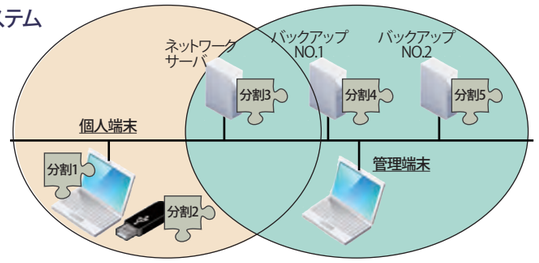
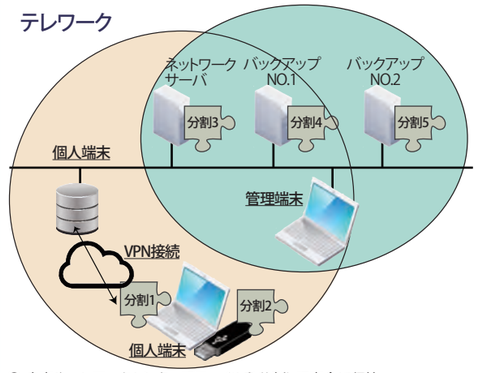
@割符を使ったソリューション事例

社内システム



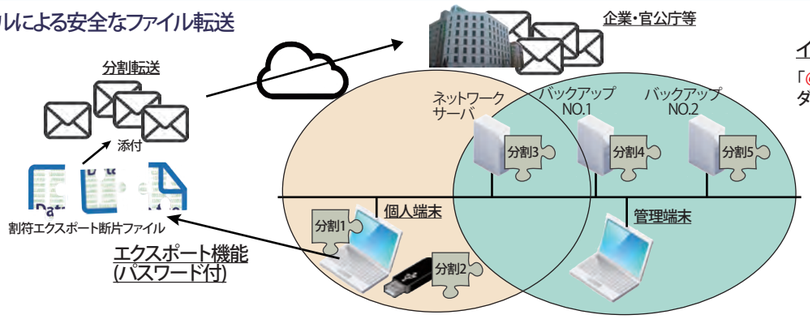
- 個人端末の分割対象ファイルに5分割(分割1から分割5)を行う。ただし、リカバリモードN－2での運用とする。
- 個人端末での復元時については、通常自分自身の分割1、USB等(分割2)、ネットワークサーバ分割3を用いる。
- 個人端末で障害等の発生時については、管理端末でバックアップ(分割3、分割4、分割5)を使用する。
- 分割3、分割4、分割5のどれかに障害が発生しても、分割1から分割5までの分割ファイルのうち3つで復元ができる。

テレワーク



- 自宅やテレワークセンターでファイルを分割して安全に保管。
- 社内管理端末にて割符からファイルを復元し、各個人の作業状況の把握が可能。

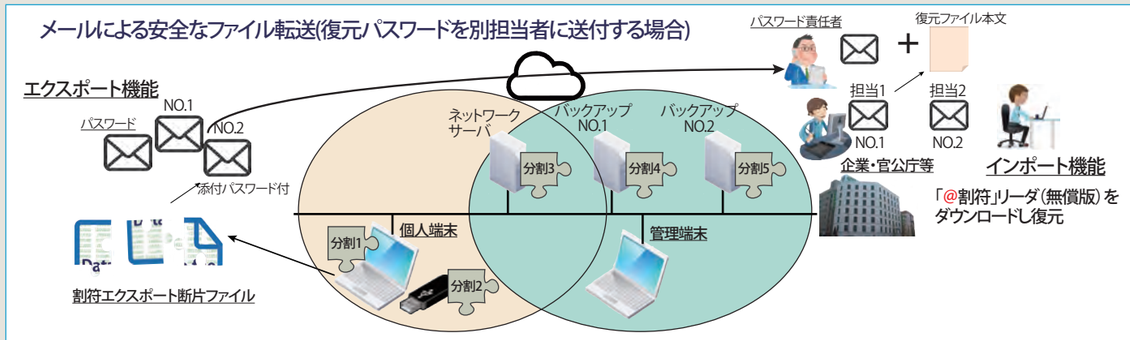
メールによる安全なファイル転送



インポート機能

「@割符」リーダ(無償版)を
ダウンロードし復元

メールによる安全なファイル転送(復元パスワードを別担当者に送付する場合)



システム要件

サポートされる オペレーティングシステム	Windows 7、Windows 8/8.1、Windows10
CPU	1 GHz以上のCPU
ハードディスク	1GB以上(割符をローカルに保存する場合は、格納するデータ量に応じた空き容量が必要です。)
メモリー	1GB以上(32ビット)または2GB以上(64ビット)

当製品に関する詳細はこちらから ▶ http://next-sharing.jp/@warifu/

開発元：Next Sharing Inc.
ネクスト・シェアリング株式会社
〒140-0004 東京都品川区南品川2-4-7アサミビル5階
[東京本社] TEL：03-6433-2340 FAX：03-5783-0734
[大阪事業所] TEL：06-6362-2007 FAX：06-6362-2008
[E-mail] info@next-sharing.jp

この製品のご用命は

Next Security Inc.

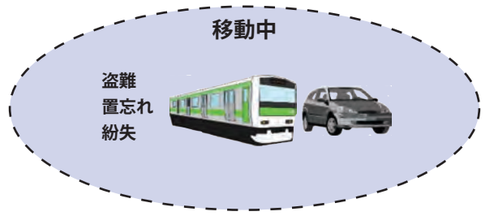
ノートPC等の端末やポータブルメディアの紛失／盗難による情報漏えいを防ぐ

秘密分散技術 @割符

ライフスタイルに沿った仕事のあり方が今後ますます多様化していくと考えられています。外出先や自宅、テレワークセンター等で仕事を行うには会社からデータを持ち出すことになり、この場合情報資産をどのように守るかというのがセキュリティ上の課題となっています。近年、セキュリティ対策の一環として、会社からのデータや端末等の持ち出しを規制している企業が多く見られますが、このポリシーのためテレワーク作業への影響や仕事の生産性の低下が懸念されています。このように本来は効率よく仕事をこなせたら良いと思うことが、セキュリティの観点から阻害されているというのが現状ではないでしょうか。
持ち出しを規制しても現実に管理することは難しく、仕事の効率化のために黙認せざるを得ないケースも少なくありません。このような実情が大きなセキュリティ問題に発展してしまう場合があります。それならば単に禁止するのではなく安全かつ確実な方法でデータや端末等を持ち出し、正々堂々と実務が遂行できる新しいソリューションを検討されてはいかがでしょうか。秘密分散技術「@割符」は、これらのセキュリティ問題を解決し、大切な情報資産の漏えいを防ぐ最適なソリューションです。

データ持ち出しの課題

端末を社内から持ち出すにあたり、移動中及び出先での端末紛失、盗難、その他の事故により、
重要データの漏えいが一番の課題となります。



移動中や出先での作業において、企業の重要情報の漏えいリスクが付きまといます。企業として、データ可用性の重要性は認識していますが、テレワークやデータの持ち出しを推進するまでには至らないのではないでしょうか。

情報の流失は、お客様へのご迷惑だけではなく、企業経営にも大きなインパクトを与えます。また事態の収拾には、
多大な時間、労力、費用が掛かります。

- 個人情報の漏えい→行政・刑事・民事等の法的責任、企業イメージの低下、取引の停止、社会的信用の失墜、謝罪広告、損害賠償等
- 営業情報の漏えい→信用低下、営業機会損失等
- 技術情報の漏えい→独自性(特許)・市場優位性の喪失、企業価値の低下、脅迫等

情報漏えいを防ぐ安全な移送方法とは

府省庁対策基準策定のためのガイドラインには、下記の具体的なデータ移送方法の例が提示されています。(項番 3.1.1(6)-2 b)

例：1個の電子情報について、分割された一方のデータからは情報が復元できない方法でファイルを2個に分割し、それぞれ暗号化を施した上で一方を電子メール、他方をDVD/USBメモリ等の外部電磁的記録媒体で郵送する方法が考えられる。

機密情報を電磁的媒体で移送するためには、必要な強度の暗号化に加えて、
複数の情報に分割して、それぞれ異なる移送経路を用いることが必要です。

@割符の特徴

- 産業技術総合研究所の安全性評価報告で、「電子割符技術の安全性は暗号技術の標準的安全性のレベルを大きく上回っていると考えられる」と報告されています。*
- ビット単位での分散処理により、原本を複数個の解読できない割符に分割します。
- 同じファイルを分割する毎に生成される割符が異なるため、以前の割符と組み合わせて復元に使うことはできません。
- 復元に必要な割符は、割符の全数(N)か、N-1、N-2から指定できます。
- ファイルを分割した時点で「データ」ではなく、単なる意味のないビット集合体の「ゴミ」となります。情報流出があった場合でも、復元に至らない数の割符ファイルの流出となるため、残りの割符が適切に管理されていれば、重大インシデントとはなりません。
- 指定フォルダにファイルを入れる等、Windowsの通常のファイル操作だけで自動で分割や復元ができます。
- スマートフォンと連携した強固な使用者認証機能を実装。

実装されている秘密分散技術（電子割符）はグローバルフレンドシップ（株）製のGFI電子割符®です。

＊産総研様との共同研究の第二期結果概要報告（2015年12月26日）

暗号化との違い

機密情報等の持ち出しには、そのファイルを分割して、それぞれを暗号化し、別の経路で移送することが求められます。

暗号化

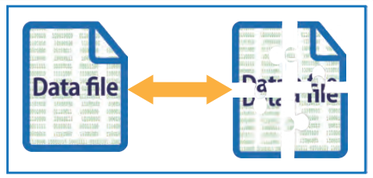
対象データを固定長のブロック単位で処理をする共通鍵暗号方式のDESやAES、異なる鍵を用いて暗号化処理をするRSA等は、

元データはその場に存在しており、実用的な時間内での解読ができないという**計算量**で安全性が担保されています。

今後高速な処理が可能になれば、鍵長等を拡大する必要があります。近年の製品で、暗号化処理を施した後に、分割する製品がありますが、あくまでも暗号化処理方式であるために、**計算量**での安全性担保製品としての位置づけなのです。

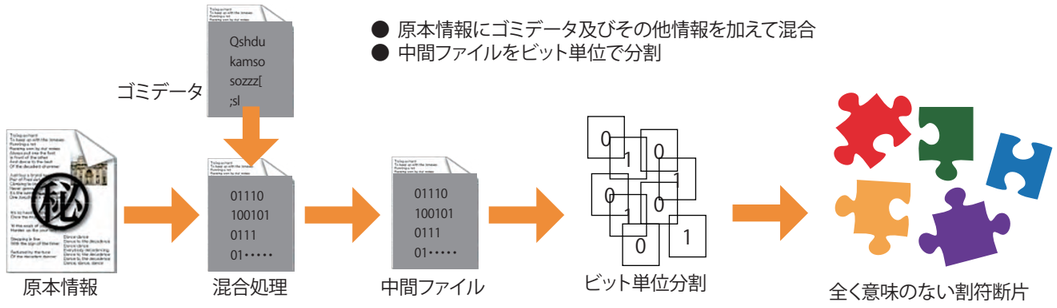
秘密分散技術(電子割符)

電子割符とは、原本データをビット単位でバラバラにして、さらにそのデータに意味のないデータを混ぜて、それを分割してデータの断片として保管するために、現状においては、実質上解読が不可能です。つまり暗号化の計算量での安全性担保に対して、電子割符は**情報量的**に安全性を担保しています。



暗号化されたデータが紛失した場合は復元が可能なため、その紛失は、重要インシデントとしての取り扱いになります。ただし、「@割符」で分割されたデータが紛失しても、単体では何の意味を持たないデータ集合体であるため、法令上の定義項に該当せず、訴訟(原告適格)になりません。また、重要インシデントとしての取り扱いにもなりません。セキュリティ対策としては実害が発生しない事はもちろん、法的にもクリアができる事が暗号化にはない秘密分散技術「@割符」の優位性です。

@割符の処理概要



- 原本情報にゴミデータ及びその他情報を加えて混合
- 中間ファイルをビット単位で分割

同じ原本情報に対し再度処理を行なっても、分割処理後の断片は絶対に同一にはなりません

主な機能

「@割符」では、ファイルを断片的に分割する際、原本データをビット単位でバラバラにし、それを分割することにより、情報量的な安全性を担保しています。操作性や管理機能を大幅に向上し、使用者に全く負担のない製品を開発しました。
さらに環境設定は使用者ではなく管理者のみが行えるため、社内セキュリティポリシーの推進も支援します。

使用者側の機能

割符基本設定画面

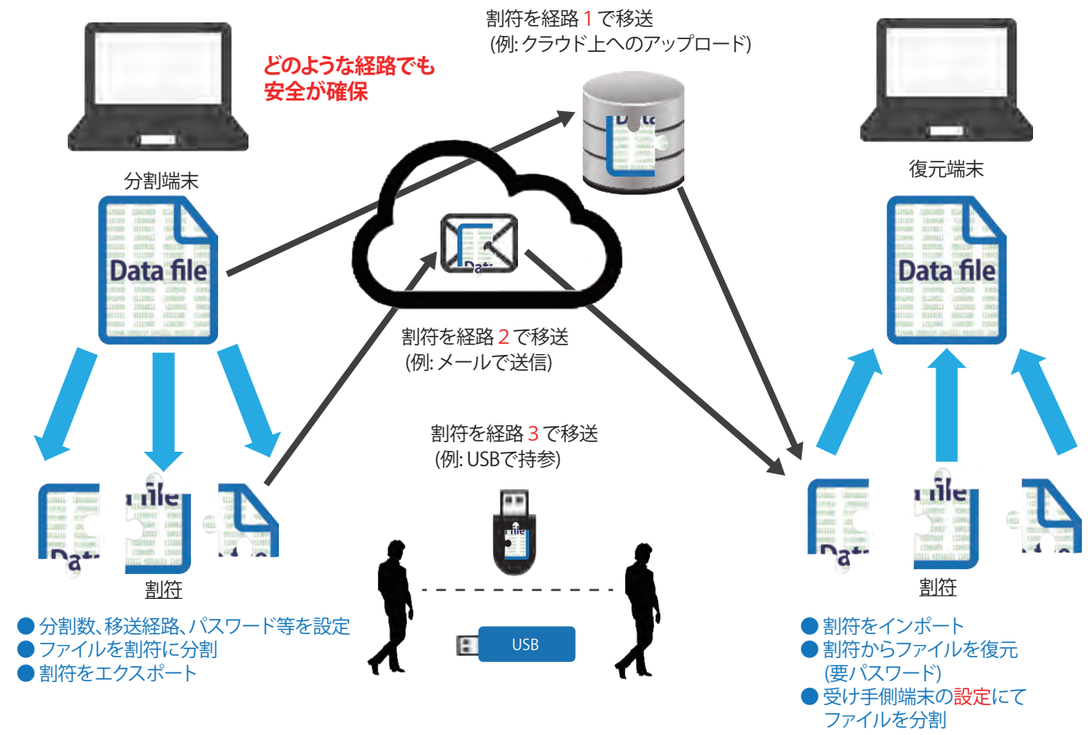
- ユーザーは、通常のWindowsのファイル操作で分割や復元が可能です。
- 割符は、Windows標準のファイル検索システムで検索ができます。
- ファイルの世代管理も可能です。
- 割符実行前の原本情報を自動記録するため、原本ファイルの名前、ハッシュ値、サイズ、パスがわかります。
- 割符を復元する前に、事前にファイルが復元可能かどうかを判別します。
- 暗号化ツールとも併用可能です。
- 端末がスリープ状態になると復元されたファイルを自動削除します。
- 割符のエクスポート及びインポートも簡単にできます。
- 割符実行後のファイルは自動削除されます。
- 割符履歴の閲覧ができます。
- ソフトの環境設定の表示ができます。

管理者側の機能

割符対象設定画面

- 割符の保存場所として、ボリュームやフォルダ(サブフォルダ含む)を設定できます。
- 割符の分割個数として2個から5個までの設定が可能です。
- 割符形式として、通常モード(すべての割符が復元に必要)とリカバリーモード(割符が1つまたは2つ無くても復元可能)から選択可能です。
- 割符様式として、データ均等割りの他に、一つの割符を最小容量にする「最小ファイルモード」を選択可能。最小の割符の容量は、全体の容量の約1/1000になります。
- 分割された割符にパスワードを設定可能です。
- 保存先を任意の場所に設定可能。例えば、ローカルドライブ、ネットワークドライブ、外部記憶装置(USB等)、FTPやWebDAVを利用したオンラインストレージ等が可能です。
- 割符条件設定として、任意の割符作業フォルダと対象拡張子を指定できます。
- 割符の保存用USBを登録できます。

ファイルのエクスポート及びインポート概念図



- 分割数、移送経路、パスワード等を設定
- ファイルを割符に分割
- 割符をエクスポート

- 割符をインポート
- 割符からファイルを復元(要パスワード)
- 受け手側端末の設定にてファイルを分割