SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

Hybrid Zero Trust Architectureにおける機械学習を用いた不正操作の検知
ML Detection Method for malicious operation in Hybrid Zero Trust Architecture

石出 港士 * 岡田怜士 * 吉倉昌利 * 松田亘 †
Koshi Ishide Satoshi Okada Masatoshi Yoshikura Wataru Matuda
藤本万里子 * 満永拓邦 *
Mariko Fujimoto Takuho Mitunaga

キーワード ゼロトラスト ハイブリッド環境 機械学習 異常検知

あらまし

近年、コロナの影響によってリモートワークが広まっているが,VPN 経由での社内環境へのアクセスはネットワーク帯域の負荷も高く,VPN 機器を起点とするサイバー攻撃被害も報告されているため, ゼロトラスト環境の需要は増加している. また企業・組織のセキュリティを取り巻く環境は標的型攻撃に代表されるように攻撃の高度化によって年々厳しさを増している. ゼロトラストアーキテクチャは VPN にかかわる課題やリソースに対するセキュリティリスクを低減することができる.[1] ゼロトラストの導入は着実に進んでいるが, 情報管理の観点から全てのビジネスプロセスと関連データをゼロトラスト環境に適応させることは難しく, 理想的なゼロトラスト環境の導入が困難なケースがある. 例えば企業における機密性の高いデータのクラウド利用がそれにあたる. そのような場合には, ゼロトラストアーキテクチャと既存環境とが共存するハイブリッド環境でビジネスプロセスが行われる. しかしながら, ハイブリッド環境ではサイバー攻撃検知のログがクラウドと既存環境に分散して保管されることとなり, 従来型の検知手法をが適用できない可能性がある. また, 従来の静的なルールベースでは環境依存が強く誤検知が多い. 本稿では, ハイブリッド環境に対する不正なアクセスを機械学習の異常検知アルゴリズムを活用して検知する手法を検討し, 仮想環境でその効果を検証する.

参考文献

[1] NIST,“ZeroTrustArchitecture, Available:https://csrc.nist.gov/publications/detail/sp/800-207/final

* 東洋大学, 〒 115-8650 東京都北区赤羽台 1-7-11 INIAD HUB-1, TOYO University, INIAD HUB-1, 1-7-11 Akabanedai, Kita-ku, Tokyo 115-8650,
† NTT 社会情報研究所, 〒 180-8585 東京都武蔵野市緑町 3-9-11 武蔵野研究開発センタ, NTT Social Informatics Laboratories,3-9-11, Musashinoshi, Midori-ku,180-8585 Tokyo