対象システム選定	事前準備	－	事務所・リモート	令和 6 年 8 月 22 日～9 月 10 日
	資料受領	－	共有ツール	令和 6 年 9 月 10 日～9 月 13 日
	リスク評価	－	事務所・リモート	令和 6 年 9 月 10 日～10 月 18 日
	対象システムの選定結果報告①（東北、中部、九州）	総合監査室	オンライン会議	令和 6 年 10 月 4 日
	対象システムの選定結果報告②（東京、関西、四国、沖縄）	総合監査室	メール	令和 6 年 10 月 11 日
	対象システムの選定結果報告③（北海道、北陸、中国）	総合監査室	メール	令和 6 年 10 月 18 日
ログ分析	ログ依頼事前 MTG①	東北、中部、九州	オンライン会議	令和 6 年 10 月 10 日～10 月 16 日
	ログ依頼事前 MTG②	東京、関西、四国、沖縄	オンライン会議	令和 6 年 10 月 18 日～10 月 24 日

実施内容		実施先	場所・手段	実施日時
	ログ依頼事前 MTG③	北海道、北陸、中国	オンライン会議	令和 6 年 10 月 25 日～10 月 28 日
	パイロットテスト	－	事務所・リモート	令和 6 年 10 月
	アクセスログ分析	－	事務所・リモート	令和 6 年 11 月～令和 7 年 1 月
	操作ログ分析	－	事務所・リモート	令和 6 年 12 月～令和 7 年 1 月
報告	中間報告	総合監査室	貴省会議室・リモート	令和 7 年 2 月 6 日
	最終報告	総合監査室	貴省会議室・リモート	令和 7 年 2 月 28 日

4. 実施担当者

本プロジェクトの体制を、「表 9 実施担当者一覧」に示す。

表 9 実施担当者一覧

所属・氏名	役割	実施内容
XXX	統括責任者	• 本プロジェクトにおける統括責任者
XXX	執行責任者 1	• 本プロジェクトにおける責任者
XXX	執行責任者 2	• 本プロジェクトにおける品質責任者
XXX	リーダー	• 本プロジェクトの進捗管理 • 課題管理 • リソース管理 • 各種調整
XXX	サブリーダー	• 本プロジェクトの進捗管理 • 課題管理 • 品質管理

所属・氏名	役割	実施内容
XXX	システム監査	• 本プロジェクトの進捗管理・品質管理の補佐 • リスク評価の実施 • 各事業者とのやり取り • ログ分析担当への作業指示、結果確認 • 実施報告書作成
XXX	システム監査	• リスク評価の実施 • 各事業者とのやり取り • ログ分析担当への作業指示、結果確認 • 実施報告書作成
XXX	システム監査	• リスク評価の実施 • 各事業者とのやり取り • ログ分析担当への作業指示、結果確認 • 実施報告書作成
XXX	システム監査	• リスク評価の実施 • 各事業者とのやり取り • ログ分析担当への作業指示、結果確認 • 実施報告書作成
XXX	システム監査	• 各事業者とのやり取り • ログ分析担当への作業指示、結果確認
XXX	執行責任者 3	• ログ分析における全体管理
XXX	データ分析	• ログ分析の品質管理 • ログ分析の課題管理 • ログ分析のリソース管理 • データ分析方法のアドバイス
XXX	データ分析	• 担当事業社のパイロットテスト、アクセスログ分析、操作ログ分析 • ログ分析結果の作成

所属・氏名	役割	実施内容
XXX	データ分析	• 担当事業社のパイロットテスト、アクセスログ分析、操作ログ分析 • ログ分析結果の作成
XXX	データ分析	• 担当事業社のパイロットテスト、アクセスログ分析、操作ログ分析 • ログ分析結果の作成
XXX	アドバイザー	• 本プロジェクトの推進に係るアドバイス
XXX	アドバイザー	• 本プロジェクトの推進に係るアドバイス
XXX	アドバイザー	• 本プロジェクトの推進に係るアドバイス
XXX	アドバイザー	• 本プロジェクトの推進に係るアドバイス
XXX	アドバイザー	• 本プロジェクトの推進に係るアドバイス
XXX	アドバイザー	• 本プロジェクトの推進に係るアドバイス

II　総合所見

1.　調査結果総括

本調査で識別した検出事項は以下のとおり分類した。

表 10 検出事項の分類

分類	内容
発見事項	ログ分析の結果、発見された問題 具体的には、非公開情報の管理の用に供するシステムについて、特定された者以外も当該情報を入手することができている状況が確認された場合を指す
気づき事項	ログ分析の過程で見つかった問題、課題等の改善が望ましい事項

非公開情報の管理の用に供するシステムについて、10 事業者各 1 システムのアクセスログ分析を実施した結果、特定された者のみが当該情報を入手することができることを確認し、調査した 1 か月分の範囲内において、発見事項は識別しなかった。

しかしながら、本調査の過程において、システムの運用管理に関し、9 件の気づき事項を検出している。

気づき事項を分類し、アクセス権管理に関し、以下の 3 つの課題が挙げられる。

(1) 共有 ID の管理不徹底

複数の事業者で共有 ID が使用されているが、共有 ID の貸出記録に誤りや漏れが発生しているなど、その管理が徹底されていないことが確認された。具体的には、以下のようなケースが見受けられた。

- 利用の都度、貸出記録を残す運用ルールが定められているものの、記録が残されていなかったケース
- 災害対応訓練時に利用する共有 ID について、訓練時の設定不備により利用ができなかったため、記録が残されていなかったケース

共有 ID の貸出管理がルール通りに実施されておらず、記録に不備がある場合、共有 ID の利用者及び操作内容の特定が困難となるリスクがある。

(2) アクセス権の管理ルール不徹底

担当者がアクセス権付与に関するルールを認識しておらず、ルール通りにアクセス権が管理されていない状況が確認された。具体的には、以下のようなケースが見受けられた。

- 休職者に対してアクセス権が付与されていたケース
- 人事情報に紐づかない ID について、利用者名が未登録のまま利用されていたケース

アクセス権管理に関するルールが徹底されない場合、休職者等のシステム利用が必要のない者にアクセス権が付与され、非公開情報への不正なアクセスや不正利用のリスクが高まる。また、特別 ID については、利用者の特定が困難となり、正確なアクセス権管理ができなくなるリスクがある。

(3) アクセス権の棚卸未実施

定期的な ID の棚卸が一部のユーザに対して実施されていないことが確認された。具体的には以下のケースが見受けられた。

- 社外ユーザの棚卸を実施する運用としていなかったケース
- 社員外の一部ユーザについて、権限の設定状況の妥当性確認は実施していたものの、アクセス権の要否の確認が実施されていなかったケース
- 定期的な棚卸を実施することがルールに定められているものの、実施時期や頻度が明確になっておらず、棚卸が 1 年以上実施されていなかったケース

アクセス権の発見的統制の不足により、アカウントのなりすまし等不正利用のリスクが高まる。また、不要なアカウントが多数存在する場合、システムのパフォーマンス低下や管理の複雑性が増大するリスクがある。

以上の課題を踏まえ、以下に所見と改善方針を示す。

共有 ID について、各事業者では人員の入替わりが頻繁である業務における利用や災害利用、臨時利用等の一時的な利用を目的にしているケースが多く見受けられた（東北、中部、北陸、関西）。

しかしながら、共有 ID の貸出に関する規程・マニュアル類が整備されていたとしても、共有 ID を利用する人数が多いこと、貸出やパスワード管理が手作業であること、一時的な利用者が使用すること等に起因して、利用者全員に運用を徹底させることが困難になり、意図した統制が行われないケースが生じやすいと考えられる。

そのため、共有 ID については、まず ID 数を必要最低限にし、利用場面も限定すること、利用上のポリシーを明確にし、周知することが望ましい。そのうえで、共有 ID の払出しにあたっては、システム上で管理し自動的に貸出の記録を残す、貸出期間経過後は ID を自動的に利用できなくするなどの仕組みを検討することが望まれる。また、セキュリティ強化の対策として多要素認証の利用も有効である。なお、現行の運用を変更することが難しい場合、管理ルールの周知徹底とともに、共有 ID の利用がルール通り実施されていることを定期的にモニタリングする仕組みを導入することが望まれる。

アクセス権の管理ルール不徹底について、ルール通りに運用するために、全担当者へルールの重要性を再周知し、教育・訓練を実施することが重要である。そのため、休職者や特別 ID に対するアクセス権の付与について、ルールが明確であるかを再確認し、全担当者に周知徹底することが望まれる。アクセス権の付与・変更時には、ルール通りの申請であるか、権限設定に誤りがないかを確認するレビュー体制を整備するなど、誤

りを防止する対策が望まれる。また、人的ミスを減少させるため、休職者が発生した場合、自動的にアクセス権を無効化するなど、アクセス権の付与や削除プロセスの自動化を検討することが望ましい。

不要なアクセス権の残存期間が長いほど、より不正利用のリスクが高まる懸念があることから、アクセス権の棚卸については、すべての利用ユーザを対象に、あらかじめ具体的な実施時期や実施頻度を定めたうえで、行うことが望ましい。なお、権限の削除や無効化するための申請や依頼は、利用者の利便性を下げることから、自発的に行われないケースがあることを考慮する必要がある。最終ログイン日時等が記録されるシステムであれば、一定期間以上ログインしていない対象ユーザについて、自動で当該ユーザのアクセス権を無効化するなどの対応を検討することが望まれる。なお、削除や無効化を自動で行うことが難しい場合、利用者自ら申請、依頼するよう定期的に通知するなどの対応を検討することが望まれる。

本調査の中で検出した気づき事項を各事業者に伝達し、事業者の改善方針を確認している。改善策を実施することにより、非公開情報への不正なアクセスのリスク、共有 ID の利用者及び操作内容の特定が困難となるリスク、アカウントの不正利用のリスク等を低減し、非公開情報の管理の用に供するシステムのアクセス権管理に係るセキュリティを向上させることが期待される。

各事業者の分析結果の詳細は個別所見に記載した。

2. 検出事項

本調査における検出事項の件数について、以下、「表 11 各事業者の検出事項の件数」に示す。各事業者の気づき事項の概略は「表 12 気づき事項一覧」に示す。

表 11 各事業者の検出事項の件数

分類	総数	対象事業者	件数
発見事項	0 件	－	0 件
気づき事項	9 件	東北電力ネットワーク株式会社	2 件
		東京電力パワーグリッド株式会社	1 件
		中部電力パワーグリッド株式会社	1 件
		北陸電力送配電株式会社	2 件
		関西電力送配電株式会社	2 件
		九州電力送配電株式会社	1 件

表 12 気づき事項一覧

#	対象事業者	カテゴリー	概略
1	東北電力ネットワーク株式会社	アクセス権の管理ルール不徹底	休職者にアクセス権を付与していた
2		共有 ID の管理不徹底	共有 ID の貸出記録に記載誤り・漏れがあった
3	東京電力パワーグリッド株式会社	アクセス権の棚卸未実施	社外ユーザのアクセス権の定期的な棚卸が実施されていなかった
4	中部電力パワーグリッド株式会社	共有 ID の管理不徹底	非常災害対応用の共有 ID の貸出記録が残されていなかった。また、記録不備によりパスワード変更がされず利用可能な状況のまま放置されていた
5	北陸電力送配電株式会社	共有 ID の管理不徹底	共有 ID の貸出記録に記載誤り・漏れがあった
6		アクセス権の棚卸未実施	一部の社員外ユーザにおいて在籍状況と照らしたアクセス権の要否の確認が実施されていなかった
7	関西電力送配電株式会社	アクセス権の管理ルール不徹底	一部の個人利用の特別 ID が利用者名で登録されていなかった
8		共有 ID の管理不徹底	共有 ID の貸出記録に記載漏れがあった
9	九州電力送配電株式会社	アクセス権の棚卸未実施	規程には定期的な ID 棚卸を行うことが定められているものの、申請ユーザを対象とした ID 棚卸は、前回実施から 1 年以上経過していた

III 個別所見

1. 各社の評価結果

1.1 北海道電力ネットワーク株式会社

1.1.1 対象システムの選定

1.1.1.1 対象システムの選定結果の概要

北海道電力ネットワーク株式会社（以下「北海道電力 NW」という。）は、①NW 情報管理システム、②託送業務システム、③配電総合システム、④設備計画システムを対象にシステム選定のためのリスク評価を実施した。

リスク評価の結果は以下のとおり。

表 13 リスク評価結果（北海道電力 NW）

システム名	システム重要度スコア	リスクの発生可能性評価スコア	トータルスコア
NW 情報管理システム	XX	XX	XX
託送業務システム	XX	XX	XX
配電総合システム	XX	XX	XX
設備計画システム	XX	XX	XX

北海道電力 NW は一部（共有 ID 管理手順やバックアップ手続等）に各システム固有の統制があるものの、「XXX」「XXX」等により、システム間で概ね同様に統制が整備されている状況であり、大規模障害の発生等も確認されなかった。

託送業務システムは、年間アクセス数が約 XXX,XXX 件、連携するシステム数は X つであり、アクセス数やインターフェースボリュームは中程度である。一方、託送業務に関連し託送情報を保持していること、社外公開機能を有していることに加え、複数の機能を持つオンプレミスサーバ群とクラウドサービスのサーバが混在している。また、X つのスクラッチシステムと X つのパッケージシステムから構成されており、システム構成の複雑性は高いこと、X つの機能ごとに X つから X つの権限区分を有しており、セキュリティモデルは複雑であると判断したこと等からログ調査の対象システムに選定した。

1.1.2 システムログの分析

1.1.2.1 ログの分析

1) アクセスログの分析結果の概要

託送業務システムの 2024 年 7 月の端末操作ログを対象に、パイロットテスト及びアクセスログ分析を実施した。

表 14 ログ分析に利用したデータ一覧（北海道電力 NW）

データ名	概要
託送業務システム利用可能ユーザ一覧	サブシステム毎の非公開情報にアクセス可能な者の名簿
アクセスログ_異動連携制御機能（TIC）	異動連携制御機能（TIC）の 1 か月分のアクセスログ
アクセスログ_高圧料金計算機能（HUB）	高圧料金計算機能（HUB）の 1 か月分の操作ログ
アクセスログ_託送業務統括機能（WORCS）	託送業務統括機能（WORCS）の 1 か月分のアクセスログ
アクセスログ_託送社外公開機能（SHIP）	託送社外公開機能（SHIP）の 1 か月分のアクセスログ
アクセスログ_低圧料金計算機能（TFP）	低圧料金計算機能（TFP）の 1 か月分のアクセスログ

(1) アクセスログ分析の対象ログ

サブシステムごとにログが存在しており、各サブシステムから取得した 2024 年 7 月分のログを分析に利用した。なお、サブシステムのうち高圧料金計算機能（HUB）はアクセスのみを記録したログは存在しないため、操作ログを分析に利用している。

(2) ホワイトリストの信頼性の確認

事業者が、以下の情報をもとに、手作業で作成した名簿をホワイトリストとして利用した。ホワイトリストを作成するために利用した情報について、以下を確認しデータの信頼性は担保されていると判断した。

表 15 データの信頼性の確認結果（北海道電力 NW）

利用情報	概要	データの信頼性の確認結果
全社ユーザ一覧（7 月 1 日、8 月 1 日時点）	人事情報に基づき、各システムの認証情報を一元管理する全社共通システム（利用者 ID 管理システム）から出力した、全社ユーザ情報である。 北海道電力 NW 及び北海道電力 HD の従業員以外（派遣社員、ほくでん情報テクノロジーなど）は、利用者情報 ID 管理システムに個別登録される。	人事情報から連携したデータをもとにしており、網羅性、正確性について十分な心証を得た。 また、個別登録の情報については北海道電力 NW が以下により 7 月時点のユーザ在籍状況を確認の上、個別登録情報と整合していることを確かめている。 ・派遣社員：派遣期間を管理している「受入一覧」及び在籍している派遣社員が記載された「請求書」の閲覧 ・ほくでん情報テクノロジー：グループ会社の人事異動情報の閲覧 このことから、網羅性、正確性について十分な心証を得た。
認可条件情報（サブシステム毎）	申請に基づきサブシステム毎に所属・役職・雇用形態単位で定義されたアクセス認可条件情報である。	各サブシステムからすべての設定データを出力した情報であり、網羅性、正確性について十分な心証を得た。
ユーザ毎の権限設定情報 ※HUB、SHIP のみ	申請に基づきユーザ単位でサブシステム毎に定義された権限情報である。	各サブシステムからステータスが有効な全データを出力した情報であり、網羅性、正確性について十分な心証を得た。
7 月度の人事発令情報	7 月中の人事異動・採用・退職情報である。	人事情報であり、網羅性、正確性について十分な心証を得た。

(3) ログデータの網羅性

ログ保管に関する資料及びログ取得手順の閲覧並びに事業者への質問により、アクセスログ及び操作ログの網羅性を確認した。

ログの保管方法は以下の 2 通りであり、いずれのシステムも、改ざんを防止するため、通常のシステム利用者や第三者がアクセスできない場所に保管している。

なお、ログを取得する際は、作業の都度、サーバ上に導入した管理ツールから特権

ID のパスワードを発行することで、特定の者のみがログにアクセスすることが可能な運用である。

① システムサーバ内に DB で保管（高圧料金計算機能（HUB）、託送社外公開機能（SHIP）が該当）

② システムサーバ内にログファイルで保管（低圧料金計算機能（TFP）、異動連携制御機能（TIC）、託送業務統括機能（WORCS）が該当）

また、ログ取得時の条件について、サブシステム毎に以下の通りであることを確かめた。

表 16 サブシステム別のログ取得条件及び網羅性の確認結果

サブシステム	取得条件及び網羅性の確認結果
託送社外公開機能（SHIP）	分析で利用したアクセスログは、対象月（7 月）の全ログのうち、USER_ID が X 桁（社内ユーザ）のログに限定している。 当該サブシステムは小売電気事業者を含む社外ユーザ（USER_ID が XX 桁）によるアクセスがあるが、システムへのアクセス経路が異なること並びに、仕様書及び実機画面の閲覧により社外ユーザは自社以外の情報（非公開情報）へのアクセスができない仕組みであることが確かめられたため、社外ユーザのログを分析対象から除外した。
高圧料金計算機能（HUB）	分析で利用したログは対象月（7 月）の全ログを対象としており、網羅性について十分であると心証を得た。
託送業務統括機能（WORCS）	
異動連携制御機能（TIC）	
低圧料金計算機能（TFP）	

以上より、ログデータの網羅性について心証を得たため、データ分析に利用可能と判断した。

(4) システム上の権限設定状況の確認

北海道電力 NW への質問及び資料の閲覧により、XXX に応じたアクセス制御が行われることを確かめた。

(5) アクセスログの月次分析

1 か月分の託送業務システムへのアクセスに係るログを抽出し、ホワイトリストと

照合した。ホワイトリストに記載されたユーザを有権限者、記載のないユーザを権限のない者と識別しアクセスしたユーザを分類した。

さらに、有権限者については、ユーザ ID が個人別に付与された ID か、共有 ID かに分類した。

上記分類に基づき、権限毎のアクセス状況を以下に示す。

表 17 アクセス状況（北海道電力 NW）

分類 1	分類 2	サブシステム	ID 数	所属	所属別 ID 数	アクセス回数※	アクセス回数/所属別 ID 数
権限のない者	—	HUB	X	–	X	XXX	XXX.XX
有権限者	個人別 ID	SHIP	XX	北海道電力 NW	XX	X,XXX	XX.XX
				ほくでん情報テクノロジー	X	XX	X.XX
		HUB	XX	北海道電力 NW	XX	XXX,XXX	XXXX.XX
				ほくでん情報テクノロジー	X	XXX	XXX.XX
		TIC TFP WORCS	XXX	北海道電力 NW	XXX	X,XXX	XX.XX
				ほくでん情報テクノロジー	X	XX	X.XX
	RPA[7]利用 ID	HUB	X	北海道電力 NW	X	X,XXX	X,XXX.XX
		WORCS	X	北海道電力 NW	X	XX	XX.XX

※HUB は操作ログを分析に利用しているため、アクセス回数ではなく、ログ件数を記載している。

アクセスログの分析結果に基づき、操作ログ分析の対象となるか、以下の検討を実施した。

- 権限のない者によるアクセスの検討

  高圧料金計算機能（HUB）において権限のない者の XID によるアクセスが検出（XXX 件）されたものの、北海道電力 NW への質問により、検出された XID はシステムユーザであり、該当 ID によるログは人が操作したログではなくシステム内部処理に伴う操作ログであることを確かめた。よって、権限のない者によるアクセスは行われていないと判断し、追加調査の対象外とした。

[7] RPA (Robotic Process Automation): RPA は、ソフトウェアロボットや「ボット」を使用して、定型的で繰り返し行われる業務プロセスを自動化する仕組みをいう。

- 共有 ID の検討

RPA 用ユーザ ID が存在するが、北海道電力 NW への質問により以下が確かめられたため不正利用のリスクは低いと判断し、共有 ID としては識別せず、追加調査の対象外とした。

・ ログイン情報を把握しているユーザが X 名（XXXX (RPA 保守を担当する部署)に所属）に限定されている
なお、X 名中 X 名は個人 ID としても権限が付与されており、X 名は個人 ID としては権限が付与されていないものの、RPA の保守に限り RPA から RPA 用ユーザのログイン情報を利用してアクセスを許可されたユーザである
・ 異動などで利用者が変更となる場合はパスワード変更する運用である

- 有権限者によるアクセス日付の妥当性の確認(有効期間外のアクセス）

ホワイトリストは異動・退職が反映されたリストになっているため、アクセス時点の所属が紐づけ可能となっており、有効期間外のアクセスがあった場合は権限のない者として検出される。システムユーザを除き権限のない者のアクセスはなかったことを確かめた。

- 有権限者によるアクセス権限の妥当性の確認

権限は人事情報と連動し設定されているため、許可された権限範囲以外のアクセスができない仕組みとなっている。なお、ホワイトリストは異動・退職が反映されたリストになっているため、異動により権限が変更になったにもかかわらずアクセスが行われた場合は権限のない者として検出される。システムユーザを除き権限のない者のアクセスはなかったことを確かめた。

- 権限のない者によるアクセスの理由確認

権限のない者によるアクセス実績がなかったため、追加検討は行わなかった。

- 非公開情報にかかる画面制御の検討

託送社外公開機能（SHIP）以外のサブシステムは論理分割に該当しないため、画面制御の検討は行わなかった。

託送社外公開機能（SHIP）においては、前述（1.1.2.1 1）(3）ログデータの網羅性)の通り小売事業者のアクセスがあるため、小売事業者がシステムにログイン後、非公開情報にアクセスできないことを確認した。

仕様書を閲覧するとともに、小売事業者によるアクセス時の各メニューについて、全 X メニューの実機画面の閲覧により、自社以外の情報が表示されないよう制御が行われていることを確かめた。

以上より、非公開情報にかかる画面制御が実装されている心証を得た。

2) 操作ログの分析結果の概要

アクセスログ分析の結果、権限のない者によるアクセスは行われていないことが確かめられたため、操作ログの分析は不要であると判断した。

1.1.3 結論

本調査の範囲において、非公開情報の管理の用に供するシステムである託送業務システムのログ分析の結果、非公開情報を入手可能な者によるアクセスのみが識別され、特定された者のみが当該情報を入手することができることになっていた。

1.1.4 検出事項

ログ分析の結果、非公開情報へ権限のない者によるアクセスは識別されず、検出事項はなかった。

1.2 東北電力ネットワーク株式会社

1.2.1 対象システムの選定

1.2.1.1 対象システムの選定結果の概要

東北電力ネットワーク株式会社（以下「東北電力 NW」という。）は、①エリア需要実績管理システム、②営業オンライン、③ロードカーブデータ収集処理システム、④契約センターシステムを対象にシステム選定のためのリスク評価を実施した。

リスク評価の結果は以下のとおり。

表 18 リスク評価結果（東北電力 NW）

システム名	システム重要度スコア	リスクの発生可能性評価スコア	トータルスコア
エリア需要実績管理システム	XX	XX	XX
営業オンライン	XX	XX	XX
ロードカーブデータ収集処理システム	XX	XX	XX
契約センターシステム	XX	XX	XX

東北電力 NW は「XXX」や「XXX」等により、各システムは概ね同様に統制が整備されている状況であり、大規模障害の発生等も確認されなかった。一方で、営業オンラインは、託送業務及び営業業務を行うシステムであることに加え、ユーザ数が多いこと（XX,XXX 名（うち社外ユーザ X,XXX 名）、アクセス数が年間 XXX,XXX,XXX 件と他システムと比較し多いこと、約 XX システムと接続するシステムであり他システムとの連携が多いこと等から、ログ調査の対象システムに選定した。

1.2.2 システムログの分析

1.2.2.1 ログの分析

1) アクセスログ分析結果の概要

営業オンラインの 2024 年 7 月の端末操作ログを対象に、パイロットテスト及びアクセスログ分析を実施した。

表 19 ログ分析に利用したデータ一覧（東北電力 NW）

データ名	概要
端末操作ログ ※アクセスログ	PC 端末における営業オンラインの認証ツール及びエミュレータの起動ログ（7 月分） アクセスログとして利用するログ情報
端末統計ログ ※操作ログ	営業オンラインシステムにて管理しているログ（7 月分） 操作ログとして利用するログ情報
XXX_OperationLog_Layout	端末統計ログのヘッダ情報
情報機器管理台帳	日々の端末一覧
ユーザ情報	ユーザ情報（人事情報に基づく利用者情報 DB より抽出）
権限設定情報	システムに付与した権限設定情報（利用権限管理システムより抽出）
端末操作ログ ※操作ログ(印刷)	端末操作ログより，営業オンラインを利用する XXX エミュレータソフトから印刷を実施したログ（7 月分）
委託業務管理ログ（操作ログ）	営業オンラインシステムのサブシステム委託業務管理のログファイル（7 月分）
給付金管理ログ（操作ログ）	営業オンラインシステムのサブシステム給付金管理のログファイル（7 月分）
XXX_XXX_OperationLog_Layout	委託業務管理ログ、給付金管理ログのヘッダ情報

(1) アクセスログ分析の対象ログ

営業オンライン上にアクセスログに該当するログはないため、PC 端末における営業オンラインの認証ツール及びエミュレータの起動ログをアクセスログとして分析に利用した。

(2) ホワイトリストの信頼性の確認

東北電力 NW でホワイトリストは作成していないことから、当法人にて以下の情報をもとに権限者リストを作成し、ホワイトリストとして利用した。

ホワイトリストを作成するために利用した利用権限管理システムの情報と利用者情報 DB のデータについて、以下を確認しデータの信頼性は担保されていると判断した。

表 20 データの信頼性の確認結果（東北電力 NW）

利用情報	概要	データの信頼性の確認結果
利用者情報 DB の情報	人事情報及び個別申請に基づく全社員の利用者情報を管理する DB 情報である。利用者と所属情報を保持している。	人事情報から連携したデータをもとにしており、網羅性、正確性について十分な心証を得た。 また、個別登録の情報について以下を確認し、網羅性、正確性について一定の心証を得た。 ・東北電力 NW による、個別登録の情報と ID カード申請情報の突合の結果、個別登録の情報と在籍状況が整合していることを確かめた。なお、対象多数のため、アクセス実績のあった NW 権限の ID を確認対象とした。 ・「XXX」の閲覧及び東北電力 NW への質問により、現品確認ルールとして「ＩＤカード管理表」を作成して XXX の ID カードの現品確認を行っており、不整合があった場合は発見できる運用であることを確かめた。
利用権限管理システムの情報	全システムの権限を管理するシステムである。所属と所属に紐づく営業オンラインシステムの権限設定を保持している。	利用権限管理システムから営業オンラインに関する設定情報を全件出力している。 また、所属と所属に紐づく権限設定情報を通査し、自社小売事業者の所属に NW 権限が設定されているなどの不審な点がないことを確かめたことから、網羅性、正確性について十分な心証を得た。

(3) ログデータの網羅性

ログ保管に関する資料及びログ取得手順の閲覧並びに東北電力 NW への質問により、アクセスログ及び操作ログの網羅性を確認した。

- アクセスログ

アクセスログ分析で利用した端末操作ログはセキュリティ管理システムに保管されておりシステム利用者や第三者がアクセスできない場所に保管している。

また、アクセスログ分析で利用した端末操作ログは、XXX（ログ取得ソフト）により取得した PC 端末の全操作ログのうち、営業オンラインの認証ツールとエミュレータの起動ログに限定して抽出している。営業オンラインシステムへのアクセス時には XXX が必要となるため、当該ログに限定することとした。なお、東北電力 NW 及び東北電力のユーザが営業オンラインにアクセスできる環境は、XXX に限られており、すべての XXX には XXX ログ取得ソフトが導入されているとの回答を得ている。

以上より、ログデータの網羅性について心証を得たため、データ分析に利用可能と判断した。

- 操作ログ

操作ログ分析で利用した端末統計ログは、営業オンライン上に保管されておりログを編集するような機能はなく、バッチ処理により XXXX 日＋1 日で削除が実行される仕様である。また、操作ログ分析で利用した端末統計ログについて、全件取得しているとの回答を得ている。

以上より、ログデータの網羅性について心証を得たため、データ分析に利用可能と判断した。

(4) システム上の権限設定状況の確認

東北電力 NW への質問及び設計書の閲覧により、権限設定について、NW 権限と HD 権限があることを確かめた。

表 21 権限設定の概要（東北電力 NW）

権限の種類	権限の内容
NW 権限	非公開情報にアクセス可能な権限
HD 権限	非公開情報にアクセス不可の権限 ※非公開情報はマスキングされ表示されない

(5) アクセスログの月次分析

1 か月分の端末操作ログから営業オンラインの起動に係るログを抽出し、ホワイトリストと照合した。ホワイトリストに記載されたユーザを有権限者、記載のないユー

ザを権限のない者と識別し、アクセスしたユーザを分類した。

さらに、有権限者については、ユーザ ID が個人別に付与された ID か、共有 ID かに分類した。

上記分類に基づき、権限毎のアクセス状況を以下に示す。

表 22 アクセス状況（東北電力 NW）

分類 1	分類 2	権限	ID 数	所属	所属別 ID 数	アクセス回数	アクセス回数/所属別 ID 数
権限のない者	—	—	XX	本店 X 支社 原子力発電等	XX	XXX	XX.XX
有権限者	個人別 ID	NW 権限	X,XXX	本社	XXX	XX,XXX	XX.XX
				支社 （X 支社合算）	X,XXX	XX,XXX	XX.XX
		HD 権限	X,XXX	本店	XXX	XX,XXX	XX.XX
				支店 （X 支店合算）	XXX	X,XXX	XX.XX
	共有 ID	NW 権限	XXX	本社	XXX	XX,XXX	XX.XX
				支社 （X 支社合算）	XX	XXX	XX.XX
		HD 権限	X,XXX	本店	X,XXX	XX,XXX	XX.XX
				支店 （X 支店合算）	X	XX	X.XX

アクセスログの分析結果に基づき、操作ログ分析の対象となるか、以下の検討を実施した。

- 権限のない者によるアクセスの検討

  権限のない者によるアクセスが XXID 検出されている。東北電力 NW への質問により、XXID のうち XID（XXX）のログはシステム処理（PC 端末のツールや OS の内部処理）で生成されるログであり、権限のない者によるアクセスではないと判断し、追加調査の対象外とした。残りの XXID について、アクセスログは PC 端末上の営業オンラインの認証アプリ実行ログであり権限がなくても実行はできるため、XXX に認証エラーとなっていることが想定される。実際に営業オンラインを操作していないことを、操作ログから確認することにした。

- 共有 ID の検討

  HD 権限について、共有 ID の利用用途を確認した結果、システム利用の共有 ID が XXX 件、個人利用の共有 ID が X,XXX 件であった。システム利用の ID は主に

RPA 及び共有メールアドレス用に利用されていた。個人 ID については、主に日々入れ替わりのある人員（派遣社員、カスタマーセンターの委託先社員等）のための利用となっており、利用の都度貸出管理が行われている。HD 権限は小売事業者も利用可能な画面に限定された権限であり、不正利用のリスクは低いため、詳細な検討は実施しない方針とした。

NW 権限について、共有 ID の利用用途を確認した結果、システム利用の共有 ID が XXX 件、個人利用の共有 IDXXX 件であった。システム利用の共有 ID は主に RPA 及びマクロツール用に利用していた。個人利用の共有 ID については、主に日々入れ替わりのある人員（派遣社員、契約センターの委託先社員、臨時員等）のための利用となっており、利用の都度貸出管理が行われている。NW 権限はすべての画面を利用可能な権限であり、不正利用のリスクが高いため、詳細な検討を実施した。

対象の共有 ID（XXXID）について、共有 ID の管理者から、7 月の共有 ID の貸出しを管理している「ID カード利用管理表」を入手した。「ID カード利用管理表」とアクセスログを、ID 及びアクセス日付をキーに突合した結果、XXXID において対応する「ID カード利用管理表」が残されており、管理者による承認の上で利用していることを確かめた。また、XID については「ID カード利用管理表」の閲覧により 7/3 から個人 ID カードとして利用していること及び、7/2 以前のログがないことから共有 ID としての利用がないことが確かめられたため対象外とした。残りの XXID について、アクセスログ XXX 件中 XX 件に対応する利用記録が残されていなかった。東北電力 NW は、記録が残されていなかったログについて、対象 ID の利用部門の「稼働表」及び「ID カード利用管理表」等の閲覧並びに本人及び ID カード利用責任者への聞き取りをもとに、利用者及び記録が残されていなかった背景について特定した。特定した内容について以下の通り回答を得た。

■利用者

XXID のうち、XID（アクセスログ X 件）は東北電力 NW 社員の利用、XXID（アクセスログ XX 件）については業務委託先の利用であった。

特定した利用者について「利用者情報 DB」の氏名と照合し、特定した所属に対する権限を「利用権限管理システム」で確認した結果、NW 権限が設定されている部署に所属していることが確かめられたため、有権限者による利用であると判断した。

■記録が残されていなかった背景

記録が残されていなかった背景を ID/ログ毎に以下の通り分類した。総じて、共有 ID の利用者及び ID カード利用責任者における、ルールや手順の理解不足並びに運用不徹底によるものであった。なお、同一の ID で複数のログがあり、それぞれ異なる背景で記録が残されていなかったケースがあるため、ID は一部重複している。

・XID/ログ X 件：配電業務のシステム使用にあたり，カードの利用権限を確認

するために起動したが，確認行為のみであったことから，「ID カード利用管理表」に記載は不要と安易に判断したもの。

・XID/ログ X 件：利用承認者が 7 月転入者であり、着任日当日の 7/1 の段階では業務運用の理解が不十分だったことから、「ID カード利用管理表」の記載が漏れたもの。

・XID/ログ X 件：スマートメーター遠隔操作業務を行う利用者に貸与する ID カードについて、「ID カード利用管理表」を記載する必要があったが記載が漏れていたもの。

・XID/ログ X 件：管理者業務を実施していた利用者が，スマートメーター遠隔操作業務を行うため追加した ID カードについて，「ID カード利用管理表」を記載する必要があったが記載が漏れていたもの。

・XXID/ログ XX 件：利用者への ID カード貸与時に「ID カード利用管理表」を記載する必要があったが、記載が漏れていたもの。

・XID/ログ X 件：既に業務を実施している利用者に対し追加で貸与する ID カードについて、「ID カード利用管理表」を記載する必要があったが記載が漏れていたもの。

・XID/ログ X 件：当該 ID は、管理者が電話受付履歴の確認や電話受付者のモニタリングを行う業務で使用しており、業務において同一の利用者が X 台の端末を使用する。そのため、X 台分の「ID カード利用管理表」への記入が必要となるが、X 台分の記入のみが行われ、X 台分の記入が漏れたもの。

・XID/ログ X 件：当該利用個所では共有 ID カードの利用時に紙媒体の管理表に手書きし、月分集計時に電子媒体の管理表へ転記する運用としているが、転記の際に記載が漏れたもの。

- 有権限者によるアクセス日付の妥当性の確認(有効期間外のアクセス)

ホワイトリストは異動が反映されたリストになっているため、アクセス時点の所属が紐づけ可能となっている。対象期間において、退職者によるアクセスは検出されなかった。休職者・出向者によるアクセスは、XXID 検出された。

休職者・出向者によるアクセスの妥当性を会社に質問し、XID は復職による通常利用であり、有効期間外のアクセスではなかったことを確かめた。

また、営業オンラインのアクセス権限は XXX 制御されている。加えて、営業オンライン上の XXX による XXX 権限制御も行われており、XID については XXX において利用権限が付与されていないため, 営業オンラインシステムを利用不可であると回答を得た。回答通り当該 XID について利用不可であったことを確かめるため、操作ログを確認することとした。

その他 XID について、休職中のため XXX において利用権限が付与されていなかったものの、休職期間中である 7/1 付で組織整備に伴う異動があり、その際にそのほかの事業所異動者と一括で XXX の利用申請がなされたことにより、営業オンラ

インが利用できる状態となった。異動発令後に利用権限が変更された情報を得たことから、営業オンラインの利用可否を確認するため，営業オンライン起動ツールを実行し確認を行っていた。当該 XID については操作ログを確認することとした。

- 有権限者によるアクセス権限の妥当性の確認

  権限は、人事情報と連動し設定されているため、許可された権限範囲以外のアクセスができない仕組みとなっている。また、人事情報の反映は、異動日から新所属情報に更新されタイムラグのない運用となっていることから、期間外に権限範囲外のアクセスが行われるリスクは低いと判断した。

- 権限のない者によるアクセスの理由確認

  東北電力 NW への質問により、権限のない者によるアクセスとして検出された XXID によるアクセスについて、権限がないにもかかわらずアクセスを行った理由を確認した結果、以下の回答を得た。いずれも 7/1 付の異動者に関連するアクセスであり、不正の兆候は見られなかった。

  ・ 2024/7/1 付の異動者（XID）：7 月定期異動で発令着任後，起動不可であることを確認するため XXX したもの
  ・ 2024/7/1 付の異動者（XID）：端末スタートアップの設定解除漏れにより XXX が自動起動したもの
  ・ PC 端末の設定変更作業用ローカルアカウント（XID）：異動期の設定変更ツールの実行時に，端末スタートアップに設定された XXX が自動起動したもの

- 非公開情報にかかる画面制御の検討

  東北電力 NW から当該システムにおける「非公開情報へのアクセス制御画面一覧」を入手し、特定した計 XXX 画面から XX 画面を無作為に抽出し、NW 権限及び HD 権限の ID の操作画面スクリーンショットを確認した。

  確認の結果、HD 権限の ID では画面上の情報がマスキングされており、非公開情報が閲覧できないことを確かめた。

  以上より、非公開情報にかかる画面制御が実装されている心証を得た。

2) 操作ログの分析結果の概要

アクセスログ分析の結果、以下の操作ログを分析した。

(1) 権限のない者によるアクセス

権限のない者によるアクセスの検討において識別した XXID の操作ログを入手し確認した結果、対象ユーザによる操作ログがなかったことを確かめた。アクセスログは XXX の実行ログのため、権限がなくても実行はできるが、操作ログは残らない。以上のことから、アクセスログで識別された XXID について、操作ログがなく、権限のない者による非公開情報の取得はなかったと判断した。

(2) 休職者・出向者によるアクセス

XXX における利用権限が無くシステムを利用不可であると回答を得た XID の操作ログを入手し確認した結果、XID 中 XID について対象ユーザによる操作ログがなかったことを確かめた。残り XID については操作ログが X 件検出されたものの、総括メニュー画面の表示のみであり、非公開情報の取得は行われていないことを確かめた。以上のことから、当該 XID について、権限のない者による非公開情報の取得はなかったと判断した。

休職中にアクセス権限があった XID の操作ログを入手し確認した結果、操作ログが XX 件検出された。東北電力 NW への質問及び操作ログの閲覧により、システム利用可否確認のためにアクセスを行い、自宅等の契約情報についてデータ検索・閲覧操作をしていたものであることを確かめた。休職中ではあるものの、在籍状況としては NW 権限にて営業オンラインを利用可能なユーザであり、営業活動（小売業務）を担当するユーザではなく、取得した情報を不正に利用するリスクは低いと考えられる。

以上のことから、休職者・出向者のアクセスとして識別された XID について、権限のない者による非公開情報の取得はなかったと判断した。

1.2.3 結論

本調査の範囲において、非公開情報の管理の用に供するシステムである営業オンラインのログ分析の結果、非公開情報を入手可能な者によるアクセスのみが識別され、特定された者のみが当該情報を入手することができることになっていた。

1.2.4 検出事項

ログ分析の結果、非公開情報へ権限のない者によるアクセスは識別されなかったが、ログ分析の過程で以下の気づき事項を検出した。

1.2.4.1 検出事項 No.1

検出事項の分類	気づき事項
概要	休職者にアクセス権を付与していた
詳細	休職者に対してはアクセス権限を付与しない方針／ルールである。休職中のため XXX 利用権限が付与されていなかったものの、休職期間中である 7/1 付で組織整備に伴う異動があり、その際にそのほかの事業所異動者と一括で、XXX がなされたことにより、営業オンラインが利用できる状態となった。それにより、休職中にアクセス確認のため、営業オンラインにアクセスを行ったログが検出されている。 なお、休職中ではあるものの、在籍状況としては NW 権限にて営業オンラインを利用可能なユーザであり、営業活動（小売業務）を担当するユーザではなく、取得した情報を不正に利用するリスクは低いと考えられる。
リスク	休職者による非公開情報への不正なアクセス、不正利用のリスクが高まる。
原因	休職者へアクセス権限を付与しないルールが周知徹底されておらず、一括設定により休職者へ権限が付与された。 また、利用者本人に、託送業務目的外の利用が不適切な利用にあたることの認識がなかったことにより、休職中に営業オンラインへのアクセスが行われた。
改善の方向性	再発防止策として以下を実施、検討している。 ・休職者へアクセス権限の付与を行わないこと及び、託送業務目的外のシステム利用は禁止であることを関係者に周知徹底した。 ・従来は事業者からの申請に基づき利用権限を停止していた。加えて、XXX 利用権限を停止する運用を開始する。 ・システム上で休職者のアクセス権を無効化するよう設定することを検討する。

1.2.4.2 検出事項 No.2

検出事項の分類	気づき事項
概要	共有 ID の貸出記録（ID カード利用管理表）に記載漏れがあった
詳細	主に日々入れ替わりのある人員（派遣社員、契約センターの委託先社員、臨時員等）の利用のため共有 ID を利用しており、利用時には、ログインに必要な共有 ID カードの貸出管理により利用者を特定できるよう運用している。 しかしながら、非公開情報へアクセスが可能な NW 権限を保有する共有 ID を対象にアクセスログと貸出記録を突合した結果、貸出記録が残されていない利用を検出した（XXID、ログ XX 件）。 なお、記入が漏れていたアクセスについて、東北電力 NW の調査によって特定された利用者及び利用用途を確認した。いずれも NW 権限にて営業オンラインを利用可能な部署に所属している利用者による利用であることを確かめられたため、権限のない者による非公開情報の入手には該当しないと判断した。
リスク	正確な利用者の特定が難しくなるリスクがある。 共有 ID による不正利用のリスクが高まる。
原因	共有 ID の利用者及び ID カード利用責任者における、ルールや手順の理解不足及び運用不徹底により、「ID カード利用管理表」への記載が行われなかった。 ログ毎の調査結果は「(1.2.2.1) 1) (5)●共有 ID の検討」に記載している。
改善の方向性	再発防止策として以下を実施、検討している。 ・ID カード管理者への運用の周知徹底及び、業務委託先責任者への注意喚起を実施した。 ・共有 ID カードを限定し、個人 ID カードへ切替えた。（当分析でアクセス実績のあった共有 IDX,XXX 中 X,XXXID を個人 ID カード化済み） ・個人 ID カードへの切り替えが困難なもの（XXXID）については，XXX による共有 ID カードの受け渡し運用に変更し，キーボックスの開閉扉とキーの抜き差し時間を記録する運用とする。（XXX） XXX

1.3　東京電力パワーグリッド株式会社

1.3.1 対象システムの選定

1.3.1.1 対象システムの選定結果の概要

東京電力パワーグリッド株式会社（以下「東京電力 PG」という。）は、①本人認証受付システム、②PG サービス業務支援システム（PGSS）、③系統運用業務支援システム、④要請応対システムを対象にシステム選定のためのリスク評価を実施した。

リスク評価の結果は以下のとおり。

表 23 リスク評価結果（東京電力 PG）

システム名	システム重要度スコア	リスクの発生可能性評価スコア	トータルスコア
本人認証受付システム	XX	XX	XX
PG サービス業務支援システム（PGSS）	XX	XX	XX
系統運用業務支援システム	XX	XX	XX
要請応対システム	XX	XX	XX

東京電力 PG は一部（システム復旧手順やバックアップ手続等）に各システム固有の統制があるものの、「XXX」等により、システム間で概ね同様に統制が整備されている状況であり、大規模障害の発生等も確認されなかった。一方で、PG サービス業務支援システム（PGSS）は、託送業務を行うシステムであることに加え、個人情報を多数保有していること、ユーザ数が多いこと（社内ユーザ X,XXX 名、社外ユーザ XX,XXX 名）、アクセス数が年間 XXX 百万件以上と相当多いこと、XXX 台以上のサーバから構成される大規模システムであること等からログ調査の対象システムに選定した。

1.3.2 システムログの分析

1.3.2.1 ログの分析

1）アクセスログ分析結果の概要

PG サービス業務支援システム（PGSS）の 2024 年 7 月の各サーバで取得されるログを対象に、パイロットテスト及びアクセスログ分析を実施した。なお、PG サービス業務支援システムのログはアクセスログと操作ログの一部が一つのファイルに出力される仕様である。

表 24 ログ分析に利用したデータ一覧（東京電力 PG）

データ名	概要
ユーザ情報	社内利用者の一覧

データ名	概要
社外利用者一覧（新増・公開）	社外ユーザ（新増・公開）の利用者一覧。以下の情報を組み合わせて、利用者特定に利用 ・事業者一覧 ・社外組織一覧 ・ユーザ一覧 ・社外ユーザクライアント認証一覧
社外利用者一覧（新増工事店）	社外ユーザ（新増工事店）の利用者一覧
社外利用者一覧（受給契約購入実績）	社外ユーザ（受給契約購入実績）の利用者一覧
社内ログ	社内ユーザのログ情報
社外ログ（新増設・公開）	社外ユーザ（新増設・公開）のログ情報
社外ログ（スイッチング）	社外ユーザ（スイッチング）のログ情報
社外ログ（新増工事店）	社外ユーザ（新増工事店）のログ情報
社外ログ（受給契約購入実績）	社外ユーザ（受給契約購入実績）のログ情報
PGSS ユーザー情報登録管理台帳	電気工事店の登録管理のための台帳。7 月以降のユーザ登録日の確認に利用

(1) アクセスログ分析の対象ログ

PG サービス業務支援システム（PGSS）のログは、機能毎にサーバが異なり、それぞれのサーバでログが取得されている。本調査では、社内、社外（新増設・公開、スイッチング、新増工事店、受給契約購入実績）の各サーバにおけるアクセスログ（一部操作ログを含む）を利用した。

(2) ホワイトリストの信頼性の確認

PG サービス業務支援システム（PGSS）では、社内と社外ユーザで、認証方法が異なっているため、それぞれの機能毎にホワイトリストを作成している。社内ユーザは、東京電力 PG が作成したユーザ情報一覧をホワイトリストとして利用した。社外ユーザはホワイトリストを作成しておらず、PG サービス業務支援システム（PGSS）に登録されている利用者一覧を利用者特定のために利用した。

社内のユーザ情報一覧は、全社員の人事情報を管理している HD 共通サービスから取得したユーザ情報及び組織情報をもとに、2024 年 7 月以降に発生した異動・退職情報、PG サービス業務支援システム（PGSS）の組織権限情報（システムに設定されている組織ごとの権限設定の情報）を突合し、利用権限を持つ組織を抽出し作成された。

ホワイトリストを作成するために利用されたデータについて、以下を確認しデータの信頼性は担保されていると判断した。

表 25 データの信頼性の確認結果（東京電力 PG）

利用情報	概要	データの信頼性の確認結果
ユーザ情報	全社員の人事情報を管理している HD 共通サービスに登録されているユーザ情報である。	システムで管理している人事情報であり、全件出力していることから、網羅性、正確性について十分な心証を得た。
組織情報	全社員の人事情報を管理している HD 共通サービスに登録されている組織情報である。	システムが管理している情報であり、全件出力していることから、網羅性、正確性について十分な心証を得た。
異動・人事通知 退職・人事通知	HD オフィスサービスセンタに登録されている社員・派遣社員等社員以外の異動情報である。	人事情報であり、2024 年 7 月 1 日以降、ユーザ情報作成までの期間の異動情報の全件を出力していることから、網羅性、正確性について十分な心証を得た。
PGSS 利用権限一覧	PG サービス業務支援システム（PGSS）に登録されている組織ごとの利用権限の設定情報である。	システムに登録されている情報であり、全件を出力していることから、網羅性、正確性について十分な心証を得た。

社外ユーザの利用者一覧は PG サービス業務支援システム（PGSS）に登録されているデータが全件出力され、加工等がされていないことから、網羅性、正確性について十分な心証を得た。

社外ユーザは機能ごとにアクセス権限が付与されており、ユーザは自身のログイン情報（ユーザ ID や事業者コード）に紐づく申込情報のみにアクセスができる仕様となっているため、他のユーザの非公開情報にアクセスできない。自身の非公開情報のみにアクセスが限定されていることから、アクセスログ分析を実施せず、アクセス状況の確認に留めた。

(3) ログデータの網羅性

ログ保管に関する資料及びログ取得手順の閲覧並びに東京電力 PG への質問により、アクセスログ及び操作ログの網羅性を確認した。

各サーバで取得されたログは、障害時の直近確認用として各サーバに X 日間保管される。また、日次でログ収集サーバに転送され、XXX 日間保存される。法令要件で保

管が必要なログはログ収集サーバからログ監理サーバに転送され X 年間保存される。

ログ収集サーバ及びログ監理サーバは XXX しており、データセンタ運用担当者以外はアクセスできない状況となっている。

オンライン・バッチにて自動で取得保管を行っていること、複数サーバで分散して保存されること、アクセス制限の状況から、改ざんのリスクは低いと判断した。

ログデータは日次で圧縮ファイルが作成されており、対象期間のログデータに欠落がないことから、網羅性について一定の心証を得たため、データ分析に利用可能と判断した。

(4) システム上の権限設定状況の確認

設計書及びメニュー画面の閲覧並びに東京電力 PG への質問により、社内ユーザの権限設定については、非公開情報へアクセス可能な X つの権限（XXX）があることを確かめた。

所属組織に基づき、どの権限を設定するかが決まっており、ログイン時に所属組織を確認し、権限に応じたメニューのみが利用可能となっている。

社外ユーザについては、XXX ことを確かめた。

表 26 権限設定の概要（東京電力 PG）

権限の種類	権限の内容
XXX	非公開情報にアクセス可能な権限 すべてのメニューにアクセス可能
XXX	非公開情報にアクセス可能な権限 システム管理を除く、すべてのメニューが利用可能
XXX	非公開情報にアクセス可能な権限 託送_業務メニュー接続の XXX のメニューが利用可能
XXX	非公開情報にアクセス可能な権限 託送_業務メニュー接続の XXX のメニューが利用可能

(5) アクセスログの月次分析

1 か月分のアクセスログとホワイトリスト及び利用者情報を照合した。社内ユーザは、ホワイトリストに記載されたユーザを有権限者、記載のないユーザを権限のない者と識別しアクセスしたユーザを分類した。社外ユーザは、利用者登録の有無により、アクセスしたユーザを分類した。

さらに、社内の有権限者については、個人別に付与された ID かそれ以外のその他の ID かに分類した。

上記分類に基づき、機能別のアクセス状況を以下に示す。

表 27 アクセス状況（東京電力 PG）

社内/社外	機能	分類 1	分類 2	ID 数	所属	所属別 ID 数	アクセス回数※1	アクセス回数/所属別 ID 数
社内	—	権限のない者	—	XXX	東京電力 PG	XXX	XX,XXX	XXX
	—	有権限者	個人別 ID	X,XXX	東京電力 PG	X,XXX	X,XXX,XXX,XXX	XXX,XXX
	—		共有 ID	X,XXX	東京電力 PG	X,XXX	XXX,XXX,XXX	XXX,XXX
社外	新増設・公開	登録なし	—	X	広域機関[8]	X	XXX,XXX	XXX,XXX
		登録あり	—	X,XXX	小売電気事業者	X,XXX	XX,XXX,XXX	XX,XXX
	スイッチング	登録なし※2	—	XX	広域機関システム登録者	XX	XXX	XX
		登録あり※2	—	XXX	広域機関システム登録者	XXX	XX,XXX,XXX	XX,XXX
	新増電気工事店	登録なし	—	XXX	－（発電者、電気工事店）	XXX	X,XXX,XXX	X,XXX
		登録あり	—	XX,XXX	電気工事店、小売電気事業者	XX,XXX	XXX,XXX,XXX	XX,XXX
	受給契約購入実績	登録なし	—	XXX	－（発電者、電気工事店）	XXX	X,XXX,XXX	XX,XXX
		登録あり	—	XX,XXX	発電者	XX,XXX	XXX,XXX,XXX	X,XXX

※1 アクセスログに一部操作ログを含むため、アクセスした際の操作数をカウントしている。

※2 広域機関にてユーザ管理しているため、PG サービス業務支援システム（PGSS）に登録の事業者リストと照合し特定できたユーザのアクセスは登録あり、特定できなかったユーザは登録なしと分類した。

アクセスログの分析結果に基づき、操作ログ分析の対象となるか、以下の検討を実施した。

[8] 電力広域的運営推進機関（Organization for Cross-regional Coordination of Transmission Operators, Japan）は電力システム改革の第 1 段階として、中立・公平な立場で、電力の安定供給を維持し、供給システムをできる限り効率化することを目的に 2015 年 4 月に設立された認可法人である。すべての電気事業者に加入義務がある。

- 権限のない者によるアクセスの検討

社内ユーザの権限のない者によるアクセスが XXXID 検出されている。アクセスログから操作を確認したところ、XXXID はエラーログが出力されている、またはログインプロセスまで到達していないログであることからログインできていないことを確かめた。アクセスを試みたログは残されているが、ログインできていないため、操作ログ分析は不要と判断した。

一方、XID は、ログインしたアクセスログが認められたため、追加で東京電力 PG に質問した。XID はアクセス権限を保持する組織の役職者であること、XID は兼務でアクセス権限を保持する組織に所属していることから、有権限者であることを確かめたため、操作ログ分析は不要と判断した。

社外ユーザの登録なしユーザについて、東京電力 PG に質問し、アクセス者を特定した。また、登録のないユーザによるアクセスは誤操作によるものであり、PG サービス業務支援システム（PGSS）にログインできていないことを確かめた。

- 共有 ID の検討

社内ユーザの有権限者において、個人別 ID ではない ID を X,XXXID 識別している。これらの ID について利用状況を確認したところ、すべて RPA やツールで利用するシステムアカウントであり、そのうち RPA 用のシステムアカウントを共有利用している ID が XXXID あった。RPA 用 ID については、RPA 用 ID の所属に基づく権限にて利用可能な情報のみにアクセスが制限されている。RPA 導入時に、実行するシステム操作に問題がないことを対象システムの業務システム主管箇所等に確認することとしており、ID 発行については申請元責任者の承認と IT サポートセンターの審査のうえ ID 登録が行われていることを確かめた。

RPA 用 ID のパスワードは利用部門で管理しており、「XXX」にて、RPA 用の ID の利用にあたり ID 管理責任者を明確にし、ID に対する作業記録管理行うこと及び定期的なパスワード変更を行うための運用を確立することが定められている。

以上により、RPA 用システムアカウントについて、所属に紐づく権限での利用であり、業務システム主幹箇所が承認した上で登録利用されていること、また、ID の管理ルールが定められていることから、個人が利用する共有 ID とは識別せず、操作ログの分析対象外と判断した。

- 有権限者によるアクセス日付の妥当性の確認(有効期間外のアクセス)

ホワイトリストは異動･退職通知をもとに有効期間を考慮したリストになっているため、ログ出力時点の所属と紐づけが可能となっている。対象期間において、有効期間外の異動者・退職者によるアクセスは検出されなかった。

- 権限のない者によるアクセスの理由確認

東京電力 PG への質問により、アクセスは誤操作によるものと考えられる。な

お、アクセス回数が多かった X 名については個別で理由を確認した。XXX とも複数業務の遂行にあたり、その業務に応じた ID を利用しているが、本来 PG サービス業務支援システムで利用する ID と他の業務で利用する ID を混同し、別の業務で利用する ID を誤って入力したことが原因であることを確かめた。

- 非公開情報にかかる画面制御の検討

  東京電力 PG への質問、画面設計書及びシステム画面の閲覧により、以下の状況となっていることを確かめた。

社内ユーザ画面	• アクセス権限がない所属のユーザがアクセスした場合、ログインできず、アクセスエラー画面が表示される。 • 所属に紐づく権限により、利用できるメニューのみリンクが有効となっており、利用できないメニューはリンクが無効化されている。
社外ユーザ画面	• 情報を検索、表示する際、必ずログインユーザの ID を検索キーに含むよう設計されており、ユーザ自身のログイン情報（ユーザ ID や事業者コード）に紐づく申込情報のみしかアクセスできないよう設計されている。

2) 操作ログの分析結果の概要

アクセスログ分析の結果、操作ログの分析対象となるログは識別されなかったため、操作ログの分析は不要であると判断した。

1.3.3 結論

本調査の範囲において、非公開情報の管理の用に供するシステムである PG サービス業務支援システムのログ分析の結果、非公開情報を入手可能な者によるアクセスのみが識別され、特定された者のみが当該情報を入手することができることになっていた。

1.3.4 検出事項

ログ分析の結果、非公開情報へ権限のない者によるアクセスは識別されなかったが、ログ分析の過程で以下の気づき事項を検出した。

1.3.4.1 検出事項 No.1

検出事項の分類	気づき事項
概要	社外ユーザのアクセス権の定期的な棚卸が実施されていない
詳細	社外ユーザは自身の申込以外の情報にアクセスできないため、社外ユーザの棚卸までは行っていない。
リスク	アカウントの乗っ取りや不正利用のリスクが高まる。 不要なアカウントが多数存在するとシステムのパフォーマンス低下や管理の複雑性が増大するリスクがある。
原因	以下のアクセス状況から定期的な棚卸は実施していない。 ・ XXX 機能は、クライアント証明書の有効期間が X 年間であり、X 年ごとに継続利用の確認または自動削除が実施される。 ・ XXX 機能は、申し込みから処理完了（送電完了）までの期間が長期化することがある。また、ユーザ自身の申込内容以外の他の申込は確認できない制御を実施している。 ・ XXX 機能は、発電者が購入実績を毎月確認している。また、ユーザ自身の申込内容以外の他の申込内容は確認できない制御を実施している。
改善の方向性	一定期間アクセスがないアカウントを削除する運用とする。 具体的な運用方法について、今後、検討を進める。

1.4 中部電力パワーグリッド株式会社

1.4.1 対象システムの選定

1.4.1.1 対象システムの選定結果の概要

中部電力パワーグリッド株式会社（以下「中部電力 PG」という。）は、①配電業務総合支援システム、②お客さまサービスシステム、③低高圧調定システム、④低圧工事契約申込電子受付システムを対象にシステム選定のためのリスク評価を実施した。

リスク評価の結果は以下のとおり。

表 28 リスク評価結果（中部電力 PG）

システム名	システム重要度スコア	リスクの発生可能性評価スコア	トータルスコア
配電業務総合支援システム	XX	XX	XX
お客さまサービスシステム	XX	XX	XX
低高圧調定システム	XX	XX	XX
低圧工事契約申込電子受付システム	XX	XX	XX

中部電力 PG は「XXX」や「XXX」等により、各システムは概ね同様に統制が整備されている状況であり、大規模障害の発生等も確認されなかった。一方で、お客さまサービスシステムは、送配電機能及び小売機能を有するシステムであることに加え、ユーザ数が多いこと（ユーザ数 X 万名超（うち社外ユーザ X,XXX 名））、アクセス数が年間 XXX 百万件超と他システムと比較し多いこと、システム構成が複数の業務処理を統合しており、複雑なクライアントサーバー構成であること等から、ログ調査の対象システムに選定した。

1.4.2 システムログの分析

1.4.2.1 ログの分析

1) アクセスログ分析結果の概要

お客さまサービスシステムの 2024 年 7 月の端末操作ログを対象に、パイロットテスト及びアクセスログ分析を実施した。なお、お客さまサービスシステムはアクセスログと操作ログが一つのファイルに出力される仕様である。

表 29 ログ分析に利用したデータ一覧

データ名	概要
ログファイル 1_A05CAACX	操作ログに該当するログ情報（XXX のサーバ群）
ログファイル 2_A07CAACX	操作ログに該当するログ情報（XXX のサーバ群）
ログのヘッダ情報	ログのヘッダ情報
インフラ業務権限マトリクス－利用可能箇所（2024 年 7 月断面）	お客さまサービスシステムを利用可能な権限グループ（XXX コード）の一覧
システム利用ユーザリスト	ユーザ情報（人事システムより作成）

(1) アクセスログ分析の対象ログ

お客さまサービスシステムでは、アクセスのみを記録したログは存在しないため、操作ログから、中部電力 PG より指定されたシステム利用開始時に必ず記録されるメ

ッセージ（「XXX」）に該当する操作ログを当法人にて抽出し、調査に利用した。

また、XXX コードが「XXX」もしくは「XXX」、氏名コードが「XXX」、「XXX」もしくは「XXX」のログについてはシステム処理のログ（ユーザが画面操作したものではない）との回答を中部電力 PG より得られたため、分析対象から除外した。

なお、同様のログを対象にして中部電力 PG もログモニタリングを実施している。

(2) ホワイトリストの信頼性の確認

中部電力 PG でホワイトリストは作成していない。お客さまサービスシステムでは、XXX に対して権限設定を行っていることから、XXX のデータをインプットとした XXX、システム利用時の認証に用いている。よって、「インフラ業務権限マトリクスー利用可能箇所」を有権限か否かの判断に利用した。

「インフラ業務権限マトリクスー利用可能箇所」について、以下を確認しデータの信頼性は担保されていると判断した。

表 30 データの信頼性の確認結果（中部電力 PG）

利用情報	概要	データの信頼性の確認結果
インフラ業務権限マトリクスー利用可能箇所（2024 年 7 月断面）	お客さまサービスシステムを利用可能な権限グループ（XXX）の一覧	変更日と変更部分を履歴として残している。 2024/7/1-7/31 の間に変更はなかった。

(3) ログデータの網羅性

ログ保管に関する資料及びログ取得手順の閲覧並びに中部電力 PG への質問により、操作ログの網羅性を確認した。

中部電力 PG への質問により、当該システムの Web アプリサーバで取得されたログは共用のログ管理システムに送付され、まとめて保管されており、中部電力の XXX が管理しているとの回答を得た。また、「XXX」を閲覧し、セキュリティ部署以外の保守端末から統合ログ管理システムへ接続できないように XXX にて制限されており、各業務システム関係者が直接ログを変更・削除することはできないことを確認した。

また、ログ抽出時のログ管理システム担当者（委託先）への作業申請メールを閲覧し、共有のログ管理システムに対して対象の Web アプリサーバ、ログファイルの日付（2024/7/1～2024/8/1）を指定して抽出しているのみであり、網羅性についても十分であるとの心証を得た。

以上より、ログデータの網羅性について心証を得たため、データ分析に利用可能と判断した。

(4) システム上の権限設定状況の確認

中部電力 PG への質問及び設計書の閲覧により、当該システムではユーザの XXX に対して権限が自動設定されることを確認した。ユーザの所属は中部電力 PG（一般送配電事業者）か、中部電力ミライズ株式会社（以下「中部電力 MZ」という。）（小売事業者）かに大別されていることを確かめた。

表 31 XXX に応じて自動付与される権限の内容

XXX	自動付与される権限
中部電力 PG	非公開情報にアクセス可能な権限
中部電力 MZ	非公開情報にアクセス不可の権限 ※非公開情報はマスキングされ表示されない

(5) アクセスログの月次分析

1 か月分の操作ログからお客さまサービスシステム利用開始時に必ず記録されるメッセージログを抽出し、「インフラ業務権限マトリクスー利用可能箇所」（2024 年 7 月断面）に記載された XXX のユーザを有権限者、記載されていない XXX のユーザを権限のない者と識別しアクセスしたユーザを分類した。

さらに、有権限者については、ユーザ ID が個人別に付与された ID か、共有 ID か、後で述べる教育用 ID に分類した。

上記分類に基づき、XXX 毎のアクセス状況を以下に示す。

表 32 アクセス状況（中部電力 PG）

分類 1	分類 2	所属	ID 数	アクセス回数 ※	アクセス回数/所属別 ID 数
権限のない者	—	—	—	—	—
有権限者	個人別 ID	中部電力 PG	X,XXX	X,XXX,XXX	XXX.XX
		中部電力 MZ	X,XXX	XX,XXX,XXX	X,XXX.XX
	共有 ID	中部電力 PG	XX	XX,XXX	XXXX.XX
		中部電力 MZ	XXX	X,XXX,XXX	X,XXX.XX
	教育用 ID	—	XX	XX,XXX	X,XXX.XX

※「システム利用開始時に必ず記録されるメッセージ」をアクセス回数とカウントしているため、システム利用開始以外の操作もカウントしている可能性がある。

アクセスログの分析結果に基づき、操作ログ分析の対象となるか、以下の検討を実施した。

- 権限のない者によるアクセスの検討
  権限のない者によるアクセスは検出されなかった。

- 教育用 ID の検討
  当該 ID について中部電力 PG へ質問し、用途としては新入社員、新規委託先の訓練であり、中部電力 PG、MZ いずれのユーザも XXX することで利用可能な旨回答を得た。また、接続されるデータベースは教育用（ダミーデータ）とすることで、本番情報（非公開情報）の利用ができないよう制御しており、ダミーデータは過去の本番データを XXX で変更したものであり非公開情報には該当しない旨回答を得た。
  利用用途が明確かつ非公開情報を保持していないため、詳細な検討は実施しない方針とした。

- 共有 ID の検討
  中部電力 MZ 所属の共有 ID について利用用途を確認した結果、システム利用の共有 ID が XX 件、個人利用の共有 ID が XXX 件であった。システム利用の共有 ID は自動ツール（RPA・VBA[9]等）を利用して顧客・電気工事店の申込情報等の登録、更新、確認等に利用されていた。なお、当該 ID のログイン情報については、必要最低限の担当者のみが確認できる台帳で XXX を管理しているとの回答を得ている。
  個人が利用することが想定されている共有 ID については、オペレータの顧客申込受付業務、お客さま対応業務の研修、問い合わせ対応及びシステム担当者の改修後動作確認で利用されており、利用の都度貸出管理が行われている。
  以上より、中部電力 MZ 所属の共有 ID について利用用途が明確であること、また、小売業者も利用可能な画面に限定された権限が自動付与されており、非公開情報へのアクセスができないことから詳細な検討は実施しない方針とした。

  中部電力 PG 所属の共有 ID について利用用途を確認した結果、システム利用の共有 ID が XX 件、個人利用の共有 ID が X 件であった。システム利用の共有 ID は自動ツール（RPA）を利用して、申込情報の csv ファイル出力、発電側課金業務における内訳書の発行や発電者への請求、工程管理システムの最適化やバックアップ等が行われていた。なお、当該 ID のログイン情報については、必要最低限の担当者のみが確認できる台帳で XXX を管理しているとの回答を得た。今回検出したシステム利用の共有 IDXX 件について、該当の台帳を閲覧し、上記運用が実施されている心証を得た。

[9] VBA (Visual Basic for Applications): VBA は、Microsoft Office アプリケーション（Excel、Word、Access など）に組み込まれているプログラミング言語である。VBA を使用することで、これらのアプリケーションを自動化し、カスタマイズすることが可能となる。

個人利用の共有 ID については、非常災害対応用で利用されており、利用の都度貸出管理が行われている。当該 ID については、XXX、不正利用のリスクが高いため、詳細な検討を実施した。

対象の共有 ID（XID）について、共有 ID の管理者から、7 月の共有 ID の貸出しを管理している「XXX」を入手した。「XXX」とアクセスログと突合したところ、当該管理簿に記録が残されていなかった。

管理簿に記録が残されていなかった理由について中部電力 PG から以下回答を得た。

- 本 ID は、20XX 年度に災害訓練にて利用をするために貸出された
- しかしながら、当日は初期設定不良で利用がされなかったため、そのまま XXX 状態であった
- 当該 ID のログイン情報が、XXX、かつ、後日初期設定不良が修正された
- 利用者は、特に意識しないまま当該 ID を利用していた

また、中部電力 PG の調査資料から以下を確認した。

- 利用者は、一般送配電事業者所属であり、有権限者であった
- 該当利用者の PC からのみ当該 ID が利用されており、かつ、利用者の業務範囲でのみ操作を行っていた
- 8 月の異動時期にパスワードリセットを行った

有権限者の利用であるため、不正アクセスには該当しないと判断したが、調査内容を裏付けるために、当法人側でも操作ログ分析を実施した。

- 有権限者によるアクセス日付の妥当性の確認(有効期間外のアクセス)

システムへのアクセスは、「インフラ業務権限マトリクスー利用可能箇所一覧」で常時制御されており、中部電力 PG より 2024 年 7 月中における当該権限情報の変更はないとの回答を得ているため、確認は不要と判断した。

- 有権限者によるアクセス権限の妥当性の確認

当該システムの権限について、基本的に XXX 設定されているため、許可された権限範囲以外のアクセスができない仕組みとなっている。なお、XXX 反映は、異動日に新所属情報に更新されタイムラグのない運用となっていることから、期間外に権限範囲外のアクセスが行われるリスクは低いと判断した。

また、XXX に紐づかない ID（コンテンポラリーユーザ）について、「XXX」を閲覧し、ユーザ登録ツールを用いて各所属部署から中部電力 HD 窓口に申請され、各所属の管理職以上の承認をもって登録される運用であることを確かめた。また、ユーザ登録ツールの操作画面を閲覧し、他の会社のユーザ登録はエラーとなり登録できないことを確かめた（中部電力 PG 権限を中部電力 MZ が申請・承認するこ

とは不可能)。なお、XXX に紐づかない ID（コンテンポラリーユーザ）を対象に XXX に一度ユーザの棚卸も実施している旨回答を得た。

コンテンポラリーユーザのアクセス権限の妥当性を確認するために、7 月中にアクセスのあったコンテンポラリーユーザ X,XXX ユーザから XX ユーザを無作為に抽出後、申請書を確認し、申請内容と実機の所属内容に不整合がないことを確かめた。

- 権限のない者によるアクセスの理由確認

  権限のない者によるアクセスは検出されなかった。

- 非公開情報にかかる画面制御の検討

  中部電力 PG が作成している仕様書から、当該システムにおける「非公開情報にアクセス可能な操作画面一覧」を特定し、特定した計 XXX 画面から XX 画面を無作為に抽出し、開発環境における中部電力 PG 所属の ID、中部電力 MZ 所属の ID の操作画面スクリーンショットを確認した。

  確認の結果、すべての画面において中部電力 MZ 所属の ID の重要情報閲覧ができないことを確かめた。なお、中部電力 PG より業務システムは、開発環境で動作確認を行ったものについて改変を行わず本番環境へ資産配布することで、同一性を担保している旨回答を得た。

  以上より、非公開情報にかかる画面制御が実装されている心証を得た。

2) 操作ログの分析結果の概要

アクセスログ分析結果の概要アクセスログ分析の結果、以下の操作ログを分析した。

(1) 中部電力 PG 非常災害対応用の共有 ID のアクセス

中部電力 PG 非常災害対応用の共有 ID のアクセスは XID、XX アクセスを識別しており、当該アクセスに関して貸出記録が残されていなかった。

当該 ID の操作ログを分析したところ、訓練で貸出された利用者の PC からのみ利用されており、かつ、お客様情報検索に係る操作のみ実行していたことを確かめた。

以上より、中部電力 PG の調査資料の内容に齟齬はなく、利用者の業務範囲でのみ操作を行っていたとの心証を得た。

1.4.3 結論

本調査の範囲において、非公開情報の管理の用に供するシステムであるお客さまサービスシステムのログ分析の結果、非公開情報を入手可能な者によるアクセスのみが識別され、特定された者のみが当該情報を入手することができることになっていた。

1.4.4 検出事項

ログ分析の結果、非公開情報へ権限のない者によるアクセスは識別されなかったが、ログ分析の過程で以下の気づき事項を検出した。

1.4.4.1 検出事項 No.1

検出事項の分類	気づき事項
概要	中部電力 PG の非常災害対応用の共有 ID、XID について、「XXX」に貸出記録が残されなかった。当該貸出記録が残されなかった結果、XXX、利用可能な状況のまま放置されていた。
詳細	中部電力 PG より経緯について以下の回答を得た。 本 ID は、20XX 年度に災害訓練にて利用をするために貸出されたが、当日は初期設定不良で利用がされなかった。そのため、「XXX」に利用記録が起票されず、XXX。後日、初期設定不良が修正され、さらに、本 ID のログイン情報が XXX、利用者は、特に意識しないまま、本 ID を利用していた。 本 ID については以下を確認できたため、結論を妨げない。 本 ID 利用者は、中部電力 PG 所属であり、有権限者であった。また本 ID は、当該利用者の PC からのみ利用され、かつ、当該利用者の業務範囲でのみ操作を行っていた。なお、8 月の異動時期に XXX を行ったため、それ以降当該ユーザによるログインはできなくなっている。
リスク	• 共有 ID の利用者、操作内容の特定が難しくなるリスク • 本来の利用目的から逸脱した操作が行われるリスク
原因	共有 ID の利用に関するルールが不足していた。 共有 ID の利用に関し、「XXX」にて、「XXX」となっており、共有 ID を利用した PG 所属員を管理簿に記載して報告することになっていたが、訓練日当日、共有 ID が利用できなかったため、貸出管理簿が提出されず、XXX も実施されなかった。
改善の方向性	再発防止策として以下を実施、検討している。 ・共有 ID の利用について、利用有無にかかわらずログイン情報を払い出した都度貸出記録を残し、申請時の利用期間経過後に XXX するようにルールを変更し、運用を周知徹底し

	ている。 ・災害専用メニューを新設し、有事の際に利用可能として災害応援対応を行う（通常時は該当メニューを表示させない）運用を、2025 年 X 月より開始予定である。

1.5　北陸電力送配電株式会社

1.5.1 対象システムの選定

1.5.1.1 対象システムの選定結果の概要

北陸電力送配電株式会社（以下「北陸電力送配電」という。）は、①営業システム、②託送システム、③計器業務システム、④需要精算システムを対象にシステム選定のためのリスク評価を実施した。

リスク評価の結果は以下のとおり。

表 33 リスク評価結果（北陸電力送配電）

システム名	システム重要度スコア	リスクの発生可能性評価スコア	トータルスコア
営業システム	XX	XX	XX
託送システム	XX	XX	XX
計器業務システム	XX	XX	XX
需要精算システム	XX	XX	XX

北陸電力送配電は「XXX」や「XXX」等の規程により、各システムは概ね同様に統制が整備されている状況であり、大規模障害の発生も確認されなかった。一方で、営業システムは、託送業務に直接関連し、多くの業務プロセスに関連するシステムであることに加え、アクセス数年間約 XXX 万件と他システムと比較して大規模である。また XX の外部システムと接続し、XX のサブシステムから構成されたホストシステムであり、複雑性が高いと判断したこと等からログ調査の対象システムに選定した。

1.5.2 システムログの分析

1.5.2.1　ログの分析

1）アクセスログ分析結果の概要

営業システムの 2024 年 7 月の端末操作ログを対象に、パイロットテスト及びアクセスログ分析を実施した。なお、営業システムには、配電系ジョブと営業系ジョブがあり、配電系ジョブは北陸電力送配電からのみアクセス可能なジョブ、営業系ジョブは北陸電力及び北陸電力送配電双方からのアクセスが可能なジョブである。配電系及び営業系でホワイトリストが異なるため、分けて分析を行った。

表 34 ログ分析に利用したデータ一覧（北陸電力送配電）

データ名	概要
共通	
#2_人事異動情報（2024 年 7-9 月）	人事異動情報（2024 年 7-9 月）
配電系	
#1_20240701_配電系ジョブアクセスログ	配電系ジョブの操作ログ（パイロットテスト用の一日分）
#15_営業システム_配電系ジョブログ_240702.xlsx～#15_営業システム_配電系ジョブログ_240731.xlsx	配電系ジョブの操作ログ（7 月分）
#8-2_ ホワイトリスト_20240701	営業システムにアクセス可能な XXX の一覧
#4_20240906_利用者名簿	非公開情報を入手可能な者の名簿（2024/9/6 断面）であり、ホワイトリストとして利用
営業系	
#9_1_営業システム_営業系ジョブログ_20240701	営業系ジョブのお客様情報にアクセスする際の操作ログ（パイロットテスト用の一日分）
#10_営業システム_営業系ジョブログ_20240702.xlsx～#10_営業システム_営業系ジョブログ_20240731.xlsx	営業系ジョブのお客様情報にアクセスする際の操作ログ（7 月分）
#11_20240906_営業ジョブ利用者名簿.xlsx	営業ジョブにアクセス可能なものの名簿（2024/9/6 断面）であり、ホワイトリストとして利用

(1) アクセスログ分析の対象ログ

営業システムから系統ごとに取得したログを分析に利用した。なお、アクセスのみを記録したログは存在しないため、操作ログを分析に利用している。

【配電系】営業システムの操作ログから配電系ジョブの全ジョブの操作ログを抽出し、アクセスログとして分析を実施

【営業系】営業システムの操作ログから営業系ジョブの操作ログを抽出後、お客さま情報が閲覧・更新可能なジョブの操作ログを抽出し、アクセスログとして分析を実施

(2) ホワイトリストの信頼性の確認

北陸電力送配電が、以下の情報をもとに、手で加工して作成した名簿をホワイトリストとして利用した。以下を確認しデータの信頼性は担保されていると判断した。

なお、入手したホワイトリストは9月6日時点の断面であり、当分析の対象月とした7月と時点が異なっている。本アクセスログ分析では、9月6日時点のホワイトリストとアクセスログとの照合を行い、照合の過程で時点による差分を検討し、アクセスのあったユーザを有権限者と権限のない者に分類する方針とした。

表 35 データの信頼性の確認結果（北陸電力送配電）

利用情報	概要	データの信頼性の確認結果
【配電系】 ユーザ一覧	人事情報及び個別申請に基づくホスト計算機のユーザ情報から、以下のユーザを抽出した情報である。 ・営業システムの利用資格を有する北陸電力送配電社員ユーザ ・北陸電力送配電から使用許可を受けた委託会社のユーザ ・テスト用 ID、システム運用のための ID	XXX をもとにしており、網羅性、正確性について十分な心証を得た。 また、個別登録の情報について北陸電力送配電へ質問を実施し、名簿作成時点で個別登録情報とユーザの在籍状況が整合していることを確かめた。なお、北陸電力送配電は在籍状況が記載された「電話一覧資料」やユーザ改廃申請との突合及び当人へのヒアリング等により整合性を確認している。このことから、網羅性、正確性について十分な心証を得た。

利用情報	概要	データの信頼性の確認結果
【営業系】 ユーザ一覧	人事情報及び個別申請に基づくホスト計算機のユーザ情報から、以下のユーザを抽出した情報である。 ・営業システムの利用資格を有する北陸電力及び北陸電力送配電社員ユーザ ・北陸電力及び北陸電力送配電から使用許可を受けた委託会社のユーザ ・テスト用 ID、システム運用のための ID	XXX をもとにしており、網羅性、正確性について十分な心証を得た。 また、上記【配電系】と同様に個別登録の情報について北陸電力送配電への質問を実施し、名簿作成時点で個別登録情報とユーザの在籍状況が整合していることを確かめた。なお、一部の小売部門のユーザにおいて、所属情報に乖離があったものの、いずれも小売部門の XXX であり、利用資格に乖離はないため、影響はないと判断した。このことから、網羅性、正確性について十分な心証を得た。

(3) ログデータの網羅性

ログ保管に関する資料及びログ取得手順の閲覧並びに北陸電力送配電への質問により、操作ログの網羅性を確認した。

ログは XXX に保存している。XXX は、XXX に設置・保存されており、一般ユーザにはログにアクセスする権限はない。XXX への保存などを実施する必要性から、XXX の運用管理者のうち特権 ID の利用が認められた管理者のみ、特権 ID を使用してログの移動を行っている。

また、ログ取得時の条件について、系統毎に以下の通りであることを確かめた。

表 36 系統別のログ取得条件及び網羅性の確認結果

系統	取得条件及び網羅性の確認結果
配電系	分析で利用したアクセスログは、対象月（7 月）かつ配電系ジョブの全ログを対象としており、網羅性について十分であると心証を得た。

系統	取得条件及び網羅性の確認結果
営業系	分析で利用したアクセスログは、対象月（7 月）かつ営業系ジョブの全ログから、お客さま番号を入力する項目を有するタスクに限定している。 非公開情報へのアクセスにはお客さま番号の入力が必要となるため当該ログを対象とし、網羅性について十分であると心証を得た。

以上より、ログデータの網羅性について心証を得たため、データ分析に利用可能と判断した。

(4) システム上の権限設定状況の確認

北陸電力送配電への質問及びユーザ一覧の閲覧により、権限設定について、利用資格として大きく送配電部門と小売部門の種類があることを確かめた。

表 37 権限設定の概要（北陸電力送配電）

権限の種類	権限の内容
送配電部門	非公開情報（他社お客さま情報）にアクセス可能な権限
小売部門	非公開情報にアクセス不可の権限

(5) アクセスログの月次分析

1 か月分の営業システムへのアクセスに係るログを系統毎に抽出し、ホワイトリストと照合した。ホワイトリストに記載されたユーザを有権限者、記載のないユーザを権限のない者と識別しアクセスしたユーザを分類した。

照合の過程で、ホワイトリスト（9 月 6 日時点）とアクセスログ（7 月時点）の時点の差異について以下の通り検討を行い、ホワイトリストと差異があるものの、アクセス時点で有権限者であることが確認できたユーザについては、有権限者に分類した。

なお、ホワイトリストと差異のないユーザについては 7 月時点においてもホワイトリストと同じであると回答を得ている。

● ホワイトリストとアクセスログの差異の検討

アクセスログとホワイトリストを照合し、ユーザ・所属・権限の種類に差異のあるアクセスユーザを抽出の上、分類を行った。

【配電系】

配電系ジョブへのアクセスがあったユーザについて、ホワイトリストと差異のあるユーザが XXX 件存在した。XXX 件について北陸電力送配電への質問により差異の理由を確認し、権限のない者によるアクセスのユーザを特定した。

・XX 件：7/1 付の所属 CD 変更処理の遅延により旧所属がアクセスログとして記録されたが、7 月時点の所属もホワイトリストと同じであり有権限者であること

を確かめた。

・X 件：7/1 付で出向したが、出向元 ID を利用してアクセスを行ったもの。出向元及び出向先いずれも送配電部門権限を持つ有権限者であることを確かめた。

・X 件：8/1 以降付の異動者であり、7 月時点での所属はアクセスログの記録通りであること及び 7 月時点で有権限者であることを確かめた。

・XX 件：退職または休職中のためホワイトリストに存在しないが、7 月時点では有権限者であることを確かめた。なお、7 月中に退職した X 名（7 月中に休職したユーザはなし）については、退職日以降にアクセスログがないことを確認している。

・XX 件：配電系の名簿作成時に、ツール用及びシステム運用用の ID を含めていなかったため抽出されたが、有権限者である。

・XX 件:配電系のアクセス権がないためホワイトリストに存在しないものであり、権限のない者と識別した。

【営業系】

営業系ジョブへのアクセスがあったユーザについて、ホワイトリストと差異のあるユーザが XXX 件存在した。XXX 件について差異の理由を確認し、権限のない者によるアクセスのユーザを特定した。

・XX 件：7/1 付の所属 CD 変更処理の遅延により旧所属がアクセスログとして記録されたが、実態はホワイトリストと同じであり有権限者であることを確かめた。

・XX 件：個別申請に基づき利用資格変更（7/1、8、22、29、8/22）が行われたため差異が発生しているが、変更前においても有権限者であることを確かめた。

・X 件：個別申請に基づき個別に利用資格が付与されていたが、8/1 以降に所属変更を伴わない人事発令により、XXX に従った資格が自動付与されたことにより差異が発生しているが、7 月時点での所属はアクセスログの記録通りであること及び、7 月時点で有権限者であることを確かめた。

・X 件：8/1 以降付の異動者であり、7 月時点での所属はアクセスログの記録通りであること及び 7 月時点で有権限者であることを確かめた。

・XX 件：退職または休職中のためホワイトリストに存在しないが、7 月時点では有権限者であることを確かめた。なお、7 月中に退職した X 名（7 月中に休職したユーザはなし）について、退職日以降にアクセスログがないことを確認している。

・X 件：情報システム部開発担当のユーザであり、ホワイトリスト時点では権限が不要となったため差異が発生しているが、7 月時点では有権限者であることを確かめた。

さらに、有権限者については、ユーザ ID が個人別に付与された ID か、共有 ID かに分類した。

上記分類に基づき、権限毎のアクセス状況を以下に示す。

表 38 アクセス状況 【配電系】

分類 1	分類 2	ID 数 ※1	所属	所属別 ID 数	アクセス回数※2	アクセス回数/所属別 ID 数
権限のない者	個人別 ID	XX	北陸電力、北陸電力送配電、XXX、XXX、XXX、XXX XXX	XX	XXX	X.XX
有権限者	個人別 ID	X,XXX	XXX など、XXX からの外部委託	XX	XX,XXX	XXX.XX
			XXX	XXX	XX,XXX	XXX.XX
			XXX	XXX	XXX,XXX	X,XXX.XX
			XXX	X	X,XXX	XXX.XX
			XXX	X	XX	XX.XX
			XXX	X	XXX	XX.XX
			XXX	XXX	XX,XXX	XXX.XX
			北陸電力送配電	X,XXX	X,XXX,XXX	X,XXX.XX
	共有 ID	X	XXX など、XXX からの外部委託	X	XXX	XXX.XX
			北陸電力送配電	X	X,XXX	XXX.XX

※1 配電系ジョブは利用資格が送配電部門のユーザのみアクセス可能であるため、権限分類の記載は省略した。

※2 操作ログを分析に利用しているため、アクセス回数ではなく、ログ件数を記載している。

表 39 アクセス状況 【営業系】

分類 1	分類 2	権限	ID 数	所属	所属別 ID 数	アクセス回数※1	アクセス回数/所属別 ID 数
権限のない者	—	—	—	—	—	—	—
有権限者	個人別 ID	送配電	X,XXX	XXX からの外部委託	XX	XX,XXX	XXX.XX
				XXX	X	XXX	XX.XX
				XXX	XX	XXX	XX.XX
				XXX	X	XXX	XX.XX

分類 1	分類 2	権限	ID 数	所属	所属別 ID 数	アクセス回数※1	アクセス回数/所属別 ID 数
				XXX	X	X	X.XX
				XXX	X	XXX	XX.XX
				北陸電力送配電	X,XXX	XXX,XXX	XXX.XX
		小売	XXX	XXX	XXX	XX,XXX	XXX.XX
				XXX	XX	XX,XXX	X,XXX.XX
				XXX	X	XXX	XX.XX
				XXX	XXX	XXX,XXX	X,XXX.XX
				XXX	XX	XX,XXX	XXX.XX
				北陸電力送配電	X	XX	XX.XX
	共有 ID	送配電	XX	XXX からの外部委託	X	XX	XX.XX
				XXX	XX	X,XXX	XXX.XX
				北陸電力送配電	X	XX,XXX	X,XXX.XX
		小売	XX	XXX	X	XXX	XX.XX
				XXX	X	XX	XX.XX
				北陸電力	XX	XX,XXX	XXX.XX

※1 操作ログを分析に利用しているため、アクセス回数ではなく、ログ件数を記載している。

アクセスログの分析結果に基づき、操作ログ分析の対象となるか、以下の検討を実施した。

- 権限のない者によるアクセスの検討

【配電系】

権限のない者によるアクセスが XXID 検出されている。アクセスログ分析に利用したログはジョブへのログインエラーも含まれるため、XXID についてアクセスを試みたもののエラーとなっていることを確認することにした。

【営業系】

権限のない者によるアクセスは検出されなかった。

- 共有 ID の検討

【配電系】

共有 ID の利用用途を確認した結果、システム利用の共有 ID が X 件、個人利用の共有 ID が X 件であった。システム利用の ID は営配登録ツール用 ID として利用されていた。個人 ID については、欠員補填や開発・保守対応での調査やリリース前の最終確認を行うための利用となっており、利用の都度貸出管理が行われている。

配電系ジョブは非公開情報を含むことから不正利用の可能性があるため、詳細な検討を実施した。

対象の共有 ID（XID）のうち個人利用の XID（操作ログ件数：XXX 件）について、共有 ID の管理者から、7 月の共有 ID の貸出しを管理している「XXX」を入手した。「XXX」とアクセスログと突合した結果、操作ログ件数 XXX 件のうち XXX 件について対応する利用記録が残されており、管理者による承認の上で利用されていることを確かめた。残りの XX 件については「XXX」上に対応する利用記録が残されていなかった。北陸電力送配電への質問により、「XXX」への時刻記入誤り及び記入漏れにより利用記録が残されなかったものであることを確かめた。あわせて、記入が漏れていた操作ログについて、共有 ID 貸出時に「XXX」と共に記入が必要となる「座席表」の記録をもとに北陸電力送配電が特定した利用者及び利用用途について回答を得た。また、共有 ID の利用時には、管理者が施錠された保管場所から XXX、PC へのログインは XXX、使用者には XXX は明かされない運用となっていると回答を得たことから、記入誤り及び漏れがあったものの管理者による承認の上で利用されていると心証を得た。

システム利用の XID については、北陸電力送配電への質問により、XXX が公開されておらず、人による利用ができないことが確かめられたため、追加検討の対象外とした。

【営業系】

共有 ID の利用用途を確認した結果、システム利用の共有 ID が XX 件（送配電：XX 件、小売：X 件）、個人利用の共有 ID が XX 件（送配電：X 件、小売：XX 件）であった。システム利用の ID は RPA 用及びシステム内部で使用する ID として利用されていた。個人利用の ID については、欠員補填やコールセンターのオペレータ用、繁忙期の業務応援用、システムテストのための利用となっており、利用の都度貸出管理が行われている。小売部門権限は小売事業者も利用可能な画面に限定された権限であり、不正利用のリスクは低いため、詳細な検討は実施しない方針とした。

送配電部門権限はすべてのお客さま情報にアクセス可能な権限であり、不正利用の可能性があるため、詳細な検討を実施した。

対象の共有 ID（XXID）のうち個人利用の XID について、共有 ID の管理者から、7 月の共有 ID の貸出しを管理している「利用管理表」を入手した。「利用管理

表」とアクセスログと突合し、管理者による承認の上で利用されていることを確かめた。

システム利用の XXID については、北陸電力送配電への質問により、XXX が公開されておらず、人による利用ができないことを確かめられたため、追加検討の対象外とした。

- 有権限者によるアクセス日付の妥当性の確認(有効期間外のアクセス)

有権限者によるアクセス一覧と人事通達を照合した結果、7 月中に異動したユーザが X ユーザ存在し、いずれも権限がない部署から権限がある部署への異動であった。当該 X ユーザによるログはすべて異動日以降のログであり、有効期間外のアクセスはなかったことを確かめた。

- 有権限者によるアクセス権限の妥当性の確認

権限は、人事情報と連動し設定されているため、許可された権限範囲以外のアクセスができない仕組みとなっている。また、7 月中に権限がない部署から権限がある部署へ異動した X ユーザについて、異動前のアクセスはなく、異動後に前所属に紐づく権限を利用したアクセスはなかったことを確かめた。

- 権限のない者によるアクセスの理由確認

【配電系】

北陸電力送配電への質問により、権限のない者によるアクセスとして識別した XXID によるアクセスについて、権限がないにもかかわらずアクセスを行った理由を確認した結果、以下の回答を得た。7/1 付の出向者による誤アクセスやジョブコードの入力誤りに関連するアクセスであり、不正の兆候は見られなかった。

・ 2024/7/1 付の出向者（XXID）：出向後は出向先ユーザ ID でアクセスが必要だが、誤って旧所属ユーザ ID でアクセスしたもの
・ 北陸電力所属の営業系権限保有者（XXID）：営業系の権限保有者であり営業システムへのアクセス権限を保有しているが配電系ジョブのアクセス権限を持たないユーザが、ジョブコードの入力誤りによりアクセスしたもの
・ 北陸電力送配電所属の権限のない者（XID）：配電設備の照会のためアクセスしたもの

【営業系】

権限のない者によるアクセスは検出されなかった。

- 非公開情報にかかる画面制御の検討

【配電系】

北陸電力送配電への質問により、配電系ジョブは小売部門の利用資格を持つ ID

からのアクセスを不可とする仕組みであることを確かめた。あわせて、配電系ジョブの全操作ログから小売部門の利用資格のログを抽出した結果、ログは存在したもののいずれもエラーとなっていることを確かめた。

以上により、非公開情報にかかる画面制御が実装されている心証を得た。

【営業系】

北陸電力送配電から、当該システムの営業系ジョブにおいて非公開情報へのアクセス制御がなされている XX 画面に対応する「データチェック仕様」一式を入手し、画面制御の仕組みを確認した。確認の結果、小売部門の利用権限を持つ ID によるアクセス時にエラーとする、もしくは XXX、非公開情報閲覧ができない仕組みであることを確かめた。

以上により、非公開情報にかかる画面制御が実装されている心証を得た。

2) 操作ログの分析結果の概要

アクセスログ分析の結果、以下の操作ログを分析した。

(1) 権限のない者によるアクセス

配電系ジョブにおいて検出した XXID の操作ログを抽出し、確認した結果、すべてエラーとなっており、ジョブ No.入力画面の表示のみであったことを確かめた。

以上のことから、アクセスログ分析で識別した XXID について、配電系ジョブへのアクセスを試みたもののエラーとなっており、非公開情報の取得は行われていないことを確かめた。

1.5.3 結論

本調査の範囲において、非公開情報の管理の用に供するシステムである営業システムのログ分析の結果、非公開情報を入手可能なものによるアクセスのみが識別され、特定されたもののみが該当情報を入手することができることになっていた。

1.5.4 検出事項

ログ分析の結果、非公開情報へ権限のない者によるアクセスは識別されなかったが、ログ分析の過程で以下の気づき事項を検出した。

1.5.4.1 検出事項 No.1

検出事項の分類	気づき事項
概要	共有 ID の貸出記録（XXX）に記載誤り・漏れがあった
詳細	非常災害時及び欠員補填時に利用するため、共有 ID を利用している。共有 ID の利用は貸出管理により、利用者を特定できるよう運用しているが、共有 ID の利用に際し、貸出記録の貸出時刻記入誤り(操作ログ X 件分)及び記入漏れ（操作ログ XX 件分）が確認された。 なお、北陸電力送配電への質問により、記入が漏れていた操作ログについて利用者及び利用用途が特定できたこと並びに、共有 ID の利用時には、XXX、使用者には XXX は明かされない運用となっていると回答を得たことから、記入誤り及び漏れがあったものの管理者による承認の上で利用されていると心証を得た。
リスク	正確な利用者の特定が難しくなるリスクがある。
原因	貸出時刻の記入誤り：非常時研修のための共有 ID 利用であり、事前準備のため XXX に記入の上で貸し出しを行ったが、誤って研修の開始時刻を記入したことにより発生した。 記入漏れ：共有 ID カードの貸出時には XXX が必要である。XXX への記入を失念したことにより発生した。
改善の方向性	再発防止策として、XXX への貸出／返却の月日時分の記入徹底を周知している。また、恒久対策として XXX を導入し、共有 ID カードの廃止を検討している。

1.5.4.2 検出事項 No.2

検出事項の分類	気づき事項
概要	一部の社員外ユーザにおいて在籍状況と照らしたアクセス権の要否の確認が実施されていない
詳細	「XXX」において、以下記載のとおり、定められている。 送配電部門権限を有する社員外のユーザのうち XXX でシステムを利用するユーザについて、申請に基づき登録・削除を行い、申請に基づく所属情報と照らして権限設定状況の妥当性を年 X 回確認している。しかしながら、ユーザの在籍状況と照らしたアクセス権の要否の確認が実施されていなかった。この場合、退職や異動などによりユーザや権限が不要となったにもかかわらず、申請が行われなかったユーザが残存し、長期間発見されないリスクがある。

	【XXX】 第 XX 条（アクセス制御） 3　管理者は、XXX 4　情報セキュリティ管理者は、XXX (1)　アクセス権の設定状況を確認する対象システムは XXX。
リスク	退職や異動により不要になったユーザや権限が長期間残存することで、アカウントを不正利用されるリスクが高まる。
原因	送配電部門権限を有する社員外のユーザのうち XXX でシステムを利用するユーザは、20XX 年 XX 月に発行されており、以降申請の都度、登録・削除等を行っている。ID 発行から間もないことから、申請に基づき登録・削除された所属情報と照らした権限設定状況の確認で充足している認識であり、在籍者名簿などに基づく在籍情報と照らしたアクセス権の要否の確認まで実施していなかった。
改善の方向性	運用中の年 X 回の権限設定状況の確認に加え、該当のユーザを利用している委託先と協議の上、不要なユーザや権限が残存しないよう、対策を講じることが望まれる。 （対策案） 年次で権限の継続申請を受けたもののみ継続利用を認めることとし、継続申請のないユーザは権限を失効する運用とする。

1.6　関西電力送配電株式会社

1.6.1 対象システムの選定

1.6.1.1 対象システムの選定結果の概要

関西電力送配電株式会社（以下「関西電力 TD」という。）は、①FTTO 作業管理、②託送 OSS（ホスト）、③検針、④大口自動検針を対象にシステム選定のためのリスク評価を実施した。

リスク評価の結果は以下のとおり。

表 40 リスク評価結果（関西電力 TD）

システム名	システム重要度スコア	リスクの発生可能性評価スコア	トータルスコア
FTTO 作業管理	XX	XX	XX
託送 OSS（ホスト）	XX	XX	XX
検針	XX	XX	XX
大口自動検針	XX	XX	XX

関西電力 TD は「XXX」や「XXX」等により、各システムは概ね同様に統制が整備されている状況であり、大規模障害の発生等も確認されなかった。一方で、託送 OSS（ホスト）は、託送業務に直接関連し、多くの業務プロセスに関連するシステムであることに加え、保持する非公開情報の量が多く、ユーザ数 XX,XXX 名（うち社外ユーザ X,XXX 名）、アクセス数年間 XXX 百万件超と大規模である。また託送契約管理を含む複数の業務処理が統合された複雑性の高いシステムであること等から、ログ調査の対象システムに選定した。

1.6.2 システムログの分析

1.6.2.1 ログの分析

1）アクセスログ分析結果の概要

託送 OSS（ホスト）の 2024 年 7 月の端末操作ログを対象に、パイロットテスト及びアクセスログ分析を実施した。

表 41 ログ分析に利用したデータ一覧（関西電力 TD）

データ名	概要
託送 OSS の操作ログ	操作ログに該当するログ情報
託送 OSS（ホスト）_2023XXXX ログ	2023 年に実施したログ監査に係る証跡であり、操作ログのヘッダ情報
ホワイトリスト（N0002）	託送 OSS（ホスト）にアクセスが許可されている XXX の一覧、関西電力 TD のログ解析システムで不正アクセスの有無を判断する際に利用されている
2024XXXX_ID 一覧	ユーザ情報

(1) アクセスログ分析の対象ログ

託送 OSS（ホスト）では、アクセスのみを記録したログは存在しない。関西電力 TD より指定されたプログラムの自動実行などのログである「XX」が含まれる行を、操作ログから除外したものを調査に利用した。

なお、同様のログを対象にして関西電力 TD もログモニタリングを実施している。

(2) ホワイトリストの信頼性の確認

託送 OSS（ホスト）では、「XXX」に対して権限設定を行っていることから、XXX、システム利用時の認証に用いている。よって、関西電力 TD のログ解析システムで不正アクセスの有無を判断する際に利用されているホワイトリスト（アクセスが許可されている XXX の一覧）を有権限か否かの判断に利用した。

ホワイトリスト（アクセスが許可されている XXX の一覧）について、以下を確認しデータの信頼性は担保されていると判断した。

表 42 データの信頼性の確認結果（関西電力 TD）

利用情報	概要	データの信頼性の確認結果
ホワイトリスト（アクセスが許可されている XXX の一覧）	託送 OSS（ホスト）にアクセスが許可されている XXX の一覧、関西電力 TD のログ解析システムで不正アクセスの有無を判断する際に利用されている	変更日と、変更時点ごとのホワイトリストを保管している 2024/7/1 に変更があったが、その後、7/31 までに変更はなかった

(3) ログデータの網羅性

ログ保管に関する資料及びログ取得手順の閲覧並びに関西電力 TD への質問により、操作ログの網羅性を確認した。

関西電力 TD への質問により、操作ログはシステムが動作している XXX に常時保存されており、システム管理者権限を持つものしかアクセスできない旨回答を得た。また、「XXX」のフローを閲覧し、アクセスする際は XXX、操作ログの削除、変更は制限されていることを確かめた。

また、ログ抽出時のクエリ[10]を閲覧し、ログファイルの日付 (2024/7/1～2024/8/1) を指定して抽出しているのみであり、網羅性についても十分であるとの心証を得た。

また、操作ログについて全件取得しているとの回答を得ている。

以上より、ログデータの網羅性について心証を得たため、データ分析に利用可能と判断した。

(4) システム上の権限設定状況の確認

関西電力 TD への質問及び設計書の閲覧により、当該システムではユーザの「XXX」に対して権限設定を行っていることから、ユーザの XXX が関西電力 TD（一般送配電事業者）なのか、関西電力ホールディングス（以下「関西電力 HD」という。）（小売

[10] クエリは、データベースや情報システムに対して特定のデータを検索、取得、更新、削除するための命令文や問い合わせのことを指す。ここでは、ログデータを検索し、抽出するための特定の条件や指示を含む。

事業者）なのかで大別されていることを確かめた。

表 43 XXX に応じて自動付与される権限の内容

XXX	自動付与される権限
関西電力 TD	非公開情報にアクセス可能な権限
関西電力 HD	非公開情報にアクセス不可の権限 ※非公開情報はマスキングされ表示されない

(5) アクセスログの月次分析

1 か月分の操作ログから、関西電力 TD より指定されたプログラムの自動実行などのログである「XX」が含まれる行を除外したログを抽出し、ホワイトリスト（アクセスが許可されている XXX の一覧）に記載された XXX のユーザを有権限者、記載されていない XXX のユーザを権限のない者と識別しアクセスしたユーザを分類した。

さらに、有権限者については、ユーザ ID が個人別に付与された ID か、共有 ID かに分類した。

上記分類に基づき、XXX 毎のアクセス状況を以下に示す。

表 44 アクセス状況（関西電力 TD）

分類 1	分類 2	XXX	ID 数	アクセス回数 ※	アクセス回数 /XXX 別 ID 数
権限のない者	個人別 ID	関西電力 TD	XX	XXX	X.XX
		関西電力 HD	X	X	X.XX
有権限者	個人別 ID	関西電力 TD	X,XXX	X,XXX,XXX	XXX.XX
		関西電力 HD	X,XXX	X,XXX,XXX	X,XXX.XX
		他社（委託先）	X	X,XXX	XXX.XX
	共有 ID	関西電力 TD	XXX	X,XXX	XX.XX
		関西電力 HD	XXX	XXX,XXX	XXX.XX

※プログラムの自動実行などのログである「XX」が含まれるレコード以外をアクセス回数とカウントしているため、システム利用開始以外の操作もカウントしている可能性がある。

アクセスログの分析結果に基づき、操作ログ分析の対象となるか、以下の検討を実施した。

- 権限のない者によるアクセスの検討
  権限のない者によるアクセスが XXID 検出されている。当該 ID のログについて

関西電力 TD へ質問したところ、これらはアクセスエラーログであり、①トランザクションコードが「XXX」、②トランザクションコードが「XXX」のログに分類される旨回答を得た。また、①は託送営業のメニュー画面へアクセスしたログだが、権限のない者は以降の画面に遷移できない、②は XXX システムから託送 OSS（ホスト）へ画面連携した時のログだが、ログは出力されるものの連携自体は遮断されており、いずれも不正アクセスには該当しない旨回答を得た。

これら XXID について、エラーログ以外の操作ログが残っていないかを確認することにした。

- 個人別 ID のうち他社（委託先）ID の検討

個人別 ID のうち、他社（委託先）のアクセスが XID 検出されている。これらの ID について、「2024XXXX_ID 一覧（ユーザ情報）」を閲覧し、在籍会社を確認したところ、XID が関西電力 TD に籍があり、残りの XID が関西電力 HD に籍があることを確かめた。また、これらの ID について人事籍がある会社の、XXX が付与されていたため、詳細な検討は実施しない方針とした。

- 共有 ID の検討

関西電力 HD の共有 ID について利用用途を確認した結果、システム利用の共有 ID が X 件、個人利用の共有 ID が XXX 件であった。システム利用の共有 ID は、RPA ライセンスが紐づいた特別 ID（XXX に紐づかない ID）であるとの回答を得た。なお、当該 ID のログイン情報については、関電サービス請求Ｔ（ガス）メンバーのみ閲覧可能との回答を得た。

個人利用の ID については、顧客への通知業務やコールセンターでの受付業務等で利用されており、利用の都度貸出管理が行われている。

また、関西電力 TD に質問し、関西電力 HD の ID については、関西電力 HD の XXX が付与されており、非公開情報のマスキング処理によるアクセス制御がされているとの回答を得た。

以上より、関西電力 HD の共有 ID について利用用途が明確かつ、小売業者も利用可能な画面に限定された権限が自動付与されており、非公開情報へのアクセスができないため、詳細な検討は実施しない方針とした。

関西電力 TD の共有 ID について利用用途を確認した結果、すべて個人利用の共有 ID であった。関西電力 TD に質問し、個人利用の ID の利用用途については、委託会社の教育・研修、送配電コールセンターによる協業応援等の利用・非常災害時の受電応援や、非常災害時の窓口応援であり、利用の都度貸出管理が行われている旨回答を得た。当該 ID については、すべての画面を利用可能な権限が付与されており、不正利用のリスクが高いため、詳細な検討を実施した。

対象の共有 ID（XXXID）について、各所の共有 ID の管理者から、7 月の共有

ID の貸出しを管理している「利用管理簿」を入手し、操作ログと突合したところ、XXID で、管理簿の記録と操作ログが整合していることを確認した。
整合が確認できなかった XXID については、操作ログ分析を実施する。

- 有権限者によるアクセス日付の妥当性の確認(有効期間外のアクセス)

当該システムへのアクセスは、XXX で制御されており、関西電力 TD は、ログ解析システムにて、ユーザの XXX がホワイトリスト（アクセスが許可されている XXX の一覧）に記載されているか否かで、有権限者か否かを判定している。また、ホワイトリストを閲覧し、記載された XXX ごとに「XXX」、「XXX」が記載されていることを確かめた。
ログ解析システム上の判定ロジックについて、関西電力 TD に質問したところ、人事異動手続期間を考慮して、XXX のアクセスを不正アクセスと判定するロジックである旨回答を得た。また、関西電力 TD よりホワイトリストの記載の XX が 2024/7/1 に追加・変更されたものの、それ以降、7 月末まで変更ない旨回答を得た。
ホワイトリストを閲覧し、今回の「XXX」に「2024/7/2」と記載された XXX が XX あったため、当該 XXX かつエラーログ以外の操作ログが残されている ID を抽出したところ、XID のアクセスを識別した。当該 ID については、操作ログ分析を実施する。

- 有権限者によるアクセス権限の妥当性の確認

当該システムの権限について、基本的に XXX し設定されているため、許可された権限範囲以外のアクセスができない仕組みとなっている。また、XXX となっていることから、期間外に権限範囲外のアクセスが行われるリスクは低いと判断した。

また、特別 ID（コンテンポラリーユーザ、社外の ID が含まれる）については、ID の申請、ID 申請部署の役職者承認後、ID 一覧に追加される運用となっている。なお関西電力 TD より、申請者配下の XXX のみ申請が可能である旨回答を得た（関西電力 TDXXX を関西電力 HD が申請・承認することは不可能である）。また、当該ユーザは XXX である旨回答を得た。
特別 ID のアクセス権限の妥当性を確認するために、7 月中にアクセスのあった特別 ID の X,XXX ユーザから XX ユーザを無作為に抽出後、登録時の申請書もしくは直近の延長申請書を閲覧し、申請内容と実機の内容に不整合がないことを確かめた。

- 権限のない者によるアクセスの理由確認

権限のない者のアクセスにて、XXID、XXX レコードのアクセスエラーログを検出している。当該アクセスエラーログ発生の背景について、関西電力 TD に質問

し、以下回答を得た。

① トランザクションコードが「XXX」のログ（託送営業のメニュー画面へアクセスしたログ。ただし、ホワイトリストにない XXX は以降の画面に遷移できない）は X レコードのみであり、メニューであれば、誰でもアクセスは可能なため、単純に誤ってアクセスしたログである。

② トランザクションコードが「XXX」のログ（XXX システムから託送 OSS（ホスト）へ画面連携した際のログ。ただし、連携自体は遮断）は XXX レコードであり、そのうち XXX レコードのアクセスは、XXX 部門の所属である。XXX 業務においては XXX などで XXX システムを閲覧する機会が頻繁にあるためログが残っている。なお、当該ログは XXX システムを閲覧した際に、託送 OSS との連携画面で出力されているものであり、連携画面へはアクセスできるが、託送 OSS への連携は遮断されている。残りの X レコードは、過去に XXX 部門に所属していた者が問い合わせ対応等で XXX システムにアクセスしたものであるが、同様に託送 OSS への連携は遮断されている。

以上より、①のログについては意図しない誤操作であり、かつ件数も少数であること、②のログについて件数は多いものの、業務上必要な理由であることを確認できたため、不正アクセスを試みたログではないと判断した。

- 非公開情報にかかる画面制御の検討

関西電力 TD が作成している仕様書から、当該システムにおける「非公開情報（契約者情報）にアクセス可能な業務画面一覧」を特定し、特定した計 XXX 画面から XX 画面を無作為に抽出し、関西電力 TD の ID、関西電力 HD の ID の操作画面スクリーンショットを確認した。なお、関西電力 HD の ID の操作画面スクリーンショットは TD の託送・事務システム G のユーザが、当該システムの維持運用業務のため、XXX、TD ユーザが代替して取得した。（XXX）

確認の結果、すべての画面において関西電力 HD の ID で契約者情報の閲覧ができないことを確かめた。

以上より、非公開情報にかかる画面制御が実装されている心証を得た。

2) 操作ログの分析結果の概要

アクセスログ分析の結果、以下の操作ログを分析した。

(1) 権限のない者によるアクセス

権限のない者によるアクセスにて、XXID、XXX レコードのアクセスエラーログを検出している。

当該 ID のログ XXX レコードを抽出し、分析を実施したところ、関西電力 TD の説明通り、トランザクションコードが「XXX」もしくは「XXX」のレコードのみであり、

エラーログ以外の操作ログがないことを確かめた。よって、不正アクセスには該当しないと判断した。

(2) 共有 ID の検討

関西電力 TD の個人利用の共有 ID、XXXID について、各所属の共有 ID の管理者から、7 月の共有 ID の貸出しを管理している「利用管理簿」を入手し、操作ログと突合したところ、XXID、XXX レコードで、管理簿の記録と操作ログで整合が確認できなかった。不整合が生じている理由について関西電力 TD に質問し、以下回答を得た。

表 45 不整合の理由についての確認結果

#	ID 数	レコード数	関西電力 TD 回答
①	XX	XX	2024/7/19 に防災訓練を開催した際に、訓練担当者が非常時対応においての共有 ID のログイン確認を行ったものであり、個別貸出していないため記録を残していない
②	XX	XX	管理者が、貸出前にテストログインしたもの（7/1 の XXX 変更に伴い）であり、個別貸出していないため記録を残していない
③	X	XX	非常時応援や新規配属者研修の実施前に管理者がテストログインしたものであり、個別貸出していないため記録を残していない
④	X	XX	「利用管理簿」への貸出記録、記載漏れ

※XID について、#①、④のレコードが存在したため、表上の合計が XXID となっている。

①の操作ログについて確認したところ、すべて 2024/7/19 に記録されたトランザクションコードが「XXX」のログ（託送営業のメニュー画面へアクセスしたログ）であること、XID あたりのレコード数が X 回以下であることを確かめた。②、③の操作ログについて確認したところ、同様に、すべてトランザクションコードが「XXX」のログであり、1ID あたりのレコード数が X 回以下であることを確かめた。

よって、上記①-③については、関西電力 TD 回答の妥当性を確認できたため、共有 ID の不正利用には当たらないと判断した。

④の操作ログ XID、XX レコードについて、ID 別に検討を実施した。

■1ID/20 レコードの詳細

④のうち XX レコードの操作ログについて、貸出記録への記載漏れの理由を関西電力 TD 担当者に質問したところ、以下の回答を得た。

- 共有 ID の貸出は、管理者により、利用の都度以下の通り実施される。
  ① 管理簿に利用者や利用時間等の情報を記録
  ② カードを利用者に貸出
  ③ 利用者からカード返却後、その旨を管理簿に記録
- 当該共有 ID 利用者（以下「同氏」という）には、もともと個人用の特別 ID が付与されていた。2024/7/1 の XXX に伴い XXX を変更するために、一時的に個人用のカードが回収され、その間、当該共有 ID が個人用として貸与され、業務を実施していた。
- 今回、都度の貸出ではなく、特定の期間中におけるカード貸与であったため、期間を通じた管理者を別途設け、貸出管理簿の記録等を行っていた。
- 同氏が出勤シフトではない X/XX に出勤（別の担当者の代わりに出勤）し、当該 ID を利用した。しかしながら、当該出勤日の管理者から期間を通じた管理者へシフト変更があったことを伝達できていなかった。
- 期間を通じた管理者は当初の予定が記載されたシフト表をもとに管理簿を記録したため、X/XX の貸出記録が残されていなかった。

また、④のうち XX レコードはいずれも 2024/X/XX に記録されたログであり（停電問い合わせ対応を実施した日であり、委託会社のシフト表と整合)、ログに残されたログイン端末情報から利用者を特定しており、第三者の利用がないことを確認した旨回答を得た。

よって、貸出記録への記載漏れは発見事項とするが、共有 ID の不正利用には当たらないと判断した。

■XID/X レコードの詳細

④のうち X レコードの操作ログについて、貸出記録への記載漏れの理由を関西電力 TD 担当者に質問したところ、ヒューマンエラーによる管理簿の更新漏れであったとの回答を得た。

また、④のうち X レコードの操作ログはいずれも 2024/X/X に記録されたログであり（委託会社のシフト表と整合)、ログに残されたログイン端末情報から利用者を特定しており(18 時まではオペレータ、その後は管理者が利用)、第三者の利用がないことを確認した旨回答を得た。

なお、当該 ID の操作ログは、2024/7/1、2024/7/15 に計 XX レコード検出しているが、いずれも管理簿に利用記録が残されていることを確認している。

よって、貸出記録への記載漏れは気づき事項とするが、共有 ID の不正利用には当たらないと判断した。

(3) 有権限者によるアクセス日付の妥当性の確認(有効期間外のアクセス）

2024/7/1 に「XXX」が「2024/X/X」と記載された XXX が XX あったため、当該 XXX かつエラーログ以外の操作ログが残されている ID のアクセスを抽出したとこ

ろ、XID を識別した。なお当該 ID は、特別 ID である。

当該 ID の操作ログを抽出し、分析を実施したところ、「2024/7/12（XXX）」までは XXX、「2024/7/16」以降は XXX による操作ログが残されていることを確かめた。

また、関西電力 TD に質問し、当該 ID の XXX 変更手続きが 7/16 に完了したため、7/12 までは旧 XXX のアクセスログが検出されている旨回答を得た。なお、旧 XXX、新 XXX ともに、託送 OSS（ホスト）へのアクセスが許可された XXX 間の変更のため、変更手続きの遅れについてのリスクは低いと判断した。

以上より、ホワイトリスト上でアクセス許可がなくなったユーザについて、「XXX」から XXX を超えたアクセスは検出されなかったため、不正アクセスには該当しないと判断した。

1.6.3 結論

本調査の範囲において、非公開情報の管理の用に供するシステムである託送 OSS（ホスト）のログ分析の結果、非公開情報を入手可能な者によるアクセスのみが識別され、特定された者のみが当該情報を入手することができることになっていた。

1.6.4 検出事項

ログ分析の結果、非公開情報へ権限のない者によるアクセスは識別されなかったが、ログ分析の過程で以下の気づき事項を検出した。

1.6.4.1 検出事項 No.1

検出事項の分類	気づき事項
概要	個人利用の特別 ID のうち XID が、利用者名で登録されていなかった。
詳細	2024 年 4 月より、「XXX」が施行され、特別 ID は利用者名にて申請することを原則とし、利用者名でない場合（共有 ID）は XXX と事前協議を行ったうえで申請を行う運用となっている。また、すべての特別 ID は有効期限 X 年がシステム設定されており、登録から X 年経過する都度、延長申請を行わなければシステム上無効化される。加えて、事業者より、延長申請の都度、利用者名でない特別 ID については、XXX との協議を実施する運用である旨回答を得た。 当該 XID は、いずれも上記ルール施行前の XXXX 年 X 月以前に登録された、有効期限が XXX の ID であり、当初共有 ID として申請されていた。しかしながら、XID とも 1ID につき 1 人しか使用していなかったことが利用実態として判明したため、ID 名を利用者名に変更した。
リスク	特別 ID の利用者特定が困難になり、正確に管理できなくな

	るリスク
原因	特別 ID に関するルールの施行前に、申請・登録された ID であり、かつ、検出時点で更新時期を迎えておらず、XXX との協議が未実施だったため。
改善の方向性	XXXX 年 X 月末で、すべての特別 ID で XXX との協議が実施される、もしくは、無効化されるため、是正される見込み。

1.6.4.2 検出事項 No.2

検出事項の分類	気づき事項
概要	関西電力 TD の共有の特別 ID のうち、XID について「利用管理簿」に貸出記録が残されていなかった。
詳細	■XID/XX レコード 共有 ID の貸出は、管理者により、利用の都度以下の通り実施される。 ① 管理簿に利用者や利用時間等の情報を記録 ② カードを利用者に貸出 ③ 利用者からカード返却後、その旨を管理簿に記録 当該共有 ID 利用者には、もともと個人用の特別 ID が付与されていたが、2024/7/1 の XXX に伴い XXX を変更するために一時的に個人用のカードが回収されており、その間、当該共有 ID が個人用として貸与され、業務を実施していた。 今回、都度の貸出ではなく、特定の期間中におけるカード貸与であったため、期間を通じた管理者を別途設け、貸出管理簿の記録等を行っていた。 同氏が出勤シフトではない X/XX に出勤（別の担当者の代わりに出勤）し、当該 ID を利用した。しかしながら、当該出勤日の管理者から期間を通じた管理者へシフト変更があったことを伝達できていなかった。 期間を通じた管理者は当初の予定が記載されたシフト表をもとに管理簿を記録したため、X/XX の貸出記録が残されていなかった。 ■XID/X レコード 2024/X/X の利用について、管理簿の更新漏れがあった。
リスク	共有 ID の利用者、操作内容の特定が難しくなるリスク
原因	共有の特別 ID に関する運用が一部徹底されていなかった。
改善の方向性	事業者より、託送 OSS（ホスト）にて、XXXX/X/X より、

	共有 ID 利用時の運用について、管理者がツール上で XXX をアップロード後に XXX が発行される仕組みが実装されている旨回答を得た。

1.7　中国電力ネットワーク株式会社

1.7.1 対象システムの選定

1.7.1.1 対象システムの選定結果の概要

中国電力ネットワーク株式会社（以下「中国電力 NW」という。）は、①託送料金システム、②営業システム③お客さま台帳検索システム、④設備保全管理システムを対象にシステム選定のためのリスク評価を実施した。

リスク評価の結果は以下のとおり。

表 46 リスク評価結果（中国電力 NW）

システム名	システム重要度スコア	リスクの発生可能性評価スコア	トータルスコア
託送料金システム	XX	XX	XX
営業システム	XX	XX	XX
お客さま台帳検索システム	XX	XX	XX
設備保全管理システム	XX	XX	XX

中国電力 NW は「XXX」や「XXX」等の規程により、各システムは概ね同様に統制が整備されている状況であり、大規模障害の発生も確認されなかった。一方で、営業システムは、託送業務に関連し託送情報を取り扱うシステムであり、アクセス数年間約 XX.X 百万件と他システムと比較して大規模である。また XX の外部システムと接続し、メインフレーム X 台の他、サーバ約 XX 台から構成されており、複雑性が高いと判断したこと等からログ調査の対象システムに選定した。

1.7.2 システムログの分析

1.7.2.1 ログの分析

1) アクセスログ分析結果の概要

営業システムの 2024 年 7 月の端末操作ログを対象に、パイロットテスト及びアクセスログ分析を実施した。当該システムは X つのサブシステム（XXX）から構成されている。また、対象ログ、アクセス制御単位はサブシステムごとに分かれており、下表のような対応関係となっている。

サブシステムごとのログ分析結果を可視化することを目的として、ログ分析は 5 つの分析単位に分割して進める方針とした。

なお、カスタマー機能を構成するXシステムのうち、Xシステム（XXX）については、操作ログからアクセスログが抽出可能という共通点から、束ねて評価した。

また、残りのXシステム（XXX）については、ログイン後、ユーザ権限に応じた操作画面に直接遷移するため、操作ログを対象として分析を実施するという共通点から、束ねて評価した。

表 47 ログ分析の全体像

	サブシステム	対象ログ	アクセス制御単位	分析単位
営業システム	営業オンライン	信頼性 Web ログ	営業オンライン利用権限 XXX 一覧	(1)営業オンライン
	分散オンライン		分散オンライン利用権限 XXX 一覧	(2)分散オンライン
	地図機能	営業地図ログ		(3)地図機能
	カスタマー機能	A システムログ	CC_利用権限一覧	(4)カスタマー機能①
		B システムログ		
		C システムログ		
		D システムログ		(5)カスタマー機能②
		E システムログ		
		F システムログ		

なお、上記いずれのログについても、アクセスログと操作ログが一つのファイルに出力される仕様である。ユーザ情報は ID 管理システムで集中管理されている。

表 48 ログ分析に利用したデータ一覧（中国電力 NW）

データ名	概要
・信頼性 Web ログ ・営業地図ログ ・A システムログ ・B システムログ ・C システムログ ・D システムログ ・E システムログ ・F システムログ	操作ログに該当するログ情報
・営業オンライン利用権限 XXX 一覧 ・分散オンライン利用権限 XXX 一覧 ・CC_利用権限一覧	アクセス制御単位ごとに、営業システムにアクセス可能な XXX、個別登録 ID（人事情報と連携しない ID）の一覧
ユーザ情報	ユーザ情報（ID 管理システムより抽出）

(1) アクセスログ分析の対象ログ

営業システムでは、アクセスのみを記録したログは存在しない。

分析単位(1)-(4)については、操作ログから中国電力 NW より指定されたメニュー画面もしくは起動時に必ず経由する画面 ID のログを抽出した。さらに、抽出したログからユーザ ID が空白となっているシステム処理のログを除外したものを調査に利用した。

分析単位(5)については、ログイン後、XXX 遷移するため、操作ログ全件から、XXX となっているシステム処理のログ、及び画面 ID が XXX を除外したものを調査に利用した。

表 49 分析単位別のログの概要

分析単位	対象ログ	アクセスログ抽出条件	除外条件
(1)営業オンライン	信頼性 Web ログ	画面 ID=XXX、XXX	ユーザ ID が空白
(2)分散オンライン		画面 ID=XXX	ユーザ ID が空白
(3)地図機能	営業地図ログ	機能コード＝XXX、XXX	ユーザ ID が空白
(4)カスタマー機能①	A システムログ	画面 ID=XXX	なし
	B システムログ	画面 ID=XXX	ユーザ ID が空白
	C システムログ	画面 ID=XXX	なし
(5)カスタマー機能②	D システムログ	なし（操作ログを分析）	ユーザ ID が空白
	E システムログ		なし

分析単位	対象ログ	アクセスログ抽出条件	除外条件
	F システムログ		画面 ID が空白、画面 ID が日本語のボタン押下の操作

(2) ホワイトリストの信頼性の確認

中国電力 NW において、ホワイトリストは作成していない。

営業システムでは、「XXX」に対して権限設定を行っていることから、XXX を受領し、システム利用時の認証に用いている。よって、利用権限 XXX 一覧（アクセス可能な XXX、個別登録 ID の一覧）を有権限か否かの判断に利用した。

なお、信頼性 Web ログ、営業地図ログには、アクセスユーザの XXX が残らない仕様であるため、分析単位(1)-(3)については、当法人にて利用権限 XXX 一覧、ユーザ情報をもとに権限者リストを作成し、ホワイトリストとして利用した。

利用権限 XXX 一覧と、分析単位(1)-(3)でホワイトリストを作成するために利用したユーザ情報について、以下を確認しデータの信頼性は担保されていると判断した。

表 50 データの信頼性の確認結果（中国電力 NW）

利用情報	概要	データの信頼性の確認結果
・営業オンライン利用権限 XXX 一覧 ・分散オンライン利用権限 XXX 一覧 ・CC_利用権限一覧	制御単位ごとに、営業システムにアクセス可能な XXX、個別登録 ID（人事情報と連携しない ID）の一覧	変更履歴情報（変更日と変更箇所）を記録に残している。2024/7/1-7/31 の間に変更はなかった。
ユーザ情報	ユーザ情報（ID 管理システムより抽出）	ID 管理システムは人事情報と自動連携しており、ID 管理システムの情報が各業務システムに自動連携される。本分析では 2024/8/1 時点で ID 管理システムより出力したユーザ情報を利用した。

(3) ログデータの網羅性

ログ保管に関する資料及びログ取得手順の閲覧並びに中国電力 NW への質問により、操作ログの網羅性を確認した。

中国電力 NW への質問により、操作ログはシステム部門が管理するログ管理サーバに常時保存されており、利用部門は当該サーバにアクセスできない旨回答を得た。

また、ログ抽出時もログファイルの日付（2024/7/1～2024/7/31）を指定して抽出

しているのみであり、網羅性についても十分であるとの心証を得た。なお、操作ログについて全件取得しているとの回答を得ている。

以上より、ログデータの網羅性について心証を得たため、データ分析に利用可能と判断した。

(4) システム上の権限設定状況の確認

中国電力 NW への質問及び設計書の閲覧により、「XXX」に対して権限設定を行っていることから、所属する組織が中国電力 NW（一般送配電事業者）なのか、中国電力（小売事業者）なのかで大別されていることを確認した。

表 51 XXX に応じて自動付与される権限の内容

XXX	自動付与される権限
中国電力 NW	非公開情報にアクセス可能な権限
中国電力	非公開情報にアクセス不可の権限 ※非公開情報はマスキングされ表示されない

(5) アクセスログの月次分析

1 か月分の操作ログから中国電力 NW より指定されたログを抽出し、分析単位ごとに、営業システムにアクセスしたユーザを有権限者と権限のない者に分類した。分析単位別の、未加工ログ（操作ログ）、分析対象ログ、権限有無の判断根拠を以下に示す。

表 52 分析単位別の分析対象ログ及び権限有無の判断根拠

分析単位	未加工ログ（操作ログ）	分析対象ログ（抽出後）※	権限有無の判断根拠
⑴営業オンライン	信頼性 Web ログ	アクセスログ	「営業オンライン利用権限 XXX 一覧」と「ユーザ情報」から作成したホワイトリストへの記載有無
⑵分散オンライン		アクセスログ	「分散オンライン利用権限 XXX 一覧」と「ユーザ情報」から作成したホワイトリストへの記載有無
⑶地図機能	営業地図ログ	アクセスログ	
⑷カスタマー機能①	A システムログ	3 システムから抽出したアクセスログをマージ	CC_利用権限一覧（アクセス可能な XXX、個別登録ユーザの一覧）への記載有無
	B システムログ		
	C システムログ		
⑸カスタマー機能②	D システムログ	3 システムの未加工ログ（操作ログ）をマージ	
	E システムログ		

分析単位	未加工ログ（操作ログ）	分析対象ログ（抽出後）※	権限有無の判断根拠
	F システムログ		

※抽出条件については、(1)アクセスログ分析の対象ログの表 49 を参照

さらに、有権限者については、ユーザ ID が個人別に付与された ID か、共有 ID かに分類した。

上記分類に基づき、分析単位別の所属毎のアクセス状況を以下に示す。

表 53 アクセス状況 分析単位(1)：営業オンライン

分類 1	分類 2	所属	ID 数	アクセス回数	アクセス回数/所属別 ID 数
権限のない者	個人別 ID	中国電力	XX	XX	X.XX
有権限者	個人別 ID	中国電力 NW	XXX	XX,XXX	XX.XX
		中国電力	X,XXX	XXX,XXX	XX.XX
	共有 ID	中国電力 NW	X	XX	X.XX

表 54 アクセス状況 分析単位(2)：分散オンライン

分類 1	分類 2	所属	ID 数	アクセス回数	アクセス回数/所属別 ID 数
権限のない者	—	—	—	—	—
有権限者	個人別 ID	中国電力 NW	XXX	XX,XXX	XX.XX
		中国電力	XXX	XXX,XXX	XXX.XX
	共有 ID	中国電力	X	XX	XX.XX

表 55 アクセス状況 分析単位(3)：地図機能

分類 1	分類 2	所属	ID 数	アクセス回数	アクセス回数/所属別 ID 数
権限のない者	—	—	—	—	—
有権限者	個人別 ID	中国電力 NW	XXX	XX,XXX	XX.XX
		中国電力	XXX	XX,XXX	XX.XX

表 56 アクセス状況 分析単位(4)：カスタマー機能①（XXX のログをマージして分析）

分類 1	分類 2	所属	ID 数	アクセス回数	アクセス回数/所属別 ID 数
権限のない者	—	—	—	—	—
有権限者	個人別 ID	中国電力 NW	X,XXX	XX,XXX	XX.XX
		中国電力	XXX	XX,XXX	XXX.XX
	共有 ID	中国電力 NW	X	XXX	XX.XX
		中国電力	X	XX	XX.XX

表 57 アクセス状況 分析単位(5)：カスタマー機能②（XXX のログをマージして分析）

分類 1	分類 2	所属	ID 数	操作回数※	アクセス回数/所属別 ID 数
権限のない者	—	—	—	—	—
有権限者	個人別 ID	中国電力 NW	X,XXX	X,XXX,XXX	X,XXX.XX
		中国電力	X,XXX	XX,XXX,XXX	XX,XXX.XX
	共有 ID	中国電力 NW	XX	X,XXX	XX.XX
		中国電力	X	XX	XX.XX

※直接画面遷移するため、操作ログをカウントしている

アクセスログの分析結果に基づき、操作ログ分析の対象となるか、以下の検討を実施した。

- 権限のない者によるアクセスの検討

  分析単位(2)-(5)では権限のない者によるアクセスはなかった。

  分析単位(1)で権限のない者によるアクセスが XXID 検出されている。当該 ID のログについて中国電力 NW へ質問したところ、これらはアクセスエラーログであり、XXX、実際にはアクセスが拒否されており、不正アクセスには該当しない旨回答を得た。

  これら XXID について、エラーログ以外の操作ログが残っていないかを確認することにした。

- 共有 ID の検討

  中国電力所属の共有 ID について分析単位(2)で X 件、分析単位(4)で X 件、分析単位(5)で X 件検出した。

  それぞれの利用用途について中国電力 NW へ質問し、分析単位(2)の X 件につい

ては、災害時等の応援派遣業務を実施する場合に利用する個人利用の ID であり、利用の都度貸出管理が行われている旨回答を得た。

一方で、分析単位(4)の X 件、分析単位(5)の X 件については、いずれもカスタマー機能の本番テストで用いる個人利用の個別登録 ID（人事情報と連携しない ID）である。貸出管理は行われていないが、中国電力販売システム開発グループ担当者が所属ごとの動作確認を実施する際に利用している旨回答を得た。また、当該 ID・パスワードは XXX 旨回答を得た。

なお、中国電力所属の ID については、中国電力の XXX が付与されており、非公開情報のマスキング処理によるアクセス制御、もしくは非公開情報が表示された画面への遷移が不可になっている旨中国電力 NW より回答を得ている。なお、マスキング処理については後述の「非公開情報にかかる画面制御の検討」で確認する。

以上より、中国電力所属の共有 ID について利用用途が明確かつ、小売業者も利用可能な画面に限定された権限が自動付与されており、非公開情報へのアクセスができないため詳細な検討は実施しない方針とした。

中国電力 NW 所属の共有 ID については、分析単位(1)で X 件、分析単位(4)で X 件、分析単位(5)で XX 件検出した。

それぞれの利用用途について中国電力 NW へ質問し、分析単位(1)の X 件及び、分析単位(5)の X 件については、いずれも災害時等の応援派遣業務を実施する場合に利用する個人利用の ID であり、利用の都度貸出管理が行われている旨回答を得た。

一方で、分析単位(4)の X 件及び、分析単位(5)の X 件については、いずれもカスタマー機能の本番テストで用いる個人利用の個別登録 ID（人事情報と連携しない ID）である。貸出管理は行われていないが、中国電力 NW サービスシステム開発グループ担当者が所属ごとの動作確認を実施する際に利用している。ID・パスワードは他部署に漏洩しないように管理しているとともに、パスワードの定期的な強制変更がシステム設定されている旨回答を得た。

また、分析単位(5)の X 件については、システム動作等の問い合わせ対応に利用する個人利用の個別登録 ID（人事情報と連携しない ID）であり、貸出管理は行われていないが、中国電力 NW 配電運営第 2 グループ担当者が利用しており、ID・パスワードは他部署に漏洩しないように管理しているとともに、パスワードの定期的な強制変更がシステム設定されている旨回答を得た。

中国電力 NW 所属の共有 ID のうち、分析単位(1)の X 件及び、分析単位(5)の X 件で利用されている災害対応用の ID については、利用者が特定の部門担当者に限定されていない、かつすべての画面を利用可能な権限が付与されており、不正利用のリスクが高いため、次の検討を実施した。

当該 ID について、各所属の共有 ID の管理者から、7 月の共有 ID の貸出しを管理している「利用管理簿」を入手し、対象のログ（分析単位⑴はアクセスログ、分析単位⑸は操作ログ）と突合したところ、管理簿の記録とログが整合していることを確認した。

- 有権限者によるアクセス日付の妥当性の確認(有効期間外のアクセス）

当該システムへのアクセスは、XXX で常時制御されており、中国電力 NW より 2024 年 7 月中における当該権限情報の変更はないとの回答を得ているため、確認は不要と判断した。

- 有権限者によるアクセス権限の妥当性の確認

当該システムの権限について、基本的に XXX 設定されているため、許可された権限範囲以外のアクセスができない仕組みとなっている。また、人事情報の反映は、異動日から新所属情報に更新されタイムラグのない運用となっていることから、期間外に権限範囲外のアクセスが行われるリスクは低いと判断した。

また、個別登録 ID（人事情報と連携しない ID）については、一括保守システム（業務システム保守管理業務を管理するシステム）によりワークフローで申請・承認後、ID 一覧に追加される運用となっている。なお、中国電力 NW より、申請者配下の XXX のみ申請が可能である旨回答を得た（中国電力 NW の XXX を中国電力が申請・承認することは不可能)。また、当該ユーザを含めて XX でユーザ棚卸を実施している旨回答を得た。

個別登録 ID のアクセス権限の妥当性を確認するために、7 月中にアクセスのあった個別登録 IDXX 件のうち XX 件について、登録時のワークフローを閲覧し、申請内容と実機の所属内容に不整合がないことを確認した。なお、X 件については、利用権限付与時期が古いため、一括保守システムでの保存期間超過によりワークフローは確認できなかったが、利用者、利用用途、利用用途に応じた所属が設定されていることを確認した。

- 権限のない者によるアクセスの理由確認

分析単位⑴で、権限のない者によるアクセスにて XXID、XX レコードのアクセスエラーログを検出している。当該アクセスエラーログ発生の背景について、中国電力 NW に質問したところ、XXX ためにログイン情報の入力を誤ったケースが多くを占めており、一方で、所属部署が異動となったユーザが異動後に営業システムの利用が可能か確かめたケースもあったとの回答を得た。

また、当該アクセスエラーログについて、ユーザごとのエラー件数を確かめたところ、最多でも XX 件前後であり上記回答と不整合はない心証が得られたため、不正アクセスを試みたログではないと判断した。

- 非公開情報にかかる画面制御の検討

中国電力 NW が作成している「画面遷移可否一覧表」を入手し、分析単位ごとに中国電力所属のユーザが遷移できる画面を特定した。

特定した画面から無作為に抽出し、中国電力 NW 所属の ID、中国電力所属の ID の操作画面スクリーンショットを確認した。

以下に、分析単位別の中国電力所属のユーザが遷移できる画面数、無作為抽出した画面数を示す。

表 58 画面の総数と無作為抽出数

分析単位	中国電力所属のユーザが遷移できる画面数	無作為抽出数
(1)営業オンライン	X,XXX	XX
(2)分散オンライン	XX	X
(3)地図機能	XX	X
(4)カスタマー機能①	XX	X
(5)カスタマー機能②	XX	X

確認の結果、すべての画面において中国電力所属の ID で非公開情報の閲覧ができないことを確認した。

以上より、非公開情報にかかる画面制御が実装されている心証を得た。

2) 操作ログの分析結果の概要

アクセスログ分析の結果、以下の操作ログを分析した。

(1) 権限のない者によるアクセス

分析単位(1)のアクセスログ分析の結果、権限のない者によるアクセスにて XXID、XX レコードのアクセスエラーログを検出している。

当該 ID の操作ログ全件を抽出したところ、XXX レコードであった。中国電力 NW の説明通り、操作ログもアクセスエラーに関する画面遷移ログや、エラーに伴い業務開始メニューを終了したログのみであり、エラー以外の操作ログがないことを確認した。よって、不正アクセスには該当しないと判断した。

1.7.3 結論

本調査の範囲において、非公開情報の管理の用に供するシステムである営業システムのログ分析の結果、非公開情報を入手可能な者によるアクセスのみが識別され、特定された者のみが当該情報を入手することができることになっていた。

1.7.4 検出事項

ログ分析の結果、非公開情報へ権限のない者によるアクセスは識別されず、検出事項はなかった。

1.8　四国電力送配電株式会社

1.8.1 対象システムの選定

1.8.1.1 対象システムの選定結果の概要

四国電力送配電株式会社（以下「四国電力送配電」という。）は、①再エネ買取管理システム、②託送お客さま管理システム、③配電情報総合提供システム、④スマートメーター管理システムを対象にシステム選定のためのリスク評価を実施した。

リスク評価の結果は以下のとおり。

表 59 リスク評価結果（四国電力送配電）

システム名	システム重要度スコア	リスクの発生可能性評価スコア	トータルスコア
再エネ買取管理システム	XX	XX	XX
託送お客さま管理システム	XX	XX	XX
配電情報総合提供システム	XX	XX	XX
スマートメーター管理システム	XX	XX	XX

四国電力送配電は「XXX」や「XXX」等の規程により、各システムは概ね同様に統制が整備されている状況であり、大規模障害の発生も確認されなかった。一方で、託送お客さま管理システムは、託送情報を取り扱うシステムであり、データ連携や処理機能数が他システムと比較して多いこと、ユーザ数 X,XXX 名（うち社外ユーザ XXX 名）、アクセス数年間約 XXX,XXX 件と多いこと等から、ログ調査の対象システムに選定した。

1.8.2 システムログの分析

1.8.2.1 ログの分析

1）アクセスログ分析結果の概要

託送お客さま管理システムの 2024 年 7 月の端末操作ログを対象に、パイロットテスト及びアクセスログ分析を実施した。なお、託送お客さま管理システムはアクセスログと操作ログが個別にファイルに出力される仕様である。

表 60 ログ分析に利用したデータ一覧（四国電力送配電）

データ名	概要

アクセスログ	託送お客さま管理システムにおけるアクセスログ情報
操作ログ	託送お客さま管理システムにおける操作ログ情報
【四国送配】名簿（7 月分)、(8 月分)	ホワイトリスト（託送お客さま管理システムにアクセス可能なユーザ情報）
画面 ID 一覧	託送お客さま管理システムにおける利用画面一覧（アクセスログ、操作ログの補足情報）
【四国送配】社内役職名簿 7.1 時点、8.1 時点	役職一覧(人事情報)

(1) アクセスログ分析の対象ログ

託送お客さま管理システムはアクセスログを分析に利用した。

(2) ホワイトリストの信頼性の確認

四国電力送配電は以下の情報をもとに、四国電力送配電が手で加工した名簿をホワイトリストとして利用した。ホワイトリストを作成するために利用した情報、及び当法人にて分析対象月直前(2024 年 6 月度)の ID 棚卸結果とホワイトリストの差分を抽出し、改廃が発生しているユーザについて、人事情報を確かめ、データの信頼性は担保されていると判断した。

表 61　データの信頼性の確認結果（四国電力送配電）

利用情報	概要	データの信頼性の確認結果
ユーザ一覧（7 月 2 日、8 月 2 日時点）	託送お客さま管理システムの実機から出力したユーザ情報、権限情報一覧である。	実機情報から直接取得したデータをもとにしており、抽出時の出力条件を確かめ、網羅性、正確性について十分な心証を得た。
【四国送配】託送システム権限設定 20240605	託送お客さま管理システムの 2024 年 6 月 5 日における ID 棚卸結果である。	四国電力送配電が実施した ID 棚卸結果をもとにしており、実施方法について質問し、網羅性、正確性について十分な心証を得た。
【四国送配】社内役職名簿 7.1 時点、8.1 時点	人事情報における役職一覧である。	人事情報であり、網羅性、正確性について十分な心証を得た。

利用情報	概要	データの信頼性の確認結果
6、7 月度の人事発令情報(対象者のみ)	ユーザ一覧と 6 月 5 日 ID 棚卸結果の差分を抽出し、対象者を選定、6 月～8 月 2 日までの当該期間における対象者の人事異動・採用・退職情報である。	対象者について、四国電力送配電へ質問及び、人事情報をもとに網羅性、正確性について十分な心証を得た。

(3) ログデータの網羅性

ログ保管に関する資料及びログ取得手順の閲覧並びに四国電力送配電への質問により、アクセスログ及び操作ログの網羅性を確認した。

アクセスログ分析で利用したログ(アクセスログ、操作ログ)は、XXX バックアップ保管している。ログが記録、保管されているサーバの、システム利用者や第三者がアクセスできない場所に保管している。

ログ抽出時の取得作業画面を閲覧し、7 月分のファイルを取得していることを確かめ、網羅性についても十分であるとの心証を得た。

以上より、ログデータの網羅性について心証を得たため、データ分析に利用可能と判断した。

(4) システム上の権限設定状況の確認

四国電力送配電への質問及び設計書の閲覧により、権限設定について、託送 SC、NW 営業、NW 配電、小売権限があることを確かめた。

表 62 権限設定の概要（四国電力送配電）

権限の種類	権限の内容
託送 SC	・非公開情報にアクセス可能な権限 ・ネットワークサービスセンター 、系統運用部、XXX （システム開発・保守の受託者）が利用
NW 営業	・非公開情報にアクセス可能な権限 ・事務系部門が利用
NW 配電	・非公開情報にアクセス可能な権限 ・配電系部門及び、XXX（配電工事の受託者）が利用
小売	・非公開情報にアクセス可能な権限 ・四国電力株式会社が利用(災害復旧対応時用) ※2024 年 6 月以降利用停止済

(5) アクセスログの月次分析

1か月分のアクセスログから託送お客さま管理システムのログインに係るログを抽出し、ホワイトリストと照合した。ホワイトリストに記載されたユーザを有権限者、記載のないユーザを権限のない者と識別しアクセスしたユーザを分類した。

さらに、有権限者については、所属会社別に分類した。

上記分類に基づき、権限毎のアクセス状況を以下に示す。

表 63 アクセス状況（四国電力送配電）

分類 1	分類 2	ID 数	所属	所属別 ID 数	アクセス回数	アクセス回数/所属別 ID 数
権限のない者	—	XX	—	—	XX	X.XX
有権限者	個人別 ID	X,XXX	四国電力送配電	XXX	XX,XXX	XX.XX
			XXX	XXX	X,XXX	.XX
			外部委託先	XX	X,XXX	XX.XX
	共有 ID	X ※1	外部委託先	X	X	X

※1 共有 ID は XXID 存在するが、本分析の中で、アクセスは検出されなかったため、ID 数は X と記載している。

アクセスログの分析結果に基づき、操作ログ分析の対象となるか、以下の検討を実施した。

- 権限のない者によるアクセスの検討

  権限のない者によるアクセスが XXID 検出されている。託送お客さま管理システムは、権限がなくてもアプリ起動はできるため、起動時のアクセスログが記録される。XXID について、操作ログが残っていないかを確認することにした。

- 共有 ID の検討

  共有 ID を確認した結果、ID 数は XXID あった。当該 ID の利用用途は、災害時における XXX が利用するものとなっており、利用の都度貸出管理が行われている。

  対象の共有 ID（XXID）について、アクセスは検出されなかった。

- 有権限者によるアクセス日付の妥当性の確認(有効期間外のアクセス)

  ホワイトリストは権限情報が反映されたリストになっているため、ログ時点の所属が紐づけ可能となっている。分析対象期間において、新規登録・異動・退職の対象者は XXID 検出された。

登録・異動によるアクセスは、XID が検出された。XID は 7/1、1ID は 7/ 4 より業務開始となっていたが､業務開始日以降のアクセスとなっていることを確かめた。

退職によるアクセスは XID が検出されたが、7/31 退職であり、それ以降のアクセスは存在しないことを確かめた。

また、異動によるアクセスは XID が検出されたが、7/1 異動であり、それ以降のアクセスが存在しないことを確かめた。

- 有権限者アクセス権限の妥当性の確認

  権限は、XXX に設定されているため、許可された権限範囲以外のアクセスができない仕組みとなっている。また、人事情報の反映は、異動日から新所属情報に更新されタイムラグのない運用となっていることから､期間外に権限範囲外のアクセスが行われるリスクは低いと判断した。

- 権限のない者によるアクセスの理由確認

  アクセスエラーログ発生の背景について、四国電力送配電に質問し、権限付与されていない人物が、当該システムへアクセスしたことからログが発生しており、また、ログには残っているが、実際には権限のない者の画面は表示されずログインエラーとなる旨、回答を得た。したがって、操作ログ分析にて、権限のない者による操作がないことを確かめた。

- 非公開情報にかかる画面制御の検討

  XXX。託送お客さま管理システム権限の有無により制御を実施している。

2) 操作ログの分析結果の概要

アクセスログ分析の結果、以下の操作ログを分析した。

(1) 権限のない者によるアクセス

権限のない者によるアクセスはXXID を識別している｡XXID の操作ログを入手し、確認した結果、XID のユーザを特定し、XID はシステム処理で生成されるログであった。ログインエラー以外の操作ログは存在せず、不正なログではないと判断した。

以上のことからアクセスログで識別された XXID について、操作ログがないため権限者のない者によるアクセスはなかったと判断した。

1.8.3 結論

本調査の範囲において、非公開情報の管理の用に供するシステムである託送お客さま管理システムのログ分析の結果、非公開情報を入手可能な者によるアクセスのみが識別され、特定された者のみが当該情報を入手することができることになっていた。

1.8.4 検出事項

ログ分析の結果、非公開情報へ権限のない者によるアクセスは識別されず、検出事項はなかった。

1.9　九州電力送配電株式会社

1.9.1 対象システムの選定

1.9.1.1 対象システムの選定結果の概要

九州電力送配電株式会社（以下「九州電力送配電」という。）は、①再エネ受付管理システム、②設備台帳管理システム、③電力輸送部門 IT システム（TSMS）、④業務支援系システムを対象にシステム選定のためのリスク評価を実施した。

リスク評価の結果は以下のとおり。

表 64 リスク評価結果（九州電力送配電）

システム名	システム重要度スコア	リスクの発生可能性評価スコア	トータルスコア
再エネ受付管理システム	XX	XX	XX
設備台帳管理システム	XX	XX	XX
電力輸送部門 IT システム（TSMS）	XX	XX	XX
業務支援系システム	XX	XX	XX

九州電力送配電は「XXX」や「XXX」、「XXX」等の全社規程、グループ規程により、各システムは概ね同様に統制が整備されている状況であり、大規模障害の発生も確認されなかった。一方で、電力輸送部門 IT システム(TSMS)は、他システムと比較しユーザ数 X,XXX 名(うち社外ユーザ X,XXX 名)、アクセス数年間 X,XXX,XXX 件と最も多く、他システムとの連携が多数あり、複数のサブシステムから構成される大規模システムであること等から、ログ調査の対象システムに選定した。

1.9.2 システムログの分析

1.9.2.1 ログの分析

1）アクセスログ分析結果の概要

電力輸送部門 IT システム(TSMS)の 2024 年 7 月の端末操作ログを対象に、パイロットテスト及びアクセスログ分析を実施した。なお、電力輸送部門 IT システム(TSMS)はアクセスログと操作ログが個別にファイルに出力される仕様である。

表 65 ログ分析に利用したデータ一覧（九州電力送配電）

データ名	概要
アクセスログ	電力輸送部門 IT システム(TSMS)におけるアクセスログ情報
九電送配従業員名簿（提出版）【20240701 時点】、【20240801 時点】	ホワイトリスト：九州電力送配電（電力輸送部門 IT システム(TSMS)にアクセス可能なユーザ情報）
QHT 従業員派遣社員名簿（提出版）【20240701 時点】、【20240801 時点】	ホワイトリスト：九電ハイテック（電力輸送部門 IT システム(TSMS)にアクセス可能なユーザ情報）
組織設定ファイルの設定内容一覧	システムに付与した権限設定情報

(1) アクセスログ分析の対象ログ

電力輸送部門 IT システム(TSMS)は端末操作ログに記録されるアクセス履歴を分析に利用した。

(2) ホワイトリストの信頼性の確認

九州電力送配電は以下の情報をホワイトリストとして利用した。ホワイトリストを作成するために利用した情報、及び当法人にて分析対象月直前(20XX 年 XX 月度)の ID 棚卸結果とホワイトリストの差分を抽出し、改廃が発生しているユーザについて、人事情報を確かめ、データの信頼性は担保されていると判断した。

表 66 データの信頼性の確認結果（九州電力送配電）

利用情報	概要	データの信頼性の確認結果
九電送配従業員名簿（提出版）【20240701 時点】、【20240801 時点】	人事情報及び個別申請に基づく全社員の利用者情報である。利用者と所属情報を保持している。	人事情報から連携したデータをもとにしており、網羅性、正確性について十分な心証を得た。また、個別登録の情報について会社へ質問し、網羅性、正確性について十分な心証を得た。
QHT 従業員派遣社員名簿（提出版）【20240701 時点】、【20240801 時点】		
TSMS 利用者棚卸リスト	電力輸送部門 IT システム(TSMS)の 20XX 年 XX 月における ID 棚卸結果である。	九州電力送配電が実施した ID 棚卸結果をもとにしている。実施方法について質問し、網羅性、正確性について十分な心証を得た。
社員外従業員用パソコン・IC カード貸出申請書	ホワイトリストと ID 棚卸結果(20XX 年 XX 月度)の差分を抽出し対象者を選定、2023 年 11 月～8 月 1 日までの当該期間における人事連携対象外の個別登録における申請書である。	対象者について、九州電力送配電へ質問及び、申請書を閲覧し、網羅性、正確性について十分な心証を得た。

(3) ログデータの網羅性

ログ保管に関する資料及びログ取得手順の閲覧並びに九州電力送配電への質問により、アクセスログ及び操作ログの網羅性を確認した。

アクセスログ分析で利用したログ(アクセスログ、操作ログ)は、XXX へ記録され、サーバにて常時保管している。ログが記録、保管されているサーバのシステム利用者や第三者がアクセスできない場所に保管している。

ログ抽出時の取得作業画面を閲覧し、7 月分を漏れなく抽出していることを確かめ、網羅性についても十分であるとの心証を得た。

以上より、ログデータの網羅性について心証を得たため、データ分析に利用可能と判断した。

(4) システム上の権限設定状況の確認

九州電力送配電への質問及び設計書の閲覧により、非公開情報へアクセスできる権限設定について、九州電力送配電用 6 権限(送配電用、設備計画用、他部門（用地以外)、他部門（用地)、業務基盤、内燃力(XXX)、九電ハイテック用 1 権限があることを確かめた。非公開情報にアクセス不可の権限として、水力部門用 1 権限があるが、画面制御にて非公開情報を制限している。そのため、画面制御機能を確かめ、ログ分析の対象外とした。

表 67 権限設定の概要（九州電力送配電）

権限の種類	権限の内容
送配電用権限 (九州電力送配電)	・非公開情報にアクセス可能な権限
設備計画用権限 (九州電力送配電)	・非公開情報にアクセス可能な権限
他部門（用地以外）権限 (九州電力送配電)	・非公開情報にアクセス可能な権限
他部門（用地）権限 (九州電力送配電)	・非公開情報にアクセス可能な権限
業務基盤権限 (九州電力送配電)	・非公開情報にアクセス可能な権限
内燃力(XXX) 権限 (九州電力送配電)	・非公開情報にアクセス可能な権限
九電ハイテック用権限	・非公開情報にアクセス可能な権限 ・九電ハイテック用権限を設定
水力部門用権限 (九州電力)	・非公開情報にアクセス不可な権限 ・九州電力用権限を設定

(5) アクセスログの月次分析

1 か月分のアクセスログから電力輸送部門 IT システム(TSMS)のログインに係るログを抽出し、ホワイトリストと照合をした。ホワイトリストに記載されたユーザを有権限者、記載のないユーザを権限のない者と識別しアクセスしたユーザを分類した。

さらに、有権限者については、所属会社別に分類した。

上記分類に基づき、権限毎のアクセス状況を以下に示す。

表 68 アクセス状況（九州電力送配電）

分類 1	分類 2	ID 数	所属	所属別 ID 数	アクセス回数	アクセス回数/所属別 ID 数
権限のない者	—	—	—	—	—	—
有権限者	個人別 ID	X,XXX	九州電力送配電	X,XXX	XXX,XXX	XX.XX
			九電ハイテック	X,XXX	XXX,XXX	XXX.XX
	共有 ID	XX	九州電力送配電	XX	XXX	XX.XX
			九電ハイテック	X	XXX	XX.XX

アクセスログの分析結果に基づき、操作ログ分析の対象となるか、以下の検討を実施した。

- 権限のない者によるアクセスの検討

  権限のない者によるアクセスは検出されなかった。

- 共有 ID の検討

  共有 ID の利用用途を確認した結果、各ベンダー作業員の確認試験用ユーザ ID が XX 件あった。当該 ID は、利用に際し、XXX がないとアクセスできない仕組みになっている。

  また、各ベンダー管理責任者が、カード利用者に責任をもってカードの配布、返却等を管理しており、TSMS 担当外となった担当者にはカード配布を停止する。

  九州電力送配電への質問により、XXID に関する利用ベンダー及び利用人数を確かめた。

- 有権限者によるアクセス日付の妥当性の確認(有効期間外のアクセス)

  ホワイトリストは権限情報が反映されたリストになっているため、ログ時点の所属が紐づけ可能となっている。分析対象期間において、追加になったユーザが XID 検出された。XID は 7/10、XID は 7/16、XID は 7/29 より業務開始となっていたが、いずれも業務開始日以降のアクセスとなっていることを確かめた。

  退職者によるアクセスは検出されなかった。

- 有権限者アクセス権限の妥当性の確認

  権限は、XXX に設定されているため、許可された権限範囲以外のアクセスができない仕組みとなっている。また、人事情報の反映は、異動日から新所属情報に更新されタイムラグのない運用となっていることから、期間外に権限範囲外のアクセスが行われるリスクは低いと判断した。

また、派遣社員等の申請によるユーザについては、登録、変更、削除等の申請承認が行われ、派遣先組織ごとの権限設定になっている。変更、削除（契約解除）の場合は、XXX ができず、端末が利用できない仕組みとなっている。そのため、システムへのアクセス自体が不可能となることから、期間外に権限範囲外のアクセスが行われるリスクは低いと判断した。

- 非公開情報にかかる画面制御の検討

  XXX ごとに画面制御を設定している。XXX の実機画面を閲覧し、電力輸送部門 IT システム(TSMS)において、XXX の設定内容一覧の通り、画面制御されていることを確かめた。

  以上より、非公開情報にアクセス可能な画面制御が実装されている心証を得た。

2）操作ログの分析結果の概要

アクセスログ分析の結果、権限のない者によるアクセスは行われていないことが確かめられたため、操作ログの分析は不要であると判断した。

1.9.3 結論

本調査の範囲において、非公開情報の管理の用に供するシステムである電力輸送部門 IT システム(TSMS)のログ分析の結果、非公開情報を入手可能な者によるアクセスのみが識別され、特定された者のみが当該情報を入手することができることになっていた。

1.9.4 検出事項

ログ分析の結果、非公開情報へ権限のない者によるアクセスは識別されなかったが、ログ分析の過程で以下の気づき事項を検出した。

1.9.4.1 検出事項 No.1

検出事項の分類	気づき事項
概要	電力輸送部門 IT システム（TSMS）の ID を管理している全社 ID 管理システム（以下 IDM という）において、XXX ユーザが登録されている。 規程には定期的な ID 棚卸を行うことが定められているものの、XXX を対象とした ID 棚卸は、前回実施(20XX 年 XX 月)から XXX 以上経過していた。
詳細	「XXX」において、以下記載のとおり定められている。しかしながら、九州電力送配電への質問及び 20XX 年 XX 月 XX 日時点の ID 棚卸結果を閲覧したところ、ID 棚卸が XXX 以上未実施となっていた。

	【XXX】 3.3.XXX 5　ＩＤは、業務担当者の変更時など定期的に棚卸を実施し、不要なＩＤがないかを確認しなければならない。 また、九州電力送配電への質問により、以下の統制を実施していることから、リスクが低減されているため、定期的な棚卸は実施していないことを確認した。 ・XXX を実施している。 ・申請ユーザがシステムを利用する端末を使用するには XXX が必要 ・XXX の場合は、XXX が利用できないことから、システムへのアクセス自体が不可能 ・XXX を利用することはできない仕組み
リスク	退職や異動により不要になったアカウントや権限が長期間残存することで、アカウントの乗っ取りや不正利用のリスクが高まる。
原因	ID 棚卸の実施に関し、定期的に棚卸を行うことは定められているものの、明確な実施時期、実施頻度は定められていない。
改善の方向性	IDM に登録された XXXID 棚卸に関し、実施時期、頻度等のルールを整備したうえで、定期的に実施することが望ましい。 なお、XXXID 棚卸を年 1 回実施する方向で運用の見直しを協議中である。

1.10　沖縄電力株式会社

1.10.1　　対象システムの選定

1.10.1.1　対象システムの選定結果の概要

沖縄電力株式会社（以下「沖縄電力」という。）は、①託送システム、②インターネット新増設申込システム、③営業システム、④電力購入管理システムを対象にシステム選定のためのリスク評価を実施した。

リスク評価の結果は以下のとおり。

表 69 リスク評価結果（沖縄電力）

システム名	システム重要度スコア	リスクの発生可能性評価スコア	トータルスコア
託送システム	XX	XX	XX
インターネット新増設申込システム	XX	XX	XX
営業システム	XX	XX	XX
電力購入管理システム	XX	XX	XX

沖縄電力は各種セキュリティ要領や「XXX」、「XXX」等の規程により、各システムは概ね同様に統制が整備されている状況であり、大規模障害の発生も確認されなかった。一方で、営業システムは、託送事業者・需要者に係る契約者情報・契約情報を保有していること、他システムと比較し、アクセス数が年間 XXX,XXX 件と最も多く、顧客や金融機関、外部委託先等の接続経路があることから、ログ調査の対象システムに選定した。

1.10.2 システムログの分析

1.10.2.1 ログの分析

1）アクセスログ分析結果の概要

営業システムの 2024 年 7 月の端末操作ログを対象に、パイロットテスト及びアクセスログ分析を実施した。なお、営業システムはアクセスログと操作ログが同一ファイルで出力される。

表 70 ログ分析に利用したデータ一覧

データ名	概要
操作ログ(アクセスログ含む)	営業システムにおけるアクセス及び操作ログ情報
【非公開情報を入手可能な者の名簿】営業システム_01_利用者マスタリスト(7 月 26 日, 7 月 31 日)	ホワイトリスト（営業システムにアクセス可能なユーザ情報）
【2024 年_台風 3 号】用地・離島発電部対応者 ID 管理表	共有 ID 利用時(台風応援ユーザ)の管理簿

(1) アクセスログ分析の対象ログ

営業システムはシステムの操作ログよりログインを行った記録を抽出し、アクセスログとして分析に利用した。

(2) ホワイトリストの信頼性の確認

沖縄電力は以下の情報をもとに作成した、ホワイトリストを利用した。ホワイトリストを作成するために利用した情報、及び当法人にて分析対象月直前(20XX 年 X 月度)の ID 棚卸の結果とホワイトリストの差分を抽出し、改廃が発生しているユーザについて、申請書を確かめ、データの信頼性は担保されていると判断した。

表 71 データの信頼性の確認結果（沖縄電力）

利用情報	概要	データの信頼性の確認結果
【非公開情報を入手可能な者の名簿】営業システム_01_利用者マスタリスト	営業システムの実機から出力した、ユーザ情報、権限情報一覧である。	実機情報から直接取得したデータをもとにしており、抽出時のクエリを確かめ、網羅性、正確性について十分な心証を得た。
営配総合情報システム利用者情報一覧（6 月分）	営業システムの実機から出力した、ユーザ情報、権限情報一覧である。	沖縄電力が実施した ID 棚卸時の情報をもとにしており、実施方法について、質問し、網羅性、正確性について十分な心証を得た。
営業システム利用者 ID 申請・管理チェックシート（6 月分）	営業システムの 20XX 年 X 月度における ID 棚卸結果である。	沖縄電力が実施した ID 棚卸結果をもとにしており、実施方法について、質問し、網羅性、正確性について十分な心証を得た。
営配システム利用者マスタメンテナンス票営業用	ホワイトリストと ID 棚卸結果(20XX 年 X 月度)の差分を抽出し、20XX 年 X 月～X 月 XX 日までの当該期間における登録変更削除における申請書である。	対象者について、沖縄電力へ質問及び、申請書を閲覧し、網羅性、正確性について十分な心証を得た。

(3) ログデータの網羅性

ログ保管に関する資料及びログ取得手順の閲覧並びに沖縄電力への質問により、アクセス及び操作ログの網羅性を確認した。

アクセスログ分析で利用したログは、XXX バックアップ保管している。ログが記録、保管されているサーバのシステム利用者や第三者がアクセスできない場所に保管している。

ログ抽出時の取得作業画面を閲覧し、7 月分のファイルを漏れなく取得していることを確かめ、網羅性についても十分であるとの心証を得た。

以上より、ログデータの網羅性について心証を得たため、データ分析に利用可能と判断した。

(4) システム上の権限設定状況の確認

沖縄電力への質問及び設計書の閲覧により、非公開情報へアクセス可能な権限設定について、送配電事業部(ネットワーク統括グループ、ネットワークサービスセンター、ネットワーク受付センター)の権限があることを確かめた。

表 72 権限設定の概要（沖縄電力）

権限の種類	権限の内容
送配電事業部 (XXX)	・非公開情報にアクセス可能な権限 ・送配電事業部が利用
その他部署	・非公開情報にアクセス不可能な権限 ・画面遷移ができず、エラー表示となる

(5) アクセスログの月次分析

1か月分の操作ログから営業システムのログインに係るログを抽出し、ホワイトリストと照合した。ホワイトリストに記載されたユーザを有権限者、記載のないユーザを権限のない者と識別しアクセスしたユーザを分類した。

さらに、有権限者については、所属組織別と外部委託先に分類した。

上記分類に基づき、権限毎のアクセス状況を以下に示す。

表 73 アクセス状況（沖縄電力）

分類1	分類2	ID数	所属	所属別ID数	アクセス回数	アクセス回数/所属別ID数
権限のない者	—	—	—	—	—	—
有権限者	個人別ID	XXX	送配電事業部	XX	XXX,XXX	X,XXX.XX
			外部委託先(グループ会社)	X	XXX,XXX	XX,XXX.XX
			上記部門以外	XXX	X,XXX,XXX	XX,XXX.XX
	共有ID	X ※1	外部委託先	X	X	X

※1 共有IDはXXID存在するが、本分析の中で、アクセスは検出されなかったため、ID数はXと記載している。

アクセスログの分析結果に基づき、操作ログ分析の対象となるか、以下の検討を実施した。

- 権限のない者によるアクセスの検討

  権限のない者によるアクセスは検出されなかった。

- 共有 ID の検討

  共有 ID の利用用途を確認した結果、災害時利用の ID が XX 件であった。当該 ID は、台風等災害時用になっており、利用の都度貸出管理が行われている。

  対象の共有 ID（XXID）について、アクセスは検出されなかった。

- 有権限者によるアクセス日付の妥当性の確認(有効期間外のアクセス)

  ホワイトリストは権限情報が反映されたリストになっているため、ログ時点の所属が紐づけ可能となっている。分析対象期間において、新規登録・異動・退職の対象者は XXID 検出された。

  登録・異動によるアクセスは、XXID が検出された。XXID は 7/1 より、XID は 7/2 より、XID は 7/5 よりアクセス有効となっており、業務開始日以降のアクセスとなっていることを確かめた。

  退職者によるアクセスは検出されなかった。

- 有権限者アクセス権限の妥当性の確認

  権限は、XXX されることから、許可された権限範囲以外のアクセスができない仕組みとなっている。また、異動、退職に関しても、XXX が行われること、また ID 棚卸を月次の頻度にて実施することにより、期間外に権限範囲外のアクセスが行われるリスクは低いと判断した。

- 非公開情報にかかる画面制御の検討

  XXX を実施している。沖縄電力への質問及び実機画面の閲覧より、権限のない者が非公開情報へアクセスした場合、XXX ができず、エラーとなることを確かめた。

  以上より、非公開情報にかかる画面制御が実装されている心証を得た。

2）操作ログの分析結果の概要

アクセスログ分析の結果、権限のない者によるアクセスは行われていないことが確かめられたため、操作ログの分析は不要であると判断した。

1.10.3　結論

本調査の範囲において、非公開情報の管理の用に供するシステムである営業システム

のログ分析の結果、非公開情報のアクセスは入手可能な者によるアクセスのみが識別され、特定された者のみが当該情報を入手することができることになっていた。

1.10.4　検出事項

ログ分析の結果、非公開情報へ権限のない者によるアクセスは識別されず、検出事項はなかった。

以上