

FENCEご紹介資料

2006年12月
富士通株式会社

FENCEとは？



お客様ニーズに合わせた段階的なアドオン*導入が可能！

暗号(FENCE-Pro)

業務上の重要データを暗号化し、セキュリティを確保します。

- 様々な暗号化方式の採用
(**ドライブ暗号**、フォルダ・メディア暗号、ファイル暗号、メール暗号)
- 暗号鍵の管理機能
- **Active Directory 連携機能**
- トレース機能

認証(FENCE-AP)

USBキーを用いた本人識別で、権限に応じたアクセス管理統制を実現します。

- PCロック機能
- 利用者限定/グループ限定機能
- Windows ログオン連携機能
- トレース機能
- FENCE-Pro/FENCE-G連携機能

情報セキュリティ対策！
内部統制強化！

漏洩抑止(FENCE-G)

職務に応じたアクセスコントロールで、企業内部からの情報漏洩を防止します。

- 外部デバイス抑止機能
- ネットワーク共有抑止機能
- 印刷抑止機能
- 通信ポート抑止機能
- **Active Directory 連携機能**
- トレース機能

証跡(FENCE-Tracer)

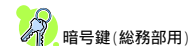
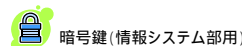
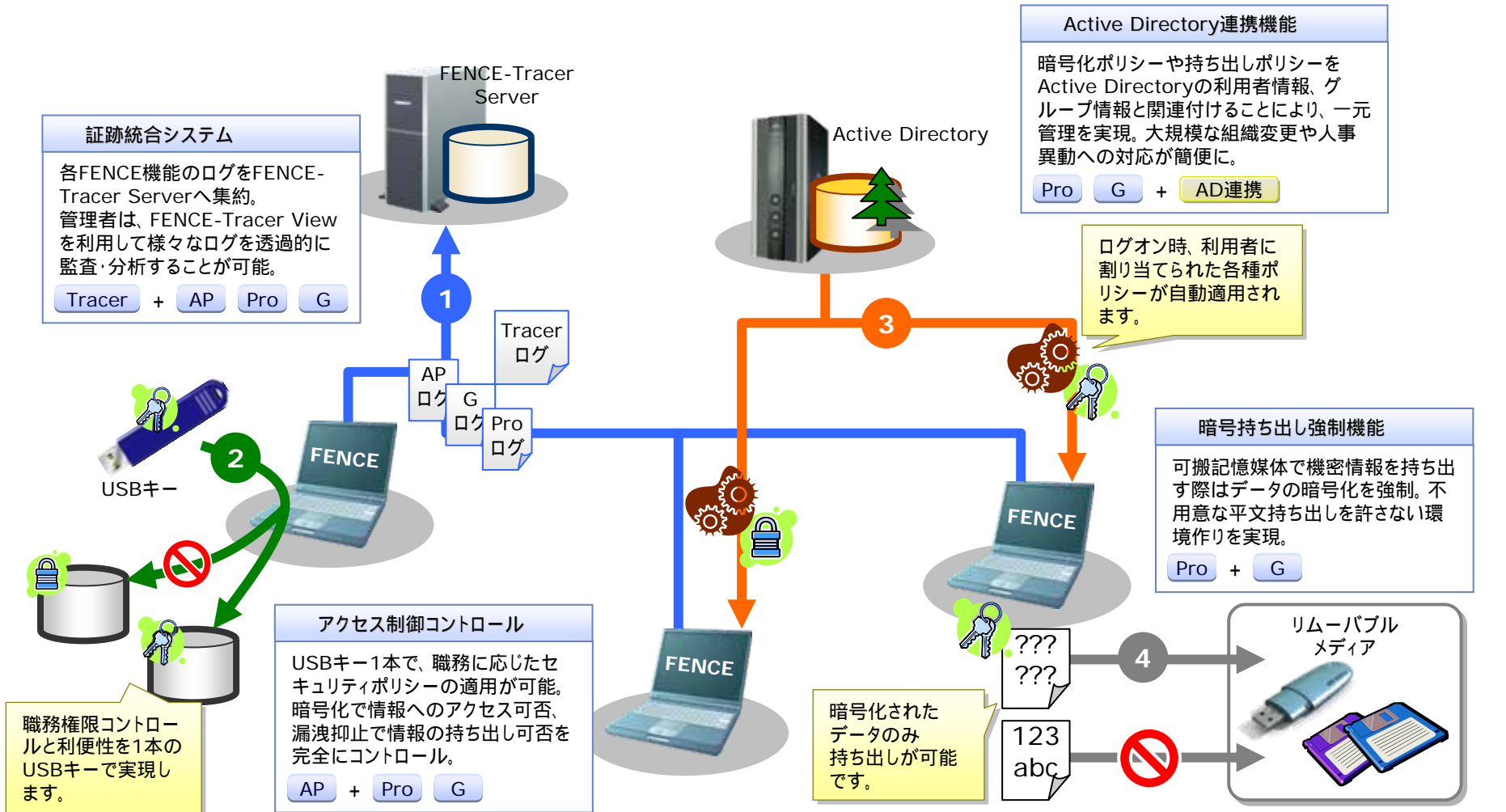
業務プロセスを可視化する、操作監視・メール監査を支援します。

- PC操作記録機能
(ログオン、ファイル操作、インターネット関連、画面キャプチャ、メールイメージなど)
- **インベントリ情報取得機能**
- アプリケーション使用制限機能
- 管理者支援機能
(**トレース**、**アラート**、レポート、バックアップなど)

* アドオンとは、既存のシステムに変更を加えることなく、システムを簡単に拡張することができる製品特性を指します。

FENCEによるトータルセキュリティソリューション

機能連携のシナジー効果によって、より強力なセキュリティ対策を実現！



お客様の課題を解決





利用者が、作成した機密データをデスクトップやマイドキュメントなどの暗号化されていないフォルダに保存してしまうんだよ。
これでは暗号化機能を導入した意味がないんだけどなぁ・・・

お客様の課題

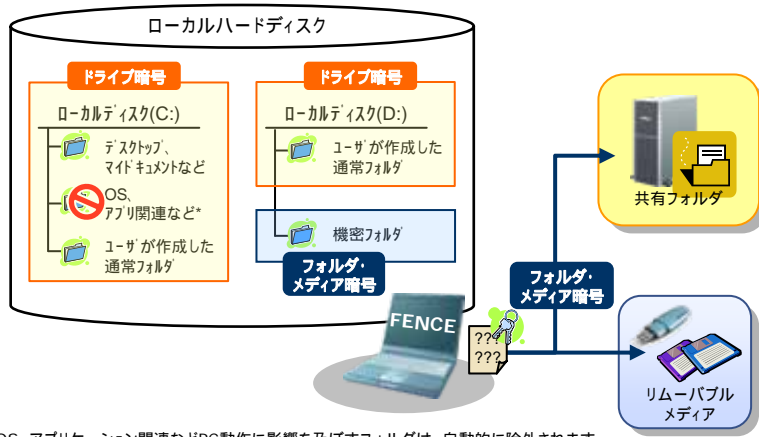
フォルダ暗号形式の場合、利用者が意図的に暗号化フォルダに保存しないかぎり暗号化されない

フォルダ暗号形式の場合、OS関連の特殊フォルダが暗号化できないなどの制約が多い

ローカルドライブに限らず、リムーバブルメディアやファイルサーバ上の共有フォルダなども暗号化したい



解決策



*OS、アプリケーション関連などPC動作に影響を及ぼすフォルダは、自動的に除外されます。

FENCE-Proのドライブ暗号、フォルダ・メディア暗号の共存運用で解決！

- ドライブ暗号は、“デスクトップ”や“マイドキュメント”の暗号化が可能、暗号化フォルダへデータを移動するなどの煩わしい操作は必要なし
- ドライブ暗号機能とフォルダ・メディア暗号機能は共存運用が可能
- ドライブ全体をドライブ暗号で保護しながら、特に重要なデータを保存しているローカルフォルダや共有フォルダをドライブ暗号とは別の暗号鍵を使用しセキュリティを高めることが可能

業務によってはセキュリティポリシーを頻繁に変更する必要があるんだ。
特に一時的にデータを持ち出さないといけないような業務の現場では、スムーズに権限変更が行えることが重要だよ。



お客様の課題

基本はセキュリティポリシーの一元管理。運用の簡便さが重要

必要に応じてセキュリティポリシーの一時変更を可能に



解決策

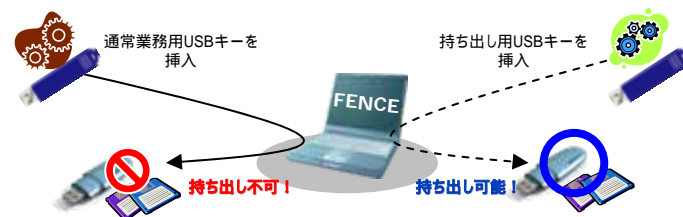
**Active Directoryでの一元管理で
大規模な組織変更・人事異動にも対応可能！**

- ADのグループやユーザにポリシーを関連付け
- ユーザのログイン時、関連付けられたポリシーを自動的に適用可能
- ポリシーの変更は、ADのグループメンバーを制御するのみ



**USBキーのアクセス制御で
臨機応変な権限変更を実現！**

- USBキーにポリシーを格納し、アクセス制御を実現
- 業務時に使用するUSBキーには、持ち出し不可ポリシーを適用
- 一時的に持ち出しが必要になった場合に、持ち出し許可ポリシーが適用されたUSBキーを貸し出し





アルバイト専用PCや特殊業務PCなど、数人のユーザしか使用できないようなアクセス制御を実現したい。ただし、Windowsアカウントやパスワードを共有するようなセキュリティを低下させる運用は避けたいんだけど…

お客様の課題

アクセス権限者以外は利用できないようなPCのグループ専用化

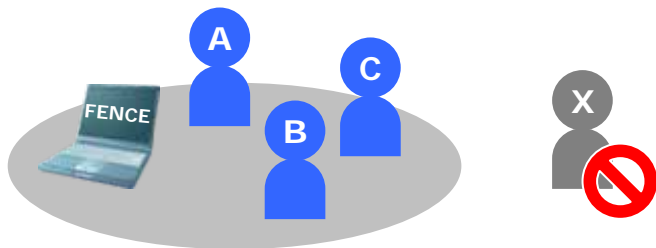
Windowsログイン方式以上の認証基盤と利便性が重要



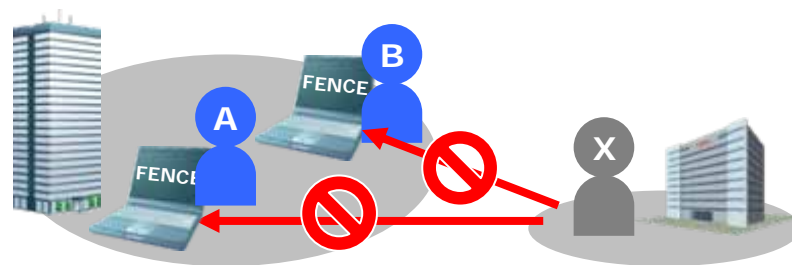
解決策

FENCE-APの**利用者・グループ限定機能**でPC利用者の**特定**が可能！

- PCの利用者を所有者のみに限定したり、数人のグループに特定することが可能
- アクセス権限を持たない利用者は一切PC操作が不可能



- PC利用者をサイト単位のグループ化が可能
- 組織や会社の違う利用者がUSBキーを持ち込んでも、PCに一切アクセス不可能



セキュリティ製品を導入すると各製品の操作ログが氾濫しちゃうよね。
ログの一元管理や有効活用を支援するような機能が組み込まれていることが
セキュリティ製品を選定するポイントになるんだけどなあ。



お客様の課題

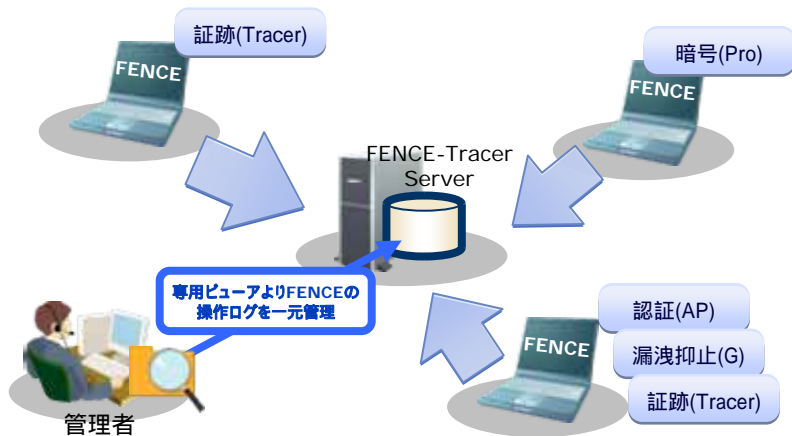
様々なセキュリティ対策に応じた製品・機能の充実性

各セキュリティ製品・機能の操作ログを一元管理する仕組み

運用管理者が操作ログを有効活用できるための支援機能



解決策



FENCEはクライアントのセキュリティ対策を
トータルに支援する機能が充実！

FENCEの操作ログはFENCE-Tracerが集約！
専用ビューアで操作ログを透過的に監視可能！

大量の操作ログを簡単に監視、分析するための
アラームやトレース、レポート機能が充実！



内部統制強化として業務プロセスの見直しは行っているがIT統制も並行して準備を進めたい。まずは、以前から現場で問題視されている不適切なデータアクセス権限の付与を見直し、ID管理へと繋げていきたいんだけど・・・

お客様の課題

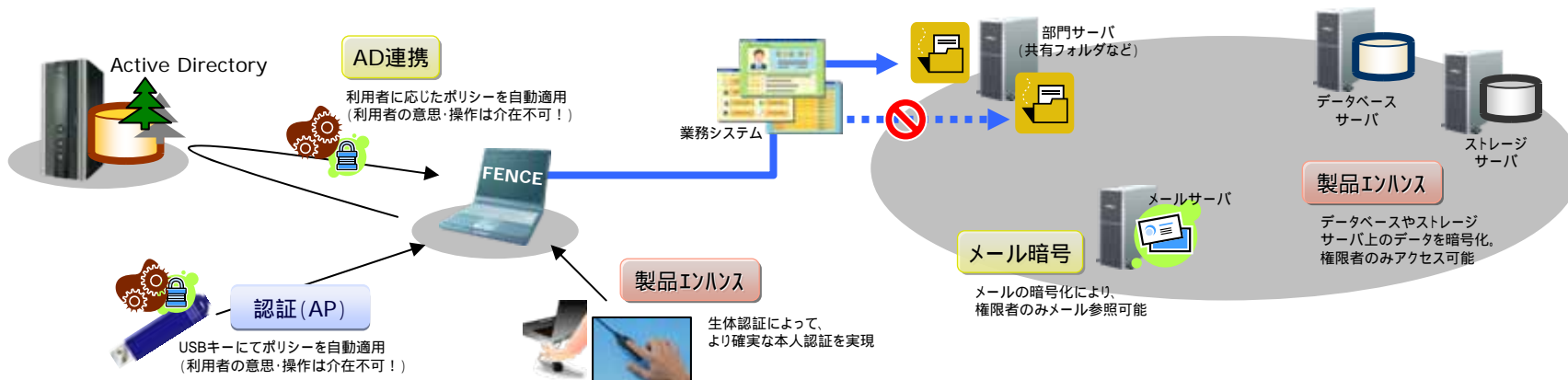
内部統制の視点におけるIT統制の推進が企業命題

職務上の権限に相応しくない過剰な権限付与の見直し



解決策

確実な本人識別と暗号化ソリューションで職務に応じたアクセスコントロールを実現





情報漏洩対策と共に内部統制強化が重要課題。
情報システムの運用状況を可視化し、透明性の高い運用を実現する監視体制を構築したいんだけど…

お客様の課題

万が一情報漏洩が起こった際の証跡管理システムの構築

内部統制強化としてのシステム運用、業務プロセスの可視化、モニタリング

信頼性の高い証跡・証拠の管理体制

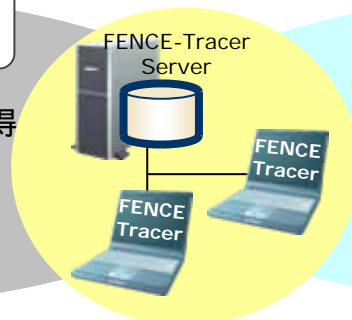


解決策

端末の操作記録により業務プロセスの可視化を実現するモニタリングプラットフォームの実現

内部統制強化

- 業務アプリ操作時の画面スナップショット取得
- 業務ワークフローの送受信メールをアーカイブ化



情報漏洩対策

- PC操作の記録
- インベントリ情報の記録
- アプリケーション使用制限
- 管理者支援機能の充実

様々な業種分野への導入実績

認証 + 暗号化のシームレス連携による利便性の向上！

PC起動フェーズ

- PC電源ON
- BIOS起動
- Windows OS起動

認証フェーズ

- USBキー挿入
(一次認証)
- PINコード入力
(二次認証)

運用フェーズ

- Windows自動ログオン
- 業務データ自動復号

要件

- 【業種】 金融(銀行・信金・保険証券・農水)
- 【運用シーン】 保険外行員のモバイルPC
- 【導入台数】 10,000台
- 【顧客要件】
 - モバイルPCの情報漏洩対策
 - 運用中のため短期間での導入が可能なこと
 - 複数の認証方式を組み合わせたセキュア化
 - 業務データの暗号化

FENCE採用ポイント

アドオン導入とインストーラーの自動化による
導入の期間短縮と簡便化を実現！

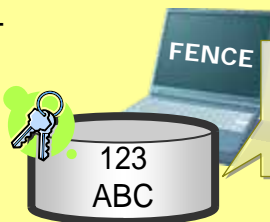
USBトークンとPINコードを利用した
2要素認証による認証基盤の強化！

認証・暗号機能の連携により
利用者は従来どおりの運用を維持！

PCロック状態
(業務データ参照不可)



PCロック解除
(業務データ参照可)



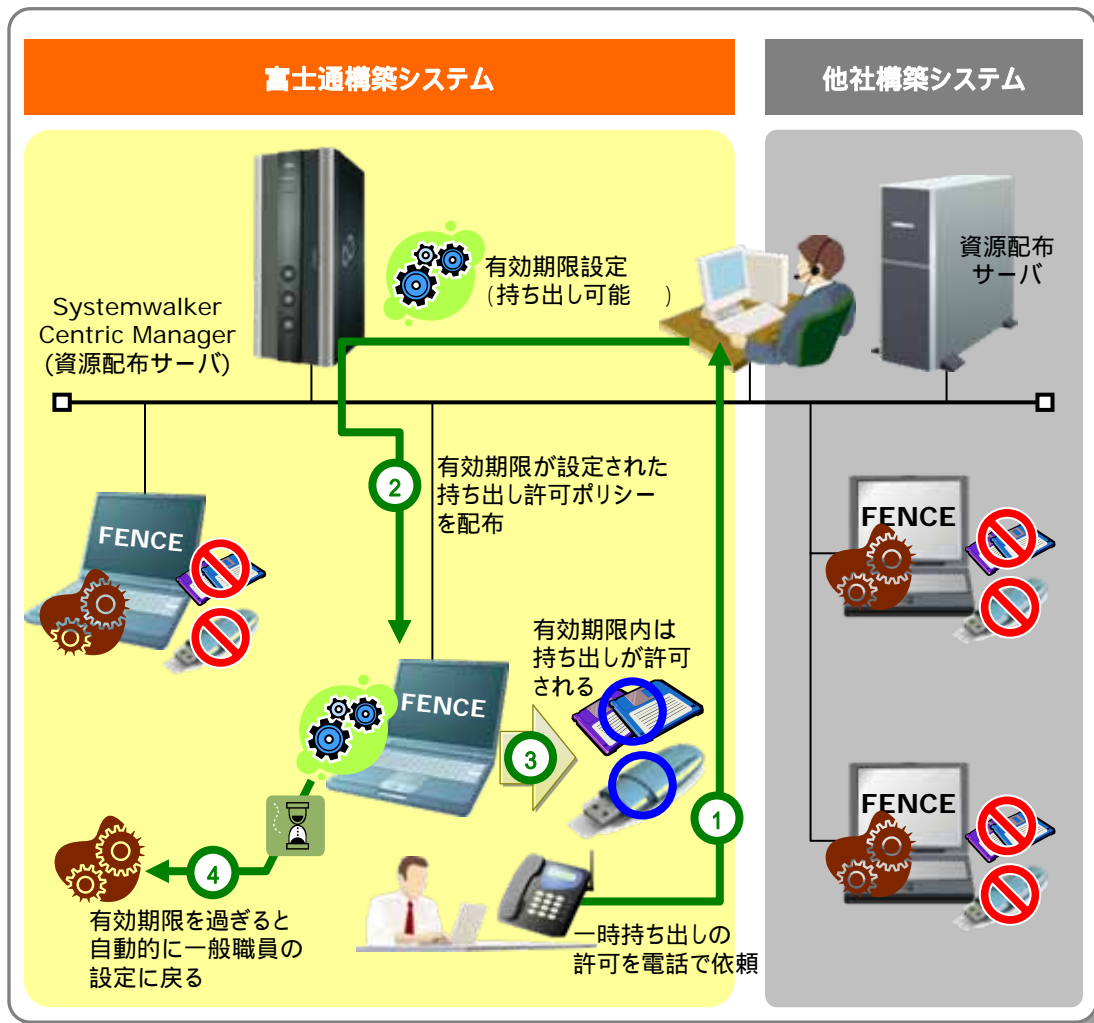
ログインユーザーに関連付いた暗号鍵で、
業務データが自動的に復号されます。

認証 (AP)

暗号 (Pro)

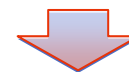
導入事例：一時的な持ち出し許可を即座に適用

持ち出し許可の有効期限を端末やユーザごとに設定可能！



要件

- 【業種】 公共(官公庁・自治体・病院・文教)
- 【運用シーン】 基幹システムに接続されたPC
- 【導入台数】 500台
- 【顧客要件】
 - 基幹システム専用PCの持ち出し制限
 - マルチベンダー環境への対応が可能なこと
 - 基本は集中管理、ただし端末単位でもポリシー変更が可能なこと
 - 導入が容易なこと



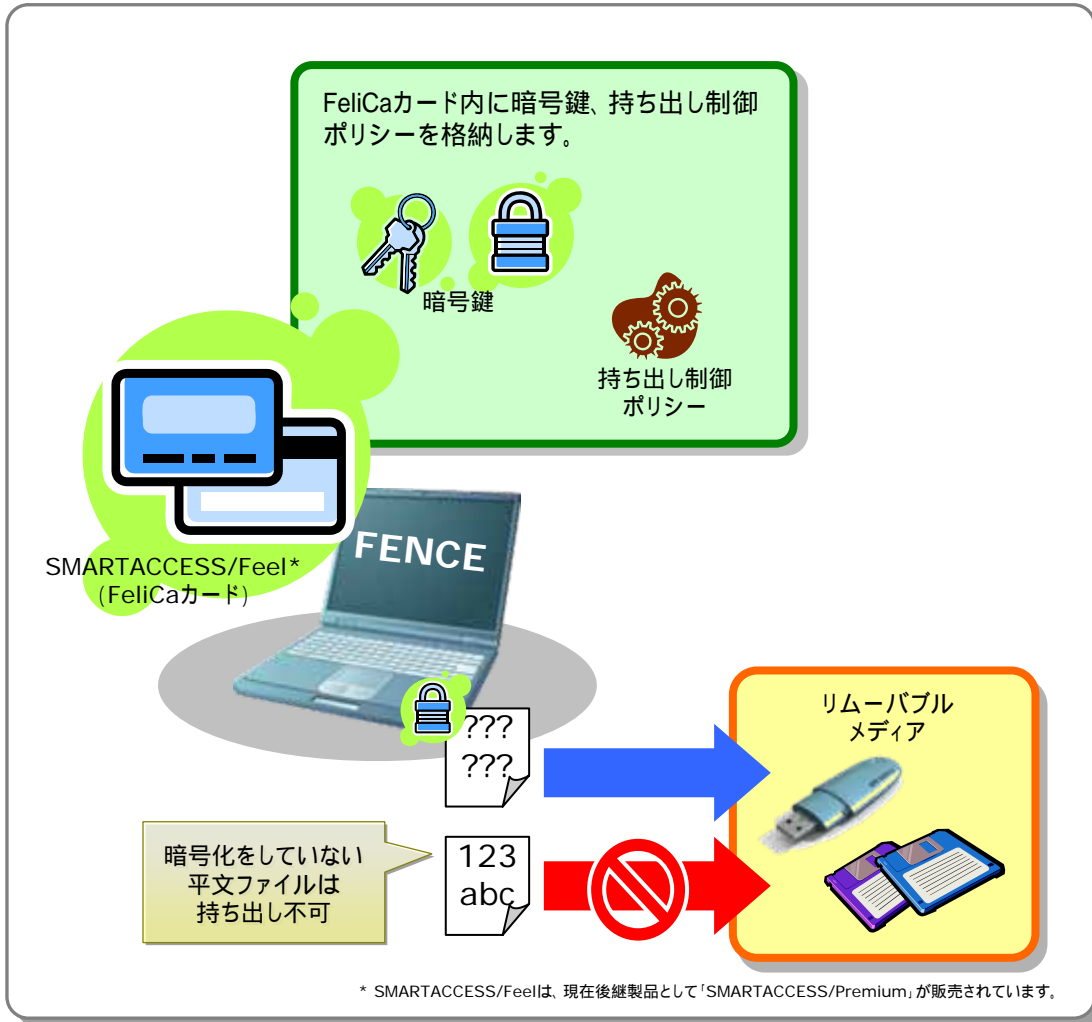
FENCE採用ポイント

漏洩抑止(G)

- マルチベンダ環境に対応した豊富な導入実績！
- 集中管理、端末やユーザ単位の管理など運用管理スタイルが選択可能！
- 期限設定、ログ取得・暗号化必須など様々な持ち出し許可方式が可能！

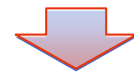
導入事例：暗号化による安全な持ち出し運用

利用者の使い勝手を維持したまま、安全なデータ持ち出し運用を実現！



要件

- 【業種】 公共(官公庁・自治体・病院・文教)
- 【運用シーン】 事務系ネットワークを利用する教職員向けPC
- 【導入台数】 1,000台
- 【顧客要件】
 - 事務系ネットワークPCの持ち出し制限、機密データの暗号化
 - FeliCaカード認証を実現するSMARTACCESS/Feelとの連携が可能なこと
 - 利用者の使い勝手を重要視



暗号(Pro)

漏洩抑止(G)

FENCE採用ポイント

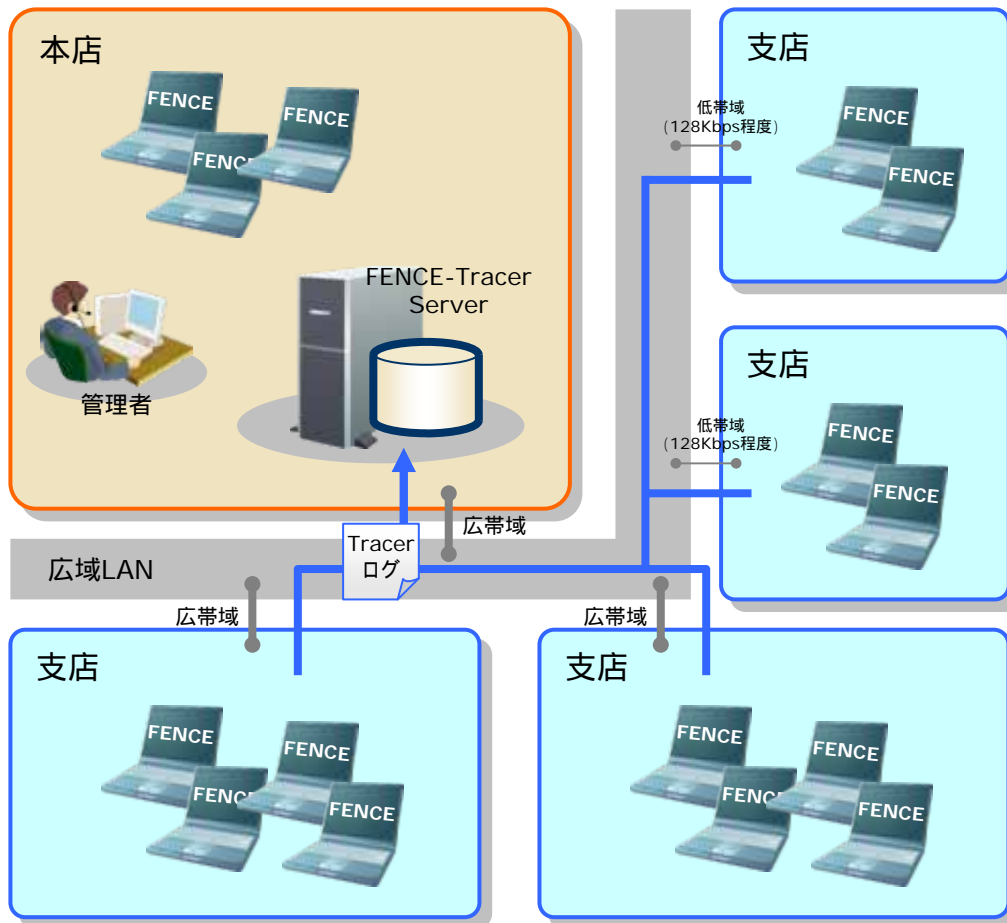
SMARTACCESS/Feelの標準プラグインによるシームレスな連携が可能！

利用者の使い勝手を損なうことなく安全なデータ持ち出し運用を実現！

持ち出し時の暗号化を強制することにより暗号し忘れなどのリスクを完全排除！

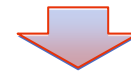
導入事例： 複数拠点のPC操作履歴を一元管理

PC操作履歴の収集、ポリシー管理を1台の専用サーバに集約！



要件

- 【業種】 製造・流通
- 【運用シーン】 業務PC
- 【導入台数】 300台
- 【顧客要件】
 - 業務PCの操作履歴を記録
(ファイル操作と持ち出し操作の追跡が目的)
 - 拠点は数箇所に分散、但し証跡管理は集中管理できること
 - 資産管理情報と連携可能なこと



FENCE採用ポイント

証跡(Tracer)

多彩なPC操作種別を漏らさず記録！

収集されるログ情報は最適化されており
大規模なネットワーク帯域を必要としない！

ポリシー配布や収集されたログの分析など
管理者ビューワからの一元管理が可能！

暗号(FENCE-Pro)

■ 金融(銀行・信金・保険証券・農水)

- ・ A銀行: 2,400L
- ・ B銀行: 2,100L
- ・ C信金: 300L
- ・ D労金: 1,300L
- ・ E生保: 65,000L
- ・ F生保: 10,000L
- ・ G損保: 24,000L
- ・ Hクレジット関連: 2,000L
- ・ I農協関連: 50,000L

■ 公共(官公庁・自治体・病院・文教)

- ・ A市: 5,100L
- ・ B医療関連: 460L
- ・ C大学: 1,000L

■ 社会基盤(電力・通信)

- ・ A通信関連: 30,000L

■ 製造・流通

- ・ A社: 550L など

総出荷ライセンス数
約645,000L
(約250社)

漏洩抑止(FENCE-G)

■ 金融(銀行・信金・保険証券・農水)

- ・ A銀行: 900L
- ・ B銀行: 1,000L
- ・ C信金: 700L
- ・ D信組: 200L
- ・ E労金: 1,700L
- ・ F生保: 70,000L
- ・ G損保: 32,000L
- ・ H農協関連: 50,000L

■ 公共(官公庁・自治体・病院・文教)

- ・ A市: 600L
- ・ B社: 1,000L
- ・ C社: 220L
- ・ D大学: 1,000L
- ・ E教育委員会: 1,000L

■ 社会基盤(電力・通信)

- ・ A社: 100L

総出荷ライセンス数
約410,000L
(約180社)

証跡(FENCE-Tracer)

■ 金融(銀行・信金・保険証券・農水)

- ・ A損保: 34,000L

■ 公共(官公庁・自治体・病院・文教)

- ・ A町: 200L
- ・ B教育関連: 400L

■ 製造・流通

- ・ A社: 600L など

総出荷ライセンス数
約40,000L
(約90社)

認証(FENCE-AP)

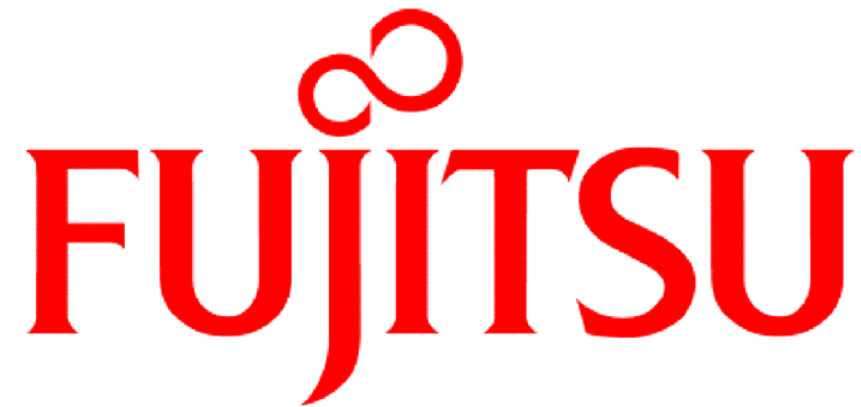
■ 金融(銀行・信金・保険証券・農水)

- ・ A生保: 70,000L
- ・ B生保: 60,000L
- ・ C農協関連: 50,000L

■ 社会基盤(電力・通信)

- ・ A電力: 250L など

総出荷ライセンス数
約396,000L
(約70社)



FUJITSU

THE POSSIBILITIES ARE INFINITE