FUJITSU
shaping tomorrow with you

暗号化・鍵管理ソリューションを含めた PCI DSS準拠支援サービスのご紹介

ご紹介

2012年7月25日
クレジットカード情報セキュリティフォーラム

富士通エフ・アイ・ピー株式会社
SaaSシステム部

Agenda

FUJITSU

1. PCI DSS準拠支援サービスの概要

2. PCI DSS要件別対応内容の紹介

3. マルチプラットフォーム対応暗号化ツール
   COMPLOCK® Ⅱ

4. 暗号鍵管理システム
   KeyMeister

5. お問い合わせ先

1．PCI DSS準拠支援サービスの概要

「PCI DSS準拠支援サービス」の概要をご紹介いたします。

1．1　サービス体系

現状分析・評価から始まり審査対応まで、ご要望に応じたサービス内容を提供いたします。

PCI DSS準拠支援サービス

分析フェーズ
現状分析・評価サービス

実装フェーズ
ポリシー策定支援サービス
ソリューション実装サービス

運用フェーズ
教育支援サービス
運用フォローアップサービス

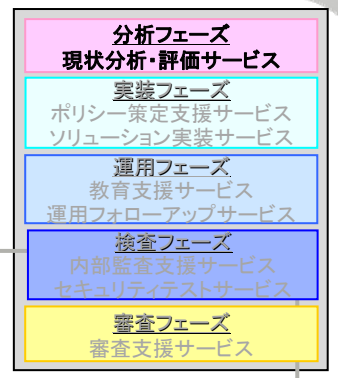
検査フェーズ
内部監査支援サービス
セキュリティテストサービス

審査フェーズ
審査支援サービス

5つのフェーズ
8つのサービス

1．2　分析：現状分析・評価サービス

PCI DSS要件をベースラインとし、現状のセキュリティ対策状況をマネジメントレベル・技術レベルから分析・評価し、ギャップ状況を洗い出します。分析・評価結果より、基準を満たすための改善提案を行います。



分析フェーズ

【現状分析・評価サービス】

現状分析の実施

調査報告書作成

改善に関するフォロー

実装フェーズへ

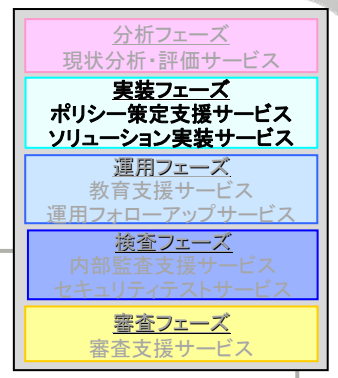
- チェックリストに基づいてヒアリング
- カード会員データに関係するシステムの設定状況の確認
- 既存の各種ポリシーの確認

- PCI DSSの要件とのギャップから不適合が懸念される事項を報告
- PCI DSSの要件準拠に向けた改善方針のご提案

- 改善方針に関するQA対応

1．3　実装：ポリシー策定支援サービス

PCI DSSの文書化要件を満たすために必要となるポリシーの整備を行います。マネジメントシステムの考え方を取り入れ、確実な運営を目指したポリシー構築を行います。



実装フェーズ

【ポリシー策定支援サービス】

ポリシー構成の設計

テンプレート提示と検討

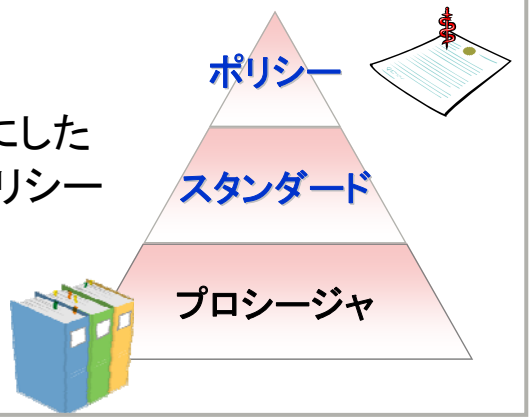
ポリシー策定

運用フェーズへ

●分析フェーズの結果に基づいて、不足するポリシーの文書を明確化
●既存ポリシーを考慮し、PCI DSS関連ポリシーの文書構成を設計

●ドキュメントテンプレートの提供と説明
●既存の業務や管理方法をインタビューし、貴社のルールとしてカスタマイズ

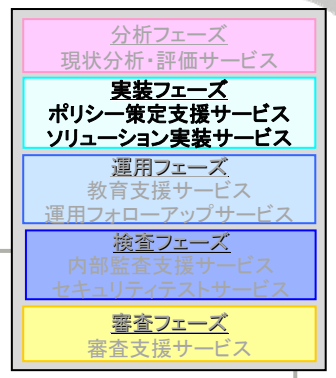
●PDCAサイクルをベースにしたマネジメントを意識したポリシー策定を実施



1．4　実装：ソリューション実装サービス

FUJITSU

PCI DSS要件の中で必要な技術的ソリューションを実装します。



実装フェーズ

【ソリューション実装サービス】

ソリューションの選定

- ●既存システムの変更が必要な部分を洗出し、必要な設定変更やソフトウェア、機器を選定
- ●運用手順変更によるセキュア化のサポート

実装ポリシーの確認

- ●システム運用手順への組み込み
- ●PCI DSSの要件に見合うソリューションの導入を確認

ソリューションの導入

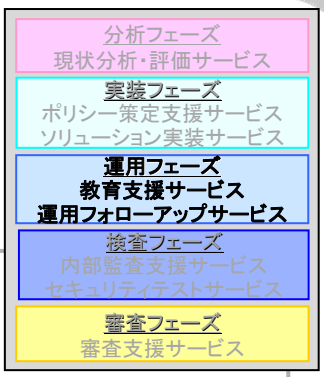
- ●各ソリューションのスムーズな初期導入を実施

運用フェーズへ

1．5　運用：教育支援サービス

FUJITSU

セキュリティに関する認識を高めるための教育実施を支援します。一般的なセキュリティに関する知識から、情報セキュリティポリシーやPCI DSSの運営に必要な各種手順への理解を高めるための教育まで、幅広く対応します。



運用フェーズ

【教育支援サービス】

教育計画の策定

●実施する教育へのご要望を確認
●教育実施の対象者、実施時期、教育の形式を決定

教育実施支援

●教育コンテンツの提供、研修の実施など、ご要望にお応えした教育実施をサポート

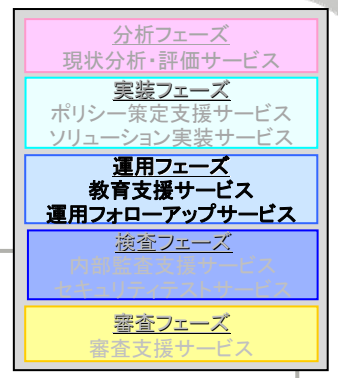
教育実施後のフォロー

●教育実施後の理解度測定を実施
●理解度測定の結果をもとに改善提案を実施

検査フェーズへ

1．6　運用：運用フォローアップサービス

構築されたPCI DSSの要件の運用を定着化させるために、PDCAサイクルを意識した運用の枠組みを提案し、確実な運用を支援します。



運用フェーズ

【運用フォローアップサービス】

運用計画の構築

●PDCAサイクルを意識したセキュリティ運用管理の年間計画を策定

運用の実施

●ポリシーに準じたセキュリティ運用管理

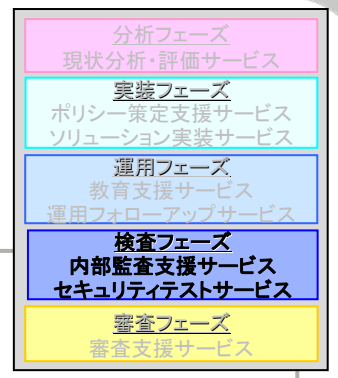
運用の支援

●会議体の定期的な開催による自立的なマネジメントシステムの運用を支援
●運用計画の進捗管理
●運用管理上で直面する課題への解決サポート

検査フェーズへ

1．7　検査：内部監査支援サービス

PCI DSS要件を監査基準に、内部監査に必要なドキュメントの作成から監査の実施および監査結果にもとづく改善提案までを行います。



検査フェーズ

【内部監査支援サービス】

内部監査計画の作成

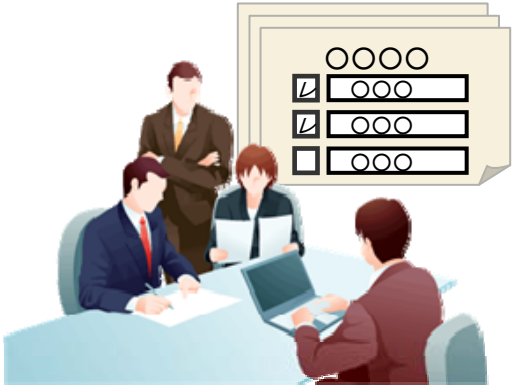
- 監査範囲、重点テーマなどの監査方針を確認
- 監査実施計画および監査手続の立案支援

内部監査の実施

- 監査実施の支援（代行も可能）
- 監査結果報告書を作成
- 監査結果報告会の開催

改善提案

- 監査結果報告書をもとに改善提案を実施

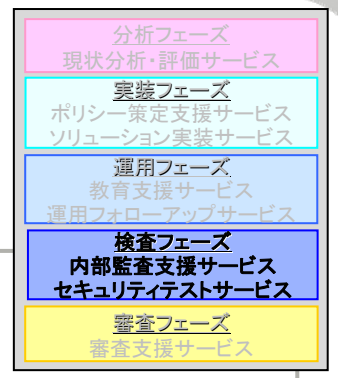


審査フェーズへ

1．8　検査：セキュリティテストサービス

FUJITSU

利用しているシステムがPCI DSS要件に対応していることを確認するために、技術的なアプローチによる検査を実施します。



検査フェーズ

【セキュリティテストサービス】

検査計画の作成

- ●PCI DSS要件に必要な検査の確認と実施範囲の検討
- ●検査スケジュール、検査方法の確定
- ●検査実施計画を作成

検査の実施

- ●検査実施
- ●検査結果報告書を作成
- ●必要に応じ報告会を実施し、検査結果をわかりやすくご説明

報告会の開催

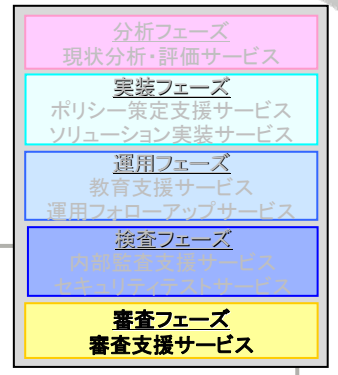
- ●検査結果報告書をもとに報告会を実施
- ●次回検査へのフォローアップ

審査フェーズへ

1．9　審査：審査支援サービス

FUJITSU

QSA（認定セキュリティ評価機関）によるPCI DSS審査に立ち会い、審査結果に対する指摘を適確に把握し、最適な改善提案を行います。



審査フェーズ

【審査支援サービス】

審査前確認

審査立会い

改善提案

PCI DSS 準拠

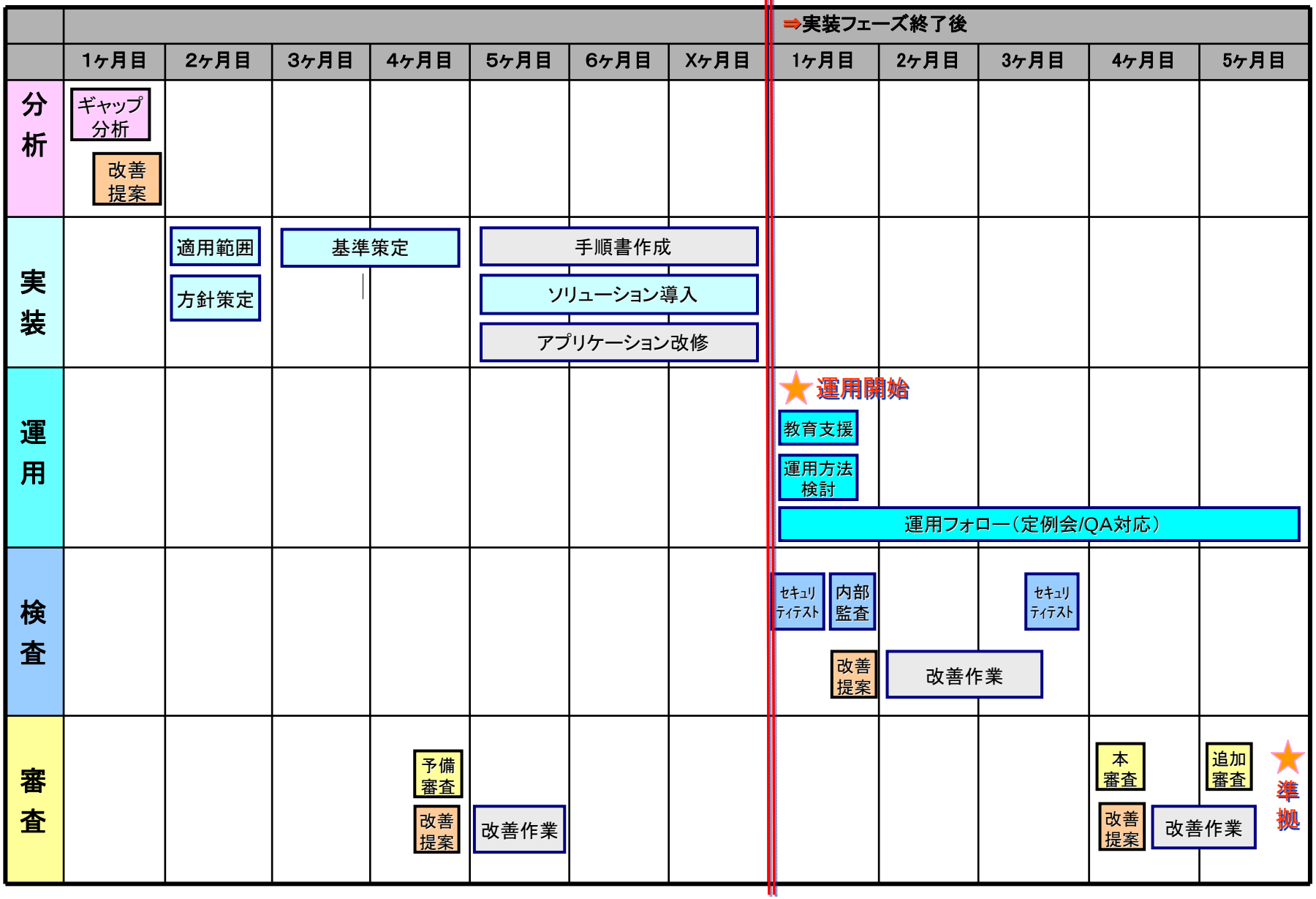
- 実際の審査の流れを確認しながら審査直前の最終確認を実施
- インタビューでよく聞かれる項目など審査のポイントをアドバイス

- QSA(認定セキュリティ評価機関)による審査に立会い
- 審査の休憩時間などに不安な点をサポート

- 審査後のフォローアップとして、審査結果をもとに改善提案を実施

1．10　標準スケジュール(案)

※ギャップ分析結果により、スケジュールは前後いたします。



2. PCI DSS要件別対応内容の紹介

PCI DSSの12要件からみた、弊社サービス内容やソリューションをご紹介します。

2．1　安全なネットワークの構築と維持

FUJITSU

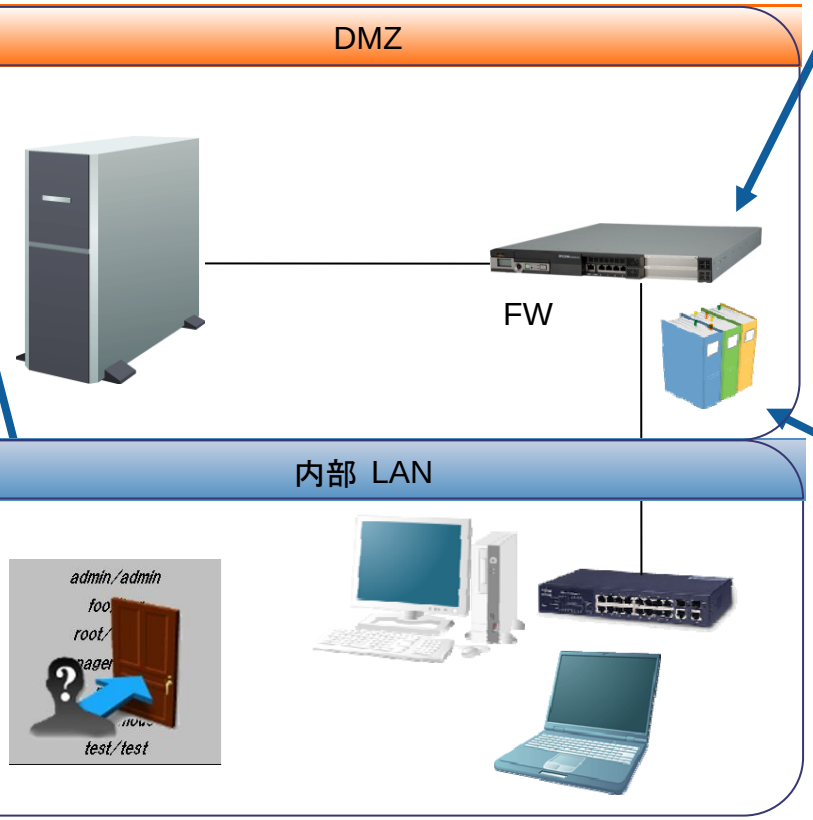
要件 1 (25項目)	カード会員データを保護するために、ファイアウォールをインストールして構成を維持する
要件 2 (21項目)	システムパスワードおよび他のセキュリティパラメータにベンダ提供のデフォルト値を使用しない

セグメント分割
(1.1.3, 1.2.3, ...)

PCI DSS対象範囲を考慮したネットワーク設計とセグメント分割をサポートします。

サーバのセキュア化
(2.1, 2.2)

セキュアサーバの構築・導入



ファイアウォール

環境に最適なFWをご提供します。

ポリシーの策定
(1.1)

PCI DSS準拠に必要な様々なドキュメント作成をサポートします。

- ◆システム変更管理基準
- ◆システム構成基準
- ◆システムセキュリティ運用基準、etc...

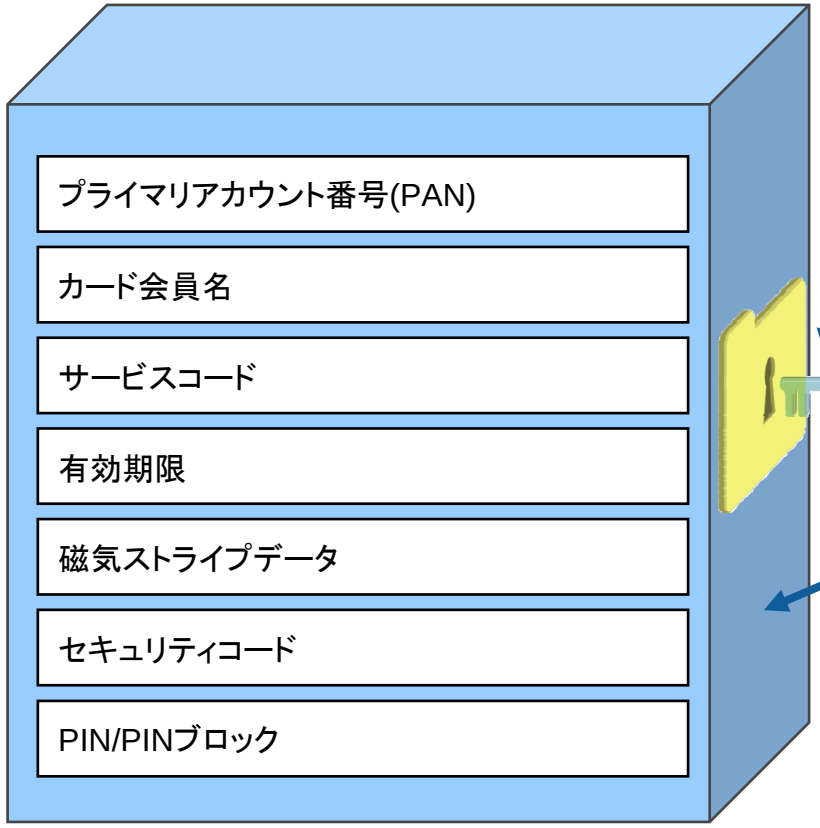
2．2　カード会員データの保護

FUJITSU

要件 3 (33項目)	保存されるカード会員データを保護する
要件 4 (9項目)	オープンな公共ネットワーク経由でカード会員データを伝送する場合、暗号化する

管理基準の策定
(3.1)

カード会員データの保護に関する基準を策定します。
基準のなかには、データの保存及び廃棄に関する事項、さらには、暗号の利用からネットワークを利用したデータの送信にまで及びます。



鍵管理
(3.4, 3.5, 3.6)

鍵管理ソリューションにより、一元的でセキュアな鍵管理方法をご提供します。

暗号化
(3.4, 4.1)

- ディスク暗号化
- ファイル暗号化
- 通信経路セキュア化

最適な対策で、カード会員データを保護します。

2．3　脆弱性管理プログラムの整備(1)

FUJITSU

要件５
(6項目)

アンチウイルスソフトウェアまたはプログラムを利用し、定期的に更新する

ウイルス対策ゲートウェイ

メール・Web経由など外部からのウィルス・ワームの侵入をガードする、ウィルス対策ゲートウェイをご提供します。

管理基準の策定
(5.2)

システム管理者だけではなく、システムの利用者も対象にしたアンチウイルスソフトウェアの管理基準を策定します。

ウイルス対策ソフト
(5.1, 5.2)

アンチウィルスソフトウェアは、PCに加え、サーバにもインストールする必要があります。

各種サーバに最適なアンチウィルスソフトウェアの導入をサポートします。

2．3　脆弱性管理プログラムの整備(2)

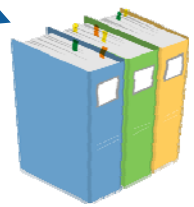
FUJITSU

要件 6
(32項目)

安全性の高いシステムとアプリケーションを開発し、保守する

開発基準の策定
(6.3, 6.4, 6.5, ...)

アプリケーションの開発・改修に関する基準を整備します。また脆弱性の管理基準も整備することで、セキュリティの恒常的な維持をサポートします。



Webアプリケーションファイアウォール
(6.6)

未知の攻撃への対策として、Webアプリケーションファイアウォール(WAF)をご提供します。

セキュリティ検査
(6.6)

Webセキュリティ脆弱性診断ツールを利用し、安価で効果的な脆弱性診断をご提供します。

2．4　強固なアクセス制御手法の導入(1)

FUJITSU

要件 7 (7項目)	カード会員データへのアクセスを、業務上必要範囲内に制限する
要件 8 (29項目)	コンピュータにアクセスできる各ユーザに一意のIDを割り当てる

管理基準の策定

カード会員データの取扱いに関する基準を策定します。
基準のなかには、データへのアクセスコントロールに関する内容を中心に、アクセス制御機能に関する要件からアクセスの付与に関する要件まで記述します。

IDベースの権限管理
(7.1, 7.2, 8.1, ...)

各役割に応じた適切な権限を付与し、管理者の操作をロギングできるソリューションをご提供します。

アカウント管理
(8.5)

運用面、システム面から、適切なアカウント管理をサポートします。

2．4　強固なアクセス制御手法の導入(2)

FUJITSU

要件 9
(28項目)

カード会員データへの物理的アクセスを制限する

管理基準の策定
(9.1, 9.2, ...)

カード会員データへの物理的なアクセスを制御するための基準を策定します。
建物への人の出入りの管理ならびにデータが保存された記憶媒体の管理、さらには、ネットワークの接続ポイントの管理までも含めます。

高セキュリティセンタ
(要件9全般)

お客様で現在のシステム設置場所の変更をご希望の場合には、当社データセンタのご提案も可能です。

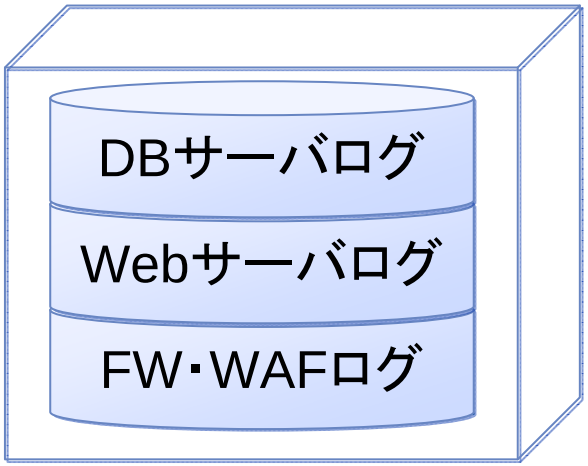
全国14箇所のセンタから、お客様のご利用形態やご希望の立地に合わせてご提案可能です。
災害対策に加え、物理アクセス制限として以下のような設備を備えています。

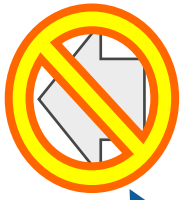
- ◆入退室管理装置(生体認証・専用カード)
- ◆各種防犯センサー
- ◆監視カメラ
- ◆媒体管理（RFID）

２．５　ネットワークの定期的な監視およびテスト(1)

FUJITSU

要件10 (29項目)	ネットワークリソースおよびカード会員データへのすべてのアクセスを追跡および監視する





管理基準の策定

システムセキュリティの管理において重要な役割を果たすログの管理基準を策定します。
ログファイルの運用から整合性の監視、保存、レビューまでを規定します。

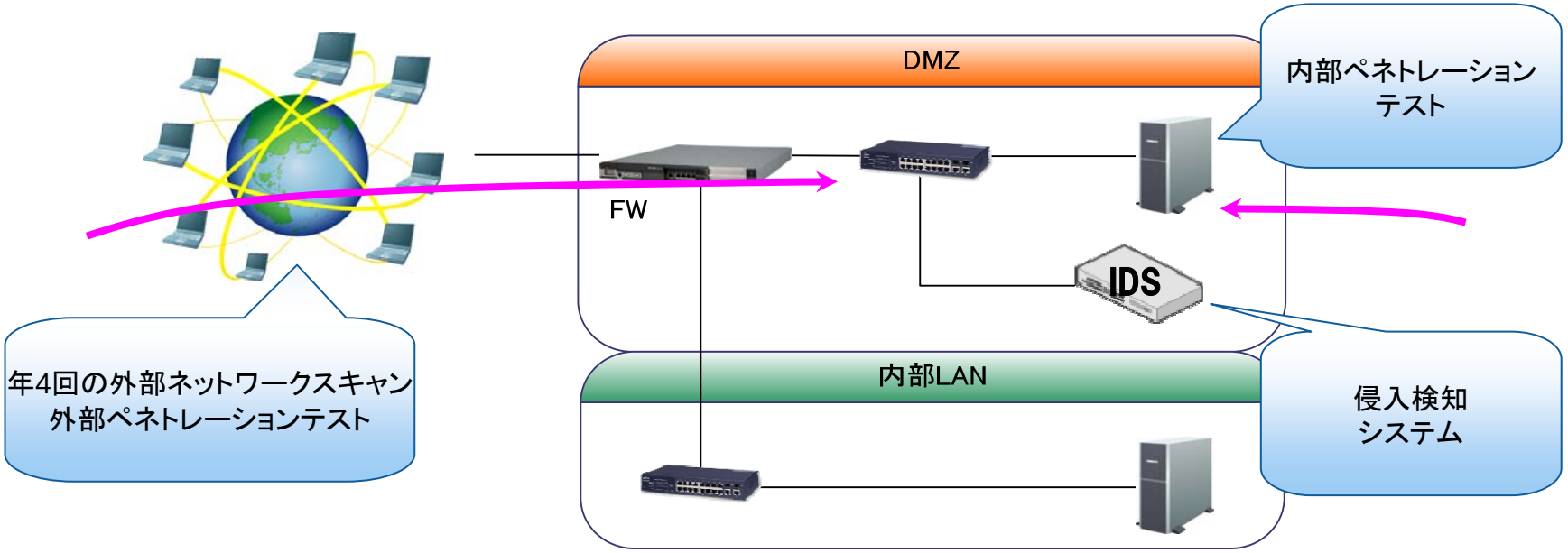
統合ログ管理
(10.5, 10.6, 10.7)

ログファイルを一括管理することで、
・ログの監視作業の効率化
・改ざん防止
を実現する統合管理ソリューションをご提供します。

２．５　ネットワークの定期的な監視およびテスト(2)

FUJITSU

要件11 (21項目)	セキュリティシステムおよびプロセスを定期的にテストする



管理基準の策定

環境の変化による新たな脆弱性の発見および管理を適切に行なうための管理基準を策定します。
重要なシステムに対するテストの実施に関する要求を規定します。

検査ソリューション
(11.2, 11.3)

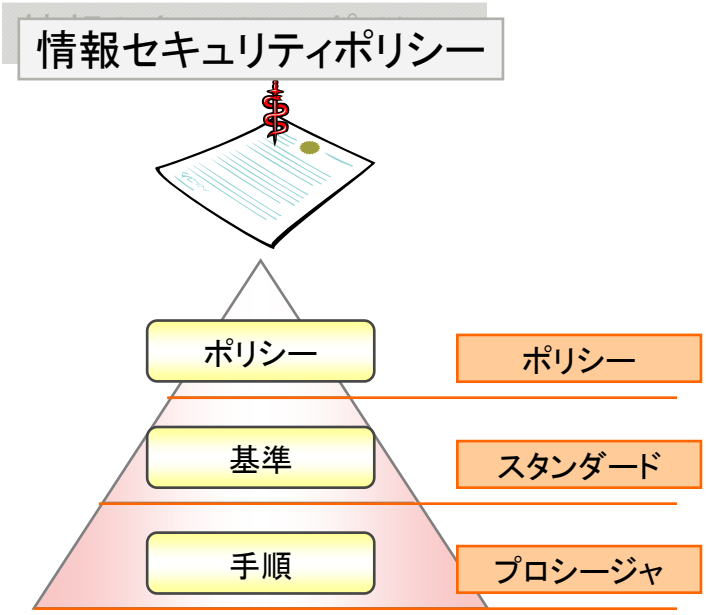
PCI DSS準拠に必要なセキュリティシステムのテストをご提供。診断結果に応じてテストの報告会を実施し、現状についてわかりやすくご説明します。

2．6　情報セキュリティポリシーの整備

FUJITSU

要件12
(40項目)

すべての担当者の情報セキュリティに関するポリシーを整備する



文書の整備

ポリシーを最上位に置く文書体系を構築し、マネジメントシステムの枠組みを作成します。
マネジメントの対象は重要なテクノロジのみならず人的セキュリティの管理にまでに及びます。

作成したマネジメントの枠組みが確実に周知するための教育実施も支援します。

【選考】
- ◆ 新規採用人員の経歴は応募時に確認すること。
- ◆ 請負業者や臨時スタッフも同様に審査すること。

人的セキュリティポリシー

【その他のポリシー】
- ◆ 重要なテクノロジに関するポリシーをそろえる。

重要な技術の利用、取得に関するポリシー

【教育】
- ◆ 雇用時及び少なくとも年に1度従業員を教育する。

教育の実施

3. マルチプラットフォーム対応暗号化ツール COMPLOCK Ⅱ

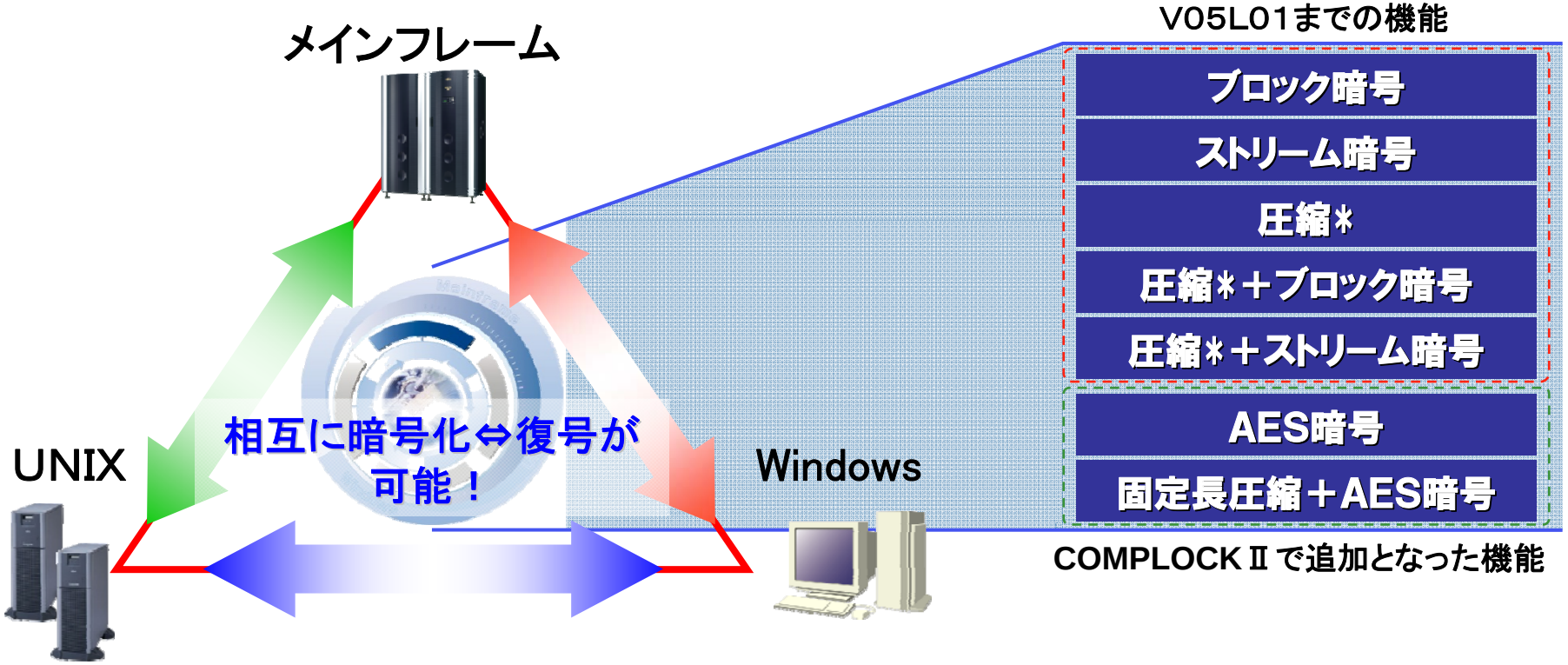
「マルチプラットフォーム対応暗号化ツール　COMPLOCK Ⅱ 」をご紹介いたします。

3．1　COMPLOCKⅡとは？

メインフレームからPCまでマルチプラットフォームに対応したファイル暗号化ツール

☆電子政府推奨暗号（総務省及び経済産業省）
「AES」（共通鍵128ビットブロック暗号）対応！

IPAの「暗号アルゴリズム確認制度」で、AES アルゴリズムを正しく実装していることを確認済みです。
（ http://www.ipa.go.jp/security/jcmvp/algval/aesval.html ）

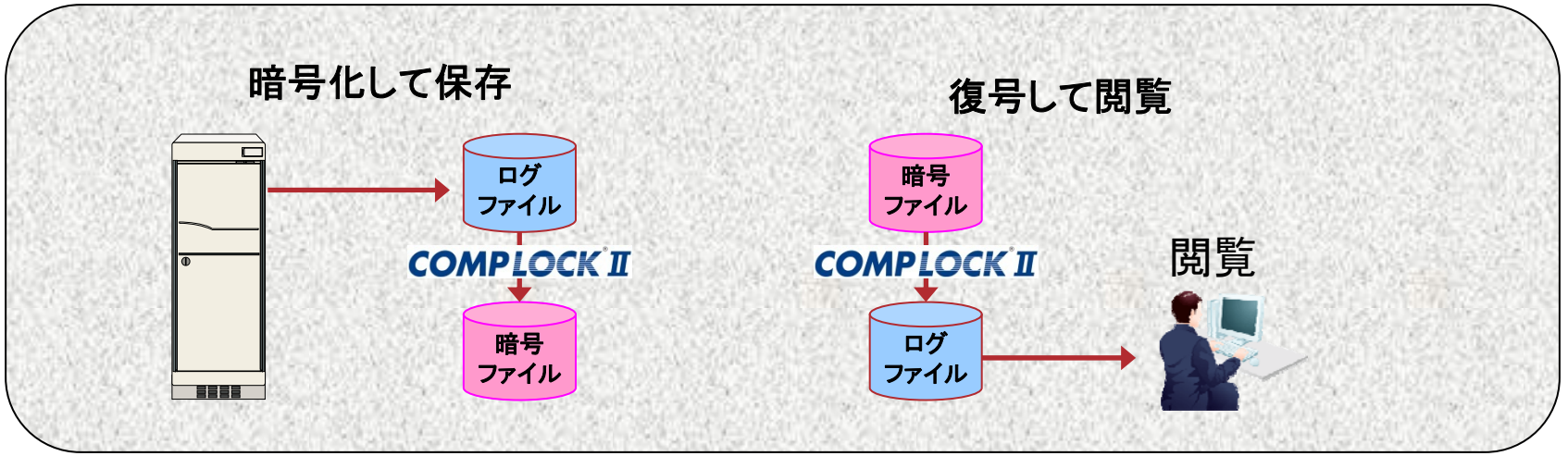


・各OS間で圧縮・暗号化データの互換があります。（文字コード変換機能やファイル転送機能はありません。）
・AS400版では扱えるファイルやCMTに制限があるため、相手先がAS400版の場合は注意してください。
・V05L01で有償オプションであった固定長圧縮オプションが標準機能になりました。

3．2　ご利用形態(1)

バックアップファイルの暗号化

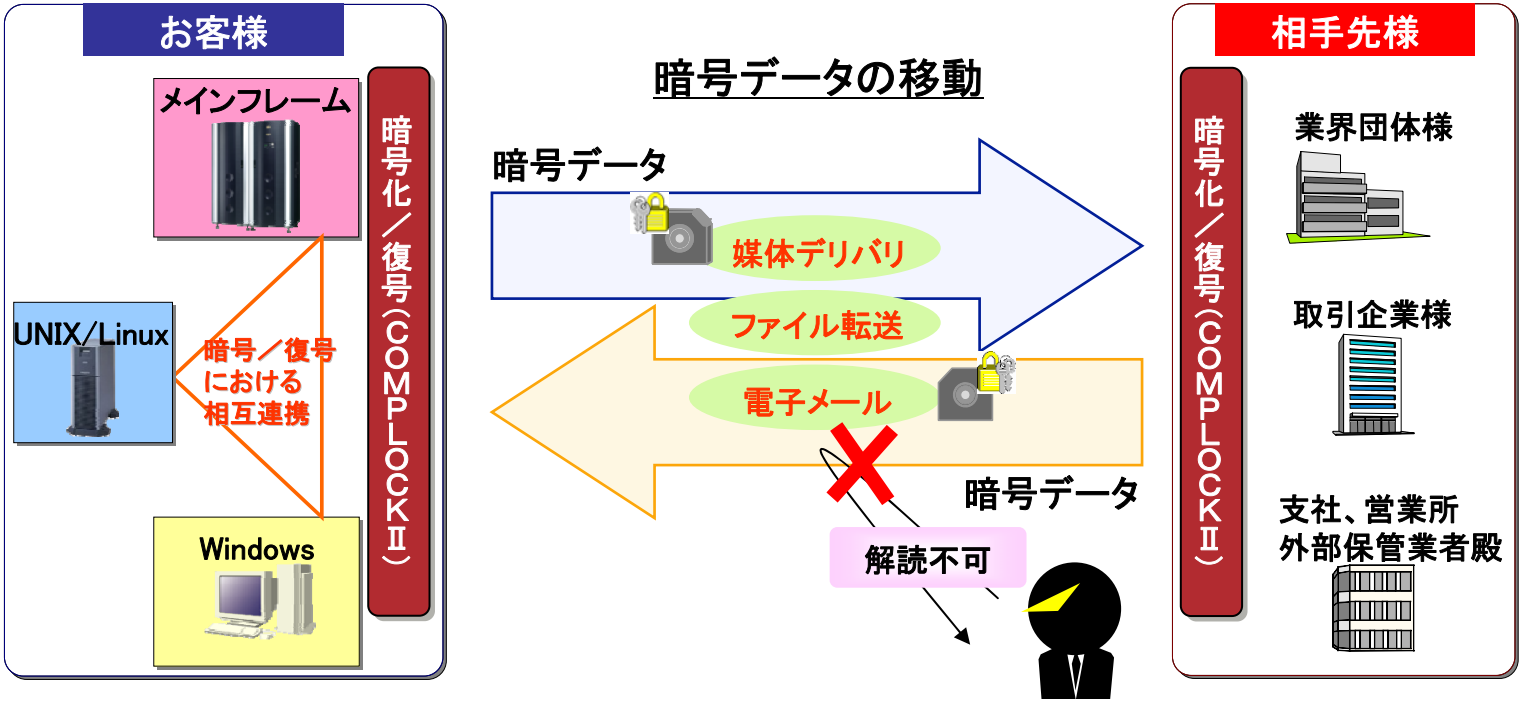
ログファイルの暗号化



3．2　ご利用形態（2）

COMPLOCKⅡはデータの暗号化において、様々なビジネスシーンにてご利用頂いております。

☆メインフレーム，UNIX/Linux，Windows等異なるOS間でファイルを相互に暗号化/復号が可能なマルチプラットフォーム暗号化ソフトウェア



★伝送／媒体等で授受されるファイルの圧縮・暗号化パッケージです。
★多くの金融機関様や一般企業様に利用されており、約1000ユーザー様以上の導入実績がございます。
※主に、金融機関（各銀行・生保・損保・クレジット・その他信用情報機関等の業界団体）様にて幅広くご利用頂いております。）

[特徴]

・マルチプラットフォーム：ﾒｲﾝﾌﾚｰﾑ・UNIX・Linux・Windows等の様々な環境にて動作する製品
・暗号化：独自のストリーム／ブロック暗号機能及び電子政府推奨のAES暗号機能を搭載
・各種オプション：暗号データを強固にするための各種オプション機能を搭載
→マルチプラットフォーム提供／AES暗号機能を併せ持つ暗号ソフトとなります。

3．3　マルチプラットフォーム

FUJITSU

メインフレーム		対象OS	必須ソフト
富士通	MSP版	MSP,MSP-EX	COBOL85（V12L20）実行時ライブラリ
	XSP版	XSP	COBOL85（V12L20）実行時ライブラリ
IBM	COBOL版	OS390,z/OS	VS COBOL Ⅱ、または、COBOL for OS390　の実行時ライブラリ
	PL/I 版	OS390,z/OS	PL/I 1.5　または、PL/I 2.3.0の実行時ライブラリ
	AS400版	OS/400　（V4R2－V7R1）	なし（V6R1、V7R1についてはV6R1、V7R1上でCOMPLOCKⅡが最初に実行されたとき、または呼び出されたときに自動的にV6R1、V7R1用にプログラム変換がおこなわれます。）
日立	COBOL版	VOS3	COBOL85(08-01以降）の実行時ライブラリが必要ですが、無い場合はスタティックリンク版のロードモジュールで動作します。
	PL/I版	VOS3	なし
日本電気	ACOS-4版	ACOS-4	なし
UNISYS	2200版	2200系（バージョン：EXEC45R1以上）	なし

UNIX、Linux		対象OS	CPU
Solaris版		日本語Solaris 9 / 10	SPARC
HP－UX版	PA-RISC版	HP-UX 11iv1,v2	PA-RISC
	Itanium2版	HP-UX 11iv2,v3	Intel® Itanium® 2
AIX版		AIX 6.1 / 7.1	POWER®プロセッサー
Linux版	Intel x86版	Red Hat Enterprise Linux 5, 6 (for x86)	Intel x86　（Intel64上では32ビット互換モード上で32ビットアプリケーションとして動作しますが、RHEL6では32ビットライブラリをご用意ください。）
	Intel x64版	Red Hat Enterprise Linux 5, 6 (for Intel64)	Intel64
	Itanium2版	Red Hat Enterprise Linux　5 (for Itanium)	Intel® Itanium® 2

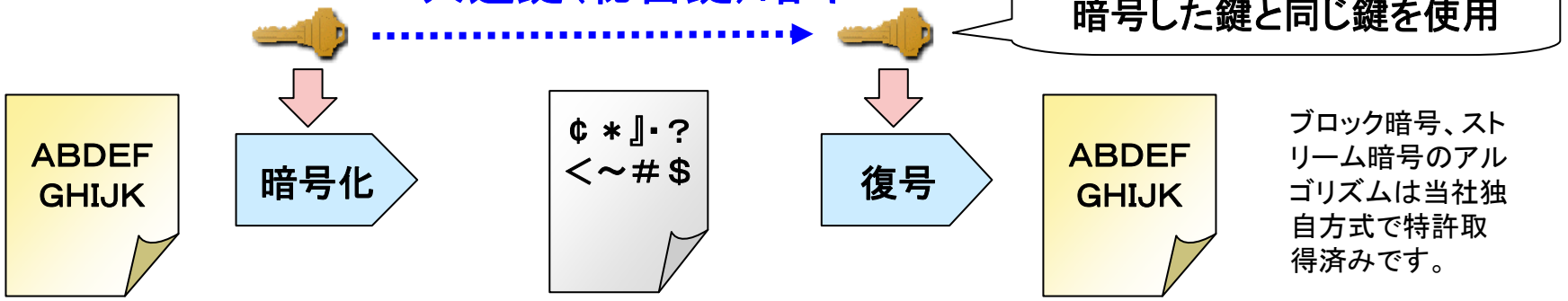
Windows	対象OS
Windows版	Windows XP / Vista (CPU:x86) / 7(Starterは除く)(CPU:x86,x64(WOW64))、 WindowsServer 2003 / 2008(CPU:x86,x64(WOW64)) / 2008R2 (CPU:x64(WOW64))

IBMと日立のCOBOL版とPL／I版の違いはCOMPLOCKⅡの開発言語の違いです。導入環境に応じて、どちらかを選択してください。

3．4　暗号アルゴリズム

FUJITSU

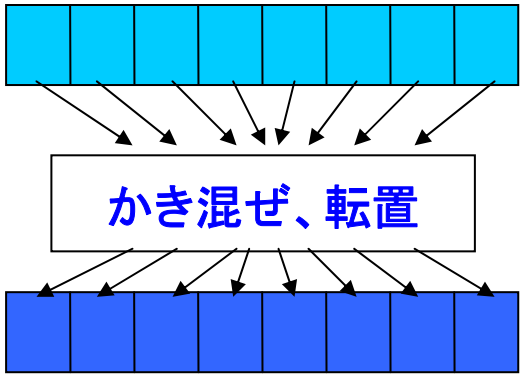
共通鍵（秘密鍵）暗号



ブロック暗号、ストリーム暗号のアルゴリズムは当社独自方式で特許取得済みです。

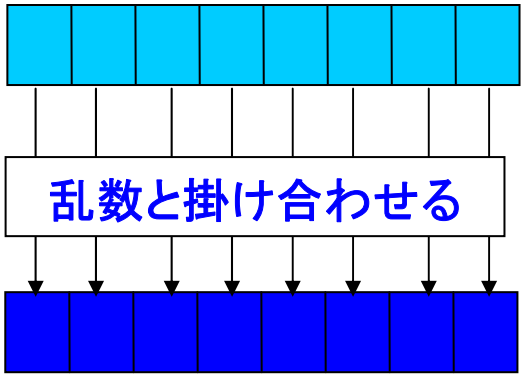
☆COMPLOCKⅡより追加

ブロック暗号



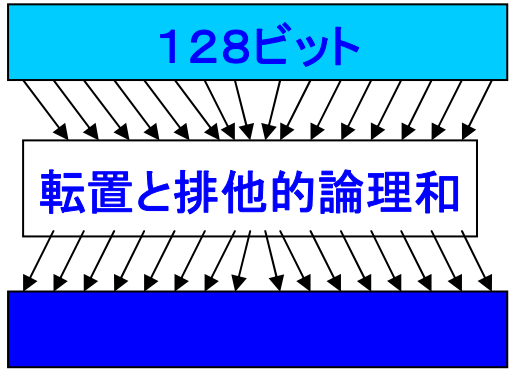
決まった長さ（ブロック）でビット単位にかき混ぜて暗号化

ストリーム暗号



乱数を生成し、乱数と掛け合わせて暗号化

AES暗号



128ビットのブロックで鍵長に応じて転置を繰り返して暗号化

要件3.4　4.2
強力な暗号化技術を利用すること

共通鍵暗号　AES、TDES

排他的論理和：XORとも言い、論理演算の1つで、2つの入力のどちらか1つのみが真であるときに真となる。

3．4　暗号アルゴリズム(AES)

FUJITSU

- AES暗号アルゴリズムは、米商務省の国立標準技術研究所（NIST）が米国の新暗号規格 (Advanced Encryption Standard) として採用した共通鍵暗号方式の128ビットブロック暗号です。（ http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf ）
- 日本でも総務省及び経済産業省が公表した電子政府推奨暗号リストの1つとして採用されています。（ http://www.cryptrec.jp/images/cryptrec_01.pdf ）
- IPAの「暗号アルゴリズム確認制度」で、COMPLOCKⅡではAES アルゴリズムを正しく実装していることを確認済みです。（ http://www.ipa.go.jp/security/jcmvp/algval/aesval.html ）

COMPLOCKⅡでは、AES暗号アルゴリズムを以下の仕様で利用できます。

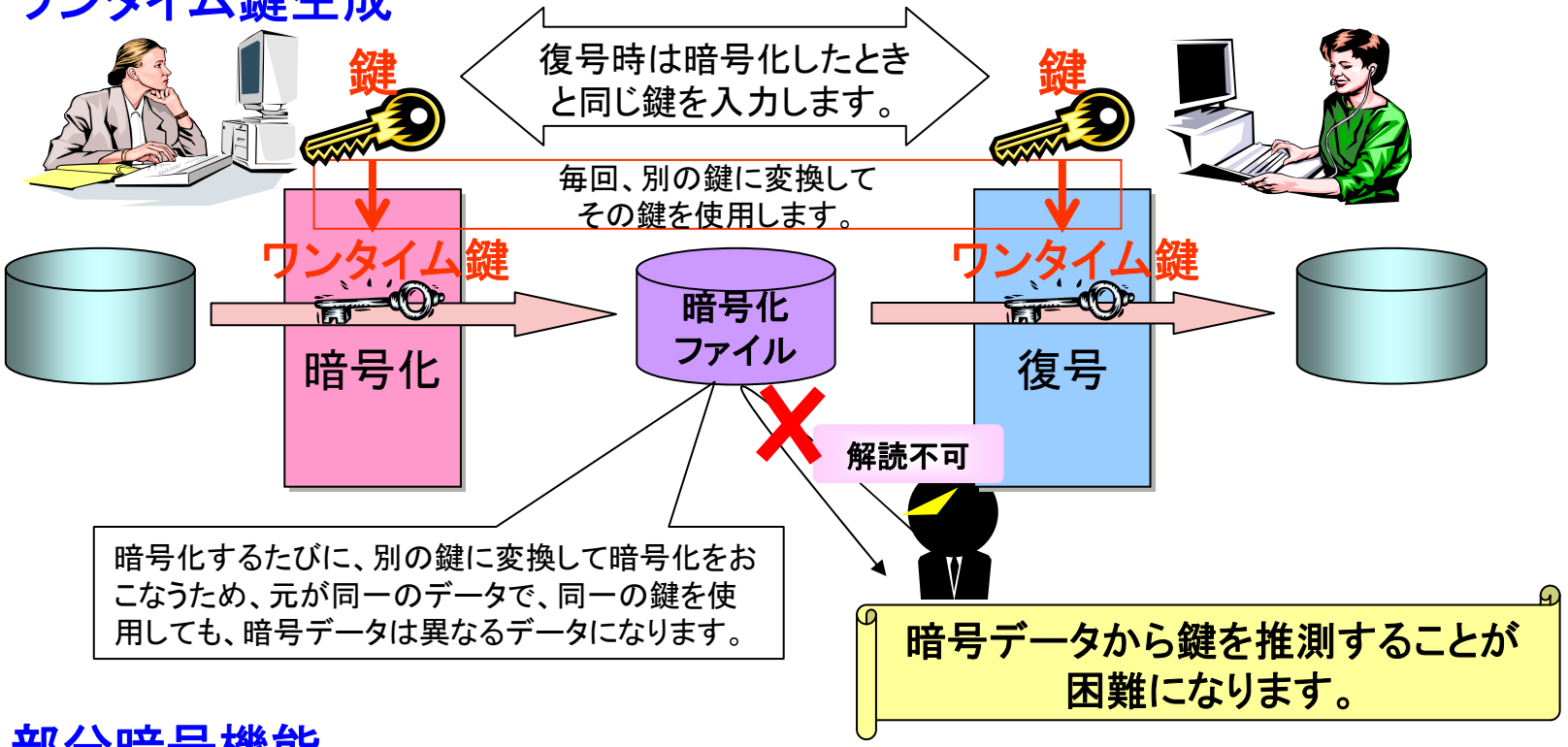
鍵長	128、192、256ビットのいずれも使用可能
ブロック長	128ビット（16バイト）
暗号利用モード	ECBモード、CBCモード
パディング方式	PKCS＃5方式　（レコード単位にパディング）

※AES暗号は128ビットを暗号化するアルゴリズムです。ファイル暗号化製品によってAES暗号の実装方法が異なりますので、CICLOCKⅡ以外の暗号化製品との互換はありません。

３．５　暗号化時のオプション機能（１）

FUJITSU

ワンタイム鍵生成



部分暗号機能

レコード内の一部分のみを最大５箇所まで暗号化することができます。

	クレジットカード番号		有効期限		氏名	

s1バイト目～e1バイト目、s2バイト目～e2バイト目　・・・　のようにパラメータで指定します。

AES暗号使用時（圧縮なし）で、対象ファイルが固定長ファイルのときのみ利用できます。

３．５　暗号化時のオプション機能（２）

FUJITSU

固定長圧縮

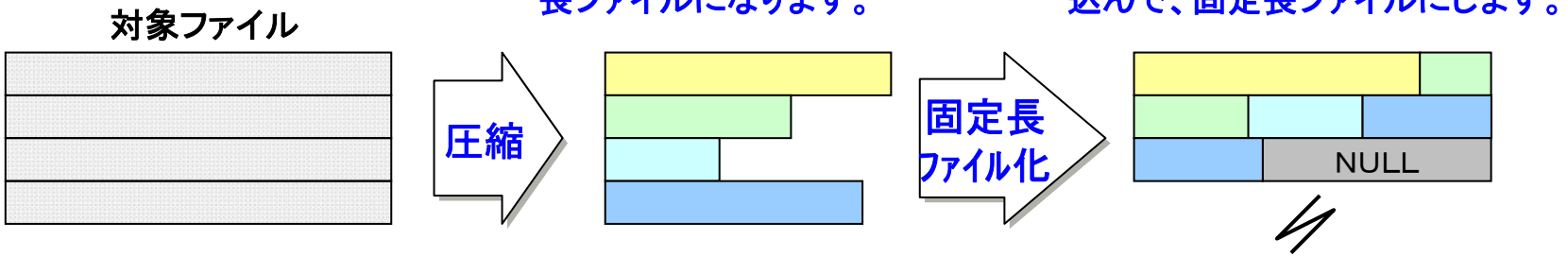
☆　COMPLOCKⅡでは
標準機能になりました。

固定長圧縮しない場合

各レコードは圧縮されて可変長ファイルになります。

固定長圧縮した場合

指定した長さのレコード長に詰め込んで、固定長ファイルにします。



※　ブロック暗号、ストリーム暗号の場合は、固定長圧縮の有無は可能ですが、AES暗号の場合は、必ず固定長圧縮形式になります。

メインフレームとUNIXやPC間でのファイル転送に便利

隣接するレコード間で、同一データを圧縮する方式を採用。

同じような内容のレコードが連続する、固定長レコードフォーマットを持ったファイルに有効です。

顧客コード	店舗コード	利用年月日	利用金額
910001	10119	070601	0005000
910001	10119	070602	0003000

圧縮データ

前レコードと同一のデータが圧縮されます。

３．６　暗号化処理イメージ（１）

FUJITSU

メインフレーム版COMPLOCK Ⅱ

メインフレーム版はバッチジョブで実行するユーティリティです。

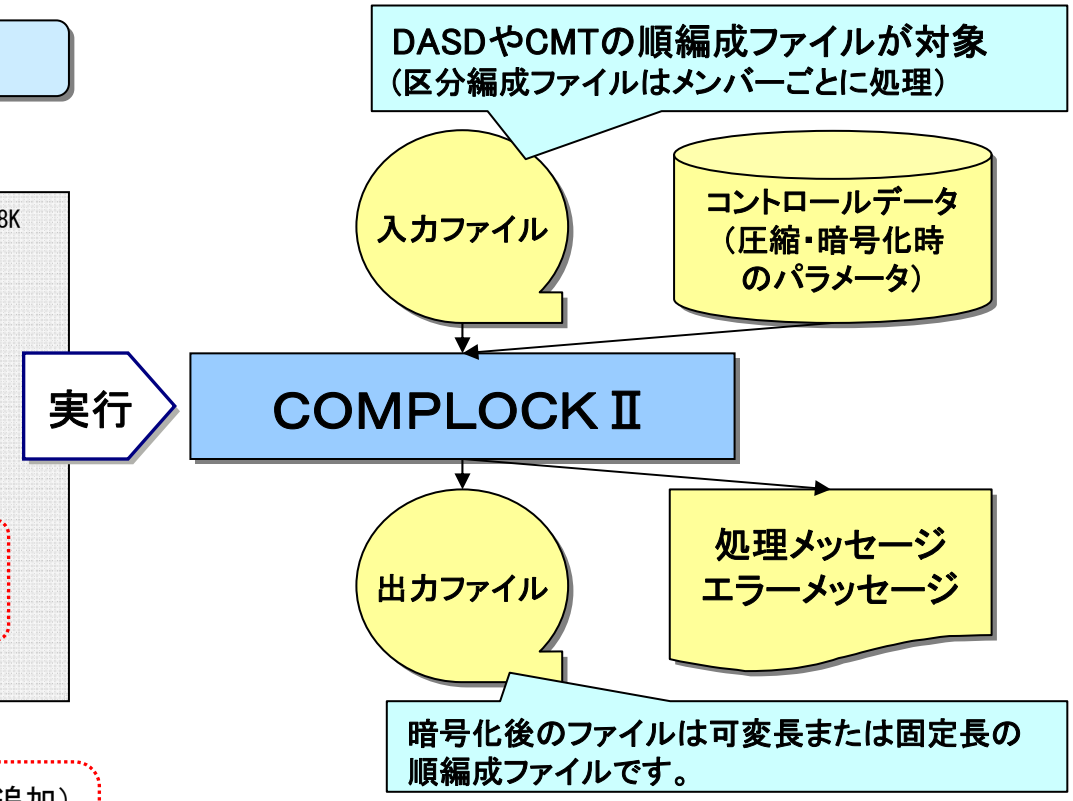
JCL（ジョブ制御文）より起動

MSP版、IBM版、VOS3版のJCL例

```
//LOCK      JOB LOCK,MSGCLASS=A,CLASS=A,REGION=2048K
//JOBLIB     DD  DSN=SYS1.COBLIB,DISP=SHR
//           DD  DSN=LOCK61.LOAD,DISP=SHR
//*** STEP1 ENOODE  ***
//ST1   EXEC PGM=LOCK6250
//CIIN       DD  DSN=DATA1,DISP=SHR
//CIOUT      DD  DSN=DATA1.ENC,UNIT=SYSDA,
//     SPACE=(TRK,(10,10),RLSE),DISP=(NEW,CATLG)
//SYSDBOUT   DD  SYSOUT=*
//SYSOUT     DD  SYSOUT=*
//CICL       DD  *
PROC=5,
 KEY=(1234567890ABCDEF),
  IV=(ABCDEF0000000000),
 CBC=ON,TABLE=256,CODE=(123456789),AUTOKEY=ON
/*
//*
```

AES暗号時のパラメータ例（COMPLOCK Ⅱで追加）

```
PROC=6,
 KEY=(1234567890ABCDEF1234567890ABCDEF),
  IV=(ABCDEF0123456789ABCDEF0123456789),
 CBC=ON,CODE1=(1234567890XYZ),AUTOKEY=ON,PAD=ON
```



※暗号化したファイルをCMT装置のハード圧縮を使用してCMTへ格納する場合、ハード圧縮の効果はなくなりますのでテープ本数が増える場合があります。

※AS400版はGUIで実行します。なお、次の制約があります。①テープからテープへの処理はできません。 ②使用できるテープはIBM標準ラベルのテープのみが対象になります。 ③ディスク上のファイルは物理ファイルのみが対象になります。 ④固定長ファイルのみが対象になります。⑤ハッシュパラメータは使用できません。

３．６　暗号化処理イメージ（２）

FUJITSU

UNIX版・Linux版COMPLOCK Ⅱ

コマンド形式で提供します。

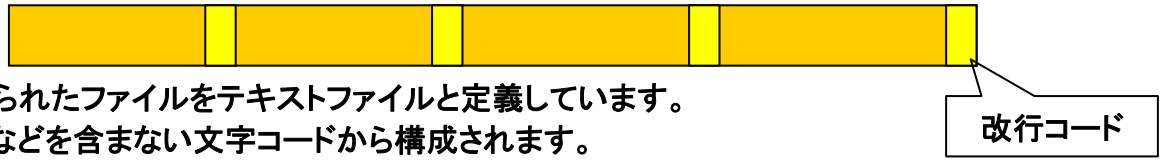
圧縮・暗号化時のコマンド例

```
encode  -i  入力ファイル名    -o  出力ファイル名  -k 鍵      ・・・・・・  他、パラメータを指定
```

ユーザが作成するシェルスクリプトからコマンドを発行することができます。

COMPLOCK Ⅱ では暗号化対象ファイルを以下の３つに分類して定義しています。
メインフレームとの互換をとるため、レコード単位で圧縮・暗号化を行います。

テキストファイル



レコードごとに改行コードで区切られたファイルをテキストファイルと定義しています。
各レコードはNULLや制御コードなどを含まない文字コードから構成されます。
改行コードを除いてデータ部だけを暗号化して出力します。

バイナリファイル

すべてのコード（バイナリコード）から構成されるファイルをバイナリファイルと定義しています。
レコード長をパラメータで与える(必須)ことにより、レコード単位での圧縮・暗号化を行います。

RDW付きファイル

レコードの長さ情報（RDW)が各レコードの先頭に付いたファイルをRDW付きファイルと定義しています。
RDWとはレコード長2バイト＋2バイトの0x0000からなる4バイトのレコード長情報です。
RDWを除いてデータ部だけを暗号化して出力します。

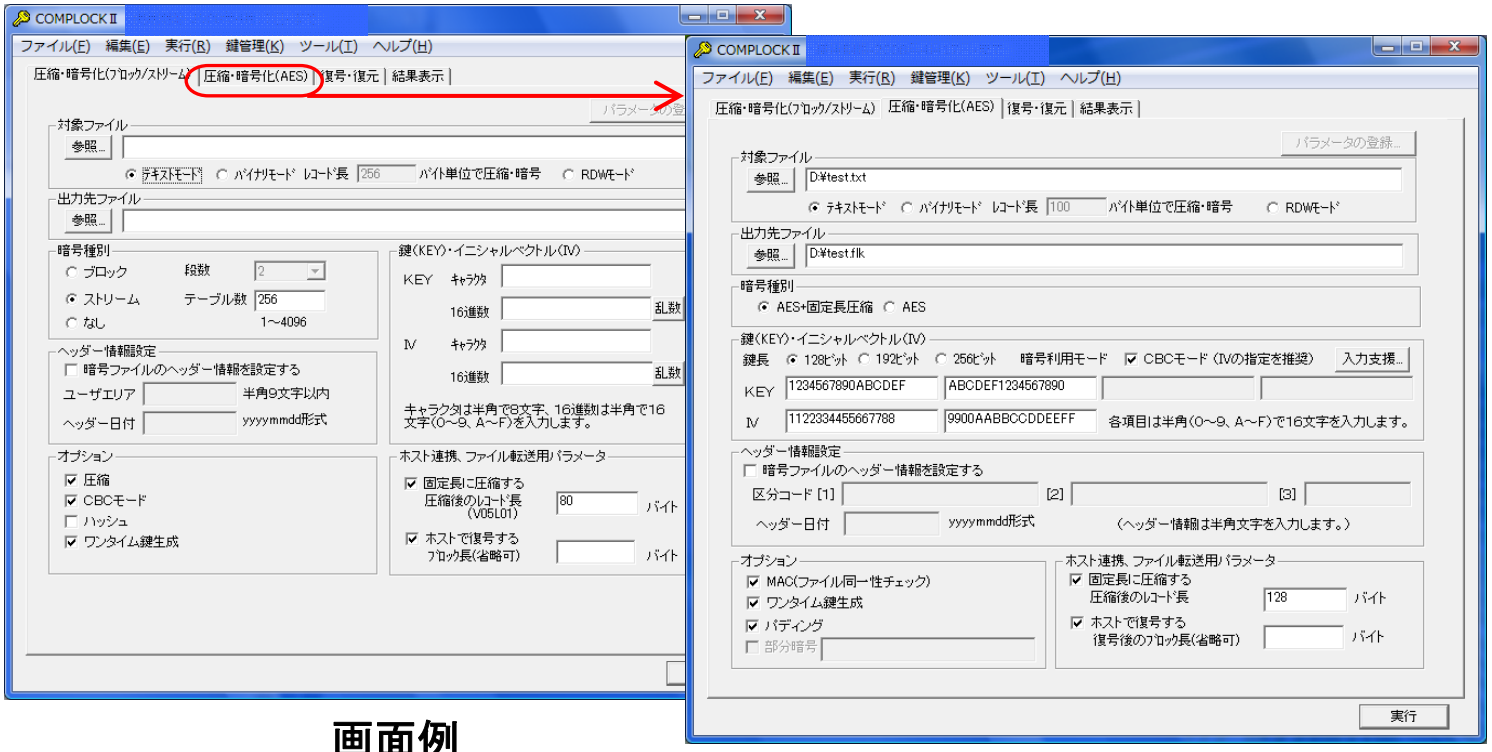
復号時にはパラメータで上記の３形式のどれに戻すかを指定します。

3．6　暗号化処理イメージ（3）

Windows版COMPLOCK Ⅱ

Windows版はGUIでご利用できます。（バッチ機能を利用してコマンドでの実行も可能。）

暗号化対象ファイルの扱いはUNIX・Linux版と同じです。



画面例　　画面例（AES暗号用）

※対象とするファイルサイズは4GB未満ですが、復号時のみ4GB以上でも可能です。

※IBMフォーマットのフロッピーは扱うことができません。

※CMTを直接、読み書きすることはできません。暗号化したファイルを別途CMT装置のユーティリティを使用してCMTと読み書きする必要があります。

3．7　動作環境・導入方法

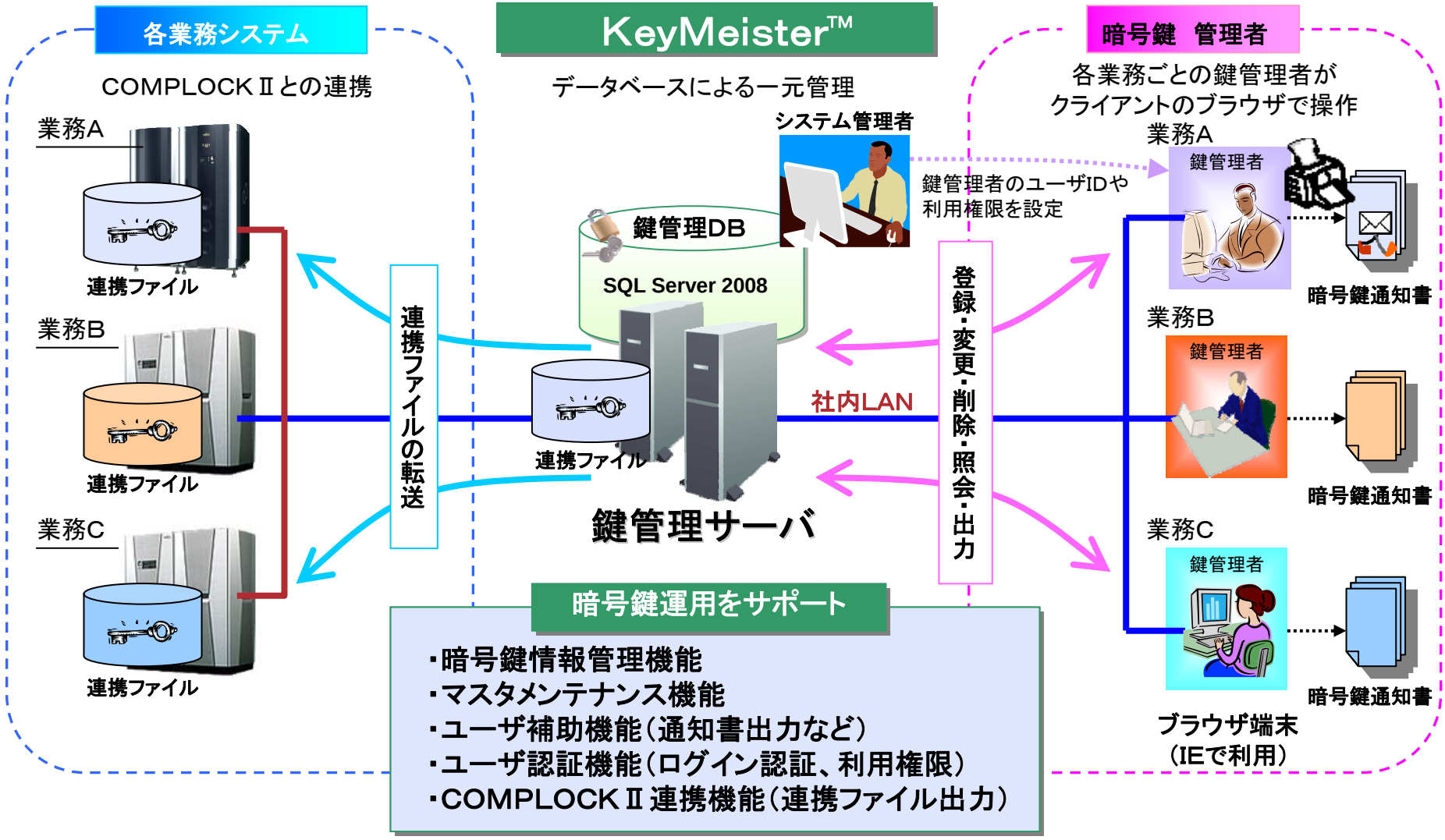
	メインフレーム版	UNIX・Linux版	Windows版
提供媒体	1/2インチCMT （富士通版は36トラック、 他は18トラック） *AS400版はCD-ROM 	CD-ROM 	CD-ROM 
メモリ	REGIONサイズ：2MB	64MB以上推奨	128MB以上推奨
ディスク容量	100ﾄﾗｯｸ（ロードモュール）	2MB以上	5MB以上
導入方法	CMTからロードモジュール、動作確認用のテスト用JCLとテストデータを各OSのデータセットユーティリティでコピーするだけです。マシンの再起動やシステムパラメータの設定は不要です。 動作確認用のジョブを実行して正常に動作するか確認することができます。	CD－ROMから、tarで固めてあるファイルをインストール先のディレクトリにコピーして展開すれば、実行形式と動作確認用のスクリプト、テストデータが展開されます。 マシンの再起動やシステムパラメータの設定は不要です。	インストーラーによりインストールします。インストール直後は1ヶ月間しか使用できません。ライセンス認証画面に表示されるシリアルNo.とMACアドレスを弊社までご連絡いただくことによって、ライセンスキーを発行します。 ライセンスキーを入力することによって正規のライセンスとしてご利用できます。

4. 暗号鍵管理システム　KeyMeister

「暗号鍵管理システム　KeyMeister」をご紹介いたします。

4．1　KeyMeisterとは？

■KeyMeisterで複数業務システムの暗号鍵運用を実現。



4．2　KeyMeisterで管理する主要項目

FUJITSU

■KeyMeisterで管理する主要項目

KeyMeisterでは、下記の表のような項目を鍵管理データベースで管理します。（下表の項目はスペースの都合上一部のみ表示。）
業務や相手先ごとに異なる鍵の運用ポリシーを設定して、鍵の有効期間管理、世代管理を行うことができます。

暗号化対象業務（区分1コード）	相手先（区分2コード）	その他（区分3コード）	鍵の文字数	KEY	IV	有効期間開始日	有効期間終了日	次回更新予定日
給与振込	A銀行	総務部	16	9A476F9E91E64E13	FFF76F9E91E64999	20111001	20111231	20111210
			16	7233B68BE092DD8D	DEF3B68BE092D111	20120101	20120331	20120310
	C銀行	経理部	32	4C3962CADCF628BF･･･	0C4962CADCF620C7･･･	20111101	20120430	20120410
			32	45C44C944FDBB2A8･･･	11144C944FDBBFFF･･･	20120501	20121030	20121010
ログ暗号化	業務Aサーバ	―	16	9A476F9E91E64E13	ABCDEF1234567890	20120101	20120630	20120601
	業務Bサーバ	―	16	5C46D7A56C727A89	1234567890123456	20120101	20120630	20120601
バックアップ	ファイル1	―	32	F992EB63A550AE66A･･･		20100101	無制限	―
	ファイル2	―	32	0C37723D56D181BC8･･･		20100101	無制限	―
	ファイル3	―	32	703672C2B94CA12BD･･･		20100101	無制限	―
設計図送付	X部品製造会社	―	8	gh&1e5#h		20120101	20121231	20121215

暗　号　化

要件3.5.1
暗号化キーへのアクセスを
必要最小限の管理者に制限する。

要件3.5.2
暗号化キーを安全に保存する。
要件3.6.1
強力な暗号化キーの生成

要件3.6.4
暗号化キーの変更

4．3　KeyMeisterの機能（1）

FUJITSU

■KeyMeister機能一覧

機能	内容
鍵情報管理機能	[鍵情報新規登録機能] 業務ごと、相手先ごとにCOMPLOCKⅡのKEY，IVや、COMPLOCKⅡ以外の暗号鍵をDBに暗号化して登録。（CSVからの一括登録も可能） [鍵情報有効期限管理機能] 有効期限間近な暗号鍵の存在をﾛｸﾞｲﾝ後のﾄｯﾌﾟﾒﾆｭｰで通知。 [一括更新機能] 有効期限間近の暗号鍵を一括で更新。
マスタメンテナンス機能	[マスタデータ更新機能] ﾕｰｻﾞIDの登録（ｼｽﾃﾑ管理者機能）、相手先マスタや業務マスタの更新、一覧の印刷。 [暗号鍵の運用ポリシの設定] 暗号鍵の使用可能文字や文字数、一括更新時の有効月数などを設定。
ユーザ補助機能	[絞込み検索機能] 暗号鍵の種類、相手先や業務、暗号鍵の有効期間による検索。 [帳票出力] 暗号鍵通知書、一覧表の帳票出力やCSVﾌｧｲﾙ出力。
ユーザ認証機能	[ログイン認証] ﾕｰｻﾞID，ﾊﾟｽﾜｰﾄﾞによるﾛｸﾞｲﾝ認証。 [権限別機能] ｼｽﾃﾑ管理者、鍵管理者による機能制限。
COMPLOCKⅡ連携機能	[連携ファイル出力] DBからCOMPLOCKⅡのKEY，IVを連携ﾌｧｲﾙに出力。 （COMPLOCKⅡの簡易鍵管理オプション（別途有償ｵﾌﾟｼｮﾝ）でCOMPLOCKⅡと連携して暗号/復号を実施）

4．3　KeyMeisterの機能（2）

FUJITSU

■鍵情報管理機能概要

★鍵登録機能

・鍵管理機能：相手先情報、業務情報、鍵情報の追加／変更／削除
・一括更新機能：有効期限切れ間近の鍵情報を一括更新することも可能

★有効期限管理機能

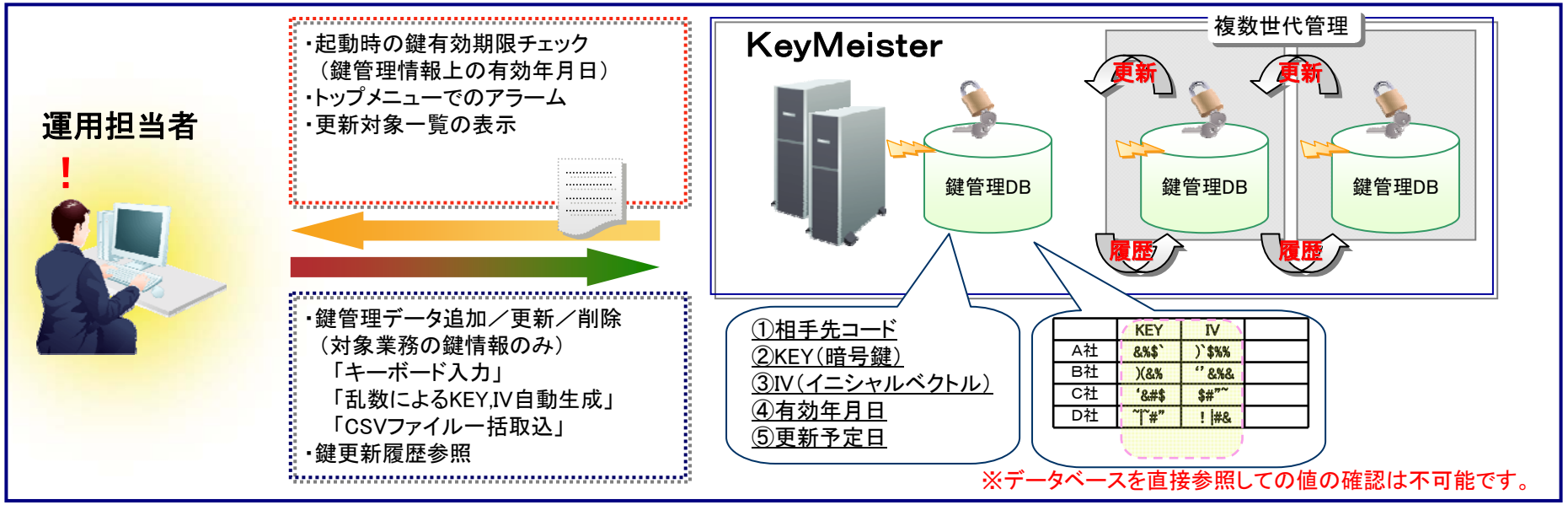
・アラーム通知機能：起動時の有効期限チェックによる定期的な暗号鍵の更新アラーム機能。定期的な暗号鍵の更新による
　セキュリティの向上。
・一覧表出力機能：更新が必要な暗号鍵の一覧表を出力する。

★鍵情報履歴保存機能

・鍵情報履歴保存機能：更新／削除時に更新前の鍵管理情報を履歴として保存します。履歴は、複数世代を管理する
　ため、削除を行わない限り過去の鍵管理情報の参照が可能となります。

★鍵情報暗号機能

・鍵情報暗号機能：暗号鍵をAES暗号で暗号化して保存します。



4．3　KeyMeisterの機能（3）

■通知書、鍵情報一覧表出力機能

★通知書出力機能

・相手先に鍵情報を連絡する通知書の印刷機能

「通知項目」

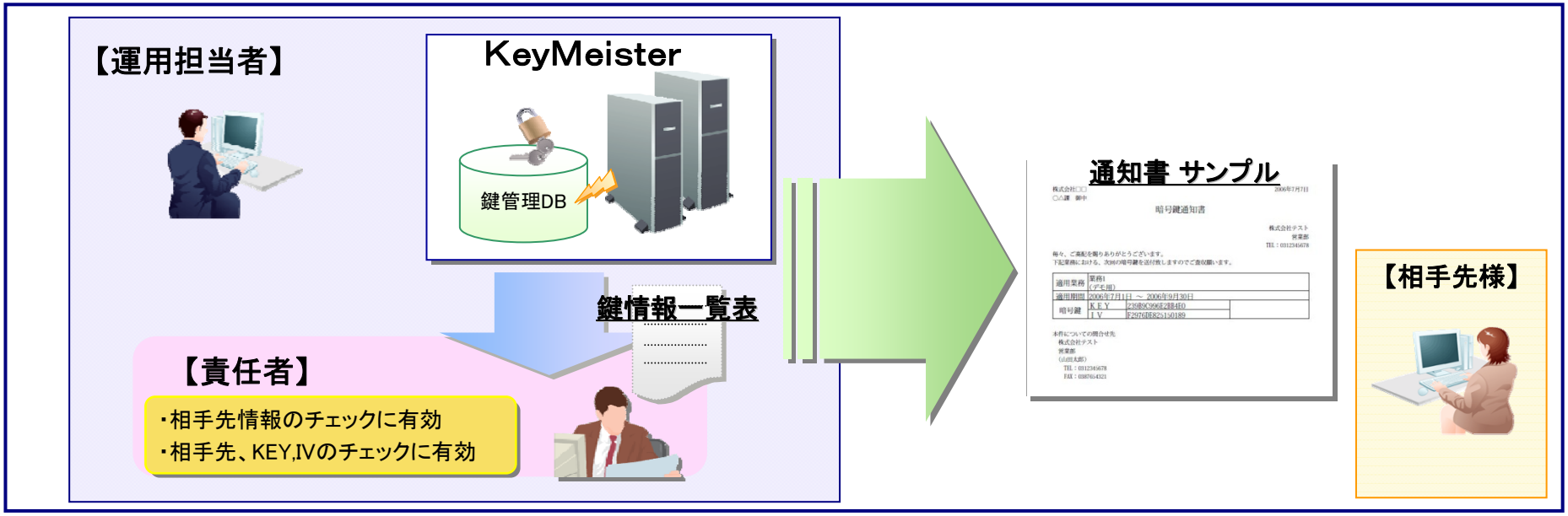
相手先名　業務名　有効期間　KEY,IV　問合せ先

★鍵情報一覧出力機能

・相手先情報の確認、管理等に用いる帳票の印刷機能

「表示内容」

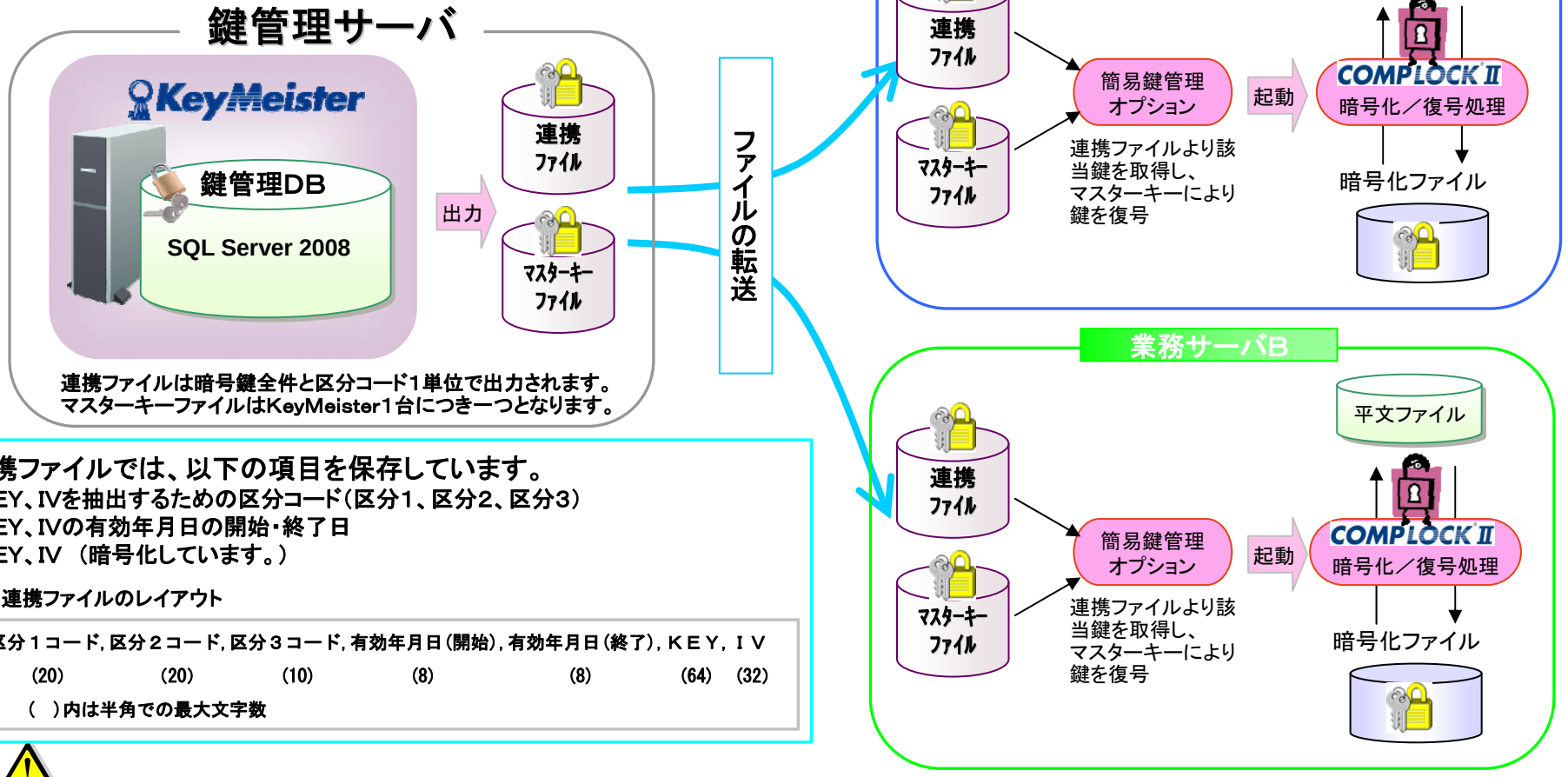
業務名コード　業務名　相手先コード　相手先名　KEY,IV　有効期間　更新予定日　通知予定日



4．4　COMPLOCKⅡとの連携（1）

■連携イメージ

・要件3.5
キー暗号化キーはデータ暗号化キーと同じ強度が必要
・要件3.6.2
安全な暗号化キーの配布



連携ファイルは暗号鍵全件と区分コード1単位で出力されます。
マスターキーファイルはKeyMeister1台につき一つとなります。

連携ファイルでは、以下の項目を保存しています。
・KEY、IVを抽出するための区分コード（区分1、区分2、区分3）
・KEY、IVの有効年月日の開始・終了日
・KEY、IV （暗号化しています。）

◆連携ファイルのレイアウト

区分１コード	区分２コード	区分３コード	有効年月日（開始）	有効年月日（終了）	ＫＥＹ	ＩＶ
(20)	(20)	(10)	(8)	(8)	(64)	(32)

（　）内は半角での最大文字数

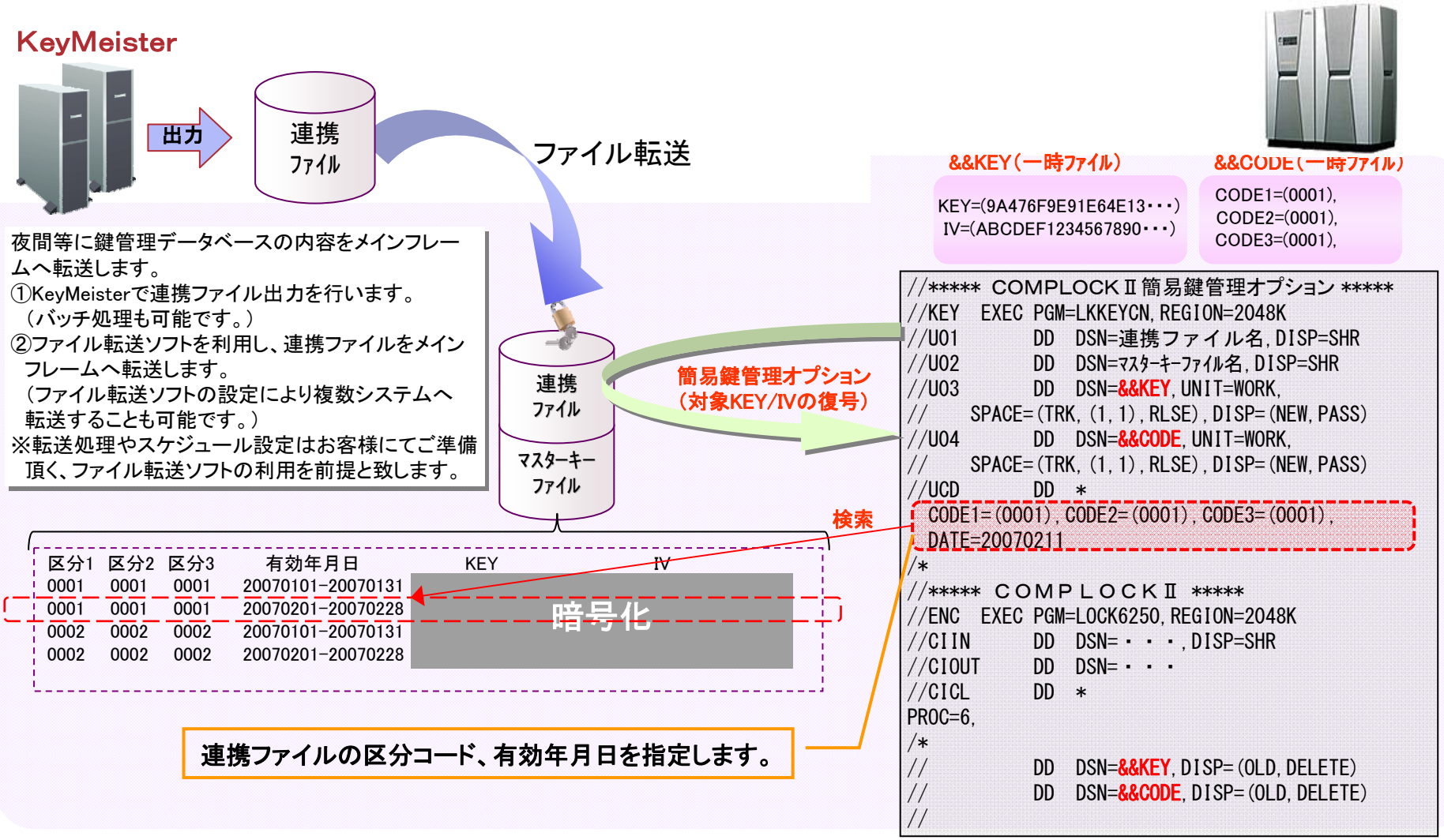
鍵管理サーバから業務サーバへファイル転送する機能はありません。
貴社の環境に応じたファイル転送ソフト等が別途必要となります。

マスターキーファイルは、連携ファイル上に暗号化されて保存されている暗号鍵を復号するための暗号鍵になります。

4．4　COMPLOCKⅡとの連携（2）

■KeyMeisterとCOMPLOCKⅡの連携について　（メインフレーム例）

区分コードと対象日付をキーに連携ファイルからKEY,IVを復号して一時ファイルに出力し、COMPLOCKⅡのステップにわたします。



4．4　COMPLOCKⅡとの連携（3）

FUJITSU

■KeyMeisterとCOMPLOCKⅡの連携について　（UNIX版、Linux版、Windows版の例）

COMPLOCKⅡのコマンドの代わりに、簡易鍵管理オプションの連携コマンドを実行して暗号化／復号をおこないます。
コマンドには鍵、IVを指定する代わりに、区分コード、有効年月日をパラメータで指定します。
パラメータで指定された区分コード、有効年月日をもとに連携ファイルを検索して鍵とIVを取り出して、暗号化／復号をおこないます。

通常の暗号化時のコマンド例

```
encode  -i  入力ファイル名    -o  出力ファイル名  -k 鍵  -v IV  ・・・・・・  他、パラメータを指定
```

鍵・IVをオプションとして指定する必要がなくなり、
暗号鍵の漏洩を防ぐことができる。

簡易鍵管理オプションの連携コマンドを使用した暗号化時のコマンド例

```
lockcnct  -i  入力ファイル名    -o  出力ファイル名  -ed 0  -cd1 0001 -cd2 0001 -cd3 0001 -dt 20120201  ・・・・・・  他、パラメータを指定
```

区分コードと有効年月日をパラメータを指定します。
※-dtパラメータを省略した場合はシステム日付で検索します。

区分コード、日付で有効な鍵を検索

指定された鍵を抽出

暗号化されている、
KEY、IVを復号

連携
ファイル

マスターキー
ファイル

KEY、IVを取得

区分1	区分2	区分3	有効年月日	KEY	IV
0001	0001	0001	20110701-20111231	暗号化	
0001	0001	0001	20120101-20120630		
0002	0002	0002	20110701-20111231		
0002	0002	0002	20120101-20120630		

連携コマンドがCOMPLOCKⅡを
起動して暗号化／復号を実行

4．5　他社製暗号ソフトの鍵管理（1）

■COMPLOCKⅡ以外の鍵管理

COMPLOCKⅡのAES暗号用の鍵長（128,192,256ビット）に対応するとともに、任意＊の文字列の鍵の生成や管理を行うことも可能となります。　＊使用できる文字は下の画面に表示されている文字で、最大64文字です。
このため、他社暗号ソフトの鍵やパスワードの管理をすることもできます。

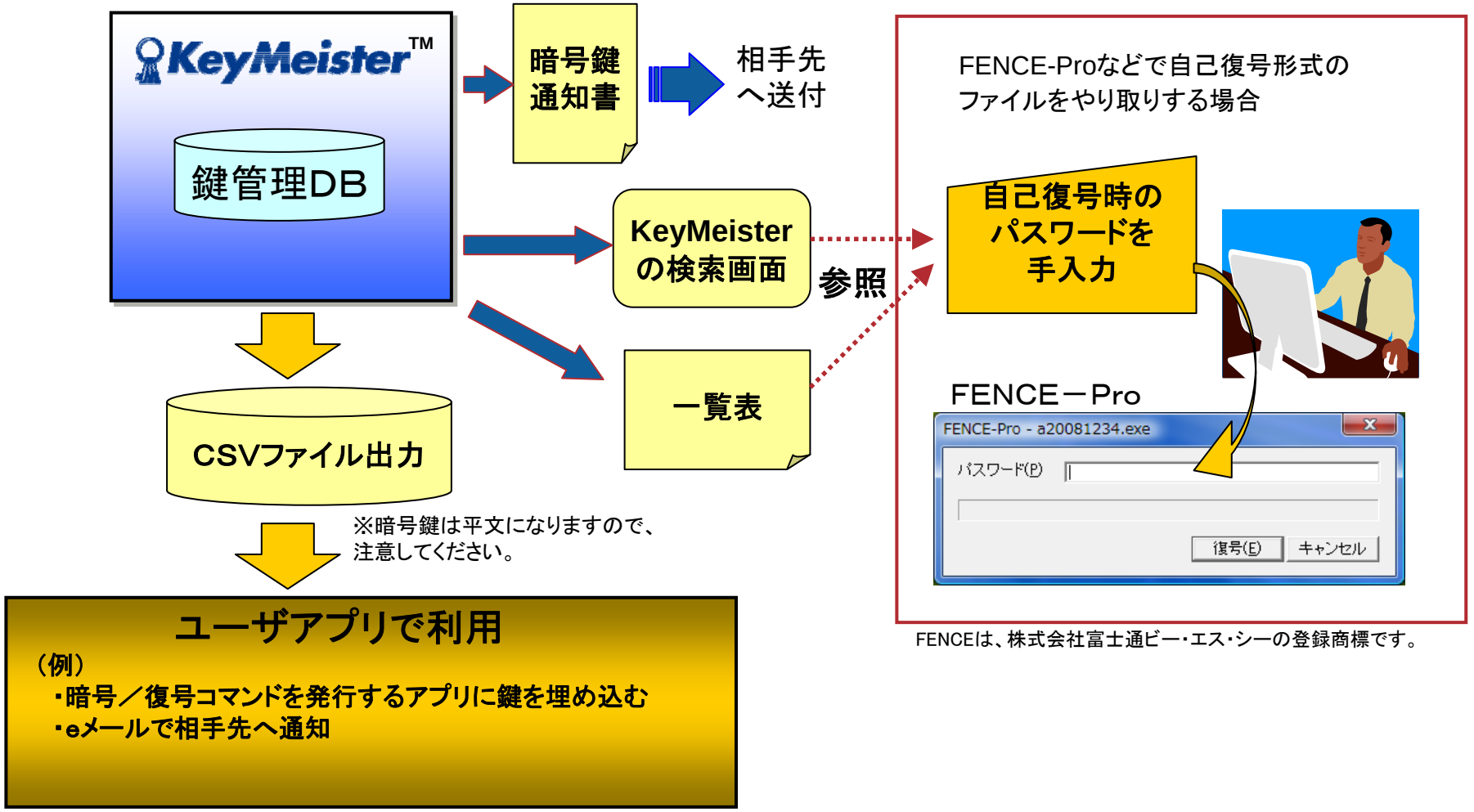
鍵の種類ごとに文字数や使用可能文字を設定して、管理することができます。

COMPLOCKⅡ以外の鍵の設定画面

4．5　他社製暗号ソフトの鍵管理（2）

■他社製暗号ソフトの鍵の運用

COMPLOCK Ⅱ 以外の鍵は連携ファイルには出力できませんが、CSVファイルに出力してユーザアプリで利用することができます。



FENCEは、株式会社富士通ビー・エス・シーの登録商標です。

4．6　ハードウェア／ソフトウェア要件

FUJITSU

■ハードウェア要件

	サーバ	クライアント
CPU	Intel Pentium III600 MHz 以上または同等の互換プロセッサ (1GHz 以上を推奨)	
メモリ	1GB以上（4GB以上を推奨）	512MB 以上のメモリ (1GB以上を推奨)
ディスク	約300MB(KeyMeisterのコンテンツ使用分のみ)(注1)	―
ディスプレイ	Super VGA (最小で 1,024x768 ピクセル) 以上の解像度の ビデオ アダプターおよびモニタ	
ドライブ	CD-ROM または DVD-ROM ドライブ	―

(注1)ミドルウェア及びミドルウェアソフトが使用するデータ領域は含まれません。

■ソフトウェア要件

	サーバ	クライアント
OS	Microsoft Windows Server 2008 Standard/Enterprise Edition SP1以上 (32ビット/64ビット) Microsoft Windows Server 2008 Standard/Enterprise Edition R2 (64ビット)	Windows XP Windows Vista Windows 7
WEBサーバソフト	Microsoft IIS 7.0サーバ (Server 2008用)(注2) Microsoft IIS 7.5サーバ (Server 2008 R2用)(注2)	―
データベース	Microsoft SQL Server 2008 Express(無償版) Microsoft SQL Server 2008 R2 Express(無償版) Microsoft SQL Server 2008 Standard/Enterprise Microsoft SQL Server 2008 Standard/Enterprise R2 Microsoft SQL Server 2008 64ビットStandard/Enterprise Microsoft SQL Server 2008 64ビットStandard/Enterprise R2	―
ブラウザ	Microsoft Internet Explorer 7.0,8.0,9.0(注3)	Microsoft Internet Explorer 7.0,8.0,9.0
PDFリーダ	Acrobat Reader 9.0,10.0(注3)	Acrobat Reader 9.0,10.0
その他	.NET Framework 3.5 SP1 ASP.NET 2.0	―

(注2)64ビットコンピュータにインストールするときは、32ビットモードを使用するようにIISを変更してください。
(注3)サーバ上でKeyMeisterを操作しない場合は、サーバにブラウザ、PDFリーダの導入の必要はありません。

5. お問い合わせ先

5. お問い合わせ先

FUJITSU

ご清聴ありがとうございました。

- ご質問、ご相談は下記窓口まで

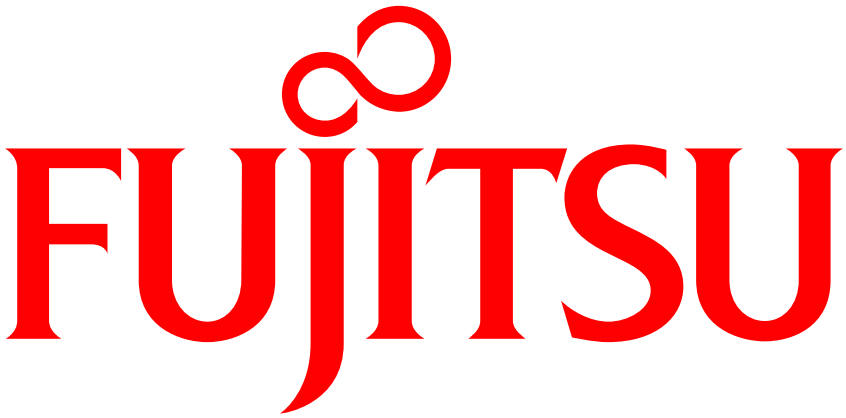
富士通エフ・アイ・ピー株式会社

アプリケーションサービス推進部

〒105-8668

東京都港区芝浦1-2-1　シーバンスN館

TEL　03-5730-0744



shaping tomorrow with you