商品・サービスの構成

モダナイズ	DX推進に向けて、レガシー化したシステムを最新技術をベースとしたシステムへ刷新
DX&AI	現場業務が抱えるさまざまな課題をITにより解決 人手で対応していた監視・確認業務にAIを適用
ネットワーク&セキュリティ	セキュリティ侵害の脅威から守るために、最新テクノロジーを活用した多層型の防御ソリューションを提供
マネージドサービス	ITシステムに必要な機器・ソフトウェアの導入・管理・運用などの業務に対し、「マネージドサービス」を提供

各サービスの詳細は下記URLよりご確認下さい。

https://www.hitachi-systems-es.co.jp/service/index.html

ネットワーク&セキュリティ 主なソリューション

お客さまのご要望	対象カテゴリ	解決ソリューション
サーバーやPC等の末端機器に対する情報漏えい防止/セキリティ対策 ・低コストで安心・快適なリモートワーク環境 ・機密情報の漏えい防止 ・メール誤送信の防止 ・マルウェア対策 ・マルウェア脅威検知と追跡	**エンドポイントセキュリティ**	ZENMU Virtual Drive SKYSEA Client View導入ソリューション グローバルセキュアデータ転送サービス 秘密分散 フォー メール 秘密分散 フォー ビデオ メール誤送信対策ツール WISE Alert メール誤送信防止ツール適用サービス マルウェア対策サービス AppGuard エンドポイントセキュリティ対策 FortiEDR メールセキュリティ対策ソリューション セキュアFAT端末ソリューション
ネットワークに接続されているシステム全体をさまざまな脅威から保護 ・IDの統合管理 ・快適かつ安全、堅ろうなネットワーク環境の構築 ・脆弱性診断 ・ランサムウェア対策	**ネットワークセキュリティ**	ID管理 – LDAP Manager・Extic導入サービス インターネット接続機能（vUTM）導入支援サービス ネットワークセキュリティソリューション（Fortinet） ゼロトラストネットワーク FortiGate ZTNA Trend Micro Deep Security導入サービス Trend Micro Webアクセスセキュリティ強化サービス Microsoft Azure Sentinel構築サービス 統合ログ管理機能 AMIYA AlogEVA適用サービス セキュリティ監視導入支援サービス LANシステム 脆弱性診断サービス Webサーバー脆弱性診断サービス GRED Webセキュリティソリューション バックアップシステム ランサムウェア対策 Rubrik
利用者限定の機器やサービスへのログイン厳密化 ・2つ以上の要素でログイン認証	**認証**	多要素認証 - EVEMA - 多要素認証 - Themis - オフィスITの認証セキュリティSmartSESAME

株式会社 日立システムズエンジニアリングサービス

本社：〒220-8132 横浜市西区みなとみらい2-2-1
横浜ランドマークタワー32階

商品のお問い合わせはこちらまで
www.hitachi-systems-es.co.jp

※本カタログに記載されている会社名、製品名は、それぞれの会社の登録商標、または商標です。
※本カタログに記載されている内容、仕様については、予告なく変更する場合があります。
※本製品を輸出する場合には、外国為替および外国貿易法ならびに、米国の輸出管理関連法規などの規制をご確認のうえ、必要な手続きをおとりください。
なお、ご不明な場合は、当社営業にお問い合わせください。

SS-2301 | 2023.12
Printed In Japan

HITACHI
Inspire the Next

ネットワーク&セキュリティ

セキュリティ侵害の脅威から守るために、
最新テクノロジーを活用した多層型の防御ソリューションを提供

株式会社 日立システムズエンジニアリングサービス

エンドポイントセキュリティ：サーバーやPCなどの末端機器に対する情報漏えい防止/セキュリティ対策

クライアント端末セキュア化

低コストで安全・快適なリモートワークを実現します

■ZENMU Virtual Drive

1. 低コストで導入可能なFAT端末
リモートワークがスタンダードとなり、VDI接続はさまざまな問題が顕在化しています。
（ネットワーク帯域不足でPCの動作が遅くなる。新たなVDI環境やネットワーク帯域の増強は膨大なコストがかかる。など）
本製品はユーザーデータ以外はローカル環境を利用するため、PC本来のパフォーマンスを生かすことができます。

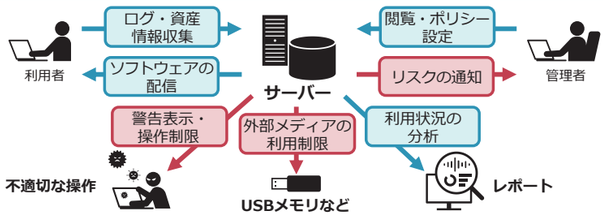
2. PC紛失時に、クラウドでデータを無効化
・ZENMU Virtual Driveはファイルのデータを無意味化し、PCとクラウドに分散保管
・クラウドの分散ファイルをPC上の分散ファイルと結合することで、ユーザーデータを復合しファイルの編集が可能
・PC紛失時には、分散ファイルの利用を無効化することで情報漏えいを防止

未接続時は、ドライブにアクセスできない
データとして無効な状態

クラウド上の分散ファイルを結合し
仮想ドライブを生成

■SKYSEA Client View導入ソリューション

・PCやサーバーなどのハードウェア情報、ソフトウェア情報、プリンターや外部メディアなどの機器情報などを一元管理
・情報資産の利用状況を把握し、セキュリティ対策や情報資産を有効に活用可能



秘密分散によるセキュア化

データの分割保管/送信で情報漏えいを防ぎます

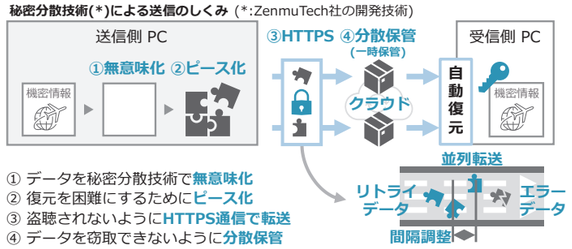
■グローバルセキュアデータ転送サービス

・秘密分散技術でデータ送信時の情報漏えいやネット環境の不安を解決

■秘密分散 フォー メール

・送信側Outlookにアドインするだけで、脱PPAPを実現
受信者はダウンロードURLからメール復元が可能
（アドインなしユーザーのケース）
・メール誤送信に気付いた時は受信側がダウンロード前であれば送信キャンセルが可能
・クラウドへの分散保管時にウイルスチェックを実施

秘密分散技術(*)による送信のしくみ（*:ZenmuTech社の開発技術）



① データを秘密分散技術で**無意味化**
② 復元を困難にするために**ピース化**
③ 盗聴されないように**HTTPS通信で転送**
④ データを窃取できないように**分散保管**

マルウェア対策

ゼロトラストルールが未知のウイルス・マルウェア攻撃を防ぎます

■マルウェア対策サービス AppGuard

1. マルウェア起動阻止機能
なりすましメールや偽サイト経由で端末に侵入したランサムウェアなどのマルウェアが起動することを阻止します。侵入されても発症しない、未知の脅威から端末を守ります。

2. 改ざん処理防止機能
悪用される可能性があるアプリケーションに対して３つの制御
（レジストリ／システムスペース／メモリへのアクセス制御）を課すことで不正アクセスを成立させません。起動したプロセスが侵害されていたとしてもシステムへの改ざん行為を制御します。

3. プライベートフォルダ
サイバー攻撃で利用される可能性が高いアプリケーションからのアクセスをフォルダ毎に遮断します。
個人情報や機密情報の格納フォルダに適用することで、ランサムウェアから重要なファイルを守ります。

ネットワークセキュリティ：ネットワークに接続されているシステム全体をさまざまな脅威から保護

セキュアなネットワーク構築

快適かつ安心、堅ろうなネットワーク環境を構築します

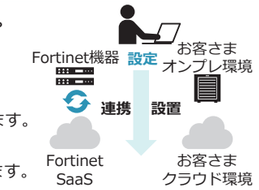
■ネットワークセキュリティソリューション(Fortinet)

お客さまの要件を確認し、Fortinet社のセキュアなネットワーク機器と維持保守サービスを提供します。

1. Fortinet機器提供サービス
FortiGateをはじめ、Fortinet社のネットワークセキュリティ機器を提供します。

2. Fortinet SaaS接続サービス
Fortinet社が提供するクラウドサービスをお客さまのクラウド環境で利用できるようセットアップします。

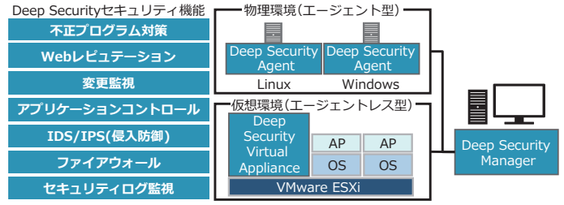
3. Fortinet 機器 プレ設定・導入サービス
お客さま要望をヒアリング、機器納入前にお客さま環境に合わせた機器設定、事前テストを実施します。



■Trend Micro Deep Security導入サービス

オンプレミスとクラウド、まとめてセキュリティリスクを低減します。
攻撃者の侵入を防ぎ、重要なデータを保護するため、お客さまのサーバー環境に適したTrend Micro社のセキュリティ機能を当社エンジニアが提案します。

・変化するセキュリティ要件に合わせて拡張可能
お客さまにフィットする機能を提案
・物理・仮想・クラウド環境を共有ポリシーで管理
運用負荷を軽減



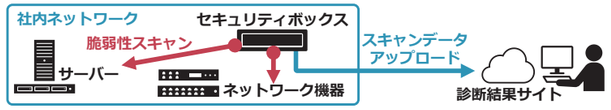
脆弱性診断

社内ネットワークの機器や公開Webサーバーの安全性を診断します

■LANシステム脆弱性診断サービス

社内ネットワークに接続されている多種多様なIP機器を診断します。

①診断装置であるセキュリティボックスを社内ネットワークに接続
②クラウド上のセキュリティ診断結果サイトで結果レポートと脆弱性の改善方法を確認



■Webサーバー脆弱性診断サービス

クラウドサービスでWebサーバーを診断します。ネットワーク環境の変更や特別なツールは不要です。

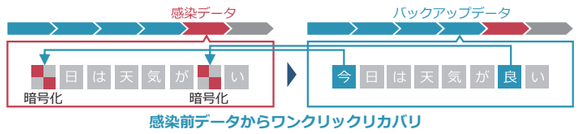
①クラウド上から公開Webサーバーを診断
②クラウド上のセキュリティ診断結果サイトで結果レポートを確認
③Webアプリケーションとプラットフォームの診断を統合
④脆弱性ごとの再診断により、対策の確認が容易

ランサムウェア対策

改ざん不可なバックアップシステム(イミュータブルファイルシステム)によりサイバー攻撃に対処できます

■バックアップシステム ランサムウェア対策 Rubrik

イミュータブル(変更不可)ファイルシステム
①認証されたAPI 経由でのみ書き込みを許可
②追記のみ可能で上書き不可なアーキテクチャ
③フィンガープリント(指紋)情報で変更がないことを保証



認証：利用者が限定されている機器やサービスへのログインを厳密化

多要素認証

生体認証（指紋、顔、静脈）やICカードの利用で安心安全なITシステムを実現します

・PCログオン、VDI、業務アプリやクラウドサービス他の認証を強化
・お客さまの業務に合わせて認証方式を選択可能
・認証基盤の構築、運用、サポートは当社がワンストップで提供