SECURITY SOLUTIONS

ベル・データ セキュリティソリューション カタログ

ベル・データ株式会社

https://www.belldata.com/

●製品、サービス、サポート内容の詳細は、上記までお問い合わせ下さい。
●製品の仕様、機能は予告なく変更する場合がありますので、ご了承下さい。
●会社名、製品名、サービス名等は、それぞれ各社の商標または登録商標です。

ベル・データ株式会社はプライバシーマーク認定事業者です。

20181025

https://www.belldata.com

セキュリティ ソリューション MAP

近年セキュリティ強化は企業の喫緊の課題となっており、もしセキュリティを原因とするトラブルが起こった場合には企業の屋台骨を揺るがすことになりかねません。また、セキュリティ対策と一口に言ってもその対象は非常に広範囲に及び、何から始めればいいのかが分かりにくくなっているのも現状です。
ベル・データでは「多層防御」という考えのもと、お客様の課題、ニーズに合わせて最適なセキュリティソリューションをご案内いたします。

メール対策

セキュアメール
- CYBERMAILΣ
ビジネス向けクラウドメール

メール無害化
- CYBERMAILΣ-ST
メール無害化機能付きクラウド

スパムメール対策
- Hosted Email Security
クラウドサンドボックス付
アンチウィルス / スパム MTA

メールアーカイブ
- MAILBASEΣ
コンプライアンス / 監査対応クラウドメールアーカイブ

<クラウドメール>

出入口対策

重要データの外部流出を防止
（出口対策）

通信のセキュリティ監査
- Deep Discovery Inspector
・高精度なセキュリティ監視センサ
・内蔵サンドボックス解析

統合 UTM
- WatchGuard
・インターネットの出入り口で企業に必要なセキュリティ機能を集約
・グラフィカルなレポートで複雑なセキュリティを「見える化」

不正な侵入を防止

● 多層防御の必要性

IPA（独立行政法人 情報処理推進機構）は、企業や組織の情報漏えい、金銭搾取などの被害の増加に伴い、特定のセキュリティ対策製品の利用だけでは、それらの被害を防ぐことが困難になってきている場合があるためウィルスによる攻撃、感染を想定した「多層防御」の必要性を説いています。「多層防御」のポイントは 4 点。
「ウィルス感染リスクの低減」「重要業務を行う端末やネットワークの分離」「重要情報が保存されているサーバーでの制限」「事後対応の準備」

公開サーバー対策（外部公開サーバーのサイバー攻撃対策）

<公開サーバー全般>

サーバー多層防御
- DeepSecurity
サーバー向け総合セキュリティ対策

<Web サーバー>

Web 改ざん対策
- WebARGUS
Web 改ざんを瞬間検知改ざんの瞬間復旧

内部対策（マルウェア感染対策・情報漏えい対策）

パッチ管理 - WSUS
・パッチ適用状況の把握
・Windows10 用メジャーアップデート管理

・効率的なパッチ適用
・WAN 回線の効率化

通信のセキュリティ監査 - Deep DiscoveryInspector
・高精度なセキュリティ監視センサ
・内蔵サンドボックス解析

バックアップ集中管理

<ActiveDirectry>
ポリシー制御

<サーバー全般>
<ファイルサーバー>
<NAS>

PC バックアップ
- Connected
・PC データ保護
・マルウェア
・ランサムウェア
感染対策

ディスク暗号化
- BitLoker
HDD の暗号化

マルウェア対策
- Webroot
・マルウェア
・ランサムウェア対策
・クラウド管理型

- WatchGuard TDR
Watch Guard UTM 製品と連携するエンドポイントマルウェア対策

［エンドポイントセキュリティ］

ポリシー管理
- Active Directry
・ID/ パスワード管理
・セキュリティポリシーの一元管理

IT 資産管
- AssetView
・クライアント操作ログ
・デバイス制御
・アプリケーション配布
・脆弱性対策管理 など

サーバー多層防御
- DeepSecurity
サーバー向け総合セキュリティ対策

サーバログ管理
- AlogConverter
ファイルサーバーアクセスログ管理

データ保護
- ARCServe
・サーバデータ保護
・マルウェア / ランサムウェア感染対策

［サーバーセキュリティ］

メール対策

セキュアメール　メール無害化

CYBERMAIL Σ

クラウド型セキュアメールサービス。
Web メール、ウイルス、スパムチェック標準装備。
その他豊富なオプション製品があります。

CYBERMAIL Σ-ST

クラウド型メール無害化サービス。
メール本文の無害化に加えて、添付ファイル無害化も提供出来る最新メールセキュリティ製品です。

スパムメール対策

Hosted Email Security

ポリシーカスタマイズが容易な MTA サービス。迷惑メール・スパムメール・メールのアンチウィルス対策に最適です。

出入口対策製品

統合 UTM

WatchGuard Firebox

高性能」、「シンプル」、「低コスト」を兼ね備えたセキュリティアプライアンス。
複数のセキュリティ機能で、巧妙化したマルウェアに対処不正なトラフィックやアクセスを可視化します。

出入口・内部対策製品

通信のセキュリティ監査

Deep Discovery Inspector

カスタムサンドボックスを内蔵した、セキュリティセンサ。ミラーポート接続なので、通信環境を変更せずに導入可能。隠れた脅威のあぶりだしに最適です。入口、出口、内部対策が 1 台で 対応可能なオールインワン製品です。

公開サーバー対策製品

Web 改ざん対策　サーバ向け

WebARGUS

Web サイトの改ざんを瞬時に検知して、1 秒未満で瞬間復旧する改ざん検知ソリューションです。
APMG の電子署名技術を駆使した高度な改ざん検知を実現します。

公開・内部対策製品

サーバ多層防御　サーバ向け

Deep Security

“脆弱性をついた攻撃”や“Web の改ざん”“情報漏洩”等、サーバーを取り巻くサイバー攻撃が多様化する中、サーバの多層防御をオールインワンで対応できる製品です。

内部対策製品

PC バックアップ　エンドポイント

Connected Backup

完全に自動化された PC データバックアップシステム。
PC リプレースの運用対策から、ランサムウェア被害時の復旧にも利用可能。

マルウェア対策　エンドポイント

WatchGuard TDR

Thread Detection & Responce（TDR）で提供する HostRansomware Prevention（HRP）では、ランサムウェアによる攻撃を検出し未然に防止します。

パッチ管理　エンドポイント

WSUS

WindowsUpdate の配信管理を行うための標準ツール。
Windows10 のメジャーアップデートの管理に必須となる製品です。

マルウェア対策　エンドポイント

Webroot

クラウド型振る舞い検知により、未知のマルウェアも隔離・駆除する次世代型エンドポイント対策ツールです。

ディスク暗号化　エンドポイント

BitLocker

Windows 標準の HDD 暗号化ツール。
ActiveDirecrty と連携して集中管理が可能です。

ポリシー管理　エンドポイント

ActiveDirectry

クライアント PC の ID やポリシーを一元管理するための、Microsoft 標準のスタンダード管理基盤です。

IT 資産管理　エンドポイント

Assetview

資産管理だけではなく、エンドポイントの多層防御をワンストップで対応できるパッケージ製品です。
必要な機能を選択して導入する事が可能となり低コストでの導入が可能です。

● 主なセキュリティ対策機能

- PC 操作ログ管理
- 個人情報検索
- デバイス制御
- ファイル制御・暗号化
- 脆弱性対策
- 不正 PC 遮断
- Web フィルタリング
- ID 監査

サーバログ管理　サーバ向け

ALogConveter

ファイルサーバー内における操作内容を時系列かつ連続的に「いつ」・「誰が」・「何をした」を記録管理する証跡管理ソリューションです。

データ保護　サーバ向け

ARCServe

万が一のランサムウェアの感染に備え適切なバックアップ取得が必要です。ARCServe は高度なバックアップ機能を搭載したスタンダード製品です。

外部・内部からの脅威を整理

セキュリティ ソリューション比較表

外部脅威

	製品名	悪意による脅威						環境による脅威	
		サイバー攻撃	マルウェア	不正アクセス	改ざん	DDoS攻撃	盗難	自然災害 火災	停電
対策・対応	CYBERMAIL Σ	●	●				●	●	●
	Hosted Email Security	●	●					●	●
	WatchGuard　Firebox	●	●	●	●	●			
	Deep Security	●	●	●	●	●			
	WebARGUS			●	●				
	Deep Discovery Inspector	●	●	●	●	●			
	Connected Backup		●				●	●	●
	WSUS	●		●					
	ALogConveter								
	WatchGuard TDR	●	●						
	Assetview	●	●	●	●	●	●		
	Webroot	●	●	●					
	BitLocker						●		
	ActiveDirectry								
	ARCServe		●				●	●	●

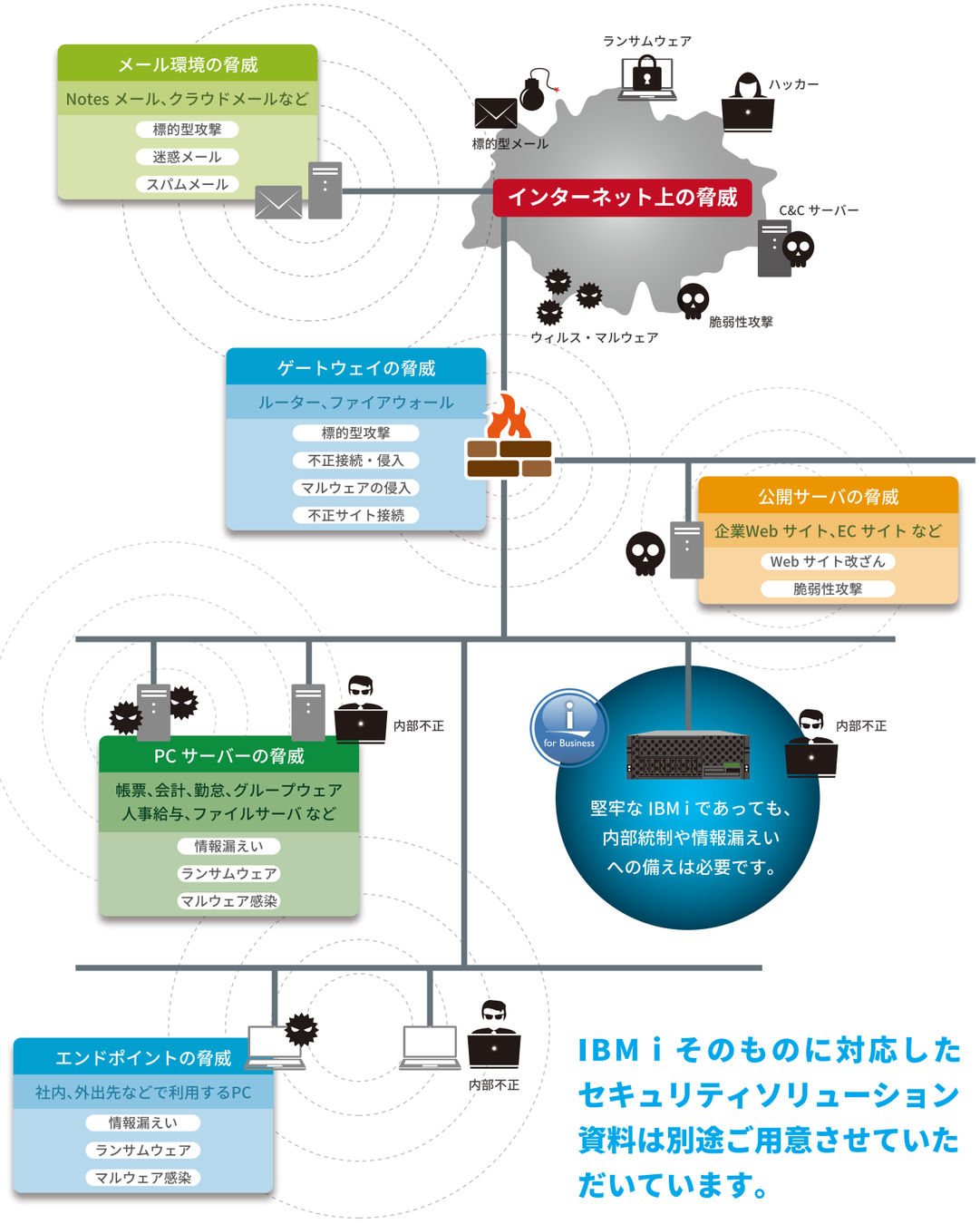
内部脅威

	製品名	故意による脅威				過失による脅威		
		不正持ち出し	不正操作	改ざん	物理的破損	紛失盗難	誤操作	設定ミス
対策・対応	CYBERMAIL Σ	●				●		
	Hosted Email Security							
	WatchGuard　Firebox							
	Deep Security		●	●			●	
	WebARGUS		●	●			●	●
	Deep Discovery Inspector	●	●	●				
	Connected Backup		●	●	●	●	●	●
	WSUS						●	
	ALogConveter	●	●	●			●	
	WatchGuard TDR							
	Assetview	●	●	●		●	●	●
	Webroot	●	●					
	BitLocker		●			●		
	ActiveDirectry		●			●	●	●
	ARCServe		●	●	●	●	●	●

IBM i のセキュリティを考える

IBM i にも迫るセキュリティ脅威

IBM i は堅牢でも周辺の危機はセキュリティの脅威にさらされており、用途に応じた対策が必要です。



IBM i そのものに対応した セキュリティソリューション 資料は別途ご用意させていただいています。