FUJITSU

標的型サイバー攻撃への内部対策

アイネットセック　イントラ　ウォール
iNetSec Intra Wall

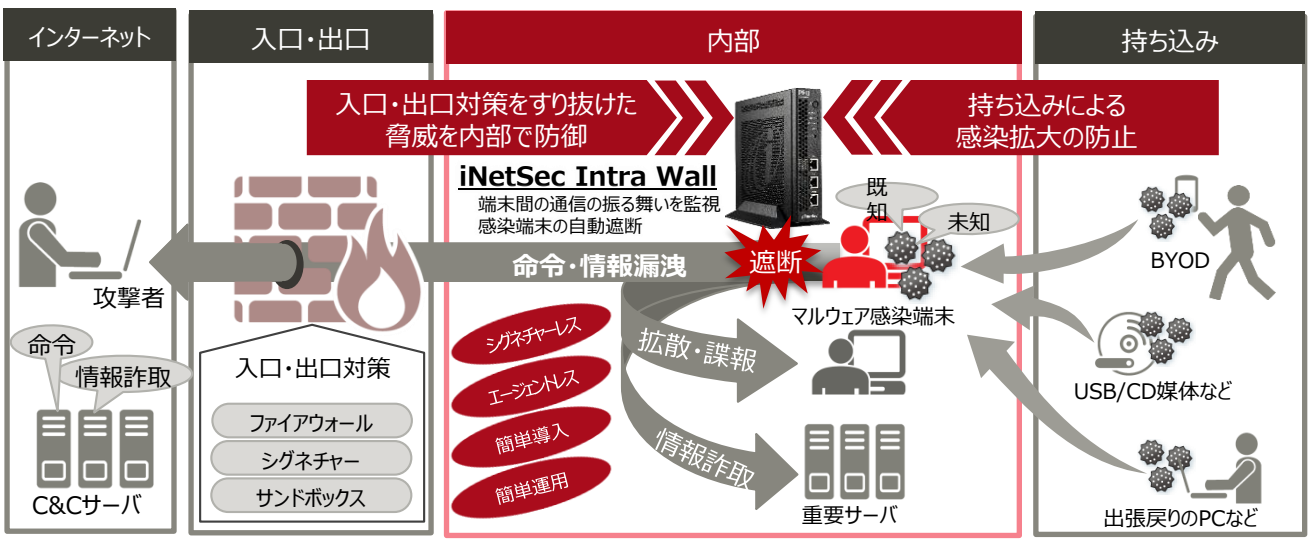
新製品　先進技術

お客様のメリット

- イントラネットに接続するだけで、既知・未知問わずマルウェア活動をリアルタイムに検知・遮断　特許出願済
- SNSやファイル共有など情報漏えいの原因となりうる禁止アプリケーションの通信検知・遮断
- 端末へのソフトウェアのインストールも不要で簡単に導入が可能

近年のサイバー攻撃では、未知のマルウェアを使用した標的型攻撃が増加しており、持ち込んだPCなどから、既存のセキュリティ対策をすり抜け、イントラネットにマルウェアが侵入するケースが増えています。
そこで、侵入を前提としたイントラネットでの未知のマルウェア対策が重要になっています。

本製品は、標的型サイバー攻撃の過程でネットワークに侵入したマルウェアの通信の振る舞いから、感染した端末を検知し、ネットワークから自動的に遮断することで被害を防止する内部対策アプライアンス製品です。振る舞い（種別、方向、順序など）からマルウェアの検知をおこなうため、亜種のマルウェアや未知のマルウェアにも効果を発揮します。また、ネットワーク内の通信を監視し、ファイル共有ソフトウェアなど業務で利用を禁止しているアプリケーションの検知・遮断によってお客様のセキュリティポリシーの統制や情報漏えい対策の強化も実現します。



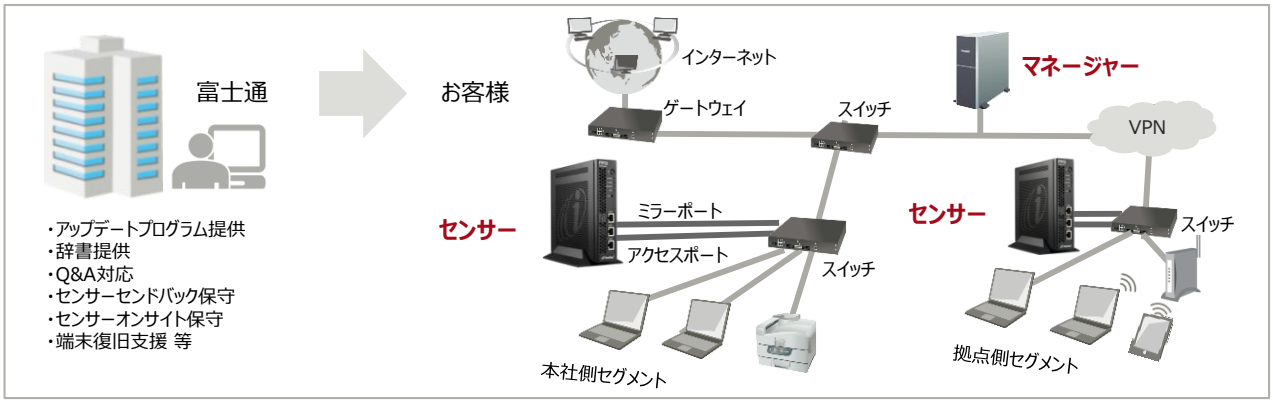
shaping tomorrow with you

構成

■ iNetSec Intra Wall は マネージャー と センサー から構成されます。

マネージャー　：センサーを統合管理するソフトウェアです。システムに1つ必要です。

センサー　：マルウェアの検知や感染端末の遮断を行うためのアプライアンスです。
タグVLAN構成の場合、16VLAN　まで管理できます。監視するスイッチのアクセスポート(またはトランクポート)とミラーポートに接続します。



価格

種別	商品	標準価格	単位	備考
製品	iNetSec Intra Wall マネージャーメディアパック	¥10,000	枚	管理用ソフトウェアのDVD媒体。
	iNetSec Intra Wall センサー	¥320,000	台	アプライアンス製品。監視するセグメントに必要。最大16タグVLANまで対応。
ライセンス	iNetSec Intra Wall セグメントライセンス1 iNetSec Intra Wall セグメントライセンス10 iNetSec Intra Wall セグメントライセンス50 iNetSec Intra Wall セグメントライセンス100	¥65,000 ¥520,000 ¥2,340,000 ¥4,160,000	年額	iNetSec Intra Wall の年間利用ライセンス。 マネージャーが管理するセグメント数分のライセンスが必要。

諸元	項目	数値
マネージャー	機器数 (MACアドレス数)	10,000 台
	センサー数	100 台
	セグメント数	250 個
	セグメントグループ数	75 個
	管理ユーザー数	800 人
センサー	機器数 (MACアドレス数)	3,000 台

マネージャー動作環境	
CPU	2GHz以上 （4コア以上を推奨）
メモリ	1GB以上 (システムで4GB以上推奨)
HDD	4GB以上の空きディスク
OS	Windows Server 2008 R2 Service Pack 1 Windows Server 2012 Service Pack なし Windows Server 2012 R2 Service Pack なし

※センサーは440Mbpsまで検知・遮断可能
(マルウェア検知のみ、アプリケーション検知は未設定の場合)

※本製品は、総務省委託研究「サイバー攻撃・検知に関する研究開発」の成果を使用しています。

※本資料中、 特許出願済 表示箇所については特許出願済の技術を含みます。

商品・サービスについてのお問い合わせは
富士通コンタクトライン（総合窓口）　0120-933-200　受付時間 9:00～17:30（土・日・祝日・当社指定の休業日を除く）
富士通公開サイト　http://jp.fujitsu.com/　詳細はこちら http://fenics.fujitsu.com/products/inetsec/

iNetSec Intra Wall
FireEye連携による標的型サイバー攻撃対策

iNetSec Intra Wall
FireEye NXシリーズ

お客様のメリット

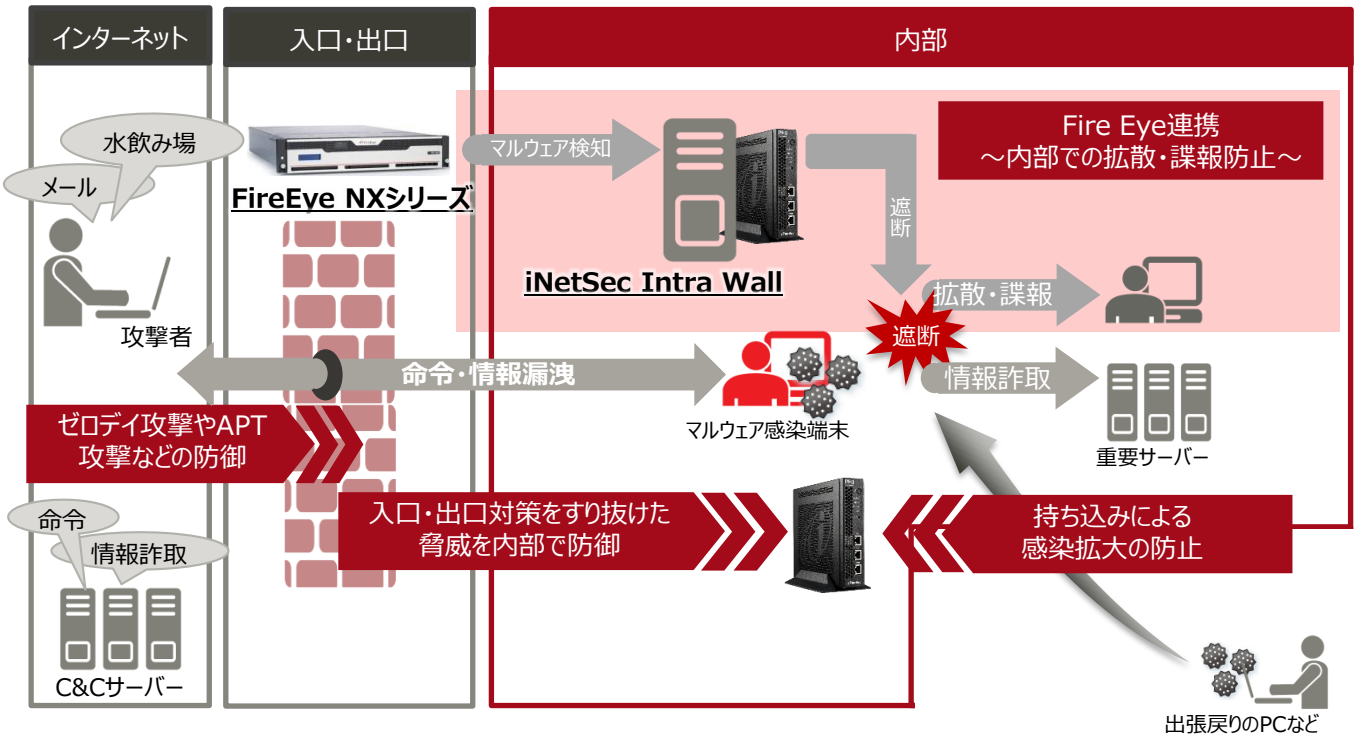
- 多層防御による標的型サイバー攻撃対策の強化
- マルウェア拡散・情報詐取の被害防止

FireEye + iNetSec 併設
FireEye + iNetSec 連携

FireEye によるゼロデイ攻撃やAPT攻撃など次世代型の脅威から情報漏えいの入口・出口対策に加え、iNetSec Intra Wall での振る舞い検知・遮断技術によりモバイルワークなどに起因するマルウェア対策を行うことにより、標的型サイバー攻撃に対して全方位的なマルウェア対策を実現することができます。

また、FireEye および iNetSec Intra Wall の異なるマルウェア検知技術を併設することにより、より未知・既知問わずマルウェアの検知率を向上させる多層防御を実現します。

さらに、FireEye と iNetSec Intra Wall を連携させることにより、FireEye のサンドボックス技術などで検知したマルウェア感染端末を iNetSec Intra Wall が自動遮断することにより、内部に侵入したマルウェアの拡散・諜報活動を最小限に封じ込めることが可能になります。



商品・サービスについてのお問い合わせは
富士通コンタクトライン（総合窓口）　0120-933-200　受付時間 9:00～17:30（土・日・祝日・当社指定の休業日を除く）
富士通公開サイト　http://jp.fujitsu.com/

shaping tomorrow with you

標的型サイバー攻撃対策
内部対策と出入口対策製品連携

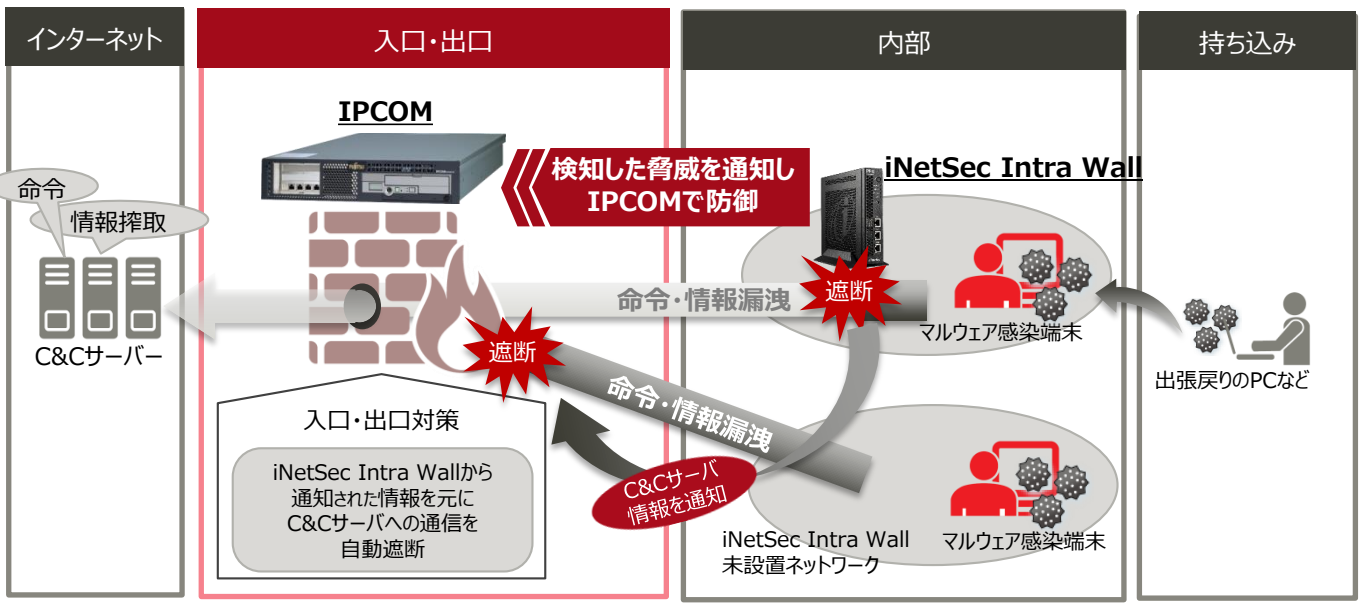
FUJITSU Network IPCOM EXシリーズ
セキュリティアプライアンス製品 iNetSec Intra Wall

お客様のメリット

- 標的型サイバー攻撃の内部対策で検知したC&Cサーバの通信を出入口対策製品で自動遮断
- 内部対策製品を導入していないネットワークからのC&Cサーバへの通信も出入口対策製品で遮断が可能
- 連携機能があることで、少ない内部対策製品の導入でも、標的型サイバー攻撃対策に対して、高い効果

近年のサイバー攻撃では、未知のマルウェアを使用した標的型サイバー攻撃が増加しており、対策が重要になっています。マルウェアの侵入対策で入口対策や、持ち込み・すり抜けを前提にマルウェアの内部対策や、情報漏えい対策で出口対策が重要になっています。

内部対策製品と出入口対策製品が連携し、内部対策製品が検知したマルウェアのC&Cサーバとの通信を出入口対策製品で遮断することで、マルウェアによる情報漏えいを防ぐことが可能になります。また、出入口対策製品のIPCOM EXシリーズはさまざまなセキュリティ機能を持っており、入口対策としても、アンチウイルス機能やシグネチャー型IPS機能などもありますので、高度なセキュリティ対策が可能になります。



※iNetSec Intra Wallは、総務省委託研究「サイバー攻撃・検知に関する研究開発」の成果を使用しています。
※IPCOM EXシリーズはIPCOM EX IN/SC/NWシリーズのE20L32以降でオプションが必要
※iNetSec Intra WallはIPCOM連携モジュール(無償)が必要

商品・サービスについてのお問い合わせは
富士通コンタクトライン（総合窓口）　0120-933-200　受付時間 9:00～17:30（土・日・祝日・当社指定の休業日を除く）
富士通公開サイト　http://jp.fujitsu.com/　詳細はこちら http://fenics.fujitsu.com/products/inetsec/

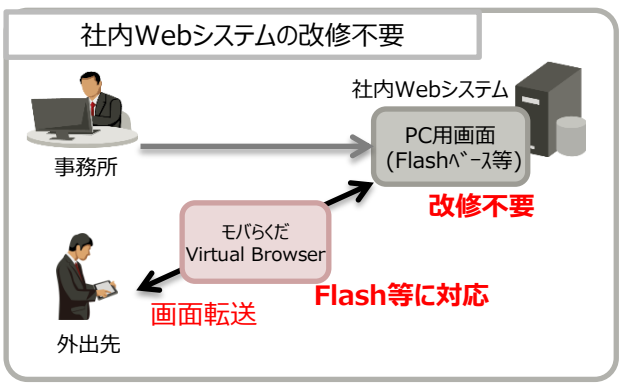
スマートデバイスの業務活用

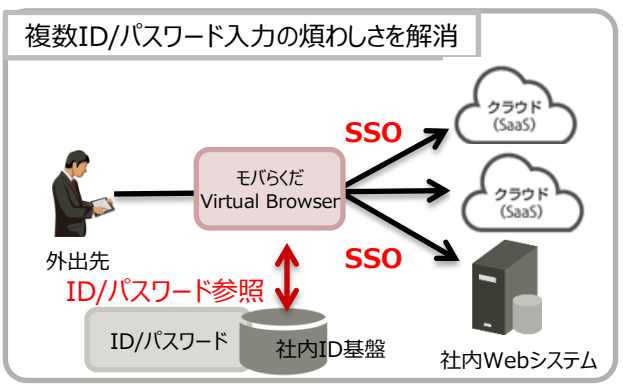
FUJITSU Thin Client Solution モバらくだ Virtual Browser

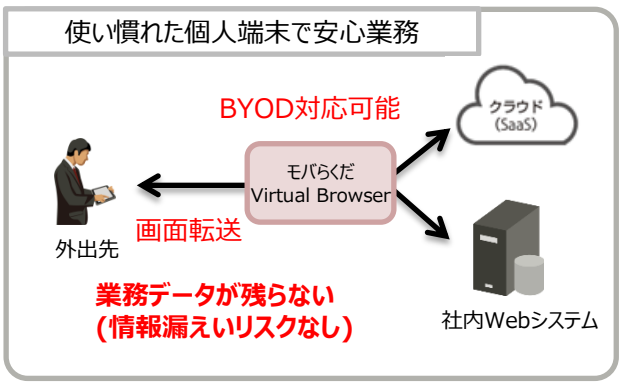
「モバらくだ Virtual Browser」は、社給端末/BYOD問わず簡単、セキュアーにスマートデバイスの業務活用を実現するソリューションです。

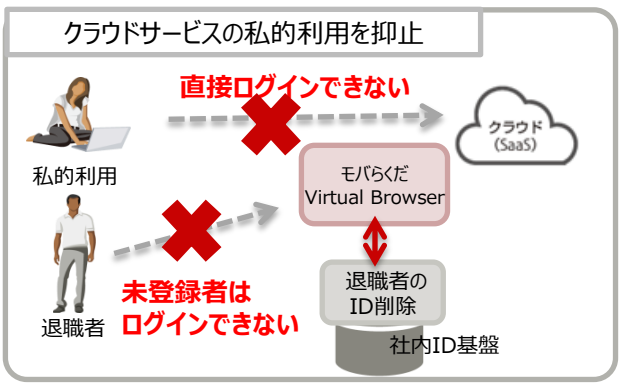
隙間時間を有効に活用でき、ビジネススピードの向上を実現します。

特長









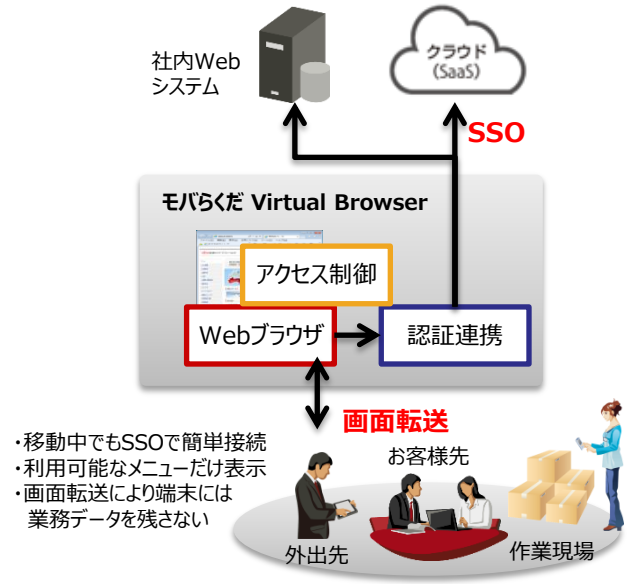
shaping tomorrow with you

社会とお客様の豊かな未来のために

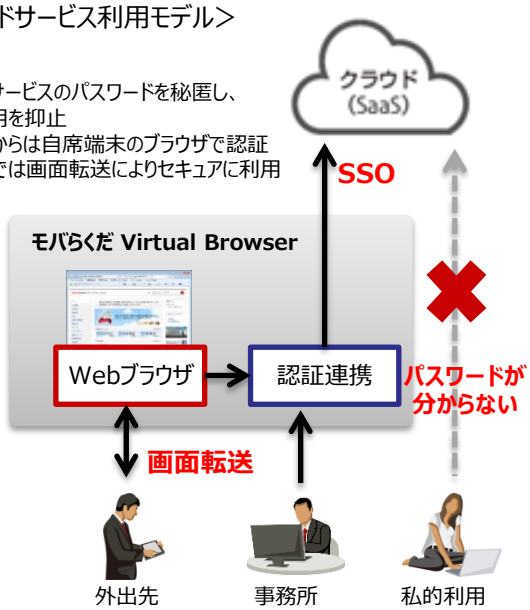
http://jp.fujitsu.com/fnets/services/solutions/thinclient.html

利用シーン

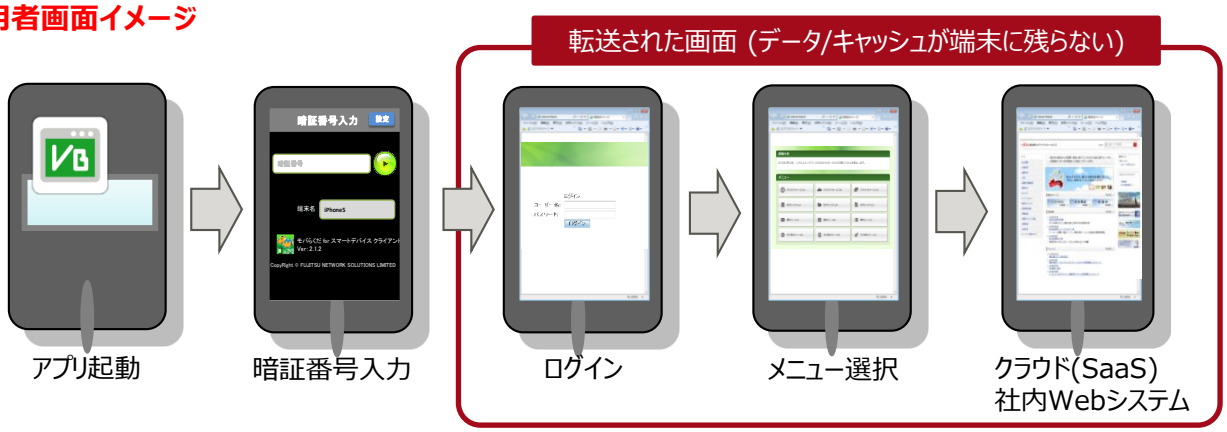
<社外ワークスタイル変革モデル>



<クラウドサービス利用モデル>



利用者画面イメージ



モデル価格（ソフトウェア、利用ライセンス、保守費用）

利用者数	初年度	次年度以降(年間)
50利用者 (同時10接続)	¥1,751,000～	¥551,000～
100利用者 (同時10接続)	¥2,016,000～	¥816,000～

※モデル価格には以下を含んでいません。
・お客様準備品(Windowsライセンス/CAL類)
・サーバ機器費、構築費用
・社内WebシステムへのSSO機能とその構築費

※モデル価格はシングル構成で試算しています。

※お客様環境(既存資産流用等)により、価格は変動します。

Green Policy Innovation

【環境配慮ソリューション】
導入により、お客様、またはグループ内の環境負荷低減に役立ちます。

お問い合わせ先
富士通コンタクトライン（総合窓口）TEL：**0120-933-200**
受付時間：9：00-17：30（土、日、祝日、当社指定の休業日を除く）
http://jp.fujitsu.com/telecom

富士通株式会社
〒105-7123 東京都港区東新橋1-5-2 汐留シティセンター

2015.9