過去発生したセキュリティインシデントでの対策が近年の事件で有効だったかの調査

選定基準： 20万件以上の情報漏洩、またはランサムウェアによる被害が大きく報道された事実

No.	発生年	企業名	概要	漏洩人数	原因	分類	対策　DB内部不正対策ガイドライン 第1.1.1版　https://www.jnsa.org/result/dbs/data/2016-01.pdf									JPCERT ランサムウエア対策特設サイト - 3.ランサムウエアの対策　h	
							ポリシーの策定 (基準の策定と、定期的なチェックと強制)	アクセス制御	認証方式	管理者の分掌	データ暗号化・鍵管理	DB周辺機器の管理 (周辺に格納されたデータの扱いや持ち込みデバイス制限)	定期監査の実施	不正な通信のリアルタイム監視・通知	監査ログの保全	ソフトウェアを最新化	定期的なバックアップ実施
	2014年	株式会社ベネッセコーポレーション	顧客DBの保守管理を担当していた再委託先の技術者が、·通常業務を装ってDBにアクセスし、大量の顧客情報を·窃取し、売却。約3504万件の情報が漏洩した。	3504万人	・運用保守担当者がシステム管理者アカウントを常用 ・DB内で個人情報が区分けされておらず、必要な権限が分離されていなかった。 ・外部媒体の利用がブロックしきれていなかった。 ・開発業務に暗号化せず本番データを利用していた。	内部犯	・定期的に見直し不要な権限を剥奪する（または強制するツールの導入） ・DBサーバ接続NWへの持ち込みデバイスなどの接続を検疫NWなどで制限 ・個人情報格納ファイルについて、パスワード設定や権限設定をツールで機械的にチェックして強制する	・個人情報などの重要情報については、情報レベルに応じた分類を行い、スキーマ、テーブル、行/列ごとにアクセス権限を行う ・管理者権限等の高権限をむやみに付与せず、必要最小限のデータアクセス権限のみ付与する	・アカウント、およびパスワードは使いまわさない ・デフォルトの管理者アカウントは無効化する ・個人ユーザを作成し、多要素認証を用いる	・管理操作をおこなうためには2人以上の管理者の作業が必要となるように運用的もしくは技術的な対策をおこなう	・開発で本番データを利用する際は、マスキング等の対策を行う ・個人情報等の重要情報は、可能な限り暗号化して保管する	・DBサーバアクセス端末ローカルへのデータ転送をブロック ・DBサーバアクセス端末の媒体接続制御 ・DB以外の周辺デバイスに保存されたファイルも、アクセス権・パスワードを適切に設定する	監査ログの取得・定期チェック・アラート 例： ・長時間ログイン ・時間外アクセス ・作業申請通りのアクセスであること ・管理者アカウントの操作	・ポリシー違反(大量データ送信、不正宛先等)のリアルタイム検知・通知 ・FWやNW監視装置を導入し不要な通信を監視・遮断	イベントログ等必要なログを随時収集し、ログ保管しておくことでログの消失や改ざんを防ぐ	重大な脆弱性に対するセキュリティパッチを速やかに適用する	・定期的なバックアップ実施 ・バックアップが正常に取得されていることを、定期的にリストアを行い確認する
01	2022年	尼崎市	再委託先従業員がデータ移行作業のためにUSBメモリを不正持ち出し、一時紛失	※漏洩は無し	内部不正	内部犯	評価不可	効果あり 再委託先従業員へのアクセス権限付与の適正化	評価不可	効果あり 管理操作時は2人以上で作業しオペミスや不正操作を抑止	効果あり 本番データを利用する際はマスキング・暗号化を行う	効果あり USBに書きだされたファイルのパスワード設定	効果あり 能動的な監査による不正の抑止効果や、作業実体の把握	評価不可	評価不可	評価不可	評価不可
02	2023年	株式会社NTTドコモ	業務委託先から利用者の情報が外部に流出した可能性	529万件	内部不正	内部犯	効果あり 個人情報格納ファイルに関するパスワード設定や権限設定を、システム的にチェックし強制する	効果あり 再委託先従業員へのアクセス権限付与の適正化	評価不可	評価不可	効果あり 本番データを利用する際はマスキング・暗号化を行う	効果あり インターネット接続可能な端末へ個人情報をダウンロードさせない	効果あり 外部通信先に不正なサイトが無いか定期チェック	効果あり クラウドストレージへのアップロードを監視・検知	評価不可	評価不可	評価不可
03	2023年	株式会社ＮＴＴマーケティングアクトＰｒｏＣＸ	元派遣社員が約10年にわたり顧客情報を管理者権限を使い不正に持ち出し	928万人	内部不正	内部犯	効果あり 定期的に見直し不要な権限を剥奪する（または強制するツールの導入）	効果あり 一般ユーザに管理者権限を付与しない	評価不可	効果あり 管理操作時は2人以上で作業しオペミスや不正操作を抑止	効果あり 個人情報をダウンロードさせる機能を実装する場合、暗号化やマスキングを可能な限り行う	効果あり 個人情報ダウンロード可能な範囲を、インターネット接続不可、USBメモリ接続不可、私用PCの接続不可等の環境に限定する	効果あり 不要な大量データの持ち出し・ダウンロードを定期監査	効果あり 媒体接続や私用PCの接続ログのリアルタイム監視・検知	評価不可	評価不可	評価不可
04	2023年	株式会社ジェイ・エス・ビー	顧客の氏名や年収などの個人情報を入手し、社外関係者に漏らした	約27万件	内部不正	内部犯	評価不可	評価不可	効果あり 多要素認証を用いて本人確認	評価不可	評価不可	評価不可	評価不可	評価不可	評価不可	評価不可	評価不可
05	2022年	トヨタコネクティッド株式会社	Github上にDBアクセス情報が公開、DB上の顧客情報が漏えいした可能性	29万人 ※漏洩はなし。閲覧された可能性のある件数	設定ミス	内部犯	効果あり アクセス権限の定期見直し/不要な権限の強制停止	効果あり アクセス権限の適切な設定	評価不可	評価不可	評価不可	評価不可	評価不可	評価不可	評価不可	評価不可	評価不可
06	2022年	リスクモンスター株式会社	クラウド移行時の設定ミスで個人情報が検索エンジンに表示される状態に	25万人	設定ミス	内部犯	効果あり アクセス権限の定期見直し/不要な権限の強制停止	効果あり アクセス権限の適切な設定	評価不可	効果あり 管理操作時は2人以上で作業しオペミスや不正操作を抑止	評価不可	評価不可	評価不可	評価不可	評価不可	評価不可	評価不可
07	2023年	トヨタコネクティッド株式会社	クラウド環境のご設定により顧客情報が約10年間閲覧可能な状態に	215万件 ※漏洩はなし。閲覧された可能性のある件数	設定ミス	内部犯	効果あり アクセス権限の定期見直し/不要な権限の強制停止	効果あり アクセス権限の適切な設定	評価不可	評価不可	評価不可	評価不可	評価不可	評価不可	評価不可	評価不可	評価不可
08	2023年	株式会社エイチーム	クラウド上で個人情報含むファイルが公開状態、流出の恐れ	約96万件	設定ミス	内部犯	効果あり アクセス権限の定期見直し/不要な権限の強制停止	効果あり アクセス権限の適切な設定	評価不可	評価不可	効果あり 個人情報を含んだファイルの暗号化	効果あり 配置ファイルにおける適切なアクセス権・パスワード設定	評価不可	評価不可	評価不可	評価不可	評価不可
09	2024年	ウォンテッドリー株式会社	不具合で個人情報が権限外の第三者に閲覧された可能性	20万578件	設定ミス	内部犯	効果あり アクセス権限の定期見直し/不要な権限の強制停止	効果あり アクセス権限の適切な設定	評価不可	評価不可	評価不可	評価不可	評価不可	評価不可	評価不可	評価不可	評価不可
10	2022年	大阪急性期・総合医療センター	サプライチェーンのVPNからランサムウェア感染、緊急以外の手術や外来診察を停止	システム破壊	ランサムウェア	外部犯	評価不可	効果あり 一般ユーザに管理者権限を付与しない	効果あり パスワードを使いまわさない	評価不可	評価不可	効果あり バックアップへの適切なアクセス権・パスワード設定	評価不可	効果あり 不正な通信の監視・通知	評価不可	効果あり VPN機器のパッチ適用	効果あり バックアップによる復旧
11	2023年	名古屋港運協会	システムのデータが暗号化されコンテナ搬出入が行えず物流に影響	※漏洩は無し	ランサムウェア	外部犯	評価不可	評価不可	評価不可	評価不可	評価不可	効果あり バックアップ適切なアクセス権・パスワード設定	評価不可	効果あり 不正な通信の監視・通知	効果あり 原因分析のためにシステムログを保存しておく	効果あり VPN機器のパッチ適用	効果あり バックアップによる復旧
12	2024年	株式会社KADOKAWA	プライベートクラウドやクラウド上のシステムが二重脅迫で業務に影響	25万件	ランサムウェア	外部犯	評価不可	評価不可	効果あり 多要素認証を用いて本人確認	評価不可	効果あり 個人情報を含んだファイルの暗号化	評価不可	評価不可	効果あり 不正な通信の監視・通知	評価不可	評価不可	効果あり バックアップによる復旧
13	2024年	ニデックインスツルメンツ株式会社	管理者アカウントが不正取得され、社内のデータが暗号化、攻撃者サイトに公開	40万2,530件	ランサムウェア	外部犯	評価不可	評価不可	効果あり 多要素認証を用いて本人確認	評価不可	効果あり 個人情報を含んだファイルの暗号化	評価不可	評価不可	評価不可	評価不可	効果あり VPN機器のパッチ適用	効果あり バックアップによる復旧
14	2024年	株式会社イセトー	VPN経由の不正アクセスで受託業務データが漏えい、一部顧客情報が公開	149万件以上	ランサムウェア	外部犯	効果あり 個人情報格納ファイルについて、パスワード設定や権限設定をツールで機械的にチェックして強制する	評価不可	評価不可	評価不可	効果あり 個人情報を含んだファイルの暗号化	効果あり 持ち出したファイルのアクセス制限	効果あり データ持ち出しの定期監査	効果あり 制限区域外へのデータ送信を監視	評価不可	効果あり VPN機器のパッチ適用	評価不可
15	2024年	カシオ計算機株式会社	ランサムウェア攻撃により個人情報など機密情報の一部が漏洩。決算発表延期	不明	ランサムウェア	外部犯	評価不可	評価不可	評価不可	評価不可	評価不可	評価不可	評価不可	効果あり 不正な通信の監視・通知	評価不可	評価不可	効果あり バックアップによる復旧
16	2024年	LINEヤフー株式会社	韓国の委託先企業がマルウェアに感染。共通認証基盤環境を経由し不正アクセス	58万人	不正アクセス	外部犯	評価不可	評価不可	効果あり 多要素認証を用いて本人確認	評価不可	評価不可	評価不可	評価不可	効果あり 不正な通信の監視・通知	評価不可	評価不可	評価不可
17	2024年	株式会社ネクストレベル	不正アクセスにより利用者の個人情報が外部に漏えい	49万6,119件	不正アクセス	外部犯	評価不可	評価不可	評価不可	評価不可	評価不可	評価不可	効果あり 大量の個人情報参照を定期チェック	効果あり 大量のデータ参照通信を監視	評価不可	評価不可	評価不可
18	2024年	サノフィ株式会社	DBへの不正アクセスにより国内の医療従事者、従業員の情報が漏えい	73万3,820件	不正アクセス	外部犯	評価不可	評価不可	効果あり 多要素認証を用いて本人確認	評価不可	評価不可	評価不可	効果あり アクセス元IPに不正なIPが無いか定期チェック	効果あり 想定外のIPからの接続を監視	評価不可	評価不可	評価不可
19	2024年	株式会社LIFULL	不正アクセスにより、DBバックアップから不動産登録者の情報漏えい懸念	21万7953件	不正アクセス	外部犯	効果あり アクセス権限の定期見直し/不要な権限の強制停止	効果あり アクセス権限の適切な設定	評価不可	評価不可	効果あり 個人情報を含んだバックアップの暗号化	効果あり バックアップデータのアクセス権限設定	評価不可	評価不可	評価不可	評価不可	評価不可