

# 当社が厳選した セキュリティサービスをご提案します

## 入口対策（製品名：Symantec.cloud）

Webやメールからのウイルスの侵入や社外公開サーバを狙った攻撃を防御



ウイルスメール・  
迷惑メール防御



攻撃者のメールが組織に着信する前に、ウイルス付きメールや迷惑メールを圧倒的な精度で遮断してくれる総合メール防御型クラウドサービス

## エンドポイント対策（製品名：CylancePROTECT）

パソコンやサーバへの感染を狙うウイルスを防御／検知したウイルスを分析



人工知能型  
ウイルス対策



世界初の完全な人工知能型ウイルス対策ソフト  
駆除率99%と業界No.1\*の圧倒的な性能を誇る

### オプション

Cylance検知監視サービス

ウイルス検知時の簡易分析を代行するオプションサービス

\* 他社の従来型製品は  
駆除率50～30%程度

## 出口対策（製品名：i-FILTER）

攻撃者やウイルスが侵入した時に最後の砦として社外への通信を検知・停止



Web  
セキュリティ



安全なWebサイトのみアクセス可能なホワイトリスト運用を実現することで、ウイルス感染時の被害を最小化

## 内部不正、証拠保全対策（製品名：SKYSEA Client View）

パソコンを統合的・効率的に管理。パソコンの操作履歴を記録することで、内部犯行を抑制



ログ管理

デバイス管理



パソコンの管理負荷を軽減するとともに、PC操作ログや外部記憶媒体の利用状況を一元管理

# ご提供可能なセキュリティサービス一覧

区分		サービス・製品	説明
入口対策	メールセキュリティ	Symantec.cloud	<ul style="list-style-type: none"> <li>クラウド型のメールセキュリティサービス</li> <li>ウイルスメールやスパムメールが従業員に着信する前に遮断</li> </ul>
	ファイアウォール (UTM)	FortiGate	<ul style="list-style-type: none"> <li>世界シェアNo.1のファイアウォール</li> <li>インターネット等の外部ネットワークから組織のネットワークを防御</li> </ul>
	IPS/IDS	Trellix Network Security Platform	<ul style="list-style-type: none"> <li>次世代型IPS</li> <li>ネットワーク機器やサーバ等への様々な攻撃を防御</li> </ul>
	WAF	デジサート クラウド型 WAF	<ul style="list-style-type: none"> <li>クラウド型のWAF(ウェブアプリケーションファイアウォール)</li> <li>ホームページ等のウェブアプリケーションに対するサイバー攻撃から防御</li> </ul>
エンドポイント対策	未知ウイルス対策	CylancePROTECT	<ul style="list-style-type: none"> <li>人工知能型(ファイル特徴点検知方式等)ウイルス対策ソフト</li> <li>未知のウイルスから強力に防御</li> </ul>
	ウイルス対策	Trend Micro Apex One	<ul style="list-style-type: none"> <li>国内シェアNo.1のウイルス対策ソフト</li> <li>ウイルスの駆除のみならず、様々な脅威からパソコンを防御</li> </ul>
出口対策	クラウドセキュリティ (CASB)	Skyhigh CASB	<ul style="list-style-type: none"> <li>クラウドサービスの利用状況を可視化</li> <li>組織のクラウドサービス利用に伴うリスクを低減</li> </ul>
	Webフィルタリング	i-FILTER	<ul style="list-style-type: none"> <li>国内シェアNo.1のWebフィルタリングソフト</li> <li>危険/不要Webサイトの閲覧を制限</li> </ul>
	Webセキュリティ (ウイルス対策)	Web Security Service	<ul style="list-style-type: none"> <li>WEBサイトからのウイルスダウンロードを遮断</li> </ul>
	メールセキュリティ (誤送信対策)	Smooth File	<ul style="list-style-type: none"> <li>クラウド型ストレージサービスを用いたセキュアなファイル送受信 (脱PPAP)</li> </ul>
	メールセキュリティ (S/MIME)	CertCONNECT	<ul style="list-style-type: none"> <li>電子証明書を用いたメールのなりすまし、改ざん、盗聴対策</li> </ul>
不正アクセス対策	PC・ファイルサーバ等の認証強化	Active Directory	<ul style="list-style-type: none"> <li>社内ネットワーク上の資産に対する認証の強化</li> <li>ユーザや組織の属性に応じて柔軟なアクセス権の設定を実現</li> </ul>
	リモートアクセス対策	FortiGate (SSL-VPN)	<ul style="list-style-type: none"> <li>社外から社内ネットワーク接続時の強固な認証</li> <li>安心・安全なテレワーク環境の提供</li> </ul>
内部不正対策	インストールアプリ管理	SKYSEA、LANSCOPE	<ul style="list-style-type: none"> <li>業務上不要なソフトウェアのインストールを制限</li> <li>パソコン別でのアプリケーションの導入状況を把握</li> </ul>
	外部記憶媒体利用制限	SKYSEA、LANSCOPE	<ul style="list-style-type: none"> <li>USBメモリ等の外部記憶媒体を適正に管理することで情報漏えいを未然に防止</li> </ul>
証拠保全対策	サーバ・ネットワーク機器ログ保存	Syslogサーバ	<ul style="list-style-type: none"> <li>サーバやネットワーク機器の各種ログを長期間保存する環境の整備</li> </ul>
	PC操作ログ保存	SKYSEA、LANSCOPE	<ul style="list-style-type: none"> <li>パソコン操作 (アプリ起動、ファイル操作等) のログを取得・収集・保存</li> <li>迅速なログ調査による事実確認が可能</li> </ul>
情報漏洩対策	攻撃者サイトへのアクセス制限	i-FILTER (ホワイト運用)	<ul style="list-style-type: none"> <li>許可されたWebサイトのみへのアクセスを可能とすることで、攻撃者が準備した危険なサイトや未知のサイトへのアクセスを禁止 (Webのホワイト運用)</li> <li>万が一、サイバー攻撃を受けた場合においても、攻撃者サイトと通信できない環境を実現</li> </ul>
拡大防止対策	内部通信監視	Deep Discovery Inspector	<ul style="list-style-type: none"> <li>ネットワーク上の通信の振る舞いを監視</li> <li>社内ネットワーク上でのウイルス感染拡大等の兆候をいち早く察知</li> </ul>

その他お客さまのニーズに合わせ、各種セキュリティサービスを取り扱っています。詳しくはお問合せください。

ICTで未来を創造する Qsol株式会社



〒810-0004 福岡市中央区渡辺通2丁目1番82号 電気ビル北館  
MAIL : qbs-security-support@qsolcorp.co.jp

受付時間 : 平日 9:00 - 17:00 (土日・祝休み)



ずっと先まで、明るくしたい。

