Press Release

2026 年 11 月 2 日

報道関係者各位

株式会社 VLC セキュリティ

大久保 修一が株式会社 VLC セキュリティ 副社長 執行役員に就任

～体制づくり・人材育成・技術支援の三つの力で、社会の安心を支える～

株式会社 VLC セキュリティ（東京都港区、代表取締役社長兼 CEO 石原 紀彦、以下「当社」）は、2026 年 11 月 1 日付で、大久保 修一が副社長 執行役員に就任したことをお知らせいたします。

サイバー攻撃の被害は企業の規模や業種を問わず広がっていますが、中堅・中小企業や工場の生産現場では、専門人材や知見の不足から、対策が十分に行き届いていない企業も少なくありません。こうした企業に対策を届けるうえで欠かせないのが、地域や業界でお客様と日々向き合う販売パートナーの存在です。当社は、販売パートナーと手を携えてグループ各社のサービスをより多くのお客様へお届けする体制づくりを進めています。大久保は、サイバーセキュリティ業界で 25 年以上にわたり事業の立ち上げを担ってきた経験を生かし、その中核となる営業体制とブランドの強化を担います。

【大久保 修一プロフィール】



2001 年 4 月　トレンドマイクロ株式会社 入社。大手から中小企業セグメントまで、エンドポイントセキュリティやネットワークセキュリティ、クラウドセキュリティにわたる総合的な対策実装をリードし、産業 IoT・OT 領域のエバンジェリストとして活動。

2020 年 8 月　アイデアラボ 創業・代表（2026 年 3 月まで）。工場のサイバーセキュリティ専門のコンサルティングを手がける。

2021 年 4 月　サイバーリーズン合同会社 入社（アイデアラボ代表と兼務）。広域営業統括本部 執行役員 統括本部長。中堅・中小企業セグメントの事業責任者として EDR・XDR・SOC の国内普及をリード。

2026 年 6 月　株式会社 VLC セキュリティ 入社。戦略推進本部 本部長。

2026 年 11 月　同社 副社長 執行役員（現任）。

【大久保 修一からのコメント】

このたび、副社長 執行役員に就任いたしました。その責任の重さに、身の引き締まる思いです。

セキュリティ対策は、導入して終わりではなく、組織に根づいて初めて力を発揮します。これまで多くのお客様や販売パートナーの皆さまと向き合うなかで、私が学んできたことです。

VLC セキュリティグループには、対策を組織に根づかせるための力がそろっています。それを一社でも多くのお客様に届けられるかは、お客様の身近で信頼を築いてこられた販売パートナーの皆さまとの協働にかかっています。皆さまと同じ目線で課題に向き合い、ともに成長できる関係を大切に、日本のサイバーセキュリティの底上げに努めてまいります。

今後ともご指導ご鞭撻のほど、よろしくお願い申し上げます。

【VLC セキュリティグループについて】

VLC セキュリティグループは、「Go Beyond! JAPAN Cyber Security」のミッションのもと、世界最先端の知見と技術を取り入れた以下 3 つの事業を柱に、日本のサイバーセキュリティの革新を牽引し、社会と産業の発展を支えます。

【VLC セキュリティグループ事業会社】

株式会社 VLC セキュリティコンサルティング

業界スタンダードに基づくセキュリティ体制構築、ISMS や P マークを始めとした認証支援を行うコンサルティング事業

株式会社 VLC セキュリティアリーナ

サイバージム(CYBERGYM)ブランドで提供する、最新の攻撃手法をリアルタイムに反映した実践的で最先端のサイバーセキュリティトレーニング事業

株式会社 VLC セキュリティラボ

AI をはじめとする最先端技術の活用と高度な知識を持ったホワイトハッカーによるセキュリティサービス事業

株式会社 VLC セキュリティ

事業内容：グループ各社を通じたトータルセキュリティソリューションの提供

本　　社：東京都港区虎ノ門 4-1-40　江戸見坂森ビル

代 表 者：代表取締役社長兼 CEO　石原 紀彦

WEB サイト: https://vlcsecurity.com/

【用語説明】

※IoT（Internet of Things）：センサーや家電、機械などのモノをインターネットにつなぎ、データのやり取りや遠隔操作を行う仕組み。
※OT（Operational Technology）：工場の生産設備やビルの制御システムなど、モノを動かし管理する技術。事務用の IT（情報技術）と区別される。
※EDR（Endpoint Detection and Response）：パソコンやサーバーなどの端末を常に監視し、攻撃の兆候を検知して調査・対処する仕組み。
※XDR（Extended Detection and Response）：端末に加え、ネットワーク・クラウド・メールなど複数の領域を横断して攻撃を検知・対処する仕組み。
※SOC（Security Operation Center）：セキュリティ機器の監視とアラートの分析を専門に行い、攻撃の検知と初動対応を担う組織・サービス。
※ホワイトハッカー：攻撃者と同等の高度な技術を、システムの弱点の発見や防御など、守る目的に生かす技術者。
※ISMS（情報セキュリティマネジメントシステム）：組織が情報を守る仕組みを継続的に改善する枠組み。ISO/IEC 27001 に基づく認証制度がある。
※P マーク（プライバシーマーク）：個人情報を適切に扱う体制を整えた事業者を、JIPDEC（日本情報経済社会推進協会）が認定する制度。