あなたのシステムをサイバー攻撃から守るための最終ディフェンス

ファイアータワー <FireTower>

ファイアータワーはアンチウイルスソフトウエア等の入り口対策を擦り抜けシステム内に侵入してくるマルウエア（APT他）をターゲットに設計されたソフトウエアです。

現在ご使用中のセキュリティー ソフトウエア等と共用することによりいままで防ぐ事ができなかった脅威からあなたのシステムを守ります。

<今、発生するかもしれな危機とは・・・>

今サイバー犯罪の被害者は年間50億人（件）以上とも言われ、その損害額は10兆円以上、新種のマルウエアと呼ばれる悪意のあるソフトウエアは日々、数十万件も発生しています。これらの多くは、既存のペリメータ ディフェンスと呼ばれるアンチウイルス製品をはじめとする入口対策のディフェンスを擦り抜けシステム内に潜入します。一旦、潜入してしまったマルウエアは、継続的にシステム内に留まり、悪意のある攻撃を繰り返し、システムやネットワーク全体に多くの脅威を与えます。

<標的型攻撃実行の最終的な目的とは・・・>

標的型攻撃の最終的な目的は、何らかのトグルにより自動的に悪意のある行動を実行させる 自動実行エントリー（Autorun Setting Entry）をターゲットのシステム内に設定しこれを安定的に存続、運用させる事です。そして継続的に悪意のある攻撃を実行し続けます。継続的な標的型攻撃は発見される場合であっても、仕掛けられてから平均で10か月以上が経過していると言われています。ターゲットとなったシステムはこの間、悪意のある攻撃を受け続けています。

<ファイアータワーは、標的型攻撃に対する最終ディフェンスです。>

ファイアータワーは現在のペリメータ ディフェンスの隙間を突く攻撃にターゲットを絞った、まったく新しいイベント トリガー ベースのセキュリティー システムです。

ネットワーク サイド中心の入口、出口対策である アンチウイルス やサンドボックス システムをはじめとするペリメータ(Perimeter) ディフェンスは、今後もサイバー攻撃防止に対する重要なソリューションの1つです。しかし今、これらディフェンス システムの隙間を突く攻撃が問題となっています。新種のAPTやマルウエアは、毎日数十万個以上も発生していると言われており、これを防止するためのプロアクティブなディフェンス システムの必要性が求められています。ファイアータワーは、使用中の如何なるペリメータ ディフェンス（アンチウイルスやサンドボックス等）とも共存でき、また、共有することでペリメータ ディフェンスの隙間を埋め、サイバー攻撃に対する保護能力を強化されます。

ファイアータワーは悪意のあるソフトウエアがエンドポイントに侵入しただけでは動作しません。
侵入したソフトウエアが実行された時点でファイアータワーの処理がスタートします。ソフトウエアの起動を感知すると、その動作内容に関するメタデータを取得し、このデータとファイアータワー独自の ホワイトリスト データベース ASR(Autorun Setting Repositry)と内容を比較し脅威の有無をリアルタイムに評価します。
ホワイトリストとの比較結果を評価（安全、危険、未知、疑わしい等）し、その内容によって、処理の中止、継続等を自動的に判断します。（保護機能実行ポリシーは、予め設定したプロファイルに従って実行されます。）

外部から侵入してくるソフトウエアの1次的な安全性の評価は、既存のペリメータ ディフェンスにより決定されます。この検査をパスし、侵入してきてしまった 悪意を持ったソフトウエアが 実行される段階で、ファイアタワーはそのソフトウエアに関するメタデータや振舞を検査し、その安全性を決定する 最終ディフェンスとして実行されます。（侵入してきた強盗が内部で暴れ始めた段階で保護機能が実行されます。）

<悪意のある攻撃がもたらす脅威とは・・・>

① ネットワーク内情報の漏洩	多くの企業や団体内部でネットワーク内の情報が収集され、これが外部へ漏洩されています。
② 遠隔操作	外部からネットワーク内部を遠隔操作によりコントロール
③ システムダウン	ある特定の時刻や特定の処理実行によってエンドポイントやサーバーをシステムダウンさせます。
④ 疑似情報の発信	メールの発信元等、情報の発信元を偽装して外部へ発信させます。
⑤ マシンやリソールを改ざん、コントロール	ネットワーク内部の情報やコンテンツを改ざん、コントロールします。 （その他）

<ファイアータワー のキーテクノロジーとは・・・>

※ **ファイアータワー ネットバリデーション テクノロジー**（外部から侵入してくるソフトウエアに関する安全性の評価）

外部から挿入される自動実行エントリー情報全てをインシデント化し、Who、What、When、Where 方式（誰が、何を、いつ、どこに対して実行したか。）によって、その変更内容（追加、変更、削除）を履歴管理します。これにより、システムに対する攻撃や、同一方法による度重なるAPT等の攻撃を監視、保護することができます。

** 静的情報による評価

自動実行エントリーに関するエントリータイプ、エントリー名、レジストリー情報、ターゲットとなるファイル情報等の静的情報を取得し悪意のある攻撃を監視し保護します。

** 動的情報による評価

過去から現在までの実行履歴と実行内容（振舞）を基にした実行タイムスタンプ情報により悪意のあるソフトウエアを監視し保護します。（Who、What、When、Where 方式）

ファイアータワー ガード（各エンドポイント上で動作するソフトウエア）は上記に関するメタデータをリアルタイムに取得し、これらの情報をクラウド上の自動実行エントリーに関するホワイトリスト データベースである ASR(Autorun Setting Repository）と組み合わせて使用することにより外部から侵入してくるソフトウエアの安全性を評価します。

※ **IHIPS（ホスト間 侵入防止システム）機能と 一括検疫処理**

通常、1台の Windows PC内には、少なくても数百個、多い物では数千個程度の自動実行（Autorun）エントリー（何らかのトグルによってPC内に保存されているプログラムが自動実行されるセッティング）が設定されています。継続的な標的型攻撃は、これら 自動実行エントリー（セッティング）を利用して実行される場合がほとんどです。また、企業や団体等、大規模ネットワーク内に悪意のあるソフトウエア（自動実行セッティング）が発見された場合、全てのPC内を検査し、これらのセッティングやファイルを検疫するためには膨大な時間とコストが必要となります。

ファイアータワーは同一の悪意のあるソフトウエアやこれを実行させるための自動実行エントリーに関連するネットワーク上の全てのエンドポイントに関する情報（どのマシン上のどこのロケーションにどのセッティングやファイルが存在しているのか）をクラウド データベース上にリアルタイムに保管しています。悪意のあるソフトウエアがネットワーク上で発見された場合でも、クラウド上のファイアータワー データベースから全エンドポイント情報を瞬時に参照し、このネットワーク上に確立された全ての脅威を、瞬時に、ワンクリックで検疫することができます。

<ファイアータワー製品種別>

① ファイアータワー ガード パーソナル エディション（FTGP）

本システムはスタンドアローンのWindows PC上へインストールします。スタンドアローン用のビューワー（コンソール）が付属しています。オプションでSOHO（小規模オフィスやご家庭）で 3台までのPCを1つのコンソール画面で一括管理するための サイバーコンソール-CyCon(**1)パーソナル エディションもご使用いただけます。<希望小売価格：¥3,300 / PC>
（ご参考価格：3台のPCを接続・管理した場合1年目の総費用 ¥13,200、2年目以降は、CyCon使用代金のみ ¥3,300/年）

② ファイアータワー ガード ビジネス エディション（FTGB）

本システムは大規模ネットワーク上の全てのエンドポイント（台数制限なし）を1つのサイバーコンソール-CyCon(**1)で一括管理（監視、保護、検疫）できます。各エンドポイントのデータを保管するお客様用のデータベースをパブリック・クラウド上に作成しご使用いただけます。各エンドポイントにはファイアータワー ガードをインストールします。
（ご参考価格：100台のPCを接続・管理した場合の総費用 ¥253,000　2年目以降も毎年同額）<SaaSサービス>

③ ファイアータワー ガード ビジネス エンハンスド エディション（FTGBE）

本システムは上記 ファイアータワーガード ビジネスの機能に加えて、お客様専用のデータベース サーバーを構築して運用するシステムです。これにより各エンドポイントのデータの保管だけではなく、ファイアータワーで使用する自動実行セッティングに関するホワイトリスト データベース-ASR(Autorun Setting Repository)(**2)もお客様専用の仕様に拡張して運用していただけます。自社のシステムでご使用になる独自のソフトウエアをホワイトリストへ登録する等、よりきめ細かい管理を行う事ができます。また、外部ネットワークとの接続を遮断したい場合にも有効です。
（ご参考価格：1,000台のPCを接続・管理した場合1年目の総費用 ¥3,575,000　2年目以降 ¥825,000/年）<別途、専用サーバーが必要です。>

<開発・販売元>

Sampan Security inc.
（米国ニューハンプシャー州）

ネットツール株式会社
神奈川県小田原市栄町1-9-10
TEL: 050-6860-3401

http://www.firetower.jp/

<ファイアータワーに関する 詳細情報をご覧いただけます。>

** ファイアータワーは米国Sampan Security inc、Windowsは米国Microsoft Corporation、その他の各社名、商品名は各社の商標または登録商標です。