WARNING

不正アクセスによる個人データ漏えい防止のための注意喚起

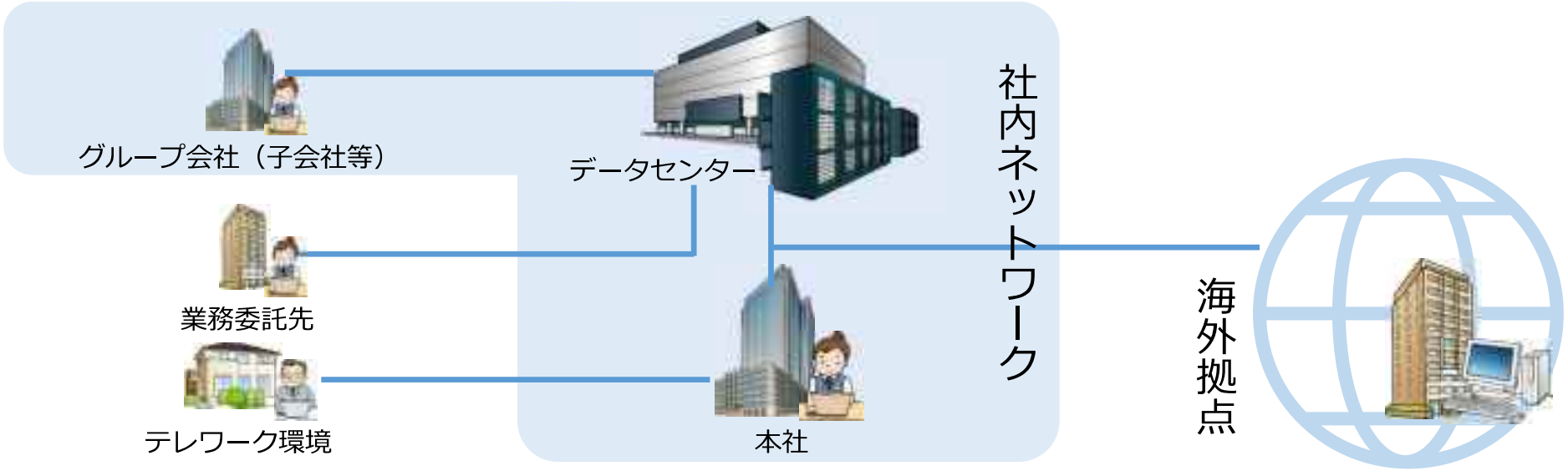
（令和６年12月11日、令和８年10月７日改訂）

PPC 個人情報保護委員会
Personal Information Protection Commission

はじめに

個人情報の取扱いを巡る環境は、デジタル技術の急速な発展、ビジネスのグローバル化、サプライチェーン等の業務委託関係の多様化等により、日々変化しており、個人情報取扱事業者(※１)は、変化する環境に応じた個人情報の適正な取扱いを図ることが求められています。

また、今般、ランサムウェアを含むサイバー攻撃の高度化・巧妙化が進み、従前見られていた情報システムの脆弱性を狙った不正アクセスに加え、グループ会社又は海外拠点における弱点となり得る関係性に起因するシステム侵入、機密情報が保存される領域への高度な水平移動等の手口による個人データの漏えいが見られます(※２)。



※１　個人情報の保護に関する法律（平成15年法律第57号。以下「法」という。）第16条第２項。

※２　個人情報保護委員会は、令和６年度第1四半期から、「監視・監督権限の行使状況の概要」と「漏えい等報告の処理状況」を公表している。
（https://www.ppc.go.jp/personalinfo/activity/?ref=gnavi）

発生事例から学ぶセキュリティ対策

個人情報保護委員会には、これらの手口によって発生した個人データの漏えい等事案が複数報告されている状況です。

報告された事案を分析したところ、以下九つの事例に類型化できる問題点が挙げられ、これら問題への措置が十分でない場合、安全管理措置（法第23条）、従業者の監督（法第24条）及び委託先の監督（法第25条）の違反と判断される可能性があります。

脆弱性への対応や強固な認証方式の採用等のセキュリティ対策は、どれか一つを講じればよいということではなく、多層的に講ずる必要があります。また、これらの事例の多くは、委託先等を含め、個人情報取扱事業者内外における複数の組織・部署が関係することから、その問題点を克服するためには、単純な技術的問題への対応にとどまらず、経営層を交えて現状の組織体制の抱える問題点や漏えい等が発生した場合に生じ得る損害等を評価し、組織的に対応することが必要となります。

個人情報取扱事業者におかれては、今回紹介する事例の原因及び対策を参考にし、必要なセキュリティ対策を行っていただくよう、お願いします。

＜事例＞

- 事例１　脆弱性が放置された事例
- 事例２　脆弱性への対応が遅れた事例
- 事例３　不正ログインの事例
- 事例４　グループ会社や海外拠点が狙われた事例
- 事例５　グループ会社間のアクセス制御不備があった事例
- 事例６　個人領域に保存したデータの漏えい事例
- 事例７　グループ会社への監督が不十分な事例
- 事例８　利用するクラウドサービスからの漏えい事例
- 事例９　APIが悪用される事例

事例１　脆弱性が放置された事例

個人情報取扱事業者が個人データを取り扱うために導入した情報システムについて、ソフトウェア等を最新状態に保つための措置を適切に行わず、また、脆弱性が公開され対処方法がリリースされていたにもかかわらず、対策を放置していたため、不正アクセスによる個人データの漏えい等を防ぐことができなかった。



原因

- ✓ システム業者との間で、情報システム導入の業務委託契約しか締結しておらず、セキュリティ対策に関するシステム保守の業務委託契約を締結していなかった。
- ✓ システム業者との間で、システム保守の業務委託契約は締結していたが、委託業務の内容に脆弱性対応が含まれていなかった。
- ✓ 脆弱性情報の収集は行っていたが、収集した脆弱性情報に基づき対策を講ずる際の役割分担が決められていなかった。
- ✓ グループ会社の間で脆弱性対策を行う役割分担が明確化されておらず、結果的に放置してしまった。
- ✓ 特に、VPN 装置等、インターネットとの接続を制御する装置の脆弱性は、攻撃に悪用されることが多い。

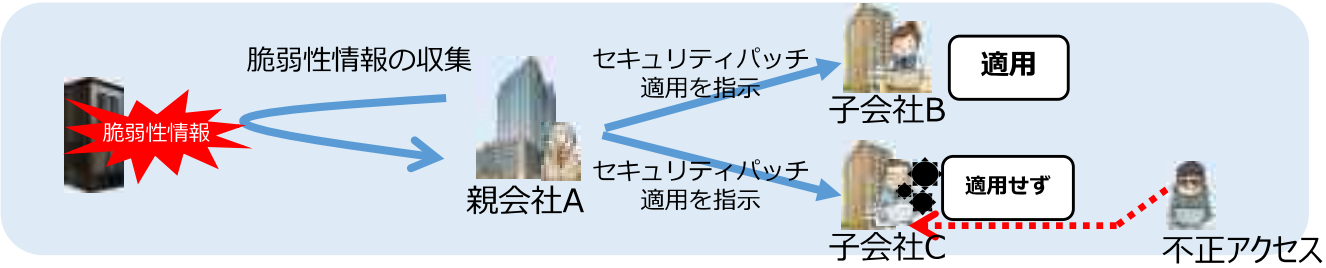
対策例

- ✓ 適切なシステム業者を選定し、情報システムの脆弱性対策等のセキュリティ対策も含めたシステム保守の業務委託契約を締結する。
- ✓ ⑴管理対象となるIT資産（外部の事業者から貸与されている物を含む。）の洗い出し、⑵脆弱性情報の収集・分析、⑶脆弱性への速やかな対処といった脆弱性対策プロセスを確実に行う。
- ✓ VPN 装置は、それ自体が意識的に利用・管理されるサーバ等と異なり、ネットワークサービスの一部として提供されるケースもあり、運用体制や脆弱性対応の責任が不明瞭なケースも多く、グループ会社内及び外部委託先との役割分担を明確化する。

※３　仮想プライベートネットワーク（Virtual Private Network）の略称であり、離れた拠点間を仮想的な専用線でネットワークでつないで通信できるようにするための仕組み。

事例２　脆弱性への対応が遅れた事例

グループ会社全体の情報システムを管理する親会社が、グループの複数会社が使用する情報システムに脆弱性が公開された際、グループ会社にセキュリティパッチを適用するよう指示したが、一部の子会社が適時に対応できなかったため、脆弱性を悪用された不正アクセスを受けた。



原因

- ✓ 一部の子会社にはシステム対応を行うための要員が十分におらず、リソースの問題から、すぐにセキュリティパッチ適用のための作業を行うことができなかった。
- ✓ 親会社において資産管理が適切に行われておらず、脆弱性情報が公開されていることに気づくのが遅く、対応が遅れてしまった。
- ✓ 社内ネットワーク内での利用にとどまるのであればリスクが小さいと考え、サポート期限が切れた機器の利用を継続した。

対策例

- ✓ グループ全体のセキュリティガバナンス向上のため、脆弱性情報収集・分析の一元管理のみならず、セキュリティパッチ適用等の対策状況を含めて一元管理する。
- ✓ ⑴管理対象となるIT資産の洗い出し、⑵脆弱性情報の収集・分析、⑶脆弱性への速やかな対処といった脆弱性対策プロセスの役割分担を関係者で認識合わせし、明確化する。
- ✓ 外部から侵入されることを想定し、社内ネットワーク上の機器についても脆弱性対策プロセスの実施を徹底する。

事例３　不正ログインの事例

個人データを取り扱う情報システムにログインするための本人認証について、利用者が正当なアクセス権を有する者であることを、識別した結果に基づき認証しなければならないところ、不十分な識別・認証による不正ログインを許し、個人データの漏えい等が発生した。



原因

- ✓ 推測されやすいID・パスワードを使用していた。
- ✓ 複数回以上のID・パスワードの入力ミス時はアカウントを一定時間ロックするなど、ブルートフォース攻撃(※４)への対策を行えていなかった。
- ✓ 脆弱性に対するセキュリティパッチは適用していたものの、過去の脆弱性によりID・パスワードが漏えいしていたにもかかわらず、ID・パスワードの初期化等の措置を行えていなかった。
- ✓ ログの保存・監視についてのルールがなかったため、不正アクセスの検知が遅れた。

対策例

- ✓ 推測されにくい複雑なパスワードを利用するよう従業者を教育する。
- ✓ 取り扱う個人データの性質及び量に応じて、多要素認証等の高い強度の認証方式を採用する。
- ✓ アカウントロック等の適切な不正ログイン対策の措置を行う。
- ✓ 脆弱性等によりID・パスワードが漏えいした可能性がある場合は、 ID・パスワードを初期化する又は利用者へ変更を案内する。
- ✓ ログの保存期間を定め、定期的に分析する。

※４　総当たり攻撃。ランダムなID・パスワードを総当たりでログイン試行する手法。

事例４　グループ会社や海外拠点が狙われた事例

国内外のグループ会社が共同で利用する情報システムに対し、海外拠点にある子会社を足がかりにした不正アクセスがなされ、攻撃者による侵入及び侵害の横展開が行われ、親会社が管理するデータセンターに保存されていた個人データがランサムウェアにより暗号化された結果、グループ全体にて個人データの漏えい等の被害が発生した。



原因

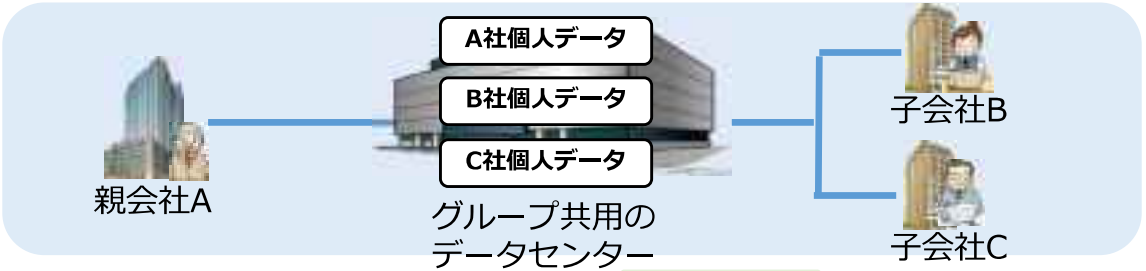
- ✓ 海外拠点は国内にある親会社のセキュリティガバナンスが行き届きにくく、情報システムの脆弱性対策が十分でなかった。
- ✓ 海外拠点に設置されていた貸与品のVPN装置が台帳にリストアップされておらず、VPN装置の存在が把握できなくなっていた。
- ✓ 子会社の情報システムと親会社のデータセンターとの間のアクセス制御が適切ではなかった。

対策例

- ✓ 国内だけの対策で完結せず、海外拠点も含めてIT資産（外部の事業者から貸与されている物を含む。）の洗い出し、脆弱性情報の収集・分析、脆弱性への対処を適切に行う。
- ✓ 子会社と親会社の間の通信は業務上必要な範囲のみ許容するなど、拠点間ネットワークのアクセス制御を強化する。

事例５　グループ会社間のアクセス制御不備があった事例

親会社がグループ会社全体の情報システムを一括管理するデータセンターを保守・管理しており、 同データセンター内のアクセス制御が不十分であったところ、グループネットワークへの不正アクセスがなされ、グループ会社全体の情報システムにおいて個人データの漏えい等が発生した。



原因

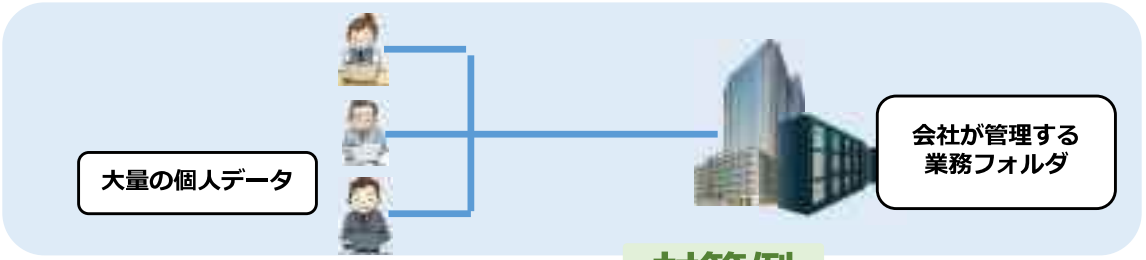
- ✓ グループ会社の個人データを管理するデータセンターにおいて、業務上の利便性等の観点から、グループ会社間で相互にアクセス可能としていた。
- ✓ 親会社が管理するグループネットワークの管理者パスワードの強度が十分ではなかった。

対策例

- ✓ グループ会社間であっても業務上の必要最小限の範囲でアクセス制御を行う。
- ✓ 同一のデータセンターで一元管理していても各会社の業務システムを極力分離独立し管理・運営する。
- ✓ 推測されにくい複雑なパスワードを利用し、管理者権限等の不正利用された際の被害が大きいアカウントには、多要素認証等の高い強度の認証方式を採用する。

事例６　個人領域に保存したデータの漏えい事例

個人情報取扱事業者の従業者が、業務で使用する電子ファイル等（個人データを含む。）を個人が管理する領域に保存しており、個人情報取扱事業者の情報システムが不正アクセスを受けた際、個人が管理する領域に保存されていた個人データについても漏えいが生じた。



原因

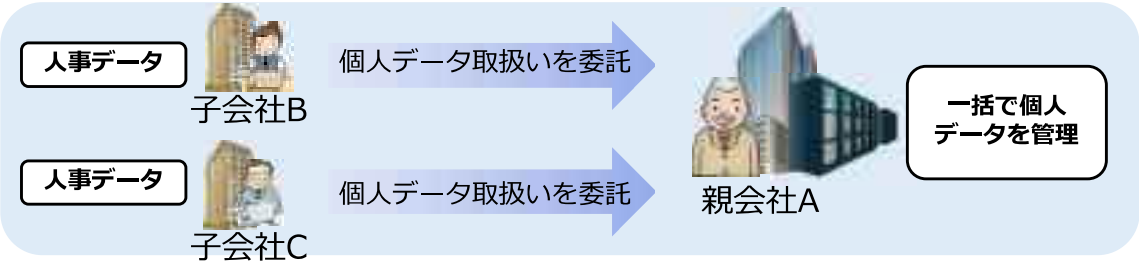
- ✓ 従業者が業務で使用する電子ファイルについて、組織として管理されておらず、従業者各自のデスクトップ端末等で加工・保存される業務運用が慣例化してしまっており、また、このような管理状況について、定期的な監査等の網にもかからなかった。
- ✓ 組織として管理されていない個人データの中には、本来は消去すべき古いデータ等が含まれているケースがあり、漏えい被害の範囲が大きくなってしまった。

対策例

- ✓ 個人情報取扱事業者における個人データの取扱いは、あらかじめ整備された個人データの取扱いに係る規律・ルールに従う。
- ✓ 個人情報管理台帳等を整備し、定められた保存場所で個人データを作成・加工・保存することを徹底する。
- ✓ 個人データを組織で管理し、取扱職員・管理媒体等を監査部門が把握した上で、定期的な監査等を行う。
- ✓ 従業者に対し、日頃から個人データの取扱いに係る規律・ルールを周知し徹底を促す。

事例７　グループ会社への監督が不十分な事例

親会社が、グループ子会社の従業者等の個人データについて、グループ子会社から個人データの取扱いの委託を受け、一括して人事システムで管理し、グループ全体の給与計算等の人事管理業務を行っていたところ、親会社の安全管理措置の不備が原因でグループ子会社の個人データが漏えいした。委託元であるグループ子会社は委託先である親会社における個人データの取扱状況を把握する等の必要かつ適切な監督を行っていなかった。



原因

- ✓ グループ会社同士であるため、一定の信頼関係が築けているとして、親会社の個人データの取扱状況について監査を行っていなかった。
- ✓ 外部の取引先とは違い、親会社に個人データを管理してもらうことは、個人データの取扱いの委託には該当せず、監督は不要だと認識していた。
- ✓ グループ全体に適用されるセキュリティポリシーが改訂されたにもかかわらず、子会社が対応できていなかった。

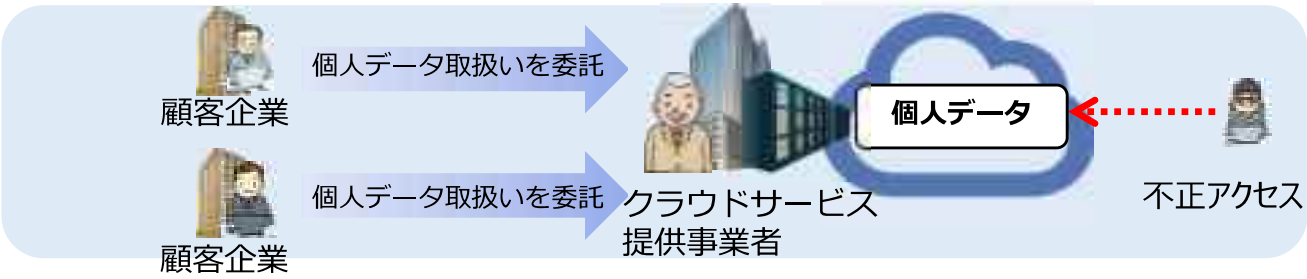
対策例

- ✓ 親会社は委託を受けた個人データを適正に管理するとともに、子会社は委託先がグループの親会社であったとしても、通常の外部委託先に対するルールと同じ基準で必要かつ適切な監督を行う。
- ✓ 例えば、親会社による自己点検又は第三者機関による検査等の結果を子会社がモニタリングするなど、親会社主導の下、効果的にグループ会社全体の安全管理措置等の取扱状況を共有し、必要かつ適切な監督を行える仕組みを構築する(※５）。

※５　グループ会社間の管理・監督については、規模や特性等に応じた多様な在り方が想定されるため、必要かつ適切な監督の方法は本例示に限定するものではない。

事例８　利用するクラウドサービスからの漏えい事例

クラウドサービス提供事業者が提供する業務システムが不正アクセスを受け、クラウド環境で管理されていた多数のクラウドサービス利用者である顧客企業の個人データが暗号化され、大量の個人データについて漏えいのおそれが生じた事案。



原因

- ✓ クラウドサービスの外部からの不正アクセス等の防止のための措置等の技術的安全管理措置に問題があった。
- ✓ 業務の委託ではないクラウドサービス利用は個人データの取扱いの委託には該当しないと考えていたため、委託先に対する個人データの取扱状況の監督を実施していなかった。

対策例

- ✓ 顧客企業は、利用しようとするクラウドサービスにおいて適切なセキュリティ対策が講じられているかを、サービス利用規約やクラウドサービスの安全性評価に関する資料等により確認し、適切なサービスを選定する。
- ✓ クラウドサービス利用が個人データの取扱いの委託となる場合、利用する顧客企業が適切に取扱状況を把握できるよう、クラウドサービス提供事業者は積極的にセキュリティレポート等の必要な情報を公開することが望ましい。

事例９　APIが悪用される事例

個人情報取扱事業者が提供するスマートフォンアプリやWebサービスにおいて、API（※６）を利用していたところ、APIの設計・設定不備により、攻撃者が当該サービスにログインした後、パラメータを書き換えることで、本来であれば取得できない他のユーザー情報を取得できる状態となっており、個人データの漏えい等が発生した事案。



原因

- ✓ 管理対象から漏れているAPIが存在した。
- ✓ URLや会員ID等のパラメータを書き換えることで、他ユーザーのデータにアクセス可能な状態であった。
- ✓ レスポンスに不要な情報が含まれていたことや、会員ID等が連番となっていたことから、攻撃者によるAPIの仕様等の推測が容易であった。
- ✓ 大量アクセスを制御するためのアクセス回数制限（レートリミット）がなかった。

対策例

- ✓ 定期的にAPIの棚卸しを行う。
- ✓ 認証（本人確認）に加え、認可（そのユーザーが当該データにアクセスする権限を有するかの確認）を都度行う仕組みを実装する。
- ✓ 不要な情報をレスポンスに含めないように設計する。会員IDや管理番号にランダムな値（UUID等）を採用する。
- ✓ 短時間での大量アクセスを検知・遮断するためのアクセス回数制限（レートリミット）を実装する。

※６　Application Programming Interfaceの略称であり、異なるシステムやアプリ間をつないでデータや機能を共有する仕組み。