クリプト便

情報漏えいを防ぐために

ユースケースに学ぶ
ファイルの安全な受け渡しハンドブック

ファイル受け渡しリスクと解決方法を解説！

NRI SECURE

情報漏えいを防ぐために

ユースケースに学ぶ
ファイルの安全な受け渡しハンドブック

目　次

はじめに 3

1. ファイルの受け渡しに潜むリスク 4

1-1. リスク①「うっかり」を誘引するメールの利用 5

1-2. リスク② 無料サービスの安易な利用 6

1-3. リスク③マイナンバーの間違った取り扱い 7

1-4. セキュアなファイル転送サービスの選択 8

2. 課題別に見るユースケース 9

2-1. 利便性とセキュリティの両立に課題 10

2-2. 郵送や宅配便の不確実性や作業負担が課題 11

2-3. メールの誤送信リスクや大容量ファイルの送付が課題 12

2-4. 部門間のファイル交換に監査面の課題 13

2-5. 銀行の厳しいセキュリティ要件に適したソリューションを模索 14

2-6. その他のユースケース 15

〈参考〉なぜ「比較表」で選んではいけないのか？ 16

クリプト便

はじめに

急速なテクノロジーの進展を背景に、企業が取り扱うデータの多様化、大容量化が進んでいます。「メールで送れないような大容量ファイルは、オンラインストレージやファイル転送サービスを使ってやりとりする」という方は少なくないでしょう。オンラインストレージやファイル転送サービスは、一定容量までは無料で使えるものも多く、ドラッグ&ドロップで簡単に送信できたり、送信側も受信側もユーザー登録が不要だったり、スマートフォンに対応していたりと、その手軽さからビジネスシーンでも多用される傾向にあります。

確かに、情報伝達にもスピード感が求められる時代においては、手間とコストをかけずにスピーディーにやりとりできるのは大きなメリットです。しかし、セキュリティ面ではどうでしょうか？ 残念ながら必要なセキュリティ要件を満たさないものも多く、安心安全とは言い難い状況にあります。

NRI セキュアテクノロジーズが提供する「**クリプト便**」は、インターネットを介して安全かつ確実に電子ファイルの交換が行えるサービスです。セキュリティ専門家が開発・運用を行い、暗号化技術・堅牢な国内データセンター、誤送信防止対策など、20 年以上に渡りサービスを提供・改善を続けたノウハウがあります。「銀行」「証券」「保険」業界が利用者全体の 4 割を占めているのは、厳しいセキュリティ要件をクリアした証でもあります。

本冊子では、改めてファイルの安全な受け渡しについて考えると共に、実際の事例を通じて課題解決のアプローチをご紹介します。社内に潜むリスクに目を向けるきっかけとして、また、ファイル転送・共有サービス選びの一助としてお役立ていただければ幸いです。

1

ファイルの受け渡しに潜むリスク

多額の賠償金の支払いや業務の停止、企業の信頼損失につながる情報漏えい事故。その多くは、誤操作や記録媒体（DVD 等）の紛失などの人的ミスが原因です。ファイルを暗号化する、第三者チェックを入れる、台帳で管理するなど、どんなに厳格なルールを設けても、人的ミスが起こる可能性をゼロにすることは困難です。

2020 年 11 月にデジタル改革担当相が内閣府の全職員に対し、文書データの送信時に使用する「パスワード付き zip ファイルを廃止する」方針を明らかにしたことはご存じでしょうか。「zip ファイルのパスワードの扱いを見ていると、セキュリティレベルを担保するための暗号化ではない」「すべての文書を zip ファイル化するのは、何でもはんこを押すのに似ている」として全廃を決めたのです。それだけ安易なファイルの受け渡しにはリスクが潜んでいるということです。

もし、まだ日常的に顧客情報や技術情報をメールで安易にやり取りしているとしたら、取り返しのつかない事態に陥る前に、できるだけ早い段階でそこに潜むリスクに目を向け、根本的な仕組みの改善を図るべきでしょう。コロナ禍でテレワークが一気に進んだことや企業が扱う情報量が年々増加していることを踏まえれば、決して軽視できない重要な問題です。メール添付、メディア郵送からの脱却へ、正しい知識をもって取り組みを進めましょう。

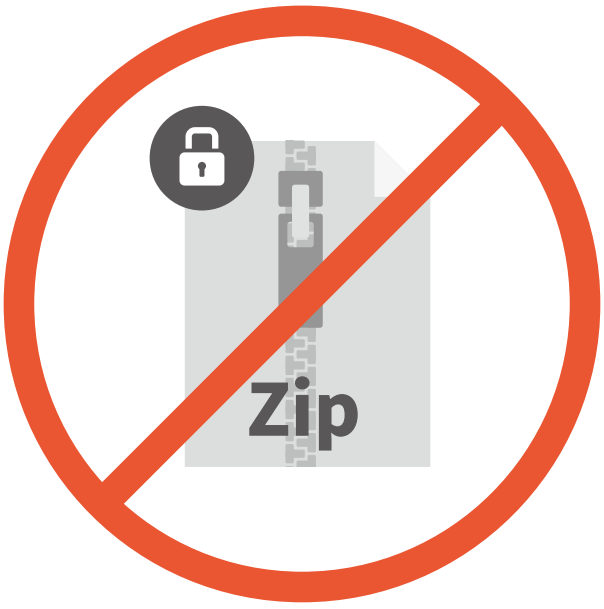
本章では、これまで当たり前に利用してきたファイルの受け渡し手段を見直すと共に、セキュアな仕組みへの改善について解説します。

1-1. リスク① 「うっかり」を誘引するメールの利用

『企業における情報セキュリティ実態調査』の2020年版[*1]によると、WEBインシデントの分野において、日本国内で「過去1年間で発生した事件・事故」の1位となったのは「電子メール、FAX、郵便物の誤送信・誤配送」です。継続的に行われているこの調査で、この順位は例年大きく変動しません。

メールで誤送信が多い原因の1つは、機密性の高いビジネス上のやり取りから、連絡や情報共有を目的としたもの、さらには宣伝・広告を目的とした配信まで、セキュリティレベルの異なるメールが受信トレイに並ぶことで、ミスを誘引しやすい構造になっていることです。また、ひとたび誤送信をしてしまったら「後の祭り」です。簡単に機密情報を送信できる環境でありながら、ミスを起こしたら取り返しがつかない状況は、大きなリスクに他なりません。

対策として添付するファイルを暗号化した場合も、簡単に復号化できる程度の暗号化では意味がありません。また、添付ファイル送信直後のメールでパスワードを連絡しても、盗聴される可能性が高まるだけです。昨今は、政府や企業でメール添付時の**「パスワード付きzipファイル」を廃止**し、送信のみでなく受信も拒否する動きが見られます。これらの理由から、保護すべき機密情報は、メールではなくセキュリティ対策が整った専門のサービスを活用することが、リスク低減に効果的だと言えます。機密情報には相応の受け渡し手段を用意することで、ユーザーに対して注意喚起を促すことにもつながります。



[*1] NRIセキュアテクノロジーズ株式会社「NRI Secure Insight 2020 企業における情報セキュリティ実態調査（2020年）」

1-2. リスク② 無料サービスの安易な利用

そもそも、無料サービスを使うのはアリなのか？ナシなのか？は誰もが気になるところでしょう。無料で便利に使える個人向けサービスがあるにもかかわらず、わざわざ有料の法人向けサービスを選ぶ意味はあるのでしょうか。結論から言えば選ぶ意味は「**あります**」。無料サービスの利用を手放しで推奨できないのは、次のようなリスクが考えられるからです。

無料サービスの利用リスク

1. 企業としての信頼性の低下

どのようなITサービスを選び取っているかによって、その企業のセキュリティ意識が問われます。取引先を含めて対外的に利用しているサービスの場合はなおさらです。たとえ機密情報ではないとしても、バナー広告がいくつも表示されるような無料サービスで業務データをやりとりするのは好ましくありません。

2. 期待すべきでない品質やサポート

一見同じように見えるサービスでも、そのサービスを裏で支える仕組みはさまざまです。ファイルの保存先となるデータセンターも、高度なセキュリティ施策に守られた堅牢なデータセンターなのか、脆弱性が散見されるデータセンターなのかは知る由もありません。また、ユーザーが万一の事態に直面しても丁寧なサポートは望めないでしょう。無料である以上、それが「あたり前」となります。

3. セキュリティレベルをコントロール不能

誰でも簡単に利用できる無料サービスは、社員が無断で外部サービスを利用する「シャドーIT」に直結します。自社の専用環境でない以上、セキュリティレベルをコントロールするのは不可能であり、万一情報漏えいが発生した場合も、「いつ」「誰が」「どこに」「何を」送ったのかを把握することはできません。把握ができないと対処することもできないため、それこそ事態は深刻です。

1-3. リスク③マイナンバーの間違った取り扱い

2015年にマイナンバー制度がスタートしてから5年以上が経過しましたが、ルールの策定が済み、社内にしっかり定着した企業がある一方で、未だ運用が確立されていない企業もあります。マイナンバーの取り扱いについては法律で厳しく定められており、「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）」も発行されていますが、具体的にどうすべきなのか分かっていない方もいるのではないでしょうか。

ガイドラインを確認すると、マイナンバーの受け渡しにふさわしくないと考えられる手段があります。ここでは各受け渡し手段をガイドラインの基準に照らして評価してみます。

マイナンバーの受け渡し手段としてアリかナシか

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です。誤送信のリスクはもちろん、暗号化の手法として多くの人が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、一般に市販されているPCパーツとツールを用いてファイルを開けることも可能なため、暗号化アルゴリズムとしては脆弱です。

2. FAX

FAXもガイドライン違反になり得ます。多くの場合、FAXは部署内で共有されているため、送信したい特定の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放置される可能性もあります。メールと同様に誤送信のリスクも否定できません。

3. 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。

1-4. セキュアなファイル転送サービスの選択

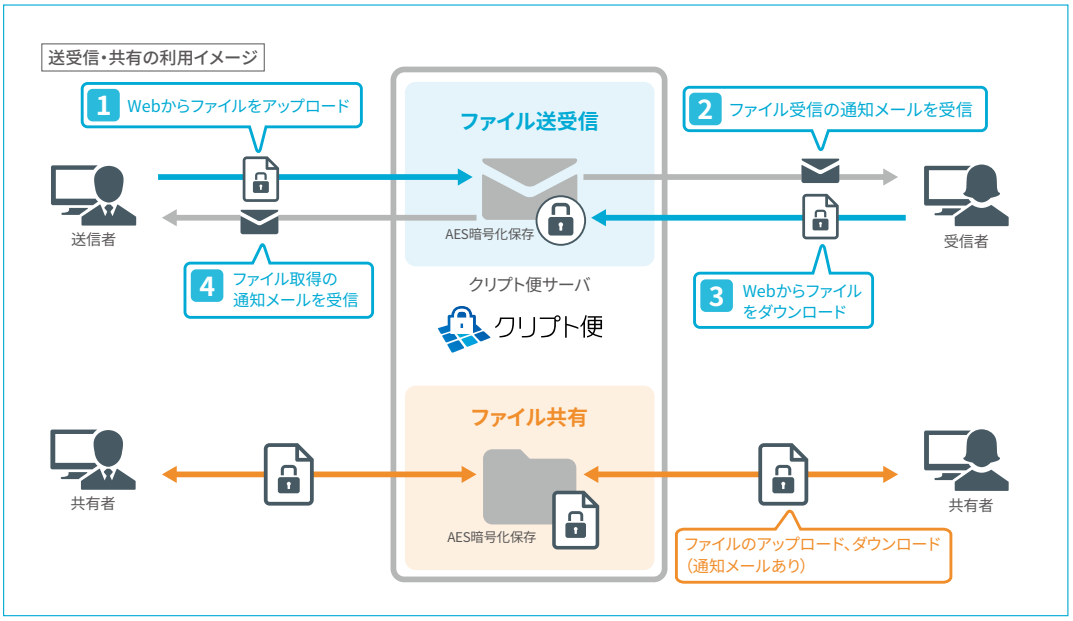
メールやFAX、郵便書留に代わる送信手段として期待されるのが、「ファイル転送サービス」です。「郵便書留の電子化」のコンセプトで開発され、送ったデータが相手に届いたかどうかの確認も可能です。しかし、一時的とはいえ、他社のサーバーに情報を預ける仕組みであるため、安全上の懸念は当然出てきます。実際、機密情報の扱いには適さないサービスが存在することも事実ですが、高いセキュリティを実現したサービスであれば、マイナンバーをはじめとした個人情報全般の受け渡しにも適しています。

「高いセキュリティを実現したサービス」を見極めるポイントを3つ記載します。

1. 通信経路の暗号化／ファイルの暗号化（AES256等）がされていること
2. 上長承認やファイルの自動削除といったセキュリティ設定がユーザーに対して強制できること
3. セキュリティチェックシートや実査などの監査に対応可能であること

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、「**クリプト便**」です。これは、セキュリティ専門企業であるNRIセキュアテクノロジーズが、金融機関での利用を想定した高水準のセキュリティレベルで提供するサービスで、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、40%を超える顧客がセキュリティ基準の高い金融関連である点も特徴です。

クリプト便の利用形態には、メーラーに近い操作でファイルを相手に届ける「ファイル送受信」に加え、双方がファイルの編集・更新が可能となる「ファイル共有」、自社システムへの組み込みにより大量なファイルの送受信を自動化する「システム連携」の3つのパターンがあります。



[*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）

2

課題別に見るユースケース

ユーザー間ファイル転送市場でシェアNo.1を獲得し続けているNRIセキュアテクノロジーズの企業向けファイル交換サービス「**クリプト便**」。2001年の販売開始以来、多くの企業・組織で利用されており、半数近くを占める金融機関のお客様の要求水準に応えながら、「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ました。こうした高度なセキュリティを重視した設計思想に共感いただいたお客様を中心に、現在も様々なビジネスの現場で日々活用されています。

本章では、クリプト便を導入されたお客様の中から、様々な課題に対する解決策としての活用パターンをご紹介すると共に、選定の決め手となったポイントや導入効果をわかりやすくお伝えしていきます。金融業界に選ばれ続けてきた高いセキュリティ水準と利便性の両立が、ポイントになっていることがお分かりいただけるかと思います。

2-1. 利便性とセキュリティの両立に課題

自社開発のファイル転送サービスを利用していたIT専門会社のA社。求められたのは、5,000以上のアカウントという大規模ユーザーの利便性向上とセキュアで効率的な運用管理の両立する新しいファイル転送サービスです。

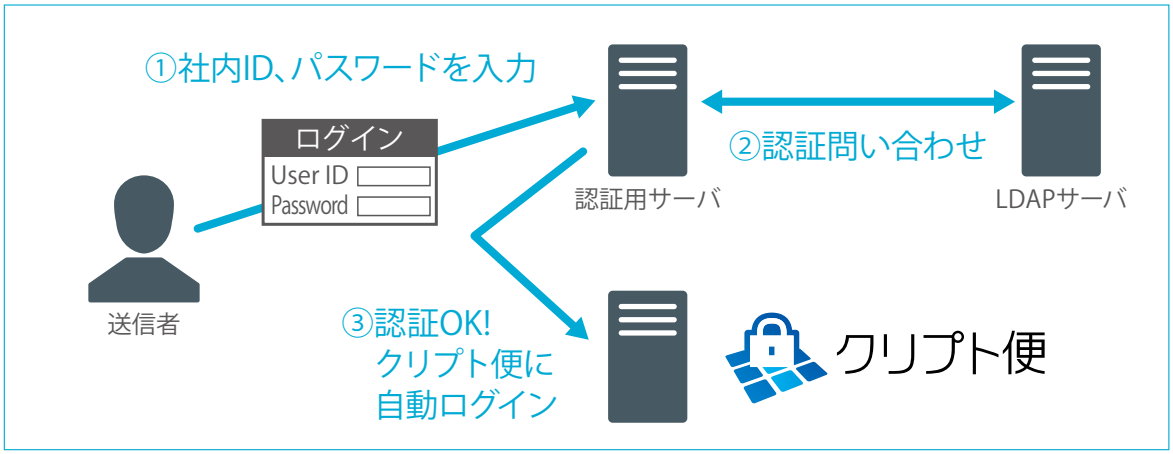
従来利用していたオンプレミスの環境は、バージョンアップを予定していたWEBブラウザに対応していない上に、ファイル容量の上限が100MBまでという制約がありました。そこでA社は、安全性、利便性、保守性の3つを主要な評価ポイントとして複数サービスを検討。すべてをクリアしていたクリプト便の採用を決めました。

大規模なユーザー移行を伴うこのプロジェクトで最も特徴的なのが、クリプト便の認証連携機能を使ったシングルサインオンの実現です。エンドユーザーは、社内認証基盤であるActive Directoryにサインオンすればシームレスにクリプト便を利用できるため、ファイル転送サービス独自のIDとパスワードを手作業で発行する手間が完全に不要になりました。また、オンプレミスからクラウドサービスへの移行により、経費の大幅な削減にも成功しています。

クリプト便の選定ポイント

- **安全性：**誤送信や盗聴の防止、ウイルス対策、ログの取得、承認機能
- **利便性：**重要データや大容量ファイル（4GB）の受送信をWEB画面で簡易に行えること
- **保守性：**クライアント環境の変化（ユーザー増減等）に迅速に対応できること

クリプト便運用イメージ



2-2. 郵送や宅配便の不確実性や作業負担が課題

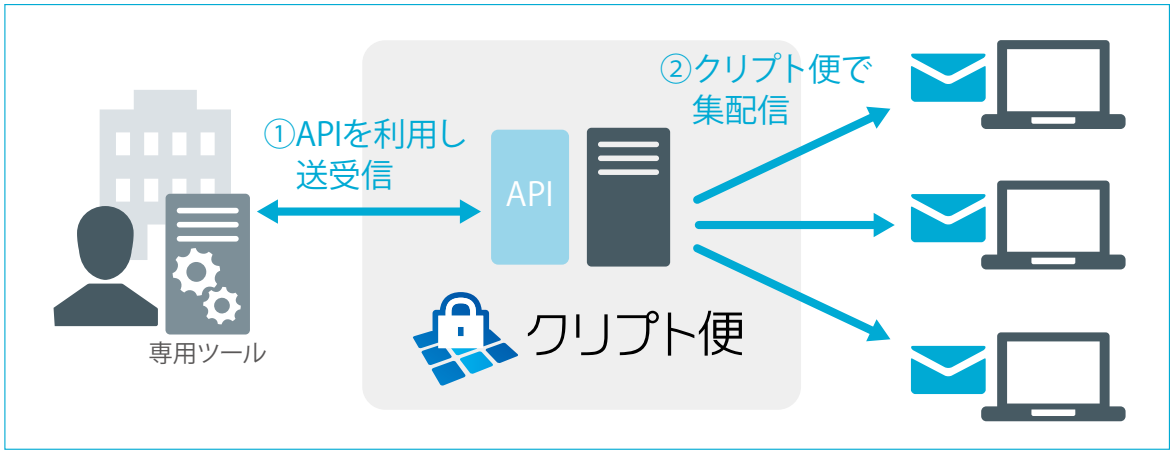
クレジットカード事業を手がけるB社の主要な業務の1つに、収納代行業務があります。取引先は1,000社以上、年間の振替件数は100万件以上に上り、ここで用いられる膨大な個人情報の受け渡しには、きわめて高いセキュリティレベルが要求されます。従来は郵送や宅急便でやり取りしていましたが、物理メディアの破損や、「着いた」「着かない」の行き違い、さらには紛失や人的ミスの可能性も否定できません。個人情報保護の重要性が高まる中、よりセキュアな方法への移行は急務だったと言えます。一方で、物理メディアの授受に伴う膨大な作業や工程の効率化、コスト削減も課題となっていました。

システム連携することで、WEBブラウザを操作せずに大量ファイルの自動送受信が行える「オートパイロットオプション」に着目したB社は、大手保険会社でも使われているこの仕組みが、最重要課題である情報セキュリティの強化に有効と判断。導入後は物理メディアの管理を外部委託する必要がなくなり、年間200万円のコスト圧縮が実現。また、APIを介して業務システム上のデータやファイルを直接クリプト便で自動送付することにより、郵送に比べデータ到着まで1～2日短縮されました。今後はクリプト便がPCIDSSに準拠したことを受けて、クレジットカード番号を含む機密データもクリプト便で送付予定です。

クリプト便の選定ポイント

- **安全性：**資料のダウンロード有無からデータの到着が可能
- **コスト削減：**郵送費やメディア管理コストの削減
- **省力化：**大量ファイルの一括送受信による作業の省力化

クリプト便運用イメージ



2-3. メールの誤送信リスクや大容量ファイルの送付が課題

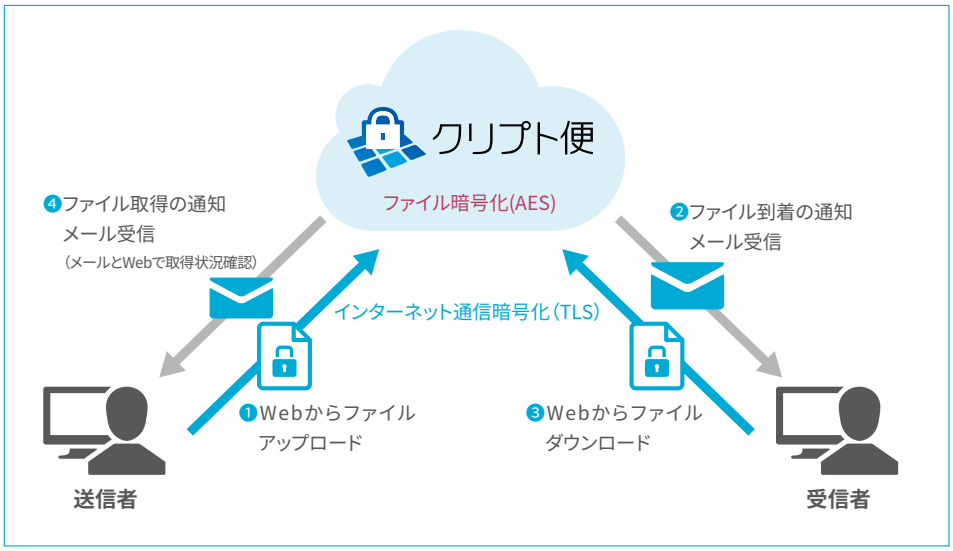
メーカーのC社では、製品へのデザイン入れ業務において、デザインのイメージ作りから、色付け、バランス調整など、完成までに加工部門との数度のやりとりが発生します。これまではデザインデータをメールの添付ファイルとして送付していましたが、昨今のデザインデータは大容量化しており、複雑なデザインになると数10MBから100MBを超えるものまであります。確実に届いたかどうか確認できない不安や、誤送信による商用デザインの外部流出というセキュリティ上の懸念も抱えていました。

上長承認機能を活用することで大容量ファイルを安全かつ確実に送受信できる上、新たなシステム開発の必要もなく比較的安価に利用できるクリプト便は、信頼性の高いシステムを求めていた同社のニーズに見事に合致。導入前は、大容量のファイルはDVDにコピーして郵送していたため、データを送り、修正を加えて戻ってくるまでに数日かかることもありましたが、クリプト便なら作成したデータをその場ですぐに送れます。作業品質を維持しながらスピードアップできるのは大きなポイントです。納期を厳守できるようになり、加工部門との信頼関係強化にも役立っています。また、同社は英語・中国語圏とやりとりすることも多く、ファイル送受信時の通知メールやWEBブラウザ上の画面が両方の言語に対応していることも業務の円滑化に貢献しています。

クリプト便の選定ポイント

- **安全性：**上長承認機能による誤送信防止
- **利便性：**大容量ファイル（4GB）を確実に送受信できる
- **汎用性：**英語・中国語に対応

クリプト便運用イメージ



2-4. 部門間のファイル交換に監査面の課題

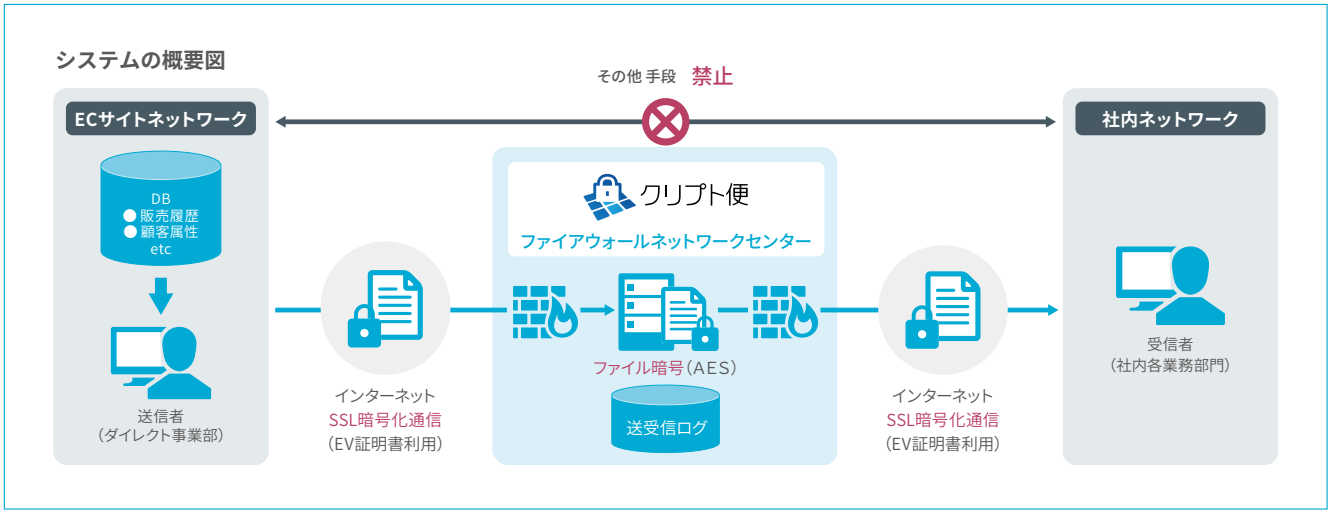
アパレル企業のＤ社のダイレクト販売部門は、指紋認証で部門全体を社内から完全に隔離するほどセキュリティを重視しており、データも業務系ネットワークとは分離したセグメントに格納し、外部に出さないポリシーを採用しています。したがって、社内の各業務部門と直接ファイルを交換できないため、暫定措置として中間サーバーを設けて必要なファイルをやり取りしていました。しかし、中間サーバー経由のファイル交換は、ネットワーク上の安全性は確保されていてもログ情報まで取得できず、監査性の面で課題が残ります。

そこで、管理者が定めたアカウント同士でのみファイル交換を許可する設定（クローズドグループ）が可能なクリプト便を採用。グローバルIP制限を掛けることで、ダイレクト販売部門のユーザーは独自のネットワークからのみアクセスを可能にしました。また、グルーバルIPで制限できない場合は、クライアント証明書による端末制限をすることで不正アクセスを防止しています。社内の各業務部門からのリクエストに対して、ECサイトから販売履歴や顧客属性などが含まれたファイルを取得し、個人が特定されないように再加工したうえで、クリプト便経由で業務部門に送信しています。また、管理者は送受信ログや実際にやり取りしたファイルの中身を確認できるため、個人情報漏えいの有無を速やかに確認できることも評価いただいています。

クリプト便の選定ポイント

- **誤送信防止**：管理者が定めた特定の相手とのみファイル交換が可能
- **アクセス制限**：グローバルIPや端末認証によるアクセス制限が可能
- **監査**：監査者はファイルの送受信ログのみでなく、実際のファイルの中身まで確認可能

クリプト便運用イメージ



2-5. 銀行の厳しいセキュリティ要件に適したソリューションを模索

E銀行では、業務統制の観点から標準化されたシステムの必要性を感じていました。また、ファイル転送に関しては2つの大きな課題がありました。1つは暗号化の問題。以前から行外宛メールの添付ファイルを自動的に暗号化ZIPにするシステムが導入されていましたが、昨今はパスワード付きZIPファイルがウィルスチェックを通せないことからZIP形式の受け取りを拒否する相手が増えています。また、もう1つの問題は大容量ファイルの安全な送信です。これまでは物理メディアにコピーして受け渡しを行っていましたが、効率が悪く、紛失のリスクもあります。

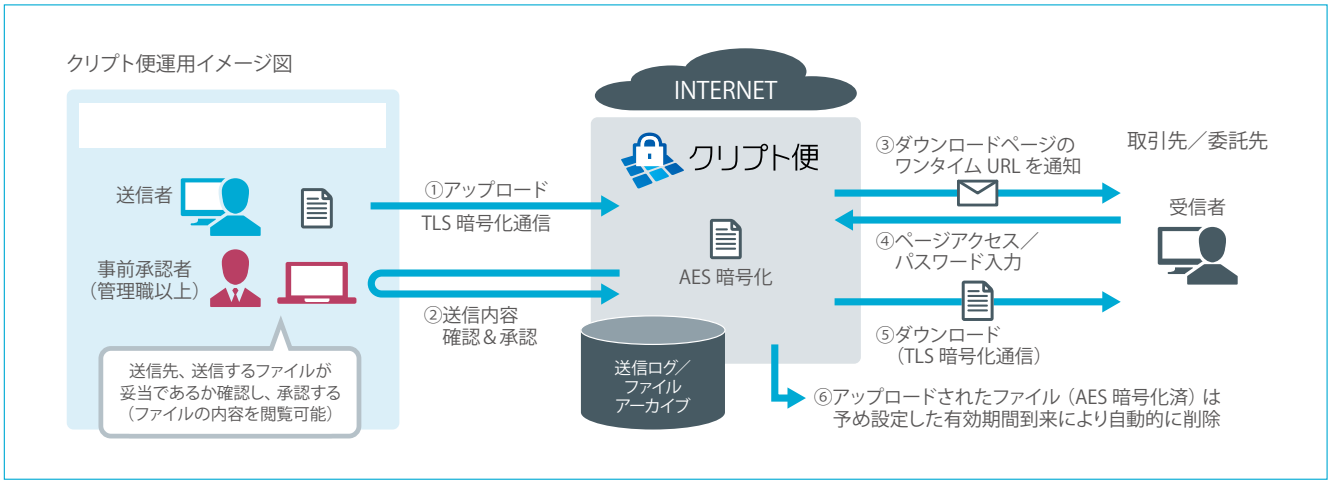
これらの課題解決に対して「内部不正による機密データの持ち出しを防げるか」「送ったファイルを長期間アーカイブして監査に対応できるか」「銀行が定めるセキュリティ要件を満たしているか」の3点を重視した結果、クリプト便の採用に至りました。

100ユーザーからスタートし、わずか9か月でユーザー数が約2倍に。大容量ファイルの送信需要が予想以上に多く、潜在的にファイル転送の悩みを抱えていた人たちのニーズにマッチしたことが伺えます。また、クリプト便はZIPファイルの送信を禁止することが作業量の削減はもちろん、信頼性の高いファイル転送サービスを同行全体で利用する統一環境を整備できたことが大きな成果です。

クリプト便の選定ポイント

- **内部不正の抑止：**ファイル送信時にダウンロードURLが相手にのみ届く
  （送信者はURLが分からないため、自宅のPCからファイル取得する等ができない）
- **監査：**送受信ログのみでなく、実際のファイルも監査者が長期間に渡って確認可能
- **セキュリティ環境：**データセンター見学等の細やかなセキュリティ仕様の確認が可能

クリプト便運用イメージ



2-6. その他のユースケース

ご紹介した5つの事例以外にも、さまざまな事業分野、さまざまな用途でクリプト便が活用されています。自社での活用を検討される際の参考資料としてお役立てください。

業界	導入前	導入後
派遣会社	派遣登録者が就業を開始する際に、対象者のマイナンバー情報の収集が必要なため、今までは郵送もしくは直接持参してもらう方法で対応していました。このため、不備があった場合は再郵送などの手間がかかっていました。	クリプト便からマイナンバー提出者のメールアドレスに空メールを送り、メールを受信した対象者は、マイナンバーカードや通知カードの写真を添付して返信するのみ。電子版往復はがきのような感覚で利用でき、素早い回収が可能になりました。
医療機関	機密性の高い患者情報のやり取りにFAXを利用していたため、誤送信のリスクが指摘されていました。	クリプト便のファイル共有機能を利用し、あらかじめ登録したアカウント内でのみファイルのやり取りを可能にしました。また、上長承認機能を利用することで自社・他社ともに承認がないとアップロードできない仕組みとすることで誤ったファイルの共有を未然に回避しています。
地方銀行	リモートワーク時に機密性の高いファイルを個人の端末にダウンロードすることはセキュリティ上望ましくありませんでした。	クリプト便のファイル共有機能が任意の日数が経過した後にファイルが自動削除される点が評価されました。また、端末認証機能により、私用のデバイスからのアクセスを制限することで、不正なダウンロードを防いでいます。
セキュリティ会社	機密情報を送付する上で、相手側に対してもログイン元を制限した厳重な管理を徹底する必要がありました。	クリプト便の端末認証機能により、グローバルIPによる制御ができない相手に対しても、ログイン端末を制限することでセキュリティ強化を実現することができました。
特許事務所	外国における知的財産の出願・権利化業務においては、各国の特許事務所との間で明細書、要約書、委任状、翻訳文など多数の書類が必要になります。	世界中のどこからでもアクセスでき、日本語・英語・中国語の3か国語に対応しているクリプト便で、外国の取引先との安全なファイル転送を実現しました。

〈参考〉なぜ「比較表」で選んではいけないのか？

市場にはファイル転送サービスがあふれています。無料で利用できるものも少なくありません。しかし、機密性の高い情報の取り扱いに適したファイル転送サービスを求めるなら、その選び方にも注意が必要です。最後に、セキュリティ重視でサービスを選ぶ際のポイントをお伝えします。

製品やサービスを選定する際に頼りがちなのが「比較表」です。一度に複数の製品やサービスを把握できる比較表は確かに便利です。しかし、安易な利用は失敗につながりかねません。なぜなら、「〇」や「×」でシンプルに表せない品質が不可視化されてしまうだけでなく、必ずしもニーズに合った比較項目が抽出できているとは限らないからです。

特に、実際の利用シーンへの適合度合いやセキュリティレベルで優劣のつくクラウドサービスの選定においては、単に機能だけを並べた比較表だけでは不十分です。セキュリティの前提は、「機能がたくさんあればよい」「大は小を兼ねる」ではなく、「**Need to Know の原則**」。機能があり過ぎることでユーザーの操作ミスを誘発し、悪意のある者に隙を与えてしまうこともあります。不要な機能には「×」が付いているほうが、セキュリティ的には評価が高い場合もあるのです。

セキュリティを主眼にサービスを選ぶ際は、提供企業がどれだけセキュリティ対策に投資しているか、その企業の従業員一人ひとりのセキュリティに対する姿勢も判断材料に入れる必要があります。これらは自社独自のチェックリストを作成することで可視化できます。PCIDSS などの基準に加え、FISC（金融情報システムセンター）の安全対策、システム監査の指標などを参考に、必要なものを抜粋していくとよいでしょう。

NRI SECURE

情報漏えいを防ぐために

ユースケースに学ぶ ファイルの安全な 受け渡しハンドブック

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