

※5：情報セキュリティポリシー

2019.07.31

1.	概要	1.1.	事業目的	本研究会は、立坑・トンネル構築技術の標準化を図り発注者・受注者間の情報共有と公開を進め、シーズとして実用新案を含む特許技術（以下まとめて「特許技術」という。）を提供する特許権者及び、特許技術のフィールドワークの場として工事を施工する建設会社及び、特許技術に係る製品を当該建設会社に製造・販売する製造会社の、相互の互惠を図ることを目的とする。
		1.2.	情報管理の概要	本研究会の情報管理は、「友の会入会契約、特許に関する契約実務等」に関する事項は研究会管理会社、また、「全体運営、特許に関しない契約実務等」に関する事項は代表幹事会社がそれぞれ分担し、これら全ての情報管理は、本「情報セキュリティポリシー」並びに従属文書の「情報セキュリティ対策」に基づく。
		1.3.	本ポリシーの目的	本研究会は業務の遂行に当たり、情報セキュリティを確保し情報資産を保全し、非公開や秘密情報の漏洩を防ぐため、情報管理に係る基本事項を本「情報セキュリティポリシー」に定める。
2.	遵守事項	2.1.	法令等の遵守	本研究会は業務を遂行するにあたり、情報セキュリティに関わる法令、その他の規定類を遵守する。
		2.2.	契約上の義務等の遵守	本研究会は、情報管理において各会員会社との契約内容並びに本「情報セキュリティポリシー」並びに従属文書の「情報セキュリティ対策」を遵守する。
3.	情報資産の保護	3.1.	契約当事者の管理	本研究会の契約当事者は、契約情報などの情報資産を不正アクセスや秘密漏洩から守るため、それぞれの契約上の責任と義務を果たす。
		3.2.	固有の情報は非公開	本研究会は、公開する情報は一般的な内容のみとし、会員情報（社名、所属部会等）の場合を除く会社情報、該当工事など固有の情報は非公開とし、応募者の秘密を守る。
		3.3.	情報資産のレベル別管理	本研究会の情報資産は、「契約書類」「研究会管理会社、代表幹事会社管理書類」「部会資料」「研究会共通資料」「研究会公開資料」の各書類分類に対する、それぞれの秘密レベルにて閲覧許諾者を制限する。
4.	情報セキュリティの体系	4.1.	情報セキュリティ対策	本ポリシーのもとに、情報資産を体系的に管理し、その保護を実効性のあるものとするため、従属文書の「情報セキュリティ対策」を策定する。
5.	組織体制	5.1.	情報資産総括責任者	代表幹事は、情報資産総括責任者として、情報セキュリティに関する統括組織である「情報セキュリティ対策本部」を設置し、本研究会を統括し、本研究会の情報資産のセキュリティ対策を推進する。
		5.2.	情報資産の部会別管理	各会員会社は、所属の各工法部会毎あるいは各製品部会毎に管理する情報を、それぞれの秘密レベルにて閲覧でき、かつ、秘密保持の義務を負う。
6.	監査	6.1.	点検・監査	情報資産総括責任者は、各部会の本「情報セキュリティポリシー」に関する遵守状況について、各部会を定期的に点検・監査し、必要に応じ適正な是正処置を講じさせ、従属文書の「情報セキュリティ対策」を維持更新する。
7.	セキュリティマネジメント	7.1.	各会員の信頼の醸成	情報資産総括責任者は、技術の進歩、事業環境の変化を考慮しつつ、監査結果を踏まえ、継続的に本研究会各部会への教育を実施し、各会員会社相互の信頼醸成と高品質の業務環境の保全を図る。