サイバーレジリエンス強化

守りの防御から「攻め」の防御へ

- ダークウェブ調査による予兆検知から侵入対策・感染時の自動復旧まで実現 -

Endpoint Cyber Resilience Suite

サイバーレジリエンス向上のための、エンドポイントセキュリティ対策ソリューション

特定

漏洩情報から攻撃リスクの予兆を検知

INTERSAFE Darkweb Monitoring

防御

外部からの侵入を無効化

HP Sure Click Enterprise

対応

対処、回復までを自動実行

AI スマートSOC for SentinelOne

検知

内部からの感染拡大の検知、防止、隔離による封じ込め

SentinelOne

国として強化！

国家レベルで**受動的防御から先手を取る防御へ**の能動的基盤が整備

▶サイバー対処能力強化法を制定（2025年5月）
▶サイバー攻撃の脅威が深刻化する中、日本は従来の“受け身”の防御から脱却し、先手を打って被害を防ぐ「能動的サイバー防御」へと国家レベルで体制を強化

サイバーキルチェーン全体をカバーする構成でご提供可能

偵察	武器化	配送	攻撃	インストール	コマンド&コントロール	目的の実行

ダークウェブ → 漏洩情報から攻撃リスクの予兆を検知 → 外部からの感染防止 → 内部からの感染拡大防止 → 対処、回復までを自動実行

INTERSAFE Darkweb Monitoring

ダークウェブに漏洩した情報は複数の攻撃者に渡ります。
漏洩した情報の削除は難しいため、いち早く漏洩を検知し、対策を始めることができます。

HP Sure Click Enterprise

攻撃者はメールやウェブなど、さまざまな手法で侵入を試みます。
ローカルの分離環境（MicroVM）でアプリケーションを実行することで、攻撃を封じ込めながら業務を継続することができます。

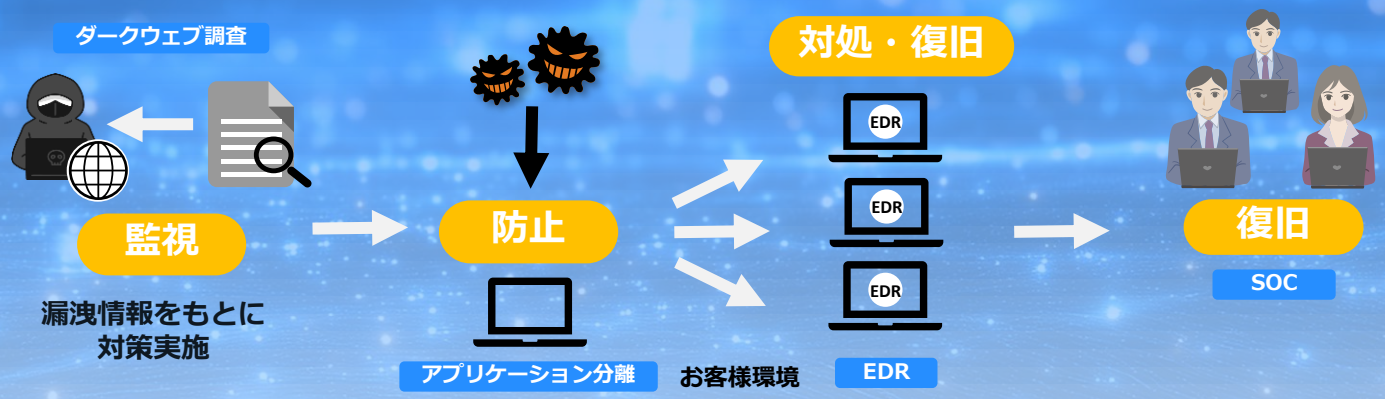
SentinelOne

USBメモリや管理漏れのIoT機器にも侵入リスクは潜んでいます。
侵入を許した場合でも、即時に検知・隔離を実行することで、サイバー攻撃の進行を止め、重要資産を守ることができます。

AI スマートSOC for SentinelOne

被害にあった場合に重要なのは、“問題の把握”と“業務継続”です。
どのような攻撃で何が起きたかを把握し、AIによって自動復元を行うことで、破壊されても業務を継続することができます。

ソリューションイメージ



プラン内容

プラン名 ＼ ソリューション	INTERSAFE Darkweb Monitoring 無償トライアル	HP Sure Click Enterprise	SentinelOne	AI スマートSOC for SentinelOne	最低ライセンス数
① チェックお試しプラン	○				1 -
② 漏洩確認プラン	○				1 -
③ 外部脅威対策プラン	○	○			100 -
④ 内部脅威対策プラン	○		○	○	1 -
⑤ フル対策プラン	○	○	○	○	100 -

※InterSafe Darkweb Monitoringは年間契約です ※HP Sure Click Enterpriseは100ライセンス以上が必要です

アルプス システム インテグレーション株式会社

本　　社　〒145-0067　東京都大田区雪谷大塚町1-7
TEL：03-5499-8045
東京営業所・札幌営業所・古川営業所・仙台営業所・いわき営業所
白金台オフィス・名古屋営業所・大阪営業所・広島営業所・福岡営業所

https://www.alsi.co.jp　　E-mail：ssg@alsi.co.jp
※ALSI(アルシー)はアルプス システム インテグレーション株式会社のコミュニケーションブランドです。

お問い合わせ、ご用命は下記へお申し付けください。

202510.ZTS