東京都保険代理業協同組合

電空の番人

セキュリティの全領域を、一気通貫で。
“電空の番人”が実現する“シームレス”な多層防御。
サイバー攻撃から企業時の情報資産を守るための、
専門家によるセキュリティ運用サービスです。

損害保険を併用することで万が一の際の補償だけでなく、損害賠償
対応費用（調査・通知・再発防止）までカバーすることが可能です。
サイバーセキュリティ対策を行うことで保険対象が明確になります。
その為には、IPA（情報処理推進機構）によるｾｷｭﾘﾃｨｱｸｼｮﾝ自己宣言を行い
EASY Forensicsでのフォレンジング解析、DDHBOXによる出口防御など
監視体制の構築から行いましょう。

サイバー攻撃の隙がないかチェック！

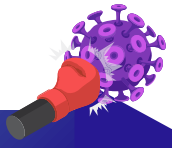
- 退職者PCやUSBの使用履歴を調査したことがない
- セキュリティソフトは入れているが、通信の監視はしていない
- 社外とのメールに添付ファイルを頻繁に使っている
- 個人情報ファイルの所在を正確に把握できていない
- UTMを入れていても、出口対策は未実施
- IPA（セキュリティ対策自己宣言 ）未実施

お問い合わせ

損害保険×サイバー対策のプロが、
最適な導入プランをご提案します。

東京都保険代理業協同組合
03-5348-6008　担当　システム委員会
https://www.tosompo.or.jp/

サイバーセキュリティ対策の順番と役割

入口門番	入口防御	内部防御	内部検知	出口防御
				
「攻撃されそうな入口」を洗い出して見張る	ウイルス・不正アクセスを一括でブロック	パソコンをウイルスから守る	侵入後の異常な動きを検知して対応	社内から外への不審な通信を監視・遮断

EASY Forensics（ASM領域）

（フォレンジックツール）
誰でも簡単にデジタル証拠を収集・調査可能
退職者端末・USB情報漏洩・内部通報への初動対応に
内部不正、個人情報漏洩を可視化・証拠化
導入だけでCSR・コンプライアンス向上効果も

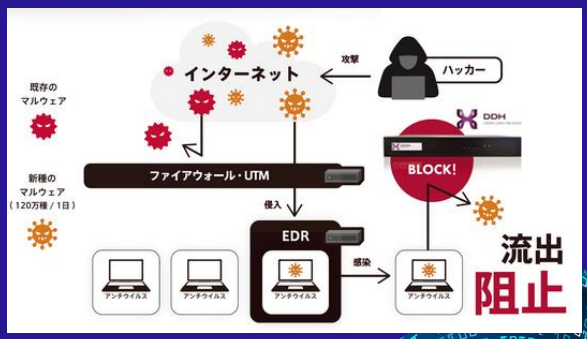
導入メリット：
- 専門業者に依頼する前段階の「簡易フォレンジック」
- 社内調査を迅速・低コストで実現
- 個人情報ファイル自動検出可

PC定期監査 / 事案発見 / データ保全

DDHBOX（NDR領域）

※次世代ネットワーク監視アプライアンス
- 不正通信・ウイルス通信をリアルタイム監視
- 社内ネットワークの“出口”を監視し、情報流出をブロック
- クラウドではなくローカル型で個人情報保護法対応
- 社内にUTMがあっても見逃してしまう出口攻撃に強い

※導入企業増加中!



【＋α：サイバー保険との連携】

保険適用の前提に「対策実施」が求められるケースがある
→ 保険金支払いのためにも、ログ管理や監視体制の整備が重要。

事故発生時に「対応体制」がある企業は信頼される
→ 取引先や顧客への説明責任を果たせる証拠となる。

フォレンジック対応や被害報告の“根拠”を保険会社に提出できる
→ EASY Forensicsで取得したレポートが、そのまま証拠資料に。