



クリプト便紹介セミナー

～デモを交えて機能やユースケースを詳しく説明～

NRIセキュアテクノロジーズ株式会社
ファイルセキュリティ事業部

* 本資料の無断での引用・転載を禁じます

本日のアジェンダ

1. クリプト便ご利用者様が増加する背景と留意点

2. クリプト便 サービス概要

3. クリプト便 デモ紹介（管理者画面／ユーザ画面）

セキュリティインシデントの発生原因

電子メールの誤送信などが
毎年第1位



2021年 n=1,616 JP		2020年 n=1222 JP	
1位	25.2% 電子メール、FAX、郵便物等の誤送信・誤配送	1位	22.1%
2位	14.9% 標的型メール攻撃	2位	16.4%
3位	14.5% 情報機器・外部記憶媒体の紛失・置き忘れ・盗損	4位	13.9%
4位	11.9% マルウェア感染	3位	14.5%
5位	11.4% 社員証、業務書類等物品の紛失・置き忘れ・盗損	6位	10.3%
6位	10.6% システム設定ミス、誤操作	5位	12.2%
7位	9.0% 情報機器、電子記憶媒体、紙媒体等の盗難・紛失	7位	10.1%
8位	6.1% DoS攻撃/DDoS攻撃	9位	4.2%
9位	5.3% ランサムウェアによる金銭等の要求	8位	6.3%
new 10位	4.0% 退職者、転職者による在職時に利用していた情報の使用	ランク外	—

[事例1] 誤設定による情報漏洩

※本スライドは複数の報道情報をもとに作成し、
原因については当社想定を含んでいます

○概要

スマホアプリ会社A社にて利用しているクラウドストレージの権限の誤設定により、顧客や従業員、取引先含む最大94万人以上の個人情報がインターネット上で長い期間閲覧できる状態にあった。

○誤設定の内容

対象ファイルへの権限が「リンクを知っている全てのユーザが閲覧可能」となっていた。

○原因(想定)

権限の設定が確かなものかの確認が不十分、もしくは設定の存在自体を意識していなかった。

A社

①ファイルをアップロード

従業員



ファイルの閲覧権限
→ 誰でも閲覧可

A社公認
クラウドストレージ

②閲覧可能



リンク(URL)を
知っているユーザ

[事例2] オンラインストレージを悪用した情報漏洩

※本スライドは複数の報道情報をもとに作成し、原因については当社想定を含んでいます

○概要

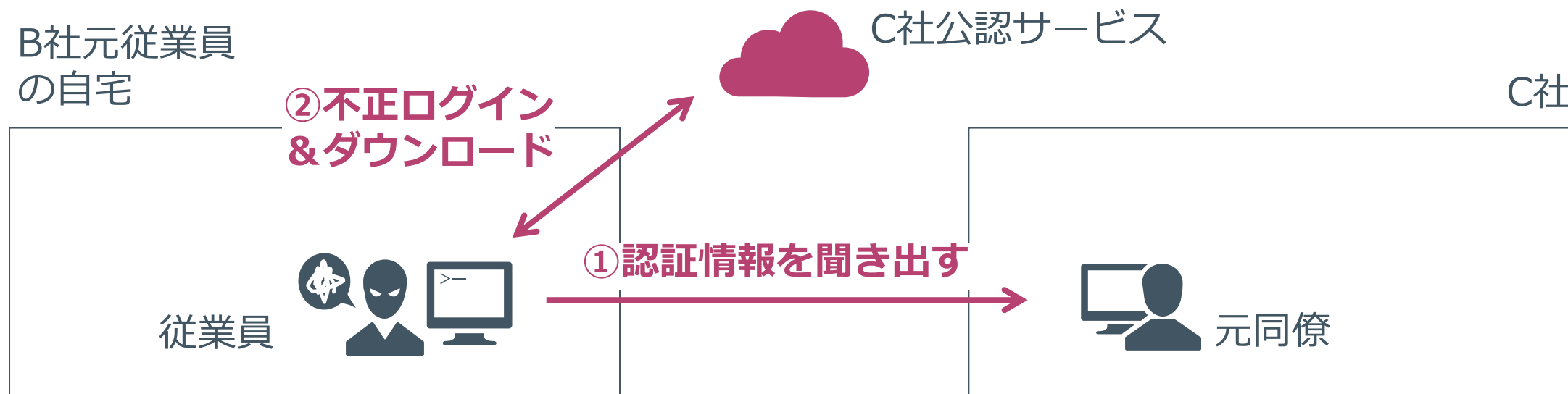
総合商社B社の元従業員が、前職の総合商社C社のオンラインストレージ環境に自宅PCからログインし、約3万7千件のファイルを不正にダウンロード。営業秘密も含まれていた。

○手法

元同僚に認証情報を聞き出して不正ログイン

○原因(想定)

オンラインストレージのログイン制御が不適切
(ソーシャル・エンジニアリング対策も不足)



[事例3] オンラインストレージを悪用した情報漏洩

※本スライドは複数の報道情報をもとに作成し、原因については当社想定を含んでいます

○概要

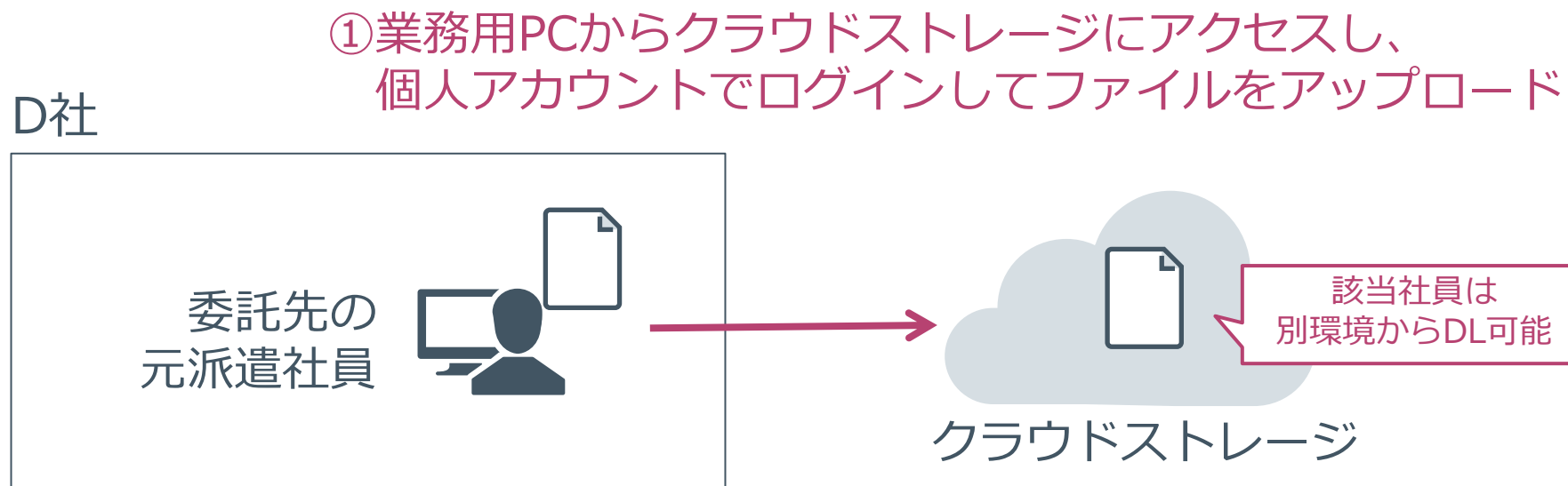
通信会社D社の業務委託先の元派遣社員が、業務使用PCから個人契約しているクラウドストレージにログインし、約596万件の個人情報を含むファイルをアップロードすることで情報を持ち出した。

○手法

個人アカウントでログインしてアップロード

○原因(想定)

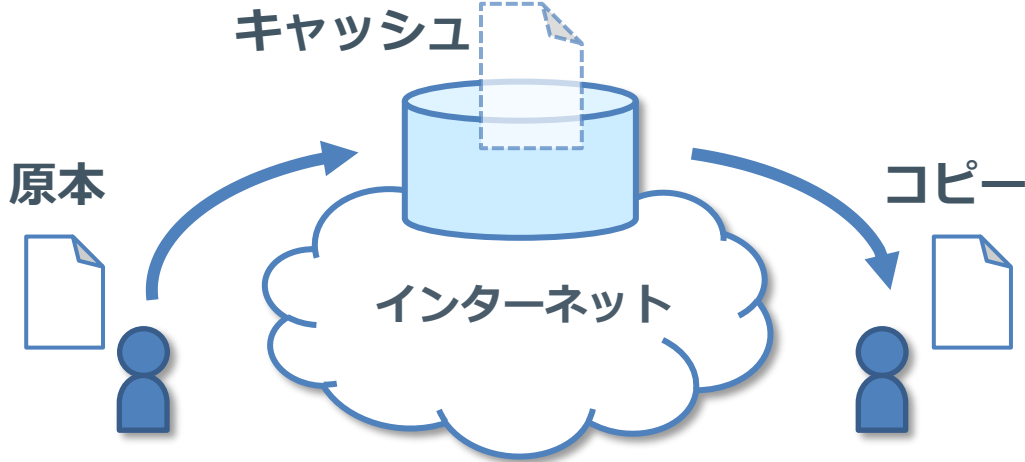
個人アカウント対策が不十分



/1/

ファイル転送/共有サービスの選び方

「ファイル転送サービス」と「ファイル共有サービス」の違いとは？

比較観点	ファイル転送サービス (クラウド上のメールサーバ)	ファイル共有サービス (クラウド上のファイルサーバ)
保管に対する考え方	なるべく クラウド上にファイルを置いておきたくない	なるべく クラウド上にファイルを置いておきたい
ファイルの原本・最新版	送信者、受信者のPC	クラウドサービス上
やり取りの期間	その場限りのやり取り	継続したやり取り
得意な機能	- ファイル受け渡し管理（受信状況確認） 誤送信防止（承認ワークフロー） - 送受信業務の自動化	- 大量ファイルの取り扱い 複数人でのファイル更新(バージョン管理) - ファイルに対する権限設定
イメージ		

対象とするファイル・業務の特性確認

ファイル転送		ファイル共有
できればクラウドに 保管したくない	クラウドへの保管に 対する考え方	なるべくクラウドに 保管したい
不要 原本はローカルPC	バージョン管理	必要 原本はクラウド
できるだけ短く	ファイルの 保管期限	十分長く
個人情報の送信 多数の宛先とのやり取り (メールの誤送信対策)	用途例	プロジェクト資料の共有 マニュアルの公開 ストレージとしての利用



クリプト便 サービス概要

クリプト便とは

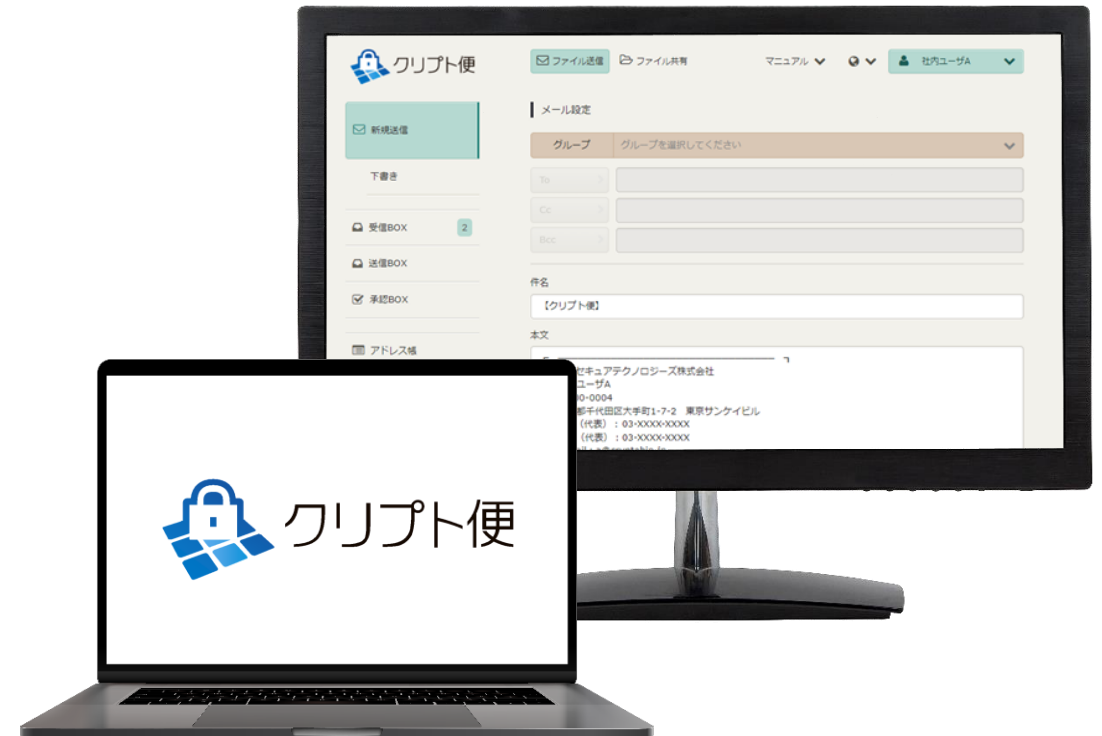
機密情報の受け渡しに特化したファイル交換サービスです。

20年以上の実績があり、公的機関や金融機関をはじめ様々な企業・団体で利用されています。

✓ 機密情報の受け渡しに特化した
安全・確実なファイル交換サービス

✓ メールライクな**ファイル送受信** ストレージライクな**ファイル共有**
ケースに応じた使い分けが可能

✓ ユーザー間ファイル転送市場ベンダー別売上シェア
13年連続No.1※



※出典：
株式会社アイ・ティ・アール
「ITR Market View：デジタルワークプレイス市場2024」
ユーザー間ファイル転送市場 売上金額シェア(2011-2023年度)

選ばれる理由

他社製品との比較において、以下3点を特にご評価いただいております。

選ばれる理由 1

人的リスクを 最小化する機能設計



暗号化やウイルスチェック等の**セキュリティ技術**だけでは回避し切れない**誤操作や悪意のある持ち出し等を防止・対策**する機能が充実。

交換相手や保存期間の制限、事前承認、送信取り消し、詳細ログ確認などを人的リスクを低減する機能を多く持ったツールです。

選ばれる理由 2

誰にでも使いやすいUI



シンプルかつ直観的なUIで「**誰にでも使いやすい**」「**業務フローを大きく変えずに使える**」といったお声をいただくことが多く、操作性も高く評価いただいています。

選ばれる理由 3

堅牢な セキュリティ環境



情報セキュリティ専門会社としての技術・ノウハウを用い、暗号化、セキュリティ診断、多段ファイアウォールなど**堅牢なセキュリティ対策を実現**。多くの金融機関に選ばれてきた実績があり、安心して選択いただいております。

第三者機関によるセキュリティ性能評価

情報セキュリティ専門企業だから実現できる堅牢なセキュリティ。第三者機関からも高い評価を得ています。

➡ ISO/IEC 27001

NRIセキュアは、ISMS（情報セキュリティマネジメントシステム）の国際規格であるISO/IEC 27001認証を全社で取得。クリプト便においても、規格にのっとった、厳格なセキュリティマネジメントを実施しています。



➡ ISO/IEC 27017 ISO/IEC 27018

クリプト便は、クラウドサービスプロバイダとしてクラウドサービスの情報セキュリティ管理に関する国際規格「ISO/IEC 27017」、および、クラウドサービスの個人情報管理に関する国際規格「ISO/IEC 27018」の認証※を取得しています。

※ クラウドサービスに関する国際規格であるISO/IEC 27017に基づくISMSクラウドセキュリティ認証(JIP-ISMS517-1.0)、およびISO/IEC 27018に基づくプライベート認証を取得。



➡ 情報セキュリティ格付け最高位「AAAis」

クリプト便の運用業務に対して、日本セキュリティ格付機構より、12年間連続で情報セキュリティ格付け最高位※の「AAAis」を付与されています。

※ 2024年1月現在サービス最高レベルの格付け



➡ PCI DSS

クリプト便は、サービスプロバイダーとしてPCI DSS※に準拠したことを示す認証を取得。従来、電子記録媒体の郵送やFAXなどで社外とやり取りしていたクレジットカード番号を含む重要情報も、クリプト便で取り扱うことが可能です。

※ PCI DSS : Payment Card Industry Data Security Standardsの略称。クレジットカード情報の漏えいを防止するために、策定されたクレジットカード業界における国際的なセキュリティ基準。



➡ ISMAPサービスリスト

クリプト便は、2023年12月25日に「政府情報システムのためのセキュリティ評価制度（以下「ISMAP（Information system Security Management and Assessment Program : イスマップ）」）において安全性の高さが認定され、ISMAPクラウドサービスリストに登録されました。

ご参考 | FISC安全管理対策基準の適合度調査

金融機関様向けにFISCが定める基準へのサービス適合度をまとめた資料はご用意があります。
お客様独自のチェックシートへの記入も対応可能です。

FISC安全管理対策基準の適合度調査（クリプト便）

2022年5月30日

NRIセキュアテクノロジーズ株式会社
ソフトウェア第一事業本部

※本書は、金融情報システムセンターによる「金融機関等コンピュータシステムの安全対策管理基準 第9版(令和3年12月版)」を基準として
クリプト便サービスの設備・運用の対応状況を記したものです。
本書に記述した対応状況は、クリプト便サービスに関するものであり、各措置等の具体的な実施内容は、弊社(NRIセキュア)基準によります。

項目	基準大項目	基準中項目	基準小項目	適合度	対応状況
統1	1 内部の統制	(1) 方針・計画	統1 システムの安全対策に係る重要事項を定めた規程を整備すること。 システムの安全対策を適切に実施するための組織体制、関係者の役割及び管理すべき事項を明確にした規程を策定すること。また、環境変化に対応するため、策定した規程を適宜改訂すること。	○	基本方針及び各種手順書を整備、または適宜改訂しております。
統2	1 内部の統制	(1) 方針・計画	統2 中長期的視点に立ったシステムの企画・開発・運用に関する計画を策定すること。 有効なシステムを長期的かつ安定的に維持するため、中長期的視点に立って、システムの企画・開発・運用に関する計画を策定すること。	○	計画を策定しております。
統3	1 内部の統制	(1) 方針・計画	統3 システム開発計画は中長期システム計画との整合性を確保するとともに、承認を得ること。 コンピュータシステム全体の信頼性向上のため、システム開発計画は、中長期システム計画と整合性がとれており、かつ内外の技術調査を実施していること。また開発責任者（システムを企画、開発する部門の長）の承認を得ていること。	○	責任者の承認済みです。
統4	1 内部の統制	(2) 組織体制	統4 セキュリティ管理体制を整備すること。 セキュリティ管理を適切に行うため、セキュリティ管理の責任者を定め、その職務範囲と権限及び責任について定めること。	○	責任者を定め、運用しております。
統5	1 内部の統制	(2) 組織体制	統5 サイバー攻撃対応態勢を整備すること。 サイバー攻撃への対応のため、サイバー攻撃対応態勢を整備するとともに、手口の高度化及び巧妙化にあわせて見直すこと。	○	社内専門の部署を有しております。
統6	1 内部の統制	(2) 組織体制	統6 システム管理体制を整備すること。 システムの安全かつ円滑な運用と不正防止のため、システムの管理手順を定め、管理体制を整備すること。	○	管理手順に則り、整備しております。
統7	1 内部の統制	(2) 組織体制	統7 データ管理体制を整備すること。 データの安全かつ円滑な運用と不正防止のため、データ管理手順を定め、管理体制を整備すること。	○	管理手順に則り、整備しております。
統8	1 内部の統制	(2) 組織体制	統8 ネットワーク管理体制を整備すること。 コンピュータネットワークの適切かつ効率的な運用と不正アクセス等の防止のため、ネットワークの管理手順を定め、管理体制を整備すること。	○	管理手順に則り、整備しております。
統9	1 内部の統制	(2) 組織体制	統9 業務組織を整備すること。 コンピュータシステムに係る業務を円滑かつ適正に運営するとともに、不正を防止するため、業務組織並びに責任及び権限を明確にし、相互牽制体制を整備すること。	○	クリプト便では開発・運用は分離・分担しております。
統10	1 内部の統制	(2) 組織体制	統10 防災組織を整備すること。 災害の予防及び被害軽減のため、防災組織を整備し、責任者を明確にすること。	○	責任者を定め、運用しております。
統11	1 内部の統制	(2) 組織体制	統11 防犯組織を整備すること。 犯罪を防止するため、防犯組織を整備し、責任者を明確にすること。	○	責任者を定め、運用しております。
統12	1 内部の統制	(2) 組織体制	統12 各種業務の規程を整備すること。 システムを円滑かつ適正に運用、管理するため、業務の各組織における責任及び権限を明確にした規程を整備すること。	○	防災、防犯、業務の規程を整備しております。
統13	1 内部の統制	(3) 管理状況の評価	統13 セキュリティ遵守状況を評価すること。 コンピュータシステムを円滑かつ適正に運用するため、セキュリティポリシー、セキュリティスタンダード等の規程に定められた事項の遵守状況を検証し、金銭職員（外部要員を含む）のセキュリティポリシーに対する意識及びセキュリティレベルの向上を図ること。	○	セキュリティレベル向上のため定期的にeラーニングを行い、達成状況をチェックしております。

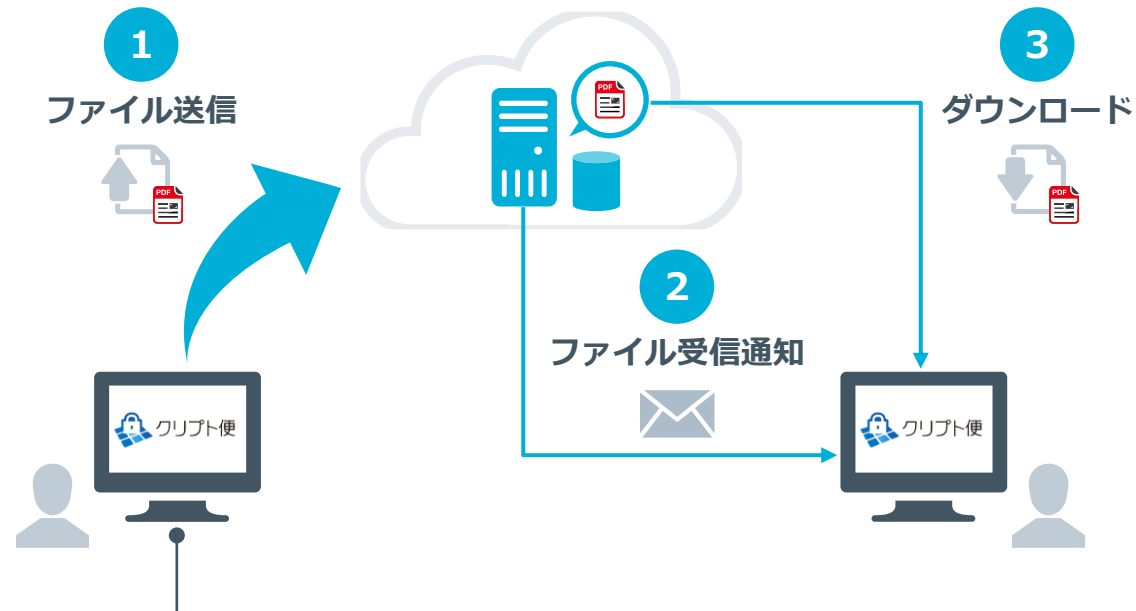
機能紹介

クリプト便の2つの基本機能

クリプト便には大きく分けて「ファイル送受信」「ファイル共有」の2つの機能があります。

ファイル送受信

最大25日間保管



メッセージにファイルを添付して送信

- ・ メール感覚で大容量ファイルを社外に安全に送信
- ・ ファイルはセキュアなクラウド環境に保管。短期間で自動削除

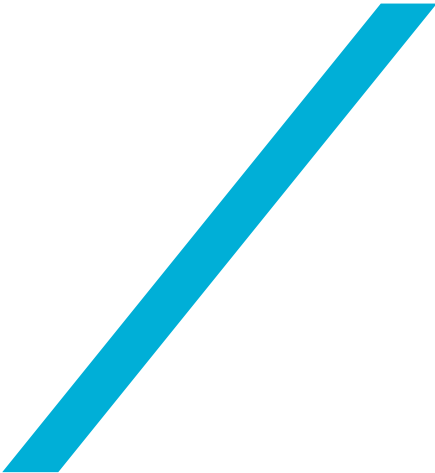
ファイル共有

無期限保管 ※自動削除設定可



共有グループにファイルをアップロード

- ・ オンラインストレージ感覚で大容量ファイルを社外と安全に共有
- ・ ファイルはセキュアなクラウド環境に保管。中長期で共有可能



機能紹介 - ファイル送受信

画面構成

シンプルでわかりやすい画面構成で、どなたでも簡単にご利用いただけます。

送受信メニューの選択

送信・共有の切替

利用グループの選択

件名・メッセージの入力

送信先の選択

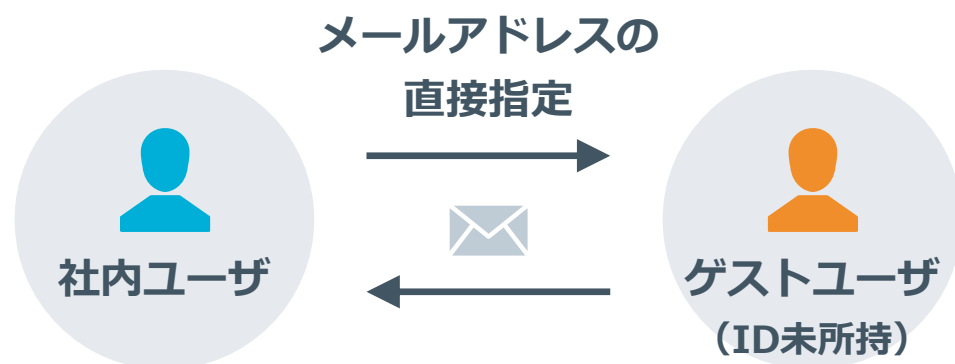
ファイルの添付

パスワードの設定

利用ケースに応じた交換相手の制御

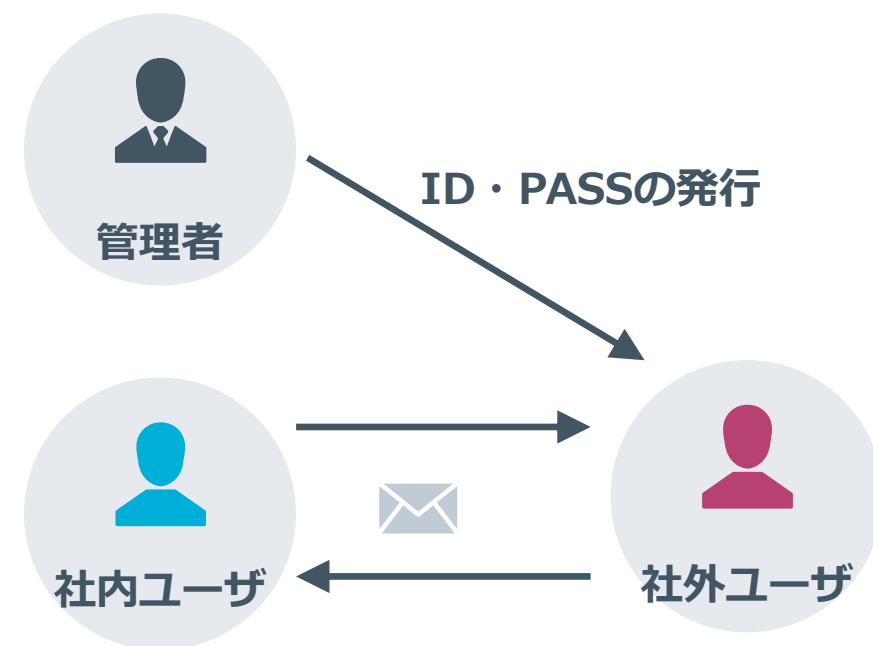
ファイル送受信では、利用ケースに応じて、ファイルの交換相手を自由に指定することも登録ユーザーに限定することも可能です。

未登録ユーザーとの自由度の高い送受信



- 都度任意のメールアドレスを指定してファイル送受信を実施します
- 様々な相手と自由度高く送受信を行いたい場合に適しています

登録ユーザーに限定した安全な送受信



- 交換相手にアカウントを付与してファイル送受信を実施します
- ユーザー登録された人物以外との送受信を禁止し、厳格な情報管理を行う場合に適しています

交換相手を制御するグループ機能



= グループ



= ゲストユーザ



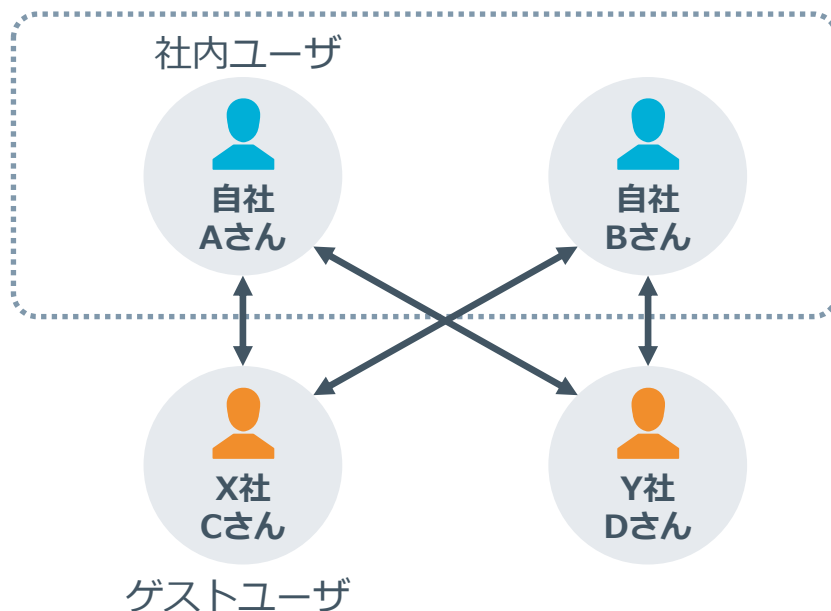
= 社内ユーザ



= 社外ユーザ

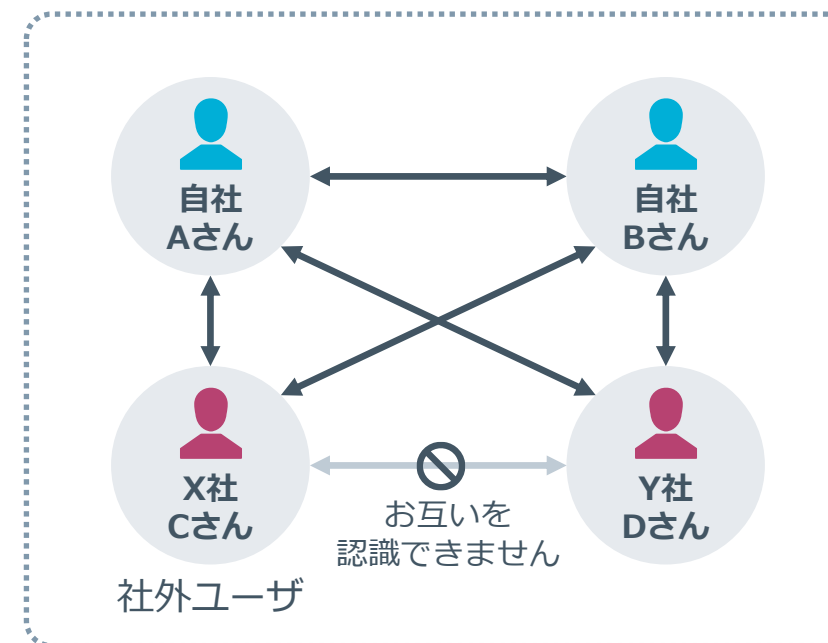
クリプト便を利用する社内・社外ユーザは必ずグループに所属し、所属グループの種別によって交換相手が制御されます。交換相手を自由に指定する場合はオープングループに、登録ユーザに限定する場合はクローズドグループに所属します。

オープングループ

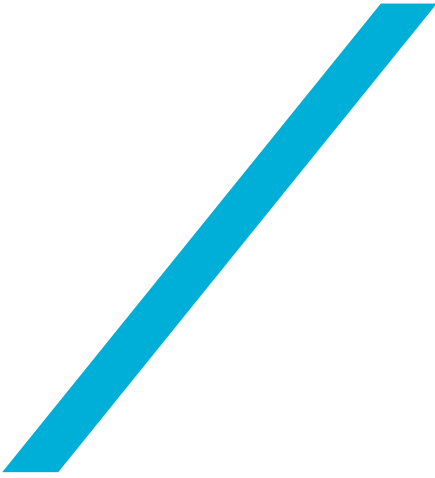


交換相手を任意指定できる
自由度の高いグループとして運用

クローズドグループ



同一グループに登録された
複数社のユーザに限定して運用



機能紹介 - ファイル共有

画面構成

シンプルでわかりやすい画面構成でどなたでも簡単にご利用いただけます。

The screenshot shows the Kryptobon web interface for file sharing. The layout is divided into several sections:

- Header:** Includes the Kryptobon logo, navigation tabs for 'ファイル送信' (File Send) and 'ファイル共有' (File Share), and user information for '社内ユーザ1'.
- Left Sidebar:** Contains a 'グループの切替' (Group Switch) section with options like 'ファイル共有', 'クローズドグループ1', 'コラボボックス', '回収ボックス', '揭示ボックス', and 'オープングループ1'. Below this is a 'ボックス一覧表示' (Box List Display) section with a search bar and a list of boxes.
- Main Content Area:** Features a search bar, a '一括ダウンロード' (Bulk Download) button, and a table of files and folders. The table columns are '名前' (Name), '更新日時' (Update Time), and 'サイズ' (Size). The table lists folders like 'アップロードしたフォルダ', 'フォルダ①-1', and 'フォルダ①-2', and files like '202310Excel.xlsx', '202310PDF.pdf', and '202310Word.docx'.
- Right Sidebar:** Contains a 'コラボボックス' (Collaboration Box) section with information about the box, storage usage, and settings for automatic deletion, approval, and labels.

Callouts and their descriptions:

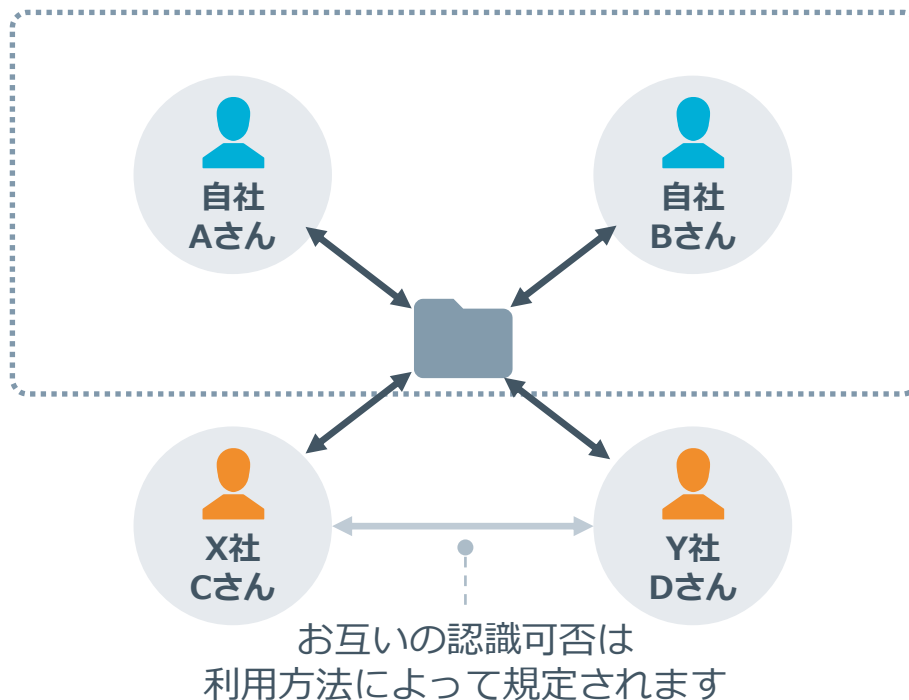
- 送信・共有の切替:** Points to the navigation tabs at the top.
- 共有ファイル/フォルダの表示:** Points to the main content area showing the list of files and folders.
- 一括ダウンロード:** Points to the '一括ダウンロード' button in the main content area.
- ボックス一覧表示:** Points to the box list section in the left sidebar.
 - ボックス=ファイル置き場
 - ボックス毎に共有相手を管理可能
- ボックス選択時 → ボックス情報、公開先の表示**
- ファイル選択時 → ファイル情報の表示**

グループの使い分け例

 = 社内ユーザ
  = ゲストユーザ
  = 社外ユーザ

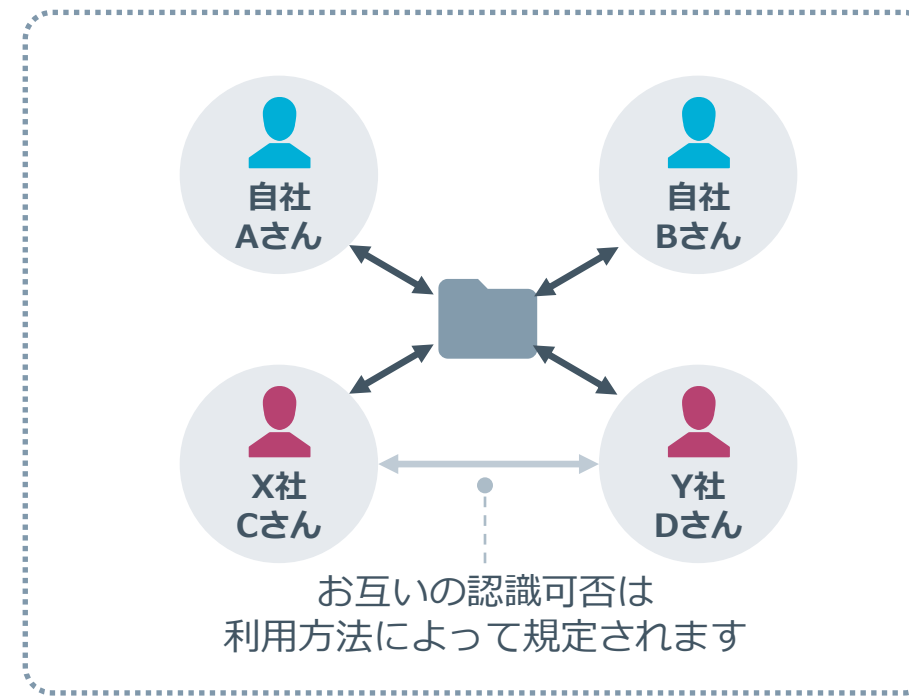
グループごとの所属メンバーの構成により、「誰が・誰とファイル交換できるか」を制御します。

オープングループ



権限を持った社内ユーザが交換相手を
任意に招待できる自由度の高いグループ

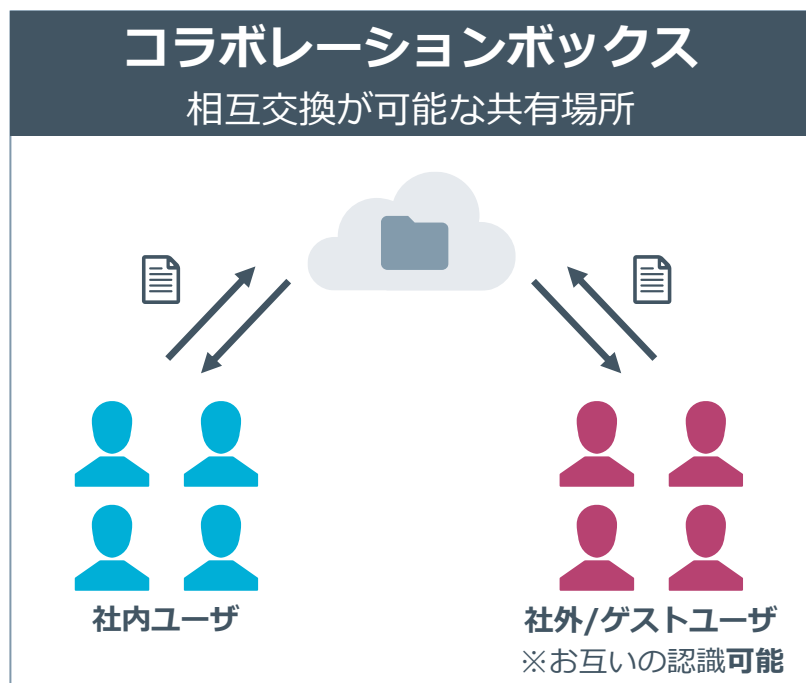
クローズドグループ



同一グループに登録された
複数社のユーザに限定して運用

利用方法を制御するボックス機能（3種類）

業務ごとに必要とされる種類の権限がプリセットされており、用途に応じて適切な権限でご利用いただけます。ボックスの権限はカスタマイズできないため、ミスや不正を誘発する特殊設定はできません。

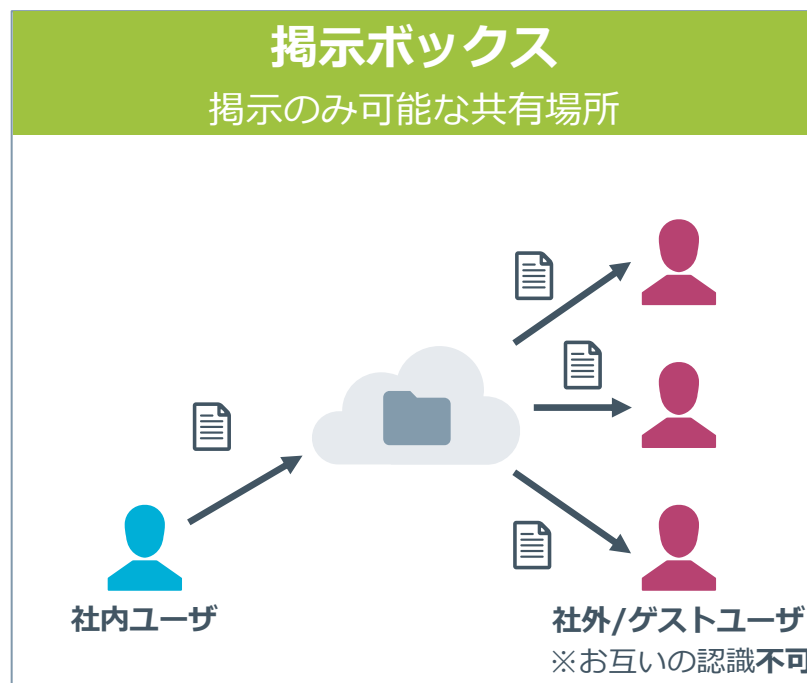


◇操作権限

社内ユーザー：取得/登録/更新/削除

社外/ゲストユーザー：取得/登録/更新/削除

- 全員がボックスに所属するユーザーを互いに認識しながら、ファイルのアップロード・ダウンロードを行うことができます。
- お互いにファイル授受が発生するプロジェクトなどで利用されます。

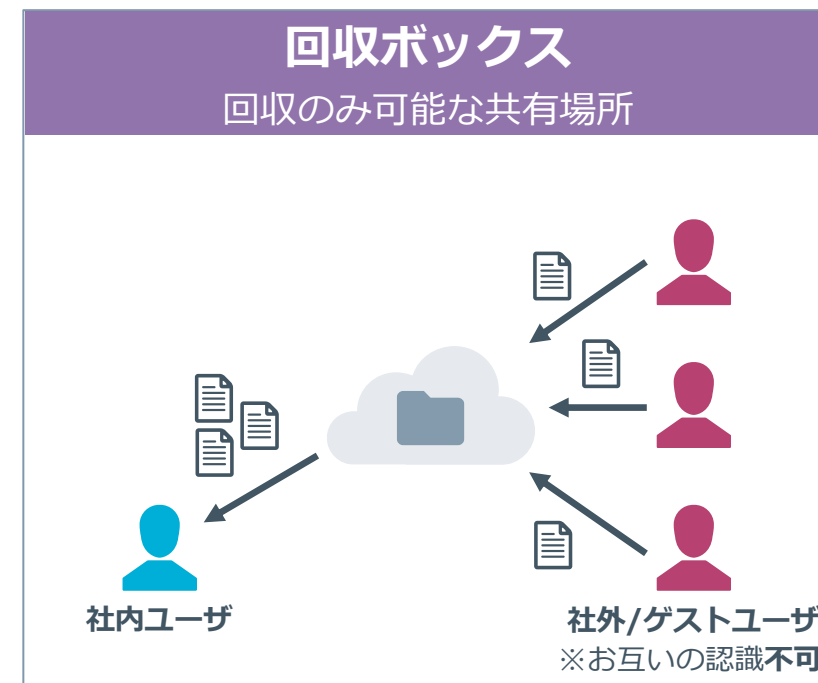


◇操作権限

社内ユーザー：取得/登録/更新/削除

社外/ゲストユーザー：取得

- 社外/ゲストユーザーは、社内ユーザーが格納したファイルのダウンロードのみ可能です。社外/ゲストユーザー同士はお互いを認識できません。
- 相手からファイルを受け取る必要がない、会員や会議出席者への資料配布などで利用されます。

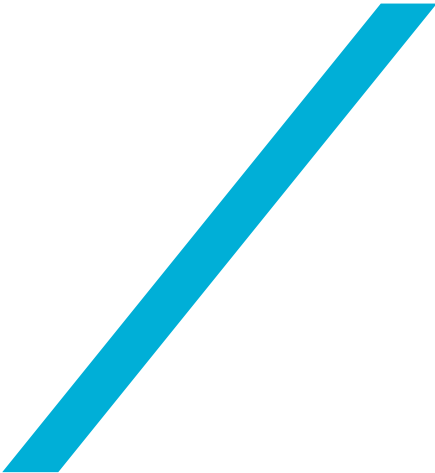


◇操作権限

社内ユーザー：取得/削除

社外/ゲストユーザー：取得/登録/更新/削除（※）

- 社外/ゲストユーザーは、社内ユーザーに共有したいファイルのアップロードのみ可能です。社外/ゲストユーザー同士はお互いを認識できません。
- 相手にファイルを渡す必要がない、提出物の回収などで利用されます。



機能紹介 – その他の機能

クリプト便機能全体像

ファイル送受信・ファイル共有のほか、用途拡大やセキュリティ強化に役立つオプション機能を多数ご用意しています。

メイン機能

ファイル送受信

ファイル送信

ユーザログ管理

ファイル受信

IPアドレス制限/
ワンタイムパスワード認証

受信時自動通知

ダウンロード時自動通知

ウイルスチェック

ユーザグループ管理

ファイル共有

ファイル共有

ユーザログ取得

アップロード時自動通知

IPアドレス制限/
ワンタイムパスワード認証

ユーザグループ管理

ボックス機能

ウイルスチェック

+

オプション機能

セキュリティ・監査強化

承認

グループ毎送信ログ監査

宛先直接入力禁止

セキュリティ強化 (PCI DSS)

ファイルアーカイブ

データセンター監査

管理者操作ログ取得

ログ保存日数延長

システム連携

オートパイロット

ユーザID連携

API

認証連携

端末認証

その他

大容量送付

画面カスタマイズ

専用ドメイン

EVサーバ証明書管理

よくある課題と対応機能 1/2

ファイル交換におけるセキュリティ課題と機能の対応表です。オプション機能検討時にご参照ください。

○：根本対策
△：部分対策

セキュリティ課題	項番	対策	ファイル送受信		ファイル共有	
			標準	オプション	標準	オプション
許可していない環境への送受信禁止	1-1	許可された環境外からのログインを禁止する（パスワード漏洩対策をする）	○IPアドレス制限	○端末認証 ○認証連携	○IPアドレス制限	○端末認証 ○認証連携
	1-2	許可していない相手先への送受信/共有を禁止する	○クローズドグループ ○送信先制限	-	○クローズドグループ	-
危険な操作の監視/対応	2-1	宛先/添付ファイルの誤設定を監視/防止する	○送信前チェック △追加メールアドレス	○承認 △宛先直接入力禁止	△追加メールアドレス	○承認
	2-2	不正操作の痕跡を確認できるようにする	△メッセージログ	○管理者操作ログ ○ファイルアーカイブ	△ファイル共有ログ	○管理者操作ログ ○ファイルアーカイブ

よくある課題と対応機能 2/2

ファイル交換におけるセキュリティ課題と機能の対応表です。オプション機能検討時にご参照ください。

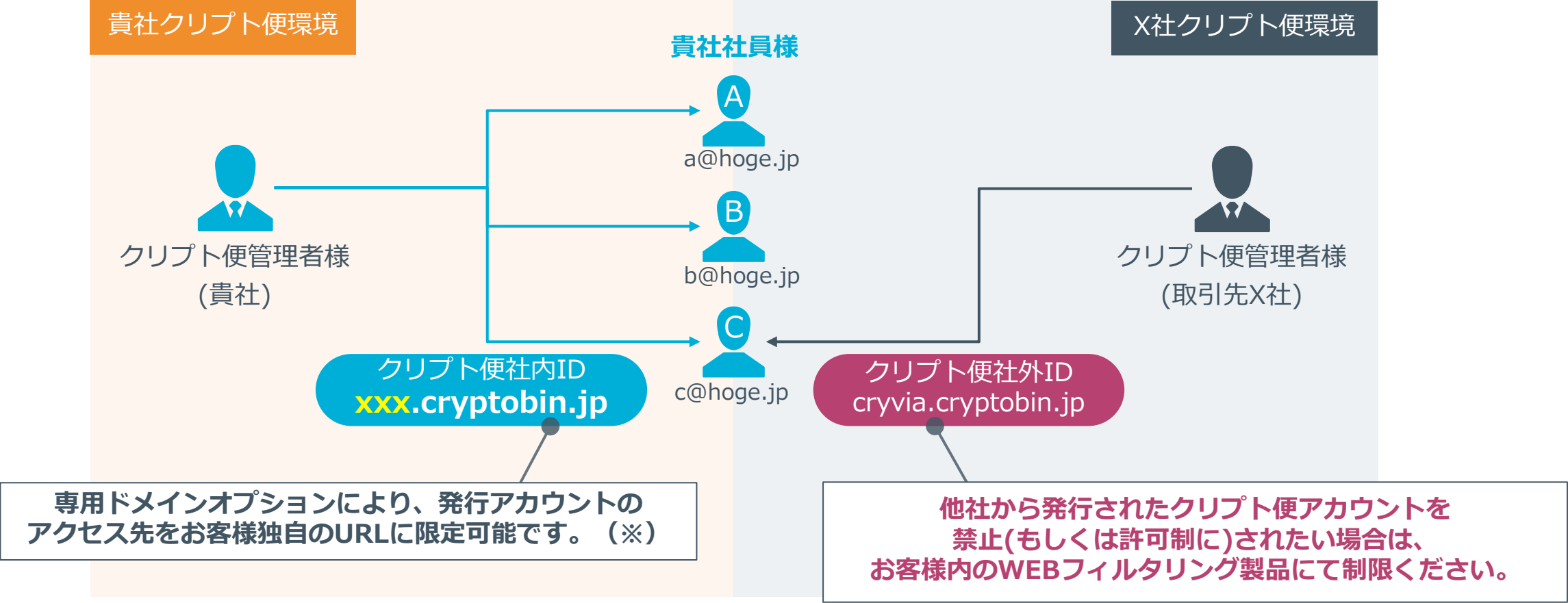
○：根本対策
△：部分対策

セキュリティ課題	項番	対策	ファイル送受信		ファイル共有	
			標準	オプション	標準	オプション
危険な操作ができない環境を用意	3-1	ウイルスファイルの送受信/共有がされないようにする	○ウイルスチェック※1 △拡張子制限	-	○ウイルスチェック※1	-
	3-2	ファイルのダウンロード権限を制限する	△ファイル持出抑止※2	-	○掲示/回収ボックス	○プレビュー (開発予定)
	3-3	ファイルを長期間保管しないようにする	○お預かり期限設定	○送受信ファイル保存 日数変更	○自動ゴミ箱移動/自動 削除	
	3-4	ヒューマンエラーによる誤送信リスクを排除する	-	△オートパイロット※3 △API ※3	-	
	3-5	当該監査人の対象外グループのログ閲覧を禁止する	-	○グループ毎 送信ログ 監査	-	○グループ毎 送信ログ 監査
不要アカウントの利用禁止	4-1	使わなくなったアカウントを棚卸する	△自動ロック	○ユーザID連携	△自動ロック	○ユーザID連携
	4-2	他社セクション発行のID利用／他社セクションのゲストユーザ利用を禁止する	-	○専用ドメイン※4 (+端末認証※5)	-	○専用ドメイン※4 (+端末認証※5)

※1 ウイルスチェックを実施するファイルサイズの上限はアップロード時100MB、ダウンロード時20MB。
※2 送信ボックスでのファイルダウンロードを禁止する設定。
※3 ヒューマンエラーを排除するには貴社側での開発・作り込みが必要。
※4 自社セクションを専用ドメイン化し、クリプト便の汎用ドメインをURLフィルタリングで禁止。URLフィルタリングは貴社側でのご用意が必要。
※5 専用ドメインと端末認証を併用することで、他社セクションのID利用禁止と、特定端末からのアクセスのみに制限も可能。

参考 | 内部不正リスクに対する専用ドメインオプションでの対策

クリプト便には無償アカウント制度はないため、社員様個人がアカウント発行するリスクは限定的です。
他社の契約環境から貸与されたアカウント利用を制限されたい場合は専用ドメインオプションをご検討ください。



※通常のユーザ利用時のアクセス先は専用ドメインのURLとなりますが、端末認証オプションの証明書インストール時など、専用ドメイン以外のURLもアクセス許可いただく必要が生じる場合がございます。

ファイル転送・共有サービスの検討時には NRIセキュアテクノロジーズにご相談ください

- 貴社ご要件に適したクリプト便の運用方法をご紹介します
- 多様なニーズにお応えできるサービスをご用意しています



ファイル転送

ファイル共有



ファイル共有

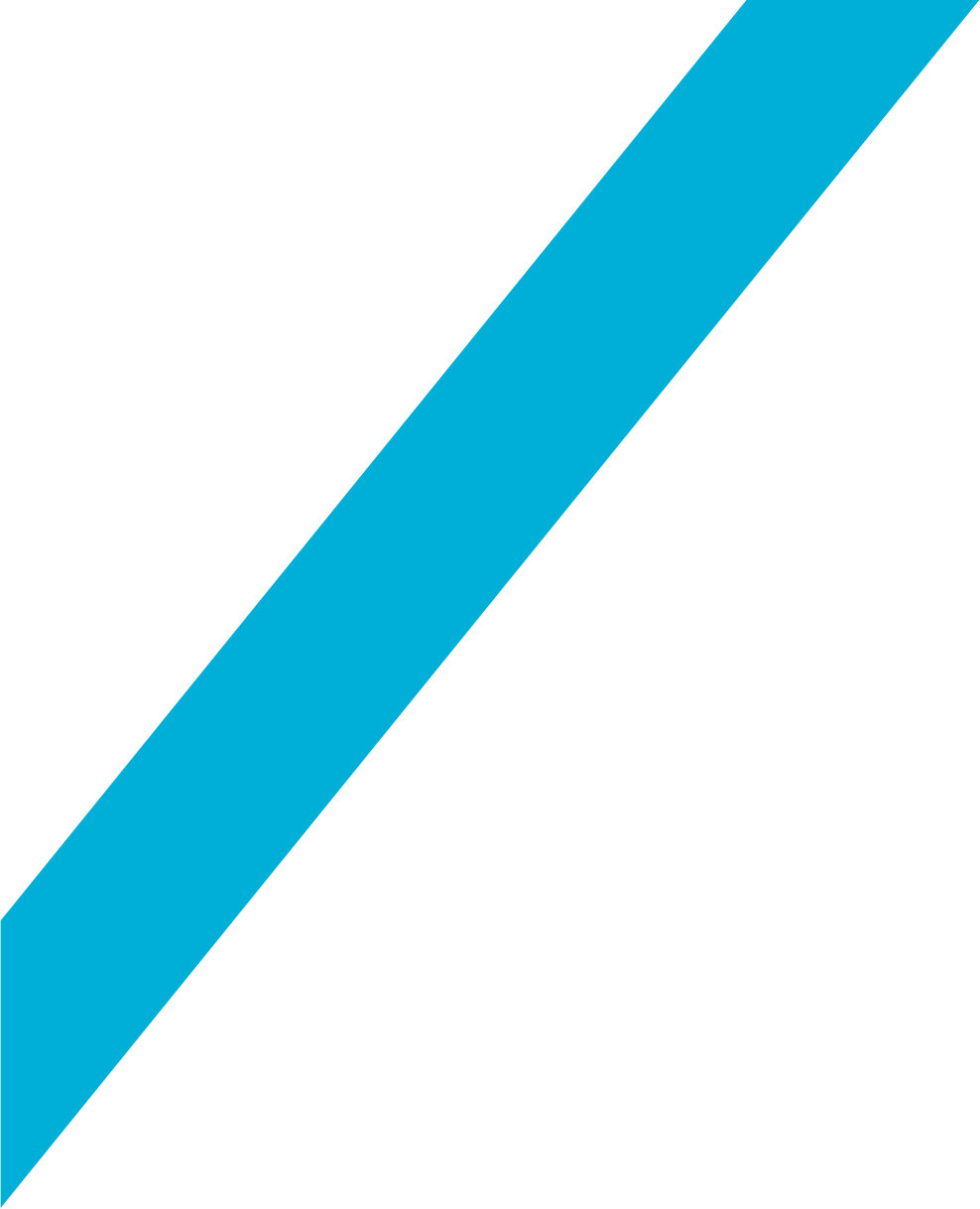


クリプト便

for m-FILTER

for m-FILTER@Cloud

UIを変更せずにPPAP対策



/NRI SECURE/