クリプト便

マイナンバー収集ガイドブック

法人が使える マイナンバー 受け渡し手段 とは？

NRI SECURE

マイナンバー収集ガイドブック

法人が使える
マイナンバー受け渡し手段とは

目　次

クリプト便

はじめに

日本国内でマイナンバー制度の運用がスタートしたのは2015年10月のこと。マイナンバーは「住民票を有するすべての方が持つ1人にひとつの12桁の番号」で、社会保障、税、災害対策の分野で横断的に使える番号を導入することにより、機関をまたいだ情報のやり取りにおいて、個人情報の特定・確認が確実かつ迅速にできるようにすることを目的としています。

事業者は従業員への給与の源泉徴収の作成等を目的に、従業員や家族のマイナンバー情報（特定個人情報）を収集し、各種手続きを行っているでしょう。また、証券会社や保険会社、健康保険組合等も加入者からマイナンバー情報を収集しています。事業者としてマイナンバー情報の収集を行う中で、そもそも自分たちはルールに沿った収集を行えているのか、より効率的な受け渡し手段はないのかと、疑問を持たれている方も多くいらっしゃるのではないでしょうか。

受け渡し手段は郵送や対面以外にも多く存在します。しかし、マイナンバー情報の取り扱い方法は法律やガイドラインで厳しく定めているため、**受け渡し手段を取捨選択する際には、ルールに則っているかどうかの確認が必要**です。

本ガイドブックでは、法律やガイドラインに即して、受け渡し手段を検討する際に特に注意すべき点を解説します。皆様の業務をより安全かつ効率的に行うためにも、これを機に受け渡し手段を見直してみてはいかがでしょうか。

1

特定個人情報の「適正な取り扱い」

マイナンバーは「特定個人情報」（マイナンバー制度により付与された個人番号をその内容に含む個人情報）の枠組みで管理されるものであり、事業者がマイナンバーを取り扱う際に参考になるのは、個人情報保護委員会が定めた『**特定個人情報の適正な取扱いに関するガイドライン（事業者編）**[*1]』です。ガイドラインの中で、「しなければならない」および「してはならない」と記述されている事項については、これらに従わなかった場合に法令違反として判断される可能性があります。そこで、まずは本章を通して、このガイドラインの中で「特定個人情報を収集する」際の重要事項を理解することから始めましょう。

[*1] 本ガイドブックは令和２年５月25日最終改正の「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」をもとに制作しており、最新版と内容が異なる場合がございます。
個人情報保護委員会：特定個人情報の適正な取扱いに関するガイドライン（事業者編）
https://www.ppc.go.jp/legal/policy/

1-1. 特定個人情報に関する安全管理措置

個人情報保護委員会が定めた『特定個人情報の適正な取扱いに関するガイドライン（事業者編）』では、「特定個人情報に関する安全管理措置」について触れられており、事業者は「特定個人情報の安全管理措置が適切に講じられるよう、当該従業者に対する必要かつ適切な監督を行わなければならない」としています。

安全管理措置と聞くと真っ先に漏えい対策を想起しがちですが、「（別添）特定個人情報に関する安全管理措置（事業者編）」においては、まず特定個人情報等の取扱いを検討する際に次の３つを明確にしておく必要があるとしています。

安全管理措置の検討において明確化すべき事項

- 個人番号を取り扱う事務の範囲
- 取り扱う特定個人情報等の範囲
- 事務取扱担当者

これらを踏まえ、特定個人情報の適正な取り扱いを実現していくために、まずは組織として基本方針を策定すると共に、事務の流れを整理し、具体的な取り扱い方法を明記した取扱規定を策定する必要があります。その上で講ずべき具体的な安全管理措置の内容として、ガイドラインには「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」「技術的安全管理措置」の４つが挙げられています。中でも「**物理的安全管理措置**」と「**技術的安全管理措置**」の２つは、マイナンバーの受け渡し手段を検討する際にしっかり読んで理解しておきたい内容です。

1-2. 物理的安全管理措置

ガイドラインでは「事業者は、特定個人情報等の適正な取り扱いのために、次に掲げる物理的安全管理措置を講じなければならない」とされています。（以降、各措置のタイトルはガイドラインのまま記載し、説明文や具体例は当社解釈により表現を一部変更しています。）

a）特定個人情報等を取り扱う区域の管理

特定個人情報などの情報漏えいを防止するために、特定個人情報ファイル（個人番号をその内容に含む個人情報ファイル）を取り扱う情報システムを管理する区域（以下、管理区域）や、特定個人情報等を取り扱う事務を実施する区域（以下、取扱区域）を明確にし、物理的な安全管理措置を講ずる必要があります。

具体例

- 入退室管理を行うと共に管理区域へ持ち込む機器を制限する。
- IC カードやナンバーキーなどによる入退室管理システムを設置する。
- 壁または間仕切りの設置、座席配置の工夫を行う。

b）機器及び電子媒体等の盗難等の防止

管理区域および取扱区域において特定個人情報を取り扱う機器、電子媒体、書類などの盗難または紛失を防止するために、物理的な安全管理措置を講ずる必要があります。

具体例

- 特定個人情報を取り扱う機器、電子媒体、書類を、施錠できるキャビネットや書庫に保管する。
- 特定個人情報ファイルを取り扱う情報システムの機器は、セキュリティワイヤーなどにより固定する。

c) 電子媒体等の取り扱いにおける漏えい等の防止

特定個人情報が記録された電子媒体や書類を管理区域もしくは取扱区域の外（事業所内を含む）へ持ち出す場合は、容易に個人番号が判明しない措置の実施、追跡可能な移送手段の利用など、安全策を講ずる必要があります。

具体例

- 持ち出すデータに対して、暗号化やパスワードによる保護、施錠できる搬送容器の使用などを検討する。
- 持ち出す書類に対して、封緘、目隠しシールの貼付を行う。

d) 個人情報の削除、機器及び電子媒体等の廃棄

個人番号に関連する事務を行う必要がなくなり、かつ法令で定められた保存期間を経過した場合には、個人番号をできるだけ速やかに復元できない手段で削除するか廃棄しなければなりません。また、個人番号や特定個人情報ファイルを削除したり、電子媒体を廃棄したりする場合には、削除または廃棄した記録を保存する必要もあります。これらの作業を委託する場合には、委託先が確実に削除または廃棄したかどうかを証明書などにより確認しなければなりません。

具体例

- 特定個人情報が記載された書類を廃棄する場合は、焼却または溶解などの復元不可能な手段を採用する。
- 特定個人情報が記録された機器や電子媒体を廃棄する場合、専用のデータ削除ソフトウェアを利用するか物理的に破壊するなど、復元不可能な手段を採用する。
- 特定個人情報を取り扱う情報システムにおいては、保存期間経過後における個人番号の削除を前提とした情報システムを構築する。
- 個人番号が記載された書類は、保存期間経過後における廃棄を前提とした手続フローを定める。

1-3. 技術的安全管理措置

ガイドラインでは「事業者は、特定個人情報等の適正な取り扱いのために、次に掲げる技術的安全管理措置を講じなければならない」とされています。（以降、各措置のタイトルはガイドラインのまま記載し、説明文や具体例は当社解釈により表現を一部変更しています。）

a）アクセス制御

情報システムを使用して個人番号に関連する事務を行う場合、取り扱い担当者や当該事務で取り扱う特定個人情報ファイルの範囲を限定するために、適切なアクセス制御を行う必要があります。

具体例

- 特定個人情報ファイルを取り扱う端末を、アクセス制御により限定する。
- ユーザーIDに付与するアクセス権により、特定個人情報ファイルを取り扱う情報システムを使用できる者をマイナンバー取り扱い担当者に限定する。

b）アクセス者の識別と認証

特定個人情報を取り扱う情報システムは、マイナンバー取り扱い担当者が正当なアクセス権を有する者であることを、識別した上で認証する必要があります。

具体例

- ユーザーID、パスワード、磁気カード・ICカードなどで識別する。

c）外部からの不正アクセス等の防止

情報システムを外部からの不正アクセスまたは不正ソフトウェアから保護する仕組みを導入し、適切に運用する必要があります。

具体例

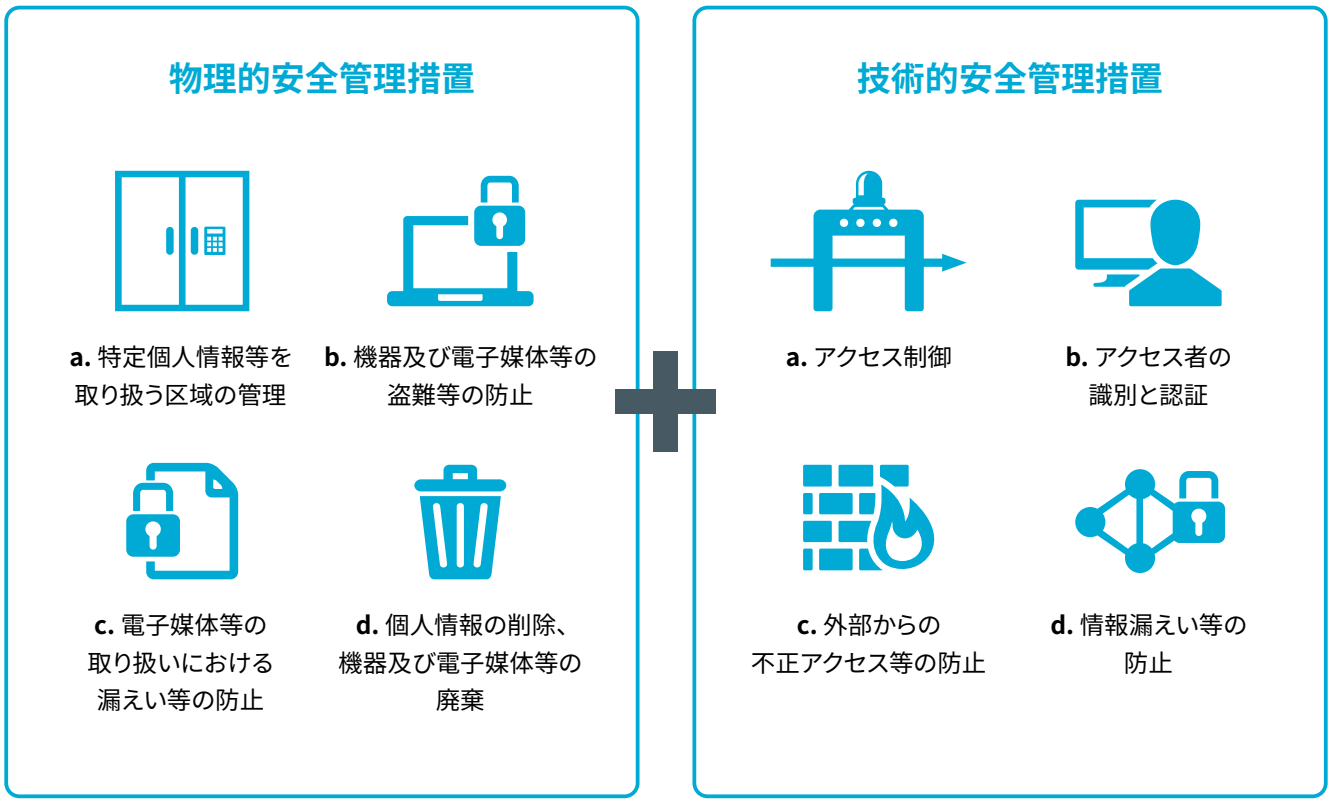
- 情報システムと外部ネットワークとの境にファイアウォールを設置し、不正アクセスを遮断する。
- 情報システムや機器にセキュリティ対策ソフトウェア（ウイルス対策ソフトウェア等）を導入する。
- 機器やソフトウェアに標準装備されている自動更新機能の活用により、常に最新の状態に維持する。
- ログの分析を定期的に行い、不正アクセスを検知する。

d) 情報漏えい等の防止

特定個人情報をインターネットなどにより外部に送信する場合、通信経路における情報漏えいを防止するための措置を講ずる必要があります。

具体例

- 通信経路を暗号化する。
- 情報システム内に保存されている特定個人情報データを暗号化またはパスワードにより保護する。



2

受け渡し手段のメリットと問題点

企業がマイナンバーの取り扱いをおざなりにした場合は、個人情報保護法よりも重い罰則を受けるようです。企業にとってはマイナンバー制度の運用そのものが大きなリスクと言っても過言ではないでしょう。便利さや安さは、人的要因による情報漏洩の起きやすさとトレードオフの関係にあることがほとんどです。便利だから、コストがかからないからといって安易な手段を選択すると、取り返しのつかない事態が発生する可能性も否定できません。

受け渡しに便利な手段は複数ありますが、ガイドラインの基準に照らしてアリなのか、ナシなのか、適切に評価する必要があります。また、たとえ適切であっても、手間やコストが掛かりすぎる手段では運用し続けるのは難しいでしょう。果たして、安全かつ簡単で、多くの人手に頼らずマイナンバーを収集する方法はあるのでしょうか。本章では、ガイドラインの内容に則って、メール（暗号化を含む）、電話、FAX、郵送、クラウドサービスといった受け渡し手段の何が問題で、どれなら指針を満たせるのか、具体的に説明します。

2-1. メール・FAX・郵便書留はアリ？ ナシ？

ここでは、メール、FAX、郵便書留などがマイナンバーの受け渡し手段としてアリかナシをガイドラインの基準に照らして評価してみます。

1. メール

マイナンバーが記載されたファイルをメールに添付するのは、ガイドライン違反になり得ます。「技術的安全管理措置」の「情報漏えい等の防止」の対策例として示されている「通信の暗号化」に触れる可能性があります。また、メールは誤送信のリスクが高いことから利用は推奨できません。

2. メール＋暗号化

暗号化の手法として多くの人が安易に利用しているメール添付時の「パスワード付き zip ファイル」は、暗号化アルゴリズムとしては脆弱なため、マイナンバーに限らず利用を控えることをお勧めします。古くから浸透している暗号化の手法ではあるものの、PC の処理能力が低い時代に合わせて作られたものであり、近年の技術と PC スペックがあれば、破ることは不可能ではありません。通信経路や誤送信からの漏えいのリスクに加え、暗号の強度不足という問題があります。

3. FAX

ガイドライン違反になり得ます。「物理的安全管理措置」の「特定個人情報等を取り扱う区域の管理」に触れる可能性があります。FAX は多くの場合、部署内で共有されているため、文書が送信相手に確実に届くとは限りません。さらに、マスキングされていないナンバーが受信トレイに長時間放置されることも想定されます。メールと同様に誤送信のリスクも否定できません。

4. 郵便書留

郵便書留は受け渡し手段として有効です。相手に確実に届き、受け取ったことを確認できるのがメリットですが、紙文書で収集したマイナンバーは適切なタイミングで電子化する必要があります。代行業者に依頼すればコストがかかり、業者が個人情報の委託先となることで法令による監督責任も発生します。

5. クラウドサービス（ファイル転送／共有サービス）

クラウドサービスはインターネットを介して簡易かつ迅速にマイナンバー情報の受け渡しができる有効な手段です。しかし、ガイドラインに準拠しているかどうかは、各クラウドサービスのセキュリティ仕様や機能により判断が分かれます。また、サービスが定める契約条項によっては次項で解説する「委託」に該当し、手間が増える可能性があるため、多数あるサービスの中から適したサービスを選択することが重要です。

各受け渡し手段とそれぞれの懸念点

メール	メール＋暗号化	FAX	郵便書留	クラウドサービス
				
● 誤送信 ● 通信経路からの漏えい	● 誤送信 ● 通信経路からの漏えい ● 暗号の強度不足	● 誤送信 ● 原本の紛失	● 郵便の手間とコスト ● 代行業者の監督責任	サービスごとに以下が異なる ● ガイドラインへの準拠度合 ● 委託への該当有無

2-2. 外部事業者の利用における注意点（委託の取扱い）

個人番号に関連する事務を委託する場合は、委託先において必要な安全管理措置が適切に講じられるよう、「委託を受けた者」（委託先）に対する必要かつ適切な監督を行う必要があります。

必要かつ適切な監督とは？

1. 委託先の適切な選定を行う
2. 委託先に安全管理措置を遵守させるために必要な契約を締結する
3. 委託先における特定個人情報の取り扱い状況を把握する

それでは、マイナンバーの受け渡しに配送業者や通信事業者などの外部事業者による配送、通信手段を利用する場合は委託に該当するのでしょうか。配送業者は通常、依頼された配送物の中身については関知しないことから、個人番号関係事務または個人番号利用事務の委託には該当しないと考えられます。また、通信事業者による通信手段を利用する場合も、通常は通信手段を提供しているに過ぎないことから、同様に個人番号関係事務または個人番号利用事務の委託には該当しないと判断できます。

さらに、マイナンバーの受け渡しにクラウドサービスを利用する場合はどうでしょうか。これは各クラウドサービスが定めるポリシーにより異なります。クラウドサービスを提供する事業者が、契約条項で電子データを取り扱わないと明確に定めている場合は、番号法上の委託に該当しません。したがって、クラウドサービスを提供する事業者に対して監督を行う義務は課されません。ただし、委託に該当しない場合も、クラウドサービスを利用する事業者は、クラウドサービス上で取り扱うデータについて、適切な安全管理措置を講ずる必要があります。そのため、**ガイドラインに準拠するための十分な機能がクラウドサービスに備わっているかを確認することが非常に重要**です。

3

「ファイル転送サービス」という選択

マイナンバーの受け渡しを対面や郵便書留等の配送で行っている事業者が、これらに代わる手段としてクラウドサービスの中でも「**ファイル転送サービス**」を選択するケースが増えています。しかし、様々な法人向けファイル転送サービスが提供されているだけでなく、無料で使える個人向けサービスもあふれており、「どれも同じように見えて、いったい何を基準に選べばよいのかわからない」と法人担当者を悩ませる原因となっています。一方で、依然として「ファイルの受け渡しなら、オンラインストレージなどの共有サービスで事足りるのでは？」という安易な考えが目立つのも事実です。

そのサービスが数々のセキュリティ施策に守られた堅牢なデータセンターを利用しているか？ なぜ無料で提供できるのか？といったことは、利用する立場からはなかなか見えにくいものです。マイナンバーの受け渡しに利用する際のサービス選定においては、製品が高い自由度や利便性を備えていることよりも重要視すべきポイントがあります。そこで本章では、番号法に照らして、マイナンバーの受け渡しに適したサービスとはどんなサービスなのかを解説していきます。

3-1. ファイル転送サービスに欠かせない３つの条件

マイナンバーの受け渡しをする際、メールやFAX、郵便書留に代わる送信手段として期待されるのが「**ファイル転送サービス**」です。「郵便書留の電子化」というコンセプトで開発され、送ったデータが相手に届いたかどうかを確認することが可能です。

しかし、一時的とはいえ、他社のサーバに情報を預ける仕組みであるため、安全上の懸念は当然出てきます。実際、機密情報の扱いには適さないサービスが存在することも事実ですが、高いセキュリティを実現したサービスなら、マイナンバーをはじめとした個人情報全般の受け渡しに適しています。

マイナンバーの受け渡しに適したサービスに欠かせない条件は、次の３つです。

条件１：契約条項で「ファイルを取り扱わない」と明記されていること。
（委託の取扱い）

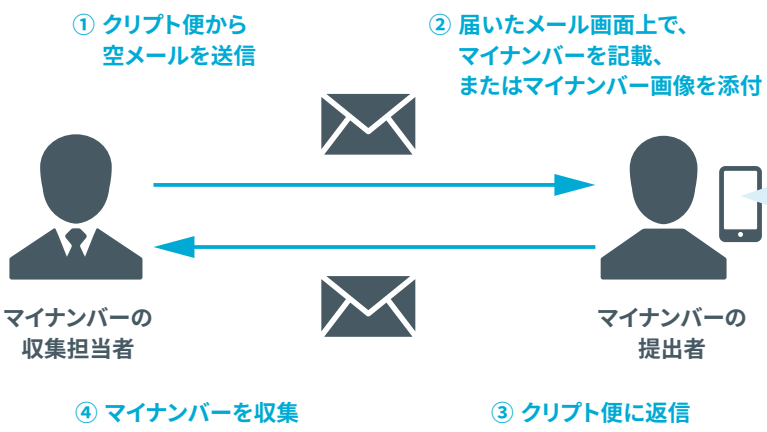
条件２：適切なアクセス制御が行えること。
（技術的安全管理措置　**a.** アクセス制御　**b.** アクセス者の識別と認証）

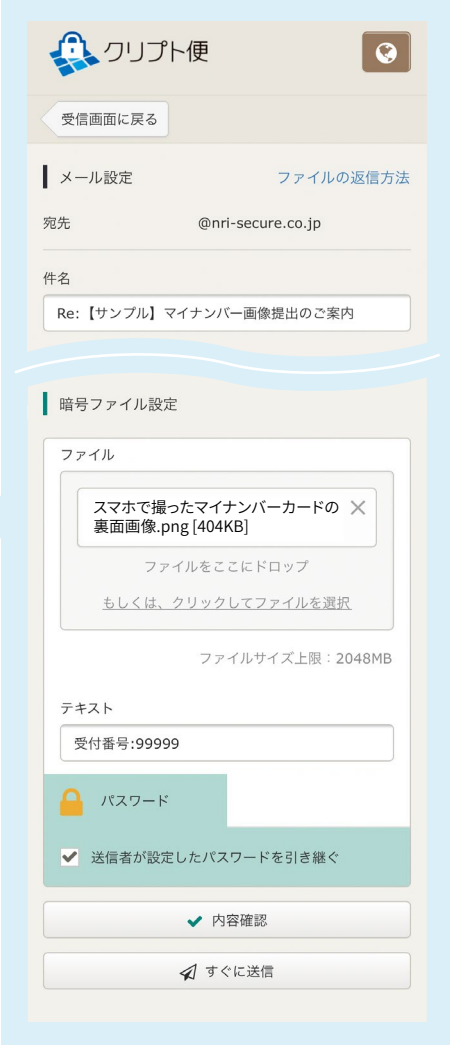
条件３：不正アクセスや情報漏洩への防止策が導入・運用されていること。
（技術的安全管理措置　**c.** 外部からの不正アクセス等の防止　**d.** 情報漏えい等の防止）

この３つの条件をクリアする数少ないサービスの一つが、NRIセキュアテクノロジーズが高水準のセキュリティレベルで提供する「**クリプト便**」です。ファイル転送市場で国内シェアNo.1[*2]であるだけでなく、その50%を超える顧客がセキュリティ要件の高い金融関連で、さらに健康保険組合等の多くの事業者でマイナンバーの受け渡しに実際に利用されている点も特徴です。クリプト便では、「ゲスト返信機能」を使ってマイナンバーを収集します。これは、ユーザーアカウントを持たない多数の個人から、安全・確実にデータを収集するための機能で、通信経路、ファイルに加え、専用のテキストエリアに入力された文章はいずれも高度に暗号化され、ガイドラインの要件を満たしています。さらに、マイナンバーの提出者に対して提出依頼メールを送信する際に、上長承認機能を利用することで相手先が間違っていないかチェックできるため効果的な誤送信防止を実現できます。「メール添付のような利便性」と「配達証明の書留に勝る安心感」を実現するサービスです。

[*2] 出典：ITR「ITR Market View：コラボレーション市場2020」、ユーザー間ファイル転送市場ベンダー別売上金額シェア（2019年度）

ゲスト返信機能によるマイナンバーの収集





3-2. クリプト便による安心安全なマイナンバー収集

クリプト便によるマイナンバー収集がなぜ安心安全なのか、先に挙げた3つの条件について、もう少し具体的に説明します。

ファイルを取り扱わない規定（条件1）

クリプト便は契約条項（約款第4条）によって、特定個人番号を含む電子データの取り扱い業務は、お客様自身で行っていただく旨を定めています。

> **クリプト便約款第4条の抜粋**
> 当社は、ファイル交換のためのプラットフォームのみを提供するものであり、当社がクリプト便サーバ上に保管されたファイル内容を閲覧することはありません。お客様は自らの責任において関連法令を遵守してファイル交換を行うものとします。24時間365日ご利用いただけますが、保守点検等、当社の都合で、平日日中以外にサービス停止させていただくことがあります。

適切なアクセス制御（条件2）

クリプト便は、利用時にID/パスワードによるログイン認証が必要となるため、適切なユーザー識別ができます。また、グローバルIPアドレスによるネットワーク制限や、クライアント証明書によりアクセスする端末を制限することも可能です。さらに、より安全に社外とやり取りしたい場合には、相手に対して社外ユーザー用アカウントを発行できるため、ログイン認証を求めたり、操作ログを取得したりすることが可能です。

不正アクセスや情報漏洩の防止（条件3）

クリプト便は、外部および内部からの不正アクセスを防止するため、主に4つの対策を実施しています。

1. 外部からの不正アクセスの予防

多段にファイルアウォールを設置し、必要な通信以外を遮断。不正アクセスの検知時は、必要に応じた被害拡大の防止、調査、対策を実施します。

2. システムへのアクセス制御と操作ログの取得

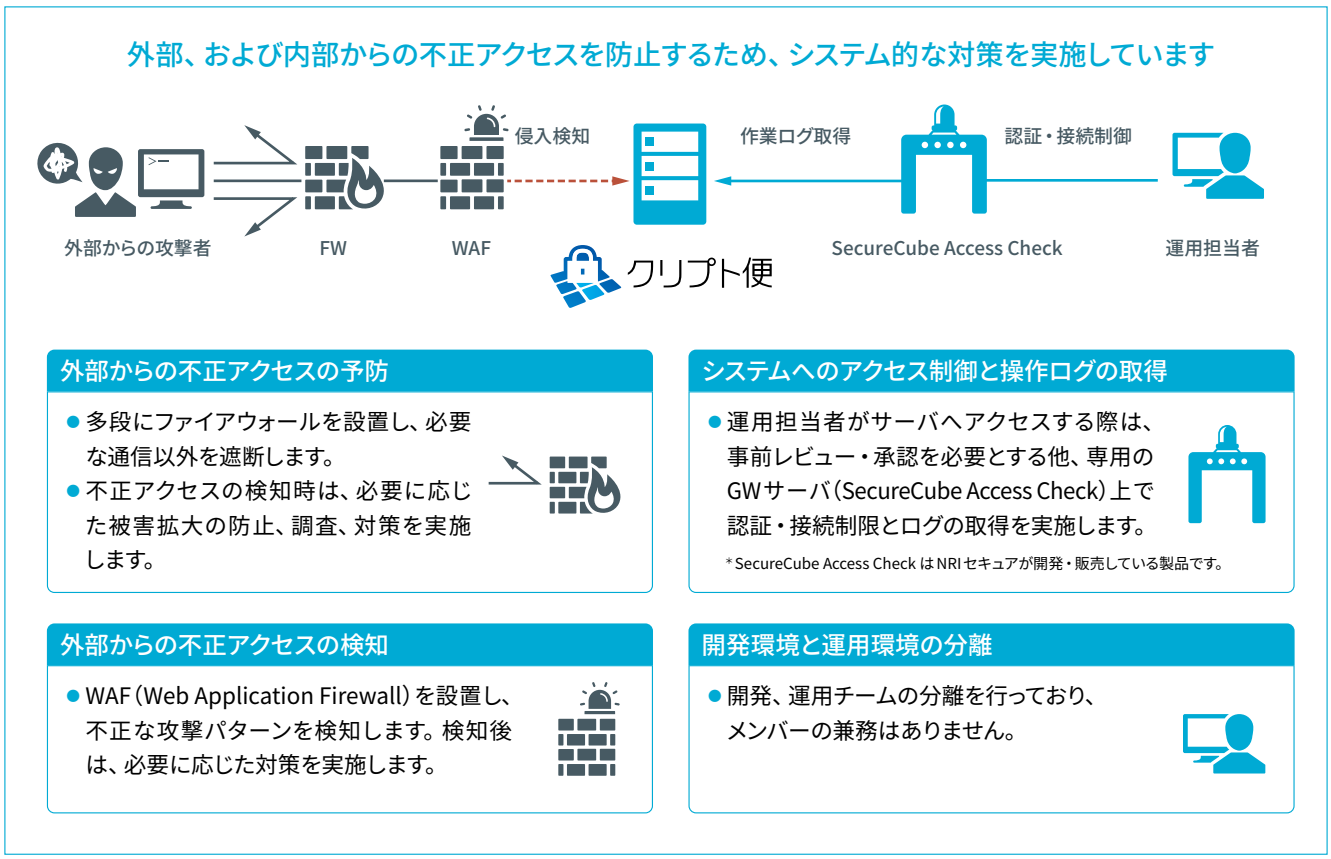
NRIセキュアテクノロジーズ社の運用担当者がサーバへアクセスする際は、事前レビュー・承認を必要とする他、専用のサーバ上で認証・接続制限とログの取得を実施します。

3. 外部からの不正アクセスの検知

WAF（Web Application Firewall）を設置し、不正な攻撃パターンを検知。検知後は、必要に応じた対策を実施します。

4. 開発環境と運用環境の分離

開発、運用チームの分離を行い、管理職以外でのメンバーの兼務はありません。



3-3. よくある質問

Q. クリプト便の利用は、個人情報の第三者提供・委託、マイナンバーの委託には該当しますか？

A. クリプト便の利用は個人情報の第三者提供・委託、マイナンバーの委託には該当しないと考えられます。

「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」及び「（別冊）金融業務における特定個人情報の適正な取扱いに関するガイドライン」に関するQ&Aでは、クラウドサービス提供事業者が個人番号をその内容に含む電子データを取り扱わないこととなっている場合、番号法上の「委託」には該当しないとされています。

「クラウドサービス事業者が個人番号をその内容に含む電子データを取り扱わないこととなっている場合」とは、契約条項に当該事業者がサーバに保存された個人データを取り扱わない旨が定められており、適切にアクセス制御を行っている場合を差し、クリプト便は約款で「当社がクリプト便サーバ上に保管されたファイル内容を閲覧することはありません」としています。また、個人データを取り扱わないとしていても、自ら果たすべき安全管理措置の一環として、適切な安全管理措置は講じています。これと同様の理由で、クリプト便の利用はマイナンバーの委託には該当しないと考えられます。

NRIセキュアテクノロジーズが実施する安全管理措置の一例

物理的安全管理措置

特定個人情報等を取り扱う区域の管理	対象外	特定個人情報を取り扱う事務はないため、取扱区域は設置していない。尚、国内データセンター内にて情報システムを管理している。
機器及び電子媒体等の盗難等の防止	○	管理区域は何重にも施錠され、容易にアクセス不可能。また、持出には申請が必要となっている。加えて、特定個人情報は取扱い区域に持出せない。
電子媒体を持ち出す場合の漏えい等の防止	対象外	特定個人情報が記録された媒体を持ち出す業務はない。
個人番号の削除、機器及び電子媒体等の廃棄	○	媒体破棄の場合には、破棄した記録は書面で管理される。個人番号の削除については、システムで自動的に削除を実施し、ログに削除された事が記録される。

技術的安全管理措置

限定された担当者のみにアクセス制限	○	個人番号関係・利用事務は業務内容に存在しない。暗号化された状態のデータにアクセスする事のみ可能。その場合においては、適切に制御が行われ、ログが保存された上で監査される。
アクセス者の識別と認証	○	本番環境へのアクセスには申請が必要であり、アクセスできる者は最低限に絞られている。
外部からの不正アクセス等の防止	○	IDS/WAF/FW といったセキュリティ機器や、アプリケーションに対するアセスの実施・ウィルスチェックソフトの導入により、不正アクセスや不正ソフトウェアからの保護を実施している。
情報漏えい等の防止	○	SSL/TLS による暗号化を実施し、通信経路の保護を実施している。また、オプションを契約頂ければ、専用線で顧客システムとつなぐ事も可能としている。

まとめ

個人情報保護委員会が定めた『特定個人情報の適正な取扱いに関するガイドライン（事業者編）』では、マイナンバーの受け渡しにおいて特定個人情報の安全管理措置が適切に講じられるよう、当該従業者に対する必要かつ適切な監督を行わなければならないとしています。マイナンバーの受け渡しに便利かつ安価な手段はいろいろありますが、こうしたガイドラインの基準に照らして適切に評価していく必要があります。

NRI セキュアテクノロジーズの「**クリプト便サービス**」は、親しみやすいメールライクな操作感と高セキュリティのファイル送受信を可能にするサービスであり、各種法令上の「委託」に該当することなくマイナンバーを含む「特定個人情報」をアップロードできます。監査部門からの厳しい外部委託ルールが課されるような場合でも、数多くの厳格な安全管理措置に対するチェック項目に適合しています。

また、以下の2つの理由から、コストのかかる委託先監査の必要なくご導入いただけます。

- 通信手段を提供しているにすぎないことから、個人番号関係事務又は個人番号利用事務の委託には該当しない。
- お客様が送受信される電子データを、弊社の担当者が閲覧・編集することができない仕様になっており、マイナンバーを取り扱わない運用になっており、約款上もその旨を明記している。

サービス開始から20年以上、現在もご契約企業の約半数を占める金融機関の要求水準に応え続け、「誤送信防止」「不正防止」「監査対策」などのセキュリティ機能を使い勝手と両立させてきたクリプト便サービスを、マイナンバーの安心安全な受け渡しにご活用ください。

マイナンバー収集ガイドブック

法人が使える
マイナンバー受け渡し手段とは？

NRIセキュアテクノロジーズ株式会社

〒100-0004 東京都千代田区大手町1-7-2 東京サンケイビル
www.nri-secure.co.jp