事　務　連　絡
令和８年 10 月８日

一般社団法人日本旅行業協会会長　殿
一般社団法人全国旅行業協会会長　殿

観光庁参事官（旅行振興）

旅行業者における個人情報の適正な取扱いの徹底について

今般、旅行業界を含む様々な業界において、外部からの不正アクセスによる個人情報の大規模な漏えい等事案が相次いで発生しているところです。

旅行業者が取り扱う旅行者の氏名、住所、連絡先、旅券情報その他の個人情報の漏えい等は、旅行者の権利利益を侵害するおそれがあるだけでなく、旅行業界全体に対する信頼を損なうものであり、決してあってはならないものです。

万が一、個人情報の漏えい等が発生した場合には、個人情報の保護に関する法律（平成 15 年法律第 57 号）その他関係法令等に基づき、被害の拡大防止をはじめ、原因の究明、影響範囲の特定、再発防止策の実施、情報漏洩の対象となった個人への通知、個人情報保護委員会への報告など必要な対応を迅速かつ適切に講ずることが求められます。併せて、登録行政庁への速やかな報告をお願いいたします。

つきましては、貴協会におかれては、傘下会員に対し、個人情報の保護に関する法律その他関係法令等の遵守を改めて徹底するとともに、各会員における個人情報の管理体制及び取扱状況について点検を行い、個人情報の適切な管理及び再発防止に万全を期すよう周知いただきますようお願いします。

（参考）令和８年 10 月７日　個人情報保護委員会
「大規模な漏えい等事案を踏まえた対応について（注意喚起）」

公表資料

創立10周年
PPC 個人情報保護委員会
Personal Information Protection Commission
日本国政府

News Release

大規模な漏えい等事案を踏まえた対応について（注意喚起）

令和８年 10 月７日

個人情報保護委員会は、大規模な漏えい等事案を踏まえた対応について、注意喚起を行うこととしましたので、お知らせいたします。

【連絡先】
個人情報保護委員会事務局
監視・監督室
電話：03-6457-9680（代）

個人情報取扱事業者の皆様へ

令和８年 10 月７日
個人情報保護委員会

大規模な漏えい等事案を踏まえた対応について（注意喚起）

近時、個人情報保護委員会（以下「当委員会」という。）では、国民に広く普及した、大量の個人情報を取り扱う個人情報取扱事業者が外部からの不正アクセスを受け、その取り扱う大量の個人データが漏えいし、又は漏えいのおそれが生じた漏えい等事案に接しています。

当委員会は、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 26 条第１項の規定による漏えい等報告を受領した事案に関して必要な調査を行い、必要に応じて指導等の権限行使等を行うことで、法第 23 条で規定する安全管理措置について、個人情報取扱事業者の自主的な改善を促しています。また、当委員会は、事業者の安全管理措置の検討に資するようガイドラインに手法の例示等を示すとともに、現在その追加、現代化を図っています。

個人情報取扱事業者のうち、特に、国民の多くが利用する事業における業界内で高いシェアを有するサービス又は顧客が事業者を指定し難いサービスを提供することで大量の個人情報を保有している事業者、機微性の高い個人情報、財産的被害につながるおそれのある個人情報又は詐欺などに利用されるおそれのある個人情報を保有している事業者その他の漏えい等が生じた場合に国民の権利利益の侵害の蓋然性が高い個人情報を保有する事業者の皆様におかれましては、下記で提供する情報も踏まえて、個人情報等の適正な取扱いをお願いします。

記

１　安全管理措置の全体像

個人情報の保護に関する法律についてのガイドライン（通則編）「10 （別添）講ずべき安全管理措置の内容」（以下「ガイドライン（通則編）別添」という。）では、法第 23 条に定める安全管理措置として、個人情報取扱事業者が具体的に講じなければならない措置や当該措置を実践するための手法の例等について示しています。ガイドライン（通則編）

別添は、「講じなければならない措置」と、当該措置を実践するための「手法の例示」で構成されており、「講じなければならない措置」は、これらに従わなかった場合、法違反と判断される可能性がありますが、「手法の例示」は、文字どおり例を示したものであって、必ずしも例示の内容の全てを講じなければ、法違反と判断されるというものではなく、また、適切な手法は例示の内容に限られません。この点、ガイドライン（通則編）別添では、「安全管理措置を講ずるための具体的な手法については、個人データが漏えい等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の規模及び性質、個人データの取扱状況（取り扱う個人データの性質及び量を含む。）、個人データを記録した媒体の性質等に起因するリスクに応じて、必要かつ適切な内容とすべきものである」としています。

2　今後の見直し予定と現時点における見直し後の技術的安全管理措置の内容

令和８年９月 16 日に開催した第 369 回個人情報保護委員会で決議したとおり、今後、ガイドライン（通則編）別添の「手法の例示」等については、現代化を含めた見直しを予定しています[1]。見直しの内容の確定は、来年４月を予定していますが、近時の動向を踏まえて、「手法の例示」として、より参考になると考えられるため、見直し予定の内容を先取りする形でお示しします。

外部からの不正アクセスとの関係では、主に安全管理措置のうち技術的安全管理措置が問題になるところ、現時点における見直し後の技術的安全管理措置の内容は別紙のとおりとなります。なお、安全管理措置には、技術的安全管理措置のほかに、個人データの取扱いに係る規律の整備、組織的安全管理措置、人的安全管理措置、物理的安全管理措置及び外的環境の把握がありますので御留意ください。

3　不要となった個人データの消去

法第 22 条は、「個人情報取扱事業者は、利用目的の達成に必要な範囲内において、個人データを正確かつ最新の内容に保つとともに、利用する必要がなくなったときは、当該個人データを遅滞なく消去するよう努めなければならない。」と規定しています。すなわち、個人情報取扱事業者は、利用目的が達成され当該目的との関係では当該個人データを保有する合理的な理由が存在しなくなった場合や、利用目的が達成されなかったものの当該目的の前提となる事業自体が中止となった場合等は、当該個人データを遅滞なく消去するよう努めなければなりません（法令の定めにより保存期間等が定められている場合は、この限りではありません。）。こうした対応が徹底されず、漏えい等事案がより深刻化するといった事例にも接していますので、保管している個人データの必要性についてその法令等の根拠とともに確認を適切に行うことを含めて、改めて注意喚起します。

---

[1] https://www.ppc.go.jp/files/pdf/260916_shiryou-2.pdf

４　その他御参考

当委員会は漏えい等報告を受領した事案を分析し、典型的な事案類型及び問題点について「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）[2]を公表し、注意喚起を行っていますので、こちらも参考にしてください。

以　上

[2] https://www.ppc.go.jp/files/pdf/261007_warning.pdf

（別紙）

10-6　技術的安全管理措置

個人情報取扱事業者は、情報システム（パソコン等の機器を含む。）を使用して個人データを取り扱う場合（インターネット等を通じて外部と送受信等する場合を含む。）、技術的安全管理措置として、次に掲げる措置を講じなければならない。

（1）アクセス制御

担当者及び個人データを取り扱う情報システムの範囲を限定するために、適切なアクセス制御を行わなければならない。

（2）アクセス者の識別と認証

個人データを取り扱う情報システムを使用する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。

（3）外部からの不正アクセス等の防止

個人データを取り扱う情報システムを外部からの不正アクセス又は不正ソフトウェアから保護する仕組みを導入し、適切に運用しなければならない。

（4）情報システムの使用に伴う漏えい等の防止

情報システムの使用に伴う個人データの漏えい等を防止するための措置を講じ、適切に運用しなければならない。

（5）不正アクセス等の検知等

個人データを取り扱う情報システムに対する不正アクセス等が発生した場合に早期に検知等するための措置を平時から講じ、組織内ネットワークにおける被害拡大を防止できるよう適切に運用しなければならない。

講じなければならない措置	手法の例示	中小規模事業者における手法の例示
(1) アクセス制御	（情報システムの限定） • 個人データを取り扱う情報システムを限定する。 • 個人データを取り扱う情報システムへのアクセスを最小化する。例えば、事前に許可した特定の IP アドレスからのみに限定する方法が考えられる。 （アクセスできる者の限定） • 個人データを取り扱う情報システムを使用できる従業者については、ユーザーID に付与するアクセス権限を最小化することにより限定する。 • 特権アカウントを割り当てる従業者、利用する端末、利用する場面等を最小限に限定する。 • 組織体制に変更が生じた場合（例えば、人事異動、従業者の退職等）等に、アクセス権限の変更を適切に行う。 • アクセス制御が適切に行われているか確認する。例えば、アクセス権限について定期的に監査するなど、アクセス権限の棚卸しを行う等の方法が考えられる。 • 組織内外からのアクセスについて、アクセス要求ごとにアクセス元の場所、アクセス時間、デバイスのセキュリティ状態等の動的コンテキストを評価し、リスクに応じてアクセスの可否を判断する仕組みを導入する。	• 個人データを取り扱うことのできる機器及び当該機器を取り扱う従業者を明確化し、個人データへの不要なアクセスを防止する。
(2) アクセス者の識別と認証	（情報システムを使用する従業者の識別・認証手法の例） • ユーザーID、パスワード、磁気・IC カード、指紋認証・静脈認証・顔認証等の方法が考えられる。 • ユーザーID・パスワードを利用する場合には、同一のユーザーID・パスワードの使い回しの原則禁止及び類似パスワードの使い回しの制限、最低パスワード文字数の設定、一定回数以上ログインに失敗した ID の停止等を行う。	• 機器に標準装備されているユーザー制御機能（ユーザーアカウント制御）により、個人情報データベース等を取り扱う情報システムを使用する従業者を識別・認証する。

講じなければならない措置	手法の例示	中小規模事業者における手法の例示
	• 個人データへのアクセス権限を有する者が使用できる端末又はアドレス等についての識別と認証を実施する。例えば、IP アドレス認証、電子証明書等の方法が考えられる。 • 組織外ネットワークからのアクセスや、管理者権限でのアクセス、重要な個人データへのアクセスにおいては、識別・認証手法を複数組み合わせる多要素認証（フィッシングに耐性のあるものを含む。）を導入する。 （情報システムを使用する従業者以外の者の識別・認証手法の例） • 従業者以外の者を適切に識別・認証する方法を採用する。例えば、同一及び類似パスワードの使い回しをしないよう周知、最低パスワード文字数の設定、一定回数以上ログインに失敗した ID の停止、多要素認証（フィッシングに耐性のあるものを含む。）の導入等が考えられる。	
(3) 外部からの不正アクセス等の防止	• 個人データを取り扱う情報システムと外部ネットワークとの接続箇所にファイアウォール等を設置し、不正アクセスを遮断する。 • 個人データを取り扱う情報システム及び機器にセキュリティ対策ソフトウェア等（ウイルス対策ソフトウェア等）を導入して適切に運用（パターンファイルや修正ソフトウェアの更新確認等を行うことを含む。）し、不正ソフトウェアの有無を確認する。 • 機器やソフトウェア等に標準装備されている自動更新機能等の活用、端末及びサーバー等のオペレーティングシステム、ミドルウェア、アプリケーション等に対するセキュリティ対策用修正ソフトウェアの適用により、ソフトウェア等を最新状態とする。 • 個人情報取扱事業者において許可していないソフトウェア等の導入を防止する。例えば、ソフトウェアの導入時の確認のほか、定期的な監査などの方法が考えられる。 • 組織が許可し、セキュリティ基準を満たしたデバイスからのみ個人データへのアクセスを許可する。	• 個人データを取り扱う機器等のオペレーティングシステムを最新の状態に保持する。 • 個人データを取り扱う機器等にセキュリティ対策ソフトウェア等を導入し、自動更新機能等の活用により、これを最新状態とする。

講じなければならない措置	手法の例示	中小規模事業者における手法の例示
(4) 情報システムの使用に伴う漏えい等の防止	(情報システムの開発、維持・管理、変更等における安全性確保) • 個人データを取り扱う情報システムの設計時に安全性を確保し、継続的に見直す（情報システムのぜい弱性を突いた攻撃への対策を講ずることも含む。）。 • 個人データを取り扱う情報システムの動作確認を行う際に、テストデータとして利用する個人データを必要最小限とする。例えば、テストデータとして個人データを利用することを禁止したり、動作確認に影響のない範囲で、個人データの一部を他のデータに置き換えるなどの方法が考えられる。 • 個人データを取り扱う情報システムの変更時に、当該変更によって情報システム又は運用環境のセキュリティが損なわれないことを検証する。 (通信の経路又は内容の暗号化) • 個人データを含む通信の経路又は内容を暗号化する。例えば、インターネットや無線 LAN 等による個人データの送信（例えば、本人又は従業者による入力やアクセス、メールに添付してファイルを送信する等を含むデータの転送等）時に、個人データの暗号化等の秘匿化（例えば、SSL/TLS、S/MIME 等）を行うなどの方法が考えられる。 • 移送する個人データについて、パスワード等による保護を行う。 (クラウドサービスを利用した情報システムの更改・廃棄) • クラウドサービスのサーバ上に保管された個人データを消去する際は、クラウドサービス提供事業者が提供する方法、暗号化消去等、容易に復元できない手段を採用する。	• メール等により個人データの含まれるファイルを送信する場合に、当該ファイルへのパスワードを設定する。

講じなければならない措置	手法の例示	中小規模事業者における手法の例示
(5)不正アクセス等の検知等	（定期的な分析） • 個人データを取り扱う情報システムの使用状況、個人データへのアクセス状況、個人データを取り扱う情報システムへの外部からのアクセス状況等のログ（例えば、認証ログ、アクセスログ、操作ログ、通信ログ等）等を一定の期間保管する。 • 当該ログ等の漏えい、滅失及び毀損並びに改ざん、不正消去等からの適切な保護を行う。 • 当該ログ等の定期的な分析により、不正アクセス等の発生又は兆候を早期に検知する。 （常時監視による早期検知） • 不正アクセス等の発生又は兆候を早期に検知等するための仕組み（例えば、IDS/IPS、EDR 等）等を導入する。 （組織内ネットワークでの被害拡大の防止） • 不正アクセス等が発生した場合でも個人データを取り扱う情報システムの被害が広がらないよう、必要な対策を講ずる。例えば、侵害を受けた又はそのおそれがある情報システムの停止・隔離、アカウントの無効化などの方法が考えられる。その他必要な対策については、10-6 技術的安全管理措置(1)から(4)の手法の例示も参照されたい。	• 個人データを取り扱う情報システムの使用状況、個人データへのアクセス状況、個人データを取り扱う情報システムへの外部からのアクセス状況等のログ等を一定の期間保管する。

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

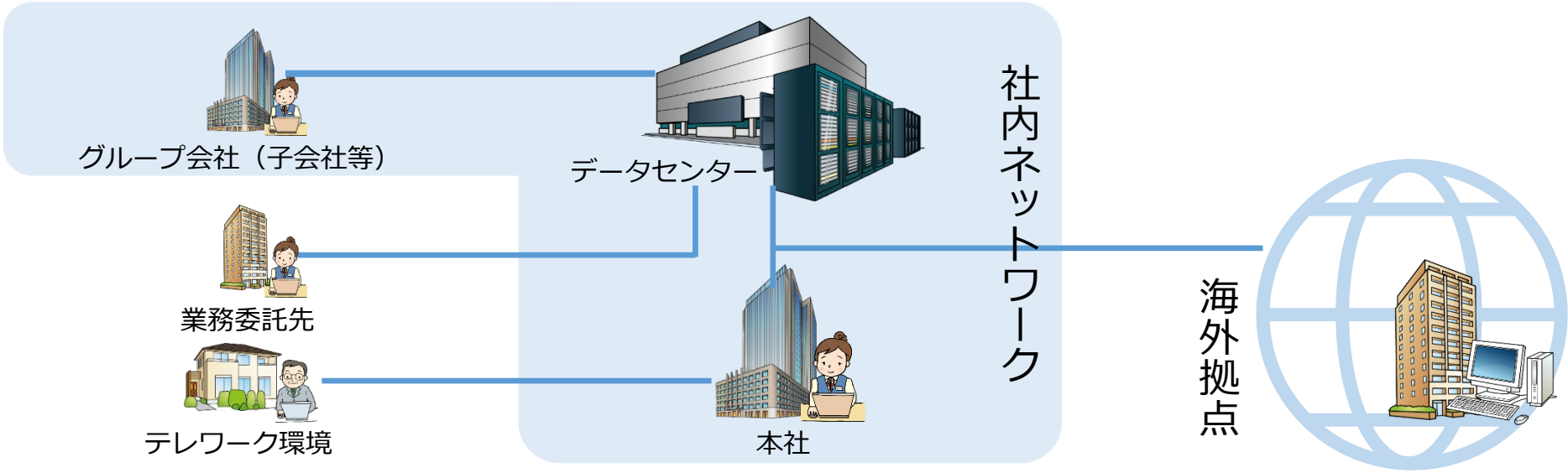
（令和６年12月11日、令和８年10月７日改訂）

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

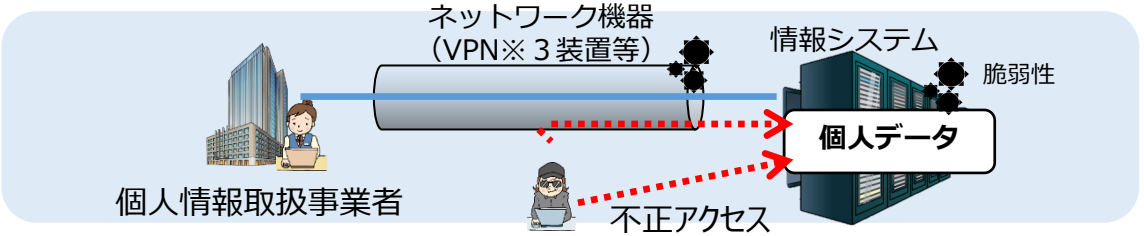
　個人情報保護委員会には、これらの手口によって発生した個人データの漏えい等事案が複数報告されている状況です。
　報告された事案を分析したところ、以下九つの事例に類型化できる問題点が挙げられ、これら問題への措置が十分でない場合、安全管理措置（法第23条）、従業者の監督（法第24条）及び委託先の監督（法第25条）の違反と判断される可能性があります。
　脆弱性への対応や強固な認証方式の採用等のセキュリティ対策は、どれか一つを講じればよいということではなく、多層的に講ずる必要があります。また、これらの事例の多くは、委託先等を含め、個人情報取扱事業者内外における複数の組織・部署が関係することから、その問題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。

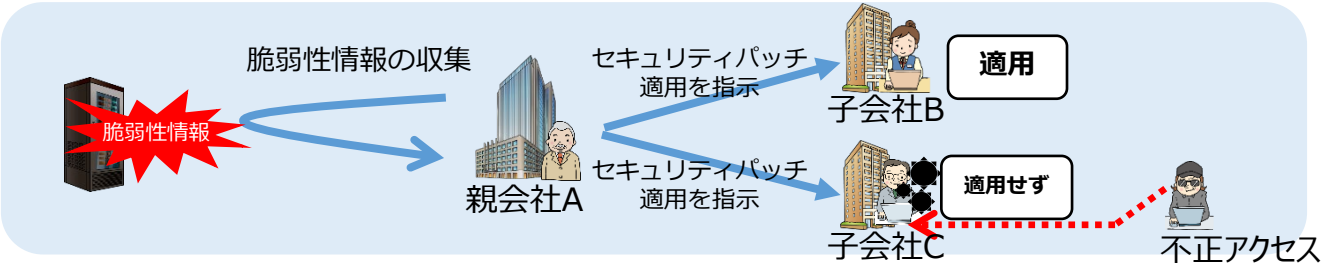
対策例

- ✓ 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。

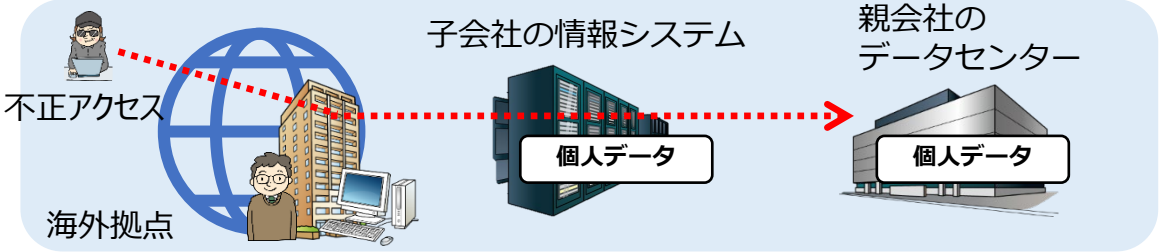
対策例

- ✓ 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

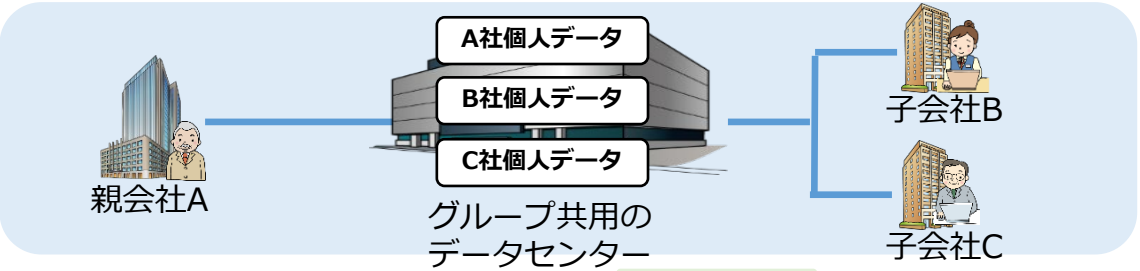
- ✓ 海外拠点は国内にある親会社のセキュリティガバナンスが行き届きにくく、情報システムの脆弱性対策が十分でなかった。
- ✓ 海外拠点に設置されていた貸与品のVPN装置が台帳にリストアップされておらず、VPN装置の存在が把握できなくなっていた。
- ✓ 子会社の情報システムと親会社のデータセンターとの間のアクセス制御が適切ではなかった。

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

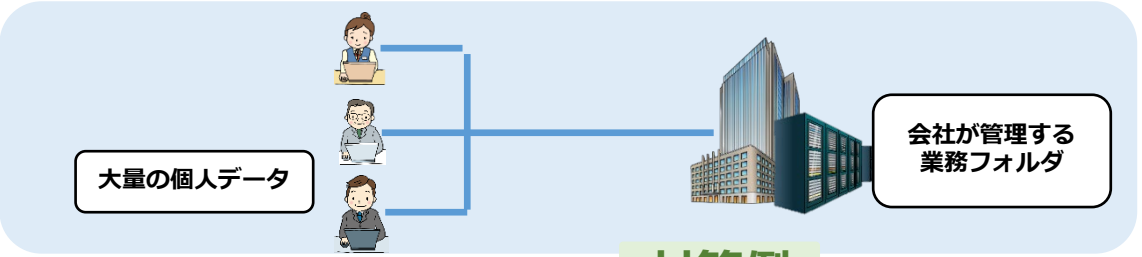
- ✓ グループ会社の個人データを管理するデータセンターにおいて、業務上の利便性等の観点から、グループ会社間で相互にアクセス可能としていた。
- ✓ 親会社が管理するグループネットワークの管理者パスワードの強度が十分ではなかった。

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

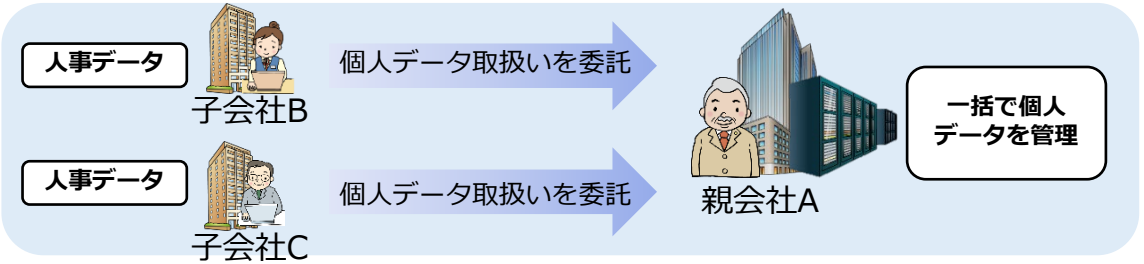
- ✓ 従業者が業務で使用する電子ファイルについて、組織として管理されておらず、従業者各自のデスクトップ端末等で加工・保存される業務運用が慣例化してしまっており、また、このような管理状況について、定期的な監査等の網にもかからなかった。
- ✓ 組織として管理されていない個人データの中には、本来は消去すべき古いデータ等が含まれているケースがあり、漏えい被害の範囲が大きくなってしまった。

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。

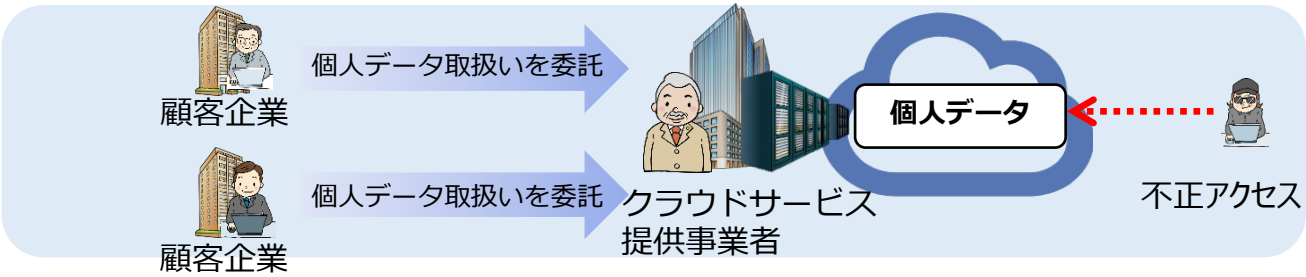
対策例

- ✓ 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。