「クラウドセキュリティ強化ソリューション」の主な取り扱い製品・サービス

最新の情報は当社ホームページをご覧ください。

共通		
包括的セキュリティ対策	クラウドセキュリティコンサルティング	クラウド利用における情報セキュリティの現状を明確にし、主にマネジメント面での対策方針立案を支援
SaaS		
❶ アカウント・権限情報		
CASB	Bitglass	シャドーITの可視化やクラウドサービスの利用状況把握・制御により、セキュアなクラウドサービスの利用を実現
	Netskope	柔軟なポリシー制御やリアルタイム制御で、セキュアなクラウドサービスの利用を実現
	McAfee MVISION Unified Cloud Edge	不正ログインの可能性や通常と異なる操作などの可視化、機密データの保護などによりセキュリティを強化
IDaaS	Okta Identity Cloud	システムごとに異なるID・パスワードを一つに統合し、クラウドを含む複数のWebシステムなどに対し1回のログインで利用を許可
二要素認証	Entrust IdentityGuard	乱数表やワンタイムパスワードなどで本人認証を強化し、不正アクセスやなりすましを防止
❷ ユーザーデータ		
ファイル暗号化	Credeon Cloud Data Protection for OneDrive	クラウドサービスへのファイルアップロード時、専用ブラウザーによりファイルを自動的に暗号化
PCのハードディスク暗号化	秘文 Data Encryption	PCのハードディスクや記録メディア、ファイルサーバー上のフォルダを暗号化
マルウェア対策	Trend Micro Cloud App Security™	Microsoft 365などのクラウドサービスを利用する際のセキュリティを強化し、ランサムウェアなどのマルウェアによる脅威から保護
	FireEye Email Threat Prevention	メールの添付ファイルや本文中のURLを、クラウド上の仮想実行環境で解析
DLP ・ファイル暗号化	Bitglass	クラウドサービスからのダウンロードファイルの自動暗号化を実現
❸ 通信路・通信データ		
VPN強制接続	秘文 Device Control	社外からのアクセスはVPN利用を強制し、通信データの盗聴対策や社内セキュリティ対策の利用を徹底
クラウド型Webプロキシ	Zscaler(Zscaler Internet Access)	社内外問わず、Webアクセスに対し共通のポリシーを適用し、セキュリティを強化
SSLインサイト・不正なクラウド利用対策	A10 Networks Thunder/AXシリーズ	マルチテナントのクラウドサービスにおいて、自社テナントのみへのアクセスを許可
SSLインサイト	Array APVシリーズ	マルチテナントのクラウドサービスにおいて、SSL暗号化通信を可視化
インターネットブレイクアウト	Fortinet セキュアSD-WAN	特定のアプリケーションのみ直接インターネットへアクセスさせることで、プロキシや回線の負荷を軽減
セキュアなリモートアクセス	Zscaler(Zscaler Private Access)	仮想アプライアンスの導入により、社内環境やプライベートクラウドなどへのセキュアなリモートアクセスを実現
PaaS / IaaS		
❶ アカウント・権限情報		
特権ID管理	ESS AdminControl	特権IDの貸出・返却などのID管理プロセスを自動化し、効率的かつ安全な特権ID管理を実現
	パワーセキュリティ	エージェントレスで、既存のシステムや特権ID運用に影響を与えず、特権ID管理や証跡管理を実現
❷ ユーザーデータ		
ファイル暗号化	Credeon Cloud Data Protection	専用ブラウザー利用により、クラウドサービスへアップロードするファイルを自動で暗号化するSDKを提供
❸ 通信路・通信データ		
VPN	Pulse Connect Secureシリーズ	社内環境やクラウド環境へ、安全かつ快適なSSL-VPNリモートアクセスを実現
	ArrayAGシリーズ	SSL-VPNにより、リモートアクセスやエクストラネットを実現
セキュアなリモートアクセス	Zscaler(Zscaler Private Access)	仮想アプライアンスの導入により、社内環境やプライベートクラウドなどへのセキュアなリモートアクセスを実現
❹ アプリケーション		
WAF	Imperva Incapsula	脆弱性を悪用した攻撃やDDoS攻撃から、設置されたWebサーバーを防御
改ざん検知	Tripwire Enterprise	サーバー、ネットワーク機器、データベースなどで構成されるインフラに対し改ざんを検知
Bot対策	PerimeterX Bot Defender	人間かBotかをAIが高い精度で識別し、Botと判断したときにはCAPTCHAを表示してアクセスをブロック
❺ ミドルウェア		
仮想パッチ (IPS)	Trend Micro Cloud One™ - Workload Security	OS、ミドルウェアの脆弱性防御のための仮想パッチ (IPS) を配布
データベース監査	PISO	システムに負荷をかけることなくデータベースへのアクセスログを記録し、不正アクセスを監視
❻ 仮想リソース		
CWPP	クラウドワークロードセキュリティサービス	IT部門に未申告で利用されているPaaS/IaaSを検知し利用者まで特定
ホスト型IDS・IPS	Trend Micro Cloud One™ - Workload Security	サーバーに必要なセキュリティ機能をオールインワンでクラウド上にて提供し、ホスト型IDS・IPSを実現
仮想化ファイアウォール	Fortinet VM-Series	マルウェアなどの脅威からアプリケーションやデータを保護し、ユーザーごとのアクセス制限も実現
	Palo Alto Networks VM-Series	利用できるアプリケーションやURLをユーザーごとに限定するなど、きめ細かな制御が可能
	Juniper Networks vSRX	ルーティング、アプリケーション識別、制御などネットワークセキュリティに求められるさまざまな機能を提供

＊❶～❻は中面の各セキュリティリスクと対策と対応しています。

株式会社 日立ソリューションズ
www.hitachi-solutions.co.jp

本カタログ掲載商品・サービスの詳細情報
www.hitachi-solutions.co.jp/security/sp/solution/task/cloud.html

S18S-16-03 | 2021.05

HITACHI
Inspire the Next

クラウドセキュリティ強化ソリューション

クラウドのビジネス利活用に求められるセキュリティを コンサルティングから運用支援までトータルで提案

ワークスタイルの多様化に伴い、場所を問わず利用できるクラウドサービスをテレワークに活用する企業が増えています。
利便性が高い一方で、企業が許可していないサービスやIT機器を、従業員が勝手に利用する「シャドーIT」や、
アクセス設定の不備による情報漏洩など、クラウド環境特有のリスクが課題となっています。
このようなリスクには、利用するクラウドサービスの種類に合ったセキュリティ対策が求められます。
「クラウドセキュリティ強化ソリューション」は、クラウドサービス利用時に実施すべきセキュリティ対策の範囲と課題を明確にし、
さまざまな製品・サービスの中からニーズに適したソリューションを提供。
安心で快適なクラウド利活用の実現を支援します。

クラウドセキュリティ強化ソリューションの特長

1. **専門家がクラウド利用時における情報セキュリティの現状を明確化**
   お客様のクラウド環境で検討すべきセキュリティ要件の整理から対策の立案まで、
   経験豊富なセキュリティコンサルタントが支援します。
2. **クラウド利用時におけるセキュリティの課題に対応した解決策の提案**
   お客様がセキュリティを強化したいポイントに応じて、さまざまな
   クラウドセキュリティ製品・サービスメニューから、課題に対応した解決策を提案します。
3. **豊富な実績・技術力を生かし、システム構築から保守までサポート**
   大規模ユーザーへの導入など、豊富な導入実績から培った技術・知識を生かし、
   お客様の環境に合わせたクラウドセキュリティシステムの構築から保守まで支援します。

クラウドサービスの種類

クラウドサービスは、アプリケーション利用者向けのSaaSと、
インフラやプラットフォームを利用する開発者向けのPaaS/IaaSの大きく2種類に分けられます。
それぞれ、利用時に考慮すべきセキュリティリスクと対策が異なります。

【アプリケーションを利用】
SaaS：Software as a Service

従業員

開発者
（仮想サーバーの構築など）

【プラットフォームを利用】（開発環境）
PaaS：Platform as a Service

【インフラを利用】
IaaS：Infrastructure as a Service

SaaS 例：Microsoft 365 など

- Microsoft 365
- Salesforce
- G Suite
- Box
- Dropbox
- Facebook

PaaS/IaaS 例：AWS（Amazon Web Services）など

- 仮想サーバー
- 仮想ネットワークデバイス

ユーザーが実施すべきセキュリティ対策の範囲

SaaS、PaaS、IaaSでは、サービス提供事業者が管理する範囲とユーザーが管理する範囲が異なるため、
それぞれの管理範囲を把握したセキュリティ対策が重要です。

【クラウドサービス種類別の管理範囲】

○：ユーザーの管理対象
●：クラウド事業者の管理対象

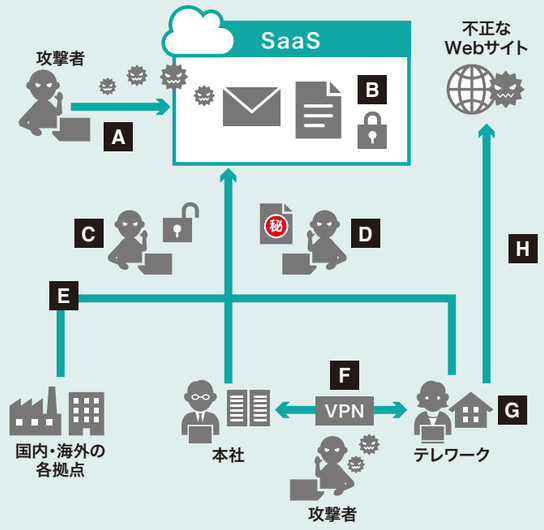
	管理項目	SaaS	PaaS	IaaS
1	アカウント・権限情報	○	○	○
2	ユーザーデータ	○	○	○
3	通信路・通信データ	○	○	○
4	アプリケーション	● *1	○ *2	○ *2
5	ミドルウェア（OS、DBサーバー、Webサーバーなど）	●	●	○
6	仮想リソース（ネットワーク、ストレージ、VM、コンテナなど）	●	●	○
7	物理インフラ	●	●	●

*1 Microsoft 365 など　*2 Webアプリケーションなど

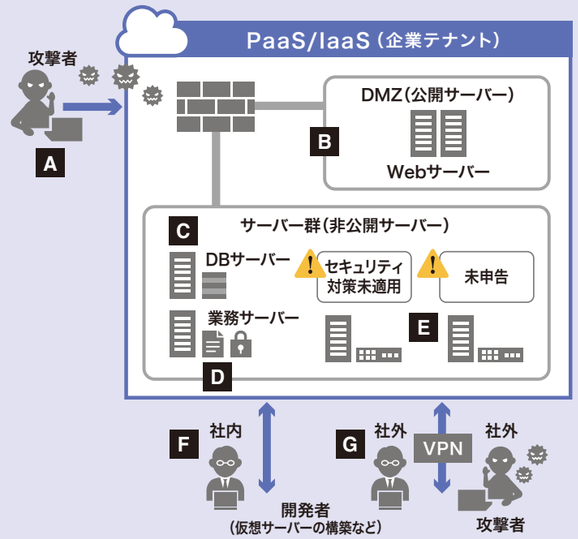
セキュリティリスク と 対策　*上記、管理項目 1 ～ 6 のセキュリティリスクと対策です

		リスク	対策
A	2	マルウェアによる攻撃	マルウェア対策
B	2	クラウドに保存したファイルの漏洩	ファイル暗号化
C	1	ID情報の流出によるなりすまし	IDaaS *3
C	3	HTTPS通信による不正な情報の持ち出し・個人テナントのクラウドサービス利用による情報の漏洩	SSLインサイト・不正なクラウド利用対策
D	1	未許可クラウドの利用による情報持ち出し	CASB *4
D	2	機密ファイルのクラウドへのアップロード	DLP *5・ファイル暗号化
E	3	回線負荷の増大による通信速度低下	インターネットブレイクアウト
F	1	不正ログインによるなりすまし	二要素認証
F	3	VPN機器のグローバルIPに対しての攻撃	セキュアなリモートアクセス
G	2	PCの盗難・紛失による情報漏洩	PCのハードディスク暗号化
H	3	インターネットへ直接接続することによるマルウェア感染や情報の流出	VPN強制接続・クラウド型Webプロキシ

SaaS



PaaS/IaaS



		リスク	対策
A	6	不正なアプリケーションを利用した攻撃・マルウェアによる攻撃	仮想化ファイアウォール
B	4	アプリケーションの脆弱性を狙った攻撃	WAF
B	4	Botを使った不正操作	Bot対策
C	5	DBの脆弱性や設定不備を利用した攻撃	DB監査
D	1	特権ユーザーによる内部不正・特権IDの脆弱なパスワード運用	特権ID管理
D	2	ファイルの漏洩	ファイル暗号化
D	4	サーバーなどに対する改ざん	改ざん検知
D	5	OSやミドルウェアの脆弱性・設定不備に対する攻撃	仮想パッチ（IPS）
D	6	不正なポートを利用した攻撃	ホスト型IDS・IPS
E	6	仮想ネットワーク・VMの構成・設定不備を利用した攻撃	CWPP *6
F	3	通信経路の盗聴	VPN
G	3	VPN機器のグローバルIPに対する攻撃	セキュアなリモートアクセス

*3 IDaas：Identity as a Service　*4 CASB：Cloud Access Security Broker　*5 DLP：Data Loss Prevention

*6 CWPP：Cloud Workload Protection Platform