

ABSTRACT

The present invention relates to a method of detecting the alteration of the driver of a windows kernel and a system using system module information that is the
5 unalterable information of the windows kernel.

The method of detecting the alteration of a windows kernel according to the present invention includes a first step of reading, by an alteration detection driver, information about a name and start and end addresses of a
10 detection target driver from system module information; a second step of extracting a function that is used by a driver object of the detection target driver using the name of the detection target driver; and a third step of determining that the detection target driver has not been
15 altered if an address of the function is a value between the start address and the end address, and determining that the detection target driver has been altered if the address of the function is not a value between the start address and the end address.