US 20240214400A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2024/0214400 A1**

Tanaka (43) **Pub. Date: Jun. 27, 2024**

(54) **ABNORMAL COMMUNICATION DISCRIMINATION APPARATUS, ABNORMAL COMMUNICATION DISCRIMINATION METHOD, AND ABNORMAL COMMUNICATION RESPONSE SYSTEM**

(71) Applicant: **Hitachi, Ltd.**, Tokyo (JP)

(72) Inventor: **Mayuko Tanaka**, Tokyo (JP)

(21) Appl. No.: **18/523,207**

(22) Filed: **Nov. 29, 2023**

(30) **Foreign Application Priority Data**

Dec. 22, 2022 (JP) 2022-205896

Publication Classification

(51) **Int. Cl.**
H04L 9/40 (2006.01)
H04L 41/22 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 63/1416*** (2013.01); ***H04L 41/22*** (2013.01); ***H04L 63/1425*** (2013.01)

(57) **ABSTRACT**

Provided is an abnormal communication discrimination apparatus which includes an eventual feature table for the evaluation of each abnormal communication detection event, and a statistical feature table for the evaluation of each condition in which a statistical amount of abnormal communication holds. The abnormal communication discrimination apparatus calculates an eventual evaluation value from each number of records to which the abnormal communication detection events of the eventual feature table are applicable, calculates a statistical evaluation value from each number of records each of which satisfies a condition that a statistical amount of abnormal communication holds, calculates a discrimination result evaluation value by applying a weighted linear sum of the eventual evaluation value and the statistical evaluation value, and performs, on the basis of the discrimination result evaluation value, discrimination of whether abnormal communication is caused by a cyber-attack or by a failure of an apparatus of the monitoring target system.