News Release

Fibergate Inc.
株式会社ファイバーゲート

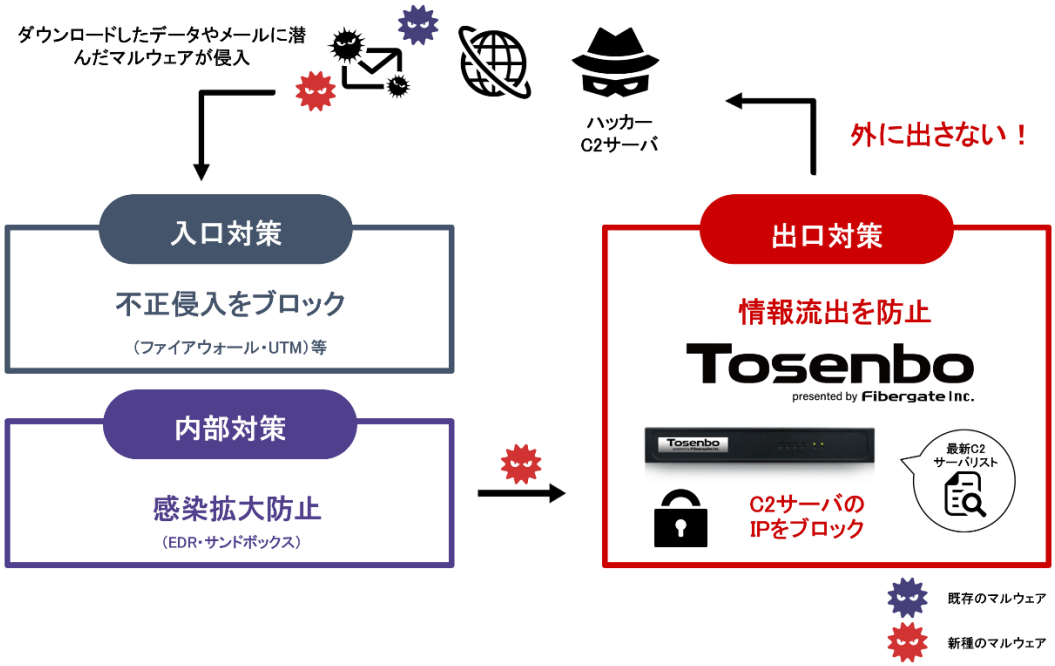
2023 年 4 月 24 日
株式会社ファイバーゲート

不正侵入遮断システム「Tosenbo®」の販売開始
～情報を漏洩させないセキュリティ対策「出口対策」～

株式会社ファイバーゲート（東証プライム・札証：9450、本社：北海道札幌市、代表取締役社長：猪又 將哲、以下「ファイバーゲート」）は、デジタルデータソリューション株式会社（本社：東京都港区、代表取締役社長：熊谷 聖司、以下「DDS」）と業務提携契約を締結し、DDS の不正侵入遮断システムを活用した「Tosenbo®」の提供を開始いたします。

＜Tosenbo®の概要＞

「Tosenbo®」は、ハッカーが使用する C2 サーバ不正通信対策により、UTM 等の入口対策では防ぎきれない脅威をブロックする不正侵入遮断システムです。



※Tosenbo®機器

ポイント①　ハッカーが使用する C2 サーバの不正通信をブロック

攻撃者からのメール受信などで C2 サーバとの不正通信を検知した時点で、自動で検知し不正通信を遮断します。

ポイント②　C2 サーバとの不正通信を検知した場合に企業様へ通知

C2 サーバとの通信を検知した時点で、ファイバーゲートより不正検知を通知します。それと同時に該当の通信を遮断しますので企業様に行っていただくことはありません。

ポイント③　既存のインターネット回線に接続するだけの簡単導入

既に使用しているインターネット回線に機器を接続するだけのため、導入工事が簡単に完了します。

※新規回線の敷設が必要であれば同時に行うことも可能です。

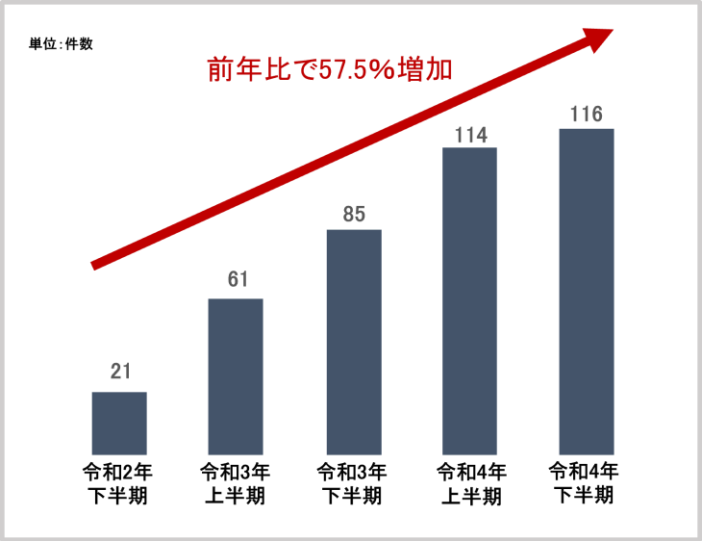
特設 WEB サイト→https://to-senbo.com

＜昨今のサイバー攻撃＞

日本国内のサイバー攻撃観測数は年々増加傾向にあり、総務省の発表によると※1 1 年間に観測されたサイバー攻撃関連の通信数は、2018 年から 2021 年の 3 年間で 2.4 倍にのぼります。サイバー攻撃の種類は多様であり、その中でも手法としてはランサムウェア※2 による被害が多く、2021 年下半期のランサムウェア被害の報告件数は 2020 年下半期に比べて約 4 倍、警察庁の発表では※3 令和 4 年中に警察庁に報告されたランサムウェアによる被害件数は前年比で 57.5%増加となっております。

なお、標的型攻撃の手法も多様化しており大企業でも被害が拡大しております。標的型攻撃は機密情報や個人情報を取得することを目的として、ウイルスが混入した添付ファイルを送付するなどしてマルウェア感染等の攻撃を実行することです。標的型攻撃は政府を

はじめ、企業や大規模団体がターゲットとなる傾向があります。そのため企業や各団体は、個人情報漏洩を防ぐためにも多角的な対策が求められております。



※警察庁　令和４年におけるサイバー空間をめぐる脅威の情勢等について
【図表１：企業・団体等におけるランサムウェア被害の報告件数の推移】参照

※1　総務省　サイバーセキュリティタスクフォース「ICT サイバーセキュリティ総合対策 2022」
https://www.soumu.go.jp/main_content/000830903.pdf　参照
※2　ランサムウェア：感染すると端末等に保存されているデータを暗号化して使用できない状態にした上で、そのデータを復号する対価（金銭や暗号資産）を要求する不正プログラムのこと。
※3　警察庁「令和４年におけるサイバー空間をめぐる脅威の情勢等について」
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf　参照

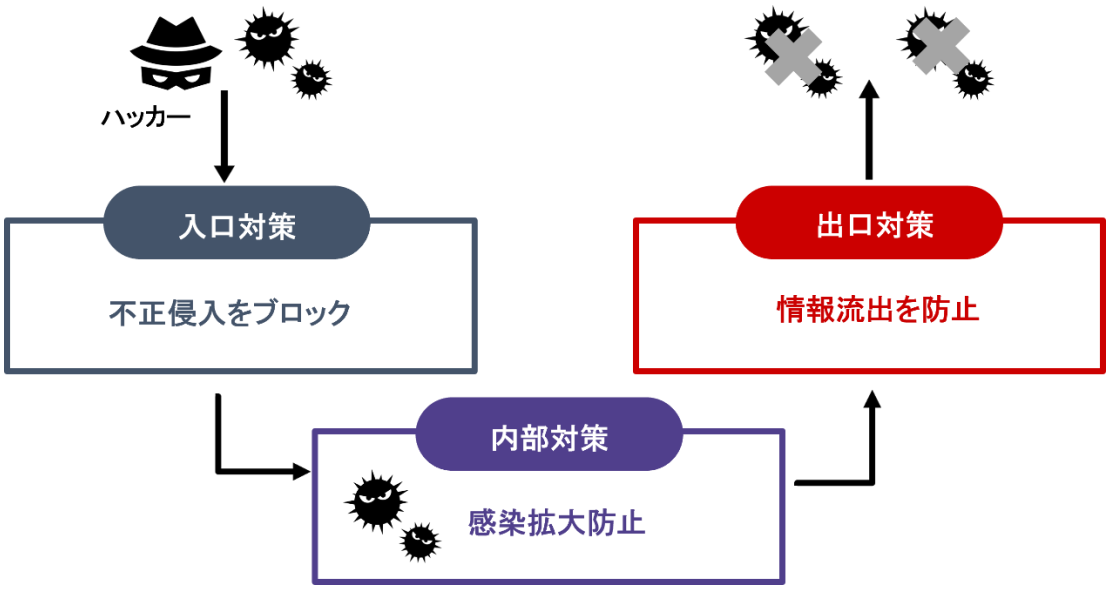
＜セキュリティ対策の種類＞

サイバー攻撃対策には、おもに「入口対策」「内部対策」「出口対策」があります。従来はファイアウォールに代表される「入口対策」が主となっており、約８割の企業が導入しているセキュリティ対策は「入口対策のみ」がほとんどです。

「入口対策」でブロックしているのは既存のマルウェアとなりますが、マルウェアは毎日 120 万件も作られるため、全てをブロックすることは不可能と言われております。そこでログ監視やファイルの暗号化など企業内で行う「内部対策」を実施し、社内情報や顧客情報などを守る必要があります。

さらに、万が一感染してしまった場合、それを外部に感染させない対策である「出口対策」が必要となります。一度感染してしまった場合、対策をとっていない場合は容易に外部へ広めてしまうリスクが発生します。

そのため、セキュリティ対策の層を増やす「多層防御」および、内部に侵入されることを前提とした出口対策を行うことが重要となります。



＜電気通信事業者としての使命＞

総務省は、2021 年 11 月に、電気通信事業者が通信の秘密等に配慮しつつ、新たな対策や取組を講じていくことが可能となるよう、電気通信事業におけるサイバー攻撃への適正な対処の在り方について検討を行う「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」を実施しています。

ファイバーゲートは電気通信事業者として、企業や施設が安心して通信環境を構築できるよう、積極的にサイバーセキュリティ対策の推進を行ってまいります。

■株式会社ファイバーゲートについて　(https://www.fibergate.co.jp/)

独立系 Wi-Fi ソリューション企業として、機器製造から電気通信サービスまでを一貫して手がける。マンション・アパート等の賃貸物件オーナー向けの『ホームユース事業』と、観光施設や各種店舗・商店街、商業施設の施設運営者向けの『ビジネスユース事業』を展開。

会社名：株式会社ファイバーゲート【英語表記：Fibergate Inc.】
代表者：代表取締役社長　猪又 將哲
所在地：〒060-0061　北海道札幌市中央区南 1 条西 8 丁目 10-3
設立：2000 年 9 月
証券コード：9450（東証プライム/札証）
電気通信事業者 登録番号：第 358 号

【本件に関するお問い合わせ先】
株式会社ファイバーゲート　ビジネスユース営業本部
TEL：03-5733-1969　Email：info@fibergate.co.jp
お問い合わせ：https://www.fibergate.co.jp/contact/

【報道関係者様　本件に関するお問い合わせ先】
株式会社ファイバーゲート　経営企画本部
TEL：03-5733-1969　Email: cp@fibergate.co.jp
お問い合わせ：https://www.fibergate.co.jp/contact/press/