



会計事務所向け情報セキュリティ研修会

**NTT DATA**

- 1.はじめに
- 2.情報セキュリティの基本概念
- 3.情報セキュリティ事故が与える影響
- 4.事業継続計画とは
- 5.会計事務所が取るべき行動
  - ・ 教育を行う
  - ・ ウイルス感染を防ぐ
  - ・ 情報を持ち出さない
  - ・ 電子化をする
  - ・ バックアップを取る

税理士業界は他の業界と比較しても早くから「コンピュータ化」が進んだ業界と言われて  
います。高度な専門性と安全性を担保するという名目の元、そのコンピュータ化は「専用機  
ベンダー」主導で行なわれ、「パソコン化」には出遅れてしまった感は否めません。

しかしながら、Windowsパソコンの流通拡大に伴い顧問先企業へのパソコン導入が進むに  
つれ、会計・税務処理に「専用機」を利用している事務所でもパソコンを利用した計算業務  
が増加し、今では専用端末のオープン化が進んでいます。これにより、会計事務所にとって  
の主たる情報資産は専用機上の会計・税務情報だけでなく、パソコンを利用して作成した計  
算補助資料・管理資料にまで拡大し、その管理・保全是事務所経営上の重要な問題となりつ  
つあります。

東日本大震災・大津波の被害を目の当たりにし、情報資産の保全についてその重要性が再  
認識されていると共にその方法も再検討を余儀なくされている状況です。

本日は、会計事務所において人命の次に重要とされる「情報資産」について、その保全方  
法を中心にお話しさせていただきたいと思えます。

また、情報資産の活用・保全という面で注目が集まる新しい仕組みについても事例を交え  
てご紹介いたします。

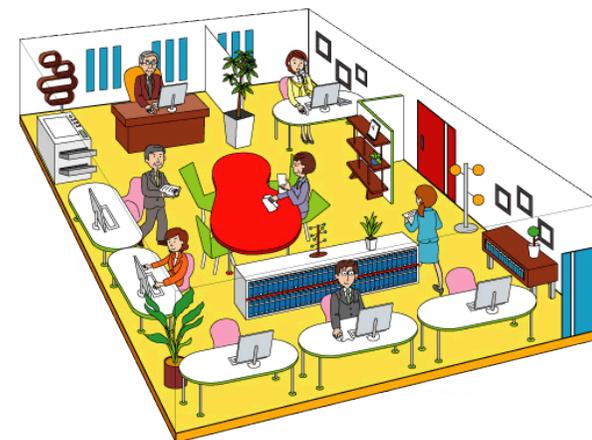
### 情報資産とは

資産とは、企業の業務遂行の過程で生み出される価値あるもののことです。資産には、不動産や商品など、目に見えるものもあれば、財務情報、人事情報、顧客情報、技術情報などの目に見えないものもあります。これらのことを、情報資産といい、情報セキュリティ上の脅威から守る必要があります。

#### 会計事務所の情報資産の一例

- ・ 顧問先のデータ（財務データ・税務データ・給与年末調整データ・事業計画など）
- ・ 事務所自身のデータ（財務データ・税務データ・給与年末調整データなど）
- ・ 顧問先一覧・顧問料一覧・打ち合わせ議事録など

企業には、多くの情報資産が蓄えられており、それらは、コンピュータ、記録媒体、紙、または人の記憶や知識など、さまざまな形態をとります。ITの普及に伴い、情報資産の価値は、ますます高まっているといえます。



### 税理士法の守秘義務

#### 税理士法 第38条 (秘密を守る義務)

税理士は、正当な理由がなくて、税理士業務に関して利しえた秘密を漏らし、又は窃用してはならない。税理士でなくなった後においても、また同様とする。

#### 税理士法 第54条 (税理士の使用人等の秘密を守る義務)

税理士又は税理士法人の使用人その他の従業者は、正当な理由がなくて、税理士業務に関して知り得た秘密を他に漏らし、又は窃用してはならない。

税理士又は税理士法人の使用人その他の従業者でなくなった後においても、また同様とする。

#### 税理士法 第59条

次の各号のいずれかに該当する者は、二年以下の懲役又は百万円以下の罰金に処する。

二 第38条（第50条第2項において準用する場合を含む。）又は第54条の規定に違反した者

### 情報セキュリティとは

情報セキュリティという言葉の意味は、まだ明確に定義されている訳ではありませんが、企業・組織における情報資産全般の機密性、完全性、可用性を確保するという意味で使われている言葉です。

#### 機密性

情報にアクセスすることが認可されたものだけがアクセスできることを確実にすること。

【対策】 情報漏えい防止・アクセス権の設定など

#### 完全性

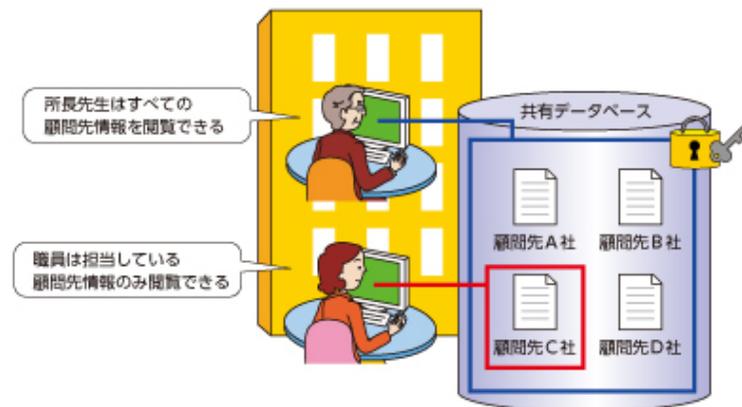
情報及び処理方法の正確さおよび完全である状態を安全防護すること。

【対策】 改ざん防止

#### 可用性

認可された利用者が、必要なときに情報にアクセスできることを確実にすること。

【対策】 機器の冗長化、バックアップ、電源対策



### 情報セキュリティポリシーとは

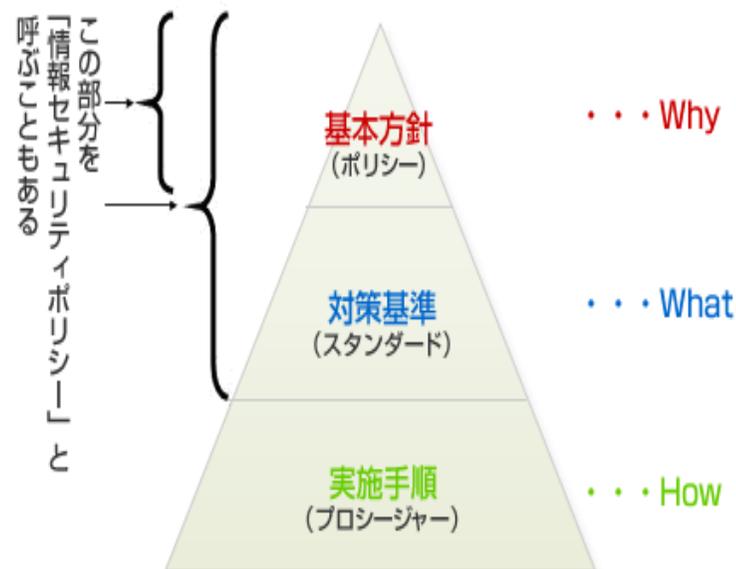
情報資産の情報セキュリティ対策について、総合的・体系的かつ具体的にとりまとめたもの。基本方針で定められた内容が、対策基準、実施手順と段階を追って具体化されていきます。

**基本方針**は、組織の経営者が、「情報セキュリティに本格的に取り組む」という姿勢を示し、情報セキュリティの目標と、その目標を達成するために企業がとるべき行動を社内外に宣言するものです。「なぜセキュリティが必要か」という「Why」について規定し、何をどこまで守るのか（対象範囲）、誰が責任者かを明確にします。

**対策基準**は、基本方針で作成した目的を受けて、「何を実施しなければならないか」という「What」について記述します。組織的に情報セキュリティ対策を行うためのルール集で、人事規程や就業規程などの類の企業の構成員が守るべき「規程類」に相当します。

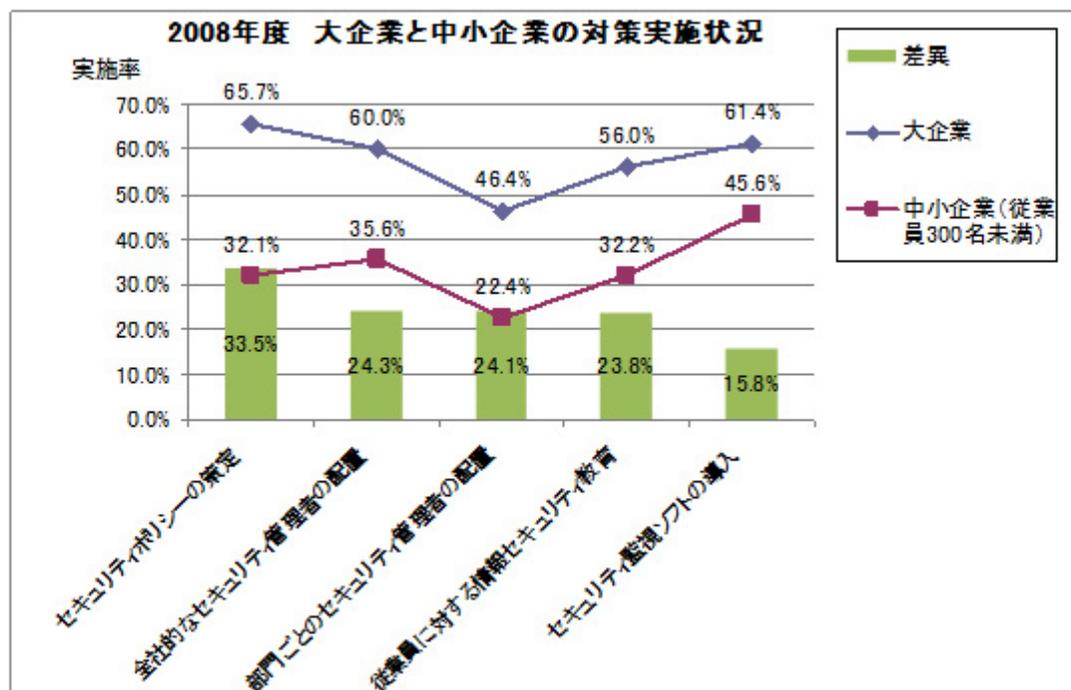
**実施手順**は、対策基準で定めた規程を実施する際に、「どのように実施するか」という「How」について記述します。マニュアル的な位置づけの文書であり、詳細な手順を記述します。

### IPAホームページより



### 中小企業のセキュリティの実態

国内の中小企業といえども、今やインターネットなしに企業活動を行うことは大変難しくなっています。しかしながら、情報セキュリティ対策については、中小企業は、大企業と比較して遅れが生じています。



中小企業の情報セキュリティ対策に関する研究会 報告書 H21年3月  
 経済産業省 「2008年度情報処理実態調査」データよりグラフ作成

情報セキュリティ対策は、情報システムに携わる担当者だけの仕事というより、経営者が率先垂範し、事務所全体として取り組む必要があります。万が一、情報セキュリティに関する事故、又は法令違反を生じさせると、会計事務所にとって重大な経営的影響を与えられてしまいます。

*Q.会計事務所で想定される情報セキュリティ事故にはどのようなものがあるのでしょうか？*

■人為的

ノートパソコンの盗難、USBメモリの紛失、パソコンの誤操作、職員による顧問先情報の不正持ち出し

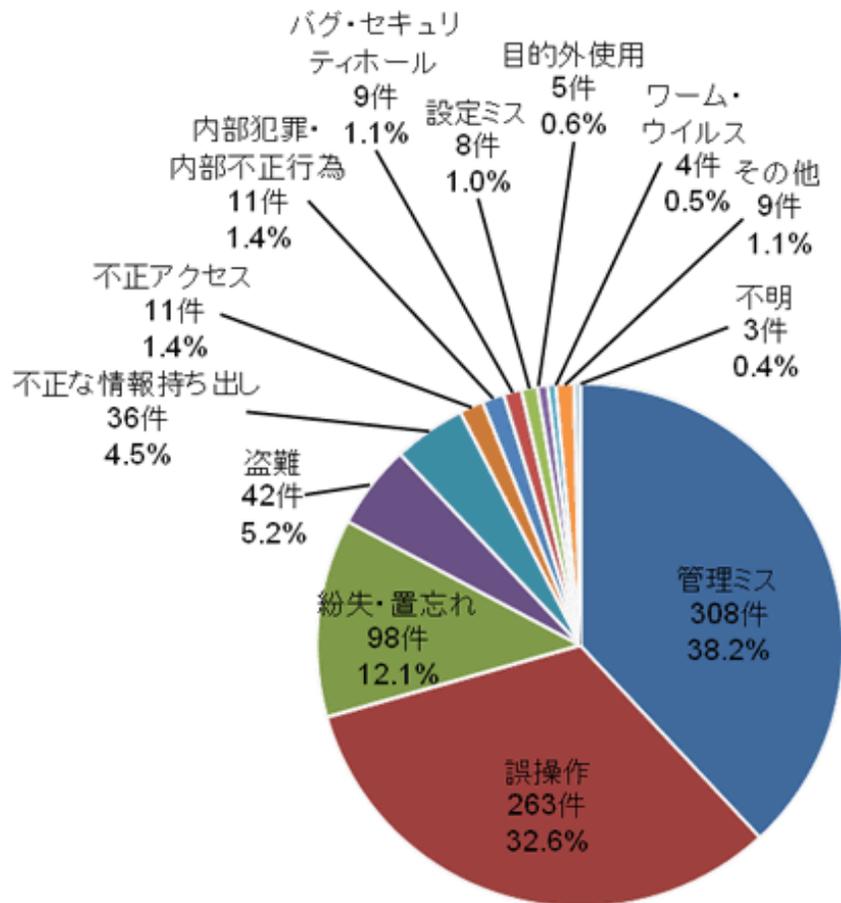
■自然的

地震、火災、水害、落雷

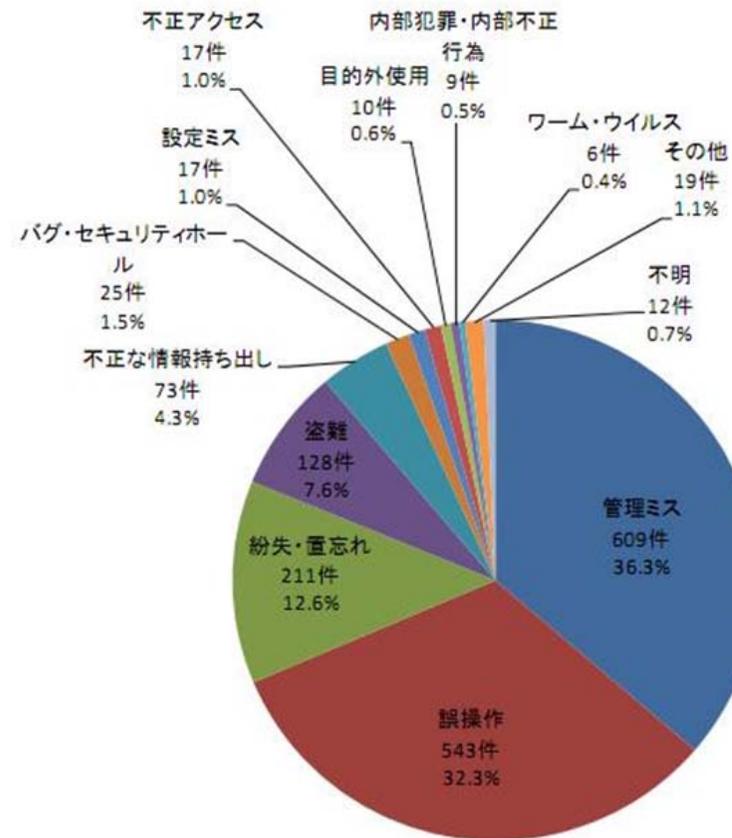
*Q.これらの情報セキュリティ事故が発生した場合、事態を収束させるまでにかかる時間とコストと影響は？*

金銭的負担（損害賠償金、見舞金、謝罪費、事故調査費用、裁判費用）  
社会的信用の低下・従業員の不安、不満・風評被害  
売上の減少（顧問先の解約、新規拡大の減少）



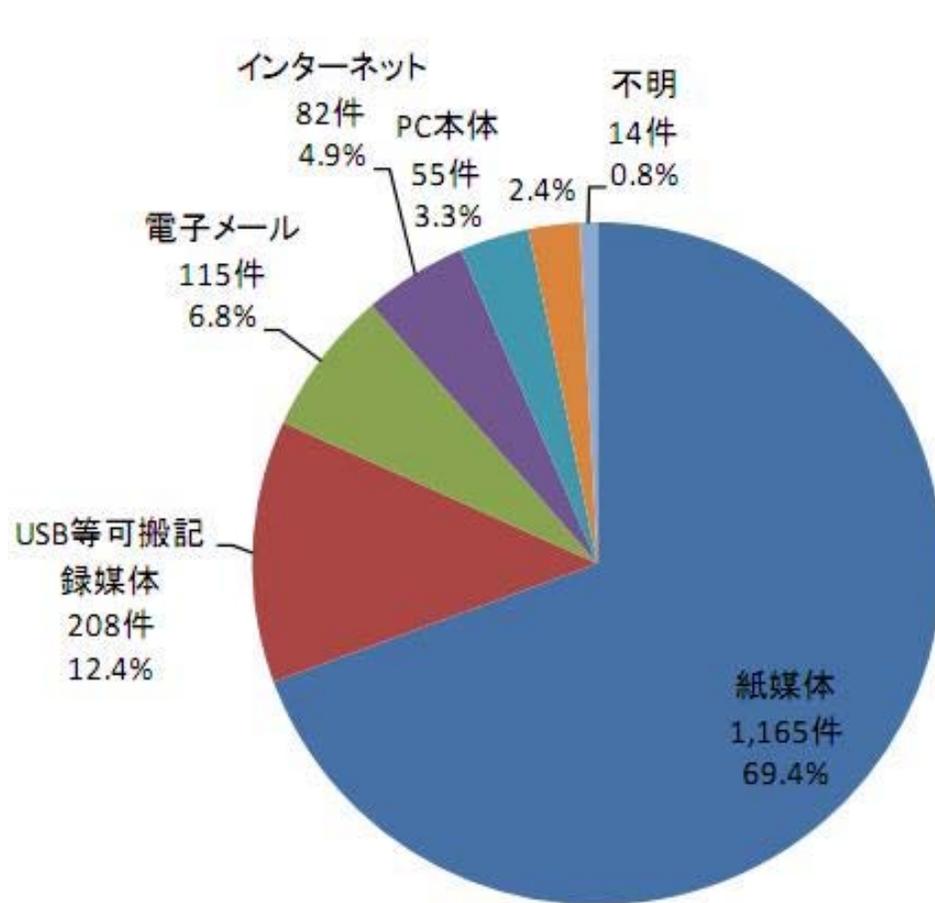


2011年度上期速報調査報告書

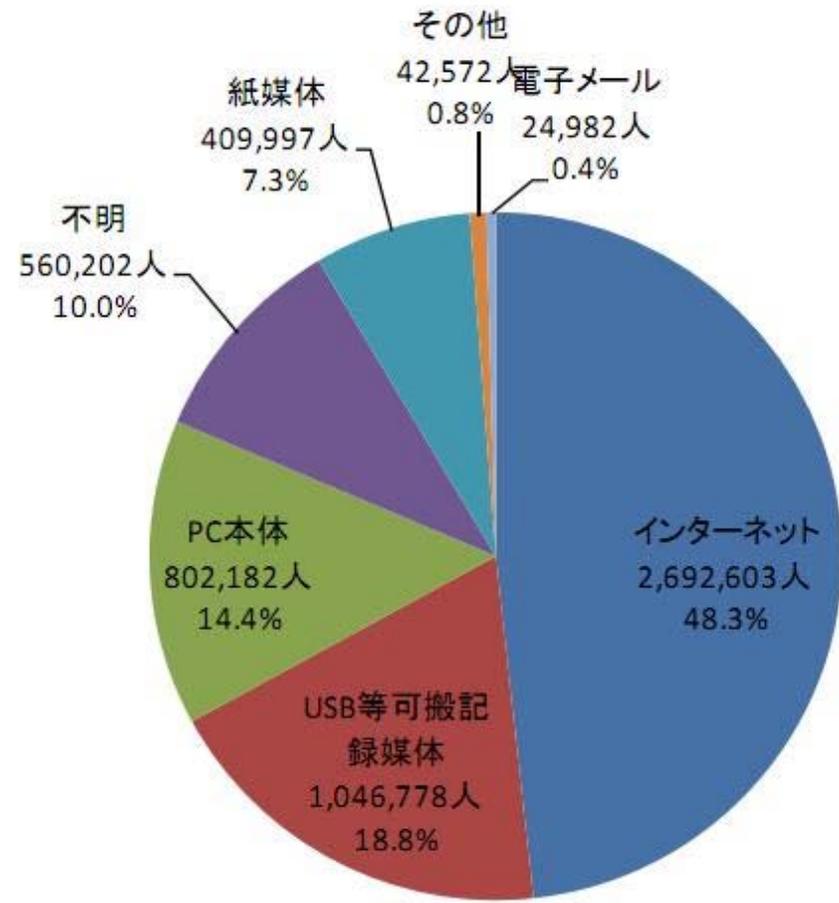


2010年度調査報告書

経路・媒体の件数比率（2010年）



経路・媒体の漏洩人数比率（2010年）



特定非営利活動法人日本ネットワークセキュリティ協会

1. 顧客の未公表の出店計画が記載されたメールを、事務所の職員が誤ってライバル企業に転送し流出させた。その結果、顧客が事業計画の変更を余儀なくされ、先行して行っていた設備投資について顧客から損害賠償請求を受けた。
2. 退職した職員が顧客の法人情報を持ち出し、転職先にその内容を流出させ、不正に使用して顧客から問い合わせがあった。このため被害法人に詫び状を送付するなどの事故対応費用が発生した。
3. 外部からの不正アクセスにより、メーリングリストに登録していた個人情報が見舞い品の購入費用が発生した。
4. 顧客名簿のデータベース化を委託した外部業者が情報を流出させたことにより、顧客の一部がプライバシーの侵害を理由に損害賠償を請求した。

株式会社 日税連保険サービス 税理士職業賠償責任保険 情報漏えい担保特約 パンフレットより

日本ネットワークセキュリティ協会（JNSA）は損害賠償として想定される金額の算出式を考案しました。この式は「損害賠償額算出式‘03」と呼ばれ、下記のように計算します。2003年に考案された算式で、何度か見直しも検討されましたが、実際の判例ときわめて近い金額が算出されているため、今も使用されている算式です。

$$\begin{aligned} \text{損害賠償額} &= \text{基礎情報価値 [500]} \\ &\quad \times \text{機微情報度 [10(x - 1) + 5(y - 1)]} \\ &\quad \times \text{本人特定容易度 [6,3,1]} \\ &\quad \times \text{情報漏えい元組織の社会的責任度 [2,1]} \\ &\quad \times \text{事後対応評価 [2,1]} \end{aligned}$$

精神的苦痛レベル（x）、経済的損失レベル（y）

年末調整のデータ100人分が漏えいした場合

$$500\text{円} \times [10(2-1) + 5(2-1)] \times 6 \times 2 \times 1 = \boxed{\phantom{000000}} \text{円}$$

$$\boxed{\phantom{000000}} \text{円} \times 100\text{人} = \boxed{\phantom{000000}} \text{円}$$

精神的苦痛レベル（x）、経済的損失レベル（y）ともに「年収」のレベル2を適用。

	精神的苦痛レベル1	レベル2	レベル3
経済的損失 レベル3	口座番号&暗証番号、クレジットカード番号&カード有効期限、銀行のアカウント&パスワード	遺言書	前科前歴、犯罪歴、与信ブラックリスト
レベル2	パスポート情報、購入記録、ISPのアカウント&パスワード、口座番号のみ、クレジットカード番号のみ、銀行のアカウントのみ	年収・年収区分、資産、建物、土地、残高、借金、所得、借り入れ記録	
レベル1	氏名、住所、生年月日、性別、金融機関名、住民票コード、メールアドレス、健康保険証番号、年金証書番号、免許証番号、社員番号、会員番号、電話番号、ハンドル名、健康保険証情報、年金証書情報、介護保険証情報、会社名、学校名、役職、職業、職種、身長、体重、血液型、身体特性、写真(肖像)、音声、声紋、体力診断、ISPのアカウントのみ	健康診断、心理テスト、性格判断、妊娠経験、手術歴、看護記録、検査記録、身体障害者手帳、DNA、病歴、治療法、指紋、レセプト、スリーサイズ、人種、地方なまり、国籍、趣味、特技、嗜好、民族、日記、賞罰、職歴、学歴、成績、試験得点、メール内容、位置情報	加盟政党、政治的見解、加盟労働組合、信条、思想、宗教、信仰、本籍、病状、カルテ、認知症、身体障害、知的障害、精神的障害、保有感染症、性癖、性生活

自然的な情報セキュリティ事故（地震・火災・水害・落雷）の発生に備えて、会計事務所においても事業継続計画(BCP: Business Continuity Planning)策定が必要です。

### BCP（事業継続計画）とは

BCP（事業継続計画）とは、企業が自然災害、大火災、テロ攻撃などの緊急事態に遭遇した場合において、事業資産の損害を最小限にとどめつつ、中核となる事業の継続あるいは早期復旧を可能とするために、平常時に行うべき活動や緊急時における事業継続のための方法、手段などを取り決めておく計画のことです。緊急事態は突然発生します。有効な手を打つことができなければ、特に中小企業は、経営基盤の脆弱なため、廃業に追い込まれるおそれがあります。また、事業を縮小し従業員を解雇しなければならない状況も考えられます。緊急時に倒産や事業縮小を余儀なくされないためには、平常時からBCPを周到に準備しておき、緊急時に事業の継続・早期復旧を図ることが重要となります。こうした企業は、顧客の信用を維持し、市場関係者から高い評価を受けることとなり、株主にとって企業価値の維持・向上につながるのです。

### DR（災害復旧）とは

DR（災害復旧）とは災害などによる致命的なシステム障害から情報システムを復旧させること。ないしはそうした障害復旧に備えるための予防的措置や機能、運用体制などのこと。

首都地域では、2～3百年間隔で関東大震災クラス(M8)の地震  
今後100年以内に発生する可能性はほとんどない。

元禄大地震 (1703年) M8.1 →→→ 220年 →→→ 関東大震災 (1923年) M7.9

ただし、その間にM7クラスの地震が数回発生している。

天明小田原地震 (M7.0)、安政江戸地震 (M6.9)、明治東京地震 (M7.0)

日本政府の地震調査研究推進本部  
30年間でM7の地震が起きる確立70%程度

東京大学地震研究所  
4年以内で50%以下、30年以内では83%以下

京都大学防災研究所  
5年以内に28%、30年以内に64%

## 東京湾北部地震M7.3を想定

(冬夕方18時 風速15m/s)

- ①建物全壊棟数・火災焼失棟数 約85万棟
- ②死者数 約11,000人

(冬朝5時 風速3m/s)

- ①建物全壊棟数・火災焼失棟数 約23万棟
- ②死者数 約5,300人

季節、時間、天候によって、火災による被害が大きく変わってきます。

南海トラフ地震 想定震度図

## 東海・東南海・南海連動型地震

2012年に想定震度が修正になりました。

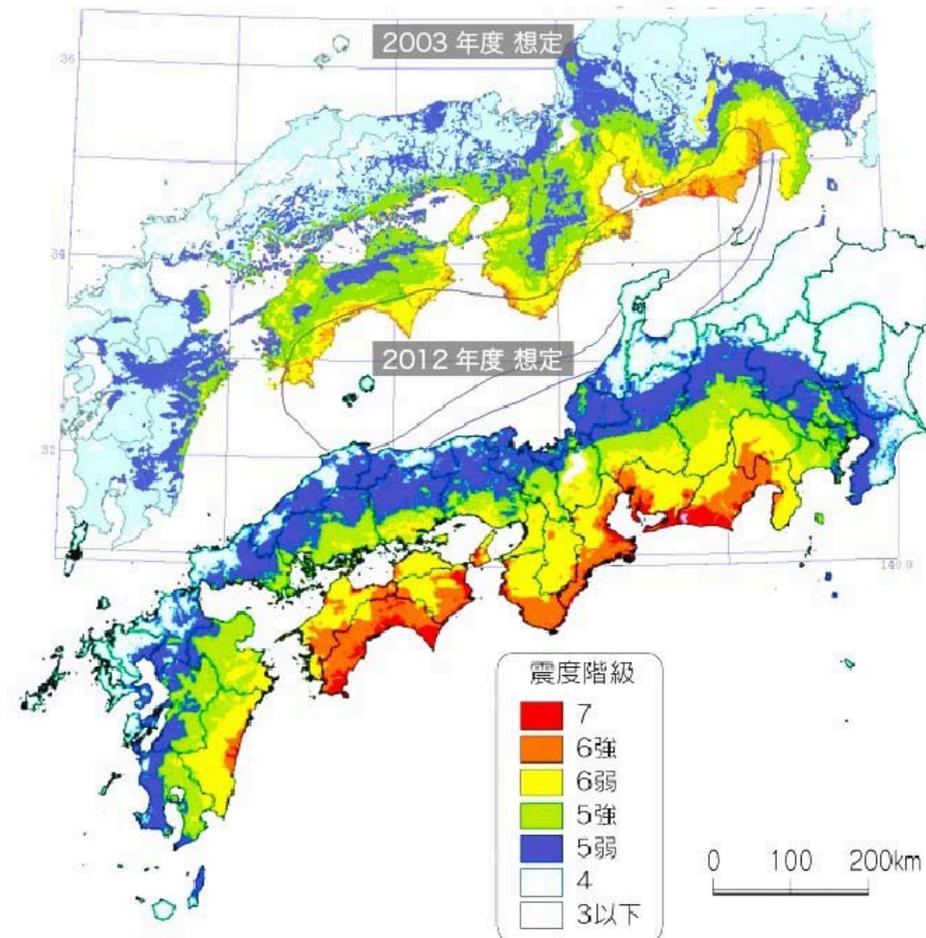
正式な被害予想は、8月下旬に内閣府から発表される予定ですが、作業部会の主査を務める関西大の河田恵昭教授は「死者が40万人に達する危険性がある」との試算を出しています。

河田教授の算定した津波の規模によると、大阪市内でもJR大阪駅（北区）や新大阪駅（淀川区）、市内のメインストリートの御堂筋や市役所（北区）も浸水域に入るほか、府咲洲庁舎（住之江区）や市営地下鉄、地下街にも大きな被害が出る事が予想されます。

### 南海地震

10年以内の確立 20%

30年以内の確立 60%



### 情報セキュリティ事故を起こさないために、会計事務所が取るべき行動

1. 教育を行う
2. ウイルス感染を防ぐ
3. 情報を持ち出さない
4. 電子化をする
5. バックアップを取る

「情報漏えいのパターン」で見たように、情報漏えいのかなりの割合が従業員の不注意やルールを守らなかったことによって起きています。

### 雇用契約時における非開示契約の締結

「非開示契約」とは従業者や外注先で当該情報を受けたものに対し、その情報を第三者に開示しない旨の義務を課す契約を言います。

### 従業者に対する教育・訓練の実施

従業者のコンプライアンス意識を高めるためには、定期的な教育・訓練の実施が不可欠です。

(参考)

中小企業情報セキュリティ対策促進事業のWEBサイトの活用

<http://www.jnsa.org/ikusei/>

無料のe-ラーニングや確認テストで、簡単な教育・訓練が行えます。

ウイルスに感染した場合、事務所のデータ破壊やデータ漏えいにとどまらず、感染が顧問先のパソコンにまで広がってしまう可能性があります。

### ウイルスに感染したときの症状

- **ファイル・データを削除される**  
データの消失、PCが起動しなくなる
- **ネットワークに負荷をかけるウイルス**  
ネットワークに負荷をかけ、感染していないPCもネットやメールができなくなる。
- **パソコンの動作が不安定になる、遅くなる**  
ウイルスはPCの使用環境を考えていないので、バグによる原因が多い。
- **ファイルをばら撒くウイルス**  
メールにエクセルファイルなどを添付して送りつづける。
- **個人情報を漏洩するウイルス**  
入力したキー情報（ID、パスワード、クレジットカードの番号など）を外部に送る
- **ホームページを攻撃するウイルス**  
ターゲットにされたホームページを閲覧不能にする。
- **バックドアを開けるウイルス（自分のPCをネット経由で他人に使われてしまう）**  
情報漏えい、犯罪に利用される（迷惑メールの送信元、ホームページ攻撃）

### 主なウイルスの感染経路

#### メールによる感染

不用意に添付ファイルを開かない  
閲覧するだけで感染するウイルスもある。

#### USBメモリによる感染

ネットにつながっていないPCが感染源  
ネットにつながっていないPCはアンチウイルスソフトのアップデートができないので感染しやすい

#### フリーソフトによる感染

フリーソフトにウイルスを混入される。  
フリーソフトはそのまま使えるので感染に気づかない。

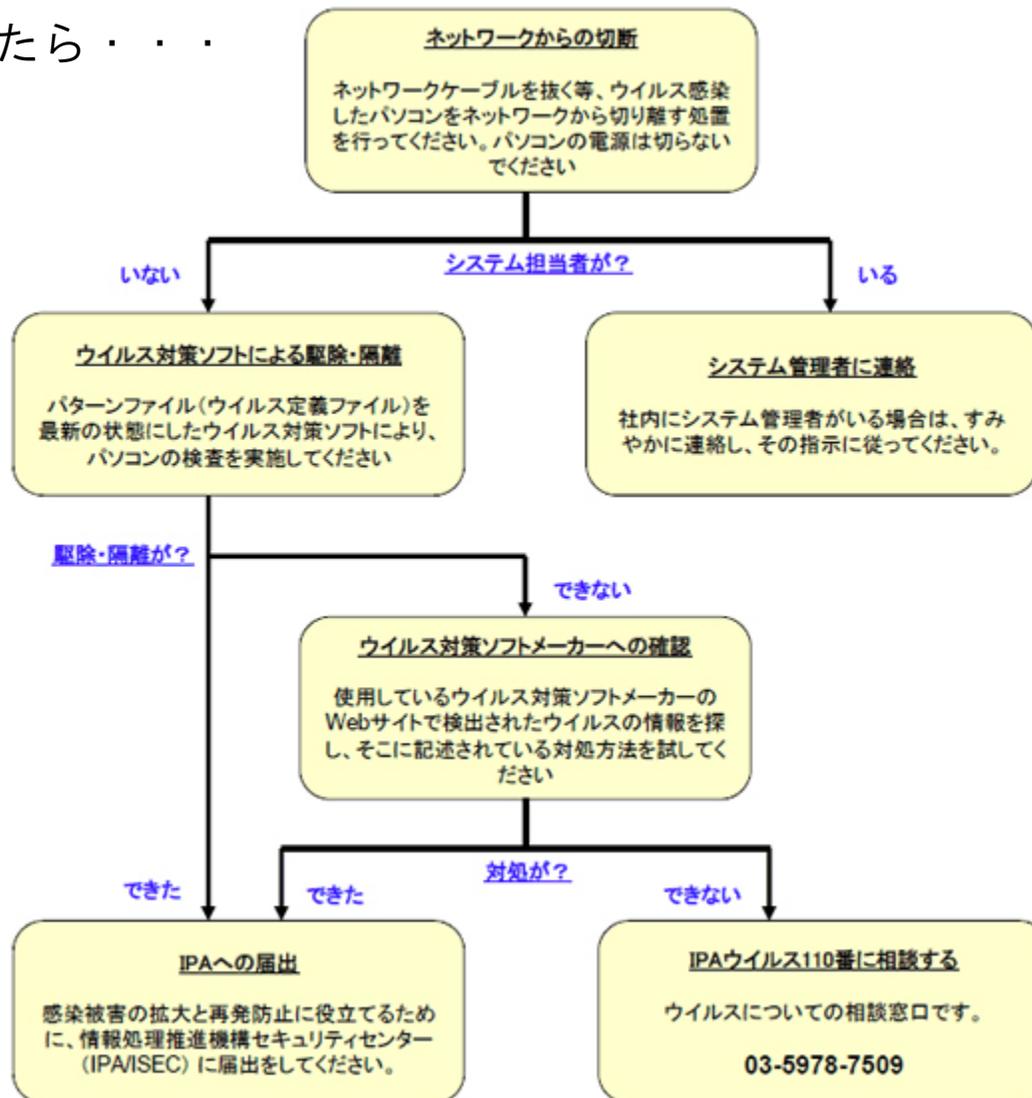
#### ホームページからの感染

ホームページを開くだけで感染するタイプもある。  
怪しいホームページを見ない。

特に目立つのがメールを介した感染です。

- ・メールの添付ファイルとしてパソコンに侵入する
- ・添付ファイルの実行により感染するが、感染したことに気付かない
- ・パソコンに登録してあるメールアドレスに、自動的にウイルス付きメールが送信される
- ・送信されたウイルス付きメールは記録が残らないため気付かない場合がある

もし、ウイルスに感染していたら・・・



[IPAへの届出](#)

# 【参考】 アンチウイルスソフト、検出率ランキング

アンチウイルスソフトは、すべてのウイルスを検出する訳ではありません！

順位	製品名	検出率	誤検出数
1	G DATA AntiVirus 22.1.0.2	99.70%	13
2	AVIRA Antivirus Premium 12.0.0.915	99.40%	15
3	Kaspersky Anti-Virus 12.0.0.374	99.30%	9
4	Sophos Anti-Virus 10.0	98.90%	14
4	F-Secure Anti-Virus 12.49.104	98.60%	4
4	Panda Cloud Free Antivirus 1.5.2	98.60%	10
4	Bitdefender Anti-Virus+ 15.0.36.1530	98.60%	4
4	BullGuard Antivirus 12.0.215	98.60%	5
4	McAfee AntiVirus Plus 11.0.654	98.60%	28
10	Fortinet FortiClient Lite 4.3.3.0436	98.50%	32
10	eScan Anti-Virus 11.0.1139.1146	98.50%	11
12	Webroot SecureAnywhere 8.0.1.95	98.20%	428
13	avast! Free Antivirus 7.0.1407	98.00%	14
14	ESET NOD32 Antivirus 5.0.95.0	97.60%	2
15	PC Tools Spyware Doctor with Antivirus 9.0.0.909	97.20%	22
16	GFI Vire Antivirus 5.0.5134	97.00%	79
17	AVG Anti-Virus 2012.0.1913	96.40%	38
18	Trend Micro Titanium AntiVirus Plus 5.0.1280	95.60%	166
19	AhnLab V3 Internet Security 8.0.5.19	94.00%	64
20	Microsoft Security Essentials 2.1.1116.0	93.10%	0

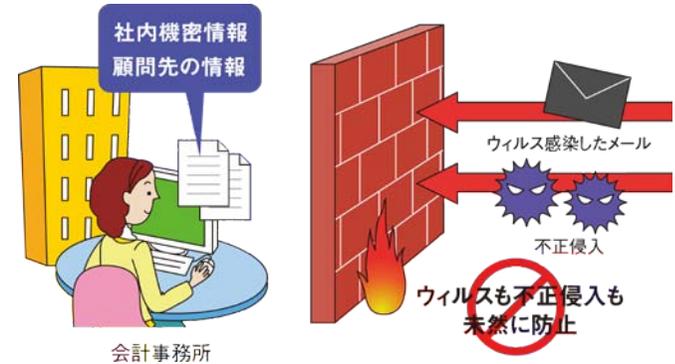
(AV-Comparatives, On-Demand Comparative March 2012)

順位	製品名	防御力	修復力	使いやすさ
1	Kaspersky: Internet Security 2012	6.0	6.0	5.0
2	BitDefender: Internet Security 2012	6.0	5.0	4.5
2	F-Secure: Internet Security 2012	5.5	5.0	5.0
4	G Data: Internet Security 2012	6.0	5.0	4.0
4	Symantec: Norton Internet Security 2012	5.5	4.0	5.5
6	AVG: Internet Security 2012	5.0	4.5	5.0
7	AVG: Anti-Virus Free Edition 2012	4.5	4.5	5.0
7	Avira: Internet Security 2012	4.5	5.0	4.5
9	Panda: Internet Security 2012	5.0	4.0	4.5
9	Trend Micro: Titanium Maximum Security 2012	5.5	3.0	5.0
11	BullGuard: Internet Security 12.0	6.0	3.0	4.0
11	GFI: Vipre Antivirus Premium 2012	5.0	3.0	5.0
11	Panda: Cloud Antivirus Free Edition 1.5.1	5.0	2.5	5.5
14	McAfee: Total Protection 2012	4.5	3.0	5.0
14	PC Tools: Internet Security 2012	4.0	4.5	4.0
14	Qihoo: 360 Antivirus 2.0	5.5	4.0	3.0
17	Avast: Free AntiVirus 6.0	4.0	3.0	5.0
17	K7 Computing: Total Security 11.1	4.5	3.5	4.0
17	Microsoft: Security Essentials 2.1	2.0	5.0	5.0
17	Norman: Security Suite Pro 9.0	3.0	4.0	5.0

(AV-TEST, Test Reports Nov/Dec 2011, Home user products)

## 【機能の概要】

- ・電子メール、ウェブサイト、USBメモリ等の可搬媒体からのウィルス感染をリアルタイムで阻止。
- ・外部からの不正アクセスを監視、遮断するファイアウォール機能を搭載。
- ・偽装されたウェブサイトの閲覧によりインストールされるスパイウェアやアドウェアのインストールをブロック。
- ・アプリケーションの社内、社外へのネットワーク通信に警告を表示し、ユーザが意図しない通信も遮断、コントロールが可能。



## 【特長1】

信頼性の高いエフセキュア社のアンチウイルスソフトを採用

## 【特長2】

1時間に1回、パターンファイルの更新を自動で参照するため、常に最新のパターンファイルでウィルス等の進入を監視します。

## 【特長3】

「達人シリーズ」を利用しているパソコンであれば、月額1,000円で何台でも利用可能です。

ウィルス感染や不正侵入からパソコンを守るための必須アイテムです。



情報を外部に持ち出した段階で、どんなに厳重な管理をしても100%安全ではなくなってしまいます。どうしても持ち出さなければならない場合の、きちんとしたセキュリティポリシーが重要です。

### 機密情報を印刷した用紙の管理

- 機密情報を印刷した用紙は、プリンタ、FAX、コピーなどで、裏紙として再利用しない
- 機密情報を出力機器に印刷した場合、すみやかに文書を自席に持ち帰るようにする
- 機密情報が印刷された用紙を廃棄する場合、細かく裁断し、鍵のかかるゴミ箱に入れ、[溶解業者](#)へ処理を依頼する

### CD、DVD、USBメモリ、SDカードの記録媒体の管理

- 私用の記録媒体は持ち込ませない
- 管理者の許可なく、自宅へ持ち帰るなど社外に持ち出さない
- 廃棄の必要がある場合、媒体を初期化したうえで、破碎してから廃棄する

### ノートパソコンにHDDパスワードを設定する

パソコンには、いくつかのパスワードがあります。代表的なものに、Windowsパスワード、BIOSパスワード、HDDパスワードがあります。

WindowsパスワードやBIOSパスワードはパソコン本体に設定されますが、HDDパスワードはHDDに設定されます。ですからHDDを抜き取って別のパソコンに接続してもパスワード入力が必要であり、その結果情報漏えいを防ぐことができます。

### ZIPファイルのパスワード機能の活用

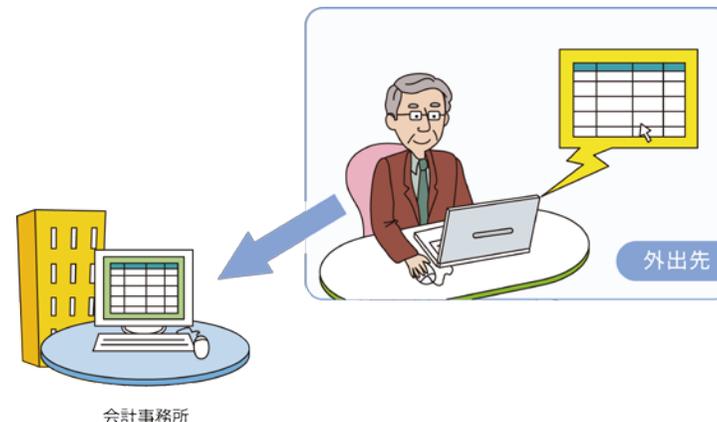
汎用性の高いZIP形式の圧縮ファイルには、パスワード機能があります。達人Cubeの「その他ツール」からも利用できますので、持ち出すデータにはパスワードを設定しましょう。

### ノートパソコンにデータを入れて持ち歩かない。

ファイルストレージを利用して、データはデータセンタに保管する。  
PC遠隔操作（リモートコントロール）を利用して、ノートパソコンは他のパソコンに繋げるだけにする。

## 【機能の概要】

- ・ 外出先や自宅のパソコンからインターネットを通じて、事務所内のパソコンに接続し、あらゆる操作が可能。
- ・ 遠隔操作側へのデータ転送やプリンタへの出力等の制御が可能。
- ・ 遠隔操作中に接続先のパソコン画面を非表示にする設定が可能。
- ・ 遠隔操作時のIPアドレスや接続時間の履歴を参照可能。



## 【特長 1】

遠隔操作中の通信は常に暗号化されており、通信経路での情報漏えいへの対策など、セキュリティは万全です。

## 【特長 2】

パソコンのロックを解除するために必要な「Ctrl+Alt+Del」キーの操作信号も送信可能。接続待機中のパソコンに対するセキュリティ確保も万全です。

## 【特長 3】

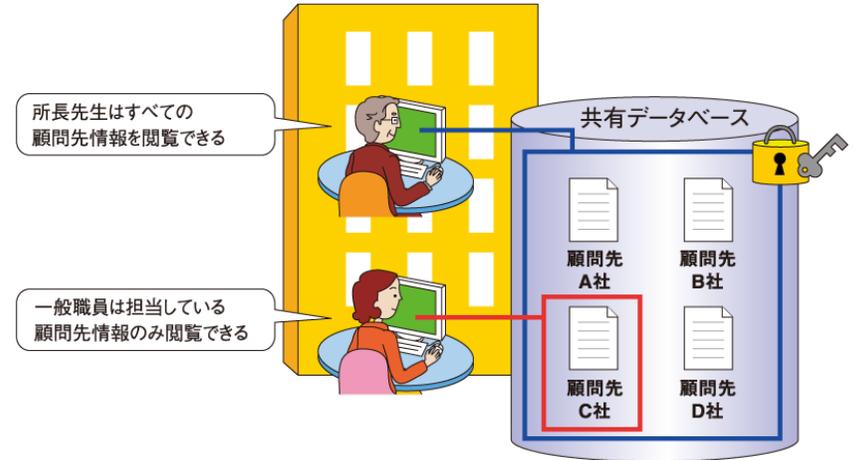
遠隔操作されるパソコンを1台単位で自由に設定できるのでニーズに合わせて無駄なくご利用いただけます。

パソコンや記録媒体(USBメモリ等)の紛失リスクを「発想の転換」により軽減できます。



## 【機能の概要】

- ・ サーバーに保存された「達人シリーズ」の申告データに対して閲覧制限を付与することができます。
- ・ 申告データ単位、データベース単位等で設定が可能。
- ・ ログ取得機能により、利用者名、接続日時、処理内容等を記録することが可能。
- ・ ウィザード機能により、画面の案内に沿って操作するだけで設定が可能。



## 【特長 1】

「達人Cube」にログインする際のアカウントによる権限管理で、専門的な知識がなくてもアクセス権限をコントロールできます。

## 【特長 2】

閲覧可能な申告データを制限することで、人為的なミスをもっと減らすことができます。

## 【特長 3】

アクセス権限の管理、ログの取得を行なうこと自体で、事務所内のセキュリティ意識を高めることができます。

事務所内で起こる「うっかり」ミスを未然に防ぐことができます。



職員の個人USBメモリを禁止して、暗号化機能、ロック機能、アンチウイルス機能のついたUSBメモリを貸与管理する。

※紛失や盗難に対するUSBメモリのセキュリティ対策には「暗号化」と「ロック」の2つがあります。

「暗号化」とはUSBメモリ内のファイルに暗号を掛けることでUSBメモリの中から情報を取り出されても内容を理解できなくする方法です。

「ロック」とはUSBメモリに鍵をかけてUSBメモリ内のファイルを見えなくする、つまり取り出すことができなくする方法です。

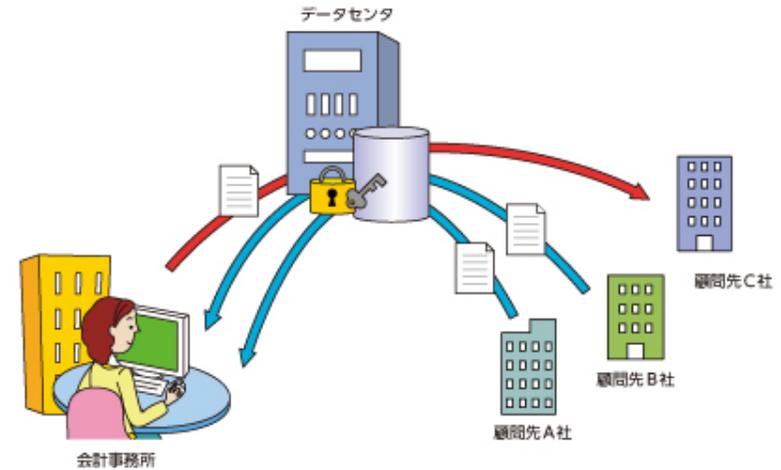
※アンチウイルス機能とはトレンドマイクロ社製「Trend Micro USB Security™ 2.0」が保存されるファイルをリアルタイムでウイルスチェック。ウイルスに感染したファイルがあると専用フォルダに自動的に隔離し、USBメモリを媒体としたウイルス感染を防止します。

### USBメモリの使用を原則禁止する

USBメモリは小さいので、ある程度職員のいる事務所では、一定の確率で紛失するリスクが生じます。また、高価なアンチウイルス機能付のUSBメモリを職員全員に貸与するには多額のコストがかかります。職員全員のUSBメモリを管理する手間を考えると、USBメモリはインターネットにつながっていない顧問先での限定利用とし、基本は、ファイル転送、パソコンの遠隔操作ソフトなどを利用し、USBメモリの使用を原則禁止とします。

## 【機能の概要】

- ・機密データや大容量のデータをカンタンな操作で安全に送信することが可能。（データセンタ経由での送受信）
- ・顧問先は「達人CubeMini」を事前導入するだけで、データの受取・送信操作が簡単に。
- ・メール配信機能により、ファイル送信と同時にメールでの配信通知が可能。
- ・履歴機能によりこれまでにファイルを送信した履歴も確認が可能。



## 【特長1】

あらゆる種類の電子データを1度に100MBまで転送できるので、USBメモリ等の可搬媒体の利用を減らすことができます。

## 【特長2】

ファイル転送時の通信はすべて暗号化されているため、安全にデータを送信することができます。

## 【特長3】

送信したファイルのステータス(ダウンロード済み、未受信等)が表示されるので、相手側の受取を確認することができます。



会計事務所内には、お客様からお預かりした大切な書類や過去の申告書など大量の紙媒体を取り扱っています。会計事務所以外の安全な場所に電子化された情報として保管しておくことが重要です。

Q.もし・・・紙媒体で保管していた場合、会計事務所の上階で火災が発生したらどうなりますか？

今までの紙媒体を一気に電子化するのは得策ではありません。まずはこれから出力する紙媒体を電子化しましょう。

電子化に必要なソフトウェアはAdobe Acrobat（36,540円）、DocuWorks（15,200円）などがあります。



DocuWorks 7

Document Handling Software

電子化することには以下のメリットもあります。

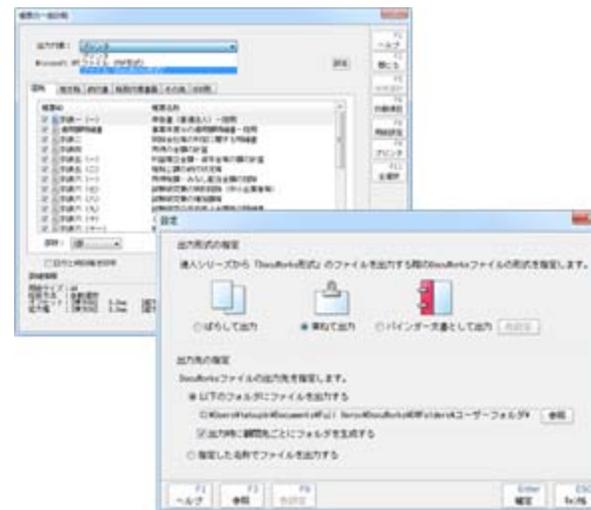
- ・ 検索が早くなる。
- ・ 閲覧制限をかけることができる。
- ・ 保管庫などが不要になる。
- ・ クラウド上に保管することができる。

## 【機能の概要】

- ・ 「達人シリーズ」で作成した帳票を「PDF形式」又は「ドキュワークス形式」で出力することが可能。

※ 「ドキュワークス形式」での出力には別途「DocuWorks®」（富士ゼロックス社製）のインストールが必要です。

- ・ 印刷と同様の操作でカンタンにPDFデータの出力が可能。



## 【特長1】

「達人シリーズ」の印刷操作と同じ操作で申告書等を電子データに出力することができます。

## 【特長2】

無償配布の「AdobeReader®」を導入するだけでカンタン・手軽に電子化をはじめることができます。

## 【特長3】

「DocuWorks®」等の電子文書管理ソフトの導入により、データの結合や抽出など、加工もできるようになります。



不慮の事故などにより大切な情報資産を失った（紛失・改ざん）場合、「バックアップ」さえ保存されていれば最悪の事態を回避することができます。ただし、折角保存している「バックアップ」もその取得方法により意味のないものになってしまいます。

### 保管場所の多重化

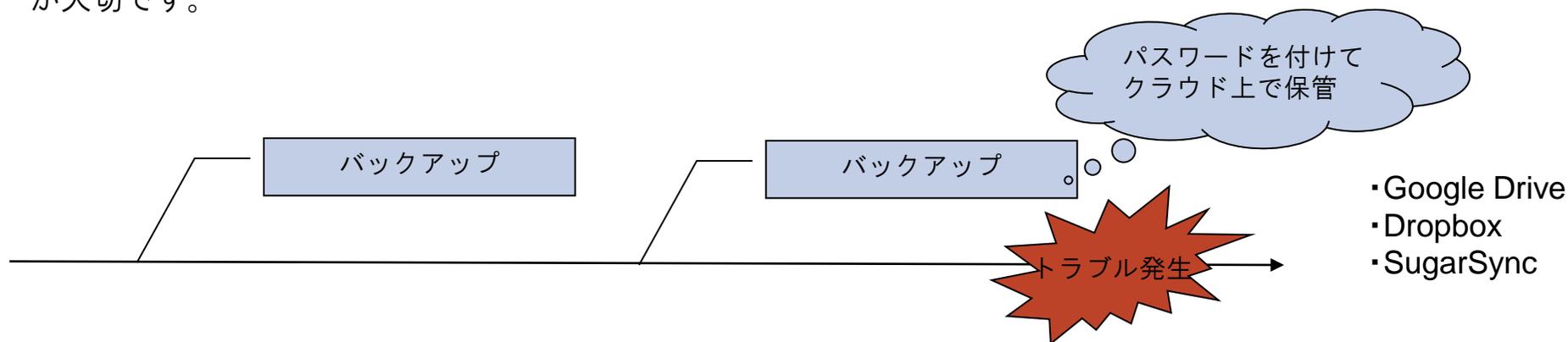
原本と同一の場所（コンピュータ、事務所）に保管していた場合、盗難・火災・災害等によりバックアップデータも消失してしまいます。原本とは別の場所且つ複数の場所に保管することで、よりリスクを低減することができます。

最近ではクラウド上で保管するサービスが多数あります。

### 保存時間の多重化

「バックアップ」の取得タイミングが直近であればあるほど、情報資産の消失や作業の手戻りを少なくすることができます。頻繁にバックアップを取得することが何よりも大切です。

しかし、直近の状態のバックアップのみの場合、情報資産の一部を消失または改ざんされた状態で保管しては意味がありません。理想的には数日から数週間程度のバックアップを重複して保持しておくことが大切です。



ヤフーの子会社であるファーストサーバ株式会社が提供するレンタルサーバーで約5,700社が預けていたシステムとデータが消失し、バックアップデータも含めてほとんどが復旧不可能となりました。

## ■ 障害の概要

6月20日（水）17時ごろ、脆弱性対策を特定のサーバー群に対して実施しました。

脆弱性対策は更新プログラムを利用して一括して対象とするサーバー群に対して実施するという運用を以前から行っており、今回も同様に作業を実施しました。

実施にあたっては検証環境において動作確認を行い対象サーバー群に問題が発生しないことを確認したうえで、本番環境で実施するという手順を取っております。

しかしながら、更新プログラム自体に不具合があったことに加えて、検証環境下での確認による防止機能が十分に働かなかったことと、メンテナンス時のバックアップ仕様の変更が重なり、今回のデータの消失（バックアップデータの消失を含む）が発生いたしました。

障害発生以来、弊社ならびに外部専門業者を交え、データ復旧を試み続けて参りました。しかしながら、極めて遺憾ではございますが、データ復旧を行うことは不可能と判断いたしました。誠に心苦しい次第ではございますが、お客様で取得されておられるバックアップデータによる再構築を行っていただきますようお願い申し上げます。 お客様のお手を煩わす事態となりましたことを、心よりお詫び申し上げます。なにとぞご理解を賜りますようお願い申し上げます。

（引用先：<http://www.fsv.jp/>）

## 【機能の概要】

- ・ 「達人シリーズ」で作成した申告データをまとめてバックアップすることが可能。
- ・ タイマー設定により、定期的にバックアップを取ることが可能。
- ・ 詳細な設定により、日付単位や週単位での取得、同一データの上書き設定などが可能。
- ・ ログの出力により、バックアップの成否なども監視が可能。

### 【特長1】

保存先は自由に参照が可能なので、ネットワーク上の他のパソコン等にカンタンにバックアップを取ることができます。

### 【特長2】

タイマーバックアップ後に自動的にパソコンの電源を切ることも可能。パソコンへの負荷を軽減することができます。

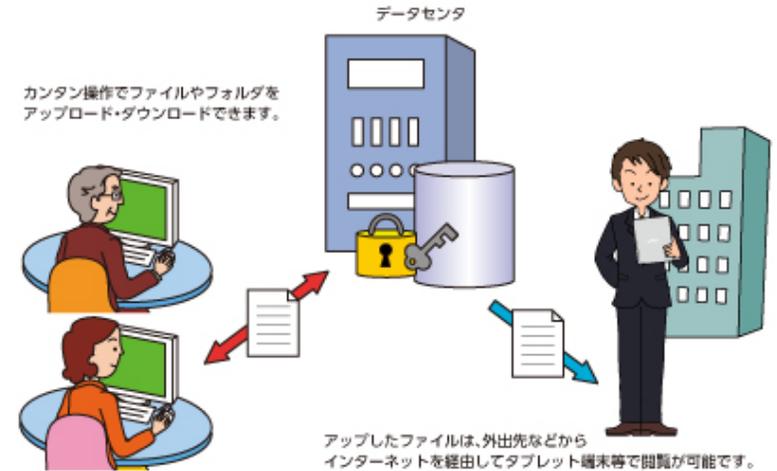
### 【特長3】

「達人Cube」をインストールするだけで無料で利用することができます。



## 【機能の概要】

- ・「達人シリーズ」のバックアップデータはもちろん、あらゆる電子データを外部のストレージに保存することが可能。
- ・ファイルのドラッグアンドドロップによるカンタン操作でデータセンタへのアップロードが可能。
- ・タイマー設定により、指定したフォルダ内のデータを自動的にデータセンタにアップロードすることが可能。
- ・外部閲覧用としてデータセンタにアップロードすることで、外出先でタブレットPC等でデータ内容を閲覧することが可能。



## 【特長 1】

データセンタへのアップロード・ダウンロードの際の通信は、SSL通信により暗号化され、セキュリティも万全です。

## 【特長 2】

データはNTTデータが運営するデータセンタに保管され、万全の体制で皆様のデータをお預かりします。

## 【特長 3】

抜群のコストパフォーマンスで「達人シリーズ」はもちろん、あらゆる電子データを保管することができます。



ご清聴ありがとうございました。

本日の研修会の内容に関するお問い合わせは

株式会社NTTデータ

公共システム事業本部

第二公共システム事業部

営業部 第三営業担当（税務サービスグループ）

中島 ・ 吉村 ・ 浜田

TEL：03-3214-4161

FAX：03-3214-4154

HP：<http://www.tatsuzin.info>



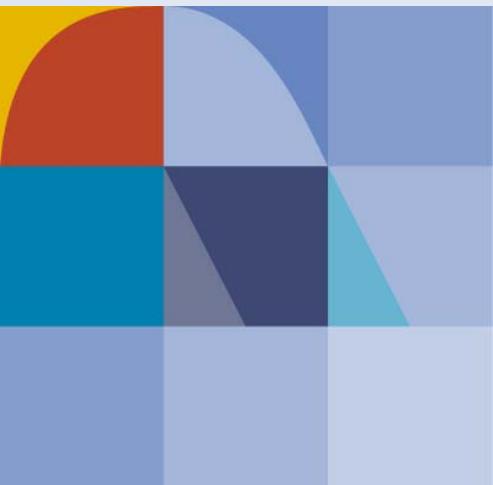
お問い合わせはお気軽に！



**0120-554-620**

達人インフォメーションセンター

受付時間：9:00～12:00 13:00～17:00  
土・日・祝日 および 弊社休業日を除く



# NTT DATA

変える力を、ともに生み出す。