

デジタルフォレンジックサービス

企業・個人の「メール・ファイル」
データ調査

ひとつでも多くのデータを提供します

- 故意的削除
- 改竄捏造
- ログ履歴調査
- パスワード解除
- HDD環境まるごと保存

DIGITAL FORENSIC 24

データ調査・証拠保全

サービス詳細内容のご案内



目次

0. 目次	P1
1. フォレンジックとは	P2
2. フォレンジックサービスの主な内容	P3
3. データ不正利用の損害賠償事例	P4
4. メール送受信抽出について	P8
5. 削除データ抽出について	P10
6. インターネット閲覧履歴について	P12
7. ソフトウェア実行履歴について	P14
8. USB機器接続履歴について	P16
9. 実績・秘密保持について	P18
10. 店舗のご案内	P19
11. 主要サービス・フォレンジックサービスの流れ	P22
12. 株式会社リプラス 企業情報	P23



デジタルフォレンジックとは

データの不正使用や削除、改竄、捏造、漏洩などによる企業損失、妨害行為への法的紛争や訴訟、損害賠償請求のために必要な証拠保全の技術を指します。デジタルツールの普及により、データやメールを使った不正や犯罪が急増、不正の痕跡を消すためデータが削除されていることが多くデータを復元し割り出す必要があります。押収した機器から証拠を突き止めるため刑事事件の捜査の一環で求められることもあります。



故意な不正行為・データ損失が 御社の大きな損害に!

信用と資産を守るサービスです

故意なメール削除

主に退職者などが証拠隠滅のために完全削除したメールデータを復元いたします。メールの不正利用の可能性の高いパソコンからメールを復元し、データを証拠としてご提出いたします。



顧客情報漏洩形跡調査

漏洩した顧客情報が保有している顧客情報なのかハッシュ値から真偽を明らかにします。



Webサイト閲覧履歴調査

各種ブラウザ (Internet Explorer, GoogleChrome, FireFox等) のインターネット閲覧履歴を抽出します。削除したものの形跡が残っていれば復元します。



ファイル削除 ゴミ箱の完全消去

故意にデータを削除しさらにゴミ箱からも削除されたデータを復元するサービスとなります。



隠蔽・捏造ファイルの調査

不正の証拠になるようなデータを別のデータに隠蔽されていても探し出すことができます。データを改ざんし証拠の捏造を行っても解析し、改ざんされたことを証明することができます。



PC 起動・ソフト使用履歴調査

パソコン上で起動したソフトウェアの履歴を一覧に致します。起動した日時、ソフトがわかることで、誰もいない時間に起動していたり、身に覚えのないソフトが動いていることがわかります。



退職した社員に顧客情報を持ち出され、 起業した会社に顧客を奪われた

社員が退職前に顧客情報を持ち出し、退職後に起業した会社でその顧客情報から顧客を奪われていた。

急に懇意にしていた取引先からもっと安いところに依頼することにしたと言われ調査したところ、退職した社員が起業した会社に依頼していることが判明した。

そのことから在職時から個人的な取引をしていた可能性があると思い、その証拠が残っていないか、在職時に使用していたパソコンの調査をして欲しい。

取引先と不審なメールのやりとりをしていた女性社員の不貞行為と情報漏洩が発覚、解雇と賠償請求を行った

ある女性社員が使用していたパソコンから不審なメールが少し見えたため、翌日チェックをするとそのメールが削除されていた。

どんな内容だったのか削除したメールの復元を行い、取引先との不倫が発覚した。さらに会社には内緒で不正な取引も行っていたため、即解雇し、賠償請求を行った。

委託勤務しているSEがデータを自宅に持ち帰り顧客情報を売却！

所属会社への賠償請求と顧客への謝罪対応を弁償させた

WEB上に顧客情報がアップロードされていることが判明し、どこから漏洩したのか調査を行ったところ、社外へ持ち出し禁止のノートPCを自宅に持ち帰ったSEがいることがわかった。そのSEの自宅のPCを調査したところ、自宅PCから削除された顧客情報が見つかり、それを証拠に賠償請求と謝罪対応を行わせた。

フォレンジックサービスの主な内容とは

1. メール送受信抽出
2. 削除データ抽出
3. インターネット閲覧履歴抽出
4. ソフトウェア実行履歴抽出
5. USB機器接続履歴抽出

1 メール送受信抽出について

- 削除されてしまったメールの復元
- 添付ファイルの抽出
- 送受信日時
- CC・BCC先



・メールタイトル

The screenshot shows an email client window with a list of emails and a detailed view of a selected email. A blue line points from the text '・メールタイトル' to the 'Subject' column of the email list. Another blue line points from the text '添付ファイル' to the attachment 'ATM_THEFTS1.ppt' in the '電子メール添付ファイル' pane. A third blue line points from the text '・メール本文' to the main body of the email.

サブジェクト	名前	終了日	開始日	CC	BCC	提出時刻	デリバリー...
PGP Trial Software Order Confirmation: 851797 ::EW49TU6I...	26FC5471-00000004.eml	trialwareor...	TrialSof...			2007/0...	2007/0...
RE: Stuff	2A29541D-0000000E.eml	"Wes Mant...	"Rasco ...			2007/0...	2007/0...
It's easy to switch to Gmail!	2D662154-00000001.eml	"mr smee" ...	"Gmail ...			2007/0...	2007/0...
Welcome to Windows Mail	31D0562C-00000001.eml	"New Wind...	"Micros...			2007/0...	
Re: New Venture	3376666D-0000000A.eml	"Wes Mant...	"John ...			2007/0...	2007/0...
A trade	3F687E04-00000001.eml	<chkwashe...	"Mr Sm...			2007/0...	
Re: New Venture	40A511AF-00000008.eml	"Wes Mant...	"John ...			2007/0...	2007/0...

電子メール添付ファイル

- 3376666D-0000000A.eml
 - OECustomProperty
 - ATM_THEFTS1.ppt

"John Washer" <chkwasher@comcast.net>
2007/07/11 14:27:15 -0600
Wes Mantooth <dollarhyde86@comcast.net>; Mr Smee <smee.rox@gmail.com>
Re: New Venture
ATM_THEFTS1.ppt

to be too risky, a budy of mine showed me how to rig the machines to keep the cards... Then we shoulder surf the pin and get the card
!

・メール本文

2 削除データ抽出について

- ・ 削除したデータを検出し抽出します
- ・ ほぼ全てのデータに対応をしております
- ・ 作成日時・更新日毎にソート可能



・削除した画像・Excel・Text等表示

The screenshot shows a forensic software interface. At the top, there are tabs for 'Hex', 'テキスト', 'フィルタ適用', and 'ナチュラル'. Below these is a preview window showing a photograph of a man. To the left is a sidebar with a file tree, including categories like 'KFF警告ファイル (0/0)', 'OCRグラフィック (0/0)', and '削除したファイル (25/25)'. Below the preview is a 'ファイルの内容' section with 'プロパティ' and '16 進インタプリタ' options. The main area is a 'ファイルリスト' (File List) table with columns for name, label, item size, extension, path, category, P-size, L-size, MD5, SHA1, SHA256, creation date, access date, and modification date.

名前	ラベル	アイテム...	拡張子	パス	カテゴリ	P-サイズ	L-サイズ	MD5	SHA1	SHA256	作成日	アクセス日時	変更済み
\$I30		1866		Mantooth.E01//パーティ...	インデッ...	4096 B	4096 B				2008/02/13 9:5...	2008/02/13 9:5...	2008/02/13 9:5...
\$I30		1092		Mantooth.E01//パーティ...	インデッ...	4096 B	4096 B				2008/02/13 9:5...	2008/02/13 9:5...	2008/02/13 9:5...
[MetaCarve]		6001		Mantooth.E01//パーティ...	プレー...	N/A	N/A				N/A	N/A	N/A
Afrit		1107		Mantooth.E01//パーティ...	フォルダ	48 B	48 B				2008/02/13 9:5...	2008/02/13 9:5...	2008/02/13 9:5...
ar_test نقیصه.doc		1870	doc	Mantooth.E01//パーティ...	Microso...	19.00 KB	19.00 KB				2008/02/13 9:5...	2008/02/13 9:5...	2006/05/27 8:0...
Astral.doc		1106	doc	Mantooth.E01//パーティ...	Microso...	38.00 KB	38.00 KB				2008/02/13 9:5...	2008/02/13 9:5...	2008/02/13 9:0...
Book of Nod		1105		Mantooth.E01//パーティ...	フォルダ	48 B	48 B				2008/02/13 9:5...	2008/02/13 9:5...	2008/02/13 9:5...
Exhume.doc		1108	doc	Mantooth.E01//パーティ...	Microso...	40.00 KB	40.00 KB				2008/02/13 9:5...	2008/02/13 9:5...	2008/02/13 9:0...
FightClub.jpg		1873	jpg	Mantooth.E01//パーティ...	JPEG	3584 B	3184 B				2008/02/13 9:5...	2008/02/13 9:5...	2007/08/15 6:2...
froghanging.jpg		1094	jpg	Mantooth.E01//パーティ...	JPEG	39.00 KB	38.95 KB				2008/02/13 9:5...	2008/02/13 9:5...	2007/08/15 6:1...
FrogMouth.jpg		1095	jpg	Mantooth.E01//パーティ...	JPEG	26.00 KB	25.87 KB				2008/02/13 9:5...	2008/02/13 9:5...	2007/08/15 6:1...
More Secret Stuff		1091		Mantooth.E01//パーティ...	フォルダ	48 B	48 B				2008/02/13 9:5...	2008/02/13 9:5...	2008/02/13 9:5...
My Confession.txt		1863	txt	Mantooth.E01//パーティ...	テキスト	232 B	232 B				2008/02/13 9:5...	2008/02/13 9:5...	2007/08/15 6:2...
qur_test نقیصه.doc		1869	doc	Mantooth.E01//パーティ...	Microso...	19.00 KB	19.00 KB				2008/02/13 9:5...	2008/02/13 9:5...	2006/05/27 8:0...
russ 2 Абакурный.doc		1868	doc	Mantooth.E01//パーティ...	Microso...	19.00 KB	19.00 KB				2008/02/13 9:5...	2008/02/13 9:5...	2006/05/27 8:0...

・ファイル名

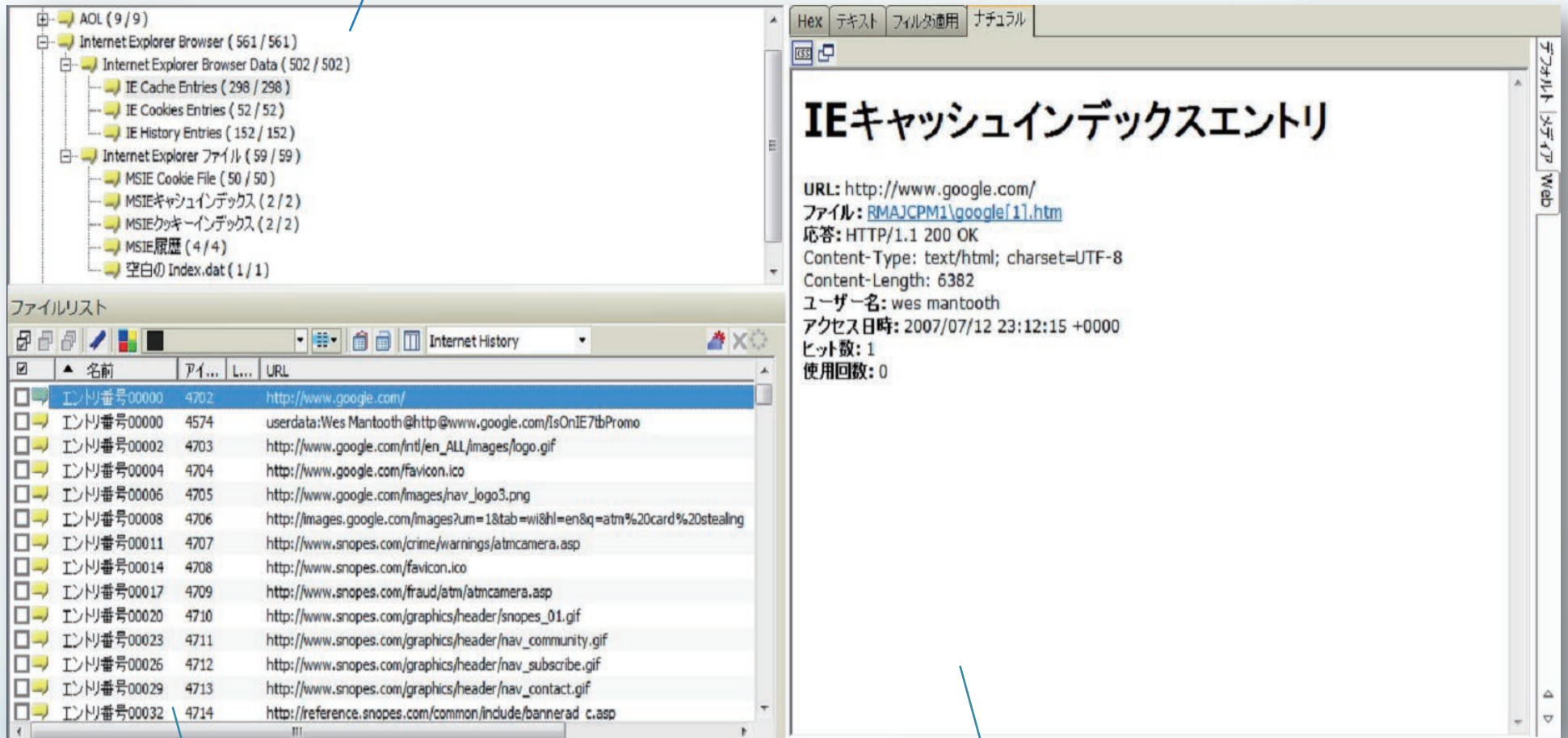
・作成日・更新日

3 インターネット閲覧履歴について

- ・ 閲覧していたURL判明
- ・ 閲覧回数までわかります
- ・ アクセス日時でソート可能



・履歴種別別



・履歴一覧

・履歴詳細

4 ソフトウェア実行履歴について

- ・ 実行したファイル名の表示
- ・ 実行ファイルの場所
- ・ 不正な実行ファイルも判明



名前	種類	データ
(既定)	REG_SZ	(値の設定なし)
HotKeysCmds	REG_SZ	"C:%Windows%system32%hkcmd.exe"
IgfxTray	REG_SZ	"C:%Windows%system32%igfxtray.exe"
IME JPN 2007 ...	REG_SZ	C:%PROGRA~1%COMMON~1%MICROS~1%IME12%IMEJP%IMJPKLMG.EXE /Preload
MFNetworkSc...	REG_SZ	C:%Program Files%Canon%Canon MF Network Scan Utility%CNMFSUT6.EXE
Persistence	REG_SZ	"C:%Windows%system32%igfxpers.exe"
Platinum	REG_SZ	"C:%Program Files%Trend Micro%Titanium%plugin%Pt%PtSessionAgent.exe" 1
RtHDVBg_DTS	REG_SZ	C:%Program Files%Realtek%Audio%HDA%RAVBg64.exe /DTSU2P
RTHDVCPL	REG_SZ	C:%Program Files%Realtek%Audio%HDA%RtkNGUI64.exe -s
Trend Micro Cl...	REG_SZ	"C:%Program Files%Trend Micro%UniClient%UIFrmWrk%UIWatchDog.exe"
WLM	REG_SZ	"C:%Program Files%Trend Micro%Titanium%Plugin%TMAS%TMAS_WLM%TMAS_WLMMon.exe"

・ 実行ファイル名

・ ファイルパス

5 USB機器接続履歴について

- 接続機器名表示
- 接続日時判明
- USBメモリ・HDD・

カードリーダーなどの種類もわかります



・ USB機器名

The screenshot shows the Windows Registry Editor with the left pane displaying a tree view of registry paths. The path 'Disk\Ven_I-O_DATA&Prod_USB_Flash_Disk&Rev_1100' is selected, and the right pane shows the corresponding registry values. A blue line points from the title 'USB機器名' to the selected path. Another blue line points from the title '機器詳細' to the 'Service' value.

名前	種類	データ
(既定)	REG_SZ	(値の設定なし)
Capabilities	REG_DWORD	0x00000010 (16)
Class	REG_SZ	DiskDrive
ClassGUID	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}
CompatibleIDs	REG_MULTI_SZ	USBSTOR\Disk USBSTOR\RAW
ConfigFlags	REG_DWORD	0x00000000 (0)
ContainerID	REG_SZ	{9c161f3d-c699-52fc-b59d-a9b675b89796}
DeviceDesc	REG_SZ	@disk.inf,%disk_devdesc%;ディスク ドライブ
Driver	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}\0412
FriendlyName	REG_SZ	MARSHAL SHELTER HDD USB Device
HardwareID	REG_MULTI_SZ	USBSTOR\DiskMARSHAL_SHELTER_HDD _____ USBSTOR\DiskMARSHAL_SHELTER_HDD _____
Mfg	REG_SZ	@disk.inf,%genmanufacturer%;(標準ディスク ドライブ)
Service	REG_SZ	disk

・ 機器詳細

選ぶなら**安心**と**信頼**の技術

一つでも多くの確かな証拠データを割り出すために、信頼の技術力を持った当社をお選びいただくことをおすすめいたします。

デジタルフォレンジック24は
特急データ復旧ウィンゲットが運営しています

データ復旧の実績

累計 **60,000** 件以上

データ復旧専門10年以上の経験で培った高度な技術と、信頼のサービスでお選びいただいております。出張サービスを業界内でもいち早くスタートさせ、お客様のニーズに合わせたサービスでご満足いただいております。



ISMS・プライバシーマーク取得企業
お客様の大切な情報を守ります

NDA（秘密保持契約）締結も可能です。ご相談ください。



IS 992505 ISO/IEC 27001:2013
本社で取得しています

オフィスは主要都市に7箇所

札幌オフィス



西11丁目駅から徒歩3分

札幌市中央区南1条西10-4-167
小六第一ビル 6F

秋葉原オフィス



秋葉原駅から徒歩5分

東京都千代田区神田須田町2-7-3
VORT秋葉原ビル5F

新宿オフィス



新宿駅から徒歩5分

東京都新宿区西新宿7丁目1-12
クロスオフィス新宿1F

関内オフィス



関内駅から徒歩5分

横浜市中区扇町1-25
キングビル3F

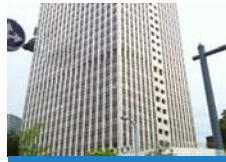
名古屋オフィス



名古屋駅から徒歩5分

名古屋市中村区名駅2-38-2
オーキッドビル 5F

大阪オフィス



大阪駅から徒歩1分

大阪市北区梅田1-1-3
大阪駅前第3ビル 7F

福岡オフィス



博多駅から徒歩5分

福岡市博多区博多駅南1-3-6
第3博多階成ビル 11F

受付窓口は”お客様の近くに”全国185拠点

※2017年4月現在



お客様の近くでご相談をモットーに全国の受付窓口だけでなく代理店・紹介店も全国に多数ございます。

日本全国、24時間365日現地へ出張対応！ 御社までお伺いし就業後にも対応可能

「機器が社内規定で持ち出すことができない」「機器を持ち出さず、社内で秘密裏に作業して欲しい」というお客様のご要望にお応えした出張サービスが当社の強みです。

まずお客様の元に出張し、現地でご相談を伺います。その後、デジタルフォレンジック作業を実施し、完了まで現地で行います。お客様の元で作業を行うため、一番迅速に対応ができるサービスです。

また、業務に影響が及ばない夜間の時間帯や社員退社後・休日の時間帯、お急ぎのお客様のための緊急対応も可能です。



DIGITAL FORENSIC 24 主要サービス

データ調査・証拠保全

デジタルフォレンジックの技術で御社の資産を守ります

MELSIC

メール・ファイル復元サービス
MELSIC (メルジック)

メール・ファイル復元

情報隠蔽のためにファイルが隠される、削除される等と証拠隠滅のためにメールやファイルが完全消去され、一般では復元できないケースがほとんどとされています。しかし、当社はメールの不正利用やファイル削除・隠蔽の可能性の高いパソコンからメールやファイルを復元し、証拠として抽出データをご提出し、御社の財産・権利をお守りします。

ANKAI

暗号化・パスワード解除サービス
ANKAI (アンカイ)

暗号化・パスワード解除

セキュリティ強化のため、暗号化したパソコンや外付けHDDが故障し、正規の方法で暗号化解除を行うことができなくなった場合、暗号化を解除することが可能です。さらに、エクセル等のファイル自体にパスワードを掛けたが忘れてしまった場合でも、パスワード解析を弊社の最新技術で行い、ファイルのパスワード解除をすることが可能です。

CHRONO DATA

HDD・SSD データ複製サービス
CHRONO DATA (クロノデータ)

HDD SSD データ複製

故障の際の備えとしてのご利用や、現在のパソコン環境のままHDDからSSDに移行する際に活用いただけます。

現状のデータを新しいHDDやSSDに複製し、データの保管・移行を行います。環境ごと複製することができるため、クローンHDDを作成し、万が一パソコンが壊れた際にそのクローンHDDを使ってパソコン環境ごと元に戻すことが可能です。

CHRONO DATA

HDD・SSD データ保全サービス
CHRONO DATA (クロノデータ)

HDD SSD データ保全

会社の内部監査や裁判に提出するための証拠として、HDDやSSDをそのままそっくり新しいHDDやSSDに複製し、データを保全します。出張や夜間での対応が可能のため、例えば就業時間外の時間にお客様の元に伺い、各パソコンのHDD内のデータを複製し、クローンHDDをお渡しするということも可能です。クローンHDDからの調査はお客様側で行っていただけます。

サービスの流れ

STEP 1

お電話またはネット予約で無料診断の申し込み

デジタルフォレンジックの無料診断を受け付けております。お電話またはインターネット専用予約ページからご予約いただけます。

お客様サポートセンター (24時間受付) インターネット予約
0120-703-845 http://www.forensic24.com/#reserved_form

STEP 2

出張・店舗へご来店・郵送

デジタルフォレンジックの初期調査を行うため、<出張・店舗へ来店・郵送>のいずれかの方法からお選びください。特にお急ぎで機器が持ち出せないお客様は出張、近くに店舗があるお客様は来店、急ぎではなく店舗も遠いお客様は郵送がそれぞれお勧めです。

※秘密保持契約(NDA)は作業前に締結可能です。お問い合わせ時もしくは出張/来店/郵送時にスタッフへお申し付けください。

STEP 3

初期調査

出張の場合は現地、来店と郵送受付の場合は店頭にて初期調査をいたします。内容によっては時間がかかる場合もございますので、ご了承ください。まずデータ証拠保全のため、お客様からお預かりいただいたHDD内の情報を完全に保全化(クローン)致します。

STEP 4

作業

初期調査が終わり次第、お客様に結果をご報告し、お見積もりやデータ復元にかかる時間などをお伝えいたします。その結果により、正式に弊社へご依頼をいただきましたら専用の機材を使用して、デジタルデータ復元作業を行います。

STEP 5

お支払い・納品・報告書提出

作業が終わりましたら、どれだけのデータが復元できたのか結果をご報告いたします。その後、お支払いをいただきます。お支払い方法はクレジット決済もしくは銀行振込での対応が可能です。

お支払い確認後、復元したデータを新しい媒体(DVD・ハードディスクなど)に入れて、お客様にご納品致します。また、調査報告書の提出も行います。

対応機器



企業理念

データ復旧で人類の「記録」を守り

クリエイティブなクラウドで「感動」を生み出し

「教育」を大切にし、「上質」を手に入れ

常に、お客様・社員の「発展幸福」を実現します

- 一つ、私たちは、お客様・社員の発展幸福の実現を一番に考え行動します
- 一つ、私たちは、正しく豊かな教育体系を確立し、上質なサービスを提供します
- 一つ、私たちは、IT技術を極限まで高め、世界一を生み出し続けます
- 一つ、私たちは、大切なデータを300年間守り、最高の感動を生み出し続けます

世界へSHIFT UP!!

業界No.1の拠点数と取引実績

世界は大容量データの時代を迎えました。当社のデータ復旧・クラウド事業は、今の時代に不可欠な存在として、ますます大きな社会的責任を負っています。

厚生労働省/東京都庁/大阪府庁/愛知県庁/神戸大学/北海道大学/九州大学ほか
大手企業様・官公庁様との取引実績多数!

ISMS (情報セキュリティマネジメントシステム)

を取得しております!

機器情報の取り扱いやアクセス管理など、様々な情報セキュリティ対策を運用しておりますが、この度ISO27001/ISMSの認証を取得いたしました!



海外展開に向けて各国の企業と協力し300年企業へ

データ復旧技術のさらなる向上のため、世界有数のデータ復旧会社を訪問。協力体制の構築を実現しました。



株式会社リプラス
代表取締役 柳町 正樹

会社概要

CORPORATE PROFILE

社名	株式会社 リプラス
代表者	代表取締役 柳町 正樹
資本金	1,000万円
創業	1999年
設立	2003年7月
従業員	50名
事業内容	●データ復旧事業部 データ復旧サービス PC設定 企業ネットワーク構築 ●クラウド事業部 オンラインストレージサービス クラウドソリューション企画・制作・販売 ●マーケティング事業部 WEB企画・制作 コールセンター機能
主要銀行	三菱東京UFJ銀行 津島支店 名古屋銀行 大治支店 岐阜信用金庫 美和支店 百五銀行 戸田支店 十六銀行 美和支店

株式会社 リプラス

<http://www.riplus.co.jp>

TEL:052-414-7561 FAX:052-414-7563 ☎0120-703-845

北海道／札幌オフィス 北海道札幌市中央区南1条西10丁目4-167 小六第一ビル6F
<http://www.data-hokkaido.com/>

東京／秋葉原オフィス 東京都千代田区神田須田町2-7-3 VORT秋葉原ビル5F
<http://www.60min-data.com>

新宿オフィス 東京都新宿区西新宿7-1-12 クロスオフィス新宿1F

神奈川／横浜オフィス 神奈川県横浜市中区扇町1-1-25 キンガビル3階 309
<http://www.data-yokohama.com/>

愛知／名古屋オフィス 愛知県名古屋市中村区名駅2-38-2 オーキッドビル5階 B-1
<http://www.data758.com/>

大治オフィス 愛知県海部郡大治町三本木寒宿84-1

大阪／大阪オフィス 大阪府大阪市北区梅田1-1-3 大阪駅前第3ビル7F 2-4号室
<http://www.data-osaka.com/>

福岡／福岡オフィス 福岡県福岡市博多区博多駅南1-3-6 第三博多倍成ビル11F
<http://www.data-fukuoka.com/>

DIGITAL FORENSIC 24

データ調査・証拠保全

<http://www.forensic24.com>

提供元



TEL: 0120 703 845 <http://www.riplus.co.jp> <http://www.forensic24.com>



0120-703-845



□札幌オフィス 北海道札幌市中央区南1条西10丁目4-167 小六第一ビル6F TEL:011-272-0600
□秋葉原オフィス 東京都千代田区神田須田町2-7-3 VORT秋葉原ビル5F TEL:03-6206-0970
□新宿オフィス 東京都新宿区西新宿7-1-12 クロスオフィス新宿 1F TEL:090-3834-7382
□横浜オフィス 神奈川県横浜市中区扇町1-1-25 キンガビル3階 309 TEL:050-2018-0428

□名古屋オフィス 愛知県名古屋市中村区名駅2-38-2 オーキッドビル5階 B-1 TEL:052-414-7561
□大治オフィス 愛知県海部郡大治町三本木寒宿84-1 TEL:052-445-0901
□大阪オフィス 大阪府大阪市北区梅田1-1-3 大阪駅前第3ビル7F 2-4号室 TEL:06-6131-8423
□福岡オフィス 福岡県福岡市博多区博多駅南1-3-6 第三博多倍成ビル11F TEL:092-452-7705

販売店・代理店