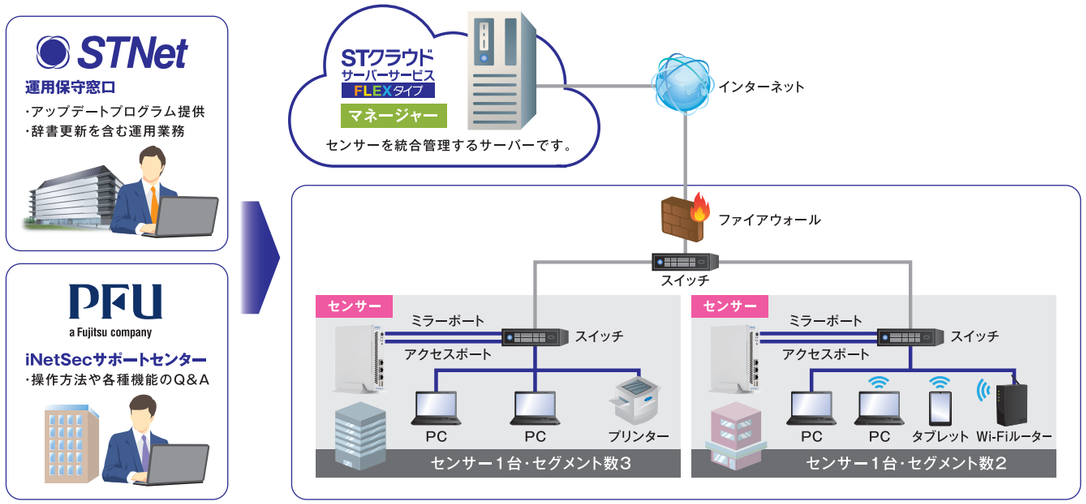
構　成

iNetSec SFは マネージャー と センサー から構成されます。



端末には、iNetSec SFセンサーと通信をおこなうための専用ソフトウェアをインストールする必要はありません。
既存ネットワークにそのまま接続するだけで利用できます。

料　金

（税抜）

項目			課金単位	料金
初期工事費		クラウド設定工事費	1契約毎	22,000円
		マネージャー設定工事費	1契約毎	184,000円
		センサー設置工事費	1センサー毎	86,000円
月額料金	基本料	クラウド利用料	1契約毎	33,800円
		マネージャー利用料	1契約毎	13,000円
	加算料	センサー利用料	1センサー毎	13,400円
		ライセンス利用料（10ライセンス未満）※	1セグメント毎	6,000円
		ライセンス利用料（10ライセンス以上）※	1セグメント毎	4,600円

※ 1セグメントあたりに1ライセンス必要となります。

<上記構成例の場合> センサー2台（2拠点）・セグメント数5

（税抜）

初期工事費		
クラウド設定工事費	マネージャー設定工事費	センサー設置工事費
22,000円	184,000円	172,000円
合計　378,000円		

月額料金		
基本料	センサー利用料	ライセンス利用料
46,800円	26,800円	30,000円
合計　103,600円		

【注意事項】※日本国内の法人のお客さま向けのサービスとなります。※本サービスは、（株）PFUが製造・販売する「iNetSec SF」を用い、お客さまへご提供するサービスです。※本サービスの提供を希望される方は、当社が定める「サービス利用規約」を承認のうえ、当社指定の方法によりお申込みを行っていただきます。※本サービスをご利用いただくにあたり、お客さま拠点に設置するセンサーは監視するスイッチのミラーポート・アクセスポートの2ポートに接続する必要があります。当該ポートに対応していない場合等は、別途お問い合わせください。※本サービスは、全ての不正アタックやウイルス攻撃等から防御することを保証するものではありません。※お申込みの混み具合や当社提供環境の状況によりお時間をいただく場合、または本サービスをご利用いただけない場合があります。※本サービスの最低利用期間は課金開始日より1年間です。最低利用期間満了前に解約される場合は、当社所定の違約金をお支払いただきます。※サービス仕様は、予告なく変更する場合があります。ご了承ください。※本チラシに記載されている会社名・製品名は各社の商標または登録商標です。

STNet
エスティネット 検索
eigyo@stnet.co.jp
TEL 087-887-2404（ビジネス営業本部）
※お問い合わせの回答は営業時間内（平日9:00～17:00）となります。
本店ビジネス営業本部 ／ TEL.087-887-2404　首都圏営業部 ／ TEL.03-4588-4211
香 川 支 店 ／ TEL.087-887-2480　愛 媛 支 店 ／ TEL.089-906-2480
徳 島 支 店 ／ TEL.088-635-2480　高 知 支 店 ／ TEL.088-879-2480

STNetのサービスが、皆さまのビジネスの力に。

データセンター・クラウド　ネットワーク　システム開発

(S)SF4-1

STNet　STNetのサービスが、皆さまのビジネスの力に。

標的型サイバー攻撃・内部対策サービス

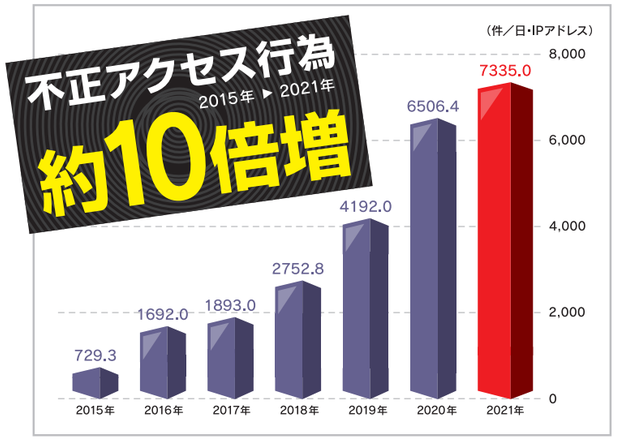
iNetSec SF on STクラウド サーバーサービス FLEXタイプ

Supported by PFU a Fujitsu company

標的型サイバー攻撃により、顧客データ、研究・開発情報など社内の機密情報が窃取される事案が相次いでいます。
事故が発生すると、情報の流出による実害に加え、企業イメージが大きく損なわれ、風評被害も追い打ちをかけます。
インターネットを利用している限り、サイバー攻撃の標的となることを前提とした対策が必要です。

急増する標的型サイバー攻撃

● 不正アクセス行為の認知件数

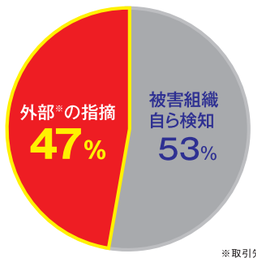


出典：警察庁（令和3年におけるサイバー空間をめぐる脅威の情勢等）

サイバー空間における探索行為は、過去7年で約10倍まで急増しています。

● セキュリティ侵害の発覚経緯

背景 標的型サイバー攻撃の多様化/巧妙化



※取引先、顧客、捜査当局等
出典：経済産業省・IPA（サイバーセキュリティ経営ガイドラインVer2.0）

約50%が外部からの指摘

サイバー攻撃の発覚経緯の約半数は外部からの指摘によるもので、実際攻撃による被害を受けていても、そのことに気づいていない企業が多数存在します。

標的型サイバー攻撃への対策

多様化、巧妙化する標的型サイバー攻撃に対しては、
従来の防御策（ファイアウォール・ウイルス対策ソフトなど）では、充分とはいえません。

「内部への侵入を前提」とし、侵入に対して、
①いかに早く気づくか　②いかに被害の拡大を防ぐか が
重要となります。

iNetSec SF

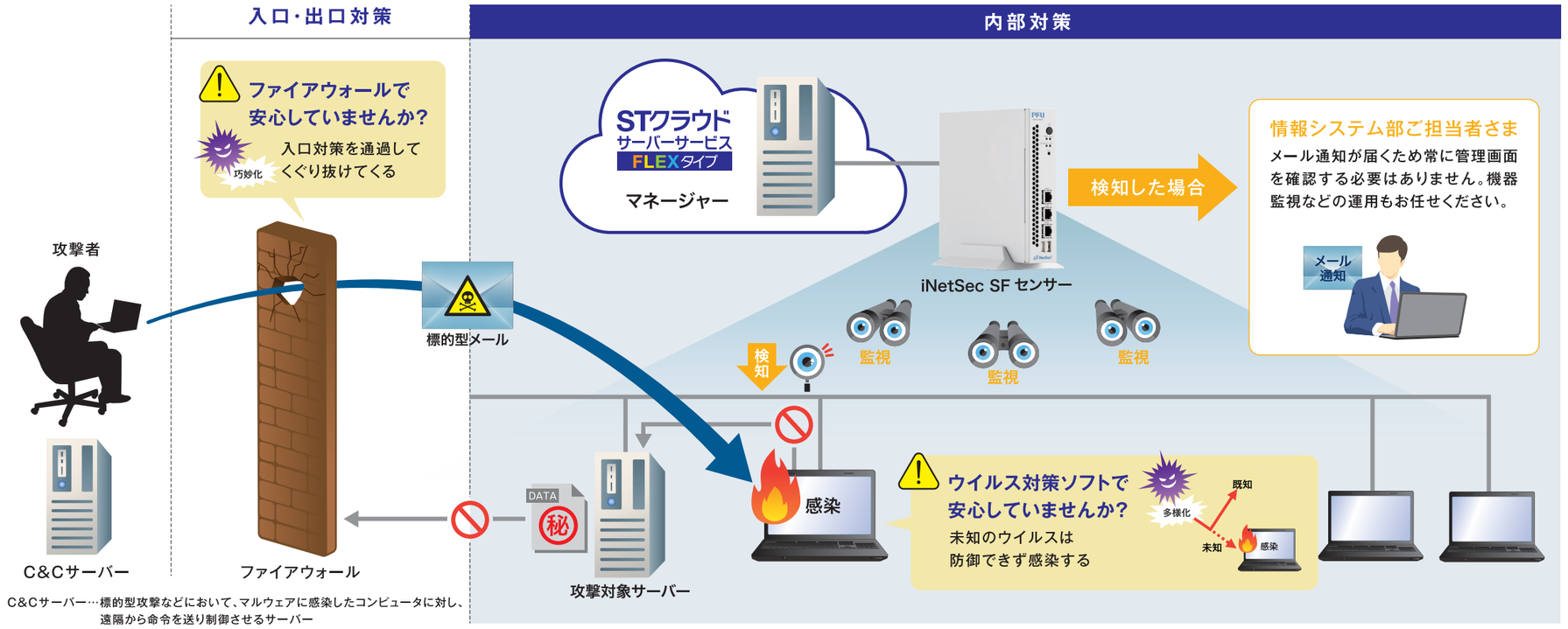
標的型サイバー攻撃による未知のマルウェア活動を検知、被害を防止

標的型サイバー攻撃・内部対策サービス iNetSec SF on STクラウド サーバーサービス FLEXタイプ

Supported by PFU a Fujitsu company

企業内へマルウェアを送り込む手口は、日々巧妙化しています。そのため、標的型サイバー攻撃には「内部への侵入を前提」とした対策が急務となっています。
「内部への侵入を前提」とした対策、そのポイントは「内部対策」の強化です。
iNetSec SF（アイネットセック エスエフ）は、標的型サイバー攻撃によるマルウェアの活動を検知し、感染端末を自動的に遮断し、被害の拡大を防ぎます。

サービス提供構成



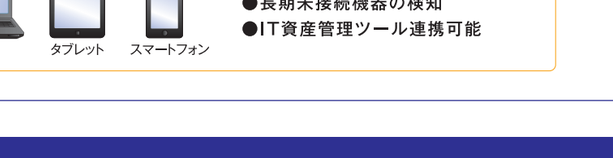
C&Cサーバー…標的型攻撃などにおいて、マルウェアに感染したコンピュータに対し、遠隔から命令を送り制御させるサーバー

サービス提供構成 特長

POINT

専用機器の購入不要!
簡単に導入可能!

月額サービスとして利用可能



- 端末のエージェント導入不要※
- ネットワーク変更不要
- ログ分析や機器監視不要

センサーを統合管理するマネージャーは、当社クラウドサーバーにてご提供します。このため、お客さまでの**サーバーの準備が不要**で、ネットワーク内に設置するセンサーも、**月額利用型**のため、簡単かつ手軽に導入が可能です。マネージャーのクラウド提供からセンサー機器の提供、設置、運用保守までSTNetにすべてお任せください。

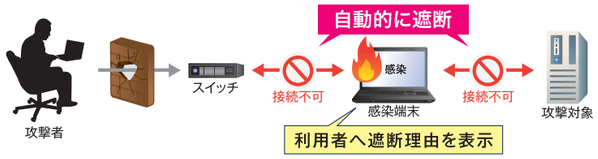
対処リスク

様々なリスクがある端末をネットワークから遮断し、被害を防止

対処リスク❶
標的型サイバー攻撃のリスクを対処

ネットワーク内の通信を監視し、標的型サイバー攻撃の過程で行われるRAT（リモートアクセス型のマルウェア）の諜報活動および感染拡大活動の振る舞いをリアルタイムで検知し、感染した端末を社内ネットワークから自動的に遮断（※）します。

※検知通知のみとして、手動による感染端末の遮断も可能です。



対処リスク❷
アプリケーションのリスクを対処

通信の振る舞いを監視し、SNSやオンラインストレージなど、業務で利用を禁止しているアプリケーションの使用（動作）を検知します。端末遮断機能により、セキュリティポリシーの統制と情報漏えい対策の強化を実現します。

対処リスク❸
「未承認機器接続」のリスクを対処

ネットワーク（有線・無線LAN）に接続されたIT機器が何かを自動検知し、識別し、許可されていないIT機器のネットワーク不正接続を自動で遮断します。持ち込みIT機器によるマルウェア感染や情報漏えいのリスクを未然に防止することが可能です。

IT機器の「見える化」を実現

- 利用申請機能付
- 長期未接続機器の検知
- IT資産管理ツール連携可能