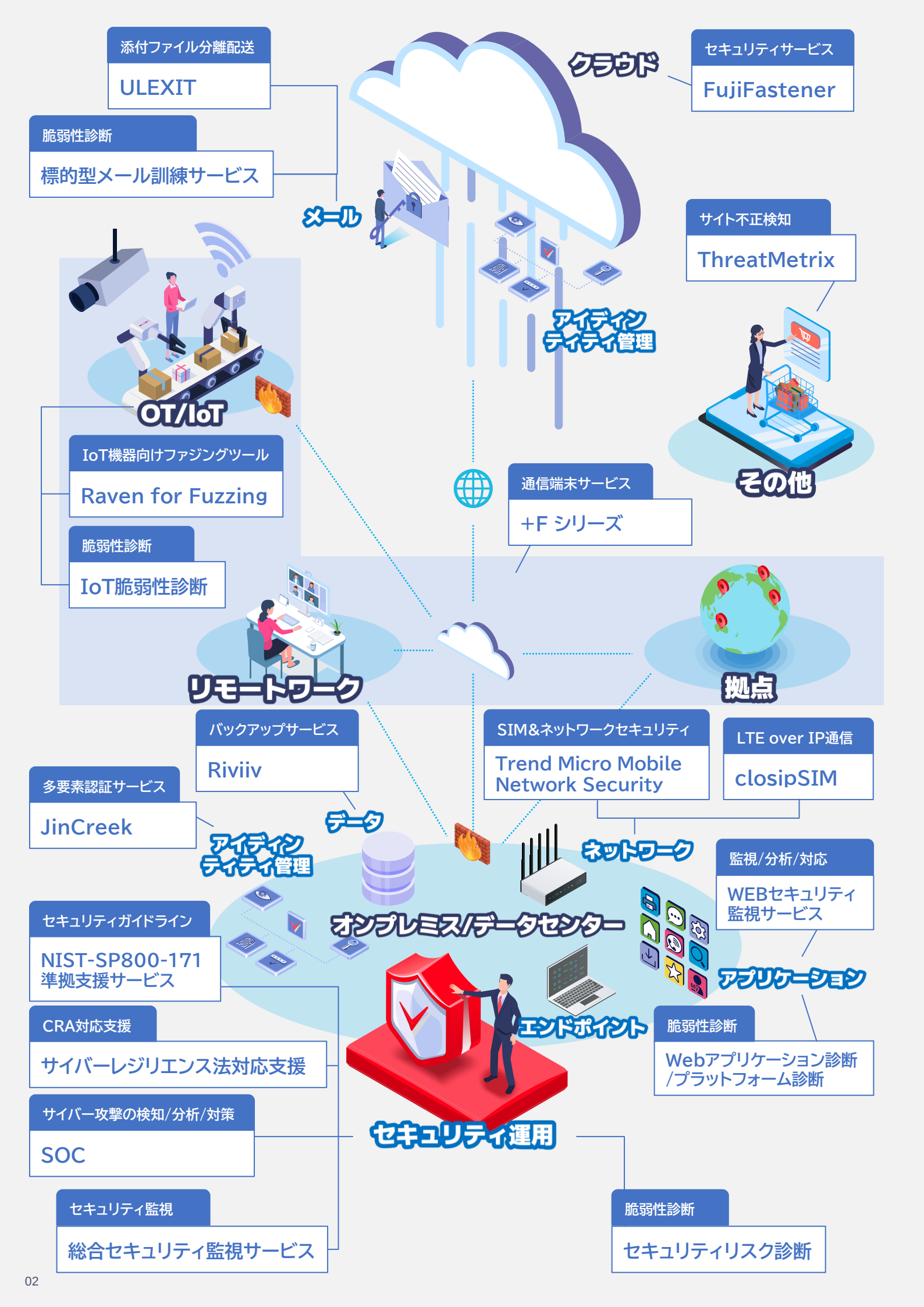
FUJISOFT

富士ソフト 総合セキュリティ対策 ソリューション


添付ファイル分離配送
ULEXIT
脆弱性診断
標的型メール訓練サービス
メール
クラウド
セキュリティサービス
FujiFastener
サイト不正検知
ThreatMetrix
アイデンティティ管理
OT/IoT
IoT機器向けファジングツール
Raven for Fuzzing
脆弱性診断
IoT脆弱性診断
通信端末サービス
+F シリーズ
その他
リモートワーク
拠点
バックアップサービス
Riviiv
SIM&ネットワークセキュリティ
Trend Micro Mobile Network Security
LTE over IP通信
closipSIM
多要素認証サービス
JinCreek
データ
アイデンティティ管理
ネットワーク
監視/分析/対応
WEBセキュリティ監視サービス
セキュリティガイドライン
NIST-SP800-171準拠支援サービス
オンプレミス/データセンター
アプリケーション
CRA対応支援
サイバーレジリエンス法対応支援
エンドポイント
脆弱性診断
Webアプリケーション診断/プラットフォーム診断
サイバー攻撃の検知/分析/対策
SOC
セキュリティ運用
セキュリティ監視
総合セキュリティ監視サービス
脆弱性診断
セキュリティリスク診断

目次

富士ソフト総合セキュリティ対策ソリューション　一覧

パブリッククラウドマネージドセキュリティサービス

FujiFastener

フジファスナー

FujiFastener Powered by CloudFastener

セキュリティコンサルから一部復旧までクラウドをまるっとお任せ

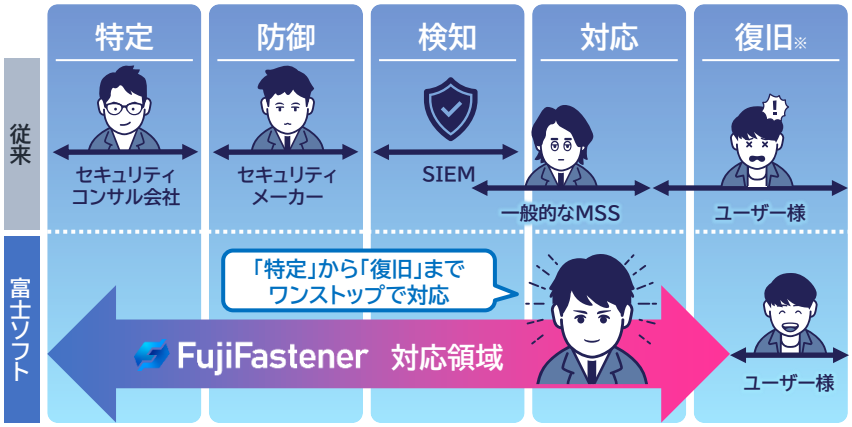
01 幅広い対応領域

マネージドセキュリティサービス

セキュリティコンサルから一部復旧まで幅広いカバレッジでお客様のクラウド環境をサポート。

多くの実績の知見を最大限活用

独立系SIerの知見を活かし、お客様のパブリッククラウドを安心してお任せいただける環境を提供。



※お客様と事前に合意した範囲での実修正作業となります。
※オプションにより一部の復旧業務まで対応可能

02 圧倒的なコストパフォーマンス

各ネイティブサービスのみを利用

例えばAWSの場合、AWS Security Hub、Amazon GuardDutyなど、AWSのネイティブ機能を使用し、『FujiFastener』に統合することで、圧倒的なコストパフォーマンスを実現。

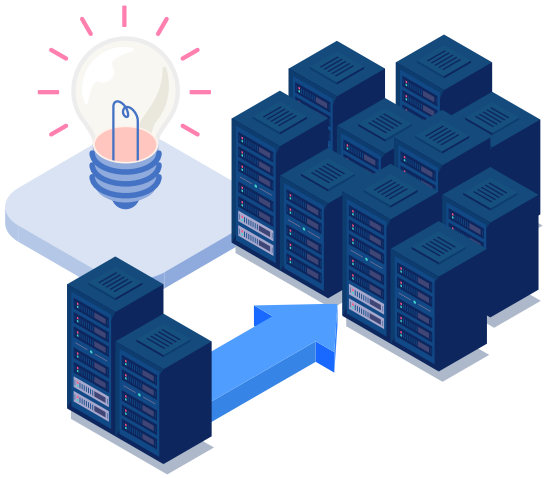
万が一の場合も素早く対応

外部のサービスは使用せず。アラートやログ情報は全てお客様のクラウド環境に残るので、スムーズなインシデント対応が可能。

03 お客様のクラウド環境に合わせて導入

事前コンサルティングで柔軟に導入

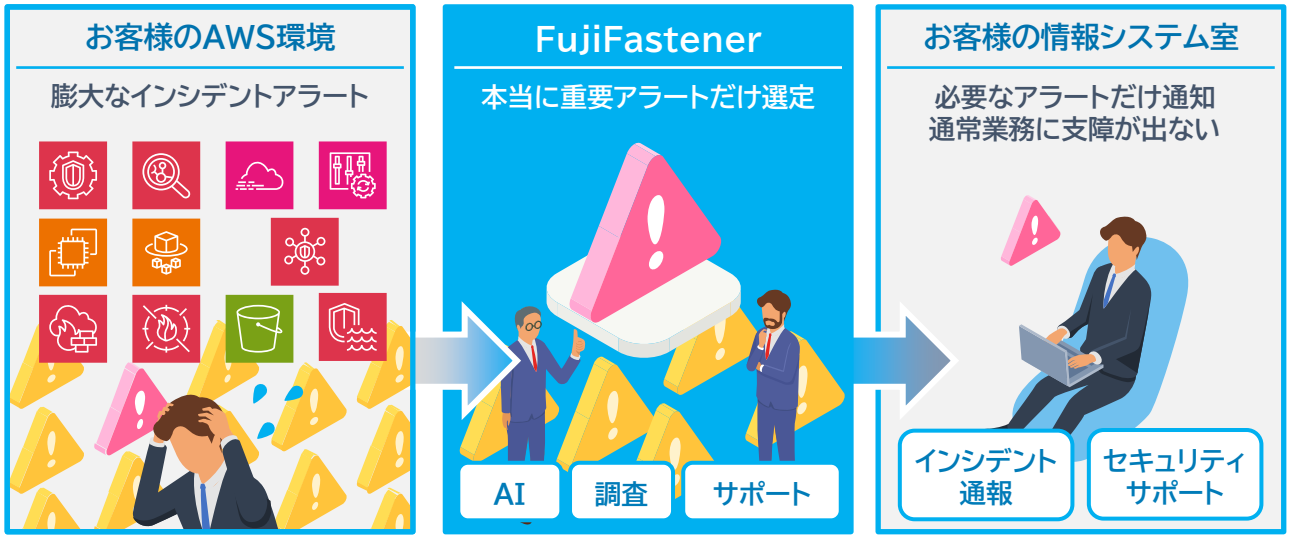
『FujiFastener』はアカウントの規模や数に関わらず、上限・下限なく導入が可能。
自社の組織体制やアカウント状況、環境、予算、マイルストーンに応じてサービスを選択し、優先順位を付け段階的に導入。
いま必要なセキュリティ対策は何か。今後どのような対策が必要か。お客様の抱えている課題や環境・状況にあわせて、柔軟にサービスを提供。



おすすめ

FujiFastener構成:AWSの場合

膨大なインシデントをFujiFastenerが精査し重要なアラートだけ通知



導入メリット

- お客様の環境に合わせてパブリッククラウドのネイディブ機能を有効化
- AIとリサーチャーが24時間365日でお客様の環境を監視、サポート
- 重要なインシデントのみをお客様にご連絡

参考価格

※2025年5月時点

項目	提供形態	課金単位	購入単位	定価
月額費用	サービス	テナント	1か月	￥1,000,000～
オンボーディング（導入費用）	サービス	初回	1回	￥500,000～

『FujiFastener』で提供している標準機能

Threat Detection 脅威検知	Amazon GuardDutyを連携し、継続的にモニタリング、調査、分析を実施し、脅威の報告とその是正案の提示もしくは是正を実施します。
Workload Vulnerability Scanner 脆弱性検知	EC2、ECR、Lambdaなどの脆弱性スキャン結果を継続的にモニタリングし、脆弱性の是正案を提示します。WAFやNetwork Firewall併用時には脆弱性スキャン結果をベースにしたカスタムシグネチャの作成も可能です。
Cloud Audit 証跡タイムライン生成、通知	AWS CloudTrailやAWS Configのイベントをタイムライン化しモニタリングします。お客様の想定されないAWSリソースの操作やAWSコンソールへのログインなど不正を検知・通知します。
Security Guardrail セキュリティ標準モニタリング	「AWS Foundational Security Best Practices」「CIS AWS Foundations Benchmark」「PCI DSS」への準拠性をモニタリングし、逸脱するリソースの検知・通知、是正案を提示します。また、リソースの修正をお客様の要望に合わせて対応いたします。
Resource Inventory AWSリソースインベントリの可視化	AWSリソースの情報を可視化し、シャドーリソースの洗い出しや他サービスと組み合わせてリソース設定の調査を実施します。 ※標準機能

お問い合わせはこちらから：https://www.fsi.co.jp/fujifastener/

Rubrik活用したマネージドバックアップサービス

Riviiv

リヴァイブ

導入費0円で復旧まで対応のランサムウェアバックアップサービス

01 イニシャルコストを大幅に低減

導入費用0円ですぐ始められる

Riviivは導入費用不要。高性能なランサムウェア対策を月額費用のみで実現。
例えば、重要なデータのみを対象とする場合やお試しでの一時利用にも有効。

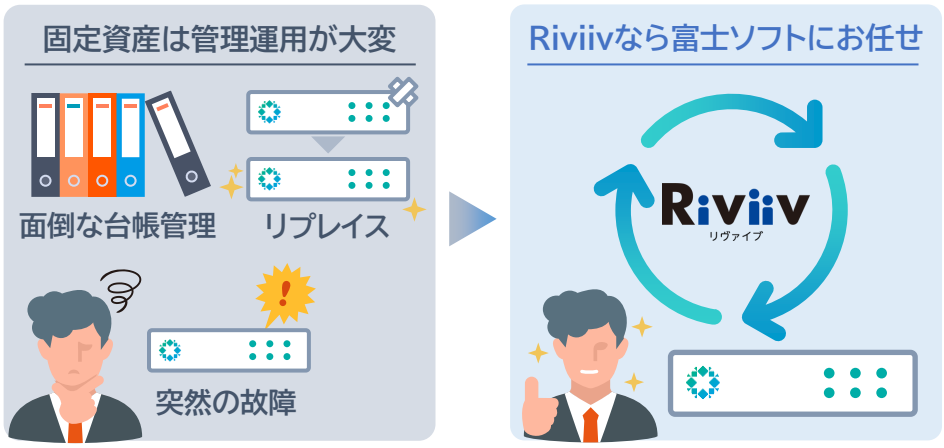
重要データの強固なセキュリティ対策に

本格導入前や試用など一時的な利用に

02 資産を持たずにRubrikを利用可能

最小限の工数で運用可能

通常、資産を持つことで管理・運用の手間増加、老朽化や故障による対応が必要となり、工数増加が発生。
Riviivであれば資産を持たずに利用可能なので煩わしい管理、リプレイス、故障対応を気にせず、強固なセキュリティの実現。



03 初期構築や導入後の運用を富士ソフトが支援

導入～復旧まで対応のマネージドサービス

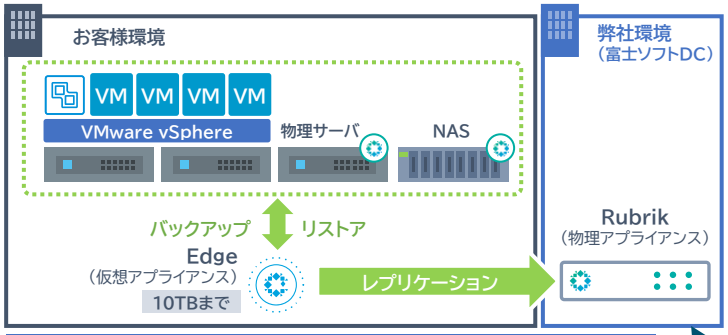
初期構築費用はもちろん、導入後の運用もすべて富士ソフトが実施。万が一の際、経験豊富なエンジニアによる復旧まで対応。ランサムウェア被害時の混乱や慌てた状況でも、Riviiv利用による安全迅速な復旧可能。

おすすめ

Riviiv構成（オンプレミス）

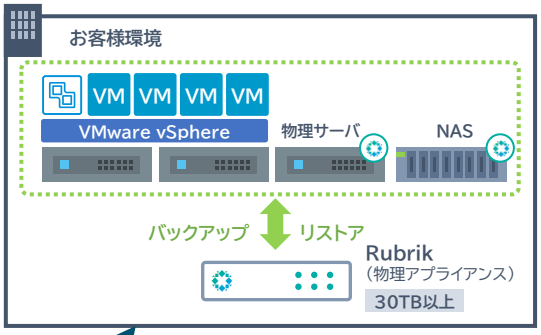
オンプレ向けRubrik共有型（マルチテナント）

お客様拠点にEdge（一次バックアップ機器）を設置して富士ソフト DCのRubrikへデータをレプリケーションする方式（10TBまで）



オンプレ向けRubrik占有型（シングルテナント）

お客様拠点に富士ソフト資産のRubrikを設置する方式（30TB～）



富士ソフト マネージドサービス

初期設定から運用中の作業など実施

導入メリット

- 富士ソフトサービスデスクがRubrik管理コンソールを通じてデータを監視
- マルチテナントは仮想アプライアンスを導入し、富士ソフトDCにレプリケーション

参考価格

※2025年5月時点

項目	課金単位	購入単位	月額料金
オンプレミス	10TB～120TB	12か月～60か月	￥600,000～
クラウド	10TB	12か月	￥200,000～
クラウド向けオプションサービス	10TB	12か月	￥80,000～

サービスのSLA（Service Level Agreement）

項目	作業名	SLA	SLO	備考
問い合わせ	受付完了	1時間以内/月	ー	インシデント管理システムへの登録日時または電話終話日時からインシデント管理システムでの受付処理を完了した時間
	1次回答	24時間以内/月	ー	インシデント管理システムにて受付処理をした時間から最初の応答を返した時間
監視	障害発生連絡	ー	1時間以内	
障害対応	障害対応進捗報告	ー	適宜	お客様に影響する障害のみ
オペレーション	バックアップ設定変更	ー	3営業日以内	お急ぎの場合などはその旨をご連絡頂ければ、ベストエフォートで対応
	リカバリ（緊急時）	ー	1営業日以内	実施タイミングについてご指定があればご相談ください
	リカバリ（緊急時以外）	ー	3営業日以内	お急ぎの場合などはその旨をご連絡頂ければ、ベストエフォートで対応

お問い合わせはこちらから：https://www.fsi.co.jp/solution/riviiv/

次世代型サイト不正検知ソリューション

ThreatMetrix

スレットメトリックス

Webサービスの「なりすまし」を防ぎ企業と顧客の資産を保護

01 オルタナティブデータで不正を検知

高度なリスク評価が可能

一般的な不正検知ツールでは利用されない「オルタナティブデータ」を利用した不正検知。
デバイス、地理位置情報、Eメールアドレス、IPアドレス、行動パターン、ユーザのデバイス操作などのシグナルを評価。

怪しいIDを追跡

デバイスとその利用者の「デジタルID」を追跡。不審なデバイスやアクセスの傾向を見逃さない監視体制。

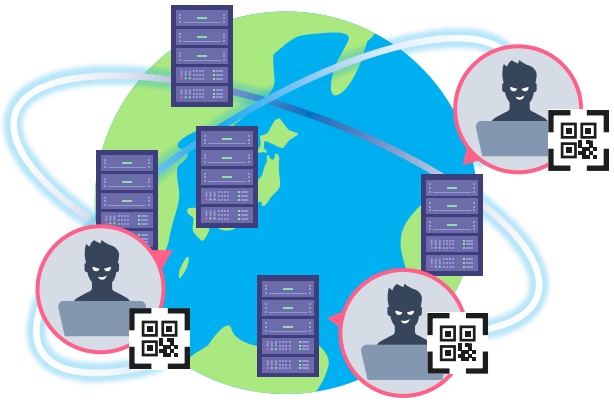
02 ワールドワイドのデジタルIDネットワーク

世界中からの脅威情報を利用

多様性に富んだ世界最大級のデジタルインテリジェンスネットワークに接続。エンドユーザのプライバシーを守りながら、リアルタイムのデジタルIDインテリジェンスを利用。

リアルタイム不正検知力

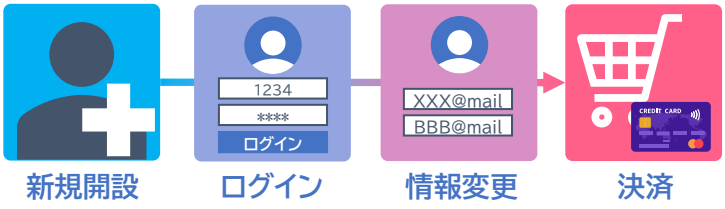
200を超える国と地域で、年間1000億件以上のトランザクション、33億以上のデジタルID、47億以上のEメールアドレスを追跡。
最新の不正傾向を反映し、国際的スレットアクターの動きも見逃さない監視体制。



03 取引のあらゆる側面で不正を検知

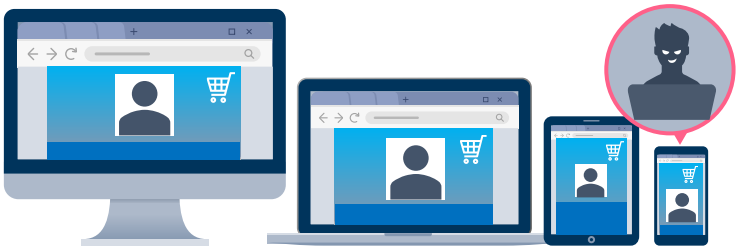
IDのすべてのフェーズに対応

支払や送金といった「最後の瞬間」だけではなく、新規アカウント開設、ログイン、アカウント管理（登録情報変更）などの様々な場面で不正を検知。エンドユーザのジャーニーにおけるあらゆる場面で犯罪の芽を叩く。



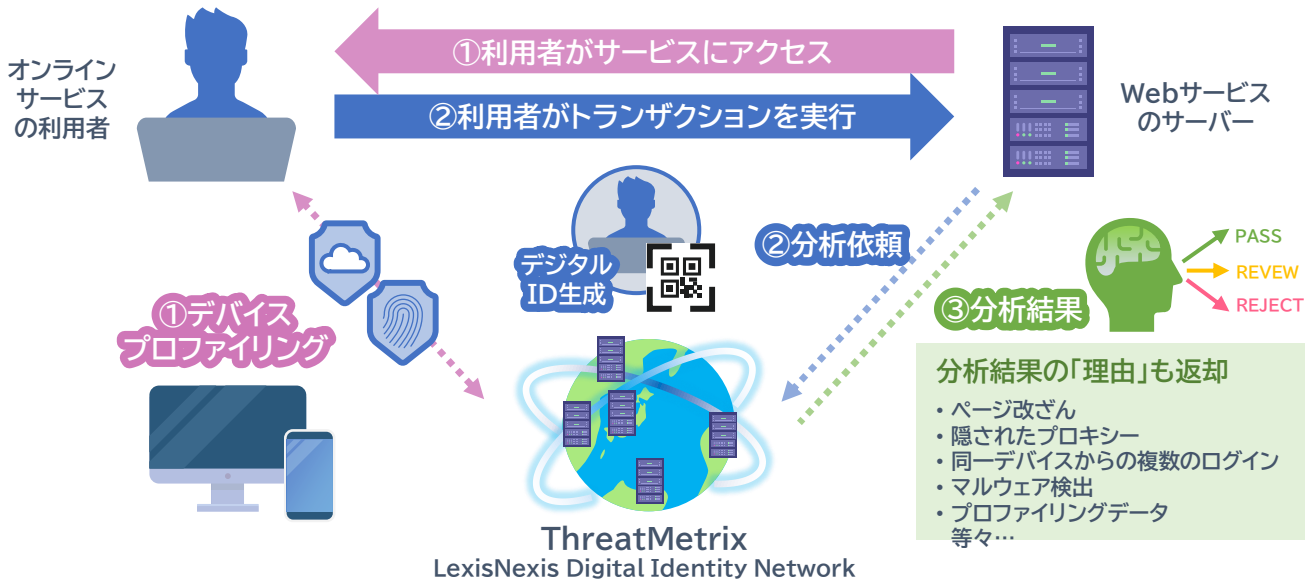
様々な業界/多くのデバイスをカバー

EC、マイページ、オンライン金融など業種を選ばずあらゆるオンラインシーンでの「なりすまし」を検知。
Web、ネイティブアプリ、PC/モバイル、国内外取引/攻撃、すべて対応。



おすすめ

ThreatMetrix



導入メリット

- ThreatMetrixが独自にデバイス情報の収集・プロファイリングを実施。サービスへの負荷を増やさず、様々な妨害手段を回避
- UXを阻害しないシステムデザイン
- 実用的なスコアによる判断、説明可能な結果を提示

参考価格

※2025年5月時点

項目	提供形態	課金単位	購入単位	定価
ThreaMetrix ご利用ライセンス	SaaS	サブスクリプション	検査実行数による	ご相談ください
導入支援サービス	受託			ご相談ください
運用支援サービス	受託			ご相談ください

オプション機能等

運用支援サービス

お客様ごとのビジネス内容、被攻撃状況に対応した、富士ソフトの専門アナリストによる運用支援サービスをご提供

BehavioSec

デバイスの操作やキータイピングなどの「クセ」を見極め、利用者本人であるかを判別する“BehavioSec”機能をオプションでご提供

Emailage

登録に使われるメールアドレスを用いて不審なユーザを検出する“Emailage”との連動が可能

Decision Trust

オルタナティブデータによる与信効率を改善する“Decision Trust”もご提供可能

お問い合わせはこちらから：https://www.fsi.co.jp/tmx/

ルーター・USBドングル・MDMサービス

+F シリーズの通信端末・サービス

累計販売数100万台以上！モバイル環境やIoT運用課題を解決

01 マルチキャリア対応したSIMフリーのルーター・USBドングル

利用シーンに応じて提案可能な充実のラインナップ

テレワークや日常業務、IoT/M2M利用まで様々なビジネスシーンに適用できるSIMロックフリー対応のモバイルルーター、M2Mルーター、USBドングルをラインナップ

ラインナップ

+F FS050W

+F FS045W

+F FS040U

+F FS010M

02 モバイル通信端末を遠隔管理可能なMDMサービス

通信速度や通信量の制御が行える法人向けのクラウド型MDMサービス

+F シリーズのモバイルルーターやM2Mルーター、USBドングルなど、各種デバイスの一括管理、遠隔操作、eSIM制御が可能な上、回線の管理、制御も可能な通信環境の統合的な管理/制御サービス。

03 他社ソリューションの通信環境として採用実績

閉域通信やSIMアプレットを利用したセキュリティーソリューション等で活躍

ソリューション	詳細は
多要素認証サービス「JinCreek」	P.12
LTE over IP通信モジュール「closipSIM搭載モバイルルーター」	P.14
セキュリティ機能内蔵SIMカードとネットワークセキュリティー「Trend Micro Mobile Network Security」	P.16

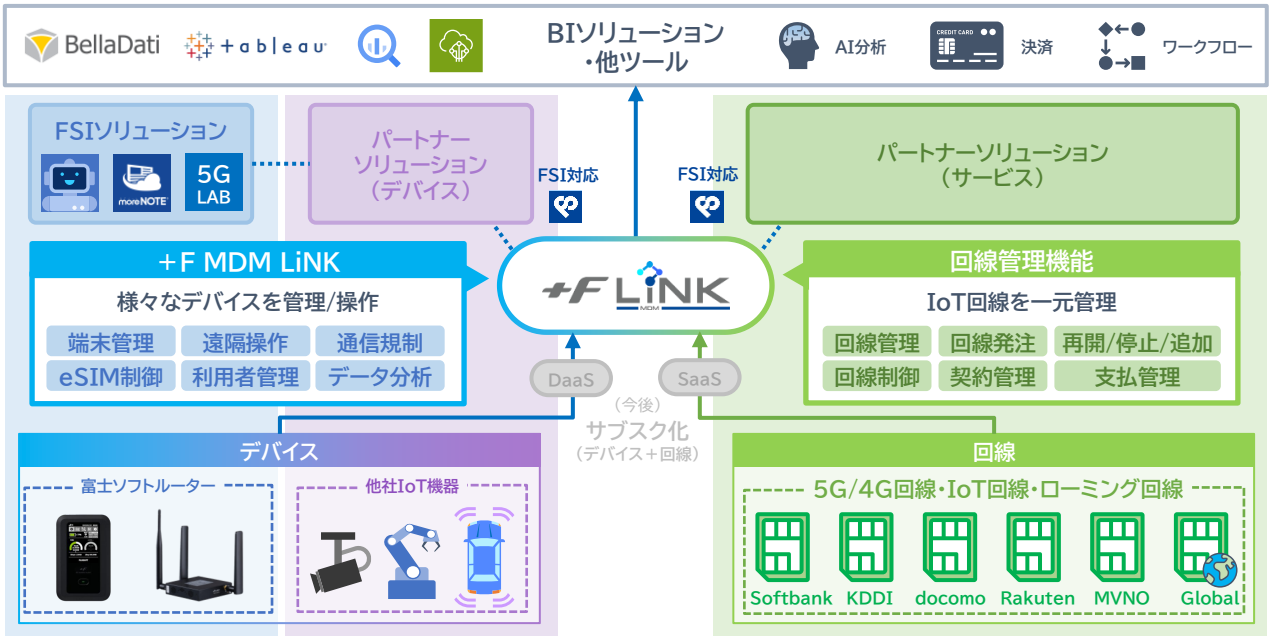
JinCreek

closipSIM搭載モバイルルーター

Trend Micro Mobile Network Security

おすすめ

+F シリーズの通信端末・サービスとパートナーソリューションの構成



導入メリット

- 利用シーンに応じて提案可能な＋Fシリーズの充実ラインナップ
- ＋F MDM LiNKで通信端末も回線も統合的に管理・制御
- 他社製ソリューションと連携して柔軟に拡張可能

参考価格

※2025年5月時点

項目	提供形態	課金単位	購入単位	定価
端末各種	＋F FS050W ＋F FS045W ＋F FS010M ＋F FS040U	販売	1台～	OPEN価格
モバイル回線(SIM)	※ モバイル回線はキャリアやデータ容量など各種取扱していますので、お気軽にお問い合わせください。	販売	1枚～	お問い合わせください
＋F MDM LiNK	初期費用：初期設定料	導入時のみ	1契約あたり	¥30,000
	初期費用：端末登録料	導入時のみ	1契約あたり	¥1,000
	基本サービス(月額)※	月額	1契約あたり	¥500
MDM	初期費用：初期設定料	導入時のみ	1契約あたり	¥20,000
	初期費用：端末登録料	導入時のみ	1契約あたり	¥1,000
	基本サービス(月額)※	月額	1契約あたり	¥500

※数量、契約年数により費用は異なります。最低利用期間は6か月間です。

オプション

＋F 充電/LANステーション

充電やLANケーブル続可能なクレードル

対象：
＋F FS050W
＋F FS045W

4G 延長アンテナ

屋内外に設置可能な延長アンテナ

対象：
＋F FS010M

USB Type-C 変換アダプター

USB Type-Cポートに＋F FS040Uを接続するための変換コネクタ

対象：
＋F FS040U

お問い合わせはこちらから：https://fsi-plusf.jp/products/

多要素認証サービス

JinCreek ＆ ＋F モバイル通信端末

最も安全性の高いSIM閉域網×”JinCreek”でオフィスと同環境

01 リモートワークのセキュリティ不安をほぼゼロへ

特許取得！検疫型多要素認証を採用

ID・パスワードに代わる多要素認証（SIM認証、デバイス認証、本人認証）後に社内ネットワークへのアクセスが可能。多要素認証はパソコンログイン時に自動で行われ、スムーズ。

LTE接続＆閉域網だからさらに安心

LTE接続でさらに安心。暗号化されたLTE接続からインターネットに接続しない閉域接続を利用することで、よりセキュアな環境を提供。

AD連携でポリシーの継続が可能

自社IPアドレス接続とAD連携により、外部アクセスという概念をなくし、社外でも社内と同じ環境を実現。

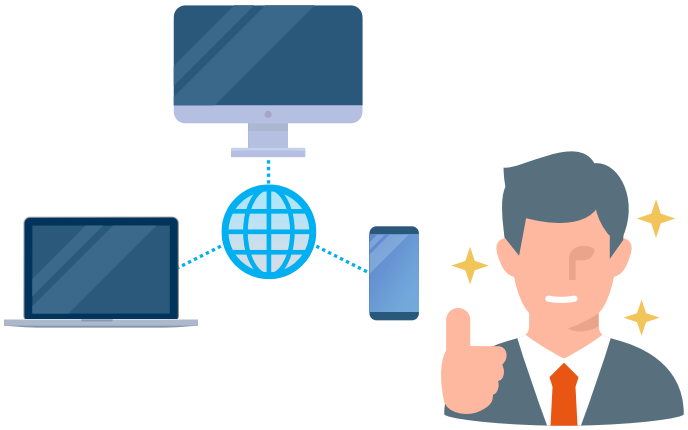
02 既存環境を利用し、導入・運用の負担を最小限に

既存のキャリアや認証システムとの連携が可能

現在のネットワーク構成もしくは認証システムを既にお持ちの場合、そのまま利用可能。ソフトウェアとの連動で、既存の環境を変更も必要なし。

グルーピング機能で運用も手間なく

グルーピング機能を利用すれば、複雑な認証設定も一括で可能。複数人で共有している端末でもそれぞれで認証設定できる、自由度の高いサービス設計。



03 いつでも、どこでも安全にサクサクつながるリモートワークを

LTE接続でストレスフリーなリモートワーク

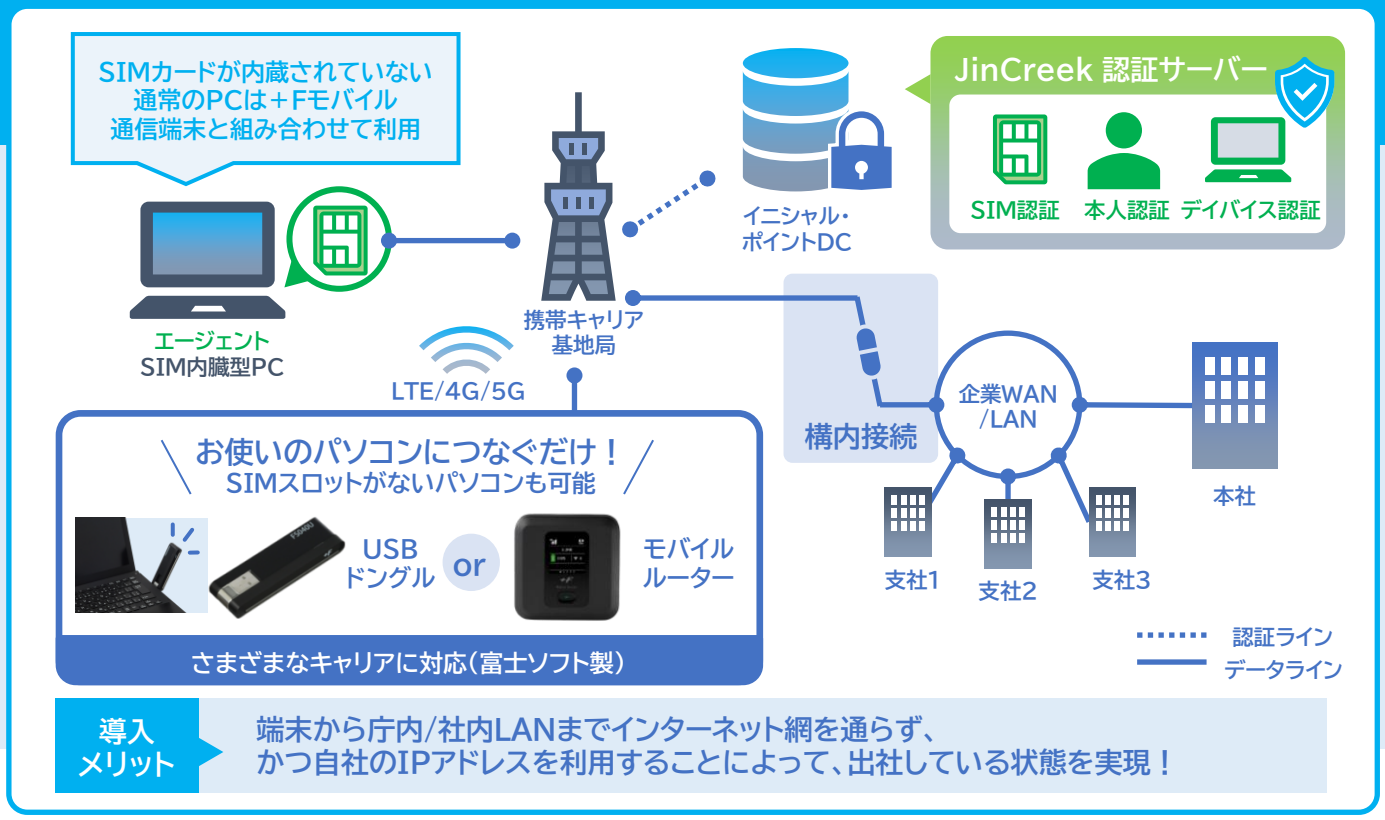
4G/5G/6GのLTE接続だから、安定した速度で利用可能。外出先でWi-Fiエリアを探す必要なく、災害時の安心。

スマートなネットワーク切り替えが可能

社外ではLTEで接続を行い、社内に戻ればWi-Fiを自動検知。ネットワークを切り替える手間なし、運用も楽々。

おすすめ

JinCreek構成



導入メリット

端末から庁内/社内LANまでインターネット網を通らず、
かつ自社のIPアドレスを利用することによって、出社している状態を実現！

参考価格

※2025年5月時点

項目	提供形態	課金単位	購入単位	定価
月額ライセンス	お問い合わせください			
年間ライセンス	お問い合わせください			

導入事例

数千名以上の職員様の安全なテレワークを実現！

課題

JinCreek for SIM閉域網を既存のパソコン（SIMが刺さらない従来のPC）で利用できるようにしたい。

テレワーク時にインターネットへの接続はせずに業務を行いたい。

効果

モバイルルーターなどの外部通信デバイスを組み合わせることができたためSIMの刺さるパソコンを新規購入せずに実現でき、費用を抑えることができた。

- 外部通信デバイスも認証要素にできたことで、予想以上にセキュリティが高くなった。
- パソコンやSIMが盗難・紛失となっても組み合わせ認証のため、単体での悪用が不可能になりセキュリティが高まった。

お問い合わせはこちらから：https://info.fsi-plusf.jp/jincreek_plusf

LTE over IP搭載モバイルルーター

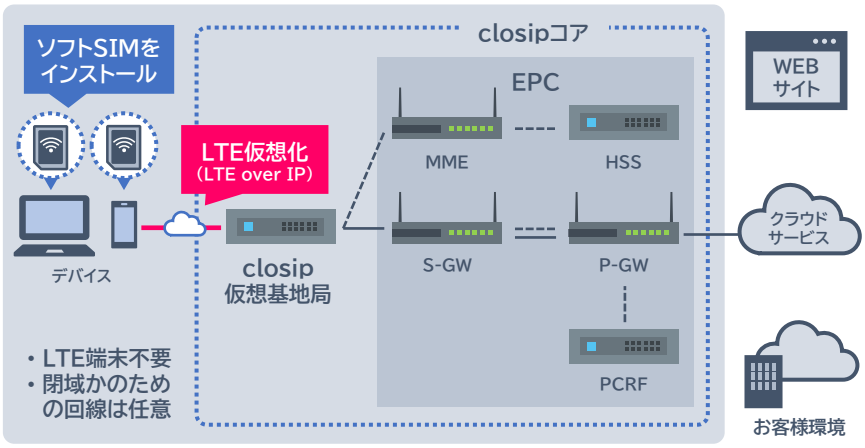
closipSIM ＆ ＋F モバイルルーター

有線回線なしでも監視カメラやIoT機器等のデータを安全に接続

01 LTE over IP通信モジュールclosipSIMを内蔵

closipSIMによる仮想閉域接続

LTE over IP通信モジュール、closipSIMを内蔵することで、モバイルルーターに接続している機器を設定した通信先と仮想閉域接続が可能。



02 管理コンソールから遠隔操作、管理

closipSIMをリモートインストール

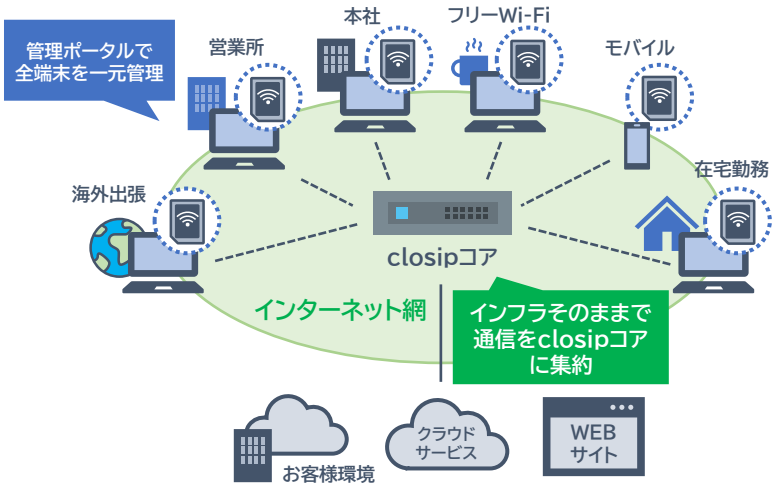
モバイルルーターに挿入したSIMを使って閉域接続用のclosipSIMをリモートインストール可能。

closipSIMの管理

管理コンソールから簡単にclosipSIMを無効化可能、不正利用防止や紛失時対策を遠隔から迅速に対応。

利用者管理

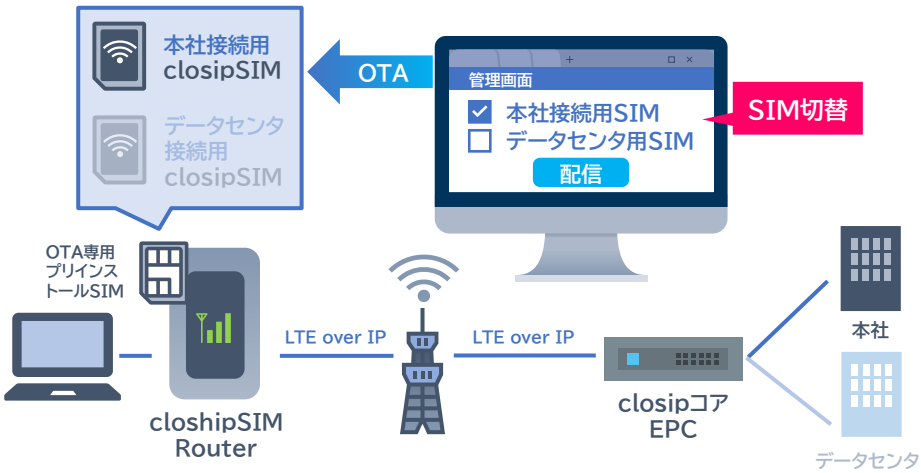
管理コンソールで利用者や利用時間を可視化して、わかりやすく把握可能。



03 用途に応じたclosipSIMの遠隔切り替え

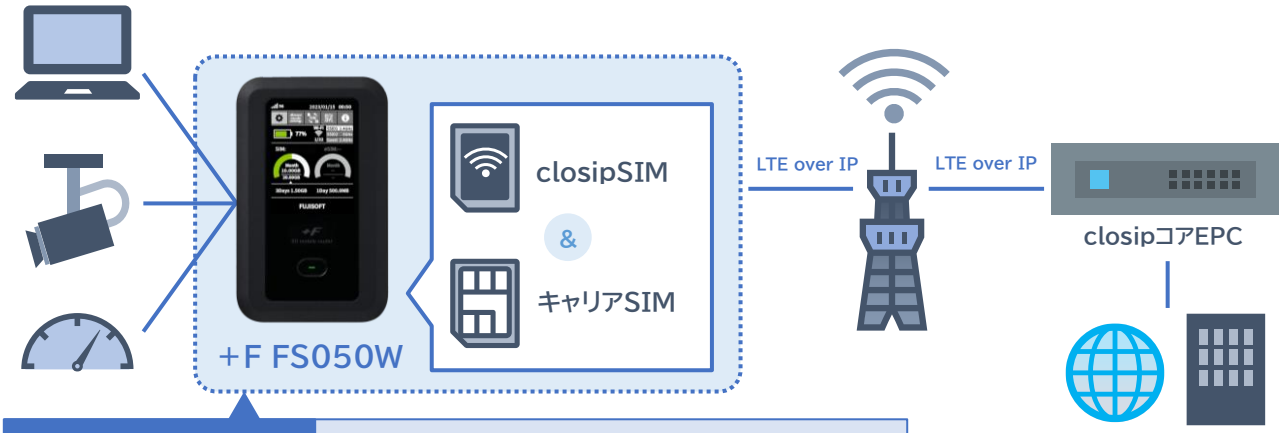
管理コンソールから遠隔SIM切り替え

SIMカードの抜き差しをすることなく、管理コンソール上で、遠隔から用途に応じた閉域接続先へ切り替え可能。



おすすめ

closipSIM搭載＋F FS050Wの構成



closipSIM Router

対応IPプロトコル: IPv4
WANポートアドレス取得方法: DHCP, PPPoE
LANポートアドレス取得方法: DHCP, IPアドレス固定
オーバーレイネットワーク: LTE over IP
認証プロトコル: 3GPP AKA

カプセリングプロトコル: ESP
暗号化: AES-256
対応IPプロトコル: IPv4
同時接続トンネル数: 1

導入メリット

端末から庁内/社内LANまでインターネット網を通らず、
かつ自社のIPアドレスを利用することによって、出社している状態を実現！

参考価格

※2025年5月時点

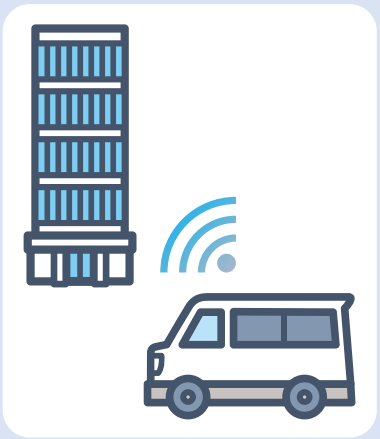
項目	提供形態	課金単位	購入単位	定価
月額ライセンス	お問い合わせください			
年間ライセンス	お問い合わせください			

導入事例

Case.1 百貨店

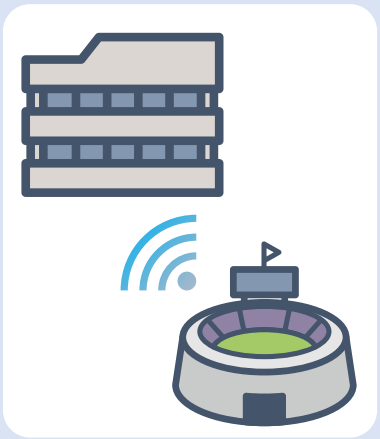
社員向けPCのセキュアなリモートアクセス環境として導入。

Case.2 報道機関



現場からの迅速な原稿データ送付のために、セキュアで高速かつ安定な通信環境として導入。

Case.3 イベント業者



イベント開催地で顧客サポートにあたりながら、現場から社内へのアクセスもストレスなく簡単に行えるテレワーク通信環境として導入。

お問い合わせはこちらから：https://info.fsi-plusf.jp/closip_plusf

セキュリティ機能内蔵SIMカードとネットワークセキュリティー

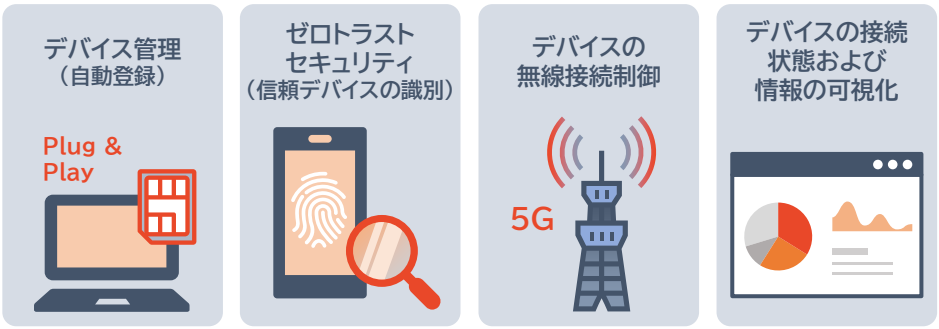
Trend Micro Mobile Network Security

セキュリティ連携で4G/5G/ローカル5G環境を安全に！

01 エンドポイントセキュリティ

IoT/IIoTエンドポイントデバイスの保護

ゼロトラストポリシーにしたがい、SIMカード内蔵セキュリティ機能により、モバイル接続されるIoTデバイスのID検証(IMEI/IMSI)や位置情報取得、無線接続を制御。



02 ネットワークセキュリティ

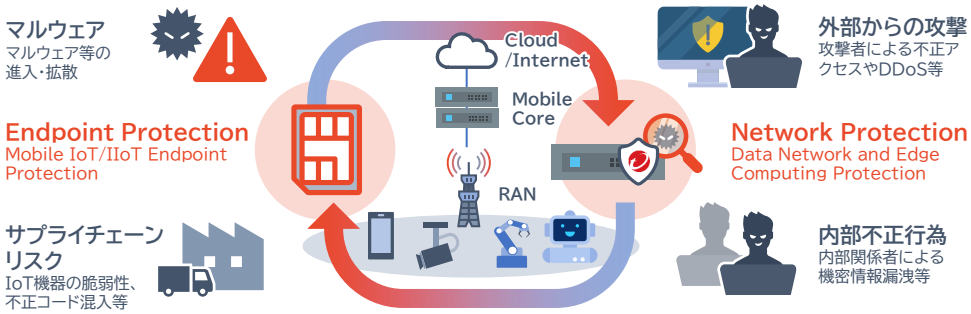
データネットワークやエッジコンピューティングの保護

モバイルネットワーク内に配置、通過する通信をモニタリング、脆弱性への攻撃や悪意あるコンテンツ、ネットワークへの侵入行為や攻撃などを検知・ブロック。

03 エンドポイント×ネットワークによるジョイントディフェンス

セキュリティ状態に応じた柔軟な制御を実現

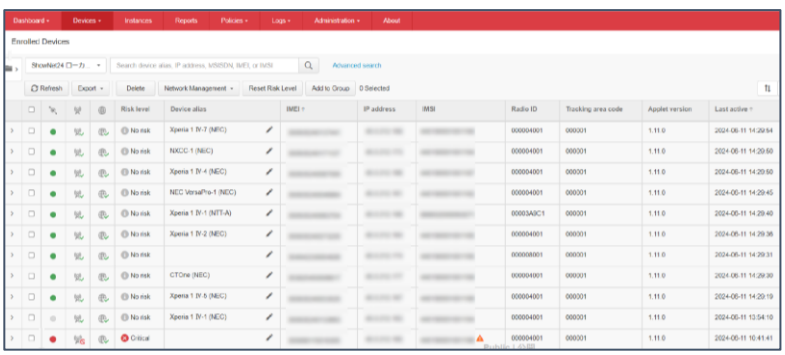
ネットワークセキュリティとエンドポイントセキュリティを組み合わせた連携により、無線アクセスとIPネットワークの複合環境においてさらに強固なセキュリティ脅威に対処が可能。



04 デバイス管理とセキュリティ状態の可視化

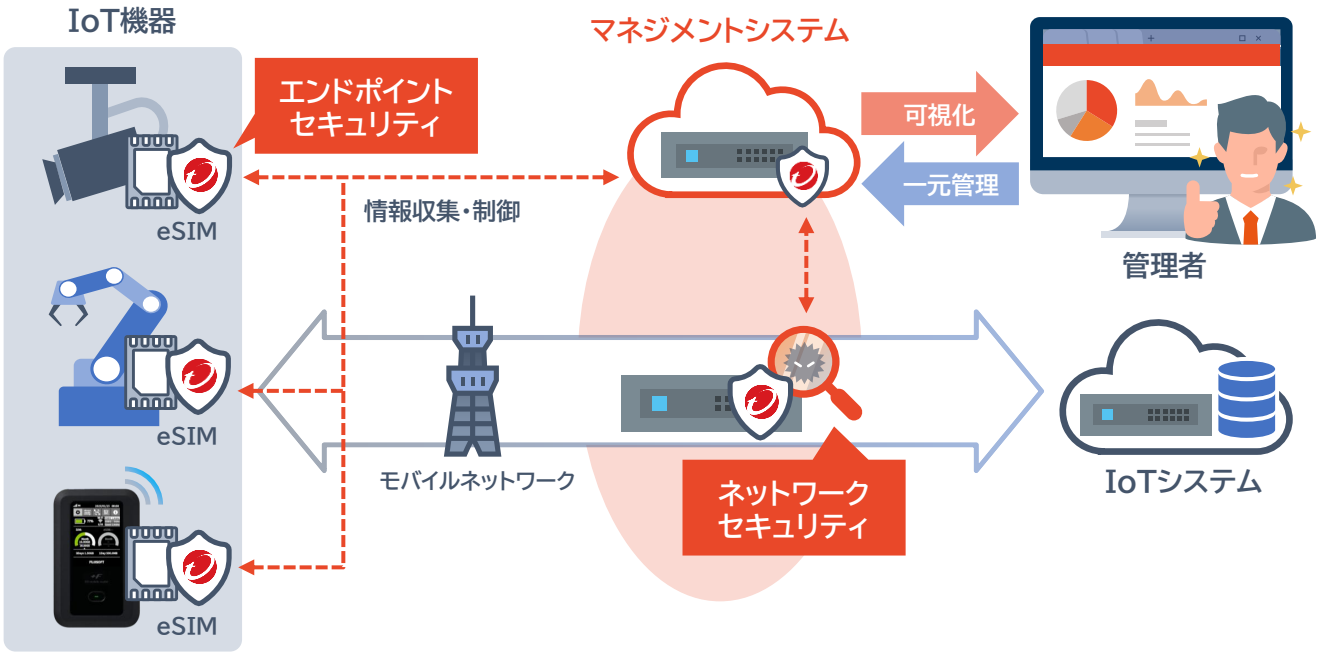
監視や運用のしやすさ

単一コンソールによる統合セキュリティ管理で、通信技術とIT技術の両方の知見を要求される運用管理者の負荷を軽減。



おすすめ

Trend Micro Mobile Network Security(TMMNS)構成



導入メリット

脆弱性を抱えたまま長期間放置されやすいIoT機器のセキュリティ課題を解決
運用管理者の業務負荷を軽減

参考価格

※2025年5月時点

項目	提供形態	購入単位	定価
TMMNS 専用SIMカード	物理SIMカード	端末台数	ご相談ください
TMMNS Endpoint Protection	サブスクリプションライセンス	端末台数	
TMMNS Network Protection	サブスクリプションライセンス	監視対象スループット	
TMMNS Management System	サブスクリプションライセンス	1環境につき1台	

コンポーネントの提供機能

機能		Endpoint Protection	Network Protection
可視化	デバイス	○	
	無線接続	○	
	ネットワーク		○
デバイス管理	デバイス情報自動登録	○	
	無線ネットワークアクセス制御	○	
セキュリティ対策（保護機能）	ゼロトラストセキュリティ（SIMスワッピング・なりすまし対策）		○
	データネットワークアクセス制御		○
	侵入検知・防御		○
	仮想パッチ		○
	異常通信		○
	URLアクセス制御		○
	Web/IoTレピュテーション		○
	SSLインスペクション		○
	Jointディフェンス	○	

お問い合わせはこちらから：https://info.fsi-plusf.jp/tmmns_plusf

メール添付ファイル分離配送サービス（脱PPAP）

ULEXIT

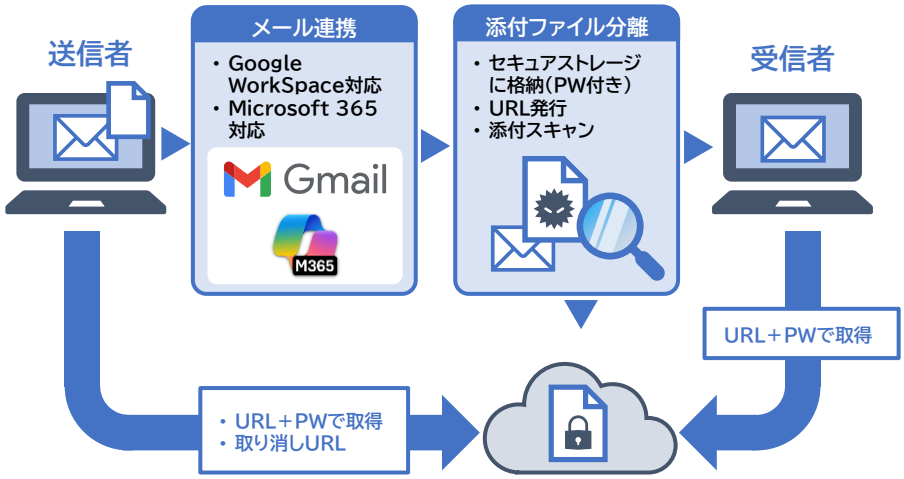
ウレキサイト

簡単導入。ユーザー側に負担をかけず、脱PPAPを実現！

01 不要な機能を省き、シンプルさを追求

脱PPAP部分のみに焦点を当てたメール添付ファイル分離配送サービス

GmailやOutlookメールサーバーとの連携が簡単に設定可能。
不要な機能を省き、簡単に導入できる仕組みで従業員1,000名以上の企業様におすすめ。
※お客様に合わせた、お手頃なプランも提案可能



02 操作数を極限まで削減

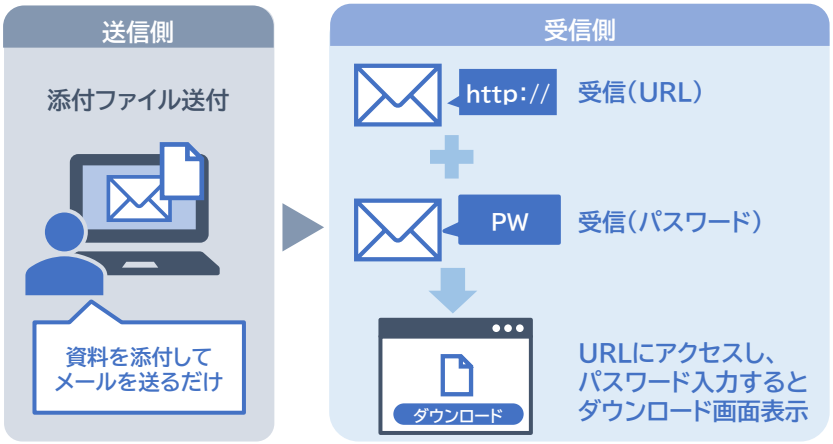
ユーザー側、システム管理側ともに手間がかからない

【ユーザー側】

送信者、受信者どちらの操作数も極限まで削減し、送信者はメールに資料を添付して送るだけ。
受信者は自動的に送られてくるURLとパスワードを利用して開封。

【システム管理者側】

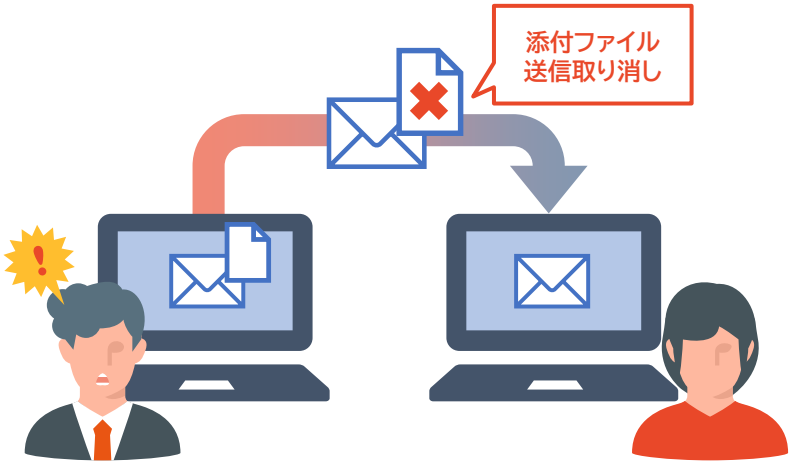
初期設定後については日常的な操作や設定は不要。メールの送信状況をすぐに確認できる画面を用意。



03 安心安全＆将来的な拡張性

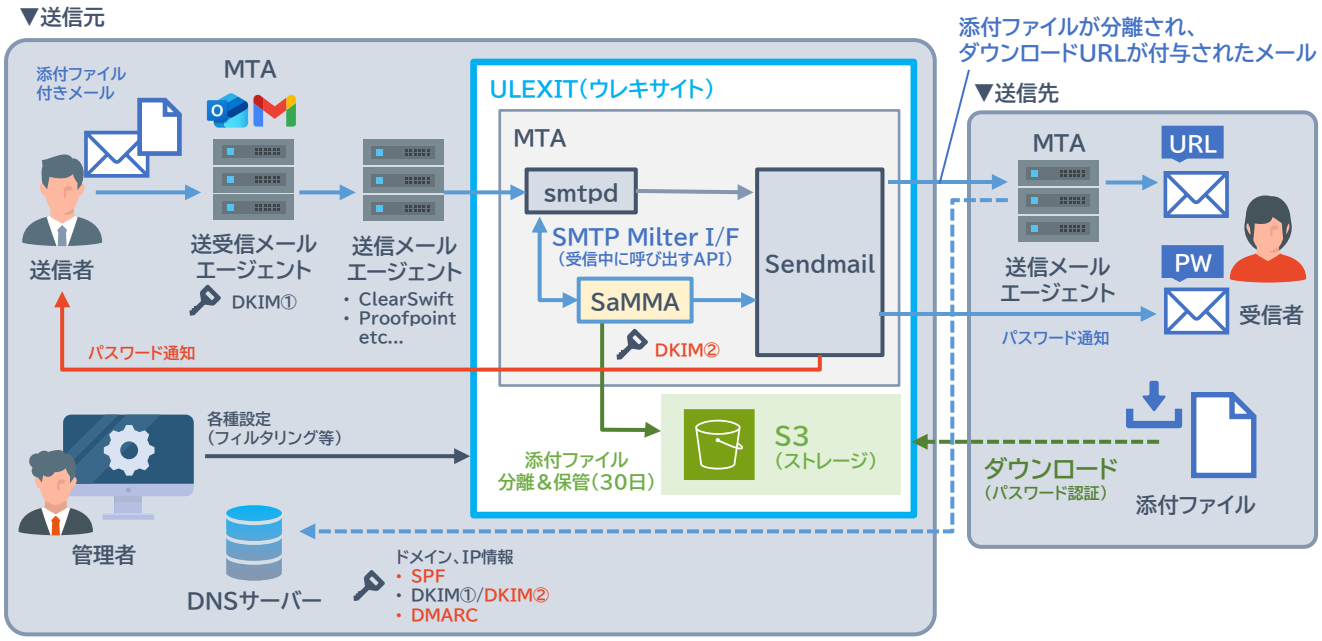
高セキュリティ＆柔軟な環境を用意

送信者が添付ファイルの取り消しができるため誤送信の対策も可能。
ULEXITをプラットフォームとし、将来的な拡張性や、お客様の要望に合わせたアップグレードを検討中。



おすすめ

ULEXITE システム全体像



導入メリット

- システム管理者の設定作業のみ、ユーザー側での設定は一切不要
- クラウドサービスとして提供

参考価格

※2025年5月時点

項目	提供形態	課金単位	購入単位	定価
月額ライセンス	クラウド	お問い合わせください		
年間ライセンス	クラウド	お問い合わせください		

動作環境

主なサポート対象メールクライアント

- Outlook (M365)
- Gmail (Google Workspace)

添付ファイルダウンロード・削除画面

OS バージョン	Windows 10 Windows 11
ブラウザ	Google Chrome 最新バージョン

お問い合わせはこちらから：https://www.fsi.co.jp/solution/ulexit/

IoT機器向けファジングツール

Raven for Fuzzing

レイブン フォー ファジング

簡単操作でIoT機器のファジングテストが可能！

01 広範囲のプロトコルを標準サポート

膨大な検査パターンを短時間で実施

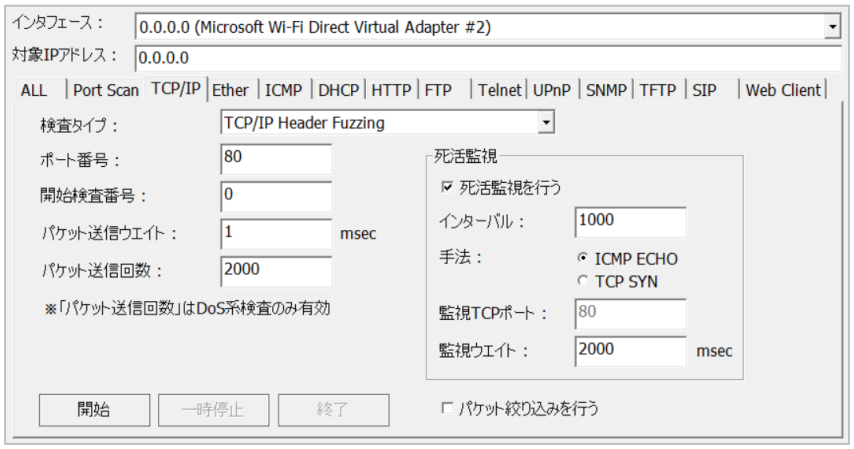
ブロードバンドルーター、ネットワーク機器、情報家電、モバイル機器などの組込み機器に既に大量の未知のセキュリティ脆弱性を発見。数百万の検査パターンを数時間で実施可能。

7層:アプリケーション層	DHCP Fuzzing, HTTP, FTP, Telnet, UPnP, SNMP, TFTP, SIP
6層:プレゼンテーション層	
5層:セッション層	
4層:トランスポート層	TCP Header Fuzzing, UDP Header Fuzzing, TCP/IP Option Fuzzing, SYN Flood DoS, Land Attack DoS
3層:ネットワーク層	ICMP Fuzzing, ICMP Ping of Death, ICMP Code/Type Fuzzing, IP Option Fuzzing (ICMP ECHO REQUEST, ICMP UNREACH HOST), IP Option Fuzzing (UDP), ARP Fuzzing, ARP DoS, IPv6, ICMPv6, DHCPv6
2層:データリンク層	Ether Type Fuzzing, Ether Unuke DoS

02 日本語UIによる簡単操作で高性能ファジングテストを実現

国産ならではの日本語対応＆簡単操作

日本語UIにより、直感的な操作が可能。検査パケット送出インタフェースの選択や検査対象機器のIPアドレスなど試験項目選択の簡単3ステップで実施可能。また、送信パケットの詳細や検査アルゴリズムまで記載した日本語マニュアルが付属。



03 国産DNAによる開発

世界クラスのセキュリティエキスパートが開発

Raven for Fuzzingは、国内外におけるセキュリティ脆弱性発見手法・脅威分析手法に関する多数の研究発表の実績を持つセキュリティ・エキスパートが開発。研究開発は国内で完結。

経産省、IPAのファジングの手引き書に掲載

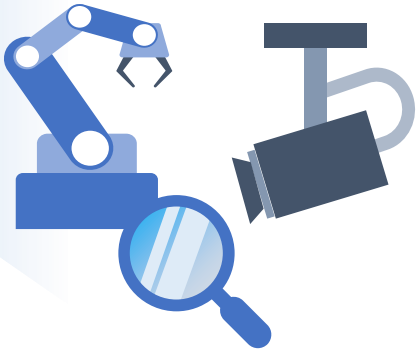
経産省の『機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き』に掲載されている
ファジングツール。
IPAの『ファジング活用の手引』に掲載されているファジングツール。

おすすめ

Raven for Fuzzing 接続構成

検査PC

監査対象



導入メリット

- 機器とネットワークの直接接続のみ
- 簡単操作でネットワーク機器をファジング検査

参考価格

※2025年5月時点

項目	提供形態	課金単位	定価
月額ライセンス	ダウンロード	インストール台数 （1ライセンス3台まで可能）	¥500,000
年間ライセンス	ダウンロード	お問い合わせください	¥5,000,000
検査代行	検査結果報告書	検査内容による	要問合せ

動作環境

環境	以下のOSの動作環境に準ずる Windows10 Windows11
備考	※ 実行には管理者権限が必要です。 ※ 動作に以下のインストールが必要となります。 • VisualStudio2019ランタイムモジュール • WinPcap(4.1.3) ※ インストール時にはインターネット接続が必要となります。 ※ アプリ実行時にはインターネット接続は必要ありません。 ※ ローカルホストに対する検査はできません。 ※ アプリケーションのインストール環境によりファンシング用パケットを生成することができない場合、正常に動作しない可能性があります。 ※ VPNクライアントや仮想のネットワーク・デバイス等がインストールされている環境や機器に直接接続して検査を実行できない環境では、正常に動作しない可能性があります。 ※ 上記条件を満たせばノートPCなどの低リソース機器でも動作可能となります。

お問い合わせはこちらから：https://www.fsi.co.jp/project/s/raven.html

脆弱性診断サービス

IoT脆弱性診断

セキュリティ×IoTのエキスパートによるセキュリティ診断

01 エキスパートエンジニアによるオーダーメイド診断

業界トップクラスの有資格者数

サイバーセキュリティの国家資格である情報処理安全確保支援士の有資格者が多数在籍。CISSPなどの国際資格や産業サイバー、ネットワークのような特化資格保持者を交えたエキスパートエンジニアが最適の診断プランを作成します。

※2024年9月時点の人数

資格	人数
CISSP	9名
産業サイバーセキュリティエキスパート	3名
情報処理安全確保支援士	305名
ネットワークスペシャリスト	45名
エンベデッドシステムスペシャリスト	43名

02 業界ガイドラインや規格への対応

認証機関や所管官庁に提示可能な品質水準

セキュリティ対策は実施だけでなく、実施内容及びその有効性を内外に適切に提示することもまた重要です。診断対象やお客様の業界に求められる業界ガイドラインや規格に適合する形態で診断を計画し、診断報告書を適合のエビデンスとして使用できる品質に作成します。

経済産業省 Ministry of Economy, Trade and Industry
機器のサイバーセキュリティ確保のためのセキュリティ検証の手引

IEC
IEC 62443 4-2

JIS
JIS T 81001-5-1

EU Cyber Resilience Act 他

03 あらゆるシステム・製品に対応できる多様な診断手法

クラウド、機器、ネットワーク、USB、Bluetooth、内部基板など、様々な診断対象、インターフェースに対する診断手法を保有しています。

Bluetooth診断

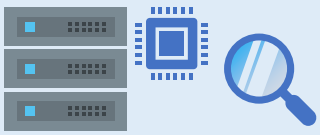
Bluetoothの無線通信経由の侵入可否や盗聴による情報窃取の可能性を検証。

ファームウェア診断

機器の内蔵ソフトウェアに起因する脆弱性の有無を確認。

ハードウェア診断

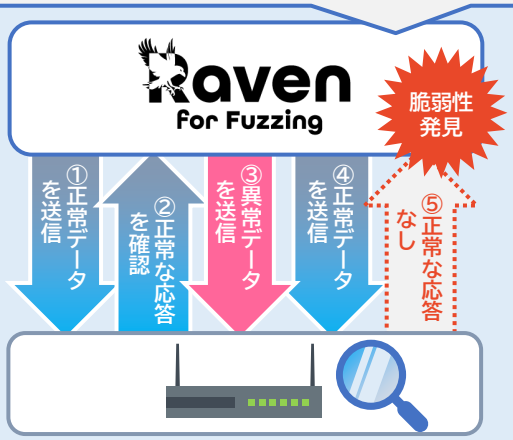
機器本体や内部基板を活用した侵入や情報窃取の可否を検証。



ネットワーク診断

Raven for Fuzzingを使用したファジングをはじめ、ネットワーク上からの攻撃手法や脆弱性の有無を検証する。

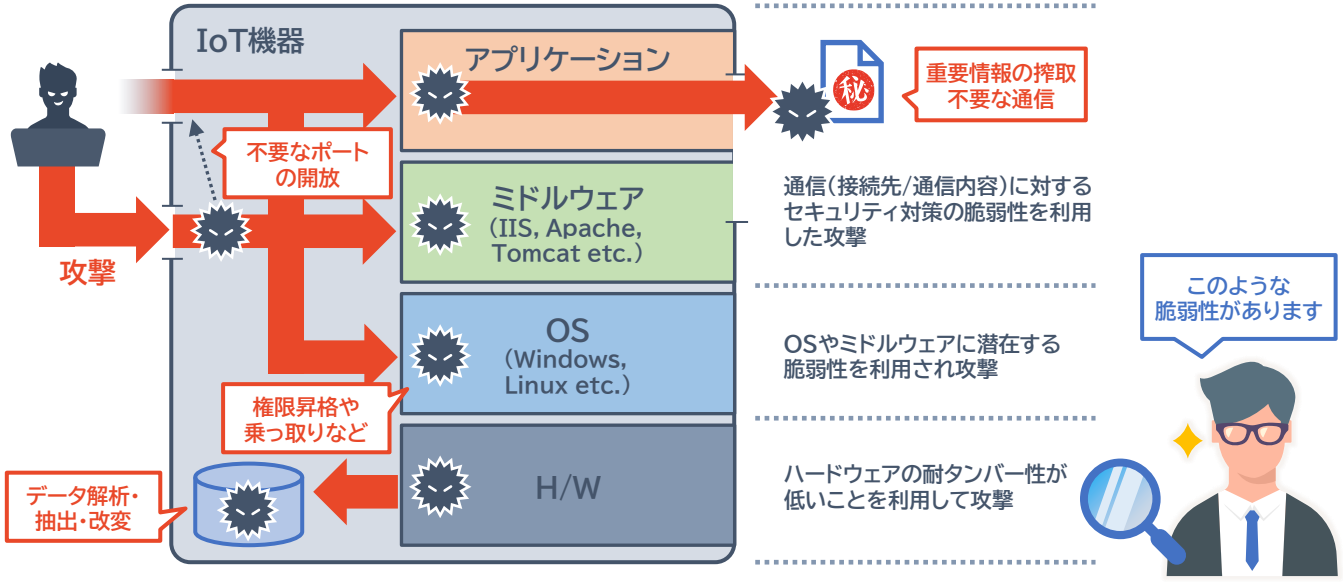
異常データ生成パターン
- 整数オーバーフロー
- バッファ・オーバーフロー
- Off by one
- 境界値未チェック
- 異常フラグ
- サービス妨害攻撃
- リソース異常消費
- …



おすすめ

IoT脆弱性診断

…脆弱性が混在(※イメージ)



導入メリット

セキュリティスペシャリストによる、機器解析、脆弱性スキャン、疑似サイバー攻撃により、機器に潜む脆弱性を発見、報告。

参考価格

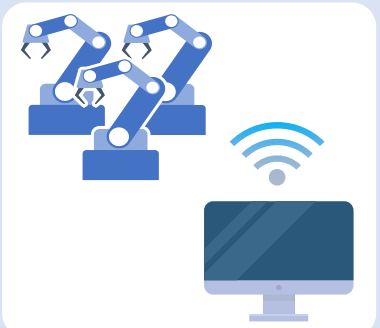
項目	提供形態	サービス単位	定価
IoT脆弱性診断	受託	1機種・1システムより	お問い合わせください

求められるIoT機器の適合規格に準拠した診断を実施

医療機器

- JIS T81001-5-1(IEC 81001-5-1)に適合した試験メニュー(日本市場向け)
- FDAガイダンスの「V. C. Cybersecurity Testing a.～d.」(米国市場向け)

制御機器



IEC62443 4-1(9.4 SVV-3:脆弱性テスト)に適合した試験メニュー

その他

経済産業省の手引き・ガイドライン『機器のサイバーセキュリティ確保のためのセキュリティ検証手引き』に基づいた試験メニュー

お問い合わせはこちらから: https://www.fsi.co.jp/project/s/back-door.html

CRA対応支援サービス

サイバーレジリエンス法対応支援

変化するEU情勢(欧州サイバーレジリエンス法(CRA))への対応

01 コンサルティングサービス

サイバーレジリエンス法に関わるセキュリティリスクの確認や対策の検討から支援

サイバーレジリエンス法における最初の課題からCRA認証取得までお客様のCRA認証取得対応を全面的に支援。

課題

- CRA準拠するために何から始めればいいのか分からない。
- 現状の対策でどれだけ準拠できているのか確認したい。

コンサルティングサービス

要求事項の整理、現状の分析、要対尾王事項の洗い出しなどを行います。

- 要求事項の整理
- 現状分析
- 要対応事項の抽出

02 リスクアセスメントサービス

サイバーレジリエンス法に特化したリスクアセスメントを実施

対象機器を守るため、システム構成を明確化し、想定されるサイバー攻撃の脅威分析、対策手法を顧客に合わせて提案。

課題

サイバー攻撃の動向を踏まえたセキュリティリスクの確認や対策の検討を行いたい。

リスクアセスメントサービス

サイバーセキュリティに特化したリスクアセスメントを行います。

- 脅威分析
- リスクアセスメント
- リスクコントロール手段の検討、評価

03 脆弱性診断サービスや脆弱性情報監視サービスも提供

対象機器の脆弱性診断や運用後の脆弱性監視にも対応

脆弱性診断を実施し、既知の脆弱性やセキュリティのさまざまな観点での検査を実施するサービス、SBOMで管理するソフトウェアに対して、定期的に脆弱性を監視し、最新の脆弱性を発見した際に通知するサービスも提供。

課題

システムを構成するソフトウェアに存在する脆弱性を確認したい。

脆弱性診断サービス

システムの構成要素を解析し、既知の脆弱性情報の収集・評価を行います。

- 既知の脆弱性検査
- ファジングテスト
- ネットワークスキャン
- 通信解析
- パケット検証
- ポートスキャン

課題

最新のセキュリティ脆弱性情報を定期的に確認する運用を行いたい。

脆弱性情報監視サービス

SBOMで管理するソフトウェアに対して定期的に脆弱性情報を監視し、最新の脆弱性を発見した際に通知します。

- 脆弱性情報の定期チェック
- 脆弱性情報の通知

おすすめ

EUサイバーレジリエンス法(EU Cyber Resilience Act)とは？

デジタル要素を含む製品に対して、製品ライフサイクルを通じて遵守すべきサイバーセキュリティの必須要件に対応することを目的とした法令が施行されます。
※2027年後半の適用予定

＼ ほとんどのデジタル製品が対象 ／

※医療機器、航空機、自動車、軍事機器は対象外

サイバーレジリエンス法に準拠できないと…

EU圏での販売不可

罰金制度あり

※最高1,500万ユーロまたは全世界の年間売上高2.5%(いずれか高い方)の罰金

富士ソフトなら…

CRA準拠するための
コンサルティング
をいたします！

導入メリット

- サイバーレジリエンス法についてのご説明から対応。
- リスクアセスメントだけでなく、脆弱性診断や脆弱性監視など、実機での試験や運用にかかわるサービスまで、ワンストップで提供

参考価格

※2025年5月時点

項目	提供形態	定価
コンサルティング	サービス	内容によるため、ご相談ください
リスクアセスメント	サービス	内容によるため、ご相談ください
脆弱性診断サービス	サービス	脆弱性診断内容によるため、ご相談ください
脆弱性監視サービス	サービス	サービス内容によるため、ご相談ください

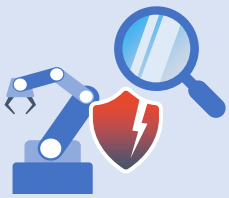
お客様の対応状況に応じた適切なサービスメニューをご提案

CRA準拠するために必要な作業を明らかにしたい要対応事項を整理したい

→ コンサルティングサービス

セキュリティリスク確認・対策がしたい

→ リスクアセスメントサービス



ソフトウェアの脆弱性を確認したい

→ 脆弱性診断サービス

最新の脆弱性を定期的に確認したい

→ 脆弱性情報監視サービス

お問い合わせはこちらから：https://www.fsi.co.jp/solution/cyber_resilience/

SOCサービス

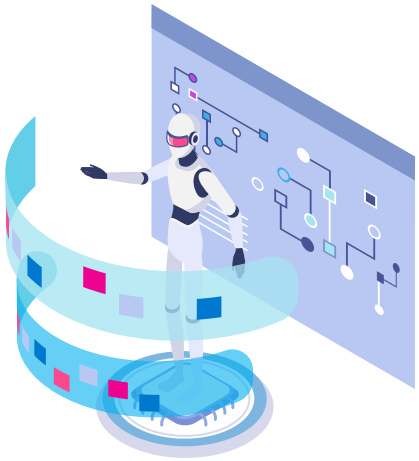
SOC（Security Operation Center）

サイバー攻撃の検出・分析、対応策アドバイスを行う専門組織

01 AIによる監視

全ネットワークの挙動と各種セキュリティ対策製品の挙動を監視

AIを活用して全ネットワークの挙動と各種セキュリティ対策製品の挙動を監視、脅威候補を絞り込み。
AIが抽出した脅威候補の通信イベントやアラートはそのまま通知せず、経験豊富なアナリストが多角的に分析。
想定される脅威内容を具体的な解説つきで報告し、対処要否の判断が容易に。



02 専門技術者による分析

無駄な通知を排除

AIが絞り込んだ脅威候補リストをセキュリティアナリストが分析し、無駄な通知を排除。ネットワーク上の通信イベントをAIとアナリストが絞り込み、真の脅威疑惑のある事象にのみフォーカスして報告。
過検知や誤検知の切り分け不要で、対処業務に専念可能。

03 わかりやすい対策提示

担当アナリストと直接相談可能

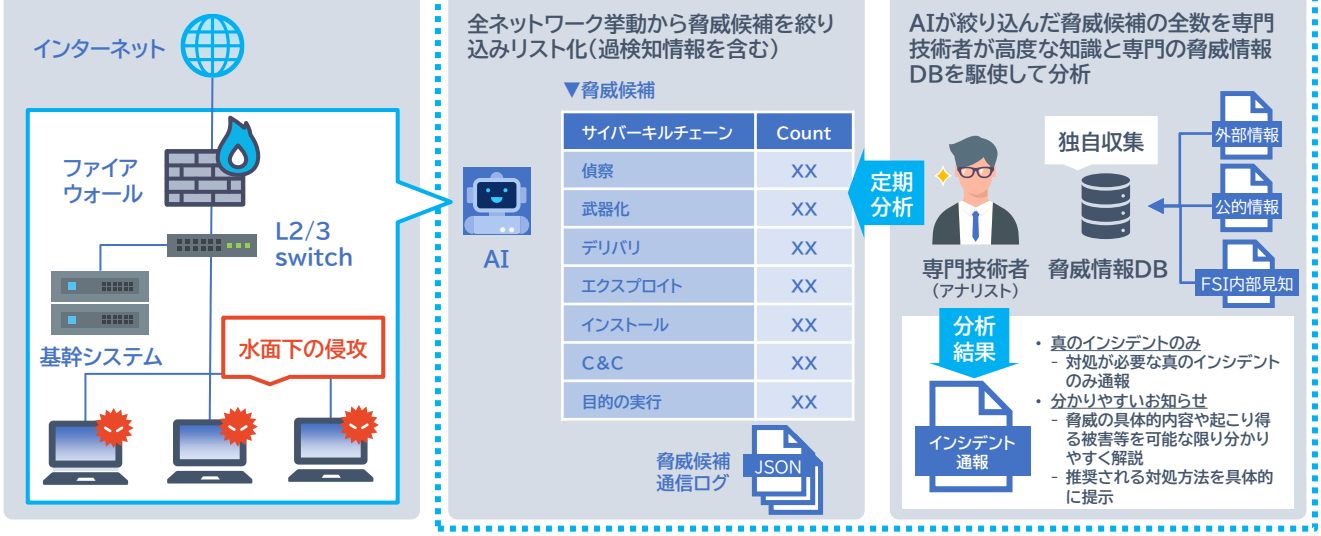
インシデントや脅威、対応策について、アナリストがお客様の立場で具体的に解説。
報告内容に関する質問は、カスタマーポータルでアナリストと直接やり取り。
調査依頼や相談も含めて定額制（時間制）で利用可能。身近なアドバイザーとして気軽に活用可能。

セキュリティ専門家の伴走支援

セキュリティ対策は導入だけでは終わりません。セキュリティの監視結果から、定期的な改善提案や、対策の長期計画策定支援等、お客様と弊社セキュリティ専門家が一緒に、お客様のビジネスを守り継続的に高める伴走型のセキュリティを提供させて頂きます。

おすすめ

富士ソフトSOC概要



導入メリット

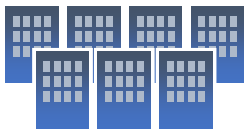
- ネットワークセンサーを設置し、包括的にデータを収集。
- AIが脅威となる候補を絞り込み、アナリストが分析。
- 必要なインシデントのみを報告し、推奨する対処方法を提示。

参考価格

項目	提供形態	条件	定価
SOCサービス	サービス	お客様IT環境の監視範囲や規模による	要相談

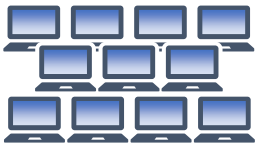
まかせて安心！セキュリティ監視にかかわる豊富な実績

セキュリティ監視運用 80社以上の導入実績



標的型攻撃対策として、2015年から実施している、セキュリティ運用実績に支えられる技術と、最新のAI監視技術の導入で、国内製造業、及び、サービス業を中心に、80社以上への導入実績があります。

約3万台と 大規模な運用実績



最大国内42拠点・約3万規模のセキュリティ監視を運用している実績があります。規模が大きく、複数の拠点があるお客様に、安心してセキュリティ監視をお任せ頂ける運用ノウハウがあり、日々の実践にて専門技術者のスキルの研鑽に努めています。

セキュリティ対策・運用 の研究は15年以上

データセンター運営で培った情報セキュリティマネジメントシステム(ISMS)運営技術をはじめ、クラウドを利用した民間、官庁の様々なお客様のシステム開発等で培ったセキュリティ対策技術等、セキュリティ研究は、“15年”以上の実績があります。

SSSマーク取得

023-0011-40

弊社セキュリティ監視サービスは、経済産業省(METI)の定める「情報セキュリティサービス基準*1」に適合したサービスとして、「情報セキュリティサービス基準適合サービスリスト*2」へ登録されています。

*1 経済産業省（METI）「情報セキュリティサービス基準」
*2 独立行政法人情報処理推進機構（IPA）「情報セキュリティサービス基準適合サービスリスト」

お問い合わせはこちらから：https://www.fsi.co.jp/project/s/soc.html

セキュリティ監視

総合セキュリティ監視サービス

監視対象を選ばず隠れた脅威を見つけ出すセキュリティ監視サービス

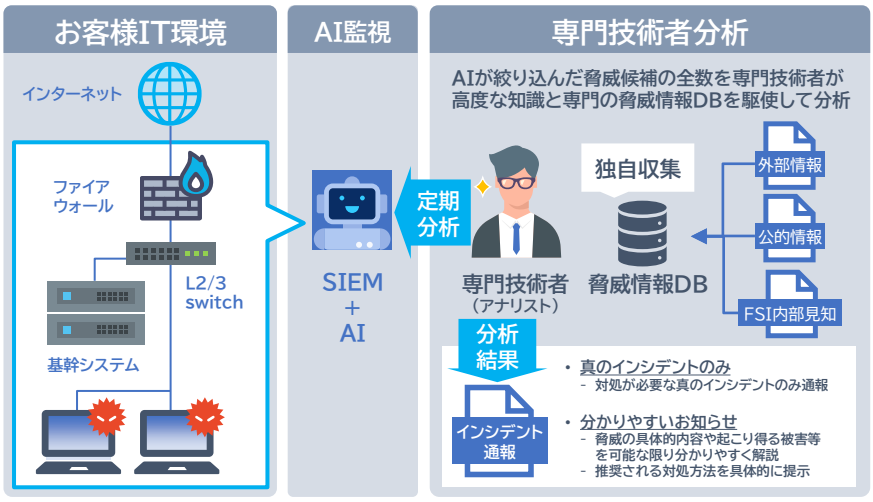
01 総合監視で隠れた脅威も検知

監視対象のログをAIを搭載したSIEMに集約して分析

個々のセキュリティ対策では検知できなかった隠れた脅威を、複数のセキュリティ対策を総合的に監視することで見つけ出します。

ネットワークのセキュリティ対策（NDR）を標準提供

本サービスは、標準でネットワークを監視/脅威を検知するNDRを提供。お客様のセキュリティ対策がEDRやUTMのみ等、単体あっても多層防御を実現し、隠れた脅威を見つけ出します。



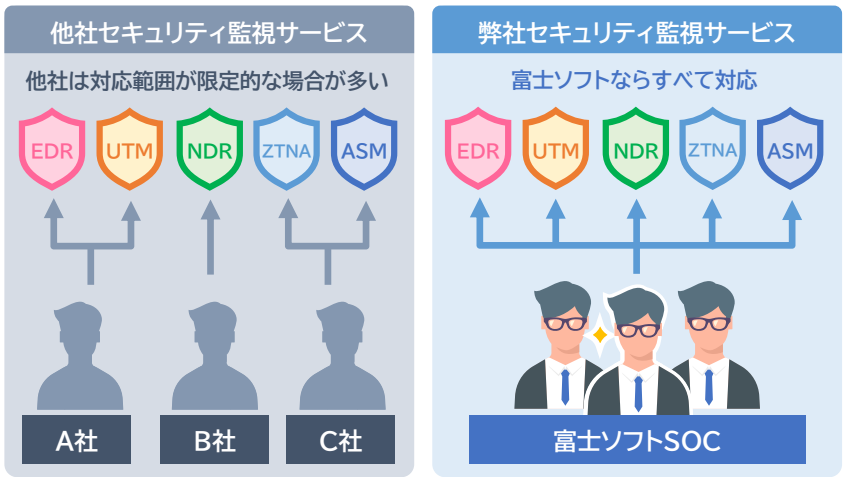
02 お客様のご要望や環境に応じた柔軟なカスタマイズ性

多様なセキュリティ機器や様々な形式のシステムにも柔軟に対応

他社サービスは、特定のセキュリティ機器に限定していることが多く、複数の監視サービスを利用する必要がありますが、本サービスは、多様なセキュリティ機器や様々な形式のシステムにも柔軟に対応し限定しないセキュリティ監視を提供します。

無駄なコストが無いセキュリティ監視

導入済みセキュリティ対策利用や成長に合わせた監視対象の追加が可能で、無駄なコストが無いセキュリティ監視を提供します。



03 攻撃の可能性と対策をわかりやすく提示

脅威の具体的な内容や起こり得る危険を分かりやすくお知らせ

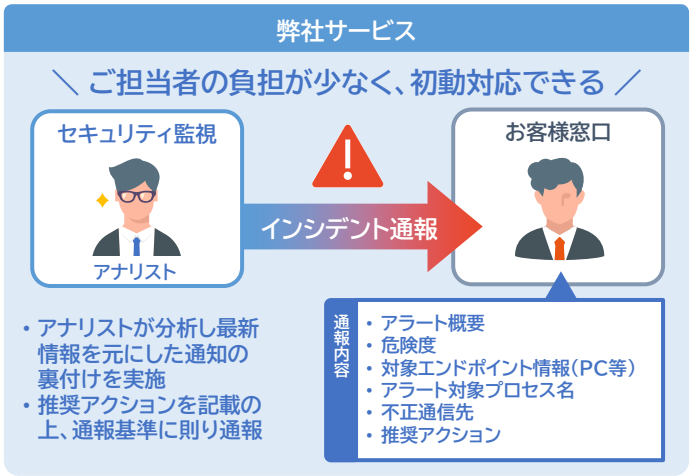
わかりやすくお知らせすることにより、お客様の判断力の向上。

AIとアナリストによるインシデント分析により真の脅威の存在が疑われる事象に絞り込み通報

真の脅威の存在が疑われる事象に絞り込むことにより、お客様の集中力の向上。

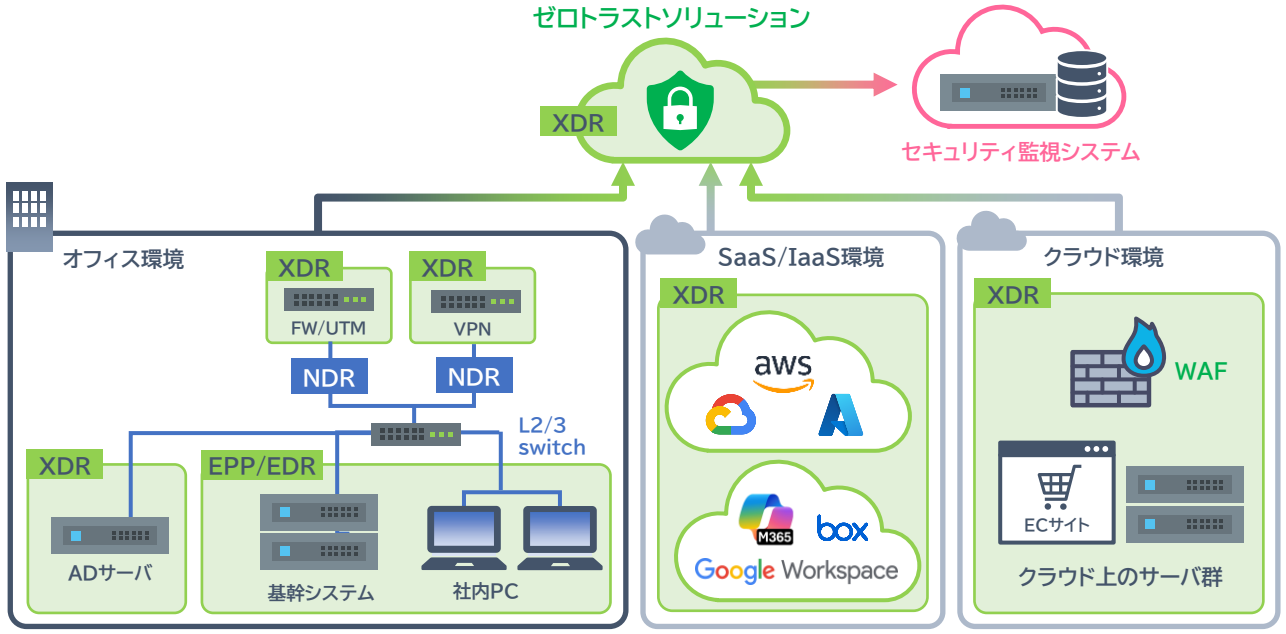
推奨される対処方法を、通報に記載

初動対応として推奨される対処方法を通報内容に記載することにより、お客様の初動対応力の向上。



おすすめ

監視対象の製品を選ばない総合セキュリティ監視



導入メリット

- ネットワークのデータを取得し、監視/脅威検知するNDRを標準提供
- 企業のIT環境も商用のWebサービス環境も、まとめてセキュリティ監視が可能
- 様々なセキュリティ製品をまとめて監視するため、お客様の運用を軽減します

参考価格

※2025年5月時点

項目	提供形態	条件	定価
総合セキュリティ監視サービス	サービス	お客様IT環境の監視範囲や規模による	要相談

脅威通報から脅威対応までのサービスを提供

基本サービス

脅威通報

各種セキュリティ製品のアラートをアナリストが分析し、その結果と初動対応方法を含め、分かりやすくお知らせ。

設定/チューニング

各種セキュリティ製品の設定と過検知/誤検知に対するチューニングを実施。

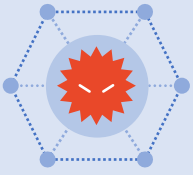
専用ポータルサイト

お客様とのコミュニケーションや各種対応ステータスを一元管理できる専用ポータルをご提供。

月次レポート

監視/分析実施状況(実績集計、脅威動向等)を、翌月に報告書化しご提供。

付加サービス



封じ込め支援

EDR機能を利用して遠隔にて、ネットワーク隔離を予め取り決めた規定に則り実施。

セキュリティ健康診断

収集した情報を元に、AIとアナリストで分析し、お客様セキュリティ状況を見える化し報告。

脅威除去支援
(オプション)

EDR機能を利用してマルウェアの駆除等、エンドポイント上の脅威の除去作業を支援。

再発防止支援
(オプション)

EDRやFW/UTM機能を利用した、同様の攻撃を抑止するための対策作業を支援。

お問い合わせはこちらから：https://www.fsi.co.jp/project/s/soc.html

Webサイト/アプリに特化して監視/分析/対応

WEBセキュリティ監視サービス

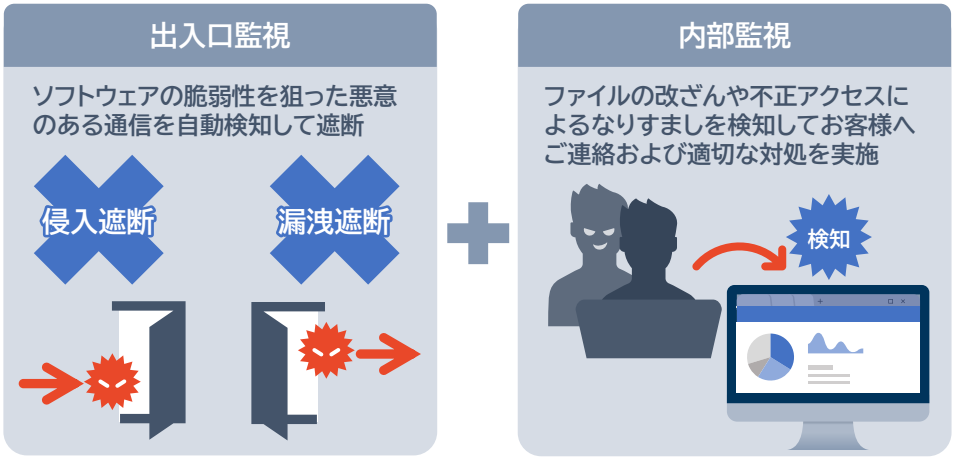
お客様のWebサイトやWebアプリ環境に、ピッタリの安心を。

01 企業の信頼とビジネスの継続性を守る「出入口監視」と「内部監視」

経験豊富なSOCアナリストが「出入口監視」と「内部監視」で機密情報を保護

■出入口監視：
外部からの悪性な通信をお客様システムへ通信が届く前に遮断することで被害を未然に防止。

■内部監視：
弊社に所属する経験豊富なSOCアナリストが詳細に分析・調査したのち、適切な対応を実施



02 お客様のご要望や環境に応じた柔軟なカスタマイズ性

統合的な脅威の可視化

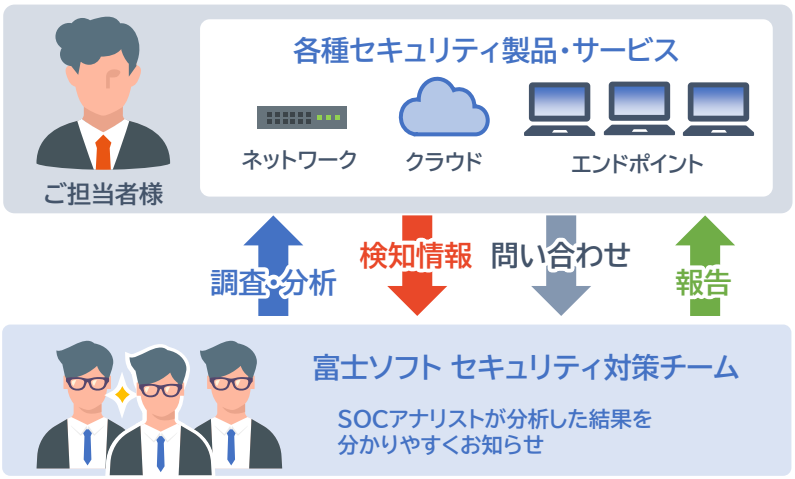
既存のセキュリティ対策で対応できない範囲まで脅威を監視。統合的な脅威の可視化が可能。

拡張可能な監視範囲

必要なログだけ取り込むことで、コスト削減。
将来的にお客様のビジネスの拡大に合わせてセキュリティ監視の範囲を拡張可能。

お客様に合わせたセキュリティ製品の選定

脅威通報や封じ込め支援など自由に組み合わせることができる高いカスタマイズ性。



03 経験豊富なSOCアナリストによる分析・対応

導入サポートから運用を行う監視サービスを提供

対処が必要な脅威を分かりやすくお知らせ。
ご担当者様の負担を少なくし、迅速な初動対応が可能。

おすすめ

標準提供機能のみでは足りないセキュリティも保護

クラウド提供セキュリティ保護機能

AWS、Azure等のクラウド標準提供のセキュリティ保護機能での監視

サードパーティ製セキュリティ製品

クラウド標準提供機能で不足を感じる場合やオンプレ環境の場合に、セキュリティ保護をサードパーティ製品を導入

導入メリット

- AWS、Azure等のクラウド標準提供のセキュリティ保護機能のみの監視も可能
- クラウド標準提供機能に不足を感じるお客様には、弊社専門家が必要な対策をご提案し、導入から監視までを実施し、標準提供機能と合わせて総合的に監視します。

参考価格

※2025年5月時点

項目	提供形態	条件	定価
Webセキュリティ監視サービス	サービス	お客様IT環境の監視範囲や規模による	要相談

Webアプリケーションに対する攻撃一覧

脅威分類	脅威概要	想定脅威	攻撃種類
なりすまし	ユーザ名やパスワード等、他のユーザの認証情報に対して不正にアクセスしたのち悪用する行為	Webアプリケーションへの不正ログイン	・Webアプリケーションの脆弱性を悪用する攻撃 ・アカウントリスト攻撃 ・辞書攻撃 ・総当たり攻撃 ・コンピュータウイルス（マルウェア）への感染
改ざん	悪意のあるデータの変更・追加・削除 等	Webコンテンツの改ざん	・Webアプリケーションの脆弱性を悪用する攻撃 ・管理者アカウントの乗っ取りによる攻撃 ・内部不正 ・コンピュータウイルス（マルウェア）への感染
否認	反証できる関係者がいない状況下で、ユーザによるアクションの実行を否定するもの	Webサーバでの不正操作の否認	・Webアプリケーションの脆弱性を悪用する攻撃 ・管理者アカウントの乗っ取りによる攻撃 ・内部不正 ・コンピュータウイルス（マルウェア）への感染
情報漏えい	情報へのアクセスが想定されていないユーザへの情報の暴露 等	Webアプリケーション経由の情報漏えい	・Webアプリケーションの脆弱性を悪用する攻撃 ・管理者アカウントの乗っ取りによる攻撃 ・内部不正 ・コンピュータウイルス（マルウェア）への感染
サービス拒否	DoS/DDoS攻撃により、サービスの利用が許可されているユーザによるアクションが拒否されるもの	アプリケーション層で行われる攻撃	・Webアプリケーションの脆弱性を悪用する攻撃
		NW、トランスポート層で行われる攻撃	・SYN、ACK、UDPフラッド攻撃
		不正なマイニングによる高負荷攻撃	・コンピュータウイルス（マルウェア）への感染
権限の昇格	特権のないユーザが特権的なアクセスを取得すると、システム全体を侵害したり破壊したりできるようになるもの	Webアプリケーションの権限昇格	・Webアプリケーションの脆弱性を悪用する攻撃 ・コンピュータウイルス（マルウェア）への感染

お問い合わせはこちらから：https://www.fsi.co.jp/project/s/soc.html

米国政府機関のセキュリティガイドライン準拠サポート

NIST-SP800-171準拠支援サービス

NIST-SP800準拠の答えはここに。

01 豊富な経験とノウハウを結集したコンサルティングサービス

準拠までの対策からその後のサポートまで一気通貫したコンサルティングサービス

蓄積してきたノウハウと富士ソフトが策定した独自の標準化フレームワークを活用。お客さまに寄り添った伴走支援を実施。

事前確認 → ヒアリング項目準備 → ヒアリング → 分析・評価 → ツール検証（オプション） → 結果報告 → 対策支援

02 NIST SP800-171準拠状況を見える化し、対策の提案

リスクを可視化し提対策の導入と改善策を提示

既存のセキュリティガイドラインやNIST SP800-171で対策をすべき項目を照合・精査し、比較検討

分類	項目	タイトル	概要
ガバナンス	3.2	意識向上と訓練	セキュリティポリシーの遵守
	3.11	リスク評価	情報資産のリスクを適切に評価
	3.12	セキュリティ評価	セキュリティ管理策を定期的に評価
セキュリティ対策の導入と運用	3.1	アクセス制御	システムへアクセスできる人/機器を制限
	3.4	構成管理	システム構成機器に求められるセキュリティ構成設定を確立
	3.5	識別と認証	システム利用者、デバイスを識別
	3.7	メンテナンス	組織のシステムのメンテナンス
	3.8	記憶媒体の保護	機密情報をセキュアに格納しアクセスできるものを制御
	3.10	物理的保護	組織のシステム、装置等への物理的アクセスを制限
	3.13	システムと通信の保護	システムの通信の監視、制御、保護
	3.14	システムと情報の完全性	脆弱性情報の収集、監視、パッチ適用など通しタイムリーにシステムと情報の完全性を担保
管理体制	3.6	インシデント対応	インシデントの追跡、報告
	3.9	要因のセキュリティ	システムへのアクセスを行う個人を審査
評価	3.3	評価と説明責任	システムの評価を行い責任の追及

NIST SP800-171の要件概要▸

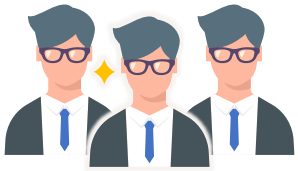
03 要件解釈から準拠状況の確認・対策実行までを伴走型の支援を実施

セキュリティポリシーに取り入れられるよう各種規定の策定・訂正支援も実施

NIST SP800-171 対策分野も幅広く提案し、ガイドラインを網羅的に対策できるよう支援します。

＼ ガイドラインをベースに対策状況を評価 ／

富士ソフト セキュリティ専門チーム



NIST SP800-171
14ファミリ(110項目)の
セキュリティ要求事項

- システム自身に対しセキュリティ技術を使う管理策
- 組織に対し適用
- システム環境に対し施す物理的管理策
- 個人に関し適用する管理策

おすすめ

現状課題の把握から対策ロードマップまでご提案

	お客様	富士ソフト
現状課題の把握	保護すべき重要情報を検出し、選定します。 お客様の環境下で、重要情報の秘匿性を保証する要件を特定します。	
	ヒアリングシートのご記入	計画策定にともない、必要な対策の実施に向けて セキュリティ専門チームによる伴走支援を行います。
対策状況の見える化	お客様が保有している情報のセキュリティに関する現状分析ドラフト案およびその解説状況と NIST SP800-171に対策するべき項目を自動検知・解説し、比較検討します。	
	お客様の現在の環境下のリスク分析を行ない、それらのリスクを明確化します。 同時に外部の導出と改善策を提示します。	
ロードマップ作製	お客様の環境下において適正な対策を選定できる ロードマップを策定いたします。	
	アセスメント結果を報告書にて提出します。	

導入メリット

- セキュリティ専門家チームが作成したロードマップを用いて情報管理の現状分析可能
- セキュリティ対策が実行完了するまで、ワンストップで支援
- NIST SP800-171準拠による事業機会の拡大

参考価格

※2025年5月時点

項目	提供形態	条件	定価
NIST SP800-171準拠支援	サービス	支援内容による	要相談

現状課題の見える化からリスク対策まで、伴走支援する各種サービスを提供

標準サービス

重要情報の定義

企業間やサプライチェーンで保護すべき重要情報を特定し定義。お客様の環境下で重要情報の機密性を保護する要件を特定。例えば重要情報を処理、格納、伝送、それらを扱う全構成要素の特定など。

現状の見える化

お客様が保持している既存のセキュリティに関する規程やガイドラインおよびその対策状況とNIST SP800-171に対する対策をすべき項目を照合・精査し比較検討。

リスクの可視化

比較検討結果からお客様の現在の環境下でのリスク分析を行ない、リスクを可視化。同時にリスクの可視化で見える対策を導出し把握し、改善方法を提案。

ロードマップ策定

可視化されたリスクの対策要件とそれらを改善する方法を精査し、お客様の環境下において最適に対策を完遂できるロードマップを策定。

オプションサービス

伴走支援

計画策定に基づき必要な対策の完遂に向けてセキュリティ専門家チームによる伴走支援。専門家チームを構成しお客様に寄り添った伴走支援を行う。

システム構築支援

システム的な対策による準備を目指すお客様へのシステム構築支援。NIST SP800-171準拠実現のためにお客様環境下に最適な構成・システムの選定をご支援。

システム導入支援

左記で定義したNIST SP800-171準拠に必要な特権アクセス管理、構成管理、ウィルス対策、通信周り要件実現のためのゼロトラストアーキテクチャの導入支援。

ポリシー策定支援

NIST SP800-171が扱う5つのセキュリティフレームワーク(特定、防御、検知、対応、復旧)を効果的にお客様のセキュリティポリシーに取り入れるため各規程の策定・改訂をご支援。

お問い合わせはこちらから：https://www.fsi.co.jp/project/s/security-assessment.html

脆弱性診断サービス

Webアプリケーション診断/プラットフォーム診断

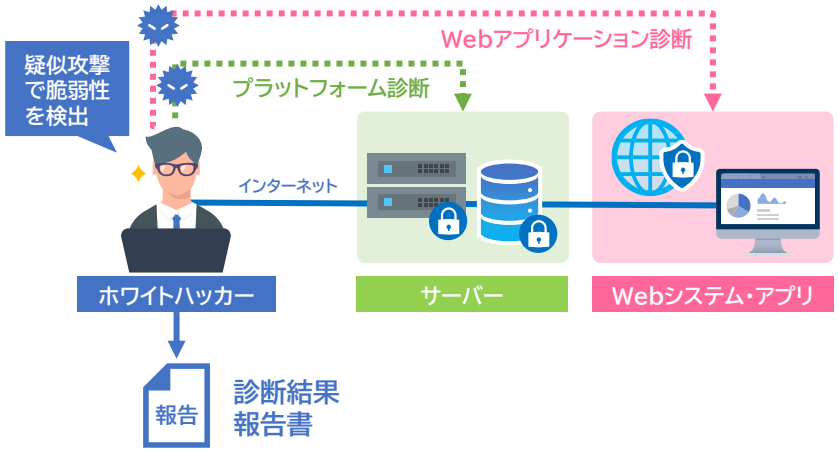
未来のリスクを今、解決！脆弱性診断で安全な明日を

01 高レベルな脆弱性診断サービスを提供

ツールと手動オペレーションによる検査を併用

セキュリティエンジニアがツールによる検査と手動オペレーションによる検査を併用し、精度の高い診断サービスを提供。
診断ツール主体では実現できない、高レベルの網羅性と検出精度を備えた診断を実現。

*【網羅性】診断項目に抜けやモレがないこと。
*【検出精度】脆弱性の検出数や検出内容の精度が高いこと



02 セキュリティスキル(ITSS レベル4)※

ISMSをベースとした高品質なスキーム

セキュリティ診断を行うエンジニアは、EC-Council セキュリティエンジニア養成講座のCEH(Certified Ethical Hacker)資格を保有し、高度なセキュリティ診断を実施。
セキュリティの認証規格であるISMSを取得し、ISMSをベースとしたスキームで診断対象情報や診断結果を厳重に管理。品質においては、個々の力量に依存せず、チームとして常に高品質の診断を提供するためのスキームを構築。

※ ITSSキャリアフレームワークと認定試験・資格の関係
(ISV Map Ver12.4)

＼診断エンジニアは全員資格取得者 ／

C|EH Certified Ethical Hacker

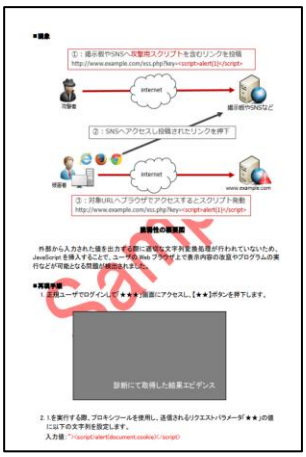
CEH(Cetified Ethical Hacker)

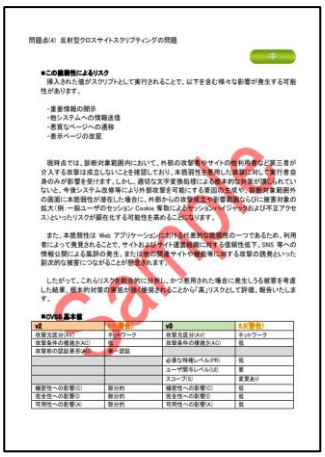
EC-Council(米国)が提供するセキュリティエンジニア向けコースウェア。
世界で有名な資格の一つで最新の攻撃手法を習得し、ハッキング技術の知識やテクニックを熟知出来るトレーニングと認定資格を受けています。

03 理解しやすい報告書

質の高い報告書

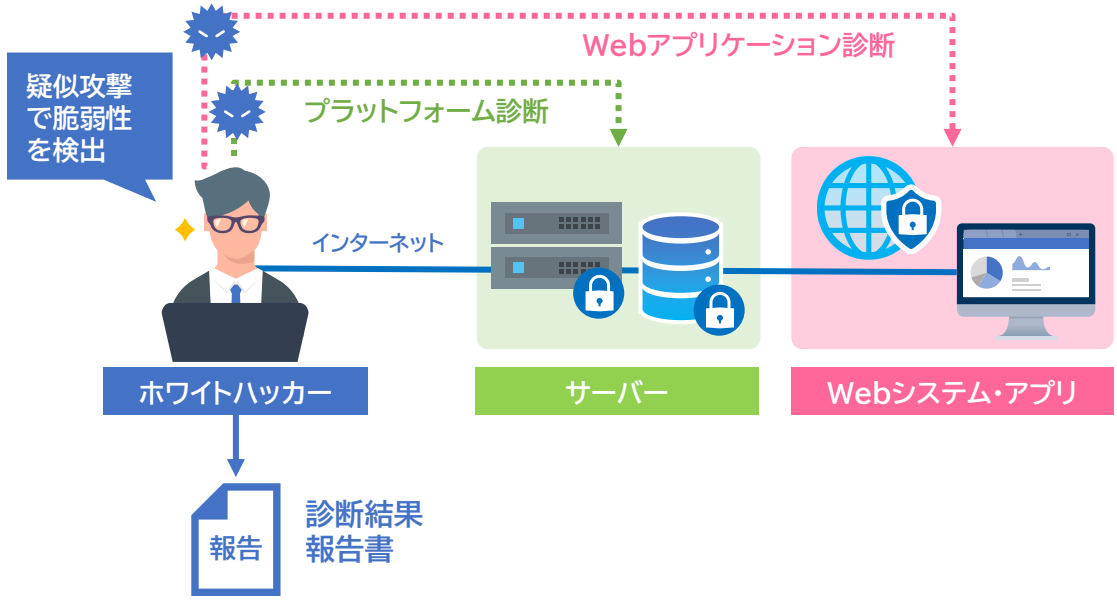
商用ツールの結果では、何百ページものレポートが生成されることも。しかし結果をいかにまとめ、次の行動に繋げるかが重要。お客様が直しやすいことを考慮し、取りまとめを意識した報告書を作成。





おすすめ

脆弱性診断サービス概要



導入メリット

- ホワイトハッカーが攻撃者と同じ手法を用いて、Webアプリケーション、プラットフォームのセキュリティ状態を評価できます。
- 顧客や取引先に対して、セキュリティ対策がしっかりと行われていることを示すことで、信頼性を高めることができます。

参考価格

※2025年5月時点

項目	提供形態	条件	定価
Webアプリケーション診断	サービス	リクエスト数,検査場所,検査時間帯 等による	要相談
プラットフォーム診断	サービス	診断対象IP数,検査場所,検査時間帯,診断手法 等による	要相談

サービスステップ

脆弱性診断サービスの流れ：ご要望に応じて、個別対応も可能です。

事前調整＆内容確認書作成

診断対象などを伺いスケジュールを決定。
決まった内容を基に診断内容確認書を作成。

診断実施

営業時間(平日10:00～18:00)に診断。
夜間・深夜・休日などのオプション対応も可能。

速報

診断中に緊急度の高い脆弱性が発見された場合は、速報としてご連絡。

結果分析/報告書作成

診断結果を診断結果報告書として取りまとめ。

報告会

診断を実施した専門エンジニアが内容を説明する報告会を開催。

診断項目

プラットフォーム診断

主に下記の項目を情報収集、診断致します。(約90,000項目)
※DoS診断についてオプションにて実施可能です。

項目
OS／ミドルウェア／アプリケーションの脆弱性チェック
サンプルスクリプトの有無のチェック
通信の盗聴可否のチェック(暗号化)
デフォルトアカウント使用のチェック
第三者中継(SPAM)のチェック
証明書の有効性チェック

Webアプリケーション診断

手動オペレーションによる診断は網羅性と検出精度が最も高く、診断結果に基づいたソースコード改修を実施できれば最も高いセキュリティレベルを実現可能。

項目	
クロスサイトスクリプティング	クロスサイトリクエストフォージェリ
SQLインジェクション	MXインジェクション
OSコマンドインジェクション	ディレクトリトラバーサル
通信の暗号化	セッションフィクセーション etc

お問い合わせはこちらから：https://www.fsi.co.jp/project/s/webapplication.html

脆弱性診断サービス

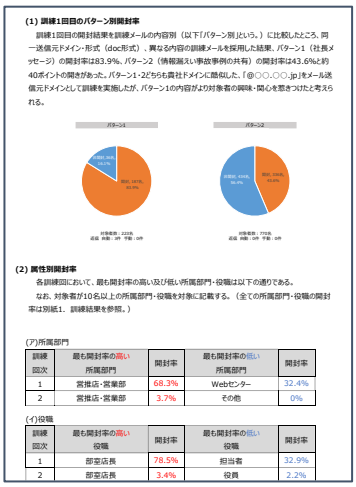
標的型メール訓練サービス

サイバー攻撃に負けない組織へ！標的型メール訓練で備えよう

01 業界での立ち位置を把握できる報告書

実績を踏まえた報告書作成

報告書には全体の集計結果を記載し、エクセルデータで対象者毎の開封状況の納品も可能。
また、ご要望に応じて累計約7,500社、約600万アドレス送信実績から、同業種との開封率比較データも報告書に記載可能。


(1) 訓練1回目のパターン別開封率

訓練1回目の開封結果を訓練メールの内容別（以下「パターン別」という。）に比較したところ、同一送信元ドメイン・形式（doc形式）、異なる内容の訓練メールを採用した結果、パターン1（社長メッセージ）の開封率は83.9%、パターン2（情報漏えい事故事例の共有）の開封率は43.6%と約40ポイントの開きがあった。パターン1・2ともに貴社ドメインに酷似した「@○○.○○.jp」をメール送信元ドメインとして訓練を実施したが、パターン1の内容がより対象者の興味・関心を惹きつけたと考えられる。

(2) 属性別開封率

各訓練回において、最も開封率の高い及び低い所属部門・役職は以下の通りである。

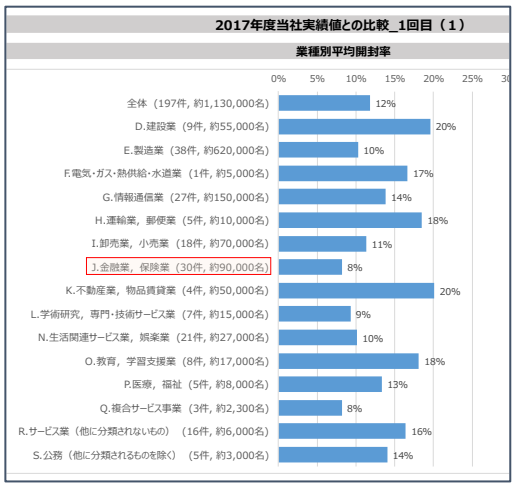
なお、対象者が10名以上の所属部門・役職を対象に記載する。（全ての所属部門・役職の開封率は別紙1、訓練結果を参照。）

(ア)所属部門

訓練回次	最も開封率の高い所属部門	開封率	最も開封率の低い所属部門	開封率
1	営推店・営業部	68.3%	Webセンター	32.4%
2	営推店・営業部	3.7%	その他	0%

(イ)役職

訓練回次	最も開封率の高い役職	開封率	最も開封率の低い役職	開封率
1	部室店長	78.5%	担当者	32.9%
2	部室店長	3.4%	役員	2.2%



02 初めてでも効果の高い訓練を実現するサポートコンテンツ

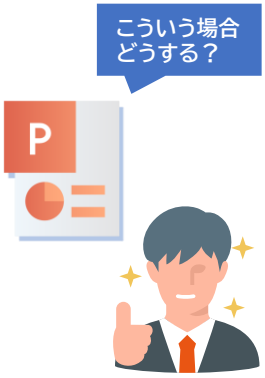
訓練の事前教育や事後教育

訓練の事前教育や事後教育に活用できる教育資料を提供。ユーザ様向けに平易な言葉で記載。PPT形式で提供し、社内ルールや初動対応ルールを追記して活用可能。

メール本文サンプル集

訓練メール内容の検討時、内容別・難易度別に分類された多数のサンプルを参考に可能。

実施前の事前教育
訓練後の事後教育



メール本文サンプル
システム・セキュリティに関する対応依頼（1）

見破るポイントは…

項目名	内容
分類	B. 内部連絡を装う依頼など
送信者名<メールアドレス>	情報システム部<system123@safesites.jp>
件名	【重要】ユーザID・パスワードの確認について（事務連絡）
本文	○○様 システム機能障害のため、ログイン設定の一部に急遽変更を加えました。つきましては、システムアクセスに問題ないことを確認するため、添付ファイルの記載した手順に従い、ユーザID及びパスワードを至急ご確認ください。 情報システム部
メール形式	添付ファイル DOC（ファイル名：確認手順書.doc）

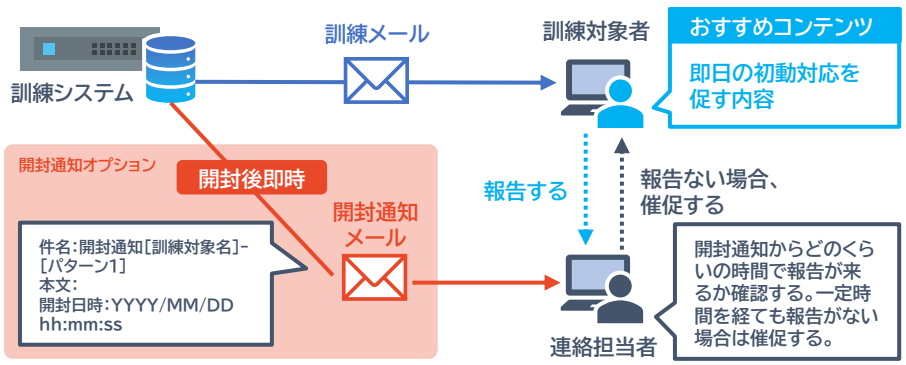
03 有償オプションによる高度な訓練を実現

開封通知オプション

「開封通知」とは、「誰が、いつ、何を開封したか」を知らせるメールであり、開封後即時に所定の連絡先の担当者へ送付し開封通知からの報告時間を確認可能。

分散装置オプション

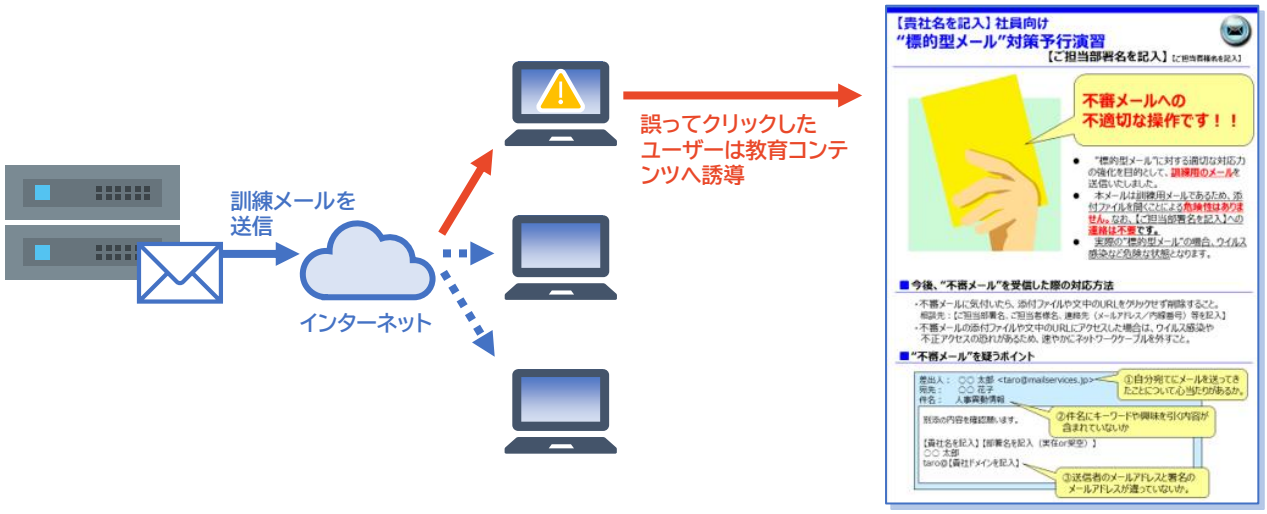
訓練メール送信を1回にまとめず午前と午後、複数日に分けるオプションメニュー。分散送信で窓口対応の負荷低減が可能。



おすすめ

標的型メール訓練サービス概要

添付ファイル方式では訓練メールの添付ファイル、URLリンク方式では訓練メール本文中のURLリンクをクリックしたユーザについて教育コンテンツ表示・ログ取得します。



導入メリット

- 従業員が実際の攻撃シナリオを体験することで、フィッシングメールやその他のサイバー攻撃に対する警戒心を高める。
- 多くの業界で求められるセキュリティトレーニング要件を満たすことで、法規制や業界標準に準拠することが可能。

参考価格

※2025年5月時点

項目	提供形態	サービス単位	定価
標的側メール訓練サービス	サービス	メール訓練内容による	お問い合わせください

標準サービスパック

STEP.1 実施内容の選択

- エキスプレス：訓練メール／ログ
- スタンダード：訓練メール／ログ・報告書
- プレミアム：訓練メール・アンケート／ログ・報告書
- プレミアム EX：訓練メール・アンケート・eラーニング／ログ・報告書

×

STEP.2 訓練回数の決定

- 訓練メール1回
- 訓練メール2回
- 訓練メール4回
- 訓練メール6回

×

STEP.3 対象数の決定

ご希望のメールアドレス数
10～300,000

サービスステップ：プレミアムパックの場合

＼ ご契約から約3ヶ月程度でのご納品（調整により、短期間での対応も可能）／

事前準備	事前テスト＆予備	訓練実施（1回ないし2回）	種明かし＆アンケート実施	報告書作成＆納品
約1週間	約1週間	送信完了から2営業日で〆	約1週間	約2週間

サイバーセキュリティお問合せ窓口
E-mail:cyber_security@fsi.co.jp

脆弱性診断サービス

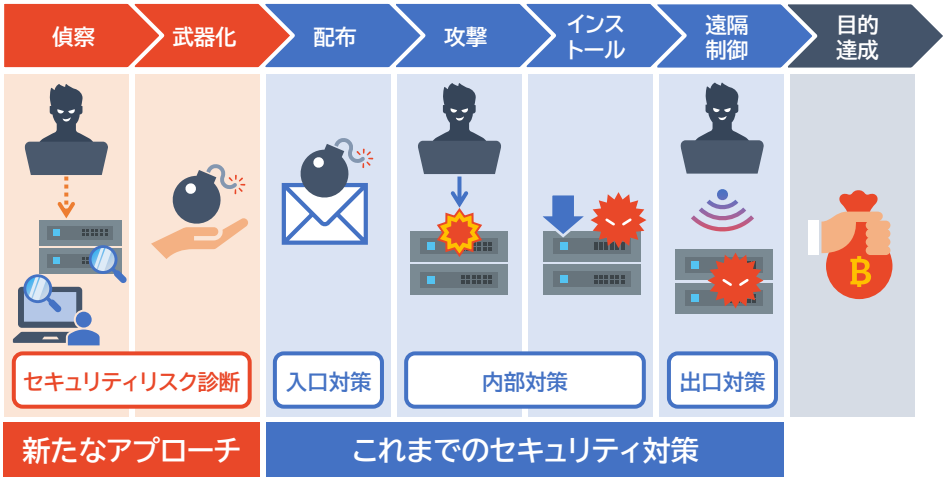
セキュリティリスク診断

見えないリスクを可視化！セキュリティリスク診断で安心

01 情報収集フェーズにフォーカスした新たなアプローチ

ドメイン情報を活用しリスクを評価

これまでのセキュリティ対策や診断では入口、内部、出口に着目、サイバー攻撃の際には、成果が上がりやすいターゲットを探す「調査活動」が実施される。
ドメイン情報からインターネット上の膨大なデータを自動収集。攻撃者視点から企業や組織のサイバーセキュリティリスクを定量化し、新たなアプローチで評価。シンプルで効果的なセキュリティソリューションの提供。



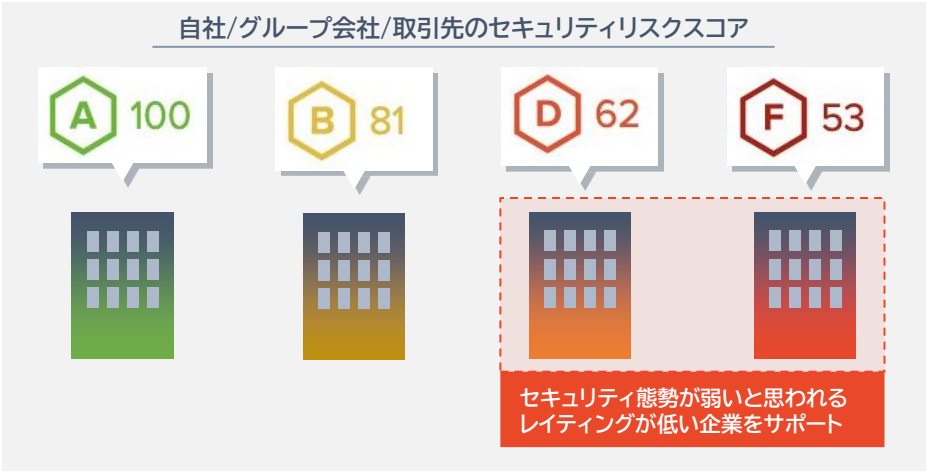
02 自社/グループ会社/取引先のセキュリティリスクの可視化

攻撃者視点の詳細な分析

インターネット上から非侵入で収集できる情報に基づき、攻撃者視点で詳細な分析と結果を提供。自社だけでなく、グループ会社や取引先のセキュリティリスクの可視化も可能。

主なご利用用途

- 自社の国内/海外拠点やグループ企業全体の状況把握に活用
- 取引先に求めるセキュリティ対策の指針として活用
- 企業買収前のリスク評価に活用



03 理解しやすい報告書

サマリーレポート

収集した脅威情報を元に、ネットワークやDNS、パッチ管理など「外部から調べることができる」計10個のカテゴリにおいて各項目100点満点のスコアリングを行い、A～Fの5段階でリスクを定量化し攻撃の“狙われやすさ”の指標評価します。

トリアージレポート

実際の狙われた対応のリスクをCVSSベースの指標について記載をし、実リスクと狙われやすさを兼ね合わせてスコア改善および実際のリスクアドバイスを記載いたします。

おすすめ

セキュリティリスク診断概要

攻撃者視点で自社/グループ会社/取引先のセキュリティリスクの可視化

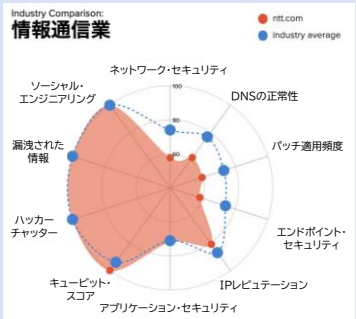
ドメイン情報からインターネット上の膨大なデータを自動収集し、攻撃者視点で企業・組織のサイバーセキュリティリスクを定量化

- 収集した脅威情報を元に独自のアルゴリズムでネットワークやDNS、パッチ管理など「外部から調べることができる」計10個のカテゴリにおいて評価

F 53	ネットワーク・セキュリティ セキュアでないネットワーク設定の検出	C 72	アプリケーション・セキュリティ 一般的なウェブアプリケーションの脆弱性検出
D 62	DNSの正常性 セキュアでないDNS設定と脆弱性有無の検出	A 100	キュービット・スコア 一般的なベストプラクティスの実装をチェックする独自のアルゴリズム
F 59	パッチ適用頻度 脆弱性とリスクを含む可能性のある古い資産	A 100	ハッカーチャッター ハッカーサイトでのお客さまの会社に関する会話(チャッター)監視
F 55	エンドポイント・セキュリティ 従業員のワークステーションまたはモバイルデバイスのセキュリティレベル測定	A 100	漏洩された情報 誤って漏洩している可能性のある企業機密情報
B 81	IPレピュテーション 企業ネットワーク内でのマルウェアやネット内などによる疑わしい活動の検出	A 100	ソーシャル・エンジニアリング ソーシャルエンジニアリングまたはフィッシング攻撃に対する従業員の認識を測定

- 各カテゴリ 100点満点のスコアリングを行い、A～Fの5段階でリスクを定量化

- 業界平均との比較が可能



- それぞれの項目についてより詳細なデータもレポート形式で提供

脆弱性	測定値
開いているポート	7,547
サイトの脆弱性	123
検出されたマルウェア	2,355
漏洩された情報	0

- お客様はドメインを入力いただくだけ！

XXXXX.co.jp 診断

導入メリット

- 組織のセキュリティリスクを一目で把握可能。どの部分に改善が必要かを明確に提案。
- リスクが発見された場合、即座に対策を講じることが可能。被害を最小限に抑える。

参考価格

※2025年5月時点

項目	提供形態	サービス単位	定価
セキュリティリスク診断	サービス	1ドメインより	お問い合わせください

セキュリティリスク診断サービスメニュー

自社の国内／海外拠点やグループ企業を把握	複数の取引先を把握	常に把握
自社やグループ企業に年に一度などで実施したい	委託先及び取引先についてセキュリティ対応を把握したい	定期的な診断および監査体制の確立を検討したい

①スポット診断サービス	②委託先管理診断サービス	③継続診断サービス
• ドメイン数:3～ • サマリーレポート • トリアージレポート • 1か月Q&A対応(メール)	• ドメイン数:50～ • サマリーレポート • 詳細レポート ※スコアD以下の企業のみ • トリアージレポート ※スコアD以下の企業のみ • 3か月Q&A対応(メール)	• ドメイン数:3～ • サマリレポート • トリアージレポート • Web会議によるセッション(年間12回) • 随時Q&Aメール対応

サービスステップ:スポット診断サービスの場合

＼ ご契約から約2週間程度でのご納品／

ドメインの指定	レポート作成	報告会	QA対応(1カ月)
• 調査するドメインの指定	• サマリーレポートおよびトリアージレポートの作成	• 左記結果に対する報告会の実施(Web会議限定)	• レポートに関するQA • その他グループ管理や委託先に関するご相談

サイバーセキュリティお問合せ窓口
E-mail:cyber_security@fsi.co.jp