

# バックアップではない、EDR でもない、 第3の選択肢

～ランサムウェアは完全には防げない・・・万が一被害に遭っても迅速に復旧～

NeuShield なら・・・

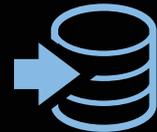
- ◎検知不要で保護
- ◎より強固な保護の実施
- ◎迅速な復旧



## EDR ソフト

ランサムウェアを検知してブロックし、  
被害を防ぐ

- ×検知できるようになるまでに  
時間がかかる
- ×検知できない場合がある



## バックアップソフト

被害に遭った際に過去のデータに  
復旧する

- ×復旧までに時間がかかる
- ×バックアップデータが感染している  
場合がある

## セキュリティソフトでは、ランサムウェアは防げません

ランサムウェアは、残念ながら EDR ソフトやバックアップソフトのような既存のテクノロジーだけで防ぎきることはできません。EDR やアンチウイルスソフトなどのシグネチャの作成には時間がかかるため、それまでの間は脆弱なままです。また、通常のバックアップソフトは復旧に一定の時間がかかり、バックアップそのものが感染している場合もあります。

### 新しいアプローチでランサムウェアに対抗し、データを保護

NeuShield Data Sentinel は、独自の「ミラーシールド」テクノロジーにより、オリジナルのファイルを保護します。ファイルが改ざんされても瞬時に元の状態に復旧させることができます。

### セーフモードでも動作する唯一のセキュリティソフト

NeuShield Data Sentinel は、Windows のセーフモード下での攻撃にも対抗できる、Microsoft が認めた唯一のソリューションです。

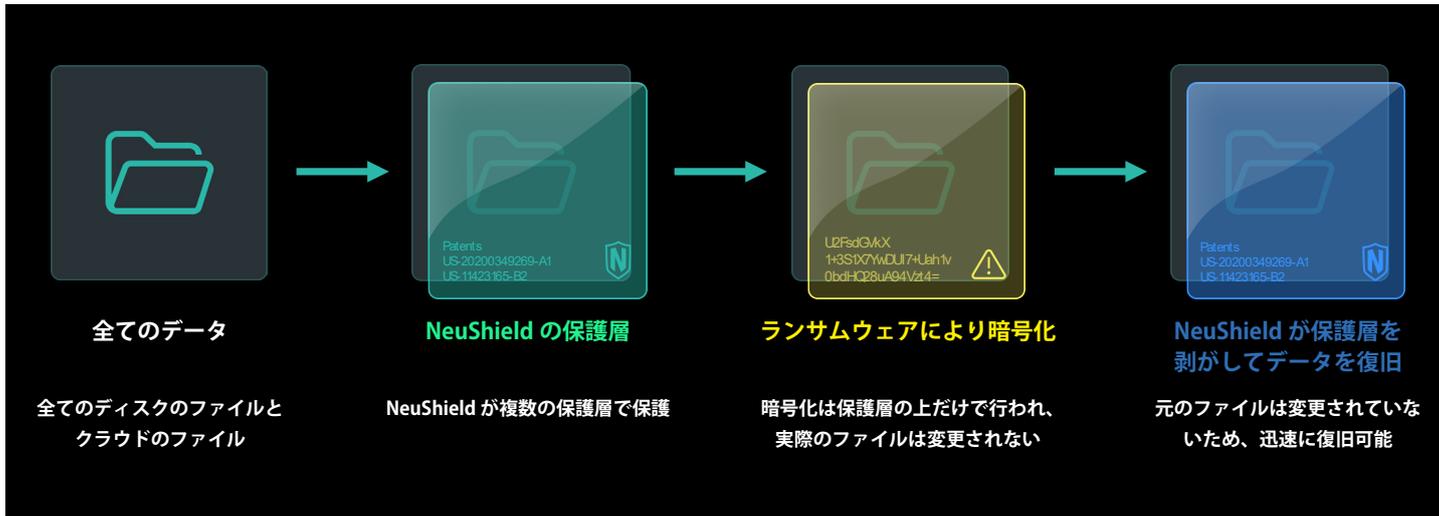
### データベース保護でデータ漏洩を防止

最大 64TB のデータベースについてデータを保護します。データベースプロセス以外からはデータを隠し、改ざんを防ぐとともに、万一侵害された場合でもデータベース全体を瞬時に復旧させることができます。



# 元ファイルを変更せずにそのまま残す「ミラーシールド」テクノロジー

NeuShield Data Sentinel は、「ミラーシールド」と呼ばれる独自の技術によって、オリジナルのファイルを保護します。NeuShield Data Sentinel がインストールされると、保護すべきファイルに保護層が追加され、それ以降はファイルが直接変更されることはありません。アプリケーションがファイルを変更しようとする、その変更は保護層に保存されます。変更後にファイルを元に戻したい場合には、保護層を消去すれば良いだけです。



万一ランサムウェアに感染し、ファイルを削除もしくは暗号化されてしまったとしても、保護層を一枚消去するだけで、直前の状態に戻すことができます。この操作はバックアップファイルをリストアするよりも遙かに高速に行う事ができ、ほとんど瞬時にデータを復旧できます。

また、保護層にはファイルの変更部分のみが記録されるため、ディスクへのアクセスが発生したとしても、それはほとんどパフォーマンスには影響しません。NeuShield Data Sentinel はコンピュータの処理性能にほとんど影響を与えることなく、ファイルを保護することができるのです。

## 主な機能

### ワンクリック復元

OS 全体を数十分で復元することができます。NeuShield は OS のスナップショットを定期的に作成するため、ユーザーはそのうちのひとつを選んで迅速にコンピュータを復旧させることができます。ワンクリック復元はランサムウェアなどのマルウェアの削除に役立ちますし、欠陥のある Microsoft のパッチを削除することもでき、オフラインでも動作します。

### NeuRestore

ブルースクリーンからの回復時にも、ワンクリック復元をご利用頂けます。NeuRestore は Windows 10 以降でサポートされた Windows Recovery Environment (Windows RE) に対応しているため、システムに不具合があった際の修復時に詳細オプションからワンクリック復元を起動することができ、直前の正常な OS 状態に戻すことができます。

### データベース保護でデータ漏洩を防止

Datacenter Edition では、最大 64TB のデータベースについてデータを保護します。データベースプロセス以外からはデータを隠し、改ざんや暗号化を防ぐとともに、万一侵害された場合でもデータベース全体を瞬時に復旧させることができます。また DB を動作可能な状態に迅速に復旧できるため、ランサムウェアからの攻撃を受けても DB を再構築する必要はありません。

に復旧させることができます。また DB を動作可能な状態に迅速に復旧できるため、ランサムウェアからの攻撃を受けても DB を再構築する必要はありません。

### 強固なデバイス保護

NeuShield Data Sentinel は、セーフモードで動作する唯一のセキュリティソフトとして Microsoft から認定を受けています。マルウェアによるブートレコード/セクタを保護し、マルウェアによる乗っ取りを防止します。また RAW/ダイレクトディスクアクセスを防止してワイプ型マルウェアがディスク上のデータを直接攻撃することを防ぎます。ロックダウン機能により、再暗号化を防止します。

### データ駆動型検知

データの状態を常に監視し、通常の変更なのか通常とは異なる動作での変更なのかを検知します。ベースラインや学習モデル、定義ファイルに依存せず、マルウェアのプロセスや感染のスキャンを行わないため、一般的なセキュリティ製品が検知できない場合でも有効です。

## NeuShield Data Sentinel のエディション

### ■クライアント版

#### NeuShield Data Sentinel Workstation Edition

- Windows 7, 8.1, 10, 11 に対応

### ■サーバー版

#### NeuShield Data Sentinel Server Edition

- Windows Server 2008 R2, 2012(R2 含む), 2016, 2019, 2022 に対応
- 最大 2TB までのファイルを保護

#### NeuShield Data Sentinel Datacenter Edition

- Windows Server 2008 R2, 2012(R2 含む), 2016, 2019, 2022 に対応
- データベース: Microsoft SQL Server 2012 以降
- 最大 64TB までのファイル (DB) を保護



## セキュリティストリングス株式会社

〒102-0082 東京都千代田区一番町 6 番地 相模屋本社ビル 7F

Email: sales@securitystrings.com

URL: <https://www.securitystrings.com>

©2024 Security Strings 本カタログに記載の会社名、商品名は各社の商標または登録商標です。

本カタログに記載されている情報は 2024 年 10 月現在のものであり、製品仕様および機能は予告なく変更される場合があります。予めご了承下さい。



お問い合わせ