セキュリティ商材のご案内

セキュリティ事業理念

標的型攻撃やランサムウェアなど、
サイバー攻撃の脅威は益々巧妙になってきています。
毎日、新しいウイルスが100万種類と作られ、ウイルス対策ソフトなどでは、未知のウイルスやサイバー攻撃に対応することが困難になってきています。

私たちは、社会になくてはならない存在であるために、最先端の技術で、安心安全なコンピュータシステム運営のための必要なセキュリティソリューションを提供していきます。

情報セキュリティ10大脅威 2026

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い（2016年以降）
1	ランサム攻撃による被害	2016年	11年連続11回目
2	サプライチェーンや委託先を狙った攻撃	2019年	8年連続8回目
3	AIの利用をめぐるサイバーリスク	2026年	初選出
4	システムの脆弱性を悪用した攻撃	2016年	6年連続9回目
5	機密情報を狙った標的型攻撃	2016年	11年連続11回目
6	地政学的リスクに起因するサイバー攻撃（情報戦を含む）	2025年	2年連続2回目
7	内部不正による情報漏えい等	2016年	11年連続11回目
8	リモートワーク等の環境や仕組みを狙った攻撃	2021年	6年連続6回目
9	DDoS攻撃（分散型サービス妨害攻撃）	2016年	2年連続7回目
10	ビジネスメール詐欺	2018年	9年連続9回目

情報処理推進機構（IPA）「情報セキュリティ10大脅威 2026」
https://www.ipa.go.jp/security/10threats/10threats2026.html

事業内容

- サイバーセキュリティソリューションの販売
- サイバーセキュリティコンサルティング
- サイバーセキュリティ環境の構築・導入・運用支援

ソリューションマップ

ネットワーク・ゲートウェイ

LTE over IP
LTEの技術を使った閉域網通信を構築

SOPHOS

Firewall,アンチウイルス、IPS、スパム対策、ZTNA

Webサーバー

WebARGUS
WEBサイトの改ざん防止
改ざんを通知、復旧します

サーバー/Mailサーバー

Sophos Email
Eメールに特化したサイバーセキュリティソフト

Metadefender CORE
複数のアンチウィルスソフトを単一サーバ上で同時可動できるプラットフォーム

クライアント

OpenText™ Core Endpoint Protection
シグネチャレスの次世代型アンチウィルスソフト

SOPHOS Intercept X
UTMと連動して情報漏洩を防止シグニチャレスUVS

Sophos MDR
世界最高峰のSOCサービス

u-trust LAN Crypt
PC、サーバーのデータ暗号化

OpenText™ Core Endpoint Backup
PC、サーバーのデータバックアップ

資産管理

LanGuard
ネットワーク/システムの脆弱性及びソフトウェア資産管理

MylogStar
端末経由で行っている操作を、記録・管理・分析することが可能

外部媒体チェック

Metadefender KIOSK
外部媒体（USB / DVD等)のウイルス検知、対策

診断

NSサイバーレスキュー
公的機関のガイドラインに準拠したトータルセキュリティ診断から
WEB診断、脆弱性診断、ペネトレーションテスト等あらゆる診断を行います

特定 → 防御 → 検知 → 対応 → 復旧

セキュリティシステム選びのポイント

未知・標的型攻撃を想定した対策

常に最新の脅威を想定した対策

パフォーマンスへの負荷が最小限

追加コスト・設備投資の必要なし

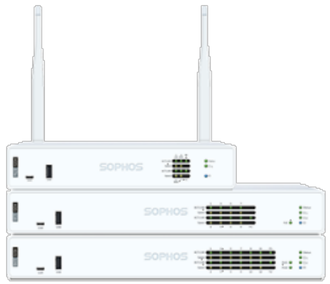
バージョンアップ等の運用が容易

セキュリティ対策→確実・最新・低コストで最大限

Sophos Firewall XGS シリーズ

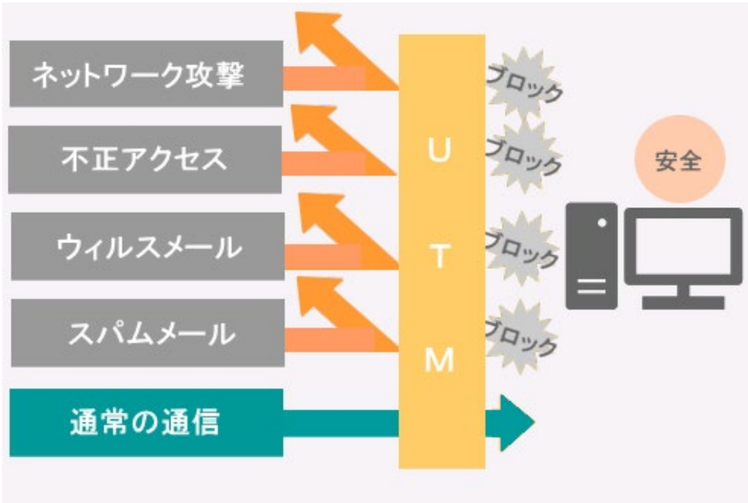
ネットワーク回線の入口に設置、不正アクセスやマルウェアの侵入を防御

複数の異なるセキュリティ機能を一つのハードウェアに統合した総合的な
セキュリティ対策ユニット



２つのマルチコアCPUで処理を高速化
高いパフォーマンスと強力な保護を実現

2つのマルチコアCPUで処理分散させ、高速化を実現。
また、Sophos FirewallのXstreamパケット処理アーキテクチャの
ディープ パケット インスペクション(DPI) エンジンが
プロキシレスのシングルパス セキュリティ スキャンと、
Xstream SSLインスペクションを提供。

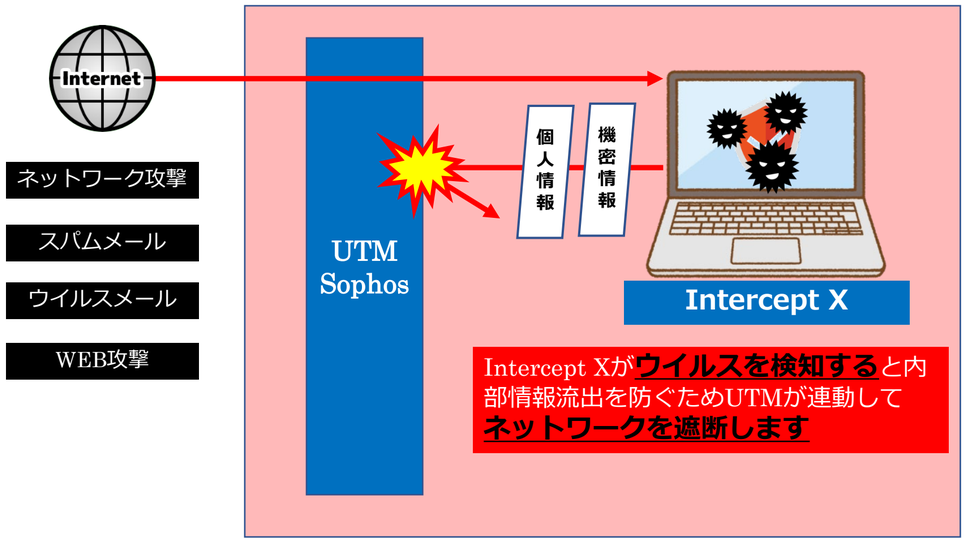


Sophos Intercept X シリーズ

業界をリードするエンドポイントセキュリティソリューション

エクスプロイト対策、ランサムウェア対策、ディープラーニングAI、制御テクノロジーを組み合わせることで包括的な多層防御を実現。1つの主要機能に依存することなく攻撃対象領域を減らし、攻撃の実行を防ぐことでエンドポイント保護

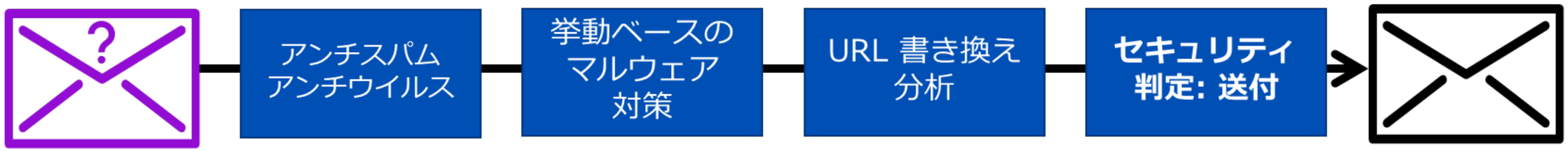
◆Sophos UTMとの連携

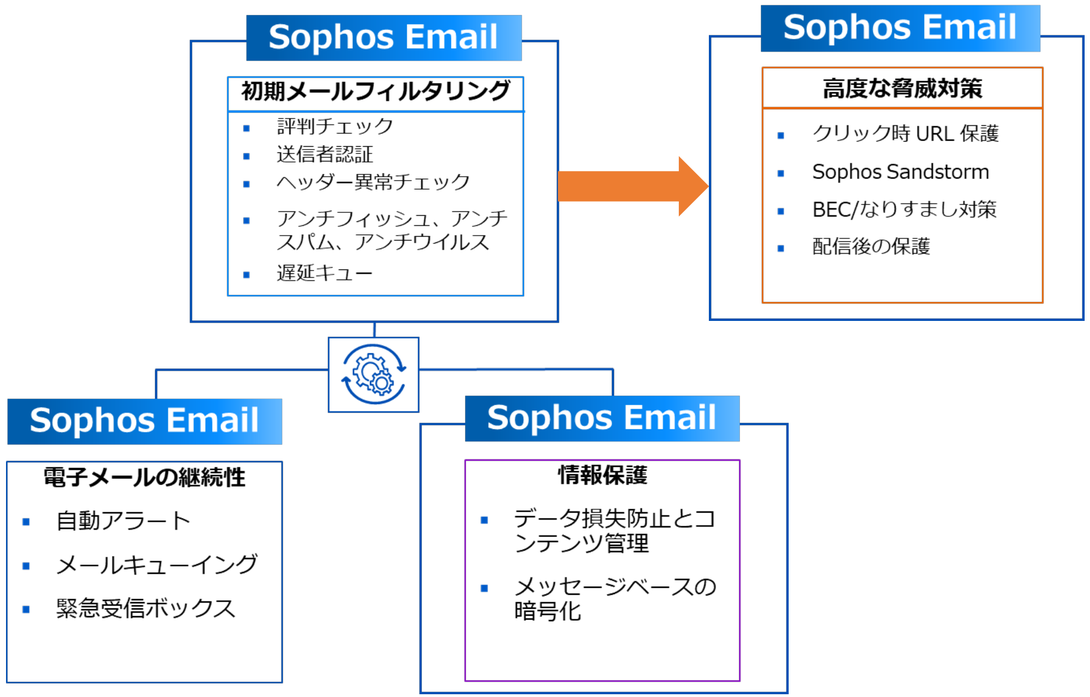


◆各審査機関で高い評価を受けております

Sophos Email

外部からのメール攻撃に対応するために必要な機能を1つに搭載



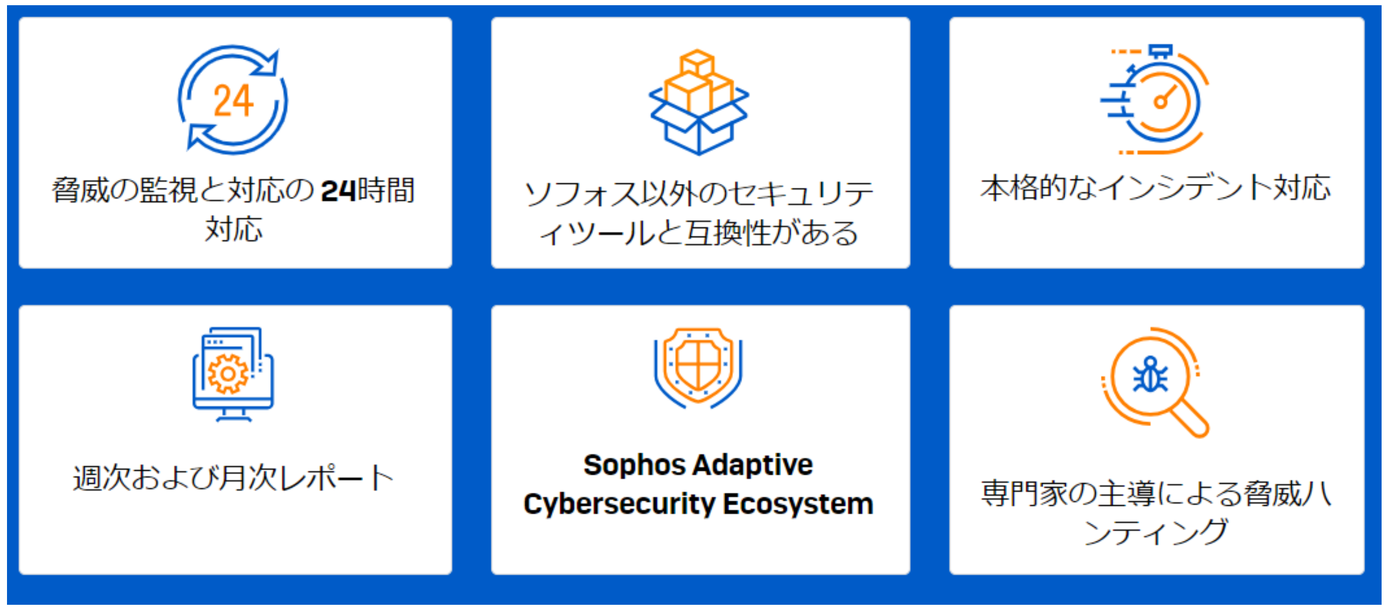


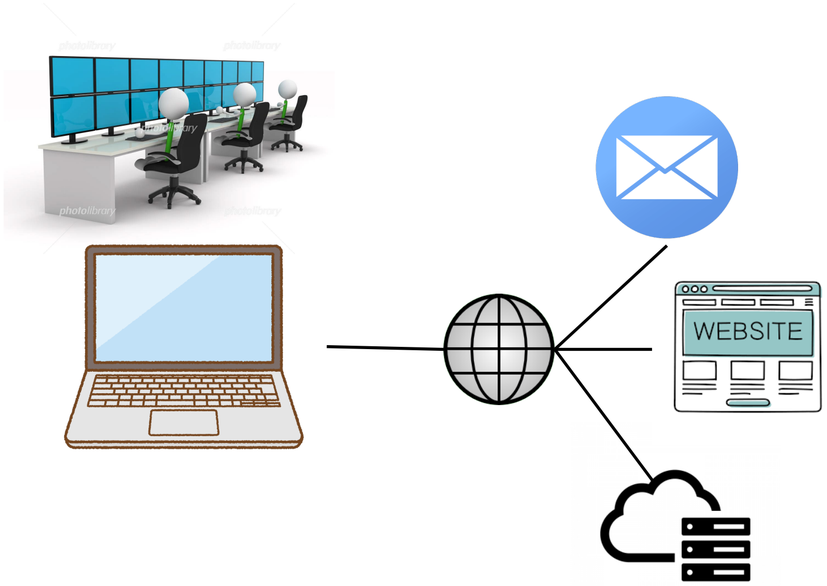
- 低容量、ユニーク、非スパム
  バルクシグネチャーやレート制限なし
- 評判の良いIPアドレスから送信
  IPレピュテーションブロックなし
- 添付ファイルが無害、あるいは添付なし
  サンドボックス回避
- URLが無害、または含まれていない
  URL書き換えやブロック、または分析を回避

Sophos MDR

脅威検出と対応を専門家が24時間で監視対応

現代セキュリティの最高峰のSOCサービス、サイバー攻撃を専門家が検出して対応する
24時間年中無休のフルマネージドサービス

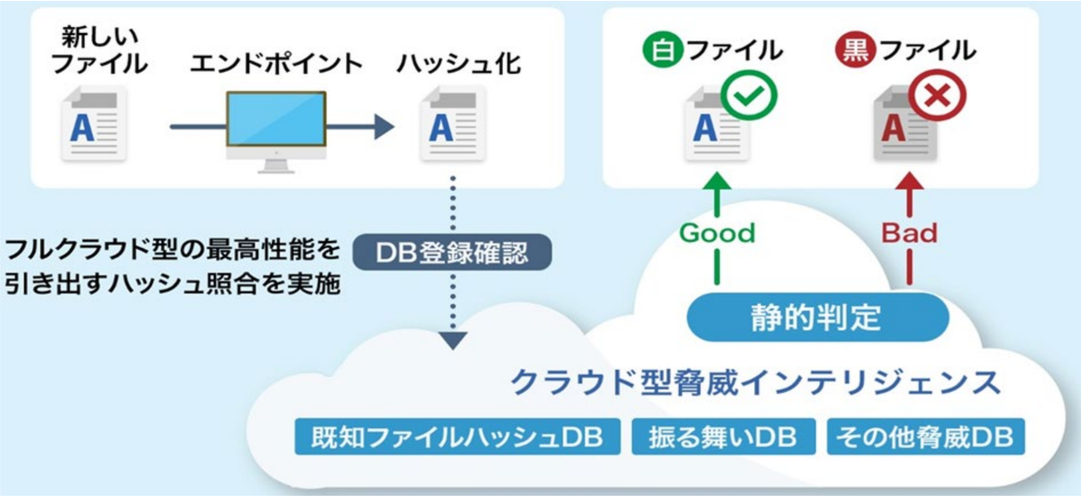




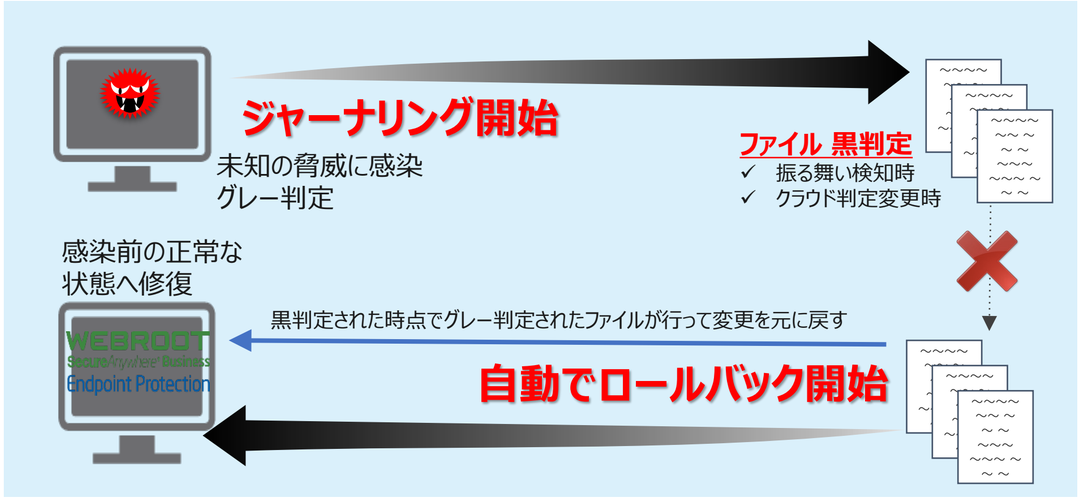
OpenText™ Core Endpoint Protection

シグニチャレスの次世代型エンドポイントセキュリティ

PC内に定義ファイルはなく、クラウド通信でウイルスを検知する
PCに負担がかからず、最新の定義ファイルで検知をします
ロールバック機能で未知のウイルスにも対応します



クラウド型ウイルス検知

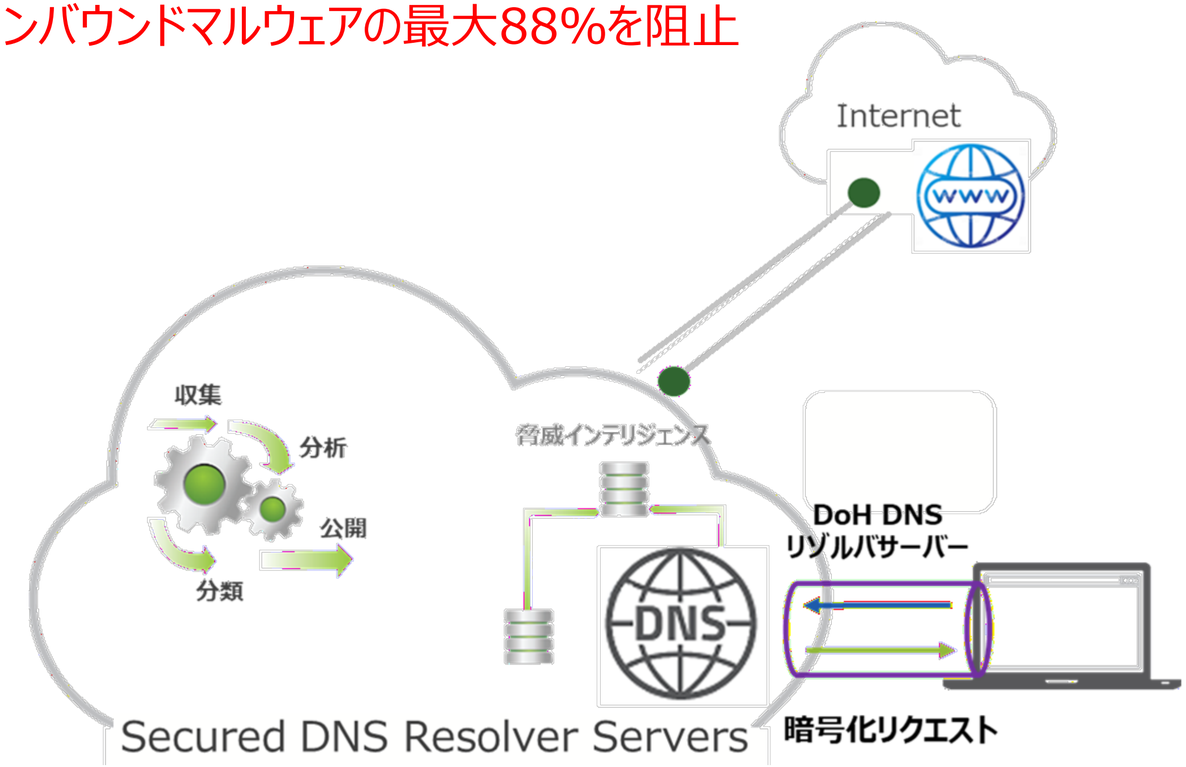


独自技術：ロールバック機能

OpenText™ Core DNS Protection（オプション）

サイトのアクセスやDNSレベルで規制、安全にサイトにアクセス

インバウンドマルウェアの最大88%を阻止

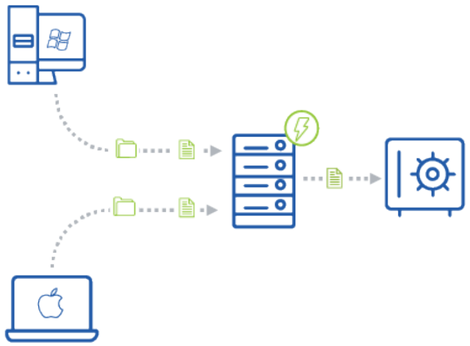


- **簡単設定**
  管理コンソールからの簡単な設定変更だけで
  サービス開始とガバナンスの実施
- **DNS通信の暗号化**
  DNS over HTTPSをサポート
- **セキュアなインターネットアクセス**
  信頼性のあるグローバルデータベース
  （BrightCloud）を採用
- **WEBサイトフィルタリング**
  80種類以上のWEBサイトカテゴリにて
  業務に不要なサイトにアクセスさせない
- **インターネットの利用状況の可視化**
  ネットワーク監視とアクセス制御、利用状況を
  モニタリング

OpenText™ Core Endpoint Backup / Cloud-to-Cloud Backup

OpenText™ Core Endpoint Backup

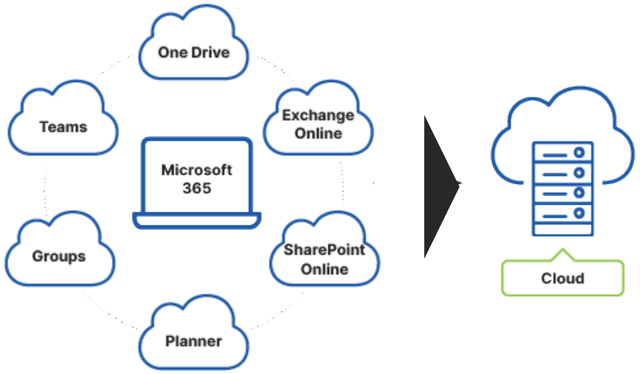
端末1台ごとのバックアップで網羅的にデータを保護



Windows PC、Windows サーバー、mac データをクラウド上に自動バックアップ
端末にエージェントを導入するだけ、あとはルールに沿って自動でデータをバックアップします。導入後は操作の必要はなく、自動でクラウドにバックアップされます。
差分リストアやポイントインタイムリカバリが可能
前回データとの差分リストアすることにより、高速でリストアが可能。
ポイントタイムリカバリーでポイントごとの柔軟なリカバリーが可能
デバイス紛失時に遠隔よりデータ消去が可能（リモートワイプ）
オンラインになった瞬間にリモートでバックアップしていた端末側のデータを削除することが可能。

OpenText™ Core Cloud-to-Cloud Backup

お客様のSaaS系クラウドサービスのデータをセキュアに保護



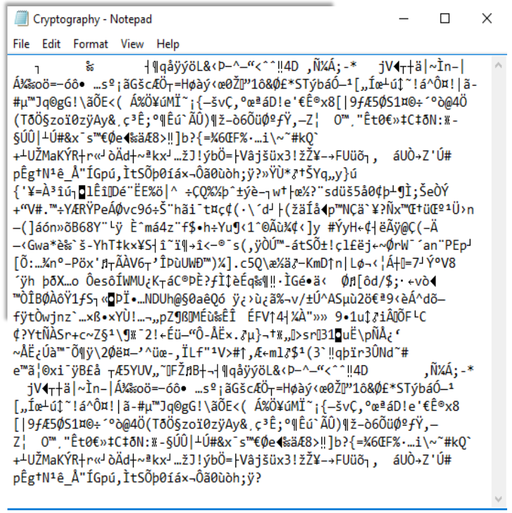
バックアップ対象サービス：
- Microsoft365(Mail, Calendar, Contacts, SharePoint, OneDrive, Teams, Notes, etc..)
- SalesForce(Catter, Objects, Attachments, Reports, Dashboards, Emails, Workflows, etc..)
- BOX
- DropBox
- Google G-Suite

使いやすさに定評があるシンプルな管理コンソール
サービス管理に費やす時間を最小限に抑えるため、一目でわかるインターフェースで誰でも簡単に運用することが可能。
複数のSaaSバックアップサービスの単一ポータル
いくつかのクラウドサービスを利用されていても同じコンソールから自動バックアップ、リカバリを行うことができます。
迅速で正確なデータ回復のためのきめ細かい制御
退職者などによるアカウント削除後でも、データを復旧することが可能です。
また過去に遡って人為的に消してしまった、消されてしまったデータを簡単に復元することも可能

u-trust LAN Crypt

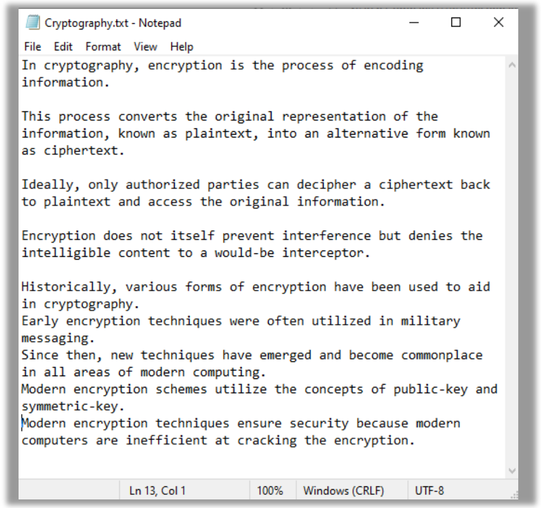
データを暗号化、データ搾取や情報漏洩の際、データの機密性を確保

ヨーロッパの軍事機密でも使われている技術でデータを暗号化、
社内のデータの閲覧権限も設定、社内外での情報漏洩を防ぎます



暗号化済みのファイル

暗号化キー



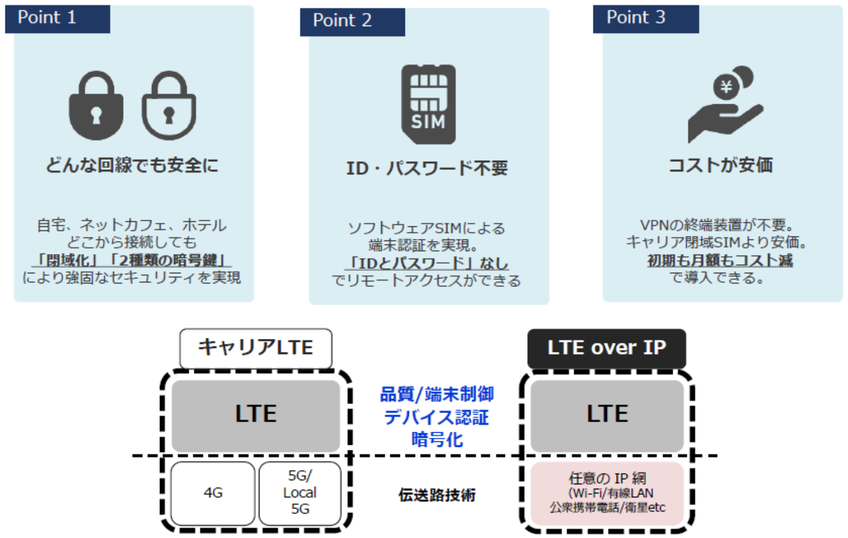
平文のファイル

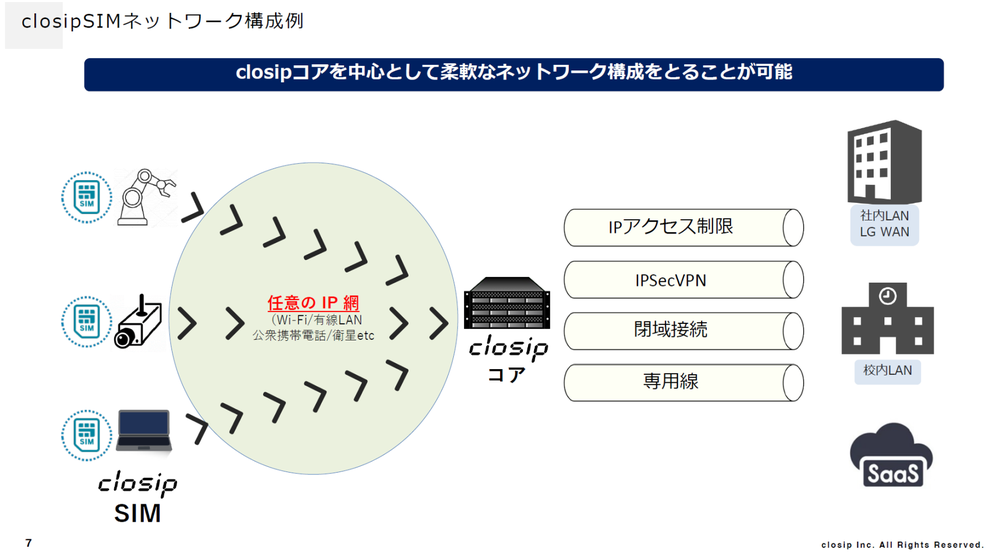
- 全社的なファイルセキュリティ管理が実現
- ユーザー単位・グループ単位でのファイルアクセス制御が可能
- ファイルの保存場所は不問（オンプレ、ローカル、クラウド、メディア）
- 暗号化・復号はバックグラウンドで自動で行われ、ユーザは意識する必要が
- ありません
- 多様なプラットフォームに対応（Windows、macOS、iOS、Android）
- APIも提供されます。

LTE over IP

LTE通信を使ったセキュアなデータ通信網

LTEプロトコルをモバイルの伝送路技術から分離し、既存のIP網で使用できるようにソフト開発をした**世界初の特許技術**
キャリアLTEと同等の機能を有しながらネットワークに縛られず、設備/通信コストの観点で優位性があります。





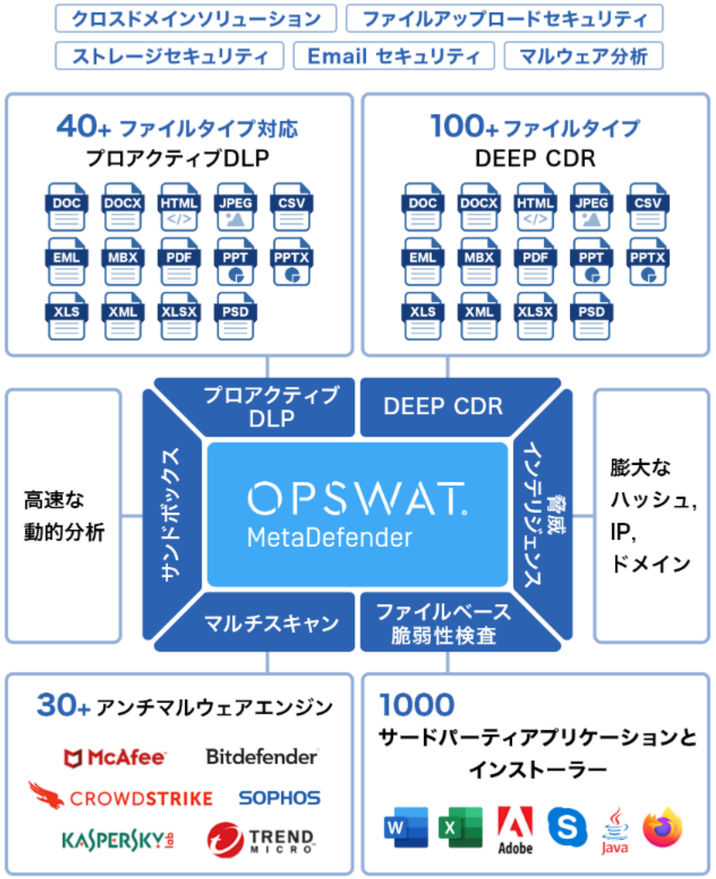
MetaDefender core

30種以上のアンチウイルスエンジンを1つのサーバで動かすプラットフォーム

- 32種類のアンチウイルスソフトの搭載で検出率を大幅に強化
  →殆どのウイルスを検知が可能

- 複数のウイルスメーカ製品を搭載する事により、検出の迅速化とエンジンの脆弱性を最小化
  →新種のウイルスにも素早く対応

- 有害マクロの除去やファイル変換機能によるファイルの無害化
  →重要ファイルが検知した場合でもファイルを安全に開封が可能



MetaDefender Kiosk

USBデバイス等の外部メディアをセキュアな環境で安全に使用

USBなどの外部メディアを高セキュリティレベルのエリアに持ち込む際、
ファイルタイプやサイズによるデータ制御や偽装拡張子チェック、ファイル変換を
自動で行い、データ判定・処理をするデータチェックポイントソリューション

WebARGUS

Webサイトを監視、改ざんに対し即時に復旧します

サーバ内の全てファイル/ディレクトリをリアルタイムで監視し、改ざんが起きた場合、0.1秒以内に元の状態に戻すことができるソリューションです。

編集	削除	追加	プロパティの変更
● 文章の編集 ● 画像の編集	● ファイル/ディレクトリの削除	● ファイル/ディレクトリの追加 ● 新規作成	● ユーザ、オーナー、パーミッション、権限などの変更
● プログラムや重要ファイルの編集による被害 ● 暗号化によるアプリーケーションの停止	● ブラックリスト削除による不正アクセス ● 設定ファイル削除による不正アクセス	● マルウェアの侵入 ● バックドアプログラムの設置	● 情報漏えい ● アプリケーションの不正操作 ● 権限奪取

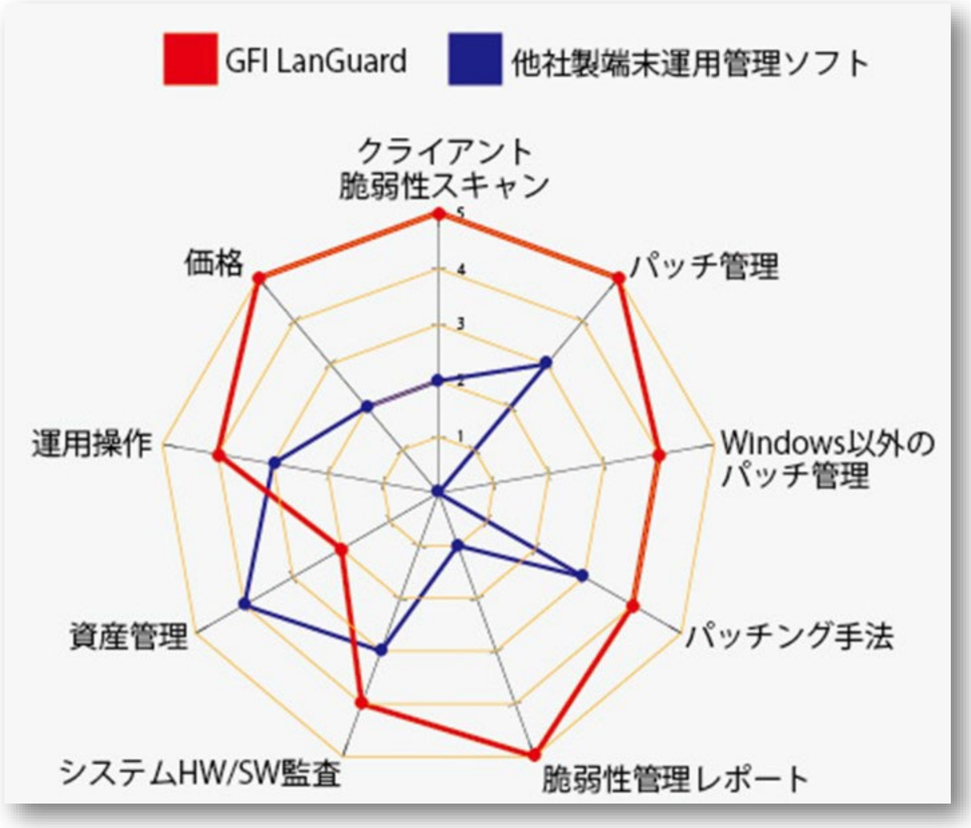
これらの被害をリアルタイムで検知し、0.1秒以内で復旧します。

GFI LanGuard

ネットワークの脆弱性、パッチ管理、それらをひとつのパッケージで対応

・ネットワーク上のシステムをスキャン
・修復されていない脆弱性をリスト化
・結果を対応したパッチや更新プログラムを取得・配布し、レポートを生成

今後のセキュリティ対策で重要視される
脆弱性管理を本製品一つで実現し、
管理者の手間を大幅に軽減します。



MylogStar（マイログスター）

業務効率化 と 情報漏えいを防ぐ ログ管理ツール

MylogStarはPC端末経由で行っている操作をログとして、記録・管理・分析することが可能です。

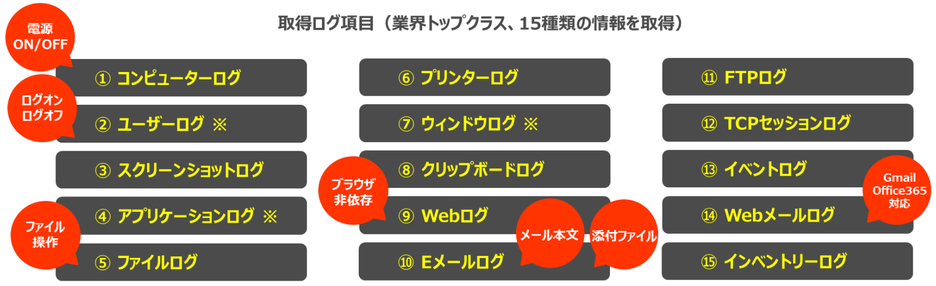
「いつ」「誰が」「どのファイルを」「どうした」といった利用者の証跡を可視化することで、

業務改善や**情報漏えい対策**に役立ちます。

いつ	誰が	どのファイルを	どこへどうした
2013/12/2 16:31:41	contoso¥tokura-m	営業日報.xlsx	Eドライブ （USBメモリー）へファイルコピーした

こんなご要望にお応えします！

- 端末の利用実態を把握したい
- 内部統制やコンプライアンスの観点から操作ログが必要
- マイナンバー法や個人情報保護法改正に対して証跡管理が必要



NSサイバーレスキュー

お客様の予算、ニーズに合わせてセキュリティ状態を診断します

情報セキュリティ対策は今や企業のスタンダードです。

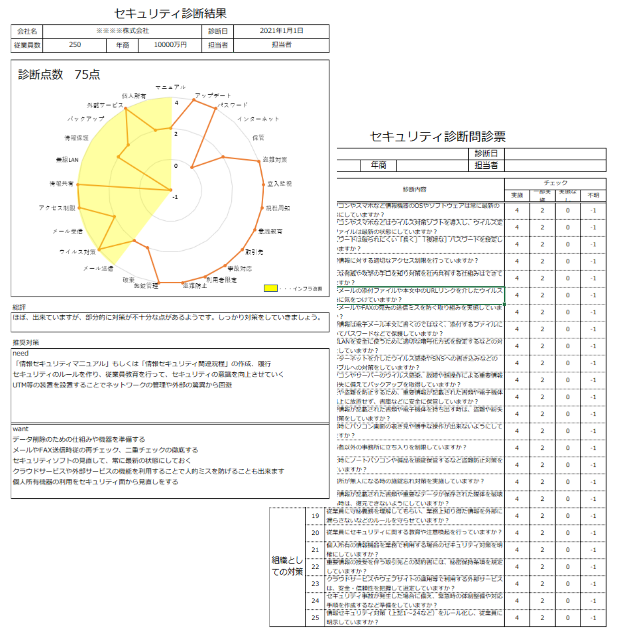
セキュリティ診断で課題を解決！

今のセキュリティ
対策が十分か
わからない…

何となくセキュリティが甘いと認識しているが周りに説明できない…

セキュリティ被害のニュースが増えていて心配…

簡易セキュリティ診断



5分でできる中小企業様向けの
セキュリティ診断

25項目の設問からセキュリティの
問題点を抽出

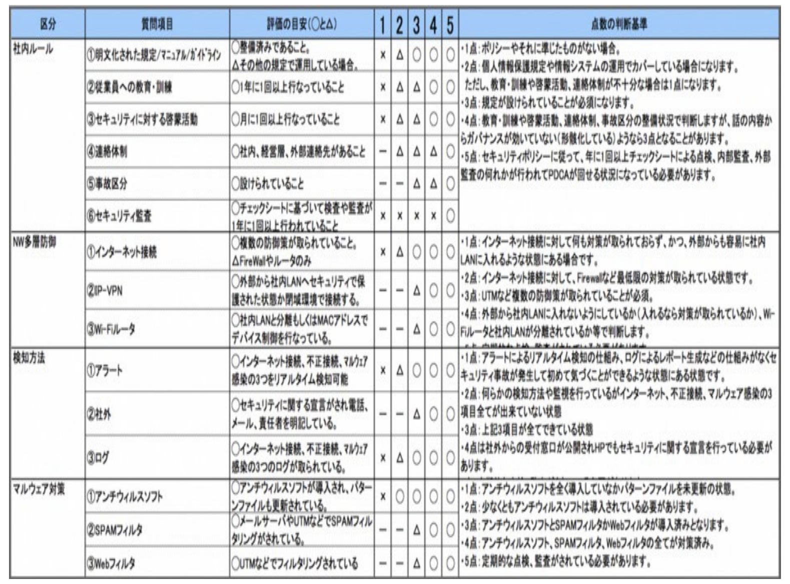
あなたの会社のセキュリティ問題
を可視化します

NSセキュリティ診断サービス

診断の流れ

アポイントメント（事前準備） ▶ ヒアリング（問診）60分程度 ▶ レポート作成 5～7営業日程度 ▶ 診断結果報告 90分程度

診断結果報告書イメージ



脆弱性診断・ペネトレーションテスト等

お客様のご希望に添えるよう
脆弱性診断をはじめ、あらゆるセキュリティ診断
を取り揃えております

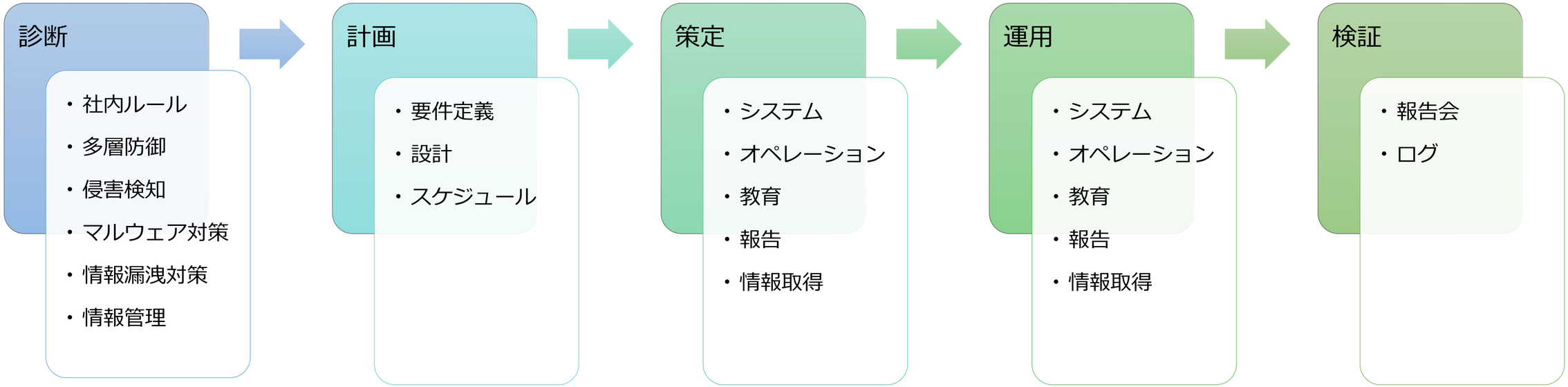
	攻撃からの防御	早期検知・被害軽減	インシデント対応
ネットワーク	プラットフォーム診断・ペネトレ ネットワーク環境のセキュリティを把握	SOC・IPS/IDS 攻撃・不正侵入を検知	デジタルフォレンジック 攻撃された際の 法的根拠となる証拠保全や 被害の特定
Web アプリケーション ・ スマホアプリ	脆弱性診断 Webサイト・サービスの セキュリティレベルを把握	WAF・DDos攻撃対策 Webサイト・サービスへの攻撃防御	サイバー保険 インシデント発生時の保険による保障
エンドポイント	IoT診断 ネットワーク機器のセキュリティを把握	EDR・簡易EDR 端末内の脅威検知・隔離	個人情報保護 端末内の個人情報検出・管理
その他	サイバーセキュリティコンサルティング・アドバイザリー リスクアセスメント・教育研修・ワークショップ・法令対応・CSIRT構築/運用支援 など継続的な支援		

5段階のリスクレベル
緊急／高／中／低　情報で
優先度の高いものからご報告します。

セカンドオピニオンとしてのご利用や
定期運用の場合、コストを抑えることが
可能です

セキュリティ・コンサルティング

システムからオペレーションまでクライアントニーズに沿った適切なソリューションを提供します。



お問合せ先

会社名：株式会社アイティークロス

住所　：名古屋市中区栄3丁目11番31号
　　ＪＭＦビル名古屋栄01 5階

TEL　：052-242-0430
MAIL　：s-itc@itcross.jp