This thesis identifies issues of process monitoring on Windows NT operating systems family and describes our implementation of an infrastructure for process monitoring. The system comprises of a core component and user defined external modules. The kernel component hooks system functions and redirects calls to the external modules running in the user space. The core component dispatches the calls to user supplied external modules that take care of the call processing. The core component defines simple API for the external modules that does not require deep knowledge of kernel programming. Moreover, this architecture simplifies versioning of the external modules. It makes them independent of a particular kernel build as long as the Windows kernel API they are monitoring is preserved. The thesis also compares our work with similar existing software and outlines future directions of development. Source codes and an executable compilation of the software are available on the attached CD. The software uses a part of GNU C Library.