



1 氏名及び役職名等 (Name and Title)

サンドロ・ガイケン、デジタルソサエティ研究所長 (ESMT ベルリン)、CYDEF 実行委員会副代表

Dr. Sandro Gaycken, Director, Digital Society Institute, ESMT Berlin, Co-President, CYDEF Executive Committee

2 略歴 (CV)

サンドロ・ガイケン博士は ESMT ベルリンのデジタルソサエティ研究所長である。かれは科学研究論文集を 5 冊、60 以上の他の出版物に寄稿している。ガイケン博士はオックスフォード・マーティン校の研究員、ハーバード・MIT グループのサイバー領域の委員、ハーバード・ケネディ校人工知能イニシアチブの上級顧問、仏国大学 CNAM のプロジェクト共同リーダーである。かれは独国の外国サイバー方針戦略、独防衛省のサイバー防衛プロセスの策定を支援し、NATO カウンターインテリジェンス事例研究に専門家として参与した。NATO の SPS 計画の理事として、戦略的サイバー防衛に関する NATO 防衛大学の講師として活躍している。かれは対ハッキング高保証電算機を生み出した HENSOLDT サイバー社、軍事サイバー作戦ツールを開発した GOROOT 社を含む幾つかの企業を創業した。

Dr Sandro Gaycken is director of the Digital Society Institute at ESMT Berlin. He has published five scientific monographs and more than 60 other publications. Dr Gaycken is an Oxford Martin School Fellow, a committee member of the Harvard-MIT group on cyber norms, a Senior Advisor for the AI Initiative at Harvard Kennedy School, and project co-lead at elite French university CNAM. He helped to create Germany's foreign cyber policy strategy, the German MoD's cyber defense process, he serves as an expert witness in NATO counterintelligence cases, as director in NATO's SPS program and a lecturer at the NATO Defense College for strategic cyberdefense. He also founded a number of companies, including HENSOLDT CYBER Ltd., producing unhackable high assurance embedded computers, and GOROOT Ltd., developing military cyber operation tools.

3 参加枠 (Time Slot)

APR 4, 1115-1145 Key Note Speech

APR 4, 1420-1450 Tr.12: Lecture 2

APR 4, 1630-1800 Tr.12: Panel Discussion

APR 5, 1620-1805 Tr.24: Group Discussion

4 講義要約 (Abstract)

基調講演: 戦略的サイバー防衛

今後はサイバー防衛を確立することが些末な問題ではないことを知るべきだ。古い技術や手法はもう役に立たない。現実的かつ信頼できるサイバー防衛とは、技術レベル、専門家、そして構築を担当するサプライヤに対して確実な構造的変化を求める。そのためサイバー防衛は恐るべき戦略的挑戦となっている。

Tr.12: サイバー防衛のための高度技術

多数の高度技術が技術的サイバー防衛に新たな概観を与えた。しかし、それは最初に産業界に努力を強いることになる。二つの傑出した試みに焦点を当てて説明しよう。それは移動目標の防衛と高保証技術であり、独産業界における工業化の試みを説明する。

Key Note Speech: "Strategic Cyberdefense"

By now, we know that building cyberdefense is far from trivial. Old technologies and processes don't work anymore and have to be considered outdated. Real reliable cyberdefense requires substantial architectural change on the technical level, expertise and suppliers have to be built. This makes cyberdefense a formidable strategic challenge.

Track 12: Advanced Technologies for Cyberdefense

A number of advanced technologies provide new outlooks for technical cyberdefense, but require industrialization efforts first. The talk will highlight two novel approaches such as moving target defense and high assurance technologies and explain some efforts of industrialization in the German industries.