# 侵入の痕跡（IoC: Indicators Of Compromise）一覧

「米国の重要インフラを狙う継続中のPLC悪用攻撃について連邦機関が警告」（TrendAI™ Research、2026年7月23日）に関する侵入の痕跡（IoC）です。CISAの情報に基づくものであり、TrendAI Vision One™ プラットフォームによって検出・ブロックされます。

## URLおよびIPアドレス

| IoC | 検出名 |
|---|---|
| 185.82.73[.]175 | 91 - C&C server |
| 141.11.164[.]153 | 91 - C&C server |
| 175.110.121[.]42 | 91 - C&C server |
| 175.110.121[.]39 | 91 - C&C server |
| 175.110.121[.]41 | 38 - Computers/Internet |
| 175.110.121[.]107 | 91 - C&C server |
| 192.142.54[.]79 | 38 - Computers/Internet |
| 84.200.205[.]165 | 38 - Computers/Internet |
| 185.225.17[.]225 | 91 - C&C server |
| 79.133.46[.]209 | 91 - C&C server |
| 88.80.150[.]199 | 91 - C&C server |
| 88.80.150[.]200 | 91 - C&C server |
| 88.80.150[.]202 | 91 - C&C server |
| 185.82.73[.]162 | 91 - C&C server |
| 185.82.73[.]164 | 91 - C&C server |
| 185.82.73[.]165 | 91 - C&C server |
| 185.82.73[.]167 | 91 - C&C server |
| 185.82.73[.]168 | 91 - C&C server |
| 185.82.73[.]170 | 91 - C&C server |
| 185.82.73[.]171 | 91 - C&C server |
| 135.136.1[.]133 | 91 - C&C server |
| ocferda[.]com | 91 - C&C server |
| uuokhhfsdlk[.]tylarion867mino[.]com | 91 - C&C server |
| tylarion867mino[.]com | 91 - C&C server |

## ファイルハッシュ

| IoC | 検出名 |
| --- | --- |
| 366e435a1ea0f597deb6ebe7c0c5acdb6e8b33eb | Backdoor.Linux.IOCONTROL.CIGBCBF |
| 95bd07b4400095acdafce05888da27228d7d07ca | Trojan.Win64.MALPDB.A |

出典：Federal Agencies Warn of Ongoing PLC Exploitation Against Critical U.S. Infrastructure（英語）／CISA共同アドバイザリ AA26-097A（英語）