

サイバーセキュリティとシグント機関 ～NSA 他 UKUSA 諸機関の取組～

＜目次＞	・ ・ ・ ・	31-93 頁
1 初めに	・ ・ ・ ・	31
2 サイバーセキュリティとシグント機関の関係	・ ・ ・ ・	32
2.1 サイバーセキュリティに対するシグント機関の任務と係わり		
2.2 米国・国家安全保障庁 NSA (National Security Agency)		
2.3 英国・政府通信本部GCHQ (Government Communications Headquarters)		
2.4 カナダ・通信保全局 CSE (Communications Security Establishment)		
2.5 オーストラリア信号局 ASD (Australian Signals Directorate)		
2.6 NZ 政府通信保全局GCSB (Government Communications Security Bureau)		
2.7 SC に貢献するシグント機関の能力基盤		
3 NSA の概観とシグント・システム	・ ・ ・ ・	42
3.1 NSA 概観		
3.2 NSA のシグント収集態勢		
3.3 シグント収集態勢：協力企業と協力国		
3.4 シグント収集態勢：主要収集プラットフォーム		
3.5 CS に特に有用なシグント・システム		
4 CNE の技法	・ ・ ・ ・	48
4.1 TAO (Tailored Access Operation)		
4.2 遠隔侵入(remote subversion, remote access, on-net)		
4.3 物理的侵入 (physical subversion、close access)		
4.4 各種機材開発		
4.5 オンライン秘匿活動 (積極工作)		
5 シグント機関による CS への貢献	・ ・ ・ ・	58
6 指導助言・情報提供	・ ・ ・ ・	58
7 CS に関する教育・研究	・ ・ ・ ・	60
8 情報システムの構築管理	・ ・ ・ ・	62
9 事案対応	・ ・ ・ ・	63
10 攻撃者の探知特定 (attribution)	・ ・ ・ ・	64
11 積極防禦 (Active Cyber Defense)	・ ・ ・ ・	67
12 制裁とサイバー作戦	・ ・ ・ ・	75
13 結語	・ ・ ・ ・	81
＜補論＞ 対中国サイバーセキュリティ対策の話題		
1. 中国による産業スパイ・サイバー攻撃対策 attribution	・ ・ ・ ・	83
2 華為問題 (中国による Supply Chain Operation)	・ ・ ・ ・	86