Next Security Inc.

テレワークにおける情報セキュリティ対策の現状と解決策

・移送中の端末の紛失、盗難等における情報資産の流失等を防ぐには！
・電子割符ソリューションによるセキュリティ対策

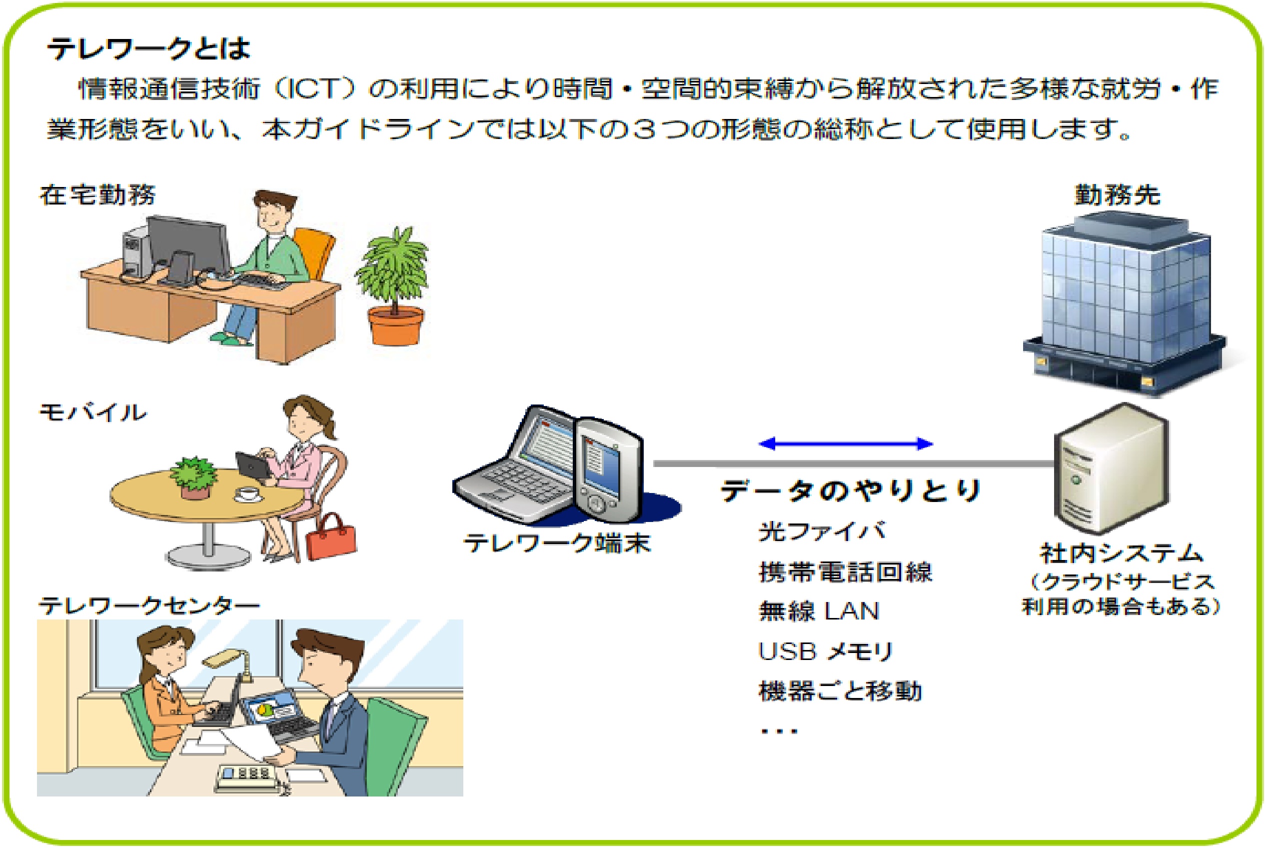
2016年12月9日

ネクスト・イット株式会社
ネクスト・セキュリティ株式会社

テレワークとは!

Next Security Inc.

情報・通信技術の利用により時間・空間的束縛から開放された多様な就労形態の事をテレワークと定義します。
尚在宅による就労に限らず、施設に依存しないモバイル型などの多様な就労・作業形態を総称します。(平成25年総務省発表資料を参考)



最近のテレワーク注目記事

Next Security Inc.

朝日新聞

近所のシェアオフィス 保育所付き

ベンチャーが開設 子供見える所で仕事

ガラス張りのオフィスから保育スペースに預けた子どもの様子が見える＝東京都世田谷区のマフィス馬事公苑

遠い職場ではなく近所のオフィスに出勤。同じ建物にある保育スペースに預けた子供の様子を横目で見ながら、電話やネットを駆使して仕事をこなす――。待機児童の解消が進まないなか、そんな働き方ができる仕事場を提供するベンチャーが現れた。「働き方改革」に力を入れる政府もこうした動きを後押しする。

「テレワーク」も可能

東京都世田谷区の閑静な住宅街。私設の美術館だったというビルの中に、認可外保育所を併設したシェアオフィス「マフィス馬事公苑」はある。

1階の30平方㍍余りの保育スペースに4人のスタッフが常駐し、10人ほどの子供を預かることができる。すぐ脇の階段を上った2階にあるガラス張りのシェアオフィスは19席を備え、無線LANや共用の複合機が使える。仕事の合間に、保育スペースにいる子供の様子をガラス越しにうかがったり、授乳しに行ったりすることもできる。

神奈川県内の設計事務所で主に戸建て住宅の設計を手がける野田景子さん(32)は、週4回前後利用する。自宅からマフィスまで自転車で15分ほど。ネットや電話でやりとりしながら社外で仕事をする「テレワーク」を認められている。

会社員の夫との間に近所の幼稚園に通う5歳の長女と、1歳半の次女。育休明けを前に次女をいったん別の認可外保育所に預けたが、自宅から電車とバスを乗り継いで1時間ほどかかった。子供2人の送り迎えの負担は重く、「これでは続かない」と判断。仕事に復帰した8月からマフィスを利用する。「次女はまだ一人で遊べないので、自宅では仕事に集中できない。ここなら通勤や子供の送迎にかかる時間を節約できるし、いつでも子供の様子が分かる安心感もある」

マフィスは2014年にオープンし、利用者は今は40人ほど。ウェブデザイナーやライターといったフリーランサーが多いが、野田さんのようにテレワークの勤め人も2割ほどいる。

「仕事はしたいけど、保育園に週5日まるまる預けるのは寂しいし、子供の成長ぶりも見たい。でも自宅では気持ちの切り替えが難しい。そんな人たちのニーズにこたえたかった」。不動産会社を辞め、マフィスを運営するオクシイ（東京都渋谷区）を創業した高田麻衣子社長(39)は話す。来年度中に首都圏で2カ所目を開く計画だ。

同じくベンチャーのママスクエア（東京都港区）も、保育スペースを併設した「サテライトオフィス」を東京都と埼玉、奈良両県の計8カ所で運営する。電話営業などを担当する自社のパート従業員が利用する施設が中心だが、契約先の企業の従業員を受け入れるオフィスもある。年度内に合計で十数カ所に増やす計画だ。

政府も普及後押し

共働き世帯の増加や介護離職の深刻化を受け、「多様で柔軟な働き方」へのニーズは強まる一方だ。働き方改革を目玉政策に据える政府は、場所や時間にとらわれずに働けるテレワークの普及策の検討を進める。その一環として厚生労働省は17年度、保育施設が近くにあるサテライトオフィスの導入を促すモデル事業を首都圏で実施する計画だ。すでにある保育施設の近所にシェアオフィスを設ける「近接・隣接型」を主に想定。運営は民間事業者に委託し、利用する企業を募る。18年度には他の地域にも広げたい考えだ。

通勤や子供の送迎の負担が大きいと、時短勤務に頼りがちになったり、仕事を辞めざるを得なくなったりすることもある。子供が病気になった時、すぐに対応するのも難しい。厚労省はモデル事業を呼び水に、マフィスやママスクエアのような「併設型」も含めてサテライトオフィスの普及を促し、子育てと仕事の両立を支援する方針だ。

（庄司将晃、末崎毅）

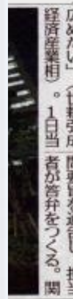
日刊工業新聞
THE NIKKAN KOGYO SHIMBUN
11月7日月曜日
2016年（平成28年）

国会質疑にテレワーク

経産省 残業大幅に削減

経済産業省は情報通信技術（ICT）を活用した在宅勤務などオフィスに依存しないテレワークを導入し、国会質疑対応で待機する職員の残業時間を大幅に削減する。ロボティック・プロセス・オートメーション（RPA）を活用した国会答弁集作成の高度化も検討し、いずれも2017年の次期通常国会からの本格導入を目指す。

AIで業務自動化 推進



〝国会待機〟の効率化は霞が関の国家公務員の長時間労働是正に有効。行政改革の目玉施策として「他省庁に広めたい」（世耕弘成経済産業相）。1日当たり数百時間の残業時間短縮につながりそうだ。

国会の委員会での質疑は、議員が事前に質問要旨を通告し、担当者が答弁をつくる。関係部局とのすり合わせが必要で、完成までに数時間を要する。通告が遅くなるほど、残業が増え、深夜に及ぶこともある。質問数によっては数百人が待機する。翌日は早朝から大臣との「答弁勉強会」（通称）を実施するため、担当者の負担は重い。

こうした国会待機での長時間労働是正に向けて、経産相はテレワークを活用する。開会中の臨時国会から一部導入した。

強固なセキュリティーを持つクラウド環境を構築。担当者はそれぞれ答弁を書き込む。世耕経産相がタブレット端末からアクセスし、自宅などで〝予習〟。追加で必要となるデータや疑問点を入力し、担当者が応じる流れだ。従来、2時間程度を要していた朝の答弁勉強会を数十分程度に短縮できた。

次期通常国会以降、答弁作成に全面的にテレワークを導入する意向。まずは関係部局の担当者間の協議にテレビ会議などICT利用を進める。

また、ロボット、人工知能（AI）技術でホワイトカラー業務の自動化を推進する。労働力の移動を通じ就業構造の転換を促すとされるRPAも使う方針。過去の国会答弁データベース（DB）をAIに学習させ、最適な回答を導き出す。経産省の一連の取り組みは霞が関の働き方改革として注目されそうだ。

テレワークのメリットと懸念事項

近年は、インターネットの高速化や、多様するライフケアスタイル、少子・高齢化対策、経済再生、雇用創出等の様々な目的での利用効果が認められていますが、情報セキュリティ(盗難、情報漏洩、機器管理等)の懸念する事項も多々あり、企業としても必要性は認めるが、中々これらのセキュリティ対策問題等で、テレワークを推進できていないのが現状である。

・ライフスタイルに沿った就労形態の変化(在宅勤務等)
・少子・高齢化に伴う労働力確保
・企業の競争力強化(時間、場所等に捉われない就労形態)
・世界的においても、テレワーク就労は、今後益々推進される。

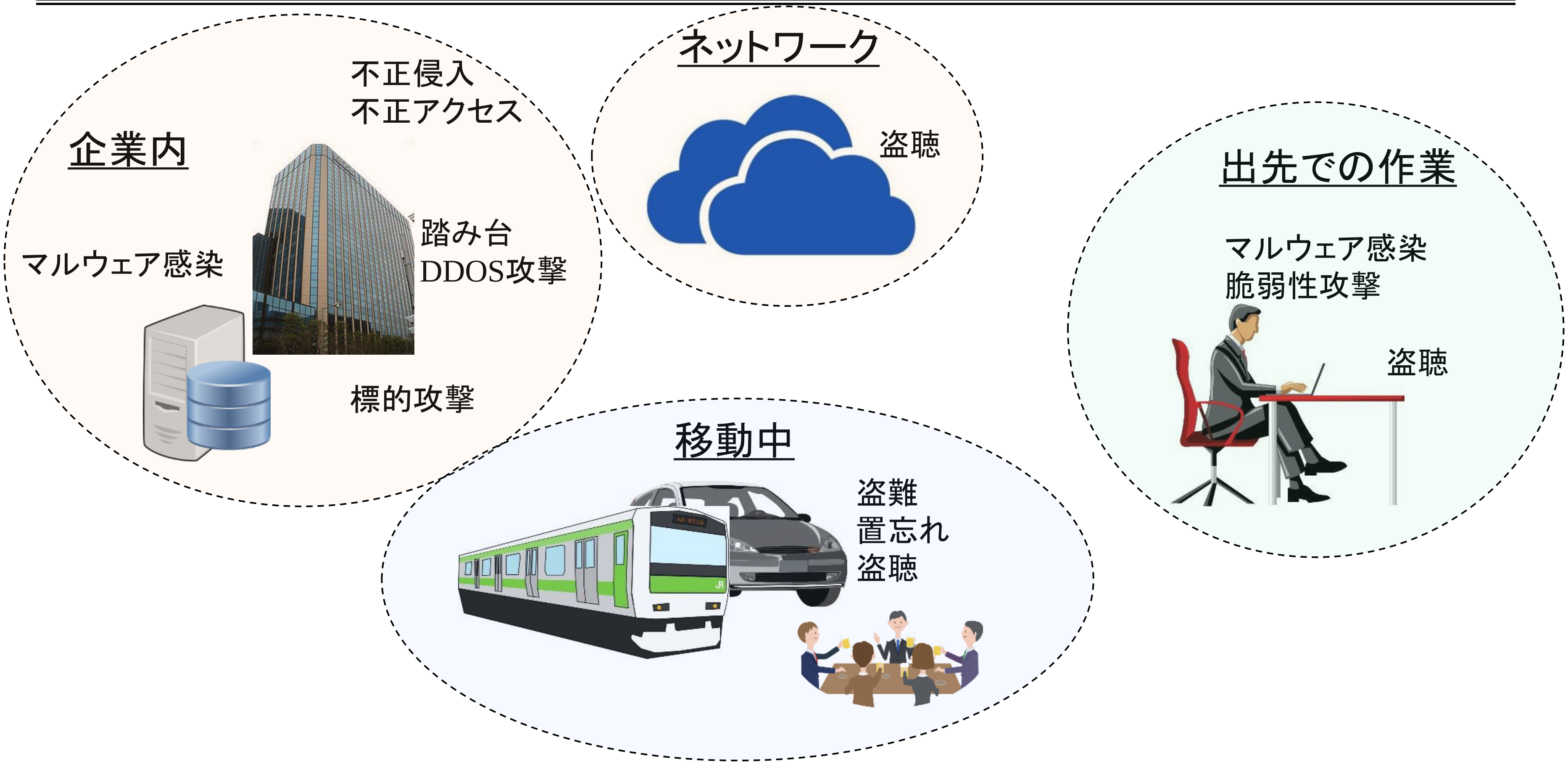
懸念事項

・情報漏洩、盗難等のセキュリティ対策は!
・情報資産の管理対策
・使用機器の管理対策(脆弱性、ウイルス対策等)

企業の情報資産管理、使用ルールの設定、教育、確実なセキュリティ対策が必要

セキュリティの脅威

Next Security Inc.



様々な脅威から、重要資産の漏洩、データ消失、事業継続不可等に繋がる。

セキュリティ脅威対策

テレワークでの作業を行なうには、企業及び使用者のセキュリティ対策が必要である。

企業/情報システム

・情報セキュリティポリシーの設定
・情報資産の分類とリスク回避
・使用ルールの設定と指導
・使用者に対しての教育
・最新のセキュリティ対策(パッチ、ウイルス対策等)
・原本保全対策(バックアップ等)

テレワークに関する事項の見直し及び対応策が不可欠です。

使用者

・設定ルールに沿っての運用
・情報セキュリティの理解(教育、啓発等)
・端末の脆弱性対策(最新パッチ、ウイルス対策等)
・端末の紛失、盗難に対して万全の対策
・情報資産に対しての安全性強化(暗号化等)
・パスワード管理の徹底
・インシデント発生時、早期の報告と対応等

教育、啓蒙及び使用者のセキュリティに対しての自覚が重要です。

テレワーク作業の内容

Next Security Inc.

テレワーク作業パターン

1. **端末持ち出し(オフライン)**

   USBメモリやパソコン等に電子データを格納して、作業場所(在宅、お客様党)で作業を行なう。

2. **端末持ち出し(オンライン)**

   電子データ等は、社内から持ち出しはせずに、作業場所(在宅、お客様等)で社内システムに接続して、データをダウンロードして作業を行なう。

3. **シンクライアント**

   端末等から社内システムに接続して、データのダウンロード等はせずに、社内システム上での閲覧、編集等を行なう。

どのパターンで在っても、情報管理、機器･情報等の移送問題が重要課題です!

端末及び情報を消失、盗難対策について

テレワーク作業での一番の懸念点は、端末の社内より持ち出すに当たり、移動中及び出先での作業中での端末消失、盗難、その他の事故により、社内の重要データの漏洩、消失等が一番の課題点と考えます。

移動中

盗難
置忘れ
盗聴

出先での作業

マルウェア感染
脆弱性攻撃

盗聴

移動中、出先での作業中において、社内の重要情報の流失リスクから企業として、可用性の重要性は理解出来るが、現状ではテレワークを推進するに至らないのが、企業の本音ではないでしょうか!

パソコン等の置き忘れ、盗難等の事例

Next Security Inc.

・県立高校長が、電車の中に、299人分のデータが入ったパソコンを置き忘れ・・・・・
・顧客情報含むPCを電車に置き忘れ紛失　ヤマハ　2016年9月16日
・図書館の利用者情報19万件含むPCが所在不明　秋田市　2016年10月12日
・職員が持ち出しデータを酒に酔って紛失　川口市　2016年10月8日
・医師が患者情報を紛失(USB)　広島病院　2016年7月15日
・車上荒らしで個人情報含むPCなどが被害　筑波大　2016年7月6日

近年の上記の様な不注意でのPC置忘れ、盗難事例は、多々多く見られる。この様に理由は様々であるが、その如何を問わず個人情報が流出したら、当然会社の管理責任が問われるだけでなく、損害賠償民事訴訟等が起これば賠償金を支払う事になります。
また会社の重要な機密情報等の流出も企業に取っては、大きな問題に発展する事は明白であり、充分なセキュリティ対策が必要である。

Next Security Inc.

(3) 漏えい原因 ※

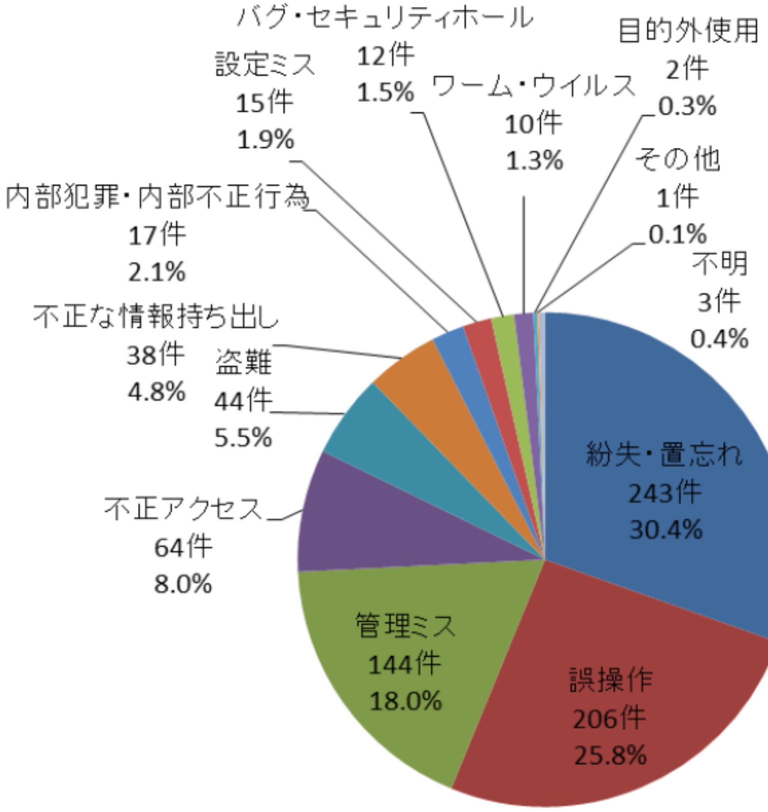


図 3：原因別の漏えい件数

出展:日本ネットワークセキュリティ協会
2016年6月17日

個人情報漏洩インシデント(2015年速報)

(4)　漏えい媒体・経路

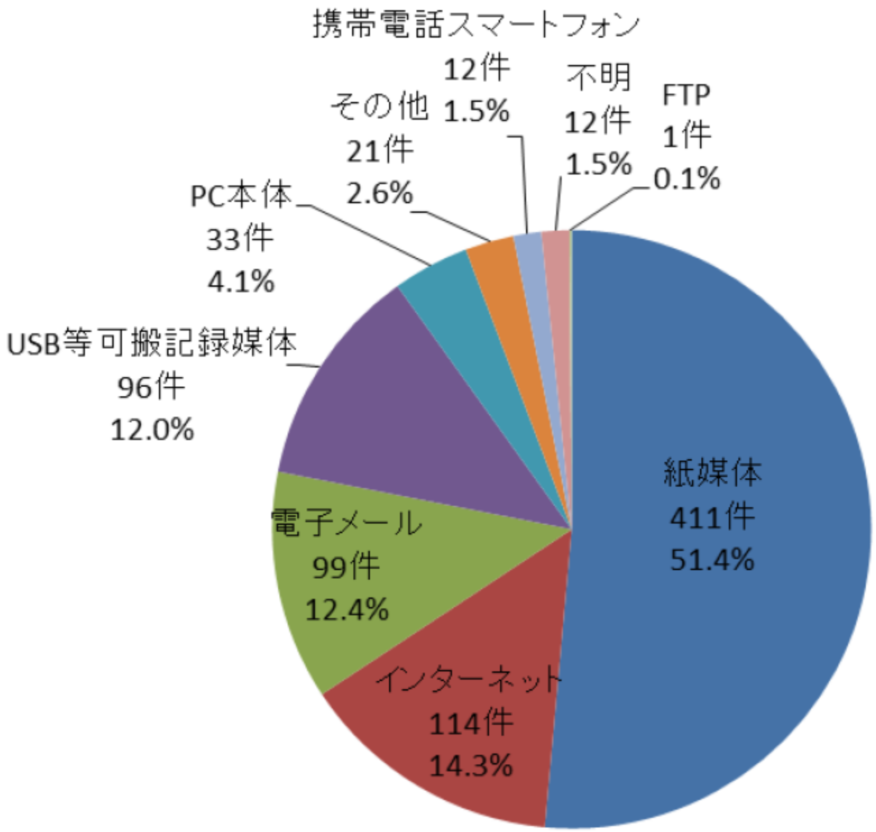


図 4：漏えい媒体・経路別の漏えい件数

出展:日本ネットワークセキュリティ協会
2016年6月17日

情報を移送する場合の懸念事項

Next Security Inc.

安全に移送する前提条件

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。

懸念事項

テレワークで在宅、お客様等での作業に於いても、端末に元データを保管したまま移送することは、移動中の端末紛失、盗難等の観点から情報漏洩等のリスクがある。

現状の企業対応(端末等の持ち出しについて)

- ・ライフスタイルの変化等で効率的な作業を行ないたいが、セキュリティ面で・・・・・・・
- ・お客様でのプレゼン等には、必要不可欠だが、管理面で・・・・・・・・・・・
- ・端末等の移送時に於いての、消失、盗難等のリスクを考えた場合・・・・・・・・・・
- ・ルール等が明確にない為に、また運用についても明確に取り決めが・・・・・・・・・

可用性については、良く理解が出きるが、情報漏洩、管理面でのリスクが心配!

表面上は、禁止している企業が多くあるが、実態については・・・・・・・・・・

情報漏洩を防ぐ安全な移送方法は!

移送中に於いて情報漏洩等を防ぐ方法としては、移送中に情報を持ち歩かない、故にテレワークのパターン3のシンクライアント方式が有効である。
しかし全ての企業でこのシンクライアント方式で行なう事は、設備、端末、回線等懸念事項から難しい問題がある。

その解決方法は!

府省庁対策基準策定のためのガイドラインより抜粋
(平成28年8月31日)

- **基本対策事項 3.1.1(6)-2 b)「複数の情報に分割し」について**

例えば、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。

秘密分散技術に関するNISC資料
(内閣官房情報セキュリティセンター)

Next Security Inc.

府省庁対策基準策定のためのガイドラインより抜粋
(平成28年8月31日)

- **基本対策事項 3.1.1(6)-2 b)「複数の情報に分割し」について**

例えば、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。

「**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**」

この様な記述では、実際にどのような技術等を用いれば要件を満たすのかが分からないので、NISCに対して問い合わせを実施(2016年9月26日)

NISCからの回答

1.府省庁ガイドラインは本来中央府省庁向けのものであるが、各自治体や民間等が参考として対策をおこなうことに制限を加えていない。
2.具体的な対策検討の際に、NISCの既公開ガイドライン等を参考とする事に制限を加えていない。

秘密分散技術に関するNISC資料

(内閣官房情報セキュリティセンター)

Next Security Inc.

政府機関の情報セキュリティ対策のための統一基準解説書より抜粋
(2005年12月版)

【強化遵守事項】

（c）行政事務従事者は、要機密情報である電磁的記録を移送する場合には、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。

解説：情報を分割し、これを異なる経路で移送することを求める事項である。
要機密情報を移送する場合には、当該要機密情報が情報量的に解読不能となるように、分割して移送を行うこと。
この考え方は、専門用語で秘密分散技術といわれ、例えば、１個の電子情報についてファイルを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 CD-ROM 等の媒体で郵送する方法が挙げられる。

秘密分散技術に関するNISC資料
(内閣官房情報セキュリティセンター)

Next Security Inc.

(b) 情報システムセキュリティ管理者は、要安定情報を取り扱うサーバ装置については、サーバ装置の運用状態を復元するために必要な措置を講ずること。

解説：サーバ装置の運用状態を復元するための必要な措置を講ずることによりサーバ装置に保存されている情報及びその情報を用いたサービスの可用性の担保を目的とした事項である。

サーバ装置の運用状態を復元するための必要な措置の例として、以下のようなものがある。

・サーバ装置の運用に必要なソフトウェアの原本を別に用意しておく。

・前回内容からの変更部分の定期的なバックアップを実施する。

・サーバ装置を冗長構成にしている場合には、サービスを提供するサーバ装置を代替サーバ装置に切り替える訓練を実施する。

・バックアップとして取得した情報からサーバ装置の運用状態を復元するための訓練を実施する。

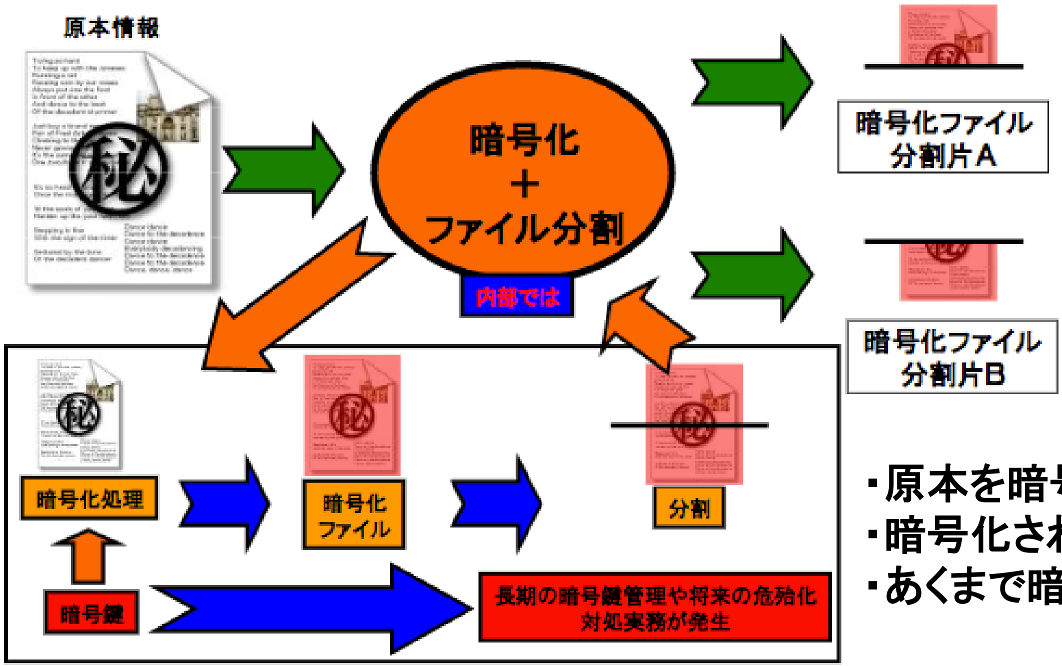
また、取得した情報を記録した電磁的記録媒体は、施錠された保管庫に保存等して、業務上の必要がある場合にこれらの情報を利用する情報システムセキュリティ管理者に限ってアクセスできるようにする。

なお、災害等を想定してバックアップを取得する場合には、記録媒体を耐火性のある保管庫や耐震性の高い施設、同時被災しない遠隔地にある施設に保存することが考えられる。その際には、情報を遠隔地に送信や移送する際のセキュリティ及び取得した情報の保管時のセキュリティを確保する必要がある。セキュリティを確保する措置の例としては、暗号や秘密分散技術を利用して情報の漏えいや改ざんを防止することが挙げられる。

<u>政府機関の情報セキュリティ対策のための統一基準解説書より抜粋
(平成24年度版)</u>

安全に端末等の情報を守るソリューション例

暗号化分散方式の処理概要



注：原本情報を暗号化＋ファイル分割で、単純に2つの暗号化ファイル分割片を生成した概念図です。

- 原本を暗号化処理をする。
- 暗号化されたファイルを分割する。
- あくまで暗号化ファイルとしての取り扱い

暗号化されたファイルを分割で大丈夫か?

Next Security Inc.

NISTの指針の通り、暗号化を行いファイルを分割して移送できる仕組みには合致するが、暗号化は解読不可能ではなく、解読される可能性がある為に、もし事故が発生した場合には、この様な仕組みであっても、重要インシデントとして取り扱う必要がある。

暗号とは、どの様な暗号であっても、キーに基にしてファイル等を解読不可能なデータに置き換えるが、キーの解読は必ず出来るので、確実に安全とは言い切れない!

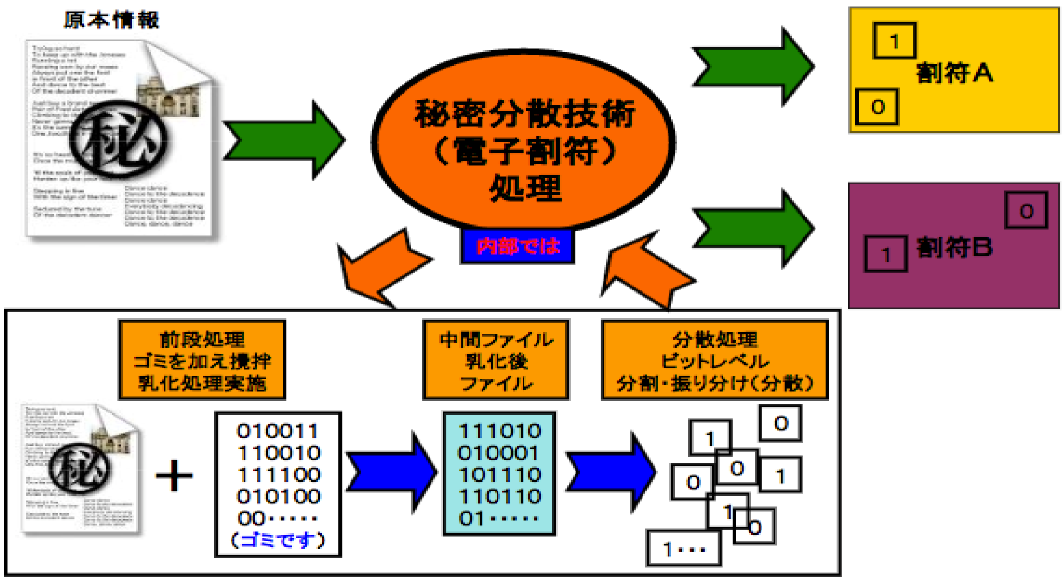
解読出来ないデータとは!

ファイルの内容をビット単位でばらして、意味不明なデータ配列として、そのデータを複数個のデータの集合体に分割する。このことにより、その単体に分割されたデータ集合体からは、基のファイル等の内容については、判別不可能となります。
故にもしこの分割されてデータの集合体が流失しても、重要インシデント事故としての取り扱いにはならない!

このソリューションが電子割符システムです。

電子割符とは!

電子割符方式の処理概要



注：原本情報を秘密分散技術（一般名称：電子割符）で、単純に2つの割符ファイルを生成した概念図です。

・原本をビット単位で拡散して、様々な情報を加えて処理を行い、その後ビットレベルで分割・振分けを行なう。

・分割・振分けしたデータの集合体単体では、全くファイルとしての軌跡を持っていない。
<u>分割単体での解読は不可能です。</u>

電子割符の特徴(GFI社)

Next Security Inc.

特徴

・原本をビット単位で、電子的分散処理を行なう。
・分割した容量は、ほぼ原本の総容量と同じです。
・同じファイルを再び分割しても、絶対に同じ分割データにはならない。
・偏差を付けて、割符に大、小の割符が可能、分割した個数の一つのみです。
(最小割符は、1/1000まで可能)
・原理的には、原本情報のデジタルデータの並びが一切残存しません。
・異なるOS間でのデータ互換性があります。
(Win,LINUX,Mac,IOS)
・分散した時点で、ファイルではなく、単なるデータ集合体として取り扱い。(ゴミ)

↓

もし情報漏洩をした場合にも、何かのデータが漏洩したのみであり、
重要インシデントとする必要が無い。

情報をに移送中の事故から守る!

Next Security Inc.

最良の提案

今までの端末等に情報を入れて、在宅、お客様でのプレゼン等に使用するが、もし情報消失、盗難、その他の障害があっても、情報漏洩もない、データ消失しても、重要インシデントとしての事故扱いも必要のない方法での移送であれば、テレワークの推進をもっと加速出来ると確信をします。

1.重要な情報は、解読不可能なデータに変化させて、分割して移送をする。
(例として、3分割した場合、移送する端末、USB,ネットワーク上等)
2.その分割したデータを現地で使用するときに復元をする。
(例としては、端末+USB Or ネットワーク上)
3.現地での作業終了したら、自動的に解読不可能なデータになります。

故に移送途中での盗難、置忘れ等による端末の紛失でも、例の様な3分割であれば、USB+ネットワークからデータの復元は可能です。
また各割符単体での情報漏洩事故であっても、単なるゴミデータが外部に流失したのみであり、重要インシデントとしての事故扱いにはなりません。
当然何らの訴訟問題になる事は有りません。

個人情報漏洩が発生した場合のリスク

Next Security Inc.

平文

平成27年02月20日経済産業省確認

組織等が個人情報を管理するに当たり、何ら技術的安全管理措置を施さずに情報漏洩をした場合には、重大なインシデントとして、法的処置等の・・・・・・・・・

暗号化

組織等が個人情報を管理するに当たり、高度な暗号化を施していても、その暗号化情報が漏洩した場合は、重大なインシデントとしての取り扱いとなる。

割符化

組織等が個人情報を管理するに当たり、秘密分散技術を用いた情報の一つの情報が漏洩しても、個人情報漏洩してのインシデントは発生しない。

法的有効性について（割符化）

1.法令上の定義項に該当しない
2.訴訟(原告適格)にならない
3.重大インシデントとしての取り扱いにならない

→

セキュリティ対策としては、実害が発生しない事は当然ながら、法的にもクリアが出来る事が、暗号化にはない電子割符の優位性です。

電子割符ソリューション(メタセパレータ)

Next Security Inc.

開発コンセプト

ライフスタイルの変化に伴い、今後必要不可欠になるワークスタイル(在宅、ワークセンター、お客様等)に必要不可欠なファイル移送中の事故(盗難、消失、情報漏洩等)を防ぐ為に開発するセキュリティ対策ソリューション製品です。(製品名:メタセパレーター)

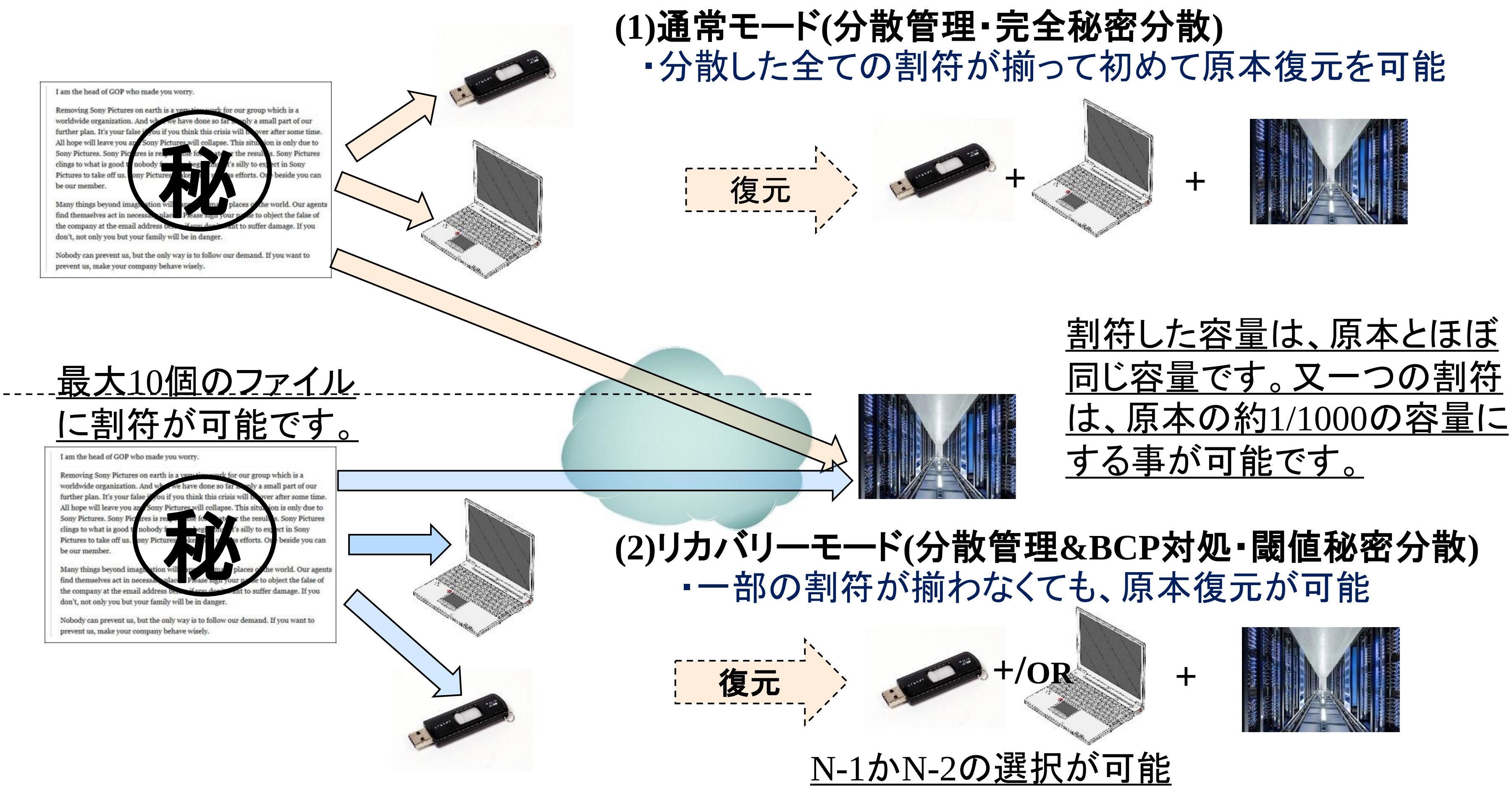
機能

・電子割符を使用して、原本を数個(2ー10)の解読出来ないデータ集合体に分割する。
・様々な機能設定が簡単な操作で可能とする。(最小集合データ作成、保管場所、パスワード等)
・原本ファイルは、分割後ローカルシステムから削除する。
・復元は、全てのデータ集合体、Nー1、Nー2とする。
・分割個数の一つの集合体を最小集合データとする機能とする。
(最小集合データとは、原本の 約1/1000)
・原本ファイルの確実な管理徹底する。(ハッシュ等)
・操作ログを確実に管理する。
・安全性をより一層確保する為に、分割集合体にもパスワード設定を可能とする。
・なるべく簡単な操作でアペレーションミスを誘発しない様なシステムとする。
・分割集合データの詳細内容の表示機能を備える。
・分割した集合データを他のシステムへの転送機能を備える。
・出先等で、復元したファイルは、PC等のスリープ状態になった場合、復元ファイルを削除する。

メタセパレータ(電子割符)の概要

Next Security Inc.

電子割符技術とは、デジタルの原本情報を特殊な処理技術を用いて、原本情報自体をビットレベルで分割することにより、割符単体では原本情報に復元する事が原理的に出来なくする技術です。



秘密分散(電子割符)と暗号化の相違点

Next Security Inc.

	電子割符方式	暗号化方式
原本管理	原本管理については、ユーザに依存するが、今回開発APLでは、動作PC上では削除する。	原本については、ユーザ依存管理
ファイル容量変化	原本ファイルの容量とほぼ同一容量、尚　割符を実行した割符ファイルの一つだけは、原本ファイルの約1/1000の容量に出来る。	AES128bit暗号時のファイル容量は、Officeファイルで4%の増加但しPPTファイルについては、36%から84%の増加します。
難解度	同じファイルを分散後、同一ファイルを分散しても、分散ファイルは、全く別の内容ファイルとなる。故に解読復元する事は、分散ファイルの復元プロセス以外では、解読不可能です。	同一ファイルを暗号化を同一キーで行なった場合は、全く同じ内容の暗号化ファイルとなる。難解度は、キーの長さにより左右されます。故に悪意を持っての復元は可能です。
管理面	ファイルを分散する時には、一切のキー等が不要、分散ファイルのみを管理する。	ファイルを暗号化するには、必ず暗号キーが必要であり、そのキーを安全に管理する必要があります。今後のコンピューターの性能向上に基づいて、キー長を大きくする必要がある。
法的な取り扱い	もし分割されたファイルの紛失であっても、単にごみデータが流失したとの判断であり、重要インシデントとしての取り扱いが不要の為に訴訟等のリスクがない。	暗号化されたファイルであっても、ファイル紛失等が発生した場合には、重要インシデント流失としての取り扱いになり、法的訴訟等が起きる可能性はあります。

暗号化を否定している訳ではなく、暗号との相互補完関係で、より一層のテレワークセキュリティを確保

メタセパレータ(秘密分散方式)のデモストレーション

開発コンセプト

・安全なテレワークの推進ツールの開発！
・簡単で取り扱いやすく、管理を最小限に！
・テレワークツールとしてのデファクト化を目指す！

デモンストレーション①
電子割符数2個

Next Security Inc.

割符を行い持ち出す場合

持ち出したいデータ

個人情報.csv
（約70KB）

メタセパレータで
２つに電子割符化

・ファイルの参照
・ドラッグアンドドロップ
・右クリックメニューから選択
（※α版では未実装）

割符①

？？？？？？？
？？？
（約40KB）

ローカル
ディスク

割符②

？？？？？？
？？？？
（約40KB）

割符されたデータは意味のないビットの並びになっている為、どのようなアプリケーションでも情報として読み取ることができません

また、作成される割符データのサイズは、オリジナルデータよりも一つ一つは小さくなります。（※表記しているサイズは目安です）

デモンストレーション①
電子割符数 2個

ext Security Inc.

復元を行い閲覧する場合

持ち出したデータ

個人情報
.csv
（約70KB）

メタセパレータで
２つの電子割符から情
報を復元

・アプリケーション上でダブルクリックして開く（ローカルディスク上には展開されません）

割符①

？？？？？？
？？？？
（約40KB）

ローカル
ディスク

復元する為に必要な、割符されたデータがそろっているため、メタセパレータ内で復元・閲覧することができます。

割符②

？？？？？？
？？？？
（約40KB）

デモンストレーション①
電子割符数 2個

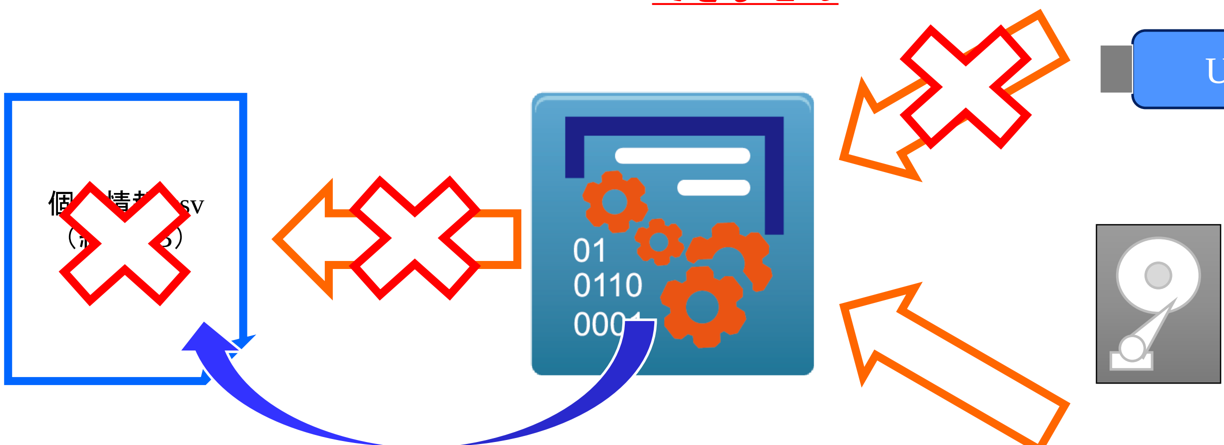
割符が不足している場合

メタセパレータで２つの電子割符から復元できません

持ち出したデータ

割符①

？？？？？？
？？？？
（約40KB）



ローカルディスク

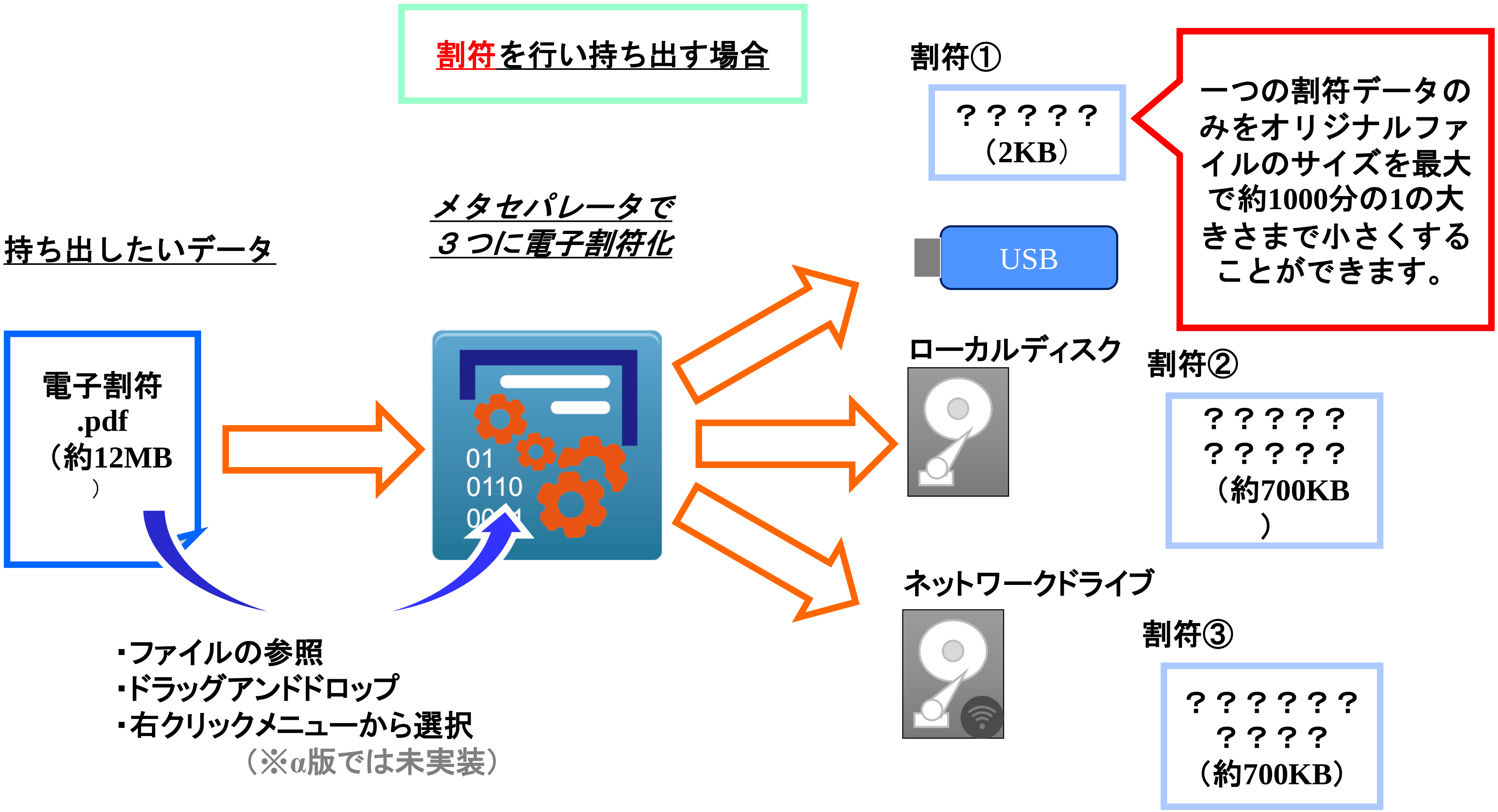
復元する為に必要な、割符されたデータがそろっていないため、メタセパレータ内で復元・閲覧することができません。

・アプリケーション上でダブルクリックして開けません（ローカルには展開されません）

割符②

？？？？？？
？？？？
（約40KB）

デモンストレーション②
電子割符数 3個・リカバリモード①・最小データ



デモンストレーション②
電子割符数 3個・リカバリモード①・最小データ

Next Security Inc.

復元を行い閲覧する場合
割符が１つ不足していても・・・

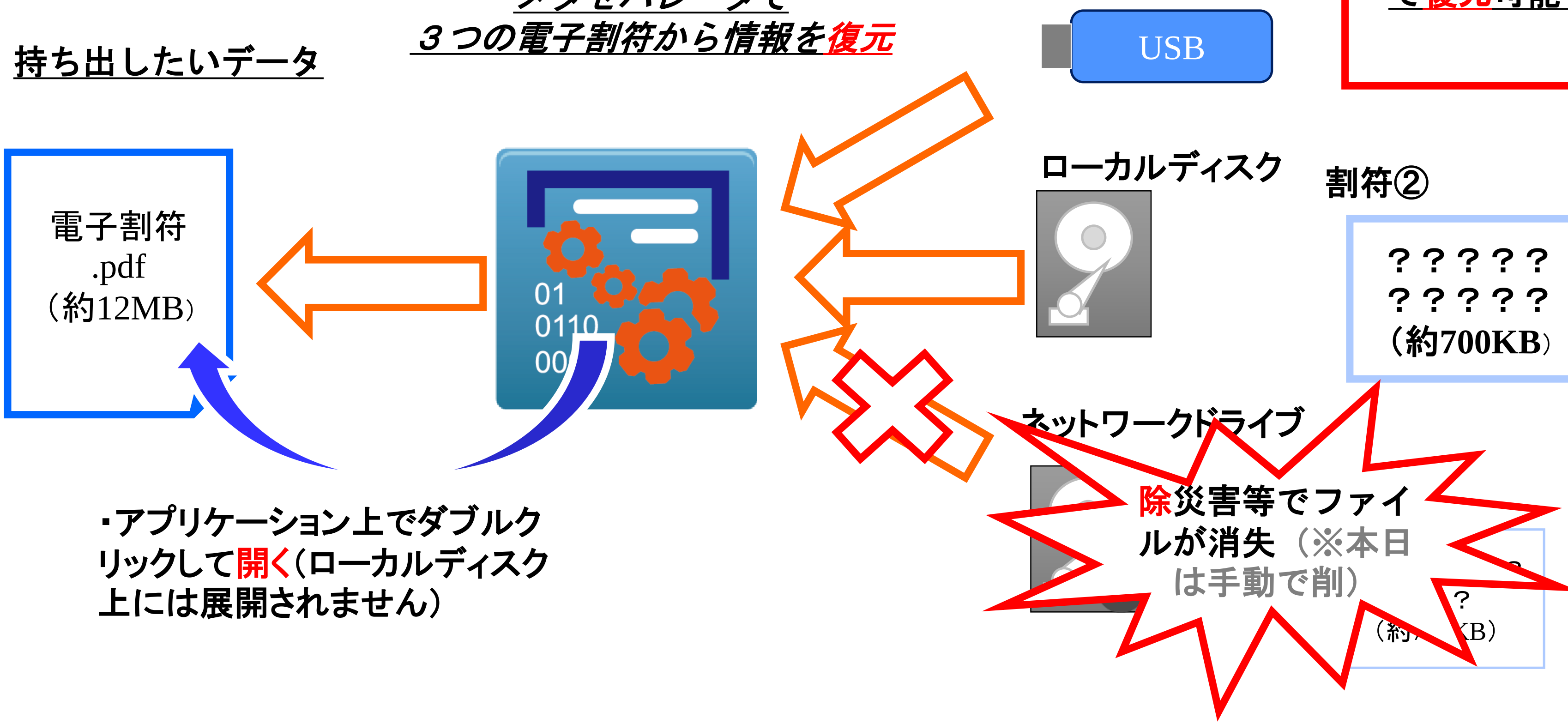
割符①

？？？？？
（2KB）

最小サイズの割符ともう一つの割符のみで復元可能です。

メタセパレータで
３つの電子割符から情報を復元

持ち出したいデータ



デモンストレーション③
電子割符数 3個・パスワードの付加

Next Security Inc.

割符を行い持ち出す場合

持ち出したいデータ

電子割符.pdf
（約12MB）

メタセパレータで３つに電子割符化
復元する為に必要なパスワードも付加

・ファイルの参照
・ドラッグアンドドロップ
・右クリックメニューから選択
（※α版では未実装）

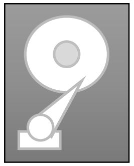
割符①

？？？？？
（500KB）

USB

電子割符化時に設定したパスワードを入力しない限り、復元することができません。

ローカルディスク



割符②

？？？？？？？
？？？？
（約500KB）

ネットワークドライブ

割符③

？？？？？？
？？？？
（約500KB）

デモンストレーション③
電子割符数3個・パスワードの付加

Next Security Inc.

<u>復元を行い閲覧する場合</u>

<u>メタセパレータで３つに電子割符から情報を復元するためにはパスワードが必要</u>

<u>持ち出したいデータ</u>

電子割符.pdf
（約12MB）

割符①

？？？？？
（2KB）

USB

復元する為に必要なパスワードが分からない限り情報が見られません。

ローカルディスク

割符②

？？？？？
？？？？？
（約700KB）

ネットワークドライブ

割符③

？？？？？？
？？？？
（約700KB）

OK

キャンセル

・パスワードが正しく入力された場合にのみ、復元されファイルが開く

・アプリケーション上でダブルクリックするとパスワード入力画面が開く

ノート/モバイルPCの安全な持ち出しソリューション例

Next Security Inc.

自社内

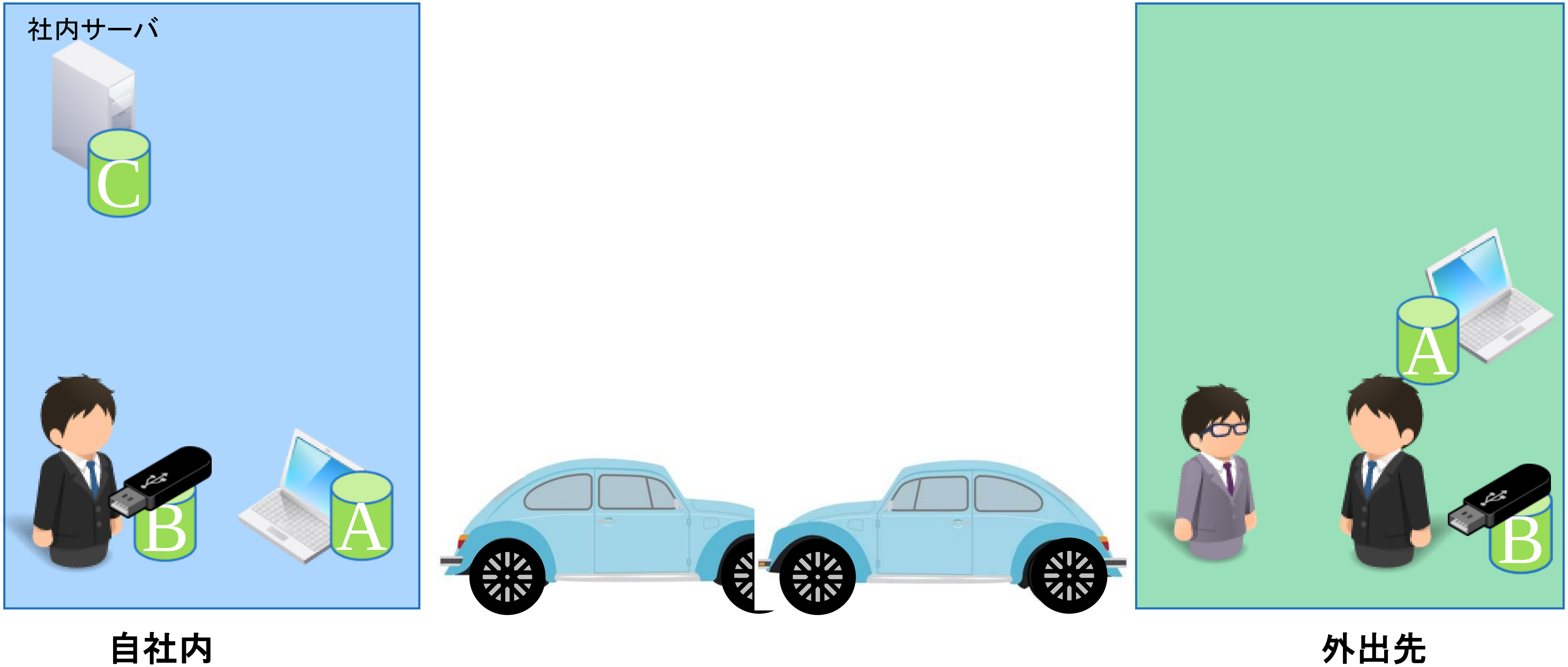
外出先

外出を行う際に、外出時に必要なファイルを解読不可能なデータ集合体に分割します。
例えば、「ファイル.file」をデータ集合体A～Cの3つに分割し、ローカル、USB、共有フォルダの3ヶ所に保存します。分割時に元のファイルは削除されます。
これらのデータ集合体は2つ以上で、元のファイルに復元することができます。

データ集合体単体は意味のない文字の羅列でしかありません。

ノート/モバイルPCの安全な持ち出しソリューション例

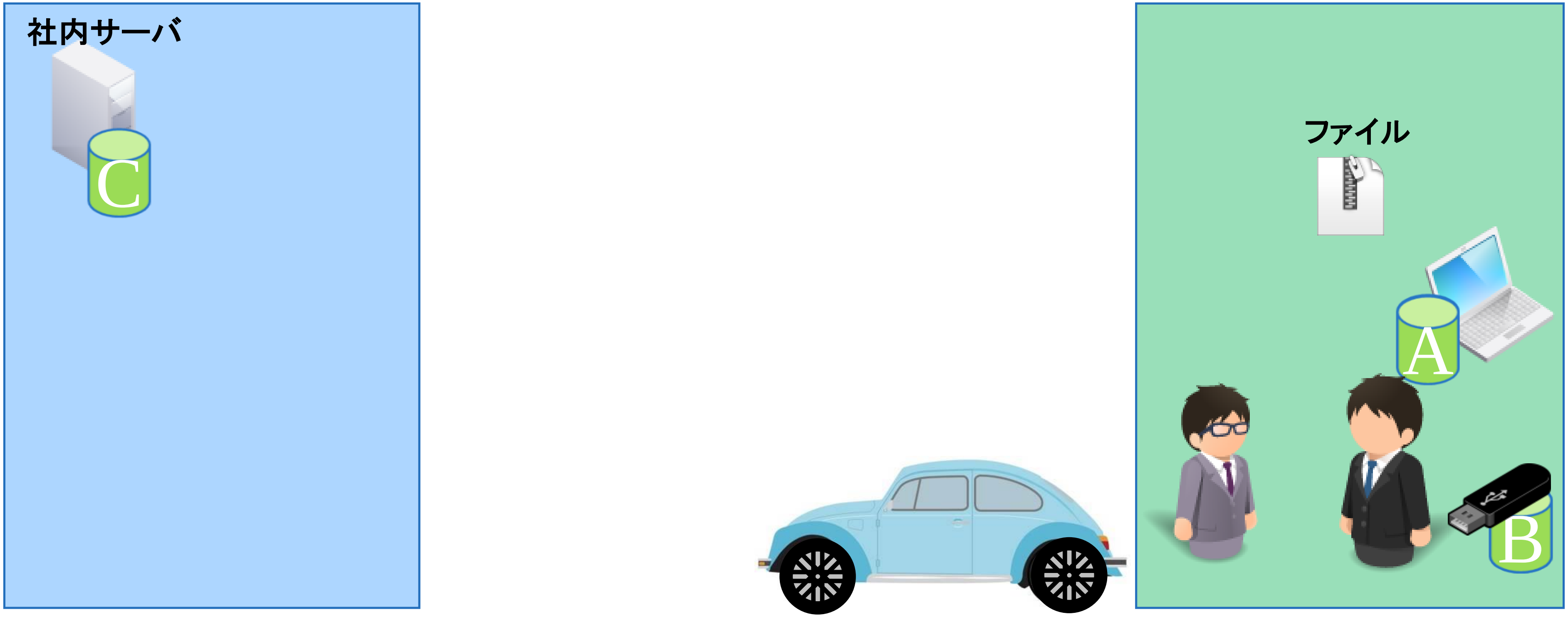
Next Security Inc.



AとBを持って外出します。

もし移動中にUSBかパソコンを紛失した場合も安心です。

ノート/モバイルPCの安全な持ち出しソリューション例



自社内　外出先

AとBを使って復元し、作業を行います。

ファイルは割符アプリケーション上でのみ展開されます。

復元ファイルは、PCを閉じた時点で消去します。（選択可能）

ノート/モバイルPCの安全な持ち出しソリューション例

自社内

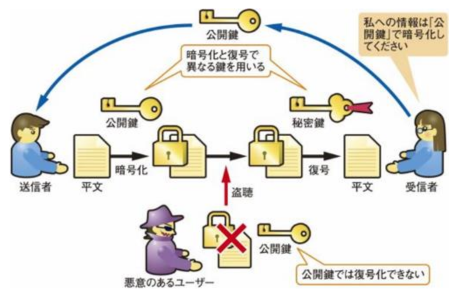
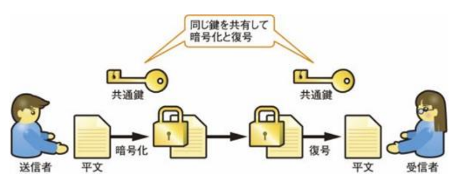
外出先

自社内に戻る際も同様に分割されたデータ集合体を持ち運ぶことで
安全にファイルを移動させることができます。

ご清聴有難う御座いました!

主要な暗号化方式（参考資料）

Next Security Inc.

暗号方式	主な用途	仕組み	暗号化アルゴリズム	メリット/デメリット	処理
公開鍵暗号 （非対称暗号） ＊処理速度：低速 ＊鍵の受渡：公開	＊SSL暗号化等用途 ＊暗号化専用鍵と符号化しかできない鍵 のペアを使う	 ＊受信側：暗号化用と復号用の異なる１組の鍵を用意し、暗号化用の鍵を送信側に通知する。この時、暗号化鍵は世間一般に公開しても問題ないので、この鍵を「公開鍵」と言う。 ＊一方、復号鍵は受信側だけが知っていれば良く、送信側に通知する必要はない。受信側だけの秘密にしておくので、この鍵を「秘密鍵」と言う。	RSA RSA は 1977 年にアルゴリズムを最初に発明した Ron Rivest, Adi Shamir そして Leonard Adleman の頭文字 ECC（楕円曲線暗号） 暗号化において楕円曲線を使用することは 1985 年に Neal KoblitzとVictor S. Miller によって提案され、ECC は 2004 年に一般的に使用されるようになった。	＊＊RSA暗号方式のメリット： ＊大きな数の素因数分解の難しさに、その安全性の基礎を置いている。 ＊鍵長を長くすれば解読は困難になる。 ＊＊RSA暗号方式のデメリット： ＊効率の良い素数の素因数分解の方法が見つかると、安全性が下がる可能性がある。 ＊鍵長を長くすれば解読は困難になるが、鍵が長いと今度は鍵生成や暗号化、復号化の計算コストが大きくなる。 ECC アルゴリズムの RSA に対する利点は鍵サイズが小さいために処理時間が短いこと、同じ鍵サイズであったとしてもセキュリティがより強い。しかしながら、全てのサービスやアプリケーションが ECC に基づく SSL 証明書と互換性があるわけではないという難点がある。 ＊ブラウザとサーバーが ECC 証明書をサポートするわけではない。 ＊ECC 署名検証には多くの計算能力が必要	公開鍵暗号化 (非対称)では RSA や楕円曲線暗号（ECC）のような暗号化アルゴリズムを使用して公開鍵と秘密鍵を作成 非対称暗号化では、公開鍵と秘密鍵を生成し、公開鍵でメッセージを暗号化し、秘密鍵でメッセージを復号 ＊「ペア」であるという仕組みを活かし、 通信相手が本人であるかどうか、正しいかどうかの認証のために応用 ＊複雑な計算処理が必要となるため、負荷が大きい ＊鍵の受け渡しや管理は非常に簡単 ＊計算負荷がかなり重いというデメリット
共通鍵暗号 （対称暗号） ＊処理速度：高速 ＊鍵の受渡：秘密	＊送受信データ暗号化 ＊用途WiFi等通信用途	 ＊送信側：公開鍵暗号方式の相手の公開鍵で暗号化し、「暗号化された共通鍵」と「暗号文」を 送付。 ＊受信側：「暗号文」と「暗号化された共通鍵」を受け取り、「暗号化された共通鍵」を「自分の秘密鍵」で復号して「共通鍵」を得る、この「共通鍵」使用して「暗号文」を復号化。	AES：Advanceed Encryption Standard ＊現在最も一般的なのは AES ＊鍵長：128,192,256bit ＊米国の連邦標準規格 ＊古くはDES（Data Encryption Standard）や3DES（Triple DES）	＊＊共通鍵暗号メリット ＊暗号化と復号のどちらの操作にも同じ鍵を使う ＊「暗号化・復号化のコストが低い」高速な処理が可能である。 ＊膨大なデータサイズのファイルの暗号化には、 高速な処理ができる共通鍵暗号が向いている。 ＊＊共通鍵暗号デメリット ＊暗号文の送信者と受信者で共通の鍵を共有する必要がある。（鍵を受け渡しする必要がある） ＊鍵を「どうやって安全に相手に伝えるか」が問題。 ＊鍵の数が膨大になる。	対称暗号では Twofish, AES もしくは Blowfish のようなアルゴリズムを用いて鍵を作成 ＊データの送り手と受け手が同一の鍵を使う方式 ＊鍵の受け渡しや管理について面倒 ＊計算負荷が軽いというメリット
ハイブリッド暗号 （共通鍵そのものを公開鍵暗号方式で相手に送る）	SSL暗号化通信方式	＊「毎回乱数で鍵を生成し、その鍵を使った共通鍵暗号でデータを暗号化」 し、そして「データの暗号化に使った鍵を、公開鍵暗号で暗号化し、それを暗号化データに添付して一緒に送る」	＊公開鍵の暗号化：RSA ＊通信データ暗号化：AES	＊データ長の短い公開鍵の暗号化を公開鍵暗号化「RAS」で暗号化 ＊データ長の長い通信データ暗号化を「AES」で行う ＊それぞれの長所を組み合わせたハイブリッド暗号化方式	「データの暗号化に使った鍵を、 公開鍵暗号で暗号化し、それを暗号化データに添付して一緒に送る」 ＊鍵を送る時だけ安全に公開鍵暗号化方式で送り、その後の通信は、高速に処理できる共通鍵暗号化方式で行う。