漏洩させない出口対策
官公庁レベルの
セキュリティを実現

導入実績台数約2,300台

ウィルスソフトやUTMだけでは情報漏洩を防げません

DDHBOX3つの強み

1 感染拡大を防ぐ
不正通信検知・遮断
24時間365日全自動

2 情報漏洩を防ぐ
情報の持ち去りをブロック

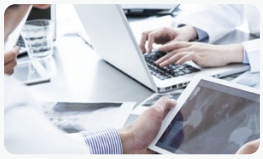
3 サイバー保険付帯
調査・対策までサポート
年間300万円分

医療現場ではDX化が推進

環境の変化によって
セキュリティリスク
が生じています。

セキュリティリスク❶

情報事故発生リスク



コロナの影響により業務が逼迫しており、情報の管理や伝達が杜撰になり情報事故が発生してしまうリスク

セキュリティリスク❷

医療システムの標的化リスク

オンライン資格確認の導入など、行政機関の情報連携が進み医療システムがサイバー攻撃の標的となる可能性が高まる

セキュリティリスク❸

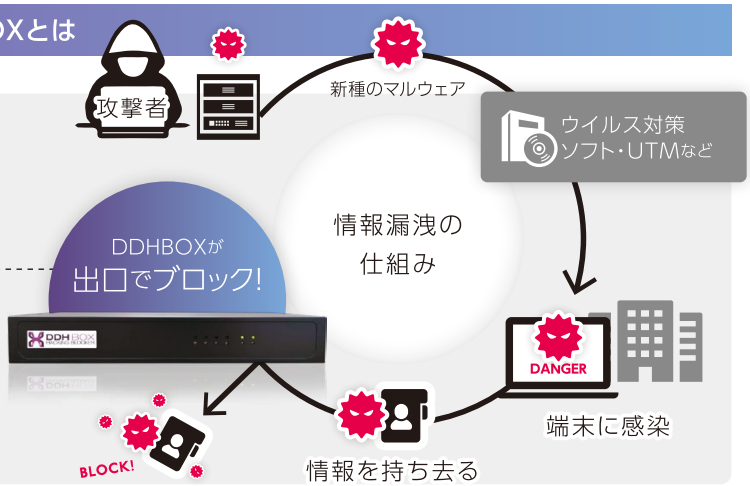
患者データの標的化リスク

攻撃者の間で価値が高い情報として取引される患者の個人情報や医療記録等が電子データ化されることによって標的に

DDHBOXとは

マルウェアの不正通信を出口でブロック、
低コストで官公庁レベルのセキュリティを。

国内最大級のセキュリティ監視センターで
毎日更新されるC2サーバ（攻撃者が侵入マルウェアに
指示を出すためのサーバ）のリストを使用しています。



DDH BOX
HACKING BLOCKER

実際にあったご依頼

CASE1 ランサムウェア感染による業務停止

ある医療機関の院内ネットワークにランサムウェアが侵入し、全業務データが暗号化されたケース。侵入を防ぐためのセキュリティ対策（入口対策）を行っていたにも関わらず感染し、業務停止に追い込まれてしまった。

調査対策費用（約）1000万円

DATA
- 業種 …… 医療（病院）
- 年商 …… 約32億6000万円
- 従業員数 … 158名

業務停止期間 約2ヶ月

CASE2 Emotet感染による信用失墜

取引先を装ったメールがA社に届き、社員がファイルを開封したことでEmotetに感染してしまったケース。A社は感染に気がつかなかったため、そのまま取引先にも感染してしまった。A社は被害者であると同時に加害者となり、信用を失った。

調査対策費用（約）550 万円

DATA
- 業種 …… 建築・建設業
- 年商 …… 約66億円
- 従業員数 … 63名

充実の事後対応

迅速な事後対応が求められる時代。

防衛省のセキュリティガイドラインをはじめ、
大企業が取引先に求めるセキュリティ体制としても事後対応は
必要項目となりました。

DDSの事後対応ソリューションを提供

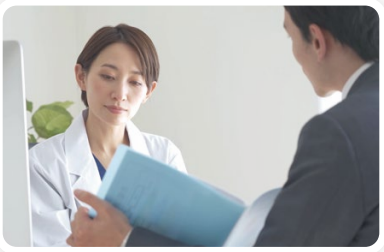
01 感染経路・被害範囲特定

感染が疑われる端末を調査し、経路や被害範囲を調査。レポートを提出。

02 データ消失時の復旧対応

業務データが消失した場合は、データ復旧技術で復旧作業を行う。

03 今後の対策をご提案



レポートを元に今後のセキュリティ対策をご提案可能。

インシデント対応会社だからできる中小企業のためのデータセキュリティ

NHOSA ノーザ
〒164-0011 東京都中野区中央1-21-4 ノーザビル ノーザ 検索 https://www.nhosa.com
TEL 03-5348-1881（代） FAX 03-5348-1885 E-mail：sales@nhosa.co.jp

- 北海道支店 TEL. 011-209-0027
- 茨城支店 TEL. 029-233-2882
- 埼玉支店 TEL. 048-645-2821
- 千葉支店 TEL. 043-204-9300
- 東京支店 TEL. 03-5348-3381
- 神奈川支店 TEL. 045-909-5781
- 静岡支店 TEL. 054-205-6900
- 金沢支店 TEL. 076-223-5010
- 名古屋支店 TEL. 052-332-0327
- 大阪支店 TEL. 06-6442-7812
- 神戸支店 TEL. 078-367-5801
- 広島支店 TEL. 082-293-7618
- 福岡支店 TEL. 092-474-1777

NHOSAQ0108022024