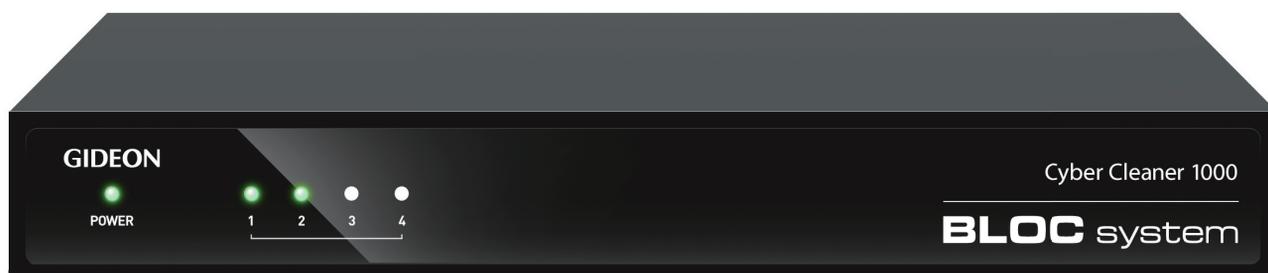


サイバーセキュリティ基本法に対応、
監視・防御・情報流出対策をシンプルに。

Cyber Cleaner[®]

サイバークリーナー

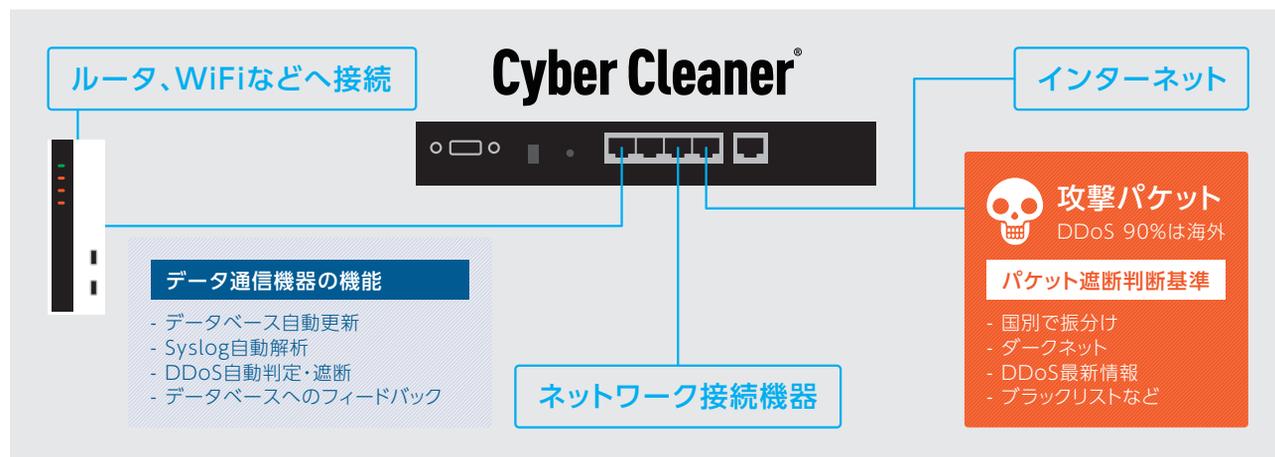


国の認定を受けた国産初の対策機器 Cyber Cleaner[®]

サイバーセキュリティ基本法に基づき、自治体などの公的機関、および、重要インフラ企業はDDoS攻撃、および標的型攻撃の対策が責務となりました。ギデオンのサイバーセキュリティ対策機器「Cyber Cleaner」は、導入、運用が簡単で、サイバー攻撃を検知し、攻撃通信を遮断することでネットワークを攻撃から守ります。さらに国別の通信制限を設定するだけで、外部からのDDoS攻撃や、内部からの情報流出を防ぐことができます。

Cyber Cleaner[®] はネットワークの出入りに置くだけ!

現在のネットワーク構成に影響を与えずL2ネットワーク上にアドオンできるため、設置は1分で完了。攻撃パケットの監視と排除に加え、内部からの情報流出も強力にブロックします。



サイバー攻撃を無力化! 4つの特長



敵から見えない

他のセキュリティ対策機器と違い、「Cyber Cleaner」はIPアドレスを持っていません。ステルス戦闘機と同様、攻撃者から機器を検知できないので、直接攻撃されることがありません。攻撃者からはまるで、すべての攻撃を吸い込んでしまうブラックホールのように見えます。



場所を選ばない

「Cyber Cleaner」はL2ネットワーク上に配置可能な機器です。既存の企業ネットワーク設定を一切変更することなく、ネットワークハブを入れ替える感覚で、どこにでも簡単に導入が可能です。このため、企業ネットワークの最初の入り口で、効率よく脅威に対抗できます。



メンテナンスフリー

NICT (独立行政法人 情報通信研究機構) のデータベースと連携し、新たな攻撃に対応するサイバー攻撃情報が更新できるため、セキュリティ対策に関して詳細な知識がなくても運用できます。機器およびデータベースが国産であることも、重要なポイントです。



高速処理・暗号化対応

パケットのヘッダ情報を検知し、データベースと照合、高速処理が可能です。ヘッダ情報を参照するため、通信が暗号化されている場合でも、攻撃の判定に影響がありません。外部からの攻撃だけでなく、内部からの情報流出についても同様にに対応できます。

日本のセキュリティは日本のデータベースで守る!

