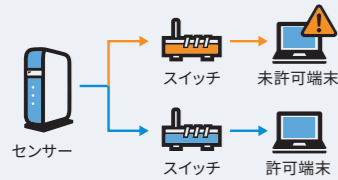


追加機能

お客様の運用管理コストを低減する多彩な機能を搭載

スイッチポート特定機能



どのスイッチのどのポートにIT機器が接続されているかを特定。効率的にIT機器の場所を把握できます。

レポート機能



IT機器種別ごとの台数、サポート切れOSの数、接続を拒否したIT機器の数等をレポート形式で確認できます。

ダッシュボード機能



ネットワーク接続機器、申請中のIT機器、長期間未接続のIT機器など、必要な情報をすぐに把握できます。

価格・機能

お客様のニーズに合わせて、オンプレミス版とクラウド版からお選びいただけます。

オンプレミス版価格

	商品名	価格	備考
製品	iNetSec SF V1.0 マネージャー	300,000円	ソフトウェアパッケージ製品、システムに1つ必須
	iNetSec SF 510センサー	225,000円	センサーにはセグメントライセンスが1つ付与されています
	iNetSec SF 510センサー ラックマウントキット	44,000円	「iNetSec SF 510センサー」をラック搭載するためのオプション製品
ライセンス	iNetSec SF 追加セグメントライセンス	44,000円～	1台のセンサーで複数のセグメントを管理する場合に必須
	iNetSec SF 標的型サイバー攻撃振る舞い検知セグメントライセンス	65,000円/年～	年間利用ライセンス 追加機能を利用するセグメント数分必要
機能追加 ライセンス	iNetSec SF 脆弱性検査セグメントライセンス	75,000円/年～	
	iNetSec SF アプリケーション監視セグメントライセンス	12,000円/年～	

クラウド版価格

商品名	価格	備考
iNetSec SF Cloud マネージャー 1年利用ライセンス	300,000円	<ul style="list-style-type: none"> クラウド版マネージャーの使用権として定額でのご利用となります。 システムに1つ必要です。 QA、機能アップデート、利用時初期セットアップ、機器辞書の更新が含まれます。
iNetSec SF Cloud 510 センサー 1年利用ライセンス	132,000円	<ul style="list-style-type: none"> お客様ネットワークに接続するセンサーです。 設置するセンサーはiNetSec SF Cloud マネージャーと接続して定額でご利用いただけます。利用時の初期設定、故障時センサー交換の費用が含まれます。タグVLANの場合、1台のセンサーで32VLANまでご利用いただけます。 センサー1台あたりの価格です。

オンプレミス版・クラウド版の機能一覧

		項目	オンプレミス版	クラウド版
諸元	管理機器数 (MACアドレス数)		300,000	10,000
	センサー数		1,000	500
	セグメントグループ数		1,000	500
	セグメント数		1,000	500
機能	基本機能	機器検知・識別	○	○
		不正接続防止	○	○
	新機能	スイッチポート特定機能	○	○
		レポート機能	○	○
		ダッシュボード機能	○	○
	他製品連携	資産管理ツール連携	○	-
		サイバー攻撃対策製品連携	○	
		ゲートウェイ製品連携	○	
	オプション機能	標的型サイバー攻撃振る舞い検知	○	
		アプリケーション監視	○	
脆弱性検査		○		

セキュリティ対策アプライアンス
iNetSec SF

“機器検知・不正接続防止”を手軽に導入できる **クラウド版**

“サイバー攻撃対策”まで行える **オンプレミス版**



ネットワークに接続するあらゆるIT機器を手軽に把握・管理！

安全に関するご注意

- ご使用の際は、取り扱い説明書をよくお読みのうえ、正しくお使いください。
 - 水、湿気、湯気、ほこり、油煙などの多い場所に設置しないでください。
- 火災、故障、感電などの原因となることがあります。表示された正しい電源、電圧および環境条件でお使いください。



環境に配慮した当社の製品に
表示する環境シンボルマークです

お問い合わせ先

株式会社PFU

<https://www.pfu.fujitsu.com/inetsec/>

- 横浜本社
〒220-8567 横浜市西区みなとみらい4-4-5 横浜アイマークプレイス
☎(045) 305-6000
- 北海道支店 ☎(011) 242-2212
- 東北支店 ☎(050) 3786-2204
- 北陸支店 ☎(050) 3819-9160
- 東海支店 ☎(052) 202-0871
- 関西支店 ☎(06) 6152-8153
- 九州支店 ☎(050) 3819-9180

こんなお客様にオススメ

- ✔ PCはもちろん、スマートデバイスやIoT機器などが急増して把握しきれない...
- ✔ IT機器が許可なく社内ネットワークに接続されたことに気づけない...
- ✔ IT機器の申請・承認作業に手間がかかりすぎ、管理が大変...

ネットワークに接続するあらゆるIT機器を手軽に検知・遮断・管理できます。



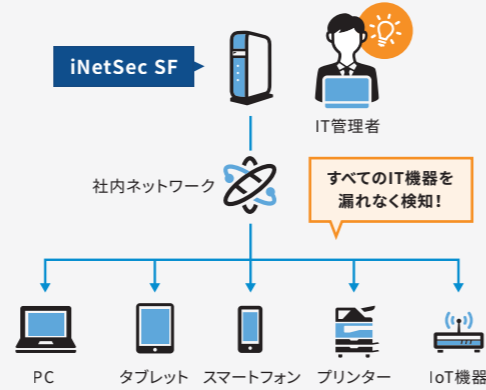
iNetSec SFは、ネットワークに接続されたすべてのIT機器を見える化し、不正持ち込み端末など、リスクのあるIT機器をネットワークから遮断するセキュリティ対策アプライアンス製品です。

特長1 IT機器を見える化

社内ネットワークにつながる 様々なIT機器を見える化

スマートデバイスやIoT機器など、社内ネットワークに接続されるIT機器は急増しています。

iNetSec SFは、PCはもちろん、スマートデバイスやプリンター、IoT機器など社内ネットワークにつながるIT機器をエージェントレスで漏れなく検知し、見える化します。

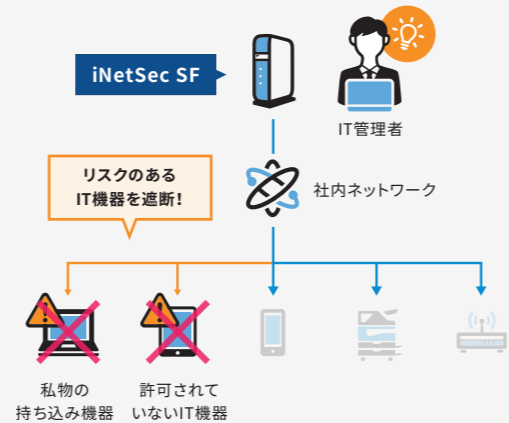


特長2 不正なIT機器を検知し、遮断

IT管理者が接続を許可していない 不正なIT機器を遮断

許可されていないIT機器が接続されると、そのIT機器がセキュリティホールとなり、情報漏洩・ウイルス感染などのリスクが高まります。

iNetSec SFは、許可されていないIT機器が接続された場合、ネットワークから自動遮断します。



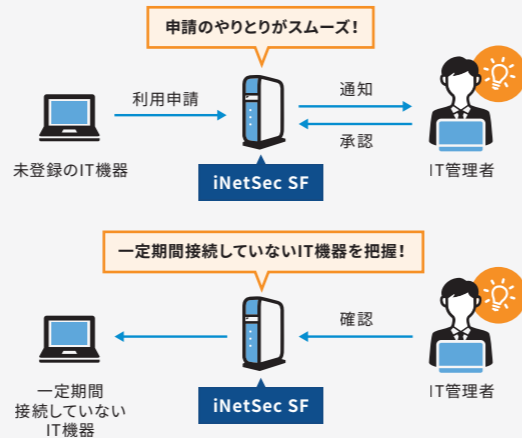
特長3 管理・運用を効率化

利用申請・承認の電子化などで 社内のIT機器を手軽に管理

端末の台帳管理や、申請・承認作業を手作業で行うのは、手間がかかりすぎます。

許可されていないPCやスマートデバイスなどの端末でネットワークを利用すると、自動的に申請画面が表示されます。IT管理者は、利用者からの申請をWEBブラウザ上で承認することができます。

長期間接続していないIT機器の抽出や削除、許可したIT機器の有効期間設定、ポリシーによる機器の自動許可・自動遮断なども行えます。



お客様の状況に合わせて**オンプレミス版**と**クラウド版**からお選びいただけます。



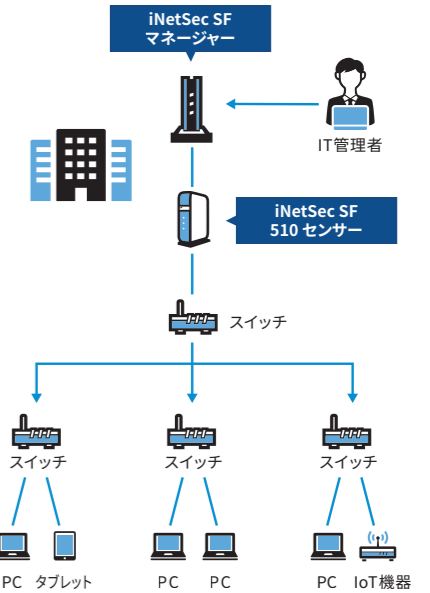
機器検知・不正接続防止に加え、サイバー攻撃対策を行いたいなら! iNetSec SF (オンプレミス版)

機能追加ライセンスで様々なリスクに対応

- 標的型サイバー攻撃対策**
マルウェア活動をリアルタイムに監視し、既知・未知のマルウェアに対しても通信の振る舞いで検知が可能。感染端末を自動的に遮断することで感染拡大を局所化します。
- 脆弱性対策**
最新のOSパッチなど、Windows端末の脆弱性を自動検知し、是正するまで接続を遮断することが可能です。
- 利用アプリケーション監視**
禁止アプリケーションを使用したIT機器を自動的に特定し、遮断します。

他製品と連携し様々なリスクに対応

- サイバー攻撃対策製品**
サイバー攻撃対策製品が検知したマルウェア感染端末をiNetSec SFが自動遮断します。
iNetSecMP 連携 FIREEYE NXシリーズ連携
FORTINET FortiGateシリーズ連携 paloalto 次世代ファイアウォール連携
- IT資産管理ツール**
資産管理ツールのエージェント導入を徹底し、エージェントを導入できないIT機器も一元管理できます。
SKYSEA Client View 連携 LanScope Cat 連携
- ゲートウェイ製品**
iNetSec SFが検知したC&Cサーバ通信をゲートウェイ製品が自動遮断します。
※本機能の利用には「iNetSec SF 標的型サイバー攻撃振る舞い検知セグメントライセンス」の購入が必要です。
IPCOM EX/EX2シリーズ



機器検知・不正接続防止を手軽に導入! iNetSec SF Cloud (クラウド版)

低コスト・スピーディーに導入

管理用ソフトウェア(マネージャー)のためのサーバ構築が不要。より低コストでスピーディーな導入が可能になり、IT管理者の負担を軽減できます。

クラウドで各事業所をまとめて管理

各事業所がVPNやWANなど専用線で接続されていないネットワーク環境でも、クラウドのマネージャーで複数の事業所に設置されたセンサーをまとめて管理可能です。

テレワークの管理者がリモート管理

管理用ソフトウェア(マネージャー)がクラウド上に配置されるため、社内ネットワークに接続されるIT機器を社外から管理することができます。

