HITACHI
Inspire the Next

制御システム向けセキュリティアセスメント・ペネトレーションテスト

｜導入事例｜ ロジスティード株式会社（旧 株式会社日立物流）様

LOGISTEED

所在地	東京都中央区京橋二丁目9番2号 ロジスティードビル
設立	1950年2月
従業員数	46,755名（連結：2023年3月末現在）
事業内容	3PL・重量機工・フォワーディングを 主体とした物流業務の包括的受託
URL	https://www.logisteed.com/jp/

※「サイバー/制御系現状分析サービス」は
「制御システム向けセキュリティアセスメント」に名称が変わりました。
※「株式会社日立物流」は2023年4月1日、「ロジスティード株式会社」へ
社名を変更しました。
※本事例内容は公開当時のものです。

物流の現場に即したリスク分析による第三者評価で、安全性をアピール

国内外に700以上もの物流拠点を運営する株式会社日立物流は、最先端の物流センターを対象に「サイバー/制御系現状分析サービス」および「ペネトレーションテスト」を実施。第三者によるセキュリティ課題の洗い出し、対策の実効性を確認することにより、明らかになったリスクに対して対策を行うことで、安心して顧客にサービスを利用してもらえるようになりました。

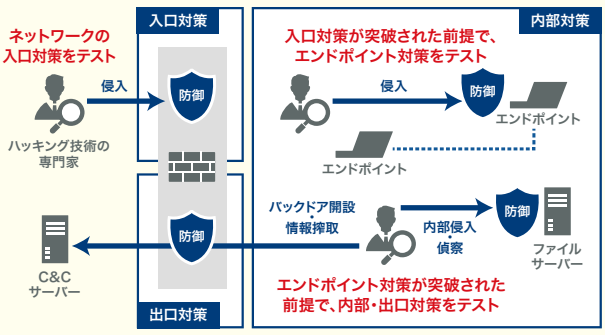
課題	効果
デジタル化の進展で物流の現場における サイバーリスクが高まっている	現場の現状に即したリスク分析にもとづき、 システムの可用性への影響と対策の優先度を把握
自社のセキュリティ対策の実効性を把握したい	ネットワーク内外の脆弱性に関する問題を特定し、 必要なセキュリティ要件を整理
顧客に安全・安心な物流サービスの提供を アピールしたい	第三者による客観的かつ信頼性の高い評価を 安心材料として提供

SOLUTION

網羅的に抽出したリスクへ有効な対策を提示

- 制御システムの可用性への影響に着目した、IPA*1の「制御システムのセキュリティリスク分析ガイド」に沿った分析より、発生し得るセキュリティの脅威とリスクを洗い出し必要な対策を明確化
- 攻撃者の視点での網羅的な「ペネトレーションテスト」により課題を抽出
- 専門性の高い第三者が安全性を客観的に評価することでシステムの信頼性が向上

*1 IPA：独立行政法人 情報処理推進機構



脅威シナリオにもとづいてハッキング技術の専門家が疑似攻撃を実施

株式会社 日立ソリューションズ

| 導入事例 |

ロジスティード株式会社（旧 株式会社日立物流）様 INTERVIEW

背景 デジタル化の進展でサイバー攻撃の脅威が拡大

「広く未来をみつめ 人と自然を大切にし 良質なサービスを通じて 豊かな社会づくりに貢献します」という経営理念のもと、主に3PL*2、重量品の輸送・移設、フォワーディング*3の3つを柱に事業を展開する日立物流グループは、世界に広がるネットワークと先駆者ならではの専門性をいかし、高度化・多様化・広範化するグローバルサプライチェーンにおいて、多様な物流ニーズに包括的に対応するソリューションを提供しています。重要な社会インフラの一つである物流は、昨今、労働力不足やEC市場の拡大といった社会の変化、IoT、AI、ロボスティクスといった技術の進化によりデジタル化が急速に進展しています。そこで懸念されるのがサイバー攻撃です。従来からセキュリティ対策されているIT環境とは異なり、これまでインターネットと繋がらなかったOT（制御システム技術）環境は対策が重視されないことも一般的に多々ありました。しかしデジタル化が進みOT環境もインターネットと接続することが増え、その境界が曖昧になるにつれ、OT環境へのサイバー攻撃が急増しています。さらに手口も多様化・高度化する一方です。

「攻撃の被害による社会的影響は大きく、お客様に安心してご利用していただくためには、お預かりする個人情報の漏洩、出荷データの改ざんといった脅威への対策の強化が重要な課題となっています」（小葉竹氏）

*2 3PL：Third（3rd）Party Logistics　物流業務を第三者企業に委託する業務形態
*3 フォワーディング：国際輸送代理業

取り組み 第三者によるリスクの評価を重視

必要なセキュリティ対策に取り組む一方で「どこまでやれば合格点なのか」「どこにリスクが存在するのか」を自社で判断するには限界があります。

「ご利用を検討されているお客様に対して、当社のセキュリティ対策は万全です、ご安心くださいと言える判断材料として、第三者の評価がほしいと考えていました」（小葉竹氏）

そこで、セキュリティ対策の現状を正しく評価し、適切な改善を進めていくために、同領域で豊富な実績を持つ日立ソリューションズの2つのサービスを実施しました。1つは、システムのセキュリティにどのようなリスクが潜んでいるかを机上で整理する「サイバー/制御系現状分析サービス」。もう1つが実際の攻撃によりネットワークの各階層の強度を確認する「ペネトレーションテスト」です。

国内外に700を超える物流拠点を運営する同社が評価対象に選んだのは、2019年に埼玉県春日部市で本格稼働した「ECプラットフォームセンター」です。複数のEC事業者で省人化設備、物流システム、倉庫内スペース、マンパワーをシェアリングし、コストは従量課金型を採用しています。同社のあらゆる技術とノウハウが凝縮された拠点であり、また複数のお客様の情報を取り扱っていることが評価対象の決め手になりました。

効果 安心感がビジネス拡大の重要なファクターに

「サイバー/制御系現状分析サービス」では、「制御システムのセキュリティリスク分析ガイド」にもとづき、日立ソリューションズの知見を踏まえてアセスメントを実施。リスクの洗い出しと対策の提案を行いました。続いて実施した「ペネトレーションテスト」では、攻撃者目線で攻撃シナリオを組み、本番システムに影響を与えないよう疑似攻撃を行いました。

「ペネトレーションテスト」について、浜田氏は以下のように振り返ります。

「外部からの侵入検査は経験があったのですが、大丈夫だと油断していたネットワークの内部に対して脆弱性を指摘されました。さっそくテスト結果を活用して、暗号化や、ネットワークの接続制限のさらなる強化など、優先順位の高いものから具体的な対策を始めています」

ECプラットフォームセンター長の村上氏も以下のように評価しています。

「実際の現場に即して脅威を想定し、対策を評価してもらえるので安心感が大きいですね。セキュリティはお客様の重要な関心事ですから、こうしたテストをクリアしている事実は、お客様に対して安全性や安心感をアピールできます。当センターを核にビジネスを拡大していくうえでも、セキュリティの確保は重要なファクターになっていくと確信しています」

展望 ノウハウの横展開でセキュリティレベルを底上げ

最初はどのようにシステムのリスクを分析し、テストしていくのかまったく見当がつきませんでしたが、日立ソリューションズの経験値やひな型をいかした提案は分かりやすく、リスクの整理の仕方やテストの進め方について、納得して実施できました。分析およびテストの結果だけではなく、それを導くプロセスにも大きな価値があり、今後の参考になりました。

「今回、日立ソリューションズの協力のもと、春日部のECプラットフォームセンターの安全・安心を確保できました。今回学んだノウハウをほかのシステムでも活用できるよう、当社内の運用ガイドラインの整備を進めるなど、日立物流全体でセキュリティレベルを底上げしていく考えです」（村上氏）

「誰がセキュリティを担保しているのか、第三者に評価してもらっている事実がお客様にとって安心を提供するために重要であることは、これからも変わりません。引き続き日立ソリューションズの知見を借りながら、対応していくことになると思います」（浜田氏）

グローバルサプライチェーンにおいて最も選ばれるソリューションプロバイダをめざす日立物流。同社に対して日立ソリューションズはこれからもセキュリティエキスパートとして、ビジネスの実情に沿った課題解決を提案していきます。

株式会社日立物流
情報セキュリティ本部
部長補佐
小葉竹 満 氏

株式会社日立物流
営業統括本部
営業開発本部
DX・イノベーション部
春日部ECPFセンター
センター長
村上 宏介 氏

日立物流ソフトウェア株式会社
システム事業統括本部
ロジスティクスシステム本部
ICTソリューション部
部長
浜田 正明 氏

本事例のwebページはこちら
www.hitachi-solutions.co.jp/security_consul/case01/

株式会社 日立ソリューションズ
www.hitachi-solutions.co.jp

本カタログ掲載商品・サービスの詳細情報
www.hitachi-solutions.co.jp/security_consul/

J21S-03-03 | 2024.06