FUJITSU

FUJITSU Security Solution
SHieldWARE

shaping tomorrow with you

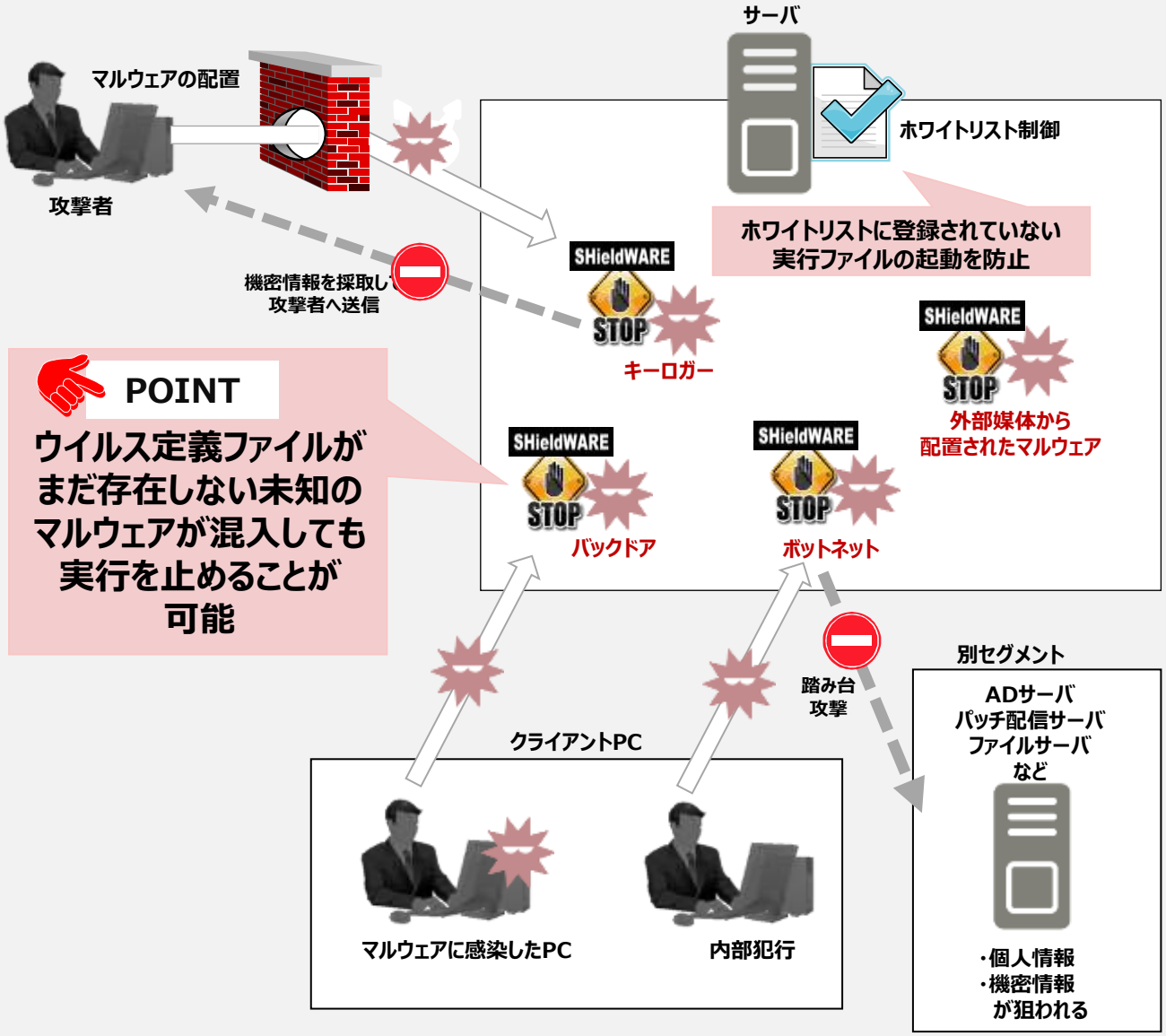
社会とお客様の豊かな未来のために

SHieldWAREは、サーバからの情報漏えいの防止や、サーバ操作のシステム監査に対応するセキュアOSソフトウェアです。

SHieldWAREの特長

実行ファイルのホワイトリスト化による未知のマルウェアの活動防止	セキュリティ強化
厳密なアクセス制御による外部アタック/内部不正操作からの防御	セキュリティ強化
不正操作によるファイルの改ざんを検知/防御	セキュリティ強化
OS操作ログの取得(監査証跡)とログ改ざん防止	内部統制の強化

ホワイトリストによる実行制御



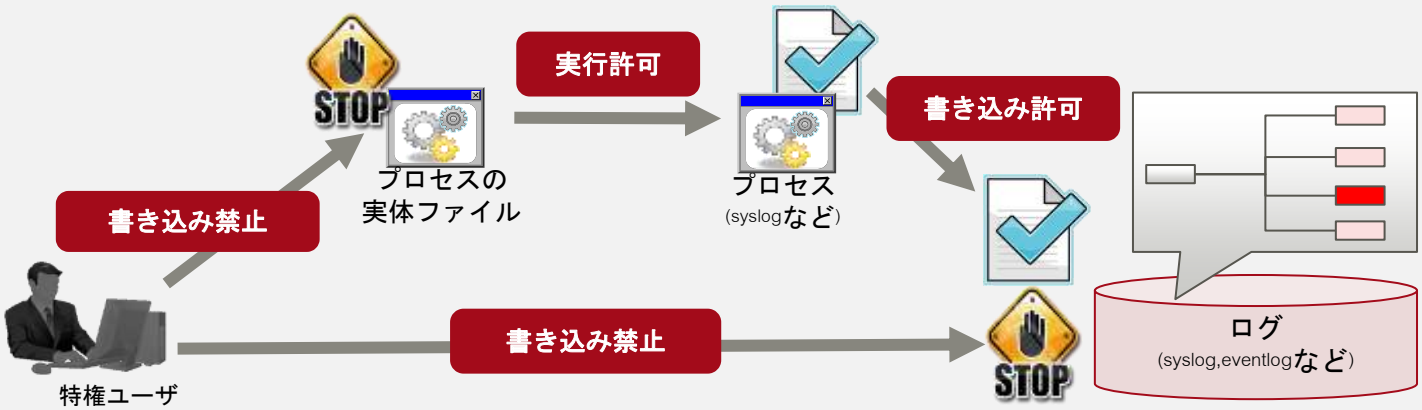
導入効果

- 未承認プログラム(マルウェア等)が配置されても、実行させないことが可能
- サーバからの重要情報の漏えいを防止することが可能
- 攻撃用の踏み台サーバとして利用されることを防止することが可能

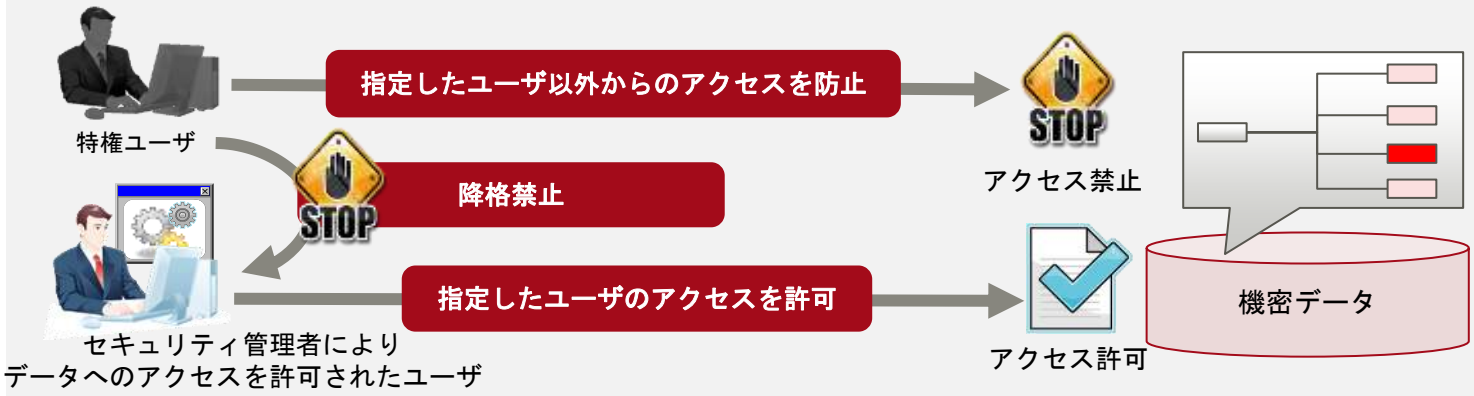
強制アクセス制御

root/Administrator/system権限などの特権IDを奪取されても、重要なファイルの改ざんや、
不正操作を防ぎ、重要なデータを守ることができます。

・ログの改ざんを防止



・過失/故意によるデータ盗難、紛失の抑制

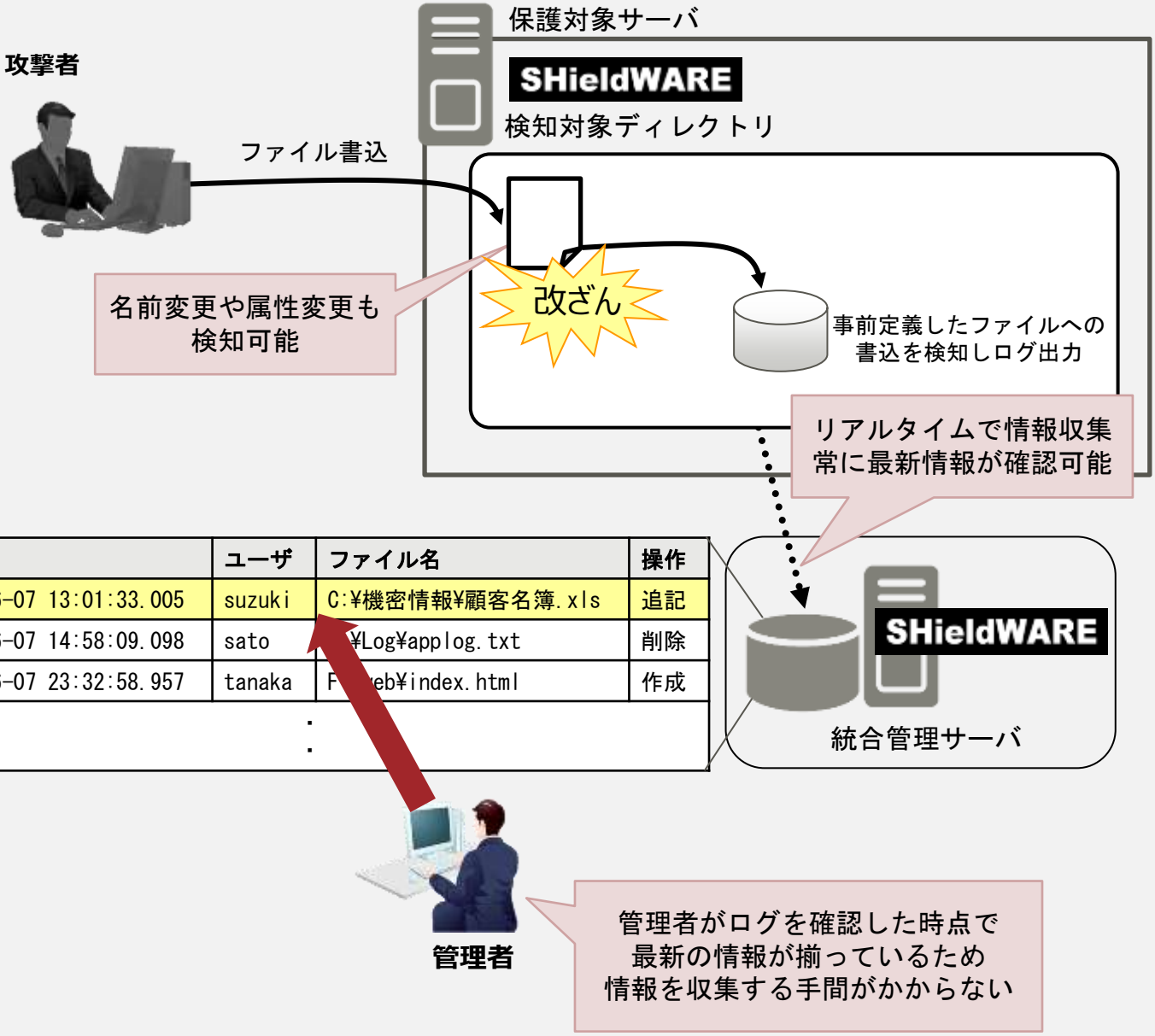


導入効果

- 特権IDを利用した不正操作の痕跡削除(ログの改ざんなど)を防止することが可能
- アプリケーションのコンフィグファイルやID情報などの改ざんを防止することが可能
- 特権IDを利用した不正なコマンド操作(ID情報奪取、ID情報改ざん)を防止することが可能

ファイル改ざん検知

OSのログでは取得できない詳細ログ（ファイル編集操作履歴など）をリアルタイムに取得できるため、
不正な操作によるファイル変更を早期に発見することができます。



日時	ユーザ	ファイル名	操作
2019-06-07 13:01:33.005	suzuki	C:¥機密情報¥顧客名簿.xls	追記
2019-06-07 14:58:09.098	sato	¥Log¥applog.txt	削除
2019-06-07 23:32:58.957	tanaka	F eb¥index.html	作成
		：	

導入効果

- リアルタイムで検知する仕組みのため、攻撃を早期発見することが可能
- 不正操作を行ったことに対する痕跡削除（ログの削除等）をリアルタイムで検知
- アクセス制御機能を利用することで「検知⇒防御」へと早期対策を行うことが可能

監査ログ

監査証跡を残すことは、コンプライアンス上不可欠な要件です。SHieldWAREはサーバ上での操作をOSのコマンドレベルで詳細に記録するため、不正侵入阻止の履歴からサーバアクセスログまで確実に採取できます。

・「いつ」「誰が」「どこから」「どのプロセス」で ファイル改ざんを行ったかを把握可能

例）ユーザ（suzuki）がサーバにログインし、あるファイルを作成して追記し削除を行い、ログアウトした場合

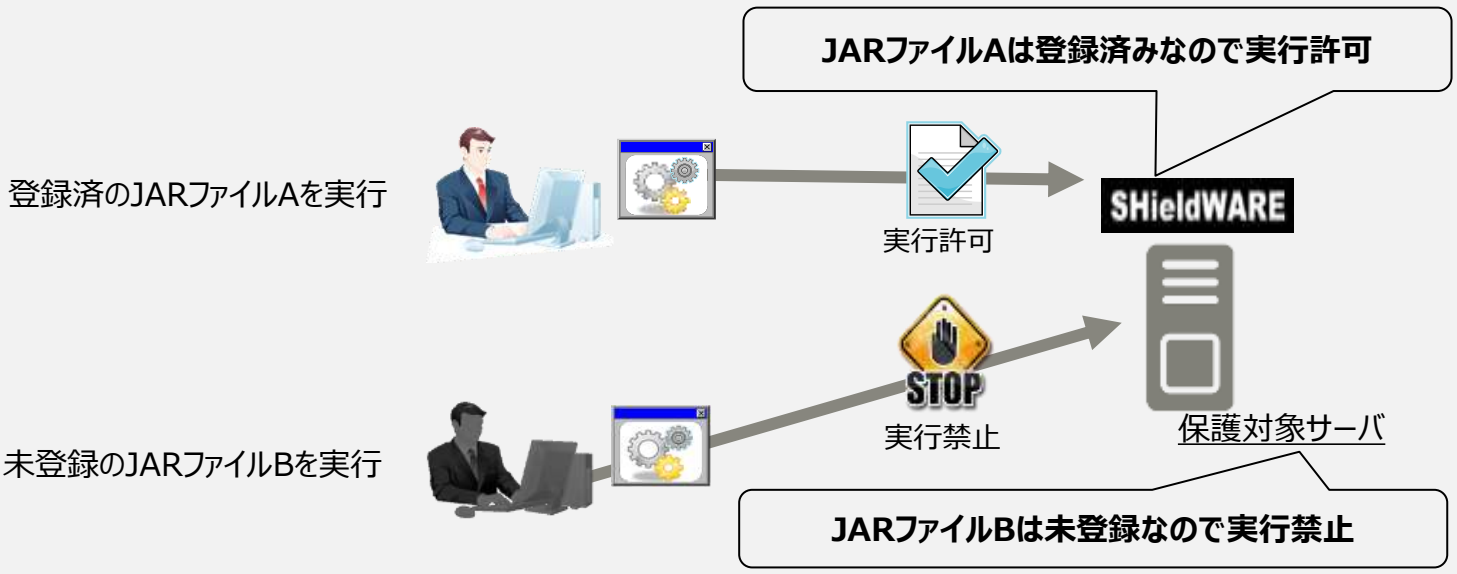
日付	IPアドレス	ソース IPアドレス	プロセス名	ログイン ユーザ名	実効 ユーザ名	メッセージタイプ	メッセージID	メッセージ
2019/7/25	192.168.1.169	192.168.1.223	sshd	suzuki	root	logout	PAM-50410	Logout
2019/7/25	192.168.1.169	192.168.1.223	usrproc	suzuki	root	fsm	LSM-11012	File deleted by UNLINK call : /data/test/testfile
2019/7/25	192.168.1.169	192.168.1.223	usrproc	suzuki	root	fsm	LSM-11012	File written by APPEND call : /data/test/testfile
2019/7/25	192.168.1.169	192.168.1.223	usrproc	suzuki	root	fsm	LSM-11012	File created by CREATE call : /data/test/testfile
2019/7/25	192.168.1.169	192.168.1.223	usrproc	suzuki	root	exec	LSM-10512	./usrproc
2019/7/25	192.168.1.169	192.168.1.223	sshd	suzuki	suzuki	login	PAM-50310	Login succeeded

導入効果

- 一般のUNIXシステムでは取得できない**「管理者権限昇格前のユーザ名」**や、Windowsシステムでは取得できない**「ログアウト」**のログなどを取得可能。
- 不正操作を時系列に沿って行動分析することが可能

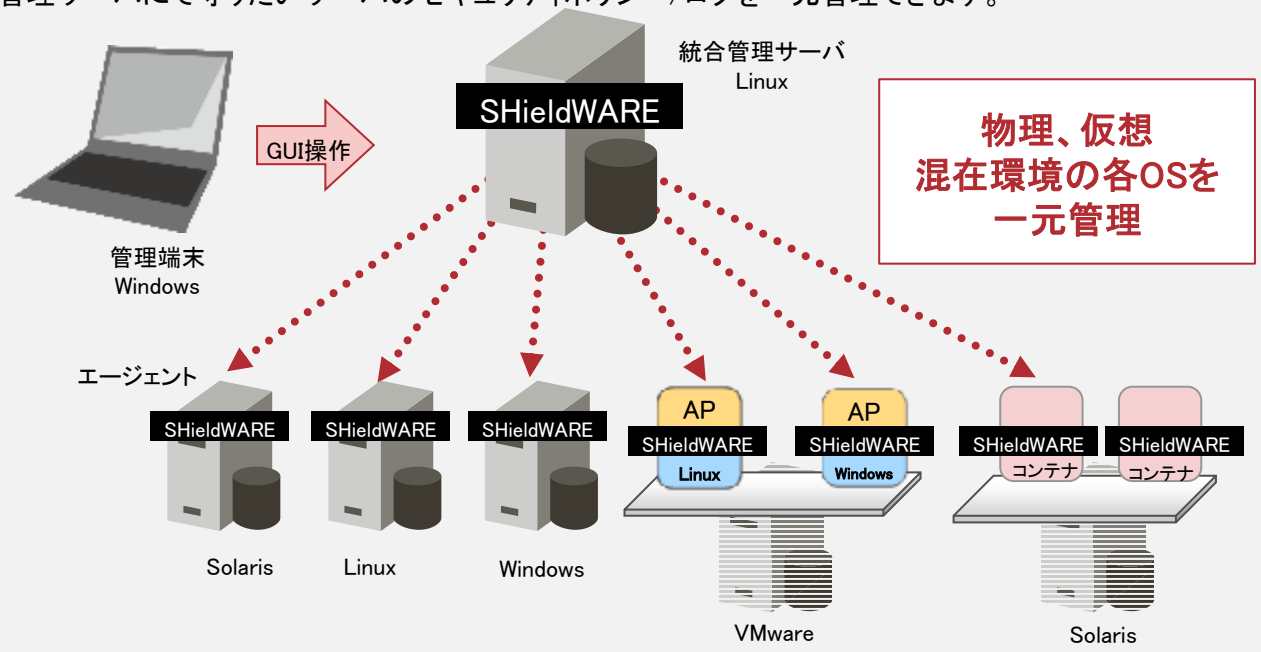
拡張子による実行制御（新機能）

既存のコマンド制御機能ではプロセス単位の制御を行うため、JVM（Java Virtual Machine）がJAR ファイルを読み込んで実行する場合に、JAR ファイル毎に実行の許可・禁止を設定することができません。
JAR ファイル毎の実行許可・禁止を設定したい場合は本機能を使用します。



システム構成

統合管理サーバにて守りたいサーバのセキュリティポリシー/ログを一元管理できます。



標準価格

■SHieldWARE メディアパック

商品名	標準価格
SHieldWARE メディアパック	10,000円
SHieldWARE 統合管理サーバ 暗号化DB Edition メディアパック	10,000円
SHieldWARE 統合管理サーバ 大規模DB Edition メディアパック	10,000円

■SHieldWARE 統合管理サーバ

商品名	標準価格
SHieldWARE 統合管理サーバ	480,000円
SHieldWARE 統合管理サーバ 暗号化DB Edition	1,500,000円
SHieldWARE 統合管理サーバ 大規模DB Edition	1,980,000円

■SHieldWARE エージェント(プラットフォーム共通)

商品名	標準価格
SHieldWARE エージェント(1-2CPUサーバ用)	380,000円
SHieldWARE エージェント(1-8CPUサーバ用)	640,000円
SHieldWARE エージェント(CPU数無制限)	980,000円

■SHieldWARE エージェント仮想環境用(プラットフォーム共通)

商品名	標準価格
SHieldWARE エージェント(仮想コンピュータ用)	280,000円

お問い合わせ先
株式会社富士通ソーシアルサイエンスラボラトリ(富士通SSL)

お問い合わせ総合窓口
〒211-0063 川崎市中原区小杉町1-403武蔵小杉タワープレイス
E-mail : ssl-info@cs.jp.fujitsu.com
当社ホームページ https://www.fujitsu.com/jp/group/ssl/