

inet Security Solution



- 2022 Edition Catalog -

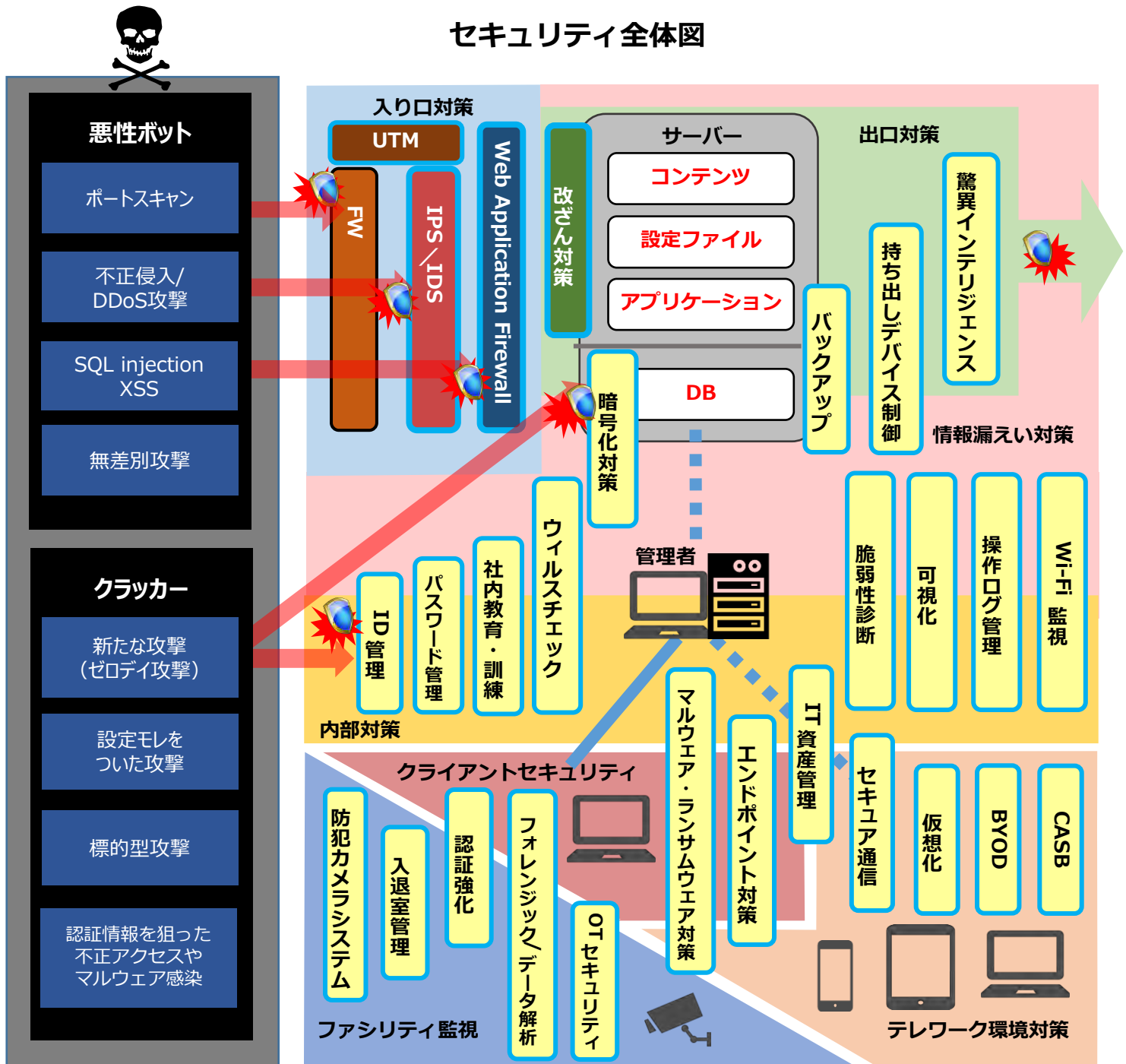
ver1.0

日々進化し高度化するサイバー攻撃

サイバー攻撃は日々高度化、巧妙化しており、サイバー攻撃によって純利益の半分以上を失う企業が出るなど、深刻な影響を引き起こす事件が発生しております。さらには、攻撃の踏み台にされて外部へ攻撃をしてしまうだけでなく、国の安全 保障上重要な技術情報の流出、重要インフラにおける供給停止など、国民の社会生活に重大な影響を及ぼす可能性のある攻撃も発生しており、その脅威は年々増加傾向にあります。そしてサイバーセキュリティは経営問題と位置づけられる時代となり、セキュリティ対策の実施を「コスト」と捉えるのではなく、将来の事業活動・成長に必須なものと位置づけて「投資」と捉えることが重要です。

こうした中、独立系DCプロバイダーのアイネットでは、多くの知見に基づき、企業が抱えるセキュリティ対策強化に向けたトータルセキュリティソリューションをご提供、課題解決までをサポート致します。

セキュリティ全体図



青枠はご提供可能なソリューション

2022年4月1日現在

カテゴリ		サービス名	掲載頁
マルウェア・ランサムウェア対策	インターネット分離	HP Sure Click Enterprise	P4
	次世代エンドポイント	EPP EDR Carbon Black Defense	P5
	標的型攻撃対策	Eメールセキュリティ FortiMailCloud	P6
入り口対策	UTM	Forti Gate	P7
	DDoS対策	IPS・IDS Deep Security as a Service	P8
	不正アクセス対策	WAF (Web Application Firewall) WebARGUSFortify	P9
脆弱性診断	脆弱性診断	手動診断/機械診断	P10
	コンサルティング	セキュリティコンサルティング	P11
内部インシデント対策	ファイルバックアップ	Infinity Dream Backup	P12
可視化・見える化	IT資産管理	Lan Scope	P13
	リモートアクセス	BOMGAR	P14
	パスワード管理	Password Safe	P15
	操作ログ管理	MyLogStar	P16
	SIEM	Alog	P17
出口対策	持ち出しデバイス管理	DeviceLock	P18
改ざん検知	システム改ざん瞬間検知・瞬間復旧	SECURE-ARGUS	P19
情報漏えい対策	ファイル暗号化	DataClasys	P20
暗号化対策	クライアントセキュリティ	セキュア moconavi	P21
		セキュア通信 remote.it	P22
		CASB Forcepoint	P23
ファシリティ制御セキュリティ	OTセキュリティ	Guardian	P24
	顔認証	FreeID	P25
	セキュリティカメラ	セキュリティカメラ	P26
	N V R	N V R	P27

入り口対策

DDoS対策

クラウド型

低コストでハイレベルなセキュリティを実現！

クラウド型総合サーバセキュリティサービス

TrendMicro Cloud One – Workload Security



充実したクラウド型の多重防御セキュリティサービス

Trend Micro Cloud One-Workload Securityは、オンプレミス製品『Trend Micro Deep Security』のクラウド版サービスです。ウェブコンソールを用いてWorkload Security Agentをインストールするだけで、サーバの管理運用が可能。そのためお客様の環境に独自の管理サーバを用意する必要がありません。サーバのセキュリティ対策に必要なハイレベルな機能を複数搭載しており、さまざまな手法を組み合わせたサーバ攻撃でも段階に応じたセキュリティ機能で驚異をブロックします。

迅速に脆弱性攻撃をブロック



IPS/IDSルールを適用することで、正規パッチが完成するまでの間、サーバの脆弱性を素早く保護します。

複数機能で多層防御を実現



複数機能を搭載することで、1サービスで攻撃フェーズに応じた多層防御を実現します。

簡単にサービス導入・運用可能

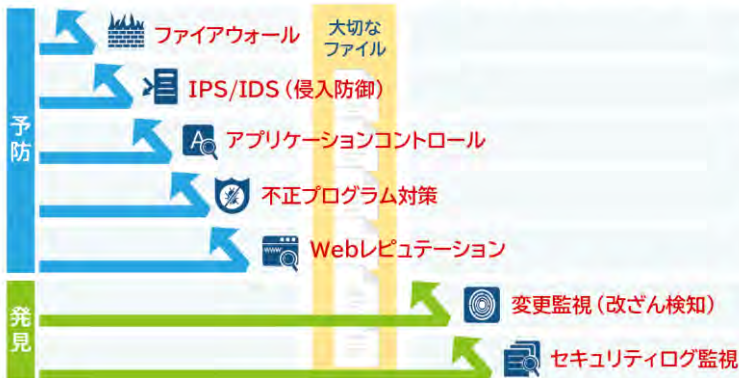


導入はウェブコンソールを用いて Workload Security Agent をインストールするだけ。誰でも簡単に運用できます。

複数機能で攻撃フェーズに応じた多層防御を実現

さまざまな手法を組み合わせたサーバ攻撃でも、段階に応じたセキュリティ機能で驚異をブロック。万が一侵入された場合に備え、攻撃に気付いて防御する発見的な対策を搭載しています。

■ 予防型対策に加え攻撃に気づいて防御する発見的対策を搭載



- ファイアウォール**
DoS攻撃など不正な通信を防御
- IPS/IDS (侵入防御)**
仮想パッチでOSやアプリケーションの脆弱性を保護
- アプリケーションコントロール**
ホスト上で実行されるアプリケーションを監視
- 不正プログラム対策**
リアルタイムにウイルスを検索
- Webレピュテーション**
不正なURLへの接続を防止
- 変更監視 (改ざん検知)**
ファイルやポート等の変更を監視
- セキュリティログ監視**
OSやミドルウェアのセキュリティイベントを集中監視

料金 (税抜)

30日間
無料お試し

Windows 2000、2003、2008、
2012、2016、RedHat、SuSE Linux、
Solaris HP-UX*、AIX*

月額費
15,000円/1Agent

年額契約については
別途ご相談ください。

出口対策

SaaS型

サーバレス

コンテンツ改ざん被害に 終止符を。



日々高度化するサイバー攻撃、改ざん被害は深刻に

日本国内の企業・組織のウェブサイトがサイバー攻撃の踏み台として悪用されている事例や、改ざんされたウェブサイトへアクセスしたユーザーに対してマルウェア感染させる事例が、JPCERT/CCや独立行政法人情報処理推進機構（IPA）より注意喚起されています。セキュリティ対策に100%はありません。多様化するサイバー攻撃に、どう対処すればよいのでしょうか？

SECURE-ARGUS でできること



サイトの改ざんをリアルタイム検知



0.1秒未満で、瞬間復旧



アラート通知

監視モードON/OFF
監視対象変更

監視設定保存

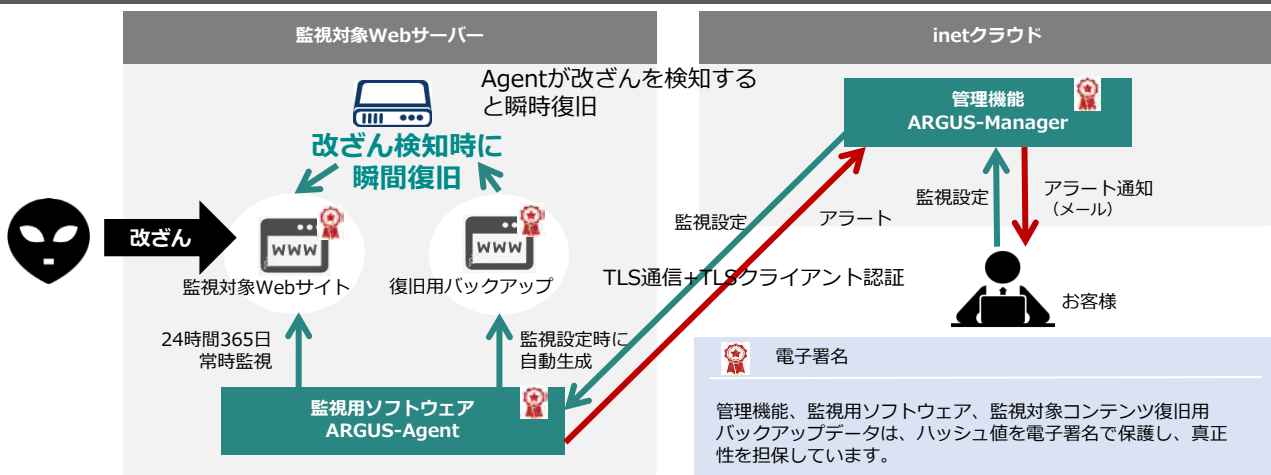


証拠保全

稼働監視

ログダウンロード

SECURE-ARGUS の改ざん検知・復旧方法



料金 (税抜)

初期費
0円

月額費
34,000円/1Agent

インストール代行費
50,000円/1Agent

監視初期設定費
個別お見積り