CLAIMS

1. An information processing device comprising:

a monitoring unit configured to monitor at least a Syscall instruction to pass processing to a kernel of an OS among instructions issued to a processor, and monitor, as a privilege level fault, an access to request for rewriting of a register in which a hook condition is set, in a Model Specific Register, the hook condition being for hooking issuance of the Syscall instruction and prevent rewriting, the monitoring unit including a hook condition setting unit to set the hook condition to the register in the Model Specific Register, the hook condition setting unit including: a hook condition monitoring unity configured to monitor an access to request for rewriting the hook condition; and a hook condition correction unit configured to correct the hook condition every time issuance of the access to request for rewriting the hook condition is detected; and

a load unit configured to load a monitoring software functioning as the monitoring unit at a predetermined region of a main memory, the monitoring software having a privilege level set higher than a privilege level of the kernel of the OS, the load unit including: a first load unit configured to perform loading of the monitoring software after loading of

BIOS; and a second load unit included in the monitoring software loaded by the first load unit, the second load unit being configured to perform loading of the kernel of the OS after loading of the monitoring software.

2. The information processing device according to claim 1, wherein the hook condition correction unit, after correcting the hook condition, issues an instruction to return control to the kernel of the OS.

3. The information processing device according to claim 1 or 2, wherein

the monitoring unit includes:

a detection unit configured to detect issuance of the Syscall instruction;

an evaluation unit configured to evaluate validity of the Syscall instruction detected; and

a proxy processing unit configured to execute the Syscall instruction by proxy in accordance with an evaluation result.

4. The information processing device according to claim 3, wherein the detection unit detects the Syscall instruction as an invalid opcode fault.

5. The information processing device according to claim 3 or 4, wherein

the evaluation unit evaluates validity based on collation with information on an API making up the Syscall instruction.

6. The information processing device according to any one of claims 3 to 5, wherein

the proxy processing unit is configured to, when the evaluation unit determines that the Syscall instruction is valid, transfer content identical with the Syscall instruction to the kernel, and when the evaluation unit determines that the Syscall instruction is invalid, return an instruction to end the Syscall instruction to the kernel.

7. The information processing device according to any one of claims 3 to 5, wherein

the proxy processing unit is configured to, when the evaluation unit determines that the Syscall instruction is valid, transfer content identical with the Syscall instruction to the kernel, and when the evaluation unit determines that the Syscall instruction is invalid, return an instruction to skip the Syscall instruction to the kernel.

8. The information processing device according to any one of claims 1 to 7, wherein the first load unit is configured to load the monitoring software functioning as the monitoring unit at privilege level 0, and the second load unit is configured to load the kernel of the OS at any one of privilege levels 1 and 2.

9. The information processing device according to claim 3, wherein the proxy processing unit executes the Syscall

instruction by proxy irrespective of validity of an evaluation result.

10. The information processing device according to claim 1, wherein the hook condition correction unit is configured to rewrite a hook condition in the register in the Model Specific Register when rewriting of the hook condition in the register is detected.

11. A method for monitoring information processing, comprising:

a Syscall instruction monitoring step of monitoring at least a Syscall instruction to pass processing to a kernel of an OS among instructions issued to a processor,

a hook condition monitoring step of monitoring, as a privilege level fault, an access to request for rewriting of a register in which a hook condition is set, in a Model Specific Register, the hook condition being for hooking issuance of the Syscall instruction and preventing rewriting, the hook condition monitoring step including a hook condition setting step of setting the hook condition to the register in the Model Specific Register, the hook condition setting step including: a hook condition monitoring step of monitoring the access to request for rewriting the hook condition; and a hook condition correction step of correcting the hook condition every time issuance of the access to request for rewriting the hook

condition is detected; and

a loading step of loading a monitoring software functioning as the instruction monitoring and the hook condition monitoring at a predetermined region of a main memory, the monitoring software having a privilege level set higher than a privilege level of the kernel of the OS, the loading step including: a first loading step of loading of the monitoring software after loading of BIOS; and a second loading step included in the monitoring software loaded at the first loading step, the second loading step being to perform loading of the kernel of the OS after loading of the monitoring software.

12. A computer readable recording medium that records a program to make a processor function as:

a monitoring unit configured to monitor at least a Syscall instruction to pass processing to a kernel of an OS among instructions issued to the processor, and monitor, as a privilege level fault, an access to request for rewriting of a register in which a hook condition is set, in a Model Specific Register, the hook condition being for hooking issuance of the Syscall instruction and prevent rewriting, the monitoring unit including a hook condition setting unit to set the hook condition to the register in the Model Specific Register, the hook condition setting unit including: a hook condition monitoring unit configured to monitor an access to request for

rewriting the hook condition; and a hook condition correction unit configured to correct the hook condition every time issuance of the access to request for rewriting the hook condition is detected; and

a load unit configured to load a monitoring software functioning as the monitoring unit at a predetermined region of a main memory, the monitoring software having a privilege level set higher than a privilege level of the kernel of the OS, the load unit including: a first load unit configured to perform loading of the monitoring software after loading of BIOS; and a second load unit included in the monitoring software loaded by the first load unit, the second load unit being configured to perform loading of the kernel of the OS after loading of the monitoring software.