北陸電力グループ
北電情報システムサービス株式会社
HISS Hokuden Information System Service Company,Inc.

テレワーク推進ソリューション

https://www.hiss.co.jp/

クラウド/セキュリティ ソリューションマップ

インターネット

SaaS
・BOX
・Microsoft 365

IaaS/PaaS
・AWS　・Microsoft Azure

インターネット接続
データセンターから高品質な
インターネットアクセス【FIT-
Cloudインターネット】

Microsoft365導入・運用
柔軟な働き方とセキュリティを両立する
コミュニケーションプラットフォームを導入
【SharePoint(ポータルサイト)】【Exchange Online】
【Teams】
【グループスケジュール・階層型アドレス帳などアドオン】

BOX導入・運用
高セキュリティ、容量無制限の
クラウドストレージを導入
Entra IDとのSSO/データ移行
/組織改正・人事異動への対応

生成AI構築サービス
Azure OpenAIを活用してセ
キュリティの高いオリジナルな生
成AI環境を構築

ログ収集・分析
セキュリティログの収集・分析・
可視化・アラート・自動対応
【Sentinel/LogAnalytics】

SSE(Security Service Edge)
SWG、CASB/DLP、ZTNAなどの要素を組み合わせて、
ゼロトラストネットワークを実現
【Prisma Access】【Netskope】【CATO Network】

ID管理(IDaaS/ID連携)
システムやサービスを利用するIDやパスワード
などのアカウント管理オンプレADとの連携
【Entra ID/Entra Connect】

ローカルブレイクアウト

閉域網接続
提携データセンターや拠点から
パブリッククラウドや提携SaaSに
セキュアかつ低遅延で閉域接続
【FIT-OCX】

AWS導入・運用
AWS導入～保守のトータルサービス
【FIT-Cloud Assist】【First-OPS】

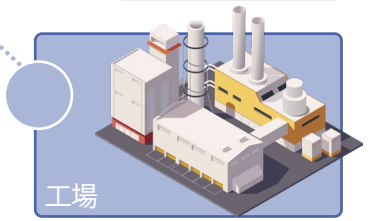
IoT/OT
IoT/OT環境の可視化
【Nozomi Networks】

SD-WAN/SASE　IDaaS　閉域/VPN

リモートWEBアクセス
社内システムへの
安全なアクセス
【Entra App Proxy】

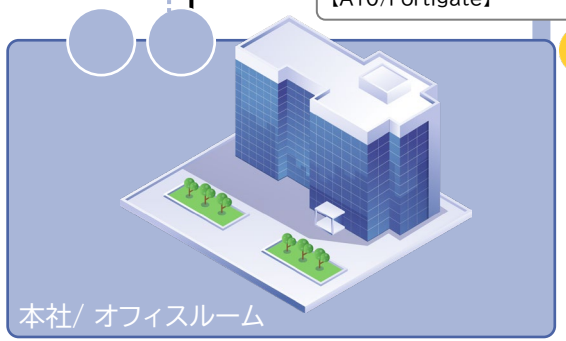
リモートアクセス(VDI)
社内ネットワークへの
安全なアクセス
【Azure Virtual Desktop】

ローカルブレークアウト
検査不要な宛先は直接クラウドへ
【A10/Fortigate】



EDR
端末を監視し、不審な振る舞いを
検知し、未知の脅威にも対応
【CrowdStrike】
【Cybereason】
【Defender for Endpoint】

EPP
マルウェア、ランサムウェア、
ウイルスなど既知の脅威から
端末を保護
【Symantec Endpoint
Protection】
【ApexOne】



社内ネットワーク
お客様環境に最適な方式・
機種にてご提案
【FIT-WiFi】【Arista】
【Cisco】【Aruba】
【Apresia】

FW/VPN導入・運用
導入～運用まで
脆弱性対応が必須
【FIT-Cloud VPN】
【Fortigate】

IT基盤構築
各種サーバおよびサービスの
設計、構築、移行
・ADサーバ
・ファイルサーバ
（FIT-Cloudストレージ）
・メールサーバ
・DNSサーバ
・Proxyサーバ

MDM・MAM
モバイルデバイスの
管理BYOD対応の
ためのアプリ単位
での管理も可能
【Intune】

eメールセキュリティ
最も危険なeメールの
セキュリティを強化
【Hennge One】
【MatrixScan】
【Guardianwall】

メール誤送信対策
誤操作による
情報漏洩を防止
【SafeAttach】
【Hennge One】

資産管理
資産の可視化とセキュリティ強化
(情報漏洩・内部統制)を同時に実
現【AssetView】【SkySea】

機器監視
サーバ・ネットワーク
の統合監視
【FIT監視サービス】
【Zabbix】

ハウジングクラウドサービス
【FIT-iDC】
【FIT-Cloud】

バックアップ
災害やセキュリティ侵害から
データを守る
【FIT-Cloudバックアップ
サービス】
【Arcserve】【Veeam】

仮想化基盤
新規導入やVMwareからの移行
【Nutanix】【Nutanix Files】

●クラウド系　●ネットワーク系　●セキュリティ系　●その他

MDM・MAM導入ソリューション

ポイント	プロダクト名
➢ 個人端末と企業データを分離管理できるため、業務用デバイスだけではなくBYODでも安全な業務が可能です。 ➢ 紛失端末への遠隔データ消去や非準拠デバイスのアクセス遮断などにより機密情報の漏えいを防止します。 ➢ 5,000名規模の企業への導入・運用実績にもとづき、お客さまにニーズに最適な導入方法をご提案します。	Microsoft Intune

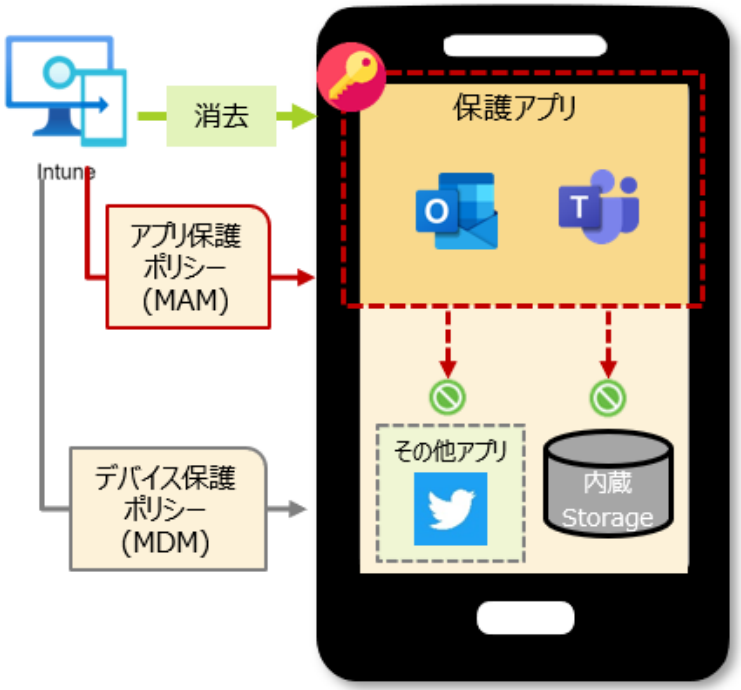
■ Intuneでできるセキュリティ対策

機能	役割	内容
モバイルデバイス管理(MDM)		
デバイス登録・情報収集	脱獄対策	デバイスを管理下に登録および情報収集を実施
デバイス操作制限		特定の操作(デバイス名変更・USB接続禁止等)を制御
リモートロック・リモートワイプ	紛失対策/盗難対策	遠隔からデバイスのロックおよびワイプを実施
位置情報取得		デバイスの位置情報取得
モバイルアプリケーション管理(MAM)		
業務データの持ち出し制限	データ漏洩対策	管理されていないデバイスからのアクセスを拒否
コピー、転送、保存制限		許可されたアプリケーション以外へのコピー、転送、保存を制御
アプリPIN		管理アプリへのアクセス時にPIN入力を要求
データ暗号化		組織データの暗号化を実施
業務データのワイプ		アプリケーション単位で業務データのワイプ(削除)を実施

■ 対策例

リモートによるデータ削除機能

Intune によるアプリケーション保護(MAM)では、管理アプリに直接ポリシーが適用され、内蔵ストレージや管理アプリ外への業務データ保管を制限します。
また、アプリ単位でリモートでのデータ消去が可能であり、BYODデバイスを用いて安全に業務を行うことができます。



北電情報システムサービス株式会社　営業部

〒930-0004 富山市桜橋通り3－1富山電気ビル2F
TEL:076-444-2310　E-mail:contact@hiss.co.jp