Korkamuy Encryption

暗号キー管理

2011 年 06 月 24 日（3.0 版）

Hokkaido NS Solutions Corporation

変更履歴

Version	日付	変更内容
2.0	2009/08/24	第 2.0 版制定
3.0	2011/06/24	第 3.0 版制定

商標

Korkamuy は、北海道エヌエスソリューションズ株式会社の登録商標です。
その他本文記載の会社名及び製品名は、それぞれ各社の商標又は登録商標です。

注意

(a) 本ソフトウェア及び付属するドキュメントに関する著作権は、北海道エヌエスソリューションズ株式会社が保持します。
(b) 本ソフトウェアは、使用許諾契約書のもとでのみ使用することができます。
(c) 本ソフトウェア及び付属するドキュメントの一部、又は全部を北海道エヌエスソリューションズ株式会社の書面による許可無く複写・複製することは、その形態を問わず禁じます。
(d) 本ソフトウェアの仕様及び付属するドキュメントに記載されている内容は、将来予告無く変更することがあります。

目次

1. 暗号キー管理

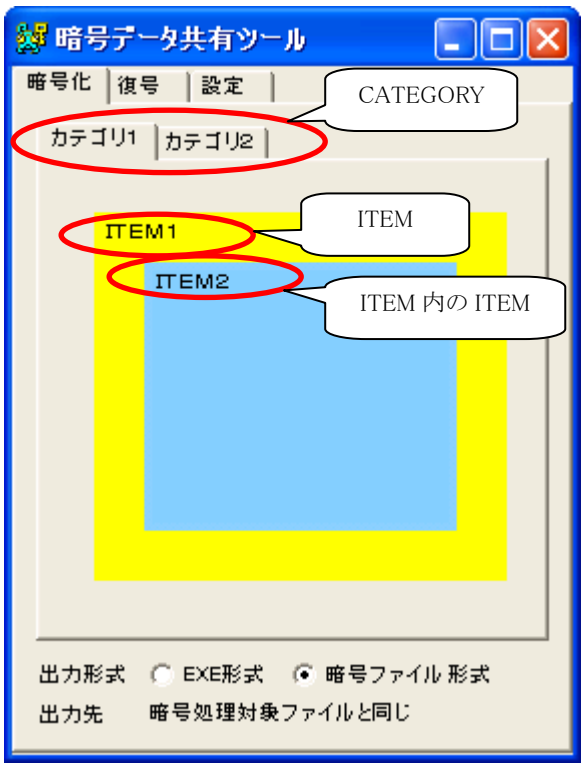
当ツールにおいて、暗号キーは、ユーザ及び用途別に管理されており、この暗号キーは、決められた構造、属性を定義した XML ファイル（＝暗号キーXML ファイル）を用い、変更することができます。

1.1. 暗号キーXML ファイル

1.1.1. データ構造

要素名	要素内容	下位要素名
USERS	ユーザ情報	USER （※複数指定可能）
USER	ユーザ別情報	CATEGORY （※複数指定可能）
CATEGORY	カテゴリ情報	ITEM （※複数指定可能）
ITEM	暗号化項目情報	KEY_INFO （※複数指定可能）
		ITEM （※複数指定可能）
KEY_INFO	暗号キー情報	KEY_START_DATE
		KEY_END_DATE
		ENCRYPTION_KEY
KEY_START_DATE	適用開始日	日付データ(YYYYMMDD)
KEY_END_DATE	適用終了日	日付データ(YYYYMMDD)
ENCRYPTION_KEY	暗号キー	任意文字列データ

（1）データ構造と画面表示の関係

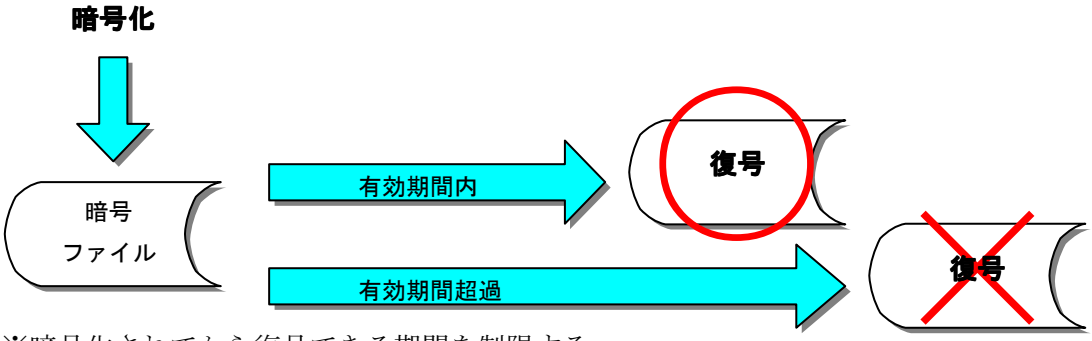


1.1.2. 属性情報

要素名	属性名	属性内容
USERS	KANSASTATUS	監査要否(ON:監査必要、OFF:監査不要)
USER	USER_NAME	ユーザID
	PASSWORD	パスワード
CATEGORY	CATEGORY_NAME	カテゴリ名称
	VALID_PERIOD	暗号ファイル有効期間(単位:日)
ITEM	ITEM_NAME	暗号化項目名称
	DISABLE_DECRYPT	復号抑止(true:復号不可、false:復号可能)
	isEditable	EXE 編集可否(true:編集可能、false:編集不可)
	Visible	表示要否(true:表示、false:非表示)
KEY_INFO	needsAuthentication	認証要否(1:認証必要、0:認証不要)
KEY_START_DATE	-	-
KEY_END_DATE	-	-
ENCRYPTION_KEY	-	-

(1) 暗号ファイル有効期間

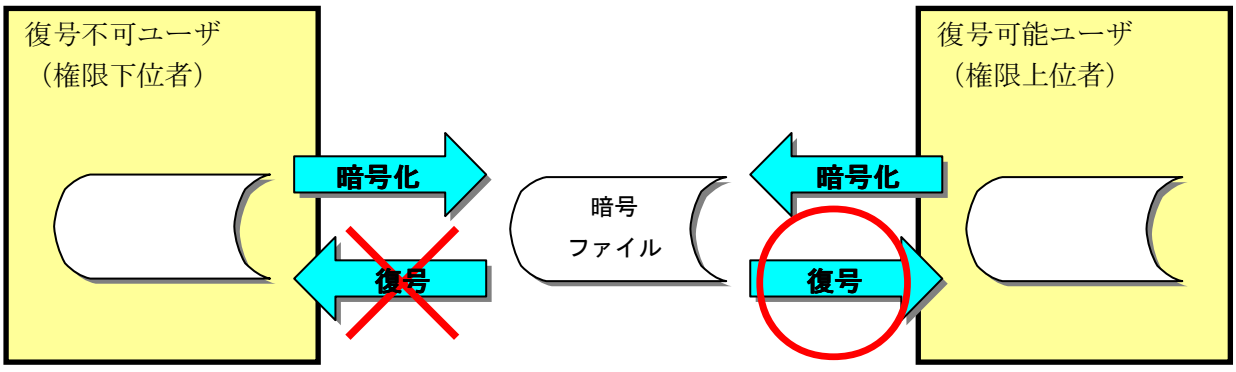
当該カテゴリで暗号化されたファイルの復号可能日数。



※暗号化されてから復号できる期間を制限する。

(2) 復号抑止

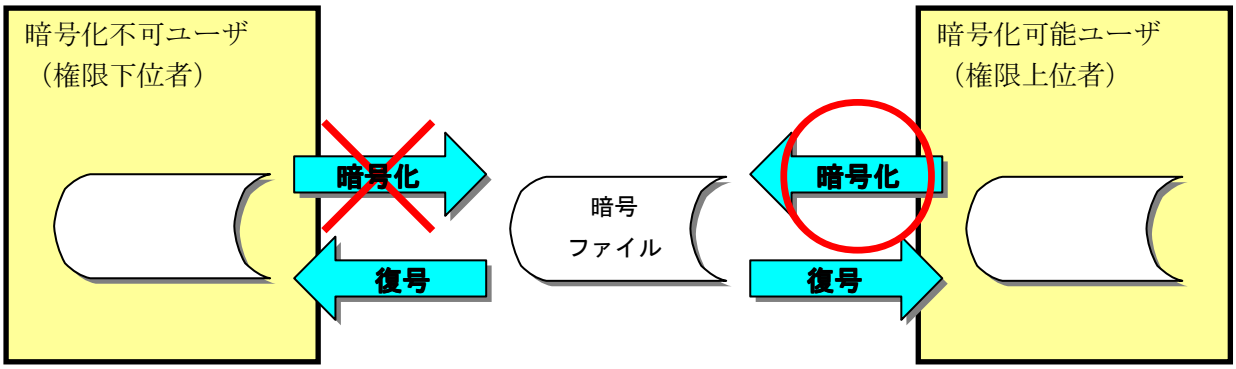
暗号化できるが復号できなくする。



※同一暗号キーを共有し、復号できるユーザを制限する場合に利用する。

（3）表示要否

復号できるが暗号化できなくする。



※同一暗号キーを共有し、暗号化できるユーザを制限する場合に利用する。

※暗号キー廃止時等、暗号化されたファイルの復号だけをさせたい場合に利用する。

（4）EXE 編集可否

EXE 形式（自己復号ファイル）で出力する際の「ファイル拡張子」や「暗号キーの生成方式」等を指定できるようにする。

詳細は操作マニュアル「３．４．EXE 情報の編集」を参照してください。

1.2. 初期組み込み情報

1.2.1. 初期組み込み暗号キーXML ファイル例

```
<?xml version="1.0" encoding="shift_jis"?>
<USERS>
<USER USER_NAME= "guest" PASSWORD= "guest">
     <CATEGORY CATEGORY_NAME="共通" VALID_PERIOD="30" >
          <ITEM ITEM_NAME="暗号化領域" DISABLE_DECRYPT="false" isEditable="false" Visible="true" >
            <KEY_INFO>
              <KEY_START_DATE>20060101</KEY_START_DATE>
              <KEY_END_DATE>20991231</KEY_END_DATE>
              <ENCRYPTION_KEY>HCFcommonKey123</ENCRYPTION_KEY>
            </KEY_INFO>
          </ITEM >
     </CATEGORY >
     <CATEGORY CATEGORY_NAME="EXE 用" VALID_PERIOD="30" >
          <ITEM ITEM_NAME="汎用" DISABLE_DECRYPT="false" isEditable="false" Visible="true" >
            <KEY_INFO needsAuthentication="0">
              <KEY_START_DATE>20060101</KEY_START_DATE>
              <KEY_END_DATE>20991231</KEY_END_DATE>
              <ENCRYPTION_KEY>EXEcommonKey123</ENCRYPTION_KEY>
            </KEY_INFO>
               <ITEM ITEM_NAME="〇〇向け" DISABLE_DECRYPT="false" isEditable="true" Visible="true" >
                 <KEY_INFO>
                   <KEY_START_DATE>20060101</KEY_START_DATE>
                   <KEY_END_DATE>20991231</KEY_END_DATE>
                   <ENCRYPTION_KEY>EXEcorpKey123</ENCRYPTION_KEY>
                 </KEY_INFO>
               </ITEM >
               <ITEM ITEM_NAME="△△向け" DISABLE_DECRYPT="false" isEditable="true" Visible="true" >
                 <KEY_INFO>
                   <KEY_START_DATE>20060101</KEY_START_DATE>
                   <KEY_END_DATE>20991231</KEY_END_DATE>
                   <ENCRYPTION_KEY>EXEcorpKey456</ENCRYPTION_KEY>
                 </KEY_INFO>
               </ITEM >
               <ITEM ITEM_NAME="□□向け" DISABLE_DECRYPT="false" isEditable="true" Visible="true" >
                 <KEY_INFO>
                   <KEY_START_DATE>20060101</KEY_START_DATE>
                   <KEY_END_DATE>20991231</KEY_END_DATE>
                   <ENCRYPTION_KEY>EXEcorpKey789</ENCRYPTION_KEY>
                 </KEY_INFO>
               </ITEM >
          </ITEM >
     </CATEGORY >
</USER>
<USER USER_NAME= "SYSTEM" PASSWORD= "XXXXXXXXXXXXXXXX">
     <CATEGORY CATEGORY_NAME="ＸＭＬ暗号化用" VALID_PERIOD="30" >
          <ITEM ITEM_NAME="暗号化領域" DISABLE_DECRYPT="true" isEditable="false" Visible="true" >
            <KEY_INFO>
              <KEY_START_DATE>20060101</KEY_START_DATE>
              <KEY_END_DATE>20991231</KEY_END_DATE>
              <ENCRYPTION_KEY>Hns_XMLsystemKey_Hns</ENCRYPTION_KEY>
            </KEY_INFO>
          </ITEM >
     </CATEGORY >
</USER>
</USERS>
```

※但し、USER_NAME、PASSWORD 以外は、実際のものと異なる場合があります。

1.2.2. SYSTEM ユーザとは

SYSTEM ユーザは、暗号キー変更時、暗号化された暗号キーXML ファイルを復号するための特別なユーザです。一般ユーザとしては、利用しないでください。

1.3. 追加暗号キーXML ファイル

ユーザ別に管理された暗号キーとは別に、少人数で気軽に暗号データを共有するために、利用者が自由に定義した暗号キーを追加することができます。全ユーザ共通のため、ユーザ情報を持たないことを除き、データ構造、属性情報は、基本の暗号キーXML ファイルとほぼ同じです。

1.3.1. 追加暗号キーXML ファイル例

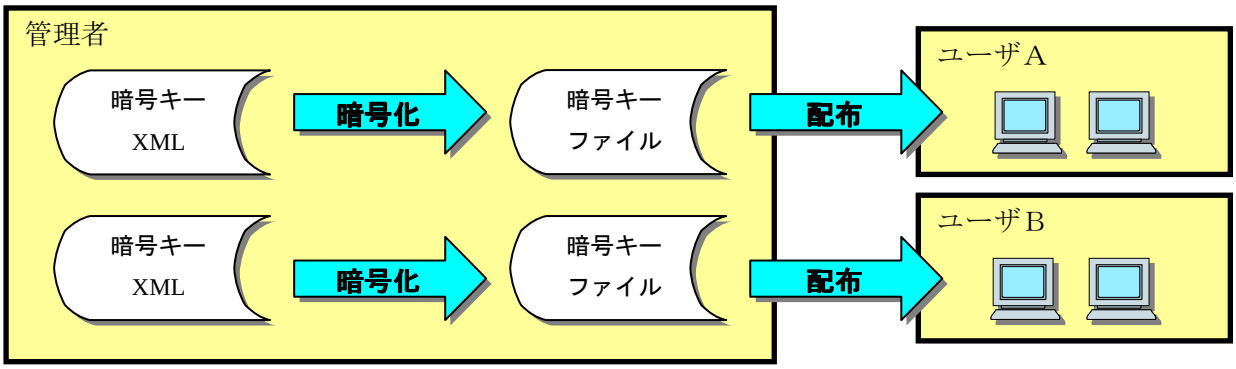
```
<?xml version="1.0" encoding="shift_jis"?>
<CATEGORIES>
    <CATEGORY CATEGORY_NAME="××Gr 用" VALID_PERIOD="360" >
        <ITEM ITEM_NAME="共通" DISABLE_DECRYPT="false" isEditable="true" Visible="true" >
          <KEY_INFO>
            <KEY_START_DATE>20060101</KEY_START_DATE>
            <KEY_END_DATE>20991231</KEY_END_DATE>
            <ENCRYPTION_KEY>GRcommonKey123</ENCRYPTION_KEY>
          </KEY_INFO>
        </ITEM >
    </CATEGORY >
    <CATEGORY CATEGORY_NAME="ﾏｲｶﾃｺﾞﾘ1" VALID_PERIOD="360" >
        <ITEM ITEM_NAME="汎用" DISABLE_DECRYPT="false" isEditable="true" Visible="true" >
          <KEY_INFO>
            <KEY_START_DATE>20060101</KEY_START_DATE>
            <KEY_END_DATE>20991231</KEY_END_DATE>
            <ENCRYPTION_KEY>MYcommonKey123</ENCRYPTION_KEY>
          </KEY_INFO>
            <ITEM ITEM_NAME="〇〇向け" DISABLE_DECRYPT="false" isEditable="true" Visible="true" >
              <KEY_INFO>
                <KEY_START_DATE>20060101</KEY_START_DATE>
                <KEY_END_DATE>20991231</KEY_END_DATE>
                <ENCRYPTION_KEY>MYcorpKey123</ENCRYPTION_KEY>
              </KEY_INFO>
            </ITEM >
            <ITEM ITEM_NAME="△△向け" DISABLE_DECRYPT="false" isEditable="true" Visible="true" >
              <KEY_INFO>
                <KEY_START_DATE>20060101</KEY_START_DATE>
                <KEY_END_DATE>20991231</KEY_END_DATE>
                <ENCRYPTION_KEY>MYcorpKey456</ENCRYPTION_KEY>
              </KEY_INFO>
            </ITEM >
            <ITEM ITEM_NAME="□□向け" DISABLE_DECRYPT="false" isEditable="true" Visible="true" >
              <KEY_INFO>
                <KEY_START_DATE>20060101</KEY_START_DATE>
                <KEY_END_DATE>20991231</KEY_END_DATE>
                <ENCRYPTION_KEY>MYcorpKey789</ENCRYPTION_KEY>
              </KEY_INFO>
            </ITEM >
        </ITEM >
    </CATEGORY >
</CATEGORIES>
```

2. 暗号キー変更

2.1. 必要性

下記に示す点を考慮し、新しく暗号キーXML ファイルを作成・管理し、定期的及び必要に応じて、暗号キーを変更することをお奨めします。

(1) ユーザ及び用途等に合わせた暗号キーの任意設定（ユーザビィリティ向上）
(2) 同一暗号キーの長期利用による暗号キー漏洩の危険性の軽減（セキュリティ向上）

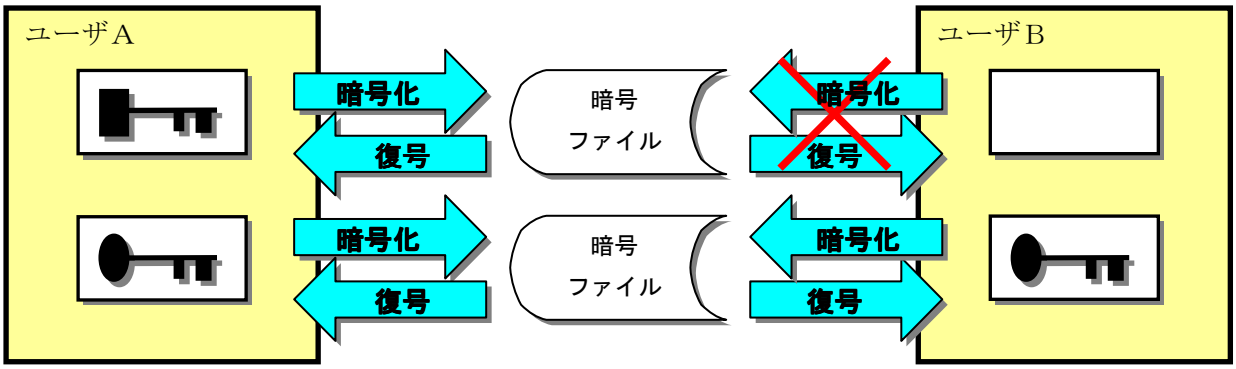


2.2. 暗号キーXML ファイルの作成

「１．１．暗号キーXML ファイル」で示したデータ構造、属性情報や「１．２．初期組み込み情報」を参考に XML ファイルを作成してください。

2.2.1. 暗号キーXML ファイル作成時の留意事項

(1) 現在利用可能ユーザと同一のユーザの場合、新しい情報に置き換えられます。
(2) 現在利用可能ユーザと異なるユーザの場合、新しく情報が追加されます。
(3) 暗号ファイルの利用期間を十分考慮し、暗号ファイル有効期間を決定してください。
(4) 同一の暗号キーを定義することによって、複数のユーザ間で共有可能な暗号ファイルを作成することができます。



(5) セキュリティ面を考慮し、SYSTEM ユーザの情報も新しい暗号キーXML ファイル内で定義し、変更することをお奨めします。SYSTEM ユーザの情報を定義する際は、パスワード漏洩による暗号化された暗号キーXML ファイルの不正復号を考慮し、**パスワードを変更**及び**自己復号不可**（DISABLE_DECRYPT=”true”）とすることを強くお奨めします。
（※自己復号不可としてもインポートは可能です。）
(6) 過去及び適用期間中の暗号キー情報を変更すると、変更前に暗号化されたファイルを復号できなくなります。
(7) ユーザパスワードも定期的に変更することをお奨めします。

2.2.2. 暗号キーXML ファイル作成パターン

（1）ユーザ毎にファイルを分ける（※推奨）
メリット　：当該ユーザ以外の情報が含まれない
デメリット：ファイル管理が多少面倒

（2）全ユーザ情報を 1 ファイル含める
メリット　：ファイル管理が容易
デメリット：ユーザ ID 等が漏洩した場合、なりすまし可能

2.3. 暗号キーXML ファイルの暗号化

暗号キー変更を行うためには、作成した暗号キーXML ファイルを特別なユーザ（SYSTEM）で復号可能な暗号キーで暗号化し、配布する必要があります。
以下の手順で暗号化してください。

（1）SYSTEM ユーザでログインする。（他ユーザでログイン後であれば、SYSTEM ユーザにユーザ ID 変更する。）
（2）作成した暗号キーXML ファイルを暗号ファイル形式で暗号化する。

2.4. 変更方法

暗号化された暗号キーXML ファイルを用い、暗号キーを変更する方法には、下記の２つの方法があります。

2.4.1. 暗号キーファイルのインポート

（1）管理・運用者作業
① 利用者への暗号化された暗号キーXML ファイルの配布とインポート後のユーザ ID とパスワードの通知

（2）利用者作業
① 暗号キーファイルインポート機能による配布ファイルのインポート

2.4.2. 暗号キーファイルの HTTP 通信による取得及びインポート（オプション機能）

（1）管理・運用者作業
① 暗号キーファイル配信サーバの構築
② 暗号化された暗号キーXML ファイルの所定ディレクトリへの配置
③ バージョン情報の更新
④ 利用者へのアクセス情報（URL 等）の通知

（2）利用者作業
① 暗号キーファイル問合せ機能による暗号キーファイルの取得及びインポート

3. 暗号キー追加

3.1. 追加暗号キーXML ファイルの作成

「１．３．追加暗号キーXML ファイル」や「１．１．暗号キーXML ファイル」で示したデータ構造、属性情報を参考に XML ファイルを作成してください。

3.2. 追加方法

3.2.1. 追加暗号キーXML ファイルの取り込み

(1) 利用者作業

①カテゴリ追加機能による追加暗号キーXML ファイルの取り込み