検知を超えた封じ込めで ランサムウェアの被害を極小化

IllumioとIIJグローバルソリューションズは共同で、マイクロセグメンテーションのハンズオンセミナー「Illumiverse Labs：Breach Containment」を開催。参加者は実際にデモ端末を操作しながら、可視化から封じ込めまでの一連の流れを体感した。

Illumiverse Labs
Breach Containment

「デモ以上、PoC未満」IIJグローバルソリューションズ発のソリューションラボ

本イベントの会場となったのが、IIJグローバルソリューションズが運営する「ソリューションラボ」だ。顧客がセキュリティ製品を「デモ以上、PoC未満」の形で体感できる施設であり、顧客自身が実際に端末を操作しながら製品を体験できる点が特徴になっている。事前にニーズをヒアリングしたうえでシナリオを設計する双方向型のプログラムを提供しており、昨年度は30件以上の企業が活用している。

IIJグローバルソリューションズ Strategy+ 部 Strategyt+ Design グループ グループリーダーの滝田 智広氏は「仕様や機能の話ではなく、お客様が求めている価値をここで実際に体感していただくこと。それがソリューションラボを設置した目的です」と話す。

侵害は「いつか」ではなく「必ず」起きる 高止まりするランサムウェア被害の現実

こうした取り組みの延長線上で今回実現したのが、本ハンズオンセミナーだ。セミナーの冒頭、Illumioの豊嶋 依里氏はランサムウェア被害の現況を数字で示した。2025年の被害報告件数は226件に上り、その復旧総額が「1,000万円以上」に上った組織は全体の5割を超え、「1か月未満」で復旧できた組織は5割強にとどまるなど、被害の長期化・高額化が続いている。

また、国内飲料メーカーのランサムウェアによる攻撃事例を振り返ると、当該企業の調査によれば、攻撃者は当該企業のグループ内のネットワーク機器を経由することで、データセンターのネットワークに侵入、ランサムウェア攻撃を実行することで複数のサーバのデータを暗号化した。この攻撃により、製品の受注・出荷が停止したほか、顧客や従業員等の個人情報、約191万件が漏えい、またはそのおそれがあるとしている。

「この事例ではEDRを導入済みだったにもかかわらず、攻撃者の手法が巧妙かつ高度であったため検知できなかったと言われています。このようにセキュリティ対策を一定レベルで実施していても、攻撃されてしまうというのが現実です」（豊嶋氏）

こうした被害の深刻化には、攻撃速度の加速も大きく影響している。事実、CrowdStrikeの2026年版グローバル脅威レポート（※）によれば、サイバー犯罪のブレイクアウトタイムは2025年にはわずか29分へと短縮され、最速はわずか27秒だった。

「AIの時代では、攻撃の高度化・自動化により、侵害はかつてとは比較にならない速度で進行し得ます。もはや問われるのは『すべてを時間内に検知できるか』ではなく、『止めるまでに攻撃者はどこまで到達できるのか』です」（豊嶋氏）

防御側がどれだけ投資しても侵害を100%防ぐことはできない。そうした現実を前提に、感染しても全滅しないサイバーレジリエンスを実現するためには、侵害後の被害拡大を封じ込める仕組みが不可欠と言えよう。

※参照元：クラウドストライク「2026 年版グローバル脅威レポート」https://www.crowdstrike.com/ja-jp/press-releases/2026-crowdstrike-global-threat-report/

可視化と封じ込めの両輪を実現する Illumio Breach Containment Platform

検知だけに頼らない封じ込めの仕組みとして、Illumioが提供するのが「Illumio Breach Containment Platform」だ。侵害前後を問わず一貫したカバレッジを提供する「Illumio Insights」と「Illumio Segmentation」の2つの製品で構成されている。

Illumio InsightsはAIセキュリティグラフを核としたハイブリッド環境対応のDetection & Response（D&R）ソリューションだ。クラウドのフローログやファ

Illumiverse Labs

Breach Containment

イアウォールログ、エージェントからのデータをAI/MLがリアルタイムで分類・ラベリングし、リスクの高い通信、外部脅威インテリジェンスDBと照合した危険なIPとの通信、地政学的リスクの観点からの国別トラフィックなどをInsights Hubダッシュボードで多角的に可視化する。IaaSであればAPI連携で既存環境に変更を与えずに数分で接続でき、エージェントレスで数百万ワークロードを分析できる。疑わしいリソースを発見した場合は「Quarantine（隔離）」機能を用いてワンクリックで環境から隔離することも可能だ。

もうひとつのIllumio Segmentationは、ハイブリッド環境において統一したポリシーを柔軟に展開し、ラテラルムーブメントを封じ込める機能だ。アプリケーション、ロケーション、ロール、環境の4種のラベルでワークロードを動的にグループ化し、IPアドレスが変わってもセキュリティポリシーが自動追従するため、ファイアウォールやACLの手動更新が不要になる。データセンターやエンドポイントに導入するエージェントはユーザースペースで動作してカーネルには一切触れないため、OSの再起動なし・通信の瞬断なしで導入でき、仮にエージェントに障害が発生しても既存のプロビジョニング済みポリシーに従って通信を継続できる。

前半ハンズオン：3つの演習でリスクを可視化

今回のハンズオンでは、これら2つの製品を実際に体験する構成となっている。前半では「Illumio Insights」を使ったリスクの可視化が行われた。仮想企業のハイブリッドクラウド環境で予期しない異常が次々と浮かび上がるシナリオのもと、参加者はCISOチームの一員として調査にあたった。

演習は、リモートアクセスツールRustDeskへの不審な通信から悪意のあるIPを特定、RDPトラフィックの急増を検知しポリシーの欠落を発見、社外への異常なアウトバウンド通信からデータ窃取の兆候を読み取るという、3つのシナリオで構成。「エントリポイントとなった不審なリモートアクセス→RDPを悪用したラテラルムーブメント→異常なアウトバウンドによるデータ窃取」という攻撃の全体像を、Illumio Insights の画面上でひとつながりのストーリーとして追体験する内容だ。

「本来は止めておくべきサービスが許可された状態

になっていることがあります。セキュリティに自信のある企業でも、こうした盲点が実際のPoC環境で見つかることは珍しくありません」（豊嶋氏）

後半ハンズオン：ポリシーでラテラルムーブメントを封じ込める

ハンズオン後半はセグメンテーション機能の実践に移った。「ランサムウェアのリスク軽減」ではTelnet・RDP・SMBなどリスクの高いプロトコルを一括ブロックするポリシーを、「環境の分離」では開発環境から本番環境へのラテラルムーブメントを防ぐポリシーをそれぞれ構築。プロビジョニング前に影響範囲をマップ上で確認できるドラフトビュー機能により、安心して適用判断できる設計を体感できる内容になっていた。

「シンプルなルール1つで、ハイブリッド環境全体にわたるリスクの高いサービスを止めることができます。まずここから着手することで、ランサムウェアの拡散経路を一気に絞り込めます」（豊嶋氏）

リスクの可視化と封じ込めを往復する今回のハンズオンは、「何が侵入を検知するか」ではなく「検知をすり抜けた攻撃を何が止めるか」という問いに、参加者が自ら手を動かしながら向き合う機会となった。少人数制で講師とインタラクティブに会話をしながら、実際の環境を触ることができるため、製品特徴を短時間で把握できることも本ハンズオンセミナーの魅力となっている。

今後も本ワークショップを開催していく予定であり、次回以降のスケジュールについては、下記のサイトで公開している。

https://www.illumio.com/illumiverse-labs

IIJグローバルが提供する「ソリューションラボ」についてはこちら
https://www.iijglobal.co.jp/service/special/solution-lab01.html

illumio

イルミオジャパン合同会社
〒104-0028 東京都中央区八重洲2-2-1
東京ミッドタウン八重洲 八重洲セントラルタワー 7F
URL：https://www.illumio.com/ja

IIJ Global

株式会社IIJグローバルソリューションズ
E-Mail：info@iijglobal.co.jp
URL：www.iijglobal.co.jp