先端科学技術研究科　修士論文要旨

所属研究室 （主指導教員）	サイバーレジリエンス構成学 （門林　雄基　（教授））		
学籍番号	2311294	提出日	令和 7年 1月 20日
学生氏名	山田　裕彌		
論文題目	メモリアクセス情報を活用したハッシュ化処理特定に基づくAPI ハッシュ難読化解除手法		

要旨

マルウェア解析において静的解析（コード解析）は，マルウェアの構造や機能を詳細に調べるために不可欠な解析方法である．しかし，静的解析は難読化と呼ばれるコードの意味を保ちながら，可読性を低下させるテクニックの影響を受けやすく，静的解析は困難になることが多い．特にAPIハッシュ難読化マルウェアは，使用するWindows API名をハッシュ化することで隠蔽するため，API名を起点にした静的解析が困難である．このAPIハッシュ難読化の対策手法として，API名とハッシュ値から構成されるデータベースを検索し難読化を解除する手法が広く知られているが，データベースにないアルゴリズムには対応できないという制約がある．そこで本研究では，マルウェアのメモリアクセス情報を活用することで，マルウェアに埋め込まれているハッシュ関数を自動で特定し，データベースを構築する手法を提案する．さらに，提案手法は構築したデータベースを参照することで，マルウェア内に埋め込まれた難読化（ハッシュ値）をAPI名に解除する．提案手法を2つの疑似マルウェアとContiランサムウェアを用いて評価した結果，APIハッシュ難読化マルウェアに対して有効性が確認された．