様 式 Ｃ－７－１

平成２１年度科学研究費補助金実績報告書（研究実績報告書）

1. 機 関 番 号 | 1 | 4 | 6 | 0 | 3 |　　2. 研究機関名　奈良先端科学技術大学院大学

3. 研 究 種 目 名　基盤研究（C）　　4. 研究期間　平 成 １９ 年 度 ～ 平 成 ２１年 度

5. 課 題 番 号 | 1 | 9 | 5 | 0 | 0 | 0 | 5 | 6 |

6. 研 究 課 題 名　プログラム難読化適用のフレームワーク

7. 研 究 代 表 者

研究者番号	研究代表者名	所属部局名	職名
80311786	フリガナ モンデン アキト 門田 暁人	情報科学研究科	准教授

8. 研究分担者(所属研究機関名については、研究代表者の所属研究機関と異なる場合のみ記入すること。)

研究者番号	研究分担者名	所属研究機関名・部局名	職名
	フリガナ		
	フリガナ		
	フリガナ		
	フリガナ		
	フリガナ		

9. 研究実績の概要

下欄には、当該年度に実施した研究の成果について、その具体的内容、意義、重要性等を、交付申請書に記載した「研究の目的」、「研究実施計画」に照らし、600 字～800 字で、できるだけ分かりやすく記述すること。また、国立情報学研究所でﾃﾞｰﾀﾍﾞｰｽ化するため、図、ｸﾞﾗﾌ等は記載しないこと。

本年度は，実用システムへの適用を想定し，難読化フレームワークにおけるゴール木の構築について，より実用的なガイドラインを提案した．また，提案したガイドラインを実用システムに適用し，その効果を評価した．

提案したガイドラインでは，秘密情報とその手がかりの関係，および，手がかり間の関係を，(1)部分-全体，(2)抽象-具体，(3)その他，の3つに分類し，Unified Modeling Languageのクラス図の記法により表現する．クラス図の作成にあたっては，手がりを3つの抽象レベル（アルゴリズム，ソースコード，機械語）に分けて記述する．これによって，手がかり間の関係が分かりやすくなるとともに，異なる抽象レベルの手がかりを網羅的に列挙しやすくなることが期待される．

提案したガイドラインの評価を目的として，C2(Cryptomeria Cipher)暗号プログラムにおいてラウンド鍵を隠蔽するケースを想定し，ガイドラインに基づくゴール木の作成を行った．その結果，従来の方法では抜けていた手がかりを列挙できており，また，クラス図の記法によって手がかり間の関係をより明確にできていることを確認した．このことから，提案ガイドラインを用いることで，難読化によって手がかりを隠蔽するのみならず，手がかり間の関係を隠蔽することが可能となり，より攻撃耐性のあるソフトウェアシステムの構築が可能となった．

10. キーワード

(1) ソフトウェア保護	(2) セキュリティ	(3) ソフトウェア開発
(4) 秘密情報	(5)	(6)
(7)	(8)	

（裏面に続く）

11.研究発表（平成２１年度の研究成果）

〔雑誌論文〕　計（ ３ ）件　　うち査読付論文　計（ ０ ）件

著　者　名	論　　文　　標　　題			
神崎雄一郎, 門田暁人	実行時間差に着目したコードの隠ぺい方法			
雑　　誌　　名	査読の有無	巻	発 行 年	最初と最後の頁
第8回情報科学技術フォーラム講演論文集	無	第1分冊	2009	361-364

著　者　名	論　　文　　標　　題			
山内寛己，門田暁人，松本健一	実行系列差分攻撃によるプログラムの耐タンパー性評価			
雑　　誌　　名	査読の有無	巻	発 行 年	最初と最後の頁
奈良先端科学技術大学院大学情報科学研究科テクニカルレポート	無	NAIST-IS-TR2009007	2009	1-15

著　者　名	論　　文　　標　　題			
牛窓朋義,門田暁人,玉田春昭,松本健一	使用クラスに基づくソフトウェアの機能面からの分類			
雑　　誌　　名	査読の有無	巻	発 行 年	最初と最後の頁
電子情報通信学会技術報告	無	Vol.109, No.170	2009	31-36

〔学会発表〕計（ ０ ）件　　うち招待講演　計（ ０ ）件

発　表　者　名	発　　表　　標　　題		
学　会　等　名	発表年月日	発　表　場　所	

〔図　書〕　計（ ０ ）件

著　者　名	出　版　社		
書　　名		発 行 年	総ページ数

12. 研究成果による産業財産権の出願・取得状況

〔出　願〕　　計（ ０ ）件

産業財産権の名称	発明者	権利者	産業財産権の種類、番号	出願年月日	国内・外国の別

〔取　得〕　　計（ ０ ）件

産業財産権の名称	発明者	権利者	産業財産権の種類、番号	取得年月日	国内・外国の別

13. 備考

※　研究者又は所属研究機関が作成した研究内容又は研究成果に関するｗｅｂページがある場合は、ＵＲＬを記載すること。
