所属：熊本高等専門学校　電子情報システム工学系

研究タイトル：

Man-At-The-End 攻撃に対するソフトウェアの保護

氏名：	神﨑雄一郎 ／KANZAKI, Yuichiro	E-mail：	kanzaki@kumamoto-nct.ac.jp
職名：	准教授	学位：	博士(工学)
所属学会・協会：	電子情報通信学会，情報処理学会		

キーワード：	ソフトウェア保護，プログラムコードの難読化
技術相談 提供可能技術：	・ソフトウェア内部の重要な情報をプログラムコードの難読化によって保護する技術 ・ソフトウェアの解析の困難さを評価する技術

研究内容：プログラムコードの難読化によるソフトウェア保護方法とその有効性評価

Man-At-The-End 攻撃からソフトウェアを保護することを目的としたプログラムコードの難読化方法や，難読化方法の有効性の評価方法について研究を行っている．

ソフトウェアに対する Man-At-The-End 攻撃（MATE 攻撃）とは？

ソフトウェアの実行可能コードを物理的に所有するエンドユーザが，そのコードを解析・改ざんする行為のこと[1]．

MATE 攻撃の例：
- ソフトウェア内の価値あるコードの解析・抜き取り
- ソフトウェア内の重要な分岐点（例えばライセンスチェック機構）の改ざん

MATE のシナリオにおける攻撃者と防御者

攻撃者（attacker）
ゴール：ソフトウェア内の重要なコードやデータを発見し，抽出・改ざんする
道具：逆アセンブラ，デバッガなど

VS

防御者（defender）
ゴール：攻撃者の攻撃成功を可能な限り遅らせる
道具：プログラムコードの難読化など

プログラムコードの難読化

MATE 攻撃を妨げる方法として，コードの意味を保ったまま人間や機械にとって解析が困難なコードに変形する「プログラムコードの難読化」がある．様々な難読化方法やツールが提案されている[2]．

我々の研究グループでは，動的難読化[4]など，難読化方法の研究に取り組んでいる．

```
if ((int )((unsigned long )(((((current_time - tmp)
& - (current_time >= tmp)) + ((current_time - tmp) &
- (current_time >= tmp))) & (((current_time - tmp) &
- (current_time >= tmp)) >> 63L)) - ((current_time -
tmp) & - (current_time >= tmp))) >> 63UL))
                :
```

Tigress[3]によって難読化された C 言語のコード（一部）の例

難読化方法の有効性評価

難読化方法の有効性を把握するには，難読化されたコードの理解の困難さ，逆難読化の困難さ，目立ちにくさなど，様々な観点からの評価指標が必要であるといわれている[2]．

我々の研究グループでは，難読化されたコードの目立ちにくさの評価方法の提案[5]などを行っている．

参考文献

[1] P. Falcarin, C. Collberg, M. Atallah, M. Jakubowski. Software Protection (Guest Editors' Introduction). IEEE Software, Special Issue on Software Protection (March/April 2011), 28, 24-27.
[2] C. Collberg and J. Nagra: Surreptitious Software: Obfuscation, Water-marking, and Tamperproofing for Program Protection. Addison-Wesley Professional, 2009.
[3] C. Collberg, The tigress C obfuscator, https://tigress.wtf/.
[4] 神﨑雄一郎，門田暁人，中村匡秀，松本健一：命令のカムフラージュによるソフトウェア保護方法，電子情報通信学会論文誌，Vol. J87-A, No. 6, pp. 755-767, June 2004.
[5] 神﨑雄一郎，尾上栄浩，門田暁人：コードの「不自然さ」に基づくソフトウェア保護機構のステルシネス評価，情報処理学会論文誌，Vol.55, No.2, pp.1005-1015, Feb. 2014.